AXIS D2210-VE Radar

ユーザーマニュアル

目次

インストール....4
検討事項....4
製品の取り付け場所....4
複数のレーダーを設置....5
レーダープロファイル....7
エリア監視プロファイル....7
カバー範囲....7
エリア検知範囲....7
エリア設置例....8
エリア監視の使用例....9
道路監視プロファイル....10
道路検知範囲....10
道路設置例....10
道路監視の使用例....12
使用に当たって....14
ネットワーク上のデバイスを検索する....14
ブラウザーサポート....14
装置のwebインターフェースを開く....14
管理者アカウントを作成する....14
安全なパスワード....15
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....15
webインターフェースの概要....15
デバイスを構成する....16
レーダープロファイルの選択....16
取り付け高さの設定....16
参照マップを使用してキャリブレーションを行う....16
検知ゾーンの設定....17
シナリオの追加....18
除外範囲の追加....19
誤報を最小限に抑える....19
レーダー画像の調整....20
画像オーバーレイを表示する....20
テキストオーバーレイを表示する....21
ビデオを表示する、録画する....21
帯域幅とストレージ容量を削減する....21
ネットワークストレージを設定する....22
ビデオを録画して見る....22
イベントのルールを設定する....22
アクションをトリガーする....22
動きが検知されたときにカメラからビデオを録画する....23
車両の逆走時にカメラからのビデオを録画する....23
レーダーで流れる赤のライトを有効にする....25
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....25
動きが検知されたときに照明を点灯する....26
レーダーでPTZカメラを制御する....27
MQTTを使用してレーダーデータを送信する....28
webインターフェース....30
ステータス....30
レーダー....31
設定....31
ストリーム....33
マップキャリブレーション....33
除外範囲....34

シナリオ 35
オーバーレイ 36
動的LEDストリップ 38
レーダーPTZオートトラッキング: 38
録画 39
アプリ 41
システム 41
時刻と位置 41
ネットワーク 43
セキュリティ 47
アカウント 53
イベント 55
MQTT 60
ストレージ 63
ストリームプロファイル 65
ONVIF 66
検知器 69
アクセサリー 69
エッジツーエッジ 69
ログ 70
プレイン設定 71
メンテナンス 72
メンテナンス 72
トラブルシューティング 73
インストールの検証 74
レーダーの設置を検証する 74
検証を完了する 75
詳細情報 76
ストリーミングとストレージ 76
ビデオ圧縮形式 76
ビットレート制御 76
オーバーレイ 78
仕様 79
製品概要 79
LEDインジケーター 79
..... 79
SDカードスロット 80
ボタン 80
コントロールボタン 80
コネクター 80
ネットワークコネクター (PoE入力) 80
ネットワークコネクター (PoE出力) 80
I/Oコネクター 81
電源コネクター 82
装置を清掃する 83
トラブルシューティング 84
工場出荷時の設定にリセットする 84
AXIS OSの現在のバージョンを確認する 84
AXIS OSをアップグレードする 84
技術的な問題、ヒント、解決策 85
パフォーマンスに関する一般的な検討事項 86
サポートに問い合わせる 86

インストール

このビデオでは、レーダーの取り付け方法の例を示します。

すべての設置シナリオの詳細な手順と重要な安全情報については、*axis.com/products/axis-d2210-ve-radar/support*でインストールガイドを参照してください。

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

検討事項

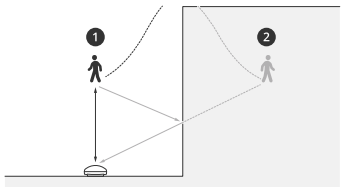
製品の取り付け場所

エリアまたは道路の監視

レーダー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。レーダーには2つのプロファイルがあり、それぞれが各シナリオ用に最適化されています。検知範囲、設置例、使用例の詳細については、を参照してください。

固形物や反射物を避ける

対象範囲内のほとんどの固体 (壁、フェンス、木、大きな茂みなど) には、その背後に死角 (レーダー陰) が生じます。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。



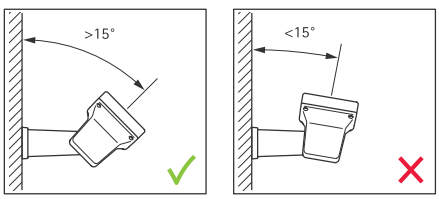
1 実際の検知
2 反射の検知 (ゴースト追跡)

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。

位置決め

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、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。

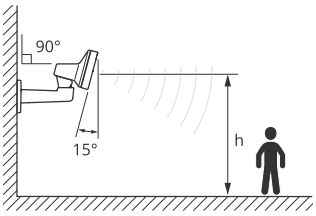


ロール角度

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

チルト角度

レーダーは0～30°チルトできますが、装置の推奨取り付けチルトは15°です。15°のチルトに調整するために、図のように、シャーシの背面部分が水平になっていることを確認してください。



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。手順については、を参照してください。

共存

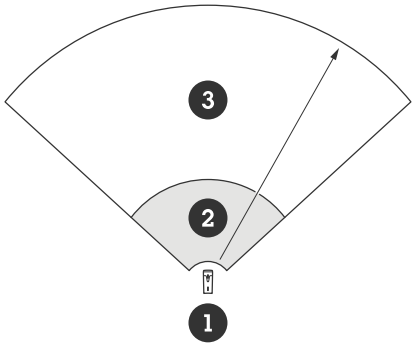
60 GHzの周波数帯域で動作する8台を超えるAxisレーダーを互いに近くに取り付けると、互いに干渉する可能性があります。干渉を避けるには、を参照してください。

複数のレーダーを設置

複数のレーダーを設置し、建物の周囲やフェンスの外側のバッファゾーンなどのエリアをカバーできます。

共存

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。

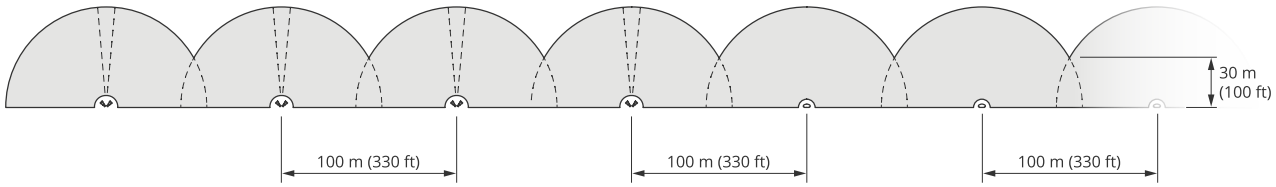


1 レーダー
2 検知領域
3 共存ゾーン

このレーダーは60 GHzの周波数帯域で動作します。60 GHz帯のレーダーは、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。

異なる周波数帯で動作するAxisレーダーは互いに干渉しません。たとえば、AXIS D2210-VEと24 GHzの周波数帯で動作する複数のAXIS D2110-VE Security Radarを組み合わせても、互いに干渉しません。



4組のAXIS D2210-VEと複数のAXIS D2110-VE Security Radarが横に並べて取り付けられている。

注

2台を超えるAXIS D2110-VEを同じ共存ゾーンに取り付ける場合は、AXIS D2110-VE Security Radarには追加の設定が必要です。詳細については、*AXIS D2110-VE Security Radarユーザーマニュアル*を参照してください。

環境

周辺環境、揺らめいている物体、旗竿、揺らめいている植物など、サイトに複数のレーダーを配置する際に確認する他の設計要素もあります。誤報を避けるために、レーダーストリームからフィルターで揺らめいている物体の除外が必要な場合があります。

レーダープロファイル

レーダーはエリア監視または道路監視に使用できます。それぞれのシナリオ用に最適化された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**: 55 km/h (34 mph)未満の速度で移動する人物、車両、不明の物体を追跡するために使用します。
- **道路監視プロファイル**。主に200 km/h (125 mph)までの速度で走行する車両を追跡するために使用します。

レーダーの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。

エリア監視プロファイル

エリア監視プロファイルは、最大55 km/hで移動する物体用に最適化されます。このプロファイルを使用すると、物体が人物、車両、または不明であるかを検知できます。これらの物体のいずれかが検知されたときにアクションをトリガーするようにルールを設定できます。高速で移動する車両を追跡するには、を使用します。

カバー範囲

AXIS D2210-VE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

レーダーが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。

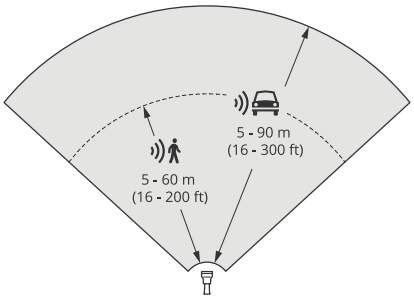
エリア検知範囲

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。

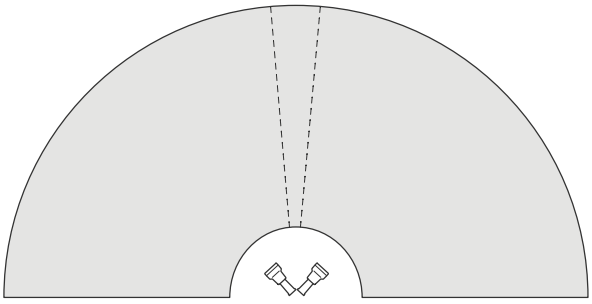
取り付け位置の高さ	チルト0°	チルト5°	10° 傾き	チルト15°	チルト20°	チルト25°	チルト30°
3.5 m (11 ft)	6.0～60+ m (19～196 + ft)	5.0～60+ m (16～196 + ft)	4.0～60+ m (13～196 + ft)	4.0～60 m (13～196 ft)	4.0～55 m (13～180 ft)	4.0～40 m (13～131 ft)	4.0～30 m (13～98 ft)
4.5 m (14 ft)	6.0～60+ m (19～196 + ft)	6.0～60+ m (19～196 + ft)	5.0～60+ m (16～196 + ft)	4.0～60+ m (13～96+ ft)	4.0～60 m (13～196 ft)	4.0～45 m (13～147 ft)	4.0～40 m (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。

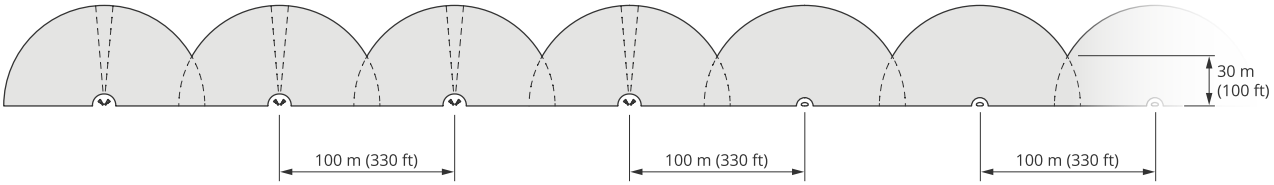
エリア設置例

例えば、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、最大8台のAXIS D2210-VE Radarを横に並べて配置できます。2台のAXIS D2210-VEを隣り合わせに配置すると、180°の範囲をカバーできます。



2台のAXIS D2210-VEを横に並べて取り付けると、180°の範囲をカバーできます。

2組以上のAXIS D2210-VEを横に並べて設置する場合は、各組の間隔を100 mあけて配置することをお勧めします。



4組のAXIS D2210-VEと複数のAXIS D2110-VE Security Radarが100 m (330 ft)の間隔で取り付けられている。

異なる周波数帯で動作するAxisレーダーは互いに干渉しません。つまり、60 GHzの周波数帯で動作するAXIS D2210-VEと、24 GHzの周波数帯で動作するAXIS D2110-VE Security Radarを同じ共存ゾーンで組み合わせることができます。

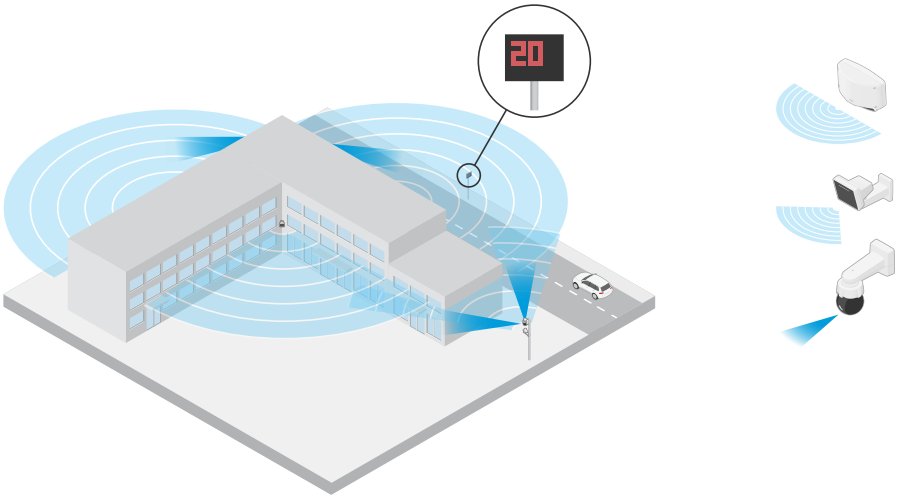
共存と干渉の詳細については、を参照してください。

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、レーダーとPTZカメラを組み合わせて設置しています。建物の長辺をカバーするために180°をカバーするAXIS D2110-VE Security Radarを使用し、短辺と角をカバーするために95°をカバーするAXIS D2210-VE Radarを使用しています。勤務時間外に人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を設定しています。侵入の疑いがある人を映像により確認するために、2台のPTZカメラを追加しています。レーダーは*AXIS Radar Autotracking for PTZ*を通じてPTZカメラを誘導できます。

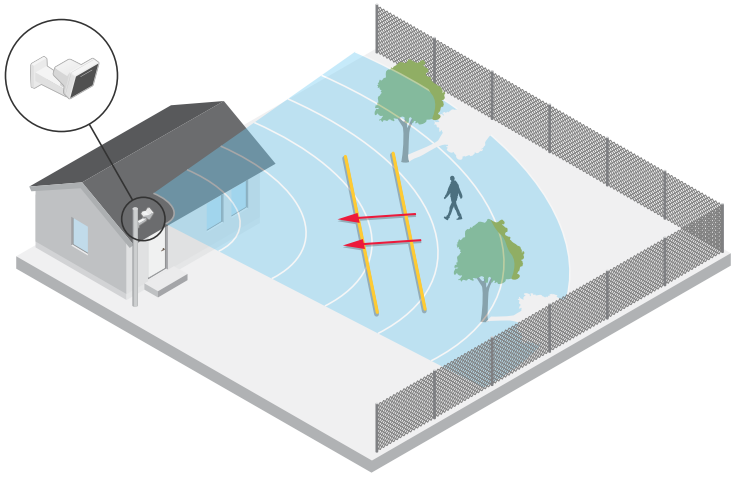
さらに、同社は勤務時間中も敷地内の安全を確保したいと考えています。建物脇の道路を通行する車両が制限速度内であることを確認するため、AXIS Radar Integration for Microbusを使用して、*AXIS D2110-VE* Security Radarの1台をMicrobus製Speed Signとペアリングしています。



複雑な撮影シーンをカバーする

敷地内の建物に重要な機器を維持しているある会社は、侵入者を防ぐために敷地周辺にフェンスを設置しています。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。同社の希望は、人が建物に近づいたときにアラームがトリガーされるようにすることです。しかし、シーンには枝が揺れる木や、反射の原因となる金属製のフェンスがあったり、サイト内を動き回る小動物がいたりと、これらすべてが誤報を引き起こす可能性があります。

誤報を減らすために、レーダーのwebインターフェースでシナリオを設定して、建物に近づく物体が2本の仮想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。これにより、意図的に建物に向かって移動する物体にはアラームがトリガーされ、たまたま仮想ラインの1本を横切っただけの物体はフィルターで除外されます。



フェンスのないサイトでは、2本のラインが仮想フェンスとして機能します。レーダーのwebインターフェースでシナリオに2本のラインを追加する方法については、を参照してください。

道路監視プロファイル

Road monitoring profile (道路監視プロファイル) は、郊外の道路や高速道路を最大200 km/h (125 mph) で走行する車両の追跡用に最適化されています。低速で移動する人やその他の物体を追跡するには、エリア監視プロファイルを使用します。詳細については、を参照してください。

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。

レーダーの取り付け高さと車両の速度は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。

道路設置例

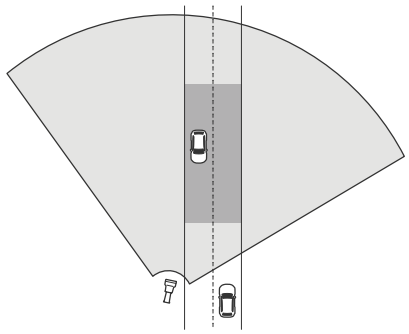
道路や高速道路を監視する際には、車両の後方に死角 (レーダー陰) ができないように、レーダーを十分な高さに取り付けてください。

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

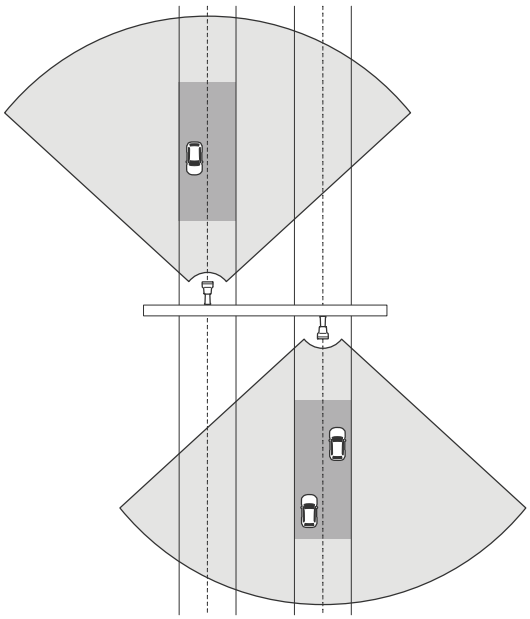
道路を走行する車両を監視するには、レーダーを道路の脇、たとえばポールに取り付けることができます。このタイプの設置では、パン角度を最大25° にすることをお勧めします。



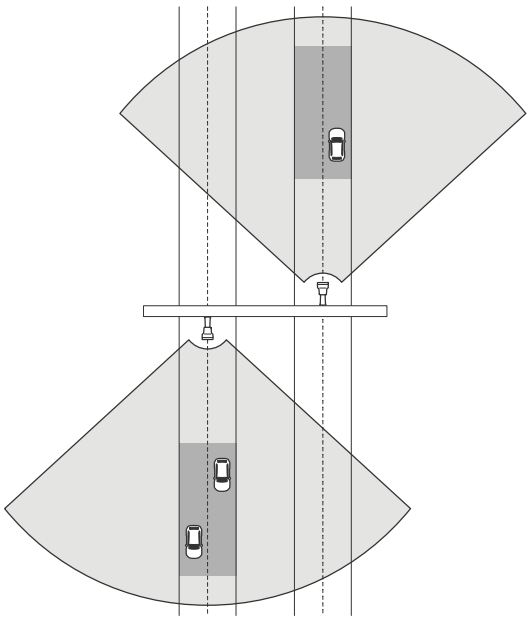
高速走行を正確に測定するには、レーダーを車両から横方向で10 m以内に設置してください。検知範囲と速度精度の詳細については、を参照してください。

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つ以上のレーダー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。



高速走行を正確に測定するには、レーダーを車両から横方向で10 m以内に設置してください。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。

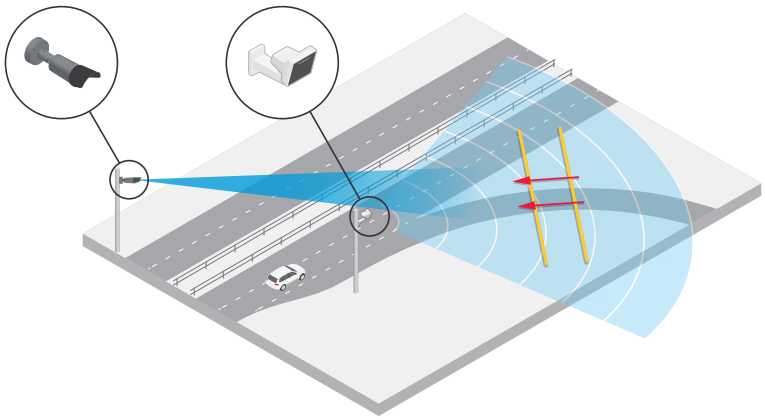
道路監視の使用例

AXIS D2210-VE Radarと道路監視プロファイルの一般的な使用例は、車両の速度を追跡して測定することです。さらに、レーダーをビジュアルカメラおよびアプリケーションAXIS Speed Monitorと併用することで、カメラのライブビューで車両の速度を可視化したり、統計処理のためにレーダーの追跡データを記録したりすることもできます。詳細については、*AXIS Speed Monitor*のユーザーマニュアルを参照してください。

道路監視プロファイルの使用する際にレーダーを設定する方法のその他の例については、次の使用例を参照してください。

高速道路のランプでの逆走の検知

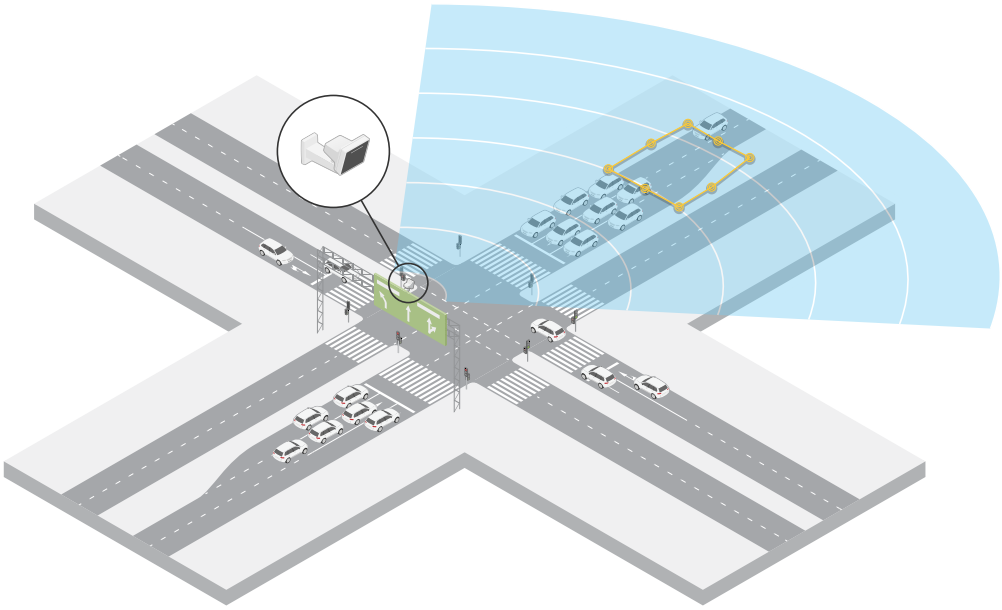
高速道路のランプで逆走車両を検知して特定するために、交通管制でAXIS D2210-VEとAxisバレット型カメラを使用しています。ランプに面したポールにレーダーを取り付け、逆走車両を検知しています。信頼性の高い検知を行うために、ライン横断シナリオを設定して、車両が2本のラインを横切ったときにのみレーダーがアラームをトリガーするようにしています。シナリオで、図に示すように2本のラインをランプ上に配置します。また、トリガー条件にする走行方向と速度も指定します。レーダーがアラームをトリガーすると、Axisバレット型カメラによりランプ上の車両の視覚的な識別が可能になります。



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レーダーを設置しています。レーダーのwebインターフェースでシナリオを設

定して、エリア内を移動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。シナリオは、交差点に向かう道路の一部だけをカバーするように設定します。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。



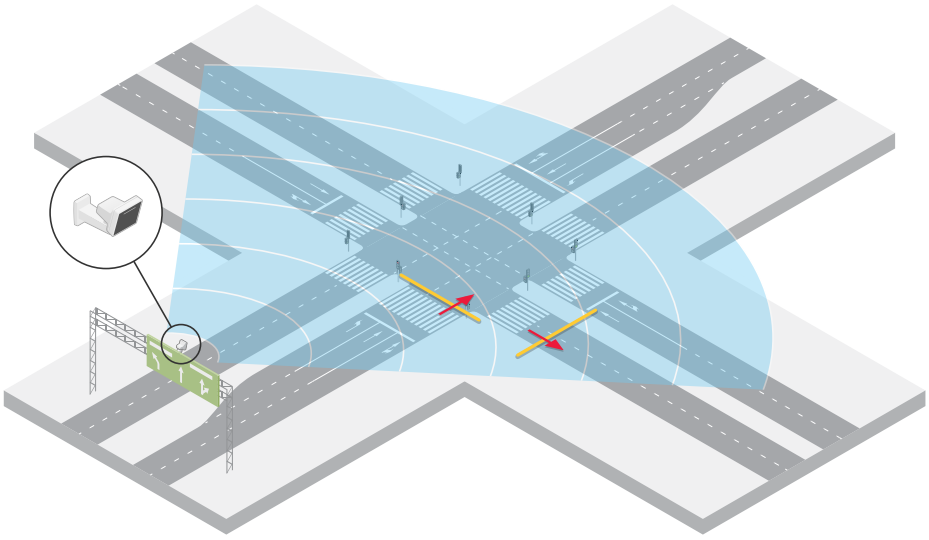
交差点での交通の流れの監視 - 方向

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レーダーを設置しています。レーダーのwebインターフェース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。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、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つのシナリオを作成しています。

注

このシナリオでは、ラインを横切る車両はカウントされませんが、代わりにレーダーの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、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

レーダープロファイルの選択

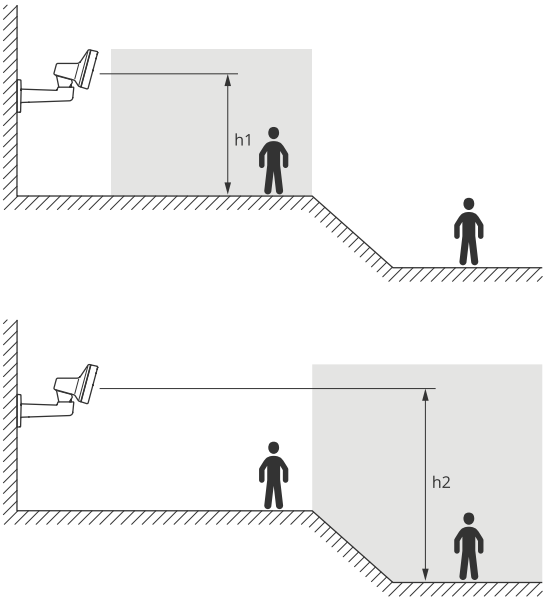
webインターフェース:
1. [Radar (レーダー)] > [Settings (設定)] > [Detection (検知)] に移動します。
2. [Radar profiles (レーダープロファイル)] でプロファイルを選択します。

取り付け高さの設定

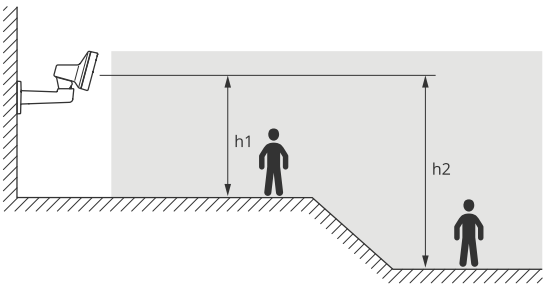
Webインターフェースでレーダーの取り付け高さを設定します。この設定によって、レーダーは通過する物体を検知し、その速度を正確に測定できます。

地面からレーダー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。

例:
対象範囲によって取り付け高さ (h1、h2) は異なります。



対象範囲の表面が平らでない場合は、レーダーを設定するときに平均高さ (この場合は (h1 + h2) / 2) を加算します。



取り付け高さの設定:
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。

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。

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。

- 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。
  感度の設定はすべてのゾーンに影響します。
  - 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。この設定はエリア監視プロファイルで使用でき、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。

レーダー画像の調整

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。

画像オーバーレイを表示する

レーダー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. [Radar > Overlays (レーダー > 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。

テキストオーバーレイを表示する

レーダーストリームにオーバーレイとしてテキストフィールドを追加することができます。これは、ビデオストリームに日付、時刻、会社名を表示する場合に便利です。

1. [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. ビデオストリームに表示するテキストを入力します。
4. 位置を選択します。ライブビューのオーバーレイテキスト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。

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。

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. [Radar (レーダー)] > [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. [Video format (ビデオ形式)]に[H.264] を選択します。
4. [Radar (レーダー)] > [Stream (ストリーム)] > [General (全般)] に移動し、Compression (圧縮率) を上げます。

注

ほとんどのWebブラウザーはH.265のデコードに対応していないため、装置はwebインターフェースでH.265をサポートしていません。その代わり、H.265デコーディングに対応したビデオ管理システムやアプリケーションを使用できます。

ネットワークストレージを設定する

ネットワーク上に録画を保存するには、以下のようにネットワークストレージを設定する必要があります。

1. [System > Storage (システム > ストレージ)] に移動します。
2. [Network storage (ネットワークストレージ)]で + [Add network storage (ネットワークストレージを追加)]をクリックします。
3. ホストサーバーのIPアドレスを入力します。
4. [Network Share (ネットワーク共有)] で、ホストサーバー上の共有場所の名前を入力します。
5. ユーザー名とパスワードを入力します。
6. SMBバージョンを選択するか、[Auto (自動)] のままにします。
7. 一時的な接続の問題が発生した場合や、共有がまだ設定されていない場合は、[Add share without testing (テストなしで共有を追加する)] を選択します。
8. [追加] をクリックします。

ビデオを録画して見る

レーダーから直接ビデオを録画する

1. [Radar (レーダー)] > [Stream (ストリーム)] に移動します。
2. 録画を開始するには、 をクリックします。
   ストレージを設定していない場合は、 および をクリックします。ネットワークストレージの設定手順については、を参照してください。
3. 録画を停止するには、もう一度 をクリックします。

ビデオを見る

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

イベントのルールを設定する

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。

アクションをトリガーする

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

注

アクティブなルールを変更する場合は、ルールを再度オンにして変更内容を有効にする必要があります。

注

ルールに使用されたストリームプロファイルの定義を変更する場合は、そのストリームプロファイルを使用するすべてのルールを再起動する必要があります。

動きが検知されたときにカメラからビデオを録画する

この例では、レーダーが動作を検知する5秒前にカメラがSDカードへの録画を開始し、1分後に停止するようにレーダーとカメラを設定する方法を説明します。

デバイスの接続:

1. レーダーのI/O出力からカメラのI/O入力にケーブルを接続します。

レーダーのI/Oポートの設定:

2. **[System (システム)] > [Accessories (アクセサリー)] > [I/O ports (I/Oポート)]** に移動し、I/Oポートを出力として設定して、標準状態を選択します。

レーダーでのルールの作成:

3. [**System > Events (システム > イベント)**] に移動し、ルールを追加します。
4. ルールの名前を入力します。
5. 条件のリストから、[**Radar motion (レーダーの動き)**] の下にあるシナリオを選択します。シナリオを設定するには、を参照してください。
6. 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、カメラに接続されているポートを選択します。
7. [**保存**] をクリックします。

カメラのI/Oポートの設定:

8. **[System (システム)] > [Accessories (アクセサリー)] > [I/O ports (I/Oポート)]** に移動し、I/Oポートを入力として設定して、標準状態を選択します。

カメラでのルールの作成:

9. [**System > Events (システム > イベント)**] に移動し、ルールを追加します。
10. ルールの名前を入力します。
11. 条件のリストから [**Digital input is active (デジタル入力がアクティブ)**] を選択し、ルールをトリガーするポートを選択します。
12. アクションのリストから、[**Record video (ビデオを録画する)**] を選択します。
13. ストレージオプションのリストから、[**SD card (SDカード)**] を選択します。
14. 既存のストリームプロファイルを選択するか、新しいプロファイルを作成します。
15. プリバッファを5秒に設定します。
16. ポストバッファを [1 minute (1分)] に設定します。
17. [**保存**] をクリックします。

車両の逆走時にカメラからのビデオを録画する

この例では、レーダーが逆走車両を検知したときにカメラがSDカードへの録画を開始するように、レーダーとカメラを設定する方法について説明します。

開始する前に

- レーダーのwebインターフェースで、ラインを横切る動きと、2本のラインを横切る車両によりトリガーするシナリオを作成します。
  詳細については、を参照してください。
- 逆走車両を検知する車線上に2本のラインを配置するようにしてください。航空写真などの参照マップを使用すると、物体が動いている場所がわかりやすくなります。
  詳細については、を参照してください。

1. レーダーに2つの送信先を作成します。

1.1. レーダーの装置インターフェースで、[System (システム)] > [Events (イベント)] > [Recipients (送信先)] に移動し、最初の送信先を追加します。
1.2. 以下の情報を追加します。
- 名前:Activate virtual port (仮想ポートのアクティブ化)
- Type (タイプ): HTTP
- URL: http://<IPaddress>/axis-cgi/virtualinput/activate.cgi <IPaddress>は、録画を開始するカメラのアドレスに置き換えてください。
- カメラのユーザー名とパスワードを入力します。

1.1. [Test (テスト)] をクリックして、すべてのデータが有効であることを確認します。
1.2. [保存] をクリックします。
1.3. 次の情報を含む2番目の送信先を追加します。
- 名前:仮想ポートの非アクティブ化
- Type (タイプ): HTTP
- URL: http://<IPaddress>/axis-cgi/virtualinput/deactivate.cgi <IPaddress>の部分をカメラのアドレスに置き換えます。
- カメラのユーザー名とパスワードを入力します。

1.1. [Test (テスト)] をクリックして、すべてのデータが有効であることを確認します。
1.2. [保存] をクリックします。

2. レーダーに2つのルールを作成します。
2.1. レーダーの装置インターフェースで、[System (システム)] > [Events (イベント)] > [Rules (ルール)] に移動し、最初のルールを追加します。
2.2. 以下の情報を追加します。
- 名前:仮想IO1のアクティブ化
- Condition (条件):[Radar motion (レーダーの動き)] で作成したシナリオを選択します。
- Action (アクション): Notifications > Send notification through HTTP (通知 > HTTPで通知を送信する)
- Recipient (送信先): Activate virtual port (仮想ポートのアクティブ化)
- Query string suffix (クエリ文字列のサフィックス): schemaversion=1&port=1

2.1. [保存] をクリックします。
2.2. 次の情報を含む別のルールを追加します。
- 名前:仮想IO1の非アクティブ化
- Condition (条件):[Radar motion (レーダーの動き)] で作成したシナリオを選択します。
- [Invert this condition (この条件を逆にする)] を選択します。
- Action (アクション): Notifications > Send notification through HTTP (通知 > HTTPで通知を送信する)
- Recipient (送信先): 仮想ポートの非アクティブ化
- Query string suffix (クエリ文字列のサフィックス): schemaversion=1&port=1

2.1. [保存] をクリックします。

3. カメラでルールを作成します。
3.1. カメラの装置インターフェースで、[System (システム)] > [Events (イベント)] > [Rules (ルール)] に移動し、ルールを追加します。

3.2. 以下の情報を追加します。
- 名前:仮想入力1のトリガー
- Condition (条件): [I/O] > [Virtual input is active (仮想入力がアクティブ)]
- ポート: 1
- Action (アクション): Recordings > Record video while the rule is active (録画 > ルールがアクティブである間、ビデオを録画する)
- Storage options (ストレージオプション): SD_DISK
- [Camera (カメラ)] と [Stream profile (ストリームプロファイル)] を選択します。

3.1. [保存] をクリックします。

レーダーで流れる赤のライトを有効にする

レーダーの前面にある動的LEDストリップを使用して、エリアが監視されていることを示すことができます。

この例では、流れる赤のライトを有効にする方法と、平日の勤務時間後にのみ流れるライトが動作するようにスケジュールを設定する方法について説明します。

スケジュールを作成する:
1. [System (システム)] > [Events (イベント)] > [Schedules (スケジュール)] に移動し、スケジュールを追加します。
2. スケジュールの名前を入力します。
3. [Type (タイプ)] で、[Schedule (スケジュール)] を選択します。
4. [Recurrent (繰り返し)] で、[Daily (日次)] を選択します。
5. 開始時刻を06:00 PMに設定します。
6. 終了時刻を06:00 AMに設定します。
7. [Days (曜日)] で、[Monday to Friday (月曜日〜金曜日)] を選択します。
8. [保存] をクリックします。

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、[Scheduled and recurring (スケジュールおよび繰り返し)] の [Schedule (スケジュール)] を選択します。
4. [Schedule (スケジュール)] ドロップダウンから作成したスケジュールを選択します。
5. [Radar (レーダー)] のアクションのリストで、[Dynamic LED strip (動的LEDストリップ)] を選択します。
6. [Pattern (パターン)] ドロップダウンからパターン [Sweeping red (流れる赤)] を選択します。
7. 継続時間を12時間に設定します。
8. [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。

動きが検知されたときに照明を点灯する

侵入者が検知ゾーンに入ったときに照明を点灯すると、抑止効果があり、侵入を録画するビジュアルカメラの画質も向上します。

この例では、レーダーが動作を検知したときにイルミネーターが点灯し、1分後に消灯するようにレーダーとイルミネーターを設定する方法を説明します。

デバイスの接続:

1. レーダーのリレーポートを介して、イルミネーターケーブルの1本を電源に接続します。別のケーブルで電源とイルミネーターの間を直接接続します。

レーダーのリレーポートの設定:

2. [System (システム)] > [Accessories (アクセサリー)] > [I/O ports (I/Oポート)] に移動し、リレーポートの通常状態として [Open circuit (開回路)] を選択します。

レーダーでのルールの作成:

3. [System > Events (システム > イベント)] に移動し、ルールを追加します。
4. ルールの名前を入力します。
5. 条件のリストから、[Radar motion (レーダーの動き)] の下にあるシナリオを選択します。シナリオを設定するには、を参照してください。
6. アクションのリストから [Toggle I/O once (I/Oを1度切り替える)] を選択し、リレーポートを選択します。
7. [Active (アクティブ)] を選択します。
8. [Duration (継続時間)] を設定します。
9. [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、レーダー、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

AXIS Speed Monitorアプリケーションでレーダーを使用して、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をレーダーにインストールするか、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。

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

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。

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。

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。

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。

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。

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。

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。

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。

動的LEDストリップ

動的LEDストリップのパターン

このページを使用して、動的LEDストリップのパターンをテストします。

Pattern (パターン):テストするパターンを選択します。

[Duration (継続時間)]:テストの継続時間を指定します。

Test (テスト):クリックして、テストするパターンを開始します。

Stop (停止):クリックして、テストを停止します。パターンの再生中にページを離れると、パターンは自動的に停止します。

通知または抑止の目的でパターンをアクティブにするには、[System (システム)] > [Events (イベント)] に移動してルールを作成します。例については、を参照してください。

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。

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。

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。

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)

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)**]。
- **Viewer (閲覧者)**:設定を変更するアクセス権を持っていません。

⋮ 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

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。

インストールの検証

レーダーの設置を検証する

注

このテストは、現在の状況下での設置の検証に役立ちます。設置の日常のパフォーマンスは、シーンの変化の影響を受ける可能性があります。

レーダーは設置後すぐに使用する準備ができていますが、使用を開始する前に検証を行することをお勧めします。これにより、設置に関する問題を特定したり、シーン内の物体 (樹木や反射面など) を管理したりできるため、レーダーの精度を高めることができます。

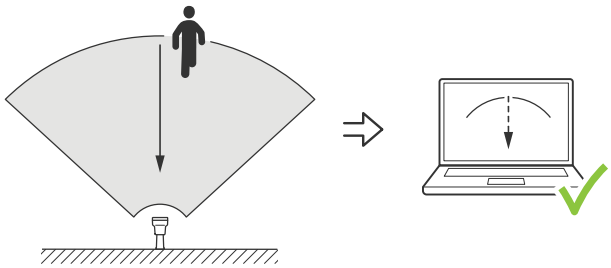
検証を試みる前に、まずを行います。その後、以下の手順に従います。

誤検知がないことを確認する

1. 検知ゾーンに人間の活動がないことを確認してください。
2. 検知ゾーン内に静止した物が検知されないことを確認するために、数分間待ってください。
3. 不要な検知がない場合は、手順4をスキップできます。
4. 不要な検知がある場合は、特定の種類の動きや物体を除外する方法、カバー範囲を変更する方法、または検知感度を調整する方法について、を参照してください。

レーダーに正面から近づくと、記号と移動方向が正しく表示されることを確認する

1. レーダーのwebインターフェースに移動し、セッションを録画します。この方法については、を参照してください。
2. レーダーの前方最大60 mの位置から始め、レーダーに向かって直進します。
3. レーダーのwebインターフェースで、セッションを確認します。検知されると、人の分類の記号が表示されます。
4. レーダーのwebインターフェースで、移動方向が正しく表示されていることを確認します。



レーダーに横から近づくと、記号と移動方向が正しく表示されることを確認する

1. レーダーのwebインターフェースに移動し、セッションを録画します。この方法については、を参照してください。
2. レーダーから30 m離れた位置から始め、レーダーの検知範囲を横切って直進します。
3. レーダーのwebインターフェースで、人の分類の記号が表示されていることを確認します。
4. レーダーのwebインターフェースで、移動方向が正しく表示されていることを確認します。

検証からデータを記録するのに役立つ、以下のような表を作成します。

テスト	合格/失敗	コメント
1.エリアに何もないときに不要な検知がないことを確認する		

2a.レーダーに正面から近づくと、対象が「人」の正しい記号で検知されることを確認する		
2b.レーダーに正面から近づくと、移動方向が正しく表示されることを確認する		
3a.レーダーに横から近づくと、対象が「人」の正しい記号で検知されることを確認する		
3b.レーダーに横から近づくと、移動方向が正しく表示されることを確認する		

検証を完了する

検証の最初の部分が正常に完了したら、次のテストを実行して検証プロセスを完了する必要があります。

1. レーダーが設定され、手順に従ったかを確認してください。
2. さらに検証を行う場合は、参照マップを追加してキャリブレーションします。
3. 該当する物体が検知されるとトリガーされるようにレーダーシナリオを設定します。デフォルトでは、[**seconds until trigger (トリガーまでの秒数)**] は2秒に設定されますが、必要に応じてwebインターフェースでこれを変更できます。
4. 該当する物体が検知されるとデータを記録するようにレーダーを設定します。手順については、を参照してください。
5. [**trail lifetime (試用期間)**] を1時間に設定して、余裕を持って席を離れ、監視エリアを歩き回り、席に戻ることができるようにします。**trail lifetime (試用期間)** は、設定した時間だけレーダーのライブビュー内で追跡が継続し、検証が完了すると無効になります。
6. レーダーの範囲の境界線に沿って歩き、システムのトレイルが歩いたルートと一致していることを確認します。
7. 検証の結果に満足できない場合は、参照マップを再キャリブレーションし、検証を繰り返す必要があります。

詳細情報

ストリーミングとストレージ

ビデオ圧縮形式

使用する圧縮方式は、表示要件とネットワークのプロパティに基づいて決定します。以下から選択を行うことができます。

Motion JPEG

Motion JPEGまたはMJPEGは、個々のJPEG画像の連続で構成されたデジタルビデオシーケンスです。これらの画像は、十分なレートで表示、更新されることで、連続的に更新される動きを表示するストリームが作成されます。人間の目に動画として認識されるためには、1秒間に16以上の画像を表示するフレームレートが必要になります。フルモーションビデオは、1秒間に30フレーム (NTSC) または25フレーム (PAL) で動画と認識されます。

Motion JPEGストリームは、かなりの帯域幅を消費しますが、画質に優れ、ストリームに含まれるすべての画像にアクセスできます。

H.264またはMPEG-4 Part 10/AVC

注

H.264はライセンスされた技術です。このAxis製品には、H.264閲覧用のクライアントライセンスが1つ添付されています。ライセンスされていないクライアントのコピーをインストールすることは禁止されています。ライセンスを追加購入するには、Axisの販売代理店までお問い合わせください。

H.264を使用すると、画質を損なうことなく、デジタル映像ファイルのサイズを削減でき、Motion JPEG形式の場合と比較すると80%以上、従来のMPEG形式と比較すると50%以上を削減できます。そのため、ビデオファイルに必要なネットワーク帯域幅やストレージ容量が少なくなります。また、別の見方をすれば、より優れた映像品質が同じビットレートで得られることになります。

H.265またはMPEG-H Part 2/HEVC

H.265を使用すると、画質を損なうことなくデジタルビデオファイルのサイズを削減でき、H.264に比べて25%以上縮小することができます。

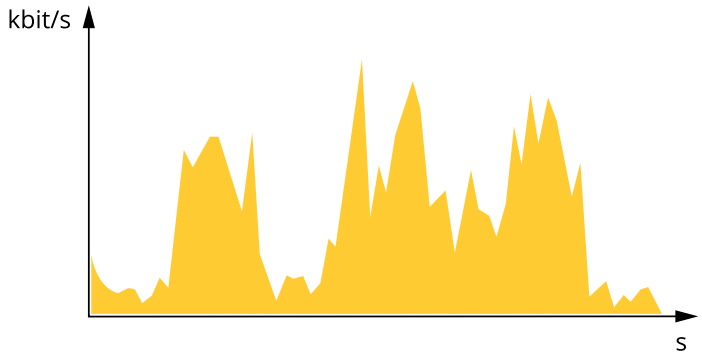
注

- H.265はライセンスされた技術です。このAxis製品には、H.265閲覧用のクライアントライセンスが1つ添付されています。ライセンスされていないクライアントのコピーをインストールすることは禁止されています。ライセンスを追加購入するには、Axisの販売代理店までお問い合わせください。
- ほとんどのWebブラウザはH.265のデコードに対応していないため、カメラはWebインターフェースでH.265をサポートしていません。その代わり、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。

ビットレート制御

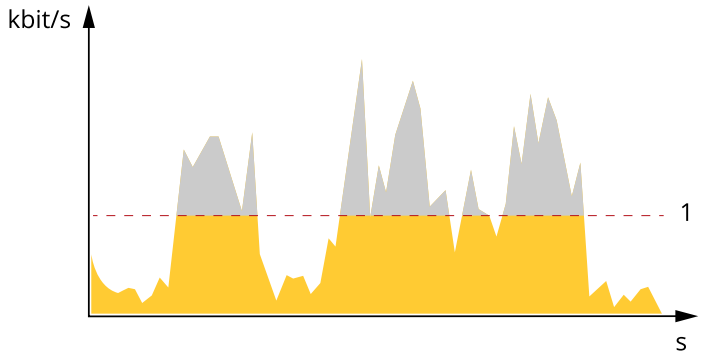
ビットレート制御で、ビデオストリームの帯域幅の使用量を管理することができます。

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。

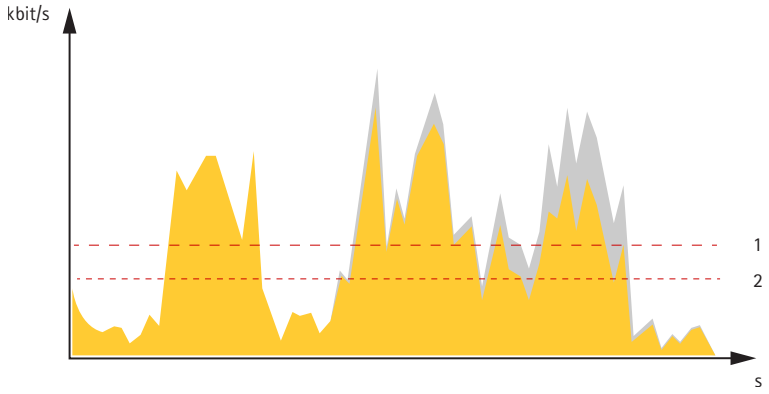


1 目標ビットレート

平均ビットレート（ABR）

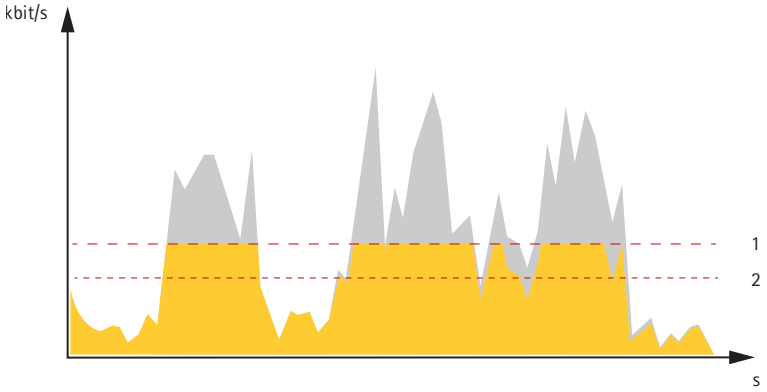
平均ビットレートでは、より長い時間スケールにわたってビットレートが自動的に調整されます。これにより、指定した目標を達成し、使用可能なストレージに基づいて最高画質のビデオを得ることができます。動きの多いシーンでは、静的なシーンと比べてビットレートが高くなります。平均ビットレートオプションを使用すると、多くのアクティビティがあるシーンで画質が向上する可能性が高くなります。指定した目標ビットレートに合わせて画質が調整されると、指定した期間 (保存期間)、ビデオストリームを保存するために必要な総ストレージ容量を定義できます。次のいずれかの方法で、平均ビットレートの設定を指定します。

- 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。



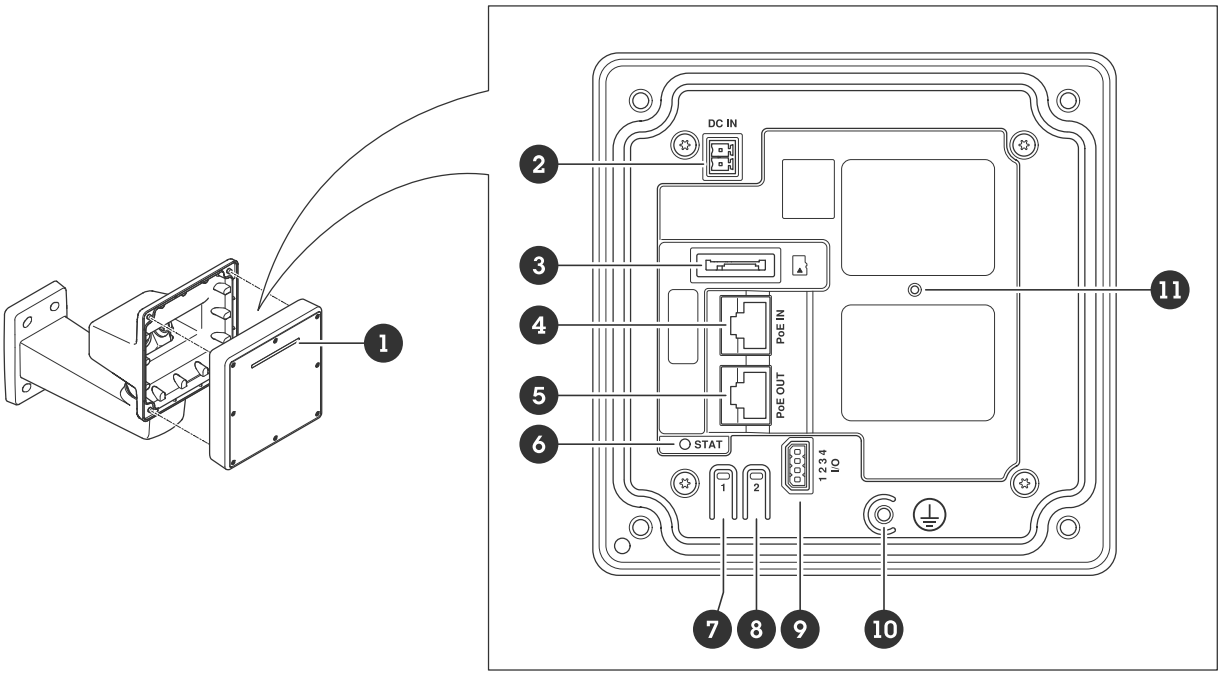
1 目標ビットレート
2 実際の平均ビットレート

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。

仕様

製品概要



1 動的LEDストリップ
2 電源コネクタ (DC)
3 microSDカードスロット
4 ネットワークコネクター (PoE入力)
5 ネットワークコネクター (PoE出力)
6 ステータスLED
7 コントロールボタン
8 アクションボタン
9 I/Oコネクター
10 アース端子ネジ
11 リセットボタン

LEDインジケーター

注

- ステータスLEDは、イベントの発生時に点滅させることができます。

ステータスLED	説明
緑	正常動作であれば緑色に点灯します。
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。
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。

動的LEDストリップのパターン
赤
青
緑
黄

白
流れる赤
流れる青
流れる緑
点滅する赤、青、白

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。

コネクター

ネットワークコネクター (PoE入力)

Power over Ethernet IEEE 802.3bt、Type 3 Class 6に準拠したRJ45イーサネットコネクター。

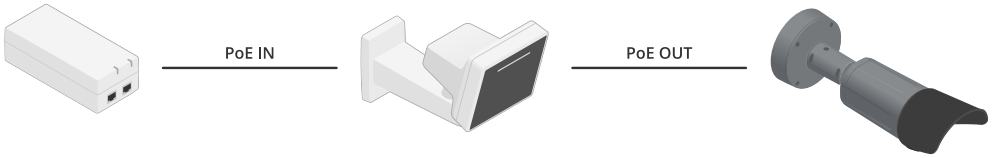
注

PoE出力には、Power over Ethernet IEEE 802.3bt、Type 3 Class 6が必要です。2番目の装置に給電しない場合は、Power over Ethernet IEEE 802.3at、Type 2 Class 4で十分です。

ネットワークコネクター (PoE出力)

Power over Ethernet IEEE 802.3at、Type 2 Class 4で最大30 Wを供給するRJ45イーサネットコネクター。

このコネクターを使用して別のPoE装置 (カメラ、警報スピーカー、2番目のAxisレーダーなど) に給電します。



注

PoE出力は、レーダーが60 Wミッドスパン (Power over Ethernet IEEE 802.3 bt、type 3) によって給電されている場合に有効になります。

注

レーダーが30 WミッドスパンまたはDC電源によって給電されている場合、PoE出力は無効になっています。

注

イーサネットケーブルの最大長は、PoE出力とPoE入力を組み合わせた合計の100 mです。PoEエクステンダーを使用して、延長することができます。

注

接続するPoE装置が30 Wを超える電力を必要とする場合は、レーダーのPoE出力ポートと装置の間に60 Wミッドスパンを追加できます。ミッドスパンが装置に給電するようになり、レーダーがイーサネット接続を可能にします。

I/Oコネクター

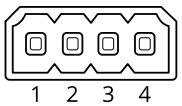
I/Oコネクターに外部装置を接続し、イベントトリガーやアラーム通知などと組み合わせて使用することができます。I/Oコネクターは、0 VDC基準点と電力 (DC出力) に加えて、以下のインターフェースを提供します。

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

状態監視入力 - デジタル入力のいたずらを検知する機能が有効になります。

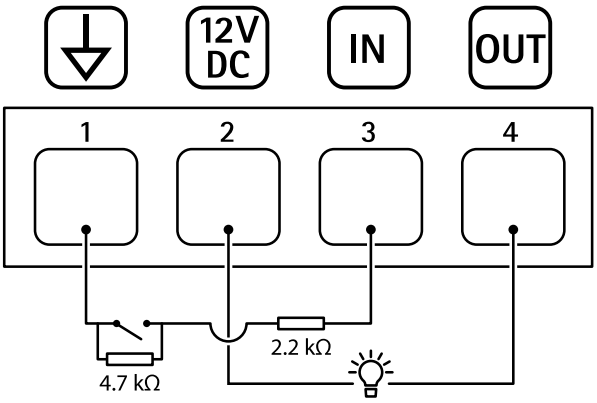
デジタル出力 - リレーやLEDなどの外部装置を接続します。接続された装置は、VAPIX®アプリケーションプログラミングインターフェースを通じたイベントまたは本装置のwebインターフェースから有効にすることができます。

4ピンターミナルブロック



機能	ピン	メモ	仕様
DCアース	1		0 VDC
DC出力	2	補助装置の電源供給に使用できます。 注:このピンは、電源出力としてのみ使用できます。	12VDC 最大負荷 = 25mA
デジタル入力	3	動作させるにはピン1に接続し、動作させない場合はフロート状態 (未接続) のままにします。	0～最大30 VDC
デジタル出力	4	アクティブ時はピン1 (DCアース) に内部で接続し、非アクティブ時はフロート状態 (未接続) になります。リレーなどの誘導負荷とともに使用する場合は、過渡電圧から保護するために、負荷と並列にダイオードを接続します。	0～30 VDC (最大)、オープンドレイン、100 mA

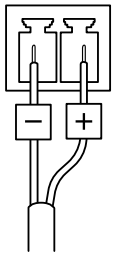
例:



1 *DCアース*
2 *DC出力12 V、最大25 mA*
3 *状態監視入力*
4 *デジタル出力*

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。



装置を清掃する

装置はぬるま湯で洗浄できます。

注意

- 強力な化学薬品は装置を損傷する可能性があります。窓ガラス用洗剤やアセトンなどの化学薬品を使用して装置をクリーニングしないでください。
- シミの原因となるため、直射日光や高温下での清掃は避けてください。

1. 圧縮空気を使用すると、装置からほこりやごみを取り除くことができます。
2. 必要に応じて、ぬるま湯に浸した柔らかいマイクロファイバーの布で装置を清掃してください。
3. シミを防ぐために、きれいな非研磨性の布で装置から水分を拭き取ってください。

トラブルシューティング

工場出荷時の設定にリセットする

重要

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

本製品を工場出荷時の設定にリセットするには、以下の手順に従います。

1. 本製品の電源を切ります。
2. コントロールボタンを押した状態で電源を再接続します。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 Edge：無料で使用でき、最小限の監視が必要な小規模システムに最適です。
- AXIS Camera Station 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。

パフォーマンスに関する一般的な検討事項

システムを設定する際には、さまざまな設定や条件が必要な帯域幅 (ビットレート) にどのように影響するかを検討することが重要です。

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。

T10193646_ja

2025-04 (M14.2)

© 2023年 – 2025 Axis Communications AB