

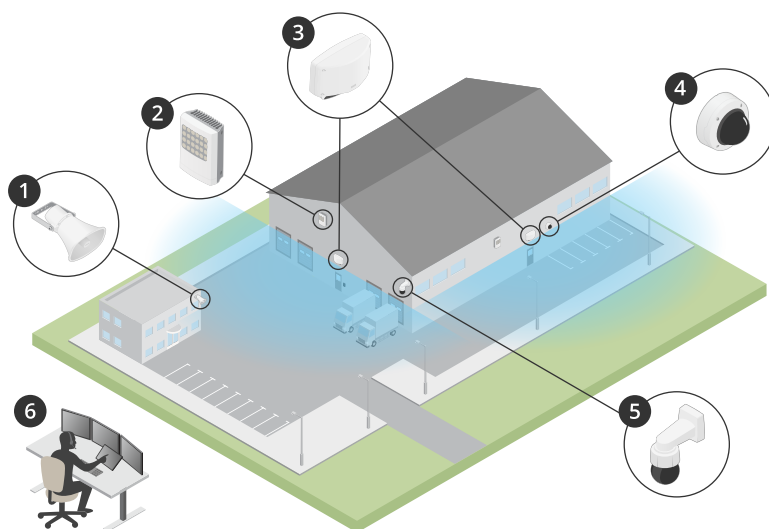
AXIS D2110-VE Security Radar

目次

ソリューションの概要	4
レーダープロファイル	4
製品の取り付け場所	4
カバー範囲	5
エリア監視プロファイル	6
複数のレーダーを設置	6
同じ共存ゾーンに2～3台のレーダーを設置する	6
同じ共存ゾーンに4～6台のレーダーを設置する	6
エリア設置例	7
エリア検知範囲	9
エリア監視の使用例	11
道路監視プロファイル	12
道路設置例	12
道路検知範囲	12
道路監視の使用例	13
使用に当たって	15
ネットワーク上のデバイスを検索する	15
ブラウザサポート	15
装置のwebインターフェースを開く	15
管理者アカウントを作成する	15
安全なパスワード	16
webインターフェースの概要	16
デバイスを構成する	17
取り付け高さの設定	17
参照マップを使用してキャリブレーションを行う	17
検知ゾーンの設定	18
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	20
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	21
ビデオを録画して見る	21
レーダーでPTZカメラを制御する	22
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	22
AXIS Radar Autotracking for PTZを使用してPTZカメラを制御する	23
イベントのルールを設定する	23
アクションをトリガーする	23
囲いが開かれたときに通知をトリガーする	24
動きが検知されたときにカメラからビデオを録画する	24
動きが検知されたときに照明を点灯する	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
webインターフェース	27
インストールの検証	28
レーダーの設置を検証する	28
レーダーの検証	28
検証を完了する	29
詳細情報	30
ストリーミングとストレージ	30
ビデオ圧縮形式	30
ビットレート制御	30
仕様	33
製品概要	33

.....	33
LEDインジケーター	33
.....	34
SDカードスロット	34
ボタン	34
コントロールボタン	34
コネクタ	34
ネットワーク コネクタ	34
ネットワークコネクタ (PoE出力).....	34
I/Oコネクタ	35
電源コネクタ	36
リレーコネクタ	36
装置を清掃する	37
トラブルシューティング	38
工場出荷時の設定にリセットする	38
AXIS OSの現在のバージョンを確認する	38
AXIS OSをアップグレードする	38
技術的な問題と解決策	39
パフォーマンスに関する一般的な検討事項	41
サイバーセキュリティ	42
脆弱性の管理	42
セキュリティ通知.....	42
安全な製品ライフサイクル管理.....	42

ソリューションの概要



- 1 C1310-Eホーンスピーカー
- 2 ドアコントローラー
- 3 D2110-VE Security Radar
- 4 固定ドームカメラ
- 5 PTZカメラ
- 6 監視センター

レーダープロファイル

注

レーダープロファイルを使用するには、装置でファームウェアバージョン10.11以降が実行されている必要があります。にアクセスして、ファームウェアを更新してください。

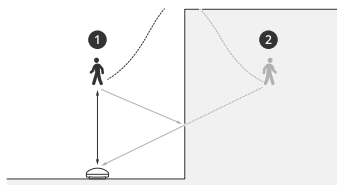
ユーザーマニュアルは、レーダーを目的に応じて使用するのに役立つように用意されています。AXIS D2110-VE Security Radarには、次の2つのプロファイルがあります。

- **エリア監視プロファイル**。55 km/h未満の速度で移動する大小両方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**。最大105km/hの速度で走行する車両を追跡するために使用します。

本ユーザーマニュアルで、**エリア監視プロファイル**または**道路監視プロファイル**に分類されていない情報は、両方のプロファイルに共通であり、どちらのプロファイルを使用するかに関係なく参照できます。

製品の取り付け場所

- レーダーは、障害物のない領域の監視を目的としています。壁、フェンス、樹木、大きな茂みなどの固体が対象範囲にあると、その背後に死角（レーダー陰）が生じます。
- レーダーを安定したポールに取り付けるか、壁面上で他の物体や設置された装置がない場所に取り付けます。レーダーの左右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。
- 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。



- 1 実際の検知
- 2 反射の検知 (ゴースト追跡)

反射物の取り扱い方法については、除外範囲の追加, on page 19を参照してください。

- 同じ共存ゾーンに2台を超えるレーダーを設置する場合は、複数のレーダーを設置, on page 6を参照してください。

カバー範囲

AXIS D2110-VEの水平方向のカバー範囲は180°です。検知範囲は、人間の場合は5600 m² (61000 ft²)、車両の場合は11300 m² (122000 ft²)です。

注

レーダーが3.5～4 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。取り付け高さは、レーダーの下の死角のサイズに影響します。

エリア監視プロファイル

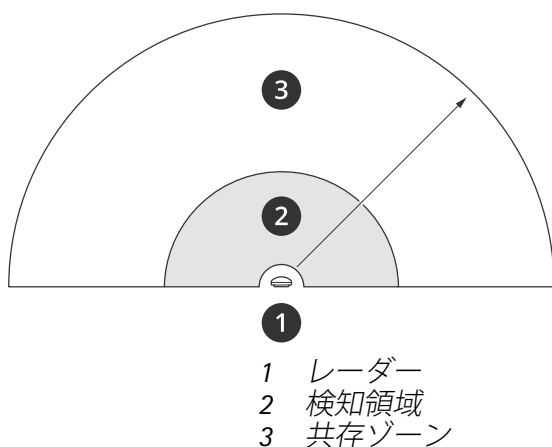
エリア監視プロファイルは、最大55 km/hで移動する物体用に最適化されます。このプロファイルを使用すると、物体が人物、車両、または不明であるかを検知できます。これらの物体のいずれかが検知されたときにアクションをトリガーするようにルールを設定できます。高速で移動する車両を追跡するには、*道路監視プロファイル*, on page 12を使用します。

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

同じ共存ゾーン内に2台以上のレーダーを配置すると、ゾーン内のレーダーからの電波が干渉を引き起こし、パフォーマンスに影響を与えることがあります。共存ゾーンの半径は350 mです。



注

共存ゾーン内のレーダーは、環境やフェンス、建物、近隣のレーダーへの向きによっても、パフォーマンスに影響を受けることがあります。

同じ共存ゾーンに2～3台のレーダーを設置する

同じ共存ゾーンに2～3台のレーダーを設置する場合は、装置インターフェースで隣接するレーダーの数を定義する必要があります。これは、レーダーのパフォーマンスを向上させ、干渉を回避するのに役立ちます。

1. [Radar (レーダー)] > [Settings (設定)] > [Coexistence (共存)] に移動します。
2. 隣接するレーダーの数を選択します。

複数のレーダーを設置する例については、*エリア設置例*, on page 7を参照してください。

同じ共存ゾーンに4～6台のレーダーを設置する

注

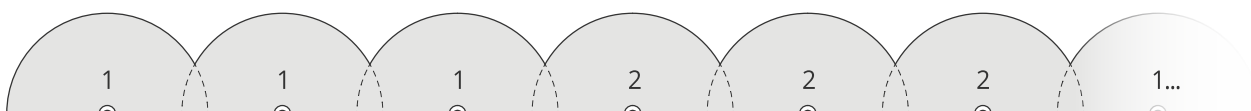
同じ共存ゾーンに最大6台のレーダーを設置するオプションは、ファームウェアバージョン11.3から利用できます。

同じ共存ゾーンに4～6台のレーダーを設置する場合、まず隣接するレーダーの数を設定してから、各レーダーをグループに追加します。最も遠くに設置されているレーダー、たとえば1番左側にあるレーダーから始めます。3つのグループに分けてレーダーを追加し、最も近いレーダー同士を同じグループに追加します。

グループ内のレーダーは互いに同期してパフォーマンスを最適化し、互いの干渉を回避します。

1. [Radar (レーダー)] > [Settings (設定)] > [Coexistence (共存)] に移動します。

2. 隣接するレーダーの数を3～5に設定します。
3. レーダーのグループを選択します。



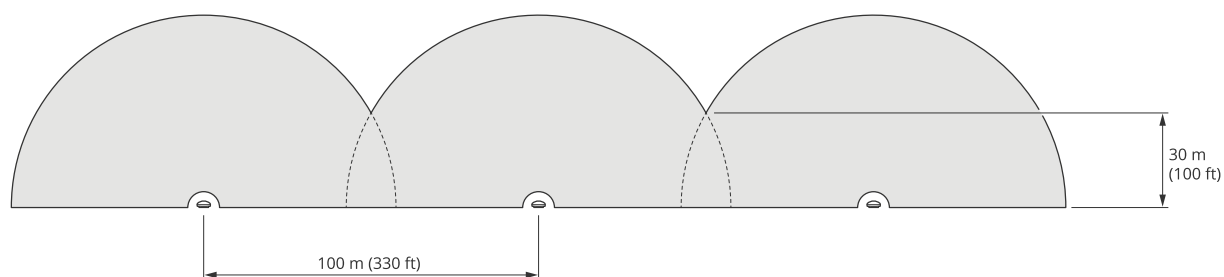
これは、同じ共存ゾーンに並べて設置した複数のレーダーをグループ化する例です。

複数のレーダーを設置するその他の例については、エリア設置例, on page 7を参照してください。

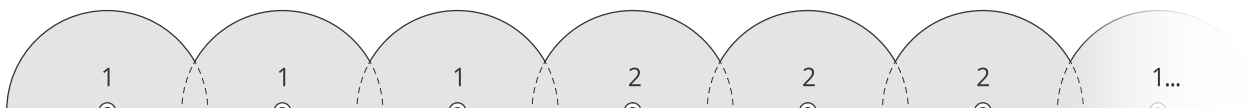
エリア設置例

複数のレーダーにより仮想フェンスを作成する

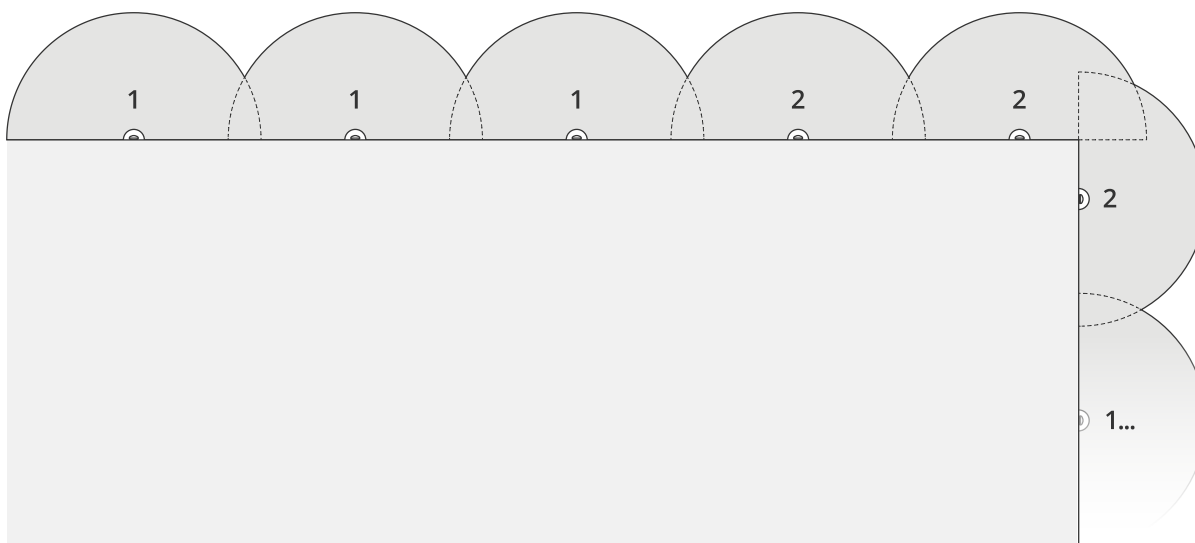
たとえば、建物に沿って、または建物の周りに、仮想フェンスを作成するには、複数のレーダーを横に並べて設置できます。100 mの間隔で配置することをお勧めします。



同じ共存ゾーンに3台以上のレーダーを設置した場合の干渉を避けるには、装置インターフェースで隣接するレーダーの数を設定します。さらに、4台以上のレーダーを設置する場合は、各レーダーをグループに追加します。



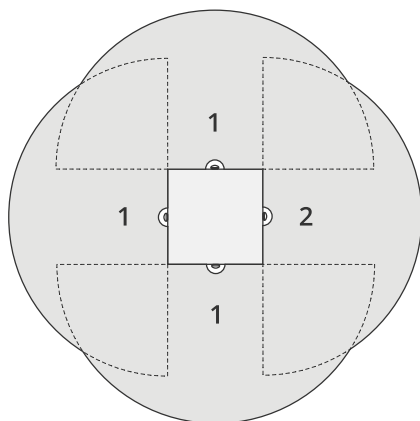
この例のように、仮想フェンスを調整してコーナーをカバーすることもできます。



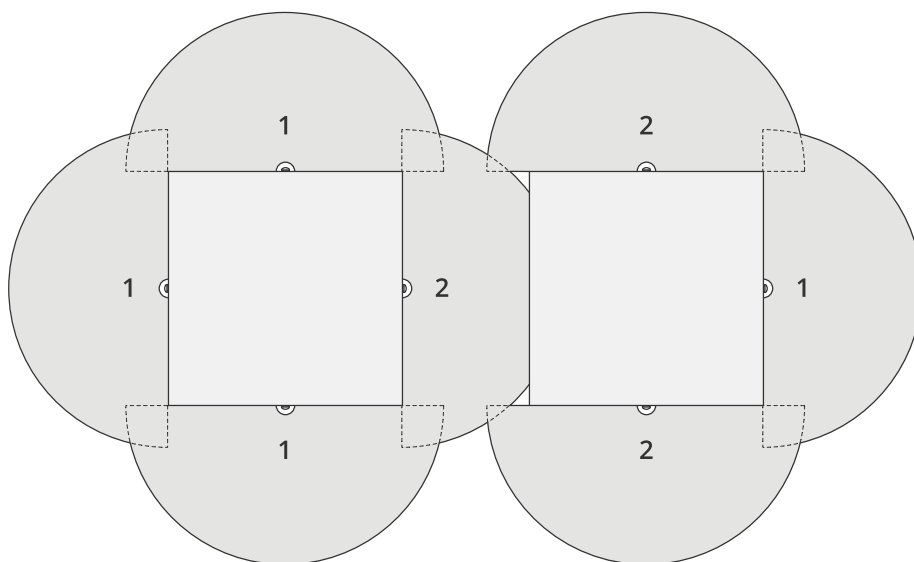
隣接するレーダーとグループの詳細については、複数のレーダーを設置, on page 6を参照してください。

建物の周囲をカバーする

建物の周囲をカバーするには、ビルの壁に外側に向けてレーダーを配置します。同じ共存ゾーンに4台以上のレーダーを設置する場合は、この例のように、装置インターフェースで隣接するレーダーの数を設定し、各レーダーをグループに追加します。



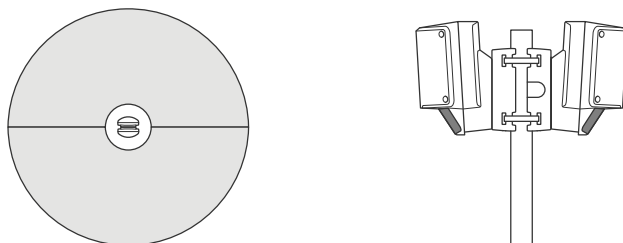
また、複数の建物の周囲をカバーすることもできます。



隣接するレーダーとグループの詳細については、複数のレーダーを設置, on page 6を参照してください。

オープンエリアをカバーする

広いオープンエリアをカバーするには、2つのポールマウントを使用して2台のレーダーを背中合わせに配置します。

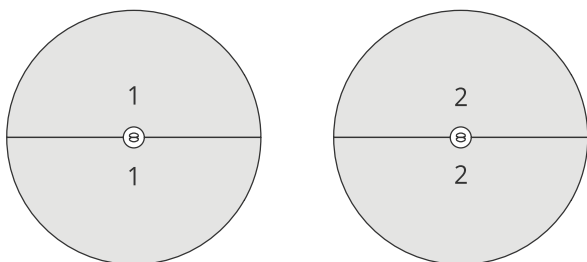


1台のレーダーからのPoE出力を使用して2番目のレーダーに電力を供給することができますが、この方法で3番目のレーダーを接続することはできません。

注

レーダーが60 Wミッドスパンから給電されている場合、レーダーのPoE出力が有効になります。

同じ共存ゾーンに複数のレーダーを背中合わせに設置する必要がある場合、装置インターフェースで隣接するレーダーの数を設定し、各レーダーをグループに追加して、干渉を回避します。これは、レーダーをグループ化して背中合わせに設置する方法の一例です。



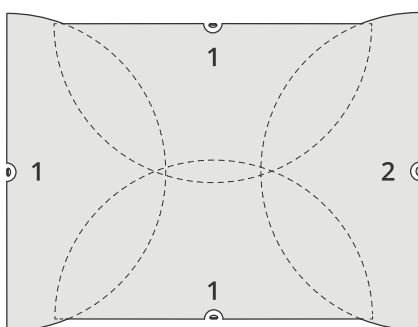
隣接するレーダーとグループの詳細については、複数のレーダーを設置, on page 6を参照してください。

複数のレーダーを向かい合わせに設置する

一般に、4台以上のレーダーを向かい合わせに設置することは、レーダー間の干渉のリスクが高まるため、お勧めしません。しかし、特定のエリアでは必要な場合があります。たとえば、サッカー場をカバーする場合、フィールドの真ん中にレーダーを設置することはできません。

4台以上のレーダーを向かい合わせに設置する場合は、レーダー間の距離を最低40 mにする必要があります。また、装置インターフェースで隣接するレーダーの数を設定し、各レーダーをグループに追加することが特に重要です。それにより、レーダーのパフォーマンスが向上します。

これは、1つのフィールドをカバーする4台のレーダーをグループ化する例です。



隣接するレーダーとグループの詳細については、複数のレーダーを設置, on page 6を参照してください。

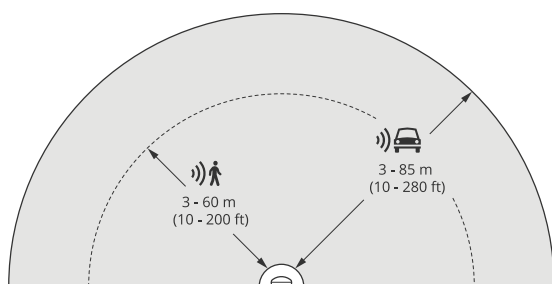
エリア検知範囲

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** (デバイスにどれだけ近づいて検知できるか) から**遠距離検知限界** (デバイス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。

エリア監視プロファイルは人間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。

- 人間の検知時は3～60 m
- 車両の検知時は3～85 m



注

- ・ レーダーを別の高さに設置する場合は、レーダーのキャリブレーションを行うときに製品のWebページに実際の取り付け高さを入力します。
- ・ 検知範囲はシーンの影響を受けます。
- ・ 検知範囲は近隣のレーダーによって影響されます。
- ・ 検知範囲は物体のタイプによって異なります。

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の人物でした。
- ・ 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、人物が検知ゾーンに入ると計測されます。
- ・ 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°	10° 傾き	チルト20°
2.5 m (8.2 ft)	3.0~60 m (9.8~197 ft)	非推奨	非推奨
3.5 m (11 ft)	3.0~60 m (9.8~197 ft)	非推奨	非推奨
4.5 m (15 ft)	4.0~60 m (13~197 ft)	非推奨	非推奨
5.5 m (18 ft)	7.5~60 m (25~197 ft)	非推奨	非推奨
6.5 m (21 ft)	7.5~60 m (25~197 ft)	5.5~60 m (18~197 ft)	非推奨
8 m (26 ft)	非推奨	9~60 m (30~197 ft)	7.5~30 m (25~98 ft)
10 m (33 ft)	非推奨	15~60 m (49~197 ft)	9~35 m (30~115 ft)
12 m (39 ft)	非推奨	23~60 m (75~197 ft)	13~38 m (43~125 ft)
14 m (36 ft)	非推奨	27~60 m (89~197 ft)	17~35 m (56~115 ft)
16 m (52 ft)	非推奨	非推奨	25~50 m (82~164 ft)

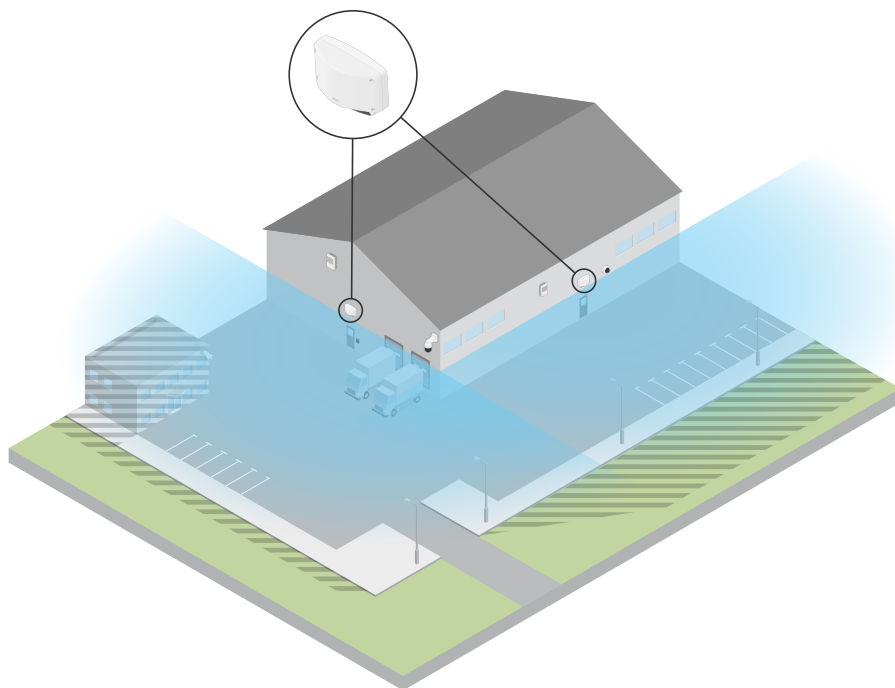
エリア監視の使用例

スイミングプールのエリアをカバーする

ある公共のプールで営業時間外に数件の侵入事件がありました。このビジネスに特有のプライバシー上の理由で、オーナーはビデオ監視装置を設置できません。そこで、レーダーを設置し、**Area monitoring profile (エリア監視プロファイル)** に設定することにしました。レーダーは建物に取り付けられて、プール全体とその周囲のほとんどのエリアをカバーします。20:00の営業終了から06:00の営業開始までの間に人間が検知されると、スピーカーから警告が発せられるようになります。

建物の周囲の現場をカバーする

化学工場では、レーダーを使用して機密性の高い建物の周囲をカバーすることで、システムに追加のセキュリティ層を設けています。セキュリティシステムには、すでにカメラ、サーマルカメラ、ドアコントローラーが含まれていました。レーダーにより、カメラが侵入者を追跡し、ズームインして、行動を録画するイベントがトリガーされるようにできました。サーマルカメラにリンクされた点滅ビーコンがトリガーされて点滅するため、侵入者はそのエリアが保護されていることを認識します。また、ドアコントローラーにより、建物への立ち入りを制限できます。さらに、レーダーにより、侵入者が機密性の高い建物に達するかなり前に、防衛システムが機能するようになります。



広いオープンエリアをカバーする

小さなショッピングセンターの屋外駐車場では、営業時間外に車両の侵入が増えています。この駐車場では交代制で1人の警備員がいます。夜間に警備を強化する必要があると感じていますが、警備員を増員することでコストを増やしたくはありません。そこで、駐車エリア全体をカバーするように、2台のセキュリティレーダーを背中合わせに設置し、**Area monitoring profile (エリア監視プロファイル)** に設定することにしました。レーダーは、勤務中の警備員に疑わしい行動を警告して、現場を調査できるように設定しています。また、レーダーによってトリガーされるホーンスピーカーを設置して、盗難を阻止するためのアラートが再生されるようにすることもできます。

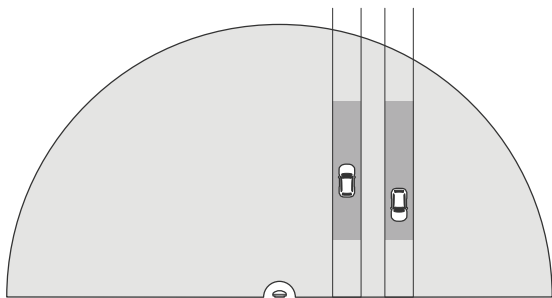
道路監視プロファイル

Road monitoring profile (道路監視プロファイル)は、市街地、立ち入り禁止区域、郊外の道路を最大105 km/hで走行する車両を追跡するために最適です。このモードは、人間やその他の種類の物体の検知には使用しないでください。車両以外の物体を追跡するには、**エリア監視プロファイル**, on page 6でレーダーを使用してください。

道路設置例

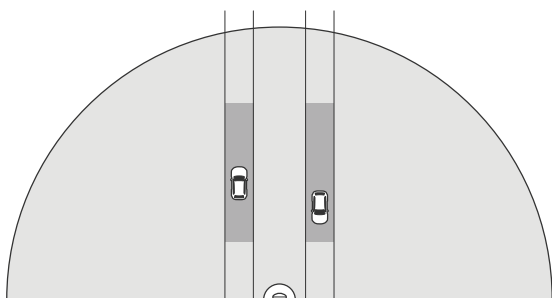
サイド取り付け

道路に沿って走行する車両を監視するには、レーダーを道路の脇に取り付けることができます。レーダーの横方向のカバー距離は10 mです。



センター取り付け

この取り付けオプションでは、安定した位置が必要です。レーダーは、道路の真ん中のポールや道路の上の橋に取り付けることができます。レーダーの両側の横方向のカバー距離は10 mです。レーダーは、センターに取り付けられた場合、横方向のより広い距離をカバーします。



注

レーダーは、Road monitoring profile (道路監視プロファイル) に設定する場合、3 m～8 mの高さに取り付けることをお勧めします。

道路検知範囲

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** (デバイスにどれだけ近づいて検知できるか) から**遠距離検知限界** (デバイス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。

このプロファイルは、車両の検知用に最適化されており、最大105 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。

最適な高さに設置した場合、検知範囲は次のとおりです。

- 60 km/hで走行する車両の場合は25～70 m。
- 105 km/hで走行する車両の場合は30～60 m。

道路監視の使用例

低速ゾーンでの車両の規制

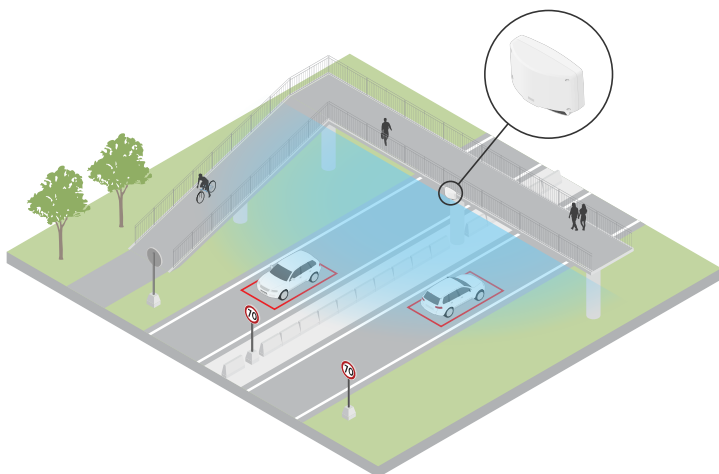
2つの倉庫の間に長い道路がある工業団地では、60 km/hの制限速度を強制するのに役立つレーダーを設置しました。**Road monitoring profile (道路監視プロファイル)**に設定した場合、レーダーは、検知ゾーン内の車両がその制限速度を超えたことを検知できます。その後、ドライバーと管理者に電子メール通知を送信するイベントをトリガーします。このリマインダーは、速度制限の遵守を強化するのに役立ちます。

閉鎖された道路を走行する迷惑車両

古い採石場への細い道路は閉鎖されましたが、この道路を走行する車両が報告されるため、当局はセキュリティレーダーを設置し、**Road monitoring profile (道路監視プロファイル)**に設定しました。レーダーは道路に沿って取り付けられ、道路の全幅をカバーします。車両がシナリオに入ると、点滅するビーコンがトリガーされ、ドライバーに道路を離れるように警告します。また、セキュリティチームにメッセージを送信して、必要に応じてユニットを派遣できるようにします。

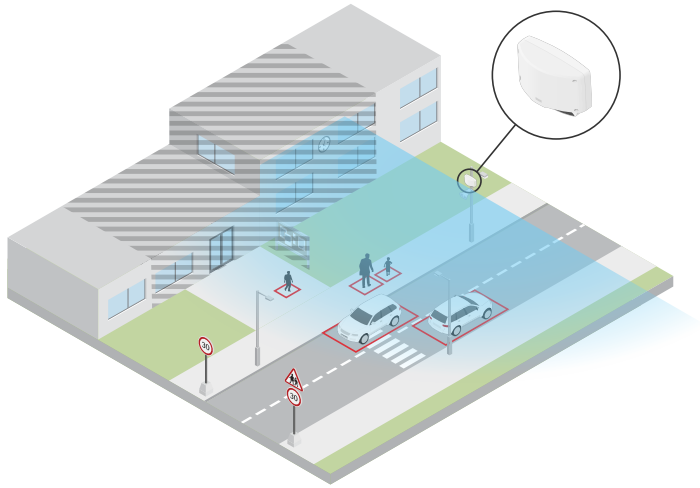
道路での認識のスピードアップ

小さな町を通る道路で、スピード違反が何件もありました。70 km/hの制限速度を適用するために、交通管制部は、道路を横断する橋にセキュリティレーダーを設置し、**Road monitoring profile (道路監視プロファイル)**に設定しました。これにより、車両の走行速度を検知し、交通管制部から交通規制のため道路にユニットを派遣するタイミングを監視できるようになりました。



人間と車両の安全確保

ある学校の職員は、対処すべき2つの安全上の問題を特定しました。学校の授業時間帯に敷地内に立ち入る不審者、規制時速20 kmのスクールゾーンに違反する車両です。レーダーをポールに取り付け、歩道の脇に設置しました。エリア監視プロファイル, on page 6を選択して、55 km/h未満で移動する人間と車両の両方をレーダーが追跡できるようにしました。これにより職員は、授業時間帯に出入りする人を追跡できるだけでなく、スクールゾーンを規定速度を超えて走行する車両があった場合にスピーカーをトリガーして歩行者に警告することもできます。



使用に当たって

ネットワーク上のデバイスを検索する

Windows®で検索したAxisデバイスにIPアドレスの割り当てを行うには、AXIS IP UtilityまたはAXIS Device Managerを使用します。いずれのアプリケーションも無料で、axis.com/supportからダウンロードできます。

IPアドレスの検索や割り当てを行う方法の詳細については、*IPアドレスの割り当てとデバイスへのアクセス方法*を参照してください。

ブラウザーサポート

以下のブラウザーでデバイスを使用できます。

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

✓: 推奨:

*: 制限付きでサポート

装置のwebインターフェースを開く

1. ブラウザーを開き、Axis装置のIPアドレスまたはホスト名を入力します。
この装置のIPアドレスが不明な場合は、AXIS IP UtilityまたはAXIS Device Managerを使用して、ネットワーク上でこの装置を見つけてください。
2. ユーザー名とパスワードを入力します。装置に初めてアクセスする場合は、管理者アカウントを作成する必要があります。管理者アカウントを作成する, *on page 15*を参照してください。

AXIS OS搭載デバイスのWebインターフェースでの全機能と設定に関する説明については、AXIS OS Webインターフェースヘルプを参照してください。

管理者アカウントを作成する

装置に初めてログインするときには、管理者アカウントを作成する必要があります。

1. ユーザー名を入力してください。
2. パスワードを入力します。安全なパスワード, *on page 16*を参照してください。
3. パスワードを再入力します。
4. 使用許諾契約書に同意します。
5. [Add account (アカウントを追加)] をクリックします。

重要

装置にはデフォルトのアカウントはありません。管理者アカウントのパスワードを紛失した場合は、装置をリセットする必要があります。工場出荷時の設定にリセットする, *on page 38*を参照してください。

安全なパスワード

重要

ネットワーク上でパスワードやその他の機密設定を行う場合は、HTTPS (デフォルトで有効になっています) を使用してください。HTTPSを使用すると、安全で暗号化された形でネットワークに接続できるため、パスワードなどの機密データを保護できます。

デバイスのパスワードは主にデータおよびサービスを保護します。Axisデバイスは、さまざまなタイプのインストールで使用できるようにするためパスワードポリシーを強制しません。

データを保護するために、次のことが強く推奨されています。

- 8文字以上のパスワードを使用する (できればパスワード生成プログラムで作成する)。
- パスワードを公開しない。
- 一定の期間ごとにパスワードを変更する (少なくとも年に1回)。

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

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。適切な取り付け高さを設定することは、レーダーが通過する物体を正しく検知し、速度を正確に測定するために重要です。また、オートトラッキングが動作するためにも非常に重要です。

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。地面に凹凸がある場合は、特定の一点からではなく、地面の平均標高から測定してください。

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

検知された物体の移動経路を把握しやすくするため、参考用のマップをアップロードすることができます。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。レーダービューがマップの位置、向き、縮尺に合うようにマップをキャリブレーションし、シーン内の特定の部分に注目する場合はマップを拡大します。

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

ズーム機能によってレーダーの検知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、除外範囲の追加, on page 19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。



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

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

検知ゾーンの設定

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

ゾーンには次の2種類があります。

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

シナリオの追加

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

シナリオを追加する:

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

エリア内で動く物体でトリガーする:

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

ラインを横断する物体でトリガーする:

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

2本のラインを横切る物体でトリガー:

1. [Line crossing (ライン横断)] を選択します。
2. [Next (次へ)] をクリックします。
3. 物体が2本のラインを横切ったときにアラームがトリガーされるようにするには、[Require crossing of two lines (2本のラインを横断することが必要)] をオンにします。
4. シーン内にラインを配置します。
マウスを使用して、ラインを移動したり形状を変更したりします。
5. 検知方向を変更するには、[Change direction (方向の変更)] をオンにします。
6. [Next (次へ)] をクリックします。
7. 検知設定を追加します。
 - 7.1. [Max time between crossings (ライン横断間の最大時間)] で、最初のラインを横切ってから2番目のラインを横切るまでの最大時間を設定します。
 - 7.2. [Trigger on object type (物体タイプでトリガー)] で、トリガーを発動する物体のタイプを選択します。
 - 7.3. [Speed limit (速度制限)] で、速度制限の範囲を追加します。
8. [Next (次へ)] をクリックします。
9. [Minimum trigger duration (最小トリガー継続時間)] でアラームの最小継続時間を設定します。
デフォルト値は2秒に設定されています。物体が2本のラインを横切るたびにシナリオをトリガーする場合は、継続時間を0秒にします。
10. [保存] をクリックします。

除外範囲の追加

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

除外範囲を追加する:

1. [Radar (レーダー)] > [Exclude zones (除外範囲)] に移動します。

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

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、人の検知範囲が広がります。
- 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、*シナリオの追加, on page 18* および *除外範囲の追加, on page 19* 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、*シナリオの追加, on page 18* 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。

ビデオを表示する、録画する

このセクションでは、デバイスの設定について説明します。ストリーミングとストレージの動作の詳細については、ストリーミングとストレージ, on page 30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ブラウザはH.265のデコードに対応していないため、装置はwebインターフェースでH.265をサポートしていません。その代わりに、H.265デコーディングに対応したビデオ管理システムやアプリケーションを使用できます。

ネットワークストレージを設定する

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

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

ビデオを録画して見る

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、ネットワークストレージを設定する, on page 21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。

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, on page 22. 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。
- AXIS Radar Autotracking for PTZを使用してPTZカメラを制御する, on page 23. 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、AXIS Radar Autotracking for PTZを使用してPTZカメラを制御する, on page 23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、除外範囲の追加, on page 19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。

イベントのルールを設定する

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

詳細については、「イベントのルールの使用開始」を参照してください。

アクションをトリガーする

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

4. 条件が満たされたら実行するAction (アクション) を選択します。

囲いが開かれたときに通知をトリガーする

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

メール送信先を追加する:

1. [System (システム)] > [Events (イベント)] > [Recipients (送信先)] に移動し、[Add recipient (送信先の追加)] をクリックします。
2. 送信先の名前を入力します。
3. 通知のタイプとして電子メールを選択します。
4. 送信先の電子メールアドレスを入力します。
5. カメラが通知を送信する際の、送信元電子メールアドレスを入力します。
6. 電子メール送信用アカウントのログイン詳細とSMTPホスト名、ポート番号を入力します。
7. 電子メールの設定をテストするには、[Test (テスト)] をクリックします。
8. [保存] をクリックします。

ルールの作成:

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

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。

以下の手順に従ってデバイスを互いに接続します。

1. レーダーのI/O出力からカメラのI/O入力にワイヤーを接続します。

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)] > [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. ルール名を入力します (例: [Record video upon motion (動体検知で録画)] など)。
5. 条件のリストで、[Radar motion (レーダーの動き)] の下にあるシナリオを選択します。
6. アクションのリストで、[Toggle I/O while the rule is active (ルールがアクティブである間、I/Oを切り替える)] を選択し、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)] > [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. 条件のリストで、[Digital input is active (デジタル入力アクティブ)] 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で、[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で、[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。

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)] > [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、シナリオの追加, on page 18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。

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。

メール送信先を追加する:

1. [System > Events > Recipients (システム > イベント > 送信先)] に移動し、送信先を追加します。
2. 送信先の名前を入力します。
3. [Type (タイプ)] 配下で [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. メールプロバイダーに従って、残りの情報を入力します。
レーダーデバイスには独自のメールサーバーがないため、メールを送信するにはメールサーバーにログインする必要があります。

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。例Tampering mail。
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で、[Notifications (通知)] の下の [Send notification to email (通知を電子メールに送信)] を選択します。
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。

webインターフェース

AXIS OS搭載デバイスのWebインターフェースで利用可能なすべての機能と設定については、AXIS OSウェブインターフェースのヘルプを参照してください。

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う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。

いつでも常に検証を行うのが良い考えです。

- ・ シーン内に除外する物体（植物や金属の表面など）がある。
- ・ レーダーをPTZカメラとペアリングし、Radar autotracking（レーダーオートトラッキング）を設定した。
- ・ レーダーの取り付け高を変更した。

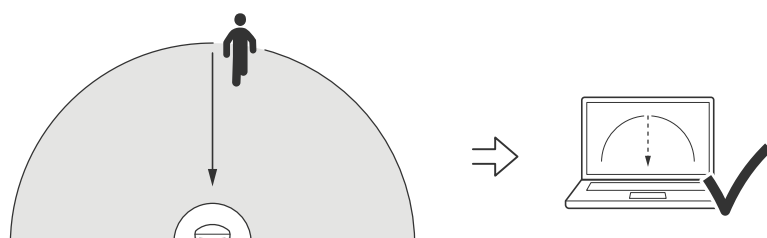
レーダーの検証

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、数分間待つてください。
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、誤報を最小限に抑える, on page 20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

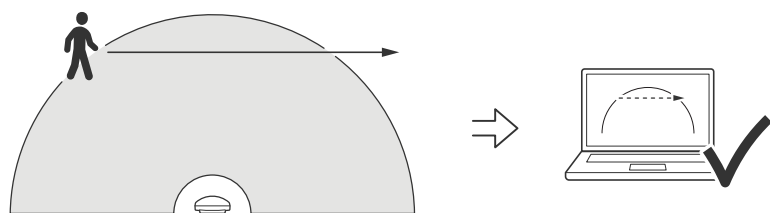
1. レーダーのwebインターフェースに移動し、セッションを録画します。この方法については、ビデオを録画して見る, on page 21を参照してください。
2. レーダーの前方60 mの位置からレーダーに向かってまっすぐ歩きます。
3. レーダーのwebインターフェースで、セッションを確認します。検知されると、人の分類の記号が表示されます。
4. レーダーのwebインターフェースで、移動方向が正しく表示されていることを確認します。



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、ビデオを録画して見る, on page 21を参照してください。
2. レーダーから60 m離れた場所から始め、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。

- 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.エリアに何も無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。

- 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。
- 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。
- 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。
- 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、ビデオを録画して見る, on page 21を参照してください。
- [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、席に帰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。
- 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。
- 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

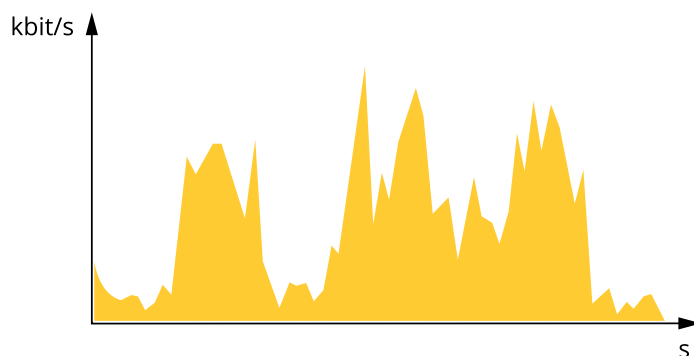
- H.265はライセンスされた技術です。このAxis製品には、H.265閲覧用のクライアントライセンスが1つ添付されています。ライセンスされていないクライアントのコピーをインストールすることは禁止されています。ライセンスを追加購入するには、Axisの販売代理店までお問い合わせください。
- ほとんどのWebブラウザはH.265のデコードに対応していないため、カメラはWebインターフェースでH.265をサポートしていません。その代わりに、H.265のデコーディングに対応した映像管理システムやアプリケーションを使用できます。

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。

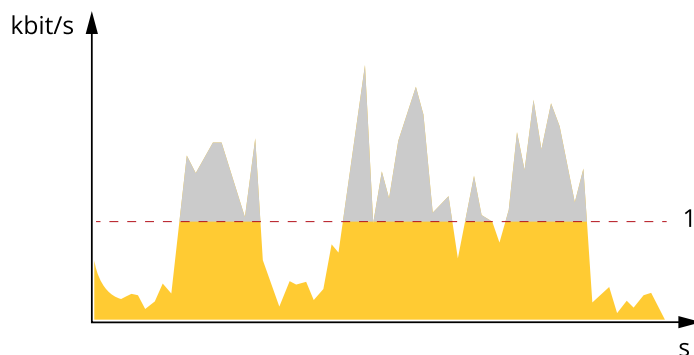
可変ビットレート (VBR)

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。

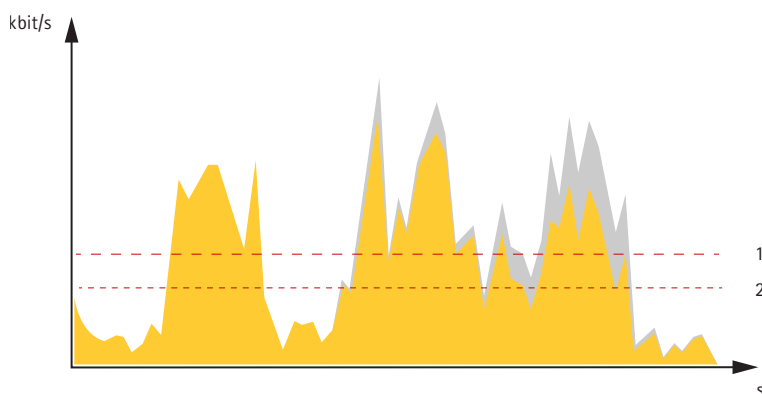


1 目標ビットレート

平均ビットレート (ABR)

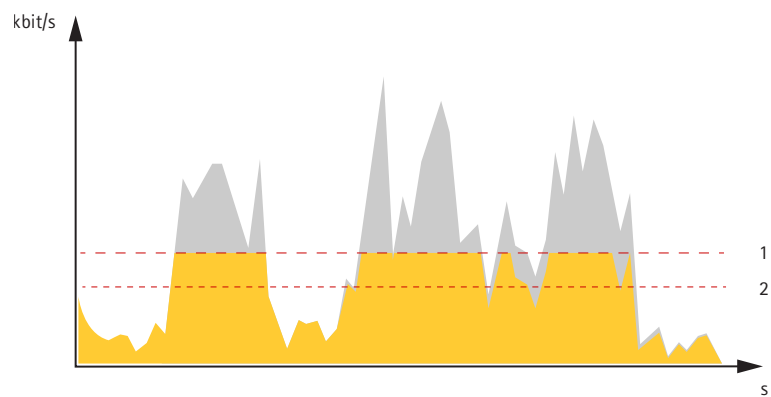
平均ビットレートでは、より長い時間スケールにわたってビットレートが自動的に調整されます。これにより、指定した目標を達成し、使用可能なストレージに基づいて最高画質のビデオを得ることができます。動きの多いシーンでは、静的なシーンと比べてビットレートが高くなります。平均ビットレートオプションを使用すると、多くのアクティビティがあるシーンで画質が向上する可能性が高くなります。指定した目標ビットレートに合わせて画質が調整されると、指定した期間 (保存期間)、ビデオストリームを保存するために必要な総ストレージ容量を定義できます。次のいずれかの方法で、平均ビットレートの設定を指定します。

- 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

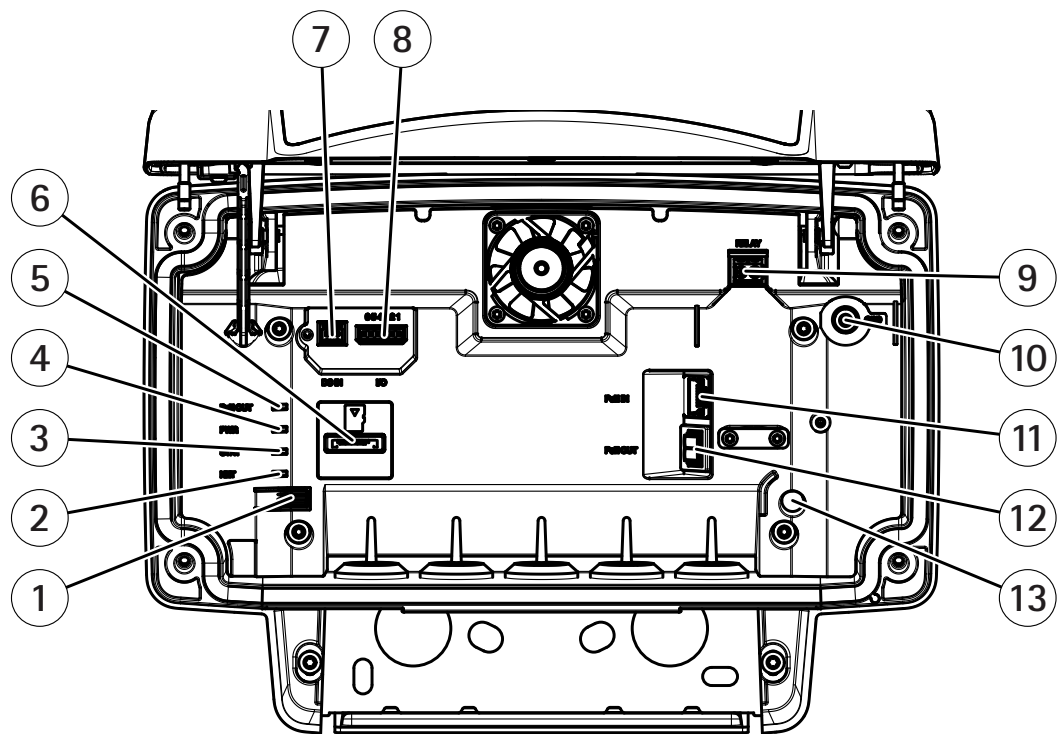
平均ビットレートオプションの中で、最大ビットレートをオンにし、目標ビットレートを指定することもできます。



- 1 目標ビットレート
- 2 実際の平均ビットレート

仕様

製品概要



- 1 コントロールボタン
- 2 ネットワークLED
- 3 ステータスLED
- 4 電源LED
- 5 PoE出力 LED
- 6 microSDカードスロット
- 7 電源コネクタ (DC)
- 8 I/Oコネクタ
- 9 リレーコネクタ
- 10 アース端子ネジ
- 11 ネットワークコネクタ (PoE入力)
- 12 ネットワークコネクタ (PoE出力)
- 13 侵入アラームセンサー

技術仕様については、仕様, on page 33を参照してください。

LEDインジケータ

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。

ネットワークLED	説明
緑	100メガビット/秒のネットワークに接続している場合、点灯します。ネットワークパケットを送受信した場合、点滅します。
オレンジ	10Mbit/sネットワークに接続している場合、点灯します。ネットワークパケットを送受信した場合、点滅します。
消灯	ネットワーク接続なし。

電源LED	説明
緑	正常動作。

PoE出力 LED	説明
消灯	PoE出力がオフになっています
緑	PoE出力がオンになっています

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の位置については、製品概要, on page 33を参照してください。
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。page 38を参照してください。
- AXIS Video Hosting Systemサービスに接続する。を参照してください。接続するには、ステータスLEDが緑色に点滅するまで、ボタンを押し続けます (約3秒間)。

コネクタ

ネットワーク コネクタ

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

▲ 注意

装置の損傷の危険があります。PoEとDCの両方を使用してデバイスの電源を入れないでください。

ネットワークコネクタ (PoE出力)

Power over Ethernet IEEE 802.3at type 2、最大30 W

このコネクタを使用して別の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電力を供給し、セキュリティレーダーがイーサネット接続を提供するようになります。

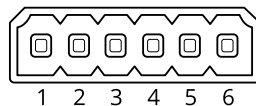
I/Oコネクター

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。

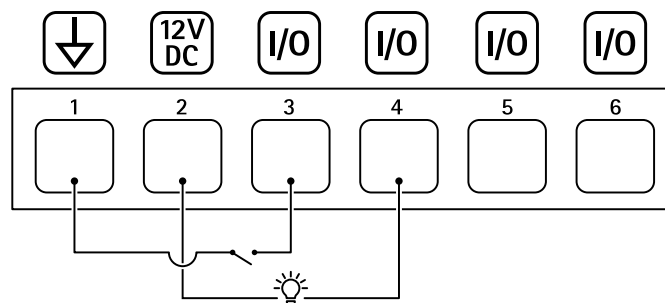
デジタル出力 - リレーやLEDなどの外部装置を接続します。接続された装置は、VAPIX®アプリケーションプログラミングインターフェースを通じたイベントまたは本装置のwebインターフェースから有効にすることができます。

6ピンターミナルブロック



機能	ピン	メモ	仕様
DCアース	1		0 VDC
DC出力	2	 補助装置の電源供給に使用できます。 注:このピンは、電源出力としてのみ使用できます。	12VDC 最大負荷 = 50 mA
設定可能 (入力または出力)	3-6	デジタル入力 - 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 - アクティブ時はピン1 (DCアース) に内部で接続し、非アクティブ時はフロート状態 (未接続) になります。リレーなどの誘導負荷とともに使用する場合は、過渡電圧から保護するために、負荷と並列にダイオードを接続します。	0~30 VDC (最大)、 オープンドレイン、 100 mA

例:

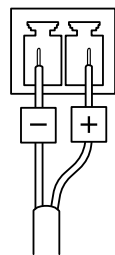


- 1 DCアース
- 2 DC出力12 V、最大50 mA
- 3 I/O (入力として設定)
- 4 I/O (出力として設定)
- 5 設定可能I/O

6 設定可能I/O

電源コネクター

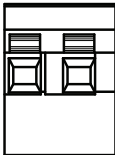
DC電源入力用2ピンターミナルブロック。定格出力が**100 W**以下または**5 A**以下の安全特別低電圧 (SELV) に準拠した有限電源 (LPS) を使用してください。



▲ 注意

装置の損傷の危険があります。PoEとDCの両方を使用してデバイスの電源を入れないでください。

リレーコネクタ



▲ 注意

リレーコネクタには単心線を使用してください。

機能	仕様
タイプ	NO (Normally Open)
定格	24 V DC/5 A
他の回路からの定格絶縁	2.5 kV

装置を清掃する

装置はぬるま湯と低刺激、非研磨性の石鹼で洗浄できます。

注意

- 強力な化学薬品は装置を損傷する可能性があります。窓ガラス用洗剤やアセトンなどの化学薬品を使用して装置をクリーニングしないでください。
- シミの原因となるため、直射日光や高温下での清掃は避けてください。
 1. 圧縮空気を使用すると、装置からほこりやごみを取り除くことができます。
 2. 必要に応じて、ぬるま湯と低刺激、非研磨性の石鹼で湿らせた柔らかいマイクロファイバーの布で装置を清掃してください。
 3. 残った洗浄剤を除去するには、ぬるま湯に浸した柔らかいマイクロファイバーの布で装置を拭いてください。
 4. シミを防ぐために、きれいな非研磨性の布で装置から水分を拭き取ってください。

Axisデバイスの清掃に関する詳細については、ホワイトペーパー「一般的な洗浄剤に対する耐薬品性」をご覧ください。

トラブルシューティング

工場出荷時の設定にリセットする

重要

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

本製品を工場出荷時の設定にリセットするには、以下の手順に従います。

1. 本製品の電源を切ります。
2. コントロールボタンを押した状態で電源を再接続します。製品概要, on page 33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

- デバイスソフトウェアのアップグレードでは、既定の設定とカスタマイズ設定が保存されます。Axis Communications ABは、新しいAXIS OSバージョンで機能が利用可能であっても、設定が保存されることを保証できません。
- AXIS OS 12.6以降、お使いのデバイスの現在のバージョンからアップグレードバージョンまでのすべてのLTSバージョンをインストールする必要があります。たとえば、現在インストールされているデバイスソフトウェアのバージョンがAXIS OS 11.2の場合、デバイスをAXIS OS 12.6にアップグレードする前に、LTSバージョンであるAXIS OS 11.11をインストールする必要があります。詳しくは、AXIS OS Lifecycleガイド: アップグレードパスを参照してください。
- アップグレードプロセス中は、装置を電源に接続したままにしてください。

注

- アクティブトラックのAXIS OSの最新バージョンで装置をアップグレードすると、製品に最新機能が追加されます。アップグレードする前に、AXIS OSと共に提供されるアップグレード手順とリリースノートを必ずお読みください。AXIS OSの最新バージョンとリリースノートについては、axis.com/support/device-software/にアクセスしてください。
- 1. AXIS OSのファイルをコンピューターにダウンロードします。これらのファイルはaxis.com/support/device-software/から無料で入手できます。
- 2. デバイ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。

技術的な問題と解決策

AXIS OSのアップグレード時の問題

AXIS OSアップグレード失敗

アップグレードに失敗した場合、装置は前のバージョンを再度読み込みます。最も一般的な理由は、AXIS OSの間違ったファイルがアップロードされた場合です。装置に対応したAXIS OSのファイル名であることを確認し、再試行してください。

AXIS OSのアップグレード後の問題

アップグレード後に問題が発生する場合は、**[Maintenance (メンテナンス)]** ページから、以前にインストールされたバージョンにロールバックします。

IPアドレスの設定で問題が発生する

IPアドレスを設定できない

- デバイス用のIPアドレスと、デバイスへのアクセスに使用するコンピューターのIPアドレスが異なるサブネットにある場合は、IPアドレスを設定することはできません。ネットワーク管理者に連絡して、適切なIPアドレスを取得してください。
- そのIPアドレスは別のデバイスで使用されている可能性があります。以下の手順で確認してください。
 1. デバイスをネットワークから切断します。
 2. コマンドウィンドウまたはDOSウィンドウで、pingコマンドとデバイスのIPアドレスを入力します。
 3. `Reply from <IP address>: bytes=32; time=10...`という応答を受取った場合は、ネットワーク上の別のデバイスでそのIPアドレスがすでに使われている可能性があります。ネットワーク管理者から新しいIPアドレスを取得し、デバイスを再度インストールしてください。
 4. `Request timed out`が表示された場合は、AxisデバイスでそのIPアドレスを使用できます。この場合は、すべてのケーブル配線をチェックし、デバイスを再度インストールしてください。
- 同じサブネット上の別のデバイスとIPアドレスの競合が発生している可能性があります。DHCPサーバーによって動的アドレスが設定される前は、Axisデバイスは静的IPアドレスを使用します。つまり、デフォルトの静的IPアドレスが別のデバイスでも使用されていると、デバイスへのアクセスに問題が発生する可能性があります。

デバイスへのアクセスの問題

ブラウザからデバイスにアクセスする際、ログインできない

HTTPSが有効になっている場合、ログインを試行するときに正しいプロトコル (HTTPまたはHTTPS) を使用していることを確認します。場合によっては、ブラウザのアドレスフィールドに手動でhttpまたはhttpsを入力する必要があります。

rootアカウントのパスワードを忘れた場合は、デバイスを工場出荷時の設定にリセットする必要があります。手順については、工場出荷時の設定にリセットする, on page 38を参照してください。

DHCPによってIPアドレスが変更された

DHCPサーバーから取得したIPアドレスは動的なアドレスであり、変更されることがあります。IPアドレスが変更された場合は、AXIS IP UtilityまたはAXIS Device Managerを使用してデバイスのネットワーク上の場所を特定してください。デバイスのモデルまたはシリアル番号、あるいはDNS名 (設定されている場合) を使用してデバイスを識別します。

必要に応じて、静的なIPアドレスを手動で割り当てることができます。手順については、axis.com/supportにアクセスしてください。

IEEE 802.1X使用時の証明書エラー

認証を正しく行うには、Axisデバイスの日付と時刻をNTPサーバーと同期させなければなりません。[System (システム) > Date and time (日付と時刻)] に移動します。

ブラウザがサポートされていません

推奨ブラウザの一覧は、ブラウザーサポート, on page 15を参照してください。

外部からデバイスにアクセスできません

装置に外部からアクセスする場合は、以下のいずれかのWindows®向けアプリケーションを使用することをお勧めします。

- AXIS Camera Station Edge : 無料で使用でき、最小限の監視が必要な小規模システムに最適です。
- AXIS Camera Station Pro:90日間の試用版を無料で使用でき、中小規模のシステムに最適です。

手順とダウンロードについては、axis.com/vmsにアクセスしてください。

MQTTの問題

MQTTオーバSSLを使用してポート8883経由で接続できない

ファイアウォールは、ポート8883を使用する通信を安全ではないとみなし、ブロックします。

場合によっては、サーバー/ブローカーによってMQTT通信用に特定のポートが提供されていない可能性があります。この場合でも、HTTP/HTTPSトラフィックに通常使用されるポート経由でMQTTを使用できる場合もあります。

- サーバー/ブローカーが、通常はポート443経由で、WebSocket/WebSocket Secure (WS/WSS) をサポートしている場合は、代わりにこのプロトコルを使用してください。サーバー/ブローカープロバイダーに問い合わせ、WS/WSSがサポートされているかどうか、どのポートと基本パスを使用するかを確認してください。
- サーバー/ブローカーがALPNをサポートしている場合、MQTTの使用は443などのオープンポートでネゴシエートできます。ALPNのサポートの有無、使用するALPNプロトコルとポートについては、サーバー/ブローカーのプロバイダーに確認してください。

このページで解決策が見つからない場合は、axis.com/supportのトラブルシューティングセクションに記載されている方法を試してみてください。

パフォーマンスに関する一般的な検討事項

システムを設定する際には、さまざまな設定や条件が必要な帯域幅 (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。

考慮すべき最も重要な要因:

- 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。

サイバーセキュリティ

サイバーセキュリティは、リスクを最小限に抑えながら、健全な製品ライフサイクルを支援します。当社のサイバーセキュリティへの取り組みに関する詳細や文書は、axis.com/about-axis/cybersecurityで確認できます。以下のサイバーセキュリティガイドラインに従って、Axisから製品に関するセキュリティ通知を受け取り、安全なライフサイクルと利用停止を確保するために製品を設定してください。

Axis Trust Centerでは、Axisが実施するセキュリティコンプライアンス、透明性、データ保護、およびプライバシーについての情報をご覧ください。

脆弱性の管理

Axisは、共通脆弱性識別子 (CVE) 採番機関 (CNA)です。当社は、セキュリティリスクを最小限に抑えるため、当社のデバイス、ソフトウェア、およびサービスの脆弱性の特定と修正において業界標準に従って対応しています。当社の脆弱性管理ポリシーに関する詳細や、脆弱性の報告については、axis.com/vulnerability-managementを参照してください。

セキュリティ通知

axis.com/security-notification-serviceでAxisのセキュリティ通知メールを受け取る用に設定してください。お使いのAxis製品に関する脆弱性、関連するセキュリティアドバイザリー、およびその他のセキュリティ関連事項に関する情報を送信いたします。

安全な製品ライフサイクル管理

Axisは、安全なライフサイクル管理を通じて、製品のライフサイクル全体でリスクを最小限に抑えています。help.axis.comに掲載されているハードニングガイドには、Axis製品のより安全な設定と操作に関する情報、および以下の情報が含まれています。

安全な初回使用 - Axis製品は、高度な保護機能がデフォルトで組み込まれているため、初回使用時から安全な初期化と暗号化された通信が可能です。

使用目的とよくある設定ミス - 当社のガイドには、Axis製品の使用目的について記載されています。これには、避けるべきよくあるセキュリティ関連の誤った使用や設定ミスについても含まれています。

脆弱性の管理とサプライチェーンの透明性 - 脆弱性の開示およびサプライチェーンの透明性向上を目的として、ソフトウェアのリリースごとに、axis.comでソフトウェア部品表 (SBOM) を公開しています。

利用停止とデータの安全な消去 - 製品のライフサイクル終了時に安全に利用を停止するために、工場出荷時の設定にリセットしてください。これにより、設定、保存されたデータ、およびセンシティブな情報が消去されます。

T10145149_ja

2026-07 (M33.2)

© 2020 – 2026 Axis Communications AB