

AXIS D2110-VE Security Radar

ユーザーマニュアル

AXIS D2110-VE Security Radar

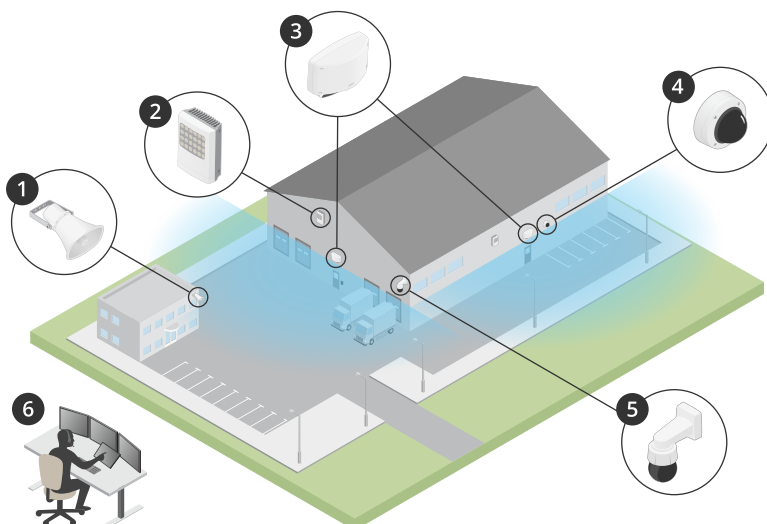
目次

ソリューションの概要	3
レーダープロファイル	3
製品の設置場所	3
カバー範囲	4
エリア監視プロファイル	5
複数のレーダーを設置する	5
エリア設置例	6
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
道路監視の使用事例	13
はじめに	15
ネットワーク上の装置を検索する	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	15
webインターフェースの概要	16
装置を構成する	17
レーダーキャリブレーションを行う	17
検知ゾーンの設定	17
誤報を最小限に抑える	20
ビデオを表示する、録画する	21
イベントのルールを設定する	22
webインターフェース	27
ステータス	27
レーダー	28
録画	35
アプリ	36
システム	36
保守	58
インストールの検証	59
レーダーの設置を検証する	59
レーダーの検証	59
検証を完了する	62
詳細情報	63
ストリーミングとストレージ	63
仕様	66
製品の概要	66
SDカードスロット	67
ボタン	67
コネクタ	67
清掃の推奨事項	70
トラブルシューティング	71
工場出荷時の設定にリセットする	71
現在のファームウェアバージョンの確認	71
ファームウェアのアップグレード	71
技術的な問題、ヒント、解決策	72
パフォーマンスに関する一般的な検討事項	73

AXIS D2110-VE Security Radar

ソリューションの概要

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

レーダープロフィール

注

レーダープロフィールを使用するには、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つのプロフィールがあります。

- ・ **エリア監視プロフィール**。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。
- ・ **道路監視プロフィール**。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。

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

製品の設置場所

- ・ 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。

AXIS D2110-VE Security Radar

ソリューションの概要

- 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、5 ページ複数のレーダーを設置する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5,600 m²、車両の場合は11,300 m²に相当します。

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。

AXIS D2110-VE Security Radar

エリア監視プロファイル

エリア監視プロファイル

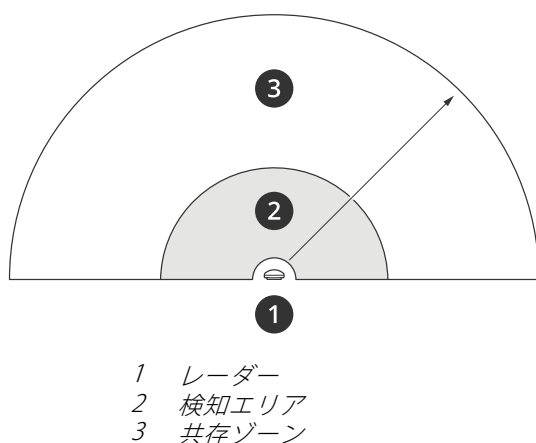
エリア監視プロファイルは、最大55 km/hで移動する物体用に最適化されます。このプロファイルを使用すると、物体が人、車両、不明のいずれであるかを検知できます。これらの物体のいずれかが検知されたときにアクションをトリガーするようにルールを設定できます。高速で移動する車両を追跡するには、12ページ、道路監視プロファイルを使用します。

複数のレーダーを設置する

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、6 ページ *エリア設置例* 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。

AXIS D2110-VE Security Radar

エリア監視プロファイル

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。



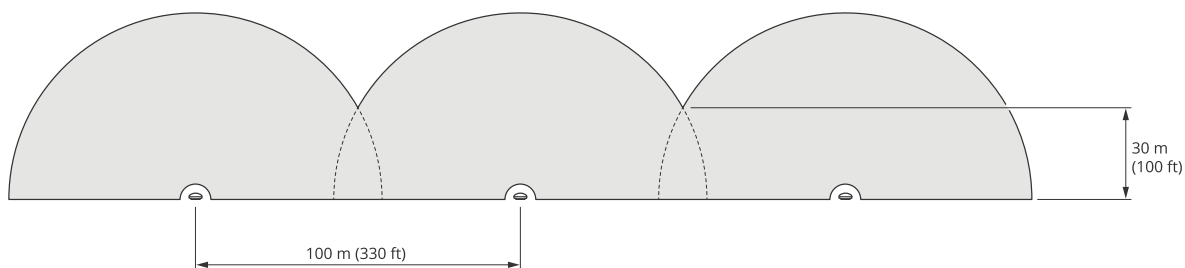
これは、同じ共存ゾーンに並べて設置した複数のレーダーをグループ化する例です。

複数のレーダーを設置するその他の例については、6 ページエリア設置例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。



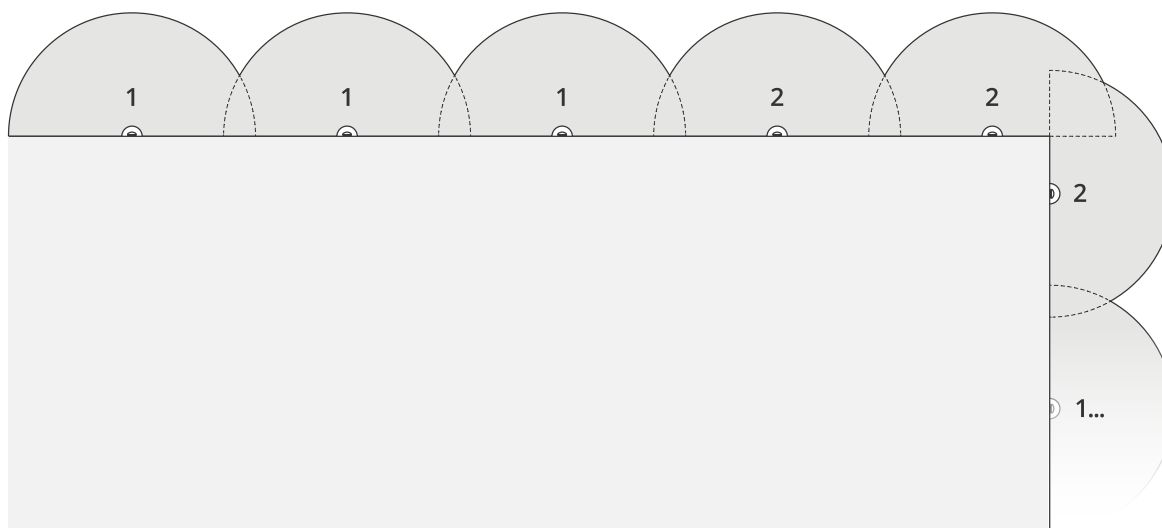
同じ共存ゾーンに3台以上のレーダーを設置した場合の干渉を避けるには、装置インターフェースで隣接するレーダーの数を設定します。さらに、4台以上のレーダーを設置する場合は、各レーダーをグループに追加します。



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。

AXIS D2110-VE Security Radar

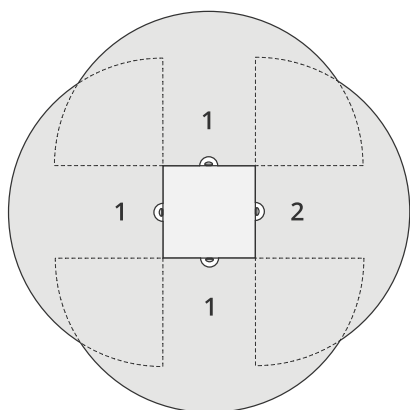
エリア監視プロファイル



隣接するレーダーとグループの詳細については、5 ページ複数のレーダーを設置するを参照してください。

建物の周囲をカバーする

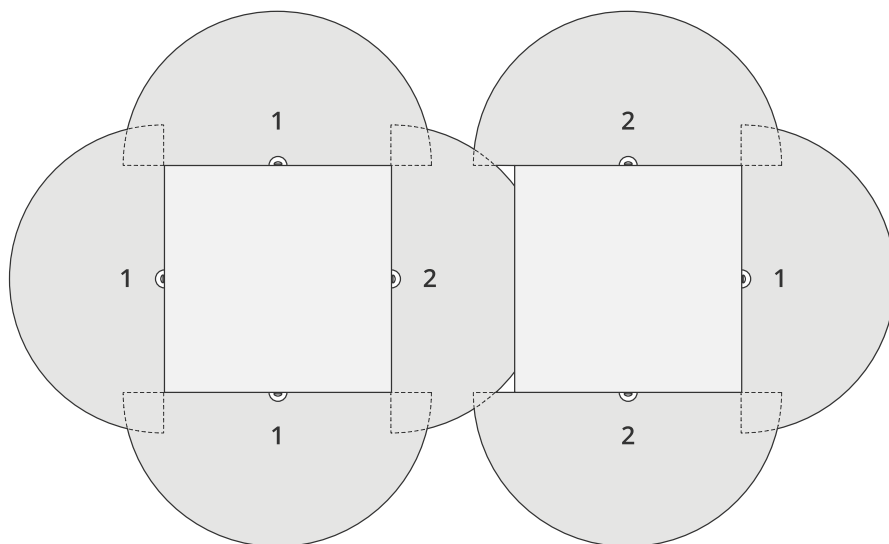
建物の周囲をカバーするには、ビルの壁に外側に向けてレーダーを配置します。同じ共存ゾーンに4台以上のレーダーを設置する場合は、この例のように、装置インターフェースで隣接するレーダーの数を設定し、各レーダーをグループに追加します。



また、複数の建物の周囲をカバーすることもできます。

AXIS D2110-VE Security Radar

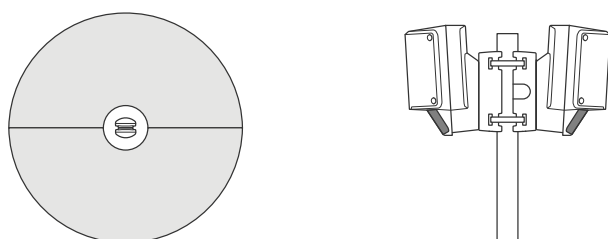
エリア監視プロファイル



隣接するレーダーとグループの詳細については、5 ページ複数のレーダーを設置する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。

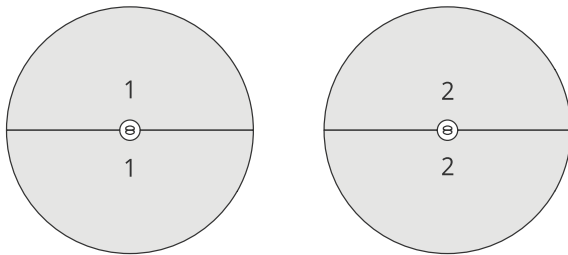
注

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。

AXIS D2110-VE Security Radar

エリア監視プロファイル



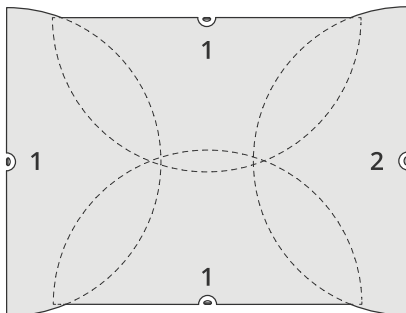
隣接するレーダーとグループの詳細については、5 ページ複数のレーダーを設置するを参照してください。

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、5 ページ複数のレーダーを設置する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** (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。

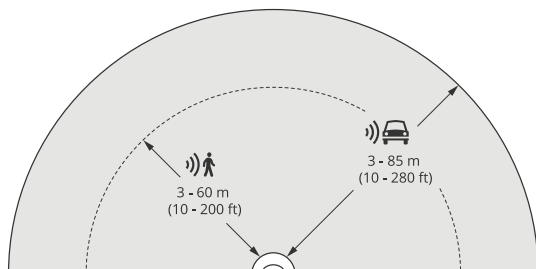
エリア監視プロファイルは人間の検知用に最適化されていますが、最大55 km/hで走行する車両やその他の物体を ± 2 km/hの速度精度で追跡するためにも使用できます。

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**

AXIS D2110-VE Security Radar

エリア監視プロファイル



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。
- ・ この人物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)]** に設定されています。

取り付け高さ	チルト0°	チルト10°	チルト20°
2.5 m	3.0～60 m	非推奨	非推奨
3.5 m	3.0～60 m	非推奨	非推奨
4.5 m	4.0～60 m	非推奨	非推奨
5.5 m	7.5～60 m	非推奨	非推奨
6.5 m	7.5～60 m	5.5～60 m	非推奨
8 m	非推奨	9～60 m	7.5～30 m
10 m	非推奨	15～60 m	9～35 m
12 m	非推奨	23～60 m	13～38 m
14 m	非推奨	27～60 m	17～35 m
16 m	非推奨	非推奨	25～50 m

AXIS D2110-VE Security Radar

エリア監視プロファイル

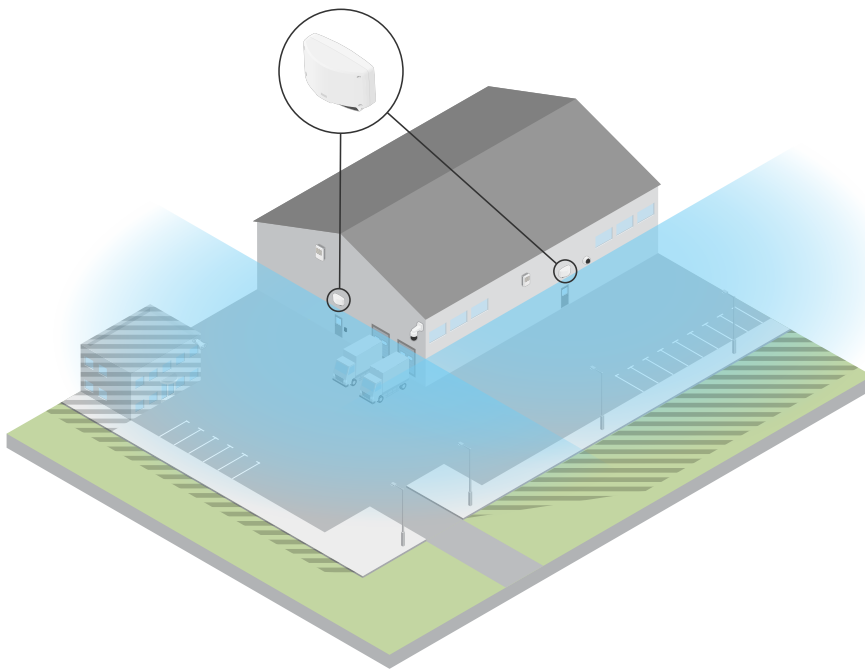
エリア監視の使用例

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)**に設定することになりました。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っています。

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なりました。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できます。



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)**に設定することになりました。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。

AXIS D2110-VE Security Radar

道路監視プロフィール

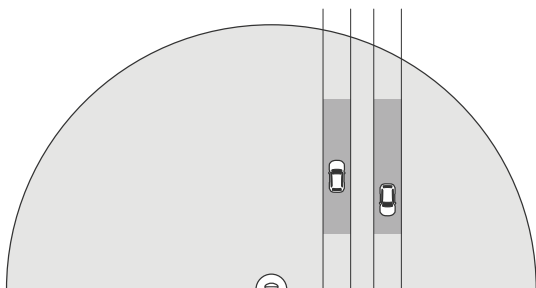
道路監視プロフィール

Road monitoring profile (道路監視プロフィール)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、5 ページ、エリア監視プロフィールでレーダーを使用してください。

道路設置例

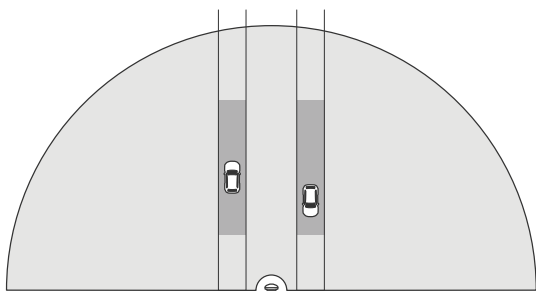
サイド取り付け

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 (道路監視プロフィール) に設定する場合、3 m～8 mの高さに取り付けをお勧めします。

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** (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。

このプロフィールは、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。

AXIS D2110-VE Security Radar

道路監視プロファイル

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**。

注

同じ共存ゾーン内のレーダーの最大数が2台を超える場合、検知限界は約10% (近距離) および20% (遠距離) 低下すると見込まれます。

道路監視の使用事例

低速ゾーンでの車両の規制

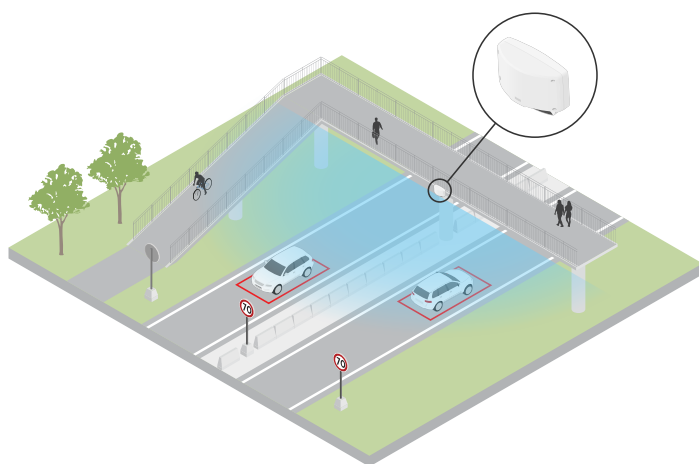
2つの倉庫の間に長い道路がある工業団地では、60 km/hの制限速度を強制するのに役立つレーダーを設置しました。**Road monitoring profile (道路監視プロファイル)** に設定した場合、レーダーは、検知ゾーン内の車両がその制限速度を超えたことを検知できます。その後、ドライバーと管理者に電子メール通知を送信するイベントをトリガーします。このリマインダーは、速度制限の遵守を強化するのに役立ちます。

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。

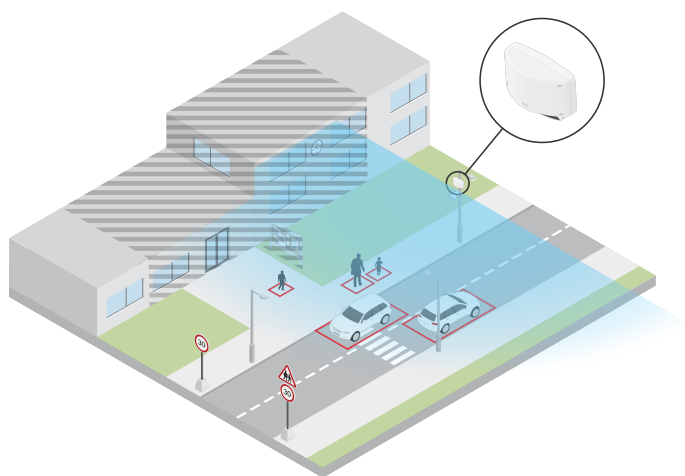


人間と車両の安全確保

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。**5 ページ エリア監視プロファイル** 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。

AXIS D2110-VE Security Radar

道路監視プロフィール



AXIS D2110-VE Security Radar

はじめに

はじめに

ネットワーク上の装置を検索する

Windows®でAxis装置を探してIPアドレスの割り当てを行う方法については、AXIS IP UtilityまたはAXIS Device Managerを使用してください。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装置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装置を使用できます。

	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、**[設定] > [Safari] > [詳細] > [Experimental Features]** 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。15ページ**管理者アカウントを作成する**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。15ページ**安全なパスワード**を参照してください。
3. パスワードを再入力します。
4. **[Add user (ユーザーの追加)]** 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。71ページ**工場出荷時の設定にリセットする**を参照してください。

AXIS D2110-VE Security Radar

はじめに

安全なパスワード

重要

Axis装置は、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装置を保護するために、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。

装置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装置は、さまざまなタイプのインストールで使われる可能性があることから、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、次のことを強く推奨します。

- 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。



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。

help.axis.com/?&piald=45364§ion=web-interface-overview

Axis装置のwebインターフェース

AXIS D2110-VE Security Radar

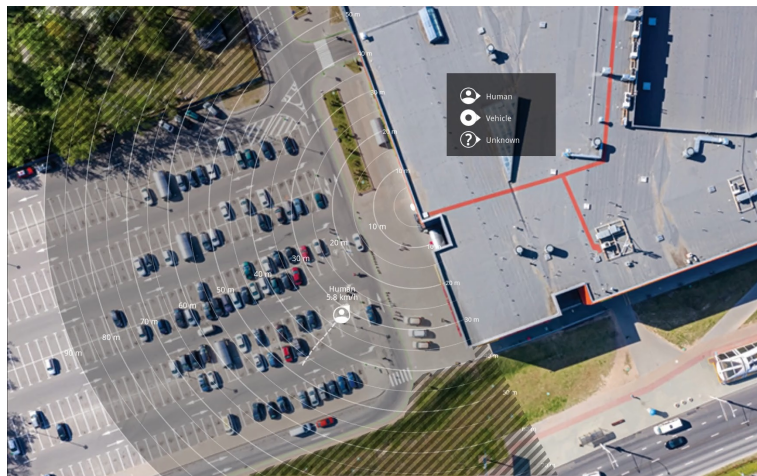
装置を構成する

装置を構成する

レーダーキャリブレーションを行う

本レーダーは取り付け後すぐにご利用いただけます。デフォルトのライブビューにはレーダーの検知範囲と検知した動きが表示され、検知ゾーンやルールをすぐに追加できます。

レーダーが地上3.5 mに設置されている場合は、他に何もする必要はありません。レーダーが別の高さに取り付けられている場合は、レーダーのキャリブレーションを行って、取り付けの高さを補正する必要があります。



物体が動いている場所を見やすくするために、平面図や航空写真など、レーダーがカバーしている範囲を示す参照マップをアップロードすることができます。

画像の要件は以下のとおりです。

- サポートされるファイル形式は、jpegとpngです。
- キャリブレーション中にレーダーの到達範囲の形状が画像に合わせて移動するため、向きは重要ではありません。

参照マップのアップロード

参照マップをアップロードし、実際のレーダー検知範囲がマップの位置、方向、縮尺に合うようにキャリブレーションします。

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. 参照マップをアップロードし、設定アシスタントの手順に従います。

検知ゾーンの設定

動きを検知する場所を決定するために、複数のゾーンを追加できます。さまざまなゾーンを使用して、さまざまなアクションをトリガーすることができます。

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。

AXIS D2110-VE Security Radar

装置を構成する

- [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 (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。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。
 - 5.1 [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。
 - 5.2 [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。
 - 5.3 [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. [Save (保存)] をクリックします。

ラインを横切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。

AXIS D2110-VE Security Radar

装置を構成する

- 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. [Save (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. [Save (保存)] をクリックします。

除外範囲の追加

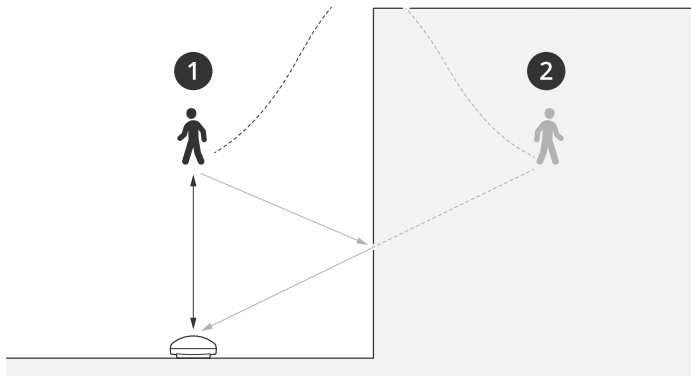
除外範囲は、動く物体が無視されるエリアです。除外範囲を追加すると、誤報の原因となる動く物体のあるエリアを無視できます。

例::

金属屋根、フェンス、車両、レンガの壁など、レーダーを反射する材質は、レーダーのパフォーマンスを低下させる可能性があります。また、反射やゴースト追跡が生じ、見かけ上の検知と実際の検知と見分けるのが困難になる場合があります。

AXIS D2110-VE Security Radar

装置を構成する



- 1 実際の検知
- 2 反射の検知

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。

注

ファームウェアバージョン11.4から、除外範囲の数に制限がなくなりました。

誤報を最小限に抑える

誤報が多すぎる場合は、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。



- **Low (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。
- **Medium (中):** デフォルトの設定です。
- **High (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、18ページシナリオの追加および19ページ除外範囲の追加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。

AXIS D2110-VE Security Radar

装置を構成する

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、18ページシナリオの追加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、装置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、63ページストリーミングとストレージ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。

- [Radar (レーダー)] > [Stream (ストリーム)] に移動します。
- ライブビューで、 をクリックします。
- [Video format (ビデオ形式) H.264] を選択します。
- [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。

AXIS D2110-VE Security Radar

装置を構成する


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. [[Add (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、 [Set up (設定)]  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、次を参照してください: 22ページネットワークストレージを設定する

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装置が実行する [Action (アクション)] を選択します。

AXIS D2110-VE Security Radar

装置を構成する

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。

誰かがハウジングを開いた場合にアラームをトリガーする

この例では、誰かがハウジングを開いた場合にアラームをトリガーする方法について説明します。

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. [Save (保存)] をクリックします。

ルールを作成する:

8. [System > Events > Rules (システム > イベント > ルール)] に移動し、ルールを追加します。
9. ルールの名前を入力します。
10. 条件のリストで、[Casing open (ケーシング開放)] を選択します。
11. アクションのリストで、[Send notification to email (電子メールに通知を送信する)] を選択します。
12. リストから送信先を選択します。
13. 電子メールの件名とメッセージを入力します。
14. [Save (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、レーダーが動きを検知する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示します。

装置の接続:

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ポートを設定する:

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、18ページシナリオの追加を参照してください。

AXIS D2110-VE Security Radar

装置を構成する

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. **[Save (保存)]**をクリックします。

カメラのI/Oポートを設定する:

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. 条件のリストから**[Digital input is active (デジタル入力 that 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. **[Save (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。

装置の接続:

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を設定する:

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、18ページシナリオの追加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。

AXIS D2110-VE Security Radar

装置を構成する

9. [Save (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。

- 25ページ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。
- 26ページAXIS Radar Autotracking for PTZを使用してPTZカメラを制御する. 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。

この手順では、PTZカメラをレーダーとペアリングする方法、カメラを調整する方法、物体の追跡を設定する方法について説明します。

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、26ページAXIS Radar Autotracking for PTZを使用してPTZカメラを制御する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. [Connect (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 (レーダー)] > [Autotracking (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 (レーダー)] > [Autotracking (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。

トラッキングは、自動的に物体または物体のグループに自動的にズームインし、カメラの視野内に収まるよう追跡します。

AXIS D2110-VE Security Radar

装置を構成する

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台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。


AXIS D2110-VE Security Radar

webインターフェース

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。
- ・  **Change account (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。
- ・  **Log out (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**: ファームウェア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。
- ・ **Legacy device interface (従来のデバイスインターフェース)**: 装置のwebインターフェースを従来のバージョンに変更します。

ステータス

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 **[Date and time (日付と時刻)]** のページに移動します。

進行中の録画

進行中の録画と指定されたストレージ容量を表示します。

AXIS D2110-VE Security Radar

webインターフェース

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、[35ページ録画](#)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。

装置情報

ファームウェア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 firmware (ファームウェアのアップグレード): 装置のファームウェアをアップグレードします。ファームウェアの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。

Connected clients (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、各クライアントのIPアドレス、プロトコル、ポート、PID/プロセスが表示されます。

レーダー

設定

General (全般)

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。

共存

AXIS D2110-VE Security Radar

webインターフェース

隣接レーダーの数: 同じ共存ゾーン内に設置された隣接するレーダーの数を選択します。これは干渉を回避するのに役立ちます。共存ゾーンの半径は350 mです。

- 0-1: 同じ共存ゾーンに1~2台のレーダーを設置する場合は、このオプションを選択します。
- 2: 同じ共存ゾーンに3台のレーダーを設置する場合は、このオプションを選択します。
- 3-5: 同じ共存ゾーンに4~6台のレーダーを設置する場合は、このオプションを選択します。
 - **Groups (グループ):** レーダーのグループ ([Group 1 (グループ1)] または [Group 2 (グループ2)]) を選択します。これも干渉を回避するのに役立ちます。各グループに3台のレーダーを追加し、最も近いレーダー同士を同じグループに追加することをお勧めします。



詳細については、5 ページ複数のレーダーを設置するを参照してください。

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は排除されますが、検知範囲が短くなる場合があります。

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 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。
 - **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。
- **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 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。


ビュー

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。

Grid opacity (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

AXIS D2110-VE Security Radar

webインターフェース

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。

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。

除外範囲の **Zone shape presets (範囲形状プリセット)** のいずれかを選択します。[Cover everything (すべてをカバー)]を選択すると、範囲がレーダーのカバーエリア全体に設定されます。[Reset to box (ボックスにリセット)]を選択すると、カバーエリアの中央に四角形が作成されます。

範囲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。
- **Line crossing (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。

AXIS D2110-VE Security Radar

webインターフェース

- **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。

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。これにより、レーダーがカバーするエリア内で物体が動いている場所がわかりやすくなります。

Upload map (マップのアップロード): アップロードする参照マップを選択します。

Set radar position on map (マップ上でレーダーの位置を設定する): マップ上でレーダーの位置を指定し、レーダーの真正面に基準点を追加して、レーダーと基準点との距離を入力します。[**Calibrate (キャリブレーション)**] をクリックして、キャリブレーションを開始します。

キャリブレーションの結果、レーダーの検知範囲が適切な縮尺で表示された参照マップが作成されます。


ストリーム

一般

Resolution (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、必要な帯域幅とストレージ容量が増大します。

Frame rate (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。

Compression (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。

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


Zipstream (Zipstream テクノロジー)

P-frames (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。値が大きいくほど、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。


AXIS D2110-VE Security Radar







webインターフェース

Bitrate control (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。
 - **Storage (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。








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。
 - **Size (サイズ):** フォントサイズを選択します。
 - **Appearance (外観):** 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。
 -  : 画像内のオーバーレイの位置を選択します。
- **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: FFFFFFFF - 白、000000 - 黒、FF0000 - 赤、6633FF - 青、669900 - 緑。 .bmp 画像の場合のみ。
- **Scene annotation (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。

AXIS D2110-VE Security Radar

webインターフェース

- **Size (サイズ):** フォントサイズを選択します。
- **Appearance (外観):** 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。
-  : 画像内のオーバーレイの位置を選択します。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。
- **Streaming indicator (ストリーミングインジケーター)  :** ビデオストリームにアニメーションを重ねて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。
 - **Appearance (外観):** 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。
 - **Size (サイズ):** フォントサイズを選択します。
 -  : 画像内のオーバーレイの位置を選択します。
- **Widget: Linegraph (ウィジェット: 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。
 - **Title (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。
 -  : 画像内のオーバーレイの位置を選択します。
 - **Size (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 axis (X軸)**
 - **Label (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 axis (Y軸)**
 - **Label (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: Meter (ウィジェット: 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。
 - **Title (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。
 -  : 画像内のオーバーレイの位置を選択します。
 - **Size (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。

AXIS D2110-VE Security Radar

webインターフェース

- **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 axis (Y軸)**
- **Label (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。

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。

レーダーPTZオートトラッキング:

初期設定を構成する:

Camera mounting height (カメラの取り付け高さ): 地面から取り付けられた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。トラッキングは、自動的に物体または物体のグループに自動的にズームインし、カメラの視野内に収まるよう追跡します。

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。

Return to home (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。

Zoom (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。

AXIS D2110-VE Security Radar

webインターフェース


録画


Ongoing recordings (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。

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。

Source (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。

Storage (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。

AXIS D2110-VE Security Radar

webインターフェース

アプリ



Add app (アプリの追加): 新しいアプリをインストールします。

Find more apps (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。

Allow unsigned apps (署名なしアプリを許可): 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。

Allow root-privileged apps (root権限アプリの許可): オンにして、root権限を持つアプリに装置へのフルアクセスを許可します。



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。

Open (開く): アプリの設定にアクセスする。利用可能な設定は、アプリケーションによって異なります。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。ライセンスキーを生成するには、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、ライセンスは装置から削除されます。
- **Settings (設定):** パラメーターを設定します。
- **Delete (削除):** 装置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

時間と場所

日付と時刻

時刻の形式は、Webブラウザ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。

AXIS D2110-VE Security Radar

webインターフェース

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。
- **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。
- **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。
- **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。

Time zone (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。

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。

装置の位置

装置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、マップ上に装置を配置できます。

- **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:** 装置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:** 分かりやすい装置名を入力します。
- **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。

メートル法 (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。

米国慣用単位 (フィート、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

AXIS D2110-VE Security Radar

webインターフェース

Assign IPv4 automatically (IPv4 自動割り当て): 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。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 address (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、固定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。

Subnet mask (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。

Hostname (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。

Hostname (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 servers (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および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。暗号化された情報の交換は、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証明書の使用により制御されます。

装置で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 > Security (システム > 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。

AXIS D2110-VE Security Radar

webインターフェース

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®: オンにすると、ネットワーク上で自動検出が可能になります。

Bonjour name (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。デフォルト名は装置名とMACアドレスです。

UPnP®: オンにすると、ネットワーク上で自動検出が可能になります。

UPnP name (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。デフォルト名は装置名とMACアドレスです。

WS-Discovery: オンにすると、ネットワーク上で自動検出が可能になります。

One-Click Cloud Connection (ワンクリッククラウド接続)

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):

- **One-click (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、装置はO3Cサービスから切断されます。装置に登録すると、**[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。
- **Always (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。装置に登録すると、装置はO3Cサービスに接続したままになります。装置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。
- **No (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。

Host (ホスト): プロキシサーバーのアドレスを入力します。

Port (ポート): アクセスに使用するポート番号を入力します。

Login (ログイン) と Password (パスワード): 必要な場合は、プロキシ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)

AXIS D2110-VE Security Radar

webインターフェース

• **Basic (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。

• **Digest (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。

• **Auto (オート):** このオプションを使用すると、装置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。**Digest (ダイジェスト)** 方式が**Basic (ベーシック)** 方式より優先されます。

Owner authentication key (OAK) (所有者認証キー、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、装置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 (パブリック)]** 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。デフォルト値は **[write (書き込み)]** です。
 - **Activate traps (トラップの有効化):** オンにすると、トラップレポートが有効になります。装置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):** 装置の起動時にトラップメッセージを送信します。
 - **Warm start (ウォームスタート):** SNMP設定が変更されたときに、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。
 - **Authentication failed (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、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。

セキュリティ

証明書

AXIS D2110-VE Security Radar

webインターフェース

証明書は、ネットワーク上の装置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

装置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。



リスト内の証明書をフィルターします。



証明書の追加: クリックして、証明書を追加します。

- **More (詳細)** : 入力または選択するフィールドをさらに表示します。
- **Secure keystore (セキュアキーストア):** [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 :

- **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。

IEEE 802.1x and IEEE 802.1AE MACsec (IEEE 802.1xおよびIEEE 802.1AE MACsec)

AXIS D2110-VE Security Radar

webインターフェース

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装置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。

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、装置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。デフォルトのオプションはEAP-TLSです。

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 certificate (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、装置は、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 identity (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 version (EAPOLのバージョン): ネットワークスイッチで使用する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。

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。

この設定は、認証方法としてEAP-TLSを使用する場合にのみ使用できます。

Mode (モード)

- **Dynamic CAK / EAP-TLS (動的CAK/EAP-TLS):** デフォルトのオプションです。セキュリティで保護された接続の後、装置はネットワーク上のMACsecをチェックします。
- **Static CAK / pre-shared key (PSK) (静的CAK/事前共有キー (PSK)):** ネットワークに接続するためのキー名と値を設定する場合に選択します。

Prevent brute-force attacks (ブルートフォース攻撃を防ぐ)

Blocking (ブロック): オンにすると、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。ページレベルと装置レベルの両方で許容される失敗の数を設定できます。

IP address filter (IPアドレスフィルター)

AXIS D2110-VE Security Radar

webインターフェース

Use filter (フィルターを使用する): 装置へのアクセスを許可するIPアドレスを絞り込む場合に選択します。

Policy (ポリシー): 特定のIPアドレスに対してアクセスを **[Allow (許可)]** するか **[Deny (拒否)]** するかを選択します。

Addresses (アドレス): 装置へのアクセスを許可するIP番号と拒否するIP番号を入力します。CIDR形式を使用できます。

カスタム署名されたファームウェア証明書

Axisのテストファームウェアまたは他のカスタムファームウェアを装置にインストールするには、カスタム署名付きファームウェア証明書が必要です。証明書は、ファームウェアが装置の所有者とAxisの両方によって承認されたと証明します。ファームウェアは、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、カスタム署名付きファームウェア証明書は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。ファーム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



Add account (アカウントの追加): 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。パスワードの長さは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):** すべての設定へのフルアクセスが許可されています。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 (システム)]** 設定。
 - アプリを追加しています。
- **ビューア:** 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。

Anonymous access (匿名アクセス)

AXIS D2110-VE Security Radar

webインターフェース

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。

Allow anonymous PTZ operating (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アカウントの追加): クリックして、新しいSSHアカウントを追加します。

- **Restrict root access (rootアクセスを制限する):** オンにすると、rootアクセスを必要とする機能が制限されます。
- **Enable SSH (SSHの有効化):** SSHサービスを使用するには、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。パスワードの長さは1~64文字である必要があります。パスワードには、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。

OpenID 設定

重要

正しい値を入力すると、装置に再度ログインできます。

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): 管理者ロールの値を入力します。

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): オペレーターロールの値を入力します。

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): 閲覧者ロールの値を入力します。

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。

AXIS D2110-VE Security Radar

webインターフェース

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。



Add a rule (ルールの追加): ルールを作成します。

Name (名前): 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と、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。



Add a condition (条件の編集): 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。

Recipients (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。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。

AXIS D2110-VE Security Radar

webインターフェース



Add a recipient (送信先の追加): クリックすると、送信先を追加できます。

Name (名前): 送信先の名前を入力します。

Type (タイプ): リストから選択します:

- **FTP**
 - **Host (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。
 - **Port (ポート):** FTPサーバーに使用するポート番号を入力します。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。
 - **Password (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があります。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。
 - **Password (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。
 - **Password (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。
- **Network storage (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。

 - **Host (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。
 - **Share (共有):** ホスト上の共有の名前を入力します。
 - **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。
 - **Password (パスワード):** ログインのパスワードを入力します。
- **SFTP**
 - **Host (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。
 - **Port (ポート):** SFTPサーバーに使用するポート番号を入力します。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。
 - **Password (パスワード):** ログインのパスワードを入力します。

AXIS D2110-VE Security Radar

webインターフェース

- **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装置は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ので、SHA-256を使用することをお勧めします。Axis装置で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装置は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ので、SHA-256を使用することをお勧めします。Axis装置で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があります。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。

- **From SIP account (送信元のSIPアカウント)**: リストから選択します。
- **To SIP address (送信先のSIPアドレス)**: SIPアドレスを入力します。
- **Test (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。
- **Email (電子メール)**
 - **Send email to (電子メールの送信先)**: 電子メールの送信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。
 - **Send email from (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。
 - **Password (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。
 - **Port (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。デフォルト値は587です。
 - **Encryption (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は、大量の添付ファイルの受信や表示を防止したり、スケジュールに従って送信された電子メールなどの受信を防止したりするセキュリティフィルターを備えています。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、メールアドレスのロックや、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**

- **Host (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。
- **Port (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。

AXIS D2110-VE Security Radar

webインターフェース

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。



Add schedule (スケジュールの追加): 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。これは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装置を接続するために、さまざまな業界で使用されています。Axis装置のファーム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。

装置をMQTTクライアントとして設定します。MQTT通信は、クライアントとブローカーという2つのエンティティに基づいています。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*ポータル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わ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 client (MQTTクライアント)

AXIS D2110-VE Security Radar

webインターフェース

Connect (接続): 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。

Broker (ブローカー)

Host (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。

Port (ポート): ポート番号を入力します。

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

Password (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。

Connect message (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トメントメッセージ

AXIS D2110-VE Security Radar

webインターフェース

最終意思テストメント(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ト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 publication (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。

+ **条件の追加:** 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の追加:** 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。

AXIS D2110-VE Security Radar

webインターフェース

MQTT overlays (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の追加): 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

Network storage (ネットワークストレージ)

Ignore (使用しない): オンに設定すると、ネットワークストレージを使用しません。

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。

- **Address (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 (ドメイン\ユーザー名) を入力します。
- **Password (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SMB 3.02、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知された場合でも、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 (アンバインド): 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。書き込み禁止の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。

Tools (ツール)

AXIS D2110-VE Security Radar

webインターフェース

・ **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 (フォーマット):** 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): オンに設定にすると、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、データストレージに関する規制に準拠したりします。SDカード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。

Tools (ツール)

- ・ **Check (チェック):** SDカードのエラーをチェックします。これは、ext4ファイルシステムの場合にのみ機能します。
- ・ **Repair (修復):** ext4ファイルシステムのエラーを修復します。VFAT形式のSDカードを修復するには、SDカードを取り出して、コンピューターに挿入し、ディスクの修復を実行します。
- ・ **Format (フォーマット):** ファイルシステムを変更したり、すべてのデータをすばやく消去したりする必要があるときなどは、SDカードをフォーマットします。使用可能なファイルシステムオプションは、vFATとext4の2つです。カードの排出や突然の停電によるデータ損失に対する回復力があるため、ext4でのフォーマットをお勧めします。ただし、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。**Encrypt (暗号化)** 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。**[Encrypt (暗号化)]** の使用後、SDカードに保存されているデータは暗号化により保護されます。
- ・ **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。**Decrypt (復号化)** 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。**[Decrypt (復号化)]** の使用後、SDカードに保存されるデータは暗号化により保護されません。
- ・ **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。

AXIS D2110-VE Security Radar

webインターフェース



Add stream profile (ストリームプロファイルの追加): 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。

Name (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。


Resolution (解像度): この設定の説明については、を参照してください。

Frame rate (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。


Compression (圧縮): この設定の説明については、を参照してください。


Zipstream (Zipstream テクノロジー)  : この設定の説明については、を参照してください。

Optimize for storage (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。

Dynamic FPS (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。


Dynamic GOP (ダイナミック group of pictures)  : この設定の説明については、を参照してください。

Mirror (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 length (GOP 長)  : この設定の説明については、を参照してください。

Bitrate control (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。

Include overlays (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、32ページオーバーレイを参照してください。

Include audio (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、ネットワークビデオテクノロジーを利用するエンドユーザー、インテグレーター、コンサルタント、メーカーが、その技術を容易に活用できるようにするためのグローバルなインターフェース規格です。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でAxis開発者コミュニティを参照してください。

AXIS D2110-VE Security Radar

webインターフェース



Add accounts (アカウントの追加): 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。パスワードの長さは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 (役割):

- **Administrator (管理者):** すべての設定へのフルアクセスが許可されています。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 (システム)] 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の追加: 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。

Audio source (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。

AXIS D2110-VE Security Radar


webインターフェース

Audio encoder (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/名前となります。

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

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 ports (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またはwebインターフェースから有効化できます。

Port (ポート)

Name (名前): テキストを編集して、ポートの名前を変更します。

Direction (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。

Normal state (標準の状態): 開回路には  を、閉回路には  をクリックします。


Current state (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。装置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、装置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。

AXIS D2110-VE Security Radar

webインターフェース

状態監視  : オンにすると、誰かがデジタルI/O装置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

Audio pairing (音声ペアリング) により、互換性のあるAxisネットワークスピーカーをメイン装置の一部であるかのように使用できます。ペアリングされると、ネットワークスピーカーは音声出力装置として機能し、音声クリップを再生したり、音声を送信したりできます。

重要

この機能をビデオ管理ソフトウェア (VMS) と共に使用するには、まず装置をスピーカーとペアリングしてから、その装置を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。

音声ペアリング

Address (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。

Password (パスワード): ユーザーのパスワードを入力します。

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。

Clear fields (フィールドのクリア): 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): クリックして、スピーカーへの接続を確立します。

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。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。

PTZペアリング

Address (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。

Password (パスワード): PTZカメラのパスワードを入力します。

Clear fields (フィールドのクリア): 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): 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 (レーダー)] > [Autotracking (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

AXIS D2110-VE Security Radar

webインターフェース

Reports (レポート)

- **View the device server report (装置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 (装置サーバーレポートをダウンロード):** 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ファイルを生成します。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。

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、[Download (ダウンロード)] をクリックします。

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。



Server(サーバー): クリックして新規サーバーを追加します。

Host (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 (フォーマット): 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とポートを選択します。

- 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)

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。

AXIS D2110-VE Security Radar

webインターフェース

プレーン設定

[Plain Config] (プレーン設定) 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。

保守

Restart (再起動): 装置を再起動します。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

リストア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)
- 静的なIPアドレス
- Default router (デフォルトルーター)
- Subnet mask (サブネットマスク)
- 802.1X settings (802.1Xの設定)
- O3C settings (O3Cの設定)

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

検証済みのファーム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の装置ファーム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「署名済みファームウェア、セキュアブート、およびプライベートキーのセキュリティ」を参照してください。

Firmware upgrade (ファームウェアのアップグレード): 新しいファームウェアバージョンにアップグレードします。新しいファームウェアには、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):** 新しいファームウェア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以前のファームウェア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、装置は以前のファームウェアバージョンに戻されます。

Firmware rollback (ファームウェアのロールバック): 以前にインストールされたファームウェアバージョンに戻します。

AXIS D2110-VE Security Radar

インストールの検証

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 17 ページ **レーダーキャリブレーションを行う** を行います。

次の場合は毎回、検証を行うことをお勧めします。

- ・ 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

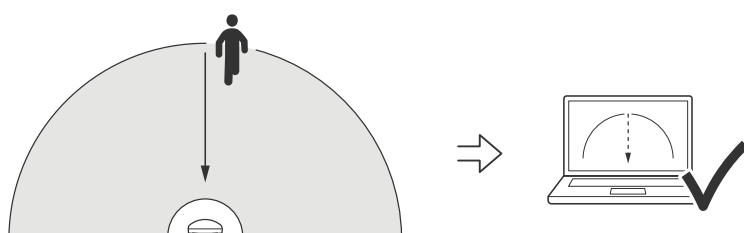
1. 検知ゾーンに人間の活動がないことを確認してください。
2. 検知ゾーン内に静止した物が検知されないことを確認するために、数分間待つてください。
3. 不要な検知がない場合は、手順 4 をスキップできます。
4. 不要な検知がある場合は、特定の種類の動きや物体を除外する方法、カバー範囲を変更する方法、または検知感度を調整する方法について、20 ページ **誤報を最小限に抑える** を参照してください。

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、22 ページ **ビデオを録画して見る** 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。

AXIS D2110-VE Security Radar

インストールの検証

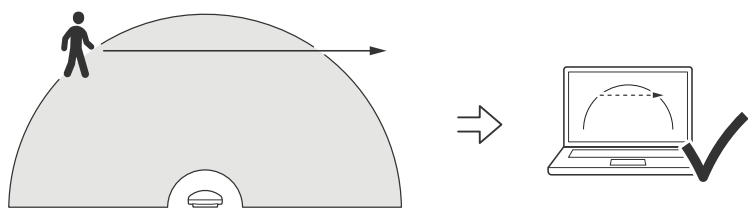


レーダーに横から近づくと、記号と移動方向が正しく表示されることを確認する

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、22ページビデオを録画して見る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。
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。

AXIS D2110-VE Security Radar

インストールの検証



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. エリアに何もい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		

AXIS D2110-VE Security Radar

インストールの検証

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、22ページビデオを録画して見る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。

AXIS D2110-VE Security Radar

詳細情報

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

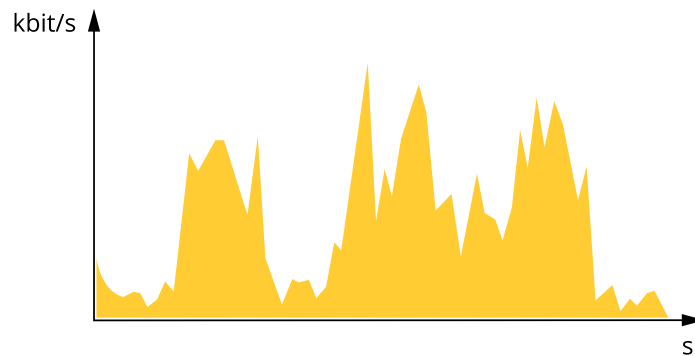
ビットレート制御で、ビデオストリームの帯域幅の使用量を管理することができます。

Variable bitrate (VBR) (可変ビットレート)

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。

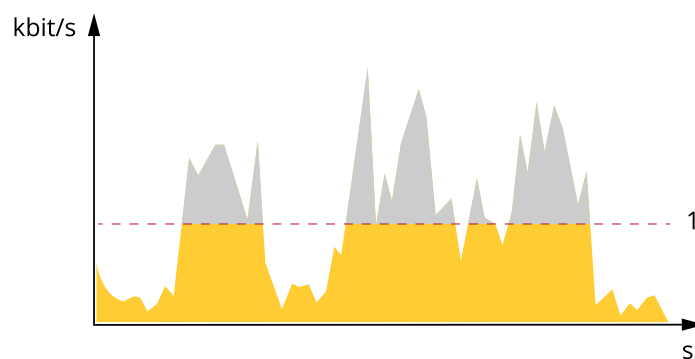
AXIS D2110-VE Security Radar

詳細情報



Maximum bitrate (MBR) (最大ビットレート)

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

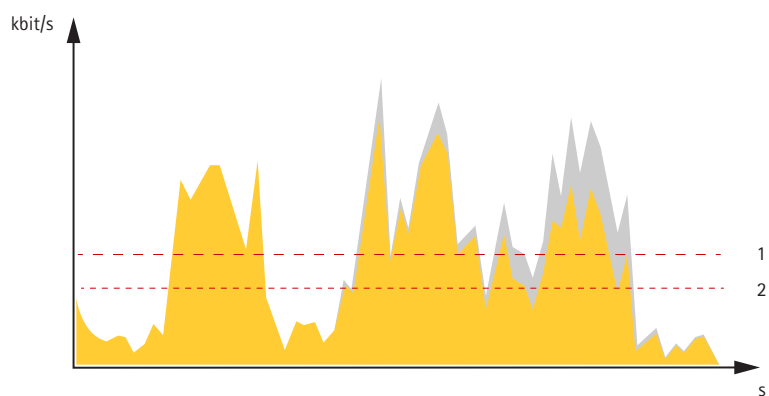
Average bitrate (ABR) (平均ビットレート)

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。

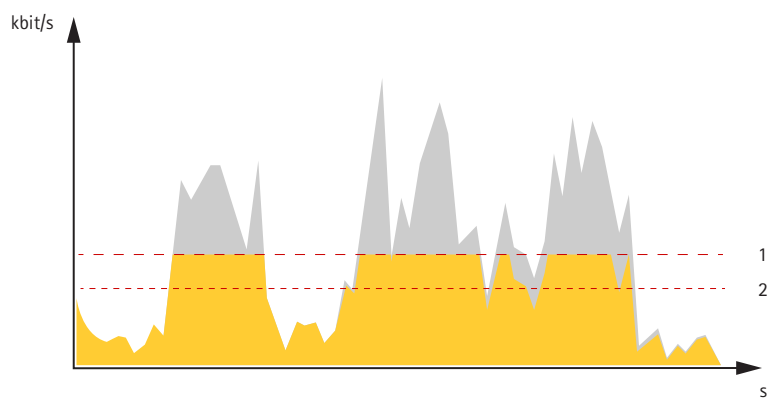
AXIS D2110-VE Security Radar

詳細情報



- 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。



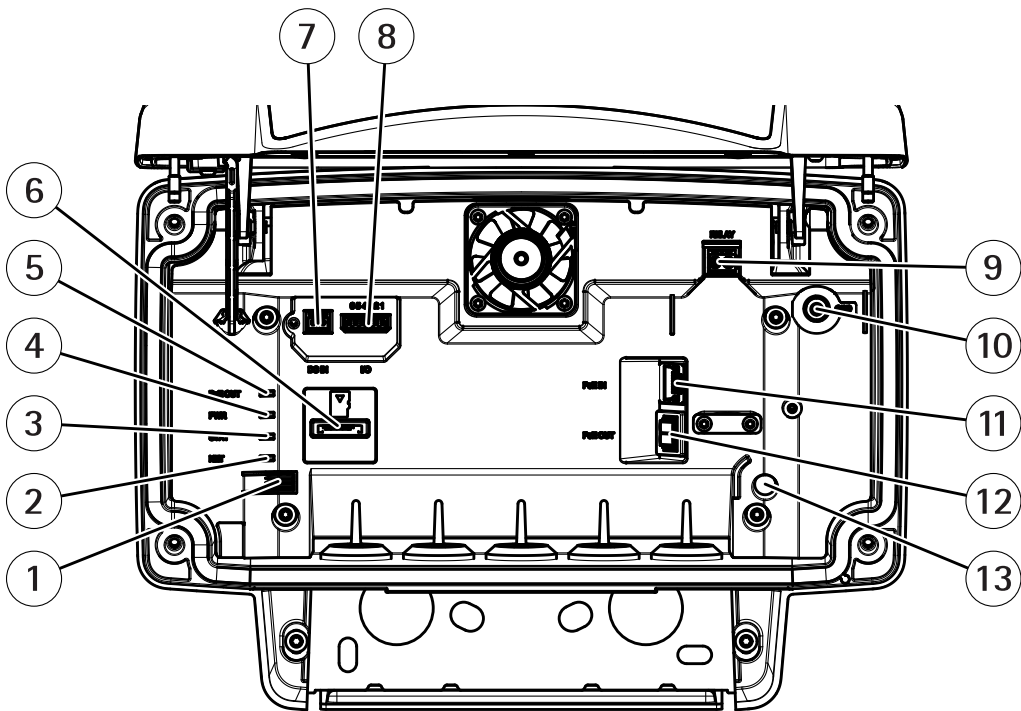
- 1 目標ビットレート
- 2 実際の平均ビットレート

AXIS D2110-VE Security Radar

仕様

仕様

製品の概要



- 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、66ページ、仕様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	正常動作の場合、緑色に点灯します。

AXIS D2110-VE Security Radar

仕様

ネットワークLED	説明
緑	100Mbit/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。
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、66ページ製品の概要を参照してください。

コントロールボタンは、以下の用途で使します。

- 製品を工場出荷時の設定にリセットする。71ページ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)。

コネクター

ネットワークコネクター

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

▲注意

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

ネットワークコネクター (PoE出力)

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

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。

AXIS D2110-VE Security Radar

仕様

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。

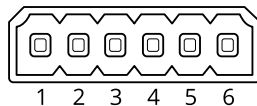
I/Oコネクタ

I/Oコネクタ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コネクタは、0 V DC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

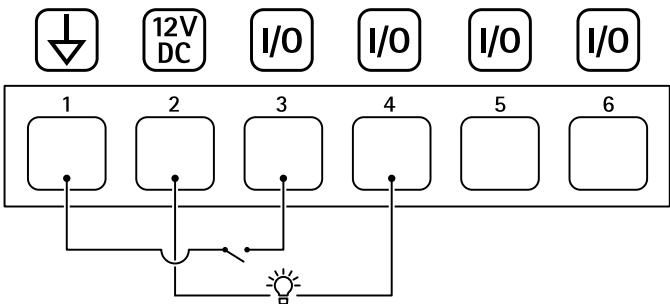


機能	ピン	備考	仕様
DCアース	1		0 V DC
DC出力	2	補助装置の電源供給に使用できます。 注: このピンは、電源出力としてのみ使用できます。	12 V DC 最大負荷 = 50 mA
設定可能 (入力または出力)	3-6	デジタル入力 - 動作させるにはピン1に接続し、動作させない場合はフロート状態 (未接続) のままにします。	0~30 V DC (最大)
		デジタル出力 - アクティブ時はピン1 (DCグラウンド) に内部で接続し、非アクティブ時はフロート状態 (未接続) になります。リレーなどの誘導負荷とともに使用する場合は、過渡電圧から保護するために、負荷と並列にダイ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

例:

AXIS D2110-VE Security Radar

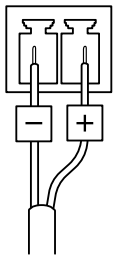
仕様



- 1 DCグランド
- 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

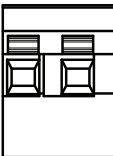
DC電源入力用2ピンターミナルブロック。定格出力が100 W以下または5 A以下の安全特別低電圧 (SELV) に準拠した有限電源 (LPS) を使用してください。



▲注意

装置の損傷の危険があります。PoEとDCの両方を使用して装置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 (ノーマルオープン)
定格	24 V DC/5 A
他の回路からの定格絶縁	2.5 kV

AXIS D2110-VE Security Radar

清掃の推奨事項

清掃の推奨事項

装置に油しみがあったり、汚れがひどい場合は、マイルドで無溶媒の中性石鹼または洗剤を使用して清掃することができます。

注意

ガソリン、ベンジン、アセトンなどの強力な洗剤は絶対に使用しないでください。

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. マイルドな洗剤とぬるま湯に浸した柔らかい布で装置を清掃します。
3. 乾いた布で慎重に拭きます。

注

水滴が乾いて跡が残ることがありますので、直射日光が当たる、または高温になる場所では清掃しないでください。

AXIS D2110-VE Security Radar

トラブルシューティング

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、以下の手順を実行します。

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。66ページ製品の概要を参照してください。
3. ステータスLEDがオレンジ色に点滅するまで、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離します。プロセスが完了すると、ステータスLEDが緑色に変わります。これで本製品は工場出荷時の設定にリセットされました。ネットワーク上に利用可能なDHCPサーバーがない場合、デフォルトのIPアドレスは192.168.0.90になります。
5. インストールおよび管理ソフトウェアツールを使用して、IPアドレスの割り当て、パスワードの設定、装置へのアクセスを行います。

axis.com/supportのサポートページに、インストールおよび管理ソフトウェアツールが用意されています。

装置のweb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。

現在のファームウェアバージョンの確認

ファームウェアは、ネットワーク装置の機能を決定するソフトウェアです。問題のトラブルシューティングを行う際は、まず現在のファームウェアバージョンを確認することをお勧めします。最新のファームウェアバージョンには、特定の問題の修正が含まれていることがあります。

現在のファームウェアを確認するには、以下の手順に従います。

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)]** でファームウェアバージョンを確認してください。

ファームウェアのアップグレード

重要

- ・ 事前設定済みの設定とカスタム設定は、ファームウェアのアップグレード時に保存されます (その機能が新しいファームウェアで利用できる場合)。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、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最新のファームウェア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。ファームウェアを更新する前に、ファームウェアととも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。最新ファームウェアおよびリリースノートについては、axis.com/support/device-softwareを参照してください。

AXIS D2110-VE Security Radar

トラブルシューティング

1. ファームウェアファイルをコンピューターにダウンロードします。ファームウェアファイルは axis.com/support/device-software から無料で入手できます。
2. 装置に管理者としてログインします。
3. [Maintenance (メンテナンス) > Firmware upgrade (ファームウェアのアップグレード)] 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。

ファームウェアのアップグレードで問題が発生する

ファームウェアのアップグレード失敗	ファームウェアのアップグレードに失敗した場合、装置は以前のファームウェアを再度読み込みます。最も一般的な理由は、間違ったファームウェアファイルがアップロードされた場合です。装置に対応したファームウェアファイル名であることを確認し、再試行してください。
ファームウェアのアップグレード後に問題が発生する	ファームウェアの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

装置が別のサブネット上にある	装置用のIPアドレスと、装置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アドレスが別の装置で使用されている	Axis装置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コマンドと装置のIPアドレスを入力します)。 <ul style="list-style-type: none"> もし、「Reply from <IPアドレス>: 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装置でその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、装置を再度インストールしてください。 もし、「Request timed out」が表示された場合は、Axis装置でその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、装置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装置と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装置は静的IPアドレスを使用します。つまり、デフォルトの静的IPアドレスが別の装置でも使用されていると、装置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が有効なときは、正しいプロトコル(HTTPまたはHTTPS)を使用してログインしてください。ブラウザーのアドレスフィールドに、手動で「http」または「https」と入力する必要がある場合があります。 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。71ページ工場出荷時の設定にリセットするを参照してください。
----------	--

AXIS D2110-VE Security Radar

トラブルシューティング

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を使用して装置のネットワーク上の場所を特定してください。装置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)を使用して装置を識別します。

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を参照してください。

IEEE 802.1X使用時の証明書エラー

認証を正しく行うには、Axis装置の日付と時刻を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 Companion: 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: 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。
- 手順とダウンロードについては、axis.com/vmsを参照してください。

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、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、ポート443などのオープンポート経由でMQTTをネゴシエーションできます。ALPNがサポートされているかどうか、どのALPNプロトコルとポートを使用するかについては、サーバー/ブローカー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。

