AXIS D6310 Air Quality Sensor

ユーザーマニュアル

目次

インストール....4
使用に当たって....5
....5
ネットワーク上のデバイスを検索する....5
ブラウザーサポート....5
装置のwebインターフェースを開く....5
管理者アカウントを作成します。....5
安全なパスワード....6
デバイスのソフトウェアが改ざんされていないことを確認する....6
デバイスを配置する....6
センサーの検知範囲....6
デバイスを構成する....7
空気質モニターの設定....7
空気質センサーのダッシュボードの設定....7
空気質センサーを設定する....8
センサーデータ統計情報のダウンロード....9
装置の初起動時のキャリブレーション....9
MQTTデータの公開....9
MQTTブローカーを設定する:....9
変数メタデータを使用してMQTTデータをパブリッシュする....10
イベントデータを使用してMQTTデータをパブリッシュする....11
プロファイルの設定....12
カスタムサイレン音声ファイルでプロファイルを設定する....12
プロファイルのインポートまたはエクスポート....12
ダイレクトSIP (P2P) を設定する....13
サーバーを介してSIPを設定する (PBX)....14
双方向コミュニケーションを作成する....14
イベントのルールを設定する....15
アクションをトリガーする....15
センサーが電子タバコの使用を検知するとビデオを録画する....16
CO2が上限閾値を超えたら音声クリップを再生する....16
PIRセンサー経由でライトとサイレンを作動させる....17
アラームがトリガーされたときにプロファイルを開始します....17
SIPを介したプロファイルの開始....18
SIP内線番号による複数のプロファイルの制御....18
優先度が異なる2つのプロファイルを実行する....19
カメラが動きを検知すると、HTTP postを使用してライトとサイレンのプロファイルを有効にする....20
カメラが動きを検知すると、仮想入力を使用してライトとサイレンのプロファイルを有効にする....21
カメラが動きを検知すると、MQTT経由でライトとサイレンのプロファイルを有効にする....22
スピーカーテストが失敗した場合に電子メールを送信する....24
アラームトリガー時にカスタムクリップを再生する....25
DTMFで音声を停止する....26
着信SIP呼び出しの音声の設定....26
webインターフェース....28
仕様....29
製品概要....29
....29
ステータスLED....30
ボタン....30
コントロールボタン....30

マイクスイッチ....30
コネクター....30
ネットワークコネクター....30
I/Oコネクター....30
RS485/RS422コネクター....31
ライトパターン名....32
サイレンのパターン名....32
装置を清掃する....34
トラブルシューティング....35
工場出荷時の設定にリセットします。....35
技術的な問題、ヒント、解決策....35
パフォーマンスに関する一般的な検討事項....37
サポートに問い合わせる....37
サイバーセキュリティ....38
脆弱性の管理....38
セキュリティ通知....38
安全な製品ライフサイクル管理....38

インストール

重要

- 大きな通気口や汚染源のある場所からは少なくとも1.5メートル (4.9フィート) 離してください。これには、通気口、ドア、窓、調理場などが含まれます。
- 空気が自由に流れる位置に装置を設置してください。
- ベイプや喫煙を効果的に検出するには、床から2.4～2.7メートル (7.9～8.9フィート) の高さの天井に装置を設置してください。
- 空気質と環境を効果的に監視するには、床から0.9～1.8メートル (3.0～5.9フィート) の高さに装置を設置してください。

取り付け方法の詳細については、インストールガイドを参照してください。

使用に当たって

⚠ 警告

光の点滅やちらつきは、光過敏性てんかんを持つ人の発作を引き起こすことがあります。

ネットワーク上のデバイスを検索する

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

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

ブラウザーサポート

以下のブラウザーでデバイスを使用できます。

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

✓:推奨

*:制限付きでサポート

装置のwebインターフェースを開く

1. ブラウザーを開き、Axis装置のIPアドレスまたはホスト名を入力します。
   本製品のIPアドレスが不明な場合は、AXIS IPUtilityまたはAXIS DeviceManagerを使用して、ネットワーク上のデバイスを検索してください。
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します。, on page 5*を参照してください。

AXIS OS搭載デバイスのWebインターフェースにおけるすべての機能および設定の説明については、*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します。

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. アカウントを入力します。
2. パスワードを入力します。*安全なパスワード, on page 6*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します。, on page 35*を参照してください。

安全なパスワード

重要

ネットワーク経由でパスワードやその他の機密性の高い設定を行う際は、HTTPS (デフォルトで有効) を使用してください。HTTPSは、安全で暗号化されたネットワーク接続を可能にし、パスワードなどのセンシティブなデータを保護します。

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

データを保護するために、次のことが強く推奨されています。

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

デバイスのソフトウェアが改ざんされていないことを確認する

装置に元のAXIS OSが搭載されていることを確認するか、またはセキュリティ攻撃が行われた後に装置を完全に制御するには、以下の手順に従います。

1. 工場出荷時の設定にリセットします。*工場出荷時の設定にリセットします。, on page 35*を参照してください。
   リセットを行うと、セキュアブートによって装置の状態が保証されます。
2. デバイスを設定し、インストールします。

デバイスを配置する

デバイスの配置は、利用状況によって異なります。以下の点を考慮しつつ、対象範囲のできるだけ近くにデバイスを設置してください。

パラメーター	配置	高さ	避けるべきこと
電子タバコの使用および喫煙	天井	2.4～2.7 m (7.9～8.9 ft)	角部
PM、VOC、NO_x、CO_2	壁	0.9～1.8 m (3～6 ft)	角部、熱源
湿度	天井または壁	すべて	窓、換気口、熱源、角部
温度	天井または壁	すべて	熱源、冷却源、角部

センサーの検知範囲

検知範囲は、センサーを中心に筒状に延びています。空気質パラメータの検知半径は2 m (6.5 ft) ですが、空気の流れや間取りなどの環境要因によって全体の検知範囲は変わります。

喫煙や電子タバコの使用を検知するセンサーの検知範囲は、12.6 m^2 (135 ft^2) です。

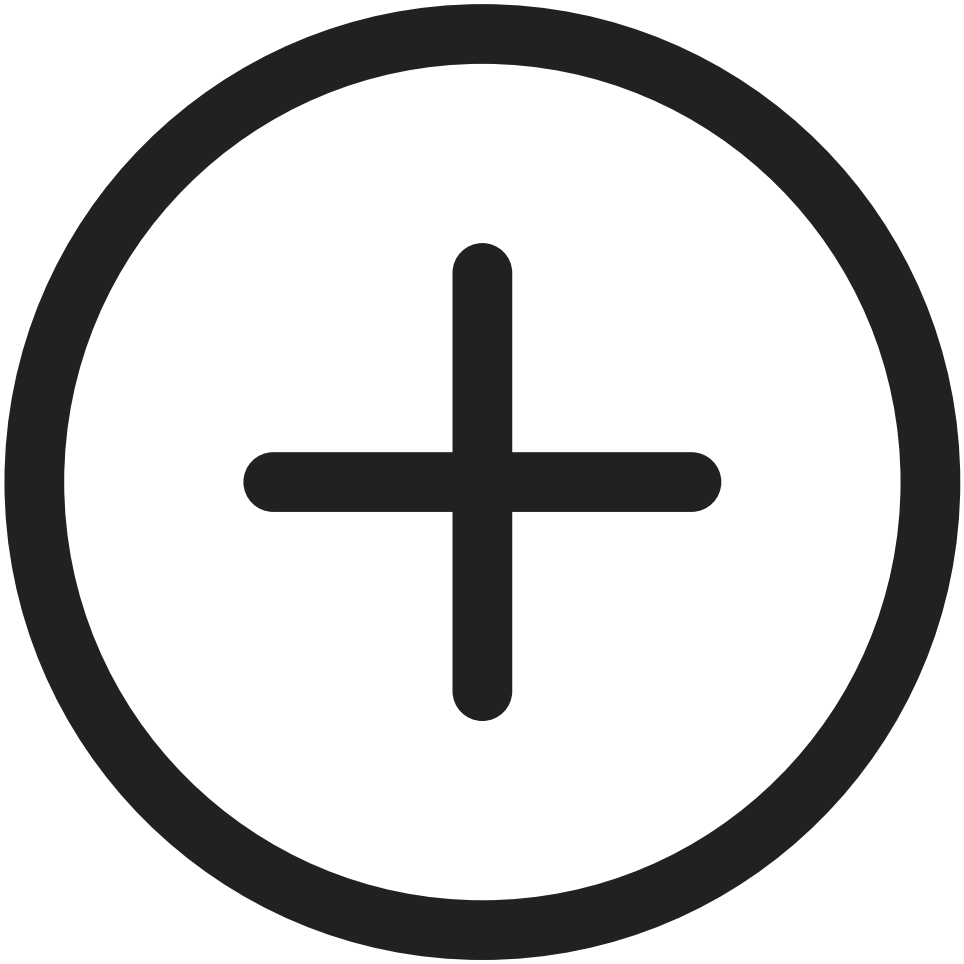
デバイスを構成する

空気質モニターの設定

空気質センサーのダッシュボードの設定

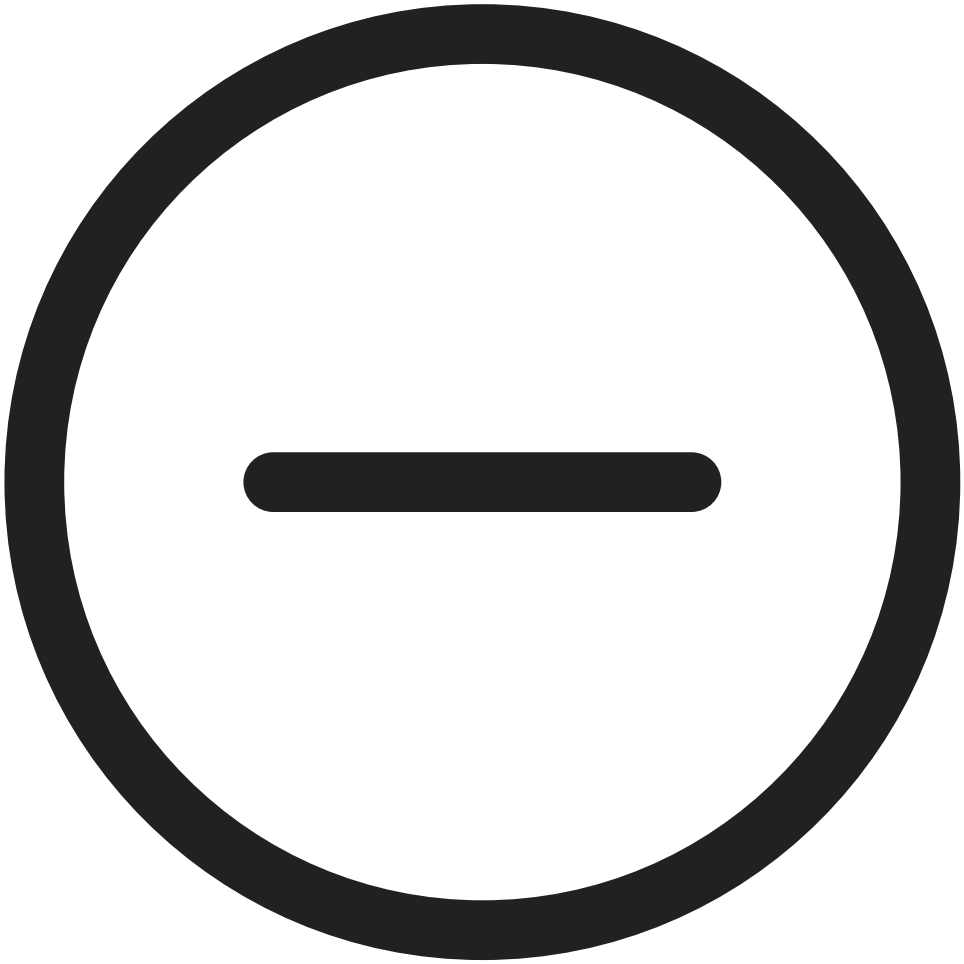
デバイスのwebインターフェースで、[Air quality monitor (空気質モニター)] > [Dashboard (ダッシュボード)] の順に移動します。

- ダッシュボードの名前を編集するには、ダッシュボード名の横の をクリックします。
- ダッシュボードにデータを表示するには、 [Edit (編集)] >



をクリックします。

- ダッシュボードでデータを非表示するには、 [Edit (編集)] >



をクリックします。

注

ダッシュボードには、一度に12のパラメーターのみが表示されます。ダッシュボードがフルの場合、新しいパラメーターを表示するには、アクティブなパラメーターを非表示にする必要があります。

空気質センサーを設定する

デバイスのwebインターフェースで、[Air quality sensor (空気質センサー)] > [Settings (設定)] に移動します。

- 温度、湿度、CO2、NOx、PM1.0、PM2.5、PM4.0、PM10.0、VOC、AQI、ヒューミデックス、暑さ指数の閾値を設定します。*設定*を参照してください。
- 電子タバコの使用の検知感度を設定します。*設定*を参照してください。
- ストレージの保持期間を設定します。*ストレージ設定*を参照してください。
- 変数メタデータ周期を設定します。*変数メタデータ*を参照してください。
- 検証期間を設定します。*検証期間*を参照してください。
- Modbusを有効にします。*Modbus*を参照してください。

センサーデータ統計情報のダウンロード

最大365日分のセンサー統計情報をCSVファイルにエクスポートし、Microsoft® Excelなどのアプリケーションで使用できます。

1. デバイスのwebインターフェースで、**[Air quality monitor (空気質モニター)]** > **[Statistics (統計)]** > **[Sensor Data Statistics (センサーデータ統計)]** に移動します。
2. 日付範囲を選択する:
   - **Custom range (カスタム範囲)**:**[From (開始)]** と **[To (終了)]** のリストから、開始日と終了日を選択します (最大365日)。
   - **Predefined range (あらかじめ定義された範囲)**:**[Predefined range (あらかじめ定義された範囲)]** のリストから期間を選択します。

   注
   カスタム範囲とあらかじめ定義された範囲の両方が選択されている場合、カスタム範囲が優先されます。

   注
   最大ダウンロード範囲は、*[Storage settings (ストレージ設定)]* で設定された保持期間に制限されます。
3. **[Source (ソース)]** リストから任意のソースを選択します。すべてのソースのデータをエクスポートするには、**[Download all data (すべてのデータをダウンロード)]** をクリックします。
4. **[Download data (データをダウンロード)]** をクリックすると、選択した統計情報がエクスポートされます。

装置の初起動時のキャリブレーション

注

- 完全なCO2精度が得られるまでには、装置の初起動から2日かかります。
- 装置の初起動時には、AQI (空気質指数) が正しく機能するまでに12時間かかります。十分なデータが得られるまで、AQIには**Calculating (計算中)** と表示されます。デバイスが再起動するたびに、キャリブレーション時間が必要です。
- 完全なVOC精度は、デバイスを1時間作動させた後に得られます。デバイスが再起動するたびに、キャリブレーション時間が必要です。
- 完全なNOx精度は、デバイスを6時間作動させた後に得られます。デバイスが再起動するたびに、キャリブレーション時間が必要です。

MQTTデータの公開

MQTTブローカーを設定する:

1. **[System (システム)]** > **MQTT** を移動します。
2. ブローカーの情報を入力します。
   - **[ホスト]**:IPアドレス
   - **Username (ユーザー名)** と **Password (パスワード)**
   - **装置トピックの接頭辞**:ここにMQTTデータが公開されます。デフォルトトピックは`axis/MAC-address`になります。
3. MQTTクライアントをオンにします。テキストが **[Status: Connected (ステータス: 接続済み)]** に変わるはずです。
4. **[Save (保存)]** をクリックします。

変数メタデータまたはイベントデータを使用してMQTTでデータをパブリッシュできます。

変数メタデータを使用してMQTTデータをパブリッシュする

変数のメタデータを有効にする:

1. [Air quality monitor (空気質モニター)] > [Settings (設定)] > [Variable metadata (変数メタデータ)] に移動します。
2. [Variable metadata (変数のメタデータ)] を有効にします。
3. データ送信周期を設定します。

MQTTデータを公開する:

1. [MQTT publication (MQTT公開)] タブで、[Add condition (条件の追加)] をクリックします。
2. [Add condition (条件の追加)] ダイアログに以下を入力します。
   - Condition (条件):空気質クラウド監視有効
   - MQTT topic (MQTTトピック): `axis/{serial}/event/tns:axis/AirQualityMonitor/VariableMetadata`
   - Payload topic (ペイロードトピック): `axis:AirQualityMonitor/VariableMetadata`
3. [追加] をクリックします。

注

[Air quality cloud monitoring active (空気質クラウド監視有効)] が表示されない場合は、[Air quality monitor (空気質モニター)] > [Setting (設定)] で変数メタデータを有効にする必要があります。

この条件は、すべてのセンサーパラメーターを選択した変数メタデータ更新頻度で以下のような形式で公開します。


```
( "topic": "axis:AirQualityMonitor/Metadata", "timestamp": 1772553621219,
"message": { "source": { "sensor_name": "D6310" }, "key": {}, "data": { "NOx":
"4.000000", "Humidity": "21.290001", "Temperature": "26.430000", "PM10.0":
"5.200000", "AQI": "28", "PM4.0": "5.000000", "PM1.0": "3.800000", "CO2":
"580", "VOC": "180.000000", "PM2.5": "4.500000", "Humidex": "25", "Heat
index": "26",
```


生成されるメタデータフィールドには以下が含まれます。

現場	説明
`topic`	条件を生成したペイロードトピック。
`timestamp`	データが生成された時点のタイムスタンプ。
`serial`	デバイスのMACアドレス。シリアル番号は、[MQTT publication (MQTT公開)] タブで、[Include serial number (シリアル番号を含める)] を有効にしている場合のみ表示されます。
`message`	条件に関する情報が含まれたJSONオブジェクト。
`message.source`	N/A
`message.source.sensor_name`	条件を生成したデバイスの名前。
`message.key`	N/A
`message.data`	データ情報を含むJSONオブジェクト。

message.data.NOx	一酸化窒素および二酸化窒素のリアルタイム濃度。
message.data.Humidity	リアルタイムの湿度情報。
message.data.Temperature	リアルタイムの温度 (°Cまたは°F)。
message.data.PM1.0	リアルタイムPM1.0濃度。
message.data.PM2.5	リアルタイムPM2.5濃度。
message.data.PM4.0	リアルタイムPM4.0濃度。
message.data.PM10.0	リアルタイムPM10.0濃度。
message.data.AQI	空気質センサーのデータに基づくリアルタイム空気質指数。
message.data.CO2	リアルタイム二酸化炭素濃度。
message.data.VOC	リアルタイム揮発性有機化合物指数。
message.data.Humidex	湿度と気温のデータに基づくリアルタイムのヒューミデックス。
message.data.Heat_index	湿度と気温のデータに基づく暑さ指数。

イベントデータを使用してMQTTデータをパブリッシュする

パラメーターの閾値に関するイベントデータを送信する:

1. **[System (システム)]** > **[MQTT]** > **[MQTT publication (MQTTパブリケーション)]** に移動します。
2. **[+ Add condition (条件の追加)** をクリックします。
3. **[Add condition (条件の追加)]** ダイアログに以下を入力します。
   - **Condition (条件)**:[Air quality monitor (空気質モニター)] > [Air quality outside of acceptable range (空気質許容範囲外)]
   - **MQTT topic (MQTTトピック)**: `axis/{serial}/event/tns:axis/AirQualityMonitor/Alarm`
   - **Payload topic (ペイロードトピック)**: `axis:AirQualityMonitor/Alarm`
4. [**追加**] をクリックします。

この条件は、選択した間隔で以下のような形式でイベントデータをパブリッシュします。

```
( "topic": "axis:AirQualityMonitor/Alarm", "timestamp": 1772553621219,
"message": { "source": { "source": "Temperature" "sensor_name": "D6210" },
"key": {}, "data": { "active": "1" } } }
```

「active」が0の場合、パラメーターは許容範囲内です。「active」が1の場合、1つ以上のパラメーターが許容範囲外です。

喫煙および電子タバコの使用に関するイベントデータを送信する:

1. **[System (システム)]** > **[MQTT]** > **[MQTT publication (MQTTパブリケーション)]** に移動します。
2. **[+ Add condition (条件の追加)** をクリックします。
3. **[Add condition (条件の追加)]** ダイアログに以下を入力します。

- Condition (条件):[Air quality monitor (空気質モニター)] > [Vaping or smoking detected (電子タバコまたはタバコの喫煙を検知)]。
- MQTT topic (MQTTトピック): `axis/{serial}/event/tns:axis/AirQualityMonitor/Vaping`
- Payload topic (ペイロードトピック: `axis:AirQualityMonitor/Vaping`

4. [追加] をクリックします。

この条件は、選択した間隔で以下のような形式でイベントデータをパブリッシュします。

```
( "topic": "axis:AirQualityMonitor/Vaping", "timestamp": 1772553621219,
"message": { "source": { "sensor_name": "D6210" }, "key": {}, "data": {
"active": "1" } } }
```

「active」が0の場合、センサーは喫煙や電子タバコの使用を検知しません。「active」が1の場合、センサーは喫煙または電子タバコの使用を検知します。

プロファイルの設定

プロファイルとは、設定された構成の集合を意味します。優先順位やパターンの異なる最大30のプロファイルを設定できます。

新しいプロファイルを設定するには、以下の手順に従います。

1. [Profiles (プロファイル)] に移動し、[+ Create (作成)] をクリックします。
2. Name (名前) とDescription (説明) を入力します。
3. プロファイルに必要な [Light (ライト)] と [Siren (サイレン)] の設定を選択します。
4. ライトとサイレンの [Priority (優先度)] を設定し、[Save (保存)] をクリックします。

プロファイルを編集するには、 ⋮ をクリックして [Edit (編集)] を選択します。

カスタムサイレン音声ファイルでプロファイルを設定する

カスタム音声ファイルでプロファイルを設定できます。最大100MBまでの音声ファイルをデバイスに保存できます。デバイスにSDカードスロットが付いている場合、これよりサイズが大きい音声ファイルにはSDカードを使用してください。

音声ファイルのアップロード:

1. [Media (メディア)] に移動し、[+ Add (追加)] をクリックします。
2. コンピューターからファイルを選択します。
3. [Storage location (保存先)]を選択します。
4. [Save (保存)] をクリックします。

音声ファイルをプロファイル内で使用する：

1. [Profiles (プロファイル)] に移動し、プロファイルを作成します。詳細については、*プロファイルの設定, on page 12*] を参照してください。
2. [Siren (サイレン)] を設定する際は、アップロードされた音声ファイルを[Pattern (パターン)] として選択します。

プロファイルのインポートまたはエクスポート

既定のプロファイルを使用する場合は、以下の方法でプロファイルをインポートできます。

1. [Profiles (プロファイル)] に移動し、[+ Import (インポート)] をクリックします。
2. 参照してファイルを見つけるか、インポートするファイルをドラッグアンドドロップします。
3. **[Save (保存)]** をクリックします。

1つ以上のプロファイルをコピーして他の装置に保存するには、以下の手順でプロファイルをエクスポートできます。

1. [profiles(プロファイル)] を選択します。
2. [**エクスポート**] をクリックします。
3. 参照して.jsonファイルを見つけます。

ダイレクトSIP (P2P) を設定する

同じIPネットワーク内の少数のユーザーエージェント間で通信が行われ、PBXサーバーが提供する追加機能が必要ない場合は、ピアツーピアを使用します。

設定オプションの詳細については、*SIP*を参照してください。

1. [System (システム)] > [SIP] > [SIP settings (SIP設定)] に移動し、[Enable SIP (SIPの有効化)] を選択します。
2. デバイスでの着信呼び出しの受信を許可するには、**[Allow incoming calls (着信呼び出しを許可)]** を選択します。
3. [Call handling (呼び出しの処理)] で、呼び出しのタイムアウトと継続時間を設定します。
4. [Ports (ポート)] で、ポート番号を入力します。
   - SIP port (SIPポート) - SIP通信に使用するネットワークポートです。このポートを経由する信号トラフィックは暗号化されません。デフォルトポート番号は5060です。必要に応じて異なるポート番号を入力します。
   - TLS port (TLS ポート) - 暗号化されたSIP通信に使用するネットワークポートです。このポートを経由する信号トラフィックは、Transport Layer Security (TLS) を使用して暗号化されます。デフォルトポート番号は5061です。必要に応じて異なるポート番号を入力します。
   - [RTP start port (RTP開始ポート)] - SIP呼び出しの最初のRTPメディアストリームで使用するポートを入力します。メディア転送のデフォルトの開始ポートは4000です。ファイアウォールによっては、特定のポート番号のRTPトラフィックをブロックする場合があります。ポート番号は1024～65535の間で指定する必要があります。
5. [NAT traversal (NATトラバーサル)] で、NATトラバーサル用に有効にするプロトコルを選択します。

注

NATトラバーサルは、デバイスがNATルーターまたはファイアウォール経由でネットワークに接続している場合に使用します。詳細については、*NATトラバーサル*を参照してください。

6. [Audio (音声)] で望ましい音声品質で、SIP呼び出しの音声コーデックを1つ以上選択します。ドラッグアンドドロップして、優先順位を変更します。
7. [Additional (追加)] で、追加のオプションを選択します。
   - UDP-to-TCP switching (UDPからTCPへの切り替え) - 通話でトランスポートプロトコルをUDP (User Datagram Protocol) からTCP (Transmission Control Protocol) に一時的に切り替えることを許可する場合に選択します。切り替えるのはフラグメンテーションを避けるためであり、要求が200バイト以内または1300バイト以上の最大転送ユニット (MTU) の場合に実行されます。
   - Allow via rewrite (経由のリライトを許可) - ルーターのパブリックIPアドレスではなく、ローカルIPアドレスを送信する場合に選択します。

- Allow contact rewrite (連絡先書き換えの許可) - ルーターのパブリックIPアドレスではなく、ローカルIPアドレスを送信する場合に選択します。
- Register with server every (サーバーへの登録を毎回行う) - 既存のSIPアカウントで、デバイスをSIPサーバーに登録する頻度を設定します。
- DTMF payload type (DTMFの積載タイプ) - DTMFのデフォルトの積載タイプを変更します。

8. [Save (保存)] をクリックします。

サーバーを介してSIPを設定する (PBX)

ユーザーエージェントどうしがIPネットワーク内外で通信する場合は、PBXサーバーを使用します。PBXプロバイダーによっては、設定に機能が追加される場合があります。

設定オプションの詳細については、*SIP*を参照してください。

1. PBXプロバイダーから以下の情報を入手してください。

- ユーザーID
- ドメイン
- パスワード
- 認証ID
- 呼び出し側ID
- レジストラ
- RTP開始ポート

2. 新しいアカウントを追加するには、[System (システム)] > [SIP] > [SIP accounts (SIPアカウント)] に移動し、[+ Account (+ アカウント)] をクリックします。
3. PBXプロバイダーから受け取った詳細情報を入力します。
4. [Registered (登録済み)] を選択します。
5. Transport mode (伝送モード)を選択します。
6. [Save (保存)] をクリックします。
7. ピアツーピアの場合と同じ方法でSIPを設定します。詳細については、*SIP*を参照してください。

双方向コミュニケーションを作成する

AXIS D6310 Air Quality Sensorを中継装置として使用し、AXIS C6110 Network Paging Consoleへの通話を接続することができます。

AXIS D6310 Air Quality SensorとAXIS C6110 Network Paging Consoleの間で双方向コミュニケーションを作成する:

1. AXIS D6310 Air Quality Sensorの筐体を開けます。詳細については、インストールガイドを参照してください。
2. マイクのスイッチをオンにします。マイクの位置は、*製品概要, on page 29*で確認できます。
3. AXIS D6310 Air Quality Sensorのwebインターフェースで、[Video (ビデオ)] > [Stream (ストリーム)] > [Audio (音声)] に移動し、[Include (含める)] をオンにします。
4. [Audio (音声)] > [Device settings (装置設定)] に移動し、[Enable input (入力を有効にする)] をオンにします。デバイスでマイクをオンにしている場合のみ、入力を有効にできます。

5. [Audio (音声)] > [AXIS Audio Manager Edge] に移動し、[Create audio site {音声サイトの作成)] をクリックします。必要に応じて、AXIS Audio Manager Edgeの設定ウィザードを完了してください。
6. AXIS Audio Manager Edgeのwebインターフェースで、[Paging recipients (ページング送信先)] に移動し、[+ Create (作成)] をクリックします。
7. [Paging recipients (ページング送信先)] の画面に以下の情報を入力します。
   - Name (名前):ページングの送信先の名前
   - 通信タイプ:双方向
   - Protocol (プロトコル):VAPIX
   - 装置:AXIS D6310
8. [Create (作成)] をクリックします。
9. AXIS C6110 Network Paging Consoleのwebインターフェースで、[Communication (通信)] > [Recipients (送信先)] に移動し、[+ Add device (デバイスの追加)] をクリックします。
10. デバイスにAXIS D6310Air Quality Sensorを追加します。[Add device (デバイスの追加)] の画面で以下の情報を使用します。
    - Name (名前):D6310
    - Location (場所):Optional (オプション):
    - Protocol (プロトコル):VAPIX
    - IP:空気質センサーのIPアドレス。お使いのデバイスのIPアドレスの確認方法については、*faq.axis.com*で確認してください。
    - Username (ユーザー名) と Password (パスワード)
11. [Save (保存)] をクリックします。
12. [Display (ディスプレイ)] > [Configuration (設定)] > [Actions (アクション)] に移動し、[+ Create (作成)] をクリックします。
13. [Add action (アクションの追加)] の画面に以下の情報を入力します。
    - Action (アクション):双方向
    - Recipient (送信先):D6310
14. [Save (保存)] をクリックします。
15. [Display (ディスプレイ)] > [Configuration (設定)] > [Buttons (ボタン)] に移動し、[+ Button 1 (ボタン1)] をクリックします。
16. [Assign action (アクションの割り当て)] をクリックします。
17. [D6310] を選択し、[Assign action (アクションの割り当て)] をクリックします。
18. AXIS C6110 Network Paging Consoleで、[D6310] を押して双方向コミュニケーションを有効にします。

イベントのルールを設定する

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 (システム)] > [Events (イベント)] に移動し、[+ Add a rule (ルールの追加)] をクリックします。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実行する Action (アクション) を選択します。

センサーが電子タバコの使用を検知するとビデオを録画する

以下の例では、空気質センサーが電子タバコの使用を検知すると、ネットワークストレージへビデオを録画する設定方法を説明します。

1. デバイスのwebインターフェースで、[System (システム)]>[Storage (ストレージ)] に移動し、ネットワークストレージが設定されていることを確認します。
2. [System (システム)]>[Events (イベント)] に移動し、ルールを追加します。以下の情報を入力します。
   - Name (名前):ルールの名前を入力します。
   - Condition (条件):[Air quality monitor (空気質モニター)] > [Vaping or smoking detected (電子タバコまたはタバコの喫煙を検知)]
   - Action (アクション): [Recordings (録画) > Record video (ビデオの録画)。
   - ストレージ:ネットワークストレージ.ネットワークストレージに保存できない場合は、[System (システム)] > [Storage (ストレージ)] に移動し、オンにします。
   - カメラ:カメラの表示エリアを選択します。
   - Stream profile (ストリームプロファイル):ストリームプロファイルを選択するか、Create a stream profile (ストリームプロファイルを新規作成) します。
   - Prebuffer (プリバッファ) とPostbuffer (ポストバッフ): 希望の値を設定します。
3. [Save (保存)] をクリックします。

CO2が上限閾値を超えたら音声クリップを再生する

この例では、空気圧センサーが設定された閾値を超えるCO2を検知すると音声クリップを再生する方法について説明します。

ルールを作成する:

1. デバイスのwebインターフェースで、[System (システム)] > [Events (イベント)] > [Rules (ルール)] に移動し、[+ Add a rule (ルールの追加)] をクリックします。
2. 以下の情報を入力します。
   - Name (名前):ルールの名前を入力します。
   - 条件:[Air quality monitor (空気質モニター)] > [Air quality outside of acceptable range (空気質許容範囲外)]
   - Sensor (センサー):CO2.
   - Action (アクション):[Audio clips (音声クリップ)] > [Play audio clip (音声クリップの再生)]。
   - Clip (クリップ):音声クリップを選択します。
3. [Save (保存)] をクリックします。

CO2アラーム範囲を設定する:

- デバイスのwebインターフェースで、[Air quality monitor (空気質モニター)] > [Settings (設定)] > [Threshold (閾値)] の順に移動します。
- [Min (最小)] と [Max (最大)] の値データを入力し、CO2範囲を設定します。

PIRセンサー経由でライトとサイレンを作動させる

この例では、PIRセンサー経由でライトとサイレンを作動する方法を説明します。ライト (シグナリングLED) とサイレンの位置については、*製品概要, on page 29*を参照してください。

ライトとサイレンのプロファイルを作成する:

1. デバイスのwebインターフェースで、[Profiles (プロファイル)] に移動し、[+ Create (作成)] をクリックします。
2. 以下の情報を入力します。
   - Name (名前):プロファイル1.
   - Description (説明):プロファイルの説明を追加します。
   - [Light (ライト)]:プロンプトが表示されたら、[Pattern (パターン)]、[Speed (速度)]、[Intensity (明るさ)]、[Color (カラー)], and [Duration (持続時間)] を選択します。
   - [Siren (サイレン)]:[Pattern (パターン)]、[Intensity (明るさ)]、[Duration (時間)] を選択します。

   注
   番号の高いプロファイルは優先度が高くなります。
   - [Priority (優先度)]:[Light priority (ライト優先度)] と [Siren priority (サイレン優先度)] を選択します。
3. [Save (保存)] をクリックします。

イベントを作成する:

1. [System (システム)] > [Events (イベント)] > [Rules (ルール)] に移動し、[+ Add a rule (ルールの追加)] をクリックします。
2. 以下の情報を入力します。
   - Name (名前):シグナリングLEDとサイレンを作動させる.
   - Condition (条件):PIRセンサー.
   - Action (アクション):ライトとサイレンのプロファイルを実行.
   - Profile (プロファイル):プロファイル1.
   - Action (アクション):開始。
3. [Save (保存)] をクリックします。

アラームがトリガーされたときにプロファイルを開始します

この例では、デジタル入力信号が変わったときにアラームをトリガーする方法について説明します。

ポートの方向入力を設定する手順:

1. [System (システム)]>[Accessories (アクセサリー)]>[I/O ports (I/Oポート)] に移動します。
2. [Port 1 (ポート1)]>[Normal state (通常状態)] に進み、[Circuit closed (閉回路)] をクリックします。

ルールの作成:

1. [System (システム)]>[Events (イベント)] に移動し、ルールを追加します。
2. ルールの名前を入力します。
3. 条件の一覧で、[I/O] > [Digital input is active (デジタル入力がアクティブ)] を選択します。

4. [Port 1 (ポート1)] を選択します:
5. アクションのリストで、[Run light and siren profile while the rule is active (ルールがアクティブの間、ライトとサイレンのプロファイルを実行)] を選択します。
6. [profile you want to start (開始するプロファイル)] を選択します。
7. [Save (保存)] をクリックします。

SIPを介したプロファイルの開始

この例では、SIPを介してアラームをトリガーする方法について説明します。

SIPを有効にする:

1. [System (システム)] > [SIP] > [SIP settings (SIP設定)] に移動します。
2. [Enable SIP (SIPの有効化)] と [Allow incoming calls (着信呼び出しを許可)] を選択します。
3. [Save (保存)] をクリックします。

ルールの作成:

1. [System (システム)]>[Events (イベント)] に移動し、ルールを追加します。
2. ルールの名前を入力します。
3. 条件のリストで、[Call (呼び出し)]>[State (状態)] を選択します。
4. 状態のリストで、[Active (アクティブ)] を選択します。
5. アクションのリストで、[Run light and siren profile while the rule is active (ルールがアクティブの間、ライトとサイレンのプロファイルを実行)] を選択します。
6. [profile you want to start (開始するプロファイル)] を選択します。
7. [Save (保存)] をクリックします。

SIP内線番号による複数のプロファイルの制御

SIPを有効にする:

1. [System (システム)] > [SIP] > [SIP settings (SIP設定)] に移動します。
2. [Enable SIP (SIPの有効化)] と [Allow incoming calls (着信呼び出しを許可)] を選択します。
3. [Save (保存)] をクリックします。

プロファイルを開始するルールを作成する:

1. [System (システム)]>[Events (イベント)] に移動し、ルールを追加します。
2. ルールの名前を入力します。
3. 条件のリストで、[Call (呼び出し)] > [State change (状態変更)] を選択します。
4. 理由のリストで、[Accepted by device (装置で受け入れ)] を選択します。
5. [Call direction (呼び出し方向)] で [Incoming (着信)] を選択します。
6. Local SIP URIに<sipを入力してください:[Ext]@[IP address]> [Ext]はプロファイルで使用する内線番号、[IP address]はデバイスのIPアドレスです。たとえば、sip:1001@192.168.0.90とします。
7. アクションのリストで、[Light and Siren (ライトとサイレン)] > [Run light and siren profile (ライトとサイレンのプロファイルを実行)] の順に選択します。
8. [profile you want to start (開始するプロファイル)] を選択します。
9. アクション [Start (開始)] を選択します。

10. **[Save (保存)]** をクリックします。

プロファイルを停止するルールを作成する:

1. [System (システム)]>[Events (イベント)] に移動し、ルールを追加します。
2. ルールの名前を入力します。
3. 条件のリストで、[Call (呼び出し)] > [State change (状態変更)] を選択します。
4. 理由のリストで、[Terminated (終了した)] を選択します。
5. [Call direction (呼び出し方向)] で [Incoming (着信)] を選択します。
6. [Local SIP URI] にsip:[Ext]@[IP address] と入力します。[Ext] はプロファイルに使用する内線番号で、[IP address] は装置のアドレスです。たとえば、sip:1001@192.168.0.90とします。
7. アクションのリストで、[Light and Siren (ライトとサイレン)] > [Run light and siren profile (ライトとサイレンのプロファイルを実行)] の順に選択します。
8. 停止するプロファイルを選択します。
9. アクション [Stop (停止)] を選択します。
10. **[Save (保存)]** をクリックします。

この手順を繰り返して、SIPで制御する各プロファイルの開始と停止のルールを作成します。

優先度が異なる2つのプロファイルを実行する

優先度が異なる2つのプロファイルを実行すると、優先度の数字が高い番号のプロファイルが優先度の数字が低い番号のプロファイルに割り込みます。

注

同じ優先度の2つのプロファイルを実行した場合、最新のプロファイルによって前のプロファイルがキャンセルされます。

この例では、デジタルI/Oポートによってトリガーされたときに、優先度4のプロファイルを優先度3のプロファイルよりも先に表示するように設定する方法について説明します。

プロファイルの作成:

1. 優先度3のプロファイルを作成します。
2. 優先度4の別のプロファイルを作成します。

ルールの作成:

1. [System (システム)]>[Events (イベント)] に移動し、ルールを追加します。
2. ルールの名前を入力します。
3. 条件の一覧で、[I/O] > [Digital input is active (デジタル入力がアクティブ)] を選択します。
4. [port (ポート)] を選択します。
5. アクションのリストで、**[Run light and siren profile while the rule is active (ルールがアクティブの間、ライトとサイレンのプロファイルを実行)]** を選択します。
6. [the profile that has the highest priority number (優先度の数字が最も高いプロファイル)] を選択します。
7. **[Save (保存)]** をクリックします。
8. [Profiles (プロファイル)] に移動し、優先度の数字が最も低い番号のプロファイルを開始します。

カメラが動きを検知すると、HTTP postを使用してライトとサイレンのプロファイルを有効にする

この例では、空気質センサーにカメラを接続する方法と、カメラにインストールされているアプリケーションAXIS Motion Guardが動きを検知すると、空気質センサーのライトとサイレンのプロファイルを有効にする方法について説明します。

開始する前に:

- 空気質センサーのオペレーター、または管理者のロールを持つ新しいユーザーを作成します。
- 空気質センサーのプロファイルを次の名前で作成します: “Light and siren profile” (ライトとサイレンのプロファイル)。
- カメラでAXIS Motion Guardを設定し、プロファイルを次の名前で作成します。“Camera profile” (カメラのプロファイル)。
- バージョン10.8.0以降のファームウェアでAXIS Device Assistantを使用してください。

カメラで送信先を作成する手順:

1. カメラの装置インターフェースで [**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. 以下の情報を入力します。
   - **Name (名前)**:空気質センサー
   - **Type (タイプ)**: HTTP
   - URL: http://<IPaddress>/axis-cgi/siren_and_light.cgi
     <IPアドレス>を空気質センサーのアドレスに置き換えます。
   - これは新しく作成された空気質センサーのユーザー名とパスワードです。
3. [**Test (テスト)**] をクリックして、すべてのデータが有効であることを確認します。
4. **[Save (保存)]** をクリックします。

カメラに2つのルールを作成する:

1. [**Rules (ルール)**] に移動し、ルールを追加します。
2. 以下の情報を入力します。
   - **Name (名前)**:空気質センサーを動きの検知で起動する
   - Condition (条件): [Applications (アプリケーション)] > [Motion Guard: Camera profile (モーションガード: カメラプロファイル)]
   - Action (アクション): [Notifications (通知)] > [Send notification through HTTP (HTTPで通知を送信する)]
   - Recipient (送信先): 空気質センサー.
     この情報は、[Events > Recipients > Name (イベント > 送信先 > 名前)] で入力した情報と同じである必要があります。
   - Method (方式): Post
   - Body (本文):

```
{  "apiVersion": "1.0",  "method": "start",  "params": {
"profile" : "Light and siren profile"  } }
```

空気質センサーのプロファイルを作成したときと同じ情報を**["profile" (プロファイル): <>]** に入力します。“Light and siren profile” (ライトとサイレンのプロファイル)。

3. **[Save (保存)]** をクリックします。
4. 次の情報を含む別のルールを追加します。
   - **Name (名前)**:空気質センサーを動きの検知で解除する
   - Condition (条件): [Applications (アプリケーション)] > [Motion Guard: Camera profile (モーションガード: カメラプロファイル)]
   - [Invert this condition (この条件を逆にする)] を選択します。

- Action (アクション): [Notifications (通知)] > [Send notification through HTTP (HTTPで通知を送信する)]
- Recipient (送信先): 空気質センサー
  この情報は、[Events > Recipients > Name (イベント > 送信先 > 名前)] で入力した情報と同じである必要があります。
- Method (方式): Post
- Body (本文):

```
{  "apiVersion": "1.0",  "method": "stop",  "params": {    "profile" : "Light and siren profile"  } }
```

空気質センサーのプロファイルを作成したときと同じ情報を**["profile" (プロファイル): <>]** に入力します。“Light and siren profile” (ライトとサイレンのプロファイル)。

5. **[Save (保存)]** をクリックします。

カメラが動きを検知すると、仮想入力を使用してライトとサイレンのプロファイルを有効にする

この例では、空気質センサーにカメラを接続する方法と、カメラにインストールされているアプリケーションAXIS Motion Guardが動きを検知すると、空気質センサーのライトとサイレンのプロファイルを有効にする方法について説明します。

開始する前に:

- 空気質センサーでオペレーター、または管理者権限を持つ新しいアカウントを作成します。
- 空気質センサーのプロファイルを作成します。*プロファイル*を参照してください。
- カメラでAXIS Motion Guardを設定し、「カメラプロファイル」というプロファイルを作成します。

カメラで2人の送信先を作成する:

1. カメラの装置インターフェースで [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. 以下の情報を入力します。
   - Name (名前):Activate virtual port (仮想ポートのアクティブ化)
   - Type (タイプ): HTTP
   - URL::://<IPaddress>/axis-cgi/virtualinput/activate.cgi
     <IPアドレス>を空気質センサーのアドレスに置き換えます。
   - これは新しく作成された空気質センサーのアカウントとパスワードです。
3. [Test (テスト)] をクリックして、すべてのデータが有効であることを確認します。
4. **[Save (保存)]** をクリックします。
5. 次の情報を含む2番目の送信先を追加します。
   - Name (名前):仮想ポートの非アクティブ化
   - Type (タイプ): HTTP
   - URL:http://<IPaddress>/axis-cgi/virtualinput/deactivate.cgi
     <IPアドレス>を空気質センサーのアドレスに置き換えます。
   - これは新しく作成された空気質センサーのアカウントとパスワードです。
6. [Test (テスト)] をクリックして、すべてのデータが有効であることを確認します。
7. **[Save (保存)]** をクリックします。

カメラに2つのルールを作成する:

1. [Rules (ルール)] に移動し、ルールを追加します。
2. 以下の情報を入力します。
   - Name (名前):仮想IO1のアクティブ化

- Condition (条件): [Applications (アプリケーション)] > [Motion Guard: Camera profile (モーションガード: カメラプロファイル)]
- Action (アクション): [Notifications (通知)] > [Send notification through HTTP (HTTPで通知を送信する)]
- Recipient (送信先): Activate virtual port (想ポートのアクティブ化)
- Query string suffix (クエリ文字列のサフィックス):schemaversion=1&port=1

3. [Save (保存)] をクリックします。
4. 次の情報を含む別のルールを追加します。
   - Name (名前):仮想IO1の非アクティブ化
   - Condition (条件): [Applications (アプリケーション)] > [Motion Guard: Camera profile (モーションガード: カメラプロファイル)]
   - [Invert this condition (この条件を逆にする)] を選択します。
   - Action (アクション): [Notifications (通知)] > [Send notification through HTTP (HTTPで通知を送信する)]
   - Recipient (送信先): Deactivate virtual port (仮想ポートの非アクティブ化)
   - Query string suffix (クエリ文字列のサフィックス):schemaversion=1&port=1
5. [Save (保存)] をクリックします。

空気質センサーのルールを作成する:
1. 空気質センサーのWebインターフェースで、[System (システム)] > [Events (イベント)] に移動し、ルールを追加します。
2. 以下の情報を入力します。
   - Name (名前):仮想入力1のトリガー
   - Condition (条件): [I/O] > [Virtual input is active (仮想入力有効)]
   - ポート:1
   - Action (アクション: [Light and siren (ライトとサイレン)] > [Run light profile while the rule is active (ルールがアクティブである間は、ライトとサイレンのプロファイルを実行)]
   - Profile (プロファイル):新しく作成したプロファイルを選択します。
3. [Save (保存)] をクリックします。

カメラが動きを検知すると、MQTT経由でライトとサイレンのプロファイルを有効にする

この例では、カメラを空気質センサーに接続する方法と、カメラが動きを検知すると空気質センサーのライトとサイレンのプロファイルを有効にする方法を説明します。

開始する前に:
- 空気質センサーのプロファイルを作成します。
- MQTTブローカーを設定し、ブローカーのIPアドレス、ユーザー名、パスワードを取得します。
- 動体検知アプリケーションが設定済みでカメラで実行中であることを確認してください。

カメラでMQTTクライアントを設定する:
1. カメラのWebインターフェースで、[System > MQTT > MQTT client > Broker (システム > MQTT > MQTTクライアント > ブローカー)] にアクセスし、以下の情報を入力します。
   - [ホスト]:ブローカーIPアドレス
   - Client ID (クライアントID):例: カメラ1
   - Protocol (プロトコル):ブローカーが設定したプロトコル

- Port (ポート):ブローカーが使用するポート番号
- ブローカーの Username (ユーザー名) と Password (パスワード)

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

MQTTパブリッシングのためにカメラで2つのルールを作成する:

1. [System > Events > Rules (システム > イベント > ルール)] に移動し、ルールを追加します。
2. 以下の情報を入力します。
   - Name (名前):動体を検知しました
   - Condition (条件): [Applications (アプリケーション)] > [Motion alarm (モーションアラーム)]
   - Action (アクション):[MQTT] > [Send MQTT publish message (MQTT公開メッセージを送信)]
   - Topic (トピック):動き
   - Payload (ペイロード):オン
   - QoS:0、1、または2
3. [Save (保存)] をクリックします。
4. 次の情報を含む別のルールを追加します。
   - Name (名前):動きなし
   - Condition (条件): [Applications (アプリケーション)] > [Motion alarm (モーションアラーム)]
     - [Invert this condition (この条件を逆にする)] を選択します。
   - Action (アクション):[MQTT] > [Send MQTT publish message (MQTT公開メッセージを送信)]
   - Topic (トピック):動き
   - Payload (ペイロード):オフ
   - QoS:0、1、または2
5. [Save (保存)] をクリックします。

空気質センサーにMQTTクライアントを設定する:

1. 空気質センサーのWebインターフェースで、[System (システム)] > [MQTT] > [MQTT client (MQTTクライアント)] > [Broker (ブローカー)] の順に移動して、以下の情報を入力します。
   - [ホスト]:ブローカーIPアドレス
   - Client ID (クライアントID):サイレン1
   - Protocol (プロトコル):ブローカーが設定したプロトコル
   - Port (ポート):ブローカーが使用するポート番号
   - Username (ユーザー名) と Password (パスワード)
2. [Save (保存)]をクリックし、[Connect (接続)]をクリックします。
3. [MQTT subscriptions (MQTTサブスクリプション)] に移動し、サブスクリプションを追加します。
   以下の情報を入力します。
   - サブスクリプションフィルター:動き
   - サブスクリプションの種類:ステートフル
   - QoS:0、1、または2
4. [Save (保存)] をクリックします。

MQTTサブスクリプションについて空気質センサーのルールを作成する:

1. [System > Events > Rules (システム > イベント > ルール)] に移動し、ルールを追加します。
2. 以下の情報を入力します。
   - Name (名前):動体を検知しました
   - Condition (条件):[MQTT] > [Stateful (ステートフル)]
   - Subscription filter (サブスクリプションフィルター): Motion (動き)
   - Payload (ペイロード):オン
   - Action (アクション: [Light and siren (ライトとサイレン)] > [Run light profile while the rule is active (ルールがアクティブである間は、ライトとサイレンのプロファイルを実行)]
   - Profile (プロファイル):アクティブにするプロファイルを選択します。
3. [Save (保存)] をクリックします。

スピーカーテストが失敗した場合に電子メールを送信する

この例では、音声デバイスは、スピーカーテストが失敗したときに定義済みの送信先に電子メールを送信するように設定されています。スピーカーテストは、毎日18:00に実行するように設定されています。

1. スピーカーテストのスケジュールを設定する方法:
   1.1. [device interface (デバイスインターフェース)] > [System (システム)] > [Events (イベント)] > [Schedules (スケジュール)] に移動します。
   1.2. 毎日 18:00 に開始し、18:01 に終了するスケジュールを作成します。「毎日午後6時」と名付けます。
2. 電子メールの送信先を作成する:
   2.1. [device interface > System > Events > Recipients (デバイスインターフェース > システム > イベント > 送信先)] に移動します。
   2.2. [Add Recipient (送信先の追加)] をクリックします。
   2.3. 送信先に「スピーカーテストの送信先」と名前を付けます
   2.4. [Type (タイプ)] 配下で [Email (電子メール)] を選択します。
   2.5. [Send email to (電子メールの送信先)] で、送信先のメールアドレスを入力します。複数のアドレスを指定する場合は、カンマで区切ります。
   2.6. 送信者の電子メールアカウントの詳細を入力します。
   2.7. [Test (テスト)] をクリックして、テストメールを送信します。

   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、スケジュールにしたがって送信された電子メールなどの受信を防止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て、メールの送信の問題が発生したり、電子メールアカウントがロックされたりしないようにしてください。

   2.8. [Save (保存)] をクリックします。
3. 自動スピーカーテストを設定します:
   3.1. [device interface > System > Events > Rules (デバイスインターフェース > システム > イベント > ルール)] に移動します。
   3.2. [Add a rule (ルールの追加)] をクリックします。
   3.3. アクションルールの名前を入力します。
   3.4. [Condition (条件)] で [Schedule (スケジュール)] を選択し、トリガーリストから選択します。
   3.5. [Schedule (スケジュール)] でスケジュールを選択します (「毎日午後6時」)。

3.6. [Action (アクション)] で [Run automatic speaker test (自動スピーカーテストの実行)] を選択します。

3.7. [Save (保存)] をクリックします。

4. スピーカーテストが失敗した場合に電子メールを送信する条件を設定します:

4.1. [device interface > System > Events > Rules (デバイスインターフェース > システム > イベント > ルール)] に移動します。

4.2. [Add a rule (ルールの追加)] をクリックします。

4.3. アクションルールの名前を入力します。

4.4. [Condition (条件)] で [Speaker test result (スピーカーテストの結果)] を選択します。

4.5. [Speaker test status (スピーカーテストのステータス)] で、[Didn't pass the test (テストに不合格)] を選択します。

4.6. [Action (アクション)] で [Send notification to email (電子メールで通知を送信する)] を選択します。

4.7. [Recipient (送信先)] で、送信先を選択します (「スピーカーテストの送信先」)

4.8. 件名とメッセージを入力し、[Save (保存)] をクリックします。

アラームトリガー時にカスタムクリップを再生する

この例では、デジタル音声入力信号が変化したときにカスタムオーディオファイルをトリガーする方法を説明します。

音声ファイルのアップロード:

1. [Media (メディア)] に移動し、[+ Add (追加)] をクリックします。
2. クリックしてコンピューターから音声ファイルを選択します。
3. [Storage location (保存先)]を選択します。
4. [Save (保存)] をクリックします。

音声ファイルでプロファイルを作成する:

1. [Profiles (プロファイル)] に移動し、[+ Create (作成)] をクリックします。
2. Name と入力し、プロファイルのライトパターンを選択します。
3. サイレンセクションで、アップロードされた音声ファイルを選択します。
4. [Intensity (強さ)] と[Intensity (持続時間)] を選択します。
5. [Save (保存)] をクリックします。

ポートの方向入力を設定する手順:

1. [System (システム)]>[Accessories (アクセサリー)]>[I/O ports (I/Oポート)] に移動します。
2. [Port 1 (ポート1)]>[Normal state (通常状態)] に進み、[Circuit closed (閉回路)] をクリックします。

ルールの作成:

1. [System (システム)]>[Events (イベント)] に移動し、ルールを追加します。
2. アクションルールの名前を入力します。
3. 条件の一覧で、[I/O>] [Digital input is active (デジタル入力がアクティブ)] を選択します。
4. [Port 1 (ポート1)] を選択します:
5. アクションのリストで、[Run light and siren profile while the rule is active (ルールがアクティブである間は、ライトとサイレンのプロファイルを実行)] を選択します。

6. アップロードした音声ファイルを含むプロファイルを選択します。
7. [Save (保存)] をクリックします。

DTMFで音声を停止する

この例では、次の方法について説明します。
- デバイスでDTMFを設定する。
- DTMFコマンドがデバイスに送信されたときに音声を停止するイベントを設定する

1. [System (システム)] > [SIP] > [SIP settings (SIP設定)] に移動します。
2. [Enable SIP (SIPの有効化)] がオンになっていることを確認します。
   オンにする必要がある場合は、必ず [Save (保存)] をクリックしてください。
3. [SIP accounts (SIPのアカウント)] に移動します。
4. SIPアカウントの横にある ⋮ > [Edit (編集)]をクリックします。
5. [DTMF] で [+ DTMFシーケンス] をクリックします。
6. [シーケンス] に「1」を入力します。
7. [Description (説明)] に「音声の停止」と入力します。
8. [Save (保存)] をクリックします。
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. [Name (名前)] に「DTMF stop audio (DTMF音声の停止)」と入力します。
11. [Condition (条件)] で [DTMF] を選択します。
12. [DTMFイベントID] で [音声の停止] を選択します。
13. [Action (アクション)] で [Stop playing audio clip (オーディオクリップの再生を停止)] を選択します。
14. [Save (保存)] をクリックします。

着信SIP呼び出しの音声の設定

SIP呼び出しの受信時に音声クリップを再生するルールを設定できます。

音声クリップの終了後にSIP呼び出しに自動的に応答する追加ルールを設定することもできます。このルールは、アラームオペレーターが音声デバイスの近くの人に注意を促し、通信回線を確立したい場合に便利です。この操作は、音声デバイスにSIP呼び出しを行い、音声デバイスで音声クリップを再生してデバイスの近くの人に警告することで行われます。音声クリップの再生が停止すると、SIP呼び出しは音声デバイスによって自動的に応答され、アラームオペレーターと音声デバイスの近くの人の間の通信が行われます。

SIP設定を有効にする:
1. WebブラウザでIPアドレスを入力して、スピーカーのデバイスインターフェースに移動します。
2. [System (システム)] > [SIP] > [SIP settings (SIP設定)] に移動し、[Enable SIP (SIPの有効化)]]を選択します。
3. デバイスで着信呼び出しの受信を許可するには、[Allow incoming calls (着信呼び出しを許可)] を選択します。
4. [Save (保存)] をクリックします。
5. [SIP accounts (SIPのアカウント)] に移動します。
6. SIPアカウントの横にある ⋮ > [Edit (編集)]をクリックします。
7. [Answer automatically (自動応答)] のチェックを外します。

SIP呼び出しの受信時に音声を再生する:

1. [Settings (設定)] > [System (システム)] > [Events (イベント)] > [Rules (ルール)] に移動し、ルールを追加します。
2. ルールの名前を入力します。
3. 条件のリストで、[State (状態)] を選択します。
4. 状態のリストで、[Ringing (呼び出し中)] を選択します。
5. アクションのリストで、[Play audio clip (音声クリップの再生)] を選択します。
6. クリップのリストで、再生する音声クリップを選択します。
7. 音声クリップを繰り返す回数を選択します。0は「1回再生」を意味します。
8. [Save (保存)] をクリックします。

音声クリップの終了後、SIP呼び出しに自動的に応答する:

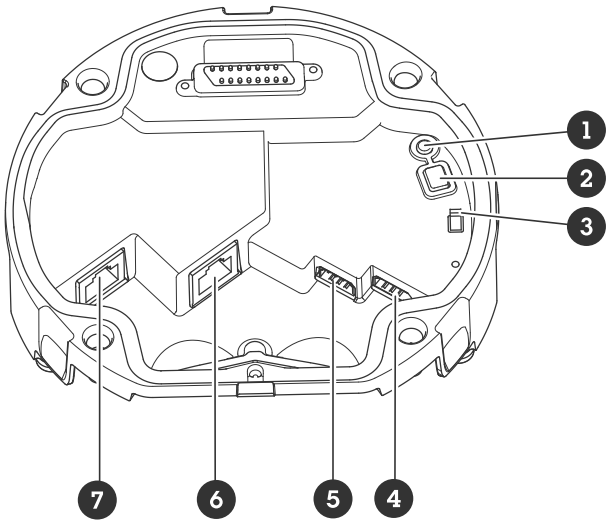
1. [Settings (設定)] > [System (システム)] > [Events (イベント)] > [Rules (ルール)] に移動し、ルールを追加します。
2. ルールの名前を入力します。
3. 条件のリストで [Audio clip playing (音声クリップを再生中)] を選択します。
4. [Use this condition as a trigger (この条件をトリガーとして使用する)] をオンにします。
5. [Invert this condition (この条件を逆にする)] をオンにします。
6. [+ Add a condition (+ 条件の追加)] をクリックして、イベントに2つ目の条件を追加します。
7. 条件のリストで、[State (状態)] を選択します。
8. 状態のリストで、[Ringing (呼び出し中)] を選択します。
9. アクションのリストで[Answer Call (呼び出しに応答する)]を選択します。
10. [Save (保存)] をクリックします。

webインターフェース

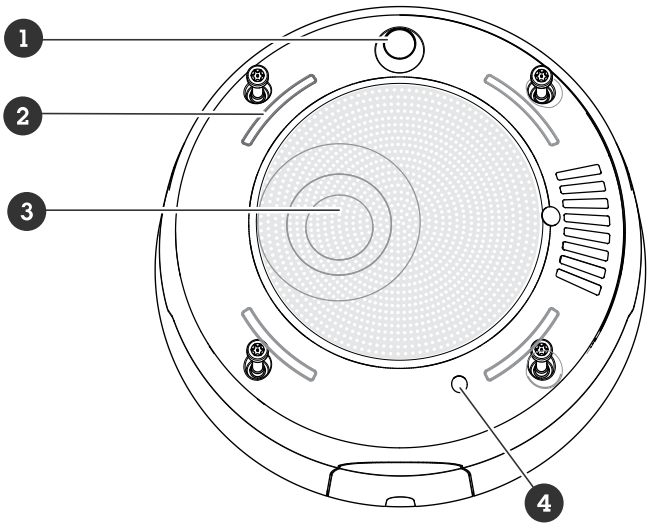
AXIS OS搭載デバイスのWebインターフェースで利用可能なすべての機能および設定については、*AXIS OS Webインターフェースヘルプ*を参照ください。

仕様

製品概要



1 ステータスLEDインジケーター
2 コントロールボタン
3 マイクスイッチ
4 I/Oコネクター
5 RS-485コネクター
6 ネットワークコネクタ (PoE出力)
7 ネットワークコネクタ (PoE入力)



1 PIRセンサー
2 シグナリングLED
3 スピーカー
4 内蔵マイク

ステータスLED

ステータスLED	説明
消灯	正常動作の場合消灯します。
緑	起動完了後、通常の操作では10秒間点灯します。
黄色	起動時に点灯.装置のソフトウェアのアップグレード中、または工場出荷時の設定にリセット中に点滅します。
オレンジ/赤	ネットワーク接続が利用できないか、失われた場合は点滅します。

ボタン

コントロールボタン

コントロールボタンは、以下の用途で使用します。

- 製品を工場出荷時の設定にリセットする。*工場出荷時の設定にリセットします。, on page 35*を参照してください。

マイクスイッチ

マイクロフォンスイッチの位置については、*製品概要, on page 29*を参照してください。

マイクロフォンスイッチは、マイクロフォンを機械的に**オン**または**オフ**にするために使用します。工場出荷時の設定では、このスイッチは**オフ**になっています。

コネクター

ネットワークコネクター

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

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

I/Oコネクター

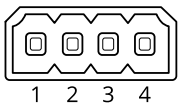
I/Oコネクターに外部装置を接続し、動体検知、イベントトリガー、アラーム通知などと組み合わせて使用することができます。I/Oコネクターは、0 VDC基準点と電力 (12V DC出力) に加えて、以下のインターフェースを提供します。

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

状態監視入力 - デジタル入力のいたずらを検知する機能が有効になります。

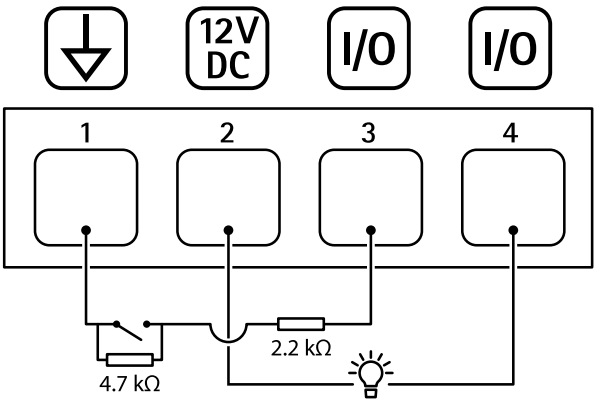
デジタル出力 - リレーやLEDなどの外部デバイス接続用。接続された装置は、VAPIX®アプリケーションプログラミングインターフェースを通じたイベントまたは本装置のwebインターフェースから有効にすることができます。

4ピンターミナルブロック



機能	ピン	メモ	仕様
DCアース	1		0 VDC
DC出力	2	⚠ 補助装置の電源供給に使用できます。 注:このピンは、電源出力としてのみ使用できます。	12VDC 最大負荷 = 25 mA
設定可能 (入力または出力)	3-4	デジタル入力/状態監視 – 動作させるにはピン1に接続し、動作させない場合はフロート状態 (未接続) のままにします。状態監視を使用するには、終端抵抗器を設置します。抵抗器を接続する方法については、接続図を参照してください。	0～30VDC (最大)
		デジタル出力 – アクティブ時はピン1 (DCアース) に内部で接続し、非アクティブ時はフロート状態 (未接続) になります。リレーなどの誘導負荷とともに使用する場合は、過渡電圧から保護するために、負荷と並列にダイオードを接続します。	0～30VDC (最大)、オープンドレイン、100 mA

例:

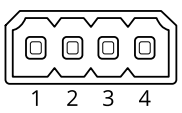


1 *DCアース*
2 *DC出力12 V、最大25 mA*
3 *I/O (状態監視として設定)*
4 *I/O (出力として設定)*

RS485/RS422コネクター

RS485/RS422シリアルインターフェース用2ピンターミナルブロック×2。シリアルポートの設定により、次のモードをサポート可能。

- 2ワイヤーRS485半二重。
- 4ワイヤーRS485全二重。
- 2ワイヤーRS422単方向
- 4ワイヤーRS422全二重ポイントツーポイント通信



機能	ピン	メモ
RS485/RS422 RX/TX A	1	(RX) 全二重RS485/RS422用 (RX/TX) 半二重用 RS485
RS485/RS422 RX/TX B	2	
RS485/RS422 TX A	3	(TX) 全二重RS485/RS422用
RS485/RS422 TX B	4	

ライトパターン名

オフ
点灯
代替
Pulse (パルス):
3つのステップでエスカレート
点滅
3回点滅
4回点滅
3回点滅して消える
4回点滅して消える
1回点滅
3回点滅

サイレンのパターン名

オフ
アラーム:高音アラーム
アラーム:低音アラーム
アラーム:鳥
アラーム:汽笛
アラーム:カーアラーム
アラーム:車のアラーム 高速
アラーム:クラシック時計
アラーム:初回出席者
アラーム:ホラー
アラーム:工業
アラーム:単一ビープ音
アラーム:ソフトクアッドビープ音
アラーム:ソフトトリプルビープ音
アラーム:トリプルハイピッチ

通知:許可
通知:呼び出し中
通知:却下
通知:完了
通知:エントリ
通知:失敗しました
通知:急ぐ
通知:メッセージ
通知:次へ
通知:オープン
[Siren (サイレン)]:代替
[Siren (サイレン)]:弾む
[Siren (サイレン)]:救急
[Siren (サイレン)]:下降調
[Siren (サイレン)]:ホームソフト

装置を清掃する

装置はぬるま湯で洗浄できます。

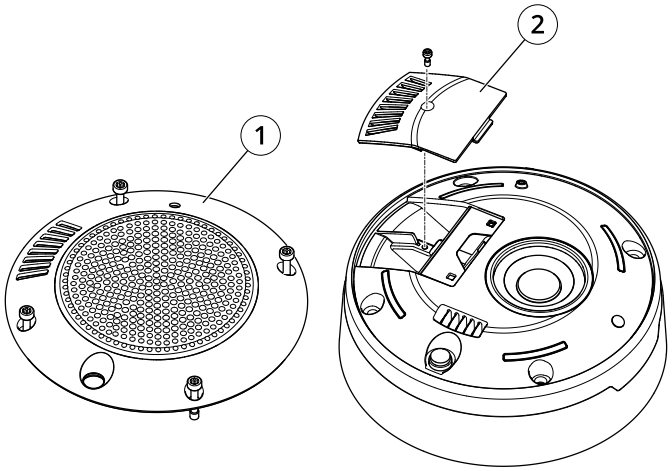
注意

- 強力な化学薬品は装置を損傷する可能性があります。窓ガラス用洗剤やアセトンなどの化学薬品を使用して装置をクリーニングしないでください。

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

注

- カバー (1) とドア (2) を取り外します。
- ブラシを使ってほこりを取り除きます。



1 カバー
2 ドア

トラブルシューティング

工場出荷時の設定にリセットします。

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。

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。

技術的な問題、ヒント、解決策

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

AXIS OSのアップグレード時の問題

AXIS OSのアップグレードに失敗する	アップグレードに失敗した場合、装置は前のバージョンを再度読み込みます。最も一般的な理由は、AXIS OSの間違ったファイルがアップロードされた場合です。装置に対応したAXIS OSのファイル名であることを確認し、再試行してください。
AXIS OSのアップグレード後の問題	アップグレード後に問題が発生する場合は、[Maintenance (メンテナンス)] ページから、以前にインストールされたバージョンにロールバックします。

IPアドレスの設定で問題が発生する

デバイスが別のサブネット上にある	デバイス用のIPアドレスと、デバイスへのアクセスに使用するコンピューターのIPアドレスが異なるサブネットにある場合は、IPアドレスを設定することはできません。ネットワーク管理者に連絡して、適切なIPアドレスを取得してください。
IPアドレスが別のデバイスで使用されている	デバイスをネットワークから切断します。pingコマンドを実行します (コマンドウィンドウまたはDOSウィンドウで、`ping`コマンドとデバイスのIPアドレスを入力します)。 • `Reply from <IP address>: bytes=32; time=10...`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。 • 「`Request timed out`」が表示された場合は、そのAXISデバイスにその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アドレスが競合している可能性がある	DHCPサーバーによって動的アドレスが設定される前は、Axisデバイスは静的IPアドレスを使用します。つまり、デフォルトの静的IPアドレスが別のデバイスでも使用されていると、デバイスへのアクセスに問題が発生する可能性があります。

ブラウザーから装置にアクセスできない

ログインできない	HTTPSが有効になっているときは、ログインを試みるときに正しいプロトコル (HTTPまたはHTTPS) を使用していることを確認してください。場合によっては、ブラウザ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。*工場出荷時の設定にリセットします。, on page 35*を参照してください。
DHCPによってIPアドレスが変更された	DHCPサーバーから取得したIPアドレスは動的なアドレスであり、変更されることがあります。IPアドレスが変更された場合は、AXIS IP UtilityまたはAXIS Device Managerを使用してデバイスのネットワーク上の場所を特定してください。デバイスのモデルまたはシリアル番号、あるいはDNS名 (設定されている場合) を使用してデバイスを識別します。 必要に応じて、静的IPアドレスを手動で割り当てることができます。手順については、*axis.com/support*にアクセスしてください。
IEEE 802.1X使用時の証明書エラー	認証を正しく行うには、Axisデバイスの日付と時刻をNTPサーバーと同期させなければなりません。[**System (システム) > Date and time (日付と時刻)**] に移動します。

装置にローカルにアクセスできるが、外部からアクセスできない

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

- AXIS Camera Station Edge:無料で使用でき、基本的な監視ニーズがある小規模システムに最適です。
- AXIS Camera Station 5:30日間の試用版を無料で使用でき、中小規模のシステムに最適です。
- AXIS Camera Station Pro:90日間の試用版を無料で使用でき、中小規模のシステムに最適です。

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

MQTTオーバSSLを使用してポート8883経由で接続できない

ファイアウォールによって、ポート8883が安全ではないと判断されたため、ポート8883を使用するトラフィックがブロックされています。	場合によっては、サーバー/ブローカーによってMQTT通信用に特定のポートが提供されていない可能性があります。この場合でも、HTTP/HTTPSトラフィックに通常使用されるポート経由でMQTTを使用できる可能性があります。 • サーバー/ブローカーが、通常はポート443経由で、WebSocket/WebSocket Secure (WS/WSS) をサポートしている場合は、代わりにこのプロトコルを使用してください。サーバー/ブローカープロバイダーに問い合わせて、WS/WSSがサポートされているかどうか、どのポートと基本パスを使用するかを確認してください。 • サーバー/ブローカーがALPNをサポートしている場合、MQTTの使用は443などのオープンポートでネゴシエートできます。ALPNのサポートの有無、使用するALPNプロトコルとポートについては、サーバー/ブローカーのプロバイダーに確認してください。

別の製品に接続した後、デバイスが起動しない	
PoEクラスが誤っている	デバイスを別の製品に接続した場合、PoEクラス4の電源が使用されていることを確認してください。

センサーデータが正確でない	
センサーデータが不正確である	AQI (大気質指数)、CO2、VOC、NOxが機能するまでには時間がかかります。*装置の初起動時のキャリブレーション, on page 9*を参照してください。

パフォーマンスに関する一般的な検討事項

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。

サポートに問い合わせる

さらにサポートが必要な場合は、*axis.com/support*にアクセスしてください。

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な情報や資料は、*axis.com/about-axis/cybersecurity* でご覧いただけます。以下のサイバーセキュリティガイドラインに従ってAxisからの製品に関するセキュリティ通知を受け取り、製品の安全なライフサイクルおよび運用停止のための設定を行ってください。

*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いただけます。

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 から、Axisのセキュリティ通知電子メールを購読してください。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、およびその他のセキュリティ関連事項について情報をお送りします。

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。

T10222990_ja

2026-09 (M9.3)

© 2025 – 2026 Axis Communications AB