AXIS D3110 Mk II Connectivity Hub

ユーザーマニュアル

ソリューションの概要

このデバイスを使うと、このような機能を持たない、または追加機能を必要とするネットワークビデオシステムへセンサーや音声を統合することが可能になります。ネットワークセキュリティを危険にさらすことなくシーンの認識を高めるのに役立ち、Axisのエンドツーエンドソリューションに最適です。

音声またはビデオ管理ソフトウェアを使用している場合は、それらのソフトウェアを使用してデバイスを設定できます。音声システムを制御するには、以下の管理ソフトウェアを使用できます。

- AXIS Audio Manager Edge - 小規模システム向け音声管理ソフトウェアです。ファームウェアが10.0以上のすべての音声デバイスにはプリインストールされています。
  - *AXIS Audio Manager Edge ユーザーマニュアル*
- AXIS Audio Manager Pro - 大規模システム向けの高度な音声管理ソフトウェアです。
  - *AXIS Audio Manager Pro ユーザーマニュアル*
- AXIS Audio Manager Center — マルチサイトシステムのリモートアクセスと管理のためのクラウドサービスです。
  - *AXIS Audio Manager Center ユーザーマニュアル*

詳細については、*音声管理ソフトウェア*を参照してください。

インストール

使用に当たって

ネットワーク上のデバイスを検索する

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

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

ブラウザーサポート

以下のブラウザーでデバイスを使用できます。

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

✓: 推奨:

*: 制限付きでサポート

装置のwebインターフェースを開く

1. ブラウザーを開き、Axis装置のIPアドレスまたはホスト名を入力します。
   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、ネットワーク上のデバイスを見つけます。
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。*管理者アカウントを作成する, on page 4*を参照してください。

AXIS OS搭載デバイスのWebインターフェースのすべての機能および設定に関する説明は、*AXIS OS Webインターフェースのヘルプ*を参照してください。

管理者アカウントを作成する

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

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

重要

装置にはデフォルトのアカウントはありません。管理者アカウントのパスワードを紛失した場合は、装置をリセットする必要があります。*工場出荷時の設定にリセットする, on page 18*を参照してください。

安全なパスワード

重要

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

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

データを保護するために、次のことが強く推奨されています。

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

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する, on page 18*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。

デバイスを構成する

このセクションでは、ハードウェアのインストールが完了した後に製品を起動して実行するために、設置者が行う必要のあるすべての重要な設定について説明しています。

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

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。

入力信号でいたずらを検知する

この例では、入力信号が切断された場合やショートした場合に電子メールを送信する方法について説明します。I/Oコネクターの詳細については、*page 14*を参照してください。

1. System (システム) > Accessories (アクセサリー)> I/O ports（I/Oポート） に移動し、該当するポートで Supervised (状態監視)をオンにします。

メール送信先を追加する:

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

ルールの作成:

1. [System > Events > Rules (システム > イベント > ルール)] に移動し、ルールを追加します。
2. ルールの名前を入力します。
3. [I/O (入力/出力)] の条件のリストで、[Supervised input tampering is active (いたずら状態監視を有効化する)] を選択します。
4. 該当するポートを選択します。
5. [Notifications (通知)] のアクションのリストで、[Send notification to email (電子メールに通知を送る)] を選択し、リストから送信先を選択します。
6. 電子メールの件名とメッセージを入力します。

7. [保存] をクリックします。

窓を開けたときにランプを点灯させる

この例では、窓のコンタクトを接続ハブに接続する方法と、接続された窓が開いたときにランプを点灯させるイベントを設定する方法について説明します。

要件

- 2ワイヤーケーブル (アース、I/O) を窓のコンタクトと接続ハブのI/Oコネクターに接続します。
- ランプを電源に接続し、接続ハブのリレーコネクターに接続します。

接続ハブのI/Oポートの設定

1. [System > Accessories (システム > アクセサリー)] に移動します。
2. 以下の情報を [Port 1 (ポート1)] に入力します。
   - 名前:窓センサー
   - Direction (方向): 入力
   - 標準の状態: 閉路
3. 以下の情報を [Port 2 (ポート 2)] に入力します。
   - 名前:ランプ
   - Direction (方向): 出力
   - 標準の状態: 開路

接続ハブに2つのルールを作成する

1. [System > Events (システム > イベント)] に移動し、ルールを追加します。
2. 以下の情報を入力します。
   - 名前:窓センサー
   - Condition (条件): デジタル入力
     [Use this condition as a trigger (この条件をトリガーとして使用する)] を選択します。
   - ポート: 窓センサー
   - Action (アクション): ルールがアクティブである間、I/Oを切り替える
   - ポート: ランプ
   - State (状態): アクティブ
3. [保存] をクリックします。

カメラが動きを検知したときにMQTTを介して接続ハブを起動する

要件

- 接続ハブでI/Oポート1の装置を設定します。
- 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。
- カメラで AXIS Motion Guardを設定します。

カメラでMQTTクライアントを設定する

1. カメラの装置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
   - 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。
   - 名前:動体を検知しました
   - Condition (条件): Applications > Motion alarm (アプリケーション > 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. [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。
   - 名前:動きなし
   - Condition (条件): Applications > Motion alarm (アプリケーション > 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. [保存] をクリックします。

接続ハブで、MQTTクライアントを設定する

1. 接続ハブの装置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)] に移動し、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): ポート1
   - Protocol (プロトコル):ブローカーが設定したプロトコル
   - ポート:ブローカーが使用するポート番号
   - 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. [保存] をクリックします。

MQTTサブスクリプション用の接続ハブにルールを作成する

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。
   - 名前:動体を検知しました
   - Condition (条件):[MQTT] > [Stateful (ステートフル)]
   - サブスクリプションフィルター: 動き
   - Payload (ペイロード):オン
   - Action (アクション): I/O > 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)
   - Port (ポート): I/O 1。
3. [保存] をクリックします。

ボタンを押したときにロックを開く

この例では、接続ハブにリレーを接続する方法と、接続ハブに接続されたボタンを誰かが押すとロックが開くイベントを設定する方法について説明します。

要件

- 2ワイヤーケーブル (COM、NO) をロックおよび接続ハブのリレーコネクターに接続します。
- 2ワイヤーケーブル (アース、I/O) をボタンと、接続ハブのI/Oコネクターに接続します。

接続ハブのI/Oポートの設定

1. [System > Accessories (システム > アクセサリー)] に移動します。
2. 以下の情報を [Port 1 (ポート1)] に入力します。
   - 名前:ボタン
   - Direction (方向): 入力
   - 標準の状態: 開路
3. 以下の情報を [Port 9 (ポート9)] に入力します。
   - 名前:ロック
   - 標準の状態: 開路

接続ハブにルールを作成する

1. [System > Events (システム > イベント)] に移動し、ルールを追加します。
2. 以下の情報を入力します。
   - 名前:ロックを開く
   - Condition (条件): [I/O] > [Digital input is active (デジタル入力がアクティブ)] [Use this condition as a trigger (この条件をトリガーとして使用する)] を選択します。
   - ポート: ボタン
   - Action (アクション): [I/O] > [Toggle I/O once (I/Oを一度切り替える)]
   - ポート: ロック
   - State (状態): アクティブ
   - Duration (継続時間): 10秒
3. [保存] をクリックします。

音声

音声をSDカードに録音する

この例では、2つのマイクからのSDカードへの録音を設定する方法を説明します。

開始する前に

- 2つのマイクを接続し、接続ハブにmicroSDカードを1枚挿入します。

1. **[Audio (音声)] > [Device settings (デバイス設定)]** に移動し、[**Input 0: IN 1 (入力0: IN 1)**] と[**Input 1: IN 2 (入力0: IN 2)**] をオンにします。
2. [**Input type (入力タイプ)**] と [**Power type (電源タイプ)**] を選択します。
3. 部屋によって音の大きさが異なることが予想される場合は、[**Automatic gain control (自動ゲインコントロール)**]をオンにします。
4. [**System > Storage > Onboard storage (システム > ストレージ > オンボードストレージ)**] に移動し、[**Retention time (保存期間)**保存期間] を設定します。
5. [**Audio > Stream (音声 > ストリーム)**] に移動し、[**Encoding (エンコーディング)**] を選択します。

注

複数のストリーム (同じソースからの録画やライブストリームなど) を実行する際にCPUの負荷を低く保つには、両方のストリームに同じエンコード方式を使用します。

6. **[Audio (音声)] > [Listen and record (視聴と録音)]** に移動し、 をクリックします。
7. をクリックします。

webインターフェース

AXIS OS搭載デバイスのWebインターフェースで利用可能なすべての機能と設定については、*AXIS OS Webインターフェースのヘルプ*に移動します。

詳細情報

分析機能とアプリ

分析機能とアプリを使用することで、Axisデバイスをより活用できます。AXIS Camera Application Platform (ACAP) は、サードパーティによるAxisデバイス向けの分析アプリケーションやその他のアプリの開発を可能にするオープンプラットフォームです。アプリとしては、デバイスにプリインストール済み、無料でダウンロード可能、またはライセンス料が必要なものがあります。

Axisの分析機能とアプリのユーザーマニュアルは、*help.axis.com*から参照できます。

AXIS Audio Analytics

AXIS Audio Analyticsは、突然の音量の増加や、インストールされたデバイス周辺の悲鳴、または叫び声など、特定のタイプの音を検知します。こうした音の検知を設定に使用し、ビデオ録画や音声メッセージの再生、セキュリティスタッフへの警告といった対応をトリガーすることができます。アプリケーションの動作について詳しくは、*AXIS Audio Analyticsユーザーマニュアル*を参照してください。

サイバーセキュリティ

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

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

Axisセキュリティ通知サービス

Axisは、Axis装置に関する脆弱性やその他のセキュリティ関連事項についての情報を提供する通知サービスを運営しています。通知を受け取るには、*axis.com/security-notification-service*で購読手続きを行うことができます。

脆弱性の管理

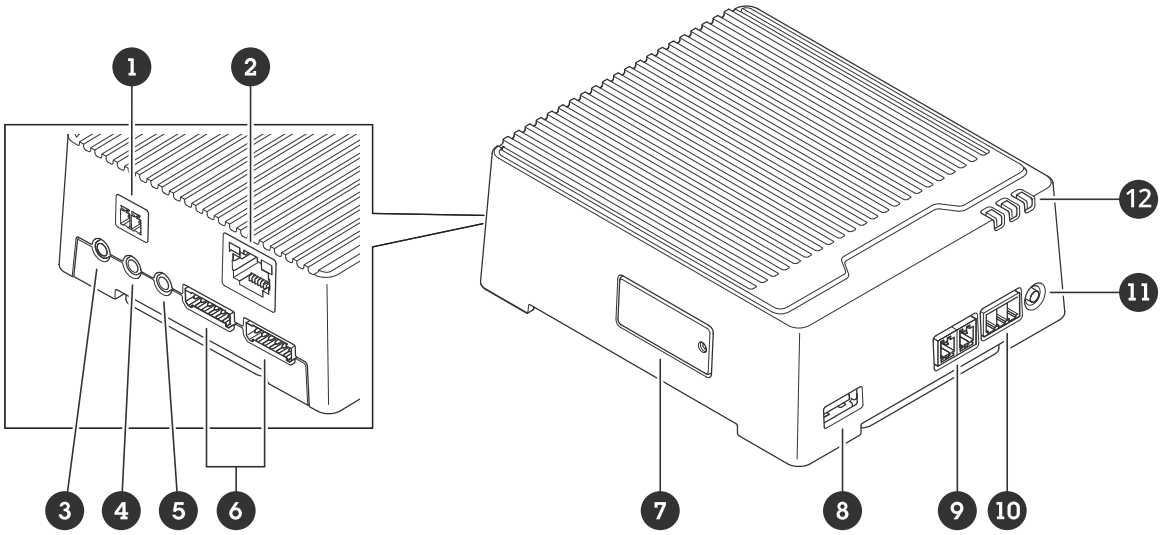
お客様の脆弱性リスクを最小限に抑えるため、Axisは**CVE (共通脆弱性識別子) 採番機関**として業界標準に従って、装置、ソフトウェア、およびサービスで発見された脆弱性の管理と対応を行っています。 Axisの脆弱性管理ポリシー、脆弱性の報告方法、すでに公開されている脆弱性、対応するセキュリティ勧告の詳細については、*axis.com/vulnerability-management*をご覧ください。

Axis装置のセキュアな動作

工場出荷時の設定のAxis装置は、セキュアなデフォルトの保護メカニズムで事前に設定されています。装置の設置時には、より多くのセキュリティ設定を使用することをお勧めします。装置のセキュリティを確保するためのベストプラクティス、リソース、ガイドラインなど、Axisのサイバーセキュリティに対する取り組みの詳細については、*axis.com/about-axis/cybersecurity*をご覧ください。

仕様

製品概要



1 電源コネクター
2 RJ45イーサネットコネクター
3 マイクポート2（アナログ）
4 マイクポート1（デジタルおよびアナログ）
5 音声出力
6 I/Oコネクター（6ピン）x2
7 microSDカードスロット
8 USBポート
9 RS485/RS422コネクター
10 リレーコネクタ
11 コントロールボタン
12 ステータスLED

SDカードスロット

推奨するSDカードについては、*axis.com*を参照してください。

microSD、microSDHC、およびmicroSDXCロゴは、SD-3C LLCの商標です。microSD、microSDHC、microSDXCは、米国および/または他の国々におけるSD-3C, LLCの商標または登録商標です。

ボタン

コントロールボタン

コントロールボタンは、以下の用途で使用します。

- 製品を工場出荷時の設定にリセットする。*工場出荷時の設定にリセットする, on page 18*を参照してください。
- インターネット経由でワンクリッククラウド接続 (O3C) サービスに接続します。接続するには、ボタンを押してから放し、ステータスLEDが緑色に3回点滅するまで待ちます。

コネクター

ネットワーク コネクター

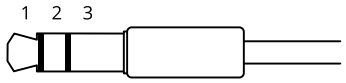
RJ45イーサネットコネクタ。

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

音声コネクター

- **音声入力** (マイクロフォンポート1) - デジタルマイクロフォン、アナログモノラルマイクロフォンまたはラインインモノラル信号用 (左チャンネルはステレオ信号で使用) 3.5 mm入力。
- **音声入力** (マイクロフォンポート2) - アナログモノラルマイクロフォンまたはラインインモノラル信号用 (左チャンネルはステレオ信号で使用) 3.5 mm入力。
- **音声出力** - 3.5 mm音声 (ラインレベル) 出力 (パブリックアドレス (PA) システムまたはアンプ内蔵アクティブスピーカーに接続可能)。一組のヘッドフォンも接続できます。音声出力には、ステレオコネクタを使用する必要があります。



音声入力

1 チップ	2 リング	3 スリーブ
アンバランス型マイクロフォン (エレクトレット電源あり、なし) またはライン入力	選択されている場合、エレクトレット電源	アース
バランス型マイクロフォン (ファントム電源あり、なし) またはライン入力、「ホット」信号	バランス型マイクロフォン (ファントム電源あり、なし) またはライン入力、「コールド」信号	アース
デジタル信号	選択されている場合、リング電源	アース

音声出力

1 チップ	2 リング	3 スリーブ
チャンネル1、アンバランス型ライン、モノラル	チャンネル1、アンバランス型ライン、モノラル	アース

I/Oコネクター

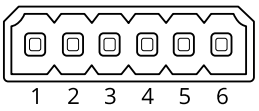
I/Oコネクターに外部装置を接続し、動体検知、イベントトリガー、アラーム通知などと組み合わせて使用することができます。I/Oコネクターは、0 VDC基準点と電力 (12 V DC出力) に加えて、以下のインターフェースを提供します。

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

状態監視入力 - デジタル入力のいたずらを検知する機能が有効になります。

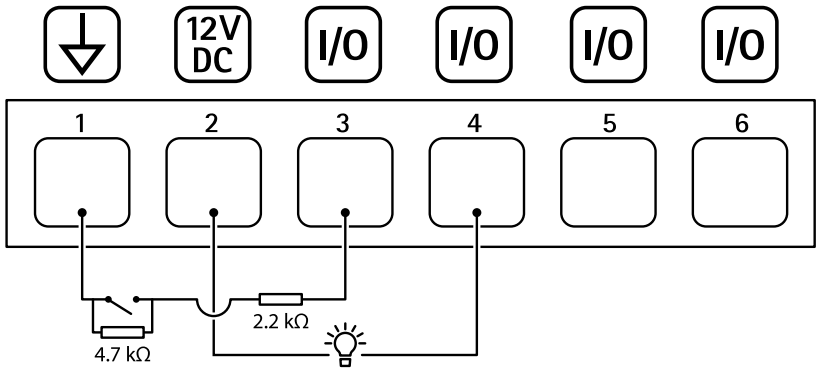
デジタル出力 - リレーやLEDなどの外部装置を接続します。接続された装置は、VAPIX®アプリケーションプログラミングインターフェースを通じたイベントまたは本装置のwebインターフェースから有効にすることができます。

6ピンターミナルブロック



機能	ピン	メモ	仕様
DCアース	1		0 VDC
DC出力	2	⚠ 補助装置の電源供給に使用できます。 注:このピンは、電源出力としてのみ使用できます。	12VDC 最大負荷 = 50 mA
設定可能 (入力または出力)	3–6	デジタル入力/状態監視 – 動作させるにはピン1に接続し、動作させない場合はフロート状態 (未接続) のままにします。状態監視を使用するには、終端抵抗器を設置します。抵抗器を接続する方法については、接続図を参照してください。	0～30 VDC (最大)
		デジタル出力 – アクティブ時はピン1 (DCアース) に内部で接続し、非アクティブ時はフロート状態 (未接続) になります。リレーなどの誘導負荷とともに使用する場合は、過渡電圧から保護するために、負荷と並列にダイオードを接続します。	0～30 VDC (最大)、オープンドレイン、100 mA

例:



1 *DCアース*
2 *DC出力12 V、最大50 mA*
3 *I/O (状態監視として設定)*
4 *I/O (出力として設定)*
5 *設定可能I/O*
6 *設定可能I/O*

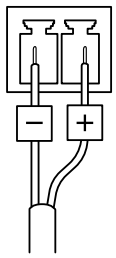
デジタルI/O向けの電気設計仕様

パラメーター	値
最小入力電圧耐久性	-30 V DC
最大入力電圧耐久性	+30 V DC
最大デジタル入力低電圧	25 ° Cで+0.50 V 85 ° Cで+0.40 V
最小デジタル入力高電圧	+1.5 V
100 mA時の最大出力低電圧	+0.6 V

10 mA時の最大出力低電圧	+0.06 V
10 kHzでの最大立ち上がり時間 (GPIOからの遅延を含む)	5 μs
10 kHzでの最大立ち下がり時間 (GPIOからの遅延を含む)	5 μs
最大出力シンク電流	100 mA
最大I/Oリーク電流	12 V DC時100 μA

電源コネクター

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

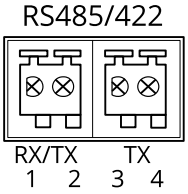


RS485/RS422コネクター

RS485/RS422シリアルインターフェース用2ピンターミナルブロック×2。

シリアルポートの設定により、次のモードをサポート可能。

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



機能	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	

装置を清掃する

装置はぬるま湯で洗浄できます。

注意

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

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

トラブルシューティング

工場出荷時の設定にリセットする

重要

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

本製品を工場出荷時の設定にリセットするには、以下の手順に従います。

1. 本製品の電源を切ります。
2. コントロールボタンを押した状態で電源を再接続します。*製品概要, on page 13*を参照してください。
3. ステータスLEDインジケーターがオレンジで点滅するまでコントロールボタンを15〜30秒間押し続けます。
4. コントロールボタンを放します。プロセスが完了すると、ステータスLEDが緑色に変わります。ネットワーク上にDHCPサーバーがない場合、装置のIPアドレスのデフォルトは次のいずれかになります。
   - **AXIS OS 12.0以降の装置:** リンクローカルアドレスサブネット（169.254.0.0/16）から取得
   - **AXIS OS 11.11以前の装置:** 192.168.0.90/24
5. インストールおよび管理ソフトウェアツールを使用して、IPアドレスの割り当て、パスワードの設定、装置へのアクセスを行います。
   *axis.com/support*のサポートページに、インストールおよび管理ソフトウェアツールが用意されています。

装置のwebインターフェースを使用して、各種パラメーターを工場出荷時の設定に戻すこともできます。[**Maintenance (メンテナンス)** > **Factory default (工場出荷時の設定)**] に移動し、[**Default (デフォルト)**] をクリックします。

AXIS OSのオプション

Axisは、アクティブトラックまたは長期サポート (LTS) トラックのどちらかに従って、装置のソフトウェアの管理を提供します。アクティブトラックでは、最新の製品機能すべてに常時アクセスできますが、LTSトラックの場合、バグフィックスやセキュリティ更新に重点を置いた定期的リリースが提供される固定プラットフォームを使用します。

最新の機能にアクセスする場合や、Axisのエンドツーエンドシステム製品を使用する場合は、アクティブトラックのAXIS OSを使用することをお勧めします。最新のアクティブトラックに対して継続的な検証が行われないサードパーティの統合を使用する場合は、LTSトラックをお勧めします。LTSにより、大きな機能的な変更や既存の統合に影響を与えることなく、サイバーセキュリティを維持することができます。Axis装置のソフトウェア戦略の詳細については、*axis.com/support/device-software*にアクセスしてください。

AXIS OSの現在のバージョンを確認する

装置の機能はAXIS OSによって決まります。問題のトラブルシューティングを行う際は、まずAXIS OSの現在のバージョンを確認することをお勧めします。最新バージョンには、特定の問題の修正が含まれていることがあります。

AXIS OSの現在のバージョンを確認するには:

1. 装置のwebインターフェース > [**Status (ステータス)**] に移動します。
2. [**Device info (デバイス情報)**] で、AXIS OSのバージョンを確認します。

AXIS OSをアップグレードする

重要

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

注

- アクティブトラックのAXIS OSの最新バージョンで装置をアップグレードすると、製品に最新機能が追加されます。アップグレードする前に、AXIS OSと共に提供されるアップグレード手順とリリースノートを必ずお読みください。AXIS OSの最新バージョンとリリースノートについては、*axis.com/support/device-software*にアクセスしてください。

1. AXIS OSのファイルをコンピューターにダウンロードします。これらのファイルは*axis.com/support/device-software*から無料で入手できます。
2. デバイスに管理者としてログインします。
3. [Maintenance (メンテナンス)] >[AXIS OS upgrade (AXIS OSのアップグレード)] に移動し、[Upgrade (アップグレード)] をクリックします。

アップグレードが完了すると、製品は自動的に再起動します。

技術的な問題と解決策

AXIS OSのアップグレード時の問題

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

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

IPアドレスの設定で問題が発生する

IPアドレスを設定できない

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

デバイスへのアクセスの問題

ブラウザからデバイスにアクセスする際、ログインできない

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

rootアカウントのパスワードを忘れた場合は、デバイスを工場出荷時の設定にリセットする必要があります。手順については、*工場出荷時の設定にリセットする, on page 18*を参照してください。

DHCPによってIPアドレスが変更された

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

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

IEEE 802.1X使用時の証明書エラー

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

ブラウザがサポートされていません

推奨ブラウザの一覧は、*ブラウザーサポート, on page 4*を参照してください。

外部からデバイスにアクセスできません

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

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

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

MQTTの問題

MQTTオーバSSLを使用してポート8883経由で接続できない

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

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

- サーバー/ブローカーが、通常はポート443経由で、WebSocket/WebSocket Secure (WS/WSS) をサポートしている場合は、代わりにこのプロトコルを使用してください。サーバー/ブローカープロバイダーに問い合わせて、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。

デバイスの動作に関する問題

フロントヒーターとワイパーが作動していない

フロントヒーターまたはワイパーがオンにならない場合は、上部カバーがハウジングユニットの底部に正しく固定されているか確認してください。

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

パフォーマンスに関する一般的な検討事項

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。
- 複数のアクティビティを同時に実行すると、音声パフォーマンスに影響する場合があります。

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。

T10208737_ja

2026-02 (M6.2)