AXIS C8110 Network Audio Bridge

ユーザーマニュアル

ソリューションの概要

本マニュアルでは、デバイスを音声システムにアクセスさせる方法と、インターフェースからデバイスを直接設定する方法について説明します。

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 Camera Station Pro - 大規模システム向けの高度なビデオ管理ソフトウェアです。
  - *AXIS Camera Station Pro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



インストールガイド (pdf) をダウンロードする:
- *axis.com/products/axis-c8110/support#support-resources*

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

デバイスへのアクセス

1. ブラウザーを開き、AxisデバイスのIPアドレスまたはホスト名を入力します。
2. ユーザー名とパスワードを入力します。初めて装置にアクセスする場合は、rootパスワードを設定する必要があります。*rootアカウントの新しいパスワードを設定する, on page 4*を参照してください。

rootアカウントの新しいパスワードを設定する

重要

デフォルトの管理者ユーザー名は**root**です。root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してください。*工場出荷時の設定にリセットする, on page 14*を参照してください



サポートのヒント:パスワードセキュリティ確認チェック

1. パスワードを入力します。安全なパスワードを設定する手順に従います。*安全なパスワード, on page 5*を参照してください。
2. パスワードを再入力して、スペルを確認します。

3. [保存] をクリックします。これでパスワードが設定されました。

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)。

追加設定

音声の検知と録音

音声を検知して録音する1つの方法は、マイクを音声ブリッジのライン入力コネクターに接続することです。屋外環境では、AXIS TU1002-VE Microphone Kitを使用できます。



AXIS TU1002-VEを使用したブリッジの設置

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かどうかを選択します。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. [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. [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、*ダイレクトSIP (P2P)を設定する, on page 6* を参照してください。

イベントのルールを設定する

特定のイベントが発生したときにデバイスにアクションを実行させるように、ルールを作成することができます。ルールは条件とアクションで構成されます。条件を使用して、アクションをトリガーすることができます。たとえば、デバイスはスケジュールに従って、または呼び出しを受信したときに音声クリップを再生したり、デバイスのIPアドレスが変更されたときに電子メールを送信したりすることができます。

詳細については、「*イベントのルールの使用開始*」を参照してください。

カメラが動きを検知したときに音声を再生する

この例では、Axisネットワークカメラが動きを検知したときにオーディオクリップを再生するための音声デバイスの設定方法について説明します。

要件

- Axis音声デバイスとAxisネットワークカメラが同じネットワーク上に配置されている。
- 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。

1. オーディオクリップのリンクを準備する:
   1.1. [Audio (音声)] > [Audio clips (音声クリップ)] に移動します。
   1.2. 音声クリップで ⋮ > [Create link (リンクの作成)]をクリックします。
   1.3. クリップの音量と繰り返し回数を設定します。
   1.4. コピーアイコンをクリックして、リンクをコピーします。
2. アクションルールの作成
   2.1. [System (システム)] > [Events (イベント)] > Recipients (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. 送信先の名前 (「Speaker」など) を入力します。
   2.4. [Type (タイプ)] ドロップダウンリストから [HTTP] を選択します。
   2.5. 音声デバイスで設定したリンクを [URL] フィールドにペーストします。
   2.6. 音声デバイスのユーザー名とパスワードを入力します。
   2.7. [保存] をクリックします。
   2.8. [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。
   2.9. アクションルールの名前 (「Play clip」など) を入力します。
   2.10. [Condition (条件)] 一覧の [Applications (アプリケーション)] で、ビデオ動体検知の代替を選択します。

注
ビデオ動体検知のオプションがない場合は、[Apps (アプリ)] に移動し、[AXIS Video Motion Detection] をクリックして、動体検知をオンにします。

   2.11. [Action (アクション)] リストから [Send notification through HTTP (HTTPで通知を送信する)] を選択します。
   2.12. [Recipient (送信先)] で送信先を選択します。
   2.13. 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. [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. [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。
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)]に移動して値を追加します。
2. ルールの名前を入力します。
3. 条件の一覧で[State (状態)]を選択します。
4. 状態の一覧で、[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)]に移動して値を追加します。
2. ルールの名前を入力します。
3. 条件の一覧で[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. 条件の一覧で[State (状態)]を選択します。

8. 状態の一覧で、[Ringing (呼び出し中)] を選択します。
9. アクションの一覧で[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。

詳細情報

セッション開始プロトコル (SIP)

セッション開始プロトコル (SIP) を使用して、VoIP呼び出しを設定、維持、および終了します。2つ以上のグループ (SIPユーザーエージェント) の間で呼び出しを行うことができます。SIP呼び出しは、SIP電話、ソフトフォン、SIP対応Axisデバイスなどを使用して行うことができます。

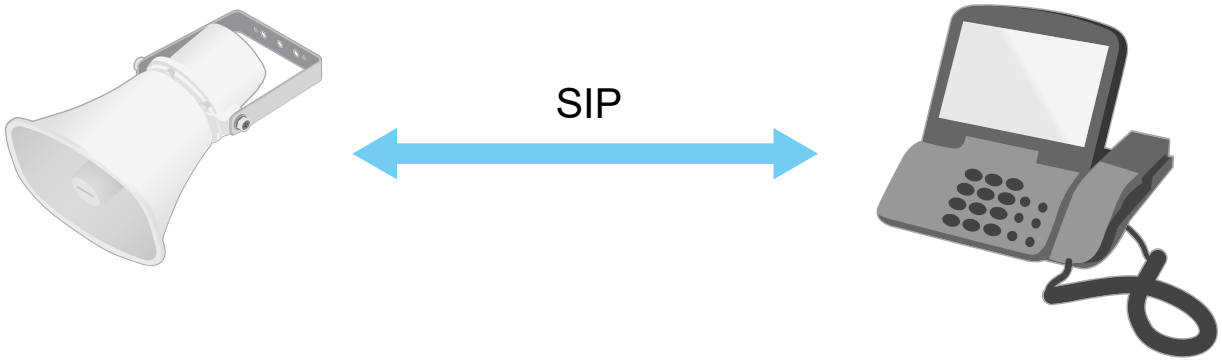
実際の音声またはビデオは、RTP (Real-time Transport Protocol) などのトランスポートプロトコルを使用して、SIPユーザーエージェントの間で交換されます。

ピアツーピア設定を使用するか、PBXを使用したネットワークを通じて、ローカルネットワークで呼び出しを行うことができます。

ピアツーピアSIP (P2PSIP)

最も基本的なタイプのSIP通信は、2つ以上のSIPユーザーエージェントの間で直接行われます。これは、ピアツーピアSIP (P2PSIP) と呼ばれます。ローカルネットワーク上で行われる場合、必要なのはユーザーエージェントのSIPアドレスだけです。この場合、通常のSIPアドレスは`sip:<local-ip>`です。

例:



ピアツーピアSIP設定を使用して、同じネットワーク上の音声デバイスを呼び出すように、SIP対応電話を設定することができます。

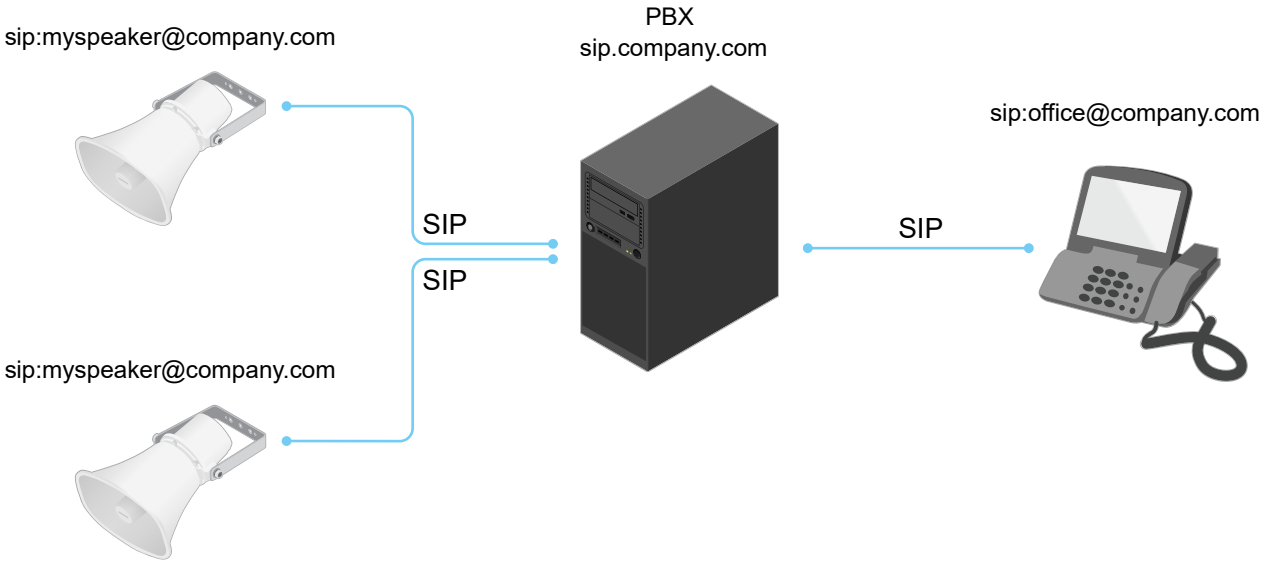
構内交換機 (PBX)

ローカルIPネットワークの外部でSIP呼び出しを行うときは、構内交換機 (PBX) をセンターハブとして機能させることができます。PBXの主要コンポーネントはSIPサーバーです。これは、SIPプロキシーまたはレジストラとも呼ばれます。PBXは従来の電話交換台のように動作します。クライアントの現在の状態を表示し、呼転送、ボイスメール、リダイレクトなどを行うことができます。

PBX SIPサーバーは、ローカルエンティティまたはオフサイトとして設定することができます。イントラネットまたはサードパーティのプロバイダーによってホストすることができます。ネットワーク間でSIP呼び出しを行うと、呼び出しは一連のPBXによって到達先のSIPアドレスの場所を照会し、ルーティングされます。

各SIPユーザーエージェントは、PBXに登録することで、正しい内線番号をダイヤすると該当のエージェントに到達できるようになります。この場合、通常のSIPアドレスは`sip:<user>@<domain>`または`sip:<user>@<registrar-ip>`です。SIPアドレスはそのIPアドレスとは無関係であり、PBXはデバイスがPBXに登録されている間は、そのデバイスをアクセス可能にします。

例:



NATトラバーサル

NAT (ネットワークアドレス変換) トラバーサルは、プライベートネットワーク (LAN) 上にあるAxisデバイスに、そのネットワークの外部からアクセスできるようにする場合に使用します。

注

ルーターが、NATトラバーサルとUPnP®に対応している必要があります。

NATトラバーサルプロトコルは個別に使用することも、ネットワーク環境に応じたさまざまな組み合わせで使用することもできます。

- ICE - ICE (双方向接続性確立) プロトコルを使用することで、ピアデバイス間の通信を成功させるために最も効率のよいパスを見つけやすくなります。STUNやTURNも有効にすると、さらにICEプロトコルで見つけやすくなります。
- STUN - STUN (NATのためのセッショントラバーサルユーティリティ) は、AxisデバイスがNATまたはファイアウォールを経由して配置されているかどうかを特定し、経由している場合に、リモートホストへの接続のために割り当てるマッピングされたパブリックIPアドレスとポート番号を取得できるようにする、クライアント/サーバーネットワークプロトコルです。IPアドレスなどのSTUNサーバーアドレスを入力します。
- TURN - TURN (NATに関するリレーを使用したトラバーサル) は、NATルーターまたはファイアウォールを経由するデバイスが、TCPやUDPを介して他のホストから着信データを受信できるようにするプロトコルです。TURNサーバーアドレスとログイン情報を入力します。

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 Client for Unified Communication Systems

このアプリケーションを使うと、SIP対応のAxisデバイスと、リンクされたMicrosoft® Teamsアカウントの間で通話できます。詳細については、*AXIS Client for Unified Communication Systemsのユーザーマニュアル*を参照してください。

webインターフェース

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

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 17*を参照してください。
3. ステータスLEDが再び黄色に変わるまで、コントロールボタンを押し続けます (10秒間)。
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、製品へのアクセスを行います。

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

AXIS OSの現在のバージョンを確認する

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

AXIS OSの現在のバージョンを確認するには:

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

AXIS OSをアップグレードする

重要

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

注

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

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

アップグレードが完了すると、製品は自動的に再起動します。

技術的な問題、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、デバイス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。デバイス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。

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

ブラウザーからデバイスにアクセスできない

ログインできない	HTTPSが有効になっているときは、ログインを試みるときに正しいプロトコル (HTTPまたはHTTPS) を使用していることを確認してください。場合によっては、ブラウザーのアドレスフィールドに手動で`http`または`https`を入力する必要があります。 rootユーザー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。*工場出荷時の設定にリセットする, on page 14*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。

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

デバイス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: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。

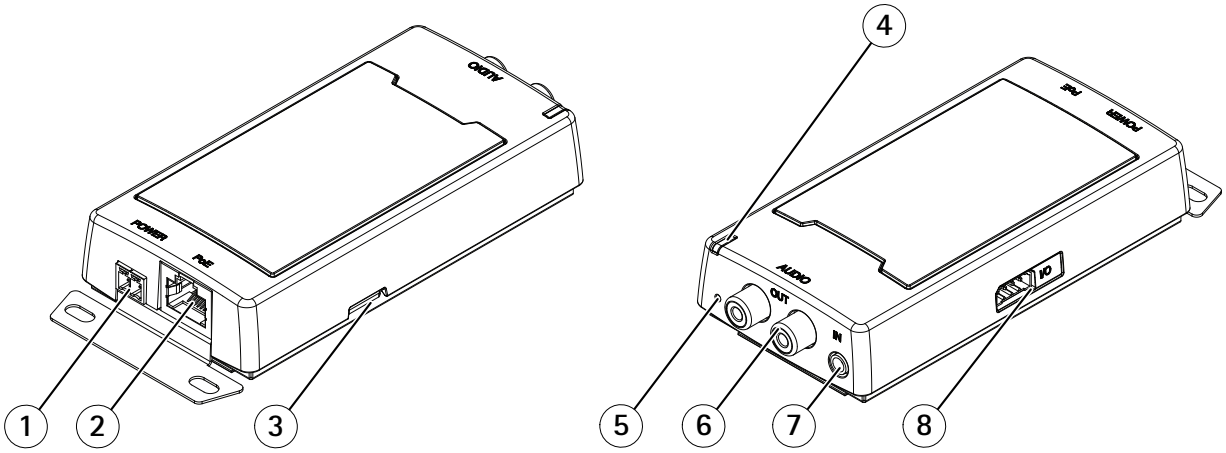
手順とダウンロードについては、*axis.com/vms*にアクセスしてください。

サウンドファイルの問題

メディアクリップをアップロードできません	以下の音声クリップがサポートされています。 • auファイル形式: µ-lawでエンコードされ、8または16 kHzでサンプリングされます。 • wavファイル形式: PCM音声でエンコードされます。8または16ビットのモノラルまたはステレオとしてのエンコードと、8～48 kHzのサンプリングレートをサポートします。 • mp3ファイル形式: ビットレート64 kbps～320 kbpsのモノラルまたはステレオ、8～48 kHzのサンプリングレート。
メディアクリップが異なる音量で再生されます	サウンドファイルは一定のゲインで録音されます。音声クリップが異なるゲインで作成されている場合、異なる音量で再生されます。同じゲインのクリップを使用していることを確認してください。

仕様

製品概要



1 *電源コネクタ (DC)*
2 *ネットワーク コネクター*
3 *SDメモリーカードスロット*
4 *ステータスLEDインジケーター*
5 *コントロールボタン*
6 *RCAコネクタ*
7 *オーディオ入力コネクター*
8 *I/Oコネクター*

LEDインジケーター

ステータスLED	説明
緑	正常動作であれば点灯します。
オレンジ	起動時に点灯し、装置のソフトウェアのアップグレード中、または工場出荷時の設定にリセット中に点滅します。
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。
赤	アップグレードに失敗すると、ゆっくり点滅します。
赤/緑	[Locate device (装置の発見)]が選択されると速く点滅します。

SDカードスロット

注意

- SDカード損傷の危険があります。SDカードの挿入と取り外しの際には、鋭利な工具や金属性の物を使用したり、過剰な力をかけたりしないでください。カードの挿入や取り外しは指で行ってください。
- データ損失や録画データ破損の危険があります。SDカードを取り外す前に、装置のwebインターフェースからマウント解除してください。本製品の稼働中はSDカードを取り外さないでください。

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。

- スピーカーテストのキャリブレーションを行う。コントロールボタンを押して離すと、テストトーンが再生されます。
- 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 14*を参照してください。

コネクター

ネットワーク コネクター

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

注意

本製品は、シールドネットワークケーブル (STP) を使用して接続してください。本製品は、用途に合ったケーブルを使用してネットワークに接続してください。ネットワーク装置がメーカーの指示どおりに設置されていることを確認します。法的要件については、Axisのホームページ*www.axis.com*でインストールガイドを参照してください。

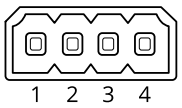
I/Oコネクター

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。

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

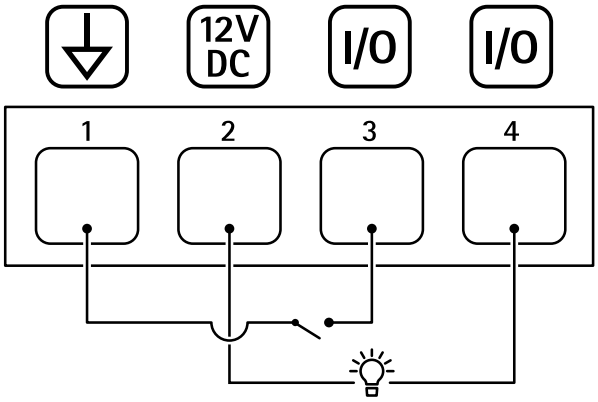
4ピンターミナルブロック



機能	ピン	メモ	仕様
DCアース	1		0 VDC
DC出力	2	⚠ 補助装置の電源供給に使用できます。 注:このピンは、電源出力としてのみ使用できます。	12VDC 最大負荷 = 50 mA
設定可能 (入力または出力)	3–4	デジタル入力 – 動作させるにはピン1に接続し、動作させない場合はフロート状態 (未接続) のままにします。	0～最大30 VDC

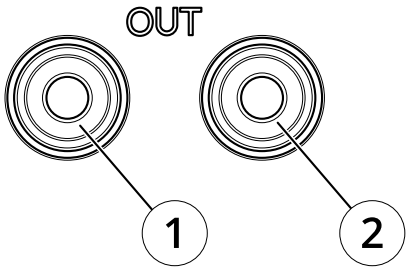
		デジタル出力 – アクティブ時はピン1 (DCアース) に内部で接続し、非アクティブ時はフロート状態 (未接続) になります。リレーなどの誘導負荷とともに使用する場合は、過渡電圧から保護するために、負荷と並列にダイオードを接続します。	0〜30 VDC (最大)、オープンドレイン、100 mA

例:



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

RCAコネクタ



	白コネクタ (×1)	赤コネクター (×2)
音声出力	音声出力 (左)	音声出力 (右)

APIコマンド

VAPIX®はAxis独自のオープンAPI (アプリケーションプログラミングインターフェース) です。VAPIX®を使用することにより、Axisデバイスで使用できるほぼすべての機能を制御することができます。VAPIX®の完全なドキュメントにアクセスするには、*axis.com/developer-community*にあるAxis開発者コミュニティに参加してください

Webブラウザーにコマンドを入力し、<deviceIP>をデバイスのIPアドレスまたはホスト名と置き換えます。

重要

APIコマンドはすぐに実行されます。デバイスをリストアまたはリセットすると、すべての設定が失われます。たとえば、アクションルールなどです。

例: Request
デバイスを再起動
Request
`http://<deviceIP>/axis-cgi/restart.cgi`

例: Request
デバイス をリストアします。このリクエストは、ほとんどの設定をデフォルト値に戻しますが、IPアドレスは保持します。
Request
`http://<deviceIP>/axis-cgi/factorydefault.cgi`

例: Request
デバイスをリセットします。このリクエストは、IPアドレスを含むすべての設定をデフォルト値に戻します。
Request
`http://<deviceIP>/axis-cgi/hardfactorydefault.cgi`

例: Request
すべてのデバイスパラメーターのリストを表示します。
Request
`http://<deviceIP>/axis-cgi/param.cgi?action=list`

例: Request
デバッグアーカイブを取得します
Request
`http://<deviceIP>/axis-cgi/debug/debug.tgz`

例: Request
サーバーレポートを取得します
Request
`http://<deviceIP>/axis-cgi/serverreport.cgi`

例: Request
300秒のネットワークトレースをキャプチャします
Request
`http://<deviceIP>/axis-cgi/debug/debug.tgz?cmd=pcapdump&duration=300`

例: Request
FTPを有効にします
Request
`http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.FTP.Enabled=yes`

例: Request
FTPを無効にします
Request
`http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.FTP.Enabled=no`

例: Request
SSHを有効にします
Request
`http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.SSH.Enabled=yes`

例: Request
SSHを無効にします
Request

```
http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.SSH.Enabled=no
```

サイバーセキュリティ

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

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

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

安全な製品ライフサイクル管理

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

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

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

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

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

T10176479_ja

2026-07 (M18.2)

© 2022 – 2026 Axis Communications AB