AXIS C1410 Mk II Network Mini Speaker

ユーザーマニュアル

目次

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。

ネットワーク音声の動作の概要。

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 6*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 7*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 23*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 23*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。

webインターフェースの概要

このビデオでは、装置のwebインターフェースの概要について説明します。

Axis装置のwebインターフェース

デバイスを構成する

リモートスピーカーテストのキャリブレーションを行い、テストを実行する

スピーカーテストを実行することで、スピーカーが意図したとおりに動作しているかどうかを遠隔で確認することができます。スピーカーテストでは、内蔵マイクロフォンによって登録されている一連のテストトーンを再生します。テストを実行するたびに、登録されている値が、キャリブレーション中に登録された値と比較されます。

注

テストは設置された場所の設置箇所からキャリブレーションする必要があります。壁の建設や撤去などによって、スピーカーの移動や地域環境の変化が発生した場合は、スピーカーのキャリブレーションをやり直す必要があります

キャリブレーション中は、担当者がインストール拠点に実際に出向いてテストトーンを聞き、スピーカーの音響経路にある予期しない障害物によってテストトーンの音が小さくなったり、遮断されたりしていないことを確認することをお勧めします。

1. [device interface > **Audio > Speaker test** (デバイスインターフェース > 音声 > スピーカーテスト)] に移動します。
2. 音声デバイスのキャリブレーションを行うには、[**Calibrate (キャリブレーション)**] をクリックします。

注

Axis製品のキャリブレーションが終了すると、いつでもスピーカーテストを実行できます:

3. スピーカーテストを実行するには、[**Test (テスト)**] をクリックします。

注

また、物理デバイスのコントロールボタンを押してキャリブレーションを実行することもできます。コントロールボタンを特定するには、*製品概要, on page 19*を参照してください。

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。P2Pの仕組みをよりよく理解するには、*ピアツーピアSIP (P2PSIP), on page 15* を参照してください 。

設定オプションの詳細については、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, on page 16*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。P2Pの仕組みをよりよく理解するには、*構内交換機 (PBX), on page 15* を参照してください 。

設定オプションの詳細については、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 8* 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。

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. [**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. [**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。

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。

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

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。

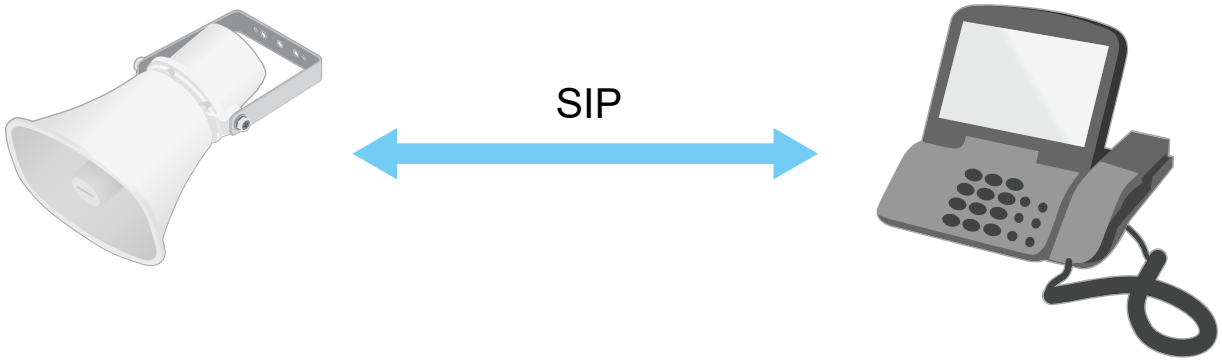
実際の音声またはビデオは、RTP (Real-time Transport Protocol) などのトランスポートプロトコルを使用して、SIPユーザーエージェントの間で交換されます。

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。

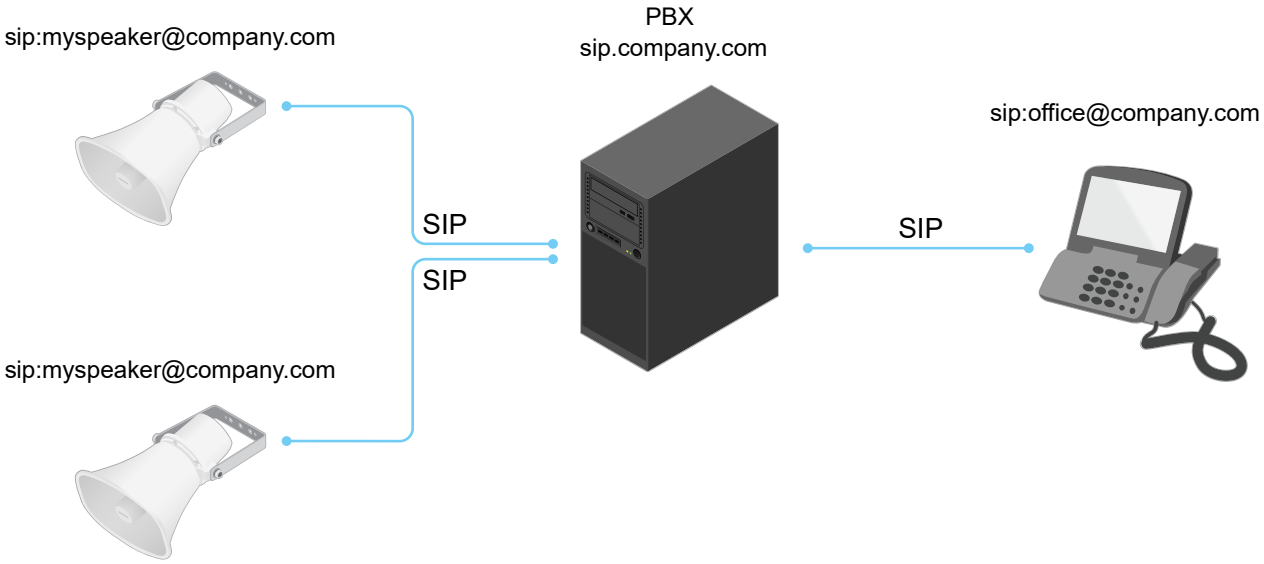
構内交換機 (PBX)

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 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。

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。

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 Edge Vault

ハードウェアベースのサイバーセキュリティプラットフォーム「Axis Edge Vault」により、Axisデバイスを保護することができます。装置のIDと整合性を保証し、不正アクセスから機密情報を保護する機能を提供します。これは、エッジデバイスセキュリティに関する専門知識を駆使して、暗号コンピューティングモジュール（セキュアエレメントやTPM）とSoCセキュリティ（TEEやセキュアブート）に基づき構築された強力な基盤により成り立っています。

署名付きOS

署名付きOSは、ソフトウェアベンダーがAXIS OSイメージを秘密鍵で署名することで実装されます。オペレーティングシステムに署名が付けられると、装置はインストール前にソフトウェアを検証するようになります。装置でソフトウェアの整合性が損なわれていることが検出された場合、AXIS OSのアップグレードは拒否されます。

セキュアブート

セキュアブートは、暗号化検証されたソフトウェアの連続したチェーンで構成される起動プロセスで、不変メモリ (ブートROM) から始まります。署名付きOSの使用に基づいているため、セキュアブートを使うと、装置は認証済みのソフトウェアを使用した場合のみ起動できます。

安全なキーストア

秘密鍵の保護と暗号化動作のセキュアな実行のための改ざん防止環境です。これにより、セキュリティ侵害が発生した場合も、不正アクセスや悪質な抽出を防止することができます。セキュリティ要件に応じて、Axisデバイスには、ハードウェアで保護された安全なキーストアが可能となるハードウェアベースの暗号コンピューティングモジュールを1つまたは複数搭載することができます。セキュリティ要件に応じて、Axis装置は、TPM 2.0 (Trusted Platform Module) やセキュアエレメント、および/またはTEE (Trusted Execution Environment) などのハードウェアベースの暗号コンピューティングモジュールを1台以上持つことができ、ハードウェアで保護されたセキュリティキーストアを提供します。さらに、一部のAxis製品には、FIPS 140-2 Level 2認定のセキュアキーストアを備えています。

AxisデバイスID

デバイスIDの信頼性を確立するには、デバイスの出所を確認できることが鍵となります。Axis Edge Vaultを搭載したデバイスには、生産工程で、工場でプロビジョニングされ、国際規格（IEEE 802.1AR）に準拠した一意のAxisデバイスID証明書が割り当てられます。これがデバイスの出所を証明するパスポートのような役割を果たします。デバイスIDは、Axisルート証明書により署名された証明要素として、セキュリティで保護されたキーストアに安全かつ永続的に格納されます。お客様のITインフラストラクチャーでデバイスIDを活用し、装置のセキュアな自動化オンボーディングや、装置のセキュアな識別に役立てることができます。

EFS（暗号化ファイルシステム）

安全なキーストアにより、ファイルシステムに強力な暗号化を適用することで、悪質な情報の抽出や設定の改ざんを防止することができます。これにより、装置が使用されていないときや、装置への認証されていないアクセスが行われたとき、Axis装置が盗難されたときに、ファイルシステムに保存されているデータが抽出されたり改ざんされたりすることがなくなります。セキュアブートプロセス中、読み書き可能なファイルシステムは復号化され、Axis装置でマウントして使用できるようになります。

Axis装置のサイバーセキュリティ機能の詳細については、*axis.com/learning/white-papers*にアクセスし、サイバーセキュリティを検索してください。

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

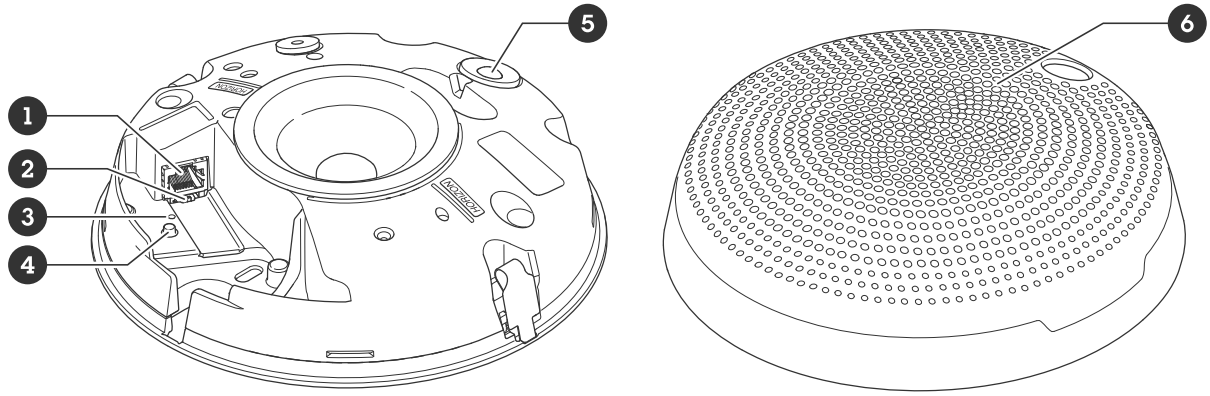
お客様の脆弱性リスクを最小限に抑えるため、Axisは**CVE (共通脆弱性識別子) 採番機関**として業界標準に従って、装置、ソフトウェア、およびサービスで発見された脆弱性の管理と対応を行っています。 Axisの脆弱性管理ポリシー、脆弱性の報告方法、すでに公開されている脆弱性、対応するセキュリティ勧告の詳細については、*axis.com/vulnerability-management*をご覧ください。

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 ネットワーク コネクター
2 マイクスイッチ
3 ステータスLEDインジケーター
4 コントロールボタン
5 PIRセンサーと前面LED
6 カバー

LEDインジケーター

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。
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。

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 23*を参照してください。

マイクロフォンを無効にするスイッチ

マイクロフォンを無効にするスイッチの場所については、*製品概要, on page 19*を参照してください。

マイクロフォンを無効にするスイッチを使用すると、マイクロフォンを機械的に**オン**または**オフ**にできます。工場出荷時の設定では、このスイッチは**オン**になっています。

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

本装置は、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。本装置は、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。

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
```

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 19*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 23*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 6*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。

音声ファイルの問題

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。

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

システムを設定する際には、さまざまな設定や条件が必要な帯域幅 (ビットレート) にどのように影響するかを検討することが重要です。

考慮すべき最も重要な要因:

- 貧弱なインフラによるネットワークの使用率が高いと帯域幅に影響します。
- 複数のAXIS Camera Application Platform (ACAP) アプリケーションを同時に実行すると、全般的な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。

T10208067_ja

2026-02 (M11.2)