

AXIS D4200-VE Network Strobe Speaker

目次

ソリューションの概要	4
インストール	5
使用に当たって	6
ネットワーク上のデバイスを検索する	6
ブラウザーサポート	6
装置のwebインターフェースを開く	6
管理者アカウントを作成する	6
安全なパスワード	7
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	7
デバイス構成	8
プロファイルの設定	8
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	8
プロファイルのインポートまたはエクスポート	8
ダイレクトSIP (P2P) を設定する	9
サーバーを介してSIPを設定する (PBX)	9
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	10
イベントのルールを設定する	10
アクションをトリガーする	11
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	11
SIPを介したプロファイルの開始	11
SIP内線番号による複数のプロファイルの制御	12
優先度が異なる2つのプロファイルを実行する	13
カメラが動きを検知したときにHTTP POSTを使用してストロボスピーカーをアクティブにする	13
カメラが動きを検知したときに仮想入力を使用してストロボスピーカーをアクティブにする	14
カメラが動きを検知したときにMQTTを介してストロボスピーカーを作動させる	16
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	17
アラームトリガー時にカスタムクリップを再生する	19
DTMFで音声を停止する	19
着信SIP呼び出しの音声の設定	20
webインターフェース	22
詳細情報	23
セッション開始プロトコル (SIP)	23
ピアツーピアSIP (P2PSIP)	23
構内交換機 (PBX)	23
NATトラバーサル	24
分析機能とアプリ	24
AXIS Audio Analytics	24
InformaCast®	25
仕様	26
製品概要	26
LEDインジケーター	27
SDカードスロット	28
ボタン	28
コントロールボタン	28
マイクスイッチ	28
コネクタ	28
ネットワーク コネクタ	28
音声コネクタ	28
I/Oコネクタ	29

ライトパターン名	30
サウンドパターン名	31
装置を清掃する	32
トラブルシューティング	33
工場出荷時の設定にリセットする	33
AXIS OSのオプション	33
AXIS OSの現在のバージョンを確認する	33
AXIS OSをアップグレードする	33
技術的な問題と解決策	34
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

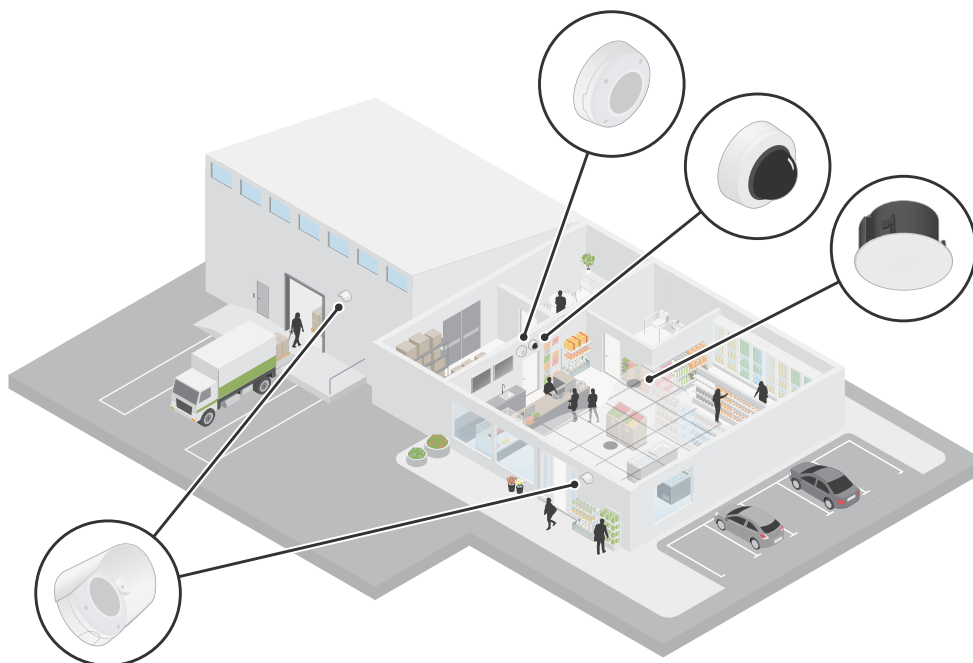
ソリューションの概要

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

重要

線路の中心から3m以内にストロボスピーカーや接続したデバイスを設置しないでください。
このビデオは、AXIS D4200-VE Network Strobe Speakerの設置方法の一例です。



このビデオを見るには、このドキュメントのWebバージョンにアクセスしてください。

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。
この装置のIPアドレスが不明な場合は、AXIS IP UtilityまたはAXIS Device Managerを使用して、ネットワーク上でこの装置を見つけてください。
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インターフェースでの全機能と設定に関する説明については、*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 33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 33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

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。これよりサイズが大きい音声ファイルは、デバイスにSDカードスロットが付いている場合は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. [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 8](#) 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. [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 (経路のリライトを許可)** - 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 9を参照してください。

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 26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。

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。

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)] > [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. **[profile you want to start (開始するプロファイル)]** を選択します。
7. **[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. **[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. **[profile you want to start (開始するプロファイル)]** を選択します。
7. **[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. **[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. **[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. **[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. [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. [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したときにHTTP POSTを使用してストロボスピーカーをアクティブにする

この例では、ストロボスピーカ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が動きを検知した場合にストロボスピーカーのプロファイルをアクティブにする方法について説明します。

開始する前に、以下をご確認ください。

- ストロボスピーカーにオペレーター、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。
- ストロボスピーカーに、「ストロボスピーカープロファイル」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。
- 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。
 - 名前: ストロボスピーカー
 - Type (タイプ): HTTP
 - URL: http://<IPaddress>/axis-cgi/siren_and_light.cgi

<IPAddress>の部分をストロボスピーカーのアドレスに置き換えます。

- 新しく作成されたストロボスピーカーのユーザーのユーザー名とパスワード。

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. [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。

- 名前:動きのある場合にストロボスピーカーをアクティブにする
- Condition (条件): [Applications (アプリケーション)] > [Motion Guard: Camera profile (Motion Guard: カメラプロファイル)]
- Action (アクション): Notifications > Send notification through HTTP (通知 > HTTPで通知を送信する)
- Recipient (送信先):ストロボスピーカー。
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 (メソッド): Post
- Body (本文):

```
{ "apiVersion": "1.0", "method": "start", "params": {  
  "profile": "Strobe speaker profile" } }
```

ここでは、ストロボスピーカーでプロファイルを作成したときに入力した情報と同じ情報を [“profile” (プロファイル): <>] に入力してください。この場合は、「Strobe speaker profile (ストロボスピーカープロファイル)」です。

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:動きのある場合にストロボスピーカーを非アクティブにする
- Condition (条件): [Applications (アプリケーション)] > [Motion Guard: Camera profile (Motion Guard: 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 > Send notification through HTTP (通知 > HTTPで通知を送信する)
- Recipient (送信先): ストロボスピーカー
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 (メソッド): Post
- Body (本文):

```
{ "apiVersion": "1.0", "method": "stop", "params": { "profile": "Strobe speaker  
profile" } }
```

ここでは、ストロボスピーカーでプロファイルを作成したときに入力した情報と同じ情報を [“profile” (プロファイル): <>] に入力してください。この場合は、「Strobe speaker profile (ストロボスピーカープロファイル)」です。

5. [保存] をクリックします。

カメラが動きを検知したときに仮想入力を使用してストロボスピーカーをアクティブにする

この例では、ストロボスピーカ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が動きを検知した場合にストロボスピーカーのプロファイルをアクティブにする方法について説明します。

開始する前に、以下をご確認ください。

- ストロボスピーカーでオペレーター、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。
- ストロボスピーカーにプロファイルを作成します。
- 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。
 - 名前: Activate virtual port (仮想ポートのアクティブ化)
 - Type (タイプ): HTTP
 - URL: http://<IPAddress>/axis-cgi/virtualinput/activate.cgi
<IPAddress>の部分をストックボスピーカーのアドレスに置き換えます。
 - 新しく作成されたストロボスピーカーアカウントのユーザーのアカウントとパスワード。
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. **[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。
 - 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
<IPAddress>の部分をストックボスピーカーのアドレスに置き換えます。
 - 新しく作成されたストロボスピーカーアカウントのユーザーのアカウントとパスワード。
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. **[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。
 - 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 (Motion Guard: カメラプロファイル)]**
 - Action (アクション): **Notifications > Send notification through HTTP (通知 > HTTPで通知を送信する)**
 - Recipient (送信先): **Activate virtual port (仮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. **[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: 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 (Motion Guard: 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 > Send notification through HTTP (通知 > HTTPで通知を送信する)**
 - Recipient (送信先): **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. [保存] をクリックします。

ストロボスピーカーにルールを作成する:

1. ストロボスピーカーの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。
 - 名前: 仮想入力1のトリガー
 - Condition (条件): [I/O] > [Virtual input (仮想入力)]:
 - ポート: 1
 - Action (アクション): Light and siren > Run light and siren profile while the rule is active (ライトとサイレン > 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する
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を介してストロボスピーカーを作動させる

この例では、カメラをMQTT経由でストロボスピーカーに接続し、カメラが動きを検知するたびにストロボスピーカーのプロファイルをアクティブにする方法を説明します。

開始する前に、以下をご確認ください。

- ストロボスピーカーに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
 - 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。

カメラにMQTTパブリッシングの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。

ストロボスピーカーにMQTTクライアントを設定する:

1. ストロボスピーカーの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):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
 - 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。

ストロボスピーカーにMQTTサブスクリプション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):[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): Light and siren > Run light and siren profile while the rule is active (ライトとサイレン > 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. [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. [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。

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. [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. [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)]>[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. [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間で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ウェブインターフェースのヘルプ*を参照してください。

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。

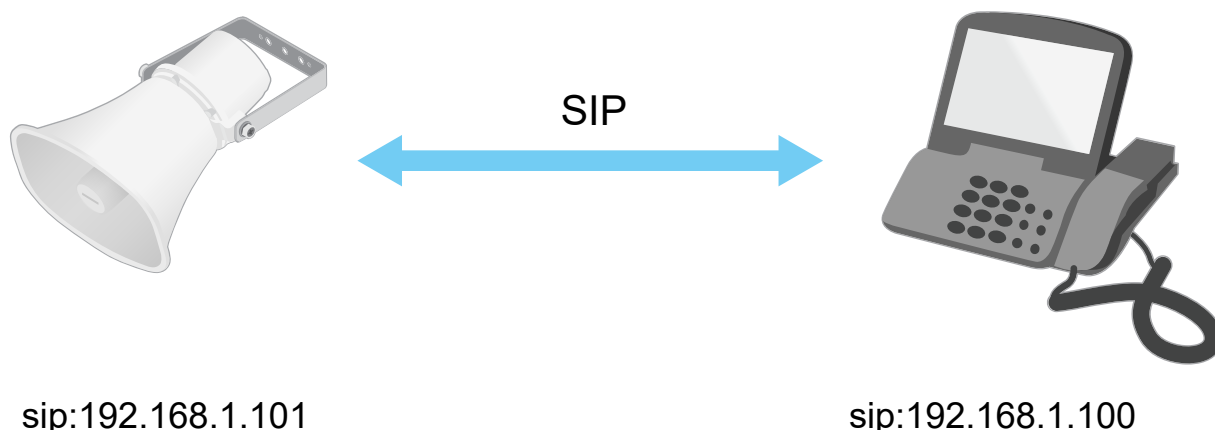
実際の音声またはビデオは、RTP (Real-time Transport Protocol) などのトランスポートプロトコルを使用して、SIPユーザーエージェントの間で交換されます。

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。

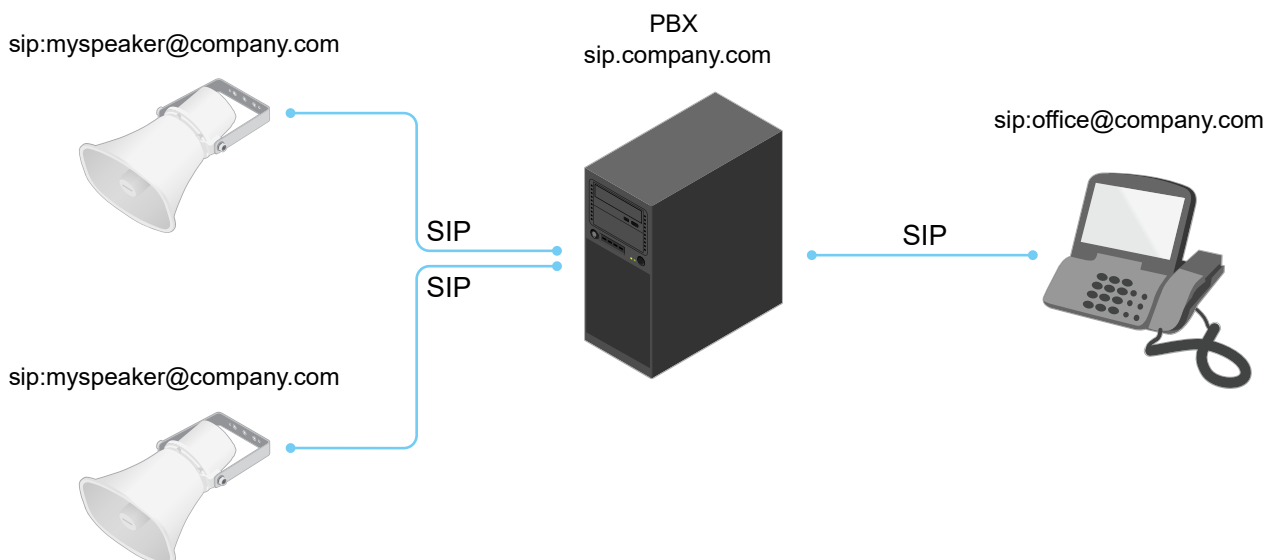
構内交換機 (PBX)

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トラバース

NAT (ネットワークアドレス変換) トラバースは、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トラバースとUPnP®に対応している必要があります。

NATトラバース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スユーティリティ) 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ス) 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

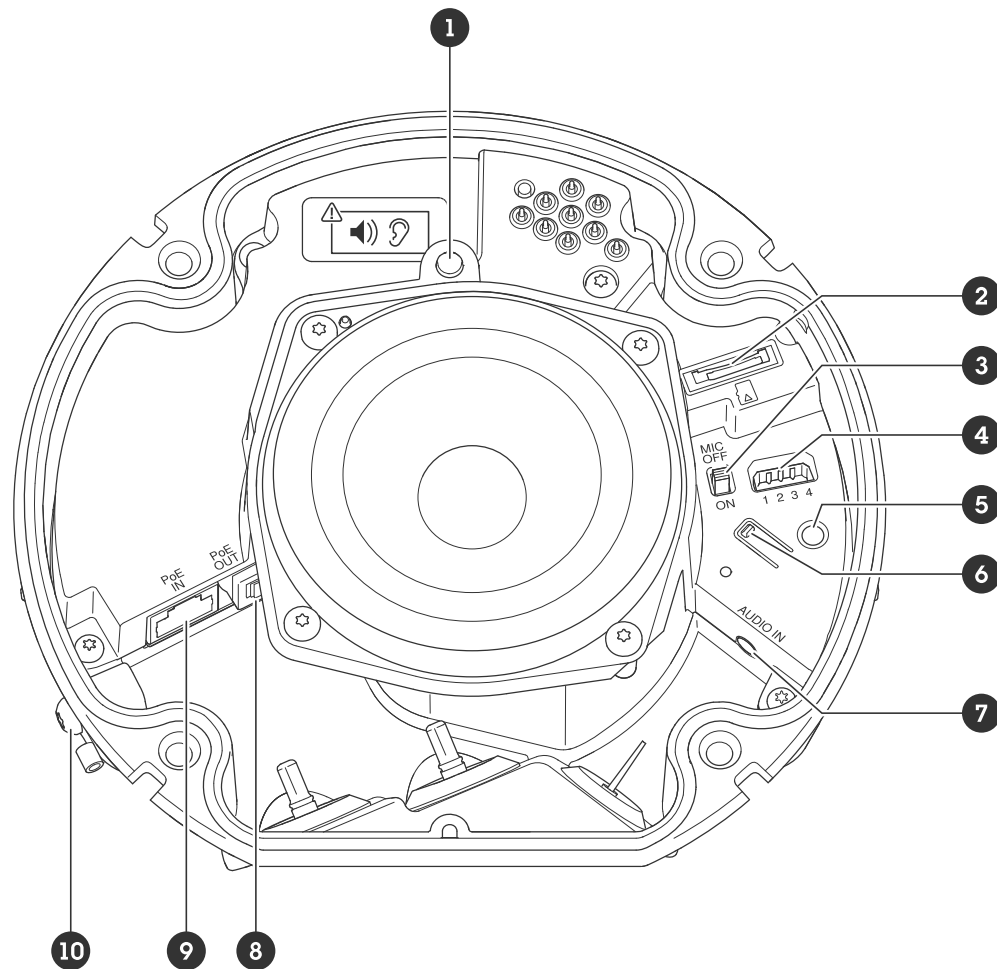
AXIS Audio Analyticsは、突然の音量の増加や、インストールされたデバイス周辺の悲鳴、または叫び声など、特定のタイプの音を検知します。こうした音の検知を設定に使用し、ビデオ録画や音声メッセージの再生、セキュリティスタッフへの警告といった対応をトリガーすることができます。アプリケーションの動作について詳しくは、AXIS Audio Analyticsユーザーマニュアルを参照してください。

InformaCast®

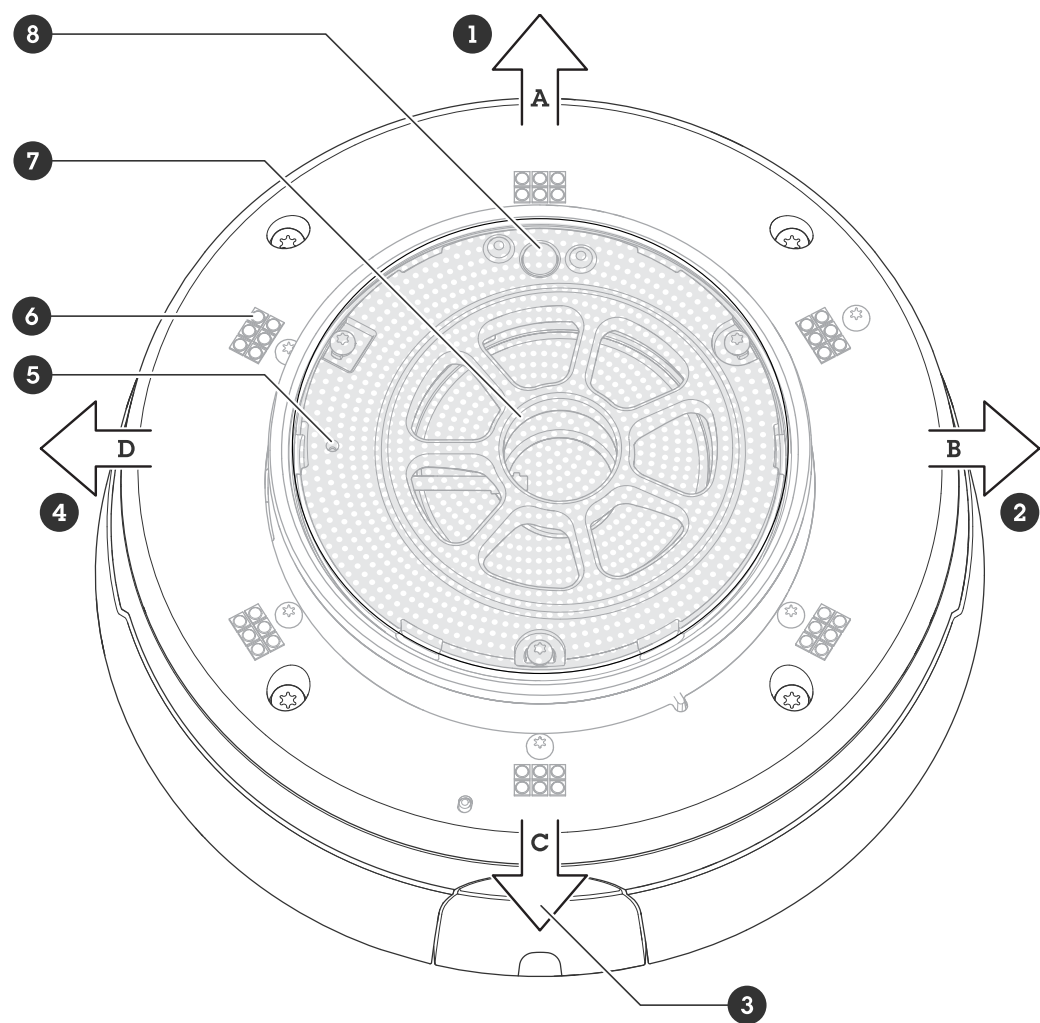
InformaCast は、Axis ネットワーク スピーカー など、組織がすでに備えている通信チャンネルを通じて、緊急メッセージを送信したり、通信を行ったりできるプラットフォームです。InformaCast 一斉通知システムは、施設全体に警戒を呼び掛ける音声アラートを配信します。このアプリケーションの詳細については、*AXIS Speaker Functionality for Singlewire InformaCast* (シングルワイヤー InformaCast 向けの AXIS スピーカーの機能) を参照してください。

仕様

製品概要



- 1 音声LED
- 2 microSDカードスロット
- 3 マイクスイッチ
- 4 I/Oコネクタ
- 5 ステータスLEDインジケータ
- 6 コントロールボタン
- 7 音声コネクタ
- 8 ネットワークコネクタ (PoE出力)
- 9 ネットワークコネクタ (PoE入力)
- 10 アース端子ネジ



- 1 ライトの向きA
- 2 ライトの向きB
- 3 ライトの向きC
- 4 ライトの向きD
- 5 内蔵マイク
- 6 シグナリングLED
- 7 スピーカー
- 8 音声LED

LEDインジケータ

ステータスLED	説明
消灯	接続時および正常動作時です。
緑	起動後正常に動作する場合、10秒間、緑色に点灯します。
オレンジ	起動中または工場出荷時の設定へリセット中、設定の復元時に点灯します。

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、テスト音が再生されます。
- 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 33*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。

マイクスイッチ

マイクロフォンスイッチの場所については、製品概要, *on page 26*を参照してください。

マイクロフォン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

ネットワーク コネクター

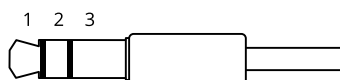
Power over Ethernet (PoE) 対応RJ45イーサネットコネクター

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。

音声コネクター

- 音声入力 - 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

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
デジタル信号	選択されている場合、リング電源	アース

注

接続ケーブルの最大長は30m (98.4フィート) です。

I/Oコネクタ

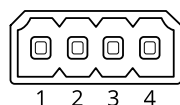
I/Oコネクタに外部装置を接続し、動体検知、イベントトリガー、アラーム通知などと組み合わせることができます。I/Oコネクタは、0 VDC基準点と電力 (12 V DC出力) に加えて、以下のインターフェースを提供します。

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。

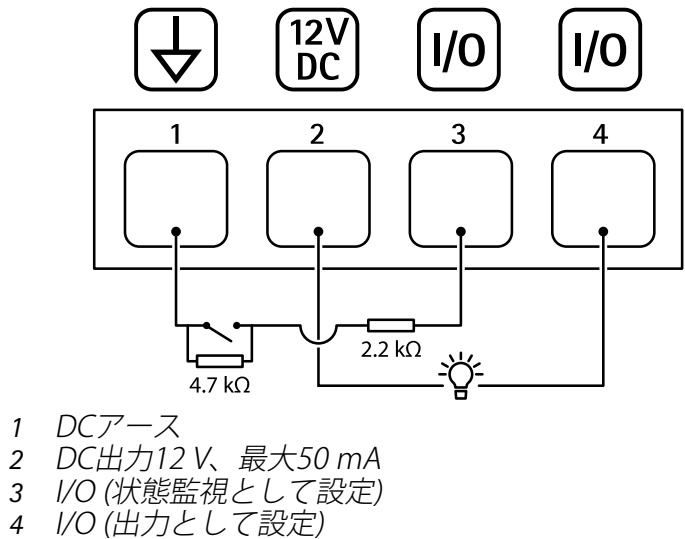
デジタル出力 - リレーやLEDなどの外部装置を接続します。接続された装置は、VAPIX®アプリケーションプログラミングインターフェースを通じたイベントまたは本装置のwebインターフェースから有効にすることができます。

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せん。	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/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:



注
 接続ケーブルの最大長は30m (98.4フィート) です。

ライトパターン名

オフ
点灯
代替
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
方向A
方向B
方向C
方向D
回転
ランダム
スピン

サウンドパターン名

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:単一ビーブ音
アラーム:ソフトクアッドビーブ音
アラーム:ソフトトリプルビーブ音
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
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

装置はぬるま湯と低刺激、非研磨性の石鹼で洗浄できます。

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、ぬるま湯と低刺激、非研磨性の石鹼で湿らせ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. 残った洗浄剤を除去するには、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拭いてください。
 4. 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。

Axisデバイスの清掃に関する詳細については、ホワイトペーパー「一般的な洗浄剤に対する耐薬品性」をご覧ください。

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 26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 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스에 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 33*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/vmsl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、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。

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。

サウンドの問題

装置の音が期待したほど大きくない	装置が正しく閉じられていること、ホーンやスピーカーエレメントに障害物がないことを確認します。
------------------	--

ライトの問題	
装置の明るさが期待ほどではない	PoE Class 4電源が使用されていることを確認します。 装置の周囲温度を確認します。装置が高温環境に設置されている場合、ライトは自動的に暗くなります。

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、一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。

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ください。

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。

T10217687_ja

2026-07 (M6.2)

© 2025 – 2026 Axis Communications AB