AXIS C8210 Network Audio Amplifier

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。

ネットワーク音声の動作の概要。

インストール

製品のインストールビデオ。

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 54*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。

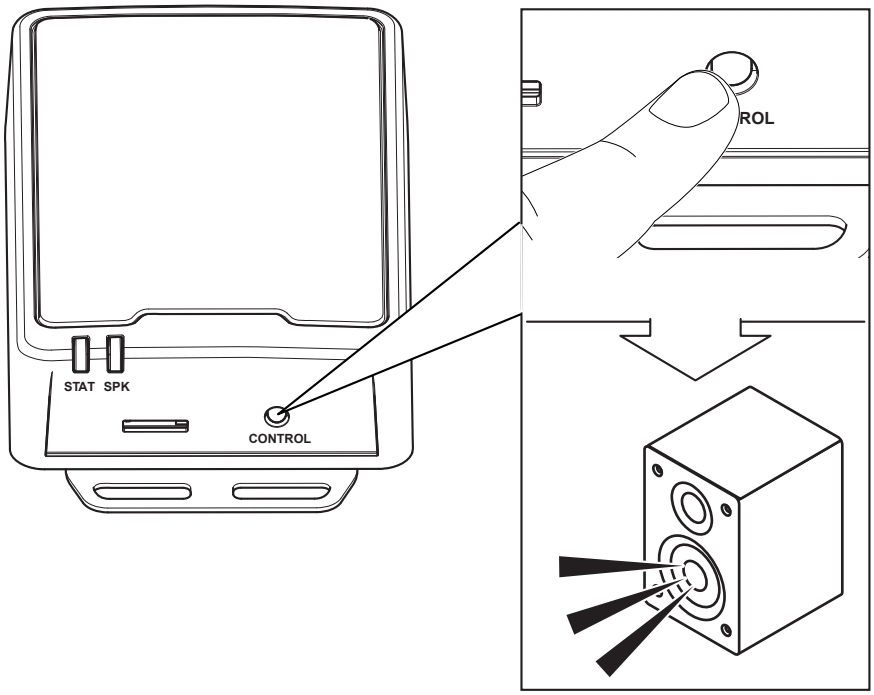
データを保護するために、次のことが強く推奨されています。

- 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

インピーダンスのテスト

スピーカーを接続した後、アンプを初めて使用する前、またはスピーカーの設定を変更した場合は、アンプに接続してインピーダンスをテストしてください。インピーダンスのテストが必要な場合はSPK LEDが緑色に点滅します。スピーカーから音が聞こえるまでコントロールボタンを押して、インピーダンステストを実行します。



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。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 11* を参照してください 。

設定オプションの詳細については、*SIP, on page 41* 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 12*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 11* を参照してください 。

設定オプションの詳細については、*SIP, on page 41* 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。

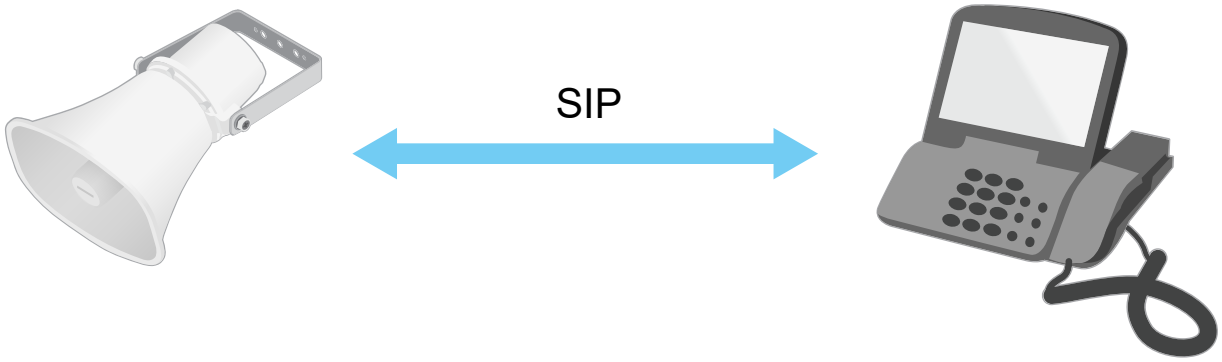
実際の音声またはビデオは、RTP (Real-time Transport Protocol) などのトランスポートプロトコルを使用して、SIPユーザーエージェントの間で交換されます。

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。

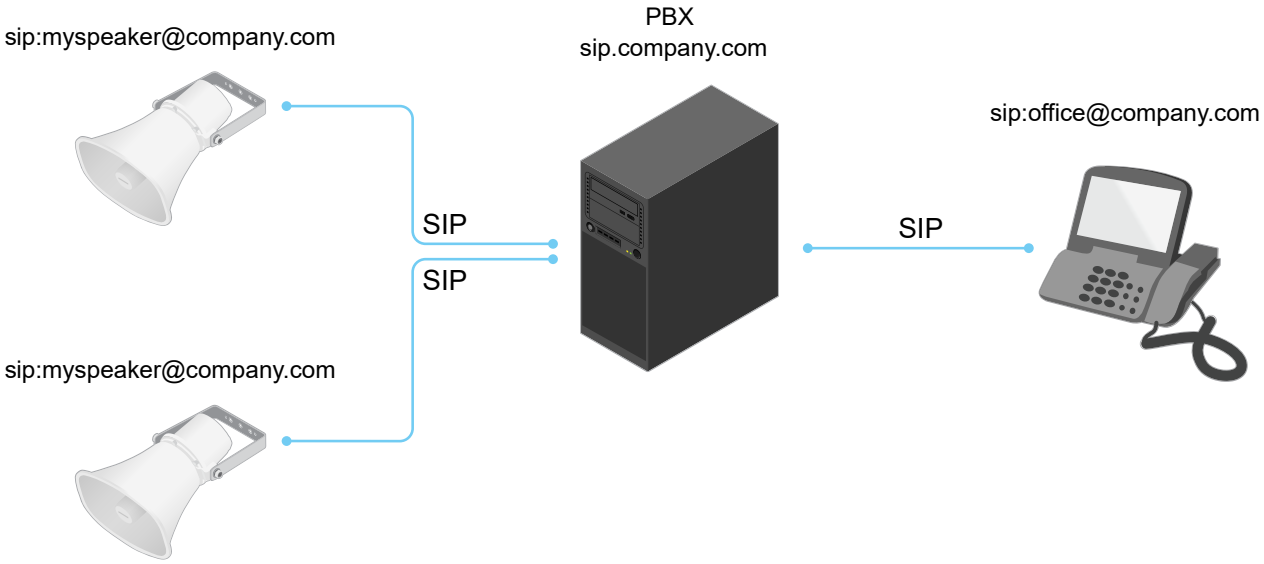
構内交換機 (PBX)

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

装置のwebインターフェースにアクセスするには、Webブラウザーで装置のIPアドレスを入力します。

メインメニューの表示/非表示を切り取ります。

リリースノートにアクセスします。

製品のヘルプにアクセスします。

言語を変更します。

ライトテーマまたはダークテーマを設定します。

ユーザーメニューは以下を含みます。

- ログインしているユーザーに関する情報。
- **アカウントの変更**:現在のアカウントからログアウトし、新しいアカウントにログインします。
- **ログアウト**:現在のアカウントからログアウトします。

コンテキストメニューは以下を含みます。

- **Analytics data (分析データ)**:個人以外のブラウザーデータの共有に同意します。
- **フィードバック**:フィードバックを共有して、ユーザーエクスペリエンスの向上に役立てます。
- **法的情報**:Cookieおよびライセンスについての情報を表示します。
- **詳細情報**:AXIS OSのバージョンやシリアル番号などの装置情報を表示します。

ステータス

音声システム情報

この情報は、AXIS Audio Manager Edgeサイトに属する装置についてのみ表示されます。

AXIS Audio Manager Edge:AXIS Audio Manager Edgeを起動します。

装置を検索

シリアル番号やIPアドレスなど装置の検索情報を表示します。

Locate device (装置を検索):発言者を特定するための音声を再生します。一部の製品では、装置のLEDが点滅します。

デバイス情報

AXIS OSのバージョンとシリアル番号を含むデバイスに関する情報を表示します。

Upgrade AXIS OS (AXIS OSのアップグレード):装置のソフトウェアをアップグレードします。アップグレードができる [Maintenance (メンテナンス)] ページに移動します。

時刻同期ステータス

装置がNTPサーバーと同期しているかどうかや、次の同期までの残り時間など、NTP同期情報を表示します。

NTP settings (NTP設定):NTP設定を表示および更新します。NTPの設定を変更できる [**Time and location (時刻と場所)**] のページに移動します。

セキュリティ

アクティブな装置へのアクセスのタイプ、使用されている暗号化プロトコル、未署名のアプリが許可されているかが表示されます。設定に関する推奨事項はAXIS OS強化ガイドに基づいています。

強化ガイド:Axis装置でのサイバーセキュリティとベストプラクティスをさらに学習できる*AXIS OS強化ガイド*へのリンクです。

接続されたクライアント

接続数と接続されているクライアントの数を表示します。

View details (詳細を表示):接続されているクライアントのリストを表示および更新します。リストには、各接続のIPアドレス、プロトコル、ポート、状態、PID/プロセスが表示されます。

進行中の録画

進行中の録画と指定されたストレージ容量を表示します。

録画: 進行中でフィルター処理された録画とそのソースを表示します。詳細については、*録画, on page 16*を参照してください

録画を保存するストレージの空き容量を表示します。

音声

AXIS Audio Manager Edge

AXIS Audio Manager Edge:アプリケーションを起動します。

音声サイトセキュリティ

CA certificate (CA証明書)：音声サイトに装置を追加するときに使用する証明書を選択します。AXIS Audio Manager EdgeでTLS認証を有効にする必要があります。

Save (保存):アクティブにして、選択内容を保存します。

デバイスの設定

入力:音声入力のオン/オフを切り替えます。入力のタイプを表示します。

入力タイプ:内蔵マイクやライン入力など、入力のタイプを選択します。

電源タイプ:入力の電源タイプを選択します。

変更を適用する:選択した内容を適用します。

エコーキャンセル:オンにすると、双方向通信時のエコーが除去されます。

個別のゲインコントロール:オンにすると、入力タイプごとに個別にゲインを調整することができます。

自動ゲインコントロール:オンにすると、サウンドの変化に合わせてゲインが動的に調整されます。

Gain (ゲイン):スライダーを使用してゲインを変更します。マイクのアイコンをクリックすると、ミュート、ミュート解除ができます。

出力:出力のタイプを表示します。

Gain (ゲイン):スライダーを使用してゲインを変更します。スピーカーのアイコンをクリックすると、ミュート、ミュート解除ができます。

自動音量制御:これをオンにすると、デバイスで周囲の騒音レベルに基づいてゲインが自動的かつ動的に調整されるようになります。自動音量制御は、ラインとテレコイルを含め、すべての音声出力に影響します。

ストリーム

エンコード方式:入力ソースストリーミングに使用するエンコード方式を選択します。エンコード方式は、音声入力がオンになっている場合にのみ選択できます。音声入力がオフになっている場合は、[**Enable audio input (音声入力を有効にする)**] をクリックしてオンにします。

エコーキャンセル:オンにすると、双方向通信時のエコーが除去されます。

音声クリップ

クリップを追加:新しい音声クリップを追加します。au、.mp3、.opus、.vorbis、.wavファイルを使用できます。

音声クリップを再生します。

音声クリップの再生を停止します。

コンテキストメニューは以下を含みます。

- **Rename (名前の変更)**:オーディオクリップの名前を変更します。
- **Create link (リンクを作成)**:使用する場合は、音声クリップを装置上で再生するURLを作成します。クリップの音量と再生回数を指定します。
- **Download (ダウンロード)**:音声クリップをコンピューターにダウンロードします。
- **削除**:装置から音声クリップを削除します。

視聴と録音

クリックしてリッスンします。

ライブ音声ストリームの連続録音を開始します。録画を停止するには、もう一度クリックします。録画が進行中の場合、再起動後に自動的に再開されます。

注

装置の入力がオンになっている場合にのみ、試聴・録音が可能です。**[Audio (音声)] > [Device settings (デバイスの設定)]** に移動し、入力がオンになっていることを確認します。

装置に設定されているストレージを表示します。ストレージを設定するには管理者権限が必要です。

録画

クリックして録画にフィルターを適用します。

From (開始):特定の時点以降に行われた録画を表示します。

To (終了):特定の時点までに行われた録画を表示します。

ソース:ソースに基づいて録画を表示します。ソースはセンサーを指します。

Event (イベント):イベントに基づいて録画を表示します。

ストレージ:ストレージタイプに基づいて録画を表示します。

進行中の録画:装置で進行中のすべての録画を表示します。

● 装置で録画を開始します。

保存先のストレージ装置を選択します。

● 装置で録画を停止します。

トリガーされた録画は、手動で停止したとき、または装置がシャットダウンされたときに終了します。

連続録画は、手動で停止するまで続行されます。装置がシャットダウンされた場合でも、録画は装置が再起動されるときまで続行されます。

録画を再生します。

録画の再生を停止します。

録画に関する情報とオプションを表示または非表示にします。

Set export range (**エクスポート範囲の設定**):録画の一部のみをエクスポートする場合は、時間範囲を入力します。装置の位置とは異なるタイムゾーンで作業する場合は、時間範囲が装置のタイムゾーンに基づくことに注意してください。

Encrypt (**暗号化**):エクスポートする録画のパスワードを設定する場合に選択します。エクスポートしたファイルをパスワードなしで開くことができなくなります。

クリックすると、録画が削除されます。

Export (**エクスポート**):録画の全体または一部をエクスポートします。

アプリ

アプリを追加:新しいアプリをインストールします。

さらにアプリを探す:インストールする他のアプリを見つける。Axisアプリの概要ページに移動します。

署名されていないアプリを許可:署名なしアプリのインストールを許可するには、オンにします。

AXIS OSおよびACAPアプリのセキュリティ更新プログラムを表示します。

注
複数のアプリを同時に実行すると、装置のパフォーマンスが影響を受ける可能性があります。

アプリ名の横にあるスイッチを使用して、アプリを起動または停止します。

開く:アプリの設定にアクセスする。利用可能な設定は、アプリケーションよって異なります。一部のアプリケーションでは設定が設けられていません。

コンテキストメニューに、以下のオプションが1つ以上含まれていることがあります。

- Open-source license (オープンソースライセンス):アプリで使用されているオープンソースライセンスに関する情報が表示されます。
- App log (アプリのログ):アプリイベントのログが表示されます。このログは、サポートにご連絡いただく際に役立ちます。
- キーによるライセンスのアクティブ化:アプリにライセンスが必要な場合は、ライセンスを有効にする必要があります。装置がインターネットにアクセスできない場合は、このオプションを使用します。
  ライセンスキーがない場合は、*axis.com/products/analytics*にアクセスします。ライセンスキーを入手するには、ライセンスコードとAxis製品のシリアル番号が必要です。
- ライセンスの自動アクティブ化:アプリにライセンスが必要な場合は、ライセンスを有効にする必要があります。装置がインターネットにアクセスできる場合は、このオプションを使用します。ライセンスをアクティブ化するには、ライセンスコードが必要です。
- Deactivate the license (ライセンスの非アクティブ化):試用ライセンスから正規ライセンスに変更する場合など、別のライセンスと交換するために現在のライセンスを無効にします。ライセンスを非アクティブ化すると、ライセンスはデバイスから削除されます。
- Settings (設定):パラメーターを設定します。
- 削除:デバイスからアプリを完全に削除します。ライセンスを最初に非アクティブ化しない場合、ライセンスはアクティブのままです。

システム

時刻と位置

日付と時刻

時刻の形式は、Webブラウザーの言語設定によって異なります。

注
装置の日付と時刻をNTPサーバーと同期することをお勧めします。

Synchronization (同期):装置の日付と時刻を同期するオプションを選択します。

- Automatic date and time（自動日付と時刻（PTP）） ：高精度時刻同期プロトコル（PTP）を使用して同期します。
- Automatic date and time (manual NTS KE servers) (日付と時刻の自動設定 (手動NTS KEサーバー)):DHCPサーバーに接続された安全なNTPキー確立サーバーと同期します。
  - Manual NTS KE servers (手動NTS KEサーバー):1台または2台のNTPサーバーのIPアドレスを入力します。2台のNTPサーバーを使用すると、両方からの入力に基づいて装置が同期し、時刻を調整します。
  - Trusted NTS KE CA certificates (信頼されたNTS KE CA証明書):安全なNTS KE時刻同期に使用する信頼できるCA証明書を選択するか、なしのままにします。
  - Max NTP poll time (最長NTPポーリング時間):装置がNTPサーバーをポーリングして最新の時刻を取得するまでの最長待機時間を選択します。
  - Min NTP poll time (最短NTPポーリング時間):装置がNTPサーバーをポーリングして最新の時刻を取得するまでの最短待機時間を選択します。
- Automatic date and time (NTP servers using DHCP) (日付と時刻の自動設定 (DHCPを使用したNTPサーバー)):DHCPサーバーに接続されたNTPサーバーと同期します。
  - Fallback NTP servers (フォールバックNTPサーバー):1台または2台のフォールバックサーバーのIPアドレスを入力します。
  - Max NTP poll time (最長NTPポーリング時間):装置がNTPサーバーをポーリングして最新の時刻を取得するまでの最長待機時間を選択します。
  - Min NTP poll time (最短NTPポーリング時間):装置がNTPサーバーをポーリングして最新の時刻を取得するまでの最短待機時間を選択します。
- Automatic date and time (manual NTP servers) (日付と時刻の自動設定 (手動NTPサーバー)):選択したNTPサーバーと同期します。
  - Manual NTP servers (手動NTPサーバー):1台または2台のNTPサーバーのIPアドレスを入力します。2台のNTPサーバーを使用すると、両方からの入力に基づいて装置が同期し、時刻を調整します。
  - Max NTP poll time (最長NTPポーリング時間):装置がNTPサーバーをポーリングして最新の時刻を取得するまでの最長待機時間を選択します。
  - Min NTP poll time (最短NTPポーリング時間):装置がNTPサーバーをポーリングして最新の時刻を取得するまでの最短待機時間を選択します。
- Custom date and time (日付と時刻のカスタム設定):日付と時刻を手動で設定する[Get from system (システムから取得)] をクリックして、コンピューターまたはモバイル装置から日付と時刻 の設定を1回取得します。

タイムゾーン:使用するタイムゾーンを選択します。時刻が夏時間と標準時間に合わせて自動的に調整されます。

- DHCP:DHCPサーバーのタイムゾーンを採用します。このオプションを選択する前に、装置がDHCPサーバー(v4またはv6)に接続されている必要があります。両方のバージョンが利用可能な場合、このデバイスはPOSIXよりIANAのタイムゾーンを優先し、DHCPv6よりDHCPv4を優先します。
  - DHCPv4は、POSIXタイムゾーンにはオプション100を、IANAタイムゾーンにはオプション101を使用します。
  - DHCPv6は、POSIXにはオプション41を、IANAにはオプション42を使用します。
- 手動:ドロップダウンリストからタイムゾーンを選択します。

注

システムは、すべての録画、ログ、およびシステム設定で日付と時刻の設定を使用します。

デバイスの位置

デバイスの位置を入力します。ビデオ管理システムはこの情報を使用して、地図上にデバイスを配置できます。

- **Latitude (緯度)**:赤道の北側がプラスの値です。
- **Longitude (経度)**:本初子午線の東側がプラスの値です。
- **向き**:デバイスが向いているコンパス方位を入力します。真北が0です。
- **ラベル**:分かりやすいデバイス名を入力します。
- **Save (保存)**:クリックして、装置の位置を保存します。

ネットワーク

IPv4

Assign IPv4 automatically (IPv4自動割り当て):IPv4 自動 IP（DHCP）を選択すると、IPアドレス、サブネットマスク、ルーターがネットワークによって自動的に割り当てられ、手動で設定する必要がなくなります。ほとんどのネットワークでは、自動IP割り当て（DHCP）を使用することをおすすめします。

IP address (IPアドレス):装置の固有のIPアドレスを入力します。孤立したネットワークの内部であれば、アドレスの重複がないことを条件に、静的なIPアドレスを自由に割り当てることができます。アドレスの重複を避けるため、固定IPアドレスを割り当てる前に、ネットワーク管理者に連絡することを推奨します。

サブネットマスク:サブネットマスクを入力して、ローカルエリアネットワーク内部のアドレスを定義します。ローカルエリアネットワークの外部のアドレスは、ルーターを経由します。

Router (ルーター):さまざまなネットワークやネットワークセグメントに接続された装置を接続するために使用するデフォルトルーター (ゲートウェイ) のIPアドレスを入力します。

Fallback to static IP address if DHCP isn't available (DHCPが利用できない場合は固定IPアドレスにフォールバックする):DHCPが利用できず、IPアドレスを自動的に割り当てることができない場合に、フォールバックとして使用する固定IPアドレスを追加するときに選択します。

注

DHCPが使用できず、装置が静的アドレスのフォールバックを使用する場合、静的アドレスは限定された範囲で設定されます。

IPv6

Assign IPv6 automatically (IPv6自動割り当て):IPv6をオンにし、ネットワークルーターに自動的に装置にIPアドレスを割り当てさせる場合に選択します。

ホスト名

Assign hostname automatically (ホスト名自動割り当て):ネットワークルーターに自動的に装置にホスト名を割り当てさせる場合に選択します。

ホスト名:装置にアクセスする別の方法として使用するホスト名を手動で入力します。サーバーレポートとシステムログはホスト名を使用します。使用できる文字は、A～Z、a～z、0～9、-、_です。

DNSの動的更新： IPアドレスの変更時に、デバイスでのドメインネームサーバーレコードの自動更新が可能となります。

DNS名の登録：デバイスのIPアドレスを指す一意のドメイン名を入力します。使用できる文字は、A～Z、a～z、0～9、-、_です。

TTL：TTL（Time to Live）とは、DNSレコードの更新が必要となるまでの有効期間を指します。

DNSサーバー

Assign DNS automatically (DNS自動割り当て):DHCPサーバーに自動的に装置に検索ドメインとDNSサーバーアドレスを割り当てさせる場合に選択します。ほとんどのネットワークでは、自動DNS (DHCP) をお勧めします。

Search domains (検索ドメイン):完全修飾でないホスト名を使用する場合は、[**Add search domain (検索ドメインの追加)**] をクリックし、装置が使用するホスト名を検索するドメインを入力します。

DNS servers (DNSサーバー):[**Add DNS server (DNSサーバーを追加)**] をクリックして、DNSサーバーのIPアドレスを入力します。このサーバーは、ホスト名からローカルネットワーク上のIPアドレスへの変換を行います。

注

DHCPが無効になっている場合、ホスト名、DNSサーバー、NTPなど、自動ネットワーク設定に依存する機能が動作しなくなる可能性があります。

HTTPとHTTPS

HTTPSは、ユーザーからのページ要求とWebサーバーから返されたページの暗号化を提供するプロトコルです。サーバーの真正性 (サーバーが本物であること) を保証するHTTPS証明書が使用されます。

デバイスでHTTPSを使用するには、HTTPS証明書をインストールする必要があります。[**System (システム) > Security (セキュリティ)**] に移動し、証明書の作成とインストールを行います。

Allow access through (次によってアクセスを許可):ユーザーが [**HTTP**]、[**HTTPS**]、または [**HTTP and HTTPS (HTTPおよびHTTPS)**] プロトコルを介して装置に接続することを許可するかどうかを選択します。

注

暗号化されたWebページをHTTPS経由で表示する場合、特に初めてページを要求するときに、パフォーマンスが低下することがあります。

HTTP port (HTTPポート):使用するHTTPポートを入力します。装置はポート80または1024～65535の範囲のポートを許可します。管理者としてログインしている場合は、1～1023の範囲の任意のポートを入力することもできます。この範囲のポートを使用すると、警告が表示されます。

HTTPS port (HTTPSポート):使用するHTTPSポートを入力します。装置はポート443または1024～65535の範囲のポートを許可します。管理者としてログインしている場合は、1～1023の範囲の任意のポートを入力することもできます。この範囲のポートを使用すると、警告が表示されます。

Certificate (証明書):装置のHTTPSを有効にする証明書を選択します。

ネットワーク検出プロトコル

Bonjour®: オンにしてネットワーク上で自動検出を可能にします。

Bonjour名:ネットワークで表示されるフレンドリ名を入力します。デフォルト名はデバイス名とMACアドレスです。

UPnP®: オンにしてネットワーク上で自動検出を可能にします。

UPnP名:ネットワークで表示されるフレンドリ名を入力します。デフォルト名はデバイス名とMACアドレスです。

WS-Discovery:オンにしてネットワーク上で自動検出を可能にします。

LLDP and CDP (LLDPおよびCDP):オンにしてネットワーク上で自動検出を可能にします。LLDPとCDPをオフにすると、PoE電力ネゴシエーションに影響する可能性があります。PoE電力ネゴシエーションに関する問題を解決するには、PoEスイッチをハードウェアPoE電力ネゴシエーションのみに設定してください。

グローバルプロキシー

Https proxy (HTTPプロキシー):許可された形式に従って、グローバルプロキシーホストまたはIPアドレスを指定します。

Https proxy (HTTPSプロキシー):許可された形式に従って、グローバルプロキシーホストまたはIPアドレスを指定します。

httpおよびhttpsプロキシーで許可されるフォーマット:

- http(s)://host:port
- http(s)://user@host:port
- http(s)://user:pass@host:port

注

装置を再起動し、グローバルプロキシー設定を適用します。

No proxy (プロキシーなし):グローバルプロキシーをバイパスするには、No proxy (プロキシーなし)を使用します。リスト内のオプションのいずれかを入力するか、コンマで区切って複数入力します。

- 空白にする
- IPアドレスを指定する
- CIDR形式でIPアドレスを指定する
- ドメイン名を指定する (www.<ドメイン名>.comなど)
- 特定のドメイン内のすべてのサブドメインを指定する (.<ドメイン名>.comなど)

ワンクリックによるクラウド接続

One-Click cloud connection (O3C) とO3Cサービスを共に使用すると、インターネットを介して、ライブビデオや録画ビデオにどこからでも簡単かつ安全にアクセスできます。詳細については、*axis.com/end-to-end-solutions/hosted-services*を参照してください。

Allow O3C (O3Cを許可):

- [ワンクリック]:デフォルトの選択肢です。O3Cに接続するには、デバイスのコントロールボタンを押してください。ボタンの押し方は、デバイスモデルにより異なります。一度押して離し、ステータスLEDが点滅するまで待つか、またはステータスLEDが点滅するまで押し続けてください。[**常時**]を有効にして接続を維持するには、24時間以内にこのデバイスをO3Cサービスに登録してください。登録しないと、このデバイスはO3Cから切断されます。
- [**常時**]:デバイスは、インターネットを介してO3Cサービスへの接続を継続的に試行します。一度デバイスを登録すれば、常時接続された状態になります。コントロールボタンに手が届かない場合は、このオプションを使用します。
- [**なし**]:O3Cを切断します。

Proxy settings (**プロキシ設定**)：必要な場合は、プロキシサーバーに接続するためのプロキシ設定を入力します。

[**ホスト**]:プロキシサーバーのアドレスを入力します。

ポート:アクセスに使用するポート番号を入力します。

[**ログイン**] と [**パスワード**]:必要な場合は、プロキシーサーバーのユーザー名とパスワードを入力します。

Authentication method (**認証方式**):

- [**ベーシック**]:この方法は、HTTP用の最も互換性のある認証方式です。ユーザー名とパスワードを暗号化せずにサーバーに送信するため、Digest (**ダイジェスト**) 方式よりも安全性が低くなります。
- [**ダイジェスト**]:この認証方式は、常に暗号化されたパスワードをネットワークに送信するため、高いセキュリティレベルが得られます。
- [**オート**]:このオプションを使用すると、デバイスはサポートされている方法に応じて認証方法を選択できます。**ダイジェスト**方式が**ベーシック**方式より優先されます。

Owner authentication key (OAK) (**オーナー認証キー**、OAK)：[Get key (**キーを取得**)]をクリックして、所有者認証キーを取得します。これは、デバイスがファイアウォールやプロキシを介さずにインターネットに接続されている場合にのみ可能です。

SNMP

SNMP (Simple Network Management Protocol) を使用すると、離れた場所からネットワーク装置を管理できます。

SNMP:使用するSNMPのバージョンを選択します。

- v1 and v2c (v1およびv2c)：
  - Read community (読み取りコミュニティ):サポートされているSNMPオブジェクトすべてに読み取り専用のアクセスを行えるコミュニティ名を入力します。デフォルト値はpublicです。
  - Write community (書き込みコミュニティ):サポートされている (読み取り専用のものを除く) SNMPオブジェクトすべてに読み取りアクセス、書き込みアクセスの両方を行えるコミュニティ名を入力します。デフォルト設定値はwriteです。
  - Activate traps (トラップの有効化):オンに設定すると、トラップレポートが有効になります。デバイスはトラップを使用して、重要なイベントまたはステータス変更のメッセージを管理システムに送信します。webインターフェースでは、SNMP v1およびv2cのトラップを設定できます。SNMP v3に変更するか、SNMPをオフにすると、トラップは自動的にオフになります。SNMP v3を使用する際は、SNMP v3管理アプリケーションでトラップを設定できます。
  - Trap address (トラップアドレス):管理サーバーのIPアドレスまたはホスト名を入力します。
  - Trap community (トラップコミュニティ):装置がトラップメッセージを管理システムに送信するときに使用するコミュニティを入力します。
  - Traps (トラップ):
    - Cold start (コールドスタート):デバイスの起動時にトラップメッセージを送信します。
    - Link up (リンクアップ):リンクの状態が切断から接続に変わったときにトラップメッセージを送信します。
    - Link down (リンクダウン):リンクの状態が接続から切断に変わったときにトラップメッセージを送信します。
    - 認証失敗:認証に失敗したときにトラップメッセージを送信します。

注

SNMP v1およびv2cトラップをオンにすると、すべてのAXIS Video MIBトラップが有効になります。詳細については、*AXIS OSポータル > SNMP*を参照してください。

- v3:SNMP v3は、暗号化と安全なパスワードを使用する、より安全性の高いバージョンです。SNMP v3を使用するには、HTTPSを有効化し、パスワードをHTTPSを介して送信することをお勧めします。これにより、権限のない人が暗号化されていないSNMP v1およびv2cトラップにアクセスすることも防止できます。SNMP v3を使用する際は、SNMP v3管理アプリケーションでトラップを設定できます。
  - プライバシー:SNMPデータを保護するために使用する暗号化方式を選択します。
  - Password for the account "initial" (「initial」アカウントのパスワード):「initial」という名前のアカウントのSNMPパスワードを入力します。HTTPSを有効化せずにパスワードを送信できますが、推奨しません。SNMP v3のパスワードは1回しか設定できません。HTTPSが有効な場合にのみ設定することをお勧めします。パスワードの設定後は、パスワードフィールドが表示されなくなります。パスワードを設定し直すには、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。

セキュリティ

証明書

証明書は、ネットワーク上のデバイスの認証に使用されます。この装置は、次の2種類の証明書をサポートしています。

- Client/server Certificates (クライアント/サーバー証明書)
  クライアント/サーバー証明書は装置のIDを認証します。自己署名証明書と認証局 (CA) 発行の証明書のどちらでも使用できます。自己署名証明書による保護は限られていますが、認証局発行の証明書を取得するまで利用できます。
- CA証明書
  CA証明書はピア証明書の認証に使用されます。たとえば、装置をIEEE 802.1Xで保護されたネットワークに接続するときに、認証サーバーのIDを検証するために使用されます。装置には、いくつかのCA証明書がプリインストールされています。

以下の形式がサポートされています:

- 証明書形式:.PEM、.CER、.PFX
- 秘密鍵形式:PKCS#1、PKCS#12

重要
デバイスを工場出荷時の設定にリセットすると、すべての証明書が削除されます。プリインストールされたCA証明書は、再インストールされます。

証明書を追加:クリックして証明書を追加します。ステップバイステップのガイドが開きます。

- **その他** :入力または選択するフィールドをさらに表示します。
- **セキュアキーストア**:[Trusted Execution Environment (SoC TEE)]、[Secure element (セキュアエレメント)] または [Trusted Platform Module 2.0] を使用して秘密鍵を安全に保存する場合に選択します。どのセキュアキーストアを選択するかの詳細については、*help.axis.com/axis-os#cryptographic-support*にアクセスしてください。
- **Key type (キーのタイプ)**:ドロップダウンリストから、証明書の保護に使用する暗号化アルゴリズムとしてデフォルトかその他のいずれかを選択します。

コンテキストメニューは以下を含みます。

- **Certificate information (証明書情報)**:インストールされている証明書のプロパティを表示します。
- **Delete certificate (証明書の削除)**:証明書の削除。
- **Create certificate signing request (証明書の署名要求を作成する)**:デジタルID証明書を申請するために登録機関に送信する証明書署名要求を作成します。

セキュアキーストア:

- **Trusted Execution Environment (SoC TEE)**: 安全なキーストアにSoC TEEを使用する場合に選択します。
- **Secure element(CC EAL6+, FIPS 140-3 Level 3)**: セキュアキーストアにセキュアエレメントを使用する場合に選択します。
- **Trusted Platform Module 2.0 (CC EAL4+, FIPS 140-2 Level 2)**:セキュアキーストアにTPM 2.0を使用する場合に選択します。

Network access control and encryption (ネットワークのアクセスコントロールと暗号化)

IEEE 802.1x

IEEE 802.1xはポートを使用したネットワークへの接続を制御するIEEEの標準規格で、有線およびワイヤレスのネットワークデバイスを安全に認証します。IEEE 802.1xは、EAP (Extensible Authentication Protocol) に基づいています。

IEEE 802.1xで保護されているネットワークにアクセスするネットワーク装置は、自己の証明を行う必要があります。認証は認証サーバーによって行われます。認証サーバーは通常、FreeRADIUSやMicrosoft Internet Authentication ServerなどのRADIUSサーバーです。

IEEE 802.1AE MACsec

IEEE 802.1AE MACsecは、メディアアクセスコントロール (MAC) セキュリティのためのIEEE標準であり、メディアアクセス独立プロトコルのためのコネクションレスデータ機密性と整合性を定義しています。

証明書

CA証明書なしで設定されている場合、サーバー証明書の検証は無効になり、デバイスは接続先のネットワークに関係なく自己の認証を試みます。

証明書を使用する場合、Axisの実装では、装置と認証サーバーは、EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) を使用してデジタル証明書で自己を認証します。

装置が証明書で保護されたネットワークにアクセスできるようにするには、署名されたクライアント証明書を装置にインストールする必要があります。

Authentication method (認証方式):認証に使用するEAPタイプを選択します。

Client certificate (クライアント証明書)：IEEE 802.1xを使用するクライアント証明書を選択します。認証サーバーは、この証明書を使用してクライアントの身元を確認します。

CA certificates (CA証明書):認証サーバーの身元を確認するためのCA証明書を選択します。証明書が選択されていない場合、デバイスは、接続されているネットワークに関係なく自己を認証しようとします。

EAP識別情報:クライアント証明書に関連付けられているユーザーIDを入力します。

EAPOLのバージョン:ネットワークスイッチで使用されるEAPOLのバージョンを選択します。

Use IEEE 802.1x (IEEE 802.1xを使用):IEEE 802.1xプロトコルを使用する場合に選択します。

これらの設定は、認証方法として**IEEE 802.1x PEAP-MSCHAPv2**を使用する場合にのみ使用できます。

- **パスワード**:ユーザーIDのパスワードを入力します。
- **Peap version (Peapのバージョン)**:ネットワークスイッチで使用するPeapのバージョンを選択します。
- **ラベル**:クライアントEAP暗号化を使用する場合は1を選択し、クライアントPEAP暗号化を使用する場合は2を選択します。Peapバージョン1を使用する際にネットワークスイッチが使用するラベルを選択します。

これらの設定を使用できるのは、認証方法として**IEEE 802.1ae MACsec (静的CAK/事前共有キー)** を使用する場合のみです。

- **Key agreement connectivity association key name (キー合意接続アソシエーションキー名)**:接続アソシエーション名 (CKN) を入力します。2～64文字 (2で割り切れる文字数) の16進文字である必要があります。CKNは、接続アソシエーションで手動で設定する必要があり、最初にMACsecを有効にするには、リンクの両端で一致している必要があります。
- **Key agreement connectivity association key (キー合意接続アソシエーションキー)**:接続アソシエーションキー (CAK) を入力します。32文字または64文字の16進数である必要

があります。CAKは、接続アソシエーションで手動で設定する必要があり、最初にMACsecを有効にするには、リンクの両端で一致している必要があります。

ブルートフォース攻撃を防ぐ

Blocking (ブロック):オンに設定すると、ブルートフォース攻撃がブロックされます。ブルートフォース攻撃では、試行錯誤を繰り返す総当たり攻撃でログイン情報や暗号化キーを推測します。

Blocking period (ブロック期間)：ブルートフォース攻撃をブロックする秒を入力します。

Blocking conditions (ブロックの条件)：ブロックが開始されるまでに1秒間に許容される認証失敗の回数を入力します。ページレベルとデバイスレベルの両方で許容される失敗の数を設定できます。

ファイアウォール

Firewall (ファイアウォール):オンにするとファイアウォールが有効になります。

Default Policy (デフォルトポリシー):ルールで定義されていない接続要求をファイアウォールがどのように処理するかを選択します。

- ACCEPT (許可): デバイスへのすべての接続を許可します。このオプションはデフォルトで設定されています。
- DROP (拒否): デバイスへのすべての接続をブロックします。

デフォルトポリシーに例外を設定するために、特定のアドレス、プロトコル、ポートからデバイスへの接続を許可またはブロックするルールを作成できます。

+ New rule (新規ルールの追加):クリックすると、ルールを作成できます。

Rule type (ルールタイプ):

- FILTER (フィルター): ルールで定義された条件に一致するデバイスからの接続を許可またはブロックする場合に選択します。
  - Policy (ポリシー)：ファイアウォールルールに [Accept (許可)] または [Drop (拒否)] を選択します。
  - IP range (IP範囲):許可またはブロックするアドレス範囲を指定する場合に選択します。[Start (開始)] と [End (終了)] にIPv4/IPv6を使用します。
  - IP address (IPアドレス):許可またはブロックするアドレスを入力します。IPv4/IPv6またはCIDR形式を使用します。
  - Protocol (プロトコル):許可またはブロックするネットワークプロトコル (TCP、UDP、または両方) を選択します。プロトコルを選択すると、ポートも指定する必要があります。
  - MAC: 許可またはブロックするデバイスのMACアドレスを入力します。
  - Port range (ポート範囲):許可またはブロックするポート範囲を指定する場合に選択します。[Start (開始)] と [End (終了)] にそれらを追加します。
  - ポート:許可またはブロックするポート番号を入力します。ポート番号は1～65535の間で指定する必要があります。
  - Traffic type (トラフィックタイプ):許可またはブロックするトラフィックタイプを選択します。
    - UNICAST (ユニキャスト): 1つの送信元から1つの送信先へのトラフィック。
    - BROADCAST (ブロードキャスト): 1つの送信元からネットワーク上のすべてのデバイスへのトラフィック。
    - MULTICAST (マルチキャスト): 複数の送信元から複数の送信先へのトラフィック。
- LIMIT (制限): ルールで定義された条件に一致するデバイスからの接続を許可しますが、過剰なトラフィックを軽減するために制限を適用する場合に選択します。
  - IP range (IP範囲):許可またはブロックするアドレス範囲を指定する場合に選択します。[Start (開始)] と [End (終了)] にIPv4/IPv6を使用します。
  - IP address (IPアドレス):許可またはブロックするアドレスを入力します。IPv4/IPv6またはCIDR形式を使用します。
  - Protocol (プロトコル):許可またはブロックするネットワークプロトコル (TCP、UDP、または両方) を選択します。プロトコルを選択すると、ポートも指定する必要があります。
  - MAC: 許可またはブロックするデバイスのMACアドレスを入力します。
  - Port range (ポート範囲):許可またはブロックするポート範囲を指定する場合に選択します。[Start (開始)] と [End (終了)] にそれらを追加します。
  - ポート:許可またはブロックするポート番号を入力します。ポート番号は1～65535の間で指定する必要があります。

- Unit (単位):許可またはブロックする接続のタイプを選択します。
- Period (期間):[Amount (量)] に関連する期間を選択します。
- Amount (量):設定した [Period (期間)] 内にデバイスの接続を許可する最大回数を設定します。上限は65535です。
- Burst (バースト):設定した [Period (期間)] に [Amount (量)] を1回超えることを許可する接続の数を入力します。一この数に達すると、設定した期間に設定した量のみ許可されます。
- Traffic type (トラフィックタイプ):許可またはブロックするトラフィックタイプを選択します。
  - UNICAST (ユニキャスト): 1つの送信元から1つの送信先へのトラフィック。
  - BROADCAST (ブロードキャスト): 1つの送信元からネットワーク上のすべてのデバイスへのトラフィック。
  - MULTICAST (マルチキャスト): 複数の送信元から複数の送信先へのトラフィック。

Test rules (テストルール):クリックして、定義したテストを追加します。

- Time in seconds (テスト時間、秒):ルールのテストに制限時間を設定します。
- Roll back (ロールバック):クリックすると、ルールをテストする前にファイアウォールを前の状態にロールバックします。
- Apply rules (ルールの適用):クリックすると、テストなしでルールが有効になります。これは推奨されません。

カスタム署名付きAXIS OS証明書

Axisのテストソフトウェアまたはその他のカスタムソフトウェアを装置にインストールするには、カスタム署名付きAXIS OS証明書が必要です。証明書は、ソフトウェアが装置の所有者とAxisの両方によって承認されたことを証明します。ソフトウェアは、一意のシリアル番号とチップIDで識別される特定の装置でのみ実行できます。署名用のキーはAxisが保有しており、カスタム署名付きAXIS OS証明書はAxisしか作成できません。

Install (インストール):クリックして、証明書をインストールします。ソフトウェアをインストールする前に、証明書をインストールする必要があります。

⋮ コンテキストメニューは以下を含みます。

- Delete certificate (証明書の削除):証明書の削除。

アカウント

アカウント

+ **アカウントを追加**:クリックして、新しいアカウントを追加します。最大100個のアカウントを追加できます。

Account (アカウント):固有のアカウント名を入力します。

New password (新しいパスワード):アカウントのパスワードを入力します。パスワードの長は1~64文字である必要があります。印刷可能なASCII文字 (コード32～126) のみを使用できます。これには、英数字、句読点、および一部の記号が含まれます。

Repeat password (パスワードの再入力):同じパスワードを再び入力します。

Privileges (権限):

- **Administrator (管理者)**:すべての設定へ全面的なアクセス権をもっています。管理者は他のアカウントを追加、更新、削除することもできます。
- **Operator (オペレーター)**:次の操作を除く、すべての設定へのアクセス権があります。
  - すべての [**System settings (システムの設定)**]。
- **Viewer (閲覧者)**:設定を変更するアクセス権を持っていません。

⋮ コンテキストメニューは以下を含みます。

Update account (アカウントの更新):アカウントのプロパティを編集します。

Delete account (アカウントの削除):アカウントを削除します。rootアカウントは削除できません。

匿名アクセス

Allow anonymous viewing (匿名の閲覧を許可する):アカウントでログインせずに誰でも閲覧者として装置にアクセスできるようにする場合は、オンにします。

匿名のPTZ操作を許可する:オンにすると、匿名ユーザーに画像のパン、チルト、ズームを許可します。

SSHアカウント

+ **Add SSH account (SSHアカウントを追加)**:クリックして、新しいSSHアカウントを追加します。

- **Enable SSH (SSHの有効化)**:SSHサービスを使用する場合は、オンにします。

Account (アカウント):固有のアカウント名を入力します。

New password (新しいパスワード):アカウントのパスワードを入力します。パスワードの長は1~64文字である必要があります。印刷可能なASCII文字 (コード32～126) のみを使用できます。これには、英数字、句読点、および一部の記号が含まれます。

Repeat password (パスワードの再入力):同じパスワードを再び入力します。

コメント:コメントを入力します (オプション)。

⋮ コンテキストメニューは以下を含みます。

Update SSH account (SSHアカウントの更新):アカウントのプロパティを編集します。

Delete SSH account (SSHアカウントの削除):アカウントを削除します。rootアカウントは削除できません。

Virtual host (仮想ホスト)

＋ Add virtual host (仮想ホストを追加):クリックして、新しい仮想ホストを追加します。

Enabled (有効):この仮想ホストを使用するには、選択します。

Server name (サーバー名):サーバーの名前を入力します。数字0〜9、文字A〜Z、ハイフン (-) のみを使用します。

ポート:サーバーが接続されているポートを入力します。

タイプ:使用する認証のタイプを選択します。Basic（ベーシンク）、Digest（ダイジェスト）、Open ID（IDを開く）、Client Credential Grant（クライアント資格情報グラント）のいずれかを選択します。

HTTPS: HTTPS を使用する場合に選択します。

⋮ コンテキストメニューは以下を含みます。

- 仮想ホストの更新
- 仮想ホストの削除

クライアント認証情報付与設定

Admin claim (管理者請求):管理者権限の値を入力します。

Verification URL (検証URL): APIエンドポイント認証用のWebリンクを入力します。

Operator claim (オペレーター請求):オペレーター権限の値を入力します。

Require claim (必須請求):トークンに含めるデータを入力します。

Viewer claim (閲覧者請求):閲覧者権限の値を入力します。

Save (保存):クリックして値を保存します。

OpenID設定

重要

OpenIDを使用してサインインできない場合は、OpenIDを設定したときに使用したダイジェストまたはベーシック認証情報を使用してサインインします。

Client ID (クライアントID)：OpenIDユーザー名を入力します。

Outgoing Proxy (発信プロキシ):OpenID接続でプロキシサーバーを使用する場合は、プロキシアドレスを入力します。

Admin claim (管理者請求):管理者権限の値を入力します。

Provider URL (プロバイダーURL):APIエンドポイント認証用のWebリンクを入力します。形式はhttps://[URLを挿入]/.well-known/openid-configurationとしてください。

Operator claim (オペレーター請求):オペレーター権限の値を入力します。

Require claim (必須請求):トークンに含めるデータを入力します。

Viewer claim (閲覧者請求):閲覧者権限の値を入力します。

Remote user (リモートユーザー):リモートユーザーを識別する値を入力します。これは、装置のwebインターフェースに現在のユーザーを表示するのに役立ちます。

Scopes (スコープ):トークンの一部となるオプションのスコープです。

Client secret (クライアントシークレット):OpenIDのパスワードを入力します。

Save (保存):クリックして、OpenIDの値を保存します。

Enable OpenID (OpenIDの有効化):現在の接続を閉じ、プロバイダーURLからの装置認証を許可する場合は、オンにします。

イベント

ルール

ルールは、製品がアクションを実行するためのトリガーとなる条件を定義します。このリストには、本製品で現在設定されているすべてのルールが表示されます。

注

最大256のアクションルールを作成できます。

＋ **ルールを追加**:ルールを作成します。

名前:アクションルールの名前を入力します。

Wait between actions (アクション間の待ち時間):ルールを有効化する最短の時間間隔 (hh:mm:ss) を入力します。たとえば、デイナイトモードの条件によってルールが有効になる場合、このパラメーターを設定することで、日の出や日没時のわずかな光の変化によりルールが反復的に有効になるのを避けられます。

Condition (条件):リストから条件を選択します。装置がアクションを実行するためには、条件を満たす必要があります。複数の条件が定義されている場合、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。特定の条件については、「*イベントのルールの使用開始*」を参照してください。

Use this condition as a trigger (この条件をトリガーとして使用する):この最初の条件を開始トリガーとしてのみ機能させる場合に選択します。つまり、いったんルールが有効になると、最初の条件の状態に関わらず、他のすべての条件が満たされている限り有効のままになります。このオプションを選択しない場合、ルールは単純にすべての条件が満たされたときに有効化されます。

Invert this condition (この条件を逆にする):選択した条件とは逆の条件にする場合に選択します。

＋ **条件を追加**:新たに条件を追加する場合にクリックします。

Action (アクション):リストからアクションを選択し、必要な情報を入力します。特定のアクションについては、「*イベントのルールの使用開始*」を参照してください。

ご利用の製品には、以下のようなルールが事前設定されている場合があります:

前面LEDの点灯：LiveStream (ライブストリーム)：マイクをオンにし、ライブストリームを受信すると、音声デバイスの前面のLEDが緑色に点灯します。

前面LEDの点灯：Recording (録音)：マイクがオンになり、録音が行われている場合は、音声デバイスの前面LEDが緑色に点灯します。

前面LEDの点灯：SIP：マイクがオンになっており、SIP呼び出しがアクティブな場合、音声デバイスの前面LEDが緑色に変わります。このイベントがトリガーされるようにするには、音声装置でSIPを有効にする必要があります。

プレアナウンストーン：着信呼び出し時にトーンを再生：音声装置に対してSIP呼び出しが行われると、事前に定義した音声クリップが再生されます。音声装置でSIPを有効にする必要があります。音声装置で音声クリップの再生中にSIPの発信者が呼び出し音を聞くようにするには、装置のSIPアカウントが呼び出しに自動応答しないように設定する必要があります。

プレアナウンストーン：着信呼び出し音の後に電話に応答：音声クリップが終了すると、着信SIP呼び出しに応答します。音声装置でSIPを有効にする必要があります。

ラウドリンガー:音声デバイスに対してSIP呼び出しが行われると、ルールが有効化されている場合は、事前に定義された音声クリップが再生されます。音声装置でSIPを有効にする必要があります。

送信先

イベントについて受信者に通知したり、ファイルを送信したりするように装置を設定できます。

注

FTPまたはSFTPを使用するように装置を設定した場合、ファイル名に付加される固有のシーケンス番号を変更したり削除したりしないでください。その場合、イベントごとに1つの画像しか送信できません。

このリストには、製品で現在設定されているすべての送信先とそれらの設定に関する情報が示されます。

注

最大20名の送信先を作成できます。

送信先を追加:クリックすると、送信先を追加できます。

名前:送信先の名前を入力します。

タイプ:リストから選択します:

- FTP
  - **[ホスト]**:サーバーのIPアドレスまたはホスト名を入力します。ホスト名を入力した場合は、必ず、[**System (システム) > Network (ネットワーク) > IPv4 and IPv6 (IPv4 と IPv6)**] で DNS サーバーを指定します。
  - **ポート**:FTPサーバーに使用するポート番号。デフォルトは21です。
  - **Folder (フォルダー)**:ファイルを保存するディレクトリのパスを入力します。FTPサーバー上に存在しないディレクトリを指定すると、ファイルのアップロード時にエラーメッセージが表示されます。
  - **Username (ユーザー名)**:ログインのユーザー名を入力します。
  - **パスワード**:ログインのパスワードを入力します。
  - **Use temporary file name (一時ファイル名を使用する)**:選択すると、自動的に生成された一時的なファイル名でファイルがアップロードされます。アップロードが完了した時点で、ファイル名が目的の名前に変更されます。アップロードが中止/中断されても、破損したファイルが発生することはありません。ただし、一時ファイルが残る可能性はあります。これにより、目的の名前を持つすべてのファイルが正常であると確信できます。
  - **Use passive FTP (パッシブFTPを使用する)**:通常は、製品がFTPサーバーに要求を送ることでデータ接続が開かれます。この接続では、対象サーバーとのFTP制御用接続とデータ用接続の両方が装置側から開かれます。一般に、装置と対象FTPサーバーの間にファイアウォールがある場合に必要となります。
- HTTP
  - **URL**:HTTPサーバーのネットワークアドレスと、要求の処理を行うスクリプトを入力します。たとえば、http://192.168.254.10/cgi-bin/notify.cgiと入力します。
  - **Username (ユーザー名)**:ログインのユーザー名を入力します。
  - **パスワード**:ログインのパスワードを入力します。
  - **Proxy (プロキシ)**:HTTPサーバーに接続するためにプロキシサーバーを渡す必要がある場合は、これをオンにし、必要な情報を入力します。
- HTTPS
  - **URL**:HTTPSサーバーのネットワークアドレスと、要求の処理を行うスクリプトを入力します。たとえば、https://192.168.254.10/cgi-bin/notify.cgiと入力します。
  - **Validate server certificate (サーバー証明書を検証する)**:HTTPSサーバーが作成した証明書を検証する場合にオンにします。
  - **Username (ユーザー名)**:ログインのユーザー名を入力します。
  - **パスワード**:ログインのパスワードを入力します。
  - **Proxy (プロキシ)**:HTTPSサーバーに接続するためにプロキシサーバーを渡す必要がある場合にオンにして、必要な情報を入力します。
- ネットワークストレージ
  NAS (network-attached storage) などのネットワークストレージを追加し、それを録画ファイルの保存先として使用することができます。ファイルは.mkv (Matroska) 形式で保存されます。
  - **[ホスト]**:ネットワークストレージのIPアドレスまたはホスト名を入力します。
  - **共有**:ホスト上の共有の名を入力します。

- Folder (フォルダー):ファイルを保存するディレクトリのパスを入力します。
- Username (ユーザー名):ログインのユーザー名を入力します。
- パスワード:ログインのパスワードを入力します。

- SFTP
  - [ホスト]:サーバーのIPアドレスまたはホスト名を入力します。ホスト名を入力した場合は、必ず、[System (システム) > Network (ネットワーク) > IPv4 and IPv6 (IPv4 と IPv6)] で DNS サーバーを指定します。
  - ポート:SFTPサーバーに使用するポート番号。デフォルトは22です。
  - Folder (フォルダー):ファイルを保存するディレクトリのパスを入力します。SFTPサーバー上に存在しないディレクトリを指定すると、ファイルのアップロード時にエラーメッセージが表示されます。
  - Username (ユーザー名):ログインのユーザー名を入力します。
  - パスワード:ログインのパスワードを入力します。
  - SSH host public key type (MD5) (SSHホスト公開鍵タイプ (MD5)):リモートホストの公開鍵のフィンガープリント (32桁の16進数) を入力します。SFTPクライアントは、RSA、DSA、ECDSA、およびED25519ホストキータイプによるSSH-2を使用するSFTPサーバーをサポートします。RSAは、ネゴシエーション時の推奨方式です。その後には、ECDSA、ED25519、DSAが続きます。SFTPサーバーで使用されている正しいMD5ホストキーを入力してください。AxisデバイスはMD5とSHA-256の両方のハッシュキーをサポートしていますが、MD5よりもセキュリティが強いため、SHA-256を使用することをお勧めします。AxisデバイスでSFTPサーバーを設定する方法の詳細については、*AXIS OSポータル*にアクセスしてください。
  - SSH host public key type (SHA256) (SSHホスト公開鍵タイプ (SHA256)):リモートホストの公開鍵のフィンガープリント (43桁のBase64エンコード文字列) を入力します。SFTPクライアントは、RSA、DSA、ECDSA、およびED25519ホストキータイプによるSSH-2を使用するSFTPサーバーをサポートします。RSAは、ネゴシエーション時の推奨方式です。その後には、ECDSA、ED25519、DSAが続きます。SFTPサーバーで使用されている正しいMD5ホストキーを入力してください。AxisデバイスはMD5とSHA-256の両方のハッシュキーをサポートしていますが、MD5よりもセキュリティが強いため、SHA-256を使用することをお勧めします。AxisデバイスでSFTPサーバーを設定する方法の詳細については、*AXIS OSポータル*にアクセスしてください。
  - Use temporary file name (一時ファイル名を使用する):選択すると、自動的に生成された一時的なファイル名でファイルがアップロードされます。アップロードが完了した時点で、ファイル名が目的の名前に変更されます。アップロードが中止/中断されても、ファイルが破損することはありません。ただし、一時ファイルが残る可能性はあります。これにより、目的の名前を持つすべてのファイルが正常であると確信できます。

- SIPまたはVMS :
  SIP:選択してSIP呼び出しを行います。
  VMS:選択してVMS呼び出しを行います。
  - 送信元のSIPアカウント:リストから選択します。
  - 送信先のSIPアドレス:SIPアドレスを入力します。
  - テスト:クリックして、呼び出しの設定が機能することをテストします。
- 電子メール
  - 電子メールの送信先:電子メールの宛先のアドレスを入力します。複数のアドレスを入力するには、カンマで区切ります。
  - 電子メールの送信元:送信側サーバーのメールアドレスを入力します。

- Username (ユーザー名):メールサーバーのユーザー名を入力します。認証の必要のないメールサーバーの場合は、このフィールドを空にします。
- パスワード:メールサーバーのパスワードを入力します。認証の必要のないメールサーバーの場合は、このフィールドを空にします。
- Email server (SMTP) (電子メールサーバー (SMTP)):SMTPサーバーの名前 (smtp.gmail.com、smtp.mail.yahoo.comなど) を入力します。
- ポート:SMTPサーバーのポート番号を0～65535の範囲で入力します。デフォルト設定値は587です。
- [暗号化]:暗号化を使用するには、SSL または TLS を選択します。
- Validate server certificate (サーバー証明書を検証する):暗号化を使用している場合にこれを選択すると、装置の身元を検証できます。この証明書は、自己署名または認証局 (CA) 発行の証明書のどちらでも可能です。
- POP authentication (POP認証):オンにすると、POPサーバーの名前 (pop.gmail.comなど) を入力できます。

注

一部の電子メールプロバイダーでは、大量の添付ファイルやスケジュール設定済みメールなどがセキュリティフィルターによって受信または表示できないようになっています。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、メールアカウントのロックや、必要な電子メールの不着などが起こらないようにしてください。

- TCP
  - [ホスト]:サーバーのIPアドレスまたはホスト名を入力します。ホスト名を入力した場合は、必ず、[System (システム) > Network (ネットワーク) > IPv4 and IPv6 (IPv4 と IPv6)] で DNS サーバーを指定します。
  - ポート:サーバーへのアクセスに使用したポート番号を入力します。

Test (テスト):クリックすると、セットアップをテストすることができます。

⋮ コンテキストメニューは以下を含みます。

View recipient (送信先の表示):クリックすると、すべての送信先の詳細が表示されます。

Copy recipient (送信先のコピー):クリックすると、送信先をコピーできます。コピーする際、新しい送信先に変更を加えることができます。

Delete recipient (送信先の削除):クリックすると、受信者が完全に削除されます。

スケジュール

スケジュールとパルスは、ルールで条件として使用することができます。このリストには、製品で現在設定されているすべてのスケジュールとパルス、およびそれらの設定に関する情報が示されます。

＋ スケジュールを追加:クリックすると、スケジュールやパルスを作成できます。

手動トリガー

手動トリガーを使用すると、ルールを手動でトリガーできます。手動トリガーは、本製品の設置、設定中にアクションを検証する目的などで使用します。

MQTT

MQTT (Message Queuing Telemetry Transport) はモノのインターネット (IoT) で使われる標準の通信プロトコルです。IoTの統合を簡素化するために設計されており、小さなコードフットプリントと最小限のネットワーク帯域幅でリモートデバイスを接続するために、さまざまな業界で使用されています。Axis装置のソフトウェアに搭載されているMQTTクライアントは、装置で生成されたデータやイベントを、ビデオ管理ソフトウェア (VMS) ではないシステムに統合することを容易にします。

デバイスをMQTTクライアントとして設定します。MQTTの通信は、2つのエンティティ (クライアントとブローカー) に基づいています。クライアントは、メッセージの送受信を行うことができます。ブローカーは、クライアント間でメッセージをルーティングする役割を担います。

MQTTの詳細については、*AXIS OSナレッジベース*を参照してください。

ALPN

ALPNは、クライアントとサーバー間の接続のハンドシェイクフェーズ中にアプリケーションプロトコルを選択できるようにするTLS/SSL拡張機能です。ALPNは、HTTPなどの他のプロトコルで使用される同じポート経由でMQTTトラフィックを有効にするために使用されます。場合によっては、MQTT通信のための専用ポートが開かれていない可能性があります。このような場合の解決策は、ALPNを使用して、ファイアウォールによって許可される標準ポートで、アプリケーションプロトコルとしてMQTTを使用するようネゴシエーションすることです。

MQTT クライアント

Connect (接続する):MQTTクライアントのオン/オフを切り替えます。

Status (ステータス):MQTTクライアントの現在のステータスを表示します。

ブローカー

[ホスト]:MQTTサーバーのホスト名またはIPアドレスを入力します。

Protocol (プロトコル):使用するプロトコルを選択します。

ポート:ポート番号を入力します。

- 1883はMQTTオーバTCPのデフォルト値です。
- 8883はMQTTオーバSSLのデフォルト値です。
- 80はMQTTオーバWebSocketのデフォルト値です。
- 443はMQTTオーバWebSocket Secureのデフォルト値です。

ALPN protocol (ALPNプロトコル):ご使用のMQTTブローカープロバイダーが提供するALPNプロトコル名を入力します。これは、MQTTオーバーSSLとMQTTオーバーWebSocket Secureを使用する場合にのみ適用されます。

Username (ユーザー名):クライアントがサーバーにアクセスするために使用するユーザー名を入力します。

パスワード:ユーザー名のパスワードを入力します。

Client ID (クライアントID)：クライアントIDを入力します。クライアントがサーバーに接続すると、クライアント識別子がサーバーに送信されます。

Clean session (クリーンセッション):接続時と切断時の動作を制御します。選択した場合、接続時と切断時にステータス情報が破棄されます。

HTTP proxy (HTTPプロキシ):最大長が255バイトのURL。HTTPプロキシを使用しない場合、このフィールドは空白のままで構いません。

HTTPS proxy (HTTPSプロキシ):最大長が255バイトのURL。HTTPSプロキシを使用しない場合、このフィールドは空白のままで構いません。

Keep alive interval (キープアライブの間隔):長時間のTCP/IPタイムアウトを待たずに、サーバーを使用できなくなったことをクライアントに検知させます。

Timeout (タイムアウト):接続を終了する時間の間隔(秒)です。デフォルト値:60

装置トピックの接頭辞:MQTTクライアントタブの接続メッセージやLWTメッセージ、MQTT公開タブの公開条件におけるトピックのデフォルト値で使用されます。

Reconnect automatically (自動再接続):切断された場合に、クライアントを自動的に再接続するかどうかを指定します。

接続メッセージ

接続が確立されたときにメッセージを送信するかどうかを指定します。

Send message (メッセージの送信):オンにすると、メッセージを送信します。

Use default (デフォルトを使用):オフに設定すると、独自のデフォルトメッセージを入力できます。

Topic (トピック):デフォルトのメッセージのトピックを入力します。

Payload (ペイロード):デフォルトのメッセージの内容を入力します。

Retain (保持する):クライアントの状態をこのTopic (トピック)に保存する場合に選択します。

QoS:パケットフローのQoS layerを変更します。

最終意思およびテスタメントメッセージ

最終意思テスタメント(LWT) を使用すると、クライアントはブローカーへの接続時、認証情報と共にテスタメントを提供します。後ほどいずれかの時点でクライアントが予期せず切断された場合(電源の停止など)、ブローカーから他のクライアントにメッセージを送信できます。このLWTメッセージは通常のメッセージと同じ形式で、同一のメカニズムを経由してルーティングされます。

Send message (メッセージの送信):オンにすると、メッセージを送信します。

Use default (デフォルトを使用):オフに設定すると、独自のデフォルトメッセージを入力できます。

Topic (トピック):デフォルトのメッセージのトピックを入力します。

Payload (ペイロード):デフォルトのメッセージの内容を入力します。

Retain (保持する):クライアントの状態をこのTopic (トピック)に保存する場合に選択します。

QoS:パケットフローのQoS layerを変更します。

MQTT公開

Use default topic prefix (デフォルトのトピックプレフィックスを使用):選択すると、[MQTT client (MQTTクライアント)] タブの装置のトピックプレフィックスで定義されたデフォルトのトピックプレフィックスが使用されます。

Include condition（条件を含める）:選択すると、条件を説明するトピックがMQTTトピックに含まれます。

Include namespaces（名前空間を含める）:選択すると、ONVIFトピックの名前空間がMQTTトピックに含まれます。

シリアル番号を含める:選択すると、装置のシリアル番号が、MQTTペイロードに含まれます。

＋ 条件を追加:クリックして条件を追加します。

Retain (保持する):保持して送信するMQTTメッセージを定義します。

- None (なし):すべてのメッセージを、保持されないものとして送信します。
- Property (プロパティ):ステートフルメッセージのみを保持として送信します。
- All (すべて):ステートフルメッセージとステートレスメッセージの両方を保持として送信します。

QoS:MQTT公開に適切なレベルを選択します。

MQTTサブスクリプション

＋ **サブスクリプションを追加**:クリックして、新しいMQTTサブスクリプションを追加します。

サブスクリプションフィルター:購読するMQTTトピックを入力します。

装置のトピックプレフィックスを使用:サブスクリプションフィルターを、MQTTトピックのプレフィックスとして追加します。

サブスクリプションの種類:

- **ステートレス**:選択すると、エラーメッセージがステートレスメッセージに変換されます。
- **ステートフル**:選択すると、エラーメッセージが条件に変換されます。ペイロードが状態として使用されます。

QoS:MQTTサブスクリプションに適切なレベルを選択します。

MQTTオーバーレイ

注
MQTTオーバーレイ修飾子を追加する前に、MQTTブローカーに接続します。

＋ **オーバーレイ修飾子を追加**:クリックして新しいオーバーレイ修飾子を追加します。

Topic filter (トピックフィルター):オーバーレイに表示するデータを含むMQTTトピックを追加します。

Data field (データフィールド):オーバーレイに表示するメッセージペイロードのキーを指定します。メッセージはJSON形式であるとします。

Modifier (修飾子):オーバーレイを作成するときに、生成された修飾子を使用します。

- **#XMP**で始まる修飾子は、トピックから受信したすべてのデータを示します。
- **#XMD**で始まる修飾子は、データフィールドで指定されたデータを示します。

SIP

設定

セッション開始プロトコル (SIP) は、ユーザー間でのインタラクティブな通信セッションに使用します。セッションには、音声およびビデオを含めることができます。

SIP setup assistant (SIP設定アシスタント):クリックすると、ステップバイステップでSIPを設定できます。

Enable SIP (SIP の有効化):このオプションをオンにすると、SIPコールの発着信が可能になります。

着信呼び出しを許可:このオプションにチェックマークを入れると、その他のSIPデバイスからの着信呼び出しを許可します。

呼び出し処理

- 呼び出しタイムアウト:誰も応答しない場合の呼び出しの最大継続時間を設定します。
- Incoming call duration (着信間隔):着信の最長時間 (最大10分) を設定します。
- End calls after (呼び出し終了):呼び出しの最長時間 (最大60分) を設定します。呼び出しの長さを制限しない場合は、[Infinite call duration (無限呼び出し期間)] を選択します。

ポート

ポート番号は1024～65535の間で指定する必要があります。

- 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開始ポート番号:SIP呼び出しで最初のRTPメディアストリームに使用されるネットワークポートです。デフォルトの開始ポート番号は4000です。ファイアウォールは、特定のポート番号のRTPトラフィックをブロックします。

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) 上にある装置を、そのネットワークの外部から利用できるようにする場合に使用します。

注

NATトラバーサルを機能させるには、ルーターがNATトラバーサルに対応している必要があります。また、UPnP®にも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良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、装置が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、経由していれば、リモートホストへの接続に割り当てるマッピングされるパブリック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。

音声

- 音声コーデックの優先度: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。

注

呼び出しを行うと送信先のコーデックが決定されるため、選択したコーデックは送信先のコーデックと一致する必要があります。

- Audio direction (音声の方向):許可されている音声方向を選択します。

その他

- **UDP-to-TCP switching (UDPからTCPへの切り替え)**:選択して、転送プロトコルを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)**:選択して、ルーターのパブリックIPアドレスの代わりに、ローカルIPアドレスを送信します。
- **Allow contact rewrite (接続のリライトを許可)**:選択して、ルーターのパブリックIPアドレスの代わりに、ローカルIPアドレスを送信します。
- **Register with server every (サーバーに登録)**:既存のSIPアカウントで、装置をSIPサーバーに登録する頻度を設定します。
- **DTMF payload type (DTMFのペイロードタイプ)**:DTMFのデフォルトのペイロードタイプを変更します。
- **Max retransmissions (最大再送回数)**:装置が試行を停止するまでにSIPサーバーへの接続を試行する最大回数を設定します。
- **Seconds until failback (フェイルバックまでの秒数)**:装置がセカンダリSIPサーバーにフェイルオーバーした後、プライマリSIPサーバーへの再接続を試みるまでの秒数を設定します。

アカウント

現在のSIPアカウントはすべて、[SIP accounts (SIPアカウント)] に一覧表示されます。登録済みのアカウントの場合、色付きの円でステータスが示されます。

● アカウントをSIPサーバーに正常に登録できました。

● アカウントに問題があります。原因として、アカウントの認証情報が正しくないため認証に失敗した、またはSIPサーバーでアカウントが見つからないことが考えられます。

[Peer to peer (default) (ピアツーピア (デフォルト))] アカウントは、自動的に作成されたアカウントです。他に少なくとも1つアカウントを作成し、デフォルトとしてそのアカウントを設定した場合、ピアツーピアアカウントを削除することができます。デフォルトのアカウントは、どのSIPアカウントから呼び出すか指定せずにVAPIX®アプリケーションプログラミングインターフェース (API) 呼び出しを行うと必ず使用されます。

＋ **アカウントを追加**:クリックすると、新しいSIPアカウントを作成できます。

- **Active (アクティブ)**:アカウントを使用できるようにします。
- [**デフォルトにする**]:このアカウントをデフォルトに設定します。デフォルトのアカウントは必須で、デフォルトに設定できるのは1つだけです。
- [**自動応答**]:着信呼び出しに自動的に応答するにはこれを選択します。
- **IPv4よりIPv6を優先**:IPv6アドレスをIPv4アドレスより優先する場合に選択します。これは、IPv4アドレスとIPv6アドレスの両方で解決されるピアツーピアアカウントまたはドメイン名に接続する場合に便利です。IPv6アドレスにマッピングされているドメイン名にはIPv6のみを優先できます。
- **名前**:わかりやすい名前を入力します。姓名、権限、または場所などにすることができます。名前がすでに使用されています。
- **ユーザーID**:装置に割り当てられた一意の内線番号または電話番号を入力します。
- [**ピアツーピア**]:ローカルネットワーク上の別のSIP装置への直接的な呼び出しに使用します。
- **登録済み**:SIPサーバーを介して、ローカルネットワークの外部のSIPデバイスへの呼び出しに使用します。
- **ドメイン (Domain)**:利用可能な場合は、パブリックドメイン名を入力します。他のアカウントを呼び出したときにSIPアドレスの一部として表示されます。
- **パスワード**:SIPサーバーに対して認証するためのSIPアカウントに関連付けられたパスワードを入力します。
- **認証ID**:SIPサーバーに対して認証するために使用される認証IDを入力します。ユーザーIDと同じ場合、認証IDを入力する必要はありません。
- **呼び出し側ID**:装置からの呼び出しの送信先に表示される名前です。
- [**レジストラ**]:レジストラのIPアドレスを入力します。
- **伝送モード**:アカウントのSIP伝送モードを選択します。UPD、TCP、またはTLS。
- **TLS version (TLSバージョン)** (トランスポートモードTLSのみ):使用するTLSのバージョンを選択します。**v1.2**と**v1.3**が最も安全なバージョンです。[**Automatic (自動)**] では、システムが処理できる最も安全なバージョンが選択されます。
- **メディアの暗号化** (TLS伝送モードでのみ):SIP呼び出しでメディア暗号化 (音声およびビデオ) のタイプを選択します。
- **証明書** (TLS伝送モードでのみ):証明書を選択します。
- **サーバー証明書の検証** (TLS伝送モードでのみ):サーバー証明書を確認します。
- **セカンダリSIPサーバー**:プライマリSIPサーバーへの登録に失敗したときに、装置がセカンダリSIPサーバーへの登録を試みるようにする場合にオンにします。

- [SIPS (SIP secure)]:SIPS (Secure Session Initiation Protocol) を使用する場合に選択します。SIPSは、トラフィックを暗号化するためにTLS伝送モードを使用します。
- プロキシー
  - ＋ プロキシー:クリックしてプロキシを追加します。
  - 優先:2つ以上のプロキシーを追加した場合は、クリックして優先順位を付けます。
  - サーバーアドレス:SIPプロキシサーバーのIPアドレスを入力します。
  - Username (ユーザー名):必要であればSIPプロキシーサーバーで使用するユーザー名を入力します。
  - パスワード:必要であればSIPプロキシーサーバーで使用するパスワードを入力します。
- ビデオ
  - View area (ビューエリア):ビデオ通話に使用するビューエリアを選択します。[なし] を選択すると、ネイティブビューが使用されます。
  - 解像度:ビデオ通話に使用する解像度を選択します。解像度は、必要な帯域幅に影響します。
  - フレームレート:ビデオ通話1秒あたりのフレーム数を選択します。フレームレートは、必要な帯域幅に影響します。
  - H.264プロファイル:ビデオ通話に使用するプロファイルを選択します。

DTMF

＋ シーケンスを追加:クリックして、新しいDTMF (Dual-Tone Multi-Frequency) シーケンスを作成します。タッチトーンによって有効になるルールを作成するには、[Events (イベント)] > [Rules (ルール)] に移動します。

シーケンス:ルールを有効にする文字を入力します。使用できる文字:0〜9、A〜D、#、および *。

Description (説明):シーケンスによってトリガーされるアクションの説明を入力します。

Accounts (アカウント):DTMFシーケンスを使用するアカウントを選択します。[peer-to-peer (ピアツーピア)] を選択した場合、すべてのピアツーピアアカウントが同じDTMFシーケンスを共有します。

プロトコル

各アカウントに使用するプロトコルを選択します。すべてのピアツーピアアカウントは同じプロトコル設定を共有します。

RTP (RFC2833) を使用:RTPパケット内でDTMF (Dual-Tone Multi-Frequency) 信号などのトーン信号およびテレフォニーイベントを許可する場合は、オンにします。

[SIP INFO (RFC2976) を使用]:オンにして、SIPプロトコルにINFO方式を含めます。INFO方式で、必要に応じたアプリケーションのレイヤー情報 (通常はセッションに関連する情報) が追加されます。

呼び出しのテスト

SIPアカウント:テスト呼び出しを行うアカウントを選択します。

SIPアドレス:呼び出しのテストを行い、アカウントが動作していることを確認するには、SIPアドレスを入力し、 をクリックします。

ストレージ

ネットワークストレージ

Network storage（ネットワークストレージ）:オンにすると、ネットワークストレージを使用できます。

Add network storage (ネットワークストレージの追加):クリックして、録画を保存できるネットワーク共有を追加します。

- アドレス:ホストサーバーのホスト名 (通常はNAS (network-attached storage) またはIPアドレスを入力します。DHCPではなく固定IPアドレスを使用するようにホストを設定するか (動的IPアドレスは変わる可能性があるため、DHCPは使用しない)、DNS名を使用することをお勧めします。Windows SMB/CIFS名はサポートされていません。
- Network share (ネットワーク共有):ホストサーバー上の共有場所の名前を入力します。各Axis装置にはそれぞれのフォルダーがあるため、複数の装置で同じネットワーク共有を使用できます。
- User (ユーザー):サーバーにログインが必要な場合は、ユーザー名を入力します。特定のドメインサーバーにログインするには、`DOMAIN\username` を入力します。
- パスワード:サーバーにログインが必要な場合は、パスワードを入力します。
- SMB version (SMBバージョン):NASに接続するSMBストレージプロトコルのバージョンを選択します。[Auto (自動)] を選択すると、装置は、セキュアバージョンであるSMB3.02、3.0、2.1 のいずれかにネゴシエートを試みます。1.0または2.0を選択すると、上位バージョンをサポートしない旧バージョンのNASに接続できます。Axis装置でのSMBサポートの詳細については、こちらをご覧ください。
- Add share without testing (テストなしで共有を追加する):接続テスト中にエラーが検出された場合でも、ネットワーク共有を追加する場合に選択します。サーバーにパスワードが必要な場合でも、パスワードを入力しなかったなど、エラーが発生する可能性があります。

ネットワークストレージを削除する:クリックして、ネットワーク共有への接続をマウント解除、バインド解除、削除します。これにより、ネットワーク共有のすべての設定が削除されます。

Unbind (バインド解除):クリックして、ネットワーク共有をアンバインドし、切断します。
Bind (バインド):クリックして、ネットワーク共有をバインドし、接続します。

Unmount (マウント解除):クリックして、ネットワーク共有をマウント解除します。
Mount (マウント):クリックしてネットワーク共有をマウントします。

Write protect (書き込み禁止):オンに設定すると、ネットワーク共有への書き込みが停止され、録画が削除されないように保護されます。書き込み保護されたネットワーク共有はフォーマットできません。

Retention time (保存期間):録画の保存期間を選択し、古い録画の量を制限したり、データストレージに関する規制に準拠したりします。ネットワークストレージがいっぱいになると、設定した時間が経過する前に古い録画が削除されます。

ツール

- 接続をテストする:ネットワーク共有への接続をテストします。
- Format (形式):ネットワーク共有をフォーマットします。たとえば、すべてのデータをすばやく消去する必要があるときです。CIFSをファイルシステムとして選択することもできます。

Use tool (ツールを使用)クリックして、選択したツールをアクティブにします。

オンボードストレージ

重要

データ損失や録画データ破損の危険があります。装置の稼働中はSDカードを取り外さないでください。SDカードを取り外す前に、SDカードをマウント解除します。

Unmount (マウント解除):SDカードを安全に取り外す場合にクリックします。

Write protect (書き込み禁止):オンにすると、SDカードへの書き込みが防止され、録画が削除されなくなります。書き込み保護されたSDカードはフォーマットできません。

Autoformat (自動フォーマット):オンにすると、新しく挿入されたSDカードが自動的にフォーマットされます。ファイルシステムをext4にフォーマットします。

使用しない:オンにすると、録画のSDカードへの保存が停止します。SDカードを無視すると、装置はカードがあっても認識しなくなります。この設定は管理者のみが使用できます。

Retention time (保存期間):録画の保存期間を選択し、古い録画の量を制限したり、データストレージの規制に準拠したりします。SDカードがいっぱいになると、保存期間が切れる前に古い録画が削除されます。

ツール

- **Check (チェック)**:SDカードのエラーをチェックします。
- **Repair (修復)**:ファイルシステムのエラーを修復します。
- **Format (形式)**:SDカードをフォーマットしてファイルシステムを変更し、すべてのデータを消去します。SDカードはext4ファイルシステムにのみフォーマットすることができます。Windows®からファイルシステムにアクセスするには、サードパーティ製のext4ドライバーまたはアプリケーションが必要です。
- **Encrypt (暗号化)**:このツールを使用して、暗号化ありでSDカードをフォーマットします。これにより、SDカードに保存されているデータはすべて削除されます。SDカードに保存する新規データはすべて暗号化されます。
- **Decrypt (復号化)**:このツールを使用して、暗号化なしでSDカードをフォーマットします。これにより、SDカードに保存されているデータはすべて削除されます。SDカードに保存する新規データは暗号化されません。
- **Change password (パスワードの変更)**:SDカードの暗号化に必要なパスワードを変更します。

Use tool (ツールを使用)クリックして、選択したツールをアクティブにします。

Wear trigger (消耗トリガー):アクションをトリガーするSDカードの消耗レベルの値を設定します。消耗レベルは0～200%です。一度も使用されていない新しいSDカードの消耗レベルは0%です。消耗レベルが100%になると、SDカードの寿命が近い状態にあります。消耗レベルが200%に達すると、SDカードが故障するリスクが高くなります。消耗トリガーを80～90%の間に設定することをお勧めします。これにより、SDカードが消耗し切る前に、録画をダウンロードしたり、SDカードを交換したりする時間ができます。消耗トリガーを使用すると、イベントを設定し、消耗レベルが設定値に達したときに通知を受け取ることができます。

ONVIF

ONVIFアカウント

ONVIF (Open Network Video Interface Forum) は、エンドユーザー、インテグレーター、コンサルタント、メーカーがネットワークビデオ技術が提供する可能性を容易に利用できるようにするグローバルなインターフェース標準です。ONVIFによって、さまざまなベンダー製品間の相互運用、柔軟性の向上、コストの低減、陳腐化しないシステムの構築が可能になります。

ONVIFアカウントを作成すると、ONVIF通信が自動的に有効になります。装置とのすべてのONVIF通信には、アカウント名とパスワードを使用します。詳細については、*axis.com*にあるAxis開発者コミュニティを参照してください。

+ アカウントを追加:クリックして、新規のONVIFアカウントを追加します。

Account (アカウント):固有のアカウント名を入力します。

New password (新しいパスワード):アカウントのパスワードを入力します。パスワードの長は1~64文字である必要があります。印刷可能なASCII文字 (コード32～126) のみを使用できます。これには、英数字、句読点、および一部の記号が含まれます。

Repeat password (パスワードの再入力):同じパスワードを再び入力します。

Privileges (権限):

- Administrator (管理者):すべての設定へ全面的なアクセス権をもっています。管理者は他のアカウントを追加、更新、削除することもできます。
- Operator (オペレーター):次の操作を除く、すべての設定へのアクセス権があります。
  - すべての [System settings (システムの設定)]。
  - アプリを追加しています。
- Media account (メディアアカウント):ビデオストリームの参照のみを行えます。

⋮ コンテキストメニューは以下を含みます。

Update account (アカウントの更新):アカウントのプロパティを編集します。

Delete account (アカウントの削除):アカウントを削除します。rootアカウントは削除できません。

ONVIFメディアプロファイル

ONVIFメディアプロファイルは、メディアストリーム設定の変更に使用する一連の設定から構成されています。独自の設定を使用して新しいプロファイルを作成することも、設定済みのプロファイルを使用してすばやく設定することもできます。

メディアプロファイルを追加:クリックすると、新しいONVIFメディアプロファイルを追加できます。

プロファイル名:メディアプロファイルに名前を付けます。

Video source (ビデオソース):設定に使用するビデオソースを選択します。

- **Select configuration (設定の選択)**:リストからユーザー定義の設定を選択します。ドロップダウンリストに表示される設定は、マルチビュー、ビューエリア、バーチャルチャンネルなど、装置のビデオチャンネルに対応しています。

Video encoder (ビデオエンコーダ):設定に使用するビデオエンコード方式を選択します。

- **Select configuration (設定の選択)**:リストからユーザー定義の設定を選択し、エンコード方式の設定を調整します。ドロップダウンリストに表示される設定は、ビデオエンコーダの設定の識別子/名前となります。ユーザー0～15を選択して、独自の設定を適用します。または、デフォルトユーザーのいずれかを選択して、特定のエンコード方式の既定の設定を使用します。

注

装置で音声を有効にすると、音声ソースと音声エンコーダ設定を選択するオプションが有効になります。

音声ソース:設定に使用する音声入力ソースを選択します。

- **Select configuration (設定の選択)**:リストからユーザー定義の設定を選択し、音声設定を調整します。ドロップダウンリストに表示される設定は、装置の音声入力に対応しています。装置に1つの音声入力がある場合、それはuser0です。装置に複数の音声入力がある場合、リストには追加のユーザーが表示されます。

音声エンコーダ:設定に使用する音声エンコード方式を選択します。

- **Select configuration (設定の選択)**:リストからユーザー定義の設定を選択し、音声エンコード方式の設定を調整します。ドロップダウンリストに表示される設定は、音声エンコーダの設定の識別子/名前として機能します。

音声デコーダ:設定に使用する音声デコード方式を選択します。

- **Select configuration (設定の選択)**:リストからユーザー定義の設定を選択し、設定を調整します。ドロップダウンリストに表示される設定は、設定の識別子/名前として機能します。

音声出力:設定に使用する音声出力形式を選択します。

- **Select configuration (設定の選択)**:リストからユーザー定義の設定を選択し、設定を調整します。ドロップダウンリストに表示される設定は、設定の識別子/名前として機能します。

Metadata (メタデータ):設定に含めるメタデータを選択します。

- **Select configuration (設定の選択)**:リストからユーザー定義の設定を選択し、メタデータ設定を調整します。ドロップダウンリストに表示される設定は、メタデータの設定の識別子/名前となります。

PTZ: 設定に使用するPTZ設定を選択します。

- **Select configuration (設定の選択)**:リストからユーザー定義の設定を選択し、PTZ設定を調整します。ドロップダウンリストに表示される設定は、PTZをサポートする装置のビデオチャンネルに対応しています。

[**Create (作成)**]:クリックして、設定を保存し、プロファイルを作成します。

Cancel (キャンセル):クリックして、設定をキャンセルし、すべての設定をクリアします。

profile_x:プロファイル名をクリックして、既定のプロファイルを開き、編集します。

検知器

音声検知

これらの設定は、音声入力ごとに利用できます。

Sound level (音声レベル):音声レベルは0～100の範囲で調整します。0が最も感度が高く、100が最も感度が低くなります。音声レベルの設定時には、アクティビティインジケーターをガイドとして使用します。イベントを作成する際に、音声レベルを条件として使用することができます。音声レベルが設定値より高くなった場合、低くなった場合、または設定値を通過した場合にアクションを起こすように選択できます。

アクセサリー

I/Oポート

デジタル入力を使用すると、開回路と閉回路の切り替えが可能な外部装置 (PIRセンサー、ドアまたは窓の接触、ガラス破損検知器など) を接続できます。

デジタル出力を使用して、リレーやLEDなどの外部デバイスを接続します。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またはwebインターフェースから有効化できます。

ポート

名前:テキストを編集して、ポートの名前を変更します。

方向: は、ポートが入力ポートであることを示します。 は、出力ポートであることを示します。ポートが設定可能な場合は、アイコンをクリックして入力と出力を切り替えることができます。

標準の状態:開回路には を、閉回路には をクリックします。

現在の状態:ポートの現在のステータスを表示します。入力または出力は、現在の状態が通常の状態とは異なる場合に有効化されます。デバイスの接続が切断されているか、DC 1Vを超える電圧がかかっている場合に、デバイスの入力は開回路になります。

注

再起動中、出力回路は開かれます。再起動が完了すると、回路は正常位置に戻ります。このページの設定を変更した場合、有効なトリガーに関係なく出力回路は正常位置に戻ります。

監視済み :オンに設定すると、誰かがデジタルI/Oデバイスへの接続を改ざんした場合に、そのアクションを検出してトリガーできます。入力が開いているか閉じているかを検知するだけでなく、誰かが改ざんした場合 (つまり、切断または短絡) も検知することができます。接続を監視するには、外部I/Oループ内に追加のハードウェア (終端抵抗器) が必要です。

ログ

レポートとログ

レポート

- View the device server report (デバイスサーバーレポートを表示):製品ステータスに関する情報をポップアップウィンドウに表示します。アクセスログは自動的にサーバーレポートに含まれます。
- Download the device server report (デバイスサーバーレポートをダウンロード):これによって、UTF-8形式で作成された完全なサーバーレポートのテキストファイルと、現在のライブビュー画像のスナップショットを収めた.zipファイルが生成されます。サポートに連絡する際には、必ずサーバーレポート .zipファイルを含めてください。
- Download the crash report (クラッシュレポートをダウンロード):サーバーの状態に関する詳細情報が付随したアーカイブをダウンロードします。クラッシュレポートには、サーバーレポートに記載されている情報と詳細なバグ情報が含まれます。レポートには、ネットワークトレースなどの機密情報が含まれている場合があります。レポートの生成には数分かかることがあります。

ログ

- View the system log (システムログを表示):装置の起動、警告、重要なメッセージなど、システムイベントに関する情報をクリックして表示します。
- View the access log (アクセスログを表示):誤ったログインパスワードの使用など、本装置への失敗したアクセスをすべてクリックして表示します。
- View the audit log (監査ログを表示):クリックすると、ユーザーやシステムのアクティビティに関する情報 (認証の成否や設定など) が表示されます。

リモートシステムログ

syslogはメッセージログ作成の標準です。これによって、メッセージを生成するソフトウェア、メッセージを保存するシステム、およびそれらを報告して分析するソフトウェアを分離することができます。各メッセージには、メッセージを生成したソフトウェアの種類を示す設備コードがラベル付けされ、重大度レベルが割り当てられます。

＋ サーバー:クリックして新規サーバーを追加します。

[ホスト]:サーバーのホスト名またはIPアドレスを入力します。

Format (形式):使用するsyslogメッセージの形式を選択します。

- Axis
- RFC 3164
- RFC 5424

Protocol (プロトコル):使用するプロトコルを選択します。

- UDP (デフォルトポートは514)
- TCP (デフォルトポートは601)
- TLS (デフォルトポートは6514)

ポート:別のポートを使用する場合は、ポート番号を編集します。

重大度:トリガー時に送信するメッセージを選択します。

タイプ:送信するログのタイプを選択します。

Test server setup (テストサーバーセットアップ):設定を保存する前に、すべてのサーバーにテストメッセージを送信します。

CA証明書設定:現在の設定を参照するか、証明書を追加します。

プレイン設定

[Plain Config] (プレイン設定) は、Axis装置の設定経験のある上級ユーザー向けのページです。ほとんどのパラメーターは、このページから設定、編集することができます。

メンテナンス

メンテナンス

Restart (再起動):デバイスを再起動します。再起動しても、現在の設定には影響がありません。実行中のアプリケーションは自動的に再起動されます。

Restore (リストア):ほとんどの設定が工場出荷時の値に戻ります。その後、装置とアプリを再設定し、プリインストールしなかったアプリを再インストールし、イベントやプリセットを再作成する必要があります。

重要

復元後に保存される設定は以下の場合のみです。

- ブートプロトコル (DHCPまたは静的)
- 静的IPアドレス
- デフォルトのルータ
- サブネットマスク
- 802.1Xの設定
- O3C settings (O3Cの設定)
- DNSサーバーIPアドレス

Factory default (工場出荷時設定):すべての設定を工場出荷時の値に戻します。その後、装置にアクセス可能なIPアドレスをリセットする必要があります。

注

検証済みのソフトウェアのみを装置にインストールするために、すべてのAxisの装置のソフトウェアにデジタル署名が付け加えられます。これによって、Axis装置の全体的なサイバーセキュリティの最低ラインがさらに上がります。詳細については、*axis.com*でホワイトペーパー「Axis Edge Vault」を参照してください。

AXIS OS upgrade (AXIS OSのアップグレード):AXIS OSの新しいバージョンにアップグレードします。新しいリリースには、機能の改善やバグの修正、まったく新しい機能が含まれています。常にAXIS OSの最新のリリースを使用することをお勧めします。最新のリリースをダウンロードするには、*axis.com/support*に移動します。

アップグレード時には、以下の3つのオプションから選択できます。

- **Standard upgrade (標準アップグレード)**:AXIS OSの新しいバージョンにアップグレードします。
- **Factory default (工場出荷時設定)**:アップグレードすると、すべての設定が工場出荷時の値に戻ります。このオプションを選択すると、アップグレード後にAXIS OSを以前のバージョンに戻すことはできません。
- **Automatic rollback (自動ロールバック)**:設定した時間内にアップグレードを行い、アップグレードを確認します。確認しない場合、装置はAXIS OSの以前のバージョンに戻されます。

AXIS OS rollback (AXIS OSのロールバック):AXIS OSの以前にインストールしたバージョンに戻します。

トラブルシューティング

Reset PTR (PTRのリセット) :何らかの理由で、**パン**、**チルト**、または**ロール**の設定が想定どおりに機能していない場合は、PTRをリセットします。新品のカメラの場合、PTRモーターは常にキャリブレーションされています。しかし、カメラの電源が失われたり、モーターが手で動かされたりした場合など、キャリブレーションが失われることがあります。PTRをリセットすると、カメラは再キャリブレーションされ、工場出荷時の設定の位置に戻ります。

Calibration (キャリブレーション) :[Calibrate (キャリブレート)] をクリックすると、パン、チルト、ロールモーターがデフォルト位置に再較正されます。

Ping：Pingを実行するホストのホスト名またはIPアドレスを入力して、**[開始]** をクリックすると、デバイスから特定のアドレスへの通信経路が適切に機能しているかどうかを確認することができます。

ポートチェック：チェックするホスト名またはIPアドレスとポート番号を入力して、**[開始]** をクリックすると、デバイスから特定のIPアドレスとTCP/UDPポートへの接続が可能かどうかを確認することができます。

ネットワークトレース

重要

ネットワークトレースファイルには、証明書やパスワードなどの機密情報が含まれている場合があります。

ネットワークトレースファイルはネットワーク上のアクティビティを録画するので、トラブルシューティングに役立ちます。

Trace time (**追跡時間**):秒または分でトレースの期間を選択し、[**ダウンロード**] をクリックします。

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 57*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。これで本製品は工場出荷時の設定にリセットされました。ネットワーク上に利用可能なDHCPサーバーがない場合、デフォルトのIPアドレスは`192.168.0.90`になります
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。

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 > Maintenance actions (メンテナンス > メンテナンスアクション)**] に移動します。[**Restore (リストア)**] をクリックすると、工場出荷時の値にリセットされますが、IPアドレスは保持されます。[**Default (デフォルト)**] をクリックすると、IPアドレスを含むすべての値がリセットされます。

現在のファームウェアを確認する

ファームウェアは、ネットワーク装置の機能を決定するソフトウェアです。問題のトラブルシューティングを行う際には、まず現在のファームウェアバージョンを確認してください。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。

現在のファームウェアを確認するには:

1. デバイスのWebページで、[**Overview (概要)**] に移動します。
2. [**Firmware version (ファームウェアバージョン)**] を確認します。

ファームウェアのアップグレード

重要
事前設定済みの設定とカスタム設定は、ファームウェアのアップグレード時に保存されます (その機能が新しいファームウェアで利用できる場合)。ただし、この動作をAxis Communications ABが保証しているわけではありません。

重要
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
最新のファームウェアでデバイスをアップグレードすると、デバイスに最新機能が追加されます。ファームウェアを更新する前に、ファームウェアととも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。最新ファームウェアおよびリリースノートについては、*axis.com/support/firmware*を参照してください。

1. 最新のファームウェアファイルをコンピューターにダウンロードします。ファームウェアファイルは*www.axis.com/support/firmware*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. [System > Maintenance > Firmware upgrade (システム > メンテナンス > ファームウェアのアップグレード)] に移動し、ページの指示に従います。アップグレードが完了すると、デバイス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 54*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：小規模から中規模のシステムに最適です。30日間の試用版を無料で使用できます。

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。

パフォーマンスに関する一般的な検討事項

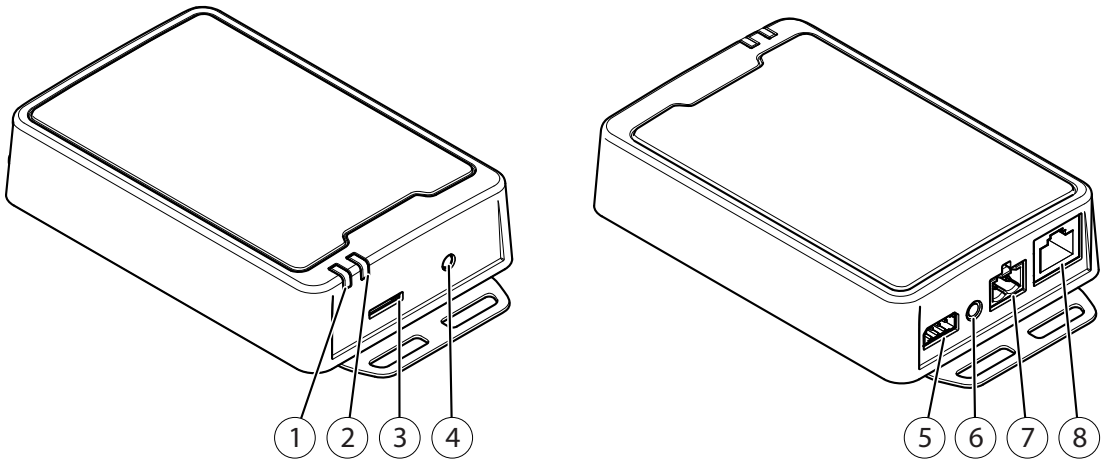
システムを設定する際には、さまざまな設定や条件が必要な帯域幅 (ビットレート) にどのように影響するかを検討することが重要です。

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。

仕様

製品概要



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

SPK LED	説明
緑	正常動作であれば緑色に点灯します。 インピーダンスのキャリブレーションが行われていない場合点滅します(緑色の短い点滅2回と長い消灯)。
赤	過電流保護が作動した場合、赤色で点滅します。

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を押して、インピーダンスのテストを実行します。コントロールボタンを押し続けると、スピーカーからトーン音が聞こえます。詳細については、*インピーダンスのテスト, on page 6*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 Plus (PoE+) 対応RJ45イーサネットコネクター

注意

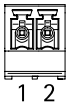
本製品は、シールドネットワークケーブル (STP) を使用して接続してください。本製品は、用途に合ったケーブルを使用してネットワークに接続してください。ネットワーク装置がメーカーの指示どおりに設置されていることを確認します。法的要件については、Axisのホームページ*www.axis.com*でインストールガイドを参照してください。

音声コネクター

- **音声入力** - 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。

	1 チップ	2 リング	3 スリーブ
音声入力	マイク/ライン入力	マイクロフォンバイアス電圧	アース

スピーカー出力のための2ピン端子ブロック。



機能	ピン	メモ
スピーカー出力 (-)	1	
スピーカー出力 (+)	2	

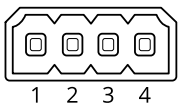
I/Oコネクター

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。

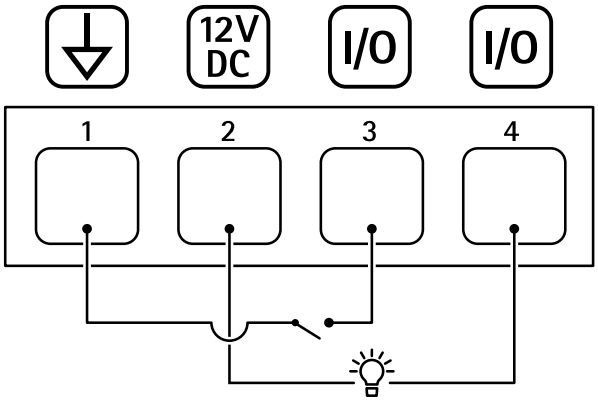
デジタル出力 - リレーやLEDなどの外部装置を接続します。接続された装置は、VAPIX®アプリケーションプログラミングインターフェースを通じたイベントまたは本装置のwebインターフェースから有効にすることができます。

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)*

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
```

T10135494_ja

2026-01 (M20.2)