# AXIS C15 Series

## AXIS C1510 Network Pendant Speaker

## AXIS C1511 Network Pendant Speaker

ユーザーマニュアル

## 目次

# ソリューションの概要

## ソリューションの概要

このマニュアルでは、デバイスを音声システムからアクセス可能にする方法と、デバイスをインターフェースから直接設定する方法 (たとえば、音声またはビデオ管理ソフトウェアを使用しないデバイスを使用する場合) 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 ユーザーズマニュアル*
- AXIS Camera Station - 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ユーザーズマニュアル*
- AXIS Companion - 小規模システム向けのビデオ管理ソフトウェアです。
  - *AXIS Companion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。

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。

*help.axis.com/?&piald=74869&section=solution-overview*

*ネットワーク音声の動作の概要。*

## 設置

### 設置


インストールガイド (pdf) をダウンロードする:

- AXIS C1510 Network Pendant Speaker

  *axis.com/products/axis-c1510/support#support-resources*
- AXIS C1511 Network Pendant Speaker

  *axis.com/products/axis-c1511/support#support-resources*

# はじめに

## はじめに

## ネットワーク上のデバイスを検索する

Windows®でAxisデバイスを探してIPアドレスの割り当てを行う方法については、AXIS IP Utilityまたはは AXIS Device Managerを使用してください。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装置を使用できます。

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

** iOS 15またはiPadOS 15でAXIS OS webインターフェースを使用するには、**[設定] > [Safari] > [詳細] > [Experimental Features]** に移動し、[NSURLSession Websocket] を無効にします。*

推奨ブラウザーの詳細については、*AXIS OSポータル*にアクセスしてください。

## 装置へのアクセス

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。
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。 *5 ページrootアカウントの新しいパスワードを設定する* 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、装置を工場出荷時の設定にリセットしてください。*44ページ工場出荷時の設定にリセットする* を参照してください。

## はじめに


*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。 *6 ページ安全なパスワード* 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. [**Save (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

Axisデバイスは、最初に設定されたパスワードをネットワーク上で平文で送信します。最初のログイン後にデバイスを保護するために、安全で暗号化されたHTTPS接続を設定してからパスワードを変更してください。

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される可能性があることから、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、次のことを強く推奨します。

- 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

### 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イス > 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、*47ページ製品の概要*を参照してください。

### ダイレクトSIP (P2P) を設定する

同じIPネットワーク内の少数のユーザーエージェント間で通信が行われ、PBXサーバーが提供する追加機能が必要ない場合は、ピアツーピアを使用します。P2Pの仕組みをよりよく理解するには、*14ページピアツーピアSIP (P2PSIP)*を参照してください 。

設定オプションの詳細については、*34ページ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. 装置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。メディア伝送用のデフォルトの開始ポートは4000です。一部のファイア

ウォールでは、特定のポート番号のポートを経由する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、*15ページNATトラバーサル*を参照してください。

6. [Audio (音声)] で望ましい音声品質で、SIP呼び出しの音声コーデックを1つ以上選択します。ドラッグアンドドロップして、優先順位を変更します。
7. [Additional (追加)] で、追加のオプションを選択します。
   - **UDP-to-TCP switching (UDP からTCPへの切り替え)** – 通話でトランスポートプロトコルをUDP (User Datagram Protocol) からTCP (Transmission Control Protocol) に一時的に切り替えることを許可するかどうかを選択します。切り替えるのはフラグメンテーションを避けるためであり、要求が200バイト以内または1300バイト以上の最大転送ユニット (MTU) の場合に実行されます。
   - **Allow via rewrite (経由のリライトを許可)** – ルーターのパブリックIPアドレスではなく、ローカルIPアドレスを送信する場合に選択します。
   - **Allow contact rewrite (連絡先書き換えの許可)** – ルーターのパブリックIPアドレスではなく、ローカルIPアドレスを送信する場合に選択します。
   - **Register with server every (サーバーへの登録を毎回行う)** – 既存のSIPアカウントで、デバイスをSIPサーバーに登録する頻度を設定します。
   - **DTMF payload type (DTMFの積載タイプ)** – DTMFのデフォルトの積載タイプを変更します。
8. [Save (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)

PBXサーバーは、IPネットワークの内外で無制限の数のユーザーエージェントの間で通信を行う必要があるときに使用します。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、*14ページ構内交換機 (PBX)*を参照してください 。

設定オプションの詳細については、*34ページ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。
   - User ID (ユーザーID)
   - Domain (ドメイン)
   - Password (パスワード)
   - Authentication ID (認証ID)
   - Caller ID (呼び出しID)
   - Registrar (レジストラ)
   - RTP start port (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. [**Save (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、*7 ページダイレクトSIP (P2P) を設定する* で解説しています。

## 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、ガイド「*イベントのルールの使用開始*」を参照してください。

### スピーカーテストが失敗した場合に電子メールを送信する

この例では、音声デバイスは、スピーカーテストが失敗したときに定義済みの送信先に電子メールを送信するように設定されています。スピーカーテストは、毎日18:00に実行するように設定されています。

1. スピーカーテストのスケジュールを設定する方法:
   1.1 [device interface (デバイスインターフェース)] > [**System (システム)**] > [**Events (イベント)**] > [**Schedules (スケジュール)**] に移動します。
   1.2 毎日 18:00 に開始し、18:01 に終了するスケジュールを作成します。「毎日午後6時」と名付けます。
2. 電子メールの送信先を作成する:
   2.1 [device interface > **System** > **Events** > **Recipients** (デバイスインターフェイス > 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 [**Save (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イス > 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 [Save (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イス > 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、[保存] をクリックします。

## カメラが動きを検知したときに音声を再生する

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

**前提条件**

- 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. 音声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 音声クリップに対して ⋮ > [Create link (リンクの作成)] を順にクリックします。

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. アクションルールを作成する:

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 [Save (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 ⋮ > 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. [Save (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. [Save (保存)] をクリックします。

## 追加設定

### 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 > System > Events > Rules (設定 > システム > イベント > ルール)**] に移動し、ルールを追加します。
2. ルールの名前を入力します。
3. 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. アクションの一覧で、[**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 > System > Events > Rules (設定 > システム > イベント > ルール)**] に移動し、ルールを追加します。
2. ルールの名前を入力します。
3. 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。

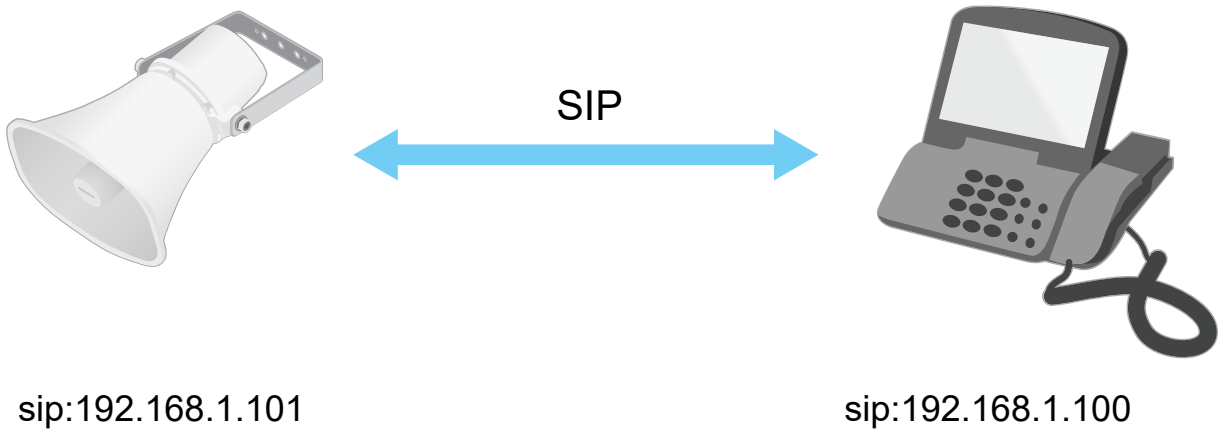
実際の音声またはビデオは、RTP (Real-time Transport Protocol) などのトランスポートプロトコルを使用して、SIPユーザーエージェントの間で交換されます。

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)

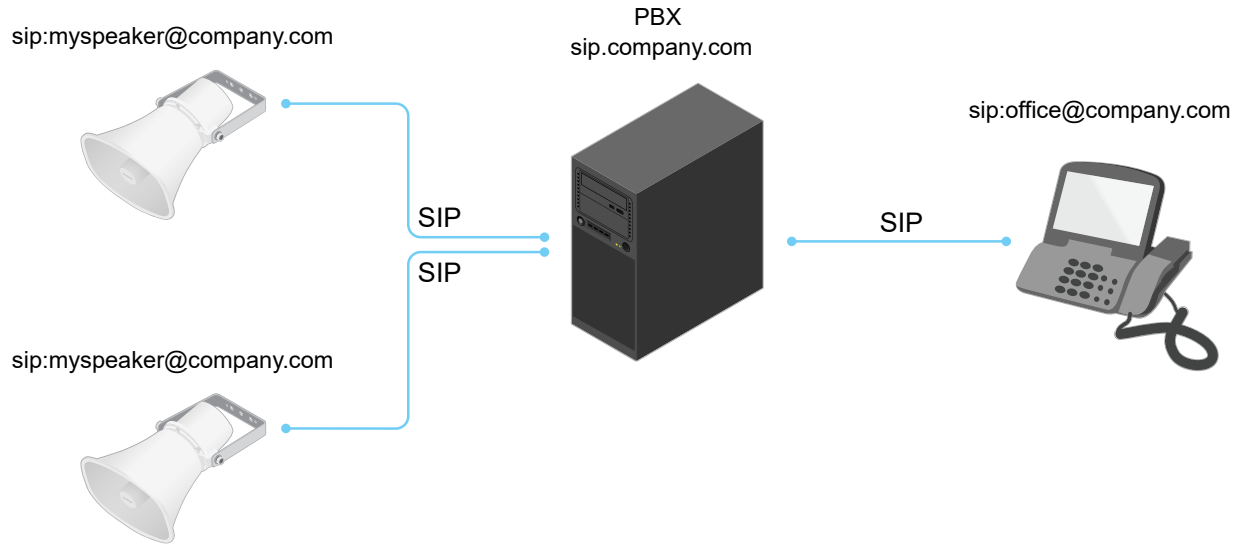
ローカルIPネットワークの外部でSIP呼び出しを行うときは、構内交換機 (PBX) をセンターハブとして機能させることができます。PBXの主要コンポーネントはSIPサーバーです。これは、SIPプロキシーまたはレジストラとも呼ばれます。PBXは従来の電話交換台のように動作します。クライアントの現在の状態を表示し、呼転送、ボイスメール、リダイレクトなどを行うことができます。

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アドレスから独立しており、PBXによって、PBXに登録されている限り装置はアクセス可能になります。

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、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。

## アプリケーション

アプリケーションを使用することで、Axis装置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装置向けの分析アプリケーションやその他のアプリケーションの開発を可能にするオープンプラットフォームです。アプリケーションには、装置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アプリケーションのユーザーマニュアルについては、*help.axis.com*を参照してください。

## webインターフェース

### 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。
- **Change account (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。
- **Log out (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**: ファームウェアのバージョンとシリアル番号を含む装置情報を表示します。

## ステータス

#### セキュリティ

アクティブな装置へのアクセスのタイプと、使用されている暗号化プロトコルを表示します。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。

**Hardening guide (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。

#### 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 [**Date and time (日付と時刻)**] のページに移動します。

#### 装置情報

ファームウェアのバージョンとシリアル番号を含む装置情報を表示します。

Upgrade firmware (ファームウェアのアップグレード): 装置のファームウェアをアップグレードします。ファームウェアの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。

Connected clients (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、各クライアントのIPアドレス、プロトコル、ポート、PID/プロセスが表示されます。

## 音声

### 概要

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。

Calibrate (キャリブレーション) : スピーカーのキャリブレーションを行います。

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

### 装置の設定

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。

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。

Input type (入力タイプ) : 入力のタイプを選択します。

Power type (電源タイプ) : 電源のタイプを選択します。

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。

### ストリーム

Encoding (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

+ **Add clip (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)**: 音声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。
- **Delete (削除)**: 装置から音声クリップを削除します。

### 聴く/録る

▶ 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。録音を停止するには、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。

### 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。

### スピーカーテスト

スピーカーテストを使用して、リモートからスピーカーが意図したとおりに動作することを確認できます。

**Calibrate (キャリブレーション)**: 最初のテストの前にスピーカーのキャリブレーションを行う必要があります。キャリブレーション時には、スピーカーから一連のテストトーンが再生され、それが内蔵マイクロフォンで登録されます。スピーカーのキャリブレーションを行う場合は、スピーカーを最終位置に取り付ける必要があります。後日、スピーカーを移動したり、壁の新設や撤去など周囲の環境が変わったりした場合は、スピーカーの再キャリブレーションが必要です。

**テストを実行**: キャリブレーション時に再生されたのと同じ一連のテストトーンを再生し、キャリブレーションの登録された値と比較します。

## 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。

Source (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。

Storage (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。

Ongoing recordings (進行中の録画): カメラで進行中のすべての録画を表示します。

カメラ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。

カメラでの録画を停止します。

**トリガーされた録画**は、手動で停止したとき、またはカメラ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。カメラがシャットダウンされた場合でも、録画はカメラ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。

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

+ **Add app (アプリの追加)**: 新しいアプリをインストールします。

**Find more apps (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。

**Allow unsigned apps (署名なしアプリを許可)**: 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。

**Allow root-privileged apps (root権限アプリの許可)**: オンにして、root権限を持つアプリに装置へのフルアクセスを許可します。

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。

**Open (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。ライセンスキーを生成するには、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、ライセンスは装置から削除されます。
- **Settings (設定)**: パラメーターを設定します。
- **Delete (削除)**: 装置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

### 時間と場所

#### 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 (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。
- **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。
- **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。
- **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。

**Time zone (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。

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、マップ上に装置を配置できます。

- **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**: 装置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**: 分かりやすい装置名を入力します。
- **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)**: 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。ほとんどのネットワークでは、自動IP (DHCP) をお勧めします。

**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、固定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。

**Subnet mask (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。

Hostname (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。

**Hostname (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 servers (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。

HTTPおよび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。暗号化された情報の交換は、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証明書の使用により制御されます。

装置で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 > Security (システム > 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。

**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**®: オンにすると、ネットワーク上で自動検出が可能になります。

**Bonjour name (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。デフォルト名は装置名とMACアドレスです。

**UPnP**®: オンにすると、ネットワーク上で自動検出が可能になります。

**UPnP name (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。デフォルト名は装置名とMACアドレスです。

**WS-Discovery**: オンにすると、ネットワーク上で自動検出が可能になります。

### One-Click Cloud Connection (ワンクリッククラウド接続)

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)**:

- **One-click (ワンクリック)**: デフォルトの設定です。インターネットを介してO3Cサービスに接続するには、装置のコントロールボタンを押し続けます。コントロールボタンを押してから24時間以内に装置をO3Cサービスに登録する必要があります。登録しない場合、装置はO3Cサービスから切断されます。装置を登録すると、[**Always (常時)**] が有効になり、装置はO3Cサービスに接続されたままになります。
- **Always (常時)**: 装置は、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。装置を登録すると、装置はO3Cサービスに接続したままになります。装置の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。
- **No (なし)**: O3Cサービスを無効にします。

**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。

**Host (ホスト)**: プロキシサーバーのアドレスを入力します。

**Port (ポート)**: アクセスに使用するポート番号を入力します。

**Login (ログイン)** と**Password (パスワード)**: 必要な場合は、プロキシ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)**

- **Basic (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。
- **Digest (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。
- **Auto (オート)**: このオプションを使用すると、装置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。**Digest (ダイジェスト)** 方式が**Basic (ベーシック)** 方式より優先されます。

**Owner authentication key (OAK) (所有者認証キー、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、装置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 (パブリック)**] 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。デフォルト値は [**write (書き込み)**] です。
  - **Activate traps (トラップの有効化)**: オンにすると、トラップレポートが有効になります。装置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)**: 装置の起動時にトラップメッセージを送信します。
  - **Warm start (ウォームスタート)**: SNMP設定が変更されたときに、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。
  - **Authentication failed (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。
  - **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、装置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、ネットワーク上の装置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

装置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。

リスト内の証明書をフィルターします。

**証明書の追加**: クリックして、証明書を追加します。

- **More (詳細)** : 入力または選択するフィールドをさらに表示します。
- **Secure keystore (セキュアキーストア)**: [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/en-us/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** :

- **セキュアエレメント (CC EAL6+)**: 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。

### 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装置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。

**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、装置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。

**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 certificate (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、装置は、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 identity (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 version (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。

Prevent brute-force attacks (ブルートフォース攻撃を防ぐ)

Blocking (ブロック): オンにすると、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。ページレベルと装置レベルの両方で許容される失敗の数を設定できます。

IP address filter (IPアドレスフィルター)

Use filter (フィルターを使用する): 装置へのアクセスを許可するIPアドレスを絞り込む場合に選択します。

Policy (ポリシー): 特定のIPアドレスに対してアクセスを [Allow (許可)] するか [Deny (拒否)] するかを選択します。

Addresses (アドレス): 装置へのアクセスを許可するIP番号と拒否するIP番号を入力します。CIDR形式を使用できます。

カスタム署名されたファームウェア証明書

Axisのテストファームウェアまたは他のカスタムファームウェアを装置にインストールするには、カスタム署名付きファームウェア証明書が必要です。証明書は、ファームウェアが装置の所有者とAxisの両方によって承認されたと証明します。ファームウェアは、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、カスタム署名付きファームウェア証明書は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。ファーム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。

## アカウント

アカウント

+ Add account (アカウントの追加): 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。パスワードの長さは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持っています。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 (システム設定)]。
- アプリを追加しています。

• **ビューア**: 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。

### Anonymous access (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。

Allow anonymous PTZ operating (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アカウントの追加): クリックして、新しいSSHアカウントを追加します。

- Restrict root access (rootアクセスを制限する): オンにすると、rootアクセスを必要とする機能が制限されます。
- Enable SSH (SSHの有効化): SSHサービスを使用するには、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。パスワードの長さは1～64文字である必要があります。パスワードには、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。

### OpenID 設定

重要

正しい値を入力すると、装置に再度ログインできます。

**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)**: 管理者ロールの値を入力します。

**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)**: オペレーターロールの値を入力します。

**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)**: 閲覧者ロールの値を入力します。

**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。

**+ Add a rule (ルールの追加)**: ルールを作成します。

**Name (名前)**: 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。

**+ Add a condition (条件の編集)**: 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: 録画**: 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、音声装置の前面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。

**事前アナウンスのトーン: 着信呼び出しでトーンを再生する:** 音声装置に対してSIP呼び出しが行われると、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。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。

**事前アナウンスのトーン: 着信呼び出しトーンの後で呼び出しに応答する:** 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**: 音声装置に対して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。

### Recipients (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。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。

**+ Add a recipient (送信先の追加)**: クリックすると、送信先を追加できます。

**Name (名前)**: 送信先の名前を入力します。

**Type (タイプ)**: リストから選択します:

- **FTP**
  - **Host (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。
  - **Port (ポート)**: FTPサーバーに使用するポート番号を入力します。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。
  - **Password (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。
  - Password (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。
  - Password (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。
- Network storage (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。
  - Host (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。
  - Share (共有): ホスト上の共有の名前を入力します。
  - 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。
  - Password (パスワード): ログインのパスワードを入力します。
- SFTP
  - Host (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。
  - Port (ポート): SFTPサーバーに使用するポート番号を入力します。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。
  - Password (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。
  - From SIP account (送信元のSIPアカウント): リストから選択します。
  - To SIP address (送信先のSIPアドレス): SIPアドレスを入力します。

- Test (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。
- Email (電子メール)
  - Send email to (電子メールの送信先): 電子メールの送信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。
  - Send email from (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。
  - Password (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。
  - Port (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。デフォルト値は587です。
  - Encryption (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、スケジュールに従って送信された電子メールなどの受信を防止したり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、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
  - Host (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。
  - Port (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。

+ Add schedule (スケジュールの追加): 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。これは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装置を接続するために、さまざまな業界で使用されています。Axis装置のファーム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。

装置をMQTTクライアントとして設定します。MQTT通信は、クライアントとブローカーという2つのエンティティに基づいています。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ポータル*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 client (MQTTクライアント)

**Connect (接続)**: 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。

**Broker (ブローカー)**

**Host (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。

**Port (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オーバー WebSocket** のデフォルト値です。
- 443は**MQTTオーバー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。

**Password (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。

**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。

**Connect message (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 publication (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 topic name (トピック名を含める)**: 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 topic namespaces (トピックの名前空間を含める)**: 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。

**+** **条件の追加**: 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の追加**: 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 overlays (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の追加)**: 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

### Settings (設定)

SIP (Session Initiation Protocol) 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。

**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。

**Allow incoming calls (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て、その他のSIP装置からの着信呼び出しを許可します。

**Call handling (呼び出し処理)**

- **Calling timeout (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。

**Ports (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**: SIP呼び出しの最初のRTPメディアストリームで使用す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。一部のファイアウォールでは、特定のポート番号のポートを経由するRTPトラフィックをブロックします。

**NAT traversal (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。

**Audio (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。

Accounts (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。

+ Add account (アカウントの追加): クリックして、新しいSIPアカウントを作成します。

- Active (アクティブ): アカウントを使用できるようにします。
- Make default (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。
- [Answer automatically (自動応答)]: 選択すると、着信呼び出しに自動的に応答します。
- Prioritize IPv6 over IPv4 (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。
- Name (名前): わかりやすい名前を入力します。姓名、役職、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。
- User ID (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。
- Peer-to-peer (Peer-to-peer): 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装置への呼び出しに使用します。
- ドメイン (Domain): 利用可能であれば、パブリックドメイン名を入力します。これは、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。
- Password (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。
- Authentication ID (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。
- Caller-ID (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。
- Registrar (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。
- SIP secure (SIPセキュア): 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。
- Proxies (プロキシ)
  - + Proxy (プロキシ): 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。
  - Password (パスワード): 必要であればSIPプロキシ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。
  - Resolution (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。
  - Frame rate (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 profile (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

+ Add sequence (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。

Sequence (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。

Use RTP (RFC2833) (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。

Test call (呼び出しのテスト)

SIP account (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 address (SIP address): 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。

マルチキャストコントローラー

Use multicast controller (マルチキャストコントローラーを使用): オンにすると、マルチキャストコントローラーが有効になります。

Audio codec (音声コーデック): 音声コーデックを選択します。

+ Source (ソース): 新しいマルチキャストコントローラーソースを追加します。

- ラベル: ソースでまだ使用されていないラベルの名前を入力します。
- Source (ソース): ソースを入力します。
- Port (ポート): ポートを入力します。
- [Priority (優先度)]: 優先度を選択します。
- Profile (プロファイル): プロファイルを選択します。
- SRTP key (SRTPキー): SRTPキーを入力します。

⋮ コンテキストメニューは以下を含みます。

Edit (編集): マルチキャストコントローラーソースを編集します。

Delete (削除): マルチキャストコントローラーソースを削除します。

### ストレージ

Network storage (ネットワークストレージ)

Ignore (使用しない): オンに設定すると、ネットワークストレージを使用しません。

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。

- Address (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` (ドメイン\ユーザー名) を入力します。
- Password (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SMB 3.02、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。
- 接続テストが失敗しても共有を追加する: 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 (アンバインド): 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。書き込み禁止の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。

Tools (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 (フォーマット)**: 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)**: オンに設定にすると、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、データストレージに関する規制に準拠したりします。SDカード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。

Tools (ツール)

- **Check (チェック)**: SDカードのエラーをチェックします。これは、ext4ファイルシステムの場合にのみ機能します。
- **Repair (修復)**: ext4ファイルシステムのエラーを修復します。VFAT形式のSDカードを修復するには、SDカードを取り出して、コンピューターに挿入し、ディスクの修復を実行します。
- **Format (フォーマット)**: ファイルシステムを変更したり、すべてのデータをすばやく消去したりする必要があるときなどは、SDカードをフォーマットします。使用可能なファイルシステムオプションは、vFATとext4の2つです。カードの排出や突然の停電によるデータ損失に対する回復力があるため、ext4でのフォーマットをお勧めします。ただし、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。**Encrypt (暗号化)** 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。[**Encrypt (暗号化)**] の使用後、SDカードに保存されているデータは暗号化により保護されます。
- **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。**Decrypt (復号化)** 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。[**Decrypt (復号化)**] の使用後、SDカードに保存されるデータは暗号化により保護されません。
- **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、ネットワークビデオテクノロジーを利用するエンドユーザー、インテグレーター、コンサルタント、メーカーが、その技術を容易に活用できるようにするためのグローバルなインターフェース規格です。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*でAxis開発者コミュニティを参照してください。

+ **Add accounts (アカウントの追加)**: 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。パスワードの長さは1～64文字である必要があります。パスワードには、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。

**Role (役割)**:

- **Administrator (管理者)**: すべての設定へのフルアクセスが許可されています。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 (システム)**] 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。

+ **メディアプロファイルの追加**: 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。

**profile_x**: 編集するプロファイルをクリックします。

## 検知

### Audio detection (音声検知)

以下の設定は、音声入力ごとに指定できます。

**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 ports (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またはwebインターフェースから有効化できます。

Port (ポート)

**Name (名前)**: テキストを編集して、ポートの名前を変更します。

**Direction (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。

**Normal state (標準の状態)**: 開回路には を、閉回路には をクリックします。

**Current state (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。装置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、装置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。

**状態監視** : オンにすると、誰かがデジタルI/O装置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

Reports (レポート)

- **View the device server report (装置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 (装置サーバーレポートをダウンロード)**: 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ファイルを生成します。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。

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、[**Download (ダウンロード)**] をクリックします。

### 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。

+ **Server( サーバー)**: クリックして新規サーバーを追加します。

**Host (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 (フォーマット)**: 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とポートを選択します。

- 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)

**重大度**: トリガー時に送信するメッセージを選択します。

**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。

## 保守

**Restart (再起動)**: 装置を再起動します。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PTZプリセットを再作成する必要があります。

重要

リストア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)
- 静的なIPアドレス
- Default router (デフォルトルーター)
- Subnet mask (サブネットマスク)
- 802.1X settings (802.1Xの設定)
- O3C settings (O3Cの設定)

**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

検証済みのファーム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の装置ファーム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「署名済みファームウェア、セキュアブート、および秘密鍵のセキュリティ」を参照してください。

**Firmware upgrade (ファームウェアのアップグレード)**: 新しいファームウェアバージョンにアップグレードします。新しいファームウェアには、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)**: 新しいファームウェア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以前のファームウェアバージョンに戻すことはできません。
- **Autorollback (オートロールバック)**: 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、装置は以前のファームウェアバージョンに戻されます。

**Firmware rollback (ファームウェアのロールバック)**: 以前にインストールされたファームウェアバージョンに戻します。

# 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、以下の手順を実行します。

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。*47ページ製品の概要*を参照してください。
3. ステータスLEDが再びオレンジ色に変わるまで、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離します。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。

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。

## 現在のファームウェアバージョンの確認

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は、まず現在のファームウェアバージョンを確認することをお勧めします。最新のファームウェアバージョンには、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、以下の手順に従います。

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 (装置情報)**] でファームウェアバージョンを確認してください。

## 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。
- 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最新のファームウェア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。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. 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*axis.com/support/firmware*から無料で入手できます。

2. 装置に管理者としてログインします。
3. [Maintenance (メンテナンス) > Firmware upgrade (ファームウェアのアップグレード)] に移動し、[Upgrade (アップグレード)] をクリックします。

アップグレードが完了すると、製品は自動的に再起動します。

## 技術的な問題、ヒント、解決策

ここ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 | Axis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)。<br>• もし、「`Reply from <IPアドレス>: 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。<br>• もし、「`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が有効なときは、正しいプロトコル (HTTPまたはHTTPS) を使用してログインしてください。ブラウザーのアドレスフィールドに、手動で「`http`」または「`https`」と入力する必要がある場合があります。<br><br>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。*44ページ工場出荷時の設定にリセットする*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。 |
| 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。[**Settings > System > Date and time (設定 > システム > 日付と時刻)**] にアクセスします。 |

### デバイスにローカルにアクセスできるが、外部からアクセスできない

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

- AXIS Camera Station: 30日間の試用版を無料で使用でき、中小規模のシステムに最適です。

手順とダウンロードについては、*axis.com/vms*を参照してください。

### 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。<br>• 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。<br>• 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。<br>• 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

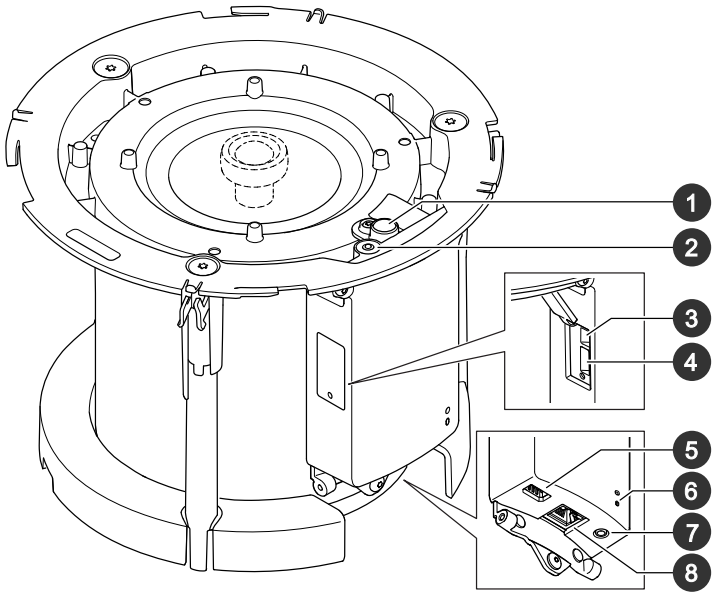
システムを設定する際には、さまざまな設定や条件が必要な帯域幅 (ビットレート) にどのように影響するかを検討することが重要です。

最も重要な検討事項には次のようなものがあります。

- 貧弱なインフラによるネットワークの使用率が高いと帯域幅に影響します。
- 複数の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

### 製品の概要




*1 正面LED*
*2 48ページコントロールボタン*
*3 48ページマイクロフォンを無効にするスイッチ*
*4 48ページSDカードスロット*
*5 49ページI/Oコネクター*
*6 ステータスLED*
*7 48ページ音声コネクター*
*8 48ページ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 |
|---|---|
| 消灯 | 正常動作の場合消灯します。 |
| 緑 | 正常動作の場合、緑色に点灯します。 |
| オレンジ | 起動時、設定のリストア時に点灯します。 |
| 赤 | アップグレードに失敗した場合に、ゆっくり点滅します。 |
| 赤/緑 | 音声デバイスが選択されていることが確認されると、赤/緑で素早く点滅します。 |

## SDカードスロット

**注意**

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

推奨するSDカードについては、*axis.com*を参照してください。

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

## ボタン

### コントロールボタン

コントロールボタンは、以下の用途で使用します。

- スピーカーテストのキャリブレーションを行う。コントロールボタンを押して離すと、テストトーンが再生されます。
- 製品を工場出荷時の設定にリセットする。*44ページ工場出荷時の設定にリセットする*を参照してください。

### マイクロフォンを無効にするスイッチ

マイクロフォンを無効にするスイッチの場所については、*47ページ製品の概要*を参照してください。

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

## コネクター

### ネットワークコネクター

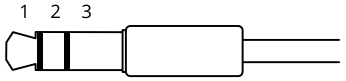
Power over Ethernet (PoE) 対応RJ45イーサネットコネクター

**注意**

本製品は、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** - ステレオマイクロフォンまたはライン入力ステレオ信号用3.5 mm入力。




音声入力

## 仕様

| 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 | 選択されている場合、エレクトレット電源 | グランド |
| バランス型マイクロフォン (ファントム電源あり、なし) またはライン、「ホット」信号 | バランス型マイクロフォン (ファントム電源あり、なし) またはライン、「コールド」信号 | グランド |
| デジタル信号 | 選択されている場合、リング電源 | グランド |
| アンバランス型ステレオマイクロフォン (エレクトレット電源あり、なし) またはライン、「左」 | アンバランス型ステレオマイクロフォン (エレクトレット電源あり、なし) またはライン、「右」 | グランド |

**音声出力**

| 1 チップ | 2 リング | 3 スリーブ |
|---|---|---|
| チャンネル1、アンバランス型ライン、モノラル | チャンネル1、アンバランス型ライン、モノラル | グランド |
| バランス型ライン、「ホット」信号 | バランス型ライン、「コールド」信号 | グランド |
| アンバランス型ステレオライン、「左」 | アンバランス型ステレオライン、「右」 | グランド |
| チャンネル1、アンバランス型ライン | チャンネル2、アンバランス型ライン | アース |

デフォルトでは内蔵マイクロフォンが使用され、外部マイクロフォンを接続すると、外部マイクロフォンが使用されます。

### I/Oコネクター

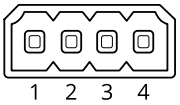
I/Oコネクターに外部装置を接続し、動体検知、イベントトリガー、アラーム通知などと組み合わせて使用することができます。I/Oコネクターは、0 V DC基準点と電力 (12 V DC出力) に加えて、以下のインターフェースを提供します。

**デジタル入力** - 開回路と閉回路の切り替えが可能なデバイス (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** - 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

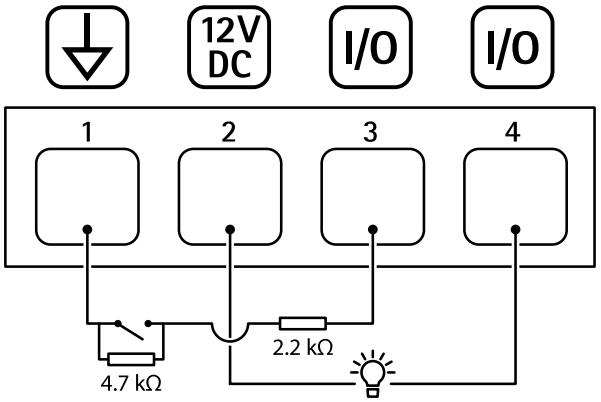



| 機能 | ピン | 備考 | 仕様 |
|---|---|---|---|
| DCアース | 1 | | 0 V DC |

## 仕様

| | | | |
|---|---|---|---|
| DC出力 | 2 | 補助装置の電源供給に使用できます。<br>注: このピンは、電源出力としてのみ使用できます。 | 12 V DC<br>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 V DC (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 V DC (最大)、オープンドレイン、100 mA |

例:




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

# APIコマンド

## 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:
デバイスの再起動

**リクエスト**
http://<deviceIP>/axis-cgi/restart.cgi

例:
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。

**リクエスト**
http://<deviceIP>/axis-cgi/factorydefault.cgi

例:
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。

**リクエスト**
http://<deviceIP>/axis-cgi/hardfactorydefault.cgi

例:
すべてのデバイスパラメーターのリストを表示します。

**リクエスト**
http://<deviceIP>/axis-cgi/param.cgi?action=list

例:
デバッグアーカイブを取得します

**リクエスト**
http://<deviceIP>/axis-cgi/debug/debug.tgz

例:
サーバーレポートを取得します

**リクエスト**
http://<deviceIP>/axis-cgi/serverreport.cgi

例:
300秒のネットワークトレースをキャプチャーします

**リクエスト**
http://<deviceIP>/axis-cgi/debug/debug.tgz?cmd=pcapdump&duration=300

例:
FTPを有効にします

## APIコマンド

**リクエスト**
`http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.FTP.Enabled=yes`

例:
FTPを無効にします

**リクエスト**
`http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.FTP.Enabled=no`

例:
SSHを有効にします

**リクエスト**
`http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.SSH.Enabled=yes`

例:
SSHを無効にします

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

ユーザーマニュアル
AXIS C15 Series

バージョン M5.2
日付: 2023年9月
製品番号 T10177746