

# AXIS A9210 Network I/O Relay Module

## 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](http://axis.com/support)からダウンロードできます。

IPアドレスの検索や割り当てを行う方法の詳細については、*IPアドレスの割り当てとデバイスへのアクセス方法を参照してください。*

### ブラウザーサポート

以下のブラウザーでデバイスを使用できます。

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

✓: 推奨:

\*: 制限付きでサポート

### 装置のwebインターフェースを開く

1. ブラウザーを開き、Axis装置のIPアドレスまたはホスト名を入力します。本製品のIPアドレスが不明な場合は、AXIS IP UtilityまたはAXIS Device Managerを使用して、ネットワーク上で装置を見つけます。
2. ユーザー名とパスワードを入力します。装置に初めてアクセスする場合は、管理者アカウントを作成する必要があります。管理者アカウントを作成する、*on page 2*を参照してください。

装置のwebインターフェースにあるすべてのコントロールとオプションの説明については、*webインターフェース, on page 6*を参照してください。

### 管理者アカウントを作成する

装置に初めてログインするときには、管理者アカウントを作成する必要があります。

1. ユーザー名を入力してください。
2. パスワードを入力します。安全なパスワード、*on page 3*を参照してください。
3. パスワードを再入力します。
4. 使用許諾契約書に同意します。
5. [ **Add account (アカウントを追加)** ] をクリックします。

#### 重要

装置にはデフォルトのアカウントはありません。管理者アカウントのパスワードを紛失した場合は、装置をリセットする必要があります。工場出荷時の設定にリセットする、*on page 44*を参照してください。

## 安全なパスワード

### 重要

ネットワーク上でパスワードやその他の機密設定を行う場合は、HTTPS (デフォルトで有効になっています) を使用してください。HTTPSを使用すると、安全で暗号化された形でネットワークに接続できるため、パスワードなどの機密データを保護できます。

デバイスのパスワードは主にデータおよびサービスを保護します。Axisデバイスは、さまざまなタイプのインストールで使用できるようにするためパスワードポリシーを強制しません。

データを保護するために、次のことが強く推奨されています。

- 8文字以上のパスワードを使用する (できればパスワード生成プログラムで作成する)。
- パスワードを公開しない。
- 一定の期間ごとにパスワードを変更する (少なくとも年に1回)。

## デバイスのソフトウェアが改ざんされていないことを確認する

装置に元のAXIS OSが搭載されていることを確認するか、またはセキュリティ攻撃が行われた後に装置を完全に制御するには、以下の手順に従います。

1. 工場出荷時の設定にリセットします。工場出荷時の設定にリセットする, on page 44を参照してください。  
リセットを行うと、セキュアブートによって装置の状態が保証されます。
2. デバイスを設定し、インストールします。

## webインターフェースの概要

このビデオでは、装置のwebインターフェースの概要について説明します。



Axis装置のwebインターフェース

## デバイスを構成する

### I/Oポートを設定する

1. [Device > I/Os and relays > AXIS A9210 > I/Os (装置 > I/Oとリレー > AXIS A9210 > I/O)] に移動します。
  2.  をクリックすると、I/Oポート設定が展開されます。
  3. ポートの名前を変更します。
  4. 通常の状態を設定します。開回路には  を、閉回路には  をクリックします。
  5. I/Oポートを入力として設定するには:
    - 5.1. [Direction (方向)] で、 をクリックします。
    - 5.2. 入力状態を監視するには、[Supervised (状態監視)] をオンにします。監視入力, on page 43を参照してください。
- 注**  
APIでは、状態監視I/Oポートと状態監視入力ポートは異なる動作をします。詳細については、「VAPIX®ライブラリ」を参照してください。
6. I/Oポートを出力として設定するには:
    - 6.1. [Direction (方向)] で、 をクリックします。
    - 6.2. 接続された装置を有効および無効にするためのURLを表示するために、[Toggle port URL (ポートURLを切り替え)] に移動します。

### リレーを設定する

1. [Device > I/Os and relays > AXIS A9210 > Relays (装置 > I/Oとリレー > AXIS A9210 > リレー)] に移動します。
2.  をクリックすると、リレー設定が展開されます。
3. [Relay (リレー)] をオンにします。
4. リレーの名前を変更します。
5. リレーを有効および無効にするためのURLを表示するために、[Toggle port URL (ポートURLを切り替え)] に移動します。

### イベントのルールを設定する

詳細については、「イベントのルールの使用開始」を参照してください。

### アクションをトリガーする

1. [System > Events (システム > イベント)] に移動し、ルールを追加します。このルールでは、装置が特定のアクションを実行するタイミングを定義します。ルールは、スケジュールや繰り返しとして設定することも、手動でトリガーするように設定することもできます。
2. [Name (名前)] に入力します。
3. アクションをトリガーするために満たす必要がある [Condition (条件)] を選択します。ルールに複数の条件を指定した場合は、すべての条件が満たされたときにアクションがトリガーされます。
4. 条件が満たされたら実行するAction (アクション) を選択します。

**注**

- アクティブなルールを変更する場合は、ルールを再度オンにして変更内容を有効にする必要があります。

## 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ブラウザで装置のIPアドレスを入力します。

### 注

このセクションで説明する機能と設定のサポートは、装置によって異なります。このアイコン  は、機能または設定が一部の装置でのみ使用できることを示しています。

 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ちます。
- **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

### 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。

## デバイス

### I/Oとリレー

AXIS A9210

I/O

入力

- 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):入力ポートであることを示します。
- 標準の状態:開回路には  を、閉回路には  をクリックします。
- 状態監視: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。
  - 並列優先接続を使用するには、[Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor (22 kΩの並列抵抗器と4.7 kΩの直列抵抗器による並列優先接続)] を選択します。
  - 直列優先接続を使用するには、[Serial first connection (直列優先接続)] を選択し、[Resistor values (抵抗器の値)] ドロップダウンリストから抵抗器の値を選択します。

出力:オンにすると、接続された装置が有効になります。

- 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):出力ポートであることを示します。
- 標準の状態:開回路には  を、閉回路には  をクリックします。
- Toggle port URL (ポートURLを切り替え): 接続された装置を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介して有効および無効にするためのURLが表示されます。

I/O: ポートが出力として設定されている場合、オンにすると接続された装置が有効になります。

- 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):  または  をクリックして、入力または出力として設定します。
- 標準の状態:開回路には  を、閉回路には  をクリックします。
- 状態監視: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。この項目は、ポートを入力として設定している場合にのみ表示されます。
  - 並列優先接続を使用するには、[Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor (22 kΩの並列抵抗器と4.7 kΩの直列抵抗器による並列優先接続)] を選択します。
  - 直列優先接続を使用するには、[Serial first connection (直列優先接続)] を選択し、[Resistor values (抵抗器の値)] ドロップダウンリストから抵抗器の値を選択します。
- Toggle port URL (ポートURLを切り替え): 接続された装置を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介して有効および無効にするためのURLが表示されます。この項目は、ポートを出力として設定している場合にのみ表示されます。

## リレー

- **リレー:**リレーをオンまたはオフにします。
- **名前:**テキストを編集して、リレーの名前を変更します。
- **Direction (方向):**出力リレーであることを示します。
- **Toggle port URL (ポートURLを切り替え):**リレーを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介して有効および無効にするためのURLが表示されます。

## AXIS A9910

1台のAXIS A9210に最大16台のAXIS A9910を接続して、128のI/O、64のリレー、64個のModbusセンサーに対応できます。AXIS A9210から最後のAXIS A9910までの最大距離は1000メートルです。

**+** 暗号化キーの追加: クリックして、暗号化された通信を確立するための暗号化キーを設定します。

**+** AXIS A9910の追加: クリックして拡張モジュールを追加します。

- **名前:**テキストを編集して、拡張モジュールの名前を変更します。
- **アドレス:**拡張モジュールの接続先のアドレスを表示します。
- **Device software version (装置のソフトウェアのバージョン):**拡張モジュールの現在のソフトウェアバージョンを表示します。
- **Upgrade device software (装置のソフトウェアのアップグレード):**クリックすると、拡張モジュールのソフトウェアがアップグレードされます。ドアコントローラーにバンドルされているバージョンにアップグレードするか、任意のバージョンをアップロードするかを選択できます。

## I/O

I/O: ポートが出力として設定されている場合、オンにすると接続された装置が有効になります。

- **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):**  または  をクリックして、入力または出力として設定します。
- **標準の状態:**開回路には  を、閉回路には  をクリックします。
- **状態監視:**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。この項目は、ポートを入力として設定している場合にのみ表示されます。
  - 並列優先接続を使用するには、[Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor (22 kΩの並列抵抗器と4.7 kΩの直列抵抗器による並列優先接続)] を選択します。
  - 直列優先接続を使用するには、[Serial first connection (直列優先接続)] を選択し、[Resistor values (抵抗器の値)] ドロップダウンリストから抵抗器の値を選択します。
- **Toggle port URL (ポートURLを切り替え):** 接続された装置を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介して有効および無効にするためのURLが表示されます。この項目は、ポートを出力として設定している場合にのみ表示されます。

## リレー

- **リレー**:リレーをオンまたはオフにします。
- **名前**:テキストを編集して、リレーの名前を変更します。
- **Direction (方向)**:出力リレーであることを示します。
- **Toggle port URL (ポートURLを切り替え)**:リレーを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介して有効および無効にするためのURLが表示されます。

## アラーム

**Device motion (装置の動き)**:オンに設定すると、装置の動きを検知したときにシステム内でアラームがトリガーされます。

**ケーシング開放**  :オンに設定すると、ドアコントローラーケーシングの開放を検知したときにシステム内でアラームがトリガーされます。ベアボンドアコントローラーでこの設定をオフにします。

**外部からのいたずら**  :オンにすると、外部からのいたずらを検知したときにシステムでアラームがトリガーされます。たとえば、誰かが外部キャビネットを開閉した場合などです。

- **状態監視入力**  :入力の状態を監視するときにオンにし、終端抵抗器を設定します。
  - 並列優先接続を使用するには、[Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor (22 kΩの並列抵抗器と4.7 kΩの直列抵抗器による並列優先接続)] を選択します。
  - 直列優先接続を使用するには、[Serial first connection (直列優先接続)] を選択し、[Resistor values (抵抗器の値)] ドロップダウンリストから抵抗器の値を選択します。

## 周辺機器

### センサー

AXIS A9210に接続されているセンサーの全体把握を表示します。RS485ポートに最大8台のModbusセンサーを直接接続できます。または、AXIS A9910を16台に拡張して、1台のAXIS A9210に64個のModbusセンサーを接続することができます。

✦ **Add (追加):** クリックしてセンサーを追加します。

**名前:** センサーの名前を入力します。

**Sensor (センサー):** センサーを接続するデバイスを選択します。

**RS485ポート:** センサーを接続するポートを選択します。

**アドレス:** センサーのアドレスを入力します。マルチドロップを使用する場合は、1~247の一意的アドレスを入力します。

**タイプ:**

- **[Custom (カスタム)]** を選択します。
  - **Export template (テンプレートのエクスポート):** クリックしてJSONファイルをダウンロードします。ファイルを編集して、後でデバイスにアップロードすることができます。
  - **Select configuration file (設定ファイルの選択):** クリックして設定ファイルを選択するか、ファイルをドラッグします。設定ファイルを編集、コピー、ダウンロード、または印刷することができます。
- **[Hugo]** または **[Tibbo]** を選択します。
  - **Read data (データの読み込み):** センサーからデータを読み込む頻度を設定します。
  - **Thresholds (閾値):** 温度、湿度、露点、気圧、照度などの利用可能なセンサー機能の閾値を設定します。

**Save (保存):** クリックして設定を保存します。

センサーのリストには以下が含まれています。

- **名前:** テキストを編集して、センサーの名前を変更します。
- **Device/Port (デバイス/ポート):** センサーが接続されているModbus IDおよびポート番号。
- **タイプ:** センサーが実行する測定または機能のタイプ (温度、湿度、照度など)。
- **モデル:** センサーのモデル名。
- **Last value (最新値):** センサーから読み取られた最新の値。
- **Last event (最終イベント):** 最後にトリガーされたイベントの理由 (選択されたパラメーターの設定値の上限または下限の超過など)。
- **ステータス:** センサーが現在オンライン状態かオフライン状態かを示します。

## 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、アプリケーションによって異なります。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/](https://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せん。

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、警告が表示されません。

**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、警告が表示されません。

**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。

### 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](http://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](http://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ます。最初にMACsecを有効にするには、リンクの両端で一致する必要があります。
- **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。—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。

## 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せん。

**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。

## 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があります。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があります。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SSLとMQTTオーバ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す。

**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。

**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せん。

**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トメントメッセージ

最終意思テストメント(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ト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せん。

**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せん。

**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。

## 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。

### 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。

## 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。

## プレーン設定

[Plain Config] (プレーン設定) 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

**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](http://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](http://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。

## 詳細情報

### 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](http://help.axis.com)から参照できます。

### AXIS Door Monitoring

このアプリケーションはドアの状態を監視し、ドアが開いている、閉まっている、ドアが長時間開いたままの状態を示します。たとえば、施錠は必要ないが開閉状態を知る必要がある防火扉に、このオプションを使用します。

通常のドアには、ドア位置センサー (REX) と、ロックおよびリーダーがあり、ドアコントローラーが必要です。

監視ドアには、ドア位置センサーとREXのみ必要で、ネットワークI/Oリレーモジュールを使用し監視することが可能です。各ネットワークI/Oリレーモジュールは、最大5つの監視ドアを接続することが可能です。

### 制限事項

このアプリケーションは、AXIS A9210でのみ利用可能です。REXはI/O 1およびI/O 2にのみ接続でき、13、14、または15にREXを設定することはできません。

### AXIS Monitoring Doorの設定

名称	説明
ドア	ドアの番号。
DPS input (DPS入力)	ドアのDPS入力。
REX input (REX入力)	ドアのREX入力。
Door open too long time (sec)(長時間のドア開放 (秒))	ドアを開放したままにできる秒数。
アクセス時間 (秒)	アクセスが許可されてからドアのロック解除を継続する秒数。
状態	ドアの状態。

### サイバーセキュリティ

サイバーセキュリティに関する製品固有の情報については、[axis.com](http://axis.com)の製品データシートを参照してください。

AXIS OSのサイバーセキュリティの詳細情報については、『AXIS OS強化ガイド』を参照してください。

### Axis Edge Vault

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

### 署名付きOS

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

### セキュアブート

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

### 安全なキーストア

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

### AxisデバイスID

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

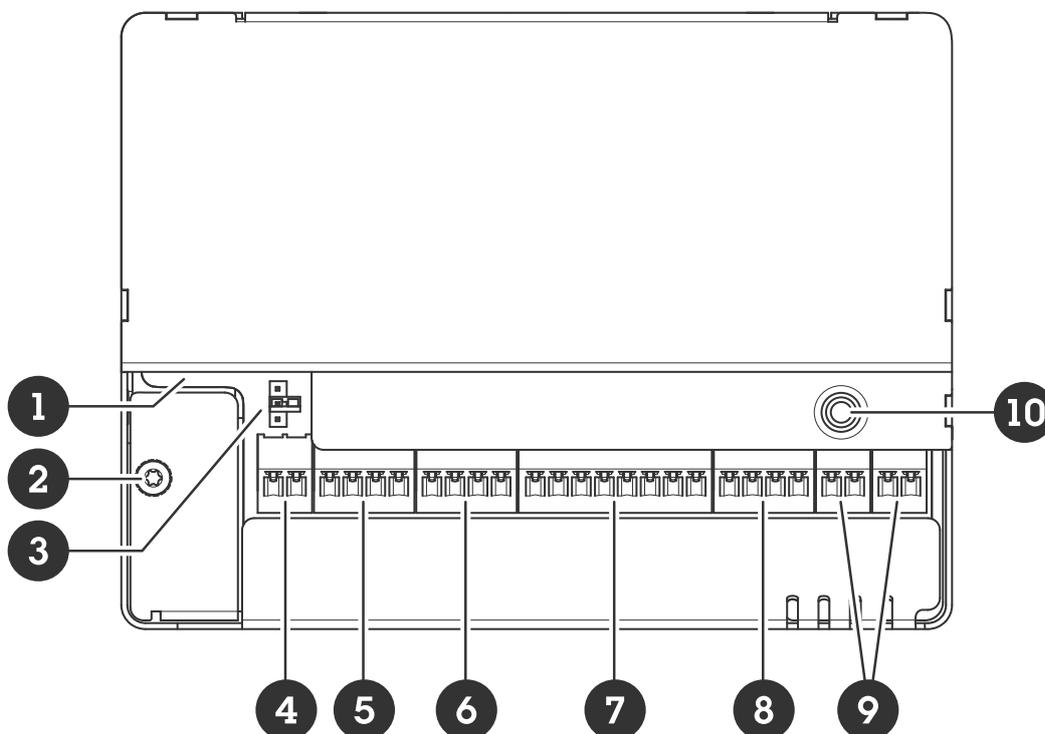
### EFS (暗号化ファイルシステム)

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

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

## 仕様

### 製品概要



- 1 ネットワーク コネクター
- 2 アース位置
- 3 リレージャンパー
- 4 電源コネクター
- 5 リレーコネクタ
- 6 入力1コネクター
- 7 RS485およびI/Oコネクター
- 8 I/Oコネクター
- 9 入力2コネクター
- 10 コントロールボタン

### LEDインジケータ

LED	カラー	説明
ステータス	緑	正常動作であれば緑色に点灯します。
	オレンジ	起動時、設定の復元時に点灯します。
	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。
ネットワー ク	緑	100 Mbit/sネットワークに接続している場合、点灯します。ネット ワークパケットを送受信した場合、点滅します。
	オレンジ	10 Mbit/sネットワークに接続している場合、点灯します。ネット ワークパケットを送受信した場合、点滅します。
	消灯	ネットワーク接続なし。

電源	緑	正常動作。
	オレンジ	ファームウェアアップグレード中は緑とオレンジで交互に点滅します。
リレー	緑	リレーアクティブ。 <sup>1</sup>
	消灯	リレーが無効です。

## 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。

- 製品を工場出荷時の設定にリセットする。工場出荷時の設定にリセットする, on page 44を参照してください。
- インターネット経由でワンクリッククラウド接続 (O3C) サービスに接続します。接続するには、ボタンを押してから放し、ステータスLEDが緑色に3回点滅するまで待ちます。

## コネクタ

### ネットワーク コネクタ

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

UL : Power over Ethernet (PoE) は、44~57 V DC、15.4 W/30 Wを提供できるEthernet IEEE 802.3af/802.3at Type 1 Class 3、またはPower over Ethernet Plus (PoE+) IEEE 802.3at Type 2 Class 4 有限電源インジェクタによって供給される必要があります。Power over Ethernet (PoE) は、AXIS T8133 Midspan 30 W 1-portが搭載されたULによって評価されています。

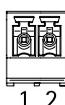
### 電源の優先順位

本装置は、PoEまたはDC入力から電源を供給できます。「ネットワーク コネクタ, on page 38」および「電源コネクタ, on page 38」を参照してください。

- 装置に電源が供給されていない状態でPoEとDCの両方を接続すると、PoEが電源供給に使用されます。
- PoEとDCの両方が接続されており、現在はPoEが電源を供給しています。PoEが失われた場合、本装置は再起動せずにDCを使用して電源を供給します。
- PoEとDCの両方が接続されており、現在はDCが電源を供給しています。DCが失われた場合、本装置は再起動し、PoEを使用して電源を供給します。
- 起動時にDCが使用されている場合、装置の起動後にPoEが接続されても、電源供給にDCが使用されます。
- 起動時にPoEが使用されている場合、装置の起動後にDCが接続されても、電源供給にPoEが使用されます。

### 電源コネクタ

DC電源入力用2ピンターミナルブロック。定格出力が $\leq 100$  Wまたは $\leq 5$  Aの安全特別低電圧 (SELV) に準拠した有限電源 (LPS) を使用してください。



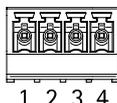
1. リレーが有効です。COMがNOに接続すると、リレーが有効になります。

機能	ピン	メモ	仕様
DCアース (GND)	1		0 V DC
DC入力	2	Power over Ethernet を使用しないときの装 置への電源供給用。 注:このピンは、電源 入力としてのみ使用で きます。	12 V DC、最大36 W

UL：アプリケーションに応じて適切な定格で、UL 603の認定を受けた電源によって供給されるDC電源。

### リレーコネクタ

ロックやゲートへのインターフェースなどの制御に使用できるフォームCリレー用の1台の4ピンターミナルブロックです。ロック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。



機能	ピン	メモ	仕様
DCアース (GND)	1		0 V DC
NO	2	Normally Open。 リレー装置の接続用。 NOとDCアースの間に フェイルセキアロッ クを接続します。 ジャンパーが使用され ていない場合、2つの リレーピンは回路の残 りの部分から電氣的に 分離されています。	最大電流 = 2A 最大電圧 = 30V DC
COM	3	コモン	
NC	4	Normally Closed。 リレー装置の接続用。 NCとDCアースの間に フェイルセーフロッ クを接続します。 ジャンパーが使用され ていない場合、2つの リレーピンは回路の残 りの部分から電氣的に 分離されています。	

### リレー電源ジャンパー

リレー電源ジャンパーが取り付けられている場合、12 V DCまたは24 V DCをリレーCOMにピンに接続します。

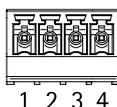
これはGNDピンとNOピン間、もしくはGNDピンとNCピン間のロックに接続するために使用できません。

電源	12 V DCでの最大電力	24 V DCでの最大電力
DC入力	2 000 mA	1 000 mA
PoE	350 mA	150 mA
PoE+	1100 mA	500 mA

### 入力1コネクタ

入力用に4ピンターミナルブロックが1個搭載されます。

終端抵抗器を使用した監視に対応しています。接続が中断されると、アラームがトリガーされま  
す。状態監視入力を使用するには、終端抵抗器を設置します。状態監視入力の接続図を使用しま  
す。監視入力, on page 43を参照してください。



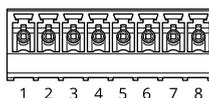
機能	ピン	メモ	仕様
DCアース	1, 3		0 V DC
入力	2, 4	デジタル入力/状態監視入力 - 有効にするにはピン1または3にそれぞれ接続し、無効にする場合はフロート状態 (未接続) のままにします。	0~30 V DC (最大)

#### 重要

AWG 24のケーブル要件を満たす場合、ケーブルの長さは最大200 m (656フィート) です。

### RS485およびI/Oコネクタ

4ピンRS485および4ピンI/Oを備えたターミナルブロック



#### RS485

機能	ピン	注	仕様
DCアース (GND)	1		0 V DC
DC出力 (+12 V)	2	Modbusセンサーなどの補助装置に電源を供給します。	12 V DC、最大200 mA
A	3		
B	4		

#### I/O

機能	ピン	注	仕様
デジタル出力	5	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	0~30 V DC (最大)、 オープンドレイン、 100 mA

		列にダイオードを接続します。	
デジタル出力	6	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
入力	7	デジタル入力/状態監視入力 - 有効にするにはピン1に接続し、無効にする場合はフロート状態 (未接続) のままにします。	0~最大30 V DC
デジタル出力	8	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

**重要**

- RS485に適したケーブル長は最大1000 m (3281 ft) です。ただし、次のケーブル要件を満たすことが前提です。シールド付きツイストペア (1組)、AWG 24、120Ωインピーダンス。
- I/Oに適したケーブル長は最大200 m (656 ft) です。

**I/Oコネクタ**

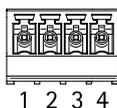
補助コネクタに外部装置を接続し、動体検知、イベントトリガー、アラーム通知などと組み合わせ使用することができます。補助コネクタは、0 V DC基準点と電力 (DC出力) に加えて、以下へのインターフェースを提供します。

**デジタル入力** - 開回路と閉回路の切り替えが可能な装置 (PIRセンサー、ドア/窓の接触、ガラス破損検知器など) を接続するための入力です。

**状態監視入力** - デジタル入力のいたずらを検知する機能が有効になります。

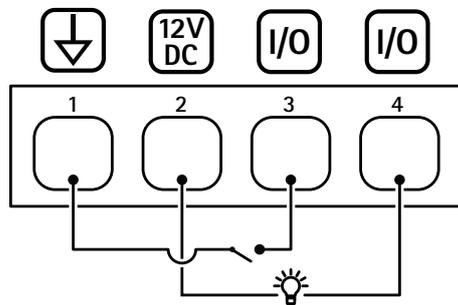
**デジタル出力** - リレーやLEDなどの外部装置を接続します。接続された装置は、VAPIX®アプリケーションプログラミングインターフェースまたは製品のWebページから起動できます。

**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 V DC
DC出力	2	補助装置の電源供給に使用できます。 注:このピンは、電源出力としてのみ使用できません。	12 V DC 最大負荷 = 合計 50 mA

設定可能 (入力または出力)	3-4	デジタル入力/状態監視入力 - 有効にするにはピン1に接続し、無効にする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共に使用する場合は、電圧過渡から保護するために、負荷と並列にダイオードを接続してください。I/Oは、内部12 V DC出力 (PIN 2) が使用されている場合、12 V DC、50 mA (複合最大) の外部負荷を駆動することができます。オープンドレイン接続を外部電源と組み合わせて使用する場合、I/Oはそれぞれ0~30 V DCで100 mAのDC電源供給に対応できます。	0~30 V DC (最大)、 オープンドレイン、 100 mA

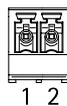


- 1 DCアース
- 2 DC出力 12V
- 3 I/O (入力として設定)
- 4 I/O (出力として設定)

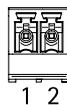
### 入力2コネクタ

ガラスの破壊検知や火災検知などの外部装置で使用する2台の2ピンターミナルブロックです。

UL：このコネクタは、盗難または火災警報用途向けとしてはULによって評価されていません。



機能	ピン	メモ	仕様
DCアース	1		0 V DC
入力	2	デジタル入力/状態監視入力 - 有効にするにはピン1に接続し、無効にする場合はフロート状態 (未接続) のままにします。	0~30 V DC (最大)



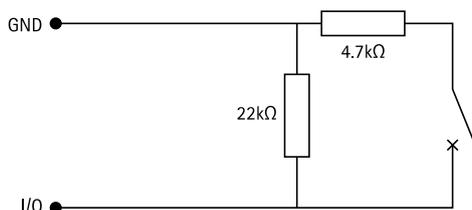
機能	ピン	メモ	仕様
DCアース	1		0 V DC
入力	2	デジタル入力/状態監視入力 - 有効にするにはピン1に接続し、無効にする場合はフロート状態 (未接続) のままにします。	0~30 V DC (最大)

### 監視入力

状態監視入力を使用するには、下図に従って終端抵抗器を設置します。

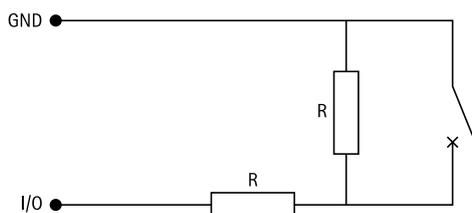
#### パラレルファースト接続

抵抗器の値は 4.7 kΩ 及び 22 kΩ である必要があります。



#### 最初の直列接続

抵抗器の値は同じで、可能な値は 1 kΩ、2.2 kΩ、4.7 kΩ、10 kΩ、1%、¼ワット標準です。



#### 注

シールド付きツイストケーブルを使用することをお勧めします。シールドを 0 V DC に接続します。

ステータス	説明
オープン	状態監視スイッチが開モードです。
終了	状態監視スイッチが閉モードです。
短絡	I/O または入力 1~5 のケーブルが GND に短絡しています。
切断	I/O または入力 1~5 ケーブルが切断され、開モードのまま GND への電流経路がありません。

## 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 37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 (25秒間)。
4. コントロールボタンを放します。プロセスが完了すると、ステータスLEDが緑色に変わります。ネットワーク上にDHCPサーバーがない場合、装置のIPアドレスのデフォルトは次のいずれかになります。
  - **AXIS OS 12.0以降の装置:** リンクローカルアドレスサブネット (169.254.0.0/16) から取得
  - **AXIS OS 11.11以前の装置:** 192.168.0.90/24
5. インストールおよび管理ソフトウェアツールを使用して、IPアドレスの割り当て、パスワードの設定、製品へのアクセスを行います。

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

### AXIS OSのオプション

Axisは、アクティブトラックまたは長期サポート (LTS) トラックのどちらかに従って、装置のソフトウェアの管理を提供します。アクティブトラックでは、最新の製品機能すべてに常時アクセスできますが、LTSトラックの場合、バグフィックスやセキュリティ更新に重点を置いた定期的リリースが提供される固定プラットフォームを使用します。

最新の機能にアクセスする場合や、Axisのエンドツーエンドシステム製品を使用する場合は、アクティブトラックのAXIS OSを使用することをお勧めします。最新のアクティブトラックに対して継続的な検証が行われないサードパーティの統合を使用する場合は、LTSトラックをお勧めします。LTSにより、大きな機能的な変更や既存の統合に影響を与えることなく、サイバーセキュリティを維持することができます。Axis装置のソフトウェア戦略の詳細については、[axis.com/support/device-software/](https://axis.com/support/device-software/)にアクセスしてください。

### AXIS OSの現在のバージョンを確認する

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

AXIS OSの現在のバージョンを確認するには:

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

## AXIS OSをアップグレードする

### 重要

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

### 注

- アクティブトラックのAXIS OSの最新バージョンで装置をアップグレードすると、製品に最新機能が追加されます。アップグレードする前に、AXIS OSと共に提供されるアップグレード手順とリリースノートを必ずお読みください。AXIS OSの最新バージョンとリリースノートについては、[axis.com/support/device-software/](https://axis.com/support/device-software/)にアクセスしてください。
1. AXIS OSのファイルをコンピューターにダウンロードします。これらのファイルは[axis.com/support/device-software/](https://axis.com/support/device-software/)から無料で入手できます。
  2. デバイ스에 管理者としてログインします。
  3. **[Maintenance (メンテナンス)] > [AXIS OS upgrade (AXIS OSのアップグレード)]** に移動し、**[Upgrade (アップグレード)]** をクリックします。

アップグレードが完了すると、製品は自動的に再起動します。

## 技術的な問題と解決策

### AXIS OSのアップグレード時の問題

#### AXIS OSアップグレード失敗

アップグレードに失敗した場合、装置は前のバージョンを再度読み込みます。最も一般的な理由は、AXIS OSの間違ったファイルがアップロードされた場合です。装置に対応したAXIS OSのファイル名であることを確認し、再試行してください。

#### AXIS OSのアップグレード後の問題

アップグレード後に問題が発生する場合は、**[Maintenance (メンテナンス)]** ページから、以前にインストールされたバージョンにロールバックします。

### IPアドレスの設定で問題が発生する

### IPアドレスを設定できない

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

### デバイスへのアクセスの問題

#### ブラウザからデバイスにアクセスする際、ログインできない

HTTPSが有効になっている場合、ログインを試行するときに正しいプロトコル (HTTPまたはHTTPS) を使用していることを確認します。場合によっては、ブラウザのアドレスフィールドに手動でhttpまたはhttpsを入力する必要があります。

rootアカウントのパスワードを忘れた場合は、デバイスを工場出荷時の設定にリセットする必要があります。手順については、工場出荷時の設定にリセットする, on page 44を参照してください。

#### DHCPによってIPアドレスが変更された

DHCPサーバーから取得したIPアドレスは動的なアドレスであり、変更されることがあります。IPアドレスが変更された場合は、AXIS IP UtilityまたはAXIS Device Managerを使用してデバイスのネットワーク上の場所を特定してください。デバイスのモデルまたはシリアル番号、あるいはDNS名 (設定されている場合) を使用してデバイスを識別します。

必要に応じて、静的なIPアドレスを手動で割り当てることができます。手順については、axis.com/supportにアクセスしてください。

#### IEEE 802.1X使用時の証明書エラー

認証を正しく行うには、Axisデバイスの日付と時刻をNTPサーバーと同期させなければなりません。[System (システム) > Date and time (日付と時刻)] に移動します。

#### ブラウザがサポートされていません

推奨ブラウザの一覧は、ブラウザーサポート, on page 2を参照してください。

### 外部からデバイスにアクセスできません

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

- AXIS Camera Station Pro:90日間の試用版を無料で使用でき、中小規模のシステムに最適です。

手順とダウンロードについては、[axis.com/vmsl](http://axis.com/vmsl)にアクセスしてください。

### MQTTの問題

#### MQTTオーバSSLを使用してポート8883経由で接続できない

ファイアウォールは、ポート8883を使用する通信を安全ではないとみなし、ブロックします。

場合によっては、サーバー/ブローカーによってMQTT通信用に特定のポートが提供されていない可能性があります。この場合でも、HTTP/HTTPSトラフィックに通常使用されるポート経由でMQTTを使用できる場合もあります。

- サーバー/ブローカーが、通常はポート443経由で、WebSocket/WebSocket Secure (WS/WSS) をサポートしている場合は、代わりにこのプロトコルを使用してください。サーバー/ブローカープロバイダーに問い合わせ、WS/WSSがサポートされているかどうか、どのポートと基本パスを使用するかを確認してください。
- サーバー/ブローカーがALPNをサポートしている場合、MQTTの使用は443などのオープンポートでネゴシエートできます。ALPNのサポートの有無、使用するALPNプロトコルとポートについては、サーバー/ブローカーのプロバイダーに確認してください。

このページで解決策が見つからない場合は、[axis.com/support](http://axis.com/support)のトラブルシューティングセクションに記載されている方法を試してみてください。

### サポートに問い合わせる

さらにサポートが必要な場合は、[axis.com/support](http://axis.com/support)にアクセスしてください。

T10202445\_ja

2026-01 (M5.5)

© 2023年 Axis Communications AB