

AXIS D1110 Video Decoder 4K

ユーザーマニュアル

目次

使用に当たって	4
ネットワーク上のデバイスを検索する	4
	4
装置の)webインターフェースを開く	4
'官'理石 /' カワノトを1FR 9 る 空会たパフロード	4
ダエなハヘノートデバルズにされていたいことを確認する	5 5
ッパイスのシシーフェースの概要	5
デバイスを構成する	6
カメラの追加	6
カメラソースを編集する	б
カメラを削除する	6
メテイアノアイルの追加	6
ンーケノスの設定	0 7
コントロールボードのキーリファレンス	/ 7
コントロールを設定する	/
アクションをトリガーする	8
音声	8
音声ファイル	8
$web_1 \ge g_2 = 7 = 7$	9
人ナータ人	9
ンークノス 辛吉	IU 11
ョー デバイスの設定	11
ビデオソース	11
アプリ	12
システム	13
時刻と位置	13
ネットワーク	14
セキュリテイ	81 ⊿ר
ノ カウノト イベント	24 25
MOTT	30
ストレージ	33
ONVIF	34
ビデオ出力	35
アクセサリー	35
山ク プロスン(売中	
ノレ1 ノ 設止	
メンテナンス	
トラブルシューティング	
詳細情報	39
ストリーミングとストレージ	39
ビデオ圧縮形式	39
外部ストレージ装置	39
サイハーセキュリテイ	39
者 石 门 さ ∪ 3	39 ⊿∧
Axis Edge Vault	4 0 4∩
AxisデバイスID	40
仕様	41

	製品概要	41
		41
	LEDインジケーター	41
	SDカードスロット	41
	ボタン	42
	コントロールボタン	42
	コネクター	42
	HDMI™コネクター	42
	ネットワーク コネクター	42
	USBコネクター	42
	音声コネクター	42
	電源コネクター	42
トラ	ラブルシューティング	44
	工場出荷時の設定にリセットする	44
	AXIS OSのオプション	44
	AXIS OSの現在のバージョンを確認する	44
	AXIS OSをアップグレードする	45
	技術的な問題、ヒント、解決策	45
	パフォーマンスに関する一般的な検討事項	47
	サポートに問い合わせる	47

使用に当たって

ネットワーク上のデバイスを検索する

Windows[®]で検索したAxisデバイスにIPアドレスの割り当てを行うには、AXIS IP Utilityまたは AXIS Device Managerを使用します。いずれのアプリケーションも無料で、*axis.com/support*から ダウンロードできます。

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

ブラウザーサポート

以下のブラウザーでデバイスを使用できます。

	Chrome™	Firefox®	Edge TM	Safari®
Windows®	推奨	\checkmark	推奨	
macOS®	推奨	\checkmark	推奨	√*
Linux®	推奨	\checkmark	推奨	
その他のオペ レーティングシ ステム	1	1	1	1

*完全にはサポートされていません。ビデオストリーミングに問題が発生した場合は、別のブラウザを使用してください。

装置のwebインターフェースを開く

- 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。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、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。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。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。

- 工場出荷時の設定にリセットします。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

カメラの追加

- 1. [Video sources (ビデオソース)] > [Camera sources (カメラソース)] に移動します。
- 2. [Add camera source (カメラソースを追加)] をクリックします。
 既定のカメラをリストから追加するには、[Network discovery (ネットワーク検出)] を選択します。
 - カメラを手動で追加する場合は、[Manual (手動)] を選択します。
 Axisカメラの場合: 名前、IPアドレス、ストリーミングプロトコル、ポート、 カメラのユーザー名とパスワードを入力します。
 - サードパーティ製のカメラの場合:名前、IPアドレス、カメラのユーザー名と パスワードを入力します。
- 3. [追加]をクリックします。

カメラソースを編集する

カメラを追加した後、[Edit (編集)] ビューから設定を編集できます。

- 1. [Video sources (ビデオソース)] > [Camera sources (カメラソース)] に移動します。
- 2. カメラソースを選択し、 ・ をクリックします。
- 3. [Edit (編集)] をクリックし、変更を行います。
- 4. [保存]をクリックします。

カメラを削除する

- 1. [Video sources (ビデオソース)] > [Camera sources (カメラソース)] に移動します。
- 2. カメラソースを選択し、 * をクリックします。
- 3. [Delete (削除)] をクリックして確定します。

メディアファイルの追加

- 1. [Video sources (ビデオソース)] > [Media sources (メディアソース)] に移動します。
- 2. 「 **Add media source (メディアソースを追加)**] をクリックします。
- 3. メディアファイルを装置にアップロードし、配置場所を選択します。
- 4. [追加]をクリックします。

シーケンスの設定

- 1. [Sequences (シーケンス)] > [Sequences (シーケンス)] に移動します。
- 2. [T Add sequence (シーケンスを追加)] をクリックします。
- 3. 新しいシーケンスの名前を入力します。
- 4. をクリックし、ビューのレイアウトを選択します。

- 5. ビューウィンドウで、[Click to select camera source or media for this segment (クリッ クしてこのセグメントのカメラソースまたはメディアを選択)] が表示されます。
- 6. [Camera (カメラ)] または [Media (メディア)] を選択し、リストからソースを選択します。
- 注
 - 低遅延モードを有効にするには、H.264ビデオコーデックのみを選択します。ネットワーク トラフィックを増大させるBフレームを無効にすることで、カメラストリームの遅延が低減 されます。
 - ・ サードパーティ製カメラの場合は、カメラのメーカーから取得したURIを追加します。
 - 7. [Add (追加)] をクリックして、ビューウィンドウがいっぱいになるまでソースを追加し続け ます。
 - 8. シーケンスにビューウィンドウをさらに追加するには、 十 をクリックします。
 - 9. [**保存**]をクリックします。
 - 10. *と* をクリックして、シーケンスを再生します。

コントロールボードを使用してビューを移動し、カメラを操作する

- 1. デコーダーにカメラを追加します。を参照してください。
- 2. AxisカメラのPTZを必ずオンにしてください。
- 3. AXIS TU9001 Control Boardをデコーダーに接続します。
- デコーダーのwebインターフェースで、[Sequences (シーケンス)] > [Joystick controls (ジョイスティックコントロール)] に移動し、[Joystick (ジョイスティック)] をオンにしま す。

コントロールボードのキーリファレンス

注

ペインを選択すると、ビューの自動変更が一時停止されます。

説明	AXIS TU9001
単一ビューでカメラのPTZをオンにします。	F1
分割ビューのペイン <p> のカメラでPTZをオ ンにします。</p>	<p> + F1</p>
分割ビューのペイン <p> のカメラを全画面に 設定し、PTZをオンにします。</p>	<p> +</p>
PTZをオフにして、全画面表示から前のシーケンスに戻ります。	
選択したカメラをパンします。	ジョイスティックを左右に動かす
選択したカメラをチルトします。	ジョイスティックを上下に動かす
選択したカメラをズームします。	ジョイスティックヘッドを左右に動かす
単一ビューでPTZプリセット <n> に移動し、 PTZをオンにします。</n>	J <n></n>
単一ビューでPTZプリセット <n> を設定し、 PTZをオンにします。</n>	ALT + J <n></n>

分割ビューのペイン <p> のPTZプリセット <n> に移動し、PTZをオンにします。</n></p>	<p> + J<n></n></p>
分割ビューのペイン <p> のPTZプリセット <n> を設定し、PTZをオンにします。</n></p>	$\langle P \rangle + ALT + J \langle N \rangle$

例:

- AXIS TU9003で2を押してからAXIS TU9002でJ1を押すと、カメラは現在の分割ビューのペイン2のPTZプリセット1に移動します。
- AXIS TU9003で5を押してからF1を押すと、現在の分割ビューのペイン5のカメラのPTZがオンになります。

コントロールボードの詳細については、ユーザーマニュアルを参照してください。

イベントのルールを設定する

特定のイベントが発生したときにデバイスにアクションを実行させるように、ルールを作成する ことができます。ルールは条件とアクションで構成されます。条件を使用して、アクションをト リガーすることができます。たとえば、デバイスは動きを検知したときに、録画を開始したり、 電子メールを送信したりすることができ、デバイスが録画をしている間にオーバーレイテキスト を表示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。

アクションをトリガーする

- [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。
- 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. 条件が満たされたときにデバイスが実行する 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。

音声

音声ファイル

本装置は音声のみのファイルをサポートしていません。

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。



・ 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装置情報を表示します。

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。

シーケンス

モニタリング

シーケンスに関する情報を表示します。

Performance control (パフォーマンスコントロール)

Latency threshold (遅延閾値):ストリームの最大遅延を選択します。閾値を超えると、遅延目標 に到達するまでフレームがドロップされます。ソフトウェアのデコードには適用されません。

Joystick controls (ジョイスティックコントロール)

Joystick (ジョイスティック)オンにすると、コントロールボードを使用してビューを移動し、カメラを操作できるようになります。

シーケンス

重要

マルチストリーム再生に関する問題を回避するには、webインターフェースに表示される推奨 事項に従ってください。

+ シーケンスを追加:クリックして、シーケンスを追加します。
 名前:シーケンスの名前を入力します。
 ●:クリックして、表示するソースの数を選択します。
 +:クリックして、シーケンスの数を選択します。
 >:クリックして、シーケンスを再生します。
 :コンテキストメニューは以下を含みます。
 シーケンスを編集
 シーケンスを削除

音声

デバイスの設定

音声出力

Enable Output (出力を有効にする):音声出力コネクターからの音声をオンまたはオフにします。

Audio out synchronization (音声出力の同期):音声出力 (3.5 mm) ポートとビデオストリームの 遅延差に合わせて時間を設定します。

ビデオソース

カメラソース

↓ Add camera source (カメラソースを追加):クリックして、新しいカメラソースを追加します。			
 Network discovery (ネットワーク探索):IPアドレスを手動で検索するか、リストから Axis装置を選択します。 			
 ストリーミングプロトコル: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。			
– 554はRTSPTのデフォルト値です。			
- 80はRTSP over HTTPのデフォルト値です。			
– 443はRTSP over HTTPSのデフォルト値です。			
– Account (アカウント):装置のユーザー名を入力します。			
– パスワード :装置のパスワードを入力します。			
 Include motion events (動きのイベントを含める):選択すると、カメラで検知された動きをイベント条件として使用できるようになります。この設定はAxisカメラにのみ使用できます。 			
– 名前 :ビデオソースの名前を入力します。			
– IPアドレス :装置のIPアドレスを入力します。			
– Account (アカウント):装置のユーザー名を入力します。			
– パスワード:装置のパスワードを入力します。			
 Include motion events (動きのイベントを含める):選択すると、カメラで検知された動きをイベント条件として使用できるようになります。この設定はAxisカメラにのみ使用できます。 			
・ コンテキストメニューは以下を含みます。			
Edit (編集) :ビデオソースのプロパティを編集します。			
削除 :ビデオソースを削除します。			
メディアソース			

Ⅰ Add media source (メディアソースを追加):クリックして、新しいメディアソースを追加します。

- メディアファイルをアップロードするか、ドラッグアンドドロップします。.mp4、. mkv、.jpeg、または.pngファイルを使用できます。
- ・ Upload location (アップロード場所):ドロップダウンリストから場所を選択します。

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ジ: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。

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

注

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

アプリ名の横にあるスイッチを使用して、アプリを起動または停止します。

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

- コンテキストメニューに、以下のオプションが1つ以上含まれていることがあります。
 - Open-source license (オープンソースライセンス):アプリで使用されているオープン ソースライセンスに関する情報が表示されます。
 - App log (アプリのログ):アプリイベントのログが表示されます。このログは、サポート にご連絡いただく際に役立ちます。
 - キーによるライセンスのアクティブ化:アプリにライセンスが必要な場合は、ライセンス を有効にする必要があります。装置がインターネットにアクセスできない場合は、この オプションを使用します。
 ライセンスキーがない場合は、axis.com/products/analyticsにアクセスします。ライセン スキーを入手するには、ライセンスコードとAxis製品のシリアル番号が必要です。
- ライセンスの自動アクティブ化:アプリにライセンスが必要な場合は、ライセンスを有効にする必要があります。装置がインターネットにアクセスできる場合は、このオプションを使用します。ライセンスをアクティブ化するには、ライセンスコードが必要です。
- Deactivate the license (ライセンスの非アクティブ化):試用ライセンスから正規ライセンスに変更する場合など、別のライセンスと交換するために現在のライセンスを無効にします。ライセンスを非アクティブ化すると、ライセンスはデバイスから削除されます。
- Settings (設定):パラメーターを設定します。
- **削除**:デバイスからアプリを完全に削除します。ライセンスを最初に非アクティブ化しない場合、ライセンスはアクティブのままです。

システム

時刻と位置

日付と時刻

時刻の形式は、Webブラウザーの言語設定によって異なります。

注

装置の日付と時刻をNTPサーバーと同期することをお勧めします。

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

- Automatic date and time (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。
 - 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サーバーに接続されている必要があります。
- **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。

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が自動的にデバイスにIP アドレスを割り当て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。

DNSサーバー

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。

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とHTTPS

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

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

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

注

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

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

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

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

ネットワーク検出プロトコル

Bonjour[®]: オンにしてネットワーク上で自動検出を可能にします。

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

UPnP[®]: オンにしてネットワーク上で自動検出を可能にします。

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

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

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

グローバルプロキシー

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

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

httpおよびhttpsプロキシーで許可されるフォーマット:

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

注

装置を再起動し、グローバルプロキシー設定を適用します。

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

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

ワンクリックによるクラウド接続

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

Allow O3C (O3Cを許可):

- [ワンクリック]:デフォルトの選択肢です。O3Cに接続するには、デバイスのコントロー ルボタンを押してください。ボタンの押し方は、デバイスモデルにより異なります。一 度押して離し、ステータスLEDが点滅するまで待つか、またはステータスLEDが点滅する まで押し続けてください。[常時]を有効にして接続を維持するには、24時間以内にこのデ バイスをO3Cサービスに登録してください。登録しないと、このデバイスはO3Cから切断 されます。
- [常時]:デバイスは、インターネットを介してO3Cサービスへの接続を継続的に試行しま す。一度デバイスを登録すれば、常時接続された状態になります。コントロールボタン に手が届かない場合は、このオプションを使用します。
- [なし]:O3Cを切断します。

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

[ホスト]:プロキシサーバーのアドレスを入力します。

ポート:アクセスに使用するポート番号を入力します。

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

Authentication method (認証方式):

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

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

SNMP

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

SNMP:使用するSNMPのバージョンを選択します。

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

注

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

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

セキュリティ

証明書

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

・ Client/server Certificates (クライアント/サーバー証明書)

クライアント/サーバー証明書は装置のIDを認証します。自己署名証明書と認証局 (CA) 発行の証明書のどちらでも使用できます。自己署名証明書による保護は限られていますが、認証局発行の証明書を取得するまで利用できます。

CA証明書

CA証明書はピア証明書の認証に使用されます。たとえば、装置をIEEE 802.1Xで保護されたネットワークに接続するときに、認証サーバーのIDを検証するために使用されます。 装置には、いくつかのCA証明書がプリインストールされています。

以下の形式がサポートされています:

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

重要

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

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

- **その他** [∨]:入力または選択するフィールドをさらに表示します。
- セキュアキーストア:[Trusted Execution Environment (SoC TEE)]、[Secure element (セキュアエレメント)] または [Trusted Platform Module 2.0] を使用して秘密鍵を安全 に保存する場合に選択します。どのセキュアキーストアを選択するかの詳細について は、help.axis.com/axis-os#cryptographic-supportにアクセスしてください。
- Key type (キーのタイプ):ドロップダウンリストから、証明書の保護に使用する暗号化ア ルゴリズムとしてデフォルトかその他のいずれかを選択します。
- - コンテキストメニューは以下を含みます。
 - Certificate information (証明書情報):インストールされている証明書のプロパティを表示します。
 - Delete certificate (証明書の削除):証明書の削除。
 - ・ Create certificate signing request (証明書の署名要求を作成する):デジタルID証明書を 申請するために登録機関に送信する証明書署名要求を作成します。

セキュアキーストア:

- Trusted Execution Environment (SoC TEE): 安全なキーストアにSoC TEEを使用する場合 に選択します。
- 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。

暗号化ポリシー

暗号化ポリシーは、データ保護のために暗号化がどのように使用されるかを定義します。

Active (アクティブ):デバイスに適用する暗号化ポリシーを選択します:

- ・ Default (デフォルト) OpenSSL: 一般的な使用向けのバランスの取れたセキュリティと パフォーマンス。
- FIPS FIPS 140-2に準拠したポリシー: 規制対象業界向けのFIPS 140-2に準拠した暗号 化。

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

IEEE 802.1x

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

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

IEEE 802.1AE MACsec

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

証明書

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ブルートフォース攻撃を防ぐ

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

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

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

ファイアウォール

Activate (アクティブ化):ファイアウォールをオンにします。

Default Policy (デフォルトポリシー):ファイアウォールのデフォルト状態を選択します。

- Allow: (許可:) 装置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。
- Deny (拒否): 装置へのすべての接続を拒否します。

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、ポートから装置への接続を許可または拒否するルールを作成できます。

- アドレス:アクセスを許可または拒否するアドレスをIPv4/IPv6またはCIDR形式で入力します。
- Protocol (プロトコル):アクセスを許可または拒否するプロトコルを選択します。
- ポート:アクセスを許可または拒否するポート番号を入力します。1~65535のポート番号 を追加できます。
- Policy (ポリシー): ルールのポリシーを選択します。

十:クリックして、別のルールを作成します。

Add rules: (ルールの追加:) クリックして、定義したルールを追加します。

- Time in seconds: (時間 (秒):) ルールのテストに制限時間を設定します。デフォルトの制限時間は300秒に設定されています。ルールをすぐに有効にするには、時間を0秒に設定します。
- Confirm rules (ルールを確認): ルールとその制限時間を確認します。1秒を超える制限時間を設定した場合、ルールはこの時間内に有効になります。時間を0に設定した場合、 ルールはすぐに有効になります。

Pending rules (保留中のルール):まだ確認していない最新のテスト済みルールの概要です。

注

時間制限のあるルールは、表示されたタイマーが切れるか、確認されるまで、[Active rules (アクティブなルール)] に表示されます。確認されない場合、タイマーが切れると、それらの ルールは [Pending rules (保留中のルール)] に表示され、ファイアウォールは以前の設定に 戻ります。それらのルールを確認すると、現在アクティブなルールが置き換えられます。

Confirm rules (ルールを確認):クリックして、保留中のルールをアクティブにします。

Active rules (アクティブなルール):装置で現在実行中のルールの概要です。

⑪_{:クリックして、アクティブなルールを削除します。}

【●:クリックして、保留中のルールとアクティブなルールの両方をすべて削除します。

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):次のアクセス権を持っています:
 - ビデオストリームのスナップショットを見て撮影する。
 - 録画を再生およびエクスポートする。
 - **PTZアカウント**アクセスをパン、チルト、ズームに使用します。

: 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。

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。

Virtual host (仮想ホスト)

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

Enabled (有効):この仮想ホストを使用するには、選択します。

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

ポート:サーバーが接続されているポートを入力します。

タイプ:使用する認証のタイプを選択します。[Basic (ベーシック)]、[Digest (ダイジェスト)]、 [Open ID] から選択します。

- コンテキストメニューは以下を含みます。
- Update (更新):仮想ホストを更新します。
- 削除:仮想ホストを削除します。

Disabled (無効):サーバーが無効になっています。

イベント

ルール

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

注

最大256のアクションルールを作成できます。

▼ ルールを追加:ルールを作成します。

名前:アクションルールの名前を入力します。

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

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

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

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

[|] 条件を追加:新たに条件を追加する場合にクリックします。

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

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

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

SIP:選択してSIP呼び出しを行います。 VMS:選択してVMS呼び出しを行います。

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

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

注

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

• TCP

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

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

コンテキストメニューは以下を含みます。

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

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

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

スケジュール

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

手動トリガー

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

MQTT

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

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

MQTTの詳細については、AXIS OSナレッジベースを参照してください。

ALPN

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

MQTT クライアント

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

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

ブローカー

[ホスト]:MQTTサーバーのホスト名またはIPアドレスを入力します。

Protocol (プロトコル):使用するプロトコルを選択します。

ポート:ポート番号を入力します。

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

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

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

パスワード:ユーザー名のパスワードを入力します。

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

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

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

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

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

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

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

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

接続メッセージ

接続が確立されたときにメッセージを送信するかどうかを指定します。

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

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

Topic (トピック):デフォルトのメッセージのトピックを入力します。

Payload (ペイロード):デフォルトのメッセージの内容を入力します。

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

QoS:パケットフローのQoS layerを変更します。

最終意思およびテスタメントメッセージ

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

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

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

Topic (トピック):デフォルトのメッセージのトピックを入力します。

Payload (ペイロード):デフォルトのメッセージの内容を入力します。

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

QoS:パケットフローのQoS layerを変更します。

MQTT公開

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

Include 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。

ストレージ

オンボードストレージ

重要

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

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

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

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

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

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

ツール

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

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

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

ONVIF

ONVIFアカウント

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

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

Account (アカウント):固有のアカウント名を入力します。

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

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

Role (権限):

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

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

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

ビデオ出力

HDMI、

HDMIケーブルを使用して、外部モニターを装置に接続できます。

Outputs (出力):現在のHDMIの状態と設定が表示されます。

 表示モードを変更するには、ドロップダウンリストから希望のモードを選択し、 [Maintenance (メンテナンス)] に移動し、[Restart (再起動)] をクリックします。デバイ スが再起動し、変更が適用されます。

アクセサリー

USB設定

デフォルトでは、USBポートが無効になっており、どのような接続にも反応しません。有効にすると、デバイスはメモリースティック、Axisコントロールボード、その他の対応するアクセサリーなどの外部USBデバイスに接続できます。

 USBポートを有効にするには、スイッチを切り替え、[Maintenance (メンテナンス)] に 移動し、[Restart (再起動)] をクリックします。デバイスが再起動し、変更が適用されま 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。

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。

CA証明書設定:現在の設定を参照するか、証明書を追加します。

プレイン設定

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

メンテナンス

メンテナンス

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

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

重要

復元後に保存される設定は以下の場合のみです。

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

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

注

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

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

アップグレード時には、以下の3つのオプションから選択できます。

- Standard upgrade (標準アップグレード):AXIS OSの新しいバージョンにアップグレード します。
- Factory default (工場出荷時設定):アップグレードすると、すべての設定が工場出荷時の 値に戻ります。このオプションを選択すると、アップグレード後にAXIS OSを以前のバー ジョンに戻すことはできません。
- 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AXIS OSの以前のバージョンに戻されます。

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

トラブルシューティング

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

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

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

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

ネットワークトレース

重要

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

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

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

詳細情報

ストリーミングとストレージ

ビデオ圧縮形式

使用する圧縮方式は、表示要件とネットワークのプロパティに基づいて決定します。以下から選択を行うことができます。

H.264またはMPEG-4 Part 10/AVC

注

H.264はライセンスされた技術です。このAxis製品には、H.264閲覧用のクライアントライセン スが1つ添付されています。ライセンスされていないクライアントのコピーをインストールする ことは禁止されています。ライセンスを追加購入するには、Axisの販売代理店までお問い合わ せください。

H.264を使用すると、画質を損なうことなく、デジタル映像ファイルのサイズを削減でき、Motion JPEG形式の場合と比較すると80%以上、従来のMPEG形式と比較すると50%以上を削減できます。 そのため、ビデオファイルに必要なネットワーク帯域幅やストレージ容量が少なくなります。また、別の見方をすれば、より優れた映像品質が同じビットレートで得られることになります。

H.265またはMPEG-H Part 2/HEVC

H.265を使用すると、画質を損なうことなくデジタルビデオファイルのサイズを削減でき、H.264 に比べて25%以上縮小することができます。

- 注
 - H.265はライセンスされた技術です。このAxis製品には、H.265閲覧用のクライアントライセンスが1つ添付されています。ライセンスされていないクライアントのコピーをインストールすることは禁止されています。ライセンスを追加購入するには、Axisの販売代理店までお問い合わせください。
 - ほとんどのWebブラウザはH.265のデコードに対応していないため、カメラはWebインター フェースでH.265をサポートしていません。その代わり、H.265のデコーディングに対応し た映像管理システムやアプリケーションを使用できます。

外部ストレージ装置

ビデオデコーダによって認識されるようにするには、外部ストレージ装置の最初のパーティションでexFATまたはext4ファイルシステムを使用する必要があります。

サイバーセキュリティ

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

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

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。

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。

AxisデバイスID

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

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

仕様

製品概要



- 4 コントロールボタン5 HDMIタイプAコネクター
- 6 音声出力
- 7 microSDカードスロット
- 8 セキュリティスロット
- **9** ステータスLED

LEDインジケーター

ステータスLED	説明
オレンジ	起動中または工場出荷時の設定へリセット中、設定の復元時に点灯しま す。
オレンジ/赤	起動中、ネットワーク接続が利用できないか失われた場合に点滅しま す。
緑	起動後正常に動作する場合、10秒間、緑色に点灯します。
	LEDが緑色に点灯した後に消灯すると、装置は動作しています。
禄/赤	識別目的の場合に点滅します。

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。

本装置は、microSD/microSDHC/microSDXCカードに対応しています。

推奨するSDカードについては、axis.comを参照してください。

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

ボタン

コントロールボタン

コントロールボタンは、以下の用途で使用します。

- 製品を工場出荷時の設定にリセットする。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。

コネクター

HDMI™コネクター

ディスプレイやパブリックビューモニターへの接続には、HDMITMコネクタを使用します。

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

USBコネクター

USBコネクターを使用して外部アクセサリーを接続します。サポートされるアクセサリーについては、製品のデータシートを参照してください。

重要

一度にサポートされるUSBストレージは1つのみです。

USBストレージを取り外す前に、装置の電源をオフにしてください。

音声コネクター

• 音声出力 - 3.5 mm音声 (ラインレベル) 出力 (パブリックアドレス (PA) システムまたはアン プ内蔵アクティブスピーカーに接続可能)。音声出力には、ステレオコネクタを使用する必 要があります。



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	アース

電源コネクター

AC/DCコネクター。付属のアダプターを使用します。

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



注

DCが利用可能な場合は、PoEよりもDCが優先されます。

トラブルシューティング

工場出荷時の設定にリセットする

重要

工場出荷時の設定へのリセットは慎重に行ってください。工場出荷時の設定へのリセットを行うと、IPアドレスを含むすべての設定が工場出荷時の値にリセットされます。

本製品を工場出荷時の設定にリセットするには、以下の手順に従います。

- 1. 本製品の電源を切ります。
- 2. コントロールボタンを押した状態で電源を再接続します。を参照してください。
- 3. ステータスLEDインジケーターがオレンジで点滅するまでコントロールボタンを15~30秒 間押し続けます。
- 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
- 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、装置へのアクセスを行います。 axis.com/supportのサポートページに、インストールおよび管理ソフトウェアツールが用意されています。

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

AXIS OSのオプション

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

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

AXIS OSの現在のバージョンを確認する

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

AXIS OSの現在のバージョンを確認するには:

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

AXIS OSをアップグレードする

重要

- 事前設定済みの設定とカスタム設定は、装置のソフト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AXIS OS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、デバイスを電源に接続したままにしてください。

注

アクティブトラックのAXIS OSの最新バージョンで装置をアップグレードすると、製品に最新機能が追加されます。アップグレードする前に、AXIS OSと共に提供されるアップグレード手順とリリースノートを必ずお読みください。AXIS OSの最新バージョンとリリースノートについては、axis.com/support/device-softwareにアクセスしてください。

- 1. AXIS OSのファイルをコンピューターにダウンロードします。これらのファイルはaxis.com/ support/device-softwareから無料で入手できます。
- 2. デバイスに管理者としてログインします。
- 3. [Maintenance (メンテナンス)] >[AXIS OS upgrade (AXIS OSのアップグレード)] に移動 し、[Upgrade (アップグレード)] をクリックします。

アップグレードが完了すると、製品は自動的に再起動します。

AXIS Device Managerを使用すると、複数の装置を同時にアップグレードできます。詳細については、axis.com/products/axis-device-managerをご覧ください。

技術的な問題、ヒント、解決策

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

AXIS OSのアップグレード時の問題

AXIS OSのアップグレードに失敗す る	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

デバイスが別のサブ
 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 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 バイスで使用されて 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 いる IPアドレスを入力します)。

- Reply from <IP address>: bytes=32; time=10...が表示された場合は、ネットワーク上の別のデバイスでそのIPアドレスがすでに使われている可能性があります。ネットワーク管理者から新しいIPアドレスを取得し、デバイスを再度インストールしてください。
- Request timed outが表示された場合は、AxisデバイスでそのIP アドレスを使用できます。この場合は、すべてのケーブル配線を チェックし、デバイスを再度インストールしてください。

同じサブネット上の 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 別のデバイスとIPア 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 ドレスが競合してい 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 る可能性がある する可能性があります。

ブラウザーから装置にアクセスできない

ログインできない	HTTPSが有効になっているときは、ログインを試みるときに正しいプロ トコル (HTTPまたはHTTPS) を使用していることを確認してください。場 合によっては、ブラウザーのアドレスフィールドに手動でhttpまたは httpsを入力する必要があります。
	rootアカウントのパスワードを忘れた場合は、装置を工場出荷時の設定 にリセットする必要があります。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、 <i>axis.com/support</i> 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。

装置にローカルにアクセスできるが、外部からアクセスできない

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

- AXIS Camera Station Edge: 無料で使用でき、最小限の監視が必要な小規模システムに最 適です。
- AXIS Camera Station 5:30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。
- AXIS Camera Station Pro:90日間の試用版を無料で使用でき、中小規模のシステムに最適です。

手順とダウンロードについては、axis.com/vmsにアクセスしてください。

MQTTオーバSSLを使用してポート8883経由で接続できない

ファイアウォールに	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
よって、ポート8883	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/
が安全ではないと判	HTTPSトラフィックに通常使用されるポート経由でMQTTを使用できる可
断されたため、ポー	能性があります。
ト8883を使用するト ラフィックがブロッ クされています。	 サーバー/ブローカーが、通常はポート443経由で、 WebSocket/WebSocket Secure (WS/WSS) をサポートしている場合 は、代わりにこのプロトコルを使用してください。 サーバー/ブローカープロバイダーに問い合わせて、WS/WSSがサ ポートされているかどうか、どのポートと基本パスを使用するか を確認してください。

サーバー/ブローカーがALPNをサポートしている場合、MQTTの使用は443などのオープンポートでネゴシエートできます。ALPNのサポートの有無、使用するALPNプロトコルとポートについては、サーバー/ブローカーのプロバイダーに確認してください。

パフォーマンスに関する一般的な検討事項

- HTTPSを使用すると、フレームレートが低下する場合があります。
- 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。
- ビデオストリームの入力と出力の間に相関関係がない場合、ビデオデコーダの性能に影響 を与える可能性があります。

サポートに問い合わせる

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

T10192361_ja

2025-06 (M11.2)

© 2023年 – 2025 Axis Communications AB