

# AXIS I8016-LVE Network Video Intercom

ユーザーマニュアル

## 目次

設定の概要	4
製品概要	5
	5
() () () () () () () () () () () () () (	0
イットワークエのノハイスを快系する	0
シンクタークェースを問く	6
表置のWCGTファーフェースを開く デバイスのソフトウェアが改ざんされていたいことを確認する	0 6
管理者アカウントを作成する	0 6
安全なパスワード	7
デバイスを構成する	8
ダイレクトSIP (P2P) を設定する	8
サーバーを介してSIPを設定する (PBX)	9
連絡先の作成	9
呼び出しボタンの設定	10
DTMFを使用して来訪時にドアのロックを解除する	10
ナイトモードを使用して低光量下で赤外線照明からメリットを得る	
webインターフェース	
人ナータ人	
」 ニューケーンヨン	
建裕     じん     レ     ハ     レ     ハ     レ     ハ     レ     ハ     ビ     レ     ・      ・      ・     ・     ・      ・      ・      ・      ・      ・      ・      ・      ・      ・      ・      ・      ・      ・      ・      ・      ・      ・      ・      ・        ・	3   1 4
SIP	14 10
呼い古し \//MCITT7ド山	۲۹ ۵۵
₩₩35年0 円 0	20 20
ノ///(QR	20 20
ビデオ	
インストール	23
画像	23
ストリーム	
オーバーレイ	32
プライバシーマスク	34
音声	
デバイスの設定	
ストリーム	
	30 حد
アフリ	/ د 20
- ノヘノム	۵C کړ
時刻と位置 設定の確認	20
成化の唯心 ネットワーク	39
ヤキュリティ	
アカウント	
イベント	
MQTT	57
ストレージ	60
ストリームプロファイル	62
ONVIF	63
検知器	66
アクセサリー	
ノレイン設定	68

メンテナンス       69         トラブルシューティング       70         詳細情報       71         Voice over IP (VoIP)       71         セッション開始プロトコル (SIP)       71         ピアツーピアSIP (2PSIP)       71         ポロション開始プロトコル (SIP)       71         オロション開始プロトコル (SIP)       71         ポロシーピアンーピアSIP (2PSIP)       71         パロトレールを設定する       73         NATトラパーサル       73         アプリケーション       73         トラブルシューティング       74         工場出荷時の設定にリセットする       74         本SISOSの現在のパージョンを確認する       74         AXIS OSの現在のパージョンを確認する       74         AXIS OSをアップグレードする       74         技術的な問題、ヒント、解決策       75         パフォーマンスに関する一般的な検討事項       76         サポートに同い合わせる       77         機器の接続       78         PoE (120) で電力を供給されるリレー       78         期の電源で電力を供給されるリレー       78         オーレー       79         インターカムからのPoEで電力を供給される12 Vフェールセキュアロック       80         インジケーター       81	メンテナンス	69
トラブルシューティング	メンテナンス	
詳細情報       71         Voice over IP (VoIP)       71         セッション開始プロトコル (SIP)       71         ピアツーピアSIP (P2PSIP)       71         構内交換機 (PBX)       72         イベントのルールを設定する       73         NATトラバーサル       73         アプリケーション       73         トラブルシューティング       74         工場出荷時の設定にリセットする       74         AXIS OSの現在のパージョンを確認する       74         AVIS OSをアップグレードする       74         AVIS OSの現在のパージョンを確認する       74         AVIS OSの現在のパージョンを確認する       74         AVIS OSの見在のパージョンを確認する       74         AVIS OSの見たのパージョンを確認する       74         AVIS OSの見たのパージョンを確認する       75         パフォーマンスに関する一般的な検討事項       76         サポートに問い合わせる       77         機器ので電力を供給されるリレー       78         別の電源で電力を供給されるリレー       78         アロントに満まされる12 Vフェールセキュアロック       79         インター       81         プロントパネルインジケーターとコントロール       81         アントロールボタン       81         マン	トラブルシューティング	70
Voice over IP (VoIP)	詳細情報	71
セッション開始プロトコル (SIP)	Voice over IP (VoIP)	71
ピアツーピアSIP (P2PSIP)	セッション開始プロトコル (SIP)	71
構内交換機 (PBX)       72         イベントのルールを設定する       73         NATトラパーサル       73         アプリケーション       73         トラブルシューティング       74         工場出荷時の設定にリセットする       74         AXIS OSの現在のパージョンを確認する       74         AXIS OSの現在のパージョンを確認する       74         技術的な問題、ヒント、解決策       75         パフォーマンスに関する一般的な検討事項       76         サポートに問い合わせる       77         機器の接続       78         PoE (12V) で電力を供給されるリレー       78         別の電源で電力を供給されるリレー       78         別の電源で電力を供給されるリレー       78         別の電源で電力を供給されるリレー       78         別の電源で電力を供給されるリレー       79         外部電源で電力を供給される12 Vフェールセキュアロック       80         仕様       81         フロントパネルインジケーターとコントロール       81         インジケーターアイコン       81         エントロールボタン       81         コントロールボタン       81         コントロールボタン       81         コネクター       81         コネクター       81         コントロールボタン       81         コントロールボタン       81         コントロールボタン       81         コネクター       82         ビロントロールボタクター       83	ピアツーピアSIP (P2PSIP)	71
イベントのルールを設定する       73         NATトラバーサル       73         アプリケーション       73         トラブルシューティング       74         工場出荷時の設定にリセットする       74         AXIS OSの現在のバージョンを確認する       74         AXIS OSをアップグレードする       74         技術的な問題、ヒント、解決策       75         パフォーマンスに関する一般的な検討事項       76         サポートに問い合わせる       77         機器の接続       78         POE (12V)で電力を供給されるリレー       78         別の電源で電力を供給されるリレー       78         別の電源で電力を供給されるリレー       78         外部電源で電力を供給される12 Vフェールセキュアロック       79         外部電源で電力を供給される12 Vフェールセキュアロック       80         仕様       81         フロントパネルインジケーターとコントロール       81         インジケーターアイコン       81         エントレールボタン       81         コントロールボタン       81         コネクター       81         コネクター       81         コントロールボタン       81         コントロールボタン       81         コネクター       81         コネクター       81         コネクター       82         レのコネクター       82         アクローレボクター       83         たの他のメッセージレベル       83	構内交換機 (PBX)	72
NATトラバーサル       73         アプリケーション       73         トラブルシューティング       74         工場出荷時の設定にリセットする       74         AXIS OSの現在のバージョンを確認する       74         AXIS OSをアップグレードする       74         技術的な問題、ヒント、解決策       75         パフォーマンスに関する一般的な検討事項       76         サポートに問い合わせる       77         機器の接続       78         PoE (12V) で電力を供給されるリレー       78         別の電源で電力を供給されるリレー       78         外部電源で電力を供給されるリレー       79         インターカムからのPoEで電力を供給される12 Vフェールセキュアロック       79         外部電源で電力を供給される12 Vフェールセキュアロック       80         仕様       81         フロントパネルインジケーターとコントロール       81         インジケーターアイコン       81         シレトロールボタン       81         コントロールボタン       81         コントロールボタン       81         コントロールボタン       81         コントロールボタン       81         コントロールボタン       81         コネクター       81         コントロールボタン       81         コントロールボタン       81         コントロールボタン       81         スクター       82         レロシトローレボタン       82         ケクター       82	イベントのルールを設定する	73
アプリケーション       73         トラブルシューティング       74         工場出荷時の設定にリセットする       74         AXIS OSの現在のバージョンを確認する       74         AXIS OSの現在のバージョンを確認する       74         AXIS OSをアップグレードする       74         技術的な問題、ヒント、解決策       75         パフォーマンスに関する一般的な検討事項       76         サポートに問い合わせる       77         機器の接続       78         PoE (12V) で電力を供給されるリレー       78         別の電源で電力を供給されるリレー       78         解電圧リレー       78         アロントパネルインジケーターとコントロール       79         外部電源で電力を供給される12 Vフェールセキュアロック       80         仕様       81         フロントパネルインジケーターとコントロール       81         インジケーターアイコン       81         メロントワネルインジケーターとコントロール       81         オンシトロールボタン       81         コントロールボタン       81         コントロールボタン       81         コネクター       81         オットワークコネクター       82         レロール       82         アントワーク       82         ケクター       82         アクター       82         アクター       82         アクター       82         アクター       82         アクレベル<	NATトラバーサル	73
トラブルシューティング       74         工場出荷時の設定にリセットする	アプリケーション	73
工場出荷時の設定にリセットする       74         AXIS OSの現在のバージョンを確認する       74         AXIS OSをアップグレードする       74         AXIS OSをアップグレードする       74         技術的な問題、ヒント、解決策       75         パフォーマンスに関する一般的な検討事項       76         サポートに問い合わせる       77         機器の接続       78         PoE (12V) で電力を供給されるリレー       78         別の電源で電力を供給されるリレー       78         解電圧リレー       79         インターカムからのPoEで電力を供給される12 Vフェールセキュアロック       79         外部電源で電力を供給される12 Vフェールセキュアロック       80         仕様       81         フロントパネルインジケーターとコントロール       81         インジケーターアイコン       81         LEDインジケーター       81         ゴントロールボタン       81         コネクター       81         ボタン       81         コネクター       81         マクター       81         マクター       82         レクコネクター       82         レクロールボタン       81         スクター       82         アクター       82         アクター       82         アクター       82         方の他の       83         アクター       83         アクター       83	トラブルシューティング	74
AXIS OSの現在のバージョンを確認する	工場出荷時の設定にリセットする	74
AXIS OSをアップグレードする       74         技術的な問題、ヒント、解決策       75         パフォーマンスに関する一般的な検討事項       76         サポートに問い合わせる       77         機器の接続       78         PoE (12V) で電力を供給されるリレー       78         別の電源で電力を供給されるリレー       78         離電圧リレー       79         インターカムからのPoEで電力を供給される12 Vフェールセキュアロック       79         インターカムからのPoEで電力を供給される12 Vフェールセキュアロック       80         仕様       81         フロントパネルインジケーターとコントロール       81         インジケーターアイコン       81         SDカードスロット       81         ゴントロールボタン       81         コントロールボタン       81         コントロールボタン       81         スクター       81         高方クター       81         高レクター       81         コントロールボタン       81         コントロールボタン       81         スクター       81         高レーク       82         ドローの       81         オクター       82         ドローの       83         ための       83         たの       83         たの他の       83         たの       83	AXIS OSの現在のバージョンを確認する	74
技術的な問題、ヒント、解決策       75         パフォーマンスに関する一般的な検討事項       76         サポートに問い合わせる       77         機器の接続       78         PoE (12W) で電力を供給されるリレー       78         別の電源で電力を供給されるリレー       78         無電圧リレー       79         インターカムからのPoEで電力を供給される12 Vフェールセキュアロック       79         外部電源で電力を供給される12 Vフェールセキュアロック       80         仕様       81         フロントパネルインジケーターとコントロール       81         インジケーターアイコン       81         エレインジケーター       81         エレー・パネルインジケーターとコントロール       81         エレー・パネルインジケーター       81         コントロールボタン       81         コネクター       81         コネクター       81         マクター       81         マクター       81         コネクター       81         マクター       81         アクター       81         マクター       81         アクター       81         アクター       81         アクター       82         安全情報       83         危険レベル       83         その他のメッセージレベル       83	AXIS OSをアップグレードする	74
パフォーマン人に関する一般的な検討事項       /6         サポートに問い合わせる       77         機器の接続       78         PoE (12V) で電力を供給されるリレー       78         別の電源で電力を供給されるリレー       78         第回後週で電力を供給されるリレー       79         インターカムからのPoEで電力を供給される12 Vフェールセキュアロック       79         外部電源で電力を供給される12 Vフェールセキュアロック       79         外部電源で電力を供給される12 Vフェールセキュアロック       80         仕様       81         フロントパネルインジケーターとコントロール       81         インジケーターアイコン       81         エントロールボタン       81         コントロールボタン       81         コントロールボタン       81         コネクター       81         マントワークコネクター       81         ネットワークコネクター       81         高力(クター       81         アクター       81         スクター       81         アクター       81         スクター       81         ミントロークリン       81         スクター       81         マクター       81         スクター       82         安全情報       83         ためレベル       83         その他のメッセージレベル       83		
サホートに問い合わせる       //         機器の接続       78         POE (12V) で電力を供給されるリレー       78         別の電源で電力を供給されるリレー       78         無電圧リレー       79         インターカムからのPoEで電力を供給される12 Vフェールセキュアロック       79         外部電源で電力を供給される12 Vフェールセキュアロック       80         仕様       81         フロントパネルインジケーターとコントロール       81         インジケーターアイコン       81         エレンジケーター       81         エレンシジケーター       81         コントロールボタン       81         コントロールボタン       81         コントロールボタン       81         コネクター       81         マントワーク コネクター       81         マクター       81         スクター       81         高声コネクター       82         安全情報       83         危険レベル       83         その他のメッセージレベル       83	パフォーマン人に関する一般的な検討事項	/6
機器の接続       78         PoE (12V) で電力を供給されるリレー	サホートに問い合わせる	//
POE (120) で電力を供給されるリレー		
別の電源で電力を供給されるリレー	POE (12V) で電刀を供給されるリレー	/8
無電圧リレー	別の電源で電力を供給されるリレー	
インダーガムがらのFOE C電力を供給される12 Vフェールセキュアロック       79         外部電源で電力を供給される12 Vフェールセキュアロック       80         仕様       81         フロントパネルインジケーターとコントロール       81         インジケーターアイコン       81         SDカードスロット       81         ボタン       81         コントロールボタン       81         コネクター       81         青声コネクター       81         安全情報       83         危険レベル       83         その他のメッセージレベル       83	無電圧リレー	
外部電源で電力を供給される12 Vノエールセキュアロック       80         仕様       81         フロントパネルインジケーターとコントロール       81         インジケーターアイコン       81         LEDインジケーター       81         SDカードスロット       81         ボタン       81         コントロールボタン       81         ネットワークコネクター       81         音声コネクター       82         ド/Oコネクター       82         安全情報       83         危険レベル       83         その他のメッセージレベル       83	イノダーカムからのPOEで電力を供給されるIZVフェールセキュアロック	
マロントパネルインジケーターとコントロール       81         インジケーターアイコン       81         LEDインジケーター       81         SDカードスロット       81         ボタン       81         コントロールボタン       81         コネクター       81         キットワークコネクター       81         音声コネクター       82         レ/Oコネクター       82         安全情報       83         危険レベル       83         その他のメッセージレベル       83	外部電源で電力を供称される12 Vノエールセキュアロック	80 01
インジケーターアイコン       81         LEDインジケーター       81         SDカードスロット       81         ボタン       81         コントロールボタン       81         コネクター       81         ネットワーク コネクター       81         音声コネクター       81         どの山ネクター       82         安全情報       83         危険レベル       83         その他のメッセージレベル       83	$\neg \Box \lor k l^2 \neq l l l \land \lor \land \land$	۱ ۵۵۱ 21
1 レンジケーター       81         LEDインジケーター       81         SDカードスロット       81         ボタン       81         コントロールボタン       81         コネクター       81         ネットワークコネクター       81         音声コネクター       81         レ〇コネクター       82         安全情報       83         危険レベル       83         その他のメッセージレベル       83	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	۵۱ 21
SDカードスロット       .81         ボタン       .81         コントロールボタン       .81         コネクター       .81         ネットワーク コネクター       .81         音声コネクター       .81         ビ/Oコネクター       .82         安全情報       .83         危険レベル       .83         その他のメッセージレベル       .83	(1)	۵۱ 21
ボタン	$SD \pi - \kappa Z \Box \gamma \kappa$	
コントロールボタン	30.53 「ハロノー	
コネクター	コントロールボタン	
ネットワークコネクター	コネクター	
音声コネクター	ニー・シン ニー・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	
VOコネクター	ー クーク・クローク 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一	
安全情報	1/0コネクター	
6険レベル	安全情報	
その他のメッセージレベル	6険レベル	
	その他のメッセージレベル	

## 設定の概要



- 1 インターコム 2 インターカムとAXIS A9801の組み合わせ 3 インターカムとAXIS A9161の組み合わせ 4 インターカムとリーダーおよびアクセスコントロールシステムの組み合わせ (AXIS A1001やAXIS A1601など)

## 製品概要







### 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<sup>®</sup>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™	Safari®
Windows®	推奨	推奨	✓	
macOS®	推奨	推奨	✓	$\checkmark$
Linux®	推奨	推奨	✓	
その他のオペ レーティングシ ステム	1	1	1	√*

\* iOS 15またはiPadOS 15でAXIS OS Webインターフェースを使用するには、

[Settings (設定)] > [Safari] > [Advanced (詳細)] > [Experimental Features (実験的機能)]に移動 し、[NSURLSession Websocket]を無効にします。

#### 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。

## 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。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。

### 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

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

デバイスのパスワードは主にデータおよびサービスを保護します。Axisデバイスは、さまざまなタイプのインストールで使用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)。

## デバイスを構成する

このセクションでは、ハードウェアのインストールが完了した後に製品を起動して実行するため に、設置者が行う必要のあるすべての重要な設定について説明しています。

## ダイレクトSIP (P2P) を設定する

VoIP (Voice over IP) は、IPネットワーク上の音声通信とマルチメディア通信を可能にするテクノロジー群です。詳細については、を参照してください。

この装置では、SIPプロトコルによってVoIPが有効になっています。SIPの詳細については、を参照 してください。

SIPSの設定には2つのタイプがあり、ダイレクトまたはピアツーピア (P2P) がその1つです。同じIP ネットワーク内の少数のユーザーエージェント間で通信が行われ、PBXサーバーが提供する追加機 能が必要ない場合は、ピアツーピアを使用します。設定する方法については、を参照してください。

- 1. [Communication > SIP > Settings (通信 > SIP > 設定)] に移動し、[Enable SIP (SIPの有効化)] を選択します。
- 2. デバイスでの着信呼び出しの受信を許可するには、[Allow incoming calls (着信呼び出し を許可)] を選択します。

#### 注意

着信呼び出しを許可すると、デバイスはネットワークに接続されたすべてのデバイスからの呼び出しを受け付けます。公共のネットワークまたはインターネットから装置にアクセスできる 場合は、着信の呼び出しを無効化することをお勧めします。

- 3. [Call handling (呼び出しの処理)] をクリックします。
- [Calling timeout (呼び出しタイムアウト)] で、応答がない場合に呼び出しが終了するまでの秒数を設定します。
- 5. 着信呼び出しを許可している場合は、[Incoming call timeout (着信呼び出しタイムアウ ト)] で着信呼び出しでタイムアウトするまでの秒数を設定します。
- 6. [Ports (ポート)] をクリックします。
- 7. [SIP port (SIPポート)] の番号と [TLS port (TLSポート)] の番号を入力します。

注

- SIP port (SIPポート) SIPセッション用。このポートを経由する信号トラフィックは暗号化 されません。デフォルトポート番号は5060です。
- TLS port (TLS ポート) TLSで保護されたSIPセッションで使用します。このポートを経由する信号トラフィックは、Transport Layer Security (TLS)を使用して暗号化されます。デフォルトポート番号は5061です。
- RTP start port (RTP開始ポート) SIP呼び出しの最初のRTPメディアストリームで使用する ポートを入力します。デフォルトの開始ポートは4000です。一部のファイアウォールで は、特定のポート番号のポートを経由するRTPトラフィックをブロックできます。ポート番 号は、1024~65535の間で指定してください。
- 8. [NAT traversal (NATトラバーサル)] をクリックします。
- 9. NATトラバーサルを有効にするためのプロトコルを選択します。

注

NATトラバーサルは、デバイスがNATルーターまたはファイアウォール経由でネットワークに 接続している場合に使用します。詳細については、を参照してください。

10. [保存] をクリックします。

## サーバーを介してSIPを設定する (PBX)

VoIP (Voice over IP) は、IPネットワーク上の音声通信とマルチメディア通信を可能にするテクノロジー群です。詳細については、を参照してください。

この装置では、SIPプロトコルによってVoIPが有効になっています。SIPの詳細については、を参照 してください。

SIPSの設定には2つのタイプがあり、PBXサーバーはそのうちの1つでです。PBXサーバーは、IP ネットワークの内外で無制限の数のユーザーエージェントの間で通信を行う必要がある場合に使 用します。PBXプロバイダーによっては、設定に機能が追加される場合があります。詳細について は、を参照してください。

- 1. PBXプロバイダーから以下の情報を入手してください。
  - ユーザーID
  - ドメイン
  - パスワード
  - 認証ID
  - 呼び出し側ID
  - レジストラ
  - RTP開始ポート
- 2. [Communication (通信)] > [SIP] > [Accounts (アカウント)] に移動し、[+ Add account (アカウントを追加)] をクリックします。
- 3. アカウントの [Name (名前)] を入力します。
- 4. [Registered (登録済み)] を選択します。
- 5. Transport mode (伝送モード)を選択します。
- 6. PBXプロバイダーからのアカウント情報を追加します。
- 7. [保存]をクリックします。
- 8. ピアツーピアの場合と同じ方法でのSIPの設定については、を参照してください。PBXプロ バイダーのRTP開始ポートを使用します。

#### 連絡先の作成

この例では、連絡先リストで新しい連絡先を作成する方法について説明します。開始する前に、 [Communication > SIP (通信 > SIP)] でSIPを有効にしてください。

新しい連絡先を作成する方法:

- 1. [Communication > Contact list (通信 > 連絡先リスト)] に移動します。
- 2. [+ Add contact (連絡先を追加)] をクリックします。
- 3. 連絡先の姓名を入力します。
- 4. 連絡先のSIPアドレスを入力します。

#### 注

SIPアドレスの詳細については、を参照してください。

5. 呼び出し元のSIPアカウントを選択します。

#### 注

可用性オプションは、[System (システム)] > [Events (イベント)] > [Schedules (スケジュー ル)] で定義します。

6. 連絡先の [Availability (可用性)] を選択します。連絡先が対応できないときに呼び出しが あった場合、フォールバックがない限り、呼び出しはキャンセルされます。

#### 注

フォールバックとは、元の連絡先が応答しない場合、または対応できない場合に転送される連絡先です。

- 7. [Fallback (フォールバック)] で、[None (なし)] を選択します。
- 8. [保存]をクリックします。

#### 呼び出しボタンの設定

デフォルトでは、呼び出しボタンはVMS (ビデオ管理ソフトウェア) 呼び出しを行うように設定されています。この設定を維持する場合は、AxisインターカムをVMSに追加するだけです。

この例では、訪問者が呼び出しボタンを押したときに連絡先リストにある連絡先を呼び出すよう に、システムを設定する方法について説明します。

- 1. [Communication > Calls > Call button (通信 > 呼び出し > 呼び出しボタン)] に移動します。
- 2. [Recipients (送信先)] で、[VMS] を削除します。
- 3. [Recipients (送信先)] で、既存の連絡先を選択するか、新しい連絡先を作成します。

呼び出しボタンを無効にするには、[Enable call button (呼び出しボタンを有効にする)] をオフ にします。

#### DTMFを使用して来訪時にドアのロックを解除する

訪問者がインターカムから呼び出しを行うと、応答者は自身のDual-Tone Multi-Frequency (DTMF) を使用して、ドアのロックを解除できます。ドアコントローラーにより、ドアのロック/ロック解 除を行います。

この例では、次の方法について説明します。

- インターカムのDTMF信号を定義する
- 次のようにインターカムを設定します。
  - ドアコントローラーにドアのロックを解除するように要求するか、または
  - 内部リレーを使用してドアのロックを解除します。

すべての設定はインターカムのWebページで行います。

開始する前に

・ 装置からのSIP呼び出しを許可し、SIPアカウントを作成します。「」および「」を参照して ください。

インターカムのDTMF信号を定義する

- 1. [Communication (通信)] > [SIP] > [DTMF] に移動します。
- 2. [+ Add sequence (シーケンスを追加)] をクリックします。
- 3. [Sequence (シーケンス)] に「1」と入力します。
- 4. [Description (説明)] に、「Unlock door (ドアロック解除)」と入力します。
- 5. [Accounts (アカウント)] で、SIPアカウントを選択します。
- 6. [保存]をクリックします。
- 内部リレーを使用してドアのロックを解除するように、インターカムを設定する
  - [System > Events > Rules (システム > イベント > ルール)] に移動し、ルールを追加します。
  - 8. [Name (名前)] フィールドに「DTMF unlock door (DTMFドアロック解除)」と入力します。
  - 9. 条件リストの [Call (呼び出し)] で、[DTMF] を選択し、続いて [Unlock door (ドアのロック解除)] を選択します。
  - 10. アクションのリストから [**I/O**] で [**Toggle I/O once (I/Oを一度切り替える)**] を選択しま す。

- 11. ポートのリストから、[Relay 1 (リレー1)] を選択します。
- 12. 継続時間を 00:00:07 に変更します。この場合、ドアのロックが7秒間解除されます。
- 13. [保存] をクリックします。

#### ナイトモードを使用して低光量下で赤外線照明からメリットを得る

日中、カメラは可視光を利用してカラー画像を提供します。しかし、可視光線が薄くなると、色の画像は明るく鮮明になります。この場合、ナイトモードに切り替えた場合、カメラは可視光と 近赤外線の両方の光を使用して、代わりに明るい画像と詳細な白黒画像を提供します。カメラが 自動的にナイトモードに切り替わります。

1. [Video > Image > Day and night (設定 > 画像 > デイナイト)] に移動し、[IR cut filter (IR カットフィルター)] が [Auto (自動)] に設定されていることを確認します。 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ブラウザーで装置のIPアドレスを入力しま 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。

#### 進行中の録画

進行中の録画と指定されたストレージ容量を表示します。

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

□ 録画を保存するストレージの空き容量を表示します。

### コミュニケーション

連絡先リスト

連絡先

 $\square$ 

➡ :クリックして、連絡先リストをjsonファイルとしてダウンロードします。 4 : クリックして、連絡先リスト (ison) をインポートします。 + Add contact (連絡先の追加):クリックして、新しい連絡先を連絡先リストに追加します。 Upload image (画像のアップロード) : クリックして、連絡先を表す画像をアップロードし ます。 First name (名):連絡先の名を入力します。 Last name (姓):連絡先の姓を入力します。 Speed dial (短縮ダイヤル) :連絡先に使用できる短縮ダイヤル番号を入力します。この番 号は、装置から連絡先を呼び出すのに使用されます。 SIPアドレス:SIPを使用する場合は、連絡先のIPアドレスまたは内線番号を入力します。 🎙 : クリックして、テスト呼び出しを行います。応答があると、呼び出しは自動的に終了しま す。 SIPアカウント:SIPを使用する場合、装置から連絡先への呼び出しに使用するSIPアカウントを選 択します。 Availability (対応可能):連絡先の対応可能スケジュールを選択します。[System (システム)] > [Events (イベント)] > [Schedules (スケジュール)] でスケジュールの追加や調整を行えます。 連絡先が対応できないときに呼び出しが試行された場合、フォールバックがない限り、呼び出し はキャンセルされます。 Fallback (フォールバック):該当する場合は、リストからフォールバックを選択します。 Notes (メモ):連絡先に関する任意の情報を追加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。

Edit contact (連絡先の編集):連絡先のプロパティを編集します。

Delete contact (連絡先の削除):連絡先を削除します。

SIP

設定

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

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

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

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

呼び出し処理

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

ポート

- ポート番号は1024~65535の間で指定する必要があります。
  - SIPポート:SIP通信に使用するネットワークポートです。このポートを経由する信号トラフィックは暗号化されません。デフォルトポート番号は5060です。必要に応じて異なるポート番号を入力します。
  - TLSポート:暗号化されたSIP通信に使用するネットワークポートです。このポートを経由 する信号トラフィックは、Transport Layer Security (TLS)を使用して暗号化されます。デ フォルトポート番号は5061です。必要に応じて異なるポート番号を入力します。
  - RTP開始ポート番号:SIP呼び出しで最初のRTPメディアストリームに使用されるネット ワークポートです。デフォルトの開始ポート番号は4000です。ファイアウォールは、特 定のポート番号のRTPトラフィックをブロックします。

NATトラバーサル

NAT (ネットワークアドレス変換) トラバーサルは、プライベートネットワーク (LAN) 上にある装置を、そのネットワークの外部から利用できるようにする場合に使用します。

注

NATトラバーサルを機能させるには、ルーターがNATトラバーサルに対応している必要があります。また、UPnP®にも対応している必要があります。

NATトラバーサルプロトコルは個別に使用することも、ネットワーク環境に応じたさまざまな組み合わせで使用することもできます。

- ICE:ICE (双方向接続性確立) プロトコルを使用することで、ピアデバイス間の通信を成功 させるために最も効率の良いパスを見つけやすくなります。STUNやTURNも有効にする と、さらにICEプロトコルで見つけやすくなります。
- STUN:STUN (NATのためのセッショントラバーサルユーティリティ)は、装置がNATまた はファイアウォールを経由して配置されているかどうかを特定し、経由していれば、リ モートホストへの接続に割り当てるマッピングされるパブリックIPアドレスとポート番号 を取得できるようにするクライアント/サーバーネットワークプロトコルです。IPアドレ スなどのSTUNサーバーアドレスを入力します。
- TURN:TURN (NATに関するリレーを使用したトラバーサル) は、NATルーターまたはファ イアウォールを経由するデバイスが、TCPやUDPを介して他のホストから着信データを受 信できるようにするプロトコルです。TURNサーバーアドレスとログイン情報を入力しま す。

音声とビデオ

• **音声コーデックの優先度**:望ましい音声品質で、SIP呼び出しの音声コーデックを1つ以上 選択します。ドラッグアンドドロップして、優先順位を変更します。

注

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

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

•	H.264 packetization mode (H.264パケット化モード):使用するパケット化モードを選択 します。
	- [オート]:(推奨) 使用するパケット化モードは本装置によって決定されます。
	<ul> <li>None (なし):パケット化モードは設定されません。このモードは、多くの場合、</li> <li>モード0と解釈されます。</li> </ul>
	- <b>0</b> : ノンインターリーブモード。
	- 1:シングルNALユニットモード。
•	<b>ビデオの方向</b> :許可されているビデオの方向を選択します。
•	Show video in call (通話中にビデオを表示) i :受信したビデオストリームをデバイスの画面に表示します。
その作	
•	UDP-to-TCP switching (UDPからTCPへの切り替え):選択して、転送プロトコルをUDP (User Datagram Protocol) からTCP (Transmission Control Protocol) に一時的に切り替えま す。切り替えるのはフラグメンテーションを避けるためであり、要求が200バイト以内ま たは1300バイト以上の最大転送ユニット (MTU) の場合に実行されます。
•	<b>Allow via rewrite (経由のリライトを許可)</b> :選択して、ルーターのパブリックIPアドレス の代わりに、ローカルIPアドレスを送信します。
•	Allow contact rewrite (接続のリライトを許可):選択して、ルーターのパブリックIPアド レスの代わりに、ローカルIPアドレスを送信します。
•	<b>Register with server every (サーバーに登録)</b> :既存のSIPアカウントで、装置をSIPサー バーに登録する頻度を設定します。
•	<b>DTMF payload type (DTMFのペイロードタイプ)</b> :DTMFのデフォルトのペイロードタイ プを変更します。
•	Max retransmissions (最大再送回数):装置が試行を停止するまでにSIPサーバーへの接続 を試行する最大回数を設定します。
•	<b>Seconds until failback (フェイルバックまでの秒数)</b> :装置がセカンダリSIPサーバーに フェイルオーバーした後、プライマリSIPサーバーへの再接続を試みるまでの秒数を設定 します。

アカウント

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

アカウントをSIPサーバーに正常に登録できました。

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

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

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

- Active (アクティブ):アカウントを使用できるようにします。
- [デフォルトにする]:このアカウントをデフォルトに設定します。デフォルトのアカウントは必須で、デフォルトに設定できるのは1つだけです。
- [自動応答]:着信呼び出しに自動的に応答するにはこれを選択します。
- IPv4よりIPv6を優先

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

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

#### DTMF

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

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

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

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

### プロトコル

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

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

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

### 呼び出しのテスト

SIPアカウント:テスト呼び出しを行うアカウントを選択します。

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

## アクセスリスト

Use access list (アクセスリストを使用する):装置への呼び出しができるユーザーを制限する場合は、オンにします。

Policy (ポリシー):

- ・ Allow (許可):アクセスリスト内のソースからの着信のみを許可する場合に選択します。
- Block (ブロック):アクセスリスト内のソースからの着信をブロックする場合に選択します。

+ Add source (ソースの追加): クリックして、アクセスリストに新しいエントリを作成します。

SIP source (SIPソース):ソースの呼び出し元IDまたはSIPサーバーアドレスを入力します。

## 呼び出し

### 呼び出しボタン

Use call button (コールボタンを使用):オンにすると、呼び出しボタンが使用できるようになります。

**Button functionality during a call (通話中のボタン機能)**:デバイスから通話が開始されたら、 コールボタンの機能を選択します。

- End the call (通話を終了):訪問者が発信中にコールボタンを押すと、通話が終了します。 訪問者がいつでも通話を終了できるようにするには、このオプションを使用してください。
- No functionality until the call has ended (通話が終了するまで機能しない):訪問者が発信中にコールボタンを押しても反応しません。訪問者が通話を終了できないようにするには、このオプションを使用してください。
- Delay before you can end the call (通話を終了できるまでの遅延):訪問者が通話を開始 した後、[Delay (seconds) (遅延 (秒))] で設定された時間内は、コールボタンを押しても 反応しません。遅延時間の経過後にコールボタンを押すと通話が終了します。このオプ ションを使用すると、訪問者が二度押しによって意図せず通話を終了するのを防ぐこと ができます。
  - Delay (seconds) (遅延(秒)): コールボタンを2回目に押したときに通話が終了する ようになるまでの時間を入力します。

Standby light (スタンバイライト):呼び出しボタン周辺の内蔵ライトのオプションを選択します。

- Auto (オート) U:装置は周囲の明るさに応じて内蔵ライトをオン/オフにします。
- On (オフ):装置がスタンドバイモードのとき、内蔵ライトは常にオンになります。
- Off (オフ):装置がスタンドバイモードのとき、内蔵ライトは常にオフになります。

Recipients (送信先):誰かが呼び出しボタンを押したときに呼び出す連絡先を1つ以上選択または 作成します。複数の送信先を追加すると、呼び出しは同時にすべての送信先に発信されます。 SIP呼び出し送信先の最大数は6ですが、VMS呼び出し送信先の数は無制限です。

Fallback (フォールバック):送信先から応答がない場合に備えて、リストからフォールバックを 追加します。

概要

#### 音声

- 注 ・ 選択した音声クリップは、呼び出し時にのみ再生されます。
  - 発信中に音声クリップやゲインを変更しても、その変更は次の呼び出しまで有効になり ません。

Ringtone (着信音):装置に着信があったときに再生する音声クリップを選択します。スライダーを使用してゲインを調整します。

Ringback tone (発信音):装置から発信があったときに再生する音声クリップを選択します。スライダーを使用してゲインを調整します。

#### VMS呼び出し

VMS呼び出し

ビデオ管理ソフトウェア (VMS) での通話を許可する:装置からVMSへの通話を許可する場合 に選択します。SIP がオフになっている場合も、VMS通話を行うことができます。

呼び出しタイムアウト:誰も応答しない場合の呼び出しの最大継続時間を設定します。

#### 分析機能

#### メタデータの設定

#### RTSPメタデータプロデューサー

メタデータをストリーミングするアプリと、それらのアプリが使用するチャンネルが一覧表示されます。

注

これは、ONVIF XMLを使用しているRTSPメタデータストリームの設定です。ここで行った変更は、メタデータ視覚化ページには影響しません。

**Producer (プロデューサー)**:メタデータを生成するアプリ。アプリの下には、アプリが装置から ストリーミングするメタデータのタイプのリストがあります。

**チャンネル**:アプリが使用するチャンネル。メタデータストリームを有効にするには、選択します。互換性またはリソース管理の理由から選択を解除します。

## ビデオ



□ クリックすると、装置に設定されているストレージが表示されます。ストレージを設定するには管理者権限が必要です。

🙀 クリックすると、その他の設定にアクセスできます。

- ・ ビデオ形式:ライブビューで使用するエンコード方式を選択します。
- **> 自動再生**:オンにすると、この装置を新しいセッションで開くたびにミュートでビデ オストリームを自動再生します。
- ・ クライアントストリームの情報:オンにすると、ライブビデオストリームを表示するブラ ウザーで使用されるビデオストリームの動的な情報が表示されます。ビットレートの情 報は、情報源が異なるため、テキストオーバーレイで表示される情報とは異なります。 クライアントのストリーム情報に含まれるビットレートは、最後の1秒間のビットレート であり、装置のエンコーディングドライバーから取得される数値です。オーバーレイの ビットレートは、過去5秒間の平均ビットレートであり、ブラウザーから提供されます。 どちらの値も、rawビデオストリームのみを対象としており、UDP/TCP/HTTPを介して ネットワーク上で転送される際に発生する追加の帯域幅は含まれていません。
- ・ Adaptive stream (適応ストリーム):オンにすると、表示クライアントの実際のディスプレイ解像度に画像解像度が適応し、ユーザーエクスペリエンスが向上し、クライアントのハードウェアの過負荷を防ぐことができます。適応ストリームが適用されるのは、ブラウザーを使用してwebインターフェースにライブビデオストリームを表示しているときだけです。適応ストリームをオンにすると、最大フレームレートは30フレーム/秒になります。適応ストリームをオンにしている間にスナップショットを撮影すると、そのスナップショットには、適応ストリームで選択した画像解像度が使用されます。
- Level grid (レベルグリッド): をクリックすると、レベルグリッドが表示されます。
   このグリッドは、画像が水平方向に配置されているかどうかを判断するのに役立ちます。
   非表示にするには、をクリックします。
- Pixel counter (ピクセルカウンター): をクリックすると、ピクセルカウンターが表示されます。ボックスをドラッグしてサイズを変更し、特定エリアを含めます。[Width (幅)] と [Height (高さ)] フィールドでボックスのピクセルサイズを定義することもできます。
- Refresh (更新): C をクリックすると、ライブビューの静止画像を更新できます。
- PTZコントロール (i):オンにすると、PTZコントロールがライブビューに表示されます。

()・1) クリックすると、ライブビューがフル解像度で表示されます。フル解像度が画面サイズより大きい場合は、小さい画像を使って画像内を移動してください。

・ クリックすると、ライブビデオストリームが全画面表示されます。ESCキーを押すと、全画面モードが終了します。

## インストール

取り付け位置 ():カメラのマウント方法によって、画像の向きが変わる場合があります。

Power line frequency (電源周波数):画像のちらつきを最小限に抑えるために、お使いの地域で 使用されている周波数を選択してください。アメリカ地域では、通常60 Hzが使用されていま す。世界の他の部分では、ほとんどの場合50 Hzで使用されています。お客様の地域の電源周波 数がわからない場合は、地方自治体に確認してください。

### 画像

表示



ワイドダイナミック レンジ

WDR : 画像の暗い部分と明るい部分の両方が見えるようにする場合にオンにします。

**ローカルコントラスト**():スライダーで画像のコントラストを調整します。値が大きいほど、 暗い部分と明るい部分のコントラストが高くなります。

**トーンマッピング**:スライダーを使用して、画像に適用されるトーンマッピングの量を調整 します。この値を0に設定すると、標準のガンマ補正のみが適用され、この値を大きくすると、 画像内の最も暗い部分と最も明るい部分の可視性が高くなります。

## ホワイトバランス

届いた光の色温度がカメラで検知される場合は、その色がより自然に見えるように画像を調整することができます。これで十分でない場合は、リストから適切な光源を選択できます。

ホワイトバランスの自動設定では、色のゆらぎを抑えるため、ホワイトバランスが緩やかに変更 されます。光源が変わったときや、カメラの電源を初めて投入したときは、新しい光源に適合す るまでに最大で30秒かかります。シーン内に色温度が異なる複数のタイプの光源がある場合は、 最も支配的な光源が自動ホワイトバランスアルゴリズムの基準になります。この動作を変更する には、基準として使用する光源に合った固定ホワイトバランスの設定を選択してください。

#### 照度環境:

- Automatic (自動):光源の色を自動的に識別し、それに合わせて色を補正します。通常は この設定をお勧めします。ほとんどの状況で使用できます。
- 自動 屋外 U:光源の色を自動的に識別し、それに合わせて色を補正します。通常はこの設定をお勧めします。屋外のほとんどの状況で使用できます。
- ・ カスタム 屋内 🙂 : 蛍光灯以外の人工照明がある部屋向けの固定カラー調整。通常の色 温度が約2800 Kの場合に適しています。
- ・ カスタム 屋外 🕕: 色温度が約5500 Kの晴天気象条件向けの固定カラー調整。
- Fixed fluorescent 1 (固定 蛍光灯1): 色温度が約4000 Kの蛍光灯向けの固定カラー調整。
- Fixed fluorescent 2 (固定 蛍光灯2): 色温度が約3000 Kの蛍光灯向けの固定カラー調整。
- ・ 固定 屋内:蛍光灯以外の人工照明がある部屋向けの固定カラー調整。通常の色温度が約 2800 Kの場合に適しています。
- ・ 固定 屋外1: 色温度が約5500 Kの晴天気象条件向けの固定カラー調整。
- ・ 固定 屋外2:色温度が約6500 Kの曇天気象条件向けの固定カラー調整。
- 街灯 水銀灯 (1):街灯で一般的に使用される水銀灯の紫外線発光に対する固定カラー調整。
- **街灯 ナトリウム灯** (1):街灯で一般的に使用されるナトリウム灯の黄色・オレンジ色を 補正する固定カラー調整。
- Hold current (現在の状態で固定):現在の設定を保持し、照度が変化しても補正を行いません。
- 手動

   :白色の被写体を利用して、ホワイトバランスを修正します。ライブビュー画像の中で、カメラに白として解釈させる物体に円をドラッグします。[Red balance (レッドバランス)] と
   [Blue balance (ブルーバランス)] スライダーを使用して、ホワイトバランスを手動で調整します。

### デイナイトモード

IR-cut filter (IRカットフィルター):

 [オート]:選択すると、IRカットフィルターのオンとオフが自動的に切り替わります。カメ ラがデイモードになっていると、IRカットフィルターが有効になり、入射する赤外線照明 がフィルターで除去されます。ナイトモードになっていると、IRカットフィルターが無効 になり、カメラの光感度が上がります。

注

- 一部の装置では、ナイトモードでIRパスフィルターが使用されます。IRパスフィルターは 赤外線照明感度を高めますが、可視光を遮断します。
- On (オン):IRカットフィルターをオンにする場合に選択します。画像はカラーですが、光 感度は低下します。
- Off (オフ):IRカットフィルターをオフにする場合に選択します。光感度が高くなると、画像は白黒になります。

Threshold (閾値):スライダーを使用して、カメラがデイモードからナイトモードに移行する光の 閾値を調整します。

- IRカットフィルターの閾値を低くするには、バーを [**Bright (明るい)**] の方向に移動しま す。カメラがナイトモードに変わるタイミングは早くなります。
- IRカットフィルターの閾値を高くするには、スライダーを [Dark (暗い)] の方に移動しま す。これにより、カメラがナイトモードに変わるタイミングが遅くなります。

## 赤外線照明 🖳

照明が内蔵されていないデバイスでは、これらのコントロールは対応するAxisイルミネーターが 接続されている場合にのみ利用できます。

Allow illumination (照明を許可):オンにすると、カメラが内蔵照明をナイトモードで使用できます。

Synchronize illumination (照明の同期):オンにすると、周囲の明るさに合わせて自動的に照明 が同期します。昼と夜の同期は、IRカットフィルターが [自動] または [オフ] に設定されている 場合にのみ機能します。

自動照明角度 U:オンにすると、自動照明角度が使用されます。照明角度を手動で設定するには、オフにします。

**照明角度 ──**:カメラの画角とは異なる角度で照明する必要がある場合などは、スライダーを 使って手動で照明の角度を設定できます。カメラが広角であれば、照明の角度をより狭角(望遠 側)に設定できます。ただし、映像の隅の部分が暗くなります。

IR波長 🕕 :赤外線照明の波長を選択します。

白色光(

照明を許可 ():オンにすると、カメラはナイトモードで白色光を使用します。

照明を同期 U:オンにすると、周囲の明るさに合わせて自動的に白色光が同期します。

### 露出

露出モードを選択すると、さまざまなタイプの光源によって生じるちらつきなど、画像内で急速 に変化する不規則な影響を緩和できます。自動露出モード、または電源ネットワークと同じ周波 数を使用することをお勧めします。

露出モード: Automatic (自動):カメラが開口、ゲイン、シャッターを自動的に調整します。 • 白動開口 :カメラが開口とゲインを自動的に調整します。シャッターは固定です。 i, :カメラがシャッターとゲインを自動的に調整します。開口は固定で 自動シャッター す。 現在の状態で固定:現在の露出設定に固定します。 ちらつき防止 :カメラが開口とゲインを自動的に調整し、次のシャッター速度のみを 使用します。1/50秒 (50 Hz) と1/60秒 (60 Hz)。 ちらつき防止 (50Hz) (i):カメラが開口とゲインを自動的に調整し、シャッター速度は 1/50秒を使用します。 ▶ :カメラが開口とゲインを自動的に調整し、シャッター速度は ちらつき防止 (60Hz) 1/60秒を使用します。 ちらつき低減 (i):これはちらつき防止と同じですが、明るいシーンでは1/100秒 (50 Hz) および1/120秒 (60 Hz) より速いシャッター速度を使用できます。 ちらつき低減 (50 Hz) ():ちらつき防止と同じですが、明るいシーンでは1/100秒より速いシャッター速度を使用できます。 ちらつき低減 (60 Hz) :ちらつき防止と同じですが、明るいシーンでは1/120秒より速 いシャッター速度を使用できます。 **手動録画** ● :開口、ゲイン、シャッターは固定です。 **露出エリア**():露出エリアを使用すると、入口のドアの前のエリアなど、シーンの選択した部 分の露出を最適化できます。 注 露出エリアは元の画像 (回転していない状態) に関連付けられているため、エリアの名前が元 の画像に適用されます。つまり、たとえばビデオストリームが90°回転した場合、ストリー ム内のゾーンの [Upper (上)] は [Right (右)] になり、 [Left (左)」は「Lower (下)」になりま す。 Automatic (自動):ほとんどの状況に適しています。 中央:画像の中央部の固定エリアを使用して露出が計算されます。このエリアは、ライブ ビュー内でサイズと位置が固定されています。 フル :ライブビュー全体を使用して露出が計算されます。 ۲Ļ :画像の上部にあるサイズと位置が固定されたエリアを使用して露出が計算されま す。 i. 下 :画像の下部にあるサイズと位置が固定されたエリアを使用して露出が計算されま す。 i. 左' :画像の左にあるサイズと位置が固定されたエリアを使用して露出が計算されま

す。

- 右 U: :画像の右にあるサイズと位置が固定されたエリアを使用して露出が計算されます。
- スポット:ライブビュー内にあるサイズと位置が固定されたエリアを使用して露出が計算 されます。
- **カスタム**:ライブビュー内の一部のエリアを使用して露出が計算されます。エリアのサイズと位置を調整できます。

**最大シャッター**:最良の画質が得られるように、シャッター速度を選択します。シャッター速度 が遅いと (露出が長いと)、動きがあるときに動きによる画像のブレが生じることがあり、シャッ ター速度が速すぎると画質に影響を与えることがあります。最大ゲインで最大シャッターが機能 すると、画質が向上します。

**最大ゲイン**:適切な最大ゲインを選択します。最大ゲインを増やすと、暗い画像で細部を確認で きるレベルは向上しますが、ノイズレベルも増加します。ノイズが多くなると、帯域幅とスト レージの使用も多くなる可能性があります。最大ゲインを高い値に設定した場合、昼と夜で照明 環境がかなり異なっていると、画像が大きく変化する可能性があります。最大シャッターで最大 ゲインが機能すると、画質が向上します。

**動き適応型の露出機能** ():これを選択して低光量下で動きによる画像のブレを減らします。

Blur-noise trade-off (ブレとノイズのトレードオフ):スライダーを使用して動きによる画像のブレとノイズの間で優先度を調整します。動く物体の細部が不鮮明になっても、帯域幅の使用とノイズが少ないことを優先する場合は、このスライダーを[低ノイズ]の方に移動します。帯域幅の使用とノイズが多くなっても、動く物体の細部を鮮明に保つことを優先する場合は、スライダーを[動きによる画像のブレが少ない]の方に移動します。

注

露出の変更は、露出時間を調整して行うこともゲインを調整しても行うこともできます。露 出時間を長くすると動きによる画像のブレが増し、ゲインを大きくするとノイズが増えま す。[Blur-noise trade-off (ブレとノイズのトレードオフ)] を [Low noise (低ノイズ)] 側に調 整した場合、自動露出にするとゲインを上げることよりも露出時間を長くすることが優先さ れ、トレードオフを [Low motion blur (動きによる画像のブレが少ない)] 側に調整するとそ の逆になります。低光量の条件下では、設定された優先度にかかわらず、最終的にはゲイン と露出時間の両方が最大値に達します。

開口のロック ():オンにすると、[Aperture (開口)] スライダーで設定された開口サイズが維持 されます。オフにすると、開口サイズをカメラで自動的に調整できます。たとえば、点灯した状 態が継続しているシーンで開口をロックすることができます。

開口:スライダーを使用して開口サイズ (レンズからどれだけ光を取り込むか)を調整しま す。暗い場所でより多くの光をセンサーに取り込み、より明るい画像を得るには、スライダーを [Open (開く)] 方向に移動します。開口を開くと被写界深度は減少し、カメラの近くまたは遠く にある物体はフォーカスが合っていないように見える可能性があります。画像のフォーカスを拡 大するには、スライダーを [Closed (閉じる)] 方向に移動します。

**露出レベル**:スライダーを使用して画像の露出を調整します。

デフォグ機能 U:オンにすると、霧の影響を検知して自動的に霧を除去するため、より鮮明な 画像が得られます。

注

コントラストが低い、光のレベルの変動が大きい、オートフォーカスがわずかにオフの場合 は、[Defog (デフォッグ)]をオンにすることをお勧めします。その場合は、映像のコントラ ストが増大するなど、画質に影響することがあります。また、光量が多すぎる場合にも、デ フォッグがオンになると画質に悪影響が出るおそれがあります。

## ストリーム

#### 概要

**解像度**:監視シーンに適した画像の解像度を選択します。解像度が高いと、帯域幅とストレージが増大します。

**フレームレート**:ネットワーク上の帯域幅の問題を避けるため、またはストレージサイズを削減 するために、フレームレートを固定値に制限できます。フレームレートをゼロのままにすると、 フレームレートは現在の状況で可能な最大値となります。フレームレートを高くすると、より多 くの帯域幅とストレージ容量が必要になります。

**Pフレーム:**Pフレームは、前のフレームからの画像の変化のみを示す予測画像です。適切なPフレーム数を入力します。値が大きいほど、必要な帯域幅は小さくなります。ただし、ネットワークが輻輳している場合には、ビデオ画質が著しく劣化する可能性があります。

**圧縮**:スライダーを使用して画像の圧縮率を調整します。圧縮率が高いほどビットレートが低くなり、画質が低下します。圧縮率が低いと画質が向上しますが、録画時により多くの帯域幅とストレージを必要とします。

**署名付きビデオ ()**:オンにすると、署名付きビデオ機能がビデオに追加されます。署名付きビ デオは、ビデオに暗号化署名を追加することでビデオをいたずらから保護します。

#### Zipstream

Zipstreamテクノロジーは映像監視用に最適化されたビットレート低減テクノロジーで、H.264またはH.265ストリームの平均ビットレートをリアルタイムで削減します。Axis Zipstream テクノロジーは、動く物体を含むシーンなど、画像内に関心領域が複数あるシーンに対して高いビットレートを適用します。シーンがより静的であれば、Zipstreamは低いビットレートを適用し、ストレージの使用量を削減します。詳細については、「Axis Zipstreamによるビットレートの低減」を参照してください。

ビットレート低減の [Strength (強度)] を選択します。

- ・ Off (オフ):ビットレート低減はありません。
- **低**:ほとんどのシーンで認識できる画質低下なし。これはデフォルトのオプションです。 あらゆるタイプのシーンでビットレートの低減に使用できます。
- **中間**:一部のシーンでは、動きのない部分など、関心の低い領域でノイズが少なく、ディ テールレベルがやや低くなることで、目に見える効果が得られます。
- 高:一部のシーンでは、動きのない部分など、関心の低い範囲でノイズが少なく、ディ テールレベルが低くなることで、目に見える効果が得られます。クラウドに接続された 装置やローカルストレージを使用する装置にはこのレベルを推奨します。
- Higher (さらに高):一部のシーンでは、動きのない部分など、関心の低い範囲でノイズが 少なく、ディテールレベルが低くなることで、目に見える効果が得られます。
- Extreme (極限):大部分のシーンで目に見える効果が得られます。ビットレートは、可能 な限り小さなストレージに最適化されています。

Optimize for storage (ストレージ用に最適化する):オンにし、画質を維持しながらビットレートを最小限に抑えます。この最適化は、Webクライアントに表示されるストリームには適用されません。この機能は、VMSがBフレームをサポートしている場合のみ使用できます。 [Optimize for storage (ストレージ用に最適化)]をオンにすると、[Dynamic GOP (ダイナミックgroup of pictures)] もオンになります。

Dynamic FPS (ダイナミックFPS) (フレーム/秒):オンにすると、シーン内のアクティビティのレベルに応じて帯域幅が変化します。動きが多い場合、より多くの帯域幅が必要です。

**下限**:シーンの動きに応じて、最小フレーム/秒とストリームのデフォルトフレーム/秒の間でフレームレートを調整するための値を入力します。フレーム/秒が1以下になるような動きの少ないシーンでは、下限を設定することをお勧めします。

**Dynamic GOP (ダイナミック group of pictures)**:オンにすると、シーン内のアクティビティのレベルに応じて、I-フレームの間隔が動的に調整されます。

上限:最大GOP長 (2つのI-フレーム間のP-フレームの最大数) を入力します。Iフレームは、他のフ レームとは無関係の自己完結型の画像フレームです。

## ビットレート制御

- Average (平均):より長い時間をかけてビットレートを自動的に調整し、使用可能なスト レージに基づいて最適な画質を提供する場合に選択します。
  - **ジ**クリックすると、利用可能なストレージ、保存時間、ビットレート制限に基づいて目標ビットレートが計算されます。
  - Target bitrate (目標ビットレート):目標とするビットレートを入力します。
  - Retention time (保存期間):録画を保存する日数を入力します。
  - **ストレージ**:ストリームに使用できるストレージの概算が表示されます。
  - Maximum bitrate (最大ビットレート):オンにすると、ビットレートの制限が設定 されます。
  - Bitrate limit (ビットレートの制限):目標ビットレートより高いビットレートの制限を入力してください。
  - ・ Maximum (最大):オンにすると、ネットワーク帯域幅に基づいてストリームの最大瞬時 ビットレートが設定されます。
    - Maximum (最大):最大ビットレートを入力します。
- Variable (可変):オンにすると、シーン内のアクティビティのレベルに基づいてビット レートが変化します。動きが多い場合、より多くの帯域幅が必要です。ほとんどの場 合、このオプションをお勧めします。

## 向き

Mirror (ミラーリング):オンにすると画像が反転します。

## 音声

Include (対象):オンにすると、ビデオストリームで音声が使用されます。 ソース
:使用する音声ソースを選択します。 ステレオ
:オンにすると、内蔵の音声だけでなく、外部のマイクからの音声も取り込むこと ができます。

## オーバーレイ

↑ :クリックするとオーバーレイが追加されます。ドロップダウンリストからオーバーレイの種類を次の中から選択します。

- テキスト:テキストをライブビュー画像に統合し、すべてのビュー、録画、スナップショットに表示する場合に選択します。独自のテキストを入力することもできます。また、あらかじめ設定された修飾子を含めることで、時間、日付、フレームレートなどを自動的に表示することもできます。
  - ・ ・ クリックすると、日付の修飾子%Fを追加して、yyyy-mm-ddを表示できます。
  - ・ クリックすると、時間の修飾子%xを追加して、hh:mm:ss (24時間制) を表示 できます。
  - Modifiers (修飾子):クリックすると、リストに表示された修飾子から選択して、テキストボックスに追加できます。たとえば、%aを選択すると曜日が表示されます。
  - **サイズ**:フォントサイズを選択します。
  - 表示:黒い背景に白いテキスト (デフォルト) など、背景色とテキストの色を選択します。
- Image (画像):ビデオストリームに静止画像を重ねて表示する場合に選択します。.bmp、. png、.jpeg、または.svgファイルを使用できます。
   画像をアップロードするには、[Images (画像)]をクリックします。画像をアップロード する前に、以下の方法を選択できます。
  - Scale with resolution (解像度に伴う拡大/縮小):選択すると、解像度に合わせて オーバーレイ画像のサイズを自動的に変更できます。
  - Use transparency (透明色を使用する):その色のRGB 16進値を選択して入力しま す。RRGGBB形式を使用します。16進数値の例:FFFFFF - 白、000000 - 黒、FF0000 - 赤、6633FF - 青、669900 - 緑。.bmp画像の場合のみ。
- シーンの注釈 :カメラが別の方向にパンまたはチルトした場合でも、ビデオストリームに同じ位置に留まるテキストオーバーレイを表示する場合に選択します。特定のズームレベル内でのみオーバーレイを表示するように選択できます。
  - ・ クリックすると、日付の修飾子%Fを追加して、yyyy-mm-ddを表示できます。
  - じ: クリックすると、時間の修飾子%xを追加して、hh:mm:ss (24時間制) を表示 できます。
  - Modifiers (修飾子):クリックすると、リストに表示された修飾子から選択して、テキストボックスに追加できます。たとえば、%aを選択すると曜日が表示されます。
  - **サイズ**:フォントサイズを選択します。
  - 表示:黒い背景に白いテキスト (デフォルト) など、背景色とテキストの色を選択します。



タイトル:ウィジェットのタイトルを入力します。 Overlay modifier (オーバーレイ修飾子):データソースとしてオーバーレイ修飾子 を選択します。MQTTオーバーレイを作成済みである場合、これらはリストの最後 に配置されます。 ●:画像内でオーバーレイの位置を選択したり、オーバーレイをクリック&ド ラッグしてライブビュー内で移動させたりできます。 サイズ:オーバーレイのサイズを選択します。 Visible on all channels (すべてのチャンネルで表示する):オフにすると、現在選 択しているチャンネルのみに表示されます。オンにすると、アクティブなチャン ネルすべてに表示されます。 Update interval (更新間隔):データの更新間隔を選択します。 Transparency (透明度):オーバーレイ全体の透明度を設定します。 Background transparency (背景の透明度):オーバーレイの背景のみの透明度を設 定します。 Points (ポイント):オンにすると、データ更新時にグラフラインにポイントが追加 されます。 Y軸 ラベル:Y軸のテキストラベルを入力します。 Dynamic scale (ダイナミックスケール):オンにすると、スケールがデータ 値に自動的に適応します。オフにして、固定スケールの値を手動で入力し ます。 Min alarm threshold (最小アラーム閾値) とMax alarm threshold (最大ア ラーム閾値):これらの値によって棒グラフに水平基準線が追加され、デー タ値が高すぎる場合や低すぎる場合に確認しやすくなります。

プライバシーマスク

 - .クリックすると、新しいプライバシーマスクを作成できます。

Privacy masks (プライバシーマスク):クリックすると、すべてのプライバシーマスクの色を変更したり、すべてのプライバシーマスクを永久に削除したりすることができます。

マスクx: クリックすると、マスクの名前変更、無効化、永久削除を行うことができます。

### 音声

デバイスの設定

**入力**:音声入力のオン/オフを切り替えます。入力のタイプを表示します。

<b>入力タイプ</b> :内蔵マイクやライン入力など、入力のタイプを選択します。
<b>電源タイプ</b>
変更を適用する :選択した内容を適用します。
Noise cancellation (ノイズキャンセル):オンに設定すると、バックグラウンドノイズを除去して音質が向上します。
エコーキャンセル:オンにすると、双方向通信時のエコーが除去されます。
<b>個別のゲインコントロール</b> :オンにすると、入力タイプごとに個別にゲインを調整することができます。
自動ゲインコントロール:オンにすると、サウンドの変化に合わせてゲインが動的に調整されます。
Gain (ゲイン):スライダーを使用してゲインを変更します。マイクのアイコンをクリックする と、ミュート、ミュート解除ができます。
ーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーー

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

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

ストリーム

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

エコーキャンセル:オンにすると、双方向通信時のエコーが除去されます。

## 音声クリップ

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

▷ <sub>音声クリップを再生します。</sub>

┛ 音声クリップの再生を停止します。

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

#### 録画

進行中の録画:装置で進行中のすべての録画を表示します。

- 装置で録画を開始します。
- └ 保存先のストレージ装置を選択します。
- 装置で録画を停止します。

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

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

▶ 録画を再生します。

┛ 録画の再生を停止します。

✓ ^ 録画に関する情報とオプションを表示または非表示にします。

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

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

Export (エクスポート):録画の全体または一部をエクスポートします。
テ クリックして録画にフィルターを適用します。
 From (開始):特定の時点以降に行われた録画を表示します。
 To (終了):特定の時点までに行われた録画を表示します。
 ソース③:ソースに基づいて録画を表示します。ソースはセンサーを指します。
 Event (イベント):イベントに基づいて録画を表示します。
 ストレージ:ストレージタイプに基づいて録画を表示します。

# アプリ



# 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。

デバイスの位置

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

- ・ Format (形式):デバイスの緯度と経度を入力するときに使用する形式を選択します。
- 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。

# 設定の確認

**インタラクティブな装置画像**:画像内のボタンをクリックして、実際のキー押下をシミュレート します。これにより、装置に物理的にアクセスしなくても、設定の試行やハードウェアのトラブ ルシューティングを行うことができます。

最新の認証情報 🕕: 最後に登録された認証情報に関する情報を表示します。

- (i) 最新の認証情報データを表示します。
- : (i) コンテキストメニューは以下を含みます。
- Reverse UID (UIDを反転させる): UIDのバイト順を反転させます。
- Revert UID (UIDを元に戻す): UIDのバイト順を元に戻します。
- Copy to clipboard (クリップボードにコピーする):UIDをコピーします。

Check credentials (認証情報の確認) (リ): UIDまたはPINを入力し、送信して認証情報を確認 します。システムは、装置で認証情報を使用した場合と同じように応答します。UIDとPINの両 方が必要な場合は、まず、UIDを入力します。

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。

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。

## 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<sup>®</sup>: 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<sup>®</sup>: 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]:デフォルトの設定です。インターネットを介してO3Cサービスに接続するには、装置のコントロールボタンを押し続けます。コントロールボタンを押してから24時間以内に装置をO3Cサービスに登録する必要があります。登録しない場合、デバイスはO3Cサービスから切断されます。装置を登録すると、[Always (常時)] が有効になり、装置はO3Cサービスに接続されたままになります。
- [常時]:装置は、インターネットを介してO3Cサービスへの接続を継続的に試行します。装置を登録すると、装置はO3Cサービスに接続したままになります。デバイスのコントロールボタンに手が届かない場合は、このオプションを使用します。
- [なし]:O3Cサービスを無効にします。

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

[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 _	<b>v2c (v1およびv2c)</b> : <b>Read community (読み取りコミュニティ)</b> :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。
	_	<b>Trap address (トラップアドレス)</b> :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。
	-	<b>Trap community (トラップコミュニティ)</b> :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。
		<ul> <li>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</li> <li>トラップメッセージを送信します。</li> </ul>
		- <b>認証失敗</b> :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。		
	<ul> <li>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。</li> </ul>	
	-	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

## 接続されたクライアント

あります。

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。

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** <sup>∨</sup>: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/en-us/axis-os#cryptographic-supportにアクセスしてください。
- Key type (キーのタイプ):ドロップダウンリストから、証明書の保護に使用する暗号化ア ルゴリズムとしてデフォルトかその他のいずれかを選択します。
- - コンテキストメニューは以下を含みます。
  - Certificate information (証明書情報):インストールされている証明書のプロパティを表示します。
  - Delete certificate (証明書の削除):証明書の削除。
  - ・ Create certificate signing request (証明書の署名要求を作成する):デジタルID証明書を 申請するために登録機関に送信する証明書署名要求を作成します。

## セキュアキーストア:

- 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に準拠した高セキュリティの暗号化。

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<sub>:クリックして、アクティブなルールを削除します。</sub>

【●: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。

SSHアカウント

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

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

Account (アカウント):固有のアカウント名を入力します。

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

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

**コメント**:コメントを入力します (オプション)。

: コンテキストメニューは以下を含みます。

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

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

Virtual host (仮想ホスト)

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

Enabled (有効):この仮想ホストを使用するには、選択します。

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

**ポート**:サーバーが接続されているポートを入力します。

タイプ:使用する認証のタイプを選択します。[Basic (ベーシック)]、[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。

## OpenID設定

重要

OpenIDを使用してサインインできない場合は、OpenIDを設定したときに使用したダイジェス トまたはベーシック認証情報を使用してサインインします。 Client ID (クライアントID): OpenIDユーザー名を入力します。

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

Admin claim (管理者請求):管理者権限の値を入力します。

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

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

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

Viewer claim (閲覧者請求):閲覧者権限の値を入力します。

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

Scopes (スコープ):トークンの一部となるオプションのスコープです。

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

Save (保存):クリックして、OpenIDの値を保存します。

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

# イベント

ルール

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

注

最大256のアクションルールを作成できます。

┿ **ルールを追加**:ルールを作成します。

名前:アクションルールの名前を入力します。

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

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

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

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

「 条件を追加:新たに条件を追加する場合にクリックします。

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

#### 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。



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 (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: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。

MQTTオーバーレイ

注

MQTTオーバーレイ修飾子を追加する前に、MQTTブローカーに接続します。

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

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

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

Modifier (修飾子):オーバーレイを作成するときに、生成された修飾子を使用します。 ・ #XMPで始まる修飾子は、トピックから受信したすべてのデータを示します。

- ・ #XMPで始まる修師士は、トヒックから受信したりへてのナーダを示します。
- ・ #XMDで始まる修飾子は、データフィールドで指定されたデータを示します。

ストレージ

ネットワークストレージ

使用しない:オンにすると、ネットワークストレージは使用されません。

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

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

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

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

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

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

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

ツール

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

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

オンボードストレージ

#### 重要

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

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

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

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

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

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

ツール

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

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

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

# ストリームプロファイル

ストリームプロファイルは、ビデオストリームに影響する設定のグループです。ストリームプロ ファイルは、たとえばイベントを作成するときや、ルールを使って録画するときなど、さまざま な場面で使うことができます。



## 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。

## ONVIFメディアプロファイル

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

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

**プロファイル名**:メディアプロファイルに名前を付けます。

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

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

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

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

注

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

**音声ソース**():設定に使用する音声入力ソースを選択します。

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

**音声エンコーダ**():設定に使用する音声エンコード方式を選択します。

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

**音声デコーダ**():設定に使用する音声デコード方式を選択します。

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

**音声出力** :設定に使用する音声出力形式を選択します。

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

Metadata (メタデータ):設定に含めるメタデータを選択します。

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

**PTZ**<sup>()</sup>:設定に使用するPTZ設定を選択します。

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

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

Cancel (キャンセル):クリックして、設定をキャンセルし、すべての設定をクリアします。 profile\_x:プロファイル名をクリックして、既定のプロファイルを開き、編集します。

#### 検知器

#### カメラに対するいたずら

カメラに対するいたずら検知器は、レンズが覆われたり、スプレーをかけられたり、ひどいピン ボケになったりしてシーンが変わり、[Trigger delay (トリガー遅延)] に設定された時間が経過し たときにアラームが発生します。いたずら検知器は、カメラが10秒以上動かなかった場合にのみ 作動します。この間に、映像からいたずらを比較検知するためのシーンモデルが検知器によって 設定されます。シーンモデルを正しく設定するには、カメラのピントを合わせ、適切な照明状態 にして、輪廓が乏しい情景 (殺風景な壁など) にカメラが向かないようにする必要があります。 「カメラに対するいたずら」は、アクションを作動させる条件として使用できます。

Trigger delay (トリガー遅延):「いたずら」条件が有効になってからアラームがトリガーされる までの最小時間を入力します。これにより、映像に影響する既知の条件に関する誤ったアラーム が発せられるのを防ぐことができます。

Trigger on dark images (暗い画像でトリガー):レンズにスプレーが吹き付けられた場合にア ラームを生成するのは困難です。照明の条件の変化などによって同じように映像が暗くなる場合 と区別できないからです。映像が暗くなるすべての場合にアラームが発生させるには、このパラ メーターをオンにします。オフにした場合は、画像が暗くなってもアラームが発生しません。

注

動きのないシーンや混雑していないシーンでのいたずら検知用。

#### 音声検知

これらの設定は、音声入力ごとに利用できます。

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

#### 衝撃検知

**衝撃検知機能**:オンにすると、装置が物が当たったり、いたずらされたときにアラームが生成されます。

**感度レベル**:スライダーを動かして、装置がアラームを生成する感度レベルを調整します。値を 低くすると、衝撃が強力な場合にのみ、装置がアラームを生成します。値を大きな値に設定する と、軽いいたずらでもアラームが生成されます。

アクセサリー

1/0ポート

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

デジタル出力を使用して、リレーやLEDなどの外部デバイスを接続します。接続された装置は、 VAPIX®アプリケーションプログラミングインターフェースまたはwebインターフェースから有効 化できます。

## ポート

**名前**:テキストを編集して、ポートの名前を変更します。

Usage (用途):リレーポートのデフォルトオプションは [Door (ドア)] です。インジケーターアイ

コンがある装置の場合、状態が変化してドアのロックが解除されると、 <sup>[]</sup> が緑色に点灯しま す。リレーをドア以外のものに使用し、状態が変化してもアイコンが点灯しないようにする場合 は、ポートに他のオプションのいずれかを選択できます。

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

標準の状態:開回路には を、 閉回路には を をクリックします。

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

#### 注

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

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

# Voice over IP (VoIP)

Voice over IP (VoIP) は、インターネットなどのIPネットワーク上の音声通信とマルチメディアセッションを可能にするテクノロジー群です。従来の電話呼び出しでは、アナログ信号は公衆交換電話網 (PSTN) 経由のサーキット伝送を通じて送信されます。VoIP呼び出しでは、アナログ信号がデジタル信号に変換され、ローカルIPネットワークまたはインターネットを経由してデータパケットで信号を送信することができます。

本製品では、セッション開始プロトコル (SIP) およびDTMF (デュアルトーン多重周波数) 信号伝達 によってVoIPが有効になっています。

例:



Axisインターカムで呼び出しボタンを押すと、1つ以上の既定の送信先への呼び出しが開始されます。送信先が応答すると、呼び出しが確立されます。VoIPテクノロジーで音声と映像が転送されます。

## セッション開始プロトコル (SIP)

セッション開始プロトコル (SIP) を使用して、VoIP呼び出しを設定、維持、および終了します。2つ 以上のグループ (SIPユーザーエージェント) の間で呼び出しを行うことができます。SIP呼び出し は、SIP電話、ソフトフォン、SIP対応Axisデバイスなどを使用して行うことができます。

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

ピアツーピア設定を使用するか、PBXを使用したネットワークを通じて、ローカルネットワークで 呼び出しを行うことができます。

## ピアツーピアSIP (P2PSIP)

最も基本的なタイプのSIP通信は、2つ以上のSIPユーザーエージェントの間で直接行われます。これは、ピアツーピアSIP (P2PSIP) と呼ばれます。ローカルネットワーク上で行われる場合、必要なのはユーザーエージェントのSIPアドレスだけです。この場合、通常のSIPアドレスはsip:

例:



ユーザーエージェントA - インターカム。SIPアドレス: sip:192.168.1.101 1 2 ユーザーエージェントB-SIPが有効な電話。SIPアドレス: sip:192.168.1.100

ピアツーピアSIP設定を使用して、同じネットワーク上でSIP対応電話などを呼び出すように、Axis インターカムを設定することができます。

#### 構内交換機 (PBX)

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

PBX SIPサーバーは、ローカルエンティティまたはオフサイトとして設定することができます。イ ントラネットまたはサードパーティのプロバイダーによってホストすることができます。ネット ワーク間でSIP呼び出しを行うと、呼び出しは一連のPBXによって到達先のSIPアドレスの場所を照 会し、ルーティングされます。

各SIPユーザーエージェントは、PBXに登録することで、正しい内線番号をダイヤすると該当の エージェントに到達できるようになります。この場合、通常のSIPアドレスはsip: <user>@<domain>またはsip:<user>@<registrar-ip>です。SIPアドレスはそのIPアドレス とは無関係であり、PBXはデバイスがPBXに登録されている間は、そのデバイスをアクセス可能に します。



- 3 PBX sip.company.com
- 4 sip:office@company.com

Axisインターカムで呼び出しボタンを押すと、呼び出しが1つ以上のPBXを経由して、ローカルIP ネットワークまたはインターネット上のSIPアドレスに転送されます。
## イベントのルールを設定する

特定のイベントが発生したときにデバイスにアクションを実行させるように、ルールを作成する ことができます。ルールは条件とアクションで構成されます。条件を使用して、アクションをト リガーすることができます。たとえば、デバイスは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。

## NATトラバーサル

NAT (ネットワークアドレス変換) トラバーサルは、プライベートネットワーク (LAN) 上にあるAxis デバイスに、そのネットワークの外部からアクセスできるようにする場合に使用します。

注

ルーターが、NATトラバーサルとUPnP®に対応している必要があります。

NATトラバーサルプロトコルは個別に使用することも、ネットワーク環境に応じたさまざまな組み 合わせで使用することもできます。

- ICE ICE (双方向接続性確立) プロトコルを使用することで、ピアデバイス間の通信を成功させるために最も効率のよいパスを見つけやすくなります。STUNやTURNも有効にすると、さらにICEプロトコルで見つけやすくなります。
- STUN STUN (NATのためのセッショントラバーサルユーティリティ)は、Axisデバイスが NATまたはファイアウォールを経由して配置されているかどうかを特定し、経由している 場合に、リモートホストへの接続のために割り当てるマッピングされたパブリックIPアドレ スとポート番号を取得できるようにする、クライアント/サーバーネットワークプロトコル です。IPアドレスなどのSTUNサーバーアドレスを入力します。
- TURN TURN (NATに関するリレーを使用したトラバーサル)は、NATルーターまたはファイ アウォールを経由するデバイスが、TCPやUDPを介して他のホストから着信データを受信で きるようにするプロトコルです。TURNサーバーアドレスとログイン情報を入力します。

## アプリケーション

アプリケーションを使用することで、Axis装置をより活用できます。AXIS Camera Application Platform (ACAP) は、サードパーティによるAxis装置向けの分析アプリケーションやその他のアプ リケーションの開発を可能にするオープンプラットフォームです。アプリケーションとしては、 装置にプリインストール済み、無料でダウンロード可能、またはライセンス料が必要なものがあ ります。

Axisアプリケーションのユーザーマニュアルについては、help.axis.comを参照してください。

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。

### 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 ネット上にある	デバイス用のIPアドレスと、デバイスへのアクセスに使用するコン ピューターのIPアドレスが異なるサブネットにある場合は、IPアドレスを 設定することはできません。ネットワーク管理者に連絡して、適切なIP アドレスを取得してください。
IPアドレスが別のデ バイスで使用されて いる	デバイスをネットワークから切断します。pingコマンドを実行します (コ マンドウィンドウまたはDOSウィンドウで、pingコマンドとデバイスの IPアドレスを入力します)。
	• Reply from <ip address="">: bytes=32; time=10が表示さ</ip>

- Reply from <IP address>: bytes=32; time=10...か表示された場合は、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 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 レスが変更された A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、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。

#### 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 よって、ポート8883 が安全ではないと判 断されたため、ポー	場合に ポート HTTPS 能性た	こよっては、サーバー/ブローカーによってMQTT通信用に特定の 、が提供されていない可能性があります。この場合でも、HTTP/ ら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 があります。
下8883を使用する下 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

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

システムを設定する際には、さまざまな設定や条件がシステムのパフォーマンスにどのように影響するかを検討することが重要です。ある要因は必要な帯域幅の量(ビットレート)に影響し、他の要因はフレームレートに影響し、帯域幅とフレームレートの両方に影響する事柄もあります。 CPUの負荷が最大に達した場合も、フレームレートに影響を及ぼします。

最も重要な検討事項には次のようなものがあります。

• 画像解像度が高い、または圧縮レベルが低いと、画像のファイルサイズが増大し、結果的 に帯域幅に影響を及ぼします。

- 多数のMotion JPEGクライアントまたはユニキャストH.264/H.265/AV1クライアントによる アクセスは帯域幅に影響します。
- 様々なクライアントが様々な解像度や圧縮方式が異なるストリームを同時に閲覧すると、 フレームレートと帯域幅の両方に影響を及ぼします。 フレームレートを高く維持するために、できる限り同一ストリームを使用してください。 ストリームプロファイルを使用すると、ストリームの種類が同一であることを確認できます。
- 異なるコーデックのビデオストリームへの同時アクセスが発生すると、フレームレートと 帯域幅の両方に影響が及ぼされます。最適な性能が実現するように、同じコーデックのス トリームを使用してください。
- ・ イベント設定を多用すると、製品のCPU負荷に影響が生じ、その結果、フレームレートに 影響します。
- 特に、Motion JPEGのストリーミングでは、HTTPSを使用するとフレームレートが低くなる 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。
- パフォーマンスの低いクライアントコンピューターで閲覧するとパフォーマンスが低下し、フレームレートに影響します。
- 複数のAXIS Camera Application Platform (ACAP) アプリケーションを同時に実行すると、フレームレートと全般的なパフォーマンスに影響する場合があります。

## サポートに問い合わせる

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

### 機器の接続

PoE (12V) で電力を供給されるリレー



- リレーの状態を確認するには、[System > Accessories (システム > アクセサリー)] に移動 し、リレーポートを検索します。
- 2. [Normal state (通常)] に設定します。

## 別の電源で電力を供給されるリレー



- リレーの状態を確認するには、[System > Accessories (システム > アクセサリー)] に移動 し、リレーポートを検索します。
- 2. [Normal state (通常)] に設定します。
  - 🎝 でフェイルセキュアをロックします。
  - <sup>o</sup> でフェイルセーフをロックします。

## 無電圧リレー



- リレーの状態を確認するには、[System > Accessories (システム > アクセサリー)] に移動 し、リレーポートを検索します。
- 2. [Normal state (通常)] に設定します。
  - **)** でフェイルセキュアをロックします。
  - o<sup>o</sup> でフェイルセーフをロックします。

## インターカムからのPoEで電力を供給される12 Vフェールセキュアロック



- リレーの状態を確認するには、[System > Accessories (システム > アクセサリー)] に移動 し、リレーポートを検索します。
- 2. [Normal state (通常)] に設定します。
  - **)** でフェイルセキュアをロックします。
  - o<sup>o</sup> でフェイルセーフをロックします。

外部電源で電力を供給される12 Vフェールセキュアロック



- リレーの状態を確認するには、[System > Accessories (システム > アクセサリー)] に移動 し、リレーポートを検索します。
- 2. [Normal state (通常)] に設定します。

  - ^ でフェイルセーフをロックします。

仕様

# フロントパネルインジケーターとコントロール

製品を電源に接続すると、フロントパネルのインジケーターが数秒間点灯します。

## インジケーターアイコン

アイコン	説明
	発信が開始されると黄色に点灯します。
7	着信が開始されると黄色に点滅します。
	通話中は青色に点灯します。
[]	ドアが開いているときは緑色に点灯します。

### LEDインジケーター

ステータスLED	説明
緑	正常動作であれば緑色に点灯します。

### SDカードスロット

#### 注意

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

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。

■ 響 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。

## コネクター

### ネットワーク コネクター

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

## 音声コネクター

音声入出力用4ピンターミナルブロック。

機能	ピン	メモ
ライン入力	1	ライン入力 (モノラル)
GND	2	音声アース
ライン出力端子	3	ライン出力 (モノラル)
GND	4	音声アース

#### 1/0コネクター

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

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

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

## 

#### 1 2 3 4 5 6

機能	ピン	ХŦ	仕様
0 V DC (-)	1		0 V DC
12 V DC	2		最大電流 = 400 mA
設定可能 (入 力または出 力)	3–4	デジタル入力 – 動作させるにはピン1に接続 し、動作させない場合はフロート状態 (未接 続) のままにします。	0~30 V DC (最大)
		デジタル出力 – 動作時にはピン1に接続され、動作していないときはフロート状態 (未接続) となっています。リレーなど、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、ダイオードを負荷と並列に接続する必要があります。	0~30 V DC (最大)
コモン	5		最大電流/電圧 = 30 V外部 電源で700 mA
NO (Normally Open) / NC (Normally Closed)	6	リレー装置の接続用。リレーピンは電気的に 他の回路から絶縁されています。	最大電流/電圧 = 30 V外部 電源で700 mA

#### 安全情報

### 危険レベル

## ▲危険

回避しない場合、死亡または重傷につながる危険な状態を示します。

### ▲警告

回避しない場合、死亡または重傷につながるおそれのある危険な状態を示します。

### ▲注意

回避しない場合、軽傷または中程度の怪我につながるおそれのある危険な状態を示します。

注意

回避しない場合、器物の破損につながるおそれのある状態を示します。

## その他のメッセージレベル

重要

製品を正しく機能させるために不可欠な重要情報を示します。

注

製品を最大限に活用するために役立つ有用な情報を示します。

T10154915\_ja

2025-04 (M17.2)

© 2020 – 2025 Axis Communications AB