AXIS D4100-VE Mk II Network Strobe Siren

ユーザーマニュアル

目次

インストール....4
....4
使用に当たって....5
....5
ネットワーク上のデバイスを検索する....5
ブラウザーサポート....5
装置のwebインターフェースを開く....5
管理者アカウントを作成します。....5
安全なパスワード....5
デバイスを構成する....7
サイレンの設置後にメンテナンスモードをオフにする....7
メンテナンスモードをオンにする....7
プロファイルの設定....7
プロファイルのインポートまたはエクスポート....7
ダイレクトSIP (P2P) を設定する....7
サーバーを介してSIPを設定する (PBX)....8
イベントのルールを設定する....9
アクションをトリガーする....9
アラームがトリガーされたときにプロファイルを開始します....9
SIPを介したプロファイルの開始....10
SIP内線番号による複数のプロファイルの制御....10
優先度が異なる2つのプロファイルを実行する....11
カメラが動きを検知したときに仮想入力によりストロボサイレンをアクティブにする....11
カメラが動きを検知したときにHTTP POSTを使用してストロボサイレンをアクティブにする....13
カメラが動きを検知したときにMQTTを介してストロボサイレンを作動させる....14
webインターフェース....17
詳細情報....18
セッション開始プロトコル (SIP)....18
ピアツーピアSIP (P2PSIP)....18
構内交換機 (PBX)....18
NATトラバーサル....18
仕様....20
製品概要....20
....20
LEDインジケーター....20
ボタン....20
コントロールボタン....20
コネクター....21
ネットワークコネクター....21
I/Oコネクター....21
ライトパターン名....22
サウンドパターン名....22
装置を清掃する....24
トラブルシューティング....25
工場出荷時の設定にリセットします。....25
AXIS OSのオプション....25
AXIS OSの現在のバージョンを確認する....25
AXIS OSをアップグレードする....26
技術的な問題と解決策....26
....28
パフォーマンスに関する一般的な検討事項....28

サポートに問い合わせる....28
サイバーセキュリティ....29
脆弱性の管理....29
セキュリティ通知....29
安全な製品ライフサイクル管理....29

インストール



使用に当たって

⚠ 警告

光の点滅やちらつきは、光過敏性てんかんを持つ人の発作を引き起こすことがあります。

ネットワーク上のデバイスを検索する

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

ブラウザーサポート

以下のブラウザーでデバイスを使用できます。

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

✓:推奨

*:制限付きでサポート

装置のwebインターフェースを開く

1. ユーザー名とパスワードを入力します。装置に初めてアクセスする場合は、管理者アカウントを作成する必要があります。*管理者アカウントを作成します。, on page 5*を参照してください。

AXIS OS搭載デバイスのWebインターフェースにおけるすべての機能および設定の説明については、*AXIS OS Webインターフェースヘルプ*を参照してください。

管理者アカウントを作成します。

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. アカウントを入力します。
2. パスワードを入力します。*安全なパスワード, on page 5*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。

安全なパスワード

重要

ネットワーク経由でパスワードやその他の機密性の高い設定を行う際は、HTTPS (デフォルトで有効) を使用してください。HTTPSは、安全で暗号化されたネットワーク接続を可能にし、パスワードなどのセンシティブなデータを保護します。

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)。

デバイスを構成する

サイレンの設置後にメンテナンスモードをオフにする

⚠ 注意

設置者の難聴や明るい光に目がくらむのを防ぐには、装置の設置時にメンテナンスモードをオンにすることをお勧めします。

装置を初めて設置した場合、メンテナンスモードはデフォルトでオンになっています。装置がメンテナンスモードの場合、サイレンは鳴らず、ライトは白色のパルスライトパターンで光ります。

[Overview (オーバービュー)] > [Maintenance (メンテナンス)] に移動し、[Maintenance mode (メンテナンスモード)] をオフにします。

メンテナンスモードをオンにする

装置のサービスを実行するには、[Overview (オーバービュー)] > [Maintenance (メンテナンス)] に移動し、[Maintenance mode (メンテナンスモード)] をオンにします。通常のライトとサイレンのアクティビティは一時停止されます。

プロファイルの設定

プロファイルとは、設定された構成の集合を意味します。優先順位やパターンの異なる最大30のプロファイルを設定できます。

新しいプロファイルを設定するには、以下の手順に従います。

1. [Profiles (プロファイル)] に移動し、[+ Create (作成)] をクリックします。
2. Name (名前) とDescription (説明) を入力します。
3. プロファイルに必要な [Light (ライト)] と [Siren (サイレン)] の設定を選択します。
4. ライトとサイレンの [Priority (優先度)] を設定し、[Save (保存)] をクリックします。

プロファイルを編集するには、 ⋮ をクリックして [Edit (編集)] を選択します。

プロファイルのインポートまたはエクスポート

既定のプロファイルを使用する場合は、以下の方法でプロファイルをインポートできます。

1. [Profiles (プロファイル)] に移動し、[+ Import (インポート)] をクリックします。
2. 参照してファイルを見つけるか、インポートするファイルをドラッグアンドドロップします。
3. [Save (保存)] をクリックします。

1つ以上のプロファイルをコピーして他の装置に保存するには、以下の手順でプロファイルをエクスポートできます。

1. [profiles(プロファイル)] を選択します。
2. [エクスポート] をクリックします。
3. 参照して.jsonファイルを見つけます。

ダイレクトSIP (P2P) を設定する

同じIPネットワーク内の少数のユーザーエージェント間で通信が行われ、PBXサーバーが提供する追加機能が必要ない場合は、ピアツーピアを使用します。

設定オプションの詳細については、*SIP*を参照してください。

1. [System (システム)] > [SIP] > [SIP settings (SIP設定)] に移動し、[Enable SIP (SIPの有効化)] を選択します。
2. デバイスでの着信呼び出しの受信を許可するには、**[Allow incoming calls (着信呼び出しを許可)]** を選択します。
3. [Call handling (呼び出しの処理)] で、呼び出しのタイムアウトと継続時間を設定します。
4. [Ports (ポート)] で、ポート番号を入力します。
   - **SIP port (SIPポート)** - SIP通信に使用するネットワークポートです。このポートを経由する信号トラフィックは暗号化されません。デフォルトポート番号は5060です。必要に応じて異なるポート番号を入力します。
   - **TLS port (TLS ポート)** - 暗号化されたSIP通信に使用するネットワークポートです。このポートを経由する信号トラフィックは、Transport Layer Security (TLS) を使用して暗号化されます。デフォルトポート番号は5061です。必要に応じて異なるポート番号を入力します。
   - [RTP start port (RTP開始ポート)] - SIP呼び出しの最初のRTPメディアストリームで使用するポートを入力します。メディア転送のデフォルトの開始ポートは4000です。ファイアウォールによっては、特定のポート番号のRTPトラフィックをブロックする場合があります。ポート番号は1024～65535の間で指定する必要があります。
5. [NAT traversal (NATトラバーサル)] で、NATトラバーサル用に有効にするプロトコルを選択します。

注

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

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

サーバーを介してSIPを設定する (PBX)

ユーザーエージェントどうしがIPネットワーク内外で通信する場合は、PBXサーバーを使用します。PBXプロバイダーによっては、設定に機能が追加される場合があります。

設定オプションの詳細については、*SIP*を参照してください。

1. PBXプロバイダーから以下の情報を入手してください。

- ユーザーID
- ドメイン

- パスワード
- 認証ID
- 呼び出し側ID
- レジストラ
- RTP開始ポート

2. 新しいアカウントを追加するには、[System (システム)] > [SIP] > [SIP accounts (SIPアカウント)] に移動し、[+ Account (+ アカウント)] をクリックします。
3. PBXプロバイダーから受け取った詳細情報を入力します。
4. [Registered (登録済み)] を選択します。
5. Transport mode (伝送モード)を選択します。
6. [Save (保存)] をクリックします。
7. ピアツーピアの場合と同じ方法でSIPを設定します。詳細については、*SIP*を参照してください。

イベントのルールを設定する

詳細については、「*イベントのルールの使用開始*」を参照してください。

アクションをトリガーする

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

アラームがトリガーされたときにプロファイルを開始します

この例では、デジタル入力信号が変わったときにアラームをトリガーする方法について説明します。

ポートの方向入力を設定する手順:

1. [System (システム)]>[Accessories (アクセサリー)]>[I/O ports (I/Oポート)] に移動します。
2. [Port 1 (ポート1)]>[Normal state (通常状態)] に進み、[Circuit closed (閉回路)] をクリックします。

ルールの作成:

1. [System (システム)]>[Events (イベント)] に移動し、ルールを追加します。
2. ルールの名前を入力します。
3. 条件の一覧で、[I/O] > [Digital input is active (デジタル入力がアクティブ)] を選択します。
4. [Port 1 (ポート1)] を選択します:
5. アクションのリストで、[Run light and siren profile while the rule is active (ルールがアクティブである間は、ライトとサイレンのプロファイルを実行)] を選択します。
6. [profile you want to start (開始するプロファイル)] を選択します。

7. **[Save (保存)]** をクリックします。

SIPを介したプロファイルの開始

この例では、SIPを介してアラームをトリガーする方法について説明します。

SIPを有効にする:

1. [System (システム)] > [SIP] > [SIP settings (SIP設定)] に移動します。
2. [Enable SIP (SIPの有効化)] と [Allow incoming calls (着信呼び出しを許可)] を選択します。
3. **[Save (保存)]** をクリックします。

ルールの作成:

1. [System (システム)]>[Events (イベント)] に移動し、ルールを追加します。
2. ルールの名前を入力します。
3. 条件のリストで、[Call (呼び出し)]>[State (状態)] を選択します。
4. 状態のリストで、[Active (アクティブ)] を選択します。
5. アクションのリストで、[Run light and siren profile while the rule is active (ルールがアクティブである間は、ライトとサイレンのプロファイルを実行)] を選択します。
6. [profile you want to start (開始するプロファイル)] を選択します。
7. **[Save (保存)]** をクリックします。

SIP内線番号による複数のプロファイルの制御

SIPを有効にする:

1. [System (システム)] > [SIP] > [SIP settings (SIP設定)] に移動します。
2. [Enable SIP (SIPの有効化)] と [Allow incoming calls (着信呼び出しを許可)] を選択します。
3. **[Save (保存)]** をクリックします。

プロファイルを開始するルールを作成する:

1. [System (システム)]>[Events (イベント)] に移動し、ルールを追加します。
2. ルールの名前を入力します。
3. 条件のリストで、[Call (呼び出し)] > [State change (状態変更)] を選択します。
4. 理由のリストで、[Accepted by device (装置で受け入れ)] を選択します。
5. [Call direction (呼び出し方向)] で [Incoming (着信)] を選択します。
6. Local SIP URIに**<sipを入力してください:[Ext]@[IP address]>** [Ext]はプロファイルで使用する内線番号、[IP address]はデバイスのIPアドレスです。たとえば、**sip:1001@192.168.0.90**とします。
7. アクションのリストで、[Light and Siren (ライトとサイレン)] > [Run light and siren profile (ライトとサイレンのプロファイルを実行)] の順に選択します。
8. [profile you want to start (開始するプロファイル)] を選択します。
9. アクション [Start (開始)] を選択します。
10. **[Save (保存)]** をクリックします。

プロファイルを停止するルールを作成する:

1. [System (システム)]>[Events (イベント)] に移動し、ルールを追加します。
2. ルールの名前を入力します。

3. 条件のリストで、[Call (呼び出し)] > [State change (状態変更)] を選択します。
4. 理由のリストで、[Terminated (終了した)] を選択します。
5. [Call direction (呼び出し方向)] で [Incoming (着信)] を選択します。
6. [Local SIP URI] にsip:[Ext]@[IP address] と入力します。[Ext] はプロファイルに使用する内線番号で、[IP address] は装置のアドレスです。たとえば、sip:1001@192.168.0.90とします。
7. アクションのリストで、[Light and Siren (ライトとサイレン)] > [Run light and siren profile (ライトとサイレンのプロファイルを実行)] の順に選択します。
8. 停止するプロファイルを選択します。
9. アクション [Stop (停止)] を選択します。
10. [Save (保存)] をクリックします。

この手順を繰り返して、SIPで制御する各プロファイルの開始と停止のルールを作成します。

優先度が異なる2つのプロファイルを実行する

優先度が異なる2つのプロファイルを実行すると、優先度の数字が高い番号のプロファイルが優先度の数字が低い番号のプロファイルに割り込みます。

注

同じ優先度の2つのプロファイルを実行した場合、最新のプロファイルによって前のプロファイルがキャンセルされます。

この例では、デジタルI/Oポートによってトリガーされたときに、優先度4のプロファイルを優先度3のプロファイルよりも先に表示するように設定する方法について説明します。

プロファイルの作成:

1. 優先度3のプロファイルを作成します。
2. 優先度4の別のプロファイルを作成します。

ルールの作成:

1. [System (システム)]>[Events (イベント)] に移動し、ルールを追加します。
2. ルールの名前を入力します。
3. 条件の一覧で、[I/O] > [Digital input is active (デジタル入力がアクティブ)] を選択します。
4. [port (ポート)] を選択します。
5. アクションのリストで、[Run light and siren profile while the rule is active (ルールがアクティブである間は、ライトとサイレンのプロファイルを実行)] を選択します。
6. [the profile that has the highest priority number (優先度の数字が最も高いプロファイル)] を選択します。
7. [Save (保存)] をクリックします。
8. [Profiles (プロファイル)] に移動し、優先度の数字が最も低い番号のプロファイルを開始します。

カメラが動きを検知したときに仮想入力によりストロボサイレンをアクティブにする

この例では、ストロボサイレンにカメラを接続する方法と、カメラにインストールされているアプリケーションAXIS Motion Guardが動きを検知した場合にストロボサイレンのプロファイルをアクティブにする方法について説明します。

開始する前に:

- ストロボサイレンでオペレーター、または管理者権限を持つ新しいアカウントを作成します。
- ストロボサイレンにプロファイルを作成します。
- カメラでAXIS Motion Guardを設定し、"Camera profile" (カメラプロファイル) というプロファイルを作成します。

カメラで2人の送信先を作成する:

1. カメラの装置インターフェースで [System > Events > Recipients (システム > イベント > 送信先)] に移動し、送信先を追加します。
2. 以下の情報を入力します。
   - Name (名前):Activate virtual port (仮想ポートのアクティブ化)
   - Type (タイプ): HTTP
   - URL::://<IPaddress>/axis-cgi/virtualinput/activate.cgi
     <IPaddress>の部分をストロボサイレンのアドレスに置き換えます。
   - 新しく作成したストロボサイレンアカウントのアカウント名とパスワード。
3. [Test (テスト)] をクリックして、すべてのデータが有効であることを確認します。
4. [Save (保存)] をクリックします。
5. 次の情報を含む2番目の送信先を追加します。
   - Name (名前):仮想ポートの非アクティブ化
   - Type (タイプ): HTTP
   - URL:http://<IPaddress>/axis-cgi/virtualinput/deactivate.cgi
     <IPaddress>の部分をストロボサイレンのアドレスに置き換えます。
   - 新しく作成したストロボサイレンアカウントのアカウント名とパスワード。
6. [Test (テスト)] をクリックして、すべてのデータが有効であることを確認します。
7. [Save (保存)] をクリックします。

カメラに2つのルールを作成する:

1. [Rules (ルール)] に移動し、ルールを追加します。
2. 以下の情報を入力します。
   - Name (名前):仮想IO1のアクティブ化
   - Condition (条件): [Applications (アプリケーション)] > [Motion Guard: Camera profile (モーションガード: カメラプロファイル)]
   - Action (アクション): [Notifications (通知)] > [Send notification through HTTP (HTTPで通知を送信する)]
   - Recipient (送信先): Activate virtual port (想ポートのアクティブ化)
   - Query string suffix (クエリ文字列のサフィックス):schemaversion=1&port=1
3. [Save (保存)] をクリックします。
4. 次の情報を含む別のルールを追加します。
   - Name (名前):仮想IO1の非アクティブ化
   - Condition (条件): [Applications (アプリケーション)] > [Motion Guard: Camera profile (モーションガード: カメラプロファイル)]
   - [Invert this condition (この条件を逆にする)] を選択します。
   - Action (アクション): [Notifications (通知)] > [Send notification through HTTP (HTTPで通知を送信する)]
   - Recipient (送信先): Deactivate virtual port (仮想ポートの非アクティブ化)
   - Query string suffix (クエリ文字列のサフィックス):schemaversion=1&port=1

5. [Save (保存)] をクリックします。

ストロボサイレンにルールを作成する:

1. ストロボサイレンのwebインターフェースで、[System (システム)] > [Events (イベント)] に移動し、ルールを追加します。
2. 以下の情報を入力します。
   - Name (名前):仮想入力1のトリガー
   - Condition (条件): I/O > Virtual input (仮想入力)
   - ポート:1
   - Action (アクション: [Light and siren (ライトとサイレン)] > [Run light profile while the rule is active (ルールがアクティブである間は、ライトとサイレンのプロファイルを実行)]
   - Profile (プロファイル):新しく作成したプロファイルを選択します。
3. [Save (保存)] をクリックします。

カメラが動きを検知したときにHTTP POSTを使用してストロボサイレンをアクティブにする

この例では、ストロボサイレンにカメラを接続する方法と、カメラにインストールされているアプリケーションAXIS Motion Guardが動きを検知した場合にストロボサイレンのプロファイルをアクティブにする方法について説明します。

開始する前に:

- ストロボサイレンにオペレーター、または管理者のロールを持つ新しいユーザーを作成します。
- ストロボサイレンに、次のプロファイルを作成します。「ストロボサイレンプロファイル」。
- カメラでAXIS Motion Guardを設定し、"Camera profile" (カメラプロファイル) というプロファイルを作成します。
- バージョン10.8.0以降のファームウェアでAXIS Device Assistantを使用してください。

カメラで送信先を作成する手順:

1. カメラの装置インターフェースで [System > Events > Recipients (システム > イベント > 送信先)] に移動し、送信先を追加します。
2. 以下の情報を入力します。
   - Name (名前):ストロボサイレン
   - Type (タイプ): HTTP
   - URL: http://<IPaddress>/axis-cgi/siren_and_light.cgi <IPaddress>の部分をストロボサイレンのアドレスに置き換えます。
   - 新しく作成されたストロボサイレンのユーザーのユーザー名とパスワードです。
3. [Test (テスト)] をクリックして、すべてのデータが有効であることを確認します。
4. [Save (保存)] をクリックします。

カメラに2つのルールを作成する:

1. [Rules (ルール)] に移動し、ルールを追加します。
2. 以下の情報を入力します。
   - Name (名前):動きのある場合にストロボサイレンをアクティブにする
   - Condition (条件): [Applications (アプリケーション)] > [Motion Guard: Camera profile (モーションガード: カメラプロファイル)]

- Action (アクション): [Notifications (通知)] > [Send notification through HTTP (HTTPで通知を送信する)]
- 送信先：ストロボサイレン.
  この情報は、[Events > Recipients > Name (イベント > 送信先 > 名前)] で入力した情報と同じである必要があります。
- Method (方式): Post
- Body (本文):

```
{  "apiVersion": "1.0",  "method": "start",  "params": {
"profile" : "Strobe siren profile"  } }
```

ストロボサイレンのプロファイルを作成したときと同じ情報を [profile (プロファイル) : <>] に入力してください。この場合は:「ストロボサイレンプロファイル」。

3. [Save (保存)] をクリックします。
4. 次の情報を含む別のルールを追加します。
   - Name (名前):動きのある場合にストロボサイレンを非アクティブにする
   - Condition (条件): [Applications (アプリケーション)] > [Motion Guard: Camera profile (モーションガード: カメラプロファイル)]
   - [Invert this condition (この条件を逆にする)] を選択します。
   - Action (アクション): [Notifications (通知)] > [Send notification through HTTP (HTTPで通知を送信する)]
   - 送信先：ストロボサイレン
     この情報は、[Events > Recipients > Name (イベント > 送信先 > 名前)] で入力した情報と同じである必要があります。
   - Method (方式): Post
   - Body (本文):

```
{  "apiVersion": "1.0",  "method": "stop",  "params": {    "profile" : "Strobe siren
profile"  } }
```

ストロボサイレンのプロファイルを作成したときと同じ情報を [profile (プロファイル) : <>] に入力してください。この場合は:「ストロボサイレンプロファイル」。

5. [Save (保存)] をクリックします。

カメラが動きを検知したときにMQTTを介してストロボサイレンを作動させる

この例では、カメラとストロボサイレンをMQTTを介して接続し、カメラにインストールされているAXIS Motion Guardアプリケーションが動きを検知すると、ストロボサイレンのプロファイルを起動する方法について説明します。

開始する前に:

- ストロボサイレンにプロファイルを作成します。
- MQTTブローカーを設定し、ブローカーのIPアドレス、ユーザー名、パスワードを取得します。
- カメラで AXIS Motion Guardを設定します。

カメラでMQTTクライアントを設定する:

1. カメラの装置インターフェースで、[System > MQTT > MQTT client > Broker (システム > MQTT > MQTTクライアント > ブローカー)] にアクセスし、以下の情報を入力します。
   - [ホスト]:ブローカーIPアドレス
   - Client ID (クライアントID):例: カメラ1
   - Protocol (プロトコル):ブローカーが設定したプロトコル
   - Port (ポート):ブローカーが使用するポート番号

- ブローカーの Username (ユーザー名) と Password (パスワード)

2. [Save (保存)]をクリックし、[Connect (接続)]をクリックします。

MQTTパブリッシングのためにカメラで2つのルールを作成する:

1. [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。
2. 以下の情報を入力します。
   - Name (名前):動体を検知しました
   - Condition (条件): [Applications (アプリケーション)] > [Motion alarm (モーションアラーム)]
   - Action (アクション):[MQTT] > [Send MQTT publish message (MQTT公開メッセージを送信)]
   - Topic (トピック):動き
   - Payload (ペイロード):オン
   - QoS:0、1、または2
3. [Save (保存)] をクリックします。
4. 次の情報を含む別のルールを追加します。
   - Name (名前):動きなし
   - Condition (条件): [Applications (アプリケーション)] > [Motion alarm (モーションアラーム)]
     - [Invert this condition (この条件を逆にする)] を選択します。
   - Action (アクション):[MQTT] > [Send MQTT publish message (MQTT公開メッセージを送信)]
   - Topic (トピック):動き
   - Payload (ペイロード):オフ
   - QoS:0、1、または2
5. [Save (保存)] をクリックします。

ストロボサイレンで、MQTTクライアントを設定する:

1. ストロボサイレンの装置インターフェースで、[System > MQTT > MQTT client > Broker (システム > MQTT > MQTTクライアント > ブローカー)] に移動し、以下の情報を入力します。
   - [ホスト]:ブローカーIPアドレス
   - Client ID (クライアントID):サイレン1
   - Protocol (プロトコル):ブローカーが設定したプロトコル
   - Port (ポート):ブローカーが使用するポート番号
   - Username (ユーザー名) と Password (パスワード)
2. [Save (保存)]をクリックし、[Connect (接続)]をクリックします。
3. [MQTT subscriptions (MQTTサブスクリプション)] に移動し、サブスクリプションを追加します。
   以下の情報を入力します。
   - サブスクリプションフィルター:動き
   - サブスクリプションの種類:ステートフル
   - QoS:0、1、または2
4. [Save (保存)] をクリックします。

ストロボサイレンにMQTTサブスクリプションのルールを作成する:

1. [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。
2. 以下の情報を入力します。
   - Name (名前):動体を検知しました
   - Condition (条件):[MQTT] > [Stateful (ステートフル)]
   - Subscription filter (サブスクリプションフィルター): Motion (動き)
   - Payload (ペイロード):オン
   - Action (アクション: [Light and siren (ライトとサイレン)] > [Run light profile while the rule is active (ルールがアクティブである間は、ライトとサイレンのプロファイルを実行)]
   - Profile (プロファイル):アクティブにするプロファイルを選択します。
3. [Save (保存)] をクリックします。

webインターフェース

AXIS OS搭載デバイスのWebインターフェースで利用可能なすべての機能および設定については、*AXIS OS Webインターフェースヘルプ*を参照ください。

詳細情報

セッション開始プロトコル (SIP)

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

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

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

ピアツーピアSIP (P2PSIP)

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

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。この場合の通常のSIPアドレスは、`sip:<user>@<domain>`または`sip:<user>@<registrar-ip>`をなります。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。

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。

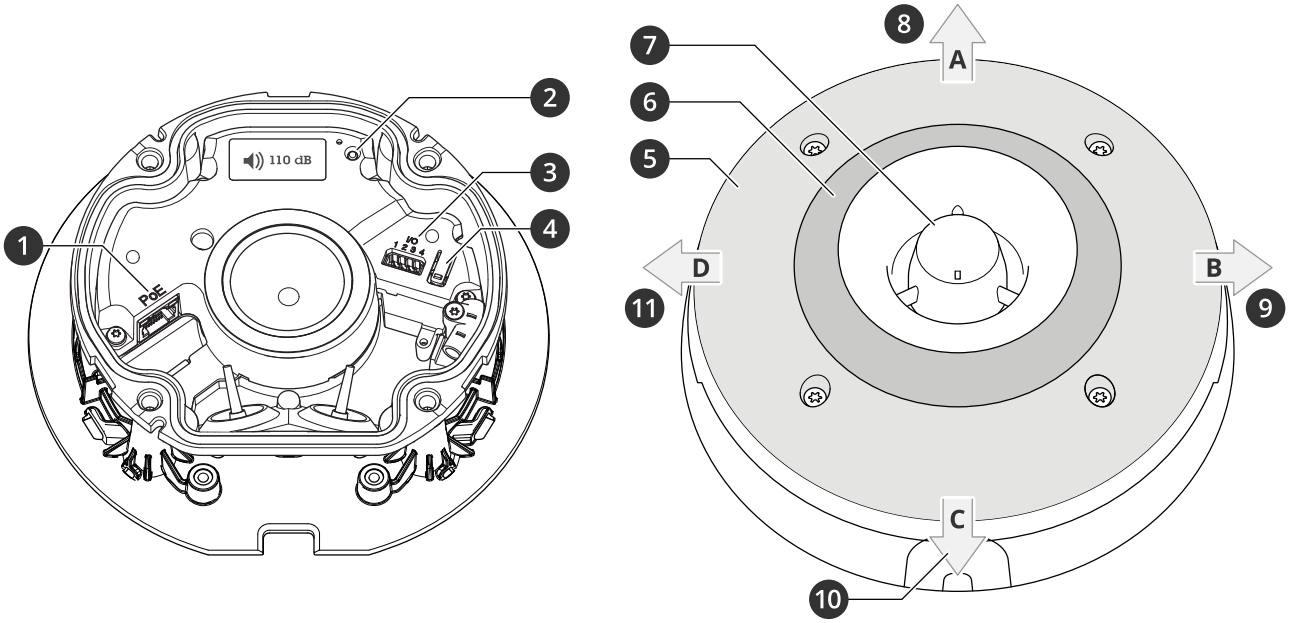
NATトラバーサルプロトコルは個別に使用することも、ネットワーク環境に応じたさまざまな組み合わせで使用することもできます。

- 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を介したリレーを使用するトラバーサル) は、NATルーターまたはファイアウォールの裏側でデバイスがTCPやUDP経由で他のホストから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。

仕様

製品概要



1 PoEネットワークコネクター
2 ステータスLEDインジケーター
3 I/Oコネクター
4 コントロールボタン
5 白色LED
6 (RGBA)赤、青、緑、オレンジLED
7 [Siren (サイレン)]:
8 ライトの向きA
9 ライトの向きB
10 ライトの向きC
11 ライトの向きD

LEDインジケーター

ステータスLED	説明
緑	起動後正常に動作する場合、10秒間、緑色に点灯します。
黄色	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。

ボタン

コントロールボタン

コントロールボタンは、以下の用途で使用します。

- 製品を工場出荷時の設定にリセットする。*工場出荷時の設定にリセットします。, on page 25*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

ネットワークコネクター

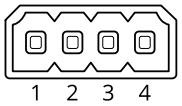
Power over Ethernet (PoE) 対応RJ45イーサネットコネクター

I/Oコネクター

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。

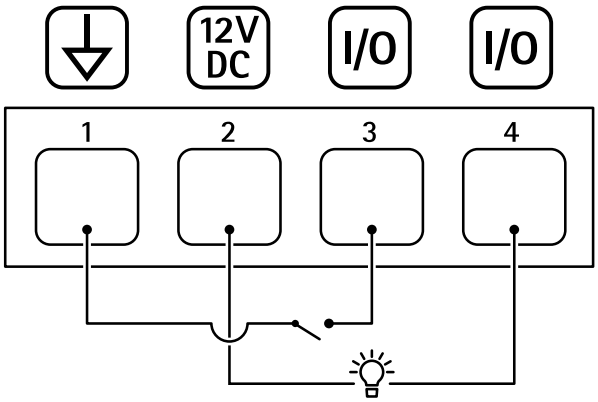
デジタル出力 - リレーやLEDなどの外部デバイス接続用。接続された装置は、VAPIX®アプリケーションプログラミングインターフェースを通じたイベントまたは本装置のwebインターフェースから有効にすることができます。

4ピンターミナルブロック



機能	ピン	メモ	仕様
DCアース	1		0 VDC
DC出力	2	⚠ 補助装置の電源供給に使用できます。 注:このピンは、電源出力としてのみ使用できます。	12VDC 最大負荷 = 50 mA
設定可能 (入力または出力)	3-4	デジタル入力 – 動作させるにはピン1に接続し、動作させない場合はフロート状態 (未接続) のままにします。	0～最大30 VDC
		デジタル出力 – アクティブ時はピン1 (DCアース) に内部で接続し、非アクティブ時はフロート状態 (未接続) になります。リレーなどの誘導負荷とともに使用する場合は、過渡電圧から保護するために、負荷と並列にダイオードを接続します。	0～30 VDC (最大)、オープンドレイン、100 mA

例:



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

ライトパターン名

オフ
点灯
一定 白 + 点滅色
代替
Pulse (パルス):
3つのステップでエスカレート
点滅
3回点滅
4回点滅
3回点滅して消える
4回点滅して消える
1回点滅
3回点滅
1回点滅 白 + 一定色
3回点滅 白 + 一定色
方向A + 一定色
方向B + 一定色
方向C + 一定色
方向D + 一定色
回転ホワイト1 + 一定色
回転テールホワイト + 一定色
ランダム 白 + 一定色
スピンホワイト + 一定色
一定 白 + 一定色

サウンドパターン名

オフ
アラーム:高音アラーム
アラーム:低音アラーム
アラーム:鳥
アラーム:汽笛
アラーム:カーアラーム
アラーム:車のアラーム 高速
アラーム:クラシック時計
アラーム:初回出席者

アラーム:ホラー
アラーム:工業
アラーム:単一ビープ音
アラーム:ソフトクアッドビープ音
アラーム:ソフトトリプルビープ音
アラーム:トリプルハイピッチ
通知:却下
通知:完了
通知:エントリ
通知:失敗しました
通知:急ぐ
通知:メッセージ
通知:次へ
通知:オープン
[Siren (サイレン)]:代替
[Siren (サイレン)]:弾む
[Siren (サイレン)]:救急
[Siren (サイレン)]:下降調
[Siren (サイレン)]:ホームソフト

装置を清掃する

装置はぬるま湯と低刺激、非研磨性の石鹸で洗浄できます。

注意

- 強力な化学薬品は装置を損傷する可能性があります。窓ガラス用洗剤やアセトンなどの化学薬品を使用して装置をクリーニングしないでください。
- シミの原因となるため、直射日光や高温下での清掃は避けてください。

1. 圧縮空気を使用すると、装置からほこりやごみを取り除くことができます。
2. 必要に応じて、ぬるま湯と低刺激、非研磨性の石鹸で湿らせた柔らかいマイクロファイバーの布で装置を清掃してください。
3. 残った洗浄剤を除去するには、ぬるま湯に浸した柔らかいマイクロファイバーの布で装置を拭いてください。
4. シミを防ぐために、きれいな非研磨性の布で装置から水分を拭き取ってください。

Axisデバイスの清掃に関する詳細については、ホワイトペーパー*「一般的な洗浄剤に対する耐薬品性」*をご覧ください。

トラブルシューティング

工場出荷時の設定にリセットします。

重要

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

本製品を工場出荷時の設定にリセットするには、以下の手順に従います。

1. 本製品の電源を切ります。
2. コントロールボタンを押した状態で電源を再接続します。*製品概要, on page 20*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。
4. コントロールボタンを放します。プロセスが完了すると、ステータスLEDが緑色に変わります。ネットワーク上にDHCPサーバーがない場合、装置IPアドレスは以下のいずれかにデフォルト設定されます。
   - **AXIS OS 12.0 以降を搭載したデバイス:** リンクローカルアドレスサブネット (169.254.0.0/16) から取得
   - **AXIS OS 11.11以前の装置：**192.168.0.90/24
5. インストールおよび管理ソフトウェアツールを使用して、IPアドレスの割り当て、パスワードの設定、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

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

注

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

技術的な問題と解決策

AXIS OSのアップグレード時の問題

AXIS OSアップグレード失敗

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

AXIS OSのアップグレード後の問題

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

IPアドレスの設定で問題が発生する

IPアドレスを設定できない

- デバイス用のIPアドレスと、デバイスへのアクセスに使用するコンピューターのIPアドレスが異なるサブネットにある場合は、IPアドレスを設定することはできません。ネットワーク管理者に連絡して、適切なIPアドレスを取得してください。
- そのIPアドレスは別のデバイスで使用されている可能性があります。以下の手順で確認してください。
  1. デバイスをネットワークから切断します。
  2. コマンドウィンドウまたはDOSウィンドウで、`ping`コマンドとデバイスのIPアドレスを入力します。
  3. 「`Reply from <IP address>: bytes=32; time=10...`」と表示された場合は、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。
  4. 「`Request timed out`」が表示された場合は、そのAXISデバイスにその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別のデバイスとIPアドレスの競合が発生している可能性があります。DHCPサーバーによって動的アドレスが設定される前は、Axisデバイスは静的IPアドレスを使用します。つまり、デフォルトの静的IPアドレスが別のデバイスでも使用されていると、デバイスへのアクセスに問題が発生する可能性があります。

デバイスへのアクセスの問題

ブラウザからデバイスにアクセスする際、ログインできない

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

rootアカウントのパスワードを忘れた場合は、デバイスを工場出荷時の設定にリセットする必要があります。手順については、*工場出荷時の設定にリセットします。, on page 25*を参照してください。

DHCPによってIPアドレスが変更された

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

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

IEEE 802.1X使用時の証明書エラー

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

ブラウザがサポートされていません

推奨ブラウザーのリストは、*ブラウザーサポート, on page 5*を参照してください。

外部からデバイスにアクセスできません

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

- AXIS Camera Station Edge:無料で使用でき、基本的な監視ニーズがある小規模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の問題

MQTTオーバSSLを使用してポート8883経由で接続できない

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

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

- サーバー/ブローカーが、通常はポート443経由で、WebSocket/WebSocket Secure (WS/WSS) をサポートしている場合は、代わりにこのプロトコルを使用してください。サーバー/ブローカープロバイダーに問い合わせて、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。

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

サウンドの問題	
装置の音が期待したほど大きくない	装置が正しく閉じられていること、ホーンやスピーカーエレメントに障害物がないことを確認します。
装置から音が出ない	装置が [Maintenance mode (メンテナンスモード)] になっているかどうかを確認します。メンテナンスモードの場合は、メンテナンスモードをオフにします。

ライトの問題	
装置の明るさが期待ほどではない	PoE Class 4電源が使用されていることを確認します。 装置の周囲温度を確認します。装置が高温環境に設置されている場合、ライトは自動的に暗くなります。

パフォーマンスに関する一般的な検討事項

考慮すべき最も重要な要因:

- 貧弱なインフラによるネットワークの使用率が高いと帯域幅に影響します。

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。

サイバーセキュリティ

サイバーセキュリティは、リスクを最小限に抑えながら、健全な製品ライフサイクルを支援します。当社のサイバーセキュリティへの取り組みに関する詳細な情報や資料は、*axis.com/about-axis/cybersecurity* でご覧いただけます。以下のサイバーセキュリティガイドラインに従ってAxisからの製品に関するセキュリティ通知を受け取り、製品の安全なライフサイクルおよび運用停止のための設定を行ってください。

*Axis Trust Center*では、Axisが実施するセキュリティコンプライアンス、透明性、データ保護、およびプライバシーについての情報をご覧いただけます。

脆弱性の管理

Axisは、*共通脆弱性識別子 (CVE) 採番機関 (CNA)*です。当社は、セキュリティリスクを最小限に抑えるため、当社のデバイス、ソフトウェア、およびサービスの脆弱性の特定と修正において業界標準に従って対応しています。当社の脆弱性管理ポリシーに関する詳細や、脆弱性の報告については、*axis.com/vulnerability-management*を参照してください。

セキュリティ通知

axis.com/security-notification-service から、Axisのセキュリティ通知電子メールを購読してください。お使いのAxis製品に関する脆弱性、関連するセキュリティアドバイザリ、およびその他のセキュリティ関連事項について情報をお送りします。

安全な製品ライフサイクル管理

Axisは、安全なライフサイクル管理を通じて、製品のライフサイクル全体でリスクを最小限に抑えています。*help.axis.com*に掲載されているハードニングガイドには、Axis製品のより安全な設定と操作に関する情報、および以下の情報が含まれています。

安全な初回使用 - Axis製品は、高度な保護機能がデフォルトで組み込まれているため、初回使用時から安全な初期化と暗号化された通信が可能です。

使用目的とよくある設定ミス - 当社のガイドには、Axis製品の使用目的について記載されています。これには、避けるべきよくあるセキュリティ関連の誤った使用や設定ミスについても含まれています。

脆弱性の管理とサプライチェーンの透明性 - 脆弱性の開示およびサプライチェーンの透明性向上を目的として、ソフトウェアのリリースごとに、*axis.com*でソフトウェア部品表 (SBOM) を公開しています。

利用停止とデータの安全な消去 - 製品のライフサイクル終了時に安全に利用を停止するために、工場出荷時の設定にリセットしてください。これにより、設定、保存されたデータ、およびセンシティブな情報が消去されます。

T10223803_ja

2026-10 (M7.2)

© 2025 – 2026 Axis Communications AB