AXIS I8307-VE Network Intercom

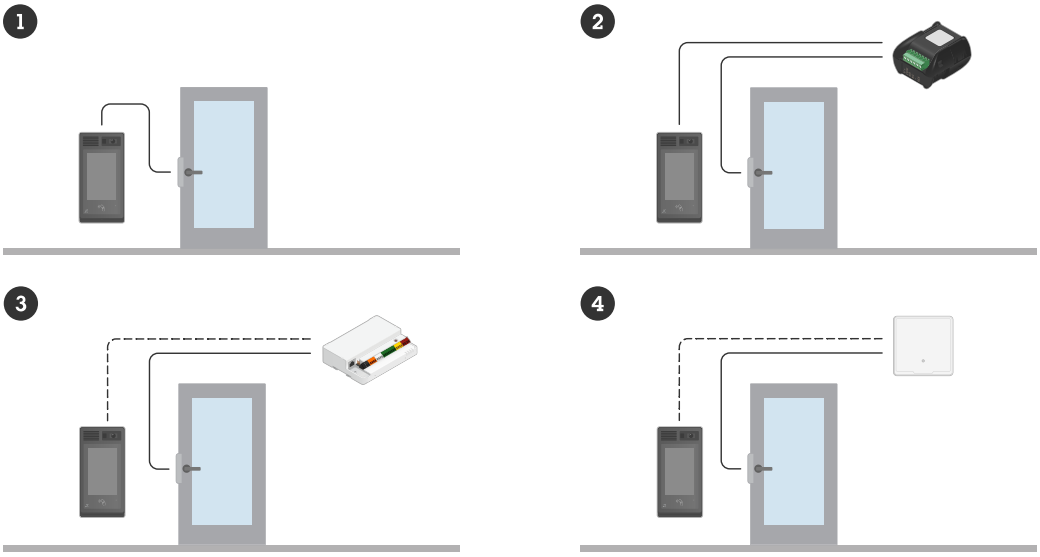
ユーザーマニュアル

目次

ソリューションの概要 4
インストール 5
　プレビューモード 5
使用に当たって 6
　ネットワーク上のデバイスを検索する 6
　　ブラウザーサポート 6
　装置のwebインターフェースを開く 6
　管理者アカウントを作成します。 6
　安全なパスワード 7
　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 7
デバイスを構成する 8
　リモートスピーカーテストのキャリブレーションを行い、テストを実行する 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 10
　ディスプレイに呼び出しボタンを追加する 10
　リーダーとして設定する 11
　　エントリーリストを使用して資格情報保持者がドアを開けられるようにします。 11
　　ドアコントローラーを使用してカードリーダーとして設定する 12
　カード上の保護されているデータを使用してセキュリティを向上させる 13
　DTMFを使用してディスプレイに地図を表示する 13
webインターフェース 15
詳細情報 16
　Voice over IP (VoIP) 16
　　セッション開始プロトコル (SIP) 16
　　ピアツーピアSIP (P2PSIP) 16
　　構内交換機 (PBX) 17
　　NATトラバーサル 18
　イベントのルールを設定する 18
　分析機能とアプリ 18
　　AXIS Client for Unified Communication Systems 18
仕様 19
　製品概要 19
　LEDインジケーター 20
　SDカードスロット 20
　ボタン 21
　　コントロールボタン 21
　コネクター 21
　　ネットワークコネクター 21
　　音声コネクター 21
　　リレーコネクタ 21
　　リーダーコネクター 22
　　I/Oコネクター 22
　　電源コネクター 23
機器の接続 25
　PoE (12V) 駆動リレー1個 25
　PoE (12V) 駆動リレー2個 25
　PoE (12V) 駆動リレー1個＋外部電源駆動リレー1個 26
　PoE (12V) 駆動リレー1個＋無電位接点リレー1個 26
　インターコムからのPoE+で電力を供給される12 Vフェールセキュアロック 27
　外部電源で電力を供給されるフェールセキュアロック 27
　PoE (24V) 駆動リレー1個＋無電位接点リレー1個 28
　OSDPを使用してドアコントローラーに接続されたリーダー 28

Wiegandを使用してドアコントローラーに接続されたリーダー 29
VAPIXリーダーを使用してAxisドアコントローラーに接続されたリーダー 29
トラブルシューティング 30
工場出荷時の設定へのリセット 30
AXIS OSのオプション 30
AXIS OSの現在のバージョンを確認する 30
AXIS OSをアップグレードする 31
技術的な問題と解決策 31
パフォーマンスに関する一般的な検討事項 33
サポートに問い合わせる 34
安全情報 35
危険レベル 35
その他のメッセージレベル 35
サイバーセキュリティ 36
脆弱性の管理 36
セキュリティ通知 36
安全な製品ライフサイクル管理 36

ソリューションの概要



1 インターコム
2 インターコムとAXIS A9801の組み合わせ
3 インターコムとAXIS A9210の組み合わせ
4 インターコムとアクセスコントロールシステムの組み合わせ

インストール



プレビューモード

プレビューモードは、設置担当者が設置中にカメラビューを微調整する際に最適です。プレビューモードでは、カメラビューにアクセスするのにログインする必要はありません。このモードは、装置の電源投入から一定時間、工場出荷時の設定状態でのみ使用できます。



このビデオでは、プレビューモードの使用方法について説明しています。

使用に当たって

ネットワーク上のデバイスを検索する

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

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

ブラウザーサポート

以下のブラウザーでデバイスを使用できます。

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

✓:推奨

*:制限付きでサポート

装置のwebインターフェースを開く

1. ブラウザーを開き、Axis装置のIPアドレスまたはホスト名を入力します。
   本製品のIPアドレスが不明な場合は、AXIS IPUtilityまたはAXIS DeviceManagerを使用して、ネットワーク上のデバイスを検索してください。
2. ユーザー名とパスワードを入力します。装置に初めてアクセスする場合は、管理者アカウントを作成する必要があります。*管理者アカウントを作成します。, on page 6*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 7*を参照してください。
3. パスワードを再入力します。
4. 使用許諾契約書に同意します。
5. [Add account (アカウントを追加)] をクリックします。

重要

装置にはデフォルトのアカウントはありません。管理者アカウントのパスワードを紛失した場合は、装置をリセットする必要があります。*工場出荷時の設定へのリセット, on page 30*を参照してください。

安全なパスワード

重要

ネットワーク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)。

デバイスのソフトウェアが改ざんされていないことを確認する

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

1. 工場出荷時の設定にリセットします。*工場出荷時の設定へのリセット, on page 30*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。

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。

リモートスピーカーテストのキャリブレーションを行い、テストを実行する

スピーカーテストを実行することで、スピーカーが意図したとおりに動作しているかどうかを遠隔で確認することができます。スピーカーテストでは、内蔵マイクロフォンによって登録されている一連のテストトーンを再生します。テストを実行するたびに、登録されている値が、キャリブレーション中に登録された値と比較されます。

注

テストは設置された場所の設置箇所からキャリブレーションする必要があります。壁の建設や取り外しなどによって、スピーカーの移動や地域環境の変化が発生した場合は、スピーカーのキャリブレーションをやり直す必要があります。

キャリブレーション中は、担当者がインストール拠点に実際に出向いてテストトーンを聞き、スピーカーの音響経路にある予期しない障害物によってテストトーンの音が小さくなったり、遮断されたりしていないことを確認することをお勧めします。

1. [device interface > **Audio > Speaker test** (デバイスインターフェース > 音声 > スピーカーテスト)] に移動します。
2. 音声デバイスのキャリブレーションを行うには、[**Calibrate (キャリブレーション)**] をクリックします。

注

Axis製品のキャリブレーションが終了すると、いつでもスピーカーテストを実行できます:

3. スピーカーテストを実行するには、[**Test (テスト)**] をクリックします。

注

また、物理デバイスのコントロールボタンを押してキャリブレーションを実行することもできます。コントロールボタンを特定するには、*製品概要, on page 19*を参照してください。

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、*Voice over IP (VoIP), on page 16*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、*セッション開始プロトコル (SIP), on page 16*を参照してください。

SIPの設定には2種類あります。ダイレクトまたはピアツーピア (P2P) のいずれかです。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、*ピアツーピアSIP (P2PSIP), on page 16*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。
4. [**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。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することができます。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、*NATトラバーサル, on page 18*を参照してください。

10. [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)

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、*Voice over IP (VoIP), on page 16*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、*セッション開始プロトコル (SIP), on page 16*を参照してください。

SIPの設定には2種類あります。1つはPBXサーバーです。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、*構内交換機 (PBX), on page 17*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. [Save (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、*ダイレクトSIP (P2P) を設定する, on page 8*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、*セッション開始プロトコル (SIP), on page 16*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. [Save (保存)] をクリックします。

ディスプレイに呼び出しボタンを追加する

この例では、訪問者が受付を呼び出すために押すボタンをディスプレイに表示するように設定する方法を説明します。

開始する前に

- 受付の連絡先を作成します。手順については、*連絡先の作成, on page 10*を参照してください。

1. [Display (ディスプレイ)] > [Pages (ページ)] に移動します。
2. [Default Homepage (デフォルトホームページ)] で、 ⋮ をクリックし、[Edit (編集)] を選択します。
3. [+ Add (追加)] をクリックします。
4. [Type (タイプ)] のリストから [Button (ボタン)] を選択します。
5. 連絡先のリストから受付を選択します。
6. ボタンのサイズを選択します。
7. [Save (保存)] をクリックしてボタンを保存します。
8. [Save (保存)] をクリックしてデフォルトホームページを保存します。

リーダーとして設定する

インターコムをリーダーとして設定し、資格情報保持者がドアを開けられるようにできます。

エントリーリストを使用すると、インターコムが認証情報をローカルに保存し、最大50名までの資格情報保持者に対してスタンドアロンのリーダーとして機能させることができます。

インターコムをドアコントローラーに接続している場合でも、インターコムは最大50件の認証情報を保存でき、要求された認証情報がエントリーリストにある場合は、インターコムがアクセス権限を管理します。要求された認証情報がエントリーリストに見つからず、**接続されたドアコントローラーを使用**オプションが有効になっている場合、要求はドアコントローラーに転送され、ドアコントローラーがアクセス権限を管理します。

エントリーリストを使用して資格情報保持者がドアを開けられるようにします。

エントリーリストを使用すると、認証情報保持者が認証情報を使用してドアを開くなどのアクションをトリガーできるように設定できます。この例では、カードを使用してドアを10回開くことができる認証情報所持者を追加する方法について説明します。

前提条件

- **[Reader (リーダー)] > [Chip types (チップタイプ)]** で正しいチップタイプがアクティブになっていることを確認します。

エントリーリストをオンにし、認証情報保持者を追加します。

1. **[Reader (リーダー)] > [Entry list (エントリーリスト)]** に移動します。
2. [Use Entry list (エントリーリストを使用)] をオンにします。
3. [+ Add credential holder (認証情報保持者を追加)] をクリックします。
4. 認証情報保持者の姓名を入力します。この名前は一意である必要があります。
5. [Card (カード)] を選択します。
6. 認証情報保持者のカードを装置でスワイプし、[Get latest (最新データを取得)] をクリックします。
7. イベント条件を [Access granted (アクセス許可)] のままにします。
8. [Valid to (有効期限)] で、[Number of times (回数)] を選択します。
9. [Number of times (回数)] に「10」と入力します。
10. **[Save (保存)]** をクリックします。

ルールの作成:

1. [System > Events (システム > イベント)] に移動します。
2. [Rules (ルール)] で、[+ Add a rule (ルールを追加)] をクリックします。
3. **[Name (名前)]** に、「Open door (ドアを開ける)」と入力します。
4. 条件のリストで、**[Entry list (エントリーリスト)] > [Access granted (アクセス許可)]** を選択します。
5. アクションのリストから、**[I/O] > [Toggle I/O once (I/Oを1回切り替え)]** を選択します。
6. ポートのリストで、[Door (ドア)] を選択します。
7. **[State (状態)]** で **[Active (アクティブ)]** を選択します。
8. 継続時間を00:00:07に設定します。
9. **[Save (保存)]** をクリックします。

ドアコントローラーを使用してカードリーダーとして設定する

ネットワーク接続

インターコムをカードリーダーとして使用するには、ドアステーションをドアコントローラーに接続することができます。ドアコントローラーは、すべての認証情報を保存し、誰がドアを通過できるかを追跡します。この例では、ネットワークを介してデバイスを接続します。また、許可されているカードの種類も変更します。

重要

ネットワーク接続はAxisドアコントローラーでのみ可能です。Axis以外のドアコントローラーに接続するには、デバイスをケーブルで物理的に接続する必要があります。*有線接続, on page 12* を参照してください。

インターコムをカードリーダーとして設定する

1. **[Reader (リーダー) > [Connection (接続)]** に移動します。
2. [**VAPIX reader (VAPIXリーダー)**] プロトコルタイプを選択します。
3. ドアコントローラーとの通信に使用するプロトコルを選択します。

注

[HTTPS] を使用している場合は、[**Verify certificate (証明書を検証する)**] をオンにすることをお勧めします。

4. ドアコントローラーのIPアドレスを入力します。
5. ドアコントローラーの認証情報を入力します。
6. **[Connect (接続)]** をクリックします。
7. 該当するドア用の入口リーダーを選択します。
8. **[Save (保存)]** をクリックします。

有線接続

ドアステーションをカードリーダーとして使用するには、ドアステーションをドアコントローラーに接続することができます。ドアコントローラーは、すべての認証情報を保存し、誰がドアを通過できるかを追跡します。この例では、装置はケーブルで接続し、Wiegandプロトコルを使用しています。また、beeperは有効で、LED用にI/Oポートを1つ使用します。また、許可されているカードの種類も変更します。

重要

未使用のI/Oポートを使用します。すでに使用されているI/Oポートを使用した場合、それらのポート用に作成されたイベントは動作しなくなります。

開始する前に

- インターコムをドアコントローラーに接続します。
  *機器の接続, on page 25*の電気配線図を参照してください。
- ドアコントローラーのハードウェアを、リーダー用のWiegandプロトコルを使用して設定します。手順については、ドアコントローラーのユーザーズマニュアルを参照してください。

インターコムをカードリーダーとして設定する

1. **[Reader (リーダー) > [Connection (接続)]** に移動します。
2. プロトコルタイプとして [**Wiegand (ウィジェット)**] を選択します。
3. [**Beeper (ビーパー)**] をオンにします。
4. [**Input for beeper (ビーパーの入力)**] で、[I3] を選択します。
5. [**Input used for LED control (LEDコントロールで使用する入力)**] で、[1] を選択します。
6. [**Input for LED1 (LED1の入力)**] で、[I1] を選択します。
7. 各状態に使用する色を選択します。

8. [Keypress format (キー操作の形式)] で、[FourBit] を選択します。
9. [Save (保存)] をクリックします。
10. [Reader > Chip types (リーダー > チップタイプ)] に移動し、使用するチップタイプをアクティブにします。

注

デフォルトのチップタイプのセットは保持できますが、特定のニーズに応じてリストを変更することをお勧めします。

11. [Add data set (データセットを追加)] をクリックして、さまざまなチップタイプのデータセットを指定します。
12. [Save (保存)] をクリックします。

カード上の保護されているデータを使用してセキュリティを向上させる

アクセスコントロールシステムのセキュリティを向上させるために、一部の種類のカードに保存されている安全なカードデータを使用することができます。データは秘密鍵によって保護されています。カードデータを読み取るには、秘密鍵とカードに関するその他の情報をデバイスに保存する必要があります。

1. [Reader > Chip types (リーダー > チップタイプ)] に移動します。
2. [Data sets (データセット)] で、編集するチップタイプを選択し、[Add data set (データセットを追加)] をクリックします。
3. カードデータに関する情報を入力します。入力する情報は、カードタイプとカードを登録した方法によって異なります。
4. OSDPまたはWiegandプロトコルを使用する場合は、[Use as UID (UIDとして使用する)] を選択して、通常のカードUID/CSNではなくUID/CSNとして安全なデータを送信します。
5. 指定したカードデータに準拠したカードのみをアクセスコントローラーに送信するには、[Required data (必須データ)] を選択します。準拠しないカードはリーダーに無視されます。
6. [Save (保存)] をクリックします。

DTMFを使用してディスプレイに地図を表示する

訪問者がインターコムから呼び出しを行い、案内が必要な場合、応答者はDTMF (Dual-Tone Multi-Frequency) 信号を使用してインターコムのディスプレイに地図を表示することができます。

この例では、次の方法について説明します。

- インターコムに地図画像をアップロードする。
- インターコムで地図画像を含むページを作成する。
- インターコムのDTMFシーケンスを定義する。
- DTMFシーケンスへの応答として、インターコムが地図ページを30秒間表示するように設定する。

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。手順については、*ダイレクトSIP (P2P) を設定する, on page 8*および *サーバーを介してSIPを設定する (PBX), on page 9* を参照してください。

地図画像のアップロード

1. [Media (メディア)] に移動します。
2. [+ Add (追加)] をクリックします。
3. 建物の地図を示す画像をドラッグアンドドロップします。推奨画像解像度は480x800ピクセル、最大解像度は2048x2048ピクセルです。

4. **[Save (保存)]** をクリックします。

ディスプレイの新規地図ページを作成します。

5. **[Display (ディスプレイ)] > [Pages (ページ)]** に移動します。
6. **[+ Add (追加)]** をクリックします。
7. ページの名前 (たとえば「Map page」) を入力します。
8. **[+ Add (追加)]** をクリックします。
9. タイプのリストから **[Image (画像)]** を選択します。
10. 画像の名前 (たとえば「Map image」) を入力します。
11. 画像のリストから地図画像を選択します。
12. **[Save (保存)]** をクリックします。
13. **[Save (保存)]** をもう一度クリックします。

DTMFシーケンスの定義

14. **[Communication (通信)] > [SIP] > [DTMF]** に移動します。
15. [**+ Add sequence (シーケンスを追加)**] をクリックします。
16. **[Sequence (シーケンス)]** に「9」と入力します。
17. **[Description (説明)]** に「Show map」と入力します。
18. アカウントを選択します。
19. **[Save (保存)]** をクリックします。

ルールの作成

20. [**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。
21. ルールの名前 (たとえば「Use DTMF to show map」) を入力します。
22. 条件のリストで、**[Call (呼び出し)] > [DTMF]** を選択します。
23. DTMFイベントIDのリストで、**[Show map (地図を表示)]** を選択します。
24. アクションのリストで、**[Display (ディスプレイ)] > [Show page (ページを表示)]** を選択します。
25. ページのリストで、**[Map page (地図ページ)]** を選択します。
26. 30秒間地図を表示する場合は、**[Duration (時間)]** に00:00:30と入力します。
27. **[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。

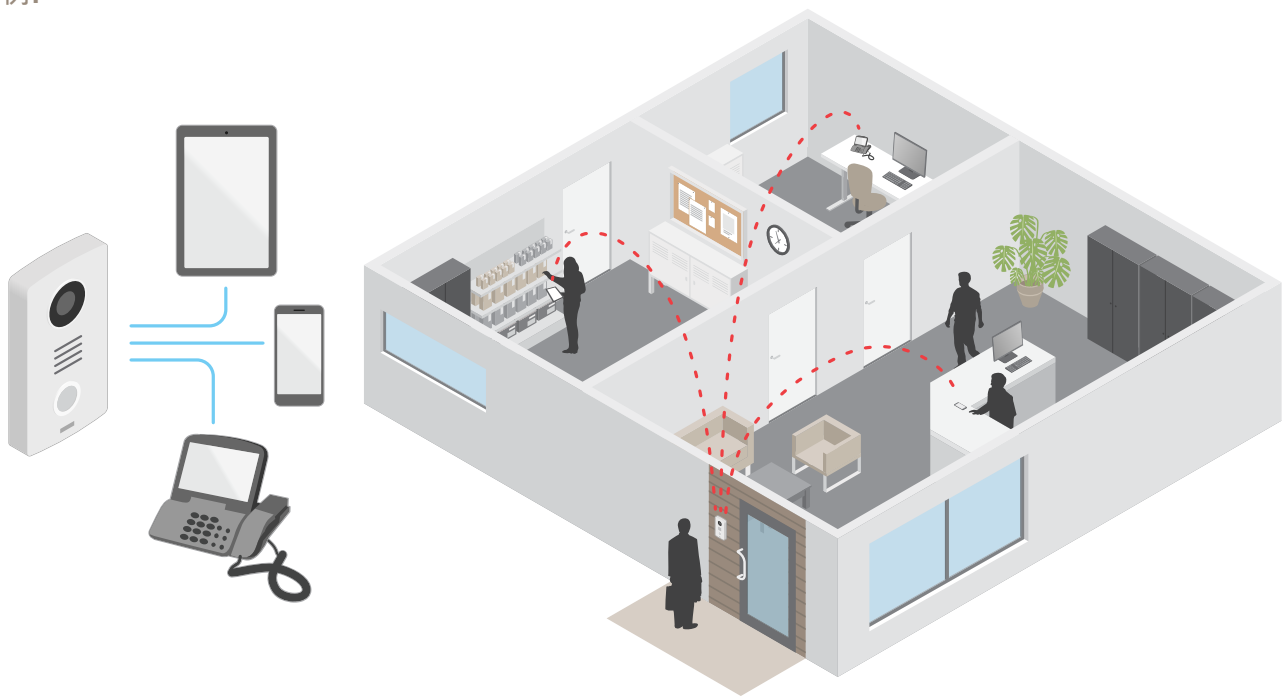
詳細情報

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。

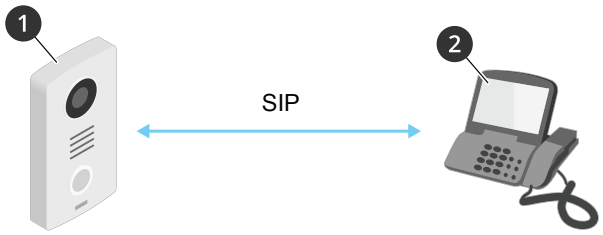
実際の音声またはビデオは、RTP (Real-time Transport Protocol) などのトランスポートプロトコルを使用して、SIPユーザーエージェントの間で交換されます。

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:<local-ip>`になります。

例:



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

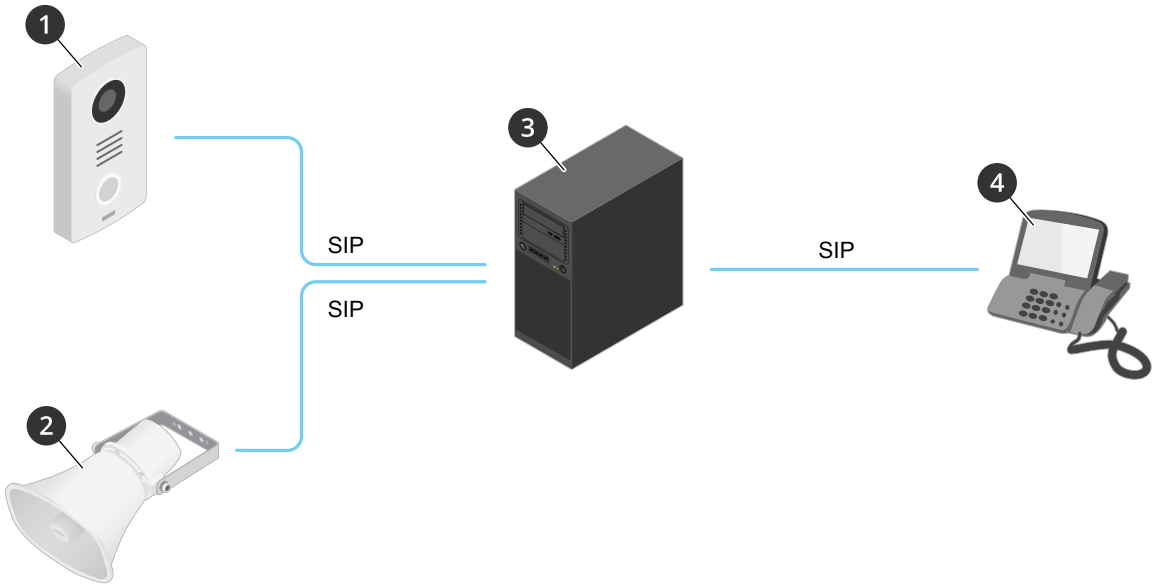
構内交換機 (PBX)

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>`になります。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。

例:



1 sip:mydoor@company.com
2 sip:myspeaker@company.com
*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。

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の裏側にあるデバイスが、TCPやUDPを介して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。

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、「*イベントのルールの使用開始*」を参照してください。

分析機能とアプリ

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

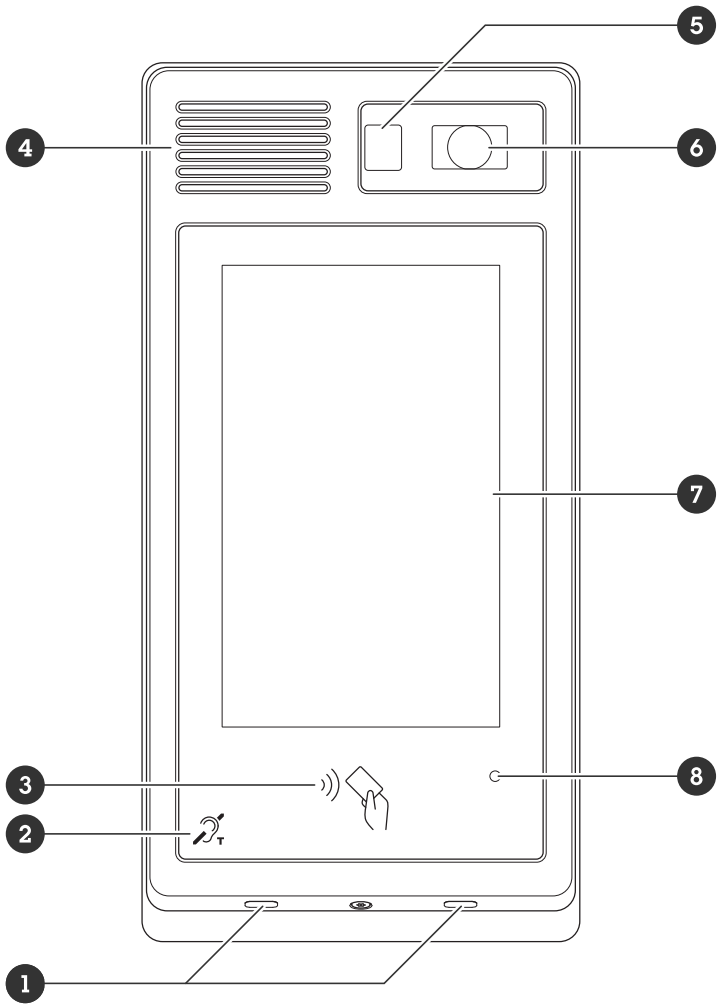
Axisの分析機能とアプリのユーザーマニュアルは、*help.axis.com*から参照できます。

AXIS Client for Unified Communication Systems

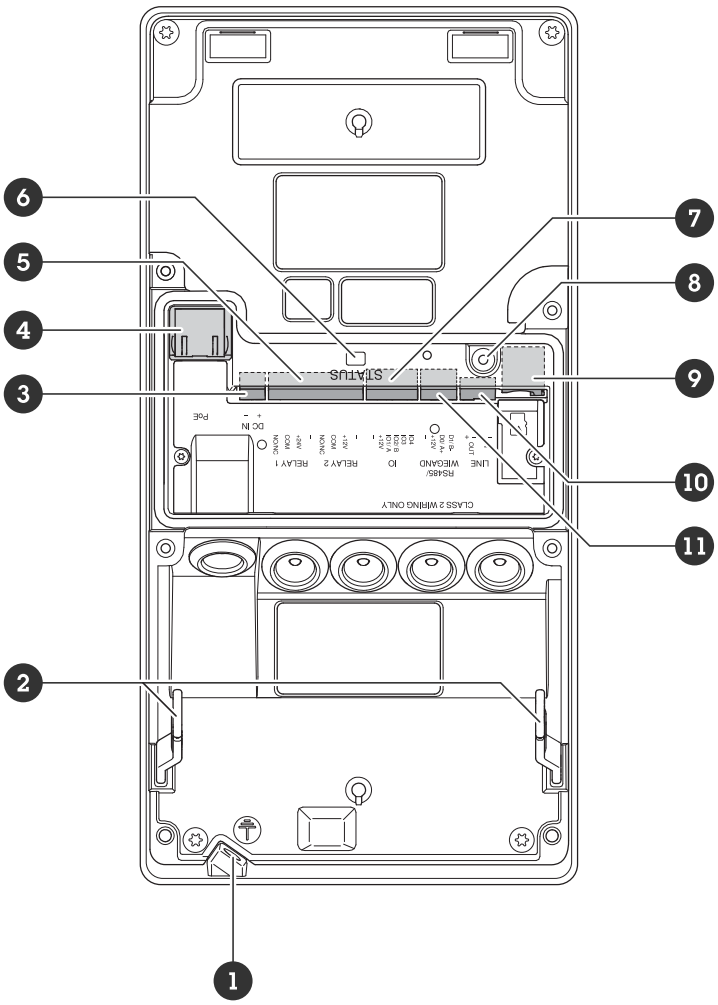
このアプリケーションを使うと、SIP対応のAxisデバイスと、リンクされたMicrosoft® Teamsアカウントの間で通話できます。詳細については、*AXIS Client for Unified Communication Systemsのユーザーマニュアル*を参照してください。

仕様

製品概要



1 マイク x2
2 Tコイル
3 RFIDリーダー
4 スピーカー
5 PIRセンサー
6 カメラ
7 ディスプレイ
8 光センサー



1 アース端子ネジ
2 設置用ヒンジ
3 電源コネクター
4 ネットワークコネクター
5 リレーコネクター x2
6 ステータスLED
7 I/Oコネクター
8 コントロールボタン
9 SDカードスロット (microSD)
10 音声コネクター
11 リーダーコネクター

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

- カードが損傷する恐れがあります。SDカードの挿入または取り出しの際は、鋭利な道具や

金属物を使用したり過度な力をかけたりしないでください。カードの挿入または取り出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。

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。*工場出荷時の設定へのリセット, on page 30*を参照してください。

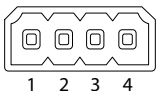
コネクター

ネットワークコネクター

Power over Ethernet Plus (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。

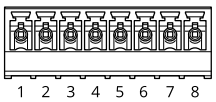


機能	ピン	メモ
ライン入力	1	ライン入力 (モノラル)
GND	2	音声アース
ライン出力端子	3	ライン出力端子
GND	4	音声アース

リレーコネクタ

ソリッドステートリレー用8ピンターミナルブロックは次の方法で使用できます。

- 標準的なリレーとして補助回路を開閉します。
- ロックを直接制御します。
- 安全リレーを通してロックを制御します。ドアの安全な側で安全リレーを使用すると、ショートを防止することができます。



機能	ピン	メモ	仕様
NO/NC	1	NO (Normally Open) / NC (Normally Closed) リレー装置の接続用。 2つの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 1 A 最大電圧 30 V DC
COM	2	コモン	
24 V DC	3	補助装置への電源供給用。 注:このピンは、電源出力としてのみ使用できます。	出力電圧24 V DC 最大電流 50 mA[1] 最大電流 300 mA[2]
DCアース	4		0 V DC
NO/NC	5	NO (Normally Open) / NC (Normally Closed) リレー装置の接続用。 2つの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 1 A 最大電圧 30 V DC
COM	6	コモン	
12 V DC	7	補助装置への電源供給用。 注:このピンは、電源出力としてのみ使用できます。	出力電圧12 V DC 最大電流100 mA[1] 最大電流 600 mA[2]
DCアース	8		0 V DC

リーダーコネクター

外部リーダー接続用4ピンターミナルブロック。

機能	ピン	メモ	仕様
DCアース	1		0 V DC
12 V DC	2	補助装置への電源供給用。 注:このピンは、電源出力としてのみ使用できます。	出力電圧12 V DC
D0/A+	3	Wiegand:DATA0出力 RS485: A+	
D1/B-	4	Wiegand:DATA1出力 RS485: B-	

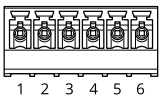
I/Oコネクター

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

1. *Power over Ethernet IEEE 802.3af/802.3at Type 1 Class 3*による給電時。
2. *Power over Ethernet Plus (PoE+) IEEE 802.3at Type 2 Class 4*または*DC*電源入よる給電時。

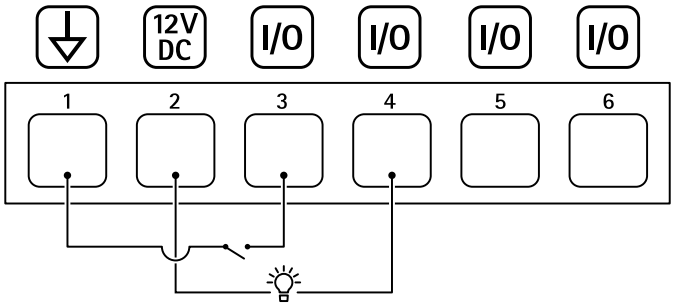
デジタル入力 - 開回路と閉回路の切り替えが可能な装置 (PIRセンサー、ドア/窓の接触、ガラス破損検知器など) を接続するための入力です。

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。



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)	3–6	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

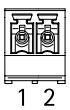
例:



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)*
5 *設定可能I/O*
6 *設定可能I/O*

電源コネクター

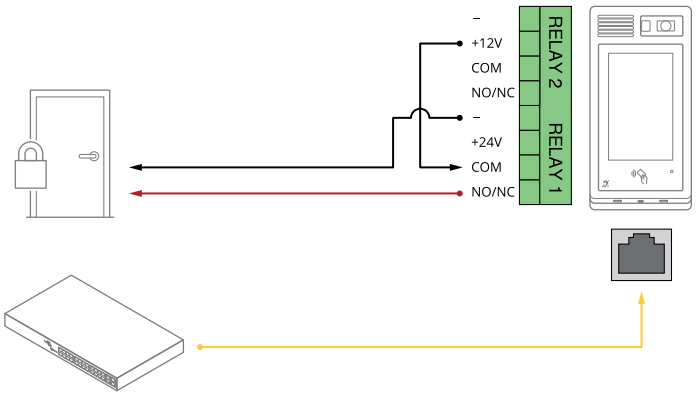
DC電源入力用2ピンターミナルブロック。定格出力が≤100 Wまたは≤5 Aの安全特別低電圧 (SELV) に準拠した有限電源 (LPS) を使用してください。



機能	ピン	メモ	仕様
DCアース	1		0 V DC
DC入力	2	Power over Ethernetを使用しないときのコントローラーへの電源供給用。 注:このピンは、電源入力としてのみ使用できます。	18～28 V DC、最大22 W出力の最大負荷 9 W

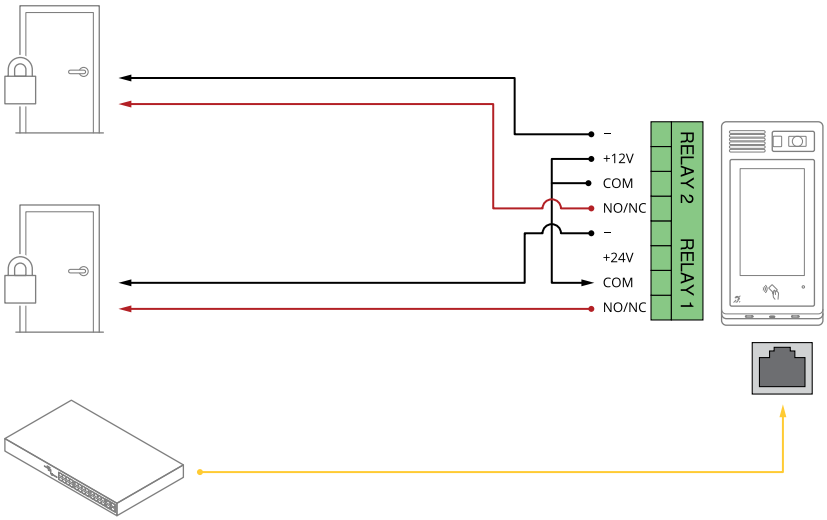
機器の接続

PoE (12V) 駆動リレー1個



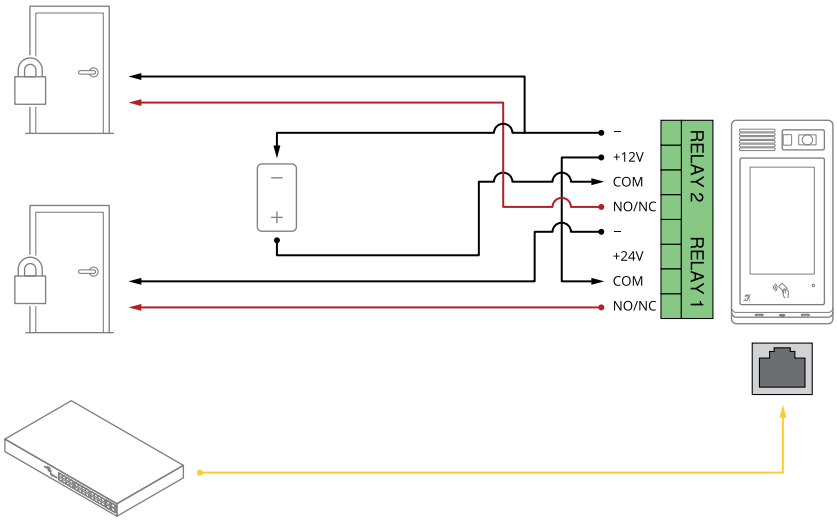
1. リレーの状態を確認するには、[System > Accessories (システム > アクセサリー)] に移動し、リレーポートを検索します。
2. [Normal state (通常)] に設定します。
   - でフェイルセキュアをロックします。
   - でフェイルセーフをロックします。

PoE (12V) 駆動リレー2個



1. 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。
   - でフェイルセーフをロックします。

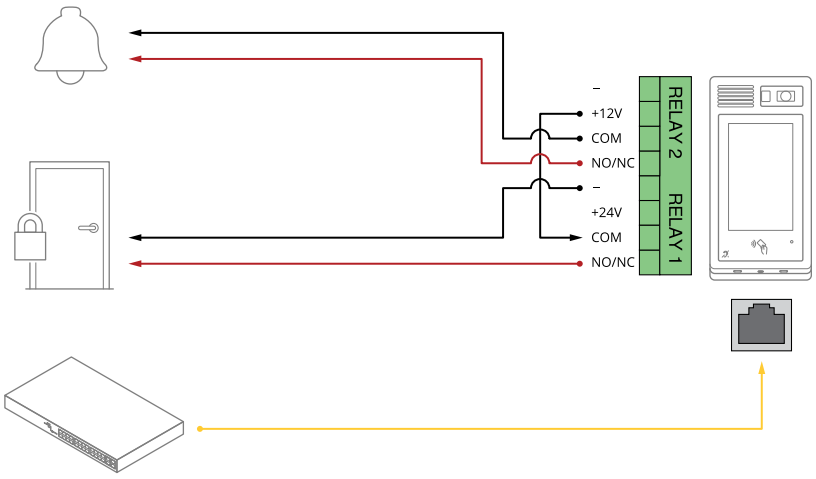
PoE (12V) 駆動リレー1個＋外部電源駆動リレー1個



1. 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。
   - でフェイルセーフをロックします。

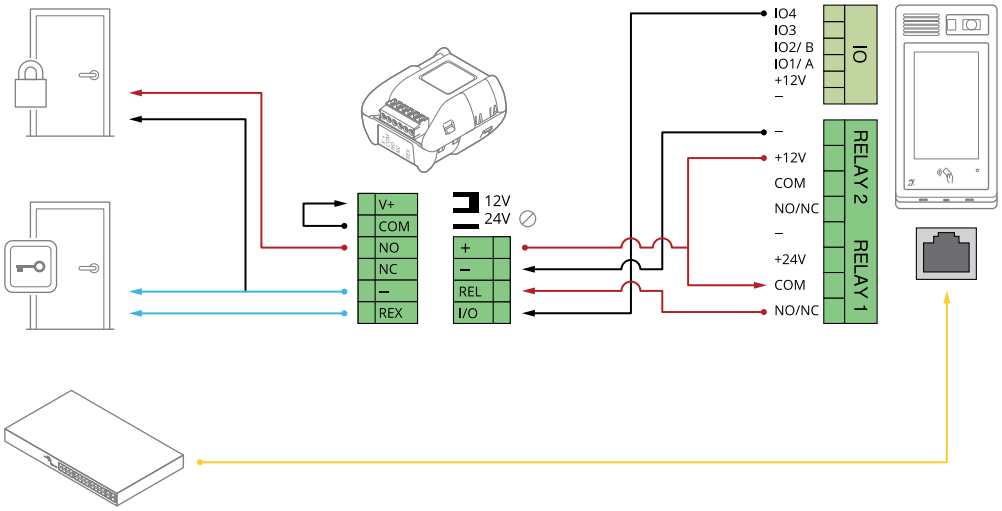
PoE (12V) 駆動リレー1個＋無電位接点リレー1個

無電位接点の例の一つはドアチャイムです。



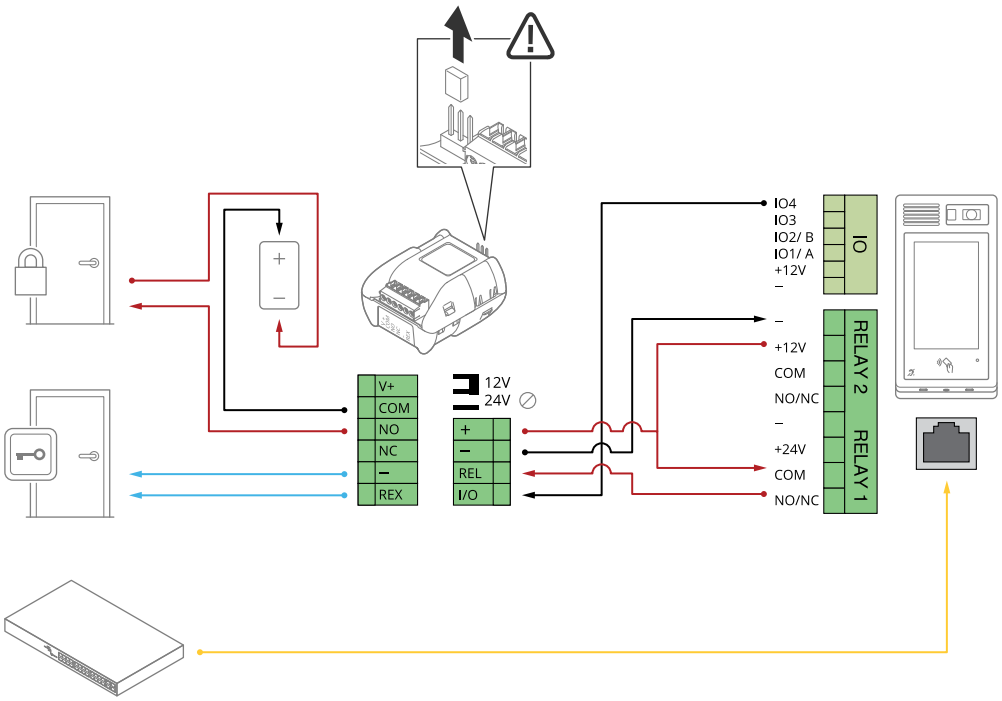
1. リレーの状態を確認するには、[System > Accessories (システム > アクセサリー)] に移動し、リレーポートを検索します。
2. [Normal state (通常)] に設定します。
   - でフェイルセキュアをロックします。
   - でフェイルセーフをロックします。

インターコムからのPoE+で電力を供給される12 Vフェールセキュアロック



1. 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。
   - でフェイルセーフをロックします。

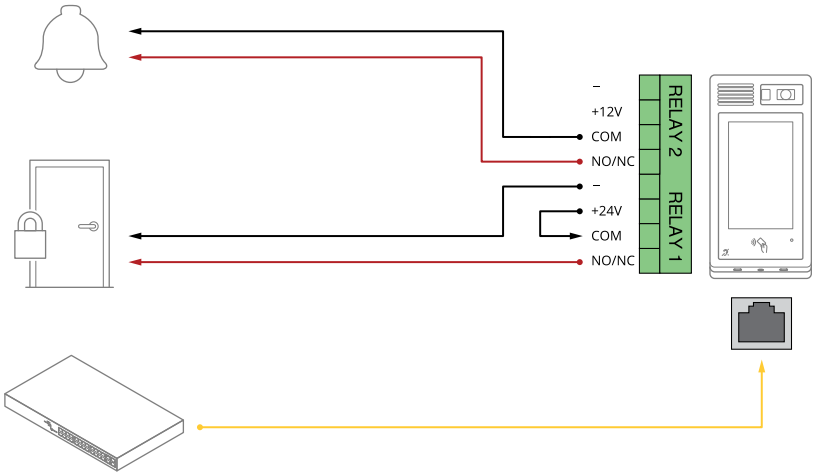
外部電源で電力を供給されるフェールセキュアロック



1. 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。
   - でフェイルセーフをロックします。

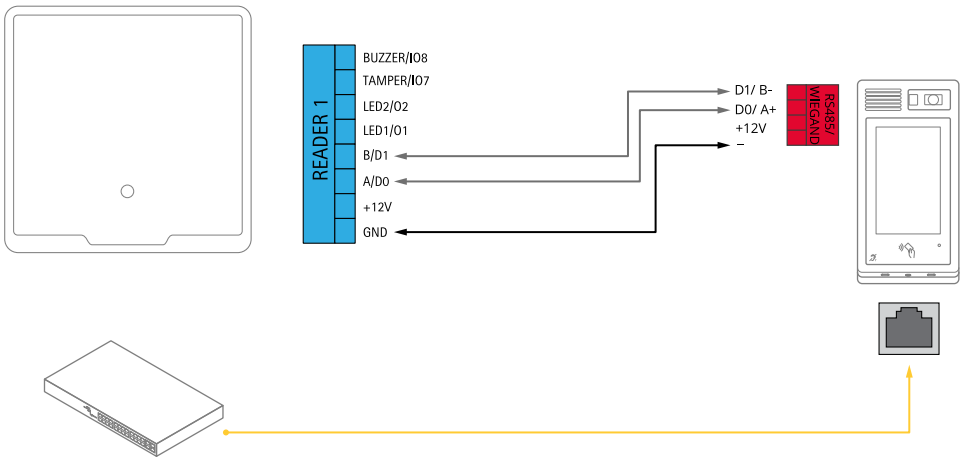
PoE (24V) 駆動リレー1個＋無電位接点リレー1個

無電位接点の例の一つはドアチャイムです。



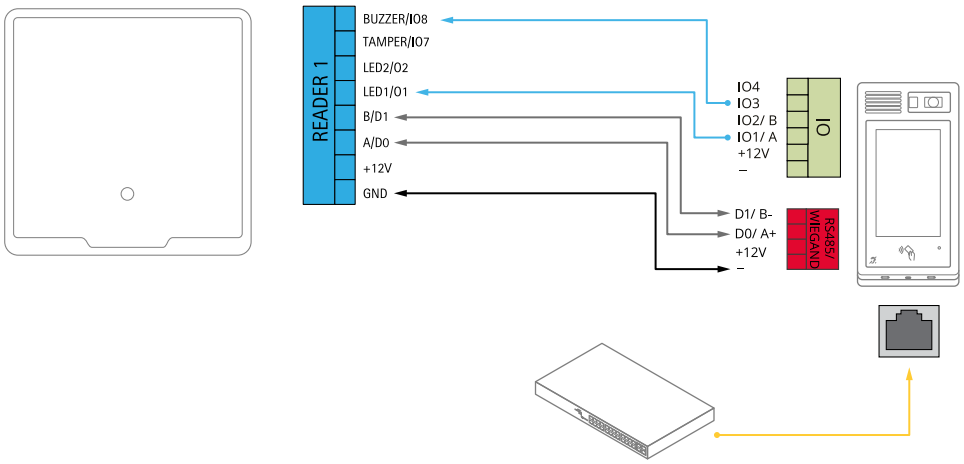
1. リレーの状態を確認するには、[System > Accessories (システム > アクセサリー)] に移動し、リレーポートを検索します。
2. [Normal state (通常)] に設定します。
   - でフェイルセキュアをロックします。
   - でフェイルセーフをロックします。

OSDPを使用してドアコントローラーに接続されたリーダー



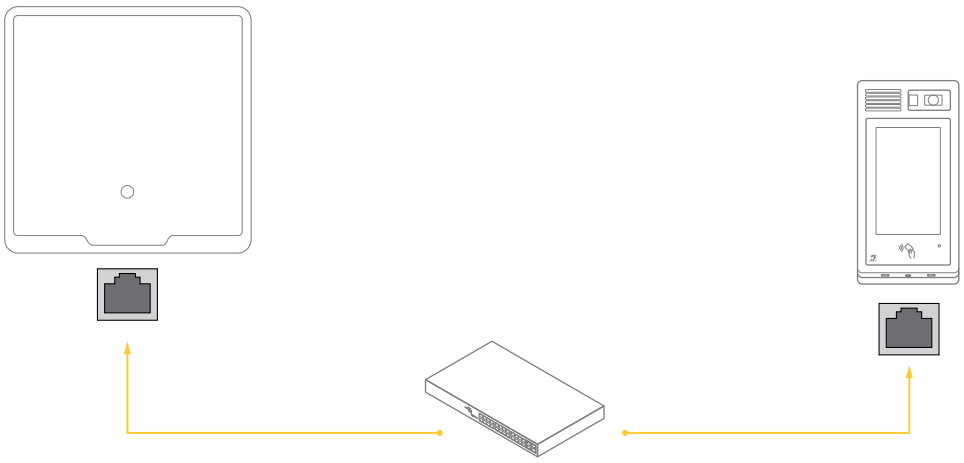
1. [Reader (リーダー)] > [Connection (接続)] > [Reader protocol (リーダープロトコル)] に移動します。
2. [Reader protocol type (リーダープロトコルタイプ)] を [OSDP] に設定し、[Save (保存)] をクリックします。

Wiegandを使用してドアコントローラーに接続されたリーダー



1. [Reader (リーダー)] > [Connection (接続)] > [Reader protocol (リーダープロトコル)] に移動します。
2. [Reader protocol type (リーダープロトコルタイプ)] を [Wiegand] に設定します。
3. [Beeper (ビーパー)] をオンにします。
4. [Input for beeper (ビーパーの入力)] で、[I3] を選択します。
5. [Input used for LED control (LEDコントロールで使用する入力)] で、[1] を選択します。
6. [Input for LED1 (LED1の入力)] で、[I1] を選択します。
7. その他の設定を調整し、[Save (保存)] をクリックします。

VAPIXリーダーを使用してAxisドアコントローラーに接続されたリーダー



1. [Reader (リーダー)] > [Connection (接続)] > [Reader protocol (リーダープロトコル)] に移動します。
2. [Reader protocol type (リーダープロトコルタイプ)] を [VAPIX reader (VAPIXリーダー)] に設定します。
3. Axisドアコントローラーに接続します。

トラブルシューティング

工場出荷時の設定へのリセット

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 19*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、*工場出荷時の設定へのリセット, on page 30*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 6*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。

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。帯域幅 (ビットレート) に影響を与える要因もあれば、フレームレートに影響を与える要因もあり、両方に影響する要因もあります。

考慮すべき最も重要な要因:

- 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。
- 多数のクライアントによるMotion JPEGまたはユニキャストH.264/H.265/AV1のアクセスは、帯域幅に影響を及ぼします。
- 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。

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。

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。

T10213214_ja

2026-10 (M12.2)

© 2025 – 2026 Axis Communications AB