

AXIS A8207-VE Mk II Network Video Door Station

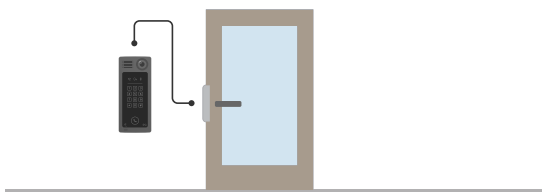
目次

ソリューションの概要	4
製品概要	5
インストール	7
使用に当たって	8
ネットワーク上のデバイスを検索する	8
ブラウザーサポート	8
装置のwebインターフェースを開く	8
管理者アカウントを作成する	8
安全なパスワード	9
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	9
webインターフェースの概要	9
追加設定	10
rootパスワードを変更する	10
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	10
ダイレクトSIP (P2P) を設定する	10
サーバーを介してSIPを設定する (PBX)	11
連絡先の作成	12
呼び出しボタンの設定	12
リーダーとして設定する	13
エントリ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。	13
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	14
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	15
DTMFを使用して来訪時にドアのロックを解除する	15
モニターへのライブ映像の送信	16
webインターフェース	17
詳細情報	18
Voice over IP (VoIP)	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)	19
イベントのルールを設定する	20
分析機能とアプリ	20
AXIS Client for Unified Communication Systems	20
日常的な使用	21
キーパッドの使用	21
トラブルシューティング	22
工場出荷時の設定にリセットする	22
AXIS OSの現在のバージョンを確認する	22
AXIS OSをアップグレードする	22
技術的な問題、ヒント、解決策	23
パフォーマンスに関する一般的な検討事項	24
仕様	26
フロントパネルインジケーターとコントロール	26
インジケーターアイコン	26
カードリーダーインジケーターストライプ	26
呼び出しボタン	26
LEDインジケーター	26
SDカードスロット	26
ボタン	26
コントロールボタン	26
コネクタ	27
HDMI™コネクタ	27
ネットワーク コネクタ	27

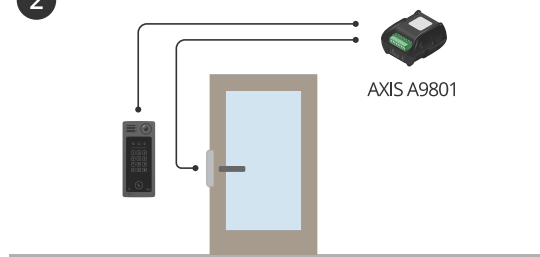
音声コネクター	27
リレーコネクタ	27
リーダーコネクター	28
I/Oコネクター	28
電源コネクター	29
安全情報	30
危険レベル	30
その他のメッセージレベル	30
サイバーセキュリティ	31
脆弱性の管理	31
セキュリティ通知	31
安全な製品ライフサイクル管理	31

ソリューションの概要

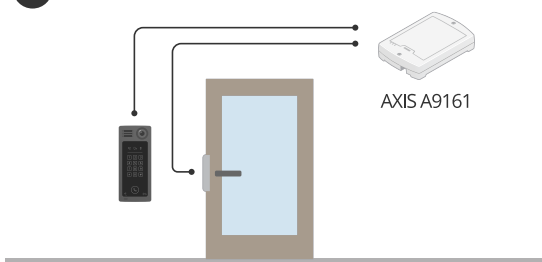
1



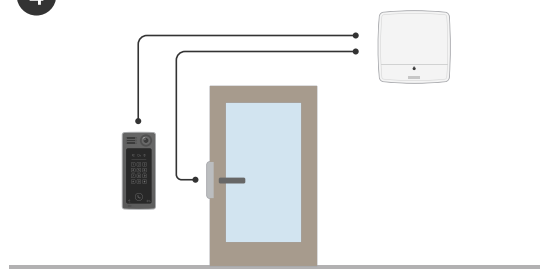
2



3

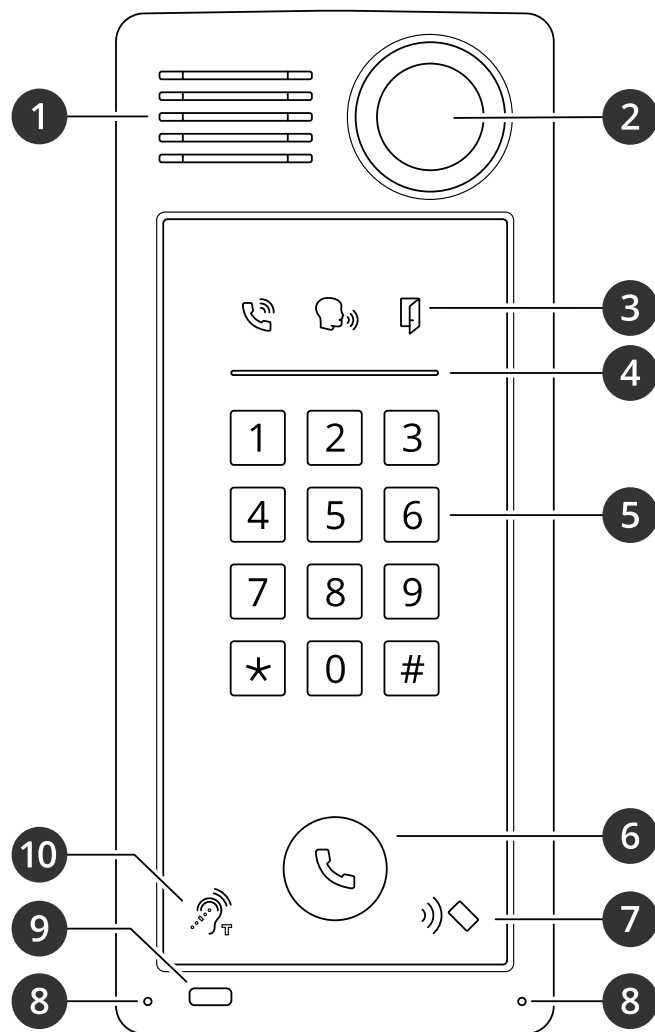


4

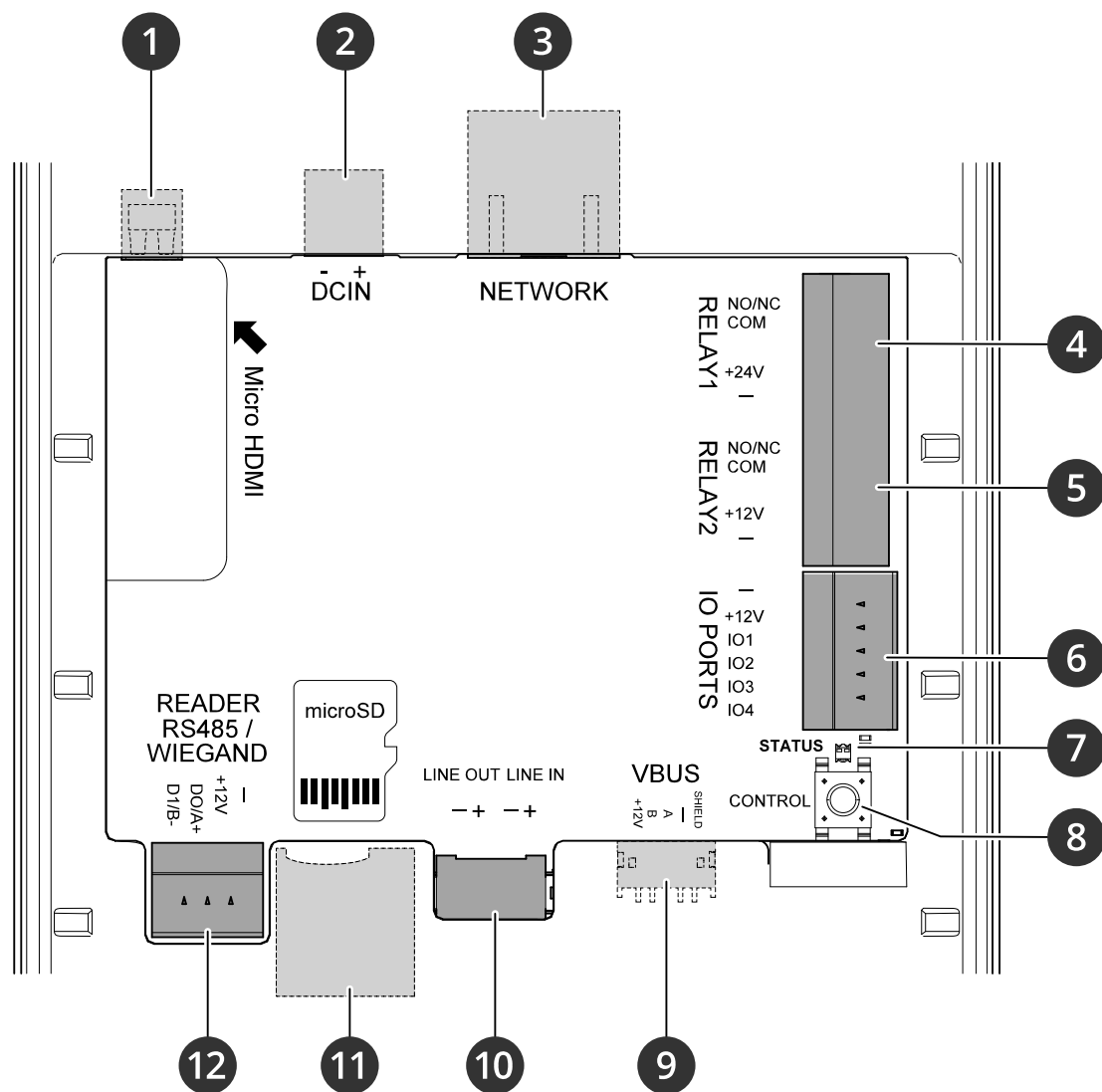


- 1 ドアステーション
- 2 ドアステーションとAXIS A9801の組み合わせ
- 3 ドアステーションとAXIS A9161の組み合わせ
- 4 ドアステーションとアクセスコントロールシステムの組み合わせ (AXIS A1001やAXIS A1601など)

製品概要



- 1 スピーカー
- 2 カメラ
- 3 インジケーターアイコン, on page 26
- 4 カードリーダーインジケーターストライプ, on page 26
- 5 キーパッド
- 6 呼び出しボタン, on page 26
- 7 カードリーダーアイコン
- 8 マイク
- 9 PIRセンサー
- 10 テレコイルアイコン



- 1 HDMI™コネクター, on page 27 (microHDMI)
- 2 電源コネクター, on page 29
- 3 ネットワーク コネクター, on page 27 (PoE+)
- 4 リレーコネクタ, on page 27
- 5 リレーコネクタ, on page 27
- 6 I/Oコネクター, on page 28
- 7 ステータスLED
- 8 コントロールボタン, on page 26
- 9 2N VBUS (未使用)
- 10 音声コネクター, on page 27
- 11 SDカードスロット, on page 26 (microSD/microSDHC/microSDXC)
- 12 リーダーコネクター, on page 28

インストール



このビデオを見るには、このドキュメントのWebバージョンにアクセスしてください。

A8207-VEリーダーのインストールビデオ。



このビデオを見るには、このドキュメントのWebバージョンにアクセスしてください。

A8207-VEリレーのインストールビデオ。

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。
この装置の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、ネットワーク上でこの装置を見つけてください。
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する, *on page 8*を参照してください。

AXIS OS搭載デバイスのWebインターフェースでの全機能と設定に関する説明については、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する

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

1. ユーザー名を入力してください。
2. パスワードを入力します。安全なパスワード, *on page 9*を参照してください。
3. パスワードを再入力します。
4. 使用許諾契約書に同意します。
5. [Add account (アカウントを追加)] をクリックします。

重要

装置にはデフォルトのアカウントはありません。管理者アカウントのパスワードを紛失した場合は、装置をリセットする必要があります。工場出荷時の設定にリセットする, *on page 22*を参照してください。

安全なパスワード

重要

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

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

データを保護するために、次のことが強く推奨されています。

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

デバイスのソフトウェアが改ざんされていないことを確認する

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

1. 工場出荷時の設定にリセットします。工場出荷時の設定にリセットする, on page 22を参照してください。
リセットを行うと、セキュアブートによって装置の状態が保証されます。
2. デバイスを設定し、インストールします。

webインターフェースの概要

このビデオでは、装置のwebインターフェースの概要について説明します。



Axis装置のwebインターフェース

追加設定

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。

rootパスワードを変更する

1. 装置インターフェースにログインし、[System > Users (システム > ユーザー)] に移動します。
2. rootユーザーの場合、 > [Update user(ユーザーの更新)] をクリックします。
3. 新しいパスワードを入力し、保存します。

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。壁の建設や撤去などによって、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 5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 18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 18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、ピアツーピアSIP (P2PSIP), on page 18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。
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。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、*Voice over IP (VoIP), on page 18*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 18*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 19*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、*ダイレクトSIP (P2P)* を設定する、*on page 10*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 18*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。

リーダーとして設定する

ドアステーション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、ドアステーション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。

ドアステーションをドアコントローラーに接続している場合でも、ドアステーションは最大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、ドアステーション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。

要件

- **[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. **[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. **[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

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、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 14を参照してください。

ドアステーション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. [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. [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、デバイス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

- ドアステーションをドアコントローラーに接続します。
電気配線図を参照してください。axis.com/products/axis-a8207-ve-mk-ii/supportからダウンロードできます。
- 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ズマニュアルを参照してください。

ドアステーション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. [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. [保存] をクリックします。

DTMFを使用して来訪時にドアのロックを解除する

訪問者がドアステーション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。

- ドアステーションのDTMF信号を定義する
- 次のようにドアステーションを設定します。
 - 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。

すべての設定はドアステーションの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。「ダイレクトSIP (P2P) を設定する, on page 10」および「サーバーを介してSIPを設定する (PBX), on page 11」を参照してください。

ドアステーションの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、ドアステーションを設定する

7. [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。

モニターへのライブ映像の送信

ネットワーク接続がなくても、デバイスからHDMIモニターにライブビデオストリームを送信できます。モニターを使用して、ドアの前にいる人物を確認します。

1. 外部モニターをHDMIコネクタと接続します。
2. [System > Video out (システム > ビデオ出力)] で、HDMI設定を調整します。

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と設定については、*AXIS OSウェブインターフェースのヘルプ*を参照してください。

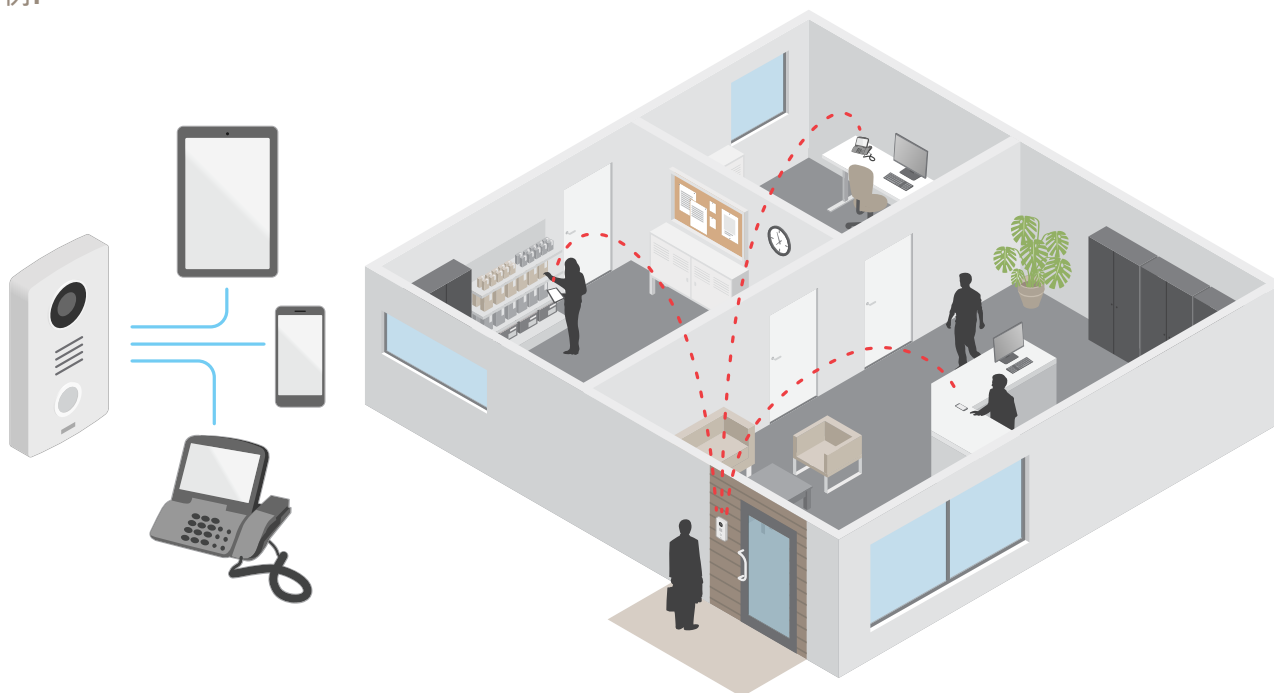
詳細情報

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ドアステーションで呼び出しボタンを押すと、1つ以上の事前定義された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。

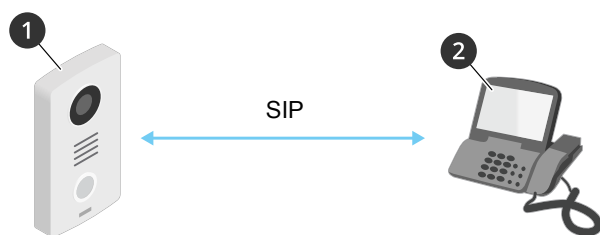
実際の音声またはビデオは、RTP (Real-time Transport Protocol) などのトランスポートプロトコルを使用して、SIPユーザーエージェントの間で交換されます。

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>です。

例:



- 1 ユーザーエージェントA - ドアステーション。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ドアステーションを設定することができます。

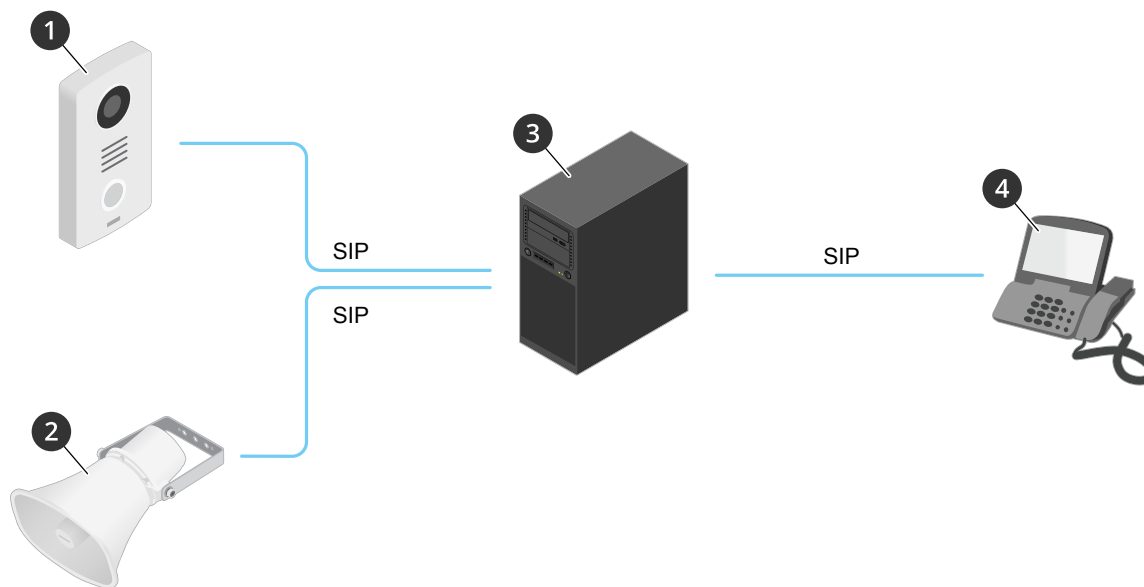
構内交換機 (PBX)

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。

例:



- 1 `sip:mydoor@company.com`
- 2 `sip:myspeaker@company.com`
- 3 **PBX** `sip.company.com`
- 4 `sip:office@company.com`

Axisドアステーション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、「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。

日常的な使用

キーパッドの使用

目的のアクション	動作
建物の中に入れてくれる人に電話します。	 を押します。
建物内の人物を呼び出します。	その人の短縮ダイヤル番号を入力し、  を押します。
自分のカードとPINを使用してドアを開きます。	カードをタップして、PINを入力します。
PINを使用してドアを開きます。	PINを入力し#を押します。
自分のカードを使用してドアを開きます。	カードをタップします。

トラブルシューティング

工場出荷時の設定にリセットする

重要

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

本製品を工場出荷時の設定にリセットするには、以下の手順に従います。

1. 本製品の電源を切ります。
2. コントロールボタンを押した状態で電源を再接続します。製品概要, on page 5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、装置のIPアドレスのデフォルトは次のいずれかになります。
 - **AXIS OS 12.0以降の装置:** リンクローカルアドレスサブネット（169.254.0.0/16）から取得
 - **AXIS OS 11.11以前の装置:** 192.168.0.90/24
5. インストールおよび管理ソフトウェアツールを使用して、IPアドレスの割り当て、パスワードの設定、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

- 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、装置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。

ファームウェアのアップグレードで問題が発生する	
ファームウェアのアップグレード失敗	ファームウェアのアップグレードに失敗した場合、デバイスは以前のファームウェアを再度読み込みます。最も一般的な理由は、間違ったファームウェアファイルがアップロードされた場合です。デバイスに対応したファームウェアファイル名であることを確認し、再試行してください。

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別のデバイスとIPアドレスが競合している可能性がある	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。

ブラウザからデバイス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、ログインを試みる時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。 |
| DHCPによってIPアドレスが変更された | rootユーザー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。工場出荷時の設定にリセットする, on page 22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。 |

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

デバイス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 Companion: 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: 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。

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。

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。

仕様

フロントパネルインジケータとコントロール

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が数秒間点灯します。

インジケータアイコン

アイコン	説明
	発信が開始されると青色に点灯します。 着信が開始されると青色に点滅します。
	通話中はオレンジ色に点灯します。
	ドアが開いているときは緑色に点灯します。

カードリーダーインジケータストライプ

このストライプは、リーダーからのフィードバックを示します。

呼び出しボタン

呼び出しボタンの周囲に組み込まれたライトを使用して、訪問者の顔を照らすことができます。

LEDインジケータ

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。

 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、以下の用途で使します。

- 製品を工場出荷時の設定にリセットする。工場出荷時の設定にリセットする, on page 22を参照してください。

コネクター

HDMI™コネクター

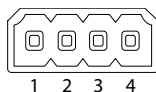
ディスプレイやパブリックビューモニターへの接続には、microHDMI™コネクタを使用します。

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。

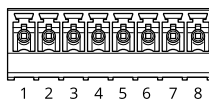


機能	ピン	メモ
ライン入力	1	ライン入力 (モノラル)
GND	2	音声アース
ライン出力端子	3	ライン出力端子
GND	4	音声アース

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氣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 350 mA ²
DCアース	4		0 V DC

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電源入による給電時。

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氣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 ³ 最大電流 700 mA ⁴
DCアース	8		0 V DC

リーダーコネクタ

外部リーダー接続用4ピンターミナルブロック。

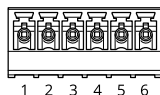
機能	ピン	メモ	仕様
DCアース	1		0 V DC
12 V DC	2	補助装置への電源供給用。 注:このピンは、電源出力としてのみ使用できます。	出力電圧12 V DC
D0/A+	3	Wiegand: DATA0出力 RS485: A+	
D1/B-	4	Wiegand: DATA1出力 RS485: B-	

I/Oコネクタ

I/Oコネクタに外部装置を接続し、動体検知、イベントトリガー、アラーム通知などと組み合わせて使用することができます。I/Oコネクタは、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。



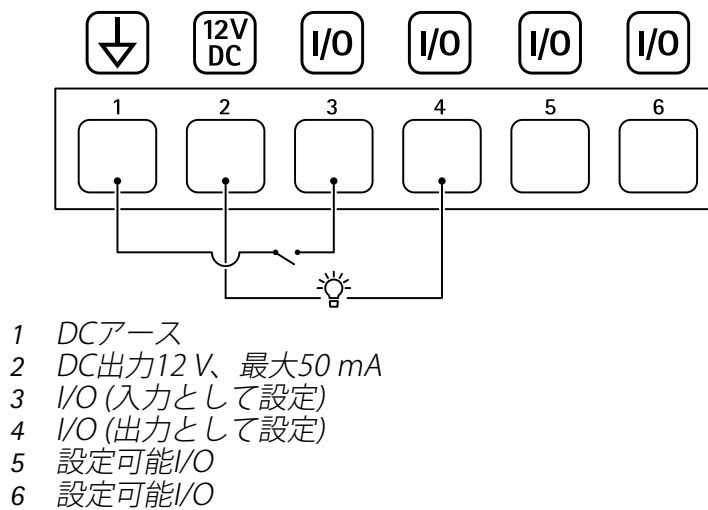
機能	ピン	メモ	仕様
DCアース	1		0 VDC

3. Power over Ethernet IEEE 802.3af/802.3at Type 1 Class 3による給電時。

4. Power over Ethernet Plus (PoE+) IEEE 802.3at Type 2 Class 4またはDC電源入による給電時。

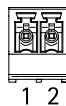
DC出力	2	 補助装置の電源供給に使用できます。 注:このピンは、電源出力としてのみ使用できません。	12VDC 最大負荷 = 50 mA
設定可能 (入力または出力)	3-6	デジタル入力 – 動作させるにはピン1に接続し、動作させない場合はフロート状態 (未接続) のままにします。	0～最大30 VDC
		デジタル出力 – アクティブ時はピン1 (DCアース) に内部で接続し、非アクティブ時はフロート状態 (未接続) になります。リレーなどの誘導負荷とともに使用する場合は、過渡電圧から保護するために、負荷と並列にダイオードを接続します。	0～30 VDC (最大)、 オープンドレイン、 100 mA

例:



電源コネクタ

DC電源入力用2ピンターミナルブロック。定格出力が ≤ 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。	8～28 V DC、最大22 W 出力の最大負荷 9 W

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や文書は、axis.com/about-axis/cybersecurityで確認できます。以下のサイバーセキュリティガイドラインに従って、Axisから製品に関するセキュリティ通知を受け取り、安全なライフサイクルと利用停止を確保するために製品を設定してください。

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ください。

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でAxisのセキュリティ通知メールを受け取る用に設定してください。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ー、およびその他のセキュリティ関連事項に関する情報を送信いたします。

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。

T10176599_ja

2026-07 (M25.2)

© 2021 – 2026 Axis Communications AB