AXIS I7020 ネットワークインターコム

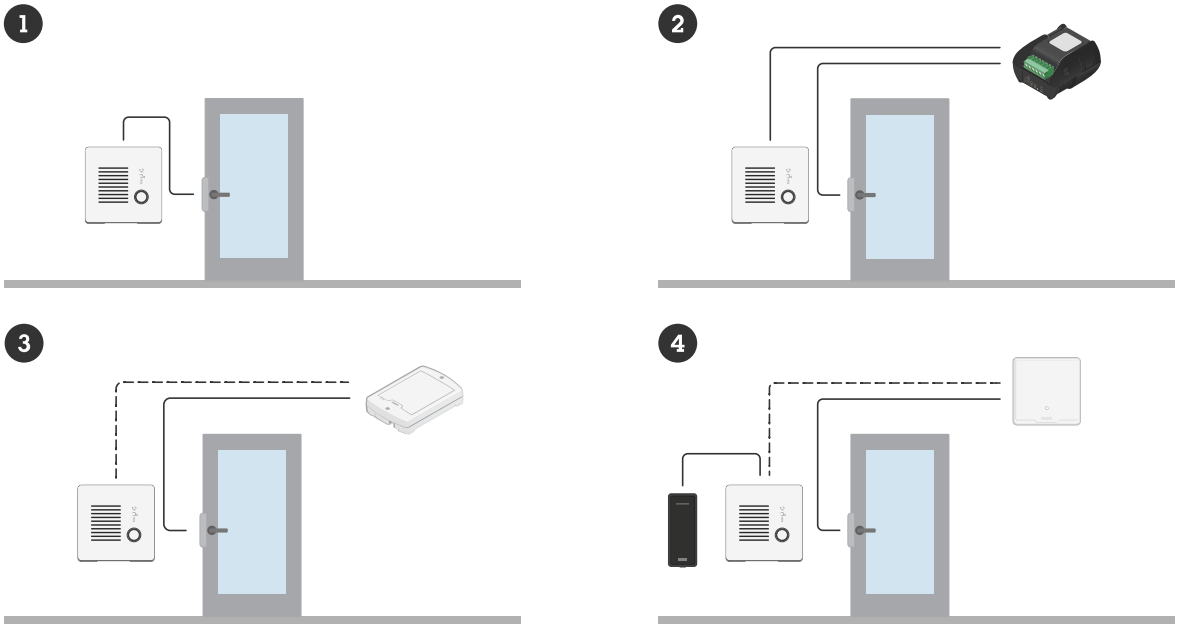
ユーザーマニュアル

目次

設定の概要 4
使用に当たって 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 6
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 6
デバイスを構成する 7
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 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
近くのカメラからのビデオ ストリームをSIP通話に含める 9
連絡先の作成 9
呼び出しボタンの設定 9
DTMFを使用して来訪時にドアのロックを解除する 10
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。 10
イベントのルールを設定する 11
アクションをトリガーする 11
webインターフェース 12
詳細情報 13
Voice over IP (VoIP) 13
セッション開始プロトコル (SIP) 13
ピアツーピアSIP (P2PSIP) 13
構内交換機 (PBX) 14
NATトラバーサル 15
分析機能とアプリ 15
AXIS Client for Unified Communication Systems 15
仕様 16
製品概要 16
フロントパネルインジケーターとコントロール 16
インジケーターアイコン 16
LEDインジケーター 16
SDカードスロット 17
ボタン 17
コントロールボタン 17
コネクター 17
ネットワークコネクター 17
音声コネクター 17
I/O、リーダー、リレーコネクター 17
機器の接続 20
Axisリーダー 20
PoE (12V) で電力を供給されるリレー 20
別の電源で電力を供給されるリレー 20
無電圧リレー 21
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 21
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 22
清掃の推奨事項 23
トラブルシューティング 24
工場出荷時の設定へのリセット 24
AXIS OSのオプション 24
AXIS OSの現在のバージョンを確認する 24
AXIS OSをアップグレードする 25

技術的な問題と解決策 25
パフォーマンスに関する一般的な検討事項 27
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
安全情報 30
危険レベル 30
その他のメッセージレベル 30

設定の概要



1 インターコム
2 インターコムとAXIS A9801の組み合わせ
3 インターカムとAXIS A9161の組み合わせ
4 インターカム、リーダー、アクセスコントロールシステムの組み合わせ

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 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 6*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 24*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 24*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 16*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 13*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 13*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 13*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 15*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 13*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 13*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 14*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 7*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。

近くのカメラからのビデオ ストリームをSIP通話に含める

Axisカメラがインターコムの近くにマウントされている場合は、カメラからのビデオストリームをインターコムのSIPおよびVMS通話に含めることができます。

要件

H.264および解像度1280x720、800x800、640x480のいずれかを備えたAxisカメラ。

インターコムをカメラに接続する方法：
1. [System > Edge-to-edge > Pairing (システム > エッジツーエッジ > ペアリング)] に移動します。
2. Camera pairing (カメラのペアリング)に、Axisカメラのアドレス、ユーザー名、パスワードを入力します。
3. [Connect (接続)] をクリックします。

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 13*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。

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。
- インターコムのDTMF信号を設定する
- 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。*ダイレクトSIP (P2P) を設定する, on page 7*および *サーバーを介してSIPを設定する (PBX), on page 8*を参照してください。

インターコムのDTMF信号を設定する。
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. **[Save (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コムを設定する
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. **[Save (保存)]** をクリックします。

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。

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。

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。

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。

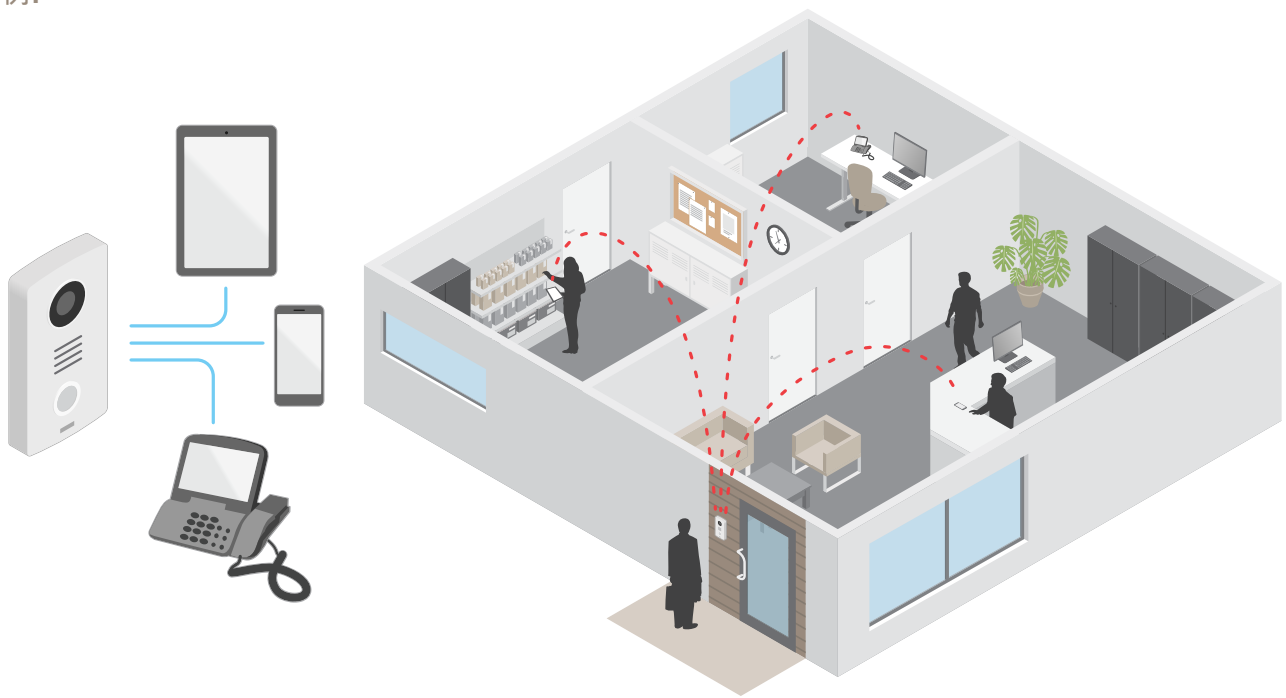
詳細情報

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。

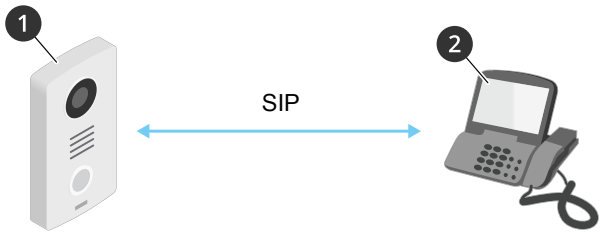
実際の音声またはビデオは、RTP (Real-time Transport Protocol) などのトランスポートプロトコルを使用して、SIPユーザーエージェントの間で交換されます。

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。

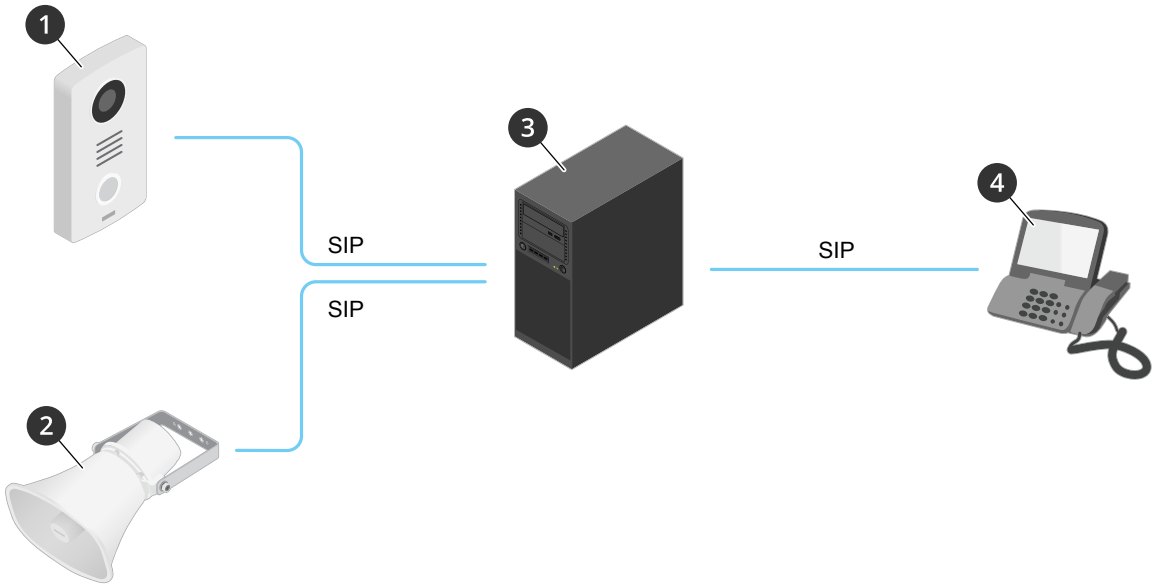
構内交換機 (PBX)

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。

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。

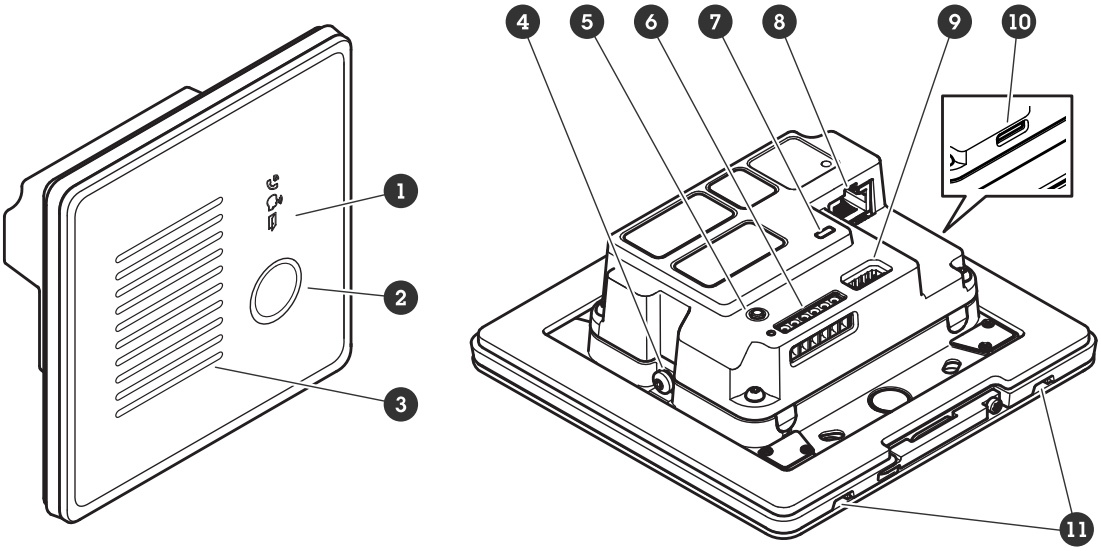
Axisの分析機能とアプリのユーザーマニュアルは、*help.axis.com*から参照できます。

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 インジケーターアイコン, on page 16
2 呼び出しボタン
3 スピーカー
4 アース端子ネジ
5 コントロールボタン, on page 17
6 I/O、リーダー、リレーコネクター, on page 17
7 ステータスLED
8 ネットワークコネクター, on page 17
9 音声コネクター, on page 17
10 SDカードスロット, on page 17 (microSD/microSDHC/microSDXC)
11 マイクロフォン (x2)

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。 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

- 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 24*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。

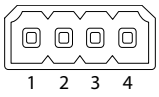
コネクター

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

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。

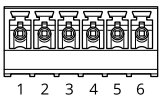


機能	ピン	メモ
ライン入力	1	ライン入力 (モノラル)
GND	2	音声アース
ライン出力端子	3	ライン出力 (モノラル)
GND	4	音声アース

I/O、リーダー、リレーコネクター

このコネクターは、I/Oおよびリレー、またはリーダーへの接続に使用できます。

6ピンターミナルブロック。



1 -
2 12V
3 A/IO1
4 B/IO2
5 COM
6 NO/NC

機能	ピン	メモ	仕様
DCアース	1		0 V DC
DC出力	2	デバイスがPoE Class 4によって給電されている場合、補助装置への給電に使用できます。 注:このピンは、電源出力としてのみ使用できます。	12 V DC I/O :最大負荷 = 50 mA リーダー/リレー: 最大負荷 = 350 mA
I/O:設定可能(入力または出力) リーダー：A	3	I/O: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。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、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します。 リーダー: RS485 - A	I/O :入力 - 0～最大30 V DC 出力 - 0～最大30V DC、オープンドレイン最大100mA
I/O:設定可能(入力または出力) リーダー：B	4	I/O:ピン3と同じ リーダー: RS485 - B	I/O:ピン3と同じ
リレー:COM	5	コモン	
リレー:NO/NC	6	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700 mA、最大電圧30 V DC

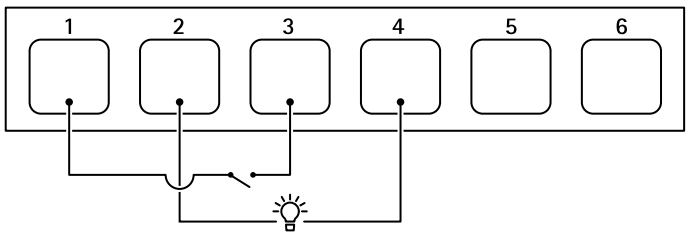
I/Oコネクター

1つのオプションは、I/Oコネクターに外部装置を接続し、いたずら警報、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です。I/Oコネクターは、0 V DC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装置インターフェースから有効にすることができます。

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 リレーのみ
6 リレーのみ

リレーコネクタ

I/Oと組み合わせて使用すると、コネクターをリレーコネクターとして使用して、ソリッドステートリレーを接続し、次のように使用できます。

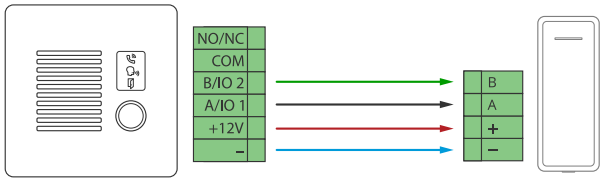
- 標準的なリレーとして補助回路を開閉します。
- ロックを直接制御します。
- 安全リレーを通してロックを制御します。ドアの安全な側で安全リレーを使用すると、ショートを防止することができます。

リーダーコネクター

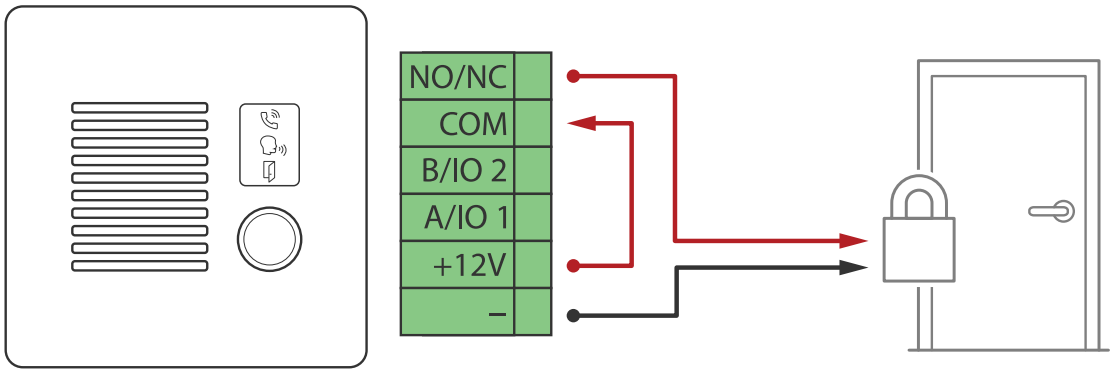
3つ目のオプションは、コネクターをリーダーコネクターとして使用して外部リーダーを接続する方法です。

機器の接続

Axisリーダー

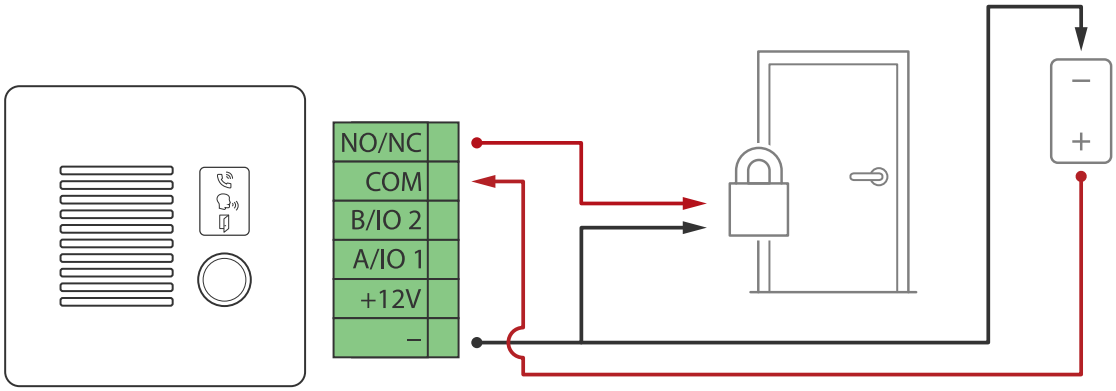


PoE (12V) で電力を供給されるリレー



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。

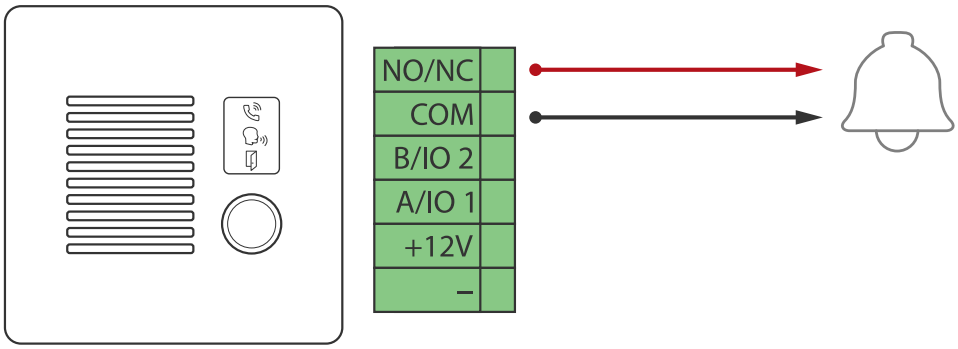
別の電源で電力を供給されるリレー



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。

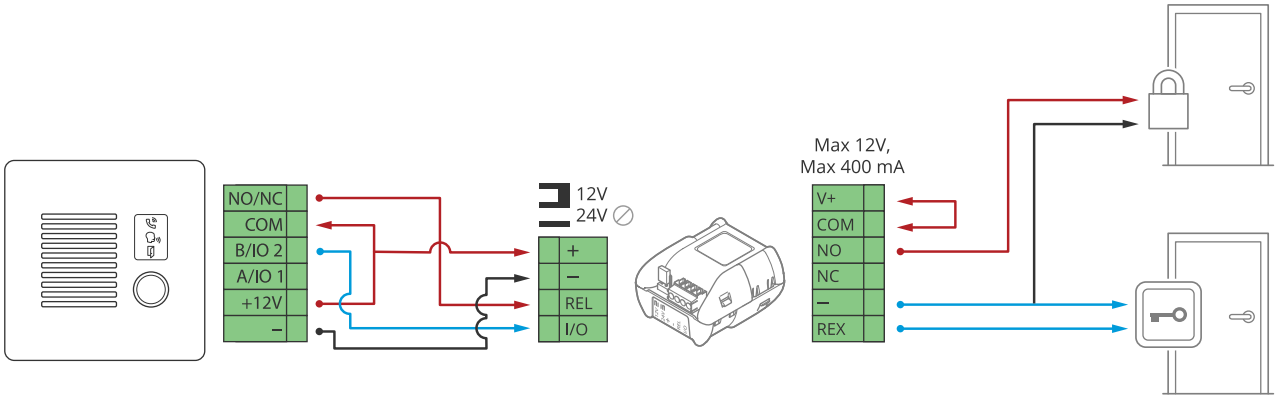
– でフェイルセーフをロックします。

無電圧リレー



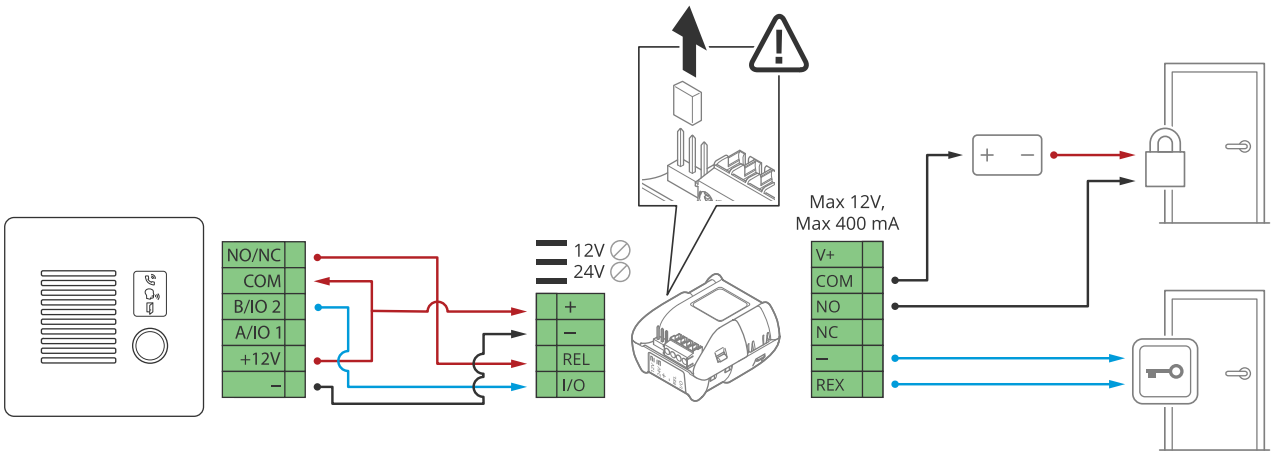
1. リレーの状態を確認するには、[System > Accessories (システム > アクセサリー)] に移動し、リレーポートを検索します。
2. [Normal state (通常)] に設定します。
   – でフェイルセキュアをロックします。
   – でフェイルセーフをロックします。

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



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。

清掃の推奨事項

AXIS I7020 Network Intercomは、上記の化学薬品を使用した1日数回の清掃に少なくとも5年間耐えることができます。

インターコムのフロントプレートは、柔らかい布を用いた定期的かつ頻繁な化学薬品による拭き取りに耐えます。フロントプレートの材料と洗剤は化学反応を起こしません。化学薬品を用いて毎日拭き取りを行っても、インターコムの物理的な完全性は維持されます。デバイスは以下の化学薬品を混ぜたぬるま湯で洗浄できます。

- イソプロパノール 70% (IPA)
- 過酸化水素 3% (H_2O_2)
- 次亜塩素酸ナトリウム<5% (NaClO) (塩素系漂白剤)
- 酢酸（10%）
- 過酢酸（0.12%）

⚠ 注意

洗剤を使用する前に、洗剤メーカーが提供する安全データシート (SDS) を読み、遵守してください。

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。アセトンやガソリ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。
- 装置に洗剤を直接スプレーしないでください。代わりに、非研磨性の布に洗剤をスプレーし、その布で装置を清掃してください。
- 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、ぬるま湯と洗剤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. 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。

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 16*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 24*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。

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。

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。

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。

T10213215_ja

2026-10 (M15.2)

© 2024 – 2026 Axis Communications AB