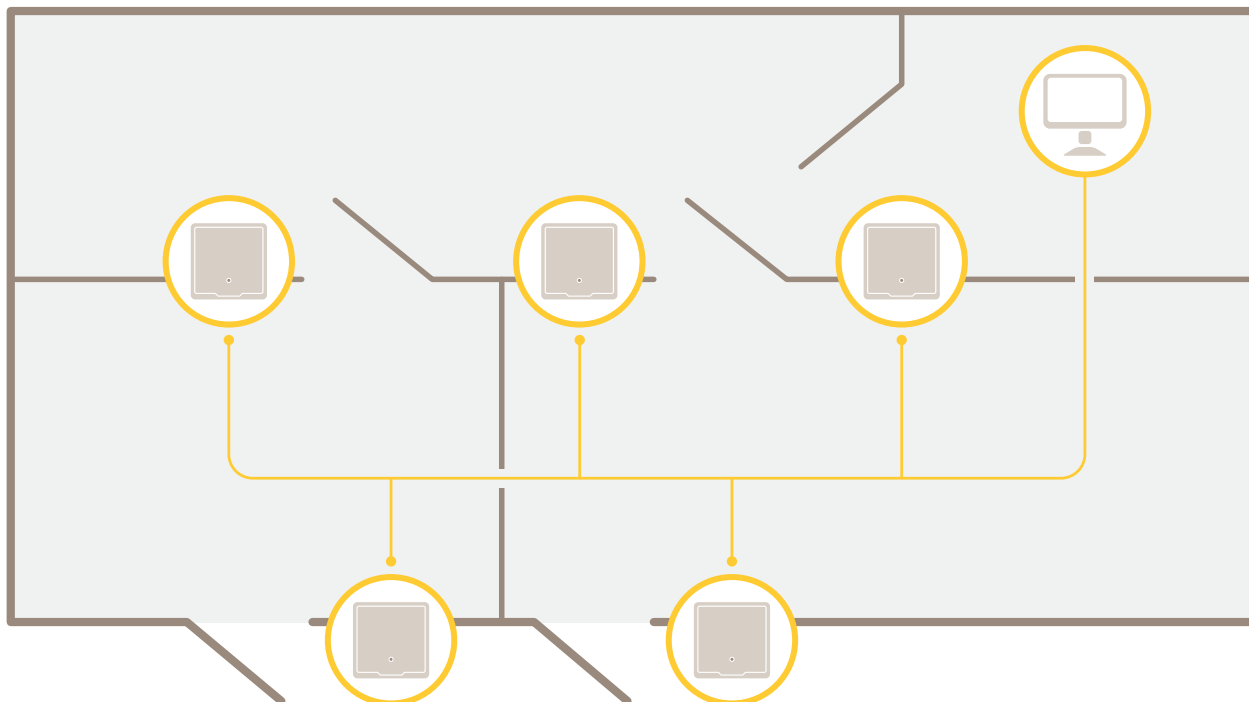


AXIS A1610-B Network Door Controller

目次

| | |
|------------------------------------|----|
| ソリューションの概要 | 3 |
| 使用に当たって | 4 |
| ネットワーク上のデバイスを検索する | 4 |
| ブラウザーサポート | 4 |
| 装置のwebインターフェースを開く | 4 |
| 管理者アカウントを作成する | 4 |
| 安全なパスワード | 5 |
| 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 | 5 |
| webインターフェースの概要 | 5 |
| デバイス構成 | 6 |
| AXIS A9910を追加する | 6 |
| エレベーターの制御 | 6 |
| ドアオーバーライド | 6 |
| webインターフェース | 7 |
| 詳細情報 | 8 |
| サイバーセキュリティ | 8 |
| 署名付きOS | 8 |
| セキュアブート | 8 |
| Axis Edge Vault | 8 |
| AxisデバイスID | 8 |
| 仕様 | 9 |
| 製品概要 | 9 |
| LEDインジケータ | 9 |
| ボタン | 10 |
| コントロールボタン | 10 |
| コネクタ | 10 |
| ネットワークコネクタ | 10 |
| 電源の優先順位 | 10 |
| リーダーコネクタ | 11 |
| 監視入力 | 12 |
| ドアコネクタ | 12 |
| リレーコネクタ | 13 |
| 補助コネクタ | 14 |
| 外部コネクタ | 15 |
| 電源コネクタ | 15 |
| 12Vバックアップ電源入力 | 16 |
| トラブルシューティング | 17 |
| 工場出荷時の設定にリセットする | 17 |
| AXIS OSのオプション | 17 |
| AXIS OSの現在のバージョンを確認する | 17 |
| AXIS OSをアップグレードする | 18 |
| 技術的な問題と解決策 | 18 |
| パフォーマンスに関する一般的な検討事項 | 20 |
| サポートに問い合わせる | 20 |

ソリューションの概要



ネットワークドアコントローラーは、既存のIPネットワークに容易に接続して給電することができ、特殊な配線は必要ありません。

各ネットワークドアコントローラーは、ドアの近くに容易に取り付けることができるインテリジェントデバイスです。最大4台のリーダーに給電したり制御したりできます。

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。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 4*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 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。

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 17*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 17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

デバイスを構成する

装置の設定方法については、*AXIS Camera Station*ユーザーマニュアルまたはサードパーティ製のソリューションを参照してください。

AXIS A9910を追加する

- ドアコントローラーのWebインターフェースで、**[Device (デバイス)] > [I/Os and relays (I/Oとリレー)]** に移動します。
- **[Add encryption key (暗号化キーの追加)]** をクリックします。
- すでに暗号化キーを生成している場合は、そのキーを入力して **[OK]** をクリックします。
- 暗号化キーは、以下の手順に沿って生成します。
 - **[Generate key (鍵を生成する)]** をクリックします。
 - **[Export key (キーをエクスポートする)]** をクリックしてキーを保存します。暗号化キーを紛失すると、デバイスへアクセスできなくなります。
 - **[OK]** をクリックします。
- **[Add AXIS A9910 (AXIS A9910を追加する)]** をクリックします。
- 名前を入力し、使用するRS485ポートとアドレスを選択します。
- **[OK]** をクリックします。

エレベーターの制御

エレベーターキャビン内にリーダーを設置し、ドアコントローラーとAXIS A9910を使用することで、各階へのアクセスを制御できます。*AXIS A9910を追加する, on page 6*を参照してください。

単一のドアコントローラーとAXIS A9910拡張モジュールに接続できる階数は最大16階です。

- コントローラーのリーダーポートの1つは、拡張モジュールに使用します。
- もう一方のリーダーポートは、エレベーターキャビン内に設置するリーダーに使用します。

ドアオーバーライド

重要

この機能はドアリレーを直接制御し、AXIS Camera Stationでのリレー設定をオーバーライドします。この機能は、Axisサポートから指示があった場合のみ使用します。

1. AXIS Camera StationのSecure Entryサービスを停止します。
2. ドアコントローラーのWebインターフェースで、**[Advanced (詳細設定)] > [Door override (ドアオーバーライド)]** に移動します。
3. ページの内容をよく読んでから **[I understand (理解しました)]** をクリックします。
4. **[Door override (ドアオーバーライド)]** をオンにし、**[Enable (有効にする)]** をクリックします。
5. ドアリレーに移動し、**[Lock (ロック)]**、**[Unlock (ロック解除)]**、または**[Access (アクセス)]** をクリックし、ドアのロック、ロック解除、またはアクセス権の付与を行います。
6. 設定するリレーに移動し、**[Activate (有効にする)]** または **[Deactivate (無効にする)]** をクリックしてリレーを有効または無効にします。

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

サイバーセキュリティ

サイバーセキュリティに関する製品固有の情報については、axis.comの製品データシートを参照してください。

AXIS OSのサイバーセキュリティの詳細情報については、『AXIS OS強化ガイド』を参照してください。

署名付きOS

署名付きOSは、ソフトウェアベンダーがAXIS OSイメージを秘密鍵で署名することで実装されます。オペレーティングシステムに署名が付けられると、装置はインストール前にソフトウェアを検証するようになります。装置でソフトウェアの整合性が損なわれていることが検出された場合、AXIS OSのアップグレードは拒否されます。

セキュアブート

セキュアブートは、暗号化検証されたソフトウェアの連続したチェーンで構成される起動プロセスで、不変メモリ (ブートROM) から始まります。署名付きOSの使用に基づいているため、セキュアブートを使うと、装置は認証済みのソフトウェアを使用した場合のみ起動できます。

Axis Edge Vault

ハードウェアベースのサイバーセキュリティプラットフォーム「Axis Edge Vault」により、Axisデバイスを保護することができます。装置のIDと整合性を保証し、不正アクセスから機密情報を保護する機能を提供します。これは、エッジデバイスセキュリティに関する専門知識を駆使して、暗号コンピューティングモジュール (セキュアエレメントやTPM) とSoCセキュリティ (TEEやセキュアブート) に基づき構築された強力な基盤により成り立っています。

AxisデバイスID

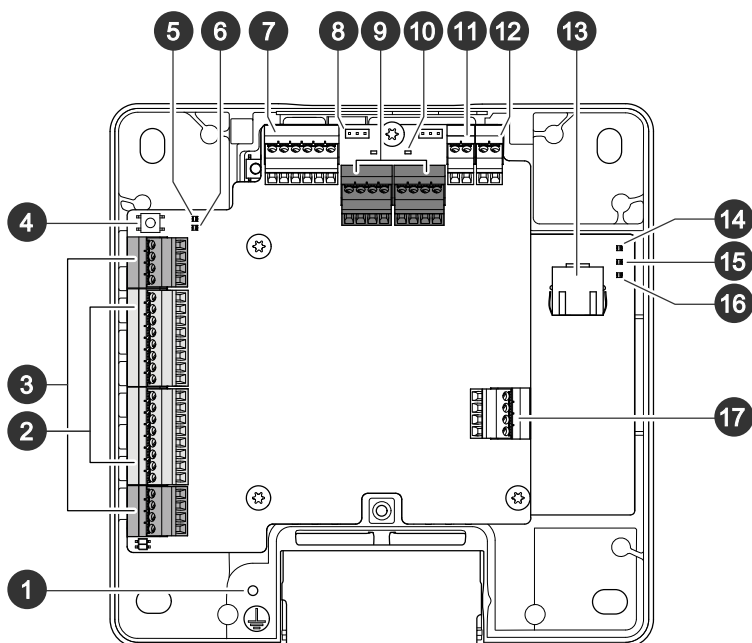
デバイスIDの信頼性を確立するには、デバイスの出所を確認できることが鍵となります。Axis Edge Vaultを搭載したデバイスには、生産工程で、工場でのプロビジョニングされ、国際規格 (IEEE 802.1AR) に準拠した一意のAxisデバイスID証明書が割り当てられます。これがデバイスの出所を証明するパスポートのような役割を果たします。デバイスIDは、Axisルート証明書により署名された証明要素として、セキュリティで保護されたキーストアに安全かつ永続的に格納されます。お客様のITインフラストラクチャーでデバイスIDを活用し、装置のセキュアな自動化オンボーディングや、装置のセキュアな識別に役立てることができます。

Axis装置のサイバーセキュリティ機能の詳細については、axis.com/learning/white-papers/にアクセスし、サイバーセキュリティを検索してください。

仕様

ULのマークが付いたテキストは、UL 294インストールでのみ有効です。

製品概要



- 1 アース位置
- 2 リーダーコネクタ、×2
- 3 ドアコネクタ、×2
- 4 コントロールボタン
- 5 リレー過電流LED
- 6 リーダー過電流LED
- 7 補助コネクタ
- 8 リレージャンパー、×2
- 9 リレーコネクタ、×2
- 10 リレーLED、×2
- 11 12Vバックアップ電源入力
- 12 電源コネクタ
- 13 ネットワークコネクタ
- 14 電源LED
- 15 ステータスLED
- 16 ネットワークLED
- 17 外部コネクタ

LEDインジケータ

| LED | カラー | 説明 |
|--------|------|---|
| ネットワーク | 緑 | 100 Mbit/sネットワークに接続している場合、点灯します。ネットワークパケットを送受信した場合、点滅します。 |
| | オレンジ | 10 Mbit/sネットワークに接続している場合、点灯します。ネットワークパケットを送受信した場合、点滅します。 |
| | 消灯 | ネットワーク接続なし。 |
| ステータス | 緑 | 正常動作であれば緑色に点灯します。 |
| | オレンジ | 起動時、設定の復元時に点灯します。 |

| | | |
|---------|------|----------------------------------|
| | 赤 | アップグレードに失敗した場合に、ゆっくり点滅します。 |
| 電源 | 緑 | 正常動作。 |
| | オレンジ | ファームウェアアップグレード中は緑とオレンジで交互に点滅します。 |
| リレー過電流 | 赤 | 短絡または過電流が検知された場合に点灯します。 |
| | 消灯 | 正常動作。 |
| リーダー過電流 | 赤 | 短絡または過電流が検知された場合に点灯します。 |
| | 消灯 | 正常動作。 |
| リレー | 緑 | リレーアクティブ。 ¹ |
| | 消灯 | リレーが無効です。 |

注

- ステータスLEDは、イベントの発生時に点滅させることができます。
- ステータスLEDを点滅させ、本製品を識別できるように設定することができます。[Setup > Additional Controller Configuration > System Options > Maintenance (設定 > 追加のコントローラー設定 > システムオプション > メンテナンス)]に移動します。

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する, on page 17を参照してください。

コネクタ

ネットワーク コネクタ

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

UL : Power over Ethernet (PoE) は、44~57 V DC、15.4 W/30 Wを提供できるUL 294認定Power over Ethernet IEEE 802.3af/802.3at Type 1 Class 3、またはPower over Ethernet Plus (PoE+) IEEE 802.3at Type 2 Class 4有限電源インジェクタによって供給される必要があります。Power over Ethernet (PoE) は、AXIS T8133 Midspan 30 W 1-portが搭載されたULによって評価されています。

電源の優先順位

本装置は、PoEまたはDC入力から電源を供給できます。「ネットワーク コネクタ, on page 10」および「電源コネクタ, on page 15」を参照してください。

- 装置に電源が供給されていない状態でPoEとDCの両方を接続すると、PoEが電源供給に使用されます。
- PoEとDCの両方が接続されており、現在はPoEが電源を供給しています。PoEが失われた場合、本装置は再起動せずにDCを使用して電源を供給します。
- PoEとDCの両方が接続されており、現在はDCが電源を供給しています。DCが失われた場合、本装置は再起動し、PoEを使用して電源を供給します。
- 起動時にDCが使用されている場合、装置の起動後にPoEが接続されても、電源供給にDCが使用されます。

1. リレーが有効です。COMがNOに接続すると、リレーが有効になります。

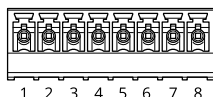
- 起動時にPoEが使用されている場合、装置の起動後にDCが接続されても、電源供給にPoEが使用されません。

リーダーコネクタ

リーダーとの通信用のRS485およびWiegandの両プロトコルに対応する8ピンターミナルブロック×2。

指定の電源出力値は、2つのリーダーポート間で共有されます。つまり、ドアコントローラーに接続されるすべてのリーダー向けに12 V DC、500 mAが供給されます。

製品のWebページで使用するプロトコルを選択します。



RS485の設定

| 機能 | ピン | 注 | 仕様 |
|----------------|-----|---|--------------------------------|
| DCアース (GND) | 1 | | 0 V DC |
| DC出力 (+12 V) | 2 | リーダーに電源を供給します。 | すべてのリーダーに合わせて12 V DC、最大500 mA |
| RX/TX | 3-4 | 全二重：RX。半二重：RX/TX。 | |
| TX | 5-6 | 全二重：TX。 | |
| 設定可能 (入力または出力) | 7-8 | 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 V DC |
| | | デジタル出力 - 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。 | 0~30 V DC (最大)、オープンドレイン、100 mA |

重要

- コントローラーからリーダーに電力を供給する場合、適格なケーブル長は最大200 mです。
- コントローラー経由でリーダーが給電されていない状況下では、シールド付きツイストペア1本、AWG 20-16というケーブル要件が満たされている場合、リーダーデータの適格なケーブル長は最大1000 m (3280.8フィート) となります。

Wiegandの設定

| 機能 | ピン | 注 | 仕様 |
|--------------|----|----------------|-------------------------------|
| DCアース (GND) | 1 | | 0 V DC |
| DC出力 (+12 V) | 2 | リーダーに電源を供給します。 | すべてのリーダーに合わせて12 V DC、最大500 mA |
| D0 | 3 | | |

| | | | |
|----------------|-----|---|--|
| D1 | 4 | | |
| O | 5-6 | デジタル出力、オープンドレイン | |
| 設定可能 (入力または出力) | 7-8 | 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 V DC |
| | | デジタル出力 - 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。 | 0~30 V DC (最大)、 オープンドレイン、 100 mA |

重要

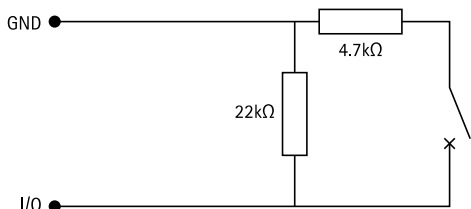
- ・ コントローラーからリーダーに電力を供給する場合、適格なケーブル長は最大150 mです。
- ・ コントローラー経由でリーダーが給電されていない状況下では、AWG 20-16というケーブル要件が満たされている場合、リーダーデータの適格なケーブル長は最大150 m (500 フィート) となります。

監視入力

状態監視入力を使用するには、下図に従って終端抵抗器を設置します。

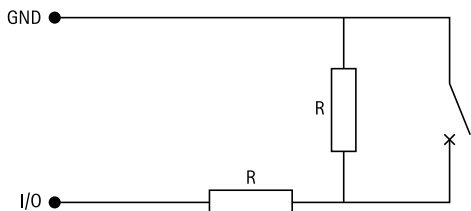
パラレルファースト接続

抵抗器の値は 4.7 kΩ及び 22 kΩである必要があります。



最初の直列接続

抵抗器の値は同じで、可能な値は1 kΩ、2.2 kΩ、4.7 kΩ、10 kΩです。



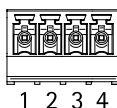
注

シールド付きツイストケーブルを使用することをお勧めします。シールドを0 V DCに接続します。

ドアコネクタ

ドア監視デバイス用4ピンターミナルブロック (×2) (デジタル入力)。

ドアモニターは終端抵抗器を使用した監視に対応しています。接続が中断されると、アラームがトリガーされます。状態監視入力を使用するには、終端抵抗器を設置します。状態監視入力の接続図を使用します。監視入力, on page 12を参照してください。



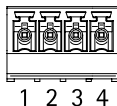
| 機能 | ピン | メモ | 仕様 |
|-------|------|---|----------------|
| DCアース | 1, 3 | | 0 V DC |
| 入力 | 2, 4 | ドアモニターとの通信対象。デジタル入力/状態監視入力 - 有効にするにはピン1または3にそれぞれ接続し、無効にする場合はフロート状態 (未接続) のままにします。 | 0~30 V DC (最大) |

重要

AWG 24のケーブル要件を満たす場合、ケーブルの長さは最大200 m (656フィート) です。

リレーコネクタ

ロックやゲートのインターフェースをコントロールするなど利用可能なForm Cリレー用4ピンのターミナルブロック×2。



| 機能 | ピン | メモ | 仕様 |
|-------------|----|---|-----------------------------------|
| DCアース (GND) | 1 | | 0 V DC |
| NO | 2 | Normally Open。 リレー装置の接続用。NOとDCアースの間にフェイルセキュアロックを接続します。 ジャンパーが使用されていない場合、2つのリレーピンは回路の残りの部分から電気的に分離されています。 | 最大電流 = リレーあたり2 A 最大電圧 = 30V DC |
| COM | 3 | コモン | |
| NC | 4 | Normally Closed。 リレー装置の接続用。NCとDCアースの間にフェイルセーフロックを接続します。 ジャンパーが使用されていない場合、2つのリレーピンは回路の残りの部分から電気的に分離されています。 | |

リレー電源ジャンパー

リレー電源ジャンパーが取り付けられている場合、12 V DCまたは24 V DCをリレーCOMにピンに接続します。

これはGNDピンとNOピン間、もしくはGNDピンとNCピン間のロックに接続するために使用できません。

| | | |
|------|----------------------------|----------------------------|
| 電源 | 12 V DCでの最大電力 ² | 24 V DCでの最大電力 ² |
| DC入力 | 1 800 mA | 750 mA |
| PoE | 900 mA | 410 mA |

注意

ロックに極性がない場合は、外部フライバックダイオードを追加することをお勧めします。

補助コネクタ

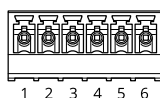
補助コネクタに外部装置を接続し、動体検知、イベントトリガー、アラーム通知などと組み合わせて使用することができます。補助コネクタは、0 V DC基準点と電力 (DC出力) に加えて、以下へのインターフェースを提供します。

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。

状態監視入力 - デジタル入力のいたづらを検知する機能が有効になります。

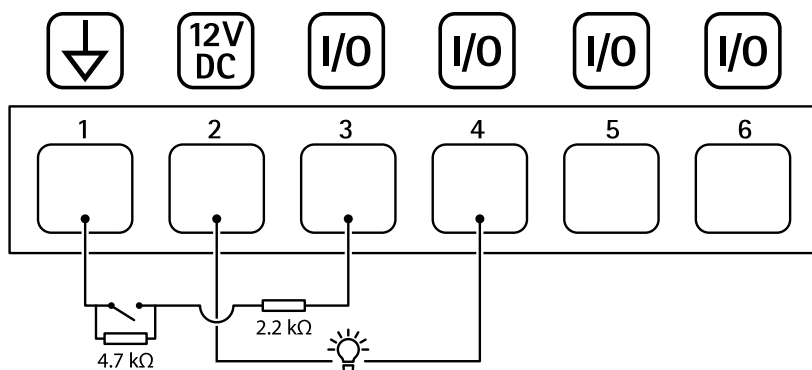
デジタル出力 - リレーやLEDなどの外部装置を接続します。接続された装置は、VAPIX®アプリケーションプログラミングインターフェースまたは製品のWebページから起動できます。

6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 |
| DC出力 | 2 | 補助装置の電源供給に使用できます。 注:このピンは電源をリレーと共有しているため、安全な側で電源出力としてのみ使用できます。 | 12 V DC 最大負荷 = I/Oあたり 50 mA |
| 設定可能 (入力または出力) | 3-6 | デジタル入力/状態監視 - 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。状態監視を使用するには、終端抵抗器を設置します。抵抗器を接続する方法については、接続図を参照してください。 | 0~30 V DC (最大) |
| | | 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。内部 12 V DC出力 (ピン2) が使用されている場合、各I/Oは12 V DC、50 mA (最大) の外部負荷に電源を供給できます。オープンドレイン接続を外部電源と組み合わせて使用する場合、I/Oは0~30 V DC、100 mAのDC給電を管理できます。 | 0~30 V DC (最大)、 オープンドレイン、 100 mA |

2. 電源は2つのリレーとAUX I/O 12 V DCとの間で共有されます。

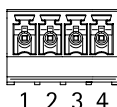


- 1 DCアース
- 2 DC出力12 V、最大50 mA
- 3 I/O (状態監視として設定)
- 4 I/O (出力として設定)
- 5 設定可能I/O
- 6 設定可能I/O

外部コネクタ

ガラスの破壊検知や火災検知などの外部デバイスで使用する4ピンターミナルブロックです。

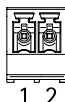
UL：このコネクタは、盗難/火災警報用途向けとしてはULによって評価されていません。



| 機能 | ピン | メモ | 仕様 |
|----------------|------|--|--------------------------------|
| DCアース | 1, 3 | | 0 V DC |
| 設定可能 (入力または出力) | 2, 4 | デジタル入力 - 動作させるにはピン1または3に接続し、動作させない場合はフロート状態 (未接続) のままにします。 | 0~30 V DC (最大) |
| | | デジタル出力 - 動作させるにはピン1または3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。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 V DC (最大)、オープンドレイン、100 mA |

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 |
|------------|----|---|---------------------|
| 0 V DC (-) | 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。 | 10.5~28 V DC、最大36 W |

UL：アプリケーションに応じて適切な定格で、UL 294、UL 293、またはUL 603の認定を受けた電源によって供給されるDC電源。

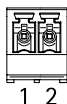
12 Vバックアップ電源入力

内蔵チャージャー付きバッテリーを使用するバックアップソリューション用です。12 V DC入力。

UL：このコネクタはULによって評価されていません。

重要

バッテリーの入力を使用する場合、外部3 Aスローブローフューズを直列に接続する必要があります。



| 機能 | ピン | メモ | 仕様 |
|------------|----|--|---------------------|
| 0 V DC (-) | 1 | | 0 V DC |
| バッテリーの入力 | 2 | 他の電源が利用できないときのドアコントローラーへの電力供給用です。 注:このピンは、バッテリー電源入力としてのみ使用できます。UPSへの接続専用です。 | 11~13.7 V DC、最大36 W |

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 9を参照してください。
3. ステータスLEDが再びオレンジ色に変わるまで、コントロールボタンを押し続けます (25秒間)。
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、製品へのアクセスを行います。

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 Portal: 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。
 - データベースのユーザーやグループ、認証情報、その他のデータの更新は、AXIS OSのアップグレード後に行われるため、最初の起動が完了するまで数分かかることがあります。必要な時間はデータの量によって異なります。
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。

4. 製品の再起動後、Webブラウザのキャッシュをクリアします。

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...という応答を受取った場合は、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、AxisデバイスでそのIPアドレスを使用できません。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する, *on page 17*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

推奨ブラウザの一覧は、[ブラウザーサポート](#), *on page 4*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、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 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/vmsl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、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。

デバイスの動作に関する問題

フロントヒーターとワイパーが作動していない

フロントヒーターまたはワイパーがオンにならない場合は、上部カバーがハウジングユニットの底部に正しく固定されているか確認してください。

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。

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。

T10181936_ja

2026-04 (M11.2)

© 2022 – 2026 Axis Communications AB