AXIS TP3604-E Cellular Back Box

ユーザーマニュアル

目次

インストール....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します。....4
安全なパスワード....4
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
デバイスを構成する....6
SIMの管理....6
APNを設定する....6
信号強度とIPアドレスを検証する....6
接続をテストする....6
管理ポートを確認する....7
カメラへの転送をオンにする....7
カメラのIP所持者を設定する....7
Local (ローカル) モード....8
Passthrough (パススルー) モード....8
イベントのルールを設定する....9
アクションをトリガーする....9
エンクロージャが開かれたときに通知をトリガーする....9
webインターフェース....11
仕様....12
製品概要....12
LEDインジケーター....12
ボタン....13
コントロールボタン....13
コネクター....13
PoE入力コネクター (PoE入力)....13
ネットワークコネクター (PoE出力)....13
電源コネクター....13
装置を清掃する....14
トラブルシューティング....15
工場出荷時の設定にリセットします。....15
AXIS OSのオプション....15
AXIS OSの現在のバージョンを確認する....15
AXIS OSをアップグレードする....16
技術的な問題と解決策....16
サポートに問い合わせる....18
サイバーセキュリティ....19
脆弱性の管理....19
セキュリティ通知....19
安全な製品ライフサイクル管理....19

インストール



このビデオでは、AXIS TP3604-E Cellular Back Boxを、AXIS P32 Dome Camera SeriesおよびAXIS P14 Bullet Camera Seriesと組み合わせて設置する方法を紹介しています。

すべての設置シナリオに対応する手順および安全に関する情報については、インストールガイドを参照ください。

使用に当たって

ネットワーク上のデバイスを検索する

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

ブラウザーサポート

以下のブラウザーでデバイスを使用できます。

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

✓:推奨

*:制限付きでサポート

装置のwebインターフェースを開く

1. ユーザー名とパスワードを入力します。装置に初めてアクセスする場合は、管理者アカウントを作成する必要があります。*管理者アカウントを作成します。, on page 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 4*を参照してください。
3. パスワードを再入力します。
4. 使用許諾契約書に同意します。
5. [Add account (アカウントを追加)] をクリックします。

安全なパスワード

重要

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

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

データを保護するために、次のことが強く推奨されています。

- 8文字以上のパスワードを使用する (できればパスワード生成プログラムで作成する)。

- パスワードを公開しない。
- 一定の期間ごとにパスワードを変更する (少なくとも年に1回)。

デバイス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. 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

デバイスを設定するには、以下の手順を従います。

1. *SIMの管理, on page 6*
2. お使いのネットワークで明示的なアクセスポイント名 (APN) が必要な場合は、*APNを設定する, on page 6*
3. *信号強度とIPアドレスを検証する, on page 6*
4. *接続をテストする, on page 6*
5. *管理ポートを確認する, on page 7*
6. *カメラへの転送をオンにする, on page 7*

SIMの管理

SIM PINが有効になっている場合、SIMの管理が必須です。SIM PINが無効になっている場合は、この手順をスキップできます。

1. SIMカードを挿入します。**[Modem (モデム)] > [SIM management (SIMの管理)] > SIM status(SIMステータス)** に移動し、モデム/SIMカードの検知を確認します。
2. SIM PINがロックされている場合は、**[Modem (モデム)] > [SIM management (SIMの管理)] > [SIM PIN] > [Unlock (ロック解除)]** に移動し、正しいPINを入力してロックを解除します。

APNを設定する

注
ネットワークで明示的なAPN (アクセスポイント名) が必要な場合にのみ、この手順を実行してください。

APNを明示的に設定するには、**[Modem (モデム)] > [Cellular network (セルラーネットワーク)] > [APN]** に移動します。

信号強度とIPアドレスを検証する

注
この手順では、セルラーネットワークへのアクセスが必要です。

1. **[System (システム)] > [Modem (モデム)] > [Cellular network (セルラーネットワーク)] > [Radio parameters (無線パラメータ)] > [Signal strength index (信号強度指数)]** で信号強度を確認します。3〜4本のバーが表示されている場合は、電波の状態が良好であることを示しています。
2. **[System (システム)] > [Modem (モデム)] > [Cellular network (セルラーネットワーク)] > [User equipment IP address (ユーザー機器IPアドレス)]** で、セルラーネットワークIPアドレスが取得されていることを確認します。

接続をテストする

注
この手順では、セルラーネットワークへのアクセスが必要です。

1. **[System (システム)] > [Modem (モデム)] > [Cellular network (セルラーネットワーク)] > [Test cellular connection (セルラー接続のテスト)]** に移動します。ホスト名またはIPアドレスを入力します。
2. 接続テストが正常に完了したことを確認します。

管理ポートを確認する

最終的なルーティングモードをオンにする前に、バックボックスの管理ポートを確認します。

1. [Cellular routing (セルラールーティング)] > [Back box management ports (バックボックス管理ポート)] に移動します。
2. ネットワークでデフォルト値がサポートされていない場合は、ポートを変更します。

カメラへの転送をオンにする

最後にカメラへの転送をオンにします。

1. [Cellular routing (セルラールーティング)] > [Main mode (メインモード)] に移動し、[Enable forwarding to connected device (接続されたデバイスへの転送を有効にする)] をクリックします。

転送を有効にすると、通常のサービスポートがカメラに転送され、バックボックス管理は引き続き予備の管理ポートから利用できます。

2. 以下の手順でカメラへのアクセスをテストします。Webブラウザーに、セルラーIPアドレスを入力し、続けてポート番号80、`http://<cellular-ip-address>:80`を入力します。
3. 以下の手順でバックボックスへのアクセスをテストします。 Webブラウザーに、セルラーIPアドレスを入力し、続けてポート番号11080 (HTTP用のデフォルトのバックボックス管理ポート)、`http://<cellular-ip-address>:11080`を入力します。

カメラのIP所持者を設定する

注

この手順は任意であり、デフォルトのサブネットの挙動を変更したり、サブネットの挙動を調整したりする必要がある場合のみ必要です。

セルラーネットワークは、IPアドレスを1つのみ割り当てます。そのIPアドレスはSIMカードのIDと紐付けられています。通常のインストールには、バックボックスと接続されたカメラが含まれます。DHCPモードによって、カメラが「所持」するIPアドレスが決定されます。これはDHCPサーバーモードの選択に関わる重要な決定です。

デフォルト (Local (ローカル) モード) では、セルラーIPはバックボックスに割り当てられたままとなり、カメラにはバックボックスのローカルネットワークからプライベートIPが割り当てられます。それでも、カメラにはセルラーネットワークからフルにアクセスできます。ほとんどの導入環境においてはこれで十分で、カメラはプライベートネットワーク上で安全に隔離された状態で維持されます。

違いが明らかになるのは、ツールがカメラ側の視点からIPを確認する場合です。VMSがカメラから報告されたIPアドレスを読み取る場合、または、カメラがそのIPアドレスをビデオオーバーレイに書き込むように設定されている場合、そのIPアドレスは、外部からカメラにアクセスするために使用されるパブリックなセルラーIPではなく、カメラのプライベートLAN IPとなります。この2つのIPアドレスは、セルラーIPがカメラではなくバックボックスが保持するSIMカードIDに紐づけられているため一致しません。

Passthrough (パススルー) モードでは、セルラーネットワークがバックボックスに割り当てる1つのIPアドレスをカメラに転送することで、この問題を解決します。パススルーを有効にすると、カメラはセルラーネットワークに属するIPアドレスとまったく同じIPアドレスを所持するため、カメラが報告するアドレス (およびビデオオーバーレイに表示されるアドレス) は、リモートからカメラにアクセスする際に使用されるアドレスと同じになります。するとカメラがセルラーIDを保持するようになるため、この選択によって、カメラがセルラーネットワーク上の他のユーザー機器 (UE) にアクセスする方法も変更されます。

このセクションの残りで、各モードの詳細を説明します。

バックボックスに接続されているカメラには、標準ポートでセルラーIP (80/443/554/22) によってアクセスできます。この場合も、バックボックスには予備の管理ポート (例: 11080/11443/11554/11022) でアクセスできます。

Local (ローカル) モードとPassthrough (パススルー) モードの違い:

Local (ローカル) モード

- カメラには、プライベートローカルサブネットが割り当てられます。
- カメラの内部IPアドレスは、セルラーネットワークからアクセス可能なIPアドレスとは異なります。
- 迷った場合は、Local DHCP (ローカルDHCP) モードオプションを使用してください。

Passthrough (パススルー) モード

- カメラには、セルラーIPアドレスが割り当てられます。

Local (ローカル) モード

Local (ローカル) モードをオンにする

1. [Cellular routing (セルラールーティング)] > [Advanced DHCP configuration (詳細DHCP設定)] > [DHCP server mode (DHCPサーバーモード)] で、[Local (ローカル)] を選択します。
2. [Cellular routing (セルラールーティング)] > [Advanced DHCP configuration (詳細DHCP設定)] > [Local private network configuration (ローカルプライベートネットワーク設定)] で、カメラのローカルIPアドレスが、ネットワークの他の到達可能なIPアドレスと競合していないことを確認します。
3. 必要に応じて、[Cellular routing (セルラールーティング)] > [Advanced DHCP configuration (詳細DHCP設定)] > [Local private network configuration (ローカルプライベートネットワーク設定)] でIPアドレスを変更します。[Starting IP address (開始IPアドレス)] と [Ending IP address (終了IPアドレス)] に同じ値を使用します。
4. [Save (保存)] をクリックします。

Passthrough (パススルー) モード

UE (ユーザー機器、この場合はカメラ) が互いに通信を行わず、トラフィックが常に別のVMS LANからUEに入ってくる場合、IPシャドウイングのためのUE間経路が存在しません。その場合、IPシャドウイングの観点からは、Passthrough (パススルー) が安全であるとみなされます。

大まかには、セルラーネットワークがカメラ側に拡張されることを意味します。これは、カメラがセルラー側のIPアドレスで直接表示される必要がある場合に役立ちます。

重大なリスク: Passthrough (パススルー) におけるIPシャドウイング

このリスクの説明は、シングルカメラの設定に適用されます。カメラが1台でも、Passthrough (パススルー) はLAN側のサブネット上で以下の2つのIPアドレスを必要とします。

- カメラ用のIPアドレス1つ。
- イーサネット側のバックボックスDHCPサーバー用のIPアドレス1つ。

シナリオ 1: UEごとの最小サブネット (/30)

このモデルでは、各UEに、個別のサブネットが割り当てられます。

- (/30) は、2つの利用可能なホストIPアドレスを提供します。
- 1つのIPアドレスがカメラに使用されます。

予備のIPアドレスがバックボックスDHCPサーバーによって内部で使用されます。

シナリオ1に関する推奨事項:

- 各UEのサブネットを別々にしてください。
- すべてのUEサブネットが一意であることを確認してください。 UE間でサブネットが重複しないようにしてください。

シナリオ 2: 多数のUEが存在する大きな共有サブネット

導入環境によっては、複数のUEに共有される1つの大きなサブネットを使用する場合があります。バックボックスDHCPサーバーと同じIPアドレスを使用する別のUEにカメラが接続しようとすると、シャドウイングのリスクが生じます。その場合、トラフィックは、本来接続すべき遠隔のUEではなく、ローカルのバックボックス側のアドレスに解決される可能性があります。

シナリオ2に関する推奨事項:

- パススルー設定で、バックボックスDHCPサーバーのIPアドレスを確認してください。
- このIPアドレスが他のUEに割り当てられていないことを確認してください。
- このIPアドレスがネットワークサービスポータルでいずれのSIMカードにも割り当てられていないことを確認してください。

Passthrough (パススルー) モードをオンにする

注

セルラーネットワークへのアクセスが必要です。

1. [Cellular routing (セルラールーティング)] > [Advanced DHCP configuration (詳細DHCP設定)] > [DHCP server mode (DHCPサーバーモード)] で、[Passthrough (パススルー)] を選択します。
2. [Cellular routing (セルラールーティング)] > [Advanced DHCP configuration (詳細DHCP設定)] > [Local private network configuration (ローカルプライベートネットワーク設定)] > [Server IP and prefix length (サーバーIPおよびプレフィックス長)] で、自動的に選択されたサーバーIPおよびサブネットプレフィックス長が、他の到達可能なIPアドレスと競合していないことを検証します。
3. [Save (保存)] をクリックします。

イベントのルールを設定する

詳細については、「*イベントのルールの使用開始*」を参照してください。

アクションをトリガーする

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

エンクロージャが開かれたときに通知をトリガーする

この例では、デバイスのハウジングまたはケーシングが開けられたときの電子メール通知を設定する方法を説明します。

メール送信先を追加する:

1. [System (システム)] > [Events (イベント)] > [Recipients (送信先)] に移動し、[Add recipient (送信先の追加)] をクリックします。
2. 送信先の名前を入力します。

3. 通知方法として**電子メール**を選択します。
4. 送信先の電子メールアドレスを入力します。
5. カメラが通知を送信する電子メールアドレスを入力します。
6. 送信電子メールアカウントのログイン詳細、SMTP ホスト名、ポート番号を指定します。
7. 電子メールの設定をテストするには、**テスト** をクリックします。
8. **[Save (保存)]** をクリックします。

ルールの作成:

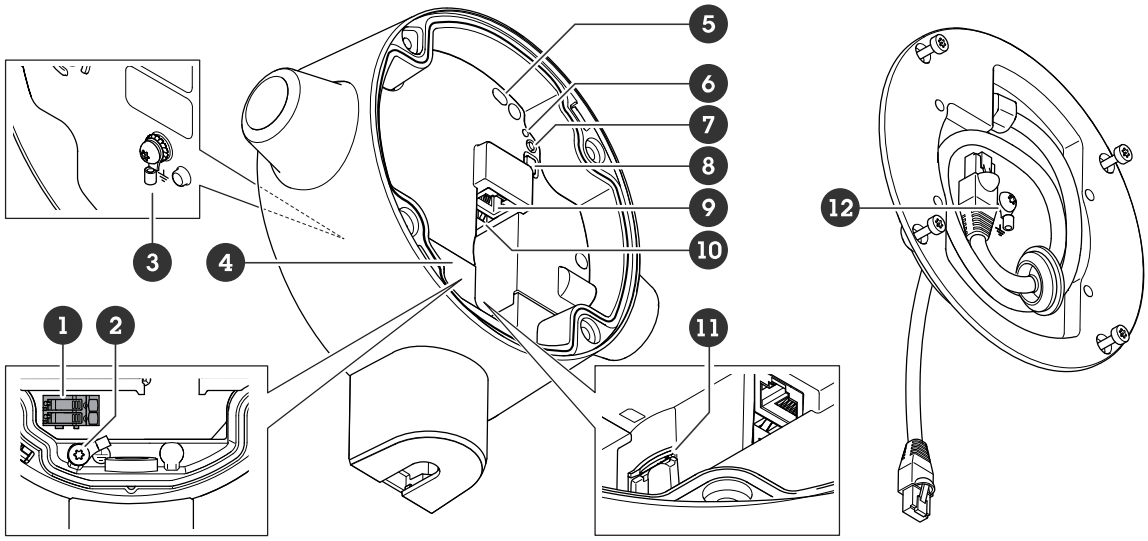
9. [**System > Events > Rules (システム > イベント > ルール)**] に移動し、[**Add a rule (ルールの追加)**] をクリックします。
10. ルールの名前を入力します。
11. 条件のリストで、[**Casing open (ケーシング開放)**] を選択します。
12. アクションのリストで、[**Send notification to email (電子メールに通知を送信する)**] を選択します。
13. リストから送信先を選択します。
14. 電子メールの件名ラインとメッセージを入力します。
15. **[Save (保存)]** 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。

仕様

製品概要



1 ACコネクタ。
2 保護アース
3 アース端子ネジ
4 保護カバー (AC)
5 ケース開放検知器
6 リセットボタン
7 ステータスLED
8 コントロールボタン
9 PoE出力 (データ)
10 PoE入力
11 SIMカードスロット
12 アーススクリュー (カメラ)

LEDインジケーター

設定モードのステータスLED

ステータスLED	説明
消灯	ケーシング検知IRセンサーが覆われています。
緑	正常に動作しており、イーサネットインターフェースは利用可能です。
黄色	起動時に点灯。装置のソフトウェアのアップグレード中、または工場出荷時の設定にリセット中に点滅します。
オレンジ/赤	イーサネットが接続しておらず、起動中にモデムが設定されています。
赤	装置のソフトウェアのアップグレードに失敗しました。

接続モードのステータスLED

ステータスLED	説明
消灯	ケーシング検知IRセンサーが覆われています。
緑	モデムはネットワークに接続されています。

黄色	起動時に点灯。装置のソフトウェアのアップグレード中、または工場出荷時の設定にリセット中に点滅します。
オレンジ/赤	起動中にモデムの設定が行われています。
赤	装置のソフトウェアのアップグレードに失敗しました。

ボタン

コントロールボタン

コントロールボタンは、以下の用途で使用します。

- 製品を工場出荷時の設定にリセットする。*工場出荷時の設定にリセットします。, on page 15*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

PoE入力コネクター (PoE入力)

RJ45イーサネットコネクター、Power over Ethernet (PoE) IEEE 802.3af/802.3at/802.3bt Type 3 Class 5.

注

このコネクターは電源入力専用です。ネットワーク接続は利用できません。

注

- PoE IEEE 802.3at Type 2 Class 4出力には、AC入力が必要です。
- PoE IEEE 802.3af Type 1 Class 3出力には、IEEE 802.3at Type 2 Class 4以上が必要です。
- PoE IEEE 802.3af Type 1 Class 3入力の場合、デバイスは動作していますが出力しません。

注

イーサネットケーブルの最大長は20 mです。

ネットワークコネクター (PoE出力)

RJ45イーサネットコネクタ。

注

- PoE IEEE 802.3at Type 2 Class 4出力には、AC入力が必要です。
- PoE IEEE 802.3af Type 1 Class 3出力には、IEEE 802.3at Type 2 Class 4以上が必要です。
- PoE IEEE 802.3af Type 1 Class 3入力の場合、デバイスは動作していますが出力しません。

注

イーサネットケーブルの最大長は20 mです。

電源コネクター

AC電源を接続するためのターミナルブロック。

注

PoE IEEE 802.3at Type 2 Class 4出力には、AC入力が必要です。

装置を清掃する

装置はぬるま湯と低刺激、非研磨性の石鹸で洗浄できます。

注意

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

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

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

トラブルシューティング

工場出荷時の設定にリセットします。

重要

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

本製品を工場出荷時の設定にリセットするには、以下の手順に従います。

1. 本製品の電源を切ります。
2. コントロールボタンを押した状態で電源を再接続します。*製品概要, on page 12*を参照してください。
3. ステータスLEDインジケーターがオレンジで点滅するまでコントロールボタンを15〜30秒間押し続けます。
4. コントロールボタンを放します。プロセスが完了すると、ステータスLEDが緑色に変わります。ネットワーク上にDHCPサーバーがない場合、装置IPアドレスは以下のいずれかにデフォルト設定されます。
   - **AXIS OS 12.0 以降を搭載したデバイス:** リンクローカルアドレスサブネット (169.254.0.0/16) から取得
   - **AXIS OS 11.11以前の装置：**192.168.0.90/24
5. インストールおよび管理ソフトウェアツールを使用して、IPアドレスの割り当て、パスワードの設定、装置へのアクセスを行います。
   *axis.com/support*のサポートページに、インストールおよび管理ソフトウェアツールが用意されています。

装置のwebインターフェースを使用して、各種パラメーターを工場出荷時の設定に戻すこともできます。[**Maintenance (メンテナンス)** > **Factory default (工場出荷時の設定)**] に移動し、[**Default (デフォルト)**] をクリックします。

AXIS OSのオプション

Axisは、アクティブトラックまたは長期サポート (LTS) トラックのどちらかに従って、装置のソフトウェアの管理を提供します。アクティブトラックでは、最新の製品機能すべてに常時アクセスできますが、LTSトラックの場合、バグフィックスやセキュリティ更新に重点を置いた定期的リリースが提供される固定プラットフォームを使用します。

最新の機能にアクセスする場合や、Axisのエンドツーエンドシステム製品を使用する場合は、アクティブトラックのAXIS OSを使用することをお勧めします。最新のアクティブトラックに対して継続的な検証が行われないサードパーティの統合を使用する場合は、LTSトラックをお勧めします。LTSにより、大きな機能的な変更や既存の統合に影響を与えることなく、サイバーセキュリティを維持することができます。Axis装置のソフトウェア戦略の詳細については、*axis.com/support/device-software*にアクセスしてください。

AXIS OSの現在のバージョンを確認する

装置の機能はAXIS OSによって決まります。問題のトラブルシューティングを行う際は、まずAXIS OSの現在のバージョンを確認することをお勧めします。最新バージョンには、特定の問題の修正が含まれていることがあります。

AXIS OSの現在のバージョンを確認するには:

1. 装置のwebインターフェース > [**Status (ステータス)**] に移動します。
2. [**Device info (デバイス情報)**] で、AXIS OSのバージョンを確認します。

AXIS OSをアップグレードする

重要

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

注

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

1. AXIS OSのファイルをコンピューターにダウンロードします。これらのファイルは*axis.com/support/device-software*から無料で入手できます。
2. デバイスに管理者としてログインします。
3. [Maintenance (メンテナンス)] >[AXIS OS upgrade (AXIS OSのアップグレード)] に移動し、[Upgrade (アップグレード)] をクリックします。

アップグレードが完了すると、製品は自動的に再起動します。

技術的な問題と解決策

AXIS OSのアップグレード時の問題

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

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

IPアドレスの設定で問題が発生する

IPアドレスを設定できない

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

デバイスへのアクセスの問題

ブラウザからデバイスにアクセスする際、ログインできない

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

rootアカウントのパスワードを忘れた場合は、デバイスを工場出荷時の設定にリセットする必要があります。手順については、*工場出荷時の設定にリセットします。, on page 15*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 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、基本的な監視ニーズがある小規模システムに最適です。
- AXIS Camera Station Pro:90日間の試用版を無料で使用でき、中小規模のシステムに最適です。

手順とダウンロードについては、*axis.com/vms*にアクセスしてください。

MQTTの問題

MQTTオーバSSLを使用してポート8883経由で接続できない

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

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

- サーバー/ブローカーが、通常はポート443経由で、WebSocket/WebSocket Secure (WS/WSS) をサポートしている場合は、代わりにこのプロトコルを使用してください。サーバー/ブローカープロバイダーに問い合わせて、WS/WSSがサポートされているかどうか、どのポートと基本パスを使用するかを確認してください。
- サーバー/ブローカーがALPNをサポートしている場合、MQTTの使用は443などのオープンポートでネゴシエートできます。ALPNのサポートの有無、使用するALPNプロトコルとポートについては、サーバー/ブローカーのプロバイダーに確認してください。

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

サ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。

T10233346_ja

2026-10 (M2.2)

© 2026 Axis Communications AB