

## **AXIS A1610 Network Door Controller**

**ユーザーマニュアル**

# AXIS A1610 Network Door Controller

## 目次

---

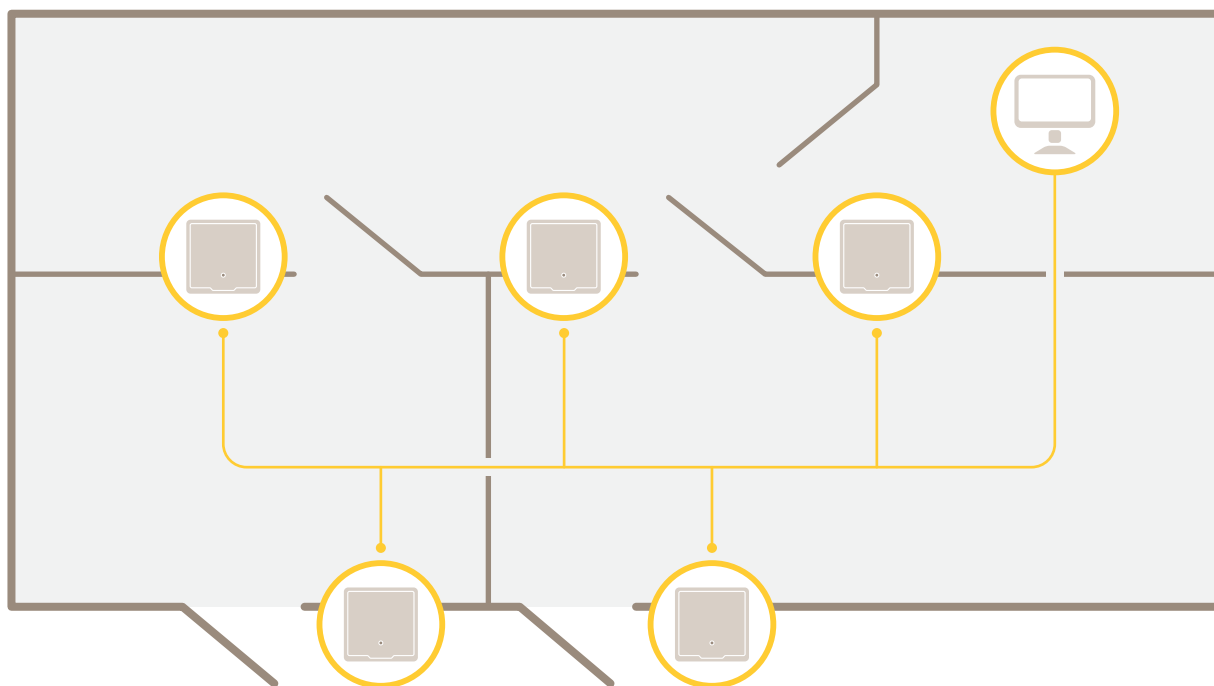
ソリューションの概要	3
はじめに	5
ネットワーク上のデバイスを検索する	5
装置のwebインターフェースを開く	5
管理者アカウントを作成する	5
安全なパスワード	6
装置のソフトウェアが改ざんされていないことを確認する	6
webインターフェースの概要	6
デバイスを構成する	7
webインターフェース	8
ステータス	8
アクセスコントロール	9
システム	9
保守	22
詳細情報	23
サイバーセキュリティ	23
仕様	24
製品の概要	24
LEDインジケータ	24
ボタン	25
コネクタ	25
トラブルシューティング	32
工場出荷時の設定にリセットする	32
AXIS OSのオプション	32
AXIS OSの現在のバージョンを確認する	32
AXIS OSをアップグレードする	32
技術的な問題、ヒント、解決策	33
パフォーマンスに関する一般的な検討事項	35
サポートに連絡する	35

# AXIS A1610 Network Door Controller

## ソリューションの概要

---

### ソリューションの概要

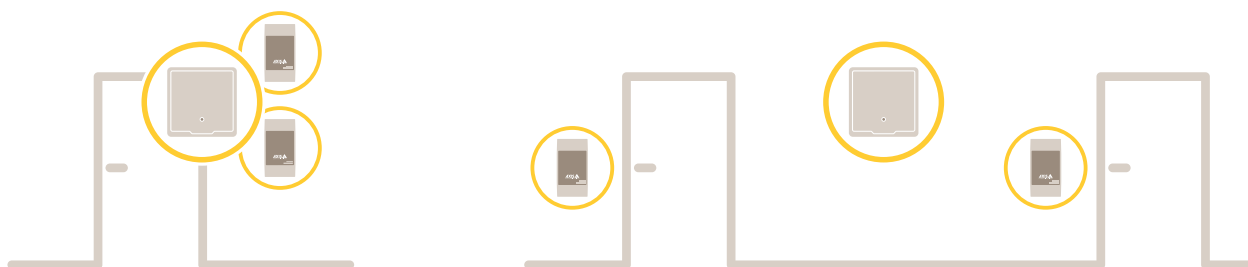


ネットワークドアコントローラーは、既存のIPネットワークに容易に接続して給電することができ、特殊な配線は必要ありません。

# AXIS A1610 Network Door Controller

## ソリューションの概要

---



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2つのリーダーに給電したり制御したりできます。

# AXIS A1610 Network Door Controller

## はじめに

### はじめに

### ネットワーク上のデバイスを検索する

Windows®でAxisデバイスを探してIPアドレスの割り当てを行う方法については、AXIS IP UtilityまたはAXIS Device Managerを使用してください。いずれのアプリケーションも無料で、[axis.com/support](http://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。

### ブラウザサポート

以下のブラウザで装置を使用できます。

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

\* iOS 15またはiPadOS 15でAXIS OS webインターフェースを使用するには、[\[設定\] > \[Safari\] > \[詳細\] > \[Experimental Features\]](#) に移動し、[\[NSURLSession Websocket\]](#) を無効にします。

推奨ブラウザの詳細については、[AXIS OSポータル](#)にアクセスしてください。

### 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 IP UtilityまたはAXIS Device Managerを使用して、ネットワーク上で装置を見つけます。

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。 [5 ページ管理者アカウントを作成する](#)を参照してください。

装置のwebインターフェースにあるすべてのコントロールとオプションの説明については、 [8 ページ、webインターフェース](#)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ます。
2. パスワードを入力します。 [6 ページ安全なパスワード](#)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。

# AXIS A1610 Network Door Controller

## はじめに

---

### 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。32ページ工場出荷時の設定にリセットするを参照してください。

## 安全なパスワード

### 重要

Axisデバイスは、最初に設定されたパスワードをネットワーク上で平文で送信します。最初のログイン後にデバイスを保護するために、安全で暗号化されたHTTPS接続を設定してからパスワードを変更してください。

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される可能性があることから、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、次のことを強く推奨します。

- 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)。

## 装置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。32ページ工場出荷時の設定にリセットする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。



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。

[help.axis.com/?&piald=81253&section=web-interface-overview](http://help.axis.com/?&piald=81253&section=web-interface-overview)

Axis装置のwebインターフェース

# AXIS A1610 Network Door Controller

## デバイスを構成する

---

### 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 A1610 Network Door Controller












## webインターフェース

### webインターフェース

装置のwebインターフェースにアクセスするには、Webブラウザで装置のIPアドレスを入力します。

注

このセクションで説明する機能と設定のサポートは、装置によって異なります。このアイコン  は、機能または設定が一部の装置でのみ使用できることを示しています。

-  メインメニューの表示/非表示を切り取ります。
-  リリースノートにアクセスします。
-  製品のヘルプにアクセスします。
-  言語を変更します。
-  ライトテーマまたはダークテーマを設定します。
-    ユーザーメニューは以下を含みます。
  - ログインしているユーザーに関する情報。
  -  **Change account (アカウントの変更)**: 現在のアカウントからログアウトし、新しいアカウントにログインします。
  -  **Log out (ログアウト)**: 現在のアカウントからログアウトします。
-  コンテキストメニューは以下を含みます。
  - Analytics data (分析データ)**: 個人以外のブラウザデータの共有に同意します。
  - フィードバック**: フィードバックを共有して、ユーザーエクスペリエンスの向上に役立てます。
  - 法的情報**: Cookieおよびライセンスについての情報を表示します。
  - About (バージョン情報)**: AXIS OSのバージョンやシリアル番号などの装置情報を表示します。
  - Legacy device interface (従来の装置インターフェース)**: 装置のwebインターフェースを従来のバージョンに変更します。

## ステータス

### 時刻同期ステータス

装置がNTPサーバーと同期しているかどうかや、次の同期までの残り時間など、NTP同期情報を表示します。

**NTP settings (NTP設定)**: NTP設定を表示および更新します。NTPの設定を変更できる [Date and time (日付と時刻)] のページに移動します。

### 装置情報

AXIS OSのバージョンとシリアル番号を含む装置情報を表示します。



# AXIS A1610 Network Door Controller


## webインターフェース


**Upgrade AXIS OS (AXIS OSのアップグレード):** 装置のソフトウェアをアップグレードします。アップグレードができる [Maintenance (メンテナンス)] ページに移動します。

## アクセスコントロール

### アラーム

**Device motion (装置の動き):** オンに設定すると、装置の動きを検知したときにシステム内でアラームがトリガーされます。

**Casing open (ケーシング開放)**  : オンに設定すると、ドアコントローラーケーシングの開放を検知したときにシステム内でアラームがトリガーされます。ベアボードコントローラーでこの設定をオフにします。

**External tamper (外部からのいたづら)**  : オンに設定すると、外部からのいたづらを検知したときにシステムでアラームがトリガーされます。たとえば、誰かが外部キャビネットを開閉した場合などです。

- **Supervised input (状態監視入力)**  : 入力の状態を監視するときにオンにし、終端抵抗器を設定します。
  - 並列優先接続を使用するには、[Parallel first connection with a 22 K $\Omega$  parallel resistor and a 4.7 K $\Omega$  serial resistor (22 k $\Omega$ の並列抵抗器と4.7 k $\Omega$ の直列抵抗器による並列優先接続)] を選択します。
  - 直列優先接続を使用するには、[Serial first connection (直列優先接続)] を選択し、[Resistor values (抵抗器の値)] ドロップダウンリストから抵抗器の値を選択します。

### 周辺機器

**Upgrade readers (リーダーのアップグレード):** クリックすると、リーダーをAXIS OSの新しいバージョンにアップグレードします。この機能では、サポート対象のリーダーがオンラインの場合にのみアップグレードします。

## システム

### 時間と場所

#### 日付と時刻

時刻の形式は、Webブラウザの言語設定によって異なります。

#### 注

装置の日付と時刻をNTPサーバーと同期することをお勧めします。

**Synchronization (同期):** 装置の日付と時刻を同期するオプションを選択します。

- **Automatic date and time (manual NTS KE servers) (日付と時刻の自動設定 (手動NTS KEサーバー)):** DHCPサーバーに接続された安全なNTPキー確立サーバーと同期します。
  - **Manual NTS KE servers (手動NTS KEサーバー):** 1台または2台のNTPサーバーのIPアドレスを入力します。2台のNTPサーバーを使用すると、両方からの入力に基づいて装置が同期し、時刻を調整します。
  - **Max NTP poll time (最長NTPポーリング時間):** 装置がNTPサーバーをポーリングして最新の時刻を取得するまでの最長待機時間を選択します。
  - **Min NTP poll time (最短NTPポーリング時間):** 装置がNTPサーバーをポーリングして最新の時刻を取得するまでの最短待機時間を選択します。
- **Automatic date and time (NTP servers using DHCP) (日付と時刻の自動設定 (DHCPを使用したNTPサーバー)):** DHCPサーバーに接続されたNTPサーバーと同期します。

# AXIS A1610 Network Door Controller

## webインターフェース

- **Fallback NTP servers (フォールバックNTPサーバー):** 1台または2台のフォールバックサーバーのIPアドレスを入力します。
- **Max NTP poll time (最長NTPポーリング時間):** 装置がNTPサーバーをポーリングして最新の時刻を取得するまでの最長待機時間を選択します。
- **Min NTP poll time (最短NTPポーリング時間):** 装置がNTPサーバーをポーリングして最新の時刻を取得するまでの最短待機時間を選択します。
- **Automatic date and time (manual NTP servers) (日付と時刻の自動設定 (手動NTPサーバー)):** 選択したNTPサーバーと同期します。
  - **Manual NTP servers (手動NTPサーバー):** 1台または2台のNTPサーバーのIPアドレスを入力します。2台のNTPサーバーを使用すると、両方からの入力に基づいて装置が同期し、時刻を調整します。
  - **Max NTP poll time (最長NTPポーリング時間):** 装置がNTPサーバーをポーリングして最新の時刻を取得するまでの最長待機時間を選択します。
  - **Min NTP poll time (最短NTPポーリング時間):** 装置がNTPサーバーをポーリングして最新の時刻を取得するまでの最短待機時間を選択します。
- **Custom date and time (日付と時刻のカスタム設定):** 日付と時刻を手動で設定する。[Get from system (システムから取得)] をクリックして、コンピューターまたはモバイル装置から日付と時刻の設定を1回取得します。

**Time zone (タイムゾーン):** 使用するタイムゾーンを選択します。時刻が夏時間と標準時間に合わせて自動的に調整されます。

- **DHCP:** DHCPサーバーのタイムゾーンを採用します。このオプションを選択する前に、装置がDHCPサーバーに接続されている必要があります。
- **Manual (手動):** ドロップダウンリストからタイムゾーンを選択します。

**注**

システムは、すべての録画、ログ、およびシステム設定で日付と時刻の設定を使用します。

## ネットワーク

### IPv4

**Assign IPv4 automatically (IPv4 自動割り当て):** ネットワークルーターに自動的に装置にIPアドレスを割り当てさせる場合に選択します。ほとんどのネットワークでは、自動IP (DHCP) をお勧めします。

**IP address (IPアドレス):** 装置の固有のIPアドレスを入力します。孤立したネットワークの内部であれば、アドレスの重複がないことを条件に、固定IPアドレスを自由に割り当てることができます。アドレスの重複を避けるため、固定IPアドレスを割り当てる前に、ネットワーク管理者に連絡することを推奨します。

**Subnet mask (サブネットマスク):** サブネットマスクを入力して、ローカルエリアネットワーク内部のアドレスを定義します。ローカルエリアネットワークの外部のアドレスは、ルーターを経由します。

**Router (ルーター):** さまざまなネットワークやネットワークセグメントに接続された装置を接続するために使用するデフォルトルーター (ゲートウェイ) のIPアドレスを入力します。

**Fallback to static IP address if DHCP isn't available (DHCPが利用できない場合は固定IPアドレスにフォールバックする):** DHCPが利用できず、IPアドレスを自動的に割り当てることができない場合に、フォールバックとして使用する固定IPアドレスを追加するときに選択します。

**注**

DHCPが使用できず、装置が静的アドレスのフォールバックを使用する場合、静的アドレスは限定された範囲で設定されます。

### IPv6

**Assign IPv6 automatically (IPv6 自動割り当て):** IPv6をオンにし、ネットワークルーターに自動的に装置にIPアドレスを割り当てさせる場合に選択します。

# AXIS A1610 Network Door Controller

## webインターフェース

### Hostname (ホスト名)

**Assign hostname automatically (ホスト名自動割り当て):** ネットワークルーターに自動的に装置にホスト名を割り当てさせる場合に選択します。

**Hostname (ホスト名):** 装置にアクセスする別の方法として使用するホスト名を手動で入力します。サーバーレポートとシステムログはホスト名を使用します。使用できる文字は、A～Z、a～z、0～9、-、\_です。

### DNS servers (DNS サーバー)

**Assign DNS automatically (DNS自動割り当て):** DHCPサーバーに自動的に装置に検索ドメインとDNSサーバーアドレスを割り当てさせる場合に選択します。ほとんどのネットワークでは、自動DNS (DHCP)をお勧めします。

**Search domains (検索ドメイン):** 完全修飾でないホスト名を使用する場合は、[Add search domain (検索ドメインの追加)]をクリックし、装置が使用するホスト名を検索するドメインを入力します。

**DNS servers (DNS サーバー):** [Add DNS server (DNSサーバーを追加)]をクリックして、DNSサーバーのIPアドレスを入力します。このサーバーは、ホスト名からローカルネットワーク上のIPアドレスへの変換を行います。

### HTTPおよびHTTPS

HTTPSは、ユーザーからのページ要求とWebサーバーから返されたページの暗号化を提供するプロトコルです。暗号化された情報の交換は、サーバーの真正性(サーバーが本物であること)を保証するHTTPS証明書の使用により制御されます。

装置でHTTPSを使用するには、HTTPS証明書をインストールする必要があります。[System > Security (システム > セキュリティ)]に移動し、証明書の作成とインストールを行います。

**次によってアクセスを許可:** ユーザーが [HTTP]、[HTTPS]、または [HTTP and HTTPS (HTTPおよびHTTPS)] プロトコルを介して装置に接続することを許可するかどうかを選択します。

#### 注

暗号化されたWebページをHTTPS経由で表示する場合、特に初めてページを要求するときに、パフォーマンスが低下することがあります。

**HTTP port (HTTPポート):** 使用するHTTPポートを入力します。装置はポート80または1024～65535の範囲のポートを許可します。管理者としてログインしている場合は、1～1023の範囲の任意のポートを入力することもできます。この範囲のポートを使用すると、警告が表示されます。

**HTTPS port (HTTPSポート):** 使用するHTTPSポートを入力します。装置はポート443または1024～65535の範囲のポートを許可します。管理者としてログインしている場合は、1～1023の範囲の任意のポートを入力することもできます。この範囲のポートを使用すると、警告が表示されます。

**Certificate (証明書):** 装置のHTTPSを有効にする証明書を選択します。

### ネットワーク検出プロトコル

# AXIS A1610 Network Door Controller

## webインターフェース

**Bonjour®:** オンにすると、ネットワーク上で自動検出が可能になります。

**Bonjour name (Bonjour 名):** ネットワークで表示されるフレンドリ名を入力します。デフォルト名は装置名とMACアドレスです。

**UPnP®:** オンにすると、ネットワーク上で自動検出が可能になります。

**UPnP name (UPnP 名):** ネットワークで表示されるフレンドリ名を入力します。デフォルト名は装置名とMACアドレスです。

**WS-Discovery:** オンにすると、ネットワーク上で自動検出が可能になります。

### One-Click Cloud Connection (ワンクリッククラウド接続)

One-Click cloud connection (O3C) とO3Cサービスを共に使用すると、インターネットを介して、ライブビデオや録画ビデオにどこからでも簡単かつ安全にアクセスできます。詳細については、[axis.com/end-to-end-solutions/hosted-services](http://axis.com/end-to-end-solutions/hosted-services)を参照してください。

#### Allow O3C (O3Cを許可):

- **One-click (ワンクリック):** デフォルトの設定です。インターネットを介してO3Cサービスに接続するには、装置のコントロールボタンを押し続けます。コントロールボタンを押してから24時間以内に装置をO3Cサービスに登録する必要があります。登録しない場合、装置はO3Cサービスから切断されます。装置を登録すると、**[Always (常時)]** が有効になり、装置はO3Cサービスに接続されたままになります。
- **Always (常時):** 装置は、インターネットを介してO3Cサービスへの接続を継続的に試行します。装置を登録すると、装置はO3Cサービスに接続したままになります。装置のコントロールボタンに手が届かない場合は、このオプションを使用します。
- **No (なし):** O3Cサービスを無効にします。

**Proxy settings (プロキシ設定):** 必要な場合は、プロキシサーバーに接続するためのプロキシ設定を入力します。

**Host (ホスト):** プロキシサーバーのアドレスを入力します。

**Port (ポート):** アクセスに使用するポート番号を入力します。

**Login (ログイン) と Password (パスワード):** 必要な場合は、プロキシサーバーのユーザー名とパスワードを入力します。

#### Authentication method (認証方式)

- **Basic (ベーシック):** この方法は、HTTP用の最も互換性のある認証方式です。ユーザー名とパスワードを暗号化せずにサーバーに送信するため、**Digest (ダイジェスト)** 方式よりも安全性が低くなります。
- **Digest (ダイジェスト):** この認証方式は、常に暗号化されたパスワードをネットワークに送信するため、高いセキュリティレベルが得られます。
- **Auto (オート):** このオプションを使用すると、装置はサポートされている方法に応じて認証方法を選択できます。**Digest (ダイジェスト)** 方式が**Basic (ベーシック)** 方式より優先されます。

**Owner authentication key (OAK) (所有者認証キー、OAK):** **[Get key (キーを取得)]** をクリックして、所有者認証キーを取得します。これは、装置がファイアウォールやプロキシを介さずにインターネットに接続されている場合にのみ可能です。

### SNMP

SNMP (Simple Network Management Protocol) を使用すると、離れた場所からネットワーク装置を管理できます。

# AXIS A1610 Network Door Controller

## webインターフェース

SNMP: 使用するSNMPのバージョンを選択します。

- v1 and v2c (v1およびv2c):
  - **Read community (読み取りコミュニティ):** サポートされているSNMPオブジェクトすべてに読み取り専用のアクセスを行えるコミュニティ名を入力します。デフォルト値は **[public (パブリック)]** です。
  - **Write community (書き込みコミュニティ):** サポートされている (読み取り専用のものを除く) SNMPオブジェクトすべてに読み取りアクセス、書き込みアクセスの両方を行えるコミュニティ名を入力します。デフォルト値は **[write (書き込み)]** です。
  - **Activate traps (トラップの有効化):** オンにすると、トラップレポートが有効になります。装置はトラップを使用して、重要なイベントまたはステータス変更のメッセージを管理システムに送信します。webインターフェースでは、SNMP v1およびv2cのトラップを設定できます。SNMP v3に変更するか、SNMPをオフにすると、トラップは自動的にオフになります。SNMP v3を使用する際は、SNMP v3管理アプリケーションでトラップを設定できます。
  - **Trap address (トラップアドレス):** 管理サーバーのIPアドレスまたはホスト名を入力します。
  - **Trap community (トラップコミュニティ):** 装置がトラップメッセージを管理システムに送信するときに使用するコミュニティを入力します。
  - **Traps (トラップ):**
    - **Cold start (コールドスタート):** 装置の起動時にトラップメッセージを送信します。
    - **Warm start (ウォームスタート):** SNMP設定が変更されたときに、トラップメッセージを送信します。
    - **Link up (リンクアップ):** リンクの状態が切断から接続に変わったときにトラップメッセージを送信します。
    - **Authentication failed (認証失敗):** 認証に失敗したときにトラップメッセージを送信します。

### 注

SNMP v1およびv2cトラップをオンにすると、すべてのAXIS Video MIBトラップが有効になります。詳細については、[AXIS OSポータル > SNMP](#)を参照してください。

- **v3:** SNMP v3は、暗号化と安全なパスワードを使用する、より安全性の高いバージョンです。SNMP v3を使用するには、HTTPSを有効化し、パスワードをHTTPSを介して送信することをお勧めします。これにより、権限のない人が暗号化されていないSNMP v1およびv2cトラップにアクセスすることも防止できます。SNMP v3を使用する際は、SNMP v3管理アプリケーションでトラップを設定できます。
  - **Password for the account "initial" (「initial」アカウントのパスワード):** 「initial」という名前のアカウントのSNMPパスワードを入力します。HTTPSを有効化せずにパスワードを送信できますが、推奨しません。SNMP v3のパスワードは1回しか設定できません。HTTPSが有効な場合にのみ設定することをお勧めします。パスワードの設定後は、パスワードフィールドが表示されなくなります。パスワードを設定し直すには、装置を工場出荷時の設定にリセットする必要があります。

### Connected clients (接続されたクライアント)

接続数と接続されているクライアントの数を表示します。

**View details (詳細を表示):** 接続されているクライアントのリストを表示および更新します。リストには、各接続のIPアドレス、プロトコル、ポート、状態、PID/プロセスが表示されます。

## セキュリティ

### 証明書

# AXIS A1610 Network Door Controller

## webインターフェース

証明書は、ネットワーク上の装置の認証に使用されます。この装置は、次の2種類の証明書をサポートしています。

- **Client/server Certificates (クライアント/サーバー証明書)**

クライアント/サーバー証明書は装置のIDを認証します。自己署名証明書と認証局 (CA) 発行の証明書のどちらでも使用できます。自己署名証明書による保護は限られていますが、認証局発行の証明書を取得するまで利用できます。

- **CA証明書**

CA証明書はピア証明書の認証に使用されます。たとえば、装置をIEEE 802.1Xで保護されたネットワークに接続するときに、認証サーバーのIDを検証するために使用されます。装置には、いくつかのCA証明書がプリインストールされています。

以下の形式がサポートされています:

- 証明書形式: .PEM、.CER、.PFX
- 秘密鍵形式: PKCS#1、PKCS#12

### 重要

装置を工場出荷時の設定にリセットすると、すべての証明書が削除されます。プリインストールされたCA証明書は、再インストールされます。




**Add certificate (証明書の追加):** クリックして証明書を追加します。

- **More (詳細)**  : 入力または選択するフィールドをさらに表示します。
- **Secure keystore (セキュアキーストア):** [Secure element (セキュアエレメント)] または [Trusted Platform Module 2.0] を使用して秘密鍵を安全に保存する場合に選択します。どのセキュアキーストアを選択するかの詳細については、[help.axis.com/en-us/axis-os#cryptographic-support](http://help.axis.com/en-us/axis-os#cryptographic-support) にアクセスしてください。
- **Key type (キーのタイプ):** ドロップダウンリストから、証明書の保護に使用する暗号化アルゴリズムとしてデフォルトかその他のいずれかを選択します。



コンテキストメニューは以下を含みます。

- **Certificate information (証明書情報):** インストールされている証明書のプロパティを表示します。
- **Delete certificate (証明書の削除):** 証明書の削除。
- **Create certificate signing request (証明書の署名要求を作成する):** デジタルID証明書を申請するために登録機関に送信する証明書署名要求を作成します。

**セキュアキーストア**  :

- **セキュアエレメント (CC EAL6+):** セキュアキーストアにセキュアエレメントを使用する場合に選択します。
- **Trusted Platform Module 2.0 (CC EAL4+, FIPS 140-2 Level 2):** セキュアキーストアにTPM 2.0を使用する場合に選択します。

IEEE 802.1x and IEEE 802.1AE MACsec (IEEE 802.1x および IEEE 802.1AE MACsec)

# AXIS A1610 Network Door Controller

## webインターフェース

IEEE 802.1xはポートを使用したネットワークへの接続を制御するIEEEの標準規格で、有線およびワイヤレスのネットワーク装置を安全に認証します。IEEE 802.1xは、EAP (Extensible Authentication Protocol) に基づいています。

IEEE 802.1xで保護されているネットワークにアクセスするネットワーク装置は、自己の証明を行う必要があります。認証は認証サーバーによって行われます。認証サーバーは通常、FreeRADIUSやMicrosoft Internet Authentication ServerなどのRADIUSサーバーです。

### 証明書

CA証明書なしで設定されている場合、サーバー証明書の検証は無効になり、装置は接続先のネットワークに関係なく自己の認証を試みます。

証明書を使用する場合、Axisの実装では、装置と認証サーバーは、EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) を使用してデジタル証明書で自己を認証します。

装置が証明書で保護されたネットワークにアクセスできるようにするには、署名されたクライアント証明書を装置にインストールする必要があります。

**Authentication method (認証方式):** 認証に使用するEAPタイプを選択します。デフォルトのオプションはEAP-TLSです。EAP-PEAP/MSCHAPv2 は、より安全なオプションです。

**Client certificate (クライアント証明書):** IEEE 802.1xを使用するクライアント証明書を選択します。認証サーバーは、この証明書を使用してクライアントの身元を確認します。

**CA certificate (CA証明書):** 認証サーバーの身元を確認するためのCA証明書を選択します。証明書が選択されていない場合、装置は、接続されているネットワークに関係なく自己を認証しようとします。

**EAP identity (EAP識別情報):** クライアント証明書に関連付けられているユーザーIDを入力します。

**EAPOL version (EAPOLのバージョン):** ネットワークスイッチで使用されるEAPOLのバージョンを選択します。

**Use IEEE 802.1x (IEEE 802.1xを使用):** IEEE 802.1xプロトコルを使用する場合に選択します。

### IEEE 802.1AE MACsec

IEEE 802.1AE MACsecは、メディアアクセスコントロール (MAC) セキュリティのためのIEEE標準であり、メディアアクセス独立プロトコルのためのコネクションレスデータ機密性と整合性を定義しています。

この設定は、認証方法としてEAP-TLSを使用する場合にのみ使用できます。

### Mode (モード)

- **Dynamic CAK / EAP-TLS (動的CAK/EAP-TLS):** デフォルトのオプションです。セキュリティで保護された接続の後、装置はネットワーク上のMACsecをチェックします。
- **Static CAK / pre-shared key (PSK) (静的CAK/事前共有キー (PSK)):** ネットワークに接続するためのキー名と値を設定する場合に選択します。

この設定は、認証方法としてEAP-PEAP/MSCHAPv2 を使用する場合にのみ使用できます。

- **Password (パスワード):** ユーザーIDのパスワードを入力します。
- **Peap version (Peapのバージョン):** ネットワークスイッチで使用するPeapのバージョンを選択します。
- **Label (ラベル):** クライアントEAP暗号化を使用する場合は1を選択し、クライアントPEAP暗号化を使用する場合は2を選択します。Peapバージョン1を使用する際にネットワークスイッチが使用するラベルを選択します。

Prevent brute-force attacks (ブルートフォース攻撃を防ぐ)

# AXIS A1610 Network Door Controller

## webインターフェース

**Blocking (ブロック):** オンにすると、ブルートフォース攻撃がブロックされます。ブルートフォース攻撃では、試行錯誤を繰り返す総当たり攻撃でログイン情報や暗号化キーを推測します。

**Blocking period (ブロック期間):** ブルートフォース攻撃をブロックする秒を入力します。

**Blocking conditions (ブロックの条件):** ブロックが開始されるまでに1秒間に許容される認証失敗の回数を入力します。ページレベルと装置レベルの両方で許容される失敗の数を設定できます。

### ファイアウォール

**Activate (アクティブ化):** ファイアウォールをオンにします。

**Default Policy (デフォルトポリシー):** ファイアウォールのデフォルト状態を選択します。

- **Allow: (許可):** 装置へのすべての接続を許可します。このオプションはデフォルトで設定されています。
- **Deny: (拒否):** 装置へのすべての接続を拒否します。

デフォルトポリシーに例外を設定するために、特定のアドレス、プロトコル、ポートから装置への接続を許可または拒否するルールを作成できます。

- **Address (アドレス):** アクセスを許可または拒否するアドレスをIPv4/IPv6またはCIDR形式で入力します。
- **Protocol (プロトコル):** アクセスを許可または拒否するプロトコルを選択します。
- **Port (ポート):** アクセスを許可または拒否するポート番号を入力します。1~65535のポート番号を追加できます。
- **Policy (ポリシー):** ルールのポリシーを選択します。



: クリックして、別のルールを作成します。

**Add rules: (ルールの追加):** クリックして、定義したルールを追加します。

- **Time in seconds: (時間 (秒)):** ルールのテストに制限時間を設定します。デフォルトの制限時間は次のように設定されています。300秒ルールをすぐに有効にするには、時間を次のように設定します。0秒
- **Confirm rules: (ルールを確認):** ルールとその制限時間を確認します。1秒を超える制限時間を設定した場合、ルールはこの時間内に有効になります。時間を次のように設定するとします。0ルールはすぐに有効になります。

**Pending rules (保留中のルール):** まだ確認していない最新のテスト済みルールの概要です。

#### 注

時間制限のあるルールは、設定した時間が経過するか確認するまで、[Pending rules (保留中のルール)]と[Active rules (アクティブなルール)]の両方に表示されます。確認しない場合、それらのルールは[Pending rules (保留中のルール)]にのみ表示され、ファイアウォールは以前に定義された設定に戻ります。それらのルールを確認すると、現在アクティブなルールが置き換えられます。

**Confirm rules (ルールを確認):** クリックして、保留中のルールをアクティブにします。

**Active rules (アクティブなルール):** 装置で現在実行中のルールの概要です。



: クリックして、アクティブなルールを削除します。



: クリックして、保留中のルールとアクティブなルールの両方をすべて削除します。

### カスタム署名付きAXIS OS証明書



# AXIS A1610 Network Door Controller

## webインターフェース

Axisのテストソフトウェアまたはその他のカスタムソフトウェアを装置にインストールするには、カスタム署名付きAXIS OS証明書が必要です。証明書は、ソフトウェアが装置の所有者とAxisの両方によって承認されたことを証明します。ソフトウェアは、一意のシリアル番号とチップIDで識別される特定の装置でのみ実行できます。署名用のキーはAxisが保有しており、カスタム署名付きAXIS OS証明書はAxisしか作成できません。

**Install (インストール):** クリックして、証明書をインストールします。ソフトウェアをインストールする前に、証明書をインストールする必要があります。



コンテキストメニューは以下を含みます。

- **Delete certificate (証明書の削除):** 証明書の削除。

## アカウント

### アカウント



**Add account (アカウントの追加):** クリックして、新しいアカウントを追加します。最大100個のアカウントを追加できます。

**Account (アカウント):** 固有のアカウント名を入力します。

**New password (新しいパスワード):** アカウントのパスワードを入力します。パスワードの長さは1~64文字である必要があります。印刷可能なASCII文字(コード32~126)のみを使用できます。これには、英数字、句読点、および一部の記号が含まれます。

**Repeat password (パスワードの再入力):** 同じパスワードを再び入力します。

**Privileges (権限):**

- **Administrator (管理者):** すべての設定へのフルアクセスが許可されています。管理者は他のアカウントを追加、更新、削除することもできます。
- **Operator (オペレーター):** 次の操作を除く、すべての設定へのアクセス権があります。
  - すべての [System (システム)] 設定。
  - アプリを追加しています。
- **ビューア:** 設定を変更するアクセス権を持っていません。



コンテキストメニューは以下を含みます。

**Update account (アカウントの更新):** アカウントのプロパティを編集します。

**Delete account (アカウントの削除):** アカウントを削除します。rootアカウントは削除できません。

## MQTT

MQTT (Message Queuing Telemetry Transport) はモノのインターネット (IoT) で使われる標準の通信プロトコルです。これはIoTの統合を簡素化するために設計されており、小さなコードフットプリントと最小限のネットワーク帯域幅でリモート装置を接続するために、さまざまな業界で使用されています。Axis装置のソフトウェアに搭載されているMQTTクライアントは、装置で生成されたデータやイベントを、ビデオ管理ソフトウェア (VMS) ではないシステムに統合することを容易にします。

装置をMQTTクライアントとして設定します。MQTT通信は、クライアントとブローカーという2つのエンティティに基づいています。クライアントは、メッセージの送受信を行うことができます。ブローカーは、クライアント間でメッセージをルーティングする役割を担います。

MQTTの詳細については、[AXIS OSポータル](#)を参照してください。

## ALPN

# AXIS A1610 Network Door Controller

## webインターフェース

ALPNは、クライアントとサーバー間の接続のハンドシェイクフェーズ中にアプリケーションプロトコルを選択できるようにするTLS/SSL拡張機能です。ALPNは、HTTPなどの他のプロトコルで使用される同じポート経由でMQTTトラフィックを有効にするために使用されます。場合によっては、MQTT通信のための専用ポートが開かれていない可能性があります。このような場合の解決策は、ALPNを使用して、ファイアウォールによって許可される標準ポートで、アプリケーションプロトコルとしてMQTTを使用するようネゴシエーションすることです。

### MQTT client (MQTTクライアント)

**Connect (接続):** MQTTクライアントのオン/オフを切り替えます。

**Status (ステータス):** MQTTクライアントの現在のステータスを表示します。

**Broker (ブローカー)**

**Host (ホスト):** MQTTサーバーのホスト名またはIPアドレスを入力します。

**Protocol (プロトコル):** 使用するプロトコルを選択します。

**Port (ポート):** ポート番号を入力します。

- 1883はMQTTオーバTCPのデフォルト値です。
- 8883はMQTTオーバSSLのデフォルト値です。
- 80はMQTTオーバー WebSocket のデフォルト値です。
- 443はMQTTオーバーWebSocket Secure のデフォルト値です。

**ALPN protocol (ALPN プロトコル):** ご使用のMQTTブローカープロバイダーが提供するALPNプロトコル名を入力します。これは、MQTTオーバーSSLとMQTTオーバーWebSocket Secureを使用する場合にのみ適用されます。

**Username (ユーザー名):** クライアントがサーバーにアクセスするために使用するユーザー名を入力します。

**Password (パスワード):** ユーザー名のパスワードを入力します。

**Client ID (クライアントID):** クライアントIDを入力します。クライアントがサーバーに接続すると、クライアント識別子がサーバーに送信されます。

**Clean session (クリーンセッション):** 接続時と切断時の動作を制御します。選択した場合、接続時と切断時に状態情報が破棄されます。

**HTTP proxy (HTTPプロキシ):** 最大長が255バイトのURL。HTTPプロキシを使用しない場合、このフィールドは空白のまま構いません。

**HTTPS proxy (HTTPSプロキシ):** 最大長が255バイトのURL。HTTPSプロキシを使用しない場合、このフィールドは空白のまま構いません。

**Keep alive interval (キープアライブの間隔):** 長時間のTCP/IPタイムアウトを待たずに、サーバーを使用できなくなったことをクライアントに検知させます。

**Timeout (タイムアウト):** 接続を終了する時間の間隔(秒)です。デフォルト値: 60

**装置トピックの接頭辞:** MQTTクライアントタブの接続メッセージやLWTメッセージ、MQTT公開タブの公開条件におけるトピックのデフォルト値で使用されます。

**Reconnect automatically (自動再接続):** 切断された場合に、クライアントを自動的に再接続するかどうかを指定します。

**Connect message (接続メッセージ)**

接続が確立されたときにメッセージを送信するかどうかを指定します。

**Send message (メッセージの送信):** オンにすると、メッセージを送信します。

**Use default (デフォルトを使用):** オフに設定すると、独自のデフォルトメッセージを入力できます。

# AXIS A1610 Network Door Controller

## webインターフェース

**Topic (トピック):** デフォルトのメッセージのトピックを入力します。

**Payload (ペイロード):** デフォルトのメッセージの内容を入力します。

**Retain (保持する):** クライアントの状態をこのTopic (トピック)に保存する場合に選択します。

**QoS:** パケットフローのQoS layerを変更します。

### 最終意思およびテストメッセージ

最終意思テストメッセージ(LWT)を使用すると、クライアントはブローカーへの接続時、認証情報と共にテストメッセージを提供します。後ほどいずれかの時点でクライアントが予期せず切断された場合(電源の停止など)、ブローカーから他のクライアントにメッセージを送信できます。このLWTメッセージは通常のメッセージと同じ形式で、同一のメカニズムを経由してルーティングされます。

**Send message (メッセージの送信):** オンにすると、メッセージを送信します。

**Use default (デフォルトを使用):** オフに設定すると、独自のデフォルトメッセージを入力できます。

**Topic (トピック):** デフォルトのメッセージのトピックを入力します。

**Payload (ペイロード):** デフォルトのメッセージの内容を入力します。

**Retain (保持する):** クライアントの状態をこのTopic (トピック)に保存する場合に選択します。

**QoS:** パケットフローのQoS layerを変更します。

## MQTT publication (MQTT公開)

**Use default topic prefix (デフォルトのトピックプレフィックスを使用):** 選択すると、[MQTT client (MQTTクライアント)] タブの装置のトピックプレフィックスで定義されたデフォルトのトピックプレフィックスが使用されます。

**Include topic name (トピック名を含める):** 選択すると、条件を説明するトピックがMQTTトピックに含まれます。

**Include topic namespaces (トピックの名前空間を含める):** 選択すると、ONVIFトピックの名前空間がMQTTトピックに含まれます。

**シリアル番号を含める:** 選択すると、装置のシリアル番号が、MQTTペイロードに含まれます。

**+ 条件の追加:** クリックして条件を追加します。

**Retain (保持する):** 保持して送信するMQTTメッセージを定義します。

- **None (なし):** すべてのメッセージを、保持されないものとして送信します。
- **Property (プロパティ):** ステートフルメッセージのみを保持として送信します。
- **All (すべて):** ステートフルメッセージとステートレスメッセージの両方を保持として送信します。

**QoS:** MQTT公開に適切なレベルを選択します。

## MQTT サブスクリプション

# AXIS A1610 Network Door Controller

## webインターフェース

**+** サブスクリプションの追加: クリックして、新しいMQTTサブスクリプションを追加します。

**サブスクリプションフィルター:** 購読するMQTTトピックを入力します。

**装置のトピックプレフィックスを使用:** サブスクリプションフィルターを、MQTTトピックのプレフィックスとして追加します。

**サブスクリプションの種類:**

- ・ **ステートレス:** 選択すると、エラーメッセージがステートレスメッセージに変換されます。
- ・ **ステートフル:** 選択すると、エラーメッセージが条件に変換されます。ペイロードが状態として使用されます。

**QoS:** MQTTサブスクリプションに適切なレベルを選択します。

## アクセサリー



### I/O ports (I/Oポート)

デジタル入力を使用すると、開回路と閉回路の切り替えが可能な外部装置 (PIRセンサー、ドアまたは窓の接触、ガラス破損検知器など) を接続できます。

デジタル出力を使用して、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webインターフェースから有効化できます。

### Port (ポート)

**Name (名前):** テキストを編集して、ポートの名前を変更します。


**Direction (方向):**  は、ポートが入力ポートであることを示します。  は、出力ポートであることを示します。ポートが設定可能な場合は、アイコンをクリックして入力と出力を切り替えることができます。

**Normal state (標準の状態):** 開回路には  を、閉回路には  をクリックします。

**Current state (現在の状態):** ポートの現在の状態を表示します。入力または出力は、現在の状態が通常の状態とは異なる場合に有効化されます。装置の接続が切断されているか、DC 1Vを超える電圧がかかっている場合に、装置の入力は開回路になります。

### 注

再起動中、出力回路は開かれます。再起動が完了すると、回路は正常位置に戻ります。このページの設定を変更した場合、有効なトリガーに関係なく出力回路は正常位置に戻ります。

**状態監視**  : オンにすると、誰かがデジタルI/O装置への接続を改ざんした場合に、そのアクションを検出してトリガーできます。入力が開いているか閉じているかを検知するだけでなく、誰かが改ざんした場合 (つまり、切断または短絡) も検知することができます。接続を監視するには、外部I/Oループ内に追加のハードウェア (終端抵抗器) が必要です。

## ログ

### レポートとログ

# AXIS A1610 Network Door Controller

## webインターフェース

### Reports (レポート)

- **View the device server report (装置サーバーレポートを表示):** 製品ステータスに関する情報をポップアップウィンドウに表示します。アクセスログは自動的にサーバーレポートに含まれます。
- **Download the device server report (装置サーバーレポートをダウンロード):** UTF-8形式で作成された完全なサーバーレポートのテキストファイルと、現在のライブビュー画像のスナップショットを収めた.zipファイルを生成します。サポートに連絡する際には、必ずサーバーレポート.zipファイルを含めてください。
- **Download the crash report (クラッシュレポートをダウンロード):** サーバーの状態に関する詳細情報が付随したアーカイブをダウンロードします。クラッシュレポートには、サーバーレポートに記載されている情報と詳細なバグ情報が含まれます。レポートには、ネットワークトレースなどの機密情報が含まれている場合があります。レポートの生成には数分かかることがあります。

### ログ

- **View the system log (システムログを表示):** 装置の起動、警告、重要なメッセージなど、システムイベントに関する情報をクリックして表示します。
- **View the access log (アクセスログを表示):** 誤ったログインパスワードの使用など、本装置への失敗したアクセスをすべてクリックして表示します。

### ネットワークトレース

#### 重要

ネットワークトレースファイルには、証明書やパスワードなどの機密情報が含まれている場合があります。

ネットワークトレースファイルはネットワーク上のアクティビティを録画するので、トラブルシューティングに役立ちます。

**Trace time (追跡時間):** 秒または分でトレースの期間を選択し、[Download (ダウンロード)] をクリックします。

### リモートシステムログ

syslogはメッセージログ作成の標準です。これによって、メッセージを生成するソフトウェア、メッセージを保存するシステム、およびそれらを報告して分析するソフトウェアを分離することができます。各メッセージには、メッセージを生成したソフトウェアの種類を示す設備コードがラベル付けされ、重大度レベルが割り当てられます。

#### +

**Server(サーバー):** クリックして新規サーバーを追加します。

**Host (ホスト):** サーバーのホスト名またはIPアドレスを入力します。

**Format (フォーマット):** 使用するsyslogメッセージの形式を選択します。

- Axis
- RFC 3164
- RFC 5424

**Protocol (プロトコル):** 使用するプロトコルを選択します。

- UDP (デフォルトポートは514)
- TCP (デフォルトポートは601)
- TLS (デフォルトポートは6514)

**Port (ポート):** 別のポートを使用する場合は、ポート番号を編集します。

**Severity (重大度):** トリガー時に送信するメッセージを選択します。

**CA certificate set (CA証明書設定):** 現在の設定を参照するか、証明書を追加します。

# AXIS A1610 Network Door Controller

## webインターフェース

### 保守

**Restart (再起動):** 装置を再起動します。再起動しても、現在の設定には影響がありません。実行中のアプリケーションは自動的に再起動されます。

**Restore (リストア):** ほとんどの設定が工場出荷時の値に戻ります。その後、装置とアプリを再設定し、プリンストールしなかったアプリを再インストールし、イベントやプリセットを再作成する必要があります。

#### 重要

リストア後に保存される設定は以下の場合のみです。

- ブートプロトコル (DHCPまたは静的)
- 静的なIPアドレス
- Default router (デフォルトルーター)
- Subnet mask (サブネットマスク)
- 802.1X settings (802.1Xの設定)
- O3C settings (O3Cの設定)
- DNSサーバーIPアドレス

**Factory default (工場出荷時設定):** すべての設定を工場出荷時の値に戻します。その後、装置にアクセス可能なIPアドレスをリセットする必要があります。

#### 注

検証済みのソフトウェアのみを装置にインストールするために、すべてのAxisの装置のソフトウェアにデジタル署名が付け加えられます。これによって、Axis装置の全体的なサイバーセキュリティの最低ラインがさらに上がります。詳細については、[axis.com](http://axis.com)でホワイトペーパー「Axis Edge Vault」を参照してください。

**AXIS OS upgrade (AXIS OSのアップグレード):** AXIS OSの新しいバージョンにアップグレードします。新しいリリースには、機能の改善やバグの修正、まったく新しい機能が含まれています。常にAXIS OSの最新のリリースを使用することをお勧めします。最新のリリースをダウンロードするには、[axis.com/support](http://axis.com/support)に移動します。

アップグレード時には、以下の3つのオプションから選択できます。

- **Standard upgrade (標準アップグレード):** AXIS OSの新しいバージョンにアップグレードします。
- **Factory default (工場出荷時設定):** アップグレードすると、すべての設定が工場出荷時の値に戻ります。このオプションを選択すると、アップグレード後にAXIS OSを以前のバージョンに戻すことはできません。
- **Autorollback (オートロールバック):** 設定した時間内にアップグレードを行い、アップグレードを確認します。確認しない場合、装置はAXIS OSの以前のバージョンに戻されます。

**AXIS OS rollback (AXIS OSのロールバック):** AXIS OSの以前にインストールしたバージョンに戻します。

# AXIS A1610 Network Door Controller

## 詳細情報

---

### 詳細情報

## サイバーセキュリティ

### 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

Axis Edge Vaultは、Axis装置を保護する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となります。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。Edge Vaultは、暗号化コンピューティングモジュール（セキュアエレメントとTPM）とSoCセキュリティ（TEEとセキュアブート）の堅固な基盤に、エッジ装置セキュリティの専門技術を組み合わせて構築されています。

### Axis デバイスID

装置の出所を確認する仕組みは、デバイスIDへの信頼を確立する鍵です。製造時、Axis Edge Vault搭載装置には工場でのプロビジョニングされた、IEEE 802.1AR準拠の一意のAxisデバイスID証明書が割り当てられます。この証明書は、装置の出所を証明するパスポートのような機能を果たします。デバイスIDは、Axisルート証明書により署名された証明書として、安全なキーストアに永続的に保存されます。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/](https://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。

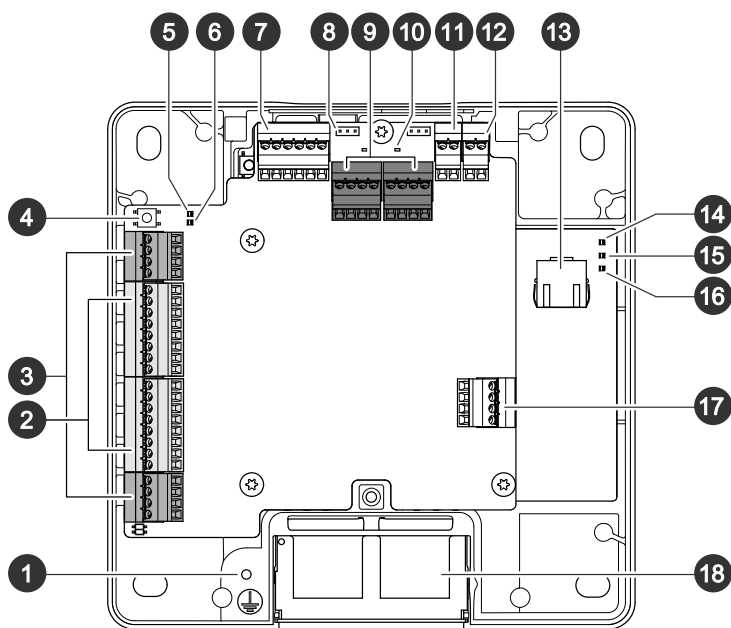
# AXIS A1610 Network Door Controller

## 仕様

### 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。

### 製品の概要



- 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
- 18 リバーシブルケーブルカバー



# AXIS A1610 Network Door Controller

## 仕様

### 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。
状態	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の交互点滅。
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	リレーが有効です。 <sup>1</sup>
	消灯	リレーが無効です。

1. COMがNOに接続するとリレーが有効になります。

#### 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。32ページ工場出荷時の設定にリセットするを参照してください。

## コネクタ

### ネットワークコネクタ

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

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

# AXIS A1610 Network Door Controller

## 仕様

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。25ページネットワークコネクタおよび31ページ電源コネクタを参照してください。

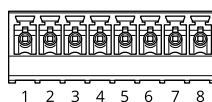
- 装置に電源が供給されていない状態でPoEとDCの両方を接続すると、PoEが電源供給に使用されます。
- PoEとDCの両方が接続されており、現在はPoEが電源を供給しています。PoEが失われた場合、本装置は再起動せずにDCを使用して電源を供給します。
- PoEとDCの両方が接続されており、現在はDCが電源を供給しています。DCが失われた場合、本装置は再起動し、PoEを使用して電源を供給します。
- 起動時にDCが使用されている場合、装置の起動後にPoEが接続されても、電源供給にDCが使用されます。
- 起動時にPoEが使用されている場合、装置の起動後にDCが接続されても、電源供給にPoE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

### 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	リーダーに電力を供給します。	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。	0~30 V DC (最大)
		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)、オーブンドレイン、100 mA

# AXIS A1610 Network Door Controller

## 仕様

### 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。
- ・ コントローラーからリーダーに電力を供給しない場合に、次のケーブル要件を満たす場合、リーダーデータ用の適格なケーブル長は最大1000 mです: シールド付きツイストペア (1組)、AWG 20-16。

### 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	リーダーに電力を供給します。	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。	0~30 V DC (最大)
		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

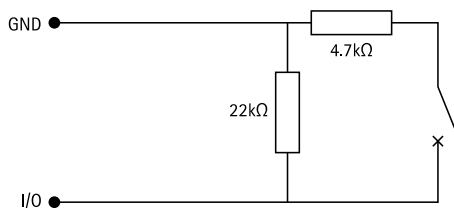
- ・ コントローラーからリーダーに電力を供給する場合、適格なケーブル長は最大150 mです。
- ・ コントローラーからリーダーに電力を供給しない場合に、次のケーブル要件を満たす場合、リーダーデータ用の適格なケーブル長は最大150 mです: AWG 20-16。

### 状態監視入力

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および22 kΩである必要があります。

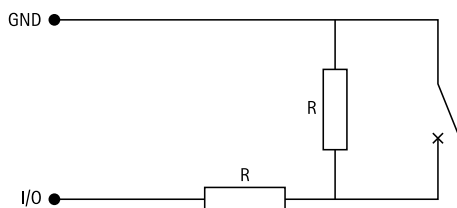


#### Serial first connection (直列優先接続)

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。

# AXIS A1610 Network Door Controller

## 仕様



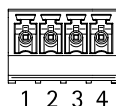
### 注

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0V DCに接続します。

### ドアコネクタ

ドア監視装置用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。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。27ページ状態監視入力を参照してください。



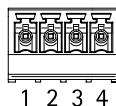
機能	ピン	備考	仕様
DCアース	1, 3		0 V DC
入力	2, 4	ドアモニターとの通信用。 デジタル入力または監視入力 - それぞれピン1または3に接続し、動作させない場合はフロート状態(未接続)のままにします。	0~30 V DC (最大)

### 重要

以下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です。AWG 24。

### 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	備考	仕様
DCアース (GND)	1		0 V DC

# AXIS A1610 Network Door Controller

## 仕様

NO	2	NO (ノーマルオープン)。リレーデバイス接続用。NOとDCアース間でフェイルセキュアロックを接続します。ジャンパー未使用時、2つのリレーピンは他の残りの回路から直流的に分離されます。	最大電流 = 2 A (リレーごと) 最大電圧 = 30 V DC
COM	3	共通	
NC	4	NC (ノーマルクローズ)。リレーデバイス接続用。NCとDCアース間でフェイルセーフロックを接続します。ジャンパー未使用時、2つのリレーピンは他の残りの回路から直流的に分離されます。	

### 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す。

電源	12 V DC での最大電力 <sup>1</sup>	24 V DC での最大電力
DC 入力	1 800 mA	750 mA
PoE	900 mA	410 mA

1. 電力は2つのリレーと AUX I/O 12 V DC の間で共有されます。

### 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

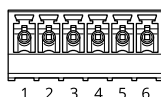
補助コネクタに外部装置を接続し、動体検知、イベントトリガー、アラーム通知などと組み合わせて使用することができます。補助コネクタは、0 V DC 基準点と電力 (DC 出力) に加えて、以下へのインターフェースを提供します。

**デジタル入力** - オープンサーキットとクローズサーキットの切り替えが可能なデバイス (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** - 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 などの外部デバイスを接続します。接続されたデバイスは、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 ページから有効にすることができます。

6 ピンターミナルブロック

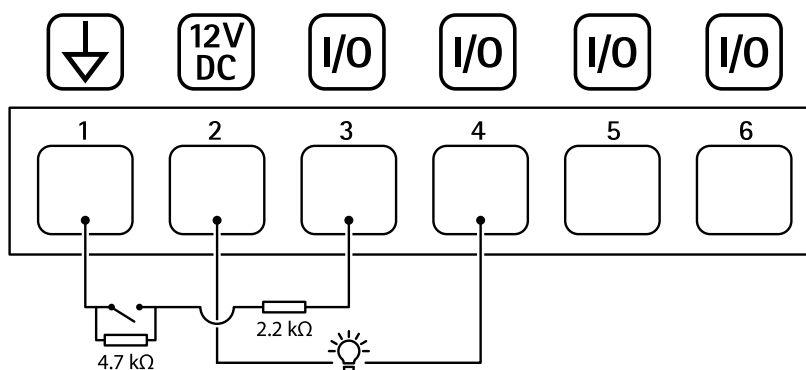


機能	ピン	備考	仕様
DC アース	1		0 V DC

# AXIS A1610 Network Door Controller

## 仕様

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。	I/Oごとに12 V DC 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/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、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。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

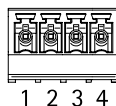


- 1 DCアース
- 2 DC出力 12 V、最大50 mA
- 3 I/O (状態監視として設定)
- 4 I/O (出力として設定)
- 5 設定可能I/O
- 6 設定可能I/O

### 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	備考	仕様
DCアース	1, 3		0 V DC

# AXIS A1610 Network Door Controller

## 仕様

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、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

### 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以下または5 A以下の安全特別低電圧 (SELV) に準拠した有限電源 (LPS) を使用してください。



機能	ピン	備考	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	備考	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

# AXIS A1610 Network Door Controller

## トラブルシューティング

### 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、以下の手順を実行します。

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。24ページ製品の概要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離します。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。これで本製品は工場出荷時の設定にリセットされました。ネットワーク上に利用可能なDHCPサーバーがない場合、デフォルトのIPアドレスは192.168.0.90になります。
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/](https://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 A1610 Network Door Controller

## トラブルシューティング

### AXIS OSをアップグレードする

#### 重要

- ・ 事前設定済みの設定とカスタム設定は、装置のソフトウェアのアップグレード時に保存されます (その機能が新しいAXIS OSで利用できる場合)。ただし、この動作をAxis Communications ABが保証しているわけではありません。
- ・ 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/](https://axis.com/support/device-software/)にアクセスしてください。

#### 注

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/](https://axis.com/support/device-software/)から無料で入手できます。
2. 装置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、ヒント、解決策

ここで解決策が見つからない場合は、[axis.com/support/](https://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。

#### AXIS OSのアップグレード時の問題

AXIS OSのアップグレードに失敗する	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、 <b>[Maintenance (メンテナンス)]</b> 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

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。
------------------	---

# AXIS A1610 Network Door Controller

## トラブルシューティング

IPアドレスが別のデバイスで使用されている	Axis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)。 <ul style="list-style-type: none"><li>もし、「Reply from &lt;IPアドレス&gt;: 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。</li><li>もし、「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。</li></ul>
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アドレスが別の装置でも使用されていると、装置へのアクセスに問題が発生する可能性があります。

### ブラウザから装置にアクセスできない

ログインできない	HTTPSが有効なときは、正しいプロトコル(HTTPまたはHTTPS)を使用してログインしてください。ブラウザのアドレスフィールドに、手動で「http」または「https」と入力する必要がある場合があります。  rootアカウントのパスワードを忘れた場合は、装置を工場出荷時の設定にリセットする必要があります。32ページ工場出荷時の設定にリセットする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。装置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)を使用して装置を識別します。  必要に応じて、静的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、 <a href="http://axis.com/support">axis.com/support</a> 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装置の日付と時刻を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。

### 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

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 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 5: 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。
- 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](http://axis.com/vms)にアクセスしてください。

### MQTTオーバSSLを使用してポート8883経由で接続できない

ファイアウォールによって、ポート8883が安全ではないと判断されたため、ポート8883を使用するトラフィックがブロックされています。	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を使用できる可能性があります。 <ul style="list-style-type: none"><li>• 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。</li><li>• サーバー/ブローカーがALPNをサポートしている場合、ポート443などのオープンポート経由でMQTTをネゴシエーションできます。ALPNがサポー</li></ul>
--	---

# AXIS A1610 Network Door Controller

## トラブルシューティング

---

トされているかどうか、どのALPNプロトコルとポートを使用するかについては、サーバー/ブローカープロバイダーに確認してください。

### パフォーマンスに関する一般的な検討事項

最も重要な検討事項には次のようなものがあります。

- ・ 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。

### サポートに連絡する

さらにサポートが必要な場合は、[axis.com/support](https://axis.com/support)にアクセスしてください。

