AXIS Camera Station Pro

ユーザーマニュアル

バージョン情報

AXIS Camera Station Proは、Axisネットワークカメラからのビデオフィードを監視、録画、管理するビデオ管理ソリューションです。アクセスコントロール、マルチサイト管理、AXIS Audio Managerとの連携、サードパーティ製システムの統合に対応しています。

アクティブ、長期サポート (LTS)、および製品別サポート (PSS) トラック*でメンテナンス対象となっているすべてのAXIS OSバージョンに対応しています。詳細については、AXIS Camera Station Proリリースノートまたは*AXIS OS Portal*を参照してください。AXIS Camera Station Proに対応する製品を確認するには、*対応製品*を参照してください。

*当社は、商業的に実現可能な限り、旧バージョンのAXIS OSとの互換性の維持に努めます。

アクセスのオプション

AXIS Camera Station Proサーバー: - お使いのシステム内のカメラ、ビデオエンコーダ、補助装置とのすべての通信を管理します。システム要件および容量計画に関する情報は、*AXIS Camera Station Proのインストールおよび移行ガイドのハードウェアガイドライン*を参照してください。

AXIS Camera Station Proクライアント - 録画、ライブビデオ、ログ、および設定にアクセスできます。任意のコンピューターにインストールでき、インターネットや社内ネットワーク上のどこからでもリモートで監視や制御を行うことができます。

AXIS Camera Station Webクライアント - AXIS Camera Station Proの録画とライブビデオにWebブラウザーからアクセスできるようになります。詳細については、*AXIS Camera Station webクライアントのユーザーマニュアル*を参照してください。

AXIS Camera Station Proモバイルアプリを開きます。- 複数のシステムの録画やライブビデオにアクセスできます。このアプリはAndroid装置やiOS装置にインストールでき、他の場所からリモートで監視を行うことができます。

ダウンロード方法

*AXIS Camera Station Proのダウンロードページ*に移動して、ダウンロード、更新、または90日間の無料トライアルを利用します。

- すべての機能を試せる90日間の無料トライアル: AXIS Camera Station Proを90日間無料で試すことができます。ライセンスは不要です。
- クライアントのみを更新 - オフライン: AXIS Camera Station Proで直接操作するクライアントを更新します。クライアントのみを更新し、サーバーを更新する必要がない場合に使用します。
- クライアントとサーバーの更新 - オフライン: クライアントとサーバーの圧縮された更新パッケージ。ダウンロード後、.ZIPファイルを展開してmsiファイルと.cabファイルにアクセスし、msiファイルを実行して更新を開始します。
- クライアントとサーバーの更新 - オンライン：更新プログラムを自動的にダウンロード、解凍、インストールします。exe.ファイルを実行し、画面の指示に従います。インストール中は、コンピューターをインターネットに接続したままにしてください。
- iOS向けモバイルアプリ: iPhoneおよびiPad向けの AXIS Camera Station Proモバイルアプリ。App Storeから入手できます。
- Android向けモバイルアプリ: Androidスマートフォンおよびタブレット向けの AXIS Camera Station Proモバイルアプリ。Google Playから入手できます。

チュートリアルビデオ

システムの使用方法の詳細な例については、*AXIS Camera Station Proチュートリアルビデオ*を参照してください。

システム機能

AXIS Camera Stationのシステム機能の詳細については、*AXIS Camera Station Pro Feature Guide*を参照してください。

最新情報?

AXIS Camera Station Proの各リリースの新機能については、*AXIS Camera Station Proの新機能*を参照してください。

管理者に役に立つリンク

- *サーバーとの接続, on page 9*
- *デバイスの設定, on page 48*
- *ストレージの設定, on page 79*
- *録画とイベントの設定, on page 85*
- *接続中のサービスの設定, on page 129*
- *サーバーの設定, on page 132*
- *セキュリティの設定, on page 143*

その他のマニュアル

- *AXIS Camera Station Webクライアント*
- *AXIS Camera Station Pro Integrator Guide*
- *AXIS Camera Stationモバイルアプリ*
- *AXIS Camera Station Proチュートリアルビデオ*
- *AXIS Camera Station Pro Troubleshooting Guide*
- *AXIS Camera Station Pro System Hardening Guide*

オペレーターに役に立つリンク

- *サーバーとの接続, on page 9*
- *クライアントの設定, on page 124*
- *ライブビュー, on page 13*
- *録画の再生, on page 27*
- *録画のエクスポート, on page 30*

クイックスタート

このガイドを使用して、システムを立ち上げて稼働させます。

開始する前に:

- インストール環境に合わせてネットワークを設定してください。*ネットワーク設定*を参照してください。
- 必要な場合は、サーバーポートを設定します。*サーバーポートの設定*を参照してください。
- システムのセキュリティが確保されていることを確認してください。*セキュリティに関する考慮事項*を参照してください。

管理者向け:

1. *ビデオ管理システムを起動する*
2. *デバイスの追加*
3. *録画方法の設定, on page 7*

オペレーター向け:

1. *ライブビデオを表示する, on page 7*
2. *録画の表示, on page 7*
3. *録画のエクスポート, on page 7*
4. *AXIS File Playerでの録画の再生と検証, on page 7*

ビデオ管理システムを起動する

AXIS Camera Station Proクライアントのアイコンをダブルクリックすると、クライアントが起動します。クライアントの初回起動時には、同じコンピューターにインストールされた AXIS Camera Station Proサーバーに自動的にログインしようとします。

クライアントが開くと、システムのライセンスを取得するよう求められます。[**License now (今すぐライセンスを取得)**] をクリックして [**Manage licences (ライセンス管理)**] ページに移動します。ここで、サーバーを組織に登録できます。詳細については、*接続中のサービスを管理する, on page 129*および *ライセンスを管理, on page 142*を参照してください。
VMS Webクライアント、システムの健全性監視、オンラインライセンス取得など、接続中のサービスにアクセスするには、システムを組織に登録してから、システムに接続する必要があります。

複数の AXIS Camera Station Proサーバーに異なる方法で接続できます。*サーバーとの接続*を参照してください。

デバイスの追加

AXIS Camera Station Proを初めて起動すると、[**Add devices (デバイスの追加)**] ページが開き、デバイスを追加するネットワークを検索します。*デバイスの追加*を参照してください。

1. 追加するデバイスをリストから選択します。デバイスが見つからない場合は、[**Manual search (手動検索)**] をクリックするか、入力して絞り込みます。
2. [**追加**] をクリックします。
3. [**Close (閉じる)**] をクリックして設定をスキップし、後で続行します。ここで設定を続行する場合は以下の手順に従います。
   3.1. [**Quick configuration (クイック設定)**] または [**Site Designer configuration (Site Designer設定)**] を選択します。詳細については、*AXIS Site Designerプロジェクトのインポート, on page 52*を参照してください。

3.2. [Add image overlay for date, time, and text (日付、時刻、テキストの画像オーバーレイを追加する)] を選択して、オーバーレイが設定されていないAxisカメラにオーバーレイを追加します。
3.3. [Next (次へ)] をクリックします。
3.4. [Recording method (録画方法)] の設定を選択します。
3.5. [Next (次へ)] をクリックします。
3.6. [Retention time (保存期間)] と [Recording storage (録画ストレージ)] を選択し、[Finish (終了)] をクリックして設定を適用します。

録画方法の設定

1. [設定] - [録画とイベント] - [録画方法] を選択します。
2. カメラを選択します。
3. [Motion detection (動体検知)] または [Continuous (連続)] をオンにします。
4. [適用] をクリックします。

ライブビデオを表示する

1. [Live view (ライブビュー)] タブを開きます。
2. ライブビデオを表示するカメラを選択します。

詳細については、*ライブビュー, on page 13*を参照してください。

録画の表示

1. [Recordings (録画)] タブを開きます。
2. 録画を表示するカメラを選択します。

詳細については、*録画, on page 27*を参照してください。

録画のエクスポート

1. [Recordings (録画)] タブを開きます。
2. 録画をエクスポートするカメラを選択します。
3. をクリックすると、選択マーカーが表示されます。
4. マーカーをドラッグして、エクスポートする録画を含めます。
5. をクリックして、[Export (エクスポート)] タブを開きます。
6. [Export... (エクスポート)] をクリックします。

詳細については、*録画のエクスポート, on page 30*を参照してください。

AXIS File Playerでの録画の再生と検証

1. エクスポートした録画を含むフォルダーに移動します。
2. AXIS File Playerをダブルクリックします。
3. をクリックすると、録画のノートが表示されます。
4. デジタル署名を検証するには、次のようにします。
   4.1. [Tools > Verify digital signature (ツール > デジタル署名の検証)] に移動します。
   4.2. [Validate with password (パスワードで検証)] を選択し、パスワードを入力します。

4.3. [Verify (検証)] をクリックして検証結果を確認します。

注

- デジタル署名は署名付きビデオとは異なります。署名付きビデオは、そのビデオが録画されたカメラを特定できるため、改ざんされていないことを確認できます。詳細については、*署名付きビデオとカメラのユーザーマニュアル*を参照してください。
- 保存されたファイルがAXIS Camera Stationデータベースと接続していない場合 (インデックスされていないファイル) 、AXIS File Playerで再生できるように変換する必要があります。ファイルの変換については、Axisテクニカルサポートにお問い合わせください。

ネットワーク設定

クライアント、サーバー、接続されているネットワークデバイスが異なるネットワーク上にある場合は、AXIS Camera Station Pro使用する前にプロキシーまたはファイアウォールを設定します。

クライアントのプロキシ設定

プロキシーサーバーがクライアントとサーバーの間にある場合は、クライアントコンピューターのWindowsでプロキシー設定を行います。詳細については、Axisサポートまでお問い合わせください。

サーバーのプロキシ設定

プロキシーサーバーがネットワークデバイスとサーバーの間にある場合は、サーバー上のWindowsでプロキシー設定を行う必要があります。詳細については、Axisサポートまでお問い合わせください。

NATとファイアウォール

クライアントとサーバーがNATまたはファイアウォールで隔てられている場合は、AXIS Camera Station ProService Controlで指定されているHTTPポート、TCPポート、ストリーミングポートが、ファイアウォールやNATを通過できるように設定します。ネットワーク管理者にサポートを依頼してください。

詳細については、*AXIS Camera Station Proのポートリスト, on page 223*を参照してください。

サーバーポートの設定

AXIS Camera Station Proサーバーでは、サーバーとクライアント間の通信にポート29202 (TCP) および29204 (HTTPS) が使用されます。必要な場合、これらのポートはAXIS Camera Station Pro Service Controlで変更できます。

注

Axis Secure Remote Access v2やその他のAxisクラウドサービスを使用せずに AXIS Camera Station Proを使用する場合のみ、ポートを変更してください。

詳細については、*全般サーバー設定*または*よくある質問*を参照してください。

セキュリティに関する考慮事項

カメラおよび録画への不正アクセスを防ぐには:

- すべてのネットワーク装置 (カメラ、ビデオエンコーダ、補助装置) で強力なパスワードを使用します。
- AXIS Camera Station Proサーバー、カメラ、ビデオエンコーダ、補助デバイスをオフィスネットワークから分離された安全なネットワークにインストールします。AXIS Camera Station Proクライアントは、インターネットアクセスのあるネットワークなど別のネットワーク上のコンピューターにインストールすることができます。
- すべてのユーザーが強力なパスワードを使用していることを確認してください。

サーバーとの接続

AXIS Camera Station Proクライアントでは、単一のサーバーまたは複数のサーバーに、さまざまな方法で接続することができます。

最後に使用したサーバー - 前のセッションで使用したサーバーに接続します。

このコンピューター - クライアントと同じコンピューターにインストールされているサーバーに接続します。

リモートサーバー - *リモートサーバーとの接続, on page 9*を参照してください。

Axis Secure Remote Access v2 - *Axis Secure Remote Access v2にサインインする, on page 10*を参照してください。

注

- サーバーへの初回接続時、クライアントはサーバーの証明書IDを確認します。正しいサーバーに接続していることを確認するには、その証明書IDを AXIS Camera Station Pro Service Controlに表示されているIDと照合します。詳細については、*全般サーバー設定, on page 223*を参照してください。
- クライアントとサーバーは、同じバージョンである必要があります。ローカルシステムやポートマッピングが設定されているシステムに接続する際にバージョンが一致していない場合、クライアントはサーバーと一致する正しいバージョンをダウンロードし、そのバージョンに切り替えることができます。
- クライアントが複数のサーバーに接続するためには、各サーバーのバージョンが同じである必要があります。デフォルトでは、クライアントのショートカットは最新バージョンを使用します。

Server list (サーバーリスト)	サーバーリストからサーバーに接続するには、[Server list (サーバーリスト)] のドロップダウンメニューからサーバーを選択します。サーバーリストを作成または編集するには、 をクリックします。*サーバーリスト*を参照してください。
Import server list (サーバーリストのインポート)	AXIS Camera Station Proからエクスポートされたサーバーリストファイルをインポートするには、右下の [Import server list (サーバーリストをインポート)] をクリックして、.mslファイルを参照します。*サーバーリスト*を参照してください。
Delete saved passwords (保存したパスワードの削除)	接続されたすべてのサーバーの保存されたユーザー名とパスワードを削除するには、[Delete saved passwords (保存したパスワードを削除)] をクリックします。

リモートサーバーとの接続

1. [リモートサーバー] を選択します。
2. [Remote server (リモートサーバー)] ドロップダウンリストからサーバーを選択するか、IPアドレスまたはDNSアドレスを入力します。サーバーが一覧に表示されていない場合は、 をクリックして、利用可能なすべてのリモートサーバーのリストを更新します。サーバーがデフォルトのポート番号 (29202) とは異なるポートでクライアントを受け入れるよう設定されている場合は、IPアドレスの後にポート番号 (192.168.0.5:46001など) を入力します。
3. 以下のいずれかの操作を行います。

- 現在のWindows® ユーザーとしてログインするには、[Log in as current user (現在のユーザーでログイン)] を選択します。
- [Log in as current user (現在のユーザーでログイン)] のチェックマークを外し、[Log in (ログイン)] をクリックします。別の認証情報を使用してログインする場合は、[Other user (その他のユーザー)] を選択して別のユーザー名とパスワードを入力します。

Axis Secure Remote Access v2にサインインする

1. [Sign in to AXIS Secure Remote Access v2 (Axis Secure Remote Access v2にサインイン)] リンクをクリックします。
2. MyAxisアカウントの認証情報を入力します。
3. [Sign in (サインイン)] をクリックします。
4. 組織を選択し、[OK] をクリックします。
5. ログインするサーバーを選択します。
6. サーバーの認証情報を使用してログインします。

注

サーバーの認証情報はMy Axisアカウントの認証情報とは異なります。

AXIS Camera Station Proクライアントの下部にあるステータスバーに、Axis Secure Remote Access v2の使用状況が表示されます。[Data used this month (今月使用したデータ)] には、組織が当月に使用した中継データの合計量が表示されます。カウンターは毎月1日の午前0時にリセットされます。

モバイルデバイスのAxis Secure Remote Access v2

モバイルデバイス (iOSおよびAndroid) でAxis Secure Remote Access v2を使用してサーバーにログインするには:

1. *axis.com/products/axis-camera-station/overview*に移動し、AXIS Camera Stationモバイルアプリをダウンロードします。
2. モバイルアプリをインストールして開きます。
3. My Axisアカウントの認証情報を使用して、Axis Secure Remote Access v2にサインインします。
4. ログインするサーバーを選択します。
5. サーバーの認証情報を使用してログインします。

注

- サーバーの認証情報はMy Axisアカウントの認証情報とは異なります。
- My Axisアカウントでサインインするには、まずユーザーとして組織に招待される必要があります。

モバイルアプリには、組織が当月に使用した中継データの合計量が表示されます。詳細については、*AXIS Camera Station Mobileアプリユーザーマニュアル*を参照してください。

クライアントのプロキシ設定

プロキシーサーバーが AXIS Camera Station Proクライアントと AXIS Camera Station Proサーバーの間にある場合は、クライアントコンピューターのWindowsでプロキシー設定を行う必要があります。詳細については、Axisサポートまでお問い合わせください。

AXIS Camera Station Proクライアント

タブ

ライブビュー	接続されたカメラからのライブビデオを表示します。ライブビューを参照してください。
録画	録画の検索、再生、エクスポートを行います。*録画*を参照してください。
スマート検索1	動き検索を使用して、録画されたビデオからイベントを見つけます。*スマート検索1*を参照してください。
データ検索	外部ソースまたはシステムからデータを検索し、各イベントの発生時に何が起こったかを追跡します。*データ検索, on page 45*を参照してください。
設定	接続されたデバイスを管理し、クライアントおよびサーバーの設定を行います。*設定*を参照してください。
ホットキー	ホットキーを表示・設定します。*ホットキー*を参照してください。
ログ	アラームログ、イベントログ、および監査ログです。*ログ*を参照してください。
アクセス管理	システムのカード所持者、グループ、ドア、ゾーン、アクセスルールを設定・管理します。*アクセス管理, on page 192*を参照してください。
スマート検索2	高度なフィルターを使用して、特徴に基づいて車両や人物を検索します。*スマート検索2, on page 39*を参照してください。
システムのヘルスモニタリング	1つまたは複数の AXIS Camera Station Proシステムからのヘルスデータを監視します。*System Health Monitoring*[BETA]*, on page 204*を参照してください。
ライブビューアラート	ライブビューアクションがトリガーされると、カメラの [ライブビューアラート] タブまたはビューに自動的に移動します。*ライブビューアクションの作成*を参照してください。
録画アラート	[アラーム] タブまたは [ログ] タブでアラームを選択し、 [Go to recordings (録画を表示)] をクリックして [録画アラート] タブを開きます。*アラームおよびログ*を参照してください。

メインメニュー

	メインメニューを開きます。
サーバー	新しい AXIS Camera Station Proサーバーに接続し、サーバーリストを表示して、すべてのサー

	バーの接続ステータスを確認します。サーバーの設定を参照してください。
アクション	録画を手動で開始または停止し、I/Oポートのステータスを変更します。*手動による録画*および *I/Oポートの監視*を参照してください。
ヘルプ	ヘルプやサポートのオプションにアクセスします。[**Help (ヘルプ)**] > [**About (バージョン情報)**] に移動して、使用中の AXIS Camera Station Proクライアントのバージョンを確認します。
ログアウト	ログアウトし、サーバーとの接続を切断します。
終了	AXIS Camera Station Proクライアントを終了して閉じます。

タイトルバー

? またはF1	ヘルプを開きます。
	全画面モードに入ります。
またはESC	全画面モードを終了します。

ステータスバー

- 警告インジケーターは、クライアントとサーバーの時刻が一致していないことを示します。タイムラインの問題を防ぐため、時刻が同期されていることを確認してください。
- サーバーの接続ステータスには、接続するサーバー数が表示されます。*接続ステータス*を参照してください。
- ライセンスステータスには、ライセンスされていないデバイス数が表示されます。*ライセンスを管理*を参照してください。
- Secure Remote Access v2の利用状況には、今月のデータ使用量が表示されます。
- **[AXIS Camera Station Proupdate available (更新が利用可能です)]** は、新バージョンが利用可能であることを示しています。管理者としてログインしている場合のみ表示されます。*AXIS Camera Station Proの更新, on page 136*を参照してください。

アラームとタスク

- [Alarms (アラーム)] タブと [Tasks (タスク)] タブには、トリガーされたイベントとシステムアラームが表示されます。アラームおよび タスクを参照してください。

ライブビュー

ライブビューは、接続されているカメラのライブビデオを表示します。複数の AXIS Camera Station Proサーバーに接続すると、すべてのビューとカメラがサーバー名ごとにグループ化されて表示されます。

ビューを使用して、AXIS Camera Station Proに追加されているすべてのカメラと装置にアクセスできます。ビューは、1台以上のカメラ、アイテムのシーケンス、マップ、またはWebページで構成できます。システムから装置を追加または削除すると、ライブビューの表示は自動的に更新されます。

また、AXIS Audio Manager Proとの統合により、ライブビューでページングインターフェースを使って音声オゾーンの設定や追加ができます。詳細については、*分割ビューでページングインターフェースを使用する, on page 21*を参照してください。

すべてのユーザーはビューにアクセスできます。ユーザーのアクセス権の詳細については、*ユーザー権限, on page 143*を参照してください。

ライブビューの設定については、*クライアント設定*を参照してください。

複数のモニター

別の画面でビューを開くには:

1. [Live view (ライブビュー)] タブを開きます。
2. 1台以上のカメラ、ビュー、シーケンスを選択します。
3. それらを別の画面にドラッグアンドドロップします。

Axisビデオデコーダに接続されたモニターでビューを開くには:

1. [Live view (ライブビュー)] タブを開きます。
2. 1台以上のカメラ、ビュー、シーケンスを選択します。
3. 選択を右クリックし、使用しているビデオデコーダに応じて [Show on AXIS T8705 (AXIS T8705で表示)] または [Show on AXIS D1110 (AXIS D1110で表示)] を選択します。

注

- AXIS T8705はAxisカメラのみをサポートしています。
- AXIS D1110は、1つの分割ビューで最大9つのストリームをサポートします。

ライブビューでのビューの管理

+	新しい分割ビュー、シーケンス、カメラビュー、マップ、Webページ、またはフォルダーを追加します。
✎	ビューまたはカメラ名を編集します。カメラの設定を編集するには、*カメラ設定を編集する*を参照してください。
🗑	ビューを削除します。ビューとすべてのセカンダリビューを編集および削除するための権限が必要です。AXIS Camera Station Proからカメラを削除するには、*カメラ, on page 55*を参照してください。
🔒	管理者は、ビューをロックして、オペレーターによるビューの移動や編集を防ぐことができます。

ライブビューで画像を管理する

Navigate (移動)	カメラビューに移動するには、分割ビューで画像を右クリックし、[**Navigate (移動)**] を選択します。
スナップショットを撮る	スナップショットを撮るには、画像を右クリックし、[**Take snapshot (スナップショットを撮る)**] を選択します。システムは、[**Configuration (設定)**] > [**Client (クライアント)**] > [**Settings (設定)**]で指定されたスナップショットフォルダーにスナップショットを保存します。 注 AXIS Camera Station Proでは、通常スナップショット取得時にビデオストリームが使用されるため、ビデオストリームと同じ解像度の画像が取得されます。ただし、スティッチ処理や歪み補正が必要なパノラマカメラや魚眼カメラの場合は、クライアント側で画面から直接スナップショットを取得します。これは、特に複数カメラのビューの場合、各画像が画面上で小さく表示されるため、解像度が低くなることがあります。
Add snapshot to export (スナップショットをエクスポートに追加する)	スナップショットをエクスポートリストに追加するには、画像を右クリックし、[**Add snapshot to Export (スナップショットをエクスポートに追加する)**] を選択します。
次に表示:	別の画面でビューを開くには、画像を右クリックし、[**Show on (次に表示)**] を選択します。
Use Mechanical PTZ (メカニカルPTZを使用)	PTZカメラと、カメラのwebインターフェースでデジタルPTZが設定されているカメラで利用することができます。メカニカルPTZを使用するには、画像を右クリックし、[**Use Mechanical PTZ (メカニカルPTZを使用)**] を選択します。マウスを使用して、ズーム、パン、チルトを実行します。
ズーム	ズームイン/ズームアウトするにはマウスのホイールを使用します。また、CTRLキーと [+] キーを同時にを押してズームインし、CTRLキーと [-] キーを同時に押してズームアウトすることもできます。
Area zoom (エリアズーム)	特定のエリアを拡大するには、拡大するエリアを囲む四角形を描きます。ズームアウトするには、マウスのホイールを使用します。画像の中央付近を拡大するには、マウスの右ボタンを使用して四角形を描くようにドラッグします。
パンとチルト	カメラを向ける画像をクリックします。連続的にパンまたはチルトを行うには、画像の中央にカーソルを移動して、ナビゲーションの矢印を表示します。クリックしてホールドして、矢印の方向にパンします。パン、チルトの速度を速くするには、クリックしてホールドして、ナビゲーションの矢印を伸ばします。

フォーカスの設定	AXISデバイスのフォーカスを調整するには、画像を右クリックし、**[Set focus (フォーカスの設定)]** を選択します。**[Near (近)]** と **[Far (遠)]** のバーを使用して手動でフォーカスを調整するか、**[AF]** をクリックして自動でフォーカスを合わせます。 ONVIFデバイスのフォーカスを調整するには、画像を右クリックし、**[Set focus (フォーカスの設定)]** を選択します。**[Focus mode (フォーカスモード)]** を選択します。選択したモードによって、ダイアログが更新されます。 • **Absolute (絶対)**: 値を入力して **[Apply (適用)]** をクリックし、特定の位置にフォーカスを設定します。 • **Relative (相対)**: フォーカスを段階的に調整します。カメラに近い物体には **[Near (近)** を使用し、カメラから遠い物体には **[Far (遠)]** を使用します。 • **Continuous (連続)**: **[Nearer (近づける)]** または **[Further (遠ざける)]** を使用してフォーカスを移動させ、終わったら **[Stop (停止)]** をクリックします。 • 自動でフォーカスを合わせるには、**[AF]** をクリックします。
フォーカスリコールゾーン	フォーカスリコールゾーンを追加または削除するには、画像を右クリックし、**[Focus recall zone (フォーカスリコールゾーン)]** を選択します。
オートトラッキングのオン/オフ	AXIS PTZ Autotrackingが設定されているAxis PTZカメラのオートトラッキングをオンまたはオフにするには、画像を右クリックし、**[Autotracking on/off (オートトラッキングのオン/オフ)]** を選択します。
プリセット	プリセットポジションに移動するには、画像を右クリックし、**[Presets (プリセット)]** を選択して、プリセットを選択します。プリセットを作成するには、*PTZプリセット*を参照してください。
プリセットを追加する	プリセットを追加するには、画像ビューを目的の位置にドラッグし、右クリックして **[Presets (プリセット)]** > **[Add preset (プリセットを追加)]** を選択します。

絶対PTZ移動	絶対PTZ位置合わせに対応するONVIFデバイスで利用できます。この機能を使用してカメラを同じ正確な座標に移動します。 絶対PTZを使用するには、ライブビューでカメラを右クリックし、**[Absolute PTZ Move (絶対PTZ移動)]** を選択します。座標系の選択: 標準座標の **[Generic (投影座標系)]**、または緯度・経度で表す **[Spherical (地理座標系)]** を選択します。パン、チルト、ズームの位置の値を入力し、移動速度を設定し、**[OK]** または **[Send (送信)]** をクリックします。
ストリームプロファイル	ストリームプロファイルを設定するには、画像を右クリックし、**[Stream profile (ストリームプロファイル)]** を選択します。*ストリームプロファイル*を参照してください。

デジタルプリセットの追加

PTZコントロール。

注

管理者は、ユーザーのメカニカルPTZをオフにすることができます。*ユーザー権限*を参照してください。

ライブビューでの録画とインスタント再生

	[Recordings (録画)] タブに移動するには、カメラまたは分割ビューを選択し、 をクリックします。
	ライブビューで進行中の録画を示します。
	動きが検知されたかどうかを示します。

	現在実行中の録画を再生するには、画像にカーソルを合わせ、[Instant replay (インスタント再生)]をクリックします。[Recordings (録画)] タブが開き、直前の5秒間の録画が再生されます。
REC	ライブビューから手動録画を行うには、画像にカーソルを合わせ、[REC] をクリックします。ボタンが黄色に変わり、録画中であることを示します。録画を停止するには、もう一度 [REC] をクリックします。

手動録画の解像度、圧縮、フレームレートなどを設定するには、*録画の方法*を参照してください。録画と再生の詳細については、*録画の再生*を参照してください。

注

管理者は、ユーザーの手動録画機能をオフにすることができます。*ユーザー権限*を参照してください。

ライブビューの音声

カメラに音声機能があり、ライブビューのプロファイルで音声をオンにしている場合は、音声を使用できます。

[Configuration (設定)] > [Devices (デバイス)] > [Stream profiles (ストリームプロファイル)] に移動し、カメラの音声を設定します。*ストリームプロファイル, on page 56*を参照してください。

音量	ビュー内で音量を変更するには、画像にカーソルを合わせてから、スピーカーボタンにカーソルを合わせ、スライダーを使用して音量を変更します。音声をミュートまたはミュート解除するには、をクリックします。
このビューのみを聞く	他のビューをミュートし、このビューのみを聞くには、画像にカーソルを合わせ、をクリックします。
スピーカーを通して話す	全二重モードで設定したスピーカーを通して話すには、画像にカーソルを合わせ、をクリックします。
Push-to-talk	設定したスピーカーから単方向および半二重モードで話すには、画像にカーソルを合わせ、をクリックしたままにします。すべての二重モードで [Push-to-talk (プッシュツートーク)] ボタンが表示されるようにするには、[Configuration (設定)] > [Client (クライアント)] > [Streaming (ストリーミング)] > [Audio (音声)] に移動して、[Use push-to-talk for all duplex modes (すべての二重モードでプッシュツートークを使用する)] をオンにします。*ストリーミング, on page 127*を参照してください。

注

管理者は、ユーザーの音声をオフにすることができます。*ユーザー権限*を参照してください。

ライブビューの画面上コントロール

注
画面上コントロールには、ファームウェア7.40以降が必要です。

	ライブビューで利用可能なカメラ機能にアクセスするには、 をクリックします。

分割ビュー

分割ビューでは、複数のビューが同じウィンドウに表示されます。分割ビューでは、カメラビュー、シーケンス、Webページ、マップ、他の分割ビューを使用できます。

注
複数の AXIS Camera Station Proサーバーに接続する場合、他のサーバーから任意のビュー、カメラ、デバイス、または音声ゾーンを分割ビューに追加できます。

分割ビューを追加するには:

1. **[Live view (ライブビュー)]** タブで、＋をクリックします。
2. [**新しい分割ビュー**] を選択します。
3. 分割ビューの名前を入力します。
4. **[Template (テンプレート)]** のドロップダウンメニューからレイアウトを選択します。
5. サイドパネルからカメラやビューをグリッドにドラッグ＆ドロップするか、ダブルクリックして開いている最初のスロットに追加します。
6. **[Save view (ビューを保存)]** をクリックします。

グリッド内のカメラやビューを編集するには、それを選択します。**[Select item to configure (設定する項目を選択)]** で以下を行うことができます。

- **[Remove (削除)]** をクリックしてグリッドから削除します。
- ドロップダウンメニューから**[PTZ preset (PTZプリセット)]** を選択します。

ホットスポットを追加する:

- フレームを選択し、**[Hotspot (ホットスポット)]** で **[Set hotspot (ホットスポットの設定)]** をクリックします。

ホットスポットにトリガーされたビデオストリームを自動的に表示する:

- **[Dynamic hotspot content (動的ホットスポットコンテンツ)]** を選択し、設定します。詳細については、*動的ホットスポット, on page 18*を参照してください。

カメラのストリームプロファイルを設定する:

- グリッドビューで右クリックし、**[Stream profile (ストリームプロファイル)]** を選択します。*ストリームプロファイル, on page 56*を参照してください。

動的ホットスポット

動的ホットスポットを使用して、複数のイベントを同時に監視します。アクションルールがトリガーされると、ホットスポットにビデオストリームが自動的に表示されます。たとえば、3つの異なる出入口で動きが検知された場合、3つすべてのカメラのビューが同時に表示されます。

ホットスポットは、アクティブなビューの数に応じてグリッドを調整します。各ビューにカウントダウンタイマーが表示され、カウントダウンが終了すると消えます。

注
ステートフルなライブビューアクションによってトリガーされるカメラでは、そのアクションがアクティブでなくなるとカウントダウンが開始します。その他のカメラとビューでは、ただちにカウントダウンが開始します。。

動的ホットスポットを作成する

動的ホットスポットを含む新しいビューを追加する:

1. [Live view (ライブビュー)] タブで、＋をクリックします。
2. [Add hotspot (ホットスポットの追加)] をクリックします。
3. [Dynamic hotspot content (動的ホットスポットコンテンツ)] を選択します。
4. 以下を設定します。
   - Number of split view cells (分割ビューのセル数): グリッド内のセル数 (アクティブなビューがない場合も)。範囲: 1〜144。
   - Countdown in seconds (カウントダウン秒数): トリガーされた各ビューが表示される時間。0に設定すると、手動で削除するまでビューが表示されます。範囲: 0〜999。
   - Seconds remaining when countdown appears in view (ビューにカウントダウンが表示されるまでの残り秒数): カウントダウンタイマーが画面に表示されるタイミングを管理します。0に設定すると常に表示されます。注: タイマーを表示すると、システムリソースが消費されます。範囲: 0〜999。
   - Mute audio on incoming views (ビュー開始時の音声のミュート): 新しいストリームはミュート状態で開始されます。それらのミュートは個別に解除できます。
   - Allow adding views with click on view (ビューのクリックによるビューの追加を許可): トリガーされたビューに加え、ビューをクリックしてホットスポットに手動でビューを追加します。
   - Allow adding views with hotkey (ホットキーによるビューの追加を許可): トリガーされたビューに加え、キーボードショートカットを使用して定義済みのビューをホットスポットに追加します。
5. [Save view (ビューを保存)] をクリックします。

既存のビューに動的ホットスポットを追加する:

1. [Live view (ライブビュー)] タブで [Edit view (ビューの編集)] をクリックします。
2. [Add hotspot (ホットスポットの追加)] をクリックします。
3. [Dynamic hotspot (動的ホットスポット)] を選択します。
4. 上記の手順4に従って設定を行います。
5. [Save view (ビューを保存)] をクリックします。

注

[Live view (ライブビュー)] タブでホットスポットを編集し、既存のホットスポットを動的ホットスポットに変換することができます。

ビューの制御と管理

動的ホットスポットの各セルには、以下が含まれます。

- **カウントダウンインジケーター**: ビューが表示されなくなるまでの残り時間を示します。
- **一時停止ボタン**: カウントダウンを一時停止し、画面を長く表示し続けます。
- **閉じるボタン**: ホットスポットからビューをただちに削除します。
- **点滅インジケーター**: ビューが再びトリガーされると、カウントダウンの枠が点滅します。

これらのコントロールは、セルを1つのビューに拡大したり、再生モードに切り替えたりすると非表示になります。任意のセルをダブルクリックすると、そのセルが全画面表示になります。拡大している間は、カウントダウンが自動的に一時停止します。動的ホットスポットは、バックグラウンドで更新され続けています。グリッドビューに戻ると、アクティブなビューが表示されます。

注

再生モードに切り替えると、カメラのストリームは固定され、更新されなくなります。ライブビューに戻して、通常の操作を再開してください。

分割ビューのドアダッシュボード

ドアを設定している場合は、分割ビューでカード所持者を支援したり、ドアやロックの状態、最近のトランザクションを監視したりできます。

1. ドアを追加する手順については、*ドアの追加, on page 157*を参照してください。
2. ドアダッシュボードを分割ビューに追加します。*分割ビュー, on page 18*を参照してください。

ダッシュボード	ドアの詳細およびロックの状態を表示するには、[Dashboard (ダッシュボード)] タブを開きます。 ダッシュボードには、以下の情報が表示されます。 • カード保持者の情報および写真を含むアクセスコントロールイベント (カード保持者がカードをスワイプしたときなど)。 • ドアの開放時間が長すぎるときなどにアラーム (アラームトリガー情報と共に)。 • 最新のトランザクション。
	イベントをブックマークし、[Transactions (トランザクション)] タブで利用できるようにするには、 をクリックします。
アクセス	手動でアクセス権を付与するには、[Access (アクセス権)] をクリックします。これにより、認証情報が提示されたときのようにドアのロックが解除されます。設定された時間が経過すると、ドアは自動的に再びロックされます。
ロック	手動でドアをロックするには、[Lock (ロック)] をクリックします。
ロック解除	手動でドアのロックを解除するには、[Unlock (ロック解除)] をクリックします。手動で再度ロックするまで、ドアはロック解除されたままになります。
施設や部屋の封鎖	ドアへのアクセスを防止するには、[Lockdown (閉鎖)] をクリックします。
トランザクション	最近のトランザクションと保存されたトランザクションを表示するには、[Transactions (トランザクション)] タブを開きます。

ドアダッシュボードでの監視と支援

分割ビューのAXIS Data Insights Dashboard

AXIS Data Insights Dashboardに、デバイスからの分析データがグラフやチャート形式で表示されます。分割ビューにダッシュボードを追加するには:

1. ダッシュボードを設定します。*AXIS Data Insights Dashboard, on page 186*を参照してください。
2. **[Live view (ライブビュー)]** タブで + をクリックします。
3. [**新しい分割ビュー**] を選択します。
4. [**Dashboards (ダッシュボード)**] フォルダーを展開します。
5. ダッシュボードをグリッドにドラッグアンドドロップします。
6. **[Save view (ビューを保存)]** をクリックします。

ダッシュボード	
Audio Analytics	AXIS Audio Analyticsイベントのデータを表示します。
定義された方向に基づく	AXIS Object Analyticsクロスラインカウントシナリオのデータを表示します。
汎用	サポートされているすべてのデータソースからのデータを表示します。
Image Health	AXIS Image Health Analyticsイベントのデータを表示します。
混雑状況	AXIS Object Analyticsのエリアの混雑状況シナリオによる混雑率データを表示します。
送受信のカウント	AXIS Object Analyticsクロスラインカウントシナリオ、AXIS People Counter、AXIS P8815-2 3D Counterのデータを表示します。
空気質モニター	AXIS Air Quality Sensorからの屋内空気質データをライブで表示します。
空気質モニターの詳細	AXIS Air Quality Sensorの集計データを表示します。

分割ビューでページングインターフェースを使用する

ページングインターフェースを使用して、ライブアナウンス、通話発信、音声デバイスからの音声ファイル再生が可能です。これにはAXIS Audio Manager Proの統合が必要です。詳しくは、*AXIS Audio Manager Proを設定する, on page 182*を参照してください。

ページングインターフェースを使用するには:

1. 分割ビューを編集するか、新しい分割ビューを追加します。
2. 1つ以上の音声ゾーンをグリッドにドラッグアンドドロップして、ページングインターフェースに変換します。

注
AXIS Camera Station Proの音声ゾーンは、AXIS Audio Manager Proサーバーで設定したゾーンと同じです。

3. **[Speak (話す)]**、**[Call (通話する)]**、または **[Play a file (ファイルを再生する)]** を選択する:
   - ライブアナウンスなどの単方向通信には、**[Speak (話す)]** を選択します。
   - インターコムで誰かと話すなどの双方向通信には、**[Call (通話する)]** を選択します。
   - AXIS Audio Manager Proサーバーから音声ファイルをスピーカーで再生するには、**[Play a file (ファイルを再生する)]** を選択します。

順次

シーケンスはビュー間で自動的に切り替わります。

注
複数の AXIS Camera Station Proサーバーに接続する場合、他のサーバーから任意のビュー、カメラ、装置をシーケンスに追加できます。

シーケンスを追加するには:

1. **[Live view (ライブビュー)]** タブで、＋をクリックします。
2. [**新しいシーケンス**] を選択します。
3. シーケンスの名前を入力します。
4. 1つ以上のビューまたはカメラを、シーケンスビューにドラッグアンドドロップします。
5. 表示する順序にビューを並べ替えます。
6. ビュークリックして設定を編集します。
7. **[Save view (ビューを保存)]** をクリックします。

PTZプリセット	PTZ機能を備えたカメラの場合、このビューがアクティブなときにカメラが移動するPTZプリセット位置を選択します。
滞留時間	各ビューが表示され次のビューに切り替わるまでの秒数。これはビューごとに個別に設定できます。

注
- シーケンスビューを別のシーケンスビューに追加することはできません。
- コンポーネントビューをリモートサーバーから直接追加することはできません。回避策として、まずコンポーネントビューをシングル分割ビューに追加し、その後、その分割ビューをリモートサーバーから追加します。
- タイムラインの再生が予期しない動作をする場合があります。再生時にはシーケンス内のすべてのカメラが表示されますが、一度にアクティブになるのは1台のみです。

シーケンスバーを使用する

シーケンスを表示する際、ビューの下部にあるバーを使用して、再生を手動で操作することができます。
- **[>]** および **[<]** を使用して、次の表示または前の表示に移動します。

- [Hold (一時停止)] または [Continue (続行)] を使用して、シーケンスを一時停止または再開します。
- カウントダウンには、次に自動的に切り替わるまでの秒数が表示されます。
- シーケンスを右クリックして、バーを非表示にします。
- [Recording (録画)] タブでシーケンスが開いている場合は、自動的に [Hold (一時停止)] に設定されるため、次へボタンまたは前へボタンを使用して手動でのみ移動できます。

カメラビュー

カメラごとの映像を表示するためのビューです。カメラビューは、分割ビュー、シーケンス、マップで使用できます。

注

複数の AXIS Camera Station Proサーバーに接続している場合、すべての接続済みのサーバーのすべてのカメラがリストに表示されます。

カメラにビューを追加するには:

1. [ライブビュー] または [録画] タブで、 + をクリックします。
2. [新しいカメラビュー] を選択します。
3. ドロップダウンメニューからカメラを選択し、[OK] をクリックします。

マップ

マップはインポートした画像です。カメラビュー、分割ビュー、音声ゾーン、シーケンス、Webページ、他のマップ、ドアをマップに配置できます。マップを使用することで、視覚的な概要がわかり、個々の装置を見つけてアクセスすることができます。大規模な設置の場合は、複数のマップを作成し、概要マップに配置することができます。

マップビューでは、アクションボタンを使用することもできます。*アクションボタントリガーの作成*を参照してください。

注

複数の AXIS Camera Station Proサーバーに接続する場合、他のサーバーから任意のビュー、カメラ、装置をマップビューに追加できます。

マップを追加するには:

1. [Live view (ライブビュー)] タブで、 + をクリックします。
2. [新しいマップ] を選択します。
3. マップの名前を入力してください。
4. [Choose image (画像を選択)] をクリックし、マップファイルを見つけます。ファイルサイズは20 MB以下でなければなりません。対応形式: BMP、JPG、PNG、GIF。
5. ビュー、カメラ、その他の装置、ドアをマップにドラッグします。
6. マップ上のアイコンをクリックして設定を編集します。
7. [Add label (ラベルを追加)] をクリックして、ラベル名を入力し、ラベルのサイズ、回転、スタイル、および色を設定します。
8. [Save view (ビューを保存)] をクリックします。

注

- 複数のアイコンとラベルについて、一部の設定は同時に編集できます。
- マップを編集すると、ユーザーアカウントからアクセスできないすべてのデバイスがマップから削除されます。
- コンポーネントビューをリモートサーバーから直接追加することはできません。回避策として、まずコンポーネントビューをシングル分割ビューに追加し、その後、その分割ビューをリモートサーバーからマップに追加します。

アイコンの設定

地図上のアイコンをクリックすると、設定が開きます。

	ドアがドアモニターありで構成されている場合のドアの物理的状態。
	ドアがドアモニターなしで構成されている場合のロックの物理的状態。
	赤い警告三角マークは、ドア、リーダー、またはドアコントローラーに対するいたずらがあったことを示しています。
アイコン	使用するアイコンを選択します。このオプションはカメラやその他のデバイスでのみ使用できます。
大きさ	スライダーを調整してアイコンのサイズを変更できます。
カラー	をクリックしてアイコンの色を変更できます。
名称	このオプションをオンにするとアイコンの名前が表示されます。アイコン名の位置を変更するには [Bottom (下端)] または [Top (上端)] を選択します。
検知範囲	対応デバイスで利用できます。このオプションをオンにすると、デバイスの検知範囲がマップ上に表示されます。検知範囲の [Range (範囲)]、[Width (幅)]、[Direction (方向)]、色を編集することができます。[Flash (フラッシュ)} をオンにすると、動体検知やその他のアクションルールによって録画がトリガーされた際に、検知範囲が点滅します。すべてのデバイスで検知範囲の点滅の全体をオフにするには、*クライアント設定, on page 124*を参照してください。
方向指示矢印	各カメラの視野の向きを示す矢印を表示します。カバー領域の有無にかかわらず、矢印を表示できます。
録画インジケーターの表示	アイコンに表示する録画インジケーターを管理します。[Small indicators (インジケーターを縮小版で表示)] をオンにすると、縮小版のインジケーターが表示されます。それぞれのトグルスイッチを使用して、[Recording (録画)]、[Motion detected (動きを検知)]、[Object detected (物体を検知)]、[Action rule active (アクションルール有効)] のインジケーターを

	表示または非表示にします。この設定はサーバーに保存されるため、すべてのクライアントで同じ設定が共有されます。
ラベル	ラベルには、テキスト、サイズ、向き、色があります。ラベルの内容に下線を付けたり、斜体にしたりすることもできます。
削除	をクリックするとアイコンがマップから削除されます。

地図の操作

ズームと移動
- マウス、キーボード、またはジョイスティックを使用して、地図のズームや移動ができます。現時点では、タッチ操作はサポートされていません。

マウス
- マウスホイールをスクロールして、ズームイン/ズームアウトします。
- ズームインしているときには、ドラッグして地図上を移動します。

キーボード
- Ctrlキーと (+) キーを同時に押してズームインし、Ctrlキーと (-) キーを同時に押してズームアウトします。
- Ctrl キーと矢印キーを使用して、パンおよびチルトします。

ジョイスティック
- ジョイスティックのヘッドを回して、ズームイン/ズームアウトします。
- ジョイスティックを傾けて、パンおよびチルトします。

スナップショットの撮影
- 地図を右クリックして、コンテキストメニューを開きます。地図のスナップショットは、ディスクに保存したり、**[Export (エクスポート)]** タブに追加したりできます。スナップショットは、現在のカメラの状態やインジケーターの状態を含め、そのときに表示されている地図をそのままキャプチャーします。

Web ページ

AXIS Camera Station に Web ブラウザの機能が組み込まれました。たとえば、Webページを分割ビューやシーケンスに追加することができます。

Webページを追加するには:

1. **[Live view (ライブビュー)]** タブで、 をクリックします。
2. [**New web page (新しいWebページ)**] を選択します。
3. Web ページの名前を入力します。
4. WebページのURLを入力します。
5. **[OK]**をクリックします。

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。

フォルダー

フォルダーを使用して、ツリービューのナビゲーションの項目を分類します。フォルダーには、分割ビュー、シーケンス、カメラビュー、マップ、Webページ、他のフォルダーを含めることができます。

フォルダーを追加するには:

1. [ライブビュー] または [録画] タブで、 + をクリックします。
2. [**新しいフォルダー**] を選択します。
3. フォルダーに名前を入力し、[OK] をクリックします。

録画

[Recordings (録画)] タブでは、録画の検索、再生、およびエクスポートを行うことができます。このタブはメインビューと2つのパネルで構成されています。ここで、サーバー名でグループ化された接続されたサーバーからビュー、画像、再生ツール、カメラを見つけることができます。ライブビューを参照してください。

メインビューから、ライブビューと同じ方法で画像を管理できます。詳細については、*ライブビューで画像を管理する, on page 14*を参照してください。

録画方法や、解像度、圧縮、フレームレートなどの録画設定を変更するには、*録画の方法*を参照してください。

注

AXIS Camera Station Proから録画を手動で削除することはできません。古い録画データを削除するには、**[Configuration (設定)] > [Storage (ストレージ)] > [Selection (選択)]** で保存期間を変更します。

録画の再生

タイムラインの複数の録画の上に再生マーカーを置くと、複数のカメラの録画を同時に再生できます。

複数のモニターを使用する場合、ライブビデオと録画ビデオを同時に表示できます。

再生タイムライン

タイムライン内の録画の上にカーソルを合わせると、録画のタイプと時間が表示されます。タイムラインをズームイン、ズームアウト、ドラッグすることで、録画を見やすく表示して検索できます。タイムラインをドラッグすると再生が一時停止し、放すと再開されます。タイムラインをスクラブして、コンテンツの全体を確認したり、特定の場面を探すことができます。

- 赤線は動体検知録画を示しています。
- 青線はアクションルールによってトリガーされた録画を示しています。

録画を検索する

	タイムライン内の日付と時刻をクリックして選択します。
	タイムラインに表示される録画タイプをフィルタリングします。
	保存されたブックマークの検索に使用します。ブックマークを参照してください。
	クリックすると、Axis装着式カメラで作成された録画とブックマークのリストが開きます。ここで、日付と時刻、録画の開始方法、カメラユーザーがAXIS Body Worn Assistantで追加したカテゴリとメモを検索できます。
スマート検索1	Smart search 1 (スマート検索1) を使用して録画を検索します。*スマート検索1*を参照してください。

録画の再生

	録画を再生します。
	録画を一時停止します。

	再生中や前の録画またはイベントの先頭に戻ります。右クリックして、録画、イベント、またはその両方に移動します。
	次の録画またはイベントの先頭に進みます。右クリックして、録画、イベント、またはその両方に移動します。
	録画内の前のフレームに移動します。この機能を使用するには、録画を一時停止してください。右クリックしてスキップするフレーム数を設定します (最大20フレーム)。
	録画内の次のフレームに移動します。この機能を使用するには、録画を一時停止してください。右クリックしてスキップするフレーム数を設定します (最大20フレーム)。
	ドロップダウンメニューの乗数を使用して再生速度を変更します。
	音声をミュートします。この機能を持つのは音声付きの録画のみです。
音声スライダー	スライドして音量を変更します。この機能を持つのは音声付きの録画のみです。
すべての装着式のメタデータを表示する	装着式システムのメタデータを示し、AXIS Body Worn Assistantからのメモとカテゴリを表示します。
パン、チルト、ズーム	画像をクリックし、スクロールしながらズームイン・ズームアウトします。特定の領域をズームインするには、スクロールする前にその場所にカーソルを合わせます。

ブックマーク

注

- ロックされた録画は、手動でロックを解除しない限り削除できません。
- ロックされた録画は、関連付けられているカメラがシステムから削除されると削除されます。

	クリックするとすべてのブックマークが表示されます。ブックマークをフィルタリングするには、アイコンをクリックします。
	新しいブックマークを追加します。
	ロックされた録画であることを意味します。録画にはブックマークの前後に2.5分以上の映像が含まれます。
	ブックマークの名前や説明の編集や、録画のロック/ロック解除を行います。

	ブックマークを削除します。複数のブックマークを削除するには、CtrlキーまたはShiftキーを押したままそれらを選択し、**[Remove (削除)]** をクリックします。
録画削除を防止	選択して録画をロックします。クリアしてロックを解除します。

ブックマークの追加

1. 録画に移動します。
2. タイムラインで、ズームインとズームアウトを行い、マーカーが目的の位置になるようにタイムラインを動かします。
3. をクリックします。
4. ブックマークの名前と説明を入力します。キーワードを使用すると、ブックマークが見つけやすくなります。
5. 録画をロックするには、[**録画削除を防止**] を選択します。

注

録画のロックを解除するには、[Prevent recording deletion (**録画削除を防止**)] をクリアするか、ブックマークを削除します。

6. [OK] をクリックして、ブックマークを保存します。

イベントカテゴリー

録画にカテゴリーを割り当てると、特定のタイプのイベントを簡単に見つけることができます。開始する前に、適切なユーザー権限を持っていることを確認してください。*ユーザーまたはグループの権限, on page 145*を参照してください。

イベントカテゴリを割り当てる

1. [Recordings (**録画**)] タブで、カテゴリーを割り当てる録画を見つけます。
2. タイムラインで録画を右クリックし、[Categoryize event (**イベントを分類する**)] を選択します。
3. 1つまたは複数のカテゴリーを追加します。
4. **[OK]**をクリックします。

イベントにカテゴリを設定すると、選択したカテゴリが録画のプレビューサムネイルに表示されます。カテゴリに色を割り当てている場合、タイムラインにはその色が表示されます。

イベントカテゴリーを削除する

1. **録画**タブで、カテゴリを削除する録画を見つけます。
2. タイムラインで録画を右クリックし、[Categoryize event (**イベントを分類する**)] を選択します。
3. 割り当てられているカテゴリの一覧から、削除するカテゴリを選択します。
4. **[削除]** をクリックします。
5. 削除する各カテゴリで、手順3～4を繰り返します。
6. **[OK]**をクリックします。

注

カテゴリーの削除権限を持っている場合、またはリストから未割り当てのカテゴリーを選択した場合にのみ、**[Remove (削除)]** ボタンを使用できます。

詳細については、*イベントカテゴリーの設定, on page 94*を参照してください。

録画のエクスポート

[Export (エクスポート)] タブから、ローカルストレージデバイスまたはネットワーク上の場所に録画をエクスポートできます。ここから録画の情報とプレビューも閲覧できます。.asf、.mp4、.mkv 形式で、複数のファイルを同時にエクスポートすることができます。

録画を再生するには、Windows Media Player (.asf) またはAXIS File Player (.asf、.mp4、.mkv) を使用します。AXIS File Playerは、インストール不要の無料のビデオおよび音声再生ソフトウェアです。

注

AXIS File Playerで再生する場合、.mp4および.mkv形式の録画は再生速度の変更が可能です。ただし.asf形式の録画は再生速度を変更できません。

開始前に、エクスポートの権限があることを確認してください。*エクスポートのユーザー権限, on page 33*を参照してください。

録画をエクスポートするには :

1. [Recordings (録画)] タブで、カメラまたはビューを選択します。
2. 録画をエクスポートリストに追加します。エクスポートに含まれていないタイムラインの録画には縞模様の色が付きます。
   2.1. をクリックすると、選択マーカーが表示されます。
   2.2. マーカーを移動して、エクスポートする録画を含めます。
   2.3. をクリックして、[Export (エクスポート)] タブを開きます。
3. [Export... (エクスポート)] をクリックします。
4. 録画のエクスポート先のフォルダーを選択します。
5. [OK]をクリックします。[Tasks (タスク)]タブに、エクスポートタスクが表示されます。

エクスポートフォルダーには以下が含まれます。

- 選択した形式の録画。
- ノートを含む.txtファイル ([Include notes (ノートを含める)]を選択した場合)。
- AXIS File Player ([Include AXIS File Player (AXIS File Playerを含める)] を選択した場合)。
- .asx形式のプレイリストファイル ([Create playlist(.asx) (プレイリストの作成(.asx)] を選択した場合)。

録画のエクスポート

[Recordings (録画)] タブ	
	複数の録画を選択するには、をクリックして、選択マーカーを目的の開始点と終了点に移動します。
	選択マーカー内の録画をエクスポートするには、 をクリックします。

[Recordings (録画)] タブ	
録画の追加	1つの録画を追加するには、録画を右クリックし、**[Export (エクスポート) > [Add recordings (録画を追加)]** を選択します。
イベント録画の追加	イベントの時間内に発生したすべての録画を追加するには、録画を右クリックして、[**Export > Add event recordings (エクスポート > イベント録画の追加)**] を選択します。
録画の削除	エクスポートリストから1つの録画を削除するには、録画を右クリックして、**[Export (エクスポート)] > [Remove recordings (録画の削除)]** を選択します。
録画の削除	選択マーカー内の複数の録画をエクスポートリストから削除するには、録画の外部を右クリックし、[**Export > Remove recordings (エクスポート > 録画の削除)**] を選択します。

[Export (エクスポート)] タブ	
音声	エクスポートした録画から音声を除外するには、**[Audio (音声)]** の列のチェックボックスをオフにします。エクスポートした録画に常に音声を含めるには、[**Configuration (設定)**] > [**Server (サーバー)**] > [**Settings (設定)**] > [**Export (エクスポート)**] で、[**Include audio when adding recordings to export (エクスポートする録画の追加時に音声を含める)**] を選択します。
	録画を編集するには、録画を選択して、をクリックします。*エクスポートする前に録画を編集する, on page 33*を参照してください。
	録画のメモを編集するには、録画を選択して、をクリックします。
	録画をエクスポートリストから削除するには、録画を選択し、 をクリックします。
エクスポートに切り替える	**[ncident report (インシデントレポート)]** タブが開いている場合は、**[Switch to export (エクスポートに切り替える)]** をクリックして **[Export (エクスポート)]** タブに戻ります。
優先ストリームプロファイル	**[Preferred stream profile (優先ストリームプロファイル)]** フィールドで、ストリームプロファイルを選択します。
プレビュー	録画をプレビューするには、エクスポートされたリスト内で録画をクリックして再生します。同じカメラからの録画の場合のみ、複数の録画をプレビューできます。
保存	エクスポートリストをファイルに保存するには、**[Save (保存)]** をクリックします。

[Export (エクスポート)] タブ	
読み込み	以前に保存したエクスポートリストを含める場合は、**[Load (読み込み)]** をクリックします。
エクスポート名	エクスポートされたフォルダーとファイルのカスタム名前を入力します。空白のままにしておくと、AXIS Camera Station Proのデフォルトの命名規則が適用されます。
カメラ名とタイムスタンプの追加	このオプションを選択して、エクスポートされたフォルダーとファイルの名前に、カメラ名とタイムスタンプを追加します。
開始時間と終了時間を調整する	録画の開始時刻と終了時刻を調整するには、プレビューのタイムラインに移動し、開始時刻と終了時刻を調整します。タイムラインには、選択した録画の前後に最大30分間の録画が表示されます。
スナップショットを追加	スナップショットを追加するには、プレビュー内のタイムラインを特定の位置までドラッグし、プレビューを右クリックして、**[Add snapshot (スナップショットを追加)]** を選択します。

高度な設定	
ノートを含める	**[Include notes (メモを含める)]** を選択すると、録画のノートが.txtファイルとしてエクスポート先フォルダーに保存され、AXIS File Playerのブックマークとして登録されます。
AXIS File Player を含める	エクスポートする録画にAXIS File Playerを添付するには、**[AXIS File Playerを含める]** を選択します。
プレイリストを作成 (.asx)	Windows Media Playerで使用される.asx形式でプレイリストを作成するには、**[Create playlist(.asx) (プレイリストを作成 (.asx))]** を選択します。録画は録画された順に再生されます。
デジタル署名を追加	画像の改ざんを防止するには、**[Add digital signature (デジタル署名を追加)]** を選択します。このオプションは、.asf形式の録画でのみ使用できます。*エクスポートした録画の再生と検証, on page 35*を参照してください。
Zipファイルにエクスポートする	Zipファイルにエクスポートするには、**[Export to Zip file (Zipファイルにエクスポート)]**」を選択し、必要に応じてパスワードを入力します。

高度な設定	
Export format (エクスポート形式)	[Export format (エクスポート形式)] のドロップダウンメニューから、録画のエクスポート形式を選択します。MP4を選択した場合、エクスポートされる録画にはG.711またはG.726形式の音声は含まれません。
編集済みのビデオエンコーディング	編集された録画に対して、[Edited video encoding(編集済みのビデオエンコーディング)]で、ビデオエンコード形式を [Automatic]、[H.264] または [M-JPEG] に設定できます。Automaticを選択すると、M-JPEG形式にはM-JPEGが使用され、その他のすべての形式にはH.264が使用されます。

エクスポートのユーザー権限

録画のエクスポートやインシデントレポートの生成には、適切な権限が必要です。どちらか一方または両方に権限を持つことができます。[Recordings (録画)]タブで をクリックすると、[connected export (接続されたエクスポート)]タブが開きます。

権限を設定するには、*ユーザー権限, on page 143*に移動します

エクスポートする前に録画を編集する

動く物体のぼかし

1. [Export (エクスポート)]タブまたは[Incident report (インシデントレポート)]タブで、録画を選択して をクリックします。
2. 対象の動く物体が最初に出現する場所にタイムラインを移動します。
3. [Bounding boxes > Add (境界ボックス > 追加)] をクリックして新しい境界ボックスを追加します。
4. [Bounding box options (境界ボックスのオプション)]> [Size (サイズ)] に移動し、サイズを調整します。
5. 境界ボックスを移動して物体の上に配置します。
6. [Bounding box options {境界ボックスのオプション) > [Fill (塗りつぶし)] に移動し、[Pixelated (モザイク)] または [Black (黒)] に設定します。
7. 録画が再生されたら、物体を右クリックし、[Add key frame (キーフレームを追加する)] を選択します。
8. 連続するキーフレームを追加するには、録画の再生中に境界ボックスを移動して物体を覆います。
9. タイムラインを移動し、録画全体にわたって境界ボックスが物体を覆っていることを確認します。
10. 終了位置を設定するには、最後のキーフレームのひし形を右クリックし、[Set end (終了位置の設定)] を選択します。これにより、終了位置以降のキーフレームが削除されます。

注

ビデオには、複数のバウンディングボックスを追加できます。境界ボックスが重なっている場合、重なった領域には、黒、ピクセル化、クリアの順で塗りつぶしが適用されます。

すべて削除	すべての境界ボックスを削除するには、[Bounding boxes > Remove all (境界ボックス > すべて削除)] をクリックします。
キーフレームの削除	キーフレームを削除するには、キーフレームを右クリックし、[Remove key frame (キーフレームの削除)] を選択します。

背景をぼかして動く物体を表示する

1. 境界ボックスを作成します。*動く物体のぼかし, on page 33*を参照してください。
2. [Bounding box options > Fill (バウンディングボックスのオプション > 塗りつぶし)] に移動し、[Clear (透明)] に設定します。
3. [Video background (ビデオ背景)] に移動し、[Pixelated (モザイク)] または [Black (黒)] に設定します。

これを除くすべてをモザイク化	リストから複数の境界ボックスを選択し、右クリックして [Pixelate all but this (これを除くすべてをモザイク化)] を選択します。選択した境界ボックスは [Clear (クリア)] になり、選択されていない境界ボックスは [Pixelated (モザイク)] になります。

バウンディングボックスの生成

分析データから境界ボックスを生成するには、カメラの分析機能がオンになっていることを確認します。*ストリームプロファイル, on page 56*を参照してください。

1. [Export (エクスポート)]タブまたは[Incident report (インシデントレポート)]タブで、をクリックします。
2. [Generate bounding boxes (境界ボックスの生成)] をクリックします。
3. 境界ボックスが移動する物体をカバーしていることを確認します。必要に応じて調整します。
4. 境界ボックスまたはビデオの背景の塗りつぶしを選択します。

AXIS Video Content Streamを使用したビデオ編集の強化

ビデオ編集を改善するには、ファームウェア5.50～9.60を適用したカメラにAXIS Video Content Stream 1.0アプリケーションをインストールします。AXIS Camera Station Proでは、システムにカメラを追加すると、自動的にインストールが開始されます。*カメラアプリケーションをインストールする*を参照してください。

エクスポートする前に録画を編集する

エクスポートした録画の再生と検証

画像の改ざんを防ぐために、パスワードの有無に関わらず、エクスポートされた録画にデジタル署名を追加できます。AXIS File Playerを使用して、デジタル署名を検証し、録画の変更を確認します。

1. エクスポートした録画を含むフォルダーに移動します。エクスポートしたZipファイルがパスワードで保護されている場合は、パスワードを入力してフォルダーを開きます。
2. AXIS File Playerを開きます。エクスポートされた録画は自動的に再生されます。
3. AXIS File Player で、 をクリックして、録画ノートを表示します。
4. **[Add digital signature (デジタル署名を追加)]**を使用してエクスポートした録画のデジタル署名を検証する:
   4.1. **[Tools (ツール)] > [Verify digital signature (デジタル署名の検証)]** に移動します。
   4.2. パスワードで保護されている場合は、**[Validate with password (パスワードを使用する)]** を選択してパスワードを入力します。
   4.3. 検証結果を表示するには、**[Verify (確認する)]** をクリックします。

インシデントレポートのエクスポート

[Incident report (インシデントレポート)] タブから、インシデントレポートをローカルストレージデバイスまたはネットワークの場所にエクスポートできます。録画、スナップショット、ノートをインシデントレポートに含めることができます。

開始前に、エクスポートの権限があることを確認してください。*エクスポートのユーザー権限, on page 33*を参照してください。

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。

インシデントレポート

インシデントレポートの生成

1. **[Recordings (録画)]** タブで、カメラまたはビューを選択します。
2. 録画をエクスポートリストに追加します。*録画のエクスポート, on page 30*を参照してください。
3. **[Switch to incident report (インシデントレポートに切り替える)]** をクリックして、**[incident report (インシデントレポート)]** タブに移動します。
4. **[Create report (レポートの作成)]** をクリックします。
5. インシデントレポートを保存するフォルダーを選択します。
6. **[OK]**をクリックします。**[Tasks (タスク)]** タブに、インシデントレポートのエクスポートタスクが表示されます。

エクスポートフォルダーには以下が含まれます。

- AXIS File Player。
- 選択した形式の録画。
- .txtファイル ([**Include notes (ノートを含める)**] を選択した場合)。
- インシデントレポート。

- プレイリスト (複数の録画をエクスポートした場合)

音声	エクスポートした録画から音声を除外するには、**[Audio (音声)]** の列のチェックボックスをオフにします。エクスポートした録画に常に音声を含めるには、[Configuration (設定)] > [Server (サーバー)] > [Settings (設定)] > [Export (エクスポート)] で、**[Include audio when adding recordings to export (エクスポートする録画の追加時に音声を含める)]** を選択します。
	録画を編集するには、録画を選択して、 をクリックします。*エクスポートする前に録画を編集する, on page 33*を参照してください。
	録画のメモを編集するには、録画を選択して、 をクリックします。
	録画をエクスポートリストから削除するには、録画を選択して、 をクリックします。
インシデントレポートに切り替える	**[Export (エクスポート)]** タブが表示されている場合、**[Switch to incident report (インシデントレポートに切り替える)]** をクリックして **[Incident report (インシデントレポート)]** タブに移動します。
優先ストリームプロファイル	[Preferred stream profile (優先ストリームプロファイル)] のドロップダウンからストリームプロファイルを選択します。
プレビュー	録画をプレビューするには、エクスポートリスト内で録画をクリックして再生します。同じカメラからの録画の場合のみ、複数の録画をプレビューできます。
保存	インシデントレポートをファイルに保存するに、**[Save (保存)]** をクリックします。
読み込み	以前に保存したインシデントレポートを読み込むには、**[Load (読み込み)]** をクリックします。
説明	**[Description (説明)]** フィールドには、説明テンプレートに既定のデータが自動的に入力されます。インシデントレポートに含める追加情報も入力できます。
カテゴリー	レポートが属するカテゴリを選択します。
参照ID	**[Reference ID (参照ID)]** は自動的に生成されます。必要に応じて、手動で変更することもできます。これはインシデントレポートを識別する一意のIDです。
ノートを含める	**[Include notes (メモを含める)]** を選択すると、録画のノートが.txtファイルとしてエクスポート先フォルダーに保存され、AXIS File Playerのブックマークとして登録されます。

編集済みのビデオエンコーディング	編集された録画に対して、[Edited video encoding(編集済みのビデオエンコーディング)]で、ビデオエンコード形式を[Automatic]、[H.264] または [M-JPEG] に設定できます。Automaticを選択すると、M-JPEG形式にはM-JPEGが使用され、その他のすべての形式にはH.264が使用されます。
開始時間と終了時間を調整する	録画の開始時刻と終了時刻を調整するには、プレビューのタイムラインに移動し、開始時刻と終了時刻を調整します。タイムラインには、選択した録画の前後に最大30分間の録画が表示されます。
スナップショットを追加	スナップショットを追加するには、プレビュー内のタイムラインを特定の位置に移動し、プレビューを右クリックして、[Add snapshot (スナップショットを追加)] を選択します

手動による録画

注

複数の AXIS Camera Station Proサーバーに接続した場合、接続されている任意のサーバーの録画を手動で開始および停止できます。これを行うには、[Selected server (選択したサーバー)] のドロップダウンリストからサーバーを選択します。

メインメニューから手動録画を開始および停止するには:

1. ☰ > [Actions (アクション)] > [Record manually (手動による録画)]に移動します。
2. 1台以上のカメラを選択します。
3. 録画を開始するには、[Start (開始)] をクリックします。
4. 録画を停止するには、[Stop (停止)]をクリックします。

[Live view (ライブビュー)] タブから手動録画を開始および停止するには:

1. [Live view] (ライブビュー) に移動します。
2. カメラのライブビューフレームにカーソルを合わせます。
3. 録画を開始するには、[REC] をクリックします。録画中はビューフレームに赤いインジケーターが表示されます。
4. 録画を停止するには、[REC] をクリックします。

スマート検索1

Smart search 1 (スマート検索1) を使用して、録画内で定義された領域内で動きがあった箇所を検索します。

検索速度を上げるには、ストリームプロファイル設定で [**Include analytics data (分析データを含める)**] を選択します。*ストリームプロファイル*を参照してください。

Smart search 1 (スマート検索1) を使用する:

1. ＋をクリックし、**[Smart search 1 (スマート検索1)]**タブを開きます。
2. 検索するカメラを選択します。
3. 対象範囲を調整する.形状には最大20個の点を追加できます。点を削除するには、その点を右クリックします。
4. [**Short-lived objects filter (一時的な物体フィルター)**] と [**Small objects filter (小さな物体フィルター)**] を使用して、望ましくない結果をフィルター処理して除去します。
5. 検索する日付と時間の範囲を選択します。Shiftキーを使用して日付の範囲を選択します。
6. [**検索**] をクリックします。

検索結果が [**Results (結果)**] タブに表示されます。1つ以上の結果を右クリックし、録画をエクスポートすることができます。

Short-lived objects filter (一時的な物体フィルター)	物体が検索結果に含まれるために、対象範囲内に存在している必要がある最小時間。
Small objects filter (小さな物体フィルター)	物体が検索結果に含まれるために必要な最小サイズ。

スマート検索1

スマート検索2

Smart search 2 (スマート検索2) を使用して、録画内で移動する人物や車両を検索します。

注

スマート検索2には以下が必要です。

- RTSPを介した分析メタデータのストリーミング。
- 9.60より前のAXIS OSを搭載するカメラにおけるAXIS Video Content Stream。*カメラアプリケーションをインストールする, on page 73*を参照してください。
- AXIS Camera Station Proサーバーとカメラの時刻同期。

AxisカメラでSmart search 2 (スマート検索2) をオンにすると、AXIS Camera Station Proはそのカメラからのメタデータの録画を開始し、それを使用してシーン内の物体を分類します。これにより、フィルターを使用して対象を探すことができます。

注

- 動体検知は検知されてもビデオがない場合があるため、連続録画の使用をお勧めします。
- 検索結果で録画のプレビューを表示する場合は、H.264形式を使用してください。
- 最適な色の分類を行うため、照明条件がカメラの仕様を満たしていることを確認してください。必要な場合は、追加の照明を使用します。

ワークフロー

1. *スマート検索2の設定, on page 182*
2. AXIS Camera Station Proサーバーとカメラの時刻同期を設定します。*時刻同期, on page 77*を参照してください。
3. フィルターを作成するか、既存のフィルターを読み込みます。*フィルターで検索する, on page 39*を参照してください。
4. 検索結果を管理します。*スマート検索の結果, on page 43*を参照してください。

フィルターで検索する

1. [**Configuration > Smart search 2 > Settings (設定 > スマート検索2 > 設定)**] をクリックして、スマート検索2で使用するカメラを選択します。
2. ＋をクリックし、**[Smart search 2 (スマート検索2)]**タブを開きます。
3. 検索条件を定義します。
4. [**検索**] をクリックします。

検索に予想以上に時間がかかる場合は、以下を1つ以上試して検索を高速化してください。

- 重要なカメラや頻繁に使用するカメラについては、バックグラウンドサーバー分類を有効にしてください。
- カメラに受信フィルターを適用して無関係な検知を減らす。
- 検索期間を短縮する。
- 検索のカメラの台数を減らす。
- エリア、物体の向き、大きさ、時間を定義し、データの量を小さくする。

カメラ	カメラによる検索を制限するには、[**Cameras (カメラ)**] をクリックして検索に含めるカメラを選択します。
検索期間	期間を指定して検索するには、[**Search interval (検索期間)**] をクリックし、複数日に

	わたる特定の期間を選択するか、期間をカスタマイズします。
人物	人物を検知するには、[Object characteristics (物体の特徴)] > [Pre-classified (事前分類済み)] > [Person (人物)] をクリックし、服の色を選択します。複数の色を選択できます。
車両	車両を検出するには、[Object characteristics (物体の特徴)] > [Pre-classified (事前分類済み)] をクリックし、車両のタイプと色を選択します。車両のタイプ色はそれぞれ複数選択できます。
映像の類似性	画像内の人物の検索結果を使用して、視覚的に類似した人物を検索できます。検索結果項目のコンテキストメニュー を開き、**[Use as visual similarity reference (映像の類似性の参照として使用)]**を選択します。次に、[Search (検索)] をクリックします。 注 類似性検索は、トリミングされた低解像度の人物画像から抽象化された画像データを作成し、他の画像データと比較します。2つの画像データが類似している場合、検索にヒットします。類似性検索は、生体認証データを使用して人物を識別することはありませんが、たとえば、人物の大まかな体型や衣服の色を認識することができます。
フリーテキスト検索	フリーテキスト検索では、自然な言語 (英語のみ) を使用して録画内で検索しているコンテンツを説明することができます。*フリーテキスト検索, on page 41*を参照してください。
範囲	範囲で絞り込むには、[Area (範囲)] をクリックし、カメラを選択して、[Filter by area on this camera (このカメラで範囲で絞り込む)] をオンにします。画像内の対象範囲を調整し、必要に応じて点を追加または削除します。
ライン横断	ライン横断で絞り込むには、[Line crossing (ライン横断)] をクリックし、カメラを選択して、[Filter by line crossing on this camera (このカメラでライン横断で絞り込む)] をオンにします。画像内のラインを調整し、必要に応じて点を追加または削除します。
大きさ	大きさで絞り込むには、[Size (大きさ)] をクリックし、カメラを選択して、[Filter by size on this camera (このカメラで大きさで絞り込む)] をオンにします。画像全体に対するパーセンテージで最小の高さと幅を調整します。
所要時間	所要時間で絞り込むには、[Duration (所要時間)] をクリックし、カメラを選択して、[Filter by duration on this camera (このカメラで所要時間で絞り込む)] をオンにします。最小期間を秒単位で調整します。

速度	速度で絞り込むには、[**Speed (速度)**] をクリックし、カメラを選択して、[**Filter by speed on this camera (このカメラで速度で絞り込む)**] をオンにします。フィルターに含める速度範囲を指定します。 注 速度フィルターは、レーダーデバイスやフュージョンカメラなど、速度を検知できる製品で使用できます。
不明な物体の検知	スマート検索2が不明として分類した検知を含めるには、[**Object characteristics (物体の特徴)**] を選択した後、**Unknown object detections (未知の物体の検知)**] を選択します。
	フィルターを保存するには、をクリックし、フィルターの名前を入力して**[Save (保存)]** をクリックします。 他のユーザーとフィルターを共有するには、[**Share with other users (他のユーザーと共有)**] を選択します。 既存のフィルターを置き換える場合は、をクリックして既存のフィルターを選択し、**[Replace (置換)]**をクリックします。
	最近の検索を読み込むには、 > **[Recent searches (最近の検索)]**をクリックし、検索を選択します。 保存したフィルターを読み込むには、 > **[Saved filters (保存したフィルター)]** > [をクリックし、フィルターを選択します。 別のユーザーと共有しているフィルターを読み込むには、 > **[Shared filters (共有フィルター)]**をクリックし、フィルターを選択します。
	フィルターをリセットするには、をクリックし、**[Reset (リセット)]**をクリックします。

フリーテキスト検索

フリーテキスト検索では、自然な言語を使用して録画内で検索しているコンテンツを説明することができます。

注

- フリーテキスト検索には最低16GBのRAMが必要です。
- フリーテキスト検索にはインターネット接続が必要です。
  - フリーテキスト検索は、初回設定時およびAxisによるモデルのアップグレード時に、インターネット接続を使用してaxis.comからAIモデルをダウンロードします。
  - フリーテキスト検索は週に一度、Axisのクラウドサービスに接続し、AIモデルが将来の規制や要件に準拠するために更新が必要かどうかを確認します。接続に失敗した

場合、システムが再接続されるまでフリーテキスト検索を使用することはできません。

– フリーテキスト検索は、すべての処理をサーバー上でローカルに実行し、ビデオ、画像、プロンプトテキストを送信するためにインターネット接続を**使用しません**。

フリーテキスト検索をオンにするには、以下の手順に従います。

1. [**Configuration (設定)**] タブを開きます。
2. [**Smart search 2 (スマート検索2)**] > [**Settings (設定)**] に移動します。
3. [Free text search (フリーテキスト検索)] で、[**Use free text search (フリーテキスト検索を使用する)**] を選択します。システムがaxis.comから必要なファイルをダウンロードします。

検索するには、以下の手順に従います。

1. [**Smart search 2 (スマート検索2)**] タブを開きます。
2. [**Object characteristics (物体の特徴)**] をクリックします。
3. [**Free text (フリーテキスト)**] をクリックします。
4. [**Show (表示)**] をクリックして、使用目的、制限、責任ある使用に関する情報を読みます。
5. 検索に含めるものと除外するものを入力します。
6. [**検索**] をクリックします。

プロンプトのガイドライン

プロンプトには次の構成を使用することをお勧めします。

```
{person, vehicle or other object} + {specific action or attributes of the person, vehicle, or object}
```

いくつかのキーワードを使用して、物体を説明します。例:

プロンプト	コメント
赤いセーターと黒い帽子を着用した女性	概ね的確
赤い服の女性	やや曖昧すぎる
身長約156cmの女性。黄色のアクセントが入ったくり色のカーディガンを羽織り、80年代後半を彷彿とさせる黄褐色の縁取りが施された黒い日よけ帽子をかぶっている。	説明が細かすぎる

監視の専門家でない人と話しているように状況を説明します。例:

プロンプト	コメント
木のそばに停車している黄色いピックアップトラック	概ね的確
無人車両、ナンバープレート: CHY67F、車種: ピックアップトラック、カラー: 黄色、位置: 大きなポプラの木のすぐそば。	警察の報告書のように細かすぎる

フリーテキスト検索が理解される可能性の高い、優れたキーワード:

記述子	例
物体の種類	人、自動車、自転車、動物
カラー	黄
天気	晴れ
有名ブランド (自動車ブランド、ロゴ)	UPSトラック

不適切なキーワード:

記述子	例
テキスト	「踊るクマの立ち入り禁止」という店の看板。
感情に関する手がかり	An angry looking man (怒っているように見える男性)
計測	14 people milling around a town square (町の広場をうろつく14人)
地方の俗語	A red hoover (赤い掃除機)

検索クエリのモデレーション

安全で品位のある環境を維持するために、侮辱的、有害、または有毒なコンテンツを含む検索はブロックされる場合があります。当社のシステムは、自然言語処理モデルと、検索禁止カテゴリーおよび禁止語のカスタムリストを使用して、各検索クエリを評価しています。

禁止語に同意できない場合、または新しい語を提案したい場合は、スマート検索のユーザーインターフェースから匿名でフィードバックを送信できます。当社のチームが受け取って確認します。

注

- フリーテキスト検索は英語にのみ対応しています。
- フリーテキスト検索は静止画像を理解します。falling (転倒)、running (走行)、stealing (盗み) などの行動については、より多くの情報が必要なため、適切な結果を得ることが困難な場合があります。
- フリーテキスト検索はクロップされた画像を使用するため、周囲の環境が含まれない可能性があります。city (都市)、urban (都会)、park (公園)、garden (庭)、lake (湖)、beach (ビーチ) などのシーンに関するキーワードを使用すると、結果の精度が低下する可能性があります。
- フリーテキスト検索機能の限界やベストプラクティスなどの詳細については、ホワイトペーパー「*Free text search in AXIS Camera Station Pro*」(AXIS Camera Station Proのフリーテキスト検索) を参照してください。

スマート検索の結果

	同じイベントに属する可能性が高い検知をグループ化するには、時間間隔ごとにグループ化します。 ドロップダウンメニューから間隔を選択します。
最新の検知を先頭に	スマート検索2では、最新の検知を先頭に、降順で検索結果が表示されます。最も古い検知結果を先頭に表示するには、 [Oldest first

	(もっとも古い検知結果を先頭に)]をクリックします。
信頼度	検索結果をさらに絞り込むには、[Confidence level (信頼度)] をクリックして、信頼度を設定します。信頼度が高くすると、不確実な分類が除外されます。
Columns (列)	検索結果のサムネールのサイズを調整するには、[Columns (列)] をクリックし、列数を変更します。
Detection view (検知ビュー)	検知された物体のトリミングしたビューをサムネールとして表示するには、[Detection view (検知ビュー)] を選択します。

制限事項

- スマート検索2は、プライマリ (ノンクロップ) ビューエリアのみに対応しています。
- スマート検索2は、ノンクロップキャプチャーモードのみに対応しています。
- ARTPEC-7以上、ファームウェアバージョン10.6未満のデバイスを使用し、ミラーリングおよび回転されたカメラストリームでスマート検索2を使用すると、問題が発生する場合があります。
- ネットワーク遅延が高いか大きく変動する場合、時刻同期の問題が発生し、分析機能メタデータに基づく検知の分類に影響する可能性があります。
- 物体タイプの分類と検知の精度は、高圧縮レベルによる低画質、大雨や雪などの気象条件のほか、カメラでの低解像度、大きい歪み、広い視野、または過度の振動から、悪影響を受けます。
- スマート検索2は、小さくて遠くにある物体を検知できない場合があります。
- 色の分類は、暗闇や赤外線照明では機能しません。
- 装着式ボディカメラはサポートされていません。
- レーダーは人物と他の車両のみを検知できます。レーダーのバックグラウンドサーバー分類をオンにすることはできません。
- サーマルカメラでは、物体の分類挙動は予測不能です。
- スマート検索2では、PTZプリセット位置が変更された場合、および位置が変更されてからしばらくの間は物体が検知されません。
- ライン横断およびエリアフィルターには、PTZ位置の変更は影響しません。

データ検索

データ検索を使用すると、外部ソースからデータを検索できます。ソースとは、イベントに関するデータを生成するシステムまたはデバイスです。詳細については、*外部データソース, on page 77*を参照してください。
例:

- アクセスコントロールシステムによって生成されたイベント。
- AXIS License Plate Verifierによりキャプチャーされたナンバープレート。
- AXIS Speed Monitorによりキャプチャーされた速度。

AXIS Camera Station Proが外部データを保存する期間変更するには、**[Configuration (設定)] > [Server (サーバー)] > [Settings (設定)] > [External data (外部データ)]** に移動します。

データを検索するには:

1. ＋をクリックして**[Data search (データ検索)]**を選択します。
2. 検索間隔を選択します。
3. ドロップダウンリストからデータソースタイプを選択します。
4. **[Search (検索)]** をクリックし、追加のフィルターを適用します。利用可能なフィルターはデータソースのタイプによって異なります。
5. 検索フィールドに任意のキーワードを入力します。*検索の最適化, on page 46*を参照してください。
6. [**検索**] をクリックします。

ビューを使用して設定している場合、データ検索はソースから生成されたデータをブックマークします。リスト内のデータをクリックすると、イベントに関連付けられた録画に移動します。

時間間隔	
ライブ	リアルタイムデータを検索するには、時間間隔として [**Live (ライブ)**] を選択します。データ検索では、最大3,000のライブデータイベントを表示できます。ライブモードは検索演算子をサポートしません。
過去1時間 – 過去30日間	あらかじめ設定された期間のデータを検索するには、利用可能なオプションから選択します：過去1時間、4時間、12時間、24時間、48時間、7日間、または30日間。
カスタム	特定の期間でデータを検索するには、**カスタム**を選択し、開始日時と終了日時を設定します。

検索結果は、さまざまなタイプのソースでフィルタリングできます。

データソースのタイプ	
All data (すべてのデータ)	このオプションには、コンポーネントと外部ソースの両方からのデータが含まれます。

アクセスコントロール	このコンポーネントからのデータのみを含める場合は、このオプションを使用します。アクセスコントロールを使用すると、ドアやゾーン、カード所持者、イベントタイプに基づいたフィルタリングが可能になります。
サードパーティ	設定されたコンポーネント以外のサードパーティソースからのデータを含める場合は、このオプションを使用します。

データソースに応じて、検索結果に異なる項目が表示される場合があります。例:

検索結果	
サーバー	イベントデータが送信されるサーバー。複数のサーバーに接続する場合にのみ表示されます。
所在地：	ドア名とドアコントローラー名およびIPアドレス。
進入速度	物体がレーダー動体検知 (RMD) ゾーンに進入するときの速度 (時速キロメートルまたは時速マイル)。
等級	物体の分類。例: 車両。

検索結果をPDFまたはテキストファイルにエクスポートするには、[**Download search result (検索結果をダウンロード)**] をクリックします。列の順序の変更や列幅の調整によって、PDF出力時の表のレイアウトを向上させることができます。PDFには最大10列が含まれます。

検索の最適化

より正確な結果を得るために、次の検索演算子を使用できます。

キーワードと完全一致させる場合は、引用符" "を使用します。	• 「"door 1"」と入力して検索すると、「door 1」を含む結果が返されます。 • 「door 1」と入力して検索すると、「door」と「1」の両方を含む結果が返されます。
ANDを使用すると、すべてのキーワードを含む一致が見つかります。	• 「door AND 1」と入力して検索すると、「door」と「1」の両方を含む結果が返されます。 • 「"door 1" AND "door forced open"」と入力して検索すると、「door 1」と「door forced open」の両方を含む結果が返されます。
任意のキーワードを含む一致を見つけるには、ORまたは | を使用します。	• 「"door 1" OR "door 2"」と入力して検索すると、「door 1」または「door 2」を含む結果が返されます。 • 「door 1 OR door 2」と入力して検索すると、「door」、「1」または「 2」を含む結果が返されます。
括弧 ( ) は、ANDまたはORとともに使用します。	• 「(door 1 OR door 2) AND "Door forced open"」と入力して検索すると、以下のいずれかを含む結果が返されます。 – 「ドア1」と「ドアのこじ開け」

	– 「ドア2」と「ドアのこじ開け」 • 「door 1 AND (door (forced open OR open too long))」と入力して検索すると、以下のいずれかを含む結果が返されます。 – 「ドア1」と「ドアのこじ開け」 – 「ドア1」と「ドアの開放時間が長すぎる」
特定の列を数字で絞り込むには、>、>=、<、または <=を使用します。	• [Max speed] > 28を検索すると、Max speed (最大速度) の列で28を超える数値が含まれる結果が返されます。 • [Average speed] < = 28」を検索すると、Average speed (平均速度列) の列で28以下の数値が含まれる結果が返されます。
特定の列内のテキストを検索するには、CONTAINSを使用します。	• 「[Cardholder] CONTAINS Oscar」を検索すると、[Cardholder] 列 (カード所持者) に「Oscar」が含まれるデータが返されます。 • 「[Door] CONTAINS "door 1"」を検索すると、[Door] 列 (ドア) に「door 1」が含まれるデータが返されます。
特定の列での完全一致を検索するには、=を使用します。	[CardholderId] = ABC123を検索すると、Cardholder (カード保持者) の列で「ABC123」に一致する結果のみが返されます。

設定

[Configuration (設定)] タブでは、接続されたデバイスの管理、およびクライアントとサーバーの設定ができます。 + をクリックし、**[Configuration (設定)]** を選択して **[Configuration (設定)]** タブを開きます。

デバイスの設定

AXIS Camera Station Proでは、装置とは、IPアドレスを有するネットワーク製品を意味します。カメラとは、ビデオソースを意味し、たとえばネットワークカメラや、マルチポートのビデオエンコーダの (アナログカメラに接続された) ビデオポートを指します。例を挙げると、4ポートビデオエンコーダは、4台のカメラに対応する1台の装置です。

注

- AXIS Camera Station ProはIPv4アドレスを持つデバイスのみに対応しています。
- ビデオポートごとに1つのIPアドレスを持つビデオエンコーダもあります。この場合、AXIS Camera Station Proによって各ビデオポートは1台のカメラに対応する1台の装置として扱われます。

AXIS Camera Station Proでは、装置の例は次のとおりです。

- ネットワークカメラ。
- 1つ以上のビデオポートを持つビデオエンコーダ。
- カメラ以外の補助デバイス (例: I/O音声デバイス、ネットワークスピーカー、ドアコントローラーなど)。
- インターコム。

ここから以下を行うことができます。

- カメラおよびビデオ機能を持たないデバイスの追加。*デバイスの追加*を参照してください。
- 接続するカメラの環境設定を編集します。*カメラ*を参照してください。
- カメラ以外のデバイスの環境設定を編集します。*その他の装置*を参照してください。
- 解像度やフォーマットなど、ストリームプロファイルを編集します。*ストリームプロファイル*を参照してください。
- 画像設定をリアルタイムで調整します。*画像の設定*を参照してください。
- PTZプリセットを追加または削除します。*PTZプリセット*を参照してください。
- 接続された装置の管理と保守を行います。*デバイスの管理*を参照してください。
- 外部データソースを管理します。*外部データソース, on page 77*を参照してください。

デバイスの追加

注

- このシステムは、ビューエリアを個々のカメラと見なします。使用する前に、カメラにビューエリアを作成する必要があります。*ビューエリアの使用*を参照してください。
- デバイスを追加すると、デバイスの時刻が AXIS Camera Station Proサーバーと同期されます。
- 装置のホスト名には、å、ä、öなどの特殊文字を使用しないことをお勧めします。

1. デバイス、ビデオストリーム、または事前録画済みビデオを見つけます。
   - *デバイスの検索, on page 50*
   - *ビデオストリームの検索, on page 51*
   - *録画済みのビデオを見つける, on page 51*

2. *デバイス、ビデオストリーム、または録画済みのビデオを追加する, on page 51*

装置を追加する前に、装置ステータス列に表示されている問題をすべて解決する必要があります。

(空白)	ステータスが表示されていない場合は、そのデバイスを AXIS Camera Station Proに追加できます。
通信中	AXIS Camera Station Proサーバーがデバイスへのアクセスを試みています。
デバイスの証明書が信頼されていません	AXIS Camera Station ProがデバイスのHTTPS証明書が信頼された発行者によって署名されていることを確認できません。リンクをクリックして新規HTTPS証明書を発行するか、AXIS Camera Station Proに既存の証明書を信頼するように指示します。
証明書認証局の有効期限が切れました	装置証明書を発行した認証局が失効しています。リンクをクリックして新規HTTPS証明書を発行するか、AXIS Camera Station Proに既存の証明書を信頼するように指示します。
デバイス証明書のアドレスが一致していません	デバイスのアドレスが証明書内のアドレスと一致していません。リンクをクリックして新規HTTPS証明書を発行するか、AXIS Camera Station Proに既存の証明書を信頼するように指示します。
通信エラー	AXIS Camera Station Proがデバイスと通信できません。
パスワードを入力します。	AXIS Camera Station Proがデバイスへのアクセスに使用する認証情報を認識しません。リンクをクリックして、デバイスの管理者アカウントのユーザー名とパスワードを入力します。デフォルトでは、入力したユーザー名とパスワードが、ユーザーの存在するすべての装置に対して、AXIS Camera Station Proによって使用されます。
パスワードを設定	rootアカウントとパスワードが設定されていないか、デバイスが使用するパスワードがデフォルトのままです。リンクをクリックして、rootユーザーのパスワードを設定します。 • パスワードを入力するか、**[Generate (生成)]** をクリックしてパスワードを取得します。生成されたパスワードのコピーを保存することをお勧めします。 • ステータスが`Set password`になっているすべてのデバイスにこのパスワードを使用するように選択します。 • デバイスでパスワードポリシーが適用されている場合、パスワードポリシーインジケーターに、パスワードが要件を満たしているかどうかが表示されます。詳細については *ユーザーを管理する。, on page 70*を参照してください。

サポートされないモデルです:	AXIS Camera Station Proがデバイスモデルをサポートしていません。
サポート対象外のファームウェア	デバイスのファームウェアは古くなっています。デバイスを追加する前に更新してください。
故障デバイス	AXIS Camera Station Proによって取得された装置パラメーターが破損しています。
チルトの向きを設定	リンクをクリックし、カメラの取り付け方法に応じてチルトの向きを [Ceiling (天井)]、[Wall (壁)]、または [Desk (デスク)] から選択します。一部のカメラモデルでは、チルトの向きの設定が必要です。
非対応のONVIFデバイス	AXIS Camera Station Proがこのサードパーティ製デバイスに対応していません。
サポートされていない装置	AXIS Camera Station Proがこのタイプのデバイスに対応していません。

注

新規HTTPS証明書は AXIS Camera Station Proから発行され、自動更新されます。

デバイスの検索

表示されていない装置を検索するには:

1. **[Configuration (設定)] > [Devices (デバイス)] > [Add devices (デバイスの追加)]** に移動します。
2. 実行中のネットワーク検索を停止するには、[**キャンセル**] をクリックします。
3. **[Manual search (手動検索)]** をクリックします。
4. 1つ以上のIP範囲内にある複数の装置を検索する手順は、以下のとおりです。
   4.1. **[Search one or more IP ranges (1つまたは複数のIP範囲を検索)]** を選択します。
   4.2. IP範囲を入力します。例: 192.168.10.*, 192.168.20-22.*, 192.168.30.0-50
   - グループ内のすべてのアドレスを対象とするには、ワイルドカードを使用します。
   - アドレスの範囲を指定するには、ダッシュを使用します。
   - コンマを使用して複数の範囲を区切る。

   4.1. デフォルトのポート80を変更する場合は、ポートの範囲を入力します。例:80, 1080-1090
   - ポートの範囲を指定するには、ダッシュを使用します。
   - コンマを使用して複数の範囲を区切る。

   4.1. [**検索**] をクリックします。
5. 1つ以上の特定のデバイスを検索する手順は、以下のとおりです。
   5.1. **[Enter one or more hostnames or IP addresses (ホスト名またはIPアドレスを1つ以上入力)]** を選択します。
   5.2. ホスト名かIPアドレスを、カンマで区切って入力します。
   5.3. [**検索**] をクリックします。
6. **[OK]**をクリックします。

ビデオストリームの検索

以下をサポートするビデオストリームを追加できます。

- プロトコル:RTSP、HTTP、HTTPS
- ビデオエンコード方式:M-JPEG (HTTPおよびHTTPS)、H.264 (RTSP)
- 音声エンコーディング:AAC、G.711 (RTSP)

サポートされるビデオストリームのURLスキーム:

- `rtsp://<address>:<port>/<path>`
  例: `rtsp://<address>:554/axis-media/media.amp`
- `http://<address>:80/<path>`
  例: `http://<address>:80/axis-cgi/mjpg/video.cgi?date=1&clock=1&resolution=1920x1080`
- `https://<address>:443/<path>`
  例: `https://<address>:443/axis-cgi/mjpg/video.cgi?date=1&clock=1&resolution=1920x1080`

1. **[Configuration (設定)] > [Devices (デバイス)] > [Add devices (デバイスの追加)]** に移動します。
2. **[Enter stream URLs (ストリームURLを入力)]** をクリックし、1つ以上のストリームURLを入力します (複数の場合はカンマ区切り)。
3. **[追加]** をクリックします。

録画済みのビデオを見つける

事前に録画したビデオを .mkv形式で AXIS Camera Station Proに追加できます。

要件:

- ビデオエンコード方式:M-JPEG、H.264、H.265
- 音声エンコーディング:AAC

1. `C:\ProgramData\Axis Communications\AXIS Camera Station Server`の下にフォルダ**PrerecordedVideos**を作成します。
2. フォルダーに.mkvファイルを追加します。
3. 事前に録画したビデオの歪みを補正するには、.mkvファイルと同じ名前の.dewarpファイルをフォルダーに追加します。詳細については、*画像の設定, on page 62*を参照してください。
4. **[Configuration > Devices > Add devices (設定 > デバイス > デバイスの追加)]** に移動して **[Include prerecorded video (事前録画済みのビデオを含める)]** をオンにします。
   事前録画済みビデオと、システムによって提供された事前録画済みビデオが見つかります。

デバイス、ビデオストリーム、または録画済みのビデオを追加する

1. マルチサーバーシステムでは、**[Selected server (選択したサーバー)]** ドロップダウンリストからサーバーを選択します。
2. **[Configuration (設定)] > [Devices (デバイス)] > [Add devices (デバイスの追加)]** に移動します。
3. 装置、ビデオストリーム、または事前録画済みビデオを選択します。**[追加]** をクリックします。
4. **[Close (閉じる)]** をクリックして設定をスキップし、後で続行します。以下の手順に従って設定を続行します。

4.1. [Quick configuration (クイック設定)] を選択して、基本設定を行います。AXIS Site Designerプロジェクトをインポートする場合は、[Site Designer configuration (Site Designer設定)] を選択します。詳細については、*AXIS Site Designerプロジェクトのインポート*を参照してください。

4.2. [Add image overlay for date, time, and text (日付、時刻、テキストの画像オーバーレイを追加する)] を選択して、オーバーレイが設定されていないAxisカメラにオーバーレイを追加します。

4.3. [Next (次へ)] をクリックします。

4.4. [Recording method (録画方法)] の設定を選択します。

4.5. [Next (次へ)] をクリックします。

4.6. [Retention time (保存期間)] と [Recording storage (録画ストレージ)] を選択し、[Finish (終了)] をクリックして設定を適用します。

AXIS Site Designerプロジェクトのインポート

AXIS Site Designerはオンラインの設計ツールです。Axisの製品およびアクセサリーを使用するサイトを構築するのに役立ちます。

AXIS Site Designerでサイトを作成している場合、このプロジェクト設定を AXIS Camera Station Proにインポートできます。アクセスコードまたはダウンロードした設定ファイルを使用してプロジェクトにアクセスできます。

AXIS Site Designerプロジェクトを AXIS Camera Station Proにインポートする:

1. アクセスコードを生成するか、プロジェクトファイルをダウンロードします。
   1.1. MyAxisアカウントで*http://sitedesigner.axis.com*にサインインします。
   1.2. プロジェクトを選択し、プロジェクトページに移動します。
   1.3. [Share (共有)] をクリックします。
   1.4. AXIS Camera Station Proサーバーがインターネットに接続されている場合は、[Generate code (コードを生成)] をクリックします。接続されていない場合は、[Download settings file (設定ファイルをダウンロード)] をクリックします。
2. AXIS Camera Station Proクライアントで、[Configuration > Devices > Add devices (設定 > 装置 > デバイスの追加)] に移動します。
3. デバイスを選択し、[Add (追加)] をクリックします。
4. [Site Designer設定] を選択して [次へ] をクリックします。
5. [アクセスコード] を選択し、アクセスコードを入力します。ダウンロードした設定ファイルを使用するには、[Choose file (ファイルの選択)] を選択します。
6. Import (インポート) をクリックします。AXIS Camera Station ProがIPアドレスまたは製品名によってプロジェクトと選択したデバイスの一致を試みます。一致しない場合は、ドロップダウンメニューから正しいデバイスを選択します。
7. [Next (次へ)] をクリックします。
8. [Recording method (録画方法)] の設定を選択します。これらの設定は、プロジェクトの設定と一致しないカメラに適用されます。
9. [Next (次へ)] をクリックします。
10. [Retention time (保存期間)] と [Recording storage (録画ストレージ)] を選択し、[Finish (終了)] をクリックして設定を適用します。

AXIS Camera Station ProがAXIS Site Designerプロジェクトから次の設定をインポートします。

	エンコーダ、ビデオデコーダ、ドアコントローラー、レーダー検知器、スピーカー:	カメラ、インターカム、F/FAシリーズ
名前とスロットが設定されたスケジュール	✓	✓
名前、アイコンの色、アイコンの場所、および項目名が設定されたマップ	✓	✓
名称	✓	✓
説明	✓	✓
連続録画: スケジュールと、フレームレート、解像度、ビデオエンコーディング、圧縮などの録画プロファイル		✓
動きによるトリガー録画: スケジュールと、フレームレート、解像度、ビデオエンコーディング、圧縮などの録画プロファイル		✓
Zipstreamの強度		✓
ライブビューと録画の音声設定		✓
録画の保存期間		✓

注

- 録画プロファイルを1つ定義した場合、またはAXIS Site Designerプロジェクトに同一の録画プロファイルが2つある場合、AXIS Camera Station Proはプロファイルを「中」に設定します。
- AXIS Site Designerプロジェクトで両方の録画プロファイルを定義している場合、AXIS Camera Station Proは連続録画プロファイルを「中」に設定し、動きによってトリガーされる録画を「高」に設定します。
- AXIS Camera Station Proはアスペクト比を最適化するため、解像度はAXIS Site Designerプロジェクトとは異なる場合があります。
- デバイスに内蔵マイクロフォンまたはスピーカーが搭載されている場合、AXIS Camera Station Proは音声設定を行うことができます。外部音声デバイスを使用するには、インストール後にオンにします。
- AXIS Camera Station Proは、AXIS Site Designerの設定が異なる場合でも、音声設定をインターコムに適用しません。インターコムでは、ライブビューのときのみ、音声が常にオンになります。

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。

サードパーティデバイスの追加

AXIS Camera Station Proには、Axis製品を追加するのと同じ方法でサードパーティ製の装置を追加できます。*デバイスの追加*を参照してください。

注

サードパーティ製の装置を、ビデオストリームとして AXIS Camera Station Proに追加することもできます。*ビデオストリームの検索, on page 51*を参照してください。

AXIS Camera Station Proは、IEC62676-2-31およびIEC62676-2-32に準拠し、サードパーティ製のデバイスの以下の機能に対応しています。

- カメラ検出
- ビデオエンコード方式:M-JPEG、H.264
- 音声エンコード方式:G.711 (1方向、装置から AXIS Camera Station Pro)
- カメラごとに1ビデオプロファイル
- ライブビュー
- 連続録画および手動録画
- 再生
- 録画のエクスポート
- デバイスイベントトリガー
- PTZ

ビューエリアの使用

一部のカメラモデルでは、ビューエリアがサポートされています。AXIS Camera Station Proでは、[Add devices (デバイスの追加)] ページでビューエリアが個別のカメラとして一覧表示されます。*デバイスの追加*を参照してください。

注

- ネットワークカメラのすべてのビューエリアが、AXIS Camera Station Proライセンスで許可されているカメラの総数のうちの1台のカメラとしてカウントされます。
- 追加できるカメラの数はライセンスによって異なります。

AXIS Camera Station Proでビューエリアを使用するには、まずカメラでビューエリアを有効にする必要があります。

1. **[設定] - [デバイス] - [カメラ]** を選択します。
2. カメラを選択し、[アドレス] 列でリンクをクリックします。
3. カメラの設定ページで、ユーザー名とパスワードを入力してログインします。
4. 設定の場所に関する手順については、**[Help (ヘルプ)]** をクリックしてください。この場所はカメラの機種やファームウェアによって異なります。

装置を交換する

デバイスを交換しても、既存の設定と録画を維持できます。新しいカメラに設定されているビデオストリーム数が、古いカメラと同じである必要があります。

装置を交換するには:

1. 交換するデバイスがクラウドストレージを使用している場合は、My Systemsの [**Cloud storage (クラウドストレージ)**] から、デバイスのクラウドストレージをオフにしてください。
2. [**Configuration (設定)**] タブを開き、[**Devices (デバイス)**] > [**Management (管理)**] に移動します。

3. 交換する装置を選択し、 をクリックします。
4. [Replace device (デバイスの交換)] ダイアログで、古い装置と交換する装置を選択します。
5. Finish (終了) をクリックします。
6. [Replaced device (デバイスの交換完了)] ダイアログが表示され、デバイスが正常に交換されたことを確認します。[OK]をクリックします。
7. 交換したデバイスがクラウドストレージを使用していた場合は、AXIS Camera Station Proサーバーでサービスを再起動します。その後、My Systemsでデバイスのクラウドストレージをオンにします。*個々のカメラのクラウドストレージをオンにする*を参照してください。
8. 新しいデバイスの設定を確認し、設定が正しく、正常に動作していることを確認します。該当する場合:
   8.1. 装置でPTZプリセットを再設定します。
   8.2. 削除されたI/Oポートを追加し、関連するアクションルールを更新します。
   8.3. 古いカメラがビデオ動体検知ACAPアプリケーションではなく内蔵ビデオ動体検知機能を使用していた場合は、動体設定を再設定します。
   8.4. 古いカメラがフェイルオーバーによる録画を使用していた場合は、SDカードを挿入するか、ストレージ選択設定で [Failover recording (フェイルオーバーによる録画)] をオフにします。

カメラ

[Configuration (設定)> [Devices (デバイス)] > [Cameras (カメラ)] に移動すると、システムに追加されているすべてのカメラのリストが表示されます。

このページでは次の操作ができます。

- カメラのアドレスをクリックして、そのwebインターフェースを開きます。この操作は、AXIS Camera Station Proクライアントと装置の間にNATまたはファイアウォールがない場合にのみ可能です。
- カメラの設定を編集します。*カメラ設定を編集する*を参照してください。
- カメラを削除します。これにより、削除されたカメラに関連付けられているすべての録画データ (ロックされているものを含む) も削除されます。

カメラ設定を編集する

カメラ設定を編集するには:

1. [設定] - [デバイス] - [カメラ] を選択します。
2. カメラを選択して [編集] をクリックします。

有効	ビデオストリームの録画と表示を禁止するには、[Enabled (有効)] の選択をクリアします。その場合にも、録画とライブビューを設定することはできます。
チャンネル	[Channel (チャンネル)] がマルチポートビデオエンコーダで使用可能な場合は、ポート番号を選択します。 [Channel (チャンネル)] がビューエリアで使用可能な場合は、ビューエリアに対応する番号を選択します。

その他の装置

[Configuration (設定)> [Devices (デバイス)] > Other devices (他のデバイス)] に移動すると、ドアコントローラー、音声デバイス、I/Oモジュールなどビデオ機能を持たないデバイスのリストが表示されます。一覧には、ドアコントローラー、音声装置、I/Oモジュールが記載されます。

対応製品の詳細については、*www.axis.com*を参照してください。*他のデバイスから音声を使用する*を参照してください。

このページでは次の操作ができます。

- 装置のアドレスをクリックして、そのwebインターフェースを開きます。この操作は、AXIS Camera Station Proクライアントと装置の間にNATまたはファイアウォールがない場合にのみ可能です。
- 名前、アドレス、パスワードなど、装置の設定を編集します。
- 装置を削除する.

他のデバイスの設定の編集

カメラ以外の装置の名前を変更するには:

1. **[設定]** - **[デバイス]** - **[他のデバイス]** を選択します。
2. デバイスを選択し、[**編集**] をクリックします。
3. 装置の新しい名前を入力します。

ストリームプロファイル

ストリームプロファイルは、解像度、ビデオ形式、フレームレート、圧縮など、ビデオストリームに影響を与える設定のグループです。**[Configuration (設定)]** > **[Devices (デバイス)]** > **[Stream profiles (ストリームプロファイル)]** に移動し、**[Stream profiles (ストリームプロファイル)]** ページを開きます。すべてのカメラのリストがページに表示されます。

ライブビューおよび録画の設定で、次のプロファイルを使用することができます。

高 - 最高の画質と解像度を実現するように最適化されます。

中 - 高画質とパフォーマンスのバランスを取るように最適化されます。

低 - パフォーマンスに最適化されます。

注

ライブビューおよび録画では、ストリームプロファイルはデフォルトで **[Automatic (自動)]** に設定されています。ビデオストリームの使用可能なサイズに応じて、ストリームプロファイルが **[High (高)]**、**[Medium (中)]**、または **[Low (低)]** に自動的に変更されます。

カメラのストリームプロファイル

AXIS Camera Station Proは、カメラにストリームプロファイルを自動的に追加し、録画ルールをカメラで直接設定できるようにします。プロファイルは、カメラのwebインターフェースの**[Stream profiles (ストリームプロファイル)]** に表示され、カメラ名とプロファイルレベルを組み合わせた名前が付けられます (例: "Camera 1_ACS_Pro_High")。

カメラのプロファイルは、以下の場合に追加または更新されます。

- カメラが AXIS Camera Station Proに追加された場合。
- AXIS Camera Station Proでストリームプロファイルが変更された場合。
- 毎晩の更新処理実行時。

AXIS Camera Station Proからカメラが削除されると、AXIS Camera Station Proによって作成されたストリームプロファイルはそのカメラから削除されます。

注

M-JPEGまたはMPEG-4形式のストリームプロファイルは、カメラに追加されません。

ストリームプロファイルの編集

1. [Configuration > Devices > Streaming profiles (設定 > 装置 > ストリームプロファイル)] を選択し、設定するカメラを選択します。
2. [Video profiles (ビデオプロファイル)] の下で、解像度、ビデオ形式、フレームレート、圧縮を設定します。
3. [Audio (音声)] の下で、マイクとスピーカーを設定します。
4. [Advanced (詳細設定)] の下で、分析データ、FFmpegストリーミング、PTZオートトラッキング物体インジケーター、カスタマイズされたストリーム設定を設定します。これらの設定は、製品によっては利用できない場合もあります。
5. [適用] をクリックします。

ビデオプロファイル

エンコーダ	• 使用可能なオプションは、装置のビデオエンコーダの設定によって異なります。サードパーティのデバイスでのみ利用できます。 • ビデオエンコーダ設定は1つのビデオプロファイルに対してのみ使用できます。 • 装置に1つしかエンコーダ設定がない場合、[Medium (中)] プロファイルだけが使用できます。
解像度	使用可能なオプションは、カメラのモデルによって異なります。解像度が高いほど画像は高画質になりますが、必要な帯域幅とストレージ容量が大きくなります。
フォーマット	使用可能なオプションは、カメラのモデルによって異なります。ほとんどのカメラは、**H.264**および**M-JPEG**に対応しています。H.264は、M-JPEGよりも少ない帯域幅とストレージ容量を必要とします。一部のカメラは**H.265**に対応しています。この形式では、圧縮率が若干向上しますが、より多くの処理能力が必要になります。当社の最新ジェネレーションのカメラはAV1に対応しています。この形式は優れた圧縮率と、切り替え可能なオーバーレイなどの数々の新機能を提供します。 AV1について詳しくは、*AV1製品*ページを参照してください。お使いのカメラがAV1に対応しているかどうかを確認するには、*対応カメラ*のページを参照してください。
Frame rate (フレームレート):	実際のフレームレートは、カメラのモデル、ネットワーク環境、コンピューターの設定によって異なります。
圧縮	低い値を設定すると画質が向上しますが、必要な帯域幅とストレージ容量が大きくなります。

注

- ファームウェアバージョン5以降を搭載するカメラのみ、音声のドロップダウンリストに表示されます。
- 5台以上のカメラが同じ音声ソースを使用する場合、ソースカメラに過負荷がかかり、性能が低下することがあります。

Zipstream

強度	H.264またはH.265ストリームのビットレート低減のレベルは、Zipstreamの強度によってリアルタイムで決定されます。このオプションは、ZipstreamをサポートするAxisデバイスでのみ使用できます。	**デフォルト**	装置のwebインターフェースページで設定されたZipstream設定を使用します。
		オフ	なし
		低	ほとんどのシーンで、視認できる画質変化なし.
		中	一部のシーンで、低ノイズと、関心の低い領域における詳細部分のわずかな画質低下が見られる.
		高	多くのシーンで、低ノイズと、関心の低い領域における詳細部分の画質低下が見られる.
		高	さらに多くのシーンで、低ノイズと、関心の低い領域における詳細部分の画質低下が見られる.
		極高	ほとんどのシーンで、低ノイズと、関心の低い領域における詳細部分の画質低下が見られる.

ストレージ用に最適化	Zipstreamは、[Optimize for storage (ストレージ用に最適化する)] プロファイルを使用して、ビデオストリームをストレージ用に最適化します。このプロファイルは、より高度な圧縮ツールを使用し、デフォルトのZipstream設定よりストレージの使用量を低減します。また、動きの多いシーンでもビットレートをさらに下げることができます。 • asf形式は、この機能で使用されるBフレームに対応していません。 • この機能は、AXIS S30シリーズレコーダーに録画されたビデオには影響しません。 • この機能を使用するには、AXIS OS 11.7.59以降が必要です。		

音声

マイク:	マイクをカメラに関連付けるには、[Built-in microphone or line in (内蔵マイクロフォンまたはライン入力)] または他の装置のマイクを選択します。*他のデバイスから音声を使用するを参照してください。*
スピーカー:	スピーカーをカメラに関連付けるには、[Built-in speaker or line out (内蔵スピーカーまたはライン出力)] または他のデバイスのスピーカーを選択します。送話には、コンピューターに接続されたマイクを使用します。*他のデバイスから音声を使用するを参照してください。*
マイクの使用対象:	1つまたは2つのストリームのマイク音声をオンにします。音声は、ライブビューと録画、ライブビューのみ、または録画のみオンにすることができます。

AXIS Audio Manager Proに接続すると、カメラに関連付けられた音声デバイスとしてAXIS Audio Manager Proサーバーから音声デバイスを選択することも可能です。詳しくは、*AXIS Audio Manager Proを設定する, on page 182*を参照してください。

高度

分析データを含める	ビデオストリーミング中にスマート検索用のデータを収集できるようにするには、[Include analytics data (分析データを含める)] を選択します。分析データをサポートするAxisデバイスでのみ使用できます。*スマート検索1*用にデータを収集すると、ビデオストリーミングの待ち時間が長くなることがあります。
FFmpegを使用	サードパーティ製デバイスとの互換性を改善するには、[Use FFmpeg (FFmpegを使用)] を選択してFFmpegストリーミングをオンにします。サードパーティのデバイスでのみ利用できます。
PTZオートトラッキング物体インジケーターを表示	PTZカメラによって検知された物体インジケーターをライブビューで表示するには、[Show PTZ autotracking object indicators (PTZオートトラッキングオブジェクトインジケーターを表示)] を選択し、ビデオストリームバッファ時間を最大2000ミリ秒に設定します。AXIS PTZオートトラッキング機能を搭載した Axis PTZカメラでのみ利用できます。AXIS Camera Station ProでAXIS PTZ Autotrackingを設定する詳細なワークフローについては、「*AXIS PTZ Autotrackingの設定*」を参照してください。
ストリームのカスタマイズ	特定のプロファイルのストリーム設定をカスタマイズするには、そのプロファイルの設定を&で区切って入力します。たとえば、「`overlays=off&color=0`」と入力すると、そのカメラのオーバーレイが非表示になります。 カスタム設定は、既存の設定を上書きします。機密情報をカスタム設定に含めないでください。

解像度、フレームレート、圧縮、ビデオ形式、音声などの**プロファイル設定をカスタマイズ**するには、カメラを選択して設定します。同じモデルで、設定方法が同じであるカメラは、複数台同時に設定できます。*設定の構成*を参照してください。

録画のプロファイル設定をカスタマイズする方法については、*録画の方法*を参照してください。

たとえば、**クライアントと**サーバーの間の接続が低速な場合、AXIS Camera Station Proライブビューの解像度やフレームレートを制限して、帯域幅の使用量を低減 AXIS Camera Station Proできます。帯域幅の使用量については、*ストリーミング*を参照してください。

他のデバイスから音声を使用する

ライブビューや録画で、他のカメラ以外のデバイスや外部デバイスからの音声をネットワークカメラまたはビデオエンコーダで使用できます。

1. カメラ以外の装置を AXIS Camera Station Proに追加します。*デバイスの追加*を参照してください。
2. デバイスからの音声を利用できるよう、カメラを設定します。*ストリームプロファイル*を参照してください。
3. ライブビューまたはや録画の音声をオンにします。*ストリームプロファイル*を参照してください。

次の例は、*AXIS Camera Station Pro ビデオチュートリアル*にあります。

- 音声デバイスを設定し、ライブアナウンスを行う.
- アクションボタンを作成して、動きが検知されたときに音声を手動で再生する.
- 動きが検知されたときに音声を自動的に再生.
- AXIS Camera Station Proで音声クリップをスピーカーに追加する.

画像の設定

AXIS Camera Station Proに接続しているカメラの画像を設定することができます。

注

画像設定の変更は即反映されます。

画像を設定するには:

1. **[Configuration (設定)] > [Devices (デバイス)] > [Image configuration (画像設定)]** に移動します。AXIS Camera Station Proにすべてのカメラのリストが表示されます。
2. カメラを選択し、リストの下にビデオフィードをリアルタイムで表示します。**[検索する文字を入力]** フィールドを使用して、リスト内の特定のカメラを検索できます。
3. 画像を設定する:

輝度 - 画像の輝度を調整します。値を大きくするほど画像が明るくなります。

カラーレベル - 色の彩度を調整します。小さい値を選択すると色の彩度が低下します。0にすると画像が白黒で表示されます。最大値にすると最高彩度になります。

シャープネス - 画像のシャープさを調整します。シャープネスを高く設定すると、特に微光の状況では画像ノイズが増えることがあります。シャープネスの値が高いと、高コントラスト部分の周囲に画像のアーティファクト (ぎざぎざなど) が生じるおそれがあります。低い値を設定すると画像ノイズは減りますが、ややぼやけた画像になります。

コントラスト - 画像のコントラストを調整します。

ホワイトバランス - ドロップダウンリストで、ホワイトバランスのオプションを選択します。ホワイトバランスは、光源の色温度にかかわらず、画像の色を調整するために使用されます。**[Automatic (自動)]** または **[Auto (自動)]** を選択すると、カメラが光源を識別して自動的に色を補

正します。満足の行く結果が得られない場合は、光源の種類に対応するオプションを選択してください。使用可能なオプションは、カメラのモデルによって異なります。

画像を回転 - 画像の回転角度を設定します。

画像のイメージ自動回転 - オンに設定すると、画像の回転が自動的に調整されます。

画像を反転 - オンにすると画像が反転します。

逆光補正 - 電球などの明るい光源によって画像の他の部分が暗くなりすぎる場合は、この機能をオンにします。

ダイナミックコントラスト (ワイドダイナミックレンジ) - オンにすると、画像内の光と影のコントラストがかなり強い場合、露出が向上します。スライダーを使用してレベルを調整します。低光量条件の場合はオフにしてください。

カスタム歪み補正設定 - カメラのレンズパラメーター、光学センター、およびチルトの向きを含む.dewarpファイルをインポートすることができます。[**Reset (リセット)**] をクリックすると、パラメーターが元の値にリセットされます。

カスタム歪み補正を設定する:

1. 以下のパラメーターを含む.dewarpファイルを作成します。
   - 必須：`RadialDistortionX`、`RadialDistortionY`、`RadialDistortionZ`、`TiltOrientation`。`TiltOrientation`に指定できる値は、`wall`、`desk`、および`ceiling`です。
   - オプション：`OpticalCenterX`と`OpticalCenterY`。光学センターを設定する場合は、これら2つのパラメーターを両方とも含める必要があります。
2. [**Import (インポート)**] をクリックして、.dewarpファイルを参照します。

以下は.dewarpファイルの例です。

```
RadialDistortionX=-43.970703 RadialDistortionY=29.148499 RadialDistortionZ=715.732193
TiltOrientation=Desk OpticalCenterX=1296 OpticalCenterY=972
```

PTZプリセット

パン/チルト/ズーム (PTZ) は、カメラをパン (左右に移動)、チルト (上下に移動)、ズームイン、ズームアウトする機能です。

[Configuration (設定)] > [Devices (デバイス)] > [PTZ presets (PTZプリセット)] に移動します。AXIS Camera Station ProにPTZに対応しているカメラのリストが表示されます。カメラをクリックすると、カメラで使用可能なすべてのプリセットが表示されます。[**Refresh (更新)**] をクリックすると、プリセットリストが更新されます。

PTZが使用可能なカメラは次のとおりです。

- PTZカメラ (メカニカルPTZが搭載されているカメラ)
- デジタルPTZ機能がオンになっている固定カメラ。
- PTZプリセットに対応したONVIFカメラ。

デジタルPTZは、カメラに内蔵されている設定ページからオンにすることができます。詳細については、カメラのユーザーズマニュアルを参照してください。設定ページを開くには、デバイスの管理ページに進み、カメラを選択して **[Address (アドレス)]** 列のリンクをクリックします。

PTZプリセットは、AXIS Camera Station Proおよびカメラの設定ページで設定できます。AXIS Camera Station ProでPTZプリセットを設定することをお勧めします。

- カメラの設定ページでPTZプリセットを設定する場合は、プリセット内でストリームのみを表示できます。ライブビューでのPTZの動きは、表示および記録ができます。
- AXIS Camera Station ProでPTZプリセットを設定する場合は、カメラのストリーム全体を閲覧できます。ライブビューでのPTZの動きは表示されず、録画されません。

注

カメラのコントロールキューがオンのときはPTZ (パン/チルト/ズーム)機能を使用できません。コントロールキューの詳細や、オン・オフの方法については、カメラのユーザーマニュアルを参照してください。

プリセットを追加するには:

1. **[設定] - [デバイス] - [PTZプリセット]** を選択し、リストからカメラを選択します。
2. メカニカルPTZを搭載したカメラの場合は、PTZコントロールを使用して、カメラビューを目的の位置に移動します。デジタルPTZを搭載したカメラの場合は、マウスホイールを使用してズームインし、カメラビューを目的の位置にドラッグします。
3. [**追加**] をクリックし、新しいプリセットの名前を入力します。
4. **[OK]**をクリックします。

- プリセットを削除するには、選択して [**Remove (削除)**] をクリックします。選択したプリセットが AXIS Camera Station Proとカメラの両方から削除されます。

デバイスの管理

装置管理には、AXIS Camera Station Proに接続された装置の管理とメンテナンスを行うためのツールが用意されています。

[Configuration (設定)] > [Devices (デバイス)] > [Management (管理)] に移動し、**[Manage devices (デバイスの管理)]** ページを開きます。

*ファームウェアアップグレード設定, on page 130*で新しいファームウェアバージョンの自動確認を設定した場合は、デバイスの新しいファームウェアバージョンが利用可能になるとリンクが表示されます。リンクをクリックして、ファームウェアバージョンをアップグレードします。*ファームウェアのアップグレード*を参照してください。

*AXIS Camera Station Proの更新, on page 136*で新しいソフトウェアバージョンの自動確認を設定した場合は、新しい AXIS Camera Station Proのバージョンが利用可能になるとリンクが表示されます。リンクをクリックして、新しいバージョンのをインストールします。

AXIS Camera Station Proが追加されたすべてのデバイスのリストを表示します。**[検索する文字を入力]** フィールドを使用して、リスト内のデバイスを検索できます。列を表示/非表示にするには、ヘッダー行を右クリックし、表示する列を選択します。ヘッダーをドラッグ＆ドロップして、列の順序を並べ替えることができます。

デバイスのリストには以下の情報が含まれています。

- **Name (名前):** デバイスが複数のカメラが接続されたビデオエンコーダの場合、または複数のビューエリアを持つネットワークカメラの場合、デバイスの名前または関連付けられたすべてのカメラの名前のリスト。
- **MAC address (MACアドレス):** デバイスのMACアドレス。
- **Status (ステータス):** デバイスのステータス。
  - **OK:** 確立されたデバイス接続の標準の状態。
  - **Maintenance (メンテナンス):** デバイスはメンテナンス中のため、一時的にアクセスできません。
  - **Not accessible (アクセスできません):** デバイスとの接続を確立できません。
  - **Not accessible over set hostname (設定されたホスト名でアクセスできません):** そのホスト名でデバイスへの接続を確立できません。
  - **Server not accessible (サーバーにアクセスできません):** デバイスが接続するサーバーとの接続を確立できません。
  - **Enter password (パスワードを入力してください):** 有効な認証情報が入力されるまで、このデバイスにアクセスすることはできません。リンクをクリックし、有効な

ユーザー認証情報を入力します。デバイスが暗号化接続に対応している場合、デフォルトで暗号化されたパスワードが送信されます。

- Set password (パスワードを設定してください):rootアカウントとパスワードが設定されていないか、デバイスで使用されているパスワードがデフォルトのままになっています。リンクをクリックして、rootユーザーのパスワードを設定します。
  - パスワードを入力するか、[Generate (生成)] をクリックして、デバイスで許容される長さを上限としたパスワードを自動的に生成します。生成されたパスワードのコピーを保存することをお勧めします。
  - [Set password] ステータスが存在するすべての装置でこのパスワードを使用する選択肢を有効にします。
  - デバイスがHTTPSをサポートしている場合は、[Enable HTTPS (HTTPSを有効にする)] を選択してHTTPSをオンにします。
- Password type: unencrypted (パスワードタイプ: 暗号化されていません): デバイスが以前に暗号化されたパスワードを使用して接続しているため、デバイスとの接続は確立されません。安全上の理由から、AXIS Camera Station Proは以前に暗号化されたパスワードを使用したデバイスで暗号化されていないパスワードを使用することを許可しません。暗号化に対応している装置では、装置の設定ページで接続のタイプを設定します。
- Certificate error (証明書エラー): デバイスの証明書にエラーがあります。
- Certificate about to expire (証明書の有効期限が間もなく切れます): デバイス上の証明書の有効期限が間もなく切れます。
- Certificate has expired (証明書の有効期限が切れています): デバイスの証明書の有効期限が切れています。
- HTTPS certificate not trusted (HTTPS 証明書が信頼されていません): デバイスのHTTPS証明書は、AXIS Camera Station Proによって信頼されていません。新しいHTTPS証明書を発行するためのリンクをクリックします。
- HTTP failed (HTTP接続失敗): デバイスとのHTTP接続を確立できません。
- HTTPS failed (HTTP接続失敗):: デバイスとのHTTPS接続を確立できません。
- HTTPおよびHTTPS接続に失敗 (pingまたはUDPはOK):デバイスとのHTTPまたはHTTPS接続を確立できません。デバイスはpingおよびUser Datagram Protocol (UDP) 通信には応答します。

- Address (アドレス): デバイスのアドレス。リンクをクリックすると、デバイスの設定ページが開きます。デバイスの追加時にどちらを使用したかに応じて、IPアドレスまたはホスト名が表示されます。*[Device configuration (装置設定)] タブ, on page 76*を参照してください。
- Hostname (ホスト名): デバイスのホスト名 (使用可能な場合)。リンクをクリックすると、デバイスの設定ページが開きます。ホスト名は、完全修飾ドメイン名で表示されます。*[Device configuration (装置設定)] タブ, on page 76*を参照してください。
- Manufacturer (メーカー): デバイスのメーカー。
- Model (モデル): デバイスのモデル。
- Firmware (ファームウェア): デバイスが現在使用しているファームウェアのバージョン。
- DHCP: デバイスがDHCPを使用してサーバーに接続しているかどうかを表示します。
- HTTPS: 装置のHTTPSステータス。*セキュリティ, on page 74*でHTTPSステータスを参照してください。
- IEEE 802.1X: デバイスのIEEE 802.1Xステータス。*セキュリティ, on page 74*でIEEE 802.1Xステータスを参照してください。
- Server (サーバー): デバイスが接続されている AXIS Camera Station Proサーバー。
- タグ: (デフォルトでは非表示) デバイスに付加されているタグ。

- **UPnPフレンドリ名:**(デフォルトでは非表示) UPnP名。デバイスを識別しやすくするために使用する、分かりやすい名前です。

デバイスで次のアクションを実行できます。

- デバイスにIPアドレスを割り当てる。*IPアドレスの割り当て*を参照してください。
- デバイスにパスワードを設定する。*ユーザーを管理する。*を参照してください。
- デバイスのファームウェアをアップグレードする。*ファームウェアのアップグレード*を参照してください。
- デバイスを再起動する。
- デバイスをリストアする：パスワードを含め、ほとんどの設定を工場出荷時の設定にリセットします。アンロードされたカメラアプリケーション、ブートプロトコル (DHCPまたは静的)、静的なIPアドレス、デフォルトルーター、サブネットマスク、システム時刻の設定はリセットされていません。

注

- 不正アクセスを防ぐため、デバイスをリストアした後は必ず新規のパスワードを設定してください。
- リセットするデバイスがクラウドストレージを使用している場合は、リセットする前に、My Systemsの [**Cloud storage (クラウドストレージ)**] から、デバイスのクラウドストレージをオフにしてください。デバイスがリセットされたら、AXIS Camera Station Proサーバーでサービスを再起動し、My Systemsでデバイスのクラウドストレージをオンにします。*個々のカメラのクラウドストレージをオンにする*を参照してください。
- デバイスにカメラアプリケーションをインストールします。*カメラアプリケーションをインストールする*を参照してください。
- デバイスの設定ページで設定を変更した後は、デバイスを再読み込みします。
- デバイスの設定. *デバイスの設定*を参照してください。
- ユーザーを管理する。*ユーザーを管理する。*を参照してください。
- 証明書の管理. *セキュリティ, on page 74*を参照してください。
- 装置データの収集. *装置データの収集*を参照してください。
- IPアドレスまたはホスト名を使用する場合に選択します。*接続, on page 75*を参照してください。
- デバイスにタグを付ける。*タグ*を参照してください。
- デバイスの認証情報を入力する。デバイスを右クリックして **[Advanced (詳細設定)] - [Enter device credentials (デバイスの認証情報の入力)]** を選択し、デバイスのパスワードを入力します。
- デバイスの設定タブに移動し、デバイスを設定します。*[Device configuration (装置設定)] タブ, on page 76*を参照してください。

IPアドレスの割り当て

AXIS Camera Station Proは複数のデバイスにIPアドレスを割り当てることができます。DHCPサーバーから自動的に新規のIPアドレスを取得するか、IPアドレス範囲から割り当てることができます。

IPアドレスの割り当て

1. **[設定] - [デバイス] - [管理]** を選択し、設定するデバイスを選択します。
2. をクリックするか、右クリックして [**Assign IP address (IPアドレスの割り当て)**] を選択します。

3. 装置にアクセスできないなど、装置を設定できない場合は、[Invalid devices (無効な装置)] ダイアログが表示されます。[**Continue (継続)**] をクリックすると、設定できない装置をスキップできます。
4. IPアドレスを割り当てる1台のデバイスを選択する場合、[**Advanced (詳細設定)**] をクリックして **[Assign IP address (IPアドレスの割り当て)]** ページを開きます。
5. [**IPアドレスを自動的に取得する (DHCP)**] を選択して、DHCPサーバーからIPアドレスを自動的に取得します。
6. [**次のIPアドレス範囲を割り当て**] を選択し、IPアドレス、サブネットマスク、デフォルトルーターを指定します。
   IP範囲を指定するには:
   - ワイルドカードを使用。例: 192.168.0.*、または10.*.1.*
   - 最初のIPアドレスと最後のIPアドレスをダッシュで区切って書く。例:192.168.0.10-192.168.0.20 (このアドレス範囲は、192.168.0.10-20に短縮もできます)、または 10.10-30.1.101
   - ワイルドカードと範囲を組み合わせる。例:10.10-30.1.*
   - コンマを使用して複数の範囲を区切る。例: 192.168.0.*,192.168.1.10-192.168.1.20

注

IPアドレス範囲を割り当てる場合、各装置が同じ AXIS Camera Station Proサーバーに接続されている必要があります。

7. **[Next (次へ)]** をクリックします。
8. 現在のIPアドレスと新しいIPアドレスを確認します。デバイスのIPアドレスを変更するには、デバイスを選択して [**IPを編集**] をクリックします。
   - [**Current IP address (現在のIPアドレス)**] セクションには、現在のIPアドレス、サブネットマスク、およびデフォルトルーターが表示されます。
   - [**New IP address (新しいIPアドレス)**] セクションでオプションを編集し、[**OK**] をクリックします。
9. 新しいIPアドレスを確認し、[**完了**] をクリックします。

デバイスの設定

1台の装置から装置設定をコピーするか、設定ファイルを適用することで、複数の装置の一部の設定を同時に行うことができます。

注

1台のデバイスですべての設定を行うには、デバイスの設定ページに移動します。*[Device configuration (装置設定)] タブ, on page 76*を参照してください。

- 設定デバイスの詳細については、*設定方法*を参照してください。
- 設定ファイルの作成方法については、*設定ファイルを作成する*を参照してください。
- コピー可能な設定については、*設定の構成*を参照してください。

設定方法

デバイスはいくつかの異なる方法で設定できます。AXIS Device managementは、設定の方法に基づいてすべてのデバイスを設定します。*デバイスの設定*を参照してください。

選択したデバイスの設定を使用する

注

この方法は、1台のデバイスでのみ利用可能で、既存の設定の一部またはすべてを再利用します。

1. **[設定] - [デバイス] - [管理]** を選択します。

2. 1台のデバイスを右クリックして、[Configure Devices (デバイスの設定)] > [Configure (設定)] を選択します。
3. 適用する設定を選択します。*設定の構成, on page 69*を参照してください。
4. [次へ] をクリックして適用する設定を確認します。
5. [完了] をクリックし、設定をデバイスに適用します。

他のデバイスから設定をコピーする

1. **[設定] - [デバイス] - [管理]** を選択します。
2. デバイスを右クリックして、**[Configure Devices (デバイスの設定)] > [Configure (設定)]** を選択します。さまざまなモデルまたはファームウェアのデバイスを選択できます。
3. [**デバイス**] をクリックして設定を再利用できるデバイスを表示します。
4. 設定をコピーするデバイスを選択し、[OK] をクリックします。
5. 適用する設定を選択します。*設定の構成, on page 69*を参照してください。
6. [次へ] をクリックして適用する設定を確認します。
7. [完了] をクリックし、設定をデバイスに適用します。

設定ファイルを使用する

設定ファイルには、1台のデバイスの設定が含まれています。この設定を使用して複数のデバイスを同時に設定したり、デバイスを向上出荷時の設定にリセットする場合などに、デバイスを再設定したりできます。1台のデバイスから作成された設定を、別のモデルまたはファームウェアのデバイスに適応することができます。これは一部の設定がすべてのデバイスで存在しない場合も可能です。

設定が存在しない場合、または設定を適用できない場合は、AXIS Camera Station Proクライアントの下部にある **[Tasks (タスク)]** タブに **[Error (エラー)]** のステータスが表示されます。タスクを右クリックし、**[Show (表示)]** を選択して、適用できなかった設定の情報を表示します。

注

この方法は経験豊富なユーザー向けです。

1. **[設定] - [デバイス] - [管理]** を選択します。
2. デバイスを右クリックして、**[Configure Devices (デバイスの設定)] > [Configure (設定)]** を選択します。
3. [**設定ファイル**] をクリックして設定ファイルを参照します。設定ファイルの作成方法については、*設定ファイルを作成する, on page 68*を参照してください。
4. .cfgファイルを選択し、[**開く**] をクリックします。
5. [次へ] をクリックして適用する設定を確認します。
6. [完了] をクリックし、設定をデバイスに適用します。

設定ファイルを作成する

設定ファイルには、1台のデバイスの設定が含まれています。これらの設定を他のデバイスにも適用することができます。設定ファイルの使用方法については、*設定方法*を参照してください。

表示されている設定は、AXIS Device Managementからアクセスできるデバイス設定です。特定の設定を検索するには、[**検索する文字を入力**] フィールドを使用します。

設定ファイルを作成するには:

1. **[設定] - [デバイス] - [管理]** を選択します。
2. 設定ファイルを作成するデバイスを選択します。
3. デバイスを右クリックし、**[デバイスの設定] - [設定ファイルの作成]** を選択します。

4. ファイルに含める設定を選択し、設定の値を必要に応じて変更します。*設定の構成*を参照してください。
5. [**次へ**] をクリックして設定を確認します。
6. [**完了**] をクリックして設定ファイルを作成します。
7. [**保存**] をクリックして設定を.cfgファイルに保存します。

設定の構成

デバイスの設定時は、デバイスのパラメーター、アクションルール、および追加の設定を構成することができます。

パラメーター

パラメーターはデバイスの動作を制御する内部設定です。パラメーターの一般的な情報は、*www.axis.com*で製品のユーザーマニュアルを参照してください。

注

- パラメーターの変更は、経験豊富なユーザーだけが行うようにしてください。
- 一部のパラメーターはAXIS Device Managementからアクセスできません。

一部のテキストフィールドには、変数を挿入することができます。この変数は、デバイスに適用される前にテキストに置き換えられます。変数を挿入するには、テキストフィールドを右クリックし、次のように選択します。

- **Insert device serial number variable (デバイスシリアル番号挿入変数):** この変数は、設定ファイルを適用するデバイスのシリアル番号に置き換えられます。
- **Insert device name variable (デバイス名挿入変数):** この変数は、設定ファイルの適用時に使用されているデバイスの名前に置き換えられます。デバイス名は、**[Device management (デバイス管理)]** ページの**[Name (名前)]** の列で確認できます。デバイスの名前を変更するには、**[Cameras (カメラ)]** または **[Other devices (他のデバイス)]** ページに移動します。
- **Insert server name variable (サーバー名挿入変数):** この変数は、設定ファイルの適用時に使用されているサーバーの名前に置き換えられます。サーバー名は、**[Device management (デバイス管理)]**ページの**[Server (サーバー)]** の列で確認できます。サーバーの名前を変更するには、AXIS Camera Station Pro Service Controlに移動します。
- **Insert server time zone variable (サーバーのタイムゾーン挿入変数):** この変数は、設定ファイルの適用時に使用されているサーバーのPOSIXタイムゾーンに置き換えられます。これは、POSIXタイムゾーンパラメーターと共に使用して、複数のタイムゾーンのサーバーからなるネットワーク内のすべてのデバイスに正しいタイムゾーンを設定することができます。

アクションルール

アクションルールは、デバイス間でコピーすることができます。アクションルールの変更は、経験豊富なユーザーだけが行うようにしてください。アクションルールの全般的な情報については、*アクションルール*を参照してください。

追加設定

- **Stream profiles (ストリームプロファイル):** ストリームプロファイルは、ビデオエンコーディング、画像、および音声設定用に事前プログラムされているライブビューの設定プロファイルです。ストリームプロファイルは、デバイス間でコピーすることができます。
- **Motion detection windows (動体検知ウィンドウ):** 動体検知ウィンドウは、カメラの視野に特定のエリアを定義するために使用します。通常、指定されたエリア内で何かが動く (または停止する) たびにアラームが生成されます。動体検知ウィンドウは、デバイス間でコピーすることができます。

ユーザーを管理する。

[Configuration (設定)] > [Devices (デバイス)] > [Management (管理)] に移動し、デバイスのユーザーを管理します。

複数のデバイスのパスワードを設定したりユーザーを削除したりする場合、いずれのデバイスにも存在しないユーザーには ⚠ が表示されます。各ユーザーは、異なるデバイスで異なるロールを持つ場合でも、1回のみ表示されます。

注

アカウントはデバイス固有であり、AXIS Camera Station Proのユーザーアカウントとは関連付けられていません。

パスワードポリシー

一部のデバイスでは、特定の基準を満たすためにパスワードが必要です。1つ以上の選択されたデバイスでパスワードポリシーが適用されている場合、パスワードの強度インジケーターは、パスワードが有効なポリシーを満たしているかどうかを示すパスワードポリシーインジケーターに置き換えられます。

- ポリシーが不要な場合、またはデバイスがONVIF対応の場合は、パスワードの強度インジケーターが通常通り表示されます。
- 異なるポリシーが設定された複数のデバイスを選択した場合、パスワードはそれらのすべての要件を満たす必要があります。
- パスワードが要件を満たしていない場合、**Non-compliant (要件を満たしていません)** と表示されます。情報アイコンにカーソルを合わせると、以下の具体的な要件が表示されます。

長さの要件 - パスワードは15文字以上でなければなりません。

複雑さの要件 - パスワードは12文字以上で、大文字1文字、小文字1文字、数字1桁、特殊文字1文字を含める必要があります。

両方 - 長さと複雑さの要件の両方を満たす必要があります。

パスワードを設定

注

- ファームウェア5.20以降のデバイスでは、64文字のパスワードをサポートします。それより古いファームウェアバージョンのデバイスでは、8文字のパスワードをサポートします。古いファームウェアを搭載したデバイスでは、個別にパスワードを設定することをお勧めします。
- サポートされているパスワードの長さが異なる複数の装置でパスワードを設定する場合、パスワードは、その中で最短の長さに収まるようにする必要があります。
- 許可されていないアクセスを防止したり、セキュリティを向上させるため、AXIS Camera Station Proに追加されたすべての装置をパスワードで保護することを強くお勧めします。

パスワードに使用できる文字は以下のとおりです。

- アルファベットA～Z、a～z
- 数字 0～9
- スペース、カンマ (,)、ピリオド (.)、コロン (:)、セミコロン (;)
- !、"、#、$、%、&、'、(、+、*、-、)、/、<、>、=、?、[、\、^、-、`、{、|、~、@、]、}

デバイスのユーザーのパスワードを設定する:

1. [Configuration > Devices > Management > Manage devices (設定 > デバイス > 管理 > デバイスの管理)] を選択します。
2. デバイスを選択し、 をクリックします。装置を右クリックして [User Management > Set password (ユーザー管理 > パスワードを設定)] を選択することもできます。

3. ユーザーを選択します。
4. パスワードを入力するか、[Generate (生成)] をクリックして強力なパスワードを生成します。
5. [OK]をクリックします。

注

[Use this password for all devices without a factory default password (工場出荷時にパスワード設定がされていないすべてのデバイスでこのパスワードを使用する)] を選択すると、ステータスが[Set password (パスワードを設定)] になっているすべてのデバイスにそのパスワードが適用されます。パスワードの長さがデバイスでサポートされている最大長を超えると、ダイアログが開く前に通知され、それらのデバイスを除外して続行するかどうか選択できます。

ユーザーを追加

ローカルユーザーまたはActive Directoryユーザーを AXIS Camera Station Proに追加するには:

1. [Configuration > Devices > Management > Manage devices (設定 > デバイス > 管理 > デバイスの管理)] を選択します。
2. デバイスを右クリックして [User Management > Add user (ユーザー管理 > ユーザーを追加)] を選択します。
3. ユーザー名とパスワードを入力し、パスワードを確認します。使用できる文字の一覧は、前述の**パスワードを設定**のセクションを参照してください。
4. [Role (ロール)] のドロップダウンリストからユーザーのアクセス権限を選択します。
   - Administrator 管理者: デバイスに無制限にアクセスできます。
   - Operator (オペレーター): ビデオストリーム、イベント、およびすべての設定 (システムオプションを除く) にアクセスできます。
   - Viewer 閲覧者: ビデオストリームにアクセスできます。
5. [Enable PTZ control (PTZコントロールを有効にする)] を選択し、ユーザーがライブビューでパン、チルト、ズームを実行できるようにします。
6. [OK]をクリックします。

ユーザーを削除

デバイスからユーザーを削除するには:

1. [Configuration > Devices > Management > Manage devices (設定 > デバイス > 管理 > デバイスの管理)] を選択します。
2. デバイスを右クリックして [User Management > Remove user (ユーザー管理 > ユーザーを削除)] を選択します。
3. [User (ユーザー)] のドロップダウンリストから、削除するユーザーを選択します。
4. [OK]をクリックします。

ユーザーを一覧

デバイスのすべてのユーザーとそのアクセス権を一覧にするには:

1. [Configuration > Devices > Management > Manage devices (設定 > デバイス > 管理 > デバイスの管理)] を選択します。
2. 装置を右クリックして [User Management > List users (ユーザー管理 > ユーザーを一覧)] を選択します。
3. [Type to search (検索する文字を入力)] のフィールドを使用して、リスト内のユーザーを検索します。

ファームウェアのアップグレード

ファームウェアはAxisデバイスの機能を決定するソフトウェアです。ファームウェアを最新の状態に保つことで、お使いのデバイスで最新の機能や改善点を利用できるようになります。

新しいファームウェアは、AXIS Camera Station Proを使用してからダウンロードするか、ハードドライブまたはメモリーカードのファイルからインポートすることができます。ダウンロード可能なファームウェアバージョンには、バージョン番号の後に**[Download (ダウンロード)]** のテキストが表示されます。ローカルクライアントにまだダウンロードされていないバージョンのファームウェアの場合、そのバージョン番号の後に **(ファイル)** と表示されています。

ファームウェアをアップグレードする際には、以下のアップグレードタイプを選択できます。

- **Standard (標準):** 選択したファームウェアバージョンにアップグレードして、既存の設定値を維持します。
- **Factory default (工場出荷時の設定):** 選択したファームウェアバージョンにアップグレードし、すべての設定を工場出荷時の値にリセットします。

ファームウェアをアップグレードするには:

1. **[設定]** - **[デバイス]** - **[管理]** を選択し、設定するデバイスを選択します。
2. をクリックするか、右クリックして [**Upgrade firmware (ファームウェアのアップグレード)**] を選択します。
3. デバイスにアクセスできないなど、設定できないデバイスがある場合は、**[Invalid devices (無効なデバイス)]** ダイアログが表示されます。[**Continue (継続)**] をクリックすると、設定できない装置をスキップできます。
4. ファームウェアのアップグレード中は、デバイスにアクセスできません。続行するには、[**はい**] をクリックします。このメッセージを今後表示しない場合は、**[Do not show this dialog again (このダイアログを今後表示しない)]**」を選択し、**[Yes (はい)]** をクリックします。
5. **[Upgrade firmware (ファームウェアのアップグレード)]** ダイアログには、デバイスモデル、各モデルのデバイスの数、既存のファームウェアバージョン、アップグレードで使用可能なファームウェアバージョン、およびアップグレードタイプが表示されます。新しいファームウェアバージョンのダウンロードが可能になると、デフォルトでデバイスがあらかじめリストで選択され、最新のファームウェアバージョンがデバイスごとにあらかじめ選択されます。
   5.1. ダウンロード可能なファームウェアバージョンのリストを更新するには、[**更新を確認**] をクリックします。ローカルのクライアントに保存されている1つ以上のファームウェアファイルを参照するには、[**参照**] をクリックします。
   5.2. アップグレードするデバイスとファームウェアのバージョン、およびアップグレードタイプを選択します。
   5.3. [**OK**] をクリックして、リスト内の装置のアップグレードを開始します。

注

デフォルトでは、ファームウェア更新は選択したすべてのデバイスで同時に行われます。更新の順序は変更することができます。*ファームウェアアップグレード設定*を参照してください。

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。

カメラアプリケーションをインストールする

カメラアプリケーションは、Axisのネットワークビデオ製品にアップロードし、インストールすることができるソフトウェアです。アプリケーションは、デバイスに検知、認識、追跡、カウントなどの機能を追加します。

AXIS Camera Station Proから直接インストールできるアプリケーションもあります。それ以外のアプリケーションは、まず、AxisのWebサイト (*www.axis.com/global/en/products/analytics-and-other-applications*) またはアプリケーションベンダーのWebサイトからダウンロードする必要があります。

これらのアプリケーションは、AXIS Camera Application Platformをサポートするデバイスにインストールすることができます。アプリケーションによっては、特定のファームウェアバージョンまたはカメラモデルにしかインストールできません。

アプリケーションにライセンスが必要な場合は、ライセンスキーファイルとアプリケーションと同時にインストールするか、デバイスの設定ページから後でインストールすることができます。

ライセンスキーファイルを取得するには、*www.axis.com/se/sv/products/camera-applications/license-key-registration#/registration*にアクセスし、アプリケーションに付属するライセンスコードを登録する必要があります。

アプリケーションをインストールできない場合は、*www.axis.com*にアクセスし、インストール先の装置モデルとファームウェアバージョンがAXIS Camera Application Platformをサポートしているかどうかをチェックしてください。

利用可能なカメラアプリケーション:

AXIS Video Motion Detection 4 - 対象範囲内で動く被写体を検知するアプリケーションです。このアプリケーションはライセンスが不要で、ファームウェア6.50以降のカメラにインストールすることができます。製品のファームウェアのリリースノートを確認し、Video Motion Detection 4をサポートしているかどうかを確認することもできます。

AXIS Video Motion Detection 2 - 対象範囲内で動く被写体を検知するアプリケーションです。このアプリケーションはライセンスが不要で、ファームウェア5.60以降のカメラにインストールすることができます。

AXIS Video Content Stream - Axisカメラが動きの追跡データを AXIS Camera Station Proに送信できるようにするアプリケーション。ファームウェア5.50～9.59を搭載したカメラにインストールできます。AXIS Video Content Streamは、AXIS Camera Station Proでのみ使用できます。

その他のアプリケーション - インストールする任意のアプリケーション。インストールを開始する前に、アプリケーションをローカルコンピューターにダウンロードしてください。

カメラアプリケーションをインストールするには:

1. **[設定] - [デバイス] - [管理]** を選択します。
2. アプリケーションをインストールするカメラを選択します。 をクリックするか、右クリックして [**Install camera application (カメラアプリケーションのインストール)**] を選択します。
3. インストールするカメラアプリケーションを選択します。他のアプリケーションをインストールする場合は、[**参照**] をクリックしてローカルのアプリケーションファイルに移動します。**[Next (次へ)]** をクリックします。
4. アプリケーションのインストール後、[**アプリケーションの上書きを許可**] を選択してアプリケーションを再インストールするか、[**アプリケーションのダウングレードを許可**] を選択して旧バージョンのアプリケーションをインストールします。

注

アプリケーションをダウングレードしたり上書きしたりすると、デバイス上の設定がリセットされます。

5. ライセンスが必要なアプリケーションの場合は、**[Install licenses (ライセンスのインストール)]** のダイアログが表示されます。
   5.1. [**はい**] をクリックしてライセンスのインストールを開始してから、[**次へ**] をクリックします。
   5.2. [**参照**] をクリックしてライセンスファイルに移動してから、[**次へ**] をクリックします。

注

AXIS Video Motion Detection 2、AXIS Video Motion Detection 4、またはAXIS Video Content Streamのインストールにはライセンスは不要です。

6. 情報を確認し、[**完了**] をクリックします。カメラのステータスが [OK] から [Maintenance] に変更され、インストールが終了すると [OK] に戻ります。

セキュリティ

HTTPSまたはIEEE 802.1Xを有効にすると、AXIS Camera Station Proの認証局 (CA) は自動的にクライアントとサーバーの証明書に署名し、それらの証明書をデバイスに配布します。CAは、プリインストールされた証明書を無視します。証明書を設定する方法の詳細については、*証明書, on page 148*を参照してください。

HTTPSまたはIEEE 802.1X証明書の管理

注

IEEE 802.1Xを有効にする前に、AXIS Camera Station ProでAxis装置の時刻が同期されていることを確認します。

1. **[設定] - [デバイス] - [管理]** を選択します。
2. デバイスを右クリックし、以下の操作を行います。
   - **[Security (セキュリティ)] > [HTTPS] > [Enable/Update (有効にする/更新する)]** を選択して、HTTPSをオンにするか、デバイスのHTTPSの設定を更新します。
   - **[Security(セキュリティ)] > [IEEE 802.1X] > [Enable/Update (有効にする/更新する)]** を選択して、IEEE 802.1Xをオンにするか、デバイスのIEEE 802.1Xの設定を更新します。
   - **[Security(セキュリティ)] > [HTTPS] > [Disable (無効にする)]** を選択して、デバイスでHTTPSを無効にします。
   - **[Security(セキュリティ)] > [IEEE 802.1X] > [Disable (無効にする)]** を選択して、デバイスでIEEE 802.1Xをオフにします。
   - [**Certificates... (証明書...)**] を選択して、証明書の概要を表示したり、証明書を削除したり、特定の証明書に関する詳細な情報を確認したりします。

注

同じ証明書が複数のデバイスにインストールされている場合、1つの項目として表示されます。これを削除すると、インストールされているすべてのデバイスから証明書が削除されます。

HTTPSとIEEE 802.1Xのステータス

装置の管理ページに、HTTPSとIEEE 802.1Xのステータスが一覧表示されます。

	ステータス	説明
HTTPS	オン	AXIS Camera Station ProはHTTPを使用してデバイスに接続します。
	オフ	AXIS Camera Station ProはHTTPを使用してデバイスに接続します。
	不明。	装置にアクセスできません。

	サポートされていないファームウェア	デバイスのファームウェアが古すぎるため、HTTPSはサポートされていません。
	サポートされていない装置	このデバイスモデルではHTTPSはサポートされていません。
IEEE 802.1X	有効	IEEE 802.1Xは、装置上でアクティブです。
	オフ	IEEE 802.1Xはアクティブではありませんが、デバイス上でアクティブにする準備ができています。
	サポートされていないファームウェア	デバイスのファームウェアが古すぎるため、IEEE 802.1Xはサポートされていません。
	サポートされていない装置	IEEE 802.1Xはこのデバイスモデルではサポートされていません。

装置データの収集

このオプションは、一般的にトラブルシューティングに使用されます。これを使用して、デバイス上の特定の場所に関するデータ収集レポートを含む.zipファイルを生成します。

デバイスデータを収集するには:

1. **[設定] - [デバイス] - [管理]** を選択します。
2. デバイスを右クリックし、[**デバイスデータの収集**] を選択します。
3. **[Data source on selected device (選択した製品のデータソース)]**のセクションで、
   - [**プリセット**] を選択し、一般に使用されているコマンドのドロップダウンリストからいずれかを選択します。

   注

   デバイスによって使用できないプリセットもあります。たとえば、PTZ状態は音声デバイスでは使用できません。
   - [**カスタム**] をクリックして、選択したサーバー上のデータ収集ソースへのURLパスを指定します。
4. **[Save as (名前を付けて保存)]** のセクションで、データ収集の.zipファイルのファイル名とフォルダーの場所を指定します。
5. データ収集が終了した時点で指定のフォルダーを開くように、[**準備完了後に保存先のフォルダーを自動的に開く**] を選択します。
6. **[OK]**をクリックします。

接続

IPアドレスまたはホスト名を使用してデバイスと通信する:

1. **[設定] - [デバイス] - [管理]** を選択します。
2. デバイスを選択して右クリックし、[**Connection (接続)**] を選択します。
   - IPアドレスを使用して装置に接続するには、[**Use IP (IPを使用する)**] を選択します。
   - ホスト名を使用して装置に接続するには、[**Use hostname (ホスト名を使用する)**] を選択します。
   - 認証情報、またはアドレスとポートの設定を変更するには、[**Edit (編集)**] を選択します。

タグ

タグは **[Device management (デバイス管理)]** ページでデバイスの整理に役立ちます。1台のデバイスに複数のタグを設定できます。

モデル、ロケーション、その他の基準をデバイスにタグ付けできます。たとえば、カメラモデルのタグを付けると、そのモデルのすべてのカメラをすばやく検索し、アップグレードすることができます。

1台のデバイスにタグを付けるには:

1. **[設定] - [デバイス] - [管理]** を選択します。
2. デバイスを右クリックして [**デバイスのタグ付け**] を選択します。
3. [Use existing tag **(既存のタグを使用)**] を選択してタグを選択するか、[Create a new tag **(新しいタグを作成)**] を選択してその名前を入力します。
4. **[OK]**をクリックします。

デバイスからタグを削除するには:

1. **[Configuration (設定)] > [Devices (装置)] > [Management (管理)]**に移動して、右上の をクリックします。
2. **[Tags (タグ)]** フォルダーからタグを選択します。タグに関連づけられているすべてのデバイスが表示されます。
3. デバイスを選択して右クリックし、**[Untag devices (デバイスのタグを削除))]** を選択します。
4. **[OK]**をクリックします。

タグを管理するには:

1. **[Configuration (設定)] > [Devices (装置)] > [Management (管理)]**に移動して、右上の をクリックします。
2. **[Device tags (デバイスのタグ)]** ページで:
   - [**タグ**] を右クリックして、[**新しいタグ**] を選択してタグを作成します。
   - タグを右クリックして [**タグの名前を変更**] を選択し、タグに付ける新しい名前を入力します。
   - タグを右クリックして [**タグを削除**] を選択すると、タグを削除できます。
   - をクリックすると、**[Device tags (デバイスのタグ)]** ページをピン留めできます。
   - タグをクリックすると関連付けられているすべてのデバイスが表示され、**[All devices (すべてのデバイス)]** をクリックすると、AXIS Camera Station Proに接続するすべてのデバイスが表示されます。
   - [**警告/エラー**] をクリックすると、アクセスできないデバイスなど、注意が必要なデバイスが表示されます。

[Device configuration (装置設定)] タブ

1台のデバイスですべての設定を行うには:

1. **[設定] - [デバイス] - [管理]** を選択します。
2. 装置のアドレスまたはホスト名をクリックして、装置の設定タブに移動します。
3. 設定を変更します。デバイスの設定については、デバイスのユーザーマニュアルを参照してください。
4. タブを閉じます。デバイスが再読み込みされ、AXIS Camera Station Proの変更が適用されます。

制限事項

- サードパーティ製デバイスの自動認証はサポートされていません。

- サドパーティ製のデバイスに対する一般的なサポートについては、保証いたしかねます。
- ビデオストリームがアクティブな状態でデバイス設定タブを使用すると、負荷が増加して、サーバーマシンのパフォーマンスに影響することがあります。

外部データソース

外部データソースとは、各イベント時点での出来事の追跡に使用できるデータを生成するシステムまたはソースです。*データ検索, on page 45*を参照してください。

[Configuration (設定)] > [Devices (デバイス)] > [External data source (外部データソース)] に移動し、すべての外部データソースのリストを表示します。列見出しをクリックすると、列の値を基準にしてデータが並べ替えられます。

アイテム	説明
名称	外部データソースの名前です。
ソースキー	外部データソースの一意の識別子です。
表示	外部データソースがリンクされているビューです。
サーバー	データソースが接続されているサーバーです。複数のサーバーに接続する場合にのみ表示されます。

外部データソースは、次の場合に自動的に追加されます。

- [Configuration > Access control > Doors and zones (設定 > アクセスコントロール > ドアとゾーン)] の順に移動してドアを作成した場合。
  AXIS Camera Station ProでAxisネットワークドアコントローラーを設定するための完全なワークフローについては、*Axisネットワークドアコントローラーの設定*を参照してください。
- 最初のイベントは、AXIS License Plate Verifierで設定した装置により受信されます。
  AXIS Camera Station ProでAXIS License Plate Verifierを設定するワークフローの詳細については、「*AXIS License Plate Verifierの設定*」を参照してください。

外部データソースをビューで設定している場合、データソースから生成されたデータは、[Data search (データ検索)] タブ内のビューのタイムラインに自動的にブックマークされます。データソースをビューに接続するには:

1. [Configuration > Devices > External data sources (設定 > 装置 > 外部データソース)] を選択します。
2. 外部データソースを選択し、[Edit (編集)] をクリックします。
3. [View (ビュー)] ドロップダウンリストからビューを選択します。
4. [OK]をクリックします。

時刻同期

[Configuration (設定)] > [Devices (デバイス)] > [Time synchronization (時刻同期)] に移動し、[Time synchronization (時刻同期)] ページを開きます。

AXIS Camera Station Proが追加されたすべてのデバイスのリストを表示します。ヘッダー行を右クリックし、表示する列を選択します。ヘッダーをドラッグ＆ドロップして、列の順序を並べ替えることができます。

デバイスのリストには以下の情報が含まれています。

- **Name (名前):** デバイスが複数のカメラが接続されたビデオエンコーダの場合、または複数のビューエリアを持つネットワークカメラの場合、デバイスの名前または関連付けられたすべてのカメラの名前のリスト。
- **Address (アドレス):** デバイスのアドレス。リンクをクリックすると、デバイスの設定ページが開きます。デバイスの追加時にどちらを使用したかに応じて、IPアドレスまたはホスト名が表示されます。*[Device configuration (装置設定)] タブ, on page 76*を参照してください。
- **MAC address (MACアドレス):** デバイスのMACアドレス。
- **Model (モデル):** デバイスのモデル。
- **Enabled (有効)**：時刻同期がオンになっているかどうかが表示されます。
- **NTP source (NTPソース):** デバイスに設定されたNTPソース。
  - **Static (スタティック):** [**Primary NTP server (プライマリNTPサーバー)**] および [**Secondary NTP server (セカンダリNTPサーバー)**] からデバイスのNTPサーバーを手動で指定します。
  - **DHCP:** 装置は、ネットワークからNTPサーバーを動的に受信します。[**DHCP**] を選択すると、[**Primary NTP server (プライマリNTPサーバー)**] および [**Secondary NTP server (セカンダリNTPサーバー)**] を指定できません。
- **Primary NTP server (プライマリNTPサーバー):** デバイスに設定されたプライマリNTPサーバー。[**Static (スタティック)**] を選択した場合にのみ使用できます。
- **Secondary NTP server (セカンダリNTPサーバー):** デバイスに設定されたセカンダリNTPサーバー。セカンダリNTPをサポートするAxis装置に限り使用できます。また [**Static (スタティック)**] が選択されている場合にのみ使用できます。
- **Server time offset (サーバー時刻オフセット):** デバイスとサーバーの時差。
- **UTC time (UTC):** デバイスの協定世界時。
- **Synced (同期済み):** 時刻同期の設定が適用されているかどうかを示します。ファームウェアバージョン9.1以降のデバイスでのみ利用可能です。
- **Time to next sync (次回同期までの残り時間):** 次回同期までの残り時間。

Windows Timeサービス (W32Time) はNetwork Time Protocol (NTP) を使用して、AXIS Camera Station Proサーバーの日時を同期します。以下の情報が表示されます。

- **Server (サーバー):** Windows Timeサービスを実行している AXIS Camera Station Proサーバー。
- **Status (ステータス):** Windows Timeサービスのステース。`Running`または`Stopped`のいずれか。
- **NTP server (NTPサーバー):** Windows Timeサービス用に設定されたNTPサーバー。

時刻同期の設定

1. [**Configuration > Devices > Time synchronization (設定 > 装置 > 時刻同期)**] を開きます。
2. 装置を選択し、[**Enable time synchronization (時刻同期を有効にする)**] を指定します。
3. NTPソースを [**Static (スタティック)**] または [**DHCP**] に指定します。
4. [**Static (スタティック)**] を指定した場合は、プライマリNTPサーバーとセカンダリNTPサーバーを設定します。
5. [**適用**] をクリックします。

Send alarm when the time difference between server and device is largermore than 2 seconds (サーバーとデバイスの時差が2秒を超えた場合にアラームを送信する)	サーバーとデバイスの時差が2秒を超えた場合にアラームを受信する場合、これを選択します。
Set the time zone manually through the device interface (デバイスのインターフェースからタイムゾーンを手動で設定する)	サーバーのタイムゾーンを使用せず、装置の設置場所の別のタイムゾーンを使用する場合は、このオプションを選択します。このオプションを選択した場合は、装置のWebインターフェースからタイムゾーンを手動で設定する必要があります。

ストレージの設定

[Configuration (設定)] - [Storage (ストレージ)] - [Management (管理)] に移動し、(Manage storage (ストレージの管理)] ページを開きます。ここで AXIS Camera Station Proのローカルストレージとネットワークストレージの概要を確認できます。

リスト	
所在地：	ストレージのパスと名前。
割り当て済み	録画に割り当てられている最大ストレージ容量。
使用中	録画データが現在使用しているストレージ容量。

リスト	
ステータス	ストレージのステータス。表示される値: • OK • **Storage full (ストレージがいっぱいです)** ストレージがいっぱいです。ロックされていない最も古い録画が上書きされます。 • **Unavailable (利用できません):** 現在、ストレージ情報を利用できません。たとえば、ネットワークストレージが削除されたか切断された場合などです。 • **Intruding data (データの混入):** AXIS Camera Station Proに割り当てられたストレージ容量を他のアプリケーションからのデータが使用しています。つまり、データベース接続のない録画、いわゆるインデックスなしの録画が、AXIS Camera Station Proに割り当てられたストレージ容量を使用しています。 • **No permissions (権限がありません):** ユーザーにストレージに対する読み取りまたは書き込み権限がありません。 • **Low space (空き容量が少なくなっています):** ドライブの空き容量が15 GB未満で、AXIS Camera Station Proが低すぎると判断しています。エラーや破損を防ぐため、AXIS Camera Station Proはストレージスライダーの位置に関係なく、強制クリーンアップを実行してドライブを保護します。強制クリーンアップの実行中、AXIS Camera Station Proは15 GB以上のストレージが利用可能になるまで録画を停止します。 • **Insufficient capacity (容量が不足しています)**: ディスクの合計サイズが32 GB未満で、AXIS Camera Station Proには不十分です。 RAIDをサポートするAXIS OSレコーダーは、次の状態になる場合もあります。 • **Online (オンライン):** RAIDシステムは正常に動作しています。RAIDシステムのいずれかの物理ディスクが故障した場合に備えた冗長性があります。 • **Degraded (性能低下):** RAIDシステム内の物理ディスクの1つが故障しています。引き続きストレージからの録画と再生は可能ですが、冗長性はありません。さらに別の物理ディスクが故障した場合、RAIDステータスは [**Failure (故障)**] に変わります。故障した物理ディスクをできるだけ早く交換することをお勧めします。故障したディスクを交換した後、RAIDステータスは [**Degraded (性能低下)**] から [**Syncing (同期中)**] に変わります。 • **Syncing (同期中):** RAIDディスクが同期中です。ストレージからの録画と再生は可能ですが、物理ディスクが故障した場合の冗長性はありません。物理ディスクが同期されると、RAIDシステムに冗長性が備わり、RAIDステータスが [**Online (オンライン)**] に変わります。 重要 同期中は、絶対にRAIDディスクを取り外さないでください。ディスクの故障につながる可能性があります。 • **Failure (故障):** RAIDシステムの複数の物理ディスクが故障しています。この場合、ストレージ内の録画はすべて失われ、

リスト	
	故障した物理ディスクを交換してからでないと録画ができなくなります。
サーバー	ローカルストレージまたはネットワークストレージが置かれているサーバー。

概要	
使用中	インデックス付き録画によって現在使用されているストレージ容量。ファイルが録画ディレクトリ内にあるが、データベースでインデックスが付けられていない場合、そのファイルは [**Other data (その他のデータ)**] カテゴリに属します。*ストレージの管理, on page 81*を参照してください。
無料	保存先ストレージの空き容量です。これは、保存先のWindowsプロパティで表示される [空き領域] と同じです。
その他のデータ	インデックス付き録画以外のファイルに使用されているため、AXIS Camera Station Proに不明なストレージ空き容量。 その他のデータ = 全容量 - 使用中容量 - 空き容量.
全容量	ストレージ容量の合計です。これは、保存先のWindowsプロパティで表示される [合計サイズ] と同じです。
割り当て済み	AXIS Camera Station Proが録画に使用できるストレージ容量。スライダーを動かして [**Apply (適用)**] をクリックすると、割り当て容量を調整できます。

ネットワークストレージ	
パス	ネットワークストレージへのパスです。
ユーザー名	ネットワークストレージへの接続で使用するユーザー名です。
パスワード	ネットワークストレージへの接続で使用するユーザー名のパスワードです。

ストレージの管理

[**Configuration (設定)**] - [**Storage (ストレージ)**] - [**Management (管理)**] に移動し、**(Manage storage (ストレージの管理)**] ページを開きます。ここで録画を保存するフォルダを指定できます。ストレージ容量が満杯になるのを防ぐため、AXIS Camera Station Proが使用できる最大量を総容量の割合で設定します。セキュリティや容量拡大のために、他のローカルストレージやネットワークドライブを追加することもできます。

注

- 複数の AXIS Camera Station Proサーバーに接続している場合は、[**Selected server (選択したサーバー)**] ドロップダウンメニューから、ストレージを管理するサーバーを選択します。
- サービスがログインにシステムアカウントを使用する場合、他のコンピューターの共有フォルダーにリンクしているネットワークドライブを追加することはできません。*ネットワークストレージにアクセスできないを参照してください。*
- ローカルストレージまたはネットワークストレージを録画の保存先としてカメラに設定しているか、ストレージに録画が含まれている場合、そのストレージを削除することはできません。

ローカルストレージまたは共有ネットワークドライブを追加する

1. **[設定] - [ストレージ] - [管理]** を選択します。
2. [**追加**] をクリックします。
3. ローカルストレージを追加するには、[**Local storage (ローカルストレージ)**] を選択し、ドロップダウンメニューからストレージの場所を選択します。
4. 共有ネットワークドライブを追加するには、[**Shared network drive (共有ネットワークドライブ)**] をクリックし、パスを入力します。例:\\ip_address\share
5. [**OK**] をクリックして、共有ネットワークドライブのユーザー名とパスワードを入力します。
6. [**OK**]をクリックします。

ローカルストレージまたは共有ネットワークドライブを削除する

ローカルストレージまたは共有ネットワークドライブを削除するには、ストレージ一覧から選択し、**[Remove (削除)]** をクリックします。

録画データを新規フォルダーに移動する

1. **[設定] - [ストレージ] - [管理]** を選択します。
2. ストレージリストからローカルストレージまたは共有ネットワークドライブを選択します。
3. [**Overview (概要)**] で、[**Move recordings to a new folder (録画データを新規フォルダーに移動する)**] にフォルダー名を入力し、録画の保存先を変更します。これにより、既存の録画データも以前のフォルダーから新規のフォルダーへ移動されます。
4. [**適用**] をクリックします。

ストレージ容量の調整

1. **[設定] - [ストレージ] - [管理]** を選択します。
2. ストレージリストからローカルストレージまたは共有ネットワークドライブを選択します。
3. [**Overview (概要)**] で、スライダーを移動して、AXIS Camera Station Proが使用できる最大容量を設定します。
4. [**適用**] をクリックします。

注

- 最適なパフォーマンスを得るために、ディスク領域の少なくとも5%を空き領域として残すことをお勧めします。
- AXIS Camera Station Proに追加するストレージの最小容量の要件は32 GBで、15 GB以上の利用可能な空き容量が必要です。
- 利用可能な空き容量が15 GB未満の場合、AXIS Camera Station Proは容量を空けるために、自動的に古い録画を削除します。

非インデックスファイルを収集する

非インデックスファイルは、ストレージの [**Other data (その他のデータ)**] の大部分を占める場合があります。非インデックスファイルとは、現在のデータベースの一部ではない、録画フォルダー内のすべてのデータを指します。このファイルには、以前のインストールからの録画または復元ポイントが使用されたときに損失したデータが含まれています。

システムは収集されたファイルを削除しませんが、それらを集めて録画ストレージの [**Non-indexed files (非インデックスファイル)**] フォルダーに配置します。ストレージは、クライアントと同じコンピューター、またはユーザーの設定に応じてリモートサーバーに配置することができます。**[Non-indexed files (非インデックスファイル)]** フォルダーにアクセスするには、サーバーへのアクセス権が必要です。AXIS Camera Station Proは、まずサーバーごとにデータを整理し、次にそのサーバーに接続されているデバイスごとにデータを整理します。

紛失した録画やログを検索したり、コンテンツを削除して空き容量を確保したりすることができます。

確認または削除のために非インデックスファイルを収集するには:

1. **[設定] - [ストレージ] - [管理]** を選択します。
2. ストレージリストからローカルストレージまたは共有ネットワークドライブを選択します。
3. [Collect non-indexed files (非インデックスファイルを収集する)] で、[Collect (収集)] をクリックしてタスクを開始します。
4. タスクが完了したら、**[Alarms and Tasks (アラームとタスク)] > Tasks (タスク)]** に移動し、タスクをダブルクリックして結果を表示します。

接続するストレージデバイスの選択

注

録画は.acsmファイルとして保存され、再生する前に変換する必要があります。ファイルの変換については、Axisテクニカルサポートにお問い合わせください。

[Configuration (設定)] - [Storage (ストレージ)] - [Selection (選択)] を選択して **[Select storage (ストレージの選択)]** ページを開きます。このページには、AXIS Camera Station Proのすべてのカメラの一覧が表示されます。ここで特定のカメラの録画データを保持する日数を指定できます。これを選択すると、**[Recording Storage (録画ストレージ)]** でストレージを確認することができます。同時に複数のカメラを設定できます。

名称	装置が複数のカメラが接続されたビデオエンコーダであるとき、または装置が複数のビューエリアのあるネットワークカメラであるとき、装置名または関連付けられたすべてのカメラ名のリストが表示されます。
アドレス	装置のアドレス。リンクをクリックすると、デバイスの設定ページが開きます。装置を追加したときに使用されたIPアドレスまたはホスト名が表示されます。*[Device configuration (装置設定)] タブ, on page 76*を参照してください。
MACアドレス	デバイスのMACアドレス。
メーカー	デバイスのメーカー。
モデル	デバイスのモデル。
使用済みストレージ	録画データが現在使用しているストレージ容量。
所在地：	ストレージのパスと名前。
保存期間	カメラ用に設定された保存期間。
最も古い録画	カメラからストレージに保存されている最も古い録画の時刻。
SDカードの再生	AXIS Camera Station ProでカメラがSDカードから直接録画を再生するように設定されているかどうかを示します。
フェイルオーバー録画	カメラがフェイルオーバーによる録画を使用するかどうかを示します。
ACS Proにコピー	SDカードへの録画データが AXIS Camera Station Proにコピーされるかどうかを示します。
フォールバック録画	カメラがフォールバック録画を使用するかどうかを示します。
サーバー	ローカルストレージまたはネットワークストレージが置かれているサーバー。

各カメラのストレージ設定は、AXIS Camera Station Proにカメラを追加した際に設定されています。カメラのストレージ設定を編集するには:

1. **[設定] - [ストレージ] - [選択]** を選択します。
2. ストレージ設定を編集するカメラを選択します。
3. [Recording storage (録画ストレージ)] で、保存先と保存期間を設定します。
4. **[SD card storage (SDカードストレージ)]** で、必要に応じて **[Playback of SD card recordings (SDカード録画の再生)]**、**[Failover recording (フェイルオーバーによる録画)]**、および**[Copy SD card recordings to ACS Pro server (SDカード録画をACS Proサーバーにコピー)]** を選択します。
5. [**適用**] をクリックします。

録画ストレージ 注 • SDカードストレージを使用するには、デバイスがVAPIXに対応しており、Axis製のSDカードを使用している必要があります。 • SDカードの機能は、M-JPEGでは動作しません。 • SDカードに録画されたビデオは、AXIS Camera Station Proによって削除されません。これらのビデオの保時期間は、カメラのSDカード保存期間設定によって監理されます。	
Store to (保存先)	ドロップダウンメニューから録画を保存するストレージを選択します。選択可能なオプションは、作成されたローカルストレージとネットワークストレージです。
保存期間	• **Unlimited (無制限)**: ストレージがいっぱいになるまで録画データを保存します。 • **Limited (制限あり)**: 録画を保持する最大日数を設定します。 注 AXIS Camera Station Pro用に予約されたストレージ容量がいっぱいになると、指定した日数が経過する前に録画が削除されます。
Maximum days to keep recordings (録画の最大保存期間)	録画を保存する日数を指定します。

SDカードストレージ	
SDカードの録画の再生	この機能をオンにすると、録画をサーバーにコピーすることなく、AXIS Camera Station Proでカメラの SDカードから直接録画を再生できます。タイムラインに表示されているSDカードの録画もエクスポートできます。この機能には、AXIS OS 5.60以降が必要です。
フェイルオーバー録画	AXIS Camera Station Proとの接続が切断されると、録画をカメラのSDカードに保存する場合に選択します。SDカードおよびファームウェア5.20以降を使用するカメラでのみ使用できます。
SDカード録画をACSサーバーにコピー	カメラのSDカードの録画をサーバーにコピーする場合に選択します。**[Schedule (スケジュール)]** を使用して、録画をいつコピーするかを設定します。デフォルトのスケジュールは **[Always (常に)** です。

録画とイベントの設定

カメラを AXIS Camera Station Proに追加すると、システムが自動的に動体録画または連続録画を設定されます。必要に応じて、後で録画方法を変更できます。*録画の方法, on page 90*を参照してください。

動体録画

すべてのAxisネットワークカメラとビデオエンコーダで動体検知を利用できます。動きが検知されたときのみの録画では、連続録画よりストレージ容量を大幅に抑えることができます。[Recording method (**録画方法**)] で、[**Motion detection (動体検知)**] をオンにして設定できます。たとえば、カメラが検知した移動物体の数が多すぎたり少なすぎたりする場合や、録画ファイルのサイズが使用可能なストレージ容量に対して大きすぎる場合に設定を構成できます。

動体録画を設定するには:

1. **[設定] - [録画とイベント] - [録画方法]** を選択します。
2. カメラを選択します。
3. [**Motion detection (動体検知)**] のチェックボックスを選択します。
4. [**Motion settings (動体設定)**] をクリックして、検知可能な物体の数などの動体検知設定を指定します。利用可能な設定はカメラによって異なります。*内蔵動体検知機能の編集*および *AXIS Video Motion Detection 2および4の編集*を参照してください。
5. ドロップダウンメニューで、[**Profile (プロファイル)**] を選択します。[**High (高)**] がデフォルトプロファイルです。
6. スケジュールを選択するか、[**New schedule... (新規スケジュール)**] をクリックして新しいカスタムスケジュールを作成します。
7. プリバッファ時間、ポストバッファ時間、およびトリガー期間を設定します。
8. [**適用**] をクリックします。

注

アクションルールを使用して動体録画を設定することもできます。アクションルールを使用する前に、Recording method (**録画方法**) で **[Motion detection (動体検知)]** がオフになっていることを確認してください。

プロファイル	録画サイズを小さくするには、解像度を低くします。プロファイル設定を編集するには、*ストリームプロファイル*を参照してください。
Schedule	録画のスケジュール。ストレージ容量への影響を軽減するには、特定の期間のみ録画してください。
イベントカテゴリー	録画を分類するイベントカテゴリー (ある場合)。
プリバッファ	動体検知の何秒前から録画に含めるか。
ポストバッファ	動体検知の何秒前後まで録画に含めるか。
Trigger period (トリガー期間)	2つのトリガー間の最小時間を設定し、連続した録画の回数を減らします。この時間の間に別のトリガーが発生した場合、録画は続行され、この時間が再び開始します。
通知	カメラが動きを検知すると、通知が送信されます。**モバイルアプリ** はAXIS Camera Stationモバイルアプリにプッシュ通知を送信します。**[Server alarm (サーバーアラーム)]** はAXIS Camera Station Proでアラームを通知します。

動体検知の設定

物体検知

AXIS Object Analyticsが人物や車両などの物体を検知し、分類すると、物体検知記録機能が録画します。イベントを見逃さないよう、動体検知機能や連続録画機能と組み合わせて使用することをお勧めします。AXIS Object Analytics は、1台のカメラにつき最大10のシナリオをサポートしています。

注

この機能を利用するには、お使いのカメラにファームウェアバージョン12.4.26以降、単一センサー、およびAXIS Object Analytics ACAPがインストールされている必要があります。

物体検知を使用するには:

1. **[設定] - [録画とイベント] - [録画方法]** を選択します。
2. カメラを選択します。
3. [**Object detection (物体検知)**] のチェックボックスを選択します。
4. 設定します。詳細については下表を参照してください。
5. [**適用**] をクリックします。

- 物体検知イベントはタイムライン上にピンク色で表示されます。

物体検知設定...	AXIS Object AnalyticsのWebインターフェースをクリックして開き、録画をトリガーするオブジェクトタイプ (人物、車両) を設定し、最小オブジェクトサイズを設定し、検知エリアを定義し、エリア滞在時間の設定を調整します。
プロファイル	ドロップダウンメニューから **[Profile (プロファイル)]** を選択します。**[High (高)]** がデフォルトのプロファイルです。録画サイズを小さくするには、解像度を小さくします。プロファイル設定を編集するには、*ストリームプロファイル*を参照してください。
Schedule	録画のスケジュールを設定します。ストレージ容量への影響を軽減するには、特定の期間のみ録画してください。
イベントカテゴリー	録画を分類するイベントカテゴリーを選択します (ある場合)。詳細については、*イベントカテゴリー, on page 29*を参照してください。
プリバッファ	物体検知の何秒前から録画に含めるかを設定します。
ポストバッファ	物体検知の何秒後まで録画に含めるかを設定します。
Trigger period (トリガー期間)	連続した録画を防ぐため、トリガー間の最小時間間隔を設定してください。この時間間隔内に別のトリガーが発生した場合、録画は続行され、トリガー期間が再開始します。
通知	AXIS Object Analytics が物体を検知すると、通知が届きます。**モバイルアプリ** はAXIS Camera Stationモバイルアプリにプッシュ通知を送信します。**サーバーアラーム**は AXIS Camera Station Proでアラームを出します。

連続録画の設定

連続録画は中断なしで画像を保存するため、他の録画オプションよりも多くのストレージ容量を必要とします。ファイルサイズを小さくするには、代わりに動体検知録画を使用することを検討してください。

連続録画を使用するには:

1. **[設定]** - **[録画とイベント]** - **[録画方法]** を選択します。
2. カメラを選択します。
3. [**Continuous (連続)**] のチェックボックスを選択します。
4. 設定します。詳細については下表を参照してください。
5. [**適用**] をクリックします。

プロファイル	ドロップダウンメニューから [Profile (プロファイル)] を選択します。[High (高)] がデフォルトのプロファイルです。録画サイズを小さくするには、解像度を小さくします。プロファイル設定を編集するには、*ストリームプロファイル*を参照してください。
Schedule	録画のスケジュールを設定します。ストレージ容量への影響を軽減するには、特定の期間のみ録画してください。
平均ビットレート	オンにすると、最大ストレージ制限が設定されます。指定された最大ストレージと保存期間に基づいて、平均ビットレートの概算がシステムに表示されます。最大平均ビットレートは50000キロビット/秒です。*平均ビットレートを設定する, on page 91*を参照してください。

手動録画

手動録画を設定するには:

1. **[設定] - [録画とイベント] - [録画方法]** を選択します。
2. カメラを選択します。
3. [**Manual (手動)**] のチェックボックスを選択します。
4. 設定します。詳細については下表を参照してください。
5. [**適用**] をクリックします。

プロファイル	ドロップダウンメニューから [Profile (プロファイル)] を選択します。[High (高)] がデフォルトのプロファイルです。録画サイズを小さくするには、解像度を小さくします。プロファイル設定を編集するには、*ストリームプロファイル*を参照してください。
イベントカテゴリー	録画を分類するイベントカテゴリーを選択します (ある場合)。
プリバッファ	録画を押す何秒前から録画に含めるかを設定します。
ポストバッファ	録画を停止した何秒後まで録画に含めるかを設定します。
録画中のブックマーク	手動録画を開始するたびに、ブックマークの詳細を追加します。ブックマークは、後で特定の録画を見つけたり識別したりするのに役立ちます。この設定はオペレーターと管理者のみに適用され、デフォルトではオフになっています。
最大継続時間	各録画の最大時間を設定します。プリバッファ時間とポストバッファ時間は含みません。無制限の場合は0に設定します。

手動録画の詳細については、*手動による録画*を参照してください。

ルールトリガー録画

ルールトリガー録画の開始と停止は、[Action rules (アクションルール)] で作成したルールに従って行われます。たとえば、ルールを使用して、I/Oポートまたは装置イベントからの信号によってトリガーされる録画を生成できます。1つのルールに複数のトリガーを指定できます。

ルールトリガー録画を作成するには、*アクションルール*を参照してください。

注

ルールを利用して動体録画を設定する場合は、録画の重複を避けるため、動体録画をオフにしてください。

フェイルオーバー録画

フェイルオーバーによる録画機能を使用すると、AXIS Camera Station Proへの接続が切断された際に、録画データをカメラのSDカードに保存できます。

AXIS Camera Station Proは、カメラのファームウェアのバージョンに基づいて、フェイルオーバー方式を自動的に選択します。

- **ファームウェア 11.11.42 以降:** カメラがサーバーとの接続を失うとフェイルオーバーによる録画が開始されます。
- **それ以前のファームウェア:** 予期せぬ接続切断が発生した場合のみ、フェイルオーバーによる録画が開始されます。計画されたサーバーの再起動では、フェイルオーバーによる録画はトリガーされません。

フェイルオーバーによる録画を設定するには、*接続するストレージデバイスの選択, on page 83*を参照してください。

注

- アップグレードの際、以前に **[Failover recording (フェイルオーバーによる録画)]** が有効になっていた場合、**[Copy SD card recordings to ACS Pro server (SDカードの録画をACS Proサーバーにコピー)]** 機能が自動的にオンになります。
- SDカードの録画は、AXIS Camera Station Proによって削除されることはありません。これらのデータの保存は、カメラのSDカードの保存期間によって監理されます。
- フェイルオーバーによる録画をオンにすると、他のサーバー上でそのカメラに設定されている既存のフェイルオーバー設定が上書きされます。
- フェイルオーバーによる録画は、カメラビューごとに、一度に1台の AXIS Camera Station Proサーバーでのみ有効にできます。

接続が回復され、**[Copy SD card recordings to ACS Pro server (SDカードの録画をACS Proサーバーにコピー)]** がオンになっている場合、録画はサーバーにコピーされ、タイムラインに濃い灰色で表示されます。カメラは20秒間のプリバッファとポストバッファを使用しますが、1〜4秒の短い中断が発生することがあります。

録画の方法	
動体検知 (プリバッファ使用)	接続が20秒以上中断した場合、カメラは接続が回復するか、SDカードがフルになるまでSDカードへの連続録画を継続します。
動体検知 (プリバッファ不使用)	• 動態録画が実行されていない状態で、接続が20秒以上中断した場合、フェイルオーバーによる録画は開始しません。 • 動態録画の実行中に接続が20秒以上中断した場合は、フェイルオーバーによる録画が開始し、接続が回復するかSDカードがフルになるまで録画を継続します。
連続録画	接続が20秒以上中断した場合、カメラは接続が回復するか、SDカードがフルになるまでSDカードへの連続録画を継続します。

フェイルオーバーによる録画にSDカードを使う

フォールバック録画

AXIS S3008 Recorderを録画ストレージとして使用する装置のフォールバック録画をオンにすることができます。オンにすると、AXIS Camera Station Proとレコーダー間の接続が切断されると、デバイスが自動的に連続録画を開始します。デバイスは、フォールバック録画に中のストリームプロファイルを使用します。

注

- この機能は、AXIS Camera Stationバージョン5.36以降、AXIS S3008 Recorderファームウエアバージョン10.4以降、およびAxisデバイスファームウェア5.50以降を必要とします。
- フォールバック録画が開始されたときに連続録画が進行中の場合、新しい連続録画が開始されます。システムは、レコーダー上にストリームの複製を作成します。

フォールバック録画をオンにするには:

1. AXIS S3008 Recorderとデバイスが追加され、レコーダーがデバイスの録画ストレージとして選択されていることを確認します。*AXIS OS Recorderの設定*を参照してください。
2. **[設定]** - **[ストレージ]** - **[選択]** を選択します。
3. 装置を選択し、[**Fallback recording (フォールバック録画)**] を選択します。
4. [**適用**] をクリックします。

録画の方法

デバイスを追加すると、AXIS Camera Station Proが自動的に動体録画または連続録画を設定します。

チェックマークは、そのデバイスが採用している録画方式を示しています。ビデオおよび音声のプロファイル設定をカスタマイズする方法については、*ストリームプロファイル*を参照してください。

録画方法を変更するには:

1. **[設定] - [録画とイベント] - [録画方法]** を選択します。
2. 1台または複数の装置を選択します。
   同じモデルの装置の場合、複数台の装置を選択し、一括して設定を変更することもできます。
3. [Recording method (録画方法)] 画面で、録画方法をオンまたはオフにします。

注
ビューエリアは動体検知をサポートしていません。

平均ビットレートを設定する

平均ビットレートでは、より長い時間にわたってビットレートが自動的に調整されます。これにより、指定のストレージに基づいて、目標ビットレートを満たし、高いビデオ品質を提供することができます。

注
- このオプションは連続録画でのみ使用できます。カメラが平均ビットレートをサポートしており、ファームウェアバージョンが9.40以降である必要があります。
- 平均ビットレートの設定は、選択したストリームプロファイルの品質に影響します。

1. [Configuration (設定)] > [Storage (ストレージ) > [Selection (選択)] に移動して、カメラの保存期間が制限されていることを確認してください。
2. [Configuration > Devices > Stream profiles (設定 > デバイス > ストリームプロファイル)] に移動し、連続録画に使用するプロファイルとしてH.264またはH.265を使用していることを確認してください。
3. **[設定] - [録画とイベント] - [録画方法]** を選択します。
4. カメラを選択し、[Continuous (連続)] をオンにします。
5. [Video settings (ビデオの設定)] で、設定済みのビデオプロファイルを選択します。
6. [Average bitrate (平均ビットレート)] をオンにし、[Max storage (最大ストレージ)] を設定します。指定された最大ストレージと保存期間に基づいて、平均ビットレートの概算がシステムに表示されます。平均ビットレートの最大値は50,000キロビット/秒です。

注
最大ストレージは、保存期間中の録画の最大容量を意味します。これは録画が指定された容量を超えないことのみを保証し、録画に十分な容量があることは保証しません。

7. [適用] をクリックします。

動体設定を編集する

装置でAXIS Object Analyticsを使用している場合は、そこで動体録画の設定を編集できます。

注
AXIS Camera Station ProでAXIS Object Analyticsを利用するには、AXIS OS 12.4が必要です。

1. [Configuration (設定)] タブを開きます。
2. [Recording and events (録画とイベント)] > [Recording method (録画方法)] に移動します。
3. 設定するカメラを選択します。
4. [Motion detection (動体検知)] をオンにします。
5. [Motion settings (動体設定)] をクリックします。

装置上でAXIS Object Analyticsを設定する方法については、*AXIS Object Analyticsユーザーマニュアル*をお読みください。

AXIS Video Motion Detection 2および4の編集

AXIS Video Motion Detection 2および4は、AXIS Camera Application Platformに対応する製品向けのカメラアプリケーションです。カメラにAXIS Video Motion Detection 2または4をインストールすると、対象範囲内で移動する対象を動体検知機能が検知します。Motion Detection 2にはファームウェア5.60以降が必要です。AXIS Video Motion Detection 4にはファームウェア6.50以降が必要です。製品のファームウェアのリリースノートを確認し、Video Motion Detection 4をサポートしているかどうかを確認することもできます。

AXIS Camera Station Proにカメラを追加する際に動体録画を選択すると、対応するファームウェアが搭載されたカメラにAXIS Video Motion Detection 2および4がインストールされます。対応のファームウェアを搭載していないカメラでは、内蔵の動体検知機能を使用します。装置管理ページから手動でアプリケーションをインストールすることもできます。*カメラアプリケーションをインストールする*を参照してください。

AXIS Video Motion Detection 2および4では、次の作成ができます。

- **Area of interest (対象範囲)**: 録画でカメラが動体を検知する範囲。検知機能は対象範囲の外にある動体を無視し、動作しません。この領域はビデオ画像の上にポリゴンの形状で表示されます。3〜20の頂点を使ってこの領域を作成できます。
- **Area to exclude (除外範囲)**: 対象範囲内で動体を無視する領域。
- **Ignore filters (無視フィルター)**: アプリケーションが検知した動体を無視するフィルターを作成します。重要な動体を無視することのないよう、このフィルターは可能な限り少なく使用し、慎重に設定してください。1度に1つのフィルターを使用し、設定します。
  - **Short-lived objects filter (一時的な物体フィルター)**: このフィルターは、画像内に現れる時間が短い物体を無視します。たとえば、通過する車両のライトによる光や、動きの速い影などです。物体がアラームをトリガーするまでに、画像内に表示されている必要がある最短時間を設定します。この時間はアプリケーションが物体を検知した時点で開始します。このフィルターはアラームを遅延させ、指定時間内に画像から物体が消えた場合はアラームをトリガーしません。
  - **Small objects filter (小さな物体フィルター)**: このフィルターは、動物などの小さな物体を無視します。幅と高さを画像全体に対するパーセンテージで指定します。このフィルターは指定した幅と高さより小さい物体を無視し、アラームをトリガーしません。フィルターが無視するには、物体の幅と高さのいずれもフィルターの値を下回る必要があります。
  - **Swaying objects filter (揺らめいている物体フィルター)**: このフィルターは、揺れている枝葉、旗、それらの影など、動く距離が短い物体を無視します。画像全体に対するパーセンテージでこの距離を設定します。このフィルターは、楕円の中心からいずれかの矢印の先端までの距離よりも短い距離を移動する物体を無視します。楕円は動きの尺度で、画像内のすべての動きに対して適用されます。

動体設定を行うには:

注

これらの設定はカメラに直接適用されます。

1. **[設定] - [録画とイベント] - [録画方法]** を選択します。
2. AXIS Video Motion Detection 2または4を使用するカメラを選択し、**[Motion Settings (動体設定)]** をクリックします。
3. 対象範囲を編集します。
4. 除外範囲を編集します。
5. 無視フィルターを作成します。
6. [**適用**] をクリックします。

新規の頂点を追加する	対象範囲に新規の頂点を追加するには、2つの点の間の線をクリックします。
頂点を削除する	対象範囲から頂点を削除するには、頂点をクリックし、さらに **[Remove Point (ポイントの削除)]** をクリックします。
除外範囲の追加	除外範囲を作成するには、[**Add Exclude Area (除外範囲を追加)**] をクリックしてから、2つの頂点を結ぶ線をクリックします。
除外範囲を削除	除外範囲を削除するには、[**除外範囲を削除**] をクリックします。
Short lived objects filter (一時的な物体フィルター)	一時的な物体フィルターを使用にするには、**[Short lived objects filter (一時的な物体フィルター)]** を選択し、**[Time (時間)]** スライダーを使用して物体がアラームをトリガーするまで画像内に表示されている必要がある最短時間を調整します。
Small objects filter (小さな物体フィルター)	小さな物体フィルターを使用にするには、**[Small objects filter (小さな物体フィルター)]** を選択します。さらに **[Width (幅)]** および **[Height (高さ)]** スライダーを使用して、無視する物体のサイズを調整します。
Swaying objects filter (揺らめいている物体フィルター)	揺らめいている物体フィルターを使用するには、**[Swaying objects filter (揺らめいている物体フィルター)]** を選択し、**[Distance (距離)]** スライダーを使用して楕円の大きさを調整します。

内蔵動体検知機能の編集

内蔵動体検知機能によって、カメラは1つ以上の対象範囲内の動きを検知し、その他のすべての動きを無視します。対象範囲は動きを検知する領域です。複数の対象範囲と除外範囲を使用したり、対象範囲内に除外範囲を配置したりできます。

対象範囲の追加、編集手順:

注

これらの設定はカメラに直接適用されます。

1. **[設定] - [録画とイベント] - [録画方法]** を選択します。
2. 動体検知機能が内蔵されているカメラを選択し、[**動体検知**] をクリックします。
3. [Window (ウィンドウ)] セクションで [**Add (追加)**] をクリックします。
4. [**検知対象**] を選択します。
5. 編集中の範囲のみを表示するには、**[Show selected window (選択したウィンドウを表示)]** を選択します。
6. ビデオ画像内の図形を移動、および、サイズ変更します。これは対象範囲です。
7. **[Object Size (物体の大きさ)]**、**[History (履歴)]**、**[Sensitivity (感度)]** を調整します。
8. あらかじめ定義された設定を使用するには、**[Low (低)]**、**[Moderate (中)]**、**[High (高)]**、または**[Very High (非常に高)]** を選択します。**[低]** を選択すると、大きな被写体が短い検出認識時間で検出されます。**[非常に高]** を選択すると、小さな被写体が長い検出認識時間で検出されます。

9. [Activity (アクティビティ)] セクションで、対象範囲内で検知された動きを確認できます。赤いピークが動きを示します。[Activity (アクティビティ)]フィールドを使用して、[Object size (物体サイズ)]、[History (履歴)]、[Sensitivity (感度)] を調整できます。
10. [OK]をクリックします。

オブジェクトサイズ	範囲の大きさに対する物体の大きさの割合。高い値に設定すると、カメラは非常に大きな物体だけを検知します。低い値に設定すると、画像内の非常に小さな被写体も検知します。
検出認識時間	物体メモリーの長さは、物体が範囲内の動かない存在と見なされるまでの時間の長さを定義します。高い値に設定すると、物体が動体検知をトリガーする時間が長くなります。低い値に設定すると、物体が動体検知をトリガーする時間が短くなります。範囲内に物体が現れない場合は、非常に高い履歴レベルを選択できます。この設定では、物体が範囲内に出現すると動体検知がトリガーされます。
感度	背景と被写体の間の明るさの違い。高感度に設定すると、カメラは通常の背景にある通常のカラーの物体を検知します。低感度に設定すると、カメラは暗い背景にある非常に輝度が高い物体だけを検知します。光の点滅だけを検知させるには、感度を低に設定します。それ以外の場合は、感度を高くすることをお勧めします。

除外範囲を追加、編集するには次のとおりにします。

1. [Edit Motion Detection (動体検知の編集)] 画面の [Window (ウィンドウ)] セクションで [Add (追加)] をクリックします。
2. [Exclude (除外)] を選択します。
3. ビデオ画像で影付きの図形を移動、およびサイズ変更します。
4. [OK]をクリックします。

対象範囲または除外範囲を削除するには、次のとおりにします。

1. [Edit Motion Detection (動体検知の編集)] 画面で、削除する範囲を指定します。
2. [削除] をクリックします。
3. [OK]をクリックします。

イベントカテゴリーの設定

イベントカテゴリーを使用すると、特定のタイプの録画を簡単に見つけることができます。イベントカテゴリーは、以下の手順に沿って作成します。

1. [Configuration (設定)] > [Recording and events (録画とイベント)] > [Event categories (イベントカテゴリー)] を選択します。
2. [新規] をクリックします。
3. イベントカテゴリーの名前を入力します。
4. 任意で、イベントカテゴリーのカラーとカスタム保持時間を設定します。
5. [適用] をクリックします。

名称	「暴行」や「交通取り締まり」など、イベントのタイプを表す名称をカテゴリー名として使用することをお勧めします。
保存期間	各イベントカテゴリーにカスタム保存期間を設定し、カメラのデフォルトの保存期間を上書きすることができます。イベントカテゴリーのカスタム保存期間は、デフォルトよりも長い場合にのみ適用されます。

詳細については、*イベントカテゴリー, on page 29*を参照してください。

I/Oポート

多くのカメラとビデオエンコーダが、外部デバイスを接続するためのI/Oポートを備えています。一部の補助装置にもI/Oポートが搭載されている場合があります。

I/Oポートには2種類あります。

入力ポート - 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装置を接続するために使用します。一例としてドアや窓のコンタクト、煙検出器、ガラス破損検知器、PIR (受動赤外線センサー) があります。

出力ポート - リレー、ドア、ロック、アラームなどの装置に接続するために使用します。AXIS Camera Station Proは出力ポートに接続された装置を制御できます。

注

- 複数の AXIS Camera Station Proサーバーに接続している場合、[**Selected server (選択したサーバー)**] のドロップダウンメニューから任意の接続中のサーバーを選択してI/Oポートを追加および管理できます。
- 管理者権限を持つユーザーは、ユーザー向けI/Oポートをオフにすることができます。*ユーザー権限*を参照してください。

アクションルールは、I/Oポートをトリガーまたはアクションとして使用します。トリガーは入力シグナルを使用します。具体的には、AXIS Camera Station Proは入力ポートに接続された装置から信号を受信することで、指定したアクションを実行します。アクションは出力ポートを使用します。具体的には、ルールがアクティブになったとき、AXIS Camera Station Proは出力ポートに接続された装置をアクティブ化または非アクティブ化できます。*アクションルール*を参照してください。

デバイスの接続やI/Oポートの設定に関する詳細については、Axis製品のユーザーマニュアルまたはインストールガイドを参照してください。一部の製品は、入力ポートとしても出力ポートとしても動作するポートを備えています。

出力ポートは手動で制御できます。*I/Oポートの監視*を参照してください。

I/Oポートの追加

I/Oポートを追加するには:

1. **[設定] - [録画とイベント] - [I/Oポート]** を選択します。
2. [**Add (追加)**] をクリックし、追加できるI/Oポートのリストを表示します。
3. ポートを選択し、[**OK**] をクリックします。
4. [**Type (タイプ)**] と [**Device (デバイス)**] の情報を確認します。必要に応じて更新します。
5. **[Port (ポート)]**、**[Active State (アクティブ状態)]**、**[Inactive State (非アクティブ状態)]** に名前を入力します。この名前は、[Action rules (アクションルール)]、[Logs (ログ)]、および [I/O Monitoring (I/O監視)] にも表示されます。

6. 出力ポートには、AXIS Camera Station Proがデバイスに接続するときの初期状態を設定できます。**[On startup set to (起動時設定)]** を選択し、**[State (状態)]** のドロップダウンメニューで初期状態を選択します。

編集	ポートを編集するには、ポートを選択し、**[Edit (編集)]** をクリックします。ダイアログでポート情報を更新し、**[OK]** をクリックします。
削除	ポートを削除するには、ポートを選択し、**[Remove (削除)]** をクリックします。
Reload I/O Ports (I/O ポートを再読み込み)	デバイスの設定ページからI/Oポートを設定する場合は、**[Reload I/O Ports (I/O ポートを再読み込み)]** をクリックしてリストを更新します。

I/Oポートの監視

注

複数の AXIS Camera Station Proサーバーに接続している場合、**[Selected Server (選択したサーバー)]** のドロップダウンメニューで接続中の任意のサーバーを選択し、I/Oポートをモニターできます。

出力ポートを手動で制御するには:

1. ☰ > **[Actions (アクション)]** > **[I/O Monitoring (I/O監視)]**に移動します。
2. 出力ポートを選択します。
3. **[Change state (状態の変更)]** をクリックします。

アクションルール

アクションルールを使用して、イベントに自動で対応します。たとえば、営業時間外にカメラが動体を検知した場合に電子メールを送信したり、I/Oポートに接続されたデバイスと連携したり、重要なイベントに関するアラートをオペレーターに送信することが可能です。

各ルールには、トリガー (ルールを起動するイベント)、アクション (トリガーによって実行される処理)、およびオプションのスケジュールを持ちます。トリガーが起動すると、ルールによってすべてのアクションが実行されます。

注

- 複数の AXIS Camera Station Proサーバーに接続している場合、**[Selected Server (選択したサーバー)]** ドロップダウンメニューで接続中の任意のサーバーを選択し、アクションルールを作成、および管理できます。
- サードパーティ製の装置の場合、使用できるアクションは装置により異なる可能性があります。これらのアクションの一部には、追加のデバイス設定が必要です。

新しいアクションルールを作成する

1. **[設定]** - **[録画とイベント]** - **[アクションルール]** を選択します。
2. **[新規..]** をクリックします。
3. ルールの名前を [**名前**] フィールドに入力します。
4. **[Schedule (スケジュール)]** で、**[Always (常時)]** または **[Custom schedule (カスタムスケジュール)]** を選択し、ドロップダウンメニューからスケジュールを選択します。新しいスケジュールの作成や既存のスケジュールの編集もできます。

5. [Triggers (トリガー)] で [Add... (追加...)] をクリックし、トリガーのタイプを選択して設定し、[OK] をクリックします。詳細については、を参照してください。詳細については、*トリガーの追加*を参照してください。
6. [Actions (アクション)] で [Add... (追加...)] をクリックし、トリガーのタイプを選択して設定し、[OK] をクリックします。詳細については、*アクションの追加*を参照してください。
7. [適用] をクリックします。
   – ルールは保存すると自動的にオンになります。

編集	既存のルールを編集するには、ルールを選択して [Edit (編集)] をクリックします。
コピー	既存のルールをコピーするには、ルールを選択して [Copy... (コピー)] をクリックします。
削除	ルールを削除するには、ルールを選択して [Remove (削除)] をクリックします。

複数のアクションルールを設定する

複数のルールを選択すると、選択したすべてのルールで共通するトリガーとアクションのみが表示されます。変更は選択したすべてのルールに適用されます。

- **[設定] - [録画とイベント] - [アクションルール] を選択します。**
- 複数のルールを選択します。
- 以下の手順に従って変更します。
  – 選択したすべてのルールに適用されるトリガーまたはアクションを追加します。
  – 選択したすべてのルールから、共通のトリガーまたはアクションを削除します。
  – 選択したすべてのルールのスケジュールを変更します。
- [適用] をクリックします。

注

複数のルールが選択されている場合、個々のトリガーやアクションを編集することはできません。変更によってルールが無効になる可能性がある場合、その変更は適用できません。

トリガーの追加

トリガーはルールを有効にします。1つのルールに複数のトリガーを含めることができます。トリガーの1つがアクティブである間、そのルールはアクティブな状態に保たれます。すべてのトリガーがアクティブであることをルールをアクティブにする条件とする場合は、[All triggers must be active simultaneously to trigger the actions (すべてのトリガーが同時にアクティブな場合にのみアクションをトリガー)] を選択します。パルストリガーでこの設定を使用する場合は、トリガー周期を長くします。パルストリガーは一時的に有効になるトリガーです。

以下のトリガーを選択できます。

動体検知 - 定義された領域内に登録した動きが、動体検知をトリガーします。*動体検知トリガーの作成, on page 98*を参照してください。

常にアクティブ - このトリガーは常にオンです。たとえば、このトリガーを常時オンのスケジュールや低プロファイルの録画アクションと組み合わせることで、パフォーマンスが限られている装置に適した2つ目の連続録画が可能になります。

ライブビュー - ライブビュートリガーは、ユーザーが特定のカメラのビデオストリームを開いたときに発生します。たとえば、このトリガーにより、カメラのLEDを使用して、誰かが監視していることをカメラの近くの人に知らせることができます。*ライブビュートリガーを作成する, on page 99*を参照してください。

システムイベントとエラー - 録画エラーが発生した場合、ストレージがいっぱいになった場合、ネットワークストレージへの接続に失敗した場合、または1台以上のデバイスが接続を喪失した場合、システムイベントとエラートリガーが有効になります。*システムイベントとエラートリガーの作成, on page 99*を参照してください。

入力/出力 - 装置のI/Oポートが接続先のドア、煙検知器、スイッチなどから信号を受信した場合に、入出力 (I/O) トリガーがアクティブになります。*入出力トリガーの作成, on page 100*を参照してください。可能であれば、入力/出力トリガーではなく、デバイスイベントトリガーを使用することをお勧めします。

デバイスイベント - このトリガーはカメラまたは補助装置から直接イベントを受信し、使用します。この機能は、AXIS Camera Station Proに目的に合ったトリガーがない場合に使用します。*デバイスイベントトリガーの作成, on page 101*を参照してください。

アクションボタン - アクションボタンを使用して、ライブビューからアクションを開始および停止できます。1つのボタンを複数のルールで使用できます。*アクションボタントリガーの作成, on page 106*を参照してください。

AXIS Entry Managerイベント - AXIS Camera Station ProがAXIS Entry Managerで設定済みのドアから信号を受信したときに、このトリガーがアクティブになります。たとえば、ドアがこじ開けられた、開いている時間が長すぎる、アクセスを拒否したなどの信号です。*AXIS Entry Managerイベントトリガーの作成, on page 107*を参照してください。

外部HTTPS - 外部HTTPSトリガーを使用すると、外部アプリケーションがHTTPS通信を通じて AXIS Camera Station Proでイベントをトリガーすることができます。*外部HTTPSトリガーの作成, on page 107*を参照してください。

動体検知トリガーの作成

カメラが一定の範囲内で動きを検知すると、動体検知トリガーがアクティブになります。カメラが検知処理を行うため、AXIS Camera Station Proに処理負荷は生じません。

注

カメラで動体録画がすでにオンになっている場合は、録画開始に動体検知トリガーを使用しないでください。動体検知トリガーを使用する前に、動体録画をオフにしておきます。動体録画をオフにするには、[**Configuration > Recording and events > Recording method (設定 > 録画とイベント > 録画方法)**] を開きます。

動体検知トリガーを作成するには:

1. **[設定] - [録画とイベント] - [アクションルール]** を選択します。
2. [**新規**] をクリックします。
3. [**追加**] をクリックして [**動体検知**] を選択します。
4. **[OK]**をクリックします。
5. ダイアログで、次のように実行します。
   5.1. 動体検知を実行するカメラを指定します。
   5.2. 連続した録画を防ぐため、トリガー間の最小時間間隔を設定してください。この時間間隔内に別のトリガーが発生した場合、録画は続行され、トリガー期間が再開始します。
   5.3. 動体検知を設定するには、[**動体設定**] をクリックします。利用可能な設定はカメラによって異なります。*内蔵動体検知機能の編集*および *AXIS Video Motion Detection 2および4の編集*を参照してください。
6. **[OK]**をクリックします。

ライブビュートリガーを作成する

ライブビュートリガーは、ユーザーが特定のカメラのビデオストリームを開いたときに発生します。たとえば、このトリガーにより、カメラのLEDを使用して、誰かが監視していることをカメラの近くの人に知らせることができます。

ライブビュートリガーを作成するには:

1. **[設定] - [録画とイベント] - [アクションルール]** を選択します。
2. [**新規**] をクリックします。
3. [**追加**] をクリックし、[**ライブビュー**] を選択します。
4. **[OK]**をクリックします。
5. トリガーカメラを選択します。
6. **[OK]**をクリックします。

システムイベントとエラートリガーの作成

トリガーとして使用する1つ以上のシステムイベントとエラーを選択します。システムイベントの例は、録画エラーが発生した場合、ストレージがいっぱいになった場合、ネットワークストレージへの接続に失敗した場合、1台以上のデバイスが接続を喪失した場合などです。

システムイベントとエラートリガーを作成するには:

1. **[設定] - [録画とイベント] - [アクションルール]** を選択します。
2. [**新規**] をクリックします。
3. [**追加**] をクリックし、[**システムイベントとエラー**] を選択します。
4. **[OK]**をクリックします。
5. トリガーの作成元になるシステムイベントまたはエラーを選択します。
6. **[OK]**をクリックします。

On recording error (**録画エラーのとき**)	[**録画エラーのとき**] を選択すると、カメラがストリーミングを停止した場合など、録画中にエラーが発生したときにトリガーがアクティブになります。
ストレージが満杯のとき	[On full storage (**ストレージの空き容量がなくなったとき**)] を選択すると、録画用のストレージの空き容量がなくなったときにトリガーがアクティブになります。

ネットワークストレージにアクセスできないとき	[On no contact with network storage (ネットワークストレージにアクセスできないとき)] を選択すると、ネットワークストレージへのアクセスに問題が発生するとトリガーがアクティブになります。
On lost connection to camera (次のカメラとの接続が切断されたとき)	[On lost connection to camera (次のカメラとの接続が切断されたとき)] を選択した場合、カメラとの接続に問題が発生するとトリガーがアクティブになります。 • [All (すべて)] を選択すると、AXIS Camera Station Proに追加されているすべてのカメラが対象となります。 • [Selected (選択済み)] を選択し、[Cameras (カメラ)] をクリックして、AXIS Camera Station Proに追加されたすべてのカメラのリストを表示します。[Select all (すべて選択)] または [Deselect all (すべて選択解除)] を使用して、すべてのカメラを選択またはクリアします。

入出力トリガーの作成

装置のI/Oポートが接続先のドア、煙検知器、スイッチなどから信号を受信した場合に、入出力 (I/O) トリガーがアクティブになります。

注

- I/Oトリガーを使用する前に、I/Oポートを AXIS Camera Station Proに追加します。*I/Oポートを参照してください。*
- 可能であれば、入力/出力トリガーではなく、デバイスイベントトリガーを使用することをお勧めします。詳細については、*デバイスイベントトリガーの作成, on page 101*を参照してください。

入出力トリガーを作成するには:

1. **[設定] - [録画とイベント] - [アクションルール]** を選択します。
2. [**新規**] をクリックします。
3. [**追加**] をクリックし、[**入力/出力**] を選択します。
4. **[OK]**をクリックします。
5. [**Trigger port and state (トリガーポートと状態)**] で、I/Oポートとトリガーの設定を行います。
6. **[OK]**をクリックします。

ポートとステータス	
入出力ポート	[I/O port (I/Oポート)] で、使用する入力または出力ポートを選択します。
Trigger state (トリガー時の状態)	[Trigger state (トリガー状態)] で、トリガーをアクティブにする必要のあるI/Oポートの状態を選択します。利用可能な状態は、ポートの設定によって異なります。
Trigger period (トリガー期間)	連続する2つのトリガー間の最小時間間隔を設定し、連続した録画を減らします。この時間間隔内に別のトリガーが発生した場合、録画は続行され、トリガー期間が再開始します。

デバイスイベントトリガーの作成

このトリガーはカメラまたは補助装置から直接イベントを受信し、使用します。この機能は、AXIS Camera Station Proに適切なトリガーがない場合に使用します。イベントはカメラによって異なり、1つ以上のフィルターを設定する必要があります。フィルターは、デバイスイベントトリガーを有効にするために満たす必要がある条件です。Axis製品のイベントとフィルターの詳細については、*axis.com/partners*および*axis.com/vapix*にあるVAPIX®のドキュメントを参照してください。

デバイスイベントトリガーを作成するには:

1. **[設定] - [録画とイベント] - [アクションルール]** を選択します。
2. [**新規**] をクリックします。
3. [**追加**] をクリックし、[**デバイスイベント**] を選択します。
4. **[OK]**をクリックします。
5. [Configure device event trigger (**デバイスイベントトリガーの設定**)] で、イベントトリガーを設定します。

注

利用可能なイベントは、選択したデバイスによって異なります。サードパーティデバイスの場合、これらのイベントの多くでは、デバイスで追加の設定が必要です。

6. [Filters (**フィルター**)] で、フィルターを選択します。
7. [Activity (**アクティビティ**)] で、経時的にデバイスイベントトリガーの現在の状態を確認します。イベントは、ステートフル、ステートレスのいずれかになります。ステップ機能は、ステートフルのイベントを示します。パルスがある直線は、ステートレスのイベントを示しています。
8. **[OK]**をクリックします。

デバイスイベントトリガーを設定	
デバイス	[Device (**デバイス**)] で、カメラまたは補助装置を選択します。
イベント	[Event (**イベント**)] で、トリガーとして使用するイベントを選択します。
Trigger period (トリガー期間)	連続する2つのトリガー間の最小時間間隔を設定し、連続した録画を減らします。この時間間隔内に別のトリガーが発生した場合、録画は続行され、トリガー期間が再開始します。

デバイスイベントの例

カテゴリー	デバイスイベント
アンプ	アンプの過負荷
音声コントロール	デジタル信号のステータス
音声ソース	音声検知
認証	アクセス要求の許可
	アクセス要求の拒否
呼び出し	状態
	状態を変更
	ネットワーク品質
	SIPアカウントのステータス
	着信映像
ケーシング	ケーシング開放
デバイス	リングパワー過電流保護
装置センサー	システム準備完了
	PIRセンサー
装置ステータス	システム準備完了
ドア	ドアのこじ開け
	ドア設備へのいたずらを検知
	ドアがロックされました
	ドアが開いている時間が長すぎます
	ドア位置
	ドアのロックが解除されました
イベントバッファ	開始
イベントロガー	アラーム欠落
	イベント欠落
	アラーム
ファン	ステータス
グローバルシーン変更	画像サービス
ハードウェアの故障	ストレージエラー
	ファンの故障
ヒーター	ステータス
入力ポート	仮想入力
	デジタル入力ポート
	手動トリガー

	状態監視入力ポート
	デジタル出力ポート
	外部入力
ライト	ステータス
照明ステータス変更	ステータス
メディア	プロファイル変更
	設定変更
モニタリング	ハートビート
MotionRegionDetector	動き
ネットワーク	ネットワークの喪失 装置によって使用されるイベントにのみ適用されます。AXIS Camera Station Proによって使用されるイベントには適用されません。
	アドレス追加
	アドレス削除
PTZ動作中	チャネル<channel name>でのPTZ動作
PTZプリセット	<channel name>でのPTZプリセット到達
PTZController	自動追跡
	PTZコントロールキュー
	PTZエラー
	PTZ準備完了
録画設定	録画の作成
	録画の削除
	設定の追跡
	録画の設定
	録画ジョブの設定
リモートカメラ	Vapixのステータス
	PTZ位置
Schedule	Pulse (パルス):
	期間
	スケジュール型イベント
状態	アクティブ
ストレージ	ストレージの中断
	録画中
システムメッセージ	アクションの失敗
いたずら検出	チルト検知

	衝撃検知
温度センサー	動作温度範囲の上
	動作温度範囲の下
	動作温度範囲内
	動作温度範囲外
トリガー	リレーおよび出力
	デジタル入力
ビデオ動体検知	VMD 4: プロファイル<プロファイル名>
	VMD 4: 任意のプロファイル
Video Motion Detection 3	VMD 3
ビデオソース	動体アラーム
	ライブストリームのアクセス
	デイナイトビジョン
	カメラに対するいたずら
	平均ビットレート低下
	ビデオソースの接続

AXISネットワークドアコントローラーの装置イベント

デバイスイベント	アクションルールのトリガー
認証	
アクセス要求の許可	システムは、カード所持者が認証情報を使用して本人確認したときにアクセスを許可しました。
強制	強制PINが使用されました。これを使用して、たとえば、無音アラームをトリガーできます。
アクセス要求の拒否	システムは、カード所持者が認証情報を使用して本人確認したときにアクセスを拒否しました。
ダブルスワイプ	カード所持者がカードを2回スワイプしました。ダブルスワイプにより、カード所持者はドアの現在の状態を無効にすることができます。たとえば、通常のスケジュール外にドアのロックを解除するために使用できます。
不正通行防止による検知	誰かが、自分より前にゾーンに入ったカード所持者の認証情報を使用しました。
Authorization with two-person rule (2人ルールにより承認)	
アクセス要求の保留中	2人のカード所持者のうち最初の1人が認証情報を使用して本人確認しました。
アクセス要求の許可	システムは、最後のカード所持者が認証情報を使用して本人確認をしたときにアクセスを許可しました。
ケーシング	
ケーシング開放	誰かがネットワークドアコントローラーのケーシングを開いたり、取り外したりしました。たとえば、保守のためにケー

	シングが開かれたときや、ケーシングがいたずらされたときに管理者に通知を送信するために使用します。
装置ステータス	
システム準備完了	システムは準備完了状態です。たとえば、Axis製品はシステムの状態を検出し、システムが起動したときに管理者に通知を送信します。[**Yes (はい)**] を選択した場合、製品が準備完了状態になると、アクションルールがトリガーされます。このルールは、イベントシステムなど、必要なすべてのサービスが開始されている場合のみトリガーできます。
ドア	
ドアのこじ開け	ドアがこじ開けられました。
ドア設備へのいたずらを検知	システムが以下を検知した場合: • デバイスのケーシングが開いているか閉じている。 • デバイス動き。 • 接続されたリーダーが壁面から取り外された。 • 接続されたドアモニター、リーダー、またはREX装置に対するいたずら。このトリガーを使用する場合は、**[Supervised input (監視入力)]** をオンにし、関連するドアコネクターの入力ポートの終端抵抗器が取り付けられていることを確認してください。
ドアがロックされました	ドアロックが施錠されました。
ドアが開いている時間が長すぎます	ドアの開放時間が長すぎます。
ドア位置	ドアモニターがドアの開閉を示します。
ドアのロックが解除されました	ドアのロックが解除されたままです。たとえば、認証情報の提示なしでドアを開けることが許可される訪問者が存在する場合に、この状態を使用できます。
入力ポート	
仮想入力	いずれかの仮想的な入力の状態が変化しました。管理ソフトウェアなどのクライアントで、さまざまなアクションを開始するために使用できます。アクティブになったときにアクションルールをトリガーする入力ポートを選択してください。
デジタル入力ポート	デジタル入力ポートの状態が変化しました。このトリガーを使用して、通知の送信やステータスLEDの点滅など、さまざまなアクションを開始します。アクティブになったときにアクションルールをトリガーする入力ポートを選択します。または、[**Any (任意)**] を選択すると、いずれかの入力ポートがアクティブになったときにアクションルールがトリガーされます。
手動トリガー	手動トリガーをアクティブにします。このトリガーを使用して、VAPIX APIを通じて手動でアクションルールを開始または停止します。
外部入力	緊急入力がアクティブまたは非アクティブになりました。
ネットワーク	
ネットワーク接続断絶	ネットワーク接続が切断されました。

	これはデバイスイベントにのみ適用され、AXIS Camera Station Proで使用されるイベントには適用されません。
アドレス追加	新しいIPアドレスが追加されました。
AddressRemoved	IPアドレスが削除されました。
Schedule	
スケジュール型イベント	既定のスケジュールの状態が変化しました。たとえば、営業時間中や週末など、特定の時間帯にビデオを録画する場合に使用します。**[Schedule (スケジュール)]**ドロップダウンメニューでスケジュールを選択します。
システムメッセージ	
アクションの失敗	アクションルールの実行に失敗し、アクションに失敗したことを通知するシステムメッセージがトリガーされました。
トリガー	
デジタル入力	物理デジタル入力ポートがアクティブまたは非アクティブになりました。

アクションボタントリガーの作成

[Live view (ライブビュー)] でアクションを開始および停止するには、アクションボタンを使用します。アクションボタンはライブビューの最下部またはマップ内にあります。1つのボタンを複数のカメラやマップに使用したり、1つのカメラやマップに複数のアクションボタンを使用したりできます。カメラのアクションボタンを追加または編集する際に、カメラのボタンを並べ替えることができます。

アクションボタンには次の2種類があります。

コマンドボタン - アクションを手動で開始するために使用します。停止ボタンが不要なアクションには、コマンドボタンを使用します。コマンドボタンには、ボタンラベルとツールチップがあります。ボタンラベルは、ボタンに表示されるテキストです。ボタンにマウスポインターを合わせるとツールチップが表示されます。

例: 出力をあらかじめ設定された時間アクティブにし、アラームを鳴らし、電子メールを送信するボタンを作成します。

トグルボタン - アクションを手動で開始および停止するために使用します。ボタンにはトグルオン状態とトグルオフ状態の2つの状態があります。ボタンをクリックすると、2つの状態が切り替わります。デフォルトではトグルボタンはトグルオン状態のときにアクションを開始しますが、トグルオフ状態でアクションを開始するように設定することもできます。
トグルボタンには、トグルオンのラベル、トグルオフのラベル、ツールチップがあります。トグルオンのラベルとトグルオフのラベルは、トグルオンとトグルオフの各状態のボタンに表示されるテキストです。ボタンにマウスポインターを合わせるとツールチップが表示されます。

例: ドアを開閉し、パルスを [as long as any trigger is active (トリガーがアクティブである間)] に設定した出力アクションを使用するボタンを作成します。

アクションボタントリガーを作成するには:

1. **[設定] - [録画とイベント] - [アクションルール]** を選択します。
2. [**新規**] をクリックします。
3. [**追加**] をクリックし、[**アクションボタン**] を選択します。
4. **[OK]**をクリックします。
5. [**ボタンの新規作成**] または [**既存のボタンを使用**] を選択します。**[Next (次へ)]** をクリックします。

6. [Create new button (ボタンの新規作成)] を選択した場合:
   6.1. [コマンドボタン] または [トグルボタン] を選択します。トグルボタンを使用してトグルオフ状態でアクションを開始する場合は、[トリガーをオフに切り替え] を選択します。
   6.2. [Next (次へ)] をクリックします。
   6.3. ボタンのラベルとツールチップを追加します。

注

アクションボタンラベルの最初の下線の次に表示される文字または数字が、そのアクションボタンのアクセスキーになります。Altキーとアクセスキーを押してアクションボタンを有効にします。たとえば、アクションボタンにA_BCという名前を付けると、このアクションボタン名はライブビューでABCに変更されます。AltキーとBキーを押してアクションボタンを有効にします。

7. [Use existing button (既存のボタンを使用)] を選択する場合:
   7.1. ボタンを検索するか、使用するボタンをクリックします。
   7.2. 既存のトグルボタンを選択した場合は、[Trigger on toggle (トリガーをオンに切り替え)] または [Trigger on untoggle (トリガーをオフに切り替え)] を選択する必要があります。
   7.3. [Next (次へ)] をクリックします。
   7.4. ボタンのラベルとツールチップを編集します。
8. ドロップダウンメニューからカメラまたはマップを選択します。
9. 複数のカメラまたはマップにボタンを追加するには、[複数のカメラに追加] または [複数のマップに追加] をクリックします。
10. カメラに複数のアクションボタンがある場合、[Arrange (配置)] をクリックしてボタンの順序を編集できます。[OK]をクリックします。
11. [Next (次へ)] をクリックします。

AXIS Entry Managerイベントトリガーの作成

AXIS Camera Station Proは、AXIS Entry Managerで設定済みのドアから信号を受信するとトリガーを有効ににします。たとえば、ドアがこじ開けられた、ドアが開いている時間が長すぎる、アクセスが拒否されたなどの信号です。

注

AXIS Entry Managerイベントトリガーは、AXIS A1001 Network Door Controllerを AXIS Camera Station Proに追加した場合にのみ使用できます。

1. [設定] - [録画とイベント] - [アクションルール] を選択します。
2. [新規] をクリックします。
3. [Add (追加)] をクリックし、[AXIS Entry Manager event (AXIS Entry Managerイベント)] を選択します。
4. [OK]をクリックします。
5. トリガーをアクティブにするイベントとドアを選択します。
6. [OK]をクリックします。

外部HTTPSトリガーの作成

外部HTTPSトリガーを使用すると、外部アプリケーションがHTTPS通信を通じて AXIS Camera Station Proでイベントをトリガーすることができます。このトリガーはHTTPS通信のみに対応するため、HTTPS要求のために、ドメイン名とパスワードを含む有効な AXIS Camera Station Proユーザー名を必要とします。

以下の要求は、HTTPのGET*メソッドGET*によってサポートされています。要求本文に記載されたJSONデータと共にPOSTを使用することもできます。

注

- 外部HTTPSトリガー要求は、Google Chromeでのみテストできます。
- 外部HTTPSトリガーは、モバイル監視アプリと同じポートを使用します。*全般サーバー設定*のモバイル通信ポートおよびモバイルストリーミングポートの説明を参照してください。
- ID "trigger1"でトリガーをアクティブにする：`https://[address]:29204/Acs/Api/TriggerFacade/ActivateTrigger?{"triggerName":"trigger1"}`
- ID "trigger1"でトリガーを非アクティブにする：`https://[address]:29204/Acs/Api/TriggerFacade/DeactivateTrigger?{"triggerName":"trigger1"}`
- ID "trigger1"でトリガーをアクティブにし、30秒後にトリガーを自動的に非アクティブにする：`https://[address]:29204/Acs/Api/TriggerFacade/ActivateDeactivateTrigger?{"triggerName":"trigger1","deactivateAfterSeconds":"30"}`

注

自動非アクティベーションのタイマーは、同じトリガーに他のコマンドが発行されるとキャンセルされます。

- ID "trigger1"でトリガーをパルスさせる (トリガーをアクティブにした直後に非アクティブにする)：`https://[address]:29204/Acs/Api/TriggerFacade/PulseTrigger?{"triggerName":"trigger1"}`

外部HTTPSトリガーを作成するには:

1. **[設定] - [録画とイベント] - [アクションルール]** を選択します。
2. [**New (新規)**] をクリックします。
3. [**追加**] をクリックし、[**外部HTTPS**] を選択します。
4. **[OK]**をクリックします。
5. トリガーの名前を [**Trigger name (トリガー名)**] に入力します。
6. クライアントがログインに使用したのと同じサーバーアドレスを使用しているサンプルURLを確認します。URLは、アクションルールの完了後にのみ機能します。
7. **[OK]**をクリックします。

外部HTTPSトリガーに対する適切なアクション

- トリガーをアクティブおよび非アクティブにする要求は、録画の開始や停止を行うアクションに適しています。
- トリガーをパルスする要求は、[**Raise Alarm (アラームを発する)**] または [**Send Email (電子メールを送信する)**] などのアクションに適しています。

スマート検索2のトリガーを作成する

以下の手順に従って、スマート検索トリガー2を作成します。

1. **[設定] - [録画とイベント] - [アクションルール]** を選択します。
2. [**新規**] をクリックします。
3. **[Add (追加)]**をクリックし、**[Smart search 2 (スマート検索2)]** を選択します。
4. **[OK]**をクリックします。
5. トリガーを選択して設定します。
   - トリガーとして使用するスマート検索フィルターを作成するには、*トリガー, on page 183*を参照してください。
   - **[High processing delay (高処理遅延)]** を選択し、スマート検索2が検出処理に1分以上を要する場合にトリガーを有効にします。

6. [OK]をクリックします。

AXIS Audio Managerのトリガーを作成する

AXIS Audio Managerのトリガーを作成する:

1. [設定] - [録画とイベント] - [アクションルール] を選択します。
2. [新規] をクリックします。
3. [Add (追加)] をクリックし、[Audio manager] を選択します。
4. [OK]をクリックします。
5. トリガーを選択して設定します。
6. [OK]をクリックします。

Device status changed (デバイスステータス変更)	デバイスステータスがオンラインまたはオフラインになったときにトリガーを有効にする場合、[Device status changed (デバイスステータス変更)] を選択します。
Playback status changed (再生ステータス変更)	再生ステータスが変化したときにトリガーを有効にする場合、[Playback status changed (再生ステータス変更)] を選択します。
Target enabled or disabled (対象有効/無効)	トリガー対象がオンまたはオフになったときにトリガーを有効にする場合、[Target enabled or disabled (対象有効/無効)] を選択します。
Volume controller volume changed (音量コントローラーの音量変更)	音量コントローラーの設定が変更されたときにトリガーを有効にする場合、[Volume controller volume changed (音量コントローラーの音量変更)] を選択します。

アクションの追加

1つのルールに複数のアクションを設定できます。ルールがアクティブになると、アクションが開始されます。

以下のアクションを使用できます。

録画 - カメラの録画を開始します。*録画アクションの作成*を参照してください。

アラームを作動する - すべての接続された AXIS Camera Station Proクライアントにアラームを送信します。*「アラームを上げる」アクションの作成*を参照してください。

出力設定 - 出力ポートの状態を設定します。これを使用して、出力ポートに接続されたデバイスを操作します (照明を点灯する、ドアをロックするなど)。*出力アクションの作成*を参照してください。

電子メールの送信 - 1つ以上の送信先に電子メールを送信します。*メール送信アクションの作成*を参照してください。

ライブビュー - すべての接続された AXIS Camera Station Proクライアントで、特定のカメラのライブビュー、ビュー、またはプリセットポジションを開きます。ライブビューアクションを使用して、開いているクライアントをタスクバーからリストアしたり、開いている他のアプリケーションの手前に移動したりすることもできます。*ライブビューアクションの作成*を参照してください。

HTTPで通知を送る - カメラ、ドアコントローラー、または外部のWebサーバーにHTTP要求を送信します。*HTTP通知アクションの作成*を参照してください。

サイレンとライト - 対応するデバイスであらかじめ設定されたプロファイルに基づいて、サイレンとライトのパターンをトリガーします。*サイレンとライトのアクションを作成する, on page 116*を参照してください。

仮想I/O - デバイスの特定の仮想入力ポートをトリガーします。*仮想I/Oアクションを作成する, on page 116*を参照してください。

AXIS Entry Manager - AXIS Entry Managerで設定されたドアコントローラーに接続されたドアへのアクセス権の付与、ドアの解錠・施錠を行います。*AXIS Entry Managerアクションの作成, on page 116*を参照してください。

モバイルアプリの通知を送信する - このアクションは、カスタムメッセージをAXIS Camera Stationモバイルアプリに送信します。*モバイルアプリ通知の送信アクションを作成する, on page 117*を参照してください。

ルールをオン/オフにする - その他のアクションルールをオンまたはオフにします。*他のアクションルールをオンまたはオフにするアクションの作成, on page 117*を参照してください。

ビデオデコーダに送信する - ビデオデコーダにビューを送信し、指定した時間モニターに表示します。*ビデオデコーダにビューを送信するアクションを作成する, on page 118*を参照してください。

アクセスコントロール - AXIS Camera Station Secure Entryのドアおよびゾーンのアクションが含まれます。*アクセスコントールアクションの作成, on page 118*を参照してください。

録画アクションの作成

録画アクションは、カメラによる録画を開始します。**[Recordings (録画)]** タブから録画にアクセスし、再生します。

録画アクションを作成するには:

1. 録画を保存先を指定するには、**[Configuration (設定)]** > **[Storage (ストレージ)]** > **[Selection (選択)]** に移動します。
2. **[設定]** - **[録画とイベント]** - **[アクションルール]** を選択します。
3. [**新規**] をクリックします。
4. [**追加**] をクリックしてトリガーを作成します。**[Next (次へ)]** をクリックします。*トリガーの追加*を参照してください。
5. [**追加**] をクリックし、[**録画**] を選択します。
6. **[OK]**をクリックします。
7. [Camera (カメラ)] で、録画を行うカメラを選択します。
8. [Video setting (ビデオ設定)] で、プロファイル、プリバッファ、ポストバッファを設定します。
9. [Event setting (イベント設定)]で、該当する場合は、録画のイベントカテゴリーを選択します。
10. **[OK]**をクリックします。

映像設定	
プロファイル	[Profile (プロファイル)] ドロップダウンメニューからプロファイルを選択します。プロファイル設定を編集するには、*ストリームプロファイル*を参照してください。
プリバッファ	動体検知の何秒前から録画に含めるかを設定します。
ポストバッファ	アクションの終了後の何秒後まで録画に含めるかを設定します。

「アラームを上げる」アクションの作成

「アラームを発する」アクションは、接続先のすべての AXIS Camera Station Proクライアントにアラームを送信します。アラームは **[Alarms (アラーム)]** タブおよびタスクバーの通知として表示されます。アラーム手順を含むファイルを添付することができます。アラームガイドは、[**アラーム**] タブのほか、[**ログ**] タブで使用できます。

「アラームを上げる」アクションを作成するには、次のように実行します。

1. **[設定] - [録画とイベント] - [アクションルール]** を選択します。
2. [**新規**] をクリックします。
3. **[Add (追加)]** をクリックしてトリガーを設定します。**[Next (次へ)]** をクリックします。*トリガーの追加*を参照してください。
4. [**追加**] をクリックし、[**アラームを上げる**] を選択します。
5. **[OK]**をクリックします。
6. **[Alarm message (アラームメッセージ)]** で、タイトル、説明、継続時間を設定します。
7. **[Alarm procedure (アラーム手順)]** を設定します。
   7.1. **[On alarm show alarm procedure (アラーム時にアラーム手順を表示)]** を選択します。
   7.2. **[Upload (アップロード)]** をクリックし、ファイルを見つけます。
   7.3. **[Preview (プレビュー)]** をクリックして、ファイルのプレビューを表示します。
   7.4. **[OK]**をクリックします。

アラームメッセージ	
タイトル	アラームのタイトルを入力します。タイトルは、[**Alarms (アラーム)**] タブの [**Alarms (アラーム)**] とタスクバーの通知に表示されます。
説明	アラームの簡単な説明を入力します。説明は [**Alarms (アラーム)**] タブの **[Alarms (アラーム)] > [Description (説明)]** とタスクバー通知に表示されます。
(Duration (s) (期間 (秒))	ポップアップ通知の継続時間を1～600秒に設定します。

出力アクションの作成

出力アクションは、出力ポートの状態を設定します。このアクションを使用して、出力ポートに接続されたデバイスをコントロールします (照明を点灯する、ドアをロックするなど)。

注

出力アクションを使用する前に、AXIS Camera Station Proに出力ポートを追加します。*I/Oポートを参照してください。*

出力アクションを作成するには:

1. **[設定] - [録画とイベント] - [アクションルール]** を選択します。
2. [**新規**] をクリックします。
3. **[Add (追加)]** をクリックしてトリガーを設定します。**[Next (次へ)]** をクリックします。*トリガーの追加*を参照してください。
4. [**追加**] をクリックし、[**出力の設定**] を選択します。
5. **[OK]**をクリックします。
6. [**Output port (出力ポート)**] で、出力ポートを選択します。

7. [State on action (アクション時の状態)] で、設定するポートの状態を選択します。利用可能なオプションは、ポートの設定によって異なります。
8. [Pulse (パルス)] を選択して、出力ポートを新しいステータスで維持する時間を設定します。

注

アクション後もポートを新しいステータスに維持するには、[パルス] のチェックマークを外します。

9. [OK]をクリックします。

For as long as any trigger is active (トリガーがアクティブである限り出力ポートの状態を維持	[トリガーがアクティブである限り出力ポートの状態を維持] を選択すると、ルールに指定されたすべてのトリガーがアクティブである限り、ポートは新しいステータスを維持します。
一定時間その状態を保つ	ポートを一定の時間だけ新しいステータスで維持するには、[Keep the state for a fixed time (一定時間その状態を保つ)]を選択し、秒数を指定します。

メール送信アクションの作成

電子メールアクションは、1つ以上の送信先に電子メールを送信します。カメラで撮影したスナップショットを電子メールに添付することができます。

注

電子メールを送信するには、まずSMTPサーバーを設定する必要があります。 *サーバーの設定*を参照してください。

メール送信アクションを作成するには:

1. [設定] - [録画とイベント] - [アクションルール] を選択します。
2. [新規] をクリックします。
3. [Add (追加)] をクリックしてトリガーを設定します。[Next (次へ)] をクリックします。 *トリガーの追加*を参照してください。
4. [追加] をクリックし、[電子メールを送信] を選択します。
5. [OK]をクリックします。
6. [Recipients (送信先)] に電子メールアドレスを追加します。
   6.1. [New Recipient (新しい送信先)] にメールアドレスを入力し、[To]、[Cc]、または [Bcc] を選択します。
   6.2. [追加] をクリックします。
7. [Contents (内容)] に電子メールの件名とメッセージを入力します。
8. [Advanced (詳細設定)] で、添付ファイル、電子メール件数、間隔を設定します。
9. [OK]をクリックします。

高度	
Attach snapshots (スナップショットを添付)	カメラの.jpgスナップショットを添付ファイルとして添付するには、**[Attach snapshots (スナップショットを添付)]** を選択し、**[Cameras (カメラ)]** をクリックします。AXIS Camera Station Proに追加されているすべてのカメラのリストが表示されます。**[Select all (すべて選択)]** をクリックしてすべてのカメラを選択するか、**[Deselect all (すべて選択解除)]**] をクリックしてすべてのカメラの選択を解除します。
Send one email for each event (イベントごとに電子メールを一通送信)	同じイベントに関する複数の電子メールを送信しないようにするには、**[Send one email for each event (イベントごとにメールを一通送信)]** を選択します。
Don't send another email for (次の電子メールを送信するまでの期間)	電子メールの送信間隔が短くなりすぎないようにするには、**[Don't send another email for (次の電子メールを送信するまでの期間)]** を選択し、ドロップダウンメニューから電子メールの最小送信間隔を設定します。

ライブビューアクションの作成

ライブビューアクションは、接続されているすべての AXIS Camera Station Proクライアントの **[Live view (ライブビュー)]** タブで特定のカメラ、ビュー、またはプリセット位置を開きます。**[Live view (ライブビュー)]** タブにホットスポット付きの分割ビューが表示されている場合、ライブビューアクションで選択したカメラがホットスポットに表示されます。ホットスポットの詳細については、*分割ビュー*を参照してください。

ライブビューアクションを使用して、開いている AXIS Camera Station Proクライアントをタスクバーからリストアしたり、開いている他のアプリケーションの手前に移動したりすることもできます。

ライブビューアクションを作成するには:

1. **[設定] - [録画とイベント] - [アクションルール]** を選択します。
2. [**新規**] をクリックします。
3. **[Add (追加)]** をクリックしてトリガーを設定します。**[Next (次へ)]** をクリックします。*トリガーの追加*を参照してください。
4. [**追加**] をクリックし、[**ライブビュー**] を選択します。
5. **[OK]**をクリックします。
6. [**Live view actions (ライブビューアクション)**] で、アクションがアクティブなときに何を表示するかを設定します。
7. [**Shown in (表示先)**] で、選択したビューの表示方法を設定します。
8. [**Bring to front (最前面に表示)**] で、[**On trigger bring application to front (トリガー時にクライアント画面を最前面に表示)**] を選択して、開いている AXIS Camera Station Proクライアントをタスクバーからリストアするか、アクションの開始時に開いている他のアプリケーションの手前に表示します。
9. **[OK]**をクリックします。

ライブビューアクション	
表示	[View (ビュー)] を選択し、ドロップダウンメニューからビューを選択します。
カメラ	[Camera (カメラ)] を選択し、ドロップダウンリストからカメラを選択します。カメラにPTZプリセット機能がある場合は、[Go to preset (プリセットに移動)] を選択し、ドロップダウンメニューから範囲を選択してプリセット位置を開きます。
No action (アクションなし)	ビューを開かない場合は、No action (アクションなし) を選択します。

Shown in (表示先)	
ライブアラートタブ	[Live alert tab ([ライブアラート] タブ)] を選択すると、選択したビューまたはカメラビューが [Live alert (ライブアラート)] タブで開きます。
Hotspot in view (ビュー内のホットスポット)	[Hotspot in view (ビュー内のホットスポット)] を選択し、ドロップダウンメニューからホットスポットのあるビューを選択します。アクションがトリガーされたときにホットスポットがライブビューに表示されている場合、ホットスポットにカメラビューが表示されます。

例:
この例では、同じアクションルールで2つのライブビューアクションを使用しています。

1. [Live alert (ライブアラート)] タブでホットスポットビューを表示するライブビューアクションを作成します。
   1.1. [Live view actions (ライブビューアクション)] で、[View (ビュー)] を選択します。
   1.2. [Hotspot view (ホットスポットビュー)] を選択します。
   1.3. [Show (表示する)]で、[[Live alert(ライブアラート)]をタブを選択します。
   1.4. **トリガー時にクライアント画面を最前面**を選択:
2. ホットスポットビューに移動してホットスポットにカメラビューを表示する別のライブビューアクションを作成します。
   2.1. [Live view actions (ライブビューアクション)] で、[Camera (カメラ)]を選択し、カメラビューを選択します。
   2.2. [Show in (表示先)] で、[Hotspot in view (ビュー内のホットスポット)] を選択します。
   2.3. [Hotspot view (ホットスポットビュー)] を選択します。

HTTP通知アクションの作成

HTTP通知アクションは、送信先にHTTP要求を送信します。カメラ、ドアコントローラー、外部のWebサーバー、HTTP要求を受信できるサーバーを送信先にすることができます。たとえば、HTTP通知を使用して、カメラの機能をオンまたはオフにしたり、ドアコントローラーに接続されたドアの開閉、施錠、解錠ができます。

GET、POST、およびPUTメソッドがサポートされています。

注

ローカルネットワークの外部の送信先にHTTP通知を送信するには、AXIS Camera Station Proサーバーのプロキシー設定の調整が必要な場合があります。詳細については、Axisサポートまでお問い合わせください。

HTTP通知アクションを作成するには:

1. **[設定] - [録画とイベント] - [アクションルール]** を選択します。
2. [**新規**] をクリックします。
3. **[Add (追加)]** をクリックしてトリガーを設定します。**[Next (次へ)]** をクリックします。*トリガーの追加*を参照してください。
4. [**追加**] をクリックし、[**HTTP通知を送信**] を選択します。
5. **[OK]**をクリックします。
6. [URL] に、送信先のアドレスと、要求を処理するスクリプトを入力します。例：`https://192.168.254.10/cgi-bin/notify.cgi`
7. 送信先で認証が必要な場合は、[**認証が必要**] を選択します。ユーザー名とパスワードを入力します。
8. 認証方法を選択します。
9. [**詳細設定**] をクリックして、詳細設定を表示します。
10. **[OK]**をクリックします。

認証方式	
ダイジェスト	盗聴からの保護に最適なため、このオプションをお勧めします。
Digest with basic as fallback (ダイジェストとその代替にベーシックを使用)	装置で使用する認証方法が不明な場合は、このオプションを使用してください。

高度	
方式	**[Method(メソッド)]** のドロップダウンメニューからHTTPメソッドを選択します。
コンテンツタイプ	POSTおよびPUTメソッドの場合、[**Content type (コンテンツタイプ)**] ドロップダウンメニューからコンテンツタイプを選択します。
本体	POSTおよびPUTメソッドの場合、[**Body (本文)**] に要求本文を入力します。
Trigger data (トリガーデータ)	ドロップダウンメニューから既定のトリガーデータを挿入することもできます。

Trigger data (トリガーデータ)	
タイプ	このアクションルールをアクティブにしたトリガー。
Source ID (ソースID)	アクションルールをトリガーしたソースを識別します。多くの場合は、カメラやその他のタイプのデバイスです。これを持たないソースもあります。
Source Name (ソース名)	アクションルールをトリガーしたソースの名前。多くの場合は、カメラやその他のタイプの

Trigger data (トリガーデータ)	
	デバイスです。これを持たないソースもあります。
時刻 (UTC)	アクションルールがトリガーされたときのUTC日時。
Time (local) (時刻 (ローカル))	アクションルールがトリガーされたときのサーバーの日時。

仮想I/Oアクションを作成する

仮想I/Oアクションを使用して、デバイス上の特定の仮想入力ポートを有効にします。装置の各ポートはそれぞれ1つのアクションに使用できます。

1. **[設定] - [録画とイベント] - [アクションルール]** を選択します。
2. [**新規**] をクリックします。
3. **[Add (追加)]** をクリックしてトリガーを設定します。**[Next (次へ)]** をクリックします。*トリガーの追加*を参照してください。
4. [**Add (追加)**] をクリックし、[**Virtual I/O (仮想I/O)**] を選択します。
5. **[OK]**をクリックします。
6. 有効にするデバイスとポートを選択します。
7. **[OK]**をクリックします。

サイレンとライトのアクションを作成する

サイレンとライトのアクションは、設定されたプロファイルに従って、AXIS D4100-E Network Strobe Sirenのサイレンとライトパターンをアクティブにします。

注

このアクションを使用するには、装置の設定ページからプロファイルを設定する必要があります。

1. **[設定] - [録画とイベント] - [アクションルール]** を選択します。
2. [**新規**] をクリックします。
3. **[Add (追加)]** をクリックしてトリガーを設定します。**[Next (次へ)]** をクリックします。*トリガーの追加*を参照してください。
4. [**Add (追加)**]をクリックし、[**Siren and light (サイレンとライト)**]を選択します。
5. **[OK]**をクリックします。
6. [**Device (デバイス)**] ドロップダウンメニューから装置を選択します。
7. [**Profile (プロファイル)**] ドロップダウンメニューからプロファイルを選択します。
8. **[OK]**をクリックします。

AXIS Entry Managerアクションの作成

AXIS Entry Managerアクションは、AXIS Entry Managerで設定したドアコントローラーに接続されたドアへのアクセス許可、ロック解除またはロックを行うことができます。

注

AXIS Entry Managerアクションは、AXIS A1001 Network Door Controllerが AXIS Camera Station Proで利用可能な場合にのみ使用できます。

1. **[設定] - [録画とイベント] - [アクションルール]** を選択します。

2. [新規] をクリックします。
3. [Add (追加)] をクリックしてトリガーを設定します。[Next (次へ)] をクリックします。*トリガーの追加*を参照してください。
4. [Add (追加)] をクリックし、[AXIS Entry Manager] を選択します。
5. [OK]をクリックします。
6. アクションを選択し、そのアクションを適用するドアを選択します。
7. [OK]をクリックします。

モバイルアプリ通知の送信アクションを作成する

モバイルアプリ通知の送信アクションでは、AXIS Camera Stationモバイルアプリにカスタムメッセージが送信されます。受信した通知をタップすると、特定のカメラビューに移動できます。*AXIS Camera Stationモバイルアプリユーザーマニュアル*を参照してください。

モバイルアプリ通知の送信アクションを作成する:

1. [設定] - [録画とイベント] - [アクションルール] を選択します。
2. [新規] をクリックします。
3. [Add (追加)] をクリックしてトリガーを設定します。[Next (次へ)] をクリックします。*トリガーの追加*を参照してください。
4. [Add (追加)] をクリックし、[Send mobile app notification (モバイルアプリ通知の送信)] を選択します。
5. [OK]をクリックします。
6. [Message (メッセージ)] に、モバイルアプリのディスプレイに表示するメッセージを入力します。
7. [Click notification and go to (通知をクリックして移動)] で、通知をタップすると表示される内容を設定します。
8. [OK]をクリックします。

通知をクリックして移動	
カメラ	通知をタップしたときに表示するカメラビューを選択します。
デフォルト	[Default (デフォルト)] を選択すると、通知をクリックすると、モバイルアプリのスタートページに移動します。

他のアクションルールをオンまたはオフにするアクションの作成

このアクションを使用すると、たとえば、従業員が認証カードをスワイプした際に、オフィス内の動体検知をオフにすることができます。

ルールをオン/オフにするアクションを作成する:

1. [設定] - [録画とイベント] - [アクションルール] を選択します。
2. [新規] をクリックします。
3. [Add (追加)] をクリックしてトリガーを設定します。[Next (次へ)] をクリックします。*トリガーの追加*を参照してください。
4. [Add (追加)] をクリックし、[Turn rules on or off (ルールをオンまたはオフにする)] を選択します。
5. [OK]をクリックします。
6. 1つ以上のアクションルールを選択します。

7. 選択したアクションルールをオンにするかオフにするかを選択します。
8. 遅延を入力してトリガーからステータスが変わるまでの時間を追加します。
9. トリガーがアクティブでなくなったときに、アクションルールを変更したままにしない場合は、[**Return to the previous state when the trigger is no longer active (トリガーがアクティブでなくなったときに前の状態に戻る)**] を選択します。上の例では、これにより、従業員がアクセスカードをリーダーから外すと動体検知が再びオンになります。
10. **[OK]**をクリックします。

ブックマークアクションの作成

ブックマークアクションは、アクションルールがトリガーされた瞬間に、録画にブックマークを追加します。

ブックマークアクションを作成するには:

1. **[設定] - [録画とイベント] - [アクションルール]** を選択します。
2. [**新規**] をクリックします。
3. **[Add (追加)]** をクリックしてトリガーを設定します。**[Next (次へ)]** をクリックします。*トリガーの追加*を参照してください。
4. **[Add (追加)]** をクリックし、**[Add bookmark (ブックマークの追加)]** を選択します。
5. **[OK]**をクリックします。
6. 名前と、必要に応じて説明を入力し、ブックマークを設定します。
7. **[OK]**をクリックします。

ビデオデコーダにビューを送信するアクションを作成する

このアクションを使用すると、ビデオデコーダにビューを送信し、指定した時間モニターに表示できます。

ビデオデコーダーアクションの送信の作成:

1. **[設定] - [録画とイベント] - [アクションルール]** を選択します。
2. [**新規**] をクリックします。
3. **[Add (追加)]** をクリックしてトリガーを設定します。**[Next (次へ)]** をクリックします。*トリガーの追加*を参照してください。
4. [**Add (追加)**] をクリックして [**Send to video decoder (ビデオデコーダにビデオを送信)**] を選択します。
5. **[OK]**をクリックします。
6. [**Decoder (デコーダ)**] で、ビューを送信するビデオデコーダを選択します。
7. [**View (ビュー)**] で、送信するカメラまたはビューを選択します。
8. [**Duration (表示時間)**]に、ビューを表示する時間を秒単位で入力します。
9. **[OK]**をクリックします。

アクセスコントールアクションの作成

アクセスコントロールアクションは、AXIS Camera Station Secure Entryで以下のアクションを実行できます。

- **ドアアクション:** 選択したドアへのアクセス許可、ロック、ロック解除、リセット、またはロックダウン。
- **ゾーンアクション:** 選択したゾーンにある選択済みのドアのロック、ロック解除、リセット、またはロックダウン。

- **アクセスルールアクション:** アクセスルールをオンまたはオフにします。

注

アクセスコントロールアクションは、AXIS Camera Station Secure Entryでのみ使用できます。

アクセスコントロールアクションを作成する:

1. **[設定] - [録画とイベント] - [アクションルール]** を選択します。
2. [**新規**] をクリックします。
3. **[Add (追加)]** をクリックしてトリガーを設定します。**[Next (次へ)]** をクリックします。*トリガーの追加*を参照してください。
4. [**Add (追加)**] をクリックし、[**Access control (アクセスコントロール)**] を選択します。
5. **[OK]**をクリックします。
6. ドアアクションを実行するには:
   6.1. [**Access control (アクセスコントロール)**] で、[**Door actions (ドアアクション)**] を選択します。
   6.2. [**Configure action (アクションの設定)**] で、ドアとアクションを選択します。
7. ゾーンアクションを実行するには:
   7.1. [**Access control (アクセスコントロール)**] で、[**Zone actions (ゾーンアクション)**] を選択します。
   7.2. [**Configure action (アクションの設定)**] で、ゾーン、ドアのタイプ、アクションを選択します。
8. アクセスルールをオンまたはオフにするには:
   8.1. [**Access control (アクセスコントロール)**] で、[**Action rule actions (アクションルールアクション)**] を選択します。
   8.2. [**Configure action (アクションの設定)**] で、オンまたはオフにするアクセスルールを選択します。
   8.3. [**Action (アクション)**] で、[**Enable (有効)**] または [**Disable (無効)**] を選択します。
9. **[OK]**をクリックします。

- アクションの一環としてレポートを保存するには、[**Save report (レポートの保存)**] を選択し、レポートの設定を行ってください。

AXIS Audio Managerのアクションを作成する

AXIS Audio Managerのアクションは、接続された音声デバイスの音声再生および音量設定を管理します。

AXIS Audio Managerのアクションを作成する:

1. **[設定] - [録画とイベント] - [アクションルール]** を選択します。
2. [**新規**] をクリックします。
3. **[Add (追加)]** をクリックしてトリガーを設定します。**[Next (次へ)]** をクリックします。*トリガーの追加*を参照してください。
4. **[Add (追加)]** をクリックし、**[Audio manager]** を選択します。
5. **[OK]**をクリックします。
6. トリガーするアクションを選択し、設定します。
7. **[OK]**をクリックします。

AXIAudio Managerのアクション	
Play audio file (音声ファイルの再生)	選択した音声ファイルを再生する場合、[Play audio file (音声ファイルの再生)] を選択します。また、リピート回数、優先度、ビジュアルプロファイルなどの再生パラメーターを設定することもできます。
Stop audio file (音声ファイルの停止)	[Stop audio file (音声ファイルの停止)] を選択して、音声再生を停止します。
Enable or disable target (対象の有効化/無効化)	[Enable or disable target 対象の有効化/無効化)] を選択して、デバイスの電源をオンまたはオフにします。
Mute volume (音量のミュート)	音量コントローラーをミュートにする場合、[Mute volume (音量のミュート)] を選択します。
Set volume (音量の設定)	[Set volume (音量の設定)] を選択して、音量コントローラーの音量を設定します。この値は正または負の値をとることができます。
Offset volume (音量のオフセット)	現在の音量レベルから音量を調節する場合、[Offset volume (音量のオフセット)] を選択します。大きくするには正の値を入力し、小さくするには負の値を入力します。

スケジュール

[Schedules (スケジュール)] ページには、録画、アクションルール、およびAXIS Secure Entryなどのコンポーネントに適用できるすべてのスケジュールが表示されます。一部のスケジュールは、インストール中にAXIS Site Designer によって自動的に作成されます。

カスタマイズされた日次・週次スケジュールの作成および編集、スケジュールの上書きができます。上書きスケジュールは常に日単位ですが、祝日などの特別な日には、日次および週次の両方のスケジュールに適用できます。

[Schedules (スケジュール)] タブは、すべての日次スケジュールと週次スケジュールを管理するためのメインビューで、次の情報が表示されます。

- Name (名前): スケジュール名。
- Type (タイプ): スケジュールが日次スケジュールか週次スケジュールかを示します。
- In use (使用中): コンポーネント、録画ルール、またはアクションルールが現在スケジュールを使用しているかどうかを示します。
- Override schedules (オーバーライドスケジュール): このスケジュールに適用されるオーバーライドスケジュールを表示します。

[Override schedules (オーバーライドスケジュール)] タブは、オーバーライドスケジュールを管理するためのメインビューで、それぞれのオーバーライドが適用される日次スケジュールおよび週次スケジュールを確認できます。

注

複数の AXIS Camera Station Proサーバーに接続している場合は、接続されている任意のサーバーでスケジュールを追加および管理できます。[Selected server (選択したサーバー)] のドロップダウンメニューからサーバーを選択して、スケジュールを管理します。

日次スケジュールと週次スケジュールの管理

日次スケジュールと週次スケジュールを管理するには、[Schedules (スケジュール)] タブに移動します。

新しい日次スケジュールまたは週次スケジュールを作成するには、[New schedule (スケジュール新規作成)] をクリックします。

スケジュールを削除するには、リストから削除するスケジュールを選択し、[Delete (削除)] をクリックします。スケジュールを削除する前に、現在使用中ではないことを確認してください。

日次スケジュールまたは週次スケジュールを作成または選択し、詳細を表示します。

- 日次スケジュールの場合、[Add dates (日付の追加)] をクリックし、スケジュールに新しい日付範囲を追加します。同じ日次スケジュールに複数の日付範囲を追加することができます。
- 時間帯を追加するには、+ をクリックするか、行をダブルクリックします。
- 日付範囲や時間帯を編集するには、それを左クリックします。
- オーバーライドスケジュールを追加するには、ドロップダウンメニューからそのスケジュールを選択し、[Add (追加)] をクリックします。オーバーライドスケジュールを削除するには、リストからそのスケジュールを選択し、[Remove (削除)] をクリックします。
- [Apply (適用)] をクリックして変更を保存します。

オーバーライドスケジュールの管理

- オーバーライドスケジュールを管理するには、[Override schedules (オーバーライドスケジュール)] タブに移動します。
- [Add dates (日付の追加)] をクリックし、スケジュールに新しい日付範囲を追加します。同じオーバーライドスケジュールに複数の日付範囲を追加することができます。
- 時間帯を追加するには、+ をクリックするか、行をダブルクリックします。
- 日付範囲や時間帯を編集するには、それを左クリックします。
- [Apply (適用)] をクリックして変更を保存します。

アクションルールの例

例: ドアがこじ開けられました

ドアがこじ開けられました

この例は、何者かが出入口のドアをこじ開けたときに録画とアラームをトリガーするアクションルールを AXIS Camera Station Proで設定する方法を示しています。

開始する前に、以下のことを完了させておく必要があります。

- Axisネットワークドアコントローラーをインストールします。*デバイスの追加, on page 48* を参照してください。
- ドアコントローラーシステムを設定します。「ドアの追加」 *ドアの追加, on page 157*。

アクションルールを作成する:

1. [設定] - [録画とイベント] - [アクションルール] を選択します。
2. [新規] をクリックします。
3. ドアこじ開けイベントをトリガーとして追加します。
   3.1. [追加] をクリックし、[デバイスイベント] を選択します。
   3.2. [OK]をクリックします。
   3.3. [Configure device event trigger (デバイスイベントトリガーの設定)] で、トリガー設定を行います。
   3.4. [Filters (フィルター)] で、フィルター設定を行います。
   3.5. [Activity (アクティビティ)] で、トリガーが信号ラインのアクティビティを示していることを確認します。
   3.6. [OK]をクリックします。

4. [Next (次へ)] をクリックします。
5. 録画アクションを追加します。
   5.1. [追加] をクリックし、[録画] を選択します。
   5.2. [OK]をクリックします。
   5.3. [Camera (カメラ)] ドロップダウンメニューからカメラを選択します。
   5.4. [Video setting (ビデオ設定)] で、プロファイル、プリバッファ、ポストバッファを設定します。
   5.5. [OK]をクリックします。
6. アラームを上げるアクションを追加します。
   6.1. [追加] をクリックし、[アラームを上げる] を選択します。
   6.2. [OK]をクリックします。
   6.3. [Alarm message (アラームメッセージ)] で、アラームのタイトルと説明を入力します。たとえば、「正面出入り口がこじ開けられました」と入力します。
   6.4. [OK]をクリックします。
7. [Next (次へ)] をクリックし、スケジュールには [Always (常時)] を選択します。
8. Finish (終了) をクリックします。

デバイスイベントトリガーを設定	
デバイス	[Device (デバイス)] ドロップダウンメニューからAXISネットワークドアコントローラーを選択します。
イベント	[Event (イベント)] ドロップダウンメニューから [Door (ドア)] > [Door forced (ドアのこじ開け)] を選択します。
Trigger period (トリガー期間)	[Trigger period (トリガー時間)] には10秒を設定します。

フィルター	
ドア名	[Door name (ドア名)] ドロップダウンメニューからドアを選択します。
ドアステータス	[Door status (ドアステータス)] ドロップダウンメニューから [Forced (こじ開け)] を選択します。

ビデオ設定	
プロファイル	[Profile (プロファイル)] のドロップダウンメニューから [High (高)] を選択します。
プリバッファ	[Prebuffer (プリバッファ)] には3秒を設定します。
ポストバッファ	[Postbuffer (ポストバッファ)] には5秒を設定します。

例: 重要人物が入ったとき

重要人物が入ったとき

この例は、重要人物が入ってきたときにウェルカムメッセージを再生してエレベーターを呼び出すアクションルールを AXIS Camera Station Proで作成する方法を示しています。

開始する前に、以下のことを完了しておく必要があります。

- Axisネットワークドアコントローラーをインストールして設定し、カード保有者を追加します。*アクセスコントロールを設定する。, on page 153*および *アクセス管理, on page 192*を参照してください。
- Axisネットワーク音声デバイスをインストールし、カメラに関連付けます。*ストリームプロファイル, on page 56*を参照してください。
- AXIS A9188 Network I/O Relay Moduleを取り付けてI/Oをエレベーターに接続し、ネットワークI/Oリレーモジュールの I/Oポートを AXIS Camera Station Proに追加します。*I/Oポート, on page 95*を参照してください。

アクションルールを作成する:

1. **[設定] - [録画とイベント] - [アクションルール]** を選択します。
2. [**新規**] をクリックします。
3. デバイスイベントをトリガーとして追加する:
   3.1. [**追加**] をクリックし、[**デバイスイベント**] を選択します。
   3.2. **[OK]**をクリックします。
   3.3. [**Configure device event trigger (デバイスイベントトリガーの設定)**] で、イベント設定を行います。
   3.4. [**Filters (フィルター)**] で、フィルター設定を行います。
   3.5. **[Activity (アクティビティ)]** で、トリガーが信号ラインのアクティビティを示していることを確認します。
   3.6. **[OK]**をクリックします。
4. **[Next (次へ)]** をクリックします。
5. ウェルカムメッセージを再生するHTTP通知を送信するアクションを追加する:
   5.1. **[Add (追加)]** をクリックして **[Send HTTP Notification (HTTP通知を送信)]** を選択します。
   5.2. **[OK]**をクリックします。
   5.3. [**URL**] に、ウェルカムメッセージにするオーディオクリップのURLを入力します。
   5.4. **[Authentication required (認証が必要)]** を選択し、音声デバイスのユーザー名とパスワードを入力します。
   5.5. **[OK]**をクリックします。
6. 出力を設定するアクションを追加する:
   6.1. [**追加**] をクリックし、[**出力の設定**] を選択します。
   6.2. **[OK]**をクリックします。
   6.3. [**Output port (出力ポート)**] のドロップダウンメニューから、エレベーターに接続されているI/Oモジュールの出力ポートを選択します。
   6.4. [**State on action (アクション時の状態)**] ドロップダウンメニューから、エレベーターを呼び出すI/Oモジュールの状態を選択します。
   6.5. **[Pulse (パルス)]**を選択し、持続時間を60秒に設定します。
   6.6. **[OK]**をクリックします。
7. **[Next (次へ)]** をクリックし、スケジュールには **[Always (常時)]** を選択します。
8. **Finish (終了)** をクリックします。

デバイスイベントトリガーを設定	
デバイス	[Device (デバイス)] ドロップダウンメニューからAXISネットワークドアコントローラーを選択します。
イベント	[Event (イベント)] ドロップダウンメニューから [Authorization (認証)] > [Access request granted (アクセス要求の許可)] を選択します。
Trigger period (トリガー期間)	[Trigger period (トリガー時間)] には10秒を設定します。

フィルター	
ドア名	[Door name (ドア名)] ドロップダウンメニューからドアを選択します。
Door side (ドア面)	[Door side (ドア面)] ドロップダウンメニューからドア面を選択します。
カード番号	[Card number (カード番号)] を選択し、その人のカード番号を入力します。

クライアントの設定

[設定] - [クライアント] を選択し、

- テーマや言語などのクライアント固有の設定を編集します。*クライアント設定, on page 124*を参照してください。
- 通知や起動オプションなどのユーザー固有の設定を編集します。*ユーザー設定, on page 125*を参照してください。
- ビデオのサイズ変更やハードウェアデコーディングなどのクライアント固有のストリーミングパフォーマンス設定を編集します。*ストリーミング, on page 127*を参照してください。

クライアント設定

これらの設定は、コンピューター上のすべての AXIS Camera Station Proユーザーに適用されます。[Configuration (設定) > [Client (クライアント)] > [Client settings (クライアント設定)] に移動します。

テーマ	
System (システム)、Light (ライト)、Dark (ダーク)	クライアントのテーマを選択します。[System (システム)] は、新規インストールのデフォルトです。 [System (システム)] を選択すると、テーマは Windows のシステムテーマに追従します。

概要	
Windowsの起動時にアプリケーションを起動	オンにすると、Windowsの起動時に AXIS Camera Station Proが自動でオンになります。

ライブビュー	
ライブビューにカメラ名を表示する	ライブビューにカメラ名を表示します。
	[Show recording indicators in live views and maps (ライブビューおよびマップで録画インジケーターを表示)] をオンにすると、動体検知による録画やアクションルールによって開始された録画のインジケーターが表示されます。
	[Show event indicators in live views and maps (ライブビューおよびマップでイベントインジケーターを表示)] をオンにすると、動体検知による録画やアクションルールによって開始された録画に対してインジケーターが表示されます。

マップ	
Allow flashing coverage areas for all maps (すべてのマップで検知範囲の点滅を許可)	この設定をオンまたはオフにし、すべてのマップで検知範囲が点滅するかどうかを管理できます。このグローバル設定はマップレベルのローカル設定には影響しません。マップ, *on page 23*を参照してください。

言語
AXIS Camera Station Proクライアントの言語を変更します。カメラを再起動して変更を適用します。

フィードバック	
Share anonymous client usage data with Axis Communications to help improve the application and user experience (匿名のクライアント使用データをAxis Communicationsと共有して、アプリケーションやユーザーエクスペリエンスの向上に協力する)	匿名データをAxisと共有して、ユーザーエクスペリエンスの向上に協力します。サーバーのこの設定を変更するには、*サーバーの設定, on page 132*を参照してください。

ユーザー設定

これらの設定は、サインインした AXIS Camera Station Proユーザーに適用されます。
[Configuration (設定)] > [Client (クライアント)] > [User settings (ユーザー設定)] に移動します。

ナビゲーションシステム	
ツリービューのナビゲーションシステム	デフォルトではオンになっています.ナビゲーションペインにビュー、カメラ、またはその両方を表示します。
Show in navigation (ナビゲーションに表示)	ドロップダウンメニューから表示する項目 (ビュー、カメラ、またはその両方) を選択します。
ビュー内の移動時にナビゲーションパスを表示します。	オンにすると、分割ビュー内で移動するときにビューの最上部にナビゲーションパスが表示されます。

通知	
Show taskbar notification on alarms (アラームに関するタスクバー通知を表示)	オンにすると、アラームの開始時にWindowsタスクバーに通知が表示されます。
Show taskbar notification for tasks (タスクに関するタスクバー通知を表示)	オンにすると、タスクの追加や完了時にWindowsのタスクバーに通知を表示されます。
[デバイスの管理] に通知を表示	オンにすると、新しいファームウェアがダウンロード可能になったときに通知が表示されます。
インターコム通知ウィンドウを表示する	オンにすると、接続されたインターコムシステムの通話ボタンが押されると、通知ウィンドウが表示されます。

スナップショット	
スナップショットの撮影時にメッセージを表示	オンにすると、誰かがスナップショットを撮ったときにメッセージが表示されます。
スナップショットの保存時にバックグランドでフォルダーを開く	オンにすると、誰かがスナップショットを撮ったときにスナップショットフォルダーが開きます。
参照	[Browse (参照)] をクリックして、スナップショットの保存先フォルダを選択します。

起動	
全画面で開始する	オンにすると、AXIS Camera Station Proが全画面モードで起動します。
最後に使用したタブを記憶する	オンにすると、前回の終了時に開いていたタブ、ビュー、カメラビューで AXIS Camera Station Proが起動します。
最後に使用したモニターを記憶する	オンにすると、前回の終了時に使用していたモニターで AXIS Camera Station Proが起動します。

注

- ビューとカメラビューはタブごとに保存されます。システムは、クライアントが同じサーバーに再接続した場合にのみこれらを記憶します。
- ライブビューでドラッグアンドドロップした動的ビューは記憶されません。
- 異なるユーザーが複数のサーバーに接続している場合、[Remember last used tabs (最後に使用したタブを記憶する)] 機能はサポートされません。

アラーム時に音を鳴らす	
No sound (サウンドなし)	アラームがトリガーされたときに音を鳴らさないようにする場合に選択します。
Beep	アラームがトリガーされたときにビープ音を鳴らす場合に選択します。
Sound file (サウンドファイル)	アラームがトリガーされたときにカスタムサウンドファイルを使用する場合、これを選択して [Browse (参照)] をクリックします。Windows Media Playerで再生可能なあらゆるファイル形式に対応しています。
再生	サウンドをテストする場合にクリックします。

着信時に音を鳴らす	
No sound (サウンドなし)	着信時に音を鳴らさないようにする場合に選択します。
Beep	着信時にビープ音を鳴らす場合に選択します。
Sound file (サウンドファイル)	着信時にカスタムサウンドファイルを使用する場合、これを選択して[Browse (参照)] をクリックします。Windows Media Playerで再生可能なあらゆるファイル形式に対応しています。
再生	サウンドをテストする場合にクリックします。

機能	
スマート検索1を表示	デフォルトで表示されます。スマート検索1を非表示にするには、オフにしてください。

警告ダイアログを表示する	
Invalid certificate warning (無効な証明書の警告)	オンにすると、無効な証明書が検知されると警告が表示されます。

ストリーミング

[Configuration (設定)> Client (クライアント) > Streaming (ストリーミング)] に移動し、ストリーミングオプションを設定します。

ビデオのサイズ変更	
自動サイズ変更	ビデオをクロップしたりアスペクト比を変更しないで利用可能なスペースに合わせて表示する場合に選択します。
ビデオ領域を埋める (場合によってはビデオの一部をクロップ)	選択すると、利用可能なスペース全体にビデオが表示されます。利用可能なスペースのアスペクト比がビデオと異なる場合、システムはそれに合わせてビデオをクロップします。

ハードウェアデコーディング	
モード	• **Automatic (自動):** グラフィックカードを使用して、3840x2160p@25fpss (4KまたはUHD) を超える解像度のストリームをデコードします。 • **On (オン):** グラフィックカードを使用して、1920x1080p@25fps (1080pまたはHD) を超える解像度のストリームをデコードします。 • **Off (オフ):** AXIS Camera Station ProはCPUを使用してビデオをデコードします。
グラフィックスカード	ドロップダウンメニューからグラフィックカードを選択します。

対応グラフィックカード	デコーダ技術
NVIDIA	PureVideo
AMD	Unified Video Decoder (UVD)
Intel	Intel Quick Sync Video (QSV)

注

- ハードウェアデコーディングは、グラフィックカードを使用してビデオをデコードします。高性能グラフィックカードを使用すると、特に高解像度の動画をストリーミングする際、ハードウェアデコーディングによってパフォーマンスが向上し、CPUの使用率を抑えることができます。ハードウェアデコーディングは、H.264およびAV1ストリームのみをサポートしています。
- 解像度が1080p未満のカメラは、ハードウェアデコーディングがオンになっていても、ハードウェアデコーディングを使用できません。
- グラフィックカードが4Kデコーディングをサポートしていない場合、ハードウェアデコーディングがオンになっていても、ハードウェアデコーディングは1080pのストリームでのみ機能します。
- システムに複数のグラフィックカードが搭載されていても、ハードウェアデコーディングには1つのグラフィックカードのみが使用されます。

帯域幅の使用量	
このクライアントではストリームプロファイルを常に [低] にして使用してください	オンにすると、ライブビューで低ストリームプロファイルが使用されます。*ストリームプロファイル*を参照してください。 この設定はH.264およびM-JPEGのビデオに影響し、帯域幅の使用量を低減します。
非アクティブタブのビデオストリームを停止する	オンにすると、非アクティブタブのビデオストリームは停止されます。これにより、帯域幅の使用量が低減されます。。

PTZ （パン、チルト、ズーム）	
PTZを開始する代わりに最初のクリックでビューを選択します	オンにすると、ビュー内の最初のクリックで選択できるます。その後のクリックでPTZ (パン/チルト/ズーム) を操作します。

音声	
Push-to-talk release delay (ms) (Push-To-Talkのリリース遅延 (ミリ秒))	**Push-to-talk (プッシュ・トゥ・トーク)** ボタンを離した後、マイクからの音声の送信が継続する時間をミリ秒単位で設定します。
全二重モードでPush-To-Talkを使用する	単方向、半二重、全二重モードでPush-To-Talkを使用する場合は、オンにします。
インターコムの音声を常に許可する	オンにすると、通話中でないときでもインターコムで会話ができます。

インスタントリプレイ	
Playback duration (s) (再生時間 (秒))	再生時間を[between 1 and 600 seconds(1~600秒)]に設定すると、タイムラインに戻って録画が再生されます。

接続中のサービスの設定

接続中のサービスを管理する

接続中のサービスでは、以下にアクセスできます。

- AXIS Camera Station Webクライアント
- デバイスの管理
- ライセンスの自動管理
- システムのヘルスモニタリング

これらのサービスにアクセスするには、システムを登録し、組織に接続する必要があります。詳細については、*システムを組織に登録する, on page 130*を参照してください。

ステータス	ステータスカードには、お使いのサーバーと接続されているサービスとの接続ステータス、および登録されている組織の名前が表示されます。
切断	サーバーを切断しても、そのサーバーは組織に登録されたままになります。

ライセンス管理	[License management (ライセンス管理)] をオンにすると、ライセンスが自動的に同期されます。システムは、ライセンスの変更内容をAXIS License Managerに送信し、更新されたライセンスの状態を取得します。システムがインターネットに接続されていない場合などに、ライセンスを手動で処理するには、[License management (ライセンス管理)] をオフにします。詳細については、「ライセンス管理」を参照してください。詳細については、*ライセンスを管理, on page 142*を参照してください。
Synchronize system (システムの同期)	[Synchronize system (システムの同期)] をオンにすると、装置およびビューがAXIS Camera Station Webクライアントおよび AXIS Device Managerと自動的に同期されます。

システムを組織に登録する

システムを登録するには:

1. [Configuration (設定)] > [Connected services (接続中のサービス)] > [Management (管理)] に移動します。
2. [Register (登録)] をクリックし、画面の指示に従います。

システムの登録に関する詳細については、*AXIS Camera Station Proのインストールと移行ガイド*を参照してください。

ファームウェアアップグレード設定

注

複数の AXIS Camera Station Proサーバーに接続している場合、[Selected server (選択したサーバー)] ドロップダウンメニューから任意のサーバーを選択して、ファームウェアのアップグレード設定を行うことができます。

1. **[設定] - [接続中のサービス] - [ファームウェアアップグレード設定]** を選択します。
2. [Automatic check for updates (更新の自動確認)] で、ファームウェアの更新を確認する頻度と方法を設定します。
3. [Upgrade order (アップグレードの順序)] で、装置を更新する順序を設定します。

ファームウェア更新の自動確認	
Check for updates (更新を確認する)	**[Every start-up (起動のたびに確認する)]** を選択すると、サーバーの起動のたびに利用可能なファームウェアのバージョンが確認されます。デフォルトでは、AXIS Camera Station Proは **[Never (確認しない)]** に設定されています。
Check now (今すぐ確認)	サーバーで利用可能なファームウェアのバージョンを確認するときにクリックします。

アップグレードの順序	
同時	複数の装置を同時にアップグレードする場合に選択します。このオプションの方が [Sequential (シーケンス)] より高速ですが、すべての装置が同時にオフラインになります。
シーケンシャル	装置を順番にアップグレードを実行する場合に選択します。このオプションの方が時間がかかりますが、装置が同時にオフラインになることはありません。シーケンシャルアップグレードを停止するには、[**Cancel remaining upgrades if one device fails (アップグレードに失敗したデバイスが見つかった場合、残りのアップグレードをキャンセルする)**] を選択します。

ファームウェアの自動確認の有効化

Axis Secure Remote Access v2

Axis Secure Remote Access v2を使用すると、暗号化されたインターネット接続経由で AXIS Camera Station Proサーバーに接続できます。

注

Axis セキュアリモートアクセス v2は、AXIS Camera Station Pro 6.8以降で利用できます。

以下の手順に従って、Axis Secure Remote Access v2を有効にします。

1. サーバーを組織に登録します。*システムを組織に登録する, on page 130*を参照してください。
2. Axis Secure Remote Access v2にサインインします。*Axis Secure Remote Access v2にサインインする, on page 10*を参照してください。

以下の手順に従って、AXIS Camera Station Proサーバーのみにアクセスを制限します。

1. My Systemsで **[Organization (組織)] > [Users (ユーザー)]** に移動します。
2. 設定するユーザーを選択します。
3. **[Roles and access (ロールとアクセス)]** をクリックします。
4. **[ACS Pro Secure Remote Access]** のロールを割り当てます。このロールは、他のAxis My Systemsの機能へのアクセスは許可されず、AXIS Camera Station Proサーバーのみへのアクセスが許可されます。

登録されると、Axis My Systemsで組織のユーザーロールを割り当ててアクセス権限を管理できます。AXIS Camera Station Proユーザーのアクセス権の詳細については、*ユーザー権限, on page 143*を参照してください。

クラウドストレージ

AXIS Camera Station Cloud Storage は、録画をクラウドに保存するライセンスサービスです。詳細については、*AXIS Camera Station Cloud Storageユーザーマニュアル*を参照してください。

重要

AXIS Camera Station Cloud Storageは、AXIS Camera Station Proバージョン6.18 以前でのみ動作します。アップグレードを行う前に、録画をローカルストレージにエクスポートすることをお勧めします。バージョン6.18より新しいバージョンにアップグレードすると、クラウドストレージサービスが利用できなくなり、現在クラウドに保存されているデータがすべて失われます。バージョン6.18向けのセキュリティ更新は、今後のバージョンでクラウドストレージサポートがリストアされるまで継続されます。

クラウドストレージサービスを使用する前に、システムを接続中のサービスに登録する必要があります。システムを登録すると、My Systemsでカメラのクラウドストレージを管理できます。

サーバーの設定

サーバーの設定

[Configuration (設定)] > [Server (サーバー)] > [Settings (設定)] に移動します。

注

複数の AXIS Camera Station Proサーバーに接続している場合は、**[Selected server (選択したサーバー)]**] のドロップダウンメニューからサーバーを選択し、そのサーバーの設定を設定します。

エクスポート	
Include audio when adding recordings to export (エクスポートする録画の追加時に音声を含める)	エクスポートリストに録画を追加するときに、音声を含めるかどうかを選択します。

ログ

アラーム、イベント、監査ログを保持する日数を指定します。7～1,000日の間で値を設定します。

Splunk、Elastic、またはSIEMツールなどのサードパーティ製システムで使用するために、ログをリアルタイムでファイルに継続的に書き込むには、**[Write audit logs to file (監査ログをファイルに書き込む)]**、**[Write event logs to file (イベントログをファイルに書き込む)]**、またはその両方を選択します。

サーバーは、`C:\ProgramData\Axis Communications\AXIS Camera Station\Core\Server\Logs` にログエントリを書き込みます。これらのファイルはプレーンテキストであり、システムレポートから除外されます。

ファイル	説明
`AcsService.exe.audit.log.export`	監査ログのエントリ
`AcsService.exe.event.log.export`	イベントログのエントリ

外部データ

外部データを保持する日数を指定します。1～1,000日の間で値を設定します。

SMTPサーバー

システムアラーム時またはアクションルールトリガー時に電子メールを送信するSMTPサーバーを追加します。

SMTPサーバーを追加するには:

1. [**SMTP servers (SMTPサーバー)**] で、[**Add (追加)**] をクリックします。
2. [**Server (サーバー)**] で、サーバーのアドレス、ポート、認証、TLSプロトコルを設定します。
3. [**Sender (送信者)**] で、送信者として表示される電子メールのアドレスと名前を入力します。

サーバー	
アドレス	SMTPサーバーのアドレスを入力します。
ポート	ポートを入力します。587は、SMTP TLS接続のデフォルトポートです。
TLSを使用する	SMTPサーバーがTLSを使用している場合に選択します。TLSはデフォルトのプロトコルです。
認証を使用する	サーバーがユーザー名とパスワードの入力を必要とする場合に選択し、認証情報を入力します。

編集	SMTPサーバーを編集するには、サーバーを選択して [**編集**] をクリックします。
削除	SMTPサーバーを削除するには、サーバーを選択して [**削除**] をクリックします。ダイアログで [**YEs (はい)**] をクリックするとサーバーが削除されます。
Test all... (すべてテスト...)	SMTPサーバーをテストするには、サーバーを選択して [**Test all... (すべてテスト...)**] をクリックします。ダイアログで、**[Recipient (送信先)]** に電子メールアドレスを入力し、**[OK]** をクリックしてテストメールを送信します。SMTPサーバーがテストを実行し、結果と可能なアクションのリストが表示されます。
矢印	サーバーを選択し、矢印キーを使って順序を設定します。システムは表示された順序でサーバーに接続します。

サーバーテストの結果	
OK	SMTPサーバーへの接続に成功しました。送信先にテストメールが届いていることを確認してください。
不明なエラー	メールの送信中に予期せぬエラーが発生しました。SMTPサーバーが正しく動作しているかどうかを確認してください。
接続できません	AXIS Camera Station ProがSMTPサーバーにアクセスできません。SMTPサーバーが正しく動作していること、AXIS Camera Station ProとSMTPサーバー間のすべてのルーターとプロキシーサーバーがトラフィックを許可していることを確認してください。

サーバーテストの結果	
設定エラー	TLSが要求されましたが、サーバーがStartTLSをサポートしていないか、認証をサポートしていないか、または対応している認証メカニズムがありません。
TLS/SSLハンドシェイクエラー	TLS/SSLネゴシエーション中に、サーバー証明書が無効であるなどのエラーが発生しました。
認証が必要	サーバーは、電子メールを送信するには認証が必要です。
認証エラー	認証情報が正しくない.
接続が切断されました	接続は確立されましたが、その後切断されました。

システムアラーム

カメラの接続が切断された場合、録画データのストレージへのアクセスが拒否された場合、サーバーが予期せずシャットダウンした場合、または録画エラーが発生した場合、システムアラームが作動します。システムアラームに関する電子メール通知を送信することができます。

注

電子メールを送信するには、まずSMTPサーバーを追加する必要があります。

システムアラームに関するメールを送信するには:

1. [**Send email on system alarm to the following recipients (システムアラーム作動時に以下の受信者に電子メールを送信する)**] を選択し、システムアラーム電子メール通知を設定します。
2. [**Recipients (送信先)**] で:
   2.1. アドレスを電子メールの [**To**]、[**Cc**]、または [**Bcc**] フィールドに含める必要があるかどうかを選択します。
   2.2. メールアドレスを入力します。
   2.3. [**Add (追加)**] をクリックして、電子メールアドレスを [**Recipients (送信先)**] ボックスに保存します。

デバイス接続	
Use hostnames instead of IP for newly added devices when possible (可能であれば、新しく追加したデバイスにIPの代わりにホスト名を使用する)	可能であれば、ホスト名を使用して新しく追加したデバイスに接続します。ホスト名が利用できない場合は、代わりにIPアドレスが使用されます。
アクセスできなくなった場合でも、ホスト名を使用し続けます。	ホスト名を使用して接続します。代わりにIPアドレスに自動的に切り替えるには、チェックボックスをオフにします。デバイスに接続するために、ホスト名またはIPアドレスの使用を手動で選択することができます。*接続, on page 75*を参照してください。

言語	
サーバーの言語を変更します	AXIS Camera Station Pro Service ControlおよびAXIS Camera Station Secure Entryの言語を変更します。例: システムアラーム、監査ログメッセージ、**[Data search (データ検索)]**タブの外部データ。カメラを再起動して変更を適用します。

装着式	
ディスク **フォルダー**	装着式システムから拒否されたコンテンツを保存するドライブとフォルダーを選択します。詳しくは、*Axis装着式ソリューション - ユーザーマニュアルの「拒否されたコンテンツストレージに録画を転送する」*を参照してください。
装着式システムから拒否されたコンテンツを保存する日数。	装着式システムから拒否されたコンテンツを保存する日数を設定します。

フィードバック	
Axis Communicationsと匿名サーバーの使用データを共有	アプリケーションやユーザーエクスペリエンスを向上するために匿名のデータをAxisと共有する場合に選択します。クライアントの設定を変更するには、*クライアント設定, on page 124*を参照してください。

高度な設定

これらの設定は、Axisサポートから指示があった場合のみ変更してください。高度な設定の変更手順は以下の通りです。

1. 設定とその値を入力します。
2. [**追加**] をクリックします。

トラブルシューティングのためにデバッグログをオンにするには、[**Enable server side debug logging (サーバー側のデバッグログ出力を有効にする)**] を選択します。この設定では使用するディスク容量が多くなります。**ProgramData**ディレクトリにある`log4net.config` ファイルがそれを上書きします。

詳しくは、*「AXIS Camera Station Pro - トラブルシューティングガイド」の「サーバーの詳細設定」*を参照してください。

コンポーネント

コンポーネントは、システムに機能を追加するソフトウェアモジュールです。**Components (コンポーネント)** ページでは、コンポーネントを管理し、そのステータスを表示できます。

インストールされているコンポーネントのリストを表示するには:

1. [**Configuration > Server > Components (設定 > サーバー > コンポーネント)**] に移動します。
2. [**Show components (コンポーネントを表示)**] をオンにします。

注

Axisはコンポーネントを高度な設定と考えています。必ずAxisサポートに確認してから、コンポーネントを表示および管理してください。

AXIS Camera Station Proの更新

AXIS Camera Station Proを更新する:

1. [Configuration > Server > Update (設定 > サーバー > 更新)] を選択します。
2. [Download and install... (ダウンロードとインストール...)] をクリックします。

注

- 更新が開始すると、手動の場合もスケジュールの場合もキャンセルできません。
- スケジュール設定された更新は自動的に開始されます。
- マルチサーバーシステムでは、常にローカルサーバーを最後に更新してください。
- ローカルサーバーを更新すると、クライアントとサービスコントロールは一時的に終了します。更新中は進行状況インジケーターは表示されません。クライアントとサーバーの両方が再起動するまで、サーバーコンピュータの電源をオンにしておいてください。

インシデントレポート

インシデントレポートの権限をオンにすると、録画、スナップショット、ノートを含むインシデントレポートを作成できます。*インシデントレポートのエクスポート, on page 35*を参照してください。

以下の手順でインシデントレポートを設定します。

1. [Configuration (設定)] > [Server (サーバー)] > [Incident report (インシデントレポート)] に移動します。
2. [Location (場所)] で、インシデントレポートの保存先を選択します。
3. [Export format (エクスポート形式)] のドロップダウンメニューから、録画のエクスポート形式を選択します。
4. [Categories (カテゴリー)] で、カテゴリーを追加または削除して、インシデントレポートをグループ化できます。サーバーのディレクトリパスで変数として設定されている場合、カテゴリー名はエクスポート先のフォルダー名となります。
   4.1. 「事故」や「窃盗」など、ボックスにカテゴリー名を入力します。
   4.2. [追加] をクリックします。
   4.3. カテゴリーを削除するには、カテゴリーを選択し、[Remove (削除)] をクリックします。
5. [Description template (説明テンプレート)] で、インシデントレポート生成時に [Description (説明)] に表示する情報を入力します。たとえば、「報告者: [氏名、電子メール、電話番号]」のように入力します。
6. [適用] をクリックします。

所在地：	
Server directory path (サーバーディレクトリパス)	インシデントレポートをコンピューターのフォルダーに保存するディレクトリパスを入力します。サーバー名、カテゴリー、ユーザー名を変数として使用できます。例：`C:\Reports\$(Server Name)\$(Category)\$(User Name)\`
Network directory path (ネットワークディレクトリパス)	インシデントレポートをネットワークストレージ上のフォルダーに保存する場合に選択します。ディレクトリパスを入力するか、ネットワークストレージの認証情報を使用します。共有は AXIS Camera Station Proサーバーからアクセスできる必要があります。録画に使用するストレージの追加方法については、*ストレージの管理*を参照してください。

Export format (エクスポート形式)	
ASF	画像の改ざんを防ぐために、**[Add digital signature (デジタル署名を追加)]** を選択します。*録画のエクスポート*にある「デジタル署名」のセクションを参照してください。**[Use password (パスワードを使用する)]** を選択して、デジタル署名にパスワードを使用することもできます。
MP4	エクスポートされた録画にはG.711またはG.726形式の音声は含まれません。

録画エクスポートのスケジュール

[Configuration (設定)] > **[Server (サーバー)]** > **[Scheduled export (エクスポートのスケジュール)]** に移動して、録画のエクスポートスケジュールを作成します。

スケジュールされた時刻になると、AXIS Camera Station Proは前回のエクスポート以降のすべての録画をエクスポートします。前回のエクスポートから1週間以上経過している場合、または前回のエクスポートがない場合は、過去1週間分の録画のみが含まれます。それより前の録画をエクスポートするには、**[Recordings (録画)]** タブを開き、手動で録画をエクスポートします。*録画のエクスポート*を参照してください。

注

複数の AXIS Camera Station Proサーバーに接続している場合は、**[Selected server (選択したサーバー)]** のドロップダウンメニューから任意のサーバーを選択して、エクスポートのスケジュールを管理します。

スケジュールされた録画をエクスポートする

1. **[Scheduled export (エクスポートのスケジュール)]** で、**[Enable scheduled export (エクスポートのスケジュールを有効にする)]** を選択します。
2. **[Cameras (カメラ)]** で、録画をエクスポートするカメラを選択します。システムは、表示されているすべてのカメラをデフォルトで選択します。**[Use all cameras (すべてのカメラを使用)]** をオフにして、リスト内の特定のカメラを選択します。
3. **[Export (エクスポート)]** で、録画の保存場所、フォーマット、プレイリストの作成を設定します。
4. **[Weekly schedule (週次スケジュール)]** で、録画をエクスポートする時刻と曜日を選択します。

5. [適用] をクリックします。

エクスポート	
Server directory path (サーバーディレクトリパス)	録画を保存するコンピューター上のフォルダーのディレクトリパスを選択して入力します。
Network directory path (ネットワークディレクトリパス)	録画をネットワークストレージ上のフォルダーに保存する場合に選択します。ディレクトリパスを入力するか、ネットワークストレージの認証情報を使用します。共有は AXIS Camera Station Proサーバーからアクセスできる必要があります。録画に使用するストレージの追加方法については、*ストレージの管理*を参照してください。
プレイリストを作成 (.asx)	Windows Media Playerで使用される.asx形式でプレイリストを作成する場合に選択します。録画は録画された順に再生されます。
Export format (エクスポート形式)	録画データをエクスポートする形式を選択します。 ASF – 画像の改ざんを防ぐために、[Add digital signature (デジタル署名を追加)]を選択します。*録画のエクスポート*にある「デジタル署名」のセクションを参照してください。[Use password (パスワードを使用する)] を選択して、デジタル署名にパスワードを使用することもできます。 MP4 - エクスポートされた録画にはG.711またはG.726形式の音声は含まれません。

Microsoft Windows 2012 Server

Microsoft Windows 2012 Serverを実行しているサーバーから録画データをエクスポートするには、Desktop Experienceをインストールします。

1. メニューから [スタート] - [管理ツール] - [サーバーマネージャー] を選択してサーバーマネージャーを開きます。
2. [管理] - [権限と機能の追加]] を選択して、権限と機能の追加ウィザードを起動します。
3. [Features Summary (機能の概要)] で、[User Interfaces and Infrastructure (ユーザーインターフェースとインフラストラクチャ)] を選択します。
4. [Desktop Experience] を選択し、[Next (次へ)] をクリックします。
5. [インストール] をクリックします。

WebRTC設定

AXIS Camera Station WebクライアントはWebRTCを使用してサーバーと通信します。

TURNの有効化	AXIS Camera Station Proサーバー上でローカルのTURNサーバーをオンにし、WebRTC通信で単一のポートを使用できるようにします。これにより、ファイアウォールの設定を簡素化できます。
Prioritize TURN (TURNを優先する):	WebRTCが中継候補のみを考慮するようにする場合に選択します。

新しい接続

> [Servers (サーバー)] > [New connection (新しい接続)]に移動して、AXIS Camera Station Proサーバーに接続します。*サーバーとの接続*を参照してください。

接続ステータス

> [Servers (サーバー)] > [Connection status (接続状態)] に移動すると、すべてのサーバーの接続状態を確認できます。

サーバー名の横にあるスライダーを使って、サーバーへの接続または切断を行います。

ステータスコード	説明	考えられる対処法
接続	クライアントはこのサーバーとの接続を試みています。	
接続	このサーバーに接続している間、クライアントはTCPを使用します。	
接続済み (Axis Secure Remote Access v2)	このサーバーに接続している間、クライアントはAxis Secure Remote Access v2を使用します。	
接続済み (HTTP)	このサーバーに接続している間、クライアントはHTTPを使用します。HTTPはTCPよりやや非効率的で、複数のサーバーに接続する場合は遅延が生じます。	
切断中	クライアントはこのサーバーとの接続を切断中です。	
切断	クライアントはこのサーバーに接続されていません。	
再接続	クライアントはこのサーバーとの接続が切断され、再接続を試みています。	
再接続に失敗	サーバーは見つかりましたが、ユーザー権限またはパスワードが変更されている可能性があります。	• [User permission (ユーザー権限)] ダイアログでユーザーを追加します。 • ユーザー名とパスワードを確認します。
ログインがキャンセルされました	ユーザーがログインをキャンセルしました。	
ユーザー名またはパスワードが不正です	[Action (アクション)]列のリンクをクリックして、正しいアカウント情報を入力します。	
ユーザーがサーバーで認証されません	サーバーはユーザーのログインを許可しません。	[User permission (ユーザー権限)] ダイアログでユーザーを追加します。

セキュリティ確認が失敗しました	WCF関連のセキュリティチェックが失敗しました。	クライアントとサーバーのコンピューターのUTC時刻を同期させます。
サーバーコンピューターと接続できません	サーバーコンピューターが指定されたアドレスで応答しませんでした。	• ネットワークが正常に動作しているかどうかをチェックします。 • サーバーが動作しているかどうかをチェックします。
サーバーが動作していません	サーバーを動作するコンピューターにはアクセスできますが、サーバーが動作していません。	サーバーを起動します。
通信障害	サーバーへの接続に失敗しました。	• サーバーコンピューターにアクセスできるかを確認します。 • ネットワークが正常に動作しているかどうかを確認します。 • サーバーが動作しているかどうかをチェックします。
無効なホスト名です	DNSがホスト名をIPアドレスに変換できません。	• ホスト名のスペルが正しいことを確認してください。 • DNS がそのホスト名を解決できることを確認してください。
同じサーバーにすでに接続済みです	クライアントはこのサーバーとすでに接続されています。	重複したサーバーエントリを削除してください。
期待されるサーバーではありません	このアドレスで予想とは異なるサーバーから応答がありました。	サーバーを正しいサーバーに更新してください。
クライアントのバージョン (x) とサーバーのバージョン (y) の互換性がありません	クライアントのバージョンがサーバーと比べて古すぎるか新しすぎます。	クライアントとサーバーの両方のコンピューターに、同じバージョンの AXIS Camera Station Proをインストールしてください。
サーバーがビジー状態	パフォーマンスの問題により、サーバーが応答できませんでした。	サーとーコンピューターやネットワークに過負荷がかかっていないことを確認してください。

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。

マルチサーバー

サーバーリスト

AXIS Camera Station Proサーバーをサーバーリストで整理できます。1台のサーバーを複数のサーバーリストに含めることができます。他の AXIS Camera Station Proクライアントでサーバーリストをインポート、エクスポート、使用できます。

> [Servers (サーバー)] > [Server lists (サーバーリスト)] に移動します。

デフォルトの [Recent connections (最近の接続)] リストには、以前のセッションで使用されたサーバーが表示されます。[Recent connections (最近の接続)] は削除できません。

	サーバーリストを選択し、 をクリックして削除します。
新しいサーバーリスト	クリックして新しいサーバーリストを追加し、名前を付けます。
追加	サーバーをサーバーリストに追加するには、サーバーリストを選択し、[Add (追加)] をクリックします。必要な情報を入力します。
Export lists (リストをエクスポート)	クリックして、すべてのサーバーリストを.mslファイル形式でエクスポートします。サーバーリストをインポートして、サーバーに接続することができます。*サーバーとの接続*を参照してください。
編集	サーバーリストのサーバーを編集するには、サーバーを選択し、[Edit (編集)] をクリックします。1度に編集できるのは1台のサーバーのみです。
削除	サーバーリストからサーバーを削除するには、サーバーを選択して [Remove (削除)] をクリックします。
リストの名前を変更する	リストをダブルクリックし、新しい名前を入力します。

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。

サーバーリスト内のサーバーの整理

スイッチの設定

AXIS Camera Station S22 Applianceシリーズのデバイスをお持ちの場合は、AXIS Camera Station Proから設定を行うことができます。[Configuration (設定) > [Switch (スイッチ)] > [Management (管理)] に移動し、認証情報を入力して、スイッチの管理ページを開きます。スイッチの設定については、*axis.com*でAXIS Camera Station S22 Appliance Seriesユーザーマニュアルを参照してください。

注

AXIS Camera Station ProはスイッチのデフォルトIPアドレスの https://192.168.0.1/ にのみ接続できます。

ライセンスを管理

[Manage licenses (ライセンス管理)] ページに、現在のライセンスステータスが表示されます。

試用	AXIS Camera Station Proをインストールすると、90日間の試用期間が与えられます。この期間中、システムのすべての機能が完全に動作します。ライセンスを購入する前に、設定を行ってすべての機能を試すことができます。
ライセンスの確認	システムのライセンス期間が自動更新されずに期限切れになった場合、AXIS License Managerはさらに30日間の猶予期間を提供します。
ライセンスの購入が必要	システムは、一番早い有効期限まで完全なライセンスを保有します。
Changes made in the system require a license synchronization (システムで行った変更にはライセンスの同期が必要)	ライセンスを保有するシステムにデバイスを追加すると、AXIS Camera Station Proがその変更をAXIS License Managerと同期してシステムのライセンスステータスの更新を試みます。自動ライセンシングを使用している場合は、このことに気づかない可能性があります。手動ライセンス方式を使用しており、60日以内に再同期を行わない場合、システムはライセンスなしの状態になります。
ライセンスなし	システムは動作していますが、機能が制限されています。録画とアクションルールは引き続き正常に動作するため、録画が失われることはありません。以下の機能は動作しません: • Live streams (ライブストリーム) • Recordings playback (録画再生) • Instant playback (インスタント再生) • Snapshots (スナップショット) • Recordings export (録画のエクスポート)

以下の2つの方法でシステムにライセンスを追加することができます。

自動ライセンス (オンラインシステム) - システムがライセンス数に影響する変更をAXIS License Managerに自動的に送信し、新しいライセンスステータスを取得します。このオプションにはインターネット接続が必要です。詳細については、*システムをオンラインでライセンスする, on page 143*を参照してください。

手動ライセンス (オフラインシステム) - このオプションを使用すると、手動でシステムファイルをエクスポートし、AXIS License Managerにアップロードし、新しいライセンスをインポートする必要があります。ライセンス数に影響するシステムの変更を行うたびに、このプロセスを繰り返す必要があります。ライセンスを手動で処理する場合や、システムにインターネット接続がない場合は、このオプションを選択します。詳細については、*オフラインのシステムをライセンスする, on page 143*を参照してください。

システムをオンラインでライセンスする

自動ライセンスを使用するには、システムを登録し、組織に接続する必要があります。

1. [Configuration (設定)] > [Licenses (ライセンス)] > [Management (管理)] に移動します。
2. [Automatic licensing (自動ライセンス)] がオンになっていることを確認します。
3. [Register... (登録...)] をクリックします。
4. My Axisアカウントを使用してサインインし、画面の指示に従います。
5. [Go to AXIS License Manager (AXIS License Managerに移動)] をクリックして、ライセンスを管理します。詳細については、help.axis.comの*My Systemsユーザーマニュアル*をお読みください。

オフラインのシステムをライセンスする

システムを手動でライセンスするには:

1. [Configuration (設定)] > [Licenses (ライセンス)] > [Management (管理)] に移動します。
2. [Automatic licensing (自動ライセンス)] をオフにします。
3. [Export system file... (システムファイルのエクスポート...)] をクリックし、コンピューターにファイルを保存します。

注

AXIS License Managerにアクセスするには、インターネット接続が必要です。クライアントコンピューターにインターネット接続がない場合は、インターネット接続のあるコンピューターにシステムファイルをコピーします。

4. *AXIS License Manager*を開きます。
5. AXIS License Managerで:
   5.1. 正しい組織を選択するか、まだ作成していない場合は作成します。詳細については、help.axis.comの*My Systemsユーザーマニュアル*をお読みください。
   5.2. [System setup (システム設定)] に移動します。
   5.3. [Upload system file (システムファイルをアップロード)] をクリックします。
   5.4. [Upload system file (システムファイルをアップロード)] をクリックし、システムファイルを選択します。
   5.5. [Upload system file (システムファイルをアップロード)] をクリックします。
   5.6. [Download license file (ライセンスファイルのダウンロード)] をクリックします。
6. AXIS Camera Station Proクライアントに戻ります。
7. [Import license file... (ライセンスファイルのインポート...)] をクリックし、ライセンスファイルを選択します。
8. [Go to AXIS License Manager (AXIS License Managerに移動)] をクリックして、ライセンスを管理します。

セキュリティの設定

ユーザー権限

[Configuration (設定)] > [Security (セキュリティ)] > [User permissions (ユーザー権限)] に移動して、AXIS Camera Station Proのユーザーとグループを確認します。

注

AXIS Camera Station Proサーバーを実行しているコンピューターの管理者には、自動的に AXIS Camera Station Proの管理者権限が付与されます。管理者グループの権限を変更したり、削除したりすることはできません。

ユーザーまたはグループを追加する前に、それらがローカルコンピューターに登録されているか、Windows® Active Directory のユーザーアカウントを持っていることを確認してください。ユーザーまたはグループを追加するには、*ユーザーまたはグループの追加*を参照してください。

ユーザーがグループに所属している場合、そのユーザーには、個人またはグループに割り当てられる最も高いフォールの権限が付与されます。たとえば、カメラXへのアクセス権を持つユーザーが、カメラYおよびZへのアクセス権を持つグループにも所属している場合、そのユーザーは3つすべてのカメラへのアクセス権を持ちます。

	エントリが1人のユーザーであることを示します。
	エントリがグループであることを示します。
名称	ローカルコンピューターまたはActive Directoryに表示されるユーザー名。
ドメイン	ユーザーまたはグループが属するドメイン。
役割	ユーザーまたはグループに割り当てられるアクセスロール。設定可能な値: 管理者、オペレーター、閲覧者。
詳細	ローカルコンピューターまたはActive Directoryに表示されるユーザーの詳細情報。
サーバー	ユーザーまたはグループが属するサーバー。

ユーザーまたはグループの追加

Microsoft Windows® とActive Directoryのユーザーとグループは AXIS Camera Station Proにアクセスできます。ユーザーを AXIS Camera Station Proに追加するには、ユーザーまたはグループを Windows® に追加する必要があります。

Windows® 10および11でユーザーを追加するには：

- WindowsキーとXを押し、**[Computer Management (コンピューターの管理)]** を選択します。
- **[Computer Management (コンピューターの管理)]** の画面で、**[Local Users and Groups (ローカルユーザーとグループ)]** > **[Users (ユーザー)]** に移動します。
- **[Users (ユーザー)]** を右クリックし、**[New user (新規ユーザー)]** を選択します。
- ポップアップダイアログで、新規ユーザーの詳細を入力し、[**User must change password at next login (ユーザーが次回ログオン時にパスワードを変更する必要があります)**] をクリアします。
- **[Create (作成)]** をクリックします。

Active Directoryドメインをご使用の場合は、ネットワーク管理者にお問い合わせください。

ユーザーまたはグループの追加

1. [**Configuration > Security > User permissions (設定 > セキュリティ > ユーザー権限)**] に移動します。
2. [**追加**] をクリックします。利用可能なユーザーとグループがリストに表示されます。
3. [**Scope (対象)**] で、ユーザーとグループを検索する場所を選択します。

4. [Show (表示)] で、ユーザーまたはグループを表示するかどうかを選択します。ユーザーまたはグループが多すぎる場合、検索結果が表示されないことがあります。フィルターを使用して検索結果を絞り込みます。
5. ユーザーまたはグループを選択し、**[Add (追加)]** をクリックします。

対象	
サーバー	ローカルコンピューター上のユーザーまたはグループを検索する場合に選択します。
ドメイン	Active Directoryのユーザーまたはグループを検索する場合に選択します。
選択したサーバー	複数の AXIS Camera Station Proサーバーに接続している場合は、サーバーを選択してそのサーバー上のユーザーまたはグループを検索します。

ユーザーまたはグループの設定

1. リストからユーザーまたはグループを選択します。
2. [Role (権限)] で、[Administrator (管理者)]、[Operator (オペレーター)]、または [Viewer (閲覧者)] を選択します。
3. [Operator (オペレーター)] または [Viewer (閲覧者)] を選択した場合は、ユーザーまたはグループの権限を設定することができます。*ユーザーまたはグループの権限*を参照してください。
4. **[Save (保存)]** をクリックします。

ユーザーまたはグループの削除

1. ユーザーまたはグループを選択します。
2. **[削除]** をクリックします。
3. ポップアップダイアログで [OK] をクリックするとユーザーまたはグループが削除されます。

ユーザーまたはグループの権限

ユーザーまたはグループに割り当てられるロールは3種類です。ユーザーまたはグループの権限の定義方法については、*ユーザーまたはグループの追加*を参照してください。

管理者 - すべてのカメラのビューのライブおよび録画ビデオへのアクセス、すべてのI/Oポートへのアクセスなど、システム全体へのフルアクセス。このロールは、システム設定にアクセスすることが求められます。

オペレーター - カメラ、ビュー、I/Oポートを選択して、ライブおよび録画ビデオにアクセスします。オペレーターは AXIS Camera Station Proのすべての機能 (システムの設定を除く) へのフルアクセスが許可されます。

閲覧者 - 選択したカメラ、I/Oポート、ビューのライブビデオにアクセスします。録画ビデオへのアクセスやシステムの設定を行うことはできません。

カメラ

[Operator (オペレーター)] または [Viewer (閲覧者)] の権限を持つユーザーまたはグループは、次のアクセス権を利用できます。

アクセス	カメラおよびすべてのカメラ機能へのアクセスを許可します。
ビデオ	このカメラからのライブ映像へのアクセスを許可します。
音声を聞く	カメラから受話するアクセスを許可します。
音声送話	カメラに送話するアクセスを許可します。
Manual Recording (手動録画)	手動で録画を開始・停止することができます。
Mechanical PTZ (メカニカルPTZ)	メカニカルPTZコントロールへのアクセスを許可します。メカニカルPTZを搭載したカメラでのみ使用できます。
PTZ優先度	PTZ優先度を設定します。数値が小さいほど、優先度が高いことを意味します。優先度を割り当てない場合は [0] に設定されます。優先度が最も高いのは管理者です。優先度の高い権限を持つユーザーがPTZカメラを操作する場合、デフォルトでは、他のユーザーは同じカメラを10秒間操作することができません。メカニカルPTZを搭載したカメラで、[**Mechanical PTZ (メカニカルPTZ)**] が選択されている場合のみ使用できます。

ビュー

[**Operator (オペレーター)**] または [**Viewer (閲覧者)**] の権限を持つユーザーまたはグループは、次のアクセス権を利用できます。複数のビューを選択し、アクセス権を設定することができます。

アクセス	AXIS Camera Station Proのビューへのアクセスを許可します。
編集	AXIS Camera Station Proで表示を編集することができます。

I/O

[**Operator (オペレーター)**] または [**Viewer (閲覧者)**] の権限を持つユーザーまたはグループは、次のアクセス権を利用できます。

アクセス	I/Oポートへのフルアクセス権を許可します。
読む	I/Oポートの状態を変更せずに確認することができます。
Write (書き込み)	I/Oポートの状態を変更することができます。

システム

リスト内でグレー表示されているアクセス権限は設定できません。チェックマークは、そのユーザーまたはグループがこの権限を持っていることを意味します。

[**Operator (オペレーター)**] 権限を持つユーザーまたはグループは次のアクセス権を利用できます。[**Take snapshots (スナップショットを撮る)**] は [**Viewer (閲覧者)**] 権限でも利用できます。

スナップショットを撮る	ライブビューおよび録画モードでスナップショットを撮影することができます。
録画のエクスポート	録画のエクスポートを許可します。
インシデントレポートの生成	インシデントレポートの生成を許可します。
Prevent access to recordings older than (これより古い録画へのアクセスを防止)	指定した分数よりも古い録画へのアクセスを防止します。ユーザーはこれらの録画を検索しても見つけることができません。
アラーム、タスク、ログへのアクセス	アラーム通知を受け取り、[Alarms and tasks (アラームとタスク)] バーと [Logs (ログ)] タブへのアクセスを許可します。
Access data search (データ検索へのアクセス)	イベント発生時の状況を追跡するためのデータ検索を許可します。
イベントにカテゴリーを追加する	**録画** タブでイベントにカテゴリを追加できるようにします。
イベントからカテゴリーを削除する	**録画**タブでイベントからカテゴリを削除できるようにします。

アクセスコントロール

[Operator (オペレーター)] 権限を持つユーザーまたはグループは次のアクセス権を利用できます。[Access Management (アクセス管理)] は [Viewer (閲覧者)] 権限でも利用できます。

アクセスコントロールの設定	ドアとゾーン、識別プロファイル、カードフォーマットとPIN、暗号化通信、マルチサーバーを設定することができます。
アクセス管理	アクセス管理ができます。また、Active Directory設定にアクセスすることができます。

AXIS Audio Manager Pro

[Operator (オペレーター)] または [Viewer (閲覧者)] の権限を持つユーザーまたはグループは、次のアクセス権を利用できます。

AXIS Audio Manager Proコンポーネント設定へのアクセス	AXIS Camera Station ProでAXIS Audio Manager Proを設定することができます。また、AXIS Audio Manager Proサーバーインターフェースにアクセスすることができます。オペレーターのみ使用できます。
AXIS Audio Manager Proインターフェースへのアクセス	AXIS Audio Manager Proサーバーインターフェースにアクセスすることができます。閲覧者のみ使用できます。

Viewer (閲覧者) のロールを持つユーザーまたはグループは、次のアクセス権を利用できます。

システムのヘルスモニタリング

[Operator (オペレーター)] 権限を持つユーザーまたはグループは次のアクセス権を利用できます。[>システムの健全性監視へのアクセス] は [Viewer (閲覧者)] 権限でも利用できます。

システムの健全性監視の設定	システムの健全性監視を設定することができます。
システムの健全性監視へのアクセス	システムの健全性監視にアクセスすることができます。

証明書

AXIS Camera Station Proサーバーとデバイスの証明書の設定を管理するには、**[Configuration (設定)] > [Security (セキュリティ)] > [Certificates (証明書)]** に移動します。

HTTPSおよびIEEE 802.1X証明書をオンにする、削除する、表示する方法については、*セキュリティ, on page 74*を参照してください。

AXIS Camera Station Proは以下として使用できます。

- **ルート認証局 (CA):** AXIS Camera Station Proは、独自のルート証明書を使用してサーバー証明書を発行しており、他のルートCAは関与していません。
- **中間認証局：**CA証明書とその秘密鍵を AXIS Camera Station Pro にインポートし、Axisデバイス用のサーバー証明書に署名して発行します。ルート証明書または中間CA証明書にすることができます。

注

AXIS Camera Station Proをアンインストールすると、Windowsの信頼されたルート証明機関からCA証明書が削除されます。インポートされたCA証明書は削除されません。これらの証明書は手動で削除する必要があります。

認証局 (CA)

CAを使用すると、クライアント/サーバー証明書がない装置で、HTTPSおよびIEEE 802.1Xをオンにすることができます。AXIS Camera Station Pro CA証明書があれば、デバイスでHTTPSまたはIEEE 802.1Xを使用するときに、クライアント/サーバー証明書を自動的に作成、署名、インストールすることができます。ルートCAとして AXIS Camera Station Proを使用するか、CA証明書をインポートして AXIS Camera Station Proに中間CAとして動作させることができます。サーバーをインストールすると、ルートCAが生成されます。

インポート	クリックすると、既存のCA証明書とその秘密鍵がインポートされます。AXIS Camera Station Proが証明書パスワードを保存します。
生成	クリックすると、新しい公開鍵と秘密鍵、および10年間有効な自己署名CA証明書が生成されます。新しい認証局を生成すると、すべてのコンポーネントの証明書が置き換えられ、コンポーネントが再起動されます。
表示	クリックすると、CA証明書の詳細が表示されます。

エクスポート	クリックしてCAをファイルにエクスポートします。エクスポートには以下の2通りの方法があります。 • **秘密鍵なしの場合:** 証明書を.cerまたは.crt形式で保存します。AXIS Camera Station Proによって署名された証明書を信頼する他のシステムに公開証明書のみをインストールする必要がある場合は、このオプションを使用します。 • **秘密鍵を使用する場合:** CAをPKCS#12形式 (.pfxまたは.p12) で保存します。CAを別の AXIS Camera Station Proサーバーにインポートする必要がある場合は、このオプションを使用します。 .cer形式、または.crt、形式の証明書は、AXIS Camera Station Proに再インポートすることはできません。
Number of dates the signed client/server certificates will be valid for (署名入りのクライアント/サーバー証明書が有効化される日数)	自動的に作成されたクライアント/サーバー証明書の有効期間を日数で設定します。最大期間は1095日 (3年間) です。CAはその有効期限を超える証明書には署名しません。

ルートCAの生成

AXIS Camera Station Proは起動すると、CAを検索します。CAが見つからない場合は、root CAが自動的に生成されます。これには自己署名ルート証明書、およびパスワードで保護された秘密鍵が含まれています。AXIS Camera Station Proによってパスワードは保存されますが、表示することはできません。AXIS Camera Station Proによって生成されたCA証明書は10年間有効です。

手動で新しいCAを生成して、古いCAと置き換えるには、*CAの置き換え, on page 150*を参照してください。

デバイスに手動で証明書をインストールしたバージョン5.45以前からアップグレードした場合、手動でインストールした証明書の期限が切れると、AXIS Camera Station Proは既存のroot CAを自動的に使用して新しい証明書をインストールします。

注

生成したCA証明書は、Windowsの信頼されたルート証明書に追加されます。

CAのインポート

他のCAからCA証明書をインストールすると、AXIS Camera Station Proを中間CAとして使用できます。証明書と秘密鍵で構成される既存のCAをインポートし、そのCAの代わりに AXIS Camera Station Proが証明書に署名することを許可します。ファイルはPKCS#12ファイルで、証明書にはCA証明書であることを示す基本制約 (2.5.29.19) があり、証明書が有効期間内に使用される必要があります。CAをインポートして既存のCAと置き換えるには、*CAの置き換え, on page 150*を参照してください。

注

- インポートされたCAがパスワードを必要としない場合、何かでパスワードが必要になるたびにダイアログが表示されます。たとえば、装置でHTTPSまたはIEEEを使用するときや、装置を追加するときなどです。[OK] をクリックして続行します。
- インポートしたCA証明書は、Windowsの信頼されたルート証明書に追加されます。
- CA証明書をインポートする際、ルート証明書がWindowsの証明書ストアにすでに存在して

いる必要があります。ルート証明書がない場合、インポートが失敗し、エラーメッセージが表示されます。AXIS Camera Station Proはその前のCAを引き続き使用します。

- AXIS Camera Station Proをアンインストールした後、インポートしたCA証明書をWindowsの信頼されたルート証明機関から手動で削除する必要があります。

CAの置き換え

HTTPS接続を使用する装置で使用される署名付き証明書を発行するCAを置き換えるには:

1. [Configuration > Security > Certificates > HTTPS (設定 > セキュリティ > 証明書 > HTTPS)] に移動します。
2. [Validate device certificate (デバイス証明書を検証する)] をオフにします。
3. [Certificate authority (認証局)] で、[Generate (生成)] または [Import (インポート)] をクリックします。
4. パスワードを入力し、[OK] をクリックします。
5. 署名入りのクライアント/サーバー証明書の有効日数を選択します。
6. [設定] - [デバイス] - [管理] を選択します。
7. 装置を右クリックし、[Security (セキュリティ)] > [HTTPS] > [Enable/Update (有効にする/更新する)] を選択します。
8. [Configuration (設定)] > [Security (セキュリティ)] > [Certificates (証明書)] > [HTTPS] に移動し、[Validate device certificate (デバイス証明書を検証する)] をオンにします。

カスタム証明書を発行する

AXIS Camera Station Pro認証局によって署名されたカスタム証明書を作成できます。たとえば、これらの証明書を外部HTTPSエンドポイントに使用できます。これらの証明書は有効期限が切れたときに、手動で更新する必要があります。カスタム証明書を発行するには:

1. [Configuration (設定)] > [Security (セキュリティ)] > [Certificates (証明書)] に移動します。
2. [Issue custom certificate (カスタム証明書の発行)] で、[Issue certificate... (証明書の発行...)] をクリックします。
3. 証明書の詳細を入力し、[OK] をクリックします。

証明書を発行する	
コモンネーム (CN)	証明書所有者を識別します。CNは通常、証明書をインストールする完全修飾ドメイン名 (FQDN) またはIPアドレスです。
Private key password (秘密鍵のパスワード)	秘密鍵を保護するパスワード。
Duration (days) (期間 (日数))	証明書の有効期間の日数。
Server authentication (サーバー認証)	サーバーの識別情報の証明にサーバーの証明書を使用している場合に選択します。通常、AXIS Camera Station ProがHTTPSを使用して接続するデバイスまたはその他のエンドポイントはサーバーデバイスと見なされ、その証明書ではサーバー認証を使用する必要があります。
Client authentication (クライアント認証)	サーバーに接続する前にクライアントの識別情報の証明にクライアントの証明書を使用している場合に選択します。たとえば、IEEE 802.1Xアクセスコントロールネットワークにアクセスする装置は、ネットワークに入る前にこの証明書を使用する必要があります。

証明書を発行する	
組織 (O)	証明書所有者の組織。
Country code (C) (国コード (C))	証明書所有者の国コード。
DNS SAN	動的ネームサーバーのサブジェクト代替名。証明書所有者に連絡するための代替FQDNです。証明書の発行時、システムはCNをDNS SANとして自動的に追加します。カンマで区切って複数のアドレスを入力できます (例: address-1.com，address-2.com)。
IP SAN	IPアドレスのサブジェクトの代替名。証明書所有者に連絡するための代替IPアドレスです。CNがIPアドレスの場合、システムはCNをIP SANとして自動的に追加します。複数のアドレスはカンマで区切って入力できます。たとえば、192.168.1.1,192.168.1.2のようになります。

HTTPS

デフォルトでは、AXIS Camera Station Proは、接続されている各デバイスでHTTPSサーバー証明書を検証し、検証済みの証明書のないデバイスには接続しません。サーバー証明書は、AXIS Camera Station Proのアクティブなcaによって署名されているか、Windows Certificate Storeを通じて検証されている必要があります。また、AXIS Camera Station Proは、[**Validate device address (デバイスアドレスの検証)**] がオンになっている場合、デバイスのHTTPS証明書のアドレスがデバイスとの通信に使用されるアドレスと一致するかどうかも検証します。

ファームウェアが7.20以降のカメラには自己署名証明書が付属しています。これらの証明書は信頼されていません。代わりに、HTTPSを使用するときに AXIS Camera Station Proが装置に新しい証明書を発行できるように、caを生成するかインポートしてください。

Validate certificate (証明書の検証)	オンにすると、有効な証明書を持つデバイスのみに接続します。証明書の検証を行なわない、無効な証明書を持つデバイスにも接続できます。
デバイスアドレスの検証	オフにすると、ホスト名を使用しないDHCPネットワークで動作がより安定します。 オンにすると、追加のセキュリティのためにアドレスが一致することが求められます。この設定は、デバイスが主にホスト名を使用しているか静的IPアドレスを持つネットワークでのみオンにすることをお勧めします。

注

- セキュアな接続（HTTPS）が利用できない場合、新規にHTTPS証明書を発行することができます。*デバイスの追加, on page 48*を参照してください
- HTTPSを使用するには、ビデオデバイスには5.70以降のファームウェア、アクセスコントロールデバイスと音声デバイスには1.25以降のファームウェアが必要です。

制限事項

- デフォルトでないポート (443以外) はサポートされていません。
- 1つのインストールバッチ内のすべての証明書は、同じパスワードを持っている必要があります。

- [Basic (ベーシック)] などの暗号化されていないチャンネルでの証明書の操作はサポートされていません。[Digest (ダイジェスト)] 通信を許可するには、デバイスを [Encrypted & unencrypted (暗号化および非暗号化)] または [Encrypted only (暗号化のみ)]に設定します。
- AXIS T85 PoE+ Network Switch SeriesではHTTPSをオンにすることはできません。

IEEE 802.1X

AXIS Camera Station Pro IEEE 802.1X認証では、要求を行うデバイスはLANへの接続を求めるAxisネットワークデバイスです。認証を行う装置は、イーサネットスイッチやワイヤレスアクセスポイントなどのネットワーク装置です。認証サーバーは通常、RADIUSおよびEAPプロトコルをサポートするソフトウェアを実行しているホストです。

IEEE 802.1Xをオンにするには、IEEE 802.1X認証CA証明書をインポートする必要があります。IEEE 802.1X認証CA証明書とIEEE 802.1Xクライアント証明書は、IEEE 802.1Xをオンにするか更新するとインストールされます。認証用の証明書は、IEEE 802.1X認証サーバーなどの外部から取得することも、AXIS Camera Station Proで直接生成することもできます。この証明書は各Axisデバイスにインストールされ、認証サーバーを検証します。

注

IEEE 802.1X証明書を使用するには、ビデオデバイスには5.50以降のファームウェア、アクセスコントロールデバイスと音声デバイスには1.25以降のファームウェアが必要です。

IEEE 802.1Xを設定するには:

1. [Configuration > Security > Certificates (設定 > セキュリティ > 証明書)] に移動します。
2. [EAPOL Version (EAPOLのバージョン)] のドロップダウンメニューで、使用するEAP (Extensible Authentication Protocol) のバージョンを選択します。
3. [EAP identity (EAP識別情報)] ドロップダウンメニューで、デバイスのMACアドレス、デバイスのホスト名、またはカスタムテキストを選択します。
4. [Custom (カスタム)] を選択する場合は、EAP IDとして使用するテキストを入力してください。
5. [Import (インポート)] をクリックし、IEEE 802.1X認証CA証明書ファイルを選択します。
6. [Common name (共通名)] ドロップダウンメニューで、各デバイスに作成される証明書の共通名として、[Device IP address (デバイスの IPアドレス)] または [Device EAP identity (デバイスの EAP ID)] を選択します。
7. [設定] - [デバイス] - [管理] を選択します。
8. 装置を右クリックし、[Security > IEEE 802.1X > Enable/Update (セキュリティ > IEEE 802.1X > 有効にする/更新する)] を選択します。

制限事項

- 複数のネットワークアダプターが搭載された装置 (ワイヤレスカメラなど) では、IEEE 802.1Xは最初のアダプター (通常は有線接続) でのみオンにできます。
- `Network.Interface.I0.dot1x.Enabled` パラメーターがないデバイスはサポートされていません。例:AXIS P39 Series、AXIS T85 Series、およびAXIS T87 Video Decoder
- [Basic (ベーシック)] などの暗号化されていないチャンネルでの証明書の操作はサポートされていません。[Digest(ダイジェスト)] 通信を許可するには、デバイスを [Encrypted & unencrypted (暗号化および非暗号化)] または [Encrypted only (暗号化のみ)] に設定します。

証明書の有効期限に関する警告

クライアント/サーバー証明書の有効期限が切れていたり有効期限が近くなっていたりすると、警告が表示されます。この警告により、特定の証明書に対してシステムアラームもトリガーされます。すべてのクライアント証明書とサーバー証明書、AXIS Camera Station Proによってインストー

ルされたデバイスCA証明書、AXIS Camera Station Pro CA証明書、およびIEEE 802.1X証明書に適用されます。警告は、[Device management (デバイス管理)] ページの [Status (ステータス)] にメッセージとして表示され、[Installed certificates (インストール済み証明書)] リストにアイコンとして表示されます。

[Certificate expiration warning (証明書の有効期限切れの警告)] で、有効期限の何日前に AXIS Camera Station Proから通知を受け取るかを指定します。

証明書の更新

サーバーと装置の間の証明書を更新する

AXIS Camera Station Proによって生成されたクライアント/サーバー証明書は、有効期限切れの警告が表示される7日前に自動的に更新されます。これには、デバイスでHTTPSまたはIEEE 802.1Xをオンにする必要があります。証明書を手動で更新するには、*セキュリティ, on page 74*を参照してください。

サーバーとクライアントの間の証明書を更新する

新規サーバー証明書は、AXIS Camera Station Pro Service Controlの **[Certificates (証明書)]** タブで生成できます。手順については、*証明書, on page 236*を参照してください。

パスワードをリセットする

1. [Configuration > Security > Certificates (設定 > セキュリティ > 証明書)] に移動します。
2. **[Validate device certificate (デバイス証明書を検証する)]** をオフにして、CA証明書を使用しているデバイスに引き続きアクセスできるようにします。
3. [Certificate authority (認証局)] で、[Generate (生成)] をクリックし、パスワードを入力します。
4. [Certificate authority (認証局)] で、[Export (エクスポート)] をクリックしてCA証明書をローカルに保存します。
5. **[Configuration (設定)]** > **[Devices (デバイス)]** > **[Management (管理)]** に移動し、選択した装置でHTTPSをオンにします。
6. **[Validate device certificate (デバイス証明書を検証する)]** をオンにします。

アクセスコントロールを設定する。

Axisネットワークドアコントローラーをシステムに追加している場合、バージョン6.x以降のAXIS Camera Stationでアクセスコントロールハードウェアを設定できます。

AXIS Camera Station ProでAxisネットワークドアコントローラーを設定する手順の詳細については、「*Axisネットワークドアコントローラーを設定する*」を参照してください。

注

開始する前に、以下の手順を実行します。

- **[Configuration (設定)]** > **[Devices (デバイス)]** > **[Management (管理)]** からコントローラーのAXIS OSバージョンをアップグレードします。
- **[Configuration (設定)]** > **[Devices (装置)]** > **[Management (管理)]** に移動し、コントローラーの日付と時刻を設定します。
- [Configuration > Devices > Management (設定 > デバイス > 管理)] に移動し、コントローラーでHTTPSをオンにします。

アクセスコントロール設定のワークフロー

1. あらかじめ定義された識別プロファイルの編集や、新しい識別プロファイルの作成を行うには、*識別プロファイル, on page 173*を参照してください。

2. カスタム設定したカードフォーマットとPIN長を使用するには、*カードフォーマットとPIN, on page 175*を参照してください。
3. ドアを追加し、識別プロファイルをドアに適用します。*ドアの追加, on page 157*を参照してください。
4. ドアを設定する:
   – *ドア位置センサーの追加, on page 164*
   – *緊急センサーを追加する, on page 166*
   – *「リーダーの追加」, on page 167*
   – *REX装置の追加, on page 169*
5. ゾーンを追加し、ゾーンにドアを追加します。*ゾーンの追加, on page 170*を参照してください。

ドアコントローラー用デバイスソフトウェアの互換性

重要

ドアコントローラーのAXIS OSをアップグレードする際は、以下の点に留意してください。

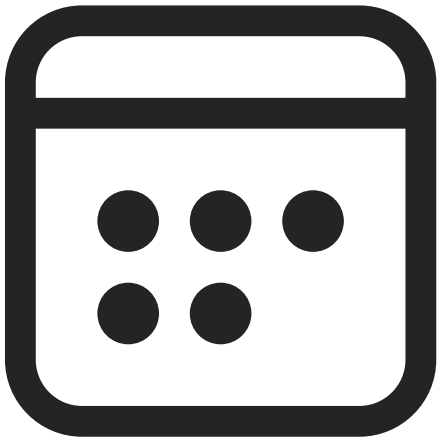
- **サポートされているAXIS OSバージョン:** 以下の対応AXIS OSバージョンは、元の推奨 AXIS Camera Station Proバージョンからアップグレードする場合、およびシステムにドアがある場合にのみ適用されます。システムがこれらの条件を満たしていない場合は、特定の AXIS Camera Station Proバージョンに対して推奨されるAXIS OSバージョンにアップグレードする必要があります。
- **サポートされている最低限のAXIS OSバージョン:** システムにインストールされている最も古いAXIS OSバージョンによって、サポートされる最低限のAXIS OSバージョンが決まります。最大で2つ前のバージョンまで対応します。AXIS Camera Station Proバージョン6.5を使用しており、すべてのデバイスを推奨されるAXIS OSバージョン12.0.86.2にアップグレードするとします。これにより、その後システムでサポートされる最低バージョンは、AXIS OS バージョン12.0.86.2になります。
- **推奨されるAXIS OSのバージョンを超えてアップグレードする場合：**特定の AXIS Camera Station Proバージョンに対して推奨されているAXIS OSのバージョンよりも新しいバージョンにアップグレードするとします。この場合は、AXIS Camera Station Proバージョンに設定されたサポート範囲内であれば、いつでも問題なく推奨のAXIS OSバージョンにダウングレードすることができます。
- **将来のAXIS OSの推奨:** システムの安定性と完全な互換性を確保するため、必ず各 AXIS Camera Station Proバージョンに推奨されるAXIS OSバージョンに従ってください。
- **トラックの変更:** ファームウェアのトラックを10.12.xxから11.0.xx以降に変更するには、工場出荷時の設定へのリセットが必要です。

以下の表は、AXIS Camera Station Proの各バージョンに対する最低限および推奨のAXIS OSバージョンを示しています。

AXIS Camera Stationバージョン	最低限のAXIS OSバージョン	推奨AXIS OSバージョン
Pro 6.17	12.6.102.1	12.9.65.3
Pro 6.16	12.6.102.1	12.9.65.3
Pro 6.15	12.5.68.1	12.8.55.1

ドアとゾーン

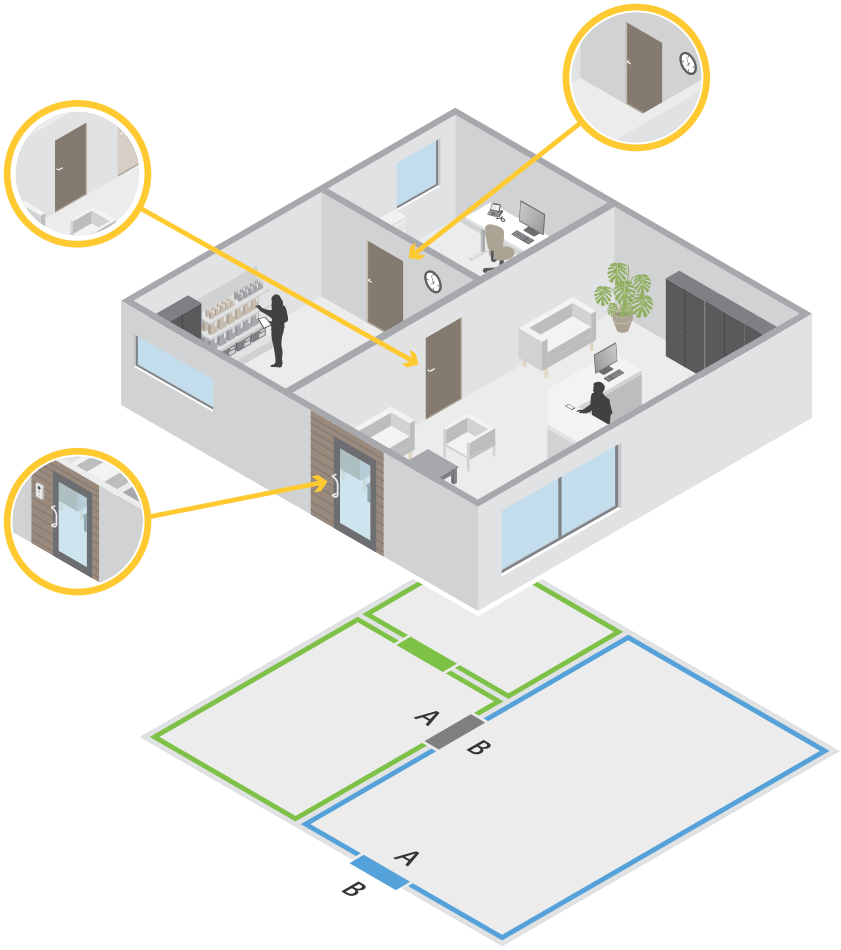
[Configuration > Access control > Doors and zones (設定 > アクセスコントロール > ドアとゾーン)] に移動して、概要を確認し、ドアとゾーンを設定します。

 手動アクション	ドアの状態を手動で設定します。**[Reset (リセット)]** (システムのルールに従う)、**[Grant access (アクセスを許可)]** (ドアを 7 秒間ロック解除)、**[Unlock (ロック解除)]** (ドアをロック解除したままにする)、**[Lock (ロック)]** (ドアをロックしたままにする)、**[Lockdown (閉鎖)]** (誰も出入りできないようにする) のオプションから選択します。
 スケジュールのロック解除	特定の時間にドアが自動でロック解除されるよう、スケジュールを設定します。それ以外の時間は、ドアはロックされたままです。スケジュールが有効になる前に、最初に入室する人が手動でドアのロックを解除できるようにするには、**First person in (最初の人)**をオンにします。
識別プロファイル	ドアの識別プロファイルを変更します。
PINチャート	ドアに関連付けられたコントローラーのピン配置図の表示。ピン配置図を印刷するには、**[Print (印刷)]** をクリックします。
セキュアチャンネル	特定のリーダーのOSDPセキュアチャンネルをオンまたはオフにします。

ドア	
名称	ドア名です。
タイプ	ドア設定のタイプ。
デバイス	ドアに接続されているデバイス。

IPアドレス	ドアに接続されているドアコントローラーのIPアドレス。
側面A	ドアのA面が面しているゾーンです。
側面B	ドアのB面が面しているゾーンです。
識別プロファイル	識別プロファイルはドアに適用されます。
バッテリー	ドアコントローラーのバッテリー状態。
ステータス	ドアの状態。 • Online (オンライン): ドアはオンラインで、正常に動作しています。 • Reader offline (リーダーがオフライン): ドア設定のリーダーがオフライン状態です。 • Reader error (リーダーエラー): リーダーがセキュアチャンネルに対応していないか、リーダーに対してオフに設定されています。 • Old firmware (ファームウェアが古い): デバイスが古いバージョンのファームウェアを実行しています。最大限のパフォーマンスとセキュリティを確保するために、ファームウェアを更新してください。
ゾーン	
名称	ゾーン名です。
ドア数	ゾーンに含まれるドアの数です。
セキュリティレベル	そのゾーンに適用されるセキュリティレベル。

ドアとゾーンの例



- グリーンゾーンとブルーゾーンの2つのゾーンがあります。
- 緑色のドア、青色のドア、茶色のドアの3つのドアがあります。
- 緑色のドアは、緑色のゾーンにある内部ドアです。
- 青色のドアは、青色のゾーン専用の周辺ドアです。
- 茶色のドアは、緑色のゾーンと青色のゾーン共通の周辺ドアです。

ドアの追加

注

- ドアコントローラーは、2つのロックがある1つのドア、またはそれぞれ1つのロックがある2つのドアで構成できます。マルチコントローラーは、追加のロック設定に対応しています。
- ドアコントローラーにドアがなく、新バージョンの AXIS Camera Station Proを使用しており、ドアコントローラーに古いソフトウェアが搭載されている場合は、システムがドアの追加を禁止します。ただし、ドアがすでにある場合、システムコントローラーのソフトウェアが古くても、システムは新しいドアの追加を許可します。

ドアを追加する:

1. [Configuration (設定)] > [Access control (アクセスコントロール)] > [Doors and zones (ドアとゾーン)]に移動します。
2. + [Add (追加)] をクリックし、ドロップダウンリストからドアのタイプを選択します。

ドアのタイプ	
ドア	ロックとリーダーに対応するドアモニター付きの標準的なドア。ドアコントローラーが必要です。
フロア	カードリーダーによってエレベーターの行き先階へのアクセス制御を行う、エレベーター制御向けのドアタイプです。詳細については、*フロアの追加BETA, on page 165*を参照ください。
監視ドア	開閉を通知できるドア。詳しくは、*監視ドアを追加する, on page 164*を参照してください。
ワイヤレスドア	ASSA ABLOY Aperio® のワイヤレスロックと通信ハブで設定可能なドア。詳しくは、*ワイヤレスロックの追加, on page 162*を参照してください。
設置済みドア	ハードウェアを選択せずにシステムに追加できる仮のドアです。

3. ドアの名前を入力し、**[Device (デバイス)]** のドロップダウンメニューでドアコントローラーを選択してドアに関連付けます。ドアを追加できない場合、コントローラーがオフラインの場合、またはHTTPSがオンになっていない場合、コントローラーはグレー表示になります。
4. **[Next (次へ)]** をクリックして [Door configuration (ドアの設定)] ページに移動します。
5. [**Primary lock (プライマリロック)**] ドロップダウンメニューで、リレーポートを選択します。
6. ドアで2つのロックを設定するには、[**Secondary lock (セカンダリロック)**] ドロップダウンメニューからリレーポートを選択します。
7. 識別プロファイルを選択します。*識別プロファイル, on page 173*を参照してください。
8. **[Sensors (センサー)]**、**[Side A (A側)]**、**[Side B (B側)]** でセンサーやリーダーを追加してドアを設定します。
9. 特定のドアの設定を行います。「 *ドア設定, on page 159*」を参照してください。
10. セキュリティレベルを設定します。 *ドアセキュリティレベル, on page 160*を参照してください。
11. **[Save (保存)]** をクリックします。

ドア設定のコピー：

1. **[Configuration (設定)]** > **[Access control (アクセスコントロール)]** > **[Doors and zones (ドアとゾーン)]**に移動します。
2. + **[Add (追加)]** をクリックします。
3. ドアの名前を入力し、**[Device (デバイス)]** のドロップダウンメニューでドアコントローラーを選択してドアに関連付けます。
4. **[Next (次へ)]** をクリックします。
5. [**Copy configuration (設定のコピー)**] ドロップダウンメニューで、既存のドアの設定を選択します。接続されているドアが表示され、コントローラーがグレー表示されている場合は、2つのドアが設定されているか、1つのドアに2つのロックが設定されています。
6. 必要に応じて設定を変更してください。
7. **[Save (保存)]** をクリックします。

ドアとゾーンの追加と設定

ドア設定

ドアを編集するには:

1. [Configuration > Access control > Door and Zones (設定 > アクセスコントロール > ドアとゾーン)] に移動します。
2. 編集するドアを選択します。
3. [Edit (編集)]をクリックします。
4. [Door settings (ドア設定)] で設定を変更し、[Save (保存)] をクリックします。

アクセス時間 (秒)	アクセスが許可された後、ドアがロック解除された状態を維持する秒数を設定します。ドアは、たとえ時間が残っていても、閉まると再びロックされます。
Open-too-long time (sec) (長時間のドア開放 (秒))	ドアモニターを設定した場合のみ有効です。ドアが開いた状態を維持できる秒数を設定します。時間が切れた時点でドアがまだ開いている場合、ドアが開いている時間が長すぎることを知らせるアラームがトリガーされます。アクションルールを設定して、このイベントが発生した際の処理を選択します。
長いアクセス時間 (秒)	この設定を有効にすると、カード所有者のアクセスが許可された後、ドアがロック解除された状態を維持する秒数を設定できます。これにより、標準のアクセス時間が上書きされます。
Long open-too-long time (sec) (長い長時間のドア開放 (秒))	ドアモニターを設定した場合のみ有効です。[Long access time (長時間アクセス時間)] が有効になっている場合、カード所持者に対してドアを開けた状態で維持できる秒数を設定します。標準の「長時間のドア開放」状態の時間を上書きします。
再ロックの遅延時間 (ms)	ドアが開いた後または閉まった後、ロック解除状態を維持する時間 (ミリ秒単位) を設定します。
再ロック	• After opening (開いた後): ドアモニターを追加した場合のみ有効です。 • After closing (閉まった後): ドアモニターを追加した場合のみ有効です。

ドアのこじ開け	ドアが強制的に開放された場合にシステムアラームを作動させるかどうかを選択します。ドア位置センサー（DPS）が必要です。
ドアが開いている時間が長すぎます	ドアが開いている時間が長すぎる場合にシステムアラームを作動させるかどうかを選択します。

ドアを削除するには:

1. [Configuration > Access control > Doors and zones > Doors (設定 > アクセスコントロール > ドアとゾーン > ドア)] を選択します。
2. リストからドアを選択します。
3. [Remove (削除)] をクリックして確定します。

手動アクション

ドアとゾーンには、以下の手動アクションを実行することができます。

リセット - 設定されたシステムルールに戻ります。

アクセスの付与 - ドアまたはゾーンのロックを7秒間解除し、再度ロックします。

ロック解除 - リセットするまでドアのロックが解除されます。

ロック - システムがカード所持者にアクセスを許可するまで、ドアをロックします。

施設や部屋の封鎖 - リセットするかロックを解除するまで、誰も出入りできません。

手動アクションを実行するには、以下の手順に従います。

1. [Configuration (設定)] > [Access control (アクセスコントロール)] > [Doors and zones (ドアとゾーン)] に移動します。
2. ドアまたはゾーンを選択します。
3. 手動アクションのいずれかをクリックします。

ドアセキュリティレベル

ドアに次のセキュリティ機能を追加できます。

2パーソンルール - 2人ルールでは、2人が有効な認証情報を使用してアクセスする必要があります。

ダブルスワイプ - ダブルスワイプすると、カード所持者はドアの現在の状態を無効にすることができます。たとえば、通常のスケジュール外でのドアのロックまたはロック解除に使用でき、システムからドアのロックを解除するよりも便利です。ダブルスワイプは既存のスケジュールには影響しません。たとえば、ドアが閉店時にロックされるようにスケジュールされていて、従業員が昼休みに店外に出ても、ドアはスケジュールに従ってロックされます。

セキュリティレベルは、新しいドアの追加時に設定するか、既存のドアに適用することができます。

既存のドアに**2人ルール**を追加するには:

1. [Configuration (設定)] > [Access control (アクセスコントロール)] > [Doors and zones (ドアとゾーン)] に移動します。
2. セキュリティレベルを設定するドアを選択します。
3. **[Edit] (編集)** をクリックします。
4. [Security level (セキュリティレベル)] をクリックします。

5. **2人ルール**をオンにします。
6. [**適用**] をクリックします。

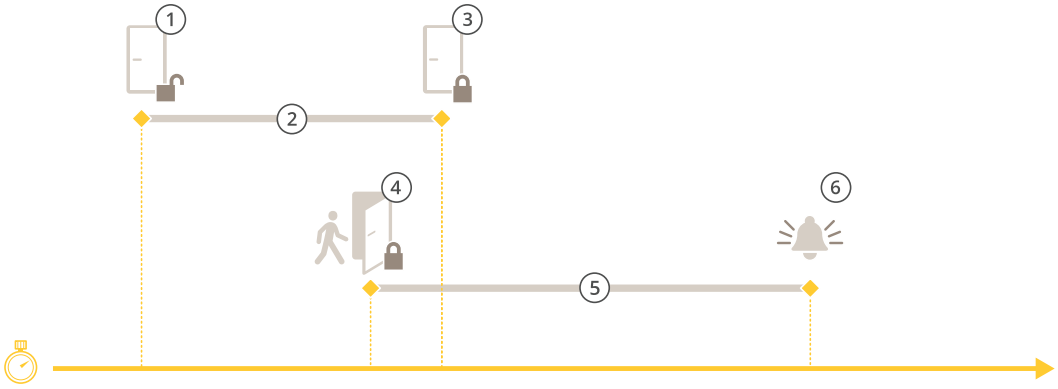
2パーソンルール	
Side A (A面) とSide B (B面)	ルールを使用するドアの面を選択します。
スケジュール	ルールがいつアクティブになるかを選択します。
タイムアウト (秒)	タイムアウトは、カードがスワイプされてから次のスワイプまで、またはその他の有効な認証情報が提供されてから次に提供されるまでの最大許容時間です。

既存のドアに**ダブルスワイプ**を追加するには:

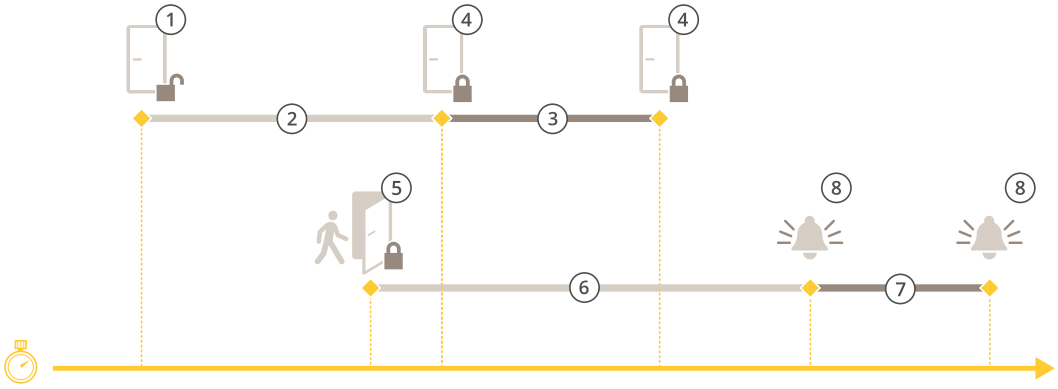
1. [Configuration (設定)] > [Access control (アクセスコントロール)] > [Doors and zones (ドアとゾーン)] に移動します。
2. セキュリティレベルを設定するドアを選択します。
3. **[Edit] (編集)** をクリックします。
4. [Security level (セキュリティレベル)] をクリックします。
5. **ダブルスワイプ**をオンにします。
6. [**適用**] をクリックします。
7. カード所持者に**ダブルスワイプ**を適用します。
   7.1. [Access Management (アクセス管理)] タブを開きます。
   7.2. 編集するカード所持者の ⋮ をクリックし、**[Edit (編集)]**をクリックします。
   7.3. [More (詳細)] をクリックします。
   7.4. [Allow double-swipe (ダブルスワイプを許可する)] を選択します。
   7.5. [**適用**] をクリックします。

ダブルスワイプ	
タイムアウト (秒)	タイムアウトは、カードがスワイプされてから次のスワイプまで、またはその他の有効な認証情報が提供されてから次に提供されるまでの最大許容時間です。

時間のオプション



1. *アクセス許可 - ロック解除*
2 *アクセス時間*
3 *アクションなし - ロックはロックされたまま*
4 *アクションの実行 (ドアの開放) – ロック施錠、またはドアが閉じるまでロック解除状態を維持*
5 *長時間のドア開放*
6 *長時間のドア開放アラームの生成*



1. *アクセス許可 - ロック解除*
2 *アクセス時間*
3 *2+3: 長いアクセス時間*
4 *アクションなし - ロックはロックされたまま*
5 *アクションの実行 (ドアの開放) – ロック施錠、またはドアが閉じるまでロック解除状態を維持*
6 *長時間のドア開放*
7 *6+7: 長い長時間のドア開放*
8 *長時間のドア開放アラームの生成*

ワイヤレスロックの追加

AXIS Camera Station Proは、ASSA ABLOY Aperio® のワイヤレスロックと通信ハブに対応しています。ワイヤレスロックは、ドアコントローラーのRS485コネクターに接続されたAperio通信ハブを介してシステムに接続します。16個のワイヤレスロックを1台のドアコントローラーに接続できます。

注

- 設定には、AxisドアコントローラーでAXIS OSバージョン11.6.16.1以降が必要です。
- 設定には、AXIS Door Controller Extensionの有効なライセンスが必要です。
- Axisドアコントローラーと AXIS Camera Station Proサーバーの時刻を同期する必要があります。
- 開始する前に、ASSA ABLOYがサポートするAperioアプリケーションを使用して、Aperioロックと Aperioハブをペアリングします。
- RS485コネクター1個につき、Aperioハブは1台のみ接続可能です。マルチドロップには対応していません。
- ワイヤレスロックは、オフライン状態ではロック解除スケジュールに従いません。

1. ドアコントローラーにアクセスします。
   1.1. **[設定] - [デバイス] - [他のデバイス]** を選択します。
   1.2. Aperio通信ハブに接続されているドアコントローラーのwebインターフェースを開きます。
2. AXIS Door Controller Extensionをオンにします。
   2.1. ドアコントローラーのwebインターフェースで、[**Apps (アプリ)**] に移動します。
   2.2. AXIS Door Controller Extensionのコンテキストメニュー を開きます。
   2.3. [**Activate license with a key (キーによるライセンスのアクティブ化)**] をクリックし、ライセンスを選択します。
   2.4. **AXIS Door Controller Extension**をオンにします。
3. 通信ハブを介してワイヤレスロックをドアコントローラーに接続します。
   3.1. ドアコントローラーのwebインターフェースで、[**Access control > Wireless locks (アクセスコントロール > ワイヤレスロック)**] に移動します。
   3.2. [**Connect communication hub (通信ハブを接続する)**] をクリックします。
   3.3. ハブの名前を入力し、[**Connect (接続)**] をクリックします。
   3.4. [**Connect wireless lock (ワイヤレスロックを接続)**] をクリックします。
   3.5. 追加するロックのアドレスと機能を選択し、[**Save (保存)**] をクリックします。
4. ワイヤレスロック付きのドアを追加し、設定します。
   4.1. AXIS Camera Station Proで、**Configuration > Access control > Doors and zones (設定 > アクセスコントロール > ドアとゾーン)**] に移動します。
   4.2. **[Doors (ドア)]** で **[Add (追加)]** をクリックします。
   4.3. **[Wireless door (ワイヤレスドア)]** を **[Door type (ドアタイプ)]** に選択し、Aperio通信ハブに接続されているドアコントローラーを選択します。
   4.4. **[Next (次へ)]** をクリックします。
   4.5. [**Wireless lock (ワイヤレスロック)**] を選択します。
   4.6. ドアのA面とB面を定義し、センサーを追加します。詳細については、*ドアとゾーン, on page 154*を参照してください。

4.7. [Save (保存)] をクリックします。

ワイヤレスロックを接続すると、ドアの概要でバッテリー残量とステータスを確認できます。

バッテリー残量	アクション
良好	なし
低	ロックは意図したとおりに作動しますが、バッテリー残量が限界に達する前にバッテリーを交換する必要があります。
重大	バッテリーを交換する.ロックが意図したとおりに動作しない可能性があります。

ロックステータス	アクション
オンライン	なし
ロックの詰まり	ロックの機械的な問題を解決してください。

ドア位置センサーの追加

ドア位置センサーは、ドアの物理的な状態を検知するスイッチです。ドアにドア位置センサーを追加し、その接続方法を設定することができます。

1. [Door configuration (ドアの設定)] ページに移動します。 *ドアの追加, on page 157*を参照してください。
2. [Sensors (センサー)] で、[Add (追加)] をクリックします。
3. **[Door position sensor (ドア位置センサー)]** を選択します。
4. ドアモニターを接続するI/Oポートを選択します。
5. [Door open if (ドアが開く条件)] で、ドアモニター回路の接続方法を選択します。
6. デジタル入力が新しい安定状態に移行するまで状態変化を無視するには、**[Debounce time (デバウンス時間)]** を設定します。
7. ドアコントローラーとドアモニターの間の接続が中断された場合にイベントをトリガーするには、[Supervised input (状態監視入力)] をオンにします。*監視入力, on page 172*を参照してください。

ドアが開く条件	
回路が開いている	ドアモニター回路はNC (Normally Closed) です。回路が開くと、ドアモニターはドアが開いている信号を送信します。回路が閉じると、ドアモニターはドアが閉じている信号を送信します。
回路が閉じている	ドアモニター回路はNO (Normally Open) です。回路が閉じると、ドアモニターはドアが開いている信号を送信します。回路が開くと、ドアモニターはドアが閉じている信号を送信します。

監視ドアを追加する

監視ドアは、開閉状態を表示できるタイプのドアです。たとえば、施錠は必要ないが開閉状態を知る必要がある防火扉に、このオプションを使用できます。

監視ドアは、ドアモニター付きの通常のドアとは異なります。ドアモニター付きの通常のドアは、ロックとリーダーをサポートしていますが、ドアコントローラーが必要です。監視ドアは、1つのドアポジションセンサーをサポートしていますが、ドアコントローラーに接続されたネットワークI/Oリレーモジュールのみが必要です。1つのネットワークI/Oリレーモジュールには、最大5つのドアポジションセンサーを接続できます。

注

監視ドアには、AXIS Monitoring Door ACAPアプリケーションを含む最新ファームウェアが搭載されたAXIS A9210 Network I/O Relay Moduleが必要です。

監視ドアを設定するには:

1. AXIS A9210を設置し、AXIS OSの最新バージョンにアップグレードします。
2. ドアポジションセンサーを取り付けます。
3. AXIS Camera Station Proで、[**Configuration (設定)**] > [**Access control (アクセスコントロール)**] > [**Doors and zones (ドアとゾーン)**] に移動します。
4. [**Add door (ドアを追加)**] をクリックします。
5. 名前)を入力します。
6. [**Type (タイプ)**] で、[**Monitoring door (監視ドア)**] を選択します。
7. [**Device (デバイス)**] で、ネットワークI/Oリレーモジュールを選択します。
8. **[Next (次へ)]** をクリックします。
9. [**Sensors (センサー)**] で、 [**Add (追加)**] をクリックし、[**Door position sensor (ドアポジションセンサー)**] を選択します。
10. ドアポジションセンサーに接続されているI/Oを選択します。
11. [**追加**] をクリックします。

フロアの追加BETA

フロアはエレベーター各階へのアクセスを管理するために使用するドアタイプです。フロアを追加すると、そのエレベーターのすべての階をグループ化するエレベーターリソースが作成されます。各フロアは、ユーザーがその階へアクセスすることを許可する前に、エレベーター内に設置されたカードリーダーを使用してユーザーを認証します。

開始する前に以下が必要です。

- システムに追加された対応ネットワークドアコントローラー (*A1610*、*A1710-B*、*A1810-B*など)。
- 追加のリレー用の*A9910 I/O Relay Expansion Module*。コントローラーにモジュールを追加するには、を参照してください。

注

この機能はベータ版です。現在、最大16のフロアおよびカードリーダーのみに対応しています。

フロアを設定するには:

1. **[Configuration (設定)]** > **[Access control (アクセスコントロール)]** > **[Doors and zones (ドアとゾーン)]** に移動します。
2. **[Add (追加)]** をクリックし、**[Floor (フロア)]** BETA を選択します。
3. フロアの名前を入力します。
4. コントローラーを選択します。
5. **[Elevator (エレベーター)]** で既存のエレベーターを選択するか、**[Create new elevator (エレベーターの新規作成)]** をクリックして新しいエレベーターを追加し、名前を入力します。

6. **[Side A (A面)]** で **[Card reader (カードリーダー)]** を選択し、リーダーを設定します。**[Side B (B面)]** は安全上の理由により設定できません。
7. **[Save and add new (保存して新規追加)]** をクリックして同じエレベーターにフロアを追加します。エレベーターとリーダーの設定は、次のフロア用に入力されたまま維持されます。このオプションは、コントローラーにリレーがある場合のみ利用できます。
8. フロアを追加したら、**[Save (保存)]** をクリックします。フロアは「エレベーター名 - フロア名」のように表示されます (例: "West Side - Floor 1")。

注

- 複数のフロアで使用されているリーダーは、最初に追加されたフロアでのみ編集することができます。
- 関連するすべてのフロアが削除されると、エレベーターは自動的に削除されます。

緊急センサーを追加する

緊急入力を追加して、ドアをロックまたはロック解除するアクションを開始するように設定できます。回路の接続方法を設定することもできます。

1. [Door configuration (ドアの設定)] ページに移動します。 *ドアの追加, on page 157*を参照してください。
2. **[Sensors (センサー)]** で、 **[Add (追加)]** をクリックします。
3. [**Emergency input (緊急入力)**] を選択します。
4. [**Emergency state (緊急状態)**] で、回路接続を選択します。
5. デジタル入力が新しい安定状態に移行するまで状態変化を無視するには、[**Debounce time (ms) (デバウンス時間 (ミリ秒))**] を設定します。
6. [**Emergency action (緊急アクション)**] で、ドアが緊急状態シグナルを受信したときにトリガーする緊急アクションを選択します。

緊急状態	
回路が開いている	緊急入力回路はNC (Normally Closed) です。緊急入力は、回路が開いたときに緊急状態信号を送信します。
回路が閉じている	緊急入力回路はNO (Normally Open) です。緊急入力は、回路が閉じたときに緊急状態信号を送信します。

緊急アクション	
ドアロック解除	緊急状態信号を受信すると、ドアのロックが解除されます。
ドアのロック	緊急状態信号を受信すると、ドアがロックされます。

IPリーダーを追加する

AXISネットワークインターコムやその他のIP対応デバイスをリーダーとして使用できます。ドアに割り当てる前に、AXIS Camera Station Proにデバイスを追加する必要があります。

注

開始する前に、IPリーダーの電源が入っており、AXIS Camera Station Proと同じネットワークに接続されていることを確認してください。

1. [Configuration (設定)] > [Devices (デバイス)] > [Add devices (デバイスの追加)] に移動します。
2. 検出されたデバイスのリストからIPリーダーを選択し、[Add (追加)] をクリックします。
3. プロンプトが表示されたら、デバイスの認証情報を入力します。

デバイスが追加されると、ドアに割り当てることができます。*「リーダーの追加」, on page 167* を参照してください。

「リーダーの追加」

ドアコントローラーは、複数の有線リーダーに対応するように設定できます。ドアの片側または両側にリーダーを追加するか選択します。

カードフォーマットやPIN長のカスタム設定を適用した場合、[Configuration (設定)] > [Access control (アクセスコントロール)] > [Doors and zones (ドアとゾーン)] の.[Card formats (カードフォーマット)] に表示されます。*ドアとゾーン, on page 154*を参照してください。

注

- ドアコントローラーに最大16台のBluetoothリーダーを追加することもできます。詳しくは、*Bluetoothリーダーの追加, on page 168*を参照してください。
- Axisネットワークインターコムを IPリーダーとして使用する場合、システムはデバイスのWebページで設定されたPIN設定を使用します。

1. [Door configuration (ドアの設定)] ページに移動します。*ドアの追加, on page 157*を参照してください。
2. ドアのどちらかの面で [Add (追加)] をクリックします。
3. [Card reader (カードリーダー)] を選択します。
4. [Reader type (リーダータイプ)] を選択します。
5. このリーダーにカスタムPIN長を使用する:
   5.1. [詳細設定] をクリックします。
   5.2. [Custom PIN length (カスタムPIN長)] をオンにします。
   5.3. [Min PIN length (最小PIN長)]、[Max PIN length (最大PIN長)]、[End of PIN character (PIN文字の終端)] をそれぞれ設定します。
6. このリーダーにカスタムカードフォーマットを使用する:
   6.1. [詳細設定] をクリックします。
   6.2. [Custom card formats (カスタムカードフォーマット)] をオンにします。
   6.3. リーダーで使用するカードフォーマットを選択します。すでに同じビット長のカードフォーマットを使用している場合は、まずそれを無効にする必要があります。カードフォーマットの設定がシステムの設定と異なる場合、クライアントに警告アイコンが表示されます。
7. [追加] をクリックします。
8. ドアの反対側の面にリーダーを追加するには、この手順を繰り返します。

AXIS Barcode Readerの設置方法については、*AXIS Barcode Readerの取り付け, on page 178*を参照してください。

リーダータイプ	
OSDP RS485 half duplex (OSDP RS485半二重)	RS485リーダーの場合は、[OSDP RS485 half duplex (OSDP RS485半二重)] とリーダーポートを選択します。

Wiegand	Wiegandプロトコルを使用するリーダーの場合は、[**Wiegand**] とリーダーポートを選択します。
IPリーダー	IPリーダーの場合は、[**IP reader (IPリーダー)**] を選択し、ドロップダウンメニューから装置を選択します。Axisネットワークインターコムを IPリーダーとして使用できます。

Wiegand	
LEDコントロール	[**Single wire (シングルワイヤー)**] または [**Dual wire (R/G) (デュアルワイヤー (R/G))**] を選択します。デュアルLEDコントロールを備えたリーダーは、通常、赤、緑のLED用にさまざまな配線を使用します。
いたずら警告	リーダーのタンパー入力を作動させる回路の状態を選択します。 • **Open circuit (開回路)**: リーダーは、回路が開くとタンパー信号を送信します。 • **Closed circuit (閉回路)**: リーダーは、回路が閉じるとタンパー信号を送信します。
Tamper debounce time (いたずらのデバウンス時間)	リーダーへのいたずら入力が新しい安定状態に移行するまで状態変化を無視するには、**[Tamper debounce time (いたずらのデバウンス時間)]** を設定します。
状態監視入力	オンにすると、ドアコントローラーとリーダーの間の接続が中断されたときにイベントがトリガーされます。*監視入力, on page 172*を参照してください。

Bluetoothリーダーの追加

AXIS A4612 Network Bluetooth Readerを使用して、Axis ドアコントローラーの有線ドアの接続範囲を拡張することができます。1つのドアコントローラーにつき、最大16のこのリーダーを割り当てることができます。各リーダーは、ドアロック、Request-to-Exit (REX)、Door Position Switch (DPS) を管理できます。

これらのリーダーを追加して使用する場合、追加のライセンスは必要ありません。

以下の手順に従って、AXIS A4612 Network Bluetooth Readerをドアに追加します。

1. AXIS A4612とドアコントローラーがペアリングされていることを確認します。*AXIS Mobile Credentialアプリを Bluetooth認証情報として使用する, on page 169*を参照してください。
2. [Door configuration (ドアの設定)] ページに移動します。*ドアの追加, on page 157*を参照してください。
3. ドアの片面で、**[Add (追加)]** をクリックし、**[Card reader (カードリーダー)]** を選択します。
4. **[IP reader (IPリーダー)]** を選択し、ドロップダウンメニューからペアリングされたAXIS A4612を選択します。このリーダーを認証情報のペアリングに使用する場合は、ペアリング用にマークを付けます。[**追加**] をクリックします。

5. [Overview (オーバービュー)] タブで、識別プロファイルを変更します。ドアの片面のみにAXIS A4612を取り付け、反対の面にREXを使用する場合は、[Tap in app (アプリでタップ)]または[Touch reader (リーダーをタッチ)] のプロファイルを使用できます。

AXIS Mobile Credentialアプリを Bluetooth認証情報として使用する

この例では、AXIS A4612 Bluetooth Readerをシステムに追加して、カード所持者がAXIS Mobile Credentialアプリを使用してドアを解錠できるようにする方法を示します。

1. Bluetoothリーダーを取り付け、ドアコントローラーに接続します。
2. ドアコントローラーのWebインターフェースでBluetoothリーダーを追加します。
   2.1. ドアコントローラーにアクセスし、[Peripherals (周辺機器)] > [Readers (リーダー)] に移動します。
   2.2. [Add reader (リーダーの追加)] をクリックします。
   2.3. [Add Bluetooth reader (Bluetoothリーダーの追加)] ダイアログに必要な情報を入力します。
   2.4. [追加] をクリックします。
3. AXIS Camera Station Proで、ドアにBluetoothリーダーを追加します。
   3.1. [Configuration (設定)] > [Access control (アクセスコントロール)] > [Doors and zones (ドアとゾーン)] に移動します。
   3.2. Bluetoothリーダーを追加するドアを選択し、[Edit (編集)] をクリックします。
   3.3. Bluetoothリーダーが取り付けられているドアの側で + [Add (追加)] をクリックします。
   3.4. [Card reader (カードリーダー)] を選択します。
   3.5. [Add IP reader (IPリーダーの追加)] で、[IP reader (IPリーダー)] を選択します。
   3.6. [Select IP reader (IPリーダーの選択)] で、追加するBluetoothリーダーを選択します。
   3.7. [追加] をクリックします。
4. ペアリングするBluetoothリーダーを選択します。システム内の1台以上のBluetoothリーダーに対して、この手順を実行する必要があります。
   4.1. 先ほど追加したBluetoothリーダーを選択します。
   4.2. [Edit] (編集) をクリックします。
   4.3. [Edit bluetooth reader (Bluetoothリーダーの編集)] で、[Use this reader for pairing (ペアリングにこのリーダーを使用する)] を選択します。
   4.4. [適用] をクリックします。
5. [Tap in app (アプリでタップ)] または [Touch reader (リーダーにタッチ)] のいずれかの識別プロファイルを選択します。詳細については、*識別プロファイル, on page 173*を参照してください。
6. カード所持者にモバイル認証情報を追加します。*認証情報の追加, on page 194*を参照してください。
7. モバイル認証情報とペアリングリーダーをペアリングします。
   7.1. ペアリングが有効になったBluetoothリーダーにカード所持者の携帯電話を近づけます。
   7.2. カード所持者に送信された電子メールに記載されている手順に従います。

REX装置の追加

ドアの片面または両面にREX (退出要求) 装置を追加できます。REX装置には、PIRセンサー、REXボタン、またはプッシュバーを使用できます。

1. [Door configuration (ドアの設定)] ページに移動します。 *ドアの追加, on page 157*を参照してください。
2. ドアのどちらかの面で [**Add (追加)**] をクリックします。
3. [**REX device (REXデバイス)**] を選択します。
4. REX装置を接続するI/Oポートを選択します。利用可能なポートが1つしかない場合は、自動的にそのポートが選択されます。
5. [**Action (アクション)**] で、ドアがREX信号を受信したときにトリガーするアクションを選択します。
6. [**REX active (REXアクティブ)**] で、ドアモニター回路の接続方法を選択します。
7. デジタル入力が新しい安定状態に移行するまで状態変化を無視するには、[**Debounce time (ms) (デバウンス時間 (ミリ秒))**] を設定します。
8. ドアコントローラーとREX装置の間の接続が中断された場合にイベントをトリガーするには、[**Supervised input (状態監視入力)**] をオンにします。*監視入力, on page 172*を参照してください。

アクション	
ドアロック解除	REX信号を受信したときにドアのロックを解除する場合に選択します。
なし	ドアがREX信号を受信した際に、何のアクションも行わないようにする場合に選択します。

REX有効	
回路が開いている	REX回路がNC (Normally Closed) の場合に選択します。REX装置は、回路が開いたときに信号を送信します。
回路が閉じている	REX回路がNO (Normally Open) の場合に選択します。REX装置は、回路が閉じたときに信号を送信します。

ゾーンの追加

ゾーンとは、グループ化されたドアがある特定の物理的領域です。ゾーンを作成したり、ゾーンにドアを追加したりできます。ドアには 2 つのタイプがあります。

- **Perimeter door (敷地周辺ドア):** このドアを通ってカード所持者がゾーンに出入りします。
- **Internal door (内部ドア):** ゾーンの内にあるドアです。

注

周辺ドアは、2つのゾーンに属することができますが、内部ドアは1つのゾーンにのみ属することができます。概要については、*ドアとゾーンの例, on page 157*を参照してください。

1. [**Configuration > Access control > Doors and zones > Zones (設定 > アクセスコントロール > ドアとゾーン > ゾーン)**] を選択します。
2. + [**Add zone (ゾーンを追加)**]をクリックします。
3. ゾーン名を入力します。
4. [**Add door (ドアを追加)**] をクリックします。
5. ゾーンに追加するドアを選択し、[**Add (追加)**] をクリックします。
6. デフォルトでは、ドアは敷地周辺ドアに設定されています。これを変更するには、ドロップダウンメニューで [**Internal door (内部ドア)**] を選択します。

7. 敷地周辺ドアでは、デフォルトでドアのA面がゾーンへの入口として使用されます。これを変更するには、ドロップダウンメニューで [Leave (退出)] を選択します。
8. ゾーンからドアを削除するには、ドアを選択し、[Remove (削除)] をクリックします。
9. [Save (保存)] をクリックします。

ゾーンを編集するには:

1. [Configuration > Access control > Doors and zones > Zones (設定 > アクセスコントロール > ドアとゾーン > ゾーン)] を選択します。
2. リストからゾーンを選択します。
3. [Edit (編集)]をクリックします。
4. 設定を変更して [Save (保存)] をクリックします。

ゾーンを削除するには:

1. [Configuration > Access control > Doors and zones > Zones (設定 > アクセスコントロール > ドアとゾーン > ゾーン)] を選択します。
2. リストからゾーンを選択します。
3. [Remove (削除)]をクリックします。
4. [Yes (はい)] をクリックします。

ゾーンセキュリティレベル

ゾーンに次のセキュリティ機能を追加できます。

アンチパスバック - ユーザーが自分より前にそのエリアに入った人と同じ認証情報を使用することを防ぎます。ユーザーがその認証情報を再び使用するためには、いったんエリアから退出する必要があります。

注

- 不正通行防止では、ゾーン内のすべてのドアにドアポジションセンサーが必要です。これにより、ユーザーがカードのスワイプ後にドアを開けたことをシステムが登録できます。
- ゾーン内のすべてのドアが同じドアコントローラーに属している場合、ドアコントローラーがオフラインになっても、不正通行防止は機能します。ただし、ゾーン内のドアが異なるドアコントローラーに属している場合は、ドアコントローラーがオフラインになると、不正通行防止は機能しなくなります。

セキュリティレベルは、新しいゾーンの追加時に設定するか、既存のゾーンに適用できます。既存のゾーンにセキュリティレベルを追加するには:

1. [Configuration (設定)] > [Access control (アクセスコントロール)] > [Doors and zones (ドアとゾーン)] に移動します。
2. セキュリティレベルを設定するゾーンを選択します。
3. [Edit] (編集) をクリックします。
4. [Security level (セキュリティレベル)] をクリックします。
5. ゾーンに追加するセキュリティ機能をオンにします。
6. [適用] をクリックします。

アンチパスバック	
Log violation only (Soft) (違反を記録のみ (ソフト))	2人目のユーザーが1人目と同じ認証情報を使用して入場することを許可する場合に選択します。このオプションでは、システムアラームのみが発生します。

アクセスを拒否 (ハード)	2人目のユーザーが1人目と同じ認証情報を使用して入場することを防ぐ場合に選択します。このオプションでも、システムアラームが発生します。
タイムアウト (秒)	この時間が経過するまで、ユーザーは再入場を許可されます。タイムアウトを設定しない場合は0を入力します。これにより、ユーザーがゾーンを離れるまでアンチパスバックが適用されます。[Deny access (Hard) (アクセス拒否 (ハード))] でタイムアウトとして0を使用するのは、ゾーン内のすべてのドアの両側にリーダーがある場合に限ります。

監視入力

状態監視入力は、ドアコントローラーへの接続が中断されると、イベントをトリガーすることができます。

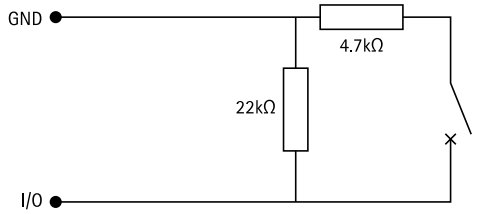
- ドアコントローラーとドアモニターの接続。*ドア位置センサーの追加, on page 164*を参照してください。
- Wiegandプロトコルを使用するドアコントローラーとリーダー間の接続。*「リーダーの追加」, on page 167*を参照してください。
- ドアコントローラーとREX装置間の接続。*REX装置の追加, on page 169*を参照してください。

監視入力を使用するには:

1. 終端抵抗は、接続図にしたがって、できるだけ周辺機器の近くに設置してください。
2. リーダー、ドアモニター、またはREX装置の設定ページに移動し、[**Supervised input (監視入力)**] をオンにします。
3. 並列優先接続図に従った場合は、[**Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor (22 KΩの並列抵抗器と4.7 KΩの直列抵抗器による並列優先接続)**] を選択します。
4. 直列優先接続図に従った場合は、[**Serial first connection (直列優先接続)**] を選択し、[**Resistor values (抵抗器の値)**] ドロップダウンメニューから抵抗器の値を選択します。

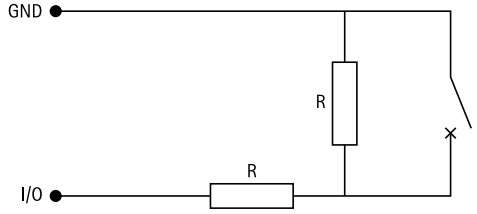
パラレルファースト接続

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、1~10 kΩの範囲内である必要があります。



識別プロファイル

識別プロファイルは、識別タイプとスケジュールを組み合わたものです。識別プロファイルを1つ以上のドアに適用して、カード所持者がドアにいつどのようにアクセスできるかを設定できます。

注
動的QRをPINと共に使用する必要があります。

識別プロファイルを作成、編集、または削除するには、**[Configuration (設定)] > [Access control (アクセス管理)] > [Identification profiles (識別プロファイル)]** を選択します。

利用可能な識別プロファイル：

カード - カード所持者がドアにアクセスする際に、カードを読み取らせる必要があります。

カードとPIN - カード所持者がドアにアクセスする際に、カードを読み取らせ、かつPINを入力する必要があります。

PIN - カード所持者がドアにアクセスする際に、PINを入力する必要があります。

カードまたはPIN - カード所持者がドアにアクセスする際に、カードを読み取らせるか、PINを入力する必要があります。

QR - カード所持者は、ドアにアクセスするためにQR Code®をカメラに提示する必要があります。QR識別プロファイルは、静的QRと動的QRの両方に使用できます。

ナンバープレート - カード所持者は、承認済みのナンバープレートを付けた車両でカメラに向かって運転する必要があります。

アプリでタップ - カード所持者は、Bluetoothリーダーの範囲内に立っている状態で、AXIS Camera Stationモバイルアプリで認証情報をタップする必要があります。

リーダーにタッチ - カード所持者は、モバイル認証情報を設定した携帯電話をBluetoothリーダーにタッチする必要があります。

*QRコードは、日本およびその他の国々におけるデンソーウェーブ社の登録商標です。

識別プロファイルを作成する

1. **[Configuration (設定)] > [Access Control (アクセスコントロール)] > [Identification profiles (識別プロファイル)]** を選択します。
2. **[Create identification profile (識別プロファイル)]** をクリックします。
3. 識別プロファイルの名前を入力します。
4. 設備コードを [Credential validation (認証情報の検証)] フィールドの1つとして使用するには、**[Include facility code for card validation (カード検証用の機能コードを含める)]** を選択します。このフィールドは、**[Access management > Settings (アクセス管理 > 設定)]** で **[Facility code (設備コード)]** をオンにしている場合のみ使用できます。
5. A面で、**[Add (追加)]** をクリックし、識別タイプとスケジュールを選択します。
   - カード保有者に複数の識別タイプの使用を求めるには、同じ行で複数のタイプを選択します。
   - カード保有者がいずれかのタイプを使用できるようにするには、**[Add (追加)]** を再度クリックして別の行を追加します。
6. B面で、**[Add (追加)]** をクリックし、識別タイプとスケジュールを選択します。
7. **[OK]**をクリックします。

識別プロファイルの設定

識別プロファイルを編集する

1. [Configuration (設定)] > [Access Control (アクセスコントロール)] > [Identification profiles (識別プロファイル)] を選択します。
2. 識別プロファイルを選択して をクリックします。
3. 識別プロファイル名を変更するには、新しい名前を入力します。
4. ドアの現在の面で編集をします。
5. ドアの反対側の面の識別プロファイルを編集するには、ここまでの手順を繰り返します。
6. [OK]をクリックします。

識別プロファイルの編集	
×	識別タイプとそれに関連するスケジュールを削除するには:
認証タイプ	識別タイプを変更するには、[Identification type (識別タイプ)] のドロップダウンメニューから1つ以上のタイプを選択します。
Schedule	スケジュールを変更するには、[Schedule (スケジュール)] ドロップダウンメニューから1つ以上のスケジュールを選択します。
+ 追加	識別タイプとそれに関連スケジュールを追加し、[Add (追加)] をクリックして、識別タイプとスケジュールを設定します。

識別プロファイルを削除する

1. [Configuration (設定)] > [Access Control (アクセスコントロール)] > [Identification profiles (識別プロファイル)] を選択します。
2. 識別プロファイルを選択して をクリックします。
3. 識別プロファイルがドアで使用されている場合は、そのドア用に別の識別プロファイルを選択します。
4. [OK]をクリックします。

既定のカードフォーマットをリセットする

1. [Configuration (設定)] > [Access Control (アクセスコントロール)] > [Card formats and PIN (カードフォーマットとPIN)] を選択します。
2. をクリックすると、カードフォーマットをデフォルトのフィールドマップにリセットできます。

カードフォーマットとPIN

カードフォーマットは、カードリーダーがカードからのデータをどのように解釈するかを定義するものです。あらかじめ定義されたカードフォーマットを使用・編集することができます。カスタムカードフォーマットを作成することも可能です。

[Configuration > Access Control > Card formats and PIN (設定 > アクセスコントロール > (カードフォーマットとPIN)] に移動して、カードフォーマットを作成、編集、または有効化します。PINの設定もできます。

カスタムカードフォーマットには、認証情報の検証に使用する以下のデータフィールドを含めることができます。

カード番号 - 認証情報のバイナリデータのサブセットであり、10進数または16進数としてエンコードされています。カード番号を使用して、特定のカードまたはカード所持者を識別します。

設備コード - 認証情報のバイナリデータのサブセットであり、10進数または16進数としてエンコードされています。設備コードを使用して、特定のエンドカスタマーまたはサイトを識別します。

PIN設定

1. [Configuration (設定)] > [Access Control (アクセスコントロール)] > [Card formats and PIN (カードフォーマットとPIN)] を選択します。
2. [PIN configuration (PIN設定)]で をクリックします。
3. [Min PIN length (最小PIN長)]、[Max PIN length (最大PIN長)]、[End of PIN character (PIN文字の終端)] をそれぞれ指定します。
4. [OK]をクリックします。

カードフォーマットを作成する

1. [Configuration (設定)] > [Access Control (アクセスコントロール)] > [Card formats and PIN (カードフォーマットとPIN)] を選択します。
2. [Add card format (カードフォーマットの追加)] をクリックします。
3. カードフォーマットの名前を入力します。
4. [Bit length (ビット長)] フィールドに、1～256の間のビット長を入力します。
5. カードリーダーから受信したデータのビット順を反転するには、[Invert bit order (ビット順を反転する)] を選択します。
6. カードリーダーから受信したデータのバイト順を反転するには、[Invert byte order (バイト順を反転する)] を選択します。このオプションは、8で割り切れるビット長を指定している場合のみ使用できます。
7. カードフォーマットで有効にするデータフィールドを選択して設定します。カードフォーマットでは、[Card number (カード番号)] か [Facility code (設備コード)] のいずれかを有効にする必要があります。
8. [OK]をクリックします。
9. カードフォーマットを有効にするには、カードフォーマット名の前にあるチェックボックスをオンにします。

注

- 同一ビット長の2つのカードフォーマットを同時にアクティブにすることはできません。たとえば、32ビットカードフォーマットを2つ定義した場合、アクティブにできるのはそのう

ちの1つだけです。一方のカードフォーマットを無効にすると、もう一方のフォーマットが有効になります。

- 1つ以上のリーダーが接続されたドアコントローラーを設定している場合は、カードフォーマットを有効または無効にのみ設定できます。
- 既定のカードフォーマットは編集できますが、削除することはできません。既定フォーマットへの変更を元に戻すには、リセットアイコンをクリックしてデフォルト設定に復元します。作成したカードフォーマットは削除することができます。

ⓘ	ⓘをクリックすると、ビット順を反転した後の出力例が表示されます。
通信可能距離	データフィールドのデータのビット範囲を設定します。この範囲は、[**Bit length (ビット長)**] に指定した範囲内である必要があります。
出力形式	データフィールドのデータの出力形式を選択します。 **Decimal (10進数)**十進記数法としても知られ、0～9の数字で構成されます。 **16進数**: 16進記数法としても知られ、0～9の数字とa～fの文字の16個の一意の記号で構成されます。
ビット順のサブ範囲	ビット順を選択します。 **Little endian (リトルエンディアン)**: 最初のビットが最小 (最下位) です。 **Big endian (ビッグエンディアン)**: 最初のビットが最大 (最上位) です。

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。

カードフォーマットの設定

カードフォーマットを編集する

1. [**Configuration (設定)**] > [**Access Control (アクセスコントロール)**] > [**Card formats and PIN (カードフォーマットとPIN)**] を選択します。
2. カードフォーマットを選択して をクリックします。
3. 既定のカードフォーマットを編集する場合は、[**Invert bit order (ビット順を反転する)**] と [**Invert byte order (バイト順を反転する)**] のみを編集できます。
4. [**OK**]をクリックします。

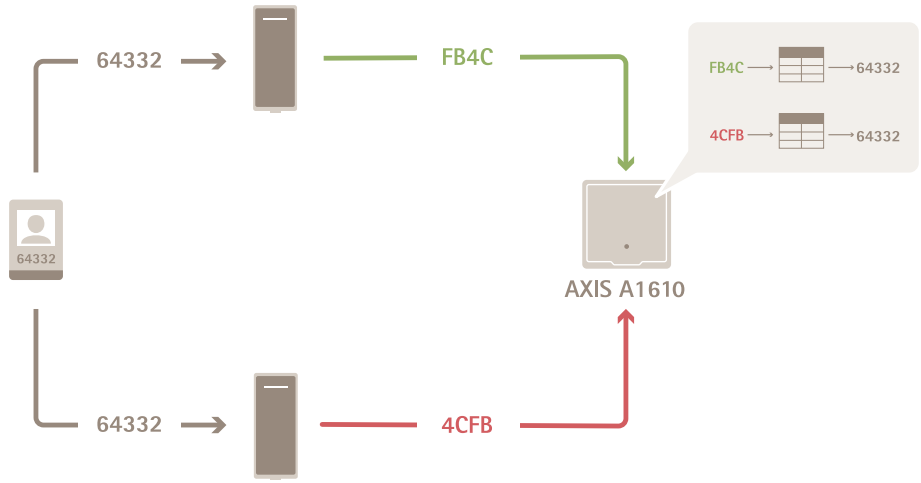
削除できるのは、カスタムカードフォーマットのみです。カスタムカードフォーマットを削除する手順は、以下のとおりです。

1. [**Configuration (設定)**] > [**Access Control (アクセスコントロール)**] > [**Card formats and PIN (カードフォーマットとPIN)**] を選択します。

2. カスタムカードフォーマットを選択し、 と[Yes (はい)]をクリックします。

カードフォーマットの設定

概要



- カード番号は10進数で64332です。
- 1台のリーダーにより、カード番号が16進数のFB4Cに変換されます。別のリーダーにより、それが16進数の4CFBに変換されます。
- FB4Cを受信したAXIS A1610 Network Door Controllerは、それをリーダーのカードフォーマット設定に従って10進数の64332に変換します。
- 4CFBを受信したAXIS A1610 Network Door Controllerは、それをバイト順序を逆にしてFB4Cに変更し、リーダーのカードフォーマット設定に従って10進数の64332に変換します。

ビット順を反転する

ビット順の反転後、リーダーから受信したカードデータは、右から左にビット順に読み取られます。

バイト順を反転する

1バイトは8ビットです。バイト順の反転後、リーダーから受信したカードデータは、右から左にバイト順に読み取られます。

26ビット標準のWiegandカードフォーマット

1. *先頭のパリティ*
2. *設備コード*
3. *カード番号*
4. *末尾のパリティ*

暗号化通信

OSDPセキュアチャンネル

AXIS Camera Station Secure Entryは、OSDP (Open Supervised Device Protocol) セキュアチャンネルに対応し、コントローラーとAxisリーダー間の回線暗号化をアクティブにします。

システム全体でOSDPセキュアチャンネルをオンにするには:

1. [**Configuration > Access control > Encrypted communication (設定 > アクセスコントロール > 暗号化通信)**] に移動します。
2. メインの暗号化キーを入力し、[**OK**] をクリックします。
3. [**OSDP Secure Channel (OSDPセキュアチャンネル)**] をオンにします。このオプションは、メインの暗号化キーを入力した後にのみ使用できます。
4. デフォルトでは、メインの暗号化キーによってOSDP Secure Channelキーが生成されます。OSDPセキュアチャンネルキーを手動で設定するには:
   4.1. [**OSDP Secure Channel (OSDPセキュアチャンネル)**]で、 をクリックします。
   4.2. [**Use main encryption key to generate OSDP Secure Channel key (メイン暗号化キーを使用してOSDPセキュアチャンネルキーを生成する)**] をクリアします。
   4.3. OSDPセキュアチャンネルキーを入力し、[**OK**] をクリックします。

特定のリーダーでOSDPセキュアチャンネルをオンまたはオフにする方法については、*ドアとゾーン*を参照してください。

AXIS Barcode Reader

AXIS Barcode Readerは、Axisカメラにインストールできるアプリケーションです。AXISドアコントローラーは、外部周辺機器の認証キーを使用してアクセスを許可し、AXISバーコードリーダーおよびAXIS License Plate Verifierを認証します。AXIS Camera Station ProでAXIS License Plate Verifierを設定するワークフローの詳細については、を参照してください。

AXIS Barcode Readerの取り付け

1. *axis.com*からアプリケーションインストールをダウンロードします。
2. [webpage of your Axis intercom or camera (Axisインタカムまたはカメラのウェブページ)] に移動します。
3. アプリケーションをインストールします。
4. ライセンスをアクティブ化します。
5. アプリケーションの起動.
6. QR精度を向上するには、以下のカメラ設定を変更することをお勧めします。
   6.1. カメラ設定に移動するには:
   6.2. [**Image (画像) >Exposure (露出)**]で、[**Blur-noise trade-off (ブレとノイズのトレードオフ)**] スライダーを中央に移動します。

AXIS Barcode Readerの設定

1. QR識別プロフィールを変更する場合 、**[Configuration (設定)] > [Access control (アクセス管理)] > [Identification profiles (識別プロファイル)]** に移動して をクリックします。*識別プロファイル*を参照してください。
2. ドアを追加する手順については、「ドアの追加」*を参照*してください。
3. このドアの識別プロファイルとして [QR]を選択します。 *ドアの設定*を参照してください。
4. 「バーコードのリーダーの追加。*リーダーの追加*を参照してください。
   4.1. ドアのどちらかの面で [**Add reader (リーダーの追加)**] をクリックします。
   4.2. [**AXIS Barcode Reader (AXIS Barcode リーダー)**]のドロップダウンリストから **リーダータイプ** を選択します。名前を入力し、[**OK**] をクリックします。

ドアコントローラーとの接続を作成します

1. AXIS Camera Station Proで:
   1.1. [**Configuration > Access control > Encrypted communication (設定 > アクセスコントロール > 暗号化通信)**] に移動します。
   1.2. [**External Peripheral Authentication Key (外部周辺機器認証)**] キーで [**Show authentication key (認証キーの表示)**]、[**Copy key (キーのコピー)**] の順にクリックします。
2. AXISバーコードリーダーが実行されている装置のwebインターフェースで:
   2.1. AXIS Barcode Readerアプリケーションを開きます。
   2.2. サーバー証明書が AXIS Camera Station Proで設定されていない場合は、[**Ignore server certificate validation (サーバー証明書の検証を無視する)**] をオンにします。より詳細な情報については、*CA証明書* を参照してください。
   2.3. サーバー証明書が AXIS Camera Station Proで設定されていない場合は、[**Ignore server certificate validation (サーバー証明書の検証を無視する)**] をオンにします。より詳細な情報については、*CA証明書* を参照してください。
   2.4. **AXIS Camera Station Secure Entry**に反対します。
   2.5. [**追加**]] をクリックし、ドアコントローラーのIPアドレスを入力し、認証キーを貼り付けます。
   2.6. ドアのドロップダウンメニューからバーコードを読み取るリーダーを選択します。

マルチサーバーBETA

マルチサーバーを使用すると、メインサーバー上のグローバルカード所持者およびカード所持者グループを接続されたサブサーバーで使用できます。

注

- 1つのシステムで最大64台のサブサーバーをサポートできます。
- AXIS Camera Station 5.47以降が必要です。
- 前提条件として、メインサーバーとサブサーバーは同じネットワーク上にある必要があります。
- メインサーバーとサブサーバーでかならず、WindowsファイアウォールがSecure Entryポートで入力TCP接続を許可するよう設定します。デフォルトポートは55767です。カスタマイズされたポート設定については、*全般サーバー設定, on page 223*を参照してください。
- サブサーバーをメインサーバーに接続すると、そのリーダーキーが置き換えられ、既存のBluetooth認証情報は無効になります。これを回避するには、サブサーバーではなくメインサーバー上でBluetooth認証情報を作成してください。

ワークフロー

1. サーバーをサブサーバーとして設定し、設定ファイルを生成します。*サブサーバーから設定ファイルを生成する, on page 180*を参照してください。
2. サーバーをメインサーバーとして設定し、サブサーバーの設定ファイルをインポートします。*設定ファイルをメインサーバーにインポートする, on page 180*を参照してください。
3. メインサーバーでグローバルなカード所持者とカード所持者グループを設定します。*カード所持者の追加, on page 192*および *「グループの追加」, on page 197*を参照してください。
4. サブサーバーからグローバルなカード所持者およびカード所持者グループを表示および監視します。*アクセス管理, on page 192*を参照してください。

サブサーバーから設定ファイルを生成する

1. サブサーバーで、[Configuration > Access control > Multi server (設定 > アクセスコントロール > マルチサーバー)] に移動します。
2. [Sub server (サブサーバー)] をクリックします。
3. [Generate (生成)] をクリックします。設定ファイルが.json形式で生成されます。
4. [Download (ダウンロード)] をクリックし、ファイルを保存する場所を選択します。

設定ファイルをメインサーバーにインポートする

1. メインサーバーで、[Configuration > Access control > Multi server (設定 > アクセスコントロール > マルチサーバー)] に移動します。
2. [Main server (メインサーバー)] をクリックします。
3. ＋[Add (追加)]をクリックし、サブサーバーから生成された設定ファイルに移動します。
4. サブサーバーのサーバー名、IPアドレス、ポート番号を入力します。
5. [Import (インポート)] をクリックして、サブサーバーを追加します。
6. サブサーバーのステータスが [Connected] と表示されます。

サブサーバーを無効にする

サブサーバーは、設定ファイルをメインサーバーにインポートする前に限り無効にできます。

1. メインサーバーで、[Configuration > Access control > Multi server (設定 > アクセスコントロール > マルチサーバー)] に移動します。
2. [Sub server (サブサーバー)] をクリックしてから、[Revoke server (サーバーを無効化)] をクリックします。
   これで、このサーバーをメインサーバーまたはサブサーバーとして設定できます。

サブサーバーを削除する

サブサーバーの設定ファイルをインポートすると、サブサーバーがメインサーバーに接続されます。

サブサーバーを削除するには、次の手順を実行します。

1. メインサーバーにアクセスします。
   1.1. [Access management > Dashboard ((アクセス管理 > ダッシュボード)] を選択します。
   1.2. グローバルカード所持者とグループをローカルカード所持者とグループに変更します。

1.3. [Configuration > Access control > Multi server (設定 > アクセスコントロール > マルチサーバー)] に移動します。
1.4. [Main server (メインサーバー)] をクリックすると、サブサーバーのリストが表示されます。
1.5. サブサーバーを選択し、[Delete (削除)] をクリックします。
2. サブサーバーから:
– [Configuration > Access control > Multi server (設定 > アクセスコントロール > マルチサーバー)] に移動します。
– [Sub server (サブサーバー)] をクリックしてから、[Revoke server (サーバーを無効化)] をクリックします。

Active Directory設定BETA

注
Microsoft Windowsのユーザーアカウント、Active Directoryユーザーおよびグループは、AXIS Camera Station Proにアクセスできます。Windowsでユーザーを追加する方法は、使用しているバージョンによって異なります。詳細については、*support.microsoft.com*にアクセスしてください。Active Directoryドメインネットワークを使用している場合は、ネットワーク管理者にお問い合わせください。

初めてActive Directory設定ページを開いたときに、AXIS Camera Station Proでカード所持者にMicrosoft Active Directoryユーザーをインポートできます。*Active Directoryユーザーをインポートする, on page 181*を参照してください。

初期設定の後、Active Directory設定ページに次のオプションが表示されます。

- Active Directory内のグループに基づいてカード所持者グループを作成および管理します。
- Active Directoryとアクセス管理システム間のスケジュールされた同期を設定します。
- 手動で同期して、Active Directoryからインポートされたすべてのカード所持者を更新します。
- Active Directoryからのユーザーデータとカード所持者のプロパティ間のデータマッピングを管理します。

Active Directoryユーザーをインポートする

AXIS Camera Station Proでカード所持者にActive Directoryユーザーをインポートするには:

1. [Configuration (設定)] > [Access control (アクセスコントロール)] > [Active directory settings BETA (Active Directory設定 BETA)]に移動します。
2. [Set up import (インポートを設定する)] をクリックします。
3. 画面に表示される手順に従ってこれら3つの主な手順を完了します。
3.1. データマッピングのテンプレートとして使用するユーザーをActive Directoryから選択します。
3.2. Active Directoryデータベースのユーザーデータをカード所持者のプロパティにマッピングします。
3.3. アクセス管理システムで新しいカード所持者グループを作成し、インポートするActive Directoryグループを選択します。

インポートされたユーザーデータを変更することはできませんが、インポートされたカード所持者に認証情報を追加することはできます。*認証情報の追加, on page 194*を参照してください。

重要
Active Directoryでユーザーを無効にすると、AXIS Camera Station Proはそのカード所持者とすべての関連データ (履歴を含む) を完全に削除します。これは元に戻せません。カード所持者の

データを失わずにカード保持者のアクセスをブロックするには、Active Directoryでカード所持者を無効にするのではなく、AXIS Camera Station Proでカード所持者を停止してください。

AXIS Audio Manager Proを設定する

AXIS Camera Station ProでAXIS Audio Manager Proサーバーに接続し、そのサーバーに接続されている音声デバイスを使用できます。

この設定には、AXIS Camera Station Pro 6.12以降および AXIS Audio Manager Pro 5.0以降が必要です。両方のサーバーは、同じサーバー上か、同じネットワーク上の別々のマシン上に設定する必要があります。

重要

同じサーバー上でAXIS Camera Station ProとAXIS Audio Manager Proの両方を実行する場合、どちらもデフォルトでポート443を使用します。接続の問題を防ぐため、いずれかを異なるポートを使用するように設定してください。

AXIS Camera Station Proのポート設定は、*全般サーバー設定, on page 223*から変更できます。AXIS Audio Manager Proのポート設定の変更方法については、*AXIS Audio Manager Proユーザーマニュアル*を参照してください。

AXIS Camera Station ProでAXIS Audio Manager Proの使用を開始するには:

1. AXIS Audio Manager Proで、以下の手順に従います。
   1.1. **[System settings (システム設定)]** > **[API access (APIアクセス)]** に移動します。
   1.2. APIをオンにし、ユーザー名とパスワードを入力します。
2. AXIS Camera Station Proでの手順：
   2.1. **[Configuration (設定)]** > **[AXIS Audio Manager Pro]** に移動し、**[Connect (接続)]** をクリックしてAXIS Audio Manager Proサーバーへの接続を設定します。
   2.2. ポップアップダイアログに、AXIS Audio Manager Proサーバーの **[Server URL (サーバーURL)]**、**[API username (APIユーザー名)]**、**[API password (APIパスワード)]** を入力し、**[Connect (接続)]** をクリックします。

接続が確立すると、以下の操作が可能です。

- AXIS Audio Manager Proサーバーの **[Server status (サーバーステータス)]** とそのサーバーに接続されている **[Device status (デバイスステータス)]** を表示する。
- 新しいAXIS Audio Manager Proタブを開き、サーバーのWebインターフェースにアクセスする。
- AXIS Camera Station Proの新しい音声関連機能を使用する。

詳しくは、*AXIS Audio Manager Pro, on page 214*を参照してください。

注

証明書関連の問題を避けるため、信頼できる認証局 (CA) から証明書を作成または取得し、AXIS Audio Manager ProにアップロードしてAXIS Camera Station Proサーバーの信頼できる証明書リストに追加することをお勧めします。詳しくは、*AXIS Audio Manager Proユーザーマニュアル*を参照してください。

スマート検索2の設定

スマート検索2を使用すると、フィルターを設定して、Axisカメラの録画から生成された録画で対象の人物や車両を見つけることができます。

要件、制限、スマート検索2の使用方法については、*スマート検索2, on page 39*を参照してください。

1. [Configuration (設定)] > [Smart search 2 (スマート検索2)] > [Settings (設定)]に移動します。
2. [Cameras (カメラ)] で:
   2.1. メタデータをスマート検索2に送信する必要のあるカメラを選択します。
   2.2. カメラに対してバックグラウンドでのサーバー分類を許可するには、[Background server classification (バックグラウンドでのサーバー分類)] で [Allow (許可)] を選択します。
   これにより、サーバーの負荷が増加しますが、ユーザーエクスペリエンスは向上します。
   2.3. サーバーに保存される検知数を制限するには、[Filter (フィルター)] で、⚙ をクリックし、[Area (エリア)]、[Size and duration (サイズと期間)]、[Swaying objects (揺らめいている物体)] のフィルターを作成します。
   これらのフィルターを使用すると、除外範囲、小さな物体、ごく短時間しか現れない物体、木の葉のような揺らめいている物体を除外することができます。
   スマート検索フィルターは既存のモーション設定フィルターを開始点として使用します。
3. [Storage (ストレージ)] で次の設定を行います。
   – 検知を保存するドライブとフォルダーを選択し、[Apply (適用)] をクリックします。
   – ストレージサイズの上限を設定し、[Apply (適用)] をクリックします。ストレージが上限に達すると、最も古い検知が削除されます。
4. **Include periods with missing metadata (メタデータがない期間を含める)]** を選択すると、メタデータが記録されていない結果も表示されます。
5. **[Let the server classify detections when you start a search (検索開始でサーバーによる検出結果分類を許可)]** を選択し、カメラが分類しなかった検出結果を含む、より詳細な検索結果を取得します。検索結果が表示されるまでの時間を短くする場合は、このオプションをオフのままにしておきます。

バックグラウンドサーバーの分類	
	サーバー分類のステータスは、サーバー分類が低速である過去1時間からのものです。分類された検知が95%未満の場合に表示されます。
	サーバー分類のステータスは、サーバー分類が低速である過去1時間からのものです。分類された検知が50%未満の場合に表示されます。

トリガー

アクションルールのトリガーにスマート検索フィルターを設定できます。以下の手順に従って、スマート検索トリガーを作成します。

1. [Configuration (設定)] > [Smart search 2 (スマート検索2)] > [Triggers (トリガー)] に移動します。
2. [Create (作成)] をクリックします。
3. フィルターを設定します。スマート検索フィルターについて詳しくは、*フィルターで検索する, on page 39*を参照してください。
4. [Next (次へ)] をクリックします。
5. 検出の [Confidence (信頼度)] レベルを調整します。信頼度を高くすると、不確実な分類が除外され、検知数が少なくなります。
6. [Next (次へ)] をクリックします。
7. トリガーの名前を入力し、[Save (保存)] をクリックします。

注

- Smart search 2 (スマート検索2) では、映像を分析し、検知を検証するために、物体がカメラの視野から外れた後、通常数秒を必要とします。たとえば、赤い車が検知されたときにアクションルールがトリガーされるように設定している場合、そのアクションは、その物体がカメラの視野から外れてから数秒が経たないとトリガーされません。
- [Visual similarity (映像の類似性)] は、スマート検索2のトリガーオプションとして使用できません。
- カメラのトリガーを作成すると、そのカメラで [Enable background processing (バックグラウンド処理を有効にする)] をオフにしていても、サーバーが対象の検出を処理できます。
- [Delayed detection periods (検出遅延時間)] は、アクションルールのトリガーを遅延させる、高処理遅延の時間を指します。これが頻繁に発生する場合は、トリガーフィルターを再設定し、カメラ数を減らし、ライン横断、エリア、サイズ、時間などのカメラのフィルターを使用して処理遅延を短くして対応できます。

アクションルールでスマート検索2のトリガーを使用するには、*スマート検索2のトリガーを作成する, on page 108*を参照してください。

System Health Monitoring[BETA]の設定

注

- 複数の AXIS Camera Station Proサーバーに接続している場合は、接続されている任意のサーバーでSystem Health Monitoringを設定できます。そのためには、[Selected server (選択したサーバー)] ドロップダウンメニューからサーバーを選択します。
- 別のネットワーク上のシステムを管理している場合、My Systemsのサーバー監視は、クラウド経由で同じ機能を提供します。

設定

クラウド接続	サーバーを組織に登録している場合は、どこからでもシステムの健全性データを確認できます。接続されていない場合は、[**Manage (管理)**] をクリックし、画面の指示に従ってください。
Data retrieval frequency (データ取得頻度)	古いデータに関する警告や一般的なパフォーマンスの問題を解決するには、データ更新頻度を低く選択してください。マルチシステム環境の場合、親システムと同じかそれより高い設定をサブシステムに使用することをお勧めします。 • **Low (低)** - デバイス数が100台を超えるシステム。 • **Medium (中)** - デバイス数が25～100台のシステム。 • **High (高)** - デバイス数が25台未満のシステム。

通知

電子メール通知を送信するには:

1. 通知の送信に使用するSMTPサーバーと電子メールアドレスを設定します。*サーバーの設定, on page 132*を参照してください。
2. 通知を受信する電子メールアドレスを設定します。*電子メール送信先の設定, on page 185* を参照してください。
3. 通知ルールを設定します。*通知ルールの設定, on page 185*を参照してください。

電子メール送信先の設定

1. [**Configuration (設定)**] > [**System Health Monitoring**] > [**Notifications (通知)**] に移動します。
2. [**Email recipients (電子メール送信先)**] で、電子メールアドレスを入力し、[**Save (保存)**] をクリックします。同じ手順を繰り返して、複数の電子メール送信先を追加します。
3. SMTPサーバーをテストするには、[**Send test email (テスト電子メールを送信)**] をクリックします。テスト電子メールが送信されたことを確認するメッセージが表示されます。

通知ルールの設定

デフォルトでは、次の2つの通知ルールがオンになっています。

システムのダウン - 単一システム設定のシステムまたはマルチシステム設定のいずれかのシステムが通常よりも長くダウンしている場合に通知を送信します。

デバイスのダウン - System Health Monitoringに一覧表示されている装置が通常よりも長くダウンしている場合に通知を送信します。

1. [**Configuration (設定)**] > [**System Health Monitoring**] > [**Notifications (通知)**] に移動します。
2. [**Notification rules (通知ルール)**]で、通知ルールをオンまたはオフにします。
3. [**Applied rules (適用されたルール)**] で、システムとデバイスのリスト、およびそれらに適用された通知ルールを確認できます。

マルチシステム

System Health Monitoringを使用すると、1つのメインシステムから複数のセカンダリシステムのヘルスデータを監視できます。

1. セカンダリシステムで、システム設定を生成します。*システム設定を生成, on page 186*を参照してください。
2. メインシステムで、システム設定をアップロードします。*他のシステムからデータを取得する, on page 186*を参照してください。
3. 他のセカンダリシステムでも、前の手順を繰り返します。
4. メインシステムから複数のシステムのヘルスデータを監視します。*System Health Monitoring*^{BETA}*, on page 204*を参照してください。

システム設定を生成

1. [Configuration (設定)] > [System Health Monitoring] > [Multisystem (マルチシステム)] に移動します。
2. [Generate (生成)] をクリックします。
3. [Copy (コピー)]をクリックし、コピーしてメインシステムにアップロードします。
4. システム設定の詳細を表示するには、[Show details (詳細を表示)] をクリックします。
5. システム設定を再生成するには、まず [Delete (削除)] をクリックして、既存の設定を削除します。

システム設定がメインシステムにアップロードされると、メインシステムの情報が [Systems with access (アクセス可能なシステム)] に表示されます。

他のシステムからデータを取得する

セカンダリシステムのシステム設定を生成してコピーすると、そのコピーをメインシステムにアップロードできます。

1. メインシステムで、[Configuration (設定)] > [System Health Monitoring] > [Multisystem (マルチシステム)] に移動します。
2. [Paste (貼り付け)] をクリックして、セカンダリシステムからコピーした情報を追加します。
3. ホストのIPアドレスを確認し、[Add (追加)] をクリックします。
セカンダリシステムは [Available systems (利用可能なシステム)] に表示されます。

分析機能を設定する

AXIS Data Insights Dashboard

AXIS Data Insights Dashboardには、装置からの分析データがグラフやチャート形式で表示されます。AXIS Data Insights Dashboardの設定ページには、システム内の装置でサポートされているすべてのアプリケーションと設定済みのシナリオが表示されます。[Analytics (分析機能)] > [Data Insights Dashboard] に移動すると以下の操作を実行できます。

- サポートされているアプリケーションを実行しているカメラとデータソースのリストを表示する。
- 各装置またはデータソースでサポートされているアプリケーションとシナリオのリストを表示する。以下のアプリケーションおよびシナリオに対応しています。
  - AXIS Object Analytics: Crossline counting (クロスラインカウント)および Occupancy (混雑状況)
  - AXIS Audio Analytics
  - AXIS Image Health Analytics
  - AXIS People Counter
  - AXIS P8815-2 3Dカウンタ
  - AXIS Air Quality Sensor (空気質モニター)

注

最大100 MBのデータを保存可能です。ただし、ストレージの保存期間には制限があります。例えば、12種類のデータタイプすべてを監視する空気質センサーの場合、保持期間は約430日間となります。

- ダッシュボードに含めるシナリオを選択する。
- シナリオにタグを付けて、ダッシュボードのデータを絞り込む (例: 同じロケーションにあるカメラをグループ化する)。

注

AXIS Object Analyticsのクロスラインカウントデータを [**In and Out counting（送受信カウント）**] ダッシュボードに表示するには、[**Direction (方向)**] フィールドで [**In (受信)**] または [**Out (送信)**] を選択して、シナリオの方向を選択します。

- シナリオのステータスを表示します。

検知対象	[**Include (含める)**] 列のスイッチをオンにすると、ダッシュボードにシナリオのデータが表示されます。
タグ	[**Tags (タグ)**] 列のドロップダウンメニューからタグを選択して、シナリオに追加します。

新しいタグを追加するには:

1. [**Tags (タグ)**] タブを開きます。
2. タグの名前を入力します。
3. 矢印をクリックします。

注

- AXIS Data Insights Dashboardは、Windowsサーバーでの暗号化接続にTLSバージョン 1.2 以降を必要とします。
- AXIS Data Insights Dashboardでは、次の場合にカメラの既存のMQTT設定が上書きされます。
  - カメラに設定済みMQTTクライアントがない場合。

  - 別の AXIS Camera Station Proサーバーに接続されているカメラのシナリオを手動でオンにする場合。
- AXIS Data Insights Dashboardに接続している間、カメラのMQTTクライアントはData Insights Dashboard専用です。
- カメラと AXIS Camera Station Proサーバーは同じネットワーク上にある必要があります。
- 最適なパフォーマンスを得るため、AXIS Camera Station ProでAXIS Data Insights Dashboardを実行するために、RAM 16 GB以上を搭載したサーバーをお勧めします。
- 保存できるデータは最大100 MBであるため、ストレージ期間は制限されます。例:
  - 4台のカメラが設置され、それぞれが車や自転車など5つの車両サブクラスを24時間365日検知するように設定された駐車場で混雑率を推定する場合、保存期間は260日になります。
  - 8台のカメラが設置され、12時間にわたって人の流れが継続する小売店舗で人数計測を行う場合、保存期間は約1,270日になります。
  - 6つのクラスでクロスラインカウントシナリオを実行するカメラで、計測が24時間継続して実行される場合、保存期間は約860日になります。

分割ビューにダッシュボードを追加する方法については、*分割ビューのAXIS Data Insights Dashboard, on page 21*を参照してください。

AXIS Data Insights Dashboardを有効にする方法

License Plate Verifier

License plate verifierページでは、各カメラにインストールされているAXIS License Plate Verifierのステータスを表示したり、リスト管理を容易にするためにカメラをグループ化したりできます。

[Cameras (カメラ)] タブには、AXIS License Plate Verifierがインストールされたすべての接続済みデバイスのリストが表示されます。

- **Camera (カメラ)**: カメラの名称。
- **Version (バージョン)**: カメラにインストールされているAXIS License Plate Verifierのバージョン。
- **Status (ステータス)**: AXIS License Plate Verifierの現在のステータス。
- **Latest event (最新イベント)**: カメラがキャプチャーした最新イベントの時刻。
- **Allowed (許可)**: カメラの許可リストに含まれるナンバープレートの数。
- **Blocked (拒否)**: カメラの拒否リストに含まれるナンバープレートの数。
- **Custom (カスタム)**: カメラのカスタムリストに含まれるナンバープレートの数。
- **Group (グループ)**: カメラが属するグループ。

[**Group (グループ)**] タブには、すべてのカメラグループと、各グループに含まれるカメラが表示されます。このタブでは次の操作ができます。

- **[New... (新規)]** をクリックして新しいグループを追加します。
- **[Delete (削除)]** をクリックして既存のグループを削除します。
- **[Group name (グループ名)]** のフィールドで、選択したグループ名を変更します。

- [Add... (追加)] をクリックして選択したグループにカメラを追加します。
- [Remove (削除)]をクリックしてグループからカメラを削除します。

グループ化されたカメラの共有リストを作成できます。詳細については、*ナンバープレート管理, on page 213*を参照してください。

装着式の設定

装着式システムの接続

装着式システムをAXIS Camera Station Proに接続し、装着式ボディカメラからの録画とメタデータを転送します。

1. [Configuration (設定)] > [Body worn (装着式)] > [Connect a body worn system (装着式システムを接続する)] に移動します。
2. [Connection method (接続方法)] で接続方法を選択します。
   - [Connect directly (直接接続)]: Body Worn ManagerのIPアドレスと認証情報を入力します。
   - [Generate connection file (接続ファイルの生成)]: Body Worn Managerにアップロードする構成ファイルを作成します。

注

サーバーのIPアドレスが変更された場合、またはAXIS Camera Stationが5.33より前のバージョンからアップグレードされた場合は、接続ファイルを作成する前にサーバー証明書を更新してください。証明書の更新方法については、*証明書, on page 148*を参照してください。

[Connect directly (直接接続)] を選択した場合:

3. [Configure direct connection (直接接続の設定)] で、Body Worn Managerの[IP address (IPアドレス)]、[User name (ユーザー名)]、[Password (パスワード)] を入力します。

1. 必要に応じて、[AXIS Camera Station system name (AXIS Camera Stationシステム名)] を変更します。この名前は、コピーや転送された録画データの保存先を示します。
2. 既存の接続をすべて終了する場合は、[End existing connections (既存の接続を終了する)] を選択します。新規接続ファイルを各AXIS Body Worn Systemコントローラーにアップロードする必要があります。
3. [Connect (接続)] をクリックします。

[Generate connection file (接続ファイルの生成)] を選択した場合:

4. [Generate connection file (接続ファイルの生成)] で [AXIS Camera Station system name (AXIS Camera Station システム名)] を変更します (任意)。この名前は録画をコピーまたは転送する場所を特定するのに役立ちます。
   4.1. 既存の接続をすべて終了する場合は、[End existing connections (既存の接続を終了する)] を選択します。新規接続ファイルを各AXIS Body Worn Systemコントローラーにアップロードする必要があります。
   4.2. [Export (エクスポート)] をクリックし、接続ファイルを保存します。
   4.3. 装着式マネージャーに接続ファイルをアップロードします。

Axis装着式システムの設定

AXIS Body Worn Cameraの録画の再生とエクスポート

スナップショット

録画をAXIS Camera Station Proに送信する際、装着式のブックマークからフォルダーにスナップショットを自動的にエクスポートします。

1. **[Configuration (設定)] > [Body worn (装着式)] > [Snapshots (スナップショット)]** に移動します。
2. **Storage location (保存先)]** に、スナップショットを保存するフォルダーのパスを入力します。
3. [**適用**] をクリックします。
4. **[Snapshot export (スナップショットのエクスポート)]** をオンにします。

CAD統合

コンピューター支援指令 (CAD) システムを統合し、指令データに基づいて装着式ボディカメラの録画を自動的に分類します。

以下の手順に従って統合を設定します。

1. **[Configuration (設定)] > [Body worn (装着式)] > [CAD integration (CAD統合)]** に移動します。
2. **[Set up integration (統合を設定する)]** をクリックします。
3. ファイル形式 (CSVまたはXML) を選択し、**[Next (次へ)]** をクリックします。
4. CADファイルが共有ネットワークドライブにある場合は、**[Shared network drive (共有ネットワークドライブ)]** をオンにします。
5. CADファイルのフォルダーパス、ファイル名 (CSVのみ)、区切り文字を入力します。
6. **[Next (次へ)]** をクリックします。
7. 各フィールドを、CADファイルに記載されている識別子に割り当てます。
   - **Officer name (オフィサー名)**: AXIS Camera Station Proのバーチャルカメラ名と一致している必要があります。名前が一致しない場合は、AXIS Camera Station Proではなく、Body Worn Managerで更新してください。
   - **Event ID (イベントID)**: 一意のディスパッチ識別子。
   - **Call category (呼び出しカテゴリー)**: 録画カテゴリー。ない場合は作成されます。
   - **Dispatch time (ディスパッチ時刻)**: RFC 3339形式の開始時刻。例: 2025-11-25T09:49:17+01:00。
   - **Clearance time (クリアランス時刻)**: RFC 3339 形式の終了時刻。
   - **Case number (ケース番号)**: このディスパッチに関連付けられたケースID。この列はファイル内に存在している必要がありますが、値は空欄のままにしておくことができます。
8. **[Finish (終了)]** をクリックし、**[Apply (適用)]** をクリックします。

9. 録画を確認するには、＋をクリックし、[CAD recordings (CAD録画)] を選択して自動的に分類されたすべての録画を表示します。日時やオフィサー名で絞り込むことができます。

注

新規カテゴリーが自動的に作成された場合、その保存期間を手動で設定する必要があります。

制限事項

以下の場合、情報が失われることがあります。

- AXIS Camera Station Proまたはコンポーネントが実行していない。
- エクスポートファイルのサイズが1 GBを超えている。
- ネットワーク認証情報の更新が必要である。

装着式の設定

装着式の録画の保存先を設定します。

録画ストレージ

新規システムユーザーの装着式システムの録画データのデフォルト保存先を選択します。

1. [Configuration (設定)] > [Body worn (装着式)] > [Body worn settings (装着式の設定)] に移動します。
2. [Recording storage (録画ストレージ)] で、[Disk (ディスク)] ドロップダウンからディスクを選択します。
3. [Save (保存)] をクリックします。

拒否された録画のストレージ

装着式システムからの拒否されたコンテンツの保存先を選択します。

1. [Rejected recordings storage (拒否された録画のストレージ)] で、[Disk (ディスク)] ドロップダウンからディスクを選択し、[Folder (フォルダー)] の名前を入力します。
2. [Number of days to keep rejected content from the body worn system (装着式システムから拒否されたコンテンツを保持する日数)] に拒否されたコンテンツを保持する日数を設定します。
3. [Save (保存)] をクリックします。

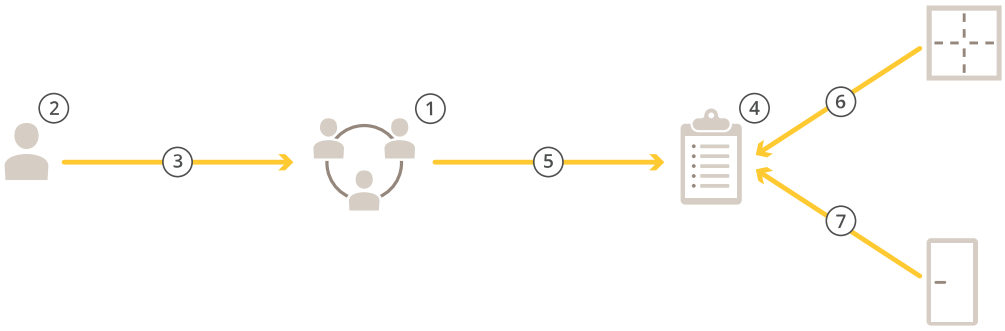
アクセス管理

[Access management (アクセス管理)] タブで、システムのカード所持者、グループ、アクセスルールの設定や管理を行います。

AXIS Camera Station ProでAxisネットワークドアコントローラーを設定する手順の詳細については、「*Axisネットワークドアコントローラーを設定する*」を参照してください。

アクセス管理のワークフロー

アクセス管理の構造には柔軟性があり、ニーズに合わせてワークフローを開発することができます。ワークフローの例:



1. *「グループの追加」, on page 197.*
2. *カード所持者の追加, on page 192.*
3. カード所持者とグループの追加。
4. *アクセスルールを追加します。, on page 197.*
5. アクセスルールへのグループの適用。
6. アクセスルールへのゾーンの適用。
7. アクセスルールへのドアの適用。

カード所持者の追加

カード所持者とは、システムに登録された一意のIDを持つ人物です。本人を識別する認証情報を含むカード所有者を設定し、いつ、どのようにドアにアクセスできるのかを定義します。

また、Active Directoryデータベース内のユーザーをカード所持者としてマッピングすることもできます。*Active Directory設定BETA, on page 181*を参照してください。

1. [Access Management (アクセス管理)] タブを開きます。
2. [Cardholder management (カード所持者監理)] > [Cardholders (カード所持者)] に移動し、 [Add (追加)] をクリックします。
3. カード所持者の姓名を入力します。必要に応じて、カード所持者に以下の詳細情報を追加します。
   - Email (電子メール) 欄に、カード所持者の電子メールアドレスを入力します。
   - Groups (グループ) から、カード所持者を追加したいグループを選択します。
   - Access rules (アクセスルール) で、そのカード所持者に適用したいアクセスルールを選択します。
4. 写真を追加するには、[Cardholder picture (カード所持者の写真)] をクリックし、以下のどちらかを選択します。

- Upload (アップロード)：デバイスから画像を追加します。
- Capture (キャプチャー)：カメラで直接写真を撮ります。

注

画像はJPG、PNG、GIF形式のいずれかである必要があります。画像は自動的に最大700×700ピクセルにリサイズされ、JPG形式に変換されます。

5. その他のオプションを設定するには、[Advanced (詳細)] をクリックします。
6. カード所持者に認証情報を追加します。*認証情報の追加, on page 194*を参照してください。
7. [Save (保存)] をクリックします。
8. バッジを印刷するには、1つ以上のカード所有者を選択し、[Print Badge BETA (バッジの印刷)] をクリックします。詳細については、*バッジBETAの印刷, on page 203*を参照してください。

検索フィールドを使用して、カード所持者の名前または苗字で検索してください。ソースでフィルタリングするには、[Filter (フィルター)]をクリックして、[Local (ローカル)]、[Global (グローバル)]、[AD]、[Center (センター)]のいずれかを選択してください。

高度	
長いアクセス時間	ドアモニターが設置されている場合、カード所持者に長いアクセス時間と長い長時間のドア開放を許可する場合に選択します。
カード所持者の停止	カード所持者を停止する場合に選択します。これによって、そのカード所持者から一時的にすべてのアクセスが削除されます。
Allow double-swipe (ダブルスワイプを許可する)	カード所有者がドアの現在の状態を上書きできるようにする場合に選択します。たとえば、カード所持者は通常のスケジュール外にドアのロックを解除するためにこれを使用できます。
閉鎖の対象外	カード所有者が閉鎖中にアクセスできるようにする場合に選択します。
Exempt from anti-passback (不正通行防止からの免除)	カード所持者に不正通行防止ルールからの免除を与える場合に選択します。不正通行防止は、カード所持者が自分より前にそのエリアに入った人と同じ認証情報を使用することを防ぎます。最初の人は、認証情報を再度使用する前に、まずそのエリアから退出する必要があります。
グローバルカード所持者	サブサーバーでカード所持者を表示および監視できるようにする場合に選択します。このオプションは、メインサーバーで作成されたカード所持者にのみ使用できます。*マルチサーバーBETA, on page 179*を参照してください。

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。

カード所持者とグループの追加

認証情報の追加

カード所持者には、次のタイプの認証情報を追加できます。

- *QRコード認証情報, on page 194*
- *PIN認証情報, on page 194*
- *モバイル認証情報, on page 195*
- *カード認証情報, on page 195*
- *ナンバープレートの認証情報, on page 195*

有効期限	
発効日	認証情報が有効になる日時を設定します。
失効日	ドロップダウンメニューからオプションを選択します。

失効日	
終了日がありません	認証情報に有効期限を設けません。
日付	認証情報が失効する日時を設定します。
最初の使用から	認証情報を初めて使用してから失効するまでの期間を選択します。最初に使用してからの日数、月数、年数、または回数を選択します。
最後の使用から	認証情報を最後に使用してから失効するまでの期間を選択します。最後に使用してからの日数、月数、または年数を選択します。

QRコード認証情報

注

QRコードを認証情報として使用するには、システムコントローラーとAXIS Barcode Readerを搭載したカメラの時刻が同期されている必要があります。両デバイスの時刻を同期させるため、同じ時刻ソースを使用することをお勧めします。

カード所持者にQRコード認証情報を追加するには：

1. [Credentials (認証情報)] で ＋ [Add (追加)] をクリックし、[QR-code (QRコード)] を選択します。
2. 認証情報の名前を入力します。
3. [Dynamic QR (動的QR)] はデフォルトで有効になっています。PIN認証情報と組み合わせて使用する必要があります。
4. 認証情報の開始日と終了日を設定します。
5. カード所持者を保存した後にQRコードを自動的に電子メールで送信するには、[Send QR code to cardholder when credential is saved (認証情報の保存時にカード所持者にQRコードを送信する)] を選択します。
6. [追加] をクリックします。

PIN認証情報

カード所持者にPIN認証情報を追加するには：

1. [Credentials (認証情報)] で ＋ [Add (追加)] をクリックし、[PIN] を選択します。
2. PINを入力します。

3. 必要に応じて、別のPINでサイレントアラームを作動させるには、**強制 PIN** を有効にし、強制PINを入力します。
4. 認証情報の**有効開始日**と **有効終了日**を設定します。
5. [**追加**] をクリックします。

モバイル認証情報

注
モバイル認証情報を受け取るには、カード保有者にメールアドレスが設定されている必要があります。

カード所持者にモバイル認証情報を追加するには：

1. [**Credentials (認証情報)**] で [**Add (追加)**] をクリックし、[**Mobile credential (モバイル認証情報)**] を選択します。
2. 認証情報の名前を入力します。
3. 認証情報の開始日と終了日を設定します。
4. [**保存後にモバイル認証情報をカード所持者に送信する**] を選択します。カード所持者に、ペアリングの手順が記載された電子メールが送信されます。
5. [**追加**] をクリックします。

例については、*AXIS Mobile CredentialアプリをBluetooth認証情報として使用する, on page 169*を参照してください。

カード認証情報

カード所持者にカード認証情報を追加するには：

1. [**Credentials (認証情報)**] で [**Add (追加)**] をクリックし、[**Card (カード)**] を選択します。
2. カードデータを手動で入力するには、カード名、カード番号、ビット長を入力します。

注
ビット長は、システムですでに定義されていない特殊なビット長のカードフォーマットを作成する場合にのみ設定可能です。

3. 前回読み取られたカードのカードデータを自動的に取得するには:
   3.1. [**Select reader (リーダーの選択)**] のドロップダウンメニューからドアを選択します。
   3.2. そのドアに接続されているリーダーにカードを読み取らせます。
   3.3. [**Get last swiped card data from the door's readers (ドアのリーダーから前回読み取ったカードデータを取得)**] をクリックします。

注
2NデスクトップUSBカードリーダーを使用して、カードデータを取得できます。詳細については、「*2NデスクトップUSBカードリーダーの設定*」を参照してください。

4. 設備コードを入力します。このフィールドは、**[Access management (アクセス管理)] > [Settings (設定)]** で **[Facility code (設備コード)]** をオンにしている場合のみ使用できます。
5. 認証情報の開始日と終了日を設定します。
6. [**追加**] をクリックします。

ナンバープレートの認証情報

カード所持者にナンバープレート認証情報を追加するには：

1. [Credentials (認証情報)] で ＋ [Add (追加)] をクリックし、[License plate (ナンバープレート)] を選択します。
2. 車両を表す認証情報名を入力します。
3. 車両のナンバープレート番号を入力します。
4. 認証情報の開始日と終了日を設定します。
5. [追加] をクリックします。

認証情報としてナンバープレート番号を使用する

この例では、ドアコントローラーと共に、AXIS License Plate Verifierをインストールしたカメラを利用することで、車両のナンバープレート番号を認証情報として使用してアクセスを許可する方法を示します。

1. ドアコントローラーとカメラを AXIS Camera Station Proに追加します。*デバイスの追加, on page 6*を参照してください。
2. 新しい装置のファームウェアを利用可能な最新バージョンにアップグレードします。*ファームウェアのアップグレード, on page 72*を参照してください。
3. ドアコントローラーに接続された新しいドアを追加します。*ドアの追加, on page 157*を参照してください。
   3.1. [Side A (側面A)] にリーダーを追加します。*「リーダーの追加」, on page 167*を参照してください。
   3.2. [Door settings (ドア設定)] で、[Reader type (リーダータイプ)] として [AXIS License Plate Verifier] を選択し、リーダーの名前を入力します。
   3.3. 必要に応じて、[Side B (側面B)] にリーダーまたはREX装置を追加します。
   3.4. Okをクリックします。
4. AXIS License Plate Verifierをカメラにインストールしてアクティブ化します。*AXIS License Plate Verifier*ユーザーマニュアルを参照してください。
5. AXIS License Plate Verifierを起動します。
6. AXIS License Plate Verifierを設定します。
   6.1. [Configuration > Access control > Encrypted communication (設定 > アクセスコントロール > 暗号化通信)] に移動します。
   6.2. [External Peripheral Authentication Key (外部周辺機器認証)] キーで [Show authentication key (認証キーの表示)]、[Copy key (キーのコピー)] の順にクリックします。
   6.3. カメラのwebインターフェースからAXIS License Plate Verifierを開きます。
   6.4. セットアップウィザードをスキップします。
   6.5. [Settings (設定)] に移動します。
   6.6. [Access control (アクセスコントロール)] で、[Type (タイプ)] に [Secure Entry] を選択します。
   6.7. [IP address (IPアドレス)] に、ドアコントローラーのIPアドレスを入力します。
   6.8. [Authentication key (認証キー)] に、先ほどコピーした認証キーを貼り付けます。
   6.9. [Connect (接続)] をクリックします。
   6.10. [Door controller name (ドアコントローラー名)] で、使用するドアコントローラーを選択します。
   6.11. [Reader name (リーダー名)] で、先ほど追加したリーダーを選択します。
   6.12. 統合をオンにします。

7. アクセス権を付与するカード所有者を追加します。*カード所持者の追加, on page 192*を参照してください。
8. 新しいカード所持者にナンバープレートの認証情報を追加します。*認証情報の追加, on page 194*を参照してください。
9. アクセスルールを追加します。*アクセスルールを追加します。, on page 197*を参照してください。
   9.1. スケジュールを追加します。
   9.2. ナンバープレートへのアクセス権を付与するカード所持者を追加します。
   9.3. AXIS License Plate Verifierリーダーのあるドアを追加します。

「グループの追加」

グループを使用すると、カード所有者とそのアクセスルールをまとめて管理できます。

1. [Access Management (アクセス管理)] タブを開きます。
2. **[Cardholder management (カード所持者)]** > **[Group (グループ)]** に移動し、 **[Add (追加)]** をクリックします。
3. グループ名と、オプションとしてグループのイニシャルを入力します。
4. **[Global group (グローバルグループ)**を選択し、サブサーバーのカード所有者を表示・監視します。このオプションは、メインサーバーで作成されたカード所持者にのみ使用できます。*マルチサーバー*[BETA]*, on page 179*を参照してください。
5. 以下の手順に従ってグループにカード所持者を追加します。
   5.1. **追加**をクリックします。
   5.2. 追加するカード所持者を選択し、**[Add (追加)]** をクリックします。
6. **[Save (保存)]** をクリックします。
7. グループ内のすべてのカード所有者のバッジを印刷するには、グループを選択し、**[Print Badge** BETA **(バッジの印刷)]** をクリックします。詳細については、*バッジ*[BETA]*の印刷, on page 203*を参照してください。

アクセスルールを追加します。

アクセスルールによって、アクセス権を付与されるための条件が定義されます。

アクセスルールの構成要素は以下のとおりです。

カード所持者とカード所持者グループ: - アクセス権が付与される人です。

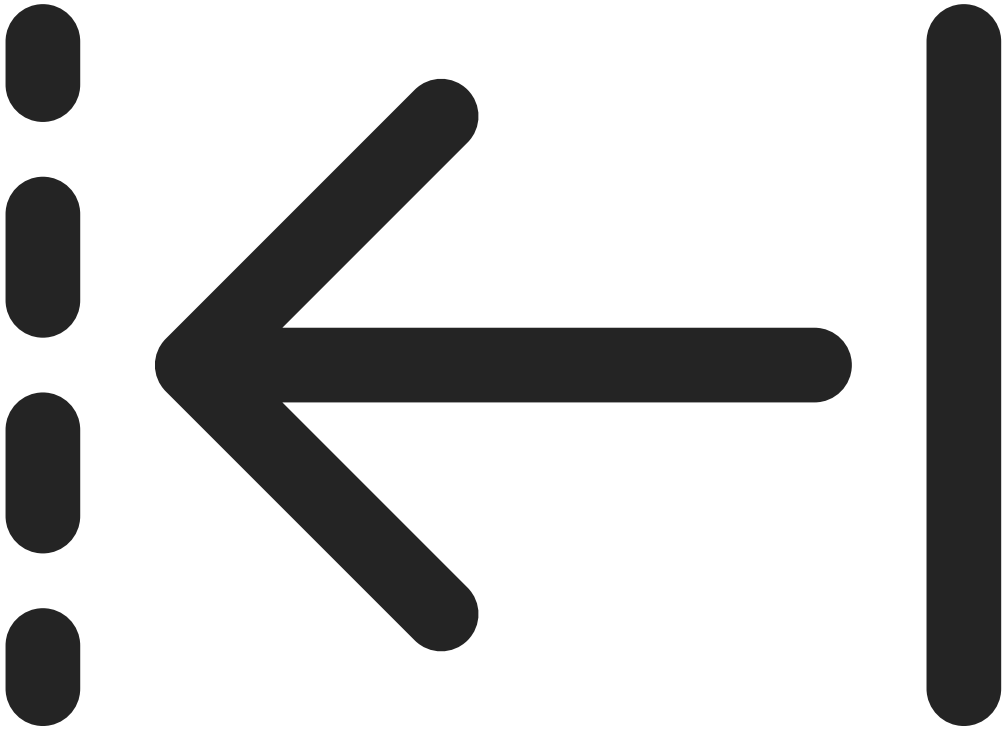
ドアとゾーン - アクセス権が適用される場所です。

スケジュール - アクセス権が付与される期間です。

アクセスルールを追加するには:

1. [Access Management (アクセス管理)] タブを開きます。
2. **[Cardholder management (カード所持者の管理)]** に移動します。

3. [Access rules (アクセスルール)]



で、 [Add (追加)] をクリックします。
4. アクセスルール名を入力し、[Next (次へ)] をクリックします。
5. カード所持者とグループを設定する:
   5.1. [Cardholders (カード所持者)] または [Groups (グループ)] で [Add (追加)] をクリックします。
   5.2. カード所持者またはグループを選択し、[Add (追加)] をクリックします。
   5.3. カード所持者やグループをアクセスルールに直接ドラッグ アンド ドロップして適用することもできます。ドラッグ操作を行うと、ドロップ可能なアクセスルールがハイライト表示されます。複数のカード所持者やグループを一度にドラッグすると、移動しようとしているものの数が表示されます。
6. ドアとゾーンを設定する:
   6.1. [Doors (ドア)] または [Zones (ゾーン)] で、 [Add (追加)] をクリックします。
   6.2. ドアまたはゾーンを選択し、[Add (追加)] をクリックします。
7. スケジュールを設定する:
   7.1. [Schedules (スケジュール)] で、 [Add (追加)] をクリックします。

7.2. 1つ以上のスケジュールを選択し、[Add (追加)] をクリックします。

8. [Save (保存)] をクリックします。

上記の構成要素の1つ以上が欠けているアクセスルールは、不完全です。すべての不完全なアクセスルールは、[Incomplete (不完全)] タブで確認することができます。

システム設定レポートをエクスポートする

システムに関するさまざまな種類の情報を含むレポートをエクスポートできます。AXIS Camera Station Proはレポートを CSV (カンマ区切り値) ファイルとしてエクスポートし、デフォルトのダウンロードフォルダーに保存します。レポートをエクスポートするには:

1. [Access Management (アクセス管理)] タブを開きます。
2. [Reports (レポート)] > [System configuration (システム設定)] に移動します。
3. エクスポートするレポートを選択し、[Download (ダウンロード)] をクリックします。

カード所持者の詳細レポート	カード所持者、認証情報、カードの有効性、前回の利用状況についての情報が記載されています。
カード所持者のアクセスレポート	カード所持者の情報と、カード所持者に関連するカード所持者グループ、アクセスルール、ドア、ゾーンについての情報が記載されています。
カード所持者グループのアクセスレポート	カード所持者グループ名と、カード所持者グループに関連するカード所持者、アクセスルール、ドア、ゾーンについての情報が記載されています。
アクセスルールレポート	アクセスルール名と、アクセスルールに関連するカード所持者、カード所持者グループ、ドア、ゾーンについての情報が記載されています。
ドアのアクセスレポート	ドアの名前と、ドアに関連するカード所持者、カード所持者グループ、アクセスルール、ゾーンについての情報が記載されています。
ゾーンのアクセスレポート	ゾーンの名前と、ゾーンに関連するカード所持者、カード所持者グループ、アクセスルール、ドアについての情報が記載されています。

カード所持者活動レポートの作成

点呼レポートは、指定されたゾーン内のカード所持者のリストを表示し、特定の時点にそこにいる人を特定するのに役立ちます。

集合レポートは、指定されたゾーン内のカード所持者のリストを表示し、緊急時に安全が確認された人と行方不明者の確認に役立ちます。避難後に建物管理者が職員や来訪者の所在を把握するのに役立ちます。マスターポイントは、緊急時に担当者が報告する指定のリーダーです。システ

ムは、サイトにいる人とサイト外にいる人のレポートを生成します。システムは、カード所持者が集合場所でチェックインするか、誰かが手動で安全であるとマークするまで、カード所持者を行方不明としてマークします。

点呼レポートと集合レポートはどちらも、カード所持者を追跡するためのゾーンを必要とします。

点呼または集合レポートを作成して実行するには、以下の手順に従います。

1. [Access Management (アクセス管理)] タブを開きます。
2. [**Reports (レポート)**] > [**Cardholder activity (カード所持者の活動)**] に移動します。
3. [**Add (追加)**] をクリックし、[**Roll call / Mustering (点呼/集合)**] を選択します。
4. レポート名を入力します。
5. レポートに含めるゾーンを選択します。
6. レポートに含めるグループを選択します。
7. 集合レポートが必要な場合は、[**Mustering point (集合場所)**] とリーダーを選択します。
8. レポートのタイムフレームを選択します。
9. **[Save (保存)]** をクリックします。
10. レポートを選択し、[**Run (実行)**] をクリックします。

点呼レポートのステータス	説明
在席	カード所持者が指定ゾーンに入り、レポートを実行するまでに退出しなかった場合。
不在	カード所持者が指定ゾーンを退出し、レポートを実行するまでに再度入らなかった場合。

集合レポートのステータス	説明
安全	カード所持者が集合場所でカードをスワイプした場合。
行方不明	カード所持者が集合場所でカードをスワイプしなかった場合。

インポートとエクスポート

カード所持者のインポート

このオプションは、CSVファイルからカード所持者、グループ、認証情報、写真をインポートします。カード所持者の写真をインポートするには、サーバーが写真にアクセスできることを確認してください。

カード所持者をインポートすると、アクセス管理システムは、すべてのハードウェア設定を含むシステム設定を自動的に保存し、以前に保存された設定を削除します。

また、Active Directoryデータベース内のユーザーをカード所持者としてマッピングすることもできます。*Active Directory設定BETA, on page 181*を参照してください。

インポートオプション	
新規	既存のカード所有者を削除し、新しいカード所有者を追加します。
更新	既存のカード所持者を更新し、新しいカード所持者を追加します。
追加	既存のカード所持者を保持し、新しいカード所持者を追加します。カード番号とカード所持者IDは一意であり、一度しか使用できません。

1. [Access Management (アクセス管理)] タブで、[Import and export (インポートとエクスポート)] をクリックします。
2. [Import cardholders (カード所持者をインポートする)] をクリックします。
3. [New (新規)]、[Update (更新)]、または [Add (追加)] を選択します。
4. **[Next (次へ)]** をクリックします。
5. [Choose a file (ファイルを選択)] をクリックし、CSV ファイルを選択して、[Open (開く)] をクリックします。
6. 列区切り文字を入力し、一意の識別子を選択して [Next (次へ)] をクリックします。
7. 各列に見出しを割り当てます。
8. [Import (インポート)] をクリックします。

インポート設定	
最初の行はヘッダー	CSVファイルに列ヘッダーが含まれている場合に選択します。
列区切り記号	CSVファイルの列区切り形式を入力します。
一意の識別子	システムでは、デフォルトでCardholder ID (カード所持者ID) を使用してカード所持者が識別されます。姓と名、またはメールアドレスを使用することもできます。これを使用して、重複する個人記録がインポートされるのを防ぎます。
カード番号の形式	デフォルトでは [Allow both hexadecimal and number (16進数と数字の両方を有効にする)] がオンになっています。

: カード所持者をエクスポートする

このオプションを実行すると、システム内のカード所持者データがCSVファイルにエクスポートされます。

1. [Access Management (アクセス管理)] タブで、[Import and export (インポートとエクスポート)] をクリックします。
2. [Export cardholders (カード所持者をエクスポートする)] をクリックします。
3. ダウンロード先を選択し、[Save (保存)] をクリックします。

AXIS Camera Station Proは設定が変更されるたびに、`C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry\Cardholder photos`のカード会員写真を更新します。

インポートの取り消し

カード所持者をインポートすると、設定が自動的に保存されます。[Undo import (インポートの取り消し)] オプションを選択すると、カード所持者データとすべてのハードウェア設定が、最後のインポートの前の状態にリセットされます。

1. [Access Management (アクセス管理)] タブで、[Import and export (インポートとエクスポート)] をクリックします。
2. [Undo import (インポートの取り消し)] をクリックします。
3. [Yes (はい)] をクリックします。

アクセス管理の設定

アクセス管理ダッシュボードで使用するカード所持者フィールドをカスタマイズする手順は、以下のとおりです。

1. [Access Management (アクセス管理)] タブで、[Settings (設定)] > [Custom cardholder fields (カード所持者フィールドをカスタマイズ)] をクリックします。
2. + [Add (追加)] をクリックして名前を入力します。カスタムフィールドは最大6つまで追加できます。
3. [追加] をクリックします。

設備コードを使用してアクセスコントロールシステムを検証するには:

1. [Access Management (アクセス管理)] タブで、[Settings (設定)] > [Facility code (設備コード)] をクリックします。
2. [Facility code on (設備コードオン)] を選択します。

注

識別プロファイルを設定するときは、[Include facility code for card validation (カード検証用の設備コードを含める)] も選択する必要があります。*識別プロファイル, on page 173*を参照してください。

QRまたはモバイル認証情報を送信するための電子メールテンプレートを編集するには：

1. [Access Management (アクセス管理)] タブで、[Settings (設定)] > [Email templates (電子メールテンプレート)] をクリックします。
2. テンプレートを編集し、[Update (更新)] をクリックします。

バッジのテンプレート BETA

バッジのテンプレートは、カード所持者の情報、写真、ロゴ、およびカスタムブランディングでカスタマイズできます。新規テンプレートの作成方法:

1. [Access management (アクセス管理)] > [Settings (設定)] > [Badge templates (バッジのテンプレート) BETA] に移動します。
2. [Create new template (テンプレートの新規作成)] をクリックします。
3. [Template name (テンプレート名)] のフィールドに名前を入力します。
4. デフォルトの印刷テンプレートとして使用するには、[Use as default template for printing (デフォルトの印刷テンプレートとして使用)] を選択します。
5. 以下の手順に従って、バッジのデザインをカスタマイズします。
   - 表面に表示するテキストフィールド (作成したカスタムフィールドも含む) を最大5つ選択します。印刷時には、入力済みのフィールドのみバッジに表示されます。
   - テキストのフォントとカラーを選択します。
   - 背景カラーまたは背景画像を追加します。

- 組織のロゴをアップロードします。
- 裏面に背景カラーまたは背景画像のいずれかを追加します。

6. [Save (保存)] をクリックして変更を保存するか、[Save as (名前を付けて保存)] をクリックして新規テンプレートを作成します。

注

テンプレートはいったん作成すると編集できません。名前の変更のみ可能です。

バッジBETAの印刷

設定済みのバッジテンプレートを使用して、カード所持者のIDバッジを印刷できます。現在、カードのエンコーダ機能はサポートされていません。開始する前に:

- カード所持者が少なくとも1つのカード認証情報を保持していることを確認します。認証情報がないカード所持者のバッジを印刷することはできません。
- CR80カードサイズと厚手のカード用紙などの印刷材料に対応するプリンターが必要です。
- ブラウザの印刷設定を以下のように設定します。
  1. 用紙サイズをCR80またはカード寸法に合わせたカスタムサイズに設定します。
  2. 縦向きに設定します。
  3. 余白をオフにするか、最小に設定します。

重要

Secure Entryは、Windowsドライバーを搭載したプリンターに対応しています。HID Fargoプリンターシリーズは、正常に動作することが確認されています。プリンターのドライバーが必要な場合は、プリンターの供給元にお問い合わせください。

以下の手順に従って、バッジを印刷します。

1. [Access management (アクセス管理)] > [Cardholder management (カード所持者の管理)] > [Cardholders (カード所持者)] に移動します。
2. 1名または複数のカード所持者を選択します。
3. [Print badge (バッジの印刷) BETA] をクリックします。
4. [Select template (テンプレートの選択)] をクリックし、[Template (テンプレート)] のドロップダウンメニューから使用するバッジテンプレートを選択します。
5. カード所持者が複数のカード認証情報を持っている場合、[Card (カード)] のドロップダウンメニューから1つ選択します。
6. [Print (印刷)] をクリックします。

注

お使いのプリンターが両面印刷に対応していない場合、まず表面のページをすべて印刷した後、カードの束を裏返してトレイに再びセットし、裏面のページを印刷してください。

System Health Monitoring[BETA]

[System Health Monitoring (システムの健全性監視)] タブを使用して、同じネットワーク上の1つまたは複数の AXIS Camera Station Proシステムの健全性データを監視します。

別のネットワーク上のシステムを管理している場合、My Systemsのサーバー監視は、クラウド経由で同じ機能を提供します。

	アクセスできる装置とシステムの概要を表示します。*在庫, on page 204*を参照してください。
	監視対象システムからの各カメラのストレージの概要と録画の詳細を表示します。*ストレージ, on page 205*を参照してください。
	監視対象システムからのSystem Health Monitoringログを表示します。*通知, on page 205*を参照してください。

制限事項

- AXIS S30および and S40 Recorder Seriesでは、録画用のストレージ容量を監視することはできません。
- 通知設定はローカルのSystem Health Monitoringサーバーにのみ影響します。
- システムは、連続録画と動きによってトリガーされる録画を除き、録画に **[None (なし)]** のフラグを立てます。

ワークフロー

1. *System Health Monitoring[BETA]の設定, on page 184*
   1.1. 通知を設定する. *通知, on page 185*を参照してください。
   1.2. マルチシステムを設定します。*マルチシステム, on page 186*を参照してください。
2. AXIS Camera Station Proシステムからのヘルスデータを監視します。
   2.1. *在庫, on page 204*
   2.2. *ストレージ, on page 205*
   2.3. *通知, on page 205*

在庫

インベントリページには、アクセスできる装置とシステムの概要が表示されます。

1. [**System Health Monitoring (システムの健全性監視)** BETA] タブで をクリックします。
2. システムの概要を表示するには、[**AXIS Camera Station**] をクリックします。
   右側のパネルに、システムとサーバーの詳細が表示されます。
3. システム内の装置の概要を表示するには、リスト内の装置をクリックします。
   デバイスにビデオソースが含まれている場合、右側のパネルにはデバイスとストレージに関する情報が表示されます。
4. システムレポートをダウンロードするには、[**Create report (レポートの作成)**] ドロップダウンメニューから [**AXIS Camera Station system report (AXIS Camera Stationシステムレポート)**] を選択します。*システムレポート, on page 218*を参照してください。
5. System Health Monitoringレポートをダウンロードするには:
   5.1. [**Create report (レポートの作成)**] のドロップダウンメニューから、[**System Health Monitoring report (システムの健全性監視レポート)**] を選択します。

5.2. レポートにデータベースを含めるには、[Include all databases (すべてのデータベースを含める)] を選択し、[Download (ダウンロード)] をクリックします。

5.3. レポートが生成されたら、クリックして保存します。

ストレージ

ストレージページには、監視対象システムからの各カメラのストレージの概要と録画の詳細が表示されます。列見出しをクリックすると、その列で並べ替えられます。

1. [System Health Monitoring (システムの健全性監視) BETA] タブでをクリックします。
2. マルチシステムヘルスデータを監視するときは、ドロップダウンメニューからシステムを選択します。

概要	
ステータス	ストレージのステータス。*ストレージの設定, on page 79*を参照してください。
所在地：	ストレージのパスと名前。
合計	ストレージ容量の合計です。保存先に関する Windows のプロパティに表示される「合計サイズ」と一致します。
割り当て済み	録画に割り当てられた最大ストレージ容量。
使用中	録画データが現在使用しているストレージ容量。
最終更新日	情報が最後に更新された時刻。

カメラ	
ステータス	(空白): 正常な状態。 警告アイコン: 保存要件が満たされていません。 情報アイコン: カメラの録画が短すぎるため、保存要件が満たされていません。
名称	カメラ名。
録画タイプ	カメラに適用される録画タイプ。
保存期間の設定	[Configuration (設定)] > [Storage (ストレージ)] > [Selection (選択)] でカメラに設定された保存期間。
現在の保存期間	録画データがストレージに保存されている日数。
最も古い録画	ストレージに保存されている最も古いカメラ録画の時刻。
最新の録画	ストレージに保存されている最新のカメラ録画の時刻。
所在地：	カメラが使用するストレージの場所。
使用済みストレージ	このカメラが録画に使用するストレージの量。
最終更新日	情報が最後に更新された時刻。

通知

通知ページには、監視対象システムからのSystem Health Monitoringログが表示されます。列見出しをクリックすると、その列で並べ替えられます。

[System Health Monitoring (システムの健全性監視) BETA] タブで をクリックします。

検出認識時間	
通知を送信しました	通知が送信された時刻。
アイテム	device downによってトリガーされた通知の場合はデバイス名が表示され、system downによってトリガーされた場合はsystemが表示されます。
システム	イベントが発生したシステム名。
ルール	通知をトリガーしたルール: System downまたはDevice down
検出	問題が検出された時刻。
解決	問題が解決された時刻。

ホットキー

[ホットキー] タブには、使用可能なホットキーが表示されます。ホットキーのタイプは、AXIS Camera Station Proの制御に何を使用するかによって異なります。

- キーボードのキーの組み合わせ
- キーパッドのキーの組み合わせ
- ジョイスティックボタン
- ジョグダイアルボタン

接続済みのサーバーからカメラまたはビューが切断されると、関連付けられているホットキーも削除されます。

システムではホットキーは次のカテゴリに分類されます。

- カメラ
- デバイスの管理
- カメラに移動する
- ビューに移動する
- ナビゲーション
- PTZプリセット
- 録画
- シーケンス
- 分割ビュー
- タブ
- その他

[Navigate to cameras (カメラに移動)] および [Navigate to views (ビューに移動)] カテゴリーのアクションに手動で割り当てる必要があります。

注

- ホットキーを追加または編集するときに、そのホットキーが別のアクションですでに使用されている場合、警告アイコンが表示されます。警告アイコンにカーソル合わせると、競合するアクションが表示されます。キャンセルするには、ESCキーを押します。ENTERキーを押すと、そのホットキーが使用され、競合するホットキーが自動的に削除されます。
- 複数のサーバーに接続している場合、[カメラに移動] カテゴリと [ビューに移動] カテゴリには、接続済みのサーバー上のカメラとビューも一覧表示されます。

ホットキーの割り当て	アクションのキーボード値がない場合は、空のフィールドをクリックしてホットキーを追加します。 • キーボードを使用してホットキーを追加する場合は、Ctrlキーとその他の1つ以上のキー、またはファンクションキー (F2～F12) を押します。 • キーパッドのホットキーを追加する場合は、数値キーの組み合わせを押すか、F1～F5のいずれかのファンクションキーを押します。 • ジョイスティックまたはジョグダイアルを使用してでホットキーを追加する場合は、ジョイスティックまたはジョグダイアルを押して割り当てます。
ホットキーの編集	アクションのキーボード値をクリックして編集します。
ホットキーの削除	アクションのキーボード値をクリックして削除します。
	をクリックすると、ホットキー表を印刷できます。
	をクリックすると、すべてのホットキーが元の設定にリセットされます。

映像監視制御ボードのキー

ホットキーマッピング - ジョイスティック	デフォルトのアクション	AXIS TU9002	AXIS T8311
ボタン1	プリセット1に移動	J1	J1
ボタン2	プリセット2に移動	J2	J2
ボタン3	プリセット3に移動	J3	J3
ボタン4	プリセット4に移動	J4	J4
ボタン5	左マウスボタンをシミュレートする	J5	L
ボタン6	左右ボタンをシミュレート	J6	R
ボタン7	分割ビュー内の前のセルを選択	左上	-
ボタン8	分割ビュー内の次のセルを選択	右上	-
ボタン9	前の録画に戻る		-
ボタン10	再生/一時停止		-

ホットキーマッピング - ジョイスティック	デフォルトのアクション	AXIS TU9002	AXIS T8311
ボタン 11	次の録画に進む	⏭	-
ボタン 12	ブックマークを追加	⚑	-
ボタン 13	ズームリング機能をデジタルズームと再生速度コントロールとで切り替える	M1	-
ボタン 14	ライブ/録画の切り替え	M2	-
ボタン 15	前のフレームに戻る	左上の切り替え	-
ボタン 16	次のフレームに進める	右上の切り替え	-

ホットキーマッピング - キーパッド	デフォルトのアクション	AXIS TU9003	AXIS T8312
A	ビューを開く	⊞	⊞
B	次のカメラ/ビューに移動する	🎥	🎥
ALT+B	前のカメラ/ビューに移動する	Alt+🎥	-
タブ	次のタブに移動する	⇥	-
ALT +TAB	前のタブに移動する	Alt+⇥	-
C	-	-	✥
D	-	-	🕒
E	-	-	🛠
プラス (+)	より遠くにフォーカスする	+	-
マイナス (-)	より近くにフォーカスする	-	-
F2	ホットキーを開く	F2	F2
F4	ログを開く	F4	F4
F5	バージョン	F5	F5
F10	オートフォーカス	F10	-

ホットキーマッピング - ジョグ	デフォルトのアクション	AXIS T8313
ジョグ1	エクスポートマーカーを表示または非表示にする	L
ジョグ2	ブックマークを追加	
ジョグ3	前の録画に戻る	
ジョグ4	再生/一時停止	
ジョグ5	次の録画に進む	
ジョグ6	ライブ/録画の切り替え	R

注

AXIS T8311 映像監視ジョイスティックは、ジョイスティックボタン7〜10をサポートしていません。

ログ

[Logs (ログ)] タブには、デフォルトで、ライブアラーム、イベント、監査ログが表示されます。以前のログも検索できます。[Configuration (設定)] > [Server (サーバー)] > [settings (設定)] ログを保持する日数を設定できます。

時間	操作の日付と時刻。
タイプ	アクションのタイプ: アラーム、イベント、または監査。
カテゴリー	操作のカテゴリー。
メッセージ	操作の簡単な説明。
ユーザー	アクションを実行する AXIS Camera Station Proユーザー。
コンピューター	AXIS Camera Station Proがインストールされているコンピューター (Windowsドメイン名)。この値はクライアントから提供され、サーバーによって個別に検証できません。
Windowsユーザー	AXIS Camera Station Proを管理するWindowsユーザー。この値はクライアントから提供され、サーバーによって個別に検証できません。User (ユーザー) 列には認証ユーザーが表示されます。
サーバー	複数のサーバーに接続する場合にのみ表示されます。 操作を実行するサーバーです。
コンポーネント	ログが生成されるコンポーネントです。

ログを検索

1. [Logs (ログ)] タブの [Log search (ログ検索)] で [Search (検索)] をクリックします。
2. フィルターボックスにキーワードを入力します。AXIS Camera Station Proは[Time (時間)] を除くログリストを検索し、すべてのキーワードを含む結果を表示します。サポート対象の検索演算子については、*検索の最適化, on page 46*を参照してください。
3. [Filter (フィルター)] で、[Alarms (アラーム)]、[Audits (監査)] 、または [Events (イベント)] を選択します。
4. カレンダーから日付または日付の範囲を選択します。
5. ドロップダウンメニューから [Start time (開始時刻)]、[End time (終了時刻)] を選択します。
6. [検索] をクリックします。

アラームログ

[Alarms (アラーム)] ログには、システムアラームと、ルールや動体検知によって生成されたアラームが表示されます。リストには、アラームの日付と時刻、アラームのカテゴリ、アラームのメッセージも示されます。アラームを参照してください。

	アラームを選択し、 をクリックすると、[Recordings (録画)] タブが開き、アラームに録画が含まれている場合は再生が開始されます。
	アラームを選択し、 をクリックすると、アラームにアラーム手順が含まれている場合にアラーム手順が開きます。

✔	アラームを選択し、✔をクリックすると、他のクライアントにアラームが確認されたことが通知されます。
💾	アラームを選択し、💾をクリックすると、ログがテキストファイルにエクスポートされます。

イベントログ

[Events (イベント)] ログには、録画、トリガー、アラーム、エラー、システムメッセージなど、カメラとサーバーのイベントがリストで表示されます。リストには、イベントの日付と時刻、イベントのカテゴリ、イベントのメッセージも示されます。イベントを選択してツールバーの 💾 をクリックすると、イベントがテキストファイルとしてエクスポートされます。

監査ログ

[Audit (監査)] ログでは、手動録画、ビデオストリームの開始または停止、アクションルール、作成済みのドア、作成済みのカード所持者など、すべてのユーザーアクションを閲覧できます。監査を選択してツールバーの 💾 をクリックすると、それらがテキストファイルとしてエクスポートされます。

ナンバープレート管理

AXIS Camera Station Proでナンバープレートリストを管理するには、**[License plate management (ナンバープレート管理)]** タブを開きます。

このタブでは、個々のカメラまたはカメラグループごとに、3つのナンバープレートリストを編集できます。

1. **[Groups (グループ)]** と **[Cameras (カメラ)]** のリストからグループまたはカメラを選択します。
2. 編集するリストを選択します。編集可能な3つのリストは、デフォルトで**Allow (許可) リスト**、**Block (ブロック) リスト**、**Custom (カスタム) リスト**の名前が付けられています。
3. リストに変更を加える:
   - リスト名を変更するには、**[Edit list name (リスト名の編集)]** をクリックします。
   - 新規のナンバープレートを追加するには、[License plate (ナンバープレート)] 列にナンバープレートを入力し、必要に応じて [Description (説明)] 列に説明を入力します。**[追加]** をクリックします。
   - 既存のナンバープレートを編集または削除するには、そのナンバープレートを選択し、**[Edit (編集)]** または **[Remove (削除)]** をクリックします。
   - CSVファイルからナンバープレートリストをインポートするには、**[Import (インポート)]** をクリックしてファイルを選択します。これにより現在のリストが上書きされるため、コピーを残しておきたい場合は、まずリストをエクスポートしてください。
   - ナンバープレートリストをCSVファイルにエクスポートするには、**[Export (エクスポート)]** をクリックします。
4. **[Apply (適用)]** をクリックして変更を保存します。

注

変更を適用すると、AXIS Camera Station Proがそのグループまたはカメラのナンバープレートリストの管理を引き継ぎます。毎晩、AXIS Camera Station Proに保存されているリストに合わせてカメラの設定が更新されます。これにより、カメラに直接保存されていたナンバープレート情報は上書きされます。

AXIS Audio Manager Pro

[AXIS Audio Manager Pro] タブを使用すると、AXIS Camera Station Proから直接 AXIS Audio Manager Proサーバーのインターフェースにアクセスできます。サーバーインターフェースについて詳しくは、*AXIS Audio Manager Proユーザーマニュアル*を参照してください。

このタブは、AXIS Camera Station ProでAXIS Audio Manager Proサーバーに接続した後にのみ表示されます。詳しくは、*AXIS Audio Manager Proを設定する, on page 182*を参照してください。

重要

Secure Remote Access v2では、AXIS Audio Manager Proサーバーインターフェースにアクセスすることはできません。

この統合により、以下のことも可能になります。

- *AXIS Audio Managerのトリガーを作成する, on page 109*。
- *AXIS Audio Managerのアクションを作成する, on page 119*。.
- マップに音声ゾーンを追加する。*マップ, on page 23*を参照してください。
- *分割ビューでページングインターフェースを使用する, on page 21*。
- AXIS Camera Station ProでAXIS Audio Manager Pro関連のユーザー権限を設定する。*ユーザーまたはグループの権限, on page 145*を参照してください。
- AXIS Audio Manager Proサーバーから音声デバイスを選択し、カメラに関連付けられた音声デバイスとして設定する。*ストリームプロファイルの編集, on page 57*を参照してください。

アラーム

[Alarms (アラーム)] タブは AXIS Camera Station Proクライアントの下部にあり、トリガーされたイベントとシステムアラームが表示されます。アラームの作成方法については、*アクションルール*を参照してください。「データベースのメンテナンスが必要です」というアラームの詳細については、*データベースのメンテナンス, on page 236*を参照してください。

時間	アラームが発生した時刻。
カテゴリー	トリガーされたアラームのカテゴリー。
説明	アラームの簡単な説明。
サーバー	複数のサーバーに接続している場合に使用できます。アラームを送信する AXIS Camera Station Proサーバー。
コンポーネント	アラームをトリガーするコンポーネントです。
	アラームの手順を示します。アラームにアラーム手順が含まれている場合のみ使用できます。
	録画に移動します。アラームに録画が含まれている場合のみ使用できます。
	選択したアラームを確認する
	アラームを削除します。最初に確認を行わなかった場合、アラームは一時的にのみ削除されます。

特定のアラームに対処するには:

1. AXIS Camera Station Proクライアントの下部にある **[Alarms and Tasks (アラームとタスク)]** をクリックし、**[Alarms (アラーム)]** タブを開きます。
2. 録画のあるアラームの場合は、アラームを選択し、をクリックして、**[Recording alerts (録画アラート)]**タブで録画に移動します。
3. 録画のないアラームの場合は、ライブビューのタブを開き、アラームをダブルクリックして、[Recording alerts (録画アラート)] タブでアラーム時刻に対応する録画を表示します。
4. アラーム手順のあるアラームの場合は、アラームを選択し、をクリックすると、アラーム手順が開きます。
5. アラームが確認されたことを他のクライアントに通知するには、アラームを選択し、をクリックします。
6. リストからアラームを削除するには、アラームを選択し、をクリックします。

タスク

[Tasks (タスク)] タブは AXIS Camera Station Proクライアントの下部にあります。

以下のタスクは個人用です。管理者と、それらを開始したユーザーにのみ表示されます。

- システムレポート
- インシデントレポートを作成
- 録画のエクスポート

管理者は、個人用タスクを含め、ユーザーによって開始されたすべてのタスクを閲覧および操作できます。

オペレーターまたは閲覧者は、以下の操作を行うことができます。

- 自分が開始したすべてのタスクと、他のユーザーによって開始された個人用以外のタスクを閲覧する。
- 開始したタスクをキャンセルまたは再試行する。再試行できるのは、インシデントレポートタスクと録画のエクスポートタスクのみです。
- リスト内のすべてのタスクの結果を閲覧する。
- 完了したタスクをリストから削除する。これはローカルクライアントにのみ影響します。

名称	タスクの名前。
開始	タスクの開始時刻。
メッセージ	タスクに関するステータスまたは情報を表示します。 表示されるステータス: • **Canceling (キャンセル中)**: タスクをキャンセルする前のクリーンアップを実行しています。 • **Canceled (キャンセル済み)**: クリーンアップが完了し、タスクがキャンセルされました。 • **Error (エラー)**: 1つ以上のデバイスでタスクの実行に失敗しました。 • **Finished (終了)**: タスクが完了しました。 • **Finished during lost connection (接続が途切れている間に終了)**: サーバーへの接続が途切れている間にタスクが完了しました。タスクのスタータスを判定できません。 • **Lost connection (接続が途切れました)**: タスク実行中にクライアントとサーバーの接続が途切れました。タスクのステータスを判定できません。 • **Running (実行中)**: タスクを実行しています。 • **Pending (保留中)**: 別のタスクが完了するのを待っています。
オーナー	タスクを開始したユーザー。
進行状況	タスクの進行状況を表示します。
サーバー	複数のサーバーに接続している場合に使用できます。タスクを実行するAXIS Camera Station Proサーバーを表示します。

1つ以上のタスクに対処するには:

1. AXIS Camera Station Proクライアントの下部にある **[Alarms and Tasks (アラームとタスク)]**をクリックし、**[Tasks (タスク)]**タブをクリックします。

2. タスクを選択し、いずれかのアクションをクリックします。

	クリックして、[Task result (タスクの結果)] ダイアログを表示します。
	クリックして、タスクをキャンセルします。
	クリックして、リストからタスクを削除します。
	録画のエクスポートまたはインシデントレポートの作成時にタスクが失敗した場合にクリックして、失敗したタスクを再試行します。

タスクの結果

タスクが複数のデバイスで実行された場合、ダイアログは個々のデバイスについて、結果を表示します。失敗したすべての動作を手動で確認して設定します。

ほとんどのタスクについて詳細情報が一覧表示されます。**[Export recordings (録画のエクスポート)]** や **[System report (システムレポート)]**などのタスクについては、タスクをダブルクリックし、ファイルが保存されているフォルダーを開きます。

MACアドレス	更新されたデバイスのMACアドレス。
アドレス	更新されたデバイスのIPアドレス。
メッセージ	タスクの実行状況に関する情報: • **Finished (修了)**: タスクが正常に完了しました。 • **Error (エラー)**: デバイスでタスクを実行できませんでした。 • **Canceled (キャンセル済み)**: タスクは完了する前にキャンセルされました。
説明	タスクに関する情報。

実行したタスクのタイプに応じて、次の詳細情報が一覧表示されます。

新しいアドレス	デバイスに新たに割り当てられたIPアドレス。
アクションルール	デバイスのファームウェアバージョンと製品名。
詳細	元のデバイスのシリアル番号とIPアドレス、および、新しいデバイスのシリアル番号とIPアドレス。
参照ID	インシデントレポートの参照ID。

レポートの作成

クライアント用設定シート

クライアント用設定シートは、トラブルシューティングの実行やサポートへの連絡時に役立ちます。

クライアントシステム設定の全体をHTML形式で表示する:

1. [Configuration (設定)] > [Server (サーバー)] > [Diagnostics (診断)] に移動します。
2. [View client configuration sheet (クライアント用設定シートの表示)] をクリックします。

サーバー用設定シート

サーバー用設定シートには、一般的な設定情報に加え、アクションルール、スケジュール、録画ストレージ、補助デバイス、ライセンスを含むカメラの設定に関する情報が含まれます。サポートに連絡する際、このシートがトラブルシューティングに役立ちます。

サーバーシステム設定の全体をHTML形式で表示する:

1. [Configuration (設定)] > [Server (サーバー)] > [Diagnostics (診断)] に移動します。
2. [View server configuration sheet (サーバー用設定シートの表示)] をクリックします。

システムレポート

システムレポートは、ご使用のシステムをAxisのカスタマーサポートが分析するとき役立つ、各種パラメーターやログファイルの入った.zipファイルです。

カスタマーサポートにお問い合わせの際は、必ずシステムレポートを作成しておいてください。

システムレポートを生成するには:

1. > [Help (ヘルプ)] > [System report (システムレポート)] に移動します。
2. 自動生成されたファイル名を変更する場合は、ファイル名を編集します。
3. [Browse... (参照)] をクリックし、システムレポートの保存先を選択します。
4. 希望の設定を選択します。
   - すぐに開く場合は、[Automatically open folder when report is ready (レポートが生成されたら保存先のフォルダーを自動的に開く)] を選択します。
   - 録画やシステムデータの詳細情報を追加する場合は、Include all databases (すべてのデータベースを含む) を選択します。
   - システムレポートの分析に役立てる場合は、[Include screenshots of all monitor (すべてのモニターのスクリーンショットを含める)] を選択します。
5. [OK]をクリックします。

システムレポートを生成します。

注

- サーバーが起動しない場合は、AXIS Camera Station Service Controlの**[Tools (ツール)]** タブから簡易システムレポートを取得できます。
- クライアントがサーバーにサインインできない場合、Axisの顧客サポートから、代わりにクライアントのログを求められることがあります。これらは、お使いのクライアントバージョン固有のフォルダー: `C:\ProgramData\Axis Communications\AXIS Camera Station\Core\Client 6.xx` 内にあります。
- 問題の内容によっては、Windowsのイベントログを収集する必要がある場合もあります。これを行うには、イベントビューアーを開き、**[Windows Logs Windows (ログ)]** に移動し、**[Application (アプリケーション)]** を右クリックし、**[Save all events as (すべてのイベントに名前を付けて保存)]** を選択します。**[System (システム)]** でも同じ手順を実施します。

このような場合、Axisの顧客サポートは、調査のために通常のサーバーログが必要になります。

AXIS Installation Verifier

AXIS Installation Verifierは、システム内のすべての装置が完全に機能することを検証するインストール後のパフォーマンステストを開始します。テストの実行は約20分かかります。

テスト	
Normal conditions (通常の状態)	AXIS Camera Station Proの現在のシステム設定を使用するデータストリーミングおよびストレージのテスト。結果は合格または不合格として表示されます。
低光量条件	一般的な低光量条件に合わせて最適化された設定を使用するデータストリームおよびストレージのテスト。結果は合格または不合格として表示されます。
ストレステスト	システムの最大許容値までデータストリームとストレージを段階的に増加させるテスト。結果には最大システム性能が表示されます。

注

- AXIS Camera Application Platform 2 (ACAP 2) 以降をサポートする装置のみテストできます。
- テスト中、AXIS Camera Station Proはメンテナンスモードになり、すべての監視活動は一時的に使用できなくなります。

テストを開始するには:

1. **[Configuration (設定)]** > **[Server (サーバー)]** > **[Diagnostics (診断)]** に移動します。
2. **[Open AXIS installation verifier... (AXIS installation verifierを開く...)]** をクリックします。
3. **[開始]** をクリックします。
4. テスト終了後、**[View report (レポートの表示)]** をクリックしてレポートを開きます。**[Save report (レポートの保存)]** をクリックして保存します。

資産の一覧

ビデオ管理システムの資産の一覧をエクスポートできます。資産の一覧には、次の名前、タイプ、モデル、ステータス、およびシリアル番号が含まれます。

- 接続されているすべてのサーバー

- 接続されているすべての装置
- 複数のターミナルへの接続時に資産の一覧をエクスポートするクライアントターミナル

資産の一覧をエクスポートするには:

1. ☰ > [Other (その他)] > [Asset list (資産の一覧)]に移動します。
2. [エクスポート] をクリックします。
3. ファイルの場所を選択し、[保存] をクリックします。
4. [Latest export (最新のエクスポート)] で、ファイルへのリンクが表示または更新されます。
5. リンクをクリックして、ファイルの場所に移動します。

Axisサービスのステータス

Axisオンラインサービスのステータスを表示するには、以下の手順に従います。

1. [Configuration (設定)] > [Server (サーバー)] > [Diagnostics (診断)] に移動します。
2. [View status of Axis services (Axisサービスのステータスの表示)] をクリックします。

AXIS Camera Station Proサービスコントロールlを開きます。

サーバーは、AXIS Camera Station Proサービスコントロールを使用して開始、停止、設定の変更を行います。これは、設置が完了した後で自動的に起動します。サーバーコンピューターが再起動した場合、Service Controlは約2分以内に自動的に再起動します。Windowsの通知エリアにあるアイコンがサービスのステータスを示します。

アイコンを右クリックし、[Open AXIS Camera Station Service Control (AXIS Camera Station Service Controlを開く)]、[Start Service (サービスの開始)]、[Stop Service (サービスの停止)]、[Restart Service (サービスの再起動)]、または [Exit (終了)] を選択します。

[スタート] メニューからService Controlを開くには:

[Start (スタート)] メニューに移動し、[All Programs (すべてのプログラム)] > [Tools (ツール) > [Service Control] を選択します。

	Running (実行中):
	起動中
	停止

Modify Settings (設定の変更)	選択してサーバーの設定を変更します。
Restore Default Settings (デフォルト設定に戻す)	クリックすると、すべての設定が元のデフォルト設定に戻ります。
開始	クリックして、サーバーのステータスを変更します。
停止	
再起動	クリックして、サーバーを再起動します。

全般サーバー設定

AXIS Camera Station Pro Service Controlで、[**Modify settings (設定を変更)**] を選択し、[**General (全般)**] タブをクリックして、全般サーバー設定を変更します。

サーバー名	サーバーの名前。サーバー名はソフトウェアクライアントに表示されます。デフォルトのサーバー名は、コンピューター名です。コンピューター名を変えても名前は変わりません。
Web client port (Webクライアントポート)	AXIS Camera Station Webクライアントはこのポートを使用します。
Ports range (ポート範囲)	ポートの範囲を指定します。その他のポートは自動的に変更されます。
Allow AXIS Camera Station Pro to add exceptions to the Windows Firewall (にWindows Firewallへの例外の追加を許可する)	ユーザーがポート範囲を変更したとき、AXIS Camera Station ProがWindows Firewallに例外を自動的に追加することを許可する場合に選択します。

注

- サーバーとクライアントの間にNATやファイアウォールなどが存在する場合は、これらのポートの通過を許可するようにNATやファイアウォールを設定します。
- ポート番号は1024～65534の範囲内にあることが必要です。

AXIS Camera Station Proのポートリスト

次の表に、AXIS Camera Station Proが使用するポートとプロトコルを示します。最適なパフォーマンスとユーザビリティを確保するため、ファイアウォールでこれらを許可する必要がある場合があります。ポート番号は、HTTPメインポート29200に基づいて計算されます。一部のセクションには、必須ポートとオプションポートの両方が記載されています。AXIS Camera Station Proが正常に動作するためには、必要なポートを常に開放しておく必要があります。オプションポートが許可されていない場合、関連する機能は動作しません。

サーバーからデバイスへ

必須				
ポート	**番号**	**プロトコル**	**方向**	**説明**
メインHTTPおよびHTTPSポート	443	HTTPS	送信	ライセンスの有効化、ファームウェアのダウンロード、接続中のサービスに使用されます。

オプション				
デフォルトWS-Discoveryポート	3702	UDP	受信および送信	ONVIFデバイスの検出に使用されるWS-Discovery Webサービス。マルチキャスト239.255.255.25-0。
デフォルトBonjourポート	5353	UDP	受信および送信	mDNS (Bonjour)によるデバイスの検出に使用されます。マルチキャスト224.0.0.251。 デフォルトのポートが利用できない場合は、別のアプリケーションがそのポートを使用しており、共有しない可能性があります。その場合は、ランダムなポートが使用されます。ランダムなポートを使用する場合、リンクローカルアドレスを持つデバイスはBonjourから検出できないことに注意してください。

クライアントからサーバーへ

すべてのポートが必要です					
ポート	**番号**	**プロトコル**	**方向**	**通信**	**説明**
メインHTTPポートとHTTPストリーミングポート	29200	HTTP	受信	ACSサーバーとクライアント	ビデオ、音声、メタデータストリーム(AES暗号化)に使用されます。
メインTCPポート	29202	TCP	受信	ACSサーバーとクライアント	バージョン6.17以降、クライアントスイッチのみに使用されます。以前はこれがメイン

					TCPポートでした。
API Webサーバーポート	29204	HTTPS	受信	サーバーとモバイルアプリ	HTTPS経由でのアプリケーションデータおよびMP4ビデオストリーミングに使用されます。
ローカルプロキシHTTPポート	29206	TCP	受信	ACSサーバー内部	モバイルアプリはSRAモジュールを呼び出します。SRAモジュールはHTTPSを受信し、HTTPに変換して、ローカルプロキシのHTTPポートに再送信します。
Webプロキシエンドポイントポート	29207	TCP	受信	ACSサーバーとコンポーネント	コンポーネントと装置間の安全な通信に使用されます。

Secure Remote Access v2のドメインとポート

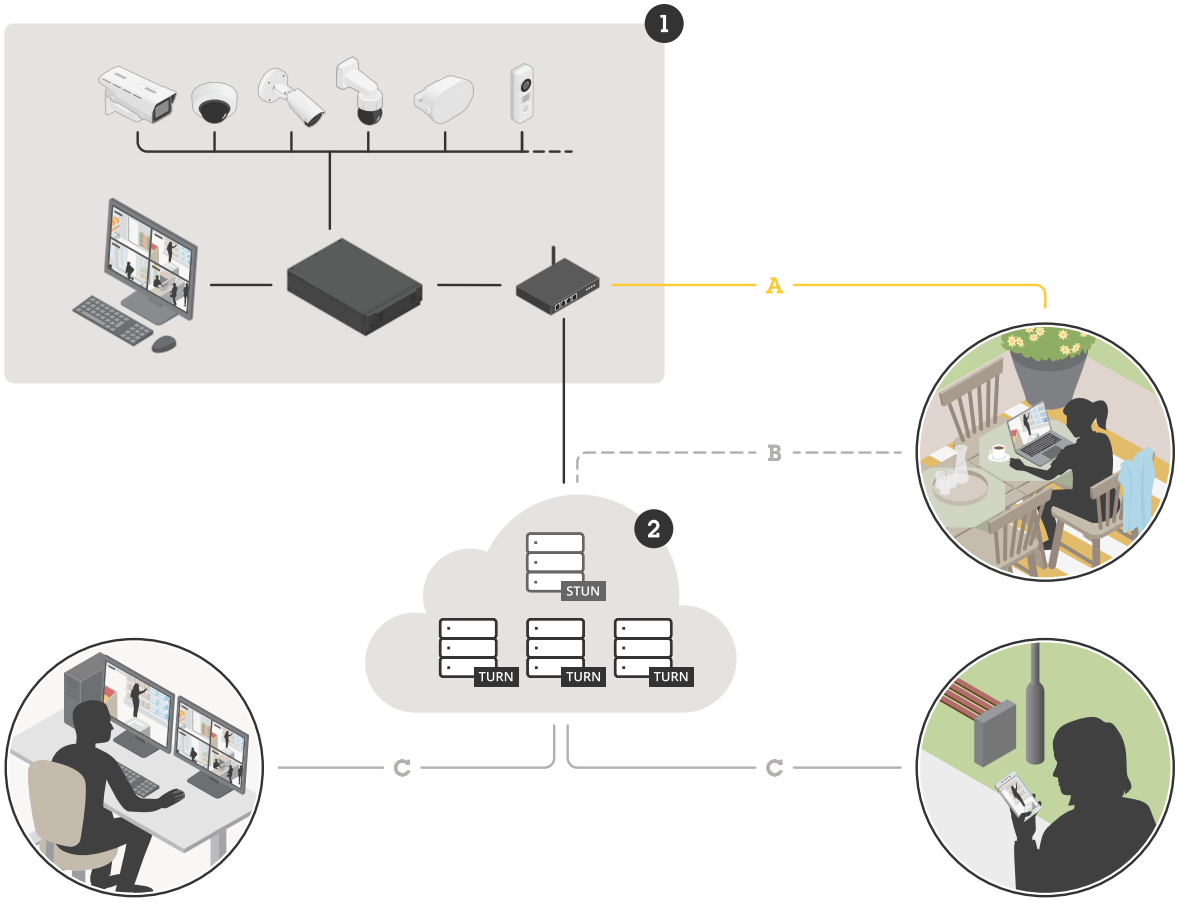


図: AXIS Camera Station ProにおけるSolution overview of Axis Secure Remote Access v2のソリューション概要

1. ローカルネットワーク上の監視対象サイトとローカル閲覧クライアント
   - A – リモート (ピアツーピア) 接続
   - B – Axis Cloud Connected Servicesへの一時的な STUN/TURN接続

名前またはタイプ	アドレス	ポート番号	プロトコル	方向
SRA v2 - My Axis サインイン	eu.login.connect.axis.com	443	TCP	受信および送信
SRA v2 - クラウドサービス通信	eu.cs.connect.axis.com	443	TCP	受信および送信
SRA v2 - クラウドサービスAPI通信	api.vms.axis.cloud	443	TCP	受信および送信
アップリンクコンポーネント	acspro.mysystems.axis.com	443	-	受信および送信
EdgeHostコンポーネント	75.2.119.140	443, 8443	-	受信および送信
EdgeHostコンポーネント	99.83.133.42	443, 8443	-	受信および送信
EdgeHostコンポーネント	cep.connect.axis.com	443, 8443	-	受信および送信

2. Axis Cloud Connected Services
   – C – Axis Cloud Connected ServicesへのリモートTURN接続

名前またはタイプ	アドレス	ポート番号	プロトコル	方向
P2Pプロキシおよびコンポーネント通信	wss://signaling.prod.webrtc.connect.axis.com	443	TCP	受信および送信
P2Pプロキシおよびコンポーネント通信	https://*.turn.prod.webrtc.connect.axis.com	443, 3478, 5349, 49152-65535	TCP	受信および送信

コンポーネント用に予約

必須						
コンポーネント	インターフェースでリッスン	番号	プロトコル	方向	通信	説明
Local WebRTC Signaling Server	localhost	29227	WSS	受信	Embeddable Client、WebClientおよびWebRTC StreamerからSignaling Server	オンプレミスのWebRTCコンポーネントの一部。
ローカルWebRTC設定	localhost	29229	HTTPS	受信	ACSクライアント(Webページ)	WebRTC設定Webページとバックエンドをホストするために使用されます。オンプレミスのWebRTCコンポーネントの一部。
ローカルTURNサーバー	すべて(0.0.0.0/INADDR_ANY)	29230	UDP	受信および送信	Embeddable Client/WebClientからTURNサーバー	ACSオンプレミスの「シングルポートWebRTC」に使用されます。
ローカルIAM (IDP)	0.0.0.0	29232	HTTPS	受信	リバースプロキシーとローカルIAM、ACS Windowsクライアントとローカル IAM	IDP_OIDCパブリックポート。

ローカル IAM (IDP)	0.0.0.0	29233	HTTPS	受信	サードパーティサービス	mTLS管理者ポート。
ローカル IAM (IDP)	127.0.0.1	29234	HTTPS	受信	サードパーティサービス	トークナイザーポート。
WebRTC	localhost	29235	HTTPS	受信	クラウドコンポーネント	オンボーディング中にWebRTCクラウド接続の設定に使用されます。WebRTCコンポーネントの一部。
サービス API	127.0.0.1	29244	NATS	受信	ACSとコンポーネントの間、およびコンポーネント同士の間、NATS経由。	NATSブローカー.
オプション						
Secure Entry (AC-MSM)	127.0.0.1	29214	HTTPS (WS)	受信	ACSクライアント (Webページ) およびコンポーネント	ACSベースポートを使用して設定可能です。古いインストールではポート8081が使用されていました。
Secure Entry (AC-MSM)	すべて (0.0.0.0/ INADDR_ ANY)	29215	HTTPS (WS)	受信	異なるサイト上の Secure Entryコンポーネント	ACSベースポートを使用して設定可能です。
システムの健全性監視	すべて (0.0.0.0/ INADDR_ ANY)	29216	HTTPS	受信	ACS (Web ページ)、SHMバックエンド (コンポーネント)	System Health Monitoring Webページのホスト、およびマルチシステム設定でのデータ共有に使用されます。
System Health Monitoring	localhost	29217	HTTPS	受信	ACS (Web ページ) およびCloud	クラウドサービスに

Cloud Service / Cloud Service					Serviceのバックエンド (コンポーネント)	使用されます。
スマート検索2	localhost	29218	HTTPS	受信	ACSクライアント (Smart Search Webページタブ) および Smart Searchバックエンド (コンポーネント)	Smart Search APIのホスト、およびクライアントWebページの提供に使用されます。
VMS API	127.0.0.1, ::1	29219	GraphQL	受信	VMS APIおよびGraphQLクライアント	ACSをGraphQL APIとしてクライアントに公開するために使用されます。
Webクライアント	localhost	29223	HTTPS	受信	WebClientからVMS API/組み込み可能クライアントへ	バックエンドはVMS APIの前でプロキシーとして機能します。
埋め込み可能クライアント	localhost	29224	HTTPS	受信	Embeddable ClientからVMS API、WebRTC Streamer、および Signaling Server	バックエンドはVMS APIの前のプロキシーとして機能します。
Webクライアントの設定	localhost	29225	HTTPS	受信	ACSクライアント (Webページ)	Web Client設定Webページとバックエンドのホストに使用されます。
埋め込み可能クライアント設定	localhost	29226	HTTPS	受信	ACSクライアント (Webページ)	Embeddable Client設定Webページとバックエンドのホストに使用されます。
オープンテレメトリ	127.0.0.1	29236	gRPC	受信	サードパーティサービス (ACSおよ	gRPC ポート.

					びその他のコンポーネント)	
オープンテレメトリ	127.0.0.1	29237	HTTPS	受信	サードパーティサービス (ACSおよびその他のコンポーネント)	HTTPポート.
Audio Manager		29238	HTTPS	受信	サードパーティ統合サービスおよびコンポーネント	Webサーバーポート.
Data Insights Dashboard	localhost	29241	HTTPS	受信		受信側Webサーバーポート。
Data Insights Dashboard	0.0.0.0	29242	MQTTS	受信および送信	カメライベントメッセージの受信者。	Mosquittoブローカー.
オープンテレメトリ	127.0.0.1	29245	HTTP	受信	OpenTele-metryコレクターからメトリックを取得するための監視エンドポイント	HTTPポート.
Smart Search 2	localhost	29247	gRPC	受信	VMS APIコアおよびSmart Searchレゾルバー	Smart Searchレゾルバー。
APIゲートウェイ	0.0.0.0	29248	HTTPS	受信	EdgeホストおよびAPI Gateway	エッジホストに使用されるAPI Gatewayのフォールバックポート。
APIゲートウェイ	0.0.0.0	29250	HTTPS	受信	ACSクライアントとAPI Gateway	ポート80および443のHTTPおよびHTTPSトラフィック用のフォールバックポート。+48とは異なります。+48ではコンポーネント証明書を使用し

						ますが、これはサーバー証明書を使用するためです。
システムの健全性監視	127.0.0.1	29251	gRPC	受信	ACSサーバーとその他のコンポーネント(該当する場合)からSHMコレクター	システムの健全性データの生成元が、SHMコレクターにデータを転送するために使用します。
システムの健全性監視	127.0.0.1	29252	HTTPS	受信	ACSサーバーとその他のコンポーネント(該当する場合)からSHMコレクター	システムの健全性データの生成元が、SHMコレクターにデータを転送するために使用されます。
AXIS Body Worn Live Receiver	127.0.0.1	29254	TCP	受信	ACSサーバーからのHTTPSリクエストを受け付けるライブストリームサーバー	ライブストリームサーバー。

その他のポート

必須

ポート	番号	プロトコル	方向	通信	説明
HTTPポート	80	HTTP	送信	ACSサーバーおよびデバイス、およびACSクライアントとACSサーバーからインターネットへ	ライセンスの有効化、ファームウェアのダウンロード、および接続中のサービスに使用されます。
HTTPポート	80	HTTP	受信	ACSクライアントとACSサーバー	ビデオストリームと装置データに使用されます。
HTTPS port (HTTPSポート)：	443	TCP	受信	ACSクライアントとACSサーバー	ビデオストリームと装置データに使用されます。

アップグレードステータスUDPポート	15156	UDP	受信および送信	ACSサーバーおよびACSサービスコントロール	ACS Service Controlはこのポートで待ち受け、ACSサーバーは進行中のアップグレードのステータスをブロードキャストします。
PostgreSQL	29210	TCP	受信および送信	PostgreSQLと負荷	電流を消費する負荷には、Data Insights Dashboard、AXIS Audio Manager Proコンポーネント、AXIS Body Wornコンポーネントが含まれます。

オプション

車載サービス	29253	UDP	受信	GNSS受信機から車載サービスコンポーネントへ	
HTTPポート	80	HTTP	送信	ACSサーバーおよびデバイス、ACSクライアントとACSサーバーからインターネットへ	ライセンスのアクティブ化、ファームウェアのダウンロード、接続中のサービスなどに使用されます。
HTTPポート	80	HTTP	受信	ACSクライアントとACSサーバー	ビデオストリームと装置データに使用されます。

データベース

データベースファイル

コアデータベースファイル

AXIS Camera Station Proは、`C:\ProgramData\AXIS Communications\AXIS Camera Station Server`下にコアデータベースファイルを保存します。

AXIS Camera Stationバージョン5.13より前の場合、データベースファイルは1つのみです。**ACS.FDB**。

AXIS Camera Stationバージョン5.13以降の場合、次の3つのデータベースファイルがあります。

- **ACS.FDB**:このメインデータベースファイルには、装置、ビュー、権限、イベント、ストリームプロファイルなどのシステム設定が含まれています。
- **ACS_LOGS.FDB**:このログデータベースファイルにはログへの参照が含まれています。
- **ACS_RECORDINGS.FDB**:この録画データベースファイルには、メタデータと、[**Configuration > Storage (設定 > ストレージ)**] で指定した場所に保存されている録画へ

の参照が含まれています。AXIS Camera Station Proでは、再生中にタイムラインに録画を表示するためにこのファイルが必要です。

コンポーネントデータベースファイル

SecureEntry.db - AXIS Secure Entryデータベースファイルには、カード所持者の写真を除くすべてのアクセスコントロールデータが含まれています。保存先は`C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry\INTERNAL\main_db`です。

smartSearch.sqlite3 - スマート検索データベースファイルには、カメラの設定と保存された検索フィルターが含まれています。保存先は`C:\ProgramData\Axis Communications\AXIS Smart Search\data`です。

データベースの設定

システムは、毎晩およびアップグレードのたびにデータベースのバックアップを行います。AXIS Camera Station Pro Service Controlで、[**Modify settings (設定を変更)**] を選択し、[**Database (データベース)**] をクリックして、バックアップ設定を変更します。

Backup folder (バックアップフォルダー)	[**Browse (参照)**] をクリックし、データベースのバックアップを保存する場所を選択します。AXIS Camera Station Proサーバーを再起動して、変更を適用します。 バックアップフォルダーのパスが正しくない場合、または AXIS Camera Station Proがネットワーク共有にアクセスできない場合、バックアップは`C:\ProgramData\Axis Communications\AXIS Camera Station Server\backup`に保存されます。
Days to keep backups (バックアップの保存日数)	バックアップを保存する日数を設定します。1から30までの任意の数字を設定できます。デフォルトは14日です。
アップグレードの進捗状況	[**View details (詳細の表示)**] をクリックして、最新のデータベースアップグレードに関する詳細を表示します。この詳細には、AXIS Camera Station Pro Service Controlの最後の再起動以降に発生したイベントが含まれます。

データベースのバックアップ

データベースには、録画やメタデータなどシステムが正常に動作するために必要な情報が格納されています。

重要

- データベースには録画は保存されません。**[Configuration (設定)]** > **[Storage (ストレージ)]**で保存先を指定し、録画データを個別にバックアップしてください。
- AXIS Camera Station Pro Service Controlのサーバー設定とデータベース設定は保存されません。

システムバックアップ

システムは [**Database (データベース)**] タブで指定されたフォルダーにシステムバックアップを自動的に保存します。*データベースの設定, on page 233*を参照してください。システムバックアップには、コアデータベースファイルとコンポーネントデータベースファイルの両方が含まれます。*データベースファイル, on page 232*を参照してください。

バックアップファイル	
System_YYYY-MM-DD-HH-mm-SSSS.zip	バックアップは夜間にトリガーされます。
PreUpgrade_YYYY-MM-DD-HH-mm-SSSS.zip	バックアップはデータベース更新の前にトリガーされます。
User_YYYY-MM-DD-HH-mm-SSSS.zip	バックアップはストレージが取り外される前にトリガーされます。

zipファイルには、以下のファイルがあります。

ACS	このフォルダーには、コアデータベースファイルであるACS.FDB、ACS_LOGS.FDB、ACS_RECORDINGS.FDBが含まれています。
コンポーネント	このフォルダーは、AXIS Camera Station Secure Entry やスマート検索などのコンポーネントを使用している場合のみ利用可能です。 • webrtc: このフォルダーにはWebRTC設定ファイルが含まれています。 • ACMSM:このフォルダーには、AXIS Camera Station Secure Entryデータベースファイルである SecureEntry.dbやカード所持者の写真が含まれています。 • smartsearch: このフォルダーには、スマート検索データベースファイル smartSearch-backup-yyyyMMddHHmmssfff.sqlite3が含まれています。
backup_summary.json	このファイルには、バックアップに関する詳細情報が含まれています。
_cluster_yyyyMMddHHmmssfff.dbcbackup	このファイルには、ロールやテーブルスペースなどのクラスタ全体のデータを含む、PostgreSQLデータベースクラスタの論理バックアップが含まれています。

メンテナンスバックアップ

[Database (データベース)] タブで、メンテナンスバックアップを保存するバックアップフォルダーを指定します。*データベースの設定, on page 233*を参照してください。メンテナンスバックアップには、コアデータベースファイルが含まれ、各データベースファイルは個別のフォルダーPreMaintenance_YYYY-MM-DD-HH-mm-SSSSに格納されます。

異なる方法でトリガーできます。

- AXIS Camera Station Proを更新すると自動的に。
- AXIS Camera Station Proサービスコントロールから**データベースメンテナー**を手動で実行する。*データベースのメンテナンス, on page 236*を参照してください。
- Windowsタスクスケジューラーで設定された、スケジュールされたデータベースメンテナンスタスクによって自動的に。*ツール, on page 238*を参照してください。

手動バックアップ

注
手動バックアップでは、コアデータベースファイルのみをバックアップできます。スマート検索データベースファイルなど、コンポーネントデータベースファイルはバックアップされません。

手動バックアップには以下の2つの方法があります。

- **オプション1:** `C:\ProgramData\AXIS Communications\AXIS Camera Station Server`に移動し、データベースファイルのコピーを作成します。次に、以下の手順に従って、PostgreSQLデータベースクラスタをバックアップします。
  1. バックアップを保存するディレクトリで、管理者としてターミナルを開きます。
  2. `"C:\Program Files\Axis Communications\AXIS Camera Station\Core\DbConsole\DbConsole.exe" backup -cluster` を実行します。
  3. バックアップは、ターミナルを開いたディレクトリ内の**yyyyMMddHHmmssfff**フォルダに保存されます。
- **オプション2:** システムレポートを生成し、**[Include all databases (すべてのデータベースを含める)]** を選択して、データベースのバックアップファイルを含めます。*システムレポート, on page 218*を参照してください。

データベースの復元

ハードウェア障害などの問題によってデータベースが失われた場合は、保存済みのバックアップのいずれかからデータベースをリストアできます。デフォルトでは、バックアップファイルは14日間保存されます。データベースのバックアップの詳細については、*データベースのバックアップ, on page 233*を参照してください。

注
データベースには録画は保存されません。**[Configuration (設定)] > [Storage (ストレージ)]**で保存先を指定し、録画を個別にバックアップしてください。

データベースを復元するには:

1. AXIS Camera Station Pro Service Controlに移動し、**[Stop (停止)]** をクリックしてサービスを停止します。
2. データベースバックアップファイルに移動します。*データベースのバックアップ, on page 233*を参照してください。
3. ファイルを抽出します。
4. 以下の手順に従って、PostgreSQLデータベースクラスタをリストアします。
   4.1. 解凍したフォルダで管理者としてターミナルを開きます。
   4.2. `"C:\Program Files\Axis Communications\AXIS Camera Station\Core\DbConsole\DbConsole.exe" restore -backup-file _cluster_yyyyMMddHHmmssfff.dbcbackup`を実行します。
   4.3. バックアップファイルのソースの信頼性の確認を求められたら、**y** をクリックします。
5. 解凍したフォルダーで、**ACS**の以下のデータベースファイルを `C:\ProgramData\AXIS Communications\AXIS Camera Station Server\` に保存します。
   - **ACS.FDB** - データベースを復元するには、このファイルをコピーする必要があります。
   - **ACS_LOGS.FDB** - ログを復元する場合は、このファイルをコピーしてください。
   - **ACS_RECORDINGS.FDB** - 録画を復元する場合は、このファイルをコピーしてください。

6. AXIS Camera Station Secure Entryを使用する場合は、C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry 2\INTERNAL\main_dbにあるRESTORE_INSTRUCTIONS.txtの手順に従ってください。
7. スマート検索を使用する場合は、smartsearchのsmartSearch-backup-yyyyMMddHHmmssfff.sqlite3をC:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Smart Search\dataにコピーし、smartSearch.sqlite3に名前を変更します。
8. VMSウェブクライアントを使用する場合は、webrtcのすべてのファイルをC:\ProgramData\Axis Communications\AXIS Camera Station\Components\WebRTCにコピーしてください。
9. AXIS Camera Station ProService Controlに戻り、[**Start (開始)**] をクリックしてサービスを開始します。

データベースのメンテナンス

「Database maintenance is required」というアラームが表示された場合、または停電後などシステムが予期せずシャットダウンした場合は、データベースのメンテナンスを実行してください。

データベースのメンテナンスを開始するには、*ツール, on page 238*を参照してください。

注

AXIS Camera Station Secure Entryは、DB Janitorを使用してデータベースファイルを監視し、必要に応じて縮小します。強制的な縮小が発生すると、アクセスコントロールシステムは一時的に利用できなくなります。

データベースに関するベストプラクティス

問題を回避するには、以下に注意してください。

ディスクエラーのチェック - ディスクエラーが原因で、データベースが破損するおそれがあります。chkdsk (Check disk、別名Error checking) などのツールを利用して、データベースに使用されているハードドライブで破損したセクターを探します。chkdskは定期的に実行してください。

ウイルス対策ソフトウェアと外部バックアップ - 一部のウイルス対策ソフトウェアはデータベースを破損する可能性があるため、データベースでウイルススキャンを実行しないでください。外部バックアップシステムを使用する場合は、アクティブなデータベースをバックアップしないでください。代わりに、バックアップフォルダー内のファイルからバックアップを作成してください。

停電 - 停電などのため予期しないシャットダウンが発生すると、データベースが破損するおそれがあります。重要なシステムでは、UPS (無停電電源装置) を使用してください。

空き容量の不足 - ハードドライブの空き容量が不足すると、データベースが破損する場合があります。この問題を回避するには、十分なメモリーを搭載したコンピューターに AXIS Camera Station Proサーバーをインストールします。ハードウェア要件については、*axis.com/products/axis-camera-station/hardware-guidelines*を参照してください。

RAMメモリーの破損 - 定期的にWindowsのメモリ診断を実行してRAMのエラーがないか確認してください。

証明書

[Certificates (証明書)] タブで、AXIS Camera Station Proのサーバー証明書を管理できます。現在のサーバー証明書に関する情報を表示したり、有効期限を確認したり、新しいサーバー証明書を生成してインポートしたり、現在のサーバー証明書をエクスポートしたりできます。サーバー証明書はC:\ProgramData\Axis Communications\AXIS Camera Station Server\certsに保存されます。

サーバー証明書

生成	新しい自己署名サーバー証明書を作成します。これにより、サーバーで使用されていた以前の証明書が置き換えられ、有効にするにはサーバーの再起動が必要になります。
インポート...	サーバー証明書をファイルからインポートします。サポートされているファイル形式はPEMとPFX/PKCS12です。2048ビット以上のRSA鍵のみサポートされています。

注

PEM 形式の中間証明書を含む証明書をインポートする場合、すべての中間証明書が .cer ファイルに含まれている必要があります。独自の証明書を作成する場合は、*インポート用の中間証明書を準備する, on page 237*を参照してください。

現在の証明書

現在のサーバー証明書に関する情報を表示します。これを使用して、クライアントが正しいサーバーに接続していることを手動で確認してます。

表示	サーバー証明書の詳細を表示します。
エクスポート...	サーバー証明書をPFXファイルとしてエクスポートします。

新規サーバー証明書の生成

- Windows キー + S を押して、AXIS Camera Station Pro サービス コントロールを検索して開きます。
- **証明書**タブで、**生成** をクリックし、新規サーバー証明書を生成します。
- サーバーを再起動して、新規サーバー証明書を適用します。

インポート用の中間証明書を準備する

中間証明書を含む証明書をAXIS Camera Station Proにインポートするには、サーバー証明書と中間証明書を 1 つのファイルに結合します。

1. サーバー証明書の 1 つと中間証明書をノートパッドで開きます。内容は以下のように構成されています：
   ```
   cert.cer
   ——BEGIN CERTIFICATE——
   MIIFTDCCB....
   ——END CERTIFICATE——
   ```
2. 1つの証明書の内容を別の証明書にコピーして貼り付け、最初の行をcombined_cert.cerに変更します。
   ```
   combined_cert.cer
   ——BEGIN CERTIFICATE——
   MIIFTDCCB....
   ——END CERTIFICATE——
   ——BEGIN CERTIFICATE——
   MIIE+zCCA+OgA.....
   ——END CERTIFICATE——
   ```
3. ファイルを保存します。

ツール

AXIS Camera Station Proサービスコントロールで、**[Modify settings (設定の変更)]** を選択し、**[Tools (ツール)]** をクリックして、データベースのメンテナンスを実行したり、部分的なシステムレポートを作成したり、ネットワークログを有効にしたり、認証局をリセットしたりします。

データベースメンテナンス

データベースメンテナーを実行する:

1. AXIS Camera Station Pro Service Controlを開きます。
2. [**Tools (ツール)**] をクリックします。
3. [**Database maintainer (データベースメンテナンス)**] で、[**Run (実行)**] をクリックします。
4. 推定ダウンタイムが表示されます。続行するには、[**はい**] をクリックします。このプロセスを開始すると、キャンセルすることはできません。

注

- メンテナンス中は、AXIS Camera Station Proサーバーと進行中のすべての録画が停止します。メンテナンスが終わると、サーバーが自動的に起動します。
- メンテナンス中はコンピューターの電源を切らないでください。
- データベースのメンテナンスを実行するには、Windowsコンピューターの管理者権限が必要です。
- データベースのメンテナンスを実行してもデータベースを回復できない場合は、Axisの技術サポートにご連絡ください。

「Database maintenance is required (データベースのメンテナンスが必要です)」というアラームが表示された場合、または停電後などシステムが予期せずシャットダウンした場合は、必ずデータベースのメンテナンスを実行してください。

また、Windowsタスクスケジューラの AXIS Camera Station Proデータベースメンテナンスタスクをオンにすると、データベースメンテナンスを自動で実行するようスケジュールを設定することもできます。トリガーを編集して、データベースメンテナンスを実行するタイミングと頻度をカスタマイズできます。

ネットワークのログ作成

ネットワークロギングを開始する:

1. AXIS Camera Station Pro Service Controlを開きます。
2. [**Tools (ツール)**] をクリックします。
3. [**Network logging (ネットワークロギング)**] をクリックし、ネットワークプロトコルアナライザーアプリケーションをダウンロードします。
4. インストールが完了したら、[**Start (開始)**] をクリックしてアプリケーションを起動します。

部分的システムレポート

部分的システムレポートは、ご使用のシステムをAxisのカスタマーサポートが分析するときに役立つ、各種パラメーターやログファイルが含まれる.zipファイルです。カスタマーサポートにお問い合わせの際は、必ずシステムレポートを作成しておいてください。

完全なシステムレポートを生成するには、*システムレポート, on page 218*を参照してください。

部分的システムレポートを生成するには:

1. AXIS Camera Station Proサービスコントロールを開きます。
2. [**Tools (ツール)**] をクリックします。

3. [Partial system report (部分システムレポート)]で、[Run (実行)] をクリックします。
4. ダイアログで求められた情報を選択し、入力します。
5. [レポートを生成する] をクリックします。

認証局をリセットする

[Reset (リセット)]をクリックすると、新しい認証局が生成され、サービスが再起動されます。

- サービスが再起動すると、ログインできるようになり、必要に応じてカスタムの認証局をインポートできます。

トラブルシューティング

本ガイドについて

このガイドは、AXIS Camera Station Proに関連する問題とトラブルシューティング方法をまとめたものです。見つけやすくするために問題はトピック別に分類されています。トピックには、音声やライブビューなどがあります。各問題には、推奨される解決策が記載されています。

ハードウェア要件、ソフトウェアのアップグレード、チュートリアルなど、その他のリソースについては、*axis.com/support* をご覧ください。

一般的な問題が発生した場合は、さらにトラブルシューティングを進める前に、AXIS Camera Station Proサーバーサービスを再起動してみてください。

1. [Configuration (設定)] > [Server (サーバー)] > [Diagnostics (診断)] に移動します。
2. [Restart AXIS Camera Station server service...(AXIS Camera Stationサーバーサービスの再起動)] をクリックします。

注

サーバーサービスの再起動にはしばらく時間がかかる場合があります。再起動をキャンセルする方法はありません。再起動中は、サーバーは利用できず、接続されたすべてのデバイスの接続が切断されます。

AXIS Camera Station Proサービス

サーバーが頻繁に再起動する

サーバーに過負荷がかかっている可能性があります。過負荷になると、タスクキューが長くなり、データベースが破損することもあります。

- AXIS Camera Station Proまたはその他のアプリケーションが、大量のリソースを使用していないか確認してください。
- データベースメンテナーを実行してください。*データベースのメンテナンス, on page 236*を参照してください。

上記のいずれでも問題が解決しない場合は、Axis Supportに連絡してください。*報告手順, on page 257* に移動します。

ビデオ管理システムの装置

一般的な問題

VMSがカメラと通信できないため、表示されているカメラが追加されなかった	1. カメラがネットワークに接続されており、電源が供給されており、カメラが動作していることを確認してください。 2. [Configuration > Add devices (設定 > デバイスの追加)] を選択して、もう一度カメラを追加してください。
ユーザーがインストールをキャンセルしたため、表示されているカメラが追加されなかった	カメラを追加するには、**[設定] - [デバイスの追加]** を選択します。
一覧表示されたカメラに、パスワードを設定できませんでした。	1. パスワードを手動で設定するには、**[Configuration (設定)] > [Devices (デバイス)] > [Management (管理)]** に移動します。 2. カメラを右クリックし、[User Management > Set password (ユーザー管理 > パスワードを設定)] を選択します。

装置を追加できない

デバイスは AXIS Camera Station Proに追加される前に別のシステムで使用されていました。	• デバイスを工場出荷時の設定にリセットしてください。 • AXIS Device Managerにデバイスを追加してみてください。
追加したイデバイスではなく、別のデバイスが追加される	互換性の問題がある可能性があります。最新のAXIS Camera Station Proバージョンを使用してください。
別のデバイスモデルを追加できない	*axis.com/support/troubleshooting*でカメラのトラブルシューティングを実施してください。

AXIS Camera Station Proからデバイスのファームウェアをアップグレードできない

カメラのファームウェアをwebインターフェースからアップグレードできない	*axis.com/support/troubleshooting*でカメラのトラブルシューティングを実施してください。
すべてのデバイスでファームウェアのアップグレードができない	• ネットワーク接続されていることを確認してください。 • ネットワーク関連の問題でない場合は、AXISサポートに連絡してください。*報告手順, on page 257* に移動します。
特定のモデルでファームウェアがアップグレードできない。	互換性の問題がある可能性があります。Axisサポートに問い合わせる. *報告手順, on page 257* に移動します。

デバイスが検出されない

ビデオ管理システムがネットワークで接続されたカメラとビデオエンコーダを自動的に検索しましたが見つかりません。

- カメラがネットワークに接続されており、電源が供給されていることを確認します。
- クライアント、サーバー、またはカメラが別のネットワーク上にある場合は、プロキシとファイアウォールの設定を行います。
  - クライアントとサーバーの間にプロキシサーバーがある場合は、クライアントのプロキシ設定を変更します。
  - クライアントとサーバーの間にNATやセキュリティシステムがある場合は、NATやセキュリティシステムを変更します。AXIS Camera Station Service Controlで指定されたHTTPポート、TCP(通信制御プロトコル) ポート、ストリーミングポートがセキュリティシステムまたはNATを通過できるように許可します。完全なポートリストを表示するには、*AXIS Camera Station Proのポートリスト, on page 223*を参照してください。
- カメラを手動で追加します。*デバイスの追加, on page 6*を参照してください。

「15秒後にカメラに再接続」メッセージの頻発

考えられる問題:

- ネットワークの過負荷。
- カメラにアクセス不可能です。カメラがネットワークに接続されていることを確認してください。
- グラフィックカードに問題があります。

グラフィックカードの問題の考えられる対処法:

- 最新のグラフィックカードドライバーをインストールします。
- より大容量のビデオメモリーを搭載した高性能なグラフィックカードにアップグレードします。
- ビデオレンダリングにCPUを使用します。[Hardware decoding (ハードウェアデコーディング)] の [Graphics card (グラフィックカード)] でそれを選択します。この設定は、[Configuration (設定)] > [Client (クライアント)] > [Streaming (ストリーミング)]で確認できます。
- ビデオと音声の設定を調整します。たとえば、低帯域幅の場合のプロファイル設定を最適化します。

録画

一般的な問題

連続録画がオンになっていない	1. 連続録画をオンにするには、[Configuration > Recording and events > Recording method (設定 > 録画とイベント > 録画方法)] に移動します。 2. カメラを選択し、[Continuous (連続)] をオンにします。
指定したドライブで録画できない	1. 別のストレージを使用するには、**[設定] - [ストレージ] - [管理]** を選択します。 2. ストレージを追加し、カメラのストレージ設定を行います。
AXIS Video Content Streamアプリケーションをインストールできない	1. アプリがを手動でインストールするには、[Configuration > Devices > Management (設定 > デバイス > 管理)] に移動します。 2. カメラを選択し、 をクリックします。

録画が開始されない

録画が開始されない場合、または録画が数秒後に停止する場合は、ディスクの容量がいっぱいになっているか、データの混入が多すぎる可能性があります。

- サーバーの設定シートの [Recording Storage (録画ストレージ)] で、空き容量があり、データの混入がないことを確認してください。
- ビデオ管理システムのストレージの上限を増やします。
- ストレージプールにさらにストレージを割り当てます。*ストレージの設定, on page 79*を参照してください。

連続録画中の録画抜け

録画抜けが発生すると、**[Recording errors (録画エラー)]** と表示されたアラームがトリガーされます。以下のような原因でギャップが発生することがあります。

- サーバーの過負荷
- ネットワークの問題
- カメラの過負荷
- ディスクの過負荷

すべてのカメラで録画抜けが発生しているかどうかを確認してください。すべてのカメラで発生していない場合は、カメラの過負荷を示している可能性があります。以下の質問を使用して原因を特定してください。

- 録画抜けが発生する頻度は？毎時か毎日か?
- 録画抜けの時間は？数秒か数時間か?
- 録画抜けは、何時に発生するか?

考えられる対処法:

- サーバーのタスクマネージャーで、通常よりも多く使用されているハードウェアリソースがないか確認してください。ディスクに過剰使用の兆候がある場合は、ディスクを追加し、いくつかのカメラの録画先を新しいディスクにしてください。
- ディスクへの書き込みデータ量を減らしてください (ビデオ設定、Zipstream、フレームレート、解像度)。AXIS Site Designerにより推定されるスループットを考慮してください。*axis.com/support/tools/axis-site-designer*を参照してください。

詳細については、*ライブビューと再生のパフォーマンス, on page 245*を参照してください。

エクスポートした録画を再生できない

Windows Media Playerでエクスポートした録画が再生されない場合は、ファイル形式を確認してください。エクスポートした録画を再生するには、Windows Media Player (.asf) またはAXIS File Player (.asf、.mp4、.mkv) を使用します。

詳細については、*AXIS File Playerでの録画の再生と検証, on page 7*を参照してください。

注

AXIS File Playerは、プレーヤーと同じフォルダーにあるすべての録画を自動的に開きます。

録画が消える

システムは指定した日数のみ録画を保存します。保管期間を変更するには、**[設定] - [ストレージ] - [選択]** に移動します。

ストレージの容量がいっぱいになると、保存期間が終了する前に、システムが録画を削除する場合があります。ストレージがいっぱいになるのを避けるために、以下の方法を試してください。

- ストレージを追加します。**[設定] - [ストレージ] - [管理]** を選択します。
- AXIS Camera Station Proに割り当てられたストレージ容量を変更します。**[設定] - [ストレージ] - [管理]** を選択します。
- 解像度やフレームレートなどを変更して、録画ファイルのサイズを小さくしてください。**[Configuration (設定)] > [Devices (デバイス)] > [Stream profiles (ストリームプロファイル)]** に移動します。
  - 録画にH.264ビデオ形式を使用します。M-JPEG形式を使用すると、必要なストレージ容量が大幅に増えます。
  - Zipstreamを使用して、録画のサイズをさらに小さくします。

フェイルオーバーによる録画の問題

カメラとサーバー間に、録画の転送に必要な十分な帯域幅がない。	帯域幅を増やしてください。
切断中にカメラがSDカードに録画しなかった。	• カメラのサーバーレポートを確認してください。*axis.com/support/troubleshooting*にアクセスしてください。 • SDカードが動作し、録画があることを確認してください。
接続が切れた後、カメラの時刻が変更された。	• 今後の録画のために、NTPを設定してください。 • カメラの時刻をサーバーと同期させるか、カメラにサーバーと同じNTPサーバーを使用してください。

注

コントロールされたサーバーシャットダウン中、または10秒未満の接続中断時は、フェイルオーバーによる録画は機能しません。

ライブビュー

ライブビューと再生のパフォーマンス

このセクションでは、AXIS Camera Station Proクライアントでフレームの欠落やグラフィックの問題が発生した場合に考えられる解決策について説明します。

クライアントハードウェア	
グラフィックカードまたはネットワークアダプターのドライバーが最新であることを確認します。	1. DirectX診断ツールを開きます (コンピューターで「dxdiag」を検索します)。 2. メーカーのWebサイトで、お使いのOSに対してドライバーが最新かどうかを確認します。 3. クライアントとサーバーが同じマシン上で実行されていることを確認します。 4. 専用コンピューター上で、クライアントを実行してみます。
モニターの数を確認する	1つのグラフィックカードにつき、モニターは2台までとすることをお勧めします。 注 仮想マシン上でのクライアントの実行はサポートされていません。
グラフィックカードが**[Configuration (設定)] > [Devices (デバイス)] > [Stream Profiles (ストリームプロファイル)]**で設定されたエンコード形式に対応していない	• グラフィックカードがストリームのエンコード形式に対応tしていることを確認してください。 • 別のエンコード形式を試してみてください。 • 対応しているエンコード形式が複数のカメラで期待通りに動作しない場合は、グラフィックカードのドライバーが最新であることを確認してください。

接続中のデバイス	
同時に多数のクライアントが接続されています。	一般的な使用事例に基づいて、システムが要件を満たし、ハードウェアガイドラインに従っていることを確認します。*「AXIS Camera Station Pro - インストールと移行ガイド」の「サーバー要件」*を参照してください。
カメラが AXIS Camera Station Pro以外のビデオ管理システムに接続されている	カメラを他のクライアントから切断し、AXIS Camera Station Pro に接続する前にカメラをデフォルト設定に戻します。
1台のカメラがさまざまなストリーム、特に高解像度のストリームを使用している	これは、特に一部のM-Lineカメラやマルチセンサーカメラで問題となる可能性があります。 • ストリームを同じストリーミングプロファイル、またはより低い解像度に変更します。*ストリームプロファイル, on page 56*を参照してください。

サーバーの過負荷	
問題の発生と同時に異常なCPUまたはRAMの使用がある	CPUまたはRAMを消費する他のアプリケーションが同時に実行していないことを確認してください。

ネットワークの問題	
問題の発生と同じ時間に異常な帯域幅の使用がある	帯域幅を大量に消費する他のアプリケーションが同時に実行されていないことを確認してください。
十分な帯域幅、リモートまたはローカルネットワーク	• ネットワークトポロジを確認します。 • カメラ、サーバー、クライアント間で使用されているスイッチ、ルーター、ネットワークアダプター、ケーブルなどのネットワーク装置の健全性チェックを行います。

ライブビューでビデオが表示されない

ライブビューで、既知のカメラからのビデオが表示されません。

- ハードウェアデコーディングをオフにします。ハードウェアデコーディングは、デフォルトで **[Auto (自動)]** に設定されています。*ストリーミング, on page 127*のハードウェアデコーディングを参照してください。
- ウイルス対策ソフトウェアがインストールされている場合は、ライブストリームや AXIS Camera Station Proのフォルダーおよびプロセスがブロックされることがあります。*よくある質問*を参照してください。

考えられるその他の対処法:

- webインターフェースでライブビューが表示されない場合、またはwebインターフェースが機能しない場合は、カメラのトラブルシューティングを行ってください。*axis.com/support/troubleshooting*にアクセスしてください。
- カメラサーバーのレポートを作成します。*axis.com/support/troubleshooting*にアクセスしてください。
- ファイアウォールが特定のポートへの接続をブロックしていないことを確認してください。*全般サーバー設定, on page 223*を参照してください。
- サポートされているWindowsサーバーのOSバージョンに対応するDesktop Experienceがインストールされていることを確認してください。*録画エクスポートのスケジュール, on page 137*を参照してください。
- 低解像度のストリームが正しく動作することを確認してください。

上記のいずれでも問題が解決しない場合は、*報告手順, on page 257*にアクセスしてください。

ハードウェアデコーディング性能

ビデオのラグ、カクつき、途切れ、ライブビュー中のCPUの高使用率が発生する場合、または「Reconnecting to camera (カメラに再接続中)」というメッセージが頻繁に表示される場合は、このトラブルシューティングガイドを使用してください。

1. グラフィックカードのドライバーを更新します。ハードウェアアクセラレーションの問題の最も一般的な原因は、ドライバーが古いことです。メーカー (NVIDIA、AMD、または Intel) のWebサイトにアクセスし、お使いのGPUモデルに対応する最新のドライバーをダウンロードします。
2. ハードウェアデコーディングモードを調整します。**[Configuration (設定)] > [Client (クライアント)] > [Streaming (ストリーミング)]** に移動します。
   – モードが **[Automatic (自動)]** または **[On (オン)]** になっており、問題が発生している場合は、**[Off (オフ)]** に設定します。パフォーマンスが向上した場合、現在のスト

リーム負荷に対してGPUの処理能力が不足している可能性があります。手順6を参照してください。

- GPUの処理能力が十分な場合に、モードが **[Off (オフ)]** になっており、CPU使用率が高い場合は、**[Automatic (自動)]** または**[On (オン)]** に設定してみてください。

3. システムリソースを監視します。Windowsのタスクマネージャーを開き (Ctrl + Shift + Esc)、**Performance (パフォーマンス)** タブに移動します。
   - ハードウェアデコーディングが無効な状態でCPU使用率が常に80%を超えている場合、は、ストリームの数や解像度に対してシステムの処理能力が不十分である可能性を示しています。
   - ハードウェアデコーディングを有効にした状態でGPU専用メモリが容量上限近くまで使用されている場合は、GPUがボトルネックになっていることを示しています。
4. 同時に表示されるカメラの数を減らすか、カメラを低解像度のストリームプロファイルに切り替えることで、システムの負荷を軽減できます。
5. カメラがH.264またはAV1形式でストリームされていることを確認します。他のコーデックは、ハードウェアデコーディングを使用しません。
6. GPUの容量を評価します。ハードウェアデコーディングをサポートしているGPUでも、解像度やフレームレートに制限がある場合があります。高解像度のストリーム数が多い設定については、*AXIS Camera Station Proクライアント要件*を確認し、VRAM容量が大きく、デコードの処理能力の高いGPUへのアップグレードを検討してください。
7. 上記のいずれの方法でも解決しない場合は、以下の情報を手元に用意して、*Axisサポート*に問い合わせてください。
   - システムハードウェア (CPU、GPU、RAM)。
   - オペレーティングシステムバージョン。
   - グラフィックスドライバーバージョン。
   - AXIS Camera Station Proバージョン。
   - 具体的な症状と再現手順。

ストレージ

ネットワークストレージにアクセスできない

ローカルシステムアカウントを使用して AXIS Camera Station Pro Service Controlにログインする場合、他のコンピューターの共有フォルダーにリンクしているネットワークストレージを追加することはできません。

以下の手順で、サービスのログオンアカウントを変更してください。

1. Windowsの [**コントロールパネル**] を開きます。
2. 「サービス」を検索します。
3. [**View local services (ローカルサービスを表示)**] をクリックします。
4. AXIS Camera Station Proを右クリックし、[**Properties (プロパティ)**] を選択します。
5. [**Log on (ログオン)**] タブに移動します。
6. [**ローカルシステムアカウント**] から [**このアカウント**] に変更します。
7. Windows Active Directoryへのアクセス権を持つユーザーを選択します。

ネットワークストレージが利用できない

ビデオ管理ソフトウェアを実行するコンピューターとサーバーがネットワークストレージと同じドメインに属していることを確認してください。

新しいユーザー名とパスワードを使用してネットワークストレージに再接続できない

認証が必要なネットワークストレージの場合、ユーザー名とパスワードを変更する前に進行中のすべての接続からネットワークストレージを切断することが重要です。

ネットワークストレージのユーザー名とパスワードを変更して再接続する手順は、以下のとおりです。

1. 進行中のすべての接続からネットワークストレージを切断します。
2. ユーザー名とパスワードを変更します。
3. [Configuration > Storage > Management (設定 > ストレージ > 管理)] を選択し、新しいユーザー名とパスワードを使用してネットワークストレージに再接続します。

動体検知

一般的な問題

AXIS Video Motion Detection アプリケーションをインストールできない	アプリがを手動でインストールするには、*カメラアプリケーションをインストールする, on page 73*を参照してください。
現在の動体検知を取得できない	カメラを工場出荷時の設定にリセットする: 1. **[設定] - [デバイス] - [管理]** を選択します。 2. 問題のあるカメラを右クリックし、**Restore the camera to factory settings (カメラを工場出荷時の設定にリセットする)** をクリックします。 リセット中はカメラを利用できません。IPおよびHTTPSの設定には影響ありません。リセットが完了すると、ステータス列に **[Set password (パスワードを設定)]** と表示されます。**[Set password (パスワードを設定)]** をクリックして、カメラをサーバーに再接続してください。
動体検知が設定されていません	1. 動体検知を手動で設定するには、**[設定] - [録画とイベント] - [録画方法]** を選択します。 2. カメラを選択し、[Motion Settings (動体設定)] をクリックして動体検知を設定します。
動体検知がオンになっていない	1. **[設定] - [録画とイベント] - [録画方法]** を選択します。 2. カメラを選択し、[Motion detection (動作検知)] をオンにして動体検知をオンにします。

動体検知によって検知される動く物体が多すぎるか少なすぎる

このセクションでは、Video Motion Detectionに関連する録画で検知数が多いまたは少ない場合に考えられる解決策について説明します。

動体設定の調整

動きの設定を選択して、動く物体を検知する範囲を調整できます。

1. **[設定] - [録画とイベント] - [録画方法]** を選択します。
2. カメラを選択して [**動体設定**] をクリックします。
3. カメラのファームウェアに合わせて設定を選択します。

AXIS Video Motion Detection 2および4	対象範囲を設定できます。*AXIS Video Motion Detection 2および4の編集, on page 92*を参照してください。
カメラ内蔵の動体検知機能	対象範囲と除外範囲を設定できます。*内蔵動体検知機能の編集, on page 93*を参照してください。

トリガー時間の調整

トリガー時間とは、連続する2つのトリガーの時間間隔です。この設定を使用して、連続する録画の回数を減らします。この時間に追加のトリガーが発生した場合、録画は続行され、トリガー時間が新たに開始します。

トリガー時間を変更するには:

1. **[設定] - [録画とイベント] - [録画方法]** を選択します。
2. カメラを選択します。
3. [**Advanced (詳細設定)**] で、[**Trigger period (トリガー期間)**] を秒単位で調整します。

アクションルール

予期せぬI/Oトリガーイベント

午前1:15頃に予期せぬ入力/出力イベントが発生する場合は、既存のI/Oトリガーをデバイスイベントトリガーに置き換えてください。

音声

ライブビューで音声が聞こえない

ライブビューで音声が聞こえない場合は、以下の手順に従ってください。

- カメラが音声対応であることを確認します。
- コンピューターにサウンドカードが装着されていて、使用可能になっていることを確認します。
- 使用中のプロファイルが音声用に設定されていることを確認します。
- ユーザーが音声に対するアクセス権があることを確認します。

音声対応プロファイルを設定する

1. [**Configuration (設定)**] > [**Devices (デバイス)**] > [**Stream profiles (ストリームプロファイル)**] に移動します。
2. カメラを選択します。
3. ビデオプロファイル設定の [**Format (形式)**] で [**MPEG-4**] または [**H.264**] を選択します。
4. [**Audio (音声)**] で、[**Microphone (マイク)**] のドロップダウンメニューからマイクを選択します。
5. [**Use microphone for (マイクの使用目的)**] のドロップダウンメニューで、音声をいつ使用するかを選択します。

6. 必要に応じて、[Speaker (スピーカー)] のドロップダウンメニューでスピーカーを選択します。
7. [OK]をクリックします。

ユーザーのアクセス権を確認および変更する

注
以下の設定の確認は、AXIS Camera Station Proで設定した管理者権限を持つユーザーがログオンして行ってください。

1. [Configuration > Security > User permissions (設定 > セキュリティ > ユーザー権限)] に移動します。
2. ユーザーまたはグループを選択します。
3. 特定の装置に対して [Audio listen (音声を聞く)] または [Audio speak (音声を話す)] を選択します。
4. [適用] をクリックします。

シーケンスで音声が聞こえない

ストリームプロファイルで音声をオンまたはオフにできます。詳細については、*ストリームプロファイル, on page 56*を参照してください。

再生中に音声が聞こえない

録画用のプロファイルで音声をオンにしていない場合、音声は録音されません。

注
M-JPEGビデオでは音声は使用できません。別のビデオフォーマットを選択してください。

録画で音声を使用にするには:

1. [Configuration > Devices > Stream profiles (設定 > デバイス > ストリームプロファイル)] に移動して、使用するビデオプロファイルのビデオ形式を設定します。
2. **[設定] - [録画とイベント] - [録画方法]** を選択します。
3. カメラを選択します。
4. [Profile (プロファイル)] ドロップダウンメニューから設定したプロファイルを選択します。
5. [適用] をクリックします。

ルールトリガー録画

既存のルールで音声を有効にするには:

1. **[設定] - [録画とイベント] - [アクションルール]** を選択します。
2. ルールを選択し、[編集] をクリックします。
3. [Next (次へ)] をクリックして [Actions (アクション)] に進みます。
4. [Record (録画)] アクションを選択し、[Edit (編集)] をクリックします。
5. 音声を使用するプロファイルを選択します。
6. [完了] をクリックして設定を保存します。

ログイン

サーバーにログインまたは接続できない

このセクションでは、単一サーバーへの接続時に発生するログインおよび接続の問題について説明します。複数のサーバーにログインしている場合は、クライアントが起動してステータスバーに接続状態を表示します。接続ステータスの詳細については、*接続ステータス, on page 139*を参照してください。

ユーザー名またはパスワードが正しくありません	• 正しく入力しているか、別のアカウントのユーザー名とパスワードを使用していないかを確認してください。 • ユーザーに AXIS Camera Station Proサーバーへのアクセス権があることを確認します。 • AXIS Camera Station Proサーバーとクライアントのクロックを同期する必要があります。ドメインユーザーの場合、ドメインサーバーのクロックをサーバーおよびクライアントと同期する必要があります。 • サーバーには追加されていないけれどもローカル管理者グループのメンバーであるユーザーは、管理者としてクライアントを実行する必要があります。 • ユーザーのアクセス権の詳細については、*ユーザー権限, on page 143*を参照してください。
ユーザーにサーバーにログインする権限がありません	**[User permissions (ユーザー権限)]** ダイアログでユーザーを追加します。
メッセージのセキュリティを確認できません	サーバーとクライアントのUTC時刻は適切に同期されている必要があります。クライアントとサーバーの時刻の差が3時間以内になるよう、調整してください。
サーバーコンピューターに接続できません	• サーバーコンピューターがネットワークに接続されていることを確認します。 • サーバーコンピューターが動作しているかを確認してください。 • ファイアウォールが適切に設定されているかを確認してください。 • サーバーアドレスが正しく入力されているかを確認してください。 • クライアントのプロキシ設定を確認してください。
サーバーから応答がありません。	正しいコンピューターに接続していること、AXIS Camera Station Proサーバーが実行中であることを確認します。
クライアントがサーバーに接続できない	ネットワークが適切に設定されているかを確認してください。 • ご使用のOSがサポートされていることを確認してください。サポートされているOSの完全なリストについては、*リリースノート*を参照してください。 • Service Controlから、AXIS Camera Station Proサーバーが実行中であることを確認するか、必要に応じてサーバーを起動します。 • クライアントとサーバーが同じネットワークに接続されていることを確認してください。そうでない場合、クライアントはサーバーの外部IPアドレスを使用する必要があります。

	• サーバーマシンで、Windowsのインターネットオプションでサーバーのプロキシー設定を行ってください。 • ログインページでクライアントプロキシー設定を行い、[**Change proxy settings (プロキシー設定の変更)**] を選択します。 • クライアントマシンで、Windowsのインターネットオプションでクライアントのプロキシー設定を行ってください。
サーバーに接続できません	• AXIS Camera Station Pro サーバーのアドレスとポートが正しいことを確認してください。Service Controlで、ポート範囲が正しく設定されていることを確認してください。 • NAT、ファイアウォール、またはウイルス対策ソフトウェアがサーバーへの接続をブロックしていないことを確認してください。詳細については、*Secure Remote Access v2のドメインとポート, on page 226*を参照してください。 • AXIS Camera Station ProService Controlを使用して、サーバーが実行中であることを確認します。 – AXIS Camera Station Proサービスコントロールを開きます。*AXIS Camera Station ProサービスコントロールIを開きます。, on page 221*を参照してください。 – [**General (全般)**] タブでサーバーのステータスを表示します。ステータスが [**Stopped (停止)**] の場合、[**Start (開始)**] をクリックしてサーバーを起動します。
サーバーを検出できません	• サーバーコンピューターがネットワークに接続されていることを確認します。 • AXIS Camera Station Pro サーバーのアドレスとポートが正しいことを確認してください。 • NAT、ファイアウォール、またはウイルス対策ソフトウェアがサーバーへの接続をブロックしていないことを確認してください。 • クライアントのDNS設定が正しいことを確認してください。 • DNSサーバーに、そのサーバーのホスト名とIPアドレスが入力されていることを確認してください。
サーバーに接続できません。	サーバーコンピューターとネットワークが過負荷になっていないことを確認してください。
サーバーとクライアントのバージョンが異なります	サーバーをアップグレードして、クライアントと同じバージョンを実行してください。
ローカルの AXIS Camera Station Proサーバーが実行されていません	サービスコントロールを使用して AXIS Camera Station Proを起動するか、ログインするリモートサーバーを選択してください。

このコンピューターには AXIS Camera Station Proサーバーがインストールされていません	AXIS Camera Station Proサーバーをインストールするか、別のサーバーを選択してください。
選択したサーバーリストは空です	サーバーリストにサーバーを追加するには、サーバーリスト選択の横にある [**Edit (編集)**] をクリックします。

ライセンス

ライセンス登録の問題

自動登録でエラーが発生した場合、以下のように対処してください。

- システムが組織に登録されていることを確認します。
- [**Configuration (設定)**] に移動し、[**Automatic licensing (自動ライセンス)**] がオンになっていることを確認します。*ライセンスを管理, on page 142*を参照してください。
- サーバーの時刻が正しいことを確認します。

詳しくは、*AXIS Camera Station Proのインストールと移行ガイド*を参照してください。

ユーザー

ドメインユーザが見つかりません

ドメインユーザーの検索が失敗する場合は、以下の手順でサービスログオンアカウントを変更してください。

1. Windowsの [**コントロールパネル**] を開きます。
2. 「サービス」を検索します。
3. [**View local services (ローカルサービスを表示)**] をクリックします。
4. AXIS Camera Station Proを右クリックし、[**Properties (プロパティ)**] を選択します。
5. [**Log on (ログオン)**] タブをクリックします。
6. [**ローカルシステムアカウント**] から [**このアカウント**] に変更します。
7. Windows Active Directoryへのアクセス権を持つユーザーを選択します。

証明書エラー

証明書エラーを解決するまで、AXIS Camera Station Proはデバイスと通信できません。

考えられるエラー	
証明書が見つかりません	理由がわかっている場合は、[**Repair (修復)**] をクリックします。不正アクセスの疑いがある場合は、証明書をリストアする前に問題を調査してください。[**Advanced (詳細設定)**] をクリックすると、証明書の詳細情報が表示されます。証明書を削除する理由として考えられること: • デバイスが工場出荷時の状態にリセットされた。 • 安全なHTTPS通信が無効になった。 • 権限のない第三者が装置に不正アクセスし、変更を行った。
信頼できない証明書	理由がわかっている場合は、[**Trust This Device (このデバイスを信頼する)**] をクリックします。わかっていない場合は、証明書を信頼する前に問題を調査してください。[**Advanced (詳細設定)**] をクリックすると、証明書の詳細情報が表示されます。

認証局のパスワードがない

パスワードが保存されていない認証局が AXIS Camera Station Proにある場合は、以下のアラームが表示されます。

認証局の認証には、パスワードの入力が必要です。Read the user manual for more information. (詳細については、ユーザーマニュアルをお読みください。)

この問題は、次の3つの方法で解決できます。

- 装置でHTTPSをオンにする
- 既存の認証局をインポートする
- 新しい認証局を生成する

装置でHTTPSをオンにするには:

1. **[設定] - [デバイス] - [管理]** を選択します。
2. リスト内でデバイスを右クリックし、**[Security (セキュリティ)] > [HTTPS] > [Enable/Update (有効化/更新)]** を選択します。
3. **[はい]** をクリックして確認します。
4. 認証局のパスワードを入力します。
5. **[OK]**をクリックします。

既存の認証局をインポートするには:

1. **[Configuration (設定)] > [Security (セキュリティ)] > [Certificates (証明書)>] > [Devices (デバイス)]** に移動します。
2. HTTPSで、**[Validate device certificate (デバイス証明書を検証する)]** をオフにします。
3. [**Certificate authority (認証局)**] で、[**Import (インポート)**] をクリックします。
4. パスワードを入力し、[**OK**] をクリックします。
5. 署名入りのクライアント/サーバー証明書の有効日数を選択します。
6. **[設定] - [デバイス] - [管理]** を選択します。

7. 装置を右クリックし、[Security (セキュリティ)] > [HTTPS] > [Enable/Update (有効にする/更新する)] を選択します。
8. [Configuration (設定)] > [Security (セキュリティ)] > [Certificates (証明書)] > [Devices (デバイス)] に移動し、[Validate device certificate (デバイス証明書を検証する)] をオンにします。

注

AXIS Camera Station Proはデバイスから切断され、一部のシステムコンポーネントが再起動します。

AXIS Camera Station Proで新しい認証局が生成されるようにするには:

1. [Configuration (設定)] > [Security (セキュリティ)] > [Certificates (証明書)>] > [Devices (デバイス)] に移動します。
2. HTTPSで、[Validate device certificate (デバイス証明書を検証する)] をオフにします。
3. [Certificate authority (認証局)] で、[Generate (生成)] をクリックします。
4. パスワードを入力し、[OK] をクリックします。
5. 署名入りのクライアント/サーバー証明書の有効日数を選択します。
6. [設定] - [デバイス] - [管理] を選択します。
7. 装置を右クリックし、[Security (セキュリティ)] > [HTTPS] > [Enable/Update (有効にする/更新する)] を選択します。
8. [Configuration (設定)] > [Security (セキュリティ)] > [Certificates (証明書)] > [Devices (デバイス)] に移動し、[Validate device certificate (デバイス証明書を検証する)] をオンにします。

注

AXIS Camera Station Proはデバイスから切断され、一部のシステムコンポーネントが再起動します。

時刻同期

Windowsタイムサービスが実行されていない

Windows TimeサービスとNTPサーバーの時刻がずれています。これは、Windows TimeサービスがNTPサーバーに接続できないことが原因である可能性があります。

- NTPサーバーがオンラインであることを確認してください。
- ファイアウォールの設定が正しいことを確認してください。
- デバイスがNTPサーバーと通信できるネットワーク上にあることを確認してください。

サポートについては、システム管理者にお問い合わせください。

Detected time difference on a device (デバイスで時差が検出されました)

装置がサーバー時間と同期していません。録画のタイムスタンプは、デバイスが録画した時刻ではなく、サーバーが録画を受信した時刻に付きます。

1. [Configuration > Devices > Time synchronization (設定 > デバイス > 時刻同期)] に移動し、サーバー時間オフセットを確認します。
2. サーバーの時間オフセットが2秒を超える場合:
   2.1. [Enable time synchronization (時刻同期を有効にする)] を選択します。
   2.2. デバイスが指定されたNTPサーバーと通信可能であることを確認します。
   2.3. [Configuration > Devices > Management (設定> 装置 > 管理)] で装置を再読み込みします。

3. サーバーのタイムオフセットが2秒未満の場合、デバイスが時刻同期のために十分なデータを送信しない可能性があります。
   3.1. [Send alarm when the time difference between server and device is larger than 2 seconds (サーバーと装置の時差が2秒を超える場合にアラームを送信する)] をオフにしてアラームをオフにします。

ヘルプが必要な場合は、Axisサポートにお問い合わせください。

Secure Remote Access v2

クラウドサービスにローカルで接続できない

クラウドサービスとの接続の問題を解決する:

1. AXIS Camera Station Proを開き、[Configuration (設定)] > [Connected services (接続中のサービス)] > [Management (管理)] に移動します。
2. [Status (ステータス)] が緑色になっていることを確認します。緑色になっていない場合は、インターネット接続を確認してください。
3. 問題が解決しない場合は、Axisサポートまでお問い合わせください。

クラウドサービスにリモートで接続できない

AXIS Camera Station Proでの手順：

1. [Menu (メニュー)] > [Help (ヘルプ)] に移動し、[Status of Axis services (Axisサービスのステータス)] をクリックします。*https://status.axis.com*のステータスページが開きます。ここからメンテナンスの通知や予定されているダウンタイムを確認することができます。
2. Axis Camera Station Proセクションでドロップダウンリストを展開し、クラウドサービスにアクセス可能かどうかを確認します。
3. ご使用のMy Axisアカウントが正しい組織に招待されていることを確認します。

AXIS Camera Station Proモバイルアプリでの手順：

1. [More (その他)] > [Help section (ヘルプセクション)] に移動し、[Status of Axis services (Axisサービスのステータス)] をクリックします。*https://status.axis.com*のステータスページが開きます。ここからメンテナンスの通知や予定されているダウンタイムを確認することができます。
2. インターネット接続が安定していることを確認します。問題の原因を特定できるよう、別のモバイルデバイスでテストしてみてください。
3. ご使用のMy Axisアカウントが正しい組織に招待されていることを確認します。

問題が解決しない場合は、Axisサポートまでお問い合わせください。

パケットロスや遅延、誤ったルーティングに関する一般的な問題

1. インターネットに接続されていることを確認してください。主に使用されるポートは80と443で、アウトバウンドトラフィックに対しても開放されている必要があります。
2. ご使用のルーターによっては、次の追加ドメインに対してポートを開放する必要がある場合があります。
   - https://eu.login.connect.axis.com (ポート 433)
   - https://eu.cs.connect.axis.com (ポート 433)
   - https://api.vms.axis.cloud (ポート 433)
   - wss://signaling.prod.webrtc.connect.axis.com (ポート 433)
   - https://*.turn.prod.webrtc.connect.axis.com (ポート443、3478、5349、49152-65535)

注

アスタリスク「*」の部分は動的で、リージョンと固定されていないサーバーIDの組み合わせで構成されます。

さらなるサポートが必要な場合は、Axisサポートにお問い合わせください。

技術サポート

AXIS Camera Station Proのライセンスバージョンをお持ちのお客様は、技術サポートをご利用いただけます。技術サポートに連絡する場合は、 > [Help (ヘルプ)] > [Online Support (オンラインサポート)] に移動するか、*axis.com/support*にアクセスします。

技術サポートにシステムレポートとスクリーンショットを送付されることをお勧めします。

システムレポートを作成するには、 > [Help (ヘルプ)] > [System report (システムレポート)] に移動します。

報告手順

このガイドを使用しても解決できない問題がある場合は、*Axis*オンラインヘルプデスクに問題をエスカレーションしてください。弊社のサポートチームが問題を理解し、解決できるようにするために、以下の情報を含める必要があります。

- 問題の再現方法または問題の発生状況に関する明確な説明。
- 問題の発生日時、および該当する場合は、影響を受けたカメラの名称またはIPアドレス。
- 問題発生直後に生成された AXIS Camera Station Proシステムレポート。問題を再現できたクライアントまたはサーバーからシステムレポートを生成してください。問題が予測可能な形で再発する場合は、サーバーとクライアントの両方でデバッグログを有効にし、問題をより詳細に把握してください。完了したら、デバッグログを無効してください。

問題によっては、サポートチームが追加情報の提供を求める場合があります。

注

ネットワークトレースやデータベースファイルなど、ファイルが1GBを超える場合は、信頼できる安全なファイル共有サービスを使用してファイルを送信してください。

補足情報	
デバッグレベルのログ	ログファイルのサイズには制限があるため、デバッグレベルのログはデフォルトで無効になっています。デバッグレベルのロギングを有効にする場合は、システムレポートの生成が完了したら無効にするようにしてください。 サーバー: **[Configuration (設定)] > [Server (サーバー)] > [Settings (設定)] > [Enable debug logging (デバッグログを有効にする)** クライアント: **[Configuration (設定)] > [Client (クライアント)] > [Settings (設定)] > [Enable debug logging (デバッグログを有効にする)**
ライブビューおよび再生のデバッグオーバーレイ	ライブビューや再生で問題が発生した場合は、デバッグオーバーレイの画面録画があると役立ちます。問題の原因を特定できるよう、この録画にはシステムクロックを含む画面全体をキャプチャーしてください。

補足情報	
	• Ctrlキーとlキーを同時に1回押すと、ライブビューにオーバーレイ情報が表示されます。 • Ctrlキーとlキーを同時に2回押すと、デバッグ情報が追加されます。 • Ctrlキーとlキーを同時に3回押すと、オーバーレイが非表示になります。
データベースファイル	データベースを調査または手動で修復する必要がある場合に使用します。システムレポートを生成する前に、[**Include database in the report (レポートにデータベースを含める)**]を選択します。AXIS Camera Station Serviceの起動に問題が発生した場合はこれを含めてください。
スクリーンショット	スクリーンショットを追加する場合は、画面全体をキャプチャーして、背景情報を多くしてください。フルスクリーンのスクリーンショットでは分かりにくいと思われる場合は、矢印で該当の部分を示してください。
画面の録画	問題を再現するのにユーザーインターフェースで多くの操作が必要になる場合など、問題を言葉で説明するのが難しい場合は画面録画を活用してください。
ファイルの録画	サポート担当者から、AXIS Camera Stationが録画データの保存に使用する.acsmおよび.acsiファイルの例を提示するよう求められる場合があります。これは、録画の再生やエクスポートに問題がある場合や、AXIS File Playerに問題がある場合に該当します。これらのファイルは、各カメラに対して選択した保存先にあります。

T10196821_ja

2026-07 (M33.8)

© 2023年 – 2026 Axis Communications AB