AXIS Camera Station 5

ユーザーマニュアル

AXIS Camera Station 5について

AXIS Camera Station 5 は、中小規模の設置環境向けに監視と録画が一体となったシステムです。

アクティブ、長期サポート（LTS）、および製品別サポート（PSS）トラック上で維持されているすべての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 5のリリース ノートまたは *AXIS OS Portal*を参照してください。AXIS Camera Station 5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 5 サーバー - 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処理します。それぞれのサーバーが通信できるカメラやエンコーダの数は、利用可能な合計帯域幅によって制限されます。

AXIS Camera Station 5 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。クライアントは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モバイル監視アプリ - 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。HTTPSを使用して AXIS Camera Station 5サーバーと通信します。*概要*のサーバー設定のセクションの説明に従って、モバイル通信およびストリーミングポートの設定を行ってください。アプリの使用方法の詳細については、『*AXIS Camera Station Mobile Appユーザーマニュアル*』を参照してください。

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 Feature Guide*を参照してください。

最新情報

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

管理者に役に立つリンク

ここでは、オペレーターが興味を持ちそうなトピックをいくつか紹介します。

- *サーバーとの接続, on page 8*
- *デバイスの設定, on page 41*
- *ストレージの設定, on page 71*
- *録画とイベントの設定, on page 76*
- *接続中のサービスの設定, on page 115*
- *サーバーの設定, on page 119*
- *ライセンスの設定, on page 128*
- *セキュリティの設定, on page 130*

その他のマニュアル

- *AXIS Camera Station Integrator Guide*
- *AXIS Camera Stationの新機能*
- *AXIS Camera Station Installation and Migration Guide*
- *AXIS Camera Stationモバイルアプリ*
- *AXIS Camera Station Feature Guide*
- *AXIS Camera Stationチュートリアルビデオ*
- *AXIS Camera Station Troubleshooting Guide*
- *AXIS Camera Station System Hardening Guide*

オペレーターに役に立つリンク

ここでは、オペレーターが興味を持ちそうなトピックをいくつか紹介します。

- *AXIS Camera Stationのオペレーター向け操作ガイド*
- *サーバーとの接続, on page 8*
- *クライアントの設定, on page 110*
- *ライブビュー, on page 13*
- *録画の再生, on page 23*
- *録画のエクスポート, on page 25*
- *AXIS Camera Station早見表 - レビューとエクスポート*

クイックスタート

このチュートリアルでは、システムを起動して実行中にする手順について説明します。

開始する前に、以下をご確認ください。

- インストール内容に応じてネットワークを設定します。*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。
- セキュリティ上の問題を考慮します。*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 5*

オペレーター向け:

1. *ライブビデオを表示する, on page 6*
2. *録画の表示, on page 6*
3. *録画のエクスポート, on page 6*
4. *AXIS File Playerでの録画の再生と検証, on page 6*

ビデオ管理システムを起動する

AXIS Camera Station 5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 5サーバーに自動的にログインしようとします。

複数の AXIS Camera Station 5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

を初めて起動すると、[Add devices (デバイスの追加) AXIS Camera Station 5] ページが開きます。AXIS Camera Station 5はネットワークで接続済みの装置を検索し、見つかった装置のリストを表示します。*デバイスの追加*を参照してください。

1. 追加するカメラをリストから選択します。カメラが見つからない場合は、[**Manual search (手動検索)**] をクリックします。
2. [**追加**] をクリックします。
3. [**クイック設定**] または [**Site Designer設定**] を選択します。**[Next (次へ)]** をクリックします。*Site Designerプロジェクトのインポート, on page 45*を参照してください。
4. デフォルト設定を使用し、録画方法が [**None (なし)**] に設定されていることを確認します。[**インストール**] をクリックします。

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 23*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 25*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)] をクリックします。検証結果ページが表示されます。

注

- デジタル署名は署名付きビデオとは異なります。署名付きビデオを使用すると、ビデオを元のカメラに戻してトレースし、録画がいたずら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

AXIS Camera Station 5クライアント、AXIS Camera Station 5サーバー、接続されているネットワーク装置が異なるネットワーク上にある場合は、AXIS Camera Station 5を使用する前にプロキシ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

プロキシサーバーによってクライアントとサーバーが分離されている場合は、クライアントのプロキシ設定を編集します。

1. AXIS Camera Station 5クライアントを開きます。
2. [Change client proxy settings (クライアントのプロキシー設定を変更)] をクリックします。
3. クライアントのプロキシー設定を変更します。*クライアントのプロキシ設定*を参照してください。
4. [OK] をクリックします。

サーバーのプロキシ設定

プロキシサーバーによってネットワーク装置とサーバーが分離されている場合は、サーバーのプロキシ設定を編集します。

1. AXIS Camera Station 5 Service Controlを開きます。
2. [Modify settings (設定の変更)] を選択します。
3. [Proxy settings (プロキシの設定)] セクションで、デフォルトのシステムアカウントのインターネットオプションを使用するか、[Use manual proxy settings (手動でプロキシを設定する)] を選択します。*概要*を参照してください。
4. [保存] をクリックします。

NATとファイアウォール

クライアントとサーバーがNATやファイアウォールなどで隔てられている場合は、NATやファイアウォールを設定して、AXIS Camera Station 5 Service 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します。NATまたはファイアウォールの設定手順については、ネットワーク管理者に問い合わせてください。

詳細については、*AXIS Camera Station 5のポートリスト, on page 192*を参照してください。

サーバーポートの設定

AXIS Camera Stationサーバーでは、ポート55752 (HTTP)、55754 (TCP)、55756 (モバイル通信)、および55757 (モバイルストリーミング) がサーバーとクライアントの間の通信に使用されます。必要な場合、これらのポートはAXIS Camera Station Service Controlで変更できます。

詳細については、*概要*または*FAQ*を参照してください。

セキュリティに関する考慮事項

カメラや録画に対する不正アクセスを防止するため、次のことに注意してください。

- 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 5サーバー、カメラ、ビデオエンコーダ、補助装置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 5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。Windows® Active Directoryは、高レベルのセキュリティを提供します。

サーバーとの接続

AXIS Camera Station 5クライアントを使用すると、同じコンピューターやネットワーク上にインストールされている1つまたは複数のサーバーに接続することができます。AXIS Camera Station 5サーバーに異なる方法で接続できます。

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 8*を参照してください。

Axisセキュアリモートアクセス - *AXISセキュアリモートアクセスにサインイン, on page 9*を参照してください。

注

初めてサーバーに接続する際に、クライアントではサーバー証明書IDが確認されます。正しいサーバーに接続していることを確認するには、AXIS Camera Station 5Service Controlに表示されている証明書IDを手動で確認します。*概要, on page 191*を参照してください。

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)**] 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 5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)	接続済みのすべてのサーバーで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。
Change client proxy settings (クライアントのプロキシ設定を変更)	サーバーに接続するには、クライアントのプロキシ設定を変更する必要がある場合があります。**Change client proxy settings (クライアントプロキシ設定の変更)**] をクリックします。*クライアントのプロキシ設定*を参照してください。

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。サーバーが一覧表示されていない場合は、 をクリックして使用可能なすべてのリモートサーバーを再読み込みします。サーバーがデフォルトのポート番号 (55754) 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. 利用可能な機能は以下のとおりです。
   - 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セキュアリモートアクセスにサインイン

重要

セキュリティおよび機能性の向上を目的として、Axis Secure Remote Access (v1) をAxis Secure Remote Access v2 へアップグレードします。現行バージョンは2025年12月1日をもって提供終了となる予定のため、それまでにAxis Secure Remote Access v2へのアップグレードを強くお勧めします。

お使いの AXIS Camera Station 5システムへの影響：

- 2025年12月1日以降、Axis Secure Remote Access (v1)を使用してシステムにリモートアクセスすることはできなくなります。
- Axis Secure Remote Access v2を使用するには、AXIS Camera Station Proバージョン6.8にアップグレードする必要があります。このアップグレードは、2026年3月1日まで、AXIS Camera Station 5をご利用中のすべてのユーザーに無料で提供されます。

注

- Axis Secure Remote Accessを使用してサーバーに接続しようとすると、サーバーはクライアントを自動的にアップグレードできません。
- プロキシーサーバーがネットワークデバイスと AXIS Camera Station 5サーバーの間にある場合、AXIS Secure Remote Accessを使用してサーバーにアクセスするには、AXIS Camera Station 5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。

1. [AXISセキュアリモートアクセスにサインイン] 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。*Axisセキュアリモートアクセス*を参照してください。
3. [Sign in (サインイン)] をクリックします。
4. [Grant (許可)] をクリックします。

クライアントのプロキシ設定

これらの設定は、AXIS Camera Station 5クライアントと AXIS Camera Station 5サーバーの間にあるプロキシサーバーに適用されます。

注

AXIS Camera Station 5サーバーとネットワークカメラの間にあるプロキシサーバーを設定する場合は、AXIS Camera Station 5 Service Controlを使用してください。*AXIS Camera Station 5 Service Control*を参照してください。

設定に適したオプションを選択します。

- Direct connection (直接接続): AXIS Camera Station 5クライアントと AXIS Camera Station 5サーバーの間にプロキシサーバーがない場合は、このオプションを選択してください。
- Use Internet Options settings (インターネットオプションの設定を使用) (デフォルト): Windows設定を使用するには、このオプションを選択します。
- Use manual proxy settings (手動でプロキシを設定する):プロキシー設定を手動で設定するには、このオプションを選択します。[手動設定] セクションで、必要な情報を提供します。
  – アドレス:プロキシーサーバーのアドレスまたはホスト名を入力します。
  – ポート:プロキシーサーバーが使用するポート番号を入力します。
  – Do not use proxy server for addresses beginning with (次で始まるアドレスにはプロキシを使用しない):プロキシーによるアクセスから除外したいサーバーを入力

します。複数のアドレスを指定する場合は、セミコロン (;) で区切ります。アドレスやホスト名にワイルドカードを使用できます。たとえば、「192.168.*」、「*.mydomain.com」とします。

- Always bypass proxy server for local addresses (ローカルアドレスには常にプロキシサーバーを使用しない):このオプションを選択すると、ローカルコンピューター上のサーバーに接続する際にはプロキシサーバーをバイパスします。ローカルアドレスにはドメイン名の拡張子はありません。たとえば、http://webserver/、http://localhost、http://loopback、http://127.0.0.1となります。

AXIS Camera Station 5 クライアント

[Configuration (設定)] タブにある [Add devices (デバイスの追加)] ページは、AXIS Camera Station 5を初めて使用するときに表示されます。*デバイスの追加*を参照してください。

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重要な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 38*を参照してください。
設定	接続されたデバイスの管理とメンテナンス、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	アクションのホットキーの一覧です。*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および管理します。*アクセス管理, on page 164*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 34*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 5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 173*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 5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	ヘルプ関連のオプションを開きます。[**Help (ヘルプ)**] > [**About (バージョン情報)**] に移動して、使用中の AXIS Camera Station 5クライアントのバージョンを確認します。
ログアウト	サーバーとの接続を切断し、AXIS Camera Station 5クライアントからログオフします。
終了	AXIS Camera Station 5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を選択します。	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

ステータスバーの表示内容はたとえば次のようになります。

- クライアントとサーバー間に時間の不一致がある場合、警告のアイコンが表示されます。タイムラインの問題が発生しないように、クライアントの時刻がサーバーの時刻と同期していることを必ず確認してください。
- 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。を参照してください。
- [Secure Remote Access Usage (セキュアリモートアクセスの使用)] には、今月使用したデータのうち、サービスレベルに含まれる量との比較で、残存または超過したデータ量が表示されます。*Axisセキュアリモートアクセス*を参照してください。
- 管理者としてログインしている場合、新しいバージョンがあると、**AXIS Camera Station 5 [update available (更新が利用できます)]**と表示されます。*AXIS Camera Station 5の更新, on page 122*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

ライブビューには、ビューとカメラ、接続されているカメラからのライブビデオが表示されます。複数の AXIS Camera Station 5サーバーに接続している場合は、接続されているサーバーのすべてのビューとカメラがサーバー名で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 5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。

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 130*」を参照してください。

ライブビューの設定方法については、*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. カメラ、ビュー、またはシーケンスを右クリックし、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方法については、「*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 5からカメラを削除する方法については、*カメラ, on page 47* を参照してください。
🔒	管理者はビューをロックして、オペレーターや閲覧者がビューを移動または編集できないようにすることが可能です。

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画像を保存します。
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 [Export (エクスポート)] タブの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が有効に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、[**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)	画像内の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。ライブビュー画像で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、ナビゲーションの矢印の方向にパンします。画像のパン、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の長さを伸ばします。
フォーカスの設定	カメラフォーカスを調整するには、画像を右クリックし、[**Set focus (フォーカスを設定)**] を選択します。被写体にピントを自動的に合わせるには、[**AF**] をクリックします。手動でピントを調節するには、[**近くへ**] または [**遠くへ**] の側でバーを選択します。カメラに近い被写体にピントを合わせるには、[**近くへ**] を使用します。カメラから遠い被写体にピントを合わせるには [**遠くへ**] を使用します。

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 > Add preset (プリセット > 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。繰り返して同じ位置に合わせるため、この機能を使用してカメラを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。座標系を選択します。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。

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。

デジタルプリセットの追加

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。

PTZ制御

注

管理者はユーザーに対してメカニカル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、画像の上にカーソルを置き、  **[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、画像の上にカーソルを置き、[REC] をクリックします。ボタンが黄色に変わり、録画中であることが示されます。録画を停止するには、もう一度 [REC] をクリックします。

解像度、圧縮、フレームレートなどの手動録画を設定するには、「*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

管理者はユーザーに対して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 49*を参照してください。

 Volume (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 113*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 5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. [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)] ドロップダウンメニューから、使用するテンプレートを選択します。
5. 1つ以上のビュー、音声ゾーン、またはカメラを、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)] をクリックして、分割ビューを現在のサーバーに保存します。

ホットスポットを設定	ホットスポットフレームを定義するには、そのフレームを右クリックし、[Set hotspot (ホットスポットを設定)] を選択します。別のフレームをクリックすると、そのフレームがホットスポット内で開きます。ホットスポットは、1つの大きなフレームと複数の小さなフレームがある非対称分割ビューの場合に便利です。通常、最大のフレームがホットスポットです。
ストリームプロファイル	カメラのストリームプロファイルを設定するには、グリッドビューでカメラを右クリックし、[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。

分割ビューの追加

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、ドアの状態や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 141*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 17*を参照してください。

ダッシュボード	ドアの詳細、ドアの状態、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。 • カード所持者がカードを通したりしたときにアクセスコントロールイベント (写真などのカード所持者の詳細情報と共に)。 • 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、誰かが認証情報を提示した場合と同じようにドアのロックが解除されます。つまり、通常

	は設定した時間が経過するとドアは自動的にロックされます。
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

順次

シーケンスはビュー間で切り替わります。

注

複数の AXIS Camera Station 5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. [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. シーケンスに表示する順序でビューを配列します。
6. 必要に応じて、ビューごとに個別の表示時間を設定します。
7. PTZ機能付きのカメラの場合、[**PTZプリセット**] ドロップダウンリストからPTZプリセットを選択します。*PTZプリセット*を参照してください。
8. [**Save view (ビューを保存)**] をクリックして、シーケンスを現在のサーバーに保存します。

滞留時間	表示時間は、ビューを表示してから次のビューに切り替えるまでの秒数です。これはビューごとに個別に設定できます。

シーケンスの追加

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 5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、マップにはカメラビュー、分割ビュー、シーケンス、Webページ、他のマップ、ドアを配置できます。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 5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. [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。ファイルの最大サイズは20MBで、サポートされるファイル形式はBMP、JPG、PNG、GIFです。
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すると、設定を編集できます。
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。

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。

8. [**Save view (ビューを保存)**] をクリックして、マップを現在のサーバーに保存します。

	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。
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。
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。
検知範囲	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。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。動体検知やその他のアクションルールによってトリガーされたカメラの録画中に、検知範囲が点滅するようにする場合は、[Flash (点滅)] をオンにします。クライアントの設定ページで、すべての装置の検知範囲の点滅をグローバルにオフにすることができます。*クライアント設定, on page 110*を参照してください。
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。

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。

マップの追加

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。

マップから音声をトリガー

Webページ

Webページビューには、インターネットのページが表示されます。分割ビューやシーケンスなどにWebページを追加できます。

Webページを追加するには:

1. [ライブビュー] タブで、 + をクリックします。
2. [**New webpage (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全体を入力します。
5. [OK] をクリックします。

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

[録画] タブでは、録画の検索、再生、エクスポートを行うことができます。このタブには、録画のビューと、接続されているサーバーのビュー、画像、再生ツール、カメラをサーバー名でグループ化した 2 つのパネルがあります。ライブビューを参照してください。

録画のメインビューから、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したりするには、*録画の方法*を参照してください。

注

AXIS Camera Station 5から録画を手動で削除することはできません。古い録画を削除するには、**[Configuration (設定)] > [Storage (ストレージ)] > [Selection (選択)]**で保存期間を変更する必要があります。

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

タイムラインを使って、再生内を移動したり、録画日時を確認したりすることができます。タイムラインの赤い線は、動体検知録画を表します。タイムラインの青い線は、アクションルールによって録画がトリガーされたことを表します。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。録画の中で、タイムラインを移動 (スクラビング) してコンテンツの概要を把握し、特定の出来事を見つけることができます。

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。
	フィルターを使用して、タイムラインに表示する録画のタイプを設定します。
	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。
スマート検索1	スマート検索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	画像をクリックして上下にスクロールして画像を拡大または縮小し、ビューを移動して画像の他の部分を表示します。エリアにズームインするには、エリア内にカーソルを置き、スクロールしてズームします。

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。
- AXIS Camera Station 5からカメラを削除すると、システムはロックされた録画を削除します。

	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、説明を編集し、録画をロック解除またはロックします。
	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、複数のブックマークを選択して、CTRLキーまたはSHIFTキーを押しながら複数のブックマークを削除します。
録画削除を防止	選択またはクリアして、録画をロックまたはロック解除します。

ブックマークの追加

1. 録画に移動します。

2. カメラのタイムラインで、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置かれ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。説明にキーワードを使用すると、ブックマークを検索しやすく、内容が分かりやすくなります。
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

ロックされた録画を削除することはできません。録画のロックを解除するには、このオプションをクリアするか、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。

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。このタブでは、録画の情報とプレビューも閲覧できます。複数のファイルを同時にエクスポートでき、.asf、.mp4、.mkvへのエクスポートを選択できます。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 28*を参照してください。

録画のエクスポート

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。録画のエクスポートタスクが**[Tasks (タスク)]**タブに表示されます。

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。
- .txtファイルのノート (**[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ファイルのプレイリスト(**[Create playlist(.asx) (プレイリスト (.asx) の作成)]**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。
	セクション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。
録画の追加	単一の録画をエクスポートするには、録画を右クリックし、[**Export > Add recordings (エクスポート > 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録画を削除するには、録画を右クリックして、[**Export > Remove recordings (エクスポート > 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に音声を含めないようにするには、[**Audio (音声)**] 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の編集 (映像の編集) を行う, on page 28*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。

[Export (エクスポート)] タブ	
	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。
エクスポートに切り替える	[Incident report (事故レポート)] タブが開いている場合、[Export (エクスポート)] タブに移動するには、[Switch to export (エクスポートに切り替える)] をクリックします。
推奨ストリームプロファイル	[Preferred stream profile (推奨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。複数の録画をプレビューできるのは、それらが1台のカメラでの録画である場合だけです。
保存	エクスポートリストをファイルに保存する場合は、[Save (保存)] をクリックします。
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。
ノートを含める	録画にノートを含めるには、[ノートを含める] を選択します。ノートは、エクスポート先のフォルダーで.txtファイルとして使用したり、AXIS File Playerで録画のブックマークとして使用したりできます。
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場所にドラッグします。プレビューを右クリックし、[Add snapshot (スナップショットの追加)] を選択します。

高度な設定	
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、[プレイリストを作成 (.asx)] を選択します。録画の再生は、録画された順番で行われます。
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する)] を選択

高度な設定	
	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 30*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する)**] を選択します。エクスポートするZipファイルにパスワードを設定することができます。
Export format (エクスポート形式)	[**Export format (エクスポート形式)**] ドロップダウンメニューから、録画のエクスポート先の形式を選択します。[MP4] を選択した場合、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。
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形式の場合にM-JPEGが使用され、その他の形式の場合はH.264が使用されます。

エクスポートのユーザー権限

録画をエクスポートしたり、インシデントレポートを生成するには、権限が必要です。どちらか一方または両方に権限を与えることができます。[**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 130*に移動します

エクスポートする前に録画の編集 (映像の編集) を行う

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 > Size (バウンディングボックスのオプション > 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 > Fill (境界ボックスのオプション > 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り合っている場合、重なっている部分は [Black (黒)]、[Pixelated (モザイク)]、[Clear (透明)] の順に塗りつぶされます。

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 28*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、カメラの分析データをオンにします。*ストリームプロファイル, on page 49*を参照してください。

1. **[Export (エクスポート)]**タブまたは**[Incident report (事故レポート)]**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. 境界ボックスが動く物体を覆っていることを確認し、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 5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のインストール*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。

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を開くと、エクスポートされた録画が自動的に再生されます。
3. AXIS File Playerで をクリックすると、録画のノートが表示されます。
4. AXIS File Playerの [**Add digital signature (デジタル署名を追加)**] で録画のデジタル署名を検証します。
   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. 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。

事故レポートのエクスポート

[Incident report (事故レポート)] タブから、事故レポートをローカルストレージまたはネットワークの場所にエクスポートできます。ここで、録画、スナップショット、ノートを事故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 28*を参照してください。

インシデントレポート

事故レポートの生成

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 25*を参照してください。
3. [**Switch to incident report (事故レポートに切り替える)**] をクリックして、[incident report (事故レポート)] 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)。
- 事故レポート。
- 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に音声を含めないようにするには、[Audio (音声)] 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の編集 (映像の編集) を行う, on page 28*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。
事故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、[Incident report (事故レポート)] に変更するには、[Switch to incident report (事故レポートに切り替える)] をクリックします。
推奨ストリームプロファイル	[Preferred stream profile (推奨ストリームプロファイル)] 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、エクスポートされたリスト内で録画をクリックすると、再生が開始します。複数の録画をプレビューできるのは、それらが1台のカメラでの録画である場合だけです。
保存	事故レポートをファイルに保存する場合は、[Save (保存)] をクリックします。
読み込み	以前に保存した事故レポートを含める場合は、[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。事故レポートに含める追加情報を併せて入力できます。
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	参照IDは自動的に生成され、必要に応じて手動で変更できます。参照IDは事故レポートを識別する一意のIDです。
ノートを含める	録画/スナップショットにノートを含めるには、[Include notes (ノートを含める)] を選択

	します。ノートは、エクスポート先のフォルダーで.txtファイルとして使用したり、AXIS File Playerで録画のブックマークとして使用したりできます。
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形式の場合にM-JPEGが使用され、その他の形式の場合は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場所に移動します。プレビューを右クリックし、[Add snapshot (スナップショットの追加)] を選択します。

手動による録画

注

複数の AXIS Camera Station 5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。それには、[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。

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、マウスポインターを置きます。
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

スマート検索1を使用して、定義された画像エリア内で動きがある録画の部分を見つけます。

検索速度を上げるには、ストリームプロファイルに [**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。

スマート検索1を使用するには:

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. 対象範囲を調整します。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. 検索の開始時刻と終了時刻、および日付を選択しますSHIFTキーを使っ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。ここで、1つまたは多数の結果を右クリックして、録画をエクスポートできます。

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

スマート検索2は、録画内で移動する人物や車両の検索に使用します。

Axisカメラのスマート検索2をオンにすると、AXIS Camera Station 5はそのカメラからのメタデータの記録を開始します。スマート検索2では、メタデータを使用してシーン内の物体を分類し、フィルタを使用して対象物を検索できます。

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を搭載するカメラではAXIS Video Content Stream。*カメラアプリケーションのインストール, on page 65*を参照してください。
- AXIS Camera Station 5サーバーとカメラの時刻同期。

注

一般的な推奨事項:

- 連続録画の使用をお勧めします。動体検知によってトリガーされる録画を使用すると、検知にビデオ録画が含まれないことがあります。
- 検索結果で録画をプレビューする場合は、H.264形式の使用をお勧めします。
- 最適な色分類のために、照明条件がカメラの仕様内であ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 161*
2. AXIS Camera Station 5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 70*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 34*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 36*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、以下の方法を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処理を有効にします。
- 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、データの量を絞り込む。

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、例えば、ある瞬間の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。
範囲	エリアでフィルターするには、[Area (エリア)] をクリックし、カメラを選択して、[Filter by area on this camera (このカメラでエリアによりフィルター)] 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	ライン横断でフィルターするには、[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によりフィルター)] をオンにします。画像内の線を調整し、必要に応じて点を追加または削除します。
サイズと継続時間	サイズと期間でフィルターするには、[Size and duration (サイズと期間)] をクリックし、カメラを選択して、[Filter by size and duration on this camera (このカメラでサイズと期間によりフィルター)] 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幅と高さを調整します。最小期間を秒単位で調整します。

速度	速度でフィルターするには、[Speed (速度)] をクリックし、カメラを選択して、[Filter by speed on this camera (このカメラで速度によりフィルター)] 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。 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 filter settings (保存したフィルター設定)]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。

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	検索結果をさらにフィルターするには、[Confidence level (信頼度)] をクリックして、信頼度を設定します。高い信頼度では、不確実な分類が無視されます。

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。
- 装着式カメラには対応していません。
- レーダーは人物と他の車両のみを検知できます。レーダーに対してバックグラウンドでのサーバー分類を有効にすることはできません。
- サーマルカメラでの物体の分類の動作は未確認です。
- スマート検索2では、PTZプリセットポジションの変更時、および位置変更後の短い再キャリブレーションの間、動く物体は検知されません。
- 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、イベントで起こったことの詳細を知るためのデータを生成するシステムまたは装置です。詳細については、*外部データソース, on page 69*を参照してください。以下にいくつかの例を示します。

- 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 5が外部データを保存する日数を変更するには、**Configuration > Server > Settings > External data (設定 > サーバー > 設定 > 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)]オプション をクリックし、追加のフィルターを適用します。フィルターはデータソースのタイプによって異なる場合があります。
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 39*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	アクセスコントロールは、データを生成するコンポーネントの一例です。この特定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。
Third party (サードパーティ)	設定し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。以下にいくつかの例を示します。

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。
場所	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。この機能はイベント情報のみをエクスポートし、録画や画像はエクスポートしません。

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`」と入力して検索すると、[Max speed] 列 (最大速度列) で28を超える数値が含まれる結果が返されます。 • 「`[Average speed] < = 28`」と入力して検索すると、[Average speed] 列 (平均速度列) に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。

設定

[Configuration (設定)] タブでは、接続された装置の管理とメンテナンス、およびクライアントとサーバーを設定できます。 ＋ 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 5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 5 では、IPv4アドレスを持つ装置のみがサポートされます。
- 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 5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 5では、装置の例は次のとおりです。

- ネットワークカメラ
- ビデオエンコーダ (1つ以上のビデオポートを装備)
- 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)
- インターカム

デバイスでは次のアクションを実行できます。

- 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、フォーマットなどに関する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 69*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。
- 装置を追加すると、装置の時刻が AXIS Camera Station 5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、または録画済みのビデオを見つけます。
   - *デバイスの検索, on page 43*
   - *ビデオストリームの検索, on page 43*
   - *録画済みのビデオを見つける, on page 44*

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 44*

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、装置をAXIS Camera Station 5に追加できます。
通信中	AXIS Camera Station 5 サーバーが装置にアクセスしようとしています。
デバイスの証明書が信頼されていません	AXIS Camera Station 5 は、装置上の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検証できません。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 5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 5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 5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 5 は装置に接続できません。
パスワードを入力	AXIS Camera Station 5 は、装置へのアクセスに使用する認証情報を認識していません。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 5によって使用されます。
パスワードの設定	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)**] をクリックしてパスワードを取得します。生成されたパスワードを表示し、そのコピーを作成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。
サポートされないモデルです:	AXIS Camera Station 5 はその装置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	装置のファームウェアのバージョンが古いため、装置を追加するには、その前にファームウェアを更新する必要があります。

故障デバイス	AXIS Camera Station 5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	カメラの設置方法に応じて、リンクをクリックし、チルトの向きを [Ceiling (天井)]、[Wall (壁)]、または [Desk (デスク)] のいずれにするかを選択します。一部のカメラモデルでは、チルトの向きを設定する必要があります。
非対応のONVIFデバイス	AXIS Camera Station 5 は、このサードパーティ製の装置をサポートしていません。
サポートされていない装置	AXIS Camera Station 5 このタイプのデバイスには対応していません。

注

新規HTTPS証明書は AXIS Camera Station 5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. **[設定]** - **[デバイス]** - **[デバイスの追加]** を選択します。
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. **[設定] - [デバイス] - [デバイスの追加]** を選択します。
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 5に追加できます。

.mkvファイルの要件:

- 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 54*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. **[設定] - [デバイス] - [デバイスの追加]** を選択します。
3. デバイスの名前を変更するには、リストにある名前をクリックし、新しい名前を入力します。
4. 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。
5. ホスト名が使える場合、デバイスについてIPの代わりにホスト名を使用するかどうかを選択します。
6. 基本的な設定のみを行う場合は、[**Quick configuration (クイック設定)**] を選択します。
Site Designerプロジェクトをインポートする場合は、*Site Designerプロジェクトのインポート*を参照してください。
7. [**Retention time (保存時間)**] 、[**Recording storage (録画ストレージ)**]、[**Recording method (録画方法)**] を選択します。

注

録画ストレージで [**Automatic (自動)**] 録画を選択した場合、各カメラのOS以外のドライブに32 GB以上の容量のストレージが割り当てられます (可能な場合)。システムは、15 GB以上の空き

容量のあるストレージを自動的に選択し、次に、録画するように設定されたカメラの台数が少ないストレージと、AXIS Camera Station 5に既に設置されているストレージを選択します。

8. [**Install (インストール)**] をクリックします。AXIS Camera Station 5により、HTTPSをサポートする装置でHTTPSが自動的に有効になります。

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 5 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Site Designer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。

サイトデザイナープロジェクトを AXIS Camera Station 5にインポートするには:

1. Site Designerプロジェクトへのアクセスコードを生成するか、または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. **サーバーがインターネットに接続されている状態で、**[Generate code (コードを生成する) AXIS Camera Station 5] をクリックします。または、サーバーがインターネットに接続されていない状態で、[**Download settings file (設定ファイルをダウンロードする)**] をクリックします。
2. AXIS Camera Station 5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. カメラを選択して [**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。または、[**Choose file (ファイルの選択)**] を選択してダウンロードしているSite Designer設定ファイルに移動します。
6. [**Import (インポート)**] をクリックします。インポート時、AXIS Camera Station 5はSite Designerプロジェクトと選択したカメラをIPアドレスまたは製品名で一致させようとします。マッチングに失敗した場合は、ドロップダウンメニューから正しいカメラを選択できます。
7. [**インストール**] をクリックします。

AXIS Camera Station 5 は、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	✓	✓
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		✓

	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
ディング、圧縮などの録画プロファイル		
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		✓
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つだけ定義した場合、または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 5はプロファイルを「中」に設定します。
- 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 5は連続録画プロファイルを「中」に、動きによるトリガー録画を「高」に設定します。
- AXIS Camera Station 5 はアスペクト比を最適化するため、インポートとSite Designerプロジェクトで解像度が異なる場合があります。
- AXIS Camera Station 5 装置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、は音声設定を行うことができます。外部音声装置を使用する場合は、装置を設置した後、装置を手動で有効にする必要があります。
- AXIS Camera Station 5 は、Site Designerの設定が異なる場合でも、音声設定をインターカムに適用しません。インターカムでは、ライブビューのみで音声が常にオンになります。

サードパーティデバイスの追加

AXIS Camera Station 5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 5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 43*を参照してください。

サードパーティ製の装置のサポートについては、*最新のテクニカルペーパー*を参照してください。

注

AXIS Camera Station Device Compatibility Toolをダウンロードおよび実行して、ネットワークビデオ製品がAXIS Camera Station 5以降と互換性があるかどうかを確認できます。このツール

は、システムがネットワークビデオ製品からビデオストリームを受信できるかどうかを確認します。「*AXIS Camera Station Device Compatibility Tool*」を参照してください。

AXIS Camera Station 5 はONVIF準拠ではありません。ただし、サードパーティ製の装置がONVIFプロファイルSに準拠し、AXIS Camera Station Device Compatibility Toolを使用して検証されている必要があります。

AXIS Camera Station 5 は、IEC62676-2-31およびIEC62676-2-32に準拠し、サードパーティ製の装置用に次の機能をサポートしています。

- 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 5)
- 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 5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

- AXIS Camera Station 5ライセンスで使用可能なカメラの総数では、ネットワークカメラのすべてのビューエリアが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 5ライセンスごとに、特定の台数のカメラがインストール可能です。

AXIS Camera Station 5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. 設定を見つけるための手順はカメラのモデルとファームウェアによって異なるため、[**Help (ヘルプ)**] をクリックして確認してください。

カメラ

[**Configuration > Devices > Cameras (設定 > 装置 > カメラ)**] を選択すると、システムに追加されているすべてのカメラが一覧表示されます。

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 5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。これを実行すると、AXIS Camera Station 5は、削除されたカメラに関連付けられたすべての録画 (ロックされた録画を含む) を削除します。

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。

オン	ビデオストリームの録画と表示を禁止するには、[Enabled (有効)] の選択を解除します。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。
ユーザー名	カメラの管理者アカウントのユーザー名。
パスワード	カメラの管理者アカウントのパスワード。AXIS Camera Station 5はこのパスワードを使用してカメラと通信します。

その他の装置

[Configuration > Devices > Other devices (設定 > 装置 > 他の装置)] を選択すると、ドアコントローラー、音声装置、I/Oモジュールなどビデオ機能を持たない装置が一覧表示されます。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。

サポートされている製品の詳細については、*www.axis.com*の「*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 5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。
- 装置を削除します。

他のデバイスの設定の編集

カメラ以外の装置の設定を編集するには:

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。

ユーザー名	装置の管理者アカウントのユーザー名。
パスワード	装置管理者アカウントのパスワード。AXIS Camera Station 5はこのパスワードを使用して装置と通信します。

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。このページにはすべてのカメラのリストが表示されます。

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

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

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。このオプションはサードパーティ製デバイスにのみ使用できます。 • 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より必要な帯域幅とストレージ容量が少なくなります。一部のカメラは**H.265**にも対応しており、この形式は圧縮率が若干向上しますが、より高い処理能力を必要とします。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。
フレーム数	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決まります。
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、動作効率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	ありません
		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。ストレージの最適化では、デフォルトのZipstream設定と比較して、より高度な圧縮ツールを使用して追加のストレージを節約します。このプロファイルを使用すると、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フレームをサポートしていません。 • 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。
講演者：	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有効にします。音声は、ライブビューと録画、ライブビューのみ、または録画のみ有効にすることができます。

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。このオプションは、分析データをサポートするAxis装置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ストリーミングを有効にします。このオプションはサードパーティ製の装置にのみ使用できます。
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。このオプションは、AXIS PTZオートトラッキングが設定されたAxis PTZカメラでのみ使用できます。AXIS Camera Station 5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、設定するカメラを選択します。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 5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 5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

ネットワークカメラやビデオエンコーダのビデオと、カメラ以外の補助装置の音声を合わせて、ライブビューや録画に使用できます。

1. カメラ以外の装置を AXIS Camera Station 5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、カメラを設定する。*ストリームプロファイル*を参照してください。
3. ライブビューや録画用に音声を有効にする。*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 5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 5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

画像の設定を変更した場合は、瞬時に適用されます。

画像を設定するには:

1. [Configuration > Devices > Image configuration (設定 > 装置 > 画像の設定)] に移動し、AXIS Camera Station 5に追加されているすべてのカメラを一覧表示します。
2. リストの下にカメラとビデオフィードがリアルタイムで表示されます。**[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. 画像を設定します。

画像設定

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同じになるようにするために使用します。[**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。利用なオプションは、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点によって、画像内の他の領域が暗く見えすぎる場合は、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、ワイドダイナミックレンジを使用して、画像内でコントラストがかなり強い場合の露出を向上させます。スライダーを使用して、ダイナミックコントラストを調整します。逆光の強い条件下ではダイナミックコントラストを有効にします。暗い条件下ではダイナミックコントラストを無効にします。

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。

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) とは、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。

[設定] - [デバイス] - [PTZプリセット] を選択して、PTZ機能を使用できるカメラを一覧表示します。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が有効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を有効にするには、カメラに内蔵の設定ページを使用します。詳細については、カメラのユーザーマニュアルを参照してください。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 5およびカメラの設定ページで設定できます。PTZプリセットは、AXIS Camera Station 5で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の動きを確認し、録画することができます。
- AXIS Camera Station 5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、表示することも記録することもできません。

注

カメラのコントロールキューが有効になっている場合、PTZは使用できません。コントロールキューの詳細と、コントロールキューを有効または無効にする方法については、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、プリセットを選択し [**削除**] をクリックします。選択したプリセットが AXIS Camera Station 5とカメラから削除されます。

デバイスの管理

装置管理には、AXIS Camera Station 5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。

[設定] - [デバイス] - [管理] を選択して「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 115*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、デバイスで使用可能な新しいファームウェアバージョンがあ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。

ファームウェアバージョンのアップグレード

*AXIS Camera Station 5の更新, on page 122*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、使用可能な新しい AXIS Camera Station 5のバージョンがあ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 AXIS Camera Station 5をインストールします。

AXIS Camera Station 5の新しいバージョンをインストールします。

AXIS Camera Station 5に追加されている装置のリストが表示されます。**[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アンドドロップして、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。

- **名前:** 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。
- **MACアドレス:** デバイスのMACアドレス。
- **ステータス:** 装置のステータス。
  - **OK:** 確立されたデバイス接続の標準の状態。
  - **メンテナンス:** 装置はメンテナンス中であるため、一時的にアクセスできません。
  - **アクセス不可:** デバイスとの接続を確立できません。
  - **設定されたホスト名ではアクセスできません:** ホスト名を使用して装置との接続を確立することはできません。
  - **サーバーにアクセス不可:** 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。
  - **パスワードを入力:** 有効なアカウント情報を入力するまでデバイスの接続は確立されません。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。
  - **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、装置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。自動生成されたパスワードを表示し、そのコピーを作成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。
    - 装置が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を有効にします。
  - **パスワードのタイプ：非暗号化：** 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、デバイスの接続は確立されません。安全上の理由から、AXIS Camera Station 5では暗号化されたパスワードを使用したことがある装置に対しては、暗号化されていないパスワードの使用を許可していません。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。
  - **証明書エラー:** 装置上の証明書にエラーがあります。
  - **まもなく証明書の有効期限です:** 装置上の証明書の有効期限が近くなっています。
  - **証明書の有効期限切れ:** デバイス上の証明書の有効期限が切れました。
  - **HTTPS証明書が信頼されていません:** 装置のHTTPS証明書が AXIS Camera Station 5 に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失敗:** デバイスとのHTTP接続を確立できません。
  - **HTTPS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。
- **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。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 69*を参照してください。
- **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 69*を参照してください。
- **メーカー:** デバイスのメーカー。

- **モデル:** デバイスのモデル。
- **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場合、表示されます。
- **HTTPS:** 装置のHTTPSステータス。*セキュリティ, on page 66*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 66*でIEEE 802.1Xステータスを参照してください。
- **サーバー:** 装置が接続されている AXIS Camera Station 5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。*ユーザー管理*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。
- デバイスに日付と時刻を設定する。*日付と時刻の設定*を参照してください。
- デバイスを再起動する。
- パスワードを含むほとんどの設定を工場出荷時の値にリセットするためにデバイスをリストアします。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

- 不正なアクセスを防止するため、デバイスを工場出荷時の設定に戻した後、パスワードを設定することを強く推奨します。
- 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 5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のインストール*を参照してください。
- デバイスの設定ページから設定を変更した場合に、デバイスを再読み込みします。
- デバイスを設定する。*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。*ユーザー管理*を参照してください。
- 証明書を管理する。*セキュリティ, on page 66*を参照してください。
- デバイスデータを収集する。*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 68*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 **[詳細設定] - [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 69*を参照してください。

IPアドレスの割り当て

AXIS Camera Station 5 は複数の装置にIPアドレスを割り当てることができます。新しいIPアドレスは、DHCPサーバーから自動的に取得したり、IPアドレス範囲から割り当てて取得したりできます。

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アドレスの割り当てで1台のデバイスを選択する場合、[**詳細設定**] をクリックすると、[IPアドレスの割り当て] ページが開きます。
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 5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。
   - 新しいIPアドレス、サブネットマスク、デフォルトルーターが [現在のIPアドレス] セクションに表示されます。
   - [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 69*を参照してください。

- デバイスの設定方法については、「 *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

デバイスを設定するには数種類の方法があります。AXIS Device managementは、設定の方法に基づいてすべてのデバイスを構成しようとします。*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、既存の設定を一部またはすべてを再利用することで、単一のデバイスの設定でのみ使用できます。

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、**[デバイスの設定]** - **[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 61*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、**[デバイスの設定]** - **[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 61*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した設定ファイルを、モデルまたはファームウェアの異なる複数のデバイスに適用することができます。一部の設定が、すべてのデバイスに存在するわけではない場合でも可能です。

設定が適用先の装置に存在しなかったり、設定を適用できない場合は、AXIS Camera Station 5クライアントの一番下にある [Tasks (タスク)] タブに「Error (エラー)」というステータスが表示されます。その場合、タスクを右クリックし、[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、**[デバイスの設定]** - **[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 60*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。これらの設定は後で他のデバイスに適用できます。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。

表示される設定は、AXIS Device managementを使用してアクセスすることが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

パラメーターとは、デバイスの動作を制御する内部的なデバイスパラメーターです。パラメーターの全般的な情報は、Axisのホームページ (*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。
- AXIS Device managementから、すべてのデバイスパラメーターにアクセスできるわけではありません。

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。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。

- **変数として、製品のシリアル番号を入力してください:** 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。
- **変数として、デバイス名を入力してください:** 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、「デバイスの管理」ページの [名前] 列で確認できます。デバイスの名前を変更するには、[カメラ] または [他のデバイス] ページを選択します。
- **変数として、サーバー名を入力してください:** 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、「デバイスの管理」ページの [サーバー] 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 5 Service Controlに移動します。
- **変数として、サーバーのタイムゾーンを入力してください:** 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

- **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および画像や音声の設定用に事前プログラムされているライブビューのプロファイルです。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。
- **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。

ユーザー管理

[設定] - [デバイス] - [管理] を選択すると、デバイスのユーザーを管理するための「デバイスの管理」ページが表示されます。

複数のデバイスに対して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は ⚠ で表示されます。個々のユーザーが別々のデバイスに別々の権限で存在する場合、各ユーザーは一度だけ表示されます。

注

アカウントは装置固有であり、AXIS Camera Station 5のユーザーアカウントとは関連付けられていません。

パスワードの設定

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装置では、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 5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にパスワードを設定するには:

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。

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 5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」セクションを参照してください。
4. [権限] フィールドのドロップダウンリストからユーザーのアクセス権を選択します。
   - **管理者:** 装置に無制限にアクセスできます。
   - **オペレーター:** ビデオストリーム、イベント、システムオプションを除くすべての設定にアクセスできます。
   - **閲覧者:** ビデオストリームにアクセスできます。
5. [PTZコントロールを有効にする] を選択すると、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なります。
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. [ユーザー] フィールド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. [検索する文字を入力] フィールドを使用すると、リスト内の特定のユーザーを検索できます。

ファームウェアのアップグレード

ファームウェアはAxis製品の機能を決定するソフトウェアです。最新のファームウェアをインストールすることで、最新の機能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 5を使用してダウンロードできるほか、ハードドライブまたはメモリーカード内のファイルからインポートすることもできます。AXIS Camera Station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 **(ダウンロード)** と表示されています。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。

- **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. 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. 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。[**はい**] をクリックして続行します。このことを確認済みで、再び表示されないようにするには、[**このダイアログを再表示しない**] を選択して [**はい**] をクリックします。
5. [ファームウェアのアップグレード] ダイアログには、装置モデル、各モデルの装置数、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一覧表示されます。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ています。
   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装置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。

日付と時刻の設定

Axisデバイスに日付と時刻を設定します。コンピューターの時刻またはNTPサーバーに同期するか、手動で設定することができます。

デバイスに日付と時刻を設定するには:

1. **[設定]** - **[デバイス]** - **[管理]** を選択します。
2. デバイスを選択して をクリックするか、右クリックして**[Set date and time (日付と時刻を設定)]**を選択します。
3. Axisデバイスの現在の日付と時刻が [**デバイスの時刻**] に表示されます。複数のデバイスを選択すると、[**デバイスの時刻**] が利用できなくなります。
4. タイムゾーンを選択します。
   - [**タイムゾーン**] ドロップダウンリストからAxis製品で使用するタイムゾーンを選択します。
   - 製品を使用している地域で夏時間が導入されている場合は、[**夏時間の調整を自動的に行う**] を選択してください。

注

タイムゾーンは、[**NTPサーバーと同期する**] または [**手動で設定する**] の時刻モードを選択している場合に設定できます。

5. [時刻モード] セクションで次のように実行します。

- [Synchronize with server computer time (コンピューターの時刻と同期する)] を選択して、製品の日付と時刻を、AXIS Camera Station 5サーバーがインストールされているサーバーコンピューターのクロックと同期させます。
- [NTPサーバーと同期する] を選択して、製品の日付と時刻をNTPサーバーに同期させます。フィールドに、NTPサーバーのIPアドレス、DNSまたはホスト名を入力します。
- [手動で設定する] を選択して、日付と時刻を手動で設定します。

6. [OK]をクリックします。

日付と時刻の設定

カメラアプリケーションのインストール

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。アプリケーションをインストールすることにより、検知、認識、追跡、カウントなどの機能を追加することができます。

AXIS Camera Station 5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。

ライセンスが必要なアプリケーションの場合は、ライセンスキーファイルをアプリケーションと同時にインストールすることも、装置の設定ページを使用して後からインストールすることもできます。

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。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。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カメラが動体追跡データを AXIS Camera Station 5に送信できるようにするアプリケーション。5.50～9.59のファームウェア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 5と組み合わせてのみ使用できます。

その他のアプリケーション - インストールを希望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. カメラに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

ダウングレードまたは上書きによって、デバイスのアプリケーション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、[ライセンスのインストール] 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のインストールで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IEE 802.1Xを有効にすると、AXIS Camera Station 5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、それらの証明書を装置に配布します。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 134*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 5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 > HTTPS > Enable/Update (セキュリティ > HTTPS > 有効にする/更新する)**] を選択して、装置でHTTPSを有効にするか、HTTPSの設定を更新します。
   - [**Security > IEEE 802.1X > Enable/Update (セキュリティ > IEEE 802.1X > 有効にする/更新する)**] を選択して、デバイスでIEEE 802.1Xを有効にするか、IEEE 802.1Xの設定を更新します。
   - [**Security > HTTPS > Disable (セキュリティ > HTTPS > 無効にする)**] を選択して、装置でHTTPSを無効にします。
   - [**Security > IEEE 802.1X > Disable (セキュリティ > IEEE 802.1X > 無効にする)**] を選択して、装置でIEEE 802.1Xを無効にします。

– [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とき、その証明書は1つの項目として表示されるだけです。その証明書を削除すると、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 5 はHTTPSを使用して装置に接続します。
	オフ	AXIS Camera Station 5 はHTTPを使用して装置に接続します。
	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	装置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	HTTPSはこのデバイスモデルではサポートされていません。
IEEE 802.1X	オン	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	装置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はこの装置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目的で使用されます。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ファイルを生成するには、このオプションを使用します。

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. [選択した製品のデータソース] セクションで次のように実行します。
   – [**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

   プリセットによっては、すべてのデバイスで使用できるわけではない場合があります。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. [名前を付けて保存] 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装置と通信する方法:

1. **[設定] - [デバイス] - [管理]** を選択します。
2. 装置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。

タグ

「デバイスの管理」ページで、タグを使用してデバイスをグループごとに分けて管理することができます。1台のデバイスに複数のタグを設定できます。

たとえばデバイスのモデルや場所に応じて、デバイスにタグを付けることができます。たとえば、カメラのモデルに応じたタグを付けると、特定のモデルの全カメラをすばやく見つけて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. **既存のタグを使用**] を選択してタグを選択するか、[**新しいタグを作成**] を選択してタグ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. [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. デバイスを選択します。デバイスを右クリックして、[**製品のタグの解除**] 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. [デバイスのタグ] ページで次のように実行します。
   - [**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 (装置)]ページを固定できます。
   - タグをクリックすると、このタグに関連付けられているすべての装置が表示され、[All devices (すべての装置)] をクリックすると、AXIS Camera Station 5に接続するすべての装置が表示されます。

– [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。装置の設定方法については、装置のユーザーマニュアルを参照してください。
4. タブを閉じると、装置が再読み込みされ、AXIS Camera Station 5で変更が実装されていることを確認できます。

制限事項

- サードパーティ製装置の自動認証はサポートされていません。
- サードパーティ製デバイスの一般的なサポートは保証できません。
- 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可能性があります。

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 38*を参照してください。

[Configuration (設定)] > [Devices (装置)] > [External data source (外部データソース)] の順に移動すると、すべての外部データソースが一覧表示されます。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 5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 5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 > Devices > Time synchronization(設定 > 装置 > 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 5に追加されている装置のリストが表示されます。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アンドドロップして、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。

- **名前:** 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。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 69*を参照してください。
- **MACアドレス:** デバイスのMACアドレス。
- **モデル:** デバイスのモデル。
- **有効:** 時刻同期が有効になっている場合に表示されます。
- **NTPソース:** 装置に設定されたNTPソースです。
  - **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)] から装置の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。
- **プライマリNTPサーバー:** 装置に設定されたプライマリNTPサーバーです。[Static (スタティック)] を選択した場合にのみ使用できます。
- **セカンダリNTPサーバー:** 装置に設定されたセカンダリNTPサーバーです。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。
- **サーバーの時間オフセット:** 装置とサーバーの時差です。
- **協定世界時:** 装置上の協定世界時です。
- **同期しました:** 時刻同期の設定が実際に適用された場合に表示されます。これは、ファームウェア9.1以降を搭載した装置にのみ適用されます。
- **次の同期までの時間:** 次の同期までの残り時間です。

Windows Timeサービス (W32Time) はNetwork Time Protocol (NTP) を使用して、AXIS Camera Station 5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。

- **サーバー:** Windows Timeサービスを実行している AXIS Camera Station 5サーバーです。
- **ステータス:** Windows Timeサービスのステータスです。`Running`または`Stopped`のいずれか。
- **NTPサーバー:** Windows Timeサービス用に設定されたNTPサーバーです。

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 larger than 2 seconds (サーバーとデバイスの時間差が2秒を超えた場合にアラームを送信する)	サーバーと装置の時間差が2秒を超えた場合にアラームを受信するには、このオプションを選択します。

ストレージの設定

[設定] - [ストレージ] - [管理] を選択して「ストレージの管理」ページを開きます。[Manage storage (ストレージの管理)] ページで、AXIS Camera Station 5に存在するローカルストレージとネットワークストレージの概要が表示されます。

リスト	
場所	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 • **ストレージ満杯:** ストレージが満杯です。ロックされていない最も古い録画が上書きされます。 • **利用不可:** ストレージ情報は、現在使用することができません。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。 • **データの割り込み:** AXIS Camera Station 5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 5に割り当てられたストレージ容量を使用しています。 • **権限がありません:** ユーザーには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。 • **容量不足:** ドライブの空き容量が15 GB未満であり、AXIS Camera Station 5はそれを少な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 5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 5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。 • **容量不足:**ディスクの合計サイズが32 GB未満であるため、AXIS Camera Station 5には十分ではありません。 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。 • **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。 • **低下:** RAIDシステム内のいずれかの物理ディスクが故障しています。ストレージからの録画と再生は引き続き可能ですが、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 (低下)**] から [**Syncing (同期)**] に変わります。 • **同期中:** RAIDディスクが同期されます。ストレージからの録画と再生は可能ですが、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。 • **故障:** RAIDシステムのいくつか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、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 73*で、[非インデックスファイルを収集する] 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よって使用されているストレージ容量は AXIS Camera Station 5には不明です。 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 5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

[設定] - [ストレージ] - [管理] を選択して「ストレージの管理」ページを開きます。このページで、録画を保存するフォルダーを指定することができます。ストレージがいっぱいにならないように、AXIS Camera Station 5が使用できる合計容量の最大割合を設定します。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 5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。
- システムアカウントを利用してサービスにログオンしている場合、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を選択します。
4. 共有ネットワークドライブを追加する場合は、[**共有ネットワークドライブ**] をクリックし、共有ネットワークドライブへのパスを入力します。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、[**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 5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 5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 5は容量を解放するために、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。

収集されたファイルは削除されませんが、録画ストレージの [**Non-indexed files (非インデックスファイル)**] フォルダーに収集され、配置されます。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 5は最初にサーバー、次にそのサーバーに接続された装置に、データを見つかった順序でフォルダーに配置します。

損失した特定の録画やログを探すか、容量を確保するために単にコンテンツを削除するかのどちらかを選択できます。

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 > Tasks (アラームとタスク > 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。

[設定] - [ストレージ] - [選択] を選択して [ストレージを選択する] ページを開きます。このページには、AXIS Camera Station 5内のすべてのカメラのリストが表示され、特定のカメラの録画を保存する日数を指定できます。選択すると、ストレージ情報が [録画ストレージ] の下に表示されます。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。
Address (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 69*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。
場所	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。
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。
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。

AXIS Camera Station 5にカメラを追加すると、すべてのカメラの録画ストレージが設定されます。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. **[適用]** をクリックします。

録画ストレージ	
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。
フェイルオーバー録画	AXIS Camera Station 5とカメラの接続が失われたときに録画をカメラのSDカードに保存する場合に選択します。接続が回復すると、フェイルオーバーによる録画が AXIS Camera Station 5に転送されます。 注 この機能は、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。
無制限	ストレージがいっぱいになるまで録画が保存されます。
制限付き	録画を保存する最大日数を設定する場合に選択します。 注 AXIS Camera Station 5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。

録画とイベントの設定

カメラを AXIS Camera Station 5に追加すると、自動的に動体録画または連続録画が設定されます。後からニーズに合わせて録画方法を変更するには、*録画の方法, on page 81*に移動します。

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。カメラが動きを検知したときのみ録画することで、連続録画に比べてストレージ容量を大幅に節約できます。[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。デフォルトは、[High (高)] プロファイルです。
6. スケジュールを選択するか、[New (新規)] 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. プリバッファおよびポストバッファの時間設定と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場合は、必ず事前に [Recording method (**録画方法**)] で [Motion detection (**動体検知**)] をオフにしてください。

プロフィール	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。
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)	連続する録画の回数を減らすための連続する2つのトリガーの時間間隔。この間隔内に追加のトリガーが発生した場合、録画は続行され、トリガー期間が再開始します。
アラームを上げる	カメラが動きを検知するとアラームを発します。

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。

動体検知の設定

連続録画の設定

連続録画は連続的に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、できるだけ動体検知録画を使用します。

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. 連続録画を使用するには、[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。

プロフィール	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。デフォルトは、[**High (高)**] 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	オンにし、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。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 81*を参照してください。

手動録画

手動で録画する方法の詳細については、*手動による録画*を参照してください。

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。

プロフィール	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。デフォルトは、[**High (高)**] 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。
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するかどうかを選択します。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、デフォルトでは無効になっています。
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。

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。ルールを利用して、I/Oポートからの信号、いたずら行為、またはAXIS Cross Line Detectionをトリガーとして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。

ルールによってトリガーされる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を使用すると、AXIS Camera Station 5への接続が失われた場合も録画を保存できます。フェイルオーバーによる録画を有効にすると、接続が20秒以上中断した場合、カメラが録画データをSDカードに保存します。カメラにはSDカードが挿入されており、機能が有効になっている必要があります。フェイルオーバーによる録画は、すべてH.264の録画形式となります。

フェイルオーバーによる録画をオンにするには、次のとおりにします。

1. **[設定] - [ストレージ] - [選択]** を選択します。
2. フェイルオーバーによる録画をサポートするカメラを指定します。
3. **[Failover recording (フェイルオーバーによる録画)]** を選択します。
4. [**適用**] をクリックします。

注

- AXIS Camera Station 5サーバーの再起動は、フェイルオーバーによる録画をトリガーしません。たとえば、データベースメンテナンスを実行する場合、AXIS Camera Station 5 Service Controlを再起動する場合、サーバーがインストールされているコンピューターを再起動する場合などです。
- フェイルオーバーによる録画を有効にすると、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、各カメラビューで一度に1台の AXIS Camera Station 5サーバーでのみ有効になります。

接続が回復すると、AXIS Camera Station 5がフェイルオーバーによる録画を自動的にインポートし、タイムライン上に濃いグレーで表示します。

カメラは録画の中断を最小限に抑えるため、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、それでも約1〜4秒の短い中断が発生することがあります。フェイルオーバーによる録画には、ハイストリームプロファイルが常に使用されます。カメラで音声が有効になっており、フェイルオーバーがオンになる前のストリームの一部である場合、音声が含まれます。

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。

注

AXIS OSバージョン11.11.42より前のバージョンを実行しているデバイスは、従来のフェイルオーバーによる録画方式を使用します。主な違いは以下の通りです。

- カメラは接続が切断されてから10秒後にフェイルオーバーによる録画を開始します。
- カメラは20秒間のプリバッファとポストバッファの代わりに、10秒間の内蔵メモリバッファを使用します。

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。代替録画をオンにすると、AXIS Camera Station 5とレコーダーの接続が失われたときに、装置は連続録画を開始します。装置は、フォールバック録画に中程度のストリームプロファイルを使用します。

注

- 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、Axis装置ファームウェア5.50以降が必要です。
- 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と装置が追加され、レコーダーが装置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

AXIS Camera Station 5 に装置を追加すると、自動的に動体録画または連続録画が設定されます。

リスト内のチェックマークは、装置が使用する録画方法を示します。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、指定されたストレージに基づいて、目的のビットレートを満たし、良好な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にのみ対応し、平均ビットレートに対応したカメラでファームウェア9.40以降を使用している必要があります。
- 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 > Storage > Selection (設定 > ストレージ > 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。録画が指定されたスペースを超えないことを保証するだけであり、録画に十分なスペースがあることは保証されません。

7. [**適用**] をクリックします。

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をサポートする製品にインストールできる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 5にカメラを追加する際に動体録画を選択すると、対応の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のインストール*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。

- **対象範囲**:録画内の1つの領域で、カメラがここで移動物体を検知します。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。
- **除外範囲**:対象範囲内のエリアで、移動物体を無視する場所です。
- **無視フィルター**:アプリケーションが検知した移動物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。
  - **一時的な物体**:このフィルターは、短い時間しか画像に現れない物体を無視します。たとえば通り過ぎる車のライトや、素早く移動する影などです。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。開始時間は、アプリケーションが物体を検知した瞬間です。このフィルターはアラームが発生するまでの時間を遅らせます。指定した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。
  - **小さな物体**:このフィルターは、小動物など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、アラームはトリガーされません。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。
  - **揺らめいている物体**:このフィルターは、揺らめいている葉、旗、その陰など、短い距離しか移動しない物体を無視します。移動の距離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、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

ここで行う設定は、カメラの設定を変更します。

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、[**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)	一時的な物体を無視する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)] を選択します。次に **[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を無視する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)]** を選択してから、**[Distance (距離)]** スライダーを使用して楕円のサイズを調整します。

内蔵動体検知機能の編集

内蔵動体検知機能を使用すると、カメラは1つ以上の対象範囲内の動きを検知します。また、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。対象範囲の中に除外範囲を配置して、動きを無視することができます。対象範囲、および除外範囲は、複数使用することが可能です。

対象範囲の追加、編集手順:

注

ここで行う設定は、カメラの設定を変更します。

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. 編集した領域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 (物体のサイズ)]**、**[History (履歴)]**、**[Sensitivity (感度)]** を手動で調整します。
8. 既定の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。

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 5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 5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接続中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 5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 5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。

装置の接続方法、I/Oポートの設定方法については、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。必要に応じて情報を変更します。
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. AXIS Camera Station 5が装置に接続するときの初期状態を出力ポートに設定できます。**[On startup set to (起動時設定)]** を選択し、**[State (状態)]** 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、ポートを選択して [**編集**] をクリックします。ポップアップ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 [**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)	装置の設定ページを使用して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 5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任意の接続中サーバーを選択して、I/Oポートを監視できます。

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 5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。多数のアクションについて、装置に追加の設定が必要となることがあります。

トリガーの追加

トリガーはルールをアクティブにします。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、トリガー期間を長くします。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 87*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。

いたずら警告 - いたずらトリガーは、装置の位置が変更される、何かがレンズを覆う、レンズのフォーカスが大幅にずれた場合にアクティブになります。*いたずら警告トリガーの作成, on page 87*を参照してください。

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。を参照してください。

AXIS Cross Line Detection - AXIS Cross Line Detectionは、カメラおよびビデオエンコーダ用のアプリケーションです。このアプリケーションは、バーチャルラインを横切る被写体を検知します。したがって、出入口の監視などに使用できます。*AXIS Cross Line Detectionトリガーの作成, on page 88*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、ストレージが一杯になった、ネットワークストレージへの接続に失敗した、1台以上の装置が接続不能などの場合、システムイベントとエラートリガーがアクティブになります。*システムイベントとエラートリガーの作成, on page 88*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 89*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、装置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 5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 90*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 95*を参照してください。

AXIS Entry Managerイベント - AXIS Camera Station 5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 96*を参照してください。

外部HTTPS - 外部HTTPSトリガーは、外部アプリケーションが AXIS Camera Station 5でHTTPS通信を介してイベントをトリガーできるようにします。*外部HTTPSトリガーの作成, on page 97*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 5に処理負荷は生じません。

注

カメラの動体録画と、動体検知トリガーを使った録画開始設定を併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. ポップアップ画面で、次のとおりに設定します。
   5.1. 動体検知を実行するカメラを指定します。
   5.2. 連続する2つの録画の時間間隔を設定すると、連続する録画の回数を減らすことができます。この間隔内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。

いたずら警告トリガーの作成

いたずら警告トリガーは、カメラの位置が変更される、何かがレンズを覆う、レンズのフォーカスが大幅にずれた場合にアクティブになります。装置がいたずら検知処理を行うため、AXIS Camera Station 5サーバーに処理負荷は追加されません。

いたずら警告トリガーは、カメラに対するいたずらがサポートされており、かつファームウェアが5.11以降であるカメラで使用することができます。

いたずら警告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、[**いたずら警告**] を選択します。
4. [OK] をクリックします。
5. **Trigger on (トリガーをオン)** - 使用するカメラを選択します。

6. [OK] をクリックします。

AXIS Cross Line Detectionトリガーの作成

AXIS Cross Line Detectionは、カメラおよびビデオエンコーダ用のアプリケーションです。仮想ラインを越えて動く物体を検知すると、トリガーをアクティブにします。たとえば、入口と出口の監視に使用することもできます。カメラが検知処理を行うため、AXIS Camera Station 5サーバーに処理負荷を追加しません。

このアプリケーションは、AXIS Camera Application Platformをサポートする装置にのみインストールできます。AXIS Cross Line Detectionをトリガーとして使用するには、*axis.com*からこのアプリケーションをダウンロードし、装置にインストールする必要があります。*カメラアプリケーションのインストール*を参照してください。

AXIS Cross Line Detection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 [**AXIS Cross Line Detection**] を選択します。
4. [OK] をクリックします。
5. **更新**] をクリックすると、リストが更新されます。
6. [**Trigger on (トリガーをオン)**] ドロップダウンメニューから使用するカメラを選択します。
   AXIS Cross Line Detectionがインストールされているカメラのみを選択できます。
7. [**Trigger period (トリガー期間)**] で、連続する2つのトリガーの間隔を設定して、連続する録画の回数を減らします。
   この間隔内に追加のトリガーが発生した場合、録画は続行され、トリガー期間が再開始します。
8. [**AXIS Cross Line Detection settings (AXIS Cross Line Detectionの設定)**] をクリックして、Webブラウザーでカメラの [**Applications (アプリケーション)**] ページを開きます。使用できる設定の詳細についてはは、AXIS Cross Line Detectionに付属するドキュメントを参照してください。

注

AXIS Cross Line Detectionを設定するには、Internet Explorerを利用し、ActiveXコントロールを許可するよう設定する必要があります。AXIS Media Controlをインストールするよう求められた場合は、[**Yes (はい)**] 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としては、録画エラーが発生した、ストレージが一杯になった、ネットワークストレージへの接続に失敗した、1台以上の装置が接続不能などがあります。

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したときに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あ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 5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 5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)**] を使用してすべてのカメラを選択したり、[**Deselect all (すべて選択解除)**] を使用してすべてのカメラの選択を解除したりできます。

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 5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、装置イベントトリガーを使用します。装置イベントトリガーを使用すると、ユーザーエクスペリエンス全体が向上します。詳細については、*デバイスイベントトリガーの作成, on page 90*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)	[Trigger period (トリガー期間)] で、連続する2つのトリガーの間隔を設定して、連続する録画の回数を減らします。 この間隔内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 5に目的に合った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。フィルターとは、装置イベントトリガーをアクティブにするために満たすべき条件です。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、経過時間に応じた装置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。ステップ関数は、ステートフルイベントのアクティビティを表します。イベントがトリガーされた時点からのパルスを含む直線は、ステートレスイベントのアクティビティを表します。
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)	[Trigger period (トリガー期間)] で、連続する2つのトリガーの間隔を設定して、連続する録画の回数を減らします。 この間隔内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	ネットワーク接続断絶 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 5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	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	誰かが強制PINを使用しました。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。
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。

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	システムが準備完了の状態になった。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。[**はい**] を選択した場合、本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にしかトリガーできません。
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とき: • 装置のケーシングが開閉された • 装置の動き • 壁に取り付けられたリーダーが取り外された • 接続されているドアモニター、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、監視入力をオンになっていて、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、認証情報を提示せずにドアを開くことを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てください。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	ネットワークの接続が失われました。 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 5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	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。アクションボタンを追加または編集する際に、カメラに配置する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。ツールチップは、ボタンにマウスポインターを合わせると表示されます。

例： 既定の時間で出力をアクティブにし、アラームを鳴らして、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。ツールチップは、ボタンにマウスポインターを合わせると表示されます。

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

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同時に押します。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キーを同時に押すとアクションボタンが起動します。

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使用することを選択した場合は、[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 5 AXIS Entry Managerで設定済みのドアから信号を受信したときに、によって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、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 5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トリガーは、外部アプリケーションが AXIS Camera Station 5でHTTPS通信を介してイベントをトリガーできるようにします。このトリガーはHTTPS通信のみをサポートし、HTTPS要求で、ドメイン名とパスワードを含む有効な AXIS Camera Station 5のユーザー名の提供を要求します。

以下の要求は、HTTPメソッドGET*で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。「*概要*」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]:55756/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]:55756/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]:55756/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]:55756/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. ログオン時にクライアントが使用したものと同じサーバーアドレスをサンプルURLが使用することを確認します。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。

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。

録音 - このアクションは、カメラから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。

アラームを上げる - このアクションは、すべての接続済みの AXIS Camera Station 5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 - この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装置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)。*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 - このアクションは、1人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。

HTTPで通知を送る - このアクションは、カメラ、ドアコントローラー、外部のWebサーバーなどに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 - このアクションは、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 104*を参照してください。

AXIS Entry Manager - このアクションは、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の許可、ロック解除またはロックを行うことができます。*AXIS Entry Managerアクションの作成, on page 104*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 104*を参照してください。

ルールをオン/オフにする - このアクションルールを使用して、他の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 105*を参照してください。

ビデオデコーダに送信する - 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。を参照してください

アクセスコントロール - このアクションには、AXIS Camera Station Secure Entryでのドアアクションとゾーン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 105*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. 録画を保存する場所を指定するには、**[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. **[OK]**をクリックします。

映像設定	
プロフィール	[**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選択します。

「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 5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)**] タブに表示されるほか、タスクバーにも通知が表示されます。アラームには、アラーム手順を含む指示をファイルの形で含めることができます。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. [**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。
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、期間を設定します。
7. [**Alarm procedure (アラーム手順)**] で:
   7.1. **アラーム時にアラームガイドを表示**] を選択します。
   7.2. [**Upload (アップロード)**] をクリックし、目的のファイルを見つけます。
   7.3. [**プレビュー**] をクリックすると、アップロードするファイルがプレビューウィンドウに表示されます。
   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))	ポップアップアラームの継続時間を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装置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 5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. [**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。
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. [**パルス**] を選択して、新しいステータスに出力ポートを維持する時間を定義します。

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状態に維持するには、2番目のオプションを選択し、秒数を指定します。

メール送信アクションの作成

メールアクションは、1人以上の送信先にメールを送信します。カメラからのスナップショットを電子メールに添付できます。

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. [**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。
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)] で、送信先を追加します。
   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. [Add (追加)] をクリックして、メールアドレスを [Recipients (送信先)] に追加します。
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)	カメラからの.jpgスナップショットを電子メール通知に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 5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)] ですべてのカメラを選択したり、[Deselect all (すべて選択解除)] ですべてのカメラの選択を解除したりできます。
Send one email for each event (イベントごとに電子メールを一通送信)	同じイベントに対して複数のメールを送信しないようにするには、[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 (次のアドレスに別の電子メールを送信しない)	メールを短い間隔で続けて送信しないようにするには、[Don't send another email for (新規の電子メールを送信しない時間間隔)] を選択して、電子メールを送信する最小の時間間隔をドロップダウンメニューから設定します。

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、特定のカメラ、ビュー、またはプリセットポジションで [Live view (ライブビュー)] タブを開きます。接続されているすべてのクライアントで [Live view (ライブビュー) AXIS Camera Station 5] タブが開きます。[Live view (ライブビュー)] タブでホットスポット付きの分割ビューを表示する場合、ライブビューアクションで選択したカメラの映像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 5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. [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。
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 5クライアントをタスクバーからリストアするか、ライブビューアクションの開始時に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	ビューを開くには、[View (ビュー)] を選択してから、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	カメラビューを開くには、[Camera (カメラ)] を選択してから、ドロップダウンメニュー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1つ選択してプリセットポジションを開きます。
No action (アクションなし)	[No action (アクションなし)] を選択すると、どのビューも開きません。

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ると、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:
[Live view (ライブビュー)] タブを開くには、ホットスポットビューに移動し、ホットスポットにカメラビューを表示して、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設定します。

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、[camera view (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要求を受信可能なサーバーを送信先にすることができます。HTTP通知を使用して、カメラの特定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を開閉、ロック、ロック解除したりできます。

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 5サーバーのプロキシ設定の調整が必要になる場合があります。*概要*を参照してください。

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. [**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。
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. [**詳細設定**] をクリックして、詳細設定を表示します。
9. [OK] をクリックします。

高度	
方式	[**Method (メソッド)**] 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。詳細については下記を参照してください。

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)	ソースIDは、アクションルールをトリガーしたソースのIDであり、多くの場合、カメラなどの装置を表します。すべてのソースにソースIDがあるわけではありません。
Source Name (ソース名)	ソース名は、アクションルールをトリガーしたソースの名前であり、多くの場合、カメラなどの装置を表します。すべてのソースにソース名があるわけではありません。
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。

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. [**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。
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 5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. [**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。
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. アクションとアクション実行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。受信した通知をクリックすると、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. [**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。
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、通知をクリックしたときに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	モバイルアプリの通知をクリックしたときに表示するカメラビューを [**Camera (カメラ)**] ドロップダウンメニューから選択します。
デフォルト	[**Default (デフォルト)**] を選択すると、モバイルアプリで通知をクリックしたときに、モバイルアプリの開始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

たとえば、従業員がアクセスカードをスワイプしたときに、オフィスの動体検知をオフにする場合に、ルールをオン/オフにするアクションを使用します。

ルールをオン/オフにする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. [**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。
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. トリガーから状態変更までに間隔が必要な場合は、遅延を入力します。
9. トリガーがアクティブでなくなったときに、選択した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。

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システムで次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、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、ロックダウン。

注

アクセスコントロールアクションは、AXIS Camera Station Secure Entryシステム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。
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. [OK] をクリックします。

スケジュール

[Schedules (スケジュール)] のページには、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含まれています。AXIS Site Designerは、インストール中にいくつかのスケジュールを作成します。

スケジュール機能では、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に加え、スケジュールの上書きも行えます。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。

- **名前**: スケジュール名。
- **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表示します。
- **Override schedules (オーバーライドスケジュール)** : 該当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、適用されている日次スケジュールと週次スケジュールを確認できます。

注

複数の AXIS Camera Station 5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)] 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。削除する前にそのスケジュールが使用中で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

ここでは、誰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 5で設定する方法を例示します。

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 41* 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 141*。

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のトリガーを追加します。
   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、トリガーの信号ラインにアクティビティが示され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。

映像設定	
プロフィール	[Profile (プロファイル)] ドロップダウンメニューから [High (ハイ)] 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
ここでは、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 5で作成する方法を例示します。

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および設定し、カード保有者を追加します。「*アクセスコントロールの設定, on page 139*」および「*アクセス管理, on page 164*」を参照してください。

- Axisネットワーク音声装置を取り付けて、音声装置をカメラに関連付けます。*ストリームプロファイル, on page 49*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 5に追加します。*I/Oポート, on page 84*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. デバイスイベントトリガーを追加します。
   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、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、トリガーの信号ラインにアクティビティが示され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ために、HTTP通知を送信するアクションを追加します。
   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します。
   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)**] 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)]** を選択して、ポートの状態を60秒維持するように設定します。
   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、重要人物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、

- テーマや言語のような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 110*を参照してください。
- 通知や起動オプションのようなユーザー固有の設定を編集します。*ユーザー設定, on page 111*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、クライアントの特定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 113*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 5ユーザーに適用されます。[Configuration > Client > Client settings (設定 > クライアント > クライアント設定)] に移動し、AXIS Camera Station 5クライアント設定を行います。

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のテーマです。 [System (システム)] を選択すると、Windowsシステムテーマに応じて、明るいテーマまたは暗いテーマが使用されます。

概要	
Windowsの起動時にアプリケーションを起動	Windowsが起動するたびに AXIS Camera Station 5を自動的に実行する場合は、オンにします。

ライブビュー	
ライブビューにカメラ名を表示する	ライブビューでカメラの名前を表示します。
	録画のタイプを示すには、[Show recording indicators in live views and maps (ライブビューとマップに録画インジケーターを表示する)] をオンにします。
	動体検知録画であるか、アクションルールによって開始された録画であるかを示すには、[Show event indicators in live views and maps (ライブビューとマップにイベントインジケーターを表示する)] をオンにします。

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)	[Flash (点滅)] を使用したすべての検知範囲の点滅をグローバルに禁止または許可するために使用します。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 20*を参照してください。

言語
AXIS Camera Station 5クライアントの言語を変更します。変更は、クライアントの再起動後に有効になります。

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。サーバーのオプションを変更するには、*サーバーの設定, on page 119*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 5ユーザーに適用されます。
[Configuration > Client > User settings (設定 > クライアント > ユーザー設定)] に移動し、AXIS Camera Station 5クライアントユーザーの設定を行います。

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	デフォルトでオンになり、ツリー表示のナビゲーションペインにビューとカメラが表示されます。
Show in navigation (ナビゲーションに表示)	選択すると、ドロップダウンメニューでビューまたはカメラ、またはその両方が表示されます。
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、誰かがタスクを追加したとき、またはタスクが完了したときにWindowsタスクバーに通知が表示されます。
[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、誰かが接続されたインターカムシステムの通話ボタンを押したときに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、スナップショットを保存するフォルダーを選択します。

起動	
全画面で開始する	オンにすると、AXIS Camera Station 5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、AXIS Camera Station 5の前回終了時に開いていたのと同じタブ、ビュー、カメラビューで AXIS Camera Station 5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、AXIS Camera Station 5の前回終了時に使用していたのと同じモニターで AXIS Camera Station 5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。これらは、クライアントが同じサーバーに再接続した場合にのみ記憶されます。
- モニター、ビュー、カメラビューを記憶するためにタブを記憶します。
- 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	アラームで通常のビープ音を鳴らさないようにする場合に選択します。

アラーム時に音を鳴らす	
Sound file (サウンドファイル)	アラーム音をカスタマイズする場合は、これを選択して、[Browse (参照)] をクリックして、サウンドファイルを見つけます。Windows Media Playerがサポートしているファイル形式を使用してください。
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)	着信時にサウンドを鳴らさないようにする場合に選択します。
Beep	着信時に通常の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)	着信音をカスタマイズする場合は、これを選択して、[Browse (参照)] をクリックして、サウンドファイルを見つけます。Windows Media Playerがサポートしているファイル形式を使用してください。
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	デフォルトでは、スマート検索1が表示されます。この機能を非表示にするには、オフにします。

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、条件に該当する場合にこの警告が表示されます。

ストリーミング

[Configuration > Client > Streaming (設定 > クライアント > ストリーミング)] を選択して、AXIS Camera Station 5クライアントの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	ビデオを使用可能な領域全体に表示する場合に選択します。ビデオのアスペクト比が崩れたり、画像がトリミングされたりすることはありません。
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)	ビデオを使用可能な領域に合わせて表示する場合に選択します。ビデオのアスペクト比が保持されます。使用可能な表示領域のアスペクト比がビデオと異なる場合、ビデオの一部がトリミングされます。

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 (サポートされている場合) を使用して、3840x2160p@25fps (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 (サポートされている場合) 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)** ハードウェアデコーディングはオフになり、AXIS Camera Station 5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。

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。高性能のグラフィックカードを搭載している場合、特に高解像度ビデオをストリーミングする場合、ハードウェアデコーディングは性能を改善してCPU使用率を下げる優れた方法です。ハードウェアデコーディングはM-JPEGおよびH.264をサポートします。
- 解像度が1080p未満のカメラは、ハードウェアデコードが [**On (オン)**] であっても、ハードウェアデコードを使用できません。
- グラフィックカードが4Kデコードをサポートしていない場合、ハードウェアデコードが [**On (オン)**] であっても、ハードウェアデコードは1080pのストリームでのみ機能します。

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ビデオに影響し、帯域幅の使用量が少なくなります。
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、帯域幅の使用量が少なくなります。

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、ビューで初めてクリックしたときに、ビューの選択がアクティブになります。ビューで行うその後すべてのクリックで、PTZを制御できます。

音声	
Push-to-talk release delay (ms) (Push-To-Talkのリリース遅延 (ミリ秒))	[Push-to-talk (プッシュツートーク)] ボタンを離した後マイクから送信される音声を何ミリ秒間保持するかを調整します。
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、インターカムからの通話がない場合でも、インターカムで聞いたり話したりできるようになります。

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

ファームウェアアップグレード設定

注

複数の AXIS Camera Station 5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)	利用可能なファームウェアバージョンを起動時に毎回確認するには、[Check for updates (更新を確認する)] ドロップダウンメニューから [Every start-up (起動時に毎回)] を選択します。デフォルトでは、AXIS Camera Station 5は [Never (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セキュアリモートアクセス

重要

セキュリティおよび機能性の向上を目的として、**Axis Secure Remote Access (v1)** を**Axis Secure Remote Access v2** へアップグレードします。現行バージョンは2025年12月1日をもって提供終了となる予定のため、それまでにAxis Secure Remote Access v2へのアップグレードを強くお勧めします。

お使いの AXIS Camera Station 5システムへの影響：

- 2025年12月1日以降、**Axis Secure Remote Access (v1)**を使用してシステムにリモートアクセスすることはできなくなります。
- **Axis Secure Remote Access v2**を使用するには、AXIS Camera Station Proバージョン6.8にアップグレードする必要があります。このアップグレードは、2026年3月1日まで、AXIS Camera Station 5をご利用中のすべてのユーザーに無料で提供されます。

Axis Secure Remote Accessを使用すると、暗号化された安全なインターネット接続経由で AXIS Camera Station 5サーバーに接続できます。Axis Secure Remote Accessは、ルーターのポートフォワーディングに依存せずにカメラにアクセスします。

注

- Axisセキュアリモートアクセスは、AXIS Camera Station 5.12以降でのみ利用可能です。
- 複数の AXIS Camera Station 5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任意のサーバーを選択して、Axis Secure Remote Accessを設定します。

Axisセキュアリモートアクセスの有効化

Axisセキュアリモートアクセスを有効にするには、お使いのMy Axisアカウントでサインインしてください。Axis Secure Remote Accessは手動でオンにする必要があります。この機能により、サーバーにリモートでサインインできるようになります。*サーバーとの接続*を参照してください。

1. **[設定] - [接続中のサービス] - [Axisセキュアリモートアクセス]** を選択します。
2. [My Axis account (My Axisアカウント)] で、My Axisアカウントの認証情報を入力します。
3. [**適用**] をクリックします。
4. [Axis Secure Remote Access] セクションで、[**Enable (有効にする)**] をクリックしてリモートアクセスをオンにします。

モバイルデバイスでのAxisセキュアリモートアクセスの有効化

モバイル装置 (iOSおよびAndroid) でセキュアリモートアクセスを使用してサーバーにログインするには:

1. モバイル装置を使用して*axis.com/products/axis-camera-station/overview*にアクセスし、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. リモートアクセスのアクティブ化に使用したものと同じMy AxisアカウントでAxis Secure Remote Access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。

モバイルアプリには、My Axisアカウントで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。

Axisセキュアリモートアクセスの使用

AXIS Camera Station 5クライアントの下部にあるステータスバーにAxis Secure Remote Accessの使用状況が表示されます。リンクをクリックすると、セキュアリモート接続がどのように使用されているかについて概要を見ることができます。

サービスレベル	Axisセキュアリモートアクセスサブスクリプションのサービスレベルを表示します。
今月に使用したデータ	今月使用したデータ量を表示します。カウンターは毎月1日の午前0時までにリセットされます。
超過	今月使用したデータのうち、サービスレベルに含まれる量を超過したデータ量を表示します。これはサブスクリプションに超過が含まれる場合にのみ利用できます。
接続	Secure Remote Accessを介して接続されているサーバーを表示します。

AXISのシステムの健全性監視クラウドサービスの設定

AXISのシステムの健全性監視クラウドサービスを使用すると、別のネットワーク上にあるシステムの健全性データを監視できます。詳細については、*組織, on page 118*を参照してください。

AXISのシステムの健全性監視クラウドサービスを設定する前に、My Axisアカウントを作成する必要があります。*my.axis.com*を参照してください。

1. [**Configuration System Health Monitoring > Settings (設定 > システムの健全性監視 > 設定)**] に移動します。
2. [**Manage (管理)**] をクリックします。
3. 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。

組織

組織はクラウドサービスの中心にあります。

- 組織は、AXIS Camera Station 5システムをさまざまなクラウドサービスのユーザーに接続します。
- クラウドベースのシステムの健全性監視をアクティブにします。詳細については、*AXISのシステムの健全性監視クラウドサービスの設定, on page 117*を参照してください。
- 組織は、サービス管理者やオペレーターなど、さまざまなユーザー権限を定義します。
- 組織は、さまざまなサイトにあるシステムを表すフォルダーなどに構成できます。組織を作成するには、My Axisアカウントが必要です。*my.axis.com*を参照してください。

組織からシステムを切断する

場合によっては、システムを現在の組織から切り離す必要があります。たとえば、システムをある組織から別の組織に移動する場合です。

1. [Configuration (設定)] > [Connected services (接続中のサービス)] > [AXIS System Health Monitoring Cloud Service (AXISシステムの健全性監視クラウドサービス)] に移動します。
2. [Disconnect (切断)] をクリックします。

ユーザーを組織に招待する

1. [Configuration (設定)] > [System Health Monitoring (システムの健全性監視)] > [Settings (設定)] に移動します。
2. [Open AXIS System Health Monitoring Cloud Service (Axisのシステムの健全性監視クラウドサービスを開く)] をクリックします。
3. ユーザーを招待する組織を選択します。
4. ユーザー設定を開き、[Manage organizations (組織の管理)] をクリックします。
5. [Users (ユーザー)] タブを開きます。
6. [Generate (生成)] をクリックします。
7. 招待コードをコピーし、招待するユーザーに送信します。

注
招待コードをユーザーと共有するときは、招待する組織の名前も含めます。

組織に参加する

誰かに組織への参加を望まれると、招待コードが届きます。組織に参加するには:

1. 招待コードをコピーします。
2. [Configuration (設定)] > [System Health Monitoring (システムの健全性監視)] > [Settings (設定)] に移動します。
3. [Open AXIS System Health Monitoring Cloud Service (Axisのシステムの健全性監視クラウドサービスを開く)] をクリックします。
4. ユーザーを招待する組織を選択します。
5. ユーザー設定を開き、[Manage organizations (組織の管理)] をクリックします。
6. [Users (ユーザー)] タブを開きます。
7. 招待コードを貼り付けます。
8. [Join (参加)] をクリックします。

サーバーの設定

サーバーの設定

AXIS Camera Station 5サーバー設定を行うには、[**Configuration > Server > Settings (設定 > サーバー > 設定)**] を選択します。

注

複数の AXIS Camera Station 5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任意のサーバーを選択して、サーバー設定を行います。

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。

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

システムアラームまたはイベント設定ルールがアクティブになったとき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)**] に、送信者の電子メールに表示するメールアドレスと名前を入力します。

サーバー	
Address (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	このサーバーにユーザー名とパスワードが必要かどうかを選択します。サーバーへのアクセスに使用するユーザー名およびパスワードを入力します。

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。ポップアッ

	プダイアログで [**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。ポップアップダイアログの **[Recipient (送信先)]**にメールアドレスを入力し、**[OK]**をクリックするとテストメールが送信されます。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、矢印を使用してリスト内のサーバーの順序を変更します。システムは、一覧表示されているのと同じ順序でサーバーを使用します。

サーバーテストの結果	
OK	SMTPサーバーと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	メールの送信時に予期しない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 5 は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 5とSMTPサーバー間のすべてのルーターとプロキシ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。
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	無効なサーバー証明書など、TLS/SSLネゴシエーション中に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	認証情報が正しくありません。
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

システムアラームは、カメラが接続を失った場合、録画ストレージへのアクセスが拒否された場合、予期しないサーバーのシャットダウンが発生した場合、または録画エラーが発生した場合に発生します。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. [**システムアラーム発生時に以下の受信者にメールを送信する**] を選択してシステムアラームメールを有効にします。
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. [**追加**] をクリックして、入力したメールアドレスを [**送信先**] ボックスに追加します。

デバイス接続	
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。IPアドレスを使用した接続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 68*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 5 Service ControlおよびAXIS Camera Station Secure Entryの名前を変更します。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。変更は再起動後に有効になります。

装着式	
ディスク **フォルダー**	装着式システムから却下されたコンテンツを受信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「却下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却下されたコンテンツを保存する日数。	却下されたコンテンツの保存期間です。

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	Axisによるアプリケーションとユーザーエクスペリエンスの向上に協力する場合に選択します。クライアントのオプションを変更するには、*クライアント設定, on page 110*を参照してください。

高度な設定

設定の変更は、Axisサポートから指示があった場合にのみ行ってください。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目的でデバッグログをアクティブにするには、[**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。この設定ではディスクのより多くの容量が使用されるため、ProgramDataディレクトリ内の`log4net.config`ファイルによってこの設定は上書きされます。

AXIS Camera Station 5の更新

AXIS Camera Station 5の最新バージョンを入手するには:

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

- 手動によるかスケジュールによるかに関わらず、いったん開始した更新は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。
- セキュアリモートアクセスを介して接続されたクライアントは更新されません。
- 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制御は一時的に終了します。更新中は、UIや進行状況の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。
- この機能は、現在使用しているタイプに関係なく、Windowsインストーラー (msi) を使用します。

事故レポート

事故レポートの権限がオンになっている場合は、事故に関する録画、スナップショット、メモを含む事故レポートを生成することができます。*事故レポートのエクスポート, on page 30*を参照してください。

以下の手順で事故レポートを設定します。

1. [Configuration > Server > Incident report (設定 > サーバー > 事故レポート)] に移動します。
2. [Location (場所)] で、事故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)] ドロップダウンメニューから、録画のエクスポート先の形式を選択します。
4. [Categories (カテゴリー)] で、カテゴリーを追加または削除して、事故レポートをグループ化できます。カテゴリーをサーバーディレクトリパスの変数として設定した場合、カテゴリーをエクスポート先のフォルダー名とすることができます。
   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、事故レポート生成時に [Description (説明)] に表示する情報を入力します。例:報告者:<名前、メール、電話番号を挿入します>。
6. [適用] をクリックします。

場所	
Server directory path (サーバーディレクトリパス)	事故レポートをコンピューターのフォルダーに保存する場合に選択して、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)	事故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 5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	[Add digital signature (デジタル署名を追加)] を選択して、デジタル署名を使用して画像の改ざんができないようにします。*録画のエクスポート*にある「デジタル署名」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。

選択した時刻に、前回のエクスポート以降のすべての録画のエクスポートが開始されます。前回のエクスポートが1週間より前に行われた場合、または前回のエクスポートがない場合は、過去1週間未満の録画のみがエクスポートされます。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 5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オンにして管理します。

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)] を選択して、エクスポートのスケジュールを使用します。
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。リストされているすべてのカメラはデフォルトとして選択されています。[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 5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)	録画をエクスポートする形式を選択します。 [ASF] - [Add digital signature (デジタル署名を追加)] を選択して、デジタル署名を使用して画像の改ざんができないようにします。*録画のエクスポート*にある「デジタル署名」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 2008 Server

Microsoft Windows 2008 Serverで動作するサーバーから録画をエクスポートするには、以下の手順でDesktop Experienceをインストールする必要があります。

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. [Features Summary (機能の概要)] で、[Add features (機能の追加)] をクリックします。
3. [Desktop Experience] を選択し、[Next (次へ)] をクリックします。
4. [インストール] をクリックします。

Microsoft Windows 2012 Server

Microsoft Windows 2012 Serverで動作するサーバーから録画をエクスポートするには、以下の手順でDesktop Experienceをインストールする必要があります。

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。

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 5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

サーバーの接続ステータスを表示するには、 > [Servers (サーバー)] > [Connection status (接続ステータス)]に移動します。

サーバー名の前にあるスライダーを使用して、サーバーに対する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 (セキュアリモートアクセスを使用)	このサーバーに接続している間、クライアントはSecure Remote Accessを使用します。	
接続 (HTTPを使用)	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	クライアントとこのサーバーの間に接続はありません。	
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	クライアントはこのサーバーとの再接続に失敗しました。サーバーは見つかっても、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。	• [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。	[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	

	ライアントコンピューターとサーバーコンピューターのUTC時刻を必ず同期させてください。	
サーバーコンピューターと接続できません	使用したアドレスのサーバーコンピューターから応答がありませんでした。	• ネットワークが正常に動作しているかどうかを確認します。 • サーバーが起動しているかどうかを確認します。
サーバーが動作していません	サーバーコンピューターに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。 • サーバーが起動しているかどうかを確認します。
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。	• ホスト名が正しいかどうかをチェックします。 • DNSに必要な情報が提供されているかどうかをチェックします。
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	想定されるサーバーとは異なるサーバーがこのアドレスで応答しました。	サーバーリストを更新し、このサーバーに接続します。
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、サーバーコンピューターの両方に、同じバージョンの AXIS Camera Station 5がインストールされているかどうかを確認します。
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かどうかを確認します。

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。

マルチサーバー

サーバーリスト

AXIS Camera Station 5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 5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)]に移動して、[Server lists (サーバーリスト)]ダイアログを開きます。

[Recent connections (最近の接続)] リストがデフォルトで表示されます。このリストには、以前のセッションで使用されたサーバーが含まれています。[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、 をクリックします。
+ New server list (新しいサーバーリストの追加)	クリックして、新しいサーバーリストを追加し、リストの名前を入力します。
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ログインすることもできます。*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	サーバーリストのサーバーを削除するには、サーバーを選択し、[Remove (削除)] をクリックします。
サーバーの名前を変更する	リストをダブルクリックし、リストの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 Seriesの装置を使用している場合は、AXIS Camera Station 5から装置を設定するオプションがあります。[Configuration > Switch > Management (設定 > スイッチ > 管理)] に移動し、認証情報を入力して、AXIS Camera Station 5クライアントでスイッチの管理ページを開きます。スイッチの設定方法については、*axis.com*でAXIS Camera Station S22 Appliance Seriesのユーザーマニュアルを参照してください。

注

AXIS Camera Station 5 はスイッチのデフォルトのIPアドレスであるhttps://192.168.0.1/にのみ接続できます。

ライセンスの設定

ライセンスページで、接続する装置のライセンスキーとライセンスステータスを表示し、ライセンスを管理することができます。

注

- 複数のAXIS Camera Station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任意のサーバーを選択して、ライセンスを管理します。
- ライセンスキーは、後で参照できるように、メモするかUSBフラッシュドライブにデジタル形式で保存することをお勧めします。紛失したライセンスキーを回復することはできません。
- AxisネットワークビデオレコーダーをAXIS License Portalに登録すると、NVR Coreライセンスが付与されます。NVR Coreライセンスは、装置のハードウェアにロックされているため、移動できません。Coreライセンスと同じ方法で、NVR CoreからUniversalへのアップグレードを行うことができます。アップグレードライセンスは、任意のシステムに移動して使用できます。

ライセンス管理

[設定] - [ライセンス] - [管理] を選択して、サーバーに接続しているライセンスされていないデバイス数に関する概要を表示します。ライセンスはオンラインでもオフラインでも管理できます。30日間の試用期間が終了する前に、すべての装置のライセンスを忘れずに追加してください。「*ライセンスの購入方法*」を参照してください。ステータスバーでライセンスステータスのリンクをクリックして、装置のライセンスに関する概要を表示することもできます。

ライセンス管理者は複数のMy AxisアカウントをAXIS Camera Stationシステムに追加できます。

オンラインでシステムにMy Axisアカウントを追加する

1. **[設定] - [ライセンス] - [管理]** を選択します。
2. [**Manage licenses online (オンラインでライセンスを管理)**] がオンになっていることを確認します。
3. [**Go to AXIS License Portal (AXISライセンスポータルに移動)**] をクリックします。
4. AXIS License Portalで、追加する新しいMy Axisアカウントを使用してサインインします。
5. [**Edit license admins (ライセンス管理者を編集)**] に移動し、アカウントがライセンス管理者として追加されていることを確認します。

オフラインでシステムにMy Axisアカウントを追加する

1. **[設定] - [ライセンス] - [管理]** を選択します。
2. [**Manage licenses online (オンラインでライセンスを管理する)**] をオフにします。
3. [**システムファイルのエクスポート**] をクリックします。
4. システムファイルをUSBフラッシュドライブに保存します。
5. AXIS License Portal (*license-portal.lp.axis.com*) に移動します。
6. 追加する新しいMy Axisアカウントでサインインします。
7. システムファイルをアップロードします。
8. [**Edit license admins (ライセンス管理者を編集)**] に移動し、アカウントがライセンス管理者として追加されていることを確認します。

インターネット接続に応じて、システムをライセンスする方法は異なります。

- *システムをオンラインでライセンスする*
- *システムをオフラインでライセンスする*
- *システム間でライセンスを移動する, on page 130*

装置ステータス

[Configuration (設定)] > [Licenses (ライセンス)] > [Device status (デバイスステータス)] に移動して、接続しているすべての装置とそれらのライセンスステータスのリストを表示します。

キー

[設定] - [ライセンス] - [キー] を選択して、接続するすべてのデバイスのライセンスごとに必要なキーを一覧表示します。

システムをオンラインでライセンスする

AXIS Camera Stationクライアントとサーバーの両方にインターネット接続が必要です。

1. **[設定] - [ライセンス] - [管理]** を選択します。
2. [**Manage licenses online (オンラインでライセンスを管理)**] がオンになっていることを確認します。
3. My Axisアカウントでサインインします。
4. [**Add license key (ライセンスキーの追加)**] で、ライセンスキーを入力します。
5. [**追加**] をクリックします。
6. AXIS Camera Stationクライアントで、**[Configuration (設定)] > [Licenses (ライセンス)] > [Keys (キー)]** に移動して、ライセンスキーが表示されていることを確認します。

システムをオフラインでライセンスする

1. **[設定] - [ライセンス] - [管理]** を選択します。
2. [**Manage licenses online (オンラインでライセンスを管理する)**] をオフにします。
3. [**システムファイルのエクスポート**] をクリックします。
4. システムファイルをUSBフラッシュドライブに保存します。
5. AXIS License Portal (*license-portal.lp.axis.com*) に移動します。
6. My Axisアカウントでサインインします。
7. [**Upload system file (システムファイルをアップロード)**] クリックして、システムファイルをUSBフラッシュドライブからアップロードします。
8. [**Add license key (ライセンスキーの追加)**] で、ライセンスキーを入力します。
9. [**追加**] をクリックします。
10. [**License keys (ライセンスキー)**] で、[**Download license file (ライセンスファイルのダウンロード)**] をクリックして、USBフラッシュドライブにファイルを保存します。
11. AXIS Camera Stationクライアントで、**[Configuration (設定)] > [Licenses (ライセンス)] > [Management (管理)]** に移動します。
12. [**Import license file (ライセンスファイルのインポート)**] をクリックし、USBフラッシュドライブのライセンスファイルを選択します。
13. **[Configuration (設定)] > [Licenses (ライセンス)] > [Keys (キー)]** に移動して、ライセンスキーが表示されていることを確認します。

システム間でライセンスを移動する

注

NVR Coreライセンスは装置のハードウェアにロックされているため、移動できません。

ライセンスを同じMy Axisアカウントで1つのシステムから別のシステムに移動するには:

1. AXIS License Portal (*license-portal.lp.axis.com*) に移動します。
2. [**My systems (マイシステム)**] から、ライセンスの移動元のシステム名をクリックします。
3. [**License keys (ライセンスキー)**] で、移動したいライセンスキーを見つけます。
4. ⋮をクリックし、[**Move (移動)**]します。
5. [**To system (システムへ)**] ドロップダウンメニューから、ライセンスの移動先のシステムを選択します。
6. [**Move license key (ライセンスキーの移動)**] をクリックし、[**Close (閉じる)**] をクリックします。アクションの詳細については、[**History (履歴)**]を参照してください。
7. [**My systems (マイシステム)**] に移動し、ライセンスが正しいシステムの下に表示されていることを確認します。

ライセンスを別のシステムに移動

システムからライセンスを解放し、異なるMy Axisアカウントを使用して別のシステムに追加するには:

1. AXIS License Portal (*license-portal.lp.axis.com*) に移動します。
2. [**My systems (マイシステム)**] から、ライセンスの移動元のシステム名をクリックします。
3. [**License keys (ライセンスキー)**] で、移動したいライセンスキーを見つけます。
4. まず、ライセンスキーのコピーを作成します。
5. ⋮をクリックし、[**Release (解放)**] をクリックします。
6. サインアウトして、別のMy Axisアカウントでサインインします。
7. [**My systems (マイシステム)**] で、ライセンスを付与するシステムをクリックします。
8. [**Add license key (ライセンスキーの追加)**] で、解放したライセンスキーを入力します。
9. [**追加**] をクリックします。アクションの詳細については、[**History (履歴)**]を参照してください。
10. [**My systems (マイシステム)**] に移動し、ライセンスが正しいシステムの下に表示されていることを確認します。

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 5に存在するユーザーとグループを表示します。

注

AXIS Camera Station 5サーバーを実行しているコンピューターの管理者は、自動的に AXIS Camera Station 5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、ユーザーまたはグループをローカルコンピューターに登録するか、Windows® Active Directoryユーザーアカウントがあることを確認します。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。

グループの一員であるユーザーには、個人またはグループに割り当てられる最上位の権限が与えられます。ユーザーは個人としてアクセス権と共にグループの一員としての権限も与えられます。たとえば、あるユーザーがユーザー個人の権限としてカメラXへのアクセス権を与えられているとします。このユーザーは、カメラYおよびZへのアクセス権を持つグループのメンバーでもあります。したがって、ユーザーはカメラX、Y、Z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与えられているアクセス権。 表示される値: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 5にアクセスできます。ユーザーを AXIS Camera Station 5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 + 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)**] ウィンドウで、 [**Local Users and Groups (ローカルユーザーとグループ)**] > [**Users (ユーザー)**]の順に移動します。
- [**Users (ユーザー)**] を右クリックし、 [**New user (新しいユーザー)**] 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)**] のチェックを外します。
- [**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。
   使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、検索結果は表示されません。フィルター機能を使用します。
5. ユーザーまたはグループを選択し、[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 5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サーバーを選択します。

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与えられる権限は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。システム設定を行うユーザーは、この権限が必要になります。

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 5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。

ビューワー - 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)	録画の手動による開始および停止を許可します。
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)**] が選択されているときにのみ使用できます。

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 5のビューへのアクセスを許可します。
編集	AXIS Camera Station 5のビューの編集を許可します。

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ポートのステータスの表示を許可します。ユーザーはポートの状態を変更できません。
Write (書き込み)	I/Oポートのステータスの変更を許可します。

システム

リスト内でグレー表示されている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取得できるようにします。
録画のエクスポート	録画のエクスポートを許可します。
事故レポートの生成	事故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、マルチサーバーの設定を許可します。
アクセス管理	アクセス管理およびActive Directory設定へのアクセスを許可します。

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システムの設定を許可します。
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システムへのアクセスを許可します。

証明書

AXIS Camera Station 5サーバーと装置間の証明書の設定を管理するには、[Configuration > Security > Certificates (設定 > セキュリティ > 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 66*を参照してください。

AXIS Camera Station 5 は次のように使用できます。

- **ルート認証局 (CA):** AXIS Camera Station 5をルートCAとして使用する場合、AXIS Camera Station 5が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、プロセスに他のルートCAは関与しません。
- **中間認証局:** このシナリオでは、Axis装置のサーバー証明書に署名して発行するために、AXIS Camera Station 5でCA証明書とその秘密鍵をインポートする必要があります。このCA証明書は、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 5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 5 CA証明書があれば、装置で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 5を使用するか、CA証明書をインポートしてAXIS Camera Station 5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 5によってパスワードが保存されます。
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、すべての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。 • **秘密鍵がない場合:** 証明書を.cerまたは.crt形式で保存します。AXIS Camera Station 5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。 • **秘密鍵がある場合:** CAをPKCS#12形式 (.pfx または.p12) で保存します。CAを別の AXIS Camera Station 5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。
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は自身の有効期限を超えた証明書には署名しません。

ルートCAの生成

AXIS Camera Station 5が開始すると、CAを探します。見つからない場合は、ルートCAを自動生成します。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 5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 5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 136*を参照してください。

装置に手動でインストールした証明書を使用するバージョン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有効期限が切れると、AXIS Camera Station 5は既存のルートCAを使用して自動的に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場合、AXIS Camera Station 5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 5が証明書に署名できるようにします。ファイルはPKCS#12ファイルでなければならず、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、有効期間内に使用されなければなりません。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 136*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。続行するには、[OK] をクリックする必要があります。
- 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。
- AXIS Camera Station 5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。

HTTPS

デフォルトでは、AXIS Camera Station 5は、接続される各装置でアクティブなHTTPSサーバー証明書の署名を検証し、検証された証明書のない装置には接続しません。サーバー証明書は、AXIS Camera Station 5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 5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、装置のHTTPS証明書のアドレスが装置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 5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。

証明書の検証を一時的に無視する	オンにすると、AXIS Camera Station 5はあらゆるHTTPS証明書を受け入れ、安全でない装置の構成が許可されます。 オフにすると、AXIS Camera Station 5は装置証明書を検証します。証明書が信頼されていない場合は、[**Device management (デバイス管理)**] の [**Status (ステータス)**] に警告メッセージが表示され、装置にはアクセスできません。
デバイスアドレスの検証	ホスト名を使用せずにDHCPネットワーク上で安定した動作を実現する場合は、オフにします。 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、装置が主にホスト名を使用して通信するネットワーク、または装置が静的な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 41*を参照してください
- HTTPSを使用するには、ビデオ装置には5.70以降のファームウェア、アクセスコントロール装置と音声装置には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。
- 暗号化されていないチャンネル上の証明書動作 (「ベーシック」など) はサポートされていません。「ダイジェスト」通信を可能にするには、装置を [Encrypted & unencrypted (暗号化および非暗号化)] または [Encrypted only (暗号化のみ)] に設定する必要があります。
- 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 5 IEEE 802.1X認証では、要求を行う装置はLANへの接続を求めるAxisネットワーク装置です。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認証サーバーなど外部から取得することも、AXIS Camera Station 5から直接取得することもできます。この証明書は各Axis装置にインストールされ、認証サーバーの検証に使用されます。

注

IEEE 802.1X証明書を使用するには、ビデオ装置には5.50以降のファームウェア、アクセスコントロール装置と音声装置には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)] 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、装置のMACアドレス、装置のホスト名、またはカスタムテキストのいずれを使用するかを選択します。
4. [Custom (カスタム)] を選択した場合は、[Custom (カスタム)] にEAP識別情報となるテキストを入力します。
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 (コモンネーム)] ドロップダウンメニューで、**が認証局として動作するときに装置ごとに作成される個々の証明書で、コモンネームとして**Device IP address (デバイスのIPアドレス) とDevice EAP identity (デバイスのEAP識別情報) AXIS Camera Station 5のどちらを使用するかを選択します。
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。
- パラメーター`Network.Interface.I0.dot1x.Enabled`が指定されていないデバイスはサポートされません。例:AXIS P39 Series、AXIS T85 Series、およびAXIS T87 Video Decoder
- 暗号化されていないチャンネル上の証明書動作 (「ベーシック」など) はサポートされていません。「ダイジェスト」通信を可能にするには、装置を [Encrypted & unencrypted (暗号化および非暗号化)] または [Encrypted only (暗号化のみ)] に設定する必要があります。

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 5によってインストールされた装置CA証明書、AXIS Camera Station 5 CA証明書、およびIEEE 802.1X証明書に対しても同様です。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、AXIS Camera Station 5に有効期限日の何日前に通知してもらいたいかを指定します。

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 5によって生成された装置クライアント/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。このためには、装置で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場合は、*セキュリティ, on page 66*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

1. [Configuration (設定)] > [Security (セキュリティ)] > [Certificates (証明書)] に移動します。
2. [Certificate renewal (証明書の更新)] で、[Renew (更新)] をクリックします。
3. サーバーを再起動して、更新された証明書を適用します。

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証明書を使用するデバイスがアクセス可能であることを確認します。
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の設定

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 5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。

- **設定 > デバイス >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. 既定の識別プロファイルを編集したり、新しい識別プロファイルを作成したりするには、*識別プロファイル, on page 153*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、*カード形式とPIN, on page 155*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 141*を参照してください。
4. ドアを設定します。
   - *「ドアモニターの追加」, on page 146*
   - *緊急入力の追加, on page 147*
   - *「リーダーの追加」, on page 148*
   - *REX装置の追加, on page 150*
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 150*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

以下の表は、AXIS Camera Station Pro5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	推奨AXIS OSバージョン
5.59	12.4.68.1
5.58	12.4.68.1
5.57	11.8.20.2

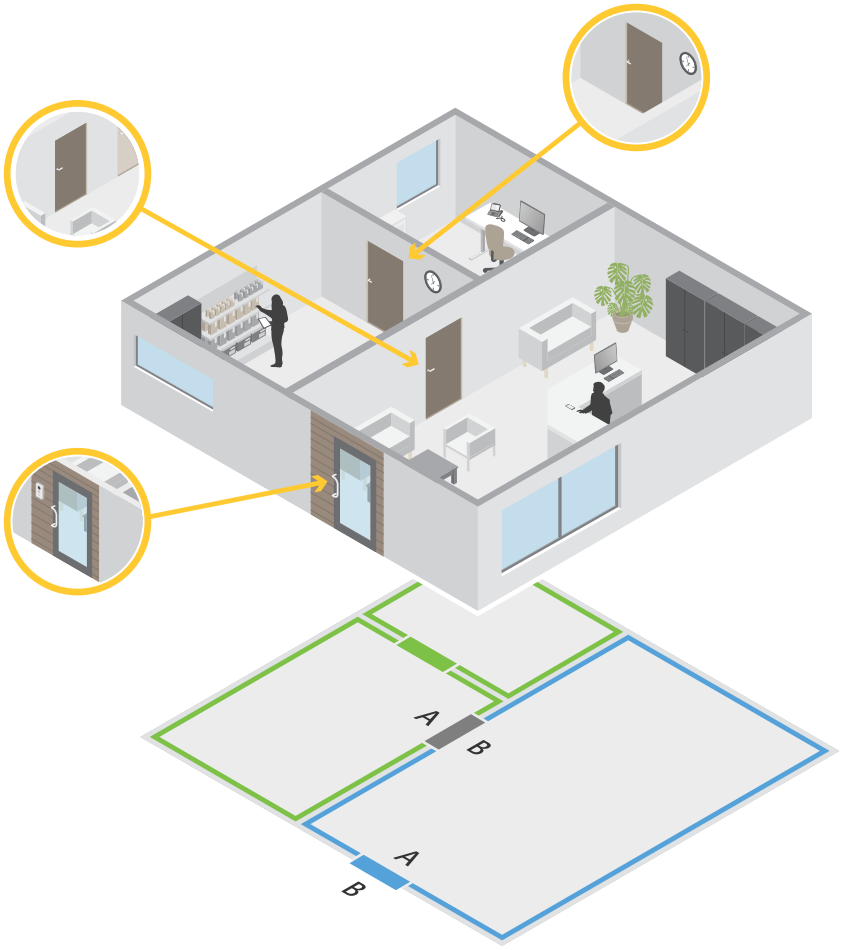
ドアとゾーン

[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。

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場合は、**[Print (印刷)]** をクリックします。
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。
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。
ドアコントローラー	ドアに接続されているドアコントローラーです。
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。
カード形式とPIN	カードのフォーマットまたはPINの長さを表示します。
ステータス	ドアのステータス。 • **オンライン:** ドアはオンラインで正しく機能しています。 • **リーダーオフライン:** ドア設定のリーダーがオフラインです。 • **リーダーエラー:** ドア設定のリーダーは、安全なチャンネルをサポートしていないか、セキュアチャンネルがリーダーに対してオフになっています。
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。

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。

新しいドアの設定を作成してドアを追加する:

1. [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。
2. + [Add door (ドアの追加)] 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。
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 145*を参照してください。
監視ドア	開閉を通知できるドア。詳しくは、を参照してください。
設置済みドア	ハードウェアを選択する必要がなく、システム内にプレースホルダーとして追加できるドア。
フロア	カードリーダーを使用してエレベーター各階へのアクセスを認証するエレベーターコントロールのドアタイプ。詳しくは、を参照してください。

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。別のドアを追加できない場合、オフラインの場合、またはHTTPSがアクティブでない場合、コントローラーはグレー表示されます。
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 153*を参照してください。
8. ドアの設定に記載されている設定を行います。「 *ドア設定, on page 143*」を参照してください。
9. *「ドアモニターの追加」, on page 146*
10. *緊急入力の追加, on page 147*
11. *「リーダーの追加」, on page 148*
12. *REX装置の追加, on page 150*
13. [保存] をクリックします。

既存のドアの設定をコピーしてドアを追加する:

1. [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。
2. [**[Add door (ドアを追加)]**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. [保存] をクリックします。

ドアを編集するには:

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. [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。

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)]をクリックします。
4. [Yes (はい)] 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。

ドアとゾーンの追加と設定

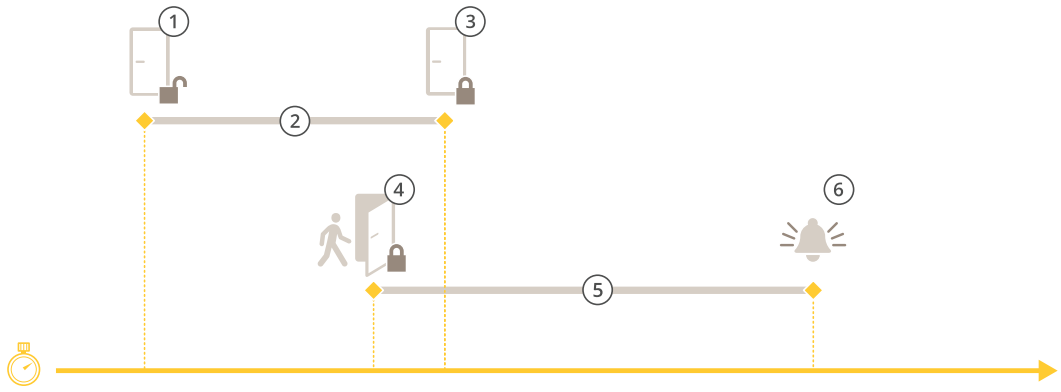
ドア設定

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。

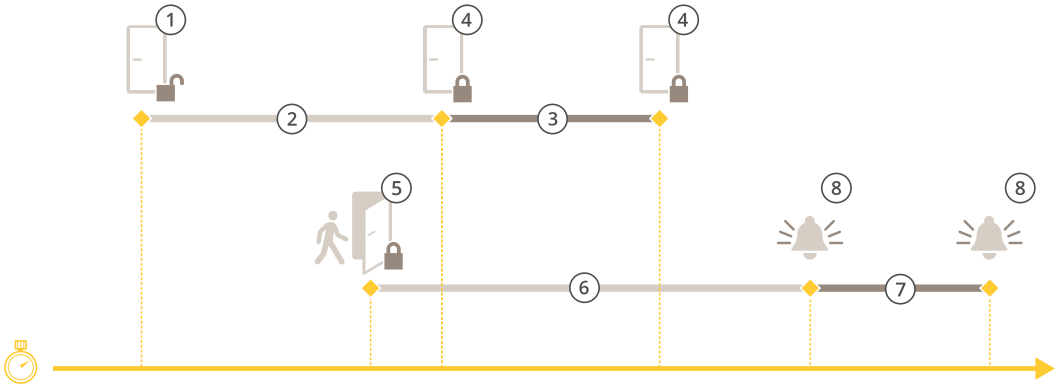
アクセス時間 (秒)	アクセスが許可されてからドアのロック解除を継続する秒数を設定します。ドアが開くか設定時間が終了するまで、ドアのロックは解除されたままになります。ドアが閉まると、アクセス時間が残っていてもドアはロックされます。
Open-too-long time (sec) (長時間のドア開放 (秒))	ドアモニターを設定している場合にのみ有効です。ドアが開いたままになる秒数を設定します。設定時間が終了したときにドアが開いていると、長時間ドア開放アラームがトリガーされます。アクションルールを設定して、長時間ドア開放イベントでトリガーするアクションを設定します。
長いアクセス時間 (秒)	アクセスが許可されてからドアのロック解除を継続する秒数を設定します。Long access time (長いアクセス時間) は、この設定がオンになっているカード所持者のアクセス時間より優先されます。
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ている場合にのみ有効です。ドアが開いたままになる秒数を設定します。設定時間が終了したときにドアが開いてい

	ると、長時間ドア開放イベントがトリガーされます。[Long access time (長いアクセス時間)] 設定をオンにしている場合、[Long open-too-long time (長い長時間のドア開放)] は、カード所持者に対してすでに設定されている [Open too long time (長時間のドア開放)] 設定よりも優先されます。
再ロックの遅延時間 (ms)	ドアの開閉後にロック解除されたままになる時間 (ミリ秒) を設定します。
再ロック	• After opening (開けた後): ドアモニターを追加した場合のみ有効です。 • After closing (閉じた後): 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	ドアがこじ開けられた場合にアラームを作動させるかどうかを選択します。
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アラームを作動させるかどうかを選択します。

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 *アクションの実行なし - ロック施錠*
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 *アクションの実行なし - ロック施錠*
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 5 は、ASSA ABLOY Aperio®のワイヤレスロックと通信ハブをサポートしています。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。

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。

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 5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。
- 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 5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. [[Add door (ドアを追加)]をクリックします。

4.3. 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、[Door type (ドアタイプ)] で [Wireless door (ワイヤレスドア)] 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 140*を参照してください。

4.7. [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	動作
良好	ありません
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なる前にバッテリーを交換する必要があります。
重大	バッテリーを交換してください。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	動作
オンライン	ありません
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。

「ドアモニターの追加」

ドアモニターとは、ドアの物理的な状態を監視するドアポジションスイッチです。ドアにドアモニターを追加し、ドアモニターの接続方法を設定できます。

1. [Door configuration (ドアの設定)] ページに移動します。*ドアの追加, on page 141*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 monitor sensor (ドアモニターセンサー)] 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 152*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。

緊急入力の追加

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 141*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。

「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。

カスタム設定のカードフォーマットやPIN長をリーダーに適用すると、そのことは [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 [Card formats (カードフォーマット)] で確認できます。 *ドアとゾーン, on page 140*を参照してください。

注

- また、ドアコントローラーには、最大16台のBluetoothリーダーを追加できます。詳しくは、*Bluetoothリーダーの追加, on page 149*を参照してください。
- AxisネットワークインターカムをIPリーダーとして使用する場合、システムは装置の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 141*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のPIN長さ設定を使用するには:
   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のカードフォーマットを使用するには:
   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現在のシステム設定と異なる場合、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、この手順を再度行います。

AXISバーコードリーダーの設置方法については、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。要件およびサポートされるデバイスについては、*IPリーダー, on page 149*を参照してください。

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	リーダーに対するいたずら入力がアクティブになるタイミングを選択します。 • Open circuit (開路):リーダーは、回路が開いたときにいたずら信号を送信します。 • Closed circuit (閉路):リーダーは、回路が閉じたときにいたずら信号を送信します。
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 152*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制限を拡張し、これらのリーダーを最大16台までドアに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。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」 *ドアの追加, on page 141*。
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。

IPリーダー

Axisネットワークインターカムは、AXIS Camera Station Secure EntryでIPリーダーとして使用することができます。

注

- これには、AXIS Camera Station 5.38以降と、ファームウェア10.6.0.2以降を搭載したAxisドアコントローラーが必要です。
- インターカムをIPリーダーとして使用するための特別な設定は必要ありません。

対応デバイス:

- ファームウェア10.5.1以降を搭載しているAXIS A8207-VE Network Video Door Station
- ファームウェア10.5.1以降を搭載しているAXIS A8207-VE Mk II Network Video Door Station
- AXIS I8116-E Network Video Intercom

REX装置の追加

REX (退出要求) 装置は、ドアの片面に取り付けるか、両面に取り付けるかを選択できます。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 141*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。使用可能なポートが1つしかない場合、ポートは自動的に選択されます。
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 152*を参照してください。

動作	
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。
ありません	ドアがREX信号を受信したときにアクションをトリガーしない場合に選択します。

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。

- **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。

- **内部ドア:** ゾーンの内部にあるドアです。

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。

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. [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。これにより、ユーザー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。

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、または既存のゾーンで設定できます。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. ドア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人目のユーザーが最初の人と同じ認証情報を使用してドアから入ることを許可する場合に、このオプションを使用します。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人目のユーザーが最初のユーザーと同じ認証情報を使用してドアから入ることを禁止する場合に、このオプションを使用します。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と入力します。その場合、ユーザーがゾーンから退出するまで、そのソーンでアンチパスバックが維持されます。[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たときにイベントをトリガーできます。

- ドアコントローラーとドアモニターの接続。*「ドアモニターの追加」, on page 146*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 148*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 150*を参照してください。

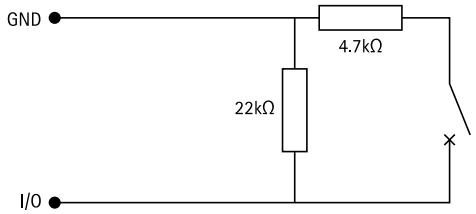
監視入力を使用するには:

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。

接続図

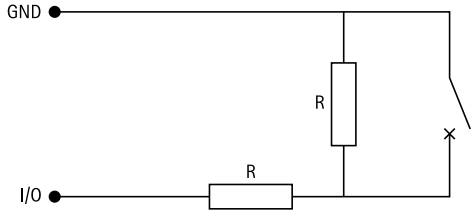
パラレルファースト接続

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。

識別タイプは、ドアにアクセスするために必要な認証情報を運ぶものです。一般的な識別タイプには、トークン、個人識別番号 (PIN)、指紋、顔立ちマップ、REX装置があります。識別タイプは、1つ以上のタイプの情報を運ぶことができます。

サポートされる識別タイプ:カード、PIN、REX、静的QR、動的QR。

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。

そのまま使用したり、必要に応じて編集して使用したりできる、デフォルトの識別プロファイルが5つ用意されています。

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。

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イブ株式会社の登録商標です。

識別プロファイルを作成する手順は、以下のとおりです。

1. **[Configuration (設定)] > [Access Control (アクセスコントロール)] > [Identification profiles (識別プロファイル)]** を選択します。
2. [**Create identification profile (識別プロファイルの作成)**] をクリックします。

3. 識別プロファイル名を入力します。
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. ドアの片側の面で識別プロファイルを設定します。
6. ドアの反対側の面で同じ手順を繰り返します。
7. [OK] をクリックします。

識別プロファイルを編集する手順は、以下のとおりです。

1. **[Configuration (設定)] > [Access Control (アクセスコントロール)] > [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)] > [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。

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。

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。

識別プロファイルの設定

カード形式とPIN

カードフォーマットは、カードにデータを保存する方法を定義します。これは、システム内で入力データを検証済みデータにする変換テーブルです。カードフォーマットごとに、保存された情報を整理する方法に対する異なるルールがあります。カードフォーマットを定義することで、コントローラーがカードリーダーから取得する情報をどのように解釈するかがシステムに通知されます。

そのまま使用したり、必要に応じて編集して使用したりできる、汎用性の高い既定のカードフォーマットも用意されています。カスタムのカードフォーマットを作成することもできます。

[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。

カードフォーマットを作成する手順は、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. [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。

ⓘ	ⓘ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)**:10を底とする位取り記数法であり、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。

カードフォーマットを編集する手順は、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。

既定のカードフォーマットをリセットするには:

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。

PIN長を設定する手順は、以下のとおりです。

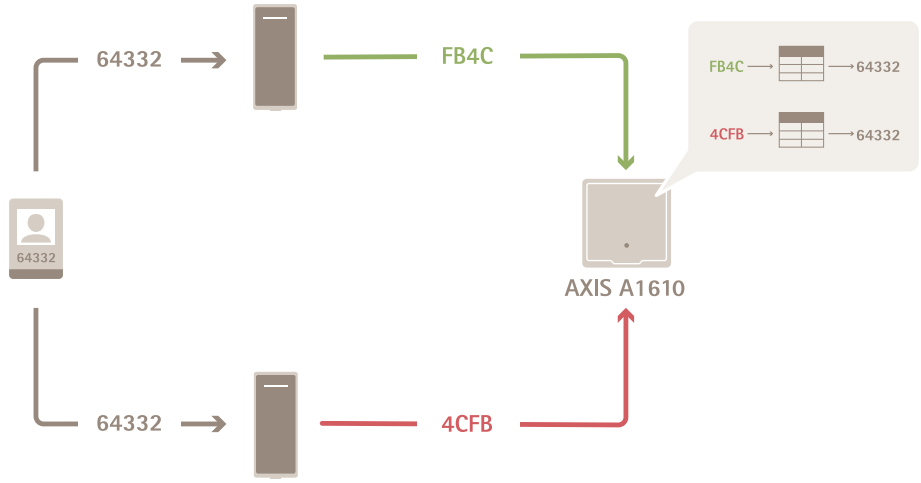
1. **[Configuration (設定)] > [Access Control (アクセスコントロール)] > [Card formats and PIN (カードフォーマットとPIN)]** を選択します。
2. **[PIN configuration (PIN設定)]**で をクリックします。
3. **[Min PIN length (最小PIN長)]**、**[Max PIN length (最大PIN長)]**、**[End of PIN character (PIN文字の終端)]** をそれぞれ指定します。
4. [OK] をクリックします。

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セキュアチャンネル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ナンバープレート検証装置を認証します。

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。デフォルトのポートは55767です。ポートのカスタマイズ設定については、*概要, on page 191*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 159*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 159*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 164*」および「*「グループの追加」, on page 168*」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 164*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 5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 5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 160*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 5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 165*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、複数のフィルターを設定して、Axisカメラから生成された録画から対象となる人物や車両を簡単に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 34*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の量を制限するには、[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。
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. 特定の期間にメタデータが記録されていないことを示す結果を表示するには、[Include periods with missing metadata (メタデータがない期間を含める)] を選択します。
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%未満であると表示されます。
	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%未満であると表示されます。

System Health Monitoring^BETA^の設定

注

- 複数の AXIS Camera Station 5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、AXIS System Health Monitoringクラウドサービスは、クラウド経由で同じ機能を提供します。詳細については、*AXISのシステムの健全性監視クラウドサービスの設定, on page 117*を参照してください。

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 119*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 162*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 162*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示す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つの通知ルールが有効になっています。

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5分間ダウンしたとき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5分間ダウンしたとき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、通知ルールが適用されたシステムと装置のリストを閲覧できます。

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 163*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 163*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 173*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)] をクリックして、コピーをメインシステムにアップロードできるようにします。
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、[Delete (削除)] をクリックして、最初に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、メインシステム情報が [Systems with access (アクセス可能なシステム)] の下に表示されます。

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した後、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入力します。
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。

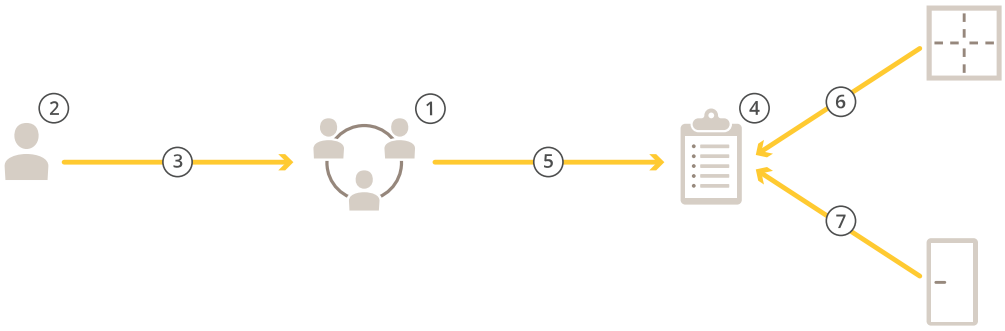
アクセス管理

[Access management (アクセス管理)] タブでは、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ができます。

AXIS Camera Station 5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。以下はワークフローの例です。



1. グループを追加するワークフローについては、*「グループの追加」, on page 168*を参照してください。
2. カード所持者を追加するワークフローについては、*カード所持者の追加, on page 164*を参照してください。
3. カード所持者とグループの追加。
4. アクションルールを追加するワークフローについては、*「アクセスルールの追加」, on page 169*を参照してください。
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。カード所持者に、個人を識別する認証情報と、その個人にドアへのアクセスを許可するタイミングと方法を設定します。

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 160*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)**] > [**Cardholders (カード所持者)**] に移動し、[**+ Add (追加)**] をクリックします。
3. カード所持者の名と姓を入力し、[**Next (次へ)**] をクリックします。
4. オプションとして [**Advanced (詳細設定)**] をクリックし、任意のオプションを選択します。
5. 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 165*を参照してください
6. [**保存**] をクリックします。
7. グループにカード所持者を追加します。

7.1. [Groups (グループ)] でカード所持者を追加するグループを選択し、[Edit (編集)] をクリックします。

7.2. [+ Add (追加)] をクリックし、グループに追加するカード所持者を選択します。複数のカード所持者を選択できます。

7.3. [追加] をクリックします。

7.4. [保存] をクリックします。

高度	
長いアクセス時間	ドアモニターが設置されていて、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。
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、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。
閉鎖の対象外	閉鎖中にカード所持者が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 158*を参照してください。

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
- PIN
- カード
- ナンバープレート

カード所持者にQR認証情報を追加するには：

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の時刻とAXIS Barcode Reader搭載カメラの時刻が同期されている必要があります。完全な時刻同期のためには、両方の装置で同じタイムソースを使用することをお勧めします。

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。動的QRとPIN認証情報と共に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。

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. 強制PINを使用して無音アラームをトリガーするには、[Duress PIN (強制PIN)] をオンにして強制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。

ドアを開けてシステム内で無音アラームをトリガーする強制PINを設定することもできます。

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、システムに存在し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 reader(s) (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)]** を有効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。

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, on page 167*の例を参照してください。

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。

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 5に追加します。*デバイスの追加, on page 5*を参照してください
2. [Synchronize with server computer time (サーバーコンピューターの時刻と同期)] を使用して、新しい装置の日付と時刻を設定します。*日付と時刻の設定, on page 64*を参照してください。
3. 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 63*を参照してください。
4. 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 141*を参照してください。
   4.1. [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 148*を参照してください。
   4.2. [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。
   4.3. 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。
   4.4. [Ok] をクリックします。
5. 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。

6. AXIS License Plate Verifierを起動します。
7. AXIS License Plate Verifierを設定します。
   7.1. [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。
   7.2. [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。
   7.3. カメラのwebインターフェースからAXIS License Plate Verifierを開きます。
   7.4. 設定は行わないでください。
   7.5. [Settings (設定)] に移動します。
   7.6. [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。
   7.7. [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。
   7.8. [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。
   7.9. [接続] をクリックします。
   7.10. [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。
   7.11. [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。
   7.12. 統合をオンにします。
8. アクセス権を付与するカード所持者を追加します。*カード所持者の追加, on page 164*を参照してください
9. 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 165*を参照してください
10. アクセスルールを追加します。*「アクセスルールの追加」, on page 169*を参照してください。
    10.1. スケジュールを追加します。
    10.2. 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。
    10.3. 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、カード所持者とそのアクセスルールをまとめて効率的に管理することができます。

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)] > [Groups (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)] を選択すると、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なります。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 158*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. [保存] をクリックします。

「アクセスルールの追加」

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)] か [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。
6. ドアとゾーンを設定する:
   6.1. [Doors (ドア)] か [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. [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。

ドア

ドアの手動ロック解除などの手動アクションについては、「」を参照してください。

ゾーン

ゾーンの手動ロック解除などの手動アクションについては、「」を参照してください。

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 5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。

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 153*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。

インポートとエクスポート

カード所持者のインポート

このオプションでは、CSVファイルからカード所持者、カード所持者グループ、認証情報、カード所持者の写真がインポートされます。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、以前に保存したものは削除します。

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 160*を参照してください。

インポートオプション	
新規	このオプションを選択すると、既存のカード所有者が削除されてから、新しいカード所有者が追加されます。
更新	このオプションを選択すると、既存のカード所持者が更新され、新規のカード所持者が追加されます。
追加	このオプションを選択すると、既存のカード所持者が保持されたうえで、新しいカード所持者が追加されます。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 (ファイルを選択する)] をクリックし、CSVファイルに移動します。**[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。一意の識別子により、重複するカード所持者レコードのインポートが防止されます。
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)] が選択されています。

: 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 5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、最後にカード所持者をインポートした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。

System Health Monitoring[BETA]

[System Health Monitoring (システムの健全性監視)]タブで、同じネットワーク上の1つ以上のAXIS Camera Station 5システムからの健全性データを監視できます。

別のネットワーク上のシステムを管理している場合、AXIS System Health Monitoringクラウドサービスは、クラウド経由で同じ機能を提供します。詳細については、*AXISのシステムの健全性監視クラウドサービスの設定, on page 117*を参照してください。

	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 173*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 174*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 175*を参照してください。

制限事項

- AXIS S3008 Recorder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。
- 連続録画または動きをトリガーとした録画を除く録画には、録画タイプとして [**None (なし)**] のフラグが付けられます。

ワークフロー

1. *System Health Monitoring[BETA]の設定, on page 162*
   1.1. 通知を設定する。*通知, on page 162*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 163*を参照してください。
2. AXIS Camera Station 5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 173*
   2.2. *ストレージ, on page 174*
   2.3. *通知, on page 175*

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を含む情報が表示されます。
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。
   右側のパネルに、装置の詳細とストレージの情報 (ビデオソースが含まれている場合) 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 185*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)] ドロップダウンメニューから、[System Health Monitoring report (System Health Monitoring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、列の値を基準にしてデータが並べ替えられます。

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 71*を参照してください。
場所	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。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	録画に割り当てられた最大ストレージ容量。
使用中	現在録画データが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):標準状態。 警告アイコン:保存期間を満たしていません。 情報アイコン:カメラの録画が短すぎるため、保存期間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	カメラからストレージに録画が保存されている日数。
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。
最新の録画	カメラからストレージに保存されている最も新しい録画の時刻。
場所	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、列の値を基準にしてデータが並べ替えられます。

[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	イベントが発生するシステムの名前。
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 5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。マウスを警告アイコンに合わせると、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るようになり、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、その空の値をクリックすると、ホットキーをこのアクションで追加できます。 • キーボードでホットキーを追加するには、Ctrlキー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でホットキーを追加する場合は、アクションに割り当てるジョイスティックまたはジョグダイアルボタンを押します。
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、値を編集します。
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、値を削除します。
	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、監査ログなどのライブログが表示されます。以前のログも検索できます。ログを保存する日数は、[Configuration > Server > settings (設定 > サーバー > 設定)] で設定できます。

時間	操作の日付と時刻。
タイプ	操作のタイプで、アラーム、イベント、または監査です。
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	AXIS Camera Station 5 アクションを実行するユーザー。
コンピューター	AXIS Camera Station 5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)。
Windowsユーザー	AXIS Camera Station 5を管理するWindowsユーザー。
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. [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 5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検索結果を表示します。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 39*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

アラームログでは、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リストに表示されます。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対応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

イベントログでは、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に表示されます。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

監査ログでは、手動録画、ビデオストリームの開始と停止、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、すべてのユーザー操作を閲覧できます。監査を選択してツールバーの  をクリックすると、監査がテキストファイルとしてエクスポートされます。

アラーム

[Alarms (アラーム)] タブは AXIS Camera Station 5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 203*」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	アラームを送信する AXIS Camera Station 5 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。
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。
	アラーム手順を表示します。アラームにアラーム手順が含まれている場合にのみ使用できます。
	録画に移動します。アラームに録画が含まれている場合にのみ使用できます。
	選択したアラームを確認する
	アラームを削除します。アラームを削除する前に確認しない場合、アラームは一時的に削除されるだけです。

特定のアラームに対処するには:

1. AXIS Camera Station 5クライアントの下部にある **[Alarms and Tasks (アラームとタスク)]**をクリックして**[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. アラームが対応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 5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あり、管理者と、タスク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
- 事故レポートを作成
- 録画のエクスポート

管理者は、個人用タスクを含めて、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。
- 自分が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、事故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。 考えられるステータス: • **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処理中。 • **Canceled (キャンセル済み)**:クリーンアップ処理が完了し、タスクがキャンセルされました。 • **Error (エラー)**:タスクは完了しましたがエラーが含まれています。たとえば、いくつかのカメラでタスクが完了していません。 • **Finished (完了)**:タスクは完了しました。 • **Finished during lost connection (接続の切断中に完了)**:サーバー接続のダウン中にタスクが完了した場合に表示されます。タスクのステータスを確認できません。 • **Lost connection (接続の切断)**:タスクの実行中にクライアントとサーバーの接続が切断された場合に表示されます。タスクのステータスを確認できません。 • **Running (実行中)**:タスクを実行しています。 • **Pending (保留中)**:サーバーの他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 5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 5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。エラーの発生したオペレーションは、手動で確認し、設定する必要があります。

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。録画のエクスポートや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て、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。
Address (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 (完了):正常に終了したタスク。 • Error (エラー):完了に失敗した装置のタスク。 • Canceled (キャンセル済み):完了前にキャンセルされたタスク。
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	事故レポートの参照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概要を含むHTML形式のレポートを表示するには、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 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

このサーバー用設定シートには、一般的な設定情報のほか、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概要を含むHTML形式のレポートを表示するには、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 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. 右上のメニューに移動します。
2. [Help (ヘルプ)] > [System report (システムレポート)] をクリックします。
3. 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。
4. [参照] をクリックしてシステムレポートの保存先を選択します。
5. 希望の設定を選択します。
   - すぐに表示する場合は、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を簡易化する場合は、Include screenshots of all monitors (すべてのモニターのスクリーンショットを含む) を選択します。
6. [OK]をクリックします。

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 5での現在のシステム設定を使用したデータストリーミングとデータストレージのテストです。出力:合格もしくは不合格
低光量条件	ゲイン設定などの、標準の低光量の状態のために最適化された設定を使用したデータストリーミングとデータストレージのテストです。出力:合格もしくは不合格
ストレステスト	システムが最大制限に達するまで、データストリーミングとデータストレージを段階的に増加するテストです。出力:最大システムパフォーマンスに関する情報

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 5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)**] をクリックするとレポートを表示でき、[**Save report (レポートの保存)**] をクリックすると保存できます。

フィードバック

クライアントを設定するときに、匿名のクライアント使用状況データを自動的に共有することを選択し、AXIS Camera Station 5とユーザーエクスペリエンスの向上に役立つフィードバックを手動で送信できます。*クライアントの設定, on page 110*を参照してください。

注

フィードバックフォームをサポートリクエストの送信に使用しないでください。

1. ☰ > [**Help (ヘルプ)**] > [**Feedback (フィードバック)**]に移動します。
2. リアクションを選択し、フィードバックを入力します。
3. [**Send (送信)**] をクリックします。

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。

装着式の設定

装着式システムと接続するには、接続ファイルを作成する必要があります。*Axis装着式システムの設定*を参照してください。

注

接続ファイルを作成する前に、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、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 134*を参照してください。

接続ファイルを作成するには:

1. ☰ > [Other (その他)] > [Body worn settings (装着式の設定)]に移動します。
2. 装着式システムに表示されているデフォルトのサイト名を変更するには、新しい名前を入力します。
3. [**エクスポート**] 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

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 5 Service Control

サーバーは、AXIS Camera Station 5 Service Controlを使用して開始と停止、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 > Tools > Service Control (すべてのプログラム > ツール > Service Control)] を選択します。

	動作中
	起動中
	停止

Modify Settings (設定の変更)	サーバー設定を変更できるようにする場合に選択します。
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。

概要

AXIS Camera Station 5 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。

サーバーの設定	
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。
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。
Server HTTP port (サーバーHTTPポート)	サーバーがクライアントとの通信で使用するHTTPポート番号。デフォルトポートは55752です。
Server TCP port (サーバーTCPポート)	サーバーがクライアントとの通信で使用するTCPポート番号。デフォルトポートは55754です。ポート番号は、サーバーポート番号に2を加算して求めます。
Mobile communication port (モバイル通信ポート)	サーバーがクライアントとの通信で使用するモバイルポート番号。デフォルトポートは55756です。ポート番号は、サーバーポート番号に4を加算して求めます。
Mobile streaming port (モバイルストリーミングポート)	サーバーがビデオストリーミングで使用するモバイルポート番号。デフォルトポートは55757です。ポート番号は、サーバーポート番号に5を加算して求めます。
Component communication port (コンポーネント通信ポート)	コンポーネントがサーバーを介してネットワーク装置と通信するために使用するポート番号。デフォルトポートは55759です。ポート番号は、サーバーポート番号に7を加算して求めます。
Ports used by AXIS Camera Station 5 components (コンポーネントが使用するポート)	ポート範囲を指定すると、コンポーネントで使用できるポートがリストに表示されます。AXIS Camera Station 5コンポーネントのデフォルトのポート範囲は55760～55764です。
Allow AXIS Camera Station 5 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に、AXIS Camera Station 5がWindows Firewallに例外を自動的に追加できるようにする場合は、このオプションを選択します。

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。

プロキシー設定	
Direct connection (直接接続)	AXIS Camera Station 5サーバーとシステム内のカメラの間にプロキシサーバーが存在しない場合は、このオプションを選択します。
System account Internet options / automatic (システムアカウントのインターネットオプション/自動)	デフォルトのプロキシー設定。このオプションは、インターネットオプションの現在のプロキシー設定をシステムアカウントに使用します。
Use manual proxy settings (手動でプロキシを設定する)	AXIS Camera Station 5サーバーとシステム内のカメラの間にプロキシサーバーがある場合は、このオプションを選択します。プロキシサーバーのアドレスとポート番号を入力します。通常、Windowsのコントロールパネルの [インターネットオプション] と同じアドレスとポート番号です。 • 特定の文字で始まるアドレスのプロキシサーバーを使用しないように指定します。 • 通信がプロキシサーバーを経由する必要のないローカルカメラについては、[Always bypass proxy server for local addresses (ローカルアドレスにはプロキシサーバを使用しない)] を選択し、カメラのローカルアドレスまたはホスト名を入力します。ワイルドカードをアドレスやホスト名 (「192」または「mydomain.com」。

AXIS Camera Station 5のポートリスト

次の表に、AXIS Camera Station 5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使いやすさのために、以下のポートをファイアウォールで許可することが必要になる場合があります。ポート番号はデフォルトのHTTPメインポート55752に基づいて計算しています。

AXIS Camera Station 5 サーバーは、装置の次のポートにデータを送信します。

ポート	番号	プロトコル	入出力	説明
メインHTTPおよびHTTPSポート	80および443	TCP	送信	ビデオストリームと装置データに使用されます。
デフォルトbonjourポート	5353	UDP	マルチキャスト (受信+送信)	mDNS Discovery (Bonjour) により装置を検知するために使用されます。マルチキャスト224.0.0.251。

				デフォルトポートにバインドできない場合は、別のアプリケーションがそのポートを使用しており、共有を拒否している可能性があります。その場合は、ランダムなポートが使用されます。ランダムポートを使用する場合、Bonjourはリンクローカルアドレスを使用する装置を検知しません。
デフォルトSSDPポート	1900	UDP	マルチキャスト(受信+送信)	SSDP (UPNP) により装置を検知するために使用されます。 マルチキャスト239.255.255.25-0。
デフォルトWS-Discoveryポート	3702	UDP	マルチキャスト(受信+送信)	Onvif装置の検知に使用されるWS-Discovery Webサービス検知。 マルチキャスト239.255.255.25-0。

AXIS Camera Station 5 サーバーは、次のポートでクライアントからデータを受信します。

ポート	番号	プロトコル	入出力	通信	説明
デフォルトSSDPポート	1900	UDP	マルチキャスト (受信+送信)	サーバーとクライアント	SSDP (UPNP) を使用してAXIS Camera Station 5サーバーを検知するために使用されます。 マルチキャスト239.255.255.2-50。
メインHTTPポートとHTTPストリーミングポート	55752	TCP	受信	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	55754	TCP	受信	サーバーとクライアント	メインHTTPポートから+2オフセット。 アプリケーションデータに使用されます (TLS 1.2暗号化)。5.15.007以下の場合、TLS 1.1暗号化が使用されます。
SSDP Webサーバーポート	55755	TCP	受信	サーバーとクライアント	メインHTTPポートから+3オフセット。 SSDP/UPNPによる AXIS Camera Station 5サーバーの検出に使用されます。
API Webサーバーポート	55756	TCP	受信	サーバーとモバイルアプリ	メインHTTPポートから+4オフセット。 MP4 over HTTPSを利用するアプリケーションデータおよびビデオストリームに使用されます。
APIメディアポート	55757	TCP	受信	サーバーとモバイルアプリ	メインHTTPポートから+5オフセット。 RTSP over HTTPを利用するビデオストリームに使用されます。

ローカルプロキシHTTPポート	55758	TCP	受信	サーバーの内部通信	メインHTTPポートから+6オフセット。 API Webサーバーポートから+2オフセット。 AXIS Camera Station 5サーバーコンピューターで内部でのみアクセス可能です。 不明な問題に対する回避策ポート。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ポートとAPIメディア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	55759	TCP	受信	サーバーとコンポーネント	メインHTTPポートから+7オフセット。 コンポーネントと装置間の安全な通信に使用されます。

コンポーネント用に予約されたポート

コンポーネント	インターフェースでリッスン	ポート	番号	プロトコル	入出力	通信	説明
Secure Entry	Localhost (127.0.0.1)	Webサーバーポート	55766	HTTPS	受信	クライアント ([Access management (アクセス管理)] タブ) とコンポーネント	メインHTTPポートから+14オフセット。 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	すべて (0.0.0.0/ INADDR_ANY)	Webサーバーポート	55767	HTTPS	受信	メインサーバーとサブサーバー	メインHTTPポートから+15オフセット。 マルチサーバー設定でメインサーバーとサブサーバー間の通信に使用します。
システムの健全性監視	すべて (0.0.0.0/ INADDR_ANY)	Webサーバーポート	55768	HTTPS	受信	クライアント ([System Health Monitoring] タブ) とコンポーネント	メインHTTPポートから+16オフセット。 System Health Monitoring Webページをホストし、マルチシステム設定でデータを共有するために使用されます。
System Health Monitoringクラウ	localhost	Webサーバーポート	55769	HTTPS	受信	AXIS Camera Station 5 (Webページ) および	メインHTTPポートから+17オフセット。

コンポーネント	インターフェースでリッスン	ポート	番号	プロトコル	入出力	通信	説明
ドサービス						CloudService-viceバックエンド(プラグイン)	システム健全性の監視クラウドサービスに使用されて、システムの健全性監視を有効にします。
スマート検索2	localhost	Webサーバーポート	55770	HTTPS	受信	クライアント ([スマート検索] タブ) とコンポーネント	メインHTTPポートから+18オフセット。 Smart Search APIをホストし、クライアントにWebページを提供するために使用されます。
			55771				将来の使用のために予約。
			55772				将来の使用のために予約。
			55773				将来の使用のために予約。
			55774				将来の使用のために予約。
			55775				将来の使用のために予約。
			55776				将来の使用のために予約。
			55777				将来の使用のために予約。

コンポーネント	インターフェースでリッスン	ポート	番号	プロトコル	入出力	通信	説明
			55778				将来の使用のために予約。
			55779				将来の使用のために予約。
			55780				将来の使用のために予約。
			55781				将来の使用のために予約。
			55782				将来の使用のために予約。
			55783				将来の使用のために予約。
ローカルIAM (IDP)	0.0.0.0	IDP_OIDC (公開)	55784	HTTPS	受信	リバースプロキシとローカルIAM	メインHTTPポートから+32オフセット。 公開ポート。
ローカルIAM (IDP)	0.0.0.0	MTLS (管理者)	55785	HTTPS	受信	サードパーティサービス	メインHTTPポートから+33オフセット。 管理者ポート。
ローカルIAM (IDP)	127.0.0.1	トークナイザー	55786	HTTPS	受信	サードパーティサービス	メインHTTPポートから+34オフセット。 トークナイザーポート。
			55787				将来の使用のために予約。
オープンテレメトリ	127.0.0.1	gRPCポート	55788	gRPC	受信	サードパーティサービス	メインHTTPポートから

コンポーネント	インターフェースでリッスン	ポート	番号	プロトコル	入出力	通信	説明
							+36オフセット。
オープンテレメトリ	127.0.0.1	HTTPポート	55789	HTTPS	受信	サードパーティサービス	メインHTTPポートから+37オフセット。
		Webサーバーポート	55790	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	
			55791				将来の使用のために予約。
			55792				将来の使用のために予約。
			55793				将来の使用のために予約。
			55794				将来の使用のために予約。
			55795				将来の使用のために予約。
NATSブローカー	127.0.0.1	NATS	55796	NATS	受信	AXIS Camera Station 5とコンポーネント間、およびコンポーネント間	メインHTTPポートから+44オフセット。
オープンテレメトリ	127.0.0.1	HTTPポート	55797	HTTP	受信	オープンテレメトリ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	メインHTTPポートから+45オフセット。

その他のポート

ポート	番号	プロトコル	入出力	通信	説明
インターネットHTTPS	80および443	TCP	送信	クライアントと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。
サーバーTCPストリーミングポート	55750	TCP	受信	サーバーと装置	メインHTTPポートから-2オフセット。
アップグレードステータスUDPポート	15156	UDP	受信+送信	サーバーとService Control	AXIS Camera Station 5 Service Controlはこのポートで待ち受け、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。

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 5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 5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`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

データベースのバックアップは毎晩および各システムアップグレードの前に作成されます。AXIS Camera Station 5 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 5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 5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。1～30の数値を使用できます。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 5 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

- データベースに録画が保存されません。代わりに、[**Configuration > Storage (設定 > ストレージ)**] で録画を保存する場所を指定します。録画を個別にバックアップします。
- AXIS Camera Station 5 Service Controlのサーバー設定、プロキシ設定、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 201*」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 200*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、コンポーネントを使用する場合にのみ利用できます。例えば、AXIS Camera Station Secure Entryやスマート検索があります。 • **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。 • **スマート検索**: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である`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。

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 201*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 5を更新すると自動的に。
- AXIS Camera Station 5 Service Controlからデータベースメンテナンスを手動で実行すると。*データベースのメンテナンス, on page 203*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 204*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2つの方法があります。

- `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。
- すべてのデータベースを含むシステムレポートを生成し、データベースのバックアップファイルをコピーします。必ず [**Include all databases (すべてのデータベースを含める)**] を選択してください。*システムレポート, on page 185*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 201*を参照してください。

注

データベースに録画が保存されません。代わりに、[Configuration > Storage (設定 > ストレージ)] で録画を保存する場所を指定します。録画を個別にバックアップします。

データベースを復元するには:

1. AXIS Camera Station 5 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 201*を参照してください。
3. ファイルを抽出します。
4. 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。
5. AXIS Camera Station Secure Entryを使用する場合は、`Components > ACMSM`内のSecureEntry.dbを`C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry 2\INTERNAL\main_db`にコピーします。
6. 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。
7. AXIS Camera Station 5 Service 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 204*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。アクセスコントロールシステムは、まれに強制縮小が行われる場合に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、データベースに対して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、現在および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 5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 - Windowsのメモリー診断を定期的に実行し、RAMメモリーでエラーを探してください。

ツール

AXIS Camera Station 5 Service Controlで [**Modify settings (設定を変更)**] を選択して [**Tools (ツール)**] タブをクリックすると、データベースのメンテナンスを開始したり、部分的システムレポートを作成したりできます。

データベースメンテナンス

- AXIS Camera Station 5 Service Controlを開きます。
- [**Tools (ツール)**] をクリックします。
- [**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。
- 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

- AXIS Camera Station 5 メンテナンス中は、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 5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。

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、AXIS Camera Station 5クライアントで ☰ > [**Help (ヘルプ)**] > [**System report (システムレポート)**]に移動します。

部分的システムレポートを生成するには:

1. [**実行**] をクリックします。
2. ダイアログで求められた情報を選択し、入力します。
3. [**レポートを生成する**] をクリックします。

システムレポートツール	
ファイル名	システムレポートのファイル名を入力します。
フォルダー	システムレポートの保存先を選択します。
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)	選択すると、システムレポートの準備ができたら自動的にフォルダーが開くようになります。
Include database file in report (サーバーレポートにデータベースファイルを含める)	選択すると、システムレポートにデータベースが含まれるようになります。AXIS Camera Station 5データベースには、システムが正常に動作するために必要な録画とデータに関する情報が保存されています。

ネットワークのログ作成

- リンクをクリックして、ネットワークプロトコルアナライザアプリケーションをダウンロードします。
- 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。

認証局をリセットする

- **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 5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。問題は関連するトピックの下に保存されており、探しているものを見つけやすくなっています。トピックは、たとえば音声やライブビューなどです。問題ごとに解決策が説明されています。

詳細情報

*axis.com/support*にアクセスしてください。

- よく寄せられる質問
- 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、トレーニング資料、その他の有益な情報

AXIS Camera Station 5サービス

サーバーが頻繁に再起動する

サーバーが過負荷になると、タスクキューが長くなり、データベースが破損することがあります。

- システムのリソース管理で、AXIS Camera Station 5または他のアプリケーションが大量のリソースを使用しているかどうかを確認します。
- データベースメンテナンスを実行します。*ユーザーマニュアル*の「データベースメンテナンス AXIS Camera Station 5」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サポートに連絡してください。*報告手順, on page 222*に移動します。

ビデオ管理システムの装置

一般的な問題

カメラに接続できない	
VMSがカメラに接続できません。一覧表示されたカメラは追加されませんでした。	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。

インストールがキャンセルされました	
ユーザーがインストールをキャンセルしました。一覧表示されたカメラは追加されませんでした。	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。

カメラのパスワードの設定に失敗した	
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

装置が AXIS Camera Station 5に追加する前に別のシステムで使用されていた場合:

- 装置を工場出荷時の設定に戻します。

装置をビデオ管理システムに追加できない場合、AXIS Device Managerへの追加を試してみてください。

追加する装置モデルとは別の装置モデルを追加できます。

- 装置が新製品の場合や、ファームウェアが新しくリリースされたものである場合、互換性の問題である可能性があります。必ず最新の AXIS Camera Station 5ソフトウェアバージョンを使用してください。

別の装置モデルを追加できない場合:

- カメラのトラブルシューティングを行い、*axis.com/support/troubleshooting*にアクセスしてください。

AXIS Camera Station 5を通じて装置のファームウェアを更新できない

webインターフェースからカメラのアップグレードができない場合:

- カメラのトラブルシューティングを行い、*axis.com/support/troubleshooting*にアクセスしてください。

すべての装置でファームウェアがアップグレードできない

- ネットワーク接続があることを確認します。
- 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 222*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。

- 互換性の問題である可能性があります。Axisサポートに連絡してください。*報告手順, on page 222*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は、ネットワークを自動的に検索して、接続済みのカメラとビデオエンコーダを検出しますが、カメラが見つかりません。

- 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。*ユーザーマニュアル*の「クライアントプロキシ設定 AXIS Camera Station 5」を参照してください。

  - 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 (Transmission Control Protocol) ポート、およびストリーミングポートがセキュリティシステムやNATを通過できるようにしてください。完全なポートリストを閲覧するには、*AXIS Camera Station 5のポートリスト*を参照してください。
  - サーバーと装置の間にプロキシサーバーがある場合は、サーバーのプロキシ設定を変更します。*ユーザーマニュアル*の「Service Control全般 AXIS Camera Station 5」で「プロキシ設定」セクションを参照してください。
- カメラを手動で追加するには、*ユーザーマニュアル*の「デバイスの追加 AXIS Camera Station 5」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おり、電源が供給されていることを確認します。
- 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。
- プロファイル設定を低帯域幅用に最適化するなど、映像と音声の設定を変更します。

録画

録画や再生に影響する可能性のあるパフォーマンスの問題については、*ライブビュー, on page 210*を参照してください。

一般的な問題

連続録画が有効にならない	
一覧表示されたカメラで連続録画がオンになっていません。	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	
システムが録画ストレージを設定できません。	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アプリケーションのインストールに失敗する	
AXIS Video Content Streamをサポートするカメラに、AXIS Video Content Streamをインストールできない場合、このエラーメッセージが表示されます。	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

数秒経っても録画が開始または停止しない場合は、ディスクがいっぱいであるか、割り込みデータが多すぎることを示しています。

- 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、割り込みデータ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。*ユーザーマニュアル*の「ストレージの設定 AXIS Camera Station 5」を参照してください。

連続録画中の録画抜け

録画抜けがあり、「**Recording errors (録画エラー)**」というラベルの付いたアラームが表示されます。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するかどうかを確認してください。一部のカメラでのみこの問題が発生する場合は、そのカメラの過負荷が原因である可能性があります。原因を見つけるために、次の質問を自問してください。

- 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:

- サーバータスクマネージャーで、システムがいずれかのハードウェアリソースを通常より多く使用しているかどうかを確認します。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。
- ディスクに書き込まれるデータ量を削減します (ビデオ設定、ZIPストリーム、フレーム/秒、解像度など)。AXIS Site Designerにより推定されるスループットにも留意してください。*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 210*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、*ユーザーマニュアル*の「エクスポートした録画の再生と検証 AXIS Camera Station 5」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

録画は指定した日数のみ保存されます。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。

ストレージが一杯になると、指定した日数が過ぎていなくても録画が削除されます。
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 5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。
  - 録画にはH.264ビデオ形式を使用してください。M-JPEG形式にはより多くのストレージ容量が必要です。
  - Zipstreamを使用して、録画のサイズをさらに小さくしてください。

フェイルオーバーによる録画の問題

接続が回復した後、フェイルオーバーによる録画がサーバーに記録されていません。

原因	解決策
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。	帯域幅を改善する
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、必ずNTPを同期させてください。 • 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サーバーを設定してください。

AXIS Camera Station 5でのフェイルオーバーによる録画は次のシナリオでは機能しません。

- 制御されたサーバーシャットダウン。
- 10秒未満の短い接続中断。

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 5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	内蔵グラフィックカードの場合、グラフィックカード1枚につき2台を超えるモニターはお勧めしません。 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. AXIS Camera Station 5が専用グラフィックカードに対応していることを確認してください。詳細は*axis.com/products/axis-camera-station/hardware-guidelines*を参照してください。 注 仮想マシン上でクライアントを実行することはできません。

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.com/products/axis-camera-station/hardware-guidelines*を参照してください。
カメラが AXIS Camera Station 5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 5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	Mラインカメラにおいて特に問題になる場合があります。 • 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。*ユーザーマニュアル*の「ストリーミングプロファイル AXIS Camera Station 5」を参照してください。

サーバーの過負荷	
問題の発生と同じ時間に異常なCPU/RAMの使用がある	CPU/RAMを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ます。

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ます。
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オンになっています。*ユーザーマニュアル*の「ストリーミング AXIS Camera Station 5」でハードウェアデコーディング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。
- カメラサーバーレポートを作成し、*axis.com/support/troubleshooting*にアクセスしてください。
- 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、ライブストリームがブロックされる可能性があります。
- AXIS Camera Station 5のフォルダーとプロセスを許可します。「*FAQ*」を参照してください。
- ファイアウォールが特定のポートでの接続をブロックしていないことを確認します。*ユーザーマニュアル*の「Service Control全般 AXIS Camera Station 5」を参照してください。
- サポートされているWindowsサーバーOSバージョンに対応するデスクトップエクスペリエンスがインストールされていることを確認します。*ユーザーマニュアル*の「スケジュールされたエクスポート AXIS Camera Station 5」を参照してください。
- 低解像度のストリームが機能するかどうかを確認します。

上記のいずれでも問題が解決しない場合は、Axisサポートに連絡するか、*報告手順, on page 222*にアクセスしてください。

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 5 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 5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 アプリケーションのインストールに失敗する	
AXIS Video Motion Detection 2または4をインストールできません。このカメラは動きの録画に内蔵の動体検知を使用しています。	アプリケーションを手動でインストールするには、*ユーザーマニュアル*の「カメラアプリケーションのインストール AXIS Camera Station 5」を参照してください。

現在の動体検知の取得に失敗する	
ビデオ管理システムがカメラから動体検知パラメーターを取得できません。このカメラは動きの録画に内蔵の動体検知を使用しています。	アプリケーションを手動でインストールするには、*ユーザーマニュアル*の「カメラアプリケーションのインストール AXIS Camera Station 5」を参照してください。

動体検知が設定されていません	
一覧表示されたカメラで動体検知を設定できません。	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。

動体検知が有効にならない	
一覧表示されたカメラで動体録画がオンになっていません。	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、ビデオ動体検知関連の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。*ユーザーマニュアル*の「AXIS Video Motion Detection 2および4の編集 AXIS Camera Station 5」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。*ユーザーマニュアル*の「内蔵動体検知の編集 AXIS Camera Station 5」を参照してください。

トリガー時間の調整

トリガー期間は2つの連続するトリガー間の間隔であり、この設定は連続する録画の回数を減らすために使用します。この間隔中に別のトリガーが発生しても録画は継続されます。別のトリガーが発生した場合、トリガー時間はその時点から再度カウントされます。

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。

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、次の操作を行ってください。

- 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)] 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)] 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)] 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 5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、*ユーザーマニュアル*の「ストリームプロファイル AXIS Camera Station 5」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有効にしていない場合、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た場合は、クライアントが起動し、ステータスバーに接続状態が表示されます。接続ステータスの詳細については、*ユーザーマニュアル*の「接続ステータス AXIS Camera Station 5」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	指定のサーバーにログインするためのユーザー名とパスワードの組み合わせが有効ではありません。	• 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。 • ユーザーが AXIS Camera Station 5サーバーへのアクセス権を持っていることを確認します。 • AXIS Camera Station 5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。 • サーバーに追加されていないが、ローカルの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。 • ユーザーアクセス権については、ユーザーマニュアルの「ユーザー権限の設定 AXIS Camera Station 5」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	ユーザーは指定したサーバーで AXIS Camera Station 5を使用できません。	[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	サーバーへの安全な接続の設定中に発生するエラーは、ほとんどの場合、クライアントとサーバーの時刻の非同期が原因です。	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	クライアントはサーバーとの接続を確立できませんでした。	• 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。	クライアントはサーバーコンピューターに接続できますが、AXIS Camera Station 5サーバーが実行されていません。	正しいコンピューターに接続していること、AXIS Camera Station 5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	クライアントがサーバーに接続できず、エラーメッセージが表示されます。	ネットワークが適切に設定されていることを確認します。 • 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 5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。 • サーバーとクライアント間にプロキシサーバーがあるかどうかを調査してください。 – Service Controlでサーバーのプロキシを設定します。 – ログインページでクライアントプロキシ設定を行い、[**Change proxy settings (プロキシ設定の変更)**] を選択します。 – Windowsのインターネットオプションでクライアントプロキシ設定を行い、[**Change Proxy settings (プロキシ設定を変更)**] でデフォルトオプションの使用を選択します。
サーバーに接続できません	サーバーへの接続中に不明なエラーが発生しました。	• AXIS Camera Station 5サーバーのアドレスとポートが正しいことを確認します。 • 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ます。詳しくは、「*Axis Secure Remote Accessへのアクセスを許可するようにファイアウォールを設定する*」を参照してください。 • AXIS Camera Station 5Service 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 5 Service Controlを開きます。*ユーザーマニュアル*の「AXIS Camera Station Service Control AXIS Camera Station 5」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	クライアントが、入力されたIPアドレスを解決できませんでした。	• 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 5サーバーのアドレスとポートが正しいことを確認します。 • 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ます。詳しくは、*「Axis Secure Remote Accessへのアクセスを許可するようにファイアウォールを設定する」*を参照してください。
サーバーとクライアントのバージョンが異なります	クライアントはサーバーよりも新しいバージョンの AXIS Camera Station 5 を実行しています。	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。
	サーバーはクライアントよりも新しいバージョンの AXIS Camera Station 5 を実行しています。	クライアントをアップグレードして、サーバーと同じバージョンを実行してください。
サーバーに接続できません。サーバーがビジー状態で応答できません。	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。	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かどうかを確認します。
ローカルの AXIS Camera Station 5 サーバーが実行されていません	[**This computer (このコンピューター)**] を使用して接続しますが、インストールされている AXIS Camera Station 5サーバーが実行されていません。	Service Controlを使用して AXIS Camera Station 5を起動するか、ログインするリモートサーバーを選択します。
このコンピューターに AXIS Camera Station 5サーバーがインストールされていません	[**This computer (このコンピューター)**] を使用して接続しようとしましたが、このコンピューターにはサーバーがインストールされていません。	AXIS Camera Station 5サーバーをインストールするか、別のサーバーを選択します。
選択したサーバーリストは空です	ログインするために選択したサーバーリストが空でした。	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。

- ライセンスキーが正しく入力されたことを確認します。
- AXIS Camera Station 5がインターネットにアクセスできるようにクライアントのプロキシ設定を変更します。
- ライセンスをオフラインで登録します。*ユーザーマニュアル*の「システムをオフラインでライセンスする AXIS Camera Station 5」を参照してください。

- サーバーIDをメモし、*license-portal.lp.axis.com*から AXIS Camera Station 5のライセンスをアクティベートします。
- サーバーの時刻が正しいことを確認します。

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、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 5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

AXIS Camera Station 5 証明書エラーを解決するまで、は装置と通信できません。

考えられるエラー		
証明書が見つかりません	装置の証明書が削除された場合。	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	装置証明書が AXIS Camera Station 5の外部で変更された。権限のない第三者が装置に不正アクセスし、変更を行った可能性があります。	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 5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 5 は装置との接続を失い、一部のシステムコンポーネントが再起動します。

AXIS Camera Station 5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 5 は装置との接続を失い、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サーバーが同期していません。これは、Windows TimeサービスがNTPサーバーに到達できないためです。

- 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。
- 装置は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、装置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. 装置が指定された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、装置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無効にします。

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。

技術サポート

AXIS Camera Station 5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には、 > [Help (ヘルプ)] > [Online Support (オンラインサポート)]を選択するか、*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連絡してください。*Axis*オンラインヘルプデスクを参照してください。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。
- 問題が発生する時刻および関係するカメラ名やIPアドレス。
- AXIS Camera Station 5 問題が発生した直後に生成されたシステムレポート。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。
- 問題を示すすべてのモニターからのスクリーンショットまたは録画 (オプション)。スクリーンショットを撮ったり録画したりするときは、デバッグオーバーレイ機能をオンにしてください。
- 必要に応じて、データベースファイルを含めてください。アップロードを速めるには、これらを除外してください。

問題によっては、サポートチームが必要に応じて要求する追加情報を含めてください。

注

たとえば、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100 MB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	より多くの情報を収集するためにデバッグレベルでのログ作成を使用する場合があります。この作業は、Axisサポートエンジニアから要求があった場合にのみ行います。手順は、*Axis*オンラインヘルプデスクで確認できます。
ライブビューデバッグオーバーレイ	場合によっては、オーバーレイ情報のスクリーンショットや、対象時間帯の値の変化を示すビデオを提供することが役立ちます。オーバーレイ情報を追加するには、次のようにします。 • Ctrlキーとiキーを同時に1回押すと、ライブビューでオーバーレイ情報が表示されます。 • Ctrlキーとi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i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。
ネットワークトレース	サポートエンジニアから要求された場合は、システムレポートを作成する際にネットワークトレースを生成してください。問題が再現可能であれば、問題が発生したときのネットワークトレースを取得してください。これには以下が含まれます。 • カメラで取得された60秒のネットワークトレース (カメラファームウェア5.20以降でのみ適用可能) 必要に応じて、次のVAPIXコマンドを使用して、ログイン、IPアドレス、および期間 (秒) を変更してください。 `http://root:pass@192.168.0.90/axis-cgi/`

補足情報	
	`debug/debug.tgz?cmd=pcapdump&duration=60` • サーバーとカメラ間での通信を示すサーバーで取得された10～30秒のネットワークトレース。
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。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。
スクリーンショット	UIに関連するライブビューの問題の場合は、スクリーンショットを使用してください。たとえば、録画のタイムラインの表示が必要な場合や説明が難しい場合です。
画面の録画	問題を言葉で説明するのが難しい場合、たとえば問題の再現に多くのUI操作が関わる場合は、画面録画を使用してください。

T10122292_ja

2026-02 (M72.2)