IP カメラ Web インターフェース ユーザー ガイド

Avigilon 高解像度 H4 および H5 IP カメラ モデル:

H5A-xx	H5EX-xx-BO1		
H5A-xx-IR	H5EX-xx-CO1		H4A-ETD-KIT
H5SL-xx	H5A-CR1-IR-xx		H4A-THC-BO
H5SL-xx-IR	H4A-xx (-B)	H4M-D	
H5M-DO	H4A-G-xx-IR (-B)	H4F-DO	H3A-xx
H4A-GB (-B)	H4A-xx-IR (-B)	H4SL-xx (-IR)	H3A-BO-IR

マルチヘッド カメラ Web インターフェース ユーザー ガイド

Avigilon マルチヘッド H4 および H5 IP カメラ モデル:

H5DH-xx　　H4A-xMH

Pro カメラ Web インターフェース ユーザー ガイド

Avigilon H4 および H5 Pro IP カメラ モデル:

H5PRO-B　　H4PRO-B

Fisheye カメラ Web インターフェース ユーザー ガイド

Avigilon H5A Fisheye カメラ モデル :

H5A-FE-xx

ビデオ インターコム Web インターフェース ユーザーガイド

Avigilon H4 ビデオ インターコム カメラ モデル:

H4VI-RO1-IR

著作権

Avigilon Corporation
avigilon.com

PDF-H4WebUI-G

改訂: 1 - JA

20211022

目次

はじめに

Avigilon 高解像度 IP カメラはすべて Web インターフェイスを備えているため、ライブ ビデオの視聴や Web ブラウザによるカメラの設定が可能です。

Webインターフェイスには、カメラの設置ガイドに記載の手順をすべて完了させてからアクセスしてください。

> **ヒント：**カメラがサポートしていない機能やオプションは無効になっています。

システム要件

Web インターフェイスには、以下の Web ブラウザのどれかを使用している Windows、Mac またはモバイル デバイスからアクセスできます。

- Microsoft Edge バージョン 44 以降
- Mozilla Firefox バージョン 3.6 以降
- Google Chrome™ バージョン 8.0 以降
- Apple Safari バージョン 5.0 以降
- Android™ 2.2 以降
- Apple iOS バージョン 5.0 以降

その他の Web インターフェース ガイド

その他のタイプのAvigilonカメラについては、次のその他のWebインターフェースガイドを確認します:

- **IP カメラ Web インターフェース ガイド** — H5A カメラ、H5SL カメラなど向けです。
- **PTZ カメラ Web インターフェース ガイド** — パン、ティルト、ズームカメラ向けです。
- **マルチヘッド カメラ Web インターフェース ガイド** — デュアルヘッドおおよびマルチセンサーカメラ向けです。
- **H4およびH5Proカメラ Webインターフェースユーザーガイド**—高解像度プロカメラ向けです。
- **H5A Fisheye カメラ Web インターフェース ガイド** — H5A Fisheye カメラ向けです。
- **ビデオ インターコム Web インターフェース ユーザーガイド**—H4 ビデオインターコム向けです。
- **APD センサー Web インターフェースガイド** — Avigilon Presence Detector 向けです。

Web インターフェイスへのアクセス

カメラを取り付けた後、Web インターフェイスにアクセスするためにカメラの IP アドレスが必要になります。IP アドレスは次の場所にあります。

- Avigilon コントロールセンター (ACC) ソフトウェア ー [セットアップ] タブを開いて、選択したカメラの詳細を表示します。
- Avigilonカメラ設定ツール ー [Network(ネットワーク)] タブに移動して、選択したカメラの詳細を表示します。

IP アドレスを取得したら、次の手順に従って Web インターフェイスにアクセスします。

メモ：Web ブラウザでクッキーを許可するように設定しておかないと、カメラ Web インターフェイスは正しく機能しません。

1. カメラと同じネットワークにアクセスしているコンピュータで、Web ブラウザにカメラの IP アドレスを次のように入力します:

   http://<カメラの *IP* アドレス>/

   例: http://192.168.1.40/
2. カメラにアクセスするためのユーザー名とパスワードの入力を求めるプロンプトが自動的に表示されます。デバイスが工場出荷時のデフォルト状態であり、2020 年 1 月 1 日以降に製造されている場合、デバイスが動作する前に管理者権限を持つユーザーを作成するように求められます。詳細については、「初期ユーザーの作成とログイン」（2ページ）を参照してください。

初期ユーザーの作成とログイン

2020 年 1 月 1 日以降に製造されたカメラには、デフォルトのユーザー名およびパスワードがなく、工場出荷時のデフォルト状態になります。

重要：カメラを操作するには、管理者特権を持つユーザーを作成する必要があります。

ヒント：2020 年 1 月 1 日前に製造されたカメラには、ログインに使用できるデフォルトのユーザー名とパスワードが付属しています。詳細については、「「ログイン」（3ページ）」を参照してください。

カメラが工場出荷時のデフォルト状態の場合、初期ユーザーを作成するために Add User(ユーザーの追加) ページにリダイレクトされます。

1. 新しい**ユーザー名**を入力するか、デフォルトである `administrator` 名を保持します。
2. ユーザーの新しい **Password(パスワード)** を入力します。安全かつ複雑なパスワードを使用することが推奨されます。
3. 新しいパスワードを確認します。
4. 初期ユーザーの場合、*Administrator(*管理者*)* ドロップダウンメニューで **Security Group(セキュリティ グループ)** を選択する必要があります。
5. [**Apply(適用)**] をクリックします。ユーザーを作成後、ログインするように求められます。

ログイン

カメラにアクセスするためのユーザー名とパスワードの入力を求めるプロンプトが自動的に表示されます。

- カメラが工場出荷時のデフォルト状態であり、2020 年 1 月 1 日以降に製造されている場合、カメラを操作する前に管理者権限を持つユーザーを作成するように求められます。ログイン時にこれらの資格情報を使用します。
- ほとんどのカメラでのデフォルトのユーザー名は`administrator`です。パスワードはありません。

ヒント：最初のログイン後にパスワードを追加することをお勧めします。詳細については、「「ユーザーとパスワードの編集」（50ページ）」を参照してください。

Live View(ライブビュー)

ログイン後、最初に表示されるページは「Live View(ライブビュー)」です。ライブビューには、ライブビデオストリームを表示する画像パネルが含まれています。

左上隅のメニュー リンクを使用して、Web インターフェイスを移動します。[**Live View(ライブビュー)**] をクリックすると、いつでもこのページに戻ることができます。

> **ヒント：**カメラがサポートしていない機能やオプションは無効になっています。

静止画を保存する

「Live View(ライブビュー)」ページに [**Save Still to SD Card(静止画像を SD カードに保存)**] ボタンが表示されている場合、カメラは Web インターフェイスからライブ ビデオのスナップショットを取る機能をサポートしています。

この機能を使用するには、カメラに次の設定が必要です：

- SD カードがカメラに挿入されています。詳細については、カメラのインストールガイドを参照してください。SD スロットに挿入された CryptR マイクロカードで FIPS レベル 3 暗号化を使用している場合、SD カードへの画像の保存はサポートされていません。
- カメラのオンボード ストレージ設定は、「Storage(ストレージ)」ページで有効になります。詳細については、「ストレージ」（35ページ）を参照してください。
- カメラのビデオ形式は、「Compression and Image Rate(圧縮および画像レート)」ページで MJPEG に設定する必要があります。詳細については、「圧縮および画像レート」（26ページ）を参照してください。

すべての要件が満たされると、[**Save Still to SD Card(静止画像を SD カードに保存)**] をクリックすることができ、「Live View(ライブビュー)」ページに表示される画像が自動的に SD カードに保存されます。

スナップショットをダウンロードするには、「「Web インターフェイスから録画ビデオをダウンロードする」（37ページ）」を参照してください。

セットアップ

メモ：カメラ モデルがサポートしていなかったり、必要なユーザー許可がない場合、一部のオプションは表示されません。

カメラの工場出荷時のデフォルト設定を使うと、取り付け後、カメラをただちに使用し始めることができます。特別な要件がある場合は、Webインターフェイスから設定をカスタマイズできます。左上のメニュー領域で[**Setup(セットアップ)**]をクリックして使用可能なすべてのセットアップページを表示させます。

各セットアップ ページにある [**Restore Defaults(デフォルトに戻す)**] ボタンを使って工場出荷時のデフォルト設定にリセットすることができます。

設定の一部はカメラの Web インターフェイスからだけ使用でき、ネットワーク ビデオ管理ソフトウェアでは変更できないことに注意してください。

H4 マルチセンサー カメラに特定の設定については、「「H4 マルチセンサー と H5A デュアルヘッドカメラ」（54ページ）」を参照してください。

H4 Edge Solution (ES) のカメラに特定の情報については、「「ACC™ES カメラ」（58ページ）」を参照してください。

H4 Thermal 高温検知カメラに固有の設定については、**H4 Thermal 高温検知カメラ ユーザーガイド**を参照してください。

一般

Setup(セットアップ) リンクをクリックしたときに表示される最初のページは、General(全般)ページです。「General(全般)」ページでは、カメラの識別情報を設定できます。

ヒント：カメラがサポートしていない機能やオプションは無効になっています。

重要：Avigilon H4 マルチセンサーおよび H5A デュアルヘッドカメラは、1 台のカメラに複数のカメラヘッドを備えています。一部の設定はカメラ全体に適用され、その他の設定は個々のヘッドに適用されます。特定のマルチヘッドカメラ設定は、All Heads(すべてのヘッド)タブ上ですべてのヘッドに対してグローバルに設定できますが。他の設定は、Head 1(ヘッド 1)～Head 4(ヘッド 4)タブを使用して、個々のヘッドごとに設定する必要があります。H4 マルチセンサーまたは H5A デュアルヘッドカメラを構成する場合、グローバルヘッド設定と個別ヘッド設定の両方が構成されていることを確認してください。

メモ：ビデオ分析または異常動作検知を備えたカメラを物理的に移動またはを調整した場合、または、フォーカスやズーム レベルを変更した場合は、正確なデータを出力するために学習の進行状況をリセットしてください。カメラの画像レート、および圧縮またはディスプレイの設定が更新されると、学習の進行状況が自動的にリセットされる可能性があります。

1. [**Name(名前)**] フィールドで、カメラに分かりやすい名前を付けます。
2. [**Location(場所)**] フィールドに、カメラの場所を記述します。

   メモ：マルチヘッド カメラの各 Head (ヘッド) について、[**Name(名前)**] と [**Location(場所)**] を設定します。
3. [**View Perspective(視点の方向)**] ドロップダウンリストで、カメラが設置されている取り付け方向を選択します。
   - **Ceiling(天井)** — カメラは天井に取り付けられており、シーンを見下ろしています。
   - **Wall(壁)** — カメラは壁に取り付けられており、シーンを水平に見ています。自己学習型解析、Unusual Motion Detection (UAD)、および改ざん検出は、現在、壁に取り付けられた H5A Fisheye カメラではサポートされていません。

4. [**デバイスの状態 LED を無効にする**] チェックボックスを選択して、カメラデに付いている LED を無効にします。
5. **H5 Pro 40 MP または 61 MP カメラのみ**

   [**Enable ONVIF compatibility (ONVIF 互換の有効化)**] チェックボックスをオンにすると、H5 Pro カメラが ONVIF® を使用してサードパーティの VMS に接続できるようになります。サードパーティの VMS に接続するには、ONVIF との互換性が必要です。

   > **重要：**40MP または 61MP H5 Pro カメラで ONVIF 互換性を有効にすると、解像度が 32MP に制限されます。32 MP ビデオストリームはサードパーティ製 VMS で使用されますが、オンボード ストレージが有効な場合には SD カードで使用されます。Enable ONVIF compatibility (ONVIF 互換の有効化) オプションを無効にして、使用可能な高解像度オプションを表示します。H5 Pro カメラを ACCシステムに接続して、カメラのフル解像度をお楽しみください。

   ONVIF は Onvif, Inc. の商標です。
6. **H4 Pro カメラのみ**

   [**Enable ONVIF compatibility (ONVIF 互換の有効化)**] チェックボックスを選択して、H4 Pro カメラの ONVIF 機能を有効にします。

   > **メモ：**すでに ONVIF が有効になっているカメラを設定するときには、[**Enable ONVIF compatibility (ONVIF 互換の有効化)**] チェックボックスは表示されません。新しいカメラでは、デフォルトで ONVIF が有効になっています。古いカメラでは、カメラのファームウェアをアップグレードした後にこのチェックボックスが表示されることがあります。[**Enable ONVIF compatibility (ONVIF 互換の有効化)**] チェックボックスを有効にすると、ONVIF 互換性を無効にすることができなくなります。カメラがACCシステムに接続されている場合、この機能を有効にする前に、ACCシステムを切断してから、カメラをに再接続する必要があります。
7. [**Mode(モード)**] ドロップダウン リストで、カメラの動作モードを選択します。

   このオプションは使用帯域幅の大きなカメラのみに表示されます。

   - **Full Feature(フル機能)**— これは標準の動作モードです。カメラの全機能を提供します。このモードでは、26 MP H5 Pro カメラで H.265 が無効になります。
   - **High Framerate(フレーム率 (高))**— このモードは、可能な限り最大の画像レートを使用しますが、4K (8 MP)、12 MP H5A Fisheye カメラ、H4 マルチセンサー カメラで自己学習映像解析、Unusual Motion Detection (UMD)、および改ざん検出を無効にし、ES カメラでは WDR を無効にします。

26 MP H5 Pro カメラでは、High Framerate(フレーム率 (高))モードで、自己学習型映像解析と Unusual Motion Detection (UMD) が無効化されます。改ざん検出は、H5Pro カメラではサポートされていません。

モデル	影響を受ける機能High Framerate(フレーム率 (高))
26 MP H5 Pro カメラ： 26C-H5PRO-B	• 自己学習型映像解析が無効 • Unusual Motion Detection (UMD) • H.265（H.265は**Full Feature(フル機能)**モード） で無効
4K（8 MP）H4 HD 解析カメラ： 8.0-H4A-x	• 最大フレームレートが増加 • 自己学習ビデオ分析と改ざん検出無効 • Unusual Motion Detection (UMD) • 三次ビデオストリームの解像度低下 • 2 次ビデオストリーム無効
H4 HD ES 解析カメラ: xx-H4A-xG-x	• 最大フレームレートが増加 • WDR 無効
H4 マルチセンサー カメラ： xx-H4A-xMH-x 12 MP H5A Fisheye カメラ： 12.0W-H5A-FE-xx	• 最大フレームレートが増加 • 自己学習ビデオ分析と改ざん検出無効 • Unusual Motion Detection (UMD) 無効

8. [**Mode(モード)**] ドロップダウンリストから、歪み補正ストリーミングモードオプションを選択して、歪み補正された Fisheye ビデオストリームをデフォルトの 360° Fisheye ビューに追加します。次の歪み補正オプションは、H5A Fisheye カメラをサードパーティ製 VMS に接続する場合の歪み補正ビューに最適です。
    - **Dewarp Streaming 90 x 4 (デワープ ストリーミング 90 x 4)** — この歪み補正モードでは、デフォルトの 360° Fisheye ストリームと 4 つの 90° ストリームを含む 5 つのストリームを Fisheye カメラから送信します。4 つの 90° ストリームは、360° のビュー全体を構成しています。
    - **Dewarp Streaming 120 x 3 (デワープ ストリーミング 120 x 3)** — この歪み補正モードでは、デフォルトの 360° Fisheye ストリームと 3 つの 120° ストリームを含む 4 つのストリームを Fisheye カメラから送信します。3 つの 120° ストリームは、360° のビュー全体を構成しています。

- **Dewarp Streaming 180 x 2 (デワープ ストリーミング 180 x 2)** — この歪み補正モードでは、デフォルトの 360° Fisheye ストリームと 2 つの 180° ストリームを含む 3 つのストリームを Fisheye カメラから送信します。2 つの 180° ストリームは、360° のビュー全体を構成しています。
- **Full Feature(フル機能)** — これは標準の動作モードです。カメラの全機能を提供します。Full Feature(フル機能) が選択されている場合、歪み補正ストリーミングオプションは利用できません。
- **High Framerate(フレーム率 (高))** — このモードは、可能な限り最大の画像レートを使用しますが、4K (8 MP)、12 MP H5A Fisheye カメラで自己学習映像解析、Unusual Motion Detection (UMD)、および改ざん検出を無効にします。

> **メモ：**
> - 歪み補正ストリーミングモード設定を選択すると、H5AFisheyeカメラは、自己学習型解析、UnusualMotionDetection(UAD)、および改ざん検出を自動的に無効にします。12MPH5AFisheyeカメラの最大フレームレートは、15fpsに縮小されます。
> - 歪み補正ストリーミングモードを有効にすると、各ストリームまたはすべてのストリームにカメラ設定を適用できます。各ストリームはヘッドと呼ばれるようになり、個々のヘッドまたはすべてのヘッドに設定を適用できます。詳細については、「カメラヘッドごとの設定を変更する」（57ページ）を参照してください。

9. **H5A Fisheye カメラ (歪み補正ストリーミングモードが有効になっている場合)**

   [**Dewarp Streaming Rotation (デワープ ストリーミングの回転)**] フィールドで、歪み補正された Fisheye ストリームの回転を徐々に設定します。この設定では、歪み補正されたストリームの回転のみを行い、デフォルトの 360° ストリームの回転は変更しません。

10. [Overlay Setting(オーバーレイ設定)] チェックボックスのいずれかを選択して、カメラのビデオストリームにその情報を表示してスタンプします。オプションは次のとおりです。

    - **Display Date(日付を表示)**

      [Display Date(日付を表示)] チェックボックスを選択すると [**Date Format (日付形式)**] ドロップダウン リストも有効になります。リストから、日付を表示するときの日付形式を選択します。
    - **Display Time(時間を表示)**
    - **Display GMT Offset(GMT オフセットを表示)**
    - **Display Name(名前を表示)**
    - **Display Location(場所を表示)**

11. [Time Settings(時間設定)] エリアで、カメラが時間を追跡する方法を選択します。

- カメラの日付と時刻を手動で設定したい場合は、このページにタイムゾーンを入力します。
- 必要に応じて、[**Automatically adjust clock for Daylight Savings Time(夏時間に合わせてクロックを自動調整)**] チェック ボックスをオンにします。
- カメラの日付と時刻を NTP サーバーに自動的に同期させたい場合は、「Network(ネットワーク)」ページで NTP サーバーを設定します。

  このページの一番下にある (Configure NTP Server(NTP サーバーの設定)) リンクをクリックして「Network(ネットワーク)」ページに進みます。NTP サーバーの設定の詳細については、「「ネットワーク」（10ページ）」を参照してください。

注意 ― 時間設定は常に最新のものでなければなりません。そうでないと、ACCソフトウェアはカメラからのビデオストリームを拒否します。時間が常に最新であることを確認するには、次のいずれかを実行する必要があります。

- ACC ソフトウェアで使用される DHCP サーバに NTP を設定します。
- 有効なパブリック NTP サーバーを使用してください。
- [Time Settings(時間設定)] フィールドに手動で正しい時刻を設定します。

12. [**Apply(適用)**] をクリックして、設定を保存します。

ネットワーク

[Network(ネットワーク)] ページでは、カメラがサーバーネットワークに接続する方法を変更したり、カメラが時間を記録する方法を指定することができます。

> **メモ：**カメラの Web インターフェイスでは、HTTPS ポート、RTSP ポート、NTP サーバーのみを設定できます。

1. ページの最上部でカメラが IP アドレスを取得する方法を選択します。
   - **Obtain an IP address automatically(IP アドレスを自動取得)**: このオプションを選択すると、自動で割り当てられる IP アドレスによってネットワークに接続します。

     IP アドレスは DHCP サーバーから取得されます。アドレスを取得できない場合、IP アドレスはデフォルトで 169.254.x.x の範囲のアドレスになります。

- **Use the following IP address (次の IP アドレスを使用)**: 手動で静的 IP アドレスを割り当てる場合に、このオプションを選択します。
  - **IP Address(IP アドレス)**：使用する IP アドレスを入力します。
  - **Subnet Mask(サブネット マスク)**：使用するサブネットマスクを入力します。
  - **Default Gateway(デフォルトのゲートウェイ)**：使用するデフォルトゲートウェイを入力します。

2. IP アドレスを設定する ARP/Ping メソッドを無効にするには、[**Disable setting static IP address through ARP/Ping method(ARP/Ping 方式での静的 IP アドレスの設定を無効にする)**] チェックボックスをオンにします。
3. カメラが IPv6 をサポートしている場合は、[**Enable IPv6 (IPv6の有効化)**] チェックボックスをオンにして 、次の設定を構成します。

   > **メモ：**IPv6 を有効にしても、IPv4 設定は無効になりません。

   a. ステートレス アドレス自動構成を使用する場合は、[**Accept Router Advertisements (ルーター通知の受信)**] チェックボックスをオンにします。
   b. [**DHCPv6 State(DHCPv6状態)**]ドロップダウンリストから、次のいずれかを選択します。
      - **Auto (自動)**: DHCPv6 ステートがルーター通知 (RA) で決まります。

        > **メモ：**この設定Accept Router Advertisements (ルーター通知の受信)を想定どおりに実行するには、 設定を有効にする必要があります。

      - **Stateful (ステートフル)**: カメラは DHCPv6 サーバーから IP アドレスと DNS および NTP 情報を受け取ります。
      - **Stateless (ステートレス)**: カメラは DHCPv6 サーバーから DNS および NTP 情報のみを受け取ります。DHCPv6 サーバーからの IP アドレスは受け入れません。
      - **Off**: カメラは DHCPv6 サーバーと通信しません。
   c. [**Static IPv6 Addresses (静的 IPv6 アドレス)**] フィールドに、優先される IPv6 アドレスを入力します。追加のアドレスについては、**+** をクリックします。

      プレフィックス長を変更するには、クラスレス ドメイン間ルーティング (CIDR) 表記を使用して優先される IPv6 アドレスを入力します。たとえば、 `2001:db8::1/32` はアドレスプレフィックスが 32 ビット長であることを示します。

      デフォルトでは、プレフィックスの長さは `/64` に設定されています。

> **メモ：**Web インターフェイスで設定したプレフィックス長が正しく表示されない場合がありますが、カメラが使用するプレフィックスは設定した長さになります。

d. [**Default Gateway(デフォルトのゲートウェイ)**] フィールドに、優先的に使用するデフォルト ゲートウェイを入力します。RA が無効になっている場合にのみ、デフォルト ゲートウェイを割り当てることができます。

カメラにアクセスするために使用することができる IPv6 アドレスは **Current IPv6 Addresses (現在の IPv6 アドレス)** エリアの下に記載されています。

4. ホスト名をカスタマイズする必要がある場合は、[**Hostname(ホスト名)**] フィールドにホスト名を入力します。
5. [DNS Lookup(DNS ルックアップ)] エリアで、カメラがドメイン名システム (DNS) サーバーアドレスを取得する方法を選択します。
    - **Obtain DNS server address automatically(DNS サーバーアドレスを自動取得する)**：DNSサーバーを自動的に見つけるには、このオプションを選択します。
    - **Use the following DNS server addresses(次の DNS サーバーアドレスを使用する)**：DNSサーバーアドレスを手動で設定するには、このオプションを選択します。最大で 3 つのアドレスを設定できます。
        - **Preferred DNS server(優先する DNS サーバー)**：このフィールドに優先 DNS サーバーのアドレスを割り当てます。
        - **Alternate DNS server 1(別の DNS サーバー 1)**：（オプション）代替 DNS サーバーのアドレスをこのフィールドに割り当てます。優先されるサーバーが使用できない場合、カメラはこのサーバーへの接続を試みます。
        - **Alternate DNS server 2(別の DNS サーバー 2)**：（オプション）別の代替DNSサーバーのアドレスをこのフィールドに割り当てます。優先されるサーバーと最初の代替サーバーの両方が使用できない場合、カメラはこのサーバーへの接続を試みます。
6. [Control Ports(制御ポート)] エリアで、カメラにアクセスするために使用する制御ポートを指定することができます。1～65534の任意のポート番号を入力できます。デフォルトのポート番号は次のとおりです。
    - **HTTP Port(HTTP ポート)**: 80

      カメラのアクセスをセキュア接続のみに制限したい場合は、[**Enable HTTP connections (HTTP 接続を有効化)**] チェックボックスをオフにします。HTTP Port(HTTP ポート) アクセスはデフォルトで有効になっています。
    - **HTTPS Port(HTTPS ポート)**: 443
    - **RTSP Port(RTSP ポート)**: 554
    - **RTSP Replay Port(RTSP Replay ポート)**: 555

7. NTP Server(NTP サーバー)エリアでは、カメラに NTP サーバーを使用して時間を維持させるかどうかを指定します。
    1. 時間を維持するために使用する NTP ソースを選択します。
        - **Always use Avigilon Control Center NTP Server (常に Avigilon Control Center NTP Server を使用する)**。Avigilonコントロールセンター™ ソフトウェアのみを使用してカメラに時間を維持させる場合は、このオプションを選択します。
        - **Always use external NTP server (常に外部 NTP サーバーを使用する)**。外部 NTP サーバのみを使用する場合は、このオプションを選択します。次に、使用する NTP サーバを設定します。
        - **Use Avigilon Control Center Server with a failover external NTP(外部の Avigilon Control Center サーバーに接続していないときに、NTP サーバーを使用する)**。デフォルトではAvigilon、カメラがAvigilonコントロールセンターソフトウェアを使用して時間を維持し、設定されている場合は、ACCサーバーに接続していないときに外部の NTP サーバを使用します。
    2. 外部 NTP サーバーを使用している場合は、サーバーの設定方法を選択します。
        - **DHCP:(DHCP:)**。
        - **Manual:(手動:)**。このオプションを選択して、[**NTP Server(NTP サーバー)**] フィールドにサーバー アドレスを入力します。
8. MTU(MTU)領域で、最大伝送単位(MTU)サイズをバイト単位で設定します。右側に表示される範囲の値を入力します。ネットワーク接続が遅い場合は、MTUサイズを小さくすることをお勧めします。
9. Ethernet Setting(イーサネット設定)エリアで、ネットワーク接続のための**Speed & Duplex(速度とデュプレックス)**を設定します。Auto-negotiation (default)(オートネゴシエーション (デフォルト))設定はほとんどのカメラに推奨される設定であり、ネットワーク接続に最適な速度とデュプレックス設定をネゴシエートします。必要に応じて、接続の速度とデュプレックス設定を手動で選択できます。
10. Security(セキュリティ)エリアで、カメラとサーバー間の通信を暗号化するためにカメラが使用し、使用すべきでない古い TLS バージョンをブロックする**Minimum TLS version(最小 TLS バージョン)**を設定します。
    - **TLS 1.2**は、セキュリティを強化するために推奨されます。
    - **TLS 1.1**は、下位互換性のために必要な場合に選択できます。
11. [**Apply(適用)**] をクリックして、設定を保存します。

802.1x ポートベース認証の設定

ネットワーク スイッチが 802.1x ポート ベース認証を必要とする場合、適切なカメラの資格情報を設定してスイッチがビデオ ストリームをブロックしないようにすることができます。

1. 左のメニューペインで **Network(ネットワーク) > 802.1X(802.1X)** を選択します。
2. 「Configure 802.1X Profiles(802.1X プロファイルの設定)」ページで、優先する認証方法を選択します。複数のプロファイルを設定できます。一度に 1 つのプロファイルしか有効にできないことに注意してください。

   [**EAP Method(EAP 方式)**] ドロップダウン リストで、次のいずれかを選択して関連のフィールドを完成します:

   - ユーザー名とパスワードの認証に **PEAP(PEAP)** を選択します。
     - **Configuration Name(設定名):** プロファイルに名前を付けます。
     - **EAP Identity(EAP アイデンティティ):** カメラを認証するために使用されるユーザー名を入力します。
     - **Password(パスワード):**カメラを認証するために使用されるパスワードを入力します。
   - 証明書認証のために **EAP-TLS(EAP-TLS)** を選択します。
     - **Configuration Name(設定名):** プロファイルに名前を付けます。
     - **EAP Identity(EAP アイデンティティ):** カメラを認証するために使用されるユーザー名を入力します。
     - **TLS Client Certificates(TLS クライアント認証):** カメラを認証するために PEM エンコードされた証明書ファイルを選択します。
     - **Private Key(秘密鍵):** カメラを認証するために PEM エンコードされた秘密鍵ファイルを選択します。
     - **Private Key Password(秘密鍵パスワード):** 秘密鍵にパスワードが設定されている場合は、ここでパスワードを入力します。
     - [**Upload Files(ファイルのアップロード)**] をクリックすると、TLS クライアント認証と秘密鍵がカメラにアップロードされます。アップロードされたファイルを使って、カメラの認証に使うための一意の認証が生成されます。一意の証明書が [Uploaded Certificate(アップロード済み証明書)] フィールドに表示されます。
3. [**Save Config(設定を保存)**] をクリックして、認証プロファイルを保存します。

   これがカメラに追加される最初のプロファイルの場合、自動的に有効になります。

   保存された設定は**Saved802.1XConfigurations(保存済みの802.1X設定)**の下に表示されます。

802.1X 認証プロファイルの切り替え

別の認証プロファイルを使用するには、保存された設定を選択して、[**Enable(有効化)**]をクリックします。

802.1X認証プロファイルの削除

認証プロファイルの1つを削除するには、保存された設定を選択して、[**Remove(削除)**]をクリックします。

SNMP の設定

簡易ネットワーク管理プロトコル (SNMP) を使用して、ネットワークに接続されているカメラの管理に役立てることができます。SNMP を有効にした状態で、カメラの状態情報を SNMP 管理ステーションに送信することができます。

「SNMP(SNMP)」ページでは、カメラの SNMP 設定を構成し、管理ステーションページに送信される状態情報を選択することができます。送信されるステータス情報またはトラップの詳細については、Avigilon Web サイト (http://avigilon.com/support-and-downloads) でカメラの管理情報ベース (MIB) ファイルを参照してください。

1. 左のメニューペインで **Network(ネットワーク) > SNMP(SNMP)** を選択します。
2. 「SNMP(SNMP)」ページで、[**EnableSNMP(SNMPの有効化)**]チェックボックスをオンにします。
3. [**Version(バージョン)**] ドロップダウン リストで、優先する SNMP バージョンを選択します。両方のバージョンを設定できますが、一度に有効にできるバージョンは 1 つだけであることに注意してください。
    - **SNMP v2c(SNMP v2c)**: SNMP v2c を使用すると、「SNMP Get」リクエストを使用してカメラの状態情報をリクエストし、カメラからトラップ通知を受け取ることができます。

      [**SNMP v2c Settings(SNMP v2c 設定)**] エリアで、[**Enable Traps(トラップの有効化)**] チェック ボックスをオンにして、カメラからのトラップ受信を有効にします。

        a. **Read Community(読み取りコミュニティ):** カメラの読み取りコミュニティ名を入力します。この名前は SNMP トラフィックの認証に使用されます。同じ読み取りコミュニティ名を持つ SNMP 管理ステーションのみがカメラから応答を受け取ります。

        b. **Trap Destination IP(トラップの送信先 IP):** トラップが送信される管理ステーションの IP アドレスを入力します。

           [Available Traps(使用可能なトラップ)] エリアでは、送信されるトラップを選択します。

            - **Temperature Alert(温度アラート):** カメラの温度がサポート対象のしきい値を上回る、または下回ると、トラップ通知が送信されます。カメラの温度が標準に戻ったときも、通知が送信されます。
            - **Camera Tampering(カメラの改ざん):** カメラのビデオ解析でシーンの突然の変化が検出された場合に、トラップ通知が送信されます。

- **Edge Storage Status(エッジ ストレージの状態):** SD カードのステータスが変化した場合に、トラップ通知が送信されます。
- **IR Illuminator Status (IR 照明の状態):** H4 マルチセンサー カメラの IR LEDリングのステータスが変化した場合に、トラップ通知が送信されます。

- **SNMP v3(SNMP v3):** SNMP V3 を使用して、「SNMP Get」リクエストで状態情報をリクエストすることができます。SNMP v3 はトラップをサポートしていません。

  SNMPv3では、カメラのユーザー名とパスワードを設定して、セキュリティを強化することができます。このカメラでは、SHA-1タイプの認証とAESタイプの暗号化が使用されます。

  [SNMP v3 Settings(SNMP v3 設定)] 領域で、次の項目を入力します。

  a. **Username(ユーザー名):** カメラに「SNMP Get」リクエストを送信する際に管理ステーションが使用しなければならないユーザー名を入力します。

  b. **Password(パスワード):** 管理ステーションが選択されたユーザー名と一緒に使用しなければならないパスワードを入力します。

4. [**Apply(適用)**] をクリックして、変更を保存します。

高度なネットワーク

ネットワーク通信のセキュリティを強化するために、サーバーおよびカメラ通信用の暗号化モジュールの連邦情報処理標準（FIPS）140-2 レベル 1 またはレベル 3 のセキュリティ要件への準拠を有効にすることができます。

メモ：
- FIPS 140-2 レベル 1 では、FIPS カメラライセンスを購入する必要があります。
- FIPS 140-2 レベル 3 では、CRYPTR マイクロカードを購入する必要があります。CRYPTR カードを有効にするには、カメラの SD カードスロットに挿入する必要があります。

1. Advanced(詳細)Network(ネットワーク)セットアップページに移動します。
2. EncryptionEngine(暗号化エンジン)ドロップダウンリストで、使用する暗号化のタイプを選択します。
   - **Open SSL**は、暗号化のデフォルトオプションです。
   - **FIPS 140-2**は、FIPS 140-2 レベル 1 暗号化を有効にします。
   - **CRYPTR micro(CRYPTR マイクロ)**は、インストールされた CRYPTR カードがキーを安全に保管できるようにし、FIPS140-2 レベル 3 の要件を満たします。

重要：設定をCRYPTR micro(CRYPTR マイクロ)に切り替えると、カメラが新しいキーと自己署名証明書を生成します。この設定を有効にすると、証明書とキーの管理が必要になる場合があります。以前のキーが認証局（CA）によって署名されていた場合、カメラへの接続を安全に保つために、新しく生成されたキーも CA が署名する必要があります。
Camera Configuration Tool（CCT）を使用して、カメラから証明書署名要求（CSR）を生成し、署名された証明書をカメラにアップロードし直すことができます。詳細については、 *Camera Configuration Tool User Guide (*カメラ設定ツール ユーザー ガイド*)*を参照してください。

3. **Apply(適用)**をクリックして設定を保存します。

重要：カメラでこの設定を変更すると、カメラを再起動する必要があり、その間ビデオストリームは失われます。Avigilonは、重要度の低い動作時間中にこの設定を適用することをお勧めします。

CRYPTR 暗号化を有効にすると、サイドメニューで選択することにより**CryptR Log(CryptR ログ)**ページにアクセスできます。CRYPTR micro の内部監査ログが 80%の容量に達すると、エントリは CRYPTR micro から自動的にプルされ、カメラの syslog に記録され、CRYPTRmicro のオーディオログが消去されます。**CryptR Log(CryptR ログ)**ページには、カメラの syslog にまだ記録されていないエントリのみが表示されます。

メモ：CRYPTR マイクロカードがカメラに挿入されて有効な状態の場合、取り出されたり使用できなくなったりすると、カメラはFIPS 140-2モードで再起動します。カードがカメラに再挿入された場合、CryptR マイクロカードを引き続き使用してキーを保存するには、CRYPTR micro (CRYPTR マイクロ)をEncryption Engine(暗号化エンジン)として再選択する必要があります。

IP フィルター

IP Filter(IP フィルター)ページでは、どの IP アドレスがカメラに接続できるかを制御できます。

有効にすると、次の 2 通りの方法で IP アドレスを制限するオプションがあります。

- 特定のIPアドレスまたはアドレスの範囲に対するDeny Access(アクセスを拒否)。
- 特定の IP アドレスまたはアドレスの範囲に限定したAllow Access(アクセスを許可)。

重要：Allow Access(アクセスを許可)オプションを使用して IP アクセスをフィルタリングすることを選択した場合、許可される正しいアドレスが構成されていることを確認してください。そうしないと、カメラからロックアウトされる可能性があります。

1. 左側のメニューペインで **Network(ネットワーク) > IP Filter(IP フィルター)** を選択します。
2. **Enable IP Filter(IP フィルターの有効化)**チェックボックスを選択して、IP フィルタリングを有効にします。
3. ページの最上部で、カメラが IP アドレスをフィルターする方法を選択します。
   - **Allow Access(アクセスを許可)**：このオプションを選択すると、以下で作成する特定の IP アドレスエントリへのアクセスのみが許可されます。正しい IP アドレスエントリを追加してください。そうしないと、カメラからロックアウトされる可能性があります。
   - **Deny Access(アクセスを拒否)**：このオプションを選択すると、以下で作成する特定の IP アドレスエントリへのアクセスが拒否されます。これはデフォルトオプションです。
4. アクセスを拒否または許可するIP Filter Entries(IP フィルター エントリー)をすべて追加します。
   a. **+**をクリックして、IP フィルターリストにエントリを追加します。
   b. 表示される**IPv4, IPv6 or CIDR range(IPv4、IPv6 または CIDR 範囲)**フィールドに、フィルタリングする IP アドレスの IPv4、IPv6、または CIDR 範囲を入力します。
   c. フィルタリングに必要なすべての IP アドレス追加が完了するまで、リストにエントリを追加し続けます。

   ヒント：最大 256 のIP Filter Entries(IP フィルター エントリー)を追加できます。
5. [**Apply(適用)**] をクリックして、設定を保存します。

   メモ：カメラへの接続に現在使用している IP アドレスへのアクセスを拒否または許可していない場合、Apply(適用)をクリックすると Web インターフェイス接続が閉じます。

Image and Display(画像および表示)

ヒント：カメラがサポートしていない機能やオプションは無効になっています。

重要：Avigilon H4 マルチセンサーおよび H5A デュアルヘッドカメラは、1 台のカメラに複数のカメラヘッドを備えています。一部の設定はカメラ全体に適用され、その他の設定は個々のヘッドに適用されます。特定のマルチヘッドカメラ設定は、All Heads(すべてのヘッド)タブ上ですべてのヘッドに対してグローバルに設定できますが。他の設定は、Head 1(ヘッド 1)～Head 4 (ヘッド 4)タブを使用して、個々のヘッドごとに設定する必要があります。H4 マルチセンサーまたは H5A デュアルヘッドカメラを構成する場合、グローバルヘッド設定と個別ヘッド設定の両方が構成されていることを確認してください。

メモ：ビデオ分析または異常動作検知を備えたカメラを物理的に移動またはを調整した場合、または、フォーカスやズーム レベルを変更した場合は、正確なデータを出力するために学習の進行状況をリセットしてください。カメラの画像レート、および圧縮またはディスプレイの設定が更新されると、学習の進行状況が自動的にリセットされる可能性があります。

「Image and Display(画像および表示)」ページで、カメラのデイ/ナイトおよび露出設定をコントロールできます。

「Image and Display(画像および表示)」ページには、カメラのライブビデオストリームを表示する画像パネルがあります。[**Apply(適用)**] をクリックして変更を保存すると、ビデオ ストリームが更新されて新しい設定を使用します。

画像パネル下の右側に次の情報が表示されます：

- Current Exposure(現在の露出)
- Current Gain(現在のゲイン)
- Current Iris(現在のアイリス)
- Last Known Light Level(最新の既知照明レベル)

多くの Avigilon 高解像度 IP カメラにはデジタル ズームとフォーカス コントロールが備わっており、このページでもカメラのズームとフォーカスを設定することができます。

1. **Zoom(ズーム)** スライダーを使用して、カメラのズーム位置を調整します。
    - ズームアウトするには、スライダーを右に動かします。
    - ズームインするには、スライダーを左に動かします。
2. カメラのフォーカスを手動で合わせるには、[**Focus(フォーカス)**] ボタンを使用します。

- フォーカスをゼロに近づけるには：
  - 大きなステップで移動するには、**<<** をクリックします。
  - 小さなステップで移動するには、**<** をクリックします。
  - ゼロにフォーカスするには **0** をクリックします。
- フォーカスを無限に近づけるには：
  - 大きなステップで移動するには、**>>** をクリックします。
  - 小さなステップで移動するには、**>** をクリックします。
  - 無限にフォーカスするには [**Inf(無限)**] をクリックします。
- 可能な場合は、[**Auto Focus(オートフォーカス)**] をクリックして、カメラにオート フォーカスさせます。

  メモ：フォーカスがマニュアルで設定されたら、変化しません。

3. 夜間にモノクロ モードでカメラのフォーカスが合っていない場合は、**IR Focus Offset(赤外線フォーカス オフセット)** スライダーを調整して、内蔵または外部の IR 照明によるフォーカス シフトを補正します。
4. マルチヘッドカメラを構成している場合、カメラ全体または個々のヘッドに適用される設定があります。
   a. [**All Heads(すべてのヘッド)**] タブを選択して、カメラヘッドのすべてに適用される設定を調整します。
   b. AllHeads(すべてのヘッド)タブでは、**Imagingmode(撮像モード)**を設定することができます。
      - **Global(グローバル)**を選択して、カメラヘッドのすべてに同じデイ/ナイトと露出設定を適用します。[AllHeads(すべてのヘッド)]タブにある設定を使って、カメラの画像設定を調節します。各番号付きヘッドタブに対して同じ設定が無効になっています。
      - **Per-head(ヘッド単位)**を選択して、各カメラヘッドに異なるデイ/ナイトと露出設定を適用します。異なるヘッドタブを選択して、各カメラヘッドの設定を変更します。
   c. 番号の付いた各ヘッドタブを選択して、各カメラヘッドのフォーカスコントロールを調整します。これらの設定は、カメラヘッドごとに手動で調整する必要があります。

5. カメラが環境照明条件を補正する方法を設定するには、次の設定を定義します。
    - **Day/Night Mode(日中/夜間モード):** [Day/Night Mode(日中/夜間モード)] ドロップダウン リストで、ビデオ画像の昼モードと夜モードの切り替え方法を設定します。
        - **Automatic(自動)**: 光のレベルがデイ/ナイトのしきい値を超えると、ビデオ画像はカラーになります。光レベルがデイ/ナイトのしきい値より低くなると、カメラが自動的に赤外線カットフィルターを開き、モノクロモードに切り替わります。赤外線照明が有効な場合は、これもオンになります。
        - 一定時間経過すると自動的にデイ/ナイトモードを **Automatic** に戻すには、[**タイムアウト後に自動復元 (Restore Automatic after Timeout)**] ボックスにチェックマークをつけます。[**タイムアウト (Timeout)**] フィールドには、タイムアウト期間として 5s と 3600s の間の値を割り当てることができます。
        - デイ/ナイトのしきい値の設定には、[**Day/Night Threshold(日中/夜間しきい値)**] スライダーを使います。スライダーを動かして、カメラが昼モードと夜モードで切り替わる照明レベルを選択します。スライダーを使用できるのは、[Day/Night Mode (日中/夜間モード)] 設定が [**Automatic(自動)**] に設定されているときだけです。

          スライダーは、次のいずれかの値を表示することがあります。
            - **日中/夜間しきい値 (EV):** スライダーの値は、露光値 (EV) です。

              昼モードでは、最後の既知の光レベルが画像パネルの下に表示され、Day/Night Threshold(日中/夜間しきい値) スライダーの青いバーとしても表示されます。
            - **Day/Night Threshold (gain dB)(日中/夜間しきい値（ゲイン dB）):** スライダーの値は、デシベル (dB) です。
        - **Hysteresis(ヒステリシス)** 設定を使用して、しきい値オフセットを絞り込みます。
            - 明暗レベル差が小さいシーンでカメラを日から夜に切り替えるときに **Low (低)** を選択します。
            - 明暗レベル差が大きい場合にカメラのモードを切り替えるときに **High(高)** を選択します。
            - デフォルト値は **Medium(中)** です。
        - **Color(カラー)**: ビデオ画像は常にカラーになります。
        - **Monochrome(モノクロ)**: ビデオ画像は常にモノクロになります。

- **External(外部)**: カメラは IR カット フィルターを開き、でデジタル入力回路の状態によってモノクロ モードに切り替わります。

  > **メモ：**既定のデジタル入力回路の状態は、「Digital Inputs and Outputs(デジタル入出力)」ページで設定されます。詳細については、「「デジタル入出力」（39ページ）」を参照してください。

- **Day/Night Delay (seconds) (日中/夜間遅延 (秒))**: 設定したしきい値に達すると、デイ/ナイトモードの切り替えが行われるまでの遅延時間を秒単位で設定します。
- **IR LED の有効化:** 手動でカメラに取り付けられている IR 照明を有効または無効にすることができます。
- **Enable Adaptive IR Compensation(適応型赤外線補正の有効化):** 適応型 IR 補償により自動の IR 調整を有効にすることができます。これにより、IR 照明によって生じた彩度をカメラがビデオ画像で自動的に調整できるようになります。
- **自動コントラスト ROI を表示 (Show Auto Contrast ROI):** このオプションを有効にすると、対象領域を表示して選択できます。コントラストは、選択した領域に基づいて自動的に調整されます。
- **Enable Night Visibility Check (夜間視認性チェックの有効化):** 手動でカメラの夜間の視認性チェックを有効または無効にすることができます。夜間視認性チェックを有効にすると、デイモードとナイトモードを定期的に切り替えて、ナイトモードからデイモードに切り替えるのに十分な光レベルがあるかどうかを確認します。無効にすると、カメラは最適度の低い方法を使用して、日中モードに切り替えるのに十分な光レベルかどうかを判断します。

  > **メモ：**夜間可視性チェックを無効にすると、カメラが夜間モードと昼間モードの切り替えを遅らせ、切り替え時間の最適性が低下する可能性があります。たとえば、カメラは必要よりも 30 分間長く夜モードになったままになります。

6. 画像の露出を調整するには、Exposure Settings(露出設定) を調整します。
   - **Flicker Control(フリッカー制御):** カメラ周辺の蛍光灯があるため、ビデオ画像が揺らぐ場合は、Flicker Control(フリッカー制御) を蛍光灯と同じ周波数に設定して、揺らぎの影響を低減できます。一般的に、ヨーロッパは**50Hz**で、北米は**60Hz**です。

     > **メモ：**このコントロールをリセットすると、数秒間ビデオストリームが停止します。

- **Enable Wide Dynamic Range(ワイド ダイナミック レンジの有効化):** ワイド ダイナミック レンジ (WDR) による自動のカラー調整を有効にすることができます。これにより、カメラはビデオ画像を調整して、明るい光と暗い影がはっきりと見えるシーンに対応できます。
- **Exposure(露出):Automatic(自動)** を選択してカメラで露出を制御できるようにするか、特定の露出レートを設定することができます。

  > **メモ：** 手動露出時間を長くすると、画像レートに影響する場合があります。

- **Exposure Offset(露出オフセット):** これは、露出オフセット値を設定することで、特殊な照明条件を補正することができる高度な設定です。負の値を指定すると、画像が持続的に暗くなり、正の値を指定すると、画像が持続的に明るくなります。
- **Maximum Exposure(最大露出):** 最大露出レベルを選択して、自動露出設定を制限することができます。[Maximum Exposure(最大露出)] のドロップダウンリストを使用できるのは、[Exposure(露出)] 設定が [Automatic(自動)] に設定されているときだけです。

  最大の露出レベルを光量が低い状況に設定すると、カメラの露出時間を制御して、画像をぼやけさせずに光量を最大にできます。
- **Priority(優先度): Max Image Rate (最大画像レート)** か **Exposure(露出)** を優先項目として選択することができます。
  - **Max Image Rate (最大画像レート)** に設定すると、カメラは優先項目として画像レートの設定を維持し、設定された画像レートで記録できるものを越えて露出を調整しません。
  - **Exposure(露出)** に設定すると、カメラは優先項目として露出設定を維持し、最高の画像をアーカイブするために設定された画像レートをオーバーライドします。
- **Maximum Iris(最大アイリス):** 最大絞り値を設定することにより、レンズが使用する最大絞り値を制限することができます。この値はF値です。この値も、レンズの最大の絞りに対する露出値 (EV) です。この設定を使用できるのは、[**Iris(アイリス)**] 設定が [**Automatic(自動)**] に設定されているときだけです。

  絞り値は、フォーカスが合っているシーンの量にも影響します。最小の F 値 (0 EV) は、絞りを可能な限り大きな値に設定します。これはカメラへの入光量を最大にしますが、シーン中のピントが合う領域は小さくなります。F値が大きくなる（負のEV）と最大の絞りが小さくなり、シーン中でピントが合う領域が増えます。カメラは、ゲインを高くするか露光時間を長くすることにより、減少した光を自動的に補正します。
- **Preferred Iris(優先アイリス):** より一般的な光の状態に合わせて露出とフォーカスが最適になるように、理想的な絞り値を設定します。この値はF値です。この値も、レンズの最大の絞りに対する露出値 (EV) です。この設定を使用できるのは、[**Iris(アイリス)**] 設定が [**Automatic(自動)**] に設定されているときだけです。

> **メモ：** Preferred Iris(優先アイリス) の値は、Maximum Iris(最大アイリス) の値以下にする必要があります。

最小の F 値 (0 EV) は、絞りを可能な限り大きな値に設定します。これはカメラへの入光量を最大にしますが、シーン中のピントが合う領域は小さくなります。F値が大きくなる（負のEV）と絞りが小さくなり、シーン中でピントが合う領域が増えます。カメラは、ゲインを高くするか露光時間を長くすることにより、減少した光を自動的に補正します。

- **BacklightCompensation(逆光補正):**シーン中に強い光があるために画像全体が暗くなる場合は、[BacklightCompensation(逆光補正)]値を適切な露出の画像になるように調整します。
- **Iris(アイリス):** を選択すると、カメラで絞りを制御することも **Automatic(自動)**、手動で絞りを **Open(開)** か **Closed(閉じる)** に設定することもできます。
- **Maximum Gain(最大ゲイン):** 最大ゲイン レベルを選択して、自動ゲイン設定を制限することができます。

  光が弱い状況用に最大ゲイン レベルを設定すると、画像に過剰なノイズを入れずに画像のディテールを最高にできます。
- **均等 (Equalization):** この設定では、カメラの画像を調整して、暖色の物体と冷色の物体の色差を均等にします。値を小さくするほど暖色のオブジェクトが目立つようになります。値を大きくすると、よりバランスの取れたビデオ画像が得られます。
- **Color Palette:** [カラー パレット (Color Palette)] を選択して、サーマル カメラから取得された情報の表示方法を変更します。このオプションは、H4 Thermal 高温検知カメラでは使用できません。次のオプションの 1 つを選択します。
  - WhiteHot – グレー スケール。白が高い温度、黒が低い温度を示します。
  - BlackHot – グレー スケール。黒が高い温度、白が低い温度を示します。
  - Rainbow – マルチカラー。赤色が高い温度、青色が低い温度を示します。

7. [**Apply(適用)**] をクリックして、変更を保存します。

調整

「Adjustments(調整)」 ページで、ビデオ画像の色、コントラスト、明るさの設定を制御できます。

「Adjustments(調整)」ページには、カメラのライブ ビデオ ストリームを表示する画像パネルも含まれています。[**Apply(適用)**] をクリックして変更を保存すると、ビデオ ストリームが更新されます。

> **ヒント：** カメラがサポートしていない機能やオプションは無効になっています。

1. 左側のメニューペインで**Image and Display(画像および表示) > Adjustments(調整)**を選択します。
2. マルチヘッドカメラを構成している場合、カメラ全体または個々のヘッドに適用される設定があります。
    a. [**All Heads(すべてのヘッド)**] タブを選択して、カメラヘッドのすべてに適用される設定を調整します。
    b. 番号が付けられた各ヘッドタブを選択して、各カメラヘッドのビデオ画像の色、コントラスト、および明るさの設定を調整します。
3. 必要に応じてビデオ画像を調整します。

    プリセット設定を使用するか、独自のカスタム設定を作成できます。[**Preset(プリセット)**] のドロップダウン リストで、希望する設定を選択します:

    a. **Avigilon:** このプリセットは、ビデオ監視に推奨される輝度と色のバランスを提供します。
    b. **Standard(標準):** このプリセットは、屋内または屋外シーンにおける一般的な昼夜変化用に設定されています。
    c. **Vivid(鮮明):** このプリセットは、より飽和した画像のために色と輝度を増加させます。
    d. **Custom(カスタム):** 次の画像設定を手動で調整する場合はこのオプションを選択します。

    > **メモ：**ワイド ダイナミック レンジが有効な場合、Brightness(輝度) および Contrast(コントラスト) 設定は無効になります。

    - **Saturation(彩度)**: 割合の数を入力することにより、ビデオの色の濃さを調整することができます。

      0 は白黒の画像を作成し、100 は濃い色の画像を作成します。
    - **Sharpness(シャープネス)**: 割合の数を入力することにより、ビデオのシャープネスを調整することができます。

      0 はシャープネスを最小にし、100 はシャープネスを最大にして、オブジェクトの端を見やすくします。
    - **Brightness(輝度)**: 割合の数を入力することにより、ビデオの輝度を調整することができます。

      0 は暗い画像を作成し、100 は明るい色の画像を作成します。
    - **Contrast(コントラスト)**: 割合の数を入力することにより、ビデオのコントラストを調整することができます。

      0 は画像中のオブジェクトとオブジェクトの間のコントラストを最小にし、100 はコントラストを最大にします。

4. **White Balance(ホワイト バランス)**ドロップダウン リストを使って、ホワイトバランス設定の制御方法を選択します:
    - **Automatic(自動)**: カメラが自動的にホワイトバランスを制御します。
    - **Custom(カスタム)**：**Red(赤)** と**Blue(青)** のレベルを手動で設定します。

    Dominant Color Compensation(ドミナント カラー補正)（使用可能な場合）：このオプションは、視野内の広い領域に 1 つの色が含まれている場合に使用するべき代替の自動ホワイトバランスアルゴリズムを有効にします。たとえば、芝生を見下ろすカメラなどです。この例では、Dominant Color Compensation(ドミナント カラー補正)ホワイトバランスモードは、ホワイトバランスをよりニュートラルな色に改善します。
5. **Temporal Filter Strength (一時フィルターの強度)** スライダーを少し左または右に動かして、シーンのノイズとぼかしの量を調整します。時間的フィルタは、数フレームにわたってノイズを平均化することによって画像ノイズを低減します。

    > **ヒント：**大きな変更を加えると画質全体が劣化する恐れがあるため、小さな調整から始めてください。

    画像にノイズが見える場合は、スライダーを右に移動して、シーン内のノイズの量を削減し、使用する帯域幅を減少させます。

    画像がぼやけて見える場合は、スライダーを左に移動して、シーン内のぼやけを減らし、使用する帯域幅を増やします。

    デフォルトでは、スライダーは真ん中の 50 に設定されています。
6. [**Apply(適用)**] をクリックして、変更を保存します。

圧縮および画像レート

「Compression and Image Rate (圧縮率と画像レート)」ページでは、ネットワーク経由でビデオを送信するためのカメラの圧縮および画質設定を変更できます。

> **メモ：**ビデオ分析または異常動作検知を備えたカメラを物理的に移動またはを調整した場合、または、フォーカスやズーム レベルを変更した場合は、正確なデータを出力するために学習の進行状況をリセットしてください。カメラの画像レート、および圧縮またはディスプレイの設定が更新されると、学習の進行状況が自動的にリセットされる可能性があります。

アクセスを容易にし、使用帯域幅を減らすために、WebインターフェイスはJPEG形式のビデオのみを表示します。このページの設定は、ネットワークビデオ管理ソフトウェアに送信されるビデオにのみ影響します。

Avigilon高解像度 H.264 IP カメラはデュアルストリーム機能を備えています。カメラのストリーミング形式が H.264 に設定されているときでも、カメラの Web インターフェイスはライブビデオを JPEG 形式で表示できます。

重要：Avigilon H4 マルチセンサーおよび H5A デュアルヘッドカメラは、1 台のカメラに複数のカメラヘッドを備えています。一部の設定はカメラ全体に適用され、その他の設定は個々のヘッドに適用されます。特定のマルチヘッドカメラ設定は、All Heads(すべてのヘッド)タブ上ですべてのヘッドに対してグローバルに設定できますが。他の設定は、Head 1(ヘッド 1)～Head 4(ヘッド 4)タブを使用して、個々のヘッドごとに設定する必要があります。H4 マルチセンサーまたは H5A デュアルヘッドカメラを構成する場合、グローバルヘッド設定と個別ヘッド設定の両方が構成されていることを確認してください。

メモ：カメラは、指定された帯域幅の上限を守るために、圧縮品質を自動的に調整する場合があります。

1. ネットワーク ビデオ管理ソフトウェアでカメラ ビデオを表示するためのストリーミング形式を、[**Format(形式)**] ドロップダウン リストで選択します。

   Onboard Storage(オンボード ストレージ) 機能を使用している場合、[**H.264(H.264)**] または [**H.265**] を選択します。詳細については、「オンボードストレージの有効化」（36ページ）を参照してください。

   メモ：[**H.265**] 形式に設定されている H4 マルチセンサー カメラヘッドは、ACC ソフトウェアバージョン 6.12.2 以降でのみ動作します。H4 マルチセンサー カメラを ACC システムに接続するには、[**Format(形式)**] を [**H.264(H.264)**] に設定するか、または ACC ソフトウェアを v6.12.2 以降にアップグレードする必要があります。

2. [**Max Image Rate (最大画像レート)**] フィールドに、カメラがネットワーク経由でストリーミングする 1 秒あたりの画像数を入力します。

   メモ：30fpsの境界を越えて画像レートを調整すると、ビデオストリームが数秒間停止します。

   カメラが High Framerate(フレーム率 (高)) モードで動作している場合、最大画像レートが増加します。High Framerate(フレーム率 (高)) モードの詳細については、「「一般」（6ページ）」を参照してください。

3. **Max Quality (最高品質)** ドロップダウン リストで、希望の画像品質レベルを選択します。

ビデオの画質は 1 が最高で、このとき最大の帯域幅が必要です。

4. [**Max Bitrate(最大ビットレート)**] フィールドで、カメラが使用できる最大帯域幅を入力します。
5. ドロップ ダウン リストで、希望する画像解像度を選択します。**Resolution(解像度)**
6. [**Keyframe Interval(キーフレームの間隔)**] フィールドに、各キーフレーム間のフレーム数を入力します。
7. [**Apply(適用)**] をクリックして、変更を保存します。

HDSM SmartCodec™™ テクノロジー設定の有効化

HDSM SmartCodec™ テクノロジーはフォアグラウンドにある物体をバックグラウンドから分離し、バックグラウンドに適用する圧縮率を増加することによって帯域幅を減少します。このようにして、変化のないバックグラウンドの帯域幅を削減しながら、対象の被写体に対して最高の品質が維持されます。

有効にして、モーションイベントが検出されない場合、カメラは自動的にアイドルシーンモードの設定に切り替わります。モーション イベントは、カメラがシーン内のピクセル モーションを検出したときのことです。詳細については、「モーション検出」（30ページ）を参照してください。

カメラはピクセル変更モーションを使用してフォアグラウンド オブジェクトを検出するため、カメラの標準のモーション検出感度設定を使用します。

> **メモ：**さらに、高度な設定は、「HDSM SmartCodec™ 高度な設定 」ページでも更新できます。詳細については、「HDSM SmartCodec™ テクノロジーの高度な設定」（30ページ）を参照してください。

1. [**Enable(有効化)**] チェックボックスをオンにして、HDSM SmartCodec 機能を有効にします。
2. [**最小画像レート (Min Image Rate)**] フィールドに、カメラがネットワーク経由でストリーミングする 1 秒あたりの画像数を入力します。
3. **[アイドル キーフレーム間隔 (Idle Keyframe Interval)**] フィールドに、シーンに動きがない場合の各キーフレーム間のフレーム数 (1～254) を入力します。
4. **[Bandwidth Reduction]** フィールドで、以下のいずれかのオプションを選択します:
    - **低**
    - **中** (推奨)
    - **高**
    - **カスタム**
5. [**Apply(適用)**] をクリックして、変更を保存します。

RTSP ストリーム URI の表示

「Compression and Image Rate(圧縮および画像レート)」ページで、カメラの RTSP (リアルタイム ストリーミング プロトコル) アドレスを生成することもできます。RTSP ストリーム URI を使用すると、多くのビデオプレーヤーを含む RTSP ストリームの表示をサポートする任意のアプリケーションから、カメラのライブビデオストリームを見ることができます。

> **メモ：**RTSP ストリームアドレスは、カメラの Web インターフェイスでのみ生成できます。

1. [Generate RTSP Stream URI(RTSP ストリーム URI を生成する)] ボタンが使用できない場合、RTSP ストリーム URI は自動生成されます。

   RTSP Stream URI(RTSP ストリームの URI)領域では、自動生成された URI が表示されます：

   - **Unicast(ユニキャスト)** — 一度に 1 台のビデオ プレーヤーからのビデオ ストリームだけを見る場合、このオプションを選択します。
   - **Multicast(マルチキャスト)** — 同時に複数のビデオ プレーヤーからビデオ ストリームを見る場合、このオプションを選択します。

     RTSP ストリームを表示するには:

     a. 生成されたアドレスをコピーしてビデオ プレーヤーに貼り付けます。ライブ ビデオ ストリームを開きます。

     b. この形式のアドレスの先頭にユーザー名とパスワードを追加します。

        rtsp://<ユーザー名>:<パスワード>@<生成された RTSP ストリーム URI>/

        例: `rtsp://admin:admin@192.168.1.79/defaultPrimary?streamType=u`

     c. ライブ ビデオ ストリームを開きます。

2. 外部ビデオ プレーヤーからカメラのライブ ビデオ ストリームを見るには、[**Generate RTSP Stream URI(RTSP ストリーム URI を生成する)**] をクリックします。

   生成されたアドレスは、[RTSPStreamURI(RTSPストリームのURI)]領域の一番下に表示されます。

静止画 URI へのアクセス

「Compression and Image Rate(圧縮および画像レート)」ページで、カメラが最後に録画した静止画像フレームにアクセスできます。

- 静止画像にアクセスするには、[StillImageURI(静止画像のURI)]領域のURIリンクをクリックします。

カメラの二次ストリームから最後に記録されたビデオ フレームが表示されます。ブラウザから画像を直接保存または印刷することができます。

HDSM SmartCodec™ テクノロジーの高度な設定

「HDSM SmartCodec™ テクノロジーの高度な設定」 ページで、モーションシーンとアイドルシーンの両方の設定を選択できます。その他の HDSM SmartCodec™ テクノロジー設定は、「圧縮および画像レート」ページの HDSM SmartCodec™ テクノロジー設定で選択できます。詳細については、「HDSM SmartCodec™™ テクノロジー設定の有効化」（28ページ）を参照してください。

1. 左のメニューペインで **Compression and Image Rate(圧縮および画像レート) > Advanced** を選択します。
2. [**モーション時 (On Motion)**] の [**バックグラウンド品質 (Background Quality)**] フィールドで (デフォルトの 6 から最低設定値の 20 の間で) バックグラウンドの圧縮品質を入力します。
3. [**アイドル シーン (On Idle Scenes)**] セクションの [**モーション後遅延 (Post-motion delay)**] フィールドで、モーション終了からカメラがアイドル シーン設定になるまでの遅延 (5～60) を入力します。
4. [**アイドル シーン (On Idle Scenes)**] セクションの [**画像レート (Image Rate)**] フィールドに、シーンに動きがない場合のエンコード フレームレート (1 秒あたりのイメージ数) を入力します。
5. [**アイドルシーン**] セクションの [**画質**] フィールドに、圧縮品質を入力します (6 ～20)。
6. [**アイドルシーン**] セクションの [**最大ビットレート**] フィールドに、毎秒の最大キロバイト数を入力します。
7. [**アイドル シーン (On Idle Scenes)**] セクションの [**キーフレーム間隔 (keyframe Interval)**] フィールドに、シーンに動きがない場合の各キーフレーム間のフレーム数 (1～254 フレーム) を入力します。
8. [**Apply(適用)**] をクリックして、変更を保存します。

モーション検出

[Motion Detection (モーション検出)] ページでは、カメラの視野内の緑のモーション検出領域を定義できます。緑でハイライトされていない領域では、モーション検出は無視されます。

モーション感度としきい値を定義するのに役立つように、モーションはイメージパネルで赤でハイライトされます。

重要：Avigilon H4 マルチセンサーおよび H5A デュアルヘッドカメラは、1 台のカメラに複数のカメラヘッドを備えています。一部の設定はカメラ全体に適用され、その他の設定は個々のヘッドに適用されます。特定のマルチヘッドカメラ設定は、All Heads(すべてのヘッド)タブ上ですべてのヘッドに対してグローバルに設定できますが。他の設定は、Head 1(ヘッド 1)～Head 4 (ヘッド 4)タブを使用して、個々のヘッドごとに設定する必要があります。H4 マルチセンサーまたは H5A デュアルヘッドカメラを構成する場合、グローバルヘッド設定と個別ヘッド設定の両方が構成されていることを確認してください。

メモ：このモーション検出設定は、カメラの視野内のピクセル変化の検出を設定します。Avigilon ビデオ解析カメラを設定している場合は、詳細な解析モーション検出や他のビデオ解析機能を Avigilon コントロールセンター クライアント ソフトウェアを使用して設定する必要があります。詳細については、『*Avigilon*コントロールセンター *Client User Guide*（クライアント ユーザー ガイド）』を参照してください。

1. モーション検出領域を定義します。

   デフォルトでは、モーション検出のために視野全体がハイライトされます。モーション検出領域を定義するには、次のツールのいずれかを使用します。

   - ビデオ画像上のすべてのモーション検出エリアを削除するには、[**Clear All(すべてクリア)**] をクリックします。
   - ビデオ画像全体にモーション検出エリアを設定するには、[**Set All(すべてを設定)**] をクリックします。
   - 特定のモーション検出エリアを設定するには、[**Select Area(領域を選択)**] をクリックしてから、ビデオ画像の任意の場所をクリックしてドラッグします。
   - 特定のモーション検出エリアをクリアするには、[**Clear Area(領域のクリア)**] をクリックしてから、モーション検出エリア上でクリックしてドラッグします。
   - [**Zoom In(ズームイン)**] ボタンと [**Zoom Out(ズームアウト)**] ボタンを使用して、ビデオ画像の特定のエリアを見つけます。

2. [**Sensitivity(感度)**] フィールドにパーセント数を入力して、モーションと見なされる前に各ピクセルがどれだけ変化する必要があるかを調整します。

   感度が高くなればなるほど、動きを検出するために必要なピクセル変化量が小さくなります。

3. [**Threshold(しきい値)**] フィールドにパーセント数を入力して、画像がモーションと見なされる前にピクセルがいくつ変化する必要があるかを調整します。

   閾値が高いほど、画像が動いたとみなされるためにはより多くのピクセルが変化しなければなりません。

4. カメラがサードパーティ製のビデオ管理システム (VMS) に接続されている場合は、[**Enable Onvif MotionAlarm Event(Onvif MotionAlarm イベントの有効化)**] チェックボックスをクリックします。

   有効になると、H.264 カメラは、適切な ONVIF プロトコルに従ってモーションアラーム情報を VMS に送信できます。

5. [**Apply(適用)**] をクリックして、変更を保存します。

改ざんの検出

[Tamper Detection (改ざんの検出)] ページで、カメラの改ざんに対する感度を設定できます。

重要：Avigilon H4 マルチセンサーおよび H5A デュアルヘッドカメラは、1 台のカメラに複数のカメラヘッドを備えています。一部の設定はカメラ全体に適用され、その他の設定は個々のヘッドに適用されます。特定のマルチヘッドカメラ設定は、All Heads(すべてのヘッド)タブ上ですべてのヘッドに対してグローバルに設定できますが。他の設定は、Head 1(ヘッド 1)～Head 4 (ヘッド 4)タブを使用して、個々のヘッドごとに設定する必要があります。H4 マルチセンサーまたは H5A デュアルヘッドカメラを構成する場合、グローバルヘッド設定と個別ヘッド設定の両方が構成されていることを確認してください。

改ざんのオプション設定方法

1. [**Sensitivity(感度)**]フィールドで、1～10の数値を入力して、シーン内の突然の変化に対するカメラの感度を定義します。設定値が高いほどカメラはシーン内の変化を検出する感度が高くなります。

   メモ：シーンが突然変化した場合、通常は誰かが不意にカメラを動かしたことが原因です。影の移動など、シーン内の小さい変化が改ざんイベントを多数発生させる場合は設定を低くします。カメラが屋内に取り付けられていて、シーンの変化が少ない場合は、この設定を上げて異常性の高いイベントをキャプチャするようにできます。

2. [**Trigger Delay (トリガー遅延)**] フィールドに、改ざんイベントが送信される前に、改ざん条件がシーン内で保持される必要がある秒数 (最大 30 秒) を入力します。

Tamper Detection Switch (改ざん検出スイッチ)

改ざん検出スイッチを備えたカメラは、デバイスが取り外されようとした際に検出されます。改ざん検出スイッチがアクティブになると、イベント通知が ACC システムに転送され、オペレータに警告するためのアラームをトリガすることができます。

さらに、Video Intercom カメラがオプションのセーフティリレー (H4VI-AC-RELY1) に接続されている場合、イベントが発生した際にセーフティリレーをロックアウト状態にするようトリガーします。この状態では、セーフティリレーはロックアウトモードを維持し、ドアをしっかりとロックしたままにし、安全な側からの出入りのみが許可されます。ロックアウト後、セーフティ リレーのクリア ボタンを押して通常の動作に戻す必要があります。セーフティ リレーの詳細については、『セーフティ リレー設置ガイド』を参照してください。

ACC システムが Avigilon Access Control Manager (ACM) ソフトウェアと統合されている場合、イベントはACM™ ソフトウェアに転送され、その構成に従って処理されます。

Tamper Detection Switch (改ざん検出スイッチ) サブセクションでは、改ざんスイッチのステータスを表示し、セーフティリレーの動作を設定できます。

1. Status (ステータス) フィールドには、改ざん検出スイッチの状態が表示されます。
    - **改ざんなし (No Tamper)**: 改ざん検出スイッチは通常の動作状態です。
    - **改ざん検出 (Tamper Detected)**: 改ざん検出スイッチがアクティブ化されました (または、カメラが正しく取り付けられていません)。カメラがセーフティリレーに接続されている場合は、ロックアウトモードが有効になり、ドアをしっかりとロックし、安全な側からの出入りのみが許可されます。
    - **無効 (Disabled)**: カメラの改ざん検出が有効になっていません。
2. 改ざん検出スイッチが有効の状態で、カメラが通知を送信するように設定したい場合は、**Enable Tamper Detection Switch (改ざん検出スイッチを有効にする)** を確認します。このオプションは、デフォルトで有効になっています。
    - カメラに接続されているセーフティ リレーによって通知を受信したら、ドアをしっかりとロックした状態でロックアウト モードがアクティブになり、安全な側からの出入りのみが許可されます。
    - ACM システムと統合された ACC システムによって受信された通知は、その設定に従って処理するために ACM システムに転送されます。
3. 改ざん検出スイッチが有効になった時のように、カメラのビューへの突然の変化を ACC システムで処理するよう設定したい場合は、**Trigger Tamper Detection Switch On Video Tamper (ビデオ改ざんに対する改ざん検出スイッチをオンにする)** を確認します。このオプションはデフォルトで無効になっています。
4. [**Apply(適用)**] をクリックして、変更を保存します。

注意 ― セーフティ リレーがロックアウト状態になった後、セーフティ リレーのクリア ボタンを手動で押して通常の動作に戻す必要があります。ビデオの改ざんは、物理的な改ざんよりも誤ったイベントを起こしやすいため、このオプションはデフォルトで無効になっています。

解析

「解析」ページで、カメラによるサードパーティ VMS システムに接続されたカメラの ONVIF 準拠の解析メタデータの送信を有効にすることができます。このオプションはデフォルトで無効になっています。

⚠ **注意 ー** このオプションは、カメラから VMS システムに解析メタデータを送信する必要があるサードパーティ VMS システムにカメラを接続する場合にのみ有効にしてください。

カメラが ACC システムに接続されている場合、解析データは異なる形式で送信されるため、このオプションを有効にするとカメラのビデオ品質が低下する場合があります。

ACC システムにカメラを接続している場合は、このオプションを有効にしないでください。

1. [**ONVIF 準拠の解析メタデータを有効にする**] チェックボックスをオンにして、カメラによる ONVIF 準拠のメタデータのサードパーティ VMS システムへの送信を有効にします。
2. [**Apply(適用)**] をクリックして、変更を保存します。

プライバシー ゾーン

「Privacy Zones(プライバシー ゾーン)」ページでは、カメラの視野にプライバシー ゾーンを設定して、表示または記録したくない領域をブロックできます。カメラは、最大 64 の プライバシーゾーンをサポートします。

重要：Avigilon H4 マルチセンサーおよび H5A デュアルヘッドカメラは、1 台のカメラに複数のカメラヘッドを備えています。一部の設定はカメラ全体に適用され、その他の設定は個々のヘッドに適用されます。特定のマルチヘッドカメラ設定は、All Heads(すべてのヘッド)タブ上ですべてのヘッドに対してグローバルに設定できますが。他の設定は、Head 1(ヘッド 1)～Head 4(ヘッド 4)タブを使用して、個々のヘッドごとに設定する必要があります。H4 マルチセンサーまたは H5A デュアルヘッドカメラを構成する場合、グローバルヘッド設定と個別ヘッド設定の両方が構成されていることを確認してください。

プライバシー ゾーンの設定

1. プライバシー ゾーンを追加するには、[**Add(追加)**] をクリックします。プライバシーゾーンボックスがビデオ画像に追加されます。
2. プライバシー ゾーン領域を定義するには、次のいずれかを実行します。
    a. プライバシー ゾーンのサイズを変更するには、ボックスの任意の辺をドラッグします。プライバシーゾーンには、長方形だけが使えます。
    b. ボックス内をクリックし、プライバシー ゾーンをドラッグして移動します。
3. [**Apply(適用)**] をクリックして、プライバシー ゾーンの設定を保存します。

プライバシー ゾーンの削除

グレー ボックスの右上隅の [**X(X)**] をクリックして、プライバシー ゾーンを削除します。

ストレージ

「Storage(ストレージ)」ページで、カメラのオンボード ストレージ機能を有効にし、カメラから録画したビデオを直接ダウンロードできます。オンボード ストレージは、SD カードまたは microSD カード スロットを備えたカメラでのみ使用できます。

重要：SD カードに障害が発生すると、カメラが連続して再起動することがあります。この障害が発生しないように、永続的な障害が検出されると、SD カードは無効になります。詳細については、「SD カードの障害」（39ページ）を参照してください。

FIPS レベル 3 暗号化用にカメラの SD スロットで CryptR マイクロカードを使用している場合、SD カードスロットでオンボードストレージを使用することはできません。2 つの microSD スロットを備えたカメラの場合、スロットはストレージまたは CryptR マイクロカードのいずれかにのみ使用できます。両方のオプションを同時に使用することはできません。

メモ：microSD カードスロットが 2 つあるカメラの場合、どちらのカードスロットかにかかわらず最初に挿入された microSD カードのみを構成できます。2 番目の microSD カードスロットは、将来の機能のために予約されています。

オンボードストレージの有効化

カメラのオンボード ストレージ機能を使用するためには、まずカメラに SD カードを挿入する必要があります。SD カードスロットの位置については、カメラのインストールマニュアルを参照してください。

ヒント：SD カードは、カメラの最高解像度のタイル化されていないストリームから録画します。ほとんどの場合、これはプライマリストリームになります。

メモ：microSD カードスロットが 2 つあるカメラの場合、どちらのカードスロットかにかかわらず最初に挿入された microSD カードのみを構成できます。2 番目の microSD カードスロットは、将来の機能のために予約されています。

1. 「Storage(ストレージ)」ページで、[**Enable Onboard Storage(オンボード ストレージの有効化)**] チェックボックスをオンにします。
2. デフォルトでは、カメラはネットワークビデオ管理サーバーと通信できないときに SD カードに記録するように設定されています。カメラでビデオをネットワーク ビデオ管理サーバーと SD カードの両方に記録する場合は、[**Record only when server connection is interrupted(サーバー接続が中断された場合にのみ録画)**] チェックボックスをオフにして設定を無効にします。
3. 次の録画モードの 1 つを選択します。
   - **Continuous(連続):** カメラは、SD カードへの記録を停止することはありません。
   - **On Motion(モーション検出時):** カメラはシーンに動きがある場合のみ記録します。

     Avigilon ビデオ解析カメラを設定している場合、On Motion(モーション検出時) 設定はカメラが Avigilon コントロールセンター クライアント ソフトウェアで設定されている方法に応じて、シーンまたは解析モーション イベントのいずれかでピクセルの変化を記録します。

   記録映像には、長さが 5 分以下またはサイズが 100 メガバイトまでのファイルに分割されます。
4. Compression and Image Rate(圧縮および画像レート) ページで、SD カードの記録容量とパフォーマンスを最大化するために、形式が [**H.264(H.264)**] または [**H.265**] に設定されていることを確認してください。

ONVIF プロファイル G

ONVIF プロファイル G を使用すると、ネットワークの停止や同様のイベントにより VMS ビデオに差異がある場合、ビデオ管理システムがカメラのオンボード ストレージからビデオを取得できます。

- ファームウェアバージョン 4.4.0.X 以降のカメラでは、ONVIF プロファイル G がすでに有効になっています。
- 4.4.0.X より古いファームウェアを搭載したカメラの場合、ファームウェアをアップグレードする際**ONVIF プロファイル G を有効にする** オプションが表示されます。

  メモ：ONVIF プロファイル G を有効にするには、SD カードを再フォーマットする必要があります。SD カードに現在記録されているすべての記録映像が失われます。プロファイル G を有効にする前に、必要なビデオクリップをダウンロードしてください。

ONVIF は Onvif, Inc. の商標です。

Web インターフェイスから録画ビデオをダウンロードする

[Recordings(録画)]セクションに一覧表示されているのは、SDカードに記録されたすべてのビデオです。

FIPS レベル 3 暗号化用にカメラの SD スロットで CryptR マイクロカードを使用している場合、SD カードスロットでオンボードストレージを使用することはできません。2 つの microSD スロットを備えたカメラの場合、スロットはストレージまたは CryptR マイクロカードのいずれかにのみ使用できます。両方のオプションを同時に使用することはできません。

Web インターフェイスから録画ビデオをダウンロードすることをお勧めします。ただし、帯域幅が限られている場合は、SD カードから直接録画ビデオをダウンロードすることもできます。詳細については、「SD カードから録画したビデオをダウンロードする」（38ページ）を参照してください。

録画したビデオを Web インターフェイスからダウンロードするには、次の手順に従います：

1. 「Storage(ストレージ)」ページで、ダウンロードするすべてのビデオの横にあるチェックボックスをオンにします。

   目的のビデオを見つけるために、日付と時間でビデオを絞り込むことができます。[**Filter(フィルター)**] チェックボックスをオンにして、時間範囲を選択します。
2. [**Download(ダウンロード)**] をクリックします。

選択したビデオファイルは、ブラウザのデフォルトのダウンロードフォルダに自動的にダウンロードされます。ブラウザでプロンプトによって確認を要求された場合は、ダウンロードを許可します。

メモ：ダウンロードが完了するまでブラウザのウィンドウを閉じないでください。そうでないと、ファイルが正しくダウンロードされないことがあります。ファイルが 1 つずつダウンロードされるため、複数のビデオファイルをダウンロードする場合は、これが重要です。

SD カードから録画したビデオをダウンロードする

Web インターフェイスから録画ビデオを直接ダウンロードするのに十分な帯域幅がない場合は、SD カードから直接録画ビデオをダウンロードすることができます。

録画したビデオを SD カードから直接ダウンロードするには、次の手順に従います：

1. [Settings(設定)]エリアで、[**EnableOnboardStorage(オンボードストレージの有効化)**]チェックボックスをオフにしてオンボードストレージを無効にし、[**Apply(適用)**]をクリックします。
2. SD カードをカメラから取り外します。
3. SD カードをカードリーダーに挿入します。
4. Windowsの自動再生ダイアログボックスが表示されたら、[**Openfoldertoviewfiles**]を選択します。
5. Avigilon Camera Footage(カメラ映像) アプリケーションを開きます。

   [Avigilon Camera Footage(カメラ映像)] ウィンドウには、SD カードに保存されているすべてのビデオ ファイルが一覧表示されます。

   - 記録映像をすべてダウンロードするには、[**Download All(すべてをダウンロード)**] をクリックします。
   - 特定のビデオをダウンロードするには、目的の動画ファイルを選択し、**Download Selected(選択したものをダウンロード)** をクリックします。
6. プロンプトが表示されたら、ビデオファイルを保存する場所を選択します。

   ファイルは SD カードからダウンロードされ、選択した場所に保存されます。
7. 準備ができたら、SD カードを取り出します。
8. SD カードをカメラに挿入し、[Enable Onboard Storage(オンボード ストレージの有効化)] を選択して、SD カードへの記録を再開します。

録画したビデオを削除する

SD カードがいっぱいになると、カメラは自動的に最も古い録画ビデオを上書きし始めます。ビデオを手動で削除して、新しい録画のためのスペースを確保することもできます。

「Storage(ストレージ)」ページで、次の方法でビデオを削除することを選択できます。

- 個々のビデオ ファイルを削除するには、[Recordings(録画)] リストで削除したいファイルをすべて選択してから [**Delete(削除)**] をクリックします。
- 録画されたすべてのビデオ ファイルを削除するには、[**Format Card(カードのフォーマット)**] をクリックして SD カードを初期化します。

SD カードの障害

SD カードに障害が発生すると、カメラが連続して再起動して、カメラの信頼性を損なうことがあります。この障害が発生しないように、永続的な障害が検出されると、SD カードは無効になります。

SD カードが無効になると、カメラと Web インターフェースが問題を通知します。

- カメラのビデオは、ビデオ画像の警告テキストをオーバーレイします: `SD` **カードの記録が無効化されました。再度有効化するにはカードを交換してください。**

  > **メモ：**[**重大な SD カード障害時のビデオ アラート オーバーレイの有効化**] チェックボックスをオフにすると、カメラの [**Storage(ストレージ)**] ページでビデオオーバーレイメッセージを無効にできます。

- カメラの Storage(ストレージ) ページを選択すると、このページで警告メッセージが表示されます: **カード エラーのために** `SD` **カード スロットが無効化されました。カードを交換してください。**

SD カードを再度有効にするには、カメラの SD カードスロットから SD カードを取り外し、正常に機能する SD カードと交換します。新しいカードを挿入すると、スピードテストが実行され、問題なく機能するかどうかが確認されます。

また、[**Storage(ストレージ)**] ページの [**再度有効化された SD カード スロットの適用**] をクリックすると、Web インターフェースで SD カードを強制的に再有効化することができます。

> **重要：**SD カードに問題がないことが確認できない限り、強制的に SD カードを再有効化することはお勧めできません。カードの障害が続く場合、カメラが再起動ループに入ることがあり、障害が続くと SD カードが再び無効になります。

デジタル入出力

「Digital Inputs and Outputs(デジタル入出力)」ページで、カメラに接続されている外付けの入出力デバイスを設定できます。このオプションは、デジタル入出力をサポートしないカメラには表示されません。

1. デジタル入力を設定するには:
    a. [Digital Inputs(デジタル入力)] エリアの [**Name(名前)**] フィールドでデジタル入力の名前を入力します。
    b. [**Circuit State(回路状態)**] ドロップダウンリストから適切な状態を選択します。オプションは次のとおりです。
        - **開 (通常)**
        - **閉 (通常)**
    c. [**Apply(適用)**] をクリックして、変更を保存します。

        デジタル入力がカメラに接続されると、[**CircuitCurrentState(回路の現在の状態)**]エリアに接続状態が表示されます。この状態は、通常、[*Open(*開*)*]または[*Closed(*閉じる*)*]です。
2. デジタル出力を設定するには:
    a. [Digital Outputs(デジタル出力)] エリアの [**Name(名前)**] フィールドでデジタル出力の名前を入力します。
    b. [**Circuit State(回路状態)**] ドロップダウンリストから適切な状態を選択します。
    c. 外部出力を制御するために、カメラの IR カット フィルターを許可するには、[**IRCF (出力)**] チェックボックスをオンにします。

        この機能は、通常、カメラが外部の IR イルミネータに接続されている場合に使用されます。有効にすると、カメラの IR カットフィルタがモノクロモードになっているときに IR 照明がオンになります。
    d. [**Duration(期間)**] フィールドで、デジタル出力がトリガーされたときにアクティブ状態で保持する時間を入力します。100～86,400,000ミリ秒の間の任意の数値を入力できます。
    e. [**Trigger(トリガー)**] をクリックして、手動で Web インターフェイスからのデジタル出力をトリガーします。
    f. [**Apply(適用)**] をクリックして、変更を保存します。

マイク

マイクがカメラでサポートされていてカメラに接続されている場合は、「Microphone(マイク)」ページで利得を調整できます。ゲイン設定が高いほど、マイクの音量が上がります。

- 右側に表示される範囲の値を入力して、[**Apply(適用)**] をクリックします。

Avigilon フィッシュアイ カメラを設定する場合、2 つのフィールドを使用できます。

1. **InternalMicrophoneGain(内蔵マイクのゲイン)**ーカメラに内蔵されたマイクの利得を設定します。
2. **External Source Gain(外部ソースのゲイン)** ー 音声入力に接続されている任意のマイクの利得を設定します。
3. いずれかのフィールドで、右側に表示される範囲の値を入力して、[**Apply(適用)**]をクリックします。

スピーカー

カメラでスピーカーがサポートされていてカメラに接続されている場合は、「Speakers(スピーカー)」ページで音量を調整できます。

- 0 から 100 までの数値を入力してスピーカーの音量を設定し、[**Apply(適用)**] をクリックします。

インターコム

「Intercom(インターコム)」ページの設定を使用して、ビデオ インターコムの SIP 接続を設定します。ビデオ インターコムは、SIP または VMS で動作するようにを構成できます。SIP を使用している場合は、次のように構成できます。

- **SIP ピアツーピア通話**。特定の SIP 電話に直接 SIP コールを発信するようにビデオ インターコムを設定するために使用されます。詳細については、「SIP ピアツーピア構成」（42ページ）を参照してください。
- **SIP/PBX サーバーの呼び出し**。PBX サーバーにビデオインターコムを拡張機能の 1 つとして登録し、PBX サーバーを SIP 電話に電話をかけるためのプロキシとして使用するために使用されます。詳細については、「SIP サーバーの構成」（43ページ）を参照してください。

ビデオ インターコムを ACCシステムと併用した場合、[**VMS(VMS)**] を [**Intercom Call Destination (インターコムの通話先)**] に選択し、「Audio (オーディオ)」ページと ACC Client でビデオ インターコムを設定します。詳細については、「音声」（48ページ）と、*ACC Client* ユーザー ガイドを参照してください。「Audio (オーディオ)」ページのコーデック、音量、マイクの設定は SIP 構成にも影響します。

重要：通話中にSIP構成設定が変更された場合、変更が適用されるとその通話はドロップされます。

SIP ピアツーピア構成

SIP ピアツーピア通話構成は、セキュリティデスクの電話など、常に同じ SIP 電話でビデオ インターコムからの通話に応答したい場所向けの簡単なセットアップです。

1. [**SIP(SIP)**] を [**Intercom Call Destination(インターコムの通話先)**] に選択します。
2. 以下の SIP Peer To Peer Call Settings(SIP ピア ツー ピア通話の設定) を構成します：
    - **Display Name(表示名)**：SIP 電話を呼び出すときに表示されるビデオ インターコムの名前を入力します。このフィールドはオプションであり、空のままにすることができます。
    - **SIP Call Destination(SIPの通話先)**：ビデオインターコムがダイヤルするSIP電話のドメインアドレスを入力します。これは、有効なIPv4、IPv6、またはDNS名である必要があります。
    - **SIP Call Destination Port(SIP の通話先ポート)**：ビデオ インターコムがダイヤルする SIP 電話の UDP ポート番号を入力します。これは、1～65534 の有効なポート番号である必要があります。デフォルトのポートは 5060 です。

> **メモ：**ポート1～1024は予約済みのIPポートです。SIPポートは、この予約済み範囲外であり、またACCシステムによって使用されるポートと重複してはいけません。

- **Allow Incoming SIP Calls(SIP 通話の着信を許可)**：このオプションを有効にすると、ビデオインターコムの SIP 通話自動応答がオンになります。このオプションを有効にすると、訪問者が通話ボタンを押さなくても、すべての SIP 電話がビデオ インターコムの IP アドレスまたはドメインアドレスに電話をかけて、ビデオインターコムを介して会話できます。

3. [**Apply(適用)**] をクリックして、変更を保存します。

SIP 電話のユーザーが電話を受ける際、電話に出て訪問者に話しかけるか、電話に出る前に別の SIP 電話に通話をリダイレクトできます。通話に応答すると、通話はリダイレクトできなくなります。訪問者の入室が承認された場合、ユーザーは DTMF コードを使用してドアへのアクセスを許可できます。詳細については、「DTMF コードの設定」（45ページ）を参照してください。

SIP サーバーの構成

SIP サーバー構成により、ビデオ インターコム SIP 通話設定をより柔軟に行うことができます。SIP サーバーは PBX サーバーとも呼ばれます。PBX サーバーを使用して、メイン SIP 番号が混雑している場合のコールリダイレクト、および PBX サーバーへの接続から利用できるその他のオプションを設定できます。通常ビデオ インターコム通話に応答するオペレーターが不在の場合は、内線番号を簡単に変更して、PBX ドメイン内の別の電話にかけることができます。

> **メモ：**ビデオ インターコムを PBX サーバーで使用するには、サーバー管理者がビデオ インターコムデバイスを PBX サーバーに追加して登録する必要があります。SIP Server Settings(SIP サーバー設定) を構成する際には、ユーザー名、認証 ID、および PBX サーバーからのその他の情報が必要となります。

PBX (SIP) サーバーには通常、プロキシ、レジストラ、およびリダイレクト機能が含まれています。プロキシはコールをルーティングし、着信コールに追加のロジックを提供します。レジストラは SIP デバイス登録要求を受け入れ、SIP ドメインの位置情報サービスとして機能します。リダイレクトサーバーは、代替 SIP アドレスに接続するようにクライアントをリダイレクトします。

1. [**SIP(SIP)**] を [**Intercom Call Destination(インターコムの通話先)**] に選択します。
2. [**PBX mode(PBX モード)**] チェックボックスを選択します。
3. 以下の SIP Peer To Peer Call Settings(SIP ピア ツー ピア通話の設定) を構成します：
    - **Display Name(表示名)**：SIP 電話を呼び出すときに表示されるビデオ インターコムの名前を入力します。このフィールドはオプションであり、空のままにすることができます。
    - **Allow Incoming SIP Calls(SIP 通話の着信を許可)**：このオプションを有効にすると、ビデオインターコムの SIP 通話自動応答がオンになります。このオプションを有効にすると、訪問者が通話ボタンを押さなくても、PBX サーバー経由で SIP 電話内線がビデオ インターコムの内線に電話をかけて、ビデオ インターコムを介して会話できます。
4. 以下の SIP Server Settings(SIP サーバー設定) を構成します：
    - **SIP Server(SIP サーバー)**：レジストラ、プロキシ、リダイレクトサーバーとして使用される SIP サーバーのドメインアドレスを入力します。これは、有効な IPv4、IPv6、または DNS 名である必要があります。
    - **SIP Server Port(SIP サーバー ポート)**：SIP サーバーとの通信に使用される UDP ポート番号を入力します。これは、1～65534 の有効なポート番号である必要があります。デフォルトのポートは 5060 です。

      > **メモ：**ポート1～1024は予約済みのIPポートです。SIPポートは、この予約済み範囲外であり、またACCシステムによって使用されるポートと重複してはいけません。

    - **SIP Username(SIP ユーザー名)**：PBX サーバーでビデオ インターコム用に設定されているユーザー名を入力します。このフィールドを空のままにすることはできません。
    - **Authentication ID(認証 ID)**：ビデオインターコムを認証するために PBX レジストラが使用するユーザー名/ID を入力します。このフィールドを空のままにすることはできません。
    - **Password(パスワード)**：ビデオ インターコムの認証に使用するパスワードを入力します。このフィールドはオプションであり、空のままにすることができます。
    - **Domain(ドメイン)**：ビデオ インターコムが登録するドメイン名を入力します。通常これは SIP サーバーと同じですが、SIP サーバーが複数のドメインを処理する場合は、これを確認する必要があります。これは、有効な IPv4、IPv6、または DNS 名である必要があります。
    - **Registration Duration(登録時間)**：SIP サーバーに再登録する前にビデオ インターコムが待機する時間を秒単位で入力します。これは 0 より大きい値である必要があります。

> **ヒント：**[RegistrationStatus(登録ステータス)]フィールドには、ビデオインターコムの現在の登録ステータスが表示されます。ビデオインターコムがSIPサーバーに正常に登録されていない場合、ステータスには登録に失敗した理由が表示されます。

- **PBX Call Destination(PBX の通話先)**：訪問者が電話をかけるときにビデオ インターコムが使用する内線番号を入力します。このフィールドを空のままにすることはできません。

5. [**Apply(適用)**] をクリックして、変更を保存します。

SIP 電話のユーザーが電話を受ける際、電話に出て訪問者に話しかけることができます。訪問者の入室が承認された場合、ユーザーは DTMF コードを使用してドアへのアクセスを許可できます。詳細については、「DTMF コードの設定」（45ページ）を参照してください。

SIP ネットワーク設定

[**SIP Port(SIP ポート)**] と [**RTP Base Port(RTP ベース ポート)**] の値を変更したり、デフォルト値を使用したりすることができます。これは両方とも、1～65534 の有効なポート番号である必要があります。[SIP Port(SIP ポート)] と [RTP Base Port(RTP ベース ポート)] を同じポートにすることはできません。また、ビデオ インターコムに割り当てられている他のカメラポートと同じにすることはできません。

RTPBasePort(RTPベースポート)は、2ポート範囲の最初のポートなので、入力「RTPBasePort(RTPベースポート)」と「RTPBasePort(RTPベースポート)」+1が使用されていないことを確認してください。

DTMF でサポートされている標準

[SIP info(SIP 情報)] および/または [RTC 2833(RTC 2833)] のチェックボックスを選択して、DTMF コードがこれらの標準の一方または両方でサポートされるようにします。デフォルトでは、両方の標準が選択されています。

DTMF コードの設定

SIP 構成でビデオ インターコムを使用するには、DTMF Codes(DTMF コード)ページを使用して、ビデオインターコムを介したドアアクセスを許可するデュアルトーン多重周波数信号をセットアップする必要があります。DTMF は、電話ボタンからのトーンを使用して、アクセスを許可するためにビデオインターコムに信号を送信します。

ヒント：DTMFコードは、アクセスを許可するためにビデオインターコムの出力#1をトリガーします。デジタル出力の設定については、*H4VI*ビデオインターコム設置ガイドを参照してください。

複数のオペレーターが存在し、どのオペレーターにアクセスを許可するかを監査する必要がある場合は、複数のDTMFコードを追加できます。ビデオインターコムDeviceLog(デバイスログ)には、使用されたDTMFコードの記録が含まれます。詳細については、「デバイスログ」（52ページ）を参照してください。

DTMF コードの追加

メモ：複数の DTMF コードがある場合、2 つの DTMF シーケンスがシーケンスの同様のサブストリングを共有することは許可されていないことに注意してください。
たとえば、1 人のユーザーの DTMF シーケンスが*123* の場合、2 番目のユーザーは *123* を含む DTMF シーケンスを使用するように設定できません。この例では、*12345* または *21234* のようなシーケンスは無効と見なされます。

1. DTMF Codes(DTMF コード)ページで、[**Add(追加)**] をクリックします。
2. [DTMF の追加] ページで、追加する DTMF コードの **Name(名前)** を入力します。
3. DTMF **Sequence(シーケンス)** を入力します。これは、オペレーターがドアアクセスを許可するために SIP 電話に入力する番号シーケンスです。

   ヒント：DTMF シーケンスには、数字 `0` ~ `9`、`#`、または`*` を使用できます。DTMF シーケンスは 3 桁以上必要です。
4. Trigger(トリガー)フィールドで、DTMF コードがアクティブにする出力を選択します。**Output 1 (アウトプット 1)**、**Output 2(アウトプット 2)**、 または両方を選択できます。選択した出力は、インターコムコール中に DTMF コードが入力されると、ビデオインターコムでトリガーされます。
5. [**Apply(適用)**] をクリックして、DTMF コードを保存します。

新しい DTMF の名前とシーケンスは、DTMF Codes(DTMF コード)ページに表示されます。

DTMF コードの変更

DTMF コードの名前またはシーケンスを変更するには、DTMF コードを選択して [**Modify(変更)**] をクリックします。変更を加え、**Apply(適用)** をクリックして、保存します。

DTMF コードの削除

1つ以上のDTMFコードを削除するには、リストからそれらを選択して、[**Delete(削除)**]をクリックします。

SIP ビデオ設定

電話と PBX サーバーがビデオをサポートしている場合、SIP ビデオはデフォルト設定で SIP 通話に自動的に含まれます。SIP Video Settings(SIP ビデオ設定)ページを使って、SIP 通話中に表示されるビデオの設定を構成します。

> **メモ：**SIP ビデオ通話では、SIP 音声通話設定も構成しておく必要があります。詳細については、「インターコム」（42ページ）を参照してください。

SIP ビデオストリームは、H.264(H.264)Format(形式)でのみサポートされます。

1. **Max Image Rate (最大画像レート)**フィールドに、カメラが SIP 通話経由でストリーミングする 1 秒あたりの画像数を入力します。
2. **Max Quality (最高品質)** ドロップダウン リストで、希望の画像品質レベルを選択します。

   ビデオの画質は 1 が最高で、このとき最大の帯域幅が必要です。
3. **MaxBitrate(最大ビットレート)**フィールドで、SIPビデオが使用できる最大帯域幅を入力します。
4. ドロップ ダウン リストで、希望する画像解像度を選択します。**SIP Video Resolution(SIP ビデオ解像度)**

   > **メモ：**SIP ビデオ通話の解像度は、1920x1080 より高く設定することはできません。選択できる唯一の解像度は、1920x1080 以下になります。プライマリストリームの解像度が SIP Video Resolution(SIP ビデオ解像度) 設定より低い解像度に低下した場合、SIP 解像度も自動的に低下します。
5. **Min Keyframe Interval(Keyframe 間隔の最小値)**フィールドに、各キーフレーム間の最小フレーム数を入力します。
6. ビデオ画像で、SIP 通話中に表示するビデオ画像の領域をカバーするようにSIP video zone(SIP ビデオ ゾーン)をクリックアンドドラッグします。

   SIP Video Resolution(SIP ビデオ解像度)設定を変更すると、SIP video zone(SIP ビデオ ゾーン)のサイズと形状が変更されます。
7. **Apply(適用)**をクリックして、SIP ビデオ設定を保存します。

音声

ビデオ インターコムの音声品質は、Audio (オーディオ) ページの設定で調整できます。

オーディオ ストリームをエンコードするには、高品質のサウンドを生成する Opus サウンド エンコーダー、または G.711 プロトコル サウンド エンコーダーから選択できます。ACC ソフトウェア リリース 6.10 以降 (または Opus プロトコルをサポートするサードパーティ製のビデオ管理システム) を使用している場合、Opus エンコーダーを使用します。それ以外の場合は、幅広くサポートされている G.711 プロトコルを使用します。

エコーキャンセルとノイズ低減は、ビデオインターコムに組み込まれています。エコーキャンセルは、マイク信号からスピーカー出力信号を除去し、相手側のオペレータに自分の声のエコーが聞こえてしまうのを防ぎます。ノイズ低減は、マイク信号からのバックグラウンドノイズを除去し、バックグラウンドノイズに対する感度を設定することができます。スピーカー音量とマイクの出力レベルを設定することもできます。

1. Audio Settings (オーディオ設定) セクションで:
    a. [**Encoding (エンコーディング)**] フィールドで、使用する音声エンコーダーを指定します。
        - **Opus**: 高品質の音声コーデック (デフォルト)。
        - **G.711**: さまざまなプラットフォームで対応。
    b. [**Echo Cancellation & Processing (エコー キャンセル & 処理)**] チェックボックスをオフにすると、エコー キャンセル、ノイズ低減、自動利得制御など、すべてのオーディオ処理が無効になります。これはデフォルトで有効になっています。
    c. [**Noise Reduction (ノイズ リダクション)**] フィールドで、バックグラウンド ノイズを低減するために適用するノイズ低減強度を指定します。

        7 のデフォルト レベルは中程度にノイズの多い環境に適し、1～3 の範囲の値は少ないバックグラウンド ノイズと静かな室内環境に適しています。

        ノイズの多い環境では、奇妙な音のバックグラウンド ノイズは、通常 **Noise Reduction (ノイズ リダクション)** 設定が低すぎることを示しています。この場合は、設定値を上げます。デフォルトよりも高い設定の場合、音声品質に影響する場合があります。

        オフに設定すると、ノイズ低減が完全に無効になります。
2. 「Device Speaker (デバイス スピーカー)」セクションでは、**Volume (ボリューム)** スライダーを使ってスピーカーの音量を調整します (0～100)。

3. Device Microphone (デバイス マイク) セクションで:
    a. **Output Level (出力レベル)** スライダーを使用してマイクの出力を調整します。デフォルトのレベルは 0 dB で、出力レベルを最大 40 dB 下げることができます。この音量レベルは、自動利得制御およびその他処理の後に適用されます。ビデオ インターコムから他のデバイスの音量に合わせて、出力レベルを下げます。
    b. マイク出力レベルをできるだけ一定に保つためには、**Auto Gain Control (自動ゲイン調整)** をオンにします。人が静かに話している際にはマイク信号が増加し、大きな声でマイクに向かって話している際には減少します。これで、オペレータの対する音量レベルが一定に保たれます。

        MicrophoneMuting(マイクのミュート)クライアントにマイACCクの行動を規制インターホン用 ドロップダウンメニューがあります。他のカメラでは、このオプションは使用できません。

        使用マイクの動作を設定するための [**Microphone Muting(マイクのミュート)**] ドロップダウンメニュー。デフォルト設定は **Never Mute (ミュートしない)**
    c. です。
        - **Never Mute (ミュートしない)**： ACC Client ユーザーはカメラからの音声をいつでも聞くことができます。
        - **Always Mute (常にミュート)**：ACC Client ユーザーは、カメラからの音声を聞くことができません。これは、一部の地域のプライバシー法で要求される場合があります。インターコムコールが開始されると、着信音がミュートされ、ACCClient には、ポップアップダイアログのみが表示されます。
        - **Unmute Only During Call (通話中だけミュート解除)**：インターコム コールの進行中、 ACCClient ユーザーは常にカメラからの音声を聞くことができます。
4. [**Apply(適用)**] をクリックして、変更を保存します。

ユーザー

Users(ユーザー) ページで、新しいユーザーの追加、既存のユーザーの編集、パスワードの変更を行うことができます。

ユーザーの追加

1. 「ユーザー」ページで、[**Add...(追加…)**] をクリックします。
2. 「AddUser(ユーザーの追加)」ページで、新しいユーザーのユーザー名とパスワードを入力します。
3. [**Security Group(セキュリティ グループ)**] ドロップダウンリストで、この新規ユーザーに与えるアクセス許可を選択します。
    - **Administrator(管理者)**: 、カメラの Web インターフェースの全機能にフルにアクセス。
    - **Operator(操作者)**: ライブ ビューとへのアクセス。ただし、セットアップ機能へのアクセスは制限付き。ユーザーがアクセスできるのは、General ページ、Image and Display(画像および表示) ページ、Compression and Image Rate(圧縮および画像レート) ページ、Motion Detection(モーション検出) ページ、Privacy Zones(プライバシー ゾーン) ページ、Digital Inputs and Outputs(デジタル入出力) ページ、Microphone(マイク) ページおよびSpeakers(スピーカー) ページだけです。新しいユーザーは、オンボード ストレージ設定も行うことができますが、ビデオ録画を削除したり、SD カードをフォーマットしたりすることはできません。
    - **ユーザー**: Live View(ライブビュー)にアクセスできますが、「セットアップ」ページにはアクセスできません。
4. [**Apply(適用)**] をクリックしてユーザーを追加します。

ユーザーとパスワードの編集

1. 「Users(ユーザー)」ページで、 ユーザー名 (セキュリティ グループ) リストからユーザーを選択して、[**Modify(変更)**] をクリックします。
2. ユーザーのパスワードを変更するには、そのユーザーに対する新しいパスワードを入力します。
3. そのユーザーのセキュリティ グループを変更するには、[**Security Group(セキュリティ グループ)**] ドロップダウン リストで別のグループを選択します。

    メモ：管理者アカウントのセキュリティ グループを変更することはできません。

4. [**Apply(適用)**] をクリックして、変更を保存します。

ユーザーの削除

メモ：デフォルト Administrator(管理者) ユーザーを削除することはできません。

1. 「Users(ユーザー)」ページで、 (Security Group) リストからユーザーを選択します。
2. [**Remove(削除)**] をクリックします。

ファームウェアの復元後のユーザー名とパスワードの保持

カメラを盗難から保護するセキュリティレイヤーを追加するために、ファームウェア復元後にカメラの現在のユーザー名とパスワードを保持するオプションが提供されています。

通常は、カメラのファームウェアを工場出荷時の既定値設定に復元した場合、カメラは既定のユーザー名とパスワードを使用するように復元されます。この機能を有効にすると、カメラは引き続き設定済みのユーザー名とパスワードを使い続けるため、カメラは、適切な資格情報なしに新しいサーバーに接続することはできなくなります。

重要：この設定を有効にした後で自分のユーザー名またはパスワードを忘れると、保証が無効になります。工場出荷時のユーザー名とパスワードを復元する主な方法は無効になります。

1. Users(ユーザー)ページの一番下にある [**Do not clear usernames or passwords on firmware revert(ファームウェア復元時にユーザー名またはパスワードを消去しない)**] チェックボックスをオンにします。
2. チェックボックスをオンにすると、次のポップアップ メッセージが表示されます。

   *Please store your administrator password in a safe place. Password recovery is not covered by warranty and loss of password may void your warranty.(*管理者パスワードを安全な場所に保管してください。パスワードの復元は保証対象ではないため、パスワードを紛失すると、保証が無効になることがあります。*)*
3. 機能の制限に同意する場合は、[**OK(OK)**] をクリックします。

カメラへのアクセスを失うことがないように、必ずパスワードのコピーを安全な場所に保管しておいてください。

システム

「System(システム)」ページでは、カメラのファームウェアのアップグレード、カメラの再起動、カメラの工場出荷時のすべての設定の復元などを手動で行うことができます。

- [**Reboot(再起動)**] をクリックしてカメラを再起動します。
- カメラのファームウェアを工場出荷時の設定に戻すには、[**Restore(復元)**] をクリックします。

ヒント：ファームウェアを元に戻した後でユーザー名とパスワードを維持する機能を有効にしている場合は、現在のユーザー名とパスワードを必ず書き留めておいてください。詳細については、「ファームウェアの復元後のユーザー名とパスワードの保持」（51ページ）を参照してください。

- (H4 マルチセンサーH4SL-DO および H4SL-BO カメラのみ) カメラのレンズが想定どおりに機能しなくり、[Image and Display(画像および表示)] ページからレンズの焦点を合わせられなくなった場合、レンズを再初期化しなければならないことがあります。

  [**Reinitialize(再初期化)**] をクリックしてレンズが再初期化されるのを待ちます。プロセスが完了すると、ページの一番下に緑のメッセージが表示されます。H4 マルチセンサー カメラの場合、一度に任意のカメラ Head (ヘッド) または All Heads(すべてのヘッド) のレンズを再初期化することができます。

- カメラのファームウェアをアップグレードするには、「「カメラのファームウェアのアップグレード」（52ページ）」を参照してください。

カメラのファームウェアのアップグレード

カメラのファームウェアを手動でアップグレードするには:

1. Avigilon の Web サイトから最新バージョンのファームウェア .bin ファイルをダウンロードし (**avigilon.com/support**)、以下のステップを完了します:
2. 「System(システム)」ページで、[Choose File] をクリックしてダウンロードし、ファームウェアファイルを参照して見つけます。
3. [**Upgrade(アップグレード)**]をクリックします。カメラのアップグレードが完了するのを待ちます。

デバイス ログ

「DeviceLog(デバイスログ)」ページで、カメラのシステムログとカメラのアクセスログを表示できます。

最新のログイベントが常に最初に表示されます。

1. [**Type(種類)**] ドロップダウン リストで、次のいずれかを選択します：
    - **Access Logs(アクセス ログ)** — Web インターフェイスにログインしたユーザーのログ。
    - **System Logs(システム ログ)**— カメラ操作のログ。
2. [**Minimum Log Level(最小ログ レベル)**] ドロップダウン リストで、表示させたいログ メッセージの最低レベルを選択します:
    - **Error(エラー)**— カメラで重大なエラーが発生したときに送信。これらは最高レベルのログメッセージです。
    - **Warning(警告)** — 無効なユーザー名やパスワードが入力された場合など、カメラがマイナーなエラーに遭遇したときに送信。
    - **Info(情報)**—カメラによって送信される状態情報。これらは最低レベルのログメッセージです。
3. [**Maximum Number of Logs(最大ログ数)**] ドロップダウン リストで、表示させたいログ メッセージの数を選択します:
4. [**Update(更新)**] をクリックします。

    ログが更新され、フィルタリングされた情報が表示されます。

WebUI の無効化

WebUI の無効化 ページで、任意の非 ONVIF API コールを含む、カメラの Web インターフェースを無効化できます。これにより、ACC クライアントまたは ONVIF 準拠の VMS 以外からのカメラへのアクセスが無効になります。

重要：Web UI と非 ONVIF API を無効にすると、ACC クライアントまたは ONVIF 準拠の VMS でのみカメラに接続できます。
この設定を元に戻すには、カメラの物理ファームウェアを元に戻すしかありません。詳細については、カメラのインストールガイドを参照してください。

Web UI および非 ONVIF API を無効化するには:

1. [**非 ONVIF API の無効化**] チェックボックスを選択します。
2. [**Apply(適用)**] をクリックします。
3. この設定を進める場合、表示される警告メッセージを読んでから、[**OK(OK)**] をクリックします。

H4 マルチセンサー と H5A デュアルヘッドカメラ

Avigilon H4 マルチセンサー と H5A デュアルヘッドカメラは、設定がカメラに搭載されているヘッド数分あることを除けば、本ガイドで説明する他のカメラと同じ設定を使用します。カメラの各ヘッドの設定を個別に行うことができます。

カメラのビデオディスプレイを見ると、カメラの各ヘッドごとに 1 つ、2、 3 または 4 つの画像パネルが表示されているのがわかります：

左上の画像パネルは常に Head 1(ヘッド 1) 用です 。奇数番号のヘッドは左側に表示され、偶数番号のヘッドは右側に表示されます。

ビデオ表示を制御するには：

- 画像パネルをクリックし、ズームとフォーカスのコントロールを使ってビデオ画像を調整します。
- 画像パネルにマウスを移動して をクリックし、画像パネルを最大に表示させます。 をクリックして、画像パネルを元に戻します。

カメラヘッドごとの設定を変更する

ビデオ画像の設定を調整すると、通常、各カメラヘッドのタブが表示されます。特定のカメラヘッドの設定を変更するには、設定ページでそのヘッドのタブを選択し、必要な変更を加えます。

タブが表示されない場合、設定はカメラ全体に適用されます。

[**AllHeads(すべてのヘッド)**]タブは、「ImageandDisplay(画像および表示)」、「Adjustments(調整)」、および「MotionDetection(モーション検出)」ページにだけ表示されます。「**AllHeads(すべてのヘッド)**」ページでは、カメラ全体に適用される設定と特定のカメラヘッドに適用される設定を変更できます。

1. [**All Heads(すべてのヘッド)**] タブを選択して、カメラ全体に適用する設定を調節します。これらの設定には Flicker Control(フリッカー制御)、および、Image and Display(画像および表示) ページの Enable WDR(WDR) だけでなく、Image and Display(画像および表示) > Adjustments(調整) ページ上の Saturation(彩度)、Brightness(輝度)、Sharpness(シャープネス)およびContrast (コントラスト) が含まれます。
2. [AllHeads(すべてのヘッド)]タブでは、**Imagingmode(撮像モード)**を設定することができます。
    - すべてのカメラ ヘッドに同じ設定を適用する場合は、[**Global(グローバル)**] を選択します。[All Heads] タブにある設定を使って、カメラの画像設定を調節します。番号付きの [Head (ヘッド)] タブに対して同じ設定が無効になります。
    - [**Per-head(ヘッド単位)**] を選択して、それぞれのカメラ ヘッドに異なる設定を適用します。各カメラ ヘッドの設定を変更するには、異なるタブを選択します。
3. 番号の付いた各タブを選択して、各カメラヘッドのフォーカス コントロールを調整します。これらの設定は、カメラヘッドごとに手動で調整する必要があります。

画像およびディスプレイのさまざまな設定の詳細については、「「Image and Display(画像および表示)」（18ページ）」を参照してください。

H4 マルチセンサー IR LED を有効化および無効化する詳しい方法については、「IR LED の有効化と無効化」（55ページ）を参照してください。

IR LED の有効化と無効化

IR LED Ring (赤外線 LED リング) ページは、 H4 マルチセンサー カメラのオプションの IR LED Ring (赤外線 LED リング) (H4AMH-AD-IRIL1) の個々の赤外線 LED を有効または無効にするために使用します。H4 マルチセンサー カメラの配置や用途に応じて IR LED Ring (赤外線 LED リング) 上の IR LED の一部を無効にする必要があるかもしれません。IR LED を無効にすると、IR 光が窓や他の反射面から反射するなどの問題を回避できます。

1. 左のメニューページで 、 IR LED Ring (赤外線 LED リング) ページに移動します。
2. 個々の IR LED のチェックボックスをLED 1 (LED 1) からLED 6 (LED 6) に選択または選択解除して、選択した LED を有効または無効にします。
3. [**Apply(適用)**] をクリックして、変更を保存します。

IR LED リングヘルスチェック

IR LED Ring (赤外線 LED リング)ページには、IR LED リングのヘルスステータス情報も表示されています。IR LED リングヘルスチェックはデフォルトで有効になっています。

- ヘルスチェックを有効または無効にするには、**Enable IR LED Ring Health Check(IR LED リング正常性チェックの有効化)**チェックボックスを選択または選択解除します。[**Apply(適用)**] をクリックして、変更を保存します。

> **メモ：**IR LED リングヘルスチェックを無効化すると、SNMP 管理ステーションでヘルスチェックステータスイベントをチェックできます (無効化されている場合) 。ヘルスチェックステータスイベントは、SNMP トラップによる通知または ACC クライアントでの ONVIF イベント通知として送信することもできます。SNMP 構成の詳細については、「「SNMP の設定」（15ページ）」を参照してください。ACC イベント通知の詳細については、ACC クライアントドキュメントを参照してください。

ヘルスチェックが有効になっている場合、アプリケーションは 15 秒ごとに各 LED との通信を監視します。**IR LED Ring Status(IR LED リングの状態)**フィールドに次のステータスメッセージが表示される場合があります：

- `Health Check disabled`(**正常性チェックが無効です**)。IR LED リングのヘルスチェックが無効になっていることを示します。
- `No error detected`(**エラーは検出されませんでした**)。IR LED リングが正常に機能していることを示します。
- `Unplugged`(**電源が入っていません**)。このカメラに IR LED リングが接続されていないことを示します。IR LED リングを接続しない場合は、Enable IR LED Ring Health Check(IR LED リング正常性チェックの有効化)チェックボックスを無効化することを検討してください。
- `Error detected in IR ring and power has been disabled. Reboot the camera and if issue persists, please contact support.`(**IR リングにエラーが検出され、電源が切れました。カメラを再起動しても問題が続く場合、サポートにご連絡ください**) ヘルスチェックがリング上のすべての LED と通信できず、IR LED リングを無効にしたことを示します。

  > **ヒント：**カメラを再起動し、IRLEDリングステータスで引き続きエラーが検出されるかどうかを確認します。再起動後もエラーが続く場合は、**avigilon.com/contact**テクニカルサポートに連絡して、IRLEDリングのトラブルシューティングのサポートを受けてください。

カメラヘッドごとの設定を変更する

ビデオ画像の設定を調整すると、通常、各カメラヘッドのタブが表示されます。特定のカメラヘッドの設定を変更するには、設定ページでそのヘッドのタブを選択し、必要な変更を加えます。

タブが表示されない場合、設定はカメラ全体に適用されます。

[**AllHeads(すべてのヘッド)**]タブは、「ImageandDisplay(画像および表示)」、「Adjustments(調整)」、および「MotionDetection(モーション検出)」ページにだけ表示されます。「**AllHeads(すべてのヘッド)**」ページでは、カメラ全体に適用される設定と特定のカメラヘッドに適用される設定を変更できます。

1. [**All Heads(すべてのヘッド)**] タブを選択して、カメラ全体に適用する設定を調節します。これらの設定には Flicker Control(フリッカー制御)、および、Image and Display(画像および表示) ページの Enable WDR(WDR) だけでなく、Image and Display(画像および表示) > Adjustments(調整) ページ上の Saturation(彩度)、Brightness(輝度)、Sharpness(シャープネス)およびContrast(コントラスト) が含まれます。
2. [AllHeads(すべてのヘッド)]タブでは、**Imaging mode(撮像モード)**を設定することができます。
    - すべてのカメラ ヘッドに同じ設定を適用する場合は、[**Global(グローバル)**] を選択します。[All Heads] タブにある設定を使って、カメラの画像設定を調節します。番号付きの [Head (ヘッド)] タブに対して同じ設定が無効になります。
    - [**Per-head(ヘッド単位)**] を選択して、それぞれのカメラ ヘッドに異なる設定を適用します。各カメラ ヘッドの設定を変更するには、異なるタブを選択します。
3. 番号の付いた各タブを選択して、各カメラヘッドのフォーカス コントロールを調整します。これらの設定は、カメラヘッドごとに手動で調整する必要があります。

ACC™ES カメラ

H4EdgeSolution(ES)カメラを構成する場合、左のメニューACCES(ACCES)のオプションをご覧ください。

H4 ES カメラは Avigilon コントロールセンター サーバー ソフトウェアを実行するサーバーコンポーネントを備えています。これにより、各 H4 ES カメラは、独自のサイトとサーバーとしても機能します。

ACC ES(ACC ES)のアプリケーション ページで、ACCサーバーソフトウェアにおけるストリーミングポートとアーカイブの設定の構成が可能です。

ACC ES(ACC ES) カメラ ステータスをチェックする

最初の ACC ES(ACC ES) アプリケーション ページで、Avigilon コントロールセンター ソフトウェアのステータスを確認できます。

- **Avigilon Control Center Information**
  - **ACC Site Name** — カメラが属するサイトの名前。
  - **ACC Server Name** — カメラの名前。
  - **ACC Server Status** - ACC サーバー ソフトウェアの状態。
  - **ACC Server Version** - ACC サーバー ソフトウェアのバージョン。

ACCES カメラの管理設定の構成

「Setup」ページで、ACC 管理者ツールの場合と同様に Avigilon コントロールセンター システム管理者の設定を行うことができます。

ACC ソフトウェアの再起動

ACC サーバー ソフトウェアが想定どおりに動作していない場合は、サーバー コンポーネントを再起動して問題の解決を試みることができます。

1. 「Setup」のページで、[**Disable ACC ES(ACC ES の無効化)**] をクリックします。
2. [**Apply(適用)**] をクリックします。

   カメラが ACC サーバー ソフトウェアをシャットダウンします。
3. [**EnableACCES(ACCESの有効化)**]をクリックして、ACCサーバーソフトウェアを再起動します。

映像が録画されたドライブのフォーマット

ACC ES HD カメラには、記録されたビデオをカメラに直接格納するソリッドステートドライブが含まれています。設定と録画ビデオデータをすべて削除する必要がある場合は、ストレージを再初期化することができます。

1. SSD を初期化するには、[**Reinitialize Storage**] をクリックします。
2. ブラウザに次のエラー メッセージが表示されたら、[**OK**] をクリックします：

   *This will require the ACC ES application to restart and will delete all ACC ES configuration settings and data. Are you sure you want to continue?(*こうすると、*ACC ES* アプリケーションが再起動して、すべての *ACC ES* 設定とデータが削除されます。続行してもよろしいですか*?)*

カメラの ACC サーバー ソフトウェアが再起動します。カメラは、ビデオをストリーミングし続けますが、ACC サーバー ソフトウェアのロードが完了するまでは何も記録されません。

通信ポートの変更

ACC Server は、様々な UDP および TCP ポートを使用して ACC クライアント ソフトウェアと通信します。ポートの範囲を変更する必要があるのは、ACC クライアント ソフトウェアが同じ NAT デバイス (ルーターなど) の背後にある ACC サーバーの複数のインスタンスにアクセスしようとしている場合、またはポートの競合がある場合のみです。

1. Service Ports およびRTP Ports エリアで、ACC サーバーにアクセスするために使用する Base Port を変更できます。
2. [**Apply**] をクリックします。
3. ブラウザに次のエラー メッセージが表示されたら、[**OK**] をクリックします：

   The new service base port or login limits will only take effect once Control Center Server is restarted. Restart Control Center Server now?(Control Center Server が再起動した場合のみ、新しいサービスのベースポートやログイン制限が有効になります。今すぐ *Control Center Server* を再起動しますか*?)*

カメラの ACC サーバー ソフトウェアが再起動します。カメラは、ビデオをストリーミングし続けますが、ACC サーバー ソフトウェアのロードが完了するまでは何も記録されません。

ログイン制限の無効化

デフォルトでは、同時に 2 人のユーザーしかサイトにログインできません。ビデオを監視しないユーザーに余分なアクセスが必要な場合は、推奨されるログイン制限を無効にすることができます。

1. Login Limit(ログイン制限) エリアで、[**Override ACC Client Login Limit(ACC クライアントログイン制限をオーバーライド)**] チェック ボックスを選択します。
2. [**Login Limit:(ログイン制限:)**] フィールドに、カメラ サイトに同時にログインできるユーザー数を入力します。
3. [**Apply(適用)**] をクリックします。

新しい設定が保存されます。2 人以上のユーザーがカメラサイトにログインできるようになりました。

メモ：2 人以上のユーザーが同時にログインすると、カメラの設定によってはカメラのパフォーマンスが低下する可能性があることに注意してください。

Storage Management の有効化

ACC クライアント ソフトウェアにビデオをアーカイブする前に、Storage Management を有効にする必要があります。このページでは、Storage Management (ストレージ管理)ビデオアーカイブを有効化し、アーカイブ済みビデオを保存するネットワークの場所を設定することが可能です。

1. [**Enable Storage Management (ストレージ管理の有効化)**] チェック ボックスを選択します。
2. [**Network Protocol (ネットワークプロトコル)**] ドロップダウン リストから、次のいずれかを選択します。
    - **CIFS(CIFS)** — 共通のインターネット ファイル システム。ネットワーク パスは一般的に次の形式を取ります：//<ホスト名または *IP*> / <パス>
    - **NFS(NFS)** — ネットワーク ファイル システム。ネットワークパスは一般的に次の形式を取ります：<ホスト名または*IP*> ： <パス>
3. [**Network Path (ネットワークパス)**] フィールドに、希望のビデオ アーカイブ ロケーションへのパスを入力します。
4. そのネットワーク ロケーションに認証が必要な場合、[**Authentication(認証)**] チェック ボックスを選択してから、[Username(ユーザー名)] と [Password(パスワード)] フィールドに認証資格情報を入力します。
5. [**Apply(適用)**] をクリックします。

次に、ACCクライアントソフトウェア内のアーカイブスケジュールを設定すると、システムが選択したネットワークの場所に、録画済みのビデオを自動的にアーカイブすることができます。詳細については、『*Avigilon*コントロールセンター*ClientUserGuide*（クライアントユーザーガイド）』を参照してください。

ACCソフトウェアログのレビュー

「Logs(ログ)」ページはAvigilonコントロールセンターシステムイベントのサイトのログを表示します。

最新のログイベントが常に最初に表示されます。

1. [**Type(種類)**] ドロップダウン リストで、次のいずれかを選択します：
   - **Daemon Logs(デーモン ログ)** — ACCサーバー操作のログ。これには、サイトへのログイン、イベントの作成などが含まれます。
   - **App Logs(アプリケーション ログ)**— Web インターフェイス内の ACC ES アプリケーション操作のログ。
2. **Minimum Log Level(最小ログ レベル)** ドロップダウン リストから、次のいずれかを選択します:
   - **Error(エラー)** — システムで重大なエラーが発生したときに送信。これらは最高レベルのログ メッセージです。
   - **Warning(警告)**— 無効なユーザー名やパスワードが入力された場合など、システム上比較的重要ではないエラーが発生した場合に送信。これはデフォルトで選択されています。
   - **Info(情報)**—システムによって送信される状態情報。これらは最低レベルのログメッセージです。
3. [**Maximum Number of Logs(最大ログ数)**] ドロップダウン リストで、表示させたいログ メッセージの数を選択します。
4. [**Update(更新)**] をクリックします。

   ログが更新され、フィルタリングされた情報が表示されます。