ネットワークカメラ

ユーザーマニュアル

法的情報

このドキュメントについて

- この文書には、製品の使用および管理に関する説明が含まれています。以下に記載されている写真、図、画像、およびその他の情報は、説明および解説のみを目的としています。
- 本ドキュメントに記載されている情報は、ファームウェアのアップデートなどの理由により、予告なく変更される場合があります。最新バージョンのドキュメントは、Hikvision のウェブサイト (***https://www.hikvision.com***) をご覧ください。別段の合意がない限り、Hangzhou Hikvision Digital Technology Co., Ltd. またはその関連会社 (以下「Hikvision」) は、明示的または黙示的を問わず、いかなる保証もいたしません。
- 本ドキュメントは、製品をサポートする専門家の指導と支援を受けてご使用ください。

本製品について

- この製品は、購入した国または地域でのみアフターサービスサポートを受けることができます。
- お選びになった製品がビデオ製品の場合は、以下の QR コードをスキャンして「ビデオ製品の使用に関する取り組み」を入手し、よくお読みください。

知的財産権の承認

- 本ドキュメントに記載される製品に組み込まれた技術に関する著作権および/または特許権は、Hikvisionが所有しています。これには、第三者から取得したライセンスを含む場合があります。
- 本文書の一部（テキスト、画像、グラフィックなど）は、Hikvision に帰属します。本文書のいかなる部分も、書面による許可なく、その全部または一部を、いかなる手段によっても、抜粋、複製、翻訳、または改変することはできません。
- HIKVISION およびその他のヒクビジョンの商標およびロゴは、各管轄区域においてヒクビジョンの財産です。
- 本文書で言及されるその他の商標およびロゴは、それぞれの所有者の財産です。

法的免責事項

- 適用される法律で許される最大限の範囲において、本書および本書に記載される製品（ハードウェア、ソフトウェア、およびファームウェアを含む）は、「現状有姿」および「すべての欠陥およびエラーを含む」状態で提供されます。HIKVISION は、明示的または黙示的を問わず、商品性、満足のいく品質、または特定の目的への適合性を含むがこれらに限定されない、いかなる保証も一切行いません。

明示的または黙示的ないかなる保証も提供しません。これには、商品性、満足のいく品質、または特定の目的への適合性に関する保証が含まれますが、これらに限定されません。製品の使用は、お客様の責任において行ってください。いかなる場合においても、HIKVISION は、事業利益の損失、事業の中断、データの損失、システムの破損、または文書の損失を含むがこれらに限定されない、特別、結果的、偶発的、または間接的な損害について、契約違反、不法行為（過失を含む）、製品責任、その他に基づくものであるかを問わず、お客様に対して一切の責任を負いません。システムの破損、または文書の損失を含む損害について、契約違反、不法行為（過失を含む）、製品責任、またはその他の理由に基づくものであっても、製品の使用に関連して生じた場合、HIKVISIONは一切の責任を負いません。これは、HIKVISIONがそのような損害または損失の可能性について事前に通知を受けていた場合でも同様です。

- お客様は、インターネットの性質上、セキュリティ上のリスクが内在していることを認識し、サイバー攻撃、ハッカーの攻撃、ウイルス感染、その他のインターネットセキュリティリスクに起因する異常な動作、プライバシーの漏洩、その他の損害について、HIKVISION は一切の責任を負わないことを認めます。ウイルス感染、またはその他のインターネットセキュリティリスクに起因する異常な動作、プライバシーの漏洩、その他の損害について一切の責任を負いません。ただし、必要に応じて、HIKVISION はタイムリーな技術サポートを提供します。
- あなたは、この製品を適用されるすべての法律に準拠して使用することに同意し、あなたの使用が適用される法律に準拠していることを確保する責任は、あなたのみに帰属します。特に、お客様は、パブリシティ権、知的財産権、データ保護およびその他のプライバシー権を含むがこれらに限定されない、第三者の権利を侵害しない方法で本製品を使用することについて責任を負います。お客様は、大量破壊兵器の開発または製造、化学兵器または生物兵器の開発または製造、核爆発または安全でない核燃料サイクルに関連するいかなる活動、または人権侵害を支援する目的での使用を含みます。
- 本文書と適用法との間に矛盾がある場合は、適用法が優先するものとします。

記号の定義

本文書中に使用される記号は、以下のとおり定義されます。

記号	説明
 **危険**	危険な状況を示し、回避されない場合、死亡または重傷を負うおそれがあります。
 **注意**	危険な状況が発生する可能性があり、回避しない場合、機器の損傷、データ損失、性能の低下、または予期しない結果を引き起こす可能性があります。
 **注**	本文の重要な点を強調または補足するための追加情報を提供します。

安全に関する指示

製品の「***安全に関する注意事項***」を入手するには、以下の QR コードをスキャンして、よくお読みください。これらの注意事項は、ユーザーが製品を正しく使用し、危険や財産の損失を防ぐことを目的としています。

図 1-1 安全に関する注意事項

目次

第1章 概要

1.1 設定手順

このセクションでは、ネットワークカメラのソフトウェア設定プロセスについて簡単に説明します。実際の状況に応じて、デバイスを設定してください。

全般的な設定手順

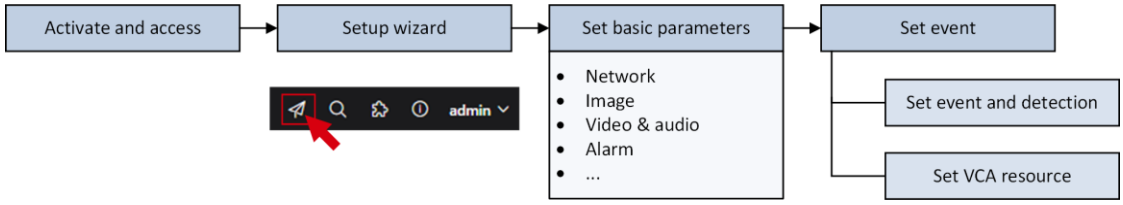

図 1-1 全体構成

- ***ウェブブラウザーからデバイスを起動してアクセスします。*** ネットワーク経由でデバイスにアクセスする場合は、デバイスを起動するためのログインパスワード（**管理者**ユーザー用）を設定する必要があります。ウェブブラウザーを開き、IP アドレスを入力します。デバイスのデフォルトの IP アドレスは 192.168.1.64 です。
- **ウィザード**に従うか、ウェブページ上の「 」 をクリックして、デバイスのパラメーターを迅速に設定します。
- ネットワーク、画像、ビデオ、オーディオ、アラームなどの基本パラメータを設定します。
- イベントおよび検出ルールを設定します。基本***イベントおよび検出***ルールを設定したり、ディープラーニング機能用に ***VCA 割り当てたりすることができますリソースを***。

1.2 ファームウェア更新

より良いユーザー体験のため、デバイスを最新のファームウェアに更新することをおすすめします。

公式ウェブサイトまたはお近くの技術専門家から最新のファームウェアパッケージを入手してください。詳細については、公式ウェブサイトをご覧ください：***https://www.hikvision.com/en/support/ download/firmware/***。

アップグレード設定については、***アップグレード***を参照してください。

1.3 システム要件

お使いのコンピュータは、製品を正常に閲覧および操作するための要件を満たしている必要があります。

オペレーティングシステム	Microsoft Windows XP SP1 以降CPU 2.0 GHz 以上
RAM	1GB 以上
ディスプレイ	1024×768 以上の解像度
ウェブブラウザー	詳細については、*プラグインのインストールを*参照してください。

第2章 デバイスのアクティベーションとアクセス

ユーザーアカウントとデータのセキュリティおよびプライバシーを保護するため、ネットワーク経由でデバイスにアクセスする場合は、デバイスをアクティブ化するためのログインパスワードを設定してください。

注意
クライアントソフトウェアの起動に関する詳細については、ソフトウェアクライアントのユーザーマニュアルを参照してください。

2.1 SADP 経由でデバイスをアクティベート

SADPソフトウェアを使用して、オンラインデバイスを検索しアクティベートしてください。

開始前に

www.hikvision.com にアクセスし、SADP ソフトウェアをダウンロードしてインストールしてください。

手順

1. ネットワークケーブルを使用して、デバイスをネットワークに接続します。
2. SADP ソフトウェアを実行して、オンラインのデバイスを検索します。
3. デバイス一覧から**デバイス状態**を確認し、**非アクティブな**デバイスを選択します。
4. パスワードフィールドに新しいパスワードを作成して入力し、パスワードを確認します。

   注意

   製品のセキュリティを強化するため、大文字、小文字、数字、特殊文字を含む 8 文字以上の強力なパスワードを設定することを強くお勧めします。また、セキュリティの高いシステムでは、パスワードを定期的にリセットすることをお勧めします。パスワードを毎月または毎週リセットすることで、製品をより確実に保護することができます。
5. **OK**をクリックします。

   デバイスの状態が「アクティブ」に変わります。
6. **オプション：**[ネットワークパラメータの変更] で、デバイスの**ネットワークパラメータを変更します**。

2.2 ブラウザ経由でデバイスをアクティブ化します

ブラウザ経由でデバイスにアクセスし、アクティブ化できます。

手順

1. ネットワークケーブルを使用して、デバイスを PC に接続します。
2. PCとデバイスのIPアドレスを同じセグメントに変更します。

注意

デバイスのデフォルトIPアドレスは192.168.1.64です。PCのIPアドレスは、192.168.1.2から192.168.1.253（192.168.1.64を除く）の範囲内で設定できます。例えば、PCのIPアドレスを192.168.1.100に設定できます。

3. ブラウザに***192.168.1.64***を入力してください。
4. デバイスアクティベーションパスワードを設定してください。

注意

製品のセキュリティを強化するため、お客様ご自身で強力なパスワード（8 文字以上で、大文字、小文字、数字、特殊文字のうち少なくとも 3 種類を含む）を設定することを強くお勧めします。また、セキュリティの高いシステムでは、パスワードを定期的にリセットすることをお勧めします。パスワードを毎月または毎週リセットすることで、製品をより確実に保護することができます。

5. **OK**をクリックしてください。
6. デバイスにログインするためにアクティベーションパスワードを入力してください。
7. **オプション：**[**Configuration]、[→]、[Network]、[→]、[Network Settings]、[→]、[TCP/IP]** の順に選択し、デバイスの IP アドレスをネットワークの同じセグメントに変更します。

2.3 ログイン

ウェブブラウザーからデバイスにログインします。

2.3.1 プラグインのインストール

一部のオペレーティングシステムおよびウェブブラウザーでは、本製品の機能の一部が制限される場合があります。正常に表示および動作させるためには、プラグインのインストールや設定が必要になる場合があります。制限される機能の詳細については、実際の製品をご確認ください。

オペレーティングシステム	ウェブブラウザー	操作
Windows	• Internet Explorer 10以降 • GoogleChrome 57 以前のバージョン • Mozilla Firefox 52 以前のバージョン	ポップアップの指示に従って、プラグインのインストールを完了してください。
	• Google Chrome 57以降 • Mozilla Firefox 52以降 • Edge 89以降	「」をクリックしてプラグインをダウンロードし、インストールしてください。
Mac OS	• Google Chrome 57+ • Mozilla Firefox 52+ • Mac Safari 16+	プラグインのインストールは不要です。 **設定 → ネットワーク→ ネットワークサービス** **→ WebSocket(s)** を選択し、WebSocketまたはWebSocketsを有効にします。一部の機能の表示と操作が制限されます。例えば、再生と画像の表示が利用できません。詳細な制限機能については、実際のデバイスをご確認ください。

注意

- このデバイスはWindowsおよびMac OSシステムのみに対応しており、Linuxシステムには対応していません。
- 一部のデバイスでは、ユーザーエクスペリエンスを向上させるため、より高度なウェブブラウザーを使用してアクセスすることをお勧めします。実際のデバイスまたは製品の仕様をご確認ください。
- 一部のデバイスモデルは、Internet Explorer ウェブブラウザーに対応していません。

2.3.2 管理者パスワードの回復

管理者パスワードを忘れた場合は、アカウントのセキュリティ設定を完了した後、ログインページで**「パスワードを忘れた場合」**をクリックしてパスワードをリセットすることができます。

セキュリティの質問または E メールを設定して、パスワードをリセットすることができます。

注意

パスワードをリセットする場合は、デバイスと PC が同じネットワークセグメントにあることを確認してください。

セキュリティの質問

アクティベーション時にアカウントのセキュリティを設定することができます。または、**[設定]→[システム]→[ユーザー管理]** に移動し、**[アカウントのセキュリティ設定]** をクリックして、セキュリティの質問を選択し、答えを入力してください。
ブラウザからデバイスにアクセスする際に、**パスワードを忘れた**場合は、「**パスワードを忘れた場合**」をクリックし、セキュリティの質問に答えて、管理者パスワードをリセットすることができます。

メール

アクティベーション時にアカウントのセキュリティを設定することができます。または、**[設定]→[システム]→[ユーザー管理]** に移動し、[**アカウントのセキュリティ設定**] をクリックして、回復操作中に確認コードを受信するメールアドレスを入力してください。

2.3.3 不正ログインロック

これは、インターネット経由でデバイスにアクセスする際のセキュリティを向上させます。

[メンテナンスとセキュリティ]→[→ セキュリティ]→[→ ログイン管理] に移動し、[**不正ログインロックを有効にする**] を有効にします。**不正ログインの**試行回数と**ロックの継続**時間は設定可能です。

不正ログイン試行

間違ったパスワードでのログイン試行が設定回数に達すると、デバイスがロックされます。

ロック時間

設定時間が経過すると、デバイスはロックを解除します。

第3章 ライブビュー

ライブビューのパラメーター、機能アイコン、および送信パラメーターの設定について説明します。

3.1 ライブビューパラメーター

対応する機能はモデルによって異なります。

3.1.1 ライブビューの開始と停止

「ライブビュー」をクリックします。「 」をクリックしてライブビューを開始します。「 」をクリックしてライブビューを停止します。

3.1.2 アスペクト比

アスペクト比は、画像の幅と高さの表示比率です。

- 4:3のウィンドウサイズを指します。
- 16:9のウィンドウサイズを指します。
- 元のウィンドウサイズを指します。
- 自己適応型ウィンドウサイズを指します。
- 元の比率のウィンドウサイズを指します。

3.1.3 ライブビュー ストリーム タイプ

必要に応じてライブビュー ストリーム タイプを選択してください。ストリーム タイプの選択に関する詳細情報は、***Stream Type*** を参照してください。

3.1.4 サードパーティプラグインを選択

特定のブラウザでライブビューが表示されない場合、ブラウザに応じてライブビュー用のプラグインを変更できます。

手順

1. **ライブビュー**をクリックします。
2. 「 」をクリックしてプラグインを選択します。
   - Internet Explorer 経由でデバイスにアクセスする際は、Webcomponents または QuickTime を選択できます。
   - その他のブラウザからデバイスにアクセスする場合は、Webcomponents、QuickTime、または MJPEG を選択できます。

3.1.5 照明

をクリックして、照明のオン/オフを切り替えます。

注意

レーザーを搭載したデバイスについて:

- 動作中の光源を直視しないでください。目に有害な場合があります。
- 適切なシールドや眼の保護具がない場合は、安全な距離から、または光が直接当たらない場所でライトを点灯してください。
- 装置の組み立て、設置、またはメンテナンスを行う場合は、ライトを点灯したり、保護メガネを着用したりしないでください。

3.1.6 ピクセルを数える

ライブビュー画像で選択した領域の高さと幅のピクセル数を測定するのに役立ちます。

手順

1. 「」をクリックして機能を有効にします。
2. 画像上でマウスをドラッグして、目的の矩形領域を選択します。
   ライブビュー画像の下部に、幅ピクセルと高さピクセルが表示されます。

3.1.7 デジタルズームを開始

画像内の任意の領域の詳細情報を見るのに役立ちます。

手順

1. 「」をクリックしてデジタルズームを有効にします。
2. ライブビュー画像で、マウスをドラッグして目的の領域を選択します。
3. ライブビュー画像をクリックすると、元の画像に戻ります。

3.1.8 補助フォーカス

電動式装置に使用します。装置がピントを合わせられない場合、画像の鮮明度を向上させます。

ABF 対応機器の場合は、レンズの角度を調整し、ピントを合わせてから、機器の ABF ボタンをクリックしてください。機器がピントを合わせます。

「」をクリックして自動フォーカスを行います。

注意

- 補助フォーカスでピントが合わない場合は、***レンズ初期化***を使用して、補助フォーカスを再度使用して画像を鮮明にしてください。
- 補助フォーカスでデバイスが明確にフォーカスできない場合、マニュアルフォーカスを使用できます。

3.1.9 レンズの初期化

レンズ初期化は、電動レンズを搭載したデバイスで使用されます。この機能は、ズームやフォーカスを長時間操作して画像がぼやけた場合に、レンズをリセットすることができます。この機能は、モデルによって異なります。

をクリックして、レンズの初期化を行います。

3.1.10 レンズパラメータの調整

PTZ は、パン、チルト、ズームの略語です。これは、デバイスの移動オプションを意味します。ライブビューインターフェースでは、方向制御ボタンをクリックしてパン/チルトの動きを制御し、ズーム/フォーカス/アイリスボタンをクリックしてレンズ制御を行うことができます。

注意

- サポートされている PTZ 機能は、カメラモデルによって異なる場合があります。
- レンズ移動のみに対応している機器では、方向ボタンは機能しません。

方向制御

方向ボタンをクリックしたままにすると、デバイスのパン/チルト操作ができます。

ズーム

- をクリックすると、レンズがズームインします。
- をクリックすると、レンズがズームアウトします。

フォーカス

- クリック をクリックすると、レンズが近距離に焦点を合わせ、近くのオブジェクトが鮮明になります。
- クリック をクリックすると、レンズが遠方に焦点を合わせ、遠くの物体が鮮明になります。

絞り

- 画像が暗すぎる場合は、 をクリックして虹彩を拡大します。
- 画像が明るすぎる場合は、 をクリックしてアイリスを絞ります。

PTZ速度

- をスライドして、パン/チルトの動きの速度を調整します。

PTZロック

PTZ ロックとは、対応するチャンネルのズーム、フォーカス、PTZ 回転機能を無効にして、PTZ 調整によるターゲットの失点を減らすことです。

注意

この機能は、特定のデバイスモデルでのみサポートされています。

「」をクリックしてPTZ操作をロックするか、「」をクリックしてロックを解除します。

PTRZ調整

PTRZ は、パン、チルト、回転、ズームの略語です。これは、デバイスの移動オプションを意味します。インターフェースでは、コントロールボタンを使用して、デバイスのパン、チルト、回転、ズームなどの動きを調整できます。

注

この機能は、特定のデバイスモデルでのみサポートされています。

設定→ PTZ→ PTRZ に移動します。

コントロールパネル

	方向ボタンをクリックして押し続けると、デバイスをパン/チルトできます。
•  • 	ボタンをクリックして押し続けると、回転位置を調整できます。

自動回復

をクリックすると、デバイスは回転位置を自動的に補正し、ライブビュー画像が正立になります。**セルフテストステータスが初期化されている**ことを確認してください。

注

- **[Configuration]** (設定) に移動し、**[→] (PTZ) [PTZ] (PTZ)** をクリックして、**セルフテストステータスを表示します。→ (PTZ) (PTZ)** をクリック
- PTZ を初期化し、PTZ セルフチェックを手動で有効にする場合は、**[Configuration]** (設定) → **[→] (PTZ) → [PTZ] (PTZ)** に移動し、**[Self-Test] (セルフテスト)** をクリックすると、PTZ が初期化されます。

レンズ調整の詳細設定については、「*レンズパラメータの調整*」を参照してください。

3.1.11 3D位置合わせを実施

3D 位置決めは、選択した領域を画像の中心に移動する操作です。

手順

1. をクリックして機能を有効にします。
2. ライブ画像から対象領域を選択します。
   - ライブ画像上の任意の点を左クリック：その点がライブ画像の中心に移動します。ズームイン、ズームアウトの効果はありません。
   - マウスを右下にドラッグすると、ライブ画像の一部がフレームで囲まれます。フレームで囲まれた部分が拡大され、ライブ画像の中心に移動します。
   - マウスを左上にドラッグすると、ライブ画像の一部がフレームで囲まれます。フレームで囲まれた領域は、ライブ画像の中心にズームアウトして移動します。
3. ボタンを再度クリックして機能をオフにします。

3.2 送信パラメーターを設定します

ネットワークの状態により、ライブビュー画像が正常に表示されない場合があります。ネットワーク環境に応じて、送信パラメータを調整して解決してください。

手順

1. **[Configuration]** (設定) に移動します。**→ (ローカル)→ (ライブビューパラメータ)** に移動します。
2. 必要な送信パラメーターを設定します。

プロトコル

TCP

TCP は、ストリーミングデータの完全な配信とより良いビデオ品質を保証しますが、リアルタイムの伝送に影響があります。安定したネットワーク環境に適しています。

UDP

UDP は、高いビデオの滑らかさを必要としない不安定なネットワーク環境に適しています。

マルチキャスト

マルチキャストは、複数のクライアントが存在する状況に適しています。選択する前に、それらのマルチキャストアドレスを設定しておく必要があります。

注意

マルチキャストの詳細については、***Multicast***を参照してください。

HTTP

HTTP は、サードパーティがデバイスからストリームを取得する必要がある場合に適しています。

再生性能最短遅延

ビデオの滑らかさを優先するよりも、リアルタイムのビデオ画像を優先します。

バランス

リアルタイムのビデオ画像と滑らかさを両立します。

滑らか

デバイスは、リアルタイムよりもビデオの滑らかさを優先します。ネットワーク環境が悪い場合、滑らかさが有効になっていても、デバイスはビデオの滑らかさを保証できません。

カスタム

フレームレートを手動で設定することができます。ネットワーク環境が悪い場合、フレームレートを下げることでライブビューの滑らかさを確保することができます。ただし、ルール情報は表示されなくなる場合があります。

3. **保存**をクリックしてください。

第 4 章 ビデオおよびオーディオ

このパートでは、ビデオおよびオーディオ関連パラメータの設定について紹介します。

4.1 ビデオ設定

この部分では、ストリームタイプ、ビデオエンコーディング、解像度などのビデオパラメータの設定について紹介します。

設定ページに移動：**設定→ ビデオ/オーディオ→ ビデオ**。

4.1.1 ストリームの種類

デバイスが複数のストリームをサポートする場合、各ストリームタイプに対してパラメーターを指定できます。

メインストリーム

このストリームは、デバイスがサポートする最高のストリームパフォーマンスを表します。通常、デバイスが実行できる最高の解像度とフレームレートを提供します。ただし、解像度とフレームレートが高いほど、通常、必要なストレージ容量が大きくなり、伝送に必要な帯域幅も大きくなります。

サブストリーム

このストリームは通常、比較的低い解像度オプションを提供し、帯域幅とストレージスペースの消費が少なくなります。

その他のストリーム

メインストリームおよびサブストリーム以外のストリームも、カスタマイズしてご利用いただくことができます。

4.1.2 ビデオタイプ

ストリームに含めるコンテンツ（ビデオおよびオーディオ）を選択します。

ビデオストリーム

ストリームにはビデオコンテンツのみが含まれます。

ビデオ＆オーディオ

ビデオコンテンツとオーディオコンテンツが複合ストリームに含まれます。

4.1.3 解像度

実際のニーズに応じてビデオの解像度を選択してください。解像度が高いほど、必要な帯域幅とストレージ容量も大きくなります。

4.1.4 ビットレートタイプと最大ビットレート

定常ビットレート

ストリームが圧縮され、比較的固定されたビットレートで伝送されることを意味します。圧縮速度は速いですが、画像にモザイクが発生する場合があります。

可変ビットレート

これは、デバイスが設定された**最大ビットレート**の下で自動的にビットレートを調整することを意味します。圧縮速度は、固定ビットレートよりも遅くなります。しかし、複雑なシーンの画質は保証されます。

4.1.5 ビデオ品質

ビットレートタイプが可変に設定されている場合、ビデオ品質は設定可能です。実際のニーズに応じて、ビデオ品質を選択してください。ビデオ品質が高いほど、必要な帯域幅も大きくなりますのでご注意ください。

4.1.6 フレームレート

フレームレートは、ビデオストリームが更新される頻度を表し、1 秒あたりのフレーム数 (fps) で測定されます。

フレームレートが高いほど、ビデオストリームに動きがある場合に有利です。これは、フレームレートが高いほど、全体的な画質が維持されるためです。ただし、フレームレートが高いほど、必要な帯域幅とストレージ容量も大きくなります。

4.1.7 ビデオエンコーディング

これは、デバイスがビデオエンコーディングに採用している圧縮規格を表します。

注意
入手可能な圧縮規格は、デバイスモデルによって異なります。

H.264

H.264 は、MPEG-4 Part 10、Advanced Video Coding とも呼ばれる圧縮規格です。画質を損なうことなく、MJPEG や MPEG-4 Part 2 よりも圧縮率を高め、ビデオファイルのサイズを小さくします。

H.264

H.264+ は、H.264 に基づく改良された圧縮コーディング技術です。H.264+ を有効にすると、最大平均ビットレートによって HDD の消費量を推定することができます。H.264 と比較して、H.264+ は、ほとんどのシーンで同じ最大ビットレートで最大 50% のストレージを削減します。

H.264+ を有効にすると、**最大平均**ビットレートを設定できます。デフォルトでは、デバイスが推奨する最大平均ビットレートが設定されています。ビデオの画質が満足できない場合は、このパラメータをより高い値に調整してください。最大平均ビットレートは、最大ビットレートよりも高く設定しないでください。

注意

H.264+ を有効にすると、**I フレーム間隔は**設定できません。

H.265

H.265 は、高効率ビデオコーディング (HEVC) および MPEG-H Part 2 としても知られ、圧縮規格です。H.264 と比較して、同じ解像度、フレームレート、画質でより優れたビデオ圧縮を実現します。

H.265

H.265+ は、H.265 に基づく改良された圧縮コーディング技術です。H.265+ を有効にすると、最大平均ビットレートによって HDD の消費量を推定することができます。H.265 と比較して、H.265+ は、ほとんどのシーンで同じ最大ビットレートでストレージを最大 50% 削減します。

H.265+ を有効にすると、**最大平均**ビットレートを設定できます。デフォルトでは、デバイスが推奨する最大平均ビットレートが設定されています。ビデオの画質が満足できない場合は、このパラメータをより高い値に調整してください。最大平均ビットレートは、最大ビットレートよりも高く設定しないでください。

注意

H.265+ を有効にすると、**I フレーム間隔は**設定できません。

Iフレーム間隔

Iフレーム間隔は、2つのIフレーム間のフレーム数を定義します。

H.264 および H.265 では、I フレーム（イントラフレーム）は、他の画像を参照することなく独立してデコードできる自己完結型のフレームです。I フレームは、他のフレームよりも多くのビットを消費します。したがって、I フレームの数が多い、つまり I フレームの間隔が短いビデオは、より安定した信頼性の高いデータビットを生成しますが、より多くのストレージ容量が必要になります。

SVC

スケーラブル映像符号化（SVC）は、H.264 または H.265 ビデオ圧縮規格の Annex G 拡張の名称です。

SVC 標準化の目的は、1 つ以上のサブセットビットストリームを含む高品質のビデオビットストリームをエンコードできるようにすることです。サブセットビットストリームは、サブセットビットストリームと同じ量のデータを使用して、既存の H.264 または H.265 設計で実現されるのと同様の複雑さと再構築品質でデコードできます。サブセットビットストリームは、より大きなビットストリームからパケットを削除して作成されます。

SVC は、古いハードウェアとの下位互換性を実現します。つまり、低解像度のサブセットしかデコードできない基本的なハードウェアでも同じビットストリームを再生でき、より高度なハードウェアでは高品質のビデオストリームをデコードすることができます。

MPEG4

MPEG4 は、MPEG-4 Part 2 を指し、Moving Picture Experts Group (MPEG) によって開発されたビデオ圧縮フォーマットです。

MJPEG

Motion JPEG (M-JPEG または MJPEG) は、フレーム内コーディング技術を使用したビデオ圧縮フォーマットです。MJPEG フォーマットの画像は、個々の JPEG 画像として圧縮されます。

プロファイル

この機能により、同じビットレートでは、プロファイルが複雑になるほど、画像の品質が高くなり、ネットワークの帯域幅の要件も高くなります。

4.1.8 スムージング

ストリームの滑らかさを指します。スムージングの値が高いほど、ストリームの滑らかさは良くなりますが、ビデオの品質はそれほど満足のいくものにはなりません。スムージングの値が低いほど、ストリームの品質は高くなりますが、滑らかさは失われます。

4.2 オーディオ設定

オーディオエンコーディング、環境ノイズフィルタリングなどのオーディオパラメータを設定する機能です。オーディオ設定ページに移動します：**設定 → ビデオ/オーディオ → オーディオ** 。

注意

一部のカメラモデルのみ対応しています。

4.2.1 オーディオエンコーディング

音声の音声圧縮を選択します。

4.2.2 オーディオ入力

注意

- 必要に応じて、オーディオ入力デバイスを接続します。
- オーディオ入力の表示は、デバイスのモデルによって異なります。

LineIn	MP3、シンセサイザー、アクティブピックアップなど、出力電力の高いオーディオ入力機器に接続する場合は、**オーディオ入力を LineIn** に設定してください。
MicIn	マイクやパッシブピックアップなど、出力の小さいオーディオ入力機器に接続する場合は、**オーディオ入力を**「**MicIn**」に設定してください。

4.2.3 オーディオ出力

注意

必要に応じて、オーディオ出力デバイスを接続してください。

デバイスのオーディオ出力のスイッチです。無効にすると、デバイスのオーディオはすべて出力されません。オーディオ出力の表示は、デバイスのモードによって異なります。

4.2.4 環境ノイズフィルター

OFF または ON に設定します。この機能を有効にすると、環境ノイズをある程度フィルタリングすることができます。

4.3 双方向オーディオ

モニタリング画面で、モニタリングセンターと対象者との双方向オーディオ機能を実現するために使用します。

開始前に

- デバイスに接続されているオーディオ入力デバイス（ピックアップまたはマイク）およびオーディオ出力デバイス（スピーカー）が正常に動作していることを確認してください。デバイスの接続については、オーディオ入力および出力デバイスの仕様を参照してください。
- デバイスに内蔵マイクとスピーカーがある場合は、双方向オーディオ機能を直接有効にすることができます。

手順

1. **ライブビュー**をクリックします。
2. ツールバーの [ ] をクリックして、カメラの双方向オーディオ機能を有効にします。
3. をクリックして、双方向オーディオ機能を無効にします。

4.4 ROI

ROI (関心領域) エンコーディングは、ビデオ圧縮において ROI と背景情報を区別するのに役立ちます。この技術は、関心領域により多くのエンコーディングリソースを割り当て、ROI の品質を向上させます。一方、背景情報にはあまり焦点を当てません。

4.4.1 ROIを設定

ROI (関心領域) エンコーディングは、関心領域により多くのエンコーディングリソースを割り当て、ROI の品質を向上させ、背景情報の品質はそれほど重視しません。

開始前に

ビデオのエンコードタイプを確認してください。ROI は、ビデオのエンコードタイプが H.264 または H. 265 の場合にサポートされます。

手順

1. **[Configuration] (設定)** に移動します。**[→] (ビデオ/オーディオ)** に移動します。**[→] (ROI) に移動します**。
2. **「有効」**にチェック**を入れます**。
3. **ストリームタイプ**を選択します。
4. をクリックして、ライブビュー上にROI領域を描画します。

   注

   調整が必要な固定領域を選択し、マウスをドラッグして位置を調整します。

5. **エリア名**と **ROI レベル**を入力します。
6. **「保存」**をクリックします。

   注

   ROI レベルが高いほど、検出された領域の画像が鮮明になります。

7. **オプション：**複数の固定領域を描画する場合は、他の領域番号を選択し、上記の手順を繰り返します。

4.5 ターゲットクロッピングの設定

画像の一部をトリミングして、その部分のみを送信・保存することで、送信帯域幅や保存容量を節約できます。

手順

1. [**Configuration**]、**[→]**、**[Video/Audio]**、**[→]**、[**Target Cropping]** の順に選択します。
2. **[有効]** をチェックし、[**ストリームタイプ]** で **[サードストリーム]** を設定します。

   注意

   ターゲットクロッピングを有効にすると、サードストリームの解像度は設定できなくなります。
3. **トリミング解像度**を選択します。

   ライブビューに赤いフレームが表示されます。
4. フレームをターゲット領域にドラッグします。
5. **保存**をクリックします。

   注意

   - ターゲットクロッピングは一部のモデルでのみ対応しており、カメラモデルによって機能が異なります。
   - ターゲットクロッピングを有効にすると、一部の機能が使用できなくなる場合があります。

4.6 ストリームに情報を表示

オブジェクト（人物、車両など）の情報がビデオストリームにマークされます。接続されたリアエンドデバイスまたはクライアントソフトウェアで、ラインクロス、侵入検知などのイベントを検出するためのルールを設定できます。

開始前に

この機能は、スマートイベントでサポートされています。**VCA** に移動し、**スマートイベント**を選択して、[**次へ**] をクリックして**スマートイベント**.

手順

1. [**Configuration]**、**[→]**、**[Video/Audio]**、**[→]**、**[Display Info. on Stream]** の順に移動します。
2. **デュアルVCAを有効にするに**チェックを入れます。
3. **保存**をクリックします。

4.7 ディスプレイ設定

画像機能を調整するためのパラメータ設定を行います。**設定 → 画像 → 表**

示設定 に移動します。

デフォルトをクリックして設定を復元します。

4.7.1 シーンモード

さまざまな設置環境に合わせて、あらかじめ定義された画像パラメータのセットがいくつか用意されています。実際の設置環境に応じてシーンを選択すると、表示設定をすばやく行うことができます。

画像調整

明るさ、**彩度**、**コントラスト**、**シャープネス**を調整することで、画像を最適に表示することができます。

露出設定

露出は、絞り、シャッター、および感光の組み合わせによって制御されます。露出パラメータを設定することで、画像効果を調整することができます。

マニュアルモードでは、**露出時間**、**ゲイン**、**スローシャッター**を設定する必要があります。

フォーカス

フォーカスモードを調整するオプションがあります。

フォーカスモード

オート

シーンの変化に応じて、自動的にピントを合わせます。オートモードでピントが合わない場合は、画像内の光源を減らし、点滅する光源を避けてください。

セミオート

PTZおよびレンズズーム後、一度フォーカスを合わせます。画像が鮮明であれば、シーンが変わってもフォーカスは変化しません。

手動

ライブビュー画面で手動でフォーカスを調整できます。

デイ&ナイト切り替え

デイ＆ナイト切り替え機能により、昼と夜でカラー画像と白黒画像を切り替えることができます。切り替えモードは設定可能です。

昼

画像は常にカラーで表示されます。

ナイト

画像は白黒またはカラーで、夜間は補助照明が点灯して鮮明なライブビュー画像を確保します。

注意

一部の機種のみ、補光機能とカラフルな画像に対応しています。

自動

カメラは、環境の光量に応じて、デイモードとナイトモードを切り替えます。

スケジュール切り替え

開始時間と**終了時間を**設定して、昼間モードの継続時間を定義します。

アラーム入力によるトリガー

トリガー状態を「**デイ**」または「**ナイト**」に設定できます。たとえば、**トリガー状態が「ナイト」**の場合、デバイスがアラーム入力信号を受信すると、モードは「**ナイト**」に切り替わります。

ビデオによってトリガー

カメラは、環境の光量に応じてデイモードとナイトモードに切り替わります。このモードは、道路交通および車両検出に対応しているデバイスに適用できます。

注意

- デイ&ナイト切り替え機能は、モデルによって異なります。
- より良い画像効果を得るために、スマート補光機能をオンにすることができます。補光設定については、*「補光設定」*を参照してください。

補助ライト設定

補助ライトを設定できます。関連するパラメーターは実際のデバイスをご確認ください。

スマート補光機能

スマート補光機能は、補光ライトが点灯しているときに露出オーバーを防ぐ。

サプリメントライトモード

デバイスがサプリメントライトに対応している場合、サプリメントライトモードを選択できます。

赤外線サプリメントライト

赤外線ライトが有効になっています。

白色光

白色光が有効になります。

混合光

IR ライトと白色光の両方が有効になっています。

スマート

特定のスマートイベントまたは動体検知を有効にした後にこのモードを選択すると、夜間状態では、デフォルトの補光モードは IR 補光モードになります。アラームが作動すると、白色光が有効になり、デバイスがターゲットを撮影します。アラームが終了すると、補光モードは IR 補光モードに切り替わります。

この機能は、IR および白色光、または IR および白色光のハイブリッド補助光を備えたデバイスモデルでのみサポートされています。

オフ

補助光はオフです。

注意

補助光モードは、デバイスモデルによって異なる場合があります。

明るさ調整モード オート

実際の環境に応じて、明るさが自動的に調整されます。

手動

スライダーをドラッグするか、値を設定して明るさを調整できます。

BLC

強い逆光の中で被写体にピントを合わせると、被写体が暗すぎてはっきりと見えなくなります。BLC（逆光補正）は、手前の被写体に当たる光を補正して、被写体をはっきりと映し出します。BLC モード**をカスタムに設定すると**、ライブビュー画像上に BLC 領域として赤い四角形を描画することができます。

WDR

WDR（ワイドダイナミックレンジ）機能は、照度の差が大きい環境でも鮮明な画像を提供する機能です。

視野内に非常に明るい部分と非常に暗い部分が同時に存在する場合は、WDR 機能を有効にしてレベルを設定することができます。WDR は、画像全体の明るさのレベルを自動的に調整し、より詳細で鮮明な画像を提供します。

注意

WDR を有効にすると、一部の機能が使用できなくなる場合があります。詳細については、実際のインターフェースを参照してください。

図4-1 WDR

HLC

画像の明るい部分が露出過度、暗い部分が露出不足の場合、HLC (High Light Compression) 機能を有効にして、明るい部分を弱め、暗い部分を明るくして、画像全体の明るさのバランスを調整することができます。

ホワイトバランス

ホワイトバランスは、カメラの白色再現機能です。環境に応じて色温度を調整するために使用します。

図4-2 ホワイトバランス

DNR

デジタルノイズリダクションは、画像のノイズを低減し、画質を向上させるために使用されます。**ノーマル**と**エキスパート**モードが選択可能です。

標準

DNR レベルを設定して、ノイズの低減度を制御します。レベルが高いほど、低減度が高くなります。

エキスパート

空間 DNR と時間 DNR の両方の DNR レベルを設定して、ノイズ低減の程度を制御します。レベルが高いほど、低減の程度が強くなります。

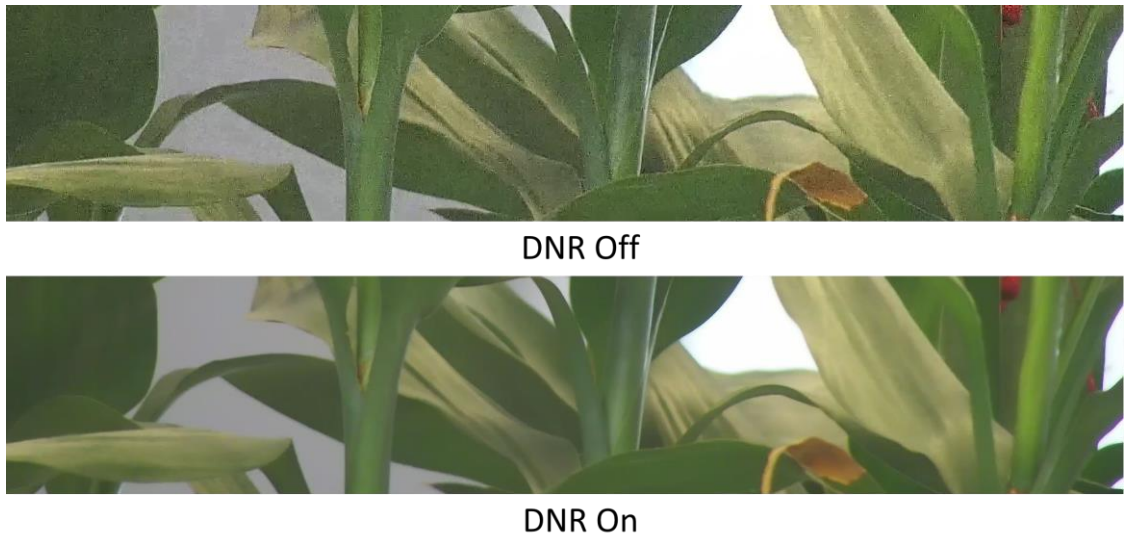

図4-3 DNR

デフォグ

環境が霧で覆われ、画像がぼやけている場合に、デフォグ機能を有効にすることができます。微妙なディテールを強調して、画像をより鮮明に表示します。

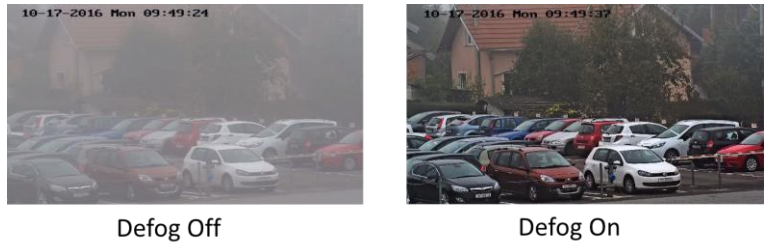

図4-4 除霧

EIS

ジッター補正技術により、ビデオ画像の安定性を高めます。

グレースケール

グレースケールの範囲を[0-255]または[16-235]から選択できます。

ミラー

ライブビュー画像が実際のシーンと逆になっている場合、この機能を使用すると画像を正常に表示することができます。

必要に応じてミラーモードを選択してください。

注意
この機能を有効にすると、ビデオ録画が一時的に中断されます。

回転

この機能を有効にすると、ライブビューが反時計回りに 90°回転します。たとえば、1280 × 720 は 720 × 1280 に回転します。
この機能を有効にすると、垂直方向の監視範囲が変更される場合があります。

注意
この機能は、特定の設定下でサポートされています。

レンズの歪み補正

電動レンズを搭載した機器では、画像に多少の歪みが生じる場合があります。この機能を有効にすると、歪みを補正することができます。

注意
- この機能は、電動レンズを搭載した一部のデバイスでのみサポートされています。
- この機能を有効にすると、画像の端が失われます。

4.7.2 画像パラメーターの切り替え

設定した時間ごとに、画像パラメーターを自動的に切り替えます。

画像パラメーターの切り替え設定ページに移動します：**設定→ 画像→ 表示設定→ 画像パラメーターの切り替え**、必要に応じてパラメーターを設定します。

スケジュール切り替えを設定

一定時間ごとに、リンクされたシーンモードに画像を自動的に切り替えます。

手順

1. **スケジュール切り替えに**チェックを入れます。
2. 対応する時間期間とリンクされたシーンモードを選択し、設定します。

注意

リンクされたシーンの設定については、***シーンモード***を参照してください。

3. **保存**をクリックします。

4.7.3 ビデオ規格

ビデオ規格は、表示される色の数および解像度を定義する、ビデオカードまたはビデオ表示デバイスの機能です。最も一般的な 2 つのビデオ規格は、NTSC および PAL です。NTSC では、1 秒間に 30 フレームが送信されます。各フレームは 525 個の個別の走査線で構成されています。PAL では、1 秒間に 25 フレームが送信されます。各フレームは 625 個の個別の走査線で構成されています。お住まいの国/地域のビデオシステムに応じて、ビデオ信号規格を選択してください。

4.7.4 ローカルビデオ出力

BNC、CVBS、HDMI、SDI などのビデオ出力インターフェースが搭載されているデバイスでは、デバイスをモニター画面に接続することで、ライブ画像を直接プレビューすることができます。

出力モードをON/OFFに設定して出力を制御します。

4.8 OSD

ビデオストリームに表示されるデバイス名、日時、フォント、カラー、テキストオーバーレイなどの OSD (オンスクリーンディスプレイ) 情報をカスタマイズできます。

OSD 設定ページに移動します：**設定→ 画像→ OSD 設定**。対応するパラメータを設定し、[**保存**] をクリックして有効にします。

文字セット

表示する情報用の文字セットを選択します。画面に韓国語を表示する必要がある場合は**EUC-KR**を選択し、それ以外の場合は**GBK**を選択します。

表示

カメラ名、日付、曜日、およびそれらの表示形式を設定します。

フォーマット設定

表示モード、**OSDサイズ**、**フォントカラー**、**配置など**、OSDパラメータを設定します。

テキストオーバーレイ

画像にカスタマイズしたオーバーレイテキストを設定します。

4.9 プライバシーマスクの設定

この機能は、ライブビューの特定の領域をブロックしてプライバシーを保護します。デバイスがどのように移動しても、ブロックされたシーンは決して見えません。

手順

1. **設定→ 画像→ プライバシーマスク**
2. **「有効」**にチェック**を入れます**。
3. 「 」をクリックします。ライブビュー上でマウスをドラッグして閉じた領域を
   描画します。**領域の角をドラッグします**。 領域のサイズを調整します。
   領域をドラッグします 領域の位置を調整します。
   「 」**をクリックします**。設定したすべての領域をクリアします。
4. **[追加]** をクリックしてプライバシーマスクを追加し、**[地域名]** および **[マスクの種類]** を設定します。
5. **「保存」**をクリックします。

4.10 画像の重ね合わせ

ライブビューにカスタマイズした画像をオーバーレイします。

開始前に

オーバーレイする画像はBMP形式で24ビットであり、最大画像サイズは128 × 128ピクセルです。

手順

1. **設定→ 画像→ 画像オーバーレイ**。
2. **「有効」**にチェック**を入れます**。
3. **「アップロード」**をクリックして画像を選択し、開きます。
   赤い四角形が表示された画像は、アップロードが正常に完了するとライブビューに表示されます。
4. 赤い四角形をドラッグして画像の位置を調整してください。
5. **保存**をクリックします。

第 5 章 ビデオ録画と画像キャプチャ

このパートでは、ビデオクリップやスナップショットの撮影、再生、および撮影したファイルのダウンロードの操作について説明します。

5.1 ストレージ設定

このセクションでは、いくつかの一般的なストレージパス設定について説明します。

5.1.1 メモリカード

メモリカードの容量、空き容量、ステータス、タイプ、およびプロパティを表示できます。データのセキュリティを確保するため、メモリカードの暗号化に対応しています。

新しいまたは暗号化されていないメモリカードを設定する

開始前に
デバイスに新しいまたは暗号化されていないメモリカードを挿入します。詳細なインストール手順は、デバイスの *クイックスタートガイド* を参照してください。

手順

1. Go to **Configuration→ Storage→ Storage Management→ HDD Management** .
2. メモリカードを選択します。

   注意
   「**アンロック**」ボタンが表示された場合は、まずメモリカードをアンロックする必要があります。詳細については *「メモリカードの状態」を確認する* を参照してください。
3. **「フォーマット」**をクリックして、メモリカードを初期化してください。
   メモリカードのステータスが「**未初期化**」から「**正常**」に変わると、メモリカードが使用可能になります。
4. **オプション：** メモリカードを暗号化します。
   1) **「暗号化フォーマット」**をクリックします。
   2) 暗号化パスワードを設定します。
   3) **「OK」**をクリックします。
      暗号化ステータスが「暗号化済み」に変わると、メモリカードは使用可能になります。

   注意
   暗号化パスワードを適切に管理してください。暗号化パスワードを忘れた場合、復元できません。
5. **オプション：** メモリカードの**容量制限**を設定します。必要に応じて、さまざまなコンテンツの保存容量をパーセンテージで入力します。

6. **保存**をクリックしてください。

暗号化メモリカードの設定

開始前に

- 暗号化されたメモリカードをデバイスに挿入してください。詳細なインストール手順は、デバイスの*クイックスタートガイド*を参照してください。
- メモリカードの正しい暗号化パスワードを確認してください。

手順

1. Go to **Configuration→ Storage→ Storage Management→ HDD Management** .

2. メモリカードを選択してください。

注意

アンロックボタンが表示された場合は、まずメモリカードをアンロックする必要があります。詳細については*「メモリカードのステータスを確認する」*を参照してください。

3. 暗号化パスワードを確認してください。

1) **パリティ**をクリックします。

2) 暗号化パスワードを入力してください。

3) **OK**をクリックしてください。

暗号化ステータスが「暗号化済み」に変わると、メモリカードが使用可能になります。

注意

暗号化パスワードを忘れた場合でも、このメモリカードを使用したい場合は、*「メモリカードを設定するか暗号化を解除する」新しい*を選択し、メモリカードをフォーマットして設定し直してください。すべての既存のデータが削除されます。

4. **オプション：**メモリカードの**クォータ**を定義します。必要に応じて、さまざまなコンテンツの保存割合をパーセンテージで入力します。

5. **保存**をクリックしてください。

メモリカードの状態を検出

デバイスはHikvisionメモリカードのステータスを検出します。メモリカードに異常が検出された場合、通知が表示されます。

開始前に

設定ページは、デバイスにHikvisionメモリカードが挿入されている場合のみ表示されます。

手順

1. **[Configuration] (設定)**に移動します。**→ (メモリカード)→ (メモリカード)Storage Management (メモリカード管理)→ Memory Card Detection (メモリカード検出)**

2. **「ステータス検出」**をクリックして、メモリカードの**残存寿命**と**健康状態**を確認します。

残存寿命

メモリカードの残寿命の割合が表示されます。メモリカードの寿命は、その容量やビットレートなどの要因によって影響を受ける場合があります。残寿命が十分でない場合は、メモリカードを交換する必要があります。

健康状態

メモリーカードの動作状況が表示されます。**アラーム**スケジュールと**リンク方法が**設定されている場合、動作状況が正常でない場合は通知されます。

注意

健康状態が「良好」でない場合は、メモリカードを交換することをおすすめします。

3. **R/W ロック**をクリックして、メモリカードへの読み書きの権限を設定します。
   - ロックを追加
     a. **ロックスイッチを**オンに設定します。
     b. パスワードを入力してください。
     c. **「保存」**をクリックしてください。
   - ロック解除
     - メモリカードをロックしたデバイスで使用すると、自動的にロックが解除されるため、ユーザーによるロック解除の手順は必要ありません。
     - ロックされたメモリカードを別のデバイスで使用する場合は、**HDD 管理で**メモリカードの手動ロック解除を行うことができます。メモリカードを選択し、**[ロック解除]** をクリックします。正しいパスワードを入力してロックを解除します。
   - ロックを解除する
     a. **ロックスイッチを**OFFに設定します。
     b. **パスワード設定**でパスワードを入力します。
     c. **「保存」**をクリックします。

注意

- **R/W ロック**を設定できるのは管理者ユーザーのみです。
- メモリカードはロックが解除されている場合のみ、読み書きが可能です。
- メモリカードにロックを追加するデバイスが工場出荷時の設定に復元された場合、**HDD 管理で**メモリカードのロックを解除することができます。

4. **武装スケジュール**と**リンク方法を**設定します。詳細については、*「」を武装の設定*スケジュールと*リンク方法*参照してください。
5. **保存**をクリックします。

5.1.2 FTPを設定します。

イベントまたはタイマースナップショットタスクによって撮影された画像を保存する FTP サーバーを設定できます。

開始前に

まず、FTPサーバーのアドレスを取得してください。

手順

1. **設定→ イベント→ アラーム設定→ FTP** .
2. FTP 設定を構成します。

   サーバーアドレスとポート

   FTP サーバーのアドレスと対応するポート。

   ユーザー名とパスワード

   FTP ユーザーは画像のアップロード権限が必要です。

   FTP サーバーが匿名ユーザーによる画像のアップロードをサポートしている場合、**匿名ユーザー**にチェックを付けることで、アップロード時にデバイス情報を非表示にできます。

   ディレクトリ構造

   FTPサーバー内のスナップショットの保存パスです。
3. **オプション：[Upload Picture]** をチェックすると、FTP サーバーにスナップショットをアップロードできるようになります。

   画像保存間隔

   画像管理を効率化するため、画像の保存間隔を1日から30日まで設定できます。同じ保存間隔で撮影された画像は、その間隔の開始日と終了日をファイル名にしたフォルダーに保存されます。

   画像名

   キャプチャされた画像の命名規則を設定します。ドロップダウンリストから**「デフォルト」**を選択すると、デフォルトの規則が使用されます。デフォルトの規則は、IPアドレス_チャンネル番号_キャプチャ時間_イベントタイプ.jpg（例：10.11.37.189_01_20150917094425492_FACE_DETECTION.jpg）です。または、デフォルトの命名規則に**カスタムプレフィックス**を追加してカスタマイズできます。
4. **オプション：「自動ネットワーク補充を有効にする」**にチェックを入れます。

   注

   リンク方法」で「**FTP/メモリカード/NAS にアップロード**」が選択されている場合、「**ネットワークの自動補充を有効にする**」も同時に有効にする必要があります。
5. **テスト**をクリックしてFTPサーバーを確認してください。
6. **「保存」**をクリックしてください。

5.1.3 NASを設定

記録ファイル、キャプチャした画像などを保存するネットワークディスクとして、ネットワークサーバーを使用します。

開始前に

まず、ネットワークディスクの IP アドレスを取得します。

手順

1. NAS の設定ページに移動します。**→ Storage→ Storage Management→ Net HDD** .
2. **「追加」**をクリックします。
3. **マウントタイプ**を設定します。

マウントタイプ

オペレーティングシステムに応じて、ファイルシステムプロトコルを選択します。

SMB/CIFS を選択した場合は、セキュリティを確保するために、ネット HDD のユーザー名とパスワードを入力してください。

4. **サーバーアドレス**と**ファイルパスを**設定してください。

サーバーアドレス

ネットワークディスクの IP アドレス。

ファイルパス

ネットワークディスクファイルの保存パス。

5. **テスト**をクリックして、ネットワークディスクが使用可能かどうかを確認します。

6. **[OK]** をクリックして、Net HDD の追加手順を完了します。

7. **オプション：**Net HDD を設定します。

編集 「」をクリックしてパラメーター設定を編集します。

削除 ネットHDDを削除します。

- 「」をクリックします。
- ネット HDD を選択し、**削除**をクリックします。

8. **保存**をクリックします。

5.1.4 eMMC 保護

eMMCの健康状態が不良の場合、自動的にeMMCをストレージメディアとして使用を停止します。

注意

eMMC 保護は、eMMC ハードウェアを搭載した特定のデバイスモデルでのみサポートされています。

設定を行うには、**[Configuration]、[→]、[System]、[→]、[System Service]** の順に選択します。**→**

eMMC は、組み込み型マルチメディアカードの略で、組み込み型の不揮発性メモリシステムです。このデバイスは、デバイスのキャプチャした画像やビデオを保存することができます。

デバイスはeMMCの健康状態を監視し、状態が不良の場合にeMMCをオフにします。そうでない場合、摩耗したeMMCを使用すると、デバイスの起動失敗を引き起こす可能性があります。

5.1.5 クラウドストレージの設定

キャプチャした画像とデータをクラウドにアップロードするのに役立ちます。プラットフォームは、画像の表示と分析のためにクラウドから直接画像を取得します。この機能は、特定のモデルでのみサポートされています。

手順

注意
クラウドストレージが有効になっている場合、写真はまずクラウドビデオマネージャーに保存されます。

1. **[Configuration] (設定)** に移動し、**[→] (ストレージ)** を選択します。**→(ストレージ管理) を選択し、[→] (クラウドストレージ)**
2. **「有効」**にチェック**を入れます**。
3. 基本パラメーターを設定します。

プロトコルバージョン	クラウドビデオマネージャーのプロトコルバージョン。
サーバー IP	クラウドビデオマネージャーの IP アドレス。IPv4 アドレスに対応しています。
サービスポート	クラウドビデオマネージャーのポート。デフォルトのポートを使用することをお勧めします。
アクセスキー	クラウドビデオマネージャーにログインするためのキー。
シークレットキー	クラウドビデオマネージャーに保存されているデータを暗号化するためのキー。
ユーザー名とパスワード	クラウドビデオマネージャーのユーザー名とパスワード。
画像ストレージプール ID	クラウドビデオマネージャー内の画像保存領域の ID です。ストレージプール ID と保存領域 ID が同じであることを確認してください。

4. **テスト**をクリックして設定を確認します。
5. **「保存」**をクリックします。

5.2 ビデオ録画

このセクションでは、手動とスケジュールされた録画、再生、および録画したファイルのダウンロードの操作について説明します。

5.2.1 自動録画

この機能では、設定した期間にビデオを自動的に録画することができます。

開始前に
連続記録を除く各記録タイプのイベント設定で、**トリガー記録**を選択します。詳細については、「*イベントとアラーム*」を参照してください。

手順

1. Go to **Configuration→ Storage→ Schedule Settings→ Record Schedule** .
2. **「有効」**にチェック**を入れます**。
3. 記録タイプを選択します。

注意

記録タイプはモデルによって異なります。

連続

スケジュールに従ってビデオが連続的に録画されます。

モーション

動体検知が有効で、リンク方法がトリガー録画に設定されている場合、対象物の動きが録画されます。

アラーム

アラーム入力が有効で、リンク方法がトリガー録画に設定されている場合、外部アラーム入力デバイスからアラーム信号を受信すると、ビデオが録画されます。

モーション| アラーム

外部アラーム入力デバイスから動体検知またはアラーム信号を受信すると、ビデオが録画されます。

モーション＆アラーム

外部アラーム入力デバイスから動体検知およびアラーム信号を受信した場合にのみビデオが録画されます。

イベント

設定されたイベントが検出されると、ビデオが録画されます。

4. 選択した記録タイプのスケジュールを設定します。設定操作については*「アラームスケジュール設定」*を参照してください。

5. 高度な録画パラメーターを設定します。

上書き

上書きを有効にすると、ストレージ容量がいっぱいになったときにビデオ記録が上書きされます。この設定を無効にすると、カメラは新しいビデオを録画できません。

事前録画

スケジュールされた時間前に録画を開始する時間範囲を設定します。

後録画

スケジュールされた時間後に録画を停止する時間期間を設定します。

ストリームタイプ

録画するストリームの種類を選択します。

注

ビットレートが高いストリームタイプを選択した場合、事前録画と事後録画の実際の時間は設定値より短くなる場合があります。

録画の有効期限

記録は、有効期限を過ぎると削除されます。有効期限は設定可能です。注意：記録が削除されると、復元することはできません。

6. **保存**をクリックしてください。

5.2.2 手動で記録

手順

1. **[設定]** の **[→] [ローカル]** に移動します。
2. 録画ビデオファイルのビデオサイズと**ビデオ保存パスを**設定します。
3. **保存**をクリックします。
4. ライブビューインターフェースで「 」をクリックして録画を開始します。「 」をクリックして録画を停止します。

次にやるべきこと

録画したビデオファイルを表示します。
「設定」→ 「ローカル」に移動し、**「ビデオの保存パス」**の**「開く」**をクリックして保存パスを開き、ファイルを表示します。

5.2.3 ビデオの再生とダウンロード

ローカルストレージまたはネットワークストレージに保存されているビデオを検索、再生、クリップ、ダウンロードすることができます。

手順

1. **再生→ ビデオ** へ移動します。
2. 検索条件を設定し、**[検索]** をクリックします。

   一致したビデオファイルがタイミングバーに表示されます。
3. クリック をクリックしてビデオファイルを再生します。
   - クリック を押して、ビデオファイルを全画面で再生します。**ESC** を押して、全画面表示を終了します。
   - クリック をクリックして、すべてのチャンネルのビデオ再生を停止します。
4. **オプション：** をクリックして、ビデオファイルをクリップします。 をもう一度クリックすると、ビデオファイルのクリップが停止します。

   注意

   [設定] の **[→] [ローカル] [→] [クリップの保存先]** に移動し、クリップしたビデオファイルの保存先を表示および変更します。
5. オプション： 再生インターフェースで、ファイルをダウンロードします。

   注意

   設定→ ローカル→ ダウンロードしたファイルの保存先、ダウンロードしたビデオファイルの保存先を表示および変更します。

5.3 キャプチャ設定

デバイスは手動または自動で画像をキャプチャし、設定された保存パスに保存できます。スナップショットを表示してダウンロードできます。

5.3.1 自動キャプチャ

この機能は、設定された時間間隔で自動的に画像をキャプチャします。

開始前に
イベントによるキャプチャが必要な場合は、イベント設定で関連するリンク方法を設定する必要があります。イベントの設定については、*「イベントとアラーム」*を参照してください。

手順

1. Go to **Configuration→ Storage→ Schedule Settings→ Picture Capture** .
2. キャプチャ スケジュールを設定します。スケジュール時間を設定するには、[***Arming スケジュールを設定***] を参照してください。

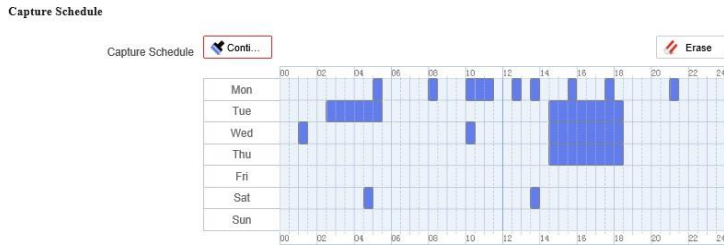

図5-1 キャプチャスケジュールの設定

3. キャプチャの種類を設定します。
   スケジュール
   設定された時間間隔で画像をキャプチャします。
   イベント
   イベントがトリガーされたときに画像をキャプチャします。
4. **フォーマット**、**解像度**、**品質**、**間隔**、および**キャプチャ数を**設定します。

注意
キャプチャした画像の解像度は、キャプチャした画像ストリームの解像度と同じになります。**ストリームタイプは**、**[詳細設定]** で選択できます。

5. **保存**をクリックします。

5.3.2 手動でキャプチャ

手順

1. **設定→ ローカル**に移動します。

2. **画像形式**と保存先をスナップショット用に設定します。

JPEG

この形式の画像サイズは比較的小さく、ネットワークでの送信に適しています。

BMP

画像は高品質で圧縮されます。

3. **保存**をクリックします。
4. ライブビューまたは再生ウィンドウの近くにある「 」をクリックして、手動で写真を撮影します。

5.3.3 画像の表示とダウンロード

ローカルストレージまたはネットワークストレージに保存されている画像を検索、表示、ダウンロードすることができます。

手順

1. Go to **Playback→ Picture**.
2. 検索条件を設定し、**[検索]** をクリックします。

一致した画像がファイル一覧に表示されます。

3. 画像を保存します。
   - 画像を選択し、**ダウンロード**をクリックしてダウンロードします。
   - **「このページをダウンロード」**をクリックして、このページの写真をダウンロードしてください。
   - **「すべてをダウンロード」**をクリックすると、すべての画像をダウンロードできます。

注意

設定→ ローカル→ 再生キャプチャ保存先再生時にキャプチャした画像の保存先を表示、変更します。

第 6 章 イベントとアラーム

この部分では、イベントの設定について紹介します。デバイスは、アラームがトリガーされると特定の応答を行います。一部のデバイスモデルでは、特定のイベントがサポートされていない場合があります。

6.1 動体検知の設定

検出領域内の移動物体を検出し、リンク動作をトリガするのに役立ちます。

手順

1. **[Configuration]** に移動し、**[→] を選択します**。**[Event] を選択し、[→] を選択します**。**[Event and Detection] を選択し**、**[→]**

2. **「有効」**にチェック**を入れます**。

3. **オプション：**画像内の移動オブジェクトを緑色で表示するには、この項目を強調表示します。

1) **「モーション用の動的分析を有効にする」**にチェックを入れます。

2) **[設定]** の **[→] [ローカル]** に移動します。

3) **ルールを有効**に設定します。

4. **設定で**モードを選択し、ルール領域とルールパラメーターを設定します。

- 通常モードに関する情報は、***通常モード***をご覧ください。
- エキスパートモードに関する情報は、***エキスパートモード***をご覧ください。

5. 武装スケジュールとリンク方法を設定します。武装スケジュールの設定については、***「武装スケジュールの設定」***を参照してください。リンク方法については、***「リンク方法の設定」を***参照してください。

6. **保存**をクリックします。

6.1.1 エキスパートモード

実際のニーズに応じて、昼と夜で異なる動体検知パラメータを設定することができます。

手順

1. **設定で「エキスパートモード」**を選択します。

2. エキスパートモードのパラメーターを設定します。

スケジュール画像設定 OFF

画像切り替えは無効になります。

自動切り替え

環境に応じて、デイ&ナイトモードを自動的に切り替えます。昼間はカラー画像、夜間は白黒画像で表示します。

スケジュール切り替え

スケジュールに従ってデイ＆ナイトモードを切り替えます。設定した時間帯はデイモード、それ以外の時間帯はナイトモードに切り替わります。

感度

感度が高いほど、動体検知の感度が高くなります。スケジュール画像設定が有効になっている場合は、昼と夜の感度を個別に設定することができます。

3. **エリア**を選択し、[ ] をクリックします。ライブ画像上でマウスをクリックしてドラッグし、マウスを離すと 1 つのエリアの描画が完了します。

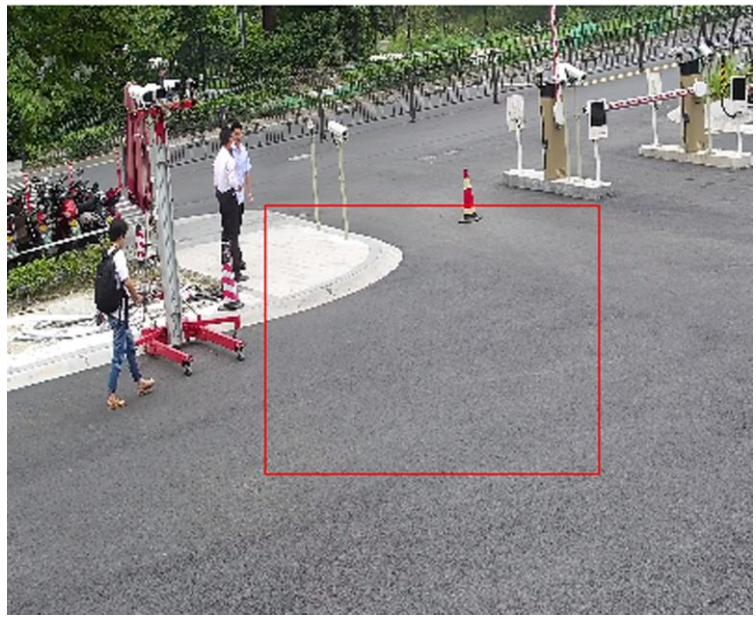

図6-1 ルール設定

4. 「 」をクリックして、すべての領域をクリアします。
5. **「Save」**をクリックします。
6. **オプション：**上記の手順を繰り返して、複数のエリアを設定します。

6.1.2 通常モード

デバイスのデフォルトパラメータに従って、動体検知のパラメータを設定できます。

手順

1. **設定で「通常モード」**を選択します。
2. 通常モードの**感度**を設定します。感度の値が高いほど、動体検知の感度が高くなります。感度を ***0*** に設定すると、動体検知および動的分析は機能しません。
3. **検出対象**を設定します。人間と車両から選択できます。検出対象を選択しない場合、人間と車両を含む、検出されたすべての対象が報告されます。この機能により、指定した対象タイプ（人間と車両）によってアラームを鳴らすことができます。

注意

この機能は、一部の機種、設定でご利用いただけません。実際の設定をご確認ください。

4. クリック をクリックします。ライブ画像上でマウスをクリックしてドラッグし、マウスを右クリックして 1 つの領域の描画を終了します。
5. **オプション：** [ ] をクリックすると、すべての領域がクリアされます。
6. **オプション：** 上記の手順を繰り返して、複数の領域のパラメータを設定することができます。

6.2 ビデオ改ざんアラームの設定

設定されたエリアが覆われ、正常に監視できなくなった場合、アラームが作動し、デバイスは特定のアラーム対応措置を講じます。

手順

1. **[Configuration]** (設定) に移動し、**[→] (イベント)** を選択します。**[→] (イベントと検出) を選択し、[→] (ビデオ改ざん)** を選択します。
2. **「有効」** にチェック**を入れます**。
3. **感度**を設定します。値が高いほど、エリアの覆いを検出するのが容易になります。
4. 「 」をクリックし、ライブビューでマウスをドラッグして領域を指定します。

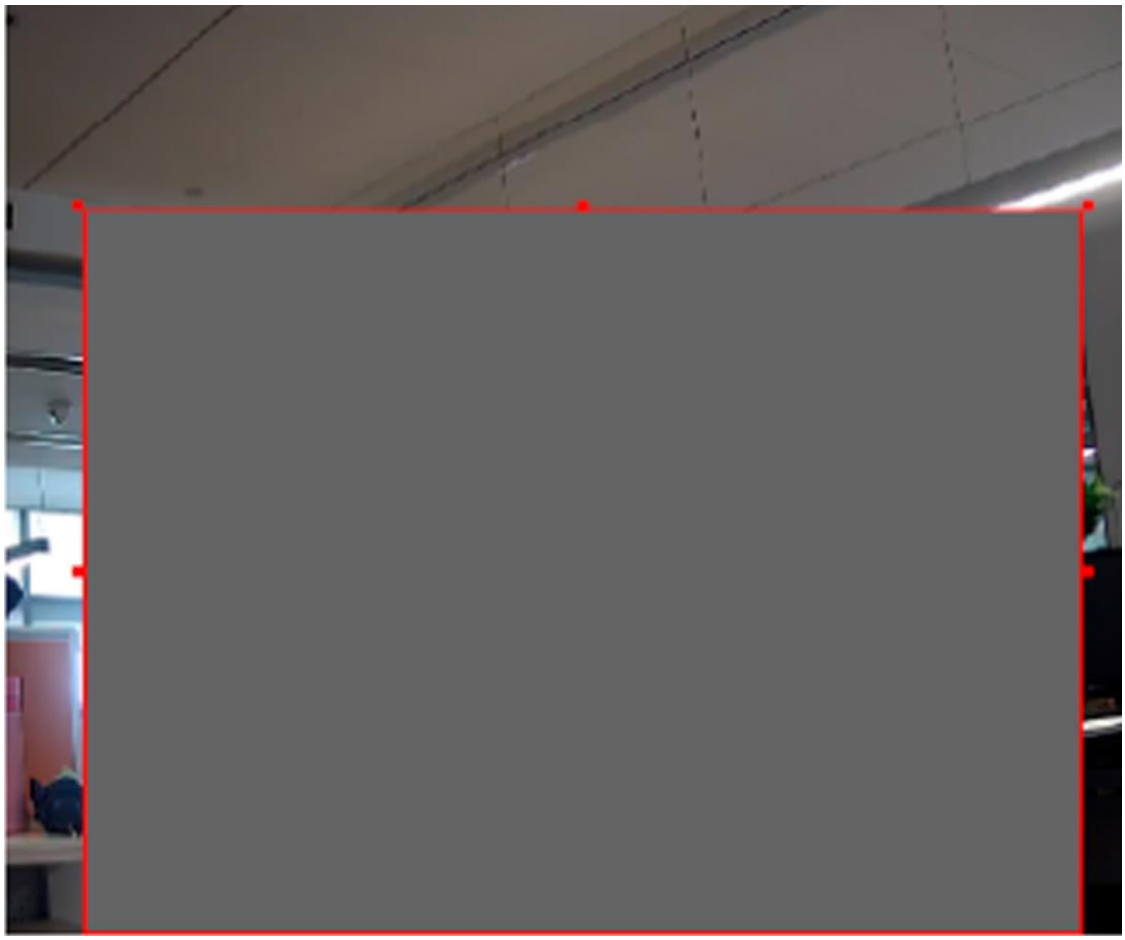

図 6-2 ビデオ改ざん領域の設定

5. オプション：[ ]をクリックして、描画した領域をすべて削除します。
6. ***スケジュール設定アラーム設定***は「」を参照してください。***リンク方法の設定は「***リンク方法の設定」を参照してください。
7. 保存をクリックしてください。

6.3 アラーム入力の設定

外部デバイスからのアラーム信号により、現在のデバイスの対応する動作がトリガーされます。

開始前に

注意
この機能は、特定のモデルでのみサポートされています。

外部アラームデバイスが接続されていることを確認してください。ケーブルの接続については、*クイックスタートガイド*を参照してください。

手順

1. **設定→ イベント→ イベントと検出→ アラーム入力**
2. **アラーム入力 NO.** を選択し、[ ] をクリックしてアラーム入力を設定します。
3. ドロップダウンリストから**アラームタイプ**を選択します。**アラーム名を**編集します。
4. **アラーム入力処理を有効にする」**にチェックを入れます。
5. ***スケジュールアラーム設定***設定については、「」を参照してください。***リンク方法「」***の設定については、リンク方法の設定を参照してください。
6. **コピー先...** をクリックして、他のアラーム入力チャンネルに設定をコピーします。
7. **「保存」**をクリックします。

6.4 例外アラームの設定

ネットワーク切断などの例外が発生すると、デバイスが対応する動作を実行します。

手順

1. **[設定]** の **[→] [イベント] [→] [イベントと検出] [→] [例外]** に移動します。
2. **例外の種類**を選択してください。**HDDが満杯です**

   HDDのストレージが満杯です。

   HDDエラー

   HDD でエラーが発生しました。**ネットワークが切断されています**。デバイスがオフラインです。

   IPアドレスの衝突

   現在のデバイスの IP アドレスが、ネットワーク内の他のデバイスの IP アドレスと重複しています。

   不正なログイン

   ユーザー名またはパスワードが正しくないため、ログインできません。
3. リンク方法の設定については、「リンク方法***の設定」***を参照してください。
4. **保存**をクリックしてください。

6.5 ビデオ画質診断の設定

デバイスのビデオ画質に異常があり、アラームのリンク方法が設定されている場合、アラームが自動的に作動します。

手順

1. **→[Configuration]** (設定) に移動し、**[→] (ビデオ品質) を選択します。[→] (イベント) を選択し、[Event and Detection] (イベントと検出) を選択します。**
2. **診断タイプ**を選択します。
3. 対応するパラメーターを設定します。

   アラーム検出間隔

例外を検出する時間間隔。

感度

値が高いほど、例外が検出されやすくなりますが、誤報の発生可能性も高まります。

アラーム遅延時間

アラームが設定回数に達すると、デバイスはアラームをアップロードします。

4. 選択した診断タイプを確認し、関連するタイプが検出されます。
5. アラーム設定スケジュールを設定します。***アラーム設定スケジュールを設定***してください。
6. リンク方法を設定します。***リンク方法の設定***を参照してください。
7. **保存**をクリックします。

注意

この機能は一部のモデルでのみサポートされています。実際の表示はモデルによって異なります。

6.6 オーディオ例外検出を設定する

オーディオ異常検出機能は、音量の急激な増減など、シーン内の異常な音を検出し、それに応じて特定のアクションを実行することができます。

手順

1. **設定→イベント→イベントと検出→オーディオ例外検出**。
2. 1つまたは複数のオーディオ異常検出タイプを選択します。

オーディオ損失検出

オーディオトラックの突然の損失を検出します。

音量急上昇検出

音の強度が急激に増加したのを検出します。**感度**と**音の強度閾値は**設定可能です。

注

- 感度が低いほど、検出をトリガーする変化の大きさが大きくなる必要があります。
- 音量閾値とは、検出の基準となる音量を指します。環境の平均音量に設定することをお勧めします。環境音が大きいほど、この値を大きくしてください。実際の環境に応じて調整してください。

音圧の急激な低下検出

音圧の急激な低下を検出します。**感度は**設定可能です。

3. スケジュール設定については、「***アラーム設定***」を参照してください。リンク方法の設定については、「リンク方法の設定」を参照してください。
4. **保存**をクリックします。

注意

この機能は一部のモデルのみに対応しています。実際の機能はモデルによって異なります。

6.7 ボケ検出の設定

レンズのピントがずれて画像がぼやけることを検出します。検出すると、リンク動作を行います。

手順

1. **設定**に移動します**。→ イベント→ イベントおよび検出→ ピントの合っていない検出**。
2. **「有効」**にチェック**を入れます**。
3. **感度**を設定します。値が高いほど、デフォーカス画像がアラームをトリガーしやすくなります。実際の環境に応じて、値を調整してください。
4. リンク方法の設定については、「*リンク方法の設定」*を参照してください。
5. **保存**をクリックします。

注意

この機能は、一部のモデルでのみ対応しています。実際の表示はモデルによって異なります。

6.8 シーン変更検知の設定

シーン変更検知機能は、シーンの変化を検知します。アラームが作動すると、特定の動作を実行することができます。

手順

1. **設定→ イベント→ イベントと検知→ シーン変更検知**に移動します。
2. **「有効」**をクリックします。
3. **感度**を設定します。値が高いほど、シーンの変化を検知しやすくなります。ただし、検知精度は低下します。
4. *スケジュールアラーム設定*設定については、「」を参照してください。*リンク方法「」*の設定については、リンク方法の設定を参照してください。
5. **「保存」**をクリックします。

注

この機能は一部のモデルでのみ対応しています。実際の表示はモデルによって異なります。

第 7 章 警報スケジュールとアラームのリンク方法

アラームスケジュールは、デバイスが特定のタスクを実行するカスタマイズされた期間です。アラームリンクは、スケジュールされた時間中に検出された特定のインシデントまたはターゲットに対する応答です。

7.1 武装スケジュールを設定する

デバイスタスクの有効時間を設定します。

手順

1. **オプション：**関連するイベントインターフェースで「**武装スケジュール」および「リンク方法」**をクリックします。
2. **「武装スケジュール」**の横にある**「編集」**をクリックします。
3. **「描画」**をクリックし、時間バーをドラッグして希望の有効時間を描画します。

注意

- 各セルは30分を表します。
- 描画した期間の上にマウスを置くと、その期間の詳細が表示され、開始時間と終了時間を微調整することができます。
- 1 日に最大 8 つの期間を設定できます。

4. **「消去」**をクリックし、時間バーをドラッグして選択した有効な時間をクリアします。
5. 設定を保存するには**「OK」**をクリックしてください。

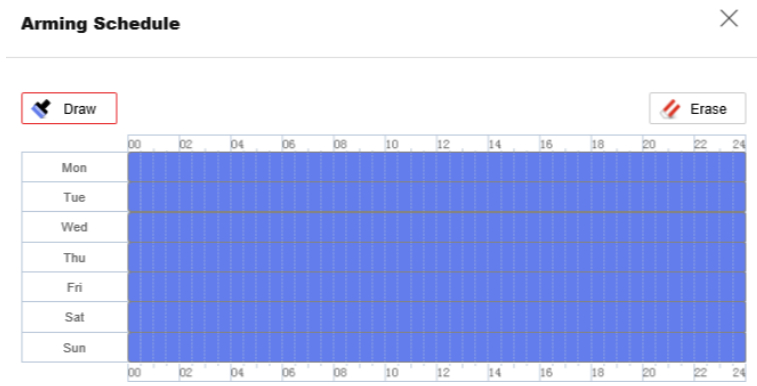

図7-1 警報スケジュール設定

7.2 リンク方法の設定

イベントやアラーム発生時にリンク機能を有効にすることができます。

7.2.1 アラーム出力のトリガー

アラーム出力デバイスが接続され、アラーム出力 No. が設定されている場合、アラームが発生すると、接続されたアラーム出力デバイスにアラーム情報を送信します。

手順

1. 設定→ イベント→ アラーム設定→ アラーム出力 .

2. アラーム出力パラメータを設定します。

自動アラーム 設定については、*「自動アラーム」*を参照してください。

手動アラーム 設定については、「*手動アラーム」*を参照してください。

手動アラーム

アラーム出力は手動でトリガーすることができます。

開始前に

アラーム出力デバイスがデバイスに接続されていることを確認してください。

手順

1. 外部アラームデバイスに接続されているアラームインターフェースに応じて、**アラーム出力 No.** を選択します。 をクリックして、アラームパラメータを設定します。

アラーム名

アラーム出力の名前をカスタマイズします。

2. 手動アラームをクリックして、手動アラーム出力を有効にします。

3. オプション：手動アラーム出力を無効にするには、**[アラームのクリア]** をクリックします。

自動アラーム

自動アラームのパラメータを設定すると、デバイスは設定されたアラームスケジュールに従って自動的にアラーム出力をトリガーします。

開始前に

アラーム出力デバイスがデバイスに接続されていることを確認してください。

手順

1. 外部アラームデバイスに接続されているアラームインターフェースに応じて、**アラーム出力 No.** を選択します。 をクリックして、アラームパラメータを設定します。

アラーム名

アラーム出力の名前をカスタマイズします。

遅延

アラームが発生してからアラーム出力が残る時間です。

2. アラームのスケジュールを設定します。設定の詳細については、*「アラームのスケジュールを設定する」*を参照してください。

3. **オプション：「コピー先...」**をクリックして、パラメータを他のアラーム出力チャンネルにコピーします。

4. **「保存」**をクリックします。

7.2.2 FTP/NAS/メモリカードへのアップロード

FTP/NAS/メモリカードへのアップロードを有効にして設定している場合、アラームがトリガーされると、デバイスはアラーム情報を FTP サーバー、ネットワーク接続ストレージ、およびメモリカードに送信します。

FTPサーバーの設定については「***FTPの設定***」を参照してください。***NASの設定***については「NASの設定」を参照してください。

メモリカードの保存設定については、「***新しいメモリカードまたは暗号化されていないを設定***メモリカード」を参照してください。

7.2.3 メールを送信

[E メールを送信] をチェックすると、アラームイベントが検出されたときに、指定したアドレスにアラーム情報が記載された E メールが送信されます。

メール設定については、「***メールの設定」*** を参照してください。

メール設定

E メール設定を行い、リンク方法として「**E メールを送信**」を有効にすると、アラームイベントが検出された場合に、指定したすべての宛先に E メール通知が送信されます。

開始前に

Eメール機能を使用する前に、DNSサーバーを設定してください。Go → **Configuration →→ Network →→ Network Settings → TCP/IP** でDNS設定を行います。

手順

1. メール設定ページに移動します：**設定→ イベント→ アラーム設定→ メール**。

2. メールパラメーターを設定します。

1) 送信者のメール情報を入力します。**送信者アドレス**、**SMTP サーバー**、および **SMTP ポートを入力します**。

2) **オプション：** メールサーバーが認証を必要とする場合は、**[認証]** をチェックし、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を入力します。

3) **メールの暗号化**を設定します。

- **TLS**を選択し、STARTTLSを無効にすると、メールはTLSで暗号化されて送信されます。SMTPポートは465に設定する必要があります。
- **TLS**を選択し、**STARTTLSを有効**にすると、メールはSTARTTLSで暗号化されて送信されます。**SMTPポートは** 25 に設定する必要があります。

注意

STARTTLS を使用する場合は、お使いのメールサーバーがプロトコルに対応していることを確認してください。お使いのメールサーバーがプロトコルに対応していない状態で [**STARTTLS を有効にする**] をチェックすると、メールは暗号化されずに送信されます。

4) **オプション：** アラーム画像付きの通知を受け取りたい場合は、**[画像添付]** をチェックします。通知メールには、設定可能な画像撮影間隔で、イベントに関する一定数のアラーム画像が添付されます。

注意

アラーム画像の数は、デバイスの機種やイベントによって異なります。

5) 受信者の情報（受信者の名前と住所を含む）を入力してください。

6) **テスト**をクリックして、機能が正しく設定されているか確認してください。

3. **「保存」**をクリックしてください。

7.2.4 監視センターへの通知

監視センターに通知] をチェックすると、アラームイベントが検出されると、アラーム情報が監視センターにアップロードされます。

7.2.5 トリガー録画

トリガー録画」にチェックを入れると、デバイスは、検出されたアラームイベントに関するビデオを録画します。録画の設定については、*「ビデオ録画と写真撮影*」を参照してください。

7.2.6 フラッシュライト

「ライトの点滅」を有効にし、「**ライトの点滅アラーム出力」**を設定すると、アラームイベントが検出されるとライトが点滅します。

点滅アラームライト出力の設定

イベントが発生すると、アラームとしてデバイスの点滅ライトを点滅させることができます。

手順

1. **設定**に移動します。**→ イベント→ アラーム設定→ 点滅アラームライト出力**。

2. 点滅時間と**点滅頻度**を設定します。**点滅時間**

1 つのアラームが発生したときの点滅の持続時間。

点滅頻度

ライトが点滅する頻度。高頻度、中頻度、低頻度、および通常点灯が選択可能です。

3. アラームのスケジュールを設定します。詳細については*「アラームスケジュール設定」を*参照してください。
4. **保存**をクリックします。

注意

一部のデバイスモデルのみが機能に対応しています。

7.2.7 音声アラーム

可聴警告を有効にし、**可聴アラーム出力を設定すると**、アラームが発生したときに、デバイスの内蔵スピーカーまたは接続された外部スピーカーから警告音が鳴ります。

可聴アラーム出力の設定については、*「可聴アラーム出力の設定」*を参照してください。

注意

この機能は、一部のカメラモデルでのみサポートされています。

可聴アラーム出力の設定

デバイスが検出エリアでターゲットを検出すると、警告として可聴アラームを鳴らすことができます。

手順

1. **設定→ イベント→ アラーム設定→ 可聴アラーム出力**.
2. **サウンドの種類**を選択し、関連するパラメーターを設定します。
   - **「プロンプト」**を選択し、必要なアラーム時間を設定します。
   - 警告とその内容を選択します。必要なアラーム時間を設定します。
   - **カスタムオーディオ**を選択します。ドロップダウンリストからカスタムオーディオファイルを選択できます。ファイルがない場合は、**[→ を追加]** をクリックして、要件を満たすオーディオファイルをアップロードできます。最大 3 つのオーディオファイルをアップロードできます。
3. **オプション：[テスト]** をクリックして、選択したオーディオファイルをデバイスで再生します。
4. 可聴アラームの武装スケジュールを設定します。詳細については、*「武装スケジュールの設定」*を参照してください。
5. **「保存」**をクリックします。

注

この機能は、特定のデバイスモデルでのみサポートされています。

7.2.8 アラームサーバー

デバイスは、HTTP、HTTPS、または ISUP プロトコルを介して、宛先 IP アドレスまたはホスト名にアラームを送信できます。宛先 IP アドレスまたはホスト名は、HTTP、HTTP、または ISUP データ送信をサポートしている必要があります。

アラームサーバーの設定

手順

1. **設定**」に移動します**。→ イベント→ アラーム設定→ アラームサーバー**。
2. **宛先IPまたはホスト名**、**URL**、および**ポート**を入力します。
3. **プロトコル**を選択します。

注意

HTTP、HTTPS、およびISUPが選択可能です。通信中のデータ送信を暗号化するため、HTTPSの使用が推奨されます。

4. **「テスト」**をクリックして、IPまたはホストが利用可能かどうかを確認してください。
5. **「保存」**をクリックします。

第 8 章 ネットワーク設定

8.1 TCP/IP

ネットワーク経由でデバイスを操作するには、TCP/IP 設定を正しく設定する必要があります。IPv4 および IPv6 の両方がサポートされています。両方のバージョンは、互いに競合することなく同時に設定できます。

Go to **Configuration→ Network→ Network Settings→ TCP/IP** for parameter settings.

NIC タイプ

ネットワーク環境に応じて、NIC（ネットワークインターフェースカード）のタイプを選択してください。

IPv4

IPv4には2つのモードが利用可能です。

DHCP

DHCP をチェックすると、デバイスはネットワークから IPv4 パラメータを自動的に取得します。この機能を有効にすると、デバイスの IP アドレスが変更されます。SADP を使用して、デバイスの IP アドレスを取得することができます。

注意

デバイスが接続されているネットワークは、DHCP (Dynamic Host Configuration Protocol) をサポートしている必要があります。

手動

デバイスのIPv4パラメーターを手動で設定できます。**IPv4アドレス**、**IPv4サブネットマスク**を入力してください。

IPv4 デフォルトゲートウェイを入力し、**[テスト]** をクリックして IP アドレスが利用可能かどうかを確認します。

IPv6

3つのIPv6モードが利用可能です。

ルート広告

IPv6アドレスは、ルート広告とデバイスのMACアドレスを組み合わせることで生成されます。

注

ルート広告モードは、デバイスが接続されているルーターのサポートが必要です。

DHCP

IPv6アドレスは、サーバー、ルーター、またはゲートウェイによって割り当てられます。

手動

IPv6 アドレス、**IPv6 サブネット**、**IPv6 デフォルトゲートウェイ**を入力します。必要な情報については、ネットワーク管理者にお問い合わせください。

MTU

最大伝送単位の略です。単一のネットワーク層トランザクションで通信できる最大のプロトコルデータ単位のサイズです。

MTUの有効な値の範囲は1280から1500です。

DNS

ドメインネームサーバーの略称です。ドメイン名でデバイスにアクセスする必要がある場合、または一部のアプリケーション（例：メール送信）で使用されるため必要です。必要に応じて、**優先DNS**サーバーと**代替DNSサーバー**を適切に設定してください。

ドメイン名設定

[動的ドメイン名を有効にする] をチェックし、**[ドメイン名を登録]** を入力します。デバイスは、ローカルエリアネットワーク内での管理を容易にするため、登録ドメイン名の下に登録されます。

注意

ダイナミック ドメイン名が有効になるには、**DHCP を**有効にする必要があります。

8.2 ドメイン名経由でのデバイスへのアクセス

ネットワークアクセスには、ダイナミック DNS (DDNS) を使用できます。デバイスのダイナミック IP アドレスをドメイン名解決サーバーにマッピングすることで、ドメイン名によるネットワークアクセスを実現できます。

デバイスのDDNSサービスはHTTPSのみをサポートしています。

開始前に

DDNSサーバーへの登録は、デバイスのDDNS設定を行う前に必要です。

手順

1. ***TCP/IP 設定***を参照して DNS パラメーターを設定してください。
2. DDNS 設定ページに移動します：**設定→ ネットワーク→ ネットワーク設定→ DDNS**。
3. 「**有効**」にチェックを入れ、**DDNS タイプ**を選択します。**DynDNS**

   ダイナミック DNS サーバーは、ドメイン名の解決に使用されます。

   NO-IP

   NO-IP サーバーは、ドメイン名解決に使用されます。
4. ドメイン名情報を入力し、**保存**をクリックします。
5. デバイスのポートを確認し、ポートマッピングを完了してください。ポートマッピングの設定については、***「ポートマッピング」***を参照してください。
6. デバイスにアクセスしてください。

   ブラウザを使用して　　ブラウザのアドレスバーにドメイン名を入力してデバイスにアクセスします。

クライアントソフトウェアを使用する場合　　クライアントソフトウェアにドメイン名を追加します。具体的な追加方法については、クライアントのマニュアルを参照してください。

8.3 PPPoE ダイヤルアップ接続によるデバイスへのアクセス

このデバイスは、PPPoE 自動ダイヤルアップ機能をサポートしています。デバイスは、モデムに接続されると、ADSL ダイヤルアップによってパブリック IP アドレスを取得します。デバイスの PPPoE パラメータを設定する必要があります。

手順

1. **[Configuration]** (設定)**→ [Network] (ネットワーク)→ [Network Settings] (ネットワーク設定)→ [PPPoE]** (PPPoE)
2. **「有効」**にチェック**を入れます**。
3. PPPoE パラメーターを設定します。

   動的IP

   ダイヤルアップに成功すると、WAN の動的 IP アドレスが表示されます。

   ユーザー名

   ダイヤルアップネットワークアクセス用のユーザー名。

   パスワード

   ダイヤルアップネットワークアクセス用のパスワード。

   確認

   ダイヤルアップパスワードをもう一度入力します。
4. **保存**をクリックしてください。
5. デバイスにアクセスしてください。

   ブラウザを使用して　　ブラウザのアドレスバーにWANの動的IPアドレスを入力してデバイスにアクセスしてください。

   クライアントソフトウェアを使用する場合　　クライアントソフトウェアに WAN 動的 IP アドレスを追加します。詳細については、クライアントのマニュアルを参照してください。

注意

取得した IP アドレスは PPPoE によって動的に割り当てられるため、カメラを再起動すると IP アドレスは常に変更されます。動的 IP の不便さを解消するには、DDNS プロバイダ（DynDns.com など）からドメイン名を取得する必要があります。詳細については、「*ドメイン名によるデバイスへのアクセス*」を参照してください。

8.4 SNMP

ネットワーク管理でデバイス情報を取得するために、SNMP（Simple Network Management Protocol）を設定することができます。

開始前に
SNMPを設定する前に、SNMPソフトウェアをダウンロードし、SNMPポート経由でデバイス情報を取得できるように設定する必要があります。

手順

1. **[Configuration]** (**設定**) に移動し、[→] (**ネットワーク**) をクリックします。→ (**ネットワーク設定**) をクリックし、[→] (**SNMP**) をクリックします
2. **SNMPv1 を有効にする**、**SNMP v2c を有効にする**、または **SNMPv3 を有効にする**を選択します。

   注意

   選択するSNMPバージョンは、SNMPソフトウェアのバージョンと一致する必要があります。
   また、必要なセキュリティレベルに応じて、異なるバージョンを使用する必要があります。SNMP v1 はセキュリティが脆弱であり、SNMP v2 ではアクセスにパスワードが必要です。SNMP v3 は暗号化機能を備えており、このバージョンを使用する場合は、HTTPS プロトコルを有効にする必要があります。
3. SNMP設定を構成します。
4. **保存**をクリックします。

8.5 IEEE 802.1Xを設定します。

IEEE 802.1Xを設定することで、接続されたデバイスのユーザー権限を認証できます。

[Configuration]、**[→]**、**[Network]**、**[→]**、[**Network Settings**]、**[→]**、**[802.1X]** の順に選択し、この機能を有効にします。
ルーターの情報に応じて、プロトコルとバージョンを選択してください。サーバーのユーザー名とパスワードが必要です。

注意

- **プロトコルを EAP-TLS** に設定する場合は、**クライアント**証明書と **CA 証明書**を選択してください。
- 機能が正常に動作しない場合は、**証明書管理**で選択した証明書が正常かどうかを確認してください。

8.6 QoSを設定

QoS（Quality of Service）は、データ送信の優先順位を設定することで、ネットワークの遅延やネットワークの混雑を改善することができます。

注意

QoS は、ルーターやスイッチなどのネットワークデバイスによるサポートが必要です。

手順

1. [**Configuration**]、**[→]**、**[Network]**、**[→]**、**[Network Settings]**、**[→]**、**[QoS]** の順に選択します。
2. **ビデオ/オーディオ DSCP**、**イベント/アラーム DSCP**、および**管理 DSCP** を設定します。

注意

ネットワークは、データ伝送の優先順位を識別することができます。DSCP 値が大きいほど、優先順位が高くなります。設定時には、ルーターでも同じ値を設定する必要があります。

3. **保存**をクリックします。

8.7 HTTP(S)

HTTP は、ハイパーメディア文書を伝送するためのアプリケーション層プロトコルです。HTTPS は、暗号化伝送と ID 認証を可能にするネットワークプロトコルで、リモートアクセスのセキュリティを向上させます。

手順

1. **[Configuration]** に移動します。**→ [Network]→ [Network Service]→ HTTP(S)** .

2. **HTTP ポート**を入力します。

注

これは、ブラウザがデバイスにアクセスする際に使用するポートを指します。例えば、

HTTP ポートを 81 に変更した場合、ログインするにはブラウザに http://192.168.1.64:81 と入力する必要があります。

3. **HTTPS** で「**有効**」を選択してください。

注

デバイスがサポートするTLSバージョンを設定するには、**TLS設定**をクリックしてください。詳細については、を参照してください。

4. **HTTPS ポート**を入力してください。

5. **オプション：**HTTPSプロトコル経由でのみデバイスにアクセスするには、[HTTPS **ブラウジング]** をチェックします。

6. **サーバー証明書**を選択します。

7. **Web認証**を設定します。**認証**

DigestとDigest/Basicがサポートされています。これは、WEBリクエストがデバイスに送信される際に認証情報が必要であることを意味します。**Digest/Basic**を選択した場合、デバイスはDigestまたはBasic認証をサポートしています。**Digest**を選択した場合、デバイスはDigest認証のみをサポートします。

ダイジェストアルゴリズム

MD5、SHA256、およびMD5/SHA256暗号化アルゴリズムをWEB認証で使用します。MD5を除くダイジェストアルゴリズムを有効にすると、互換性の問題により、サードパーティプラットフォームがデバイスにログインしたり、ライブビューを有効にしたりできなくなる可能性があります。高強度の暗号化アルゴリズムの使用が推奨されます。

8. **保存**をクリックしてください。

8.8 マルチキャスト

マルチキャストは、複数の宛先デバイスに同時にデータ送信を行うグループ通信です。

設定→ ネットワーク→ ネットワークサービス→ マルチキャストでマルチキャストの設定を行います。

IPアドレス

これはマルチキャストホストのアドレスを表します。

8.8.1 マルチキャスト検出

設定→ ネットワーク→ ネットワーク設定→ TCP/IP を選択して、この機能を有効にします。

マルチキャスト検出を有効にする] をチェックすると、オンラインネットワークカメラは、LAN 内のプライベートマルチキャストプロトコルを介してクライアントソフトウェアによって自動的に検出されます。

8.9 RTSP

RTSP (Real Time Streaming Protocol) は、ストリーミングメディア用のアプリケーション層制御プロトコルです。

手順

1. **設定→ ネットワーク→ ネットワークサービス→ RTSP** へ移動します。
2. **ポート**を入力します。
3. **マルチキャスト**パラメーターを設定します。

   ストリームタイプ

   マルチキャストソースとしてのストリームタイプ。

   ビデオポート

   選択したストリームのビデオポート。

   オーディオポート

   選択したストリームのオーディオポート。
4. **RTSP認証**を設定します。**認証**

   ダイジェストとダイジェスト/ベーシックがサポートされています。これは、RTSPリクエストがデバイスに送信される際に認証情報が必要であることを意味します。**ダイジェスト/ベーシック**を選択した場合、デバイスはダイジェストまたはベーシック認証をサポートしています。**ダイジェスト**を選択した場合、デバイスはダイジェスト認証のみをサポートしています。

   ダイジェストアルゴリズム

   RTSP認証でMD5、SHA256、およびMD5/SHA256暗号化アルゴリズムが使用されます。MD5を除くダイジェストアルゴリズムを有効にした場合、サードパーティプラットフォームがログインできない可能性があります。

デバイスまたはライブビューを有効にできない場合があります。互換性の問題のためです。高強度の暗号化アルゴリズムの使用が推奨されます。

5. **保存**をクリックしてください。

8.10 SRTPを設定

Secure Real-time Transport Protocol (SRTP) は、ユニキャストおよびマルチキャストアプリケーションの両方で RTP データに暗号化、メッセージ認証、整合性、および再生攻撃保護を提供することを目的とした、リアルタイムトランスポートプロトコル (RTP) インターネットプロトコルです。

手順

1. [**Configuration**]、**[→]**、**[Network]**、**[→]**、**[Network Service]**、**[→]**、**[SRTP]** の順に選択します。

2. **ポート**番号を入力します。

3. **マルチキャスト**パラメーターを設定します。

ストリームタイプ

マルチキャストソースとしてのストリームタイプ。

ビデオポート

選択したストリームのビデオポート。

オーディオポート

選択したストリームのオーディオポート。

4. **サーバー証明書**を選択してください。

5. **暗号化アルゴリズム**を選択してください。

6. **保存**をクリックします。

注

- この機能は、特定のデバイスモデルのみに対応しています。
- 機能が正常に動作しない場合は、***証明書管理***で選択した証明書が正常かどうかを確認してください。

8.11 Bonjour

サービス検出、アドレス割り当て、ホスト名解決などの技術群であるゼロコンフィグレーションネットワーク（zeroconf）の実装です。Bonjour は、マルチキャストドメインネームシステム（mDNS）サービスレコードを使用して、ローカルネットワーク上のプリンタ、他のコンピュータ、およびそれらのデバイスが提供するサービスを検出します。

設定→ ネットワーク→ ネットワークサービス→ Bonjour を選択して機能を有効にし、[保存] をクリックします。

保存をクリックします。

この機能を有効にすると、デバイスはローカルエリアネットワーク内でサービス情報を送信および受信します。

8.12 WebSocket(s)

Google Chrome 57 以降、または Mozilla Firefox 52 以降を使用してデバイスにアクセスする場合は、WebSocket または WebSockets プロトコルを有効にする必要があります。そうしないと、ライブビュー、画像キャプチャ、デジタルズームなどが使用できません。

設定→ ネットワーク→ ネットワークサービス→ WebSocket(s) でパラメータを設定し、[保存] をクリックします。
保存をクリック
します。

WebSocket

TCP ベースの全二重通信プロトコルポートで、HTTP プロトコルによるプラグイン不要のプレビュー用です。

WebSockets

HTTPS プロトコルによるプラグイン不要のプレビュー用 TCP ベースの全二重通信プロトコルポート。

8.13 ポートマッピング

ポートマッピングを設定することで、指定したポート経由でデバイスにアクセスできます。

手順

1. Go to **設定→ ネットワーク→ ネットワークサービス→ NAT** .
2. ポートマッピングモードを選択します。

   自動ポートマッピング　　詳細な情報は「*自動ポートマッピングの設定*」を参照してください。

   手動ポートマッピング　　詳細情報は「*手動ポートマッピングの設定*」を参照してください。
3. **保存**をクリックします。

8.13.1 自動ポートマッピングの設定

手順

1. **[UPnP™ を有効にする]** をチェックし、カメラにわかりやすい名前を選択します。または、デフォルト名を使用することもできます。
2. ポートマッピングモードを「**自動**」に設定します。
3. **保存**をクリックします。

注

ルーターのUPnP™機能は同時に有効に設定する必要があります。

8.13.2 手動ポートマッピングを設定

手順

1. **UPnP™の有効化**を確認し、デバイスにわかりやすい名前を指定するか、デフォルトの名前を使用できます。

2. ポートマッピングモードを「**手動**」に設定し、外部ポートを内部ポートと同じに設定します。
3. 「**保存**」をクリックします。

次に実行する操作
ルーターのポートマッピング設定インターフェースに移動し、ポート番号と IP アドレスをデバイスと同じに設定します。詳細については、ルーターのユーザーマニュアルを参照してください。

8.13.3 ルーターでのポートマッピングの設定

以下の設定は特定のルーターを対象としています。ルーターのモデルによって設定内容が異なります。

手順

1. **WAN接続タイプ**を選択します。
2. ルーターの **IP アドレス**、**サブネットマスク**、その他のネットワークパラメータを設定します。
3. Go to **Forwarding→ Virtual Severs** 、そして **Port Number** と **IP Address** を入力します。
4. **保存**をクリックしてください。

例
カメラが同じルーターに接続されている場合、あるカメラのポートを IP アドレス 192.168.1.23、ポート番号 80、8000、554 に設定し、別のカメラのポートを IP アドレス 192.168.1.23、ポート番号 81、8001、555 に設定することができます。
8201に設定できます。

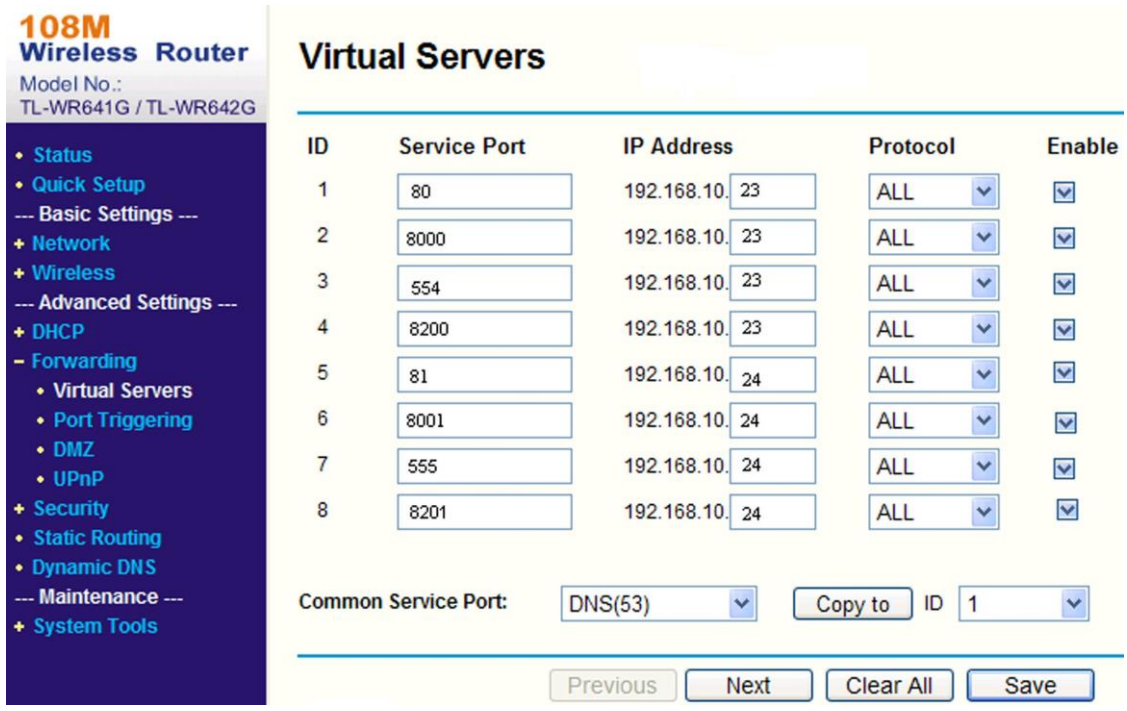

図8-1 ルーターでのポートマッピング

注意

ネットワークカメラのポートは、他のポートと競合してはなりません。たとえば、ルーターのウェブ管理ポートの一部は 80 です。カメラポートが管理ポートと同じ場合は、カメラポートを変更してください。

8.14 RTCP

このデバイスは、RTCP (Real-time Transport Control Protocol) を使用してパケットを順番に配信し、信頼性の高い配信メカニズムと、フロー制御や輻輳制御のためのサービスを提供しています。

[Configuration]、**[→]**、**[Network]**、**[→]**、[**Network Service**]、**[→]**、[**RTCP]** の順に選択し、**[Enable]** をオンにして機能を有効にします。

8.15 ワイヤレスダイヤル

オーディオ、ビデオ、および画像のデータを 3G/4G ワイヤレスネットワーク経由で転送できます。

注意

この機能は、特定のデバイスモデルでのみサポートされています。

8.15.1 ワイヤレスダイヤルを設定

内蔵のワイヤレスモジュールにより、デバイスからインターネットにダイヤルアップアクセスできます。

開始する前に

SIMカードを入手し、3G/4Gサービスをアクティベートしてください。SIMカードを対応するスロットに挿入してください。

手順

1. **設定→ ネットワーク→ ネットワーク設定→ ワイヤレスダイヤル** .
2. 機能の有効化を確認してください。
3. **ダイヤルパラメータ**に移動して、パラメータを設定し、保存します。
4. **ダイヤルプランの**横**の設定**をクリックします。詳細情報は「*アラームスケジュール設定*」を参照してください。
5. **ダイヤル状態を**表示します。

リフレッシュをクリックします。 ダイヤル状態をリフレッシュします。

切断をクリックします。 3G/4G ワイヤレスネットワークを切断します。

ダイヤル状態が「接続中」に変わると、ダイヤルが正常に接続されたことを意味します。

6. ネットワーク内のコンピュータの **IP アドレス**からデバイスにアクセスします。

- ブラウザにIPアドレスを入力してデバイスにアクセスしてください。
- クライアントアプリケーションにデバイスを追加します。**IP/ドメイン**を選択し、IP アドレスおよびその他のパラメータを入力して、デバイスにアクセスします。

7. **オプション：**4G SIM カード情報とネットワークキャリア情報を表示することができます。

注意

一部のデバイスモデルで**パフォーマンスモード**または**プロアクティブモードが**有効になっている場合、ワイヤレスモードをアップグレードできます。必要に応じて、専門家の指導に従ってワイヤレスモードをアップグレードしてください。

8. **オプション：[再キャンプ]** をクリックして、デバイスをワイヤレスネットワークに手動で再接続します。デバイスは 10 秒間機内モードを維持した後、自動的にネットワークに接続します。

9. **オプション：[有効]** をチェックして **[自動再キャンプ]** を有効にし、**[再キャンプ間隔]** を設定します。デバイスは、設定された**再キャンプ間隔で**自動的にワイヤレスネットワークに再接続します。

注意

機能はデバイスモデルによって異なる場合があります。

8.15.2 ワイヤレスエキスパート設定

ワイヤレスの専門家向け設定では、デバイスが接続する 3G/4G ワイヤレスネットワークの詳細情報を確認でき、専門家がネットワークの問題をトラブルシューティングするのに役立ちます。

セル無線周波数パラメーター

セル無線周波数パラメータは、デバイスが接続している現在のワイヤレスネットワークに関する情報を提供します。

[設定]→ [ネットワーク]→ [ネットワーク設定]→ [ワイヤレスダイヤル]→ [エキスパート設定] を選択して、セルの無線周波数パラメータを表示します。

ネットワーク情報

現在の携帯電話ネットワーク情報が表示されます。**[更新]** をクリックすると、さまざまなセルの周波数情報を表示できます。

無線周波数変動

過去 7 日間にデバイスが接続した携帯電話ネットワークの変動を記録します。**「レポートのエクスポート」**をクリックし、暗号化パスワードを設定して確認すると、変動レポートがエクスポートされます。

バンドロック

デバイスのデータ転送速度を高速化する一連のバンドをロックして、ネットワークの速度を向上させることができます。

手順

1. **設定→ ネットワーク→ ネットワーク設定→ ワイヤレスダイヤル→ エキスパート設定→ バンドのロック** .

2. **「有効」**にチェック**を入れます**。

3. 「追加」をクリックし、バンドを入力します。

注意

- 入力するバンド番号は、B（+）番号またはN（+）番号のいずれかです。例えば、B1またはN1を入力できます。
- 最大 5 つのバンドがサポートされています。

4. **オプション：** をクリックして、選択したバンドを削除します。**Clear All** をクリックして、リストをすべて消去することもできます。

ベースバンドパケットのキャプチャ

この機能は、プロトコル相互作用パケットをキャプチャして、4G モジュールと基地局間の通信障害の特定に役立ちます。

手順

注意

この機能は、専門家および技術サポートスタッフ専用です。

1. [Configuration] (構成) [→] (ネットワーク) [→] (ネットワーク設定) [→] (ワイヤレスダイヤル) [→] (エキスパート設定) に移動します。
2. [キャプチャベースバンドパケット] の後ろにある [設定] をクリックして、設定インターフェースに入ります。
3. 「有効」にチェックを入れてこの機能を有効にします。
4. キャプチャ 期間と保存パスを設定します。保存パスはデバイスの実際の保存方法に依存します。**このパス下のキャプチャ パケットを**削除するには、[**このパス**下のキャプチャ パケットを削除] をクリックします。
5. 「保存」をクリックします。
6. 「パケットのキャプチャを開始」をクリックして、ベースバンド パケットのキャプチャを開始します。
7. **オプション：** [キャプチャの停止] をクリックして、キャプチャプロセスを停止します。
8. キャプチャが完了したら、[キャプチャしたパケットをエクスポート] をクリックしてレポートを保存します。

速度テスト

手順

1. [Configuration] (設定) に移動し、[→] (ネットワーク) をクリックします。→ (ネットワーク) をクリックし、[→] (ワイヤレス設定) をクリックします。→ (ワイヤレスダイヤル)
2. **速度テストの**背後にある**設定**をクリックして、設定インターフェースに入ります。
3. デフォルトのサーバーを選択するか、サーバーアドレスを入力します。以下の手順に従って、近くのサーバーアドレスを取得できます。

注意

以下の手順に従って、近くのサーバーアドレスを取得できます。

a. 以下のウェブサイトにアクセスして、近くのサーバーのアドレスを取得してください：
https://www.speedtest.net/speedtest- servers-static.php.

b. 近くの速度測定ステーションのURLを選択してコピーし、**サーバーアドレス**に貼り付けます。

4. **「速度テスト」**をクリックしてテストを開始します。
   テストが完了すると、速度の詳細を確認できます。また、**「速度テスト結果のエクスポート」**をクリックすることもできます。

8.16 WLAN AP（アクセスポイント）

このデバイスはWLAN AP機能を使用して無線アクセスポイントとして使用できます。スマートフォンやPCをデバイスのAPに接続することで、スマートフォンやPCからデバイスにアクセスし、パラメーターを設定できます。

注意

この機能は、特定のデバイスモデルでのみサポートされています。

8.16.1 WLAN APを設定する

手順

1. **[Configuration]** (設定) に移動し、**[→] (ワイヤレス) を選択します。→ (ネットワーク) を選択します。→ (ワイヤレス AP)** を選択します。
2. WLAN AP モードを選択します。

   オン

   機能は有効です。

   メンテナンスモード

   デバイスが冷間起動（デバイスのスイッチを**ON**に切り替える）後、WLAN AP機能は自動的に5分間有効になります。その後、デバイスの4G通信が正常な場合はWLAN AP機能がオフになり、4G通信が異常な場合はオンのままになります。

   オフ

   機能は無効です。
3. 関連するパラメーターを設定してください。

   SSID

   一部のデバイスモデルでは、デバイスのデフォルトSSIDは「Hik-シリアル番号」という名前で設定されています。

   一部のデバイスモデルでは、デバイスのデフォルトSSIDはデバイスラベルに「Default SSID」と表示されます。

   必要に応じて設定できます。

   セキュリティモード

   WPA2-個人モードがサポートされています。

   暗号化方式

   AESと**TKIP**が選択可能です。

   パスワード

デバイス AP 経由のワイヤレス接続用のパスワードです。デフォルトのパスワードは、カメラの 9 桁のシリアル番号です。初回ログイン後に、デフォルトのパスワードを変更し、強固なパスワードを設定してください。

注意

製品のセキュリティを強化するため、お客様ご自身で強力なパスワード（大文字、小文字、数字、特殊文字を含む 8 文字以上）を設定することを強くお勧めします。また、特にセキュリティの高いシステムでは、パスワードを定期的にリセットすることをお勧めします。パスワードを毎月または毎週リセットすることで、製品をより確実に保護することができます。

4. **保存**をクリックしてください。

注意

機能はデバイスモデルによって異なる場合があります。

次にやるべきこと

モバイルフォンまたはPCをAPに接続できます。

8.16.2 AP経由でのデバイスへのアクセス

デバイスがネットワークに接続できない場合は、デバイスの AP 経由でデバイスにアクセスできます。

手順

1. **[Configuration]** (設定)**→ [Network] (ネットワーク)→ [Network Settings] (ネットワーク設定)→ [WLAN AP] (**WLAN AP**)** をオンにして、WLAN AP 機能を有効にします。一部のデバイスモデルでは、デバイスのコールド起動 **(**デバイスのスイッチを **ON** にすること**)** 後、WLAN AP 機能は 5 分間自動的にオンになり、その後、デバイスの 4G 通信が正常であれば WLAN AP 機能はオフになり、デバイスの 4G 通信が異常であれば WLAN AP 機能はオンのままになります。
機能は、デバイスの4G通信が正常な場合はオフになり、4G通信が異常な場合はオンのままになります。

2. スマートフォンまたはPCのWLANリストでデバイスのWLAN APを検索します。

3. パスワードを入力し、スマートフォンまたはPCをAPに接続します。

注意

- APの名はSSID（デフォルトは「Hik-シリアル番号」）です。パスワードはデフォルトでシリアル番号です。シリアル番号は、**設定→ システム→ システム設定から**取得できます。

  →基本情報。

- 一部のデバイスモデルでは、APの名はデバイスのラベルに表示されている「Default SSID」です。

4. ブラウザにIPアドレスを入力してください。

注意

デバイスのAPのデフォルトIPは192.168.8.1です。

結果

接続されたデバイスが**「接続デバイス」**インターフェースに表示されます。

8.17 トラフィックシェーピング

トラフィックシェーピングは、送信前にビデオデータパケットを整形および平滑化するために使用されます。

これは、ネットワークの輻輳による遅延やパケット損失を改善し、ビデオの品質を確保するのに役立ちます。シェーピングのレベルは設定可能です。

8.18 データ監視

デバイスが使用する SIM カードデータまたは有線ネットワークデータを表示および管理できます。SIM カードデータは、ネットワークキャリアが提供するデータサービスです。有線ネットワークデータは、通常 4G ルーターを介して提供されます。

手順

1. **[Configuration] (構成)** に移動します。**→ (ネットワーク)→ (ネットワーク設定)→ (データモニタリング)** を選択します。
2. **「有効」**にチェックを**入れます**。
3. データプランに応じて、以下のパラメーターを設定します。

   プランタイプ

   日次、**月次**、または**年次**から選択できます。

   データプラン

   使用可能なデータ量を入力し、単位を選択してください。

   アラーム閾値

   使用データ量がデータプランの設定割合に達すると、デバイスはアラームメッセージを送信し、OSD またはポップアップウィンドウに通知を表示します。
4. **リンク方法を「通常」**から選択します。

   「E メール送信」または**「監視センターに通知」**が選択されている場合、使用データがしきい値に達すると、デバイスは E メールまたは監視センターにアラームメッセージを送信します。
5. **保存**をクリックします。

注意

機能はデバイスモデルによって異なります。

8.19 Wi-Fi

Wi-Fi パラメータを設定して、デバイスをワイヤレスネットワークに接続します。

注意

この機能は、一部のデバイスモデルでのみサポートされています。

8.19.1 デバイスをWi-Fiに接続する

開始前に

無線ルーターまたはAPのユーザーマニュアルを参照し、SSID、キー、その他のパラメーターを設定してください。

手順

1. TCP/IP 設定ページに移動します：**設定→ ネットワーク→ ネットワーク設定→ TCP/IP**。
2. **WLAN**を選択してパラメーターを設定します。詳細な設定は***TCP/IP***を参照してください。

注意

Wi-Fiを安定して使用するには、DHCPの使用はおすすめしません。

3. Wi-Fi 設定ページに移動します：**設定→ ネットワーク→ ネットワークサービス→ Wi-Fi**。
4. パラメーターを設定し、保存します。
   1) Wi-Fi機能を有効にします。
   2) **「リフレッシュ」**をクリックして利用可能な無線ルーターまたはAPを表示し選択するか、手動で追加するには「＋」をクリックします。
   3) **SSID** を選択または入力します。これは、ワイヤレスルーターまたは AP の SSID と同じである必要があります。ネットワークのパラメータは、**Wi-Fi** に自動的に表示されます。
   4) **ネットワークモード**を「**管理**」に選択します。
   5) 必要に応じて**セキュリティモード**を選択し、パラメータはルーターまたは AP で設定したワイヤレスネットワーク接続と同じにしてください。
   6) **「保存」**をクリックします。

次にやるべきこと

TCP/IP 設定ページに移動します：**設定→ ネットワーク→ ネットワーク設定→ TCP/IP**、そして **Wlan** をクリックして **IPv4 アドレス**を確認し、デバイスにログインします。

8.20 ISUPを設定

デバイスが ISUP プラットフォーム（旧称 Ehome）に登録されている場合、パブリックネットワークを介してデバイスにアクセスして管理したり、データを送信したり、アラーム情報を転送したりすることができます。

手順

1. **[Configuration]** (設定) に移動し、**[→] (ネットワーク)** を選択します。**→ (プラットフォームアクセス) を選択し**、**[→] (ISUP) を選択します**
2. **オプション：**アクセスセンターを選択します。
3. **「有効」**にチェック**を入れます**。
4. プロトコルバージョンを選択し、関連するパラメータを入力します。
5. **保存**をクリックします。
   機能が正しく設定されると、登録状態が**「オンライン」**に変わります。

8.21 Hik-Connect 経由でカメラにアクセスする

Hik-Connect は、モバイルデバイス用のアプリケーションです。このアプリを使用すると、ライブ画像の表示、アラーム通知の受信などを行うことができます。

開始前に

カメラをネットワークケーブルでネットワークに接続してください。

手順

1. 以下の方法に従って、Hik-Connect アプリケーションをダウンロードしてインストールしてください。
   - お使いのスマートフォンに対応したアプリケーションをダウンロードするには、***https://appstore.hikvision.com*** にアクセスしてください。
   - 当社の公式ウェブサイトにアクセスしてください。次に、**「サポート」→「→ ツール」→「→ Hikvision App Store」**の順に移動してください。
   - 以下のQRコードをスキャンしてアプリケーションをダウンロードしてください。

注意

インストール中に「不明なアプリ」などのエラーが発生した場合、以下の2つの方法で問題を解決してください。

- ***https://appstore.hikvision.com/static/help/index.html*** にアクセスし、トラブルシューティングを参照してください。
- ***https://appstore.hikvision.com/*** にアクセスし、インターフェースの右上にある「**インストールヘルプ**」をクリックして、トラブルシューティングを参照してください。

2. アプリケーションを起動し、Hik-Connectユーザーアカウントを登録してください。
3. 登録後、ログインしてください。
4. アプリで、右上隅の「+」をタップし、カメラの QR コードをスキャンしてカメラを追加します。QR コードは、カメラまたはパッケージ内のカメラのクイックスタートガイドの表紙に記載されています。
5. 指示に従ってネットワーク接続を設定し、カメラを Hik-Connect アカウントに追加します。
   詳細な情報は、Hik-Connectアプリのユーザーマニュアルをご参照ください。

8.21.1 カメラで Hik-Connect サービスを有効にする

Hik-Connect サービスを使用する前に、お使いのカメラで Hik-Connect サービスを有効にする必要があります。このサービスは、SADP ソフトウェアまたはウェブブラウザーから有効にすることができます。

ウェブブラウザーから Hik-Connect サービスを有効にする

ウェブブラウザーから Hik-Connect サービスを有効にするには、以下の手順に従ってください。

開始前に

サービスを有効にする前に、カメラをアクティブ化する必要があります。

手順

1. ウェブブラウザーからカメラにアクセスします。
2. プラットフォームアクセス設定インターフェースに入ります。**設定→ ネットワーク→プラットフォームアクセス → Hik-Connect**。
3. **「有効」**にチェック**を入れます**。
4. ポップアップウィンドウで「利用規約」および「プライバシーポリシー」をクリックして確認してください。
5. カメラ用の認証コードを作成するか、古い認証コードを変更します。

   注意

   カメラを Hik-Connect サービスに追加する際に、確認コードが必要になります。
6. 設定を保存してください。

SADP ソフトウェア経由で Hik-Connect サービスを有効にする

この部分では、有効化されたカメラの SADP ソフトウェアを使用して Hik-Connect サービスを有効にする方法について説明します。

手順

1. SADP ソフトウェアを実行します。
2. カメラを選択し、「**ネットワークパラメータの変更**」ページに入ります。
3. **「Hik-Connect を有効にする」**にチェックを入れます。
4. 検証コードを作成するか、古い検証コードを変更してください。

   注意

   カメラを Hik-Connect サービスに追加する際に、確認コードが必要になります。
5. 「利用規約」と「プライバシーポリシー」をクリックしてご確認ください。
6. 設定を確認してください。

8.21.2 Hik-Connect の設定

手順

1. 以下の方法のいずれかでHik-Connectアプリケーションをダウンロードしてインストールしてください。
   - お使いのスマートフォンシステムに応じて、***https://appstore.hikvision.com*** からアプリケーションをダウンロードしてください。
   - 当社の公式ウェブサイトにアクセスしてください。次に、**[サポート]、[→]、[ツール]、[→]、[Hikvision App Store]** の順に選択してください。
   - 以下のQRコードをスキャンしてアプリケーションをダウンロードしてください。

注意

インストール中に「不明なアプリ」などのエラーが発生した場合、以下の2つの方法で問題を解決してください。

- ***https://appstore.hikvision.com/static/help/index.html*** にアクセスし、トラブルシューティングを参照してください。
- ***https://appstore.hikvision.com/*** にアクセスし、インターフェースの右上にある「**インストールヘルプ**」をクリックして、トラブルシューティングを参照してください。

2. アプリケーションを起動し、Hik-Connectユーザーアカウントを登録してください。
3. 登録後、ログインしてください。

8.21.3 Hik-Connect にカメラを追加する

手順

1. モバイルデバイスをWi-Fiに接続します。
2. Hik-Connect アプリにログインしてください。
3. ホーム画面で、右上隅の「+」をタップしてカメラを追加します。
4. カメラ本体または *クイックスタートガイド*の表紙にある QR コードをスキャンします。

注意

QR コードがない場合や、QR コードがぼやけて認識できない場合は、カメラのシリアル番号を入力してカメラを追加することもできます。

5. カメラの認証コードを入力します。

注意

- 必要な確認コードは、カメラで Hik-Connect サービスを有効にする際に作成または変更したコードです。
- 確認コードを忘れた場合は、ウェブブラウザーで**プラットフォーム**アクセス設定ページから現在の確認コードを確認できます。

6. ポップアップインターフェースの「**ネットワークに接続**」ボタンをタップします。
7. カメラの機能に応じて、「**有線接続**」または「**無線接続**」を選択します。

ワイヤレス接続	携帯電話が接続している Wi-Fi パスワードを入力し、「**次へ**」をタップして Wi-Fi 接続プロセスを開始します。(Wi-Fi を設定する場合は、カメラをルーターから 3 メートル以内に設置してください。)
有線接続	カメラをネットワークケーブルでルーターに接続し、結果画面で「**接続済み**」をタップします。 をタップします。

注意

ルーターは、スマートフォンが接続している同じルーターである必要があります。

8. 次のインターフェースで「**追加**」をタップして、追加を完了します。
詳細な情報は、Hik-Connect アプリのユーザーマニュアルを参照してください。

8.22 オープンネットワークビデオインターフェースを設定する

オープンネットワークビデオインターフェースプロトコルを介してデバイスにアクセスする必要がある場合は、ユーザー設定を構成してネットワークのセキュリティを強化することができます。

手順

1. **[Configuration]** (構成) に移動します。→ **[Network] (ネットワーク)** に移動します。→ **[Platform Access] (プラットフォームアクセス)** に移動します。→ **[Open Network Video Interface] (**
2. 「**有効**」にチェック**を入れます**。
3. 認証モードを選択します。
   - **ダイジェスト**を選択した場合、デバイスはダイジェスト認証のみをサポートします。
   - 「**Digest&ws-username token**」を選択した場合、デバイスはダイジェスト認証またはws-username token認証をサポートします。
4. **[追加]** をクリックして、オープンネットワークビデオインターフェースユーザーを設定します。
5. **保存**をクリックします。
6. **オプション：** 上記の手順を繰り返して、オープンネットワークビデオインターフェースユーザーを追加します。
7. **オプション：** ユーザーを管理します。
   - をクリックして、選択したオープンネットワークビデオインターフェースのユーザーを削除します。
   - をクリックして、選択したオープンネットワークビデオインターフェースユーザーを変更します。

8.23 SDK サービスを設定します。

デバイスをクライアントソフトウェアに追加する場合は、SDK サービスまたは拡張 SDK サービスを有効にする必要があります。

手順

1. 「**Configuration**」→「**→**」→「**Network**」→「**→**」→「**Platform Access**」→「**→**」→「**SDK Service**」の順に選択します。
2. **SDK サービスの**パラメーターを設定します。
   1) SDKプロトコルを使用してデバイスをクライアントソフトウェアに追加するには、**[有効]** をチェックします。
   2) **ポート**番号を入力します。
3. **拡張SDKサービスの**パラメーターを設定します。
   1) **[有効]** をオンにして、TLSプロトコル経由の SDK を使用してデバイスをクライアントソフトウェアに追加します。
   2) **オプション：[TLS 設定]** をクリックして、デバイスがサポートする TLS バージョンを有効にします。詳細については、***TLS***
   を参照してください。
   3) **ポート**番号を入力します。
   4) データ転送のセキュリティを確保するために、サーバー証明書を選択します。**証明書管理**をクリックして、証明書を追加することができます。詳細については、***証明書管理***を参照してください。
4. **保存**をクリックします。

第 9 章 システムとセキュリティ

システムメンテナンス、システム設定、セキュリティ管理について紹介し、関連するパラメータの設定方法を説明します。

9.1 システム設定

9.1.1 デバイス情報の表示

デバイス番号、モデル、シリアル番号、ファームウェアバージョンなどのデバイス情報を表示できます。

設定画面を開く→ **システム**→ **システム設定**→ **基本情報で**デバイス情報を確認できます。

9.1.2 日時

タイムゾーン、時間同期、および夏時間（DST）を設定することで、デバイスの日時を設定できます。

手動で時間を同期する

手順

1. **[Configuration]** (**設定**) に移動し、**[→] (システム)** を選択します。**→ (システム設定) を選択し**、**[→] (時刻設定) を選択します**
2. **タイムゾーン**を選択します。
3. **手動で時間を同期**を選択します。
4. 時間同期方法を選択します。
   - **[時刻の設定]** を選択し、ポップアップカレンダーから日付と時刻を手動で入力または選択します。
   - **「コンピュータの時間と同期」**をクリックして、デバイスの時間をローカルPCの時間と同期します。
5. **「保存」**をクリックします。

NTPサーバーを設定

正確で信頼性の高い時刻ソースが必要な場合、NTPサーバーを使用できます。

開始前に

NTP サーバーを設定するか、NTP サーバーの情報を入手してください。

手順

1. **[Configuration]** (構成)→ **[System] (システム)**→ **[System Settings] (システム設定)**→ **[Time Settings]** (時刻設定)
2. **タイムゾーン**を選択します。

3. **NTP** をクリックします。
4. **サーバーアドレス**、**NTP ポート**、および**間隔**を設定します。

注意

サーバーアドレスはNTPサーバーのIPアドレスです。

5. **テスト**をクリックしてサーバー接続を確認します。
6. **保存**をクリックします。

衛星による時刻同期

注意

この機能はデバイスによって異なります。

手順

1. **設定**を開く→ **システム**→ **システム設定**→ **時間設定** .
2. **衛星時刻同期**を選択..
3. **間隔**を設定します。
4. **保存**をクリック。

DSTを設定

デバイスが設置されている地域で夏時間（DST）を採用している場合、この機能を設定できます。

手順

1. Go to **Configuration**→ **System**→ **System Settings**→ **Time Settings**
2. 「**有効**」にチェック**を入れます**。
3. **開始時間**、**終了時間**、**およびDSTバイアス**を選択します。
4. **保存**をクリックします。

9.1.3 RS-232を設定します。

RS-232は、デバイスのデバッグや周辺機器へのアクセスに利用できます。RS-232は、通信距離が短い場合、デバイスとコンピュータまたは端末間の通信を実現できます。

開始前に

RS-232ケーブルを使用して、デバイスをコンピュータまたは端末に接続します。

手順

1. Go to **Configuration**→ **System**→ **System Settings**→ **RS-232** .
2. RS-232パラメーターを、デバイスとコンピュータまたはターミナルに一致するように設定します。
3. **保存**をクリックします。

9.1.4 RS-485を設定します。

RS-485は、デバイスを外部デバイスに接続するために使用されます。通信距離が長い場合、RS-485を使用してデバイスとコンピュータまたはターミナルの間でデータを送信できます。

開始前に

RS-485ケーブルを使用して、デバイスとコンピュータまたは端末を接続します。

手順

1. Go to **Configuration→ System→ System Settings→ RS-485** .
2. RS-485パラメーターを設定します。

注意

デバイスとコンピュータまたはターミナルのパラメーターはすべて同じに保つ必要があります。

3. **保存**をクリックしてください。

9.1.5 ライブビュー接続を設定

リモートライブビュー接続の数を制御します。

ライブビュー接続は、同時にストリーミングできる最大ライブビューの数を制御します。

設定画面を開き、**[→] > [→] > [System Settings]** > **[→] > [System Service]** を選択し、リモート接続の上限を設定します。

9.1.6 位置設定

位置は、デバイスの現在の経度と緯度を表示し、アップロードします。

自動アップロード

「有効」にチェックを入れ、**位置情報アップロード間隔**を設定します。

デバイスは設定された間隔で位置情報を送信します。手動でデバイスの位置情報を更新するには、**[リフレッシュ]** をクリックしてください。

手動設定

「有効」にチェックを入れ、**位置情報アップロード間隔**を設定します。デバイスの経度と緯度を入力し、「**保存**」をクリックします。

デバイスは設定された間隔で設定された位置情報を送信します。

注意

この機能は、デバイスモデルによって異なる場合があります。

9.1.7 外部デバイス

補足ライト、ハウジングのワイパー、LED ライト、ヒーターなどの外部デバイスをサポートするデバイスは、ハウジングと併用することで、ウェブブラウザーから制御することができます。外部デバイスは、モデルによって異なります。

9.1.8 オープンソースソフトウェアのライセンスを表示

右上隅にある「 」をクリックし、「**Open Source Software Description**」を選択してライセンスをダウンロードします。エディタでライセンスを表示できます。

9.1.9 Wiegand

注意

この機能は、一部のカメラモデルでのみサポートされています。

[有効] をチェックし、プロトコルを選択します。デフォルトのプロトコルは SHA-1 26 ビットです。

有効にすると、認識されたナンバープレート番号が、選択した Wiegand プロトコルを介して出力されます。

9.2 ユーザーとアカウント

9.2.1 ユーザー アカウントと権限を設定します。

管理者は、他のアカウントを追加、変更、削除したり、ユーザーレベルごとに異なる権限を付与したりすることができます。

注意

ネットワーク上で本機を使用する際のセキュリティを強化するため、アカウントのパスワードは定期的に変更してください。3 ヶ月ごとにパスワードを変更することをお勧めします。リスクの高い環境で使用する場合は、毎月または毎週パスワードを変更することをお勧めします。

手順

1. Go to **Configuration→ System→ User Management→ User Management**
2. **[追加]** をクリックします。**ユーザー名**を入力し、**レベル**を選択して、**パスワード**を入力します。必要に応じて、ユーザーにリモートアクセス権限を割り当てます。

   管理者

   管理者はすべての操作権限を有し、ユーザーとオペレーターを追加し、権限を割り当てることができます。

ユーザー

ユーザーには、ライブビデオの視聴、PTZ パラメータの設定、および自分のパスワードの変更の権限を割り当てることができますが、その他の操作の権限は割り当てられません。

オペレーター

オペレーターには、管理者に対する操作とアカウントの作成を除くすべての権限を付与できます。

変更 ユーザーを選択し、[✎] をクリックしてパスワードと権限を変更します。

削除 ユーザーを選択し、🗑 をクリックします。

注意

管理者は、最大 31 個のユーザーアカウントを追加できます。

3. **OK**をクリックします。

9.2.2 同時ログイン

管理者は、ウェブブラウザーからシステムに同時にログインできるユーザーの最大数を設定できます。

設定→ システム→ ユーザー管理→ オンラインユーザー、**[全般]** をクリックし、[同時ログイン] を設定します。

同時ログインを設定します。

9.2.3 オンラインユーザー

デバイスにログインしているユーザーの情報を表示します。

[設定] の **[→] [システム] [→] [ユーザー管理] [→] [オンラインユーザー]** に移動して、オンラインユーザーの一覧を表示します。

9.3 メンテナンス

9.3.1 再起動

ブラウザからデバイスを再起動できます。

Go to **Maintenance and Security→ Maintenance→ Restart** , and click **Restart**.

9.3.2 アップグレード

開始前に

正しいアップグレードパッケージを取得する必要があります。

注意

アップグレード中は電源を切らないでください。アップグレードが完了すると、デバイスは自動的に再起動します。

手順

1. **→[メンテナンスとセキュリティ]、[→]、[メンテナンス]、[アップグレード]** の順に選択します。
2. アップグレードする方法を選択してください。

   ファームウェア　　アップグレードファイルの正確なパスを特定します。

   ファームウェアディレクトリ　アップグレードファイルが含まれるディレクトリを特定します。
3. 「」をクリックしてアップグレードファイルを選択します。
4. **「アップグレード」** をクリックします。

9.3.3 復元とデフォルト

復元とデフォルトは、デバイスのパラメーターをデフォルト設定に復元します。

手順

1. **[メンテナンスとセキュリティ]、[→]、[→]、[バックアップと復元]** の順に選択します。
2. 必要に応じて **「復元」** または **「デフォルト」** をクリックします。

   復元　ユーザー情報、IP パラメータ、およびビデオフォーマットを除くデバイスパラメータをデフォルト設定にリセットします。

   デフォルト　すべてのパラメーターを工場出荷時のデフォルト設定にリセットします。

   注意

   この機能を使用する際はご注意ください。工場出荷時設定にリセットすると、すべてのパラメーターがデフォルト設定にリセットされます。

9.3.4 設定ファイルのインポートとエクスポート

同じパラメータを持つ他のデバイスのバッチ設定を高速化します。

手順

1. 設定ファイルをエクスポートします。
   1) Go to **Maintenance and Security→ Maintenance→ Backup and Restore→ Backup** .
   2) **「エクスポート」** をクリックし、暗号化パスワードを入力して現在の設定ファイルをエクスポートします。
   3) 保存先パスを設定し、構成ファイルをローカルコンピュータに保存します。
2. 設定ファイルをインポートします。
   1) ウェブブラウザーから、設定が必要なデバイスにアクセスします。
   2) **[メンテナンスとセキュリティ]** に移動します。**→[メンテナンス]** を選択します。**→[バックアップと復元]** を選択します。**→[リセット]** を選択します。
   3) 「」をクリックして保存した設定ファイルを選択します。
   4) 設定ファイルをエクスポートした際に設定した暗号化パスワードを入力します。

5)「**インポート**」をクリックします。

9.3.5 ログの検索と管理

ログは問題の特定とトラブルシューティングに役立ちます。

手順

1. **[メンテナンスとセキュリティ]** に移動します**。→[メンテナンス] を選択します**。**→[ログ]** を選択します。

2. 検索条件を設定します：**主要タイプ**、**副次タイプ**、**開始時間**、**終了時間**。

3. **検索**をクリックします。

一致したログファイルがログ一覧に表示されます。

4. **オプション：[エクスポート]** をクリックして、ログファイルをコンピュータに保存します。

9.3.6 セキュリティ監査ログの検索

デバイスのセキュリティログファイルを検索および分析して、不正侵入を発見し、セキュリティイベントをトラブルシューティングすることができます。

手順

注意

この機能は、一部のカメラモデルでのみサポートされています。

1. [**メンテナンスとセキュリティ]、[→]、[→]、[セキュリティ]、[監査ログ]** の順に選択します。

2. ログの種類、**開始時間**、**終了時間**を選択します。

3. **検索**をクリックします。

検索条件に一致するログファイルがログ一覧に表示されます。

4. **オプション：[エクスポート]** をクリックして、ログファイルをコンピュータに保存します。

9.3.7 SSH

Secure Shell (SSH) は、セキュリティで保護されていないネットワーク上でネットワークサービスを運用するための暗号化ネットワークプロトコルです。

Go to **Maintenance and Security→ Maintenance→ Device Debugging** , and click **Settings** of **SSH**. ポート番号を編集できます。**Save**をクリックします。

注意

この機能は慎重に使用してください。この機能を有効にすると、デバイス内部情報の漏洩というセキュリティ上のリスクがあります。

9.3.8 診断情報のエクスポート

診断情報には、実行ログ、システム情報、ハードウェア情報が含まれます。

Go to **Maintenance and Security→ Maintenance→ Device Debugging→ Diagnose Information**.**Export** をクリックします。ポップアップウィンドウで、必要な診断情報をチェックし、**Export** をクリックして、デバイスの対応する診断情報をエクスポートします。

9.3.9 診断

4G ネットワークに対応しているデバイスでは、診断により、通信パケット、デバイスの電源、ネットワーク情報を取得し、今後のメンテナンスやトラブルシューティングに役立てることができます。

デバイス パケットのキャプチャ

この機能は専門家専用であり、デバイスと外部デバイス間の通信パケットを取得し、今後の問題診断やデバッグに利用されます。

手順

注意

この機能は専門家および技術サポートスタッフ専用です。

1. **[メンテナンスとセキュリティ]、[→]、[→]**、[**Device Debugging**] の順に選択し、[**Device Packet Capture**] の **[Settings]** をクリックします。

   デバイスパケットのキャプチャ] をクリックします。
2. **「有効」**にチェックを入れてこの機能を有効にします。

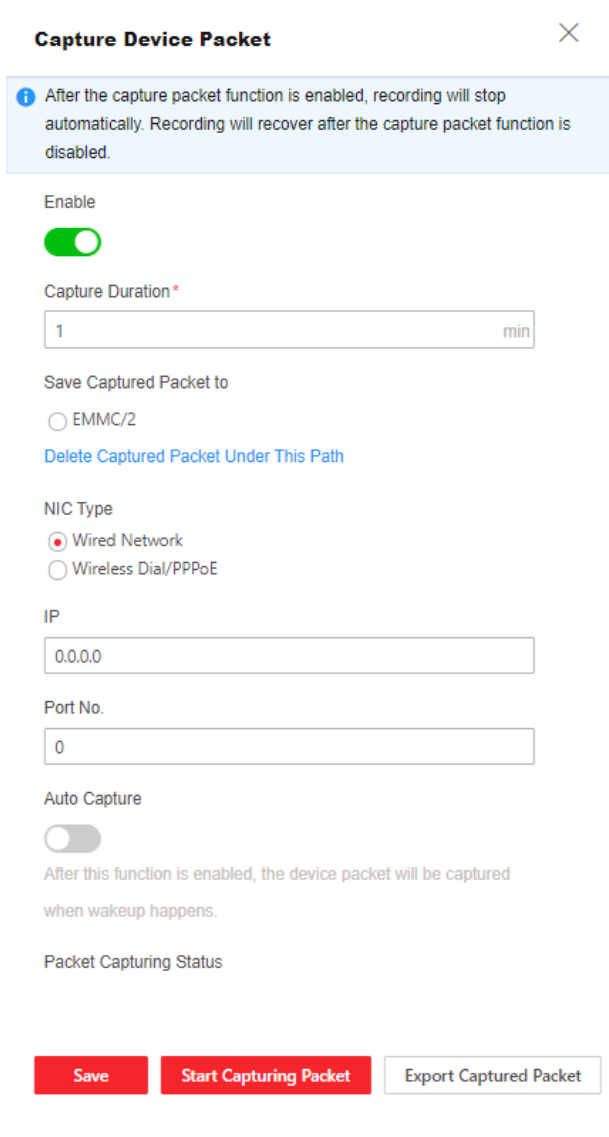

図9-1 キャプチャデバイス パケット

3. **キャプチャ時間を**必要に応じて設定してください。
4. パケットの保存先を選択してください。

注意

a. 保存先パスは、デバイスの実際の保存方法によって異なります。
b. **「このパス下のキャプチャ済みパケットを削除」**をクリックすると、保存されたパケットファイルを削除できます。

5. NIC タイプ、IP、およびポートを設定します。
6. **オプション：[自動キャプチャ]**を選択すると、ウェイクアップ時にデバイスパケットがキャプチャされます。
7. **「保存」**をクリックします。
8. **「パケットのキャプチャを開始」**をクリックします。

9. キャプチャが完了したら、**[キャプチャしたパケットをエクスポート]** をクリックしてレポートを保存します。

デバイス情報のエクスポート

[メンテナンスとセキュリティ]、**[→]**、**[→]**、**[Device Debugging]**、**[→]**、**[Export Device Info]** の順に選択し、**[Export]** をクリックして、電圧、電流、電源、4G データなどのデバイス情報をエクスポートします。

9.4 セキュリティ

セキュリティパラメータを設定することで、システムのセキュリティを向上させることができます。

9.4.1 IPアドレスフィルターを設定

IPアドレスフィルターはアクセス制御のためのツールです。特定のIPアドレスからのアクセスを許可または拒否するために、IPアドレスフィルターを有効にできます。

IPアドレスはIPv4を指します。

手順

1. **[メンテナンスとセキュリティ]**、**[→]**、**[セキュリティ]**、**[→]**、**[IP アドレス フィルター]** の順に選択します。

2. **「有効」**にチェック**を入れます**。

3. IP アドレス フィルターの種類を選択します。

ブロックリスト　　リストに指定されたIPアドレスはデバイスにアクセスできません。

許可リスト　リストに指定されたIPアドレスのみがデバイスにアクセスできます。

4. IPアドレスフィルターリストを編集します。

追加　リストに新しいIPアドレスまたはIPアドレス範囲を追加します。

 　リスト内の選択したIPアドレスまたはIPアドレス範囲を編集します。

 　リストから選択したIPアドレスまたはIPアドレス範囲を削除します。

5. **保存**をクリックします。

9.4.2 MACアドレスフィルターを設定する

MACアドレスフィルターはアクセス制御のためのツールです。特定のMACアドレスからのアクセスを許可または拒否するために、MACアドレスフィルターを有効にできます。

手順

1. **→[メンテナンスとセキュリティ]**、**[→]**、**[セキュリティ]**、**[MAC アドレスフィルター]** の順に選択します。

2. **「有効」**にチェック**を入れます**。

3. MACアドレスフィルターの種類を選択します。

ブロックリスト　　リストに表示されているMACアドレスは、デバイスにアクセスできません。

許可リスト　リストに指定されたMACアドレスのみがデバイスにアクセスできます。

4. MACアドレスフィルターリストを編集します。

追加　リストに新しいMACアドレスを追加します。

　　リスト内の選択したMACアドレスを編集します。

　　リスト内の選択したMACアドレスを削除します。

5. **保存**をクリックします。

9.4.3 タイムアウト設定の制御

この機能を有効にすると、設定したタイムアウト時間内にウェブブラウザーからデバイスに対して操作（ライブ画像の表示を除く）を行わないと、自動的にログアウトされます。

[メンテナンスとセキュリティ]、[→]、[セキュリティ]、[→]、[ログイン管理]、[→]、[タイムアウト設定] の順に選択し、設定を完了します。

9.4.4 証明書管理

サーバー/クライアント証明書および CA 証明書を管理し、証明書の有効期限が近づいた場合、または有効期限が切れた場合、あるいは異常があった場合にアラームを送信するのに役立ちます。

注意

この機能は、特定のデバイスモデルでのみサポートされています。

サーバー証明書/クライアント証明書

注

デバイスには、デフォルトの自己署名サーバー/クライアント証明書がインストールされています。証明書 ID は***デフォルト***です。

自己署名証明書を作成してインストールする

手順

1. [**メンテナンスとセキュリティ**]、[**→**]、[**セキュリティ**]、[**→**]、[**Certificate Management**] の順に選択します。

2. 「**自己署名証明書を作成**」をクリックします。

3. 証明書情報を入力します。

注

入力する証明書 ID は既存のものと同一にできません。

4. 「**保存**」をクリックして証明書を保存し、インストールします。

作成した証明書が、**サーバー/クライアント**証明書リストに表示されます。

証明書が特定の機能で使用されている場合、その機能名は列
「機能」列に表示されます。

5. **オプション：[プロパティ]** をクリックすると、証明書の詳細を確認できます。

自己署名証明書をインストールする

自己署名証明書を信頼できる第三者に送信し、署名を取得した後、証明書をデバイスにインストールできます。

開始する前に

まず、自己署名証明書を作成します。作成方法については、*「自己署名証明書の作成とインストール」*を参照してください。

手順

1. **[メンテナンスとセキュリティ]**、**[→ セキュリティ]**、**[→ 証明書管理]** の順に選択します。

2. **サーバー/クライアント証明書**リストから自己署名証明書を選択します。

3. **「証明書リクエストの作成」**をクリックします。

4. リクエスト情報を入力します。

5. **「保存」**をクリックします。

証明書要求の詳細がポップアップウィンドウに表示されます。

6. リクエストの内容をコピーし、リクエストファイルとして保存してください。

7. ファイルを信頼できる第三者に送信し、署名を取得します。

8. 第三者から返送された証明書を受け取った後、デバイスにインストールします。

1) **「インポート」**をクリックします。

2) **証明書ID**を入力します。

注意

入力する証明書IDは、既存のものと同一にしてはいけません。

3) クリック をクリックして証明書ファイルを選択してください。

4) **自己署名証明書**を選択します。

5) **保存**をクリックします。

インポートした証明書は、**[サーバー/クライアント証明書]** リストに表示されます。

証明書が特定の機能で使用されている場合、その機能名は「機能」列に表示されます。
「機能」列に表示されます。

9. **オプション：[プロパティ]** をクリックして、証明書の詳細を表示します。

他の承認済み証明書をインストール

既に認証済み証明書（デバイスで作成されていないもの）がある場合、デバイスに直接インポートできます。

手順

1. **[メンテナンスとセキュリティ]**、**[→]**、**[セキュリティ]**、**[→ 証明書管理]** の順に移動します。

2. **サーバー/クライアント**証明書リストで**「インポート」**をクリックします。

3. **証明書ID**を入力してください。

注

入力する証明書IDは、既存のものと同一にしてはいけません。

4. クリック をクリックして証明書ファイルを選択します。
5. **証明書とキー**を選択し、証明書に応じて**キーの種類**を選択してください。

独立したキー	証明書に独立したキーがある場合は、このオプションを選択します。 参照をクリックしてプライベートキーを選択し、プライベートキーのパスワードを入力してください。
PKCS#12	証明書と同じ証明書ファイルにキーがある場合は、このオプションを選択し、パスワードを入力します。

6. **保存**をクリックします。

インポートした証明書は、[**サーバー/クライアント証明書**] リストに表示されます。

証明書が特定の機能で使用されている場合、その機能名は「機能」列に表示されます。

機能に表示されます。

CA証明書をインストールする

開始前に

事前にCA証明書を用意してください。

手順

1. [**メンテナンスとセキュリティ**]、[**→**]、[**セキュリティ**]、[**→ 証明書管理**] の順に選択します。
2. **CA証明書**の一覧で「**インポート**」をクリックします。
3. **証明書 ID** を入力します。

注

入力する証明書 ID は、既存の証明書 ID と同一にしてはいけません。

4. クリック をクリックして証明書ファイルを選択します。
5. **保存**をクリックします。

インポートされた証明書は**CA証明書**リストに表示されます。

証明書が特定の機能で使用されている場合、その機能名は「**機能**」

列に表示されます。

証明書有効期限アラームを有効にする

手順

1. **有効にする場合は**、[有効にする] **を選択します**。有効にすると、証明書の有効期限が近づいた、または有効期限が切れた、あるいは異常が発生した場合に、E メールまたはカメラが監視センターにリンクして通知されます。
2. **有効にする場合は**、**有効にする機能にチェックマークを付け**ます。

注意

- 有効期限の1日前に通知する日数を1に設定すると、有効期限の前日にカメラが通知します。1日から30日まで設定できます。デフォルトは7日です。
- 有効期限前のリマインダー日を 1 に設定し、検出時間を 10:00 に設定した場合、証明書が翌日の 9:00 に有効期限が切れる場合、カメラは 1 日目の 10:00 にリマインダーを表示します。

3. **保存**をクリックしてください。

9.4.5 TLS

トランスポート層セキュリティ (TLS) プロトコルは、主に 2 つ以上の通信するコンピュータアプリケーション間のプライバシーとデータの整合性を確保することを目的としています。TLS 設定は、HTTP(S) および拡張 SDK サービスに有効です。

[メンテナンスとセキュリティ]、**[→ セキュリティ]**、[**→ TLS**] の順に選択し、目的の TLS プロトコルを有効にします。

保存をクリックします。

注意

この機能は慎重に使用してください。この機能を有効にすると、デバイス内部情報の漏洩というセキュリティ上のリスクがあります。

第10章 VCAリソース

VCAリソースは、デバイスがサポートするスマート機能の集合体です。

10.1 オープンプラットフォームの設定

HEOP (Hikvision Embedded Open Platform) を使用すると、サードパーティが開発したアプリケーションをインストールして、その機能やサービスを実行することができます。HEOP 対応デバイスでは、以下の手順に従って、スマートアプリケーションをインポートして実行することができます。

手順

1. **VCA** インターフェースに移動します。

注意

アプリケーションをインストールする前に、インストールしたいアプリケーションが以下の条件を満たしていることを確認してください。

- 各アプリケーションには独自の名前が割り当てられています。
- アプリケーションが使用するフラッシュメモリの容量が、デバイスの使用可能なフラッシュメモリの容量よりも小さい。
- アプリケーションのメモリおよび演算能力は、デバイスの使用可能メモリおよび演算能力以下である。

2. **「アプリケーションのインポート」**をクリックし、ローカルパスを閲覧してアプリケーションパッケージを選択し、インポートします。
3. **「ライセンスのインポート」**をクリックし、ローカルのパスを閲覧してライセンスファイルを選択し、インポートします。
4. **オプション：**アプリケーションを設定します。

クリック	アプリケーションを有効または無効にします。
クリック	アプリケーションを削除します。
クリック	ログをエクスポートします。
クリック	ローカルパスを選択し、アプリケーションパッケージをインポートしてアプリケーションを更新します。
クリック	メモリの断片化をクリアして、より多くのメモリを解放し、よりスマートなアプリケーションを使用できるようにします。
詳細を表示	アプリケーションを選択し、クリックしてページに詳細を表示します。

10.2 スマートアプリケーション

スマートアプリケーションに関連する一般的なパラメータを設定します。

VCA に移動します**。→ アプリケーションの設定→ 全般設定で**、以下のパラメータを設定します。

カメラ情報

カメラ情報の設定については、*「カメラ情報の設定」*を参照してください。

FTP

FTPの設定については、*「FTPの設定*」を参照してください。

メール

メールの設定については、「*メールの設定」*を参照してください。

アラーム出力

アラーム出力の設定については、「*自動アラーム」*を参照してください。

可聴アラーム出力

可聴アラーム出力の設定については、*「可聴アラーム出力の設定」*を参照してください。

アラームサーバー

アラームサーバーの設定については、*「アラームサーバー」*を参照してください。

メタデータ

メタデータの設定については、*メタデータ*をご参照ください。

10.2.1 カメラ情報を設定する

デバイスに関する特定の情報をカスタマイズします。複数のデバイスを管理している場合に、特定のデバイスを識別するのに役立ちます。

VCA に移動します**。→ アプリケーションを設定します。→ 全般設定→ カメラ情報で**、**デバイス番号**と**カメラ情報を**設定します。

10.2.2 メタデータ

メタデータは、アルゴリズム処理の前にデバイスが収集する生データです。多くの場合、サードパーティの統合に使用されます。

VCA に移動**→ アプリケーションの設定→ 一般設定→ メタデータ** 必要な機能のメタデータをアップロード可能にする設定です。

注意

この機能は、カメラモデルによって異なる場合があります。

スマートイベント

スマートイベントのメタデータには、ターゲット ID、ターゲット座標、時間などが含まれます。

顔キャプチャ

顔キャプチャのメタデータには、ルール情報、ターゲット ID、ターゲット座標、時間情報などが含まれます。カメラは、デフォルトでは画像全体を検出します。顔キャプチャの設定で領域が設定されている場合、カメラは設定された領域を検出します。

10.2.3 AcuSearch

ターゲットを検出した後、そのターゲットのPOS情報をネットワークビデオレコーダーに送信します。接続されたネットワークビデオレコーダー上で、正確かつ迅速な検索を実現します。

開始前に

- この機能を使用するには、接続されたネットワークビデオレコーダー（NVR）が AcuSearch をサポートしていることを確認してください。
- この機能を有効にすると、**スマートイベントまたはマルチターゲット検出が**有効になっている場合、実行中のスマートアプリケーションは無効になります。

  または**マルチターゲット検出が**有効になっている間は、進行中のスマートアプリケーションが無効になります。
- この機能は特定のモデルでのみサポートされています。実際の表示はモデルによって異なります。

手順

1. デバイスで機能を有効にします。

2. 接続されたネットワークビデオレコーダーで機能を設定します。

1) ネットワークビデオレコーダーで、選択したチャンネル（設定済みのカメラデバイスを参照）の AcuSearch 機能を有効にします。

2) ネットワークビデオレコーダーの再生ページで、AcuSearch ボタンをクリックします。

3) ネットワークビデオレコーダーで対象をクリックすると、その対象を含む画像が検索されます。

4) 画像をクリックすると、その前後のビデオが再生されます。

注意

NVRの実際の設定については、NVRの *ユーザーマニュアル*をご参照ください。

10.3 スマートイベント

注意

- 一部のデバイスモデルでは、VCA ページでスマートイベント機能を有効にしてから、機能設定ページを表示する必要があります。
- 機能はモデルによって異なります。

10.3.1 侵入検知の設定

これは、あらかじめ定義された仮想領域への侵入や滞留を検知するために使用します。侵入や滞留が発生した場合、デバイスはリンク動作を実行できます。

開始前に

- **VCA** に移動し、アプリケーションを選択します。**スマートイベント**を選択し、**[次へ]** をクリックして機能を有効にします。
- HEOP 対応デバイスでは、**VCA** に移動して**スマートイベントを**インポートし、有効にしてください。

手順

1. **VCA** に移動し、**[→] を選択します。アプリケーションを設定します。→ スマートイベント→ 侵入検知**。
2. **「有効」**にチェック**を入れます**。
3. **「追加」**をクリックしてルールを追加し、検出領域を設定します。
   1) 検出領域を描画します。をクリックし、ライブビューをクリックして頂点を指定し、検出領域の境界を描画し、右クリックで描画を完了します。
   2) ターゲットの検出精度を向上させるため、ターゲットの最小サイズと最大サイズを設定します。最大サイズと最小サイズの間にあるサイズのターゲットのみが検出されます。と をクリックし、ライブビュー内でマウスをドラッグして最小サイズと最大サイズのターゲットを描画します。
   3) **オプション：[** **]** をクリックして、すべての設定領域を削除します。
4. パラメーターを設定

   します。

   検出対象

   この機能を使用すると、指定したターゲットタイプによってアラームをトリガーすることができます。検出ターゲットが選択されていない場合、検出されたすべてのターゲットが報告されます。

   注意

   この機能は、特定のデバイスモデルで特定の設定の場合にのみ使用できます。実際の設定をご確認ください。

   しきい値

   しきい値は、オブジェクトが領域内に留まる時間のしきい値を表します。1 つのオブジェクトがしきい値を超える時間、その領域内に留まった場合、アラームが作動します。しきい値の値が大きいほど、アラームが作動するまでの時間が長くなります。

   感度

   感度は、許容されるターゲットの身体の一部が、あらかじめ定義された領域に入った割合を表します。感度= 100 - S1/ST× 100。S1 は、あらかじめ定義された領域を通過するターゲットの身体の一部を表します。ST は、ターゲットの身体全体を表します。感度の値が大きいほど、アラームが作動しやすくなります。

   ターゲット有効性

   有効性を高く設定すると、必要なターゲットの特徴がより明確になり、アラームの精度が向上します。特徴があまり明確ではないターゲットは見逃されます。

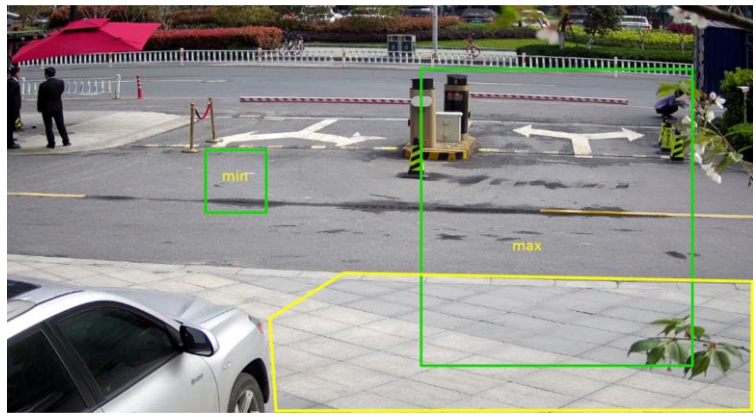

図10-1 ルール設定

5. **オプション：**上記の手順を繰り返して、複数のエリアのパラメータを設定することができます。
6. 武装スケジュールの設定については、*「武装スケジュールの設定」*を参照してください。リンク方法の設定については、*「リンク方法の設定」*を参照してください。
7. **保存**をクリックします。

10.3.2 ラインクロス検出の設定

これは、あらかじめ定義された仮想ラインを横切る物体を検出するために使用されます。検出された場合、デバイスはリンク動作を実行することができます。

開始前に

- **VCA** に移動し、アプリケーションを選択します。**スマートイベント**を選択し、**[次へ]** をクリックして機能を有効にします。
- HEOP 対応デバイスでは、**VCA でスマートイベントを**インポートして有効にしてください。

手順

1. **VCA** に移動し、**[→] を選択します。アプリケーションを設定します。→] を選択し、[スマートイベント] を選択します。→] を選択し、**[ラインクロス検出]を選択します。
2. **「有効」**にチェック**を入れます**。
3. **「追加」**をクリックしてルールを追加し、検出領域を設定します。
   1) 検出ラインを描画します。をクリックすると、ライブビューに矢印付きのラインが表示されます。ライブビュー上の希望の位置にラインをドラッグします。
   2) 検出精度を向上させるため、ターゲットの最小サイズと最大サイズを設定します。最大サイズと最小サイズの間にあるサイズのターゲットのみが検出されます。「」をクリックし、「」をクリックした後、ライブビュー内でマウスをドラッグして最小サイズと最大サイズのターゲットサイズを描画します。
   3) **オプション：[**] をクリックして、すべての設定領域を削除します。
4. パラメーターを設定します。

   検出対象

   この機能により、指定したターゲットタイプによってアラームを鳴らすことができます。検出ターゲットが選択されていない場合、検出されたすべてのターゲットが報告されます。

注意

この機能は、特定のデバイスモデルで特定の設定の場合にのみ使用できます。実際の設定をご確認ください。

方向

ラインを通過する物体の進行方向を表します。

A<->B：両方向からラインを越える物体を検知し、アラームが作動します。

A->B：A サイドから B サイドに設定されたラインを横切る物体のみ検出されます。

B->A：B サイドから A サイドに設定されたラインを横切るオブジェクトのみ検出されます。

感度

これは、許容されるターゲットの身体の一部が、あらかじめ定義されたラインを通過する割合（%）を表します。感度 = 100 - S1/ST × 100。S1 は、あらかじめ定義されたラインを通過するターゲットの身体の一部を表します。ST は、ターゲットの身体全体を表します。感度の値が高いほど、アラームが作動しやすくなります。

ターゲットの有効性

有効性を高く設定すると、必要なターゲットの特徴がより明確になり、アラームの精度が向上します。特徴があまり明確でないターゲットは検出されなくなります。

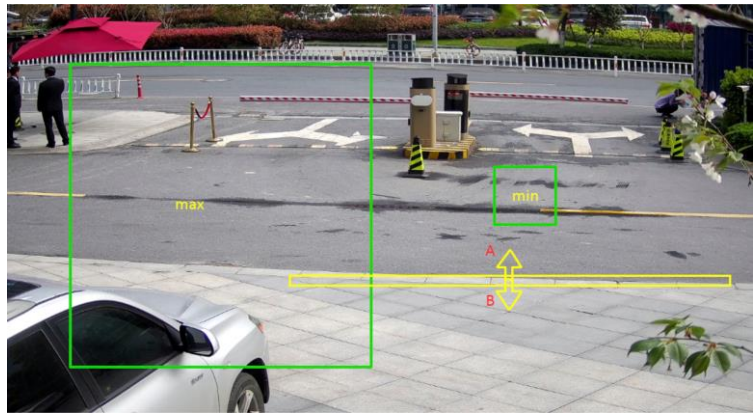

図10-2 ルール設定

5. **オプション：**上記の手順を繰り返して、複数のエリアのパラメータを設定することができます。
6. 武装スケジュールの設定については、*「武装スケジュールの設定」*を参照してください。リンク方法の設定については、*「リンク方法の設定」*を参照してください。
7. **保存**をクリックします。

10.3.3 入口検知の設定

これは、あらかじめ定義された仮想領域に外部から侵入した物体を検出するために使用されます。検出された場合、デバイスはリンク動作を実行することができます。

開始前に

- **VCA** に移動し、アプリケーションを選択します。**スマートイベント**を選択し、**[次へ]** をクリックして機能を有効にします。
- HEOP 対応デバイスでは、**VCA でスマートイベントを**インポートして有効にしてください。

手順

1. **VCA** に移動します**。→ アプリケーションを設定します。→ スマートイベント→ 入口検知**。
2. **「有効」**にチェック**を入れます**。
3. **「追加」**をクリックしてルールを追加し、検出領域を設定します。
   1) 検出領域を描画します。をクリックし、ライブビューをクリックして頂点を指定し、検出領域の境界を描画します。右クリックで描画を完了します。
   2) ターゲットの最小サイズと最大サイズを設定して検出精度を向上させます。最大サイズと最小サイズの間にあるサイズのターゲットのみが検出されます。「」をクリックし、「」をクリックし、ライブビュー内でマウスをドラッグして最小サイズと最大サイズのターゲットサイズを描画します。
   3) **オプション：[** **]** をクリックして、すべての設定領域を削除します。
4. パラメーターを設定

   します。

   検出対象

   この機能により、指定したターゲットタイプによってアラームをトリガーすることができます。検出ターゲットが選択されていない場合、検出されたすべてのターゲットが報告されます。

   注意

   この機能は、特定のデバイスモデルで特定の設定の場合にのみ使用できます。実際の設定をご確認ください。

   感度

   これは、あらかじめ定義された領域を通過した許容ターゲットの身体部分の割合を表します。感度= 100 - S1/ST× 100。S1 は、あらかじめ定義された領域を通過したターゲットの身体部分を意味します。ST は、ターゲットの身体全体を表します。感度の値が高いほど、アラームが作動しやすくなります。

   ターゲット有効性

   有効性を高く設定すると、必要なターゲットの特徴がより明確になり、アラームの精度が向上します。特徴があまり明確でないターゲットは検出されなくなります。

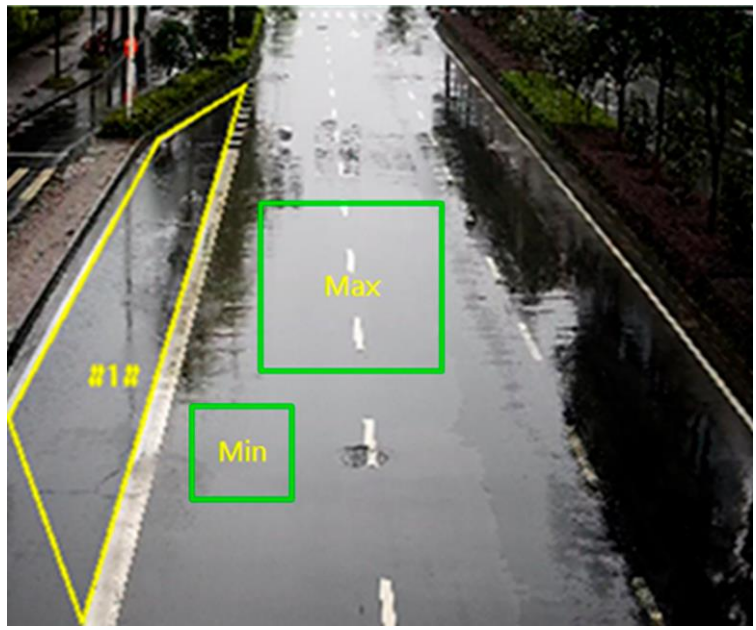

図10-3 ルール設定

5. **オプション：**上記の手順を繰り返して、複数のエリアのパラメータを設定することができます。
6. 武装スケジュールの設定については、*「武装スケジュールの設定」*を参照してください。リンク方法の設定については、*「リンク方法の設定」*を参照してください。
7. **保存**をクリックします。

10.3.4 出口検知の設定

あらかじめ定義した仮想領域から物体が退出することを検知します。この状態が発生すると、デバイスはリンク動作を実行します。

開始前に

- **VCA** に移動し、アプリケーションを選択します。**スマートイベント**を選択し、**[次へ]** をクリックして機能を有効にします。
- HEOP 対応デバイスでは、**VCA でスマートイベントを**インポートして有効にしてください。

手順

1. **VCA** に移動し、**→ を選択します。アプリケーションを設定します。→ を選択し、スマートイベント→ を選択します。出口検知 を選択します。**
2. **「有効」**にチェック**を入れます。**
3. **「追加」**をクリックしてルールを追加し、検出領域を設定します。
   1) 検出領域を描画します。をクリックし、ライブビューをクリックして頂点を指定し、検出領域の境界を描画します。右クリックで描画を完了します。
   2) ターゲットの最小サイズと最大サイズを設定して検出精度を向上させます。最大サイズと最小サイズの間にあるサイズのターゲットのみが検出されます。「」をクリックし、「」をクリックし、ライブビュー内でマウスをドラッグして最小サイズと最大サイズのターゲットサイズを描画します。

3) **オプション：**[ ]をクリックして、すべての設定領域を削除します。

4. パラメーターを設定

します。

検出対象

この機能により、指定したターゲットタイプによってアラームをトリガーすることができます。検出ターゲットが選択されていない場合、検出されたすべてのターゲットが報告されます。

注意

この機能は、特定のデバイスモデルで特定の設定の場合にのみ使用できます。実際の設定をご確認ください。

感度

これは、あらかじめ定義された領域を通過した許容ターゲットの身体部分の割合を表します。感度= 100 - S1/ST× 100。S1は、あらかじめ定義された領域を通過したターゲットの身体部分を意味します。STは、ターゲットの身体全体を表します。感度の値が高いほど、アラームが作動しやすくなります。

ターゲット有効性

有効性を高く設定すると、必要なターゲットの特徴がより明確になり、アラームの精度が向上します。特徴があまり明確ではないターゲットは検出されなくなります。

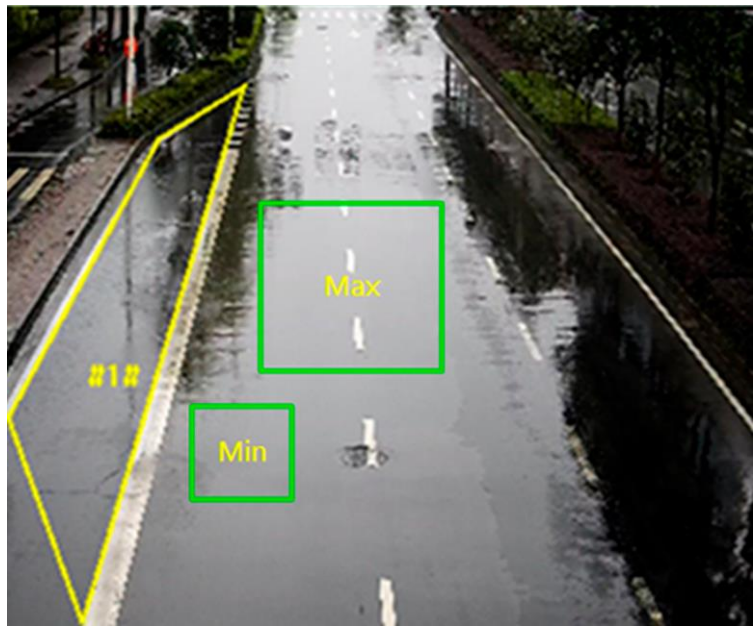

図10-4 ルール設定

5. オプション：上記の手順を繰り返して、複数のエリアのパラメータを設定することができます。

6. 武装スケジュールの設定については、*「武装スケジュールの設定」*を参照してください。リンク方法の設定については、*「リンク方法の設定」*を参照してください。

7. 保存をクリックします。

10.3.5 無人手荷物検出を設定

これは、あらかじめ定義された領域に残っているオブジェクトを検出するために使用されます。リンク方法は、オブジェクトが領域から離れてから、設定された時間経過後にトリガーされます。

開始前に

- **VCA** に移動し、アプリケーションを選択します。**スマートイベント**を選択し、**[次へ]** をクリックして機能を有効にします。
- HEOP 対応デバイスでは、**VCA** に移動して**スマートイベントを**インポートし、有効にしてください。

手順

1. **VCA** に移動し、**[→] を選択します。アプリケーションを設定します。→] を選択し、[スマートイベント] をクリックします。**

   →] を選択し、[無人手荷物検出] をクリックします。

2. **「有効」**にチェック**を入れます。**
3. **「追加」**をクリックしてルールを追加し、検出領域を設定します。
   1) 検出領域を描画します。 をクリックし、ライブビューをクリックして頂点を指定し、検出領域の境界を描画します。右クリックで描画を完了します。
   2) ターゲットの最小サイズと最大サイズを設定して検出精度を向上させます。最大サイズと最小サイズの間にあるサイズのターゲットのみが検出されます。「 」をクリックし、「 」をクリックし、ライブビュー内でマウスをドラッグして最小サイズと最大サイズのターゲットサイズを描画します。
   3) **オプション：[**] をクリックして、すべての設定領域を削除します。
4. パラメーターを設定します。

   感度

   感度は、許容されるターゲットの身体部分の、あらかじめ定義された領域に入った割合を表します。感度= 100 - S1/ST×100。S1 は、あらかじめ定義された領域を通過するターゲットの身体部分を意味します。ST は、ターゲットの身体全体を表します。感度の値が高いほど、アラームが作動しやすくなります。

   閾値

   領域内に残されたオブジェクトの時間を表します。オブジェクトが領域から離れ、設定された時間経過後にアラームが作動します。

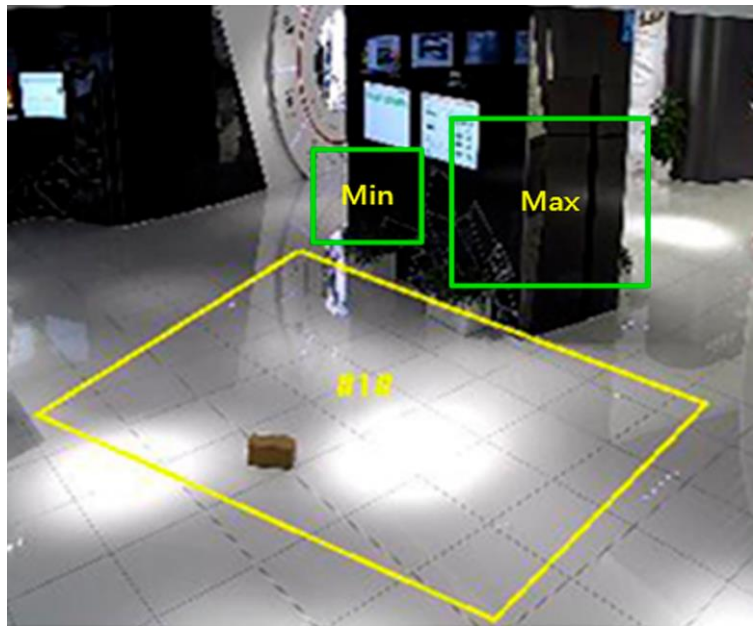

図10-5 ルール設定

5. **オプション：**上記の手順を繰り返して、複数の領域のパラメータを設定することができます。
6. 武装スケジュールの設定については、*「武装スケジュールの設定」*を参照してください。リンク方法の設定については、*「リンク方法の設定」*を参照してください。
7. **保存**をクリックします。

注意
この機能は一部のモデルでのみサポートされています。実際の表示はモデルによって異なります。

10.3.6 オブジェクト除去検出の設定

展示品など、あらかじめ設定した検出領域からオブジェクトが削除されたかどうかを検出します。検出された場合、デバイスはリンク動作を行い、スタッフは財産の損失を防ぐための措置を講じることができます。

開始前に

- **VCA** に移動し、アプリケーションを選択します。**スマートイベント**を選択し、**[次へ]** をクリックして機能を有効にします。
- HEOP 対応デバイスでは、**VCA** に移動して**スマートイベントを**インポートし、有効にしてください。

手順

1. **VCA** に移動し、**→ を選択します。アプリケーションを設定します。→ を選択し、スマートイベント→ オブジェクトの削除検出** を選択します。
2. **「有効」**にチェック**を入れます。**
3. **「追加」**をクリックしてルールを追加し、検出領域を設定します。
   1) 検出領域を描画します。⬡ をクリックし、ライブビューをクリックして頂点を指定し、検出領域の境界を描画します。右クリックで描画を完了します。

2) 検出精度を向上させるため、ターゲットの最小サイズと最大サイズを設定します。最大サイズと最小サイズの間にあるサイズのターゲットのみが検出されます。をクリックし、をクリックし、ライブビュー内でマウスをドラッグして最小サイズと最大サイズのターゲットサイズを描画します。

3) **オプション：**[ ]をクリックして、すべての設定領域を削除します。

4. パラメーターを設定します。

感度

感度は、許容されるターゲットの身体部分の、あらかじめ定義された領域に入った割合を表します。感度= 100 - S1/ST×100。S1 は、あらかじめ定義された領域を通過するターゲットの身体部分を意味します。ST は、ターゲットの身体全体を表します。感度の値が高いほど、アラームが作動しやすくなります。

閾値

領域からオブジェクトが除去された時間のしきい値。値を 10 に設定すると、オブジェクトが領域から 10 秒間消えた後にアラームが作動します。

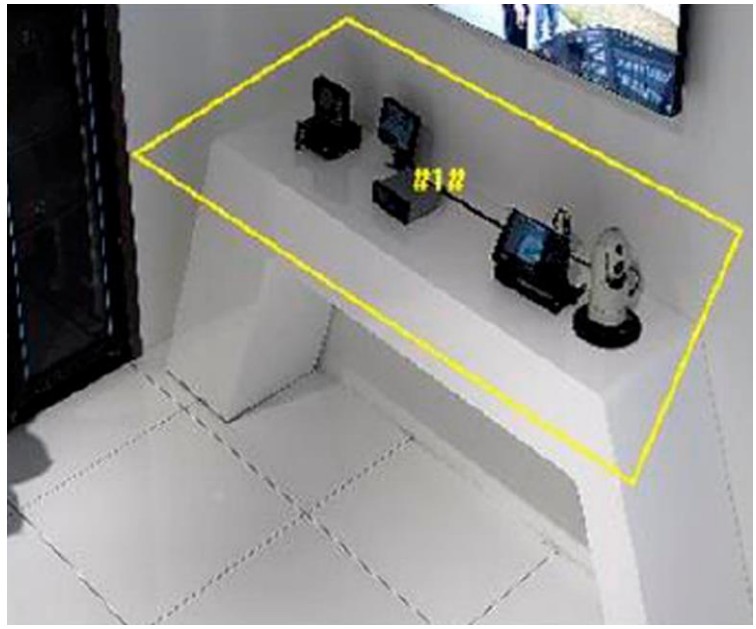

図10-6 ルール設定

5. オプション：上記の手順を繰り返して、複数の領域のパラメータを設定することができます。

6. 武装スケジュールの設定については、***「武装スケジュールの設定」***を参照してください。リンク方法の設定については、「***リンク方法の設定」を参照してください***。

7. **保存**をクリックします。

注意

この機能は一部のモデルでのみサポートされています。実際の表示はモデルによって異なります。

10.3.7 滞留検出の設定

あらかじめ設定したエリアにターゲットが滞留しているかどうかを検知します。ターゲットが設定エリアに滞留した時間が設定しきい値に達すると、デバイスはリンク動作を実行します。

開始前に

- **VCA** に移動し、アプリケーションを選択します。**スマートイベント**を選択し、**[次へ]** をクリックして機能を有効にします。
- HEOP 対応デバイスでは、**VCA** に移動して**スマートイベントを**インポートし、有効にしてください。

手順

1. **VCA** に移動し、**→ を選択します。アプリケーションを設定します。→ を選択し、スマートイベントを選択します。→ を選択し、不審者検知を選択します**。
2. **「有効」**にチェック**を入れます**。
3. **「追加」**をクリックしてルールを追加し、検出領域を設定します。
   1) 検出領域を描画します。「 」をクリックし、ライブビューをクリックして頂点を指定し、検出領域の境界を描画し、右クリックで描画を完了します。
   2) ターゲットの検出精度を向上させるため、ターゲットの最小サイズと最大サイズを設定します。最大サイズと最小サイズの間にあるサイズのターゲットのみが検出されます。 と をクリックし、ライブビュー内でマウスをドラッグして最小サイズと最大サイズのターゲットを描画します。
   3) **オプション：** [ ] をクリックして、すべての設定領域を削除します。
4. ルールを設

   定します。

   しきい値

   しきい値は、対象が領域内に留まる時間のしきい値を表します。1 つの対象がしきい値を超える時間、その対象が領域内に留まっていると、アラームが作動します。しきい値の値が大きいほど、アラームが作動するまでの時間が長くなります。

   感度

   感度は、許容されるターゲットの身体部分が、あらかじめ定義された領域に入った割合を表します。感度= 100 - S1/ST×100。S1 は、あらかじめ定義された領域を通過するターゲットの身体部分を意味します。ST は、ターゲットの身体全体を表します。感度の値が高いほど、アラームが簡単に作動します。

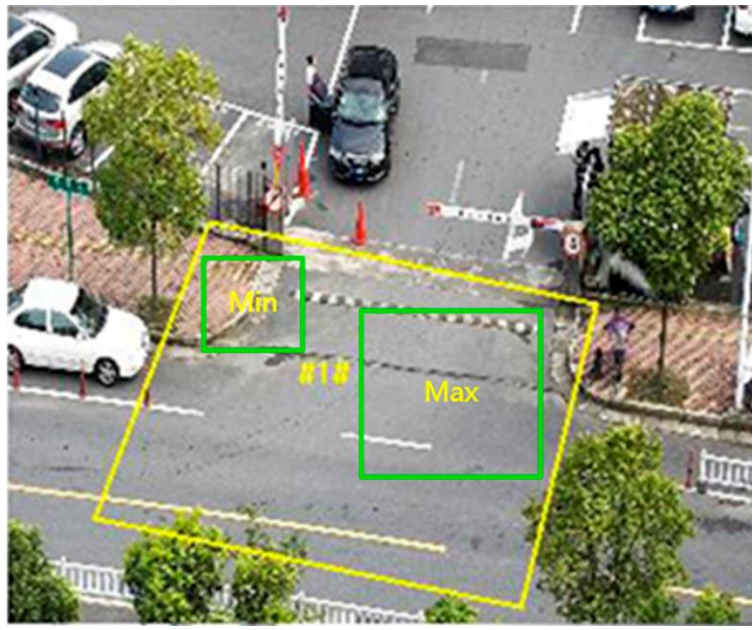

図10-7 ルール設定

5. **オプション：** 上記の手順を繰り返して、複数のエリアのパラメータを設定することができます。
6. 武装スケジュールの設定については、*「武装スケジュールの設定」*を参照してください。リンク方法の設定については、*「リンク方法の設定」*を参照してください。
7. **保存**をクリックします。

注

この機能は、特定のモデルでのみサポートされています。実際の表示はモデルによって異なります。

10.3.8 人集まり検出の設定

あらかじめ設定したエリアの人数を検知します。設定した人数を超えた場合、リンク動作を行うことができます。

開始前に

- **VCA** に移動し、アプリケーションを選択します。**スマートイベント**を選択し、**[次へ]** をクリックして機能を有効にします。
- HEOP 対応デバイスでは、**VCA** に移動して**スマートイベントを**インポートし、有効にしてください。

手順

1. **VCA** に移動→ **アプリケーションを設定→ スマートイベント→ 人物集中の検出** .
2. **「有効」**を選択します。
3. **「追加」**をクリックしてルールを追加し、検出領域を設定します。
   1) 検出領域を描画します。「◇」をクリックし、ライブビューをクリックして頂点を指定し、検出領域の境界を描画し、右クリックで描画を完了します。
   2) **オプション：** [🗑] をクリックして、すべての設定領域を削除します。

4. ルールを設定します。

パーセンテージ

これは、あらかじめ定義されたエリア内の人々の割合を表します。ライブビューの人々の割合が設定値を超えた場合、デバイスはアラームをトリガーします。

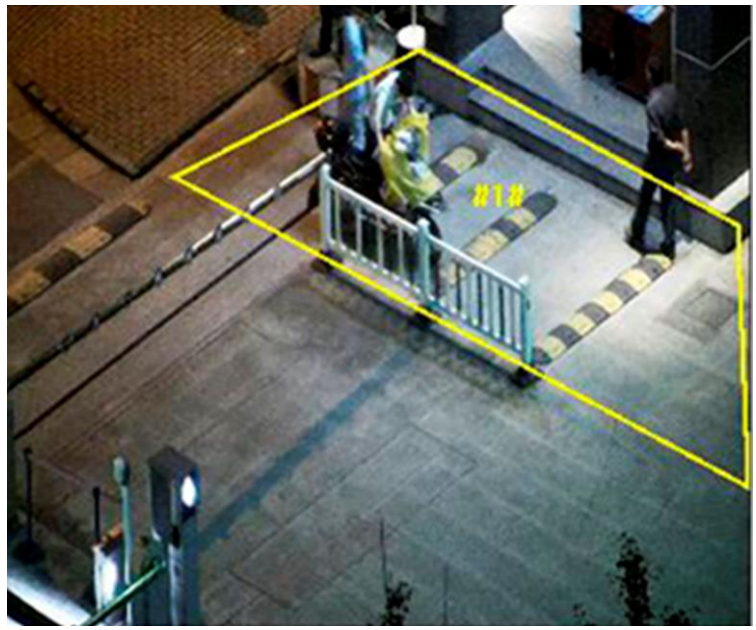

図10-8 ルール設定

5. オプション：上記の手順を繰り返して、複数のエリアのパラメータを設定することができます。

6. 武装スケジュールの設定については、*「武装スケジュールの設定」*を参照してください。リンク方法の設定については、*「リンク方法の設定」*を参照してください。

7. 保存をクリックします。

注意

この機能は一部のモデルでのみサポートされています。実際の表示はモデルによって異なります。

10.3.9 高速移動検出の設定

あらかじめ設定したエリア内で高速で動くターゲットがあった場合、デバイスはリンク動作を行い、アラームを鳴らします。

開始前に

- **VCA** に移動し、アプリケーションを選択します。**スマートイベント**を選択し、**[次へ]** をクリックして機能を有効にします。
- HEOP 対応デバイスでは、**VCA** に移動して**スマートイベントを**インポートし、有効にしてください。

手順

1. VCA に移動します。→ アプリケーションを設定します。→ スマートイベント→ **Fast Moving Detection** .

2.「**有効**」にチェック**を入れます**。

3. **「追加」**をクリックしてルールを追加し、検出領域を設定します。

1) 検出領域を描画します。をクリックし、ライブビューをクリックして頂点を指定し、検出領域の境界を描画します。右クリックで描画を完了します。

2) 検出精度を向上させるため、ターゲットの最小サイズと最大サイズを設定します。最大サイズと最小サイズの間にあるサイズのターゲットのみが検出されます。をクリックし、をクリックし、ライブビュー内でマウスをドラッグして最小サイズと最大サイズのターゲットサイズを描画します。

3) **オプション：**[ ]をクリックして、すべての設定領域を削除します。

4. ルールを設

定します。

感度

感度は、許容されるターゲットの身体の一部が、あらかじめ定義された領域に入った割合を表します。感度 = 100 - S1/ST × 100。S1 は、あらかじめ定義された領域を通過したターゲットの身体の一部を表します。ST は、ターゲットの身体全体を表します。感度の値が高いほど、アラームが簡単に作動します。

図10-9 ルール設定

5. **オプション：**上記の手順を繰り返して、複数のエリアのパラメータを設定することができます。

6. 武装スケジュールの設定については、***「武装スケジュールの設定」***を参照してください。リンク方法の設定については、***「リンク方法の設定」***を参照してください。

7. **保存**をクリックします。

注

この機能は一部のモデルでのみ対応しています。実際の表示はモデルによって異なります。

10.3.10 駐車検知機能

あらかじめ設定したエリア内の駐車違反を検知します。駐車時間が設定した閾値を超えると、リンク動作を行います。高速道路や一方通行道路に適用できます。

開始前に

- **VCA** に移動し、アプリケーションを選択します。**スマートイベント**を選択し、**[次へ]** をクリックして機能を有効にします。
- HEOP 対応デバイスでは、**VCA でスマートイベントを**インポートして有効にしてください。

手順

1. **VCA** に移動します**。→ アプリケーションを設定します。→ スマートイベント→ 駐車検出**。
2. **「有効」**を確認します。
3. **「追加」**をクリックしてルールを追加し、検出領域を設定します。
   1) 検出領域を描画します。をクリックし、ライブビューをクリックして頂点を指定し、検出領域の境界を描画します。右クリックで描画を完了します。
   2) ターゲットの最小サイズと最大サイズを設定して検出精度を向上させます。最大サイズと最小サイズの間にあるサイズのターゲットのみが検出されます。「」をクリックし、「」をクリックし、ライブビュー内でマウスをドラッグして最小サイズと最大サイズのターゲットサイズを描画します。
   3) **オプション：[** **]** をクリックして、すべての設定領域を削除します。
4. ルールを設

   定します。

   しきい値

   しきい値は、その地域における駐車時間のしきい値を表します。駐車時間がしきい値を超えると、アラームが作動します。しきい値の値が大きいほど、アラームが作動するまでの時間が長くなります。

   感度

   感度は、許容可能なターゲットのうち、あらかじめ定義された領域に入った部分の割合を表します。感度= 100 - S1/ST× 100。S1 は、あらかじめ定義された領域を通過するターゲット部分を表します。ST は、ターゲット全体を表します。感度の値が高いほど、アラームが簡単に作動します。

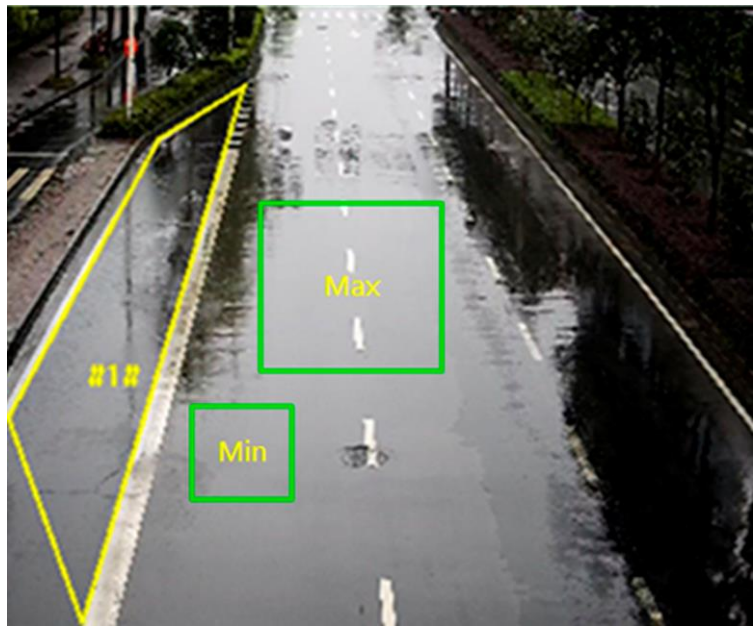

図10-10 ルール設定

5. **オプション：**上記の手順を繰り返して、複数の領域のパラメータを設定することができます。
6. 武装スケジュールの設定については、*「武装スケジュールの設定」*を参照してください。リンク方法の設定については、*「リンク方法の設定」*を参照してください。
7. **保存**をクリックしてください。

注意
この機能は一部のモデルでのみサポートされています。実際の表示はモデルによって異なります。

10.4 顔キャプチャ

設定したルールエリア内のルールに該当する顔をキャプチャし、キャプチャした画像をアップロードします。

注意
- 一部のデバイスモデルでは、まずVCAページでこの機能を有効にする必要があります。
- この機能は、特定のデバイスモデルでのみサポートされています。

10.4.1 顔キャプチャの設定

設定した領域に表示される顔をキャプチャすることができます。

開始前に

- **VCA** に移動し、アプリケーションを選択します。**顔キャプチャ**を選択し、**[次へ]** をクリックして機能を有効にします。
- HEOP 対応デバイスでは、**VCA** に移動して**顔キャプチャを**インポートし、有効にしてください。

手順

1. **VCA** に移動します**。→ アプリケーションを設定します。→ 顔キャプチャ→ ルール**。
2. **「有効」**にチェックを入れてルール設定を有効にします。
3. をクリックして、顔キャプチャを有効にする検出領域を描きます。ライブビューウィンドウで、左クリックで端点を指定して領域を描き、右クリックで領域の描画を終了します。描画する領域は、ライブビュー画像の 1/2 から 2/3 程度にすることをお勧めします。
4. 瞳孔距離を描画します。

   最低瞳孔距離

   をクリックして、最小瞳孔距離を描きます。ビデオ画像内の顔の瞳孔距離が最小瞳孔距離よりも小さい場合、その顔は検出されません。

   最大瞳孔距離

   をクリックして、最大瞳孔距離を描画します。ビデオ画像内の顔の瞳孔距離が最大瞳孔距離よりも大きい場合、その顔は検出されません。

   テキストフィールドに距離の値を入力することもできます。
5. **オプション：**シールド領域の設定については、*「シールド領域の設定」*を参照してください。
6. 武装スケジュールの設定については、*「武装スケジュールの設定」*を参照してください。リンク方法の設定については、*「リンク方法の設定」*を参照してください。
7. **保存**をクリックします。
8. オーバーレイおよびキャプチャの設定については、「*オーバーレイおよびキャプチャ」*を参照してください。高度なパラメータの設定については、*「顔キャプチャアルゴリズムのパラメータ」*を参照してください。

結果

キャプチャした画像は、**再生→ 画像で**表示およびダウンロードできます。詳細については、*「画像のダウンロード表示と」*を参照してください。

10.4.2 オーバーレイとキャプチャ

キャプチャパラメーターと、ストリームと画像に表示する情報を設定します。

ストリームにVCA情報を表示

ストリームにスマート情報を表示します。これにはターゲットとルール情報が含まれます。

アラーム画像にターゲット情報を表示

アラーム画像にターゲット情報をオーバーレイ表示します。

背景画像設定

ターゲット画像と比較して、背景画像は追加の環境情報を提供するシーン画像です。背景画像の画質と解像度を設定できます。背景画像を監視センターにアップロードする必要がある場合は、**[背景のアップロード] を**チェックします。一部のデバイスでは、**[顔画像] を**チェックして、キャプチャした顔画像をアップロードすることもできます。

ターゲット画像設定

カスタム、顔写真、上半身写真、全身写真から選択可能です。

注意

カスタムを選択すると、**幅、頭の高さ、体の**高さを必要に応じてカスタマイズできます。画像の高さを固定するには、

[画像の高さを固定] **を**チェックします。

顔の美化

顔美化] をチェックし、必要に応じて美化レベルを調整します。

注意

顔美化は、撮影した顔写真をわずかに調整し、顔のノイズを軽減します。

顔の強化

顔強調」にチェックを入れると、暗い場所でもより鮮明な顔写真を撮影することができます。

テキストオーバーレイ

必要な項目をチェックして、撮影された写真に表示する順番を調整することができます。**デバイス番号とカメラ情報の**設定については、*「カメラ情報の設定」*をご覧ください。

10.4.3 顔キャプチャアルゴリズムのパラメータ

顔キャプチャ機能のアルゴリズムライブラリのパラメータを設定および最適化するために使用します。

バージョン

現在のアルゴリズムのバージョンを表します。

キャプチャパラメーター

ベストショット

ターゲットが検出領域から離れた後の最良のショットです。

キャプチャ閾値

キャプチャとアラームをトリガーする顔の品質を表します。値が高いほど、キャプチャとアラームをトリガーするための品質が高くなります。

キャプチャ回数

これは、設定されたエリアに顔がいる間にその顔がキャプチャされる回数を指します。デフォルト値は 1 です。

クイックショット

顔写真の評価値がクイックショットのしきい値よりも高い場合、その顔写真がキャプチャされ、アップロードされます。それ以外の場合、最大キャプチャ間隔に達した評価値が最も高い写真がアップロード用に選択されます。

クイックショット閾値

クイックショットをトリガーする顔の品質を指します。

最大撮影間隔

1回のクイックショットの最大撮影時間を指します。

キャプチャ時間

設定されたエリアに顔がいる間にその顔がキャプチャされる回数です。

重複顔の削除

この機能を使用すると、特定の顔の繰り返しキャプチャをフィルタリングすることができます。

重複削除の類似度閾値

重複削除ライブラリ内の画像と新しくキャプチャされた顔の類似度です。類似度値が設定値よりも高い場合、キャプチャされた画像は重複顔とみなされ、削除されます。

重複削除ライブラリのグレード閾値

顔評価のしきい値で重複チェックを行います。顔評価が設定値以上になると、キャプチャした顔を重複削除ライブラリに保存されている顔写真と比較します。

重複削除ライブラリの更新時間

各顔画像が重複削除ライブラリに追加されてから削除されるまでの時間。

顔の露出

チェックボックスをオンにすると、顔の露出チェックが有効になります。

参照明るさ

顔露出モードでの顔の基準明るさ。顔が検出されると、カメラは設定した値に応じて顔の明るさを調整します。値が高いほど、顔は明るくなります。

最低露出時間

カメラが顔を露出する最小時間。

注意

顔認識機能が有効になっている場合、WDR機能を無効にし、手動アイリスを選択してください。

顔フィルタリング時間

カメラが顔を検出してからキャプチャを行うまでの時間間隔です。検出された顔が、設定されたフィルタリング時間よりも短い時間、シーン内に留まっている場合、キャプチャはトリガーされません。たとえば、顔フィルタリング時間が5秒に設定されている場合、カメラは、顔が5秒間シーン内に留まっているときに、検出した顔をキャプチャします。

注意

顔フィルタリング時間（0秒以上）が長いと、実際のキャプチャ時間が上記の設定値よりも短くなる可能性があります。

顔姿勢フィルター

顔姿勢フィルターは、特定の姿勢の顔をフィルタリングすることができます。スライダーの右側の数字は、顔キャプチャアクションで許容される姿勢の角度を表しています。このフィルターを設定する際に、顔の向きを示す図を表示するには、[ ] をクリックしてください。

特徴情報のアップロード

特徴とは、アルゴリズムが顔画像から識別できる特徴情報のことを指します。この情報をアップロードする機能をチェックしてください。

パラメーターを復元

デフォルト設定に戻す

「復元」をクリックすると、高度な設定のすべての設定が工場出荷時のデフォルトに戻ります。

10.4.4 シールド領域の設定

シールド領域では、設定したスマート機能ルールを無効にする特定の領域を設定することができます。

手順

1. **シールド領域**を選択します。
2. 「 」をクリックしてシールド領域を描画します。この手順を繰り返し、追加のシールド領域を設定します。
3. **オプション：**描画した領域を選択してクリックし、[ ] をクリックして、選択した描画領域を削除します。
4. **オプション：**[ ] をクリックして、描画した領域をすべて削除します。
5. **「保存」**をクリックします。

10.5 ユーザー管理

人管理は、あらかじめ定義した領域内の人数や変化を検知・分析するために使用されます。入口や出口、スーパーマーケットなどに適用できます。

注

- 一部のデバイスモデルでは、まずVCAページで「**People Management**」を有効にする必要があります。
- この機能は、特定のデバイスモデルでのみサポートされています。

10.5.1 エリア別人数カウント

あらかじめ定義したエリアの人数をカウントし、人数変化や混雑状況を検知します。人数異常や待ち時間異常が発生すると、デバイスはアラームをトリガーすることができます。

「人密度設定」を参照して、人密度検出を設定してください。

人数異常検知の設定については、「人数異常検知の設定」を参照してください。

待ち時間異常検知を設定するには、***「待ち時間異常検知」***を参照してください。

人密度を設定する

この機能は、設定されたルール領域の人密度レベルを検出します。

開始前に

- **VCA** に移動します。**→ [アプリケーション] を選択し**、[**People Management]** を選択して **[Next]** をクリックし、機能を有効にします。
- HEOP 対応デバイスでは、**VCA** に移動して **People Management** をインポートし、有効にしてください。

手順

1. **VCA** に移動します**。→ アプリケーションを設定します。→ 人数管理→ エリア別人数カウント→ ルール**。

2. 「**追加**」をクリックしてルールを追加し、その名前を設定します。

3. ルールを設定します。

図10-11 ルールを設定

人員数 OSD

ライブビューウィンドウにリアルタイムの人数を表示します。マウスをドラッグしてOSDウィンドウの位置を調整できます。

注

人密度アラームは、**例外ごとのアラーム回数**、**アラーム間隔**、および**最初のアラーム遅延**の設定をサポートしていません。

4. クリッ[ク] ライブビューウィンドウで領域を描画し、ライブビューウィンドウ内の終了点を左クリックしてセットルール領域の境界を定義し、右クリックで描画を完了します。

注意

- 同時に設定できる領域は最大 8 つまでです。
- 領域が重ならないようにご注意ください。

5. **人密度アラーム**を有効にするには、**人密度アラームに**チェックを入れます。

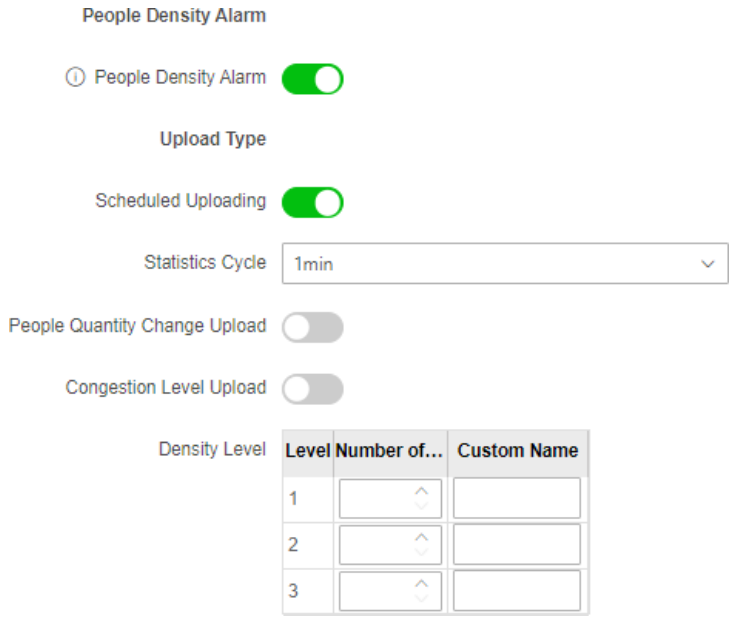

図 10-12 人数アラーム

スケジュールされたアップロード

デバイスは、設定された統計サイクル内で人密度情報をアップロードします。

人数の変化アップロード

デバイスは、設定されたルール区域内で人数に変化が生じた場合、その変化情報をアップロードします。

混雑レベルアップロード

設定ルール区域の混雑レベルに変化があった場合、混雑情報をアップロードします。

密度レベル人数

設定ルールエリアの人数の下限を入力して、各レベルの範囲を設定します。

カスタム名

レベルに付ける名前。

注

- **カスタム名の前の人数を**設定します。
- 最大 3 つのレベルを設定できます。レベル 1 からレベル 3 にかけて密度が増加します。

6. 武装スケジュールを設定します。***武装スケジュール設定***を参照してください。
7. リンク方法を設定します。***リンク方法の設定***を参照してください。
8. **保存**をクリックします。

9. オプション：テキストオーバーレイを設定します。詳細な設定については、「*オーバーレイとキャプチャ*」を参照してください。

10. オプション：バージョンを表示し、フィルタリング条件を設定します。詳細設定については、*「詳細設定」*を参照してください。

人数異常検知を設定します。

この機能は、設定されたルール領域内の人数を検知し、アラーム発生条件に該当した場合にアラームを鳴らします。

開始前に

- **VCA** に移動し、**→ を選択します。Application を選択し**、**People Management** を選択して **Next** をクリックし、機能を有効にします。
- HEOP をサポートするデバイスでは、**VCA** に移動して **People Management** をインポートし、有効にしてください。

手順

1. VCA に移動します**。→ アプリケーションを設定します。→ People Management→ エリア別人数カウント→ ルール**。

2.「追加」をクリックしてルールを追加し、その名前を設定します。

3. ルールを設定します。

図10-13 ルールを設定する

人数のOSD

ライブビューウィンドウにリアルタイムの人数を表示します。マウスをドラッグしてOSDウィンドウの位置を調整できます。

例外ごとのアラーム回数

アラームがトリガーされた後のアラーム回数です。チェックボックスをオンにして回数を設定しないと、デバイスはアラームを送信し続けます。

アラーム間隔

設定された**アラーム間隔**内では、同じアラームはアップロードされません。

最初のアラーム遅延

最初のアラームがトリガーされると、設定された時間後にアラームがアップロードされます。

4. 「」をクリックしてライブビューウィンドウに領域をドラッグし、ライブビューウィンドウ内の終了点を左クリックして設定したルールの境界を定義し、右クリックで描画を完了します。

注意

- 同時に最大 8 つの領域を設定できます。
- 領域が重ならないようにご注意ください。

5. 「**地域の人物例外アラーム**」をチェックし、「**アラームトリガー条件**」と「**アラームしきい値**」を設定します。

注

- 「**無人の状況を無視**」を有効にすると、そのエリアに人がいない場合、デバイスはアラームを発しません。
- この機能は、値が設定されたアラームしきい値未満であり、その領域内に人がいない場合に、潜在的なアラーム状態をフィルタリングします。

  アラームしきい値未満で、その領域内に人がいない場合に発生するアラームをフィルタリングできます。

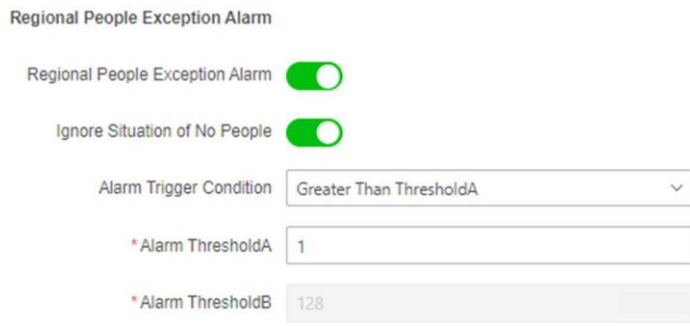

図 10-14 エリアの人物例外アラーム

6. アラームスケジュールを設定します。***アラームスケジュール設定***を参照してください。
7. リンク方法を設定します。***リンク方法の設定***を参照してください。
8. **保存**をクリックします。
9. **オプション：**テキストオーバーレイを設定します。詳細設定については、***「オーバーレイとキャプチャ」***を参照してください。
10. **オプション：**バージョンを表示し、フィルタリング条件を設定します。詳細設定については、***「詳細設定」***を参照してください。

待ち時間異常検知

この機能は、設定されたルール領域の待機時間を検出し、待機時間がアラーム発生条件を満たした場合にアラームを発生させます。

開始前に

- Go to **VCA→ アプリケーションを選択し**、**[People Management]** を選択して **[Next]** をクリックして機能を有効にします。
- HEOP をサポートするデバイスでは、**VCA** に移動して **People Management** をインポートして有効にしてください。

手順

1. **VCA** に移動します。**→ アプリケーションを設定します。→ People Management→ エリア別人数カウント→ ルール**。
2. **「追加」**をクリックしてルールを追加し、その名前を設定します。
3. ルールを設定します。

図10-15 ルールを設定する

人員数 OSD

ライブビューウィンドウにリアルタイムの人数を表示します。マウスをドラッグしてOSDウィンドウの位置を調整できます。

例外ごとのアラーム回数

アラームが作動した後のアラームの回数です。チェックせずに時間を設定しない場合、アラームは繰り返し鳴ります。

アラーム間隔

設定した**アラーム間隔**内に、同じアラームはアップロードされません。

最初のアラーム遅延

最初のアラームが作動すると、設定された時間後にアラームがアップロードされます。

注意

滞留時間例外アラームは、**アラームトリガー条件**が**しきい値 A より大きい**場合にのみ、**例外ごとのアラーム回数**、**アラーム間隔**、および**最初のアラーム遅延**の設定をサポートします。

4. 「」をクリックしてライブビューウィンドウに領域を描画し、ライブビューウィンドウの終了点を左クリックして設定ルールの境界を定義し、右クリックで描画を完了します。

注意

- 同時に最大 8 つの領域を設定できます。
- 領域が重ならないようにしてください。

5. **「ドウェル時間例外アラーム」**をチェックし、**「アラームトリガー条件」**と「**アラームしきい値**」を設定します。

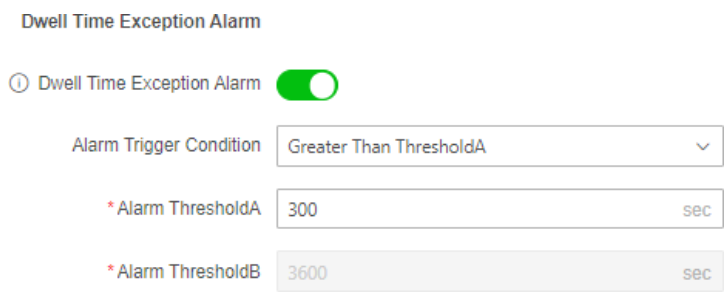

図 10-16 滞留時間例外アラーム

6. アラームのスケジュールを設定します。*アラームのスケジュール設定*を参照してください。
7. リンク方法を設定します。*リンク方法の設定*を参照してください。
8. **保存**をクリックします。
9. **オプション：**テキストオーバーレイを設定します。詳細な設定については、「*オーバーレイとキャプチャ*」を参照してください。
10. **オプション：**バージョンを表示し、フィルタリング条件を設定します。詳細設定については、*「詳細設定」*を参照してください。

10.5.2 オーバーレイとキャプチャ

Go to **VCA→ People Management→ Overlay & Capture**.キャプチャした画像にオーバーレイする情報をチェックします。↑ ↓をクリックして、順番を調整することもできます。

10.5.3 詳細設定

人管理機能の高度なパラメーターを設定し、**保存**をクリックします。**バージョン**

現在のアルゴリズムバージョンを表します。

アルゴリズムモード

インストール環境に応じてモードを選択します。

フィルター

ターゲットサイズ

これは、ターゲット検出ウィンドウのサイズを表します。このピクセルよりも大きいターゲットは、実際のターゲットとしてカウントされます。特定の固定ターゲットの誤報を除去することができます。

移動量

これはターゲットの移動量またはターゲットの幅を表します。ターゲットの移動量が設定されたパーセンテージ未満の場合、そのターゲットはカウントされません。

最低待機時間

設定値未満の待機時間はフィルタリングされます。

信頼度

閾値が高いほど、ターゲットの検出が困難になりますが、精度も高くなります。

注

フィルタリング設定は専門家に操作してください。フィルタ設定は、検出アルゴリズムを調整して検出範囲、感度などを変更できます。

10.6 人数のカウント

人数のカウントは、特定のエリアに出入りする人の数を測定するために使用されます。

注

- 一部のデバイスモデルでは、まずVCAページで**「人数のカウント」**を有効にする必要があります。
- この機能は、特定のデバイスモデルでのみサポートされています。

10.6.1 人流量計測ルールを設定する

検出ルールとアルゴリズムのパラメータを設定すると、デバイスはルールエリアに出入りする人数を計算し、リンク方法をトリガーして、データを自動的にアップロードします。

開始前に

- **VCA** に移動し、アプリケーションを選択します。**People Counting** を選択し、**[Next]** をクリックして機能を有効にします。
- HEOP 対応デバイスでは、**VCA** に移動して **People Counting** をインポートし、有効にしてください。

手順

1. **VCA** に移動します。**→ アプリケーションを設定します**。**→ People Counting→ Rule**
2. **「有効」**にチェックを入れて機能を有効にします。
3. **「追加」**をクリックして検出領域を追加します。
4. 「」をクリックして、ポリゴン検出領域（カウント領域）を描画します。ライブビューウィンドウで終了点を左クリックし、右クリックで描画を完了します。
5. 「／」をクリックして検出ラインを描画します。矢印は入力方向を示しています。方向を変更するには「」をクリックしてください。

注意

検出精度を向上させるため、以下のルールに従って検出領域を描画してください。

- 検出領域は、アクセスに出入りする人を完全にカバーする必要があります。
- 検出線は、赤色の検出領域内に完全に含まれており、通過する人の経路と垂直に配置する必要があります。

6. オプション：検出エリアと検出ラインを調整します。

「 」**をクリックし、**選択した検出領域または線をクリアします。

「 」**をクリックし、**すべての検出領域と線をクリアします。

7. オプション：上記の手順を繰り返して、最大 3 つの検出エリアと対応する検出ラインを描きます。

8. 人計数パラメーターを設定します。

OSDオーバーレイコンテンツ

ライブビュー画像に表示するカウントデータの種類をドロップダウンリストから選択し、ライブビュー画像内の人数カウントデータの表示位置を調整します。

注意

OSDオーバーレイは、現在の日の人の数のみをカウントします。データは、デバイスが再起動された場合または日次リセット時間に自動的にクリアされます。

日次リセット時間

デバイスは、デフォルト設定で毎日00:00にデータをクリアします。ドロップダウンリストから時間を選択できます。選択後、選択した時間ごとに毎日自動的にカウントデータがクリアされます。

「手動リセット」をクリックすると、手動でデータリセットを実行し、現在の人のカウントデータをクリアできます。

9.「保存」をクリックします。

10. アラーム設定スケジュールを設定します。***アラーム設定スケジュール設定***を参照してください。

11. リンク方法を設定します。***リンク方法の設定***を参照してください。

12.「保存」をクリックします。

13. オプション：人数のカウントデータのアップロードパラメータを設定します。

データアップロードをクリックしてインターフェースに入ります。設定が完了したら、**保存**をクリックします。

リアルタイムデータアップロード

リアルタイムデータをプラットフォームに送信してください。

データを定期的にアップロードする

データ統計サイクルを設定すると、乗客の流れの計数データが**データ統計サイクル**に従って一定間隔でプラットフォームにアップロードされます。

14. オプション：人数のカウントに関する詳細パラメータを設定します。

詳細をクリックしてインターフェースに入ります。設定が完了したら、**保存**をクリックします。

バージョン

現在のアルゴリズムバージョンを表します。

ストレージデータをクリア

デバイスに保存されているすべての人数カウントデータを削除します。この機能は慎重に使用してください。

結果

- ターゲットが進入方向に沿って検出エリアを通過し、検出ラインを通過した場合、そのターゲットは進入数としてカウントされます。
- ターゲットが退出方向に沿って検出エリアを横切り、検出ラインを通過した場合、退出数としてカウントされます。

10.7 道路交通

道路交通の監視には、車両検出および混合交通検出を使用できます。このデバイスは、通過する自動車および非自動車を撮影し、撮影画像とともに関連情報をアップロードします。

注

- 一部のデバイスモデルでは、VCAページで最初に**「道路交通」**を選択する必要があります。
- この機能は、特定のデバイスモデルでのみサポートされています。

10.7.1 車両検出の設定

設定された車線に進入した車両を検知し、車両の画像とナンバープレートを撮影して保存することができます。アラームが作動し、撮影画像がアップロードされます。

開始前に

- **VCA** に移動し、アプリケーションを選択します。**「Road Traffic」**を選択し、**「Next」**をクリックして機能を有効にします。
- デバイスが正しくインストールされていることを確認してください。
- 画像パラメータが正しく設定されていることを確認してください。
- キャプチャされたナンバープレートの画像が十分に鮮明であることを確認してください。

手順

1. **VCA** に移動します**。→ アプリケーションを設定します。→ 道路交通→ ルール**、そして検出タイプとして**「車両検出」**を選択します。
2. **「有効」**にチェック**を入れます**。
3. 動作モードを選択します。

   入口/出口

   検出された車両のナンバープレート情報は、車両が検出領域を通過し、入口/出口で検出をトリガーした際にアップロードされます。

   市街地道路

車両が検出エリアを通過し、市道で検出をトリガーした際に、検出された車両のナンバープレート情報がアップロードされます。

アラーム入力

入力アラームがナンバープレートの撮影と認識動作をトリガーすることを意味します。

注

- **アラーム**入力が選択されている場合、アラーム入力 A<-1 は自動的に車両検出のトリガーに割り当てられ、そのアラームタイプは常に NO になります。
- A<-1 アラーム入力を車両検出のトリガーに使用する場合、他の基本イベントには使用できません。
- **アラーム入力**を選択して保存すると、A<-1 に設定されていたリンク方法はキャンセルされます。

4. レーンの総数を選択してください。

5. 車線をクリックしてドラッグして位置を設定するか、線の端をクリックしてドラッグして線の長さと角度を調整します。

青い検出線はナンバープレートのトリガーラインであり、主にエントランス/エグジットシーンでキャプチャ効率を向上させるために使用されます。ナンバープレート付きの車両が通過できるように、画面の下中央部に配置することをおすすめします。

6. 画像内の車両のサイズが赤い枠のサイズに近くなるように、カメラのズーム比を調整してください。調整できるのは赤い枠の位置のみです。

注意

各レーンごとに1つのナンバープレートのみを同時に検出できます。

7. **エリア**と**国/地域**を選択してください。

8. 検出モードを設定してください。

車両優先度

デバイスはまず車両の重量を測定し、次にナンバープレートを認識して分析を行います。これにより精度が向上しますが、設置環境が不十分な場合、一部の結果が失われることがあります。

ナンバープレート & 車両

ナンバープレートと車両モードでは、デバイスはナンバープレートと車両を同時に検出し、アラーム情報と撮影した画像をアップロードします。

注意

設置や補助照明に問題がない場合は、**車両**優先モードを選択することをお勧めします。ナンバープレートの認識に関する問題が解決したら、モードを「**ナンバープレート＆車両**」モードに切り替えることができます。

9. 「**重複したナンバープレートを削除**」にチェックを入れ、**時間間隔**を設定します。デフォルトの時間間隔は4分です。

10. 「**保存**」をクリックします。

11. 「**武装スケジュールとリンク方法**」に移動します。ブロックリスト、許可リスト、その他のリストについて、武装スケジュールとリンク方法を個別に設定できます。

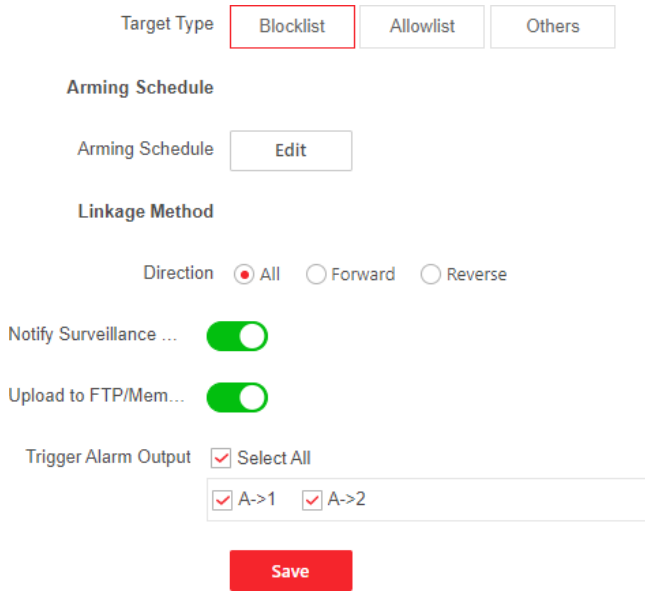

図 10-17 警報設定とリンク方法

1) ブロックリスト、許可リスト、その他のリストを選択します。
2) 武装スケジュールを設定します。詳細については*「武装スケジュールの設定」*を参照してください。
3) リンク方法を設定します。各ルールに対応するリンク方法のチェックボックスをオンにし、**保存**をクリックして設定を保存します。

方向

選択した方向に向かって移動する車両のみが、選択したリンク方法をトリガーします。

すべて

すべては、すべての移動方向の車両が考慮されることを意味します。特別な用途がない場合は、**「すべて」**を選択することを強くお勧めします。

前方

前方は、車両がカメラに向かって移動することを意味します。

後退

後退とは、車両がカメラから離れる方向に移動することを意味します。

Wiegand リンク方法

このデバイスは、Wiegand プロトコルを介してサードパーティのプラットフォームにレポートを送信することができます。

デバイスが Wiegand インターフェースに対応しており、Wiegand インターフェースで正しく接続されていることを確認してください。

システム設定で、Wiegand が有効になっており、プロトコルが正しく設定されていることを確認してください。詳細については、***Wiegand*** を参照してください。

Wiegand リンクを有効にし、外部デバイスに接続されている Wiegand インターフェースを選択してください。

リンクは、検出された車両の走行方向が設定された方向と同じ場合にのみトリガーされます。

12. **道路交通→ オーバーレイ＆キャプチャ]** に移動して、キャプチャした画像の画像パラメータとテキストオーバーレイを設定します。詳細については、*「オーバーレイとキャプチャ」* を参照してください。
13. ライセンスプレートブロックリストとアロリストのインポートまたはエクスポート。詳細については、*「ブロックリストインポートまたはエクスポート」とアロリストの*を参照してください。

10.7.2 混合交通検出ルールを設定する

設定された車線に進入した自動車および非自動車を検知し、ターゲットの画像を撮影して保存することができます。アラームが作動し、撮影画像がアップロードされます。

開始前に

- **VCA** に移動し、アプリケーションを選択します。**「道路交通」**を選択し、**「次へ」**をクリックして機能を有効にします。
- デバイスが正しくインストールされていることを確認してください。
- 画像パラメータが正しく設定されていることを確認してください。

手順

1. **VCA** に移動します**。→ アプリケーションを設定します。→ 道路交通→ ルール**、そして検出タイプとして**「混合交通検出」**を選択します。
2. **「有効」**にチェック**を入れます**。
3. 車線の総数を選択します。
4. 車線をクリックしてドラッグして位置を設定するか、線の端をクリックしてドラッグして線の長さと角度を調整します。

   青い検出線はナンバープレートのトリガー線であり、主に「入口/出口」シーンでキャプチャ効率を向上させるために使用されます。画面の下中央に配置することをおすすめします。これにより、ナンバープレート付きの車両が完全に通過できることを確認できます。
5. 画像内の車両の大きさが赤い枠の大きさに近くなるように、カメラのズーム率を調整してください。調整できるのは赤い枠の位置のみです。

注意
各車線ごとに1つのナンバープレートのみを同時に撮影できます。

6. **領域**と**国/地域**を選択してください。
7. **重複したナンバープレートを削除するに**チェックを入れ、**時間間隔**を設定します。デフォルトの時間間隔は4分です。
8. **保存**をクリックしてください。

9. 「**武装スケジュールとリンク方法**」に移動します。ブロックリスト、許可リスト、その他のリストについて、武装スケジュールとリンク方法を個別に設定できます。

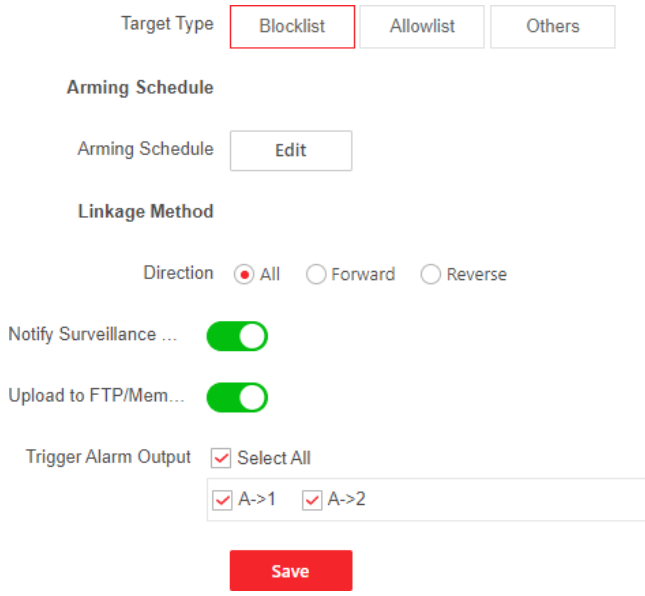

図 10-18 アーミングスケジュールとリンク方法

1) ブロックリスト、アロリスト、その他のリストを選択します。
2) 武装スケジュールを設定します。詳細については ***「武装スケジュールの設定」*** を参照してください。
3) リンク方法を設定します。各ルールに対応するリンク方法のチェックボックスをオンにし、**[保存]** をクリックして設定を保存します。

方向

選択した方向に向かって移動する車両のみが、選択したリンク方法をトリガーします。

すべて

すべてとは、すべての移動方向の車両が対象となることを意味します。特別な用途がない場合は、**すべて**を選択することを強くお勧めします。

前方

前進とは、車両がカメラに向かって進むことを意味します。

後退

後進とは、車両がカメラから離れる方向への移動を意味します。

Wiegand リンク方法

このデバイスは、Wiegand プロトコルを介してサードパーティのプラットフォームにレポートを送信することができます。

デバイスが Wiegand インターフェースに対応しており、Wiegand インターフェースで正しく接続されていることを確認してください。

Wiegand が有効になっており、システム設定でプロトコルが正しく設定されていることを確認してください。詳細については、***Wiegand*** を参照してください。

Wiegand リンクを有効にし、外部デバイスに接続されている Wiegand インターフェースを選択します。

検出された車両の走行方向が設定された方向と同じ場合にのみ、リンクがトリガーされます。

10. **道路交通→ オーバーレイ＆キャプチャ]** に移動して、キャプチャした画像の画像パラメータとテキストオーバーレイを設定します。詳細については、*「オーバーレイとキャプチャ」* を参照してください。

11. ナンバープレートブロックリストとアロリストをインポートまたはエクスポートします。詳細については、*「ブロックリストとインポートまたはエクスポート」アロリストの*を参照してください。

10.7.3 オーバーレイとキャプチャ

車両検出および混合交通検出でキャプチャした画像の画像パラメータを設定できます。

VCA に移動し、「**Road Traffic**」を選択します。

VCA に移動し、**[→] を選択します。アプリケーションを設定します。→ Road Traffic→ Overlay & Capture** 。

注

機能はデバイスモデルによって異なります。

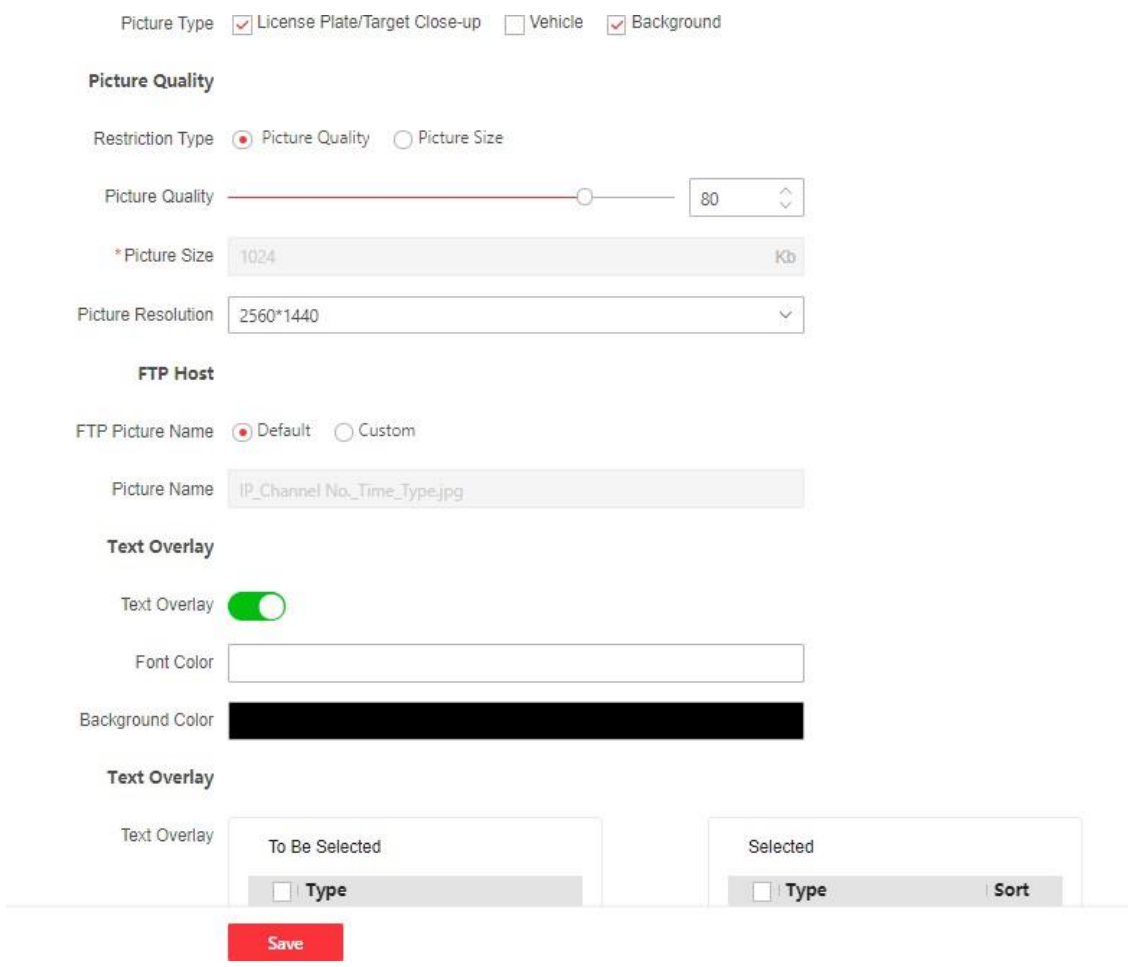

図10-19 オーバーレイ & キャプチャ

画像品質

値が大きいほど画像が鮮明になりますが、より多くのストレージ容量が必要になります。

画像サイズ

値が大きいほど、必要なストレージ容量も大きくなります。また、ネットワーク伝送の要件レベルも高くなります。

画像解像度

撮影される背景画像の解像度。

画像キャプチャ間隔

カメラは、アラームを連続的にトリガーし、各間隔でキャプチャした画像をアップロードすることができます。**キャプチャ間隔**を確認し、間隔を設定してください。

FTP画像名

車両検出と混合交通検出でキャプチャされた画像の命名規則をFTPサーバーで設定できます。

デフォルトを選択すると、デフォルトのルールが使用されます。

「カスタム」を選択し、画像名の情報を設定し、画像名パラメーターの順序を調整するには「↑ ↓」をクリックします。カスタムモードで**「Capture Time」**が選択されていない場合、同じ車両によって後からトリガーされた画像は、同じ画像名のため、以前にキャプチャされた画像と置き換えられます。

設定の詳細については、「***FTPの設定***」を参照してください。

注意

テキストオーバーレイ

キャプチャした画像にカメラ、デバイス、または車両情報をオーバーレイ表示し、[↑ ↓] をクリックしてオーバーレイテキストの順序を調整することができます。

色ボックスを選択してフォントの色と背景の色を設定し、ポップアップパレットまたはドロップダウンボックスから目的の色をクリックします。

10.7.4 ブロックリストと許可リストのインポート/エクスポート

ブロックリストと許可リストは、必要に応じてインポートおよびエクスポートすることができ、このインターフェースでリストの内容を確認することができます。

手順

1. **「インポート」**をクリックして、選択したファイルをインポートします。
2. 「🗀」をクリックして、PCのローカルディレクトリを開きます。
3. ブロックリストと許可リストのファイルを探し、クリックして選択します。**「開く」**をクリックして確認します。

注意

- インポートするファイルは、カメラで必要なファイルテンプレートと一致している必要があります。テンプレートとして、カメラから空のブロックリストおよび許可リストファイルをエクスポートし、その内容を入力することをお勧めします。
- ファイルは.xls形式で保存されており、セルの書式はテキストに設定されている必要があります。

4. **「インポート」**をクリックして、選択したファイルをインポートします。
5. **「すべてエクスポート」**をクリックして、ライセンスプレート一覧をエクスポートします。
6. **オプション：[追加]** をクリックしてナンバープレートを追加し、関連情報を 1 つずつ設定します。
7. **オプション：** [▽] をクリックして、フィルタリングのタイプを選択します。**All Types**、**Wiegand CardID**、**License Plate No.**、および **Type** を選択できます。**Type** では、**Keywords** を選択して、特定のフィルタリングタイプを定義できます。**[Search]** をクリックして、結果を表示します。
8. **オプション：** ナンバープレート番号を選択し、「🗑」をクリックすると、ブロックリストまたは許可リストからナンバープレートを削除できます。
9. **オプション：** プレート番号を選択し、「✎」をクリックすると、ブロックリストまたは許可リストからナンバープレートの関連情報を編集できます。

10.7.5 詳細パラメーター設定

VCA に移動し、アプリケーションを選択します。アプリケーション設定インターフェースに入り、[
「詳細」をクリックして高度なパラメーターを設定します。設定完了後、**「保存」**をクリックします。

注意

機能はデバイスモデルによって異なります。

バージョン

現在のアルゴリズムのバージョンを表します。

インテリジェント情報のオーバーレイ

ビデオに、関連するインテリジェント情報または POS 情報をオーバーレイ表示します。

10.8 AIオープンプラットフォーム

AIオープンプラットフォームは、ユーザーが提供したトレーニング資料に基づいてモデルライブラリを生成し、そのモデルライブラリをデバイスにロードして、ユーザーがタスクやルールを設定できるようにするものです。シーン内のターゲットがルールをトリガーすると、デバイスはリンク動作を実行し、パーソナライズされたスマートアプリケーションを実現します。

注

- この機能は、特定のデバイスモデルでのみサポートされています。
- 特定のデバイスモデルでは、まずVCAページで**AI Open Platformを**有効にする必要があります。

10.8.1 AI Open Platformの設定

手順

1. VCA に移動します**。→ アプリケーションを設定します。→ AI Open Platform**。

注意

- ヘルメット検出、炭鉱の安全検出など、AI Open Platform による設定が可能な特定のスマート機能があります。
- 特定の機能を選択すると、デバイスは対応する機能のモデルパッケージをロードします。
- 機能はデバイスモデルによって異なります。実際のデバイスをご確認ください。

- **ヘルメット検出では**、設定された検出エリア内でヘルメットを着用していない対象物を検出し、アラームを鳴らします。
- **炭鉱の安全検出の場合、VCA→ アプリケーションの設定→ 炭鉱の安全管理** に移動し、この機能を有効にしてください。炭鉱のシナリオでは、検出エリア内の人や鉱山用車両などのターゲットを検出し、ベルトがアイドラーから逸脱していないか、

ヘルメットを着用していない人を検出します。炭鉱の安全検出用に設定されたルールに従ってアラームを鳴らします。

2. **オプション：モデルライブラリ**にモデルを追加します。ローカルパスから**モデル**ライブラリと関連する**ラベルファイル**を選択し、**モデル名を**設定します。モデルタイプは次のとおりです。

検出モデル

ライブビュー内の特定のターゲットを検出し、検出結果とターゲットの座標位置を提供します。

分類モデル

画像またはターゲットを属性に基づいて分類します。

混合モデル

ライブビュー内のターゲットを検出します。

注

最大モデルパッケージ数は、デバイスがサポートするモデルパッケージの最大数を指します。

3. モデルを選択し、有効にします。
4. **分析モード**を選択してください。

ライブビデオ分析	デバイスはライブビデオを分析して、ターゲットの検出と結果のアップロードを行います。
スケジュールキャプチャ分析	デバイスは設定された**自動切り替え間隔**に基づいてキャプチャし、キャプチャした画像を分析して結果をアップロードします。

5. **オプション：**必要に応じて、**オーバーレイターゲットフレーム**と**ルールオーバーレイを**有効にします。

ターゲットフレームのオーバーレイ	アラーム画像にターゲットフレームをオーバーレイします。
ルールオーバーレイ	アラーム画像にルール情報をオーバーレイします。

6. 武装スケジュールとリンク方法を設定します。武装スケジュールの設定については、*「武装スケジュールの設定」*を参照してください。リンク方法の設定については、*「リンク方法の設定」*を参照してください。
7. リンクされたチャンネルのルールを設定します。詳細については*「ルールを設定」*を参照してください。
8. **保存**をクリックします。

10.8.2 ルールを設定

リンクされたチャンネルのルールを設定します。

開始前に

VCA→ AI Open Platform で関連するモデルが選択されており、タスクの設定が完了していることを確認してください。

手順

1. **チャンネル管理で**チャンネルを選択するには、**リンクされたチャンネル**をクリックしてください。
2. リンクされたチャンネルの「⚙ 」 をクリックしてルールを設定します。

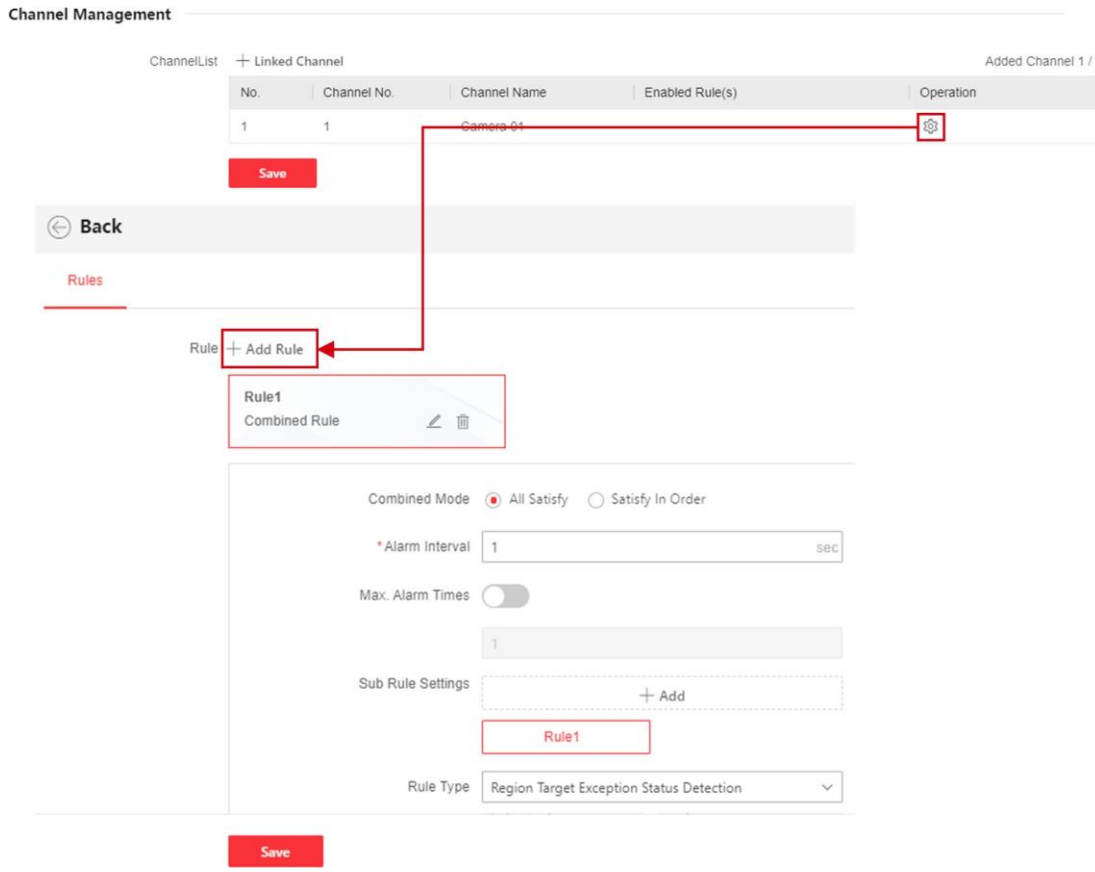

図10-20 ルールを設定する

3. 「**Add Rule**」をクリックします。ルールを選択し、「✎」をクリックしてルール名を変更し、ルールタイプを選択します。

地域ターゲット例外状態検出

あらかじめ定義した仮想ルールエリア内のターゲットを検出してその数をカウントし、設定ルールと比較します。トリガー条件を満たすと、アラームがトリガーされます。

ラインクロスターゲット検出

あらかじめ定義した仮想ルールラインをターゲットが横切ったかどうかを検出し、検出した場合にアラームをトリガーします。

完全分析ルール

事前定義された仮想ルール領域内のすべてのターゲットを検出および分析します。

ラインクロスターゲットカウント

あらかじめ定義した仮想ルールラインを横切るターゲットを検出して、その数をカウントします。

領域内ターゲット数カウント

事前に定義された仮想ルール領域内のターゲットの数を検出およびカウントします。

複合ルール

定義済みの仮想ルールエリアで、**ゾーンターゲットの異常状態検出**および**ラインクロスターゲット検出**に対応しています。検出順序は、**全条件一致**、または**順序一致**の**複合モード**を設定できます。

注

ルールタイプはモデルパッケージによって異なります。実際のデバイスをご確認ください。

4. 検出ルールを設定し、ルール領域または線を引きます。

- ルール領域の描画：ライブビューウィンドウで「⬭」をクリックし、凸形状の領域を描画します。ライブビューウィンドウで終了点を左クリックして設定したルール領域の境界を定義し、右クリックで描画を完了します。
- ルールラインを描く：[／]をクリックすると、ライブビデオに矢印付きのラインが表示されます。ラインをライブビューウィンドウ内の任意の場所にドラッグします。

5. ルールパラメーターを設定します。

オブジェクト

モデルの検出対象の種類。

属性

モデルの検出対象の属性。

期間

ステータスの継続時間。設定した時間が経過すると、アラームが作動します。

アラーム間隔

設定されたアラーム間隔中に、同じタイプのアラームは 1 回だけ通知されます。

感度

感度が高いほど、アラームが鳴りやすくなります。感度が高すぎると、誤報が発生しやすくなります。実際の状況に応じて設定してください。

最大アラーム回数

アラームをトリガーする状態でアラームが作動する最大回数です。

カウント間隔

カウントの時間帯。

アルゴリズムの有効性

アルゴリズムによって与えられた信頼度しきい値が、設定された有効期間以上になると、アラームがトリガーされ、アップロードされます。

ラインクロス

ターゲットがラインを通過する方向。

数量

数量を確認し、ドロップダウンボックスからアラームルールを選択します。アラームルールに応じて、しきい値または範囲（**最小と最大**）を設定します。対象の数値が設定したアラームルールに該当すると、デバイスがアラームを発します。

レポート時間間隔

地域ターゲット数カウントを選択した際に、カウント結果をアップロードする時間間隔を指します。

注意

ルールパラメーターはルールによって異なります。実際のデバイスをご確認ください。

6. **保存**をクリックしてください。

第11章 EPTZ

EPTZ（電子 PTZ）は、カメラを物理的に動かすことなく、画像の一部をデジタルでズームおよびパンする高解像度機能です。EPTZ 機能を使用する場合は、お使いのデバイスが**サードストリーム**に対応していることを確認してください。サードストリームと EPTZ は、同時に有効にする必要があります。

注意

この機能は、特定のデバイスモデルでのみサポートされています。

11.1 パトロール

手順

1. **[設定]**、**[→]**、**[EPTZ]** の順に移動します。
2. **「有効」**にチェック**を入れます**。
3. デフォルトの**ストリームタイプはサードストリーム**であり、設定は変更できません。
4. **アプリケーションモード**で**「パトロール」**を選択します。
5. **「保存」**をクリックします。

次に実行する操作

パトロール設定の詳細については、ライブビュー画面のPTZ操作を参照してください。

11.2 自動追尾

手順

1. **設定→ EPTZ** へ移動します。
2. **「有効」**にチェック**を入れます**。
3. デフォルトの**ストリームタイプはサードストリーム**であり、設定変更はできません。
4. **アプリケーションモード**で**「自動追跡」**を選択します。
5. をクリックして描画を開始します。ライブビューのビデオをクリックして、検出領域の 4 つの頂点を指定し、右クリックして描画を完了します。
6. ルールを設定します。

   検出対象

   人間と車両が検出可能です。検出対象が選択されていない場合、検出されたすべての対象が追跡されます。これには人間と車両も含まれます。

   注意

   この機能に対応しているカメラは、一部のカメラのみです。

   感度

これは、追跡可能な対象の身体部分の割合を表します。感度= 100 - S1/ST× 100。S1は、事前定義された領域内に進入した対象の身体部分を表します。STは、対象の全体的な身体を表します。感度の値が高いほど、対象を容易に追跡できます。

7. **保存**をクリックします。

付録A. FAQ

以下のQRコードをスキャンして、デバイスのよくある質問を確認してください。一部のよくある質問は、特定のモデルにのみ適用されます。

See Far, Go Further

www.hikvision.com
support@hikvision.com

HIKVISION

UD39407B