HiLook

ネットワークカメラ

ユーザーマニュアル

免責事項

この文書について

- 本ドキュメントには、製品の使用および管理に関する指示が含まれています。以下に示す写真、図表、画像、およびその他すべての情報は、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、ファームウェアの更新その他の理由により、予告なく変更される場合があります。最新版はHikvisionウェブサイト（***https://www.hikvision.com***）でご確認ください。別段の合意がない限り、杭州海康威視デジタル技術有限公司およびその関連会社（以下「Hikvision」）は、明示的または黙示的を問わず、一切の保証を行いません。
- 本製品をサポートする訓練を受けた専門家の指導と支援のもとで、本ドキュメントをご利用ください。

本製品について

- 本製品は、購入され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。
- お選びいただいた製品が映像製品の場合は、以下のQRコードをスキャンして「映像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。

知的財産権に関する承認

- Hikvision は、本書に記載された製品に組み込まれた技術に関連する著作権および/または特許を所有しており、これには第三者から取得したライセンスが含まれる場合があります。
- 本文書のテキスト、写真、図表など、その一部または全部は、書面による許可なく、いかなる手段によっても抜粋、複製、翻訳、改変することはできません。
- HiLook およびその他の Hikvision の商標およびロゴは、さまざまな法域における Hikvision の所有物です。
- 記載されているその他の商標およびロゴは、それぞれの所有者に帰属します。

法的免責事項

- 適用される法律で認められる最大限の範囲において、本書および記載されている製品（そのハードウェア、ソフトウェア、ファームウェアを含む）は「現状のまま」「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、商品性、満足のいく品質、特定目的への適合性を含むがこれらに限定されない、明示または黙示の保証を行いません。本製品の使用は、お客様ご自身の リスクにおいて行われます。いかなる場合においても、HIKVISIONは、特別損害、結果的損害、付随的損害、間接損害（事業利益の損失、事業中断、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損害について、契約違反、不法行為（過失を含む）、製造物責任その他のいかなる法的根拠に基づくものであっても、本製品の使用に関連して生じた場合、たとえ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あっても、一切の責任を負いません。

- お客様は、インターネットの性質上、固有のセキュリティリスクが存在することを認識し、サイバー攻撃、ハッカー攻撃、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動作、プライバシー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、必要に応じてタイムリーな技術サポートを提供します。
- お客様は、適用されるすべての法律に従って本製品を使用することに同意し、お客様の使用が適用される法律に準拠していることを確認する責任はお客様のみにあります。特に、本製品の使用が第三者の権利（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）を侵害しない方法で行う責任を負います。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、核爆発物または安全でない核燃料サイクルに関連する文脈における活動、または人権侵害を支援する活動を含むがこれらに限定されない。
- 本文書と適用される法律との間に矛盾が生じた場合、後者が優先する。

記号の定義

本ドキュメントで使用される記号は、以下の通り定義されます。

記号	説明
危険	回避しなければ死亡または重傷を負う危険な状況があることを示します。
注意	回避しなければ、機器の損傷、データの損失、性能の低下、または予期しない結果をもたらす可能性のある潜在的な危険な状況を示します。
注記	本文の重要な点を強調または補足する追加情報を提供します。

安全上の注意

製品の「***安全上の注意***」を入手するには、以下のQRコードをスキャンし、よくお読みください。これらの指示は、ユーザーが製品を正しく使用し、危険や財産の損失を避けることを目的としています。

図1-1 安全上の注意

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。

一般的な設定手順

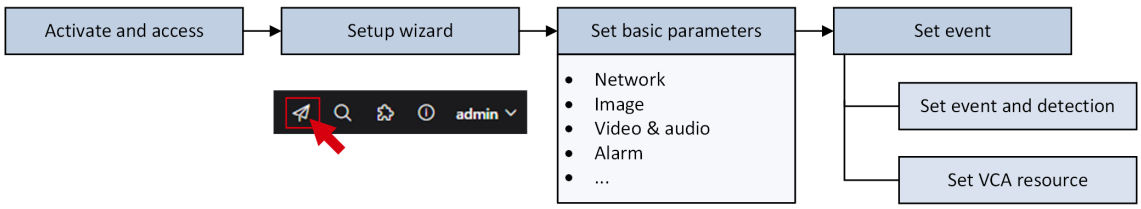

図1-1 一般的な設定手順

- ***ウェブブラウザでデバイスを起動しアクセスします。*** ネットワーク経由でデバイスにアクセスする際、起動にはログインパスワード（**管理者**ユーザー用）の設定が必要です。ウェブブラウザを開きIPアドレスを入力します。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、デバイスパラメータを素早く設定します。
- 基本パラメータ（ネットワーク、画像、動画・音声、アラームなど）を設定します。
- イベントと検知ルールを設定します。基本の***イベントと検知***ルールを設定するか、深層学習機能用に***VCAリソースを割り当てることができます***。

1.2 ファームウェア更新

ユーザーエクスペリエンス向上のため、最新のファームウェアへの更新をお勧めします。最新のファームウェアパッケージは、公式ウェブサイトまたは現地の技術担当者から入手してください。詳細については、公式ウェブサイト ***https://www.hikvision.***com/en/support/download/firmware/ をご覧ください。
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

お客様のコンピュータは、本製品を適切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 解像度以上
Webブラウザ	詳細は、*プラグインのインストールを*参照してください。

第2章 デバイスの起動とアクセス

ユーザーアカウントとデータのセキュリティと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際には、ログインパスワードを設定してデバイスをアクティベートする必要があります。

注記

クライアントソフトウェアのアクティベーションに関する詳細情報は、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によるデバイスのアクティベーション

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、アクティベートします。

開始前に

www.hikvision.com にアクセスし、SADPソフトウェアを入手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、オンライン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強化のため、ご自身で選択した強力なパスワード（大文字、小文字、数字、特殊文字を含む8文字以上）の設定を強く推奨します。特に高セキュリティシステムでは、パスワードを定期的に（月次または週次で）リセットすることで、製品をより効果的に保護できます。

5. **[OK]**をクリックします。
   デバイスのステータスが「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**ネットワーク設定**を変更します。

2.2 ブラウザ経由でのデバイス起動

ブラウザからデバイスにアクセスして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アドレスを同一セグメントに変更します。

注記

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）に設定できます。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***を入力します。
4. デバイス起動パスワードを設定します。

注意

製品のセキュリティ強化のため、ご自身で選択した強力なパスワード（8文字以上で、大文字、小文字、数字、特殊文字の少なくとも3種類を含む）の作成を強く推奨します。また、特に高セキュリティシステムでは、パスワードを定期的に（月次または週次で）リセットすることで製品をより効果的に保護できます。

5. **[OK]**をクリックします。
6. アクティベーションパスワードを入力してデバイスにログインします。
7. オプション：**設定 → ネットワーク → ネットワーク設定 → TCP/IP** に移動し、デバイスのIPアドレスをネットワークの同一セグメントに変更します。

2.3 ログイン

Webブラウザ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では、デバイスの機能の表示や操作が制限される場合があります。正常な表示と操作を確保するために、プラグインのインストールや特定の設定を行う必要があります。制限される機能の詳細については、実際のデバイスを参照してください。

オペレーティングシステム	Web ブラウザ	操作
	● Internet Explorer 10以降	ポップアップの指示に従っ

オペレーティングシステム	Web ブラウザ	操作
Windows	● Google Chrome 57 およびそれ以前のバージョン ● Mozilla Firefox 52 およびそれ以前のバージョン	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以降 ● Mac Safari 16以降	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)** に移動し、WebSocket または WebSockets を有効にして通常表示を行ってください。一部の機能の表示および操作が制限されます。例えば、再生および画像表示は利用できません。詳細な制限機能については、実際のデバイスを参照してください。

注意

- 本デバイスはWindowsおよびMac OSシステムのみをサポートし、Linuxシステムはサポートしていません。
- 特定のデバイスでのユーザーエクスペリエンス向上のため、より高度なウェブブラウザでのアクセスを推奨します。実際のデバイスまたは製品仕様をご参照ください。
- 一部のデバイスモデルではInternet Explorerウェブブラウザをサポートしていません。

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、ログインページの「**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できます。セキュリティの質問またはメールを設定することで、パスワードをリセットできます。

注記

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

セキュリティの質問

アカウントのセキュリティは、アクティベーション時に設定できます。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、その答えを入力してください。
ブラウザ経由でデバイスにアクセスする際、「**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回答することで管理者パスワードをリセットできます。

Eメール

アクティベーション中にアカウントのセキュリティを設定できます。または、**[設定]→[システム]→[ユーザー管理]** に移動し、**[アカウントセキュリティ設定]** をクリックして、回復操作プロセス中に確認コードを受け取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

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向上に役立ちます。
[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**ロック期間は**設定可能です。

不正ログイン試行回数

設定回数を超える不正なパスワード入力が行われた場合、デバイスはロックされます。

ロック時間

設定された時間が経過すると、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、機能アイコン、伝送パラメータの設定について紹介します。

3.1 ライブビューパラメータ

対応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。ライブビューを開始するには「 」をクリックします。ライブビューを停止するには「 」をクリックします。

3.1.2 アスペクト比

アスペクト比とは、画像の幅と高さの表示比率です。

- 4:3 はウィンドウサイズを指します。
- 16:9 ウィンドウサイズを示します。
- 元のウィンドウサイズを指します。
- 自己適応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、*ストリームタイプ*を参照してください。

3.1.4 サードパーティ製プラグインの選択

特定のブラウザでライブビューが表示できない場合、ブラウザに応じてライブビュー用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. プラグインを選択するには、[ ] をクリックします。
   - Internet Explorerでデバイスにアクセスする場合、WebcomponentsまたはQuickTimeを選択できます。
   - その他のブラウザでデバイスにアクセスする場合、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装置のオン/オフを切り替えます。

注意

レーザー搭載デバイスについて：

- 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。
- 適切な遮蔽や保護具がない場合は、安全な距離で点灯するか、光が直接当たらない場所で点灯してください。
- 装置の組み立て、設置、または保守作業中は、光を点灯させないでください。また、眼の保護具を着用してください。

3.1.6 ピクセルカウント

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を取得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、目的の矩形領域を選択します。
   幅ピクセルと高さピクセルがライブビュー画像の下部に表示されます。

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確認するのに役立ちます。

手順

1. デジタルズームを有効にするには、 をクリックします。
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

電動式デバイス用です。デバイスが明確に焦点を合わせられない場合に画像品質を向上させます。

ABF対応デバイスでは、レンズ角度を調整後、デバイス上のABFボタンをクリックしてフォーカスします。これによりデバイスは明確にフォーカスできます。

をクリックすると自動で焦点が合います。

注意

- 補助フォーカスでピントが合わない場合、*レンズ初期化*を実行した後、再度補助フォーカスを使用すると画像が鮮明になります。

- 補助フォーカスでも装置が明確に焦点を合わせられない場合、手動フォーカスを使用できます。

3.1.9 レンズ初期化

レンズ初期化は電動レンズ搭載デバイスで使用します。長時間ズームやフォーカス操作で画像がぼやけた場合にレンズをリセットする機能です。機能は機種によって異なります。レンズ初期化を操作するには、 をクリックしてください。

3.1.10 レンズパラメータ調整

PTZはパン（水平方向移動）、チルト（垂直方向移動）、ズームの略称です。これはデバイスの動作オプションを指します。ライブビュー画面では、方向制御ボタンをクリックしてパン/チルト動作を制御し、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実現できます。

注

- 対応するPTZ機能はカメラモデルによって異なります。
- レンズ動作のみをサポートするデバイスでは、方向ボタンは無効です。

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

- をクリックすると、レンズが近くに焦点を合わせ、近くの物体が鮮明になります。
- 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。

アイリス

- 画像が暗すぎる場合、 をクリックしてアイリスを拡大します。
- 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込みます。

パン・チルト速度

 をスライドさせてパン/チルト動作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回転機能を無効化し、PTZ調整によるターゲットの消失を減らすことを意味します。

注記

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。

をクリックするとPTZ操作がロックされ、 をクリックするとロックが解除されます。

PTRZ調整

PTRZはパン、チルト、回転、ズームの略称です。デバイスの動作オプションを指します。インターフェースでは、制御ボタンを使用してデバイスの動作（パン、チルト、回転、ズームなど）を調整できます。

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。

設定 → PTZ → PTRZ に移動します。

コントロールパネル

	方向ボタンを長押ししてデバイスのパン/チルトを行います。
●  ● 	ボタンをクリックしたままにすると、回転位置を調整できます。

自動復旧

をクリックすると、デバイスが回転位置を自動的に補正し、ライブビュー画像を正立表示にします。**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。

注記

- **設定 → PTZ → PTZ** に移動し、**自己診断ステータスを**確認してください。
- PTZを手動で初期化し自己診断を有効にするには、**設定 → PTZ → PTZ** に移動し「**自己診**

断」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、「*レンズパラメータ調整*」を参照してください。

3.1.11 3D位置調整の実行

3D 位置決めは、選択した領域を画像の中心に再配置する機能です。

手順

1. 「 」をクリックして機能を有効にします。
2. ライブ画像内で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（ズーム効果なし）。
   – マウスを押したまま右下方向にドラッグし、ライブ映像上で領域を枠で囲む：枠で囲まれた領域が拡大され、ライブ映像の中心に再配置されます。
   – マウスを押したまま左上方向にドラッグしてライブ映像の一部を枠で囲む：枠で囲まれた領域がズームアウトされ、ライブ映像の中心に再配置されます。
3. ボタンを再度クリックすると機能をオフにします。

3.2 伝送パラメータの設定

ネットワーク環境によりライブ映像が正常に表示されない場合があります。異なるネットワーク環境では、伝送パラメータを調整することで問題を解決できます。

手順

1. **設定 → ローカル → ライブビューパラメータ** に移動します。
2. 送信パラメータを必要に応じて設定します。

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優れた映像品質を保証しますが、リアルタイム伝送には影響が出ます。安定したネットワーク環境に適しています。

UDP

UDPは、高い動画の滑らかさを要求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場合に適しています。選択前に、それらのクライアントに対してマルチキャストアドレスを設定する必要があります。

注記

マルチキャストの詳細については、*マルチキャスト*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状況に適しています。

再生パフォーマンス

最短遅延

デバイスは、動画の滑らかさよりもリアルタイムの映像を優先します。

バランス型

デバイスはリアルタイム映像と滑らかさの双方を確保します。

滑らか

デバイスはリアルタイムよりも動画の滑らかさを優先します。ネットワーク環境が悪い場合、滑らかさが有効であっても、デバイスは動画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てライブビューを滑らかに表示できますが、ルール情報が表示されない場合があります。

3. **[保存]**をクリックします。

第4章 映像と音声

本章では、映像・音声関連パラメータの設定について説明します。

4.1 動画設定

本節では、ストリームタイプ、動画エンコーディング、解像度などの動画パラメータ設定について説明します。
設定ページへの移動：**設定 → ビデオ/オーディオ → ビデオ**。

4.1.1 ストリームタイプ

デバイスが複数のストリームをサポートしている場合、各ストリームタイプごとにパラメータを指定できます。

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性能を表します。通常、デバイスが実現可能な最高の解像度とフレームレートを提供します。ただし、高解像度と高フレームレートは、通常、より大きなストレージ容量と、伝送におけるより高い帯域幅要件を意味します。

サブストリーム

このストリームは比較的低解像度のオプションを提供し、帯域幅とストレージ容量の消費を抑えます。

その他のストリーム

メインストリームとサブストリーム以外のストリームも、カスタマイズされた用途向けに提供される場合があります。

4.1.2 ビデオタイプ

ストリームに含まれるべきコンテンツ（動画と音声）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

複合ストリームに動画コンテンツと音声コンテンツが含まれます。

4.1.3 解像度

実際のニーズに応じてビデオ解像度を選択してください。解像度が高いほど、より多くの帯域幅 とストレージが必要となります。

4.1.4 ビットレートタイプと最大ビットレート

固定ビットレート

ストリームは比較的固定されたビットレートで圧縮・伝送されます。圧縮速度は速いですが、画像にモザイクが発生する可能性があります。

可変ビットレート

設定された**最大ビットレート**内で、デバイスが自動的にビットレートを調整します。圧縮速度は固定ビットレートよりも遅くなりますが、複雑なシーンの画質を保証します。

4.1.5 映像品質

ビットレートタイプを可変に設定した場合、動画品質は設定可能です。実際のニーズに応じて動画品質を選択してください。なお、動画品質が高いほど、より高い帯域幅が必要となります。

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、フレーム毎秒（fps）で測定されます。
動画ストリームに動きがある場合、フレームレートが高いほど画質が維持される利点があります。ただし、フレームレートが高いほど、より多くの帯域幅とより大きなストレージ容量が必要となります。

4.1.7 動画エンコーディング

デバイスが動画エンコーディングに採用する圧縮規格を指します。

注記

利用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（MPEG-4 Part 10、Advanced Video Coding）は、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、動画ファイルのサイズを縮小します。

H.264+

H.264+はH.264を基盤とした改良型圧縮符号化技術です。H.264+を有効にすると、 で最大平均ビットレートに基づくHDD消費量を推定できます。H.264と比較し、H.264+はほとんどのシーンで最大ビットレートを同等としながらストレージを最大50%削減します。
H.264+を有効にした場合、**最大平均ビットレート**は設定可能です。デフォルトでは推奨最大平均ビットレートが設定されます。映像品質が不十分な場合は、このパラメータを高い値に調整できます。最大平均ビットレートは最大ビットレートを超えてはいけません。

注記

H.264+を有効にした場合、**Iフレーム間隔は**設定不可となります。

H.265

H.265（High Efficiency Video Coding：HEVC、MPEG-H Part 2）は圧縮規格です。H.264と比較し、同等の解像度・フレームレート・画質において優れた動画圧縮を実現します。

H.265+

H.265+はH.265を基盤とした改良型圧縮符号化技術です。H.265+を有効化すると、最大平均ビットレートに基づくHDD消費量の推定が可能になります。H.265と比較し、H.265+はほとんどのシーンにおいて最大ビットレートを同等としながら、ストレージ容量を最大50%削減します。
H.265+を有効にした場合、**最大平均ビットレート**は設定可能です。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ます。動画品質が満足のいくものでない場合、このパラメータをより高い値に調整できます。最大平均ビットレートは、最大ビットレートを超えてはいけません。

注記

H.265+が有効な場合、**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において、Iフレーム（イントラフレーム）は他の画像を参照せずに独立してデコード可能な自己完結型フレームです。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フレームが多い（つまりIフレーム間隔が小さい）動画は、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を必要とします。

SVC

スケーラブル動画符号化（SVC）は、H.264またはH.265動画圧縮規格のAnnex G拡張機能の名称である。
SVC標準化の目的は、高品質な動画ビットストリームをエンコード可能とすることにある。このビットストリームには、既存のH.264またはH.265設計と同等の複雑度と再構成品質で、かつサブセットビットストリームと同量のデータを用いてデコード可能な、1つ以上のサブセットビットストリームが含まれる。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することで 生成される。
SVCは旧式ハードウェアへの前方互換性を実現する：低解像度サブセットのみをデコード可能な基本ハードウェアでも同一ビットストリームを利用可能であり、一方、より高度なハードウェアでは高品質ビデオストリームのデコードが可能となる。

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、イントラフレーム符号化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、個別の JPEG 画像として圧縮されます。

プロファイル

この機能は、同じビットレートでは、プロファイルが複雑であるほど、画質は高くなり、ネットワーク帯域幅の要件も高くなることを意味します。

4.1.8 スムージング

ストリームの滑らかさを指します。平滑化値が高いほどストリームの流動性は向上しますが、映像品質は満足のいくものではなくなる可能性があります。平滑化値が低いほどストリームの品質は高くなりますが、流動性に欠ける場合があります。

4.2 オーディオ設定

オーディオエンコーディングや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：**設定 → ビデオ/オーディオ → オーディオ**。

注意

この機能は特定のカメラモデルのみがサポートしています。

4.2.1 オーディオエンコーディング

オーディオのオーディオエンコーディング圧縮を選択します。

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てください。
- オーディオ入力の表示は、デバイスモデルによって異なります。

ライン入力	デバイスをMP3プレーヤー、シンセサイザー、アクティブピックアップなど高出力のオーディオ入力機器に接続する場合、**オーディオ入力をLineInに設定してください。**
マイク入力	**オーディオ入力**を**マイク入力**に設定してください。これは、マイクやパッシブピックアップなど、低出力のオーディオ入力デバイスに接続する場合に適用されます。

4.2.3 オーディオ出力

注意

オーディオ出力デバイスを必要に応じて接続してください。

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一切出力されません。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。機能を有効にすると、環境内のノイズがある程度除去さ

れます。

4.3 双方向オーディオ

監視画面上で監視センターと対象者間の双方向音声機能を実現するために使用されます。

開始前に

- 本機に接続された音声入力デバイス（ピックアップまたはマイク）および音声出力デバイス（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、音声入力・出力デバイスの仕様を参照してください。
- 本機に内蔵マイクとスピーカーがある場合、双方向音声機能を直接有効にできます。

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、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、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、動画圧縮において関心領域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ることで、関心領域の品質を向上させ、背景情報への注力を減らします。

4.4.1 ROIの設定

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ることで、ROI の品質を向上させ、背景情報への焦点を弱めるのに役立ちます。

開始前に

ビデオの符号化方式を確認してください。ROIは、ビデオ符号化方式がH.264またはH.265の場合にサポートされます。

手順

1. **設定 → ビデオ/オーディオ → ROI** に移動します。
2. **[有効化]** 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. **領域番号**を選択し、ライブビュー上でROI領域を描画するには「 」をクリックします。

注記

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。

注記

ROIレベルが高いほど、検出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必要がある場合は、他の領域番号を選択し、上記の手順を繰り返します。

4.5 対象領域の切り抜き設定

画像のトリミングが可能で、ターゲット領域の画像のみを送信・保存することで、伝送帯域幅とストレージを節約できます。

手順

1. **設定 → ビデオ/オーディオ → ターゲットクロッピング** に移動します。
2. **有効化**をチェックし、**ストリームタイプを第三ストリーム**に設定します。

注記

ターゲットクロッピングを有効化すると、サードストリームの解像度は設定できなくなります。

3. **クロッピング解像度**を選択します。
   ライブビューに赤い枠が表示されます。
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。

注記

- ターゲットクロッピングに対応しているのは特定のモデルのみであり、機能はカメラモデルによって異なります。
- ターゲットクロッピングを有効にした後、一部の機能が無効になる場合があります。

4.6 ストリーム上の情報表示

対象物（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。接続された末端

デバイスまたはクライアントソフトウェアで、ライン越え、侵入などのイベントを検出する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、**スマートイベントを**有効にします。

手順

1. **設定 → 映像/音声 → ストリーム上の情報表示** 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 表示設定

画像特性を調整するためのパラメータ設定を提供します。
設定 → 画像 → 表示設定 に移動します。
デフォルトをクリックすると設定が復元されます。

4.7.1 シーンモード

異なる設置環境向けに、あらかじめ定義された複数の画像パラメータセットが用意されています。実際の設置環境に応じてシーンを選択することで、表示設定を迅速に行えます。

画像調整

明るさ、彩度、コントラスト、シャープネスの調整により、画像を最適に表示できます。

露出設定

露出は、絞り、シャッター、感度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、画像効果を調整できます。
手動モードでは、**露光時間、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を提供します。

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焦点が合います。自動モードで焦点が合いにくい場合は、画像内の光源を減らし、点滅する光を避けてください。

半自動

PTZ操作とレンズズーム後、一度だけフォーカスを調整します。画像が鮮明な場合、シーンが変わってもフォーカスは変更されません。

手動

ライブビュー画面で手動で焦点を調整できます。

デイ/ナイト切替

デイ/ナイト切り替え機能により、昼間モードと夜間モードでカラー画像と白黒画像を提供します。切り替えモードは設定可能です。

デイ

画像は常にカラー表示されます。

ナイト

画像は白黒またはカラフルで、夜間でも鮮明なライブビュー画像を確保するため補助照明が作動します。

注記

補助照明とカラフルな画像に対応しているのは特定のデバイスモデルのみです。

自動

カメラは環境の光量に応じて昼間モードと夜間モードを切り替えます。

スケジュール切替

開始時間と**終了時間を**設定し、デイモードの継続時間を定義します。

警報入力によるトリガー

トリガー状態を「**昼**」または「**夜**」に設定できます。例えば**トリガー**状態が「**夜**」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が**夜間に**切り替わります。

映像トリガー

カメラは環境の光量に応じて昼間モードと夜間モードを切り替えます。このモードは、デバイスが道路交通や車両検知をサポートしている場合に適用されます。

注記

- デイ/ナイト切替機能は機種によって異なります。
- より良い画像効果を得るために、スマート補助ライトをオンにできます。補助ライトの設定については、*「補助ライト設定」*を参照してください。

補助光設定

補助ライトを設定できます。関連するパラメータについては、実際のデバイスを参照してください。

スマート補助光

スマート補助光は補助光点灯時に露出オーバーを回避します。

補助光モード

デバイスが補助光をサポートしている場合、補助光モードを選択できます。

IR補助光

赤外線ライトが有効です。

ホワイトライト

白色光が有効です。

混合光

赤外線ライトと白色ライトの両方が有効です。

スマート

特定のスマートイベントやモーション検知を有効にした後、このモードを選択すると、夜間状態ではデフォルトの補助照明モードは赤外線補助照明モードになります。警報 がトリガーされると、白色光が有効になり、デバイスが対象を捕捉します。警報終了後、補助照明モードは赤外線補助照明モードに切り替わります。
赤外線ライトと白色ライト、または赤外線と白色ライトのハイブリッド補助照明を搭載したデバイスモデルのみが本機能をサポートします。

オフ

補助照明は無効です。

注記

補助照明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。

輝度調整モード

自動

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

強い逆光下にある被写体に焦点を合わせると、被写体が暗すぎてはっきり見えなくなることがあります。BLC（バックライト補正）は、手前の被写体への光量を補正し、鮮明に映

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できます。

WDR

WDR（ワイドダイナミックレンジ）機能は、強い明暗差のある環境でもカメラが鮮明な画像を提供することを支援します。
視野内に非常に明るい領域と非常に暗い領域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できます。WDRは画像全体の明るさを自動的に調整し、より詳細な鮮明な画像を提供します。

注

WDRを有効にした場合、他の機能の一部がサポートされない場合があります。詳細は実際のインターフェースを参照してください。

WDR Off　　WDR On

図4-1 WDR

HLC

画像の明るい領域が露出オーバーで暗い領域が露出不足の場合、HLC（ハイライト圧縮）機能を有効にすることで明るい領域を弱め、暗い領域を明るくし、画像全体の明るさのバランスを実現できます。

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

使用されます。

Cold　　Warm　　Auto White Balance

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**モードと**エキスパート**モードが選択可能です。

通常

DNRレベルを設定してノイズ低減の度合いを制御します。レベルが高いほど低減効果が強くなります。

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、ノイズ低減度合いを制御します。レベルが高いほど、より強力な低減効果があります。

DNR Off

DNR On

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できます。これによ

り微細なディテールが強調され、画像がより鮮明に表示されます。

Defog Off　　Defog On

図4-4 デフォグ

EIS

ジッター補正技術を用いて映像の安定性を向上させます。

グレースケール

グレースケールの範囲は [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反転している場合、この機能により画像を正常に表示できます。
必要に応じてミラーモードを選択してください。

注

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。例えば、1280×720が720×1280に回転します。
この機能を有効にすると、垂直方向の監視有効範囲が変化する場合があります。

注記

この機能は特定の設定下でサポートされます。

レンズ歪み補正

電動レンズを搭載したデバイスでは、画像にある程度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、歪みを補正できます。

注意

- この機能は、電動レンズを搭載した特定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、画像の端部が失われます。

4.7.2 画像パラメータ切り替え

デバイスは設定された時間間隔で画像パラメータを自動的に切り替えます。
画像パラメータ切り替え設定ページへ移動：**設定 → 画像 → 表示設定 → 画像パラメータ切り替え**、必要に応じてパラメータを設定してください。

スケジュール切り替えを設定

特定の時間間隔で画像をリンクされたシーンモードに自動切替します。

手順

1. **スケジュール切り替えに**チェックを入れます。
2. 対応する時間帯とリンク先シーンモードを選択し設定します。

注記

リンク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

ビデオ規格とは、ビデオカードまたはビデオ表示装置が定義する表示色数と解像度を指します。最も一般的な規格はNTSCとPALです。NTSCでは毎秒30フレームが伝送され、各フレームは525本の走査線で構成されます。PALでは、毎秒25フレームが送信されます。各フレームは625本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

本装置に BNC、CVBS、HDMI、SDI などのビデオ出力インターフェースが装備されている場合、本装置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 で選択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、色、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：**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化します。

文字セット

表示情報用の文字コードを選択します。画面に韓国語を表示する必要がある場合は**EUC-KR**を選択してください。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、および関連する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**などのOSDパラメータを設定します。

テキストオーバーレイ

画像上にカスタマイズされ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

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する機能です。デバイスがどのように動いても、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** に移動します。
2. **[有効化]** にチェックを入れます。
3. 「 」をクリックし、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て	領域のサイズを調整します。
領域をドラッグ	領域の位置を調整します。
クリック	設定した領域をすべてクリアします。

4. **[追加]**をクリックしてプライバシーマスクを追加し、領域名と**マスクタイプ**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、24 ビットの BMP 形式である必要があり、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** に移動します。
2. 「**有効化**」にチェックを入れます。
3. 「**アップロード**」をクリックし、画像を選択して開きます。
   アップロードが成功すると、赤い四角で囲まれた画像が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ます。
5. 「**保存**」をクリックします。

第5章 動画録画と画像キャプチャ

このパートでは、動画クリップやスナップショットのキャプチャ、再生、キャプチャしたファイルのダウンロード操作について紹介します。

5.1 保存設定

このパートでは、いくつかの一般的な保存パスの設定について紹介します。

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、プロパティを確認できます。データセキュリティを確保するため、メモリカードの暗号化をサポートしています。

新規または暗号化されていないメモリカードの設定

開始前に

新しいメモリカードまたは暗号化されていない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については、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. **設定 → ストレージ → ストレージ管理 → HDD管理** に移動します。
2. メモリカードを選択します。

注意

「**ロック解除**」ボタンが表示される場合は、まずメモリカードのロックを解除する必要があります。詳細は「*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ます。
   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、メモリカードは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」に変わったら、メモリカードは使用可能になります。

注意

暗号化パスワードは適切に保管してください。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**クォータ**を設定します。必要に応じて、異なるコンテンツを保存する割合を入力してください。
6. 「**保存**」をクリックします。

暗号化メモリカードの設定

開始前に

- 暗号化済み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については、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把握しておく必要があります。

手順

1. **設定 → ストレージ → ストレージ管理 → HDD管理** に移動します。
2. メモリーカードを選択してください。

注記

アンロックボタンが表示された場合は、まずメモリカードのロックを解除する必要があります。詳細は「*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ます。
   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」に変わったら、メモリーカードを使用できる状態です。

注

暗号化パスワードを忘れてしまい、このメモリーカードを引き続き使用したい場合は、*「新しいメモリーカードまたは暗号化されていないメモリーカードの設定」を*参照して、メモリーカードをフォーマットおよび設定してください。既存のコンテンツはすべて削除されます。

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、異なるコンテンツを保存するための割合を入力してください。
5. 「**保存**」をクリックします。

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、通知を受け取ります。

開始前に

設定ページは、Hikvisionメモリーカードがデバイスに挿入されている場合にのみ表示されます。

手順

1. **設定 → ストレージ → ストレージ管理 → メモリカード検出** に移動します。
2. **「状態検出」**をクリックし、メモリカードの「**残存寿命**」と「**健全性状態**」を確認します。

残存寿命

メモリカードの残存寿命をパーセンテージで表示します。メモリカードの寿命は、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。残存寿命が十分でない場合は、メモリカードを変更する必要があります。

健全性状態

メモリカードのコンディションを表示します。アーミング**スケジュールと連動**方法が設定されている場合、健全状態が「良好」以外になると通知を受け取ります。

注意

健康状態が「良好」でない場合は、メモリカードの交換をお勧めします。

3. **R/Wロック**をクリックし、メモリカードの読み書き権限を設定します。
    1. ロックを追加します。**ロックスイッチ**をONに選択します。
    2. パスワードを入力します。
    3. **保存**をクリック

ロック解除

- ロックした端末でメモリカードを使用すると、自動的にロックが解除されるため、ユーザーによる解除操作は不要です。
- ロック付きのメモリーカードを別のデバイスで使用する場合、**HDD管理で**手動でロックを解除できます。メモリーカードを選択し、「**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てください。
    1. ロック解除**ロックスイッチを**OFFに設定してください。
    2. **パスワード設定**でパスワードを入力します。
    3. **「保存」**をクリックします。

注記

- **R/Wロックの**設定は管理者ユーザーのみ可能です。

- メモリカードはロック解除時にのみ読み書きが可能です。
- メモリカードにロックを追加したデバイスを工場出荷時設定に復元した場合、**HDD管理画面で**メモリカードのロックを解除できます。

4. 警戒スケジュールと**連動方法**の設定を行います。詳細は「警戒スケジュール*と連動方法の設定*」を参照してください。
5. 「**保存**」をクリックします。

5.1.2 FTPの設定

イベントまたは定時スナップショット タスクでキャプチャされた画像を保存するために、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]** に移動します。
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ユーザーは画像アップロード権限を持つ必要があります。
FTPサーバーが匿名ユーザーによる画像アップロードをサポートしている場合、アップロード時にデバイス情報を非表示にするために「**匿名**」にチェックを入れることができます。

ディレクトリ構造

FTPサーバー上のスナップショット保存パス。

3. オプション：**[画像をアップロード]** にチェックを入れると、FTP サーバーへのスナップショットのアップロードが可能になります。

画像保存間隔

画像管理を効率化するため、1日から30日の範囲で画像保存間隔を設定できます。同一間隔で撮影された画像は、期間の開始日と終了日に基づいて命名されたフォルダに一括保存されます。

画像名

キャプチャ画像の命名規則を設定します。ドロップダウンリストで「**デフォルト**」を選択すると、既定の規則（例：10.11.37.189_01_20150917094425492_FACE_DETECTION.jpg）が適用されます。または、デフォルト命名規則に**カスタム接頭辞**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。

注記

リンク方式でFTP/メモリーカード/NASへのアップロードと自動ネットワーク補充を有効にするには、両方を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サーバーを確認します。
6. 「**保存**」をクリックします。

5.1.3 NASの設定

ネットワークサーバーをネットワークディスクとして使用し、記録ファイルやキャプチャ画像などを保存します。

開始前に

ネットワークドライブのIPアドレスを事前に取得してください。

手順

1. NAS設定ページに移動：**設定 → ストレージ → ストレージ管理 → 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、セキュリティを確保するため、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**アドレスとディスクの**ファイルパス**を設定します。

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先パス。

5. **[テスト]**をクリックし、ネットワークディスクが利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設定を編集します。
削除	Net HDD を削除します。 ● をクリックします。 ● Net 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 の健康状態が悪い場合に、自動的に eMMC のストレージメディアとしての使用を停止します。

注記

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、**設定 → システム → システム設定 → システムサービス** に移動してください。
eMMC（Embedded Multimedia Cardの略称）は、組み込み型の不揮発性メモリシステムです。デバイスの撮影した画像や動画を保存できます。
デバイスはeMMCの健全性を監視し、状態が不良の場合にeMMCを無効化します。劣化したeMMCを使用すると、デバイスの起動失敗につながる可能性があります。

5.1.5 クラウドストレージの設定

キャプチャした画像や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 や分析のために、クラウドから直接画像を要求します。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を有効にした場合、画像はまずクラウドビデオマネージャーに保存されます。

1. **設定 → ストレージ → ストレージ管理 → クラウドストレージ** に移動します。
2. 「**有効化**」にチェックを入れます。
3. 基本パラメータを設定します。

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アドレスをサポートします。
サービスポート	クラウドビデオマネージャーのポート番号。デフォルトポートの使用を推奨します。

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た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ストレージ領域のID。ストレージプールIDとストレージ領域IDが同一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テストします。
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、手動録画・スケジュール録画の操作、録画ファイルの再生およびダウンロードについて説明します。

5.2.1 自動録画

この機能は、設定された時間帯に自動的にビデオを録画します。

操作前に

「**連続**」以外の各録画タイプで、イベント設定内の「**トリガー録画**」を選択してください。詳細は*「イベントとアラーム」*を参照してください。

手順

1. **[設定]→[ストレージ]→[スケジュール設定]→[録画スケジュール]** に移動します。
2. 「**有効化**」にチェックを入れます。
3. レコードタイプを選択します。

注記

レコードタイプはモデルによって異なります。

連続

スケジュールに従い、ビデオが連続的に録画されます。

モーション検知

動体検知が有効で、連動方式として録画トリガーが選択されている場合、物体の動きが記録されます。

アラーム

外部警報入力デバイスからの警報信号を受信後、動画を録画します。

モーション | アラーム

外部警報入力デバイスから警報信号を受信した場合、または動きが検出された場合に映像が記録されます。

モーション＆アラーム

外部アラーム入力デバイスからモーションが検出され、かつアラーム信号を受信した場合にのみ録画されます。

イベント

設定されたイベントが検出された場合に動画を録画します。

4. 選択した録画タイプにスケジュールを設定します。設定操作については*「警戒スケジュール設定」*を参照してください。
5. 詳細録画パラメータを設定します。

上書き

ストレージ容量が満杯になった際に録画データを上書きするには「**上書きを有効にする**」を選択します。無効の場合、カメラは新規録画を行えません。

事前録画

スケジュールされた時間より前に録画する期間を設定します。

後録り

スケジュールされた時刻後に録画を停止する設定時間。

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、プリレコードおよびポストレコードの実際の時間は設定値より短くなる可能性があります。

録画の有効期限

有効期限を超過した録画は削除されます。有効期限は設定可能です。録画が削除されると復元できないことにご注意ください。

6. **[保存]**をクリックします。

5.2.2 手動での録画

手順

1. **[設定]** → **[ローカル]** に移動します。

2. 録画ファイルの「**動画サイズ**」と「**動画保存パス**」を設定します。
3. 「**保存**」をクリックします。
4. ライブビュー画面で「 」をクリックして録画を開始します。「 」をクリックすると録画を停止します。

次の操作

録画された動画ファイルを確認します。
設定 → ローカルに移動し、**動画保存パス**の横にある「**開く**」をクリックして保存パスを開き、ファイルを確認します。

5.2.3 動画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た動画を検索、再生、クリップ、ダウンロードできます。

手順

1. **再生 → 動画** に移動します。
2. 検索条件を設定し、「**検索**」をクリックします。
   一致した動画ファイルがタイミングバーに表示されます。
3. 「 」をクリックして動画ファイルを再生します。
   – 「 」をクリックすると動画ファイルを全画面で再生します。**ESCキー**を押すと全画面表示を終了します。
   – 「 」をクリックすると、全チャンネルの動画再生を停止します。
4. オプション：動画ファイルをクリップするには「 」をクリックします。再度「 」をクリックするとクリップ操作を停止します。

注記

設定 → ローカル → クリップ保存パス に移動し、クリップした動画ファイルの保存パスを確認・変更できます。

5. オプション：再生画面で「 」をクリックするとファイルをダウンロードできます。

注記

設定 → ローカル → ダウンロード済みファイル保存パス に移動し、ダウンロード済み動画ファイルの保存パスを確認・変更できます。

5.3 キャプチャ設定

本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。スナップショットの閲覧とダウンロードが可能です。

5.3.1 自動キャプチャ

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

イベントトリガー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連動方法を設定する必要があります。イベント設定については「*イベントとアラーム*」を参照してください。

手順

1. **設定** → **ストレージ** → **スケジュール設定** → **画像キャプチャ** に移動します。
2. 撮影スケジュールを設定します。スケジュール時間の設定については「*警戒スケジュール設定*」を参照してください。

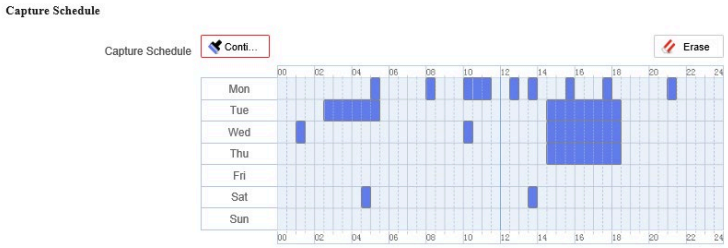

図5-1 キャプチャスケジュールの設定

3. キャプチャタイプを設定します。

   スケジュール

   設定した時間間隔で画像をキャプチャします。

   イベントトリガー

   イベントが発生し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**、**画質**、**間隔**、および**撮影枚数を設定**します。

注

キャプチャ画像の解像度は、キャプチャ画像ストリームの解像度と同じです。**詳細設定**で**ストリームタイプ**を選択できます。

5. **[保存]**をクリックします。

5.3.2 手動でのキャプチャ

手順

1. **[設定]** → **[ローカル]** に移動します。
2. スナップショットの**画像形式**と保存先を設定します。

JPEG

この形式の画像サイズは比較的小さく、ネットワーク伝送に適しています。

BMP

画質を保ちつつ圧縮されます。

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付近の「 」をクリックし、手動で画像をキャプチャします。

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、ダウンロードできます。

手順

1. **再生** → **画像** に移動します。
2. 検索条件を設定し、「**検索**」をクリックします。
   一致した画像がファイルリストに表示されます。
3. 画像をダウンロードします。

– 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**」をクリックすると、このページの画像をダウンロードできます。
– 「**すべてダウンロード**」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。

注記

設定 → **ローカル** → **再生キャプチャ保存パス** に移動し、再生時のキャプチャ画像の保存パスを確認・変更できます。

第6章 イベントとアラーム

このセクションではイベントの設定について説明します。デバイスはトリガーされたアラームに対して特定の応答を行います。特定のイベントは一部のデバイスモデルでサポートされない場合があります。

6.1 動体検知の設定

検知領域内の移動物体を検知し、連動動作をトリガーするのに役立ちます。

手順

1. **設定 → イベント → イベントと検知 → モーション検知** に移動します。
2. 「**有効化**」にチェックを入れます。
3. オプション：画像内の移動物体を緑色で表示するには、ハイライトを選択します。
   1) 「**動体検出の動的解析を有効にする**」にチェックを入れます。
   2) **設定 → 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を設定します。
   – 通常モードに関する情報は、***通常モード***を参照してください。
   – エキスパートモードの詳細については、***「エキスパートモード」を***参照してください。
5. 警戒スケジュールと連動方法を設定します。警戒スケジュール設定については***「警戒スケジュールの設定***」***を***参照してください。連動方法については「***連動方法の設定***」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、昼と夜で異なる動き検知パラメータを設定できます。

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です。

自動切替

システムが環境に応じて昼/夜モードを自動切替。昼間はカラー画像、夜間は白黒

画像を表示。

スケジュール切替

システムはスケジュールに従って昼/夜モードを切り替えます。設定期間中は昼モード（ ）に、その他の期間中は夜モードに切り替わります。

感度

感度値が高いほど、動き検出の感度が高くなります。スケジュール画像設定が有効な場合、昼と夜の感度を個別に設定できます。

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＆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。

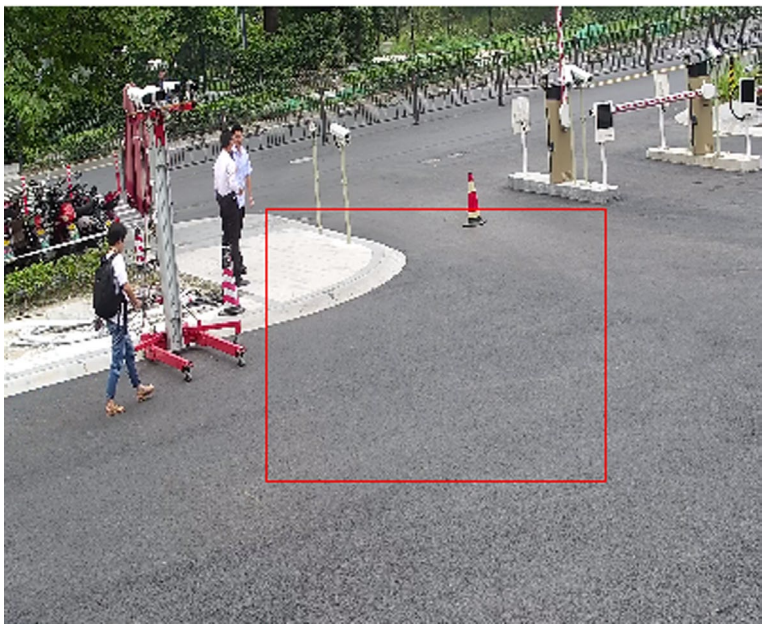

図6-1 ルール設定

4. 「 」をクリックすると、すべてのエリアがクリアされます。
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基づいて、動き検知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、動き検出の感度が高くなります。感度を***0***に設定すると、動き検出と動的分析は機能しません。

3. **検知対象**を設定します。人物と車両が選択可能です。検知対象を選択しない場合、人物と車両を含む全ての検知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（人物と車両）による警報発動が可能です。

注記

本機能は特定のデバイスモデルかつ特定の設定下でのみ利用可能です。実際の設定をご確認ください。

4. 「 」をクリックします。ライブ映像上でマウスをクリック＆ドラッグし、右クリックで1つのエリアの描画を終了します。
5. オプション：をクリックすると、すべてのエリアをクリアできます。
6. オプション：上記の手順を繰り返すことで、複数の領域のパラメータを設定できます。

6.2 映像改ざん警報の設定

設定した領域が覆われ、正常に監視できなくなった場合、警報が作動し、デバイスは特定の警報対応アクションを実行します。

手順

1. 「**設定**」→「**イベント**」→「**イベントと検知**」→「**映像改ざん検知**」に移動します。
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、エリア覆いを検出しやすくなります。
4. 「 」をクリックし、ライブビュー上でマウスをドラッグしてエリアを描画します。

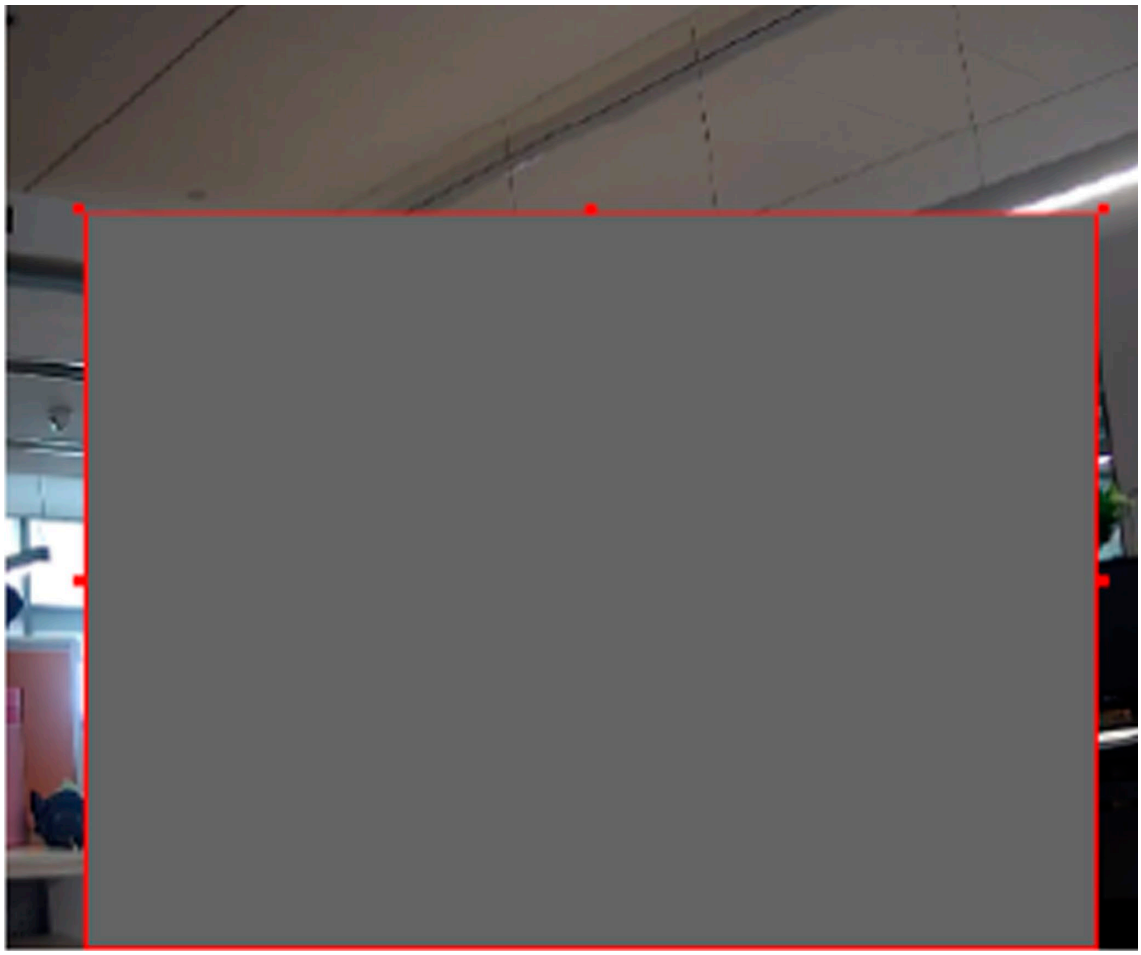

図6-2 映像改ざん検知エリアの設定

5. オプション：🗑 をクリックすると、描画した領域をすべて削除できます。
6. スケジュール設定については「*警備スケジュール設定*」を参照してください。*連動方法*の設定については「連動方法設定」を参照してください。
7. 「**保存**」をクリックします。

6.3 アラーム入力の設定

外部デバイスからの警報信号が、現在のデバイスの対応するアクションをトリガーします。

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。

外部警報装置が接続されていることを確認してください。ケーブル接続については*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 → イベントと検知 → アラーム入力** に移動します。
2. **アラーム入力番号**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. 「**Enable Alarm Input Handling**」にチェックを入れます。
5. スケジュール設定については「*セットアミングスケジュール設定」*を参照してください。*連動方法*の設定については「連動方法設定」を参照してください。
6. 「**Copy to...**」をクリックし、設定を他の警報入力チャンネルにコピーします。
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アクションを実行します。

手順

1. 「**設定**」→「**イベント**」→「**イベントと検知**」→「**例外**」に移動します。
2. **例外タイプ**を選択します。

HDD 満杯

HDDのストレージ容量が満杯です。

HDDエラー

HDDでエラーが発生しました。

ネットワーク切断

デバイスがオフラインです。

IPアドレスの競合

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と同一です。

不正なログイン

ユーザー名またはパスワードが正しくありません。

3. 連携方法の設定については、連携方法*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 映像品質診断の設定

デバイスの映像品質が異常で、警報連動が設定されている場合、警報が自動的に作動します。

手順

1. **設定 → イベント → イベントと検知 → 映像品質診断** に移動します。

2. **診断タイプ**を選択します。
3. 対応するパラメータを設定します。

警報検出間隔

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、誤検知の可能性も高くなります。

アラーム遅延時間

設定回数に達した時点で、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すると、関連するタイプが検出されます。
5. 警戒スケジュールを設定します。*「警戒スケジュール設定」*を参照してください。
6. 連動方法を設定します。*連動方法設定*を参照してください。
7. 「**保存**」をクリックします。

注記

本機能は一部モデル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。

6.6 音声異常検知の設定

音声異常検知機能は、音量の急激な増減など、シーン内の異常な音を検知し、特定の対応措置を講じることができます。

手順

1. **設定** → **イベント** → **イベントと検知** → **音声異常検知** に移動します。
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。

音声喪失検出

音声トラックの突然の喪失を検出します。

音量急増検知

音量の急激な増加を検出します。感度と**音量閾値は**設定可能です。

注記

- 感度が低いほど、検出をトリガーするにはより大きな変化が必要です。
- 音量閾値は検出時の音量基準値を指します。環境の平均音量に設定することを推奨します。周囲の音量が大きいほど、この値は高く設定する必要があります。実際の環境に応じて調整してください。

音圧レベルの急激な低下検出

音量の急激な低下を検知します。**感度は**設定可能です。

3. スケジュール設定については「警戒スケジュール設定」を参照してください。*連動方法*の設定については「連動方法設定」を参照してください。
4. 「**保存**」をクリックします。

注記

本機能は特定モデルのみ対応しています。実際の機能はモデルによって異なります。

6.7 ピント外れ検出の設定

レンズのピント外れによるぼやけた画像を検出できます。発生した場合、デバイスは連動動作を実行できます。

手順

1. **設定 → イベント → イベントと検出 → ピント外れ検出** に移動します。
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、ピント外れ画像が警報を発生しやすくなります。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。

注記

本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。

6.8 シーン変化検知の設定

シーン変化検出機能は、シーンの変化を検知します。アラームが作動した際に特定のアクションを実行できます。

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. 「**有効化**」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変化を検知しやすくなりますが、検知精度は低下します。
4. スケジュール設定については「警戒スケジュール設定」を参照してください。*連動方法*の設定については「連動方法設定」を参照してください。
5. 「**保存**」をクリックします。

注記

本機能は一部モデル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 警戒スケジュールと警報連動

武装スケジュールとは、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時間枠です。警報連動とは、スケジュールされた時間内に検知された特定の事象または対象に対する応答です。

7.1 警備スケジュール設定

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：関連イベントインターフェースで「**武装スケジュールと連動方法**」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。

注記

- 各セルは30分を表します。
- 描画した時間帯にマウスを合わせると、具体的な時間帯が表示され、開始時間と終了時間を微調整できます。
- 1日に最大8つの時間帯を設定できます。

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時間をクリアします。
5. **[OK]**をクリックして設定を保存します。

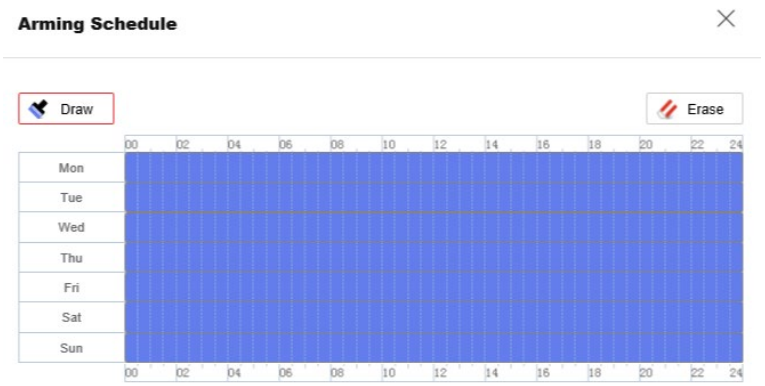

図7-1 警戒スケジュール設定

7.2 連動方法の設定

イベントまたはアラーム発生時に連動機能を有効にできます。

7.2.1 警報出力のトリガー

デバイスが警報出力デバイスに接続され、警報出力番号が設定されている場合、警報が発生するとデバイスは接続された警報出力デバイスに警報情報を送信します。

手順

1. **設定 → イベント → アラーム設定 → アラーム出力** に移動します。
2. アラーム出力パラメータを設定します。

自動アラーム	設定に関する詳細は、***自動警報***を参照してください。
手動アラーム	設定に関する詳細は、***手動アラーム***を参照してください。

手動アラーム

アラーム出力を手動でトリガーできます。

開始前に

アラーム出力デバイスが本装置に接続されていることを確認してください。

手順

1. 外部警報装置に接続された警報インターフェースに応じて、**警報出力番号を選択します**。警報パラメータを設定するには、 をクリックします。

   アラーム名

   アラーム出力用の名前を任意に設定します。
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：手動警報を無効にするには「**Clear Alarm**」をクリックします。

自動警報

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作動スケジュールで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本装置に接続されていることを確認してください。

手順

1. 外部警報装置に接続された警報インターフェースに応じて、**警報出力番号を選択します。** をクリックして警報パラメータを設定します。

   アラーム名

   アラーム出力用の名前をカスタム設定します。

   遅延時間

   警報発生後、警報出力が維持される時間間隔を指します。
2. アラームスケジュールを設定します。設定方法については*「アラームスケジュール設定」を*参照してください。
3. オプション：**「コピー先…」**をクリックし、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/メモリー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*メモリカード*の設定」*を参照してください。

7.2.3 電子メール送信

「**メール送信**」にチェックを入れると、アラームイベントが検出された際に、指定されたアドレス宛にアラーム情報を含む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

メールが設定され、連携方法として**「メール送信」**が有効になっている場合、アラームイベントが検出されると、デバイスは指定されたすべての受信者にメール通知を送信します。

開始前に

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。**設定 → ネットワーク → ネットワーク設定 → 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：**設定 → イベント → アラーム設定 → メール**

2. メールパラメータを設定します。
   1) 送信者情報（**送信者アドレス**、**SMTPサーバー**、**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、**「認証」**にチェックを入れ、サーバーへのログイン用ユーザー名とパスワードを入力します。
   3) **メール暗号化**を設定します。
      - **TLS**を選択しSTARTTLSを無効にした場合、メールはTLSで暗号化されて送信されます。SMTPポートは465に設定してください。
      - **TLS**を選択し**STARTTLSを有効**にした場合、メールはSTARTTLSで暗号化されて送信され、**SMTPポートは**25に設定する必要があります。

      注記

      STARTTLSを使用する場合は、メールサーバーがプロトコルをサポートしていることを確認してください。メールサーバーがプロトコルをサポートしていない状態で**「STARTTLSを有効にする」**にチェックを入れると、メールは暗号化されずに送信されます。

   4) オプション：アラーム画像付き通知を受け取りたい場合は、**「画像添付」**にチェックを入れます。通知メールには、設定可能な画像キャプチャ間隔で、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

      アラーム画像の枚数は、デバイスモデルやイベントの種類によって異なる場合があります。

   5) 受信者の情報（氏名、住所など）を入力します。
   6) **「テスト」**をクリックし、機能が正しく設定されているか確認します。
3. **「保存」**をクリックします。

7.2.4 監視センターへの通知

監視センター通知にチェックを入れると、警報イベントが検出された際に警報情報が監視センターにアップロードされます。

7.2.5 録画トリガー

録画をトリガーするにチェックを入れると、デバイスは検知されたアラームイベントに関するビデオを録画します。
録画設定については、*「動画録画と静止画キャプチャ」*を参照してください。

7.2.6 点滅ライト

点滅ライトを有効化し、**点滅ライト警報出力を設定すると**、警報イベントが検出された際にライトが点滅します。

点滅警報灯出力の設定

イベント発生時、装置の点滅ライトを警報として作動させることができます。

手順

1. **設定 → イベント → アラーム設定 → 点滅アラームライト出力** に移動します。
2. 点滅時間と**点滅頻度**を設定します。

点滅時間

1回の警報発生時に点滅が持続する時間。

点滅頻度

ライトが点滅する速度。高頻度、中頻度、低頻度、常時点灯から選択可能。

3. 警戒スケジュールを設定します。詳細は*「警戒スケジュールの設定」*を参照してください。
4. 「**保存**」をクリックします。

注

本機能は特定のデバイスモデルのみ対応しています。

7.2.7 音声警告

音声警告を有効にし、**音声警報出力を設定**すると、警報発生時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。
可聴警報出力の設定については、*「可聴警報出力の設定」*を参照してください。

注記

この機能は特定のカメラモデルでのみサポートされています。

音声アラーム出力の設定

デバイスが検知エリア内で対象物を検出すると、警告として可聴警報が作動します。

手順

1. **設定 → イベント → アラーム設定 → 音声アラーム出力** に移動します。
2. **音源タイプ**を選択し、関連パラメータを設定します。
   – **プロンプト**を選択し、必要な警報時間を設定します。

– **警告**を選択し、その内容を設定します。必要な警報時間を設定します。
– **カスタム音声**を選択します。ドロップダウンリストからカスタム音声ファイルを選択できます。ファイルがない場合は、**設定 → 追加**をクリックして要件を満たす音声ファイルをアップロードできます。最大3つの音声ファイルをアップロード可能です。

3. オプション：**テスト**をクリックすると、選択した音声ファイルをデバイスで再生できます。
4. 音声アラームの武装スケジュールを設定します。詳細は「*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。

注記

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

本デバイスは、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、HTTPS、またはISUPデータ伝送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 → イベント → アラーム設定 → アラームサーバー** に移動します。
2. **宛先IPまたはホスト名**、**URL**、**ポート**を入力します。
3. **プロトコル**を選択します。

注記

HTTP、HTTPS、ISUPが選択可能です。通信中のデータ伝送を暗号化するため、HTTPSの使用を推奨します。

4. **[テスト]**をクリックし、IPまたはホストが利用可能か確認します。
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前に、TCP/IP設定を適切に構成する必要があります。IPv4とIPv6の両方がサポートされています。両バージョンは互いに競合することなく同時に設定可能です。

設定 → ネットワーク → ネットワーク設定 → TCP/IP でパラメータ設定を行います。

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）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にチェックを入れると、デバイスはネットワークから自動的にIPv4パラメータを取得します。機能有効化後、デバイスのIPアドレスは変更されます。SADPを使用してデバイスのIPアドレスを取得できます。

注

デバイスが接続されているネットワークは、DHCP（ダイナミックホスト構成プロトコル）をサポートしている必要があります。

マニュアル

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

IPv6

3つのIPv6モードが利用可能です。

ルートアドバタイズメント

IPv6アドレスは、ルートアドバタイズメントとデバイスのMACアドレスを組み合わせて生成されます。

注記

ルートアドバタイズメントモードは、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確認してください。

MTU

最大伝送単位を意味します。単一のネットワーク層トランザクションで通信可能な最大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場合や、一部のアプリケーション（例：メール送信）で必要となります。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」にチェックを入れ、**「登録ドメイン名」**を入力します。この登録ドメイン名でデバイスが登録され、ローカルエリアネットワーク内での管理が容易になります。

注記

動的ドメイン名を有効にするには、**DHCPが**有効になっている必要があります。

8.2 ドメイン名による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）を利用できます。デバイスの動的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、ドメイン名経由のネットワークアクセスを実現します。本デバイスのDDNSサービスはHTTPSのみをサポートします。

開始前に

デバイスのDDNS設定を行う前に、DDNSサーバーへの登録が必要です。

手順

1. ***TCP/IP***を参照し、DNSパラメータを設定します。
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. **「有効にする」**をチェックし、**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ます。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ます。

ブラウザ経由	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経由	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

本デバイスはPPPoE自動ダイヤルアップ機能をサポートしています。モデムに接続後、ADSLダイヤルアップにより公衆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. **[設定] → [ネットワーク] → [ネットワーク設定] →** [**PPPoE**] に移動します。
2. **[有効化]** にチェックを入れます。
3. PPPoEパラメータを設定します。

動的IP

ダイヤルアップ接続成功後、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接続用のパスワード。

確認

ダイヤルアップパスワードを再度入力してください。

4. **[保存]**をクリックします。
5. デバイスにアクセスします。

ブラウザによるアクセス	ブラウザのアドレスバーに WAN 動的 IP アドレス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	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

トウェアによる方法　す。詳細はクライアント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経由で動的に割り当てられるため、カメラの再起動後は常にIPアドレスが変更されます。動的IPの不便さを解消するには、DDNSプロバイダ（例：DynDns.com）からドメイン名を取得する必要があります。詳細情報は「*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

SNMP（Simple Network Management Protocol）を設定して、ネットワーク管理でデバイス情報を取得できます。

開始前に

SNMP設定前に、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受信できる環境を整えてください。

手順

1. **設定 → ネットワーク → ネットワーク設定 → SNMP** に移動します。
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**にチェックを入れます。

注記

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させる必要があります。
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は安全ではなく、SNMP v2はアクセスにパスワードを必要とします。SNMP v3は暗号化を提供し、第3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の設定

IEEE 802.1Xを設定することで、接続デバイスのユーザー権限を認証できます。
設定 → ネットワーク → ネットワーク設定 → 802.1X に移動し、機能を有効にします。ルーター情報に基づきプロトコルとバージョンを選択します。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、**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、**証明書管理**で選択した証明書に異常がないか確認してください。

8.6 QoSの設定

QoS（Quality of Service）は、データ送信の優先度を設定することで、ネットワークの遅延や輻輳を改善するのに役立ちます。

注記

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

手順

1. **設定** → **ネットワーク** → **ネットワーク設定** → **QoS** に移動します。
2. **ビデオ/オーディオDSCP**、**イベント/アラームDSCP**、**管理DSCP**を設定します。

   注記

   ネットワークはデータ伝送の優先度を識別できます。DSCP値が大きいほど優先度が高くなります。設定時にはルーター側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は暗号化伝送と身元認証を可能にするネットワークプロトコルであり、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. **[設定]** → **[ネットワーク]** → **[ネットワークサービス]** → **[HTTP(S)]** に移動します。
2. **HTTPポート**を入力します。

注記

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、ログインにはブラウザでhttp://192.168.1.64:81を入力する必要があります。

3. **HTTPS** の**有効**化にチェック**を入れます**。

注

「**TLS設定**」をクリックすると、デバイスがサポートするTLSバージョンを設定できます。詳細はを参照してください。

4. **HTTPSポート**を入力します。
5. オプション：**HTTPSブラウジングに**チェックを入れ、HTTPSプロトコル経由でのみデバイスにアクセスします。
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

ダイジェスト認証とダイジェスト/ベーシック認証がサポートされています。これは、デバイスへのWEBリクエスト送信時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認証またはベーシック認証をサポートします。**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。

ダイジェストアルゴリズム

WEB認証におけるMD5、SHA256、およびMD5/SHA256暗号化アルゴリズム。MD5以外のダイジェストアルゴリズムを有効にした場合、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 デバイスへのログインやライブビューを有効化できない可能性があります。強度の高い暗号化アルゴリズムの使用を推奨します。

8. [**保存**]をクリックします。

8.8 マルチキャスト

マルチキャストは、データ送信が複数の宛先デバイスに同時に送信されるグループ通信です。

マルチキャスト設定は、**[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]** で設定します。

IPアドレス

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 に移動し、この機能を有効にしてください。
マルチキャスト検出を有効にするにチェックを入れ、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がオンラインネットワークカメラを自動的に検出できるようにします。

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]** に移動します。
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

   ダイジェスト認証とダイジェスト/基本認証がサポートされています。これは、RTSPリクエストをデバイスに送信す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/基本認証**を選択した場合、デバイスはダイジェスト認証または基本認証をサポートします。**ダイジェスト認証**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。

   ダイジェストアルゴリズム

   RTSP認証におけるMD5、SHA256、およびMD5/SHA256暗号化アルゴリズム。MD5以外のダイジェストアルゴリズムを有効にした場合、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へのログインやライブビューの有効化を行えない可能性があります。強度の高い暗号化アルゴリズムの使用を推奨します。
5. **[保存]**をクリックします。

8.10 SRTPの設定

セキュアリアルタイムトランスポートプロトコル（SRTP）は、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あり、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 データの暗号化、メッセージ認証と完全性、および再生攻撃からの保護を提供することを目的としています。

手順

1. **[設定]→[ネットワーク]→[ネットワークサービス]→[SRTP]** に移動します。
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**を選択します。
5. **暗号化アルゴリズム**を選択します。
6. **[保存]**をクリックします。

注記

- 特定のデバイスモデルのみがこの機能をサポートしています。
- 機能が正常に動作しない場合は、***証明書管理***で選択した証明書に異常がないか確認してください。

8.11 Bonjour

Bonjour は、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設定ネットワーク (zeroconf) を実装したものです。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、プリンタ、他のコンピュータ、およびそれらのデバイスがローカルネットワーク 上で提供するサービスなどのデバイスを検索します。

設定 → ネットワーク → ネットワークサービス → Bonjour に移動し、機能有効化後「**保存**」をクリックします。

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

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 プロトコルを有効にする必要があります。有効にしない場合、ライブビュー、画像キャプチャ、デジタルズームなどの機能を使用できません。
設定 → ネットワーク → ネットワークサービス → WebSocket に移動してパラメータを設定し、**保存**をクリックします。

WebSocket

HTTPプロトコル経由のプラグイン不要プレビュー用、TCPベース全二重通信プロトコルポート。

WebSockets

HTTPSプロトコル経由のプラグイン不要プレビュー用TCPベース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、指定したポートからデバイスにアクセスできます。

手順

1. **設定 → ネットワーク → ネットワークサービス → NAT** に移動します。
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	詳細については「*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	詳細については「*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**」にチェックを入れ、カメラのフレンドリーネームを選択します。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™機能も同時に有効にしてください。

8.13.2 手動ポートマッピングの設定

手順

1. 「**UPnP™を有効にする**」にチェックを入れ、デバイスにわかりやすい名前を付けるか、デフォルト名を使用します。
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値に設定します。
3. 「**保存**」をクリックします。

次の操作

ルーターのポートマッピング設定画面で、ポート番号とIPアドレスをデバイス設定と同じに設定してください。詳細はルーターの取扱説明書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設定

以下の設定は特定のルーター向けです。ルーターの機種によって設定内容は異なります。

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. 「**転送**」→「**仮想サーバー**」に移動し、**ポート**番号と**IPアドレス**を入力します。
4. 「**保存**」をクリックします。

例

カメラが同一ルーターに接続されている場合、1台のカメラのポートをIPアドレス192.168.1.23で80、8000、554に設定し、別のカメラのポートをIPアドレス192.168.1.24で81、8001、555、8201に設定できます。

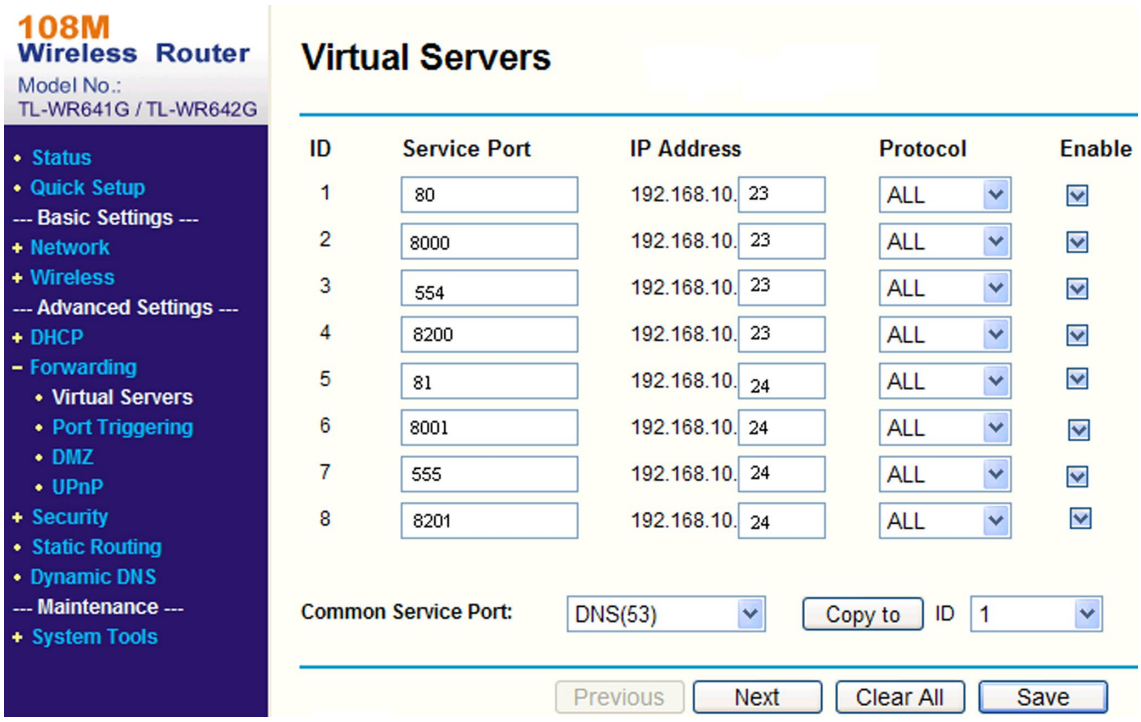

図 8-1 ルーターでのポートマッピング

注記

ネットワークカメラのポートは他のポートと競合できません。例えば、ルーターのWeb管理ポートが80の場合、カメラのポートが管理ポートと同じであれば変更してください。

8.14 RTCP

本デバイスは、パケットを順番に配信する信頼性の高い配信メカニズムを提供し、フロー制御や輻輳制御のサービスを提供するために、RTCP（リアルタイムトランスポート制御プロトコル）に依存しています。

設定 → ネットワーク → ネットワークサービス → RTCP に移動し、**[有効化]** をチェックして機能を有効にします。

8.15 ワイヤレスダイヤル

音声、動画、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することができます。

注記

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設定

内蔵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へのダイヤルアップアクセスが可能になります。

開始前に

SIM カードを入手し、3G/4G サービスを有効にしてください。SIM カードを対応するスロットに挿入します。

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** に移動します。
2. 機能の有効化を確認します。
3. 「**ダイヤルパラメータ**」で設定を行い、保存します。
4. 「**ダイヤルプラン**」の横にある「**設定**」をクリックします。詳細情報は「*武装スケジュール設定*」を参照してください。
5. **ダイヤル状態**を確認します。

   [更新]をクリック　ダイヤル状態を更新します。

   切断をクリック　3G/4G無線ネットワークを切断します。

   ダイヤル状態が「接続済み」に変わると、ダイヤルが成功したことを意味します。
6. ネットワーク内のコンピューターの**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ます。
   – クライアントアプリケーションでデバイスを追加します。**IP/ドメイン**を選択し、IPアドレスと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カード情報と通信キャリア情報を確認できます。

注意

パフォーマンスモードまたは**プロアクティブモード**で動作する特定のデバイスモデルでは、無線モードのアップグレードが可能です。必要に応じて、専門家の指導のもとで無線モードをアップグレードしてください。

8. オプション：**[再接続]**をクリックすると、デバイスを手動で無線ネットワークに再接続できます。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：**自動再接続を**有効にするには「**有効**」をチェックし、**再接続間隔**を設定します。設定された**間隔で**自動的に無線ネットワークに再接続します。

注

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 ワイヤレス詳細設定

ワイヤレスエキスパート設定では、 が接続する 3G/4G ワイヤレスネットワークの詳細情報を提供し、専門家が潜在的なネットワーク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

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無線ネットワーク情報を提供します。

設定 → ネットワーク → ネットワーク設定 → 無線ダイヤル → 詳細設定 に移動すると、セル無線周波数パラメータを確認できます。

ネットワーク情報

現在のセルラーネットワーク情報を表示します。**「更新」**をクリックすると、異なるセルの周波数情報を確認できます。

無線周波数変動

過去7日間にデバイスが接続したセルラーネットワークの変動を記録します。**「レポートをエクスポート」**をクリックし、暗号化パスワードを設定・確認して変動レポートをエクスポートできます。

バンドロック

デバイスがより高速なデータレートを取得できる一連の周波数帯域をロックし、ネットワーク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 → 無線ダイヤル → 詳細設定 → ロックバンド** に移動します。
2. **「有効化」**にチェックを入れます。
3. **「追加」**をクリックし、帯域を入力します。

注記

- 入力するバンドは「B + 番号」または「N + 番号」形式とします。例：B1 または N1。
- 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：選択したバンドを削除するには「 」をクリックします。**「Clear All」**をクリックするとリスト全体をクリアできます。

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通信パケットをキャプチャし、4Gモジュールと基地局間の通信障害の特定を支援します。

手順

注意

本機能は専門家および技術サポートスタッフ専用です。

1. **設定** → **ネットワーク** → **ネットワーク設定** → **無線ダイヤル** → **専門家設定** に移動します。
2. 「**ベースバンドパケットキャプチャ**」の「**設定**」をクリックし、設定画面に入ります。
3. 「**有効化**」にチェックを入れて機能を有効にします。
4. キャプチャ時間と保存先を設定します。保存先はデバイスの実際のストレージ方式に依存します。「**このパス下のキャプチャ済みパケットを削除**」をクリックするとキャプチャ済みパケットを削除できます。
5. **[保存]** をクリックします。
6. 「**パケットキャプチャ開始**」をクリックしてベースバンドパケットをキャプチャします。
7. オプション: **[キャプチャを停止]** をクリックしてキャプチャ処理を停止します。
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. 「**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**」→「**詳細設定**」に移動します。
2. 「**速度テスト**」の「**設定**」をクリックして設定画面に入ります。
3. デフォルトサーバーを選択するか、サーバーアドレスを入力します。以下の手順で近くのサーバーアドレスを取得できます。

注意

以下の手順で近くのサーバーアドレスを取得できます。

1. 最寄りのサーバーアドレスを取得するには、こちらのウェブサイトにアクセスしてください：***https://www.speedtest.net/speedtest-servers-static.php***
2. 近くの速度テストステーションの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。
   テスト完了後、速度の詳細を確認できます。「**速度テスト結果をエクスポート**」をクリックすることも可能です。

8.16 WLAN AP（アクセスポイント）

本デバイスはWLAN AP機能により無線アクセスポイントとして使用可能です。スマートフォンやPCを本デバイスのAPに接続することで、端末へのアクセスやパラメータ設定をスマートフォンやPCから行えます。

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。

8.16.1 WLAN APの設定

手順

1. **[設定] → [ネットワーク] → [ネットワーク設定] → [WLAN AP]** に移動します。
2. WLAN APモードを選択します。

   オン

   機能が有効になります。

   メンテナンスモード

   デバイスのコールドブート（デバイスのスイッチを**ONにすること**）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機能が無効になり、4G通信が異常な場合は有効のままとなります。

   オフ

   関数は無効化されています。
3. 関連するパラメータを設定します。

   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」と命名されています。
   特定のデバイスモデルでは、デバイスのデフォルトSSIDはデバイスラベル上で「Default SSID」と表示されます。
   必要に応じて定義できます。

   セキュリティモード

   WPA2-パーソナルモードがサポートされています。

   暗号化方式

AES および **TKIP** を選択できます。

パスワード

本機AP経由の無線接続用パスワード。初期パスワードはカメラの9桁シリアル番号です。初回ログイン後、初期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。

ご注意

製品のセキュリティ強化のため、ご自身で設定した強力なパスワード（大文字、小文字、数字、特殊文字を含む8文字以上）の使用を強く推奨します。特に高セキュリティシステムでは、パスワードを定期的に（月次または週次で）リセットすることで、製品をより効果的に保護できます。

4. 「**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る場合があります。

次の手順

携帯電話や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、デバイスのAP経由でアクセスできます。

手順

1. **設定 → ネットワーク → ネットワーク設定 → WLAN AP** に移動し、WLAN AP機能を有効にします。

   特定のデバイスモデルでは、デバイスのコールドブート（デバイスのスイッチを**ONにすること**）後、WLAN AP機能が自動的に5分間オンになります。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、4G通信が異常であればオンのままになります。

2. スマートフォンまたはPCのWLANリストから、対象デバイスのWLAN APを検索します。
3. パスワードを入力し、携帯電話またはPCをAPに接続します。

注記

- AP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 → 基本情報**から確認できます。

- 一部のデバイスモデルでは、AP名はデバイスラベルに記載の「Default SSID」となります。

4. ブラウザにIPアドレスを入力します。

注記

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は「**接続済みデバイス**」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、送信前のビデオデータパケットを整形・平滑化するために使用されます。
これにより、ネットワーク輻輳による遅延やパケット損失を改善し、ビデオ品質を確保します。整形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 ルーターを通じて提供されます。

手順

1. **設定 → ネットワーク → ネットワーク設定 → データモニタリング** に移動します。
2. 「**有効化**」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を設定します。

プランタイプ

日単位、**月単位**、**年単位**から選択可能です。

データプラン

利用可能なデータ量を入力し、単位を選択してください。

事前警告閾値

使用データ量がデータプランの指定割合に達すると、デバイスが警告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. **通常連動**を選択します。

「**メール送信**」または「**監視センター通知**」を選択した場合、使用データが閾値に達すると、デバイスはメールまたは監視センターへ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。

注記

この機能は、デバイスの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。

注記

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。

8.19.1 デバイスをWi-Fiに接続する

開始前に

SSID、キー、その他のパラメータの設定については、無線ルーターまたはアクセスポイントの取扱説明書を参照してください。

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. パラメータを設定するには**WLAN**を選択します。詳細な設定については***TCP/IP***を参照してください。

注記

Wi-Fiを安定して使用するには、DHCPの使用は推奨されません。

3. Wi-Fi設定ページに移動：**設定 → ネットワーク → ネットワークサービス → Wi-Fi**。
4. パラメータを設定して保存します。
   1) Wi-Fi機能を有効にするためにチェックを入れます。
   2) **Refresh**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・選択するか、＋ をクリックして手動で追加します。
   3) **SSID**を選択または入力します。これは無線ルーターまたはアクセスポイントのSSIDと一致している必要があります。
      ネットワークのパラメータは自動的に**Wi-Fiに**表示されます。
   4) **ネットワークモード**を「**管理**」に設定します。

5) 必要に応じて**セキュリティモード**を選択し、その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のパラメータと同じである必要があります。
6) 「**保存**」をクリックします。

次の操作

TCP/IP設定ページへ移動：**設定 → ネットワーク → ネットワーク設定 → TCP/IP、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の設定

デバイスがISUPプラットフォーム（旧称Ehome）に登録されると、パブリックネットワーク経由でデバイスの閲覧・管理、データ送信、アラーム情報の転送が可能になります。

手順

1. **設定 → ネットワーク → プラットフォームアクセス → ISUP** に移動します。
2. オプション：アクセスセンターを選択します。
3. 「**有効化**」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 HiLookVisionによるカメラアクセス

HiLookVisionはモバイル端末用アプリケーションです。本アプリを使用すると、ライブ映像の閲覧やアラーム通知の受信などが可能です。

始める前に

ネットワークケーブルでカメラをネットワークに接続してください。

手順

1. 以下の方法でHiLookVisionアプリケーションを入手しインストールしてください。
https://appstore.hikvision.com にアクセスし、お使いの携帯電話のシステムに応じてアプリケーションをダウンロードしてください。当社公式サイトにアクセスし、「**サポート**」→「**ツール**」→「**Hikvision App Store**」に進んでください。下記の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、画面右上の「**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、HiLookVisionユーザーアカウントを登録してください。
3. 登録後、ログインします。
4. アプリ内で右上の「+」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コードはカメラ本体またはパッケージ内のクイックスタートガイド表紙に記載されています。
5. 画面の指示に従いネットワーク接続を設定し、カメラをHiLookVisionアカウントに追加します。

詳細はHiLookVisionアプリユーザーマニュアルを参照してください。

8.21.1 カメラでのHiLookVisionサービスの有効化

HiLookVision サービスをご利用になる前に、カメラで HiLookVision サービスを有効にする必要があります。
SADPソフトウェアまたはWebブラウザからサービスを有効化できます。

Web ブラウザで HiLookVision サービスを有効にする

Web ブラウザで HiLookVision 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

サービスを有効化する前に、カメラのアクティベーションが必要です。

手順

1. Webブラウザで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画面に入ります。**設定 → ネットワーク → プラットフォームアクセス → HiLookVision**。
3. 「**有効化**」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」と「プライバシーポリシー」をクリックし、内容を確認してください。
5. カメラ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。

注記

カメラをHiLookVisionサービスに追加する際には、検証コードが必要です。

6. 設定を保存します。

SADPソフトウェア経由でHiLookVisionサービスを有効化する

このセクションでは、アクティベート済みのカメラのSADPソフトウェアを使用してHiLookVisionサービスを有効化する方法を説明します。

手順

1. SADPソフトウェアを起動します。
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. 「**HiLookVisionを有効にする**」にチェックを入れます。
4. 認証コードを作成するか、既存の認証コードを変更します。

注記

カメラをHiLookVisionサービスに追加する際には検証コードが必要です。

5. 「利用規約」と「プライバシーポリシー」をクリックして読みます。
6. 設定を確認します。

8.21.2 HiLookVisionの設定

手順

1. 以下の方法でHiLookVisionアプリケーションを入手・インストールしてください。

https://appstore.hikvision.com にアクセスし、お使いの携帯電話のシステムに応じてアプリケーションをダウンロードしてください。当社公式サイトにアクセスし、「**サポート**」→「**ツール**」→「**Hikvision App Store**」に進んでください。下記の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、画面右上の「**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、HiLookVision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 HiLookVisionへのカメラ追加

手順

1. モバイルデバイスをWi-Fiに接続します。
2. HiLookVisionアプリにログインします。
3. ホーム画面で右上の「+」をタップし、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認識できないほどぼやけている場合は、カメラのシリアル番号を入力して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てください。

注意

- 必要な認証コードは、カメラでHiLookVisionサービスを有効化する際に作成または変更したコードです。
- 認証コードを忘れた場合は、ウェブブラウザから**プラットフォーム**アクセス設定ページで現在の認証コードを確認できます。

6. ポップアップ画面で**「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。

無線接続

スマートフォンが接続している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設定時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	ネットワークケーブルでカメラをルーターに接続し、結果画面で「**接続済み**」をタップします。

注意

ルーターは、お使いの携帯電話が接続しているものと同じである必要があります。

8. 次の画面で「**追加**」をタップし、追加を完了します。

詳細については、HiLookVision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の設定

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セキュリティを強化できます。

手順

1. **設定 → ネットワーク → プラットフォームアクセス → オープンネットワークビデオインターフェース** に移動します。
2. **[有効化]** 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。
   - **ダイジェスト＆ws-usernameトークン**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トークン認証をサポートします。
4. 「**追加**」をクリックし、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、Open Network Video Interface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Open Network Video Interfaceユーザーを削除します。
   - 選択したOpen Network Video Interfaceユーザーを変更するには、[ ]をクリックします。

8.23 SDKサービスの設定

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. **[設定]** → **[ネットワーク]** → **[プラットフォームアクセス]** → **[SDKサービス]** に移動します。
2. **SDKサービスの**パラメータを設定します。
   1) SDKプロトコルでクライアントソフトウェアにデバイスを追加するには「**有効化**」にチェックを入れます。
   2) **ポート**番号を入力します。
3. **拡張SDKサービスの**パラメータを設定します。
   1) **[有効化]** にチェックを入れると、TLS プロトコル経由の SDK でデバイスをクライアントソフトウェアに追加できます。
   2) オプション: **[TLS設定]**をクリックし、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) データ伝送のセキュリティを確保するため、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できます。詳細は***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 → システム → システム設定 → 基本情報 に移動してデバイス情報を表示します。

9.1.2 日付と時刻

タイムゾーン、時刻同期、夏時間（DST）の設定により、デバイスの時刻と日付を設定できます。

手動で時刻を同期する

手順

1. **設定 → システム → システム設定 → 時刻設定** に移動します。
2. 「**タイムゾーン**」を選択します。
3. 「**手動時刻同期**」を選択します。
4. 時刻同期方法を選択します。
   – 「**時刻を設定**」を選択し、手動で入力するか、ポップアップカレンダーから日付と時刻を選択します。

「**コンピューターの時刻と同期**」をクリックすると、デバイスの時刻がローカルPCの時刻と同期されます。

5. 「**保存**」をクリックします。

NTPサーバーの設定

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サーバー情報を入手してください。

手順

1. **[設定] → [システム] → [システム設定] → [時刻設定]** に移動します。
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、間隔**を設定します。

> **注記**
> サーバーアドレスはNTPサーバーのIPアドレスです。

5. サーバー接続をテストするには「**テスト**」をクリックします。
6. [**保存**]をクリックします。

衛星による時刻同期

> **注記**
> この機能は、デバイスによって異なります。

手順

1. **設定 → システム → システム設定 → 時間設定** に移動します。
2. 「**衛星時刻同期**」を選択します。
3. **間隔**を設定します。
4. 「**保存**」をクリックします。

夏時間設定

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. **設定 → システム → システム設定 → 時刻設定** に移動します。
2. 「**有効**」にチェックを入れます。
3. **開始時刻、終了時刻、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の設定

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

開始前に

RS-232ケーブルでデバイスをコンピュータまたは端末に接続してください。

手順

1. **設定 → システム → システム設定 → RS-232** に移動します。
2. デバイスとコンピュータまたは端末を一致させるようRS-232パラメータを設定します。
3. 「**保存**」をクリックします。

9.1.4 RS-485の設定

RS-485は、デバイスを外部機器に接続するために使用されます。通信距離が長すぎる場合、RS-485を使用してデバイスとコンピュータまたは端末間でデータを送信できます。

開始前に

RS-485 ケーブルで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. **設定 → システム → システム設定 → RS-485** に移動します。
2. RS-485パラメータを設定します。

> **注意**
> デバイスとコンピュータまたは端末のパラメータはすべて同一に保つ必要があります。

3. **[保存]**をクリックします。

9.1.5 ライブビュー接続の設定

リモートライブビュー接続量を制御します。
ライブビュー接続は、同時にストリーミングできるライブビューの最大数を制御します。
設定 → システム → システム設定 → システムサービス に移動し、リモート接続数の上限を設定します。

9.1.6 位置情報設定

位置情報は、デバイスの現在の経度と緯度を表示およびアップロードします。

自動アップロード

「**有効にする**」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。
設定した間隔でデバイスが位置情報をアップロードします。「**更新**」をクリックすると手動で位置情報を更新できます。

手動設定

「**有効にする**」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アップロードします。

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

補助ライト、ハウジング上のワイパー、 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については、ハウジングと併用する場合、Web ブラウザ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ライセンスの表示

右上隅の をクリックし、「**オープンソースソフトウェアの説明**」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 ウィーガンド

注記

この機能は特定のカメラモデルでのみサポートされています。

[有効化] 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ウィーガンドプロトコルで出力されます。

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の設定

管理者は、他のアカウントの追加、変更、削除、および異なるユーザーレベルに異なる権限を付与することができます。

注意

ネットワーク上でデバイス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デバイスを使用する場合は、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. **設定 → システム → ユーザー管理 → ユーザー管理** に移動します。
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、**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権限を割り当てます。

管理者

管理者は全ての操作権限を持ち、ユーザーやオペレーターの追加、権限の割り当てが可能です。

ユーザー

ユーザーにはライブ映像の閲覧、PTZパラメータの設定、自身のパスワード変更の権限を割り当てられますが、その他の操作権限はありません。

オペレーター

オペレーターには、管理者操作とアカウント作成を除く全ての権限を割り当てることができます。

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。

注記

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、Web ブラウザ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 に移動し、**[一般]** をクリックして、**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が表示されます。

設定 → システム → ユーザー管理 → オンラインユーザー に移動し、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。
[メンテナンスとセキュリティ] → [メンテナンス] → [再起動] に移動し、**[再起動]** をクリックします。

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入手する必要があります。

注意
プロセス中に電源を切断しないでください。アップグレード後、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**」に移動します。
2. アップグレード方法を選択します。

   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指定します。

   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属するディレクトリを指定します。

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、デバイスパラメータをデフォルト設定に復元するのに役立ちます。

手順
1. **[メンテナンスとセキュリティ] → [メンテナンス] → [バックアップと復元]** に移動します。
2. 必要に応じて「**復元**」または「**既定値**」をクリックします。

   復元　ユーザー情報、IPパラメータ、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を工場出荷時のデフォルトにリセットします。

注意

この機能を使用する際は注意してください。工場出荷時のデフォルトにリセットすると、すべてのパラメータ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での一括設定を迅速に行うのに役立ちます。

手順

1. 設定ファイルをエクスポートします。
   1) **[メンテナンスとセキュリティ]→[メンテナンス]→[バックアップと復元]→[バックアップ]** に移動します。
   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、設定ファイルをローカルコンピュータに保存します。
2. 設定ファイルのインポート
   1) 設定対象デバイスにWebブラウザでアクセスします。
   2) **[メンテナンスとセキュリティ]→[メンテナンス]→[バックアップと復元]→[リセット]** に移動します。
   3) 「🗀」をクリックし、保存した設定ファイルを選択します。
   4) 設定ファイルのエクスポート時に設定した暗号化パスワードを入力します。
   5) **[Import]**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]→[メンテナンス]→[ログ]** に移動します。
2. 検索条件として「**主要タイプ**」「**副次タイプ**」「**開始時刻**」「**終了時刻**」を設定します。
3. **[検索]**をクリックします。
   一致したログファイルがログリストに表示されます。

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・分析し、不正侵入を検知してセキュリティイベントのトラブルシューティングを行うことができます。

手順

注記

この機能は特定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**」→「**メンテナンス**」→「**セキュリティ監査ログ**」に移動します。
2. ログの種類、**開始時刻**、**終了時刻**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。
[メンテナンスとセキュリティ]→[メンテナンス]→[デバイスデバッグ] に移動し、**[SSH の設定]** をクリックします。ポート番号を編集できます。**[保存]** をクリックします。

注意

本機能は慎重にご利用ください。機能を有効にした場合、デバイス内部情報の漏洩リスクが存在します。

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。
「**メンテナンスとセキュリティ**」→「**メンテナンス**」→「**デバイスデバッグ**」→「**診断情報**」に移動します。「**エクスポート**」をクリックします。ポップアップウィンドウで、必要な診断情報にチェックを入れ、「**エクスポート**」をクリックすると、デバイスの対応する診断情報をエクスポートできます。

9.3.9 診断

4G ネットワークをサポートするデバイスでは、診断により、将来のメンテナンスやトラブルシューティングのために、通信パケット、デバイスの電源、ネットワーク情報を取得することができます。

デバイスパケットのキャプチャ

この機能は専門家向けに用意されており、将来の問題診断やデバッグのために、デバイスと外部デバイス間の通信パケットを取得するために使用されます。

手順

注
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**」→「**メンテナンス**」→「**デバイスデバッグ**」に移動し、「**キャプチャデバイスパケット**の設定」をクリックします。
2. 「**有効化**」にチェックを入れてこの機能を有効にします。

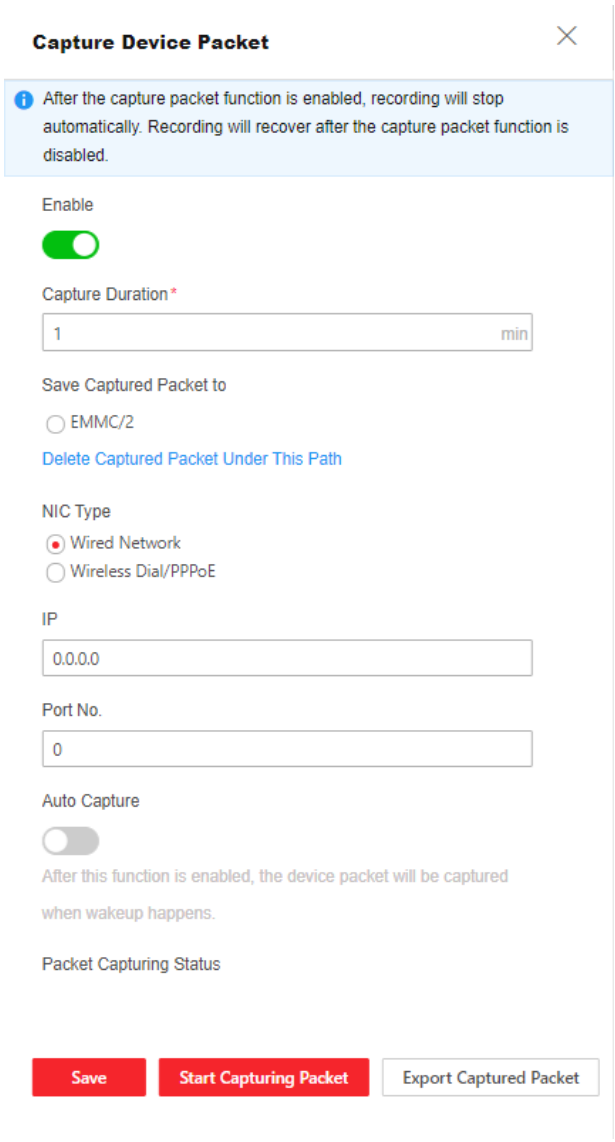

図9-1 キャプチャデバイスパケット

3. **キャプチャ時間を**必要に応じて設定します。
4. パケット保存先パスを選択します。

注記

1. 保存パスオプションは、デバイスの実際の保存方法に依存します。
2. 保存されたパケットファイルを削除するには、「**このパス下のキャプチャ済みパケットを**削除」をクリックします。

5. NICタイプ、IP、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. 「**パケットキャプチャ開始**」をクリックします。
9. キャプチャ完了後、「**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]→[メンテナンス]→[デバイスデバッグ]→[デバイス情報のエクスポート] に移動し、**[エクスポート]** をクリックすると、電圧、電流、電力、4Gデータなどのデバイス情報をエクスポートできます。

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強化できます。

9.4.1 IPアドレスフィルターの設定

IPアドレスフィルターはアクセス制御ツールです。特定のIPアドレスからのアクセスを許可または禁止するために有効化できます。

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**」に移動します。
2. 「**有効化**」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	リスト内の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	リスト内の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。
	リスト内の選択済みIPアドレスまたはIPアドレス範囲を変更します。
	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の設定

MACアドレスフィルタ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禁止するために有効にできます。

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**に移動します。
2. 「**有効にする**」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	リスト内の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	リスト内の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アドレスを変更します。
	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 制御タイムアウト設定

この機能を有効にすると、設定したタイムアウト期間内にWebブラウザ経由でデバイスに対して操作を行わない場合（ライブ画像の閲覧を除く）、自動的にログアウトされます。設定は、**[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] → [制御タイムアウト設定]** で完了します。

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 証明書の管理、証明書の有効期限が近づいた場合や、期限切れ/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。

注記

本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

注記

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。

自己署名証明書の作成とインストール

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** に移動します。
2. 「**自己署名証明書の作成**」をクリックします。
3. 証明書情報を入力します。

注記

入力する証明書IDは既存のものと重複できません。

4. **[保存]**をクリックして証明書を保存・インストールします。
   作成された証明書は、**サーバー/クライアント**証明書リストに表示されます。
   特定の機能で使用されている場合、機能名が「**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。

自己署名リクエスト証明書のインストール

自己署名証明書を信頼できる第三者に送信して署名を受け、その証明書をデバイスにインストールすることができます。

始める前に

まず自己署名証明書を作成してください。手順については*「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]** に移動します。
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. 「**証明書要求の作成**」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. リクエスト内容をコピーし、リクエストファイルとして保存します。
7. 信頼できる第三者に署名のためにファイルを送信します。
8. 第三者から返送された証明書を受け取ったら、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、既存のものと同じであってはなりません。

3) 「🗀」をクリックし、証明書ファイルを選択します。
4) **「自己署名リクエスト証明書」**を選択します。
5) **[保存]**をクリックします。
インポートされた証明書は、**サーバー/クライアント**証明書リストに表示されます。
特定の機能で使用されている証明書の場合、機能名が「**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確認します。

他の認証済み証明書のインストール

認証済み証明書（デバイスで作成されていないもの）を既に所持している場合、 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」**に移動します。
2. **サーバー/クライアント**証明書リストの［インポート］をクリックします。
3. **証明書ID**を入力します。

注記

入力する証明書IDは、既存のものと同じであってはなりません。

4. 「🗀」をクリックし、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**を選択します。

独立した鍵	証明書に独立した鍵が含まれている場合は、このオプションを選択してください。 秘密鍵を参照して選択し、秘密鍵のパスワードを入力します。
PKCS#12	証明書と鍵が同一の証明書ファイルにある場合は、このオプションを選択し、パスワードを入力してください。

6. **[保存]**をクリックします。
インポートされた証明書は、**サーバー/クライアント**証明書リストに表示されます。
特定の機能で使用される証明書の場合、機能名が「**機能**」列に表示されます。

CA証明書のインストール

開始前に

事前にCA証明書を準備してください。

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]** に移動します。
2. **CA**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**を入力します。

注記

入力する証明書IDは既存のものと重複できません。

4. 「 」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。
   特定の機能で使用されている場合、機能名が「**機能**」列に表示されます。

証明書の有効期限アラームを有効にする

手順

1. 「**証明書有効期限アラームを有効にする**」にチェックを入れます。有効にすると、証明書の有効期限が近づいている、または期限切れ・異常状態になった際に、メール通知または監視センターへのカメラリンク通知を受け取ります。
2. 「**有効期限前の通知間隔（日数）**」、「**アラーム頻度（日数）**」、「**検知時間（時間）**」を設定します。

注記

- 有効期限前のリマインド日を1日に設定すると、カメラは有効期限の前日に通知します。設定可能範囲は1～30日です。デフォルトのリマインド日は7日です。
- 有効期限前のリマインド日を1日に設定し、検知時間を10:00に設定した場合、証明書が翌日の9:00に失効するならば、カメラは初日の10:00に通知します。

3. [**保存**]をクリックします。

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、主に通信する2つ以上のコンピュータアプリケーション間でプライバシーとデータ完全性を提供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 に移動し、必要な 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

本機能は慎重にご利用ください。機能を有効にした場合、デバイス内部情報の漏洩リスクが存在します。

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）により、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、その機能やサービスを実行することができます。HEOPをサポートするデバイスでは、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。

注記

アプリケーションをインストールする前に、インストールする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固有の名前が付与されています。
- アプリケーションが占有するフラッシュメモリ領域が、デバイスの利用可能なフラッシュメモリ領域より小さいこと。
- アプリケーションのメモリおよび演算能力は、デバイスの利用可能なメモリおよび演算能力よりも小さい。

2. **「アプリケーションのインポート」**をクリックし、ローカルパスを参照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、ローカルパスを参照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	ローカルパスを参照し、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	メモリの断片化を解消し、より多くのメモリを解放して、より多くのスマートア

	プリケーションを有効にします。
詳細を表示	アプリケーションを選択し、クリックするとページに詳細が表示されます。

10.2 基本設定

スマートアプリケーションに関連する一般パラメータを設定します。

VCA → アプリケーション設定 → 一般設定 に移動し、以下のパラメータを設定します。

カメラ情報

カメラ情報設定については、*「カメラ情報の設定」*を参照してください。

FTP

FTP 設定については、*「FTP の設定」*を参照してください。

Eメール

Eメールの設定については、「*Eメールの設定」*を参照してください。

警報出力

警報出力の設定については、「*自動警報」*を参照してください。

可聴警報出力

可聴警報出力の設定については、*「可聴警報出力の設定」*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

メタデータ設定については、「*メタデータ」*を参照してください。

10.2.1 カメラ情報の設定

デバイスの特定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 → アプリケーション設定 → 一般設定 → カメラ情報 に移動し、**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

メタデータとは、デバイスがアルゴリズム処理前に収集する生データです。 やサードパーティ統合などでよく使用されます。

VCA → アプリケーション設定 → 一般設定 → メタデータ設定 に移動し、必要な機能のメタデータアップロードを有効にします。

注

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画像全体を検出します。顔キャプチャ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

デバイスはターゲットを検知後、そのPOS情報をネットワークビデオレコーダーに送信します。これにより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

- 本機能を利用するには、接続先の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。
- 機能を有効化すると、進行中のスマートアプリケーションは無効化されますが、**スマートイベント**または**マルチターゲット型検出**は有効なままとなります。
- 本機能は特定モデル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。

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）に対して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画面で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上で対象をクリックし、その対象を含む画像を検索します。
4) 画像をクリックすると、その瞬間の前後映像を再生します。

注記

NVRの実際の設定については、NVRのユーザーマニュアルを参照してください。

10.3 スマートイベント

注記

- 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されます。検知が発生した場合、デバイスは連動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でスマートイベントを**インポートし有効化してください。

手順

1. **VCA → アプリケーション設定 → Smart Event → 侵入検知** に移動します。
2. **[有効化]** 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、検知エリアを設定します。
   1) 検知エリアを描画します。 をクリックし、ライブビュー上で頂点を指定して検知エリアの境界線を描画し、右クリックで描画を完了します。
   2) 検出精度向上のため、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ターゲットのみが検出対象となります。 と をクリックし、ライブビュー上でマウスをドラッグして最小・最大ターゲットサイズを描画します。
   3) オプション： をクリックすると、設定領域をすべて削除します。

4. パラメータを設定します。

検出対象

この機能により、指定したターゲットタイプでアラームをトリガーできます。検出対象を選択しない場合、検出された全ターゲットが報告されます。

注記

本機能は特定のデバイスモデルかつ特定の設定下でのみ利用可能です。実際の設定をご確認ください。

閾値

しきい値とは、対象物が領域内に滞留する時間の閾値を指します。1つの対象物が滞留する時間がしきい値を超えると、警報が作動します。しきい値の値が大きいほど、警報作動までの時間は長くなります。

感度

感度とは、許容対象物の身体部位が事前定義領域に侵入する割合を指します。感度 = 100 - S1/ST × 100。S1は事前定義領域を横切る対象物身体部位、STは対象物身体全体を表します。感度の値が高いほど、警報がより容易に作動します。

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である必要があり、警報の精度が向上します。特徴が不明確なターゲットは見逃される可能性があります。

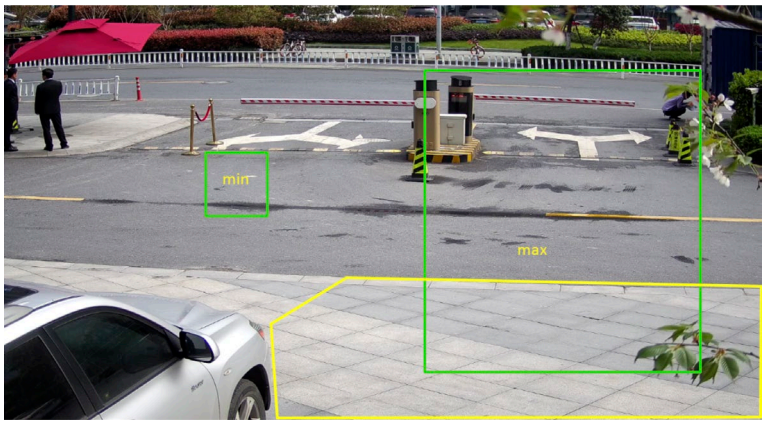

図10-1 ルール設定

5. オプション：上記の手順を繰り返すことで、複数のエリアのパラメータを設定できます。
6. 警戒スケジュール設定については*「警戒スケジュール設定」*を参照してください。連動方法設定については*「連動方法設定」*を参照してください。
7. 「**保存**」をクリックします。

10.3.2 ライン越え検知の設定

あらかじめ設定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、デバイスは連動アクションを実行できます。

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でスマートイベントを**インポートし有効化します。

手順

1. **VCA → アプリケーション設定 → Smart Event → ラインクロッシング検出** に移動します。
2. **[有効化]** 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、検知エリアを設定します。
   1) 検知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。ラインをドラッグしてライブビュー上の任意の位置に移動させます。
   2) 検出精度向上のため、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ターゲットのみが検出対象となります。 と をクリックし、ライブビュー上でマウスをドラッグして最小・最大ターゲットサイズを描画します。
   3) オプション: をクリックすると、すべての設定領域を削除できます。
4. パラメータを設定します。

検出対象

この機能により、指定したターゲットタイプでアラームをトリガーできます。検出対象を選択しない場合、検出された全ターゲットが報告されます。

注記

本機能は特定のデバイスモデルかつ特定の設定下でのみ利用可能です。実際の設定をご確認ください。

方向

対象物がラインを横切る方向を示します。

A<->B: 両方向からラインを横切る物体を検知し、アラームが作動します。

A->B: 設定されたラインをA側からB側へ横切る物体のみ検出可能。

B->A: 設定されたラインをB側からA側へ横切る物体のみを検出できます。

感度

これは、許容対象物の身体部位のうち、事前定義されたラインを越える部分の割合を表します。感度 = 100 - S1/ST × 100。S1は事前定義されたラインを越える対象物の身

体部位を表します。STは対象物の身体全体を表します。感度の値が高いほど、警報がより容易に作動します。

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、警報の精度が向上します。特徴が不明瞭なターゲットは見落とされる可能性があります。

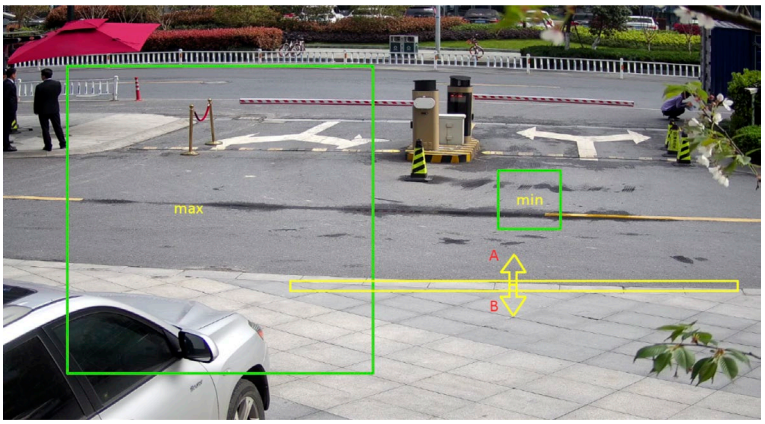

図10-2 ルール設定

5. オプション：上記の手順を繰り返すことで、複数のエリアのパラメータを設定できます。
6. 警戒スケジュール設定については*「警戒スケジュール設定」*を参照してください。連動方法設定については*「連動方法設定」*を参照してください。
7. 「**保存**」をクリックします。

10.3.3 区域進入検知の設定

外部から事前に定義された仮想領域に侵入する物体を検出するために使用されます。侵入が発生した場合、デバイスは連動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でスマートイベントを**インポートし有効化します。

手順

1. **VCA → アプリケーション設定 → Smart Event → 区域進入検知** に移動します。
2. **[有効化]** 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、検知エリアを設定します。
   1) 検知エリアを描画します。 をクリックし、ライブビュー上で頂点を指定して検知エリアの境界を描画し、右クリックで描画を完了します。

2) 検出精度向上のため、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ターゲットのみが検出対象となります。 と をクリックし、ライブビュー上でマウスをドラッグして最小・最大ターゲットサイズを描画します。
3) オプション： をクリックすると、設定領域をすべて削除します。

4. パラメータを設定します。

検出対象

この機能により、指定したターゲットタイプでアラームをトリガーできます。検出対象を選択しない場合、検出された全ターゲットが報告されます。

注記

本機能は特定のデバイスモデルかつ特定の設定下でのみ利用可能です。実際の設定をご確認ください。

感度

許容対象の身体部位が事前定義領域を横切る割合を表します。感度 = 100 - S1/ST × 100。S1は事前定義領域を横切る対象身体部位、STは対象身体全体を示します。感度値が高いほど、アラームが容易に作動します。

ターゲット有効性

有効性を高く設定すると、必要な標的特徴がより明確である必要があり、警報精度が向上します。特徴が不明確な標的は見逃される可能性があります。

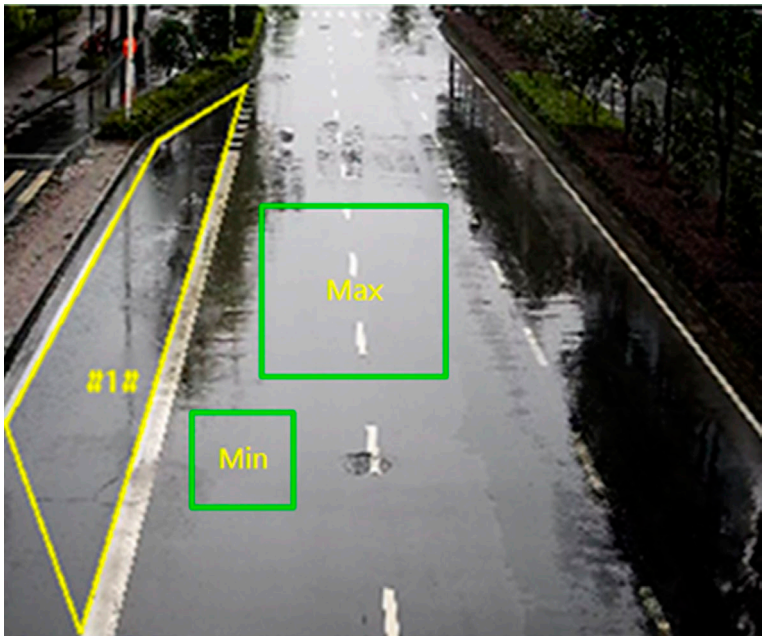

図10-3 ルール設定

5. オプション：上記の手順を繰り返すことで、複数のエリアのパラメータを設定できます。

6. 警戒スケジュール設定については*「警戒スケジュール設定」*を参照してください。連動方法設定については*「連動方法設定」*を参照してください。
7. 「**保存**」をクリックします。

10.3.4 領域退出検知の設定

あらかじめ定義された仮想領域から対象物が退出することを検出します。検出された場合、デバイスは連動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でスマートイベントを**インポートし有効化します。

手順

1. **VCA → アプリケーション設定 → Smart Event → 区域退出検知** に移動します。
2. **[有効化]** 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、検知エリアを設定します。
   1) 検知エリアを描画します。 をクリックし、ライブビュー上で頂点を指定して検知エリアの境界を描画し、右クリックで描画を完了します。
   2) 検出精度向上のため、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ターゲットのみが検出対象となります。 と をクリックし、ライブビュー上でマウスをドラッグして最小・最大ターゲットサイズを描画します。
   3) オプション**:** をクリックすると、設定領域をすべて削除します。
4. パラメータを設定します。

検出対象

この機能により、指定したターゲットタイプでアラームをトリガーできます。検出対象を選択しない場合、検出された全ターゲットが報告されます。

注記

本機能は特定のデバイスモデルかつ特定の設定下でのみ利用可能です。実際の設定をご確認ください。

感度

許容対象の身体部位が事前定義領域を横切る割合を表します。感度 = 100 - S1/ST × 100。S1は事前定義領域を横切る対象身体部位、STは対象身体全体を示します。感度値が高いほど、警報がより容易に作動します。

ターゲット有効性

有効性を高く設定すると、必要な標的の特徴がより明確である必要があり、警報の精

度が向上します。特徴が不明確な標的は見逃される可能性があります。

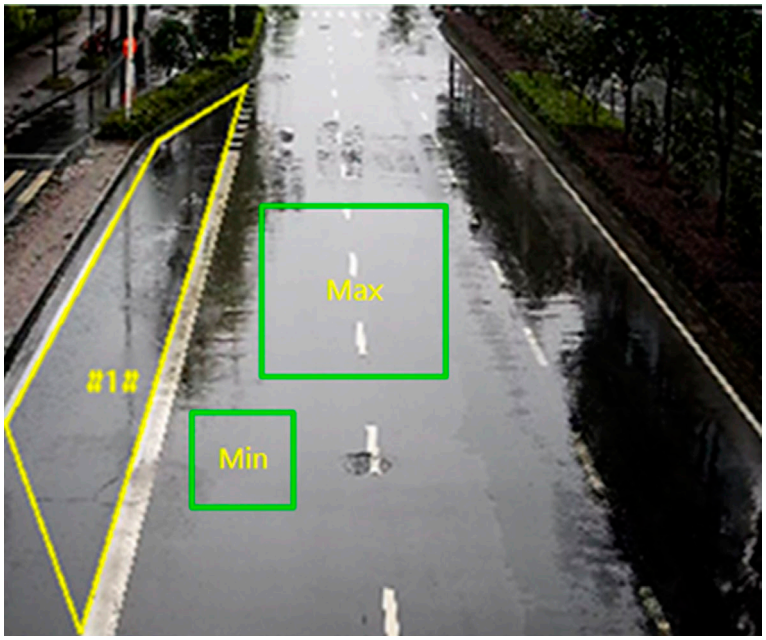

図10-4 ルール設定

5. オプション：上記手順を繰り返すことで、複数領域のパラメータを設定できます。
6. 警戒スケジュール設定については、*「警戒スケジュールの設定」*を参照してください。連動方法設定については、*「連動方法の設定」*を参照してください。
7. 「**保存**」をクリックします。

10.3.5 無人手荷物検知の設定

これは、事前定義された領域内に放置された物体を検出するために使用されます。物体が領域内に放置され、設定された時間経過後に連動方法がトリガーされます。

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でスマートイベントを**インポートし有効化します。

手順

1. **VCA → アプリケーション設定 → Smart Event → 無人手荷物検知** へ移動。
2. **[有効化]** 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、検知エリアを設定します。
   1) 検知エリアを描画します。 をクリックし、ライブビュー上で頂点を指定して検知エリアの境界線を描画し、右クリックで描画を完了します。

2) 検出精度向上のため、対象物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対象物のみが検出対象となります。 と をクリックし、ライブビュー上でマウスをドラッグして最小・最大対象サイズを描画します。
3) オプション： をクリックすると、設定領域をすべて削除できます。

4. パラメータを設定します。

感度

感度とは、許容対象物の身体部位が事前定義領域に入る割合を表します。感度 = 100 - S1/ST × 100。S1は事前定義領域を横切る対象物身体部位、STは対象物身体全体を表します。感度値が高いほど、警報が容易に作動します。

閾値

対象物が領域内に残留する時間を表します。対象物が領域内に残留し、設定時間経過後に警報が作動します。

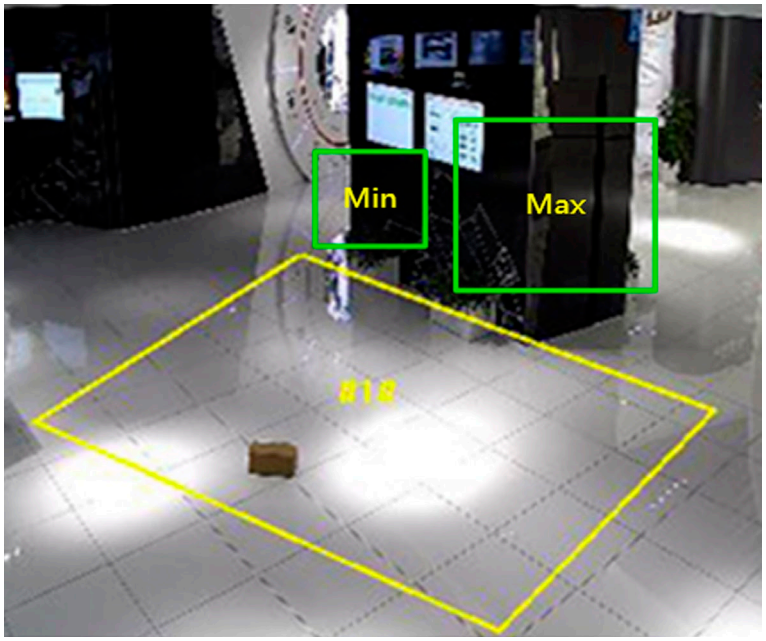

図10-5 ルール設定

5. オプション：上記の手順を繰り返すことで、複数の領域のパラメータを設定できます。
6. 警戒スケジュール設定については「*警戒スケジュール設定*」を参照してください。連動方法設定については「*連動方法設定*」を参照してください。
7. 「保存」をクリックします。

注

本機能は一部モデル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。

10.3.6 展示物撤去検知の設定

展示物など、あらかじめ設定された検知エリアからオブジェクトが除去されたかどうかを検知します。除去が発生した場合、デバイスは連動動作を実行し、スタッフは財産損失を軽減する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。**「Smart Event」**を選択し、**「次へ」**をクリックして機能を有効化します。
- HEOP対応デバイスでは、**VCAでSmart Eventを**インポートし有効化してください。

手順

1. **VCA → アプリケーション設定 → Smart Event → オブジェクト除去検知** に移動します。
2. **[有効化]** 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、検知領域を設定します。
   1) 検知領域を描画します。 をクリックし、ライブビュー上で頂点を指定して検知領域の境界を描画し、右クリックで描画を完了します。
   2) 検出精度向上のため、対象物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対象物のみが検出対象となります。 と をクリックし、ライブビュー上でマウスをドラッグして最小・最大対象サイズを描画します。
   3) オプション：をクリックすると、設定領域をすべて削除します。
4. パラメータ設定

感度

感度とは、許容対象物の身体部位が事前定義領域に入る割合（%）を指します。感度 = 100 - S1/ST × 100。S1は事前定義領域を横切る対象物身体部位、STは対象物身体全体を表します。感度値が高いほど、警報が容易に作動します。

閾値

領域から対象物が除去された時間のしきい値。値を10に設定すると、対象物が領域から消えて10秒後に警報が作動します。

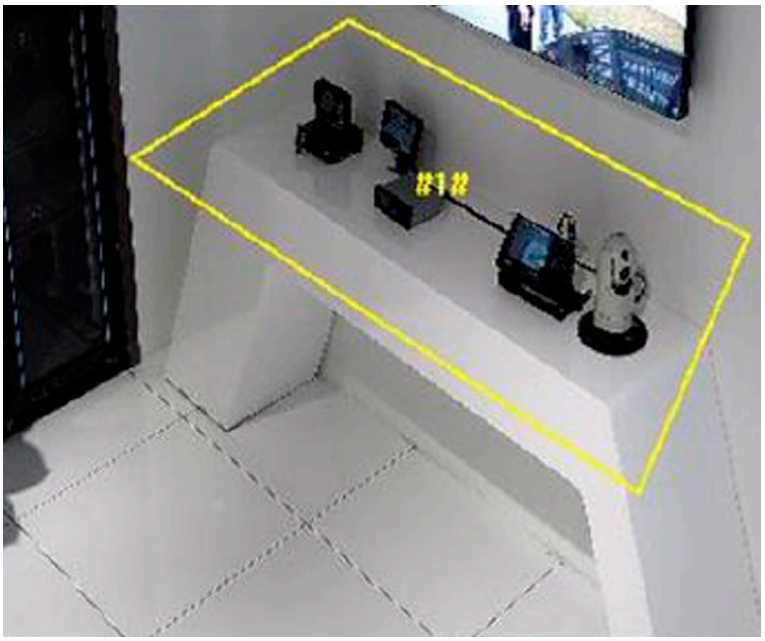

図10-6 ルール設定

5. オプション：上記の手順を繰り返すことで、複数の領域のパラメータを設定できます。
6. 警戒スケジュール設定については*「警戒スケジュール設定」*を、連動方法設定については*「連動方法設定」*を参照してください。
7. 「**保存**」をクリックします。

注

本機能は一部モデル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。

10.3.7 徘徊検知の設定

あらかじめ定義されたエリア内でターゲットが滞留しているかどうかを検出します。ターゲットが設定された領域で滞留する時間が設定された閾値に達した場合、デバイスは連動アクションを実行できます。

開始前に

- **VCAに移動**し、アプリケーションを選択します。**Smart Eventを選択**し、**[次へ]**をクリックして機能を有効にします。
- HEOP対応デバイスについては、**VCAでスマートイベントを**インポートし有効化してください。

手順

1. **VCA → アプリケーション設定 → スマートイベント → 徘徊検知** に移動します。
2. **[有効化]** 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、検知エリアを設定します。
   1) 検知エリアを描画します。 をクリックし、ライブビュー上で頂点を指定して検知エリアの境界を描画し、右クリックで描画を完了します。
   2) 検出精度向上のため、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ターゲットのみが検出対象となります。 と をクリックし、ライブビュー上でマウスをドラッグして最小・最大ターゲットサイズを描画します。
   3) オプション： をクリックすると、設定領域をすべて削除できます。
4. ルールを設定します。

閾値

閾値は、対象物が領域内に滞留する時間の閾値を表します。1つの対象物が滞留する時間が閾値を超えると、警報が作動します。閾値の値が大きいほど、警報作動までの時間は長くなります。

感度

感度は、許容対象物の身体部位が事前定義領域に入る割合を表します。感度 = 100 - S1/ST × 100。S1は事前定義領域を横切る対象物の身体部位、STは対象物全体の身体を表します。感度の値が高いほど、警報がより容易に作動します。

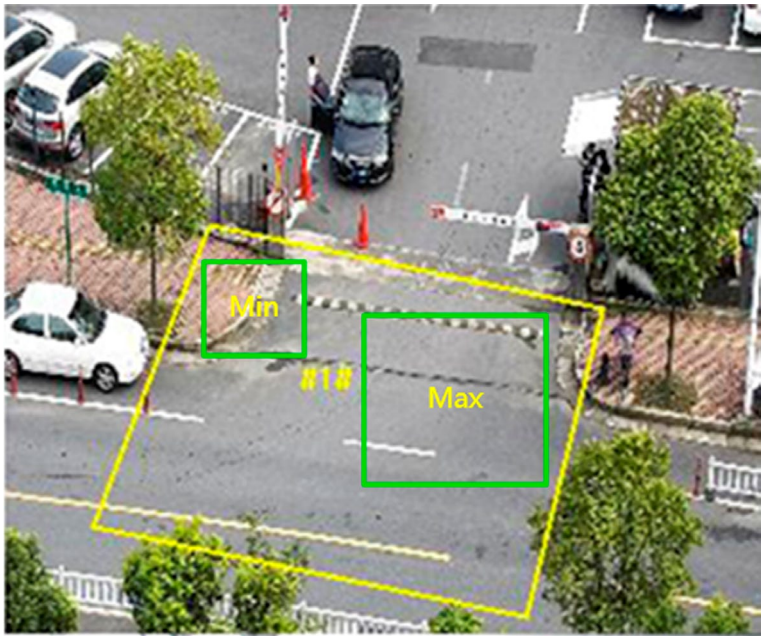

図10-7 ルール設定

5. オプション：上記の手順を繰り返すことで、複数のエリアのパラメータを設定できます。
6. 警戒スケジュール設定については*「警戒スケジュール設定」*を参照してください。連動方法設定については*「連動方法設定」*を参照してください。
7. 「**保存**」をクリックします。

注

本機能は一部モデル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。

10.3.8 人集まり検知の設定

事前に定義されたエリア内の人密度を検出します。人密度が設定されたパーセンテージを超えた場合、デバイスは連動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をサポートするデバイスについては、**VCAに移動してSmart Eventを**インポートし有効化してください。

手順

1. **VCA → アプリケーション設定 → スマートイベント → 人物集結検知** に移動します。
2. **[有効化]** 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、検知エリアを設定します。
   1) 検知エリアを描画します。 をクリックし、ライブビュー上で頂点を指定して検知エリアの境界を描画し、右クリックで描画を完了します。
   2) オプション**:** をクリックすると、設定済みの領域をすべて削除できます。
4. ルールを設定します。

   パーセンテージ

   事前定義された領域内の人物の割合を表します。ライブビュー内の人物割合が設定値を超えた場合、デバイスが警報を発します。

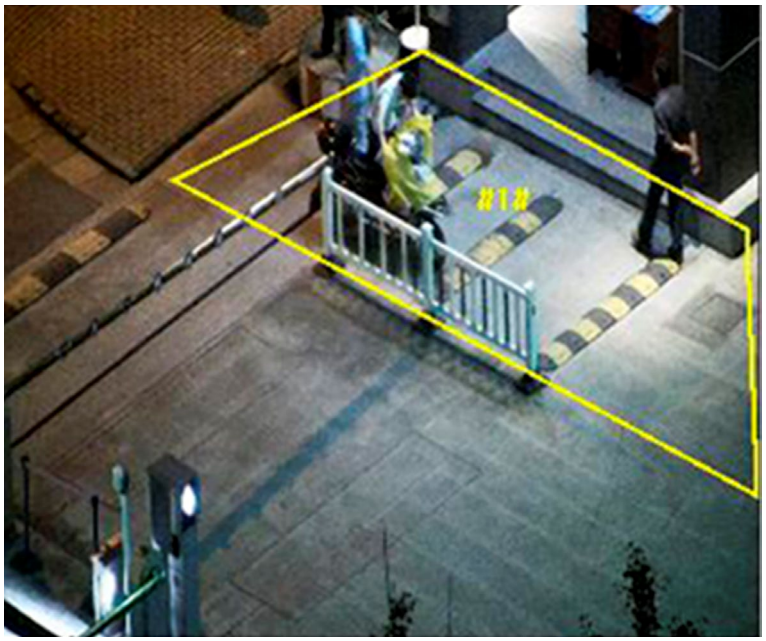

図10-8 ルール設定

5. オプション：上記の手順を繰り返すことで、複数のエリアのパラメータを設定できます。
6. 警戒スケジュール設定については*「警戒スケジュール設定」*を参照してください。連動方法設定については*「連動方法設定」*を参照してください。
7. 「**保存**」をクリックします。

注

本機能は一部モデル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。

10.3.9 高速移動検知の設定

あらかじめ設定されたエリア内で高速移動するターゲットが検出されると、デバイスは連動動作を実行し、警報を発します。

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**インポートし有効化してください。

手順

1. **VCA → アプリケーション設定 → Smart Event → 高速移動物体検知** に移動します。
2. **[有効化]** 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、検知エリアを設定します。

1) 検出領域を描画します。 をクリックし、ライブビュー上で頂点を指定して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) 検出精度向上のため、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ターゲットのみが検出対象となります。 と をクリックし、ライブビュー上でマウスをドラッグして最小・最大ターゲットサイズを描画します。
3) オプション：をクリックすると、設定領域をすべて削除できます。

4. ルール設定

感度

感度とは、許容対象物の身体部位が事前定義領域に侵入する割合（%）を指します。感度 = 100 - S1/ST × 100。S1は事前定義領域を横切る対象物身体部位、STは対象物身体全体を表します。感度値が高いほど、警報が容易に作動します。

図10-9 ルール設定

5. オプション：上記の手順を繰り返すことで、複数のエリアのパラメータを設定できます。
6. 警戒スケジュール設定については*「警戒スケジュール設定」*を参照してください。連動方法設定については*「連動方法設定」*を参照してください。
7. 「**保存**」をクリックします。

注

本機能は一部モデル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 駐車検知の設定

事前定義されたエリア内の駐車違反を検知します。駐車時間が設定しきい値を超えた場合、 デバイスは連動動作を実行できます。高速道路や一方通行道路で適用可能です。

開始前に

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

手順

1. **VCA → アプリケーション設定 → Smart Event → 駐車検知** に移動します。
2. **[有効化]** 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、検知エリアを設定します。
   1) 検知エリアを描画します。 をクリックし、ライブビュー上で頂点を指定して検知エリアの境界線を描画し、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ターゲットのみが検出対象となります。 と をクリックし、ライブビュー上でマウスをドラッグして最小・最大ターゲットサイズを描画してください。
   3) オプション**:** をクリックすると、設定領域をすべて削除できます。
4. ルールを設定します。

閾値

しきい値は、領域内の駐車時間の閾値を表します。駐車時間がしきい値を超えると警報が作動します。しきい値の値が大きいほど、警報作動までの時間が長くなります。

感度

感度は、許容対象物の一部が事前定義された領域に入る割合を表します。感度 = 100 - S1/ST × 100。S1は事前定義領域を通過する対象物の一部、STは対象物全体を表します。感度の値が高いほど、警報がより容易に作動します。

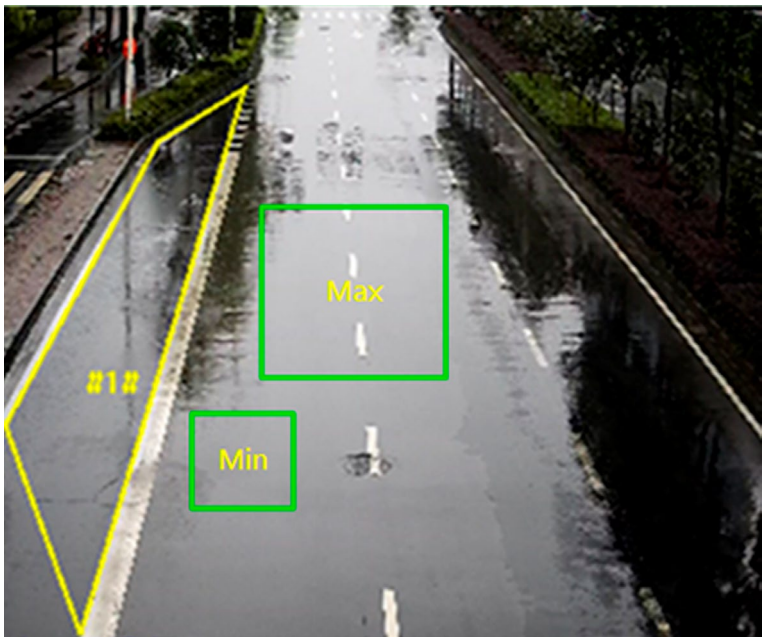

図10-10 ルール設定

5. オプション：上記の手順を繰り返すことで、複数のエリアのパラメータを設定できます。
6. 警戒スケジュール設定については*「警戒スケジュール設定」*を参照してください。連動方法設定については*「連動方法設定」*を参照してください。
7. 「保存」をクリックします。

注

本機能は一部モデル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。

10.4 顔キャプチャ

設定されたルールエリア内でルールに合致する顔をデバイスがキャプチャし、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

設定された領域に現れる顔をキャプチャできます。

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で顔検出を**インポートし有効化します。

手順

1. **VCA → アプリケーション設定 → 顔認識 → ルール** に移動します。
2. **[Enable]**にチェックを入れ、ルール設定を有効化します。
3. 「▭」をクリックし、顔検出を有効にしたい領域を描画します。ライブビューウィンドウで左クリックで端点を指定し、右クリックで領域描画を終了します。描画領域はライブビュー画像の1/2～2/3を占めることを推奨します。
4. 瞳孔間距離を測定する。

   最小瞳孔間距離

   をクリックして最小瞳孔間距離を描画します。動画画像内の顔の瞳孔間距離が最小瞳孔間距離より小さい場合、顔は検出されません。

   最大瞳孔間距離

   をクリックして最大瞳孔間距離を描画します。動画画像内の顔の瞳孔間距離が最大瞳孔間距離より大きい場合、顔は検出されません。

   距離の値をテキストフィールドに入力することもできます。
5. オプション：シールド領域設定については、「*シールド領域の設定」*を参照してください。
6. 警戒スケジュール設定については*「警戒スケジュール設定*」を参照してください。連動方法設定については*「連動方法設定」*を参照してください。
7. 「**保存**」をクリックします。
8. オーバーレイとキャプチャ設定については、*「オーバーレイとキャプチャ*」を参照してください。詳細パラメータ設定については、*「顔キャプチャアルゴリズムパラメータ」*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**閲覧・ダウンロードできます。詳細は*画像の閲覧とダウンロード*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と、ストリームおよび画像に表示する情報の設定を選択します。

ストリームにVCA情報を表示

ターゲットやルール情報を含むスマート情報をストリームに表示します。

アラーム画像にターゲット情報を表示

ターゲット情報をアラーム画像に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。監視センターに背景画像をアップロードする必要がある場合は、**「背景アップロード」**にチェックを入れます。一部のデバイスでは、キャプチャした顔画像をアップロードするために**「顔画像」**にもチェックを入れることができます。

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。

注記

カスタムを選択した場合、必要に応じて**幅**、**頭の高さ**、**体の高さをカスタマイズ**できます。

固定画像高さをチェックすると、画像の高さを設定できます。

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てください。

注

顔美化機能は、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。

顔の強調

顔強調を確認すると、暗い場所でもより鮮明でクリアな顔写真を撮影できます。

テキストオーバーレイ

必要な項目を選択し、撮影画像への表示順序を調整できます。
デバイス番号と**カメラ情報を**設定するには、**カメラ情報の*設定***を参照してください。

10.4.3 顔検出アルゴリズムのパラメータ

顔検出機能のアルゴリズムライブラリのパラメータを設定・最適化するために使用されま

す。

バージョン

現在のアルゴリズムバージョンを示します。

キャプチャパラメータ

ベストショット

ターゲットが検出領域を離れた後のベストショット。

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示します。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に満たすべき品質が高くなります。

キャプチャ回数

設定されたエリア内に顔がいる間、その顔がキャプチャされる回数。デフォルト値は1。

クイックショット

顔画像の評価値がクイックショット閾値を超えた場合、その顔画像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（ ）に達した中で評価値が最も高い画像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基準値です。

最大撮影間隔

1回のクイックショットが占める最大時間を指します。

キャプチャ回数

設定された領域内に顔がいる間に撮影される回数を指します。

重複顔の除去

この機能は、特定の顔の重複したキャプチャをフィルタリングするのに役立ちます。

重複除去の類似度閾値

新規にキャプチャされた顔と重複除去ライブラリ内の画像との類似度です。類似度値が設定値を超える場合、キャプチャされた画像は重複顔とみなされ除外されます。

重複除去ライブラリ評価閾値

重複チェックをトリガーする顔評価閾値です。顔評価が設定値を超える場合、キャプチャされた顔を重複除去ライブラリ内の既存顔画像と比較します。

重複除去ライブラリ更新時間

各顔画像が重複除去ライブラリに追加されてから削除されるまでの期間。

顔露出

チェックボックスをオンにすると顔露出が有効になります。

基準輝度

顔露出モードにおける顔の基準輝度。顔が検出されると、カメラは設定値に基づい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。

最小露出時間

カメラが顔を露出する最小時間。

注意

顔露出を有効にする場合、WDR機能が無効化され、手動アイリスが選択されていることを確認してください。

顔フィルタリング時間

カメラが顔を検出してから撮影するまでの時間間隔を指します。検出された顔が設定されたフィルタリング時間より短い時間だけシーン内に留まった場合、撮影はトリガーされません。例えば、顔フィルタリング時間を5秒に設定した場合、顔が5秒間シーン内に留まり続けたときにカメラは検出された顔を撮影します。

注記

顔フィルタリング時間（0秒より長い）を設定すると、実際の撮影時間が上記設定値を下回る可能性が高まる場合があります。

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できます。スライダー右側の図は、顔キャプチャ動作で許容される姿勢角度を示します。このフィルター設定時の顔向き方向を説明する図を表示するには、 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可能な特徴情報を指します。この情報をアップロードするには、該当機能にチェックを入れてください。

パラメータを復元

デフォルトに戻す

[復元]をクリックすると、詳細設定のすべての設定が工場出荷時のデフォルト値に復元されます。

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が無効となる特定の領域を設定できま

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。複数のシールド領域を設定する場合は、上記の手順を繰り返します。
3. オプション：描画した領域を選択してクリックし、[ ]をクリックすると、選択した描画領域を削除できます。
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 人物管理

人物管理は、事前定義された領域内の人数と変化を検知・分析するために使用されます。出入口や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、VCAページで事前に「**人員管理**」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 エリア別人数計測

あらかじめ定義されたエリア内の人数をカウントし、人数変化や混雑状況を検知します。人数異常や待機時間異常が発生した場合、デバイスはアラームをトリガーできます。

人密度検出の設定については、*「人密度設定」*を参照してください。

人の*異常検知*の設定については、「人の異常検知の設定」を参照してください。

待機時間異常検知の設定については「待機時間異常検知」を参照してください。

人密度設定

この機能は、設定されたルール区域内の人口密度のレベルを検出します。

開始前に

- **VCA → アプリケーション選択**に移動し、「**People Management**」を選択して「**次へ**」をクリックし、機能を有効化します。
- HEOP対応デバイスでは、**VCAでPeople Managementを**インポートし有効化してください。

手順

1. **VCA → アプリケーション設定 → 人物管理 → 地域別人物カウント → ルール** に移動します。
2. **「追加」**をクリックしてルールを追加し、名前を設定します。
3. ルールを設定します。

図10-11 ルール設定

人数表示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。OSDウィンドウの位置は、マウスをドラッグして調整できます。

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、最初のアラーム遅延**の設定をサポートしていません。

4. ライブビューウィンドウで をクリックし領域を描画、ライブビューウィンドウで端点を左クリックして設定ルールの境界を定義、右クリックで描画を終了します。

注

- 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. **人口密度アラーム**をチェックして機能を有効にします。

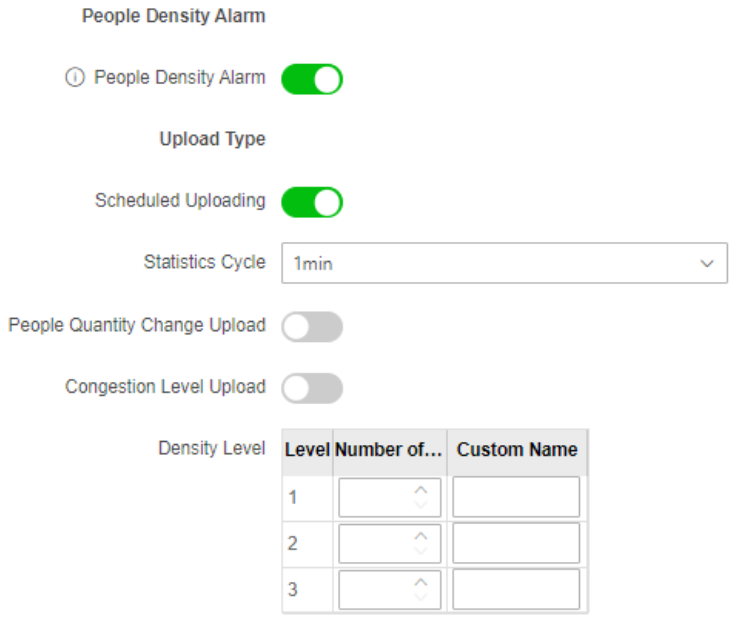

図10-12 人口密度アラーム

スケジュールアップロード

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。

人数変化アップロード

設定ルール区域で変化があった場合、デバイスは人の量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

設定されたルール区域で混雑レベルに変化があった場合、デバイスは混雑情報をアップロードします。

密度レベル

人数

設定ルール区域における人数の下限値を入力することで、各レベルごとの範囲を設定します。

カスタム名

レベル名。

注記

- **カスタム名**の前に**人数**を設定してください。
- 最大3レベルまで設定可能。レベル1からレベル3にかけて密度が増加します。

6. 警戒スケジュールを設定します。*「警戒スケジュールの設定」*を参照してください。
7. 連動方式を設定します。*「連動方式の設定」*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。詳細な設定については、*「詳細設定」*を参照してください。

人物例外検知の設定

この機能は、設定されたルール領域内の人数を検知し、状況が警報発動条件を満たした場合に警報を発します。

開始前に

- **VCA → アプリケーション選択**に移動し、「**人物管理**」を選択して「**次へ**」をクリックし、機能を有効化します。
- HEOPをサポートするデバイスについては、**VCA**に移動し、**People Management**をインポートして有効化してください。

手順

1. **VCA → アプリケーション設定 → 人管理 → 地域別人数計測 → ルール** に移動します。
2. 「**追加**」をクリックしてルールを追加し、名前を設定します。
3. ルールを設定します。

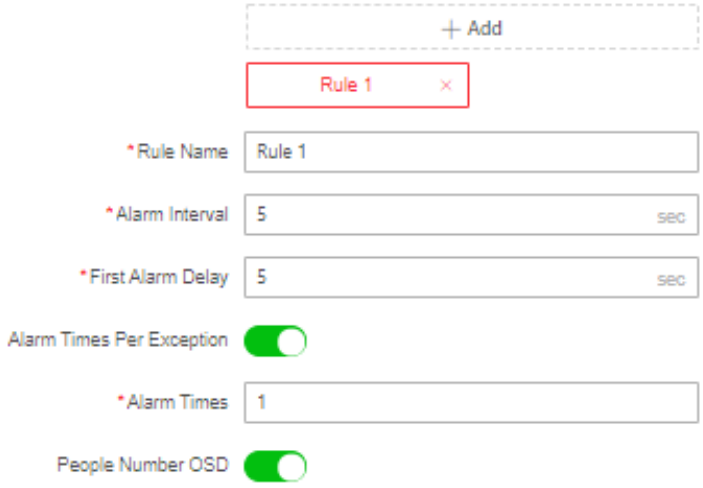

図10-13 ルール設定

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。OSDウィンドウの位置はマウスでドラッグして調整できます。

例外ごとのアラーム時間

アラーム発生後のアラーム継続時間を指します。チェックせず時間を設定しない場合、デバイスはアラームを継続送信します。

アラーム間隔

設定された**アラーム間隔**内で、同一アラームはアップロードされません。

初回アラーム遅延

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

4. 「 」をクリックし、ライブビューウィンドウ内で領域を描画します。ライブビューウィンドウ内で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終了します。

注記

- 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. 「**区域内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「**アラーム閾値**」を設定します。

注記

- 「**無人状態を無視**」を有効にすると、エリア内に人がいない場合、デバイスは警報を発しません。
- この機能により、設定した**警報閾値**未満の値でかつ領域内に人がいない場合の潜在的な警報条件をフィルタリングできます。

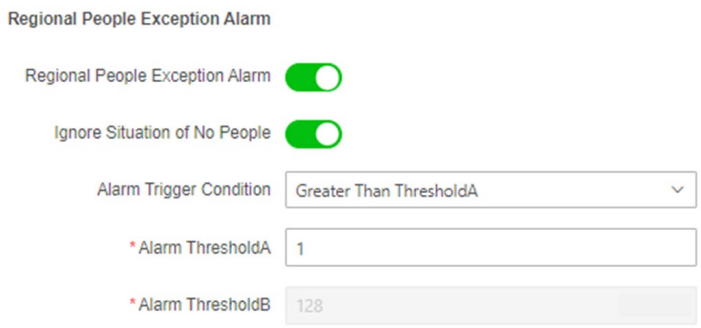

図10-14 区域人例外警報

6. 警戒スケジュールを設定します。*「警戒スケジュールの設定」*を参照してください。
7. 連動方式を設定します。*「連動方式の設定」*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。詳細な設定については、*「詳細設定」*を参照してください。

待機時間例外検出

この機能は、設定されたルール領域の待機時間を検知し、待機時間が警報発生条件を満たした場合に警報を発します。

開始前に

- **VCA → アプリケーション選択**に移動し、「**People Management**」を選択して「**次へ**」をクリックし、機能を有効化してください。
- HEOP対応デバイスでは、**VCAでPeople Managementを**インポートし有効化してください。

手順

1. **VCA → アプリケーション設定 → 人物管理 → 地域別人物カウント → ルール** に移動します。
2. 「**追加**」をクリックしてルールを追加し、名前を設定します。
3. ルールを設定します。

図10-15 ルール設定

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。OSDウィンドウの位置はマウスでドラッグして調整できます。

例外ごとのアラーム時間

アラーム発生後のアラーム継続時間を指します。チェックせず時間を設定しない場

合、デバイスはアラームを継続送信します。

アラーム間隔

設定された**アラーム間隔**内で、同一アラームはアップロードされません。

初回アラーム遅延

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

注記

滞留時間例外アラームは、**アラームトリガー条件が閾値Aより大きい**場合に限り、**例外ごとのアラーム回数**、**アラーム間隔**、**初回アラーム遅延**の設定をサポートします。

---

4. 「 」をクリックし、ライブビューウィンドウ内で領域を描画します。ライブビューウィンドウ内で終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終了します。

注

- 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. 「**滞留時間例外アラーム**」をチェックし、「**アラームトリガー条件**」と「**アラーム閾値**」を設定します。

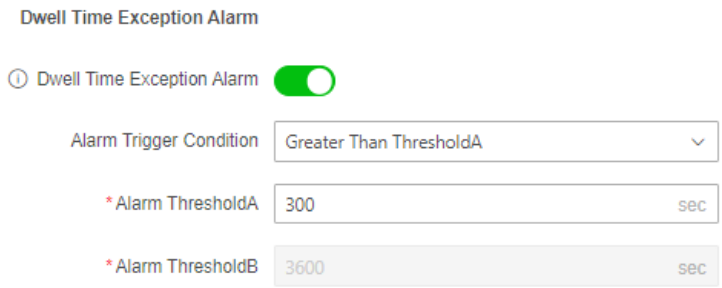

図10-16 滞留時間例外アラーム

6. 警戒スケジュールを設定します。*「警戒スケジュールの設定」*を参照してください。
7. 連動方法を設定します。*「連動方法の設定」*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。詳細な設定については、*「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

VCA → People Management → Overlay & Capture に移動します。キャプチャした画像に重ねて表示したい情報をチェックします。また、↑ ↓ をクリックして順序を調整することもできます。

10.5.3 詳細設定

人物管理機能の詳細パラメータを設定し、「**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示します。

アルゴリズムモード

設置状況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示します。このピクセルサイズを超えるターゲットは実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による誤検知を除去できます。

変位

ターゲットの変位またはターゲット幅を表します。設定されたパーセンテージ未満の変位を持つターゲットはカウントされません。

最小待機時間

設定値より短い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は困難になるが、精度も高くなる。

注意

フィルタリング設定は専門家が操作する必要があります。フィルタ設定により検出アルゴリズムを調整し、検出範囲や感度などを変更できます。

10.6 人数カウント

人数のカウントは、エリアへの入退場者数を計算するために使用されます。

注意

- 一部のデバイスモデルでは、まずVCAページで**人流計測を**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 人数カウントルールの設定

検知ルールとアルゴリズムパラメータを設定すると、デバイスはルールエリアへの入退場者数を計算し、連動アクションをトリガーし、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。**「人流計測」**を選択し、**「次へ」**をクリックして機能を有効化します。
- HEOP対応デバイスでは、**VCAで**「**人流計測**」をインポートし有効化してください。

手順

1. **VCA → アプリケーション設定 → 人数カウント → ルール** に移動します。
2. 機能を有効にするには**「有効にする」**をチェックします。
3. **「追加」**をクリックして検知エリアを追加します。
4. 「 」をクリックして多角形検知エリア（カウントエリア）を描画します。ライブビューウィンドウで左クリックで頂点を指定し、右クリックで描画を終了します。
5. 「 」をクリックして検知ラインを描画します。矢印は進入方向を示します。
   「 」をクリックすると方向を変更できます。

   注意

   計数精度向上のため、以下のルールに従って検知エリアを描画してください。
   - 検知エリアは、出入りする人の経路を完全にカバーする必要があります。
   - 検知ラインは赤色検知エリア内に完全に収まり、通行者の経路に対して垂直である必要があります。

6. オプション：検知エリアと検知ラインを調整してください。

クリック ✕ 選択した検知エリアまたはラインをクリアします。

クリック 🗑 すべての検出領域と検出ラインをクリアします。

7. オプション：上記の手順を繰り返し、最大3つの検知エリアと対応する検知ラインを描画します。
8. 人数カウントパラメータを設定します。

OSDオーバーレイ内容

ライブビュー画像に表示するカウントデータタイプ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での人流計測データの表示位置を調整します。

注

OSDオーバーレイは当日の人のみを集計します。デバイス再起動時または日次リセット時刻にデータは自動消去されます。

日次リセット時間

デフォルトでは毎日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刻を選択可能です。選択後、毎日この時刻にカウントデータが自動クリアされます。

「手動リセット」をクリックすると、データリセットを手動でトリガーし、現在の人数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. 警戒スケジュールを設定します。*「警戒スケジュールの設定」*を参照してください。
11. 連動方式を設定します。*「連動方式設定」*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：人流計測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。設定完了後、**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ます。

定期的なデータアップロード

データ統計サイクルを設定すると、乗客数カウントデータが設定された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：人流計測の高度なパラメータを設定します。

詳細設定をクリックして画面に入ります。設定完了後、**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示します。

ストレージデータのクリア

デバイスに保存されている全ての人数計測データを消去します。この機能は慎重に使用してください。

結果

- 対象が進入方向に沿って検知エリアを横切り、検知ラインを越えた場合、進入数としてカウントされます。
- 対象が退出方向に沿って検知エリアを通過し、検知ラインを越えた場合、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、車両検知および混合交通検知が利用できます。本装置は、通過する自動車および非自動車を捕捉し、捕捉した画像とともに、関連情報をアップロードします。

注記

- 特定のデバイスモデルでは、まず **VCA** ページで**「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 車両検知の設定

設定レーンに進入した車両を検知し、車両画像とナンバープレート画像をキャプチャして保存できます。アラームが作動し、キャプチャ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。
- デバイスが正しく設置されていることを確認してください。
- 画像パラメータが適切に設定されていることを確認してください。
- 撮影されたナンバープレート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 → アプリケーション設定 → 道路交通 → ルール** に移動し、検出タイプとして**車両検出**を選択します。
2. **[有効化]** 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、車両が検出エリアを通過し、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

車両が検知エリアを通過し、市街地での検知をトリガーすると、検知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。

警報入力

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。

注記

- **アラーム入力**を選択した場合、アラーム入力 A<-1 は自動的に車両検知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 となります。
- A<-1 アラーム入力を車両検知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 に対して以前設定されていた連動方法はキャンセルされます。

4. 車線総数を選択します。
5. 車線ラインをクリックしてドラッグし位置を設定するか、ライン端をクリックしてドラッグしラインの長さと角度を調整します。

   青い検知ラインはナンバープレート検知のトリガーラインであり、主に「**出入口**」シーンで撮影効率を向上させるために使用されます。画面の中央下部付近に配置し、ナンバープレート付きのフルサイズ車両が確実に通過できるようにすることを推奨します。
6. カメラのズーム倍率を調整し、画像内の車両サイズが赤い枠に近くなるようにします。調整可能なのは赤い枠の位置のみです。

注記

各レーンで同時に撮影できるナンバープレートは1枚のみです。

7. **エリア**と**国/地域**を選択します。
8. 検知モードを設定します。

車両優先

本装置はまず車両スケールを検知し、その後ナンバープレートを捕捉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には結果が失われる場合があります。

ナンバープレート＆車両

ナンバープレート＆車両モードでは、デバイスがナンバープレートと車両を同時に検知し、警報情報と撮影画像をアップロードします。

注記

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推奨します。ナンバープレート認識の問題が解決された後、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. 「**重複ナンバープレート削除**」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連動方法**」に移動します。ブロックリスト、許可リスト、その他のリストごとに武装スケジュールと連動方法を個別に設定でき、それぞれ順に設定する必要があります。

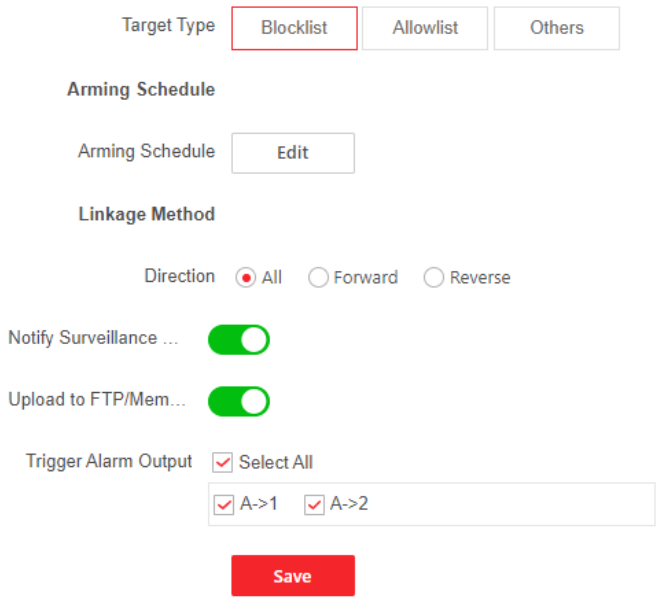

図10-17 警戒スケジュールと連動方法

1) ブロックリスト、許可リスト、その他のリストをクリックして選択します。
2) 警戒スケジュールを設定します。詳細は*「警戒スケジュールの設定」*を参照してください。
3) 連動方法を設定します。各ルールに対応する連動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、選択した連動方法をトリガーできます。

全方向

「**すべて**」は、全移動方向の車両が対象となります。特別な用途がない場合は「**すべて**」を選択することを強く推奨します。

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

後退は、車両がカメラから離れて移動することを意味します。

ウィーガンド連携

本デバイスは、ウィーガンドプロトコルを介してサードパーティプラットフォームへレポートを送信できます。
デバイスがウィーガンドインターフェースをサポートしていること、およびデバイスがウィーガンドインターフェースで接続されていることを確認してください。
システム設定でウィーガンドが有効化され、プロトコルが適切に設定されていることを確認してください。詳細は*ウィーガンド*を参照してください。
ウィーガンド連動を有効にし、外部デバイスに接続されたウィーガンドインターフェースを選択してください。

検出された車両の進行方向が設定された方向と一致した場合にのみ連動がトリガーされます。

12. **道路交通 → オーバーレイとキャプチャ**に移動し、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。詳細は*オーバーレイとキャプチャ*を参照してください。
13. ナンバープレートブロックリストと許可リストをインポートまたはエクスポートします。詳細は「*ブロックリストと許可リストのインポートまたはエクスポート*」を参照してください。

10.7.2 混合交通検知ルールの設定

設定レーンに進入する自動車と非自動車を検知し、対象の画像をキャプチャ・保存できます。アラームが作動し、キャプチャ画像をアップロード可能です。

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。
- デバイスが正しく設置されていることを確認してください。
- 画像パラメータが適切に設定されていることを確認してください。

手順

1. **VCA → アプリケーション設定 → 道路交通 → ルール** に移動し、検知タイプとして「**混合交通検知**」を選択します。
2. **[有効化]** にチェック**を入れます**。
3. 車線総数を選択します。
4. 車線ラインをクリック＆ドラッグして位置を設定するか、ライン端をクリック＆ドラッグして長さと角度を調整します。

青色の検知ラインはナンバープレート検出のトリガーラインであり、主に「**出入口**」シーンで撮影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フルサイズ車両が確実に通過できるよう、画面中央下部への配置を推奨します。

5. カメラのズーム倍率を調整し、画像内の車両サイズが赤い枠に近くなるようにします。調整可能なのは赤い枠の位置のみです。

注記

各レーンで同時に撮影できるナンバープレートは1枚のみです。

6. **エリア**と**国/地域**を選択します。
7. 「**重複ナンバープレートを除去**」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**」をクリックします。
9. 「**武装スケジュールと連動方法**」に移動します。ブロックリスト、許可リスト、その他のリストごとに武装スケジュールと連動方法を個別に設定でき、それぞれ順に設定する必要があります。

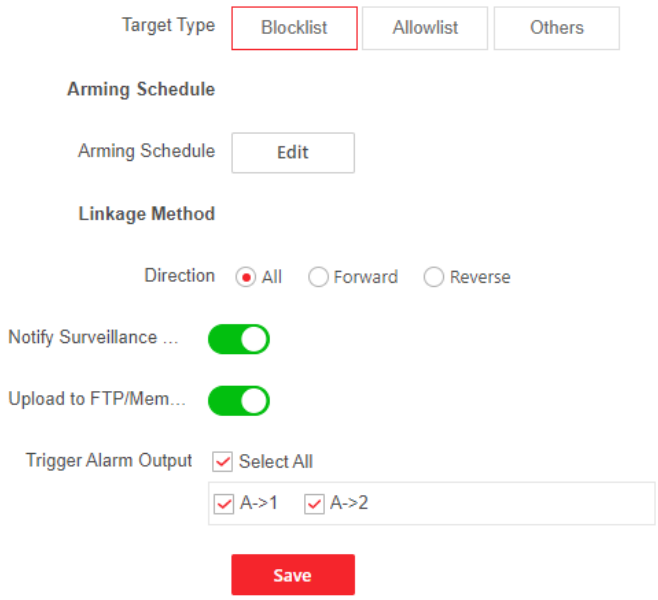

図10-18 警戒スケジュールと連動方法

1) ブロックリスト、許可リスト、その他のリストをクリックして選択します。
2) 警戒スケジュールを設定します。詳細は *「警戒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選択し、**[保存]**をクリックして設定を保存します。

方向

選択した方向へ移動する車両のみが、選択した連動方法をトリガーできます。

すべて

「**すべて**」は、すべての移動方向の車両が対象となります。特別な用途がない場合は「**すべて**」を選択することを強く推奨します。

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

後退は、車両がカメラから離れて移動することを意味します。

ウィーガンド連携

本デバイスは、ウィーガンドプロトコルを介してサードパーティプラットフォームへレポートを送信できます。
デバイスがウィーガンドインターフェースをサポートしていること、およびデバイスがウィーガンドインターフェースで接続されていることを確認してください。
システム設定でウィーガンドが有効化され、プロトコルが適切に設定されていることを確認してください。詳細は*ウィーガンド*を参照してください。
ウィーガンド連動を有効にし、外部デバイスに接続されたウィーガンドインターフェースを選択してください。

検出車両の進行方向が設定方向と一致した場合にのみ連動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**」で、撮影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およびアロリストをインポートまたはエクスポートします。詳細は「*ブロックリストとアロリストのインポート/エクスポート*」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、キャプチャ画像の画像パラメータを設定できます。

VCA に移動し、**道路交通**を選択します。

VCA → アプリケーション設定 → 道路交通 → オーバーレイとキャプチャ に移動しま

す。

注

この機能は、デバイスモデルによって異なります。

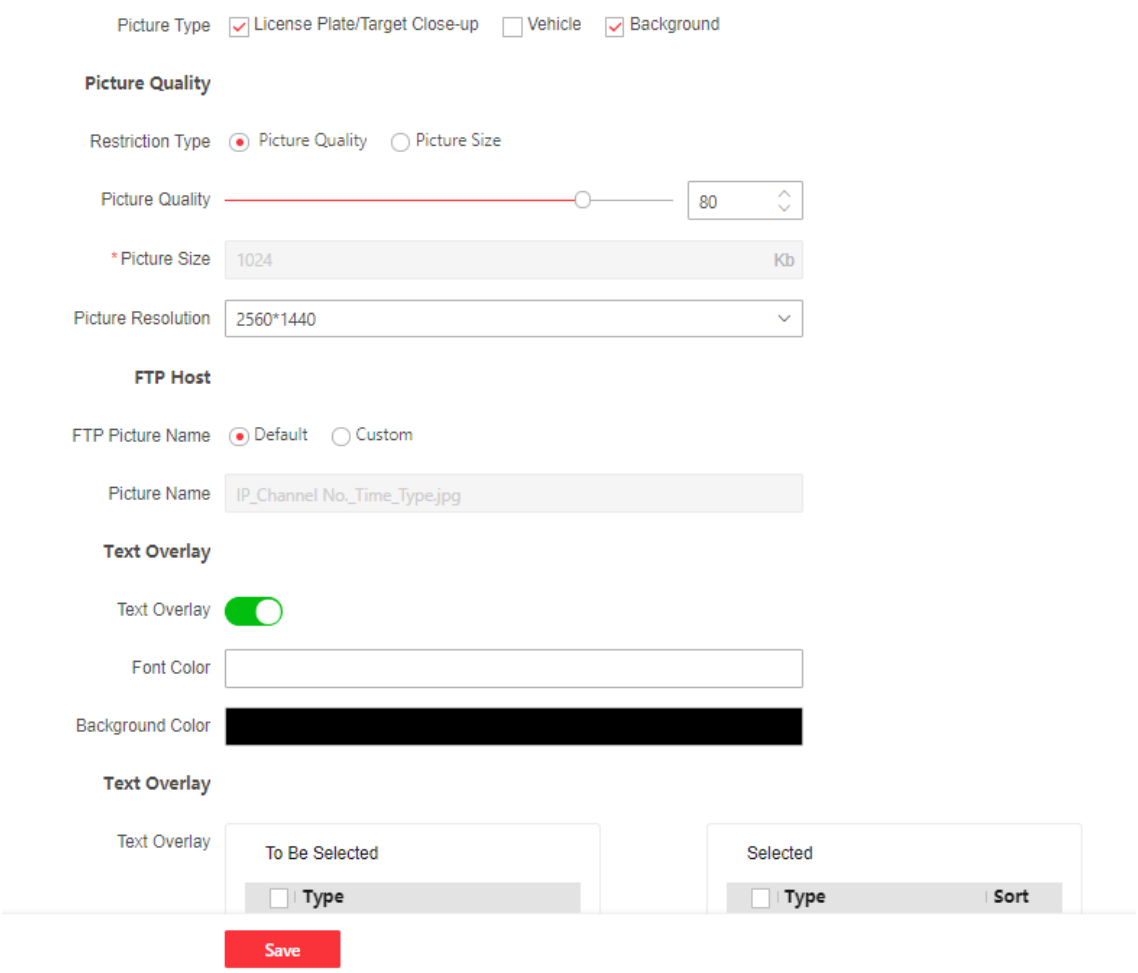

図 10-19 オーバーレイ＆キャプチャ

画質

数値が大きいほど画質は鮮明になりますが、必要な保存容量も大きくなります。

画像サイズ

値が大きいほど、より多くのストレージ容量が必要となります。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

キャプチャされる背景画像の解像度。

画像キャプチャ間隔

カメラは、設定された間隔ごとにアラームを連続的にトリガーし、キャプチャした画像をアップロードします。

撮影間隔を確認し、間隔を設定してください。

FTP ファイル名

車両検知および混合交通検知でキャプチャした画像の命名規則をFTPサーバーで設定できます。

デフォルトを使用する場合は「デフォルト」を選択します。

カスタムを選択し、画像名の情報を選択し、↑ ↓ をクリックして画像名パラメータの順序を調整します。カスタムモードで**キャプチャ時刻**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キャプチャ画像は、同じ画像名のため、以前にキャプチャされた画像を置き換えます。

注記

FTP設定の詳細については、「***FTPの設定***」を参照してください。

テキストオーバーレイ

キャプチャ画像にカメラ、デバイス、または車両情報をオーバーレイ表示できます。

↑ ↓ をクリックすると、オーバーレイテキストの順序を調整できます。

色ボックスを選択してフォント色と背景色を設定し、ポップアップパレットまたはドロップダウンボックスで希望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を必要に応じてインポートおよびエクスポートでき、このインターフェースでリストの内容を確認できます。

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&許可リストファイルを探し、クリックして選択します。**「開く」**をクリックして確定します。

注意

- インポートするファイルは、カメラが要求するファイルテンプレートに対応している必要があります。カメラから空のブロックリスト&許可リストファイルをテンプレートとしてエクスポートし、内容を記入することをお勧めします。
- ファイル形式は.xls形式とし、セル形式はテキストに設定してください。

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」**をクリックしてナンバープレートリストをエクスポートします。
6. オプション：**[Add]**をクリックし、ナンバープレートを1つずつ追加して関連情報を設定します。
7. オプション： をクリックし、フィルタリングタイプを選択します。**全タイプ**、**Wiegandカード ID**、**ナンバープレート番号**、**タイプ**から選択可能です。**タイプ**については、**キーワード**を選択して具体的なフィルタリングタイプを定義できます。**Search**をクリックすると結果が表示されます。
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プレートを削除できます。
9. 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該当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、**「詳細設定」**をクリックして詳細パラメータを設定します。設定完了後、**「保存」**をクリックします。

注

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バージョンを示します。

インテリジェント情報のオーバーレイ

動画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、ユーザーが提供するトレーニング素材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、ユーザーがタスクと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検出されルールがトリガーされると、デバイスは連動アクションを実行でき、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。

注記

- 本機能は特定のデバイスモデルでのみサポートされます。
- 特定のデバイスモデルでは、まずVCAページで**AIオープンプラットフォームを**有効にする必要があります。

10.8.1 AIオープンプラットフォームの設定

手順

1. **VCA → アプリケーション設定 → AI Open Platform** に移動します。

注記

- AIオープンプラットフォーム経由で設定可能な特定スマート機能（例：ヘルメット検知、炭鉱安全検知など）をサポートします。
- 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ので、実際のデバイスをご確認ください。

  - **ヘルメット検知では**、設定された検知エリア内でヘルメットを着用していない対象を検知し、警報を発します。
  - **炭鉱安全検知では、VCA → アプリケーション設定 → 炭鉱安全管理** に移動し機能を有効化してください。炭鉱シナリオにおいて、検知エリア内の人物や鉱山車両などの対象物を検知し、ベルトがローラーから外れた場合や被爆者がヘルメットを着用していない場合を検知します。炭鉱安全検知の設定ルールに基づき警報を発します。

2. オプション：**モデルライブラリ**へのモデル追加。ローカルパスから**モデル**ライブラリと関連**ラベルファイル**を選択し、**モデル名を**設定します。モデルタイプは以下の通りです。

検知モデル

ライブビュー内の特定対象物を検知し、検知結果と対象物の座標位置を提供する。

分類モデル

画像または対象物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分類します。

注記

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化します。
4. **分析モード**を選択します。

ライブ動画分析	デバイスはライブ映像を分析し、ターゲット検出と結果アップロードを実現します。
スケジュール撮影分析	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を行い、キャプチャした画像を分析し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	ターゲットフレームをアラーム画像に重ねて表示します。
ルールオーバーレイ	アラーム画像にルール情報を重ねて表示します。

6. 警戒スケジュールと連動方法を設定します。警戒スケジュール設定については*「警戒スケジュールの設定」*を参照してください。連動方法設定については*「連動方法の設定」*を参照してください。
7. 連動チャンネルのルールを設定します。詳細は*「ルールの設定」*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 で関連モデルが選択され、タスク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「Linked Channel」**をクリックし、チャンネルを選択します。

2. リンク済みチャネルの「⚙ 」をクリックしてルールを設定します。

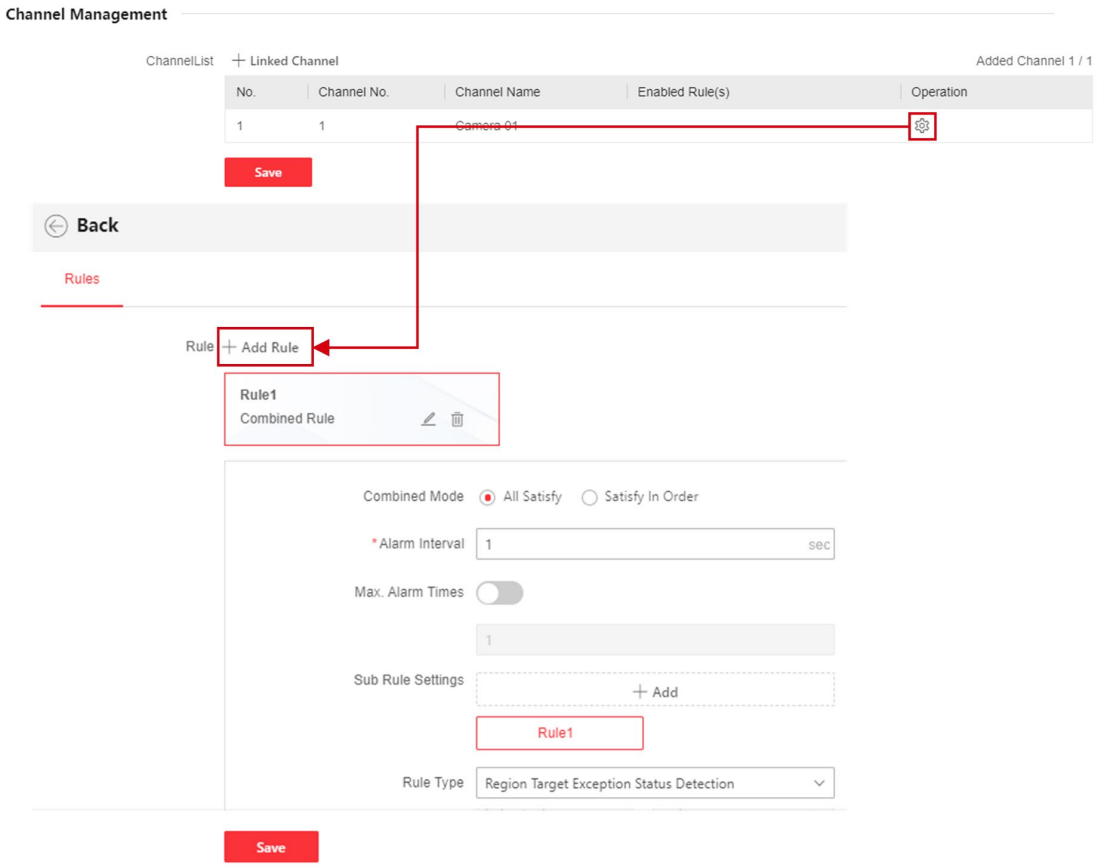

図10-20 ルール設定

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

事前定義された仮想ルール領域内のターゲットを検出し、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した場合、アラームをトリガーします。

ライン越えターゲット検出

事前定義された仮想ルールラインを横断するターゲットを検知し、検知時にアラームをトリガーします。

フル分析ルール

事前定義された仮想ルール領域内の全ターゲットを検出・分析します。

ライン越えターゲット計数

事前に定義された仮想ルールラインを横断するターゲットを検知し、その数をカウントします。

領域内ターゲット数計測

事前定義された仮想ルール領域内のターゲットを検知し、数をカウントします。

複合ルール

において、事前定義された仮想ルール領域内での**地域ターゲット例外状態**検出および**ライン越えターゲット検出**をサポートします。検出順序については、**複合モード**を「**全て満たす**」または「**順序通り満たす**」に設定できます。

注記

ルールタイプはモデルパッケージによって異なります。実際の機器を参照してください。

4. 検知ルールを設定し、ルール領域または線を引く。
   - 検知領域の描画：をクリックし、ライブビューウィンドウ内で凸形状の領域を描画します。ライブビューウィンドウ内で終点を左クリックして設定領域の境界を定義し、右クリックで描画を終了します。
   - ルールラインの描画：をクリックするとライブ映像に矢印付き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位置にドラッグします。
5. ルールパラメータの設定。

対象物

モデルの検出対象タイプ。

属性

モデルの検出対象プロパティ。

期間

ステータスの持続時間。設定され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、同一タイプのアラームは通知を1回のみトリガーします。

感度

感度値が高いほど、アラームはより簡単に作動します。感度値が大きすぎると、誤作動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において、アラームがトリガーされる最大回数。

カウント間隔

カウントを行う時間間隔。

アルゴリズム有効性

アルゴリズムが示す信頼閾値が設定された有効期間以上である場合、アラームがトリ

ガーされアップロードされる。

ラインクロス

ターゲットがラインを横切る方向。

数量

数量を確認し、ドロップダウンボックスから警報ルールを選択します。警報ルールに応じて**閾**値または 範囲（**最小値と最大**値）**を**設定します。対象物の数が設定された警報ルールを満たした場合、デバイスは警報を発します。

レポート時間間隔

地域対象数カウントを選択した場合、カウント結果をアップロードする時間間隔を指します。

注記

ルールパラメータはルールによって異なります。実際のデバイスを参照してください。

6. 「**保存**」をクリックします。

第11章 EPTZ

EPTZ（電子PTZ）は、物理的なカメラの動きを伴わずに画像の一部をデジタルズームおよびパンする高解像度機能です。EPTZ機能を使用するには、お使いのデバイスが**サードストリーム**をサポート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。

注記

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** に移動します。
2. **[有効化]** 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。

次の手順

パトロール設定の詳細については、ライブビュー画面でのPTZ操作を参照してください。

11.2 自動追跡

手順

1. **設定** → **EPTZ** に移動します。
2. 「**有効化**」にチェックを入れます。
3. **ストリームタイプは**デフォルトで**サードストリーム**であり、設定できません。
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。ライブビューの映像をクリックして検知領域の4つの頂点を指定し、右クリックで描画を完了します。
6. ルールを設定します。

検出対象

人物と車両が選択可能です。検出対象が選択されていない場合、人物と車両を含むす

べての検出対象が追跡されます。

注

この機能は特定のカメラモデルのみが対応しています。

感度

許容対象の身体部位のうち追跡対象となる割合を示します。感度 = 100 - S1/ST × 100。S1は事前定義領域に進入した対象身体部位、STは対象身体全体を表します。感度値が高いほど対象の追跡が容易になります。

7. 「**保存**」をクリックします。

A. よくある質問

以下のQRコードをスキャンすると、本デバイスのよくある質問を確認できます。

一部のFAQは特定モデルにのみ適用されることにご注意ください。