ネットワークカメラ

ユーザーマニュアル

法的情報

このドキュメントについて

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

本製品について

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

知的財産権の承認

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

法的免責事項

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

明示的または黙示的ないかなる保証も提供しません。これには、商品性、満足のいく品質、または特定の目的への適合性に関する保証が含まれますが、これらに限定されません。製品の使用は、お客様の責任において行ってください。いかなる場合においても、HIKVISION は、事業利益の損失、事業の中断、データの損失、システムの破損、または文書の損失を含むがこれらに限定されない、特別、結果的、偶発的、または間接的な損害について、お客様に対して一切の責任を負いません。システムの破損、または文書の損失を含む損害について、契約違反、不法行為（過失を含む）、製品責任、またはその他の理由に基づくものであっても、製品の使用に関連して生じた場合であっても、HIKVISIONは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、セキュリティ上のリスクが内在していることを認識し、サイバー攻撃、ハッカーの攻撃、ウイルス感染、その他のインターネットセキュリティリスクに起因する異常な動作、プライバシーの漏洩、その他の損害について、HIKVISION は一切の責任を負わないことを認めるものとします。ウイルス感染、またはその他のインターネットセキュリティリスクに起因する異常な動作、プライバシーの漏洩、その他の損害について一切の責任を負いません。ただし、必要に応じて、HIKVISION はタイムリーな技術サポートを提供します。
- あなたは、この製品を適用されるすべての法律に準拠して使用することに同意し、あなたの使用が適用される法律に準拠していることを確保する責任は、あなたのみに帰属します。特に、お客様は、パブリシティ権、知的財産権、データ保護およびその他のプライバシー権を含むがこれらに限定されない、第三者の権利を侵害しない方法で本製品を使用することについて責任を負います。お客様は、大量破壊兵器の開発または製造、化学兵器または生物兵器の開発または製造、核爆発または安全でない核燃料サイクルに関連するいかなる活動、または人権侵害を支援する目的での使用を含みます。
- 本文書と適用法との間に矛盾がある場合は、適用法が優先するものとします。

記号の定義

本文書中に使用される記号は、以下のとおり定義されます。

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

安全に関する指示

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

図 1-1 安全に関する注意事項

目次

第1章 システム要件

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

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

第2章 デバイスのアクティベーションとアクセス

ユーザーアカウントとデータのセキュリティ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場合は、デバイスをアクティブにするログインパスワードを設定してください。

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

2.1 SADP 経由でデバイスをアクティベートする

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

開始前に

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

手順

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

   注意

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

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

2.2 ブラウザ経由でデバイスをアクティブ化

ブラウザ経由でデバイスにアクセスし、アクティベートできます。

手順

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

注意

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

3. ブラウザに***192.168.1.64***を入力してください。
4. デバイス起動パスワードを設定してください。

注意

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

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

2.3 ログイン

ウェブブラウザーからデバイスにログインします。

2.3.1 プラグインのインストール

一部のオペレーティングシステムおよびウェブブラウザーでは、カメラ機能の表示および操作が制限される場合があります。正常に表示および操作を行うためには、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、実際の機器をご確認ください。

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

注意

カメラは Windows および Mac OS システムのみに対応しており、Linux システムには対応していません。

2.3.2 管理者パスワードの回復

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

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

注意

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

セキュリティの質問

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

メール

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

2.3.3 不正ログインロック

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

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

不正ログイン試行

間違ったパスワードでログインを試行した回数が設定された回数に達すると、デバイスがロックされます。

ロック時間

設定した期間が経過すると、デバイスはロックを解除します。

第3章 ライブビュー

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

3.1 ライブビューパラメーター

対応する機能はモデルによって異なります。

3.1.1 表示制御

ディスプレイ制御領域では、ライブビューのデコードモード、マウントタイプ、および表示モードを選択できます。ソフトウェアまたはハードウェアのデコードモードを選択した後、対応する複数のマウントタイプと表示モードから1つを選択できます。

デコードモード

- **ソフトウェア**デコードモードとは、ライブビューのビデオがコンピュータの CPU によってデコードされるモードです。ライブビューのパフォーマンスは、コンピュータのデコード能力によって異なります。
- **ハードウェア**デコードモードとは、ライブビュービデオがカメラによってデコードされるモードです。

マウントタイプ

カメラの実際の取り付けタイプに応じて、天井取り付け、ウォールマウント、テーブル取り付けから選択できます。すべての取り付けタイプアイコンの説明は、次のとおりです。

表 3-1 取り付けタイプの説明

アイコン	説明
	ウォールマウント
	テーブル取り付け
	天井取り付け

注意

取り付けタイプは実際のモデルによって異なります。取り付けタイプが1種類のみのモデルでは、取り付けタイプを選択できません。

表示モード

ライブビューウィンドウのレイアウトの表示モードを選択できます。使用できる表示モードは、選択したデコードモードによって異なります。すべての表示モードアイコンの説明は、次のとおりです。

表 3-2 表示モードアイコンの説明

アイコン	説明	アイコン	説明
	魚眼ビュー。		円筒形ビュー。
	180度パノラマビュー。		360度パノラマビュー。
	360度パノラマビューとPTZビュー。		360度パノラマビューと3つのPTZビュー。
	360度パノラマビューと6つのPTZビュー。		360度パノラマビューと8つのPTZビュー。
	2つのPTZビュー。		4つのPTZビュー。
	魚眼ビューと3つのPTZビュー。		魚眼ビューと8つのPTZビュー。

アイコン	説明	アイコン	説明
	半球ビュー。		AR半球ビュー。
	4つのPTZビューの融合。		パノラマビュー。
	180度デュアルチャンネルパノラマビュー。		パノラマビューと3つのPTZビュー。
	パノラマビューと8つのPTZビュー。		

注意

- 機能は表示モードによって異なる場合があります。
- ハードウェアデコードモードを選択した場合、
  - 表示モードを切り替えるには再起動が必要です。
  - フィッシュアイビューの表示モードにおいて、デコードモードをソフトウェアデコードモードに切り替えることができます。
  - フィッシュアイビューの表示モードで***VCAリソース***を設定でき、表示モードが180度パノラマビューまたは180度デュアルチャンネルパノラマビューの場合、***CuFngラインと水平半径の角度***を設定できます。
- ソフトウェアデコードモードを選択した場合、すべての表示モードで***VCAリソース***を設定できます。

3.1.2 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。

3.1.3 アスペクト比

アスペクト比は、画像の幅と高さの表示比率です。

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

3.1.4 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のストリームタイプを選択してください。ストリームタイプの選択に関する詳細情報は、***Stream Type*** をご参照ください。

3.1.5 サードパーティプラグインを選択してください

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

手順

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

3.1.6 ライト

をクリックして、照明のオン/オフを切り替えます。

注意

レーザーを搭載したデバイスについて:

- 動作中の光源を直視しないでください。目に有害な場合があります。
- 適切な遮光装置や保護メガネがない場合は、安全な距離から、または光が直接当たらない場所で照明を点灯してください。
- 装置の組み立て、設置、またはメンテナンスを行う際は、ライトを点灯したり、保護メガネを着用したりしないでください。

3.1.7 ピクセルを数える

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

手順

1. 「 」をクリックして機能を有効にします。

2. 画像上でマウスをドラッグして、目的の矩形領域を選択します。
ライブビュー画像の下部に、幅ピクセルと高さピクセルが表示されます。

3.1.8 デジタルズームを開始します

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. 「 」をクリックしてデジタルズームを有効にします。

2. ライブビュー画像で、マウスをドラッグして目的の領域を選択します。

3. ライブビュー画像をクリックすると、元の画像に戻ります。

3.1.9 補助フォーカス

電動式デバイスに使用します。デバイスが明確に焦点を合わせることができない場合に、画像の品質を向上させることができます。

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

「 」をクリックして自動でピントを合わせます。

注意

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

3.1.10 レンズの初期化

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

をクリックして、レンズの初期化を行います。

3.1.11 レンズパラメータの調整

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

注意

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

方向制御

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

ズーム

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

フォーカス

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

絞り

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

PTZ速度

- をスライドして、パン/チルトの動きの速度を調整します。

3.1.12 3D位置調整

3D 位置決めは、選択した領域を画像の中心に移動する操作です。

手順

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

3.2 送信パラメーターを設定します

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

手順

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

プロトコル

TCP

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

UDP

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

マルチキャスト

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

注意

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

HTTP

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

再生性能最短遅延

ビデオの滑らかさを優先するよりも、リアルタイムのビデオ画像を優先します。

バランス

デバイスは、リアルタイムのビデオ画像と滑らかさを両立します。

滑らか

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

カスタム

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

3. **保存**をクリックしてください。

第 4 章 ビデオおよびオーディオ

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

4.1 ビデオ設定

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

設定ページに移動：**設定→ ビデオ/オーディオ→ ビデオ** .

4.1.1 ストリームの種類

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

メインストリーム

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

サブストリーム

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

その他のストリーム

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

4.1.2 ビデオタイプ

ストリームに含めるコンテンツ（ビデオおよびオーディオ）を選択します。

ビデオストリーム

ストリームにはビデオコンテンツのみが含まれます。

ビデオ＆オーディオ

ビデオコンテンツとオーディオコンテンツが複合ストリームに含まれます。

4.1.3 解像度

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

4.1.4 ビットレートタイプと最大ビットレート

定常ビットレート

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

可変ビットレート

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

4.1.5 ビデオ品質

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

4.1.6 フレームレート

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

ビデオ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、画像品質が全体的に維持されるため有利です。フレームレートが高いほど、必要な帯域幅とストレージ容量も大きくなることにご注意ください。

4.1.7 ビデオエンコーディング

これは、デバイスがビデオエンコーディングに採用している圧縮規格を表します。

注意

入手可能な圧縮規格は、デバイスモデルによって異なります。

H.264

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

H.264

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

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

注意

H.264+ を有効にすると、**I フレーム間隔は**設定できません。

H.265

H.265 は、High Efficiency Video Coding (HEVC) および MPEG-H Part 2 としても知られ、圧縮規格です。H.264 と比較すると、同じ解像度、フレームレート、画質でより優れたビデオ圧縮を実現します。

H.265

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

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

注意

H.265+ を有効にすると、**I フレーム間隔は**設定できません。

Iフレーム間隔

Iフレーム間隔は、2つのIフレーム間のフレーム数を定義します。

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

SVC

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

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

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

MPEG4

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

MJPEG

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

プロファイル

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

4.1.8 スムージング

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

4.2 オーディオ設定

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

注意

一部のカメラモデルのみ対応しています。

4.2.1 オーディオエンコーディング

オーディオの音声圧縮を選択します。

4.2.2 オーディオ入力

注意

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

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

4.2.3 オーディオ出力

注意

必要に応じて、オーディオ出力デバイスを接続してください。

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

4.2.4 環境ノイズフィルター

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

4.3 双方向オーディオ

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

開始前に

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

手順

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

4.4 ROI

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

4.4.1 ROIを設定

ROI (関心領域) エンコーディングは、関心領域により多くのエンコーディングリソースを割り当て、ROI の品質を向上させ、背景情報への焦点を弱めるのに役立ちます。

開始前に

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

手順

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

注

調整が必要な固定領域を選択し、マウスをドラッグしてその位置を調整します。

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

注

ROI レベルが高いほど、検出された領域の画像が鮮明になります。

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

4.5 ターゲットクロッピングの設定

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

手順

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

注意

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

3. **トリミング解像度**を選択します。

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

注意

- ターゲットクロッピングは一部のモデルでのみ対応しており、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すると、一部の機能が使用できなくなる場合があります。

4.6 ストリームに情報を表示

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

開始前に

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

スマートイベント.

手順

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

4.7 ディスプレイ設定

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

示設定 に移動します。

デフォルトをクリックして設定を復元します。

4.7.1 シーンモード

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

画像調整

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

露出設定

露出は、絞り、シャッター、および感光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、画像効果を調整することができます。

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

フォーカス

フォーカスモードを調整するオプションがあります。

フォーカスモード

オート

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

セミオート

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

手動

ライブビュー画面で手動でフォーカスを調整できます。

デイ&ナイト切り替え

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

昼

画像は常にカラーで表示されます。

ナイト

画像は白黒またはカラーで、夜間でも鮮明なライブビュー画像を確保するために補助照明が点灯します。

注意

一部の機種のみ、補光機能とカラフルな画像に対応しています。

自動

カメラは、環境の光量に応じてデイモードとナイトモードを切り替えます。

スケジュール切り替え

開始時間と**終了時間を**設定して、昼間モードの継続時間を定義します。

アラーム入力によるトリガー

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

ビデオによってトリガー

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

注意

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

補助ライト設定

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

スマート補光機能

スマート補光機能は、補光ライトが点灯しているときに露出オーバーを防ぐ。

サプリメントライトモード

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

赤外線サプリメントライト

赤外線ライトが有効になっています。

白色光

白色光が有効になります。

混合光

IR ライトと白色光の両方が有効になっています。

スマート

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

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

オフ

補助光はオフです。

注意

補助光モードは、デバイスモデルによって異なる場合があります。

明るさ調整モード オート

実際の環境に応じて、明るさが自動的に調整されます。

手動

スライダーをドラッグするか、値を設定して明るさを調整できます。

BLC

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

WDR

WDR (ワイドダイナミックレンジ) 機能は、照度の差が大きい環境でも鮮明な画像を提供するカメラに役立ちます。

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

注意

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

図4-1 WDR

HLC

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

ホワイトバランス

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

図4-2 ホワイトバランス

DNR

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

標準

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

エキスパート

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

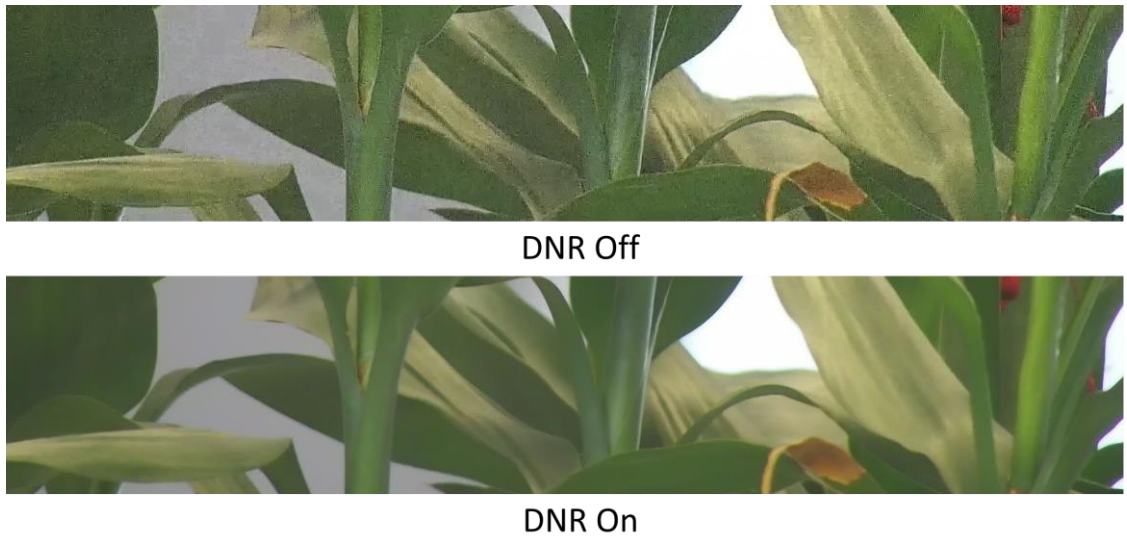


図4-3 DNR

デフォグ

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

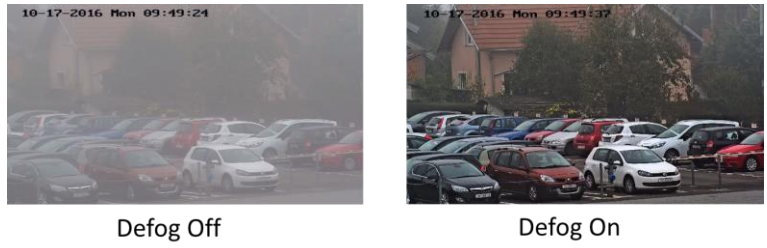


図4-4 除霧

EIS

ジッター補正技術により、ビデオ画像の安定性を高めます。

グレースケール

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

ミラー

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

必要に応じてミラーモードを選択してください。

注意
この機能を有効にすると、ビデオ録画が一時的に中断されます。

回転

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

注意
この機能は、特定の設定下でサポートされています。

レンズの歪み補正

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

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

4.7.2 画像パラメーターの切り替え

設定した時間ごとに、画像パラメーターを自動的に切り替えます。

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

スケジュール切り替えを設定

一定時間ごとに、リンクされたシーンモードに画像を自動的に切り替えます。

手順

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

注意

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

3. **保存**をクリックします。

4.7.3 ビデオ規格

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

4.7.4 ローカルビデオ出力

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

出力モードをON/OFFに設定して出力を制御します。

4.7.5 切断線と水平半径の角度

ハードウェアデコードモードで 180 度パノラマビューまたは 180 度デュアルチャンネルパノラマビューの表示モードを選択すると、特定のターゲットのライブビューを任意に調整するために、切断線と水平半径の角度を調整することができます。ライブビューは、設定した角度に応じて変化します。

1. **ライブ**ビューページで、ハードウェアデコードモードにおいて180度パノラマビューまたは180度デュアルチャンネルパノラマビューの表示モードを選択します。
2. **設定→ 画像→ 表示設定→ ビデオ調整**に移動し、**切断線と水平半径の角度**を設定します。

180度パノラマ表示

角度を0°、30°、60°、90°、120°、180°から選択できます。30°の角度を例に取ると、ライブビューは次のように変更されます:

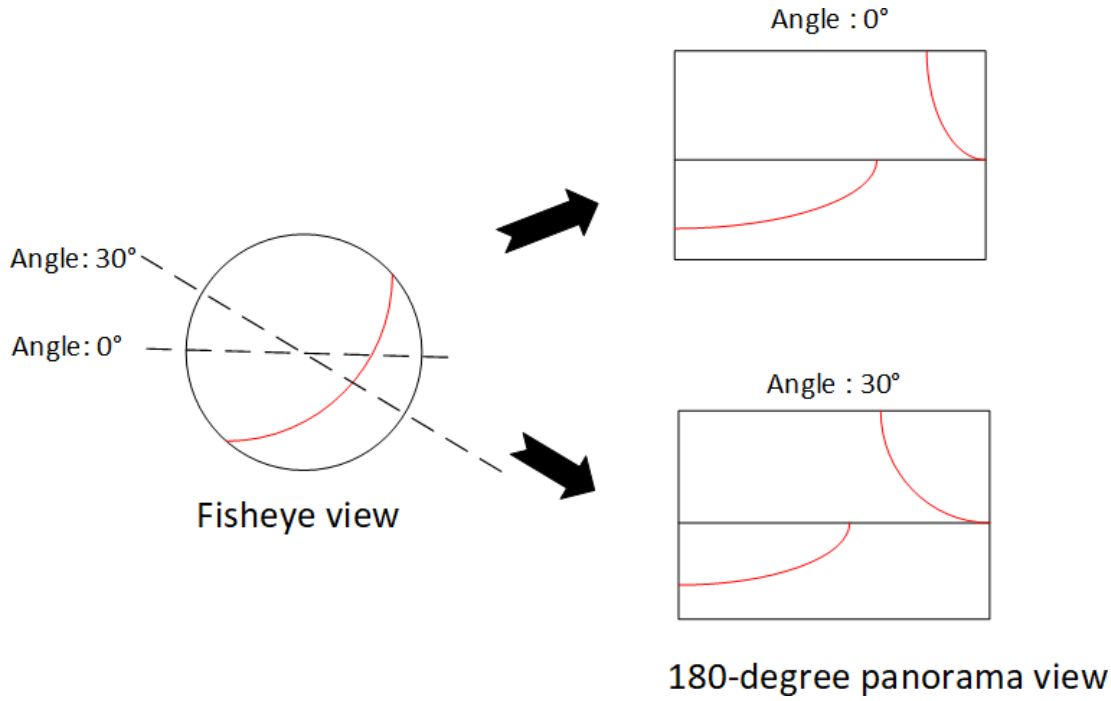


図4-5 180度パノラマビューの角度を設定する

注
実際のライブビューは、カメラモデルやマウントタイプによって異なります。

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にします。

文字セット

表示する情報の文字コードを選択してください。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**を選択してください。

表示

カメラ名、日付、曜日、およびそれらの表示形式を設定します。一部のデバイスモデルでは、表示情報としてチルト角度も設定できます。

フォーマット設定

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

テキストオーバーレイ

画像にカスタマイズしたオーバーレイテキストを設定します。

4.9 プライバシーマスクの設定

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

手順

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

4.10 画像を重ねる

ライブビューにカスタム画像を重ねます。

開始する前に

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

手順

1. **[Configuration]**、**[→]**、**[Image]**、**[→]**、**[Picture Overlay]** の順に選択します。
2. **「有効」**にチェック**を入れます**。
3. **「アップロード」**をクリックして画像を選択し、開きます。
   アップロードが成功すると、赤い四角形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 ビデオ録画と画像キャプチャ

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

5.1 ストレージ設定

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

5.1.1 メモリカード

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

新しいまたは暗号化されていないメモリカードの設定

開始前に
新しい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ます。詳細なインストール手順は、デバイスの *クイックスタートガイド* を参照してください。

手順

1. **設定→ ストレージ→ ストレージ管理→ HDD 管理** .
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、まずメモリカードをロック解除する必要があります。詳細については *「メモリカードの状態」を確認する* を参照してください。
3. **フォーマット**をクリックしてメモリカードを初期化します。
   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、メモリカードが使用可能になります。
4. **オプション：** メモリカードを暗号化します。
   1) **「暗号化フォーマット」**をクリックします。
   2) 暗号化パスワードを設定します。
   3) **「OK」**をクリックします。
   暗号化状態が「暗号化済み」に変わると、メモリーカードは使用可能になります。

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

6. **保存**をクリックしてください。

暗号化メモリカードの設定

開始前に

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

手順

1. **[Configuration]** (設定) に移動します。**→(ストレージ) を選択します。→(ストレージ管理) を選択します。→(HDD 管理) を選択します。**

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、まずメモリカードをロック解除する必要があります。詳細については*「メモリカードの状態」を確認する*を参照してください。

3. 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てください。

3) **OK**をクリックしてください。

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

注意

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

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

5. **保存**をクリックしてください。

メモリカードの状態を検出

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

開始前に

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

手順

1. **[Configuration]** (**設定**) に移動します。**→(メモリカード) を選択します。→(メモリカード管理) を選択します。→(メモリカード検出) を選択します。**

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

残存寿命

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

健康状態

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

注意

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

3. **R/W ロック**をクリックして、メモリカードへの読み書きの権限を設定します。

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

注意

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

4. **アーミングスケジュール**と**リンク方法を**設定します。詳細については、*「」をアーミングスケジュールの設定*と*リンク方法*参照してください。

5. **保存**をクリックします。

5.1.2 FTPを設定します。

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

開始前に

まず、FTPサーバーのアドレスを取得してください。

手順

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

FTP プロトコル

FTP および SFTP を選択できます。ファイルのアップロードは、SFTP プロトコルを使用して暗号化されます。

サーバー IP アドレスとポート番号

FTP サーバーのアドレスと対応するポート番号。

ユーザー名とパスワード

FTPユーザーは画像のアップロード権限が必要です。

FTPサーバーが匿名ユーザーによる画像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「**匿名ログイン**」にチェックを付けることができます。

注意

SFTP プロトコルを選択した場合、匿名ログインはサポートされません。

ディレクトリ構造

FTPサーバー内のスナップショットの保存パス。

3. **オプション：[画像をアップロード]** をチェックすると、FTP サーバーにスナップショットをアップロードできるようになります。

画像保存間隔

画像管理を効率化するため、画像の保存間隔を1日から30日まで設定できます。同じ保存間隔でキャプチャされた画像は、保存間隔の開始日と終了日を名前としたフォルダーに保存されます。

画像名

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

4. **オプション：「自動ネットワーク補充を有効にする」**にチェックを入れます。

注意

リンク方法で「FTP/メモリカード/NAS にアップロード」と**「自動ネットワーク補充」**が同時に有効になっている必要があります。

5. **テスト**をクリックしてFTPサーバーを確認してください。
6. **「保存」**をクリックします。

5.1.3 NASを設定

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

開始前に

まず、ネットワークディスクの IP アドレスを取得します。

手順

1. NAS の設定ページに移動します。**→ Storage→ Storage Management→ Net HDD** .
2. **「追加」**をクリックします。
3. **マウントタイプ**を設定し
   ます。**マウントタイプ**
   オペレーティングシステムに応じて、ファイルシステムプロトコルを選択します。
   SMB/CIFS を選択した場合は、セキュリティを確保するために、ネット HDD のユーザー名とパスワードを入力してください。
4. ディスクの**サーバーアドレス**と**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パス。
5. **テスト**をクリックして、ネットワークディスクが使用可能かどうかを確認します。
6. **[OK]** をクリックして、Net HDD の追加手順を完了します。
7. **オプション：**Net HDD を設定します。
   編集　「」をクリックしてパラメーター設定を編集します。
   削除　ネット HDD を削除します。
   - をクリックします。
   - ネット HDD を選択し、**削除**をクリックします。
8. **保存**をクリックします。

5.1.4 eMMC 保護

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

注意

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

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

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

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

5.1.5 クラウドストレージの設定

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

手順

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

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

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

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

5.2 ビデオ録画

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

5.2.1 自動録画

この機能では、設定した期間にビデオを自動的に録画することができます。

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

手順

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

注意

記録タイプはモデルによって異なります。

連続

スケジュールに従ってビデオが連続的に録画されます。

モーション

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

アラーム

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

モーション| アラーム

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

モーション＆アラーム

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

イベント

設定されたイベントが検出されると、ビデオが録画されます。

4. 選択した記録タイプのスケジュールを設定します。設定操作については*「アラームスケジュール設定」*を参照してください。
5. 高度な録画パラメーターを設定します。

上書き

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

事前録画

スケジュールされた時間前に録画を開始する時間範囲を設定します。

後録画

スケジュールされた時間後に録画を停止する時間期間を設定します。

ストリームタイプ

録画するストリームの種類を選択します。

注

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

録画の有効期限

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

6. **保存**をクリックしてください。

5.2.2 手動で記録

手順

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

次にやるべきこと

録画したビデオファイルを表示します。
[Configuration] (設定) > **[→] (ビデオ設定)** > **[Local] (ローカル)** に移動し、**[Video Saving Path] (ビデオの保存パス)** の横にある **[Open] (開く)** をクリックして保存パスを開き、ファイル

5.2.3 ビデオの再生とダウンロード

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

手順

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

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

注意

[設定] の **[→] [ローカル] [→] [クリップ保存パス]** に移動し、クリップしたビデオファイルの保存パスを表示および変更します。

5. オプション： 再生インターフェースで、ファイルをダウンロードします。

注意

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

5.3 キャプチャ設定

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

5.3.1 自動キャプチャ

この機能は、設定された時間間隔で自動的に画像をキャプチャします。

開始前に

イベント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リンク方法を設定する必要があります。イベントの設定については、「*イベントとアラーム*」を参照してください。

手順

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

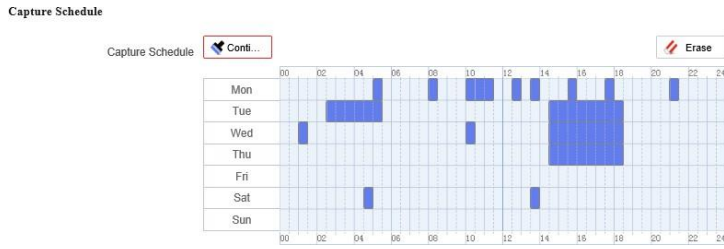


図5-1 キャプチャスケジュールの設定

3. キャプチャの種類を設定します。

   スケジュール

   設定された時間間隔で画像をキャプチャします。

   イベント

   イベントがトリガーされたときに画像をキャプチャします。

4. **フォーマット**、**解像度**、**品質**、**間隔**、および**キャプチャ数を**設定します。

   注意

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

5. **保存**をクリックします。

5.3.2 手動でキャプチャ

手順

1. **設定→ ローカル**に移動します。

2. **画像形式**と保存先をスナップショット用に設定します。

JPEG

この形式の画像サイズは比較的小さく、ネットワークでの送信に適しています。

BMP

画像は高品質で圧縮されます。

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

5.3.3 画像の表示とダウンロード

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

手順

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

一致した画像がファイル一覧に表示されます。

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

注意

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

第 6 章 イベントとアラーム

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

6.1 動体検知の設定

検出領域内の移動物体を検出し、リンク動作をトリガするのに役立ちます。

手順

1. **設定→ イベント→ イベントと検知→ 動体検知** .

2. **「有効」**にチェック**を入れます**。

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

1) **「モーション用の動的分析を有効にする」**にチェックを入れます。

2) **[設定]** の **[→] [ローカル]** に移動します。

3) **ルールを有効**に設定します。

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

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

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

6. **保存**をクリックします。

6.1.1 エキスパートモード

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

手順

1. **設定で「エキスパートモード」**を選択します。

2. エキスパートモードのパラメーターを設定します。

スケジュール画像設定 OFF

画像切り替えは無効になります。

自動切り替え

環境に応じて、デイ＆ナイト機能を自動切替します。昼間はカラー画像、夜間は白黒画像で表示します。

スケジュール切り替え

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

感度

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

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

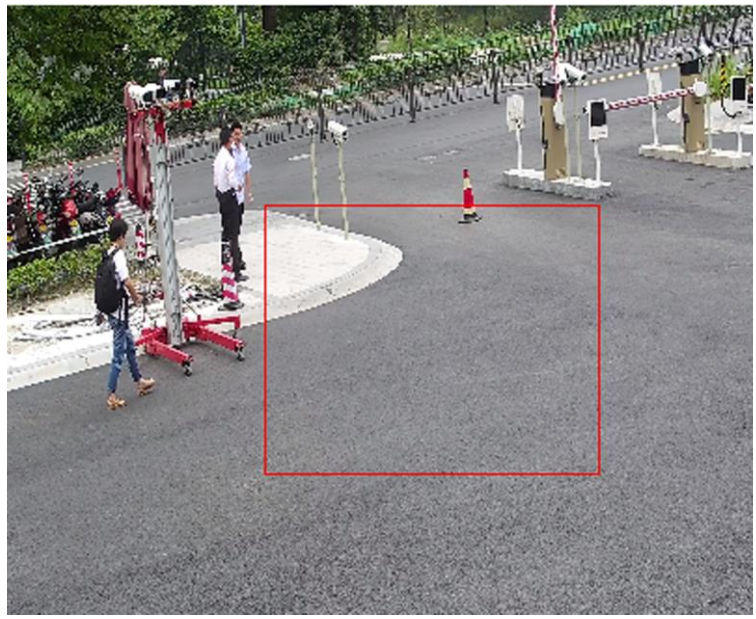


図6-1 ルール設定

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

6.1.2 通常モード

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

手順

1. **設定で「通常モード」**を選択します。
2. 通常モードの**感度**を設定します。感度の値が高いほど、動体検知の感度が高くなります。感度を ***0*** に設定すると、動体検知および動的分析は有効になりません。
3. をクリックします。ライブ画像上でマウスをクリックしてドラッグし、マウスを右クリックして 1 つの領域の描画を終了します。
4. **オプション：**[ ] をクリックして、すべての領域をクリアします。
5. **オプション：**上記の手順を繰り返して、複数のエリアのパラメータを設定することができます。

6.2 ビデオ改ざんアラームの設定

設定したエリアが覆われ、正常に監視できなくなった場合、アラームが作動し、デバイスは特定のアラーム対応措置を実行します。

手順

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

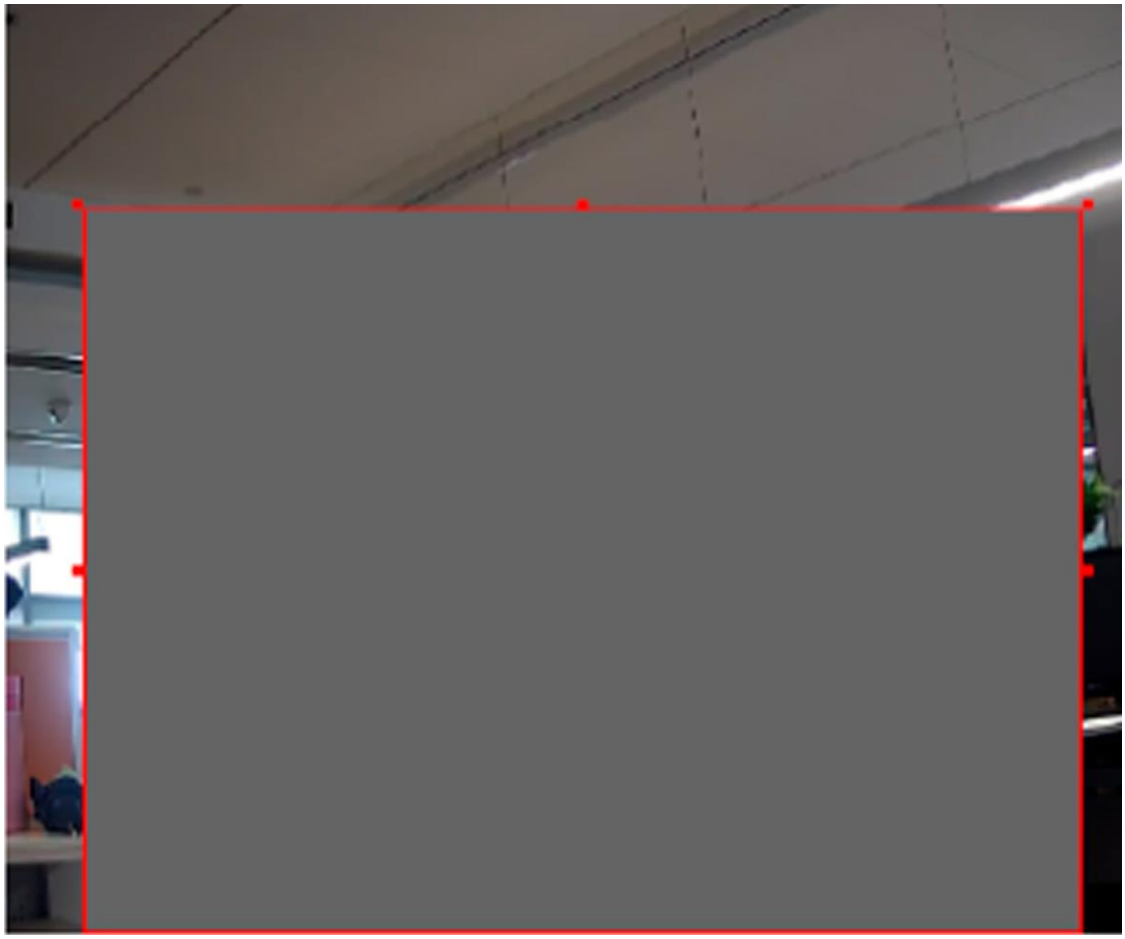


図 6-2 ビデオ改ざん領域の設定

5. **オプション：** をクリックすると、描画した領域をすべて削除できます。
6. ***スケジュールアラーム設定***設定については、「」を参照してください。***リンク方法「」***の設定については、リンク方法の設定を参照してください。
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アラーム信号により、現在のデバイスの対応する動作がトリガーされます。

開始前に

注意
この機能は、一部のモデルでのみサポートされています。

外部アラーム装置が接続されていることを確認してください。ケーブルの接続については、*クイックスタートガイド*をご覧ください。

手順

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

6.4 例外アラームの設定

ネットワーク切断などの例外が発生すると、デバイスは対応するアクションを実行します。

手順

1. **設定→ イベント→ イベントと検出→ 例外**を選択します。
2. **例外の種類**を選択します。

HDD 満杯

HDDのストレージが満杯です。

HDDエラー

HDD でエラーが発生しています。

ネットワークが切断されています

デバイスがオフラインです。

IP アドレスの衝突

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

不正なログイン

ユーザー名またはパスワードが正しくないため、ログインできません。

異常な再起動

デバイスが異常な再起動を行います。

3. リンク方法の設定については、「リンク方法*の設定」*を参照してください。

4. **保存**をクリックしてください。

6.5 ビデオ画質診断の設定

デバイスのビデオ品質が異常で、アラームのリンクが設定されている場合、アラームが自動的に作動します。

手順

1. **設定」**に移動します**。→ イベント→ イベントと検出→ ビデオ品質診断**。

2. **診断タイプ**を選択します。

3. 対応するパラメーターを設定します。

アラーム検出間隔

例外を検出する時間間隔。

感度

値が高いほど、例外が検出されやすくなり、誤った情報が伝達される可能性が高まります。

アラーム遅延時間

アラームが設定回数に達すると、デバイスはアラームをアップロードします。

4. 選択した診断タイプを確認し、関連するタイプが検出されます。

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

6. リンク方法を設定します。*リンク方法の設定*を参照してください。

7. **保存**をクリックしてください。

注意

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

6.6 振動検出の設定

デバイスが振動しているかどうかを検出するために使用します。この機能を有効にすると、デバイスはアラームを報告し、リンク動作をトリガーします。

手順

1. **設定」**に移動し、**「→」を選択します。「→」を選択し、「Event」を選択します。「→」を選択し、「Vibration Detection」**を選択します。

2. **「有効」**にチェック**を入れます**。

3. スライダーをドラッグして検出感度を設定します。数値を入力して感度を設定することもできます。

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

5. リンク方法を設定します。*リンク方法の設定*を参照してください。

6. **保存**をクリックします。

注意

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

6.7 オーディオ例外検出を設定する

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

手順

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

   オーディオ損失検出

   オーディオトラックの突然の損失を検出します。

   音量急上昇検出

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

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

   音圧の急激な低下検出

   音圧の急激な低下を検出します。**感度は**設定可能です。
3. ***スケジュールスケジュール設定***設定は「アラーム」を参照してください。リンク方法の設定は ***「リンク方法設定」***を参照してください。
4. **保存**をクリックします。

注意

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

6.8 ボケ検出の設定

レンズのピントが合っていないためにぼやけた画像を検出することができます。この機能を使用すると、デバイスはリンク動作を実行することができます。

手順

1. **設定**に移動し、**→イベント→イベントと検出→ ピント外れ検出を選択します**。
2. **「有効」**にチェック**を入れます**。
3. **感度**を設定します。値が高いほど、ピントがずれた画像でアラームが鳴りやすくなります。実際の環境に合わせて値を調整してください。
4. リンク方法の設定については、「*リンク方法の設定」*を参照してください。
5. **保存**をクリックします。

注意

この機能は一部のモデルでのみ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。

6.9 シーン変更検知の設定

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

手順

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

注意

この機能は一部のモデルでのみ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。

第 7 章 警報スケジュールとアラームのリンク

アラームリンクは、指定した時間内に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。アラームリンクは、指定した時間内に特定のインシデントやターゲットが検出された場合の対応です。

7.1 武装スケジュールを設定する

デバイスタスクの有効時間を設定します。

手順

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

注意

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

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

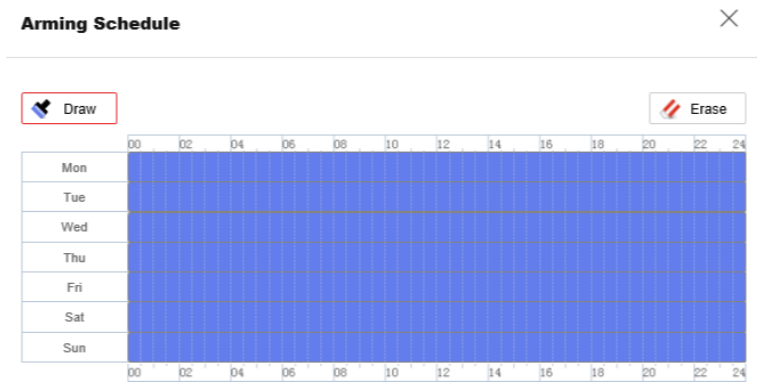


図7-1 アーミングスケジュール設定

7.2 リンク方法の設定

イベントまたはアラームが発生したときに、リンク機能を有効にすることができます。

7.2.1 アラーム出力のトリガー

デバイスがアラーム出力デバイスに接続されており、アラーム出力 No. が設定されている場合、アラームが作動すると、デバイスは接続されたアラーム出力デバイスにアラーム情報を送信します。

手順

1. 設定→ イベント→ アラーム設定→ アラーム出力 .

2. アラーム出力パラメータを設定します。

自動アラーム 設定については、*「自動アラーム」*を参照してください。

手動アラーム 設定については、「*手動アラーム」*を参照してください。

手動アラーム

アラーム出力を手動でトリガーすることができます。

開始前に

アラーム出力デバイスがデバイスに接続されていることを確認してください。

手順

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

アラーム名

アラーム出力の名前をカスタマイズします。

2. 手動アラームをクリックして、手動アラーム出力を有効にします。

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

自動アラーム

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

開始前に

アラーム出力デバイスがデバイスに接続されていることを確認してください。

手順

1. 外部アラーム装置に接続されているアラームインターフェースに応じて、**アラーム出力番号**を選択します。 をクリックして、アラームパラメータを設定します。

アラーム名

アラーム出力の名前をカスタマイズします。

遅延

アラームが発生してからアラーム出力が続く時間です。

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

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

4.「保存」をクリックします。

7.2.2 FTP/NAS/メモリカードへのアップロード

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

FTP サーバーの設定は「FTP の設定」を参照してくださ
い。*NAS 設定*のは「NAS の設定」を参照してください。

メモリカードの保存設定は「*新しいまたは暗号化されていないの設定*メモリカード」を参照してください。

7.2.3 メール送信

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

メール設定については、*「メール設定」*を参照してください。

メールの設定

メールが設定され、リンク方法として**「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、指定した宛先にすべてメール通知が送信されます。

開始前に

E メール機能を使用する前に、DNS サーバーを設定してください。**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. メールパラメーターを設定します。

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

2) **オプション：** メールサーバーが認証を必要とする場合は、**[認証]** をチェックし、サーバーにログインするためのユーザー名とパスワードを入力します。

3) **メールの暗号化**を設定します。

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

注意

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

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

注意

アラーム画像の数は、デバイスの機種やイベントによって異なります。

5) 受取人の情報（受取人の名前と住所を含む）を入力してください。

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

3. **「保存」**をクリックしてください。

7.2.4 監視センターに通知

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

7.2.5 トリガー録画

録画のトリガー] をチェックすると、デバイスは、検出されたアラームイベントに関するビデオを録画します。録画の設定については、*「ビデオ録画と画像キャプチャ」*を参照してください。

7.2.6 音声警告

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

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

注意

この機能は、一部のカメラモデルでのみサポートされています。

可聴アラーム出力の設定

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

手順

1. **設定→ イベント→ アラーム設定→ 可聴アラーム出力** .

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

注

この機能は、特定のデバイスモデルでのみサポートされています。

7.2.7 アラームサーバー

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

アラームサーバーの設定

手順

1. **設定→ 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**、および**ポート**を入力します。
3. **プロトコル**を選択します。

注意

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

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

第 8 章 ネットワーク設定

8.1 TCP/IP

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

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

NIC タイプ

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

IPv4

IPv4には2つのモードが利用可能です。

DHCP

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

注意

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

手動

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

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

IPv6

3つのIPv6モードが利用可能です。

ルート広告

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

注

ルート広告モードは、デバイスが接続されているルーターのサポートが必要です。

DHCP

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

手動

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

MTU

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

MTUの有効な値の範囲は1280から1500です。

DNS

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

ドメイン名設定

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

注意

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

8.2 ドメイン名経由でのデバイスへのアクセス

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

開始前に

デバイスのDDNS設定を構成する前に、DDNSサーバーへの登録が必要です。

手順

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

   ダイナミック DNS サーバーは、ドメイン名の解決に使用されます。

   NO-IP

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

   ブラウザから　　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によるアクセス　　クライアントソフトウェアにドメイン名を追加してください。具体的な追加方法は、クライアントのマニュアルを参照してください。

8.3 PPPoE ダイヤルアップ接続によるデバイスへのアクセス

本機は、PPPoE 自動ダイヤルアップ機能に対応しています。本機は、モデムに接続すると、ADSL ダイヤルアップにより公衆 IP アドレスを取得します。本機の PPPoE パラメータを設定する必要があります。

手順

1. [**Configuration**]、**[→]**、**[Network]**、**[→]**、**[Network Settings]**、**[→]**、**[PPPoE]** の順に選択します。
2. **「有効」**にチェックを入れます。
3. PPPoE パラメーターを設定します。

   動的IP

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

   ユーザー名

   ダイヤルアップネットワークアクセス用のユーザー名。

   パスワード

   ダイヤルアップネットワークアクセス用のパスワード。

   確認

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

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

   クライアントソフトウェアによる設定 クライアントソフトウェアに WAN の動的 IP アドレスを追加してください。詳細については、クライアントのマニュアルを参照してください。

注

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

8.4 SNMP

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

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

手順

1. [**Configuration**]、**[→]**、**[Network]**、**[→]**、**[Network Settings]**、**[→]**、**[SNMP]** の順に選択します。
2. **SNMPv1 を有効にする**、**SNMP v2c を有効にする**、または **SNMPv3 を有効にする**を選択します。

注

選択するSNMPバージョンは、SNMPソフトウェアのバージョンと一致する必要があります。
また、必要なセキュリティレベルに応じて、異なるバージョンを使用する必要があります。SNMP v1 は安全ではなく、SNMP v2 ではアクセスにパスワードが必要です。SNMP v3 は暗号化機能を備えており、このバージョンを使用する場合は、HTTPS プロトコルを有効にする必要があります。

3. SNMP設定を構成します。
4. **保存**をクリックします。

8.5 IEEE 802.1X を設定する

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

設定→ ネットワーク→ ネットワーク設定→ 802.1X を選択し、機能を有効にします。
ルーターの情報に応じて、プロトコルとバージョンを選択します。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** に設定する場合は、**クライアント**証明書と **CA 証明書**を選択してください。
- 機能が正常でない場合、**証明書管理**で選択された証明書が正常でないかどうかを確認してください。

8.6 QoSを設定する

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

注意

QoS は、ルーターやスイッチなどのネットワーク機器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**、および**管理 DSCP** を設定します。

注意

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

3. **保存**をクリックします。

8.7 HTTP(S)

HTTP は、ハイパーメディア文書を伝送するためのアプリケーション層プロトコルです。HTTPS は、暗号化伝送と ID 認証を可能にするネットワークプロトコルであり、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

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

HTTP ポートが 81 に変更されました。ログインするには、ブラウザに http://192.168.1.64:81 と入力してください。

3. **HTTPS** の「**有効**」にチェックを入れてください。

注意

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

4. **HTTPS ポート**を入力してください。
5. **オプション：**HTTPS プロトコル経由でのみデバイスにアクセスするには、[HTTPS **ブラウジング]** をチェックします。
6. **サーバー証明書**を選択します。
7. **Web 認証**を設定します。**認証**

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

Digest アルゴリズム

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

8. **保存**をクリックします。

8.8 マルチキャスト

マルチキャストは、データ送信を複数の宛先デバイスに同時に送信するグループ通信です。

マルチキャストの設定は、[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] で行います。

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 に移動して、この機能を有効にします。

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

8.9 RTSP

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

手順

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

   ストリームタイプ

   マルチキャストソースとしてのストリームタイプ。

   ビデオポート

   選択したストリームのビデオポート。

   オーディオポート

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

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

   ダイジェストアルゴリズム

   MD5、SHA256、およびMD5/SHA256暗号化アルゴリズムがRTSP認証で使用されています。MD5以外のダイジェストアルゴリズムを有効にすると、サードパーティプラットフォームがデバイスにログインできなくなる可能性があります。

デバイスにログインしたり、ライブビューを有効にしたりできなくなる可能性があります。互換性の問題のためです。高強度の暗号化アルゴリズムの使用が推奨されます。

5. **保存**をクリックします。

8.10 SRTPを設定

Secure Real-time Transport Protocol (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、整合性、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. [**Configuration**]、**[→]**、**[Network]**、**[→]**、**[Network Service]**、**[→]**、**[SRTP]** の順に選択します。

2. **ポート**番号を入力します。

3. **マルチキャスト**パラメーターを設定します。

ストリームタイプ

マルチキャストソースとしてのストリームタイプ。

ビデオポート

選択したストリームのビデオポート。

オーディオポート

選択したストリームのオーディオポート。

4. **サーバー証明書**を選択します。

5. **暗号化アルゴリズム**を選択してください。

6. **保存**をクリックします。

注

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

8.11 Bonjour

これは、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を含む、ゼロ設定ネットワーク (zeroconf) の実装です。Bonjour は、マルチキャストドメインネームシステム (mDNS) サービスレコードを使用して、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 を選択して機能を有効にし、[保存] をクリックします。

保存をクリックします。

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

8.12 WebSocket(s)

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

[Configuration]、**[→]**、**[Network]**、**[→]**、**[Network Service]**、**[→]**、**[WebSocket(s)]** の順に選択してパラメータを設定し、[Save] をクリックします。

保存をクリックします。

WebSocket

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

WebSockets

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

8.13 ポートマッピング

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

手順

1. **設定→ ネットワーク→ ネットワークサービス→ NAT** を選択します。
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　詳細な情報は「*自動ポートマッピングの設定*」を参照してください。

   手動ポートマッピング　詳細については、「*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]** をチェックし、カメラにわかりやすい名前を選択します。または、デフォルトの名前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。

注意

ルーターのUPnP™機能も同時に有効にしておく必要があります。

8.13.2 手動ポートマッピングを設定

手順

1. **UPnP™ を有効にします**。デバイスにわかりやすい名前を付けます。または、デフォルトの名前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「**手動**」に設定し、外部ポートを内部ポートと同じに設定します。
3. 「**保存**」をクリックします。

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

8.13.3 ルーターでポートマッピングを設定する

以下の設定は特定のルーター用です。ルーターのモデルによって設定が異なります。

手順

1. **WAN接続タイプ**を選択します。
2. ルーターの **IP アドレス**、**サブネットマスク**、その他のネットワークパラメータを設定します。
3. Go to **Forwarding→ Virtual Severs**、**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
カメラが同じルーターに接続されている場合、あるカメラのポートを IP アドレス 192.168.1.23、ポート番号 80、8000、554 に設定し、別のカメラのポートを IP アドレス 192.168.1.23、ポート番号 81、8001、555 に設定することができます。
8201に設定できます。

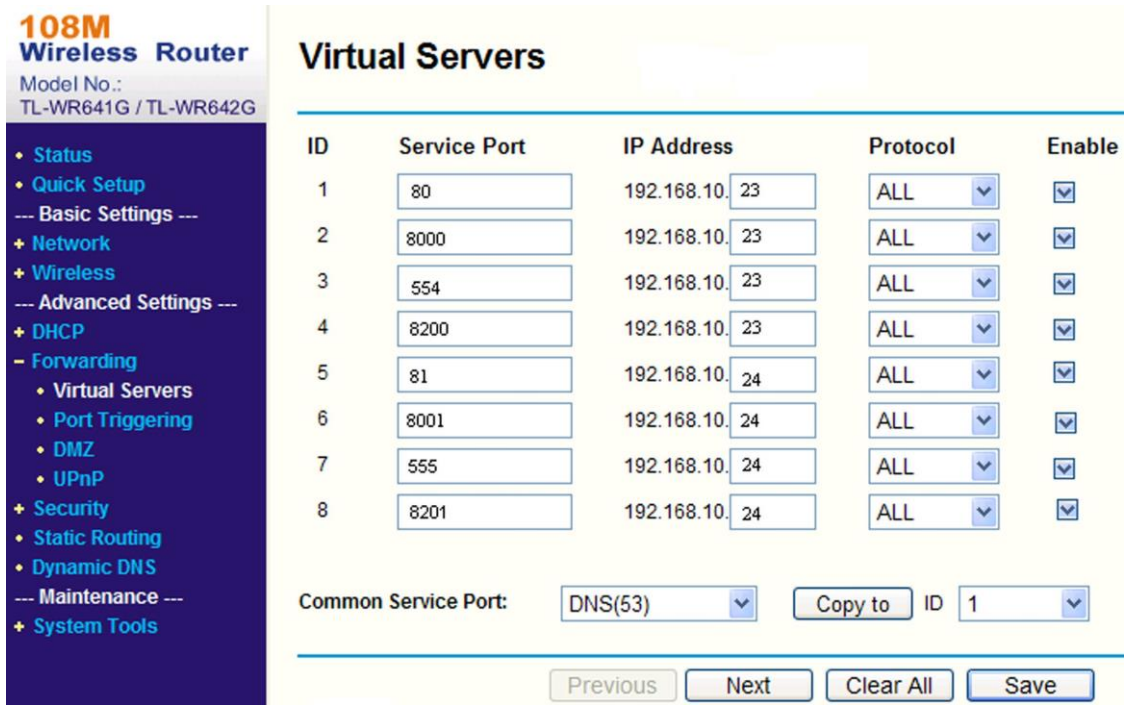


図8-1 ルーターでのポートマッピング

注意

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

8.14 SIP

SIP（Session Initiation Protocol）は、音声、ビデオ、メッセージングアプリケーションを含むリアルタイムセッションの開始、維持、終了に使用されるシグナリングプロトコルです。

この機能を有効にし、パラメーターを設定します。設定を保存し、SIPサーバーにデバイスを登録するには**「保存」**をクリックします。ウィンドウを再読み込みし、デバイスが登録されているかどうかを確認してください。

8.15 ISUPを設定してください。

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を介してデバイスにアクセスして管理したり、データを送信したり、アラーム情報を転送したりすることができます。

手順

1. **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」**にチェック**を入れます**。
4. プロトコルバージョンを選択し、関連するパラメータを入力します。
5. **保存**をクリックします。
   機能が正しく設定されると、登録状態が「**オンライン**」に変わります。

8.16 Hik-Connect 経由でカメラにアクセスする

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

開始前に

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. 以下の方法のいずれかでHik-Connectアプリケーションをダウンロードしてインストールしてください。
   - ***https://appstore.hikvision.com*** にアクセスし、お使いのモバイル端末のシステムに対応したアプリケーションをダウンロードしてください。
   - 弊社の公式ウェブサイトにアクセスしてください。次に、**[サポート]、[→]、[ツール]、[→]、[Hikvision App Store]** の順に選択してください。
   - 以下のQRコードをスキャンしてアプリケーションをダウンロードしてください。

注意

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

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

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

   詳細な情報は、Hik-Connect アプリのユーザーマニュアルをご参照ください。

8.16.1 カメラで Hik-Connect サービスを有効にする

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

ウェブブラウザーで Hik-Connect サービスを有効にする

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

開始前に

サービス有効化前に、カメラをアクティブ化する必要があります。

手順

1. ウェブブラウザーからカメラにアクセスします。
2. プラットフォームアクセス設定インターフェースに入ります。**設定→ネットワーク→プラットフォームアクセス → Hik-Connect**。
3. **「有効」にチェックを入れます**。
4. ポップアップウィンドウで「利用規約」および「プライバシーポリシー」をクリックして読みます。
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。

注意

カメラを Hik-Connect サービスに追加する際に、確認コードが必要になります。

6. 設定を保存してください。

SADP ソフトウェア経由で Hik-Connect サービスを有効化してください。

このパートでは、有効化されたカメラの SADP ソフトウェアを介して Hik-Connect サービスを有効にする方法について説明します。

手順

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

注意

カメラを Hik-Connect サービスに追加する際に、確認コードが必要になります。

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、同意してください。
6. 設定を確認してください。

8.16.2 Hik-Connect の設定

手順

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

注意

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

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

2. アプリケーションを起動し、Hik-Connectユーザーアカウントに登録してください。

3. 登録後、ログインしてください。

8.16.3 Hik-Connect にカメラを追加する

手順

1. モバイルデバイスをWi-Fiに接続します。

2. Hik-Connect アプリにログインします。

3. ホーム画面で、右上隅の「+」をタップしてカメラを追加します。

4. カメラ本体または *クイックスタートガイド*の表紙にある QR コードをスキャンします。

注意

QR コードがない、または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カメラを追加することもできます。

5. カメラの認証コードを入力してください。

注意

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

6. ポップアップインターフェースの「**ネットワークに接続**」ボタンをタップします。

7. カメラの機能に応じて、「**有線接続**」または「**無線接続**」を選択してください。

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

注意

ルーターは、スマートフォンが接続している同じルーターである必要があります。

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

8.17 オープンネットワークビデオインターフェースを設定する

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

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**」にチェックを入れます。

3. 認証モードを選択します。
   - **ダイジェスト**を選択した場合、デバイスはダイジェスト認証のみをサポートします。
   - 「**Digest&ws-username token**」を選択した場合、デバイスはダイジェスト認証またはws-username token認証をサポートします。
4. **[追加]** をクリックして、オープンネットワークビデオインターフェースユーザーを設定します。
5. **「保存」**をクリックします。
6. **オプション：**上記の手順を繰り返して、オープンネットワークビデオインターフェースユーザーを追加します。
7. **オプション：**ユーザーを管理します。
   - （削除）をクリックして、選択したオープンネットワークビデオインターフェースユーザーを削除します。
   - （オープンネットワークビデオインターフェースを編集）をクリックして、選択したオープンネットワークビデオインターフェースユーザーを変更します。

8.18 SDK サービスを設定します。

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

手順

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

第 9 章 システムとセキュリティ

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

9.1 システム設定

9.1.1 デバイス情報の表示

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

設定を開く→ **システム→ システム設定→ 基本情報** でデバイス情報を表示します。

9.1.2 日時

デバイスの時刻と日付を設定するには、タイムゾーン、時刻同期、および夏時間（DST）を設定します。

手動で時間を同期する

手順

1. [**Configuration]** (設定)→ **[System] (システム)→ [System Settings] (システム設定)→ [Time Settings]** (時刻**設定)** を選択します。
2. **タイムゾーン**を選択します。
3. **手動時刻同期**を選択します。
4. 時間同期の方法を選択します。
   - **[時刻を設定]** を選択し、手動で日付と時刻を入力するか、ポップアップカレンダーから選択します。
   - **「コンピュータと同期」**をクリックして、デバイスの時間をローカルPCの時間と同期します。
5. **「保存」**をクリックします。

NTP サーバーを設定

正確で信頼性の高い時刻ソースが必要な場合、NTP サーバーを使用できます。

開始前に

NTP サーバーを設定するか、NTP サーバーの情報を入手してください。

手順

1. Go to **Configuration→ System→ System Settings→ Time Settings** .
2. **タイムゾーン**を選択します。

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

注意

サーバーアドレスはNTPサーバーのIPアドレスです。

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

衛星による時刻同期

注意

この機能はデバイスによって異なります。

手順

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

DSTを設定

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

手順

1. [**Configuration**] (**構成**) [**→**] (**システム**) [**→**] (**システム設定**) [**→**] (**時間設定**) [Enable] (有効) [
2. **「有効」**にチェック**を入れます**。
3. **開始時間**、**終了時間**、**およびDSTバイアス**を選択します。
4. **保存**をクリックします。

9.1.3 RS-232を設定します。

RS-232はデバイスのデバッグや周辺機器へのアクセスに使用できます。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ターミナル間の通信を実現できます。

開始前に

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

手順

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

9.1.4 RS-485を設定します。

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

開始前に

デバイスとコンピュータまたはターミナルをRS-485ケーブルで接続します。

手順

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

注意

デバイスとコンピュータまたは端末のすべての設定を同じに保つ必要があります。

3. **保存**をクリックしてください。

9.1.5 ライブビュー接続を設定

リモートライブビュー接続の最大数を制御します。

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

設定→ システム→ システム設定→ システムサービスを選択し、リモート接続数の上限を設定します。

9.1.6 場所設定

位置情報を表示し、デバイスの現在の経度と緯度をアップロードします。

自動アップロード

「有効」にチェックを入れ、**位置情報アップロード間隔**を設定します。

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

手動設定

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

デバイスは設定された間隔で設定された位置情報を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 オープンソースソフトウェアのライセンスを表示

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

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

注意

ネットワーク上で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. **[Configuration] (構成)** に移動し、**[→] (リモートアクセス) を選択します。→(リモートアクセス) を選択し、[→] (ユーザー管理) を選択**
2. **[追加]** をクリックします。**ユーザー名**を入力し、**レベル**を選択して、**パスワード**を入力します。必要に応じて、ユーザーにリモートアクセス権限を割り当てます。

   管理者

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

   ユーザー

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

   オペレーター

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

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

   削除　ユーザーを選択し、[🗑] をクリックします。

   注意

   管理者は、最大 31 個のユーザーアカウントを追加できます。
3. **OK**をクリックします。

9.2.2 同時ログイン

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

Go to **Configuration→ System→ User Management→ Online Users**、**General** をクリックし、同時ログインを 31 に設定します。
同時ログインを設定します。

9.2.3 オンラインユーザー

デバイスにログインしたユーザーの情報を表示します。

[Configuration] (設定) **[→] (システム) [→] (ユーザー管理) [→] (オンラインユーザー)** に移動して、オンラインユーザーのリストを表示します。

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]、**[→]**、**[→]**、**[Restart]** の順に選択し、**[Restart]** 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取得する必要があります。

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

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

   ファームウェア　　アップグレードファイルの正確なパスを特定します。

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

9.3.3 復元とデフォルト

復元とデフォルトは、デバイスのパラメーターをデフォルト設定に復元します。

手順

1. **→[メンテナンスとセキュリティ]、[→ のメンテナンス]、[バックアップと復元]** の順に選択します。

2. 必要に応じて**「復元」**または**「デフォルト」**をクリックします。

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

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

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

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ことができます。

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]** に移動します。**→ [メンテナンス] を選択します。→ [バックアップと復元] を選択します。→ [バックアップ]** を選択します。

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) 設定ファイルをローカルコンピュータに保存する保存先パスを設定します。

2. 設定ファイルをインポートします。

1) ウェブブラウザーから、設定が必要なデバイスにアクセスします。

2) **[メンテナンスとセキュリティ]、[→]、[→]、[バックアップと復元]、[→]、[リセット]** の順に選択します。

3) 「」をクリックして、保存した設定ファイルを選択します。

4) 設定ファイルをエクスポートする際に設定した暗号化パスワードを入力してください。

5) **インポート**をクリックしてください。

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]、[→]、[→]、[Log]** の順に選択します。

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

3. **検索**をクリックします。

一致したログファイルがログ一覧に表示されます。

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

9.3.6 セキュリティ監査ログの検索

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

手順

注意
この機能は、一部のカメラモデルでのみサポートされています。

1. Go to **Maintenance and Security→ → Security Audit Log**.
2. ログの種類、**開始時間**、**終了時間**を選択します。
3. **検索**をクリックします。

   検索条件に一致するログファイルがログ一覧に表示されます。
4. **オプション：[エクスポート]** をクリックして、ログファイルをコンピュータに保存します。

9.3.7 SSH

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

Go to **Maintenance and Security→ Maintenance→ Device Debugging** , and click **Settings** of **SSH**.ポートの番号を編集することができます。**Save** をクリックします。

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

9.3.8 診断情報のエクスポート

診断情報には、実行ログ、システム情報、ハードウェア情報が含まれます。

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

9.4 セキュリティ

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

9.4.1 IP アドレス フィルターを設定する

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

IPアドレスはIPv4を指します。

手順

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

2. 「**有効**」にチェック**を入れます**。

3. IP アドレス フィルターの種類を選択します。

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

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

4. IPアドレスフィルターリストを編集します。

追加　リストに新しいIPアドレスまたはIPアドレス範囲を追加します。

 　リスト内の選択したIPアドレスまたはIPアドレス範囲を編集します。

 　リストから選択したIPアドレスまたはIPアドレス範囲を削除します。

5. **保存**をクリックします。

9.4.2 MACアドレスフィルターを設定する

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

手順

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

2. 「**有効**」にチェック**を入れます**。

3. MACアドレスフィルターの種類を選択します。

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

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

4. MACアドレスフィルターリストを編集します。

追加　リストに新しいMACアドレスを追加します。

 　リスト内の選択したMACアドレスを編集します。

 　リスト内の選択したMACアドレスを削除します。

5. **保存**をクリックします。

9.4.3 タイムアウト設定の制御

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

Go to **Maintenance and Security→ Security→ Login Management→ Control Timeout** Settingsで設定を完了します。

9.4.4 証明書管理

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

注意

この機能は、特定のデバイスモデルでのみサポートされています。

サーバー証明書/クライアント証明書

注

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

自己署名証明書を作成してインストールする

手順

1. [**メンテナンスとセキュリティ**]、**[→]**、**[セキュリティ]**、**[→]**、**[Certificate Management]** の順に選択します。
2. **「自己署名証明書を作成」**をクリックします。
3. 証明書情報を入力します。

   注

   入力する証明書 ID は既存のものと同一にできません。
4. **「保存」**をクリックして証明書を保存し、インストールします。
   作成した証明書が、**サーバー/クライアント**証明書リストに表示されます。

   証明書が特定の機能で使用されている場合、その機能名は列
   「機能」列に表示されます。
5. **オプション：[プロパティ]** をクリックすると、証明書の詳細を確認できます。

自己署名証明書をインストールする

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

開始する前に

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

手順

1. **[メンテナンスとセキュリティ]、[→ セキュリティ]、[→ 証明書管理]** の順に選択します。
2. **サーバー/クライアント証明書**リストから自己署名証明書を選択します。
3. **「証明書リクエストの作成」**をクリックします。
4. リクエスト情報を入力します。
5. **「保存」**をクリックします。

   証明書要求の詳細がポップアップウィンドウに表示されます。
6. リクエストの内容をコピーし、リクエストファイルとして保存してください。
7. ファイルを信頼できる第三者に送信し、署名を取得します。
8. 第三者から返送された証明書を受け取った後、デバイスにインストールします。
   1) **「インポート」**をクリックします。
   2) **証明書ID**を入力します。

      注意

      入力する証明書IDは、既存のものと同一にしてはいけません。
   3) クリック をクリックして証明書ファイルを選択してください。
   4) **自己署名証明書**を選択します。
   5) **保存**をクリックします。

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

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

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

他の承認済み証明書をインストール

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

手順

1. **[メンテナンスとセキュリティ]、[→]、[セキュリティ]、[→ 証明書管理]** の順に移動します。
2. **サーバー/クライアント**証明書リストで**「インポート」**をクリックします。
3. 入力**証明書ID**。

注意

入力する証明書IDは、既存のものと同一であってはなりません。

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

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

6. **保存**をクリックします。

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

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

機能に表示されます。

CA証明書をインストールする

開始前に

事前にCA証明書を用意してください。

手順

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

注

入力する証明書 ID は、既存の証明書 ID と同一にしてはいけません。

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

インポートされた証明書は**CA証明書**リストに表示されます。

証明書が特定の機能で使用されている場合、その機能名は「**機能**」

列に表示されます。

証明書有効期限アラームを有効にする

手順

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

注意

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

3. **保存**をクリックしてください。

9.4.5 TLS

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

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

保存をクリックします。

注意

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

第10章 VCAリソース

VCAリソースは、デバイスがサポートするスマート機能の集合体です。

10.1 オープンプラットフォームの設定

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

手順

1. **VCA** インターフェースに移動します。

注意

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

- 各アプリケーションには独自の名前が割り当てられています。
- アプリケーションが使用するフラッシュメモリの容量が、デバイスの使用可能なフラッシュメモリの容量以下であること。
- アプリケーションのメモリおよび演算能力は、デバイスの使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、ローカルパスを閲覧してアプリケーションパッケージを選択し、インポートします。

3. **「ライセンスのインポート」**をクリックし、ローカルのパスを閲覧してライセンスファイルを選択し、インポートします。

4. **オプション：**アプリケーションを設定します。

クリック	アプリケーションを有効または無効にします。
クリック	アプリケーションを削除します。
クリック	ログをエクスポートします。
クリック	ローカルパスを選択し、アプリケーションパッケージをインポートしてアプリケーションを更新します。
詳細を表示	アプリケーションを選択し、クリックしてページに詳細を表示します。

10.2 スマートアプリケーション

スマートアプリケーションに関連する一般的なパラメータを設定します。

Go to **VCA→ アプリケーションの→ 全般設定**を設定して、以下のパラメータを設定します。

FTP

FTPの設定については、*「FTPの設定」*を参照してください。

メール

メールの設定については、「*メールの設定」*を参照してください。

アラーム出力

アラーム出力の設定については、「*自動アラーム」*を参照してください。

可聴アラーム出力

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

アラームサーバー

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

10.2.1 カメラ情報の設定

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

VCA に移動**→ アプリケーションの設定→ 全般設定→ デバイス番号**と**カメラ情報を**設定する**カメラ情報**。

10.3 スマートイベント

注意

- この機能は、ソフトウェアデコードモードまたはハードウェアデコードモードのフィッシュアイビュー表示モードでのみサポートされています。
- 一部のデバイスモデルでは、まずVCAページでスマートアプリケーションを有効にする必要があります。アプリケーションを有効にするには、十分な**メモリ**、**RAM**、**およびFLASH**を確保してください。そうでない場合、他のアプリケーションを最初に無効にする必要があります。

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内に侵入したり、その領域内に留まっている物体を検出するために使用されます。検出された場合、デバイスはリンク動作を実行することができます。

開始前に

- **VCA** に移動し、システムに付属のスマートアプリケーションのいずれかを選択します。

手順

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

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

しきい値

しきい値は、その領域にオブジェクトが留まっている時間のしきい値を表します。1 つのオブジェクトの滞留時間がしきい値を超えると、アラームが作動します。しきい値の値が大きいほど、アラームが作動するまでの時間が長くなります。

感度

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

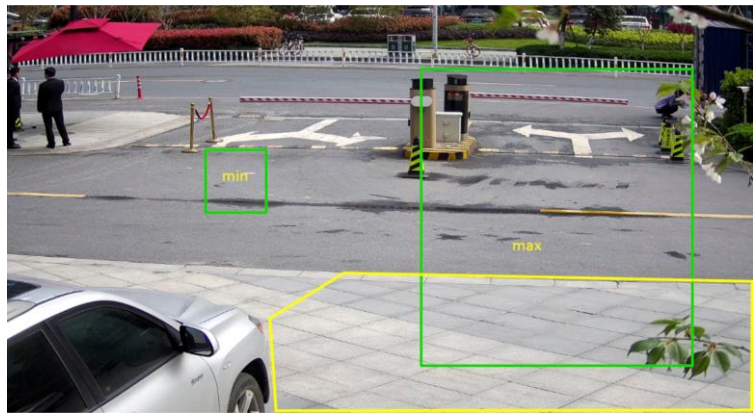


図10-1 ルール設定

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

10.3.2 ラインクロス検出の設定

これは、あらかじめ定義した仮想ラインを横切る物体を検出するために使用します。これが発生すると、デバイスはリンク動作を実行できます。

開始前に

- **VCA** に移動し、システムに付属のスマートアプリケーションのいずれかを選択します。

手順

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

   方向

   これは、オブジェクトがラインを通過する方向を表します。

   A<->B：両方向からラインを通過するオブジェクトが検出され、アラームが作動します。

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

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

   感度

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

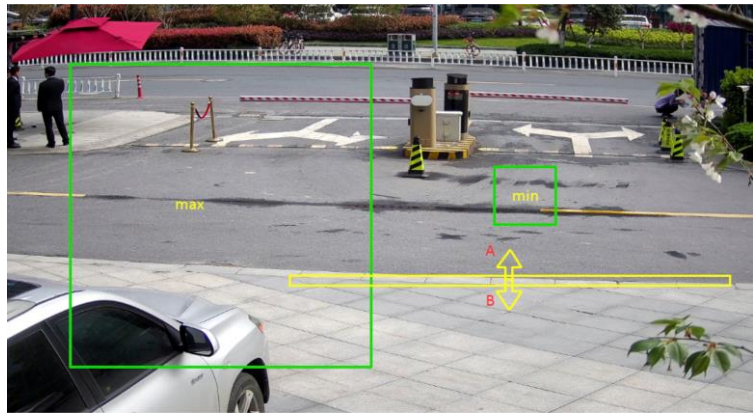


図10-2 ルール設定

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

10.3.3 入口検知の設定

これは、あらかじめ定義した仮想領域に外部から物体が侵入したことを検出するために使用します。侵入が検出されると、デバイスはリンク動作を実行します。

開始前に

- **VCA** に移動し、システムに付属のスマートアプリケーションのいずれかを選択します。

手順

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

   感度

   これは、定義済みの領域を通過する許容ターゲットの身体部分の割合を表します。感度= 100 - S1/ST× 100。S1 は、定義済みの領域を通過するターゲットの身体部分を表します。ST は、ターゲットの身体全体を表します。感度の値が高いほど、アラームが簡単に作動します。

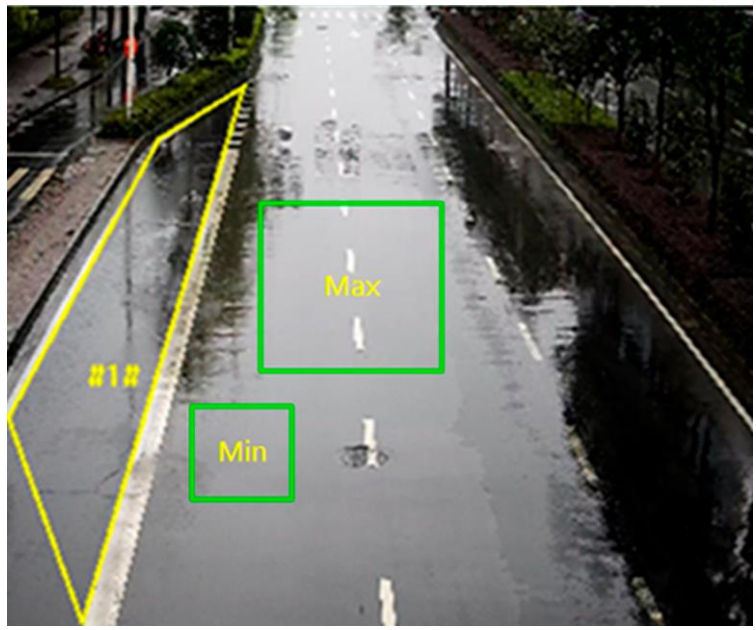


図10-3 ルール設定

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

10.3.4 出口検知

あらかじめ定義した仮想領域から出口を検知します。出口を検知すると、リンク動作を実行します。

開始前に

- **VCA** に移動し、システムに付属のスマートアプリケーションのいずれかを選択します。

手順

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

4. パラメーターを設定します。

感度

これは、定義済みの領域を通過する許容ターゲットの身体部分の割合を表します。感度= 100 - S1/ST× 100。S1 は、定義済みの領域を通過するターゲットの身体部分を意味します。ST は、ターゲットの身体全体を表します。感度の値が高いほど、アラームが簡単に作動します。

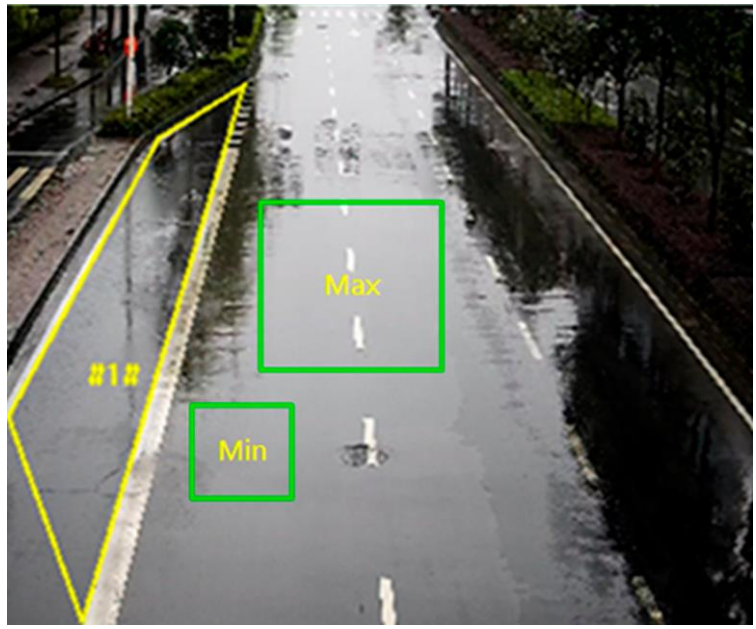


図10-4 ルール設定

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

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

7. **保存**をクリックします。

10.3.5 無人手荷物検出の設定

これは、あらかじめ定義された領域内に残された物体を検出するために使用されます。リンク方法は、物体が領域内に残され、設定された時間経過後にトリガーされます。

開始前に

- **VCA** に移動し、システムに付属のスマートアプリケーションのいずれかを選択します。

手順

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

2. **「有効」**にチェックを入れます。

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

4. パラメーターを設定します。

感度

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

閾値

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

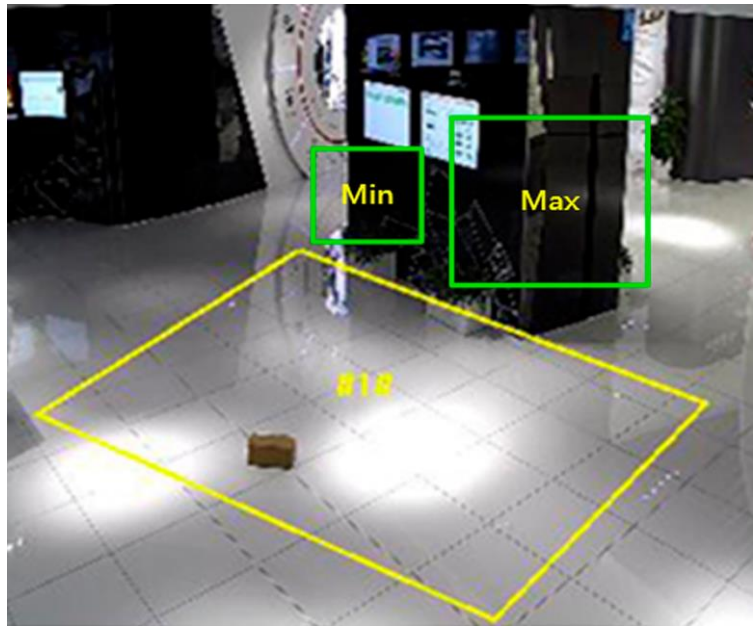


図10-5 ルール設定

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

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

7. 保存をクリックしてください。

注意

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

10.3.6 オブジェクト除去検出の設定

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

開始前に

- **VCA** に移動し、システムに付属のスマートアプリケーションのいずれかを選択します。

手順

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

   感度

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

   閾値

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

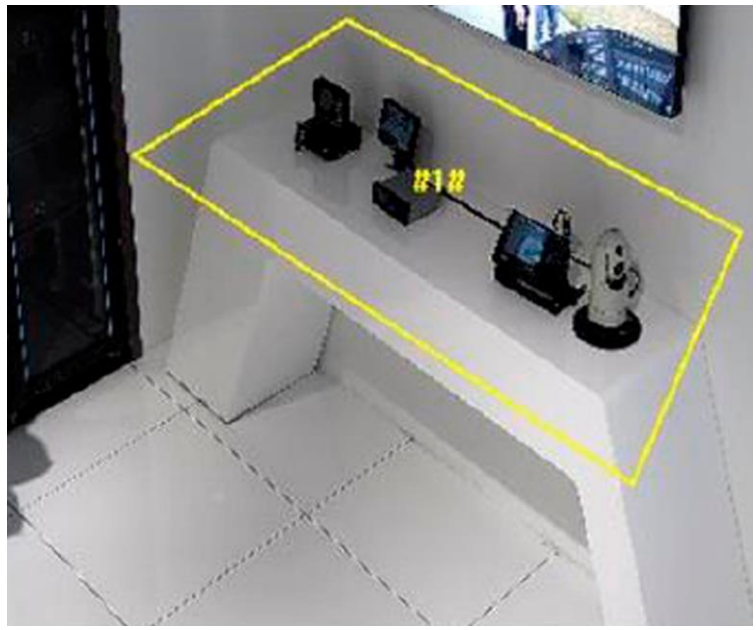


図10-6 ルール設定

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

注意

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

10.4 人管理

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

注

- この機能は、ソフトウェアデコードモードまたはハードウェアデコードモードのフィッシュアイビュー表示モードでのみサポートされています。
- 特定のデバイスモデルでは、まずVCAページでアプリケーションを有効にする必要があります。アプリケーションを有効にするには、十分な**メモリ**、**RAM**、**およびFLASHが**確保されていることを確認してください。そうでない場合は、他のアプリケーションを最初に無効にする必要があります。

10.4.1 キュー管理

キューに並んでいる人数と各人の待ち時間をカウントするために使用します。

地域ごとの待ち行列の検出を設定するには、「地域ごとの待ち行列の設定」を参照してください。待ち時間の検出を設定するには、「待ち時間の検出の設定」を参照してください。

キュー***管理統計***を設定および表示するには、「キュー管理統計」を参照してください。

注意

キュー管理は、特定のモデルでのみサポートされています。

地域の人々の待ち行列を設定

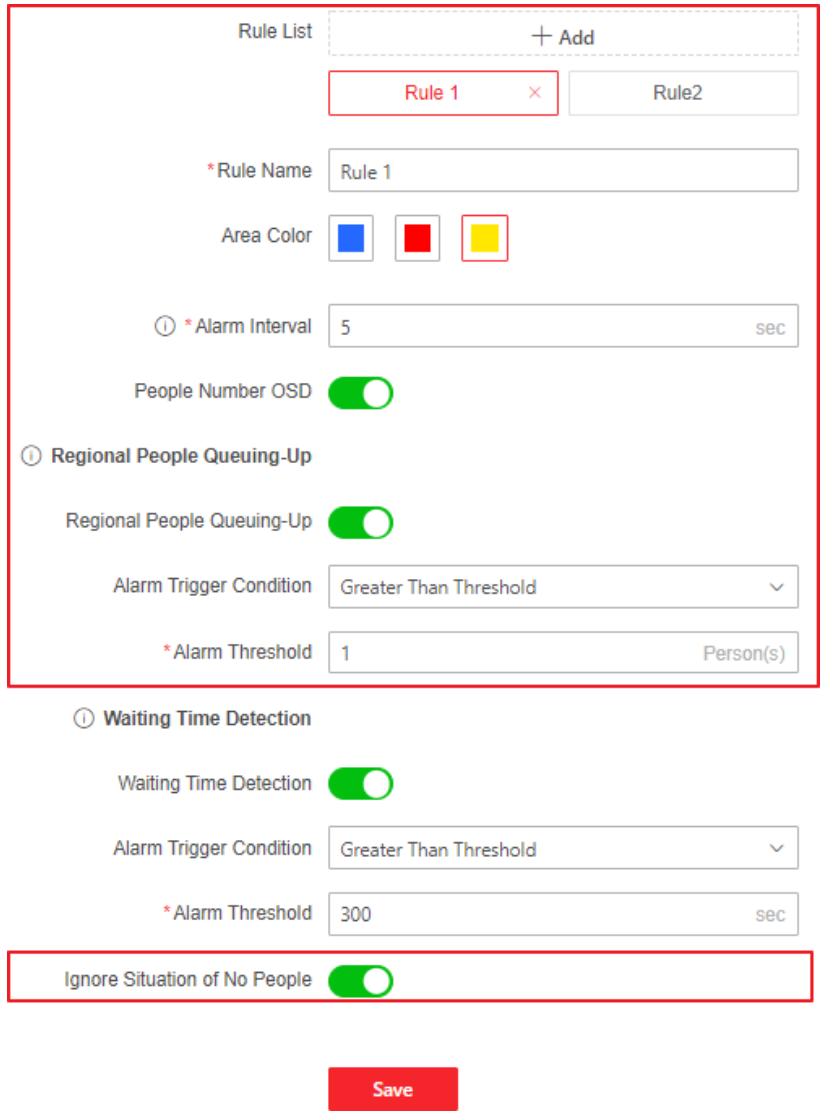
これは、定義されたエリアにキューイングアップしている人の数をカウントするために使用されます。アラームのしきい値条件とアラームのトリガーが両方満たされた場合にアラームが作動します。

開始前に

- **VCA** に移動し、アプリケーションを選択します。**People Management** 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では、**VCA** に移動して **People Management** をインポートし、有効にしてください。

手順

1. **VCA** に移動します**。→ アプリケーションを設定します。→ People Management→ Queue Management→ Rule** .
2. **「追加」**をクリックし、必要に応じてルール名を変更します。



3. **エリアの色**を選択し、[ ] をクリックしてルール領域を描画します。ライブビューウィンドウで、セットしたルール領域の境界となる端点を左クリックし、右クリックして描画を終了します。

注意

- 最大 8 つのエリアを同時に設定できます。
- 領域が重ならないようにご注意ください。

4. ルールパラメーターを設定します。

アラーム間隔

設定されたアラーム間隔中、同じタイプのアラームは 1 回だけ通知されます。

人数表示 OSD

ライブビューウィンドウ内にいる人の数を表示します。

人物がいない状況を無視

シーンに人がいない場合、デバイスはアラームをトリガーしません。この機能は、値が設定されたアラームしきい値未満であり、シーンに人がいない場合、潜在的なアラーム状態をフィルタリングします。

5. **地域の人々の待ち行列**を選択し、**アラームトリガー**条件と**アラームしきい値**を設定します。設定エリアの人数がアラームしきい値に達し、トリガー条件を満たすと、アラームが作動します。
6. **保存**をクリックします。

注意

複数のエリアのパラメーターを設定するには、上記のステップを繰り返し実行してください。

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

注意

ルールリストでルールを選択し、[ ]をクリックするか、**[Copy to...]** をクリックして、関連する武装スケジュールおよびリンク方法の設定を他のルールにコピーします。

8. **オプション：**データアップロードを設定するには、**[Data Upload]** をクリックします。リアルタイムアップロードとスケジュールアップロードの両方がサポートされています。設定が完了したら、**[Save]** をクリックします。

リアルタイムアップロード

リアルタイムアップロードを確認し、デバイスは検出されたターゲットID、待機時間、および地域の人数をリアルタイムでアップロードします。

スケジュールされたアップロード

デバイスは、待機時間が指定された時間以上の人数をアップロードします。

例えば、最低滞在時間を 10 秒に設定し、2 つのエリアをカバーする場合、デバイスは、積算ポイントで、**滞在時間が**

たとえば、最低滞在時間を 10 秒に設定し、2 つのエリアをカバーする場合、デバイスは、2 つのエリアでそれぞれ滞在時間が 10 秒以上になったときに、その時点の人数をアップロードします。

9. **オプション：**オーバーレイおよびキャプチャのパラメータを設定します。詳細な設定については、「*オーバーレイおよび」キャプチャ*を参照してください。
10. **オプション：**バージョンを表示し、フィルタリング条件を設定します。詳細設定については、*「詳細設定」*を参照してください。

次に実行する操作

アプリケーション表示→ キュー管理統計に移動して、詳細なデータ分析を表示します。詳細な設定については、「*キュー管理統計」*を参照してください。

待機時間検出の設定

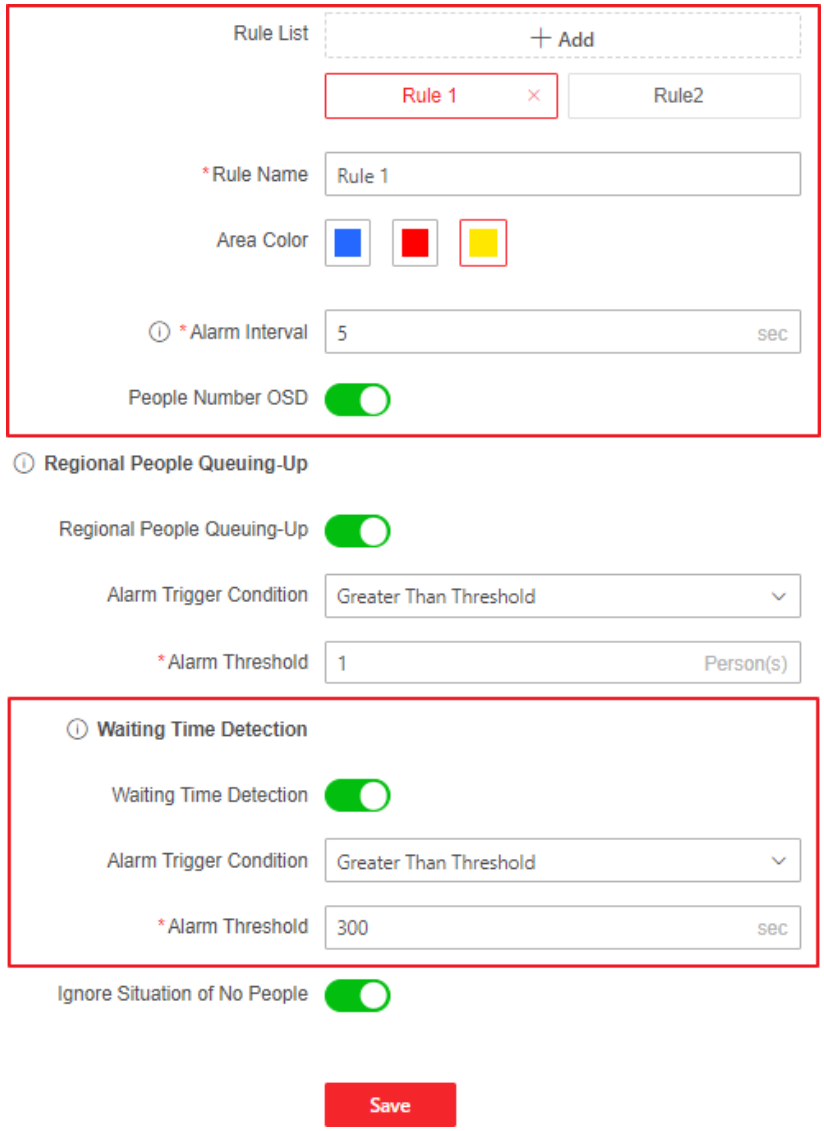
検出エリアに入った各人の待機時間をカウントするために使用します。アラームしきい値条件とアラームトリガーの両方が満たされた場合にアラームが作動します。

開始前に

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

手順

1. **VCA** に移動します。**→ アプリケーションを設定します。→ People Management→ Queue Management→ Rule**
2. **「追加」**をクリックし、必要に応じてルール名を変更します。



3. **エリアカラー**を選択し、[ ]をクリックしてルールエリアを描画します。ライブビューウィンドウで、設定したルールエリアの境界となる端点を左クリックし、右クリックして描画を終了します。

注意

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

4. ルールパラメーターを設定します。

アラーム間隔

設定したアラーム間隔中に、同じタイプのアラームは 1 回だけ通知されます。

人数のOSD

ライブビューウィンドウ内の人数を表示します。

5. **待機時間検出**を選択し、**アラームトリガー**条件と**アラームしきい値**を設定します。設定したエリアでの待機時間がアラームしきい値に達し、トリガー条件を満たすと、アラームが作動します。

6. **保存**をクリックします。

注意

上記のステップを繰り返し、複数の領域のパラメーターを設定できます。

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

注

ルールリストでルールを選択し、[ ] または **[Copy to...]** をクリックして、関連する武装スケジュールとリンク方法の設定を他のルールにコピーします。

8. **オプション：データアップロード**をクリックして、データアップロードを設定します。リアルタイムアップロードとスケジュールアップロードの両方がサポートされています。設定が完了したら、**保存**をクリックします。

リアルタイムアップロード

「**Real-Time Upload**」にチェックを付けると、デバイスが検出されたターゲットID、待機時間、および地域の人数をリアルタイムでアップロードします。

スケジュールアップロード

待機時間が指定した時間以上の人数データをデバイスがアップロードします。

最低滞在時間」以上の人の人数をアップロードします。

たとえば、最低滞在時間を 10 秒に設定し、2 つのエリアをカバーする場合、デバイスは、2 つのエリアでそれぞれ滞在時間が 10 秒以上になった時点で、その時点の人数をアップロードします。

9. **オプション：**オーバーレイおよびキャプチャのパラメータを設定します。詳細な設定については、「*オーバーレイおよび」キャプチャ*を参照してください。

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

次に実行する操作

アプリケーション画面に移動します。→ **キュー管理統計** 詳細なデータ分析を表示します。詳細設定については、*「キュー管理統計」*を参照してください。

キュー管理統計

キュー管理はデータ分析とレポート出力に対応しています。

開始前に

キュー管理の設定については、*「地域ごとの待ち行列の設定」*および「*待ち時間検出の設定*」を参照してください。

- **「待ち行列時間分析」**と**「複数エリア比較」**を選択すると、異なるエリアの待ち行列の人数を比較することができます。
- 「**待ち時間分析とマルチレベル比較」**を選択すると、異なる待ち時間レベルの待ち行列の人数を比較できます。
- **「キュー状態分析」**と**「複数エリア比較」**を選択すると、異なるエリアでキューが特定の長さで滞在する時間と期間を比較できます。
- **キューの状態**分析と**マルチレベル比較**を選択すると、異なるキューの長さのレベルにおけるキューの滞在時間と滞在時間を比較できます。

手順

注

オンボードメモリカードが取り付けられている場合、このデバイスは 1 ヶ月分のデータを保存できます。メモリカードが取り付けられていない場合、このデバイスは 1 週間分のデータしか保存できません。

1. アプリケーションディスプレイの**「→ キュー管理統計」**に移動します。

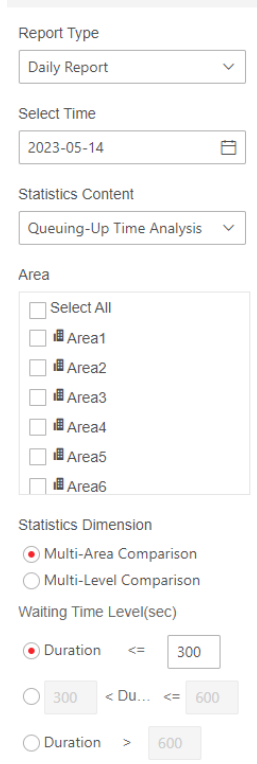


図10-7 キュー管理統計

2. **レポートの種類**と**統計時間を**を選択します。
3. **統計内容**を選択します。**待ち時間分析**

   キューイングアップ時間分析は、さまざまな待機時間レベルの人の数を計算します。

   キュー状態分析

   キュー状態分析は、キューが特定の長さで保持される時間と期間を計算します。
4. **統計の寸法**を選択します。**複数エリア比較**

   複数の領域と 1 つのレベルを分析対象として選択し、分析チャートを作成することができます。

   マルチレベル比較

   複数のレベルとエリアを分析対象として選択し、エリアごとに 1 つの分析チャートを作成します。
5. 1つまたは複数の領域を選択します。
6. **待機時間レベル**を設定します。ご希望の範囲にチェックを入れ、値を入力してください。
7. **検索**をクリックしてレポートを生成します。
8. **オプション：[エクスポート]**をクリックして、データをエクスポートします。

10.4.2 交差分析

交差点分析は、交差点のようなシーンにおける乗客の流れを検出するために使用されます。

注
この機能は、特定のモデルでのみサポートされています。

交差点分析の設定

開始前に

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

手順

1. **VCA** に移動します。**→ アプリケーションを設定します。→ People Management→ Intersection Analysis→ Rule**
2. **「有効にする」**にチェックを入れて機能を有効にします。
3. 「◇」をクリックしてルール領域を描画します。ライブビューウィンドウ内の終了点を左クリックしてルール領域の境界を定義し、右クリックで描画を完了します。
4. 領域の各辺の矢印の方向を調整します。矢印は、交差点から流れが離れる方向を示します。
5. **「武装スケジュールとリンク方法」**に移動し、武装スケジュールを設定し、チェックボックスをオンにしてリンク方法を選択します。武装スケジュールの設定については、***「武装スケジュールの設定」***を参照してください。リンク方法の設定については、***「リンク方法の設定」***を参照してください。
6. **データアップロード**」に移動し、アップロードするデータの種類を選択します。交差点分析レポートは、設定済みのメールアドレスに送信することができます。
7. **保存**をクリックします。

次にやるべきこと
アプリケーション表示の「→ 交差分析統計」に移動して、詳細なデータ分析を表示します。詳細な設定については、***「交差分析統計」***を参照してください。

交差点分析統計

交差点分析機能を有効にすると、交差点分析データを確認できます。画面には、入口の方向と総人数に対する入口ごとの人数が重ねて表示されます。特定の入口から流入する人数と、他のすべての入口から流出する人数が計算されます。

開始前に

まず、交差分析機能を設定してください。

手順

1. **アプリケーションディスプレイの「→」の「Intersection Analysis Statistics」**に移動します。
2. **「入口」**でフローを選択します。
3. **レポートの種類**と**開始時間を**設定します。
4. **検索**をクリックします。
   条件に一致するデータ情報が表示されます。

10.4.3 オーバーレイとキャプチャ

キャプチャパラメーターを設定し、ストリームと画像に表示する情報を選択します。

Go to **VCA→ People Management→ Overlay & Capture** .

ストリームにVCA情報を表示します。

ストリーム上にスマートな情報を表示し、ターゲットとルールに関する情報を表示します。

アラーム画像にターゲット情報を表示

アラーム画像にターゲット情報をオーバーレイ表示します。

テキストオーバーレイ

キャプチャした画像にオーバーレイする情報を選択します。また、↑ ↓をクリックして順序を調整できます。

10.4.4 詳細設定

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

現在のアルゴリズムバージョンを表します。

アルゴリズムモード

インストール環境に応じてモードを選択してください。

フィルター

ターゲットサイズ

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

移動量

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

最低待機時間

設定値未満の待機時間はフィルタリングされます。

信頼度

閾値が高いほど、ターゲットの検出が困難になりますが、精度も高くなります。

注

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

ストレージデータの消去

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

10.5 ヒートマップ

ヒートマップは、データを色で表現したグラフです。カメラのヒートマップ機能は、設定されたエリアにおける顧客の訪問時間や滞在時間を分析するために使用されます。

注意

- この機能は、ソフトウェアデコードモードまたはハードウェアデコードモードのフィッシュアイビュー表示モードでのみサポートされています。
- 特定のデバイスモデルでは、まずVCAページでアプリケーションを有効にする必要があります。アプリケーションを有効にするには、十分なメモリ、RAM、およびFLASHが確保されていることを確認してください。そうでない場合は、まず他のアプリケーションを無効にする必要があります。

10.5.1 ヒートマップの設定

ヒートマップの統計データを照会する場合は、まずカメラを設定してください。

開始前に

- **VCA** に移動し、アプリケーションを選択します。**People Management** を選択し、**Next** をクリックして機能を有効にします。
- HEOP 対応デバイスでは、**VCA** に移動して **People Management** をインポートし、有効にしてください。
- ヒートマップデータを検索する前に、まずストレージパスを設定してください。ストレージ設定については、*Storage SeFngs をご確認ください*。

手順

1. Go to **VCA→ Set Application→ People Management→ Heat Map Configuration** .
2. 機能を有効にするには**「有効」**にチェックを入れます。
3. 検出領域を描画します。⬡をクリックし、ライブビューをクリックして頂点を指定し、検出領域の境界を描画し、右クリックで描画を完了します。
4. 描画した領域のパラメーターを設定します。

   予想される人数

   ヒートマップカウントの最大人数を指します。

ON

カメラが、実際のシーンにいる人の最大人数と、設定された予想人数を比較し、大きい方をヒートマップの最大人数として採用することを指します。

OFF

カメラが、実際の人の数をヒートマップの最大値とすることを意味します。

5. **保存**をクリックします。
6. アラーム設定スケジュールを設定します。***アラーム設定スケジュールを設定***を参照してください。
7. リンク方法を設定します。***リンク方法の設定***を参照してください。
8. **オプション：[データアップロード]** をクリックして、データアップロードに関する情報を設定します。**[保存]** をクリックして設定を保存します。

データアップロードの種

類：滞在時間

これは、検出領域内でターゲットが滞在する時間を指します。

滞在時間と人数

これは、検出領域内のターゲットの滞在時間と、検出領域内の人数を指します。

次に実行する操作

ヒートマップの統計は、**[アプリケーション表示]** タブで計算されます。**[アプリケーション表示]** に移動して

をクリックしてヒートマップ統計を確認してください。

10.5.2 ヒートマップデータを表示

ヒートマップは、事前に定義されたエリア内の人流を観察し、計算して、その流れの統計情報をグラフ形式で表示します。ショッピングモール、スーパーマーケット、博物館など、大規模な人流が発生するシーンに適用可能です。ヒートマップを活用することで、顧客の好みを分析し、商品の配置を最適化することができます。

開始前に

ヒートマップの設定を完了してください。詳細については、「***ヒートマップの設定***」を参照してください。

手順

1. **アプリケーション画面**に移動し、**→ ヒートマップを選択します**。
2. **レポートタイプ**を選択します。日次レポート、週次レポート、月次レポート、年次レポートから選択可能です。
3. **ヒートマップの種類**を選択します。空間ヒートマップと時間ヒートマップが選択可能です。
4. **統計の種類**を選択してください。滞在時間と人数による選択が可能です。
5. **統計の時間を**指定します。
6. **検索**をクリック。

日次レポートは、選択した日付のデータを計算します；週次レポートは、選択した日付が含まれる週のデータを計算します；月次レポートは、選択した日付が含まれる月のデータを計算します；年次レポートは、選択した日付が含まれる年のデータを計算します。

例

計算後、空間ヒートマップと時間ヒートマップでデータを表示できます。

空間ヒートマップ

画像全体のさまざまなエリアにおける人の累積滞在時間を統計的に分析します。

異なる熱値は異なる色に対応しており、その中、赤（255、0、0）が最も高い熱、青（0、0、255）が最も低い熱を表します。最も高い熱値と最も低い熱値は、N レベルに分けられ、それぞれ異なる色に対応しています。

時間熱マップ

画像全体における全人の総滞在時間について統計分析を行います。

時間ヒートマップは線グラフで表示され、**エクスポートをクリックすると**データをExcelファイルとしてエクスポートできます。

10.6 人数のカウント

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

注

- この機能は、ソフトウェアデコードモードまたはハードウェアデコードモードのフィッシュアイビュー表示モードでのみサポートされています。
- 一部のデバイスモデルでは、まずVCAページでアプリケーションを有効にする必要があります。アプリケーションを有効にするには、十分な**メモリ**、**Smart RAM**、**およびFLASH**が必要です。不足している場合は、他のアプリケーションを無効にする必要があります。

10.6.1 人流量カウントルールを設定する

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

開始前に

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

手順

1. **VCA** に移動します。**→ アプリケーションを設定します**。**→ People Counting→ Rule**
2. **「有効」**にチェックを入れて機能を有効にします。

3. **「追加」**をクリックして検出領域を追加します。
4. 「」をクリックして、ポリゴン検出領域（カウント領域）を描画します。ライブビューウィンドウで終了点を左クリックし、右クリックで描画を完了します。
5. 検出ラインを描きます。矢印は進入方向を示します。方向を変更するには、をクリックしてください。
   - 検出領域が一方通行のみをサポートする場合、をクリックして直線の検出線を描画することをおすすめします。
   - 検出領域が複数方向に対応する場合、または検出領域内に壁や障害物がある場合は、をクリックしてポリラインを描画することをおすすめします。

注意

カウント精度を向上させるため、以下のルールに従って検出領域を描画してください。

- 検出領域は、アクセス区域に出入りする人をすべてカバーする必要があります。
- 検出ラインは、赤色の検出領域内に完全に含まれており、通過する人の経路と垂直に配置する必要があります。

6. **オプション：**検出エリアと検出ラインを調整します。

   「　　」**をクリックし、**選択した検出領域または線をクリアします。

   「　　」**をクリックし、**すべての検出領域と線をクリアします。

7. **オプション：**上記の手順を繰り返して、最大 3 つの検出エリアと対応する検出ラインを描きます。
8. 人計数パラメーターを設定します。

OSDオーバーレイコンテンツ

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

注意

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

日次リセット時間

デバイスはデフォルトで毎日00:00にデータをクリアします。ドロップダウンリストから時間を選択できます。選択後、毎日その時間点にカウントデータが自動的にクリアされます。

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

9. **「保存」**をクリックします。
10. アラーム設定スケジュールを設定します。***アラーム設定スケジュールを設定する***を参照してください。
11. リンク方法を設定します。***リンク方法の設定***を参照してください。
12. **保存**をクリックします。
13. **オプション：**人数のカウントデータのアップロードパラメータを設定します。

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

リアルタイムデータアップロード

リアルタイムデータをプラットフォームに送信します。

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、乗客流動カウントデータが**データ統計サイクル**に従って間隔ごとにプラットフォームにアップロードされます。

14. オプション：人数のカウントに関する詳細パラメータを設定します。

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

バージョン

現在のアルゴリズムのバージョンを表します。

ストリームにVCA情報を表示

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

ストレージデータをクリア

デバイスに保存されているすべての人のカウントデータをクリアします。この機能は注意して使用してください。

結果

- ターゲットが、入室方向に沿って検出エリアを通過し、検出ラインを通過した場合、1 人の入室ターゲットとしてカウントされます。
- ターゲットが退出方向に沿って検出エリアを横切り、検出ラインを通過した場合、1 つの退出ターゲットとしてカウントされます。

次に実行する操作

アプリケーション表示」に移動して、詳細な人数のカウントデータ分析を表示します。詳細な設定については、「***人数のカウントデータの表示***」を参照してください。

10.6.2 人計数データ表示

デバイスに保存された人計数データを、テーブル、棒グラフ、線グラフで表示できます。

開始前に

まず、人数のカウントデータを設定してください。

手順

1. アプリケーション表示「→人数カウント統計」に移動します。

2. レポートの種類、統計の種類、開始時間を設定します。

3. 検索をクリックします。

データを確認するには、**テーブル**、**棒グラフ**、**線グラフ**を選択できます。また、人数の統計データをExcelでエクスポートできます。

10.7 データ認識情報の検索とエクスポート

データ認識機能は、再起動、武装、およびアラーム統計のデータを検索およびエクスポートするために使用されます。

開始前に

管理ユーザーアカウントでデバイスにログインしてください。

手順

1. **アプリケーション表示→ データ認識**へ移動します。
2. 検索条件を選択します。

統計の種類	オプション
記録の再起動	再起動の種類、開始時間、終了時間。
アラーム設定	アラーム設定の種類、開始時間、終了時間。
アラーム統計の取得	レポートの種類、アラームターゲット、プロトコル、武装 IP アドレス、および開始時刻。
アラーム品質統計	レポートタイプ、アラームターゲット、開始時間。

3. **検索**をクリック。

   条件に一致するデータ情報が表示されます。
4. **オプション：[エクスポート]** をクリックして、データ情報をローカルデバイスに保存します。

付録A. よくある質問

以下のQRコードをスキャンして、デバイスのよくある質問を確認してください。一部のよくある質問は、特定のモデルにのみ適用されます。

See Far, Go Further

www.hikvision.com
support@hikvision.com

HIKVISION