



ネットワークカメラ

ユーザーマニュアル

UM77112603

法的情報

この文書について

- 本書には、本製品の使用および管理に関する説明が記載されています。以下、写真、図表、画像、その他すべての情報は、説明のためのものです。
- 本書に記載されている情報は、ファームウェアの更新や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。
- 本書は、本製品のサポートに精通した専門家の指導と支援を受けながら使用してください。

この商品について

- 本製品は、購入された国または地域においてのみアフターサービスを受けることができます。

知的財産権の承認

- 本書に記載された製品に具現化された技術に関連する著作権および／または特許を所有し、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。
- その他記載されている商標およびロゴは、各所有者の財産です。

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た製品、そのハードウェア、ソフトウェア、ファームウェアは、「現状のまま」、「すべての欠点およびエラーとともに」提供されます。
- 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適合していることを確認することについては、お客様が単独で責任を負うものとします。特に、お客様は、肖像権、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責任を負うものとします。大量破壊兵器の開発または生産、化学兵器または生物兵器の開発または生産、核爆発物または安全でない核燃料サイクルに関連する活動、または人権侵害の支援など、禁止されている最終用途のために本製品を使用してはなりません。
- 本書と適用される法律の間に矛盾がある場合は、後者が優先されます。

シンボル規約

本書で使用される記号は以下のように定義されています。

シンボル	説明
 危険	この表示を無視して誤った取り扱いをすると、人が死亡または重傷を負う可能性が想定される内容を示しています。
 注意	回避しなければ、機器の損傷、データ損失、性能低下、または予期せぬ結果につながる可能性のある、潜在的に危険な状況を示します。
 注	本文の重要なポイントを強調または補足するための追加情報を提供します。

内容

第1章 システム要件	1
第2章 機器のアクティベーションとアクセス	2
2.1 SADP経由で機器をアクティブにする	2
2.2 ブラウザ経由で機器を起動する	2
2.3 ログイン	3
2.3.1 プラグインのインストール	3
2.3.2 管理者パスワード復旧	4
2.3.3 不正ログインロック	5
第3章 ライブビュー	6
3.1 ライブビューのパラメーター	6
3.1.1 ディスプレイコントロール	6
3.1.2 ライブビューの開始と停止	8
3.1.3 アスペクト比	8
3.1.4 ライブビューストリームタイプ	9
3.1.5 サードパーティプラグインを選択	9
3.1.6 ライト	9
3.1.7 ピクセル数	9
3.1.8 デジタルズーム開始	10
3.1.9 補助フォーカス	10
3.1.10 レンズの初期化	10
3.1.11 レンズパラメーター調整	10
3.1.12 3Dポジショニングの実施	11
3.2 送信パラメーターの設定	12
第4章 ビデオとオーディオ	13
4.1 ビデオ設定	13
4.1.1 ストリームタイプ	13
4.1.2 ビデオタイプ	13
4.1.3 解像度	13

4.1.4	ビットレートタイプと最大ビットレート.....	14
4.1.5	ビデオ画質.....	14
4.1.6	フレームレート.....	14
4.1.7	ビデオエンコーディング.....	14
4.1.8	スムージング.....	16
4.2	音声設定.....	16
4.2.1	音声エンコード.....	17
4.2.2	音声入力.....	17
4.2.3	音声出力.....	17
4.2.4	環境ノイズフィルター.....	17
4.3	双方向オーディオ.....	17
4.4	ROI.....	18
4.4.1	ROIの設定.....	18
4.5	ターゲットクロッピングの設定.....	19
4.6	複数ストリーム情報表示.....	19
4.7	ディスプレイ設定.....	19
4.7.1	シーンモード.....	20
4.7.2	画像パラメータスイッチ.....	25
4.7.3	ビデオ規格.....	26
4.7.4	ローカルビデオ出力.....	26
4.7.5	切断線と水平半径の角度.....	26
4.8	OSD.....	27
4.9	プライバシーマスクの設定.....	28
4.10	画像オーバーレイ.....	28
第5章	ビデオ録画と画像キャプチャ.....	29
5.1	ストレージ設定.....	29
5.1.1	メモリーカード.....	29
5.1.2	FTPの設定.....	31
5.1.3	NASの設定.....	32
5.1.4	eMMC保護機能.....	33

5.1.5 クラウドストレージの設定.....	33
5.2 ビデオ録画.....	34
5.2.1 自動録画の設定.....	34
5.2.2 手動録画の設定.....	36
5.2.3 ビデオの再生とダウンロード.....	36
5.3 キャプチャ構成.....	37
5.3.1 自動キャプチャ.....	37
5.3.2 手動キャプチャ.....	37
5.3.3 写真を見るダウンロードする.....	38
第6章 イベントとアラーム.....	39
6.1 モーション検知の設定.....	39
6.1.1 エキスパートモード.....	39
6.1.2 ノーマルモード.....	40
6.2 ビデオタンパリングアラームの設定.....	41
6.3 アラーム入力設定.....	42
6.4 異常アラームの設定.....	42
6.5 ビデオ画質診断の設定.....	43
6.6 振動検知の設定.....	43
6.7 オーディオ異常検知の設定.....	44
6.8 デフォーカス検知の設定.....	44
6.9 シーンチェンジ検知の設定.....	45
第7章 警戒スケジュールとアラーム連動.....	46
7.1 警戒スケジュールの設定.....	46
7.2 リンクメソッドの設定.....	46
7.2.1 トリガーアラーム出力.....	47
7.2.2 FTP/NAS/メモリーカードのアップロード.....	48
7.2.3 メール送信.....	48
7.2.4 監視センターに通知.....	49
7.2.5 トリガー録画.....	49
7.2.6 警告音.....	49

7.2.7 アラームサーバー	50
第8章 ネットワーク設定	51
8.1 TCP/IPの設定	51
8.2 ドメイン名による機器へのアクセス	52
8.3 PPPoEダイヤルアップ接続による機器へのアクセス	53
8.4 SNMPの設定	53
8.5 IEEE 802.1Xの設定	54
8.6 QoSの設定	54
8.7 HTTP(S)の設定	55
8.8 マルチキャスト	56
8.8.1 マルチキャスト検出	56
8.9 RTSPの設定	56
8.10 SRTPの設定	57
8.11 Bonjourの設定	57
8.12 WebSocket(s)の設定	58
8.13 ポートマッピング	58
8.13.1 自動ポートマッピングの設定	58
8.13.2 手動ポートマッピングの設定	58
8.13.3 ルーターにポートマッピングを設定する	59
8.14 SIPの設定	60
8.15 ISUPの設定	60
8.16 Guarding Vision経由でカメラにアクセス	60
8.16.1 カメラのGuarding Visionサービスを有効にする	61
8.16.2 Guarding Visionのセットアップ	62
8.16.3 Guarding Visionにカメラを追加	63
8.17 オープンネットワークビデオインターフェース(ONVIF)の設定	63
8.18 SDKサービスの設定	64
第9章 システムとセキュリティ	65
9.1 システム設定	65
9.1.1 機器情報の表示	65

9.1.2 時刻と日付	65
9.1.3 RS-232の設定	66
9.1.4 RS-485の設定	67
9.1.5 ライブビュー接続の設定	67
9.1.6 位置情報の設定	67
9.1.7 オープンソースソフトウェアライセンスの表示	68
9.2 ユーザーとアカウント	68
9.2.1 ユーザーアカウント権限の設定	68
9.2.2 同時ログイン	69
9.2.3 オンラインユーザー	69
9.3 メンテナンス	69
9.3.1 再起動	69
9.3.2 アップグレード	69
9.3.3 バックアップと復元	70
9.3.4 設定ファイルのインポートとエクスポート	70
9.3.5 ログの検索と管理	70
9.3.6 セキュリティ監査ログの検索	71
9.3.7 SSHの設定	71
9.3.8 診断情報のエクスポート	71
9.4 セキュリティ	71
9.4.1 IPアドレスフィルターの設定	72
9.4.2 MACアドレスフィルターの設定	72
9.4.3 操作タイムアウト設定	73
9.4.4 ライセンス管理	73
9.4.5 TLSの設定	76
第10章 VCAリソース	77
10.1 オープンプラットフォームの設定	77
10.2 一般設定	77
10.2.1 カメラ情報の設定	78
10.3 スマートイベント	78

10.3.1 侵入検知の設定	78
10.3.2 ラインクロス検知の設定	79
10.3.3 領域侵入検知の設定.....	81
10.3.4 領域退出検知の設定.....	82
10.3.5 放置手荷物検知の設定	83
10.3.6 持ち去り検知の設定	85
10.4 人物カウントアラーム	86
10.4.1 待ち行列管理	87
10.4.2 交差点分析.....	94
10.4.3 オーバーレイとキャプチャ	95
10.4.4 詳細設定.....	95
10.5 ヒートマップ.....	96
10.5.1 ヒートマップの設定	96
10.5.2 ヒートマップデータの表示	97
10.6 人数集計.....	98
10.6.1 人数カウントールの設定	98
10.6.2 人数集計データの表示.....	100
10.7 データウェア情報の検索とエクスポート.....	101

第1章 システム要件

お使いのコンピュータは、本製品を正しく使用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以上 CPU2.0GHz以上

RAM 1G以上

ディスプレイ 解像度1024×768以上

ウェブブラウザ 詳しくはプラグインのインストールをご覧ください。

第2章 機器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機器にアクセスする際には、機器を起動するためのログインパスワードを設定する必要があります。



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経由で機器をアクティブにする

SADPソフトウェアを介してオンライン機器を検索し、アクティブ化します。

始める前に

<https://e-camera.net/soft.html> にアクセスし、SADP ソフトウェアをインストールします。

ステップ

1. ネットワークケーブルを使用して機器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. デバイスリストから機器のステータスを確認し、非アクティブデバイスを選択します。
4. 新しいパスワードを作成し、パスワードフィールドに入力し、パスワードを確認します。



注意

製品の安全性を高めるため、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)を作成することを強くお勧めします。特にセキュリティの高いシステムでは、毎月または毎週パスワードをリセットすることで、より製品を保護することができます。

5. OKをクリックします。

機器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ーの変更]で機器のネットワークパラメーターを変更します。

2.2 ブラウザ経由で機器を起動する

ブラウザ経由で機器にアクセスし、アクティベーションを行うことができます。

ステップ

1. ネットワークケーブルを使って機器とPCを接続します。
 2. PCと機器のIPアドレスを同じセグメントに変更します。
-



本機のデフォルトIPアドレスは192.168.1.64です。PCのIPアドレスは192.168.1.2～192.168.1.253 (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に設定することができます。

3. ブラウザで**192.168.1.64**を入力します。
 4. 機器のアクティベーションパスワードを設定します。
-



製品のセキュリティを高めるため、お客様ご自身で強力なパスワード(大文字、小文字、数字、特殊文字のうち少なくとも3つを含む8文字以上)を作成されることを強くお勧めします。特にセキュリティの高いシステムでは、毎月または毎週パスワードをリセットすることで、より製品を保護することができます。

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、機器にログインします。
7. オプション:**Configuration**→**Network**→**Network Settings**→**TCP/IP**にアクセスして、機器の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

ウェブブラウザで機器にログインします。

2.3.1 プラグインのインストール

OSやブラウザによっては、カメラ機能の表示や操作が制限される場合があります。正常に表示操作するためには、プラグインをインストールしたり、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、実機にてご確認ください。

オペレーティングシステム	ウェブブラウザ	オペレーション
ウィンドウズ	<ul style="list-style-type: none"> インターネットエクスプローラー 10以上 Google Chrome 57以前のバージョン Mozilla Firefox 52以前のバージョン 	ポップアップ表示に従って、プラグインのインストールを完了します。
	<ul style="list-style-type: none"> グーグルクローム 57+ Mozilla Firefox 52+ エッジ 89+ 	 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。
マックOS	<ul style="list-style-type: none"> グーグルクローム57+ Mozilla Firefox 52+ Mac Safari 16+ 	プラグインのインストールは不要。 設定 → ネットワーク → ネットワークサービス → WebSocket(s) で WebSocket または Web Socket を有効にして通常表示。一部機能の表示操作が制限されます。 例えば、再生やピクチャは使用できません。制限機能の詳細については、実機にてご確認ください。



カメラはWindowsと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ません。

2.3.2 管理者パスワード復旧

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。

パスワードをリセットするには、セキュリティの質問や電子メールを設定します。



パスワードをリセットする必要がある場合は、機器と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

アカウントのセキュリティは、アクティベーション中に設定できます。または、**設定** → **システム** → **ユーザー管理** に進み、**アカウントセキュリティ設定** をクリックし、セキュリティの質問を選択し、答えを入力することもできます。

ブラウザ経由で機器にアクセスする際、「パスワードを忘れた場合」をクリックし、セキュリティ質問に答えて管理者パスワードをリセットすることができます。

電子メール

アクティベーション時にアカウント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** に進み、**アカウントセキュリティ設定** をクリックし、回復操作プロセス中に認証コードを受信するためのメールアドレスを入力することができます。

2.3.3 不正ログインロック

インターネット経由で機器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、

「**不正ログインのロック機能を有効にします。**」を有効にします。

不正なログイン試行回数とロック持続期間は設定可能です。

不正なログイン試行(回数)

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

ロック時間設定時間経過後、装置はロックを解除します。

第3章 ライブビュー

ライブビューパラメーター、ファンクションアイコン、送信パラメーター設定を紹介。

3.1 ライブビューのパラメーター

対応機能は機種によって異なります。

3.1.1 ディスプレイコントロール

表示コントロールエリアでは、ライブビューのデコードモード、マウントタイプ、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、それに応じて複数のマウントタイプと表示モードのいずれかを選択できます。

デコードモード

- ソフトウェアデコードモードとは、ライブビュー映像が、コンピュータのCPUによってデコーディングされることを示します。ライブビューの性能は、コンピュータのデコード能力に依存します。
- ハードウェアデコーディングモードとは、ライブビュー映像がカメラによってデコーディングされることです。

マウントタイプ

カメラの実際のマウントタイプに応じて、天吊り、壁掛け、テーブル設置を選択できます。すべてのマウントタイプのアイコンの説明は次のとおりです：

表3-1 マウントタイプの説明

アイコン	説明
	壁面 : 壁掛け
	デスクトップ : テーブル取り付け
	天井 : 天井取り付け



注
マウントタイプは実際の機種によって異なります。マウントタイプが1種類しかない機種の場合、マウントタイプを選択することはできません。

表示モード

ライブビューウィンドウのレイアウトに表示モードを選択できます。利用可能な表示モードは、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の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
	フィッシュアイ：魚眼的な視点。		シリンダー：円柱の眺め。
	180度のパノラマビュー。		360度のパノラマビュー。
	360度パノラマビューとPTZビュー。		360度のパノラマビューと3つのPTZビュー。
	360度のパノラマビューと6つのPTZビュー。		360度のパノラマビューと8つのPTZビュー。
	2PTZ：2つのPTZビュー。		4PTZ：4つのPTZビュー。
	フィッシュアイビューと3つのPTZビュー。		フィッシュアイビューと8つのPTZビュー。

アイコン	説明	アイコン	説明
	ドームカメラ : 半球の眺め。		ARドームカメラ : 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の 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

- 表示モードによって機能が異なる場合があります。
- ハードウェアデコーディングモードを選択した場合、
 - 表示モードの切り替えには再起動が必要です。
 - 魚眼表示の表示モードで、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。
 - 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、**VCA Resource**を設定することができます。
- ソフトウェアデコーディングモードを選択すると、すべての表示モードで**VCA Resource**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

アスペクト比とは、画像の幅と高さの表示比率のこと。

-  は4:3のウィンドウサイズを指す。
-  は16:9のウィンドウサイズを指す。
-  は元のウィンドウサイズを指す。
-  は自己適応ウィンドウサイズを指す。
-  は元の比率のウィンドウサイズを指す。

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ます。

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。

3.1.5 サードパーティプラグインを選択

特定のブラウザでライブビューが表示できない場合は、ブラウザに応じてライブビュー用のプラグインを変更することができます。

ステップ

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でアクセスする場合は、Web componentsまたはQuickTimeを選択できます。
 - 他のブラウザでアクセスする場合は、Web components、QuickTime、MJPEGを選択できます。

3.1.6 ライト

 をクリックして、イルミネーターをオンまたはオフにします。



注意

レーザー付き装置用:

- 動作中の光源を凝視しないでください。目に有害な場合があります。
 - 適切な遮蔽物や目の保護具がない場合は、安全な距離で、または直接光が当たらない場所でのみライトを点灯してください。
 - 装置の組み立て、設置、メンテナンスの際は、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 ピクセル数

ライブビュー画像で選択され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。

ステップ

1. 機能を有効にするには、 をクリックします。
2. 画像上でマウスをドラッグして、必要な矩形領域を選択します。
幅ピクセルと高さピクセルは、ライブビュー画像の下部に表示されます。

3.1.8 デジタルズーム開始

画像内の任意の領域の詳細情報を見るのに役立つ。

ステップ

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希望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

モーター駆動の装置に使用される。ピントが合わない場合、画像を改善することができる。

ABFをサポートしている機器の場合、レンズの角度を調整し、フォーカスを合わせ、機器のABFボタンをクリックします。機器は明確に焦点を合わせることができます。

自動的にフォーカスを合わせるには、 をクリックします。



注

- 補助フォーカスを使用してもピントが合わない場合は、レンズの初期化を行い、再度補助フォーカスを使用することで、画像を鮮明にすることができます。
 - 補助フォーカスを使用してもピントがはっきりしない場合は、マニュアルフォーカスを使用してください。
-

3.1.10 レンズの初期化

レンズ初期化機能は、電動レンズを搭載した装置で使用します。この機能は、長時間のズームやフォーカスの結果、画像が不鮮明になった場合にレンズをリセットすることができます。この機能は機種によって異なります。

 をクリックしてレンズの初期化を操作します。

3.1.11 レンズパラメーター調整

PTZとは、パン、チルト、ズームの略。それは装置の動きの選択を意味します。ライブビューインターフェイスでは、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実現することができます。



注

- サポートされるPTZ機能は、カメラの機種によって異なる場合があります。
 - レンズの動きのみをサポートする機種では、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、機器をパン/チルトします。

ズーム

- ・  をクリックすると、レンズがズームインする。
- ・  をクリックすると、レンズがズームアウトする。

フォーカス

- ・  をクリックすると、レンズが近くにピントを合わせ、近くの被写体がクリアになります。
- ・  をクリックすると、レンズが遠くまでピントを合わせ、遠くの被写体をはっきり見えるようになります。

アイリス

- ・ 画像が暗すぎる場合は  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ます。

PTZスピード

- ・  をスライドさせて、パン/チルトの移動速度を調整します。

3.1.12 3Dポジショニングの実施

3Dポジショニングは、選択した領域を画像の中心に移動させることである。

ステップ

1. 機能を有効にするには、 をクリックします。
2. ライブ画像でターゲットエリアを選択する。
 - ライブ画像上のポイントを左クリック: ポイントはライブ画像の中央に移動します。拡大縮小の効果はありません。
 - マウスをホールドしたまま右下の位置までドラッグすると、ライブ画像上のエリアがフレーム化されます。フレーム化されたエリアは拡大され、ライブ画像の中央に移動します。
 - マウスを押したまま左上の位置までドラッグして、ライブ画像上の領域を枠で囲みます。枠で囲まれた領域はズームアウトされ、ライブ画像の中央に移動します。
3. 機能をオフにするには、もう一度ボタンをクリックします。

3.2 伝送パラメーターの設定

ネットワーク状況によっては、ライブビュー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に応じて、伝送パラメータを調整することで問題を解決できます。

ステップ

1. 設定 → ローカル → ライブビューパラメーター に移動します。
2. 必要に応じて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を保証し、より良い映像品質を提供しますが、リアルタイム性に影響する場合があります。安定したネットワーク環境に適しています。

UDP

UDP は映像の滑らかさ(フルエンシー)をそれほど要求しない不安定なネットワーク環境に適しています。

MULTICAST

複数のクライアントが存在する状況に適しています。選択前にマルチキャストアドレスを設定する必要があります。



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、サードパーティが機器からストリームを取得する必要がある場合に適している。

再生パフォーマンス

最短遅延

機器は映像のリアルタイム性を、再生の滑らかさよりも優先します。

バランス

機器は映像のリアルタイム性と滑らかさの両方を確保します。

滑らかさ(流暢)

機器は映像の滑らかさを、リアルタイム性よりも優先します。

ネットワーク環境が悪い場合、スムーズ設定を有効にしても、映像の滑らかさを確保できないことがあります。

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は、フレームレートを下げることで、ライブビューを滑らかにできます。

ただし、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 ビデオとオーディオ

本章では、映像および音声に関する各種パラメーターの設定について説明します。

4.1 ビデオ設定

本項では、ストリームの種類、映像のエンコード、解像度などの映像パラメーター設定について説明します。

設定 → ビデオおよび音声 → ビデオ に移動します。

4.1.1 ストリームタイプ

機器が複数のストリームをサポートしている場合は、ストリームタイプごとにパラメーターを指定できます。

メインストリーム

機器が提供する最も高いパフォーマンスのストリームです。通常、機器が対応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、解像度とフレームレートが高いほど、記録に必要なストレージ容量が増え、伝送時の帯域幅要件も高くなります。

サブストリーム

比較的低い解像度の選択肢を提供するストリームで、帯域幅とストレージの消費を抑えられます。

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にも、用途に応じてカスタマイズされたストリームが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コンテンツ(ビデオとオーディオ)を選択します。

ビデオストリーム

ストリームに含まれるのはビデオコンテンツのみ。

ビデオおよびオーディオストリーム

映像コンテンツと音声コンテンツを含む複合ストリームです。

4.1.3 解像度

運用要件に応じて映像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が増加します。

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(CBR)

ストリームが比較的固定されたビットレートで圧縮・送信される方式です。圧縮速度は速い一方、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(VBR)

設定した最大ビットレートの範囲内で、機器が自動的にビットレートを調整する方式です。圧縮速度は定数ビットレートに比べて遅くなりますが、複雑なシーンの画質を維持できます。

4.1.5 ビデオ画質

ビットレートタイプが可変(VBR)の場合に設定可能です。

実運用に応じて映像品質を選択してください。映像品質を高く設定すると、より高い帯域幅が必要になります。

4.1.6 フレームレート

フレームレートは、動画ストリームの更新頻度を示し、単位は fps(frames per second)です。被写体の動きがある場合は、高いフレームレートが有利で、全体の画質を維持しやすくなります。フレームレートが高いほど、必要な帯域幅やストレージ容量も増加します。

4.1.7 ビデオエンコード

機器が映像の圧縮に採用する規格を指します。



利用可能な圧縮規格は機種により異なります。

H.264

H.264(MPEG-4 Part 10, Advanced Video Coding)は圧縮規格の一つです。画質を損なわずに圧縮率を高め、MJPEG や MPEG-4 Part 2 と比べて動画ファイルサイズを縮小します。

H.264+

H.264+は、H.264をベースに改良された圧縮符号化技術です。H.264+を有効にすることで、最大平均ビットレートで HDDの消費量を見積もることができます。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ストレージを最大50%削減します。

H.264+が有効な場合、Max.平均ビットレートは設定可能です。機器はデフォルトで推奨される最大平均ビットレートを提供します。ビデオ画質が満足のいくものでない場合は、パラメーター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ないようにしてください。



H.264+が有効な場合、Iフレーム間隔は設定できません。

H.265

H.265(HEVC: High Efficiency Video Coding、MPEG-H Part 2)は圧縮規格です。
H.264 と比較して、同一の解像度・フレームレート・画質条件で、より高い圧縮効率を実現します。

H.265+

H.265 を基盤とした改良型の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基づいて HDD 消費量を見積もることができます。

多くのシーンで、同じ最大ビットレートの場合、H.265 と比較して最大約 50% のストレージ削減が可能です。

H.265+ 有効時は、最大平均ビットレートを設定できます。デフォルトで推奨値が提示されますが、画質が不十分な場合は値を上げて調整できます。最大平均ビットレートは、最大ビットレートを超えないようにしてください。



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 フレーム間に挟まる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)は他の画像参照なしに独立してデコード可能な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多くのビットを消費します。

そのため、I フレームが多い(=I フレーム間隔が短い)動画は、データビットがより安定・信頼性が高くなる一方で、より多くのストレージ容量を必要とします。

SVC

Scalable Video Coding(SVC)は、H.264 または H.265 の拡張である Annex G を指します。

SVC の目的は、高品質のビデオビットストリームに、1 つ以上のサブセット・ビットストリームを含められるようにすることです。これらのサブセットは、同等量のデータで既存の H.264/H.265 設計と同程度の復元品質・デコード複雑度でデコードできることを目指しています。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間引くことで生成されます。

SVC は旧式ハードウェアへの前方互換性を実現します。同一ビットストリームを、低解像度のサブセットのみをデコードできる基本的なハードウェアでも再生でき、より高性能なハードウェアでは高品質ストリームとしてデコードできます

MPEG4

Moving Picture Experts Group(MPEG)が策定した動画圧縮形式である MPEG-4 Part 2 を指します。

MJPEG

Motion JPEG(M-JPEG または MJPEG)は、イントラフレーム符号化技術を用いる動画圧縮形式です。MJPEG では各フレームが個別の JPEG 画像として圧縮されます。

プロファイル(Profile)

同一ビットレートにおいて、プロファイルが複雑になるほど画像品質は向上しますが、必要とされるネットワーク帯域も増加します。

4.1.8 スムージング

ストリームの滑らかさを指す。スムージングの値が高いほど、ストリームの滑らかさは向上しますが、ビデオの品質はあまり満足のいくものではありません。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、流暢でないように見えるかもしれません。

4.2 音声設定

音声エンコードや環境ノイズフィルターなど、音声に関するパラメーターを設定する機能です。

設定 → ビデオおよび音声 → 音声 に移動します。



本機能は一部の機種のみ対応しています。

4.2.1 音声エンコード

使用する音声の圧縮方式(エンコード方式)を選択します。

4.2.2 音声入力



- 必要に応じてオーディオ入力機器を接続します。
- 音声入力の表示は機種によって異なります。

Line In (ラインイン)	出力が高い音声入力機器(例:MP3 プレーヤー、シンセサイザー、アクティブピックアップ)に接続する場合は、音声入力を を LineIn に設定します。
Mic In (マイクイン)	出力が低い音声入力機器(例:マイク、パッシブピックアップ)に接続する場合は、音声入力を MicIn に設定します。

4.2.3 音声出力



必要に応じて音声出力機器を接続してください。

機器音声出力のスイッチです。無効にすると全ての機器音声が出れなくなります。表示される音声出力の項目は機種により異なります

4.2.4 環境ノイズフィルター

[環境ノイズフィルターを適用中] をOFFまたはONに設定します。

この機能をONにすると、環境中のノイズをある程度低減できます。

4.3 双方向オーディオ

監視センターと監視画面上の対象との間で、双方向の音声通話を実現するために使用します。

始める前に

機器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。接続方法は各音声入出力デバイスの仕様を参照してください。

機器に内蔵マイクとスピーカーがある場合は、双方向音声機能をそのまま有効にできます。

ステップ

1. ライブビューをクリックします。
2. カメラの双方向音声機能を有効にするには、ツールバーの をクリックします。
3. をクリックし、双方向音声機能を無効にします。

4.4 ROI(関心領域)

ROI(関心領域)エンコードは、映像圧縮において ROI と背景情報を区別し、関心領域により多くのエンコード資源を割り当てて画質を向上させる技術です。背景は相対的に重視されません。

4.4.1 ROIの設定

ROI エンコードにより、関心領域に多くのエンコード資源を割り当てて画質を向上させ、背景は相対的に低い画質になります。

始める前に

映像のコーディングタイプを確認してください。ROI は H.264 または H.265 の場合に対応します。

ステップ

1. **設定** → **ビデオおよび音声** → **ROI** に移動します。
2. **有効** をチェックします。
3. **ストリームタイプ**を選択します。
4. **リージョン番号**を選択し、 をクリックして、ライブビュー上にROI 領域を描画する。



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。



ROIレベルが高ければ高いほど、検出された領域の画像は鮮明になります。

-
7. **オプション**:複数の固定領域を描く必要がある場合は、他のリージョン番号を選択し、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

画像をトリミングし、ターゲットエリアの画像のみを送信保存することで、送信帯域幅とストレージを節約することができます。

ステップ

1. 設定 → ビデオおよび音声 → 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」にサードストリーム を設定します。



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ません。

-
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フレームが表示されます。
 4. フレームをターゲットエリアまでドラッグする。
 5. 保存をクリックする。



- ターゲットクロッピングは一部の機種のみ対応し、機種によって機能が異なります。
 - ターゲットクロッピングを有効にすると、いくつかの機能が無効になる場合があります。
-

4.6 複数ストリーム情報表示

映像ストリームに物体(人、車両など)の情報をマークします。接続された後端デバイスまたはクライアントソフトで、ラインクロッシング、侵入などのイベント検知ルールを設定できます。

始める前に

この機能はスマートイベントでサポートされます。**VCA** に移動し、**スマートイベント** を選択して**スマートイベント** を有効化してください。

ステップ

1. 設定 → ビデオおよび音声 → 複数ストリーム情報表示 に移動します。.
2. デュアル VCA を有効化にチェックをします。
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ー設定を提供します。

設定 → 画像 → ディスプレイ設定.に移動します。

「デフォルトに復帰」をクリックすると設定を初期値に復元します。

4.7.1 シーンモード

さまざまな設置環境に合わせて、あらかじめいくつかの画像パラメーター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と、表示設定を素早く行えます。

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、最適な画像表示を実現します。

露光設定

露出は、アイリス、シャッター、感度の組み合わせで制御されます。露出パラメーターを設定して、画像効果を調整できます。

マニュアルモードでは、露光時間、ゲイン、スローシャッターを設定します。

フォーカス

フォーカスモードを調整するためのオプションを提供します。

フォーカスモード

自動

シーンが変わると自動的にピントが合う。オートモードでピントの合った画像が得られない場合は、画像内の光源を減らし、光の点滅を避けてください。

半自動

PTZとレンズのズーミングの後、機器は一度焦点を合わせます。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わりません。

手動

ライブビュー画面で手動でフォーカスを調整します。

デイナイト切替

デイ/ナイト切替機能により、昼夜モードでカラー画像とモノクロ画像を提供します。切替モードは設定可能です。

昼：

画像は常にカラーである。

夜間：

画像は白黒またはカラ-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ライトが有効になります。



注 一部の機種のみが補助照明およびカラフルイメージに対応しています。

自動：

カメラは周囲の明るさに応じてデイモードとナイトモードを切り替える。

スケジュール切替：

開始時刻と終了時刻を設定し、デイモードの期間を定義する。

イベントトリガー：

トリガー状態を昼または夜に設定することができます。例えば、「トリガー状態」が「夜」の場合、機器がアラーム入力信号を受信すると、モードは「夜」に変わります。

映像トリガー：

周囲の明るさに応じて、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、機器が道路交通および車両検出に対応している場合に適用されます。:



- ・ デイナイト切替の機能は、機種によって異なります。
 - ・ より良い画質のため、スマート補助光を有効にできます。補助光の設定については「補助光設定」を参照してください。
-

補助光設定

補助光の設定が可能です。関連パラメーターは実機仕様を参照してください。

スマート補助光

補助光点灯時の白飛び(露出オーバー)を防ぎます。

補助光モード

機器が補助光に対応している場合、補助光モードを選択できます。

IR補助光

IRライトが有効。

白色光

白色光が有効。

ミックスライト

IRライトとホワイトライトの両方が有効。

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、夜間の状態では、デフォルトの補助光モードはIR補助光モードになります。アラームがトリガーされると、白色ライトが有効になり、機器はターゲットを捕捉します。アラーム終了後、補助光モードはIR補助光モードに切り替わります。

IRと白色光、またはIRと白色光のハイブリッド補助光を搭載した機種のみが、この機能をサポートしています。

オフ

補助光は無効です。



補助光モードは、機種により異なる場合があります。

照度コントロール

自動

実際の環境に応じて自動的に明るさを調整します。

手動

スライダー操作または値の入力で明るさを調整します。

BLC

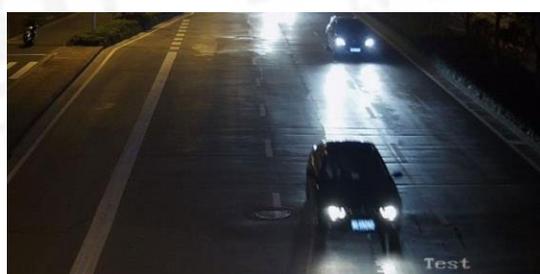
強い逆光でピントを合わせると、暗くてよく見えません。BLC(逆光補正)は、手前の被写体への光を補正して、被写体を鮮明にします。BLCモードがカスタムに設定されている場合、ライブビュー画像上にBLCエリアとして赤い四角形を描くことができます。

WDR

WDR(ワイドダイナミックレンジ)機能は、照度差の激しい環境でも鮮明な画像を提供するのに役立ちます。視野内に非常に明るい部分と非常に暗い部分の両方が同時に存在する場合、WDR機能を有効にし、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バランスを自動的に調整し、細部まで鮮明な画像を提供します。



注 WDRが有効な場合、他の機能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ご参照ください。



WDR Off



WDR On

図4-1 WDR

HLC

画像の明部が白飛びし、暗部が黒つぶれしている場合は、HLC(High Light Compression)機能を有効にすることで、明部を弱め、暗部を明るくし、画面全体の明暗バランスを整えます。

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。環境に合わせて色温度を調整します。



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(DNR)は、画像のノイズを低減し、画質を向上させる機能です。モードは「Normal(標準)」と「Expert(詳細)」から選択できます。

Normal(標準)

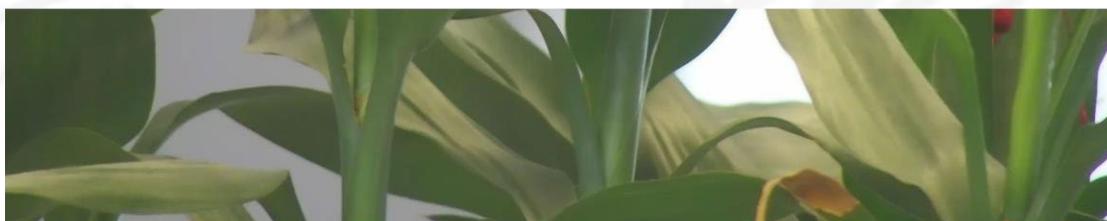
- DNRレベルを設定して、ノイズ低減の度合いを制御します。レベルが高いほど、低減効果が強くなります。

Expert(詳細)

- 空間DNRおよび時間DNRの両方に対してレベルを設定し、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。



DNR Off



DNR On

図4-3 DNR

デフォグ(Defog)

映像が霧がかかっている、もしくは、画像が白けている場合に有効にします。
微細なディテールを強調し、画像をよりクリアに表示します。



Defog Off



Defog On

図4-4 デフォグ

EIS

ジャイター補正技術により、動画画像の安定性を向上させます。

グレースケール

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

ミラー

ライブビュー映像が実際のシーンと左右反転している場合、この機能により映像を通常表示にします。必要に応じてミラーモードを選択する。



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90°反時計回りに回転します。
例えば、1280×720 は、720×1280 に回転します。
この機能を有効にすると、縦方向の監視範囲が変わる場合があります。



本機能は、特定の設定においてのみサポートされます。

レンズ歪み補正

電動レンズ搭載機では、映像が多少歪んで見える場合があります。
この機能を有効にすると歪みが補正されます。



この注機能は、電動レンズを搭載した一部の機器でのみサポートされています。
この機能を有効にすると、画像の端が失われる場合があります。

4.7.2 画像パラメータースイッチ

機器は、設定した時間帯に応じて自動的に画像パラメーターを切り替えます。

次の手順で画像パラメータースイッチ設定ページに移動します：

設定 → 画像 → ディスプレイ設定 → 画像パラメーター切替 で、必要に応じてパラメーターを設定します。

スケジュール切替設定

特定の時間帯に、画像をリンクされたシーンモードへ自動的に切り替えます。

ステップ

1. **○スケジュール切替** にチェックを入れます。
2. 対応する時間帯とリンクされたシーンモードを選択・設定します。



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、表示可能な色数や解像度を定義するビデオカード/表示デバイスの機能です。最も一般的なビデオ規格は NTSC と PAL です。

- ・ NTSC: 毎秒30フレームを送信。各フレームは525本の走査線で構成。
- ・ PAL: 毎秒25フレームを送信。各フレームは625本の走査線で構成。

お住まいの国/地域のビデオシステムに合わせ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

機器にBNC、CVBS、HDMI、SDIなどのビデオ出力インターフェイスが装備されている場合は、機器をモニターに接続してライブ映像を直接プレビューできます。

出力モードをON/OFFで選択し、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ディングモードで、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した場合、特定の対象を望ましいライブビューで表示できるよう、切断線と水平半径の間の角度を調整できます。設定した角度に応じてライブビューが変化します。

1. ライブビュー画面で、ハードウェアデコードモードにて「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 → ディスプレイ設定 → ビデオ設定 に進み、「切断線と水平半径の間の角度」を設定します。

180度のパノラマビュー

角度は0°、30°、60°、90°、120°、180°から選択できます。

30°の角度を例にとると、ライブビューは以下のように変化します:

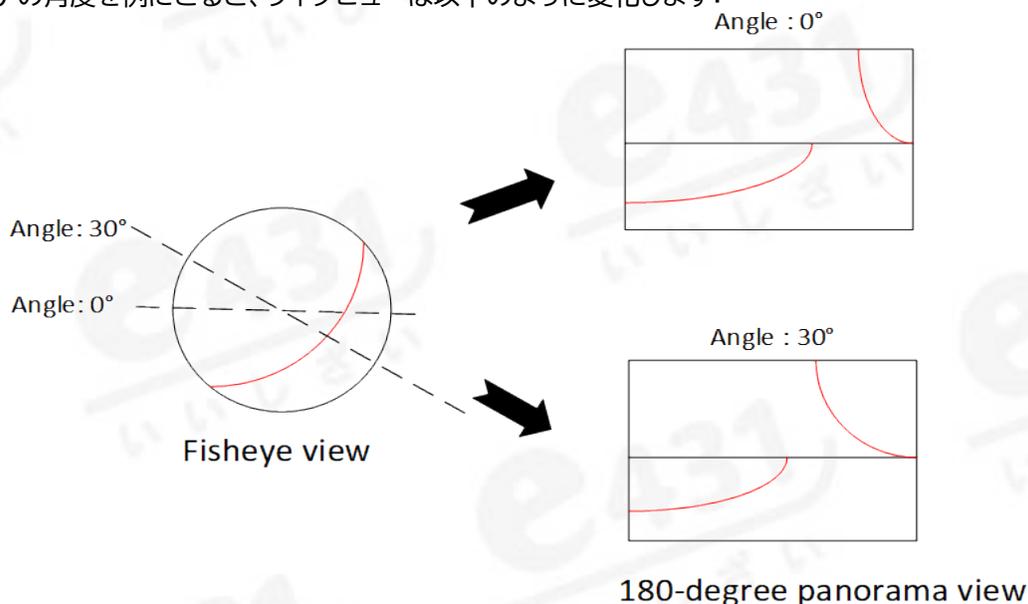


図4-5 180度パノラマビューの角度を設定する



実際のライブビューは、カメラの機種やマウントタイプによって異なります。

4.8 OSD

デバイス名、日時、フォント、色、テキストオーバーレイなど、ビデオストリーム上に表示される OSD 情報をカスタマイズできます。

設定 → 画像 → **OSD設定** に移動します。

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。

キャラクターセット

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

表示

カメラ名、日付、曜日、およびそれらの表示形式を設定します。機種によっては、表示情報としてチルト角を設定できる場合があります。

フォーマット設定

表示モード、OSDフォント、フォント色、位置合わせなどのOSDパラメーターを設定します。

テキストオーバーレイ

画像上にカスタムのオーバーレイテキストを設定します。

「+追加」をクリックして、テキストを追加します。

4.9 プライバシーマスクの設定

この機能は、ライブビュー内の特定領域をブロックしてプライバシーを保護します。
機器がどのように動いても、ブロックされたシーンは表示されません。

ステップ

1. 設定 → 画像 → プライバシーマスク に移動します。
2. 有効をチェックします。
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：領域のサイズを調整します。
領域全体をドラッグ：領域の位置を調整します。
をク  ク：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、リージョン名 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 画像オーバーレイ

ライブビューにカスタマイズした画像を重ねて表示します

始める前に

オーバーレイする画像は **BMP** 形式(24-bit)で、ある必要があります。
最大画像サイズは、128×128ピクセルです。

ステップ

1. 設定 → 画像 → 画像オーバーレイ に進む。
2. 有効をチェックします。
3. “アップロード”をクリックして、写真を選択し、開きます。
アップロードが成功すると、ライブビューに赤い枠付きで画像が表示されます。
4. 赤い枠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

概要

本章では、ビデオ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説明します。

5.1 ストレージ設定

一般的なストレージパスの設定について説明します。

5.1.1 メモリーカード

メモリーカードの容量、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、メモリーカードの暗号化に対応しています。

新規または未暗号化メモリーカードの設定

始める前に

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を機器に挿入します。インストールの詳細については、機器のクイックスタートガイドを参照してください。

ステップ

1. 設定 → ストレージ → ストレージマネジメント → HDD マネジメント に進みます。
2. メモリーカードを選択します。



ロック解除ボタンが表示された場合は、まずメモリーカードのロックを解除する必要があります。詳しくは、[メモリーカードステータスの検出](#)をご覧ください。

-
3. “フォーマット” をクリックしてメモリーカードを初期化します。
メモリーカードのステータスが「未初期化」から「通常」に変われば、使用可能な状態です。
 4. オプション:メモリー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 に変わると、メモリーカードは使用可能な状態になります。



暗号化パスワードは大切に保管してください。忘れた場合、暗号化パスワードの再取得はできません。

-
5. オプション:メモリーカードのクォータ(割り当て)を定義します。ニーズに応じて、異なるコンテンツの保存割合を入力します。
 6. [保存]をクリックします。

暗号化済みメモリーカードの設定

始める前に

- 暗号化済みのメモリーカードを機器に挿入します。詳しい取り付けは、機器のクイックスタートガイドを参照してください。
- メモリーカードの正しい暗号化パスワードを知っておく必要があります。

ステップ

1. 設定 → ストレージ → ストレージマネジメント → HDD マネジメント に進みます。
2. メモリーカードを選択します。



ロック解除ボタンが表示された場合は、まずメモリーカードのロックを解除する必要があります。詳しくは [メモリーカードステータスの検出](#) をご覧ください。

3. 暗号化パスワードを検証します。

- 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になると、メモリーカードは使用可能な状態になります。



暗号化パスワードを忘れ、なおかつこのメモリーカードを使い続けたい場合は、「新規または未暗号化メモリーカードの設定」を参照してフォーマットと再設定を行ってください。既存の内容はすべて削除されます。

4. オプション:メモリーカードのクォータ(割り当て)を定義します。ニーズに応じて、各コンテンツの保存割合(%)を入力します。
5. [保存]をクリックします。

メモリーカードステータスの検出

機器は **特殊メモリーカード**のステータスを検出します。メモリーカードに異常が検出された場合は通知を受け取ります。

始める前に

設定ページは、**特殊メモリーカード**が機器にインストールされている場合にのみ表示されます。

ステップ

1. 設定 → ストレージ → ストレージマネジメント → メモリーカード検出 に進みます。
2. ステータス検出をクリックして、メモリーカードの残り寿命とヘルスステータスを確認します。

残り寿命

- 残り寿命の割合(%)が表示されます。
- メモリーカードの寿命は容量やビットレートなどの要因で左右されます。残り寿命が十分でない場合はメモリーカードを交換してください。

ヘルステータス

- メモリーカードの状態を表示します。
- 警戒スケジュールおよびリンクメソッドが設定されている場合、ヘルステータスが「good(良好)」以外であれば通知が届きます。



ヘルステータスが「good(良好)」でない場合はメモリーカードの交換を推奨します。

3. R/W ロックをクリックし、メモリーカードへの読み書きの許可を設定します。

- ロックをする場合
 - a. ロックスイッチをONにします。
 - b. パスワードを入力します。
 - c. [保存]をクリックします。
- ロック解除
 - メモリーカードをロックした機器上で使用する場合は、ロック解除は自動的に行われるため、ユーザー側での操作は不要です。
 - ロックされたメモリーカードを別の機器で使用する場合は、「HDDマネジメント」から手動でロック解除できます。対象のメモリーカードを選択して「解除」をクリックし、正しいパスワードを入力して解除してください。
- ロックを解除して取り外す場合
 - a. ロックスイッチをOFFにします。
 - 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。



- R/Wロックの設定は管理者(admin)ユーザーのみ行えます。
 - メモリーカードはロック解除されている場合にのみ読み書きが可能です。
 - メモリーカードにロックをかけた機器を工場出荷状態にリセットした場合は、「HDD マネジメント」からメモリーカードを解除してください。
-

4. 「起動スケジュール」と「リンクメソッド」を設定します。詳細は「起動スケジュールとリンクメソッドの設定」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

イベントや定時スナップショットタスクで取得した画像を保存するために、FTPサーバーを設定できます。

始める前に

まずFTPサーバーのアドレスを確認してください。

ステップ

1. 設定 → イベント → アラーム設定 → FTP に移動します。
2. FTP設定を行います。

FTPプロトコル

- ・ FTPとSFTPが選択できます。
- ・ SFTPプロトコルを使用することにより、ファイルのアップロードは暗号化されます。

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。

ユーザー名とパスワード

- ・ 画像をアップロードできる権限を持つ FTP ユーザーを指定してください。
- ・ 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は、アップロード中に機器情報を隠すために「Anonymous Login(匿名ログイン)」をチェックできます。



SFTPプロトコルが選択されている場合、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 サーバー上でスナップショットを保存するパスを指定します。
3. オプション:スナップショットをFTPサーバーにアップロードする場合は、「画像をアップロード」をチェックして有効にします。

画像のファイリング間隔

- ・ 画像管理を容易にするため、画像整理間隔を 1日～30日 の間で設定できます。
- ・ 同じ時間間隔で取得された画像は、開始日と終了日を名前に含む1つのフォルダにまとめて保存されます。

画像ファイル名

- ・ 取得画像の命名規則を設定します。ドロップダウンで Default(デフォルト) を選ぶと、既定ルール(IPアドレス_チャンネル番号_キャプチャ時刻_イベント種類.jpg、例: 10.11.37.189_01_20150917094425492_FACE_DETECTION.jpg)が使われます。
 - ・ また、既定の命名規則に Custom Prefix(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:「ネットワークの自動補充を有効にする」をチェックします。



リンクメソッドでの 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」は、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サーバーの接続を確認します。
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、録画ファイルやキャプチャ画像などを保存出来ます。

始める前に

最初にネットワークディスクのIPアドレスを確認して下さい。

ステップ

1. NAS の設定ページに移動します: **設定** → **ストレージ** → **ストレージマネジメント** → **ネット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。
マウントタイプマウントタイプ
 - ・ 使用している OS に応じてファイルシステムプロトコルを選択してください。
 - ・ **SMB/CIFS**が選択されている場合は、セキュリティ確保のためにNet 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アドレスを入力します。

ファイルパス

ネットワークディスク上の保存先パスを入力します。

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を追加する手順を終了します。
7. オプション:追加後にNet HDDの設定を行います。

編集 パラメーター設定を編集するには、 をクリックします。

削除 Net HDDを削除します。

- ・  をクリックする。
- ・ 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保護機能

eMMC のヘルスステータスが低下したときに、eMMC を記憶媒体としての使用を自動的に停止する機能です。



eMMC保護は、eMMCハードウェアを搭載した一部機種のみでサポートされています。

設定 → **システム** → **システム設定** → **システムサービス** にアクセスして設定を行います。

eMMCはembedded multimedia cardの略で、組み込み型の不揮発性メモリシステムです。機器のキャプチャ画像やビデオを保存することができます。

機器はeMMCの健康状態を監視し、状態が悪くなるとeMMCの電源を切ります。そうでない場合、消耗したeMMCを使用すると、機器の起動に失敗する可能性があります。

5.1.5 クラウドストレージの設定

撮影した画像やデータをクラウドにアップロードする機能です。プラットフォームは画像や解析のためにクラウドから直接画像を要求します。該当機能は一部の機種のみでサポートされています。



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

ステップ

1. 設定 → ストレージ → ストレージマネジメント → 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が使用するプロトコルのバージョンを指定します。
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。
サブポート	クラウドビデオマネージャーのポート番号を入力します。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です。
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です。
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認証情報を入力します。
画像保存プールID	クラウドビデオマネージャーの画像保存領域のIDを指定します。ストレージプールIDとストレージリージョン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

この章では、手動録画およびスケジュール録画、再生、録画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 自動録画の設定

この機能は、設定した時間帯に自動的にビデオを録画することができます。

始める前に

連続を除く各記録タイプについて、イベント設定でトリガー記録を選択します。詳細は[イベントとアラーム](#)を参照してください。

ステップ

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. 録画タイプを選択します。



注 録画タイプは、機種によって異なります。

連続

スケジュールに従って常時録画します。

モーション

動体検知が有効で、リンクメソッドとしてトリガー録画が選択されている場合、対象の動きが検出されると録画します。

アラーム

外部アラーム入力機器からの信号を受けた場合に録画します(アラーム入力有効で、連動方法にトリガー録画が設定されていること)。

モーション| アラーム(モーションまたはアラーム)

動体検知または外部アラーム入力機器からの信号のいずれかがあったときに録画します。

モーション&アラーム(モーションかつアラーム)

動体検知があり、かつ外部アラーム入力機器からアラーム信号を受信した場合のみ、録画します。

イベント

設定したイベントが検出されたときに録画します。

4. 選択した録画タイプのスケジュールを設定します。設定操作は「起動スケジュールの設定」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

ストレージ容量がいっぱいになったときに録画ファイルを上書きする場合は「上書きを有効化」をオンにしてください。無効にすると新しい録画ができなくなります。

事前記録

スケジュール開始前に遡って録画する時間(秒または設定単位)を指定します。

事後記録

スケジュール終了後に録画を継続する時間を指定します。

ストリームタイプ

録画に使用するストリーム(メイン/サブ等)を選択します。



高いビットレートのストリームを選択した場合、実際の事前記録/事後記録の時間は設定値より短くなることがあります。

録画期限

録画ファイルは設定した保存期限を超えると削除されます。期限は設定可能です。削除された録画は復元できない点にご注意ください。

6. [保存] をクリックします。

5.2.2 手動録画の設定

ステップ

1. 設定 → ローカル に移動します。
2. 録画するビデオファイルの「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. ライブビュー画面の  をクリックすると録画が開始されます。録画を停止するには、 をクリックします。

次に行うこと

録画したビデオファイルを確認します。

設定 → ローカル に移動し、「ビデオ保存パス」の後ろにある「開く」をクリックして、保存先を開き、ファイルを確認します。

5.2.3 ビデオの再生とダウンロード

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

ステップ

1. 再生 → ビデオ 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。
条件に合致した動画ファイルはタイミングバー上に表示されます。
3.  をクリックしてしてビデオファイルを再生します。
 をクリックすると全画面で再生します。**ESC**キーを押してフルスクリーンを終了します。
 をクリックすると、全チャンネルのビデオ再生を停止します。
4. オプション:ビデオファイルをクリップするには、 をクリックします。ビデオファイルのクリップを停止するには、再度  をクリックします。



クリップした動画ファイルの保存先は「設定」→「ローカル」→「クリップ保存パス」で確認・変更できます。

5. オプション:再生画面上的の  アイコンをクリックしてファイルをダウンロードします



ダウンロードした動画ファイルの保存先は「設定」→「ローカル」→「ダウンロード保存パス」で確認・変更できます。

5.3 キャプチャ構成

本機は手動または自動で静止画をキャプチャして、設定された保存パスに保存できます。保存されたスナップショットは参照および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、設定した時間帯に自動で静止画をキャプチャ(取得)します。

始める前に

イベントによるトリガーでキャプチャを行う場合は、イベント設定で関連するリンクメソッドを設定してください。イベント設定の詳細は「イベントとアラーム」を参照してください。

ステップ

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. キャプチャスケジュールを設定します。スケジュール時間の設定については、起動スケジュールの設定を参照してください。

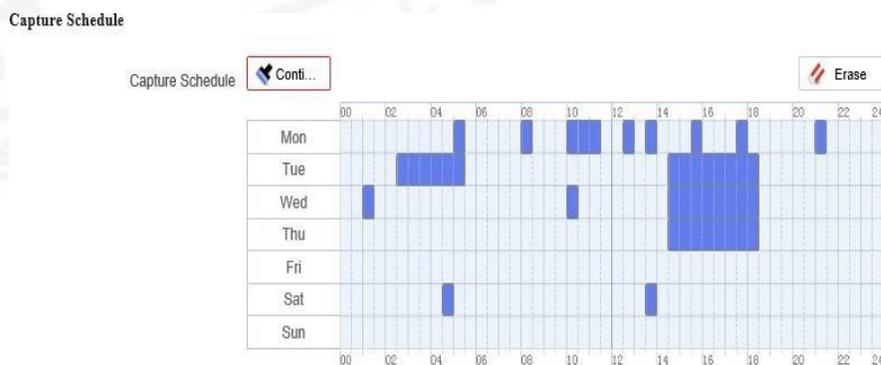


図5-1 キャプチャスケジュールの設定

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

イベントがトリガーされたときに写真をキャプチャします。

4. フォーマット、解像度、画質、間隔、キャプチャ枚数を設定します。



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。ストリームの種類は、「詳細」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 手動キャプチャ

ステップ

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フォーマットと保存パスを設定します。

JPEG

ファイルサイズが比較的小さく、ネットワーク転送に適しています。

BMP

圧縮率が低く、画質が良好な形式です。

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  をクリックすると、手動で画像をキャプチャできます。

5.3.3 写真を見るダウンロードする

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。

ステップ

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。
 - 条件に合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。
 - ダウンロードする画像を選択してから、「ダウンロード」をクリックしてダウンロードします。
 - 現在表示中のページ内の画像をダウンロードするには、「このページをダウンロード」をクリックします。
 - すべての画像を一括でダウンロードするには、「すべてダウンロード」をクリックします。



再生時に表示されるキャプチャ画像の保存パスは、設定 → ローカル → 再生キャプチャ保存パスで確認・変更できます。

第6章 イベントとアラーム

本章ではイベントの設定について説明します。機器はトリガーされたアラームに対して所定の動作を行います。機種によっては一部のイベントがサポートされない場合があります。

6.1 モーション検知の設定

検出領域内の移動物体を検出し、連動動作をトリガーするための機能です。

ステップ

1. 設定 → イベント → イベントと検出 → 動体検知 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: 移動物体を画像上で緑色に表示する場合は、「ハイライト」を有効にします。
 - 1) 「動体解析を有効にする」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ーを設定します。
 - ノーマルモードの説明は、[ノーマルモード](#) を参照してください。
 - エキスパートモードの説明は、[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リンクージ方法を設定します。警戒スケジュールの設定については、[アーミングスケジュールの設定](#) を参照してください。リンクメソッドについては、[リンクメソッドの設定](#) 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ーを設定できます。

ステップ

1. 構成 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。

オートスイッチ

周囲環境に応じてシステムが昼夜モードを自動で切り替えます。昼はカラー画像、夜は白黒画像を表示します。

スケジュール切替

設定した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、その他の期間は夜モードになります

感度

感度の値が高いほど、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な場合、昼と夜の感度を別々に設定できます。

- 領域を選択し、 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、マウスを離すと一つの検知エリアを描画できます。



図6-1 ルールの設定

- すべての領域をクリアするには、 をクリックします。
- [保存]をクリックします。
- オプション:複数のエリアを設定するには、上記の手順を繰り返します。

6.1.2 ノーマルモード

機器のデフォルトパラメーターに従って、動体検知のパラメーターを設定できます。

ステップ

- 設定 で、ノーマルモード を選択する。
- ノーマル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、動体検知および動体解析は有効になりません。
-  をクリックします。ライブ映像上でマウスをクリックしてドラッグし、領域を描画したら右クリックして1つの領域の描画を完了します。
- オプション:すべての領域をクリアするには、 をクリックします。
- 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ーを設定することができます。

6.2 ビデオタンパリングアラームの設定

設定した領域が覆われて通常監視できない状態になったとき、アラームが作動し機器が所定のアラーム応答動作を行います。

ステップ

1. 設定 → イベント → イベントと検知 → タンパリングアラーム に移動します。
2. 有効 をオンにします。
3. 感度 を設定します。数値が高いほど、領域の覆われを検出しやすくなります。
4.  をクリックし、ライブビューでマウスをドラッグして領域を描画します。

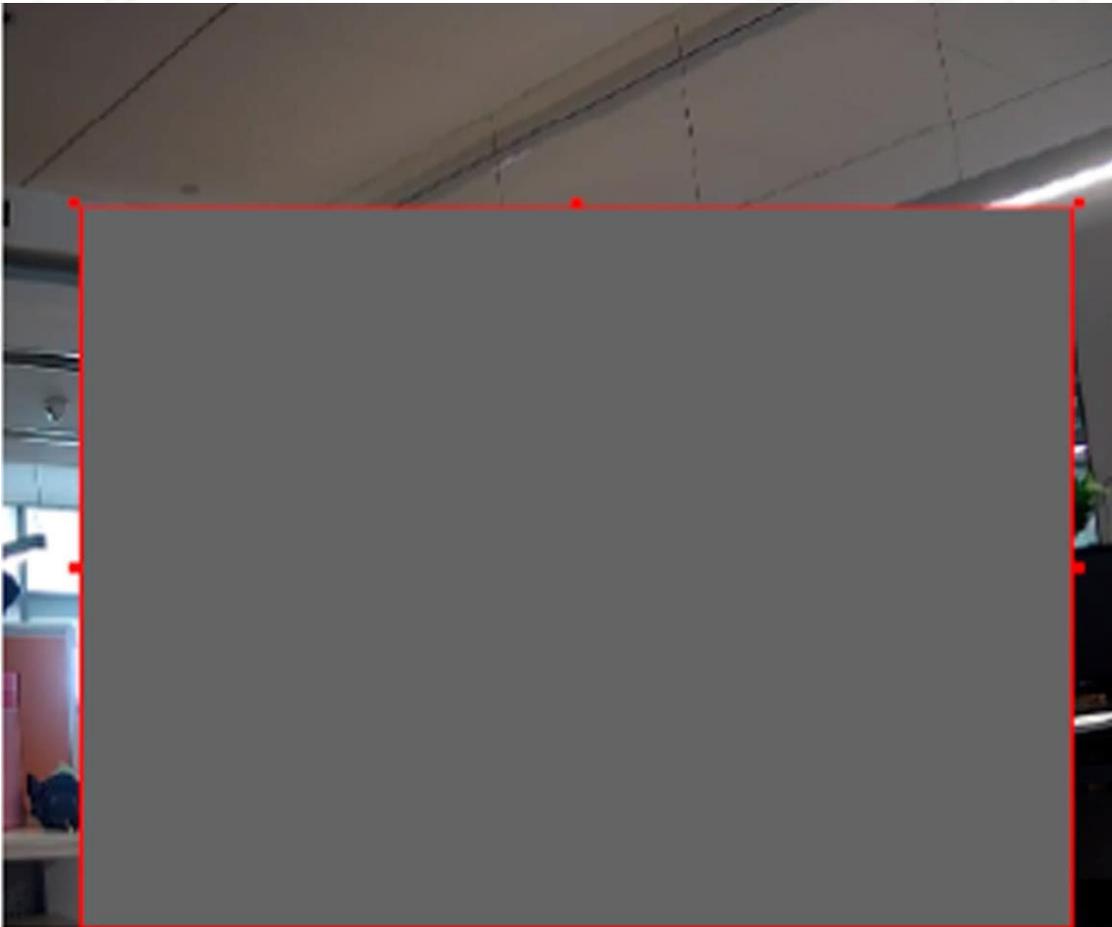


図6-2 ビデオタンパリングアラーム領域の設定

5. オプション:描画したすべての領域を削除するには、 をクリックします。
6. スケジュールされた時間を設定するには、「[警戒スケジュールの設定](#)」を参照してください。リンクメソッドを設定するには「[リンクメソッドの設定](#)」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

外部機器からのアラーム信号により、本機が対応する動作を実行します。

始める前に



本機能は、一部の機種でのみサポートされています。

外部アラーム機器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。

ステップ

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 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化 にチェックを入れます。
5. スケジュールされた時間を設定するには、「[警戒スケジュールの設定](#)」を参照してください。リンクメロッドを設定するには「[リンクメロッドの設定](#)」を参照してください。
6. コピー先に... 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出来ます。
7. [保存] をクリックします。

6.4 異常アラームの設定

ネットワーク切断などの例外(異常)が発生したときに、本機が対応する動作を実行します。

ステップ

1. 設定 → イベント → イベントと検知 → 異常 に移動します。
2. 例外の種類を選択してください。

HDDフル

HDDストレージがいっぱいです。

HDDエラー

HDDにエラーが発生した。

ネットワーク切断中

ネットワークが切断された。

IPアドレスの競合

現在の機器のIPアドレスは、ネットワーク内の他の機器のIPアドレスと同じです。

不正なログイン

ユーザー名またはパスワードが正しく入力されていない。

異常な再起動

機器が異常に再起動する。

3. リンクメソッドの設定については、「[リンクメソッドの設定](#)」を参照してください。
4. [保存]をクリックします。

6.5 ビデオ画質診断の設定

映像品質に異常があり、アラーム連動が設定されている場合に、自動的にアラームが作動します。

ステップ

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. 以下の対応パラメーターを設定します。

アラーム検出間隔

例外を検出するための時間間隔。

感度

この値が高ければ高いほど、例外が発見されやすくなり、誤報の可能性が高くなります。

アラーム遅延時間

設定した回数に達したときに機器がアラームを送信します。

4. 選択した診断タイプにチェックを入れると、そのタイプに応じた検出が行われます。
5. 警戒スケジュールの設定は「[警戒スケジュールの設定](#)」を参照してください。
6. リンクメソッドの設定については、「[リンクメソッドの設定](#)」を参照してください。
7. [保存]をクリックします。



本機能は、一部の機種でのみサポートされています。実際の表示は機種により異なります。

6.6 振動検知の設定

機器が振動しているかどうかを検出するための機能です。本機能を有効にすると、振動を検知してアラーム報知および連動動作を実行します。

ステップ

1. 設定 → イベント → イベントと検知 → 振動検知 に移動します。
2. 有効にする にチェックをいれます。
3. スライダーをドラッグして検知感度を設定します。数値を入力して感度を設定することもできます。
4. 警戒スケジュールの設定は「[警戒スケジュールの設定](#)」を参照してください。
5. リンクメソッドの設定については、「[リンクメソッドの設定](#)」を参照してください。
6. [保存]をクリックします。



本機能は一部の機種でのみサポートされています。実際の表示は機種により異なります。

6.7 オーディオ異常検知の設定

音声異常検知は、シーン内の異常な音(音量の急激な増加・減少など)を検出し、検出時に所定の応答動作を実行する機能です。

ステップ

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つまたは複数の音声異常検知タイプを選択します。

オーディオロス検知

オーディオトラックの突然の損失を検出します。

音量急増検知

急激な音の強さの増加を検出します。感度と音量閾値を設定できます。



- ・ 感度が低いほど、検出が発生するためにはより大きな変化が必要になります。
- ・ 音量閾値は検出の参照となる音量レベルです。周囲の平均音量に合わせて設定することを推奨します。環境音が大きいかほど閾値は高く設定してください。実環境に応じて調整できます。

音量急低下検知

音量の急激な減少を検出します。感度を設定できます。

3. 警戒スケジュールの設定は「[警戒スケジュールの設定](#)」を参照してください。リンクメソッドの設定については、「[リンクメソッドの設定](#)」を参照してください
4. [保存]をクリックします。



本機能は、一部の機種でのみサポートされています。実際の機能は機種により異なります。

6.8 デフォーカス検知の設定

レンズのピントずれにより映像がぼやけた場合に検出できます。検出時に機器が連動動作を実行できます。

ステップ

1. 設定 → イベント → イベントと検知 → デフォーカス検知 に移動します。
2. 有効にする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、ピントずれによるぼやけ映像でアラームが発生しやすくなります。実際の設置環境に合わせて調整してください。
4. リンクメソッドの設定については、[「リンクメソッドの設定」](#)を参照してください。
5. 保存をクリックする。



注
本機能は一部の機種でのみサポートされています。実際の表示は機種により異なります。

6.9 シーンチェンジ検知の設定

本機能は、シーン(映像内容)の変化を検出する機能です。検出時に所定の応答動作を行えます。

ステップ

1. 設定 → イベント → イベントと検知 → シーンチェンジ検知 に移動します。
2. 有効にする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、シーンの変化を検出しやすくなります。ただし、検出の精度は低下する可能性があります。
4. 警戒スケジュールの設定は[「警戒スケジュールの設定」](#)を参照してください。リンクメソッドの設定については、[「リンクメソッドの設定」](#)を参照してください。
5. [保存]をクリックします。



注
本機能は一部の機種でのみサポートされています。実際の表示は機種により異なります。

第7章 警戒スケジュールとアラーム連動

警戒スケジュールは、機器が特定の動作を行うようにカスタマイズされた時間帯のことです。アラーム連動とは、スケジュールされた時間内に検知された特定の事象や対象に対する応答を指します。

7.1 警戒スケジュールの設定

機器の動作が有効となる時間を設定します。

ステップ

1. オプション:関連イベント画面で「警戒スケジュール」と「リンクメソッド」をクリックします。
2. 警戒スケジュール の右の「編集」をクリックする。
3. 描画 をクリックし、タイムバーをドラッグして希望の有効時間を描画します。



- 各セルは30分を表します。
- 描画した時間帯の上にマウスを移動すると、具体的な時間帯が表示され、開始時刻と終了時刻を微調整できます。
- 1日に最大8つの期間を設定できる。

4. 消去をクリックし、タイムバーをドラッグして選択した有効時間を消去します。
5. OKをクリックして設定を保存します。

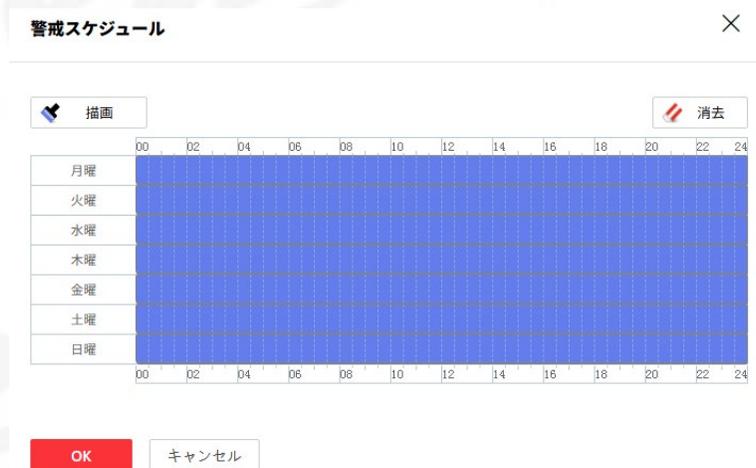


図 7-1 警戒スケジュールの設定

7.2 リンクメソッドの設定

イベントやアラーム発生時に連携機能を有効にすることができます。

7.2.1 トリガーアラーム出力

機器がアラーム出力装置に接続され、アラーム出力番号が設定されている場合、アラームが発生すると機器は接続されたアラーム出力装置へアラーム情報を送信します。

ステップ

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ーを設定します。

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 コンフィギュレーションについては、手動アラームを参照してください。

手動アラーム

手動でアラーム出力をトリガーできます。

始める前に

アラーム出力装置が機器に接続されていることを確認してください。

ステップ

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ーを設定します。
アラーム名
アラーム出力の名前をカスタム設定します。
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:手動アラーム出力を無効にするには、[アラームを解除]をクリックします。

自動アラーム

自動アラームパラメーターを設定すると、設定された警戒スケジュール内で機器が自動的にアラーム出力をトリガーします。

始める前に

アラーム出力装置が接続されていることを確認してください。

ステップ

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ーを設定します。

アラーム名

アラーム出力の名前をカスタム設定します。

遅延

アラーム発生後にアラーム出力が維持される時間の長さを指します。

2. 警戒スケジュールを設定します。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。
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/メモリーカードへのアップロード

FTP/NAS/メモリーカードのアップロードを有効にして設定した場合、アラームが発生すると機器は、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(NAS)、およびメモリーカードへ送信します。

FTPサーバーを設定するには、「[FTPを設定する](#)」を参照してください。

NASの設定については、「[NASを設定する](#)」を参照してください。

メモリーカードの保存の設定については、「[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](#)」を参照してください。

7.2.3 メール送信

電子メールを送信 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機器は指定したアドレスへアラーム情報を添えてメールを送信します。

電子メールの設定については、[電子メールの設定](#)を参照してください。

電子メールの設定

電子メールが設定され、リンクメソッドとして「電子メールを送信」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、機器は指定されたすべての受信者に電子メール通知を送信します。

始める前に

Eメール機能を使用する前にDNSサーバーを設定します。

DNSの設定は、[設定](#) → [ネットワーク](#) → [ネットワーク設定](#) → [TCP/IP](#) に移動します。

ステップ

1. メールの設定ページに移動します：[設定](#) → [イベント](#) → [アラーム設定](#) → [Email](#)

2. マールのパラメーターを設定します。

1) 送信者のメール情報(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は、「[認証方式](#)」にチェックを入れ、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) マールの暗号化方式を設定します。

- [TLS](#) を選択し、[STARTTLS](#) を無効にした場合は、TLSで暗号化されてメールが送信されます。[SMTPポート](#)は、[465](#)に設定してください。

- [TLS](#) を選択し、[STARTTLS](#)を有効化 にチェックを入れた場合は、[STARTTLS](#)で暗号化されてメールが送信されます。[SMTPポート](#)は[25](#)に設定してください。



- 注
- [STARTTLS](#) を使用する場合は、メールサーバーがこの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 [STARTTLS](#) をサポートしていない状態で「[STARTTLS](#)を有効化」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:アラーム時の画像付き通知を受け取りたい場合は、[添付画像] をオンにします。
通知メールには、イベントに関する一定数のアラーム画像が添付され、画像の取得間隔は設定可能です。



添付されるアラーム画像の枚数は、機種やイベントの種類により異なる場合があります。

- 5) 受信者の情報(受信者名およびメールアドレス)を入力します。
6) 機能が正しく設定されているかどうかを確認するには、「テスト」をクリックします。

3. [保存]をクリックします。

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たときに、アラーム情報が監視センターにアップロードされます。

7.2.5 トリガー録画

トリガー録画をオンにすると、機器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 警告音

音声警告を有効にし、音声アラーム出力を設定すると、機器の内蔵スピーカーまたは接続された外部スピーカーがアラーム発生時に警告音を再生します。音声アラーム出力の設定については、[音声アラーム出力の設定](#) を参照してください。



本機能は一部の機種でのみサポートされています

音声アラーム出力の設定

機器が検出領域内で対象を検出した場合、警告として音声アラームをトリガーできます。

ステップ

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. 「音声種別」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、必要な鳴動回数を設定します。
 - 警告を選択し、その内容を設定します。必要な鳴動回数を設定します。
 - カスタムオーディオを選択すると、ドロップダウンリストからカスタム音声ファイルを選べます。ファイルがない場合は、「編集」→「+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。最大で3つの音声ファイルをアップロードできます。
3. オプション: 選択したオーディオファイルを機器で再生するには、[テスト]をクリックします。
4. 音声アラームの警戒スケジュールを設定します。詳細は、「[警戒スケジュールを設定する](#)」を参照してください。
5. [保存]をクリックします。



本機能は一部の機種でのみサポートされています

7.2.7 アラームサーバー

機器は HTTP、HTTPS、または ISUP プロトコルを通じて宛先の IP アドレスまたはホスト名へアラームを送信できます。宛先の IP アドレスまたはホスト名は HTTP、HTTPS、または ISUP による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

ステップ

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. 送信先の IP またはホスト名、URL、ポート番号を入力します。
3. プロトコルタイプ を選択します。



HTTP、HTTPS、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 の使用を推奨します。

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 の設定

TCP/IP 設定は、ネットワーク経由で機器を操作する前に正しく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おり、両バージョンを同時に設定しても互いに干渉しません。

パラメーターの設定は、設定 → ネットワーク → ネットワーク設定 → TCP/IP に移動します。

NICタイプ

ネットワーク状況に応じてNIC(Network Interface Card)のタイプを選択します。

IPv4

IPv4には2つのモードがあります。

DHCP

DHCPにチェックを入れると、機器は自動的にネットワークからIPv4パラメーターを取得します。本機能を有効にすると、機器の IP アドレスは変更されます。機器の IP アドレスは SADP を使って確認できます。

 注 機器が接続されるネットワークは DHCP(Dynamic Host Configuration Protocol) をサポートしている必要があります。

手動

機器の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、および 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

IPv6には3つのモードがあります。

ルートの広告

IPv6アドレスは、ルート広告と機器のMacアドレスを組み合わせで生成される。

 注 ルート広告モードは、機器が接続され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 Address、IPv6 Subnet、IPv6 Default Gateway 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相談してください

MTU

MTU は Maximum Transmission Unit の略で、単一のネットワーク層トランザクションで送受信できる最大のプロトコルデータ単位のサイズを指します。

MTU の有効範囲は 1280 ~ 1500 です。

DNS

DNS は Domain Name Server の略です。ドメイン名で機器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)で必要になります。必要に応じてメイン DNS サーバー と A サブ DNS サーバー を適切に設定してください。

ドメイン名設定

ダイナミックドメイン名の有効化にチェックを入れ、ドメイン名の登録 を入力します。これにより、機器は登録ドメイン名でローカルエリアネットワーク内で管理しやすく登録されます。



ダイナミックドメイン名を有効にするには DHCP を有効にする必要があります。

8.2 ドメイン名による機器へのアクセス

ダイナミックDNS(DDNS)を使用してネットワーク経由でアクセスできます。機器の動的 IP アドレスをドメイン名解決サーバーに紐づけることで、ドメイン名を使ったネットワークアクセスを実現します。

始める前に

DDNS サーバーへの登録が必要です。機器の DDNS 設定を行う前に登録を完了してください。

ステップ

1. DNS パラメーターを設定するには **TCP/IP** を参照してください。
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** をチェックし、**DDNS タイプ** を選択します。

DynDNS

ドメイン名解決に ダイナミックDNS サーバーを使用します。

NO-IP

ドメイン名解決に NO-IP サーバーを使用します。

4. ドメイン名情報を入力し、[保存]をクリックします。
5. 機器のポートを確認し、ポートマッピングを完了させます。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. 機器へアクセスします。

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機器にアクセスします。

クライアントソフトから クライアントソフトにドメイン名を追加します。

追加方法の詳細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機器へのアクセス

本機は PPPoE 自動ダイヤルアップ機能をサポートしています。機器がモデムに接続された後、ADSL ダイヤルアップにより機器はグローバル(パブリック)IP アドレスを取得します。機器の PPPoE パラメーターを設定する必要があります。

ステップ

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 にチェックを入れます。
3. PPPoE パラメーターを設定する。

動的デバイスIPアドレス

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

ダイヤルアップ接続用のユーザー名を入力します。

パスワード

ダイヤルアップ接続用のパスワードを入力します。

パスワード確認

ダイヤルアップ接続用のパスワードをもう一度入力します。

4. [保存]をクリックします。
5. 機器へアクセスします。

ブラウザから ブラウザのアドレスバーにWANダイナミックIPアドレスを入力し、機器にアクセスします。

クライアントソフトから クライアントソフトウェアにWAN ダイナミックIP アドレスを追加します。
詳細はクライアントのマニュアルを参照してください。



注
取得される IP アドレスは PPPoE により動的に割り当てられるため、カメラを再起動すると IP アドレスが常に変わります。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してください。詳細は「8.2 ドメイン名による機器へのアクセス」を参照してください。

8.4 SNMPの設定

ネットワーク管理で機器情報を取得するために、SNMP(Simple Network Management Protocol)を設定できます。

始める前に

SNMP を設定する前に、SNMP ソフトウェアをダウンロードして、SNMP ポート経由で機器情報を受信できるように準備してください。

ステップ

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 有効、SNMP v2cを有効化、または SNMPv3 有効 にチェックを入れます。



注
選択する SNMP バージョンは、使用する SNMP ソフトウェアと同じである必要があります。また、求められるセキュリティレベルに応じて適切なバージョンを選んでください。SNMP v1 は安全性が低く、SNMP v2c はアクセスにパスワードが必要です。SNMP v3 は暗号化を提供し、SNMP v3 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の設定を構成します。
4. [保存]をクリックします。

8.5 IEEE 802.1Xの設定

IEEE802.1Xを設定することで、接続機器のユーザー権限を認証することができます。

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。

ルーターの情報に従って、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
プロトコルをEAP-TLS に設定した場合は、クライアント証明書とCA証明書を選択してください。
機能に異常がある場合は、証明書管理で選択した証明書に問題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のに役立ちます。



注
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。

ステップ

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
ネットワークはデータ送信の優先度を識別できます。DSCP 値が大きいほど優先度は高くなります。
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)の設定

HTTP はハイパーメディア文書を送受信するためのアプリケーション層プロトコルです。
HTTPS は通信の暗号化と本人確認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高めます。

ステップ

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。



これはブラウザが機器へアクセスする際に使用するポートを指します。例えば HTTP Port を 81 に変更した場合、ブラウザでログインするには `http://192.168.1.64:81` のようにポートを指定してアクセスする必要があります。

-
3. **HTTPS** で有効 にチェックをいれます。



TLS 設定 をクリックすると、機器がサポートするTLSバージョンを設定できます。詳細は該当項目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 プロトコル経由でのみ機器にアクセスするには、**HTTPS ブラウジングを有効化**にチェックを入れます。
 6. **サーバー証明書**を選択します。
 7. HTTP(S)認証を設定します。

認証モード

ダイジェスト認証とダイジェスト/ベーシック認証に対応しており、WEB リクエストを機器に送信する際に認証情報が必要です。ダイジェスト/ベーシックを選択した場合は、機器が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、機器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 認証で使用する暗号化アルゴリズムとして MD5、SHA256、MD5/SHA256 が選択できます。MD5 以外のダイジェストアルゴリズムを有効にすると、互換性の問題でサードパーティプラットフォームが機器へログインできない、あるいはライブビューが有効にならない場合があります。より強力な暗号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機器グループに同時に向けられるグループ通信方式です。

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 に移動して行ってください。

IPアドレス

マルチキャストホストのアドレスを指します。

8.8.1 マルチキャスト検出

設定 → ネットワーク → ネットワークサービス → TCP/IPにアクセスして、この機能を有効にします。

「マルチキャスト検出を有効化」にチェックを入れると、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オンラインのネットワークカメラを自動検出できるようになります。

8.9 RTSPの設定

RTSP(Real Time Streaming Protocol)は、ストリーミングメディアを制御するためのアプリケーション層プロトコルです。

ステップ

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

マルチキャストのソースとなるストリームタイプを指定します。

ビデオポート

選択したストリームのビデオポートを指定します。

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を指定します。

4. RTSP認証を設定します。

認証モード

digest と digest/basic がサポートされており、RTSP リクエストを機器へ送信する際に認証情報が必要になります。digest/basic を選択すると機器は digest または basic 認証をサポートします。digest を選択すると機器は digest 認証のみをサポートします。

ダイジェストアルゴリズム

RTSP 認証で使用する暗号化アルゴリズムとして MD5、SHA256、MD5/SHA256 が選択できます。MD5 以外のダイジェストアルゴリズムを有効にすると、互換性の問題によりサードパーティのプラットフォームが機器にログインできない、あるいはライブビューが利用できない可能性があります。強度の高い暗号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

SRTP(Secure Real-time Transport Protocol)は、RTP(Real-time Transport Protocol)に対して暗号化、メッセージ認証と整合性、リプレイ攻撃対策を提供するためのインターネットプロトコルで、ユニキャストおよびマルチキャストの両方の用途で RTP データを保護します。

ステップ

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ーを設定します。

ストリームタイプ

マルチキャストのソースとなるストリームタイプを指定します。

ビデオポート

選択したストリームのビデオポートを指定します。

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を指定します。

4. サーバー証明書 を選択します。
5. 暗号化アルゴリズム を選択する。
6. [保存]をクリックします。



- 一部の機器モデルのみ本機能をサポートします。
 - 機能に異常がある場合は、Certificate Management(証明書管理)で選択した証明書に問題がないか確認してください。
-

8.11 Bonjourの設定

Bonjour はゼロコンフィギュレーションネットワークング(zeroconf)の実装であり、サービス探索、アドレス割り当て、ホスト名解決などの技術群を含みます。Bonjour はマルチキャスト DNS(mDNS) サービスレコードを使用して、プリンターや他のコンピュータ、及びそれら機器が提供するサービスをローカルネットワーク上で検出します。

設定 → ネットワーク → ネットワークサービス → Bonjourに移動して機能を有効にし、[保存]をクリックしてください。

機能を有効にすると、機器はローカルエリアネットワーク内でサービス情報を配信および受信します。

8.12 WebSocket(s)の設定

Google Chrome 57 以降、または Mozilla Firefox 52 以降のバージョンで機器を閲覧する場合、WebSocket または WebSockets プロトコルを有効にする必要があります。これを有効にしないと、ライブビュー、画像キャプチャ、デジタルズームなどが利用できません。

パラメーター設定は、**設定** → **ネットワーク** → **ネットワークサービス** → **WebSocket(s)** に移動して行き、「保存」をクリックしてください。

WebSocket

HTTP プロトコル経由でプラグイン不要のプレビューを行うための、TCP ベースの全二重通信プロトコル用ポートです。

WebSockets

HTTPS プロトコル経由でプラグイン不要のプレビューを行うための、TCP ベースの全二重通信プロトコル用ポートです。

8.13 ポートマッピングの設定

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機器にアクセスすることができます。

ステップ

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

ステップ

1. **UPnP™**を有効化 にチェックを入れ、カメラのフレンドリ名を選択するか、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 **自動** に設定します。
3. [保存]をクリックします。



ルーター側でも UPnP™ 機能が有効になっている必要があります。

8.13.2 手動ポートマッピングの設定

ステップ

1. **UPnP™**を有効化 にチェックを入れ、機器のフレンドリ名を選択するか、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番号に設定します。
3. [保存]をクリックします。

次に行うこと

ルーターのポートマッピング設定画面に移動し、機器側で設定したポート番号と IP アドレスと同じ値をルーター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 ルーターにポートマッピングを設定する

以下の設定例は特定のルーター向けのものであり、ルーターの機種によって設定方法は異なります。

ステップ

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、およびその他のネットワークパラメーターを設定します。
3. Forwarding → Virtual Servers に進み、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、以下のように設定できます。

- カメラ A(IP: 192.168.1.23)のポート:80、8000、554
- カメラ B(IP: 192.168.1.24)のポート:81、8001、555、8201。

108M Wireless Router
Model No.: TL-WR641G / TL-WR642G

- Status
- Quick Setup
- Basic Settings ---
- + Network
- + Wireless
- Advanced Settings ---
- + DHCP
- Forwarding
 - Virtual Servers
 - Port Triggering
 - DMZ
 - UPnP
- + Security
 - Static Routing
 - Dynamic DNS
- Maintenance ---
- + System Tools

Virtual Servers

ID	Service Port	IP Address	Protocol	Enable
1	80	192.168.10.23	ALL	<input checked="" type="checkbox"/>
2	8000	192.168.10.23	ALL	<input checked="" type="checkbox"/>
3	554	192.168.10.23	ALL	<input checked="" type="checkbox"/>
4	8200	192.168.10.23	ALL	<input checked="" type="checkbox"/>
5	81	192.168.10.24	ALL	<input checked="" type="checkbox"/>
6	8001	192.168.10.24	ALL	<input checked="" type="checkbox"/>
7	555	192.168.10.24	ALL	<input checked="" type="checkbox"/>
8	8201	192.168.10.24	ALL	<input checked="" type="checkbox"/>

Common Service Port: DNS(53) Copy to ID 1

Previous Next Clear All Save

図8-1 ルーターのポートマッピング



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いけません。例えば、ルーターの管理用 Web 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カメラのポート番号を変更してください。

8.14 SIP

SIP(Session Initiation Protocol)は、音声、映像、メッセージングなど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。「保存」をクリックして設定を保存し、SIPサーバーに機器を登録します。ウィンドウを更新し、機器が登録されたかどうかを確認してください。

8.15 ISUPの設定

機器が 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機器へのアクセスや管理、データ送信、アラーム情報の転送が可能になります。

ステップ

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. プロトコルのバージョンを選択し、関連するパラメーターを入力します。
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 Guarding Vision経由でカメラにアクセス

Guarding Visionはモバイル端末向けアプリケーションです。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行えます。

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ます。

ステップ

1. 以下の方法でGuarding Vision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://e-camera.net/>にアクセスし、ソフトウェア → スマートフォンアプリケーション からお使いのスマートフォンのシステムに合わせてアプリケーションをダウンロードしてください。
2. アプリケーションを起動し、Guarding Visionユーザーアカウントに登録します。
3. 登録後、ログインしてください。
4. アプリで右上の「+」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にに記載されているか、カメラ同梱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. 画面の指示に従ってネットワーク接続を設定し、Guarding Visionアカウントにカメラを追加します。

8.16.1 カメラのGuarding Visionサービスを有効にする

Guarding Visionサービスを使用する前に、カメラでGuarding Vision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にすることができます。

WebブラウザからGuarding Visionサービスを有効にする方法

以下の手順で、Webブラウザ経由でGuarding Visionサービスを有効にします。

始める前に

サービスを有効にする前にカメラを「アクティベート」する必要があります。

ステップ

1. ウェブ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移動します。
設定→ ネットワーク→ プラットフォームアクセス→ Guarding Vision .
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の「利用規約」と「プライバシーポリシー」をクリックして内容を確認します。
5. 検証コード(Verification Code)を作成するか、既存の検証コードを変更します。



認証コードはカメラをGuarding Visionサービスに追加する際に必要となります。

6. 設定を保存します。

SADPソフトウェア経由でGuarding Visionサービスを有効にする方法

以下は、既にアクティベートされたカメラに対して SADP ソフトウェアで Guarding Vision を有効にする手順です。

ステップ

1. SADP ソフトウェアを起動します。
2. カメラを選択し、**Modify Network Parameters** 画面iに入ります。。
3. **Enable Hik-Connect** 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。



認証コードはカメラをGuarding Visionサービスに追加する際に必要となります。

5. 「利用規約」と「プライバシーポリシー」をクリックしてお読みください。
6. **Modify** をクリックして、設定を確定します。

8.16.2 Guarding Visionのセットアップ

ステップ

1. 以下の方法でGuarding Vision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://e-camera.net/>にアクセスし、ソフトウェア → スマートフォンアプリケーション からお使いのスマートフォンのシステムに合わせてアプリケーションをダウンロードしてください。
2. アプリケーションを起動し、Guarding Visionユーザーアカウントに登録します。
3. 登録後、ログインしてください。

8.16.3 Guarding Visionにカメラを追加

ステップ

1. モバイル端末をWi-Fiに接続します。
2. Guarding Vision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カバーにあるQRコードを読み取ってください。



QRコードがなかったり、かすれて認識できない場合は、カメラのシリアル番号を入力してカメラを追加することもできます。

5. カメラの認証コードを入力します。



- 必要な認証コードは、カメラでGuarding Visionサービスを有効にする際に作成または変更するコードです。
- 認証コードをお忘れの場合は、Webブラウザからプラットフォームアクセスの設定ページで現在の認証コードを確認することができます。

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、有線接続またはワイヤレス接続を選択します。

ワイヤレス接続 モバイル端末が接続しているWi-Fiのパスワードを入力し、「次へ」をタップして、Wi-Fi接続を開始します。
(Wi-Fiを設定する際は、ルーターから3m以内にカメラを設置してください)

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」をタップします。



ルーターはモバイル端末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」をタップして追加を完了します。

8.17 オープンネットワークビデオインターフェース(ONVIF)の設定

Open Network Video Interface プロトコルを使用して機器にアクセスする必要がある場合は、ユーザー設定を行ってネットワークセキュリティを強化できます。

ステップ

1. 設定 → ネットワーク → プラットフォームアクセス → ONVIF 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。
 - Digest を選択すると、機器は、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、機器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、Open Network Video Interface 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。
 -  をクリックして、選択したOpen Network Video Interface ユーザーを変更します。

8.18 SDKサービスの設定

機器をクライアントソフトウェアに追加したい場合は、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。

ステップ

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ーを設定します。
 - 1) 有効 にチェックを入れて、SDK プロトコルで機器をクライアントソフトに追加できるようにします。
 - 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 にチェックを入れて、TLS 上の SDK(SDK over TLS)プロトコルで機器をクライアントソフトに追加できるようにします。
 - 2) オプション:**TLS 設定** をクリックして、機器がサポートするTLSバージョンを有効にします。
詳細は、[TLS](#)を参照して下さい。
 - 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に、サーバー証明書を選択します。証明書を追加するには、**ライセンス管理** をクリックします。詳細については、「[ライセンスの管理](#)」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

システムのメンテナンス、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ーの設定方法を説明します。

9.1 システム設定

9.1.1 機器情報の表示

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機器情報を表示できます。

設定 → システム → システム設定 → 基本的な情報 にアクセスして機器情報を表示してください。

9.1.2 時刻と日付

タイムゾーン、時刻同期、夏時間(DST)を設定することで、機器の時刻と日付を設定できます。

手動で時刻を同期させる

ステップ

1. 設定 → システム → システム設定 → 時間設定. に移動します。
2. タイムゾーン を選択します。
3. 手動時間同期 を選択します。
4. 時刻同期方法 を1つ選択します。
 - 「時間を設定」を選択し、手動で入力するか、カレンダーをクリックし、ポップアップカレンダーから日付と時刻を選択します。
 - 「コンピュータ時刻に同期します」をクリックし、機器の時刻をローカルPCの時刻と同期させます。
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タイムソースが必要な場合は、NTPサーバーを使用することができます。

始める前に

NTPサーバーを設定するか、NTPサーバー情報を取得する。

ステップ

1. 設定 → システム → システム設定 → 時間設定. に移動します。
2. タイムゾーン を選択します。

3. ONTP時刻同期 を選択します。
4. サーバーのIPアドレス、NTPポート、間隔を設定します。



サーバーのIP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テストします。
6. [保存]をクリックします。

衛星による時刻同期



本機能は、機器によって異なります。

ステップ

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(サマータイム)設定

機器が設置されている地域がサマータイムを採用している場合、この機能を設定することができます。

ステップ

1. 設定 → システム → システム設定 → 時間設定 .に移動します。
2. 有効 にチェックを入れます。
3. 開始時間、終了時間、および夏時間補正を選択します。
4. [保存]をクリックします。

9.1.3 RS-232の設定

RS-232は機器のデバッグや周辺機器の接続に使用できます。RS-232は、通信距離が短い場合、機器とコンピュータまたは端末間の通信を実現することができます。

始める前に

機器をRS-232ケーブルで、コンピュータまたは端末に接続します。

ステップ

1. 設定 → システム → システム設定 → RS-232 に移動します。
2. 機器とコンピュータまたは端末が一致するように RS-232 パラメーターを設定します。
3. [保存]をクリックします。

9.1.4 RS-485設定

RS-485 は機器を外部機器に接続するために使用されます。通信距離が長い場合に、機器とコンピュータまたは端末間でデータを送信するために RS-485 を使用できます。

始める前に

機器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。

ステップ

1. 設定 → システム → システム設定 → RS-485 に移動します。
2. RS-485のパラメーターを設定します。



機器とコンピュータまたは端末のパラメーターはすべて同じにしておく必要があります。

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

リモートのライブビュー接続数を制御します。ライブビュー接続は、同時にストリーミング可能な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 に入り、リモート接続数の上限を設定します。

9.1.6 位置情報の設定

位置情報は、機器の現在の経度と緯度を表示及び、アップロードします。

自動アップロード

有効 をチェックし、**位置情報更新間隔**を設定します。

機器は、設定された間隔で、位置をアップロードします。また、[更新]をクリックして、機器の位置情報を手動でアップグレードすることもできます。

手動設定

有効 にチェックを入れ、**位置情報更新間隔**を設定します。機器の経度と緯度を入力し、[保存]をクリックします。

機器は設定した位置情報を設定した間隔でアップロードします。



本機能は、機種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ライセンスの表示

右上にある、「ヘルプの注意」をクリックし、**オープンソフトウェアの説明**を選択するとライセンスをダウンロードできます。ダウンロードしたライセンスはエディタで表示できます。

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。



ネットワーク上で機器を安全に使用するため、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か月ごとの変更を推奨します。高リスク環境で使用する場合は、毎月または毎週の変更を推奨します。

ステップ

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、[ユーザータイプ]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

管理者はすべての操作の権限を持ち、ユーザーやオペレーターの追加、権限の割り当てを行うことができます。

ユーザー

ユーザーには、ライブ映像の閲覧、PTZパラメーターの設定、パスワードの変更などの権限を割り当てることができますが、それ以外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できます。

削除 ユーザーを選択し、 をクリックし削除します。



管理者は最大31のユーザーアカウントを追加できます。

3. **[OK]** をクリックします。
-

9.2.2 同時ログイン

管理者は、ウェブブラウザからシステムに同時にログインす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、 一般パラメーター をクリックし、同時ログイン を設定し、最後に [OK] をクリックします。

9.2.3 オンラインユーザー

機器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 に移動して、オンラインユーザーのリストを確認してください。

9.3 メンテナンス

9.3.1 再起動

ブラウザから機器を再起動することができます。

メンテナンスとセキュリティ → メンテナンス → 再起動 に進み、再起動 をクリックします。

9.3.2 アップグレード

始める前に

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。



処理中に電源を切らないでください。アップグレード後に機器は自動的に再起動します。

ステップ

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. アップグレードする方法を1つ選択します。

アップグレードファイル	アップグレードファイルの正確なパスを見つける。
アップグレードディレクトリ	アップグレードファイルが属するディレクトリを探します。
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 バックアップと復元

バックアップと復元 は、機器のパラメーターをデフォルト設定に戻すのに役立ちます。

ステップ

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. にアクセスしてください。
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パラメーター、ビデオフォーマットを除く機器のパラメーターをデフォルト設定に戻す。
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に戻します。



この機能を使用する際は注意してください。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初期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

これは、同じパラメーターを持つ他の機器への一括設定のスピードアップに役立ちます。

ステップ

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て、設定ファイルをローカルコンピュータに保存します。
2. 設定ファイルをインポートします。
 - 1) ウェブブラウザで設定が必要な機器にアクセスする。
 - 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) をクリックして、保存され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) インポートをクリックする。

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。

ステップ

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(主タイプ、副タイプ、開始時間、終了時間)を設定します。
3. [検索]をクリックします。

条件に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:ログファイルをコンピュータに保存するには、「エクスポート」をクリックします。

9.3.6 セキュリティ監査ログの検索

機器のセキュリティログファイルを検索・解析することで、不正侵入を発見し、セキュリティ事象のトラブルシューティングを行うことができます。

ステップ



本機能は、一部のカメラモデルでのみサポートされています。

1. メンテナンスとセキュリティ→ 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:ログファイルをコンピュータに保存するには、「エクスポート」をクリックします。

9.3.7 SSHの設定

Secure Shell (SSH) は、信頼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安全に操作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→ デバイスのデバッグ に移動し、SSH の [設定] をクリックします。

有効 にチェックを入れると、ポート番号を編集できます。編集したら、[保存] をクリックし設定を保存します。



注意

本機能の使用には注意が必要です。本機能を有効にした場合、機器内部情報漏洩のセキュリティ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→ デバイスのデバッグ→診断情報 に移動し、[エクスポート] をクリックします。

9.4 セキュリティ

セキュリティパラメーターを設定することで、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の設定

IPアドレスフィルターは、アクセス制御のためのツールです。IPアドレスフィルターを有効にすることで、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ことができます。

IPアドレスはIPv4を指します。

ステップ

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 にチェックをいれます。
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アドレスは機器にアクセスできません。

許可リスト リスト内のIPアドレスのみが機器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する。

追加 新しいIPアドレスまたはIPアドレス範囲をリストに追加します。

 リストで選択したIPアドレスまたはIPアドレス範囲を変更します。

 リストで選択した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アドレスフィルターは、アクセス制御のためのツールです。MACアドレスフィルターを有効にすることで、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ことができます。

ステップ

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 に移動します。
2. 有効 にチェックをいれます。
3. MACアドレスフィルターのタイプを選択します。

ブロックリスト リストにあるMACアドレスは機器にアクセスできません。

許可リスト リスト内のMACアドレスのみが機器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する。

追加 新しいMACアドレスをリストに追加する。

 リストで選択したMACアドレスを変更します。

 リストで選択した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 操作タイムアウト設定

本機能を有効にすると、Webブラウザ経由で機器に対して操作(ライブ映像の閲覧は含みません)を行わない状態が、設定したタイムアウト期間続いた場合に自動的にログアウトされます。

メンテナンスとセキュリティ→セキュリティ→ログイン管理→コントロールタイムアウト設定 に移動して設定を完了します。

9.4.4 ライセンス管理

ライセンス管理機能では、サーバー/クライアント証明書および CA 証明書を管理でき、証明書の有効期限が近い場合や期限切れ・異常がある場合にアラームを送信できます。



本機能は、一部の機種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



機器にはデフォルトで自己署名のサーバー/クライアント証明書がインストールされています。証明書の 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

ステップ

1. メンテナンスとセキュリティ→セキュリティ→ライセンス管理 に移動します。
 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。
-



入力する証明書 ID は既存の証明書と同じにできません。

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。
証明書が特定の機能で使用される場合、その機能が、[機能]の列に表示されます。
 5. オプション:[属性]をクリックすると、証明書の詳細を確認できます。
-

自己署名要求証明書のインストール

自己署名証明書を信頼できるサードパーティに送って署名してもらい、証明書を機器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ます。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。

ステップ

1. メンテナンスとセキュリティ→ セキュリティ→ ライセンス管理 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. 保存したファイルを信頼できる第三者に送付して署名を依頼します。
8. 第三者から署名済みの証明書が返送されたら、機器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。



入力された証明書IDは、既存のものと同じにできません。

- 3) 証明書ファイルを選択します。
- 4) 自己署名要求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。
証明書が特定の機能で使用される場合、その機能名が次の列に表示されます。
9. オプション:[属性] をクリックすると、証明書の詳細が表示されます。

その他の認定証明書をインストールする

すでに外部で発行された認証済み証明書をお持ちの場合は、その証明書を直接機器にインポートできます。

ステップ

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



入力する証明書 ID は既存のものと同じにできません。

4.  をクリックして、証明書ファイルを選択します。

5. [証明書と鍵]を選択し、証明書に従って「鍵の種類」を選択します。

自己署名要求証明書 証明書に独立した鍵がある場合は、このオプションを選択する。
ブラウズして秘密鍵を選択し、秘密鍵のパスワードを入力する。

証明書とキー 証明書の鍵が同じ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は、リストの機能列に該当する機能名が表示されます。

CA証明書のインストール

始める前に

事前にCA証明書を用意してください。

ステップ

1. メンテナンスとセキュリティ→ セキュリティ→ ライセンス管理 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。



入力される証明書IDは、既存のものと同じに出来ません。

4. [保存]をクリックします。

インポートした証明書は、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は、リストの機能列に該当する機能名が表示されます。

証明書有効期限切れアラームの有効化

ステップ

1. [証明書期限切れ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い場合、期限切れ、または異常がある場合にメールやカメラから監視センターへのリンクで通知を受け取れます。
2. 有効期限切れ前に通知する(日数)、アラームの頻度(日数)、検出時間(時間)を設定します。



- 有効期限前リマインダーを1に設定すると、有効期限の前日にリマインダーが表示されます。1~30日の設定が可能です。デフォルトは7日間です。
- 有効期限切れ前に通知する日数を1日、検出時間を10:00に設定し、証明書の有効期限が翌日の9:00に切れる場合、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の設定

トランスポートレイヤーセキュリティ(TLS)プロトコルは、主に通信するアプリケーション間でプライバシーとデータの整合性を提供することを目的としています。

TLSの設定は、HTTP(S)と拡張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、使用するTLSプロトコルにチェックを入れて有効にします。設定後は、保存をクリックしてください。



本機能の使用には注意が必要です。本機能を有効にした場合、機器内部情報漏洩のセキュリティリスクが存在します。

第10章 VCAリソース

VCAリソースは、機器がサポートするスマート機能の集合です。

10.1 オープンプラットフォームの設定

HEOP(Hikvision Embedded Open Platform)は、サードパーティの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できるプラットフォームです。HEOP をサポートする機器では、スマートアプリケーションをインポートして実行するために以下の手順に従ってください。

ステップ

1. VCAインターフェースに移動します。



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に適合していることを確認してください。

- 各アプリケーションはそれぞれ専用の名前を持っていること。
- アプリケーションが占有するFLASHメモリ容量は、機器の利用可能なFLASHメモリ容量より小さいこと。
- アプリケーションのメモリと計算能力は、機器の利用可能なメモリと計算能力よりも小さいこと。

2. [重要なアプリケーション]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：アプリケーションの設定を行います。

	アプリケーションを有効または無効にする。
	アプリケーションを削除する。
	ログをエクスポートする。
	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する。
詳細を見る	アプリケーションを選択し、クリックすると詳細が表示されます。

10.2 一般設定

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ーを設定します。

VCA → アプリケーションの設定 → 一般設定 にアクセスして、以下のパラメーターを設定します。

FTP

FTP設定については、「[FTPを設定する](#)」を参照してください。

Eメール

電子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。

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。

音声アラーム出力

音声アラーム出力の設定については、「[音声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

機器固有の情報をカスタマイズします。複数の機器を管理している場合に、特定の機器を識別するのに役立ちます。

VCA → アプリケーションの設定 → 一般設定 → カメラ情報 にアクセスして、カメラ情報とデバイス番号を設定します。

10.3 スマートイベント



- 本機能は、ソフトウェアデコーディングモード、またはハードウェアデコーディングモードのフィッシュアイ表示モードでのみサポートされます。
- 一部の機種では、VCA ページでスマートアプリケーションを先に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ために十分なメモリ(RAM/FLASH)があることを確認してください。足りない場合は、他のアプリケーションを無効にする必要があります。

10.3.1 侵入検知の設定

侵入検知は、あらかじめ定義した仮想領域に物体が進入・滞留することを検出するための機能です。事象が発生した場合、機器は連動処理を行うことができます。

始める前に

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

ステップ

1. VCA→アプリケーションの設定→スマートイベント→侵入検知に移動します。
2. 有効にチェックを入れます。
3. [+追加] をクリックしてルールを追加し、検出領域を設定する。
 - 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、右クリックして描画を完了します。
 - 2) 検出精度を向上させるために、対象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だけが検出対象になります。☐ 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、対象の最小サイズと最大サイズを描画します。
 - 3) オプション：すべての設定領域を削除するには、☒ をクリックします。
4. パラメーターを設定します。

しきい値

しきい値は領域内で対象が滞留する時間の閾値を表します。1つの対象が滞在する時間がこの閾値を超えるとアラームが発生します。しきい値の値が大きいほど、アラームが発生するまでの時間は長くなります。

感度

感度は、許容される対象の体部分が定義領域に入る割合(%)を表します。

感度(Sensitivity) = $100 - S1/ST \times 100$ で計算されます。ここで、S1 は、定義領域を横切る対象の体部分、ST は対象の全体です。感度の値が高いほど、アラームが発生しやすくなります。

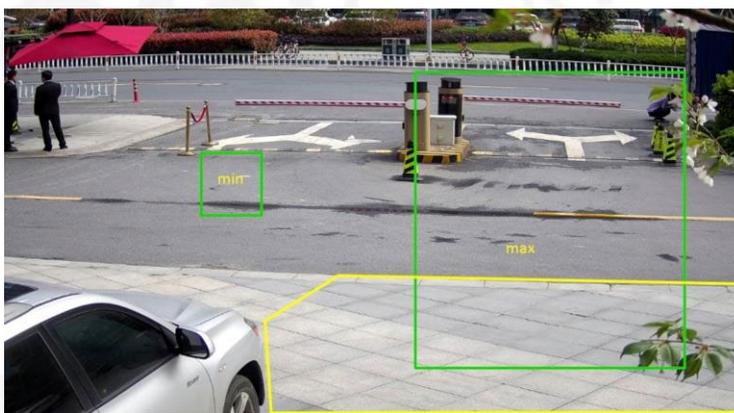


図10-1 ルールの設定

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ーを設定することができます。
6. 警戒スケジュールの設定については、「[警戒スケジュールの設定](#)」を参照。リンクメソッドの設定については、「[リンクメソッドの設定](#)」を参照してください。
7. [保存] をクリックします。

10.3.2 ラインクロス検知の設定

ラインクロス検知は、あらかじめ定義した仮想線を物体が横切ることを検出するための機能です。事象が発生した場合、機器は連動処理を行うことができます。

始める前に

- VCAにアクセスし、システムに付属するスマートアプリケーションのいずれかを選択する。

ステップ

1. VCA→ アプリケーションの設定 → スマートイベント→ ラインクロス検知 に移動します。
2. 有効にチェックを入れます。
3. [+追加] をクリックしてルールを追加し、検出領域を設定します。

- 1) 検出線を描画します。☑ をクリックすると、ライブビューに矢印付きの線が表示されます。ラインをライブビュー上の任意の位置にドラッグします。
- 2) 検出精度を向上させるために、対象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だけが検出対象となります。☒ と ☒ をクリックし、ライブビューでマウスをドラッグして、ターゲットの最小サイズと最大サイズを描画します。
- 3) オプション:すべての設定領域を削除するには、🗑 をクリックします。

4. パラメーターを設定します。

方向

これは、物体が線を横切る方向を表す。

A<->B: 両方向からラインを横切る物体を検出し、アラームを発生させます。

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します。

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検出します。

感度

感度は、許容される対象の体部分が定義済みの線を横切る割合(%)を表します。
感度 = $100 - S1/ST \times 100$ 。ここで、S1 は、あらかじめ定義されたラインを横切る対象の体部分、STは、対象体全体を表します。感度の値が高いほど、アラームが作動しやすくなります。

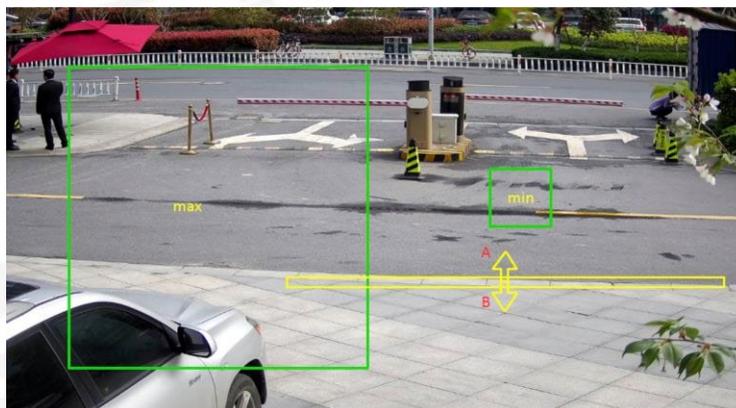


図10-2 ルールの設定

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ーを設定することができます。
6. 警戒スケジュールの設定については、[警戒スケジュールの設定](#)を参照。リンクメソッドの設定については、[リンクメソッドの設定](#)を参照してください。
7. [保存]をクリックします。

10.3.3 領域進入検知の設定

領域進入検知は、あらかじめ定義した仮想領域の外側から内部へ物体が進入することを検出するための機能です。事象が発生した場合、機器は連動処理を行うことができます。

始める前に

- VCAに移動し、システムに付属しているいずれかのスマートアプリケーションを選択してください。

ステップ

1. VCA → アプリケーションの設定 → スマートイベント → 領域進入検知 へ移動します。
2. 有効にチェックを入れます。
3. [+追加] をクリックしてルールを追加し、検出領域を設定します。
 - 1) 検出領域を描画します。 をクリックし、ライブビュー上で頂点を指定し、検出領域の境界を描画し、右クリックして描画を完了します。
 - 2) 検出精度を向上させるために、対象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だけが検知対象となります。 と  をクリックしてから、ライブビュー上でドラッグして、最小サイズと最大サイズを描画します。
 - 3) オプション:すべての設定領域を削除するには、 をクリックします。
4. パラメータを設定します。

感度

感度は、許容される対象の体部分が定義領域を横切る割合(%)を表します。感度 = $100 - S1/ST \times 100$ で、起算されます。ここで S1 は、あらかじめ定義された領域を横切る対象の体部分、ST は対象の全体です。感度の値が高いほど、アラームが発生しやすくなります。

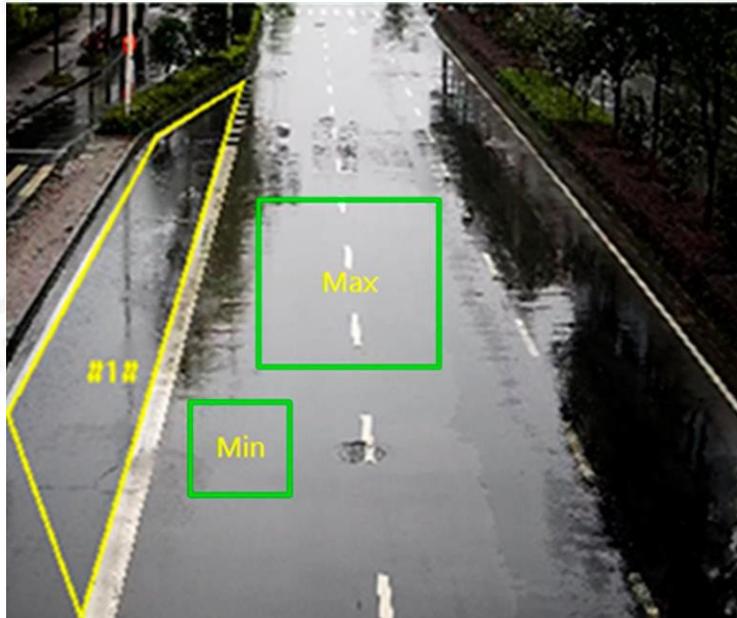


図10-3 ルールの設定

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ーを設定することができます。
6. 警戒スケジュールの設定については、**警戒スケジュールの設定**を参照。リンクメソッドの設定については、**リンクメソッドの設定**を参照してください。
7. [保存]をクリックします。

10.3.4 領域退出検知の設定

領域退出検知は、あらかじめ定義した仮想領域から物体が退出することを検出するための機能です。事象が発生した場合、機器は連動処理を行うことができます。

始める前に

- VCAに移動し、システムに付属しているいずれかのスマートアプリケーションを選択してください。

ステップ

1. VCA→アプリケーションの設定 → スマートイベント→ 領域退出検知 へ移動します。
2. 有効にチェックを入れます。
3. [+追加] をクリックしてルールを追加し、検出領域を設定します。
 - 1) 検出領域を描画します。 をクリックし、ライブビュー上で頂点を指定し、検出領域の境界を描画し、右クリックして描画を完了します。
 - 2) 検出精度を向上させるために、対象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だけが検知対象となります。 と  をクリックしてから、ライブビュー上でドラッグして、最小サイズと最大サイズを描画します。
 - 3) オプション:すべての設定領域を削除するには、 をクリックします。

4. パラメーターを設定します。

感度

感度は、許容される対象の体部分が定義領域を横切る割合(%)を表します。

感度 = $100 - S1/ST \times 100$ で、起算されます。ここで S1 は、あらかじめ定義された領域を横切る対象の体部分、ST は対象の全体です。感度の値が高いほど、アラームが発生しやすくなります。

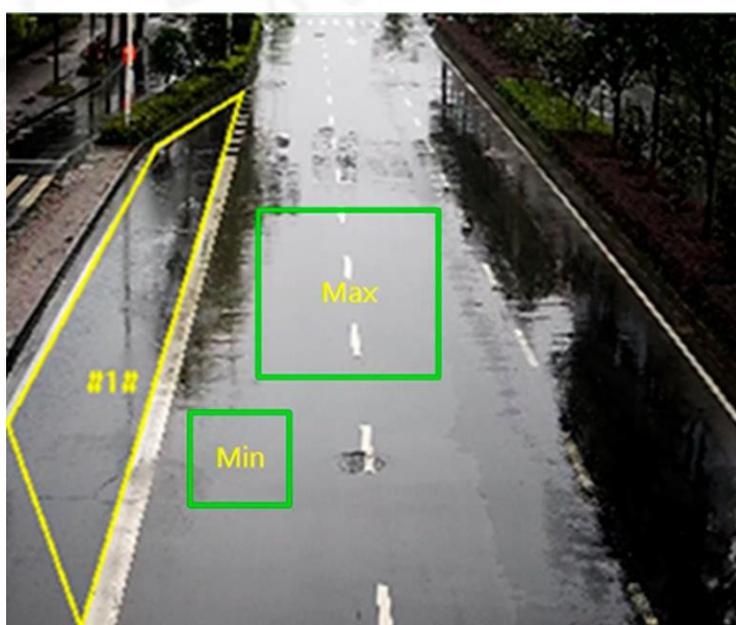


図10-4 ルールの設定

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ーを設定することができます。警戒スケジュールの設定については、[警戒スケジュールの設定](#)を参照。リンクメソッドの設定については、[リンクメソッドの設定](#)を参照してください。
6. [保存]をクリックします。

10.3.5 放置手荷物検知の設定

放置手荷物検知は、あらかじめ定義した領域内に放置された物体を検出するための機能です。物体が領域内に放置され、設定した時間滞留すると連動処理をトリガーできます。

始める前に

- VCAに移動し、システムに付属しているいずれかのスマートアプリケーションを選択してください。

ステップ

1. VCA→アプリケーションの設定 → スマートイベント→ 放置手荷物検知 へ移動します。
2. 有効にチェックを入れます。
3. [+追加] をクリックしてルールを追加し、検出領域を設定します。

- 1) 検出領域を描画します。 をクリックし、ライブビュー上で頂点を指定し、検出領域の境界を描画し、右クリックして描画を完了します。
- 2) 検出精度を向上させるために、対象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だけが検知対象となります。 と  をクリックしてから、ライブビュー上でドラッグして、最小サイズと最大サイズを描画します。
- 3) オプション:すべての設定領域を削除するには、 をクリックします。

4. パラメーターを設定します。

感度

感度は、許容される対象の体部分が定義領域を横切る割合(%)を表します。

感度 = $100 - S1/ST \times 100$ で、起算されます。ここで S1 は、あらかじめ定義された領域を横切る対象の体部分、ST は対象の全体です。感度の値が高いほど、アラームが発生しやすくなります。

しきい値

しきい値は領域内に放置された物体の滞留時間を表します。物体が放置され設定した時間滞留するとアラームが発生します。

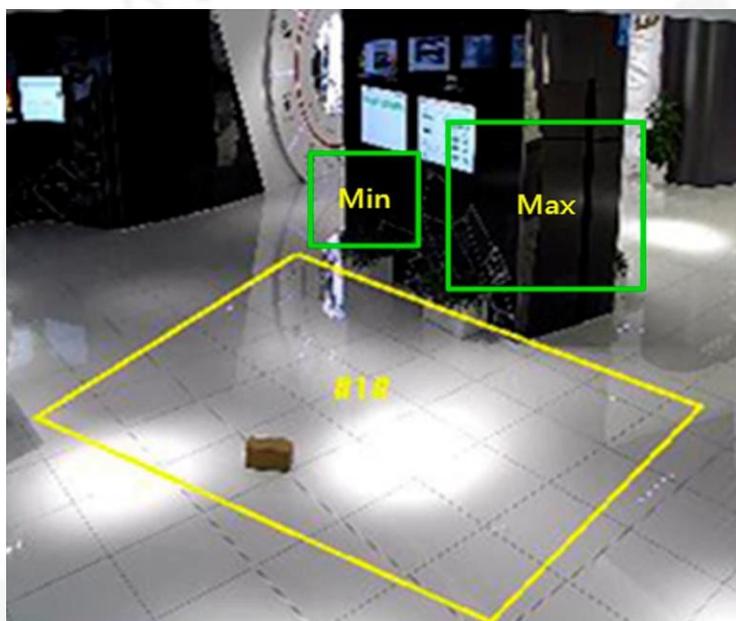


図10-5 ルールの設定

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ーを設定することができます。
6. 警戒スケジュールの設定については、[警戒スケジュールの設定](#)を参照。リンクメソッドの設定については、[リンクメソッドの設定](#)を参照してください。
7. [保存]をクリックします。



本機能は一部の機種でのみサポートされています。実際の表示は機種によって異なります。

10.3.6 持ち去り検知の設定

持ち去り検知は、展示物などあらかじめ定義した検出領域から物体が撤去されたかどうかを検出する機能です。事象が発生した場合、機器は連動処理を行い、スタッフが財産被害を最小限に抑えるための対応を行います。

始める前に

VCAに移動し、システムに付属しているいずれかのスマートアプリケーションを選択してください。

ステップ

1. VCA→アプリケーションの設定 → スマートイベント→ 持ち去り検知 へ移動します。
2. 有効にチェックを入れます。
3. [+追加] をクリックしてルールを追加し、検出領域を設定します。
 - 1) 検出領域を描画します。 をクリックし、ライブビュー上で頂点を指定し、検出領域の境界を描画し、右クリックして描画を完了します。
 - 2) 検出精度を向上させるために、対象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だけが検知対象となります。 と  をクリックしてから、ライブビュー上でドラッグして、最小サイズと最大サイズを描画します。
 - 3) オプション:すべての設定領域を削除するには、 をクリックします。
4. パラメーターを設定します。

感度

感度は、許容される対象の体部分が定義領域を横切る割合(%)を表します。

感度 = $100 - S1/ST \times 100$ で、起算されます。ここで S1 は、あらかじめ定義された領域を横切る対象の体部分、ST は対象の全体です。感度の値が高いほど、アラームが発生しやすくなります。

しきい値

しきい値は、領域から物体が撤去された後の経過時間を表します。例えば値を 10 に設定した場合、物体が領域から消失してから 10 秒後にアラームが発生します。

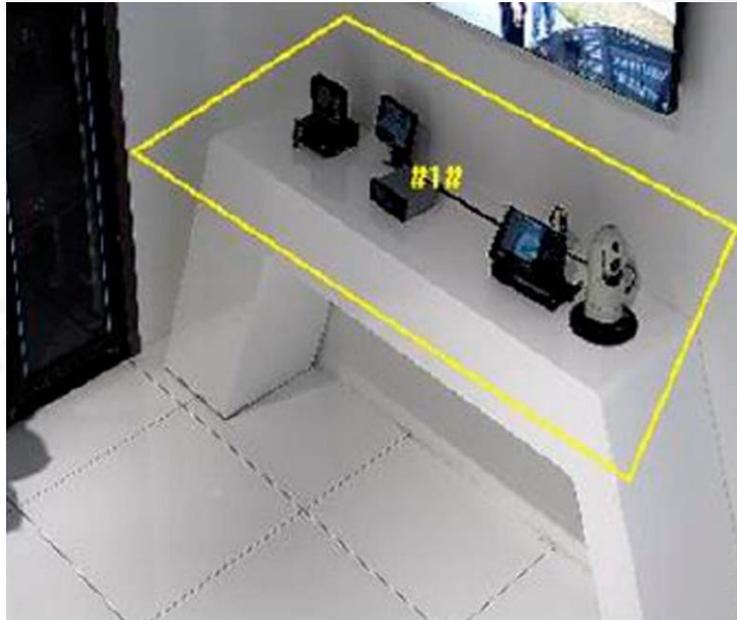


図 10-6 ルールの設定

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ーを設定することができます。
6. 警戒スケジュールの設定については、**警戒スケジュールの設定**を参照。リンクメソッドの設定については、**リンクメソッドの設定**を参照してください。
7. [保存]をクリックします。



注 本機能は一部の機種でのみサポートされています。実際の表示は機種によって異なります。

10.4 ・人物カウントアラーム

人物カウントアラームは、あらかじめ定義した領域内の人数および人数の変動を検出・解析するための機能です。出入口やスーパーなどでの利用に適しています。



- 本機能は、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魚眼表示モードでのみサポートされます。
 - 一部機種では、VCA ページでアプリケーションを先に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ために十分なメモリ(RAM/FLASH)があることを確認してください。足りない場合は、他のアプリケーションを無効にしてください。
-

10.4.1 待ち行列管理

待ち行列管理は、列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の機能です。地域別の列検知や待機時間検知、統計表示機能があります。

領域内人数カウント検知の設定については「[領域内人数カウント検知の設定](#)」を参照してください。

待機時間検知の設定については「[待機時間検知の設定](#)」を参照してください。

待ち行列管理統計の設定・表示については「[待ち行列管理統計の設定](#)」を参照してください。



注

待ち行列管理は一部の機種でのみサポートされています。

領域内人数カウント検知の設定

定義したエリア内の列に並んでいる人数をカウントします。アラームは、アラームしきい値条件とアラーム発生条件の両方が満たされたときに発生します。

始める前に

- VCAに移動し、アプリケーションを選択します。人物カウントアラームを選択し、「次へ」をクリックして機能を有効にします。
- HEOPをサポートする機器では、VCAから、人物カウントアラームをインポートし、有効化してください。

ステップ

1. VCA → アプリケーションの設定 → 人物カウントアラーム → 待ち行列管理 → ルール設定 へ。
2. 「+追加」をクリックし、必要に応じてルール名を編集します。

ルールリスト + 追加

Area1 ×

*ルール名

エリアの色

① *アラーム間隔 秒

人数の画面表示

① 領域内人数カウント検知

領域内人数カウント検知

アラーム発生条件

*アラームしきい値 人

① 待機時間検知

待機時間検知

アラーム発生条件

*アラームしきい値 秒

人物不在状況を無視

保存

3. 領域の色を選択し、 をクリックしてルール領域を描画します。ライブビュー画面上で終点を左クリックしてルールエリアの境界を定義し、右クリックで描画を終了します。



同時に最大8エリアまで設定可能。
エリアが重ならないようにしてください。

4. ルールの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 回のみ通知をトリガーします。

人数の画面表示

ライブビュー画面に人数を表示します。

人物不在状況を無視

シーン内に人が存在しない場合はアラームを発生させません。これは、設定したアラームしきい値未満かつシーン内に人がいない場合に発生する不要なアラームをフィルタリングするための機能です。

5. [領域内人数カウント検知]を選択し、[アラーム発生条件]と[アラームしきい値]を設定します。設定エリア内の人数がアラームしきい値と発生条件を満たすとアラームが発生します。



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ーを設定することができます。

6. [保存]をクリックします。

7. 警戒スケジュールの設定については、[警戒スケジュールの設定](#)を参照。リンクメソッドの設定については、[リンクメソッドの設定](#)を参照してください。



ルールリストでルールを選択し、をクリックするか、[コピー先...]をクリックして、関連する警戒スケジュールとリンクメソッド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、データの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]をクリックしてください。

リアルタイムアップロード

リアルタイムアップロードにチェックを入れると、検出されたターゲットID、待機時間、地域番号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

機器は、滞在時間が積分ポイントの最小滞在時間以上である人数をアップロードします。

例:最小滞在時間を 10 秒に設定し、2 エリアに対象がいる場合、積分ポイントにおいてそれぞれのエリアで滞在時間が 10 秒以上になった時点で人数をアップロードします。

9. オプション:オーバーレイとキャプチャのパラメーターを設定します。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:詳細をクリックし、フィルタリング条件を設定します。詳細設定については、[高度な設定](#)を参照してください。

次に行うこと

詳細なデータ分析を表示するには、[アプリケーション表示](#)→[待ち行列管理統計](#)にアクセスしてください。詳細設定については、[待ち行列管理統計](#)を参照してください。

待ち時間検出の設定

検知エリアに入る各人の待ち時間をカウントするために使用されます。アラームは、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ときに発生します。

始める前に

- VCAに移動し、アプリケーションを選択します。人物カウントアラームを選択し、「次へ」をクリックして機能を有効にしてください。
- HEOPをサポートする機器では、VCAから人物カウントアラームをインポートして有効化してください。

ステップ

1. VCA → アプリケーションの設定 → 人物カウントアラーム → 待ち行列管理 → ルール設定 へ移動します。
2. 「+追加」をクリックし、必要に応じてルール名を編集します。

ルールリスト + 追加

Area1	Area2 ×
-------	--

*ルール名

エリアの色

① *アラーム間隔 秒

人数の画面表示

① 領域内人数カウント検知

領域内人数カウント検知

アラーム発生条件

*アラームしきい値 人

① 待機時間検知

待機時間検知

アラーム発生条件

*アラームしきい値 秒

人物不在状況を無視

保存

3. 領域の色を選択し、 をクリックしてルール領域を描画します。ライブビュー画面上で終点を左クリックしてルールエリアの境界を定義し、右クリックで描画を終了します。



同時に最大8エリアまで設定可能。
エリアが重ならないようにしてください。

4. ルールの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内では、同一種類のアラームは一度だけ通知されます。

人数表示

ライブビュー画面に人数を表示します。

5. 待機時間検知を選択し、アラーム発生条件とアラームしきい値を設定します。設定したエリア内の待ち時間がアラーム閾値およびトリガー条件を満たしたときにアラームが発生します。
6. [保存]をクリックします。



上記の手順を繰り返すことで、複数エリアのパラメーターを設定することができます。

7. 警戒スケジュールの設定については、[警戒スケジュールの設定](#)を参照。リンクメソッドの設定については、[リンクメソッドの設定](#)を参照してください。



ルールリストでルールを選択し、 をクリックするか、[コピー先...]をクリックして、関連する警戒スケジュールとリンクメソッド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、データのアップロードを設定します。リアルタイムのアップロードと予定の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。

リアルタイムのアップロード

リアルタイムアップロードにチェックを入れると、検出されたターゲットID、警戒時間、地域番号をリアルタイムでアップロードします。

予定のアップロード

機器は、滞在時間が積分ポイントの最小滞在時間以上である人数をアップロードします。

例: 最小滞在時間を 10 秒に設定し、2 エリアが対象の場合、積分ポイントにおいてそれぞれのエリアで滞在時間が 10 秒以上になった時点で人数をアップロードします。

9. オーバーレイとキャプチャのパラメーターを設定します。詳細は「[オーバーレイとキャプチャ](#)」を参照してください。
10. オプション: 詳細をクリックし、フィルタリング条件を設定します。詳細設定については、[高度な設定](#)を参照してください。

次に行うこと

詳細なデータ分析を表示するには、アプリケーション表示→待ち行列管理統計にアクセスしてください。詳細設定については、[待ち行列管理統計](#)を参照してください。

待ち行列管理統計

待ち行列管理統計は、データ分析とレポート出力をサポートします。

始める前に

待ち行列管理の設定については、「[領域別の人数待ち設定](#)」および「[待ち時間検出の設定](#)」を参照してください。

- 「キューイングアップ時間分析」と「複数エリア比較」を選択すると、複数エリアの列の人数を比較できます。
- 「キューイングアップ時間分析」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ごとの列人数を比較できます。
- 「キューステータス分析」と「複数エリア比較」を選択すると、異なるエリアで列がある長さの状態にとどまった時間と継続時間を比較できます。
- 「キューステータス分析」と「マルチレベル比較」を選択すると異なる列長レベルでの列の時間と継続時間を比較できます。

ステップ



注
内蔵メモ리카ードが装着されている場合、機器は最大1か月分のデータを保存できます。メモ리카ードがない場合は、最大1週間分のデータしか保存できません。

1. アプリケーション表示→ 待ち行列管理統計へ移動します。

レポートタイプ
日次レポート

時間を選択
2026-02-25

統計内容
待ち行列形成時間解析

エリア
 すべて選択
 エリア1
 エリア2
 エリア3
 エリア4
 エリア5
 エリア6

統計ディメンション
 複数エリアの比較
 多重レベル比較

待機時間レベル(秒)
 継続時間 <= 300
 300 < 継続... <= 600
 継続時間 > 600

検索

図10-7 待ち行列管理統計

2. レポートタイプと時間を選択します。

3. 統計内容を選択します。

待ち行列形成時間解析

さまざまな待ち時間レベルの人数を計算する。

待ち行列状態分析

列がある長さにとどまっている時間と継続時間を算出します。

4. 統計ディメンションを選択します。

複数エリアの比較

複数のエリアと1つのレベルを選択して解析し、解析チャートが作成されます。

多重レベル比較

複数のレベルとエリアを選択でき、各エリアごとに解析チャートが作成されます。

5. 1つ以上のエリアにチェックを入れます。

6. 待ち時間レベルを設定します。希望する範囲を1つチェックし、値を入力する。

7. [検索]をクリックしてレポートを作成します。

8. オプション:データをエクスポートするには、 エクスポートをクリックします。

10.4.2 交差点分析

交差点分析は、交差点のようなシーンでの通行人の流れを検出するための機能です。



本機能は、一部の機種でのみサポートされています。

交差点分析

始める前に

- VCAに移動し、アプリケーションを選択します。人物カウントアラームを選択し、「次へ」をクリックして機能を有効にしてください。
- HEOPをサポートする機器では、VCAから人物カウントアラームをインポートして有効化してください。

ステップ

1. VCA → アプリケーションの設定 → 人物カウントアラーム → 交差点分析 → ルール設定 へ移動します。
2. 有効のスイッチをオンにし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。ライブビュー画面上の端点を左クリックして、設定されたルールエリアの境界を定義し、右クリックして描画を終了します。
4. 各辺の矢印方向を調整します。矢印はその辺から交差点外へ流出する方向を表します。
5. 「警戒スケジュールとリンク方法」に移動して、警戒スケジュールを設定し、リンクメソッドのチェックボックスにチェックを入れて連動方法を選択します。警戒スケジュールの設定については、「[警戒スケジュールの設定](#)」を参照してください。リンクメソッドの設定については、「[リンクメソッドの設定](#)」を参照してください。
6. データアップロードに進み、アップロードするデータの種類の種類を選択します。設定したEメールアドレスに交差点分析レポートを送信することができます。
7. [保存]をクリックします。

次に行うこと

アプリケーション表示 → 交差点分析統計に移動し、詳細なデータ分析を確認してください。
詳細設定については、[交差点分析統計](#)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した後、交差点分析データを表示できます。図には入口方向と、総人数に対する各入口から入ってきた人数の割合がオーバーレイ表示されます。ある入口から流入し、他のすべての入口へ流出した人数も計算されます。

始める前に

最初に交差点分析機能を設定してください。

ステップ

1. アプリケーションの表示 → 交差点解析統計. に移動します。
2. 「進入」で解析したい流れを選択します。
3. レポートタイプと時間を選択します。
4. [検索]をクリックします。
条件に合致した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

ストリームおよび画像に表示する情報とキャプチャパラメーターを設定します。

VCA → 人物カウントアラーム → オーバーレイとキャプチャ に移動します。

ストリームにVCA情報を表示

ターゲットやルール情報など、スマート情報をストリーム上に表示します。

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します。

テキストオーバーレイ

キャプチャした画像に重ねて表示する情報を選択します。。また、↑ ↓ をクリックして順序を調整することもできます。

10.4.4 詳細設定

人物カウントアラーム機能の詳細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

これは現在のアルゴリズムのバージョンを示します。

アルゴリズムモード

設置シーンに合わせてモードを選択します。

フィルター

ターゲットサイズ

ターゲット検出ウィンドウのサイズを示します。このピクセルより大きいターゲットを実際のターゲットとしてカウントできます。一定の固定対象による誤報を除去できます。

オフセット

ターゲットの変位または幅を示します。設定した割合より変位が小さいターゲットはカウントされません。

最小待機時間

設定値より短い待ち時間はフィルタリングされます。

確度

しきい値が高いほどターゲットの検出は困難になりますが、精度は高くなります。



フィルター設定は専門家が操作すべきです。フィルター設定により検出アルゴリズムの検出範囲や感度などを調整できます。

ストレージデータのクリア

機器に保存されたすべての人数カウントデータを消去します。使用には注意してください。

10.5 ヒートマップ

ヒートマップは色でデータを視覚的に表現する図表です。本機のヒートマップ機能は、設定した領域内での来訪回数や滞留時間を解析するために使用します。



- 本機能は、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表示モードでのみサポートされます。
 - 一部機種では、VCA ページでアプリケーションを先に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ために十分なメモリ(RAM/FLASH)があることを確認してください。足りない場合は、他のアプリケーションを無効にしてください。
-

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参照したい場合は、あらかじめカメラの設定を行ってください。

始める前に

- VCAに移動し、アプリケーションを選択します。人物カウントアラームを選択し、「次へ」をクリックして機能を有効にしてください。
- HEOPをサポートする機器では、VCAから人物カウントアラームをインポートして有効化してください
- 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ます。ストレージの設定については、「[ストレージの設定](#)」を参照して下さい。

ステップ

1. VCA → アプリケーションの設定 → 人物アラームマネジメント → ヒートマップ設定 に移動します。
2. 有効のスイッチをオンにして機能を有効にします。
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。
4. 描画した領域のパラメーターを設定します。

予想人数

ヒートマップ集計で扱う最大人数を示します。

オン

実際のシーンでの最大人数と設定した想定人数を比較し、より大きい方をヒートマップの最大人数として扱います。

オフ

実際のシーンの人数をヒートマップの最大値として扱います。

5. [保存]をクリックします。
6. 警戒スケジュールの設定については、「[警戒スケジュールの設定](#)」を参照してください。
7. リンクメソッドの設定については、「[リンクメソッドの設定](#)」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、データのアップロード情報を設定します。
[保存]をクリックして設定を保存します。

データタイプのアップロード

- 滞留時間 検出領域内の対象の滞留時間を示します。
滞在時間と人数 検出領域内の対象の滞留時間と領域内の人数を示します。

次に行うこと

ヒートマップ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をクリックして、ヒートマップの統計情報を確認してください。

10.5.2 ヒートマップデータの表示

ヒートマップは、あらかじめ定義した領域内の人流を観察・集計し、その統計をグラフ形式で表示する機能です。商業施設、スーパーマーケット、博物館などの大量の来訪者があるシーンに適用できます。ヒートマップにより来訪者の好み(滞在しやすい場所)を把握し、商品配置の調整などに活用できます。

始める前に

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。

ステップ

1. アプリケーションの表示→ ヒートマップ. に移動します。
2. レポートタイプを選択します。日次、週次、月次、年次のレポートが選択できます。
3. ヒートマップ種別を選択します。空間ヒートマップと時間ヒートマップが選択できます。
4. 統計タイプを選択します。滞在時間別または、人数別が選択できます。
5. 時間を選択します。
6. [検索]をクリックします。

日次レポートは選択した日付のデータを算出します。
週次レポートは選択した日付が属する週のデータを算出します。
月次レポートは選択した日付が属する月のデータを算出します。
年次レポートは選択した日付が属する年のデータを算出します。

例) 集計が完了すると、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

画像全体の各領域における累積滞在を統計解析します。
異なるヒート値は異なる色に対応し、赤(255, 0, 0)が最も高いヒート、青(0, 0, 255)が最も低いヒートを表します。最高ヒート値と最低ヒート値は N 段階に分割され、それぞれ異なる色に対応します。

時間ヒートマップ

画像全体のすべての人の総滞在時間を統計解析します。

時間ヒートマップは折れ線グラフで表示され、Export をクリックするとデータを Excel ファイルでエクスポートできます。

10.6 人数集計

人数カウントは、あるエリアに出入りする人数を算出するための機能です。



- 本機能は、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表示モードでのみサポートされます。
 - 一部機種では、VCA ページでアプリケーションを先に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ために十分なメモリ(RAM/FLASH)があることを確認してください。
-

10.6.1 人数カウントルールの設定

検出ルールおよびアルゴリズムパラメーターを設定すると、機器はルールエリア内の出入り人数を算出し、連動動作をトリガーし、データを自動アップロードします。

始める前に

- VCAに移動し、アプリケーションを選択します。人物カウントアラームを選択し、「次へ」をクリックして機能を有効にしてください。
- HEOPをサポートする機器では、VCAから人物カウントアラームをインポートして有効化してください

ステップ

1. VCA → アプリケーションの設定 → 人数集計 → ルール設定 に移動します。
2. 有効のスイッチをオンにして機能を有効にします。
3. 「+追加」をクリックし、集計エリアを追加します。
4.  をクリックして多角形の集計エリア(カウントエリア)を描画します。ライブビュー画面上で端点を左クリックし、右クリックで描画を終了します。
5. 検知ラインを描画します。矢印は入場方向を示し、クリックで方向を変更できます。
 - 集計エリアが一方向にしか対応していない場合は、 をクリックして直線の検知ラインを描画することを推奨します。
 - 集計エリアが複数の方向に対応している場合や、集計エリア内に壁や障害物がある場合は、 をクリックして折れ線で検知ラインを描画することを推奨します。



計数精度を向上させるため、以下のルールに従って集計エリアを描いてください。

- 集計エリアは出入りする通路を覆うように設定してください。
 - 検知ラインは赤い集計エリア内に完全に含まれ、通行する人の進行経路に対して垂直になるようにしてください。
-

6. オプション:集計エリアや検知ラインを調整できます。。

 をクリックする選択した集計エリアまたは検知ラインを消去します。

 すべての集計エリアおよび検知ラインを消去するには「すべて消去」をクリックします。

7. オプション:上記のステップを繰り返し、最大3つの集計エリアと対応する検知ラインを描画できます。
-

8. 人数集計の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計数データの種類のドロップダウンリストから選択し、ライブビュー画像における人の計数データの表示位置を調整します。



OSDオーバーレイは、現在の日の人数のみをカウントします。データは機器の再起動時または毎日のリセット時に自動的にクリアされます。

毎日のリセット時間

既定では機器は毎日 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任意の時刻を選択できます。選択後、毎日その時刻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て現在の人数カウントデータを消去できます。

9. [保存]をクリックします。

10. 警戒スケジュールの設定については、「[警戒スケジュールの設定](#)」を参照してください。

11. リンクメソッドの設定については、「[リンクメソッドの設定](#)」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:人数集計データのアップロードパラメーターを設定します。

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。

定期的にデータをアップロードする

データ統計周期を設定すると、設定した周期で通行量データが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: 人数集計の詳細パラメーターを設定します。

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

バージョン

これは現在のアルゴリズムのバージョンを示します。

ストリームにVCA情報を表示

ターゲットやルール情報などのスマート情報をストリームに表示します。

ストレージデータのクリア

機器に保存されたすべての人数カウントデータを消去します。使用には注意してください。

結果

- 対象が入場方向に沿って検出エリアを横切り検出線を越えた場合、1 人の入場としてカウントされます。
- 対象が退場方向に沿って検出エリアを横切り検出線を越えた場合、1 人の退場としてカウントされます。

次に何をすべきか

詳細な人数集計データ分析を表示するには、「アプリケーション表示」に進みます。詳細な設定については、「[人数集計データの表示](#)」を参照してください。

10.6.2 人数集計データの表示

機器に保存された人数カウントデータを、表、棒グラフ、折れ線グラフで表示できます。

始める前に

まず、人数集計の設定を完了してください。

ステップ

1. アプリケーション表示 → 人数集計 に移動します。
2. レポートタイプ、統計タイプ、時間を選択を設定します。
3. [検索]をクリックします。

表、棒グラフ、折れ線グラフを選択してデータを表示できます。

エクスポート 機能で人数カウントデータを Excel にエクスポートできます。。

10.7 データ検知情報の検索とエクスポート

データ検知機能は、再起動履歴、起動履歴、およびキャプチャアラーム統計などのデータを検索・エクスポートするために使用します。

始める前に

管理者(admin)ユーザーアカウントで機器にログインしてください。

ステップ

1. アプリケーション表示 → データ認識 に移動します。
2. 検索条件を選択します。
統計タイプ 録画の再開 または、監視有効化中 を選択します。
録画の再開 再起動のタイプ(通常の再起動 又は、異常再起動)を選択します。
監視有効化中 監視種別(現在の警戒、警戒履歴、異常切断)を選択します。
3. [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。。
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機器に保存します。