

The logo features the word "HIKVISION" in a bold, italicized, white sans-serif font, centered within a red horizontal bar. The bar has a white diagonal stripe on the left side.

HIKVISION

ネットワークカメラ

ユーザーマニュアル

法的情報

©2020 Hangzhou Hikvision Digital Technology Co., Ltd. 禁・無断複製。

本マニュアルについて

本マニュアルには製品の使用および管理についての指示が含まれています。ここに記載されている写真、表、画像およびその他すべての情報は説明のみを目的としています。本マニュアルに含まれる情報は、ファームウェア更新やその他の理由で通知なく変更されることがあります。このマニュアルの最新版は、Hikvision Webサイト

(<https://www.hikvision.com/>)でご確認ください。

本マニュアルは、本製品をサポートする訓練を受けた専門家の指導・支援を受けた上でご使用ください。

商標

HIKVISION およびその他Hikvisionの商標およびロゴは、様々な裁判管轄地域においても Hikvision の所有物です。

言及されているその他の商標およびロゴは、各権利保有者の所有物です。

免責事項

適用法で認められる最大限の範囲で、本マニュアルおよび説明されている製品（ハードウェア、ソフトウェア、および本製品を含む）は、「現状のまま」および「すべての欠陥とエラーがある」状態で提供されます。HIKVISIONは、明示あるいは黙示を問わず、商品性、満足な品質、または特定目的に対する適合性などを一切保証しません。本製品は、お客様の自己責任においてご利用ください。HIKVISIONは、本製品の利用に関連する事業利益の損失や事業妨害、データの損失、システムの障害、文書の損失に関する損害を含む特別、必然、偶発または間接的な損害に対して、それが契約に対する違反、不法行為(過失を含む)、製品の責任または製品の使用に関連するものであっても、たとえHIKVISIONがそうした損害および損失について通知を受けていたとしても、一切の責任を負いません。

お客様はインターネットが本質的に持つセキュリティリスクについて認識し、HIKVISIONは、異常操作、プライバシー漏えいまたはサイバー攻撃、ハッキング、ウィルス感染やその他のセキュリティリスクから生じるその他の損害に対して一切の責任を負わないものとし、ます。ただし、必要であればHIKVISIONは適宜技術サポートを提供します。




お客様には、すべての適用法に従って本製品を利用し、さらにご自分の利用法が適用法を順守していることを確認する責任があります。特に、肖像権、知的財産権、またはデータ保護等のプライバシー権を非限定的に含むサードパーティの権利を侵害しない手段で本製品を利用する責任があります。大量破壊兵器の開発や生産、化学兵器・生物兵器の開発や生産、核爆発物や危険な核燃料サイクル、または人権侵害に資する活動を含む、禁じられている最終用途の目的で本製品を使用してはなりません。

本マニュアルと適用法における矛盾がある場合については、後者が優先されます。

D'SSECURITY

記号の定義

本書で使用されている記号は以下のように定義されます。

記号	説明
 危険	回避しないと、死亡または重傷を招く可能性のある危険な状況を示します。
 注意	潜在的に危険となりうる状況を表しており、防止できなかった場合、機器の損傷、データの消失、性能劣化など、予測不能な結果が生じる可能性があります。
 注意	本文中の重要点を強調したりそれを補う追加情報を提供します。

D'SSECURITY

安全上の指示

これらの指示は、ユーザーが製品を正しく使用し、危険や財産損失を回避できるように保証することを目的としています。

法規と規則

- 本器は、各国の法規、電気安全規則、火災予防規則に準じて使用する必要があります。

輸送

- 輸送中は、デバイスを元のパッケージまたは類似したパッケージに梱包してください。

電源

- 入力電圧はIEC60950-1規格に準拠している必要があります：SELV（安全特別低電圧）および制限電源。詳細については該当の資料を参照してください。
- プラグが適切に電源ソケットに接続されていることを確認してください。
- 1台の電源アダプターに2台以上の機器を接続してはなりません。過負荷によって過熱したり、火災発生の危険があります。

システムのセキュリティ

- インストールをする者およびユーザーは、パスワードや、セキュリティ環境設定およびその設定を担います。

バッテリー

- バッテリーの不適切な使用や交換を行うと、爆発の危険性があります。
- 同一または同等のタイプのもので交換してください。使用済みのバッテリーは、地元の規定に従って廃棄してください。

メンテナンス

- 製品が正しく動作しない場合、販売店または最寄りのサービスセンターに連絡してください。承認されていない修理や保守行為による問題について、当社はいかなる責任も負いません。
- 一部のデバイスコンポーネント（電解コンデンサなど）は、定期的に交換する必要があります。製品の平均寿命は変動するため、定期的な点検をお勧めします。詳細については、販売店にお問い合わせください。

使用環境

- 実行環境がデバイスの要件を満たしていることを確認します。動作温度は-30°C～60°C（-22°F～140°F）、動作湿度は95%以下（結露なきこと）である必要があります。
- レーザー装置を使用している場合は、デバイスのレンズがレーザービームにさらされていないことを確認してください。焼損するおそれがあります。
- デバイスを強い電磁波や埃の多い環境にさらさないでください。
- 屋内用デバイスの場合、乾燥した換気の良い場所に設置してください。
- レンズを太陽や極端に明るい場所に向けないでください。

緊急

- デバイスから煙や異臭、異音が発生した場合、すぐに電源を切り、電源ケーブルを抜いて、サービスセンターにご連絡ください。

時間同期

- ローカル時刻がネットワークの時刻と同期されていない場合、初回のアクセス時に手動でカメラの時刻を設定します。Webブラウザ/クライアントソフトウェアを使用してカメラにアクセスし、時刻設定のインターフェイスへ移動します。

目次

CHAPTER 1 システム要件.....	1
CHAPTER 2 デバイスのアクティベーションとアクセス	2
2.1 SADPを使用してデバイスをアクティブにする	2
2.2 ブラウザを使用してデバイスをアクティブにする.....	3
2.3 ログイン	4
2.3.1 プラグインのインストール	4
2.3.2 管理者パスワードの回復	6
2.3.3 不正ログインロック	7
CHAPTER 3 ライブビュー.....	8
3.1 ライブ画像のパラメーター.....	8
3.1.1 ライブビューの有効化または無効化.....	8
3.1.2 アスペクト比率の調整.....	8
3.1.3 ライブビューストリームタイプ.....	9
3.1.4 サードパーティプラグインを選択する	9
3.1.5 明るい.....	9
3.1.6 ピクセル数をカウントする	9
3.1.7 デジタルズームの開始.....	10
3.1.8 補助フォーカス.....	10
3.1.9 レンズ初期化.....	10
3.1.10 ライブビューのクイック設定.....	11
3.1.11 レンズパラメータ調整.....	11
3.1.12 3Dポジショニングの実行.....	12

3.2	伝送パラメータを設定する	13
3.3	スムーズストリーミング設定	14
CHAPTER 4	ビデオとオーディオ	16
4.1	ビデオ設定	16
4.1.1	ストリームタイプ	16
4.1.2	ビデオタイプ	17
4.1.3	解像度	18
4.1.4	ビットレートタイプと最大ビットレート	18
4.1.5	ビデオ画質	18
4.1.6	フレームレート	18
4.1.7	ビデオエンコーディング	19
4.1.8	平滑化	21
4.2	ROI	22
4.2.1	ROIを設定する	22
4.2.2	顔追跡のROIを設定する	23
4.2.3	ターゲット追跡のROIを設定する	23
4.2.4	ナンバープレート追跡のROIを設定する	24
4.3	ストリーム上の情報表示	24
4.4	音声設定	25
4.4.1	音声圧縮	25
4.4.2	音声入力	25
4.4.3	音声出力	25
4.4.4	環境ノイズフィルター	26
4.5	双方向音声	26
4.6	ディスプレイ設定	27

4.6.1	シーンモード	27
4.6.2	画像パラメータ切替	31
4.6.3	ビデオ規格	32
4.6.4	ローカルビデオ出力	32
4.7	OSD.....	32
4.8	プライバシーマスクの設定.....	33
4.9	オーバーレイ画像.....	34
4.10	ターゲットクロップの設定.....	34
チャプター 5	ビデオ録画と画像キャプチャ.....	36
5.1	ストレージ設定	36
5.1.1	新規または暗号化されていないメモ리카ードの設定.....	36
5.1.2	FTP設定	39
5.1.3	NAS設定.....	40
5.1.4	eMMCの保護	41
5.1.5	クラウドストレージの設定	41
5.2	ビデオ録画.....	43
5.2.1	自動録画	43
5.2.2	手動で録画する	45
5.2.3	ライトストレージ設定.....	45
5.2.4	ビデオの再生とダウンロード.....	46
5.3	キャプチャ設定	47
5.3.1	自動的にキャプチャする	47
5.3.2	手動でキャプチャする.....	47
5.3.3	タイミングウェイクの設定	48
5.3.4	画像の表示とダウンロード	48

チャプター 6	イベントとアラーム	50
6.1	基本イベント	50
6.1.1	動体検知の設定	50
6.1.2	ビデオ干渉アラームの設定	53
6.1.3	PIRアラームの設定	54
6.1.4	異常検知アラームの設定	54
6.1.5	アラーム入力の設定	55
6.1.6	ビデオ品質診断の設定	55
6.1.7	振動検知の設定	56
6.2	スマートイベント	57
6.2.1	音声異常の検知	57
6.2.2	焦点ボケ検知の設定	58
6.2.3	シーン変化検知	59
6.2.4	顔検知の設定	59
6.2.5	ビデオロスの設定	60
6.2.6	侵入検知の設定	60
6.2.7	ラインクロス検知の設定	62
6.2.8	範囲進入検知の設定	63
6.2.9	領域退出検知の設定	64
6.2.10	放置手荷物検知の設定	66
6.2.11	オブジェクト除去検知の設定	67
6.2.12	領域指定	68
6.2.13	サイズフィルターの設定	69
チャプター 7	ネットワーク設定	70
7.1	TCP/IP	70

7.1.1	マルチキャスト	71
7.1.2	マルチキャスト検出	72
7.2	SNMP	72
7.3	SRTPの設定	73
7.4	ポートマッピング	74
7.4.1	自動ポートマッピングの設定	74
7.4.2	手動ポートマッピングの設定	75
7.4.3	ルータのポートマッピング設定	76
7.5	ポート	77
7.6	ドメイン名を使用したデバイスへのアクセス	78
7.7	PPPoEダイヤルアップ接続を経由したデバイスへのアクセス	79
7.8	ワイヤレスダイヤル	81
7.8.1	ワイヤレスダイヤルを設定	81
7.8.2	許可リストの設定	82
7.9	Wi-Fi	82
7.9.1	デバイスをWi-Fiに接続する	83
7.10	ネットワークサービスの設定	84
7.11	オープンネットワークビデオインターフェイスの設定	85
7.12	ISUPの設定	86
7.13	アラームサーバの設定	87
7.14	Hik-Connect経由でカメラにアクセスする	87
7.14.1	カメラの Hik-Connect サービス有効化	88
7.14.2	Hik-Connectの設定	90
7.14.3	Hik-Connectにカメラを追加する	91

CHAPTER 8 監視スケジュールとアラーム連動	93
8.1 監視スケジュールの設定	93
8.2 リンク方式の設定.....	93
8.2.1 トリガアラームアウトプット	94
8.2.2 FTP/NAS/メモリカードのアップロード.....	95
8.2.3 Eメール送信	95
8.2.4 監視センターに通知する	97
8.2.5 録画をトリガー.....	97
8.2.6 ライト点滅	97
8.2.7 音声警報.....	98
CHAPTER 9 システムとセキュリティ	100
9.1 デバイス情報を表示.....	100
9.2 ログの検索と管理.....	100
9.3 同時ログイン.....	100
9.4 設定ファイルのインポートとエクスポート	101
9.5 診断情報のエクスポート	101
9.6 再起動 101	
9.7 復元とデフォルト.....	101
9.8 アップグレード	102
9.9 オープンソースのソフトウェアライセンスを表示する	103
9.10 ウィーガンド	103
9.11 メタデータ	104
9.12 時間と日付.....	104
9.12.1 手動による時間同期	104
9.12.2 NTPサーバの設定	105

9.12.3	衛星による時間同期	105
9.12.4	DST設定	106
9.13	RS-485の設定.....	106
9.14	RS-232の設定.....	107
9.15	消費電力モード	107
9.16	外部機器	108
9.16.1	補助光の設定.....	108
9.16.2	ヒーター	109
9.17	セキュリティ	110
9.17.1	認証	110
9.17.2	IPアドレスフィルタの設定	111
9.17.3	HTTPSの設定	112
9.17.4	QoSの設定	112
9.17.5	IEEE 802.1xの設定	113
9.17.6	コントロールタイムアウト設定	113
9.17.7	セキュリティ監査ログの検索.....	114
9.17.8	セキュリティ強化	114
9.17.9	SSH	114
9.18	証明書の管理	115
9.18.1	自己署名証明書の作成.....	115
9.18.2	証明書要求の作成	115
9.18.3	証明書のインポート	116
9.18.4	サーバ/クライアント証明書のインストール.....	116
9.18.5	CA証明書のインストール.....	117
9.18.6	証明書有効期限切れアラームを有効化	117

9.19 ユーザーとアカウント	118
9.19.1 ユーザーアカウントと権限の設定	118
9.19.2 同時ログイン.....	119
9.19.3 オンラインユーザ	119
CHAPTER 10 VCAリソースの割り当て	120
10.1 スマートモードの切り替え.....	120
10.2 顔キャプチャ	122
10.2.1 顔キャプチャの設定	122
10.2.2 オーバーレイとキャプチャー.....	123
10.2.3 顔キャプチャアルゴリズムのパラメータ	125
10.2.4 シールド区域の設定	127
10.3 道路交通量.....	127
10.3.1 車両検知の設定.....	128
10.3.2 混合トラフィックの検知ルールを設定.....	129
10.3.3 画像アップロード設定.....	130
10.3.4 カメラ設定	131
10.3.5 ブロックリスト&許可リストをインポート/エクスポート.....	131
10.4 マルチターゲットタイプ検知	132
10.4.1 マルチターゲットタイプ検知のルールを設定.....	132
10.4.2 オーバーレイとキャプチャー.....	133
10.4.3 マルチターゲットタイプ検知のアルゴリズムパラメータ	134
10.4.4 シールド区域の設定	135
10.5 顔のカウント	136
10.5.1 顔カウント検知のルールを設定	136
10.5.2 オーバーレイとキャプチャー.....	137

10.5.3	顔カウントのアルゴリズムパラメータ	138
10.5.4	顔カウント結果の表示.....	140
10.6	待ち行列管理	140
10.6.1	エリア内行列の設定	140
10.6.2	待機時間検知の設定	142
10.6.3	待ち行列管理統計	143
10.7	カウント	144
10.7.1	カウントの設定.....	145
10.7.2	計数統計の表示.....	146
10.8	安全帽検出.....	146
10.8.1	安全帽検出の設定	146
10.9	顔比較とモデリング.....	147
10.9.1	顔比較.....	148
10.9.2	顔モデリング.....	152
CHAPTER 11	オープンプラットフォーム	154
11.1	オープンプラットフォームの設定.....	154
CHAPTER 12	スマート表示	156
CHAPTER 13	EPTZの設定	157
13.1	パトロール.....	157
13.2	自動追跡機能.....	157
CHAPTER 14	パターンリンク	159
14.1	パターンリンクの設定	159
A.	デバイスコマンド	161
B.	デバイスの通信マトリックス	162

CHAPTER 1 システム要件

お使いのコンピュータは、製品の正常なアクセスやオペレーションに関する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 またはそれ以上
CPU	2.0 GHz またはそれ以上
RAM	1G またはそれ以上
ディスプレイ	解像度 1024×768 またはそれ以上
ウェブ ブラウザ	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。

D'SSECURITY

CHAPTER 2 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やデータのセキュリティとプライバシーを保護するには、ネットワーク経由でデバイスにアクセスする際に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する必要があります。

注意

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を使用してデバイスをアクティブにする

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、アクティブにします。

始める前に

www.hikvision.comにアクセスして、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デバイスをネットワークに接続します。
2. SADPソフトウェアを実行し、オンラインデバイスを検索します。
3. デバイスリストから**[Device Status]**にチェックを入れ、**[未アクティブ]**状態のデバイスを
選択します。

4. パスワードフィールドに新たなパスワードを入力して、パスワードを確認します。
-



お使いの製品のセキュリティ向上のため、ご自身で選択した強力なパスワード（最低8文字を使用し、大文字、小文字、数字および特殊記号を含むもの）を作成することを強く推奨します。また、定期的にパスワードを再設定し、特に高いセキュリティ システムでは、毎月または毎週パスワードを再設定すると、より安全に製品を保護できます。

5. **[OK]**をクリックします。
[Device Status]が**[アクティブ]** に変わります。
6. オプション: **[Modify Network Parameters]**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 ブラウザを使用してデバイスをアクティブにする

ブラウザ経由でデバイスにアクセスしてアクティブにすることが可能です。

ステップ

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。
-



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**～**192.168.1.253**で設定することが可能です（**192.168.1.64**を除く）。たとえば、PCのIPアドレスを**192.168.1.100**と設定することが可能です。

3. ブラウザに **192.168.1.64** と入力します。

4. デバイスアクティベーションパスワードを設定します。

注意

製品のセキュリティを高めるため、ご自分で選択した強力なパスワード (大文字、小文字、数字、特殊記号のうち、少なくとも3つのカテゴリで構成された文字を8文字以上含むパスワード) を設定するよう強くお勧めします。また、定期的にパスワードを再設定し、特に高いセキュリティ システムでは、毎月または毎週パスワードを再設定すると、より安全に製品を保護できます。

5. [OK]をクリックします。
6. アクティベーションパスワードを入力して、デバイスにログインします。
7. オプション: [環境設定]→[ネットワーク]→[基本]→[TCP/IP]と移動して、デバイスの IP アドレスをご利用のネットワークと同じセグメントに変更します。

2.3 ログイン

Webブラウザを使用して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

一部のオペレーションシステムおよびWebブラウザでは、カメラ機能の表示や操作が制限される場合があります。プラグインをインストールするか、特定の設定を完了して、通常が表示と動作を確認する必要があります。制限された機能の詳細については、実際のデバイスを参照してください。

オペレーティングシステム	ウェブ ブラウザ	操作
Windows	<ul style="list-style-type: none"> ● Internet Explorer 8以降 ● Google Chrome 57 以前のバージョン ● Mozilla Firefox 52 以前のバージョン 	<p>ポップアッププロンプトに従って、プラグインのインストールを完了します。</p>
	<ul style="list-style-type: none"> ● Google Chrome 57以降 ● Mozilla Firefox 52以降 	<p> Download Plug-in をクリックして、プラグインをダウンロードおよびインストールします。</p>
Mac OS	<ul style="list-style-type: none"> ● Google Chrome 57以降 ● Mozilla Firefox 52以降 ● Mac Safari 16以降 	<p>プラグインのインストールは不要です。</p> <p>[環境設定]→[ネットワーク]→[詳細設定]→[ネットワークサービス]と移動して、WebSocketまたはWebsocketを有効化して標準表示にします。特定の機能で表示や操作が制限されています。たとえば、再生および画像が使用できません。制限された機能の詳細については、実際のデバイスを参照してください。</p>

 **注意**

このカメラは、WindowsおよびMacのOSのみをサポートし、Linuxシステムはサポートしていません。

2.3.2 管理者パスワードの回復

アカウントのセキュリティ設定を完了した後に管理者パスワードを忘れた場合、ログインページで**[Forget Password]**をクリックしてパスワードをリセットすることが可能です。パスワードをリセットするには、セキュリティ用の質問またはEメールを設定します。

 **注意**

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

セキュリティ用の質問

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可能です。または、**[環境設定]→[システム]→[ユーザー管理]**と移動して、**[アカウントセキュリティ設定]**をクリックして、セキュリティ用の質問を選択し、回答を入力します。

ブラウザからデバイスへのアクセス時に**[Forget Password]**をクリックしてセキュリティ用の質問に答えると、管理者パスワードをリセットすることが可能です。

Eメール

アクティベーション中にアカウントのセキュリティを設定することが可能です。または、**[環境設定]→[システム]→[ユーザー管理]**と移動して、**[アカウントセキュリティ設定]**をクリックして、オペレーションプロセスの回復中に検証コードを受信するためのE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

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ることができます。

[環境設定]→[システム]→[セキュリティ]→[セキュリティサービス]と移動して、[不法ログインのロック機能を有効にします]にチェックを入れます。[不正なログイン試行]と[ロック持続期間]の設定が可能です。

不正なログイン試行

誤ったパスワードによるログイン試行が設定回数に達すると、デバイスはロックされます。

ロック持続期間

設定期間が経過すると、デバイスはロックを解除します。

D'SSECURITY

CHAPTER 3 ライブビュー

ここでは、ライブビューのパラメータ、機能アイコン、伝送パラメータの設定について説明します。

3.1 ライブ画像のパラメーター

サポートされている機能はモデルによって異なります。







3.1.1 ライブビューの有効化または無効化

この機能を使用して、チャンネルのライブビューをすばやく有効化または無効化します。

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

3.1.2 アスペクト比率の調整

ステップ

1. [ライブビュー]をクリックします。
2.  をクリックしてアスペクト比を選択します。
 -  は、4：3のウィンドウサイズを表します。
 -  は、16：9のウィンドウサイズを表します。
 -  は、元のウィンドウサイズを表します。
 -  は、自動調整のウィンドウサイズを表します。
 -  は、オリジナル比率のウィンドウサイズを表します。


3.1.3 ライブビューストリームタイプ

ニーズに合わせてライブビュー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の詳細については、**ストリームタイプ**を参照してください。

3.1.4 サードパーティプラグインを選択する


特定のブラウザでライブビューを表示できない場合、ブラウザに応じてライブビューのプラグインを変更することが可能です。

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からデバイスにアクセスする場合は、**Webcomponents**または**QuickTime**を選択することが可能です。他のブラウザからデバイスにアクセスする場合は、**Webcomponents**、**QuickTime**、**VLC**、**MJPEG**を選択することが可能です。


3.1.5 明るい

をクリックして照明器のオン/オフを切り替えることができます。

3.1.6 ピクセル数をカウントする

これにより、ライブビュー画像で選択した領域の高さと幅のピクセルを取得することができます。


ステップ

1. をクリックして機能を有効化します。
2. 画像上でマウスをドラッグして、好みの長方形の領域を選択します。
幅ピクセルや高さピクセルは、ライブビュー画像の下部に表示されます。

3.1.7 デジタルズームの開始

これにより画像内の任意の領域で詳細情報を表示できるようになります。


ステップ

1. をクリックしてデジタルズームを有効化します。
2. ライブビュー画像で、マウスをドラッグして領域をお好みに合わせて選択します。
3. ライブビュー画像をクリックすると、元の画像に戻ります。

3.1.8 補助フォーカス

これは電動デバイスに使用されます。デバイスのフォーカスがクリアにならない場合、画像を改善することが可能です。

ABFをサポートするデバイスの場合、レンズ角度を調整し、フォーカスを合わせてから、デバイスのABFボタンをクリックします。デバイスはクリアにフォーカスできるようになります。

をクリックすると、自動的にフォーカスします。


注意

- デバイスが補助フォーカスでフォーカスできない場合、**[レンズの初期化]**を実行してから再度補助フォーカスを使用すると、画像をクリアにすることができます。
 - 補助フォーカスでデバイスのフォーカスがクリアにならない場合、手動フォーカスを使用することが可能です。
-

3.1.9 レンズ初期化

電動レンズを装備したデバイスでは、レンズの初期化が使用されます。長時間のズームやフォーカスによって画像がぼやけてしまう場合、この機能を使用してレンズをリセットすることが可能です。この機能はカメラのモデルによって異なります。

レンズ初期化（手動）

をクリックして、レンズの初期化を行います。


レンズ初期化（自動）

[環境設定]→[システム]→[メンテナンス]→[レンズ補正]と移動して、この機能を有効化します。監視スケジュールを設定すると、設定した時間中、自動的にレンズの補正が行われます。

3.1.10 ライブビューのクイック設定

ライブビューページでPTZ、ディスプレイ設定、OSD、ビデオと音声、VCAリソース設定を簡単に行えます。

ステップ

1. をクリックすると、クイック設定ページが表示されます。
2. PTZ、ディスプレイ設定、OSD、ビデオと音声、VCAリソースパラメータを設定します。
 - PTZの設定については**レンズパラメータ調整**を参照してください。
 - ディスプレイの設定については**ディスプレイ設定**を参照してください。
 - OSDの設定については**OSD**を参照してください。
 - 音声およびビデオの設定については**ビデオとオーディオ**を参照してください。
 - VCAの設定については**VCAリソースの割り当て**を参照してください。



注意

この機能は特定のデバイスでのみサポートされます。



3.1.11 レンズパラメータ調整

レンズのフォーカス、ズーム、アイリスを調整します。


ズーム

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



フォーカス

- をクリックすると、レンズが遠くをフォーカスし、遠くの被写体がクリアになります。
- をクリックすると、レンズが近くをフォーカスし、近くの被写体がクリアになります。

PTZ速度

 をスライドして、パン・チルト動作の速度を調整します。

アイリス

- 画像が暗すぎる場合、 をクリックして、アイリス（絞り）を開いてください。
- 画像が明るすぎる場合、 をクリックして、アイリス（絞り）を閉じてください。

PTZロック


PTZロックとは、対応するチャンネルのズーム、フォーカス、PTZ回転の機能を無効にして、PTZ調整による被写体の欠落を減らすことです。

[環境設定]→[PTZ]と移動して、[Enable PTZ Lock]にチェックを入れて、[保存]をクリックします。

3.1.12 3Dポジショニングの実行

3Dポジショニングでは、選択した領域を画像の中央に移動します。

ステップ

1.  をクリックして機能を有効化します。
2. ライブ画像のターゲット領域を選択します。
 - ライブ画像上で任意のポイントを左クリックします。そのポイントがライブ画像の中央に移動します。ズームやズームアウトのエフェクトは使えません。
 - ホールドしたままマウスを右下の位置にドラッグして、ライブ領域をフレーム化します。フレーム化された領域がズームされ、ライブ画像の中央に移動します。
 - ホールドしたままマウスを左上の位置にドラッグして、ライブ領域をフレーム化します。フレーム化された領域がズームアウトされ、ライブ画像の中央に移動します。
3. 再度ボタンをクリックして、機能をオフにします。

3.2 伝送パラメータを設定する

ライブビュー画像は、ネットワークの状態により異常な表示をする場合があります。異なるネットワーク環境では、伝送パラメータを調整して問題を解決することが可能です。

ステップ

1. [環境設定]→[ローカル]と移動します。
2. 必要に応じて伝送パラメータを設定します。

プロトコル

TCP

TCPによりストリーミングデータの完全配信とビデオ画質の向上は保証されますが、リアルタイム伝送に影響が及ぶことになります。安定したネットワーク環境に適しています。

UDP

UDPは、ビデオ動画で高度な滑らかさが要求され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、マルチキャストアドレスを設定する必要があります。

注意

マルチキャストに関する詳細は、**マルチキャスト**を参照してください。

HTTP

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

再生パフォーマンス

最短遅延

デバイスはビデオ画像において、滑らかさよりもリアルタイムを優先します。

バランス

デバイスはビデオ画像において、リアルタイムと滑らかさの両方に重きを置きます。

滑らかさ

デバイスはビデオ画像において、リアルタイムよりも滑らかさを優先します。ネットワーク環境が劣悪な場合、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することはできません。

カスタム

フレームレートを手動で設定することが可能です。ネットワーク環境が劣悪な場合、フレームレートを下げて、ライブビューを滑らかにすることが可能です。ただし、ルール情報を表示できない場合があります。

3. **[OK]**をクリックします。

3.3 スムーズストリーミング設定

これは、不安定なネットワーク状態によって発生する遅延やネットワークの輻輳に対処し、Webブラウザやクライアントソフトウェア上でライブビューストリームをスムーズに保つ機能です。

始める前に

デバイスをクライアントソフトウェアに追加し、クライアントソフトウェアでNPQプロトコルを選択してから、スムーズストリーミング機能を設定します。

この機能を有効化する前に、**[ビットレートタイプ][定数]**、**[SVC][オフ]**がそれぞれ選択されていることを確認してください。**[環境設定]→[ビデオとオーディオ]→[ビデオ]**と移動して、パラメータを設定します。

ステップ

1. 設定ページへ移動します：**[環境設定]→[ネットワーク]→[詳細設定]→[スムーズストリーミング]**。
2. **[スムーズストリーミングを有効化]**にチェックを入れます。
3. スムーズストリーミングのモードを選択します。

自動

解像度とビットレートは自動調整になりますが、解像度が優先されます。この2つのパラメータの上限は、**[ビデオ]**のページで設定した

値を超えることはありません。**[環境設定]**→**[ビデオとオーディオ]**→**[ビデオ]**と移動して、**[スムーズストリーミング機能]**を有効にしてから**[解像度]**と**[最大ビットレート]**を設定します。このモードでは、フレームレートは自動的に最大値に調整されます。

解像度優先度

解像度は**[ビデオ]**ページの設定値のまま、ビットレートは自動的に調整されます。**[環境設定]**→**[ビデオとオーディオ]**→**[ビデオ]**と移動して、スムーズストリーミング機能を有効にしてから**[最大ビットレート]**を設定します。このモードでは、フレームレートは自動的に最大値に調整されます。

エラー補正

解像度とビットレートは、**[ビデオ]**のページの設定値のままになります。このモードは、送信中のデータエラーを修正して、画像品質を確保するために使用します。**[エラー補正比率]**は0～100の範囲で設定可能です。

比率が0の場合、データの再送信によりデータエラーが修正されません。比率が0より大きい場合、エラーデータは、ストリームやデータの再送信の時に追加される冗長データにより修正されます。値が大きいくらいほど生成されるデータは冗長化し、データエラーの修正も多くなりますが、必要になる帯域幅も大きくなります。比率が100の場合、冗長データは元のデータと同じ大きさになるため、必要になる帯域幅も2倍になります。

注意

エラー補正モードで帯域幅が十分であることを確認してください。

4. 設定を保存します。

CHAPTER 4 ビデオとオーディオ

このパートでは、ビデオと音声関連のパラメータの設定について説明します。

4.1 ビデオ設定

このパートでは、ストリームタイプ、ビデオエンコーディング、解像度など、ビデオパラメータの設定について説明します。

設定ページへ移動します：**[環境設定]**→**[ビデオとオーディオ]**→**[ビデオ]**。

4.1.1 ストリームタイプ

デバイスが複数のストリームをサポートしている場合、ストリームタイプごとにパラメータを指定することが可能です。

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となります。通常は、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、解像度やフレームレートが上がると、一般的にストレージ容量が大きくなり、転送時に必要になる帯域幅も大きくなることとなります。

サブストリーム

このストリームは通常、比較的低解像度のオプションを提供するので、消費する帯域幅やストレージ容量は少なく済みます。

その他のストリーム

使用方法をカスタマイズできるように、メインストリームやサブストリーム以外のストリームも提供される場合があります。

カスタムビデオを設定する

必要に応じて、ビデオストリームを新たに設定することが可能です。カスタムビデオのストリームの場合、プレビューはできますが、録画や再生はできません。

ステップ

注意

- この機能は特定のデバイスでのみサポートされます。
 - デバイスを復元すると（デフォルト設定の復元ではありません）、カスタムビデオのストリーム量やその名前は保持されますが、関連するパラメータは復元されます。
-

1. **+**をクリックして、ストリームを追加します。
 2. 必要に応じてストリーム名を変更します。
-

注意

ストリーム名には最大32文字の文字や記号（&、<、>、'、"を除く）が使用可能です。

3. ストリームパラメータ（解像度、フレームレート、最大ビットレート、ビデオエンコーディング）をカスタマイズします。
 4. オプション: 必要に応じてストリームの説明を追加します。
 5. オプション: カスタムストリームが不要な場合は、**×**をクリックして削除します。
 6. **[保存]**をクリックします。
-

4.1.2 ビデオタイプ

ストリームに含めるコンテンツ（ビデオや音声）を選択します。

ビデオ

ストリームにはビデオコンテンツのみが含まれます。

ビデオとオーディオ

ビデオと音声のコンテンツは、コンポジットストリームに含まれます。

4.1.3 解像度

実際のニーズに合わせてビデオ解像度を選択してください。解像度を上げると、必要になる帯域幅やストレージが大きくなります。

4.1.4 ビットレートタイプと最大ビットレート

固定ビットレート

ストリームをある程度固定されたビットレートで圧縮して送信します。圧縮速度は速くなりますが、画像にモザイクが表示されることがあります。

可変ビットレート

デバイスが、設定された**[最大ビットレート]**以下でビットレートを自動的に調整します。圧縮速度は、平均的なビットレートよりも遅くなります。しかし、複雑なシーンでの画質がその分保証されます。

4.1.5 ビデオ画質

[ビットレートタイプ]が「可変」に設定されている場合、ビデオ品質を設定することが可能です。実際のニーズに合わせ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、必要になる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のことで、フレーム/秒 (fps) で計測されます。

高いフレームレートは映像品質を一貫して維持するので、ビデオストリーム中に動きがある場合には有利です。フレームレートを上げると、必要になる帯域幅やストレージ容量が大きくなりますのでご注意ください。

4.1.7 ビデオエンコーディング

デバイスがビデオエンコーディングで採用する圧縮規格になります。

注意

利用可能な圧縮規格は、デバイスモデルによって異なります。

H.264

H.264は、MPEG-4 Part 10、動画圧縮規格（AVC）とも呼ばれる圧縮規格です。画質を圧縮しないと、圧縮率が上昇し、ビデオファイルがMJPEGやMPEG-4 Part 2を下回るサイズになります。

H.264+

H.264+ は、H.264 をベースに改善された圧縮符号化技術です。H.264+ を有効にすると、その最大平均ビットレートによる、HDD の消費量を見積もることができます。H.264+ では、ほとんどの場面で、同じ最大ビットレートでも、H.264 と比較して、ストレージが最高50%節約されます。

H.264+が有効な場合、**[最大平均ビットレート]**が設定可能です。デバイスはデフォルトで最大平均ビットレート（推奨）を提供しています。ビデオ画質が不十分な場合、パラメータをさらに高い値に調整することが可能です。最大平均ビットレートは、最大ビットレートより大きくできません。

注意

H.264+が有効な場合、**[ビデオの品質]**、**[Iフレーム間隔]**、**[プロフィール]**、**[SVC]**は設定できません。

H.265

H.265は、高効率ビデオコーディング（HEVC）、MPEG-H Part 2 とも呼ばれる圧縮規格です。

解像度、フレームレート、画質は同じですが、H.264よりもビデオ圧縮率が高くなります。

H.265+

H.265+ は、H.265 をベースに改善された圧縮符号化技術です。H.265+を有効にすると、最大平均ビットレートでHDDの消費量を見積もることが可能になります。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最高50%のストレージを節約します。H.265+が有効な場合、**[最大平均ビットレート]**が設定可能です。デバイスはデフォルトで最大平均ビットレート（推奨）を提供しています。ビデオ画質が不十分な場合、パラメータをさらに高い値に調整することが可能です。最大平均ビットレートは、最大ビットレートより大きくできません。

注意

H.265+が有効な場合、**[ビデオの品質]**、**[Iフレーム間隔]**、**[プロフィール]**、**[SVC]**は設定できません。

Iフレーム間隔

Iフレーム間隔は、2つのIフレーム間のフレーム数を定義します。

H.264およびH.265におけるIフレーム（すなわちイントラフレーム）は、他の画像を参照せずに独立してデコードできる自己完結型フレームとなります。Iフレームは、他のフレームよりも多くのビットを消費します。したがって、Iフレームが多い、すなわちIフレーム間隔が短いビデオほど、データビットの生成が安定になり、信頼性も高くなりますが、必要になるストレージ容量が大きくなります。

SVC

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

SVC標準化の目的は、サブセットビットストリームと同じ量のデータで既存のH.264 または H.265デザインを使用して達成されるのと同様の複雑さと再構成画質でデコードできるサブセットビットストリームを1つ以上含む、高画質ビデオビットストリームのエンコードを可能にすることです。サブセットビットストリームは、大きなビットストリームからパケットをドロップすることによって生成されます。

SVCは古いハードウェアとの上位互換性を有しています。高度なハードウェアを使用すると、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と同じビットストリームが消費されますが、それよりも高画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とも呼ばれ、MPEG (Moving Picture Experts Group) が開発したビデオ圧縮形式です。

MJPEG

モーションJPEG (M-JPEGまたはMJPEG) は、フレーム内符号化技術を用いた動画圧縮方式です。MJPEG形式の画像は、個別のJPEG画像として圧縮されます。

プロフィール

この機能は、同じビットレートの下では、プロフィールが複雑になるほど、画像の品質が高くなり、ネットワーク帯域幅の要件も高くなることを意味します。

4.1.8 平滑化

ストリームのスムーズさを指します。スムージングの値が大きいと、ストリームはよりなめらかになりますが、ビデオの品質が十分でない可能性があります。スムージングの値が小さいと、ストリームの品質は向上しますが、なめらかには見えなくなるかもしれません。

4.2 ROI

ROI（関心領域）エンコーディングは、ビデオ圧縮の際ROIと背景情報を識別するのに役立ちます。このテクノロジーでは、関心領域により多くのエンコーディングリソースが割り当てられるため、ROIは向上しますが、背景情報のフォーカスは減少します。

4.2.1 ROIを設定する

ROI (関心領域) エンコーディングにより、関心領域により多くのエンコーディングリソースを割り当てることができるようになり、ROIは向上しますが、背景情報のフォーカスは減少します。

始める前に

ビデオのコーディングタイプを確認してください。ROIは、ビデオのコーディングタイプがH.264またはH.265の場合にサポートされます。

ステップ

1. [環境設定]→[ビデオとオーディオ]→[ROI]と移動します。
2. [有効化]にチェックを入れます。
3. [ストリームタイプ]を選択します。
4. ROI 領域を指定するには、[固定リージョン]で[リージョン番号]を選択します。
 - 1) [領域指定]をクリックします。
 - 2) マウスをビュー画面上でクリックアンドドラッグして、固定領域を指定します。
 - 3) [領域指定を中止する] をクリックします。

注意

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. [リージョン名]と[ROI レベル]を入力します。

6. **[保存]**をクリックします。

 **注意**

ROIレベルが高いほど、検出される領域の画像がクリアになります。

7. オプション: 複数の固定領域を指定する必要がある場合、他の領域番号を選択して、上記の手順を繰り返します。

4.2.2 顔追跡のROIを設定する

ROIで顔追跡機能が有効で、顔がライブ画像に表示されると、顔の画像は周囲よりクリアになります。

ステップ

1. ROI 設定ページへ移動します: **[環境設定]**→**[ビデオとオーディオ]**→**[ROI]**。
2. **[顔追跡有効]**にチェックを入れます。
3. **[ダイナミックトラッキング]**で**[ROI レベル]**を選択します。

 **注意**

ROI レベルは画像品質の向上レベルを意味します。値が大きいほど、画像の品質はよくなります。

4. **[保存]**をクリックします。

4.2.3 ターゲット追跡のROIを設定する

この機能を有効にすると、ライブ画像や録画で、動いているターゲットが他の領域よりもクリアになります。

始める前に

[環境設定] → **[PTZ]** → **[スマートトラッキング]** と移動して、スマート追跡設定を完了します。

ステップ

1. **[環境設定]**→**[ビデオとオーディオ]**→**[ROI]**と移動します。
-

2. **[目標追跡有効]**にチェックを入れます。
3. ターゲット追跡の**[ROI レベル]**を設定します。値が大きいほど画像はクリアになります。
4. **[保存]**をクリックします。

4.2.4 ナンバープレート追跡のROIを設定する

ROI でナンバープレート追跡のROI機能が有効で、ナンバープレートがライブ画像に表示されると、ナンバープレートの画像は周囲よりクリアになります。

ステップ

1. ROI 設定ページへ移動します：**[環境設定]**→**[ビデオとオーディオ]**→**[ROI]**。
2. **[ナンバープレート追跡有効]**にチェックを入れます。
3. **[ダイナミックトラッキング]**で**[ROI レベル]**を選択します。

注意

ROI レベルは画像品質の向上レベルを意味します。値が大きいほど、画像の品質はよくなります。

4. **[保存]**をクリックします。

4.3 ストリーム上の情報表示

被写体（人間、車両など）の情報は、ビデオストリームに記録されます。接続された背面デバイスやクライアントソフトウェアにルールを設定し、ラインクロスや侵入などのイベントを検知することができます。

ステップ

1. 設定ページに移動します：**[環境設定]**→**[ビデオとオーディオ]**→**[複数ストリーム情報表示]**。
2. **[デュアル VCA 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。

4.4 音声設定

これは、音声エンコーディング、環境ノイズフィルタリングなどの音声パラメータを設定する機能です。

音声設定ページへ移動します：**[環境設定]**→**[ビデオとオーディオ]**→**[オーディオ]**。

4.4.1 音声圧縮

音声の音声エンコード圧縮を選択します。

4.4.2 音声入力

注意

- 必要に応じて音声入力デバイスを接続する。
- 音声入力表示は、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、高出力で音声入力デバイスに接続する場合、 [音声入力] を [LineIn] に設定します。
MicIn	マイクやパッシブピックアップなど、低出力の音声入力デバイスに接続する場合、 [音声入力] を [MicIn] に設定します。

4.4.3 音声出力

注意

必要に応じて音声出力デバイスを接続する。

これは、デバイスの音声出力のスイッチです。必要に応じて音声出力を調整することが可能です。無効にすると、デバイスの音声出力が全く出なくなります。音声出力表示は、デバイスのモデルによって異なります。

4.4.4 環境ノイズフィルター

オフまたはオンに設定できます。この機能が有効の場合、環境中のノイズをある程度フィルターできます。





4.5 双方向音声

モニタリングセンターとモニタリング画面のターゲット間の双方向音声機能が可能になります。

始める前に

- デバイスに接続されている音声入力デバイス（ピックアップやマイクロフォン）と音声出力デバイス（スピーカー）が正常に動作していることを確認します。デバイス接続については、音声入出力の各デバイスの仕様を参照してください。
- デバイスにマイクとスピーカーが内蔵されている場合、双方向音声機能を直接有効化することが可能です。

ステップ

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、カメラの双方向音声機能を有効にします。
3.  をクリックして、 を選択し、スライダーを動かして音量を調整します。
4.  をクリックして、双方向音声機能を無効にします。

4.6 ディスプレイ設定

画像の機能を調整するためのパラメータ設定が利用できます。

[環境設定]→[画像]→[ディスプレイ設定]と移動します。

[デフォルト]をクリックして、設定を復元します。

4.6.1 シーンモード

さまざまな導入環境に合わせて予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。実際の導入環境に合わせてシーンを選択し、ディスプレイ設定をスピーディに行います。

画像設定

[輝度]、[彩度]、[色彩]、[コントラスト]、[明度]を調整して、卓越した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、光感度の組み合わせによって制御されます。画像効果は、露出パラメータを設定することで調整することが可能です。

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]を設定する必要があります。

フォーカス

フォーカスモードと最小フォーカス距離を調整するオプションが利用できます。

フォーカスモード

自動

シーンが変化すると、デバイスは自動的にフォーカスを合わせます。オートモードで画像のフォーカスが不十分な場合、画像の光源を減らし、ライトの点滅を控えてください。

セミオート

PTZやレンズがズームすると、ただちにデバイスはフォーカスを合わせます。画像が鮮明な場合、シーンが変化してもフォーカスは変わりません。

手動

ライブビューページでフォーカスを手動で調整することが可能です。

最低撮影距離

シーンとレンズ間の距離が最小フォーカス距離より近い場合、レンズはフォーカス合わせません。

日中/夜間切り替え

日中/夜間切り替え機能により、日中モードではカラー画像を、夜間モードで白黒画像を表示できるようになっています。モードの切り替えは設定可能です。

日

画像は常にカラー表示です。

夜間

画像は常に白黒表示です。

自動

カメラは日中モードと夜間モードを光量に応じて自動的に切り替えます。

スケジュール切替

[開始時間]と**[終了時間]**を設定し、日中モードの継続時間を設定します。

アラーム入力トリガー

2種類のトリガー・モードを利用できます：**日**と**ナイト**。たとえば、トリガーモードが夜

間の場合、デバイスがアラーム入力信号を受信すると、画像は白黒表示に切り替わります。

注意

日中/夜間切り替え機能はモデルによって異なります。

グレースケール

グレースケールは[0-255]または[16-235]の範囲を選択することが可能です。

回転

有効にすると、ライブビューは反時計回りに90°回転します。たとえば、1280×720は回転して720×1280になります。

この機能を有効にすると、垂直方向で監視の有効範囲を変更することが可能です。

レンズ歪み補正

電動レンズを備えたデバイスでは、画像が若干度歪曲して見えることがあります。この機能を有効にすると、歪曲を補正できます。

注意

- この機能は、電動レンズを装備した特定の装置でのみサポートされます。
 - 尚、この機能を有効にすると、画像の端が欠落します。
-

BLC

強い逆光が当たっている被写体に焦点を合わせると、被写体は暗くなりすぎて明瞭に見えなくなります。BLC（逆光補正）により、光を補正して手前の被写体がクリアに見えるようになります。BLCモードが**カスタマイズ**に設定されている場合、ライブビュー画像上に赤い四角形でBLC領域を指定することが可能です。

WDR

WDR (ワイドダイナミックレンジ)機能により、照明の差が大きい環境でもカメラはクリアな画像を提供できるようになります。

フィールド内に非常に明るい領域と非常に暗い領域の両方が同時に存在する場合、WDR機能を有効にして、レベルを設定することが可能です。WDRは、自動的に画像全体の輝度のバランスをとって、細部までクリアな画像を提供します。

注意

WDRを有効にすると、他の一部の機能がサポートされ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イスを参照してください。

HLC

画像の明るい領域が露出過剰で、暗い領域が露出不足の場合、HLC (ハイライト圧縮) 機能を有効にして、明るい領域を暗くし、暗い領域を明るくすることで、画像全体の光のバランスを保つことができます。

ホワイトバランス

ホワイトバランスは、カメラの白色のレンディション機能です。環境に合わせて色温度を調整するために使用します。

デジタルノイズリダクション

デジタルノイズリダクションは、画像ノイズを低減し、画質を向上させるために使用します。[ノーマルモード]と[エキスパートモード]が選択できます。

ノーマル

DNRレベルを設定して、ノイズリダクション率を制御します。レベルが高いほど、ノイズリダクション率が高くなります。

エキスパート

空間DNRと時間DNRの両方に対してDNRレベルを設定して、ノイズリダクション率を制御します。レベルが高いほど、ノイズリダクション率が高くなります。

くもり除去

環境にかすみがかかり、画像がぼやけている時にはくもり除去機能を有効化できます。細部が強調され、画像がより明瞭になります。

EIS

ジッター補正技術を用いて、ビデオ画像の安定性を向上させます。

ミラー

ライブビュー画像が実際のシーンと反転している場合、この機能により画像を正常に表示させることができます。

必要に応じてミラーモードを選択します。

注意

この機能を有効にすると、ビデオ録画が短時間中断されます。

4.6.2 画像パラメータ切替

デバイスは、設定された時間内に自動的に画像パラメータを切り替えます。

[画像パラメータ切替設定]のページに移動します：**[環境設定]→[画像]→[画像パラメータ切替]**で、必要に応じてパラメータを設定します。

スイッチの機能を設定する

特定の時間帯になったら、自動的に画像パラメータをシーンに切り替えます。

ステップ

1. **[有効化]**にチェックを入れます。
2. 該当の時間帯やシーンを選択して設定します。

注意

シーン設定については、**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。

4.6.3 ビデオ規格

ビデオ規格は、表示される色数や解像度を定めるビデオカードやビデオディスプレイデバイスの機能です。最も一般的に使用されているビデオ規格はNTSCとPALの2つです。NTSCでは、毎秒30フレームが送信されます。各フレームは、525本の個別のスキャンラインで構成されています。PALでは、毎秒25フレームが送信されます。各フレームは、625本の個別のスキャンラインで構成されています。お住まいの国のビデオ方式に合わせて、ビデオ信号規格を選択してください。

4.6.4 ローカルビデオ出力

デバイスに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、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可能です。

出力モードのオン/オフを選択して、出力を制御します。

4.7 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、OSD（オンスクリーンディスプレイ）情報をカスタマイズすることが可能です。

[OSD設定]のページに移動します：**[環境設定]**→**[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。

キャラクターセット

表示される情報のキャラクター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、**[EUC-KR]**を選択します。それ以外の場合は、**[GBK]**を選択します。

表示情報

カメラ名、日付、週、関連する表示フォーマットを設定します。

テキストオーバーレイ

画像にカスタマイズされたオーバーレイテキストを設定します。

OSDパラメータ

[表示モード]、**[OSDサイズ]**、**[フォント色]**、**[位置合わせ]**などのOSDパラメータを設定します。

4.8 プライバシーマスクの設定

この機能では、ライブビュー内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。デバイスをどのように動かしても、ブロックされたシーンは表示されません。

ステップ

1. **[プライバシーマスク設定]**のページへ移動します：**[環境設定]**→**[画像]**→**[プライバシーマスク]**。
2. **[プライバシーマスクを有効化]**にチェックを入れます。
3. **[領域指定]**をクリックします。ライブビューでマウスをドラッグし、保護する領域を指定します。

領域の角をドラッグする

領域のサイズを調整します。

領域をドラッグする

領域の位置を調整します。

[すべてクリア]をクリックする

設定した領域をすべて消去します。

4. **[領域指定を中止する]**をクリックします。
5. **[保存]**をクリックします。

 **注意**

設定がサポートできるエリアは4つまでです。

4.9 オーバーレイ画像

カスタマイズした画像をライブビューに重ねて表示します。

始める前に

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

ステップ

1. [画像オーバーレイ設定]のページへ移動します：**[環境設定]→[画像]→[画像オーバーレイ]**。
2. **[ブラウザ]**をクリックして画像を選択し、**[アップロード]**をクリックします。
正常にアップロードされると、ライブビューに赤い四角形の画像が表示されます。
3. **[ピクチャオーバーレイを有効]**にチェックを入れます。
4. 画像をドラッグして位置を調整します。
5. **[保存]**をクリックします。

4.10 ターゲットクロップの設定

画像をトリミングし、ターゲット領域の画像のみを送信、保存して、送信帯域幅やストレージを節約することが可能です。

ステップ

1. **[環境設定]→[ビデオとオーディオ]→[区域クリッピング]**と移動します。
2. **[区域クリッピング有効]**にチェックを入れ、**[ストリームタイプ]**に**[3番目のストリーム]**を設定します。

 **注意**

ターゲットクロップを有効にすると、3番目のストリーム解像度は設定できなくなります。

3. **[クリッピング解像度]**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領域にドラッグします。
5. [保存]を押す。

 **注意**

- ターゲットクロップは一部のモデルのみでサポートされ、機能はカメラのモデルによって異なります。
 - ターゲットクロップを有効にすると、一部の機能が無効になる場合があります。
-

D'SSECURITY

CHAPTER 5 ビデオ録画と画像キャプチャ

このパートでは、ビデオクリップと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の操作について説明します。

5.1 ストレージ設定

このパートでは、複数の共通ストレージパスの構成について説明します。

5.1.1 新規または暗号化されていないメモリカードの設定

始める前に

新規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。インストールの詳細については、デバイスの『クイックスタートガイド』を参照してください。

ステップ

1. [環境設定]→[ストレージ]→[ストレージマネジメント]→[HDD マネジメント]と移動します。
2. メモリカードを選択します。

注意

[アンロック]ボタンが表示されたら、まず最初にメモリカードのロックを解除する必要があります。詳細については**メモリカード状態の検出**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[未フォーマット]から[通常]に変わると、メモリカードは使用可能な状態になります。
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) 暗号パスワードを設定します。
 - 3) [OK]をクリックします。

[暗号化ステータス]が[暗号化済み]に変わると、メモリカードは使用可能な状態になり

ます。

注意

暗号パスワードは大切に保管してください。暗号パスワードを忘れた場合、パスワードを確認することはできません。

5. オプション: メモリカードの[ハードディスク容量配属]を定義します。必要に応じて、さまざまなコンテンツを保存する率（パーセンテージ）を入力します。
6. [保存]をクリックします。

メモリカード状態の検出

デバイスは、Hikvisionメモリーカードの状態を検出します。メモリカードが異常を検出すると、通知されます。

始める前に

設定のページは、Hikvisionメモリーカードがデバイスに取り付けられている場合のみ表示されます。

ステップ

1. [環境設定]→[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]と移動します。
2. [状態検知]をクリックして、メモリカードの[残り寿命]と[健全性の状態]を確認します。

残り寿命

録画残り時間をパーセンテージで示しています。メモリーカードの録画残り時間は、カードの容量と録画のビットレートなどの要素で変動します。録画残り時間が充分でない場合にはメモリーカードの交換が必要です。

健全性の状態

メモリーカードの状態を示します。正常性のステータスは、良好、異常、損傷の3種類です。**[監視スケジュール]** および **[リンク方式]** が設定されている状態でステータスが良好以外になった場合、通知されます。

注意

正常性ステータスが「良好」以外になった場合、メモリーカードの交換が推奨されます。

3. **[R/W ロック]**をクリックして、メモリーカードの読み取りと書き込みの許可を設定します。
 1. ロックを追加して、**[ロック切替]**でオンを選択してください。
 2. パスワードを入力します。
 3. **[保存]**をクリックします。

アンロック

- ロックされたメモリーカードをロックを行ったデバイスで使用すると、自動的にアンロックされます。ユーザー側ではアンロックの操作は必要ありません。
- ロックされたメモリーカードを他のデバイスで使用する場合、**[HDD管理]**からメモリーカードを手動でアンロックすることが可能です。メモリーカードを選択し、**[アンロック]**をクリックします。パスワードを正しく入力するとアンロックされます。
 1. ロックを外して、**[ロック切替]**でオフを選択してください。
 2. **[パスワード設定]**でパスワードを入力します。
 3. **[保存]**をクリックします。

注意

- **R/Wロック**を設定できるのは管理者ユーザーのみです。
 - メモリーカードはアンロックされている場合のみ読み書きが可能です。
 - メモリーカードをロックしたデバイスが工場出荷状態に復元された場合、**[HDD管理]**からメモリーカードをアンロックすることが可能です。
-

4. **[アラームスケジュール]**と**[リンク方法]**を設定します。詳細については**監視スケジュールの設定とリンク方式の設定**を参照してください。
 5. **[保存]**をクリックします。
-

5.1.2 FTP設定

FTPサーバを設定すると、イベントや時間指定のスナップショットタスクによってキャプチャされた画像を保存できるようになります。

始める前に

はじめにFTPサーバのアドレスを取得します。

ステップ

1. [環境設定]→[ネットワーク]→[詳細設定]→[FTP]と移動します。
2. FTP 設定を設定します。

FTPプロトコル

FTPとSFTPが選択可能です。アップロードするファイルは、SFTPプロトコルを使用して暗号化されます。

サーバアドレスとポート

FTPサーバのアドレスと対応するポート。

ユーザー名とパスワード

FTPユーザーは画像アップロードの権限が必要です。

FTPサーバが匿名ユーザーによる画像アップロードをサポートする場合、**[匿名]**にチェックを入れ、アップロード中にデバイス情報を非表示にすることが可能です。

ディレクトリ構造

FTPサーバにスナップショットを保存するパス。

画像保存間隔

画像をよりよく管理するために、画像保存間隔を 1 日から 30 日の範囲で設定できます。同じ時間間隔でキャプチャした画像はすべて、その時間間隔の開始日と終了日から生成された名前のフォルダに保存されます。

画像の名前

キャプチャした画像の命名ルールを設定します。ドロップダウンリストで[デフォルト]を選択すると、「IP address_channel number_capture time_event type.jpg」のようにデフォルトのルールを使用することが可能です（例：

10.11.37.189_01_20150917094425492_FACE_DETECTION.jpg）。または[カスタムプリフィックス]をデフォルト命名ルールに追加してカスタマイズすることもできます。

3. [画像アップロード]にチェックを入れて、FTP サーバへのスナップショットのアップロードを有効化します。
4. [自動ネットワーク補填機能を有効にする]にチェックを入れます。

注意

[リンク方式]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填機能を有効にする]は両方同時に有効化する必要があります。

5. [テスト]をクリックして、FTP サーバを確認します。
6. [保存]をクリックします。

5.1.3 NAS設定

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

始める前に

はじめに、ネットワークディスクのIPアドレスを取得します。

ステップ

1. [NAS 設定]のページへ移動します：[環境設定]→[ストレージ]→[ストレージマネジメント]→[NetHDD]。
2. [HDD No.]をクリックします。ディスクのサーバアドレスとファイルパスを入力します。

サーバアドレス

ネットワークディスクのIPアドレス。

ファイルパス

ネットワークディスクファイルの保存先パス。

マウンティングタイプ

オペレーションシステムに合わせてファイルシステムプロトコルを選択します。

[SMB/CIFS]が選択されている場合、セキュリティを保証するために、ネットワークHDDのユーザー名とパスワードを入力します。

3. [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。
4. [保存]をクリックします。

5.1.4 eMMCの保護

eMMCの健全性の状態が不良の場合、ストレージメディアとしてのeMMCの使用を自動的に停止します。

注意

eMMCの保護は、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ます。

設定を行うには、[環境設定]→[システム]→[メンテナンス]→[システムサービス]と移動します。

eMMCは、エンベデッドマルチメディアカードの略称で、組み込み型の不揮発性メモリーシステムです。デバイスのキャプチャ画像やビデオを保存することができます。

デバイスは、eMMCの健全性の状態を監視し、状態が不良の場合、eMMCをオフにします。そのままの状態でも消耗したeMMCを使用すると、デバイスが起動を失敗する恐れがあります。

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、クラウドからの画像に対して、画像の分析を直接要求します。この機能は特定のデ

バイスでのみサポートされます。

ステップ



注意

クラウドストレージが有効になっている場合、画像は優先的にクラウドストレージサーバに保存されます。

1. **[環境設定]**→**[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]**と移動します。
2. **[クラウドストレージ有効]**にチェックを入れます。
3. 基本パラメータを設定します。

プロトコルバージョン	クラウドストレージサーバのプロトコルバージョン。
サーバIP	クラウドストレージサーバのIPアドレス。IPv4アドレスをサポートします。
サーバポート	クラウドストレージサーバのポート。6001はデフォルトのポート番号なので、編集しないでください。
ユーザー名とパスワード	クラウドストレージサーバのユーザー名とパスワード。
画像ストレージプールID	クラウドストレージサーバ内の画像ストレージ領域ID。ストレージプールIDとストレージ領域 IDが同じであることを確認します。

4. **[テスト]**をクリックして、設定されている各設定をテストします。
5. **[保存]**をクリックします。

5.2 ビデオ録画

このパートでは、手動やスケジュール予約による録画、再生、録画ファイルのダウンロードの操作を説明します。

5.2.1 自動録画

この機能を使用すると、設定された時間帯にビデオを自動的に録画することが可能です。

始める前に

[**継続**]以外の各録画タイプのイベント設定で[**録画をトリガー**]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。

ステップ

1. [環境設定]→[ストレージ]→[スケジュール設定]→[記録スケジュール]と移動します。
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。

注意

録画タイプはモデルにより異なります。

連続

ビデオはスケジュールに従って継続的に録画されます。

動体

動体検知が有効で、リンク方式でトリガー録画が選択されている場合、被写体の動きが記録されます。

アラーム

アラーム入力が有効で、リンク方式でトリガー録画が選択されている場合、外部アラーム入力デバイスからアラーム信号を受信した後にビデオが記録されます。

動体 | アラーム

動体を検知した時、または外部アラーム入力デバイスからアラーム信号を受信した時にビデオが録画されます。

動体&アラーム

動体を検知し、かつ外部アラーム入力デバイスからアラーム信号を受信した時のみビデオが録画されます。

イベント

イベントを検知した時、ビデオが録画されます。

4. 選択した録画タイプのスケジュールを設定します。設定操作については、**監視スケジュールの設定**を参照してください。
5. [詳細設定]をクリックして、詳細設定を行います。

上書き

ストレージ容量がいっぱいになった場合、ビデオ録画を上書きするには、**[上書き]**を有効にします。上書きができないと、カメラは新しいビデオを録画することができなくなります。

プレ録画

スケジュールされた時間の前に録画する時間。

ポスト録画

スケジュールされた時間の後に録画する時間。

ストリームタイプ

録画のストリーム種別を選択します。

注意

ストリームタイプを高いビットレートで選択すると、実際のプレ録画やポスト録画の時間が、設定値よりも短くなる場合があります。



録画の有効期限

録画は有効期限を過ぎると削除されます。有効期限の時間は設定可能です。一旦削除された録画は復元できませんので注意してください。

6. **[保存]**をクリックします。

5.2.2 手動で録画する

ステップ

1. **[環境設定]**→**[ローカル]**と移動します。
2. 録画されるファイルの**[記録ファイルサイズ]**と保存パスを設定します。
3. **[保存]**をクリックします。
4. をクリックすると録画を開始します。をクリックすると録画を停止します。

5.2.3 ライトストレージ設定

ライトストレージを有効にすると、監視中のシナリオ内で動体がない場合、ビデオストリームのフレームレートとビットレートを下げて、メモ리카ードのストレージ時間を長くすることができます。

ステップ

1. **[環境設定]**→**[ストレージ]**→**[ストレージマネジメント]**→**[Lite ストレージ]**と移動します。
2. **[有効化]**にチェックを入れて、レベルを設定します。レベルが高いほど、フレームレートとビットレートも大きくなり、推奨ストレージ時間は短くなります。
3. ストレージ時間を設定します。デバイスはビットレートを自動的に計算し、メモ리카ードの容量とレベルに合わせて推奨されるストレージ時間を提供します。ストレージ時間をデバイスの推奨時間に設定することをお勧めします。

注意

- ライトストレージが有効になっている場合、フォーマットされていないメモ리카ードは自動的にフォーマットされます。
- メモ리카ードに表示される空き容量は、デフォルトの場合、**[ストレージ]**→**[ストレージマネジメント]**→**[ハードディスク容量配属]**にある**[録画の比率（パーセンテージ）]**割り当てられます。必要に応じて調整することが可能です。

- この機能は一部のデバイスモデルのみでのサポートになります。
-

5.2.4 ビデオの再生とダウンロード

ローカルストレージやネットワークストレージに保存されたビデオの検索、再生、ダウンロードが可能です。

ステップ

1. **[再生]**をクリックします。
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. ▶をクリックして、ビデオファイルを再生します。
 - ✂をクリックして、ビデオファイルをクリップします。
 - ⏮をクリックして、ビデオファイルをフルスクリーンで再生します。**[ESC]**ボタンを押して、フルスクリーン表示を終了します。

注意

[環境設定]→**[ローカル]**と移動して、**[クリップの保存]**をクリックしてクリップされたビデオファイルの保存パスを変更します。

4. 再生インターフェースで⏴をクリックして、ファイルをダウンロードします。
 - 1) 検索条件を設定し、**[検索]**をクリック します。
 - 2) ビデオファイルを選択して、**[ダウンロード]**をクリックします。

注意

[環境設定]→**[ローカル]**と移動して、**[ダウンロードファイルの保存]**をクリックしてダウンロードしたビデオファイルの保存パスを変更します。

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することが可能です。スナップショットを表示およびダウンロードすることが可能です。

5.3.1 自動的にキャプチャする

この機能を使用すると、設定された時間帯に画像を自動的にキャプチャすることが可能です。

始める前に

イベントトリガーのキャプチャが必要な場合、イベント設定で関連するリンク方式を設定する必要があります。イベント設定については**イベントとアラーム**を参照してください。

ステップ

1. **[環境設定]**→**[ストレージ]**→**[スケジュール設定]**→**[キャプチャー]**→**[キャプチャパラメータ]**と移動します。
2. キャプチャタイプを設定します。

タイミング

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時に画像をキャプチャします。

3. **[フォーマット]**、**[解像度]**、**[品質]**、**[間隔]**、**[キャプチャ番号]**を設定します。
4. スケジュール時間の設定については、**監視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。

5.3.2 手動でキャプチャする

ステップ

1. **[環境設定]**→**[ローカル]**と移動します。
2. スナップショット用に、**[画像フォーマット]**と**[パスの保存]**を設定します。

JPEG

このフォーマットの画像サイズは比較的小さく、ネットワーク伝送に適しています。

BMP

画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傍にある  をクリックして、画像を手動でキャプチャします。

5.3.3 タイミングウェイクの設定

デバイスがスリープ状態になると、設定された時間間隔でスリープを解除して、画像をキャプチャおよびアップロードします。

ステップ

1. **[環境設定]**→**[システム]**→**[システム設定]**→**[Power Consumption Mode]**と移動して、**[Sleep Schedule]**で**[時間スケジュール]**をクリックし、**[Sleep Capture Interval]**を設定します。
2. **[環境設定]**→**[イベント]**→**[基本イベント]**→**[Timing Wake]**と移動します。
3. **[有効化]**にチェックを入れます。
4. **[キャプチャタイプ]**を選択します。
5. リンク方式の設定については、**リンク方式の設定**を参照してください。
6. **[保存]**をクリックします。

結果

デバイスがスリープキャプチャ間隔でスリープを解除すると、画像をキャプチャしてアップロードします。

5.3.4 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上に保存された画像の検索、閲覧およびダウンロードができます。

ステップ

1. **[画像]**をクリックします。
2. 検索条件を設定し、**[検索]**をクリックします。
一致する画像がファイルリストに表示されます。

3. 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。
-

 **注意**

[環境設定]→**[ローカル]**と移動して、**[スナップショットを保存]**をクリックし、画像の保存パスを変更します。

D'SSECURITY

CHAPTER 6 イベントとアラーム

このパートでは、イベントの設定について説明します。デバイスは、トリガーされたアラームに対して一定の対処をします。

6.1 基本イベント

6.1.1 動体検知の設定

検知領域内で動体を検知し、連動アクションを作動させることができるようになります。

ステップ

1. [環境設定]→[イベント]→[基本イベント]→[動体検知]と移動します。
2. [動体検知有効]にチェックを入れます。
3. オプション: 画像内の動体を緑で強調して表示します。
 - 1) [モーションの動的解析を有効]にチェックを入れます。
 - 2) [環境設定]→[ローカル]と移動します。
 - 3) [ルール]を[有効化]に設定します。
4. [設定モード]を選択し、ルールの領域とパラメータを設定します。
 - 通常モードの詳細については、**通常モード**を参照してください。
 - エキスパート・モードの詳細については、**エキスパートモード**を参照してください。
5. [監視スケジュール]と[リンク方式]を設定します。監視スケジュールの設定に関する詳細については、**監視スケジュールの設定**を参照してください。リンク方式の詳細については、**リンク方式の設定**を参照してください。
6. [保存]をクリックします。

エキスパートモード

実際のニーズに合わせて、日中と夜間に異なる動体検知パラメータを設定することが可能です。

ステップ

1. **[環境設定]**で**[エキスパートモード]**を選択します。
2. エキスパートモードのパラメータを設定します。

定期画像設定

オフ

画像切替が無効になります。

自動切替

システムは、環境にあわせて日中/夜間モードを自動的に切り替えます。日中はカラー画像、夜間は白黒画像で表示されます。

スケジュール切替

システムにより、スケジュールに合わせて日中/夜間モードが自動的に切り替わります。設定された時間帯が日中モードになり、それ以外の時間帯は夜間モードに切り替わります。

感度

感度の値が高いほど、動体検知の感度も上がります。スケジュールされた画像設定が有効になっている場合、日中/夜間の感度を個別に設定することが可能です。

3. **[領域]**を選択して、**[領域指定]**をクリックします。ライブ画像上でマウスをクリックアンドドラッグして、マウスを離すと領域の指定が終了します。



図 6-1 ルールを設定する

描画をやめる 領域の指定を終了します。

すべてクリア 領域をすべて削除します。

4. **[保存]**をクリックします。

5. オプション: 複数の領域を設定するには、上記の手順を繰り返します。

通常モード

デバイスのデフォルトパラメータに合わせて動作検知パラメータを設定することが可能です。

ステップ

1. **[環境設定]**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、動体検知の感度も上がります。感度が0に設定されている場合、動体検知とダイナミック分析は有効になりません。

3. **[領域指定]** をクリックします。ライブビデオ上でマウスをクリックアンドドラッグして、マウスを離すと領域の指定が終了します。

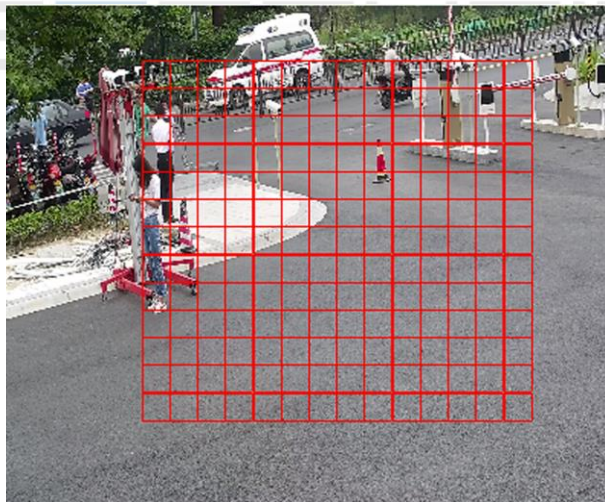


図 6-2 ルールを設定する

描画をやめる 領域の指定を終了します。

すべてクリア 領域をすべて削除します。

4. オプション: 複数の領域のパラメータを設定する場合、上記の手順を繰り返します。

6.1.2 ビデオ干渉アラームの設定

設定されたエリアが隠れてしまい、正常に監視できない場合、アラームが作動し、デバイスは特定のアラーム対処アクションを実行します。

ステップ

1. **[環境設定]**→**[イベント]**→**[基本イベント]**→**[ビデオ干渉]**と移動します。
2. **[有効化]**にチェックを入れます。
3. **[感度]**を設定します。値が大きいほど、隠れた領域を検知しやすくなります。
4. **[領域指定]**をクリックして、ライブビデオ上でマウスをドラッグし領域を指定します。

描画をやめる 指定を終了します。

すべてクリア 領域をすべて削除します。

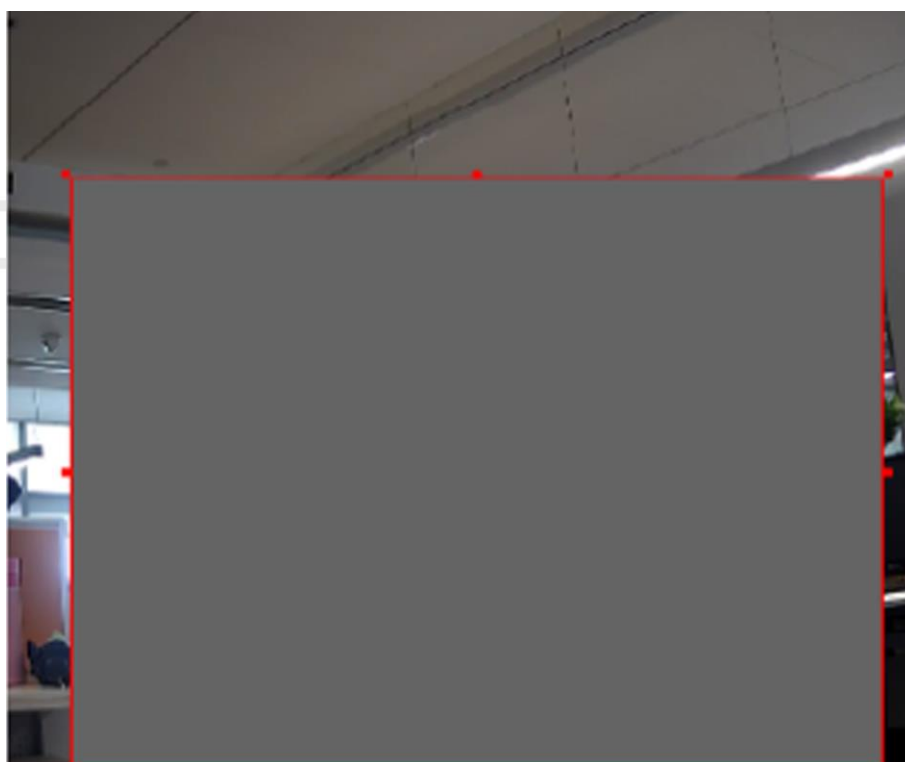


図 6-3 ビデオ干渉の領域を設定する

5. スケジュール時間の設定については**監視スケジュールの設定**を参照してください。リンク方式の設定については**リンク方式の設定**を参照してください。
6. **[保存]**をクリックします。

6.1.3 PIRアラームの設定

PIR (受動型赤外線) アラームは、侵入者が検知視界内で動いた際にアラームを起動します。人や、犬、猫などの血流のある生物によって発せられる熱エネルギーを検知できます。

ステップ

注意

PIRアラームは、一部のモデルのみのサポートになります。

1. [環境設定]→[高度な設定]→[基本イベント]→[PIR アラーム]と移動します。
2. [PIR アラームを有効化]にチェックを入れます。
3. スケジュール時間の設定については[監視スケジュールの設定](#)を参照してください。リンク方式の設定については[リンク方式の設定](#)を参照してください。
4. [保存]をクリックします。

6.1.4 異常検知アラームの設定

ネットワーク切断などの異常検知時に、デバイスを作動させ、対応するアクションを実行させることが可能です。

ステップ

1. [環境設定]→[イベント]→[基本イベント]→[異常検知設定]と移動します。
2. [異常検知タイプ]を選択します。

HDDフル	HDDに空きがありません。
HDDエラー	HDDにエラーが発生しました。
ネットワーク切断	デバイスがオフラインです。
IPアドレス競合	現在のデバイスのIPアドレスは、ネットワーク内の他のデバイスのIPアドレスと同じです。
不正ログイン	ユーザー名またはパスワードが違います。
電圧不安定	電源電圧が変動しています。

3. リンク方式の設定については**リンク方式の設定**を参照してください。
4. **[保存]**をクリックします。

6.1.5 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、ご利用中のデバイスで対応するアクションが作動します。

始める前に

外部アラームデバイスが接続されていることを確認します。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. **[環境設定]→[イベント]→[基本イベント]→[アラーム入力]**と移動します。
2. **[アラームインプットを処理します]**にチェックを入れます。
3. ドロップダウンリストから**[アラーム入力番号]**と**[アラームの種類]**を選択します。**アラーム名**を編集します。
4. スケジュール時間の設定については**監視スケジュールの設定**を参照してください。リンク方式の設定については**リンク方式の設定**を参照してください。
5. **[...にコピーする]**をクリックし、設定を他のアラーム入力チャンネルにコピーします。
6. **[保存]**をクリックします。

6.1.6 ビデオ品質診断の設定

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

ステップ

1. **[環境設定]→[イベント]→[基本イベント]→[ビデオ品質診断]**と移動します。
2. **[診断タイプ]**を選択します。
3. 対応するパラメータを設定します。

アラーム検知間隔

異常を検知する時間間隔。

感度

値が大きいほど異常を検知しやすくなりますが、誤情報になる可能性も高くなります。

アラーム遅延時間

アラームが設定された回数に達すると、デバイスはアラームをアップロードします。

4. **[有効化]**にチェックを入れると、選択した診断タイプが検知されます。
5. 監視スケジュールを設定します。**監視スケジュールの設定**を参照してください。
6. リンク方式を設定します。**リンク方式の設定**を参照してください。
7. **[保存]**をクリックします。

注意

この機能は特定のデバイスでのみサポートされます。実際の表示はモデルによって異なります。

6.1.7 振動検知の設定

デバイスの振動を検知するために使用します。この機能が有効になっている場合、デバイスはアラームを報告し、連動アクションを作動します。

ステップ

1. **[環境設定]**→**[イベント]**→**[基本イベント]**→**[振動検知]**と移動します。
2. **[有効化]**にチェックを入れます。
3. スライダーをドラッグして検知感度を設定します。また、数値を入力して感度を設定することも可能です。
4. 監視スケジュールを設定します。**監視スケジュールの設定**を参照してください。
5. リンク方式を設定します。**リンク方式の設定**を参照してください。
6. **[保存]**をクリックします。

注意

この機能は特定のデバイスでのみサポートされます。実際の表示はモデルによって異なります。

6.2 スマートイベント

注意

- 一部のデバイスモデルでは、まず **[リソース割り当て]** のページでスマートイベント機能を有効化して、**[機能設定]** のページを表示する必要があります。
 - この機能はカメラのモデルによって異なります。
-

6.2.1 音声異常の検知

音声異常の検知機能により、音量の急激な増大/減少など、監視シーンでの異常音声を検知し、特定のアクションを連動させることが可能です。

ステップ

1. **[環境設定]**→**[イベント]**→**[基本イベント]**→**[オーディオ異常検知]**と移動します。
2. 音声異常検知タイプを選択します（複数選択可）。

オーディオロス検知

オーディオトラックの突発的な欠落を検知します。

音量急増検出

音量の急増を検知します。**[感度]**と**[音響インテンシティ値]**は設定することができます。

 **注意**

- 感度の値が低いほど、変化の検知が鈍くなります。
 - **[音量のしきい値]**は、検知する音量の基準を表します。周辺の平均的な音量で設定することをお勧めします。周辺の音が大きいほど、値も大きくなります。実際の環境に合わせて調整できます。
-

音響急降検出

音量の急激な減少を検知します。**[感度]**は設定することができます。

3. スケジュール時間の設定については**監視スケジュールの設定**を参照してください。リンク方式の設定については**リンク方式の設定**を参照してください。
 4. **[保存]**をクリックします。
-

 **注意**

この機能はカメラのモデルによって異なります。

6.2.2 焦点ボケ検知の設定

レンズの焦点ボケによりぼやけた画像を検知することが可能です。そのような場合、デバイスはアクションを連動させることが可能です。

ステップ

1. **[環境設定]**→**[イベント]**→**[スマートイベント]**→**[焦点ボケ検知]**と移動します。
2. **[有効化]**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、焦点ボケ画像によるアラームを作動しやすくなります。実際の環境に合わせて値を調整することが可能です。
4. リンク方式の設定については、**リンク方式の設定**を参照してください。

5. **[保存]**をクリックします。

 **注意**

この機能は特定のデバイスでのみサポートされます。実際の表示はモデルによって異なります。

6.2.3 シーン変化検知

シーン変化検知の機能は、監視シーンの変化を検知します。このアラームがトリガーされた場合、特定一部のアクションを行うことができます。

ステップ

1. **[環境設定]**→**[イベント]**→**[スマートイベント]**→**[シーン変化検知]**と移動します。
2. **[有効化]**をクリックします。
3. **[感度]**を設定します。値が高いほど、シーン変化を検知しやすくなります。ただし、検知の精度は低下します。
4. スケジュール時間の設定については**監視スケジュールの設定**を参照してください。リンク方式の設定については**リンク方式の設定**を参照してください。
5. **[保存]**をクリックします。

 **注意**

この機能はカメラのモデルによって異なります。

6.2.4 顔検知の設定

検知領域内で顔を検知することができるようになります。顔が検知されると、デバイスはアクションを連動させます。

ステップ

1. **[環境設定]**→**[イベント]**→**[スマートイベント]**→**[顔検出]**と移動します。
2. **[顔検知を有効にする]**にチェックを入れます。
3. オプション: 画像内の顔を強調して表示します。
 - 1) **[顔検知のダイナミック解析を有効にする]**にチェックを入れます。

- 2) **[環境設定]**→**[ローカル]**と移動して、**[ルール]**を設定して**有効化**します。
4. **[感度]**を設定します。感度が低いほど、顔の輪郭や不明瞭な顔は検知しにくくなります。
5. **[監視スケジュール]**と**[リンク方式]**を設定します。監視スケジュールの設定に関する詳細については、**監視スケジュールの設定**を参照してください。リンク方式の詳細については、**リンク方式の設定**を参照してください。
6. **[保存]**をクリックします。

6.2.5 ビデオロスの設定

この機能により、時間内のビデオ信号の損失を検知し、アクションを連動させることが可能です。

ステップ

1. **[環境設定]**→**[イベント]**→**[基本イベント]**→**[ビデオロス]**と移動します。
2. **[有効化]**にチェックを入れます。
3. スケジュール時間の設定については**監視スケジュールの設定**を参照してください。リンク方式の設定については**リンク方式の設定**を参照してください。
4. **[保存]**をクリックします。

6.2.6 侵入検知の設定

事前定義された仮想領域に侵入し徘徊するオブジェクトを検知するため使用します。そのような場合、デバイスはアクションを連動させることが可能です。

ステップ

1. **[環境設定]**→**[イベント]**→**[スマートイベント]**→**[侵入検出]**と移動します。
2. **[有効化]**にチェックを入れます。
3. **[領域]**を選択します。検知領域の設定については、**領域指定**を参照してください。
4. ルールを設定します。

感度

感度は、許容ターゲットの体（または本体）の一部が予め定義した領域に侵入している率（パーセンテージ）を表します。感度 = $100 - S1/ST \times 100$ 。S1は、予め定義した領域を通過するターゲットの体（または本体）の一部を表します。STはターゲット全体を表します。

感度の値が高いほど、アラームが作動しやすくなります。

しきい

しきい値は、オブジェクトが領域内で徘徊する時間のしきい値を表します。1つのオブジェクトがしきい値を超えてとどまっている場合、アラームが作動します。しきい値の値が大きいほど、アラームが作動するまでの時間は長くなります。

検知ターゲット

人間と車両に対して利用可能です。検知ターゲットが選択されていない場合、検知されたすべてのターゲット（人体や車両など）が報告されます。

ターゲットの妥当性

妥当性を高く設定すると、ターゲットの求められる特徴がより明確になるので、アラームの精度が高くなります。特徴がはっきりしないターゲットは検知されません。



図 6-4 ルールを設定する

5. オプション: 複数の領域のパラメータを設定する場合、上記の手順を繰り返します。
6. 監視スケジュールの設定については、**監視スケジュールの設定**を参照してください。リンク方式の設定については、**リンク方式の設定**を参照してください。
7. **[保存]**をクリックします。

6.2.7 ラインクロス検知の設定

予め定義した仮想ラインを通過するオブジェクトを検知するために使用します。そのような場合、デバイスはアクションを連動させることが可能です。

ステップ

1. [環境設定]→[イベント]→[スマートイベント]→[線のクロス検出]と移動します。
2. [有効化]にチェックを入れます。
3. [ライン]を1つ選択して、サイズフィルタを設定します。サイズフィルタの設定については、**サイズフィルタの設定**を参照してください。
4. [領域指定]をクリックすると、ライブビデオに矢印の付いたラインが表示されます。ライブビデオ上で任意の場所にラインをドラッグします。
5. ルールを設定します。

方向

オブジェクトがラインを通過する方向を表します。

A<->B: 双方向でラインを通過するオブジェクトを検知することが可能で、アラームも作動します。

A->B: AサイドからBサイドに設定されたラインを通過する対象のみ検知できます。

B->A: BサイドからAサイドに設定されたラインを通過する対象のみ検知できます。

感度

感度は、許容ターゲットの体（または本体）の一部が予め定義したラインを通過している率（パーセンテージ）を表します。 $\text{感度} = 100 - S1/ST \times 100$ 。S1は、予め定義したラインを通過するターゲットの体（または本体）の一部を表します。STはターゲット全体を表します。感度の値が高いほど、アラームが作動しやすくなります。

検知ターゲット

人間と車両に対して利用可能です。検知ターゲットが選択されていない場合、検知されたすべてのターゲット（人体や車両など）が報告されます。

ターゲットの妥当性

妥当性を高く設定すると、ターゲットの求められる特徴がより明確になるので、アラームの精度が高くなります。特徴がはっきりしな

いターゲットは検知されません。

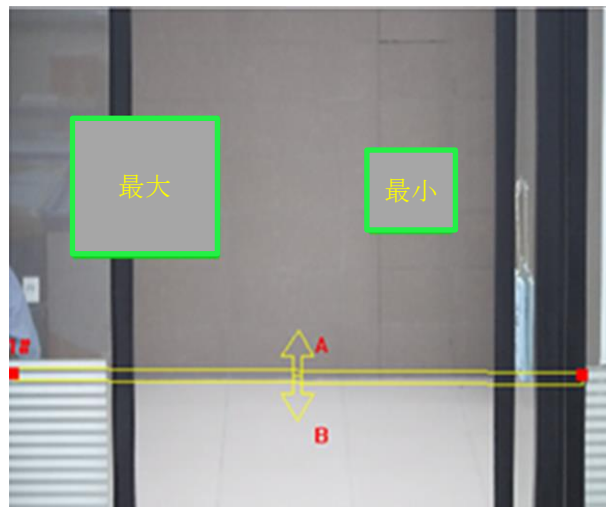


図 6-5 ルールを設定する

6. オプション: 複数の領域のパラメータを設定する場合、上記の手順を繰り返します。
7. 監視スケジュールの設定については、**監視スケジュールの設定**を参照してください。リンク方式の設定については、**リンク方式の設定**を参照してください。
8. **[保存]**をクリックします。

6.2.8 範囲進入検知の設定

領域外から予め定義した仮想領域に進入するオブジェクトを検知するため使用します。そのような場合、デバイスはアクションを連動させることが可能です。

ステップ

1. **[環境設定]**→**[イベント]**→**[スマートイベント]**→**[範囲進入検知]**と移動します。
2. **[有効化]**にチェックを入れます。
3. **[領域]**を1つ選択します。領域の設定については、**領域指定**を参照してください。
4. 検知ターゲット、感度、ターゲットの妥当性を設定します。

感度

感度は、許容ターゲットの体（または本体）の一部が予め定義した領域に進入している率（パーセンテージ）を表します。感度 = $100 - S1/ST \times 100$ 。S1は、予め定義した領域を通過するターゲットの体（または本体）の一部を表します。STはターゲット全体を表します。

感度の値が高いほど、アラームが作動しやすくなります。

検知ターゲット 人間と車両に対して利用可能です。検知ターゲットが選択されていない場合、検知されたすべてのターゲット（人体や車両など）が報告されます。

ターゲットの妥当性 妥当性を高く設定すると、ターゲットの求められる特徴がより明確になるので、アラームの精度が高くなります。特徴がはっきりしないターゲットは検知されません。

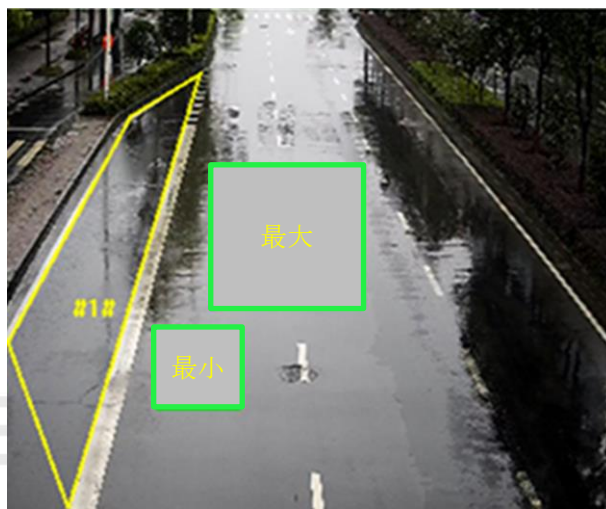


図 6-6 ルールを設定する

5. オプション: 複数の領域のパラメータを設定する場合、上記の手順を繰り返します。
6. 監視スケジュールの設定については、**監視スケジュールの設定**を参照してください。リンク方式の設定については、**リンク方式の設定**を参照してください。
7. **[保存]**をクリックします。

6.2.9 領域退出検知の設定

予め定義した仮想領域を退出するオブジェクトを検知するために使用します。そのような場合、デバイスはアクションを連動させることが可能です。

ステップ

1. **[環境設定]**→**[イベント]**→**[スマートイベント]**→**[領域退出検知]**と移動します。
2. **[有効化]**にチェックを入れます。

3. **[領域]**を1つ選択します。検知領域の設定については、**領域指定**を参照してください。
4. 検知ターゲット、感度、ターゲットの妥当性を設定します。

感度

感度は、許容ターゲットの体（または本体）の一部が予め定義した領域に進入している率（パーセンテージ）を表します。感度 = $100 - S1/ST \times 100$ 。S1は、予め定義した領域を通過するターゲットの体（または本体）の一部を表します。STはターゲット全体を表します。感度の値が高いほど、アラームが作動しやすくなります。

検知ターゲット

人間と車両に対して利用可能です。検知ターゲットが選択されていない場合、検知されたすべてのターゲット（人体や車両など）が報告されます。

ターゲットの妥当性

妥当性を高く設定すると、ターゲットの求められる特徴がより明確になるので、アラームの精度が高くなります。特徴がはっきりしないターゲットは検知されません。

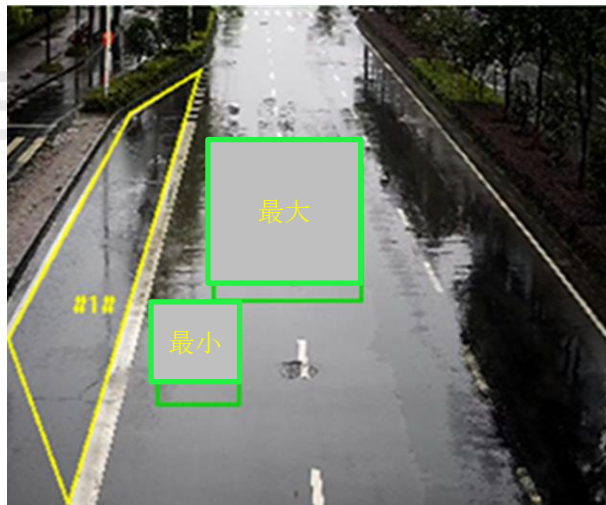


図 6-7 ルールを設定する

5. オプション: 複数の領域のパラメータを設定する場合、上記の手順を繰り返します。
6. 監視スケジュールの設定については、**監視スケジュールの設定**を参照してください。リンク方式の設定については、**リンク方式の設定**を参照してください。
7. **[保存]**をクリックします。

6.2.10 放置手荷物検知の設定

予め定義された仮想領域に放置されたオブジェクトを検知するために使用します。オブジェクトが領域内に放置され、設定時間以上とどまっていると、リンク方式が作動します。

ステップ

1. [環境設定]→[イベント]→[スマートイベント]→[放置手荷物検知]と移動します。
2. [有効化]にチェックを入れます。
3. [領域]を1つ選択します。検知領域の設定については、**領域指定**を参照してください。
4. ルールを設定します。

感度

感度は、許容ターゲットの体（または本体）の一部が予め定義した領域に侵入している率（パーセンテージ）を表します。感度 = $100 - S1/ST \times 100$ 。S1は、予め定義した領域を通過するターゲットの体（または本体）の一部を表します。STはターゲット全体を表します。感度の値が高いほど、アラームが作動しやすくなります。

しきい

領域内でオブジェクトが放置される時間を表します。オブジェクトが領域内に放置され、設定時間以上とどまっていると、アラームが作動します。

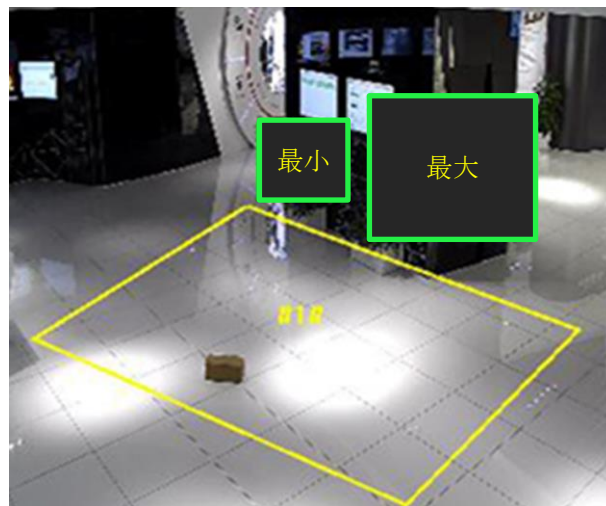


図 6-8 ルールを設定する

5. オプション: 複数の領域のパラメータを設定する場合、上記の手順を繰り返します。

6. 監視スケジュールの設定については、**監視スケジュールの設定**を参照してください。リンク方式の設定については、**リンク方式の設定**を参照してください。
7. **[保存]**をクリックします。

6.2.11 オブジェクト除去検知の設定

陳列された展示物など、予め定義された検知領域からオブジェクトが持ち去られていないかどうかを検知します。その際、デバイスはアクションを連動させることができるので、スタッフは盗難防止の対策をとることが可能になります。

ステップ

1. **[環境設定]**→**[イベント]**→**[スマートイベント]**→**[物体撤去検知]**と移動します。
2. **[有効化]**にチェックを入れます。
3. **[領域]**を選択します。領域の設定については、**領域指定**を参照してください。
4. ルールを設定します。

感度

範囲[1-100]。許容ターゲットの体（または本体）の一部が予め定義した領域から出ている率（パーセンテージ）を表します。

$$\text{感度} = 100 - S1/ST \times 100$$

S1は、予め定義した領域から出ているターゲットの体（または本体）の一部を表します。STはターゲット全体を表します。

例: 値を60に設定した場合、ターゲットの40%の部分が領域を出ている時のみ、除去ターゲットとみなすことが可能になります。

しきい

範囲[5-100秒]は、オブジェクトが領域から除去されてからの時間のしきい値です。値を10に設定すると、10秒間オブジェクトが範囲から離れた後にアラームを起動します。



図 6-9 ルールを設定する

5. オプション: さらに領域を設定する場合、上記手順を繰り返してください。
6. 監視スケジュールの設定については、**監視スケジュールの設定**を参照してください。リンク方式の設定については、**リンク方式の設定**を参照してください。
7. **[保存]**をクリックします。

注意

この機能は特定のデバイスでのみサポートされます。実際の表示はモデルによって異なります。

6.2.12 領域指定

このセクションでは、エリアの環境設定について説明します。

ステップ

1. **[領域指定]** をクリックします。
2. ライブビデオ上でクリックして、検知領域の範囲を指定し、右クリックで指定を完了します。
3. **[保存]**をクリックします。

注意

[すべてクリア]をクリックして、予め定義した領域をすべて消去します。

6.2.13 サイズフィルターの設定

このパートでは、サイズフィルターの設定について説明します。ターゲットのサイズが最大値～最小値の範囲にある場合のみ検知して、アラームが作動します。

ステップ

1. **[最大サイズ]**をクリックして、ライブビデオ上でマウスをドラッグしてターゲットの最大サイズを指定します。
2. **[最小サイズ]**をクリックして、ライブビデオ上でマウスをドラッグしてターゲットの最小サイズを指定します。
3. **[保存]**をクリックします。

D'SSECURITY

CHAPTER 7 ネットワーク設定

7.1 TCP/IP

ネットワーク経由でデバイス进行操作する前に、TCP/IPの設定を適切に行っておく必要があります。IPv4 と IPv6 の両方がサポートされています。両方のバージョンを同時に設定しても、互いに競合することはありません。

[環境設定]→[ネットワーク]→[基本設定]→[TCP/IP]と移動して、パラメータを設定します。

NICタイプ

ネットワーク条件に合わせてNIC（ネットワークインタフェースカード）タイプを選択します。

IPv4

2種類のIPv4モードが利用できます。

DHCP

[DHCP]にチェックを入れると、デバイスは自動的にネットワークからIPv4パラメータを取得します。機能を有効化すると、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可能です。

注意

デバイスが接続されているネットワークは、DHCP（ダイナミック・ホスト・コンフィギュレーション・プロトコル）をサポートしている必要があります。

手動

IPv4パラメータを手動で設定することが可能です。[IPv4アドレス]、[IPv4サブネットマスク]、[IPv4 デフォルトゲートウェイ]を入力し、[テスト]をクリックしてIPアドレスが使用可能かどうかを確認します。

IPv6

3種類のIPv6モードが利用できます。

ルート広告

IPv6アドレスは、ルート通知とデバイスのMACアドレスを組み合わせて生成されます。

注意

ルート通知モードでは、デバイスが接続されているルータからのサポートが必要です。

DHCP

IPv6アドレスは、サーバ、ルータ、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問い合わせてください。

MTU

Maximum Transmission Unit (最大送信単位) 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可能な最大のプロトコルデータユニットのサイズです。

MTU の有効な値の範囲は 1280～1500 です。

DNS

Domain Name Server (ドメインネームサーバ) の略です。ドメイン名を持つデバイスにアクセスする際に、必要になります。また、一部のアプリケーション (Eメール送信など) で必要になる場合もあります。必要に応じて、[優先DNSサーバ]と[代替DNSサーバ]を適切に設定します。

ダイナミックドメイン名

[ダイナミックドメイン名の有効化]にチェックを入れて、[ドメイン名の登録]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に、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を有効化するには、[DHCP]を有効化する必要があります。

7.1.1 マルチキャスト

マルチキャストは、データ送信先デバイスのグループに同時にアドレス指定されるグループ通信です。マルチキャストを設定すると、ソースデータを複数の宛先へ効率的に送信することが可能です。

[環境設定]→[ネットワーク]→[基本設定]→[マルチキャスト]と移動して、マルチキャストを

設定します。

IPアドレス

マルチキャストホストのアドレスを表します。

ストリームタイプ

マルチキャスト送信元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。

FECポート

選択したストリームのFECポート。

FEC比率

前方誤り訂正の比率。

7.1.2 マルチキャスト検出

[マルチキャスト発見有効]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経由で、クライアントソフトウェアがオンラインのネットワークカメラを自動的に検知することが可能です。

7.2 SNMP

SNMPネットワーク管理プロトコルを設定して、ネットワーク送信時にアラームイベントや異常メッセージを取得することが可能です。

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、SNMPポート経由でデバイス情報を滞りなく受信する必要があります。

ステップ

1. 設定ページへ移動します：**[環境設定]**→**[ネットワーク]**→**[詳細設定]**→**[SNMP]**。

2. **[SNMPv1 有効]**、**[SNMP v2 c 有効]**、**[SNMPv3 有効]**のいずれかにチェックを入れます。

 **注意**

SNMP バージョンは SNMP ソフトウェアのバージョンと同じにする必要があります。尚、必要なセキュリティのレベルに応じて、異なるバージョンの使用が必要になる場合もあります。SNMPv1は安全ではありません。SNMPv2ではアクセスするためのパスワードが必要です。また SNMP v3 は暗号化を提供し、ます。バージョン 3 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 の設定を行います。
4. **[保存]**をクリックします。

7.3 SRTPの設定

セキュアリアルタイム転送プロトコル (SRTP) は、ユニキャストアプリケーションとマルチキャストアプリケーションの双方におけるRTPデータに対し、暗号化、メッセージ認証、整合性、リプレイ攻撃からの保護を提供するための、リアルタイム転送プロトコル (RTP) インターネットプロトコルです。

ステップ

1. **[環境設定]**→**[ネットワーク]**→**[詳細設定]**→**[SRTP]**と移動します。
2. **[サーバ証明書]**を選択 します。
3. **[暗号化アルゴリズム]**を選択 します。
4. **[保存]**をクリックします。

 **注意**

- この機能は一部のデバイスモデルのみでのサポートになります。
 - 機能が異常な場合、証明書の管理にて選択した証明書に異常があるかどうかを確認します。
-

7.4 ポートマッピング

ポートマッピングを設定すると、指定したポートを経由してデバイスにアクセスすることが可能です。

始める前に

デバイスのポートがネットワーク内の他のデバイスのポートと同じ場合は、**ポート** を参照して、デバイスポートを変更します。

ステップ

1. [環境設定]→[ネットワーク]→[基本設定]→[NAT]と移動します。
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 詳細情報については、**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 詳細情報については、**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。

USSECURITY

7.4.1 自動ポートマッピングの設定

ステップ

1. [UPnP™を有効にする]にチェックを入れて、カメラのフレンドリ名を選択してください。デフォルトの名前を使用することも可能です。
2. ポートマッピングモードを[自動]で選択します。
3. [保存]をクリックします。

注意

同時にルーターのUPnP™機能を有効化する必要があります。

7.4.2 手動ポートマッピングの設定

ステップ

1. **[UPnP™を有効にする]**にチェックを入れて、デバイスのフレンドリ名を選択してください。デフォルトの名前を使用することも可能です。
2. ポートマッピングモードを**[手動]**で選択し、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。

次にすべきこと

ルータポートマッピング設定インターフェイスと移動して、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、ルータのユーザーマニュアルを参照してください。

D'SSECURITY

7.4.3 ルータのポートマッピング設定

次の設定は、一部のルータに適用されます。設定はルータのモデルによって異なります。

ステップ

1. [WAN 接続タイプ]を選択します。
2. ルータの[IP アドレス]、[サブネットマスク]などのネットワークパラメータを設定します。
3. [転送]→[仮想サーバ]と移動して、[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に接続されている場合、一方のカメラのポートをIPアドレス 192.168.1.23 上の 80、8000および 554 に設定し、別のカメラのポートをIP192.168.1.24 上の 81、8001、555、8201 に設定できます。

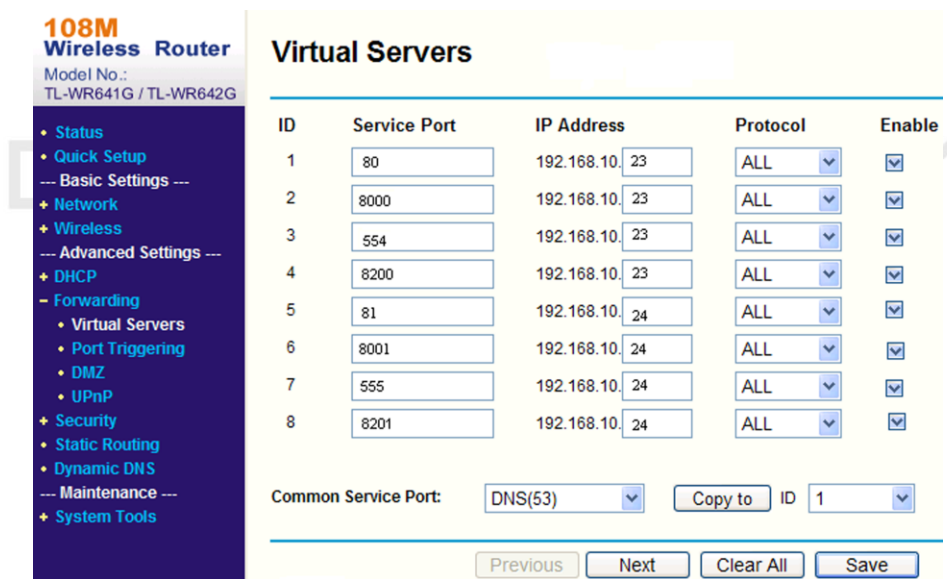


図 7-1 ルータのポートマッピング設定

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いけません。例えば、一部のルータの Web マネジメントサポートは 80 番です。カメラのポートが管理ポートと同じである場合、変更してください。

7.5 ポート

ポートの競合によりデバイスがネットワークにアクセスできない場合、デバイスポートを変更することが可能です。

注意

デフォルトのポートパラメータは勝手に変更しないでください。変更すると、デバイスにアクセスできなくなる恐れがあります。

[環境設定]→[ネットワーク]→[基本設定]→[ポート]と移動して、ポートを設定します。

HTTPポート

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になります。たとえば、**HTTPポート**が81に変更された場合、ブラウザに**http://192.168.1.64:81**と入力してログインする必要があります。

HTTPSポート

ブラウザが証明書を使用してデバイスにアクセスする際に使用するポートになります。セキュアなアクセスを確保するには、証明書認証が必要です。

RTSPポート

リアルタイムストリーミングプロトコルのポートになります。

SRTPポート

セキュアリアルタイム転送プロトコルのポートになります。

サーバーポート

クライアントがデバイスを追加する際に使用するポートになります。

拡張SDKサービスポート

クライアントがデバイスを追加する際に使用するポートになります。セキュアなアクセスを確保するには、証明書認証が必要です。

WebSocketポート

プラグインフリーのプレビュー向けTCPベースの全二重通信プロトコルのポート。

WebSocketsポート

プラグインフリーのプレビュー向けTCPベースの全二重通信プロトコルのポート。セキュアなアクセスを確保するには、証明書認証が必要です。

注意

- 拡張SDKサービスポート、WebSocketポート、WebSocketsポートは、一部のモデルのみでのサポートになります。
 - この機能をサポートするデバイスモデルの場合、**[環境設定]→[ネットワーク]→[詳細設定]→[ネットワークサービス]**と移動して有効化します。
-

7.6 ドメイン名を使用したデバイスへのアクセス

ネットワークアクセスにダイナミックDNS（DDNS）を使用することが可能です。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にマッピングして、ドメイン名経由のネットワークアクセスを実現できます。

始める前に

デバイスのDDNSの設定を適用する前に、DDNSサーバへの登録が必要になります。

ステップ

1. DNS パラメータの設定については、**TCP/IP** を参照してください。
2. DDNS 設定のページへ移動します：**[環境設定]→[ネットワーク]→[基本設定]→[DDNS]**。
3. **[DDNS 有効]**にチェックを入れて、**[DDNS タイプ]**を選択します。

DynDNS

ダイナミックDNSサーバは、ドメイン名解決で使⽤します。

NO-IP

NO-IPサーバは、ドメイン名解決で使⽤します。

4. ドメイン名情報を入力して、**[保存]**をクリックします。
5. デバイスポートを確認してポートマッピングを入力します。デバイスポートを確認するには、**ポート**を参照してください。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。

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

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

7.7 PPPoEダイヤルアップ接続を経由したデバイスへのアクセス

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

ステップ

1. **[環境設定]**→**[ネットワーク]**→**[基本設定]**→**[PPPoE]**と移動します。
2. **[PPPoE 有効]**にチェックを入れます。

3. PPPoE パラメータを設定します。

動的IP

ダイヤルアップに成功すると、WANのダイナミックIPアドレスが表示されます。

ユーザ名

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再度入力します。

4. [保存]をクリックします。

5. デバイスにアクセスします。

ブラウザ経由 ブラウザのアドレスバーにWANのダイナミックIPアドレスを入力して、デバイスにアクセスします。

クライアントソフトウェア経由 WANのダイナミックIPアドレスをクライアントソフトウェアに追加します。詳細についてはクライアントマニュアルを参照してください。

注意

取得したIPアドレスはPPPoE経由で動的にアサインされるものであり、カメラをリブートするたびに変わります。動的IPによる制約を解消するには、DDNS事業者(例: DynDns.com)からドメイン名を取得する必要があります。詳細情報については**ドメイン名を使用したデバイスへのアクセス**を参照してください。

7.8 ワイヤレスダイヤル

音声、ビデオ、画像のデータは、3G/4Gのワイヤレスネットワークを経由して転送することが可能です。

注意

この機能は特定のデバイスでのみサポートされます。

7.8.1 ワイヤレスダイヤルを設定

内蔵ワイヤレスモジュールは、デバイス向けにインターネットへのダイヤルアップアクセスを提供します。

始める前に

SIMカードを入手して、3G/4Gサービスを有効化します。対応するスロットにSIMカードを挿入します。

ステップ

1. [環境設定]→[ネットワーク]→[詳細設定]→[ワイヤレスのダイヤル]と移動します。
2. チェックを入れて、機能を有効化します。
3. [ダイヤルパラメータ]をクリックして、パラメータを設定し保存します。
4. [ダイヤルプラン]をクリックします。詳細については、**監視スケジュールの設定**を参照してください。
5. オプション: [許可リスト]を設定します。詳細については、**許可リストの設定**を参照してください。
6. [ダイヤルステータス]をクリックします。

[更新]をクリック ダイヤルステータスを更新します。

[切断]をクリック 3G/4Gワイヤレスネットワークを切断します。

[ダイヤルステータス]が[接続済み]になると、ダイヤルが成功したことを意味します。

7. ネットワーク内のコンピュータの **IP アドレス** を経由してデバイスにアクセスします。
 - ブラウザにIPアドレスを入力して、デバイスにアクセスします。

- デバイスをクライアントアプリケーションに追加します。**[IP/ドメイン]**を選択して、IPアドレスとその他のパラメータを入力し、デバイスにアクセスします。

7.8.2 許可リストの設定

デバイスからアラームメッセージを受信するには、管理者の携帯電話番号を許可リストに追加します。

ステップ

1. 許可リスト設定のページへ移動します：**[環境設定]**→**[高度な設定]**→**[ワイヤレスダイヤル]**→**[許可リスト]**。
2. **[SMS アラーム有効]**にチェックを入れます。
3. 許可リスト内の**+**をクリックします。
 - 1) アラームメッセージを受信する携帯電話番号を入力します。
 - 2) **[SMSで再起動する]**にチェックを入れます。
 - 3) 特定のイベントを選択すると、イベント発生時に携帯電話でアラームメッセージを受信することが可能になります。
 - 4) **[保存]**をクリックします。
 - 5) オプション: 複数の受信者を設定するには、上記の手順を繰り返します。



許可リストのパラメータを変更します。



すでに設定されている許可リストを削除します。

テストSMSを送信

携帯電話にメッセージを送信してテストします。

4. **[保存]**をクリックします。

7.9 Wi-Fi

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

注意

この機能は特定のデバイスでのみサポートされます。

7.9.1 デバイスをWi-Fiに接続する

始める前に

SSID、キーなどのパラメータの設定については、ワイヤレスルータまたはAPのユーザーマニュアルを参照してください。

ステップ

1. TCP/IP のページへ移動します：**[環境設定]**→**[ネットワーク]**→**[基本設定]**→**[TCP/TCP]**。
2. **[WLAN]**を選択して、パラメータを設定します。設定の詳細については、**TCP/IP** を参照してください。

注意

安定したWi-Fiを利用するために、DHCPの使用はお勧めしません。

3. Wi-Fi 設定ページへ移動します：**[環境設定]**→**[ネットワーク]**→**[詳細設定]**→**[Wi-Fi]**。
4. パラメータを設定して保存します。
 - 1) **[検索]** をクリックします。
 - 2) **[SSID]**を選択します。SSIDは、ワイヤレスルータまたはAP と同じにする必要があります。ネットワークのパラメータは、自動的に**[Wi-Fi]**として表示 されます。
 - 3) **[ネットワークモード]**で**[管理]**を選択します。
 - 4) ワイヤレスネットワークに接続するためのキーを入力します。キーはルータ上でワイヤレスネットワーク接続用にご自身で設定したものです。

次にすべきこと

TCP/IPのページへ移動します：**[環境設定]**→**[ネットワーク]**→**[基本設定]**→**[TCP/IP]**を選択して、**[WLAN]**をクリックし、**[IPv4 アドレス]**にチェックを入れてデバイスにログインします。

7.10 ネットワークサービスの設定

必要に合わせて、特定のプロトコルのオン/オフのステータスを制御することが可能です。

ステップ

注意

この機能はカメラのモデルによって異なります。

1. [環境設定]→[ネットワーク]→[詳細設定]→[ネットワークサービス]と移動します。
2. ネットワークサービスを設定します。

WebSocketとWebSockets

Google Chrome 57 以降のバージョンまたは Mozilla Firefox 52 以降のバージョンを使用してデバイスにアクセスする場合、WebSocketまたはWebSocketsプロトコルを有効化する必要があります。それ以外の場合、ライブビュー、画像キャプチャ、デジタルズームなどは使用できません。

デバイスがHTTPを使用している場合、WebSocketを有効化します。

デバイスがHTTPSを使用している場合、WebSocketsを有効化します。

WebSocketsを使用する場合、**[サーバ証明書]**を選択します。

注意

サーバ証明書を選択する際、予め証明書管理を完了しておく必要があります。詳細情報については、**証明書の管理**を参照してください。

SDKサービスと拡張SDKサービス

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場合、**[SDKサービスを有効化]**にチェックを入れます。

SDK over TLS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場合、**[拡張SDKサービスを有効化]**にチェックを入れます。

拡張SDKサービスを使用する場合、**[サーバ証明書]**を選択します。

注意

- サーバ証明書を選択する際、予め証明書管理を完了しておく必要があります。詳細情報については、**証明書の管理**を参照してください。
 - デバイスとクライアントソフトウェア間の接続を設定する場合、拡張SDKサービスを使用し、通信を監視モードに設定してデータ転送を暗号化することをお勧めします。監視モードの設定については、クライアントソフトウェアのユーザーマニュアルを参照してください。
-

TLS（トランスポート層セキュリティ）

このデバイスはTLS1.1とTLS1.2を提供します。必要に応じて、1つまたは複数のプロトコルバージョンを有効化します。

Bonjour

チェックを外して、プロトコルを無効化します。

3. **[保存]**をクリックします。

7.11 オープンネットワークビデオインターフェイスの設定

Open Network Video Interfaceのプロトコルを使用してデバイスにアクセスする必要がある場合、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可能です。

ステップ

1. **[環境設定]**→**[ネットワーク]**→**[詳細設定]**→**[統合プロトコル]**と移動します。
 2. **[Open Network Video Interface を有効化]**にチェックを入れます。
 3. **[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イス・ユーザーを設定します。
-

- | | |
|-----------|---------------------------------------|
| 削除 | 選択したオープンネットワークビデオインターフェイス・ユーザーを削除します。 |
| 変更 | 選択したオープンネットワークビデオインターフェイス・ユーザーを変更します。 |

4. **[保存]**をクリックします。
5. オプション: さらにオープンネットワークビデオインターフェイス・ユーザーを追加する場合、上記の手順を繰り返します。

7.12 ISUPの設定

デバイスがISUPプラットフォーム（旧称Ehome）に登録されている場合、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、パブリックネットワーク経由でアラーム情報を転送したりすることが可能です。

ステップ

1. **[環境設定]**→**[ネットワーク]**→**[詳細設定]**→**[プラットフォームへのアクセス]**と移動します。
2. プラットフォームアクセスモードで、**[ISUP]**を選択します。
3. **[有効化]**を選択します。
4. プロトコルバージョンを選択して、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、レジスタ状態はオンラインになります。

7.13 アラームサーバの設定

デバイスは、HTTP、HTTPS、またはISUPプロトコルを使用して、送信先のIPまたはホスト名にアラームを送信することが可能です。送信先のIPまたはホスト名は、HTTP、HTTP、またはISUP データ転送をサポートしている必要があります。

ステップ

1. [環境設定]→[ネットワーク]→[詳細設定]→[アラームサーバー]と移動します。
2. [送信先の IP またはホスト名]、[URL]、[ポート]を入力します。
3. [プロトコル]を選択します。



HTTP、HTTPS、ISUPが選択可能です。通信中にデータ転送を暗号化するため、HTTPSを使用することをお勧めします。

4. [テスト]をクリックして、IP またはホストが使用可能かどうかを確認します。
5. [保存]をクリックします。

7.14 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。このアプリを使用して、ライブ画像を表示したり、アラーム通知を受信したりすることが可能です。

始める前に

ネットワークケーブルを使用して、カメラをネットワークに接続します。

ステップ

1. Hik-Connect アプリケーションの入手およびインストール方法は次の通りです。
<https://appstore.hikvision.com> にアクセスして、お使いの携帯電話システムをご確認の上、アプリケーションをダウンロードしてください。当社の公式サイトもご覧ください。次に、[サポート]→[ツール]→[**Hikvision App Store**]と移動します。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ます。



i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、トラブルシューティングの確認方法は次の2通りです。

<https://appstore.hikvision.com/static/help/index.html>にアクセスをして、トラブルシューティングの項目を参照してください。<https://appstore.hikvision.com/>にアクセスし、画面の右上隅にある[Installation Help]をクリックして、トラブルシューティングの項目を参照してください。

2. アプリを起動して、Hik-Connect ユーザーアカウントを登録します。
3. 登録後にログインします。
4. アプリ上で右上隅の「+」をタップして、カメラの QR コードをスキャンしカメラを追加します。QR コードはカメラの上、またはデバイスのパッケージに同梱されているカメラのクイックスタートガイドの表紙にあります。
5. プロンプトにしたがってネットワーク接続を設定し、カメラをあなたの Hik-Connect アカウントに追加してください。

詳細な情報については、Hik-Connect アプリのユーザマニュアルを参照してください。

7.14.1 カメラの Hik-Connect サービス有効化

Hik-Connect サービスは、サービスを使用する前に、お使いのカメラに対して有効化する必要があります。

SADP ソフトウェア、または Web ブラウザ経由でサービスを有効化することができます。

Web ブラウザ経由の Hik-Connect サービス有効化

Webブラウザ経由のHik-Connectサービス有効化の手順は次のとおりです。

始める前に

このサービスを有効化する前に、カメラを有効化する必要があります。

ステップ

1. カメラに Web ブラウザ経由でアクセスします。
2. プラットフォームアクセス設定インターフェイスに入ります。[環境設定]→[ネットワーク]→[詳細設定]→[プラットフォームへのアクセス]
3. [プラットフォームアクセスモード]で Hik-Connect を選択します。
4. [有効化]にチェックを入れます。
5. クリックして、ポップアップ ウィンドウ上で「利用規約」と「プライバシー ポリシー」を確認してください。
6. カメラの認証コードを作成するか、認証コードを変更してください。

注意

認証コードはカメラを Hik-Connect サービスに接続する際に必要になります。

7. 設定を保存します。

SADP ソフトウェア経由の Hik-Connect サービス有効化

このパートでは、アクティブ化されたカメラのSADPソフトウェアを経由してHik-Connectサービスを有効化する方法について説明します。

ステップ

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

 **注意**

認証コードはカメラを Hik-Connect サービスに接続する際に必要になります。

5. クリックして「利用規約」と「プライバシー ポリシー」を確認してください。
6. 設定を確認します。

7.14.2 Hik-Connect の設定

ステップ

1. Hik-Connect アプリケーションの入手およびインストール方法は次の通りです。
<https://appstore.hikvision.com> にアクセスして、お使いの携帯電話システムをご確認の上、アプリケーションをダウンロードしてください。当社の公式サイトもご覧ください。次に、[サポート]→[ツール]→[**Hikvision App Store**]と移動します。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ます。



 **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、トラブルシューティングの確認方法は次の2通りです。

<https://appstore.hikvision.com/static/help/index.html> にアクセスをして、トラブルシューティングの項目を参照してください。<https://appstore.hikvision.com/> にアクセスし、画面の右上隅にある [**Installation Help**] をクリックして、トラブルシューティングの項目を参照してください。

2. アプリを起動して、Hik-Connect ユーザーアカウントを登録します。
3. 登録後にログインします。

7.14.3 Hik-Connectにカメラを追加する

ステップ

1. 携帯端末を Wi-Fi に接続します。
2. Hik-Connect アプリにログインします。
3. ホームページ右上隅の「+」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コードが見つからない、またはコードがぼやけてしまい認識できない場合、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可能です。

5. カメラの認証コードを入力してください。

注意

- 必要になる認証コードとは、カメラでHik-Connectサービスを有効化する際に作成または変更したコードになります。
 - 検証コードを忘れてしまった場合は、Web ブラウザから **[プラットフォームアクセス]** 設定ページを開くことで、現在の認証コードをチェックすることができます。
-

6. ポップアップ表示の**[ネットワークに接続]**をタップします。
7. カメラの機能に合わせて、**[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 携帯電話が接続しているWi-Fiパスワードを入力して、**[次へ]**をタップするとWi-Fiの接続処理が開始します。(Wi-Fiを設定する際には、ルータから3メートル以内の範囲にカメラを置いてください。)

有線接続 ネットワークケーブルを使用してカメラをルーターに接続し、処理結果を知らせるポップアップ表示の**[接続済み]**をタップします。

注意

ルータは、携帯電話が接続しているルータと同じである必要があります。

8. 次のインターフェイスで**[追加]**をタップして、追加を完了します。

詳細な情報については、Hik-Connect アプリのユーザマニュアルを参照してください。

D'SSECURITY

CHAPTER 8 監視スケジュールとアラーム連動

監視スケジュールとは、デバイスが特定のタスクを実行する時間帯で、ユーザー仕様で設定します。アラーム連動は、スケジュールされた時間内に検知された特定のインシデントやターゲットに対する応答です。

8.1 監視スケジュールの設定

デバイスのタスクに対する有効時間を設定します。

ステップ

1. **[監視スケジュール]**をクリックします。
2. タイムバーをドラッグして、任意の有効時間を指定します。

注意

1日最大8件の時間帯を設定することが可能です。

3. 時間帯を調整します。
 - 選択した時間帯をクリックし、任意の値を入力します。 **[保存]**をクリックします。
 - 選択した時間帯をクリックします。両端をドラッグして、時間帯を調整します。
 - 選択した時間帯をクリックして、タイムバーにドラッグします。
4. オプション: **[...にコピーする]**をクリックして、同じ設定を他の日にコピーします。
5. **[保存]**をクリックします。

8.2 リンク方式の設定

イベント発生時のリンク機能を有効化することが可能です。

8.2.1 トリガアラームアウトプット

デバイスがアラーム出力デバイスに接続され、アラーム出力No.が設定されている場合、アラームが作動すると、接続されているアラーム出力デバイスにアラーム情報が送信されます。

ステップ

1. [環境設定]→[イベント]→[基本イベント]→[アラーム出力]と移動します。
2. アラーム出力パラメータを設定します。

自動アラーム 環境設定の詳細については、**自動アラーム**を参照してください。

手動アラーム 環境設定の詳細については、**手動アラーム**を参照してください。

3. [保存]をクリックします。

手動アラーム

アラーム出力は手動で作動させることが可能です。

ステップ

1. 手動アラームのパラメータを設定します。

アラーム出力番号

外部アラームデバイスに接続されているアラームインターフェイスに応じて、アラーム出力No.を選択します。

アラーム名

アラーム出力の名前を設定します (オプション)。

遅延

[手動]を選択します。

2. [手動アラーム]をクリックして、手動アラームを有効化します。
3. オプション: [アラームのクリア]をクリックして、手動アラームを無効化します。

自動アラーム

自動アラームのパラメータを設定すると、設定した監視スケジュールで自動的にアラーム

出力が作動します。

ステップ

1. 自動アラームのパラメータを設定します。

アラーム出力番号

外部アラームデバイスに接続されているアラームインターフェイスに応じて、アラーム出力No.を選択します。

アラーム名

アラーム出力の名前を設定します (オプション)。

遅延

アラーム発生後、アラーム出力が継続する時間を指します。

2. 監視スケジュールを設定します。設定の詳細については、**監視スケジュールの設定**を参照してください。
3. **[...にコピーする]**をクリックし、パラメータを他のアラーム出力チャンネルにコピーします。
4. **[保存]**をクリックします。

8.2.2 FTP/NAS/メモリカードのアップロード

FTP/NAS/メモリカードのアップロードを有効化および設定している場合、アラームが作動すると、デバイスはアラーム情報を FTPサーバ、ネットワーク接続ストレージ、メモリカードに送信します。

FTPサーバの設定については、**FTP設定**を参照してください。

NASの設定については、**NAS設定**を参照してください。

メモリカードのストレージ設定については、**新規または暗号化されていないメモリカードの設定**を参照してください。

8.2.3 Eメール送信

[Eメールの送付]にチェックを入れると、アラームイベントを検知したときに、デバイスは指定されたアドレスにメールでアラーム情報を送信します。

Eメールの設定については、**Eメールの設定**を参照してください。

Eメールの設定

Eメールが設定されていて、かつリンク方式として**[Eメールの送付]**が有効化になっている場合、デバイスはアラームイベントを検知すると、指定されたすべての宛先に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際、予めDNSサーバを設定する必要があります。**[環境設定]**→**[ネットワーク]**→**[基本設定]**→**[TCP/IP]**と移動して、DNSを設定します。

ステップ

1. Eメール設定のページへ移動します：**[環境設定]**→**[ネットワーク]**→**[詳細設定]**→**[Eメール]**。
2. Eメールパラメータを設定します。
 - 1) 送信者の差出人アドレス、SMTPサーバ、SMTPポートなど、送信者のEメール情報を入力します。
 - 2) オプション: Eメールサーバで認証が必要な場合、**[認証]**にチェックを入れて、ユーザー名とパスワードを入力しサーバにログインします。
 - 3) **[メールの暗号化]**を設定します。
 - SSLまたはTLSを選択し、STARTTLSを無効化した場合、EメールはSSLまたは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。
 - SSLまたはTLSを選択し、STARTTLSを有効化した場合、E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、Eメールサーバがプロトコルをサポートしていることを確認してください。**[STARTTLSの有効化]**にチェックを入れても、Eメールサーバがプロトコルをサポートしていない場合、Eメールは暗号化されずに送信されます。

- 4) オプション: アラーム画像の通知を受信する場合、**[画像の添付]**にチェックを入れます。通知メールには、イベントにおいて、予め設定した間隔でキャプチャされたアラーム画像が3つ添付されています。
- 5) 宛先の名前やアドレスなど、宛先の情報を入力します。
- 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ます。

3. **[保存]**をクリックします。

8.2.4 監視センターに通知する

[監視センターに通知する]にチェックを入れると、アラームイベントが検知されたときに、アラーム情報が監視センターにアップロードされます。

8.2.5 録画をトリガー

[録画をトリガー]にチェックを入れると、デバイスは検知したアラームイベントの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。

8.2.6 ライト点滅

[ライト点滅]を有効化し、**[点滅アラーム光出力]**を設定すると、イベントが検知されたときにライトが点滅します。

点滅アラーム光出力の設定

イベント発生時、アラームとしてデバイスのライトを点滅させることが可能です。

ステップ

1. **[環境設定]**→**[イベント]**→**[基本イベント]**→**[点滅アラーム光出力]**と移動します。
2. **[点滅時間]**、**[点滅頻度]**、**[輝度]**を設定します。

点滅時間

1回のアラーム発生時に点滅が継続する時間。

点滅頻度

ライトの点滅速度。高頻度、中頻度、低頻度、通常点灯で選択することができます。

輝度

ライトの輝度。

3. 監視スケジュールを設定します。詳細については**監視スケジュールの設定**を参照してください。

4. **[保存]**をクリックします。

 **注意**

この機能は一部のデバイスモデルのみでのサポートになります。

8.2.7 音声警報

[音声警報]を有効化して**[音声アラーム出力]**を設定すると、アラームの発生時、デバイス内蔵スピーカーまたは接続されている外部スピーカーから警告音が鳴ります。

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。

 **注意**

この機能は特定のデバイスでのみサポートされます。

音声アラーム出力の設定

デバイスが検知エリアでターゲットを検知すると、警告として音声アラームが作動します。

ステップ

1. **[環境設定]**→**[イベント]**→**[基本イベント]**→**[音声アラーム出力]**と移動します。
2. **[音声種別]**を選択し、関連するパラメータを設定します。
 - **[Prompt]**を選択し、必要なアラーム回数を設定します。
 - **[警告]**とその内容を選択します。必要なアラーム回数を設定します。
 - **[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することが可能です。使用可能なファイルがない場合、**[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することが可能です。
最大3つまでのオーディオファイルをアップロードすることが可能です。
3. オプション:**[テスト]**をクリックして、デバイス上の選択した音声ファイルを再生します。
4. 音声アラームの監視スケジュールを設定します。詳細については**監視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。

 **注意**

この機能は特定のデバイスでのみサポートされます。

D'SSECURITY

CHAPTER 9 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について説明します。

9.1 デバイス情報を表示

デバイスNo.、モデル、シリアルNo.、ファームウェアバージョンなどのデバイス情報を表示することが可能です。

デバイス情報を表示するには、**[環境設定]**→**[システム]**→**[システム設定]**→**[基本的な情報]**と移動します。

9.2 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. **[環境設定]**→**[システム]**→**[メンテナンス]**→**[ログ]**と移動します。
2. 検索条件として**[メインリスト]**、**[サブリスト]**、**[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。
一致したログファイルがログリストに表示されます。
4. オプション:**[エクスポート]**をクリックし、お使いのコンピュータにログファイルを保存します。

9.3 同時ログイン

管理者は、Webブラウザからシステムに同時にログインできる最大ユーザー数を設定することが可能です。

[環境設定]→[システム]→[ユーザー管理]と移動して、[一般]をクリックし、[同時ログイン]を設定します。

9.4 設定ファイルのインポートとエクスポート

これにより、同じパラメータを持つ他のデバイスのバッチ設定を高速化できます。

[環境設定]→[システム]→[メンテナンス]→[アップグレードとメンテナンス]と移動します。インポートまたはエクスポートする必要があるデバイスパラメータを選択して、インターフェイスのインストラクションに従って設定ファイルをインポートまたはエクスポートします。

9.5 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。

[環境設定]→[システム]→[メンテナンス]→[アップグレードとメンテナンス]と移動します。必要な診断情報にチェックを入れて、[診断情報]をクリックし、デバイスに関する該当の診断情報をエクスポートします。

9.6 再起動

ブラウザを使用してデバイスを再起動することが可能です。

[環境設定]→[システム]→[メンテナンス]→[アップグレードとメンテナンス]と移動し、[再起動]をクリックします。

9.7 復元とデフォルト

[復元]や[デフォルト]により、デバイスパラメータをデフォルト設定に戻すことができるようになります。

ステップ

1. [環境設定]→[システム]→[メンテナンス]→[アップグレードとメンテナンス]と移動します。

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。

復元する 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（ユーザー情報、IPパラメータ、ビデオフォーマットを除く）。

デフォルト すべてのパラメータを工場出荷時のデフォルトにリセットします。

 **注意**

十分に注意の上、この機能を使用してください。工場出荷時のデフォルトにリセットすると、すべてのパラメータがデフォルト設定にリセットされます。

9.8 アップグレード

始める前に

適切なアップグレードパッケージを入手する必要があります。

 **注意**

処理中に電源を切らないでください。アップグレード後、デバイスは自動的に再起動します。

ステップ

1. **[環境設定]**→**[システム]**→**[メンテナンス]**→**[アップグレードとメンテナンス]**と移動します。

2. アップグレード方法を 1 つ選択します。

ファームウェア アップグレードファイルの正確なパスを指定します。

ファームウェアディレクトリ アップグレードファイルが置かれたディレクトリを特定します。

3. **[参照]**をクリックして、アップグレードファイルを検索します。

4. **[アップグレード]**をクリックします。

9.9 オープンソースのソフトウェアライセンスを表示する

[環境設定]→[システム]→[システム設定]→[バージョン情報]と移動して、[ライセンスを表示する]をクリック します。

9.10 ウィーガンド

注意

この機能は一部のモデルのカメラでのみサポートされます。

[有効化]にチェックを入れて、プロトコルを設定します。デフォルトのプロトコルはSHA-1（26ビット）です。

有効化すると、選択したWiegandプロトコルを経由して、認識されたナンバープレート番号が出力されます。

D'SSECURITY

9.11 メタデータ

メタデータとは、アルゴリズム処理の前にカメラが収集する生データです。これにより、ユーザーはさまざまなデータの使用状況を調べることもできます。

[環境設定]→[システム]→[メタデータ設定]と移動して、任意の機能でメタデータのアップロードを有効化します。

スマートイベント

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

9.12 時間と日付

デバイスの時間と日付を設定するには、タイムゾーン、時間同期、サマータイム（夏時間）を設定します。

9.12.1 手動による時間同期

ステップ

1. **[環境設定]→[システム]→[システム設定]→[時間設定]**と移動します。
2. **[タイムゾーン]**を選択します。
3. **[手動時間同期]**をクリックします。
4. ワンタイム同期の方法を選択します。
 - **[時間セット]**を選択して、ポップアップカレンダーから日付と時間を手動で入力または選択します。
 - **[コンピュータの時間と同期します]**にチェックを入れて、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。

9.12.2 NTPサーバの設定

正確で信頼性の高い時刻ソースが必要な場合、NTPサーバを使用することが可能です。

始める前に

NTPサーバを設定、またはNTPサーバ情報を取得します。

ステップ

1. [環境設定]→[システム]→[システム設定]→[時間設定]と移動します。
2. [タイムゾーン]を選択します。
3. [NTP]をクリックします。
4. [サーバアドレス]、[NTPポート]、[間隔]を設定します。

注意

サーバアドレスはNTPサーバのIPアドレスです。

5. [テスト]をクリックして、サーバ接続をテストします。
6. [保存]をクリックします。

9.12.3 衛星による時間同期

注意

この機能はデバイスのモデルによって異なります。

ステップ

1. [環境設定]→[システム]→[システム設定]→[時間設定]と移動します。
2. [衛星時間同期]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。

9.12.4 DST設定

デバイスを設置する地域でサマータイム（夏時間）が採用されている場合、この機能を設定することが可能です。

ステップ

1. [環境設定]→[システム]→[システム設定]→[サマータイム]と移動します。
2. [サマータイム有効]にチェックを入れます。
3. [開始時間]、[終了時間]、[DST バイアス]を選択します。
4. [保存]をクリックします。

9.13 RS-485の設定

RS-485は、デバイスを外部機器に接続するために使用します。通信距離が長すぎる場合、RS-485を使用してデバイスとコンピュータまたは端末との間でデータを送信することが可能です。

始める前に

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

ステップ

5. [環境設定]→[システム]→[システム設定]→[RS-485]と移動します。
6. RS-485 パラメータを設定します。

注意

デバイス、コンピュータ、端末のパラメータはすべて同じにする必要があります。

7. [保存]をクリックします。

9.14 RS-232の設定

RS-232は、デバイスのデバッグや周辺機器へのアクセスに使用することが可能です。また、通信距離が短い場合、デバイスとコンピュータまたは端末との間の通信が可能になります。

始める前に

RS-232ケーブルを使用して、デバイスとコンピュータまたは端末を接続します。

ステップ

1. [環境設定]→[システム]→[システム設定]→[RS-232]と移動します。
2. RS-232 パラメータは、デバイスとコンピュータまたは端末が一致するように設定します。
3. [保存]をクリックします。

9.15 消費電力モード

デバイスの動作中に消費電力を切り替えるために使用します。

注意

この機能は特定のデバイスでのみサポートされます。

[環境設定]→[システム]→[システム設定]→[Power Consumption Mode]と移動して、任意の消費電力モードを選択します。

高消費モード

すべての機能が有効になっている状態でデバイスが動作します。

低消費リアルタイムモード

デバイスのDSPは通常に動作します。メインストリームのビデオをハーフフレームレートで録画し、リモートログイン、プレビュー、環境設定をサポートします。

低電力スリープ

デバイスの電力が[Threshold of Low Power Sleep Mode]を下回る場合、デバイスはスリープモードに入ります。

デバイスの電力がしきい値を10%上回るまで回復すると、デバイスはユーザー設定モードに入ります。

スリープ予約

スリープ予約の時間中、デバイスはスリープモードに入ります。それ以外の時間帯は、ユーザー設定モードに入ります。

注意

スリープ予約の設定については、**監視スケジュールとアラーム連動**を参照してください。デバイスは目覚まし機能をサポートしています。詳細については、**タイミングウェイクの設定**を参照してください。

9.16 外部機器

補助光、ハウジングのワイパー、LEDライトなどの外部機器をサポートするデバイスは、ハウジングで使用する際にこれらをWebブラウザ経由で制御することが可能です。外部機器はモデルによって異なります。

輝度

実際のシーンに合わせて、**[ロービームの明るさ]**と**[ハイビームの明るさ]**を調整します。

タイミング

補助光（LED）は設定したスケジュールでオンになります。**[開始時間]**と**[終了時間]**を指定する必要があります。

自動

補助光は周囲の光量に応じてオンになります。

9.16.1 補助光の設定

補助光を設定すると、関連するパラメータを利用のデバイスで確認することが可能です。

スマート補助光

スマート補助光は、補助光点灯時の過剰暴露を防止します。

補助光モード

デバイスが補助光をサポートしている場合、補助光モードを選択することが可能です。

赤外線モード

赤外線光が有効になります。

白色ライトモード

白色ライトが有効になります。

ミックスモード

赤外線光と白色ライトの両方が有効になります。

オフ

補助光が無効になります。

輝度調整モード

自動

輝度は、実際の環境に応じて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、値を設定して輝度を調整することが可能です。

9.16.2 ヒーター

ヒーターを有効化して、デバイスのレンズ周囲の霧を取り除くことが可能です。

[環境設定]→[システム]→[システム設定]→[外部機器]と移動して、必要なモードを選択します。

9.17 セキュリティ

システムのセキュリティを向上させるには、セキュリティパラメータを設定します。

9.17.1 認証

ネットワークアクセスのセキュリティを向上させるには、RTSPやWeb認証を設定します。**[環境設定]→[システム]→[セキュリティ]→[認証]**と移動して、必要に応じて認証プロトコルと認証方法を選択します。

RTSP認証

ダイジェストとダイジェスト/基本がサポートされているので、RTSP要求がデバイスに送信されると、認証情報が必要になります。**[ダイジェスト/基本]**を選択すると、デバイスはダイジェスト認証または基本認証をサポートします。**[ダイジェスト]**を選択すると、デバイスはダイジェスト認証のみをサポートします。

RTSPダイジェストアルゴリズム

RTSP認証におけるMD5、SHA256、MD5/SHA256の暗号化アルゴリズム。MD5以外のダイジェストアルゴリズムを有効化すると、互換性により、サードパーティのプラットフォームがデバイスにログインできなくなったり、ライブビューを有効化できなくなるおそれがあります。高強度の暗号化アルゴリズムを使用することをお勧めします。

WEB認証

ダイジェストとダイジェスト/基本がサポートされているので、WEB要求がデバイスに送信されると、認証情報が必要になります。**[ダイジェスト/基本]**を選択すると、デバイスはダイジェスト認証または基本認証をサポートします。**[ダイジェスト]**を選択すると、デバイスはダイジェスト認証のみをサポートします。

WEBダイジェストアルゴリズム

WEB認証におけるMD5、SHA256、MD5/SHA256の暗号化アルゴリズム。MD5以外のダイジェストアルゴリズムを有効化すると、互換性により、サードパーティのプラットフォームがデバイスにログインできなくなったり、ライブビューを有効化できなくなるおそれがあります。高強度の暗号化アルゴリズムを使用することをお勧めします。

注意

認証要件を表示するには、プロトコル固有の内容を参照してください。

9.17.2 IPアドレスフィルタの設定

IPアドレスフィルタは、アクセス制御用のツールです。IPアドレスフィルタを有効化して、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可能です。

IPアドレスはIPv4になります。

ステップ

1. [環境設定]→[システム]→[セキュリティ]→[IP アドレスフィルタ]と移動します。
2. [IP アドレスフィルタを有効化]にチェックを入れます。
3. IP アドレスフィルタのタイプを選択します。

禁止 リストのIPアドレスは、デバイスにアクセスできません。

許可 リストのIPアドレスのみが、デバイスにアクセスできます。

4. IP アドレスフィルタリストを編集します。

追加 新たにIPアドレスやIPアドレス範囲をリストに追加します。

変更 リストで選択したIPアドレスやIPアドレス範囲を変更します。

削除 リストで選択したIPアドレスやIPアドレス範囲を削除します。

5. [保存]をクリックします。

9.17.3 HTTPSの設定

HTTPSは、暗号化された送信とID認証を有効化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。

ステップ

1. [環境設定]→[ネットワーク]→[詳細設定]→[HTTPS]と移動します。
2. [有効化]にチェックを入れると、HTTP または HTTPS プロトコル経由でカメラにアクセスできます。
3. [HTTPS ブラウジングを有効化]にチェックを入れると、HTTPS プロトコル経由でのみカメラにアクセスできます。
4. [サーバ証明書]を選択 します。
5. [保存]をクリックします。

注意

機能が異常な場合、[証明書の管理]で選択した証明書に異常があるかどうかを確認します。

9.17.4 QoSの設定

QoS(サービス品質)により、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輻輳を改善することが可能になります。

注意

QoSは、ルータやスイッチなどのネットワークデバイスによりサポートされている必要があります。

ステップ

1. [環境設定]→[ネットワーク]→[詳細設定]→[QoS]と移動します。
2. [ビデオ/音声 DSCP]、[アラーム DSCP]、[管理 DSCP]を設定します。

 **注意**

ネットワークは、データ転送の優先度を識別することが可能です。DSCPの値が大きいほど優先度は高くなります。環境設定の際に同じ値をルータに設定する必要があります。

3. **[保存]**をクリックします。

9.17.5 IEEE 802.1xの設定

IEEE 802.1x は、ポート単位でネットワークアクセスを制御します。これにより、LAN/WLANのセキュリティレベルが向上します。デバイスがIEEE 802.1x 標準のネットワークに接続する際には、認証が必要になります。

[環境設定]→[ネットワーク]→[詳細設定]→[802.1x]と移動して、機能を有効化します。

ルータ情報に従って、**[プロトコル]**と**[EAPOLバージョン]**を設定します。

プロトコル

EAP-LEAP、EAP-TLS、EAP-MD5が選択可能です。

EAP-LEAPとEAP-MD5

EAP-LEAPまたはEAP-MD5を使用する場合、認証サーバを設定する必要があります。

802.1xのユーザー名とパスワードを予めサーバに登録します。認証ユーザー名とパスワードを入力します。

EAP-TLS

EAP-TLSを使用している場合、IDとプライベートキーパスワードを入力して、CA証明書、ユーザー証明書、秘密鍵をアップロードします。

EAPOLバージョン

EAPOL バージョンは、ルータまたはスイッチと同一にする必要があります。

9.17.6 コントロールタイムアウト設定

この機能が有効になっている場合、設定されたタイムアウト時間内にWeb ブラウザ経由でデバイスの操作が行われないと（ライブ画像の表示中を除く）、ログアウトされます。

[環境設定]→[システム]→[セキュリティ]→[アドバンスドセキュリティ]と移動して、設定を完了します。

9.17.7 セキュリティ監査ログの検索

デバイスのセキュリティログファイルを検索および分析することで、不正侵入を検出し、セキュリティイベントのトラブルシューティングを行うことが可能になります。

ステップ

注意

この機能は一部のモデルのカメラでのみサポートされます。

1. **[環境設定]**→**[システム]**→**[メンテナンス]**→**[セキュリティ監査ログ]**と移動します。
2. ログタイプ、**[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。
検査条件に一致するログファイルがログリストに表示されます。
4. オプション:**[エクスポート]**をクリックし、お使いのコンピュータにログファイルを保存します。

9.17.8 セキュリティ強化

セキュリティ強化は、ネットワークセキュリティを強化するソリューションです。この機能を有効化すると、リスクの高い機能、プロトコル、デバイスのポートが無効になり、より安全な代替の機能、プロトコル、ポートが有効になります。

[環境設定]→**[システム]**→**[セキュリティ]**→**[アドバンスドセキュリティ]**と移動します。**[セキュリティ強化]**にチェックを入れて、**[保存]**をクリックします。

9.17.9 SSH

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

SSH機能のデフォルトは無効になっています。

注意

十分に注意の上、この機能を使用してください。この機能を有効化すると、デバイス内部の情報漏洩のセキュリティリスクが発生します。

9.18 証明書の管理

サーバ/クライアント証明書とCA証明書を管理して、証明書が有効期限に近い場合、または期限切れ/異常な場合にアラームを送信することができます。

9.18.1 自己署名証明書の作成

ステップ

1. [自己署名証明書の作成]をクリックします。
2. プロンプトに従って、[証明書 ID]、[国]、[ホスト名/IP]、[妥当性]などのパラメータを入力します。

注意

証明書IDは、64文字以内の数字または文字とします。

3. [OK]をクリックします。
4. オプション: 証明書をエクスポートする場合は、[エクスポート]をクリックします。証明書を再作成するため証明書を削除する場合は、[削除]をクリックします。証明書の詳細を表示する場合は、[証明書のプロパティ]をクリックします。

9.18.2 証明書要求の作成

始める前に

自己署名証明書を選択します。

ステップ

1. [証明書要求の作成]をクリックします。
2. 関連情報を入力します。
3. [OK]をクリックします。

9.18.3 証明書のインポート

ステップ

1. **[インポート]**をクリックします。
2. **[証明書要求の作成]**をクリックします。
3. **[証明書 ID]**を入力します。
4. **[ブラウザ]**をクリックして、任意のサーバ/クライアント証明書を選択します。
5. 任意のインポート方法を選択し、必要な情報を入力します。
6. **[OK]**をクリックします。
7. オプション: 証明書をエクスポートする場合は、**[エクスポート]**をクリックします。証明書を再作成するため証明書を削除する場合は、**[削除]**をクリックします。証明書の詳細を表示する場合は、**[証明書のプロパティ]**をクリックします。

注意

- 証明書は16通まで可能です。
 - 特定の機能が証明書を使用している場合、証明書は削除できません。
 - 証明書を使用している機能は、**[機能]**の欄に表示されます。
 - 既存の証明書と同じIDの証明書を作成し、既存の証明書と同じ内容の証明書をインポートすることはできません。
-

9.18.4 サーバ/クライアント証明書のインストール

ステップ

1. **[環境設定]**→**[システム]**→**[セキュリティ]**→**[証明書の管理]**と移動します。
2. **[自己署名証明書の作成]**、**[証明書要求の作成]**、**[インポート]**をクリックして、サーバ/クライアント証明書をインストールします。

自己署名証明書の作成 **自己署名証明書の作成**を参照してください。

証明書要求の作成 **証明書要求の作成**を参照してください。

証明書のインポート **証明書のインポート**を参照してください。

9.18.5 CA証明書のインストール

ステップ

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。
3. **[ブラウザ]**をクリックして、任意のサーバ/クライアント証明書を選択します。
4. 任意のインポート方法を選択し、必要な情報を入力します。
5. **[OK]**をクリックします。

注意

証明書は16通まで可能です。

9.18.6 証明書有効期限切れアラームを有効化

ステップ

1. **[証明書有効期限切れアラームを有効にする]**をクリックします。有効化すると、証明書がまもなく期限切れ、既に期限切れ、または異常であることを知らせる Eメールまたは監視センターのカメラリンクを受信します。
2. **[有効期限切れの前に通知する (日数)]**、**[アラームの頻度 (日数)]**、**[検出時間 (時間)]**を設定します。

注意

- 有効期限前の通知日を「1」に設定すると、カメラは有効期限の前日に通知します。1～30日で設定できます。デフォルトの通知日は7日です。
 - 有効期限前の通知日を「1」に設定して、検出時間を10：00に設定して、さらに証明書の有効期限は翌日の9：00に切れる場合、カメラは初回通知日（期限前日）の10：00に通知することになります。
-

3. **[保存]**をクリックします。

9.19 ユーザーとアカウント

9.19.1 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、異なるユーザーレベルに異なる権限を付与したりすることが可能です。

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に、アカウントのパスワードを定期的に変更してください。パスワードは3か月ごとに変更することをお勧めします。リスクの高い環境でデバイスを使用する場合、月ごとや週ごとにパスワードを変更することをお勧めします。

ステップ

1. [環境設定]→[システム]→[ユーザー管理]→[ユーザー管理]と移動します。
2. [追加]をクリックします。[ユーザー名]を入力し、[レベル]を選択して、[パスワード]を入力します。必要に応じてリモート許可をユーザーに割り当てます。

管理者

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

ユーザ

ユーザーには、ライブビデオの表示、PTZパラメータの設定、自身のパスワードの変更の権限を割り当てることが可能ですが、他の操作の権限を割り当てることはできません。

オペレータ

オペレーターには、管理者の操作とアカウントの作成以外のすべての権限を割り当てることが可能です。

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

削除 ユーザーを選択して、**[削除]**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することが可能です。

3. **[OK]**をクリックします。

9.19.2 同時ログイン

管理者は、Webブラウザからシステムに同時にログインできる最大ユーザー数を設定することが可能です。

[環境設定]→**[システム]**→**[ユーザー管理]**と移動して、**[一般]**をクリックし、**[同時ログイン]**を設定します。

9.19.3 オンラインユーザ

デバイスにログインしているユーザーの情報が表示されます。

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

CHAPTER 10 VCAリソースの割り当て

リソース割り当てにより、実際のニーズに合わせて特定のVCA機能を有効化することができます。これにより、必要な機能により多くのリソースを割り当てることができます。

ステップ

1. [環境設定]→[システム]→[システム設定]→[リソース割り当て]と移動します。
2. 任意のVCA機能を選択します。
3. 設定を保存します。

注意

一部のVCA機能は相互に排他的です。特定の機能や複数の機能を選択して保存すると、他の機能は非表示になりません。

10.1 スマートモードの切り替え

Smart機能を有効化して、必要に応じて検知目標を選択することが可能です。

ステップ

1. [環境設定]→[システム]→[システム設定]→[Smart Mode Switch]と移動します。
2. 任意のSmart Modeを選択します。

表 10-1 スマートモードのスマート機能

スマートモード	検知ターゲット	スマート機能
---------	---------	--------

キャプチャーモード

デバイスは検知エリアでターゲットをキャプチャーし、キャプチャーされた画像をアップロードします。必要に応じて、キャプチャーするターゲットを選択することが可能です。

	顔	顔キャプチャ
	自動車	道路交通量
	その他の組み合わせ	マルチターゲットタイプ検知

比較モード

デバイスは、ルール領域内のターゲットを識別、キャプチャー、比較して、ターゲットの属性とモデルを収集します。

	顔	顔キャプチャ 顔比較とモデリング
	顔+人体	マルチターゲットタイプ検知 顔比較とモデリング

パターンモード

デバイスは、キャプチャーされた顔、人体、車両情報を別のチャンネルからリンクさせて、ターゲットのパターンを表示します。

	チャンネル1：顔 チャンネル2：顔+人体 +車両+非車両	パターンリンク 顔キャプチャ マルチターゲットタイプ検知 顔比較とモデリング
	チャンネル1：顔+人体 チャンネル2：顔+人体 +車両+非車両	パターンリンク マルチターゲットタイプ検知 顔比較とモデリング
監視中	-	

3. **[保存]**をクリックします。

i注意

- 比較モードでは、チャンネル2だけがモニタリングモードをサポートします。
 - Pattern Modeは、2チャンネルデバイスでのみサポートされます。人体検知をサポートしているのはチャンネル1のみです。
-

10.2 顔キャプチャ

デバイスは、設定されたエリアに表示される顔をキャプチャできるので、顔情報もキャプチャ画像と一緒にアップロードされます。

i注意

- 顔キャプチャをサポートするデバイスでは、**[リソース割り当て]**で機能を有効化する必要があります。詳細については、**VCAリソースの割り当て**を参照してください。
 - 顔キャプチャは特定のモデルでのみサポートされます。
-

10.2.1 顔キャプチャの設定

設定されたエリアに表示される顔をキャプチャすることが可能です。

始める前に

この機能を有効化するには、**[リソース割り当て]**と移動して、**[顔キャプチャ]**を選択します。

ステップ

1. **[環境設定]**→**[顔キャプチャ]**と移動します。
 2. シールド区域の設定については、**シールド区域の設定**を参照してください。
 3. **[ルール]**を選択して、**[ルール]**にチェックを入れます。
 4. をクリックして、検知エリアを指定します。指定エリアは、ライブビュー画像の1/2~2/3を占めることをお勧めします。
 5. をクリックして、ライブビュー上の顔の瞳孔間距離に基づいて長方形を指定します。
-



図 10-1 顔キャプチャの設定

デバイスは、設定された最小瞳孔間距離によって、そのエリアに人の顔があるかどうかを検知します。

6. 監視スケジュールの設定については、**監視スケジュールの設定**を参照してください。リンク方式の設定については、**リンク方式の設定**を参照してください。
7. **[保存]**をクリックします。
8. オーバーレイとキャプチャーの設定については、**オーバーレイとキャプチャー**を参照してください。アドバンスド パラメータの設定については、**顔カウントのアルゴリズムパラメータ**を参照してください。

結果

[画像]では、キャプチャされた顔画像を表示およびダウンロードすることが可能です。詳細については、**画像の表示とダウンロード**を参照してください。

10.2.2 オーバーレイとキャプチャー

キャプチャパラメータと、ストリームやピクチャに表示する情報の設定を選択します。

VCA情報をオリジナル画像で表示します

ターゲットやルール情報など、ストリームのSmart情報を表示します。

キャプチャ画像の上に目標情報を表示する

アラーム画像とターゲット情報を重ね合わせます。

ターゲット画像の設定

カスタマイズ、ヘッドショット、半身ショット、全身ショットが選択可能です。

注意

[カスタマイズ]を選択した場合、必要に応じて**[幅]**、**[頭の高さ]**、**[胴体の高さ]**をカスタマイズすることが可能です。

[固定値]にチェックを入れると、画像の高さを設定することが可能です。

背景画像の設定

ターゲット画像と比較すると、背景画像は、Environment Infoを提供するシーン画像となります。背景画像の品質と解像度を設定することが可能です。背景画像を監視センターにアップロードする必要がある場合、**[バックグラウンドアップロード]**にチェックを入れます。

人数カウントをオーバーレイする

フローオーバーレイのタイプを選択します。

毎日のリセット時刻を選択します。今すぐリセットする場合、**[手動リセット]**をクリックします。

カメラ

カメラのデバイスNo.とカメラ情報を設定して、キャプチャ画像にオーバーレイ表示することが可能です。

テキストオーバーレイ

任意のアイテムにチェックを入れて、  でキャプチャーした画像に表示する順番を調整することが可能です。

デバイスNo.とカメラ情報の内容は同じページにある必要があります。

10.2.3 顔キャプチャアルゴリズムのパラメータ

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

[環境設定]→[顔キャプチャ]→[高度な設定]→[パラメータ]と移動します。

顔キャプチャバージョン

アルゴリズムライブラリのバージョンです。

パラメータ検知

生成速度

対象を識別する速度です。値が高いほど対象は素早く認識されます。値を非常に小さくした場合、設定された領域に最初から顔が存在する場合、その顔はキャプチャされません。しかし、壁の模様やポスターなどの顔を誤って認識することは少なくなります。デフォルトの値である 3 が推奨値です。

感度

対象を識別する感度です。値が大きいほど顔を検知しやすくなりますが、誤認識が起こる可能性も高くなります。デフォルトの値である 3 が推奨値です。

キャプチャパラメータ

ベストショット

ターゲットが検知エリアから離れた後のベストショット。

キャプチャー回数

設定されたエリア内に留まっている間に顔がキャプチャーされるキャプチャ回数を示します。デフォルト値は「1」です。

キャプチャー間隔

顔をキャプチャする際のフレーム間隔です。デフォルト値である 1 を設定するとカメラは毎フレーム、顔をキャプチャします。

キャプチャしきい値

キャプチャーとアラームのトリガーとなる顔の品質を表します。値が大きくなると、キャプチャーとアラームのトリガーとなる品質は高くなります。

クイックショット

クイックショットのしきい値と最大キャプチャ間隔を定義することが可能です。

クイックショットのしきい値

クイックショットのトリガーとなる顔の品質を表します。

顔露光

チェックボックスをチェックして [顔露出] を有効化します。

参考明度

顔露出モードにおける顔の基準輝度を示します。顔が検出された場合、カメラは設定された値にもとづいて顔の明るさを調整します。値が大きいほど顔は明るくなります。

最小時間

カメラが顔を露出する最小時間です。デフォルトの値は 1 分です。

注意

顔露出が有効になっている場合には、WDR 機能が無効になっており、かつ手動絞りが選択されていることを確認してください。

顔認証フィルタリング時間

カメラが顔を検知してからキャプチャーのアクションを実行するまでの時間間隔を指します。検知された顔がシーン内に留まっている時間が、設定されたフィルタリング時間よりも短い場合、キャプチャーは作動しません。たとえば、顔のフィルタリング時間が5秒に設定されている場合、顔が5秒間シーンに留まっているときに、カメラは検知した顔をキャプチャーします。

注意

顔認証フィルタリング時間 (0秒より長い) により、上記の設定値よりも実際のキャプチャー時間が短くなる可能性があります。



デフォルトに戻す

[復元]をクリックして詳細設定内のすべての設定項目を工場出荷時のデフォルトに復元します。

10.2.4 シールド区域の設定

シールド区域を使用すると、設定されたSmart機能のルールが無効なエリアでも、特定のエリアを設定することができます。

ステップ

1. [シールド区域]を選択します。
2. をクリックして、シールド区域を指定します。さらにシールド区域を設定するには、上記の手順を繰り返します。
3. オプション:  をクリックして指定した領域を消去します。
4. [保存]をクリックします。

10.3 道路交通量

設定された車線に入る自動車、非自動車、歩行者を検知してキャプチャーすることにより、道路上のターゲットの迅速な検知と包括的な監視を実現します。

注意

この機能は一部のデバイスモデルのみでのサポートになります。

10.3.1 車両検知の設定

設定された車線に入る車両を検知し、車両の画像とナンバープレートをキャプチャーして保存することが可能です。アラームを作動させて、キャプチャをアップロードすることが可能です。

始める前に

[環境設定] → [システム] → [システム設定] → [リソース割り当て] と移動して、[道路交通] を選択します。

ステップ

1. [環境設定]→[道路交通]→[検出設定]と移動して、検知タイプで[車両の検知]を選択します。
2. [有効化]にチェックを入れます。
3. 車線番号を選択します。
4. 車線ラインをクリックアンドドラッグして位置を設定するか、またはラインの端点をクリックアンドドラッグしてラインの長さや角度を調整してください。
5. 画像上の車両の大きさが、赤枠の大きさに近くなるようにカメラのズームを調整してください。赤枠は位置飲み調整可能です。

注意

各車線につき、一度に 1 つだけナンバープレートのキャプチャが可能です。

6. [地域]と[国/地域]を選択します。
7. ナンバープレート情報アップロードモードを選択します。

入口/出口

車両が検知エリアを通過して入口/出口で検知が作動すると、検知された車両のナンバープレート情報がアップロードされます。

市街路

車両が検知エリアを通過して市街路で検知が作動すると、検知された車両のナンバープレート情報がアップロードされます。

アラーム入力

入力されたアラームにより、ナンバープレートのキャプチャと認識アクションが作動します。

 **注意**

アラーム入力を選択すると、車両の検知を作動させるためにA<-1のアラーム入力が自動的に割り当てられ、アラームの種類は常に[NO]となります。A<-1のアラーム入力を使用して車両の検知を作動させる場合、他の基本イベントには適用できません。アラーム入力を選択して保存すると、以前に設定したA<-1に対するリンク方式はキャンセルになります。

8. **[検知モード]**を選択します。
 9. **[Remove Duplicated License Plates]**にチェックを入れて、**[時間間隔]**を設定します。デフォルトの時間間隔は4分です。
-

 **注意**

ナンバープレートは8つまでサポートされます。

10. 監視スケジュールとリンク方式を設定します。監視スケジュールの設定については、**監視スケジュールの設定**を参照してください。リンク方式の設定については、**リンク方式の設定**を参照してください。
11. **[保存]**をクリックします。

10.3.2 混合トラフィックの検知ルールを設定

設定された車線に入る自動車、非自動車、歩行者を検知すると、ターゲットの画像をキャプチャーして保存することが可能です。アラームを作動させて、キャプチャをアップロードすることが可能です。

始める前に

[環境設定] → [システム] → [システム設定] → [リソース割り当て] と移動して、[道路交通] を選択します。

ステップ

1. [環境設定]→[道路交通]→[検出設定]と移動して、検知タイプで**[混合トラフィックの検知]**を選択します。
 2. **[有効化]**にチェックを入れます。
-

3. 車線番号を選択します。
4. **[地域]**と**[国/地域]**を選択します。
5. 監視スケジュールとリンク方式を設定します。監視スケジュールの設定については、**監視スケジュールの設定**を参照してください。リンク方式の設定については、**リンク方式の設定**を参照してください。
6. **[保存]**をクリックします。

10.3.3 画像アップロード設定

車両の検知や混合トラフィックの検知でキャプチャーされた画像のパラメータを設定することが可能です。

[環境設定]→**[道路交通]**→**[画像]**と移動します。

画質

値が大きいほど画像はクリアになりますが、ストレージ容量も大きくなります。

画像サイズ

値が大きいほど必要になるストレージ容量も大きくなります。また、ネットワーク伝送の要件レベルも高くなります。

ナンバープレート補正

値が大きいほどナンバープレートの画質はクリアになりますが、必要になるストレージ容量も大きくなります。

[License Plate Enhancement]にチェックを入れて、レベルを設定します。デフォルトのレベルは 50 である。

オーバーレイ

カメラ、デバイス、車両の情報をキャプチャ画像にオーバーレイするには、↑ ↓をクリックして、オーバーレイテキストの順番を調整します。

カメラの設定の場合、**[環境設定]→[道路交通]→[カメラ]**と移動して、関連するパラメータを設定し、**[保存]**をクリックします。

10.3.4 カメラ設定

各カメラのパラメータを設定して、管理を向上させることが可能です。

[環境設定]→[道路交通]→[カメラ]と移動して、関連するパラメータを設定し、**[保存]**をクリックします。

10.3.5 ブロックリスト&許可リストをインポート/エクスポート

任意でブロックリストと許可リストをインポートおよびエクスポートするには、このインターフェイスでリスト内容にチェックを入れます。

ステップ

1. **[ブラウザ]**をクリックして、PCのローカルディレクトリを開きます。
2. ブロックリスト&許可リストファイルを探し、クリックして選択します。**[開く]**をクリックして確認します。

注意

インポートするファイルは、カメラに必要なファイルテンプレートに対応している必要があります。カメラから空のブロックリスト&許可リストファイルをテンプレートとしてエクスポートして、内容を入力することをお勧めします。ファイルは.xls形式で、セルはテキスト形式である必要があります。

3. **[インポート]**をクリックし、選択したファイルをインポートします。
4. **[エクスポート]**をクリックして、PCのローカルディレクトリを開きます。
5. PCのローカルディレクトリでディレクトリを選択します。
6. ファイル名のテキストフィールドにファイル名を入力します。
7. **[保存]**をクリックします。

10.4 マルチターゲットタイプ検知

マルチターゲットタイプ検知とは、人間の顔、人体、車両など、複数のタイプに当てはまるターゲットのデータを検知、キャプチャー、アップロードすることです。



注意

一部のデバイスモデルでは、まず [リソース割り当て] のページで、[マルチターゲットタイプ検知] を有効化する必要があります。

10.4.1 マルチターゲットタイプ検知のルールを設定

マルチターゲットタイプ検知のルールとアルゴリズムパラメータを設定すると、デバイスは複数のタイプを有するターゲットをキャプチャーして、リンクアクションを自動的に作動させます。

ステップ

1. [環境設定]→[マルチターゲットタイプ検知]→[ルール]と移動します。
2. [ルール]にチェックを入れます。
3.  をクリックして、ライブ画像上に検知エリアを指定します。
4. テキストフィールドに最小瞳孔間距離を入力するか、 をクリックして最小瞳孔間距離を指定します。

最小瞳孔距離

最小瞳孔間距離は、2つの瞳孔の間のエリアの最小サイズを表し、デバイスが顔を識別するための基準となります。

5. 監視スケジュールを設定します。**監視スケジュールの設定**を参照してください。
6. リンク方式を設定します。**リンク方式の設定**を参照してください。
7. [保存]をクリックします。

次にすべきこと

[画像] に移動して、キャプチャ画像を検索して表示します。

[Smart Display] に移動して、現在キャプチャされているターゲット画像を確認します。

10.4.2 オーバーレイとキャプチャー

キャプチャパラメータと、ストリームやピクチャに表示する情報の設定を選択します。

VCA情報をオリジナル画像で表示します

ターゲットやルール情報など、ストリームのSmart情報を表示します。

キャプチャ画像の上に目標情報を表示する

アラーム画像とターゲット情報を重ね合わせます。

ターゲット画像の設定

カスタマイズ、ヘッドショット、半身ショット、全身ショットが選択可能です。

注意

[カスタマイズ]を選択した場合、必要に応じて[幅]、[頭の高さ]、[胴体の高さ]をカスタマイズすることが可能です。

[固定値]にチェックを入れると、画像の高さを設定することが可能です。

背景画像の設定

ターゲット画像と比較すると、背景画像は、Environment Infoを提供するシーン画像となります。背景画像の品質と解像度を設定することが可能です。背景画像を監視センターにアップロードする必要がある場合、[バックグラウンドアップロード]にチェックを入れます。

人数カウントをオーバーレイする

フローオーバーレイのタイプを選択します。

毎日のリセット時刻を選択します。今すぐリセットする場合、[手動リセット]をクリックします。

カメラ

カメラのデバイスNo.とカメラ情報を設定して、キャプチャ画像にオーバーレイ表示することが可能です。

テキストオーバーレイ

任意のアイテムにチェックを入れて、  でキャプチャーした画像に表示する順番を調整することが可能です。

デバイスNo.とカメラ情報の内容は同じページにある必要があります。

10.4.3 マルチターゲットタイプ検知のアルゴリズムパラメータ

マルチターゲットタイプ検知のアルゴリズムライブラリのパラメータを設定および最適化するために使用します。

[環境設定]→[マルチターゲットタイプ検知]→[高度な設定]と移動します。

HMSバージョン

現在のアルゴリズムバージョンを表し、編集することはできません。

デフォルトに戻す

[復元]をクリックして詳細設定内のすべての設定項目を工場出荷時のデフォルトに復元します。

パラメータ検知

生成速度

検知エリア内のオブジェクトがターゲットかどうかを判断するスピードです。値が高いほど、オブジェクトの検知が早くなります。デフォルト値での使用をお勧めします。

感度

ターゲットを認識する感度です。値が大きいほどターゲットを検知しやすくなりますが、誤認識が起こる可能性も高くなります。デフォルト値での使用をお勧めします。

キャプチャパラメータ

ベストショット

キャプチャしきい値

キャプチャーとアラームのトリガーになる顔の品質を表します。値が大きくなると、キャプチャーとアラームのトリガーとなる品質は高くなります。

顔露光

この機能を有効にすると、人物の顔がシーンに表示されたときに、デバイスが自動的に露光レベルを調整します。

参考明度

顔露出モードにおける顔の基準輝度を示します。実際のシーンの顔が設定した基準輝度より明るい場合、デバイスは露光レベルを下げます。実際のシーンの顔が設定した基準輝度より暗い場合、デバイスは露光レベルを上げます。

最小時間

顔がシーンからいなくなった後、デバイスが顔露出レベルを維持する時間。

顔認証フィルタリング時間

カメラが顔を検知してからキャプチャーのアクションを実行するまでの時間間隔を指します。検知された顔がシーン内に留まっている時間が、設定されたフィルタリング時間よりも短い場合、キャプチャーは作動しません。たとえば、顔のフィルタリング時間が5秒に設定されている場合、顔が5秒間シーンに留まっているときに、カメラは検知した顔をキャプチャーします。

10.4.4 シールド区域の設定

シールド区域を使用すると、設定されたSmart機能のルールが無効なエリアでも、特定のエリアを設定することができます。

DISSECURITY

ステップ

1. **[シールド区域]**を選択します。
2. をクリックして、シールド区域を指定します。さらにシールド区域を設定するには、上記の手順を繰り返します。
3. オプション: **X** をクリックして指定した領域を消去します。
4. **[保存]**をクリックします。

10.5 顔のカウント

顔カウント検知では、重複する顔を除外しながら、特定のエリアを出入りするオブジェクトを数えることが可能です。

注意

- 一部のデバイスモデルでは、まず **[リソース割り当て]** のページで、**[顔のカウント]** を選択する必要があります。
 - この機能は、一部のカメラモデルでのみサポートされます。
-

10.5.1 顔カウント検知のルールを設定

顔カウント検知のルールとアルゴリズムパラメータを設定すると、デバイスはターゲットをキャプチャーして、リンクアクションを自動的に作動させます。

ステップ

1. **[環境設定]**→**[顔のカウント]**→**[ルール]**と移動します。
2. **[ルール]**にチェックを入れます。
3. テキストフィールドに最小瞳孔間距離を入力するか、をクリックして最小瞳孔間距離を指定します。指定された瞳孔間の間隔はライブビューに下のボックスに表示されます。







最小瞳孔距離

最小瞳孔間隔は、2つの瞳孔の間のエリアによって形作られる最小サイズの四角形で表され、カメラがターゲットを識別するための基準となります。

4. テキストフィールドに最大瞳孔間距離を入力するか、をクリックして最大瞳孔間距離を指定します。

最大瞳孔間距離

最大瞳孔間隔は、2つの瞳孔の間のエリアによって形作られる最大サイズの四角形で表され、カメラがターゲットを識別するための基準となります。

5. をクリックして、検知エリアを指定します。ライブビューウィンドウ上で頂点を左クリックでエリアを指定して、右クリックでエリア指定を終了します。
6. をクリックして、検知ラインを指定します。矢印は進入方向を示します。をクリックすると、方向を変えることが可能です。
 - ターゲットが進入方向に沿ってカウントエリアを通過した場合や検知ラインを通過した場合、進入数としてカウントされます。
 - ターゲットが退出方向に沿ってカウントエリアを通過した場合や検知ラインを通過した場合、退出数としてカウントされます。
7. と をクリックして、範囲 A と範囲 B を指定します。2つのエリアが重なっていないことを確認します。をクリックすると、方向を変えることが可能です。
 - ターゲットが範囲Aから範囲Bに入ると、進入数にカウントされます。
 - ターゲットが範囲Bから範囲Aに入ると、退出数にカウントされます。
8. 監視スケジュールを設定します。**監視スケジュールの設定**を参照してください。
9. リンク方式を設定します。**リンク方式の設定**を参照してください。

10.5.2 オーバーレイとキャプチャー

キャプチャパラメータと、ストリームやピクチャに表示する情報の設定を選択します。

VCA情報をオリジナル画像で表示します

ターゲットやルール情報など、ストリームのSmart情報を表示します。

キャプチャ画像の上に目標情報を表示する

アラーム画像とターゲット情報を重ね合わせます。

ターゲット画像の設定

カスタマイズ、ヘッドショット、半身ショット、全身ショットが選択可能です。

注意

[**カスタマイズ**]を選択した場合、必要に応じて[**幅**]、[**頭の高さ**]、[**胴体の高さ**]をカスタマイズすることが可能です。

[**固定値**]にチェックを入れると、画像の高さを設定することが可能です。

背景画像の設定

ターゲット画像と比較すると、背景画像は、Environment Infoを提供するシーン画像となります。背景画像の品質と解像度を設定することが可能です。背景画像を監視センターにアップロードする必要がある場合、[**バックグラウンドアップロード**]にチェックを入れます。

人数カウントをオーバーレイする



フローオーバーレイのタイプを選択します。

毎日のリセット時刻を選択します。今すぐリセットする場合、[**手動リセット**]をクリックします。

カメラ

カメラのデバイスNo.とカメラ情報を設定して、キャプチャ画像にオーバーレイ表示することが可能です。

テキストオーバーレイ

任意の項目にチェックを入れて、でキャプチャーされた画像に表示する順番を調整することが可能です。

デバイスNo.とカメラ情報の内容は同じページにある必要があります。

10.5.3 顔カウントのアルゴリズムパラメータ

顔カウントのアルゴリズムパラメータを設定および最適化するために使用します。

注意

これらの機能はモデルによって異なります。

顔キャプチャモード

現在のアルゴリズムバージョンを表し、編集することはできません。

ベストショット

ターゲットが検知エリアから離れた後のベストショット。

キャプチャー回数

設定されたエリア内に留まっている間に顔がキャプチャーされるキャプチャ回数を示します。デフォルト値は「1」です。

キャプチャしきい値

キャプチャーとアラームのトリガーになる顔の品質を表します。値が大きくなると、キャプチャーとアラームのトリガーとなる品質は高くなります。

顔露光

デバイスは、画像内の顔を検知すると、顔の輝度を調整します。

参考明度

顔露出モードにおける顔の基準輝度を示します。顔が検出された場合、カメラは設定された値にもとづいて顔の明るさを調整します。値が大きいほど顔は明るくなります。

最小持続時間

カメラが顔を露出する最小時間です。

注意

顔露出が有効になっている場合、WDR機能が無効になっていることと、手動絞りが選択されていることを確認してください。

リアルタイムアップデートデータ

有効化すると、リアルタイム人数カウントデータがプラットフォームにアップロードされます。

データ統計周期

必要に応じて、データ統計周期を選択します。

アルゴリズム有効性

値が大きいほどターゲットを検知しにくくなりますが、検知精度が高くなります。

デフォルトに戻す

[復元]をクリックして詳細設定内のすべての設定項目を工場出荷時のデフォルトに復元します。

10.5.4 顔カウント結果の表示

ステップ

1. [アプリケーション]に移動します。
2. 検索条件を設定して、[カウント]をクリックします。
一致した結果は、[顔画像比較統計]と[人数統計]のエリアに表示されます。

10.6 待ち行列管理

並んでいる人の数と、各人の待ち時間をカウントするために使用します。

注意

待ち行列管理は一部のデバイスでのみサポートされます。

10.6.1 エリア内行列の設定

定められたエリア内で並んでいる人をカウントするために使用します。アラームしきい値の条件とアラームのトリガーがともに満たされると、アラームが作動します。

始める前に

この機能を有効化するには、[リソース割り当て]に移動して、[待ち行列管理]を選択します。

ステップ

1. [環境設定]→[待ち行列管理]と移動します。
2. [エリア内行列]を選択します。
3. [エリア追加]をクリックして検知エリアを指定して、[エリア名]と[アラーム間隔]を設定します。さらにエリアを設定するには、上記の手順を繰り返します。

アラーム間隔

設定されたアラーム間隔の間、同じタイプのアラームに対する通知は1回だけとなります。



図 10-2 エリア内行列の設定

4. オプション: [OSD]にチェックを入れると、エリア名とリアルタイムでの行列人数が表示されます。
5. [アラームしきい値]を設定します。アラームしきい値の条件が満たされると、アラームが作動します。
6. 監視スケジュールの設定については、**監視スケジュールの設定**を参照してください。リンク方式の設定については、**リンク方式の設定**を参照してください。
7. [保存]をクリックします。

10.6.2 待機時間検知の設定

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します。アラームしきい値の条件とアラームのトリガーがともに満たされると、アラームが作動します。

始める前に

この機能を有効化するには、[リソース割り当て]に移動して、[待ち行列管理]を選択します。

ステップ

1. [環境設定]→[待ち行列管理]と移動します。
2. [待機時間検知]を選択します。
3. [エリア追加]をクリックして検知エリアを指定して、[エリア名]と[アラーム間隔]を設定します。さらにエリアを設定するには、上記の手順を繰り返します。

アラーム間隔

設定されたアラーム間隔の間、同じタイプのアラームに対する通知は1回だけとなります。



図 10-3 待機時間検知の設定

4. [アラームしきい値]を設定します。アラームしきい値の条件が満たされると、アラームが作動します。
5. 監視スケジュールの設定については、**監視スケジュールの設定**を参照してください。
リンク方式の設定については、**リンク方式の設定**を参照してください。
6. [保存]をクリックします。

7. オプション: **[環境設定]**→**[ローカル]**と移動して、**[POS 情報を表示]**と**[ルール]**を有効化します。
- 検知エリアと、人がそこに留まっている時間は、ライブビューに表示することが可能です。

10.6.3 待ち行列管理統計

待ち行列管理は、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、**エリア内行列の設定**と**待機時間検知の設定**を参照してください。

- **[待ち行列時間解析]**と**[範囲比較]**を選択すると、異なるエリア内の行列人数を比較します。
- **[待ち行列時間解析]**と**[多重レベル比較]**を選択すると、異なる待機時間レベルの行列人数を比較します。
- **[待ち行列ステータス解析]**と**[範囲比較]**を選択すると、異なるエリアで一定の長さの行列が発生する回数と行列の持続時間を比較します。
- **[待ち行列ステータス解析]**と**[多重レベル比較]**を選択すると、異なる待ち行列長レベルでの行列回数と持続時間を比較します。

ステップ

注意

オンボードメモリカードがインストールされている場合、デバイスは最長1カ月までデータを保存することが可能です。メモリカードがインストールされていない場合、デバイスは最長1週間までしかデータを保存できません。

1. 解析モードを選択します。

待ち行列時間解析

待ち行列時間解析では、異なる待機時間レベルの人数を計算します。

待ち行列ステータス解析

待ち行列ステータス解析では、行列が一定の長さで発生する回数と持続時間を計算します。

2. 統計タイプを選択します。

範囲比較

複数のエリアと1つのレベルを選択して解析を行い、解析グラフを作成することが可能です。

多重レベル比較

複数のエリアとレベルを選択して解析を行い、各エリアごとの解析グラフを作成することが可能です。

3. エリアにチェック（複数可）を入れます。
4. 待ち行列長レベルを設定します。任意の範囲のチェックボックスにチェック（複数可）を入れて、値を入力します。
5. **[レポートタイプ]**と**[統計時間]**を選択します。
6. **[カウント]**をクリックすると、レポートが生成されます。

10.7 カウント

特定の設定エリアに出入りする人の数を計算することができます。

注意

カウントは一部のモデルでのみサポートされます。

10.7.1 カウントの設定

エリアに入出入りするオブジェクトを計算してイベントのアラームを出し、データをアップロードするために使用します。

ステップ

1. [環境設定]→[カウント]と移動します。
2. [カウントを有効化]にチェックを入れます。
3. オプション: [OSD オーバーレイを有効化]にチェックを入れると、エリアを出入りした人数がリアルタイムでライブビデオ上に表示されます。

注意

オーバーレイ情報のカウントは当日の数のみです。デバイスが再起動されたとき、または午前0時になったときに、この数はクリアされます。または、0をクリックして、手動で数をクリアすることも可能です。




4. 検知ラインを設定すると、ラインを通過するオブジェクトが検知され、カウントされます。
 -  検知ラインを指定します。
 -  検知ラインを削除します。
 -  方向を変えます。



図 10-4 カウントの設定

5. 監視スケジュールの設定については、**監視スケジュールの設定**を参照してください。
リンク方式の設定については、**リンク方式の設定**を参照してください。
6. **[保存]**をクリックします。

10.7.2 計数統計の表示

デバイスまたはメモリカードに保存されている計数統計を表示およびエクスポートすることが可能です。

始める前に

[カウントの設定]へ移動して、まず待ち行列管理を設定します。

ステップ

1. **[アプリケーション]**に移動します。
2. **[レポートタイプ]**を選択します。
3. **[統計タイプ]**を選択します。
4. **[開始時間]**を選択します。
5. **[カウント]**をクリックします。
6. オプション:**[エクスポート]**をクリックして、計数統計をエクスポートします。
計数統計は、表、折れ線グラフ、棒グラフで表示することが可能です。

10.8 安全帽検出

この機能は、設定した監視エリア内で安全帽（ヘルメット）を着用していないターゲットを検知して、アラームを作動させます。

注意

この機能は一部のデバイスモデルのみでのサポートになります。

10.8.1 安全帽検出の設定

始める前に

[環境設定]→**[システム]**→**[システム設定]**→**[リソース割り当て]**と移動して、**[安全帽検出]**を

有効化します。

ステップ

1. **[環境設定]**→**[安全帽検出]**と移動して、**[安全帽検出を有効化]**にチェックを入れます。
2. オプション:**[ターゲットの生成スピード]**を設定します。

ターゲット生成速度

検知エリアに入る顔のターゲットの生成スピードを表します。この値が大きくなるほど、生成速度も速くなります。

3. 検知エリアを設定します。
 - 1) 検知エリアを選択します。
 - 2) **[領域指定]**をクリックして、ライブビュー画像内のエリアの頂点を指定します。
 - 3) 右クリックで指定を終了します。

[エリア指定を中止]をクリックして、エリア指定を終了します。

[すべてクリア]をクリックして、再度エリアを指定します。

4. 監視スケジュールの設定については、**監視スケジュールの設定**を参照してください。
リンク方式の設定については、**リンク方式の設定**を参照してください。
5. **[保存]**をクリックします。

10.9 顔比較とモデリング

一部のデバイスモデルでは、まず **[リソース割り当て]** のページで、**[マルチターゲットタイプ検知]**または**[顔キャプチャ]**を有効化する必要があります。


10.9.1 顔比較

顔比較は、キャプチャーされた顔と顔画像ライブラリ内の顔を比較することを目的としています。

顔画像ライブラリの設定



顔画像ライブラリは、モデル化された人間の顔や情報を格納するために使用します。

ステップ

1. [環境設定]→[顔画像ライブラリ]と移動します。
2. 顔画像ライブラリを作成します。
 - 1) をクリックして、顔画像ライブラリを追加します。
 - 2) ライブラリ名、しきい値、注釈を入力します。

しきい

設定したしきい値よりも顔の類似性が高いと、顔画像の比較アラームがアップロードされます。

- 1) [OK]をクリックします。
 - 2) オプション: 顔画像ライブラリを変更します。任意のライブラリを選択して、をクリックし、関連するパラメータを変更します。
 - 3) オプション: ライブラリを削除します。任意のライブラリを選択して、をクリックします。
3. 顔画像をライブラリに追加します。

注意

画像形式はJPEGで、サイズは1ファイルあたり300KB以下である必要があります。

顔画像を1つ追加する [追加]をクリックして、顔の詳細情報を含む顔画像をアップロードします。

顔画像を一括でインポートする [インポート]をクリックして、画像パスを選択します。

注意

- 顔画像を一括でインポートすると、画像の名前が顔の名前とし

て保存されます。その他の顔情報については、手動で1つずつ変更する必要があります。

- エクスポートやインポートの認証コードは、8~16桁の数字、大文字、小文字を組み合わせたものである必要があります。

4. オプション: 顔情報を変更します。

- 1) 顔画像ライブラリを選択します。
- 2) ターゲットの顔画像を選択します。検索機能を使用すると、名前や性別などの検索条件を入力して **[検索]** をクリックすると画像を検索することが可能です。
- 3) **[変更]** をクリックします。
- 4) 詳細情報を編集します。

 **注意**

顔画像は変更できません。

5) **[OK]** をクリックします。

DISSECURITY

5. ライブラリ内の顔画像ごとにモデルを作成します。

モデリング処理では、各顔画像の顔モデルが作成されます。顔モデルは、顔画像の比較を行う上で必要になります。

モデリング 1つまたは複数の顔画像を選択して、**[モデリング]**をクリックします。

一括モデリング 顔画像ライブラリを選択して、**[一括モデリング]**をクリックします。

6. オプション: さらに顔のライブラリを作成する場合、手順を繰り返します。

7. **[保存]**をクリックします。

顔画像の比較を設定

この機能では、キャプチャーされた画像とライブラリ内の顔画像を比較して、比較結果を出力します。監視スケジュールとリンク方式が設定されている場合、比較結果により、特定のアクションを作動させることが可能です。

始める前に

まず、顔画像ライブラリを作成して、顔画像を追加する必要があります。**顔画像ライブラリの設定**を参照してください。

ステップ

1. **[環境設定]**→**[比較とモデリング]**→**[顔比較とモデリング]**と移動します。
2. **[顔画像の比較]**を選択します。
3. **[顔画像比較を有効化]**にチェックを入れます。
4. 参照する顔画像ライブラリを選択します。
5. オプション: マルチターゲットタイプキャプチャのアラーム中に顔比較情報を受信する場合、**[マルチターゲットタイプキャプチャアラーム中に顔比較情報をレポート]**にチェックを入れます。
6. 任意の顔情報を選択して、アップロードします。
7. 顔の比較モードを選択します。

ベスト比較 デバイスは、ターゲットの顔が検知エリア内にいるときに、その

顔を継続的にキャプチャーおよび比較して、その顔がエリアを離れるときに、最高スコアが付けられた顔画像と関連するアラーム情報をアップロードします。

クイック比較

デバイスは、顔の評価が設定された**[キャプチャ時の顔グレーディング閾値]**を超えたときに、ターゲットの顔をキャプチャーして比較します。

キャプチャ時の顔グレーディングしきい値

デバイスが顔をキャプチャーしてアップロードするかどうかを判断するための顔評価のしきい値。

最大キャプチャ間隔

ターゲットが検知エリアにいるときに行われる各キャプチャーの最大間隔。顔の評価が設定したしきい値に達しない場合でも、カメラは最大間隔に達したときにキャプチャーを行います。

クイック設定モード

実際に使用するシナリオに合わせて、モードを選択します。カスタムモードでは、**[比較のタイムアウト]**と**[比較回数]**を設定することが可能です。

8. 監視スケジュールを設定します。**監視スケジュールの設定**を参照してください。
9. リンク方式を設定します。**リンク方式の設定**を参照してください。

顔比較結果の表示

ステップ

1. [アプリケーション]に移動します。
2. 検索条件を設定して、[カウント]をクリックします。
一致した結果は、[顔画像比較統計]のエリアに表示されます。

10.9.2 顔モデリング

顔モデリングは、顔画像の収集、顔モデルの作成、監視センターへのデータのアップロードを目的としています。

始める前に

顔の画像の収集には、顔キャプチャまたはマルチターゲットタイプ検知を設定する必要があります。設定手順については、**顔キャプチャ**または**マルチターゲットタイプ検知**を参照してください。

ステップ

1. [環境設定]→[比較とモデリング]→[顔比較とモデリング]と移動します。
2. [顔モデリング]を選択して開始します。
3. [顔モデリングを有効化]にチェックを入れます。
4. モデリングのパラメータを設定します。

マルチターゲットタイプキャプチャのアラーム時における顔モデリング情報のレポート

マルチターゲットタイプ検知が作動すると、アラーム情報には、検知した顔の顔モデリング情報が含まれます（有効化になっている場合）。

クイックキャプチャー

デバイスは、設定されたキャプチャ時の顔グレーディングしきい値より高いスコアの顔を検知すると、顔モデリングを開始します。

キャプチャ時の顔グレーディングしきい値

デバイスが顔をキャプチャーしてアップロードするかどうかを判断するための顔評価のしきい値。値が大きいほど、画質が向上します。

最大キャプチャ間隔

ターゲットが検知エリアにいるときに行われる各キャプチャーの最大間隔。顔の評価が設定したしきい値に達しない場合でも、カメラは最大間隔に達したときにキャプチャーを行います。

5. 監視スケジュールを設定します。**監視スケジュールの設定**を参照してください。
6. リンク方式を設定します。**リンク方式の設定**を参照してください。

D'SSECURITY

CHAPTER 11 オープンプラットフォーム

オープンプラットフォームにより、サードパーティが機能やサービスを開発したり実行したりできるアプリケーションをインストールすることが可能になります。

注意

この機能は一部のデバイスモデルのみでのサポートになります。

11.1 オープンプラットフォームの設定

ステップ

1. [環境設定]→[プラットフォームを開く]と移動します。

注意

アプリケーションをインストールする前に、下部の免責事項を読み、インストールするアプリケーションが次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は独自の排他的な名前を有しています。
 - アプリケーションが占めるフラッシュメモリ容量は、デバイスの使用可能なフラッシュメモリ容量よりも小さくなります。
 - アプリケーションのメモリおよびコンピューティング能力は、デバイスの利用可能なメモリおよびコンピューティング能力よりも低くなります。
-

2. [アプリのインストール]で[ブラウザ]をクリックして、インポートしたアプリケーションパッケージを選択します。

3. [インポート]をクリックして、インストールを完了します。

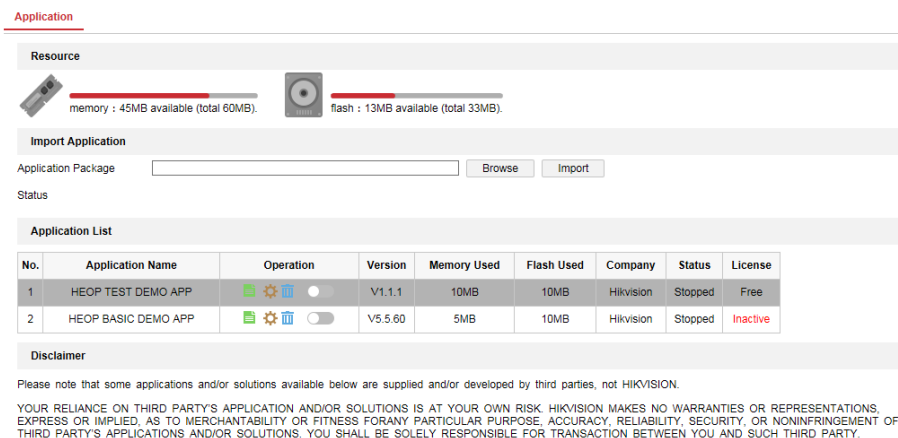


図 11-1 オープンプラットフォーム

アプリケーション名、操作、バージョン、使用のメモリ、使用のフラッシュ、会社、ステータス、ライセンスなど、インストールされているアプリケーションとその関連情報が**[アプリケーションリスト]**に表示されます。

4. オプション: アプリケーションを設定する。



ログをエクスポートする。



権限を設定する。



アプリケーションを削除する。



アプリケーションを有効化または無効化する。

5. オプション: アプリケーションの表示中に、**[ブラウザ]**をクリックして、アプリケーション証明書をインポートします。

CHAPTER 12 スマート表示

Smart機能を有効化すると、キャプチャ画像を表示することが可能です。

レイアウトプレビュー

[レイアウトプレビュー]をクリックおよび選択します。ニーズに合わせて内容を選択します。リアルタイム解析を選択すると、リアルタイム解析に限定して内容を選択することが可能です。

検出属性

[検出属性]をクリックおよび選択します。この機能を有効化すると、ターゲット解析の属性情報が表示され、選択した情報が属性解析エリアに表示されます。

D'SSECURITY

CHAPTER 13 EPTZの設定

EPTZ（電子PTZ）は、物理的なカメラの動きを必要とせずに、画像の一部をデジタルでズームやパンする高解像度機能です。

始める前に

EPTZ機能を使用する場合、ライブビューで第4ストリームが選択されていることを確認します。第4ストリームとEPTZの両方を同時に有効化する必要があります。

13.1 パトロール

ステップ

1. [環境設定]→[EPTZ]と移動します。
2. [EPTZ を有効化]にチェックを入れます。
3. [第4ストリーム]にチェックを入れます。
4. [アプリケーション]で[パトロール]を選択します。
5. [保存]をクリックします。

次にすべきこと

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

13.2 自動追跡機能

ステップ

1. [環境設定]→[EPTZ]と移動します。
2. [EPTZ を有効化]にチェックを入れます。
3. [第4ストリーム]にチェックを入れます。
4. [アプリケーション]で[Auto-Track 機能]を選択します。
5. [検知エリア]をクリックして、指定を開始します。
6. ライブビデオ上でクリックして、検知エリアの4つの頂点を指定し、右クリックで指定を完了します。

7. ルールを設定します。

検知ターゲット

人間と車両に対して利用可能です。検知ターゲットが選択されていない場合、検知されたすべてのターゲット（人体や車両など）が追跡されます。

 **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ます。

感度

許容ターゲットの体（または本体）の一部が追跡されている率（パーセンテージ）を表します。感度 = $100 - S1/ST \times 100$ 。S1は、予め定義したエリアに進入しているターゲットの体（または本体）の一部を表します。STはターゲット全体を表します。感度の値が高いほど、ターゲットは追跡されやすくなります。

8. **[保存]**をクリックします。

D'SSECURITY

CHAPTER 14 パターンリンク

パターンリンクが設定されると、デバイスは、キャプチャされた顔や人体情報を別のチャンネルからリンクさせることが可能です。

注意

この機能はマルチチャンネルのデバイスでのみサポートされます。

14.1 パターンリンクの設定

パターンリンクが設定されると、デバイスは、キャプチャされた顔、人体、車両情報を別のチャンネルからリンクさせることが可能です。

始める前に

スマートモードの切り替えを確認して、**[Pattern Mode]**にチェックを入れます。

ステップ

1. **[環境設定]**→**[パターンリンク]**→**[キャリブレーション]**と移動します。
2. **[ポイントの追加]**をクリックして、カメラ 1 のポイントを画像内のリファレンスに移動し、カメラ 2 の同じ数のポイントに対応するリファレンスに移動します。

ポイントの削除 選択したポイントをすべて削除します。

すべてクリア ポイントをすべて削除します。

3. 追加したポイントを別のリファレンスに移動する場合、ステップ 2 を繰り返します。
少なくとも 12 個のキャリブレーションポイントを追加することをお勧めします。

 **注意**

- ポイントは分散している必要があり、ポイントの3/4を1つのラインに配置することはできません。
 - デバイスは4～64のキャリブレーションポイントをサポートしています。
-

4. **[パリティ]**をクリックして、カメラ 1 とカメラ 2 のポイントが同じリファレンス位置にあることを確認します。同じ位置にない場合、再度ポイントを調整またはキャリブレーションします。
 - チャンネル2とチャンネル1が同じリファレンスにある場合、キャリブレーションは成功です。
 - チャンネル2とチャンネル1が同じリファレンスにない場合、キャリブレーションは失敗です。ステップ2で、再度ポイントを調整またはキャリブレーションします。
5. **[ルール]**をクリックして、**[パターンリンクを有効化]**にチェックを入れます。
6. **[保存]**をクリックします。

D'SSECURITY

A. デバイスコマンド

デバイス共通のシリアルポートコマンドを取得するには、次のQRコードをスキャンします。コマンドリストには、すべてのHikvisionネットワークカメラでよく使用されるシリアルポートコマンドが含まれていますので注意してください。



D'SSECURITY

B. デバイスの通信マトリックス

デバイスの通信マトリックスを取得するには、次のQRコードをスキャンします。
このマトリックスには、Hikvisionネットワークカメラのすべての通信ポートが含まれてい
ますので注意してください。



D'SSECURITY



See Far, Go Further