



ネットワークカメラ

ユーザーマニュアル

法的情報

このドキュメントについて

- この文書には、製品の使用および管理に関する手順が記載されています。本文中に含まれる図、表、画像その他の情報は、説明および参考目的のみを目的としています。
- 本ドキュメントに記載されている情報は、ファームウェアの更新またはその他の理由により、事前の通知なしに変更される場合があります。最新のバージョンは、Hikvisionのウェブサイト (<https://www.hikvision.com>) でご確認ください。別途合意がない限り、杭州 Hikvision デジタルテクノロジー株式会社またはその関連会社（以下「Hikvision」といいます）は、明示的または黙示的ないかなる保証もいたしません。
- 本ドキュメントは、製品をサポートする専門家の指導と支援を受けて使用してください。

本製品について

- この製品は、購入された国または地域でのみアフターサービスサポートを受けることができます。
- 選択された製品が動画製品の場合、以下のQRコードをスキャンして「動画製品の利用に関する取り組み」を取得し、必ずお読みください。



知的財産権に関する承認

- 本ドキュメントに記載される製品に組み込まれた技術に関する著作権および/または特許権は、Hikvisionが所有しています。これには、第三者から取得したライセンスを含む場合があります。
- 本文書の一部（テキスト、画像、グラフィックなど）はすべてHikvisionに帰属します。本文書のいかなる部分も、書面による許可なしに、引用、複製、翻訳、または改変を行うことはできません。
- **HIKVISION** およびその他のHikvisionの商標およびロゴは、各管轄区域においてHikvisionの財産です。
- その他の商標およびロゴは、それぞれ該当する所有者の財産です。

法的免責事項

- 適用される法律で許される最大限の範囲において、本文書および記載された製品（ハードウェア、ソフトウェア、ファームウェアを含む）は「現状有姿」かつ「一

切の瑕疵およびエラーを含む」状態で提供されます。ヒクビジョンは、明示的または黙示的ないかなる保証もいたしません。

明示的または黙示的な一切の保証（商品性、満足のいく品質、または特定の目的への適合性を含むがこれらに限定されない）は、一切提供されません。製品の使用は、お客様の責任において行われます。いかなる場合においても、HIKVISIONは、特別損害、間接損害、付随的損害、または派生的損害（事業利益の損失、事業の中断、データの損失を含むがこれらに限定されない）について、契約違反、不法行為（過失を含む）、製品責任、またはその他のいかなる理由に基づくものであっても、一切の責任を負いません。システムの破損、または文書の損失を含む損害について、契約違反、不法行為（過失を含む）、製品責任、またはその他の理由に基づくものであっても、製品の使用に関連して生じた場合であっても、HIKVISIONは一切の責任を負いません。

- あなたは、インターネットの性質上、内在するセキュリティリスクが存在することを承認し、HIKVISIONは、サイバー攻撃、ハッカー攻撃、ウイルス感染、またはその他のインターネットセキュリティリスクに起因する異常な動作、プライバシー漏洩、またはその他の損害について一切の責任を負いません。ただし、必要に応じて適切な技術サポートを提供します。
- あなたは、この製品を適用されるすべての法律に準拠して使用することに同意し、あなたの使用が適用される法律に準拠していることを確保する責任はあなたのみにあります。特に、あなたは、第三者の権利（**publicity rights**、知的財産権、データ保護その他のプライバシー権を含むがこれらに限定されない）を侵害しない方法で本製品を使用する責任を負います。お客様は、大量破壊兵器の開発または製造、化学兵器または生物兵器の開発または製造、核爆発に関連する活動、または安全でない核燃料サイクルに関連する活動、または人権侵害を支援する活動を含む、いかなる活動にも使用してはなりません。
- 本文書と適用される法律との間に矛盾が生じた場合、後者が優先されます。

©杭州 Hikvision デジタルテクノロジー株式会社。著作権所有。

記号の定義

本文書中に使用される記号は、以下のとおり定義されます。

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

安全注意事項

以下のQRコードをスキャンして製品の「安全注意事項」を取得し、必ずお読みください。
これらの注意事項は、ユーザーが製品を正しく使用し、危険や財産損失を防止するための
ものです。



図1-1 安全注意事項

目次

第1章 概要	1
1.1 設定手順.....	1
1.2 ファームウェアの更新	1
1.3 システム要件	1
第2章 デバイスのアクティベーションとアクセス	3
2.1 SADP経由でデバイスをアクティブ化.....	3
2.2 ブラウザ経由でデバイスをアクティベート.....	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	5
2.3.3 不正ログインロック	6
第3章 ライブビュー.....	7
3.1 ライブビューパラメーター.....	7
3.1.1 ライブビューの開始と停止.....	7
3.1.2 アスペクト比	7
3.1.3 ライブビュー ストリーム タイプ.....	7
3.1.4 サードパーティプラグインを選択.....	7
3.1.5 ライト	8
3.1.6 ピクセルを数える.....	8
3.1.7 デジタルズーム	8
3.1.8 補助フォーカス.....	8
3.1.9 レンズ初期化	9
3.1.10 レンズパラメーター調整	9
3.1.11 3D位置決めを実施	11
3.2 伝送パラメーターの設定.....	11

第4章 動画と音声	13
4.1 動画設定	13
4.1.1 ストリームの種類	13
4.1.2 動画形式	13
4.1.3 解像度	13
4.1.4 ビットレートタイプと最大ビットレート	14
4.1.5 動画品質	14
4.1.6 フレームレート	14
4.1.7 動画エンコード	14
4.1.8 スムージング	16
4.2 オーディオ設定	16
4.2.1 オーディオエンコード	17
4.2.2 オーディオ入力	17
4.2.3 オーディオ出力	17
4.2.4 環境ノイズフィルター	17
4.3 双方向オーディオ	17
4.4 ROI	18
4.4.1 ROIを設定	18
4.5 ターゲットクロッピングを設定	19
4.6 ストリームに情報を表示	19
4.7 設定を表示	19
4.7.1 シーンモード	20
4.7.2 画像パラメーター切り替え	25
4.7.3 ビデオ規格	26
4.7.4 ローカルビデオ出力	26
4.8 OSD	26
4.9 プライバシーマスクを設定	27

4.10 画像を重ねる	27
第5章 動画録画と画像キャプチャ	28
5.1 ストレージ設定	28
5.1.1 メモリカード.....	28
5.1.2 FTPを設定.....	30
5.1.3 NASを設定.....	31
5.1.4 eMMC保護	32
5.1.5 クラウドストレージの設定	32
5.2 動画録画	33
5.2.1 自動録画	33
5.2.2 手動録画	35
5.2.3 動画の再生とダウンロード	35
5.3 キャプチャ設定	36
5.3.1 自動キャプチャ	36
5.3.2 手動でキャプチャ	36
5.3.3 画像の表示とダウンロード	37
第6章 イベントとアラーム	38
6.1 モーション検出の設定	3
6.1.1 エキスパートモード.....	38
6.1.2 通常モード.....	39
6.2 動画改ざんアラームの設定	40
6.3 アラーム入力の設定	41
6.4 例外アラームを設定	42
6.5 動画品質診断を設定	42
6.6 オーディオ例外検出を設定	43
6.7 ボケ検出の設定	44
6.8 シーン変更検出の設定	44

第7章 警報スケジュールとアラーム連携	45
7.1 武装スケジュール設定	45
7.2 連動方法の設定	45
7.2.1 アラーム出力トリガー設定	46
7.2.2 FTP/NAS/メモ리카ードへのアップロード	47
7.2.3 メール送信	47
7.2.4 監視センターへの通知	48
7.2.5 録画を開始	48
7.2.6 点滅するライト	48
7.2.7 音による警告	49
7.2.8 アラームサーバー	50
第8章 ネットワーク設定	51
8.1 TCP/IP	51
8.2 ドメイン名によるデバイスへのアクセス	52
8.3 PPPoEダイヤルアップ接続経由でのデバイスへのアクセス	53
8.4 SNMP	53
8.5 IEEE 802.1Xの設定	54
8.6 QoSを設定	54
8.7 HTTP(S)	55
8.8 マルチキャスト	56
8.8.1 マルチキャスト検出	56
8.9 RTSP	56
8.10 SRTPを設定	57
8.11 Bonjour	57
8.12 WebSocket(s)	58
8.13 ポートマッピング	58
8.13.1 自動ポートマッピングを設定	58

8.13.2 手動ポートマッピングを設定	58
8.13.3 ルーターでのポートマッピングを設定	59
8.14 RTCP	60
8.15 ワイヤレスダイヤル	60
8.15.1 ワイヤレスダイヤルを設定	60
8.15.2 ワイヤレスエキスパート設定	61
8.16 WLAN AP（アクセスポイント）	63
8.16.1 WLAN APを設定	63
8.16.2 AP経由でのデバイスへのアクセス	64
8.17 トラフィックシェーピング	65
8.18 データ監視	65
8.19 Wi-Fi	65
8.19.1 デバイスをWi-Fiに接続	66
8.20 ISUPを設定	66
8.21 Hik-Connect経由でカメラにアクセスする	67
8.21.1 カメラでHik-Connectサービスを有効にする	67
8.21.2 Hik-Connectを設定する	68
8.21.3 カメラをHik-Connect追加する	69
8.22 オープンネットワークビデオインターフェースの設定	70
8.23 SDK サービスの設定	70
第9章 システムとセキュリティ	7
9.1 システム設定	71
9.1.1 デバイス情報の表示	71
9.1.2 日時	71
9.1.3 RS-232の設定	72
9.1.4 RS-485を設定	73
9.1.5 ライブビュー接続設定	73

9.1.6 位置設定	73
9.1.7 外部デバイス	74
9.1.8 オープンソースソフトウェアのライセンスを表示.....	74
9.1.9 Wiegand	74
9.2 ユーザーとアカウント.....	74
9.2.1 ユーザー アカウントと権限の設定.....	74
9.2.2 同時ログイン	75
9.2.3 オンラインユーザー	75
9.3 メンテナンス.....	75
9.3.1 再起動	75
9.3.2 アップグレード.....	75
9.3.3 復元とデフォルト設定.....	76
9.3.4 設定ファイルのインポートとエクスポート.....	76
9.3.5 ログの検索と管理.....	77
9.3.6 セキュリティ監査ログの検索.....	77
9.3.7 SSH	77
9.3.8 診断情報の	78
9.3.9 診断	78
9.4 セキュリティ.....	80
9.4.1 IPアドレスフィルタの設定	80
9.4.2 MACアドレスフィルタの設定.....	80
9.4.3 タイムアウト設定の制御	81
9.4.4 証明書管理.....	81
9.4.5 TLS	84
第10章 VCA リソース.....	85
10.1 オープンプラットフォームを設定.....	85
10.2 一般設定	86

10.2.1 カメラ情報の設定	86
10.2.2 メタデータ	86
10.2.3 AcuSearch.....	87
10.3 スマートイベント	87
10.3.1 侵入検知の設定	88
10.3.2 ライン越え検出を設定	89
10.3.3 領域進入検出を設定	91
10.3.4 領域退出検出を設定	92
10.3.5 無人手荷物検出を設定	94
10.3.6 物体除去検出設定	95
10.3.7 不審者滞留検出の設定	97
10.3.8 人の集まり検出の設定	98
10.3.9 高速移動検出を設定	99
10.3.10 駐車検出設定	101
10.4 顔検出	102
10.4.1 顔検出設定	102
10.4.2 オーバーレイとキャプチャ	103
10.4.3 顔検出アルゴリズムのパラメーター	104
10.4.4 シールド領域を設定	106
10.5 人材管理	107
10.5.1 地域別人員カウント	107
10.5.2 オーバーレイとキャプチャ	113
10.5.3 詳細設定	113
10.6 人数のカウント.....	114
10.6.1 人数のカウントルールを設定.....	114
10.7 道路交通	116
10.7.1 車両検出の設定	116

10.7.2 混合交通検出ルール設定	119
10.7.3 オーバーレイとキャプチャ	121
10.7.4 ブロックリストと許可リストのインポートまたはエクスポート	123
10.7.5 高度なパラメーター設定	124
10.8 AIオープンプラットフォーム	124
10.8.1 AIオープンプラットフォームの設定	124
10.8.2 ルールを設定	125
第11章 EPTZ	129
11.1 パトロール	129
11.2 自動追跡	129
付録A. FAQ	131

第1章 概要

1.1 設定手順

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

一般的な設定プロセス

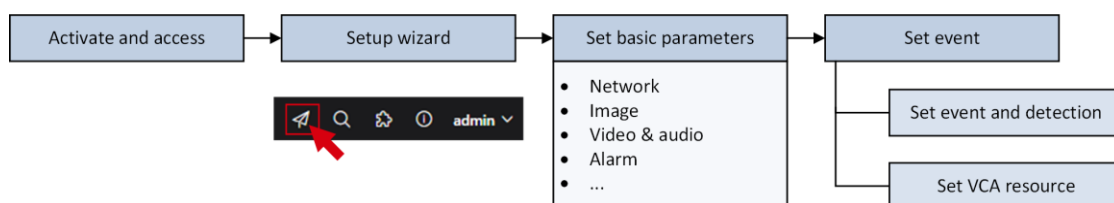


図1-1 一般的な設定プロセス

- ウェブブラウザでデバイスを起動し、アクセスします。 ネットワーク経由でデバイスにアクセスする際、デバイスを起動するためにログインパスワード（管理者ユーザー用）を設定する必要があります。ウェブブラウザを開き、IPアドレスを入力します。デバイスのデフォルトIPアドレスは192.168.1.64です。
- ウィザードに従うか、ウェブページ上の「」をクリックして、デバイスのパラメータを迅速に設定します。
- ネットワーク、画像、動画、音声、アラームなど、基本的なパラメータを設定します。
- イベントと検出ルールを設定します。基本的なイベントと検出ルールを設定するか、深層学習機能用にVCAリソースを割り当てることができます。

1.2 ファームウェア更新

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

最新のファームウェアパッケージは、公式ウェブサイトまたは現地の技術担当者から入手してください。詳細については、公式ウェブサイトをご覧ください：

<https://www.hikvision.com/en/support/download/firmware/> .

アップグレード設定については、アップグレードを参照してください。

1.3 システム要件

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

ネットワークカメラ ユーザ

オペレーティングシステム Microsoft Windows XP SP1 以降

CPU 2.0 GHz 以上

RAM 1GB 以上

ディスプレイ 1024×768 ピクセル以上の解像度

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

第2章 デバイスのアクティベーションとアクセス

ユーザーアカウントとデータのセキュリティとプライバシーを保護するため、ネットワーク経由でデバイスにアクセスする際は、デバイスをアクティベートするために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情報は、ソフトウェアクライアントのユーザーマニュアルをご参照ください。

2.1 SADP 経由でデバイスをアクティベートする

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

開始前に

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

手順

1. ネットワークケーブルを使用してデバイスをネットワークに接続します。
2. SADP ソフトウェアを実行し、オンラインデバイスを検索します。
3. デバイス一覧から**デバイス状態**を確認し、**非アクティブ**なデバイスを選択します。
4. 新しいパスワードをパスワード欄に入力し、パスワードを確認してください。



注意

製品のセキュリティを強化するため、ご自身で選択した強固なパスワード（大文字、小文字、数字、特殊文字をそれぞれ最低8文字以上含む）を作成することを強くおすすめします。また、特に高セキュリティシステムでは、パスワードを定期的にリセットすることをおすすめします。月次または週次でのパスワードのリセットは、製品の保護をさらに強化します。

5. **OK**をクリックしてください。
デバイス状態が「**アクティブ**」に変わります。
6. **オプション**：デバイスのネットワークパラメーターを「**ネットワークパラメーターの変更**」で変更できます。

2.2 ブラウザ経由でデバイスをアクティブ化します。

ブラウザ経由でデバイスにアクセスし、アクティベートできます。

手順

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

注意

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

3. ブラウザに**192.168.1.64**を入力します。
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強化するため、ご自身で選択した強固なパスワード（8文字以上で、大文字、小文字、数字、特殊文字の少なくとも3つを含む）を設定することを強くおすすめします。また、特に高セキュリティシステムでは、パスワードを定期的に変更することをおすすめします。月次または週次でのパスワード変更は、製品の保護をさらに強化します。

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

2.3 ログイン

ウェブブラウザ経由でデバイスにログインします。

2.3.1 プラグインのインストール

一部のオペレーティングシステムやウェブブラウザでは、デバイスの機能の表示や動作が制限される場合があります。正常な表示と動作を確保するためには、プラグインのインストールまたは特定の設定を完了する必要があります。詳細な制限機能については、実際のデバイスをご確認ください。

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

注意

- このデバイスはWindowsおよびMac OSシステムのみに対応しており、Linuxシステムには対応していません。
- 一部のデバイスでのユーザー体験を向上させるため、より高度なウェブブラウザを使用することをおすすめします。実際のデバイスまたは製品仕様をご確認ください。
- 一部のデバイスモデルでは、Internet Explorerウェブブラウザがサポートされていません。

2.3.2 管理者パスワードの回復

管理パスワードを忘れた場合、アカウントのセキュリティ設定を完了後にログインページで「パスワードを忘れた場合」をクリックしてパスワードをリセットできます。

パスワードをリセットするには、セキュリティ質問またはメールアドレスを設定してくだ

注意

パスワードをリセットする際は、デバイスとPCが同じネットワークセグメントに接続され

ていることを確認してください。

セキュリティ質問

→アカウントのセキュリティはアクティベーション時に設定できます。または、**設定→システム→ユーザー管理→アカウントセキュリティ設定**をクリックし、セキュリティ質問を選択して回答を入力してください。

ブラウザからデバイスにアクセスする際、パスワードを忘れた場合は「パスワードを忘れた」をクリックし、セキュリティ質問に回答することで管理者のパスワードをリセットできます。

メール

→アカウントのセキュリティ設定は、アクティベーション時に設定できます。または、**設定→システム→ユーザー管理**に移動し、**アカウントセキュリティ設定**をクリックし、回復操作時に検証コードを受け取るためのメールアドレスを入力してください。

2.3.3 不正ログインロック

インターネット経由でデバイスにアクセスする際のセキュリティを強化します。

「メンテナンスとセキュリティ」→「→ セキュリティ」→「→ ログイン管理」に移動し、「不正ログインロックを有効にする」をオンにします。不正ログイン試行回数とロック時間は設定可能です。

不正ログイン試行

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

ロック時間

設定時間が経過すると、デバイスはロックを解除します。

第3章 ライブビュー

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

3.1 ライブビューパラメーター

対応する機能はモデルによって異なります。

3.1.1 ライブビューの開始と停止

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

3.1.2 アスペクト比

アスペクト比は、画像の幅と高さの表示比率です。

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

3.1.3 ライブビュー ストリーム タイプ

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

3.1.4 サードパーティプラグインを選択してください。

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

手順

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

3.1.5 照明

💡 をクリックして、イルミネーターをオンまたはオフにします。



注意

レーザーを搭載したデバイスについて：

- ・ 操作中の光源を直視しないでください。目に有害な場合があります。
 - ・ 適切な遮光装置や保護具が用意されていない場合は、安全な距離から点灯するか、光が直接当たらない場所で点灯してください。
 - ・ 装置の組み立て、設置、またはメンテナンスを行う際は、絶対に光を点灯させないでください。または、目保護具を着用してください。
-

3.1.6 ピクセルを数える

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

手順

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

3.1.7 デジタルズームを開始

画像内の任意の領域の詳細情報を確認するのに役立ちます。

手順

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

3.1.8 補助フォーカス

モーター駆動式デバイスで使用されます。デバイスが明確にピントを合わせられない場合、画像の品質を向上させることができます。

ABF対応のデバイスでは、レンズの角度を調整し、フォーカスを合わせ、デバイスのABFボタンをクリックしてください。デバイスが明確にフォーカスします。

「」 をクリックすると、自動的にフォーカスが合います。

注意

- 補助フォーカスでピントが合わない場合は、レンズ初期化を使用し、その後再び補助フォーカスを使用して画像をクリアにできます。
 - 補助フォーカスでデバイスが明確にフォーカスできない場合は、マニュアルフォーカスを使用できます。
-

3.1.9 レンズ初期化

レンズ初期化は、モーター駆動式レンズを搭載したデバイスで利用されます。この機能は、長時間ズームまたはフォーカス操作により画像がぼやける場合に、レンズをリセットします。この機能はモデルによって異なります。

 をクリックしてレンズ初期化を実行します。

3.1.10 レンズパラメーターの調整

PTZは「パン、チルト、ズーム」の略称です。これはデバイスの動作オプションを指します。ライブビューインターフェースでは、方向制御ボタンをクリックしてパン/チルト動作を制御し、ズーム/フォーカス/アイリスボタンをクリックしてレンズ制御を実現できま

注意

- 対応するPTZ機能は、カメラモデルによって異なる場合があります。
 - レンズの動きのみをサポートするデバイスでは、方向ボタンは無効です。
-

方向制御



方向ボタンをクリックして長押しすると、デバイスをパン/チルトできます。

ズーム

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

フォーカス

- クリック  をクリックすると、レンズが近距離に焦点を合わせ、近くの対象物が鮮明になります。
- クリック  をクリックすると、レンズが遠方に焦点を合わせ、遠くの物体が鮮明になります。

アイリス

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

PTZ速度

- ・  をスライドさせて、パン/チルトの動きの速度を調整します。

PTZロック

PTZロックとは、対応するチャンネルのズーム、フォーカス、およびPTZ回転機能を無効化し、PTZ調整によるターゲットの消失を軽減するための機能です。

注

この機能は、特定のデバイスモデルでのみサポートされています。

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

PTRZ調整

PTRZは、パン、チルト、回転、ズームの略称です。これはデバイスの動作オプションを指します。インターフェースでは、コントロールボタンを使用してデバイスの動作を調整できます。例えば、デバイスのパン、チルト、回転、ズームなどです。

注意

この機能は、特定のデバイスモデルでのみサポートされています。

設定に移動し、→ **PTZ** を選択し、→ **PTRZ** を選択します。

コントロールパネル

	方向ボタンをクリックして長押しすると、デバイスをパン/チルトできます。
・  ・ 	ボタンをクリックして長押しすると、回転位置を調整できます。

自動回復

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

注意

- ・ 設定→ PTZ→ PTZ に移動し、セルフテストステータスを確認してください。
- ・ PTZを初期化し、PTZの自己診断を手動で有効にするには、設定 → PTZ → PTZ へ移動し、[自己診断] をクリックします。これにより、PTZが初期化されます。

レンズ調整の詳細な設定については、「[レンズパラメーター調整](#)」を参照してください。

3.1.11 3D位置合わせを実施

3D位置決めは、選択した領域を画像の中心に移動させる操作です。

手順

1.  をクリックして機能を有効にします。
2. ライブ画像内でターゲット領域を選択します。
 - ライブ画像上の任意の点を左クリックすると、その点がライブ画像の中心に移動します。ズームイン/ズームアウトの効果はありません。
 - マウスを右下方向にドラッグしてライブ画像の領域をフレームで囲むと、フレーム内の領域がズームインされ、ライブ画像の中心に移動します。
 - マウスを左上方向にドラッグしてライブ画像の一部をフレームで囲むと、フレーム内の領域がズームアウトされ、ライブ画像の中心に移動します。
3. ボタンを再度クリックして機能をオフにします。

3.2 送信パラメーターを設定します。

ライブビュー画像がネットワーク環境により正常に表示されない場合があります。異なるネットワーク環境では、送信パラメーターを調整することで問題を解決できます。

手順

1. 設定に移動し、→ Local→ Live View Parameters を選択します。
2. 必要な送信パラメーターを設定します。

プロト

コル

TCP

TCPはストリーミングデータの完全な送信とより良い動画品質を保証しますが、リアルタイム送信に影響を与える可能性があります。安定したネットワーク環境に適しています。

UDP

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

マルチキャスト

マルチキャストは、複数のクライアントが存在する場合に適しています。選択前に、それらに対してマルチキャストアドレスを設定する必要があります。



注意

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

HTTP

HTTPは、第三者がデバイスからストリームを取得する必要がある場合に適しています。

再生性能最短遅延

デバイスは、動画の滑らかさよりもリアルタイムの動画画像の取得を優先します。

バランス

デバイスは、リアルタイム動画画像と滑らかさを両立させます。

滑らか

デバイスは、リアルタイムよりも動画の滑らかさを優先します。ネットワーク環境が不良な場合、デバイスは動画の滑らかさを保証できません。これは、滑らかさが有効に設定されていても同様です。

カスタム

フレームレートを手動で設定できます。ネットワーク環境が不良な場合、フレームレートを低下させてスムーズなライブビューを表示できます。ただし、ルール情報が表示されない場合があります。

3. 保存をクリックしてください。

第4章 動画と音声

このセクションでは、動画と音声に関連するパラメーターの設定について説明します。

4.1 動画設定

このセクションでは、ストリームタイプ、動画エンコード、解像度などの動画パラメーターの設定について説明します。

設定ページに移動: **設定→ビデオ/オーディオ→ビデオ**。

4.1.1 ストリームタイプ

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

メインストリーム

このストリームは、デバイスがサポートする最高のストリーム性能を表します。通常、デバイスが対応可能な最高の解像度とフレームレートを提供します。ただし、高い解像度とフレームレートは、通常、より大きなストレージ容量と高い帯域幅要件を必要とします。

サブストリーム

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

その他のストリーム

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

4.1.2 動画タイプ

ストリームに含めるコンテンツ（動画と音声）を選択してください。

動画ストリーム

ストリームには動画コンテンツのみが含まれます。

ビデオ&オーディオ

動画コンテンツと音声コンテンツが複合ストリームに含まれます。

4.1.3 解像度

実際のニーズに応じて動画の解像度を選択してください。高い解像度には、より高い帯域幅とストレージ容量が必要です。

4.1.4 ビットレートタイプと最大ビットレート

定常ビットレート

これは、ストリームが比較的一定のビットレートで圧縮され送信されることを意味します。圧縮速度は速いですが、画像にモザイクが発生する可能性があります。

可変ビットレート

設定された**最大ビットレート**内で、デバイスが自動的にビットレートを調整します。圧縮速度は定常ビットレートよりも遅いですが、複雑なシーンの画質を保証します。

4.1.5 動画品質

ビットレートタイプが可変に設定されている場合、動画品質は設定可能です。実際のニーズに応じて動画品質を選択してください。ただし、高い動画品質にはより高い帯域幅が必要です。

4.1.6 フレームレート

フレームレートは、動画ストリームが更新される頻度を表すもので、フレーム毎秒（fps）で測定されます。

動画ストリームに動きがある場合、高いフレームレートは画像の品質を保つため有利です。ただし、高いフレームレートはより高い帯域幅と大きなストレージ容量を必要とします。

4.1.7 動画エンコード

これは、デバイスが動画エンコードに採用する圧縮規格を指します。



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（MPEG-4 Part 10、Advanced Video Coding）は、圧縮規格です。画像品質を低下させずに、MJPEGやMPEG-4 Part 2よりも圧縮率を向上させ、動画ファイルのサイズを削減します。

H.264+

H.264+は、H.264を基盤とした改良された圧縮符号化技術です。H.264+を有効にすると、最大平均ビットレートに基づいてHDDの消費量を推定できます。H.264と比較して、H.264+はほとんどのシーンで同じ最大ビットレートながら、ストレージを最大50%削減できます。

H.264+を有効にした場合、**最大平均ビットレート**は設定可能です。デバイスはデフォルトで推奨される最大平均ビットレートを表示します。動画の品質が不十分な場合は、パラメーターを高い値に調整できます。最大平均ビットレートは、最大ビットレートを超



はいけません。

H.264+を有効にした場合、**Iフレーム間隔**は設定できません。

H.265

H.265 (High Efficiency Video Coding、HEVC、MPEG-H Part 2) は、動画圧縮規格です。H.264と比較して、同じ解像度、フレームレート、画像品質において、より高い動画圧縮効率を実現します。

H.265+

H.265+は、H.265を基盤とした改良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に基づいてHDDの消費量を推定できます。H.265と比較して、H.265+はほとんどのシーンで同じ最大ビットレートながら、ストレージを最大50%削減できます。

H.265+を有効にした場合、**最大平均ビットレート**は設定可能です。デバイスはデフォルトで推奨される最大平均ビットレートを表示します。動画の品質が十分でない場合は、パラメーターを高い値に調整できます。最大平均ビットレートは、最大ビットレートを



はいけません。

H.265+を有効にした場合、**Iフレーム間隔**は設定できません。

Iフレーム間隔

Iフレーム間隔は、2つのIフレーム間のフレーム数を定義します。

H.264およびH.265では、Iフレーム（またはイントラフレーム）は、他の画像への参照なしで独立してデコード可能な自己完結型のフレームです。Iフレームは他のフレームよりも多くのビットを消費します。したがって、Iフレームが多い動画（つまりIフレーム間隔が短い動画）は、より安定した信頼性の高いデータビットを生成しますが、より多くのストレージスペースを必要とします。

SVC

Scalable Video Coding (SVC) は、H.264またはH.265動画圧縮規格のAnnex G拡張機能の名称です。

SVC標準化の目的は、既存のH.264またはH.265設計と同等の複雑さと再構築品質でデコード可能な1つまたは複数のサブセットビットストリームを含む、高品質な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、より大きなビットストリームからパケットを削除することで生成されます。

SVCは古いハードウェアとの前方互換性を実現します：同じビットストリームは、低解像度のサブセットのみをデコードできる基本ハードウェアで消費可能であり、より高度なハードウェアでは高画質の動画ストリームをデコード可能です。

MPEG4

MPEG-4 (MPEG-4 Part 2) は、Moving Picture Experts Group (MPEG) によって開発された動画圧縮形式です。

MJPEG

Motion JPEG (M-JPEGまたはMJPEG) は、イントラフレーム符号化技術を使用した動画圧縮形式です。MJPEG形式の動画は、個々のJPEG画像として圧縮されます。

プロファイル

この機能は、同じビットレート下で、プロファイルが複雑になるほど画像の品質が向上し、ネットワーク帯域幅の要件も高くなることを意味します。

4.1.8 スムージング

これはストリームの滑らかさを指します。スムージングの値が高いほど、ストリームの滑らかさは向上しますが、動画の品質は満足のいくものではなくなる可能性があります。スムージングの値が低いほど、ストリームの品質は向上しますが、滑らかさが欠ける場合があります。

4.2 オーディオ設定

オーディオエンコードや環境ノイズのフィルタリングなどのオーディオパラメーターを設定する機能です。オーディオ設定ページに移動してください：**設定 → ビデオ/オーディオ → オーディオ**。

注意

この機能は、一部のカメラモデルのみ対応しています。

4.2.1 オーディオエンコード

オーディオのオーディオエンコード圧縮を選択してください。

4.2.2 オーディオ入力

注意

- 必要に応じてオーディオ入力デバイスを接続してください。
 - オーディオ入力の表示は、デバイスモデルによって異なります。
-

LineIn	MP3、シンセサイザー、アクティブピックアップなど、高出力のオーディオ入力デバイスに接続する場合、オーディオ入力を LineIn に設定してください。
MicIn	デバイスがマイクやパッシブピックアップなど、低出力のオーディオ入力デバイスに接続されている場合は、オーディオ入力を MicIn に設定してください。

4.2.3 オーディオ出力

注意

必要に応じてオーディオ出力デバイスを接続してください。

これはデバイスのオーディオ出力の切り替えスイッチです。無効にすると、デバイスのすべてのオーディオ出力が停止します。オーディオ出力の表示は、デバイスのモードによって異なります。

4.2.4 環境ノイズフィルター

OFFまたはONに設定します。この機能が有効になっている場合、環境のノイズを一定程度フィルター処理できます。

4.3 双方向オーディオ

監視画面上で監視センターと対象の間で双方向オーディオ機能を実装するために使用されます。

開始前に

- オーディオ入力デバイス（ピックアップまたはマイク）とオーディオ出力デバイス（スピーカー）がデバイスに正しく接続され、正常に動作していることを確認してください。デバイス接続に関する詳細は、オーディオ入力および出力デバイスの仕様書をご確認ください。
- デバイスに内蔵のマイクとスピーカーが搭載されている場合、双方向オーディオ機能を直接有効にできます。

手順

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

4.4 ROI

ROI（関心領域）エンコーディングは、動画圧縮においてROIと背景情報を区別するのに役立ちます。この技術は、関心領域に更多的エンコードリソースを割り当てることで、ROIの品質を向上させるとともに、背景情報への注目を軽減します。

4.4.1 ROIを設定

ROI（Region of Interest）エンコーディングは、ROIに更多的エンコードリソースを割り当てることで、ROIの品質を向上させます。一方、背景情報はより少ないリソースで処理されます。

開始前に

動画のコーデックタイプを確認してください。ROIは、動画のコーデックタイプがH.264またはH.265の場合にサポートされます。

手順

1. 設定に移動し、**→**を選択します。次に、**Video/Audio**を選択し、**→ ROI**を選択します。
2. 「有効」にチェックを入れます。
3. ストリームタイプを選択します。
4. 地域番号を選択し、をクリックして、ライブビュー上にROI領域を描画します。



調整が必要な固定領域を選択し、マウスをドラッグしてその位置を調整します。

5. 領域名とROIレベルを入力します。
6. 「保存」をクリックします。



ROIレベルが高いほど、検出された領域の画像がより鮮明になります。

7. オプション：他の領域番号を選択し、複数の固定領域を描画する必要がある場合は、上記のステップを繰り返し実行してください。

4.5 ターゲットクロッピングを設定

画像のトリミングを行い、ターゲット領域の画像のみを送信して保存することで、送信帯域幅とストレージを節約できます。

手順

1. 設定に移動し、→、**Video/Audio**、→、**Target Cropping** を選択します。
2. 「有効」にチェックを入れ、ストリームタイプを「**Third Stream**」に設定します。

注意

ターゲットクロッピングを有効にすると、第三ストリームの解像度は設定できません。

3. **クロッピング解像度**を選択してください。
ライブビューに赤いフレームが表示されます。
4. フレームを目的の領域までドラッグします。
5. 「保存」をクリックします。

注意

- ・ターゲットクロッピング機能は一部のモデルのみに対応しており、カメラモデルによって機能内容が異なります。
- ・ターゲットクロッピングを有効にした後、一部の機能が使用できなくなる場合があります。

4.6 ストリームに情報を表示する

オブジェクト（例：人間、車両など）の情報は動画ストリームにマークされます。接続された後方装置またはクライアントソフトウェアで、線越え、侵入などを含むイベントを検出するためのルールを設定できます。

開始前に

この機能はスマートイベントでサポートされています。**VCA** を選択し、スマートイベントを選択して次へをクリックしてスマートイベントを有効にします。

手順

1. 設定に移動し、→ を選択します。**Video/Audio** を選択し、→ を選択します。**Display Info. on Stream** を選択します。
2. デュアル**VCA**を有効にします。
3. 保存をクリックします。

4.7 表示設定

画像の機能を調整するためのパラメーター設定を提供します。設定 → 画像 → 表示設定 へ移動してくだ

さい。

デフォルトをクリックして設定を元に戻します。

4.7.1 シーンモード

異なるインストール環境向けに事前に定義された複数の画像パラメーターセットが用意されています。実際のインストール環境に応じてシーンを選択することで、表示設定を迅速に設定できます。

画像調整

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

露出設定

露出は、絞り、シャッター速度、および感度の組み合わせで制御されます。露出パラメーターを設定することで、画像の効果を調整できます。

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

フォーカス

フォーカスモードを調整するオプションが用意されています。

フォーカス

モード

オート

デバイスはシーンの変化に応じて自動的にフォーカスを調整します。オートモードで十分なフォーカスが得られない場合は、画像内の光源を減らし、フラッシュライトを避けてください。

セミオート

PTZとレンズのズーム後に一度フォーカスを調整します。画像がクリアな場合、シーンが変化してもフォーカスは変更されません。

マニュアル

ライブビュー画面で手動でフォーカスを調整できます。

昼/夜切り替え

昼夜切替機能により、昼間モードと夜間モードでカラー画像と白黒画像を表示できます。切替モードは設定可能です。

昼

画像は常にカラー表示です。

夜

画像は白黒またはカラー表示となり、夜間でもクリアなライブビュー画像を確保するため、補助照明が有効になります。



注意

補助照明とカラー画像に対応するデバイスモデルは一部に限られます。

自動

カメラは、環境の光条件に応じて昼モードと夜モードを切り替えます。

スケジュール切り替え

開始時間と終了時間を設定して、デイモードの期間を定義します。

アラーム入力でトリガーされます

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

ビデオによってトリガーされます

カメラは環境の光条件に応じてデイモードとナイトモードを切り替えます。このモードは、デバイスが道路交通と車両検出をサポートする場合に適用されます。



注意

- 日/夜切り替え機能はモデルによって異なります。
 - スマート補助光をオンにすると、より良い画像効果を得ることができます。補助光の設定については、[補助光設定](#)を参照してください。
-

補光設定

補助ライトを設定し、実際のデバイスを参照して関連するパラメーターを確認してください。

スマートサプリメントライト

スマートサプリメントライトは、サプリメントライトがオンの時に露出過多を回避します。

補光ライトモード

デバイスが補助光に対応している場合、補助光モードを選択できます。

赤外線サプリメントライト

赤外線ライトが有効になっています。

白色ライト

白色光が有効です。

混合光

赤外線光と白色光の両方が有効です。

スマート

特定のスマートイベントまたはモーション検出を有効にした後、このモードを選択すると、夜間状態ではデフォルトの補助光モードは赤外線補助光モードになります。アラームがトリガーされると、白色光が有効になり、デバイスがターゲットを捕捉します。アラームが終了すると、補助光モードは赤外線補助光モードに切り替わります。

この機能は、赤外線と白色光、または赤外線と白色光のハイブリッド補助光を搭載したデバイスモデルのみが対応しています。

オフ

補助照明はオフです。



注意

補助光モードは、デバイスモデルによって異なる場合があります。

明るさ調整モード オート

明るさ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、値を設定して明るさを調整できます。

BLC

強い逆光下で被写体に焦点を合わせると、被写体が暗すぎてはっきり見えなくなります。BLC（逆光補正）は、被写体への光を補正し、被写体をはっきり見えるようにします。BLCモードをカスタムに設定すると、ライブビュー画像に赤い四角形を描画し、その領域をBLC領域として指定できます。

WDR

WDR（ワイドダイナミックレンジ）機能は、強い明暗差のある環境でもカメラがクリアな画像を提供するように支援します。

視野内に非常に明るい領域と非常に暗い領域が同時に存在する場合、WDR機能を有効にし、レベルを設定できます。WDRは画像全体の明るさを自動的に調整し、詳細がより鮮明なクリアな画像を提供します。



注意

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



図4-1 WDR

HLC

画像の明るい部分が過露出になり、暗い部分が露出不足になった場合、HLC（ハイライト圧縮）機能を有効にすることで、明るい部分を弱め、暗い部分を明るくし、全体の明るさのバランスを調整できます。

ホワイトバランス

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



図4-2 ホワイトバランス

DNR

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

標準

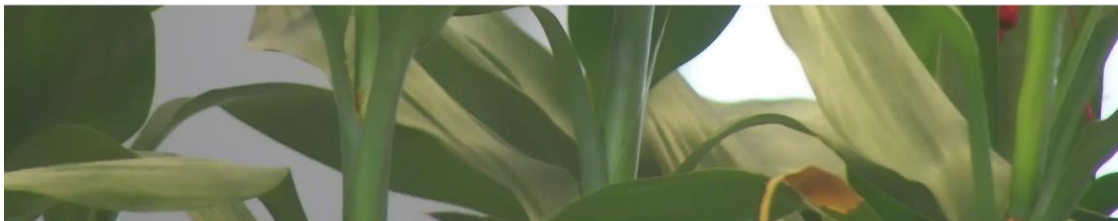
DNR レベルを設定してノイズ低減の度合いを調整します。レベルが高いほど、低減の度合いが強くなります。

エキスパート

スペースDNRとタイムDNRの両方のDNRレベルを設定し、ノイズ低減の程度を調整します。レベルが高いほど、ノイズ低減の程度が強くなります。



DNR Off



DNR On

図4-3 DNR

デフォグ

環境が霧がかかっており、画像がぼやけている場合にデフォグ機能を有効にできます。これにより、微細な詳細を強調し、画像がよりクリアに表示されます。



Defog Off



Defog On

図4-4 デフォグ

EIS

ジッター補償技術を使用して、動画画像の安定性を向上させます。

グレースケール

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

ミラー

ライブビュー画像が実際のシーンと逆になっている場合、この機能は画像を正常に表示するのに役立ちます。

必要に応じてミラーモードを選択してください。

注意

この機能を有効にすると、動画の録画が一時的に中断されます。

回転

この機能を有効にすると、ライブビューが反時計回りに90°回転します。例えば、1280 × 720は720 × 1280に回転します。

この機能を有効にすると、垂直方向の監視範囲が変更される場合があります。

注意

この機能は、特定の設定下で利用可能です。

レンズ歪み補正

モーター駆動レンズを搭載したデバイスでは、画像が多少歪んで表示される場合があります。この機能を有効にすると、歪みを補正できます。

注意

- この機能は、モーター駆動レンズを搭載した特定のデバイスでのみサポートされています。
 - この機能を有効にすると、画像の端が失われます。
-

4.7.2 画像パラメーター切り替え

デバイスは、設定された時間間隔で画像パラメーターを自動的に切り替えます。

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

スケジュール切り替えを設定

指定した時間帯に自動的にリンクされたシーンモードに切り替えます。

手順

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



注意

リンクされたシーンの設定については、シーンモードを参照してください。

3. 保存をクリックします。

4.7.3 ビデオ標準

ビデオ規格は、ビデオカードまたはビデオ表示装置がサポートする色数と解像度を定義する機能です。最も一般的に使用されるビデオ規格はNTSCとPALです。NTSCでは、1秒間に30フレームが送信されます。各フレームは525本の個別の走査線で構成されています。PALでは、1秒間に25フレームが送信されます。各フレームは625本の個別のスキャンラインで構成されています。お住まいの国または地域のビデオシステムに応じて、適切なビデオ信号規格を選択してください。

4.7.4 ローカルビデオ出力

デバイスにBNC、CVBS、HDMI、SDIなどのビデオ出力インターフェースが搭載されている場合、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できます。

出力モードをON/OFFで選択して出力を制御します。

4.8 OSD

OSD（画面表示）情報（デバイス名、日時、フォント、色、動画ストリームに表示されるテキストオーバーレイなど）をカスタマイズできます。

OSD設定ページに移動：**設定→画像→OSD設定**。対応するパラメーターを設定し、**保存**をクリックして適用します。

文字セット

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

表示

カメラ名、日付、曜日、およびそれらの表示形式を設定します。

フォーマット設定

OSDパラメーターを設定します。表示モード、OSDサイズ、フォントカラー、および配置など。

テキストオーバーレイ

画像にカスタムオーバーレイテキストを設定します。

4.9 プライバシーマスクを設定します

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

手順

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

4.10 画像の重ね合わせ

ライブビューにカスタマイズした画像をオーバーレイします。

開始前に

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

手順

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

第5章 動画の録画と画像のキャプチャ

このセクションでは、動画クリップとスナップショットの撮影、再生、および撮影済みファイルのダウンロードに関する操作について説明します。

5.1 ストレージ設定

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

5.1.1 メモリカード

メモリカードの容量、空き容量、状態、種類、およびプロパティを確認できます。メモリカードの暗号化機能をサポートしており、データセキュリティを確保できます。

新しいまたは暗号化されていないメモリカードを設定する

開始前に

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

手順

1. 設定→ストレージ→ストレージ管理→HDD管理を選択します。
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場合は、まずメモリカードをアンロックする必要があります。詳細については「[メモリカードの状態を確認する](#)」を参照してください。

3. 「フォーマット」をクリックして、メモリカードを初期化してください。
メモリカードのステータスが「未初期化」から「正常」に変わると、メモリカードは使用可能になります。
4. オプション：メモリカードを暗号化します。
 - 1) 「暗号化フォーマット」をクリックします。
 - 2) 暗号化パスワードを設定します。
 - 3) 「OK」をクリックします。

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



注意

暗号化パスワードを適切に管理してください。暗号化パスワードを忘れた場合、復元できません。

5. オプション：メモリカードのクォータを設定します。必要に応じて、異なるコンテンツの保存割合をパーセンテージで入力してください。

6. 保存をクリックしてください。

暗号化メモ리카ードの設定

開始前に

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

手順

1. 設定に移動し、→ ストレージ → ストレージ管理 → HDD 管理 を選択します。
2. メモ리카ードを選択します。



注意

アンロックボタンが表示される場合は、まずメモ리카ードをアンロックする必要があります。詳細については「メモ리카ードの状態を確認する」を参照してください。

3. 暗号化パスワードを確認します。
 - 1) パリティをクリックします。
 - 2) 暗号化パスワードを入力してください。
 - 3) OKをクリックしてください。

暗号化ステータスが「暗号化済み」になると、メモ리카ードが使用可能になります。



注意

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

4. オプション：メモ리카ードのクォータを定義します。必要に応じて、異なるコンテンツの保存割合をパーセンテージで入力してください。
5. 保存をクリックしてください。

メモ리카ードの状態を検出

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

開始前に

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

手順

1. 設定に移動し、→ ストレージ → ストレージ管理 → メモ리카ード検出 を選択します。
2. 「ステータス検出」をクリックして、メモ리카ードの残存寿命と健康状態を確認します。
残存寿命

残りの寿命のパーセンテージが表示されます。メモ리카ードの寿命は、容量やビットレートなどの要因に影響を受ける場合があります。残りの寿命が不足している場合は、メモ리카ードを交換する必要があります。

健康状態

メモ리카ードの状態で、その状態を表示します。**Arming Schedule**（武装スケジュール）と**Linkage Method**（リンク方法）を設定した際に、健康状態が「良好」以外の場合、



通知が表示されます。

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

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

- ロックを追加
 - a. ロックスイッチをオンに設定します。
 - b. パスワードを入力してください。
 - c. 「保存」をクリックしてください。
- ロック解除
 - ・メモ리카ードをロックしたデバイスで使用する場合、ロック解除は自動的に行われ、ユーザーによるロック解除の手順は不要です。
 - ・ロックされたメモ리카ードを別のデバイスで使用する場合、**HDD管理画面**から手動でロックを解除できます。メモ리카ードを選択し、「**ロック解除**」をクリックします。正しいパスワードを入力してロックを解除してください。
- ロックを解除する
 - a. ロックスイッチをOFFに設定します。
 - b. パスワード設定でパスワードを入力します。
 - c. 「保存」をクリックします。



注意

- ・ **R/W** ロックを設定できるのは管理者ユーザーのみです。
- ・ メモ리카ードはロックが解除されている場合のみ読み書き可能です。
- ・ メモ리카ードにロックを追加するデバイスを工場設定に復元した場合、**HDD管理画面**からメモ리카ードのロックを解除できます。

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、「アラームスケジュールとリンク方法の設定」セクションを参照してください。

5. 保存をクリックします。

5.1.2 FTPを設定します。

イベントまたはタイマーによるスナップショットタスクでキャプチャされた画像を保存するためのFTPサーバーを設定できます。

開始前に

まず、FTPサーバーのアドレスを取得してください。

手順

1. 設定に移動→ イベント→ アラーム設定→ FTP .

2. FTP設定を構成します。

サーバーアドレスとポート

FTP サーバーのアドレスと対応するポート。

ユーザー名とパスワード

FTP ユーザーは画像のアップロード権限が必要です。

FTP サーバーが匿名ユーザーによる画像アップロードをサポートしている場合、**匿名ユーザー**

にチェックを付けることで、アップロード時にデバイス情報を非表示にできます。

ディレクトリ構造

FTPサーバー内のスナップショットの保存パスです。

3. オプション: 「画像のアップロード」にチェックを付けると、スナップショットをFTPサーバーにアップロードできるようになります。

画像保存間隔

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

画像名

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

4. オプション: 自動ネットワーク更新を有効にするにチェックを付けます。



「リンク方法」で「FTP/メモ리카ード/NASへのアップロード」を選択し、「自動ネットワーク補充を有効にする」を同時に有効にする必要があります。

5. テストをクリックしてFTPサーバーを確認してください。

6. 「保存」をクリックしてください。

5.1.3 NASを設定

ネットワークサーバーをネットワークドライブとして設定し、記録ファイルやキャプチャした画像などを保存します。

開始前に

まず、ネットワークディスクのIPアドレスを取得してください。

手順

1. NASの設定ページに移動します: 設定→ ストレージ→ ストレージ管理→ Net HDD .

2. 「追加」をクリックします。

3. マウントタイプを設定します。

マウントタイプ

オペレーティングシステムに応じてファイルシステムプロトコルを選択します。

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

4. サーバーアドレスとファイルパスを設定してください。

サーバーアドレス

ネットワークディスクのIPアドレス。

ファイルパス

ネットワークディスクのファイルの保存パスです。

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

6. [OK] をクリックして、Net HDD の追加手順を完了します。

7. オプション: Net HDD を設定します。

編集 「」をクリックしてパラメーター設定を編集します。

削除 ネット HDD を削除します。

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

8. 保存をクリックします。

5.1.4 eMMC保護

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



注意

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

設定に移動し、→ システム→ システム設定→ システム サービスを選択して設定を行います。

eMMC (Embedded Multimedia Card) は、組み込み型の非揮発性メモリシステムです。このデバイスでキャプチャされた画像や動画を保存することができます。

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

5.1.5 クラウドストレージの設定

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

手順



注意

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

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

プロトコルバージョン	クラウドビデオマネージャーのプロトコルバージョン。
サーバー IP	クラウドビデオマネージャーのIPアドレスです。IPv4アドレスに対応しています。
サービスポート	クラウドビデオマネージャーのポート番号。デフォルトのポートを使用することをおすすめします。
アクセスキー	クラウド動画マネージャーにログインするためのキーです。
シークレットキー	クラウドビデオマネージャーに保存されたデータを暗号化するためのキーです。
ユーザー名とパスワード	クラウドビデオマネージャーのユーザー名とパスワード。
画像ストレージプールID	クラウド動画マネージャー内の画像ストレージ領域のIDです。ストレージプールIDとストレージ領域IDが一致していることを確認してください。

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

5.2 ビデオ録画

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

5.2.1 自動録画

この機能は、設定された時間帯に動画を自動的に録画します。

開始前に

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

手順

1. 設定に移動し、[→] > [Storage] > [→] > [Schedule Settings] > [→] > [Record Schedule] を選択します。
 2. 「有効」にチェックを入れます。
-

3. 記録タイプを選択します。

注意

記録タイプはモデルによって異なります。

連続

動画はスケジュールに従って継続的に録画されます。

モーション

モーション検出が有効で、トリガー録画が連携方法として選択されている場合、対象物の動きが録画されます。

アラーム

アラーム入力 that 有効で、リンク方法として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後に動画が録画されます。

モーション | アラーム

モーションが検出された場合、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場合、動画が記録されます。

モーション & アラーム

動画は、外部アラーム入力デバイスからアラーム信号を受信し、かつ動作が検出された場合にのみ記録されます。

イベント

設定されたイベントが検出された際に動画が記録されます。

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

上書き

上書きを有効にすると、ストレージ容量が満杯になった際に動画記録を上書きします。そうでない場合、カメラは新しい動画を記録できません。

事前録画

スケジュールされた時間前に録画する期間を設定します。

後録画

スケジュールされた時間後に録画を停止するまでの時間設定。

ストリームの種類

録画するストリームの種類を選択してください。

注

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

録画の有効期限

録画は、有効期限を過ぎると削除されます。有効期限は設定可能です。注意：録画が削除されると、復元できません。

6. 保存をクリックしてください。

5.2.2 手動で録画

手順

1. 設定に移動し、→ **Local** を選択します。
2. 録画した動画ファイルの動画サイズと**保存先**を設定します。
3. 「**保存**」をクリックします。
4. ライブビューインターフェースで「」をクリックして録画を開始します。「」をクリックして録画を停止します。

次にやるべきこと

録画した動画ファイルを表示します。

設定に移動し、→ **Local**を選択し、**動画保存パス**をクリックして保存パスを開き、ファイルを確認します。

5.2.3 動画の再生とダウンロード

ローカルストレージまたはネットワークストレージに保存された動画を検索、再生、クリップ、ダウンロードできます。

手順

1. 再生→ **Video** を選択します。
2. 検索条件を設定し、**[検索]**をクリックします。
一致した動画ファイルがタイミングバーに表示されます。
3. クリ  ク をクリックして動画ファイルを再生します。
 - クリ  ク をクリックして動画ファイルを全画面で再生します。**ESC**キーを押して全画面表示を終了します。
 - クリック すべてのチャンネルの動画再生を停止します。
4. オプション: 「」をクリックして動画ファイルをクリップします。再度「」をクリックして動画ファイルのクリップを停止します



設定に移動し、→ **Local**→ **Clip Saving Path** を選択し、クリップした動画ファイルの保存パスを確認または変更します。

5. オプション:  再生インターフェースでファイルをダウンロードします。



設定に移動し、→ **Local**→ **Downloaded File Saving Path** を選択し、ダウンロードした動画ファイルの保存パスを確認または変更します。

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撮影し、設定された保存先に保存できます。スナップショットを表示したりダウンロードしたりできます。

5.3.1 自動撮影

この機能は、設定された時間間隔で自動的に画像を撮影します。

開始前に

イベントトリガーによる撮影が必要な場合は、イベント設定で関連する連携方法を設定する必要があります。イベント設定については、「イベントとアラーム」を参照してください。

手順

1. 設定に移動し、→ ストレージ→ スケジュール設定→ 画像キャプチャ を選択します。
2. キャプチャスケジュールを設定します。スケジュール時間の設定については、「アラーム設定」の「スケジュール設定」を参照してください。

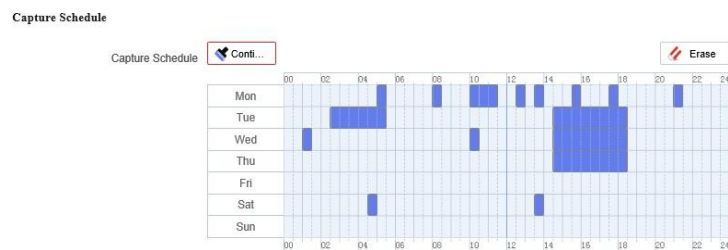


図5-1 キャプチャ スケジュールを設定

3. キャプチャの種類を設定します。

スケジュール

設定された時間間隔で画像をキャプチャします。

イベントトリガー

イベントが発生した際に画像をキャプチャします。

4. フォーマット、解像度、品質、間隔、およびキャプチャ数を設定します。

注意

キャプチャした写真の解像度は、キャプチャした写真ストリームの解像度と同じです。
詳細設定でストリームタイプを選択できます。

5. 保存をクリックします。

5.3.2 手動で撮影

手順

1. 設定に移動し、→ Local を選択します。

2. スナップショットのイメージ形式と保存先を設定します。

JPEG

この形式の画像サイズは比較的小さいため、ネットワーク送信に適しています。

BMP

画像は高品質で圧縮されます。

3. 保存をクリックします。
4. ライブビューまたは再生ウィンドウの近くにある「」をクリックして、手動で画像をキャプチャします。

5.3.3 画像の表示とダウンロード

ローカルストレージまたはネットワークストレージに保存された画像を検索結果から表示し、ダウンロードできます。

手順

1. 再生に移動し、→ 画像を選択します。
2. 検索条件を設定し、検索をクリックします。
一致した画像がファイル一覧に表示されます。
3. 画像をダウンロードします。
 - 画像を選択し、ダウンロードをクリックしてダウンロードします。
 - 「このページをダウンロード」をクリックして、このページの写真をダウンロードします。
 - 「すべてダウンロード」をクリックして、すべての画像をダウンロードします。



注意

設定に移動し、→ **Local** → **Playback Capture Saving Path** を選択し、再生時にキャプチャした画像の保存パスを確認または変更できます。

第6章 イベントとアラーム

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

6.1 モーション検出の設定

検出領域内の移動物を検出し、連携アクションをトリガーします。

手順

1. 設定に移動→イベント→イベントと検出→モーション検出。
2. 「有効」にチェックを入れます。
3. オプション：画像内の移動する対象を緑色で表示するには、該当項目をハイライトします。
 - 1) 「モーション用の動的分析を有効にする」にチェックを入れます。
 - 2) 設定に移動し、→ **Local** を選択します。
 - 3) ルールを有効に設定します。
4. 設定でモードを選択し、ルール領域とルールパラメーターを設定します。
 - 通常モードに関する情報は、通常モードを参照してください。
 - エキスパートモードに関する情報は、エキスパートモードを参照してください。
5. 武装スケジュールとリンク方法を設定します。武装スケジュールの設定に関する情報は、武装スケジュールの設定を参照してください。リンク方法に関する情報は、リンク方法の設定を参照してください。
6. 保存をクリックします。

6.1.1 エキスパートモード

日中の動作検出パラメーターと夜間の動作検出パラメーターを、実際のニーズに応じて設定できます。

手順

1. 設定画面で「エキスパートモード」を選択します。
2. エキスパートモードのパラメーターを設定します。

スケジュールされた画

像設定をオフにします。

画像切り替えは無効です。

自動切り替え

システムは環境に応じて自動的に昼夜モードを切り替えます。昼間はカラー画像を表示し、夜間は白黒画像を表示します。

スケジュール切り替え

システムはスケジュールに従って昼夜モードを切り替えます。設定された時間帯には昼モードに切り替わり、その他の時間帯には夜モードに切り替わります。

感度

感度の値が高いほど、動作検出の感度が高くなります。スケジュールされた画像設定が有効になっている場合、昼と夜の感度を個別に設定できます。

3. **領域**を選択し、をクリックします。ライブ画像上でマウスをクリックしてドラッグし、マウスを離して1つの領域の描画を完了します。



図6-1 ルールを設定

4. をクリックして、すべての領域をクリアします。
5. 「保存」をクリックします。
6. オプション：複数の領域を設定するには、上記のステップを繰り返し実行します。

6.1.2 通常モード

デバイスのデフォルト設定に従って、モーション検出パラメーターを設定できます。

手順

1. 設定で「通常モード」を選択してください。
2. 通常モードの**感度**を設定します。感度の値が高いほど、動作検出の感度が高くなります。感度を**0**に設定すると、動作検出と動的分析は機能しません。
3. **検出対象**を設定します。人間と車両が選択可能です。検出対象が選択されていない場合、検出されたすべての対象（人間と車両を含む）が報告されます。この機能は、指定した対象タイプ（人間と車両）によるアラームのトリガーを可能にします。

注意

この機能は、特定のデバイスモデルおよび設定条件下でのみ利用可能です。実際の設定をご確認ください。

4. クリック  . ライブ画像上でマウスをクリックしてドラッグし、その後マウスを右クリックして1つの領域の描画を完了します。
5. オプション :  をクリックして、すべての領域をクリアします。
6. オプション : 上記のステップを繰り返し、複数の領域のパラメーターを設定できます。

6.2 動画改ざんアラームを設定

設定した領域が覆われて正常に監視できなくなった場合、アラームがトリガーされ、デバイスが特定のアラーム対応アクションを実行します。

手順

1. 設定に移動し、→、Event、→、Event and Detection、→、Video Tampering の順に選択します。
2. 「有効」にチェックを入れます。
3. 感度を設定します。値が高いほど、検出対象領域を容易に検出できます。
4. 「」をクリックし、ライブビューでマウスをドラッグして領域を指定します。

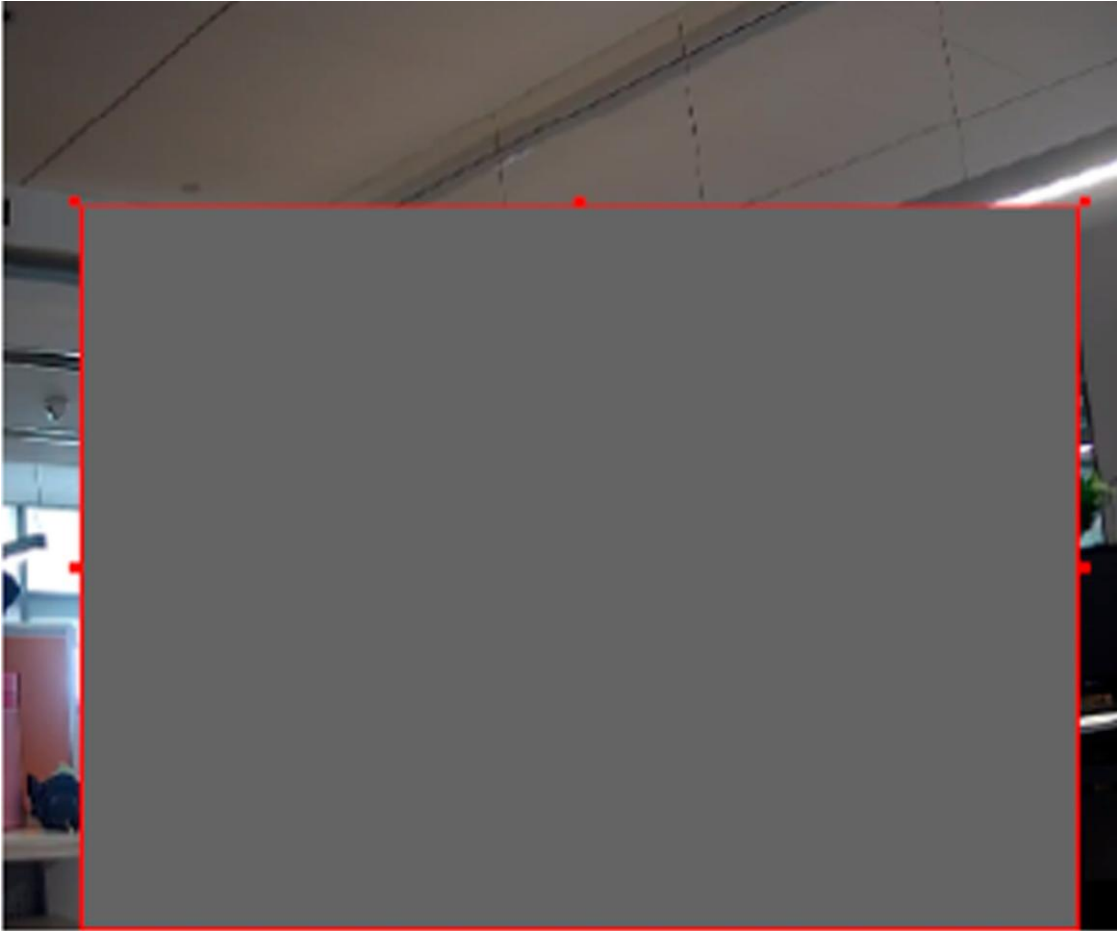


図6-2 動画改ざん領域の設定

5. オプション:  をクリックして、描画したすべての領域を削除します。
6. スケジュール設定については「[**Set Arming Schedule**](#)」を参照してください。リンク方法の設定については「[**Linkage Method SeFngs**](#)」を参照してください。
7. 「保存」をクリックします。

6.3 アラーム入力の設定

外部デバイスからのアラーム信号が、現在のデバイスの対応する動作をトリガーします。

開始前に

注意事項

この機能は、特定のモデルでのみサポートされています。

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

手順

1. 設定に移動し、→、Event、→、Event and Detection、→、Alarm Input を選択します。
2. アラーム入力番号を選択し、[] をクリックしてアラーム入力を設定します。
3. アラームの種類をドロップダウンリストから選択してください。アラーム名を編集してください。
4. アラーム入力処理を有効にするにチェックを入れます。
5. スケジュール設定は「アラームスケジュール設定」を参照してください。リンク 方法 の設定は「リンク方法設定」を参照してください。
6. 「コピー先」をクリックして、設定を他のアラーム入力チャンネルにコピーします。
7. 「保存」をクリックします。

6.4 例外アラームを設定します。

ネットワーク接続の切断などの例外が発生した場合、デバイスが対応するアクションを実行します。

手順

1. →→設定に移動し、イベント>例外>例外イベントと検出>→を選択します。
2. 例外の種類を選択し

ます。HDD 満杯

HDDのストレージが満杯です。

HDDエラー

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

IPアドレスの衝突

現在のデバイスのIPアドレスがネットワーク内の他のデバイスと同一です。

不正なログイン

ユーザー名またはパスワードが正しくないため、ログインできません。

3. リンク設定方法については、リンク設定方法のセクションを参照してください。
4. 保存をクリックしてください。

6.5 動画品質診断を設定してください。

デバイスの動画品質が異常で、アラーム連携が設定されている場合、アラームが自動的にトリガーされます。

手順

1. 設定に移動し、→イベント→イベントと検出→ビデオ品質診断を選択します。

2. 診断タイプを選択します。
3. 対応するパラメーターを設定します。
アラーム検出間隔

例外を検出する時間間隔。

感度

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

アラーム遅延時間

デバイスは、アラームが設定された回数に達するとアラームを送信します。

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



注意

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

6.6 オーディオ例外検出を設定します。

音声異常検出機能は、シーン内の異常な音（例えば、音量の急激な増加/減少など）を検出し、それに応じて特定のアクションを実行できます。

手順

1. 設定に移動し、→ イベント → イベントと検出 → オーディオ異常検出を選択します。
2. 1つまたは複数のオーディオ異常検出タイプを選択します。

オーディオ損失検出

オーディオトラックの突然の喪失を検出します。

音量急上昇検出

音の強度が急激に増加したのを検出します。感度と音の強度閾値は設定可能です。



- 感度が低いほど、検出をトリガーする変化の大きさが大きくなる必要があります。
- 音強度閾値は、検出のための音強度の基準値を指します。環境内の平均音強度を設定することを推奨します。環境音が大きいほど、値を高く設定する必要があります。実際の環境に応じて調整可能です。

音圧の急激な低下検出

音圧の急激な低下を検出します。感度は設定可能です。

3. スケジュール設定は「アラーム スケジュール設定」を参照してください。連携方法の設定は「連携方法設定」を参照してください。
4. 保存をクリックします。

注意

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

6.7 ボケ検出の設定

レンズのピント外れによるぼやけた画像を検出できます。検出された場合、デバイスは連動した動作を実行します。

手順

1. 設定に移動し、→ イベント、→ イベント、検出、→ **Defocus Detection**を選択します。
 2. 「有効」にチェックを入れます。
 3. 感度を設定します。値が高いほど、ボケた画像がアラームをトリガーしやすくなります。実際の環境に応じて値を調整できます。
 4. リンク方法の設定については、リンク方法設定を参照してください。
 5. 保存をクリックします。
-

注

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

6.8 シーン変更検出の設定

シーン変更検出機能は、シーンの変更を検出します。アラームがトリガーされた際に、特定のアクションを実行できます。

手順

1. 設定に移動し、→ イベント、→ イベントと検出、→ シーン変更検出を選択します。
 2. 「有効」をクリックします。
 3. 感度を設定します。値が高いほど、シーンの変化を検出する感度が高くなります。ただし、検出精度が低下します。
 4. スケジュール設定については「アラームスケジュール設定」を参照してください。連携方法の設定については「連携方法設定」を参照してください。
 5. 保存をクリックします。
-

注意

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

第7章 アーミングスケジュールとアラームリンク

武装スケジュールは、デバイスが特定のタスクを実行するカスタマイズされた時間枠です。アラーム連携は、スケジュールされた時間中に検出された特定のイベントまたはターゲットに対する応答です。

7.1 武装スケジュールを設定する

デバイスタスクの有効時間を設定します。

手順

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

注意

- 各セルは30分を表します。
 - 描画した時間範囲にマウスを合わせると、具体的な時間範囲が表示され、開始時間と終了時間を微調整できます。
 - 1日につき最大8つの期間を設定できます。
4. 「消去」をクリックし、時間バーをドラッグして選択した有効な時間をクリアします。
 5. OKをクリックして設定を保存します。

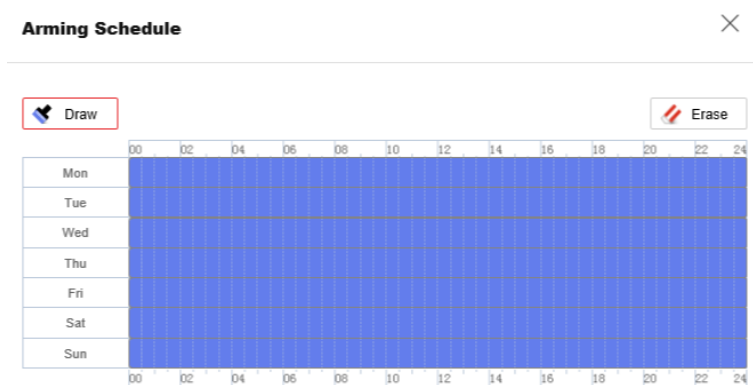


図7-1 アーミング スケジュール設定

7.2 リンク方法の設定

イベントまたはアラームが発生した際にリンク機能を有効にできます。

7.2.1 アラーム出力トリガー

デバイスがアラーム出力デバイスに接続されており、アラーム出力番号が設定されている場合、アラームがトリガーされると、デバイスは接続されたアラーム出力デバイスにアラーム情報を送信します。

手順

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

自動アラーム 設定に関する詳細情報は、自動アラームを参照してください。

手動アラーム 設定に関する情報は、手動アラームを参照してください。

手動アラーム

手動でアラーム出力をトリガーできます。

開始前に

アラーム出力デバイスがデバイスに接続されていることを確認してください。

手順

1. 外部アラーム装置に接続されたアラームインターフェースに応じて、アラーム出力番号を選択してください。アラームパラメーターを設定するには、[

アラーム名

アラーム出力に任意の名前を付けます。

2. 手動アラームをクリックして、手動アラーム出力を有効にします。
3. オプション：手動アラームを無効にするには、**Clear Alarm** をクリックします。

自動アラーム

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

開始前に

アラーム出力デバイスがデバイスに接続されていることを確認してください。

手順

1. 外部アラーム装置に接続されたアラームインターフェースに応じて、アラーム出力番号を選択してください。アラームパラメーターを設定するには、[

アラーム名

アラーム出力に任意の名前を指定します。

遅延

アラームが発生した後、アラーム出力が継続する時間です。

2. アラームのスケジュールを設定します。設定の詳細については、「アラームスケジュールを設定」を参照してください。
3. オプション：[コピー先]をクリックして、パラメーターを他のアラーム出力チャンネルにコピーします。
4. 「保存」をクリックします。

7.2.2 FTP/NAS/メモリカードへのアップロード

FTP/NAS/メモリカードへのアップロードを有効化し設定した場合、アラームが発生すると、デバイスはアラーム情報をFTPサーバー、ネットワーク接続ストレージ、およびメモリカードに送信します。

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

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

7.2.3 メール送信

「メール送信」にチェックを付けると、アラームイベントが検出された際に、指定されたアドレスにアラーム情報を含むメールが送信されます。

メール設定については、「メールの設定」を参照してください。

メールの設定

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

開始前に

メール機能を使用する前に、DNSサーバーを設定してください。設定画面で「→」→「Network」→「→」→「Network Settings」→「TCP/IP」を選択し、DNS設定を行ってください。

手順

1. メール設定ページに移動します：設定 → イベント → アラーム設定 → メール。
2. メールパラメーターを設定します。
 - 1) 送信者のメール情報を入力します。送信者アドレス、SMTPサーバー、およびSMTPポートを入力します。
 - 2) オプション: メールサーバーが認証を必要とする場合、[認証]をチェックし、ユーザー名とパスワードを入力してサーバーにログインしてください。
 - 3) メールの暗号化を設定します。
 - TLSを選択し、STARTTLSを無効にすると、メールはTLSで暗号化されて送信され

ます。SMTPポートは465に設定する必要があります。

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

注意

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

- 4) **オプション**：アラーム画像付きの通知を受け取りたい場合は、「**添付画像**」にチェックを入れてください。通知メールには、イベントに関する一定数のアラーム画像が添付され、画像の撮影間隔は設定可能です。

注意

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

- 5) 受信者の情報（受信者の名前と住所）を入力してください。
6) 「**テスト**」をクリックして、機能が正しく設定されているか確認してください。

3. 「**保存**」をクリックしてください。

7.2.4 監視センターへの通知

「**監視センターに通知**」にチェックを付けると、アラームイベントが検出された際にアラーム情報が監視センターにアップロードされます。

7.2.5 トリガー記録

トリガー記録を確認し、デバイスは検出されたアラームイベントに関する動画を記録します。記録設定については、「**動画記録と画像キャプチャ**」を参照してください。

7.2.6 フラッシュライト

フラッシュライトを有効にし、フラッシュライトアラーム出力を設定すると、アラームイベントが検出された際にライトが点滅します。

フラッシュアラームライト出力の設定

イベントが発生した際に、デバイスのフラッシュライトをアラームとして点滅させることができます。

手順

1. 設定に移動し、→ **イベント**、→ **アラーム設定**、→ **フラッシュアラームライト出力**を選択します。
2. 点滅時間と点滅頻度を設定します。点滅時間

アラームが発生した際に点滅が継続する時間。

点滅頻度

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

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



一部のデバイスモデルのみが機能に対応しています。

7.2.7 音声警告

音声警告を有効にし、音声アラーム出力を設定すると、デバイス内蔵のスピーカーまたは接続された外部スピーカーから、アラームが発生した際に警告音が再生されます。

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



この機能は、特定のカメラモデルでのみサポートされています。

聴覚アラーム出力の設定

デバイスが検出領域内でターゲットを検出した場合、警告として聴覚アラームがトリガーされます。

手順

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



この機能は、特定のデバイスモデルでのみサポートされています。

7.2.8 アラームサーバー

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

アラームサーバーの設定

手順

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



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

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

第8章 ネットワーク設定

8.1 TCP/IP

ネットワーク経由でデバイス进行操作する前に、TCP/IP設定を適切に構成する必要があります。IPv4とIPv6の両方がサポートされています。両バージョンは互いに干渉することなく同時に構成可能です。

設定→ネットワーク→ネットワーク設定→TCP/IPを選択し、パラメーター設定を行います。

NIC タイプ

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

IPv4

IPv4には2つのモードが利用可能です。

DHCP

DHCPを有効にすると、デバイスはネットワークからIPv4パラメーターを自動的に取得します。この機能有効化後、デバイスのIPアドレスが変更されます。デバイスのIPアドレスはSADPを使用して取得できます。



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

手動

デバイスのIPv4パラメーターを手動で設定できます。IPv4アドレス、IPv4サブネットマスク、および

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

IPv6

3つのIPv6モードが利用可能です。

ルート広告

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



ルート広告モードは、デバイスが接続されているルーターのサポートが必要です。

DHCP

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

手動

IPv6アドレス、IPv6サブネット、IPv6デフォルトゲートウェイを入力してください。必要な情報はネットワーク管理者にお問い合わせください。

MTU

MTUは「最大伝送単位」の略称です。これは、単一のネットワーク層トランザクションで送信可能な最大のプロトコルデータ単位のサイズを指します。

MTUの有効な値の範囲は1280から1500です。

DNS

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

ドメイン名設定

「動的ドメイン名の有効化」をオンにし、「ドメイン名登録」に入力します。デバイスは、ローカルエリアネットワーク内での管理を容易にするため、登録ドメイン名の下に登録されます。



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

8.2 ドメイン名でのデバイスへのアクセス

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

デバイスのDDNSサービスはHTTPSのみをサポートしています。

開始前に

DDNSサーバーへの登録は、デバイスのDDNS設定を行う前に必要です。

手順

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

DynDNS

ダイナミック DNS サーバーはドメイン名解決に使用されます。

NO-IP

NO-IP サーバーはドメイン名解決に使用されます。

4. ドメイン名情報を入力し、**保存**をクリックします。
5. デバイスのポートを確認し、ポートマッピングを完了してください。ポートマッピングの設定については、「**ポートマッピング**」を参照してください。
6. デバイスにアクセスしてください。

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

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

8.3 PPPoEダイヤルアップ接続経由でデバイスにアクセスする

このデバイスはPPPoE自動ダイヤルアップ機能に対応しています。デバイスがモデムに接続されると、ADSLダイヤルアップ経由でパブリックIPアドレスを取得します。デバイスのPPPoEパラメーターを設定する必要があります。

手順

1. 設定→ネットワーク→ネットワーク設定→PPPoEを選択します。
2. 「有効」にチェックを入れます。
3. PPPoEパラメーターを設定します。

動的IP

ダイヤルアップ接続が成功すると、WANの動的IPアドレスが表示されます。

ユーザー名

ダイヤルアップネットワークへの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へのアクセス用のパスワード。

確認

ダイヤルアップパスワードをもう一度入力してください。

4. 保存をクリックしてください。
5. デバイスにアクセスしてください。

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

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



取得したIPアドレスはPPPoE経由で動的に割り当てられるため、カメラを再起動するとIPアドレスが常に変更されます。動的IPの不便さを解消するには、DDNSプロバイダー（例：DynDns.com）からドメイン名を取得する必要があります。詳細情報は「ドメイン名経由でのデバイスへのアクセス」を参照してください。

8.4 SNMP

SNMP（Simple Network Management Protocol）を設定することで、ネットワーク管理においてデバイス情報を取得できます。

開始前に

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

手順

1. 設定→ ネットワーク→ ネットワーク設定→ **SNMP** へ移動します。
2. **SNMPv1**、**SNMP v2c**、または**SNMPv3**の有効化を確認します。

注意

選択するSNMPバージョンは、SNMPソフトウェアのバージョンと一致する必要があります。

また、必要なセキュリティレベルに応じて異なるバージョンを使用する必要があります。SNMP v1はセキュリティが不十分であり、SNMP v2はアクセスにパスワードが必要です。SNMP v3は暗号化を提供し、第3バージョンを使用する場合、HTTPSプロトコルを有効にする必要があります。

-
3. SNMP設定を構成します。
 4. 保存をクリックします。

8.5 IEEE 802.1Xを設定します。

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

設定に移動し、→、**Network**、→、**Network Settings**、→、**802.1X** の順に選択し、機能を有効にします。

ルーターの情報に応じてプロトコルとバージョンを選択してください。サーバーのユーザー名とパスワードが必要です。

注意

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

8.6 QoSを設定

QoS（Quality of Service）は、データ送信の優先順位を設定することで、ネットワーク遅延とネットワーク混雑を改善するのに役立ちます。

注意

QoSは、ルーターやスイッチなどのネットワーク機器のサポートが必要です。

手順

1. 設定に移動し、→、**Network**、→、**Network Settings**、→、**QoS** を選択します。
 2. ビデオ/オーディオ **DSCP**、イベント/アラーム **DSCP**、および**管理 DSCP** を設定します。
-

注意

ネットワークはデータ伝送の優先度を識別できます。**DSCP**値が大きいほど優先度が高くなります。設定時にルーターでも同じ値を設定する必要があります。

3. **保存**をクリックします。

8.7 HTTP(S)

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

手順

1. **設定**に移動し、→ **ネットワーク** → **ネットワーク サービス** → **HTTP(S)** を選択します。
2. **HTTP** ポートを入力します。

注

これは、ブラウザがデバイスにアクセスする際に使用するポートを指します。例えば、**HTTP** ポートを **81** に変更した場合、ログインにはブラウザに `http://192.168.1.64:81` と入力する必要があります。

3. **HTTPS** の「有効」にチェックを入れます。

注

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

4. **HTTPS** ポートを入力してください。
5. オプション：**HTTPS** ブラウジングにチェックを付けると、デバイスにアクセスする際は**HTTPS** プロトコルのみを使用します。
6. サーバー証明書を選択します。
7. **Web**認証を設定します。

認証

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

ダイジェストアルゴリズム

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

8. **保存**をクリックしてください。

8.8 マルチキャスト

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

設定に移動し、→、**Network**、→、**Network Service**、→、**Multicast**の順に選択し、マルチキャスト設定を行います。

IPアドレス

マルチキャストホストのアドレスを表します。

8.8.1 マルチキャスト検出

設定に移動し、→、**Network**、→、**Network Settings**、→、**TCP/IP**の順に選択し、この機能を有効にします。

「マルチキャスト検出を有効にする」にチェックを付け、その後、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によってオンラインのネットワークカメラが自動的に検出されます。

8.9 RTSP

RTSP (Real Time Streaming Protocol) は、ストリーミングメディアの制御を目的としたアプリケーション層のプロトコルです。

手順

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

ストリームタイプ

マルチキャストソースとしてのストリームタイプ。

ビデオポート

選択したストリームのビデオポート。

オーディオポート

選択したストリームのオーディオポート。

4. **RTSP認証**を設定します。

認証

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

ダイジェストアルゴリズム

RTSP認証でMD5、SHA256、およびMD5/SHA256暗号化アルゴリズムが使用されます。

MD5を除くダイジェストアルゴリズムを有効にした場合、サードパーティプラットフォームがログインできない可能性があります。

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

5. 保存をクリックしてください。

8.10 SRTPを設定

Secure Real-time Transport Protocol (SRTP) は、ユニキャストおよびマルチキャストアプリケーションにおけるRTPデータに対して暗号化、メッセージ認証、完全性、および再送信攻撃保護を提供するReal-time Transport Protocol (RTP) のインターネットプロトコルです。

手順

1. 設定に移動し、→、**Network**、→、**Network Service**、→、**SRTP** の順に選択します。
2. ポート番号を入力します。
3. マルチキャストパラメーターを設定します。

ストリームタイプ

マルチキャストソースとしてのストリームタイプ。

ビデオ ポート

選択したストリームのビデオポートです。

オーディオポート

選択したストリームのオーディオポート。

4. サーバー証明書を選択してください。
5. 暗号化アルゴリズムを選択します。
6. 保存をクリックします。



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

8.11 Bonjour

Bonjourは、サービス検出、アドレス割り当て、ホスト名解決を含むゼロコンフィグレーション ネットワーキング (zeroconf) の実現技術です。Bonjourは、マルチキャスト ドメイン ネーム システム (mDNS) サービス レコードを使用して、ローカル ネットワーク上のプリンター、他のコンピュータ、およびそれらのデバイスが提供するサービスを検出します。

設定→ ネットワーク→ ネットワークサービス→ **Bonjour** を有効にし、クリック
保存をクリックします。

機能有効化後、デバイスはローカルエリアネットワーク内でサービス情報を送信および受信します。

8.12 WebSocket(s)

Google Chrome 57 以降または Mozilla Firefox 52 以降を使用する場合、WebSocket プロトコルを有効にする必要があります。そうでない場合、ライブビュー、画像キャプチャ、デジタルズームなどの機能は使用できません。

設定に移動し、→、**Network**、→、**Network Service**、→、**WebSocket(s)** の順に選択し、パラメーターを設定した後、
保存をクリックします。

WebSocket

TCPベースのフルデュプレックス通信プロトコルで、HTTPプロトコル経由のプラグイン不要のプレビュー用にポートを指定します。

WebSockets

TCPベースのフルデュプレックス通信プロトコルポート。HTTPSプロトコル経由でプラグイン不要のプレビューが可能です。

8.13 ポートマッピング

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

手順

1. 設定に移動し、→、**Network**、→、**Network Service**、→、**NAT** の順に選択します。
2. ポートマッピングモードを選択します。

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

手動ポートマッピング詳細情報は「[手動ポートマッピングの設定](#)」を参照してください。

3. 保存をクリックします。

8.13.1 自動ポートマッピングの設定

手順

1. UPnP™ を有効にします。カメラのフレンドリー名を選択するか、デフォルトの名前を使用できます。
2. ポートマッピングモードを「自動」に設定します。
3. 「保存」をクリックします。



ルーターのUPnP™機能も同時に有効にしておく必要があります。

8.13.2 手動ポートマッピングを設定

手順

1. 「UPnP™ を有効にする」を選択し、デバイスにわかりやすい名前を付けます。または、デフォルトの名前を使用することもできます。

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

次にやるべきこと

ルーターのポートマッピング設定画面に移動し、ポート番号とIPアドレスをデバイスと同じに設定します。詳細については、ルーターのユーザーマニュアルを参照してください。

8.13.3 ルーターでのポートマッピングの設定

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

手順

1. WAN接続タイプを選択します。
2. ルーターのIPアドレス、サブネットマスク、その他のネットワーク設定を指定します。
3. 「転送」→「→ 仮想サーバー」に移動し、ポート番号とIPアドレスを入力します。
4. 「保存」をクリックします。

例

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

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

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

Virtual Servers

ID	Service Port	IP Address	Protocol	Enable
1	80	192.168.10.23	ALL	☒
2	8000	192.168.10.23	ALL	☒
3	554	192.168.10.23	ALL	☒
4	8200	192.168.10.23	ALL	☒
5	81	192.168.10.24	ALL	☒
6	8001	192.168.10.24	ALL	☒
7	555	192.168.10.24	ALL	☒
8	8201	192.168.10.24	ALL	☒

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

Previous Next Clear All Save

図8-1 ルーターでのポートマッピング

注意

ネットワークカメラのポートは、他のポートと衝突しないようにする必要があります。例えば、ルーターのウェブ管理ポートが80である場合があります。カメラのポートが管理ポートと同じ場合は、ポートを変更してください。

8.14 RTCP

このデバイスは、パケットを順序通りに送信し、信頼性の高い送信メカニズムを提供するため、およびフロー制御や混雑制御のためのサービスを提供するために、RTCP（Real-time Transport Control Protocol）に依存しています。

設定に移動し、→、**Network**、→、**Network Service**、→、**RTCP** の順に選択し、**Enable** をオンに設定して機能を有効化してください。

8.15 ワイヤレスダイヤル

音声、動画、画像のデータは、3G/4G無線ネットワーク経由で転送可能です。

注意

この機能は、特定のデバイスモデルでのみサポートされています。

8.15.1 ワイヤレスダイヤルを設定

内蔵のワイヤレスモジュールは、デバイスからインターネットへのダイヤルアップ接続を提供します。

開始前に

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

手順

1. 設定→ネットワーク→ネットワーク設定→ワイヤレスダイヤルを選択します。
2. 機能の有効化を確認してください。
3. ダイヤルパラメーターに移動し、パラメーターを設定して保存します。
4. ダイヤルプランの背後にある「設定」をクリックします。詳細な情報は「[アラーム設定スケジュールを設定](#)」を参照してください。
5. ダイヤル状態を表示します。

「リフレッシュ」をクリックします。 ダイヤル状態をリフレッシュします。

「切断」をクリックします。 3G/4G ワイヤレスネットワークを切断します。

ダイヤル状態が「接続済み」になると、ダイヤルが正常に完了したことを意味します。

6. ネットワーク内のコンピュータのIPアドレスを使用してデバイ

- 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。
- クライアントアプリケーションにデバイスを追加します。IP/ドメインを選択し、デバイスにアクセスするためのIPアドレスその他のパラメーターを入力します。

7. オプション：4G SIMカードの情報とネットワークキャリア情報を表示できます。



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

8. オプション：手動でデバイスを無線ネットワークに再接続するには、[Re-Camp] をクリックします。デバイスは10秒間機内モードを維持し、その後自動的にネットワークに接続されます。
9. オプション：「Auto Re-Camp」を有効にするには「有効」を選択し、その後「Re-Camp 間隔」を設定します。デバイスは設定された Re-Camp 間隔ごとに自動的に無線ネットワークに再接続します。



この機能は、デバイスモデルによって異なる場合があります。

8.15.2 ワイヤレスエキスパート設定

ワイヤレスエキスパート設定は、デバイスが接続する3G/4Gワイヤレスネットワークの詳細情報を提供し、専門家が潜在的なネットワーク問題をトラブルシューティングするのに役立ちます。

セル無線周波数パラメーター

セル無線周波数パラメーターは、デバイスが接続している現在の無線ネットワーク情報を提供します。

設定に移動し、→ ネットワーク → ネットワーク設定 → ワイヤレスダイヤル → 専門家設定を選択し、セルラジオ周波数パラメーターを表示します。

ネットワーク情報

現在のセルラーネットワーク情報を表示します。リフレッシュをクリックすると、異なるセルの周波数情報を表示できます。

無線周波数変動

デバイスが過去7日間で接続したセルラーネットワークの変動を記録します。レポートのエクスポートをクリックし、暗号化パスワードを設定して確認すると、変動レポートをエクスポートできます。

バンドロック

デバイスがより高速なデータ転送速度を取得するバンドのセットをロックすることで、ネットワーク速度を向上させることができます。

手順

1. 設定に移動し、→、**Network**、→、**Network Settings**、→、**Wireless Dial**、→、**Expert Settings**、→、**Lock Band** を選択します。
2. 「有効」にチェックを入れます。

3. 「追加」をクリックし、バンドを入力します。

注意

- ・ 入力するバンドは、B+ 番号または N+ 番号で指定する必要があります。例：B1 または N1。
- ・ 最大5つのバンドがサポートされています。

4. オプション: 「」をクリックして、選択したバンドを削除します。また、「Clear All」をクリックすると、リスト全体をクリアできます。

ベースバンド パケットのキャプチャ

この機能は、4G モジュールと基地局間の通信障害を特定するために、プロトコル相互作用パケットをキャプチャします。

手順

注意

この機能は、専門家および技術サポートスタッフ専用です。

1. 設定に移動→ネットワーク→ネットワーク設定→ワイヤレスダイヤル→エキスパート設定。
2. 「キャプチャ ベースバンド パケット」の背後にある「設定」をクリックして、設定画面を開きます。
3. 「有効」にチェックを入れてこの機能を有効にします。
4. キャプチャ期間と保存先を設定します。保存先はデバイスの実際の保存方法に依存します。このパス下のキャプチャ済みパケットを削除するには、「このパス下のキャプチャ済みパケットを削除」をクリックします。
5. 「保存」をクリックします。
6. 「パケットのキャプチャを開始」をクリックして、ベースバンド パケットのキャプチャを開始します。
7. オプション: キャプチャを停止するには、「キャプチャの停止」をクリックします。
8. キャプチャが完了したら、「キャプチャしたパケットをエクスポート」をクリックしてレポートを保存します。

速度テスト

手順

1. 設定に移動し、→ネットワーク→ネットワーク設定→ワイヤレスダイヤル→専門家設定を選択します。
2. 速度テストの横にある「設定」をクリックして設定画面を開きます。
3. デフォルトのサーバーを選択するか、サーバーアドレスを入力します。以下の手順に従って、近くのサーバーアドレスを取得できます。

注意

以下の手順に従って、近くのサーバーアドレスを取得できます。

- a. 以下のウェブサイトアクセスして、近くのサーバーのアドレスを取得してください : **<https://www.speedtest.net/speedtest-servers-static.php>** .
 - b. 近くの速度測定ステーションのURLを選択し、コピーして「サーバーアドレス」に貼り付けます。
-

4. 「速度テスト」をクリックしてテストを開始します。

テストが完了すると、速度の詳細を確認できます。また、「速度テスト結果のエクスポート」をクリックすることもできます。

8.16 WLAN AP（アクセスポイント）

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

注意

この機能は、特定のデバイスモデルでのみサポートされています。

8.16.1 WLAN APを設定する

手順

1. 設定に移動し、→、ネットワーク、→、ネットワーク設定、→、**WLAN AP** を選択します。

2. WLAN AP モードを選択します。

オン

機能は有効です。

メンテナンスモード

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

オフ

機能は無効です。

3. 関連するパラメーターを設定してください。

SSID

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

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

必要に応じて定義できます。

セキュリティモード

WPA2-個人用モードがサポートされています。

暗号化方式

AESとTKIPが選択可能です。

パスワード

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



注意

製品のセキュリティを強化するため、ご自身で選択した強固なパスワード（大文字、小文字、数字、特殊文字を含む8文字以上）を設定することを強くおすすめします。また、特に高セキュリティシステムでは、パスワードを定期的に変更することをおすすめします。月次または週次でのパスワード変更は、製品の保護をさらに強化します。

4. 保存をクリックしてください。



注意

機能はデバイスモデルによって異なる場合があります。

次にやるべきこと

スマートフォンまたはPCをAPに接続できます。

8.16.2 AP経由でのデバイスへのアクセス

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

手順

1. 設定に移動し、→ **ネットワーク** → **ネットワーク設定** → **WLAN AP** を有効にします。一部のデバイスモデルでは、デバイスを冷間起動（デバイスのスイッチを**オン**に切り替える）後、WLAN AP 機能が自動的に5分間有効になり、その後、デバイスの4G通信が正常な場合はWLAN AP 機能は、デバイスの4G通信が正常な場合はオフになり、異常な場合はオンのままになります。
2. スマートフォンまたはPCのWLANリストでデバイスのWLAN APを検索します。
3. パスワードを入力し、スマートフォンまたはPCをAPに接続します。



注意

- AP名はSSID（デフォルトは「Hik-シリアル番号」）です。パスワードはデフォルトでシリアル番号です。シリアル番号は、**設定** → **システム** → **システム設定** から取得できます。
→ **基本情報**。
- 一部のデバイスモデルでは、AP名はデバイスのラベルに表示されている「Default SSID」です。

4. ブラウザにIPアドレスを入力してください。



注意

デバイスのAPのデフォルトIPは192.168.8.1です。

結果

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

8.17 トラフィックシェーピング

トラフィックシェーピングは、送信前に動画データパケットを整形し、平滑化するために使用されます。

これにより、ネットワークの混雑による遅延の改善、パケット損失の削減、および動画品質の維持が実現されます。シェーピングレベルは設定可能です。

8.18 データ監視

デバイスが使用するSIMカードデータまたは有線ネットワークデータを表示し管理できます。SIMカードデータはネットワークキャリアが提供するデータサービスです。有線ネットワークデータは通常、4Gルーター経由で提供されます。

手順

1. 設定に移動し、→、**Network**、→、**Network Settings**、→、**Data Monitoring** を選択します。
2. 「有効」にチェックを入れます。
3. データプランに応じて、以下のパラメーターを設定してください。

プランタイプ

日次、月次、または年次から選択できます。

データプラン

使用可能なデータ量を入力し、単位を選択してください。

事前アラーム閾値

使用したデータがデータプランのセットされたパーセンテージに達すると、デバイスがアラームメッセージを送信し、OSDまたはポップアップウィンドウに通知を表示します。

4. 「通常連携」を選択してください。
「メール送信」または「監視センター通知」を選択した場合、使用データが閾値に達すると、デバイスはメールでアラームメッセージを送信するか、監視センターに通知します。
5. 保存をクリックします。



機能はデバイスモデルによって異なります。

8.19 Wi-Fi

Wi-Fiパラメーターを設定して、デバイスを無線ネットワークに接続します。



この機能は、特定のデバイスモデルでのみサポートされています。

8.19.1 デバイスをWi-Fiに接続する

開始前に

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

手順

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



Wi-Fiの安定した使用のため、DHCPの使用は推奨されません。

3. Wi-Fi 設定ページに移動します：設定→ネットワーク→ネットワークサービス→Wi-Fi。
4. パラメーターを設定し、保存します。
 - 1) Wi-Fi機能を有効にします。
 - 2) 「リフレッシュ」をクリックして利用可能な無線ルーターまたはAPを表示して選択するか、手動で追加するには「+」をクリックしてください。
 - 3) SSIDを選択または入力してください。これは、無線ルーターまたはAPのSSIDと一致する必要があります。ネットワークのパラメーターは、Wi-Fiに自動的に表示されます。
 - 4) ネットワークモードを「管理」に選択してください。
 - 5) セキュリティモードを必要に応じて選択し、パラメーターはルーターまたはAPで設定した無線ネットワーク接続のパラメーターと一致させる必要があります。
 - 6) 「保存」をクリックします。

次にやるべきこと

TCP/IP設定ページに移動します：設定→ネットワーク→ネットワーク設定→TCP/IP、そしてクリック

Wlan をクリックし、IPv4 アドレスを確認し、デバイスにログインします。

8.20 ISUPを設定

デバイスがISUPプラットフォーム（旧称Ehome）に登録されると、デバイスにアクセスして管理し、データを送信したり、アラーム情報をパブリックネットワーク経由で転送したりできます。

手順

1. 設定に移動→ネットワーク→プラットフォームアクセス→ISUP .
2. オプション：アクセスセンターを選択します。
3. 「有効」にチェックを入れます。
4. プロトコルバージョンを選択し、関連するパラメーターを入力します。
5. 保存をクリックします。

機能が正しく設定されると、登録状態が「オンライン」に変わります。

8.21 Hik-Connect経由でカメラにアクセスします。

Hik-Connectはモバイルデバイス用のアプリケーションです。このアプリを使用すると、ライブ映像の閲覧、アラーム通知の受信などが行えます。

開始前に

カメラをネットワークケーブルでネットワークに接続してください。

手順

1. 以下の方法のいずれかでHik-Connectアプリケーションをダウンロードしてインストールしてください。
 - <https://appstore.hikvision.com> にアクセスし、お使いのモバイル端末のシステムに対応したアプリケーションをダウンロードしてください。
 - 当社の公式ウェブサイトアクセスし、サポート → Tools → Hikvision App Store を選択します。
 - 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てください。



注意

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

- ・ <https://appstore.hikvision.com/static/help/index.html> にアクセスし、トラブルシューティングを参照してください。
 - ・ <https://appstore.hikvision.com/> にアクセスし、インターフェースの右上にある「インストールヘルプ」をクリックしてトラブルシューティングを参照してください。
-
2. アプリケーションを起動し、Hik-Connectユーザーアカウントに登録してください。
 3. 登録後、ログインしてください。
 4. アプリ内で、右上にある「+」をタップし、カメラのQRコードをスキャンしてカメラを追加します。QRコードはカメラ本体またはパッケージ内のクイックスタートガイドのカバーに表示されています。
 5. 画面の指示に従ってネットワーク接続を設定し、カメラをHik-Connectアカウントに追加してください。
- 詳細な情報は、Hik-Connect アプリのユーザーマニュアルをご参照ください。

8.21.1 カメラでHik-Connectサービスを有効にする

Hik-Connect サービスは、サービスをご利用になる前にカメラで有効にする必要があります。サービスはSADP ソフトウェアまたはウェブブラウザを通

じて有効にできます。

Webブラウザ経由でHik-Connectサービスを有効にする

Webブラウザを使用してHik-Connectサービスを有効にするには、以下の手順に従ってください。

開始前に

サービスを利用するには、まずカメラを有効にする必要があります。

手順

1. ウェブブラウザからカメラにアクセスします。
2. プラットフォームアクセス設定画面を開きます。設定→ネットワーク→プラットフォームアクセス → Hik-Connect。
3. 「有効化」にチェックを入れます。
4. ポップアップウィンドウで「利用規約」と「プライバシーポリシー」をクリックして読みます。
5. カメラの検証コードを作成するか、既存の検証コードを変更します。



注意

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

-
6. 設定を保存してください。

Hik-Connect サービスを SADP ソフトウェア経由で有効にする

このセクションでは、アクティベート済みのカメラのSADP ソフトウェアを使用して Hik-Connect サービスを有効にする方法について説明します。

手順

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



注意

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

-
5. 「利用規約」と「プライバシーポリシー」をクリックして読み、同意してください。
 6. 設定を確認してください。

8.21.2 Hik-Connect の設定

手順

1. 以下の方法のいずれかで Hik-Connect アプリケーションを取得してインストールしてください。
 - お使いのスマートフォンに対応したアプリケーションをダウンロードするには、
<https://appstore.hikvision.com> にアクセスしてください。

- 当社の公式ウェブサイトアクセスし、サポート →→ **Tools** →→ **Hikvision App Store** の順に選択します。
- 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てください。



注意

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

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

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

8.21.3 Hik-Connect にカメラを追加する

手順

1. モバイルデバイスをWi-Fiに接続します。
2. Hik-Connect アプリにログインします。
3. ホーム画面の右上にある「+」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表示されているQRコードをスキャンしてください。

注意

QRコードが欠落しているか、認識できないほどぼやけている場合は、カメラのシリアル番号を入力してカメラを追加することもできます。

-
5. カメラの検証コードを入力してください。

注意

- 必要な検証コードは、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です。
- 検証コードを忘れた場合は、ウェブブラウザからプラットフォームアクセス設定ページで現在の検証コードを確認できます。

-
6. ポップアップ画面の「ネットワークに接続」ボタンをタップしてください。
 7. カメラの機能に応じて「有線接続」または「無線接続」を選択してください。

ワイヤレス接続	スマートフォンが接続しているWi-Fiのパスワードを入力し、「次へ」をタップしてWi-Fi接続プロセスを開始します。（Wi-Fi設定時、カメラをルーターから3メートル以内の範囲に配置してください。）
有線接続	ネットワークケーブルでカメラをルーターに接続し、結果画面で

「接続済
み」をタ
ップしま
す。
をタップ
します。



注意

ルーターは、スマートフォンが接続しているものと同じものを使用してください。

8. 次の画面で「追加」をタップして追加を完了してください。

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

8.22 オープンネットワークビデオインターフェースを設定

Open Network Video Interface プロトコル経由で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できます。

手順

1. 設定 → → Network → → Platform Access → → Open Network Video Interface を選択します。
2. 「有効」を選択してください。
3. 認証モードを選択してください。
 - ダイジェストを選択した場合、デバイスはダイジェスト認証のみをサポートします。
 - 「Digest&ws-username token」を選択した場合、デバイスはダイジェスト認証またはws-username token認証をサポートします。
4. 「追加」をクリックして、Open Network Video Interface ユーザーの構成を設定します。
5. 保存をクリックします。
6. オプション：上記のステップを繰り返し、追加のOpen Network Video Interfaceユーザーを追加します。
7. オプション：ユーザーを管理します。
 - 「」をクリックして、選択したOpen Network Video Interfaceユーザーを削除します。
 - 「」をクリックして、選択したOpen Network Video Interfaceユーザーを編集します。

8.23 SDK サービスを設定する

クライアント ソフトウェアにデバイスを追加するには、SDK サービスまたは Enhanced SDK サービスを有効にする必要があります。

手順

1. 設定に移動し、→、Network、→、Platform Access、→、SDK Service を選択します。
2. SDK サービスのパラメーターを設定します。
 - 1) SDK プロトコルを使用してクライアント ソフトウェアにデバイスを追加するには、[有効] をチェックします。
 - 2) ポート番号を入力します。
3. 拡張 SDK サービスのパラメーターを設定します。
 - 1) 「有効」にチェックを付けて、SDK 経由で 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します。
 - 2) オプション：デバイスがサポートする TLS バージョンを有効にするには、[TLS 設定] をクリックします。詳細については、[**TLS**](#) を参照してください。
 - 3) ポート番号を入力します。

- 4) サーバー証明書を選択して、データ送信のセキュリティを確保します。証明書を追加するには「**証明書管理**」をクリックします。詳細については 「**証明書管理**」 を参照してください。
4. **保存** をクリックします。

第9章 システムとセキュリティ

システムメンテナンス、システム設定、およびセキュリティ管理について説明し、関連するパラメーターの設定方法について解説します。

9.1 システム設定

9.1.1 デバイス情報の表示

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

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

9.1.2 日時

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

手動で時間を同期する

手順

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

NTPサーバーを設定します。

正確で信頼性の高い時刻ソースが必要な場合、NTPサーバーを使用できます。

開始前に

NTPサーバーを設定するか、NTPサーバーの情報を取得してください。

手順

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

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



注意

サーバーアドレスはNTPサーバーのIPアドレスです。

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

衛星で時間を同期します。



注意

この機能は、使用するデバイスによって異なります。

手順

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

DSTを設定

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

手順

1. **設定**に移動し、→**システム**→**システム設定**→**時間設定** を選択します。
2. 「有効」にチェックを入れます。
3. **開始時間**、**終了時間**、および**DSTバイアス**を選択します。
4. **保存**をクリックしてください。

9.1.3 RS-232を設定します。

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

開始前に

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

手順

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

9.1.4 RS-485を設定します。

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

開始前に

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

手順

1. 設定→ システム→ システム設定→ **RS-485** を選択します。
2. RS-485パラメーターを設定します。



デバイスの設定とコンピュータまたは端末の設定をすべて同じに保つ必要があります。

3. 保存をクリックしてください。

9.1.5 ライブビュー接続を設定

リモートライブビュー接続の最大接続数を制御します。

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

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

9.1.6 場所設定

位置情報を表示し、デバイスの現在の経度と緯度をアップロードします。

自動アップロード

「有効」にチェックを入れ、**位置情報アップロード間隔**を設定します。

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

手動設定

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

デバイスは設定された間隔で設定された位置情報をアップロードします。



この機能は、デバイスモデルによって異なる場合があります。

9.1.7 外部デバイス

外部デバイスに対応したデバイス（補助照明、ハウジングのワイパー、LED照明、ヒーターなど）は、ハウジングと組み合わせて使用する場合、ウェブブラウザ経由で制御可能です。外部デバイスはモデルによって異なります。

9.1.8 オープンソースソフトウェアライセンスを表示

画面の右上隅で「」をクリックし、「**Open Source Software Description**」を選択してライセンスをダウンロードできます。ライセンスはエディターで確認できます。

9.1.9 Wiegand



注意

この機能は、特定のカメラモデルでのみサポートされています。

「有効」にチェックを入れ、プロトコルを選択します。デフォルトのプロトコルはSHA-1 26bit です。

有効に設定されている場合、認識された車番は選択されたWiegandプロトコル経由で出力されます。

9.2 ユーザーとアカウント

9.2.1 ユーザーアカウントと権限の設定

管理者は、他のアカウントを追加、変更、または削除し、異なるユーザーレベルに異なる権限を付与できます。



注意

ネットワーク上でデバイスを使用する際のセキュリティを強化するため、アカウントのパスワードを定期的に変更してください。パスワードは3ヶ月ごとに変更することを推奨します。高リスク環境でデバイスを使用する場合、パスワードは毎月または毎週変更することを推奨します。

手順

1. 設定→システム→ユーザー管理→ユーザー管理 へ移動します。
2. 「追加」をクリックします。ユーザー名を入力し、レベルを選択し、パスワードを入力します。必要に応じてユーザーにリモートアクセス権限を付与します。

管理者

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

ユーザー

ユーザーはライブ動画の閲覧、PTZパラメーターの設定、自身のパスワードの変更権限が割り当てられますが、その他の操作権限はありません。

オペレーター

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

変更 ユーザーを選択し、[]をクリックしてパスワードと権限を変更します。

削除 ユーザーを選択し、[]をクリックします。



管理者は最大31つのユーザーアカウントを追加できます。

3. **OK**をクリックします。

9.2.2 同時ログイン

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

設定に移動し、→ **システム** → **ユーザー管理** → **オンラインユーザー** を選択し、**一般**をクリックし、
同時ログインを設定します。

9.2.3 オンラインユーザー

デバイスにログインしているユーザーの情報を表示します。

設定に移動し、→ **システム** → **ユーザー管理** → **オンラインユーザー** を選択して、オンラインユーザーのリストを表示します。

9.3 メンテナンス

9.3.1 再起動

ブラウザからデバイスを再起動できます。

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

9.3.2 アップグレード

開始前に

正しいアップグレードパッケージを取得する必要があります。



注意

プロセス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。

手順

1. → 「メンテナンスとセキュリティ」に移動し、「→ のメンテナンス」を選択し、「アップグレード」をクリックします。
2. アップグレードする方法を選択してください。
ファームウェア アップグレードファイルの正確なパスを特定します。
ファームウェア ディレクトリ アップグレードファイルが格納されているディレクトリを特定します。
3. 「」をクリックしてアップグレードファイルを選択します。
4. 「アップグレード」をクリックします。

9.3.3 復元とデフォルト

復元とデフォルトは、デバイスのパラメーターをデフォルト設定に復元します。

手順

1. 「メンテナンスとセキュリティ」に移動し、→ **Maintenance** → **Backup and Restore** を選択します。
2. 必要に応じて「復元」または「デフォルト」をクリックしてください。

復元 ユーザー情報、IPパラメーター、および動画形式を除くデバイスのパラメーターをデフォルト設定にリセットします。

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



注意

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

9.3.4 設定ファイルのインポートとエクスポート

同じパラメーターを持つ他のデバイスでのバッチ設定を迅速化します。

手順

1. 設定ファイルをエクスポートします。
 - 1) メンテナンスとセキュリティに移動し、→ を選択します。メンテナンス→ を選択し、バックアップと復元→ を選択します。バックアップ。
 - 2) 「エクスポート」をクリックし、暗号化パスワードを入力して現在の設定ファイルをエクスポートします。
 - 3) 設定ファイルをローカルコンピュータに保存するための保存先を設定します。
-

2. 設定ファイルをインポートします。
 - 1) 設定が必要なデバイスにウェブブラウザでアクセスします。
 - 2) メンテナンスとセキュリティに移動し、→メンテナンス→バックアップと復元→リセットを選択します。
 - 3) 「」をクリックして、保存した設定ファイルを選択します。
 - 4) 設定ファイルをエクスポートする際に設定した暗号化パスワードを入力してください。

5) インポートをクリックしてください。

9.3.5 ログの検索と管理

ログは問題の特定とトラブルシューティングに役立ちます。

手順

1. メンテナンスとセキュリティに移動します。→ **Maintenance**→ **Log**。
2. 検索条件を設定します：主要タイプ、サブタイプ、開始時間、終了時間。
3. **検索**をクリックします。
一致したログファイルがログ一覧に表示されます。
4. オプション: ログファイルをコンピュータに保存するには、**エクスポート**をクリックします。

9.3.6 セキュリティ監査ログの検索

デバイスのセキュリティログファイルを検索し分析することで、不正な侵入を特定し、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できます。

手順



この機能は、特定のカメラモデルでのみサポートされています。

1. メンテナンスとセキュリティに移動します。→ **メンテナンス**→ **セキュリティ監査ログ**。
2. ログの種類、開始時間、終了時間を選択します。
3. **検索**をクリックします。
検索条件に一致するログファイルがログ一覧に表示されます。
4. オプション: **エクスポート**をクリックして、ログファイルをコンピュータに保存します。

9.3.7 SSH

Secure Shell (SSH) は、非暗号化ネットワーク上でネットワークサービスを提供するための暗号化ネットワークプロトコルです。

「メンテナンスとセキュリティ」→「→メンテナンス」→「→デバイスデバッグ」に移動し、**SSHの設定**をクリックします。ポート番号を編集できます。**保存**をクリックします。



この機能は慎重に使用してください。この機能を有効にした場合、デバイス内部情報の漏洩リスクが存在します。

9.3.8 診断情報のエクスポート

診断情報には、実行ログ、システム情報、ハードウェア情報が含まれます。

「メンテナンスとセキュリティ」に移動し、→ を選択します。次に「メンテナンス」を選択し、→ を選択します。次に「デバイスデバッグ」を選択し、→ を選択します。次に「診断情報」を選択し、エクスポートをクリックします。ポップアップウィンドウで、必要な診断情報を選択し、エクスポートをクリックしてデバイスの対応する診断情報をエクスポートします。

9.3.9 診断

4Gネットワークに対応したデバイスでは、診断を行うことで、今後のメンテナンスやトラブルシューティングに役立つ通信パケット、デバイスの電源状態、およびネットワーク情報を取得できます。

デバイス パケットのキャプチャ

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

手順

注意

この機能は専門家および技術サポートスタッフ専用です。

1. 「メンテナンスとセキュリティ」→「→メンテナンス」→「→デバイスデバッグ」に移動し、
[デバイスパケットのキャプチャ]をクリックします。
2. 「有効」にチェックを入れてこの機能を有効にします。

Capture Device Packet

After the capture packet function is enabled, recording will stop automatically. Recording will recover after the capture packet function is disabled.

Enable

Capture Duration *

1

min

Save Captured Packet to

EMMC/2

Delete Captured Packet Under This Path

NIC Type

Wired Network

Wireless Dial/PPPoE

IP

0.0.0.0

Port No.

0

Auto Capture

After this function is enabled, the device packet will be captured when wakeup happens.

Packet Capturing Status

Save

Start Capturing Packet

Export Captured Packet

図9-1 キャプチャデバイス パケット

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

注意

- a. 保存パスオプションは、デバイスの実際の保存方法に依存します。
 - b. 「このパス下のキャプチャ済みパケットを削除」をクリックすると、保存されたパケットファイルを削除できます。
5. NIC タイプ、IP、およびポートを設定します。
 6. オプション：自動キャプチャを選択すると、デバイスが起動した際にパケットが自動的にキャプチャされます。
 7. 「保存」をクリックします。
 8. 「パケットのキャプチャを開始」をクリックします。

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

デバイス情報のエクスポート

「メンテナンスとセキュリティ」→「→」→「メンテナンス」→「→」→「Device Debugging」→「→」→「Export Device Info」を選択し、電圧、電流、電力、4Gデータなどのデバイス情報をエクスポートするには「エクスポート」をクリックします。

9.4 セキュリティ

セキュリティパラメーターを設定することで、システムセキュリティを強化できます。

9.4.1 IPアドレスフィルターを設定する

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

IPアドレスはIPv4を指します。

手順

1. メンテナンスとセキュリティに移動します。→セキュリティ→IPアドレスフィルター。
2. 「有効」にチェックを入れます。
3. IPアドレスフィルターの種類を選択します。

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

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

4. IPアドレスフィルターリストを編集します。

追加 リストに新しいIPアドレスまたはIPアドレス範囲を追加します。



リスト内の選択したIPアドレスまたはIPアドレス範囲を編集



します。リスト内の選択したIPアドレスまたはIPアドレス範

囲を削除します。

5. 保存をクリックします。

9.4.2 MACアドレスフィルターを設定

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

手順

1. メンテナンスとセキュリティに移動します。→セキュリティ→MACアドレスフィルター。

2. 「有効」にチェックを入れます。
3. MACアドレスフィルターの種類を選択してください。

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

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

4. MACアドレスフィルターリストを編集します。

追加 リストに新しいMACアドレスを追加します。



リスト内の選択したMACアドレスを編集しま



す。リスト内の選択したMACアドレスを削除
します。

5. 保存をクリックします。

9.4.3 タイムアウト設定の制御

この機能が有効になっている場合、設定されたタイムアウト期間内にウェブブラウザ経由でデバイスに対して操作を行わない（ライブ画像の表示を除く）場合、自動的にログアウトされます。

メンテナンスとセキュリティに移動し、→セキュリティ→ログイン管理→制御タイムアウト設定を選択し、設定を完了します。

9.4.4 証明書管理

サーバー/クライアント証明書およびCA証明書を管理し、証明書が有効期限切れ間近または有効期限切れ/異常な状態になった場合にアラームを送信します。



注意

この機能は、特定のデバイスモデルでのみサポートされています。

サーバー証明書/クライアント証明書



注

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

自己署名証明書を作成してインストールする

手順

1. 「メンテナンスとセキュリティ」に移動し、「→セキュリティ」を選択し、「→証明書管理」を選択します。
2. 「自己署名証明書を作成」をクリックします。
3. 証明書情報を入力します。



注

入力する証明書 ID は既存のものと同一にできません。

4. 「保存」をクリックして証明書を保存し、インストールします。
作成された証明書は、サーバー/クライアント証明書一覧に表示されます。

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

5. オプション: [プロパティ] をクリックして証明書の詳細を確認します。

自己署名証明書をインストールする

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

開始前に

まず、自己署名証明書を作成します。作成とインストールの手順は「自己署名証明書の作成とインストール」を参照してください。

手順

1. 「メンテナンスとセキュリティ」→「→セキュリティ」→「→証明書管理」に移動します。
2. サーバー/クライアント証明書リストから自己署名証明書を選択します。
3. 「証明書リクエストの作成」をクリックします。
4. リクエスト情報を入力します。
5. 「保存」をクリックします。
証明書リクエストの詳細がポップアップウィンドウに表示されます。
6. 要求内容をコピーし、要求ファイルとして保存します。
7. ファイルを信頼できる第三者に送信して署名を取得します。
8. 第三者から返送された証明書を受け取った後、デバイスにインストールします。
 - 1) 「インポート」をクリックします。
 - 2) 証明書IDを入力します。

注意

入力する証明書IDは、既存のものと同一にすることはできません。

-
- 3) クリック  をクリックして証明書ファイルを選択してください。
 - 4) 自己署名証明書を選択します。
 - 5) 保存をクリックします。

インポートした証明書が「サーバー/クライアント証明書」リストに表示されます。

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

9. オプション: プロパティをクリックして証明書の詳細を確認します。

他の認証済み証明書をインストール

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

手順

1. メンテナンスとセキュリティに移動し、→ セキュリティ、→ 証明書管理を選択します。
2. サーバー/クライアント証明書の一覧で「インポート」をクリックします。

3. 証明書 ID を入力します。



入力する証明書 ID は、既存のものと同一にしてはいけません。

4. クリック をクリックして証明書ファイルを選択します。

5. 証明書とキーを選択し、証明書に応じてキーの種類を選択してください。

独立したキー 証明書に独立したキーが含まれている場合は、このオプションを選択してください。

プライベートキーを選択し、プライベートキーのパスワードを入力してください。

PKCS#12

証明書が同じ証明書ファイル内に鍵を含む場合、このオプションを選択し、パスワードを入力してください。

6. 保存をクリックします。

インポートされた証明書は、**サーバー/クライアント**証明書リストに表示されます。

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

CA証明書をインストール

開始前に

事前にCA証明書を用意してください。

手順

1. メンテナンスとセキュリティに移動し、→ **セキュリティ**、→ **証明書管理**を選択します。

2. **CA証明書**の一覧で「インポート」をクリックします。

3. 証明書 ID を入力します。



入力する証明書 ID は既存のものと同一にしてはいけません。

4. クリック をクリックして証明書ファイルを選択します。

5. クリック

インポートした証明書が**CA**証明書リストに表示されます。

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

証明書有効期限アラームを有効にする

手順

1. 証明書有効期限アラームを有効にします。有効にすると、証明書が間もなく有効期限切れになる、または有効期限切れまたは異常が発生した場合、メールまたは監視センターへのカメラリンクが送信されます。

2. 「有効期限前に通知する日数（日）」、「アラーム頻度（日）」、「検出時間（時間）」を設定します。

注意

- 有効期限前のリマインダー日を1に設定した場合、カメラは有効期限の1日前にリマインダーを送信します。1日から30日まで設定可能です。デフォルトのリマインダー日は7日です。
- 有効期限の1日前にリマインダーの日を設定し、検出時間を10:00に設定した場合、証明書が翌日の9:00に有効期限切れになる場合、カメラは最初の日の10:00にリマインダーを表示します。

3. 保存をクリックしてください。

9.4.5 TLS

Transport Layer Security (TLS) プロトコルは、2つ以上の通信するコンピュータアプリケーション間のプライバシーとデータ整合性を主に提供することを目的としています。TLS設定は、HTTP(S)および強化されたSDKサービスに有効です。

メンテナンスとセキュリティに移動し、→セキュリティ、→TLSの順に選択し、希望のTLSプロトコルを有効にします。クリック
保存をクリックします。

注意

この機能は慎重に使用してください。この機能を有効にした場合、デバイス内部情報の漏洩リスクが存在します。

第10章 VCA リソース

VCAリソースは、デバイスがサポートするスマート機能の集合体です。

10.1 Open Platform の設定

HEOP（Hikvision Embedded Open Platform）は、第三者がアプリケーションをインストールし、その機能やサービスを開発・実行できるようにするプラットフォームです。HEOP対応デバイスでは、以下の手順に従ってスマートアプリケーションをインポートして実行できます。

手順

1. **VCA** インターフェースに移動します。

注意

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

- ・各アプリケーションには独自の名前が割り当てられています。
- ・アプリケーションが使用するフラッシュメモリの容量は、デバイスの利用可能なフラッシュメモリ容量よりも小さいです。
- ・アプリケーションのメモリ容量と処理能力は、デバイスの利用可能なメモリ容量と処理能力よりも小さいです。

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

クリック 	アプリケーションを有効または無効にします。
クリック 	アプリケーションを削除してください。
クリック 	ログのエクスポートをクリックしてください。
クリック 	ローカルパスを選択し、アプリケーションパッケージをインポートしてアプリケーションを更新します。
クリック 	メモリの断片化をクリアし、より多くのメモリを解放して、より多くのスマートアプリケーションを実行可能にします。
詳細を表示	アプリケーションを選択し、クリックしてページに詳細を表示します。

10.2 一般設定

スマートアプリケーションに関連する一般的なパラメーターを設定します。

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

カメラ情報

カメラ情報の設定については、[カメラ情報の設定](#)を参照してください。

FTP

FTPの設定については、[「FTPの設定」](#)を参照してください。

メール

メールの設定については、[「メールの設定」](#)を参照してください。

アラーム出力

アラーム出力の設定については、[「自動アラーム」](#)を参照してください。

音鳴りアラーム出力

音声アラーム出力の設定については、[「音声アラーム出力の設定」](#)を参照してください。

アラームサーバー

アラームサーバーの設定については、[アラームサーバー](#)を参照してください。

メタデータ

メタデータの設定については、[「メタデータ」](#)を参照してください。

10.2.1 カメラ情報の設定

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

VCA 設定に移動します。→ **アプリケーション設定に移動します。**→ **一般設定に移動します。**→ **カメラ情報に移動し、デバイス番号とカメラ情報を設定します。**

10.2.2 メタデータ

メタデータは、デバイスがアルゴリズム処理前に収集する raw データです。第三者システムとの統合に頻繁に使用されます。

VCA にアクセスし、→アプリケーションを設定し、→一般設定→メタデータ設定に移動し、希望する機能のメタデータアップロードを有効にします。

注意

この機能は、カメラのモデルによって異なる場合があります。

スマートイベント

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

顔検出

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

10.2.3 AcuSearch

デバイスは、ターゲットを検出後にターゲットのPOS情報をネットワークビデオレコーダーに送信します。これにより、接続されたネットワークビデオレコーダーでの正確かつ迅速な検索を実現します。

開始前に

- AcuSearchに対応した接続されたネットワークビデオレコーダー（NVR）が機能に対応していることを確認してください。
- 機能が有効化されると、**スマートイベント** または **マルチターゲット検出** が有効になっている間は、進行中のスマートアプリケーションが無効になります。
- この機能は特定のモデルでのみサポートされています。実際の表示はモデルによって異なります。

手順

1. デバイスで機能を有効にします。
 2. 接続されたネットワークビデオレコーダーで機能を設定します。
 - 1) ネットワークビデオレコーダーで、選択したチャンネル（設定済みのカメラデバイスを参照）に対してAcuSearch機能を有効にします。
 - 2) ネットワークビデオレコーダーの再生画面でAcuSearchボタンをクリックします。
 - 3) ネットワークビデオレコーダー上でターゲットをクリックして、そのターゲットを含む画像を検索します。
 - 4) 画像をクリックして、その前後の一連の動画を再生します。
-

注意

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

10.3 スマートイベント

注意

- 一部のデバイスモデルでは、機能設定ページを表示するには、まずVCAページでス
-

マートイベント機能を有効にする必要があります。

- 機能はモデルによって異なります。
-

10.3.1 侵入検知の設定

事前に定義された仮想領域内に物体が侵入したり、滞留したりすることを検出します。この状況が発生した場合、デバイスは連携アクションを実行できます。

開始前に

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

手順

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

検出対象

この機能は、指定したターゲットの種類でアラームをトリガーします。検出ターゲットが選択されていない場合、検出されたすべてのターゲットが報告されます。

注意

この機能は、特定のデバイスモデルおよび設定下でのみ利用可能です。実際の設定をご確認ください。

しきい値

しきい値は、対象物が領域内に滞留する時間の閾値を表します。1つの対象物が滞留する時間がしきい値を超えると、アラームがトリガーされます。しきい値の値が大きいほど、アラームのトリガー時間が長くなります。

感度

感度は、許容対象の身体の一部が事前定義された領域に入る割合を表します。感度= $100 - S1/ST \times 100$ 。S1は事前定義された領域を横切る対象の身体の一部を表し、STは対象の身体全体を表します。感度の値が大きいほど、アラームがより簡単にトリガーされます。

ターゲット有効性

有効期間を長く設定すると、必要なターゲットの特徴がより明確になり、アラーム

の精度が向上します。特徴が明確でないターゲットは検出されなくなります。

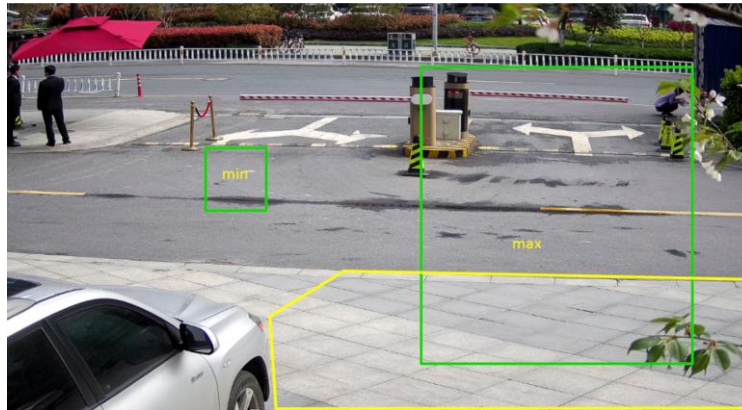


図10-1 ルール設定

5. オプション：上記のステップを繰り返し、複数の領域のパラメーターを設定できます。
6. 武装スケジュール設定については、「武装スケジュール設定」を参照してください。リンク方法設定については、「リンク方法設定」を参照してください。
7. 保存をクリックします。

10.3.2 線越え検出の設定

これは、事前に定義された仮想ラインを横切る物体を検出するために使用されます。検出された場合、デバイスは連動動作を実行できます。

開始前に

- VCA にアクセスし、アプリケーションを選択します。Smart Event を選択し、次へをクリックして機能を有効にします。
- HEOP対応デバイスでは、VCAに移動してSmart Eventをインポートし、有効化します。

手順

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

検出対象

この機能は、指定されたターゲットの種類に基づいてアラームをトリガーします。検

出対象が選択されていない場合、検出されたすべてのターゲットが報告されます。

注意

この機能は、特定のデバイスモデルおよび設定条件下でのみ利用可能です。実際の設定をご確認ください。

方向

これは、対象物が線を超える方向を表します。

A<->B: 線を超える方向が両方からである場合、オブジェクトが検出され、アラームがトリガーされます。

A->B: A側からB側へ設定されたラインを横切る対象物のみが検出可能です。

B->A: B側からA側へ設定された線を越える物体のみが検出されます。

感度

これは、許容可能なターゲットの身体の一部が事前に定義された線を超える割合を表します。感度 = $100 - S1/ST \times 100$ 。S1は、事前に定義された線を超えるターゲットの身体の一部を表します。STは、ターゲットの全体的な身体を表します。感度の値が高いほど、アラームがより簡単にトリガーされます。

ターゲットの有効性

有効期間を長く設定すると、必要なターゲットの特徴がより明確になり、アラームの精度が向上します。特徴が明確でないターゲットは検出されなくなります。

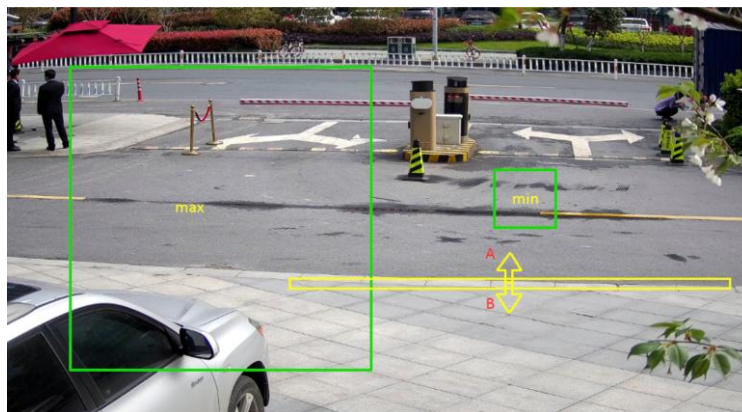


図10-2 ルール設定

5. オプション：上記のステップを繰り返し、複数の領域のパラメーターを設定できます。
6. 武装スケジュール設定については、「武装スケジュール設定」を参照してください。リンク方法設定については、「リンク方法設定」を参照してください。
7. 保存をクリックします。

10.3.3 領域の入口検出を設定

これは、外部から事前に定義された仮想領域に物体が侵入したことを検出するために使用されます。検出された場合、デバイスは連携動作を実行できます。

開始前に

- **VCA** にアクセスし、アプリケーションを選択します。スマートイベントを選択し、次へをクリックして機能を有効にします。
- HEOP対応デバイスを使用する場合、**VCA**に移動し、**Smart Event**をインポートして有効化します。

手順

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

検出対象

この機能は、指定されたターゲットの種類に応じてアラームを発生させます。検出対象が選択されていない場合、検出されたすべてのターゲットが報告されます。

注意

この機能は、特定のデバイスモデルおよび設定下でのみ利用可能です。実際の設定をご確認ください。

感度

これは、許容可能なターゲットの身体部分が事前定義された領域を横切る割合を表します。 $\text{感度} = 100 - S1/ST \times 100$ 。S1は事前定義された領域を横切るターゲットの身体部分を表します。STはターゲットの全体的な身体を表します。感度の値が高いほど、アラームがより容易にトリガーされます。

ターゲット有効性

有効期間を長く設定すると、必要なターゲットの特徴がより明確になり、アラームの精度が向上します。特徴が明確でないターゲットは検出されなくなります。

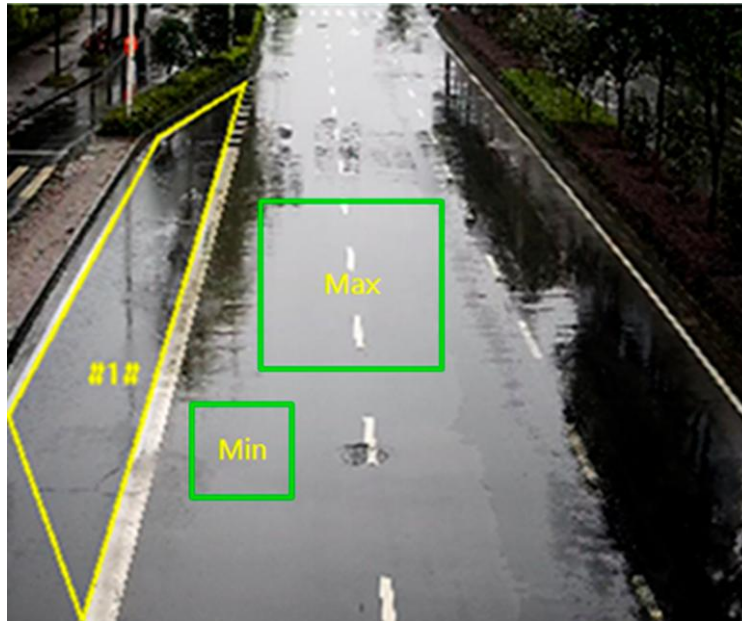


図10-3 ルール設定

5. オプション：上記のステップを繰り返し、複数の領域のパラメーターを設定できます。
6. 武装スケジュール設定については、「武装スケジュール設定」を参照してください。リンク方法設定については、「リンク方法設定」を参照してください。
7. 保存をクリックします。

10.3.4 領域退出検出の設定

これは、事前に定義された仮想領域から物体が退出するのを検出するために使用されます。この状況が発生した場合、デバイスは連携動作を実行できます。

開始前に

- **VCAに移動**し、アプリケーションを選択します。スマートイベントを選択し、次へをクリックして機能を有効にします。
- HEOP対応デバイスでは、**VCAに移動**し、**Smart Event**をインポートして有効化します。

手順

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

小サイズと最大サイズのターゲットを描画します。

3) オプション：  をクリックして、すべての設定領域を削除します。

4. パラメーター

を設定します。

検出対象

この機能は、指定されたターゲットの種類に応じてアラームを発生させます。検出対象が選択されていない場合、検出されたすべてのターゲットが報告されます。

注意

この機能は、特定のデバイスモデルおよび設定下でのみ利用可能です。実際の設定をご確認ください。

感度

これは、許容可能なターゲットの身体部分が事前定義された領域を横切る割合を表します。感度 = $100 - S1/ST \times 100$ 。S1は事前定義された領域を横切るターゲットの身体部分を表し、STはターゲットの全体を表します。感度の値が高いほど、アラームがより簡単にトリガーされます。

ターゲット有効性

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

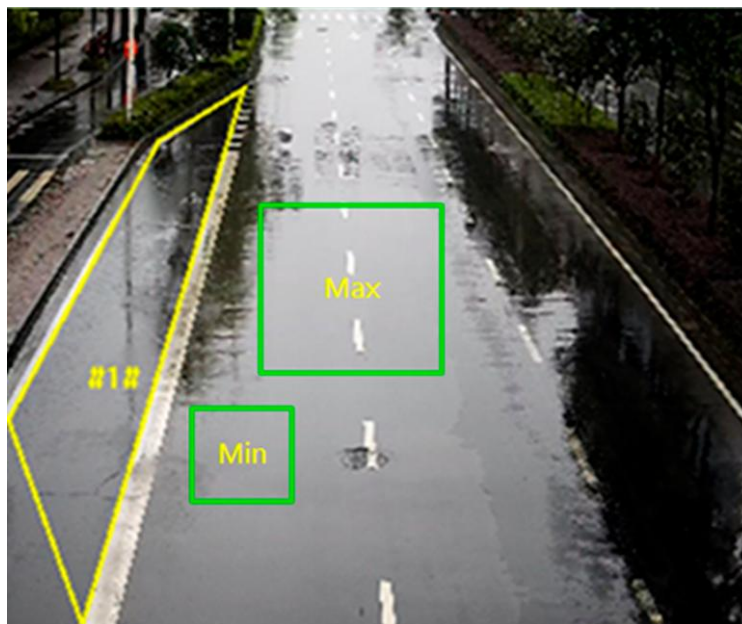


図10-4 ルール設定

5. オプション：上記のステップを繰り返し、複数の領域のパラメーターを設定できます。
6. 武装スケジュール設定については、「武装スケジュール設定」を参照してください。リンク方法設定については、「リンク方法設定」を参照してください。
7. 保存をクリックします。

10.3.5 無人手荷物検出を設定

これは、事前に定義された領域内に残されたオブジェクトを検出するために使用されます。オブジェクトが領域内に残ったまま一定時間経過すると、リンク方法がトリガーされます。

開始前に

- **VCAに移動**し、アプリケーションを選択します。スマートイベントを選択し、次へをクリックして機能を有効にします。
- HEOP対応デバイスでは、**VCAに移動**し、**Smart Event**をインポートして有効化します。

手順

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

感度

感度は、許容可能なターゲットの身体部位のうち、事前定義された領域に入る割合を表します。 $\text{感度} = 100 - S1/ST \times 100$ 。S1は、事前定義された領域を通過するターゲットの身体部位を表します。STは、ターゲットの身体全体を表します。感度の値が高いほど、アラームがより容易にトリガーされます。

閾値

これは、オブジェクトが領域内に残っている時間を表します。オブジェクトが領域から離れても、設定された時間内に領域内に残っている場合、アラームがトリガーされます。

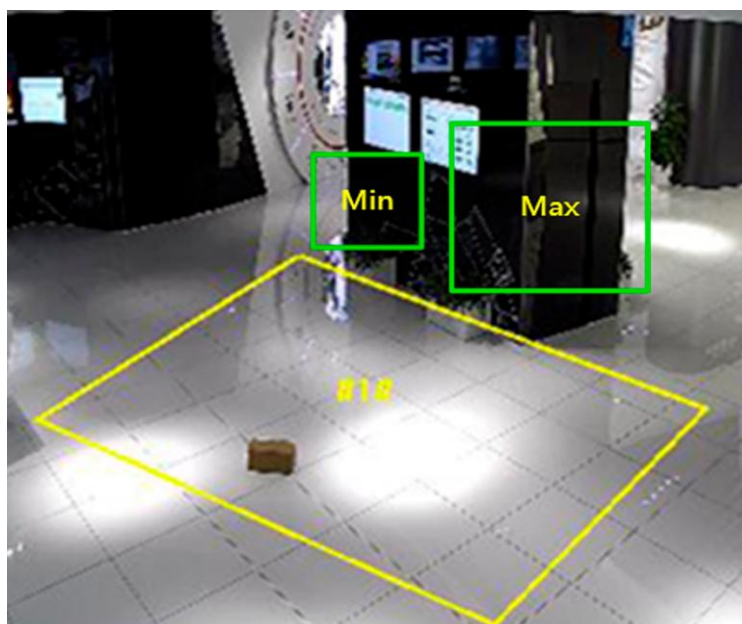


図10-5 ルール設定

5. オプション: 上記の手順を繰り返し行うことで、複数の領域のパラメーターを設定できます。
6. 武装スケジュール設定については、「武装スケジュール設定」を参照してください。リンク方法設定については、「リンク方法設定」を参照してください。
7. 保存をクリックします。



注意

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

10.3.6 オブジェクト除去検出の設定

このシステムは、展示品など事前に定義された検出領域から物体が取り除かれたかどうかを検出します。検出された場合、デバイスは連携動作を実行し、スタッフは財産損失を軽減するための措置を講じることができます。

開始前に

- **VCA** にアクセスし、アプリケーションを選択します。 **Smart Event** を選択し、次へをクリックして機能を有効にします。
- HEOP対応デバイスでは、**VCA**にアクセスして**Smart Event**をインポートし、機能を有効化します。

手順

1. **VCA**に移動します「→」を選択します「**Application**」を選択します「→」を選択します「**Smart Event**」を選択します「→」を選択します「**Object Removal Detection**」を選択します。
2. 「有効」にチェックを入れます。

3. 「追加」をクリックしてルールを追加し、検出領域を設定します。
 - 1) 検出領域を描画します。☒をクリックし、ライブビューをクリックして頂点を指定し、検出領域の境界を描画します。右クリックで描画を完了します。

- 2) ターゲットの最小サイズと最大サイズを設定して検出精度を向上させます。最大サイズと最小サイズの間にあるサイズのターゲットのみが検出されます。「」をクリックし、「」をクリックし、ライブビュー内でマウスをドラッグして最小サイズと最大サイズのターゲットを描画します。
- 3) オプション:  をクリックして、すべての設定領域を削除します。
4. パラメーターを設定します。

感度

感度は、許容可能なターゲットの身体部位のうち、事前定義された領域に入る割合を表します。感度 = $100 - S1/ST \times 100$ 。S1は、事前定義された領域を通過するターゲットの身体部位を表します。STは、ターゲットの身体全体を表します。感度の値が高いほど、アラームがより容易にトリガーされます。

閾値

領域から対象物が除去された後の時間閾値。値を10に設定すると、対象物が領域から消えてから10秒後にアラームがトリガーされます。

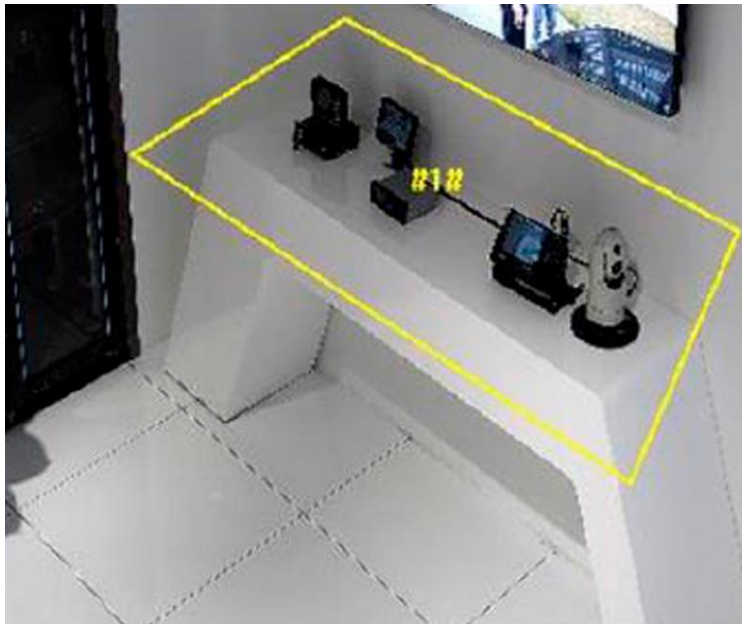


図10-6 ルール設定

5. オプション: 上記のステップを繰り返し、複数の領域のパラメーターを設定できます。
6. 武装スケジュール設定については、**[武装スケジュールを設定]**を参照してください。リンク方法の設定については、**[リンク方法の設定]**を参照してください。
7. 保存をクリックします。

注意

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

10.3.7 滞留検出の設定

事前に定義された領域内にターゲットが滞留しているかどうかを検出します。ターゲットが設定された領域内で滞留する時間が設定された閾値に達した場合、デバイスは連携動作を実行できます。

開始前に

- **VCA** にアクセスし、アプリケーションを選択します。 **Smart Event** を選択し、次へをクリックして機能を有効にします。
- HEOP対応デバイスでは、**VCAに移動してSmart Eventをインポートし**、機能を有効にします。

手順

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

しきい値は、オブジェクトが領域内に滞留する時間のしきい値を表します。1つのオブジェクトが領域内に滞留する時間がしきい値を超えると、アラームがトリガーされます。しきい値の値が大きいほど、アラームのトリガー時間が長くなります。

感度

感度は、許容対象の身体の一部が事前定義された領域に入る割合を表します。感度= $100 - S1/ST \times 100$ 。S1は事前定義された領域を横切る対象の身体の一部を表し、STは対象の身体全体を表します。感度の値が大きいほど、アラームがより簡単にトリガーされます。



図10-7 ルール設定

5. オプション：上記のステップを繰り返し、複数の領域のパラメーターを設定できます。
6. 武装スケジュール設定については、「武装スケジュール設定」を参照してください。リンク方法設定については、「リンク方法設定」を参照してください。
7. 保存をクリックしてください。

注意

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

10.3.8 人集まり検出の設定

事前に定義された領域内の人密度を検出します。人密度が設定されたパーセンテージを超えると、デバイスは連携アクションを実行できます。

開始前に

- VCA にアクセスし、アプリケーションを選択します。Smart Event を選択し、次へをクリックして機能を有効にします。
- HEOP対応デバイスでは、VCAにアクセスしてSmart Eventをインポートし、機能を有効化します。

手順

1. VCAに移動し、→を選択します。アプリケーション→を選択し、Smart Event→を選択し、People Gathering Detectionを選択します。
2. 「有効」にチェックを入れます。
3. 「追加」をクリックしてルールを追加し、検出領域を設定します。
 - 1) 検出領域を描画します。をクリックし、ライブビューをクリックして頂点を指定し、検出領域の境界を描画します。右クリックで描画を完了します。

2) オプション :  をクリックして、すべての設定領域を削除します。

4. ルールを設定します。

パーセンテージ

これは、事前定義された領域内の人々の割合を表します。ライブビュー内の人々の割合が設定値を超えると、デバイスがアラームをトリガーします。

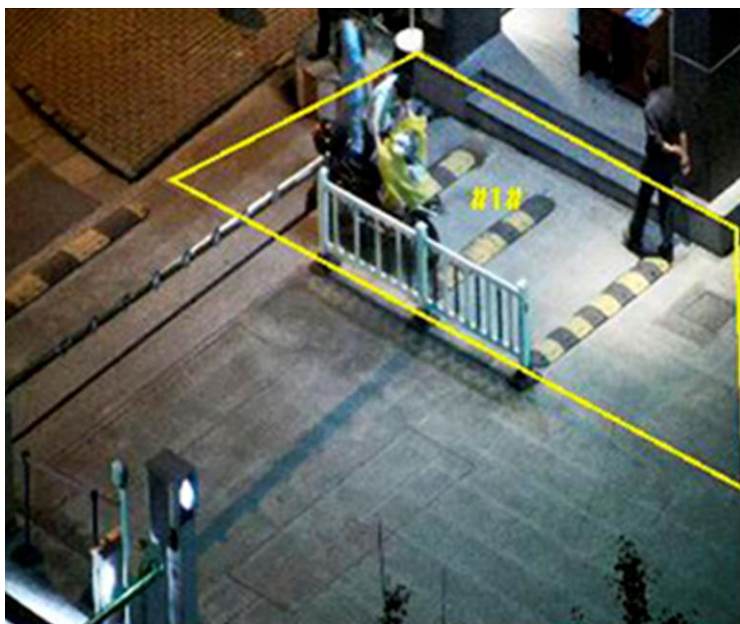


図10-8 ルール設定

5. オプション：上記のステップを繰り返し、複数の領域のパラメーターを設定できます。
6. 武装スケジュール設定については、「武装スケジュール設定」を参照してください。リンク方法設定については、「リンク方法設定」を参照してください。
7. 保存をクリックしてください。



注意

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

10.3.9 高速移動検出の設定

事前に定義された領域内で高速で移動するターゲットが検出された場合、デバイスは連動動作を実行し、アラームをトリガーします。

開始前に

- **VCA** にアクセスし、アプリケーションを選択します。 **Smart Event** を選択し、次へをクリックして機能を有効にします。
- HEOP対応デバイスでは、**VCA**に移動して**Smart Event**をインポートし、機能を有効にします。

手順

1. **VCA**に移動し、→ を選択します。アプリケーション→ を選択し、**Smart Event**→ を選択し、

Fast Moving Detectionを選択します。

2. 「有効」にチェックを入れます。

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

感度

感度は、許容可能なターゲットの身体部位のうち、事前定義された領域に入る割合を表します。感度 = $100 - S1/ST \times 100$ 。S1は、事前定義された領域を横切るターゲットの身体部位を表します。STは、ターゲットの身体全体を表します。感度の値が高いほど、アラームがより容易にトリガーされます。



図10-9 ルール設定

5. オプション：上記のステップを繰り返し、複数の領域のパラメーターを設定できます。
6. 武装スケジュール設定については、「武装スケジュール設定」を参照してください。リンク方法設定については、「リンク方法設定」を参照してください。
7. 保存をクリックします。

注

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

10.3.10 駐車検知機能

事前に定義されたエリア内で駐車違反を検出します。駐車時間が設定された閾値を超えると、デバイスは連携動作を実行できます。高速道路や一方通行道路での使用に適しています。

開始前に

- **VCA** にアクセスし、アプリケーションを選択します。スマートイベントを選択し、次へをクリックして機能を有効にします。
- HEOP対応デバイスでは、**VCA**にアクセスして**Smart Event**をインポートし、有効化してください。

手順

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

4. ルール
を設定
します。
しきい値

しきい値は、地域内の駐車時間のしきい値を表します。駐車時間がしきい値を超えると、アラームがトリガーされます。しきい値の値が大きいほど、アラームのトリガー時間が長くなります。

感度

感度は、許容可能なターゲットの一部が事前定義された領域に入る割合を表します。 $\text{感度} = 100 - S1/ST \times 100$ 。S1は、事前定義された領域を通過するターゲットの一部を表します。STは、ターゲット全体を表します。感度の値が高いほど、アラームがより容易にトリガーされます。

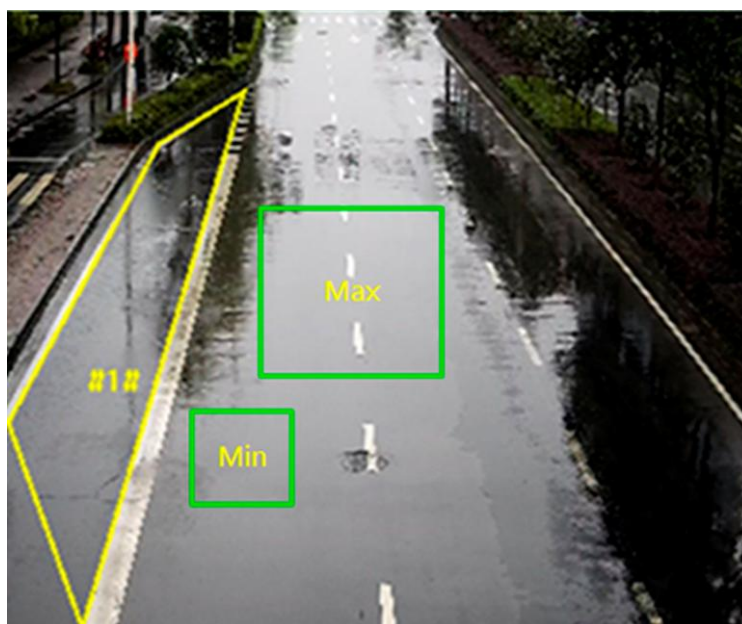


図10-10 ルール設定

5. オプション：上記のステップを繰り返し、複数の領域のパラメーターを設定できます。
6. 武装スケジュール設定については、「武装スケジュール設定」を参照してください。リンク方法設定については、「リンク方法設定」を参照してください。
7. 保存をクリックしてください。

注意

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

10.4 顔認識

デバイスは、設定されたルール領域内のルールに一致する顔をキャプチャし、キャプチャした画像をアップロードします。

注意

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

10.4.1 顔認識設定

設定された領域に表示される顔が撮影可能です。

開始前に

- **VCA** に移動し、アプリケーションを選択します。顔検出を選択し、次へをクリックして機能を有効にします。
- HEOP対応デバイスでは、**VCAに移動してFace Capture**をインポートし、有効化してください。

手順

1. **VCA**に移動し、→を選択します。アプリケーションを設定し、→を選択します。**Face Capture**を選択し、→ **Rule**を選択します。
2. 「有効にする」にチェックを入れて、ルール設定を有効にします。
3. 「」をクリックして、顔検出を有効にしたい検出領域を描画します。ライブビューウィンドウで左クリックで端点を指定し、右クリックで領域の描画を完了します。描画した領域は、ライブビュー画像の1/2から2/3の範囲内に収まるようにすることをおすすめします。
4. 瞳孔距離を描画します。

最小瞳孔距離

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

最大瞳孔距離

「」をクリックして最大瞳孔距離を描画します。動画画像内の顔の瞳孔距離が最大瞳孔距離を超える場合、顔は検出されません。

距離の値をテキストフィールドに入力することもできます。

5. オプション：シールド領域の設定については、「シールド領域の設定」を参照してください。
6. 武装スケジュール設定については、「武装スケジュール設定」を参照してください。リンク方法設定については、「リンク方法設定」を参照してください。
7. 保存をクリックしてください。
8. オーバーレイとキャプチャの設定については、「オーバーレイとキャプチャ」を参照してください。高度なパラメーター設定については、「顔キャプチャアルゴリズムパラメーター」を参照してください。

結果

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

10.4.2 オーバーレイとキャプチャ

ストリームと画像に表示するキャプチャパラメーターと情報を設定します。

ストリームにVCA情報を表示

ストリームにターゲットとルール情報を含むスマート情報を表示します。

アラーム画像にターゲット情報を表示

アラーム画像にターゲット情報をオーバーレイ表示します。

背景画像設定

ターゲット画像と比較して、背景画像は追加の環境情報を提供するシーン画像です。背景画像の画質と解像度を設定できます。背景画像を監視センターにアップロードする必要がある場合は、「**背景アップロード**」にチェックを付けてください。一部のデバイスでは、キャプチャした顔画像をアップロードするために「**顔画像**」にもチェックを付けることができます。

ターゲット画像設定

カスタム、顔写真、上半身写真、全身写真から選択可能です。

注意

カスタムを選択した場合、必要に応じて幅、頭の高さ、体の高さをカスタマイズできます。画像の高さを固定するには「**固定画像高さ**」にチェックを付けてください。

顔の美化

顔の美化にチェックを入れ、必要に応じて美化レベルを調整できます。

注

顔の美化機能は、撮影した顔の写真をわずかに調整し、顔のノイズを軽減します。

顔の補正

顔の美化機能を確認し、暗い環境でもより鮮明な顔写真を撮影できます。

テキストオーバーレイ

表示したい項目を選択し、表示順序を調整できます。カメラ情報を設定するには「カメラ情報設定」を参照し、デバイス番号とカメラ情報を設定してください。

10.4.3 顔認識アルゴリズムのパラメーター

顔認識機能のアルゴリズムライブラリのパラメーターを設定し最適化するために使用されます。

バージョン

現在のアルゴリズムのバージョンを表します。

キャプチャパラメーター

ベストショット

ターゲットが検出領域から離れた後の最良のショット。

キャプチャ閾値

顔の品質がキャプチャとアラームをトリガーする基準を表します。値が高いほど、キャプチャとアラームをトリガーするために必要な品質が向上します。

キャプチャ回数

設定された領域内に顔がいる間にキャプチャされる回数を指します。デフォルト値は1です。

クイックショット

顔画像のグレード値がクイックショット閾値を超える場合、その顔画像がキャプチャされアップロードされます。そうでない場合、最大キャプチャ間隔に達した最高グレード値の画像がアップロード用を選択されます。

クイックショット閾値

顔の認識精度が、高速撮影を可能にする品質を表します。

最大撮影間隔

これは、1回のクイックショットで占める最大時間を指します。

キャプチャ回数

設定された領域内に顔がいる間に、その顔がキャプチャされる回数を指します。

重複顔の削除

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

重複削除の類似度閾値

新規にキャプチャされた顔と重複削除ライブラリ内の画像の類似性です。類似性値が設定した値を超える場合、キャプチャされた画像は重複顔とみなされ、削除されます。

重複削除ライブラリのグレード閾値

重複チェックをトリガーする顔のグレード閾値です。顔のグレードが設定値を超える場合、キャプチャされた顔は重複削除ライブラリ内の顔画像と比較されます。

重複削除ライブラリ更新時間

各顔画像が重複削除ライブラリに追加されてから削除されるまでの時間です。

顔の露出

チェックボックスをオンにすると、顔の露出チェックが有効になります。

参照明るさ

顔露出モードにおける顔の基準明るさ。顔 **detected** された場合、カメラは設定した値に応じて顔の明るさを調整します。値が高いほど、顔は明るくなります。

最小露光時間

カメラが顔を露出する最小時間。



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

顔フィルタリング時間

これは、カメラが顔を検出してからキャプチャを実行するまでの時間間隔を指します。検出された顔がシーン内に設定されたフィルタリング時間よりも短い時間滞在した場合、キャプチャはトリガーされません。例えば、顔フィルタリング時間が5秒に設定されている場合、カメラは顔がシーン内に5秒間滞在し続けた場合に検出され



てキャプチャします。

顔検出の処理時間（0秒を超える場合）は、実際の撮影時間が設定値を超える可能性を高める可能性があります。

顔姿勢フィルター

顔姿勢フィルターは、特定の姿勢の顔をフィルタリングします。スライダーの右側の図は、顔キャプチャ動作で許容される姿勢角度を表します。このフィルターを設定する際、顔の回転方向を説明する図を表示するには、「」をクリックしてください。

特徴情報のアップロード

特徴とは、アルゴリズムが顔画像から識別できる特徴情報を指します。この情報をアップロードする機能にチェックを付けてください。

パラメーターの復元

デフォルト設定に戻す

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

10.4.4 シールド領域の設定

シールド領域は、設定したスマート機能ルールが無効になる特定の領域を設定できます。

手順

1. シールド領域を選択します。
2. 「」をクリックしてシールド領域を描画します。上記のステップを繰り返し、追加のシールド領域を設定します。
3. オプション: 描画した領域を選択し、クリックしてから「」をクリックして、選択した描画領域を削除します。
4. オプション: 「」をクリックして、描画されたすべての領域を削除します。
5. 「保存」をクリックします。

10.5 人物管理

人管理は、事前に定義された領域内の人数と変化を検出および分析するために使用されます。入口と出口、スーパーマーケットなどに応用可能です。

注意

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

10.5.1 地域別人流カウント

事前に定義されたエリア内の人数をカウントし、人数変化や混雑状況を検出します。人数異常または待機時間異常が発生した場合、デバイスはアラームをトリガーします。

「人密度設定」を参照して、人密度検出を設定してください。

「人検出の例外設定」を参照して、人検出の例外設定を設定してください。

待機時間例外検出を設定するには、待機時間例外検出を参照してください。

人密度を設定

この機能は、設定されたルール領域内の人密度レベルを検出します。

開始前に

- VCA**→ にアクセスし、**アプリケーション**を選択し、**People Management** を選択し、次へをクリックして機能を有効にします。
- HEOP対応デバイスでは、**VCA**にアクセスし、**People Management**をインポートして有効化してください。

手順

- VCA**に移動します。→ **アプリケーション**を設定します。→ **People Management** を選択します。→ **地域別人流カウント**→ **ルール**を選択します。
- 「追加」をクリックしてルールを追加し、その名前を設定します。
- ルールを設定します。

+ Add

Rule 1 x

* Rule Name Rule 1

* Alarm Interval 5 sec

* First Alarm Delay 5 sec

Alarm Times Per Exception ☒

* Alarm Times 1

People Number OSD ☒

図10-11 ルールを設定

人員数 OSD

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



注

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

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



注意

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

5. 「人密度アラーム」を有効にするには、チェックボックスをオンにします。

People Density Alarm

① People Density Alarm ☒

Upload Type

Scheduled Uploading ☒

Statistics Cycle

People Quantity Change Upload ☐

Congestion Level Upload ☐

Density Level

Level	Number of...	Custom Name
1		
2		
3		

図10-12 人数密度アラーム

スケジュールされたア
ップロード

デバイスは、設定された統計サイクル内で人の密度情報をアップロードします。

人数の変化のアップロード

デバイスは、設定されたルール区域内で変化が発生した場合、人の数量変化情報をアップロードします。

混雑レベルアップロード

デバイスは、設定されたルール区域内で混雑レベルに変化が生じた場合、混雑情報をアップロードします。

密度レベルの人数

設定ルール領域の人数の下限を入力することで、各レベルごとの範囲を指定します。

カスタム名

レベルの名前。



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

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

9. オプション：テキストオーバーレイを設定します。詳細な設定については、「オーバーレイとキャプチャ」を参照してください。
10. オプション：バージョンを表示し、フィルタリング条件を設定します。詳細な設定については、**Advanced SeFngs**を参照してください。

人検出の例外設定

この機能は、設定されたルール領域内の人数を検出し、状況がアラームトリガー条件を満たした場合にアラームを発生させます。

開始前に

- **VCA** に移動し、**→**を選択します。アプリケーションを選択し、**People Management** を選択し、次へをクリックして機能を有効にします。
- HEOP対応デバイスでは、**VCA** にアクセスし、**People Management** をインポートして有効化します。

手順

1. **VCA** にアクセスします**→ アプリケーションを設定します→ 人事管理→ 地域別人員カウント→ ルール**。
2. 「追加」をクリックしてルールを追加し、その名前を設定します。
3. ルールを設定します。

The screenshot shows the 'Rule 1' configuration page. At the top, there is a dashed box with a '+ Add' button. Below it is a red-bordered box containing 'Rule 1' and a close icon. The main form has the following fields: '*Rule Name' with the value 'Rule 1'; '*Alarm Interval' with the value '5' and a unit of 'sec'; '*First Alarm Delay' with the value '5' and a unit of 'sec'; 'Alarm Times Per Exception' with a green toggle switch; '*Alarm Times' with the value '1'; and 'People Number OSD' with a green toggle switch.

図10-13 ルールを設定する

人員数 OSD

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

例外ごとのアラーム時間

アラームがトリガーされた後のアラームの時間を指します。この設定を確認せずに時間を設定しない場合、デバイスはアラームを継続して送信し続けます。

アラーム間隔

設定された**アラーム間隔**内では、同じアラームは送信されません。

最初のアラーム遅延

最初のアラームがトリガーされた場合、設定された時間経過後にアラームが送信されます。

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



注意

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

5. 地域別人員例外アラームを確認し、アラームトリガー条件とアラーム閾値を設定してください。



注意

- ・ 「無人時のアラーム無視」を有効にすると、地域内に人がいない場合でもアラームは発動しません。
- ・ この機能は、設定値未満の値の場合に潜在的なアラーム条件をフィルタリングします。アラーム閾値と地域内に人がいない状態。

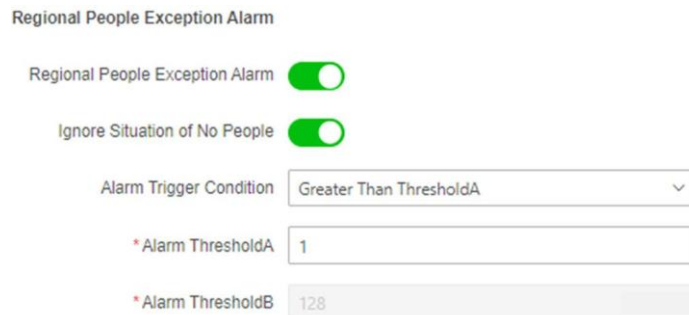


図10-14 地域内の人物不在アラーム

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

待機時間例外検出

この機能は、設定されたルール領域の待機時間を検出します。待機時間がアラーム発動条件を満たすと、アラームがトリガーされます。

開始前に

- **VCA** にアクセスします→ 「アプリケーション」を選択し、「**People Management**」を選択し、**次へ**をクリックして機能を有効にします。
- HEOP対応デバイスでは、**VCA**にアクセスして**People Management**をインポートし、有効化します。

手順

1. **VCA** にアクセスし、→を選択します。アプリケーションを設定し、→を選択し、**People Management**を選択し、→を選択します。**Regional People Counting**を選択し、→を選択します。**Rule**を選択します。
2. 「追加」をクリックしてルールを追加し、その名前を設定します。
3. ルールを設定します。

+ Add

Rule 1 ×

*Rule Name Rule 1

*Alarm Interval 5 sec

*First Alarm Delay 5 sec

Alarm Times Per Exception ☒

*Alarm Times 1

People Number OSD ☒

図10-15 ルールを設定する

人数のOSD

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

例外ごとのアラーム時間

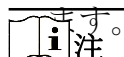
アラームがトリガーされた後のアラーム時間を指します。チェックを外して時間を設定しない場合、デバイスはアラームを継続して送信します。

アラーム間隔

設定されたアラーム間隔内では、同じアラームは送信されません。

最初の警報遅延

最初のアラームがトリガーされた場合、アラームは設定された時間経過後に送信され



待機時間例外アラームは、アラームトリガー条件が閾値Aを超える場合に限り、アラーム回数/例外、アラーム間隔、および最初のアラーム遅延の設定をサポートします。

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



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

5. 「滞在時間例外アラーム」を確認し、アラームトリガー条件とアラーム閾値を設定してください。

Dwell Time Exception Alarm

☒ Dwell Time Exception Alarm

Alarm Trigger Condition: Greater Than ThresholdA

* Alarm ThresholdA: 300 sec

* Alarm ThresholdB: 3600 sec

図10-16 滞在時間異常アラーム

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

10.5.2 オーバーレイとキャプチャ

→VCA 設定に移動し、[People Management] > [→] > [Overlay & Capture] を選択します。キャプチャした画像にオーバーレイ表示する情報を確認します。また、[↑ ↓]をクリックして順序を調整できます。

10.5.3 詳細設定

人管理機能の高度なパラメーターを設定し、保存をクリックします。バージョン

現在のアルゴリズムバージョンを表します。

アルゴリズムモード

インストール環境に応じてモードを選択してください。

フィルター

ターゲットサイズ

これはターゲット検出ウィンドウのサイズを表します。このピクセルサイズを超えるターゲットは、実際のターゲットとしてカウントされます。これにより、特定の固定ターゲットによる誤報を排除できます。

移動量

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

最小待機時間

設定値未満の待機時間はフィルタリングされます。

信頼度

閾値が高いほど、ターゲットの検出が困難になりますが、精度も高くなります。



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

10.6 人数のカウント

人数のカウントは、エリアに出入りする人の数を計算するために使用されます。



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

10.6.1 人流量計測ルールを設定する

検出ルールとアルゴリズムパラメーターを設定した後、デバイスはルール領域内での入退室人数を計算し、連携アクションをトリガーし、データを自動的にアップロードします。

開始前に

- VCA** にアクセスし、アプリケーションを選択します。「**People Counting**」を選択し、**次へ**をクリックして機能を有効にします。
- HEOP対応デバイスでは、**VCA**にアクセスして**People Counting**をインポートし、有効化します。

手順

- VCA**に移動します→アプリケーションを設定します→**People Counting**→**Rule**。
 - 「有効」にチェックを入れて機能を有効にします。
 - 「追加」をクリックして検出領域を追加します。
 - をクリックして、多角形検出領域（カウント領域）を描画します。ライブビューウィンドウで終了点を左クリックし、右クリックで描画を完了します。
 - 「」をクリックして検出線を描画します。矢印は進入方向を示します。方向を変更するには「」をクリックしてください。
-

注意

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

- ・ 検出領域は、アクセスエリアに出入りする人をすべてカバーする必要があります。
- ・ 検出線は、赤色の検出領域内に完全に含まれており、通過する人の経路と垂直でなければなりません。

6. オプション：検出領域と検出線を調整します。

「」をクリックして、選択した検出領域または線をクリアします。

「」をクリックし、すべての検出領域と線をクリアします。

7. オプション：上記のステップを繰り返し、最大3つの検出領域と対応する検出線を設定します。

8. 人計数パラメーターを設定します。

OSDオーバーレイコンテンツ

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

注意

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

日次リセット時間

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

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

9. 保存をクリックしてください。

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

11. リンク方法を設定します。 リンク方法の設定を参照してください。

12. 保存をクリックします。

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

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

リアルタイムデータアップロード

リアルタイムデータをプラットフォームに送信します。

定期的なデータアップロード

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

14. オプション：人数カウントの高度な設定を指定します。

「詳細設定」をクリックして設定画面に移動します。設定が完了したら「保存」をクリックします。

バージョン

現在のアルゴリズムのバージョンを表します。

ストレージデータのクリア

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

結果

- ターゲットが進入方向に沿って検出領域を通過し、検出ラインを横切った場合、その数を進入数としてカウントします。
- ターゲットが検出領域を退出方向に沿って通過し、検出線を越えた場合、その数は退出数としてカウントされます。

10.7 道路交通

道路交通監視には、車両検出と混合交通検出機能が利用可能です。この装置は、通過する自動車と非自動車を検出し、検出した画像と共に関連情報をアップロードします。



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

10.7.1 車両検出を設定する

セットされた車線に入る車両を検出でき、車両の画像とナンバープレートを撮影して保存できます。アラームが鳴り、撮影データがアップロードされます。

開始前に

- VCA**にアクセスし、アプリケーションを選択します。**道路交通**を選択し、**次へ**をクリックして機能を有効にします。
- デバイスが正しくインストールされていることを確認してください。
- 画像パラメーターが適切に設定されていることを確認してください。
- キャプチャされたナンバープレートの画像が十分に鮮明であることを確認してください。

手順

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

入口/出口

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

市街地道路

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

アラーム入力

これは、入力アラームがナンバープレート撮影と認識アクションをトリガーすること
を意味します。



- ・アラーム入力を選択された場合、アラーム入力 A<-1 が自動的に車両検出のトリガーに割り当てられ、そのアラームタイプは常に NO になります。
- ・アラーム入力 A<-1 を車両検出のトリガーとして使用する場合、他の基本イベントには使用できません。
- ・アラーム入力を選択され保存されると、以前に設定された A<-1 のリンク方法がキャンセルされます。

-
4. レーンの総数を選択してください。
 5. レーンラインをクリックしてドラッグして位置を設定するか、ラインの端をクリックしてドラッグしてラインの長さや角度を調整します。

青い検出線はナンバープレートのトリガーラインであり、主に「入口/出口」シーンでキャプチャ効率を向上させるために使用されます。画面の下中央に配置することをおすすめします。これにより、ナンバープレート付きの車両が完全に通過できることを確認できます。

6. カメラのズーム比を調整し、画像内の車両のサイズが赤いフレームのサイズに近くなるようにします。赤いフレームの位置のみ調整可能です。



注意

各車線ごとに、一度に1つのナンバープレートのみを認識できます。

-
7. エリアと国/地域を選択してください。
 8. 検出モードを設定してください。

車両優先順位

デバイスはまず車両のスケールを検出してから、ナンバープレートを捕捉して分析を行います。これにより精度が向上しますが、設置環境が不十分な場合、一部の検出結果が失われることがあります。

ナンバープレート & 車両

ナンバープレートと車両モードでは、デバイスはナンバープレートと車両を同時に検出します。アラーム情報とキャプチャした画像をアップロードします。



注意

インストールと補助ライトに問題がない場合は、**車両優先**モードを選択することをおすすめします。ナンバープレート認識の問題が解決された後、モードを**ナンバープレート&車両**モードに切り替えることができます。

-
9. 「重複したナンバープレートを削除」にチェックを入れ、**時間間隔**を設定してください。デフォルトの時間間隔は4分です。
 10. 「保存」をクリックします。

11. 「武装スケジュールとリンク方法」に移動します。ブロックリスト、許可リスト、その他のリストごとに武装スケジュールとリンク方法を独立して設定でき、それぞれを個別に設定する必要があります。

Target Type ☒ Blocklist ☐ Allowlist ☐ Others

Arming Schedule

Arming Schedule

Linkage Method

Direction ☒ All ☐ Forward ☐ Reverse

Notify Surveillance ... ☒

Upload to FTP/Mem... ☒

Trigger Alarm Output ☒ Select All

☒ A->1 ☒ A->2

図10-17 アーミングスケジュールとリンク方法

- 1) ブロックリスト、許可リスト、その他のリストを選択します。
- 2) アラーム設定スケジュールを設定します。詳細については「[アラーム設定スケジュールの設定](#)」を参照してください。
- 3) リンク方法を設定します。各ルールに対応するリンク方法のチェックボックスを選択し、[保存]をクリックして設定を保存します。

方向

選択した方向に進む車両のみが、選択したリンク方法をトリガーします。

すべて

すべては、すべての移動方向の車両が考慮されます。特別な用途がない場合は、すべてを選択することを強く推奨します。

前方

前方とは、車両がカメラの方向に向かって移動することを意味します。

後方

逆方向とは、車両がカメラから離れて移動することを指します。

ワイガンド接続

このデバイスは、Wiegandプロトコルを介して第三者プラットフォームにレポートを送信できます。

デバイスがWiegandインターフェースに対応しており、Wiegandインターフェースで正しく接続されていることを確認してください。

システム設定でWiegandが有効化されており、プロトコルが適切に設定されていることを確認してください。詳細については[Wiegand](#)を参照してください。

Wiegand リンクを有効にし、外部デバイスに接続された Wiegand インターフェースを選択してください。

リンクは、検出された車両の進行方向が設定された方向と一致した場合にのみトリガーされます。

12. 「**道路交通**」→「**オーバーレイ & キャプチャ**」に移動し、キャプチャした画像のイメージパラメーターとテキストオーバーレイを設定します。詳細については「[オーバーレイとキャプチャ](#)」を参照してください。
13. ナンバープレートブロックリストとアロリストをインポートまたはエクスポートします。詳細については「[ブロックリストとアロリストのインポートまたはエクスポート](#)」を参照してください。

10.7.2 混合交通検出ルールを設定します。

セットされた車線に入る自動車および非自動車を検出でき、目標物の画像を撮影して保存できます。アラームが鳴動し、撮影データがアップロードされます。

開始前に

- **VCA**にアクセスし、アプリケーションを選択します。**道路交通**を選択し、**次へ**をクリックして機能を有効にします。
- デバイスが正しくインストールされていることを確認してください。
- 画像パラメーターが適切に設定されていることを確認してください。

手順

1. **VCA** にアクセスし、**→** を選択します。アプリケーション設定で、**→**、**Road Traffic**、**→ Rule** を選択し、検出タイプとして「**Mixed-traffic Detection**」を選択します。
2. 「**有効**」にチェックを入れます。
3. レーンの総数を選択してください。
4. レーンラインをクリックしてドラッグして位置を設定するか、ラインの端をクリックしてドラッグしてラインの長さや角度を調整します。

青い検出線はナンバープレートのトリガーラインであり、主に「**入口/出口**」シーンでキャプチャ効率を向上させるために使用されます。画面の下中央に配置することをおすすめします。これにより、ナンバープレート付きの車両が完全に通過できることを確認できます。

5. カメラのズーム比率を調整し、画像内の車両のサイズが赤いフレームのサイズに近くなるようにします。赤いフレームの位置のみ調整可能です。



注意

各車線ごとに、一度に1つのナンバープレートのみを認識できます。

6. **エリア**と**国/地域**を選択してください。
7. **重複したナンバープレートを削除する**にチェックを入れ、**時間間隔**を設定してください。デフォルトの時間間隔は4分です。
8. **保存**をクリックしてください。

9. 「武装スケジュールとリンク方法」に移動します。ブロックリスト、許可リスト、その他のリストごとに武装スケジュールとリンク方法を独立して設定でき、それぞれを1つずつ設定する必要があります。

Target Type **Blocklist** Allowlist Others

Arming Schedule

Arming Schedule **Edit**

Linkage Method

Direction ☒ All ☐ Forward ☐ Reverse

Notify Surveillance ... ☒

Upload to FTP/Mem... ☒

Trigger Alarm Output ☒ Select All

☒ A->1 ☒ A->2

Save

図10-18 アーミングスケジュールとリンク方法

- 1) ブロックリスト、許可リスト、その他のリストを選択します。
- 2) アラーム設定スケジュールを設定します。詳細については「[アラーム設定スケジュールの設定](#)」を参照してください。
- 3) リンク方法を設定します。各ルールに対応するリンク方法のチェックボックスを選択し、**[保存]**をクリックして設定を保存します。

方向

選択した方向に進む車両のみが、選択したリンク方法をトリガーします。

すべて

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

前方

前方とは、車両がカメラの方向に向かって移動することを意味します。

後方

逆方向とは、車両がカメラから離れて移動することを指します。

ワイガンド接続

このデバイスは、Wiegandプロトコルを介してサードパーティのプラットフォームにレポートを送信できます。

デバイスがWiegandインターフェースに対応しており、Wiegandインターフェースで接続されていることを確認してください。

システム設定でWiegandが有効化されており、プロトコルが正しく設定されていることを確認してください。詳細については[Wiegand](#)を参照してください。

Wiegand リンクを有効化し、外部デバイスに接続された Wiegand インターフェースを選択してください。

リンクは、検出された車両の進行方向が設定された方向と一致した場合にのみトリガーされます。

10. 「**道路交通**」 → 「**オーバーレイ & キャプチャ**」に移動し、キャプチャした画像のイメージパラメーターとテキストオーバーレイを設定します。詳細については[「オーバーレイとキャプチャ」](#)を参照してください。
11. ナンバープレートブロックリストとアロリストをインポートまたはエクスポートします。詳細については[「ブロックリストとアロリストのインポートまたはエクスポート」](#)を参照してください。

10.7.3 オーバーレイとキャプチャ

車両検出と混合交通検出でキャプチャした画像の画像パラメーターを設定できます。

VCAに移動し、**道路交通**を選択します。

→ **VCA**に移動し、アプリケーションを設定します。→ を選択し、**Road Traffic**を選択します。

を選択し、**Overlay & Capture**を選択します。



機能はデバイスモデルによって異なります。

Picture Type ☒ License Plate/Target Close-up ☐ Vehicle ☒ Background

Picture Quality

Restriction Type ☒ Picture Quality ☐ Picture Size

Picture Quality 80

* Picture Size 1024 Kb

Picture Resolution 2560*1440

FTP Host

FTP Picture Name ☒ Default ☐ Custom

Picture Name IP_Channel! No_Time_Type.jpg

Text Overlay

Text Overlay ☒

Font Color

Background Color

Text Overlay

Text Overlay	To Be Selected	Selected
☐ Type		☐ Type Sort

Save

図10-19 オーバーレイ & キャプチャ

画像品質

値が大きいほど画像が鮮明になりますが、より多くのストレージ容量が必要になります。

画像サイズ

値が大きくなるほど、必要なストレージ容量も大きくなります。また、ネットワーク伝送の要件も高くなります。

画像解像度

撮影された背景画像の解像度。

画像キャプチャ間隔

カメラは、設定された間隔ごとにアラームを連続してトリガーし、キャプチャした画像をアップロードします。**キャプチャ間隔**を確認し、間隔を設定してください。

FTP画像名

車両検出と混合交通検出でキャプチャされた画像の命名規則をFTPサーバーで設定できます。

デフォルトを選択すると、デフォルトのルールが使用されます。

「カスタム」を選択し、画像名の情報を設定し、画像名パラメーターの順序を調整するには「↑ ↓」をクリックします。カスタムモードで「**Capture Time**」が選択されていない場合、同じ車両によって後からトリガーされた画像は、同じ画像名のため、以前にキャプチャされた画像と置き換えられます。



FTP設定の詳細については、「**FTPの設定**」を参照してください。

テキストオーバーレイ

カメラ、デバイス、または車両情報をキャプチャした画像にオーバーレイ表示し、[↑ ↓]をクリックしてオーバーレイテキストの順序を調整できます。

色ボックスを選択し、ポップアップパレットまたはドロップダウンボックスから希望の色をクリックして、フォント色と背景色を設定します。

10.7.4 ブロックリストとホワイトリストのインポート/エクスポート

ブロックリストと許可リストを必要に応じてインポートおよびエクスポートでき、このインターフェースでリストの内容を確認できます。

手順

1. 「インポート」をクリックして、選択したファイルをインポートします。
2. 「」をクリックして、PCのローカルディレクトリを開きます。
3. ブロックリストと許可リストのファイルを探し、クリックして選択します。「開く」をクリックして確認します。



- ・ インポートするファイルは、カメラが要求するファイルテンプレートと一致する必要があります。テンプレートとしてカメラから空のブロックリストと許可リストファイルをエクスポートし、内容を記入することをおすすめします。
- ・ ファイルは.xls形式で保存されており、セルの書式はテキストに設定されている必要があります。

-
4. 「インポート」をクリックして、選択したファイルをインポートします。
 5. 「すべてエクスポート」をクリックして、ライセンスプレート一覧をエクスポートします。
 6. オプション：[追加]をクリックして、ナンバープレートを追加し、関連する情報を1つつ設定します。
 7. オプション：▼をクリックしてフィルタリングの種類を選択します。**All Types**、**Wiegand CardID**、**License Plate No.**、および**Type**が選択可能です。**Type**については、**Keywords**を選択して特定のフィルタリング種類を定義できます。**Search**をクリックして結果を表示します。

8. オプション：プレート番号を選択し、「」をクリックすると、ブロックリストまたは許可リストからプレートを削除できます。
9. オプション：プレート番号を選択し、をクリックすると、ブロックリストまたは許可リストから該当するナンバープレートの関連情報を編集できます。

10.7.5 詳細パラメーター設定

VCAに移動し、アプリケーションを選択します。アプリケーションの設定画面に入り、「詳細」をクリックして高度なパラメーターを設定します。設定完了後、「保存」をクリックします。



注意

機能は、デバイスモデルによって異なります。

バージョン

現在のアルゴリズムのバージョンを表します。

インテリジェント情報のオーバーレイ

動画に、関連するインテリジェント情報またはPOS情報をオーバーレイ表示します。

10.8 AIオープンプラットフォーム

AIオープンプラットフォームは、ユーザーが提供するトレーニングデータに基づいてモデルライブラリを生成し、そのモデルライブラリをデバイスに読み込み、ユーザーがタスクとルールを構成できるようにします。シーン内でターゲットが検出されルールがトリガーされると、デバイスは連携アクションを実行し、パーソナライズされたスマートアプリケーションを実現できます。



注

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

10.8.1 AI Open Platform を設定する

手順

1. **VCAに移動→アプリケーションを設定→AI Open Platform。**



注意

- ・ AI Open Platform 経由で設定可能な特定のスマート機能（例：ヘルメット検出、炭鉱安全検出など）がサポートされています。
 - ・ 特定の機能を選択すると、デバイスは対応する機能のモデルパッケージをロードします。
 - ・ 機能はデバイスモデルによって異なります。実際のデバイスをご確認ください。
-
- ヘルメット検出機能では、設定された検出領域内でヘルメットを着用していない対象物を検出し、アラームを鳴らします。
 - 石炭鉱山安全検出の場合、**VCA→アプリケーション設定→石炭鉱山安全管理**にアクセスし、機能を有効にしてください。石炭鉱山シナリオでは、検出領域内の対象物
-

(人、鉱山車など)を検出します。ベルトがアイドラから外れた場合も検出します。

ヘルメットを着用していない人がいます。これは、石炭鉱山の安全検知のための設定されたルールに従ってアラームを鳴らします。

2. オプション：モデルをモデルライブラリに追加します。ローカルパスからモデルライブラリと関連するラベルファイルを選択し、モデル名を設定します。モデルの種類は以下の通りです。

検出モデル

ライブビュー内で特定のターゲットを検出し、ターゲットの検出結果と座標位置を提供します。

分類モデル

画像またはターゲットを属性に基づいて分類します。

混合モデル

ライブビュー内のターゲットを検出します。



最大モデルパッケージ数は、デバイスがサポートするモデルパッケージの最大数を指します。

3. モデルを選択し、有効にします。

4. 分析モードを選択します。

ライブ動画分析 デバイスはライブ動画を分析し、ターゲット検出と結果のアップロードを実現します。

スケジュールキャプチャ分析 デバイスは設定された自動切り替え間隔に基づいてキャプチャし、キャプチャした画像を分析して結果をアップロードします。

5. オプション：必要に応じてオーバーレイターゲットフレームとルールオーバーレイを有効にできます。

ターゲットフレームのオーバーレイアラーム画像にターゲットフレームをオーバーレイ表示します。

ルールオーバーレイ アラーム画像にルール情報を重ねて表示します。

6. アラームのスケジュール設定とリンク方法を設定します。アラームのスケジュール設定については、「[アラームスケジュール設定](#)」を参照してください。リンク方法の設定については、「[リンク方法設定](#)」を参照してください。

7. リンクされたチャンネルのルールを設定します。詳細については「[ルール設定](#)」を参照してください。

8. 保存をクリックします。

10.8.2 ルールを設定

リンクされたチャンネルのルールを設定します。

開始前に

VCA→ AIオープンプラットフォームで関連するモデルが選択されており、タスクの設定が完了していることを確認してください。

手順

1. **チャンネル管理**でチャンネルを選択するには、**リンクされたチャンネル**をクリックしてください。
2. リンクされたチャンネルの「」 をクリックしてルールを設定します。

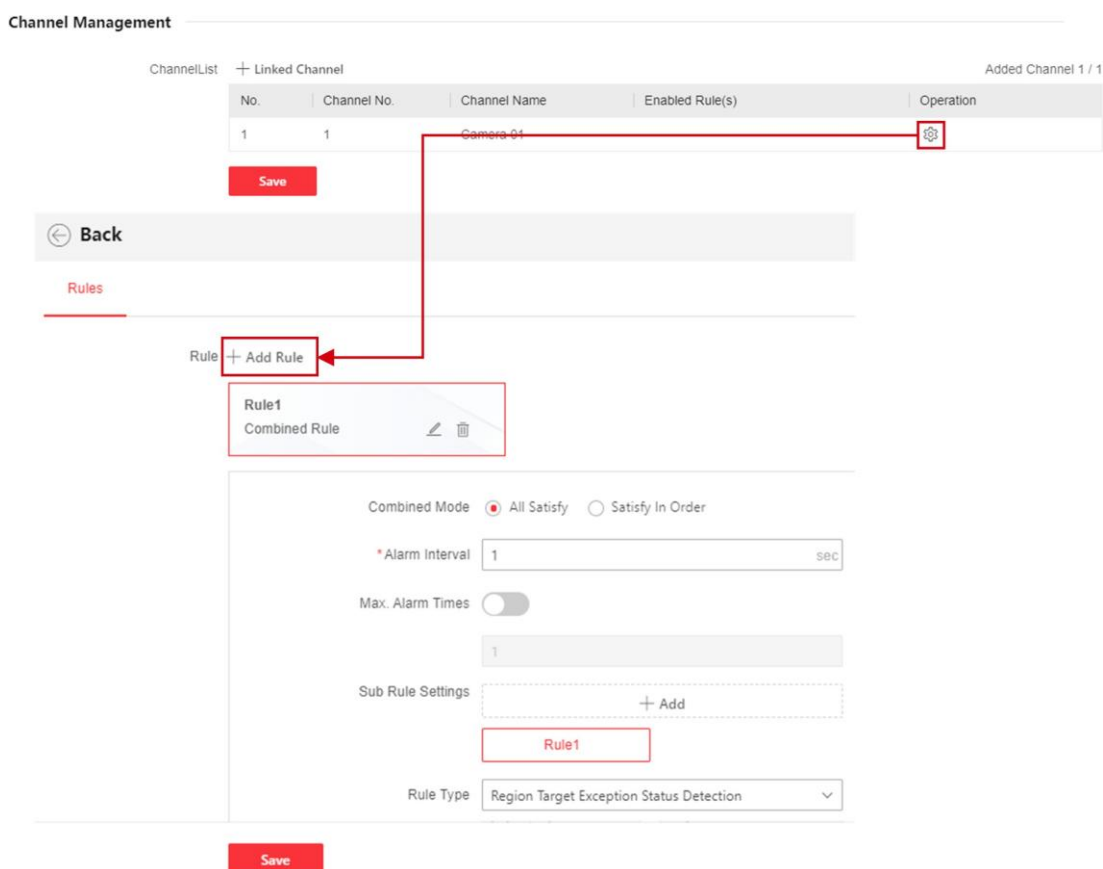


図10-20 ルールを設定する

3. 「Add Rule」をクリックします。ルールを選択し、「」をクリックしてルール名を変更し、ルールタイプを選択します。

地域ターゲット例外状態検出

事前に定義された仮想ルール領域内のターゲットの数を検出し、設定されたルールと比較します。トリガー条件を満たした場合、アラームをトリガーします。

ラインクロスターゲット検出

事前に定義された仮想ルールラインを横切るターゲットを検出し、検出した場合にアラームをトリガーします。

フル分析ルール

事前に定義された仮想ルール領域内のすべてのターゲットを検出および分析します。

ライン越えターゲットカウント

事前に定義された仮想ルールラインを横切るターゲットの数を検出およびカウントします。

領域内ターゲット数カウント

事前に定義された仮想ルール領域内のターゲットの数を検出およびカウントします。

複合ルール

事前定義された仮想ルール領域内で、**地域ターゲットの例外状態検出と線越えターゲット検出**をサポートします。検出順序として、**Combined Mode**を「すべて一致」または「順序通り一致」に設定できます。



ルールタイプはモデルパッケージによって異なります。実際のデバイスをご確認ください。

4. 検出ルールを設定し、ルール領域または線を引きます。
 - ルール領域を描画します：をクリックしてライブビューウィンドウに凸形状の領域を描画し、ライブビューウィンドウ内の終了点を左クリックしてルール領域の境界を定義し、右クリックで描画を完了します。
 - ルール線を描画：をクリックすると、ライブ動画に矢印付きの線が表示されます。線をライブビューウィンドウ内の希望の位置にドラッグします。
5. ルールパラメーターを設定します。

オブジェクト

モデルの検出対象の種類。

属性

モデルの検出対象の属性。

期間

ステータスの持続時間。設定された時間が経過するとアラームがトリガーされます。

アラーム間隔

設定されたアラーム間隔中に、同じ種類のアラームは**1**つの通知のみをトリガーします。

感度

感度値が高いほど、アラームがトリガーされやすくなります。感度値が過大の場合、誤報が発生しやすくなります。実際の状況に応じて設定してください。

最大アラーム回数

アラームがトリガーされる状態において、アラームがトリガーされる最大回数です。

カウント間隔

カウントの対象となる時間間隔。

アルゴリズムの有効性

アルゴリズムによって指定された信頼閾値が設定された有効期間以上になった場合、アラームがトリガーされ、アップロードされます。

ラインクロス

ターゲットがラインを横切る方向。

数量

数量を確認し、ドロップダウンボックスからアラームルールを選択します。アラームルールに応じて閾値または範囲（**最小値と最大値**）を設定します。ターゲットの数が設定されたアラームルールを満たすと、デバイスがアラームをトリガーします。

報告時間間隔

地域ターゲット数カウントを選択した場合、カウント結果をアップロードする時間間隔を指します。



ルールパラメーターはルールによって異なります。実際のデバイスをご確認ください。

6. 保存をクリックしてください。

第11章 EPTZ

EPTZ（電子式PTZ）は、物理的なカメラの移動なしで画像の一部をデジタルズームやパニングする高解像度機能です。EPTZ機能を使用するには、デバイスが**Third Stream**に対応していることを確認してください。Third StreamとEPTZは同時に有効に設定する必要があります。



この機能は、特定のデバイスモデルでのみサポートされています。

11.1 パトロール

手順

1. 設定に移動し、→ **EPTZ** を選択します。
2. 「有効」にチェックを入れます。
3. デフォルトのストリームタイプは「**Third Stream**」であり、設定できません。
4. アプリケーションモードで「パトロール」を選択します。
5. 「保存」をクリックします。

次に実行する操作

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

11.2 自動追尾

手順

1. 設定に移動し、→ **EPTZ** を選択します。
2. 「有効」にチェックを入れます。
3. デフォルトのストリームタイプは「**Third Stream**」であり、設定できません。
4. アプリケーションモードで「自動追跡」を選択します。
5. 「」をクリックして描画を開始します。ライブビューの動画をクリックして検出領域の4つの頂点を指定し、右クリックで描画を完了します。
6. ルールを設定します。

検出対象

人間と車両が選択可能です。検出対象が選択されていない場合、検出されたすべての対象が追跡されます（人間と車両を含む）。



この機能は、特定のカメラモデルのみに対応しています。

感度

これは、追跡可能なターゲットの身体部分の割合を表します。感度= $100 - S1/ST \times 100$ 。
S1は、事前定義された領域内に進入したターゲットの身体部分を表します。**ST**は、
ターゲットの全体的な身体を表します。感度の値が高いほど、ターゲットが追跡し
やすくなります。

7. 保存をクリックします。

付録A. FAQ

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



