ネットワークカメラ

ユーザーマニュアル

ビデオ製品の活用への取り組み

Hikvision 製品をお選びいただき、ありがとうございます。

技術は私たちの生活のあらゆる側面に影響を及ぼす。当社は、ハイテク企業として、事業の効率化や生活の質の向上に技術が果たす役割を認識するとともに、不正使用の危険性を認識しています。例えば、ビデオ製品は、現実の、完全な、および鮮明な画像を記録することができる。これは、遡及的に高い価値を提供し、リアルタイムの事実を保存する。ただし、ビデオ・データの不適切な配布、使用および/または処理が行われる場合、第三者の正当な権利および利益を侵害する結果となることもある。Hikvisionは、「Technology for the Good」を理念に、ビデオ技術やビデオ製品のエンドユーザー全員が、法令や倫理慣習を遵守し、共同でより良い地域づくりを目指すことを求めています。

以下の取り組みをよくお読みください:

- 誰もがプライバシーに合理的な期待を持っており、ビデオ製品のインストールがこの合理的な期待と矛盾してはならない。したがって、公共の場にビデオ製品を設置する場合には、合理的かつ効果的な方法で警告を発し、監視範囲を明確にしなければならない。非公開地域については、ビデオ製品をインストールする際に、第三者の権利および利益が評価されるものとする。ビデオ製品のインストールには、ステークホルダーの同意を得た後にのみビデオ製品をインストールし、高度に不可視なビデオ製品をインストールしないことが含まれるが、これに限定されない。
- ビデオ製品の目的は、特定の時間および空間内で、特定の条件下で、リアルアクティビティを記録することである。したがって、すべての利用者は、第三者の肖像権、プライバシーその他正当な権利を侵害することを避けるために、まず、当該特定の範囲において自己の権利を合理的に定義するものとする。
- ビデオ製品の使用中、大量の生物学的データ(顔画像など)を含む、現実のシーンから導出されたビデオ画像データが生成され続け、そのデータをさらに適用または再処理することができる。ビデオ製品自体は、ビデオ製品によってキャプチャされた画像のみに基づいてデータをどのように使用するかに関して、良品と不良品とを区別することができなかった。データ使用量の結果は、データコントローラの使用方法と目的によって異なります。従って、データ管理者は、適用されるすべての法律および規則ならびにその他の規範要件を遵守するだけでなく、国際的規範、社会道徳、善良な道徳、共通の慣行およびその他の強制力のない要件を尊重し、個人のプライバシー、肖像およびその他の権利および利益を尊重するものとする。
- ビデオ製品によって連続的に生成されるビデオデータを処理するとき、様々な利害関係者の権利、価値及び他の要求が常に考慮されるべきである。この点で、製品セキュリティおよびデータセキュリティは、極めて重要である。したがって、すべてのエンドユーザおよびデータコントローラは、データセキュリティを確保し、データ漏洩、不適切な開示および不適切な使用を回避するために、すべての合理的かつ必要な措置を講じなければならず、これには、アクセス制御の設定、ビデオ製品が接続される適切なネットワーク環境(インターネットまたはイントラネット)の選択、ネットワークセキュリティの確立および絶えず最適化が含まれるが、これらに限定されな

い。

- 映像作品は、世界中の社会保障の向上に大きく貢献しており、社会生活においても積極的な役割を果たしていくものと考えています。人権侵害や犯罪行為につながるビデオ製品の悪用は、技術革新や製品開発の本来の意図に反する。したがって、各ユーザーは、各製品が適切かつ合理的な方法で、誠実に使用されることを保証するために、各ユーザーの製品アプリケーションの評価および追跡メカニズムを確立しなければならない。

法的情報

©2021 八州日光ディジタルテクノロジー(株)無断転載を禁じます。

本書について

本マニュアルには、本製品を使用および管理するための説明書が含まれる。以下、写真、チャート、画像、その他の情報は、単に説明のためのものである。本マニュアルに記載されている情報は、ファームウェアの更新その他の理由により、予告なく変更される場合があります。本書の最新版は、ヒックビジョンホームページ(https://www.hikvision.com/)をご覧ください。
本マニュアルは、本製品をサポートする訓練を受けた専門家の指導と援助を得て使用してください。

商標

HIKVISION その他のHikvisionの商標およびロゴは、さまざまな管轄区域におけるHikvisionの特性である。
記載されている他の商標およびロゴは、それぞれの所有者の特性である。

免責事項

適用される法律によって許可される最大限の範囲まで、本マニュアルおよび記載される本製品は、そのハードウエア、ソフトウエアおよび会社とともに、「現状のまま」および「すべての障害およびエラーを伴って」提供される。HIKVISIONは、明示か黙示かを問わず、商品性、満足できる品質または特定目的への適合性を含むがこれらに限定されない保証を一切行わない。お客様による本製品の使用は、お客様自身のリスクである。いかなる場合においても、HIKVISIONは、契約違反、不法行為(過失を含む)、本製品の使用に関連して、たとえ当該損害または損失の可能性がHIKVISIONに通知されていたとしても、契約違反、不法行為(過失を含む)、本製品責任またはその他に基づくかを問わず、事業利益の損失、事業中断またはデータの喪失、システムの腐敗または文書の喪失に対する損害を含む、特別、派生的、付随的または間接的損害につき、貴社に一切責任を負わない。
貴社は、INTERNETのNATUREが固有のセキュリティリスクを提供し、HIKVISIONは、CYBER-ATTACK、HACKER ATTACK、VIRUS INFECTION、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操作、プライバシーリーケージ、またはその他の損害に対して一切責任を負わないことを認める。ただし、HIKVISIONは、必要な場合、タイムリーな技術サポートを提供する。
お客様は、本製品をすべての適用される法律に準拠して使用することに同意し、お客様の使用が適用される法律に準拠することを保証する単独の責任を負います。特に、貴社は、本製品を、限定なしに、出版権、知的財産権、またはデータ保護およびその他のプライバシー権を含む、第三者の権利を侵害しない方法で、使用する責任を負う。貴殿は、本製品を、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、核爆発性または安全でない核燃料サイクルに関連する文章における活動、または人権侵害の支援を含む、いかなる禁止された最終用途にも使用してはならない。

本マニュアルと適用される法律との間に矛盾が生じた場合、後者が優先する。

シンボル条約

本明細書で見られる記号は、以下のように定義される。

記号	説明
危険	取扱いを誤った時に、死亡もしくは重傷を負う可能性が想定されるものをいいます。
注意	回避しないと、装置の損傷、データの損失、性能の劣化、または予期しない結果を招く可能性のある危険な状況を示します。
注	本文の重要なポイントを強調または補足するための追加情報を提供します。

安全上のご注意

これらの取扱説明書は、危険または物的損失を回避するために、ユーザーが製品を正しく使用できることを保証することを目的としています。

法令

- 本装置は、地域の法律、電気安全規則、および防火規則に準拠して使用されるべきである。

電気

- 本製品の使用にあたっては、国・地域の電気安全規制を厳守しなければなりません。
- 装置は、したたり、はねたりしてはならず、また、花瓶のような液体で満たされた物体は、装置上に置かれてはならない。
- 山頂、鉄塔、森林などの特殊な条件下で、装置の入口開口部にサージサプレッサーを設ける。
- 注意: 火災の危険を減らすため、ヒューズの種類と定格が同じものとのみ交換してください。
- 装置は、アースされた電源コンセントに接続する必要があります。
- 適切な容易にアクセス可能な切断装置は、機器の外部に組み込まれなければならない。
- 適切な過電流保護装置は、建物の仕様を超えない範囲で、機器の外部に組み込まれるものとする。
- 建物の電気設備には、全極主電源スイッチを組み込まなければならない。
- AC主電源に接続するための端子の正しい配線を確認してください。
- 機器は、必要に応じて、IT配電システムに接続するように設計されている。

バッテリ

- バッテリーを摂取しないでください。ケミカルバーンハザード！
- 本機のリモコンにはボタン型電池が使用されています。コイン/ボタン電池を飲み込んだ場合、わずか2時間で激しい内部熱傷を引き起こし、死に至ることがある。
- 新しく使用済みの電池は子供から離しておいてください。
- リモコンの電池カバーがしっかり閉まらない場合は、使用を中止し、子どもの手の届かないところに保管してください。
- 電池を飲み込んだり、電池が身体の内部にあると疑われる場合は、ただちに医師の診療を受けてください。
- 注意: バッテリーを正しくないタイプと交換すると、爆発する危険があります。使用済みのバッテリを廃棄する場合は、指示に従ってください
- 注意事項: リスクーD'EXPLOSION SI LA BATTERIE EST REMPLACÉE PAR UNE BATTERIE DE TYPE INCORRECT.METTRE AU REBUT AUX 命令をUSAGÉES CONFORMÉMENTしてバッテリーを起動します。
- 不適切なタイプのバッテリーを不適切に交換すると、予防措置が無効になる可能性があります（リチウムバッテリーの種類によっては、そのような場合など）。
- 火や高温のオーブンに入れたり、機械的に破砕したり、電池を切ったりすると爆発することがありますので、廃棄しないでください。

- 爆発、可燃性の液体・気体の漏れの原因となるような、電池の周囲の温度が極めて高い場所に放置しないでください。
- バッテリーに極端に低い空気圧をかけないでください。爆発したり、可燃性の液体やガスが漏れたりする恐れがあります。
- + 直流で使用される、または直流を生成する機器の正端子を識別します。- 直流で使用される、または直流を生成する機器の負端子を識別します。

防火

- 照明されたろうそくのような裸の火炎源は、装置上に置かなければならない。
- 本器のシリアルポートは、デバッグ専用です。

高温面防止

-

注意: ホットパーツ！部品を取り扱う際に指が焼けてしまった。電源を切った後、1/30 時間待ってから、部品を取り扱ってください。このステッカーは、マークされたアイテムがホットであり、注意を払わずにタッチされるべきではないことを示すためのものである。このステッカーを有する装置の場合、この装置は、制限されたアクセス位置に設置することを意図しており、アクセスは、サービスマンによって、または、その位置に適用される制限の理由について、およびとられる予防措置について指示されたユーザによってのみ得ることができる。

設置

- 本取扱説明書の指示に従って機器を設置してください。
- けがを防止するために、この装置は、設置指示に従って床/壁にしっかりと取り付けられなければならない。
- 不安定な場所には絶対に置かないでください。装置が落下し、人が重傷を負ったり、死亡したりすることがあります。

電源

- 入力電圧は、IEC60950-1 規格: SELV (安全特別低電圧)および制限電源に適合する必要があります。詳細な情報については、該当するドキュメントを参照してください。
- 電源は、IEC 60950-1 またはIEC 62368-1 規格に準拠した限定電源またはPS2 要件を満たす必要があります。
- 過負荷による過熱や火災の危険を避けるため、1 つの電源アダプタに複数のデバイスを接続しないでください。
- プラグが電源ソケットに正しく接続されていることを確認します。

白色照明器(サポートされている場合)

- 本製品から放射される可能性のある有害な光放射。
- 動作中の光源に注意しないでください。目に有害なことがあります。
- カメラの組み立て、取り付け、保守の際は、適切な眼用保護具を着用するか、白色光を点灯しないでください。

輸送

- 装置を輸送する際は、装置を元の包装または類似の包装に保管してください。

システムセキュリティ

- インストーラとユーザーは、パスワードとセキュリティの設定を担当します。

保守

- 正常に動作しない場合は、販売店または最寄りのサービスセンターにご連絡ください。
- 弊社は、無断修理またはメンテナンスによって生じた問題については一切の責任を負いません。
- 少数のデバイスコンポーネント(電解コンデンサなど)では、定期的な交換が必要です。平均寿命は異なりますので、定期的な点検をお勧めします。詳細については、ディーラーにお問い合わせください。

洗浄

- 製品カバーの内外の汚れは、乾いた柔らかい布で拭いてください。アルカリ性の洗剤は使用しないでください。

環境の使用

- レーザー装置を使用しているときは、デバイスレンズがレーザー光にさらされていないか、焼損している可能性がありますのでご注意ください。
- 高電磁放射やほこりの多い環境にデバイスをさらさないでください。
- 室内専用機器の場合は、乾燥した換気の良い環境に設置してください。
- レンズを太陽や他の明るい光に向けないでください。
- 実行環境がデバイスの要件を満たしていることを確認します。使用温度は-30 ～ 60 ° C (-22 ～ 140 ° F)、使用湿度は95%以下(結露なし)とします。
- カメラを極端に高温、低温、ほこりっぽい場所や湿気の多い場所に置かないでください。また、高電磁放射にさらさないでください。

緊急事態

- 装置から煙、臭気、騒音が発生した場合は、直ちに電源を切って電源ケーブルを抜き、サービスセンターにご連絡ください。

時刻同期

- ローカル時刻がネットワークの時刻と同期されていない場合は、初めてアクセスするときにデバイス時刻を手動で設定します。Webブラウズ/クライアントソフトウェア経由でデバイスにアクセスし、時刻設定インタフェースに移動します。

反射

- デバイスレンズに反射面が近すぎないことを確認します。デバイスからのIR 光がレンズに反射して反射することがあります。

目次

第1章システム要件 1
第 2 章デバイスの起動とアクセス 2
2.1 SADP 経由でのデバイスの有効化 2
2.2 ブラウザ経由でデバイスをアクティブにする 3
2.3 ログイン 3
2.3.1 プラグインのインストール 3
2.3.2 管理者パスワードのリセット 4
2.3.3 不正ログインロック 5
第 3 章ライブビュー 6
3.1 ライブビューパラメータ 6
3.1.1 ライブビューの有効化と無効化 6
3.1.2 アスペクト比の調整 6
3.1.3 ライブビューストリームの種類 6
3.1.4 第三者プラグインを選択する 6
3.1.5 ウィンドウ部門 7
3.1.6 可視光 7
3.1.7 カウント画素 7
3.1.8 デジタルズーム開始 7
3.1.9 補助焦点 7
3.1.10 レンズ初期化 8
3.1.11 クイックセットライブビュー 8
3.1.12 レンズパラメータ調整 8
3.1.13 3Dポジショニングの実施 9
3.2 送信パラメータを設定する 9
3.3 スムーズストリーミングの設定 11
第 4 章ビデオとオーディオ 13
4.1 ビデオ設定 13
4.1.1 ストリームタイプ 13

4.1.2 ビデオタイプ 14
4.1.3 解像度 14
4.1.4 ビットレート・タイプと最大のビットレート 14
4.1.5 ビデオ品質 14
4.1.6 フレームレート 15
4.1.7 ビデオエンコーディング 15
4.1.8 スムージング 17
4.2 ROI 17
4.2.1 ROI設定 17
4.2.2 顔追跡ROIの設定 18
4.2.3 目標追跡ROIの設定 18
4.2.4 ライセンスプレート追跡ROIの設定 19
4.3 ストリームに情報を表示する 19
4.4 オーディオ設定 19
4.4.1 オーディオエンコーディング 20
4.4.2 オーディオ入力 20
4.4.3 音声出力 20
4.4.4 環境ノイズフィルタ 20
4.5 双方向オーディオ 20
4.6 設定を表示する 21
4.6.1 シーンモード 21
4.6.2 画像パラメータスイッチ 24
4.6.3 ビデオ標準 25
4.6.4 ローカルビデオ出力 25
4.7 OSD 25
4.8 プライバシーマスクの設定 26
4.9 オーバレイ画像 26
4.10 目標作付設定 27
第 5 章ビデオ録画とピクチャキャプチャ 28
5.1 ストレージ設定 28

5.1.1 新規または未暗号化メモリカードの設定 28
5.1.2 FTPの設定 30
5.1.3 NASの設定 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 ビデオ録画 33
5.2.1 自動的に記録する 33
5.2.2 手動で記録する 34
5.2.3 ライト・ストレージの設定 35
5.2.4 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 自動的に取り込む 36
5.3.2 マニュアルで取り込む 36
5.3.3 タイミングウェイクの設定 37
5.3.4 ピクチャ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 基本事象 38
6.1.1 動体検知の設定 38
6.1.2 ビデオ・タンパリング・アラームを設定する 40
6.1.3 PIRアラームを設定する 41
6.1.4 例外アラームを設定する 42
6.1.5 アラーム入力の設定 42
6.1.6 ビデオ品質診断の設定 43
6.1.7 振動検出を設定する 43
6.2 スマートイベント 44
6.2.1 オーディオ例外の検出 44
6.2.2 デフォーカス検出の設定 45
6.2.3 シーン変更の検出 45
6.2.4 顔検出の設定 46
6.2.5 ビデオロスを設定する 46

6.2.6 セット侵入検出 46
6.2.7 ライン交差検出の設定 48
6.2.8 領域入口検出の設定 49
6.2.9 領域退出の検出の設定 50
6.2.10 無人手荷物検知の設定 51
6.2.11 物体除去検出設定 52
6.2.12 描画領域 53
6.2.13 サイズフィルタの設定 53
第 7 章ネットワーク設定 55
7.1 TCP/IP 55
7.1.1 マルチキャスト 56
7.1.2 マルチキャスト検出 57
7.2 SNMP 57
7.3 SRTPの設定 58
7.4 ポートマッピング 58
7.4.1 オートポートマッピング を設定する 59
7.4.2 手動ポートマッピングの設定 59
7.4.3 ルータでのポートマッピングの設定 59
7.5 ポート 60
7.6 ドメイン名を介したデバイスへのアクセス 61
7.7 PPPoEダイヤルアップ接続によるデバイスへのアクセス 62
7.8 ワイヤレスダイヤル 63
7.8.1 ワイヤレスダイヤルの設定 63
7.8.2 許可リストの設定 64
7.9 Wi-Fi 64
7.9.1 デバイスをWi-Fi に接続する 64
7.10 ネットワークサービスを設定する 65
7.11 オープンネットワークビデオインターフェースの設定 66
7.12 ISUPの設定 67
7.13 アラームサーバーの設定 67

7.14 Hik-Connect 経由でカメラにアクセスする 68
7.14.1 カメラのHik-Connectサービスを有効にする 68
7.14.2 Hik-Connect のセットアップ 70
7.14.3 Hik-Connectにカメラを追加する 70
第 8 章準備スケジュールとアラームリンク 72
8.1 アーミングスケジュールの設定 72
8.2 連携方法の設定 72
8.2.1 トリガアラーム出力 72
8.2.2 FTP/NAS/メモリカードのアップロード 74
8.2.3 電子メールの送信 74
8.2.4 通知サーベイランスセンター 75
8.2.5 トリガ記録 75
8.2.6 ライトの点滅 75
8.2.7 警告音 76
第9章システムとセキュリティ 77
9.1 デバイス情報を表示する 77
9.2 ログの検索と管理 77
9.3 同時ログイン 77
9.4 設定ファイルのインポートとエクスポート 77
9.5 診断情報のエクスポート 78
9.6 再起動 78
9.7 復元とデフォルト 78
9.8 アップグレード 78
9.9 Open Source ソフトウェアライセンスの表示 79
9.10 ウィーガンド 79
9.11 メタデータ 79
9.12 日時 79
9.12.1 手動で時間を同期させる 80
9.12.2 NTP サーバの設定 80
9.12.3 衛星で時刻を同期する 80

9.12.4 DST設定 81
9.13 RS-485の設定 81
9.14 RS-232の設定 81
9.15 消費電力モード 82
9.16 外部機器 82
9.16.1 サプリメント可視光の設定 83
9.16.2 ヒータ 84
9.17 セキュリティ 84
9.17.1 認証 84
9.17.2 IP アドレスフィルタの設定 85
9.17.3 HTTPS の設定 85
9.17.4 Set QoS 86
9.17.5 IEEE 802.1Xを設定する 86
9.17.6 コントロールタイムアウト設定 87
9.17.7 セキュリティ監査ログの検索 87
9.17.8 セキュリティ強化 87
9.17.9 SSH 87
9.18 証明書管理 88
9.18.1 自己署名証明書の作成 88
9.18.2 証明書要求の作成 88
9.18.3 輸入証明書 89
9.18.4 サーバ/クライアント証明書のインストール 89
9.18.5 CA証明書のインストール 89
9.18.6 Enable Certificate Expiration Alarm 90
9.19 ユーザーとアカウント 90
9.19.1 ユーザーアカウントと許可の設定 90
9.19.2 同時ログイン 91
9.19.3 オンラインユーザー 91
第10 章VCA リソースの割り当て 92
10.1 カウント 92

10.1.1 カウント設定 92
10.1.2 ビューカウント統計 93
10.2 フェースキャプチャ 94
10.2.1 顔キャプチャの設定 94
10.2.2 オーバーレイとキャプチャ 95
10.2.3 顔キャプチャアルゴリズムパラメータ 95
10.2.4 シールド領域の設定 97
10.3 マルチターゲット型検出 97
10.3.1 マルチターゲットタイプ検出ルールの設定 98
10.3.2 オーバーレイとキャプチャ 98
10.3.3 マルチターゲットタイプ検出アルゴリズムパラメータ 99
10.3.4 シールド領域の設定 100
10.4 キュー管理 100
10.4.1 地域住民のキューイングアップの設定 100
10.4.2 待ち時間検出の設定 101
10.4.3 キュー管理統計 102
10.5 顔カウント 103
10.5.1 顔カウント検出ルールの設定 104
10.5.2 オーバーレイとキャプチャ 105
10.5.3 顔カウントアルゴリズムパラメータ 105
10.5.4 顔カウント結果の表示 107
10.6 顔の比較とモデリング 107
10.6.1 面比較 107
10.6.2 フェイスモデリング 110
10.7 ハードハード検出 110
10.7.1 Hard Hart Detection を設定する 111
10.8 道路交通 112
10.8.1 車両検知の設定 112
10.8.2 混在トラフィック検出ルールの設定 113
10.8.3 画像設定をアップロードする 113

10.8.4 カメラの設定 114
10.8.5 ブロックリストおよび許可リストのインポートまたはエクスポート 114
第 11 章 プラットフォームを開く 116
11.1 オープンプラットフォームの設定 116
第 12 章スマートディスプレイ 118
第13章EPTZ 119
13.1 パトロール 119
13.2 自動追跡 119
A. デバイスコマンド 121
B. デバイス通信マトリックス 122

第1章システム要件

お使いのコンピュータは、製品を正しく訪問し、操作するための要件を満たしている必要があります。

オペレーティングシステム	Microsoft Windows XP SP1 以降のバージョン
CPU	2.0 GHz以上
RAM	1G以上
表示	1024×768 解像度以上
Web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 章デバイスの起動とアクセス

ユーザーアカウントとデータのセキュリティとプライバシーを保護するために、ネットワーク経由でデバイスにアクセスするときにデバイスをアクティブ化するためのログインパスワードを設定する必要があります。

注

クライアントソフトウェアのアクティベーションの詳細については、ソフトウェアクライアントのユーザーマニュアルを参照してください。

2.1 SADP 経由でのデバイスの有効化

SADP ソフトウェアを介してオンラインデバイスを検索し、アクティブ化します。

開始前に

SADPソフトウェアをインストールするには、www.hikvision.comにアクセスしてください。

手順

1. ネットワークケーブルを使用してデバイスをネットワークに接続します。
2. SADPソフトウェアを実行して、オンラインデバイスを検索します。
3. デバイスリストからデバイスステータスをチェックし、Inactive device を選択します。
4. パスワードフィールドに新しいパスワードを作成して入力し、パスワードを確認します。

注意

製品のセキュリティを高めるために、独自に選択した強力なパスワード(大文字、小文字、数字、特殊文字を含む8 文字以上を使用) を作成することを強くお勧めします。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勧めします。毎月または毎週パスワードをリセットすると、製品の保護が向上します。

5. [OK]をクリックします。
   Device Status がActive に変更されます。
6. オプション: 「ネットワークパラメータの変更」で、デバイスのネットワークパラメータを変更します。

2.2 ブラウザ経由でデバイスをアクティブにする

ブラウザからデバイスにアクセスし、アクティブ化できます。

手順

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

注

デバイスのデフォルトIP アドレスは192.168.1.64 です。PC のIP アドレスは、192.168.1.2 ～ 192.168.1.253(192.168.1.64 を除く)の範囲で設定できます。たとえば、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 と入力します。
4. デバイスのアクティベーションパスワードを設定します。

注意

製品のセキュリティを高めるために、独自に選択した強力なパスワードを作成することを強くお勧めします(大文字、小文字、数字、特殊文字の3 つ以上のカテゴリを含む、最低8 文字を使用)。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勧めします。毎月または毎週パスワードをリセットすると、製品の保護が向上します。

5. [OK]をクリックします。
6. アクティベーションパスワードを入力して、デバイスにログインします。
7. 必要に応じて、「設定→ネットワーク→基本→ TCP/IP」に移動して、機器のIPアドレスをネットワークの同じセグメントに変更します。

2.3 ログイン

Web 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

特定のオペレーションシステムおよびウェブブラウザは、カメラ機能の表示および動作を制限することができる。プラグインをインストールするか、または特定の設定を完了して、正常な表示および操作を保証する必要があります。詳細な制限機能については、実際の装置を参照してください。

オペレーティングシステム	Webブラウザ	操作
Windows	● Internet Explorer 8+	ポップアップ・プロンプトに従っ

オペレーティングシステム	Webブラウザ	操作
	● Google Chrome 57以前のバージョン ● Mozilla Firefox 52 以前のバージョン	て、プラグインのインストールを完了します。
	● Google Chrome 57+ ● Mozilla Firefox 52+	クリックしてプラグインをダウンロードし、インストールします。 Download Plug-in
マックOS	● Google Chrome 57+ ● Mozilla Firefox 52+ ● マックサファリ16+	プラグインインストールは不要です。 「設定→ネットワーク 詳細設定→ネットワークサービス」に進み、WebSocket または Websocket を通常表示に有効にします。特定の機能の表示・動作が制限されています。たとえば、「再生」と「画像」は使用できません。詳細な制限機能については、実際の装置を参照してください。

注

このカメラはWindows/Mac OSのみ対応しており、Linuxには対応していません。

2.3.2 管理者パスワードのリセット

管理者パスワードを忘れた場合は、アカウントのセキュリティ設定を完了した後、ログインページの「パスワードを忘れた」をクリックしてパスワードをリセットできます。
セキュリティの質問または電子メールを設定することで、パスワードをリセットできます。

注

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

セキュリティーに関する質問

アクティベーション中にアカウントセキュリティを設定できます。または、→ユーティリティユーザ管

理の設定に進み、アカウントセキュリティ設定をクリックし、セキュリティの問題を選択して答えを入力します。
「パスワードを忘れてください」をクリックし、セキュリティの質問に答えると、ブラウザ経由でデバイスにアクセスするときに管理者パスワードをリセットできます。

電子メール

アクティベーション中にアカウントセキュリティを設定できます。または、→ユーティリティの「ユーザ管理」で「アカウントセキュリティ設定」を選択し、復元処理中に確認コードを受信するメールアドレスを入力します。

2.3.3 不正ログインロック

インターネット経由でデバイスにアクセスする場合のセキュリティの向上に役立ちます。
→ユーティリティセキュリティセキュリティサービスの設定に進み、不正ログイン→の有効化を有効にします。不正なログイン試行とロック継続時間は設定可能です。

不正なログインの試行

間違ったパスワードでログインしようとすると、設定した時間に達すると、デバイスがロックされます。

ロック時間

設定した時間が経過すると、デバイスはロックを解除します。

第 3 章ライブビュー

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

3.1 ライブビューパラメータ

サポートされる関数は、モデルによって異なります。

3.1.1 ライブビューの有効化と無効化

この機能は、チャンネルのライブビューを素早く有効または無効にするために使用します。
- クリックしてライブビューを開始します。▶
- ライブビューを停止するには、をクリックします。■

3.1.2 アスペクト比の調整

手順

1. ライブビューをクリックします。
2. クリックしてアスペクト比を選択します。
   - 4:3は、4:3のウィンドウサイズを指します。
   - 16:9は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。
   - 自己適応ウィンドウサイズを指します。
   - 元の比率ウィンドウ・サイズを指します。

3.1.3 ライブビューストリームの種類

必要に応じてライブビューストリームの種類を選択します。ストリームタイプの選択の詳細については、「ストリームタイプ」を参照してください。

3.1.4 第三者プラグインを選択する

特定のブラウザーでライブビューを表示できない場合は、ブラウザー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. クリックしてプラグインを選択します。

Internet Explorer を介してデバイスにアクセスすると、Webcomponents またはQuickTime を選

択できます。他のブラウザからデバイスにアクセスする場合は、Web コンポーネント、QuickTime、VLC、またはMJPEG を選択できます。

3.1.5 ウィンドウ部門

- 1 × 1のウィンドウ分割を指します。
- 2 × 2ウィンドウ分割を指します。
- 3 × 3のウィンドウ分割を指します。
- 4 × 4のウィンドウ分割を指します。

3.1.6 可視光

[クリック]をクリックして、イルミネータの電源をオンまたはオフにします。

3.1.7 カウント画素

これは、ライブビュー画像内の選択された領域の高さ及び幅ピクセルを得るのに役立つ。

手順

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

3.1.8 デジタルズーム開始

これは、画像内の任意の領域の詳細な情報を見るのに役立つ。

手順

1. クリックしてデジタルズームを有効にします。
2. ライブビュー画像で、マウスをドラッグして目的のリージョンを選択します。
3. ライブビュー画像をクリックすると、元の画像に戻ります。

3.1.9 補助焦点

これは、電動装置に使用される。それは、装置が明確に焦点を合わせることができない場合、画像を改善することができる。
ABFをサポートするデバイスの場合は、レンズ角度を調整してから、デバイスのABFボタンをクリックします。装置は明確に焦点を合わせることができる。
クリックすると自動的にフォーカスします。

注

- 補助フォーカスでピントを合わせることができない場合は、「レンズ初期化」を使用し、再度補助

フォーカスを使用して画像を鮮明にすることができます。
- 補助フォーカスがデバイスのフォーカスを明確にサポートできない場合は、マニュアルフォーカスを使用できます。

3.1.10 レンズ初期化

レンズの初期化は、電動レンズを装備したデバイスで使用されます。長時間ズームやフォーカスで画像がぼやけると、レンズをリセットすることができます。この関数は、モデルによって異なります。

手動レンズ初期化

クリックしてレンズ初期化を行います。

オートレンズ初期化

「構成→系→保守→レンズ補正」に進み、本機能を有効にします。アーミングスケジュールを設定すると、設定した時間帯に自動的にレンズ補正が行われます。

3.1.11 クイックセットライブビュー

ライブビューページで、PTZ、ディスプレイ設定、OSD、ビデオ/オーディオ、VCA リソース設定を素早くセットアップできます。

手順

1. クイックセットアップページを表示します。
2. PTZ、ディスプレイ設定、OSD、ビデオ/オーディオ、VCA リソースパラメータを設定します。
   - PTZの設定については、「レンズパラメータの調整」を参照してください。
   - 表示設定については、「表示設定」を参照してください。
   - OSD設定については、OSDを参照してください。
   - オーディオとビデオの設定については、「ビデオとオーディオ」を参照してください。
   - VCA の設定については、「VCA リソースの割り当て」を参照してください。

注

この関数は、特定のモデルによってのみサポートされます。

3.1.12 レンズパラメータ調整

レンズのフォーカス、ズーム、アイリスの調整に使用します。

ズーム

- クリックすると、レンズがズームインします。

- クリックして、レンズがズをズームアウトします。

フォーカス

- クリックすると、レンズの焦点が遠くに合い、遠くの物体が透明になります。
- クリックすると、レンズの焦点が近くに合い、近くの物体が透明になります。

PTZ速度

スライドさせて、パン/チルトの動きの速度を調整します。

アイリス

- 画像が暗すぎる場合は、をクリックしてアイリスを拡大します。
- 画像が明るすぎる場合は、アイリスを止めるときにクリックします。

PTZロック

PTZ ロックとは、対応するチャンネルのズーム、フォーカス、PTZ 回転機能を無効にすることで、PTZ 調整によって発生するターゲットの欠落を減らすことができます。
「設定→ PTZ」に移動し、「PTZ ロックを有効にする」にチェックを入れ、「保存」を選択します。

3.1.13 3Dポジショニングの実施

3D位置決めは、選択された領域を画像中心に再配置することである。

手順

1. クリックして機能を有効にします。
2. ライブ画像の対象領域を選択します。
   - ライブ画像上のポイントを左クリックすると、そのポイントがライブ画像の中心に再配置されます。ズームインまたはズームアウトの効果がありません。
   - マウスを右下の位置に持ってドラッグして、ライブ上の領域をフレーム化します。フレーム化された領域はズームインされ、ライブ画像の中心に再配置されます。
   - マウスを左上に持ってドラッグし、ライブ上の領域をフレーム化します。フレーム化された領域はズームアウトされ、ライブ画像の中央に再配置されます。
3. ボタンをもう一度クリックすると、機能がオフになります。

3.2 送信パラメータを設定する

ライブビュー画像は、ネットワーク状態に応じて異常表示されてもよい。異なるネットワーク環境では、送信パラメータを調整して問題を解決できます。

手順

1. 「設定→ローカル」に移動します。
2. 必要に応じて送信パラメータを設定します。

プロトコル

TCP

TCP は、ストリーミングデータの完全な配信とより優れたビデオ品質を保証しますが、リアルタイム伝送は影響を受けます。これは、安定したネットワーク環境に適している。

UDP

UDPは、高いビデオ流動性を要求しない不安定なネットワーク環境に適している。

マルチキャスト

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

注

マルチキャストの詳細については、「マルチキャスト」を参照してください。

HTTP

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

プレイパフォーマンス

最短遅延

デバイスは、リアルタイムビデオイメージをビデオの流行よりも優先させます。

バランス

この装置は、リアルタイムのビデオ画像と流動性の両方を保証する。

流動剤

このデバイスは、ティールタイムよりもビデオフルエンスを優先します。ネットワーク環境が悪い場合、フルエンシーが有効になっていても、デバイスはビデオフルエンシーを保証できません。

カスタム

フレームレートは手動で設定できます。ネットワーク環境が悪い場合は、フレームレートを下げて、滑らかなライブビューを得ることができます。ただし、ルール情報が表示できない場合があります。

3. [OK]をクリックします。

3.3 スムーススストリーミングの設定

ネットワークの不安定な状況による待ち時間やネットワークの混雑に対応し、Webブラウザやクライアントソフトウェア上のライブビューストリームをスムーズに保つ機能です。

開始前に

スムーズストリーミング機能を設定する前に、デバイスをクライアントソフトウェアに追加し、クライアントソフトウェアでNPQ プロトコルを選択します。
Bitrate TypeがConstantに選択され、SVCがOFFに選択されていることを確認してから、機能を有効にします。設定→ビデオ/オーディオ→ビデオに移動して、パラメータを設定します。

手順

1. 設定画面:スムーズストリーミングの→にある「設定→網→詳細設定」に進みます。
2. スムーズストリーミングを有効にするをオンにします。
3. スムーズストリーミングのモードを選択します。

自動	解像度とビットレートは自動的に調整され、解像度が優先されます。これら2 つのパラメータの上限は、「ビデオ(Video)」ページで設定した値を超えません。設定→ビデオ/オーディオ→ビデオに移動し、解像度と最大を設定します。スムーズストリーミング機能を有効にする前のビットレート。このモードでは、フレームレートは自動的に最大値に調整される。
決議の優先順位	解像度はビデオページの設定値と同じままで、ビットレートは自動的に調整されます。設定→ビデオ/オーディオ→ビデオに移動し、最大を設定します。スムーズストリーミング機能を有効にする前のビットレート。このモードでは、フレーマートは自動的に最大値に調整される。
フレームレート優先度	劣悪なネットワークの下でも、画像は依然として滑らかであるが、画質は良くないことがある。
誤り訂正	解像度およびビットレートは、ビデオページの設定値と同じままです。このモードは、伝送中のデータエラーを訂正して画質を確保するために使用される。エラー訂正率は0～100の範囲で設定できます。比率が0の場合、データ再送によりデータ誤りを訂正する。比率が0より大きい場合、ストリームおよびデータ再送信に追加される冗長データを介してエラーデータが修正されます。値が大きいほど、冗長な日付が生成され、より多くのデータエラーが修正されますが、より大きな帯域幅が必要になります。比率が100 の場合、冗長データは元のデータと同じ大きさになり、帯域幅は2 倍必要になります。

注

エラー訂正モードでは、帯域幅が十分であることを確認します。

4. 設定を保存します。

第 4 章ビデオとオーディオ

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

4.1 ビデオ設定

このパートでは、ストリームタイプ、ビデオエンコーディング、解像度などのビデオパラメータの設定について説明します。
設定画面:設定→ビデオ/オーディオ→ビデオに移動します。

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は、ストリームタイプごとにパラメータを指定できます。

メインストリーム

ストリームは、装置がサポートする最良のストリーム性能を表す。これは、通常、装置が行うことができる最良の解像度及びフレームレートを提供する。しかし、高い解像度およびフレームレートは、通常、伝送において、より大きなストレージスペースおよびより高い帯域幅要件を意味する。

サブストリーム

ストリームは、通常、比較的低い解像度オプションを提供し、これは、より少ない帯域幅及びストレージスペースを消費する。

その他のストリーム

メインストリームおよびサブストリーム以外のストリームも、カスタマイズされた使用のために提供されてもよい。

カスタムビデオの設定

必要に応じて、追加のビデオストリームを設定できます。カスタムビデオストリームの場合、プレビューはできますが、録画や再生はできません。

手順

注

- この機能は、特定のカメラモデルでのみサポートされます。
- デバイスを復元した後(デフォルト設定に復元しない)、カスタムビデオストリームの数量とその名前は保持されますが、関連するパラメータは復元されます。

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

> **注**
>
> ストリーム名には最大32 文字の文字と記号(&、<、>、'、または" を除く) を使用できます。

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

4.1.2 ビデオタイプ

ストリームに含めるコンテンツ(ビデオとオーディオ)を選択します。

ビデオ

ストリームにはビデオコンテンツのみが含まれます。

ビデオとオーディオ

ビデオコンテンツとオーディオコンテンツは、コンポジットストリームに含まれます。

4.1.3 解像度

実際のニーズに応じて、ビデオ解像度を選択します。より高い解像度は、より高い帯域幅およびストレージ装置を必要とする。

4.1.4 ビットレート・タイプと最大のビットレート

固定ビットレート

これは、ストリームが圧縮され、比較的固定されたビットレートで送信されることを意味する。圧縮速度は速いが、画像上にモザイクが生じることがある。

可変ビットレート

これは、装置が設定された最大値の下でビットレートを自動的に調整することを意味する。硝酸塩。圧縮速度は、一定ビットレートの速度よりも遅い。しかし、それは複雑なシーンの画質を保証する。

4.1.5 ビデオ品質

ビットレート・タイプが可変に設定されている場合、ビデオ品質は設定可能である。実際のニーズ

に合わせて画質を選択します。より高いビデオ品質は、より高い帯域幅を必要とすることに留意されたい。

4.1.6 フレームレート

フレームレートは、ビデオストリームが更新される周波数を記述するためのものであり、フレーム毎秒(fps)によって測定される。
より高いフレームレートは、ビデオストリームに動きがあるときに、全体を通して画質を維持するので有利である。より高いフレームレートは、より高い帯域幅およびより大きなストレージスペースを必要とすることに留意されたい。

4.1.7 ビデオエンコーディング

これは、装置がビデオ符号化に採用する圧縮規格を表す。

注
利用可能な圧縮規格は、デバイスモデルによって異なる。

H.264

H.264, MPEG—4 Part 10、Advanced Video Codingとしても知られる圧縮規格である。画質を圧縮しないと、MJPEGやMPEG—4 Part 2よりも圧縮率が高くなり、映像ファイルのサイズが小さくなる。

H.264+

H. 264+は、H.264に基づく改善された圧縮符号化技術である。H.264+ を有効にすると、HDD の消費量を最大平均ビットレートで見積もることができます。H.264と比較して、H.264+は、ほとんどのシーンにおいて同じ最大ビットレートで50%までストレージを減少させる。
H.264+が有効の場合、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与える。ビデオ品質が不十分な場合は、パラメータをより高い値に調整できます。最大。平均ビットレートは、最大ビットレートを超えてはならない。

注
H.264+が有効になっている場合、ビデオ品質、Iフレーム間隔、プロファイル、SVC、メインストリームスムージング、およびROIはサポートされません。

H.265

H.265, HEVC(High Efficiency Video Coding)およびMPEG—Hパート2としても知られる圧縮規格である。H.264と比較すると、同じ解像度、フレームレート、および画質でより良好なビデオ圧縮を提供する。

H.265+

H. 265+は、H.265に基づく改善された圧縮符号化技術である。H.265+ を有効にすると、HDD の消費量を最大平均ビットレートで見積もることができます。H.265と比較して、H.265+は、ほとんどのシーンにおいて同じ最大ビットレートで50%までストレージを減少させる。
H.265+が有効の場合、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与える。ビデオ品質が不十分な場合は、パラメータをより高い値に調整できます。最大。平均ビットレートは、最大ビットレートを超えてはならない。

注

H.265+ が有効な場合、ビデオ品質、I フレーム間隔、プロファイル、SVC は設定できません。

Iフレーム間隔

I フレーム間隔は、2 つのI フレーム間のフレーム数を定義します。
H.264およびH.265では、Iフレーム、すなわちイントラフレームは、他の画像を参照することなく独立して復号することができる自己完結型フレームである。Iフレームは、他のフレームよりも多くのビットを消費する。したがって、より多くのIフレーム、言い換えれば、より小さいIフレーム間隔を有するビデオは、より多くのストレージ空間を必要としながら、より安定した信頼性のあるデータビットを生成する。

SVC

スケーラブル・ビデオ・コーディング(SVC)は、H.264またはH.265ビデオ圧縮規格のAnnex G拡張の名前である。
SVC 標準化の目的は、サブセットビットストリームと同じ量のデータを持つ既存のH.264 またはH.265 デザインを使用して達成されたものと同様の複雑さと再構成品質で、それ自体をデコードできる1 つ以上のサブセットビットストリームを含む高品質ビデオビットストリームのエンコードを可能にすることです。サブセットビットストリームは、大きなビットストリームからパケットをドロップすることによって生成されます。
SVC は、古いハードウェアの前方互換性を可能にします。同じビットストリームは、低解像度サブセットのみをデコードできる基本的なハードウェアによって消費できますが、より高度なハードウェアは高品質のビデオストリームをデコードできます。

MPEG4

MPEG4は、MPEG−4パート2を参照して、MPEG(Moving Picture Experts Group)によって開発されたビデオ圧縮フォーマットである。

MJPEG

Motion JPEG (M−JPEGまたはMJPEG)は、フレーム内符号化技術が使用されるビデオ圧縮フォーマットである。MJPEG形式の画像は、個々のJPEG画像として圧縮される。

プロファイル

この関数は、同じビットレートの下では、プロファイルが複雑になるほど、画像の品質が高くなり、ネットワーク帯域幅に対する要求も高くなることを意味する。

4.1.8 スムージング

これは、流れの滑らかさを指す。平滑化の値が高いほど、ストリームの流動性は良くなるが、ビデオ品質はそれほど満足できるものではない。平滑化の値が低いほど、ストリームの品質は高くなるが、流動性はないように見える。

4.2 ROI

ROI (Region of Interest)符号化は、ビデオ圧縮においてROIと背景情報とを識別するのに役立つ。この技術は、より多くの符号化リソースを関心領域に割り当て、したがって、ROIの品質を向上させるが、背景情報はあまり焦点が当てられていない。

4.2.1 ROI設定

ROI (関心領域)符号化は、より多くの符号化リソースを関心領域に割り当てるのに役立ち、したがって、ROIの品質を向上させるのに役立つが、背景情報はあまり焦点が当てられない。

開始前に

ビデオコーディングの種類を確認してください。ROIは、ビデオ符号化タイプがH.264またはH.265である場合にサポートされる。

手順

1. 設定→ビデオ/オーディオ→ ROI に移動します。
2. 有効をチェックします。
3. ストリームタイプを選択します。
4. ROI領域を描画するには、Fixed RegionでRegion No.を選択します。
   1) Draw Area をクリックします。

2) ビュー画面上でマウスをクリックしてドラッグし、固定領域を描画します。
3) Stop Drawingをクリックします。

注

調整する必要がある固定領域を選択し、マウスをドラッグして位置を調整します。

5. Region Name とROI Level を入力します。
6. 保存をクリックします。

注

ROIレベルが高いほど、検出された領域の画像はより鮮明になる。

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

4.2.2 顔追跡ROIの設定

ROIで顔追跡機能を有効にし、ライブピクチャに顔が現れると、顔の画像は周囲よりも鮮明になる。

手順

1. ROI設定ページ:設定→ビデオ/オーディオ→ ROIに移動します。
2. [Enable Face Tracking]をチェックします。
3. 動的領域でROIレベルを選択します。

注

ROIレベルは、画質向上レベルを意味する。値が大きいほど、画質は良好となる。

4. 保存をクリックします。

4.2.3 目標追跡ROIの設定

動くターゲットは、機能を有効にした後、ライブ画像または録画中の他の領域よりも明確になります。

開始前に

「設定→」→「スマートトラッキング」に移動して、スマートトラッキング設定を完了します。

手順

1. 設定→ビデオ/オーディオ→ ROI に移動します。
2. 「ターゲット追跡を有効にする」をオンにします。
3. 目標追跡のためにROIレベルを設定する。値が高いほど、ターゲットは明確である。

4. 保存をクリックします。

4.2.4 ライセンスプレート追跡ROIの設定

ナンバープレート追跡ROI機能が有効になっており、ライブ画像にナンバープレートが表示されている場合、ナンバープレートの画像は周囲の画像よりも鮮明になります。

手順

1. ROI設定ページ:設定→ビデオ/オーディオ→ ROIに移動します。
2. ライセンスプレート追跡を有効にするをチェックします。
3. 動的領域でROIレベルを選択します。

注

ROIレベルは、画質向上レベルを意味する。値が大きいほど、画質は良好となる。

4. 保存をクリックします。

4.3 ストリームに情報を表示する

オブジェクト(例えば、人間、車両等)の情報は、ビデオストリームにおいてマークされる。接続されたリアエンドデバイスまたはクライアントソフトウェアにルールを設定して、回線の交差や侵入などのイベントを検出できます。

手順

1. 設定ページ:ストリームの設定→ビデオ/オーディオ→ディスプレイ情報に移動します。
2. Dual-VCA を有効にするをチェックします。
3. 保存をクリックします。

4.4 オーディオ設定

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

4.4.1 オーディオエンコーディング

オーディオのオーディオエンコード圧縮を選択します。

4.4.2 オーディオ入力

注

- 必要に応じて、オーディオ入力デバイスを接続します。
- オーディオ入力表示は、機器の機種によって異なります。

ラインイン	MP3、シンセサイザ、アクティブピックアップなど、オーディオ入力デバイスが高出力で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LineInに設定します。
MicIn	マイクやパッシブピックアップなど、出力電力の低いオーディオ入力機器に接続したときに、オーディオ入力をMicInに設定します。

4.4.3 音声出力

注

必要に応じて、オーディオ出力デバイスを接続します。

これは、デバイス音声出力のスイッチである。無効にすると、すべてのデバイスオーディオが出力できなくなります。音声出力表示は、デバイスモードによって異なります。

4.4.4 環境ノイズフィルタ

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

4.5 双方向オーディオ

これは、監視画面において監視センタとターゲットとの間の双方向音声機能を実現するために使用される。

開始前に

- 装置に接続されている音声入力装置(ピックアップまたはマイク)および音声出力装置(スピーカ)が正常に動作していることを確認します。機器接続用オーディオ入出力機器の仕様を参照

してください。

- マイクとスピーカを内蔵している場合は、直接双方向音声機能を有効にすることができます。

手順

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

4.6 設定を表示する

これは、画像特徴を調整するためのパラメータ設定を提供する。
「コンフィギュレーション→のイメージ→ディスプレイ設定」に移動します。
デフォルトをクリックして設定を復元します。

4.6.1 シーンモード

異なる設置環境に対して予め定義された画像パラメータのいくつかのセットがある。実際の設置環境に合わせてシーンを選択し、表示設定を高速化します。

画像調整

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

露出設定

露出は、アイリス、シャッター、および光感度の組み合わせによって制御される。露出パラメータを設定することで、画像効果を調整できます。
手動モードでは、露出時間、ゲイン、スローシャッターを設定する必要があります。

フォーカス

フォーカスモードを調整するオプションを提供します。

フォーカスモード

自動

装置は、シーンが変化するにつれて自動的に焦点を合わせる。オートモードでピントの合ったイメージが得られない場合は、イメージの光源を減らし、可視光の点滅を避けてください。

セミオート

PTZ およびレンズのズーム後、デバイスは一度フォーカスします。画像が鮮明である場合、シーンが変化しても焦点は変化しない。

マニュアル

ライブビューページでフォーカスを手動で調整できます。

デイ/ナイトスイッチ

デイ/ナイトスイッチ機能はデイモードでカラー画像を提供し、ナイトモードでフィルライトをオンにすることができます。スイッチモードは設定可能です。

日

画像は常にカラーである。

夜

画像は、黒/白又はカラフルであり、補助光は、夜間に明瞭なライブビュー画像を保証することが可能になる。

注

特定のデバイスモデルのみが、補助光および色彩豊かな画像をサポートする。

自動

照度に応じてデイモードとナイトモードが自動的に切り替わります。

Scheduled-Switch

開始時刻と終了時刻を設定して、日モードの期間を定義します。

注

Day/Night Switch 機能はモデルによって異なります。

グレースケール

グレースケールの範囲は[0-255]または[16-235]に設定できます。

回転

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を720×1280に回転させる。
この機能を有効にすると、モニタリングの有効範囲を垂直方向に変更できます。

レンズの歪み補正

電動レンズ搭載機器では、画像がある程度歪んで見えることがあります。歪みを補正するには、この関数を有効にします。

注

- この機能は、電動レンズを備えた特定の装置によってのみサポートされる。
- この機能を有効にすると、画像のエッジが失われます。

BLC

強いバックライトに焦点を合わせると、被写体が暗すぎてはっきりと見えなくなります。BLC (backlight compensation)は、前方の物体に対する可視光を補償して明確にする。BLCモードがカスタムに設定されている場合は、ライブビュー画像上にBLC領域として赤い矩形を描画できます。

WDR

WDR (ワイドダイナミックレンジ)機能は、カメラが強い照度差のある環境で鮮明な画像を提供するのに役立ちます。
視野内に非常に明るい領域と非常に暗い領域が同時にある場合は、WDR機能を有効にし、レベルを設定できます。WDR は、画像全体の明るさレベルのバランスを自動的に調整し、より詳細な鮮明な画像を提供します。

注

WDR を有効にすると、他の一部の機能がサポートされなくなる場合があります。詳細は、実際のインタフェースを参照してください。

HLC

画像の明るい部分が露出過多で、暗い部分が露出不足の場合、HLC (High Light Compression)機能を有効にすると、明るい部分を弱め、暗い部分を明るくすることができ、画像全体の光のバランスをとることができます。

ホワイトバランス

ホワイトバランスとは、カメラの白演出機能です。これは、環境に応じて色温度を調整するために使用される。

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、画質を向上させるために使用します。ノーマルモードとエキスパートモードを選択できます。

通常

騒音低減度を制御するDNR レベルを設定します。レベルが高いほど、還元度が強いことを意味する。

専門家

空間DNR、時間DNRともにDNRレベルを設定し、騒音低減度を制御する。レベルが高いほど、還元度が強いことを意味する。

デフォグ

環境が曇り、画像がミストのときにデフォッグ機能を有効にできます。それは、画像がより明瞭に見えるように、微妙な細部を強調する。

EIS

ジッタ補償技術を用いて、映像の安定性を高める。

鏡

ライブビュー画像が実際のシーンの反転である場合、この機能は、画像を正常に表示するのに役立つ。
必要に応じてミラーモードを選択します。

注

機能を有効にすると、ビデオ録画はすぐに中断されます。

4.6.2 画像パラメータスイッチ

設定した時間帯に自動的に画像パラメータを切り替えます。
イメージパラメータ切り替え設定ページ:コンフィギュレーション→イメージ→イメージパラメータスイッチに移動し、必要に応じてパラメータを設定します。

SETスイッチ

一定時間内に自動的に画像パラメータをシーンに切り替えます。

手順

1. 有効をチェックします。
2. 対応する期間とシーンを選択して設定します。

注

シーン構成については、「シーンモード」を参照してください。

3. 保存をクリックします。

4.6.3 ビデオ標準

ビデオ標準は、表示される色の量と解像度を定義するビデオカードまたはビデオディスプレイデバイスの機能です。使用される最も一般的なビデオ規格は、NTSC とPAL の2 つです。NTSCでは、毎秒30 フレームが送信されます。各フレームは、525本の個々の走査線から構成される。PALでは、毎秒25フレームが送信される。各フレームは、625本の個々の走査線から構成される。国/地域のビデオシステムに応じてビデオ信号規格を選択します。

4.6.4 ローカルビデオ出力

BNC、CVBS、HDMI、SDIなどのビデオ出力インタフェースを搭載している場合は、モニタ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。
出力を制御するON/OFF として出力モードを選択します。

4.7 OSD

ビデオストリームに表示されるデバイス名、時間/日付、フォント、色、テキストオーバーレイなどのOSD (オンスクリーンディスプレイ)情報をカスタマイズできます。
OSD設定ページ:設定→のイメージ→ OSD設定に進みます。対応するパラメーターを設定し、「保存(Save)」をクリックして有効にします。

文字集合

表示情報の文字セットを選択します。韓国語を画面に表示する場合は、EUC-KRを選択します。それ以外の場合は、GBK を選択します。

表示情報

カメラ名、日付、週、関連する表示形式を設定します。

テキストオーバーレイ

画像にカスタマイズしたオーバーレイテキストを設定します。

OSD パラメータ

表示モード、OSDサイズ、フォントカラー、配置などのOSDパラメータを設定します。

4.8 プライバシーマスクの設定

この機能は、プライバシーを保護するためにライブビュー内の特定の領域をブロックする。装置がどのように動いても、ブロックされたシーンは決して見えない。

手順

1. プライバシーマスク設定ページ:コンフィギュレーション→イメージプライバシーマスクに移動します。
2. プライバシーマスクを有効にするをチェックします。
3. Draw Area をクリックします。ライブビューでマウスをドラッグして、閉じた領域を描画します。

エリアの角をドラッグします。	領域のサイズを調整します。
領域をドラッグする	エリアの位置を調整します。
Clear Allをクリックする	設定したすべての領域をクリアします。

4. Stop Drawingをクリックします。
5. 保存をクリックします。

4.9 オーバレイ画像

カスタマイズした画像をライブビューにオーバーレイします。

開始前に

オーバーレイするピクチャは、24ビットのBMPフォーマットでなければならず、最大ピクチャサイズは128×128ピクセルである。

手順

1. 画像オーバーレイ設定ページ:設定→画像→画像オーバーレイに移動します。
2. 参照をクリックして画像を選択し、アップロードをクリックします。
   アップロードに成功すると、赤い長方形のピクチャがライブビューに表示されます。
3. 画像オーバーレイを有効にするをオンにします。
4. ピクチャをドラッグして位置を調整します。
5. 保存をクリックします。

4.10 目標作付設定

画像の切り抜き、ターゲット領域の画像のみの送信と保存を行って、送信帯域幅とストレージを節約することができます。

手順

1. 「コンフィギュレーション→ビデオ/オーディオ→対象クロップ」に移動します。
2. 「ターゲットの切り抜きを有効にする」をオンにし、「3 番目のストリーム」を「ストリームタイプ」に設定します。

注

ターゲットクロップを有効にした後、3 番目のストリーム解像度を設定することはできません。

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

注

- ターゲット切り出しに対応しているモデルは一部のみで、機能はカメラのモデルによって異なります。
- ターゲットクロップを有効にすると、一部の機能が無効になる場合があります。

第 5 章ビデオ録画とピクチャキャプチャ

ここでは、ビデオクリップやスナップショットの取り込み、再生、取り込んだファイルのダウンロードの操作について説明します。

5.1 ストレージ設定

この部分は、いくつかの共通ストレージ経路の構成を導入する。

5.1.1 新規または未暗号化メモリカードの設定

開始前に

新しいまたは暗号化されていないメモリカードをデバイスに挿入します。インストールの詳細については、デバイスのクイックスタートガイドを参照してください。

手順

1. 構成→のストレージ→のストレージ管理→のHDD 管理に移動します。
2. メモリカードを選択します。

注

ロック解除ボタンが表示された場合は、まずメモリカードのロックを解除する必要があります。詳細は、「メモリカードステータスの検出」を参照してください。

---

3. 「フォーマット」をクリックして、メモリーカードを初期化します。
   メモリカードの状態が初期化されていない状態から正常状態になると、メモリカードは使用可能な状態になります。
4. オプション: メモリカードを暗号化します。
   1) 暗号化形式をクリックします。
   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。
      Encryption Status(暗号化ステータス)が Encrypted(暗号化済み)に変わると、メモリカードは使用可能な状態になります。

注

暗号化パスワードは適切に保管してください。暗号化パスワードを忘れた場合は見つけられません。

---

5. オプション: メモリカードのクォータを定義します。お客様のご要望に応じて、異なるコンテンツを保存する割合を入力します。

6. 保存をクリックします。

メモリカード状態検出

デバイスはHikvisionメモリカードのステータスを検出します。メモリカードの異常を検出すると、通知を受信します。

開始前に

設定ページは、デバイスにHikvisionメモリカードが取り付けられている場合にのみ表示されます。

手順

1. 設定→保存→保存管理→メモリカード検知に移動します。
2. Status Detection(ステータス検出)をクリックして、メモリカードの残りの寿命と正常性ステータスを確認します。

残存寿命

それは残存寿命のパーセンテージを示す。メモリカードの寿命は、その容量およびビットレートのような要因によって影響され得る。残りの寿命が足りない場合は、メモリーカードを交換する必要があります。

ヘルス状況

メモリカードの状態が表示されます。ステータスには、良、不良、破損の3つの記述があります。アーミングスケジュールおよびリンクメソッドが設定されている場合、ヘルスステータスが正常以外の場合は、通知を受け取ります。

注

正常性状態が「良好」でない場合は、メモリカードを変更することをお勧めします。

3. 「R/Wロック」をクリックして、メモリカードの読み込み/書き込みの許可を設定します。
    1. LockSelect を追加して、Lock Switch をON にします。
    2. パスワードを入力します。
    3. 保存をクリックする

ロック解除

- ロックをかけた機器でメモリカードを使用すると、自動的にロック解除が行われ、ユーザー側でのロック解除手順は不要になります。
- 別の機器でメモリカード(ロック付き)を使用する場合は、HDD管理に進み、手動でメモリカードのロックを解除することができます。メモリカードを選択し、「ロック解除」をクリックします。正しいパスワードを入力してロックを解除します。
    1. ロックスイッチを「OFF」にしてロック選択を解除します。
    2. パスワード設定にパスワードを入力します。
    3. 保存をクリックします。

注

- 管理者ユーザのみがR/Wロックを設定できます。
- メモリカードの読み出し/書き込みは、ロックが解除されているときのみ可能です。
- メモリーカードにロックをかける機器を工場出荷時の状態に戻すと、HDD Managementでメモリーカードのロックを解除することができます。

4. 準備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、「準備スケジュールの設定」および「リンク方法の設定」を参照してください。
5. 保存をクリックします。

5.1.2 FTPの設定

イベントまたは時間指定スナップショットタスクによってキャプチャされたイメージを保存するようにFTP サーバを設定できます。

開始前に

最初にFTP サーバアドレスを取得します。

手順

1. 「コンフィギュレーション→ネットワーク 詳細設定」→「FTP」に移動します。
2. FTP 設定を構成します。

FTP プロトコル

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

サーバアドレスとポート

FTP サーバアドレスと対応するポート。

ユーザー名とパスワード

FTP ユーザーには、画像をアップロードする権限が必要です。
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は、Anonymous(匿名)をオンにすると、アップロード中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 サーバ内のスナップショットの保存パス。

ピクチャファイル間隔

写真管理を改善するには、写真ファイリング間隔を1日から30日に設定します。同じ時間間隔で撮影した画像は、時間間隔の開始日時と終了日時の名前が付けられた1つのフォルダに保存されます。

ピクチャ名

撮影した画像の命名規則を設定します。ドロップダウンリストでDefault を選択して、デフォル

トルール、つまりIP address_channel number_capture time_event type.jpg を使用できます。(例: 10.11.37.189_01_20150917094425492_FACE_DETECTION.jpg)。または、デフォルトの命名ルールにカスタムプレフィックスを追加してカスタマイズすることもできます。

3. FTP サーバーへのスナップショットのアップロードを有効にするには、画像のアップロードをオンにします。
4. 自動ネットワーク補充を有効にするをオンにします。

注

連携方法のFTP/メモリカード/NASへのアップロードと自動ネットワーク補充の有効化は、両方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 サーバを確認します。
6. 保存をクリックします。

5.1.3 NASの設定

ネットワークサーバーをネットワークディスクとして取得し、録画ファイルやキャプチャ画像などを保存します。

開始前に

最初にネットワークディスクのIP アドレスを取得します。

手順

1. NAS 設定ページ:構成→ストレージ域管理→ネットHDD に移動します。
2. 「HDD No.」をクリックします。ディスクのサーバーアドレスとファイルパスを入力します。

サーバーアドレス

ネットワークディスクのIP アドレス。

ファイルパス

ネットワークディスクファイルの保存パス。

取付形式

オペレーション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 を選択した場合のセキュリティを保証するには、ネットHDD のユーザー名とパスワードを入力します。

3. Test(テスト)をクリックして、ネットワークディスクが使用可能かどうかを確認します。
4. 保存をクリックします。

5.1.4 eMMC保護

eMMCの健康状態が悪い場合、ストレージ媒体としてのeMMCの使用を自動的に停止することである。

注

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

設定については、「構成→システム→保守システムサービス」を参照してください。
eMMCは、組み込みマルチメディアカードの略で、組み込み型不揮発性メモリシステムです。それは、装置の捕捉された画像又はビデオをストレージすることができる。
デバイスは、eMMCの健全性ステータスを監視し、そのステータスが悪いときにeMMCをオフにする。さもなければ、摩耗したeMMCを使用することは、デバイスブート障害につながる可能性がある。

5.1.5 クラウドストレージの設定

これは、キャプチャされた写真およびデータをクラウドにアップロードするのに役立つ。プラットフォームは、画像および分析のためにクラウドから画像を直接要求する。この関数は、特定のモデルによってのみサポートされます。

手順

注意

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

1. 「構成→ Storage → Storage Management → Cloud Storage」に移動します。
2. Cloud Storage を有効にするをチェックします。
3. 基本パラメータの設定を行います。

プロトコルバージョン	クラウドビデオマネージャ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のIP アドレス。IPv4アドレスをサポートします。
サーブポート	クラウドビデオマネージャのポート。デフォルトのポートを使用することをお勧めします。
AccessKey	クラウドビデオマネージャにログインするためのキー。
シークレットキー	クラウドビデオマネージャに保存されているデータを暗号化するためのキー。

ユーザー名とパスワード	クラウドビデオマネージャのユーザー名とパスワード。
Picture Storage Pool ID	クラウドビデオマネージャの画像保存領域のID。ストレージ・プールIDとストレージ・リージョンIDが同じであることを確認してください。

4. Test(テスト)をクリックして、設定をテストします。
5. 保存をクリックします。

5.2 ビデオ録画

録画済みファイルのマニュアル録画、スケジュール録画、再生、ダウンロードの動作を紹介します。

5.2.1 自動的に記録する

この機能は、設定した時間帯にビデオを自動的に録画することができます。

開始前に

Continuous 以外の各レコードタイプのイベント設定でTrigger Recording 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→保存→予約設定→記録予約に移動します。
2. 有効をチェックします。
3. レコードタイプを選択します。

注

レコードの種類は、モデルによって異なります。

連続

映像は、スケジュールに従って連続的に録画されます。

モーション

動き検出が可能であり、トリガ記録がリンク方法として選択されると、オブジェクトの動きが記録される。

アラーム

アラーム入力を有効にして、連動方式にトリガー録画を選択した場合、外部アラーム入力機器からアラーム信号を受けてから映像を録画します。

Motion |アラーム

動きを検知したときや、外部アラーム入力機器からアラーム信号を受信したときに、映像を記録します。

モーション&アラーム

動きを検知し、外部アラーム入力機器からアラーム信号を受信した場合のみ、映像を記録します。

イベント

設定されたイベントが検出されると、ビデオが記録されます。

4. 選択したレコード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、「アーミングスケジュールの設定」を参照してください。
5. 詳細設定を設定するには、詳細をクリックします。

上書き

保存領域がいっぱいになったときにビデオレコードを上書きするには、「上書き」を有効にします。それ以外の場合、カメラは新しいビデオを記録することができない。

プリレコード

スケジュールされた時刻の前に記録するように設定した期間。

ポストレコード

予定時刻以降に録画を中止するように設定した時間。

ストリームタイプ

記録するストリームの種類を選択します。

注

ビットレートが高いストリームタイプを選択すると、プリレコードとポストレコードの実際の時間が設定値よりも小さくなる場合があります。

録音期限

録音が有効期限を超えると、録音は削除されます。有効期限は設定可能です。いったん録音内容を消去すると、元に戻すことはできませんのでご注意ください。

6. 保存をクリックします。

5.2.2 手動で記録する

手順

1. 「設定→ローカル」に移動します。
2. 録音ファイルのファイルサイズと保存パスを設定します。
3. 保存をクリックします。
4. ライブビューインターフェースをクリックして録画を開始します。録音を中止するにはクリックします。

5.2.3 ライト・ストレージの設定

ライト・ストレージが有効にされた後、ビデオストリームのフレームレートとビットレートを減少させて、監視シナリオに移動物体がないときのメモリカードのストレージ時間を長くすることができる。

手順

1. 「構成→ストレージ・→・ストレージ・マネジメント・→・ライト・ストレージ」に移動します。
2. [有効]をチェックし、レベルを設定します。レベルが高いほど、フレームレートおよびビットレートは大きく、推奨ストレージ時間は短い。
3. 保存期間を設定するデバイスは自動的にビットレートを計算し、メモリカードの容量とレベルに応じて推奨されるストレージ時間を提供します。保存時間をおすすめ時間に設定することをおすすめします。

注

- ライトストレージが有効な場合、フォーマットされていないメモリカードは自動的にフォーマットされます。
- メモリーカードの表示可能な空き容量は、ストレージ域→のストレージ域管理→割り当てのレコードの割合に従って、既定で割り当てられます。必要に応じて調整できます。
- 特定のデバイスモデルのみがこの機能をサポートする。

5.2.4 動画の再生とダウンロード

ローカルストレージやネットワークストレージに保存されている動画を検索、再生、ダウンロードできます。

手順

1. 再生をクリックします。
2. 検索条件を設定し、「検索」をクリックします。
   マッチしたビデオファイルがタイミングバーに表示されました。
3. クリックすると、動画ファイルが再生されます。▶
   - クリックしてビデオファイルをクリップします。✂
   - ライブビュー画像をダブルクリックすると、動画ファイルがフルスクリーンで再生されます。ESCを押して全画面を終了します。

注

「構成→ローカル」に移動し、「クリップを保存」を選択して、クリップされたビデオファイルの保存先を変更します。

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

注

設定→ローカルに移動し、ダウンロードしたファイルの保存をクリックして、ダウンロードしたビデオファイルの保存先を変更します。

5.3 キャプチャ設定

デバイスは、手動または自動で写真をキャプチャし、構成された保存経路にそれらを保存することができる。スナップショットを表示およびダウンロードできます。

5.3.1 自動的に取り込む

設定した時間帯に自動的に画像を取り込む機能です。

開始前に

イベントトリガによるキャプチャが必要な場合は、イベント設定で関連するリンケージ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. 「構成→ストレージ域→予定設定→キャプチャ」の「キャプチャ」パラメータに移動します。
2. キャプチャの種類を設定します。

   タイミング

   設定した時間間隔でピクチャを取り込みます。

   イベント・トリガー

   イベントがトリガーされたときに画像をキャプチャします。
3. フォーマット、解像度、品質、間隔、キャプチャ番号を設定します。
4. スケジュール時間の設定については、「準備スケジュールの設定」を参照してください。
5. 保存をクリックします。

5.3.2 マニュアルで取り込む

手順

1. 「設定→ローカル」に移動します。
2. スナップショットのイメージ形式と保存パスを設定します。

   JPEG

   このフォーマットのピクチャサイズは比較的小さく、これはネットワーク伝送にとってより良好である。

   BMP

画像は良好な品質で圧縮される。
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をクリックして、手動で画像をキャプチャします。

5.3.3 タイミングウェイクの設定

装置は、スリープしているとき、設定された時間間隔でウェイクアップし、写真をキャプチャし、それらをアップロードする。

手順

> **注**
>
> この関数は、特定のデバイスモデルによってのみサポートされます。

1. 電力消費モードの→の「設定→システム設定」の「スリープスケジュール」で、「スリープキャプチャ間隔」を設定するタイムスケジュールを選択します。
2. 設定→イベント→基本イベント→タイミングウェイクに入ります。
3. 有効をチェックします。
4. キャプチャタイプを選択します。
5. 連動方法の設定については、「連動方法の設定」を参照してください。
6. 保存をクリックします。

結果

デバイスは、設定されたスリープキャプチャ間隔でウェイクアップし、写真をキャプチャし、それらをアップロードする。

5.3.4 ピクチャの表示とダウンロード

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

手順

1. ピクチャをクリックします。
2. 検索条件を設定し、「検索」をクリックします。
   マッチしたピクチャがファイルリストに表示されます。
3. 画像を選択し、Download(ダウンロード)をクリックしてダウンロードします。

> **注**
>
> 設定→ローカルに移動し、再生時にスナップショットを保存を選択して画像の保存先を変更します。

第 6 章イベントとアラーム

このパートでは、イベントの構成について説明します。装置は、トリガされたアラームに一定の応答を取る。

6.1 基本事象

6.1.1 動体検知の設定

これは、検出領域内の移動物体を検出し、連動動作をトリガするのに役立つ。

手順

1. 「設定→イベント→基本イベント→動作検知」に進みます。
2. [動作検出を有効にする]をチェックします。
3. オプション: 画像内の移動オブジェクトを緑色で表示するには、ハイライトします。
   1) 動作の動的分析を有効にするをチェックします。
   2) 「設定→ローカル」に移動します。
   3) ルールを有効に設定します。
4. 「構成モード」を選択し、ルール・リージョンとルール・パラメーターを設定します。
   – ノーマルモードについては、「ノーマルモード」を参照してください。
   – エキスパートモードについては、「エキスパートモード」を参照してください。
5. アーミングスケジュールとリンク方法を設定します。アーミングスケジュールの設定については、「アーミングスケジュールの設定」を参照してください。連動方法については、「連動方法の設定」を参照してください。
6. 保存をクリックします。

エキスパートモード

実際のニーズに応じて、昼夜別の動き検出パラメータを設定できます。

手順

1. 設定でエキスパートモードを選択します。
2. エキスパートモードのパラメータを設定します。

予約画像の設定

OFF

画像切り替えができません。

オートスイッチ

環境に応じて昼夜モードを自動的に切り替えます。昼間はカラー画像、夜間は白黒画像を表示します。

Scheduled-Switch

スケジュールに応じて昼夜モードを切り替えます。設定期間中はデイモードに切り替わり、それ以外の期間はナイトモードに切り替わります。

感度

感度の値が高いほど、動き検出の感度が高い。スケジュール設定が有効になっている場合は、昼夜別に設定できます。

3. エリアを選択し、Draw Area 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、マウスを放して1 つの領域の描画を終了します。

図 6-1 ルールの設定

描画の停止 1エリアの描画を終了します。

すべてクリア すべての領域を削除します。

4. 保存をクリックします。
5. (オプション) 上記の手順を繰り返して、複数のエリアを設定します。

通常モード

動作検出パラメータは、デバイスのデフォルトパラメータに従って設定できます。

手順

1. Configurationでnormalモードを選択します。

2. ノーマルモードの感度を設定します。感度の値が高いほど、動き検出の感度が高い。感度が0に設定されている場合、動き検出および動的解析は効果を発揮しない。
3. Detection Target を設定します。ヒトおよびビヒクルが利用可能である。検出ターゲットが選択されない場合、人間及び車両を含む全ての検出ターゲットが報告される。
4. Draw Area をクリックします。ライブビデオ上でマウスをクリックしてドラッグし、マウスを放して1つの領域の描画を終了します。

   描画の停止　　1 つの領域の描画を停止します。

   すべてクリア　　すべての領域をクリアします。

5. (オプション) 上記の手順を繰り返すことで、複数の領域のパラメータを設定できます。

6.1.2 ビデオ・タンパリング・アラームを設定する

設定されたエリアがカバーされており、正常に監視できない場合、アラームがトリガされ、デバイスは特定のアラーム応答動作を行う。

手順

1. 設定→イベント→基本イベント→ビデオ改ざんに移動します。
2. 有効をチェックします。
3. 感度を設定します。この値が大きいほど、面積被覆の検出が容易になる。
4. Draw Area をクリックし、ライブビューでマウスをドラッグして領域を描画します。

   描画の停止　　描画を終了します。

   すべてクリア　　描画されたすべての領域を削除します。

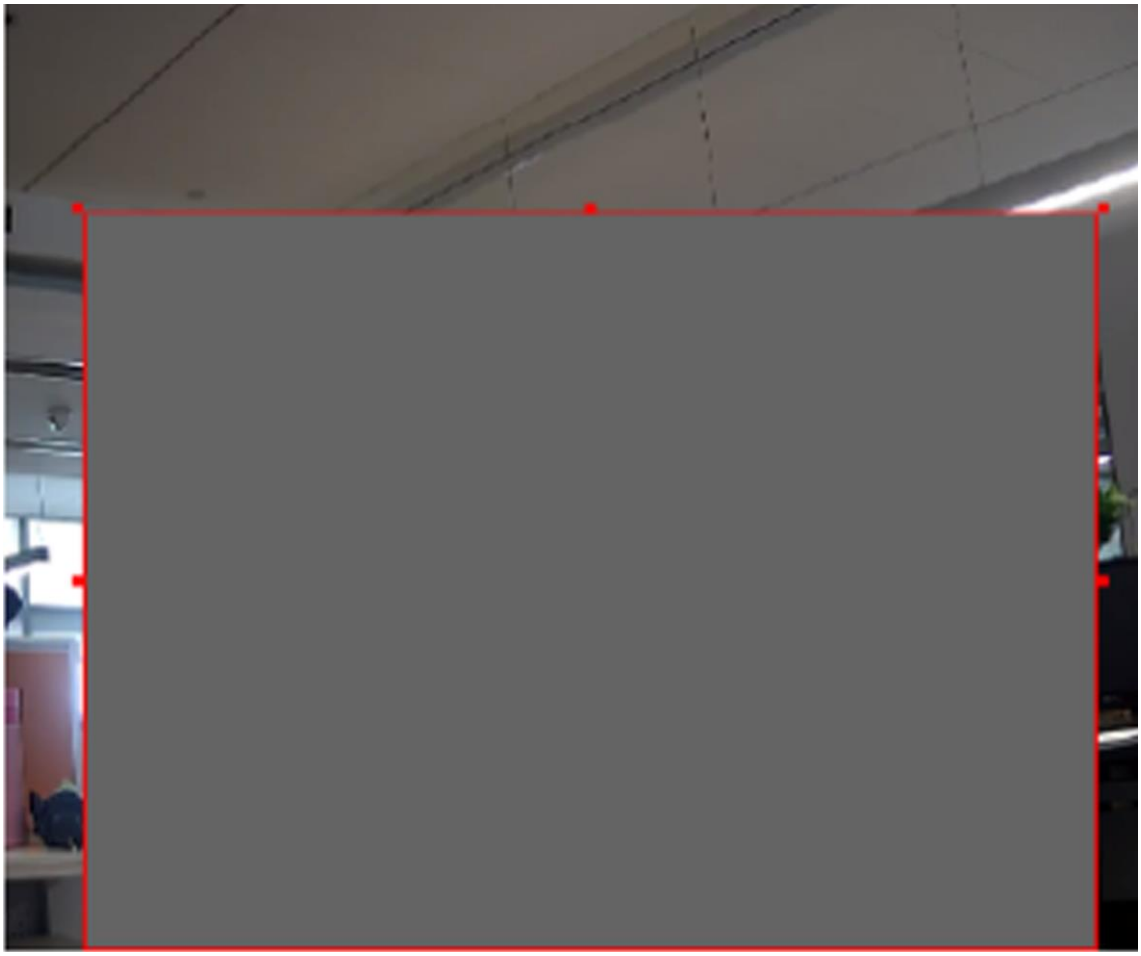

図 6-2 ビデオ・タンパリング・エリアの設定

5. スケジュール時間の設定は、「アーミングスケジュールの設定」を参照してください。連携方法の設定については、「連携方法の設定」を参照してください。
6. 保存をクリックします。

6.1.3 PIRアラームを設定する

侵入者が検出器の視野内を移動すると、PIR（受動赤外線）アラームがトリガーされます。ヒト、またはイヌ、ネコなどの任意の他の温血生物によって放散される熱エネルギーを検出することができる。

手順

注

PIRアラームに対応している機種は一部のみです。

1. 「構成→高度構成→基本事象→ PIRアラーム」に進みます。
2. 「PIRアラームを有効にする」をチェックします。

3. スケジュール時間の設定は、「アーミングスケジュールの設定」を参照してください。連携方法の設定については、「連携方法の設定」を参照してください。
4. 保存をクリックします。

6.1.4 例外アラームを設定する

ネットワーク切断などの例外によって、デバイスが対応するアクションを実行することができます。

手順

1. 「設定→イベント→基本イベント 除外」に移動します。
2. 例外タイプを選択します。

HDD フル	HDD ストレージがいっぱいです。
HDD エラー	HDD にエラーが発生しました。
ネットワーク切断	デバイスはオフラインです。
IP アドレスの競合	現在の機器のIPアドレスは、ネットワーク内の他の機器のIPアドレスと同じです。
不正ログイン	ユーザー名またはパスワードの入力が間違っている。
電圧不安定	電源電圧が変動している。

3. 連携方法の設定については、「連携方法の設定」を参照してください。
4. 保存をクリックします。

6.1.5 アラーム入力の設定

外部装置からのアラーム信号は、現在の装置の対応する動作をトリガする。

開始前に

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

手順

1. 構成→イベント→基本イベント→アラームインプットに進みます。
2. 「アラーム入力処理を有効にする」をチェックします。
3. ドロップダウンリストから[アラーム入力番号]と[アラームタイプ]を選択します。アラーム名を編集します。
4. スケジュール時間の設定は、「アーミングスケジュールの設定」を参照してください。連携方法の設定については、「連携方法の設定」を参照してください。
5. [コピー先。。.]をクリックして、他のアラーム入力チャンネルに設定をコピーします。
6. 保存をクリックします。

6.1.6 ビデオ品質診断の設定

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

手順

1. →イベント→基本イベント→画質診断に進みます。
2. Diagnosis Type を選択します。
3. 対応するパラメータを設定します。

アラーム検出間隔

例外を検出する時間間隔。

感度

値が高いほど、例外が検出されやすくなり、誤情報の可能性が高くなる。

アラーム遅延時間

アラームが設定された回数に達すると、装置はアラームをアップロードする。

4. [有効]をチェックすると、選択した診断タイプが検出されます。
5. アーミングスケジュールを設定します。準備スケジュールの設定を参照してください。
6. リンク方法を設定します。リンク方法の設定を参照してください。
7. 保存をクリックします。

注

この関数は、特定のモデルによってのみサポートされます。実際の表示は機種によって異なります。

6.1.7 振動検出を設定する

これは、装置が振動しているかどうかを検出するために使用される。デバイスは、アラームを報告し、機能がイネーブルされている場合、リンケージアクションをトリガする。

手順

1. →イベント→基本イベント→振動検知に進みます。
2. 有効をチェックします。
3. スライダをドラッグして検出感度を設定します。また、数字を入力して感度を設定することもできます。
4. アーミングスケジュールを設定します。準備スケジュールの設定を参照してください。
5. リンク方法を設定します。リンク方法の設定を参照してください。
6. 保存をクリックします。

注

この関数は、特定のモデルによってのみサポートされます。実際の表示は機種によって異なります。

6.2 スマートイベント

注

- 機種により機能が異なります。
- この機能を有効にするには、Smart Event on VCA Resourceページを選択する必要がある場合があります。特定のモデルでは、この関数はシングルチャネルモードでサポートされます。詳細は参照。
- 特定のモデルでは、スマートイベントが使用されているとき、EISは利用できない。

6.2.1 オーディオ例外の検出

音声例外検出機能は、音の強さの急激な増加/減少のような監視シーンにおける異常な音を検出し、いくつかのアクションが応答として取られることができる。

手順

1. 「設定→イベント→スマートイベントオーディオ例外検知」に移動します。
2. 1 つまたは複数のオーディオ例外検出タイプを選択します。

オーディオロス検出

オーディオトラックの突然の消失を検出します。

音量検出の急増

サウンド強度の急激な増加を検出します。Sensitivity および Sound Intensity Threshold は設定可能です。

注

- 感度が低ければ低いほど、検出をトリガーするための変化はより重要であるはずである。
- 音響インテンシティのしきい値とは、検出のための音響インテンシティの基準を指します。環境中の平均音響強度として設定することをお勧めします。環境音が大きければ大きいほど、その値は高くなければならない。実環境に合わせて調整できます。

音量検出の急激な低下

音響インテンシティの急激な低下を検知します。感度は設定可能です。

3. スケジュール時間の設定は、「アーミングスケジュールの設定」を参照してください。リンク方法の設定については、「リンク方法の設定」を参照してください。
4. 保存をクリックします。

注

機種により機能が異なります。

6.2.2 デフォーカス検出の設定

レンズの焦点ぼけによるぼけ画像を検出することができます。それが発生した場合、デバイスは、リンケージアクションをとることができる。

手順

1. 構成→イベント・→・スマート・イベント・→・デフォーカス検知に進む。
2. 有効をチェックします。
3. 感度を設定します。値が高いほど、焦点ぼけイメージがアラームをトリガーしやすくなります。実際の環境に合わせて値を調整することができます。
4. 連動方法の設定については、連動方法の設定を参照してください。
5. 保存をクリックします。

注

この関数は、特定のモデルによってのみサポートされます。実際の表示は機種によって異なります。

6.2.3 シーン変更の検出

シーン変化検出機能は、監視シーンの変化を検出する。アラームがトリガされると、いくつかのアクションを取ることができる。

手順

1. 「設定→イベント→スマートイベントシーン変更検知」に移動します。
2. 有効をクリックします。
3. 感度を設定します。この値が大きいほど、シーンの変化を検出しやすい。しかし、検出精度は低下する。
4. スケジュール時間の設定は、「アーミングスケジュールの設定」を参照してください。連携方法の設定については、「連携方法の設定」を参照してください。
5. 保存をクリックします。

注

機種により機能が異なります。

6.2.4 顔検出の設定

これは、検出領域内の顔を検出するのに役立つ。顔が検出されると、デバイスはリンクアクションをトリガーします。

手順

1. 「設定→の行動→スマートイベントフェイス検知」に移動します。
2. Enable Face Detectionをチェックします。
3. オプション: ハイライトして画像に顔を表示します。
   1）顔検出のために動的分析を有効にするをチェックします。
   2）「設定→ローカル」に移動し、「規則」を「有効」に設定します。
4. 感度を設定します。感度が低ければ低いほど、顔または不明瞭な顔のプロファイルを検出することはより困難である。
5. アーミングスケジュールとリンク方法を設定します。アーミングスケジュールの設定については、「アーミングスケジュールの設定」を参照してください。連動方法については、「連動方法の設定」を参照してください。
6. 保存をクリックします。

6.2.5 ビデオロスを設定する

この機能は、ビデオ信号の時間的損失を検出し、リンク動作をトリガすることができる。

手順

1. 設定→イベント→基本イベント→ビデオロスに移動します。
2. 有効をチェックします。
3. スケジュール時間の設定は、「アーミングスケジュールの設定」を参照してください。連携方法の設定については、「連携方法の設定」を参照してください。
4. 保存をクリックします。

6.2.6 セット侵入検出

あらかじめ定義された仮想領域に入ったり反復したりするオブジェクトを検出するために使用されます。それが発生した場合、デバイスは、リンケージアクションをとることができる。

手順

1. 「設定→イベント→スマートイベント→侵入検知」に進みます。
2. 有効をチェックします。

3. リージョンを選択します。検出領域の設定については、「Draw Area」を参照してください。
4. ルールを設定します。

感度	感度は、予め定義された領域に入る許容可能な標的の身体部分のパーセンテージを表す。感度 = 100 - S1/ST × 100。S1は、所定の領域を横切る目標身体部分を表す。STは、完全な標的体を表す。感度の値が高いほど、アラームをトリガーしやすくなります。
しきい値	「しきい値」は、領域内で反復するオブジェクトの時間のしきい値を表します。1つのオブジェクトが留まる時間が閾値を超える場合、アラームがトリガされる。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。
検出対象	ヒトおよびビヒクルが利用可能である。検出ターゲットが選択されない場合、人間及び車両を含む全ての検出ターゲットが報告される。
目標有効性	有効性を高く設定すると、必要なターゲット機能がより明確になり、アラーム精度が高くなります。あまり明白でない特徴を有する標的は、欠落しているであろう。

図 6-3 ルールの設定

5. (オプション) 上記の手順を繰り返すことで、複数の領域のパラメータを設定できます。
6. アーミングスケジュールの設定については、「アーミングスケジュールの設定」を参照してください。連動方法の設定については、連動方法の設定を参照してください。
7. 保存をクリックします。

6.2.7 ライン交差検出の設定

これは、所定の仮想線を横切る物体を検出するために使用される。それが発生した場合、デバイスは、リンケージアクションをとることができる。

手順

1. 構成→イベント・→・スマート・イベント・→行交差検知に進む。
2. 有効をチェックします。
3. 1行を選択し、サイズフィルタを設定します。サイズフィルタの設定については、「サイズフィルタの設定」を参照してください。
4. Draw Area をクリックすると、ライブビデオに矢印付きの線が表示されます。必要に応じて、ライブビデオ上の場所にラインをドラッグします。
5. ルールを設定します。

方向	それは、物体が線を横切る方向を表す。 A<->B:両方向から線を横切るオブジェクトを検出し、アラームをトリガすることができます。 A→B:A側からB側に構成線を横切る物体のみを検出することができる。 B→A:構成線をB側からA側に横切る物体のみを検出することができる。
感度	これは、予め定義された線を横切る許容可能なターゲットの身体部分のパーセンテージを表す。感度 = 100 - S1/ST × 100。S1は、所定の線を横切る目標身体部分を表す。STは、完全な標的体を表す。感度の値が高いほど、アラームをトリガーしやすくなります。
検出対象	ヒトおよびビヒクルが利用可能である。検出ターゲットが選択されない場合、人間及び車両を含む全ての検出ターゲットが報告される。
目標有効性	有効性を高く設定すると、必要なターゲット機能がより明確になり、アラーム精度が高くなります。あまり明白でない特徴を有する標的は、欠落しているであろう。

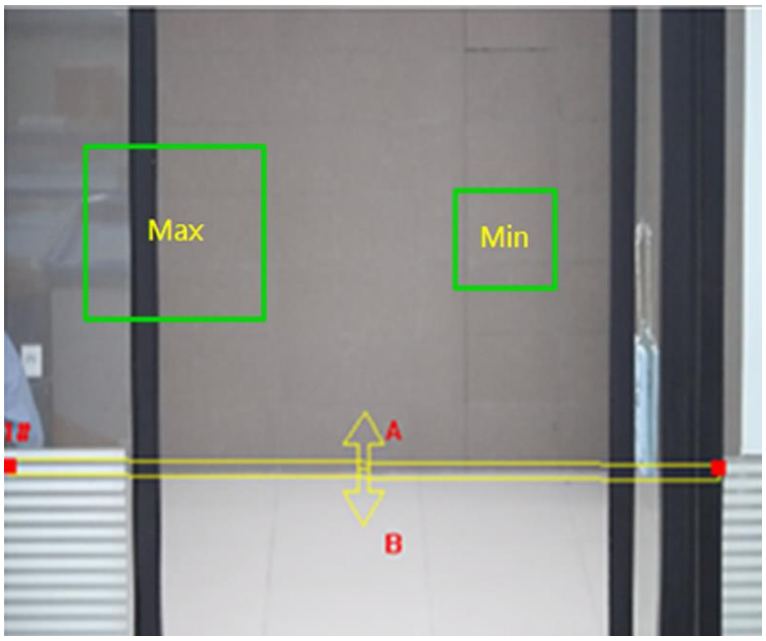

図 6-4 ルールの設定

6. (オプション) 上記の手順を繰り返すことで、複数の領域のパラメータを設定できます。
7. アーミングスケジュールの設定については、「アーミングスケジュールの設定」を参照してください。連動方法の設定については、連動方法の設定を参照してください。
8. 保存をクリックします。

6.2.8 領域入口検出の設定

外部から定義済みの仮想領域に入るオブジェクトを検出するために使用されます。それが発生した場合、デバイスは、リンケージアクションをとることができる。

手順

1. 構成→イベント→スマートイベント→リージョンエントランスディテクションに進みます。
2. 有効をチェックします。
3. リージョンを1つ選択します。リージョン設定については、「Draw Area」を参照してください。
4. 検出目標、感度、目標有効性を設定します。

感度	これは、予め定義された領域を横切る許容可能なターゲットの身体部分のパーセンテージを表す。感度 = 100 - S1/ST × 100。S1は、所定の領域を横切る目標身体部分を表す。STは、完全な標的体を表す。感度の値が高いほど、アラームをトリガーしやすくなります。
検出対象	ヒトおよびビヒクルが利用可能である。検出ターゲットが選択されない場合、人間及び車両を含む全ての検出ターゲットが報告される。
目標有効性	有効性を高く設定すると、必要なターゲット機能がより明確になり、アラーム精度が高くなります。あまり明白でない特徴を有する標的は、

欠落しているであろう。

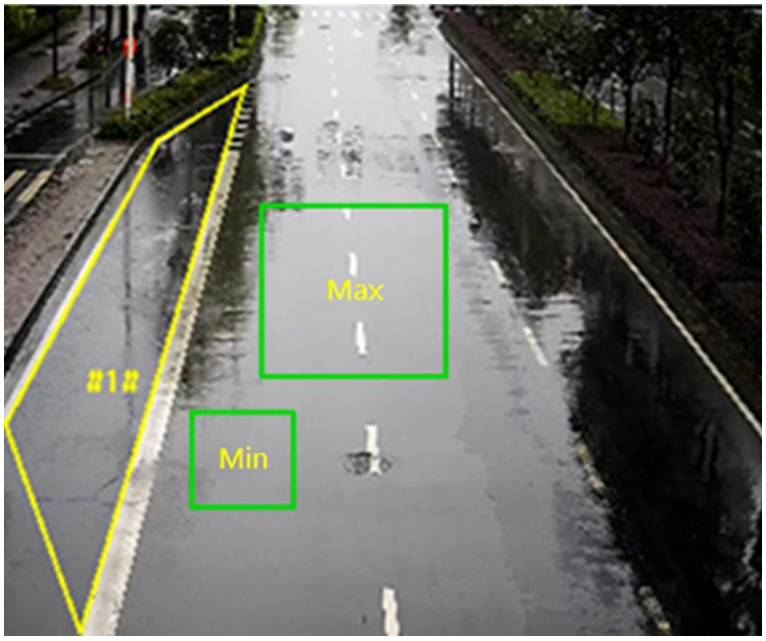

図 6-5 ルールの設定

5. (オプション) 上記の手順を繰り返すことで、複数の領域のパラメータを設定できます。
6. アーミングスケジュールの設定については、「アーミングスケジュールの設定」を参照してください。連動方法の設定については、連動方法の設定を参照してください。
7. 保存をクリックします。

6.2.9 領域退出の検出の設定

事前定義された仮想領域から出るオブジェクトを検出するために使用されます。それが発生した場合、デバイスは、リンケージアクションをとることができる。

手順

1. コンフィギュレーション→イベント→スマートイベントリージョン終了検知に移動
2. 有効をチェックします。
3. リージョンを1つ選択します。検出領域の設定については、「Draw Area」を参照してください。
4. 検出目標、感度、目標有効性を設定します。

感度 これは、予め定義された領域を横切る許容可能なターゲットの身体部分のパーセンテージを表す。感度 = 100 - S1/ST × 100。S1は、所定の領域を横切る目標身体部分を表す。STは、完全な標的体を表す。感度の値が高いほど、アラームをトリガーしやすくなります。

検出対象 ヒトおよびビヒクルが利用可能である。検出ターゲットが選択されない場合、人間及び車両を含む全ての検出ターゲットが報告される。

目標有効性　　有効性を高く設定すると、必要なターゲット機能がより明確になり、アラーム精度が高くなります。あまり明白でない特徴を有する標的は、欠落しているであろう。

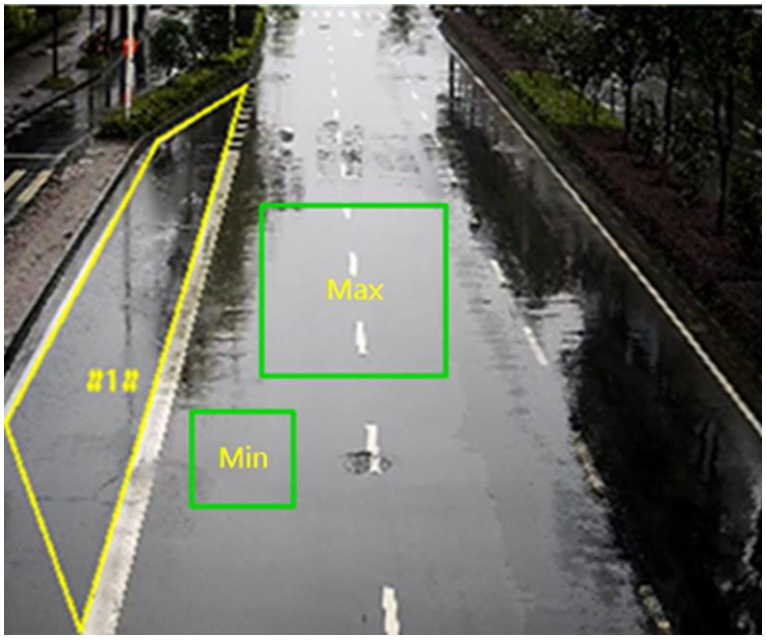

図 6-6 ルールの設定

5. (オプション) 上記の手順を繰り返すことで、複数の領域のパラメータを設定できます。
6. アーミングスケジュールの設定については、「アーミングスケジュールの設定」を参照してください。連動方法の設定については、連動方法の設定を参照してください。
7. 保存をクリックします。

6.2.10 無人手荷物検知の設定

定義済み領域に残っているオブジェクトを検出するために使用されます。リンケージメソッドは、オブジェクトが残された後にトリガーでき、設定された期間、リージョンに留まります。

手順

1. 「→イベント→スマートイベント・→・アンアテンデッド・バゲージ・ディテクション」に移動します。
2. 有効をチェックします。
3. リージョンを1つ選択します。検出領域の設定については、「Draw Area」を参照してください。
4. ルールを設定します。

感度　　感度は、予め定義された領域に入る許容可能な標的の身体部分のパーセンテージを表す。感度 = 100 - S1/ST × 100。S1は、所定の領域を横切る目標身体部分を表す。STは、完全な標的体を表す。感度の値が高いほど、アラームをトリガーしやすくなります。

しきい値　　これは、領域内に残されたオブジェクトの時間を表す。アラームは、オブジェクトが放置され、設定された時間の間、領域内に留まった後にトリガされる。

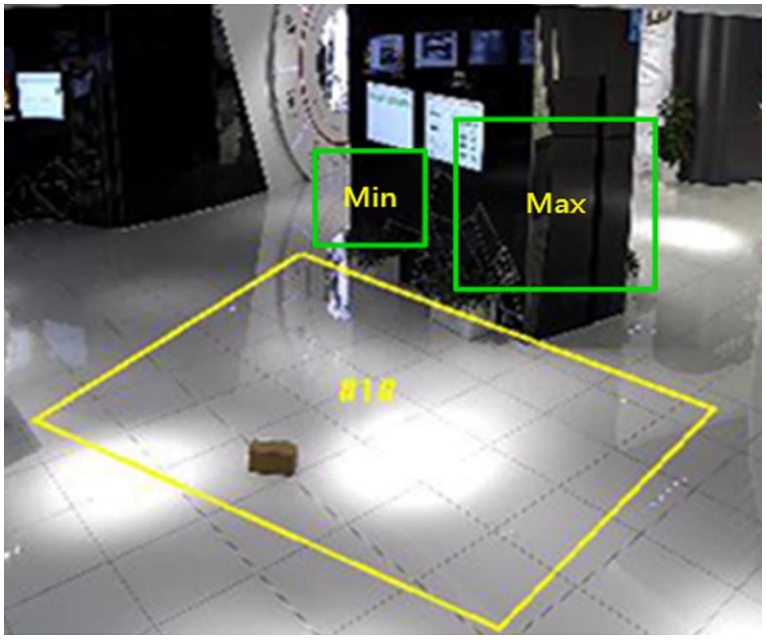

図 6-7 ルールの設定

5. (オプション) 上記の手順を繰り返すことで、複数の領域のパラメータを設定できます。
6. アーミングスケジュールの設定については、「アーミングスケジュールの設定」を参照してください。連動方法の設定については、連動方法の設定を参照してください。
7. 保存をクリックします。

6.2.11 物体除去検出設定

それは、ディスプレイ上の展示物のように、物体が所定の検出領域から除去されたかどうかを検出する。このような事態が発生した場合には、装置は連携動作を行うことができ、スタッフは、不動産の損失を低減するための措置を講じることができる。

手順

1. 「設定→イベント→スマートイベントオブジェクト削除検知」に移動します。
2. 有効をチェックします。
3. リージョンを選択します。リージョン設定については、「Draw Area」を参照してください。
4. ルールを設定します。

感度　　これは、予め規定された領域を離れる許容可能な標的の身体部分のパーセンテージを表す。
感度 = 100 − S1/ST*100

	S1は、所定の領域を離れる目標身体部分を表す。STは、完全な標的体を表す。 例: 値を60 に設定すると、ターゲットの40% の身体部分が領域を離れた場合にのみ、ターゲットを除去されたオブジェクトとしてカウントできます。
しきい値	領域から削除されたオブジェクトの時間のしきい値。値を10に設定すると、10秒間領域からオブジェクトが消えた後にアラームが発生します。

5. オプション: 上記の手順を繰り返して、より多くの領域を設定します。
6. アーミングスケジュールの設定については、「アーミングスケジュールの設定」を参照してください。連動方法の設定については、「連動方法の設定」を参照してください。
7. 保存をクリックします。

注

この関数は、特定のモデルによってのみサポートされます。実際の表示は機種によって異なります。

6.2.12 描画領域

ここでは、エリアの構成について紹介します。

手順

1. Draw Area をクリックします。
2. ライブビューをクリックして検出領域の境界を描き、右クリックして描画を完了します。
3. 保存をクリックします。

注

すべてクリアをクリックして、定義済みの領域をすべてクリアします。

6.2.13 サイズフィルタの設定

この部分では、サイズフィルタの設定について説明します。最小値と最大値との間の大きさを有するターゲットのみが検出され、アラームをトリガする。

手順

1. Max をクリックします。サイズを変更し、ライブビューでマウスをドラッグして、最大ターゲットサイズを描画します。

2. 最小をクリックします。サイズを変更し、ライブビューでマウスをドラッグして、最小ターゲットサイズを描画します。
3. 保存をクリックします。

第 7 章ネットワーク設定

7.1 TCP/IP

ネットワーク経由でデバイスを操作する前に、TCP/IP 設定を適切に構成する必要があります。IPv4 とIPv6 の両方がサポートされます。両方のバージョンは、互いに競合することなく同時に設定できます。
パラメータ設定については、「コンフィギュレーション→ネットワーク 基本設定」→「TCP/IP」を参照してください。

NIC タイプ

ネットワークの状態に応じて、NIC (Network Interface Card)タイプを選択します。

IPv4

2 つのIPv4 モードを使用できます。

DHCP

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

注

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

マニュアル

デバイスのIPv4 パラメータは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、Test(テスト)をクリックして IP アドレスが使用可能かどうかを確認します。

IPv6

3 つのIPv6 モードを使用できます。

ルート広告

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

注

ルートアドバタイズメントモードでは、デバイスが接続されているルータからのサポートが必要です。

DHCP

IPv6 アドレスは、サーバー、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。

マニュアル

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

MTU

これは最大伝送単位を意味する。これは、単一のネットワーク層トランザクションで通信できる最大のプロトコルデータユニットのサイズです。
MTU の有効な値の範囲は1280 ～1500 です。

DNS

ドメインネームサーバの略。ドメイン名でデバイスにアクセスする必要がある場合に必要です。また、それは、いくつかのアプリケーション(例えば、電子メールの送信)にも必要とされる。必要に応じて、「優先DNS サーバ」と「代替DNS サーバ」を適切に設定します。

動的ドメイン名

Enable Dynamic Domain Name をチェックし、Register Domain Name を入力します。デバイスは、ローカルエリアネットワーク内での管理を容易にするために、レジスタドメイン名の下に登録されます。

注

動的ドメイン名を有効にするには、DHCP を有効にする必要があります。

7.1.1 マルチキャスト

マルチキャストは、データ送信が宛先デバイスのグループに同時にアドレス指定されるグループ通信です。マルチキャストを設定すると、送信元データを複数の受信者に効率的に送信できます。
マルチキャスト設定については、「コンフィギュレーション→ネットワーク 基本設定」→「マルチキャスト」に進みます。

IPアドレス

マルチキャストホストのアドレスを表します。

ストリームタイプ

マルチキャスト送信元のストリームタイプ。

ビデオポート

選択したストリームのビデオポート。

オーディオポート

選択したストリームのオーディオポート。

FECポート

選択されたストリームのFEC ポート。

FEC比率

前方誤り訂正の比率。

7.1.2 マルチキャスト検出

「マルチキャスト検出を有効にする」をオンにすると、LAN 内のプライベートマルチキャストプロトコルを介して、オンラインネットワークカメラをクライアントソフトウェアで自動的に検出できます。

7.2 SNMP

ネットワーク送信時にアラームイベントと例外メッセージを取得するように、SNMP ネットワーク管理プロトコルを設定できます。

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するように管理する必要があります。

手順

1. 「設定」ページ「設定→ネットワーク→詳細設定SNMP」に移動します。
2. 「SNMPv1 を有効にする」、「SNMP v2c を有効にする」、または「SNMPv3 を有効にする」をオンにします。

注

選択するSNMP バージョンは、SNMP ソフトウェアと同じである必要があります。
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 はセキュアではなく、SNMP v2 はアクセスにパスワードを必要とします。また、SNMP v3 は暗号化を提供し、3 番目のバージョンを使用する場合は、HTTPS プロトコルを有効にする必要があります。

3. SNMP の設定を行います。
4. 保存をクリックします。

7.3 SRTPの設定

SRTP (Secure Real-time Transport Protocol) は、RTP (Real-time Transport Protocol) インターネットプロトコルで、ユニキャストアプリケーションとマルチキャストアプリケーションの両方で、RTPデータに暗号化、メッセージ認証と整合性、およびリプレイ攻撃保護を提供することを目的としています。

手順

1. 「コンフィギュレーション→ネットワーク 詳細設定」→「SRTP」に移動します。
2. 「サーバ証明書」を選択します。
3. 暗号化アルゴリズムを選択します。
4. 保存をクリックします。

注

- この機能をサポートするのは、特定のデバイスモデルのみである。
- 機能に異常がある場合は、選択した証明書が証明書管理に異常があるかどうかを確認します。

7.4 ポートマッピング

ポートマッピングを設定することで、指定したポートを介してデバイスにアクセスできます。

開始前に

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

手順

1. 「コンフィギュレーション→ネットワーク 基本設定→」NAT に移動します。
2. ポートマッピングモードを選択します。

オートポートマッピング	詳細については、「自動ポートマッピングの設定」を参照してください。
手動ポートマッピング	詳細については、「マニュアル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。

7.4.1 オートポートマッピング を設定する

手順

1. 「UPnP™を有効にする」をチェックし、カメラのフレンドリな名前を選択するか、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Auto に選択します。
3. 保存をクリックします。

注

ルータのUPnP™機能を同時に有効にする必要があります。

7.4.2 手動ポートマッピングの設定

手順

1. 「UPnP™を有効にする」をオンにして、デバイスのわかりやすい名前を選択するか、デフォルト名を使用します。
2. ポートマッピングモードを手動に選択し、外部ポートを内部ポートと同じに設定します。
3. 保存をクリックします。

次にどうするか

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

7.4.3 ルータでのポートマッピングの設定

以下の設定は、特定のルータに関するものです。設定は、ルータのモデルによって異なります。

手順

1. 「WAN 接続種別」を選択します。
2. ルータのIP Address、Subnet Mask、およびその他のネットワークパラメータを設定します。
3. 「→ 仮想サーバの転送」に進み、ポート番号とIP アドレスを入力します。
4. 保存をクリックします。

例

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

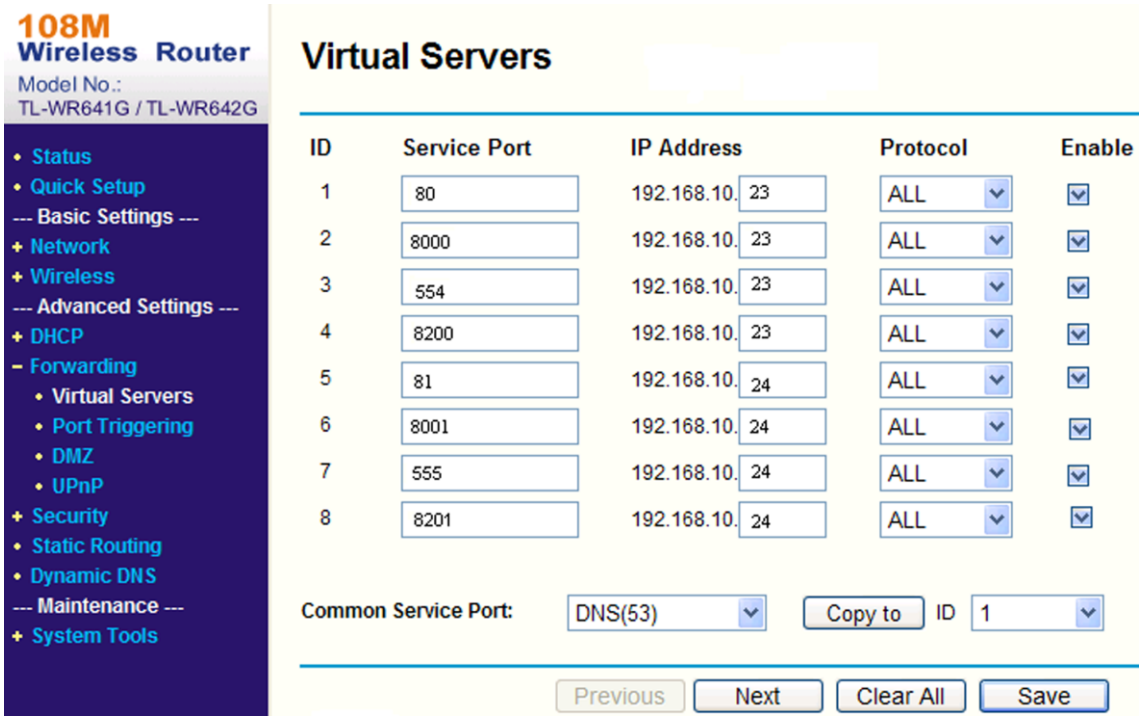

図7-1 ルータでのポートマッピング

注

ネットワークカメラのポートが他のポートと競合することはありません。たとえば、ルーターの一部のWeb 管理ポートは80 です。管理ポートと同じ場合は、カメラポートを変更します。

7.5 ポート

デバイスポートは、ポートの競合によりデバイスがネットワークにアクセスできない場合に変更できます。

注意

デフォルトのポートパラメータは自由に変更しないでください。変更すると、デバイスにアクセスできなくなる可能性があります。

ポート設定については、「設定→ネットワーク 基本設定→ポート」に進みます。

HTTP ポート

ブラウザがデバイスにアクセスする際に使用するポートを指します。たとえば、HTTP Port が81 に変更された場合、ログインのためにブラウザーにhttp://192.168.1.64:81を入力する必要があります。

HTTPS ポート

これは、ブラウザが証明書を使用してデバイスにアクセスするときに使用するポートを指します。証明書の検証は、安全なアクセスを保証するために必要である。

RTSPポート

リアルタイム・ストリーミング・プロトコルのポートを指します。

SRTP ポート

セキュアなリアルタイムトランスポートプロトコルのポートを指します。

サーバーポート

これは、クライアントがデバイスを追加するポートを参照します。

拡張SDKサービスポート

これは、クライアントがデバイスを追加するポートを参照します。証明書の検証は、安全なアクセスを保証するために必要である。

WebSocket ポート

プラグイン・フリー・プレビュー用のTCPベースの全二重通信プロトコル・ポート。

WebSockets ポート

プラグイン・フリー・プレビュー用のTCPベースの全二重通信プロトコル・ポート。証明書の検証は、安全なアクセスを保証するために必要である。

注

- Enhanced SDK Service Port、WebSocket Port、およびWebSockets Port は、特定のモデルでのみサポートされています。
- その機能に対応している機器の場合は、「設定→ネットワーク 詳細設定→ネットワークサービス」で有効にしてください。

7.6 ドメイン名を介した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。装置の動的IPアドレスをドメイン名解決サーバにマッピングし、ドメイン名を介したネットワークアクセスを実現することができる。

開始前に

デバイスのDDNS 設定を行う前に、DDNS サーバーへの登録が必要です。

手順

1. TCP/IP を参照して、DNS パラメータを設定します。
2. 「DDNS設定」ページ:「コンフィギュレーション→ネットワークベーシック設定」→の「DDNS」に移動します。
3. DDNS を有効にするをチェックし、DDNS タイプを選択します。

DynDNS

ドメイン名解決にはダイナミックDNS サーバが使用されます。

NO-IP

ドメイン名解決にNO-IP サーバを使用します。

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

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

7.7 PPPoEダイヤルアップ接続によるデバイスへのアクセス

PPPoEオートダイヤルアップ機能をサポートしています。デバイスがモデムに接続されると、デバイスはADSL ダイヤルアップによってパブリックIP アドレスを取得します。デバイスのPPPoE パラメータを設定する必要があります。

手順

1. PPPoEの→の「コンフィギュレーション→基本設定」に進みます。
2. PPPoEを有効にするをチェックします。
3. PPPoE パラメータを設定します。

ダイナミックIP

ダイヤルアップに成功すると、WAN の動的IP アドレスが表示されます。

ユーザー名

ダイヤルアップネットワークアクセスのユーザー名。

パスワード

ダイヤルアップネットワークアクセスのパスワード。

確認

ダイヤルアップパスワードをもう一度入力します。

4. 保存をクリックします。
5. デバイスにアクセスします。

ブラウザ別	ブラウザのアドレスバーにWAN 動的IP アドレスを入力して、デバイスにアクセスします。

クライアントソフトウェア別	クライアントソフトウェアにWAN 動的IP アドレスを追加します。詳しくは、クライアントマニュアルを参照してください。

注

取得したIP アドレスはPPPoE 経由で動的に割り当てられるため、カメラの再起動後は常にIPアドレスが変更されます。動的IPの不都合を解決するには、DDNSプロバイダ(DynDns.comなど)からドメイン名を取得する必要があります。詳細については、「ドメイン名によるデバイスへのアクセス」を参照してください。

7.8 ワイヤレスダイヤル

音声、映像、映像のデータを3G/4G無線ネットワーク経由で転送できます。

注

この関数は、特定のデバイスモデルによってのみサポートされます。

7.8.1 ワイヤレスダイヤルの設定

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

開始前に

SIM カードを取得し、3G/4G サービスをアクティブにします。SIM カードを対応するスロットに挿入します。

手順

1. 「ワイヤレスダイアル」→の「設定→ネットワーク 詳細設定」に移動します。
2. 機能が有効になっていることを確認します。
3. Dial Parameters(ダイヤルパラメータ)をクリックして、パラメータを設定および保存します。
4. ダイヤルプランをクリックします。詳細については、「準備スケジュールの設定」を参照してください。
5. オプション: Allowlist を設定します。詳細については、「許可リストの設定」を参照してください。
6. ダイヤルステータスをクリックします。

更新をクリック	ダイヤルステータスを更新します。
切断をクリック	3G/4G無線ネットワークを切断します。

「ダイヤルステータス」が「接続済み」に変わると、ダイヤルが成功したことを意味します。

7. ネットワーク内のコンピュータのIP アドレスを介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/Domain を選択し、IP アドレスやその他のパラメータを入力してデバイスにアクセスします。

7.8.2 許可リストの設定

装置からアラームメッセージを受信するために、管理者の携帯電話番号をアロウリストに追加します。

手順

1. 「すべてのリスト設定」ページ:「設定→の詳細設定」→の「ワイヤレスダイヤル→の許可」リストに移動します。
2. 「SMSアラームを有効にする」をチェックします。
3. allowlist をクリックします。+
   1) アラームメッセージを受信するときは、携帯電話番号を入力してください。
   2) SMS 経由での再起動をチェックします。
   3) 特定のイベントを選択すると、イベントが発生したときに携帯電話がアラームメッセージを受信できます。
   4) 保存をクリックします。
   5) 必要に応じて、上記の手順を繰り返して複数の受信者を設定します。

	allowlist パラメータを変更します。
×	すでに設定されているallowlist を削除します。
テストSMS送信	テストのために携帯電話にメッセージを送信します。

4. 保存をクリックします。

7.9 Wi-Fi

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

注

この関数は、特定のデバイスモデルによってのみサポートされます。

7.9.1 デバイスをWi-Fi に接続する

開始前に

SSID、キー、その他のパラメータを設定するには、ワイヤレスルーターまたはAP のユーザーマニュアルを参照してください。

手順

1. 「TCP/IP 設定」ページ: 「設定→ネットワークへの基本設定→ TCP/IP」に進みます。
2. Wlanを選択してパラメータを設定します。詳細な設定については、TCP/IP を参照してください。

注

Wi-Fi を安定して使用するために、DHCP を使用することはお勧めしません。

3. 「Wi-Fi 設定」ページ:「設定→ネットワーク→詳細設定」Wi-Fi に移動します。
4. パラメータを設定し、保存します。
   1) 検索をクリックします。
   2) SSID を選択します。これは、ワイヤレスルーターまたはAP と同じにする必要があります。ネットワークのパラメータが自動的にWi-Fi に表示されます。
   3) 「管理」として「ネットワークモード」を選択します。
   4) キーを入力して、ワイヤレスネットワークを接続します。キーは、ルーターに設定したワイヤレスネットワーク接続のキーである必要があります。

次にどうするか

「TCP/IP 設定」ページ:「設定→ネットワーク 基本設定→ TCP/IP」に移動し、「Wlan」を選択してIPv4 アドレスを確認し、装置にログインします。

7.10 ネットワークサービスを設定する

特定のプロトコルのON/OFF状態を任意に制御できます。

手順

注

この関数は、モデルによって異なります。

1. 「設定→ネットワーク→詳細設定ネットワークサービス」に移動します。
2. ネットワークサービスを設定します。

WebSocket & WebSockets

Google Chrome 57 以上のバージョンまたはMozilla Firefox 52 以上のバージョンを使用してデバイスにアクセスする場合は、WebSocket またはWebSockets プロトコルを有効にする必要があります。ライブビュー、画像取り込み、デジタルズームなどは使用できません。
デバイスがHTTP を使用する場合は、WebSocket を有効にします。
デバイスがHTTPS を使用している場合は、WebSockets を有効にします。
WebSocket を使用する場合は、「サーバ証明書」を選択します。

注

サーバ証明書を選択する前に、証明書の管理を完了します。詳細については、「証明書管理」を参照してください。

SDKサービス&拡張SDKサービス

SDK プロトコルでクライアントソフトウェアにデバイスを追加するには、SDK サービスを有効にするをオンにします。

Enable Enhanced SDK Service をオンにして、SDK over TLS プロトコルでデバイスをクライアントソフトウェアに追加します。

拡張SDK サービスを使用する場合は、サーバー証明書を選択します。

注

- サーバ証明書を選択する前に、証明書の管理を完了します。詳細については、「証明書管理」を参照してください。
- デバイスとクライアントソフトウェア間の接続を設定する場合は、Enhanced SDK Service を使用し、Arming Mode で通信を設定してデータ送信を暗号化することをお勧めします。アーミングモードの設定については、クライアントソフトウェアのユーザーマニュアルを参照してください。

TLS (トランスポート層セキュリティ)

デバイスは、TLS1.1およびTLS1.2を提供します。必要に応じて、1 つ以上のプロトコルバージョンを有効にします。

ボンジョール

プロトコルを無効にするには、チェックを解除します。

3. 保存をクリックします。

7.11 オープンネットワークビデオインターフェースの設定

Open Network Video Interface プロトコルを介してデバイスにアクセスする必要がある場合は、ネットワークセキュリティを強化するためにユーザー設定を構成できます。

手順

1. 「コンフィギュレーション→ネットワーク 詳細設定→インテグレーションプロトコル」に移動します。
2. 「ネットワークビデオインターフェイスを開く」をオンにします。
3. 「追加」を選択して、「ネットワークビデオインターフェイスを開く」ユーザを設定します。

削除 選択したOpen Network Video Interface ユーザーを削除します。

変更 選択したOpen Network Video Interface ユーザーを変更します。

4. 保存をクリックします。
5. (オプション) Open Network Video Interface ユーザーをさらに追加するには、上記の手順を繰り返します。

7.12 ISUPの設定

装置がISUPプラットフォーム(以前はEhomeと呼ばれていた)に登録されている場合、装置を訪問して管理し、データを送信し、公衆ネットワークを介してアラーム情報を転送することができる。

手順

1. 「設定→ネットワーク→詳細設定」→「プラットフォームアクセス」に移動します。
2. プラットフォームアクセスモードとしてISUP を選択します。
3. 有効を選択します。
4. プロトコルバージョンを選択し、関連パラメータを入力します。
5. 保存をクリックします。
   機能が正しく設定されると、レジスタの状態がオンラインになります。

7.13 アラームサーバーの設定

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

手順

1. 設定→ネットワーク 詳細設定→アラームサーバーに移動します。
2. 「宛先IP」または「ホスト名」、「URL」、および「ポート」を入力します。
3. オプション: Enable をオンにしてANR を有効にします。
4. プロトコルを選択します。

注

HTTP、HTTPS、ISUP が選択可能です。通信中のデータ送信は暗号化されるため、HTTPS を使用することをお勧めします。

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

7.14 Hik-Connect 経由でカメラにアクセスする

Hik-Connectは、モバイルデバイスのためのアプリケーションである。Appを使用すると、ライブ画像の表示、アラーム通知の受信などができます。

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ます。

手順

1. 次の方法でHik-Connectアプリケーションを取得してインストールします。

お使いの携帯電話機に合わせて、https://appstore.hikvision.comをご覧になって、アプリケーションをダウンロードしてください。弊社オフィシャルサイトをご覧ください。次に、「→ツール・→・ヒックビジョン・アプリ・ストアの支援」に行きます。以下のQRコードをスキャンして、アプリケーションをダウンロードします。

注

インストール中に「Unknown app」などのエラーが発生した場合は、2つの方法で問題を解決します。

トラブルシューティングを参照するには、https://appstore.hikvision.com/static/help/index.html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隅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ます。

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ます。
3. 登録後にログインします。
4. アプリの右上にある「+」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、カメラまたはパッケージ内のカメラの「クイックスタートガイド」のカバーに表示されます。
5. プロンプトに従って、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ます。

詳細については、Hik-Connectアプリの取扱説明書を参照してください。

7.14.1 カメラのHik-Connectサービスを有効にする

Hik-Connectサービスは、サービスを使用する前にカメラで有効にする必要があります。
このサービスは、SADP ソフトウェアまたはWeb ブラウザを介して有効にできます。

Web ブラウザ経由のHik-Connect サービスの有効化

Web ブラウザ経由でHik-Connect サービスを有効にするには、次の手順に従います。

開始前に

サービスを有効にする前にカメラを有効にする必要があります。

手順

1. Webブラウザでカメラにアクセスします。
2. プラットフォームアクセスコンフィギュレーションインターフェイスに入ります。コンフィギュレーション→ネットワーク→詳細設定→プラットフォームアクセス
3. プラットフォームアクセスモードとしてHik-Connect を選択します。
4. 有効をチェックします。
5. ポップアップウィンドウの「利用規約」と「プライバシーポリシー」をクリックしてお読みください。
6. 検証コードを作成するか、カメラの古い検証コードを変更します。

注

カメラを「Hik-Connect」サービスに追加する場合は、確認コードが必要です。

7. 設定を保存します。

SADP ソフトウェア経由のHik-Connect サービスの有効化

このパートでは、起動したカメラの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を紹介します。

手順

1. SADPソフトウェアを実行します。
2. カメラを選択し、[ネットワークパラメータの変更]ページを入力します。
3. 「Hik-Connect を有効にする」をチェックします。
4. 確認コードを作成するか、古い確認コードを変更します。

注

カメラを「Hik-Connect」サービスに追加する場合は、確認コードが必要です。

5. 「サービス条件」と「プライバシーポリシー」をクリックして読んでください。
6. 設定を確認します。

7.14.2 Hik-Connect のセットアップ

手順

1. 次の方法でHik-Connectアプリケーションを取得してインストールします。

お使いの携帯電話機に合わせて、https://appstore.hikvision.comをご覧になって、アプリケーションをダウンロードしてください。弊社オフィシャルサイトをご覧ください。次に、「→ツール・→・ヒックビジョン・アプリ・ストアの支援」に行きます。以下のQRコードをスキャンして、アプリケーションをダウンロードします。

注

インストール中に「Unknown app」などのエラーが発生した場合は、2つの方法で問題を解決します。

トラブルシューティングを参照するには、https://appstore.hikvision.com/static/help/index.html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隅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ます。

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ます。
3. 登録後にログインします。

7.14.3 Hik-Connectにカメラを追加する

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. ホームページの右上にある「+」をタップしてカメラを追加します。
4. カメラ本体またはQuick Start Guideカバーの QRコードをスキャンします。

注

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

5. カメラの確認コードを入力します。

注

- 必要な検証コードは、カメラでHik-Connectサービスを有効にしたときに作成または変更するコードです。
- 確認コードを忘れた場合は、Web ブラウザ経由でPlatform Access 設定ページで現在の確認コードを確認できます。

6. ポップアップインターフェースの「ネットワークに接続」ボタンをタップします。
7. カメラの機能に応じて、「有線接続」または「無線接続」を選択します。

ワイヤレス接続	携帯電話が接続したWi-Fiパスワードを入力し、「次へ」をタップしてWi-Fi接続プロセスを開始します。(Wi-Fi を設定するときは、ルータから3 メートル以内にカメラを設置してください。)
有線接続	カメラをネットワークケーブルでルータに接続し、結果インタフェースで[接続]をタップします。

注

ルーターは、携帯電話が接続しているものと同じである必要があります。

8. 次のインターフェースで「追加」をタップして追加を終了します。

詳細については、Hik-Connectアプリの取扱説明書を参照してください。

第 8 章準備スケジュールとアラームリンク

アーミングスケジュールは、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期間である。アラームリンケージは、スケジュールされた時間中に検出された特定のインシデントまたはターゲットに対する応答である。

8.1 アーミングスケジュールの設定

デバイスタスクの有効時間を設定します。

手順

1. Arming Schedule をクリックします。
2. タイムバーをドラッグして、目的の有効時間を描きます。

> **注**
>
> 1 日に最大8 つの期間を設定できます。

3. 期間を調整します。
   - 選択した期間をクリックし、目的の値を入力します。保存をクリックします。
   - 選択した期間をクリックします。両端をドラッグして、期間を調整します。
   - 選択した期間をクリックし、タイムバーにドラッグします。
4. 必要に応じて、「Copy to...」をクリックして、同じ設定を他の日にコピーします。
5. 保存をクリックします。

8.2 連携方法の設定

イベントやアラームが発生したときにリンク機能を有効にすることができます。

8.2.1 トリガアラーム出力

装置がアラーム出力装置に接続され、アラーム出力No.が設定されている場合、アラームがトリガされると、装置は接続されたアラーム出力装置にアラーム情報を送信します。

手順

1. 構成→イベント→基本イベント→アラームアウトプットに進みます。
2. アラーム出力のパラメータを設定します。

自動アラーム	構成の詳細については、「自動アラーム」を参照してください。
手動アラーム	構成の詳細については、マニュアルアラームを参照してください。

3. 保存をクリックします。

手動アラーム

アラーム出力を手動でトリガすることができます。

手順

1. 手動アラームパラメータを設定します。

   アラーム出力番号

   外部アラーム機器に接続するアラームインタフェースに合わせて、アラーム出力番号を選択してください。

   アラーム名

   アラーム出力の名前を編集します。

   遅延

   マニュアルを選択します。
2. [手動アラーム] をクリックして、手動アラーム出力を有効にします。
3. オプション: Clear Alarm をクリックして、手動アラーム出力を無効にします。

自動アラーム

自動アラームパラメータを設定すると、設定したアーミングスケジュールで自動的にアラーム出力がトリガされます。

手順

1. 自動アラームパラメータを設定します。

   アラーム出力番号

   外部アラーム機器に接続するアラームインタフェースに合わせて、アラーム出力番号を選択してください。

   アラーム名

   アラーム出力の名前をカスタマイズします。

   遅延

   アラーム発生後、アラーム出力が残っている時間を表します。
2. アラームスケジュールを設定します。設定の詳細については、「アーミングスケジュールの設定」を参照してください。
3. Copy to...をクリックして、パラメータを他のアラーム出力チャネルにコピーします。
4. 保存をクリックします。

8.2.2 FTP/NAS/メモリカードのアップロード

FTP/NAS/メモリカードのアップロードを有効にして設定した場合、アラームがトリガーされると、デバイスはアラーム情報をFTP サーバ、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 の設定」を参照してFTP サーバを設定します。
NAS 設定については、「NAS の設定」を参照してください。
メモリカードのストレージ構成については、「新しいメモリカードまたは暗号化されていないメモリカードの設定」を参照してください。

8.2.3 電子メールの送信

Eメール送信を確認し、アラームイベントが検出された場合、デバイスは、指定されたアドレスにアラーム情報と共にEメールを送信する。
電子メールの設定については、「電子メールの設定」を参照してください。

電子メールを設定する

電子メールが構成され、送信電子メールがリンク方法としてイネーブルされると、装置は、アラームイベントが検出された場合に、全ての指定された受信者に電子メール通知を送信する。

開始前に

Email 機能を使用する前に、DNS サーバーを設定してください。DNS 設定については、TCP/IP の→の「設定→ネットワーク 基本設定」を参照してください。

手順

1. 「電子メール設定」ページ:「設定→ネットワーク 詳細設定」→の「電子メール」に移動します。
2. メールパラメータを設定します。
   1) 送信者のアドレス、SMTP サーバー、SMTP ポートなど、送信者の電子メール情報を入力します。
   2) オプション: 電子メールサーバーで認証が必要な場合は、「認証」をオンにし、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ます。
   3) E-mail 暗号化を設定します。
      - SSL または TLS を選択し、STARTTLS を無効にすると、メールは SSL または TLS で暗号化された後に送信されます。SMTP ポートは465 に設定する必要があります。
      - SSL またはTLS を選択し、STARTTLS を有効にすると、E メールはSTARTTLS によって暗号化された後に送信されます。SMTP ポートは25 に設定する必要があります。

注

STARTTLS を使用する場合は、プロトコルが電子メールサーバーでサポートされていることを確認します。プロトコルが電子メールサーバーでサポートされていないときに「STARTTLS を有効にする」をオンにすると、電子メールは暗号化されずに送信されます。

4) オプション: アラーム画像の通知を受けたい場合は、添付画像を確認してください。通知メールには、設定可能な画像取り込み間隔でイベントに関する3つのアラーム画像が添付されています。
5) 受信者の名前と住所を含む受信者の情報を入力します。
6) テストをクリックして、機能が適切に設定されているかどうかを確認します。

3. 保存をクリックします。

8.2.4 通知サーベイランスセンター

Check Notify Surveillance Centerでは、アラームイベントが検出されると、アラーム情報が監視センターにアップロードされます。

8.2.5 トリガ記録

トリガ記録をチェックし、装置は、検出されたアラームイベントに関するビデオを記録する。
録画設定については、「録画・撮影」を参照してください。

8.2.6 ライトの点滅

点滅ライトを有効にして点滅ライトアラーム出力を設定した後、アラームイベントが検出されるとライトが点滅します。

点滅アラームの照明出力を設定する

イベントが発生すると、デバイスの点滅ライトをアラームとしてトリガーできます。

手順

1. 構成→イベント→基本イベント→点滅アラームライトアウトプットに進みます。
2. 点滅時間、点滅頻度、明るさを設定します。

点滅時間

1 つのアラームが発生したときに点滅が続く時間です。

点滅頻度

ライトが点滅する速度。高周波、中周波、低周波、ノーマルオンが選択可能です。

輝度

可視光の明るさ。

3. アーミングスケジュールを設定します。詳細については、「準備スケジュールの設定」を参照してください。
4. 保存をクリックします。

注

特定のデバイスモデルのみがこの機能をサポートする。

8.2.7 警告音

警告音を有効にしてアラーム音出力を設定した後、アラームが発生すると、デバイスまたは接続された外部スピーカーの内蔵スピーカーが警告音を再生します。
可聴アラーム出力の設定については、「可聴アラーム出力の設定」を参照してください。

注

この機能は、特定のカメラモデルでのみサポートされます。

アラーム音の出力を設定する

装置が検出領域内のターゲットを検出すると、警告として可聴アラームをトリガすることができる。

手順

1. 構成→イベント→基本イベント→可聴アラームアウトプットに進みます。
2. サウンドタイプを選択し、関連パラメータを設定します。
   - 「プロンプト」を選択し、必要なアラーム時間を設定します。
   - 警告とその内容を選択します。必要なアラーム時間を設定します。
   - カスタムオーディオを選択します。ドロップダウンリストからカスタムオーディオファイルを選択できます。使用可能なファイルがない場合は、「追加(Add)」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(Test)」をクリックして、選択したオーディオファイルをデバイスで再生します。
4. 可聴アラームのアーミングスケジュールを設定します。詳細については、「準備スケジュールの設定」を参照してください。
5. 保存をクリックします。

注

この関数は、特定のデバイスモデルによってのみサポートされます。

第9章システムとセキュリティ

システムメンテナンス、システム設定、セキュリティ管理を紹介し、関連パラメータの設定方法を説明します。

9.1 デバイス情報を表示する

デバイス番号、モデル、シリアル番号、ファームウェアバージョンなどのデバイス情報を表示できます。
設定→ユーティリティの「システム設定」→「基本情報」に入り、装置情報を表示します。

9.2 ログの検索と管理

Log 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. Go to Configuration → System → Maintenance → Log.
2. 検索条件Major Type、Minor Type、Start Time、End Timeを設定します。
3. 検索をクリックします。
   一致したログファイルがログリストに表示されます。
4. 必要に応じて、「エクスポート」を選択して、コンピュータにログファイルを保存します。

9.3 同時ログイン

管理者は、Web ブラウザを介してシステムに同時にログインするユーザーの最大数を設定できます。
→ユーティリティの「ユーザ管理」から「全般」を選択し、「同時ログイン」を設定します。

9.4 設定ファイルのインポートとエクスポート

これは、同じパラメータを持つ他のデバイスでのバッチ構成を高速化するのに役立ちます。
構成→システム→保守→のアップグレードおよび保守を入力します。インポートまたはエクスポートする必要があるデバイスパラメータを選択し、インターフェイスの指示に従って設定ファイルをインポートまたはエクスポートします。

9.5 診断情報のエクスポート

診断情報には、実行中のログ、システム情報、ハードウェア情報が含まれます。
「構成→システム→保守→のアップグレードおよび保守」に移動します。希望する診断情報を確認し、Diagnose Informationをクリックして、対応するデバイスの診断情報をエクスポートします。

9.6 再起動

ブラウザ経由でデバイスを再起動できます。
「設定→システムメンテナンス→アップグレード&メンテナンス」に進み、「再起動」を選択します。

9.7 復元とデフォルト

Restore and Default は、デバイスパラメータをデフォルト設定に復元するのに役立ちます。

手順

1. 「構成→システム→保守→のアップグレードおよび保守」に移動します。
2. 必要に応じて、「復元」または「デフォルト」をクリックします。

復元	ユーザー情報、IPパラメーター、ビデオフォーマットを除くデバイス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を工場出荷時のデフォルトにリセットします。

注

この機能を使用する場合は、注意してください。工場出荷時の設定にリセットすると、すべてのパラメータがデフォルト設定にリセットされます。

9.8 アップグレード

開始前に

正しいアップグレードパッケージを入手する必要がある。

注意

プロセス中に電源を切断しないでください。アップグレード後にデバイスが自動的にリブートします。

手順

1. 「構成→システム→保守→のアップグレードおよび保守」に移動します。
2. アップグレードする方法を1 つ選択します。

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見つけます。
ファームウェアディレクトリ	アップグレードファイルが属するディレクトリを見つけます。

3. 参照をクリックして、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。

9.9 Open Source ソフトウェアライセンスの表示

「装置についてのシステム→システム設定」→の「構成」に移動し、「ライセンスの表示」を選択します。

9.10 ウィーガンド

注

この機能は、特定のカメラモデルでのみサポートされます。

有効をオンにし、プロトコルを選択します。デフォルトのプロトコルはSHA-1 26bit です。
有効になっている場合、認識されたナンバープレート番号は、選択されたWiegandプロトコルを介して出力されます。

9.11 メタデータ

メタデータは、アルゴリズム処理の前に装置が収集する生データである。それは、しばしば、サードパーティ統合のために使用される。
設定→システムメタデータ設定に移動して、目的の機能のメタデータアップロードを有効にします。

道路交通

道路交通のメタデータは、シーン内の車両位置、車両ID、ナンバープレート、有効性、移動方向、国/地域などを含む車両情報が検出される。

9.12 日時

タイムゾーン、時刻同期、およびサマータイム(DST)を設定することで、デバイスの日時を設定で

きます。

9.12.1 手動で時間を同期させる

手順

1. 「構成→システム→システム設定→時刻設定」に移動します。
2. [タイムゾーン]を選択します。
3. 手動時刻同期をクリックします。
4. 1 つの時間同期方式を選択します。
   - 時刻設定を選択し、手動で入力するか、ポップアップカレンダーから日付と時刻を選択します。

同期をチェックします。デバイスの時刻をローカルPCの時刻と同期させるコンピュータの時刻。

5. 保存をクリックします。

9.12.2 NTP サーバの設定

正確で信頼性の高い時間ソースが必要な場合は、NTP サーバを使用できます。

開始前に

NTP サーバを設定するか、NTP サーバ情報を取得します。

手順

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

注

「サーバアドレス」はNTP サーバのIP アドレスです。

5. テストをクリックして、サーバー接続をテストします。
6. 保存をクリックします。

9.12.3 衛星で時刻を同期する

注

この機能は、機器によって異なります。

手順

1. 設定→ユーティリティの「システム設定→時刻設定」に入ります。
2. 衛星時刻同期を選択します。
3. 間隔を設定します。
4. 保存をクリックします。

9.12.4 DST設定

装置の設置場所がDST(Daylight Saving Time)の場合は、この機能を設定できます。

手順

1. 構成→システム設定→サマータイムに移動します。
2. DST を有効にするをチェックします。
3. Start Time、End Time、およびDST Biasを選択します。
4. 保存をクリックします。

9.13 RS-485の設定

RS-485は、デバイスを外部デバイスに接続するために使用される。通信距離が長すぎる場合は、RS-485を使用して、デバイスとコンピュータまたは端末との間でデータを送信することができます。

開始前に

RS-485ケーブルで機器、コンピュータ、端末を接続します。

手順

1. コンフィギュレーション→システム設定→ RS-485に進みます。
2. RS-485パラメータを設定します。

> **注**
> デバイスとコンピュータまたは端末のパラメータはすべて同じにしておく必要があります。

3. 保存をクリックします。

9.14 RS-232の設定

RS-232 は、デバイスのデバッグや周辺機器へのアクセスに使用できます。RS—232は、通信距離が短い場合に、装置とコンピュータまたは端末との間の通信を実現することができる。

開始前に

RS-232ケーブルでコンピュータまたは端末に接続します。

手順

1. コンフィギュレーション→システム設定→ RS-232に進みます。
2. RS-232 パラメータを、デバイスとコンピュータまたはターミナルが一致するように設定します。
3. 保存をクリックします。

9.15 消費電力モード

デバイスが動作しているときに消費電力を切り替えるために使用します。

注

この機能は、特定のカメラモデルでのみサポートされます。

「構成→システム→システム設定」→「電力消費モード」に進み、目的の電力消費モードを選択します。

フル消費モード

デバイスは、すべての機能が有効になっている状態で動作します。

低消費リアルタイムモード

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

低電力スリープ

デバイス電力が低電力スリープモードのしきい値よりも低い場合、デバイスはスリープモードに入る。

デバイス電力が閾値を10%上回るまで回復すると、デバイスはユーザ構成モードに入る。

予定睡眠

デバイスがスケジュールされたスリープ時間中である場合、スリープモードに入り、そうでない場合、デバイスはユーザ構成モードに入る。

注

スケジュールされたスリープスケジュールの設定については、「アーミングスケジュールとアラームリンク」を参照してください。

デバイスは、タイミングウェイクをサポートする。詳細については、「Set Timing Wake」を参照してください。

9.16 外部機器

サプリメント可視光、ハウジング上のワイパー、LED可視光などの外部機器をサポートする機器は、Webブラウザを介して、ハウジングで使用するときに制御できます。外付けデバイスはモデル

によって異なります。

輝度

実際のシーンに応じてLow Beam BrightnessとHigh Beam Brightnessを調整します。

タイミング

設定したスケジュールでLED可視光が点灯します。開始時刻と終了時刻を設定する必要があります。

自動

環境照明に応じてLEDライトが点灯します。

9.16.1 サプリメント可視光の設定

サプリメント可視光を設定し、実際の機器を参照してパラメータを設定できます。

スマートサプリメント可視光

スマートサプリメント可視光は、サプリメント可視光が点灯しているときに、過剰露可視光を回避する。

補足ライトモード

サプリメント可視光に対応している場合は、サプリメント可視光モードを選択できます。

IRモード

IR可視光が有効になります。

ホワイトライトモード

白色光が有効になります。

ミックスモード

IR可視光および白色可視光の両方が使用可能である。

Off

サプリメント可視光は無効です。

明るさ調整モード

自動

実際の環境に合わせて明るさが自動的に調整されます。

マニュアル

スライダをドラッグしたり、値を設定したりして、明るさを調整することができます。

9.16.2 ヒータ

ヒーターを有効にして、デバイスのレンズ周辺の霧を取り除くことができます。
「設定→システム→システム設定→外部機器」に進み、必要に応じてモードを選択します。

9.17 セキュリティ

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

9.17.1 認証

RTSP とWEB 認証を設定することで、ネットワークアクセスのセキュリティを向上させることができます。
→ユーティリティのセキュリティー→認証の設定に進み、必要に応じて認証のプロトコールと方式を選択します。

RTSP認証

ダイジェストとdigest/basic がサポートされています。つまり、RTSP 要求がデバイスに送信されるときに認証情報が必要になります。digest/basic を選択した場合は、デバイスがダイジェストまたは基本認証をサポートしていることを意味します。ダイジェストを選択すると、デバイスはダイジェスト認証のみをサポートします。

RTSPダイジェストアルゴリズム

MD5, RTSP 認証でのSHA256 およびMD5/SHA256 暗号化アルゴリズム。MD5 以外のダイジェストアルゴリズムを有効にすると、互換性があるため、サードパーティプラットフォームがデバイスにログインできなかったり、ライブビューを有効にできなかったりすることがあります。高強度の暗号化アルゴリズムが推奨される。

WEB 認証

ダイジェストとdigest/basic がサポートされています。つまり、WEB 要求がデバイスに送信されるときに認証情報が必要になります。digest/basic を選択した場合は、デバイスがダイジェストまたは基本認証をサポートしていることを意味します。ダイジェストを選択すると、デバイスはダイジェスト認証のみをサポートします。

WEBダイジェストアルゴリズム

MD5, WEB 認証におけるSHA256 およびMD5/SHA256 暗号化アルゴリズム。MD5 以外のダイジェストアルゴリズムを有効にすると、互換性があるため、サードパーティプラットフォームがデバイスにログインできなかったり、ライブビューを有効にできなかったりすることがあります。高強度の暗号化アルゴリズムが推奨される。

注

認証要件を表示するには、プロトコルの特定の内容を参照してください。

9.17.2 IP アドレスフィルタの設定

IPアドレスフィルタは、アクセス制御のためのツールです。IP アドレスフィルタを有効にして、特定のIP アドレスからの訪問を許可または禁止できます。

IP アドレスとは、IPv4 を指します。

手順

1. →ユーティリティのセキュリティー→ IPアドレスフィルターの設定に移動します。
2. IP アドレスフィルタを有効にするをオンにします。
3. IP アドレスフィルタのタイプを選択します。

禁止	リスト内のIP アドレスはデバイスにアクセスできません。
許容	リスト内のIP アドレスのみがデバイスにアクセスできます。

4. IPアドレスフィルタリストを編集します。

追加	新しいIP アドレスまたはIP アドレス範囲をリストに追加します。
変更	リストで選択したIP アドレスまたはIP アドレス範囲を変更します。
削除	リストで選択したIP アドレスまたはIP アドレス範囲を削除します。

5. 保存をクリックします。

9.17.3 HTTPS の設定

HTTPS は、暗号化された送信とアイデンティティ認証を可能にするネットワークプロトコルで、リモートアクセスのセキュリティを向上させます。

手順

1. 「設定→ネットワーク 詳細設定」→「HTTPS」に移動します。
2. HTTP または HTTPS プロトコルでカメラにアクセスできることを確認します。
3. HTTPS Browsing を有効にして、HTTPS プロトコルでのみカメラにアクセスできることを確認します。
4. サーバ証明書を選択します。
5. 保存をクリックします。

注

機能に異常がある場合は、選択した証明書がCertificate Managementで異常であるかどうかを確認します。

9.17.4 Set QoS

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輻輳の改善に役立ちます。

注

ルータやスイッチなどのネットワークデバイスからのQoS サポートが必要です。

手順

1. 「コンフィギュレーション→ネットワーク 詳細コンフィギュレーション→ QoS」に移動します。
2. Video/Audio DSCP、Alarm DSCP、Management DSCPを設定します。

注

ネットワークは、データ送信の優先順位を識別できます。DSCP値が大きいほど優先度が高い。設定中は、router に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。

9.17.5 IEEE 802.1Xを設定する

IEEE 802.1x はポートベースのネットワークアクセス制御です。LAN/WLAN のセキュリティレベルを強化します。デバイスがIEEE 802.1x規格でネットワークに接続される場合は、認証が必要です。
→ Network → Advanced Settings → 802.1X に移動し、機能を有効にします。
ルータ情報に従って、Protocol とEAPOL Version を設定します。

プロトコル

EAP-LEAP、EAP-TLS、EAP-MD5 が選択可能

EAP-LEAPとEAP-MD5

EAP-LEAP またはEAP-MD5 を使用する場合は、認証サーバを設定する必要があります。802.1Xのユーザー名とパスワードを事前にサーバーに登録する。認証用のユーザー名とパスワードを入力します。

EAP-TLS

EAP-TLS を使用する場合は、Identify(識別)、Private Key Password(秘密鍵パスワード)を

入力し、CA 証明書、ユーザー証明書、および秘密鍵をアップロードします。

EAPOLバージョン

EAPOLのバージョンは、ルータまたはスイッチのバージョンと同一である必要があります。

9.17.6 コントロールタイムアウト設定

この機能を有効にすると、設定したタイムアウト時間内にWebブラウザ経由でデバイスに操作(ライブ画像の閲覧を含まない)を行わなかった場合にログアウトします。
設定→ユーティリティのセキュリティ→詳細セキュリティに進み、設定を完了します。

9.17.7 セキュリティ監査ログの検索

デバイスのセキュリティログファイルを検索して分析し、不正な侵入を見つけてセキュリティイベントのトラブルシューティングを行うことができます。

手順

注

この機能は、特定のカメラモデルでのみサポートされます。

1. →ユーティリティ保守→セキュリティ監査ログの設定に移動します。
2. ログタイプ、開始時刻、終了時刻を選択します。
3. 検索をクリックします。
   検索条件に一致するログファイルがログリストに表示されます。
4. 必要に応じて、「エクスポート」を選択して、ログファイルをコンピュータに保存します。

9.17.8 セキュリティ強化

セキュリティ強化は、ネットワークセキュリティを強化するためのソリューションです。この機能を有効にすると、危険な機能、プロトコル、デバイスのポートが無効になり、より安全な代替機能、プロトコル、ポートが有効になります。
「設定→システムセキュリティ→アドバンストセキュリティ」に移動します。「セキュリティ強化」をチェックし、「保存」をクリックします。

9.17.9 SSH

セキュアシェル(SSH)は、セキュアでないネットワーク上でネットワークサービスを操作するための暗号化ネットワークプロトコルです。
SSH 機能はデフォルトで無効になっています。

⚠注意

関数は注意して使用してください。機器内部情報漏洩のセキュリティリスクは、機能が有効になっている場合に発生します。

9.18 証明書管理

これは、サーバ/クライアント証明書およびCA証明書を管理し、証明書が有効期限に近いか、または期限切れ/異常である場合にアラームを送信するのに役立つ。

注

この関数は、特定のデバイスモデルによってのみサポートされます。

9.18.1 自己署名証明書の作成

手順

1. 自己署名証明書の作成をクリックします。
2. プロンプトに従って、証明書ID、国/地域、ホスト名/IP、有効性、およびその他のパラメータを入力します。

   注

   証明書ID は数字または文字で、64 文字以内にする必要があります。

3. [OK]をクリックします。
4. 必要に応じて、「エクスポート」をクリックして証明書をエクスポートするか、「削除」をクリックして証明書を削除して証明書を再作成するか、「証明書のプロパティ」をクリックして証明書の詳細を表示します。

9.18.2 証明書要求の作成

開始前に

自己署名証明書を選択します。

手順

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

9.18.3 輸入証明書

手順

1. インポートをクリックします。
2. 証明書要求の作成をクリックします。
3. 証明書ID を入力します。
4. 「ブラウザ」をクリックして、目的のサーバ/クライアント証明書を選択します。
5. 目的のインポート方法を選択し、必要な情報を入力します。
6. [OK]をクリックします。
7. 必要に応じて、「エクスポート」をクリックして証明書をエクスポートするか、「削除」をクリックして証明書を削除して証明書を再作成するか、「証明書のプロパティ」をクリックして証明書の詳細を表示します。

注

- 16までの証明書が許可されます。
- 特定の機能が証明書を使用している場合は、削除できません。
- 証明書を使用している関数は、functions 列で表示できます。
- 既存の証明書と同じID の証明書を作成し、既存の証明書と同じ内容の証明書をインポートすることはできません。

9.18.4 サーバ/クライアント証明書のインストール

手順

1. →ユーティリティセキュリティー→証明書管理の設定に移動します。
2. 「自己署名証明書の作成」、「証明書要求の作成」、「インポート」の順にクリックして、サーバー/クライアント証明書をインストールします。

自己署名証明書の作成	「自己署名証明書の作成」を参照してください。
証明書要求の作成	「証明書要求の作成」を参照してください。
輸入証明書	輸入証明書参照

9.18.5 CA証明書のインストール

手順

1. インポートをクリックします。
2. 証明書ID を入力します。

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

注

16までの証明書が許可されます。

9.18.6 Enable Certificate Expiration Alarm

手順

1. Enable Certificate Expiration Alarmをチェックします。有効になっている場合、証明書がすぐに期限切れになるか、期限切れになっているか、異常になっているかの電子メールを受信するか、カメラが監視センターにリンクします。
2. Remind Me Before Expiration（日）、Alarm Frequency（日）、Detection Time（時)を設定します。

注

- 満了前のリマインド日を1に設定すると、カメラは満了前の日をリマインドします。1～30日間はご利用いただけます。7日はデフォルトのリマインダー日です。
- 満了前のリマインド日を1に設定し、検出時刻を10:00に設定し、翌日9:00に証明書が満了すると、カメラは初日10:00にリマインドします。

3. 保存をクリックします。

9.19 ユーザーとアカウント

9.19.1 ユーザーアカウントと許可の設定

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

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高めるために、アカウントのパスワードを定期的に変更してください。3 か月ごとにパスワードを変更することをお勧めします。危険性の高い環境で使用する場合は、毎月または毎週パスワードを変更することをお勧めします。

手順

1. 「設定→ユーティリティユーザ管理→ユーザ管理」に移動します。

2. 追加をクリックします。ユーザー名を入力し、レベルを選択してパスワードを入力します。必要に応じて、ユーザーにリモート権限を割り当てます。

管理者

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

利用者

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

オペレータ

オペレータには、管理者に対する操作およびアカウントの作成を除いて、すべての権限を割り当てることができます。

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

注

管理者は、最大31 個のユーザーアカウントを追加できます。

3. [OK]をクリックします。

9.19.2 同時ログイン

管理者は、Web ブラウザを介してシステムに同時にログインするユーザーの最大数を設定できます。
→ユーティリティの「ユーザ管理」から「全般」を選択し、「同時ログイン」を設定します。

9.19.3 オンラインユーザー

デバイスにログインしているユーザーの情報が表示されます。
「設定→ユーティリティユーザ管理→オンラインユーザ」に移動して、オンラインユーザの一覧を表示します。

第10 章VCA リソースの割り当て

VCA リソースには、実際のニーズに応じて特定のVCA 機能を有効にするオプションが用意されています。これは、目的の機能にさらに多くのリソースを割り当てるのに役立ちます。

手順

1. 「設定→システム設定→ VCAリソース」に進みます。
2. 目的のVCA機能を選択します。
3. 設定を保存します。

注

いくつかのVCA機能は、相互に排他的である。特定の機能を選択して保存した場合、他の機能は非表示になりません。

10.1 カウント

これは、特定の構成された領域に入る人または出る人の数を計算するのに役立つ。

注

カウントは、特定のモデルによってのみサポートされます。

10.1.1 カウント設定

リージョンに出入りするオブジェクト、アラームイベント、データのアップロードを計算するために使用されます。

手順

1. 設定→カウントに移動します。
2. Enable Counting をチェックします。
3. オプション:「OSDオーバーレイを有効にする」をオンにすると、リージョンに出入りする人のリアルタイム数がライブビデオに表示されます。

注

オーバーレイ情報は、当日の数のみをカウントします。この番号は、装置が再始動されたとき、または深夜になったときにクリアされる。クリックして手動で番号を消去することもできます。0

4. 検出ラインを設定し、ラインを横切るオブジェクトを検出し、カウントします。

／	検出線を描画します。
✕	検出行を削除します。
⇌	方向を変更します。

図10-1 カウントの設定

5. アーミングスケジュールの設定については、「アーミングスケジュールの設定」を参照してください。連動方法の設定については、連動方法の設定を参照してください。
6. 保存をクリックします。

10.1.2 ビューカウント統計

デバイスまたはメモリカードに保存されているカウント統計を表示およびエクスポートできます。

開始前に

Set Counting に移動して、キュー管理を最初に設定します。

手順

1. アプリケーションに移動します。
2. レポートタイプを選択します。
3. 統計タイプを選択します。
4. [開始時刻]を選択します。
5. カウントをクリックします。
6. 必要に応じて、「エクスポート」を選択して、カウント統計をエクスポートします。
   計数統計は、表、折れ線グラフ、および棒グラフで表示できます。

10.2 フェースキャプチャ

装置は、構成された領域に現れる顔をキャプチャすることができ、顔情報は、キャプチャされた画像と共にアップロードされる。

注

- 顔キャプチャをサポートするデバイスでは、VCA Resourceで機能を有効にする必要があります。詳細については、「VCA リソースの割り当て」を参照してください。
- 顔キャプチャは、特定のモデルによってのみサポートされます。

10.2.1 顔キャプチャの設定

設定した領域に表示される顔をキャプチャできます。

開始前に

この機能を有効にするには、「VCA リソース」に移動し、「顔キャプチャ」を選択します。

手順

1. 「設定→の顔キャプチャ」に移動します。
2. 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。
3. 「ルール」を選択し、「ルール」をチェックします。
4. min を入力します。テキストフィールド内の瞳孔距離、またはクリックしてminを描画します。瞳孔距離。

   最小。ひとみ距離

   min.瞳孔距離は、2つの瞳孔間の最小領域を指し、装置が顔を認識することが基本である。
5. テキストフィールドに最大瞳孔距離を入力するか、クリックして最大瞳孔距離を描画します。
6. クリックすると、顔キャプチャを有効にする検出領域が描画されます。ライブビューウィンドウでエンドポイントを左クリックして領域を描画し、右クリックして領域の描画を終了します。描画領域は、ライブビュー画像の1/2～2/3を占めることが推奨される。
7. アーミングスケジュールの設定については、「アーミングスケジュールの設定」を参照してください。連動方法の設定については、連動方法の設定を参照してください。
8. 保存をクリックします。
9. オーバーレイと取り込みの設定については、「オーバーレイと取り込み」を参照してください。高度なパラメータ設定については、「顔キャプチャアルゴリズムパラメータ」を参照してください。

結果

撮影した顔画像をピクチャで見たり、ダウンロードしたりできます。詳細については、「ピクチャの表示とダウンロード」を参照してください。

10.2.2 オーバーレイとキャプチャ

取り込みパラメータと、ストリームと画像に表示する情報の設定を選択します。

ストリームにVCA 情報を表示する

ターゲットとルール情報を含むスマート情報をストリームに表示します。

アラーム画面にターゲット情報を表示する

アラーム画面をターゲット情報でオーバーレイします。

ターゲット画像設定

カスタムショット、ヘッドショット、ハーフボディショット、フルボディショットを選択できます。

注

「カスタム」を選択すると、必要に応じて幅、頭部高さ、および身長をカスタマイズできます。

Fixed Valueをチェックすると、写真の高さを設定できます。

背景画像の設定

対象画像と比較すると、背景画像は、シーン画像が余分な環境情報を提供する。背景画質、解像度を設定します。バックグラウンドイメージを監視センターにアップロードする必要がある場合は、「バックグラウンドアップロード」をチェックします。

人数オーバーレイ

フローオーバーレイタイプを選択します。
1日のリセット時間を選択します。すぐにリセットする場合は、「手動リセット」をクリックします。

カメラ

撮影した画像にオーバーレイできるカメラの機器番号とカメラ情報を設定します。

テキストオーバーレイ

撮影した画像に表示する場合は、希望する項目を確認し、順番を調整することができます。

デバイスNo.とカメラ情報の内容は、同じページにある必要があります。

10.2.3 顔キャプチャアルゴリズムパラメータ

これは、顔キャプチャのためのアルゴリズムライブラリのパラメータを設定し、最適化するために使用される。
「設定→顔キャプチャの詳細設定」→の「パラメータ」に移動します。

フェイスキャプチャバージョン

アルゴリズムライブラリのバージョンが一覧表示されます。

検出パラメータ

発電速度

ターゲットを識別する速度。値が高いほど、ターゲットはより速く認識される。値を非常に低く設定し、設定された領域に最初から顔があった場合、この顔はキャプチャされません。これは、壁画又はポスターにおける顔の誤った情報を減少させることができる。デフォルト値の3 をお勧めします。

感度

標的を同定する感度。値が大きいほど顔が認識しやすくなり、誤情報の可能性が高くなる。デフォルト値の3 をお勧めします。

キャプチャパラメータ

ベストショット

ターゲット後の最良のショットは検出領域を離れる。

撮影時間

これは、設定された領域に顔が滞在している間に顔がキャプチャされるキャプチャ時間を指す。デフォルト値は1です。

キャプチャしきい値

これは、キャプチャおよびアラームをトリガする顔の品質を意味する。値を大きくすると、キャプチャおよびアラームをトリガするためにより良い品質を満たす必要があることを意味します。

クイックショット

クイックショットしきい値と最大キャプチャ間隔を定義できます。

クイックショットしきい値

それは、クイックショットをトリガーする顔の質を意味する。

顔面暴露

チェックボックスをオンにすると、顔の露出が有効になります。

基準輝度

顔の露出モードにおける、顔の基準となる明るさのことです。顔を検出すると、設定した値に応じてカメラが顔の明るさを調整します。値が高いほど、顔は明るい。

最小持続時間

カメラの最小持続時間は、顔を露光する。

注

顔の露出が有効になっている場合は、WDR機能が無効になっていることを確認し、マニュアルアイリスを選択してください。

顔フィルタリング時間

カメラが顔を検出し、キャプチャアクションを実行するまでの時間間隔を意味します。検出された顔が設定されたフィルタリング時間未満の間シーン内に留まる場合、キャプチャはトリガされない。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5秒間シーンにとどまっているときに検出された顔をキャプチャする。

注

顔フィルタリング時間(0sより長い)は、実際のキャプチャ時間の可能性を、上記の設定値未満に増加させることができる。

デフォルトに戻す

Restore(復元)をクリックして、詳細設定のすべての設定を工場出荷時のデフォルトに復元します。

10.2.4 シールド領域の設定

シールド領域では、設定したスマート関数ルールが無効な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. 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て、より多くのシールド領域を設定する。
3. (オプション) 描画領域を削除するには、をクリックします。
4. 保存をクリックします。

10.3 マルチターゲット型検出

マルチターゲットタイプ検出は、人間の顔、人体、および車両などの複数のタイプのターゲットのデータを検出し、キャプチャし、アップロードすることである。

注

- この関数は、特定のデバイスモデルによってのみサポートされます。
- 特定のデバイスモデルでは、VCAリソースページでマルチターゲットタイプ検出を最初に有効にする必要があります。

10.3.1 マルチターゲットタイプ検出ルールの設定

マルチターゲットタイプ検出ルールおよびアルゴリズムパラメータを設定した後、デバイスは、複数のタイプのターゲットをキャプチャし、リンクアクションを自動的にトリガする。

手順

1. 「設定→マルチターゲットタイプ検知→規則」に進みます。
2. ルールをチェックします。
3. ライブ画像上に検出領域をクリックして描画します。
4. minを入力します。テキストフィールド内の瞳孔距離、またはクリックしてminを描きます。瞳孔距離。

   最小。ひとみ距離

   min.瞳孔距離は、2つの瞳孔間の最小領域を指し、装置が顔を認識することが基本である。
5. アーミングスケジュールを設定します。準備スケジュールの設定を参照してください。
6. リンク方法を設定します。リンク方法の設定を参照してください。
7. 保存をクリックします。

次にどうするか

ピクチャに移動して、取り込んだピクチャを検索し、表示します。
スマートディスプレイに移動して、現在撮影されているターゲットピクチャを表示します。

10.3.2 オーバーレイとキャプチャ

取り込みパラメータと、ストリームと画像に表示する情報の設定を選択します。

ストリームにVCA 情報を表示する

ターゲットとルール情報を含むスマート情報をストリームに表示します。

アラーム画面にターゲット情報を表示する

アラーム画面をターゲット情報でオーバーレイします。

ターゲット画像設定

カスタムショット、ヘッドショット、ハーフボディショット、フルボディショットを選択できます。

注

「カスタム」を選択すると、必要に応じて幅、頭部高さ、および身長をカスタマイズできます。

Fixed Valueをチェックすると、写真の高さを設定できます。

背景画像の設定

対象画像と比較すると、背景画像は、シーン画像が余分な環境情報を提供する。背景画質、解像度を設定します。バックグラウンドイメージを監視センターにアップロードする必要がある場合は、「バックグラウンドアップロード」をチェックします。

人数オーバーレイ

フローオーバーレイタイプを選択します。
1日のリセット時間を選択します。すぐにリセットする場合は、「手動リセット」をクリックします。

カメラ

撮影した画像にオーバーレイできるカメラの機器番号とカメラ情報を設定します。

テキストオーバーレイ

撮影した画像に表示する場合は、希望する項目を確認し、順番を調整することができます。

デバイスNo.とカメラ情報の内容は、同じページにある必要があります。

10.3.3 マルチターゲットタイプ検出アルゴリズムパラメータ

これは、マルチターゲットタイプ検出のためのアルゴリズムライブラリのパラメータを設定し、最適化するために使用される。
構成のために、構成→「マルチターゲットタイプ検知→高度構成」に進みます。

HMSバージョン

現在のアルゴリズムバージョンを参照しますが、これは編集できません。

デフォルトの復元

Restore(復元)をクリックして、詳細設定のすべての設定を工場出荷時のデフォルトに復元します。

検出パラメータ

発電速度

これは、検出領域内の物体がターゲットであるか否かを決定する速度である。値が高いほど、ターゲットはより速く検出される。デフォルト値を推奨します。

感度

それは、標的を認識する感度である。この値が大きいほど、ターゲットが認識しやすくなり、誤情報の可能性が高くなる。デフォルト値を推奨します。

キャプチャパラメータ

ベストショット

キャプチャしきい値

キャプチャとアラームをトリガーする顔の品質を指します。値を大きくすると、キャプチャおよびアラームをトリガするためにより良い品質を満たす必要があることを意味します。

顔面暴露

機能を有効にすると、人間の顔がシーンに現れたときに、装置は露出レベルを自動的に調整

します。

基準輝度

顔の露出モードにおける、顔の基準となる明るさを表します。実際のシーンの顔が設定した基準輝度よりも明るい場合、デバイスは露出レベルを下げます。実際のシーンの顔が設定された基準よりも暗い場合、デバイスは露光レベルを増加させる。

最小持続時間

顔がシーン内で消えた後、装置が顔露出レベルを維持する余分な時間。

顔フィルタリング時間

カメラが顔を検出し、キャプチャアクションを実行するまでの時間間隔を意味します。検出された顔が設定されたフィルタリング時間未満の間シーン内に留まる場合、キャプチャはトリガされない。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5秒間シーンにとどまっているときに検出された顔をキャプチャする。

10.3.4 シールド領域の設定

シールド領域では、設定したスマート関数ルールが無効な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. 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て、より多くのシールド領域を設定する。
3. (オプション) 描画領域を削除するには、をクリックします。
4. 保存をクリックします。

10.4 キュー管理

これは、各人のキューイングアップ人数および待ち時間をカウントするために使用される。

注

キュー管理は、特定のモデルによってのみサポートされます。

10.4.1 地域住民のキューイングアップの設定

これは、定義された領域内のキューイング・アップ人物をカウントするために使用される。アラームしきい値条件とアラームトリガーの両方が満たされると、アラームがトリガーされます。

開始前に

この機能を有効にするには、「VCA リソース」に移動し、「キュー管理」を選択します。

手順

1. コンフィギュレーション→キューマネージメントに移動します。
2. 「リージョナル・ピープル・キューイングアップ」を選択します。
3. 「領域の追加」をクリックして、検出領域を描画し、「領域名」と「アラーム間隔」を設定します。
   上記の手順を繰り返し、より多くの領域を設定します。

アラーム間隔

設定されたアラーム間隔の間、同じタイプのアラームは、1つの通知のみをトリガする。

図10-2 リージョナル・ピープル・キューイングアップの設定

4. 必要に応じて、OSDをオンにすると、リージョン名とそのリアルタイムキューイング人数が表示されます。
5. アラームのしきい値を設定します。アラームしきい値条件が満たされると、アラームがトリガーされます。
6. アーミングスケジュールの設定については、「アーミングスケジュールの設定」を参照してください。連動方法の設定については、連動方法の設定を参照してください。
7. 保存をクリックします。

10.4.2 待ち時間検出の設定

これは、検出領域に入る各人の待ち時間をカウントするために使用される。アラームしきい値条件とアラームトリガーの両方が満たされると、アラームがトリガーされます。

開始前に

この機能を有効にするには、「VCA リソース」に移動し、「キュー管理」を選択します。

手順

1. コンフィギュレーション→キューマネージメントに移動します。
2. Waiting Time Detection(待機時間検出)を選択します。
3. 「領域の追加」をクリックして、検出領域を描画し、「領域名」と「アラーム間隔」を設定します。
   上記の手順を繰り返し、より多くの領域を設定します。

   アラーム間隔

   設定されたアラーム間隔の間、同じタイプのアラームは、1つの通知をトリガするだけである。

図 10-3 待機時間検出の設定

4. アラームのしきい値を設定します。アラームしきい値条件が満たされると、アラームがトリガーされます。
5. アーミングスケジュールの設定については、「アーミングスケジュールの設定」を参照してください。連動方法の設定については、連動方法の設定を参照してください。
6. 保存をクリックします。
7. 必要に応じて、「設定→ローカル」で「POS 情報と規則の照会」を有効にします。
   検出領域および検出領域に滞在する時間は、ライブビュー上で見ることができる。

10.4.3 キュー管理統計

キュー管理は、データ分析とレポート出力をサポートします。

開始前に

キュー管理の設定については、「地域人員のキューアップの設定」および「待ち時間の検出の設定」を参照してください。

- 「キューイングアップ時間分析」と「地域比較」を選択して、異なる地域のキューイングアップ人

数を比較します。
- キューイングアップ時間分析とマルチレベル比較を選択して、異なる待ち時間レベルのキューイングアップ人数を比較します。
- キューステータス分析と地域比較を選択して、キューが異なるリージョンで特定の長さに留まる時間と継続時間を比較します。
- 異なるキュー長レベルでキューの時間と継続時間を比較するには、「キューステータス分析」と「複数レベル比較」を選択します。

手順

注

内蔵メモリーカードを装着すると、最大1口分のデータを保存できます。NOメモリーカードを装着すると、本機は1週間分のデータしか保存できません。

1. 分析モードを選択します。

   キューイングアップ時間分析

   待ち行列時間分析は、異なる待ち時間レベルの人数を計算する。

   キューステータス分析

   キューステータス分析は、キューが一定の長さを維持する時間と継続時間を計算します。
2. 統計タイプを選択します。

   地域比較

   複数の領域および1つのレベルを分析のために選択することができ、分析チャートを描くことができる。

   マルチレベル比較

   複数のレベルおよび領域を分析のために選択することができ、各領域について1つの分析チャートが描かれる。
3. 1つまたは複数のリージョンをチェックします。
4. キュー長レベルを設定します。1つ以上の所望の範囲チェックボックスと入力値をチェックします。
5. レポートタイプと統計時間を選択します。
6. Counting をクリックしてレポートを生成します。

10.5 顔カウント

顔カウント検出は、重複した顔を除去し、特定の構成された領域に入った又は出た物体の数を計算することができる。

注

- 特定のデバイスモデルでは、最初にVCAリソースページでのフェースカウントを選択する必要

があります。
- この機能に対応しているカメラの機種があります。

10.5.1 顔カウント検出ルールの設定

顔カウント検出規則及びアルゴリズムパラメータを設定した後、装置は、ターゲットを捕捉し、リンク動作を自動的にトリガする。

手順

1. 「設定→面数計算→規則」に移動します。
2. ルールをチェックします。
3. minを入力します。テキストフィールド内の瞳孔距離、またはクリックしてminを描画します。瞳孔距離。描画された瞳孔の距離は、ライブビューの下のボックスに表示される。□

   最小。ひとみ距離

   min.瞳孔距離は、2つの瞳孔間の領域によって構成される最小の正方形サイズを指し、カメラがターゲットを識別するための基本的な基準である。
4. テキストフィールドに最大瞳孔距離を入力するか、またはクリックして最大瞳孔距離を描画します。□

   最大。ひとみ距離

   最大瞳孔距離は、2つの瞳孔間の領域によって構成される最大の正方形サイズを指し、カメラがターゲットを識別するための基本的な基準である。
5. クリックすると、検知領域が描画されます。ライブビューウィンドウでエンドポイントを左クリックして領域を描画し、右クリックして領域の描画を終了します。⬡
6. 検出線を引くにはクリックします。矢印は方向の入力を示し、クリックして方向を変更できます。⁄ ⇌
   - ターゲットが入射方向に沿って計数領域を横切り、検出線を横切る場合、それは入射数として計数される。
   - ターゲットが出口方向に沿って計数領域を横切り、検出線を横切る場合、それは出口数として計数される。
7. 領域Aと領域Bをクリックして描画します。2つの領域が重ならないことを確認します。方向を変更するには、クリックします。A B ⇌
   - ターゲットがA領域からB領域に入る場合、それは入力数としてカウントされる。
   - ターゲットがB領域からA領域に入る場合、それは出口番号としてカウントされる。
8. アーミングスケジュールを設定します。準備スケジュールの設定を参照してください。
9. 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。

10.5.2 オーバーレイとキャプチャ

取り込みパラメータと、ストリームと画像に表示する情報の設定を選択します。

ストリームにVCA 情報を表示する

ターゲットとルール情報を含むスマート情報をストリームに表示します。

アラーム画面にターゲット情報を表示する

アラーム画面をターゲット情報でオーバーレイします。

ターゲット画像設定

カスタムショット、ヘッドショット、ハーフボディショット、フルボディショットを選択できます。

注

「カスタム」を選択すると、必要に応じて幅、頭部高さ、および身長をカスタマイズできます。

Fixed Valueをチェックすると、写真の高さを設定できます。

背景画像の設定

対象画像と比較すると、背景画像は、シーン画像が余分な環境情報を提供する。背景画質、解像度を設定します。バックグラウンドイメージを監視センターにアップロードする必要がある場合は、「バックグラウンドアップロード」をチェックします。

人数オーバーレイ

フローオーバーレイタイプを選択します。
1日のリセット時間を選択します。すぐにリセットする場合は、「手動リセット」をクリックします。

カメラ

撮影した画像にオーバーレイできるカメラの機器番号とカメラ情報を設定します。

テキストオーバーレイ

撮影した画像に表示する場合は、希望する項目を確認し、順番を調整することができます。

デバイスNo.とカメラ情報の内容は、同じページにある必要があります。

10.5.3 顔カウントアルゴリズムパラメータ

これは、顔カウントのためのアルゴリズムパラメータのパラメータを設定し、最適化するために使用される。

注

これらの関数は、異なるモデルに従って変化する。

顔キャプチャモード

現在のアルゴリズムバージョンを参照しますが、これは編集できません。

ベストショット

ターゲットの後の最良のショットは、検出領域を離れる。

撮影時間

これは、設定された領域に顔が滞在している間に顔がキャプチャされるキャプチャ時間を指す。デフォルト値は1です。

キャプチャしきい値

キャプチャとアラームをトリガーする顔の品質を指します。値を大きくすると、キャプチャおよびアラームをトリガするためにより良い品質を満たす必要があることを意味します。

顔面暴露

デバイスは、画像内の顔を検出したときに、顔の明るさを調整します。

基準輝度

顔の露出モードにおける、顔の基準となる明るさのことです。顔を検出すると、設定した値に応じてカメラが顔の明るさを調整します。値が高いほど、顔は明るい。

最小。期間

カメラが顔を露出する最短時間です。

注

顔の露出が有効になっている場合は、WDR機能が無効になっていることを確認し、マニュアルアイリスを選択します。

リアルタイム更新データ

使用可能になった後、リアルタイムの人数カウントデータがプラットフォームにアップロードされる。

データ統計サイクル

必要に応じてデータ統計サイクルを選択します。

アルゴリズムの有効性

値が高いほど、ターゲットの検出は困難であるが、検出精度は高い。

デフォルトの復元

Restore(復元)をクリックして、詳細設定のすべての設定を工場出荷時のデフォルトに復元します。

10.5.4 顔カウント結果の表示

手順

1. アプリケーションに移動します。
2. 検索条件を設定し、「カウント」をクリックします。
   一致した結果は、Face Picture Comparison Statistics and People Counting Statisticsareaに示されている。

10.6 顔の比較とモデリング

特定のデバイスモデルでは、VCAリソースページでマルチターゲットタイプ検出またはフェースキャプチャを最初に有効にする必要があります。

注

この関数は、特定のデバイスモデルによってのみサポートされます。

10.6.1 面比較

顔比較は、キャプチャされた顔を顔画像ライブラリ内の顔と比較することによって、顔認識の目的に役立つ。

顔写真ライブラリの設定

顔画像ライブラリは、モデル化された人間の顔及び情報をストレージするために使用される。

手順

1. コンフィギュレーション→の顔画像ライブラリに移動します。
2. 顔写真ライブラリを作成します。
   1) クリックして、顔写真ライブラリを追加します。
   2) ライブラリー名、しきい値、および注釈を入力します。

      しきい値

      設定された閾値よりも高いファス類似度は、顔画像比較アラームアップロードをトリガする。
   3) [OK]をクリックします。
   4) オプション:顔写真ライブラリを変更します。目的のライブラリを選択し、関連するパラメータをクリックして変更します。
   5) オプション: ライブラリを削除します。目的のライブラリを選択し、をクリックします。
3. 顔写真をライブラリに追加します。

注

画像形式はJPEGで、1ファイルあたり300KB以下のサイズにしてください。

顔写真を1枚追加　追加をクリックし、顔の詳細情報を含む顔写真をアップロードします。

顔写真を一括してインポートする　取り込みをクリックし、画像パスを選択します。

注

- 顔画像を一括してインポートすると、顔名として画像名が保存されます。その他の顔情報については、手動で1つずつ変更する必要があります。
- エクスポートおよびインポートの検証コードは、数値、大文字、小文字を含む8～16桁の組み合わせである必要があります。

4. オプション: 顔情報を変更します。
   1) 顔写真ライブラリを選択します。
   2) 対象とする顔画像を選択します。名前や性別などの検索条件を入力して画像を検索し、「検索」をクリックします。
   3) 変更をクリックします。
   4) 詳細情報を編集します。

   注

   顔写真は変更できません。

   5) [OK]をクリックします。
5. ライブラリ内の各顔ピクチャのモデルを作成します。

   モデリングプロセスは、各顔画像に対して顔モデルを構築する。顔画像の比較を有効にするためには、顔モデルが必要である。

   モデリング　1つ以上の顔写真を選択し、Modeling(モデリング)をクリックします。

   バッチモデリング　顔写真ライブラリを選択し、「バッチモデリング」をクリックします。

6. 必要に応じて、これを繰り返すと、顔ライブラリがさらに作成されます。
7. 保存をクリックします。

顔写真の比較を設定する

キャプチャした画像とライブラリ内の顔画像を比較し、比較結果を出力します。比較結果は、アーミングスケジュールおよびリンケージ方法が設定されたときに、特定のアクションをトリガすることができる。

開始前に

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

手順

1. 構成→比較およびモデリング・→顔面比較およびモデリングに進みます。
2. 「顔画像の比較」を選択します。
3. 「顔画像の比較を有効にする」をチェックします。
4. 参照として顔写真ライブラリを選択します。
5. オプション: マルチターゲットタイプキャプチャアラーム中に顔比較情報を受信する場合は、マルチターゲットタイプキャプチャアラーム中にレポート顔比較情報をチェックします。
6. アップロードする顔情報を選択します。
7. 顔比較モードを選択します。

最良の比較	装置は、顔ターゲットが検出領域に留まっているときにターゲット顔を連続的に捕捉して比較し、ターゲット顔がその領域を離れたときに最良のスコアの顔画像及び関連するアラーム情報をアップロードする。
迅速な比較	装置は、顔の等級付けが、捕捉のための設定された顔の等級付け閾値を超えるときに、ターゲット顔を捕捉し、比較する。

キャプチャのフェースグレーディングしきい値

顔を取り込んでアップロードするかどうかをデバイスが判断するための顔のグレーディングしきい値(face grading threshold)。

最大。撮影間隔

ターゲットが検出領域にあるときの2つのキャプチャ間の最大間隔。顔の等級が設定したしきい値に達していなくても、最大間隔に達すると撮影されます。

クイックセットアップモード

実際の使用シナリオに従ってモードを選択します。カスタムモードでは、「比較タイムアウト」と「比較時間」を設定できます。

8. アーミングスケジュールを設定します。準備スケジュールの設定を参照してください。
9. 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。

顔面比較結果の表示

手順

1. アプリケーションに移動します。
2. 検索条件を設定し、「カウント」をクリックします。
   一致した結果を顔画像比較統計領域に示す。

10.6.2 フェイスモデリング

顔モデリングは、顔画像を収集し、顔モデルを作成し、データを監視センタにアップロードする目的に役立つ。

開始前に

顔画像収集のために、顔キャプチャまたはマルチターゲットタイプ検出を構成すべきである。設定手順については、フェースキャプチャまたはマルチターゲットタイプ検出を参照してください。

手順

1. 構成→比較およびモデリング・→顔面比較およびモデリングに進みます。
2. [Face Modeling]を選択して開始します。
3. [Enable Face Modeling]をチェックします。
4. モデリングのパラメータを設定します。

   マルチターゲット型キャプチャアラームにおける顔モデリング情報のレポート

   人物がマルチターゲットタイプの検出をトリガすると、アラーム情報は、チェックされた場合、検出された顔の顔モデリング情報を含む。

   クイックキャプチャ

   装置は、キャプチャのために設定された顔格付け閾値よりも高いスコアを有する顔を検出すると、顔モデリングを開始する。

   キャプチャのフェースグレーディングしきい値

   顔を取り込んでアップロードするかどうかをデバイスが判断するための顔のグレーディングしきい値(face grading threshold)。より高い値は、より良好な画質を意味する。

   最大。撮影間隔

   ターゲットが検出領域にあるときの2つのキャプチャ間の最大間隔。顔の等級が設定したしきい値に達していなくても、最大間隔に達すると撮影されます。
5. アーミングスケジュールを設定します。準備スケジュールの設定を参照してください。
6. リンク方法を設定します。リンク方法の設定を参照してください。

10.7 ハードハード検出

この機能は、設定された監視領域で、ハードハットを着用せずにアラームをトリガーするターゲッ

トを検出します。

注

特定のデバイスモデルのみがこの機能をサポートする。

10.7.1 Hard Hart Detection を設定する

開始前に

コンフィギュレーション→システム設定→ VCAリソースに移動して、ハードハット検知を有効にします。

手順

1. 構成→のハードハット検出に移動し、ハードハット検出を有効にするをオンにします。
2. オプション: ターゲット生成速度を設定します。

   目標発電速度

   検出領域に入る顔の目標生成速度を指します。この値が大きいほど、発生速度は速い。
3. 検出領域を設定します。
   1) 検出領域を選択します。
   2) Draw Area をクリックし、ライブビュー画像でリージョンのエンドポイントをクリックして描画します。
   3) 右クリックして描画を終了します。

   Stop Drawing をクリックします。 領域の描画を終了します。

   Clear Allをクリックする 再度領域を描画します。

図 10-4 ハード検出

4. アーミングスケジュールの設定については、「アーミングスケジュールの設定」を参照してください。連動方法の設定については、連動方法の設定を参照してください。
5. 保存をクリックします。

10.8 道路交通

設定した車線に入ると、自動車、非自動車、歩行者を検知・捕捉し、道路上の目標物の迅速な検知と総合的な監視を実現します。

注

この機能をサポートするのは、特定のデバイスモデルのみである。

10.8.1 車両検知の設定

設定した車線に進入した車両を検知し、車両とそのナンバープレートの写真を撮影・保存することができます。アラームがトリガーされ、キャプチャをアップロードできます。

開始前に

「コンフィギュレーション→システム設定→ VCAリソース」に移動し、「ロードトラフィック」を選択します。

手順

1. 「構成→道路交通→検出構成」に進み、検出種別として「車両検出」を選択します。
2. 有効をチェックします。
3. レーン番号を選択します。
4. レーンラインをクリックしてドラッグしてその位置を設定するか、またはラインエンドをクリックしてドラッグしてラインの長さと角度を調整します。
5. 映像中の車両の大きさが赤枠の大きさに近くなるように、カメラのズーム倍率を調整します。赤枠の位置のみ調整可能です。

注

レーンごとに一度にキャプチャできるナンバープレートは1 つだけです。

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

出入口	検知された車両のナンバープレート情報は、車両が検知エリアを通過するとアップロードされ、出入り口の検知をトリガーします。
シティストリート	検出された車両のナンバープレート情報は、車両が検出エリアを通過し、市街地で検出をトリガするときにアップロードされる。
アラーム入力	これは、入力アラームがナンバープレート捕捉および認識動作をトリガすることを意味する。

注

アラーム入力が選択されると、アラーム入力A<-1は自動的に車両検知をトリガするように割り当てられ、そのアラームタイプは常にNOになります。A<-1アラーム入力が車両検知をトリガするために使用される場合、他の基本イベントには使用できません。アラーム入力を選択して保存した場合は、A<-1のリンク方式は解除されます。

8. 検出モードを選択します。
9. 重複したライセンスプレートの削除をチェックし、時間間隔を設定します。デフォルトの時間間隔は4 分です。

注

ナンバープレートは最大8枚までサポートされています。

10. アーミングスケジュールとリンク方法を設定します。アーミングスケジュールの設定については、「アーミングスケジュールの設定」を参照してください。連動方法の設定については、連動方法の設定を参照してください。
11. 保存をクリックします。

10.8.2 混在トラフィック検出ルールの設定

設定した車線に進入した自動車、非自動車、歩行者を検出し、目標物の絵を捉えて保存することができる。アラームがトリガーされ、キャプチャをアップロードできます。

開始前に

「コンフィギュレーション→システム設定→ VCAリソース」に移動し、「ロードトラフィック」を選択します。

手順

1. 「構成→道路交通→検出構成」に進み、「混合交通検出」を検出種別として選択します。
2. 有効をチェックします。
3. レーン番号を選択します。
4. 地域と国/地域を選択します。
5. アーミングスケジュールとリンク方法を設定します。アーミングスケジュールの設定については、「アーミングスケジュールの設定」を参照してください。連動方法の設定については、連動方法の設定を参照してください。
6. 保存をクリックします。

10.8.3 画像設定をアップロードする

車両検知、混交検知では、撮影画像の画像パラメータを設定できます。
「→道路交通→の設定」画面に移動します。

画質

値が大きいほど、ピクチャはより明瞭になるが、より大きなストレージスペースも必要とされる。

画像サイズ

値が大きいほど、必要なストレージ空間は大きくなる。また、ネットワーク伝送要求のレベルも高くなる。

ライセンスプレートの拡張

値が大きいほど、ナンバープレートはより明瞭であるが、より大きな貯蔵スペースも必要とされる。

ライセンスプレートの拡張をチェックし、レベルを設定します。デフォルトのレベルは50 です。

オーバレイ

キャプチャした画像にカメラ、デバイス、または車両の情報をオーバーレイし、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。↑ ↓

カメラの設定については、「設定→道路交通→カメラ」に移動して、関連パラメータを設定し、「保存」をクリックします。

10.8.4 カメラの設定

各カメラのパラメータを設定することで、管理を向上させることができます。

「設定→道路交通→カメラ」に移動して、関連パラメータを設定し、「保存」をクリックします。

10.8.5 ブロックリストおよび許可リストのインポートまたはエクスポート

必要に応じてblocklist とallowlist をインポートおよびエクスポートし、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. Browse(参照)をクリックして、PC ローカルディレクトリを開きます。
2. blocklist & allowlist ファイルを検索し、クリックして選択します。開くをクリックして確定します。

注

インポートするファイルは、カメラが必要とするファイルテンプレートに対応している必要があります。テンプレートとしてカメラから空のブロックリストおよびallowlistファイルをエクスポートし、コンテンツを入力することをお勧めします。ファイルは。xls にある必要があります。 書式とセルの書式は「テキスト」にする必要があります。

3. 「読み込み」をクリックして、選択したファイルを読み込みます。
4. Export(エクスポート)をクリックして、PC のローカルディレクトリを開きます。
5. PC ローカルディレクトリ内のディレクトリを選択します。
6. ファイル名テキストファイルのファイル名を指定します。

7. 保存をクリックします。

第 11 章 プラットフォームを開く

オープンプラットフォームを使用すると、サードパーティがその機能とサービスを開発および実行するためのアプリケーションをインストールできます。

注

特定のデバイスモデルのみがこの機能をサポートする。

11.1 オープンプラットフォームの設定

手順

1. コンフィギュレーション→オープンプラットフォームに移動します。

注

アプリケーションをインストールする前に、下部にある「ディスクレーマ」を参照して、インストールするアプリケーションが以下の条件に適合していることを確認してください。

- 各アプリケーションは、それ自身の排他的な名前を有する。
- アプリケーションが占有するFLASH メモリ空間は、デバイスの使用可能なFLASH メモリ空間よりも小さくなります。
- アプリケーションのメモリおよび計算能力は、デバイスの利用可能なメモリおよび計算能力よりも小さい。

2. 「アプリのインストール」で、「参照」をクリックし、インポートしたアプリケーションパッケージを選択します。
3. インポートをクリックしてインストールを完了します。

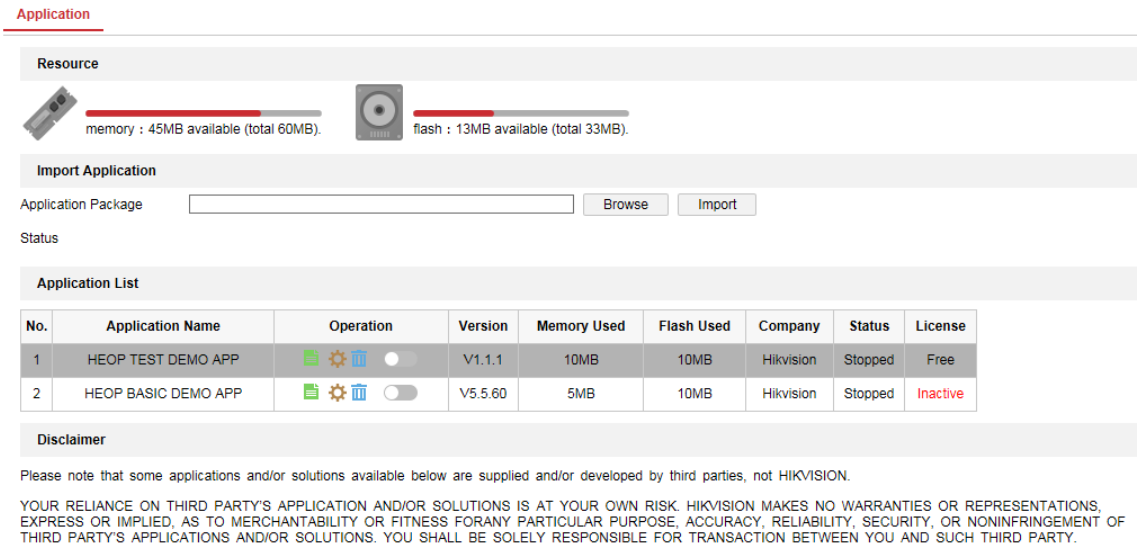

図 11-1 プラットフォームを開く

インストールされたアプリケーションおよびそれらの関連情報は、アプリケーション名、動作、バージョン、使用されたメモリ、使用されたフラッシュ、会社、ステータス、およびライセンスなどのアプリケーションリストに表示される。

4. オプション: アプリケーションを設定します。

	ログのエクスポート。
	許可を設定します。
	アプリケーションを削除します。
	アプリケーションを有効または無効にします。

5. (オプション) アプリケーション表示で、「参照」をクリックし、アプリケーション証明書をインポートします。

第 12 章スマートディスプレイ

スマート機能を有効にすると、撮影した画像を表示できます。

注

この関数は、特定のデバイスモデルによってのみサポートされます。

レイアウトプレビュー

[レイアウトのプレビュー]をクリックして選択します。必要に応じてコンテンツを選択します。リアルタイム解析を選択すると、リアルタイム解析のみの内容を選択できます。

検出属性

Detection Attribute をクリックして選択します。この機能を有効にすると、ターゲット分析の属性情報を表示でき、選択した情報が属性分析領域に表示されます。

第13章EPTZ

EPTZ (Electronic PTZ) は、物理的なカメラの動きを伴わずに、画像の一部にデジタルズームおよびパンする高解像度機能です。EPTZ 機能を使用する場合は、ライブビューで「Fourth Stream」を選択していることを確認します。第4のストリームおよびEPTZは、両方とも同時にイネーブルされるべきである。

注

この関数は、特定のデバイスモデルによってのみサポートされます。

13.1 パトロール

手順

1. 構成→ EPTZ に移動します。
2. Enable EPTZ をチェックします。
3. 4番目のストリームをチェックします。
4. [アプリケーションのパトロール]を選択します。
5. 保存をクリックします。

次にどうするか

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

13.2 自動追跡

手順

1. 構成→ EPTZ に移動します。
2. Enable EPTZ をチェックします。
3. 4番目のストリームをチェックします。
4. ApplicationでAuto-trackingを選択します。
5. Detection Areaをクリックして描画を開始します。
6. ライブビデオをクリックして検知領域の4つの頂点を指定し、右クリックして描画を完了します。
7. ルールを設定します。

検出対象

ヒトおよびビヒクルが利用可能である。検出ターゲットが選択されない場合、人間及び車両を含む全ての検出ターゲットが追跡される。

注

この機能に対応しているカメラの機種があります。

感度	これは、追跡される許容可能なターゲットの身体部分のパーセンテージを表す。感度 = 100 - S1/ST × 100。S1は、所定の領域に入る目標身体部分を表す。STは、完全な標的体を表す。感度の値が高いほど、より容易にターゲットを追跡することができる。

8. 保存をクリックします。

A. デバイスコマンド

次のQRコードをスキャンして、デバイス共通シリアルポートコマンドを取得します。
コマンド・リストは、すべてのHikvisionネットワーク・カメラに共通して使用されるシリアル・ポート・コマンドを含むことに留意されたい。

B. デバイス通信マトリックス

次のQRコードをスキャンして、デバイスの通信マトリックスを取得します。
マトリックスは、Hikvisionネットワークカメラのすべての通信ポートを含むことに留意されたい。

See Far, Go Further