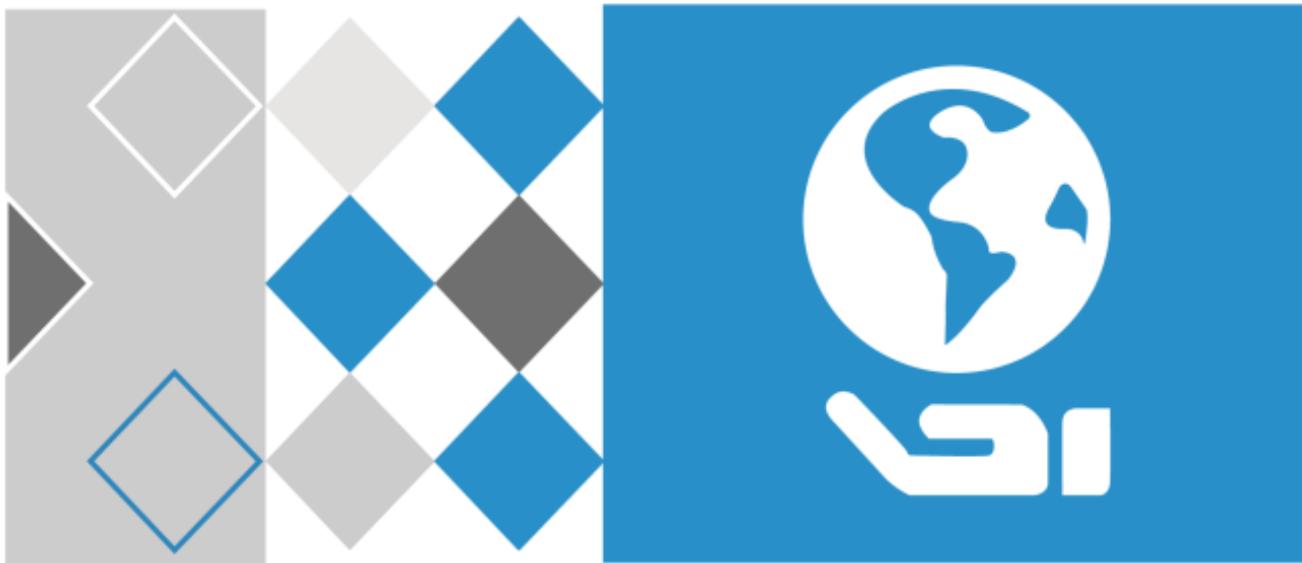


HiLock



ネットワークカメラ

ユーザーマニュアル

免責事項

この文書について

- 本ドキュメントには、製品の使用および管理に関する指示が含まれています。以下に示す写真、図表、画像およびその他すべての情報は、説明および解説のみを目的としています。
- 本ドキュメントに記載されている情報は、ファームウェアの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。最新版はHikvisionウェブサイト（<https://www.hikvision.com>）でご確認ください。別途合意がない限り、杭州海康威視デジタル技術有限公司またはその関連会社（以下「Hikvision」）は、明示的または默示的を問わず、一切の保証を行いません。
- 本製品をサポートする訓練を受けた専門家の指導と支援のもとで、本ドキュメントをご利用ください。

本製品について

- 本製品は、購入された国または地域でのみアフターサービスサポートを受けることができます。
- お選びいただいた製品が映像製品の場合は、以下のQRコードをスキャンして「映像製品の使用に関する取り組み」を入手し、よくお読みください。



知的財産権に関する認識

- Hikvision は、本書に記載された製品に組み込まれた技術に関する著作権および/または特許を所有しており、これには第三者から取得したライセンスが含まれる場合があります。
- 本文書のテキスト、画像、グラフィックなど、その一部はすべて Hikvision に帰属します。書面による許可なく、本文書のいかなる部分も、その全部または一部を、いかなる手段によっても抜粋、複製、翻訳、または改変することはできません。
- **HiLook** および他の Hikvision の商標およびロゴは、さまざまな法域における Hikvision の所有物です。
- 記載されている他の商標およびロゴは、それぞれの所有者に帰属します。

法的免責事項

- 適用される法律で許容される最大限の範囲において、本ドキュメントおよび記載されている製品（そのハードウェア、ソフトウェア、ファームウェアを含む）は、「現状有姿

のまま」かつ「すべての欠陥およびエラーを含む」状態で提供されます。HIKVISIONは、商品性、満足のいく品質、特定目的への適合性など、明示または默示を問わず、いかなる保証も行いません。本製品のご利用は、お客様ご自身のリスクにおいて行われます。いかなる場合においても、HIKVISIONは、特別損害、結果的損害、付随的損害、間接損害（事業利益の損失、事業中断、データ損失、システムの破損、または文書の損失を含むがこれらに限定されない損害について、契約違反、不法行為（過失を含む）、製造物責任その他のいかなる法的根拠に基づくものであっても、本製品の使用に関連して生じた場合、たとえHIKVISIONがそのような損害または損失の可能性について事前に通知を受けていた場合であっても、一切の責任を負いません。

- お客様は、インターネットの本質に内在するセキュリティリスクを認識し、サイバー攻撃、ハッカー攻撃、ウイルス感染、その他のインターネットセキュリティリスクに起因する異常動作、プライバシー漏洩その他の損害について一切の責任を負いません。ただし、必要に応じてタイムリーな技術サポートを提供します。
- お客様は、適用される全ての法令を遵守して本製品を使用することに同意し、お客様の使用が適用法令に準拠していることを確認する責任はお客様のみにあります。特に、本製品の使用が第三者の権利（パブリシティ権、知的財産権、データ保護およびその他のプライバシー権を含むがこれらに限定されない）を侵害しない方法で行う責任を負います。お客様は、大量破壊兵器の開発または製造、化学兵器または生物兵器の開発または製造、核爆発物または安全でない核燃料サイクルに関連する文脈における活動、または人権侵害を支援する活動。
- 本文書と適用される法律との間に矛盾が生じた場合、後者が優先する。

© Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

ファームウェアの更新

ユーザー エクスペリエンス向上のため、お使いのデバイスを最新のファームウェアにできるだけ早く更新することをお勧めします。

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

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

アップグレード設定については、「アップグレード」を参照してください。

記号の定義

本ドキュメントで使用される記号は、以下の通り定義されています。

記号	説明
 危険	回避しなければ死亡または重傷を負う危険な状況があることを示す。
 注意	回避しなければ、機器の損傷、データの損失、性能の低下、または予期しない結果をもたらす可能性のある潜在的な危険な状況を示します。
 注記	本文の重要な点を強調または補足する追加情報を提供します。

安全上の注意

これらの指示は、ユーザーが製品を正しく使用し、危険や財産の損失を避けることを目的としています。

法令 規制

- 本装置は、現地の法令、電気安全規制、防火規制に準拠して使用してください。

電気

- 本製品の使用にあたっては、当該国および地域の電気安全規制を厳守しなければなりません。
- 本機器は、水滴や飛沫にさらされないようにし、花瓶などの液体が入った容器を機器の上に置かないでください。
- 山頂、鉄塔、森林などの特殊な条件下では、機器の入力開口部にサージサプレッサを設置してください。
- 注意：火災の危険を減らすため、ヒューズは同じ種類および定格のものと交換してください。
- 本装置は、接地された電源コンセントに接続してください。
- 機器外部に適切な容易にアクセス可能な遮断装置を設置すること。
- 機器外部に、建物の仕様を超えない適切な過電流保護装置を設置すること。
- 建物の電気設備には、全極電源スイッチを設置すること。
- AC 電源への接続用端子の正しい配線を確認してください。
- 本装置は、必要に応じてIT配電システムへの接続用に設計・改造されています。

電池

- 電池を飲み込まないでください。化学火傷の危険性があります！
- 本製品にはコイン型/ボタン型電池が含まれています。コイン型/ボタン型電池を飲み込むと、わずか2時間で重度の内部やけどを引き起こし、死に至る可能性があります。
- 新品および使用済み電池は、子供の手の届かない場所に保管してください。
- 電池ケースが確実に閉まらない場合は、製品の使用を中止し、子供の手の届かない場所に保管してください。
- 電池が飲み込まれた、または体内に挿入された可能性がある場合は、直ちに医師の診察を受けてください。
- 注意：誤った種類の電池と交換すると爆発の危険があります。使用済み電池は指示に従って廃棄してください。
- 注意：誤った種類の電池と交換すると爆発の危険があります。使用済み電池は指示に従って廃棄してください。
- 誤った種類の電池への不適切な交換は、安全装置を無効にする可能性があります（例：一部のリチウム電池タイプの場合）。
- 電池を火中や高温のオーブンに投入したり、機械的に押しつぶしたり切断したりしない

でください。爆発の原因となる可能性があります。

- 電池を極端に高温の環境に放置しないでください。爆発や可燃性液体・ガスの漏出の原因となる可能性があります。
- 電池を極端に低い気圧にさらさないでください。爆発や可燃性液体・ガスの漏出の原因となる可能性があります。
- + は直流を使用または発生する機器のプラス端子を示します。- は直流を使用または発生する機器のマイナス端子を示します。

防火

- 点灯したろうそくなどの裸火を機器の上に置かないでください。
- 本装置のシリアルポートは、デバッグ専用です。

高温表面防止

-  注意: 高温部品! 部品を扱う際に指を火傷する恐れがあります。電源を切ってから30分待ってから部品を扱ってください。このステッカーは、表示された部品が高温になる可能性があり、注意を払わずに触れてはいけないことを示すものです。このステッカーが付いている装置は、アクセスが制限された場所に設置することを意図しており、サービス担当者またはその場所への制限の理由と取るべき予防措置について指導を受けたユーザーのみがアクセスできます。

設置

- 本マニュアルの指示に従って装置を設置してください。
- 負傷を防ぐため、設置指示に従い本機器を床/壁に確実に固定してください。
- 機器を不安定な場所に設置しないでください。機器が落下し、重大な人身事故や死亡事故を引き起こす恐れがあります。

電源

- 入力電圧は、IEC60950-1規格: SELV (安全超低電圧) および限定電源に準拠している必要があります。詳細については、該当する文書を参照してください。
- 電源は、IEC 60950-1 または IEC 62368-1 規格に基づく限定電源または 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機器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てください。

白色光照明装置（対応機種の場合）

- 本製品からは危険な可能性のある光放射が発生します。
- 動作中の光源を直視しないでください。目に有害な場合があります。
- カメラの組み立て、設置、またはメンテナンス時には、適切な保護メガネを着用するか、白色光を点灯しないでください。

輸送

- 輸送中は、本製品を元の梱包材または同等の梱包材に入れてください。

システムのセキュリティ

- パスワードおよびセキュリティ設定は、設置者および使用者が責任を負います。

保守

- 製品が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までご連絡ください。
- 無許可の修理やメンテナンスによって生じた問題については、当社は一切の責任を負いません。

お手入れ

- 製品カバーの内側および外側の表面を清掃する際は、柔らかく乾いた布をご使用ください。アルカリ性洗剤は使用しないでください。

使用環境

- レーザー機器を使用する際は、装置のレンズがレーザー光に直接当たらないようにしてください。そうでないと、レンズが焼損する恐れがあります。
- 高電磁放射環境や粉塵の多い環境に装置を曝さないでください。
- 屋内専用機器は、乾燥した換気の良い環境に設置してください。
- レンズを太陽やその他の強い光源に向けてはいけません。
- 動作環境が装置の要求を満たしていることを確認してください。動作温度は-30°C~60°C (-22°F~140°F)、動作湿度は95%以下（結露なし）である必要があります。
- カメラを極端な高温・低温、粉塵や湿気の多い場所に置かないでください。また、強い電磁放射にさらさないでください。

緊急時

- 本機から煙、異臭、異音が発生した場合は、直ちに電源を切り、電源ケーブルを抜いてサービスセンターに連絡してください。

時刻同期

- ローカル時間がネットワーク時間と同期していない場合、初回アクセス時に手動でデバイスの時刻を設定してください。Web ブラウザ/クライアントソフトウェアからデバイスにアクセスし、時刻設定インターフェースに移動します。

反射

- 装置レンズの近くに反射面が近接していないことを確認してください。装置からの赤外線がレンズに反射し、反射を引き起こす可能性があります。

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によるデバイスのアクティベーション	2
2.2 ブラウザ経由でのデバイス起動	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回復	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タイプ	6
3.1.4 サードパーティ製プラグインの選択	6
3.1.5 照明	7
3.1.6 ピクセルカウント	7
3.1.7 デジタルズーム開始	7
3.1.8 補助フォーカス	7
3.1.9 レンズ初期化	8
3.1.10 クイックセットライブビュー	8
3.1.11 レンズパラメータ調整	8
3.1.12 3D位置決めを実施	9
3.2 伝送パラメータ設定	9
3.3 スムーズストリーミングの設定	10
第4章 映像と音声	12
4.1 ビデオ設定	12

4.1.1 ストリームタイプ	12
4.1.2 動画タイプ	13
4.1.3 解像度	13
4.1.4 ビットレートタイプと最大ビットレート	13
4.1.5 ビデオ品質	13
4.1.6 フレームレート	14
4.1.7 ビデオエンコーディング	14
4.1.8 スムージング	16
4.2 ROI	16
4.2.1 ROI の設定	16
4.3 ストリーム上の情報表示	17
4.4 オーディオ設定	17
4.4.1 オーディオエンコーディング	17
4.4.2 オーディオ入力	17
4.4.3 オーディオ出力	18
4.4.4 環境ノイズフィルター	18
4.5 双方向オーディオ	18
4.6 表示設定	19
4.6.1 シーンモード	19
4.6.2 画像パラメータ切り替え	22
4.6.3 ビデオ規格	22
4.6.4 ローカルビデオ出力	23
4.7 OSD	23
4.8 プライバシーマスク設定	23
4.9 オーバーレイ画像	24
4.10 ターゲットクロップの設定	24
第5章 ビデオ録画と画像キャプチャ	26
5.1 ストレージ設定	26
5.1.1 新規または暗号化されていないメモリカードの設定	26

5.1.2 FTP の設定	28
5.1.3 NAS の設定	29
5.1.4 eMMC保護	30
5.1.5 クラウドストレージの設定	30
5.2 ビデオ録画	31
5.2.1 自動録画	31
5.2.2 手動録画	32
5.2.3 Liteストレージの設定	33
5.2.4 動画の再生とダウンロード	33
5.3 キャプチャ設定	34
5.3.1 自動キャプチャ	34
5.3.2 手動キャプチャ	34
5.3.3 タイミングウェイクの設定	35
5.3.4 画像の表示とダウンロード	35
第6章 イベントとアラーム	36
6.1 基本イベント	36
6.1.1 モーション検知の設定	36
6.1.2 ビデオ改ざん警報の設定	38
6.1.3 PIR警報の設定	39
6.1.4 例外アラーム設定	40
6.1.5 アラーム入力の設定	40
6.1.6 映像品質診断の設定	41
6.1.7 振動検知設定	41
6.2 スマートイベント	42
6.2.1 音声異常検出	42
6.2.2 焦点外れ検出の設定	43
6.2.3 シーン変化の検出	43
6.2.4 顔検出の設定	44
6.2.5 映像喪失設定	44

6.2.6 侵入検知の設定	44
6.2.7 ライン越え検知の設定	45
6.2.8 区域進入検知の設定	47
6.2.9 区域退出検知の設定	48
6.2.10 無人荷物検知の設定	49
6.2.11 物体除去検知の設定	50
6.2.12 描画領域	51
6.2.13 サイズフィルターの設定	51
第7章 ネットワーク設定	52
7.1 TCP/IP	52
7.1.1 マルチキャスト	53
7.1.2 マルチキャスト検出	54
7.2 SNMP	54
7.3 SRTPの設定	54
7.4 ポートマッピング	55
7.4.1 自動ポートマッピングの設定	56
7.4.2 手動ポートマッピングの設定	56
7.4.3 ルータでのポートマッピング設定	56
7.5 ポート	57
7.6 ドメイン名によるデバイスへのアクセス	58
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	59
7.8 ワイヤレスダイヤル	60
7.8.1 ワイヤレスダイヤル設定	60
7.8.2 許可リストの設定	61
7.9 Wi-Fi	61
7.9.1 デバイスをWi-Fiに接続	61
7.10 ネットワークサービスの設定	62
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	63
7.12 ISUPの設定	64

7.13 アラームサーバーの設定	64
7.14 HiLookVision経由でカメラにアクセス	65
7.14.1 カメラで HiLookVision サービスを有効にする	66
7.14.2 HiLookVisionの設定	67
7.14.3 HiLookVisionへのカメラ追加	67
第8章 警戒スケジュールと警報連動	69
8.1 警戒スケジュール設定	69
8.2 連動方法の設定	69
8.2.1 アラーム出力のトリガー	69
8.2.2 FTP/NAS/メモリカードへのアップロード	71
8.2.3 メール送信	71
8.2.4 監視センターへの通知	72
8.2.5 録画のトリガー	72
8.2.6 点滅ライト	72
8.2.7 音声警告	73
第9章 システムとセキュリティ	75
9.1 デバイス情報の表示	75
9.2 ログの検索と管理	75
9.3 同時ログイン	75
9.4 設定ファイルのインポートとエクスポート	75
9.5 診断情報のエクスポート	76
9.6 再起動	76
9.7 復元とデフォルト設定	76
9.8 アップグレード	76
9.9 オープンソースソフトウェアライセンスの表示	77
9.10 ウィーガンド	77
9.11 メタデータ	77
9.12 日付と時刻	78
9.12.1 手動で時刻を同期する	78

9.12.2 NTP サーバーの設定	78
9.12.3 衛星による時刻同期	79
9.12.4 夏時間設定	79
9.13 RS-485の設定	79
9.14 RS-232の設定	80
9.15 消費電力モード	80
9.16 外部デバイス	81
9.16.1 補助照明設定	81
9.16.2 ヒーター	82
9.17 セキュリティ	82
9.17.1 認証	82
9.17.2 IP アドレスフィルタの設定	83
9.17.3 HTTPS の設定	84
9.17.4 QoS の設定	84
9.17.5 IEEE 802.1Xの設定	84
9.17.6 制御タイムアウト設定	85
9.17.7 セキュリティ監査ログの検索	85
9.17.8 セキュリティ強化	86
9.17.9 SSH	86
9.18 証明書管理	86
9.18.1 自己署名証明書の作成	86
9.18.2 証明書要求の作成	87
9.18.3 証明書のインポート	87
9.18.4 サーバー/クライアント証明書のインストール	87
9.18.5 CA証明書のインストール	88
9.18.6 証明書有効期限アラームの有効化	88
9.19 ユーザーとアカウント	89
9.19.1 ユーザーアカウントと権限の設定	89
9.19.2 同時ログイン	90

9.19.3 オンラインユーザー	90
第10章 VCAリソースの割り当て	91
10.1 スマートモードの切り替え	91
10.2 顔キャプチャ	92
10.2.1 顔キャプチャの設定	93
10.2.2 オーバーレイとキャプチャ	94
10.2.3 顔キャプチャアルゴリズムのパラメータ	94
10.2.4 シールド領域の設定	96
10.3 道路交通	96
10.3.1 車両検出の設定	97
10.3.2 混合交通検出ルールの設定	98
10.3.3 画像アップロード設定	98
10.3.4 カメラ設定	99
10.3.5 ブロックリストと許可リストのインポート/エクスポート	99
10.4 マルチターゲットタイプ検出	100
10.4.1 マルチターゲットタイプ検出ルール設定	100
10.4.2 オーバーレイとキャプチャ	100
10.4.3 マルチターゲットタイプ検出アルゴリズムのパラメータ	101
10.4.4 シールド領域の設定	102
10.5 顔検出	103
10.5.1 顔検出ルールの設定	103
10.5.2 オーバーレイとキャプチャ	104
10.5.3 顔検出アルゴリズムのパラメータ	105
10.5.4 顔検出結果の表示	106
10.6 キュー管理	106
10.6.1 地域別待ち行列設定	106
10.6.2 待機時間検出の設定	107
10.6.3 キュー管理統計	108
10.7 カウント	109

10.7.1 カウント設定	109
10.7.2 カウント統計の表示	110
10.8 ヘルメット検出	111
10.8.1 ヘルメット検出の設定	111
10.9 顔画像比較とモデリング	112
10.9.1 顔写真比較	112
10.9.2 顔モデリング	114
第11章 オープンプラットフォーム	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	117
第13章 EPTZの設定	118
13.1 パトロール	118
13.2 自動追跡	118
第14章 パターン運動	120
14.1 パターンリンクの設定	120

第1章 システム要件

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

オペレーティングシステム	Microsoft Windows XP SP1 以降
CPU	2.0 GHz 以上
RAM	1GB以上
ディスプレイ	1024×768 解像度以上
Webブラウザ	詳細はプラグインのインストールを参照

第2章 デバイスのアクティベーションとアクセス

ユーザー アカウントとデータのセキュリティおよびプライバシーを保護するため、ネットワーク経由でデバイスにアクセスする際には、ログイン パスワードを設定してデバイスをアクティベートする必要があります。

注記

クライアント ソフトウェアのアクティベーションに関する詳細情報は、ソフトウェア クライアントのユーザーマニュアルを参照してください。

2.1 SADPによるデバイスのアクティベーション

SADP ソフトウェアを使用してオンライン デバイスを検索し、アクティベートします。

開始前に

www.hikvision.com にアクセスし、SADP ソフトウェアを入手してインストールしてください。

手順

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

注意

製品のセキュリティ強化のため、ご自身で選択した強力なパスワード（大文字、小文字、数字、特殊文字を含む8文字以上）の設定を強く推奨します。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（月次または週次で）リセットすることで、製品をより効果的に保護できます。

5. [OK]をクリックします。
デバイスステータスが「アクティブ」に変わります。
6. オプション：[ネットワーク パラメータの変更]でデバイスのネットワーク 設定を変更します。

2.2 ブラウザ経由でのデバイス起動

ブラウザからデバイスにアクセスしてアクティベートできます。

手順

1. ネットワークケーブルを使用してデバイスをPCに接続します。
2. PCとデバイスのIPアドレスを同一セグメントに変更します。



デバイスのデフォルトIPアドレスは192.168.1.64です。PCのIPアドレスは192.168.1.2から192.168.1.253（192.168.1.64を除く）に設定できます。例：PCのIPアドレスを192.168.1.100に設定可能。

3. ブラウザに**192.168.1.64**を入力します。
4. デバイス起動パスワードを設定します。



製品のセキュリティ強化のため、ご自身で選択した強力なパスワード（8文字以上で、大文字、小文字、数字、特殊文字の少なくとも3種類を含む）の作成を強く推奨します。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（月次または週次で）リセットすることで製品をより効果的に保護できます。

5. 「OK」をクリックします。
6. アクティベーションパスワードを入力してデバイスにログインします。
7. オプション：設定 → ネットワーク → 基本 → TCP/IP に移動し、デバイスのIPアドレスをネットワークの同一セグメントに変更します。

2.3 ログイン

Webブラウザからデバイスにログインします。

2.3.1 プラグインのインストール

特定のオペレーティングシステムやウェブブラウザでは、カメラ機能の表示や操作が制限される場合があります。正常な表示と操作を確保するには、プラグインのインストールや特定の設定が必要です。詳細な制限機能については、実際のデバイスをご確認ください。

オペレーティングシステム	ウェブブラウザ	操作
Windows	<ul style="list-style-type: none"> • Internet Explorer 8以降 • Google Chrome 57 および 	ポップアップの指示に従ってプラグインのインストー

オペレーティングシステム	ウェブブラウザ	操作
	それ以前のバージョン ● Mozilla Firefox 52 および それ以前のバージョン	ルを完了してください。
	● Google Chrome 57以降 ● Mozilla Firefox 52以降	 Download Plug-in をクリックしてプラグインをダウンロードし、インストールしてください。
Mac OS	● Google Chrome 57以上 ● Mozilla Firefox 52+ ● Mac Safari 16以上	プラグインのインストールは不要です。 設定 → ネットワーク → 詳細設定 → ネットワークサービスに移動し、WebSocket または Websockets を有効にして通常表示を行ってください。 一部の機能の表示および操作は制限されます。例えば、再生および画像機能は利用できません。詳細な制限機能については、実際のデバイスをご参照ください。



注意

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

2.3.2 管理者パスワードの回復

管理者パスワードを忘れた場合、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場合」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。

注意

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。

セキュリティの質問

アカウントのセキュリティは、アクティベーション時に設定できます。または、[設定] → [システム] → [ユーザー管理] に移動し、[アカウントセキュリティ設定] をクリックして、セキュリティの質問を選択し、その答えを入力してください。

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

Eメール

アクティベーション中にアカウントのセキュリティを設定できます。または、[設定] → [システム] → [ユーザー管理] に移動し、[アカウントセキュリティ設定] をクリックして、回復操作プロセス中に確認コードを受け取るメールアドレスを入力してください。

2.3.3 不正ログインロック

インターネット経由でデバイスにアクセスする際のセキュリティ向上に役立ちます。

設定 → システム → セキュリティ → セキュリティサービスを移動し、不正ログインロックを有効にします。不正ログインの試行回数とロック期間は設定可能です。

不正ログイン試行

設定回数を超える不正なパスワード入力が行われた場合、デバイスがロックされます。

ロック時間

設定され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紹介します。

3.1 ライブビューパラメータ

サポートされる機能はモデルによって異なります。

3.1.1 ライブビューの有効化と無効化

この機能は、チャンネルのライブビューをすばやく有効または無効にするために使用します。

- ▶ をクリックするとライブビューが開始されます。
- をクリックするとライブビューを停止します。

3.1.2 アスペクト比の調整

手順

- 「Live View」をクリックします。
- をクリックしてアスペクト比を選択します。
 - 4:3はウィンドウサイズを指します。
 - 16:9のウィンドウサイズを指します。
 - 元のウィンドウサイズを指します。
 - 自動適応ウィンドウサイズを指します。
 - 元の比率のウィンドウサイズを指します。

3.1.3 ライブビューストリームタイプ

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

3.1.4 サードパーティ製プラグインの選択

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

手順

- 「ライブビュー」をクリックします。
- [□] をクリックしてプラグインを選択します。

Internet Explorerでデバイスにアクセスする場合、WebcomponentsまたはQuickTimeを選択できます。その他のブラウザでデバイスにアクセスする場合、Webcomponents、QuickTime、VLC、またはMJPEGを選択できます。

3.1.5 照明

 をクリックして照明装置のオン/オフを切り替えます。

3.1.6 ピクセルカウント

ライブビュー画像内の選択領域の高さと幅のピクセルを取得するのに役立ちます。

手順

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

3.1.7 デジタルズームの開始

画像内の任意の領域の詳細情報を確認するのに役立ちます。

手順

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

3.1.8 補助焦点

電動式デバイス用です。デバイスが明確に焦点を合わせられない場合、画像の改善が可能です。

ABF対応デバイスでは、レンズ角度を調整後、デバイス上のABFボタンをクリックしてフォーカスします。これによりデバイスは明確に焦点を合わせられます。

 をクリックすると自動でフォーカスします。

注記

- 補助フォーカスでピントが合わない場合、レンズ初期化を実行後、再度補助フォーカスを使用すると画像が鮮明になります。
 - 補助フォーカスでも装置が明確に焦点を合わせられない場合、手動フォーカスを使用できます。
-

3.1.9 レンズ初期化

レンズ初期化は電動レンズ搭載デバイスで使用されます。長時間ズームやフォーカス操作により画像がぼやける場合にレンズをリセットする機能です。この機能は機種によって異なります。

手動レンズ初期化

レンズ初期化を操作するには、 をクリックします。

自動レンズ初期化

→ → → 設定 → システム → メンテナンス → レンズ補正 の順に選択し、本機能を有効化します。設定スケジュールを指定すると、指定時間帯に自動的にレンズ補正が行われます。

3.1.10 クイックセットライブビュー

ライブビュー画面で、PTZ、表示設定、OSD、映像/音声、VCAリソース設定を素早く設定できます。

手順

1.  をクリックし、クイック設定ページを表示します。
2. PTZ、表示設定、OSD、映像/音声、VCAリソースパラメータを設定します。
 - PTZ設定については、レンズパラメータ調整を参照してください。
 - 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。
 - 音声・映像設定については、「映像と音声」を参照してください。
 - VCA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。



この機能は特定のモデルでのみサポートされています。

3.1.11 レンズパラメータ調整

レンズのフォーカス、ズーム、アイリスを調整するために使用します。

ズーム

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

フォーカス

-  をクリックすると、レンズが遠くに焦点を合わせ、遠くの物体が鮮明になります。

- をクリックすると、レンズが近くに焦点を合わせ、近くの物体が鮮明になります。

PTZ スピード

 をスライドさせてパン/チルト動作の速度を調整します。

アイリス

- 画像が暗すぎる場合は、○をクリックして絞り口径を大きくします。
- 画像が明るすぎる場合は、○をクリックしてアイリスを絞り込みます。

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回転機能を無効化し、PTZ調整による対象物の消失を減らすことを意味します。

設定 → PTZ に移動し、Enable PTZ Lock をチェックして Save をクリックします。

3.1.12 3D ポジショニングの実行

3D ポジショニングは、選択した領域を画像の中心に再配置する機能です。

手順

- 「」をクリックして機能を有効にします。
- ライブ画像内で対象領域を選択します。
 - ライブ画像上の任意の点を左クリック：その点がライブ画像の中心に移動します（ズーム効果なし）。
 - マウスを押したまま右下方向にドラッグし、ライブ映像上で領域を枠で囲む：枠で囲まれた領域が拡大され、ライブ映像の中心へ再配置されます。
 - マウスを押したまま左上にドラッグしてライブ映像の一部を枠で囲む：枠で囲まれた領域がズームアウトされ、ライブ映像の中心に再配置されます。
- ボタンを再度クリックすると機能をオフにします。

3.2 伝送パラメータの設定

ネットワーク環境によりライブ映像が正常に表示されない場合があります。異なるネットワーク環境では、伝送パラメータを調整することで問題を解決できます。

手順

- 「設定」→「→ Local」を選択します。
- 必要に応じて伝送パラメータを設定します。

プロトコル

TCP

TCPはストリーミングデータの完全な配信と優れた画質を保証しますが、リアルタ

イム伝送には影響が出ます。安定したネットワーク環境に適しています。

UDP

UDPは、高画質の滑らかさを求める不安定なネットワーク環境に適しています。

マルチキャスト

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



注記

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

HTTP

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

再生パフォーマンス

最短遅延

デバイスは、動画の滑らかさよりもリアルタイムの映像を優先します。

バランス型

デバイスはリアルタイム映像と滑らかさの双方を確保します。

滑らかさ優先

デバイスはリアルタイム性よりも動画の滑らかさを優先します。ネットワーク環境が悪い場合、滑らかさが有効であっても、デバイスは動画の滑らかさを保証できません。

カスタム

フレームレートを手動で設定できます。ネットワーク環境が悪い場合、フレームレートを下げてライブビューの滑らかさを確保できます。ただし、ルール情報が表示されない場合があります。

3. [OK]をクリックします。

3.3 スムーズストリーミングの設定

不安定なネットワーク環境による遅延やネットワーク輻輳に対処し、ウェブ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滑らかに保つ機能です。

開始前に

スムーズストリーミング機能を設定する前に、クライアントソフトウェアにデバイスを追

加し、クライアントソフトウェアでNPQプロトコルを選択してください。

機能を有効化する前に、ビットレートタイプが「定数」に、SVCが「OFF」に選択されていることを確認してください。設定を行うには、[Configuration] → [→] → [Video/Audio] → [→] → [Video] に移動します。

手順

1. 設定ページに移動: 設定 → ネットワーク → 詳細設定 → スムースストリーミング。
2. 「Smooth Streamingを有効にする」にチェックを入れます。
3. スムース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値は、ビデオページで設定した値を超ません。Smooth Streaming機能を有効化する前に、設定 → Video/Audio → Video に移動し、の前に解像度と最大ビットレートを設定してください。このモードでは、フレームレートは自動的に最大値に調整されます。

解像度優先

解像度はビデオページで設定した値のまま維持され、ビットレートが自動的に調整されます。設定画面 → ビデオ/オーディオ → ビデオ に移動し、スムーズストリーミング機能を有効化する前に最大ビットレートを設定してください。このモードでは、フレームレートが自動的に最大値に調整されます。

エラー補正

解像度とビットレートはビデオページで設定した値のまま維持されます。このモードは、伝送中のデータエラーを補正し画質を確保するために使用されます。エラー補正率は0～100の範囲で設定可能です。

比率が0の場合、データ再送信によりエラーが修正されます。比率が0より大きい場合、ストリームに追加された冗長データと再送信によりエラーデータが修正されます。値が高いほど冗長データが増加し、より多くのデータエラーが修正されます。必要な帯域幅も大きくなります。比率が100の場合、冗長データは元のデータと同量となり、帯域幅は2倍必要となります。



エラー訂正モードでは、帯域幅が十分であることを必ず確認してください。

4. 設定を保存します。

第4章 映像と音声

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

4.1 ビデオ設定

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

設定ページへの移動: 設定 → ビデオ/オーディオ → ビデオ。

4.1.1 ストリームタイプ

デバイスが複数のストリームをサポートしている場合、各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

このストリームは、デバイスがサポートする最高のストリーム性能を表します。通常、デバイスが実現可能な最高の解像度とフレームレートを提供します。ただし、高解像度と高フレームレートは、通常、より大きなストレージ容量と、伝送におけるより高い帯域幅要件を意味します。

サブストリーム

このストリームは比較的低解像度のオプションを提供し、帯域幅とストレージ容量の消費を抑えます。

その他のストリーム

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

カスタム動画の設定

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はプレビュー可能ですが、録画や再生はできません。

手順

注記

- この機能は特定のカメラモデルでのみサポートされています。
 - デバイスの復元後（デフォルト設定への復元ではない）、カスタム動画ストリームの数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。
-

- ストリームを追加するには、[+] をクリックします。
 - 必要に応じてストリーム名を変更します。
-

注記

ストリーム名には、32文字以内の英数字（&、<、>、'、"を除く）を使用できます。

- 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、動画エンコード）をカスタマイズします。
- 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。
- オプション：カスタムストリームが不要な場合は、[x]をクリックして削除します。
- 「保存」をクリックします。

4.1.2 ビデオタイプ

ストリームに含まれるべきコンテンツ（動画と音声）を選択します。

ビデオ

ストリームには動画コンテンツのみが含まれます。

動画と音声

複合ストリームには動画コンテンツと音声コンテンツが含まれます。

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てください。解像度が高いほど、より多くの帯域幅とストレージが必要となります。

4.1.4 ビットレートタイプと最大ビットレート

固定ビットレート

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

可変ビットレート

設定された最大ビットレート内で、デバイスが自動的にビットレートを調整します。圧縮速度は定ビットレート方式より遅くなりますが、複雑なシーンの画質を保証します。

4.1.5 映像品質

ビットレートタイプが可変に設定されている場合、動画品質は設定可能です。実際のニ

ズに応じて動画品質を選択してください。高い動画品質にはより高い帯域幅が必要となる点に注意してください。

4.1.6 フレームレート

フレームレートは動画ストリームの更新頻度を表し、フレーム毎秒 (fps) で測定されます。

動画ストリーム内に動きがある場合、フレームレートが高いほど画質が維持される利点があります。ただし、フレームレートが高いほど、より多くの帯域幅とより大きなストレージ容量が必要となります。

4.1.7 動画エンコーディング

これは、デバイスがビデオエンコーディングに採用する圧縮規格を表します。

注

利用可能な圧縮規格はデバイスモデルによって異なります。

H.264

H.264 (MPEG-4 Part 10、Advanced Video Coding) は、圧縮規格です。画質を損なうことなく、MJPEGやMPEG-4 Part 2よりも圧縮率を高め、動画ファイルのサイズを縮小します。

H.264+

H.264+はH.264を基盤とした改良型圧縮符号化技術です。H.264+を有効にすると、最大平均ビットレートからHDD消費量を推定できます。H.264と比較し、H.264+はほとんどのシーンで同等の最大ビットレートを維持しながら、ストレージ容量を最大50%削減します。H.264+を有効にした場合、最大平均ビットレートは設定可能です。デフォルトでは推奨最大平均ビットレートが設定されます。映像品質が不十分な場合は、このパラメータを高い値に調整できます。最大平均ビットレートは最大ビットレートを超えてはいけません。

注記

H.264+が有効な場合、ビデオ品質、フレーム間隔、プロファイル、およびSVCは設定できません。

H.265

H.265 (高効率ビデオコーディング (HEVC) およびMPEG-H Part 2としても知られる) は、圧縮規格です。H.264と比較して、同じ解像度、フレームレート、画質でより優れたビデ

オ圧縮を提供します。

H.265+

H.265+はH.265を基盤とした改良型圧縮符号化技術です。H.265+を有効化すると、最大平均ビットレートに基づくHDD消費量の推定が可能になります。H.265と比較し、H.265+はほとんどのシーンにおいて最大ビットレートを同等としながらストレージ容量を最大50%削減します。

H.265+を有効にした場合、**最大平均ビットレート**は設定可能です。デフォルトでは推奨最大平均ビットレートが設定されます。の映像品質が不十分な場合、このパラメータを高い値に調整できます。最大平均ビットレートは最大ビットレートを超えてはいけません。

注記

H.265+を有効にした場合、**動画品質**、**Iフレーム間隔**、**プロファイル**、**SVC**は設定不可となります。

Iフレーム間隔

Iフレーム間隔は、2つのIフレーム間のフレーム数を定義します。

H.264およびH.265において、Iフレーム（イントラフレーム）は他の画像を参照せずに独立してデコード可能な自己完結型フレームです。Iフレームは他のフレームよりも多くのビットを消費します。したがって、Iフレームが多い（つまりIフレーム間隔が小さい）動画は、より安定した信頼性の高いデータビットを生成しますが、より多くのストレージ容量を必要とします。

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動画圧縮規格のAnnex G拡張機能の名称である。

SVC標準化の目的は、高品質な動画ビットストリームをエンコード可能とすることです。このビットストリームには、サブセットビットストリームが1つ以上含まれており、それ自体が既存のH.264またはH.265設計と同等の複雑度と再構築品質で、かつサブセットビットストリームと同量のデータでデコード可能です。サブセットビットストリームは、より大きなビットストリームからパケットを削除することで生成されます。

SVCは旧式ハードウェアへの前方互換性を実現する：低解像度サブセットのみをデコード可能な基本ハードウェアでも同一ビットストリームを利用可能であり、一方、より高度なハードウェアでは高品質ビデオストリームのデコードが可能となる。

MPEG4

MPEG4（MPEG-4 Part 2）は、Moving Picture Experts Group（MPEG）によって開発されたビ

デオ圧縮フォーマットです。

MJPEG

Motion JPEG（M-JPEGまたはMJPEG）は、イントラフレーム符号化技術を用いた動画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

この機能は、同じビットレートでは、プロファイルが複雑であるほど、画質は高くなり、ネットワーク帯域幅の要件も高くなることを意味します。

4.1.8 スムージング

ストリームの滑らかさを指します。スムージングの値が高いほど、ストリームの流動性は向上しますが、映像品質は満足のいくものではなくなる可能性があります。スムージングの値が低いほど、ストリームの品質は高くなりますが、流動性に欠けるように見える場合があります。

4.2 ROI

ROI（関心領域）エンコーディングは、動画圧縮において関心領域と背景情報を区別するのに役立ちます。この技術は、関心領域により多くのエンコーディングリソースを割り当てる、関心領域の品質を向上させます。一方、背景情報にはあまり重点が置かれません。

4.2.1 ROIの設定

ROI（関心領域）エンコーディングは、関心領域により多くのエンコーディングリソースを割り当てることで、ROIの品質を向上させます。一方、背景情報への注力は低くなります。

開始前に

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

手順

1. [設定] → [→] → [ビデオ/オーディオ] → [→] → [ROI] に移動します。

2. [有効化] にチェックを入れます。

3. ストリームタイプを選択します。

4. 固定領域で領域番号を選択し、ROI領域を描画します。

1) 描画をクリックします。

2) ビュー画面上でマウスをクリック&ドラッグし、固定領域を描画します。

3) 描画停止をクリックします。



調整が必要な固定領域を選択し、マウスをドラッグして位置を調整します。

5. 領域名とROIレベルを入力します。

6. 「保存」をクリックします。



ROIレベルが高いほど、検出領域の画像が鮮明になります。

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

4.3 ストリームへの情報表示

オブジェクト（人、車両など）の情報がビデオストリームにマークされます。接続された末端デバイスまたはクライアントソフトウェアで、ライン越え、侵入などのイベントを検出するルールを設定できます。

手順

1. 設定ページへ移動: 設定 → 映像/音声 → ストリーム上での情報表示。
2. 「デュアルVCAを有効にする」にチェックを入れます。
3. [保存]をクリックします。

4.4 オーディオ設定

オーディオエンコーディングや環境ノイズフィルタリングなどのオーディオパラメータを設定する機能です。

オーディオ設定ページに移動: 設定 → ビデオ/オーディオ → オーディオ。

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ディング圧縮を選択します。

4.4.2 オーディオ入力



- 必要に応じてオーディオ入力デバイスを接続してください。

- オーディオ入力の表示は、デバイスモデルによって異なります。

ライン入力	MP3、シンセサイザー、アクティブピックアップなど、高出力のオーディオ入力デバイスに接続する場合は、オーディオ入力を LineIn に設定してください。
マイク入力	オーディオ入力をマイク入力に設定するのは、マイクやパッシブピックアップなど、低出力のオーディオ入力デバイスに接続する場合です。

4.4.3 オーディオ出力



オーディオ出力デバイスを必要に応じて接続してください。

これはデバイスのオーディオ出力のスイッチです。必要に応じて出力音量を調整できます。無効にすると、デバイスのオーディオは一切出力されません。オーディオ出力の表示は、デバイスの モードによって異なります。

4.4.4 環境ノイズフィルター

OFFまたはONに設定します。機能を有効にすると、周囲の雑音をある程度除去できます。

4.5 双方向音声

監視画面上で監視センターと対象者間の双方向音声機能を実現するために使用されます。

開始前に

- 本機に接続された音声入力デバイス（ピックアップまたはマイク）と音声出力デバイス（スピーカー）が正常に動作していることを確認してください。デバイスの接続については、音声入力・出力デバイスの仕様を参照してください。
- 本装置に内蔵マイクとスピーカーがある場合、双方向音声機能を直接有効にできます。

手順

1. 「ライブビュー」をクリックします。
2. ツールバーの「」をクリックし、カメラの双方向オーディオ機能を有効にします。
3. 「」をクリックし、「」を選択、スライダーを動かして音量を調整します。
4. 「」をクリックし、双方向オーディオ機能を無効にします。

4.6 表示設定

画像機能を調整するためのパラメータ設定を提供します。

設定 → 画像 → 表示設定 に移動します。

デフォルトをクリックすると設定が復元されます。

4.6.1 シーンモード

様々な設置環境向けに事前定義された画像パラメータセットが複数用意されています。実際の設置環境に応じてシーンを選択すると、表示設定を迅速に行えます。

画像調整

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

露出設定

露出は、アイリス、シャッター、感度の組み合わせによって制御されます。露出パラメータを設定することで、画像効果を調整できます。

手動モードでは、露光時間、ゲイン、スローシャッターを設定する必要があります。

フォーカス

フォーカスモードと最短撮影距離を調整するオプションが用意されています。

フォーカスモード

オート

シーンの変化に応じて自動的に焦点が合います。自動モードで焦点が合わない場合は、画像内の光源を減らし、点滅する光を避けてください。

半自動

PTZ操作とレンズズーム後、一度だけフォーカスを調整します。画像が鮮明な場合、シーンが変化してもフォーカスは変更されません。

手動

ライブビュー画面で手動で焦点を調整できます。

最小焦点距離

被写体とレンズの距離が最小焦点距離より短い場合、レンズはフォーカスしません。

デイ/ナイト切替

デイ/ナイト切替機能は、デイモードではカラー画像、ナイトモードでは白黒画像を提供します。切替モードは設定可能です。

昼

画像は常にカラーで表示されます。

ナイト

画像は常に白黒です。

自動

カメラは照明に応じて昼モードと夜モードを自動的に切り替えます。

スケジュール切り替え

開始時間と終了時間を設定し、デイモードの継続時間を定義します。

アラーム入力によるトリガー

トリガーモードは昼間と夜間の2種類が利用可能です。例えばトリガーモードが夜間の場合、デバイスが警報入力信号を受信すると画像が白黒に切り替わります。

注記

デイ/ナイト切替機能は機種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] から選択できます。

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が720×1280に回転します。

この機能を有効にすると、垂直方向のモニタリングの有効範囲が変化する場合があります。

レンズ歪み補正

電動レンズを搭載したデバイスでは、画像にある程度の歪みが生じる場合があります。この機能を有効にすると、歪みを補正します。

注

- この機能は電動レンズ搭載の特定のデバイスでのみサポートされています。
- この機能を有効にすると、画像の端部が失われます。

BLC

強い逆光下にある被写体に焦点を合わせると、被写体が暗すぎてはっきり見えなくなる場合があります。BLC（バックライト補正）は、被写体側の光量を補正し、被写体を鮮明に映し出します。BLCモードをカスタムに設定すると、ライブビュー画像上にBLC領域として赤い四角形を描画できます。

WDR

WDR（ワイドダイナミックレンジ）機能は、強い明暗差のある環境でもカメラが鮮明な画像を提供することを支援します。

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

注意

WDRを有効にした場合、他の機能の一部がサポートされないことがあります。詳細は実際のインターフェースを参照してください。

HLC

画像の明るい領域が露出オーバーで暗い領域が露出不足の場合、HLC（ハイライト圧縮）機能を有効にすることで明るい領域を弱め、暗い領域を明るくし、全体の明るさのバランスを実現します。

ホワイトバランス

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

DNR

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

ノーマル

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

エキスパート

空間ノイズリダクションと時間ノイズリダクションの両方のDNRレベルを設定し、ノイズ低減度合いを制御します。レベルが高いほど、より強力な低減効果が得られます。

デフォグ

環境が霧で覆われ画像が霞んでいる場合にデフォグ機能を有効化できます。微細なディテールを強調し、画像をより鮮明に表示します。

EIS

ジッター補正技術を用いて動画画像の安定性を向上させます。

ミラー

ライブビュー画像が実際のシーンと逆になっている場合、この機能により画像を正常に表示できます。

必要に応じてミラーモードを選択してください。



この機能を有効にすると、ビデオ録画が一時的に中断されます。

4.6.2 画像パラメータ切替

デバイスは設定された時間間隔で画像パラメータを自動的に切り替えます。

画像パラメータ切り替え設定ページに移動: 設定 → 画像 → 画像パラメータ切り替え、必要に応じてパラメータを設定してください。

設定切替

特定の時間間隔で画像パラメータをシーンに自動切替

手順

- 「有効にする」をチェックします。
 - 対応する時間帯とシーンを選択し設定します。
-



シーン設定については、シーンモードを参照してください。

- 「保存」をクリックします。

4.6.3 ビデオ規格

ビデオ規格とは、ビデオカードまたはビデオ表示装置が定義する表示可能な色数と解像度を指します。最も一般的なビデオ規格はNTSCとPALです。NTSCでは毎秒30フレームが伝送され、各フレームは525本の走査線で構成されます。PALでは毎秒25フレームが送信されま

す。各フレームは625本の走査線で構成されています。お住まいの地域のビデオシステムに合わせてビデオ信号規格を選択してください。

4.6.4 ローカルビデオ出力

本装置に BNC、CVBS、HDMI、SDI などのビデオ出力インターフェースが装備されている場合、モニター画面に接続することでライブ映像を直接プレビューできます。
出力モードを ON/OFF で選択して出力を制御します。

4.7 OSD

OSD（オンスクリーンディスプレイ）情報は、デバイス名、日時、フォント、ビデオストリーム上に表示されるテキストオーバーレイなどをカスタマイズできます。

OSD 設定ページに移動: 設定 → 画像 → OSD 設定。対応するパラメータを設定し、[保存] をクリックして有効にします。

文字セット

表示情報の文字セットを選択します。画面に韓国語を表示する必要がある場合、では 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、曜日、およびそれらの表示形式を設定します。

テキストオーバーレイ

画像上にカスタム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、位置合わせなどの OSD パラメータを設定します。

4.8 プライバシーマスクの設定

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

手順

1. プライバシーマスク設定ページへ移動: 設定 → 画像 → プライバシーマスク。
2. 「プライバシーマスクを有効にする」にチェックを入れます。
3. 「領域を描画」をクリック。ライブビュー上でマウスをドラッグし、閉じた領域を描画します。

領域の角をドラッグ 領域のサイズを調整します。
グ

領域をドラッグ 領域の位置を調整します。

「すべてクリア」 設定した領域をすべてクリアします。
をクリック

4. 「描画を終了」をクリックします。
5. 「保存」をクリックします。



最大4つの領域の設定が可能です。

4.9 オーバーレイ画像

ライブビューにカスタマイズした画像をオーバーレイ表示します。

開始前に

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

手順

1. 画像オーバーレイ設定ページに移動: 設定 → 画像 → 画像オーバーレイ。
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。
アップロード成功後、ライブビューに赤い四角で囲まれた画像が表示されます。
3. 「画像オーバーレイを有効にする」にチェックを入れます。
4. 画像をドラッグして位置を調整します。
5. 「保存」をクリックします。

4.10 ターゲットクロップの設定

画像のトリミングが可能で、対象領域の画像のみを送信・保存することで、伝送帯域幅とストレージを節約できます。

手順

1. 設定 → 動画/音声 → ターゲットクロッピングに移動します。
2. [ターゲットクロッピングを有効にする]にチェックを入れ、[ストリームタイプ]で [サードストリーム]を設定します。

注記

ターゲットクロッピングを有効にした後、サードストリームの解像度は設定できません。

3. クロッピング解像度を選択します。
ライブビューに赤い枠が表示されます。
 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

- ターゲットクロッピングに対応しているのは特定のモデルのみであり、機能はカメラモデルによって異なります。
 - ターゲットクロッピングを有効にした後、一部の機能が無効になる場合があります。
-

第5章 動画録画と静止画撮影

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

5.1 ストレージ設定

このパートでは、いくつかの一般的な保存パスの設定について紹介します。

5.1.1 新規または暗号化されていないメモリカードの設定

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てください。詳細なインストール手順については、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. [設定] → [→] → [ストレージ] → [→] → [ストレージ管理] → [→] → [HDD管理] に移動します。
2. メモリカードを選択します。

注記

アンロックボタンが表示された場合は、まずメモリーカードのロックを解除する必要があります。詳細は「メモリーカードのステータス確認」を参照してください。

3. 「フォーマット」をクリックしてメモリカードを初期化します。
メモリカードのステータスが「初期化されていません」から「正常」に変わると、メモリカードが使用可能になります。
4. オプション: メモリカードを暗号化します。
 - 1) 「暗号化フォーマット」をクリックします。
 - 2) 暗号化パスワードを設定します。
 - 3) [OK]をクリックします。

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

注意

暗号化パスワードは適切に保管してください。パスワードを忘れた場合、復元できません。

5. オプション: メモリカードのクォータを設定します。必要に応じて、異なるコンテンツを保存するための割合を入力してください。
6. 「保存」をクリックします。

メモリカードの状態を検出

本デバイスはHikvisionメモリーカードのステータスを検出します。メモリーカードに異常が検出された場合、通知を受け取ります。

開始前に

設定ページは、Hikvisionメモリーカードがデバイスに挿入されている場合にのみ表示されます。

手順

1. 設定 → ストレージ → ストレージ管理 → メモリカード検出 に移動します。
2. [ステータス検出]をクリックし、メモリカードの残存寿命と健全性ステータスを確認します。

残存寿命

メモリカードの残存寿命をパーセンテージで表示します。メモリカードの寿命は、容量やビットレートなどの要因によって影響を受ける場合があります。残存寿命が十分でない場合は、メモリカードを交換する必要があります。

健全性状態

メモリカードの状態を表示します。状態は「良好」「不良」「破損」の3種類です。設定済みの「武装スケジュール」および「運動方法」において、健康状態が「良好」以外の場合、通知が送信されます。

注意

健康状態が「良好」でない場合は、メモリカードの交換をお勧めします。

3. R/Wロックをクリックし、メモリカードの読み書き権限を設定します。

1. ロックを追加し、ロックスイッチをONに設定します。
2. パスワードを入力します。
3. 「保存」をクリック

ロック解除

- ロックしたデバイスでメモリカードを使用すると、自動的にロックが解除されるため、ユーザー側で解除操作を行う必要はありません。
- ロックされたメモリカードを別のデバイスで使用する場合、HDD管理に移動してメモリカードを手動でロック解除できます。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. ロック解除ロックスイッチをOFFに設定してください。
 2. パスワード設定でパスワードを入力してください。

3. 保存をクリックしてください。



注記

- **R/Wロック**を設定できるのは管理者ユーザーのみです。
- メモリカードはロック解除時にのみ読み書きが可能です。
- メモリカードにロックを追加したデバイスを工場出荷時設定に復元した場合、**HDD管理**画面でメモリカードのロックを解除できます。

4. 警戒スケジュールと連動方法の設定を行います。詳細は「警戒スケジュールと連動方法の設定」を参照してください。

5. 「保存」をクリックします。

5.1.2 FTPの設定

イベントまたは定時スナップショットタスクでキャプチャされた画像を保存するために、FTPサーバーを設定できます。

開始前に

まずFTPサーバーのアドレスを取得してください。

手順

1. [設定] → [→] → [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とSFTPが選択可能です。ファイルアップロードはSFTPプロトコルで暗号化されます。

サーバーアドレスとポート

FTPサーバーのアドレスと対応するポート。

ユーザー名とパスワード

FTPユーザーは画像アップロード権限を持つ必要があります。

FTPサーバーが匿名ユーザーによる画像アップロードをサポートしている場合、「匿名」にチェックを入れると、アップロード時にデバイス情報を非表示にできます。

ディレクトリ構造

FTPサーバー上のスナップショット保存パス。

画像保存間隔

画像管理を効率化するため、保存間隔を1日から30日の間で設定できます。同一間隔で撮影された画像は、期間の開始日と終了日をフォルダ名として1つのフォルダに保存されます。

画像名

撮影画像の命名規則を設定します。ドロップダウンリストで「デフォルト」を選択すると、既定の規則（例: 10.11.37.189_01_20150917094425492_FACE_DETECTION.jpg）が適用されます。または、デフォルト命名規則にカスタム接頭辞を追加してカスタマイズできます。

3. 「画像をアップロード」にチェックを入れ、スナップショットをFTPサーバーにアップロードできるようにします。
 4. 「自動ネットワーク補充を有効にする」にチェックを入れます。
-



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を有効にする」は、同時に有効にする必要があります。

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

5.1.3 NASの設定

記録ファイルやキャプチャ画像などを保存するネットワークディスクとしてネットワークサーバーを利用します。

開始前に

ネットワークドライブのIPアドレスを事前に取得してください。

手順

1. NAS設定ページに移動: **構成** → **ストレージ** → **ストレージ管理** → **Net HDD**.
2. **HDD番号**をクリック。ディスクのサーバーアドレスとファイルパスを入力。

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。

マウントタイプ

オペレーティングシステムに応じてファイルシステムプロトコルを選択してください。

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

3. **【テスト】**をクリックし、ネットワークディスクが利用可能か確認します。
4. 「保存」をクリックします。

5.1.4 eMMC保護

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



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

設定を行うには、[Configuration] → [→] → [System] → [→] → [Maintenance] → [→] → [System Service] に移動してください。

eMMC (Embedded Multimedia Cardの略称) は、組み込み型の不揮発性メモリシステムです。デバイスの撮影画像や動画を保存できます。

デバイスはeMMCの健全性状態を監視し、状態が不良の場合にeMMCを無効化します。これにより、劣化したeMMCの使用によるデバイス起動失敗を防止します。

5.1.5 クラウドストレージの設定

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

手順



注意

クラウドストレージが有効な場合、画像は優先的にクラウドストレージサーバーに保存されます。

1. [設定] → [→] → [Storage] → [→] → [Storage Management] → [→] → [Cloud Storage] に移動します。
2. 「クラウドストレージを有効にする」にチェックを入れます。
3. 基本パラメータを設定します。

プロトコルバージョン クラウドストレージサーバーのプロトコルバージョン。

ポート

サーバーIP クラウドストレージサーバーのIPアドレス。IPv4アドレスをサポートします。

サーバーポート クラウドストレージサーバーのポート。デフォルトポートは6001であり、編集は推奨されません。

ユーザー名とパス クラウドストレージサーバーのユーザー名とパスワード。

ワード

画像ストレージプールID クラウドストレージサーバー内の画像ストレージリージョンのIDです。ストレージプールIDとストレージリージョンIDが一致していることを確認してください。

4. [テスト]をクリックして設定をテストします。
5. [保存]をクリックします。

5.2 ビデオ録画

このセクションでは、手動録画・スケジュール録画の操作、録画ファイルの再生およびダウンロードについて説明します。

5.2.1 自動録画

この機能は、設定された時間帯に自動的にビデオを録画します。

開始前に

連続記録を除く各記録タイプのイベント設定で「トリガー記録」を選択してください。詳細は「イベントとアラーム」を参照してください。

手順

1. 設定 → → → ストレージ → → → スケジュール設定 → → → レコードスケジュールに移動します。
2. 「有効化」にチェックを入れます。
3. レコードタイプを選択します。

注記

記録タイプは機種によって異なります。

連続

スケジュールに従い動画を連続記録します。

モーション検知

動体検知が有効で、連動方式として録画トリガーが選択されている場合、物体の動きが記録されます。

アラーム

外部警報入力デバイスからの警報信号を受信後、動画を録画します。

モーション | アラーム

外部アラーム入力デバイスからモーションが検出された場合、またはアラーム信号を受信した場合に映像が記録されます。

モーション&アラーム

外部アラーム入力デバイスからモーションが検出され、かつアラーム信号を受信した場合にのみ録画されます。

イベント

設定されたイベントが検出された際に動画を記録します。

- 選択した録画タイプにスケジュールを設定します。設定操作については「**警戒スケジュール設定**」を参照してください。
- 詳細設定**をクリックして詳細設定を行います。

上書き

ストレージ容量が満杯になった際に録画データを上書きするには「**上書きを有効にする**」を選択します。無効の場合、カメラは新規録画を行えません。

事前録画

スケジュールされた時刻より前に録画する期間を設定します。

後録り

スケジュールされた時刻後に録画を停止する設定時間。

ストリームタイプ

録画するストリームの種類を選択します。



ビットレートが高いストリームタイプを選択した場合、プリレコードおよびポストレコードの実際の時間は設定値より短くなる可能性があります。

録画の有効期限

有効期限を超過した録画データは削除されます。有効期限は設定可能です。削除された録画データは復元できませんのでご注意ください。

- [保存]をクリックします。

5.2.2 手動録画

手順

- [設定] → [→] → [ローカル] に移動します。
- 録画ファイルの保存先と保存パスを設定します。
- 「保存」をクリックします。
- 「」をクリックして記録を開始します。「」をクリックして記録を停止します。

5.2.3 ライトストレージの設定

ライトストレージを有効にすると、監視対象エリアに動きがない場合、動画ストリームのフレームレートとビットレートを低下させ、メモリカードの保存時間を延長できます。

手順

1. 設定 → ストレージ → ストレージ管理 → Lite ストレージ に移動します。
2. 「有効化」にチェックを入れ、レベルを設定します。レベルが高いほど、フレームレートとビットレートは大きくなり、推奨保存時間は短くなります。
3. 保存時間を設定します。デバイスはメモリカードの空き容量とレベルに基づき、ビットレートを自動計算し推奨保存時間を提示します。デバイスの推奨時間での設定をお勧めします。

注記

- ライトストレージを有効にすると、フォーマットされていないメモリーカードは自動的にフォーマットされます。
 - メモリカードの表示空き容量は、デフォルトで「ストレージ内の記録割合」 → 「ストレージ管理」 → 「クオータ」に基づいて割り当てられます。必要に応じて調整できます。
 - 本機能は特定の機種のみ対応しています。
-

5.2.4 動画の再生とダウンロード

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

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。
一致した動画ファイルがタイムバー上に表示されます。
3. 「▶」をクリックして動画ファイルを再生します。
 - 「▶」をクリックして動画ファイルをクリップします。
 - 「▶」をクリックすると動画ファイルを全画面で再生します。ESCキーを押すと全画面表示を終了します。

注記

設定 → Local に移動し、クリップ保存先をクリックして切り取った動画ファイルの保存パスを変更します。

4. 再生画面で「↓」をクリックするとファイルをダウンロードできます。
 - 1) 検索条件を設定し、[検索]をクリックします。

- 2) 動画ファイルを選択し、「ダウンロード」をクリックします。
-



注記

設定 → **Local** に移動し、「ダウンロードしたファイルを保存する場所」をクリックして、ダウンロードした動画ファイルの保存パスを変更します。

5.3 キャプチャ設定

本デバイスは手動または自動で画像をキャプチャし、設定された保存パスに保存できます。スナップショットの閲覧とダウンロードが可能です。

5.3.1 自動キャプチャ

設定された時間間隔で自動的に画像をキャプチャします。

開始前に

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

手順

1. 設定 → ストレージ → スケジュール設定 → キャプチャ → キャプチャパラメータに移動します。
2. キャプチャタイプを設定します。

タイミング

設定された時間間隔で画像をキャプチャします。

イベントトリガー

イベント発生時に画像をキャプチャします。

3. フォーマット、解像度、画質、間隔、撮影枚数を設定します。
4. スケジュール時間の設定については「アーミングスケジュールの設定」を参照してください。
5. [保存]をクリックします。

5.3.2 手動でのキャプチャ

手順

1. 「設定」→「→ ローカル」に移動します。
2. スナップショット用の画像形式と保存先を設定します。

JPEG

この形式の画像サイズは比較的小さく、ネットワーク伝送に適しています。

BMP

画質を保ちつつ圧縮されます。

3. 「保存」をクリックします。
4. ライブビューまたは再生ウィンドウ付近の「」をクリックし、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

デバイスがスリープ状態の場合、設定された時間間隔で起動し、画像をキャプチャしてアップロードします。

手順

1. [設定] → [→] → [システム] → [→] → [システム設定] → [→] → [消費電力モード] の [スリープスケジュール] で、時間スケジュールをクリックし、スリープキャプチャ間隔を設定します。
2. 設定 → イベント → 基本イベント → タイミングウェイクを選択します。
3. [有効化] にチェックを入れます。
4. キャプチャタイプを選択します。
5. 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起動し、画像をキャプチャしてアップロードします。

5.3.4 写真の閲覧とダウンロード

ローカルストレージまたはネットワークストレージに保存された画像を、検索・閲覧・ダウンロードできます。

手順

1. 「写真」をクリックします。
2. 検索条件を設定し、「検索」をクリックします。
一致した画像がファイルリストに表示されます。
3. 画像を選択し、「ダウンロード」をクリックして保存します。

注記

設定 → Local に移動し、「再生時にスナップショットを保存」をクリックして画像の保存パスを変更します。

第6章 イベントとアラーム

本節ではイベントの設定について説明します。デバイスはトリガーされたアラームに対して特定の対応を行います。

6.1 基本イベント

6.1.1 動体検知の設定

検知領域内の移動物体を検知し、連動動作をトリガーするのに役立ちます。

手順

1. 設定 → イベント → 基本イベント → モーション検知 に移動します。
2. 「モーション検知を有効にする」にチェックを入れます。
3. オプション: 画像内の移動物体を緑色で表示するにはハイライトを選択。
 - 1) 「動体検出の動的解析を有効にする」にチェックを入れる。
 - 2) 設定 → Local に移動。
 - 3) ルールを有効に設定。
4. 設定モードを選択し、ルール領域とルールパラメータを設定します。
 - 通常モードの詳細については、「通常モード」を参照してください。
 - エキスパートモードの詳細については、「エキスパートモード」を参照してください。
5. 警戒スケジュールと連動方法を設定します。警戒スケジュール設定については「警戒スケジュールの設定」を参照してください。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、昼と夜で異なる動き検知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。

スケジュールされたイメージ設定

OFF

画像切り替えは無効です。

自動切り替え

システムが環境に応じて昼/夜モードを自動切替。昼間は カラー画像、夜間は白黒画像を表示。

スケジュール切替

システムはスケジュールに従って昼/夜モードを切り替えます。設定期間中は昼モードに、その他の期間中は夜モードに切り替わります。

感度

感度の値が高いほど、動き検出の感度が高くなります。スケジュール画像設定が有効な場合、昼と夜の感度を個別に設定できます。

3. エリアを選択し、「エリア描画」をクリックします。ライブ画像上でマウスをクリック&ドラッグし、マウスを離すと1つのエリア描画が完了します。



図6-1 ルール設定

描画を終了

1つの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領域を設定します。

通常モード

デバイスのデフォルトパラメータに基づいて、動き検知パラメータを設定できます。

手順

1. 設定で通常モードを選択します。
2. 通常モードの感度を設定します。感度の値が高いほど、動き検知の感度が高くなります。感度を0に設定すると、動き検知と動的分析は機能しません。
3. 「領域描画」をクリックします。ライブ映像上でマウスをクリック&ドラッグし、マウスを離して領域描画を終了します。

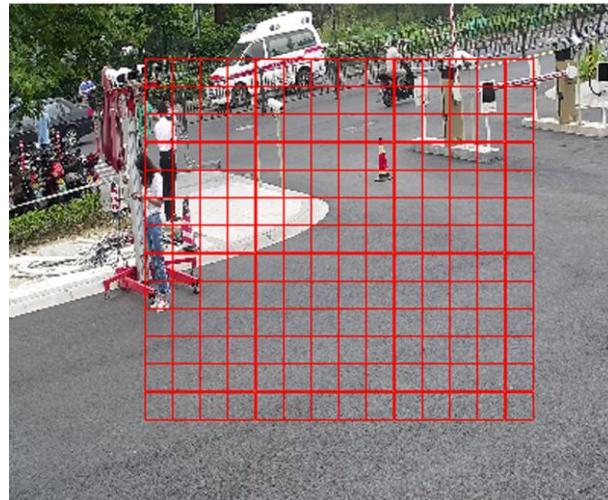


図6-2 ルール設定

描画を停止 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。

4. 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 映像改ざん警報の設定

設定されたエリアが覆われ、正常に監視できなくなったり場合、アラームがトリガーされ（）、デバイスは特定のアラーム対応アクションを実行します。

手順

1. 設定 → → イベント → → 基本イベント → → 映像改ざん へ移動。
2. 「有効」にチェックを入れる。
3. 感度を設定します。値が高いほど、エリア覆いを検出しやすくなります。
4. 「領域を描画」をクリックし、ライブビュー上でマウスをドラッグして領域を描画します。

描画終了 描画終了

すべてクリア 描画した領域をすべて削除します。

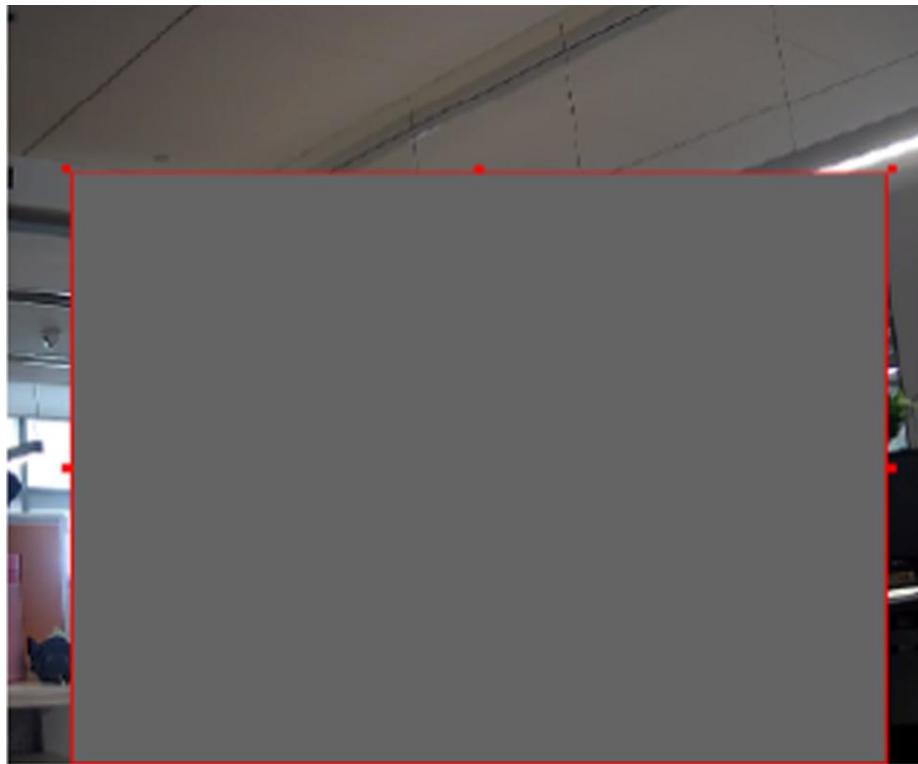


図6-3 ビデオ改ざん検知エリアの設定

5. スケジュール設定については「**警備スケジュール設定**」を参照してください。**運動方法**の設定については「**運動方法設定**」を参照してください。
6. 「**保存**」をクリックします。

6.1.3 PIR警報の設定

PIR（パッシブ赤外線）警報は、侵入者が検知器の視野内で移動した際に作動します。人間や犬、猫などの温血動物が発する熱エネルギーを検知できます。

手順



PIRアラームに対応しているのは特定のモデルのみです。

1. 設定 → 詳細設定 → 基本イベント → **PIR警報** に移動します。
2. 「**PIRアラームを有効にする**」にチェックを入れます。
3. スケジュール設定については「**警備スケジュール設定**」を参照してください。**運動方法**の設定については「**運動方法設定**」を参照してください。
4. 「**保存**」をクリックします。

6.1.4 例外アラームの設定

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

手順

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

HDD 満杯 HDDのストレージが満杯です。

HDD エラー HDDでエラーが発生しました。

ネットワーク切断 デバイスがオフラインです。

IP アドレスの競合 現在のデバイスのIPアドレスが、ネットワーク内の他のデバイスと同一です。

不正なログイン ユーザー名またはパスワードが正しくありません。

電圧が不安定です 電源電圧が変動しています。

3. 連動方法の設定については、連動方法設定を参照してください。

4. 「保存」をクリックしてください。

6.1.5 アラーム入力の設定

外部デバイスからのアラーム信号が、現在のデバイスの対応するアクションをトリガーします。

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てください。ケーブル接続についてはクイックスタートガイドを参照してください。

手順

1. 設定 → イベント → 基本イベント → アラーム入力 に移動します。
2. 「アラーム入力処理を有効にする」にチェックを入れる。
3. ドロップダウンリストから「警報入力NO.」と「警報タイプ」を選択します。「警報名」を編集します。
4. スケジュール設定については「武装スケジュール設定」を参照。連動方法設定については「連動方法設定」を参照。
5. 「コピー先...」をクリックし、設定を他の警報入力チャンネルにコピーします。
6. 「保存」をクリックします。

6.1.6 映像品質診断の設定

デバイスの映像品質が異常でアラーム連動が設定されている場合、アラームが自動的にトリガーされます。

手順

1. [設定] → [イベント] → [基本イベント] → [画質診断] に移動します。
2. 診断タイプを選択します。
3. 対応するパラメータを設定します。

アラーム検出間隔

例外を検出する時間間隔。

感度

値が高いほど例外が検出されやすくなりますが、誤検知の可能性も高くなります。

アラーム遅延時間

設定回数に達した時点でデバイスがアラームをアップロードします。

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. 警戒スケジュールを設定します。「警戒スケジュール設定」を参照してください。
6. 連動方法を設定します。「連動方法設定」を参照してください。
7. 「保存」をクリックします。

注記

本機能は特定モデルのみ対応しています。実際の表示はモデルによって異なります。

6.1.7 振動検知の設定

デバイスが振動しているかどうかを検出するために使用されます。この機能を有効にすると、デバイスはアラームを報告し、連動アクションをトリガーします。

手順

1. 設定 → イベント → 基本イベント → 振動検出 に移動します。
2. [有効化] にチェックを入れます。
3. スライダーをドラッグして検知感度を設定します。数値を入力して感度を設定することも可能です。
4. 作動スケジュールを設定します。「作動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。

注記

本機能は特定のモデルでのみサポートされています。実際の表示はモデルによって異なります。

6.2 スマートイベント

注

- 特定のデバイスモデルでは、VCAリソースページでスマートイベント機能を有効にする必要があります。これにより、機能設定ページが表示されます。
 - 機能はモデルによって異なります。
-

6.2.1 音声異常検知

音声異常検知機能は、音量の急激な増減など、シーン内の異常な音を検知し、特定のアクションを実行することができます。

手順

- 設定 → イベント → スマートイベント → 音声異常検出 に移動します。
- 1つまたは複数の音声異常検出タイプを選択します。

オーディオ喪失検出

オーディオトラックの急激な消失を検出します。

音量急増検出

音量の急激な増加を検出します。感度と音量閾値は設定可能です。

注記

- 感度が低いほど、検出をトリガーするにはより大きな変化が必要です。
 - 音量閾値は検出時の音量基準値を指します。環境の平均音量に設定することを推奨します。周囲の音量が大きいほど、この値は高く設定する必要があります。実際の環境に応じて調整してください。
-

音圧レベルの急激な低下検出

音量の急激な低下を検出します。感度は設定可能です。

- スケジュール設定については「警戒スケジュール設定」を参照してください。**連動方法**の設定については「連動方法設定」を参照してください。
- 「保存」をクリックします。

 **注記**

機能は機種によって異なります。

6.2.2 ピント外れ検出の設定

レンズの焦点外れによるぼやけた画像を検出できます。発生した場合、デバイスは連動動作を実行できます。

手順

1. 設定 → → イベント → → スマートイベント → → 焦点外れ検出 へ移動。
 2. [有効化] にチェックを入れます。
 3. 感度を設定します。値が高いほど、焦点外れ画像がアラームをトリガーしやすくなります。実際の環境に応じて値を調整できます。
 4. 連動方法の設定については、「連動方法設定」を参照してください。
 5. [保存]をクリックします。
-

 **注**

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

6.2.3 シーン変化検出

シーン変化検知機能は、シーンの変化を検知します。アラームが作動した際に特定のアクションを実行できます。

手順

1. 設定 → イベント → スマートイベント → シーン変化検出 に移動します。
 2. [有効化]をクリックします。
 3. 感度を設定します。値が高いほどシーン変化を検出しやすくなりますが、検出精度は低下します。
 4. スケジュール設定は「武装スケジュール設定」を参照。連動方法設定は「連動方法設定」を参照。
 5. 「保存」をクリックします。
-

 **注記**

機能は機種によって異なります。

6.2.4 顔検出の設定

検出領域内の顔を検出するのに役立ちます。顔が検出されると、デバイスは連動アクションをトリガーします。

手順

1. 設定 → → イベント → → スマートイベント → → 顔検出 に移動します。
2. 「顔検出を有効にする」にチェックを入れます。
3. オプション: ハイライト表示で画像内の顔を強調表示します。
 - 1) [顔検出の動的分析を有効にする]にチェックを入れます。
 - 2) 設定 → Local に移動し、ルールを有効に設定します。
4. 感度を設定します。感度が低いほど、顔のプロファイルや不明瞭な顔の検出が難しくなります。
5. 警戒スケジュールと連動方法を設定します。警戒スケジュール設定の詳細は「[警戒スケジュールの設定](#)」を参照してください。連動方法の詳細は「[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 映像喪失設定

この機能は、映像信号の損失をタイムリーに検出し、連動動作をトリガーすることができます。

手順

1. 設定 → イベント → 基本イベント → 映像喪失 に移動します。
2. 有効化をチェックします。
3. スケジュール設定については「[警備スケジュール設定](#)」を参照し、連動方法設定については「[連動方法設定](#)」を参照してください。
4. 「保存」をクリックします。

6.2.6 侵入検知の設定

これは、事前に定義された仮想領域への侵入および滞留を検知するために使用されます。検知された場合、デバイスは連動動作を実行できます。

手順

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

感度

感度は、許容対象の身体部位が事前定義領域に侵入する割合を表します。感度 = $100 - S1/ST \times 100$ 。S1は事前定義領域を横切る

対象身体部位、STは対象身体全体を指します。感度値が高いほど、警報が容易にトリガーされます。

閾値

閾値は、対象物が領域内に滞留する時間の閾値を表します。1つの対象物が滞留する時間が閾値を超えると、警報が作動します。閾値の値が大きいほど、警報作動までの時間は長くなります。

検出対象

人物と車両が選択可能です。検出対象が選択されていない場合、人物と車両を含む全ての検出対象が報告されます。

ターゲット有効性

有効性を高く設定すると、必要なターゲットの特徴がより明確である必要があり、警報の精度が向上します。特徴が不明瞭なターゲットは見落とされる可能性があります。



図6-4 ルール設定

- オプション：上記手順を繰り返すことで、複数エリアのパラメータを設定できます。
- 警戒スケジュール設定については「警戒スケジュール設定」を参照してください。連動方法設定については「連動方法設定」を参照してください。
- 「保存」をクリックします。

6.2.7 ライン越え検知の設定

あらかじめ設定された仮想ラインを横切る物体を検出するために使用されます。検出された場合、デバイスは連動動作を実行できます。

手順

- 設定 → イベント → スマートイベント → ライン横断検知に移動します。
- [有効化] にチェックを入れます。

3. ラインを1つ選択し、サイズフィルターを設定します。サイズフィルター設定については、「**サイズフィルターの設定**」を参照してください。
4. 「**描画領域**」をクリックすると、ライブ映像に矢印付きの線が表示されます。この線をライブ映像上の任意の位置までドラッグします。
5. ルールを設定します。

方向

対象物が線を横切る方向を表します。

A<=>B: 両方向から線を横切るオブジェクトを検知し、アラームが作動します。

A->B: 設定された線をA側からB側へ横切る物体のみを検出できます。

B->A: 設定されたラインをB側からA側へ横切る物体のみを検出できます。

感度

これは、許容対象物の身体部分が、あらかじめ定義されたラインを横切る割合を表します。感度 = $100 - S1/ST \times 100$ 。S1は、あらかじめ定義されたラインを横切る対象物の身体部分を表します。STは対象物の身体全体を表します。感度の値が高いほど、アラームがより簡単に作動します。

検出対象

人および車両が選択可能です。検出対象が選択されていない場合、人および車両を含む全ての検出対象が報告されます。

ターゲット有効性

有効性を高く設定すると、必要なターゲットの特徴がより明確である必要があり、警報の精度が向上します。特徴が不明瞭なターゲットは見落とされる可能性があります。

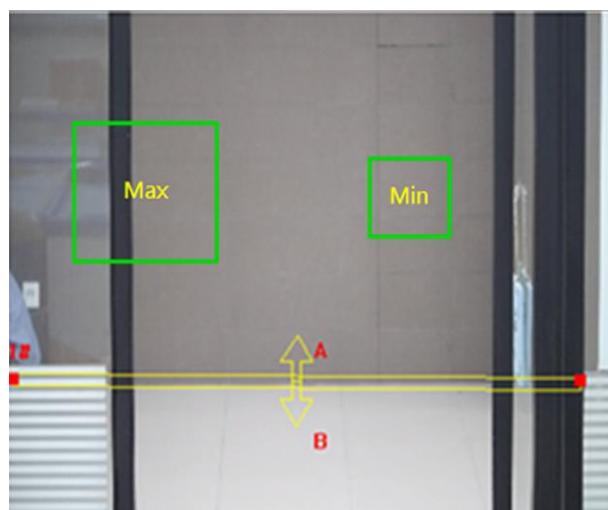


図6-5 ルール設定

6. オプション: 上記の手順を繰り返すことで、複数エリアのパラメータを設定できます。

7. 警戒スケジュール設定については「警戒スケジュール設定」を参照してください。連動方法設定については「連動方法設定」を参照してください。
8. 「保存」をクリックします。

6.2.8 区域進入検知の設定

外部から事前に定義された仮想領域に侵入する物体を検出するために使用されます。検出された場合、デバイスは連動動作を実行できます。

手順

1. 設定 → イベント → スマートイベント → 領域進入検知 に移動します。
2. [有効化] にチェックを入れます。
3. 1つの領域を選択します。領域設定については、[描画領域](#)を参照してください。
4. 検知対象、感度、対象の有効性を設定します。

感度

許容対象の身体部位が事前定義された領域を横切る割合を表します。感度 = $100 - S1/ST \times 100$ 。S1は事前定義領域を横切る対象身体部位、STは対象身体全体を表します。感度値が高いほど、アラームが容易に作動します。

検出対象

人および車両が選択可能です。検出対象が選択されていない場合、人および車両を含むすべての検出対象が報告されます。

ターゲット有効性

有効性を高く設定すると、必要な対象の特徴がより明確である必要があり、警報の精度が向上します。特徴が不明瞭な対象は見落とされる可能性があります。

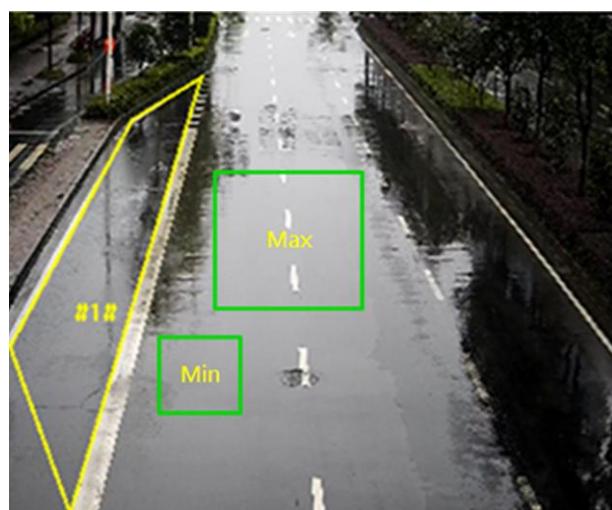


図6-6 ルール設定

5. オプション: 上記の手順を繰り返すことで、複数エリアのパラメータを設定できます。

6. 警戒スケジュール設定については「[警戒スケジュール設定](#)」を参照してください。連動方法設定については「[連動方法設定](#)」を参照してください。
7. 「保存」をクリックします。

6.2.9 領域退出検知の設定

これは、事前に定義された仮想領域から物体が退出することを検出するために使用されます。検出された場合、デバイスは連動動作を実行できます。

手順

1. 設定 → イベント → スマートイベント → 領域退出検出
2. 有効化をチェックします。
3. 1つの領域を選択します。検出領域の設定については、[描画領域](#)を参照してください。
4. 検出対象、感度、対象の有効性を設定します。

感度

許容対象の身体部位が事前定義領域を横切る割合を表します。
 感度 = $100 - S1/ST \times 100$ 。S1は事前定義領域を横切る対象身体部位、STは対象身体全体を表します。感度の値が高いほど、アラームが容易に作動します。

検出対象

人間と車両が選択可能です。検出対象が選択されていない場合、人間と車両を含むすべての検出対象が報告されます。

ターゲット有効性

有効性を高く設定すると、必要な対象の特徴がより明確である必要があり、警報の精度が向上します。特徴が不明瞭な対象は見落とされる可能性があります。

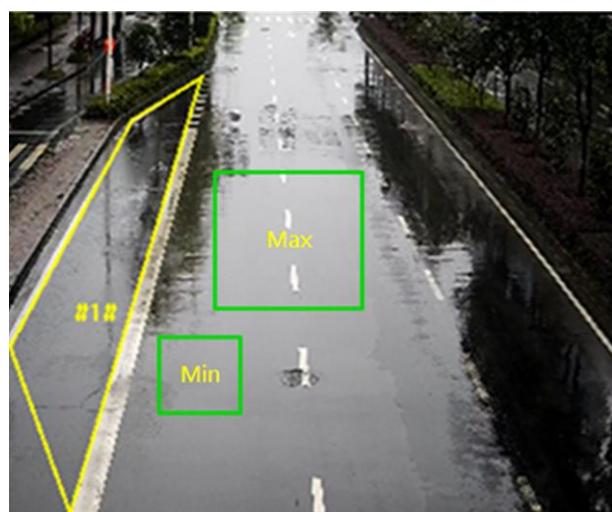


図6-7 ルール設定

5. オプション：上記手順を繰り返すことで複数エリアのパラメータを設定できます。

6. 警戒スケジュール設定については「警戒スケジュール設定」を参照してください。連動方法設定については「連動方法設定」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

これは、事前に定義された領域内に残された物体を検出するために使用されます。物体が領域内に残され、設定された時間経過後に連動方法がトリガーされます。

手順

1. 設定 → イベント → スマートイベント → 無人手荷物検知に移動します。
2. [有効化]にチェックを入れます。
3. 検出領域設定については「領域描画」を参照の上、領域を1つ選択します。
4. ルールを設定します。

感度

感度とは、許容対象物の身体部位が事前定義領域に侵入する割合(%)を指します。感度 = $100 - S1/ST \times 100$ 。S1は事前定義領域を横切る対象物身体部位、STは対象物身体全体を表します。感度値が高いほど、警報が容易に作動します。

閾値

対象物が領域内に残留する時間を示します。対象物が領域内に残留し、設定時間経過後に警報が作動します。

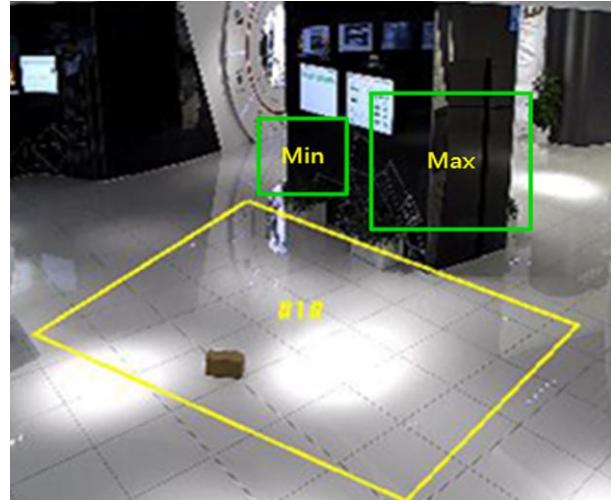


図6-8 ルール設定

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. 警戒スケジュール設定については「警戒スケジュール設定」を参照してください。連動方法設定については「連動方法設定」を参照してください。
7. [保存]をクリックします。

6.2.11 オブジェクト除去検知の設定

展示品など、事前に定義された検知領域からオブジェクトが除去されたかどうかを検知します。発生した場合、デバイスは連動動作を実行でき、スタッフは財産損失を軽減するための措置を講じることができます。

手順

1. 設定 → イベント → スマートイベント → オブジェクト除去検出 に移動します。
2. 「有効化」をチェックします。
3. 領域を選択します。領域設定については、[描画領域](#)を参照してください。
4. ルールを設定します。

感度

範囲 [1-100]。これは、許容対象物の身体部位が事前定義された領域から外れる割合（パーセント）を表します。

$$\text{感度} = 100 - S1/ST * 100$$

S1: 事前定義された領域から外れるターゲットの身体部分。

ST: ターゲットの身体全体。

例: 値を60に設定した場合、ターゲットの身体部分の40%が領域外に出た場合にのみ、対象が除去された物体としてカウントされます。

閾値

範囲 [5-100秒]。領域から除去されたオブジェクトの時間閾値。値を10に設定した場合、オブジェクトが領域から消えて10秒後にアラームが作動する。

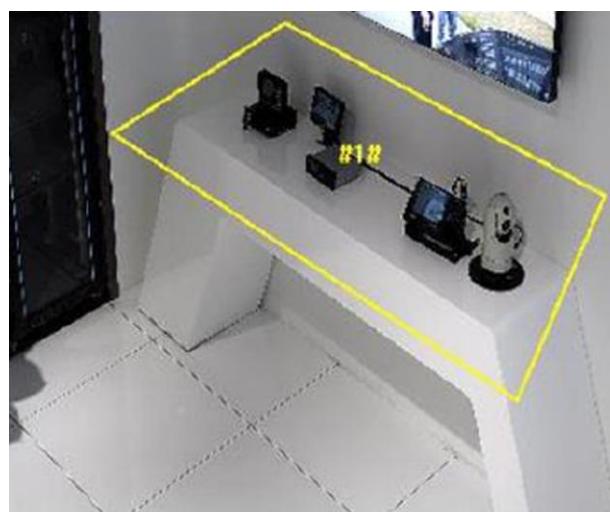


図6-9 ルール設定

5. オプション: 上記の手順を繰り返して、さらに領域を設定します。
6. 警戒スケジュール設定については「[警戒スケジュール設定](#)」を参照。連動方法設定については「[連動方法設定](#)」を参照。
7. 「保存」をクリックします。



注

本機能は特定モデルでのみ対応しています。実際の表示はモデルによって異なります。

6.2.12 エリア描画

このセクションでは領域の設定について説明します。

手順

1. 「描画領域」をクリックします。
 2. ライブビュー上で検出領域の境界線を描画し、右クリックで描画を終了します。
 3. 「保存」をクリックします。
-



注記

「すべてクリア」をクリックすると、事前に定義された領域をすべて消去します。

6.2.13 サイズフィルターの設定

このセクションでは、サイズフィルターの設定について説明します。最小値と最大値の間のサイズを持つターゲットのみが検出され、アラームがトリガーされます。

手順

1. 「最大サイズ」をクリックし、ライブビュー上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. 「最小サイズ」をクリックし、ライブビュー上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ています。両バージョンは互いに競合することなく同時に設定可能です。

設定に移動 → ネットワーク → 基本設定 → パラメータ設定には**TCP/IP**を使用します。

NICタイプ

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

IPv4

IPv4 モードは 2 種類利用可能です。

DHCP

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



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

手動

デバイスのIPv4パラメータを手動で設定できます。IPv4アドレス、IPv4サブネットマスク、IPv4デフォルトゲートウェイを入力し、「テスト」をクリックしてIPアドレスが利用可能か確認します。

IPv6

3 つの IPv6 モードが利用可能です。

ルートアドバタイズメント

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。



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

DHCP

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

手動

IPv6アドレス、IPv6サブネット、IPv6デフォルトゲートウェイを入力します。必要な情報はネットワーク管理者に確認してください。

MTU

最大伝送単位 (Maximum Transmission Unit) の略称です。単一のネットワーク層トランザクションで通信可能な最大プロトコルデータ単位のサイズを指します。

MTUの有効な値の範囲は1280から1500です。

DNS

ドメインネームサーバーの略称です。ドメイン名でデバイスにアクセスする場合や、一部のアプリケーション（例：メール送信）で必要となります。必要に応じて優先DNSサーバーと代替DNSサーバーを適切に設定してください。

動的ドメイン名

動的ドメイン名を有効にし、登録ドメイン名を入力します。これにより、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、デバイスが登録ドメイン名で登録されます。



動的ドメイン名を有効にするには、DHCPが有効になっている必要があります。

7.1.1 マルチキャスト

マルチキャストは、データ送信が複数の宛先デバイス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先に効率的に送信できます。

設定 → ネットワーク → 基本設定 → マルチキャストでマルチキャスト設定を行います。

IPアドレス

マルチキャストホストのアドレスを指します。

ストリームタイプ

マルチキャストソース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

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

7.2 SNMP

SNMP（Simple Network Management Protocol）を設定して、ネットワーク管理でデバイス情報を取得できます。

開始前に

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

手順

1. 設定ページに移動: **Configuration** → **Network** → **Advanced Settings** → **SNMP**.
2. **SNMPv1**を有効にする、**SNMP v2c**を有効にする、または**SNMPv3**を有効にするにチェックを入れます。

注記

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

また、必要なセキュリティレベルに応じて異なるバージョンを使用する必要があります。SNMP v1は安全ではなく、SNMP v2はアクセスにパスワードを必要とします。SNMP v3は暗号化を提供し、第3バージョンを使用する場合はHTTPSプロトコルを有効にする必要があります。

3. SNMP設定を構成します。
4. [保存]をクリックします。

7.3 SRTPの設定

セキュアリアルタイムトранSPORTプロトコル (SRTP) は、リアルタイムトランスポー

トプロトコル（RTP）インターネットプロトコルであり、ユニキャストおよびマルチキャストアプリケーションの両方で、RTPデータに対する暗号化、メッセージ認証および完全性、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. [設定] → [→] → [ネットワーク] → [→] → [詳細設定] → [→] → [SRTP] に移動します。
 2. 「サーバー証明書」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。
-

注記

- 特定のデバイスマodelのみが本機能をサポートします。
 - 機能が異常な場合は、証明書管理で選択した証明書に異常がないか確認してください。
-

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、指定したポート経由でデバイスにアクセスできます。

開始前に

デバイスのポートがネットワーク内の他のデバイスと重複している場合は、「ポート」を参照し、デバイスのポートを変更してください。

手順

1. [設定] → [→] → [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。

自動ポートマッピング 詳細については「[自動ポートマッピングの設定](#)」を参照してください。

手動ポートマッピング 詳細については、[手動ポートマッピングの設定](#)を参照してください。

3. [保存]をクリックします。

7.4.1 自動ポートマッピングの設定

手順

- 「UPnP™を有効にする」にチェックを入れ、カメラのフレンドリーネームを選択します（デフォルト名を使用することも可能です）。
 - ポートマッピングモードを「自動」に設定します。
 - [保存]をクリックします。
-



ルーターのUPnP™機能も同時に有効にしてください。

7.4.2 手動ポートマッピングの設定

手順

- 「UPnP™を有効にする」にチェックを入れ、デバイスにわかりやすい名前を付けるか、デフォルト名を使用します。
- ポートマッピングモードを「手動」に設定し、外部ポートを内部ポートと同じ値に設定します。
- 「保存」をクリックします。

次の操作

ルーターのポートマッピング設定画面で、ポート番号とIPアドレスを に設定し、デバイス側と同一にします。詳細はルーターの取扱説明書を参照してください。

7.4.3 ルーターでのポートマッピング設定

以下の設定は特定のルーター向けです。ルーターの機種によって設定内容は異なります。

手順

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

例

カメラが同一ルーターに接続されている場合、1台のカメラのポートをIPアドレス192.168.1.23で80、8000、554に設定し、別のカメラのポートをIPアドレス192.168.1.24で81、8001、555、8201に設定できます。

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

Common Service Port: DNS(53) ID 1

図 7-1 ルーター上のポートマッピング

■注記

ネットワークカメラのポートは他のポートと競合できません。例えば、ルーターのWeb管理ポートが80の場合、カメラのポートが管理ポートと同一であれば変更してください。

7.5 ポート

ポート競合によりデバイスがネットワークにアクセスできない場合、デバイスのポートを変更できます。

△注意

デフォルトのポート設定を任意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。

設定 → ネットワーク → 基本設定 → ポート設定を行うにはポート設定へ移動してください。

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。例えば、HTTPポートを81に変更した場合、ログインにはブラウザで`http://192.168.1.64:81`を入力する必要があります。

HTTPSポート

証明書を使用してブラウザがデバイスにアクセスするポートを指します。安全なアクセスを確保するため、証明書検証が必要です。

RTSPポート

リアルタイムストリーミングプロトコルのポートを指します。

SRTPポート

セキュアリアルタイムトランSPORTプロトコルのポートを指します。

サーバーポート

クライアントがデバイスを追加する際に使用するポートを指します。

拡張SDKサービスポート

クライアントがデバイスを追加する際に使用するポートを指します。安全なアクセスを確保するため、証明書検証が必要です。

WebSocketポート

プラグイン不要のプレビュー用、TCPベースの全二重通信プロトコルポート。

WebSocketsポート

プラグイン不要のプレビュー用TCPベース全二重通信プロトコルポート。安全なアクセスを確保するため証明書検証が必要です。

注記

- 強化されたSDKサービスポート、WebSocketポート、およびWebSocketsポートは特定のモデルでのみサポートされています。
- この機能をサポートするデバイスマodelについては、**設定** → **ネットワーク** → **詳細設定** → **ネットワークサービス** に移動して有効にしてください。

7.6 ドメイン名によるデバイスへのアクセス

ネットワークアクセスにはダイナミックDNS (DDNS) を使用できます。デバイスの動的IPアドレスをドメイン名解決サーバーにマッピングすることで、ドメイン名経由のネットワークアクセスを実現します。本デバイスのDDNSサービスはHTTPSのみをサポートします。

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

- TCP/IP**を参照し、DNSパラメータを設定します。
- DDNS設定ページへ移動: **設定** → **ネットワーク** → **基本設定** → **DDNS**。
- 「**DDNSを有効にする**」にチェックを入れ、**DDNSタイプ**を選択します。

DynDNS

動的DNSサーバーはドメイン名解決に使用されます。

NO-IP

NO-IPサーバーはドメイン名解決に使用されます。

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

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

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

7.7 PPPoEダイヤルアップ接続によるデバイスへのアクセス

本デバイスはPPPoE自動ダイヤルアップ機能をサポートしています。デバイスがモdemに接続されると、ADSLダイヤルアップによりパブリック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. 設定 → ネットワーク → 基本設定 → PPPoE に移動します。
2. PPPoEを有効にするにチェックを入れます。
3. PPPoEパラメータを設定します。

動的IP

ダイヤルアップ接続成功後、WANの動的IPアドレスが表示されます。

ユーザー名

ダイヤルアップネットワークアクセス用のユーザー名。

パスワード

ダイヤルアップネットワーク接続用のパスワード。

確認

ダイヤルアップパスワードを再度入力してください。

4. [保存] をクリックします。
5. デバイスにアクセスします。

ブラウザ経由 ブラウザのアドレスバーにWANの動的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によるアクセス 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。詳細はクライアントマニュアルを参照してください。

注意

取得したIPアドレスはPPPoE経由で動的に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の不便さを解消するには、DDNSプロバイダ（例: DynDns.com）からドメイン名を取得する必要があります。詳細情報は「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、動画、画像のデータを3G/4G無線ネットワーク経由で転送できます。

注意

本機能は特定のデバイスモデルでのみサポートされています。

7.8.1 ワイヤレスダイヤルの設定

内蔵ワイヤレスモジュールにより、デバイスからインターネットへのダイヤルアップアクセスが可能になります。

開始前に

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

手順

- [設定] → [→] → [ネットワーク] → [→] → [詳細設定] → [→] → [ワイヤレスダイヤル] に移動します。
- 機能の有効化を確認します。
- [ダイヤルパラメータ]をクリックし、パラメータを設定して保存します。
- 「ダイヤルプラン」をクリックします。詳細は「[武装スケジュールの設定](#)」を参照してください。
- オプション: 許可リストを設定します。詳細は「[許可リストの設定](#)」を参照してください。
- 「ダイヤルステータス」をクリックします。

[更新]をクリック ダイヤル状態を更新します。

切断をクリック 3G/4G ワイヤレスネットワークを切断します。

ダイヤル状態が「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。

- ネットワーク内のコンピューターのIPアドレスから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でデバイスを追加します。IP/ドメインを選択し、デバイスにアクセスするためのIPアドレスやその他のパラメータを入力します。

7.8.2 許可リストの設定

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

手順

1. 許可リスト設定ページへ移動: 設定 → 詳細設定 → ワイヤレスダイヤル → 許可リスト。
2. 「SMSアラームを有効にする」にチェックを入れます。
3. 許可リスト内の「+」をクリックします。
 - 1) アラームメッセージを受信する携帯電話番号を入力します。
 - 2) 「SMS経由での再起動」にチェックを入れます。
 - 3) 特定のイベントを選択すると、そのイベント発生時に携帯電話にアラームメッセージが送信されます。
 - 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受信者を設定します。
 - ✓ 許可リストのパラメータを変更します。
 - ✗ 設定済みの許可リストを削除する。
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。

注記

この機能は特定のデバイスモデルでのみサポートされています。

7.9.1 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の設定については、無線ルーターまたはアクセスポイントの取扱説明書を参照してください。

手順

1. TCP/IP設定ページに移動: 設定 → ネットワーク → 基本設定 → TCP/IP。
 2. パラメータ設定には「Wlan」を選択します。詳細な設定についてはTCP/IPを参照してください。
-



注意

Wi-Fiを安定して使用するには、DHCPの使用は推奨されません。

3. Wi-Fi設定ページへ移動: 設定 → ネットワーク → 詳細設定 → Wi-Fi.
4. パラメータを設定して保存します。
 - 1) [検索]をクリックします。
 - 2) SSIDを選択してください。これは無線ルーターまたはアクセスポイントと同じである必要があります。
ネットワークのパラメータは自動的にWi-Fiに表示されます。
 - 3) ネットワークモードを「管理」に選択します。
 - 4) ワイヤレスネットワークに接続するためのキーを入力します。キーは、ルーターで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。

次の操作

TCP/IP設定ページへ移動: 設定 → ネットワーク → 基本設定 → TCP/IP、WlanをクリックしてIPv4アドレスを確認し、デバイスにログインします。

7.10 ネットワークサービスの設定

特定のプロトコルのON/OFF状態を必要に応じて制御できます。

手順



注記

この機能は機種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以降またはMozilla Firefox 52以降でデバイスにアクセスする場合、WebSocketプロトコルを有効にする必要があります。有効にしないと、ライブビュー、画像キャプチャ、デジタルズームなどが使用できません。
デバイスがHTTPを使用している場合、WebSocketを有効にしてください。
デバイスがHTTPSを使用している場合は、WebSocketsを有効にしてください。
WebSocketsを使用する場合、サーバー証明書を選択してください。

注意

サーバー証明書を選択する前に、証明書管理を完了してください。詳細については、[証明書管理](#)を参照してください。

SDKサービスおよび拡張SDKサービス

SDKプロトコルを使用してデバイスをクライアントソフトウェアに追加するには、[\[SDKサービスを有効にする\]](#)をチェックしてください。

「[拡張SDKサービスを有効にする](#)」にチェックを入れると、TLSプロトコル経由のSDK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](#)を選択してください。

注意

- サーバー証明書を選択する前に、証明書管理を完了してください。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際は、データ伝送を暗号化するため、拡張SDKサービスの使用とアーミングモードでの通信設定を推奨します。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 (Transport Layer Security)

本デバイスは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てください。

Bonjour

プロトコルを無効化するにはチェックを外してください。

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プロトコル経由でデバイスにアクセスする必要がある場合、ユーザー設定を構成してネットワークセキュリティを強化できます。

手順

1. 設定 → ネットワーク → 詳細設定 → 統合プロトコルに移動します。
2. 「**Open Network Video Interfaceを有効にする**」にチェックを入れます。
3. 「追加」をクリックし、Open Network Video Interfaceユーザーを設定します。

削除

選択したオープンネットワークビデオインターフェースユーザーを削除します。

変更 選択したオープンネットワークビデオインターフェースユーザーを変更します。

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

7.12 ISUPの設定

デバイスがISUPプラットフォーム（旧称: Ehome）に登録されると、パブリックネットワーク経由でデバイスの閲覧・管理、データ送信、アラーム情報の転送が可能になります。

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. [有効化] 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、登録状態がオンラインに変わります。

7.13 アラームサーバーの設定

本装置は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へ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、HTTPS、またはISUPデータ伝送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、ポートを入力します。
3. プロトコルを選択します。

注記

HTTP、HTTPS、ISUPが選択可能です。通信中のデータ伝送を暗号化するため、HTTPSの使用を推奨します。

4. **[テスト]**をクリックし、IPまたはホストが利用可能か確認します。
5. 「保存」をクリックします。

7.14 HiLookVisionによるカメラアクセス

HiLookVisionはモバイル端末用アプリケーションです。本アプリを使用すると、ライブ映像の閲覧やアラーム通知の受信などが可能です。

開始前に

ネットワークケーブルでカメラをネットワークに接続してください。

手順

1. 以下の方法でHiLookVisionアプリケーションを入手しインストールしてください。

- <https://appstore.hikvision.com> にアクセスし、お使いの携帯電話のシステムに応じてアプリケーションをダウンロードしてください。
- 当社公式サイトにアクセスし、「サポート」→「→ ツール」→「→ Hikvision App Store」へ進む。
- 下記のQRコードをスキャンしてアプリケーションをダウンロードしてください。



注意

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

- 1) <https://appstore.hikvision.com/static/help/index.html> にアクセスし、トラブルシューティングを参照してください。
 - 2) <https://appstore.hikvision.com/> にアクセスし、画面右上の「インストールヘルプ」をクリックしてトラブルシューティングを参照してください。
-

2. アプリケーションを起動し、HiLookVisionユーザー アカウントを登録してください。
3. 登録後、ログインします。
4. アプリで右上の「+」をタップし、カメラのQRコードをスキャンしてカメラを追加します。QRコードはカメラ本体またはパッケージ内のクイックスタートガイド表紙に記載されています。
5. 画面の指示に従いネットワーク接続を設定し、カメラをHiLookVisionアカウントに追加します。
6. 詳細については、HiLookVisionアプリ ユーザーマニュアルを参照してください。

7.14.1 カメラでHiLookVisionサービスを有効にする

HiLookVisionサービスをご利用になる前に、カメラでHiLookVisionサービスを有効にする必要があります。

SADPソフトウェアまたはWebブラウザからサービスを有効化できます。

Webブラウザ経由でのHiLookVisionサービスの有効化

Web ブラウザで HiLookVision サービスを有効にするには、以下の手順に従ってください。

開始前に

サービスを有効化する前に、カメラのアクティベーションが必要です。

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設定インターフェースに入ります。設定 → 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HiLookVisionを選択します。
4. 「有効化」にチェックを入れます。
5. ポップアップウィンドウで「利用規約」と「プライバシーポリシー」をクリックして読みます。
6. カメラの認証コードを作成するか、既存の認証コードを変更します。



カメラをHiLookVisionサービスに追加する際には認証コードが必要です。

7. 設定を保存します。

SADPソフトウェア経由でHiLookVisionサービスを有効にする

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

手順

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

注記

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

5. 「利用規約」と「プライバシーポリシー」をクリックして読みます。
6. 設定を確認します。

7.14.2 HiLookVisionの設定

手順

1. 以下の方法でHiLookVisionアプリケーションを入手しインストールしてください。
 - <https://appstore.hikvision.com> にアクセスし、お使いの携帯電話のシステムに応じてアプリケーションをダウンロードしてください。
 - 当社公式サイトにアクセスし、「サポート」→「→ ツール」→「→ Hikvision App Store」へ進む。
 - 下記のQRコードをスキャンしてアプリケーションをダウンロードしてください。



注意

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

- 1) <https://appstore.hikvision.com/static/help/index.html> にアクセスし、トラブルシューティングを参照してください。
 - 2) <https://appstore.hikvision.com/> にアクセスし、画面右上の「インストールヘルプ」をクリックしてトラブルシューティングを参照してください。
-
2. アプリケーションを起動し、HiLookVisionユーザー アカウントを登録してください。
 3. 登録後、ログインします。

7.14.3 HiLookVisionへのカメラ追加

手順

1. モバイルデバイスをWi-Fiに接続します。
2. HiLookVisionアプリにログインします。
3. ホーム画面で右上の「+」をタップし、カメラを追加します。

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



QRコードがない場合や認識できないほどぼやけている場合は、カメラのシリアル番号を入力して追加することもできます。

5. カメラの認証コードを入力してください。



- 必要な認証コードは、カメラでHiLookVisionサービスを有効化する際に作成または変更するコードです。
 - 認証コードを忘れた場合、ウェブブラウザ経由でプラットフォームアクセス設定ページから現在の認証コードを確認できます。
-

6. ポップアップ画面で「ネットワークに接続」ボタンをタップします。

7. カメラの機能に応じて「有線接続」または「無線接続」を選択します。

無線接続

スマートフォンが接続しているWi-Fiパスワードを入力し、「次へ」をタップしてWi-Fi接続プロセスを開始します。（Wi-Fi設定時はカメラをルーターから3メートル以内に設置してください）

有線接続

ネットワークケーブルでカメラをルーターに接続し、結果画面で「接続済み」をタップします。



ルーターは、スマートフォンが接続しているものと同じである必要があります。

8. 次の画面で「追加」をタップして追加を完了します。

9. 詳細については、HiLookVisionアプリのユーザーマニュアルを参照してください。

第8章 警戒スケジュールと警報連動

武装スケジュールとは、デバイスが特定のタスクを実行するカスタマイズされた時間帯です。アラーム連動とは、スケジュールされた時間帯に検知された特定の事象や対象に対する対応です。

8.1 警戒スケジュール設定

デバイスタスクの有効時間を設定します。

手順

1. 「武装スケジュール」をクリックします。
2. タイムバーをドラッグして希望の有効時間を設定します。



1日に最大8つの期間を設定できます。

3. 時間帯を調整します。
 - 選択した時間帯をクリックし、希望の値を入力します。「保存」をクリックします。
 - 選択した時間枠をクリックします。両端をドラッグして時間枠を調整します。
 - 選択した時間枠をクリックし、タイムバー上でドラッグします。
4. オプション:[コピー先...]をクリックし、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 連動方法設定

イベントまたはアラーム発生時に連動機能を有効にできます。

8.2.1 アラーム出力のトリガー

デバイスが警報出力デバイスに接続され、警報出力番号が設定されている場合、警報がトリガーされると、デバイスは接続された警報出力デバイスに警報情報を送信します。

手順

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

自動アラーム 設定に関する詳細は「[自動警報](#)」を参照してください。

手動アラーム 設定に関する情報は、「[手動アラーム](#)」を参照してください。

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ーできます。

手順

1. 手動アラームのパラメータを設定します。

警報出力番号

外部警報装置に接続された警報インターフェースに応じて、警報出力番号を選択します。

アラーム名

アラーム出力に名前をカスタム設定します。

遅延時間

手動を選択します。

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

自動アラーム

自動アラームのパラメータを設定すると、デバイスは設定された作動スケジュールで自動的にアラーム出力をトリガーします。

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

外部警報装置に接続された警報インターフェースに応じて、警報出力番号を選択します。

警報名

アラーム出力に名前をカスタム設定します。

遅延時間

アラーム発生後、アラーム出力が残存する時間間隔を指します。

2. アラームスケジュールを設定します。設定方法については「アラームスケジュール設定」を参照してください。
3. 「コピー先...」をクリックし、パラメータを他のアラーム出力チャンネルにコピーします。
4. 「保存」をクリックします。

8.2.2 FTP/NAS/メモリーカードへのアップロード

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

FTPサーバーの設定については、「[FTPの設定](#)」を参照してください。

NASの設定については、「[NASの設定](#)」を参照してください。

メモリーカードの保存設定については、「[新しいメモリーカードまたは暗号化されていないメモリーカードの設定](#)」を参照してください。

8.2.3 メール送信

「メール送信」にチェックを入れると、アラームイベントが検出された際に、デバイスがアラーム情報を含むメールを指定されたアドレスに送信します。

メール設定については、「[メール設定](#)」を参照してください。

メール設定

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

開始前に

メール機能を使用する前に、DNSサーバーを設定してください。設定 → ネットワーク → 基本設定 → TCP/IP のDNS設定で設定します。

手順

1. メール設定ページへ移動: 設定 → ネットワーク → 詳細設定 → メール。
2. メールパラメータを設定します。
 - 1) 送信者のメールアドレス情報（送信者アドレス、SMTPサーバー、SMTPポート）を入力します。
 - 2) オプション: メールサーバーが認証を必要とする場合、「認証」にチェックを入れ、サーバーにログインするためのユーザー名とパスワードを入力します。
 - 3) メール暗号化を設定します。
 - SSLまたはTLSを選択し、STARTTLSを無効にした場合、メールはSSLまたはTLSで暗号化されて送信されます。SMTPポートは465に設定してください。
 - SSLまたはTLSを選択し、STARTTLSを有効にした場合、メールはSTARTTLSによって暗号化された後に送信され、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、メールサーバーがプロトコルをサポートしていることを確認してください。メールサーバーがプロトコルをサポートしていない状態でSTARTTLSを有効にすると、メールは暗号化されずに送信されます。

- 4) オプション: アラーム画像付き通知を受け取りたい場合は、「画像添付」にチェックを入れます。通知メールには、設定可能な画像キャプチャ間隔で、イベントに関するアラーム画像が3枚添付されます。
 - 5) 受信者の情報（受信者名と住所を含む）を入力します。
 - 6) 「テスト」をクリックし、機能が正しく設定されているか確認します。
3. 「保存」をクリックします。

8.2.4 監視センターへの通知

監視センター通知にチェックを入れると、警報イベント検出時に警報情報が監視センターにアップロードされます。

8.2.5 録画トリガー

録画をトリガーするにチェックを入れると、デバイスは検知されたアラームイベントに関するビデオを録画します。

録画設定については、「動画録画と静止画キャプチャ」を参照してください。

8.2.6 点滅ライト

点滅ライトを有効にし、点滅ライト警報出力を設定すると、警報イベントが検出された際にライトが点滅します。

点滅アラームライト出力の設定

イベント発生時、装置の点滅ライトを警報として作動させることができます。

手順

1. 設定 → イベント → 基本イベント → 点滅アラームライト出力 に移動します。
2. 点滅時間、点滅頻度、輝度を設定します。

点滅時間

1回の警報発生時に点滅が持続する時間。

点滅頻度

ライトが点滅する速度。高周波、中周波、低周波、常時点灯から選択可能。

明るさ

光の明るさ。

- 警戒スケジュールを設定します。詳細は「[警戒スケジュールの設定](#)」を参照してください。
 - [保存]**をクリックします。
-



特定のデバイスモデルのみが本機能をサポートしています。

8.2.7 音声警告

音声警告を有効にし、音声アラーム出力を設定すると、アラーム発生時にデバイスの内蔵スピーカーまたは接続された外部スピーカーから警告音が鳴ります。

可聴警報出力の設定については、「[可聴警報出力の設定](#)」を参照してください。



この機能は特定のカメラモデルでのみサポートされています。

音声アラーム出力の設定

デバイスが検知エリア内で対象物を検出した場合、警告として可聴警報を鳴らすことができます。

手順

- 設定 → イベント → 基本イベント → 音声アラーム出力に移動します。
- 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、必要な警報時間を設定します。
 - 警告を選択し、その内容を設定します。必要な警報時間を設定します。
 - カスタムオーディオを選択します。ドロップダウンリストからカスタムオーディオファイルを選択できます。ファイルがない場合は、[追加]をクリックして要件を満たすオーディオファイルをアップロードできます。最大3つのオーディオファイルをアップロードできます。
- オプション: [テスト]をクリックすると、選択した音声ファイルをデバイスで再生します。
- 音声アラームの武装スケジュールを設定します。詳細は「[武装スケジュールの設定](#)」を参照してください。
- 「保存」をクリックします。



注

本機能は特定のデバイスモデルでのみサポートされています。

第9章 システムとセキュリティ

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

9.1 デバイス情報の表示

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

設定画面で、[→] → [System] → [→] → [System Settings] → [→] → [Basic Information] の順に選択すると、デバイス情報を表示できます。

9.2 ログの検索と管理

ログは問題の特定とトラブルシューティングに役立ちます。

手順

1. 設定 → システム → メンテナンス → ログ に移動します。
2. 主要タイプ、副次タイプ、開始時刻、終了時刻の検索条件を設定します。
3. 「検索」をクリックします。
一致したログファイルがログリストに表示されます。
4. オプション: エクスポートをクリックしてログファイルをコンピュータに保存します。

9.3 同時ログイン

管理者は、Webブラウザ経由でシステムに同時にログインできるユーザー数の最大値を設定できます。

設定 → システム → ユーザー管理 に移動し、一般 をクリックして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

同じパラメータを持つ他のデバイスでの一括設定を迅速に行うのに役立ちます。

設定画面 (→) → システム (→) → メンテナンス (→) → アップグレードとメンテナンス (Upgrade & Maintenance) を選択します。インポートまたはエクスポートが必要なデバイスパラメータを選択し、画面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、実行ログ、システム情報、ハードウェア情報が含まれます。

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 に移動します。必要な 診断情報を確認し、診断情報をクリックしてデバイスの対応する診断情報をエクスポートします。

9.6 再起動

ブラウザからデバイスを再起動できます。

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

9.7 復元とデフォルト

復元とデフォルトは、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. [設定] → [システム] → [メンテナンス] → [アップグレードとメンテナンス] 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、ビデオフォーマットを除くデバイスパラメータをデフォルト設定にリセットします。

デフォルト

すべてのパラメータを工場出荷時のデフォルトにリセットします。

注意

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

9.8 アップグレード

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ります。

⚠ 注意

プロセス中は電源を切斷しないでください。アップグレード後、デバイスは自動的に再起動します。

手順

1. [設定] → [システム] → [メンテナンス] → [アップグレードとメンテナンス] に移動します。
2. アップグレード方法を選択します。
ファームウェア アップグレードファイルの正確なパスを指定します。
ファームウェアディレクトリ アップグレードファイルが属するディレクトリを指定します。
3. [参照]をクリックしてアップグレードファイルを選択します。
4. [アップグレード]をクリックします。

9.9 オープンソースソフトウェアライセンスの表示

設定 → システム → システム設定 → デバイス情報 に移動し、[ライセンスを表示]をクリックします。

9.10 ウィーガンド

■ i 注

この機能は、特定のカメラモデルでのみサポートされています。

[有効化] をチェックし、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 26 ビットです。

有効にすると、認識されたナンバープレート番号が選択したウィーガンドプロトコルで出力されます。

9.11 メタデータ

メタデータは、アルゴリズム処理の前にカメラが収集する生データです。これにより、ユーザーはさまざまなデータ活用方法を探求することができます。

設定 → システム → メタデータ設定 に移動し、目的の機能のメタデータアップロードを有効にします。

スマートイベント

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

9.12 日時設定

タイムゾーン、時刻同期、夏時間（DST）の設定により、デバイスの日時を設定できます。

9.12.1 手動での時刻同期

手順

1. [設定] → [→] → [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. [手動で時刻を同期] をクリックします。
4. 時刻同期方法を選択します。
 - 「時刻を設定」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。
5. 「コンピューターの時刻と同期」にチェックを入れると、デバイスの時刻がローカルPCの時刻と同期されます。
6. 「保存」をクリックします。

9.12.2 NTPサーバーの設定

正確で信頼性の高い時刻ソースが必要な場合、NTPサーバーを使用できます。

開始前に

NTPサーバーを設定するか、NTPサーバー情報を入手してください。

手順

1. [設定] → [→] → [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. サーバーアドレス、NTPポート、間隔を設定します。

注記

サーバーアドレスはNTPサーバーのIPアドレスです。

5. サーバー接続をテストするには「テスト」をクリックします。
6. [保存]をクリックします。

9.12.3 衛星による時刻同期



注記

この機能は、デバイスによって異なります。

手順

1. 設定 → システム → システム設定 → 時間設定 に移動します。
2. 「衛星時刻同期」を選択します。
3. 間隔を設定します。
4. [保存]をクリックします。

9.12.4 夏時間設定

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

手順

1. 設定 → システム → システム設定 → DST に移動します。
2. [DSTを有効にする]にチェックを入れます。
3. 開始時刻、終了時刻、DSTバイパスを選択します。
4. [保存]をクリックします。

9.13 RS-485の設定

RS-485は、本装置を外部機器に接続するために使用されます。通信距離が長すぎる場合、RS-485を使用して本装置とコンピュータまたは端末間でデータを伝送できます。

始める前に

デバイスとコンピュータまたはターミナルをRS-485ケーブルで接続してください。

手順

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



注意

デバイスとコンピュータまたはターミナルのパラメータはすべて同一に保つ必要があります。

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。通信距離が短い場合、RS-232 によりデバイスとコンピュータまたは端末間の通信を実現できます。

開始前に

RS-232ケーブルでデバイスをコンピュータまたは端末に接続してください。

手順

1. 設定 → システム → システム設定 → **RS-232** に移動します。
2. RS-232パラメータを設定し、デバイスとコンピュータまたは端末を対応させます。
3. 「保存」をクリックします。

9.15 消費電力モード

デバイス動作時の消費電力を切り替えるために使用します。



この機能は特定のカメラモデルでのみサポートされています。

設定 → システム → システム設定 → 消費電力モードに移動し、目的の消費電力モードを選択します。

フル消費モード

すべての機能が有効な状態で動作します。

低消費電力リアルタイムモード

デバイスのDSPは通常動作します。メインストリームは半分のフレームレートで動画を記録し、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[†]

デバイスの電力が低電力スリープモードのしきい値を下回ると、デバイスはスリープモードに入ります。

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

スケジュールスリープ

デバイスがスケジュールされたスリープ時間中にあればスリープモードに入り、そうでない場合はユーザー設定モードに入ります。

注記

スケジュールされたスリープのスケジュール設定については、「**武装スケジュールとアラーム連動**」を参照してください。

本デバイスはタイミングウェイクをサポートします。詳細は「**タイミングウェイクの設定**」を参照してください。

9.16 外部デバイス

補助灯、ハウジングワイパー、LEDライトなどの外部デバイスをサポートするデバイスは、ハウジングと併用時にWebブラウザ経由で制御可能です。外部デバイスはモデルによって異なります。

輝度

ロービームの明るさとハイビームの明るさを実際の状況に合わせて調整してください。

タイミング

設定したスケジュールに基づきLEDライトが点灯します。開始時刻と終了時刻を設定してください。

自動

LEDライトは周囲の明るさに応じて点灯します。

9.16.1 補助照明設定

補助照明を設定でき、関連パラメータについては実際のデバイスを参照してください。

スマート補助光

スマート補助光は、補助光点灯時に露出オーバーを回避します。

補助光モード

デバイスが補助光をサポートしている場合、補助光モードを選択できます。

IRモード

IRライトが有効になります。

白色光モード

白色光が有効です。

ミックスモード

赤外線ライトと白色ライトの両方が有効です。

オフ

補助照明は無効です。

輝度調整モード

自動

実際の環境に応じて明るさが自動的に調整されます。

手動

スライダーをドラッグするか、値を設定して輝度を調整できます。

9.16.2 ヒーター

デバイスのレンズ周辺の曇りを除去するためにヒーターを有効にできます。

設定 → システム → システム設定 → 外部デバイス に移動し、必要に応じてモードを選択してください。

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、システムの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 および 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。

設定 → システム → セキュリティ → 認証 に移動し、必要に応じて認証プロトコルと方法を選択します。

RTSP認証

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

RTSPダイジェストアルゴリズム

RTSP認証におけるMD5、SHA256、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した場合、互換性の問題によりサードパーティプラットフォームがデバイスへのログインやライブビューの有効化を行えない可能性があります。強度の高い暗号化アルゴリズム の使用を推奨します。

WEB認証

ダイジェスト認証とダイジェスト/ベーシック認証をサポートしています。これは、デバイスへのWEBリクエスト送信時に認証情報が必要であることを意味します。ダイジェスト/ベーシックを選択した場合、デバイスはダイジェスト認証またはベーシック認証

をサポートします。ダイジェストのみを選択した場合、デバイスはダイジェスト認証のみをサポートします。

WEBダイジェストアルゴリズム

WEB認証における暗号化アルゴリズムとしてMD5、SHA256、MD5/SHA256が利用可能です。MD5以外のダイジェストアルゴリズムを有効化した場合、互換性の問題によりサーバーパーティプラットフォームがデバイスへのログインやライブビューの有効化を行えない可能性があります。強度の高い暗号化アルゴリズムの使用を推奨します。

注意

認証要件については、プロトコルの詳細内容をご参照ください。

9.17.2 IPアドレスフィルターの設定

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。特定のIPアドレスからのアクセスを許可または禁止するために有効化できます。

IPアドレスはIPv4を指します。

手順

- 設定 → → → システム → → → セキュリティ → → → IPアドレスフィルタに移動します。
- 「IPアドレスフィルタを有効にする」にチェックを入れます。
- IPアドレスフィルターの種類を選択します。

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。

許可 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。

- IPアドレスフィルタリストを編集します。

追加 リストに新しいIPアドレスまたはIPアドレス範囲を追加します。

変更 リスト内の選択したIPアドレスまたはIPアドレス範囲を変更します。

削除 リスト内の選択したIPアドレスまたはIPアドレス範囲を削除します。

- [保存] をクリックします。

9.17.3 HTTPSの設定

HTTPS は、暗号化された送信と ID 認証を可能にするネットワークプロトコルです。これにより、リモートアクセスのセキュリティが向上します。

手順

1. 設定 → ネットワーク → 詳細設定 → **HTTPS** に移動します。
2. 「有効化」にチェックを入れ、HTTPまたはHTTPSプロトコル経由でカメラにアクセスできるようにします。
3. HTTPSプロトコル経由でのみカメラにアクセスするには、[HTTPSブラウジングを有効にする]にチェックを入れます。
4. サーバー証明書を選択します。
5. [保存]をクリックします。

注記

機能が正常に動作しない場合、証明書管理で選択した証明書に異常がないか確認してください。

9.17.4 QoSの設定

QoS (Quality of Service) は、データ送信の優先度を設定することで、ネットワーク遅延やネットワーク輻輳の改善に役立ちます。

注記

QoS は、ルーターやスイッチなどのネットワークデバイスのサポートが必要です。

手順

1. 設定 → ネットワーク → 詳細設定 → **QoS** に移動します。
2. ビデオ/オーディオDSCP、アラームDSCP、管理DSCPを設定します。

注記

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

3. [保存]をクリックします。

9.17.5 IEEE 802.1Xの設定

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。IEEE 802.1x規格でネットワークに接続するデバイスは、認証が必要

です。

設定 → → → ネットワーク → → → 詳細設定 → → → 802.1X に移動し、機能を有効にします。

ルーター情報に基づいてプロトコルとEAPOLバージョンを設定する。

プロトコル

EAP-LEAP、EAP-TLS、およびEAP-MD5が選択可能

EAP-LEAP および EAP-MD5

EAP-LEAP または EAP-MD5 を使用する場合、認証サーバーを設定する必要があります。事前にサーバーに 802.1X 用のユーザー名とパスワードを登録してください。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、Identify、Private Key Password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バージョンは、ルーターまたはスイッチのバージョンと一致している必要があります。

9.17.6 制御タイムアウト設定

この機能を有効にすると、設定されたタイムアウト期間内に Web ブラウザからデバイスに対して操作（ライブ画像の表示は含まない）を行わない場合、ログアウトされます。

設定を完了するには、[設定] → [システム] → [セキュリティ] → [詳細セキュリティ] に移動してください。

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・分析して、不正侵入を発見し、セキュリティイベントの問題を解決することができます。

手順

注記

この機能は特定のカメラモデルでのみサポートされています。

1. 設定 → システム → メンテナンス → セキュリティ監査ログ に移動します。
2. ログの種類、開始時刻、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. オプション: エクスポートをクリックしてログファイルをコンピュータに保存します。

9.17.8 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向上させるソリューションです。この機能を有効にすると、デバイスのリスクの高い機能、プロトコル、ポートが無効化され、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 → 詳細セキュリティ に移動します。セキュリティ強化にチェックを入れ、保存をクリックします。

9.17.9 SSH

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

SSH 機能は、デフォルトでは無効になっています。



注意

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

9.18 証明書管理

サーバー/クライアント証明書および CA 証明書の管理、証明書の有効期限が近づいた場合や、期限切れ/異常があった場合にアラームを送信するのに役立ちます。

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. プロンプトに従い、証明書ID、国、ホスト名/IP、有効期間、その他のパラメータを入力してください。



証明書IDは数字または文字で、64文字以内である必要があります。

3. [OK]をクリックします。

4. オプション: [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 証明書のインポート

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. 「参照」をクリックし、目的のサーバー/クライアント証明書を選択します。
5. 必要なインポート方法を選択し、必要な情報を入力します。
6. [OK]をクリックします。
7. オプション: [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

- 最大16個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、証明書を削除することはできません。
 - 証明書を使用している機能は、機能欄で確認できます。
 - 既存の証明書と同一のIDを持つ証明書を作成したり、既存の証明書と同一の内容を持つ証明書をインポートすることはできません。
-

9.18.4 サーバー/クライアント証明書のインストール

手順

1. [構成] → [→] → [システム] → [→] → [セキュリティ] → [→] → [証明書管理] に移動します。

- 「自己署名証明書を作成」、「証明書要求を作成」、「インポート」を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。

自己署名証明書を作成 [自己署名証明書の作成を参照](#)

証明書要求の作成 [証明書要求の作成を参照](#)

証明書のインポート [「証明書のインポート」を参照](#)

9.18.5 CA証明書のインストール

手順

- 【インポート】をクリックします。
- 証明書IDを入力します。
- 【参照】をクリックし、目的のサーバー/クライアント証明書を選択します。
- 必要なインポート方法を選択し、必要な情報を入力します。
- 【OK】をクリックします。



最大16個の証明書が許可されます。

9.18.6 証明書有効期限アラームの有効化

手順

- 「証明書有効期限アラームを有効にする」にチェックを入れます。有効にすると、証明書の有効期限が近づいている、または期限切れ・異常状態になった際に、監視センタ宛てのメールまたはカメラリンクで通知を受け取ります。
- 「有効期限前の通知間隔（日数）」、「アラーム頻度（日数）」、「検知時間（時間）」を設定します。



- 有効期限前のリマインド日を1日に設定すると、カメラは有効期限の前日に通知します。設定可能範囲は1~30日です。デフォルトのリマインド日は7日です。
 - 有効期限前のリマインド日を1日に設定し、検知時間を10:00に設定した場合、証明書が翌日の9:00に失効するならば、カメラは初日の10:00に通知します。
-

- 【保存】をクリックします。

9.19 ユーザーとアカウント

9.19.1 ユーザーアカウントと権限の設定

管理者は、他のアカウントの追加、変更、削除、および異なるユーザーlevelに異なる権限を付与することができます。

⚠ 注意

ネットワーク上でデバイスを使用する際のセキュリティを強化するため、アカウントのパスワード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推奨します。デバイスが高リスク環境で使用される場合、パスワードは毎月または毎週変更することを推奨します。

手順

- 設定 → システム → ユーザー管理 → ユーザー管理に移動します。
- 「追加」をクリックします。ユーザー名を入力し、レベルを選択し、パスワードを入力します。必要に応じてユーザーにリモート権限を割り当てます。

管理者

管理者は全ての操作権限を持ち、ユーザーとオペレーターの追加、権限の割り当てが可能です。

ユーザー

ユーザーにはライブ映像の閲覧、PTZパラメータの設定、自身のパスワード変更の権限を割り当てられますが、その他の操作の権限はありません。

オペレーター

オペレーターには、管理者操作とアカウント作成を除く全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

ユーザーを選択し、削除をクリックします。

■ i 注記

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 ブラウザからシステムに同時にログインできるユーザーの最大数を設定できます。

設定 → システム → ユーザー管理 に移動し、[全般] をクリックして [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 → システム → ユーザー管理 → オンラインユーザー に移動し、オンラインユーザーの一覧を表示します。

第10章 VCAリソースの割り当て

VCA リソースでは、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提供されます。これにより、必要な機能により多くのリソースを割り当てることができます。

手順

1. [設定] → [→] → [システム] → [→] → [システム設定] → [→] → [VCAリソース] に移動します。
2. 必要なVCA機能を選択します。
3. 設定を保存します。

注記

一部のVCA機能は排他的です。特定の機能または複数の機能を選択して保存すると、他の機能は非表示になります。

10.1 スマートモードの切り替え

スマート機能を有効にすると、必要に応じて検出対象を選択できます。

手順

1. 設定 → システム → システム設定 → スマートモード切り替え に移動します。
2. 希望のスマートモードを選択します。

表 10-1 スマートモードのスマート機能

スマートモード	検出対象	スマート機能
---------	------	--------

キャプチャモード

デバイスは検知エリア内の対象物をキャプチャし、撮影した画像をアップロードします。必要に応じてキャプチャ対象を選択できます。

	顔	顔キャプチャ
	自動車	道路交通
	その他の組み合わせ	マルチターゲット型検出

比較モード

本装置は、規定領域内のターゲットを認識・捕捉・比較し、ターゲットの属性及びモデルを収集する。

	顔	顔キャプチャ
--	---	--------

		顔画像比較とモデリング
顔+人体		マルチターゲット型検出 顔画像比較とモデリング

パターンモード

デバイスは、異なるチャネルでキャプチャされた顔、人体、車両情報をリンクし、ターゲットパターンを表示します。

	チャンネル1: 顔 チャンネル2: 顔+人体+自動車+非自動車	パターン連携 顔検出 マルチターゲット型検出 顔画像比較とモデリング
	チャンネル1: 顔+人体 チャンネル2: 顔+人体+自動車+非自動車	パターン連結マルチターゲット型検出 顔画像比較とモデリング
監視	-	

3. [保存]をクリックします。

■ i注記

- 比較モードでは、チャンネル2のみ監視モードをサポートします。
- パターンモードは2チャネルデバイスでのみサポートされます。人体検知はチャンネル1のみが対応しています。

10.2 顔キャプチャ

本デバイスは設定エリアに現れた顔をキャプチャでき、顔情報はキャプチャ画像と共にアップロードされます。

■ i注記

- 顔キャプチャ対応デバイスでは、VCAリソースで機能を有効にする必要があります。詳細は「VCAリソースの割り当て」を参照してください。
- 顔検出は特定モデルでのみサポートされています。

10.2.1 顔キャプチャの設定

設定された領域に表示される顔をキャプチャできます。

開始前に

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 → 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」にチェックを入れます。
4. 「○」をクリックし、検出領域を描画します。描画領域はライブビュー画像の1/2～2/3を占めることを推奨します。
5. 「□」をクリックし、ライブビュー上の顔の瞳孔間距離に基づいて長方形を描画します。



図10-1 顔検出設定

デバイスは設定された最小瞳孔距離に基づき、対象領域内に人間の顔が存在するか否かを検知します。

6. 警戒スケジュール設定については「警戒スケジュール設定」を参照してください。運動方法設定については「運動方法設定」を参照してください。
7. [保存]をクリックします。
8. オーバーレイとキャプチャ設定については、「オーバーレイとキャプチャ」を参照してください。詳細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

キャプチャされた顔画像は「画像」で閲覧・ダウンロードできます。詳細は「画像の閲覧とダウンロード」を参照してください。

10.2.2 オーバーレイとキャプチャ

キャプチャパラメータと、ストリームおよび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

ターゲットやルール情報を含むスマート情報をストリーム上に表示します。

アラーム画像にターゲット情報を表示

アラーム画像にターゲット情報をオーバーレイ表示します。

ターゲット画像設定

カスタム、ヘッドショット、上半身ショット、全身ショットから選択可能。

注記

カスタムを選択した場合、必要に応じて幅、頭の高さ、体の高さをカスタマイズできます。

固定値にチェックを入れると、画像の高さを設定できます。

背景画像設定

対象画像と比較して、背景画像は追加の環境情報を提供するシーン画像です。背景画像の品質と解像度を設定できます。監視センターに背景画像をアップロードする必要がある場合は、「背景アップロード」にチェックを入れてください。

人数カウントオーバーレイ

フロー オーバーレイの種類を選択します。

日次リセット時刻を選択します。即時リセットする場合は「手動リセット」をクリックしてください。

カメラ

カメラにデバイス番号とカメラ情報を設定できます。これらは撮影画像にオーバーレイ表示されます。

テキストオーバーレイ

で、必要な項目を選択し、撮影画像に表示する順序を調整できます。

デバイス番号とカメラ情報の内容は同一ページに記載してください。

10.2.3 顔検出アルゴリズムのパラメータ

顔検出アルゴリズムライブラリのパラメータ設定と最適化に使用します。

設定 → 顔検出 → 詳細設定 → パラメータに移動します。

顔検出バージョン

アルゴリズムライブラリのバージョンが表示されます。

検出パラメータ

生成速度

対象を識別する速度。値が高いほど対象の認識が速くなります。値をかなり低く設定し、設定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。壁画やポスター内の顔の誤認識を減らせます。デフォルト値の3が推奨されます。

感度

対象を識別する感度。値が高いほど顔を認識しやすくなりますが、誤認識の可能性も高まります。デフォルト値の3が推奨されます。

キャプチャパラメータ

ベストショット

ターゲットが検出エリアを離れた後のベストショット。

キャプチャ回数

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

キャプチャ間隔

画像をキャプチャするフレーム間隔。デフォルト値である1を設定した場合、カメラは毎フレームで顔をキャプチャすることを意味します。

キャプチャ閾値

キャプチャとアラームをトリガーする顔の品質を示します。値が高いほど、キャプチャとアラームをトリガーするために必要な品質が高くなります。

クイックショット

クイックショットの閾値と最大キャプチャ間隔を設定できます。

クイックショット閾値

クイックショットをトリガーする顔の品質を表します。

顔露出

チェックボックスをオンにすると、顔の露出を有効にします。

基準輝度

顔露出モードにおける顔の基準輝度。顔を検出すると、カメラは設定値に基づいて顔の明るさを調整します。値が高いほど顔は明るくなります。

最小露出時間

カメラが顔を露出する最小時間。デフォルト値は1分です。

注意

顔露出を有効にする場合、WDR機能が無効化され、手動アイリスが選択されていることを必ず確認してください。

顔フィルタリング時間

カメラが顔を検出してから撮影アクションを実行するまでの時間間隔を指します。検出された顔が設定されたフィルタリング時間未満の時間でシーン内に留まった場合、撮影はトリガーされません。例えば、顔フィルタリング時間を5秒に設定した場合、カメラは顔が5秒間シーン内に留まり続けた時点で検出された顔を撮影します。

注記

顔フィルタリング時間（0秒より長い値）を設定すると、実際の撮影時間が上記設定値を下回る可能性が高まります。

デフォルトに戻す

[復元]をクリックすると、詳細設定のすべての設定が工場出荷時のデフォルト値に復元されます。

10.2.4 シールド領域の設定

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

手順

1. 「シールド領域」を選択します。
2. 「」をクリックしてシールド領域を描画します。複数のシールド領域を設定する場合は、上記の手順を繰り返します。
3. オプション：描画した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 道路交通

自動車、非自動車、歩行者は、設定された車線に入ると検出・捕捉され、関連情報と捕捉された画像がアップロードされます。

注記

特定のデバイスモデルのみがこの機能をサポートしています。

10.3.1 車両検知設定

設定された車線に進入した車両を検知し、車両画像とナンバープレート画像を撮影・保存できます。警報が作動し、撮影データがアップロードされます。

開始前に

設定 → システム → システム設定 → VCA リソース に移動し、道路交通を選択します。

手順

1. 設定 → 道路交通 → 検知設定 に移動し、検知タイプとして車両検知を選択します。
2. [有効化] にチェックを入れます。
3. 車線番号を選択します。
4. 車線ラインをクリック＆ドラッグして位置を設定するか、ライン端をクリック＆ドラッグして長さと角度を調整します。
5. カメラのズーム倍率を調整し、画像内の車両サイズが赤い枠のサイズに近くなるようにします。調整可能なのは赤い枠の位置のみです。

注記

各レーンにつき、一度に1枚のナンバープレートのみを撮影できます。

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

入口/出口

車両が検知エリアを通過し、入退場時の検知をトリガーすると、検知された車両のナンバープレート情報がアップロードされます。

市街地

車両が検知エリアを通過し、市街地での検知をトリガーすると、検知された車両のナンバープレート情報がアップロードされます。

アラーム入力

入力アラームがナンバープレートの撮影および認識動作をトリガーすることを意味します。

注記

アラーム入力を選択した場合、アラーム入力A<-1が自動的に車両検知のトリガーに割り当てられ、そのアラームタイプは常にNOとなります。A<-1アラーム入力を車両検知のトリガーに使用する場合、他の基本イベントには使用できません。アラーム入力を選択して保存すると、A<-1に対して事前に設定されていた連動方法はキャンセルされます。

8. 検知モードを選択します。

9. 「重複ナンバープレート除去」にチェックを入れ、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。
-

 **注記**

最大8枚のナンバープレートに対応します。

10. 警戒スケジュールと連動方法を設定します。警戒スケジュールの設定については「[警戒スケジュールの設定](#)」を参照してください。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。

10.3.2 混合交通検知ルールの設定

設定レーンに進入する自動車、非自動車、歩行者を検知でき、対象物の画像をキャプチャして保存できます。アラームが作動し、キャプチャした画像はにアップロードされます。

開始前に

設定 → システム → システム設定 → VCA リソース に移動し、道路交通を選択します。

手順

1. 設定 → 道路交通 → 検出設定 に移動し、検出タイプとして「混合交通検出」を選択します。
2. [有効化] にチェックを入れます。
3. 車線番号を選択します。
4. 地域と国/地域を選択します。
5. 警戒スケジュールと連動方法を設定します。警戒スケジュールの設定については「[警戒スケジュールの設定](#)」を参照してください。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。

10.3.3 画像アップロード設定

車両検知および混合交通検知でキャプチャした画像の画像パラメータを設定できます。

設定 → 道路交通 → 画像 に移動します。

画質設定

値が大きいほど画像は鮮明になりますが、より大きなストレージ容量も必要となります。

画像サイズ

値が大きいほど、より多くのストレージ容量が必要となります。また、ネットワーク伝

送の要件レベルも高くなります。

ナンバープレート強調

値が大きいほどナンバープレートは鮮明になりますが、より多くのストレージ容量も必要です。

ナンバープレート強調を確認し、レベルを設定します。デフォルトレベルは50です。

オーバーレイ

撮影画像にカメラ・デバイス・車両情報を重ねて表示できます。  をクリックするとオーバーレイテキストの順序を調整できます。

カメラ設定については、[Configuration] → [→] → [Road Traffic] → [→] → [Camera] で関連パラメータを設定し、[Save] をクリックします。

10.3.4 カメラ設定

各カメラのパラメータを設定し、管理を改善できます。

設定 → Road Traffic → Camera に移動し、関連するパラメータを設定して Save をクリックします。

10.3.5 ブロックリストと許可リストのインポート/エクスポート

ブロックリストと許可リストは必要に応じてインポートおよびエクスポートでき、このインターフェースでリストの内容を確認できます。

手順

1. 「参照」をクリックしてPCのローカルディレクトリを開きます。
2. ブロックリスト&許可リストファイルを探し、クリックして選択します。「開く」をクリックして確定します。

注記

インポートするファイルは、カメラが要求するファイルテンプレートと一致している必要があります。カメラから空のブロックリスト&許可リストファイルをテンプレートとしてエクスポートし、内容を記入することをお勧めします。ファイル形式は.xls形式で、セル形式はテキストである必要があります。

-
3. 「インポート」をクリックして選択したファイルをインポートします。
 4. 「エクスポート」をクリックしてPC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ィールドにファイル名を指定します。
 7. 「保存」をクリックします。

10.4 マルチターゲットタイプ検出

マルチターゲットタイプ検出は、人間の顔、人体、車両など、複数のタイプのターゲットを検出し、データをキャプチャしてアップロードするものです。

注記

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有効にする必要があります。

10.4.1 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とアルゴリズムパラメータを設定すると、デバイスは複数のタイプのターゲットをキャプチャし、自動的に連携アクションをトリガーします。

手順

1. 設定 → マルチターゲット型検出 → ルールに移動します。
2. ルールを確認します。
3. 「○」をクリックし、ライブ画像上に検出領域を描画します。
4. テキストフィールドに最小瞳孔距離を入力するか、□をクリックして最小瞳孔距離を描画します。

最小瞳孔間距離

最小瞳孔間距離とは、2つの瞳孔間の最小距離を指し、デバイスが顔を認識するための基本条件です。

5. 警戒スケジュールを設定します。「警戒スケジュール設定」を参照してください。
6. 連動方法を設定します。「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。

次の操作

「画像」に移動し、撮影済み画像を検索・表示します。

スマートディスプレイに移動し、現在キャプチャされたターゲット画像を確認します。

10.4.2 オーバーレイとキャプチャ

キャプチャパラメータと、ストリームおよび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

ターゲットやルール情報を含むスマート情報をストリーム上に表示します。

アラーム画像にターゲット情報を表示

アラーム画像にターゲット情報をオーバーレイ表示します。

ターゲット画像設定

カスタム、ヘッドショット、上半身ショット、全身ショットから選択可能。

注記

カスタムを選択した場合、必要に応じて幅、頭の高さ、体の高さをカスタマイズできます。

固定値にチェックを入れると、画像の高さを設定できます。

背景画像設定

対象画像と比較して、背景画像は追加の環境情報を提供するシーン画像です。背景画像の品質と解像度を設定できます。監視センターに背景画像をアップロードする必要がある場合は、「背景アップロード」にチェックを入れてください。

人数カウントオーバーレイ

フローオーバーレイの種類を選択します。

日次リセット時刻を選択します。即時リセットする場合は「手動リセット」をクリックしてください。

カメラ

カメラにデバイス番号とカメラ情報を設定できます。これらは撮影画像にオーバーレイ表示されます。

テキストオーバーレイ

で、必要な項目を選択し、撮影画像に表示する順序を調整できます。

デバイス番号とカメラ情報の内容は同一ページに記載してください。

10.4.3 マルチターゲット型検出アルゴリズムのパラメータ

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

設定を行うには、[設定] → [→] → [マルチターゲットタイプ検出] → [→] → [詳細設定]に移動します。

HMSバージョン

現在のアルゴリズムバージョンを指し、編集はできません。

デフォルト値に戻す

[復元]をクリックすると、詳細設定のすべての設定が工場出荷時のデフォルト値に復元されます。

検出パラメータ

生成速度

検出領域内の対象物がターゲットであるか否かを判断する速度です。値が高いほど、ターゲットがより速く検出されます。デフォルト値が推奨されます。

感度

ターゲットを認識する感度です。値が高いほどターゲットが認識されやすくなりますが、誤検知の可能性も高くなります。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

キャプチャ閾値

撮影とアラームをトリガーする顔の品質を指します。値が高いほど、撮影とアラームをトリガーするために満たすべき品質が高くなります。

顔露出

機能を有効にすると、デバイスはシーンに人間の顔が出現した際に自動的に露出レベルを調整します。

基準輝度

顔露出モードにおける顔の基準輝度を指します。実際のシーン内の顔が設定され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。実際のシーン内の顔が設定された基準よりも暗い場合、デバイスは露出レベルを上げます。

最小持続時間

顔認識モードにおいて、顔認識レベルを維持する追加時間。

顔フィルタリング時間

カメラが顔を検出してから撮影アクションを実行するまでの時間間隔を指します。検出された顔が設定されたフィルタリング時間未満しかシーン内に留まらない場合、撮影はトリガーされません。例えば、顔フィルタリング時間が5秒に設定されている場合、カメラは顔が5秒間シーン内に留まり続けたときに検出された顔を撮影します。

10.4.4 シールド領域の設定

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

手順

1. 「シールド領域」を選択します。
2. 「」をクリックしてシールド領域を描画します。複数のシールド領域を設定する場合は、上記の手順を繰り返します。
3. オプション: 描画した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。

10.5 顔数カウント

顔検出機能は重複する顔を排除し、設定された特定のエリアに出入りした対象物の数を計算します。

注

- 特定のデバイスモデルでは、まず **VCA** リソースページで「顔カウント」を選択する必要があります。
- この機能をサポートしているのは特定のカメラモデルのみです。

10.5.1 顔検出カウント規則の設定

顔カウント検出ルールとアルゴリズムパラメータを設定すると、デバイスは自動的にターゲットをキャプチャし、連動アクションをトリガーします。

手順

- 設定 → 顔検出 → ルール に移動します。
- [Rule] にチェックを入れます。
- テキストフィールドに最小瞳孔間距離を入力するか、[□]をクリックして最小瞳孔間距離を描画します。描画した瞳孔間の距離はライブビューアのボックスに表示されます。

最小瞳孔距離

最小瞳孔距離とは、2つの瞳孔間の領域で構成される最小の正方形サイズを指し、カメラが対象を識別するための基本基準となります。

- テキストフィールドに最大瞳孔距離を入力するか、□をクリックして最大瞳孔距離を描画します。

最大瞳孔距離

最大瞳孔距離とは、2つの瞳孔間の領域で構成される最大正方形サイズを指し、カメラが対象を識別するための基本基準となります。

- 「○」をクリックして検知領域を描画します。ライブビューウィンドウで左クリックで端点を指定し、右クリックで領域描画を終了します。
- 「/」をクリックして検知ラインを描画します。矢印は進入方向を示し、「⇄」をクリックすると方向を変更できます。
 - 対象が進入方向に沿って計数エリアを通過し、検出ライン()を横切った場合、進入数としてカウントされます。
 - 対象が退出方向に沿って計数エリアを通過し、検出ラインを越えた場合、退出数としてカウントされます。
- ⒶとⒷをクリックして領域AとBを描画します。両領域が重ならないようにしてください。方向変更には⇄をクリックします。
 - 対象がA領域からB領域へ進入した場合、進入数としてカウントされます。

- ターゲットがB領域からA領域へ進入した場合、退出としてカウントされます。
8. 警戒スケジュールを設定します。「**警戒スケジュールの設定**」を参照してください。
9. 連動方式を設定します。「**連動方式設定**」を参照してください。

10.5.2 オーバーレイとキャプチャ

キャプチャパラメータと、ストリームおよび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

ターゲットやルール情報を含むスマート情報をストリーム上に表示します。

アラーム画像にターゲット情報を表示

アラーム画像にターゲット情報をオーバーレイ表示します。

ターゲット画像設定

カスタム、ヘッドショット、上半身ショット、全身ショットから選択可能。



カスタムを選択した場合、必要に応じて幅、頭の高さ、体の高さをカスタマイズできます。

固定値にチェックを入れると、画像の高さを設定できます。

背景画像設定

対象画像と比較して、背景画像は追加の環境情報を提供するシーン画像です。背景画像の品質と解像度を設定できます。監視センターに背景画像をアップロードする必要がある場合は、「**背景アップロード**」にチェックを入れてください。

人数カウントオーバーレイ

フロー オーバーレイの種類を選択します。

日次リセット時刻を選択します。即時リセットする場合は「**手動リセット**」をクリックしてください。

カメラ

カメラにデバイス番号とカメラ情報を設定できます。これらは撮影画像にオーバーレイ表示されます。

テキストオーバーレイ

で、必要な項目を選択し、撮影画像に表示する順序を調整できます。

デバイス番号とカメラ情報の内容は同一ページに記載してください。

10.5.3 顔検出アルゴリズムのパラメータ

顔検出アルゴリズムのパラメータを設定および最適化するために使用します。

注記

これらの機能は、モデルによって異なります。

顔キャプチャモード

現在のアルゴリズムバージョンを指し、編集はできません。

ベストショット

ターゲットが検知エリアを離れた後のベストショット。

キャプチャ回数

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

キャプチャ閾値

顔の品質が一定基準に達した際に撮影と警報をトリガーする閾値です。値が高いほど、トリガーに必要な品質が厳しくなります。

顔検出

デバイスは画像内で顔を検出すると、顔の明るさを調整します。

基準輝度

顔露出モードにおける顔の基準輝度。顔を検出した場合、カメラは設定した値に基づいて顔の明るさを調整します。値が高いほど、顔は明るく表示されます。

最小露光時間

カメラが顔を露出する最小時間。

注記

顔露出を有効にする場合、WDR機能が無効化され、手動アイリスが選択されていることを確認してください。

リアルタイム更新データ

有効化後、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ます。

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てください。

アルゴリズム有効性

値が高いほど対象の検出は困難になりますが、検出精度は高くなります。

デフォルト設定に戻す

[復元]をクリックすると、詳細設定のすべての設定が工場出荷時のデフォルト値に復元されます。

10.5.4 顔検出結果の表示

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「顔画像比較統計」および「人数カウント統計」領域に表示されます。

10.6 キュー管理

列に並んでいる人数と各人の待機時間を計測します。

注記

キュー管理は特定のモデルでのみサポートされています。

10.6.1 特定区域における列に並んでいる人の設定

定義された区域内の列に並んでいる人をカウントするために使用されます。アラーム閾値条件とアラームトリガーの両方が満たされた場合にアラームが作動します。

開始前に

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. [設定] → [→] → [Queue Management] に移動します。
2. 「地域別待機者」を選択します。
3. 「Add Region」をクリックし、検知エリアを描画して「Region Name」と「Alarm Interval」を設定します。複数のエリアを設定する場合は上記の手順を繰り返します。

アラーム間隔

設定したアラーム間隔中、同一タイプのアラームは通知を1回のみトリガーします。



図10-2 地域別待機列の人数設定

4. オプション: **OSD**にチェックを入れると、地域名とリアルタイムの列に並んでいる人数が表示されます。
5. アラーム閾値を設定します。アラーム閾値条件が満たされるとアラームがトリガーされます。
6. 警戒スケジュール設定については「警戒スケジュール設定」を参照。連動方法設定については「連動方法設定」を参照。
7. 「保存」をクリックします。

10.6.2 待機時間検出の設定

検知エリアに入場した各人の待機時間を計測します。警報閾値条件と警報トリガーの両方が満たされた場合に警報が作動します。

開始前に

機能を有効にするには、**VCAリソース**に移動し、**キューマネージメント**を選択します。

手順

1. [設定] → [→] → [Queue Management] に移動します。
2. 「待機時間検出」を選択します。
3. 「領域追加」をクリックし、検知領域を描画して「領域名」と「アラーム間隔」を設定します。複数の領域を設定する場合は上記手順を繰り返します。

アラーム間隔

設定したアラーム間隔中、同一タイプのアラームは1回の通知のみをトリガーします



図10-3 待機時間検出の設定

4. アラーム閾値を設定します。アラーム閾値条件が満たされるとアラームがトリガーされます。
5. 警戒スケジュール設定については「警戒スケジュール設定」を参照してください。連動方法設定については「連動方法設定」を参照してください。
6. [保存]をクリックします。
7. オプション: 設定 → ローカルで「POS情報とルールの表示」を有効にします。検知エリアと検知エリアに滞在する時間数はライブビューで確認できます。

10.6.3 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ています。

開始前に

列管理の設定については、「地域別列待ち設定」および「待機時間検出設定」を参照してください。

- 「列待ち時間分析」と「地域比較」を選択すると、異なる地域の列待ち人数を比較できます。
- 「待ち時間分析と多段階比較」を選択すると、異なる待ち時間レベルごとの待機者数を比較できます。
- 「待ち行列状態分析」と「地域比較」を選択すると、異なる地域における特定の待ち行列長が維持される時間と継続時間を比較できます。
- 「待ち行列状態分析と複数レベル比較」を選択すると、異なる待ち行列長レベルにおける待機時間と継続時間を比較できます。

手順

注記

内蔵メモリカードを装着した場合、本装置は最大1か月分のデータを保存できます。メモリカード未装着の場合、保存可能なデータは最大1週間分となります。

1. 分析モードを選択します。

待ち時間分析

待ち時間分析は、異なる待機時間レベルごとの人数を算出します。

キュー状態分析

キューの状態分析は、キューが特定の長さを維持する時間と期間を算出します。

2. 統計タイプを選択します。

地域比較

複数の地域と1つのレベルを選択して分析でき、分析チャートを作成できます。

複数レベル比較

複数のレベルと地域を選択して分析でき、地域ごとに1つの分析チャートが作成されます。

3. 1つ以上の地域を選択します。

4. キュー長レベルを設定します。必要な範囲のチェックボックスを1つ以上選択し、値を入力します。

5. レポートタイプと統計時間を指定します。

6. 「カウント」をクリックしてレポートを生成します。

10.7 カウント

特定の設定エリアへの入退場者数を計算するのに役立ちます。

注記

カウント機能は特定のモデルでのみサポートされています。

10.7.1 カウント設定

この機能は、領域への入退場するオブジェクトの計算、アラームイベントの発生、およびデータのアップロードに使用されます。

手順

1. [設定] → [→] → [カウント] に移動します。
2. 「カウントを有効化」にチェックを入れます。

3. オプション: **OSDオーバーレイを有効にする**にチェックを入れると、リアルタイムで領域に出入りする人数がライブ映像上に表示されます。

注記

オーバーレイ情報は当日の人数のみをカウントします。デバイスの再起動時または深夜0時に数値はリセットされます。手動で数値をクリアするには「0」をクリックすることも可能です。

4. 検知ラインを設定すると、ラインを越えた対象物が検知・カウントされます。



検知ラインを描画します。



検出ラインを削除します。



方向を変更します。



図10-4 カウント設定

5. 警戒スケジュール設定については「[警戒スケジュール設定](#)」を参照してください。連動方法設定については「[連動方法設定](#)」を参照してください。
6. [保存]をクリックします。

10.7.2 カウント統計情報の表示

デバイスまたはメモリカードに保存された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

まず「[カウント設定](#)」でキューマネージャーを設定してください。

手順

1. アプリケーションに移動します。
2. レポートの種類を選択してください。

3. 統計の種類を選択します。
4. 開始時間を選択します。
5. 「カウント」をクリックします。
6. オプション: エクスポートをクリックしてカウント統計をエクスポートします。
カウント統計は、表、折れ線グラフ、棒グラフで表示できます。

10.8 ヘルメット検知

この機能は、設定された監視領域内でヘルメットを着用していない対象を検出し、がアラームをトリガーします。



特定のデバイスモデルのみが本機能をサポートしています。

10.8.1 ヘルメット検知の設定

開始前に

設定 → システム → システム設定 → VCA リソース に移動し、ヘルメット検知を有効にしてください。

手順

1. [設定] → [→] → [ヘルメット検出] に移動し、[ヘルメット検出を有効にする] にチェックを入れます。
2. オプション: ターゲット生成速度を設定します。

ターゲット生成速度

これは、検出領域に入ってくる顔のターゲット生成速度を指します。値が大きいほど、生成速度は速くなります。

3. 検出領域を設定します。
 - 1) 検出領域を選択します。
 - 2) [領域を描画]をクリックし、ライブビュー画像上で領域の端点をクリックして描画します。
 - 3) 右クリックで描画を終了します。

描画停止をクリック 領域の描画を終了します。
タ

「すべてクリア」 領域を再度描画します。
をクリック

4. 警戒スケジュール設定については、「警戒スケジュール設定」を参照してください。
連動方法設定については、「連動方法設定」を参照してください。

5. 「保存」をクリックします。

10.9 顔画像比較とモデリング

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型検出または顔キャプチャを事前に有効にする必要があります。

10.9.1 顔画像比較

顔画像比較は、キャプチャされた顔画像を顔画像ライブラリ内の画像と比較することで、顔認識を実現します。

顔画像ライブラリの設定

顔画像ライブラリは、モデル化された人間の顔と情報を保存するために使用されます。

手順

1. 設定 → 顔画像ライブラリに移動します。
2. 顔画像ライブラリを作成します。
 - 1) [+]をクリックして顔画像ライブラリを追加します。
 - 2) ライブラリ名、閾値、備考を入力します。

閾値

設定した閾値を超える顔類似度の場合、顔写真比較アラームのアップロードがトリガーサれます。

- 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編集します。対象ライブラリを選択し、[⚙️]をクリックして関連パラメータを変更します。
- 5) オプション: ライブラリを削除します。対象ライブラリを選択し、[✖️]をクリックします。

3. ライブラリに顔画像を追加する。

注記

画像形式はJPEGとし、ファイルサイズは1ファイルあたり300KB以下であること。

顔写真を1枚追加

「追加」をクリックし、詳細な顔情報を含む顔写真をアップロードしてください。

顔写真を一括でインポート

[インポート]をクリックし、画像のパスを選択します。

注意

- 顔写真を一括インポートする場合、写真名が顔名として保存

されます。その他の顔情報は、手動で1つずつ修正する必要があります。

- エクスポートおよびインポート用の検証コードは、8~16桁の数字、大文字、小文字の組み合わせである必要があります。

4. オプション: 顔情報の修正

- 1) 顔写真ライブラリを選択します。
- 2) 対象の顔写真を選択します。検索機能を使用し、検索条件を入力して写真を検索し、「検索」をクリックします。
- 3) 「変更」をクリック。
- 4) 詳細情報を編集します。



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写真に対してモデルを作成します。

モデリング処理により、各顔写真に対応する顔モデルが構築されます。顔写真比較を有効にするには、顔モデルが必要です。

モデリング 1つ以上の顔写真を選択し、[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. オプション: 繰り返し操作で追加の顔ライブラリを作成します。

7. 「保存」をクリックします。

顔写真比較の設定

この機能は、撮影された画像をライブラリ内の顔画像と比較し、比較結果を出力します。比較結果は、武装スケジュールと連動方法が設定されている場合に特定のアクションをトリガーできます。

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。「顔写真ライブラリの設定」を参照してください。

手順

1. 設定 → 比較とモデリング に移動します。
2. 「顔写真比較」を選択します。

- 「顔写真比較を有効にする」にチェックを入れます。
- 参照用として顔写真ライブラリを選択します。
- アップロードする情報を選択します。
- 比較モードを選択します。

ベスト比較

対象顔が検知エリア内に留まっている間、デバイスは対象顔を継続的に撮影・比較します。対象顔がエリア外に出た際に、最もスコアの高い顔写真と関連する警報情報をアップロードします。

クイック比較

顔評価が設定された「顔評価閾値（撮影用）」を超えた時点で、対象の顔を撮影・比較します。

撮影用顔評価閾値

デバイスが顔のキャプチャとアップロードの可否を判断するための顔評価閾値。

最大撮影間隔

対象が検知エリア内にいる場合、2回のキャプチャ間の最大間隔。設定された閾値に達していないなくても、最大間隔に達した時点でカメラがキャプチャを実行します。

クイック設定モード

実際の使用シナリオに応じ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回数を設定できます。

- 警戒スケジュールを設定します。「警戒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。連動方法設定を参照。

顔写真比較結果の表示

手順

- アプリケーションに移動します。
- 検索条件を設定し、「カウント」をクリックします。
一致結果は「顔写真比較統計」エリアに表示されます。

10.9.2 顔モデリング

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

開始前に

顔画像収集には、顔キャプチャまたはマルチターゲット型検出の設定が必要です。設定手順については「顔キャプチャまたはマルチターゲット型検出」を参照してください。

手順

- 設定 → → → 比較とモデリングに移動します。

2. 「顔モデリング」を選択して開始します。
3. 「フェイスモデリングを有効にする」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警報における顔モデリング情報の報告

人物がマルチターゲット型検出をトリガーした場合、アラーム情報にはチェックされている場合に限り、検出された顔の顔モデリング情報が含まれます。

クイックキャプチャ

デバイスは、設定された顔評価閾値を超えるスコアの顔を検出した際に、顔モデリングを開始します。

顔キャプチャ評価閾値

デバイスが顔のキャプチャとアップロードの可否を判断するための顔評価閾値。値が高いほど画質が優れていることを示す。

最大撮影間隔

対象が検知エリア内にいる場合、2回のキャプチャ間の最大間隔。設定された閾値（）に達していなくても、最大間隔に達した時点でカメラはキャプチャを実行します。

5. 警戒スケジュールを設定します。「警戒スケジュール設定」を参照してください。
6. 連動方法の設定。[連動方法設定](#)を参照。

第11章 オープンプラットフォーム

オープンプラットフォームにより、サードパーティが機能やサービスを開発・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。

注記

特定のデバイスモデルのみが本機能をサポートします。

11.1 オープンプラットフォームの設定

手順

1. [設定] → [→] → [Open Platform] に移動します。

注意

アプリケーションをインストールする前に、下部の免責事項をお読みいただき、インストールしたい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には固有の名前があります。
- アプリケーションが占有するフラッシュメモリ容量が、デバイスの利用可能なフラッシュメモリ容量を下回っていること。
- アプリケーションのメモリおよび演算能力は、デバイスの利用可能なメモリおよび演算能力よりも小さい。

2. 「アプリインストール」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。

インストールされたアプリケーションとその関連情報（アプリケーション名、操作、バージョン、使用メモリ、使用フラッシュ、会社、ステータス、ライセンスなど）がアプリケーションリストに表示されます。

4. オプション：アプリケーションを設定します。



ログをエクスポートします。



権限を設定します。



アプリケーションを削除します。



アプリケーションの有効化または無効化。

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、キャプチャした画像を表示できます。

レイアウトレビュー

クリックして「レイアウトレビュー」を選択します。必要に応じて内容を選択します。リアルタイム分析を選択した場合、リアルタイム分析専用コンテンツのみを選択できます。

検出属性

クリックして「検出属性」を選択します。この機能を有効にすると、対象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の設定

EPTZ（電子 PTZ）は、物理的なカメラの動きを伴わずに、画像の一部をデジタルでズームおよびパンする高解像度機能です。

開始前に

EPTZ機能を使用するには、ライブビューで「第四ストリーム」を選択していることを確認してください。第四ストリームとEPTZは同時に有効にする必要があります。

13.1 パトロール

手順

1. 設定 → EPTZ に移動します。
2. 「EPTZを有効にする」にチェックを入れます。
3. 「第四ストリーム」にチェックを入れます。
4. アプリケーションで「パトロール」を選択します。
5. 「保存」をクリックします。

次の手順

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

13.2 オートトラッキング

手順

1. 「設定」→「」→「EPTZ」に移動します。
2. 「EPTZを有効にする」にチェックを入れます。
3. 「第四ストリーム」にチェックを入れます。
4. アプリケーションで「自動追跡」を選択します。
5. 「検出領域」をクリックして描画を開始します。
6. ライブ映像をクリックして検知領域の四つの頂点を指定し、右クリックで描画を完了します。
7. ルールを設定します。

検出対象

人物と車両が選択可能です。検出対象が選択されていない場合、人物と車両を含むすべての検出対象が追跡されます。



特定のカメラモデルのみが本機能をサポートします。

感度

これは、追跡可能な対象の身体部位が追跡される割合を表します。感度 = $100 - S1/ST \times 100$ 。S1は事前定義領域に進入した対象の身体部位、STは対象の身体全体を表します。感度の値が高いほど、対象はより容易に追跡されます。

8. [保存]をクリックします。

第14章 パターンリンク

パターンリンク設定後、デバイスは異なるチャネルから取得した顔と人体の情報を関連付けられます。

注

この機能はマルチチャンネルデバイスでのみサポートされます。

14.1 パターンリンクの設定

パターンリンク設定後、デバイスは異なるチャネルから取得した顔、人体、車両情報をリンクできます。

開始前に

スイッチスマートモードを参照し、パターンモードを確認してください。

手順

1. 設定 → → パターンリンク → → キャリブレーション に移動します。
2. 「ポイント追加」をクリックし、カメラ1のポイントを画像内の基準点に移動させ、カメラ2の同番号ポイントを対応する基準点に移動させます。

ポイント削除	選択したポイントをすべて削除します。
すべてクリア	すべてのポイントを削除します。
3. 手順2を繰り返し、追加したポイントを異なる基準点に移動します。少なくとも12個のキャリブレーションポイントを追加することを推奨します。

注記

- ポイントは分散配置し、3/4ポイントが1直線上にならないようにしてください。
 - 本装置は4~64個のキャリブレーションポイントに対応しています。
4. 「パリティ」をクリックし、カメラ1とカメラ2のポイントが同一基準位置にあるか確認します。異なる場合はポイントを調整するか、再キャリブレーションを行ってください。
 - チャンネル2とチャンネル1が同じ基準点にある場合、キャリブレーションは成功です。
 - チャンネル2とチャンネル1が同じ基準点にない場合、キャリブレーションは失敗です。ステップ2を繰り返し、ポイントを調整するか、再度キャリブレーションを行ってください。

5. 「ルール」をクリックし、「パターンリンクを有効にする」をチェックします。
6. 「保存」をクリックします。



UD22027B-F