デジタルビデオレコーダー

ユーザーマニュアル

法的情報

このマニュアルについて

このユーザーマニュアルには、本製品の使用および管理方法に関する説明が記載されています。以下、写真、図表、画像、その他すべての情報は、説明および解説のためのものです。本書に記載されている内容は、ファームウェアのアップデートなどにより、予告なく変更されることがあります。このユーザーマニュアルの最新版は、Hikvision のウェブサイト (***https://www.hikvision.com/***) をご覧ください。
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を受けながら、本マニュアルを使用してください。

商標について

HIKVISION およびその他の Hikvision の商標およびロゴは、さまざまな管轄区域における Hikvision の財産です。
その他、記載されている商標およびロゴは、それぞれの所有者の財産です。
HDMI™ および HDMI High-Definition Multimedia Interface の用語、ならびに HDMI ロゴは、米国およびその他の国における HDMI Licensing Administrator, Inc. の商標または登録商標です。

免責事項

適用される法律が許す最大限の範囲において、本マニュアルおよび記載された製品、そのハードウェア、ソフトウェア、ファームウェアは、「有りのまま」かつ「すべての欠陥および誤りを含む」状態で提供されています。Hikvision は、商品性、満足のいく品質、特定目的への適合性を含むがこれに限定されない、明示または黙示の保証を一切行いません。本製品の使用は、お客様ご自身の責任において行われるものとします。Hikvision がそのような損害や損失の可能性を知らされていたとしても、本製品の使用に関連し、特に事業利益の損失、事業の中断、またはデータの損失、システムの破損、文書の損失に対する損害など、契約違反、不法行為（過失を含む）、製品責任、またはその他のいずれに基づいても、いかなる特別、必然、付随的、間接損害についても、Hikvision がお客様に責任を負うことはないものとします。
お客様は、インターネットの性質上、固有のセキュリティリスクがあることを認め、Hikvision はサイバー攻撃、ハッカー攻撃、ウイルス感染、またはその他のインターネットセキュリティリスクに起因する異常動作、プライバシー漏洩またはその他の損害について一切の責任を負いません。ただし、Hikvision は必要に応じて適時に技術サポートを提供します。
お客様は、本製品をすべての適用法に従って使用することに同意し、お客様の使用が適用法に適合していることを確認する責任を負うものとします。特に、お客様は、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第三者の権利を侵害しない方法で本製品を使用する責任を負うものとします。お客様は、本製品を、大量破壊兵器の開発または製造、化学兵器または生物兵器の開発または製造、核爆発物または安全でない核燃料サイクルに関連する活動、あるいは人権侵害の支援を含む、禁止された最終用途に使用してはならないものとします。
本書と適用される法律の間に矛盾がある場合、後者が優先されます。

法規制情報

FCC 情報

コンプライアンスの責任ある当事者によって明示的に承認されていない変更または改造は、機器を操作するユーザーの権限を無効にする可能性があることに留意してください。
FCC 対応：この装置は、FCC 規則のパート 15 に従って、クラス A デジタルデバイスの制限に準拠していることが試験により確認されています。これらの制限は、住宅用設備の有害な干渉に対して適切に保護するように設計されています。本機は、無線周波エネルギーを発生、使用、放射することがあり、指示に従わずに設置、使用した場合、無線通信に有害な干渉を引き起こす可能性があります。ただし、特定の設置場所において干渉が発生しないことを保証するものではありません。本機がラジオやテレビの受信に有害な干渉を引き起こす場合（装置の電源を切ったり入れたりすることで判断できます）、ユーザーは以下の手段の 1 つ以上によって干渉を修正するよう試みることが推奨されます。

- 受信アンテナの向きや位置を変えてみる。
- 機器と受信機の距離を離してみる。
- 受信機が接続されている回路とは別の回路のコンセントに機器を接続してみる。
- 販売店または経験豊富なラジオ / テレビ技術者に相談してみる。

FCC 条件
本機は FCC 規則パート 15 に適合しています。動作は次の 2 つの条件を満たす必要があります。

- 本機は有害な干渉を引き起こすことはありません。
- 本機は、望ましくない動作を引き起こす可能性のある干渉を含め、受信したすべての干渉を受け入れる必要があります。

EU 適合宣言

CE

本機および付属品には "CE" のマークがあり、EMC 指令 2014/30/EU、LVD 指令 2014/35/EU、RoHS 指令 2011/65/EU に基づく欧州規格に適合しています。

2012/19/EU（WEEE 指令）。このマークがついた製品は、EU 圏内では未分別の一般廃棄物として処理することができません。本機を適切にリサイクルするために、同等の新品を購入する際に地域の販売店に本機を返却するか、指定された回収場所に廃棄してください。詳しくはこちらをご覧ください。
http://www.recyclethis.info.

2006/66/EC（電池指令）：本機には、欧州連合で未分別の一般廃棄物として処理できない電池が含まれています。具体的な電池の情報については、製品の説明書を参照してください。電池にはこのマークが表示され、カドミウム（Cd）、鉛（Pb）、水銀（Hg）を示す文字が含まれている場合があります。適切なリサイクルのために、電池は購入先または指定された回収場所に出してください。詳しくはこちらをご覧ください。***http://www.recyclethis.info.***

カナダ ICES-003 準拠

本機は CAN ICES-3 (A)/NMB-3 (A) 規格の要求事項を満たしています。

適用機種

このマニュアルは、以下の機種に適用されます。

表 1-1 適用機種

シリーズ	モデル
DS-7200HGHI-K1	DS-7216HGHI-K1
DS-7200HGHI-K2	DS-7216HGHI-K2
	DS-7224HGHI-K2
	DS-7232HGHI-K2
DS-7100HQHI-K1	DS-7104HQHI-K1
	DS-7108HQHI-K1
	DS-7116HQHI-K1
DS-7200HQHI-K1	DS-7204HQHI-K1
	DS-7208HQHI-K1
	DS-7216HQHI-K1
DS-7200HQHI-K1/SSD	DS-7204HQHI-K1/SSD(512G)
	DS-7204HQHI-K1/SSD(1T)
DS-7200HQHI-K2	DS-7208HQHI-K2
	DS-7216HQHI-K2
	DS-7224HQHI-K2
	DS-7232HQHI-K2
DS-7200HQHI-K/P	DS-7204HQHI-K1/P
	DS-7208HQHI-K2/P
	DS-7216HQHI-K2/P
DS-7300HQHI-K4	DS-7304HQHI-K4
	DS-7308HQHI-K4
	DS-7316HQHI-K4
	DS-7324HQHI-K4
	DS-7332HQHI-K4
DS-8100HQHI-K8	DS-8124HQHI-K8
	DS-8132HQHI-K8

シリーズ	モデル
DS-7200HUHI-K1	DS-7204HUHI-K1
	DS-7208HUHI-K1
DS-7200HUHI-K1/E	DS-7204HUHI-K1/E
	DS-7208HUHI-K1/E
DS-7200HUHI-K2	DS-7204HUHI-K2
	DS-7208HUHI-K2
	DS-7216HUHI-K2
DS-7200HUHI-K2/SSD	DS-7208HUHI-K2/SSD
DS-7200HUHI-K/P	DS-7204HUHI-K1/P
	DS-7208HUHI-K2/P
	DS-7216HUHI-K2/P
DS-7300HUHI-K4	DS-7304HUHI-K4
	DS-7308HUHI-K4
	DS-7316HUHI-K4
	DS-7324HUHI-K4
	DS-7332HUHI-K4
DS-8100HUHI-K8	DS-8108HUHI-K8
	DS-8116HUHI-K8
	DS-8124HUHI-K8
	DS-8132HUHI-K8
DS-9000HUHI-K8	DS-9008HUHI-K8
	DS-9016HUHI-K8
	DS-9024HUHI-K8
	DS-9032HUHI-K8
DS-7200HTHI-K1	DS-7204HTHI-K1
DS-7200HTHI-K2	DS-7204HTHI-K2
	DS-7208HTHI-K2
DS-7200HTHI-K2/SSD	DS-7204HTHI-K2/SSD
DS-7300HTHI-K4	DS-7316HTHI-K4
DS-8100HTHI-K8	DS-8116HTHI-K8

シリーズ	モデル
DS-9000HTHI-K8	DS-9016HTHI-K8
iDS-7200HQHI-K1/2S	iDS-7204HQHI-K1/2S
iDS-7200HQHI-K/4S	iDS-7208HQHI-K1/4S
iDS-7200HQHI-K/4S	iDS-7216HQHI-K1/4S
	iDS-7208HQHI-K2/4S
	iDS-7216HQHI-K2/4S
iDS-7200HQHI-K1/S(B)	iDS-7204HQHI-K1/2S(B)
	iDS-7208HQHI-K1/4S(B)
	iDS-7216HQHI-K1/4S(B)
iDS-7200HQHI-K2/4S(B)	iDS-7208HQHI-K2/4S(B)
	iDS-7216HQHI-K2/4S(B)
iDS-7200HUHI-K/4S	iDS-7204HUHI-K1/4S
	iDS-7208HUHI-K1/4S
	iDS-7204HUHI-K2/4S
	iDS-7208HUHI-K2/4S
iDS-7200HUHI-K/4S(B)	iDS-7204HUHI-K1/4S(B)
	iDS-7208HUHI-K1/4S(B)
	iDS-7204HUHI-K2/4S(B)
	iDS-7208HUHI-K2/4S(B)
iDS-7300HUHI-K4/16S	iDS-7316HUHI-K4/16S
iDS-9000HUHI-K8/16S	iDS-9016HUHI-K8/16S
iDS-7200HQHI-M1/S	iDS-7204HQHI-M1/S
	iDS-7208HQHI-M1/S
	iDS-7216HQHI-M1/S
iDS-7200HQHI-M1/FA	iDS-7204HQHI-M1/FA
	iDS-7208HQHI-M1/FA
	iDS-7216HQHI-M1/FA
iDS-7200HQHI-M2/S	iDS-7208HQHI-M2/S
	iDS-7216HQHI-M2/S
	iDS-7232HQHI-M2/S

シリーズ	モデル
iDS-7200HQHI-M2/FA	iDS-7208HQHI-M2/FA
	iDS-7216HQHI-M2/FA
iDS-7200HUHI-M1/S	iDS-7204HUHI-M1/S
	iDS-7208HUHI-M1/S
iDS-7200HUHI-M1/FA	iDS-7204HUHI-M1/FA
	iDS-7208HUHI-M1/FA
iDS-7200HUHI-M2/S	iDS-7204HUHI-M2/S
	iDS-7208HUHI-M2/S
	iDS-7216HUHI-M2/S
iDS-7200HUHI-M2/FA	iDS-7204HUHI-M2/FA
	iDS-7208HUHI-M2/FA
iDS-7300HQHI-M4/S	iDS-7316HQHI-M4/S
iDS-8100HQHI-M8/S	iDS-8116HQHI-M8/S

記号について

本書で使用する記号は、次のように定義されています。

シンボルマーク	説明
危険	この表示を無視して誤った取り扱いをすると、人が死亡または重傷を負う可能性が想定される状況を示しています。
注意	この表示を無視して誤った取り扱いをすると、機器の損傷、データの損失、パフォーマンスの低下、または予期しない結果につながる可能性があり、潜在的に危険な状況を示します。
メモ	本文の重要なポイントを強調または補足するための追加情報です。

安全上のご注意

- すべてのパスワードおよびその他のセキュリティセッティングの適切な設定は、設置者および / またはエンドユーザーの責任です。
- 本製品の使用にあたっては、国や地域の電気安全に関する規制を厳守してください。
- プラグをコンセントにしっかりと差し込んでください。1 つの電源アダプターに複数の機器を接続しないでください。アクセサリーや周辺機器を接続したり取り外したりする前に、本機の電源を切ってください。
- 感電事故：メンテナンスの前に、すべての電源を切断してください。
- 本機は必ず接地されたコンセントに接続してください。
- コンセントは機器の近くに設置し、容易にアクセスできるようにしてください。
- ϟ は危険物であることを示し、端子に接続された外部配線は、指導を受けた人が設置する必要があります。
- 本機を不安定な場所には絶対に設置しないでください。機器が落下して、重大な人身事故や死亡事故を引き起こす可能性があります。
- 入力電圧は IEC62368 の SELV（安全特別低電圧）および LPS（制限電圧）を満たす必要があります。
- 高い保護導体電流を実現 ! 電源に接続する前にアースに接続してください。
- 本機から万一、煙やにおい、異音がしたらすぐに電源を切り、電源ケーブルを抜いて、サービスセンターへご連絡ください。
- UPS と併用し、HDD はなるべく工場出荷時の推奨品を使用してください。
- 本機には、コイン / ボタン電池が使用されています。電池を飲み込むと、わずか 2 時間で体内に重度の火傷を負い、死に至る可能性があります。
- 本機は、子供がいる可能性のある場所での使用には適していません。
- 注意：異なる種類の電池と交換した場合、爆発する危険性があります。
- 異なる種類の電池と交換すると、安全装置が無効になることがあります（例：一部のリチウム電池の場合）。
- バッテリーを火や高温のオーブンに入れたり、機械的に押しつぶしたり、切断したりすると、爆発する恐れがあります。
- 爆発や引火性液体・気体の漏洩の恐れがあるため、極端に高温の場所に電池を放置しないでください。
- 電池を極端に低い気圧の場所に置くと、爆発したり、可燃性の液体やガスが漏れたりすることがありますのでご注意ください。
- 使用済みの電池は、説明書に従って廃棄してください。
- ファンブレードやモーターに体の一部を近づけないでください。修理の際は、電源を切ってください。
- モーターに近づかないでください。修理の際は、電源を切ってください。

予防と注意点

機器を接続し操作する前に、以下の注意事項をご確認ください。

- 本機は屋内専用です。風通しがよく、ほこりのない、液体のない環境に設置してください。
- レコーダーがラックや棚に正しく固定されていることを確認してください。落下などにより大きな衝撃を受けると、レコーダー内の精密電子機器を破損させる原因となります。
- 機器に水滴や水がかからないようにしてください。また、花瓶など、液体の入った物を機器の上に置かないでください。
- ろうそくなどの火を機器の上に置かないでください。
- 新聞紙、テーブルクロス、カーテンなどで換気口を覆い、換気を妨げないでください。ベッド、ソファー、敷物などの上に機器を置いて開口部を塞がないでください。
- 一部の機種では、AC 電源に接続するための端子が正しく配線されていることを確認してください。
- 一部の機種では、IT 配電システムへの接続を前提に設計されており、必要に応じて変更されています。
-  は、電池ホルダ自体の識別と、電池ホルダ内のセルの位置の識別を行います。
- ＋は直流を使用する、あるいは直流を発生する機器のプラス端子を特定します。－は直流電流を使用する機器、または直流電流を発生する機器のマイナス端子を識別します。
- 十分な換気のために、本機の周囲には 200mm 以上の間隔を空けてください。
- 一部の機種では、AC 電源に接続するための端子が正しく配線されていることを確認してください。
- 取扱説明書または使用説明書に記載されている電源のみを使用してください。
- 本機の USB ポートは、マウス、キーボード、USB メモリー、Wi-Fi ドングルの接続にのみ使用します。
- 取扱説明書または使用説明書に記載されている電源のみを使用してください。
- 鋭利な刃物や角には触れないようにしてください。
- 本機が 45℃以上で動作している場合、または S.M.A.R.T. の HDD 温度が記載値を超えている場合は、本機を涼しい環境で動作させるか、HDD を交換して S.M.A.R.T. の HDD 温度を記載値以下にするようにしてください。

目次

第 1 章 基本操作 1
1.1 本機の起動 1
1.1.1 工場出荷時のユーザーと IP アドレス 1
1.1.2 ローカルメニューで起動する 1
1.1.3 SADP 経由で起動する 2
1.1.4 クライアントソフトウェアで起動する 3
1.1.5 Web ブラウザーで起動する 7
1.2 TCP/IP の設定 7
1.3 HDD の設定 9
1.4 信号入力の設定 9
1.5 エンハンスド IP モードの設定 9
1.6 PoC カメラの接続 10
1.7 ネットワークカメラの追加 11
1.7.1 自動検索されたオンラインネットワークカメラを追加する 12
1.7.2 ネットワークカメラを手動で追加する 12
1.7.3 カスタマイズされたプロトコル経由でネットワークカメラを追加する 14
1.8 5MP 長距離伝送の設定 15
1.9 プラットフォームへの接続 15
1.9.1 Hik-Connect を設定する 15
1.9.2 ISUP を設定する 17
第 2 章 カメラの設定 19
2.1 画像パラメータの設定 19
2.2 OSD の設定 19
2.3 プライバシーマスクの設定 20
2.4 IP カメラの設定ファイルのインポート / エクスポート 22
2.5 IP カメラの時刻同期 22
2.6 カメラ VCA データの保存 22
2.7 IP カメラのアップグレード 23

第 3 章 ライブビュー 24
3.1 ライブビューの開始 24
3.1.1 ライブビューを設定する 24
3.1.2 カメラの自動切替えを設定する 25
3.1.3 ライブビューレイアウトを設定する 26
3.1.4 チャンネルゼロエンコーディングの設定 27
3.1.5 補助モニターを使用する 28
3.2 デジタルズーム 29
3.3 ライブビューストラテジー 29
3.4 3D ポジショニング 30
3.5 顔認識 30
3.6 PTZ コントロール 33
3.6.1 PTZ パラメーターを設定する 33
3.6.2 プリセットを設定する 34
3.6.3 プリセットを呼び出す 35
3.6.4 パトロールを設定する 35
3.6.5 パトロールを呼び出す 38
3.6.6 パターンを設定する 38
3.6.7 パターンを呼び出す 39
3.6.8 リニアスキャンリミットの設定 39
3.6.9 ワンタッチパーク 40
3.6.10 補助機能 41
第 4 章 録画と再生 42
4.1 録画 42
4.1.1 録画パラメーターを設定する 42
4.1.2 H.265 ストリームアクセスを有効にする 44
4.1.3 手動で録画する 44
4.1.4 録画スケジュールを設定する 44
4.1.5 連続録画の設定する 46
4.1.6 動体検知トリガー録画の設定 46
4.1.7 イベントトリガー録画の設定 46
4.1.8 アラームトリガー録画の設定 47

4.1.9 画像キャプチャーの設定 47
4.1.10 休日録画を設定する 47
4.1.11 録画とキャプチャーの冗長化設定 48
4.1.12 1080p Lite モードの設定 49
4.2 再生 50
4.2.1 インスタント再生 50
4.2.2 通常の動画を再生する 50
4.2.3 スマート検索された動画を再生する 51
4.2.4 カスタム検索されたファイルを再生する 52
4.2.5 タグファイルを再生する 52
4.2.6 サブピリオドで再生する 54
4.2.7 ログファイルを再生する 54
4.2.8 外部ファイルを再生する 55
4.3 再生操作 56
4.3.1 ノーマル / スマート / カスタム動画 56
4.3.2 重要 / カスタムモードでのプレイストラテジーの設定 56
4.3.3 ビデオクリップを編集する 56
4.3.4 メインストリームとサブストリームの切り替え 57
4.3.5 サムネイルビュー 57
4.3.6 早送り 57
4.3.7 デジタルズーム 58
第 5 章 スマート解析 59
5.1 エンジン設定 59
5.2 タスク設定 60
5.3 エンハンスド VCA モードの設定 61
5.4 顔画像比較 61
5.4.1 顔検知 61
5.4.2 顔画像ライブラリー管理 62
5.4.3 顔画像比較の設定 63
5.4.4 顔画像検索 65

5.5 ペリメータープロテクション 68
5.5.1 侵入検知 68
5.5.2 ラインクロッシング検知 70
5.5.3 領域入口検知 71
5.5.4 領域出口検知 72
5.6 人体検知 73
5.6.1 人体検知 73
5.6.2 人体検索 74
5.7 動体検知 76
5.8 車両検知 77
5.8.1 車両検知の設定 77
5.8.2 車両検索 77
5.9 ターゲット検知 78
5.10 人数カウント統計の表示 79
5.11 ヒートマップ 79
第 6 章 イベント 81
6.1 通常イベントアラーム 81
6.1.1 ビデオロスアラームを設定する 81
6.1.2 ビデオタンパリングアラームの設定 81
6.1.3 センサーのアラームを設定する 81
6.1.4 異常アラームを設定する 82
6.2 VCA イベントアラーム 83
6.2.1 置き去り検知 83
6.2.2 持ち去り検知 84
6.2.3 音声異常検知 85
6.2.4 デフォーカス検知 86
6.2.5 突発的なシーンチェンジ検知 88
6.2.6 PIR アラーム 89
6.3 アーミングスケジュールの設定 90
6.4 リンケージアクションの設定 91
6.4.1 フルスクリーンモニタリング自動切換えを設定する 91
6.4.2 ブザーを設定する 91

6.4.3 サーベイランスセンターへ通知する 92
6.4.4 メールリンケージを設定する 92
6.4.5 アラーム出力を作動する 92
6.4.6 PTZ リンケージを設定する 93
6.4.7 オーディオとライトアラームリンケージを設定する 93
第 7 章 ファイル管理 94
7.1 ファイル検索 94
7.2 ファイルのエクスポート 94
7.3 スマートサーチ 94
第 8 章 POS 設定 95
8.1 POS 接続の設定 95
8.2 POS テキストオーバーレイの設定 99
8.3 POS アラームの設定 100
第 9 章 ストレージ 101
9.1 ストレージデバイスの管理 101
9.1.1 ローカル HDD を管理する 101
9.1.2 ネットワークディスクを追加する 104
9.1.3 eSATA を管理する 105
9.2 ディスクアレイ 106
9.2.1 ディスクアレイを作成する 107
9.2.2 アレイを再構築する 109
第 10 章 ネットワーク設定 112
10.1 DDNS の設定 112
10.2 PPPoE の設定 112
10.3 ポートマッピング (NAT) の設定 113
10.4 Wi-Fi の設定 114
10.5 SNMP の設定 116
10.6 電子メールの設定 117
10.7 ポートの設定 118
10.8 ONVIF の設定 120

第 11 章 ユーザー管理とセキュリティ 121
11.1 ユーザーアカウントの管理 121
11.1.1 ユーザーを追加する 121
11.1.2 管理者ユーザーを編集する 122
11.1.3 Operator/Guest User を編集する 123
11.2 ユーザー権限の管理 124
11.2.1 ユーザー権限を設定する 124
11.2.2 ロック画面のライブビューの権限を設定する 127
11.3 パスワードセキュリティの設定 128
11.3.1 GUID ファイルをエクスポートする 128
11.3.2 セキュリティに関する質問を設定する 129
11.3.3 予約メールの設定 130
11.4 パスワードのリセット 131
11.4.1 GUID でパスワードをリセットする 131
11.4.2 セキュリティ質問でパスワードをリセットする 132
11.4.3 Hik-Connect でパスワードをリセットする 132
11.4.4 予約メールでパスワードをリセットする 133
第 12 章 システム管理 134
12.1 デバイスの設定 134
12.2 時間の設定 135
12.2.1 手動時刻同期 135
12.2.2 NTP を同期する 135
12.2.3 DST を同期する 135
12.3 ネットワークの検知 136
12.3.1 ネットワークトラフィックをモニタリングする 136
12.3.2 ネットワーク遅延とパケットロスをテストする 137
12.3.3 ネットワークパケットをエクスポートする 137
12.3.4 ネットワークリソースの統計情報 138
12.4 ストレージデバイスのメンテナンス 138
12.4.1 不良セクターを検知する 138
12.4.2 S.M.A.R.T. 検知 139
12.4.3 HDD のヘルスステータス検知 140

12.4.4 ディスククローンを設定する 141
12.4.5 データベースを修復する 142
12.5 本機のアップグレード 142
12.5.1 ローカルバックアップデバイスによるアップグレード 142
12.5.2 FTP によるアップグレード 143
12.5.3 Web ブラウザーによるアップグレード 144
12.5.4 Hik-Connect によるアップグレード 144
12.6 機器設定ファイルのインポート / エクスポート 144
12.7 ログの管理 145
12.7.1 ログを保存する 145
12.7.2 ログファイルの検索とエキスポート 146
12.7.3 サーバーへログをアップロードする 147
12.7.4 一方向認証 148
12.7.5 双方向認証 148
12.8 初期設定への復元 149
12.9 セキュリティ管理 150
12.9.1 ONVIF を設定する 150
12.9.2 IP/MAC アドレスフィルター 151
12.9.3 RTSP 認証 152
12.9.4 RTSP ダイジェストアルゴリズム 152
12.9.5 ISAPI サービス 152
12.9.6 HTTP 認証 153
12.9.7 HTTP/ ウェブダイジェストアルゴリズム 153
12.9.8 画像 URL ダイジェスト認証 153
12.9.9 SADP サービスの無効化 153
第 13 章 付録 154
13.1 適用可能な電源アダプターのリスト 154
13.2 用語集 154
13.3 通信マトリクス 156
13.4 デバイスコマンド 156

13.5 よくある質問 157

13.5.1 マルチ画面ライブビューで、一部のチャンネルが「No Resource」と表示されたり、画面が黒くなったりするのはなぜですか？ 157

13.5.2 ネットワークカメラを追加した後、ビデオレコーダーが危険なパスワードを通知するのはなぜですか？ 157

13.5.3 ビデオレコーダーがストリームの種類をサポートしていないと通知するのはなぜですか？ 158

13.5.4 再生画質を向上させる方法は？ 158

13.5.5 アナログチャンネルのライブビューに「NO VIDEO」が表示されるのはなぜですか？ 158

13.5.6 ビデオレコーダーが H.265 で画像を録画していることを確認する方法は？ 158

13.5.7 再生時のタイムラインが一定でないのはなぜですか？ 159

13.5.8 ネットワークカメラの追加時に、ビデオレコーダーがネットワークに到達できないことを通知するのはなぜですか？ 159

13.5.9 ネットワークカメラの IP アドレスが自動的に変更されるのはなぜですか？ 159

13.5.10 ビデオレコーダーが IP 競合を通知しているのはなぜですか？ 159

13.5.11 シングルまたはマルチチャネルのカメラで再生すると、画像が固まるのですが？ 160

13.5.12 ビデオレコーダーが起動すると、ビープ音が鳴るのですが？ 160

13.5.13 動体検知を設定しても、録画された動画がないのはなぜですか？ 160

13.5.14 PTZ カメラをコアキトロン経由で制御できないのはなぜですか？ 161

13.5.15 RS-485 経由で PTZ が応答しないように見えるのはなぜですか？ 161

13.5.16 動画の音質が良くないのですが？ 161

第 1 章 基本操作

1.1 本機の起動

1.1.1 工場出荷時のユーザーと IP アドレス

- 工場出荷時の管理者アカウント：admin
- 工場出荷時の IPv4 アドレス：192.168.1.64.

1.1.2 ローカルメニューで起動する

初回アクセス時には、管理者パスワードを設定し、本機を起動する必要があります。起動前には操作はできません。また、Web ブラウザー、SADP、クライアントソフトウェアを使用して起動することもできます。

ステップ

1. 管理者パスワードを 2 回入力する。

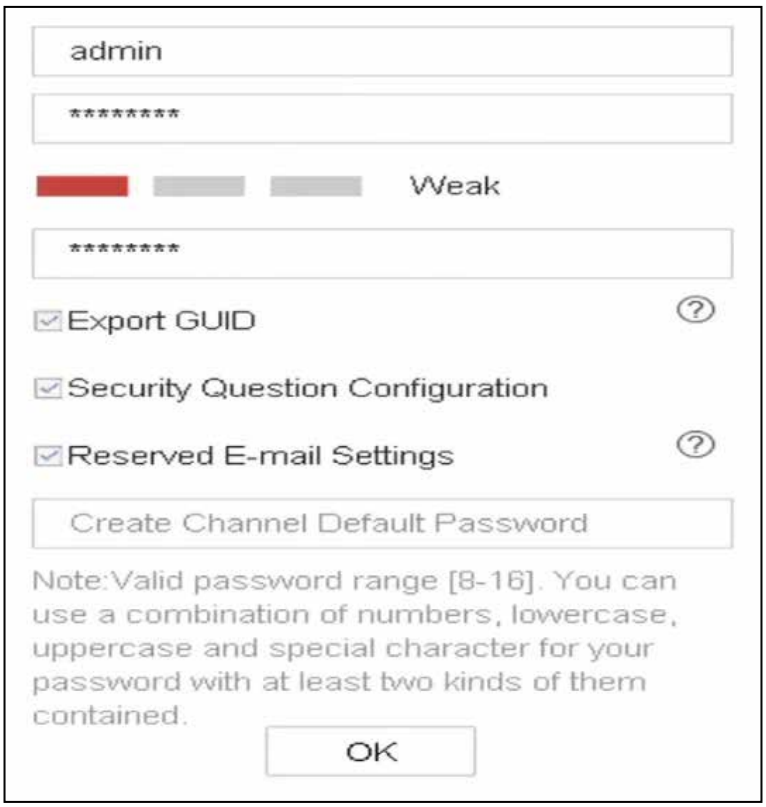


図 1-1 ローカルメニューで起動する

警告

製品の安全性を高めるため、お客様ご自身で強力なパスワード（8 文字以上、大文字、小文字、数字、特殊文字の 3 種類以上）を設定することを強くお勧めします。また、定期的にパスワードをリセットすることをお勧めします。特にセキュリティの高いシステムでは、毎月または毎週パスワードをリセットすることで、製品をより安全に保護することができます。

2. IP カメラを起動するためのパスワードを入力します。
3. オプション：**Export GUID**、**Security Question Configuration**、**Reserved E-mail Settings** のいずれかにチェックを入れます。
4. **OK** ボタンをクリックします。

メモ

- 本機の起動後は、パスワードを適切に保管しておく必要があります。
- デフォルトプロトコルで接続されている IP カメラに、パスワードを複製することができます。
- 機種により、利用できるパスワード再設定機能が異なる場合があります。

次は

- **Export GUID** を有効にした場合、今後のパスワード再設定のために、引き続き GUID ファイルを USB フラッシュドライバにエクスポートしてください。
- **Security Question Configuration** を有効にした場合、今後のパスワードの再設定を行うために、引き続きセキュリティ質問を設定します。
- **Reserved E-mail Settings** を有効にした場合、今後の予約メールの再設定を行うために、引き続きセキュリティ質問を設定します。

1.1.3 SADP 経由で起動する

SADP ソフトウェアは、オンライン機器の検出、本機の起動、パスワードのリセットに使用されます。

ご使用の前に

付属のディスクまたは公式ホームページから SADP ソフトウェアを入手し、画面の指示に従って SADP をインストールしてください。

ステップ

1. 本機の電源をコンセントに接続し、電源を入れてください。
2. SADP ソフトを起動して、オンラインレコーダの検索を行ってください。
3. デバイスリストから本機のステータスにチェックを入れ、非アクティブのレコーダーを選択してください。

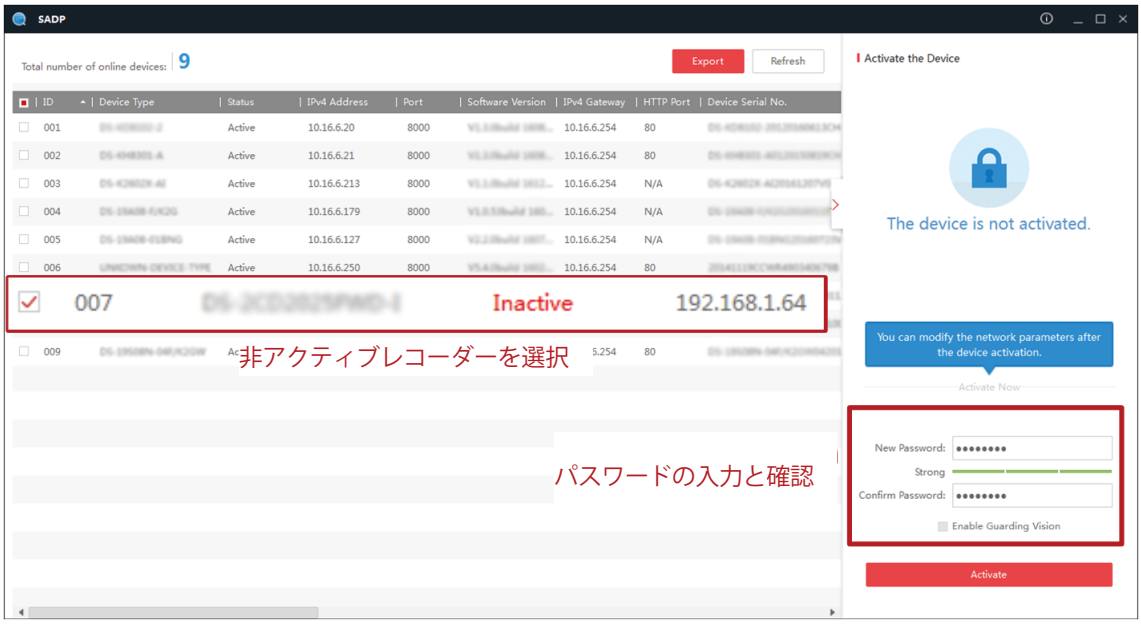


図 1-2 SADP による起動

4. 新しいパスワードを作成してパスワード欄に入力し、入力したパスワードを確認してください。

メモ

製品の安全性を高めるため、お客様ご自身で強力なパスワード（8 文字以上、大文字、小文字、数字、特殊文字の 3 種類以上）を設定することを強くお勧めします。また、定期的にパスワードをリセットすることをお勧めします。特にセキュリティの高いシステムでは、毎月または毎週パスワードをリセットすることで、製品をより安全に保護することができます。

5. **Activate** をクリックしてください。

1.1.4 クライアントソフトウェアで起動する

クライアントソフトウェアは、複数の種類のデバイスに対応する汎用性の高い動画管理ソフトウェアです。

ご使用の前に

付属のディスクまたは公式ホームページからクライアントソフトウェアを入手し、画面の指示に従ってインストールしてください。

ステップ

1. クライアントソフトを起動すると、以下のようなソフトウェアのコントロールパネルが表示されます。

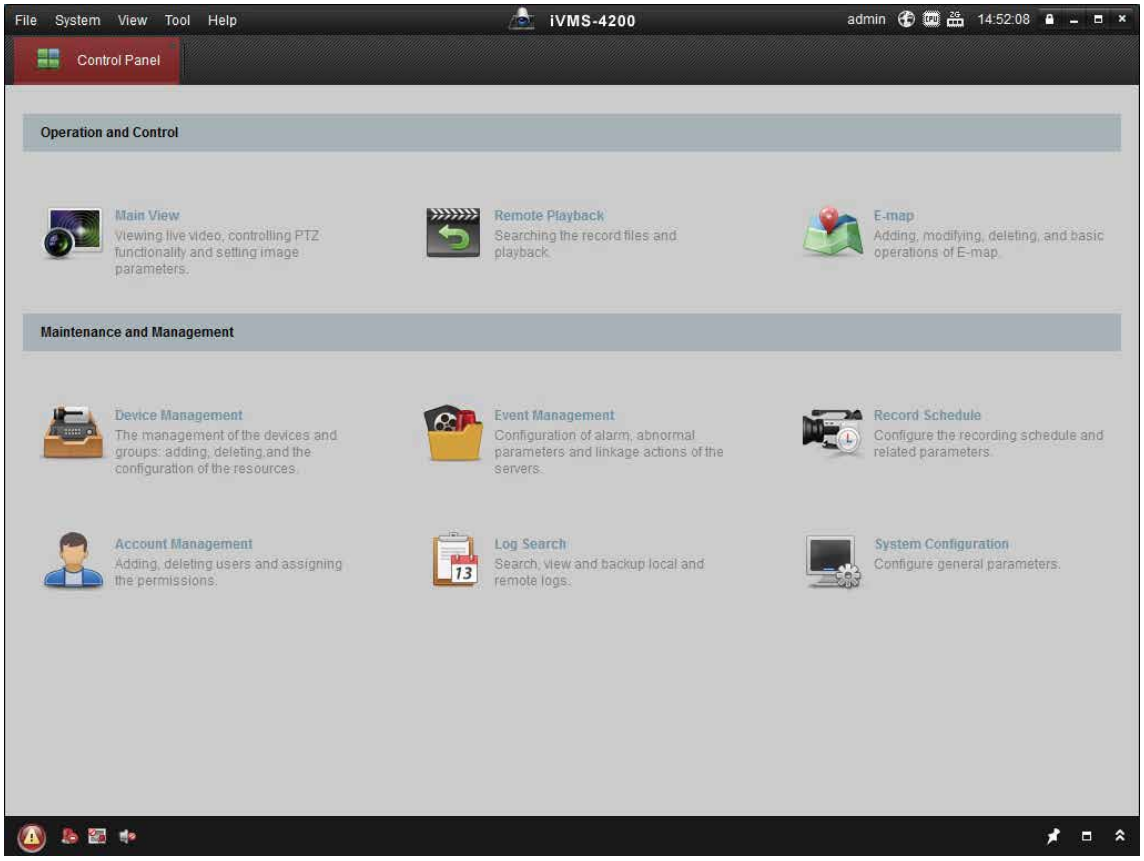


図 1-3 操作パネル

2. **Device Management** をクリックすると、下図のようなデバイス管理インターフェイスになります。

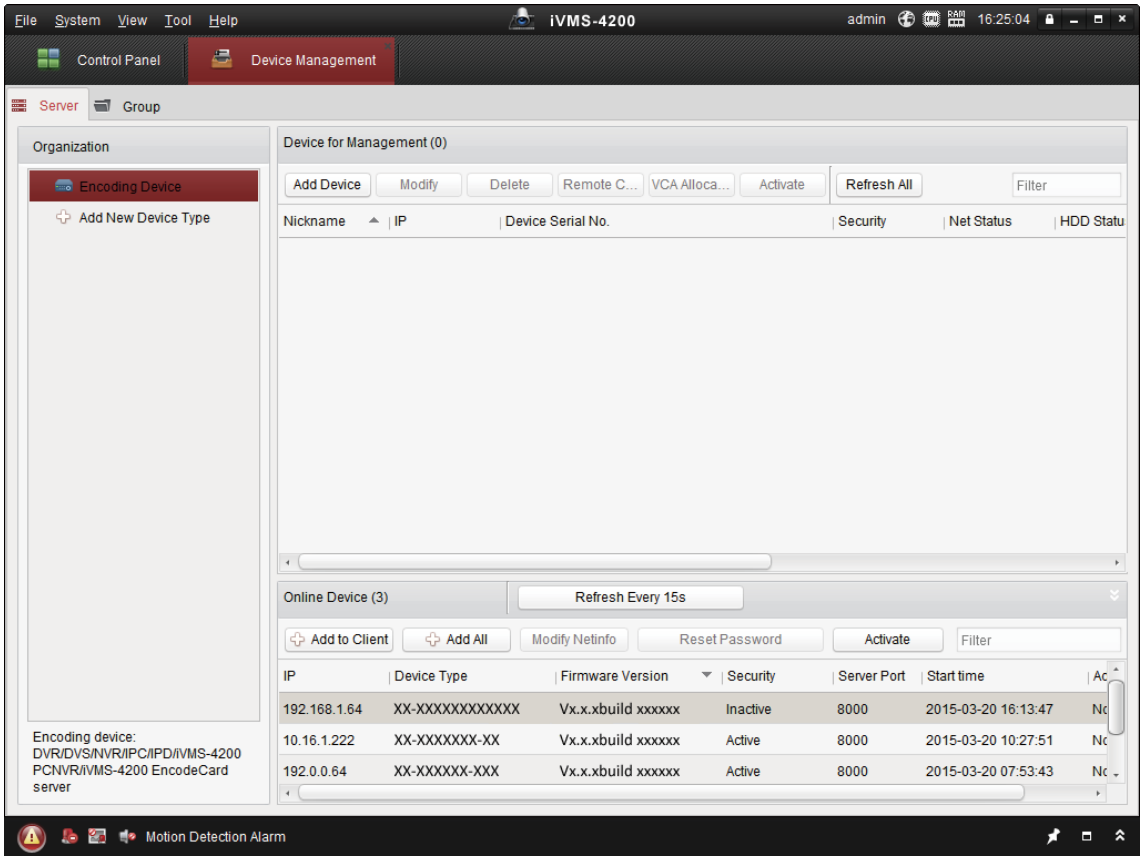


図 1-4 デバイス管理インタフェース

3. 機器一覧から本機のステータスにチェックを入れ、非アクティブのレコーダーを選択します。
4. **Activate** をクリックすると、起動インターフェースが表示されます。
5. パスワードを作成してパスワード欄に入力し、入力したパスワードを確認してください。

メモ

製品の安全性を高めるため、お客様ご自身で強力なパスワード（8 文字以上、大文字、小文字、数字、特殊文字の 3 種類以上）を設定することを強くお勧めします。また、定期的にパスワードをリセットすることをお勧めします。特にセキュリティの高いシステムでは、毎月または毎週パスワードをリセットすることで、製品をより安全に保護することができます。

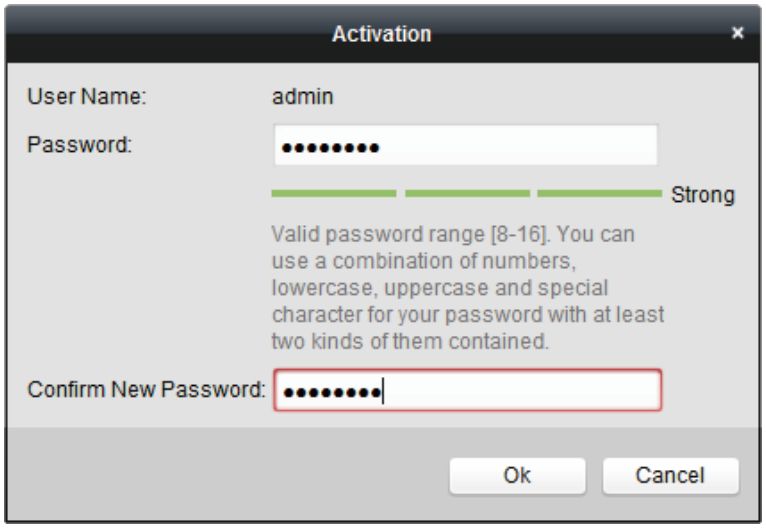


図 1-5 起動

6 **OK** ボタンをクリックすると起動します。

7. **Modify Netinfo** をクリックすると、下図のようなネットワークパラメータ変更インターフェースが表示されます。

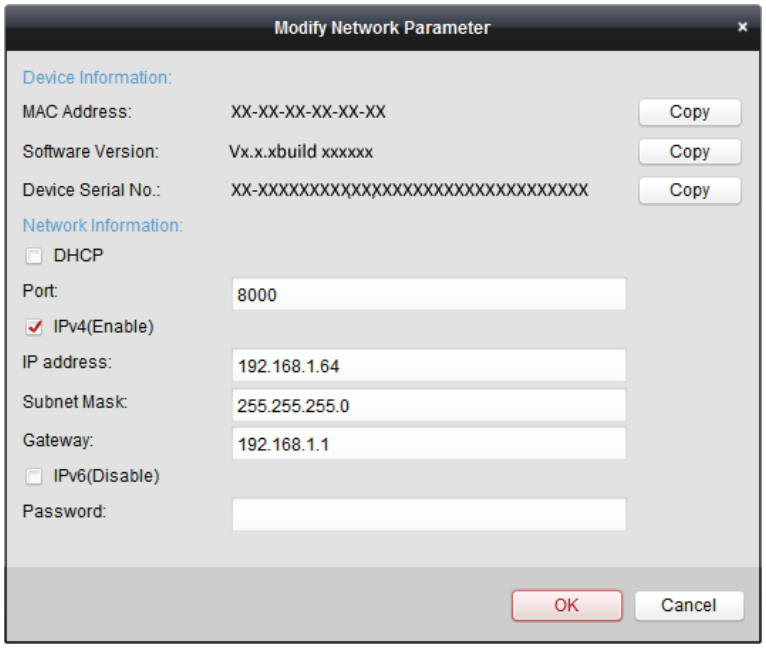


図 1-6 ネットワークパラメータの変更

8. 本機の IP アドレスをパソコンと同じサブネットに変更してください。

IP アドレスを手動で変更します。**Enable DHCP** にチェックを入れてください。

9. パスワードを入力すると、IP アドレスが変更されます。

1.1.5 Web ブラウザーで起動する

Web ブラウザーで本機にアクセスできます。以下の Web ブラウザーのいずれかをご利用ください。
Internet Explorer 6.0 以上、Apple Safari、Mozilla Firefox、Google Chrome 対応解像度は 1024 × 768 以上です。

ご使用の前に

本機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。

ステップ

1. Web ブラウザーへ IP アドレスを入力し、**Enter** キーを押します。

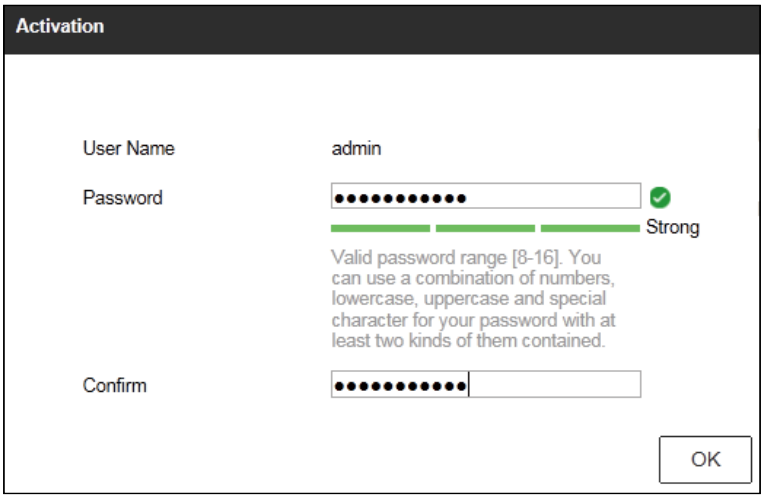


図 1-7 Web ブラウザーの起動

2. 管理者ユーザーアカウントのパスワードを設定します。

メモ

製品の安全性を高めるため、お客様ご自身で強力なパスワード（8 文字以上、大文字、小文字、数字、特殊文字の 3 種類以上）を設定することを強くお勧めします。また、定期的にパスワードをリセットすることをお勧めします。特にセキュリティの高いシステムでは、毎月または毎週パスワードをリセットすることで、製品をより安全に保護することができます。

3. **OK** ボタンをクリックします。
4. オプション：セキュリティ質問、パスワード回復メール、または将来のパスワード再設定用の GUID ファイルのエクスポートを設定します。
5. **OK** ボタンをクリックします。
6. ライブ映像の視聴や本機の管理を行う前に、プラグインをインストールしてください。プラグインのインストールを終了するために、Web ブラウザーを終了する必要がある場合があります。

1.2 TCP/IP の設定

ネットワーク上で本機を操作する前に、TCP/IP が正しく設定されている必要があります。IPv4 と IPv6 の両方が利用可能です。

ステップ

1. 次の順に進みます。**System → Network → TCP/IP**

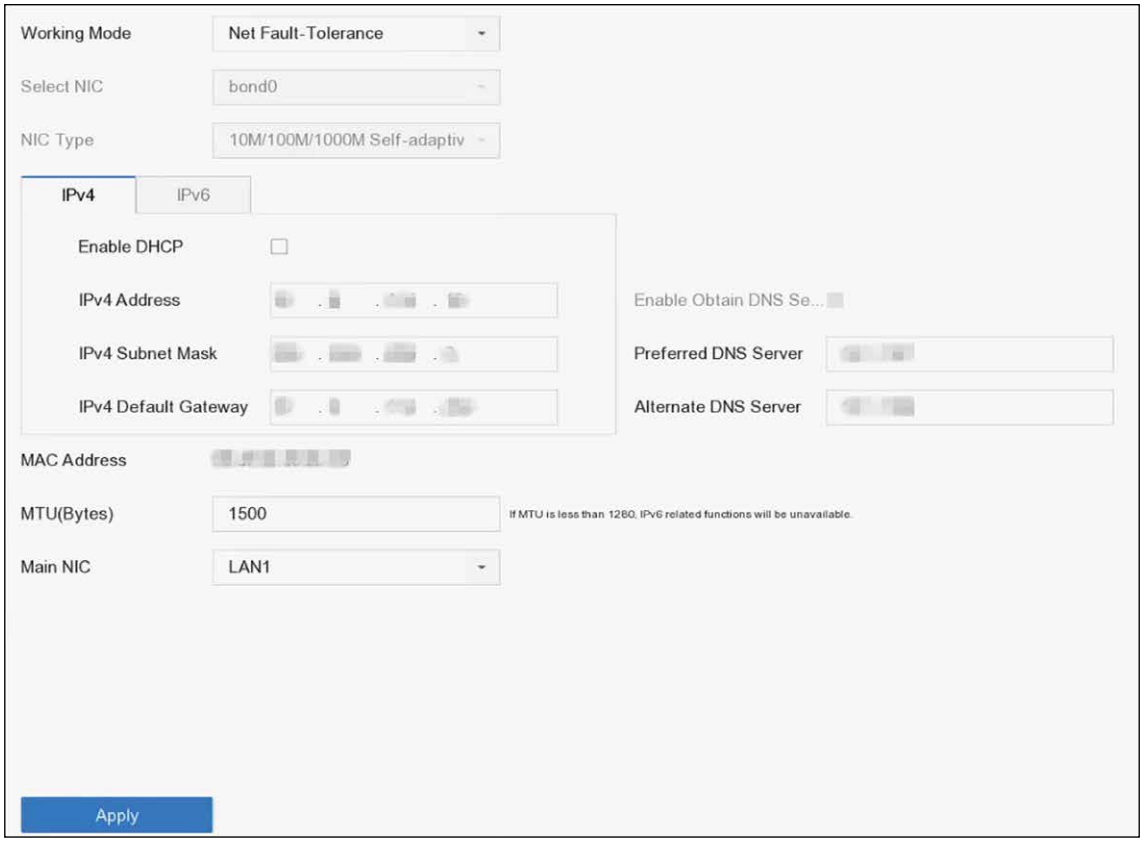


図 1-8 TCP/IP の設定

2. **Working Mode** は **Net-Fault Tolerance** または **Multi-Address Mode** のいずれかを選択します。

   Net-Fault Tolerance

   2 枚の NIC カードは同じ IP アドレスを使用し、メイン NIC を LAN1 または LAN2 に選択することができます。これにより 1 枚の NIC カードが故障した場合でも、自動的にもう 1 枚のスタンバイ NIC カードが有効になり、システムの正常な動作を確保することができます。

   Multi-Address Mode

   2 枚の NIC カードのパラメータは独立して設定することができます。パラメータ設定の「Select NIC」で LAN1 または LAN2 を選択することができます。NIC カード 1 枚をデフォルトルートとして選択します。システムがエクストラネットと接続すると、データはデフォルトルートで転送されます。
3. **IPv4** または **IPv6** を必要に応じてクリックしてください。
4. オプション：ネットワーク上に DHCP サーバーがある場合、**Enable DHCP** にチェックを入れて IP 設定を自動的に取得します。
5. 関連するパラメーターを設定します。

   メモ

   有効な MTU 値の範囲は 500 ～ 1500 です。
6. **Apply** をクリックします。

1.3 HDD の設定

本機の記憶媒体に問題がないか確認します。HDD を最低 1 台搭載して初期化するか、RAID を作成して初期化するかのどちらかです。

1.4 信号入力の設定

アナログ信号と IP 信号の入力タイプを設定することができ、1 つのアナログチャンネルを無効にすると、1 つの IP チャンネルを追加することができます。

ステップ

1. 次の順に進みます。**Camera → Camera → Analog**

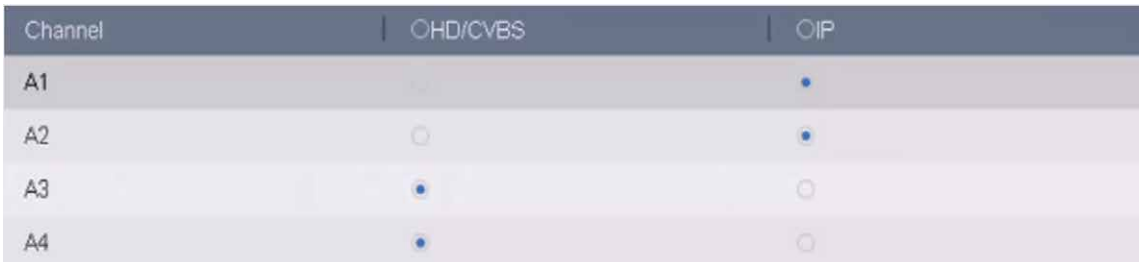


図 1-9 信号入力の種類

2. 各チャンネルの信号入力の種類を **HD/CVBS** または **IP** から選択します。

   HD/CVBS

   Turbo HD、AHD、HDCVI、CVBS の 4 種類のアナログ信号入力をチャンネルごとにランダムに接続することが可能です。

   IP

   チャンネルにネットワークカメラを接続することができます。

3. **Apply** をクリックします。ネットワークカメラの最大アクセス可能台数は、**Max. IP Camera Number** で確認できます。

1.5 エンハンスド IP モードの設定

拡張 IP モードを有効にすると、最大数のカメラに接続できますが、2K/4K 出力解像度が無効になり、境界保護、人または車両の動体検出、顔検出、顔写真の比較機能がアナログチャンネルで使用できなくなります。

メモ

本機能は一部の機種のみ対応しています。

次の順に進み **System → General**、**Enhanced IP Mode** にチェックを入れてください。

1.6 PoC カメラの接続

P シリーズのデバイスは、接続された PoC カメラを自動的に検出し、同軸通信で消費電力を管理し、コアキトロンを介してカメラに電力を供給することができます。

ご使用の前に

- 本機が PoC（Power over Coaxitron）カメラ接続に対応していることを確認してください。
- PoC カメラを DVR に接続します。

ステップ

1. 次の順に進みます。**Menu → Camera → PoC Status**
2. 任意のチャンネルの PoC をオンにします。
3. 接続されている PoC カメラのステータスを確認してください。
- 本機の消費電力が AF カメラより小さい場合、AF カメラまたは AT カメラを接続すると映像が出ず、ライブビュー動画に「Insufficient Power for PoC」がオーバーレイ表示されます。
- 本機の消費電力が AF カメラより高く、AT カメラより低い場合、AF カメラを接続すると正常に電源が入り、AT カメラを接続すると電源が入った後、電源が切れて映像が出ず、ライブビュー画像に「Insufficient Power for PoC」とオーバーレイ表示されます。
- 本機の消費電力が AT カメラより大きい場合、AF カメラまたは AT カメラを接続すると、正常に電源が入ります。
4. 接続されている AF または AT のカメラ番号と接続可能なカメラ番号を確認してください。

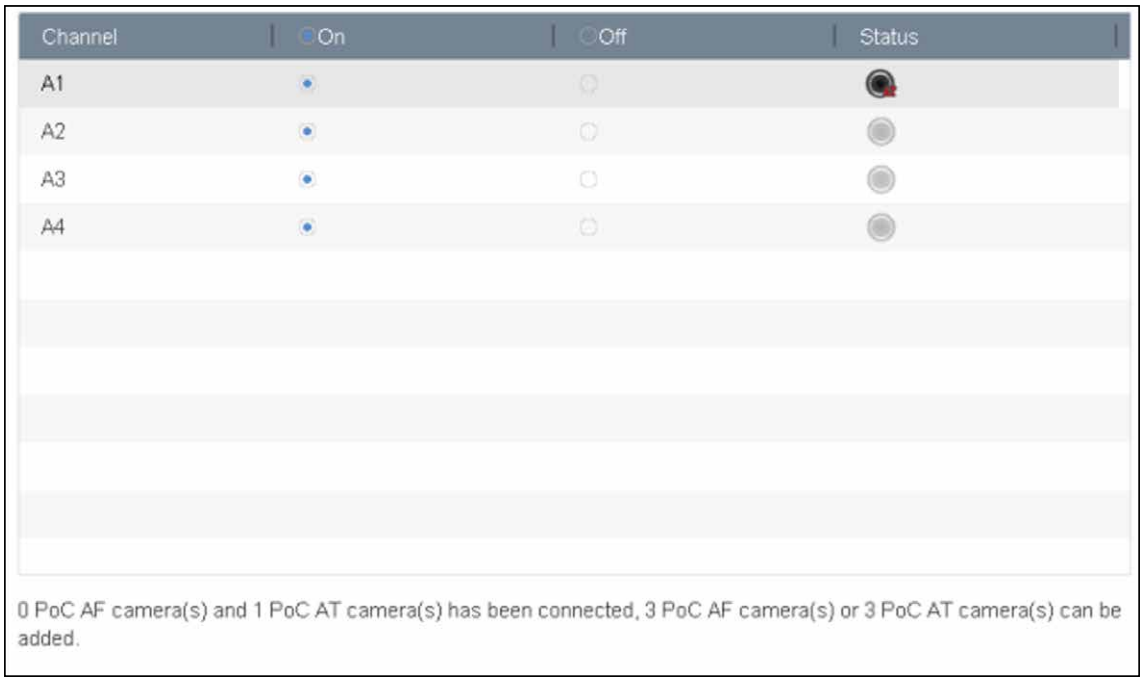


図 1-10 Poc ステータス

メモ

- Hikvision の PoC カメラのみ対応しています。
- 接続可能な最大 AT/AF カメラ数は、機種によって異なります。

警告

PoC に対応していないカメラ、または Hikvision 製以外のカメラの場合は、PoC 機能をオフにしてください。さもないと、カメラや DVR に永久的な損傷を与える可能性があります。

1.7 ネットワークカメラの追加

ライブ映像の取得や動画ファイルの録画を行う前に、本機の接続リストにネットワークカメラを追加する必要があります。

ご使用の前に

ネットワーク接続が有効で正しいこと、追加する IP カメラが有効になっていることを確認します。

ステップ

1. メインメニューバーの をクリックします。
2. タイトルバーの **Custom Add** タブをクリックします。

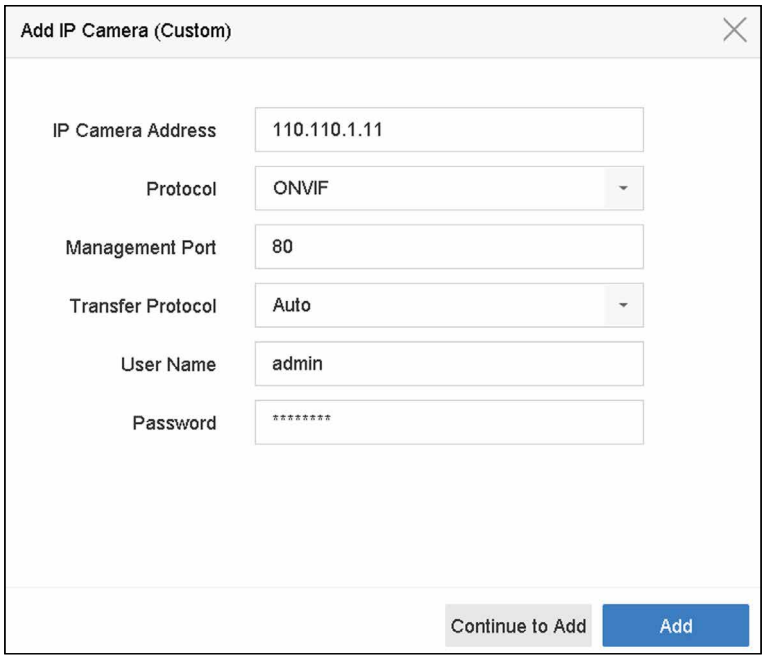


図 1-11 IP カメラの追加

3. IP アドレス、プロトコル、管理ポートや追加するその他の IP カメラ情報を入力します。
4. IP カメラのログインユーザー名とパスワードを入力します。
5. **Add** をクリックして、IP カメラの追加を終了します。
6. オプション：**Continue to Add** をクリックして IP カメラをさらに追加することができます。

1.7.1 自動検索されたオンラインネットワークカメラを追加する

ステップ

1. メインメニューバーの をクリックします。
2. 下部にある **Number of Unadded Online Device** をクリックします。
3. 自動的に検索されたオンラインネットワークカメラを選択します。
4. **Add** をクリックして、本機と同じログインパスワードを持つカメラを追加します。

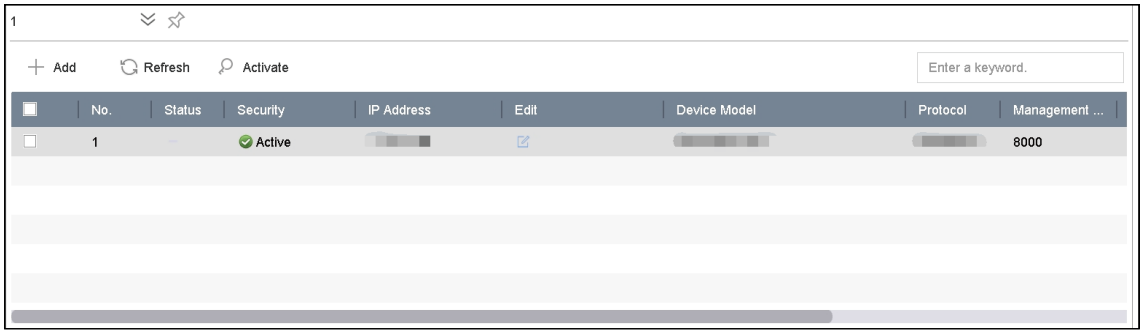


図 1-12 自動検索されたオンラインネットワークカメラの追加

メモ

追加するネットワークカメラが起動していない場合は、カメラ管理インタフェースのネットワークカメラリストで起動することができます。

1.7.2 ネットワークカメラを手動で追加する

ライブ映像を表示したり、動画ファイルを録画したりする前に、本機にネットワークカメラを追加する必要があります。

ご使用の前に

ネットワーク接続が有効で正しいこと、ネットワークカメラが起動していることを確認します。

ステップ

1. メインメニューバーの をクリックします。
2. **Custom Add** をクリックします。
3. パラメータを設定します。例：**IP カメラアドレス**、**プロトコル**など。

メモ

管理ポートの範囲は 1 ～ 65535 です。

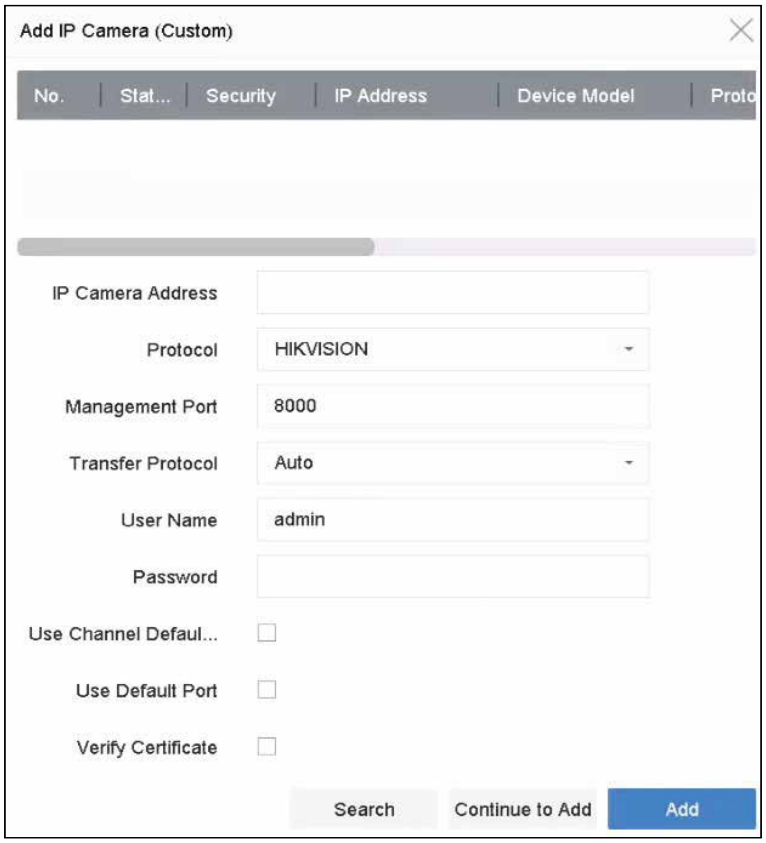


図 1-13 ネットワークカメラの追加

4. オプション：カメラの追加にデフォルトのパスワードを使用する場合は、**Use Channel Default Password** にチェックを入れます。
5. オプション：デフォルトの管理ポートを使用してカメラを追加する場合は、**Use Default Port** にチェックを入れます。SDK サービスの場合、デフォルトのポート値は 8000 です。拡張 SDK サービスの場合、デフォルト値は 8443 です。

メモ

HIKVISION プロトコルを使用する場合のみ有効な機能です。

6. オプション：**Verify Certificate** にチェックを入れて、カメラ認証の検証を行います。この認証は、より安全なカメラ認証を実現するためのカメラの識別形式です。この機能を使うには、最初にネットワークカメラの証明書を本機にインポートする必要があります。詳しくは参照してください。

メモ

拡張 SDK サービスは、HIKVISION プロトコルを使用する場合のみ利用可能です。

7. **Add** をクリックします。
8. オプション：**Continue to Add** にチェックを入れると、他のネットワークカメラを追加できます。

1.7.3 カスタマイズされたプロトコル経由でネットワークカメラを追加する

標準プロトコルを使用しないネットワークカメラの場合、カスタマイズしたプロトコルを設定して追加することができます。このシステムは 8 つのカスタマイズされたプロトコルを提供します。

ステップ

1. 次の順に進みます。**More Settings → Protocol**

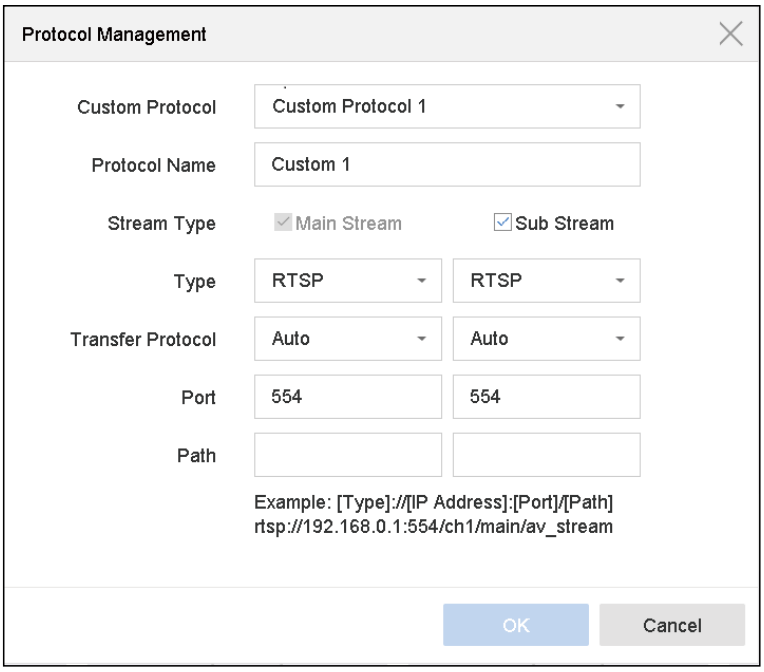


図 1-14 プロトコル管理

2. プロトコルのパラメータを設定します。

Type

カスタムプロトコルを採用したネットワークカメラは、標準的な RTSP によるストリーム取得に対応している必要があります。

Path

メインストリーム、サブストリームを取得するための URL（Uniform Resource Locator）については、ネットワークカメラのメーカーにお問い合わせください。

メモ

追加するネットワークカメラが、プロトコルのタイプと転送プロトコルをサポートしている必要があります。

3. **OK** ボタンをクリックします。
4. **Custom Add** をクリックすると、カメラが追加されます。
5. パラメータを設定します。
6. **OK** ボタンをクリックします。

1.8 5MP 長距離伝送の設定

一部の機種で、5MP の長距離伝送を設定することができます。

ステップ

1. 次の順に進みます。**Camera → Camera → Analog**
2. をクリックすると、MP 長距離伝送設定のインターフェースに入ります。

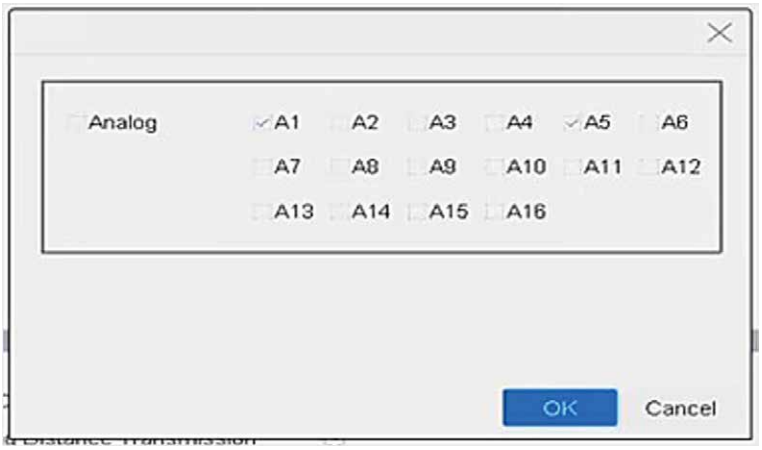


図 1-15 5MP 長距離伝送設定

3. チャンネル（複数可）を選択して 長距離伝送を有効にします。
4. **OK** ボタンをクリックします。
5. **Apply** をクリックします。

1.9 プラットフォームへの接続

1.9.1 Hik-Connect を設定する

Hik-Connect は、本機にアクセスし、管理するための携帯電話アプリケーションとプラットフォームサービスを提供し、監視システムへの便利なリモートアクセスを可能にします。

ステップ

1. 次の順に進みます。**System → Network → Advanced → Platform Access**
2. **Enable** にチェックを入れると、機能が有効になります。次に、サービス規約が表示されます。
   1）認証コードを入力します。
   2）QR コードをスキャンして、サービス規約とプライバシーステートメントをお読みください。
   3）**Hik-Connect** は、インターネットに接続できる環境が必要です。サービスを有効にする前に、サービス利用規約およびプライバシーステートメントをお読みになり 同意をチェックしてください。
   4) **OK** ボタンをクリックしてください。

メモ

- 工場出荷時では Hik-Connect は無効になっています。
- 認証コードは工場出荷時では空欄です。6 ～ 12 文字の英数字が含まれる必要があり、大文字と小文字は区別されます。

3. オプション：以下のパラメータを設定します。
   - **Custom** にチェックを入れ、必要に応じて **Server Address** を入力します 。
   - **Enable Stream Encryption** にチェックを入れます。リモートアクセスやライブビューを行うには、認証コードが必要になります。
   - **Time Sync** にチェックを入れると、NTP サーバーの代わりに Hik-Connect で時刻を同期します。
4. 本機を Hik-Connect のアカウントでバインドします。
   1）スマートフォンで QR コードを読み取り、Hik-Connect アプリをダウンロードします。
   https://appstore.hikvision.com からダウンロードすることもできます。または、下記の QR コードをご利用ください。詳しくは Hik-Connect モバイルクライアント ユーザーマニュアルを参照ください。

図 1-16 Hik-Connect のダウンロード

   2）Hik-Connect で本機の QR を読み取り、バインドする。

メモ

本機がすでにアカウントとバインドされている場合は Unbind をクリックして、現在のアカウントとのバインドを解除します。

1.9.2 ISUP を設定する

SDK は Intelligent Security Uplink Protocol (ISUP) をベースにしています。NVR、スピードドーム、DVR、ネットワークカメラ、モバイル NVR、モバイルデバイス、デコードデバイスなどのデバイスにアクセスするための API、ライブラリファイル、コマンドをサードパーティのプラットフォーム用に提供します。このプロトコルにより、サードパーティのプラットフォームは、ライブビュー、再生、双方向オーディオ、PTZ 制御などの機能を使用することができます。

ステップ

メモ

本機能は一部の機種のみ対応しています。

1. 次の順に進みます。**System → Network → Advanced → Platform Access**

図 1-17 ISUP 設定

2. **Access Type** は **ISUP** を選択 します。
3. **Enable** にチェックを入れます。

メモ

ISUP を有効にすると、他のプラットフォームのアクセスは無効となります。

4. 関連するパラメーターを設定します。

Server Address

プラットフォームサーバーの IP アドレスです。

Server Port

プラットフォームサーバーのポートで、1024 ～ 65535 の範囲で指定します。実際のポートは、プラットフォームから提供されるものです。

Device ID

デバイス ID はプラットフォームから提供されるものとします。

Version

使用可能な ISUP プロトコルバージョンは、V5.0 のみです。

Encryption Password

ISUP V5.0 バージョンを使用する場合、暗号化パスワードが必要となり、デバイスとプラットフォーム間でより安全な通信をします。ISUP プラットフォームにデバイスを登録した後に、確認のために暗号化パスワードを入力します。空欄や、"ABCDEF " は使用できません。

5. **Apply** をクリックして設定を保存し、本機を再起動します。

次は

本機を再起動すると、登録ステータス（オンライン / オフライン）を確認できます。

第 2 章 カメラの設定

2.1 画像パラメータの設定

Camera → Display と進んで、昼夜の切り替え、バックライト、コントラスト、彩度などの画像パラメータをカスタマイズすることができます。

Image Settings

明るさ、コントラスト、彩度などの画像パラメータをカスタマイズしてください。

Exposure

カメラの露光時間（1/10000 ～ 1 秒）を設定します。露出値を大きくすると、明るい画像になります。

Day/Night Switch

時間や周囲の明るさに応じて、カメラを昼 / 夜自動切替モードに設定します。夜間、光が弱くなるとナイトモードに切り替わり、高画質な白黒映像が得られます。

Backlight

カメラのワイドダイナミックレンジ（0 ～ 100）を設定します。周囲の照明と被写体の明るさの差が大きい場合、画像全体の明るさのバランスをとるために WDR 値を設定することができます。

Image Enhancement

ビデオストリームのノイズを低減するために、画像のコントラストを最適化します。

2.2 OSD の設定

カメラの OSD（オンスクリーンディスプレイ）の設定（日時、カメラ名など）を行うことができます。

ステップ

1. 次の順に進みます。**Camera → Display**
2. 必要に応じてカメラを選択します。
3. **Camera Name** でカメラの名前を編集します。
4. **Display Name**、**Display Date**、**Display Week** にチェックを入れると、画像に情報が表示されます。
5. 日付形式、時刻形式、表示モードを設定します。

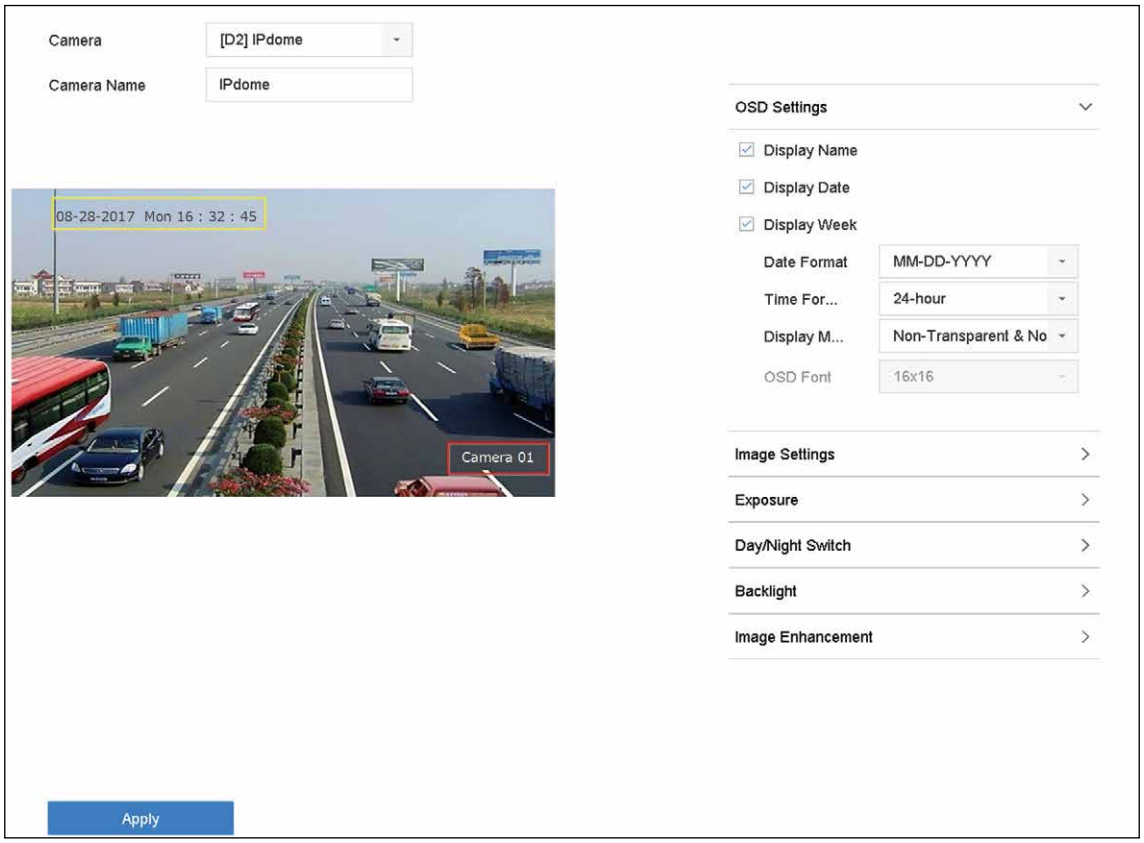


図 2-1 OSD 設定

6. プレビューウィンドウのテキストフレームをドラッグして、OSD の位置を調整することができます。
7. **Apply** をクリックします。

2.3 プライバシーマスクの設定

プライバシーマスクは、映像の一部をライブビューから隠したり、マスク領域で録画することで、個人のプライバシーを保護できます。

ステップ

1. 次の順に進みます。**Camera → Privacy Mask**
2. プライバシーマスクを設定するカメラを選択します。
3. **Enable** にチェックを入れます。
4. ウィンドウにゾーンを描画します。このゾーンは、異なるフレームカラーで表示されます。

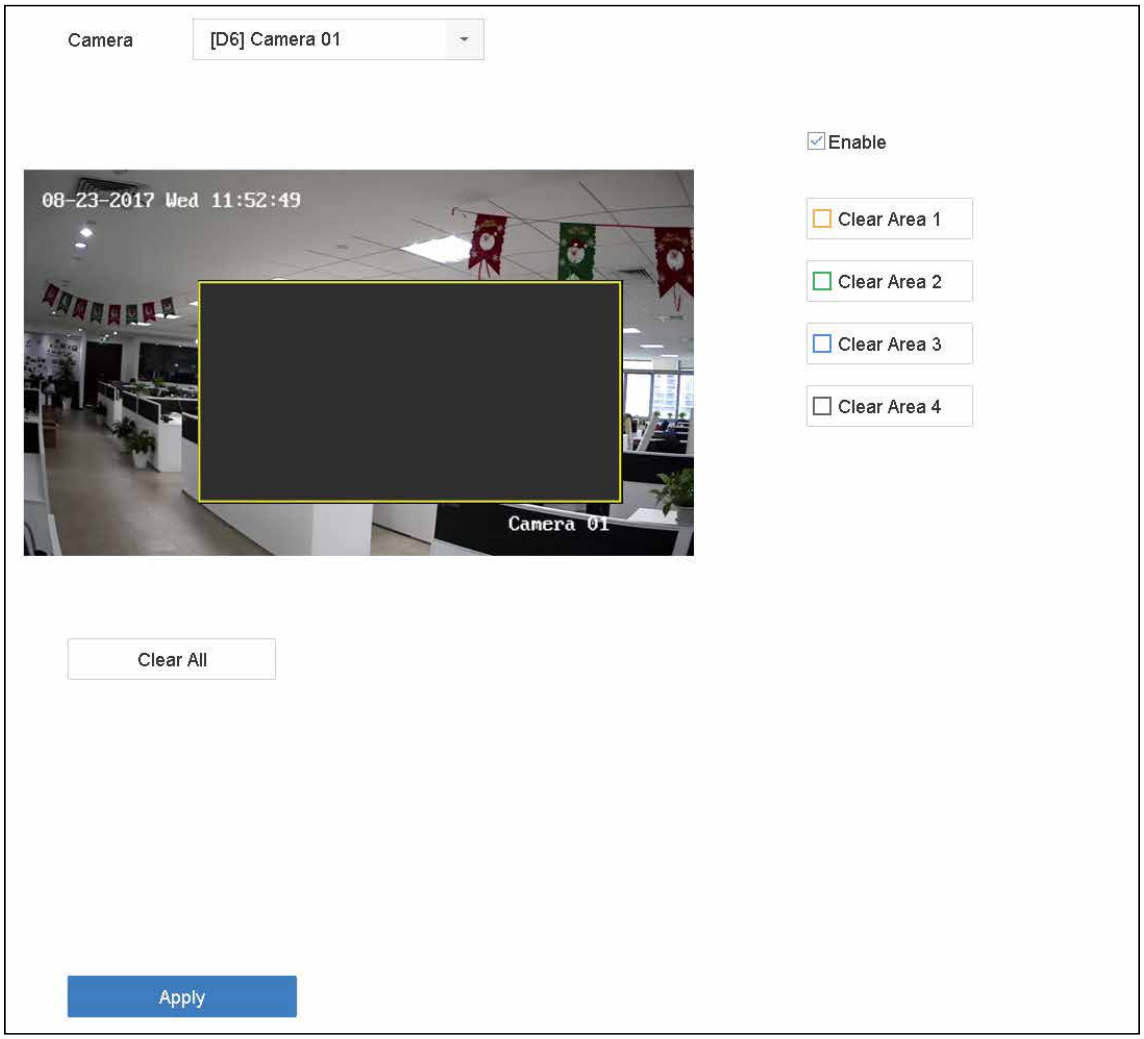


図 2-2 プライバシーマスクの設定

メモ

- プライバシーマスクのゾーンは最大 4 つまで設定でき、各エリアのサイズも調整可能です。
- 設定したプライバシーマスクのゾーンを解除するには、ウィンドウの右側にあるゾーン 1 ～ 4 の解除アイコンをクリックするか、または **Clear All** をクリックすると、すべてのゾーンがクリアされます。

5. **Apply** をクリックします。

2.4 IP カメラの設定ファイルのインポート / エクスポート

IP アドレス、管理ポート、管理者のパスワードなど、IP カメラの情報を Microsoft Excel 形式で保存し、ローカルデバイスにバックアップすることが可能です。エクスポートしたファイルは、PC 上で内容の追加や削除などの編集が可能で、Excel ファイルを他の機器に取り込めば、設定をコピーすることもできます。

ご使用の前に

設定ファイルをインポートする場合は、設定ファイルが格納されているストレージデバイスを機器に接続してください。

ステップ

1. 次の順に進みます。**Camera → IP Camera Import/Export**
2. **IP Camera Import/Export** をクリックすると、検出された外部デバイスの内容が表示されます。
3. IP カメラの設定ファイルをエクスポートまたはインポートします。
   – **Export** をクリックして、選択したローカルバックアップデバイスに設定ファイルをエクスポートします。
   – 設定ファイルをインポートするには、選択したバックアップデバイスからファイルを選択し **Import** をクリックします。

メモ

インポート処理完了後、設定を有効にするために本機を再起動する必要があります。

2.5 IP カメラの時刻同期

この機能を有効にすると、接続された IP カメラの時刻を自動的に同期させることができます。

ステップ

メモ

本機能は一部の機種のみ対応しています。

1. 次の順に進みます。**Camera → Camera → IP Camera**
2. IP カメラのウィンドウにカーソルを合わせて をクリックします。
3. **Enable IP Camera Time Sync** にチェックを入れます。
4. **OK** ボタンをクリックします。

2.6 カメラ VCA データの保存

カメラの VCA データを本機に保存すると、カメラの VCA データを検索できるようになります。
次の順に進み **Storage → Advanced**、機能を有効にします。

2.7 IP カメラのアップグレード

IP カメラのアップグレードは、本機から行うことができます。

ご使用の前に

USB フラッシュメモリーを本機に挿入し、IP カメラのバージョンアップファームウェアが入っていることを確認ししてください。

ステップ

1. カメラ管理インターフェースで、カメラを選択します。
2. 次の順に進みます。**More Settings → Upgrade**
3. USB メモリーからファームウェアのアップグレードファイルを選択します。
4. **Upgrade** をクリックします。
   バージョンアップが完了すると、IP カメラは自動的に再起動します。

第 3 章 ライブビュー

ライブビューは、各カメラから取得した映像をリアルタイムに表示します。

3.1 ライブビューの開始

メインメニューバーの　をクリックします。

- ウィンドウを選択し、チャンネルリストからカメラをダブルクリックすると、そのカメラのライブ映像が再生されます。
- ウィンドウをダブルクリックすると、シングルスクリーンモードで表示されます。もう一度ダブルクリックすると、シングルスクリーンモードが終了します。
- 再生ウィンドウ下部のツールバーを使って、キャプチャー、インスタント再生、オーディオのオン / オフ、デジタルズーム、ライブビューストラテジー、情報表示、録画開始 / 停止などを実行します。
- をクリックして自動切替を開始 / 停止します。自動的に次の画面に切り替わります。
- ウィンドウにカーソルを合わせ、マウスを右クリックすると、そのウィンドウのショートカットメニューが表示されます。ショートカットメニューは、ウィンドウによって異なります。

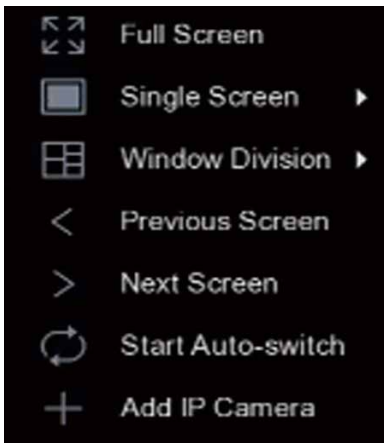


図 3-1 ショートカットメニュー

3.1.1 ライブビューを設定する

ライブビューの設定をカスタマイズすることができます。出力インターフェース、画面表示までのドウェルタイム、音声のミュートやオン、各チャンネルの画面番号などを設定できます。

ステップ

1. 次の順に進みます。**System → Live View → General**

図 3-2 ライブビュー - ゼネラル

2. ライブビューのパラメーターを設定します。

Video Output Interface

設定するビデオ出力を選択します。

Live View Mode

ライブビューの表示モードを選択します（例：2*2、1*5 など）。

Dwell Time

ライブビューで自動切替えを使用するときに、カメラが切り替わるまでの待ち時間（秒）です。

Enable Audio Output

選択したビデオ出力の音声出力を有効 / 無効にするかどうかを設定します。

Volume

選択した出力インターフェースのライブビュー音量、再生、双方向音声を調整します。

Event Output

イベント映像を表示する出力を選択します。

Full Screen Monitoring Dwell Time

アラームイベント画面を表示する時間を秒単位で設定します。

3. **OK** ボタンをクリックします。

3.1.2 カメラの自動切替えを設定する

カメラの自動切替えを設定し、異なる表示モードで再生することができます。

ステップ

1. 次の順に進みます。**System → Live View → General**
2. **Video Output Interface**、**Live View Mode**、**Dwell Time** を設定します。

Video Output Interface

ビデオ出力インターフェースを選択します。

Live View Mode

ライブビューの表示モードを選択します。（例：2 × 2、1 × 5 など）

Dwell Time

自動切替えを有効にした場合のカメラ切替時の滞留時間（秒）です。滞留時間の範囲は 5 秒から 300 秒です。

3. **View Settings** に進んでビューレイアウトを設定します。
4. **OK** ボタンをクリックして、設定を保存します。

3.1.3 ライブビューレイアウトを設定する

ライブビューは、各カメラから取得した映像をリアルタイムに表示します。

カスタムライブビューレイアウトを設定する

ステップ

1. 次の順に進みます。**System → Live View → View**
2. **Set Custom Layout** をクリックします。
3. Custom Layout Configuration インターフェースの ＋ をクリックします。
4. レイアウト名を編集します。
5. ツールバーからウィンドウ分割モードを選択します。

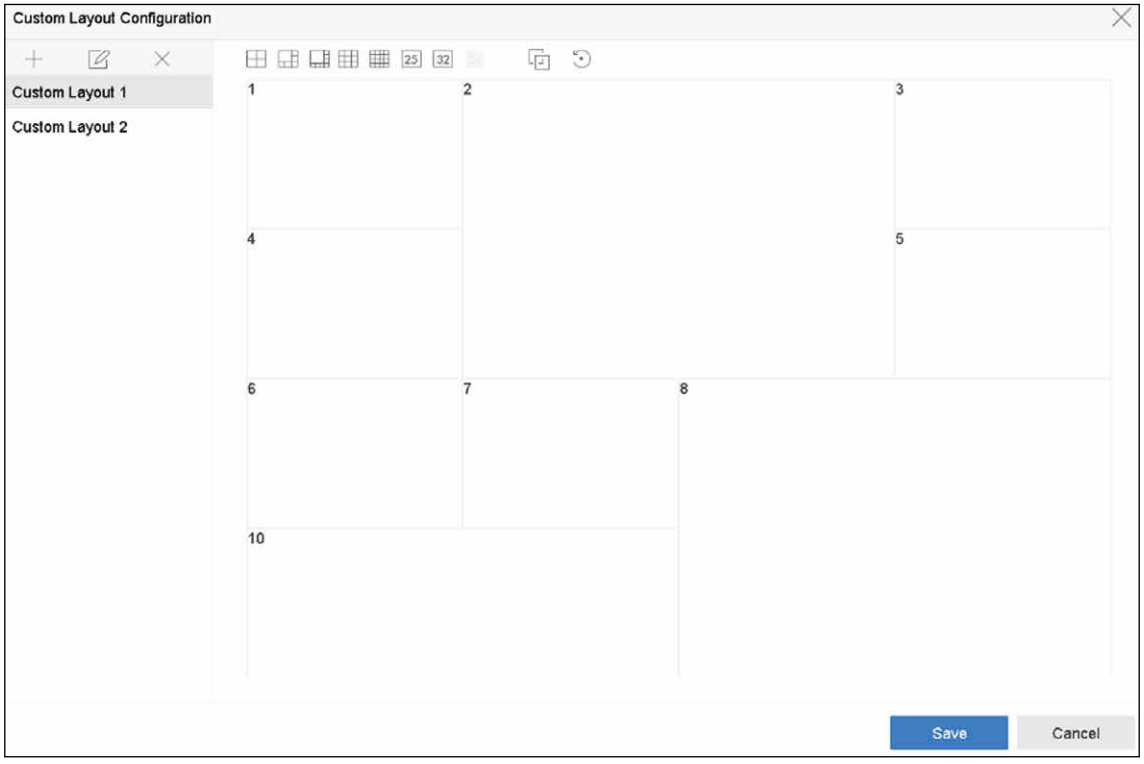


図 3-3 ライブビューのレイアウト設定

6. 複数ウィンドウを選択し をクリックしてウィンドウを結合します。選択されたウィンドウは、矩形領域内にある必要があります。
7. **Save** をクリックします。
   正常に設定されたレイアウトがリストに表示されます。
8. オプション：一覧からライブビューレイアウトを選択し をクリックすると名前の編集ができ、 をクリックすると、名前が削除されます。

ライブビューモードを設定する

ステップ

1. 次の順に進みます。**System → Live View → View**
2. ビデオ出力インターフェースを選択します。
3. ツールバーからレイアウトまたはカスタムレイアウトを選択します。
4. 分割ウィンドウを選択し、リスト内のカメラをダブルクリックすると、そのウィンドウにカメラがリンクします。

メモ

- また、ライブビューインターフェースの任意のウィンドウにカメラをクリック＆ドラッグして、カメラの順番を設定することができます。
- テキストフィールドに番号を入力すると、リストからカメラをすばやく検索することができます。

5. **Apply** をクリックします。
6. オプション： をクリックすると、全チャンネルのライブビューを開始します。また、 をクリックすると、すべてのライブビューチャンネルを停止します。

3.1.4 チャンネルゼロエンコーディングの設定

Web ブラウザーや CMS（クライアント管理システム）ソフトウェアから多数のチャンネルをリアルタイムでリモート表示する必要がある場合、画質に影響を与えずに必要な帯域幅を減らすために、チャンネルゼロエンコーディングを有効にしてください。

ステップ

1. 次の順に進みます。**System → Live View → Channel-Zero**
2. **Enable Channel-Zero Encoding** にチェックを入れます。

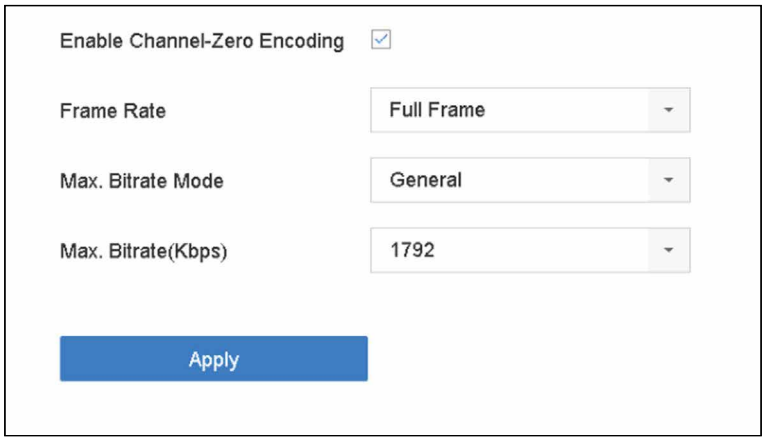


図 3-4 チャネルゼロエンコーディング

3. **Frame Rate**、**Max. Bitrate Mode**、**Max. Bitrate** を設定します。

メモ

フレームレートとビットレートが高いほど、高い帯域幅が必要になります。

4. **Apply** をクリックします。
   CMS や Web ブラウザーを使って、1 つの画面ですべてのチャンネルを見ることができます。

3.1.5 補助モニターを使用する

ライブビューの一部の機能は、補助モニター中でも使用できます。補助モニターの機能は以下です。

Single Screen

選択したカメラの全画面表示に切り替わります。カメラはドロップダウンリストから選択することができます。

Multi-screen

異なる表示レイアウトオプションを切り替えます。レイアウトのオプションは、ドロップダウンリストから選択することができます。

Next Screen

ライブビューで表示するカメラの台数が最大台数に満たない場合、この機能をクリックすると、次の組の表示に切り替わります。

Playback

再生モードに入ります。

PTZ Control

PTZ コントロールモードに入ります。

Main Monitor

メイン操作モードに入ります。

メモ

メイン出力モニターのライブビューモードでは、Aux 出力モードが有効な場合、メニュー操作はできません。

3.2 デジタルズーム

デジタルズームは、ライブ映像を異なる倍率（1 倍～ 16 倍）で拡大表示します。

ステップ

1. ライブビューを開始します。
2. ツールバーの をクリックします。
3. スライドバーを動かすか、マウスホイールをスクロールすることで、異なる倍率（1 倍～ 16 倍）に画像を拡大・縮小することができます。

図 3-5 デジタルズーム

3.3 ライブビューストラテジー

ステップ

1. ライブビューモードで をクリックすると、フルスクリーンモードのデジタルズーム操作インターフェイスに入ります。
2. ライブビューストラテジーを **Real-time**、**Balanced**、**Fluency** から選択します。

3.4 3D ポジショニング

3D ポジショニングは、特定のライブ映像エリアをズームイン / ズームアウトします。

ステップ

メモ

本機能は一部の機種のみ対応しています。

1. ライブビューを開始し をクリックします。
2. 映像をズームイン / ズームアウトします。
   – ズームイン：ビデオ映像内の任意の位置をクリックし、右下方向に矩形領域をドラッグすると、拡大表示することができます。
   – ズームアウト：矩形領域を左上方向にドラッグすると、位置が中央に移動し、矩形領域が縮小表示することができます。

3.5 顔認識

顔認識インターフェースに入り、リアルタイムの顔認識結果や他人認識結果を見ることができます。

ご使用の前に

顔検出と顔写真比較機能が設定されていることを確認してください。詳しくは**顔画像比較**を参照してください。

ステップ

メモ

本機能は一部の機種のみ対応しています

1. ライブビューインターフェースに進み、ツールバーの をクリックします。
2. 、 または をクリックして ウィンドウ分割を設定します。
3. 見たいウィンドウを選択します。
4. 左下のカメラ一覧からひとつのカメラをダブルクリックします。

図 3-6 顔認識

5. **Records** をクリックすると、選択したカメラのリアルタイム顔認識記録が表示されます。また、記録は右のウィンドウに表示されます。上部に総数、成功数、失敗数などの顔検出数を表示することができます。
6. オプション：未登録の顔写真については、記録一覧からダブルクリックして顔写真ライブラリーに追加することができます。

メモ

ゲストユーザーとオペレーターユーザーの場合、未登録の顔写真を顔写真ライブラリーに追加するには、ローカルパラメーター設定の権限が必要です。

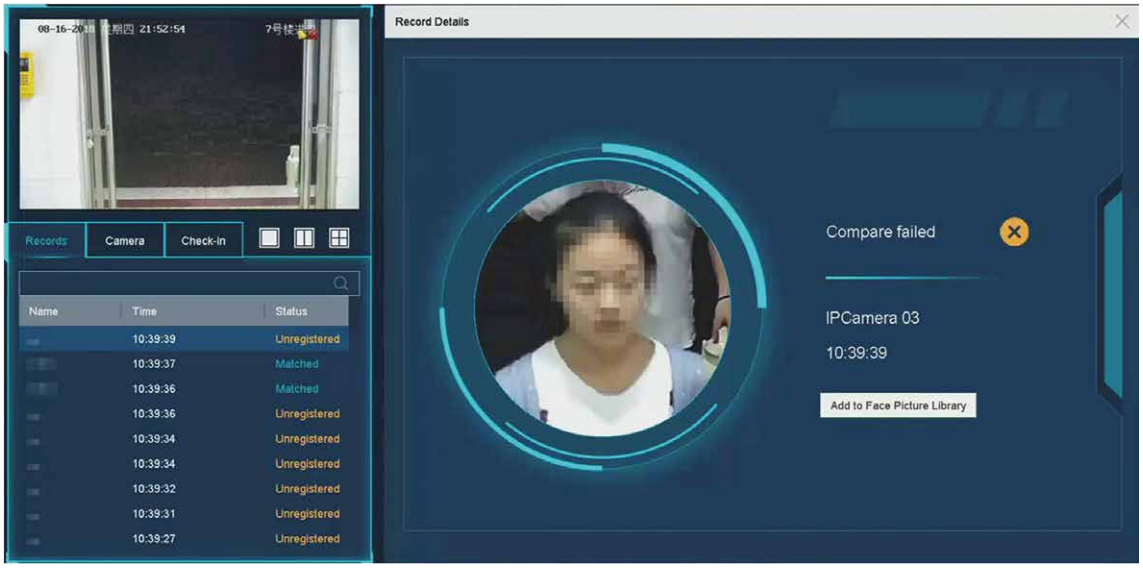


図 3-7 未登録の顔写真の追加

7. オプション：**Check-in** をクリックすると、顔写真ライブラリーのチェックイン記録（**Total No.**、**Checked In**、**Unchecked In**）が表示されます。
8. オプション：右上の をクリックすると、表示に関する設定を任意に行うことができます。

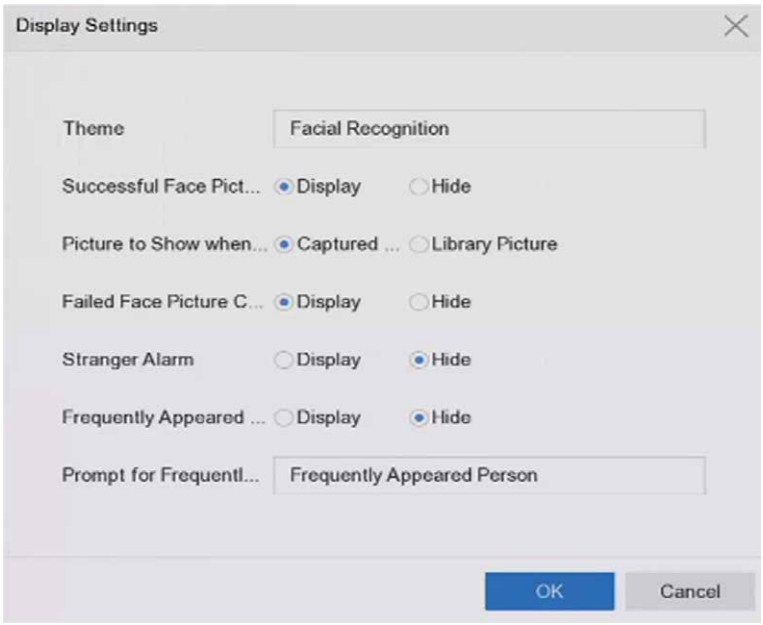


図 3-8 顔認識表示設定

9. オプション：右上の をクリックすると、記録の検索とエクスポートができます。
   1）検索条件を任意に設定します。
   2) **Search** をクリックします。
   3) **Export Attendance Record** または **Export Check-in Record** をクリックします。

メモ

- エクスポートする前に、USB メモリーを挿入していることを確認してください。
- 記録をクリックすると、この個人の出欠情報をカレンダーで確認できます。
- ゲストおよびオペレーターの場合、録画の検索とエクスポートには、「カメラ権限」の「ローカルビデオエクスポート権限」が必要です。

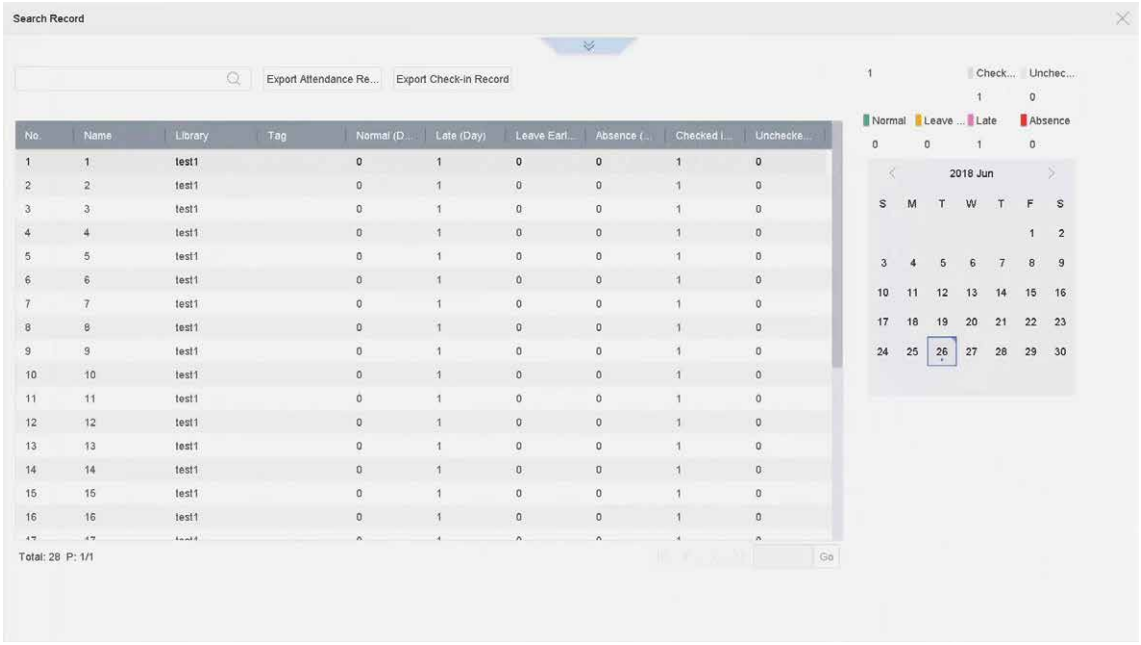


図 3-9 顔認識検索記録

3.6 PTZ コントロール

3.6.1 PTZ パラメーターを設定する

以下の手順で、PTZ のパラメータを設定します。PTZ カメラを制御する前に、PTZ パラメーターの設定を行う必要があります。

ステップ

1. カメラのクイック設定ツールバーの をクリックします。
2. **PTZ Parameters Settings** をクリックして、PTZ のパラメータを設定します。

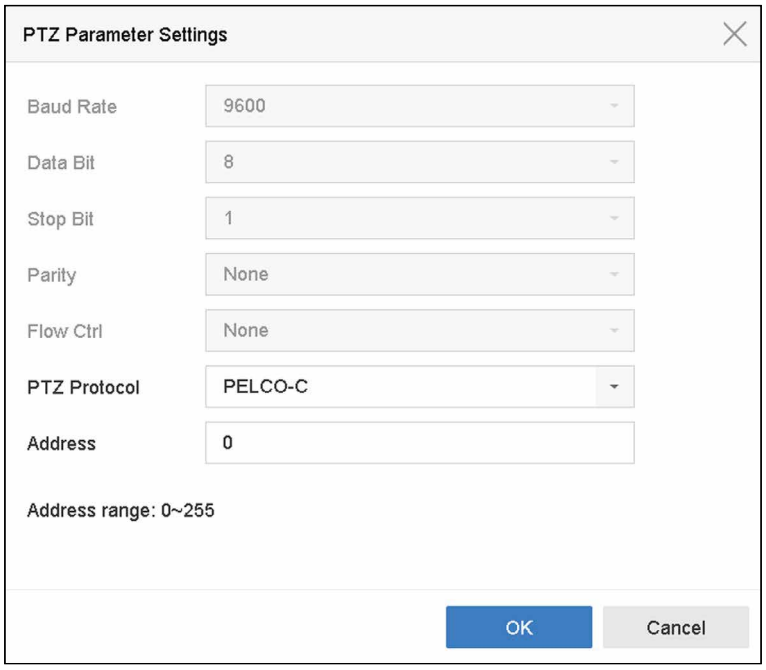


図 3-10 PTZ パラメータの設定

3. PTZ のパラメータを編集します。

メモ

すべてのパラメータは、PTZ カメラのパラメータと正確に一致している必要があります。

4. **OK** ボタンをクリックして、設定を保存します。

3.6.2 プリセットを設定する

プリセットには、PTZ の位置やズーム、フォーカス、アイリスなどのステータスが記録されています。プリセットを呼び出すと、あらかじめ設定された位置にカメラをすばやく移動させることができます。

ステップ

1. PTZ カメラのライブビューのクイック設定ツールバーの をクリックします。
2. 方向ボタンをクリックすると、カメラを任意の場所に移動させることができます。
3. ズーム、フォーカス、アイリスのステータスを調整します。
4. ライブビューの右下にある をクリックすると、プリセットの設定ができます。

図 3-11 プリセットの設定

5. ドロップダウンリストから、プリセット番号（1 ～ 255）を選択します。
6. プリセット名を入力します。
7. **Apply** をクリックして、プリセットを保存します。

8. オプション：**Cancel** をクリックすると、プリセットの位置情報をキャンセルすることができます。
9. オプション：ライブビューの右下にある をクリックすると、設定したプリセットがに表示されます。

図 3-12 設定されたプリセットの表示

3.6.3 プリセットを呼び出す

プリセットとは、イベントが発生したときに、カメラが窓などの指定した位置に向くようにするものです。

ステップ

1. PTZ カメラのライブビューのクイック設定ツールバーの をクリックします。
2. ライブビューの右下にある をクリックすると、プリセットの設定ができます。
3. ドロップダウンリストから、プリセット番号を選択します。
4. **Call** をクリックして呼び出すか、ライブビューの右下にある をクリックし、次に設定したプリセットをクリックして呼び出します。

図 3-13 プリセットを呼ぶ出す (1)

図 3-14 プリセットを呼ぶ出す (2)

3.6.4 パトロールを設定する

パトロールは、PTZ をキー ポイントに移動し、次のキー ポイントに移動する前に設定された時間内にそこに留まるよう設定できます。キーポイントはプリセットに対応しています。

ステップ

1. PTZ カメラのライブビューのクイック設定ツールバーの をクリックします。

2. **Patrol** をクリックして、パトロールの設定を行います。

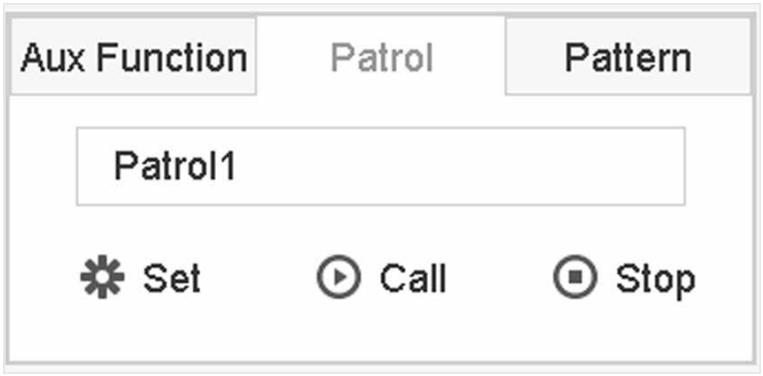


図 3-15 パトロールの設定

3. パトロール番号を選択します。
4. **Set** をクリックします

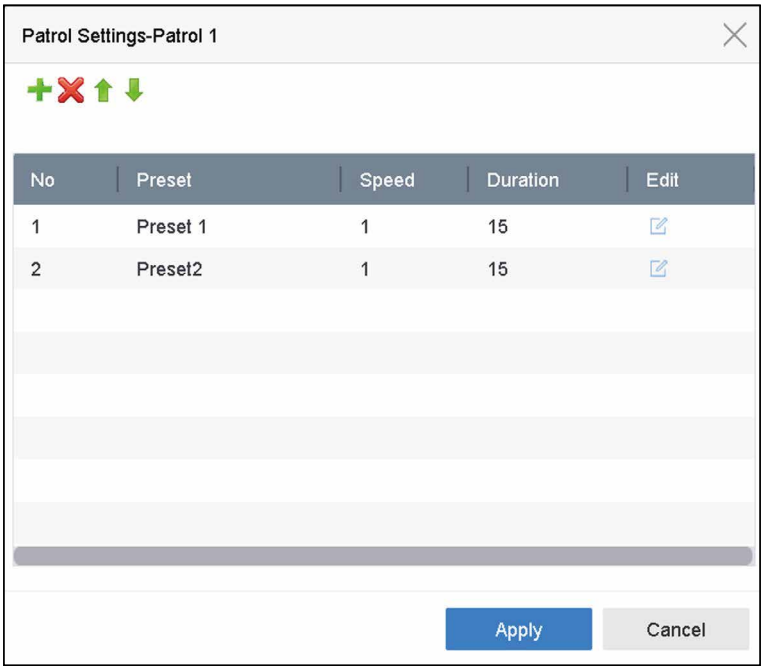


図 3-16 パトロールの設定

5. ✚ をクリックするとパトロールへキーポイントを追加できます。

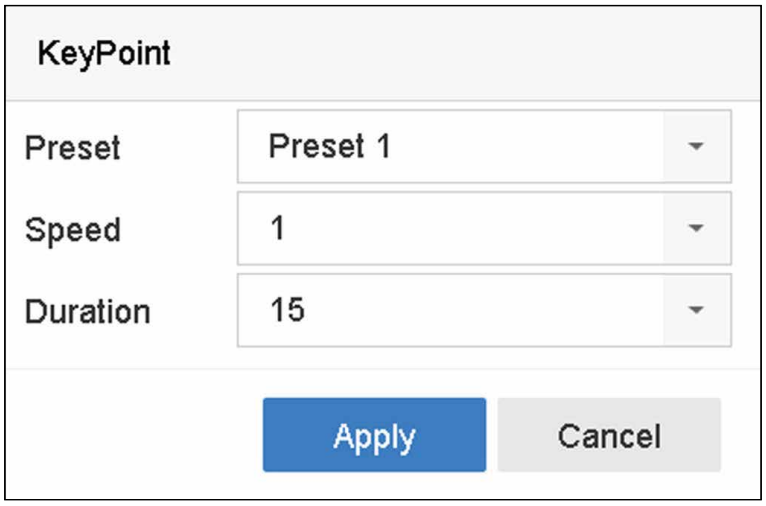


図 3-17 キーポイントの設定

1）キーポイントのパラメータを設定します。

Preset

PTZ が移動する際に従う順序を確定します。

Speed

PTZ があるキーポイントから次のキーポイントへ移動する速度を設定します。

Duration

対応するキーポイントに留まる時間を指します。

2）**Apply** をクリックして、パトロールへキーポイントを保存します。

6. その他の操作は以下の通りです。

表 3-1 操作説明

操作	説明	操作	説明
✖	削除するキーポイントを選択します。	✎	追加したキーポイントを編集します。
↑	キーポイントの順番を調整します。	↓	キーポイントの順番を調整します。

7. **Apply** をクリックして、パトロールの設定を保存します。

3.6.5 パトロールを呼び出す

パトロールを呼び出すと、あらかじめ設定されたパトロール経路に従って PTZ が移動します。

ステップ

1. PTZ カメラのライブビューのクイック設定ツールバーの をクリックします。
2. PTZ コントロールパネルの **Patrol** をクリックします。

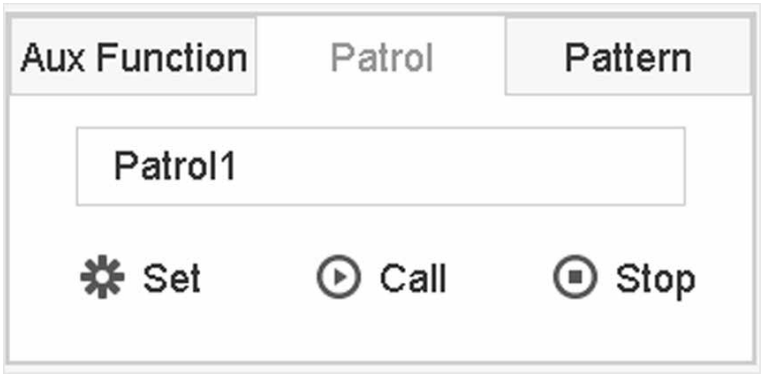


図 3-18 パトロールの設定

3. **Patrol** を選択します。
4. **Call** をクリックすると、パトロールを開始します。
5. オプション：**Stop** をクリックすると、パトロールを停止します。

3.6.6 パターンを設定する

PTZ の動きを記録することでパターンを設定することができます。パターンを呼び出すことで、あらかじめ設定された経路に従って PTZ を移動させることができます。

ステップ

1. PTZ カメラのライブビューのクイック設定ツールバーの をクリックします。
2. **Pattern** をクリックしてパターンを設定します。

図 3-19 パターン設定

3. パターン番号を選択します。

4. パターンを設定します。
   1）**Record** をクリックして録音を開始します。
   2) コントロールパネル上の対応するボタンをクリックして、PTZ カメラを移動します。
   3）**Stop** をクリックして録音を停止します。PTZ の動きがパターンとして記録されます。

3.6.7 パターンを呼び出す

あらかじめ設定されたパターンに従って、PTZ カメラを移動させる手順を説明します。

ステップ

1. PTZ カメラのライブビューのクイック設定ツールバーの をクリックします。
2. **Pattern** をクリックしてパターンを設定します。

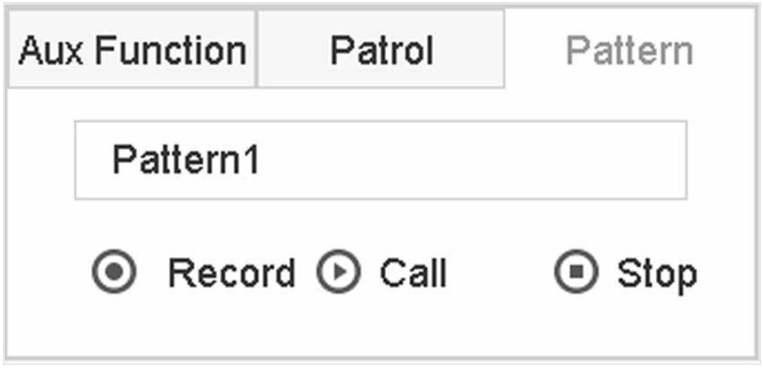


図 3-20 パターン設定

3. パターンを選択します。
4. **Call** をクリックして、パターンを開始します。
5. オプション：**Stop** をクリックしてパターンが停止します。

3.6.8 リニアスキャンリミットの設定

リニアスキャンはあらかじめ設定された範囲内で、水平方向にスキャンを実行します。

ご使用の前に

接続されている IP カメラが PTZ 機能に対応し、正しく接続されていることを確認してください。

メモ

本機能は一部の機種のみ対応しています。

ステップ

1. PTZ カメラのライブビューのクイック設定ツールバーの をクリックします。
2. 方向ボタンをクリックしてカメラを任意の場所に移動し、Left Limit または Right Limit をクリックして対応するリミットにその場所をリンクします。

メモ

スピードドームリニアは左リミットから右リミットまで走査しますので、左リミットを右リミットの左側に設定する必要があります。また、左リミットから右リミットへの角度は 180º 以下でなければなりません。

3.6.9 ワンタッチパーク

特定のスピードドームモデルでは、一定時間操作がない場合（パークタイム）、あらかじめ定義されたパークアクション（スキャン、プリセット、パトロールなど）を自動的に開始するように設定することができます。

ご使用の前に

この機能を使用する前に、接続するカメラがリニアスキャンに対応しており、HIKVISION プロトコルに対応していることを確認してください。

ステップ

1. PTZ カメラのライブビューのクイック設定ツールバーの をクリックします。
2. **Park (Quick Patrol)**、**Park (Patrol 1)**、または **Park (Preset 1)** をクリックして、パークアクションを有効にします。

   Park (Quick Patrol)

   このドームはパークタイム終了後、あらかじめ設定されたプリセット 1 からプリセット 32 まで順番にパトロールを開始します。未定義のプリセットはスキップされます。

   Park (Patrol 1)

   パークタイム終了後、あらかじめ設定されたパトロール 1 の経路に従ってドームが移動します。

   Park (Preset 1)

   パークタイム終了後、あらかじめ設定されたプリセット 1 の位置にドームが移動します。

   メモ

   パークタイムは、スピードドーム設定インターフェース経由でのみ設定できます。初期設定値は 5 秒です。

3. オプション：**Stop Park (Quick Patrol)**、**Stop Park (Patrol 1)**、または **Stop Park (Preset 1)** をクリックしてパークアクションを無効にできます。

3.6.10 補助機能

ライト、ワイパー、3D ポジショニング、センターなどの補助機能を PTZ コントロールパネルで操作することができます。

ご使用の前に

接続されている IP カメラが PTZ 機能に対応し、正しく接続されていることを確認してください。

ステップ

1. PTZ カメラのライブビューのクイック設定ツールバーの をクリックします。 インターフェースの右側に PTZ コントロールパネルが表示されます。
2. **Aux Function** をクリックします。

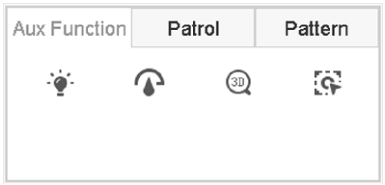


図 3-21 補助機能の設定

3. アイコンをクリックすると、補助機能を操作することができます。アイコンの説明については、表を参照してください。

図 3-2 補助機能アイコンの説明

アイコン	説明
	ライト on/off
	ワイパー on/off
	3D ポジショニング
	センター

第 4 章 録画と再生

4.1 録画

4.1.1 録画パラメーターを設定する

次の順に進みます。 Camera → Video Parameters.

Main Stream

メインストリームとは、ハードディスクドライブに記録されるデータに影響を与える主要なストリームのことで、記録画質や画像サイズを直接決定するものです。
サブストリームと比較すると、メインストリームは解像度やフレームレートが高く、より高品質な映像にすることができます。

Frame Rate (FPS - Frames per Second)

1 秒間に何枚のフレームをキャプチャするかということです。フレームレートが高いほど、映像に動きがある場合に画質を維持できるため有利です。

Resolution

画像解像度とは、デジタル画像にどれだけの詳細な情報を保持できるかを示すものです。解像度が高ければ高いほど、細部の表現力が高まります。解像度は、ピクセル列数（幅）×ピクセル行数（高さ）で指定することができます（例：1024 × 768）。

Bitrate

ビットレート（kbit/s または Mbit/s）は、しばしば速度と呼ばれますが、実際には距離 / 時間単位ではなく、ビット数 / 時間単位を定義しています。

Enable H.264+

H.264+ は、インテリジェント解析技術に予測符号化、ノイズ抑制、長期ビットレート制御を組み合わせ、低ビットレートを実現しており、ストレージコストの削減に大きな役割を果たすとともに、投資に対する高いリターンを提供することが可能です。

Enable H.265+

H.265+ は、標準的な H.265/HEVC 圧縮をベースに最適化したエンコーディング技術です。H.265+ では、H.265/HEVC とほぼ同じ映像品質でありながら、必要な伝送帯域とストレージ容量が少なくなっています。

メモ

- 解像度、フレームレート、ビットレートの設定を高くすると、より良い映像品質になりますが、より多くのインターネット帯域を必要とし、ハードディスクドライブの記憶領域をより多く使用します。
- H.264+ あるいは H.265+ エンコーディング技術は、一部の機種のみに対応しています。

Sub-Stream

サブストリームとは、メインストリームと並行して動作する第二のコーデックのことです。直接録画の画質を犠牲にすることなく、インターネットへの送信帯域を削減することができます。
サブストリームは、多くの場合、ライブ映像を見るためのアプリが独占的に使用します。この設定は、インターネットの速度が限られているユーザーにとって、最も有益なものです。

Picture

画像は、連続録画またはイベント録画でキャプチャされたライブ画像のことを指します。(**Storage → Capture Schedule → Advanced**)

Picture Quality

画質を低、中、高に設定します。画像の品質が高いほど、必要なストレージ容量も多くなります。

Interval

ライブ画像のキャプチャ間隔です。

Capture Delay Time

画像をキャプチャする時間です。

高度なパラメータの設定

ステップ

1. 次の順に進みます。**Storage → Schedule → Record**
2. **Enable Schedule** にチェックを入れて、予定された録画を有効にします。
3. **Advanced** をクリックして、高度なパラメータを設定します。

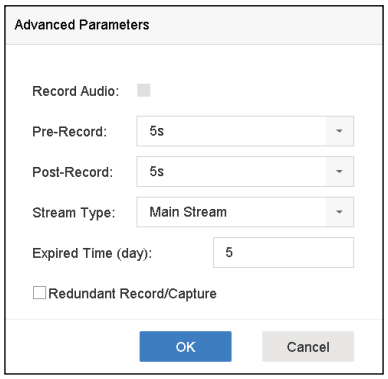


図 4-1 高度な録画設定

Record Audio

音声の録音を有効または無効にします。

Pre-record

予定時刻やイベントの前に録画するように設定した時間です。例:10時にアラームで録画が作動した場合、録画前時間を 5 秒に設定すると、9 時 59 分 55 秒から録画されます。

Post-record

イベント終了後に録画するように設定した時間、または予定された時間です。例：アラームが作動して 11 時に録画が終了した場合、録画後時間を 5 秒に設定すると、11 時 00 分 05 秒まで録画されます。

Stream Type

メインストリームとサブストリームを選択して録画することができます。サブストリームを選択すると、同じ保存容量でより長い時間録画することができます。

Expired Time

有効期限は、録画したファイルが HDD に保存される期間です。期限に達すると、ファイルは削除されます。有効期限を 0 に設定すると、ファイルは削除されません。ファイルの実保存時間は、HDD の容量によって決定されます。

Redundant Record/Capture

リダンダント記録またはキャプチャーを有効にすると、記録とキャプチャー画像をリダンダント HDD に保存することができます。

4.1.2 H.265 ストリームアクセスを有効にする

初回アクセス時は、IP カメラ（H.265 映像フォーマットに対応）の H.265 ストリームに自動的に切り替わります。
次の順に進み **Camera → More Settings → H.265 Auto Switch Configuration**、この機能を有効にします。

4.1.3 手動で録画する

をクリックすると、ライブビューでの録画を手動で開始 / 停止することができます。

4.1.4 録画スケジュールを設定する

設定した録画スケジュールに従って、カメラが自動的に録画を開始 / 停止します。

ご使用の前に

- ビデオファイル、ピクチャー、ログファイルを保存する前に、HDD を本機に取り付けたり、ネットワークディスクを追加していることを確認してください。
- Motion、Alarm、M | A (motion or alarm)、M & A (motion and alarm)、および 録画やキャプチャーした Event を有効にする前に、動体検知の設定やアラーム入力の設定、その他のイベントの設定を行う必要があります。詳しくは **VCA イベントアラーム**を参照してください。

ステップ

1. 次の順に進みます。**Storage → Schedule → Record**
2. カメラを選択します。
3. **Enable Schedule** にチェックを入れます。
4. 録画の種類を選択します。

   Continuous

   録画予約

   Event

   すべてのイベントトリガーアラームによって撮られた録画。

Motion

動体検知で撮られた録画。

Alarm

アラームで撮られた録画。

M/A

動体検知またはアラームで撮られた録画。

M&A

動体検知やアラームで撮られた録画。

POS

POS やアラームで撮られた録画。

5. タイムバー上のカーソルをドラッグして、録画スケジュールを設定します。

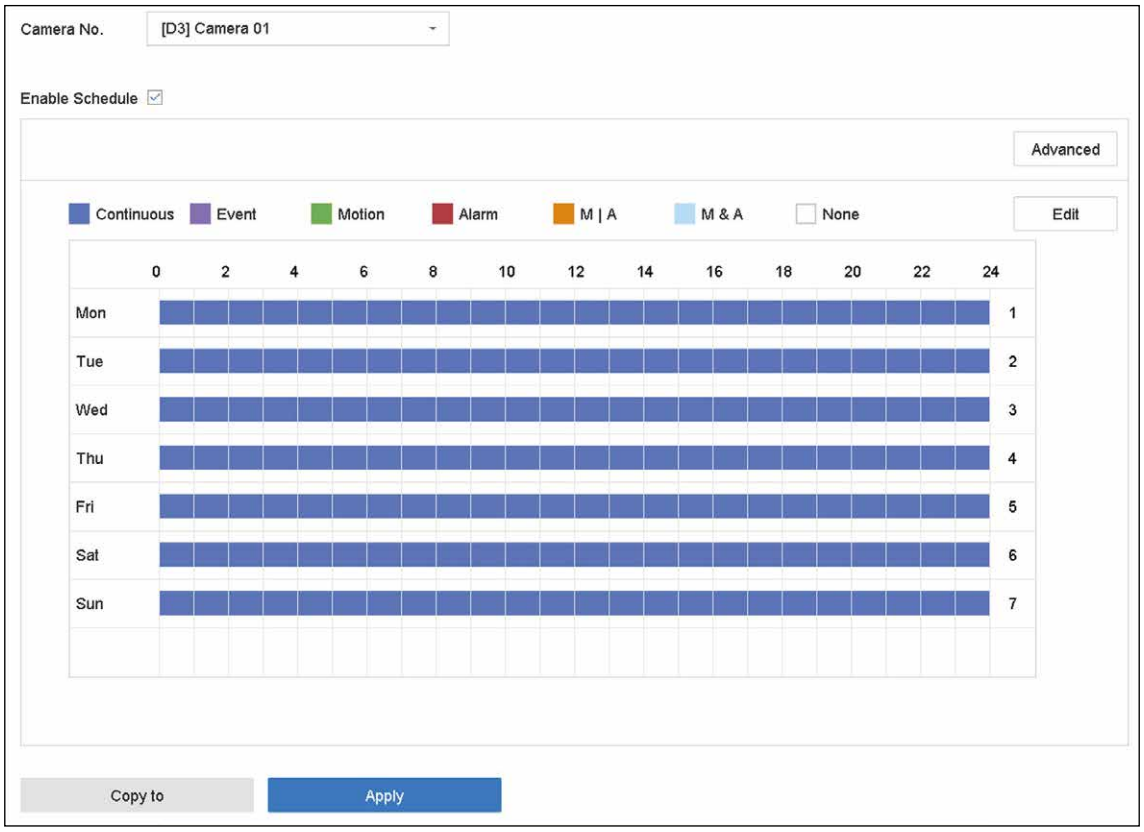


図 4-2 録画スケジュール

メモ

- 上記の手順を繰り返して、曜日ごとのスケジュール録画やキャプチャーを設定することができます。
- 初期設定では、1 日ごとに連続録画されます。

6. オプション：録画予約を他のカメラにコピーします。
   1）**Copy to** をクリックします。
   2) 同じスケジュール設定で複製するカメラを選択します。
   3) **OK** ボタンをクリックしてください。
7. **Apply** をクリックします。

4.1.5 連続録画の設定する

設定したタイムスケジュール内で連続的に録画することが可能です。

ステップ

1. 次の順に進みます。**Camera → Encoding Parameters → Recording Parameters**
2. カメラのメインストリーム／サブストリームの連続録画パラメーターを設定します。
3. 次の順に進みます。**Storage → Recording Schedule**
4. タイムバー上でマウスをドラッグして、連続録画スケジュールを設定します。**録画スケジュールを設定する**を参照してしてください。

4.1.6 動体検知トリガー録画の設定

動体検知イベントで作動する録画を設定することができます。

ステップ

1. 次の順に進みます。**System → Event → Normal Event → Motion Detection**
2. 動体検知を設定し、動体イベントが発生したときに録画を作動するチャンネル（複数可）を選択します。詳しくは**リンケージアクションの設定**を参照してください。
3. 次の順に進みます。**Camera → Encoding Parameters → Recording Parameters**
4. カメラのメインストリーム／サブストリームのイベント録画パラメーターを設定します。
5. 次の順に進みます。**Storage → Recording Schedule**
6. 録画の種類は **Motion** を選択します。
7. タイムバー上でマウスをドラッグして、動体検知スケジュールを設定します。**録画スケジュールを設定する**を参照してしてください。

4.1.7 イベントトリガー録画の設定

動体検知、動体検知とアラーム、顔検知、車両検知、ラインクロス検知などで作動する録画を設定することができます。

ステップ

1. 次の順に進みます。**System → Event**
2. イベント検知を設定し、イベントが発生したときに録画を作動するチャンネル（複数可）を選択します。詳しくは**イベント**を参照してください。
3. 次の順に進みます。**Camera → Encoding Parameters → Recording Parameters**
4. カメラのメインストリーム／サブストリームのイベント録画パラメーターを設定します。
5. 次の順に進みます。**Storage → Recording Schedule**

6. 録画の種類は **Event** を選択します。
7. タイムバー上でマウスをドラッグして、イベント検知の録画スケジュールを設定します。**録画スケジュールを設定する**を参照してしてください。

4.1.8 アラームトリガー録画の設定

動体検知、動体検知、顔検知、車両検知、ラインクロス検知などで作動する録画を設定することができます。

ステップ

1. 次の順に進みます。**System → Event → Normal Event → Alarm Input**
2. アラームインプットを設定し、アラームが発生したときに録画を作動するチャンネル（複数可）を選択します。詳しくは**イベント**を参照してください。
3. 次の順に進みます。**Camera → Encoding Parameters → Recording Parameters**
4. カメラのメインストリーム／サブストリームのイベント録画パラメーターを設定します。
5. 次の順に進みます。**Storage → Recording Schedule**
6. 録画の種類は **Alarm** を選択します。
7. タイムバー上でマウスをドラッグして、アラーム録画スケジュールを設定します。**録画スケジュールを設定する**を参照してしてください。

4.1.9 画像キャプチャーの設定

画像は、連続録画またはイベント録画でキャプチャされたライブ画像のことを指します。この機能は一部の機種のみ対応しています。

ステップ

1. 次の順に進みます。**Camera → Encoding Parameters → Capture**
2. 画像パラメータを設定します。

   Resolution

   キャプチャする画像の解像度を設定します。

   Picture Quality

   画質を低、中、高に設定します。画像の品質が高いほど、必要なストレージ容量も多くなります。

   Interval

   ライブ画像のキャプチャ間隔です。
3. 次の順に進みます。**Storage → Capture Schedule**
4. 画像キャプチャーを設定するカメラを選択します。
5. キャプチャスケジュールを設定します。**録画スケジュールを設定する**を参照してしてください。

4.1.10 休日録画を設定する

休日には別の録画プランが必要な場合があります。この機能により、その年の休日の録画スケジュールを設定することができます。

ステップ

1. 次の順に進みます。**System → Holiday**
2. リストから休日の項目を選択します。
3. をクリックして、選択した祝日を編集します。
4. **Enable** にチェックを入れます。

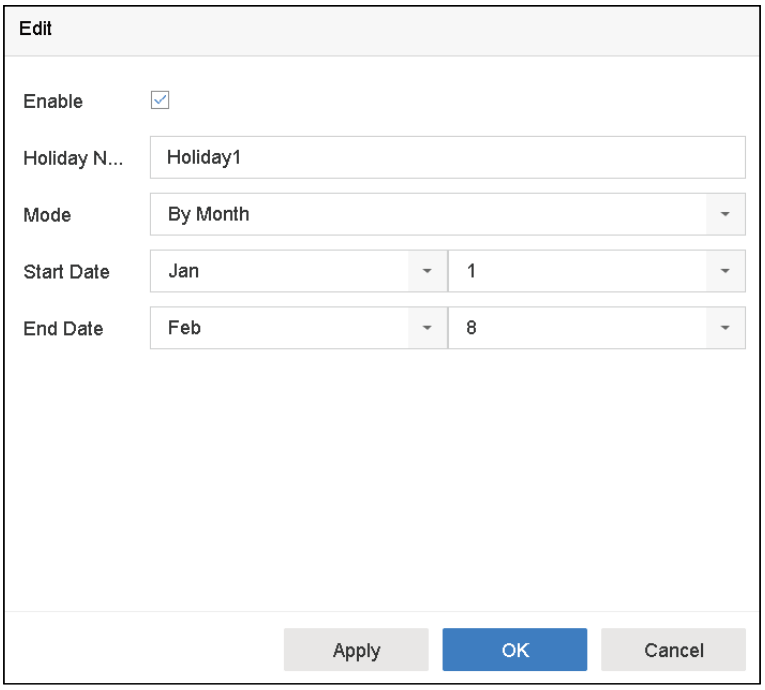


図 4-3 休日設定の編集

5. **Holiday Name**、**Mode**、**Start Date**、**End Date** を設定します。
6. **OK** ボタンをクリックします。
7. 休日キャプチャスケジュールを設定します。詳しくは**録画スケジュールを設定する**を参照してしてください。

4.1.11 録画とキャプチャーの冗長化設定

記録ファイルやキャプチャー画像を R/W HDD だけでなく冗長 HDD にも保存する冗長記録・キャプチャーを可能にすることで、データの安全性と信頼性を効果的に向上させることができます。

ご使用の前に

HDD のプロパティを **Redundancy** に設定する前に、ストレージモードを **Group** に設定する必要があります。詳細については **HDD グループの設定**を参照してください。少なくともう 1 台、Read/Write の HDD があることを確認してください。

ステップ

1. 次の順に進みます。**Storage → Storage Device**
2. 一覧から HDD を選択し をクリックして Local HDD Settings インターフェースに入ります。
3. HDD のプロパティを **Redundancy** に設定します。
4. 次の順に進みます。**Storage → Schedule Settings → Record Schedule/Capture Schedule**
5. **Advanced** をクリックして、カメラ録画パラメータを設定します。

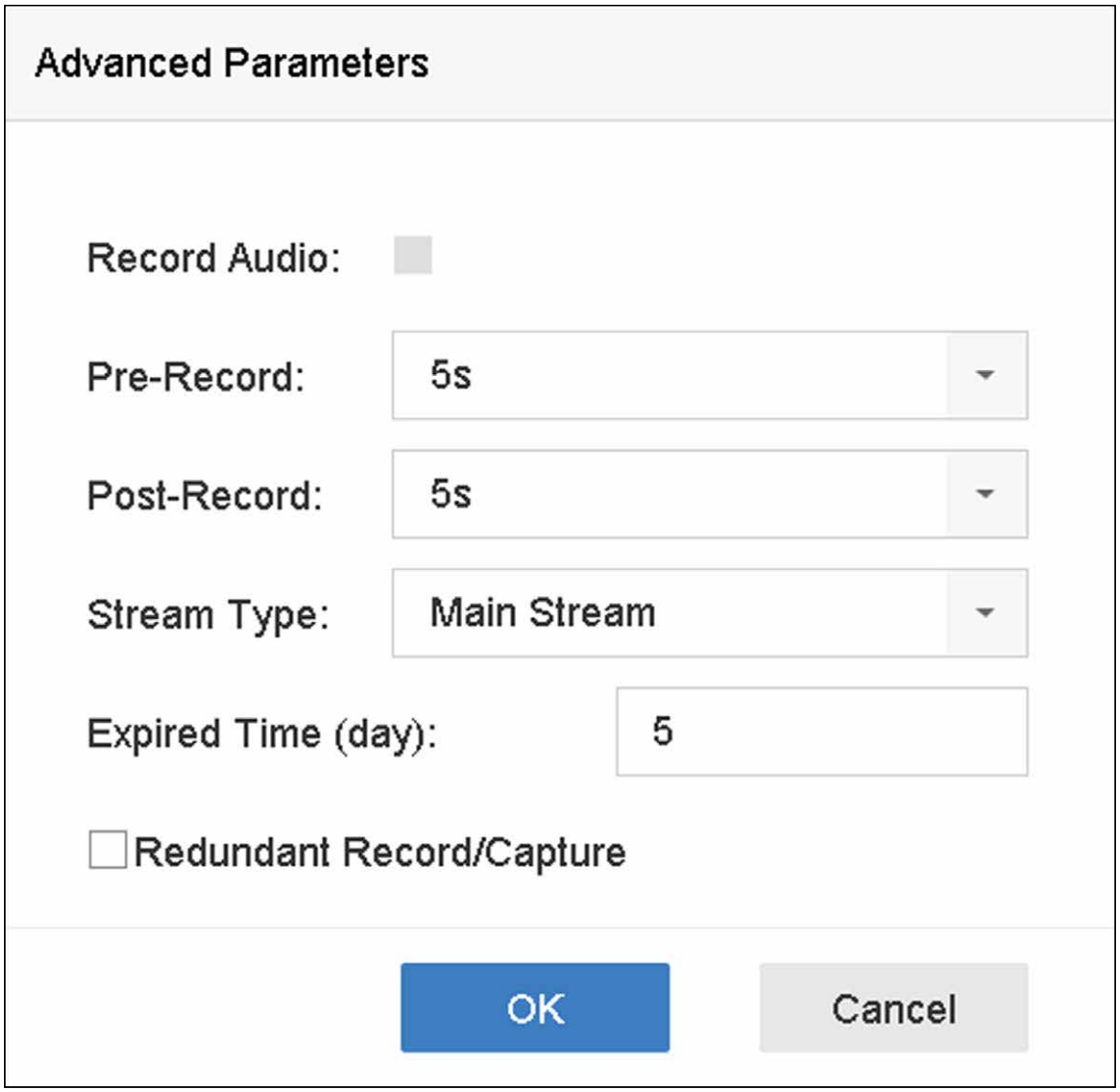


図 4-4 録画パラメータ

6. **Redundant Record/Capture** にチェックを入れます。
7. **OK** ボタンをクリックして、設定を保存します。

4.1.12 1080p Lite モードの設定

1080P Lite モードが有効な場合、1080P Lite（リアルタイム）でのエンコード解像度に対応します。そうでない場合は、1080P（非リアルタイム）までの対応となります。
Storage → Advanced に進み、**1080P Lite Mode** を有効または無効に設定します。

4.2 再生

4.2.1 インスタント再生

インスタント再生は、直近 5 分間に記録された録画ビデオファイルを再生することができます。映像が見つからない場合は、直近 5 分間の録画がないことを意味します。

Live View でカメラを選択した後、ウィンドウの下部にカーソルを移動して、ツールバーにアクセス、 をクリックすると、インスタント再生が開始されます。

図 4-5 再生

4.2.2 通常の動画を再生する

Playback に進み、日付とカメラを選択します（複数可）。 1 4 8 9 16 は、カメラをグループ化したり、動画を再生するためのウィンドウ分割ショートカットです。また、リストからカメラを選択して、複数のカメラの同時再生も可能です。

再生ウィンドウにカーソルを合わせ、下部のツールバーで再生操作を行います。詳しくは**再生操作**を参照してください。

メモ

256 倍速再生に対応しています。

図 4-6 通常の動画の再生

4.2.3 スマート検索された動画を再生する

スマート再生モードでは、動体検知、ラインクロス及び侵入検知の情報が含まれる動画を解析し、赤色でマークすることができます。

Playback に進み、**Smart** をクリック、次に動体検知 ( )、ラインクロス ( )、または侵入検知 ( ) をクリックすると、見たい動画を再生することができます。

人物および車両の動体検知を有効にしている一部のカメラでは、 または をクリックして、人物や車のターゲットを探索します。人物または車のターゲットを含む動画を再生している場合、本機は動画（人物または車のターゲットを含む）をラインクロス検知 ( ) または侵入検知 ( ) の二重解析はできません。

図 4-7 スマートサーチによる再生

4.2.4 カスタム検索されたファイルを再生する

カスタム検索で動画を再生することができます。

ステップ

1. **Playback** に進みます。
2. リストからカメラ（複数可）を選択します。
3. 左下角の **Custom Search** をクリックします。
4. 検索方法を選択します。例：**Appearance で検索**を選択します。
5. 検索条件を設定します。
6. **Start Search** をクリックします。検索結果リストには、1 チャンネルが表示されます。
7. **Channel** をクリックして、見たいチャンネルを選択します。選択したチャンネルの検索結果が表示されます。
8. オプション： をクリックすると動画が再生されます。
9. をクリックしてファイルをロックします。ロックされたファイルは、上書きされません。
10. オプション：検索結果をバックアップデバイスにエクスポートします。
    1) 検索結果一覧からファイルを選択するか、または **Select All** をクリックすると、すべてのファイルが選択されます。
    2）クリック **Export** をクリックして、選択したファイル (複数）をバックアップデバイスにエクスポートします。

メモ

- をクリックすると、エクスポートの進行状況が表示されます。
- をクリックすると、検索インターフェースに戻ります。

4.2.5 タグファイルを再生する

ビデオタグは再生中に、ある時点の人物や場所などの情報を記録することができます。ビデオタグ（複数可）を使用して、ビデオファイルや位置の時点を検索することができます。

タグファイルの追加

ステップ

1. **Playback** に進みます。
2. ビデオファイル（複数）を検索し、再生します。
3. をクリックしてタグを追加します。
4. タグ情報を編集します。
5. **OK** ボタンをクリックします。

メモ

最大 1 つのビデオファイルに最大 64 個のタグを追加することができます。

タグファイルを再生する

ステップ

1. **Playback** に進みます。
2. 左下の **Custom Search** をクリックします。
3. 時間やタグのキーワードを含む検索条件を入力します。

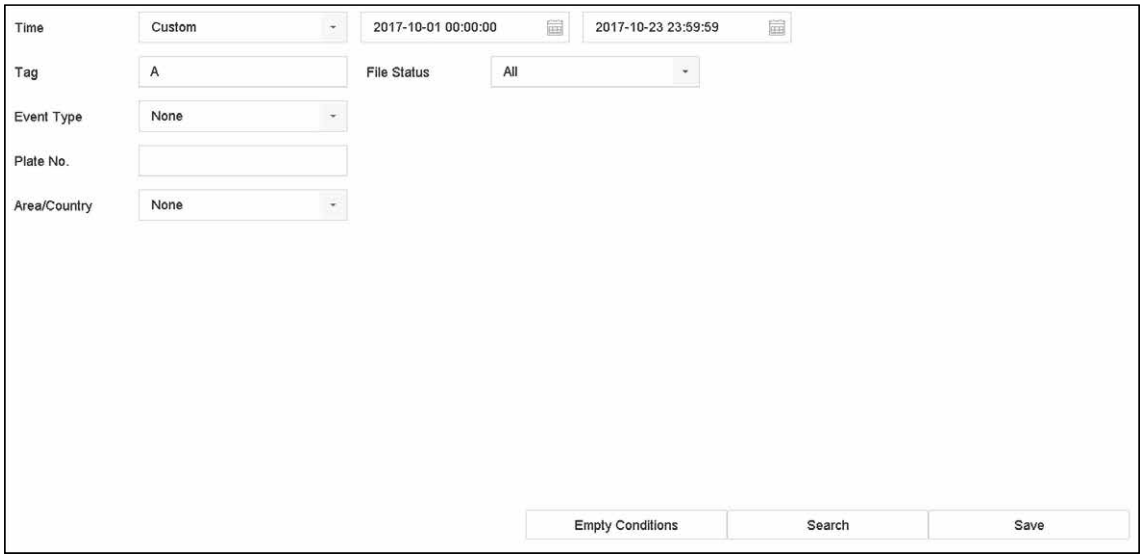


図 4-8 タグ検索

4. **Search** をクリックします。

図 4-9 検索されたタグファイル

5. タグファイルを選択し、検索結果のインターフェイスで動画を再生します。

4.2.6 サブピリオドで再生する

ビデオファイルは、画面上で複数のサブピリオドを同時に再生することができます。

ステップ

1. **Playback** に進みます。
2. 左下の ⊞ をクリックします。
3. カメラを選択します。
4. ビデオの検索開始時刻と終了時刻を設定します。
5. 右下の異なる時間帯を選択します（例：4-Period）。

メモ

定義された分割画面数に従って、選択された日付のビデオファイルを平均的に分割して再生することができます。例：16:00 ～ 22:00 に存在するビデオファイルがあり、6 画面表示モードを選択した場合、各画面で 1 時間ずつ同時に再生することができます。

4.2.7 ログファイルを再生する

システムログを検索し、チャンネルに関連する録画ファイル（複数可）を再生する。

ステップ

1. 次の順に進みます。**Maintenance → Log Info**
2. **Log Search** をクリックします。
3. 検索時間や種類を設定し、**Search** をクリックします。

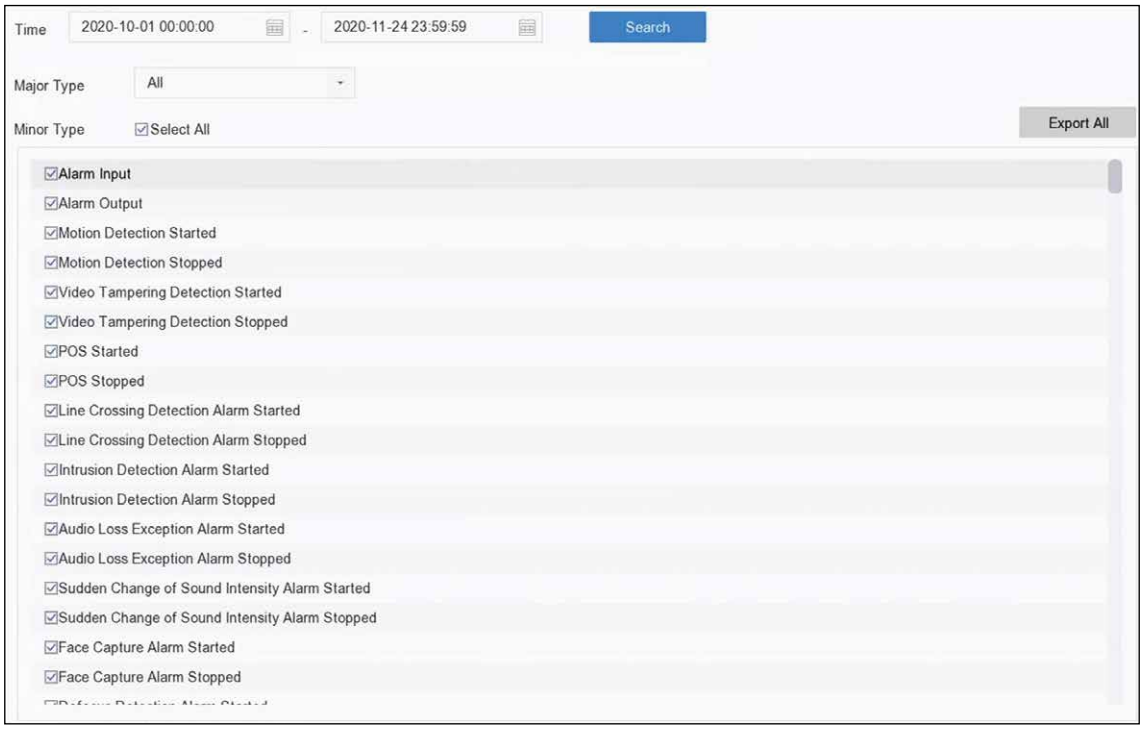
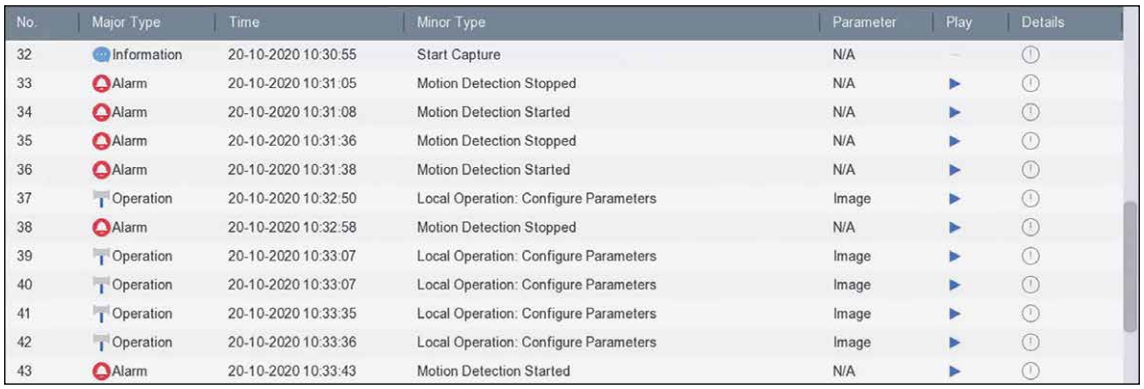


図 4-10 ログファイルの検索

4. 動画ファイルのあるログを選び、クリックするとログファイルの再生が始まります。



No.	Major Type	Time	Minor Type	Parameter	Play	Details
32	Information	20-10-2020 10:30:55	Start Capture	N/A		
33	Alarm	20-10-2020 10:31:05	Motion Detection Stopped	N/A		
34	Alarm	20-10-2020 10:31:08	Motion Detection Started	N/A		
35	Alarm	20-10-2020 10:31:36	Motion Detection Stopped	N/A		
36	Alarm	20-10-2020 10:31:38	Motion Detection Started	N/A		
37	Operation	20-10-2020 10:32:50	Local Operation: Configure Parameters	Image		
38	Alarm	20-10-2020 10:32:58	Motion Detection Stopped	N/A		
39	Operation	20-10-2020 10:33:07	Local Operation: Configure Parameters	Image		
40	Operation	20-10-2020 10:33:07	Local Operation: Configure Parameters	Image		
41	Operation	20-10-2020 10:33:35	Local Operation: Configure Parameters	Image		
42	Operation	20-10-2020 10:33:36	Local Operation: Configure Parameters	Image		
43	Alarm	20-10-2020 10:33:43	Motion Detection Started	N/A		

図 4-11 ログファイルの再生

4.2.8 外部ファイルを再生する

外部ストレージデバイスのファイルを再生することができます。

ご使用の前に

ビデオファイルが保存されているストレージデバイスを本機に接続します。

ステップ

1. **Playback** に進みます。
2. 左下の をクリックします。
3. をクリックするか、ファイルをダブルクリックして再生します。

4.3 再生操作

4.3.1 ノーマル / スマート / カスタム動画

再生時に、以下の 3 つのモードを選択して動画を再生することができます。

Normal

連続録画の動画ファイル。

Smart

イベントやアラームで作動した録画による動画ファイル。

Custom

カスタム条件で検索された動画ファイル。

4.3.2 重要 / カスタムモードでのプレイストラテジーの設定

スマート動画やカスタム動画の再生モードでは、ノーマル動画とスマート / カスタム動画で別々に再生速度を設定したり、ノーマル動画をスキップするように選択することができます。
スマート / カスタムビデオ再生モードでは、 をクリックして再生ストラテジーを設定します。

- **Do not Play Normal Videos** にチェックを入れると、ノーマル動画をスキップして、スマート（動体 / ラインクロス / 侵入）動画およびカスタム（検索された動画）のみを通常速度（X1）で再生します。
- **Do not Play Normal Videos** のチェックを外すと、ノーマル動画とスマート / カスタム動画の再生速度を別々に設定できます。滞留時間の範囲は X1 から XMAX です。

メモ

速度の設定は、1 チャンネル再生モード時のみ可能です。

4.3.3 ビデオクリップを編集する

再生中にビデオクリップをカットしてエキスポートすることができます。

ステップ

1. **Playback** に進みます。
2. 下のツールバーの をクリックします。
3. 開始時刻と終了時刻を設定します。 をクリックで時間帯を設定するか、タイムバーの時間区分を設定します。
4. をクリックして、ビデオクリップをストレージデバイスに保存します。

4.3.4 メインストリームとサブストリームの切り替え

再生中にメインストリームとサブストリームの切り替えが可能です。

アイコン	説明
	メインストリームで動画を再生する。
	サブストリームで動画を再生する。

メモ

メインストリームとサブストリームのエンコーディングパラメータは、**Storage → Encoding Parameters** で設定できます。

4.3.5 サムネイルビュー

再生インターフェースのサムネイル表示で、タイムバーの必要なビデオファイルを便利に見つけることができます。
再生モードでは、タイムバー上にカーソルを置くと、プレビューサムネイルが表示されます。

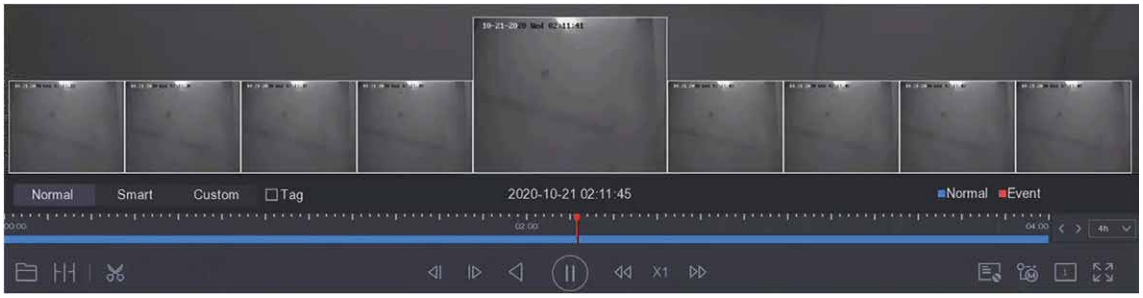


図 4-12 サムネイルビュー

サムネイルをクリックすると、フルスクリーン再生に入ることができます。

4.3.6 早送り

マウスを押したままタイムバー上をドラッグすると、動画ファイルの早送りになります。
動画再生モードでは、マウスをホールドしたまま再生タイムバーをドラッグすると、動画ファイルの早送りが表示されます。
必要なタイミングでマウスを離すと、フルスクリーン再生になります。

4.3.7 デジタルズーム

デジタルズームは、ライブ映像を異なる倍率（1 倍～ 16 倍）で拡大表示します。

ステップ

1. ライブビューを開始します。
2. ツールバーの をクリックします。
3. スライドバーを動かすか、マウスホイールをスクロールすることで、異なる倍率（1 倍～ 16 倍）に画像を拡大・縮小することができます。

図 4-13 デジタルズーム

第 5 章 スマート解析

メモ

このセクションの機能は、特定のモデルでのみ使用できます。

5.1 エンジン設定

各エンジンは、指定された VCA タイプを作業モードとして処理します。エンジンの動作モードは任意に設定できます。

ステップ

1. 次の順に進みます。**Smart Analysis → Engine Settings → Engine Configuration**

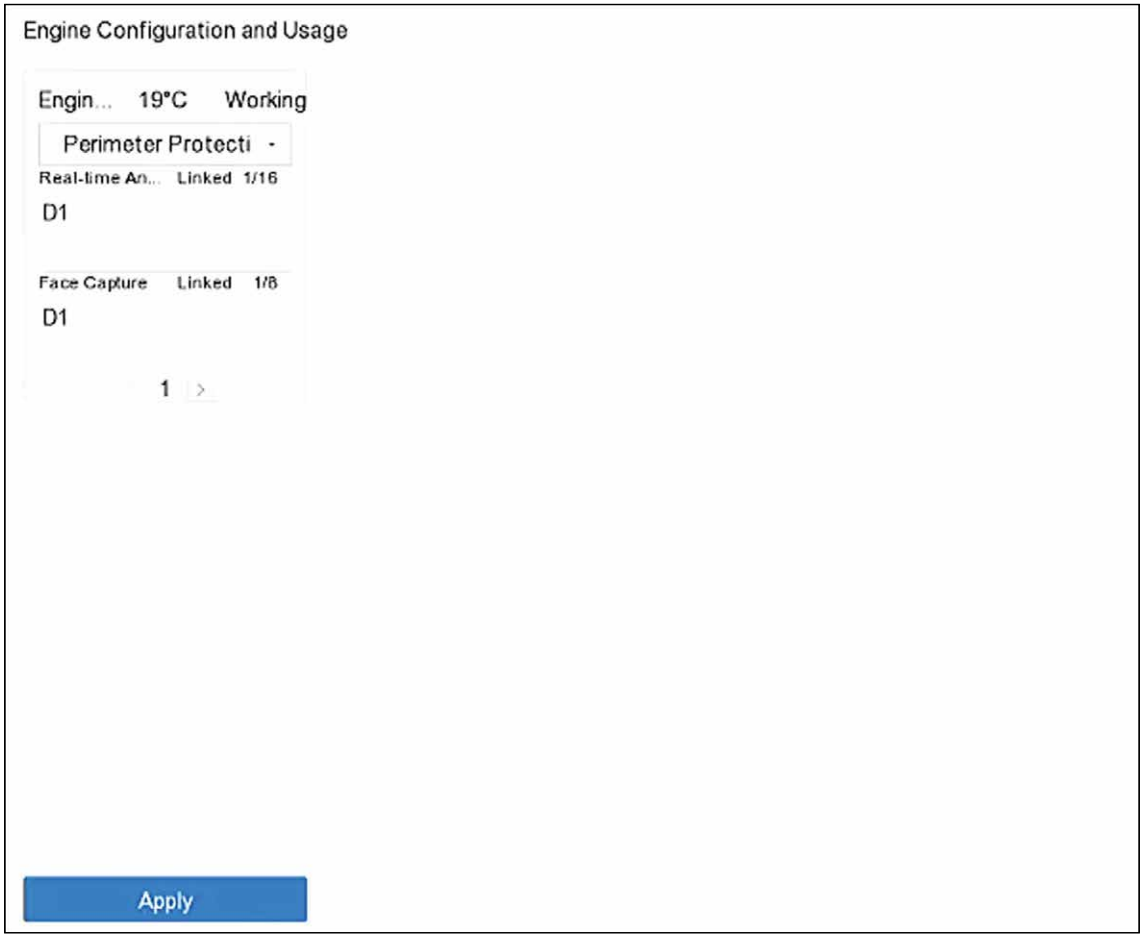


図 5-1 エンジン設定

2. 各エンジンの使用方法を設定します。各機能のエンジン温度や連動するチャンネルのステータスを確認することができます。

メモ

エンジンがチャンネル（複数可）とバインドされている場合、エンジンの作業モードを切り替えるとエンジンとチャンネルのバインドが解除され、チャンネルの関連スマートイベントがキャンセルされます。

3. **Apply** をクリックして、設定を保存します。

5.2 タスク設定

タスクのステータスはタスク設定で確認することができます。スマート解析の結果は、興味を引く人物や乗り物の画像を検索する際のフィルタリングに利用されます。

ご使用の前に

人体検知 / 車両検知、ラインクロス検知、侵入検知、領域入口、領域出口の Save VCA Pictures にチェックを入れます。

ステップ

メモ

この章は、iDS シリーズの一部の機種にのみ適用されます。

1. 次の順に進みます。**Smart Analysis → Smart Analysis → Task Configuration**
2. カメラにチェックを入れ、対応する解析モードを有効にします。選択した解析モードでエンジンが利用可能であることを確認してください。
3. 自動解析を有効にします。

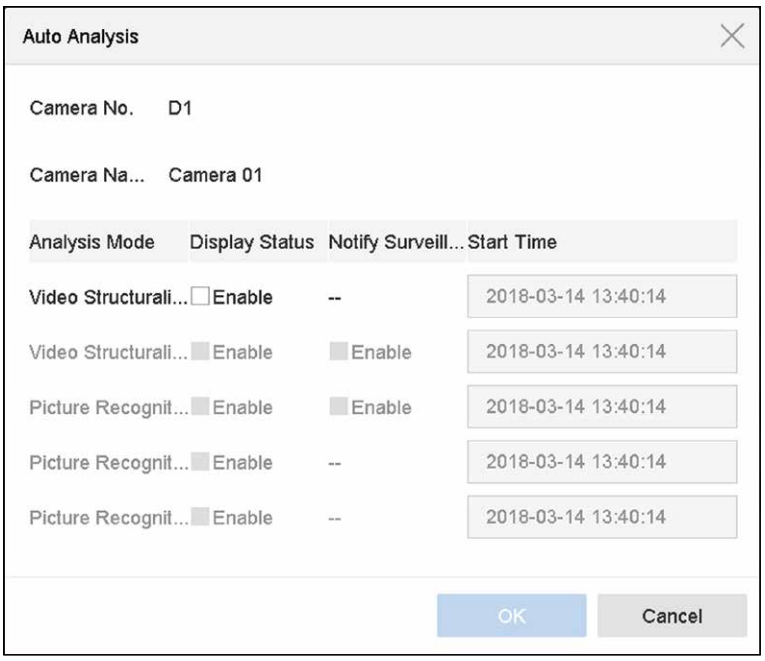


図 5-2 自動解析

1) **Edit** をクリックします。
2) オプション：Enable of Display Status と Notify Surveillance Center にチェックを入れます。
3) 解析する動画の **Start Time** を設定してください。
4) **OK** ボタンをクリックしてください。

4. カメラにチェックを入れ、Enabled をクリックすると解析を開始します。
   タスクステータスには Disabled、Waiting、Enabled の 3 つの状態があります。
   - **Disabled**：カメラで解析タスクが有効になっていません。
   - **Waiting**：カメラの解析タスクが有効になっています。デバイスはデータ解析待ちです。
   - **Enabled**：カメラの解析タスクが有効で、デバイスがカメラのデータを解析しています。
5. オプション：非リアルタイム顔画像比較解析モードでは、**View Record** をクリックすると、1 日ごとの経過が表示されます。

5.3 エンハンスド VCA モードの設定

エンハンスト VCA モードを有効にすることで、ラインクロス検出や侵入検知のための接続可能なチャンネル数を最大化することができます。ただし、HUHI-K シリーズの 2K/4K HDMI 出力解像度と 4MP/5MP/8MP 信号入力は無効となります。また、HQHI-K シリーズでは、CVBS 出力とチャンネルゼロエンコーディングを無効にします。
次の順に進み **System → General、Enhanced VCA Mode** にチェックを入れてください。

5.4 顔画像比較

本機は顔画像比較アラームや顔認識機能に基づく接続カメラの顔キャプチャに対応しています。
次の順に進みます。**Smart Analysis → Smart Analysis → Engine Configuration** 少なくとも 1 つのエンジン用途を顔認証に設定してください。詳しくは**エンジン設定**を参照してください。

メモ

この章は、iDS シリーズの一部の機種にのみ適用されます。

5.4.1 顔検知

顔検知は、監視映像に現れる顔を検知するものです。人物の顔が検知されると、リンケージアクションが作動します。

ステップ

1. 次の順に進みます。**System → Event → Smart Event**
2. **Face Detection** をクリックします。

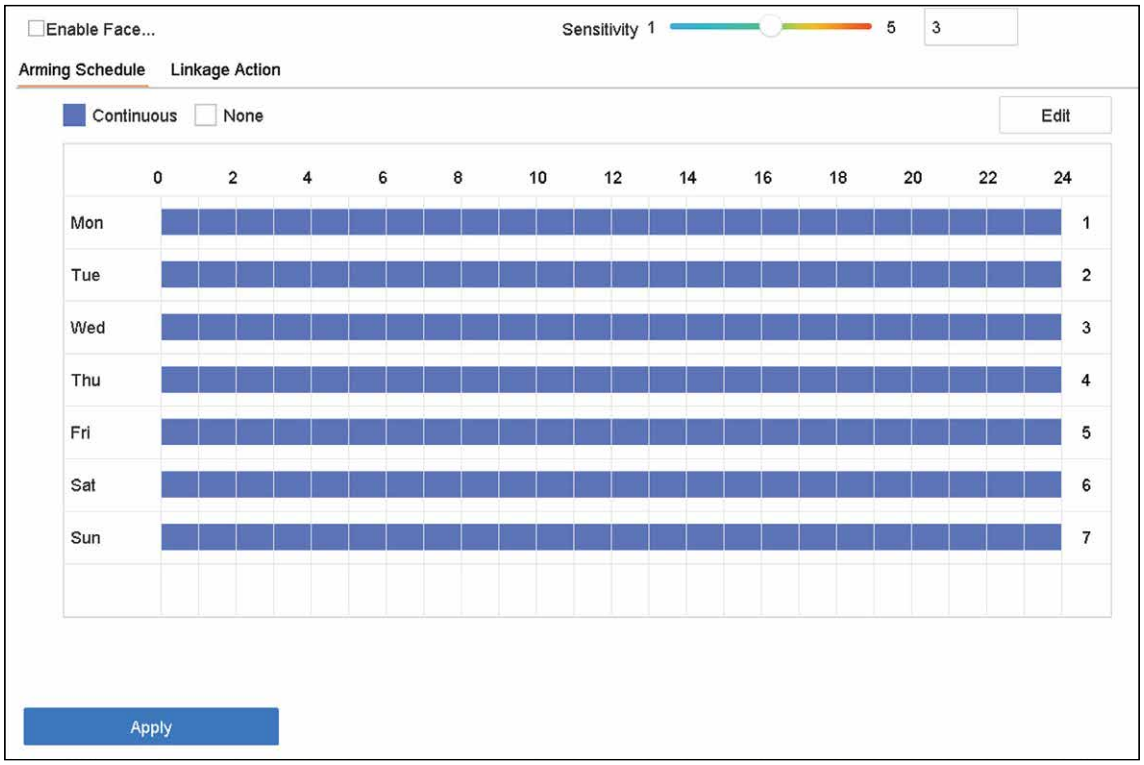


図 5-3 顔検知

3. 設定するカメラを選択します。
4. **Enable Face Detection** にチェックを入れます。
5. オプション：**Save VCA Picture** にチェック を入れると、顔検知のキャプチャー画像が保存されます。
6. 検知感度を設定します。感度の範囲 [1-5] 値が大きいほど、顔の検知がしやすくなります。
7. アーミングスケジュールを設定します。**アーミングスケジュールの設定**を参照してください。
8. リンケージアクションを設定します。**リンケージアクションの設定**を参照してください。
9. **Apply** をクリックします。

5.4.2 顔画像ライブラリー管理

顔画像ライブラリーは、主に顔画像の保存と顔画像の比較に使用されます。

顔画像ライブラリーの追加

ローカル GUI や Hik-Connect アプリから顔画像ライブラリーを作成することができます。ここでは、ローカル GUI の操作を例にとって説明します。

ステップ

1. 次の順に進みます。**Smart Analysis → Face Picture Database**
2. ＋ をクリックします。
3. 顔画像ライブラリーの名前を入力します。
4. **OK** ボタンをクリックします。

メモ

または をクリックすると、ライブラリ名を編集したり、ライブラリーを削除したりすることができます。

顔画像ライブラリーへのアップロード

顔画像の比較は、ライブラリーにある顔画像をもとに行います。顔画像 1 枚をアップロードすることも、複数の顔画像をライブラリーにインポートすることもできます。

ご使用の前に

- 画像形式が JPEG または JPG であることを確認してください。
- それぞれの画像につき、顔が 1 つだけであることを確認してください。
- あらかじめすべての画像をバックアップデバイスにインポートしておいてください。

ステップ

1. リストから顔画像ライブラリーを選択します。
2. **Add** または **Import Face Picture Library** をクリックします。
3. 画像（複数可）をインポートしてください。
   - **Add**：インポートする画像を選択し、**Import** をクリックします。
   - **Import Face Picture Library**：インポートする複数の画像を選択し、**Import** をクリックします。
4. オプション：画像を選択し、**Copy to** をクリックすると、現在のライブラリにアップロードされている画像が他のライブラリーにコピーされます。
5. オプション：画像を選択し、**Edit** をクリックして画像情報を修正します。
6. オプション：リストから画像を選び、**Delete** をクリックすると、その画像が削除されます。
7. オプション:ライブラリーを選択し、**Export Face Picture Library** をクリックすると、ライブラリーがバックアップデバイスにエクスポートされます。
8. オプション：または をクリックすると、図や一覧で表示されます。

5.4.3 顔画像比較の設定

検知された顔画像を指定された顔画像ライブラリーと比較します。比較に成功した場合、アラームが作動します。

ステップ

1. 次の順に進みます。**System → Event → Smart Event → Face Picture Comparison**

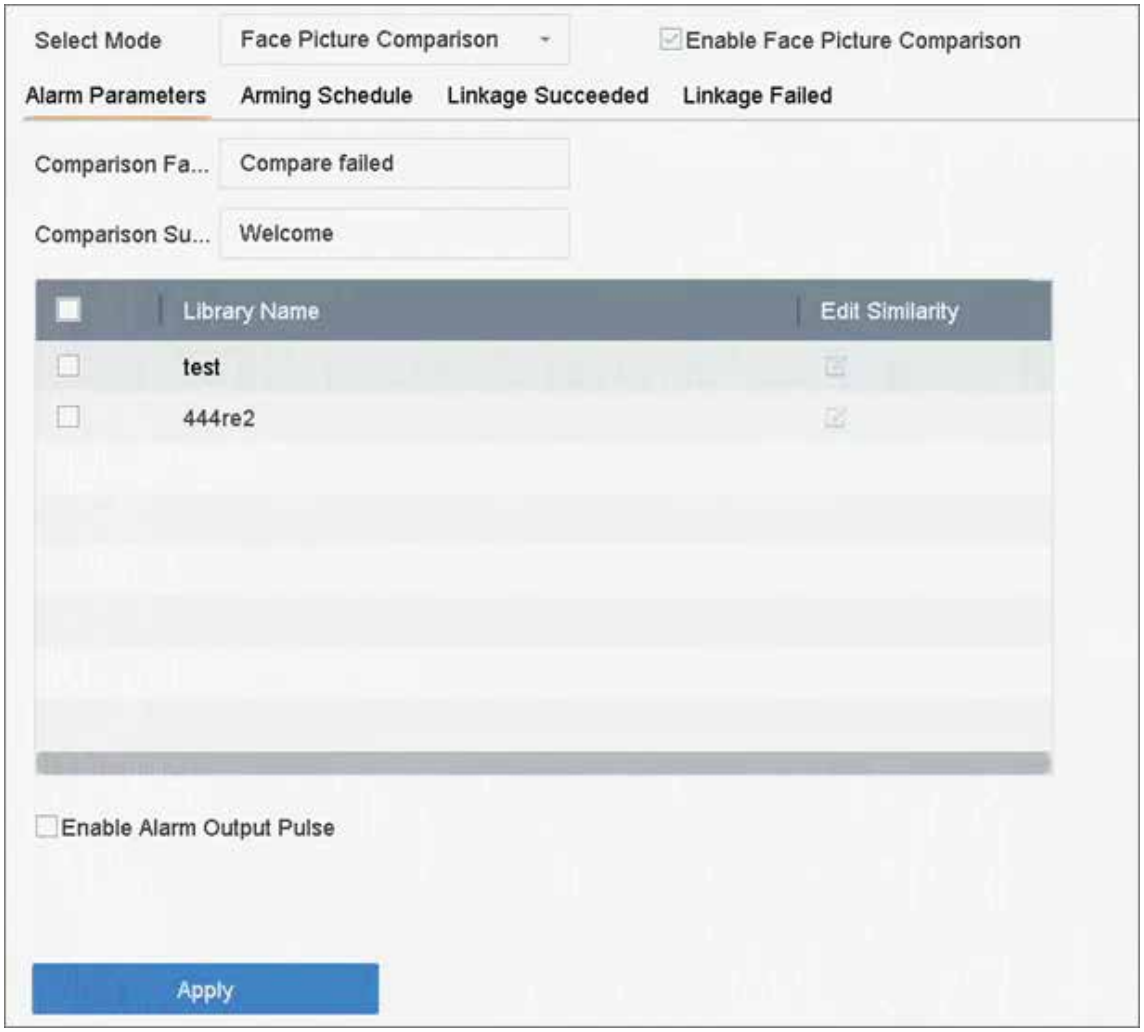


図 5-4 顔画像比較

2. カメラを選択します。
3. **Mode** は **Face Picture Comparison** を選択します。
4. **Enable Face Picture Comparison** にチェックを入れます。
5. オプション：**Comparison Failed Prompt**、**Comparison Succeeded Prompt**、**Enable Alarm Output Pulse** を設定します。

Comparison Failed Prompt

顔画像比較に失敗すると、ライブビューの **Target Detection** (チェック済 **Facial Detection**) または **Facial Recognition** にプロンプトを表示します。ライブビューの をクリックすると顔認識インターフェイスに入ります。

Comparison Succeeded Prompt

顔画像比較が成功すると Facial Recognition にプロンプトが表示されます。ライブビューの をクリックすると顔認識インターフェイスに入ります。

Enable Alarm Output Pulse

通常、ゲートと連動しています。人がゲートを通過するとき、比較に成功すればゲートを開けるためのパルスが作動します。パルスは 100 ～ 900ms です。**System → Event → Normal Event → Alarm Output** で **Alarm Output Pulse (ms)** を設定することができます。

6. 顔画像ライブラリーを選択し、類似性を設定します。
7. アーミングスケジュールを設定します。**アーミングスケジュールの設定**を参照してください。
8. 顔画像比較に成功した場合と失敗した場合の連動動作を設定します。**リンケージアクションの設定**を参照してください。
9. **Apply** をクリックして、設定を保存します。

5.4.4 顔画像検索

Face Picture Comparison Event で検索する

顔画像比較結果で顔画像を検索します。

ステップ

1. 次の順に進みます。**Smart Analysis → Smart Search → Face Search → Search by Event**
2. 開始時刻と終了時刻を設定します。
3. チャンネルを選択します。
4. **Event Type** は **Face Picture Comparison** を選択します。
5. **Start Search** をクリックします。検索結果リストには、1 チャンネルが表示されます。
6. **Channel** をクリックして、見たいチャンネルを選択してください。選択したチャンネルの検索結果が表示されます。

次は

検索結果の表示を参照してください。

アップロードされた画像で検索

アップロードされた画像から顔画像を検索できます。

ステップ

1. 次の順に進みます。**Smart Analysis → Smart Search → Face Search → Search by Picture**

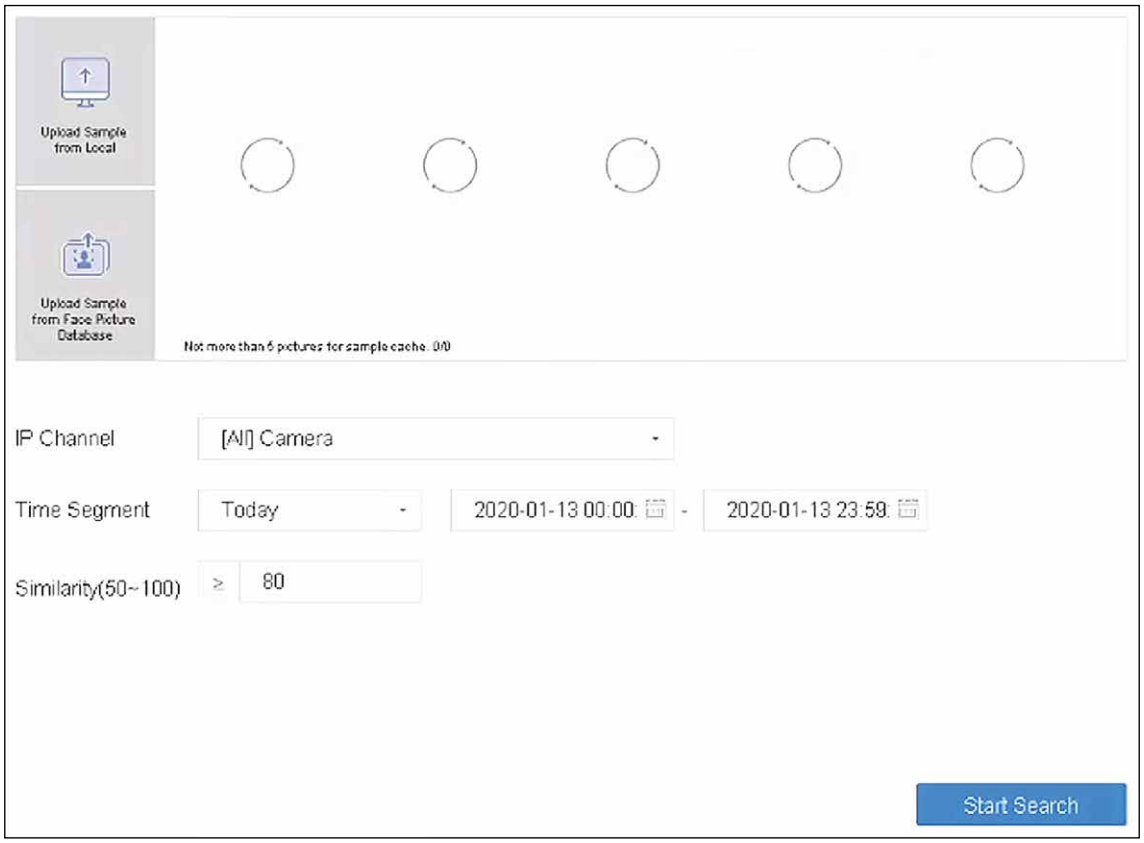


図 5-5 アップロードされた画像で検索

2. チャンネルを選択します。
3. 検索する顔画像を選択します。
   - **Upload Sample from Local** をクリックし、ローカルディレクトリから顔画像を選択します。
   - **Upload Sample from Face Picture Database** をクリックし、作成された顔画像ライブラリーから顔画像を選択します。
4. 開始時刻と終了時刻を設定します。
5. **Similarity** 値（範囲：:0 ～ 100）を設定します。サンプルとライブラリーの顔画像の類似度を解析し、設定した類似度より高い画像を表示します。
6. **Start Search** をクリックします。検索結果リストには、1 チャンネルが表示されます。
7. **Channel** をクリックして、見たいチャンネルを選択してください。選択したチャンネルの検索結果が表示されます。

次は

検索結果の表示を参照してください。

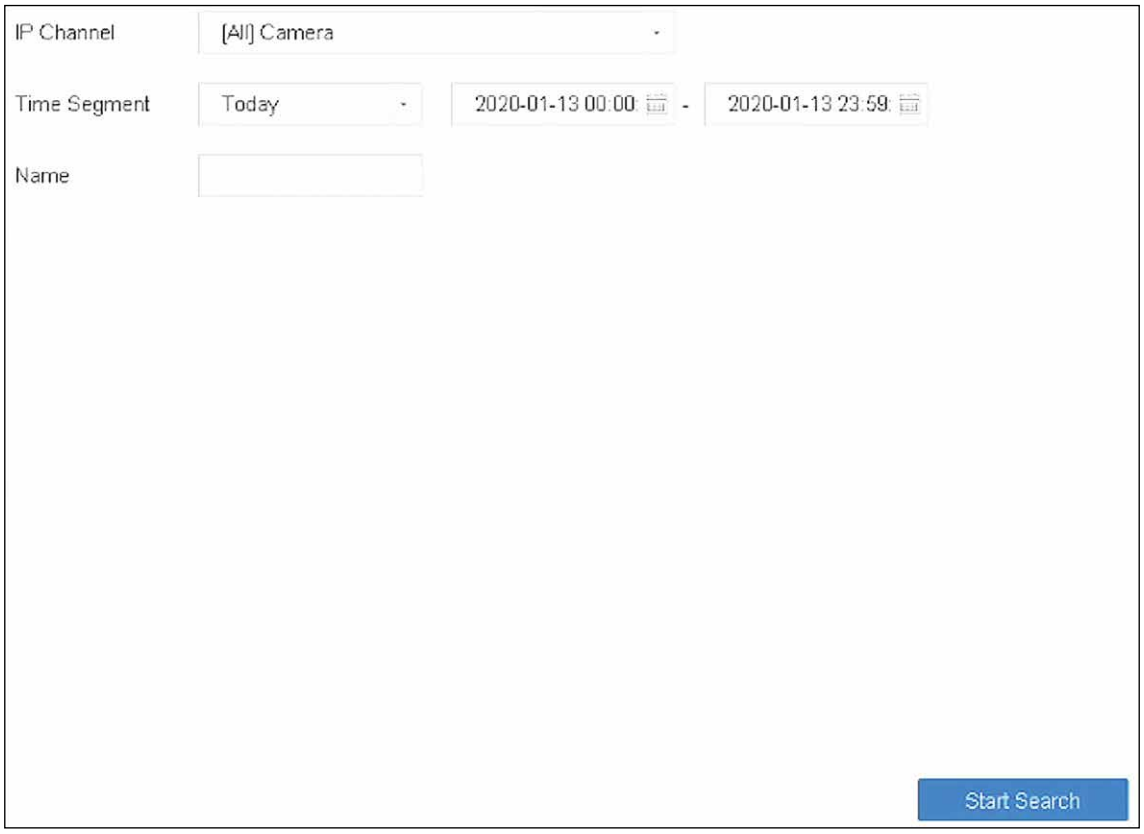


図 5-6 個人名で検索

2. 検索する顔画像の開始時刻と終了時刻を設定します。
3. チャンネルを選択します。
4. 名前を入力します。
5. **Start Search** をクリックします。検索結果リストには、1 チャンネルが表示されます。
6. **Channel** をクリックして、見たいチャンネルを選択してください。選択したチャンネルの検索結果が表示されます。

次は

検索結果の表示を参照してください。

Appearance で検索

外見から顔画像を検索します。

ステップ

1. 次の順に進みます。**Smart Analysis → Smart Search → Face Search → Search by Appearance**
2. 検索条件を設定します。
3. **Start Search** をクリックします。検索結果リストには、1 チャンネルが表示されます。
4. **Channel** をクリックして、見たいチャンネルを選択してください。選択したチャンネルの検索結果が表示されます。

次は

検索結果の表示を参照してください。

検索結果の表示

- ファイルをダブルクリックすると、関連動画が表示されます。
- **Add to Face Database** をクリックすると、選択したファイル（複数可）が顔画像ライブラリーに追加されます。
- **Add to Sample** をクリックすると、選択したファイル（複数可）がサンプル画像（複数可）として追加されます。サンプル画像（複数可）を使って、他の画像を検索することができます。**アップロードされた画像で検索**を参照 してください。
- **Export** をクリックして、選択したファイルをバックアップデバイスにエクスポートします。**Select All** をクリックすると、すべてのファイルを選択できます。

メモ

- をクリックすると、エクスポートの進行状況が表示されます。
- をクリックすると、検索インターフェースに戻ります。

5.5 ペリメータープロテクション

iDS シリーズの一部機種が対象です。次の順に進みます。**Smart Analysis → Smart Analysis → Engine Configuration** 少なくとも 1 つのエンジン用途を **Perimeter Protection** に設定してください。詳しくは**エンジン設定**を参照してください。

5.5.1 侵入検知

侵入検知機能は、あらかじめ設定された仮想領域内に侵入し、不審な人物や車両などを検知する機能です。アラームが発生した際に、特定のアクションを作動することができます。

ステップ

1. 次の順に進みます。**System → Event → Smart Event**
2. **Intrusion** をクリックします。

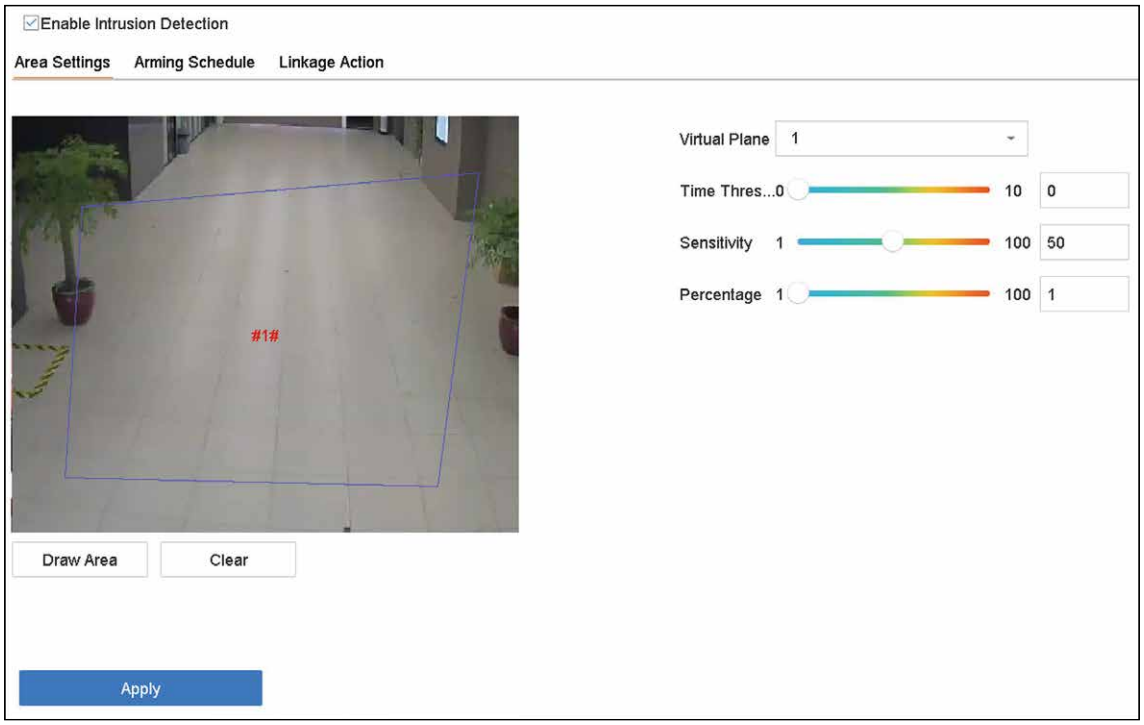


図 5-7 侵入検知

3. **Enable Intrusion Detection** にチェックを入れます。
4. オプション：**Save VCA Picture** にチェックを入れ、キャプチャーした侵入検知画像を保存します。
5. 検知ルールと検知エリアを設定します。
   1）virtual panel を選択します。最大 4 つのバーチャルパネルを選択できます。
   2）**Time Threshold** と **Sensitivity** を設定します。

   Time Threshold

   対象が領域内に留まっている時間です。定義された検知エリア内の物体の継続時間がしきい値を超えると、本機はアラームを鳴らします。

   Sensitivity

   アラームを作動させることができる物体の大きさです。値が高いほど検知アラームが作動しやすくなります。
   3）**Draw Area** をクリックします。
   4) プレビューウィンドウに四角形を描きます。
6. アーミングスケジュールを設定します。**アーミングスケジュールの設定**を参照してください。
7. リンケージアクションを設定します。**リンケージアクションの設定**を参照してください。
8. **Apply** をクリックします。

メモ

iDS-7200 シリーズでは **Target Detection** を **Human** または **Vehicle** に設定できます。選択されたタイプのターゲットのみがアラームを作動します。

5.5.2 ラインクロッシング検知

クロッシング検知は、設定された仮想ラインを横切る人、車両、物体を検知します。検知方向は、左から右、または右から左の双方向に設定できます。

ステップ

1. 次の順に進みます。**System → Event → Smart Event**
2. **Line Crossing** をクリックします。

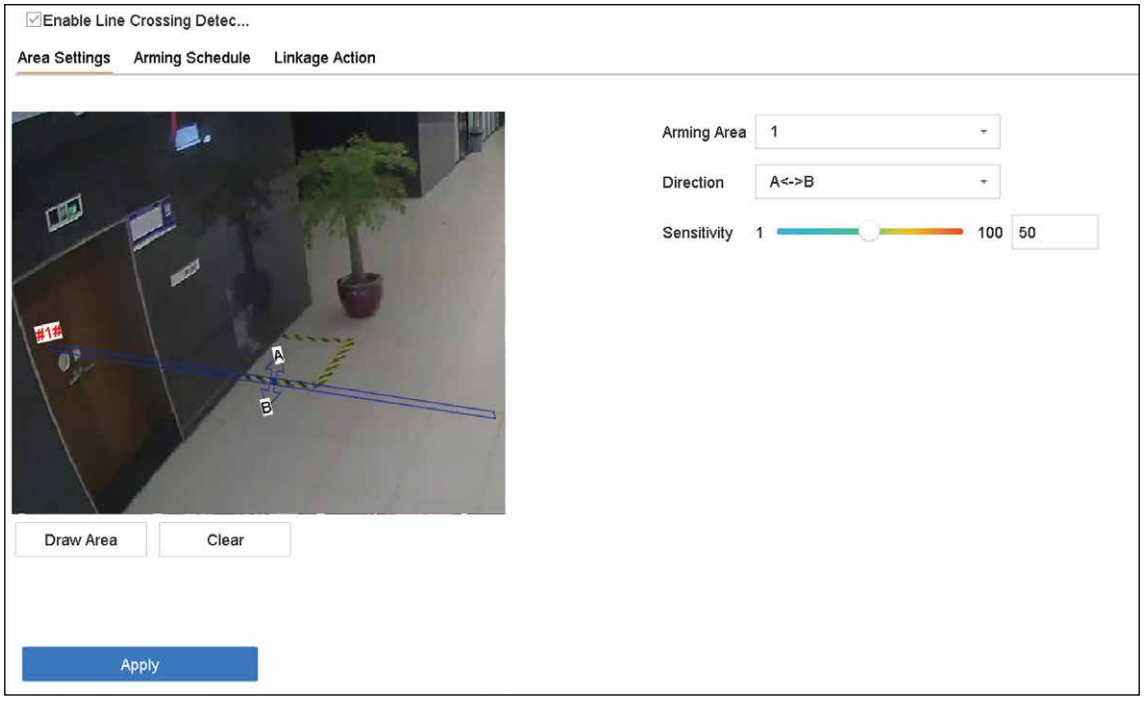


図 5-8 ラインクロッシング検知

3. カメラを選択します。
4. **Enable Line Crossing Detection** にチェックを入れます。
5. オプション：**Save VCA Picture** をクリックして、ラインクロッシング検知のキャプチャー画像を保存します。
6. ラインクロッシング検知ルールと検知エリアを設定します。
   1）アーミングエリアを選択します。
   2) Direction は **A<->B**、**A->B**、または **A<-B** を選択します。

A<->B

B 側の矢印のみ表示されます。設定されたラインを物体が両方向に横切った場合、それを検知してアラームを発生させることができます。

A->B

設定されたラインを A 側から B 側へ横切る物体のみを検出することができます。

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することができます。

3) 検知感度を設定します。値が高いほど検知アラームが作動しやすくなります。
4）**Draw Region** をクリックします。
5) プレビューウィンドウに仮想線を描画します。

7. アーミングスケジュールを設定します。**アーミングスケジュールの設定**を参照してください。
8. リンケージアクションを設定します。**リンケージアクションの設定**を参照してください。
9. **Apply** をクリックします。

メモ

iDS-7200 シリーズでは **Target Detection** を **Human** または **Vehicle** に設定できます。選択されたタイプのターゲットのみがアラームを作動します。

5.5.3 領域入口検知

領域入口検知は、あらかじめ設定された仮想領域に入った対象を検知します。

ステップ

1. 次の順に進みます。**System Management → Event Settings → Smart Event**
2. **Region Entrance Detection** をクリックします。

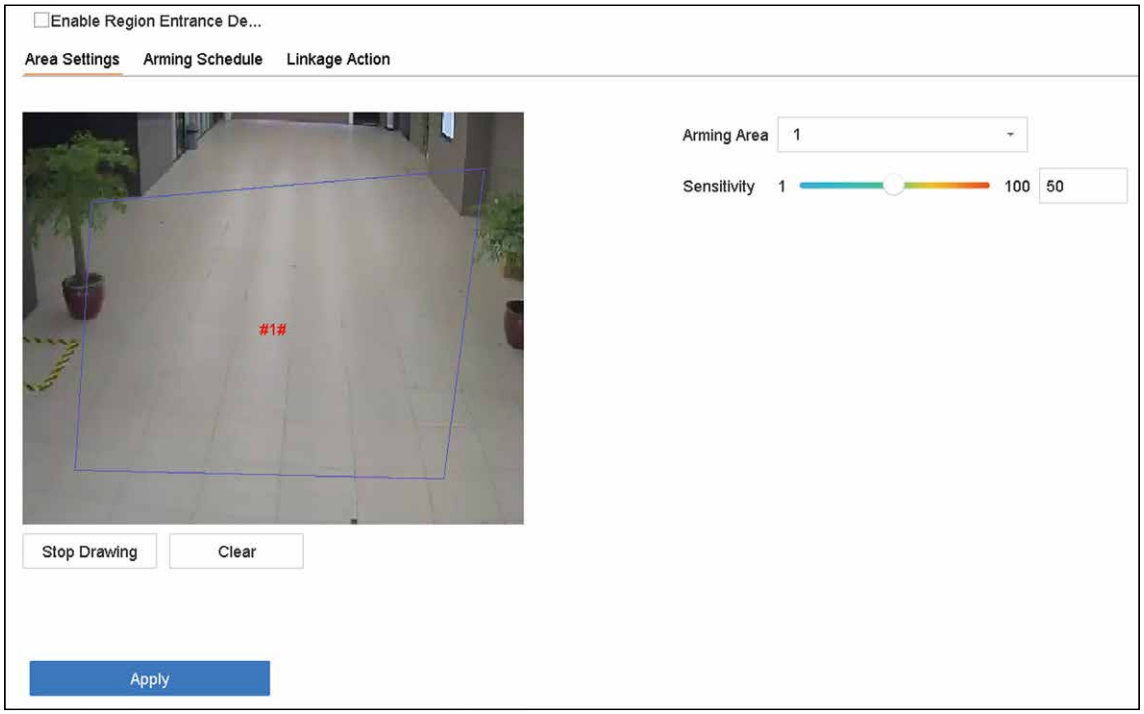


図 5-9 領域入口検知

3. カメラを選択します。
4. **Enable Region Entrance Detection** にチェックを入れます。
5. オプション：**Save VCA Picture** にチェックを入れ、領域入口検知画像のキャプチャー画像を保存します。

6. 検知ルールと検知エリアを設定します。
   1）**Arming Region** を選択します。最大 4 つまで領域が選択できます。
   2）**Sensitivity** を設定します。数値が高いほど検知アラームが出やすくなります。範囲は [0-100] です。
   3）**Draw Region** をクリックし、プレビューウィンドウに四角形を描画します。
7. アーミングスケジュールを設定します。**アーミングスケジュールの設定**を参照してください。
8. リンケージアクションを設定します。**リンケージアクションの設定**を参照してください。
9. **Apply** をクリックします。

5.5.4 領域出口検知

領域出口検知は、あらかじめ設定された仮想領域から抜け出る対象を検知する機能です。

ステップ

1. 次の順に進みます。**System → Event → Smart Event**
2. **Region Exiting** をクリックします。

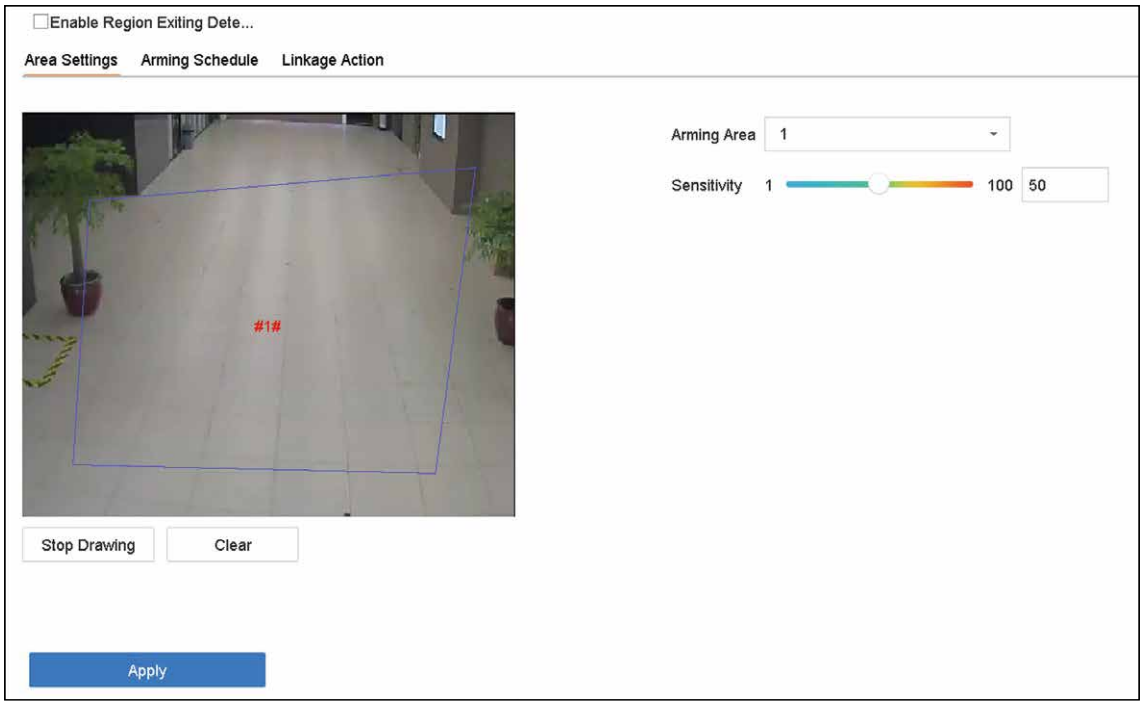


図 5-10 領域出口検知

3. カメラを選択します。
4. **Enable Region Exiting Detection** にチェックを入れます。
5. オプション：**Save VCA Picture** にチェックを入れると、キャプチャーされた領域出口検知画像を保存します。
6. 以下の手順で、検知ルールと検知領域を設定します。
   1）**Arming Region** を選択します。最大 4 つまで領域が選択できます。
   2）**Sensitivity** を設定します。値が高いほど検知アラームが作動しやすくなります。範囲は [0-100] です。
   3）**Draw Region** をクリックし、プレビューウィンドウに四角形を描画します。

7. アーミングスケジュールを設定します。**アーミングスケジュールの設定**を参照してください。
8. リンケージアクションを設定します。**リンケージアクションの設定**を参照してください。
9. **Apply** をクリックします。

5.6 人体検知

次の順に進みます。**Smart Analysis → Smart Analysis → Engine Configuration** 少なくとも 1 つのエンジン用途を **Picture Recognition-Human Body** に設定してください。詳しくは**エンジン設定**を参照してください。
次の順 **Smart Analysis → Smart Analysis → Task Configuration** に進み、カメラ用タスクを有効にします。詳細は**タスク設定**を参照してください。

メモ
この章は、iDS シリーズの一部の機種にのみ適用されます。

5.6.1 人体検知

人体検知は、監視シーンに現れる人体を検知し、その人体画像をキャプチャします。

ご使用の前に

接続されたカメラは人体検知に対応しています。

ステップ

1. 次の順に進みます。**System → Event → Smart Event**
2. **Human Body** をクリックします。
3. オプション：IP カメラが人体検知に対応していない場合は、**Enable Local Human Body Detection** にチェックを入れます。本機は復号化リソースを使用して人体検知を行います。この機能を有効にする前に、**Smart Analysis → Smart Analysis → Engine Configuration** の順に進み、少なくとも 1 つのエンジンは **Video Structuralization-Real-Time** を選択します。
4. この機能を有効にすると、カメラがサポートしているスマートイベントが変更されます。
5. 人体検知を設定するカメラを選択します。
6. **Save VCA Picture** にチェックを入れ、人体検知のキャプチャー画像を保存します。
7. **Target of Interest (Human Body)** にチェックを入れ、人体検知で作動しない非人体画像と動画を破棄します。この機能は、ローカルな人体検知にのみ有効です。
8. 検知領域を設定します。

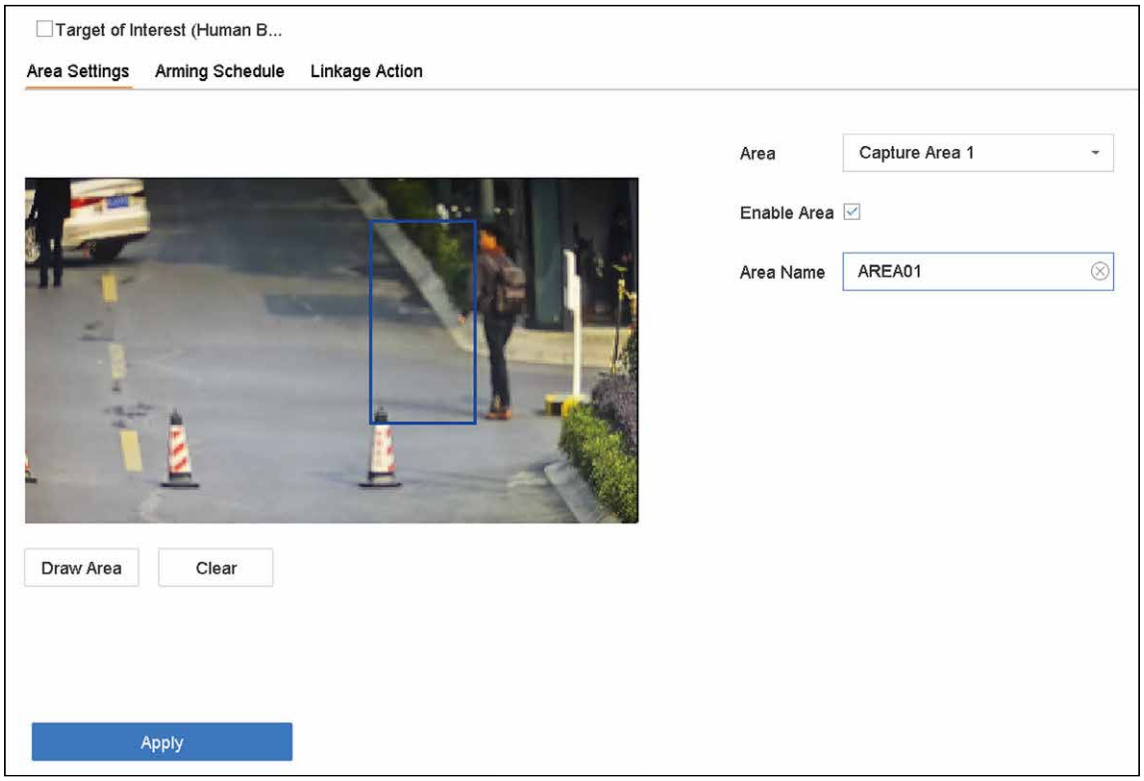


図 5-11 人体検知

1) 設定する検出エリアを Area のドロップダウンリストから選択します。最大 8 つまでエリアの選択が可能です。
2) **Enable Area** にチェックを入れ、選択した検出エリアを有効にします。
3) **Scene Name** にエリア名を入力します。シーン名は最大 32 文字まで使用できます。
4) **Draw Area** をクリックしてプレビューウィンドウに四角形を描画し、**Stop Drawing** をクリックします。

9. アーミングスケジュールを設定します。**アーミングスケジュールの設定**を参照してください。
10. リンケージアクションを設定します。**リンケージアクションの設定**を参照してください。
11. **Apply** をクリックして、設定を有効にします。

5.6.2 人体検索

Appearance で検索

手動で指定した検索条件に従って人体画像を検索します。

ステップ

1. 次の順に進みます。**Smart Analysis → Smart Search → Human Body Detection → Search by Appearance**
2. 検索条件を指定します。
3. **Start Search** をクリックします。検索結果リストには、1 チャンネルが表示されます。
4. **Channel** をクリックして、見たいチャンネルを選択してください。選択したチャンネルの検索結果が表示されます。

5. オプション：エクスポートの検索結果
   1) 検索結果のインターフェイスから結果ファイルを選択するか、または Select All をクリックして、すべてのファイルを選択します。
   2）**Export** をクリックして、選択したファイル (複数可）をバックアップデバイスにエクスポートします。

メモ

をクリックすると、エクスポートの進行状況が表示されます。 をクリックすると、検索インターフェースに戻ります。

アップロードされた画像で検索

検索精度を上げるために、一人の人物をキャプチャした写真を複数枚アップロードし、キャプチャーした人体画像と比較します。

ご使用の前に

USB メモリに人体画像をインポートし、デバイスに接続します。

ステップ

メモ

- 同一画像内に複数のターゲットが存在する場合、最大 30 枚のターゲット画像を解析し表示することができます。
- 最大許容画像サイズは 3840 × 2160 です。
- 画像は JPG または JPEG 形式に限ります。
- 画像名（拡張子を含む）は 64 文字までです。
- アップロードした画像が鮮明で、認識できることを確認してください。

1. 次の順に進みます。**Smart Analysis → Smart Search → Human Body Detection → Search by Picture**
2. チャンネルを選択します。
3. **Upload Sample** をクリックします。
4. **Upload Sample from Local** をクリックし、ローカルディレクトリから顔画像を選択します。
5. 開始時刻と終了時刻を設定します。
6. USB フラッシュドライブ内の画像を選択し **Import** をクリックします。
7. 関連する画像を選択し **Upload** をクリックします。
8. 検索条件を指定します。

   Similarity

   サンプルとライブラリーの顔画像の類似度を解析し、設定した類似度より高い画像を表示します。
9. **Start Search** をクリックします。検索結果リストには、1 チャンネルが表示されます。
10. オプション：エクスポートの検索結果
    1) 検索結果のインターフェイスから結果ファイルを選択するか、または **Select All** をクリックして、すべてのファイルを選択します。
    2）**Export** をクリックして、選択したファイル (複数可）をバックアップデバイスにエクスポートします。

メモ

をクリックすると、エクスポートの進行状況が表示されます。 をクリックすると、検索インターフェースに戻ります。

検索結果をサンプル画像として追加する

検索した人体画像をサンプル画像として追加することができます。そのあとでサンプル画像から人体画像を検索します。

ステップ

1. 人体画像を検索します。
2. 検索結果のインターフェースで、画像をクリックして選択し **Add to Sample** をクリックします。
3. 検索条件設定インターフェースに戻ると、選択したサンプルが一覧表示されます。

5.7 動体検知

動体検知機能により、監視エリア内の動体を検知し、アラームを発生させることができます。

ステップ

1. 次の順に進みます。**System → Event → Normal Event → Motion Detection**
2. カメラを選択します。
3. **Enable** にチェックを入れます。
4. 検出エリアとルールを設定します。
   1) **Draw Area** をクリックして、プレビュー画面上に検出エリア（複数可）を描画します。
   2) マウスを右クリックし、次に **Stop Drawing** をクリックして描画を終了します。
   3) **Sensitivity** (0 ～ 100) を設定します。これにより、動きがどの程度でアラームを作動させやすいかをキャリブレーションすることができます。値が高いほど、動体検知しやすくなります。
   4) オプション：一部のアナログ PIR カメラの場合、**False Alarm Filter** にチェックを入れアラームを減らします。
   5) オプション：iDS M シリーズ、iDS K（B）シリーズの一部機器では、人物や車両が写ったアナログカメラ動画の解析ができます。アナログカメラの下で **Human** または **Vehicle** にチェックを入れます。選択された種類のターゲットのみがアラームを作動させるので、他のオブジェクトに起因する誤報を減らすことができます。

メモ

- 動体検知の **Target Detection** は PIR アラームと競合するため **False Alarm Filter** と **Human** と **Vehicle** の **Target Detection** を同時に有効にすることはできません。
- 動体検知の **Target Detection** は拡張 IP モードや、顔検知、顔画像比較、境界保護（ラインクロス検知、侵入検知）などのスマートイベントとも競合する可能性があります。

5. アーミングスケジュールを設定します。**アーミングスケジュールの設定**を参照してください。
6. リンケージアクションを設定します。**リンケージアクションの設定**を参照してください。
7. **Apply** をクリックします。

5.8 車両検知

道路交通の監視のため、車両検知が可能です。車両検知では、通過した車両を検知し、そのナンバープレートの画像をキャプチャすることができます。アラーム信号を送信して、監視センターに通知することができます。

5.8.1 車両検知の設定

道路交通の監視のため、車両検知を行うことができます。車両検知では、通過した車両を検知し、ナンバープレートの画像をキャプチャすることができます。

ステップ

1. 次の順に進みます。**System → Event → Smart Event**
2. 設定するカメラを選択します。
3. **Vehicle** をクリックします。
4. **Enable Vehicle Detection** にチェックを入れます。
5. オプション：**Save VCA Picture** にチェック を入れると、車両検知のキャプチャー画像を保存します。
6. アーミングスケジュールを設定します。**アーミングスケジュールの設定**するを参照してください。
7. リンケージアクションを設定します。**リンケージアクションの設定**を参照してください。
8. **Area Settings**、**Picture**、**Overlay Content**、**Blocklist**、**Allowlist** を含むルールを設定します。

   Area Settings

   最大 4 レーンまで選択できます。

   Blocklist and Allowlist

   最初にエクスポートしてファイルの形式を確認し、編集して本機にインポートすることができます。
9. **Apply** をクリックします。

メモ

車両検知の詳細はネットワークカメラ取扱説明書を参照してください。

5.8.2 車両検索

一致した車両画像を検索して閲覧することができます。

ステップ

1. 次の順に進みます。**Smart Analysis → Smart Search → Vehicle Search**
2. 車両検索用の IP カメラを選択します。
3. 検索条件を設定します。

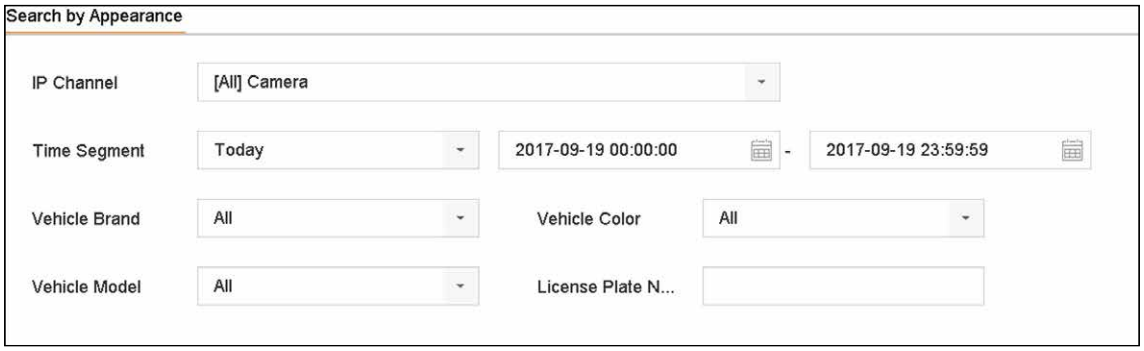


図 5-12 車両検索

4. **Start Search** をクリックします。検索結果リストには、1 チャンネルが表示されます。
5. Channel をクリックして、見たいチャンネルを選択してください。選択したチャンネルの検索結果が表示されます。
6. エクスポートの検索結果
   1) 検索結果のインターフェイスから結果ファイルを選択するか、または **Select All** をクリックして、すべてのファイルを選択します。
   2）**Export** をクリックして、選択したファイル (複数可）をバックアップデバイスにエクスポートします。

メモ

をクリックすると、エクスポートの進行状況が表示されます。

5.9 ターゲット検知

ライブビューモードでは、ターゲット検知機能により、最後の 5 秒とその後の 10 秒の間にスマート検知、顔検知、車両検知、人体検知を行います。

ステップ

1. ライブビューモードで、**Target** をクリックしてターゲット検知インターフェースに入ります。
2. 異なる検知タイプを選択します。Smart detection ( )、vehicle detection ( )、facial detection ( )、human body detection ( ) です。

メモ

サーマルカメラの場合、温度測定イベントはスマート検知 ( ) の中で、顔キャプチャーと顔温度測定は顔検知 ( ) の中で行われます。

3. ヒストリカル分析 ( ) またはリアルタイム解析 ( ) を選択して結果を得ることができます。

メモ

検知したスマート解析の結果が一覧で表示されます。リスト内の結果をクリックすると、関連する動画が再生されます。

4. オプション：画像キャプチャーが必要なチャンネルを選択することができます。未選択のチャンネルは画像をキャプチャーしません。
   1）ライブビューインターフェース左下の をクリックします。
   2) チャンネルを選択すると、チェックを入れたチャンネル（複数可）が画像をキャプチャーします。デフォルトでは全チャンネルが選択されています。
   3) **Finish** をクリックします。

5.10 人数カウント統計の表示

ヒトカウント統計は、設定された特定のエリアに出入りした人数を計算し、分析用の日次 / 週次 / 月次 / 年次レポートを作成します。

ステップ

1. ローカルデバイスの GUI から **Smart Analysis → Smart Report → Counting** の順に進みます。
2. カメラを選択します。
3. レポートの種類を選択します。
4. 分析する **Date** を設定します。人数カウントグラフが表示されます。

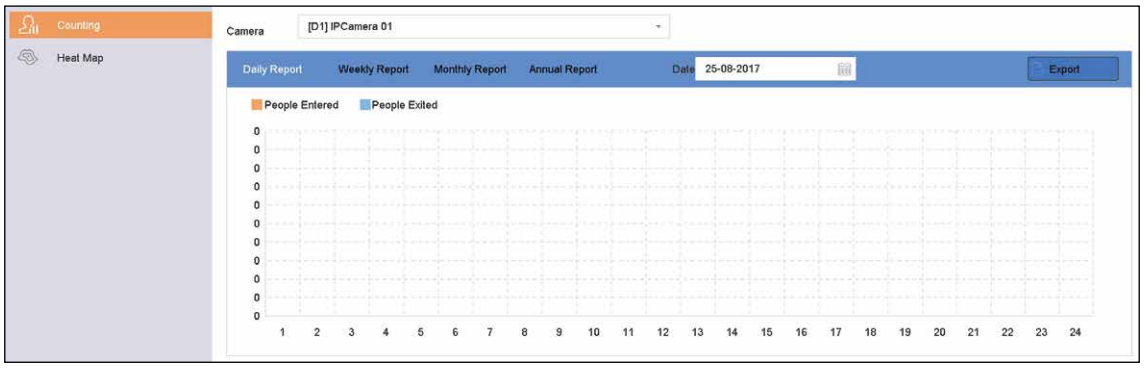


図 5-13 人数カウントインターフェース

5. オプション：**Export** をクリックして、レポートを Microsoft Excel 形式でエクスポートします。

5.11 ヒートマップ

ヒートマップは、データをグラフ化したものです。ヒートマップ機能は、特定のエリアにどれだけの人が訪れ、滞在したかを分析するために使用されます。

ご使用の前に

ヒートマップ機能は接続された IP カメラのサポートが必要で、対応する構成の設定が必要です。

ステップ

1. 次の順に進みます。**Smart Analysis → Heat Map**
2. カメラを選択します。
3. レポートの種類を選択します。
4. 分析する **Date** を設定します。

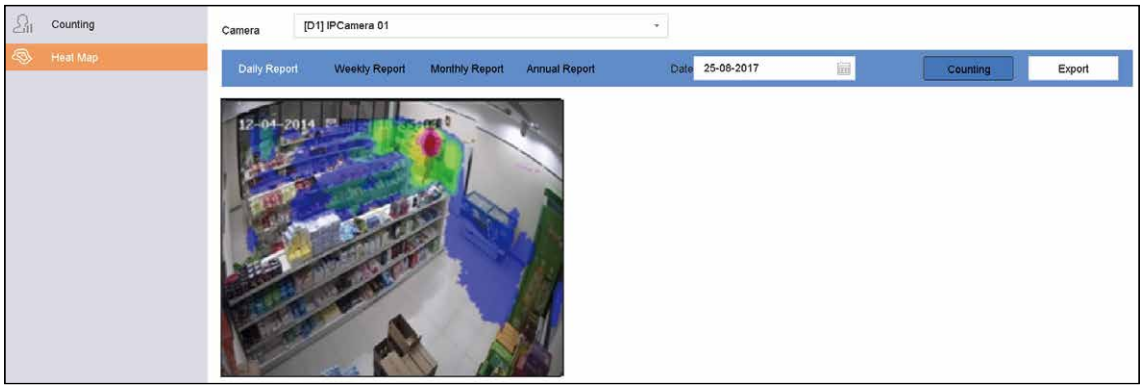


図 5-14 ヒートマップインターフェース

5. **Counting** をクリックします。結果は、異なる色でマークされたグラフィックで表示されます。

メモ

上図のように、赤のカラーブロック（255, 0, 0）はトラフィックの多いエリア、青のカラーブロック（0, 0, 255）はトラフィックの少ないエリアを表しています。

6. オプション：**Export** をクリックして、統計情報レポートを Microsoft Excel 形式でエクスポートします。

第 6 章 イベント

6.1 通常イベントアラーム

6.1.1 ビデオロスアラームを設定する

ビデオロス検知は、チャンネルのビデオロスを検出し、アラーム応答アクションを実行します。

ステップ

1. 次の順に進みます。**System → Event → Normal Event → Video Loss**
2. カメラを選択します。
3. **Enable** にチェックを入れます。
4. アーミングスケジュールを設定します。**アーミングスケジュールの設定**を参照してください。
5. リンケージアクションを設定します。**リンケージアクションの設定**を参照してください。

6.1.2 ビデオタンパリングアラームの設定

カメラレンズが覆われた場合、ビデオタンパリング検知によりアラームが作動し、アラーム応答アクションを実行します（複数可）。

ステップ

1. 次の順に進みます。**System → Event → Normal Event → Video Tampering**
2. カメラを選択します。
3. **Enable** にチェックを入れます。
4. ビデオタンパリングエリアを設定します。プレビュー画面上でドラッグして、カスタマイズしたビデオタンパリング領域を描画します。
5. **Sensitivity** (0-2) を設定します。3 つのレベルがあります。Sensitivity は、動きがどの程度でアラームを作動させやすいかどうかをキャリブレーションします。値が大きいほど、より簡単にビデオタンパリング検知をすることができます。
6. アーミングスケジュールを設定します。**アーミングスケジュールの設定**を参照してください。
7. リンケージアクションを設定します。**リンケージアクションの設定**を参照してください。

6.1.3 センサーのアラームを設定する

外部センサーアラームの処理動作を設定します。

ステップ

1. 次の順に進みます。**System → Event → Normal Event → Alarm Input**
2. リストからアラーム入力の項目を選択し をクリックします。
3. アラーム入力の種類を選択します。
4. アラーム名を編集します。
5. **Input** にチェックを入れます。

6. アーミングスケジュールを設定します。**アーミングスケジュールの設定**を参照してください。
7. リンケージアクションを設定します。**リンケージアクションの設定**を参照してください。

6.1.4 異常アラームを設定する

異常イベントは、ライブビューウィンドウにイベントヒントを取り込み、アラーム出力やリンクアクションをトリガーするように設定することができます。

ステップ

1. 次の順に進みます。**System → Event → Normal Event → Exception**
2. オプション：イベントヒントを有効にすると、ライブビューウィンドウに表示されます。
   1）**Enable Event Hint** にチェックを入れます。
   2）をクリックして、イベントのヒントを得るための異常の種類を選択します。

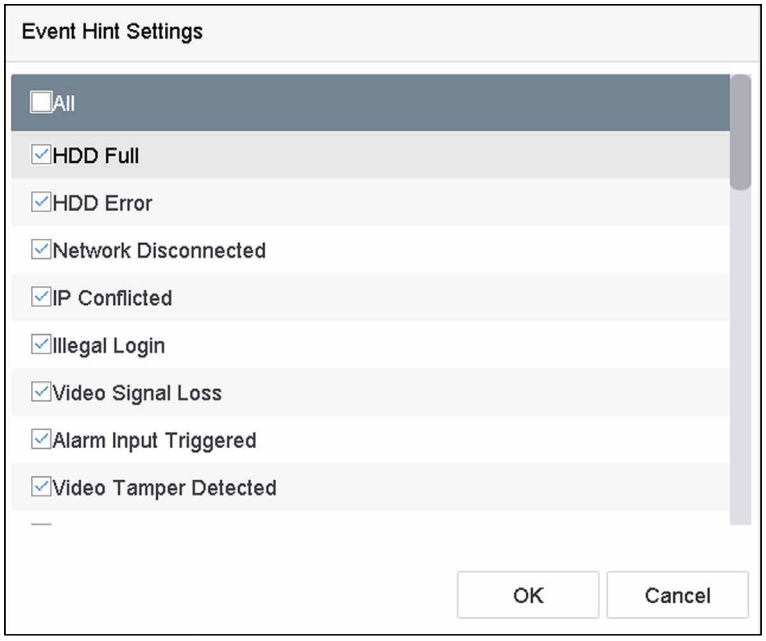


図 6-1 イベントヒントの設定

3. 異常の種類を選択します。

図 6-2 異常処理

4. リンケージアクションを設定します。**リンケージアクションの設定**を参照してください。

6.2 VCA イベントアラーム

接続された IP カメラから送信される VCA 検知の受信に対応しています。最初に IP カメラ設定インターフェースの VCA 検知を有効化し、設定します。

メモ

- VCA 検知は、接続する IP カメラが対応している必要があります。
- VCA 検知の詳細な手順については、ネットワークカメラのユーザーマニュアルを参照してください。

6.2.1 置き去り検知

置き去り検知は、手荷物、財布、危険物など、あらかじめ設定された領域に残された対象物を検知し、アラームが作動した際に一連のアクションを起こすことができます。

ステップ

1. 次の順に進みます。**System → Event → Smart Event**
2. **Unattended Baggage** をクリックします。

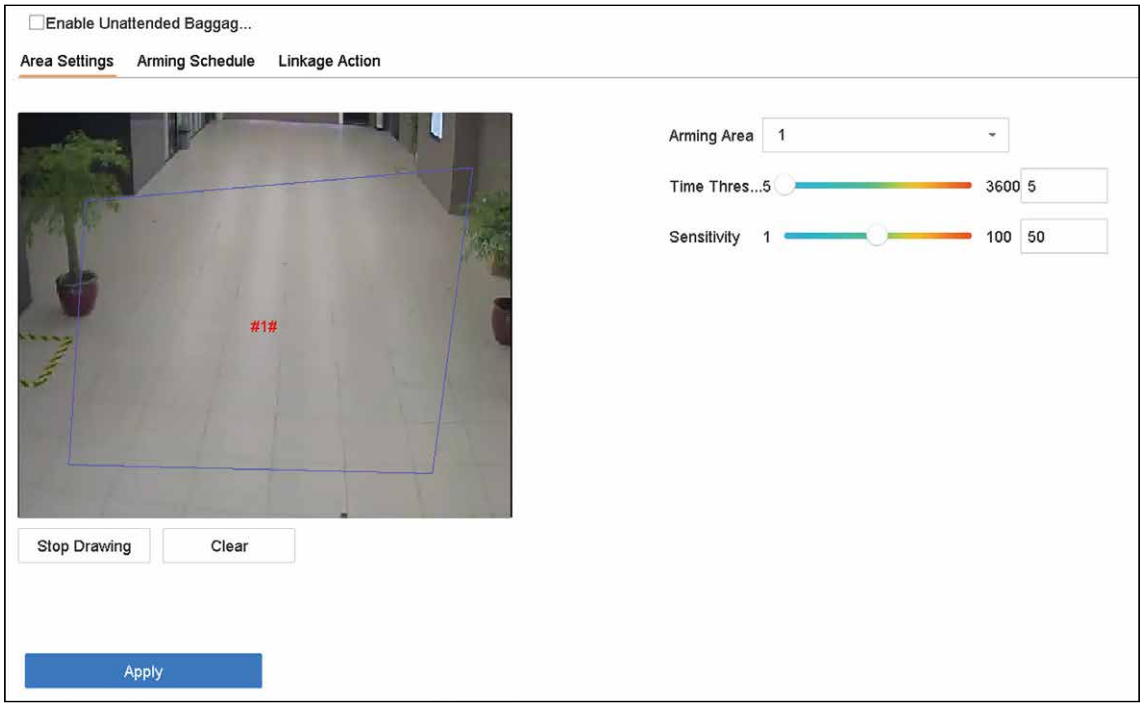


図 6-3 置き去り検知

3. カメラを選択します。
4. **Enable Unattended Baggage Detection** にチェックを入れます。
5. オプション：**Save VCA Picture** にチェックを入れると、キャプチャした置き去り検知画像を保存します。
6. 検知ルールと検知エリアを設定します。
   1）**Arming Region** を選択します。最大 4 つまで領域が選択できます。

2) スライダーをドラッグして **Time Threshold** と **Sensitivity** を設定します。

Time Threshold

対象が指定した領域に留まっている時間です。値が 10 の場合、対象が領域内に 10 秒間留まった後、アラームが作動します。その範囲は [5 秒～ 20 秒] です。

Sensitivity

背景画像と対象の類似性です。値が高いほど検知アラームが作動しやすくなります。

3）**Draw Region** をクリックし、プレビューウィンドウに四角形を描画します。

7. アーミングスケジュールを設定します。**アーミングスケジュールの設定**を参照してください。
8. リンケージアクションを設定します。**リンケージアクションの設定**を参照してください。
9. **Apply** をクリックします。

6.2.2 持ち去り検知

持ち去り検知機能は、展示物などあらかじめ設定された領域から持ち出された対象を検知し、アラームが作動した際に一連のアクションを実行することができます。

ステップ

1. 次の順に進みます。**System → Event → Smart Event**
2. **Object Removable** をクリックします。

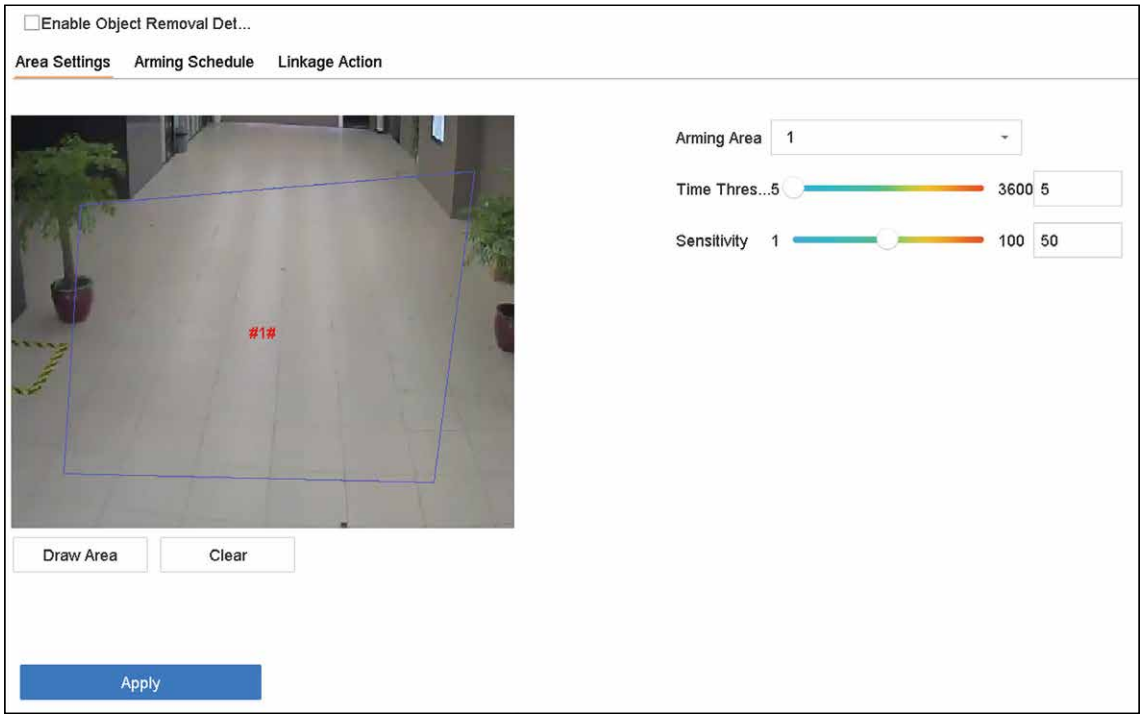


図 6-4 持ち去り検知

3. 設定するカメラを選択します。
4. **Enable Object Removable Detection** にチェックを入れます。

5. オプション：**Save VCA Picture** にチェックを入れると、キャプチャーした持ち去り検知画像を保存します。
6. 以下の手順で、検知ルールと検知領域を設定します。
   1）Arming Region を選択します。最大 4 つまで領域が選択できます。
   2) マウスをドラッグして **Time Threshold** と **Sensitivity** を設定します。

      Time Threshold

      領域から対象が持ち出された時刻です。値が 10 の場合、対象が 10 秒間領域から消えた後、アラームが作動します。範囲は [5 秒～ 20 秒] です。

      Sensitivity

      背景画像の類似度です。感度が高いほど非常に小さな物体でもその領域から持ち出されれば、アラームが作動します。

   3）**Draw Area** をクリックし検知領域の 4 つの頂点を指定して、プレビューウィンドウに四角形を描画します。
7. アーミングスケジュールを設定します。**アーミングスケジュールの設定**を参照してください。
8. リンケージアクションを設定します。**リンケージアクションの設定**を参照してください。
9. **Apply** をクリックします。

6.2.3 音声異常検知

音声異常検知は、音の強さが急に大きくなったり小さくなったりするなどの監視シーンにおける異常な音を検出します。

ステップ

1. 次の順に進みます。**System → Event → Smart Event**
2. **Audio Exception** をクリックします。

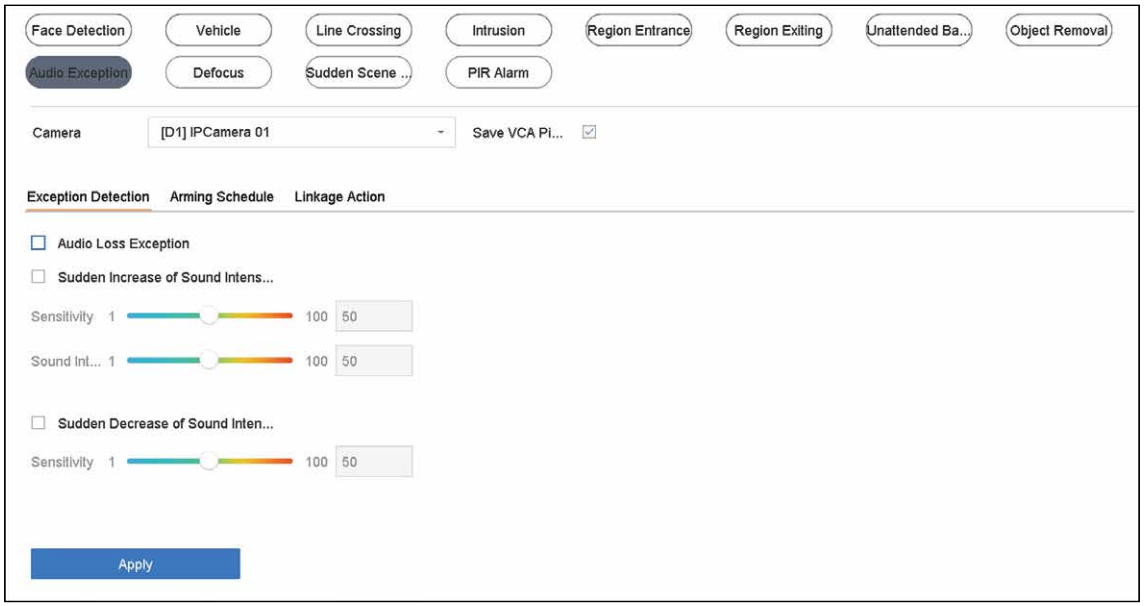


図 6-5 音声異常検知

3. 設定するカメラを選択します。
4. オプション：**Save VCA Picture** にチェックを入れると、キャプチャーした音声異常検知画像を保存します。
5. 検知ルールを設定します :
   1）**Exception Detection** を選択します。
   2）**Audio Loss Exception**、**Sudden Increase of Sound Intensity Detection** および / または **Sudden Decrease of Sound Intensity Detection** にチェックを入れます。

   Audio Loss Exception

   監視シーンで急な音の立ち上がりを検知します。**Sensitivity** と **Sound Intensity Threshold** の設定で、急激な音の立ち上がりの検出感度やしきい値を設定することができます。

   Sensitivity

   値が小さいほど、検知を作動するその変化が厳格になります。範囲は [1-100] です。

   Sound Intensity Threshold

   環境中の音をフィルタリングすることができます。環境音が大きい程、値を大きくする必要があります。環境に応じて調整してください。範囲は [1-100] です。

   Sudden Decrease of Sound Intensity Detection

   監視シーンで急激な音量の低下を検知します。検出感度 [1 ～ 100] を設定する必要があります。
6. アーミングスケジュールを設定します。**アーミングスケジュールの設定**を参照してください。
7. リンケージアクションを設定します。**リンケージアクションの設定**を参照してください。
8. **Apply** をクリックします。

6.2.4 デフォーカス検知

レンズデフォーカスによる画像のピンボケを検出することができます。

ステップ

1. 次の順に進みます。**System → Event → Smart Event**
2. **Defocus** をクリックします。

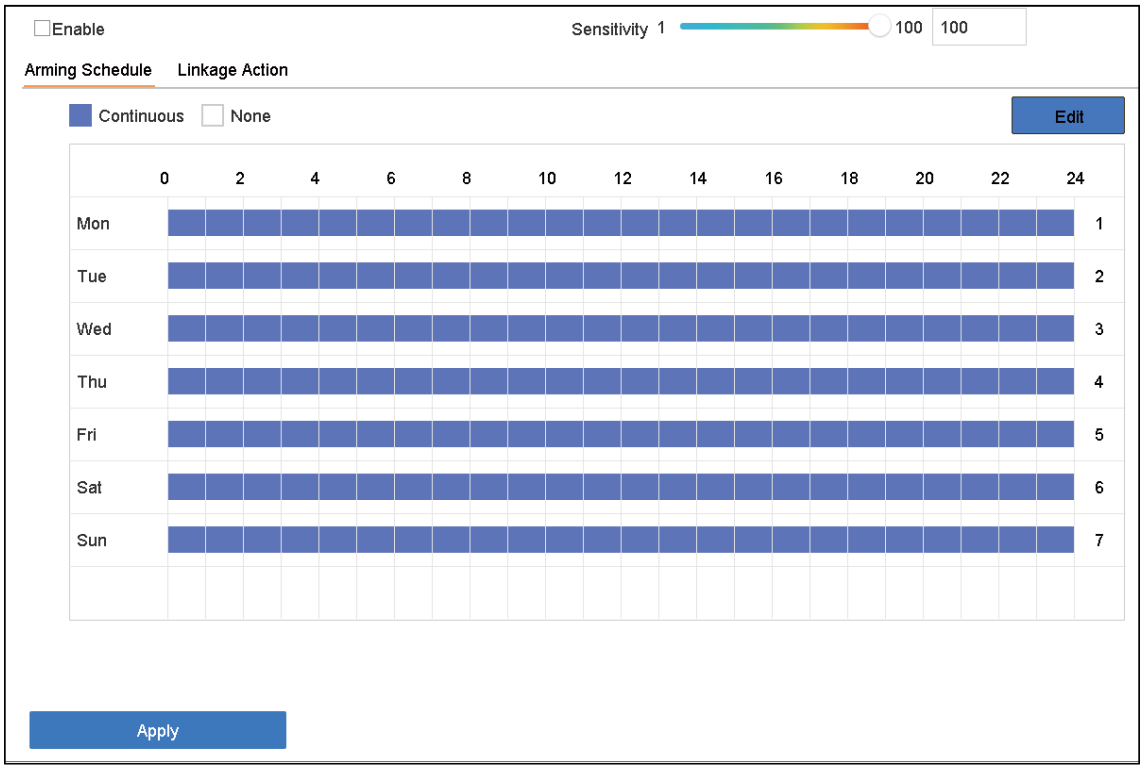


図 6-6 デフォーカス検知

3. 設定するカメラを選択します。
4. **Enable** にチェックを入れます。
5. オプション：**Save VCA Picture** にチェックを入れると、キャプチャーしたデフォーカス検知画像を保存します。
6. **Sensitivity** をドラッグして検出感度を設定します。

メモ

感度の範囲 [1-100]。値が大きいほど、デフォーカス画像を検知しやすくなります。

7. アーミングスケジュールを設定します。**アーミングスケジュールの設定**を参照してください。
8. リンケージアクションを設定します。**リンケージアクションの設定**を参照してください。
9. **Apply** をクリックします。

6.2.5 突発的なシーンチェンジ検知

シーンチェンジ検知は、カメラの意図的な回転など、外的要因による監視環境の変化を検出するものです。

ステップ

1. 次の順に進みます。**System → Event → Smart Event**

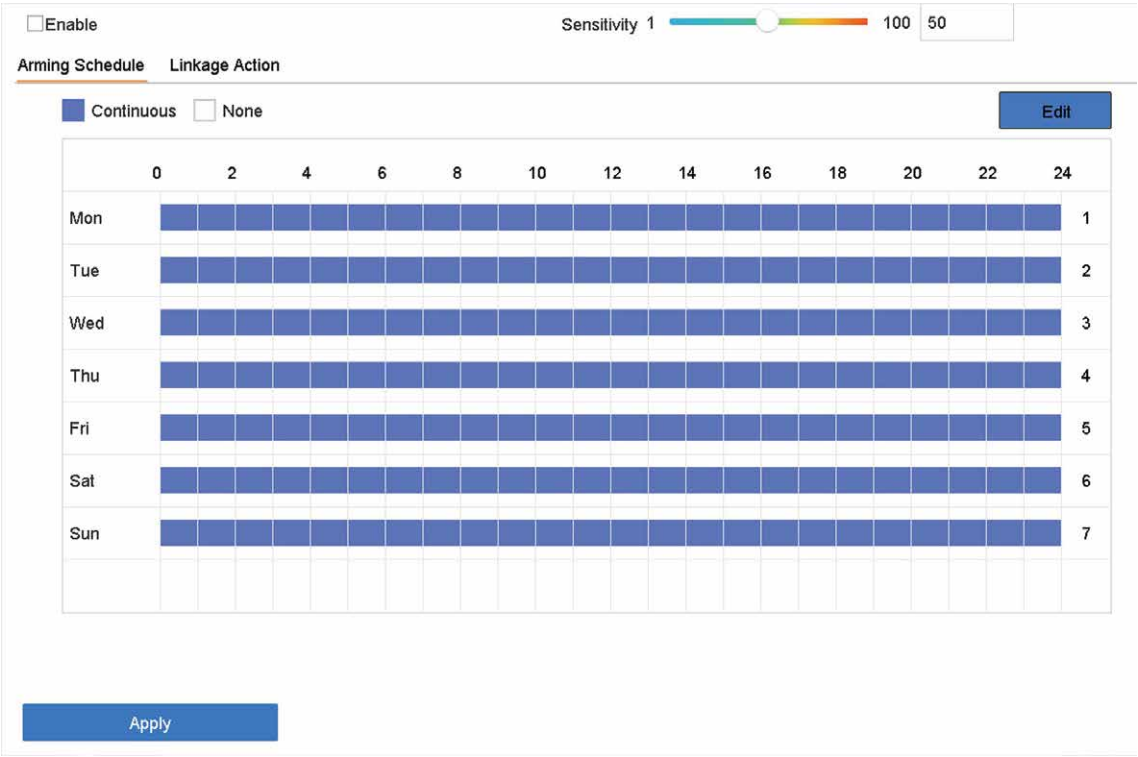


図 6-7 突発的なシーンチェンジ検知

3. 設定するカメラを選択します。
4. **Enable** にチェックを入れます。
5. オプション：**Save VCA Picture** にチェックを入れると、キャプチャーした突発的なシーンチェンジ検知の画像を保存します。
6. **Sensitivity** をドラッグして検出感度を設定します。

メモ

感度の範囲 [1-100]。値が高いほどシーンの変化でアラームが作動しやすくなります。

7. アーミングスケジュールを設定します。**アーミングスケジュールの設定**を参照してください。
8. リンケージアクションを設定します。**リンケージアクションの設定**を参照してください。
9. **Apply** をクリックします。

6.2.6 PIR アラーム

侵入者が検知器の視野内に入ると、PIR（受動的赤外線）アラームが作動します。人や犬、猫などの温血動物が放つ熱エネルギーを検出することができます。

ステップ

1. 次の順に進みます。**System → Event → Smart Event**
2. **PIR Alarm** をクリックします。

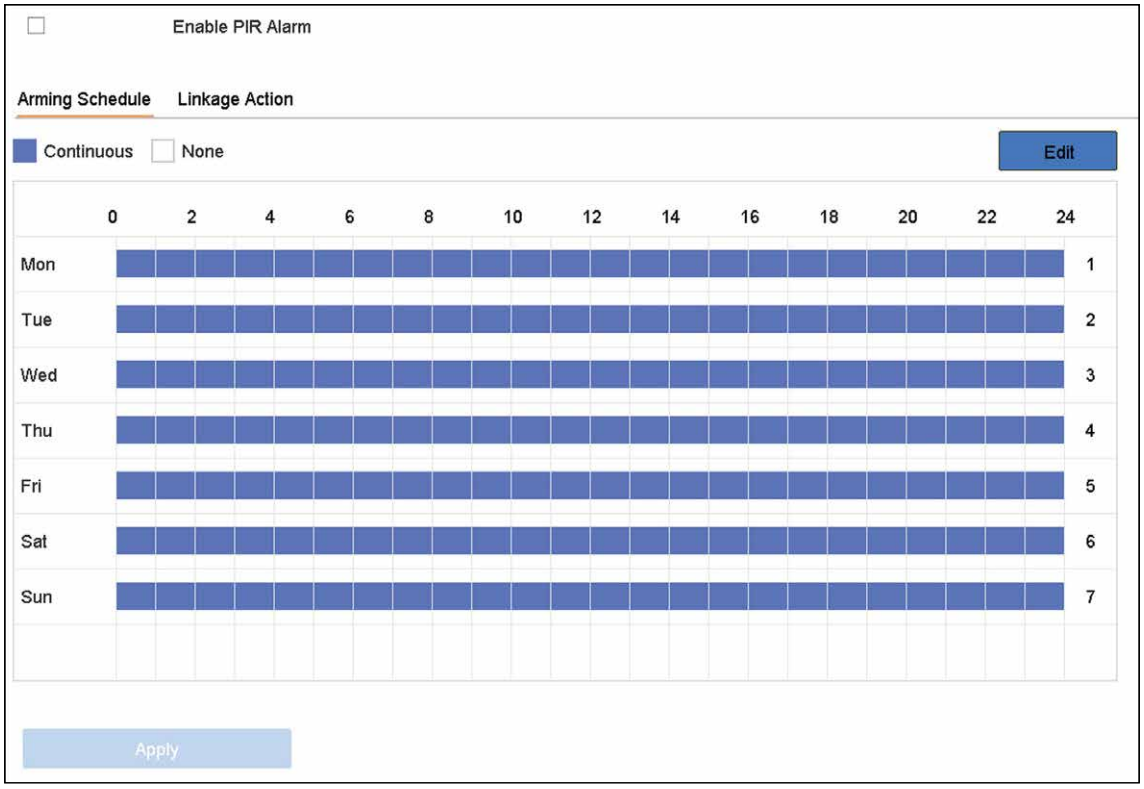


図 6-8 PIR アラーム

3. 設定するカメラを選択します。
4. **PIR Alarm** にチェックを入れます。
5. オプション:**Save VCA Picture** にチェックを入れると、キャプチャーした PIR アラーム画像を保存します。
6. アーミングスケジュールを設定します。**アーミングスケジュールの設定**を参照してください。
7. リンケージアクションを設定します。**リンケージアクションの設定**を参照してください。
8. **Apply** をクリックします。

6.3 アーミングスケジュールの設定

ステップ

1. **Arming Schedule** をクリックします。
2. **Edit** をクリックします。
3. 曜日を選択し、期間を設定します。1 日に最大 8 つまで時間帯を設定することができます。

メモ

時間帯の繰り返しや重複はできません。

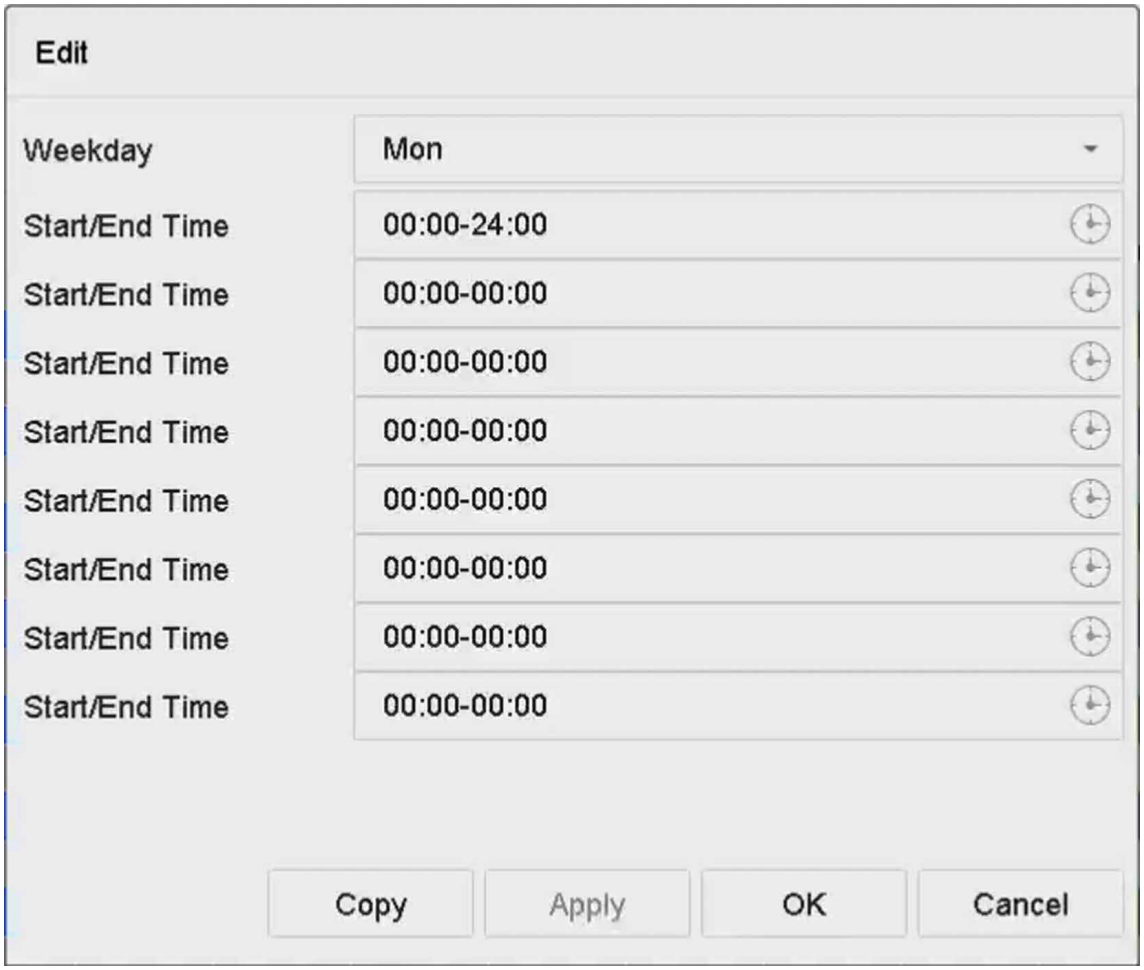


図 6-9 アーミングスケジュールの設定

4. **Copy** をクリックして、現在の曜日のアーミングスケジュール設定を他の曜日にコピーできます。
5. **Apply** をクリックして、設定を保存します。

6.4 リンケージアクションの設定

アラームまたは異常が発生すると、Event Hint Display、Full Screen Monitoring、Audible Warning（ブザー）、Notify Surveillance Center、Trigger Alarm Output、Send Email などのアラームリンケージアクションが作動します。

6.4.1 フルスクリーンモニタリング自動切換えを設定する

アラームが発生すると、ローカルモニターはフルスクリーンモニタリング用に設定されたアラームチャンネルのビデオ画像をフルスクリーンで表示します。また、複数のチャンネルで同時にアラームが発生した場合、滞留時間自動切替え設定をする必要があります。

メモ

アラームが停止し、ライブビューインターフェースに戻ると自動切替えは終了します。

ステップ

1. 次の順に進みます。**System → Live View → General**
2. イベント出力と滞留時間を設定します。

   Event Output

   イベント映像を表示する出力を選択します。

   Full Screen Monitoring Dwell Time

   アラームイベント画面を表示する時間を秒単位で設定します。複数のチャンネルで同時にアラームが発生した場合、それらのフルスクリーン画像は 10 秒間隔（デフォルトの滞留時間）で切り替ります。
3. アラーム検知の **Linkage Action** インターフェースに進んでください。（例：動体検知、ビデオタンパーリング、顔検知など）。
4. **Full Screen Monitoring** アラームリンケージアクションを選択します。
5. フルスクリーンモニタリング用に **Trigger Channel** でチャンネル（複数可）を選択します。

6.4.2 ブザーを設定する

アラームを検知すると、ブザーが鳴ります。

ステップ

1. 次の順に進みます。**System → Live View → General**
2. **Enable Audio Output** にチェックを入れます。
3. オーディの音量を設定します。
4. **Apply** をクリックします。
5. アラーム検知の **Linkage Action** インターフェースに進んでください。（例：動体検知、ビデオタンパーリング、顔検知など）。
6. アラームリンケージアクションとして **Buzzer** を選択してください。

6.4.3 サーベイランスセンターへ通知する

本機はイベントが発生すると、リモートアラームホストに異常またはアラーム信号を送信します。アラームホストとは、クライアントソフトウェア（iVMS-4200、iVMS-5200 など）がインストールされている PC を指します。

ステップ

1. 次の順に進みます。**System → Network → Advanced → More Settings**
2. アラームホスト IP とアラームホストポートを設定します。
3. アラーム検知の **Linkage Action** インターフェースに進んでください。（例：動体検知、ビデオタンパーリング、顔検知など）。
4. **Notify Surveillance Center** を選択します。

6.4.4 メールリンケージを設定する

アラームを検知した際に、アラーム情報を記載した電子メールをユーザーまたは複数ユーザーに送信することができます。

ステップ

1. 次の順に進みます。**System → Network → Advanced → Email**
2. E メールのパラメータを設定します。
3. **Apply** をクリックします。
4. アラーム検知の **Linkage Action** インターフェースに進んでください。（例：動体検知、ビデオタンパーリング、顔検知など）。
5. **Send Email** アラームリンケージアクションを選択します。

6.4.5 アラーム出力を作動する

アラーム出力は、アラーム入力、動体検知、ビデオタンパーリング検知、顔検知、ラインクロス検知、その他すべてのイベントによって作動します。

ステップ

1. アラーム検出の **Linkage Action** に進んでください。（例：動体検知、顔検知、ラインクロス検知、侵入検知など）。
2. **Trigger Alarm Outputs** で、作動するアラーム出力（複数可）を選択します。
3. 次の順に進みます。**System → Event → Normal Event → Alarm Output**
4. リストからアラーム出力の項目を選択します。

6.4.6 PTZ リンケージを設定する

アラームイベント、またはVCA検知イベントが発生すると、PTZアクション（プリセット / パトロール / パターンの呼び出しなど）を作動することができます。

ご使用の前に

接続したPTZまたはスピードドームがPTZアクションに対応していることを確認してください。

ステップ

1. アラーム検知またはVCA検知の **Linkage Action** インターフェースに進んでください。（例：顔検知、ラインクロス検知、侵入検知など）。
2. **PTZ Linkage** を選択します。
3. PTZアクションを行うカメラを選択します。
4. アラームイベント発生時に呼び出すプリセット / パトロール / パターン No. を選択します。

メモ

リンケージアクションに設定できるPTZの種類は、毎回1つだけです。

6.4.7 オーディオとライトアラームリンケージを設定する

一部のカメラでは、アラームリンケージ動作を音声アラームまたは光アラームに設定することができます。

ご使用の前に

- カメラがオーディオとライトアラームリンケージに対応していることを確認してください。
- オーディオ出力と音量が正しく設定されていることを確認してください。

ステップ

1. アラーム検知（モーション検知など）のリンケージアクションインターフェースに進みます。
2. お好みの **Audio and Light Alarm Linkage** を設定してください。
3. **Apply** をクリックします。

メモ

Hik-Connectを使って、カスタマイズした音声メッセージを録音したり、カメラに音声メッセージを送ったりすることができます。カスタマイズした音声メッセージは、音声連携に利用することができます。

第 7 章 ファイル管理

7.1 ファイル検索

詳細な条件を指定して、動画や画像を検索することができます。

ステップ

1. 次の順に進みます。**File Management → All Files/Human Files/Vehicle Files**
2. 時間やカメラ、イベントタイプなどの細かい条件を指定します。

メモ

- **All Files** は **Time**、**Camera File Type**、**Event type** を選択します。
- **Human Files** は **Time**、**Camera**、**File Type** を選択します。
- **Vehicle Files** は **Time**、**Camera**、**File Type**、**Plate No.**、**Area/Country** を選択します。

3. **Search** をクリックして結果を表示します。一致したファイルが表示されます。
4. メニューの **Target Picture** または **Source Picture** を選択すると、関連する画像のみを表示することができます。
   – Target Picture：車両クローズアップの検索結果を表示します。
   – Source Picture：カメラでキャプチャしたオリジナル画像の検索結果を表示します。

7.2 ファイルのエクスポート

バックアップ用のファイルを USB デバイスや eSATA HDD にエクスポートすことができます。

ステップ

1. ファイルを検索します。詳しくは**ファイル検索**を参照してください。
2. ファイルを選択します。
3. **Export** をクリックします。
4. オプション:車両ファイルについては **Backup License Plate Statistics Info** をクリックすると、ナンバープレート統計情報を後でエクスポートすることができます。
5. ファイルをエクスポートするには **Video and log** として選択して **OK** ボタンをクリックします。
6. バックアップデバイスとフォルダのパスを選択します。
7. **OK** ボタンをクリックします。

7.3 スマートサーチ

File Management → Smart Search で人体ファイル、顔ファイル、車両を検索できます。詳しくは**人体検索**、**顔画像比較**、**車両検索**を参照してください。

第 8 章 POS 設定

本機は POS マシン / サーバーに接続し、トランザクションメッセージを受信してライブビューまたは再生中に画像にオーバーレイを表示したり、POS イベントアラームを作動したりすることができます。

メモ

本機能は一部の機種のみ対応しています。

8.1 POS 接続の設定

ステップ

1. 次の順に進みます。**System → POS**
2. **Add** をクリックします。

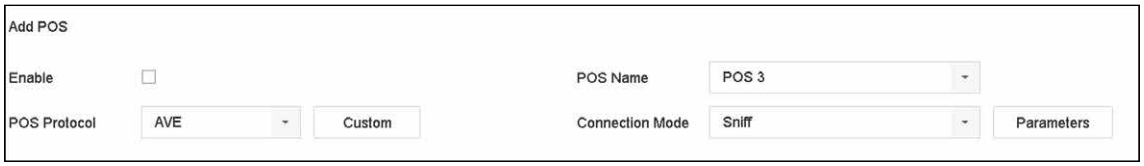


図 8-1 POS 設定

3. ドロップダウンリストから POS デバイスを選択します。
4. **Enable** にチェックを入れます。

メモ

各機器がサポートする POS デバイスの数は、そのチャネル数の半分です。例：DS-9616NI-I8 モデルでは 8 台の POS デバイスがサポートされています。

5. **POS Protocol** を選択します。

メモ

新しいプロトコルを選択した場合、新しい設定を有効にするために本機を再起動してください。

Universal Protocol

Advancedをクリックすると、ユニバーサルプロトコルを選択する際の設定項目が増えます。POS オーバーレイ文字の開始行識別子、改行タグ、終了行タグ、および文字の大文字小文字を区別するプロパティを設定することができます。また、オプションでフィルタリング識別子と XML プロトコルを確認することができます。

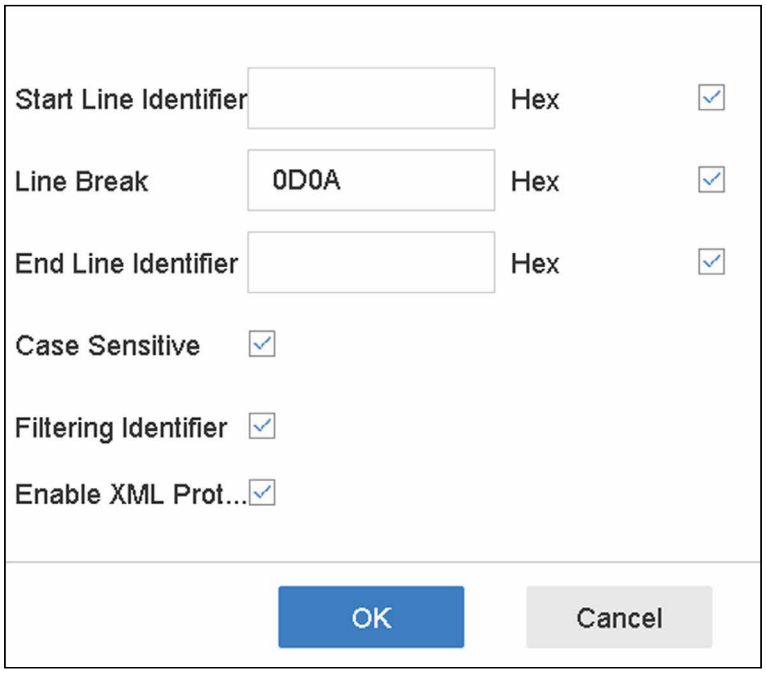


図 8-2 ユニバーサルプロトコルの設定

EPSON

EPSON プロトコルでは、固定された開始行タグと終了行タグが使用されます。

AVE

AVE プロトコルでは、固定された開始行タグと終了行タグが使用されます。シリアルポートおよび仮想シリアルポートの接続タイプに対応しています。

Custom をクリックして、AVE の設定を行います。**Rule** は **VSI-ADD** または **VNET** を選択します。送信する POS メッセージのアドレスビットを設定します。**OK** ボタンをクリックして、設定を保存します。

NUCLEUS

Custom をクリックして、NUCLEUS の設定を行います。

従業員番号、シフト番号、端末番号を入力します。POS デバイスから送信された一致するメッセージが有効な POS データとして使用されます。

メモ

RS-232 接続の通信では、NUCLEUS プロトコルを使用する必要があります。

6. **Connection Mode** を選択して **Parameters** をクリックし、各接続モードのパラメータを設定します。

TCP Connection

TCP 接続を使用する場合、ポートは 1 ～ 65535 の範囲で設定し、POS 機ごとにポートを固有にする必要があります。
POS メッセージを送信するデバイスの **Allowed Remote IP Address** を設定します。

UDP Connection

UDP 接続を使用する場合、ポートは 1 ～ 65535 の範囲で設定し、POS 機ごとにポートを固有にする必要があります。
POS メッセージを送信するデバイスの Allowed Remote IP Address を設定します。

USB-to-RS-232 Connection

USB-to-RS-232 変換ポートのパラメータ（Serial Port Number、Baud Rate、Data Bit、Stop Bit、Parity、Floe Ctrt）を設定します。

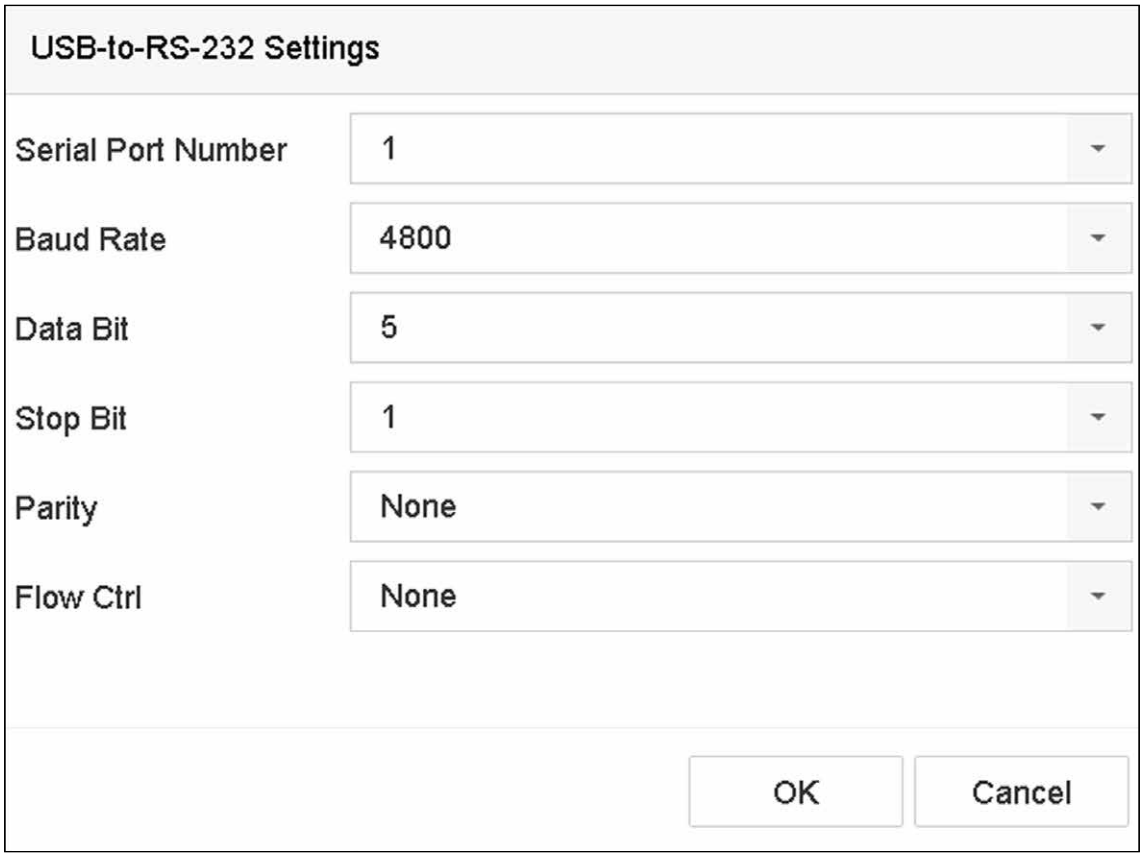


図 8-3 USB-to-RS-232 の設定

RS-232 Connection

本機と POS 機器を RS-232 で接続します。**Menu → Configuration → RS-232** の順で **RS-232** の設定を行うことができます。Usage は Transparent Channel に設定されている必要があります。

Multicast Connection

マルチキャストプロトコルで本機と POS 機器を接続する場合は、マルチキャストアドレスとポートを設定します。

Sniff Connection

本機と POS 機器を Sniff で接続します。Source Address と Destination Address の設定を行います。

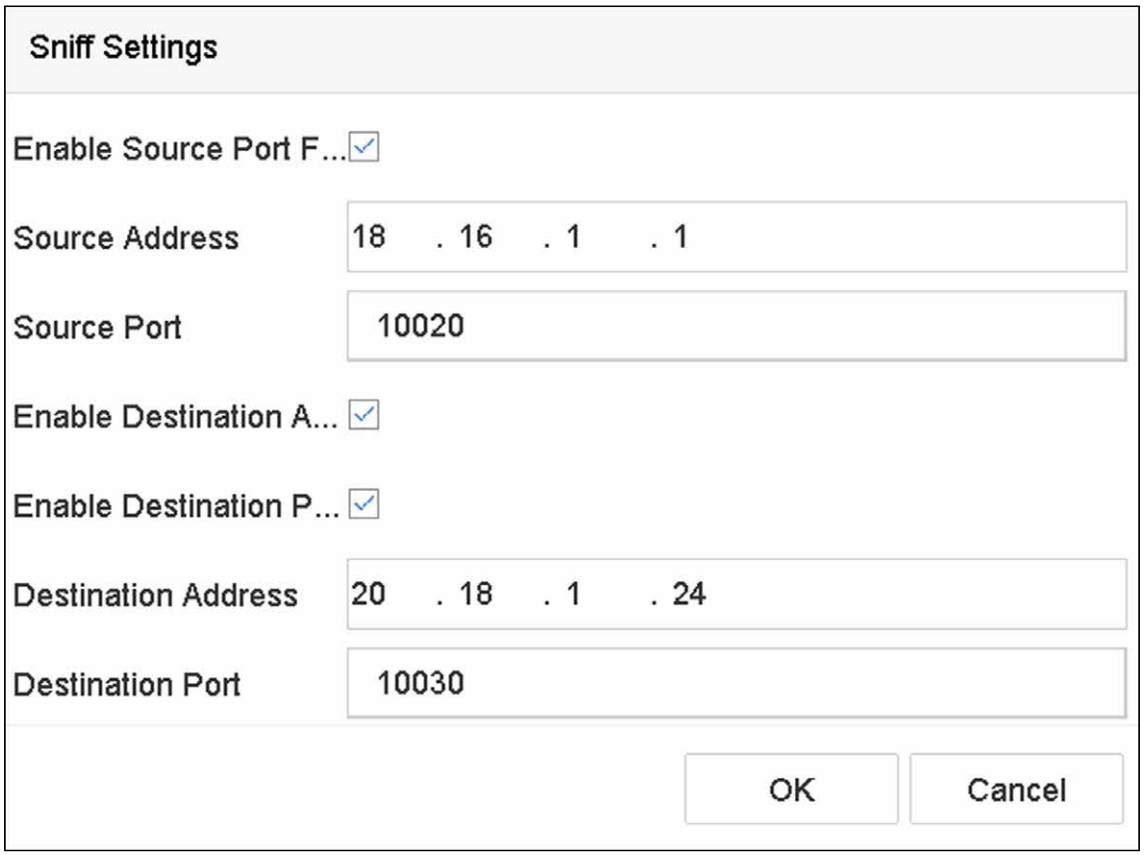


図 8-4 Sniff の設定

8.2 POS テキストオーバーレイの設定

ステップ

1. 次の順に進みます。**System → POS**
2. **Channel Linkage and Display** をクリック します。

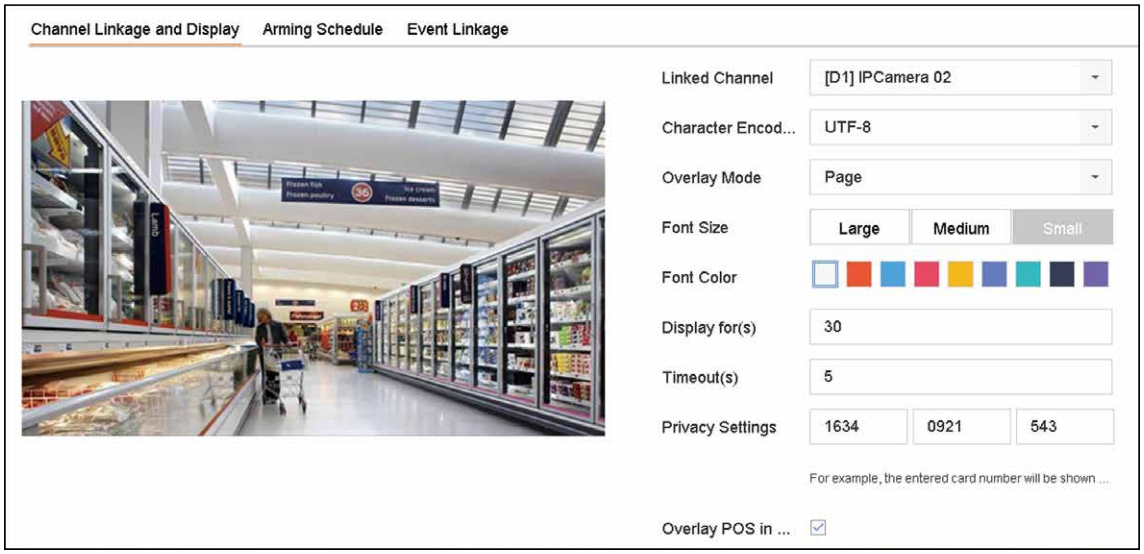


図 8-5 オーバーレイ文字設定

3. **linked channel** をクリックして、POS 文字をオーバーレイします。
4. 有効な POS の文字オーバーレイを設定します。
   - 文字コード形式：現在、Latin-1 形式を使用できます。
   - スクロールまたはページモードで表示する文字のオーバーレイモード
   - 文字サイズと文字色
   - 文字の表示時間（秒）。値の範囲は 5 ～ 3600 秒です。
   - POS イベントのタイムアウト。値の範囲は 5 ～ 3600 秒です。定義された時間内に本機が POS メッセージを受信しなかった場合、トランザクションは終了します。
5. **Privacy Settings** で、POS のプライバシー情報（カード番号、ユーザー名など）を画像に表示しないように設定します。
   定義されたプライバシー情報は、代わりに画像上に *** で表示されます。
6. **Overlay POS in Live View** にチェックを入れます。この機能を有効にすると、ライブビュー画像に POS 情報がオーバーレイ表示されます。

メモ

枠をドラッグして、POS 設定画面のプレビュー画面でテキストボックスのサイズと位置を調整することができます。

7. **Apply** をクリックして、設定を有効にします。

8.3 POS アラームの設定

POS イベントは、チャンネルを作動して録画を開始したり、フルスクリーンモニターリングや音声警告を作動して監視センターに通知したり、電子メールを送信したりすることができます。

ステップ

1. 次の順に進みます。**Storage → Recording Schedule**
2. POS イベントのアーミングスケジュールを設定します。
3. 次の順に進みます。**System → POS**
4. POS の追加または編集のインターフェイスで **Event Linkage** をクリックします。

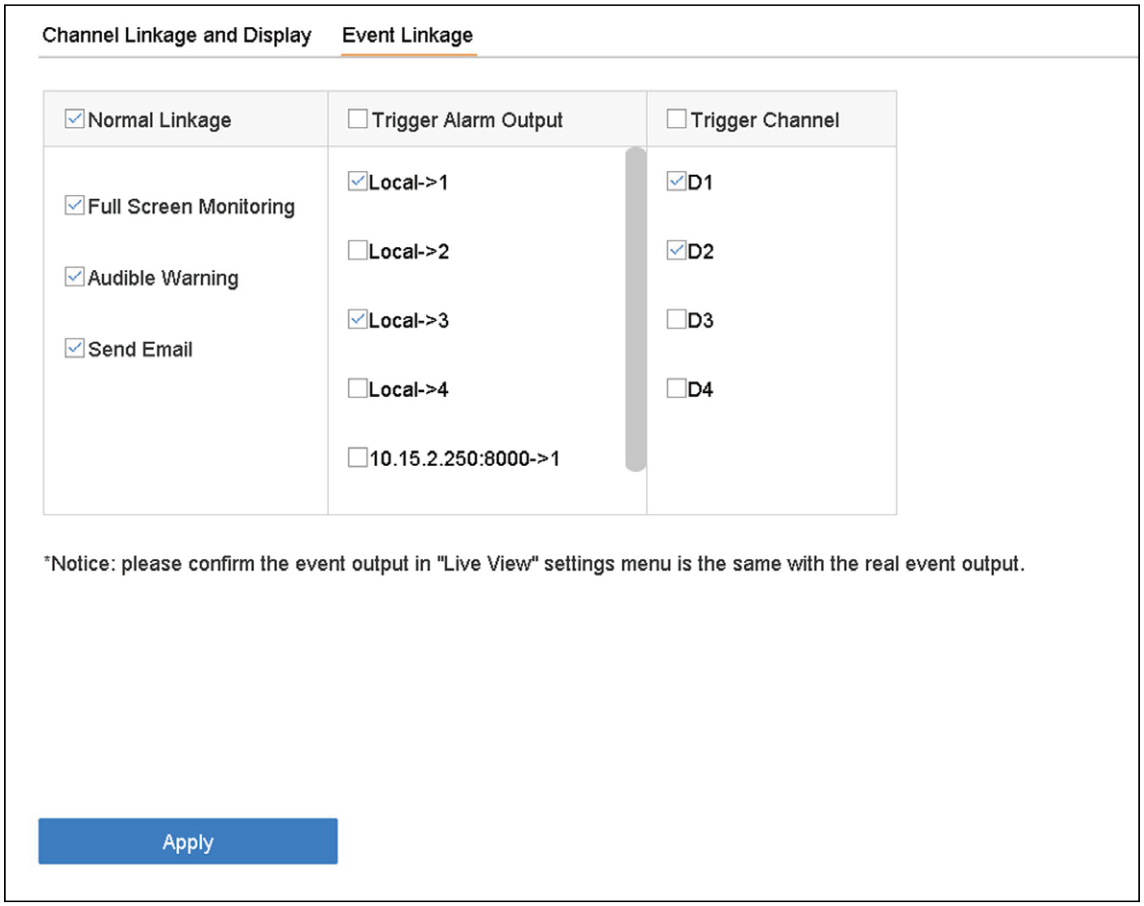


図 8-6 POS のカメラ作動の設定

5. 通常のリンケージアクションを選択します。
6. 作動するアラーム出力を 1 つまたは複数選択します。
7. POS アラームが作動したときに、チャンネルを 1 つまたは複数選択して、録画または全画面監視を行います。
8. **Apply** をクリックして、設定を保存します。

第 9 章 ストレージ

メモ

この章で扱う利用できる機能は機種により異なる場合があります。

9.1 ストレージデバイスの管理

9.1.1 ローカル HDD を管理する

HDD グループの設定

複数の HDD をグループ化して管理することが可能です。HDD の設定により、指定したチャンネルの動画を特定の HDD グループに録画することができます。

ステップ

1. 次の順に進みます。**Storage → Storage Mode**
2. **Mode** は **Group** を選択します。
3. **Apply** をクリックします。
4. 次の順に進みます。**Storage → Storage Device**
5. HDD を選択します。

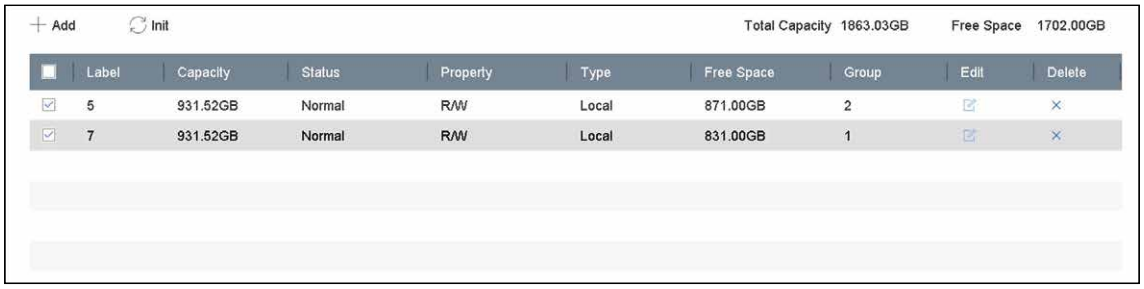


図 9-1 ストレージデバイス

6. をクリックして、Local HDD Settings インターフェイスに入ります。

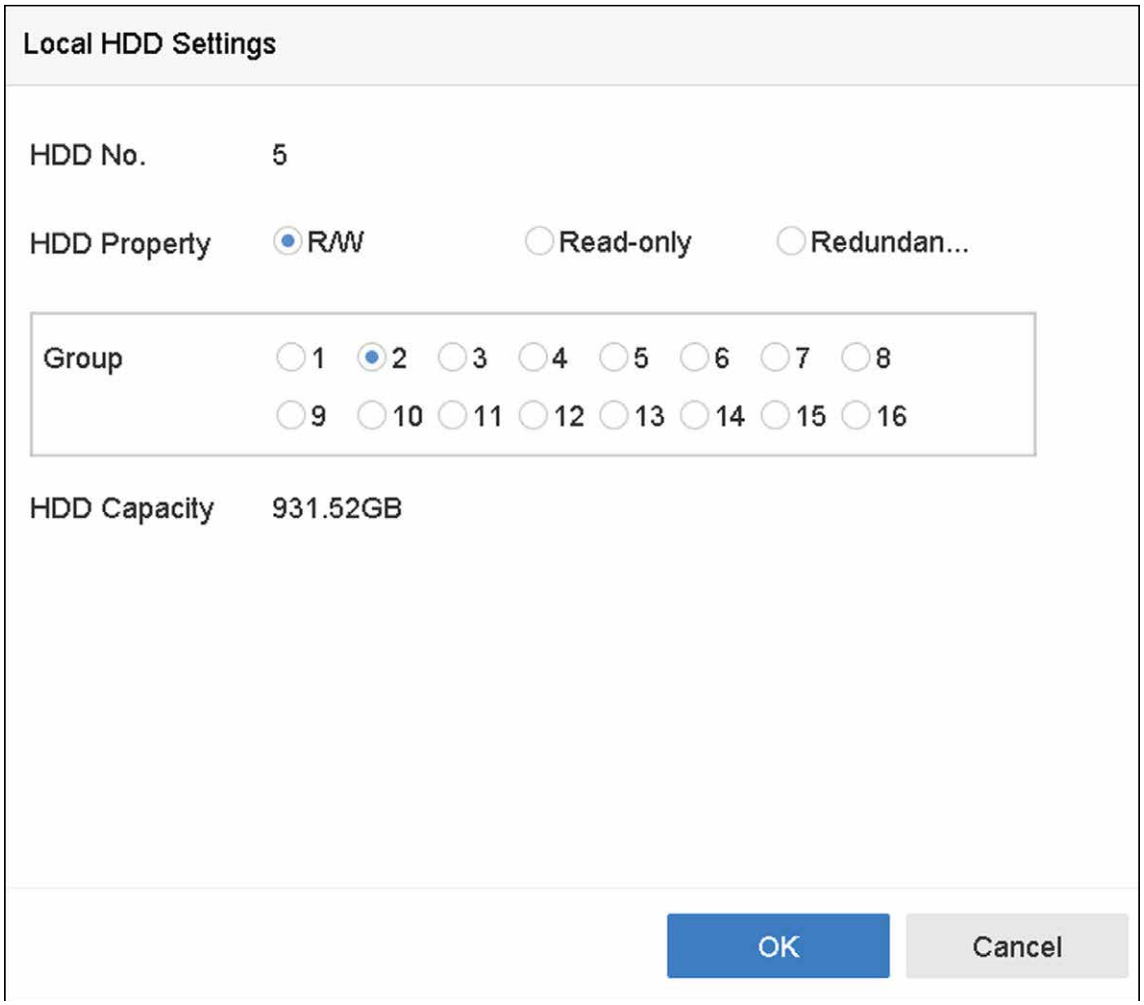


図 9-2 ローカル HDD の設定

7. HDD のグループ番号を選択します。
8. **OK** ボタンをクリックします。

メモ

HDD のグループ番号を変更した場合、HDD のカメラを再グループ化します。

9. 次の順に進みます。**Storage → Storage Mode**
10. リストからグループ番号を選択します。
11. HDD グループに動画や画像を保存する関連カメラを選択します。
12. **Apply** をクリックします。

HDD プロパティの設定

HDD のプロパティは、R/W、Read-only、Redundant のいずれかに設定可能です。

ご使用の前に

保存モードを Group に設定します。詳細な手順については **HDD グループの設定**を参照してください。

ステップ

1. 次の順に進みます。**Storage → Storage Device**
2. 希望する HDD の をクリックします。
3. **HDD Property** を選択します。

   R/W

   HDD は読み出しと書き込みの両方に対応しています。

   Read-only

   読み取り専用 HDD のファイルは上書きされません。

   Redundant

   R/W HDD だけでなく、リダンダント HDD にも動画や画像を保存することができます。データの安全性と信頼性を効果的に高めることができます。少なくともう 1 台、読み出し / 書き込みの HDD があることを確認してください。
4. **OK** ボタンをクリックします。

HDD 割り当て設定

各カメラには、動画や画像を保存するための割り当て容量を設定することができます。

ステップ

1. 次の順に進みます。**Storage → Storage Mode**
2. **Mode** は **Quota** を選択 します。
3. 割り当てを設定するカメラを選択します。
4. **Max. Record Capacity (GB)** と **Max. Picture Capacity (GB)** のテキストフィールドに記憶容量を入力します。
5. **Copy to** をクリックして、現在のカメラの割り当て設定を他のカメラにコピーします。
6. **Apply** をクリックします。

メモ

- 割り当て容量を 0 に設定すると、すべてのカメラが HDD の全容量を動画や画像に使用するようになります。
- 本機を再起動すると、新しい設定が有効になります。

9.1.2 ネットワークディスクを追加する

割り当てられた NAS や IP SAN のディスクを本機に追加し、ネットワーク HDD として使用することができます。

ステップ

1. 次の順に進みます。**Storage → Storage Device**
2. **Add** をクリックします。

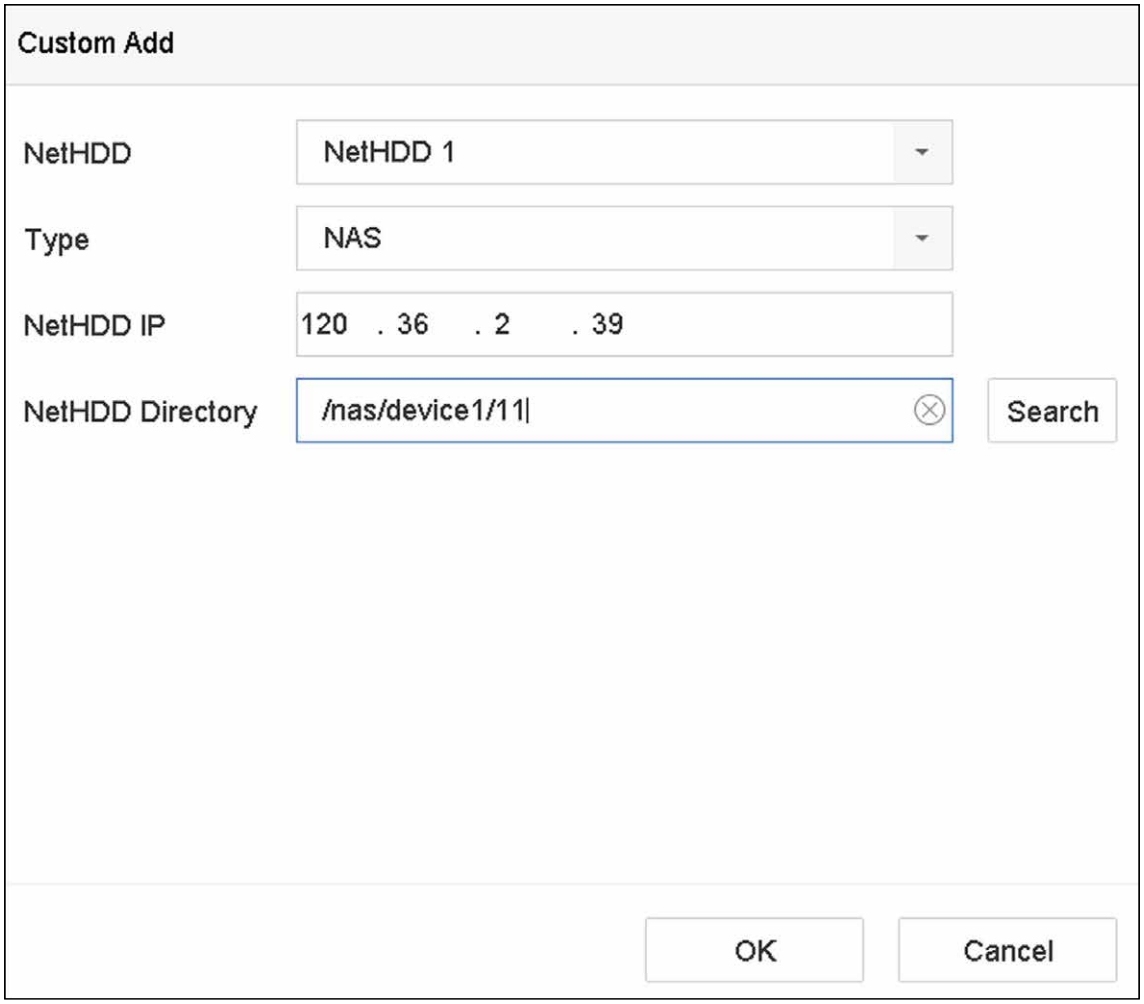


図 9-3 NetHDD の追加

3. **NetHDD** タイプを選択 します。
4. **NetHDD IP** を入力して **Search** をクリックすると利用可能な NetHDD が検索されます。
5. 希望する NetHDD を選択します。
6. **OK** ボタンをクリックします。
7. HDD 一覧に追加した NetHDD が表示されます。新しく追加された NetHDD を選択し **Init** をクリックします。

9.1.3 eSATA を管理する

メモ

eSATA 機能は一部の機種にしか搭載されていません。

データストレージ用 eSATA の設定

本機に外部 eSATA デバイスが接続されている場合、eSATA の使用状況をデータストレージとして設定し、eSATA を管理することができます。

ステップ

1. 次の順に進みます。**Storage → Advanced**
2. eSATA**Usage** は **Export** または **Record/Capture** を選択 します。

Export

eSATA はバックアップ用に使用します。

Record/Capture

録画 / キャプチャーには eSATA を使用します。操作方法については、次の手順を参照してください。

図 9-4 eSATA モード

次は

eSATA の使用方法が Record/Capture として設定されている場合は、ストレージデバイスのインターフェースに入り、プロパティを編集や初期化を行います。

自動バックアップの eSATA の設定

自動バックアップを設定した場合、本機はバックアップ開始時刻から 24 時間先のローカル動画を eSATA にバックアップします。

ご使用の前に

外付けの eSATA ハードディスクドライブが正しく接続されているか、また使用タイプが Export. として設定されているか確認してください。詳しくは **eSATA を管理する**を参照してください。

ステップ

1. 次の順に進みます。**Storage → Auto Backup**
2. **Auto Backup** をクリックします。
3. **Start Backup at** でバックアップ開始時刻を設定します。

メモ

バックアップに失敗した日は、翌日のバックアップ開始時刻の 48 時間前に本機がバックアップを行います。

4. バックアップするチャンネルを選択します。
5. 希望する **Backup Stream Type** を選択します。
6. **Overwrite** タイプを選択します。
   - **Disable**: HDD が一杯になると、書き込みを停止します。
   - **Enable**: HDD の容量がいっぱいになると、古いファイルを削除して新しいファイルの書き込みを続けます。
7. **Apply** をクリックします。

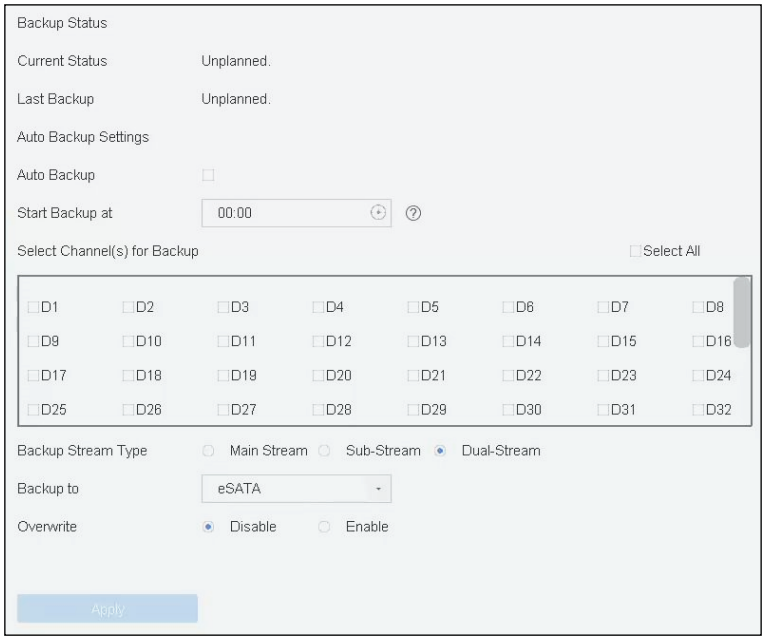


図 9-5 自動バックアップの eSATA の設定

9.2 ディスクアレイ

ディスクアレイは、複数の物理ディスクドライブを 1 つの論理ユニットにまとめたデータストレージ仮想化技術です。「RAID」とも呼ばれ、複数の HDD にデータを保存し、1 つのディスクが故障してもデータを復元できるよう、十分な冗長性を持たせています。データは、必要な冗長性と性能に基づいて、「RAID レベル」と呼ばれるいくつかの方法のいずれかでドライブに分散されます。

メモ

このセクションの機能は、特定のモデルでのみ使用できます。

9.2.1 ディスクアレイを作成する

本機は、ソフトウェアベースのディスクアレイをサポートしています。必要に応じて RAID 機能を有効にし、各 HDD の容量が 4TB 以上であることを確認してください。本機の SATA インターフェースが 16 個以下の場合、ディスクアレイに搭載できる HDD は 8 台までとなります。本機に 24 個の SATA インターフェイスがある場合、ディスクアレイに搭載できる HDD は 12 個までとなります。アレイの作成には、ワンタッチ設定と手動設定の 2 つの方法があります。

ワンタッチ作成

ワンタッチ設定でディスクアレイを作成します。ワンタッチ設定で作成されるアレイの種類は、デフォルトで RAID 5 です。

ご使用の前に

HDD を 3 台以上搭載してください。10 台以上の HDD を搭載した場合、2 つのアレイが作成されます。HDD の信頼性と安定した動作を維持するために、同じモデル、容量のエンタープライズクラスの HDD を使用することをお勧めします。

ステップ

1. 次の順に進みます。**Storage → Advanced**
2. **Enable RAID** にチェックを入れます。
3. **Apply** をクリックし本機を再起動すると、設定が有効になります。
4. 再起動後、次の順に進みます。**Storage → RAID Setup → Physical Disk**
5. **One-touch Config.** をクリックします。
6. **Array Name** を編集して **OK** をクリックすると、設定を開始します。

メモ

4 台以上の HDD を搭載した場合、アレイ再構築用のホットスペアディスクが作成されます。

7. オプション：作成された配列は、本機が自動的に初期化します。**Storage → RAID Setup → Array** の順に進むと作成された配列の情報が表示されます。

手動作成

RAID 0、RAID 1、RAID 5、RAID 6、または RAID 10 アレイを手動で作成します。

ステップ

1. 次の順に進みます。**Storage → Advanced**
2. **Enable RAID** にチェックを入れます。
3. **Apply** をクリックし本機を再起動すると、設定が有効になります。
4. 再起動後、次の順に進みます。**Storage → RAID Setup → Physical Disk**
5. **Create** をクリックします。

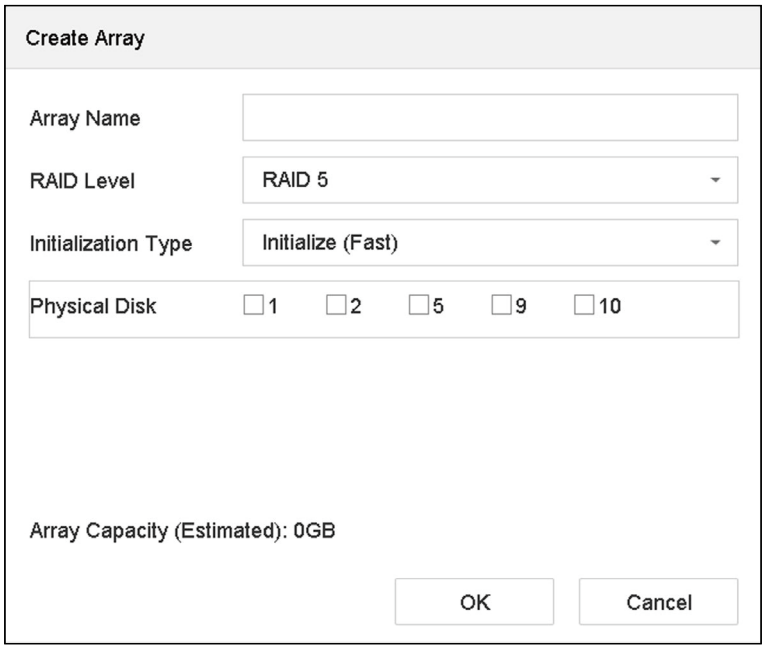


図 9-6 アレイの作成

6. **Array Name** を入力します。
7. 必要とする **RAID Level** を選択します。
8. アレイを設定する物理ディスクを選択します。

表 9-1 必要な HDD の台数

RAID Level	必要な HDD の台数
RAID 0	HDD2 台以上
RAID 1	HDD2 台以上
RAID 5	HDD3 台以上
RAID 6	HDD4 台以上
RAID 10	HDD の台数は 4 台から 16 台の偶数台である必要があります。

9. **OK** ボタンをクリックします。
10. オプション：作成された配列は、本機が自動的に初期化します。**Storage → RAID Setup → Array** の順に進むと作成された配列の情報が表示されます。

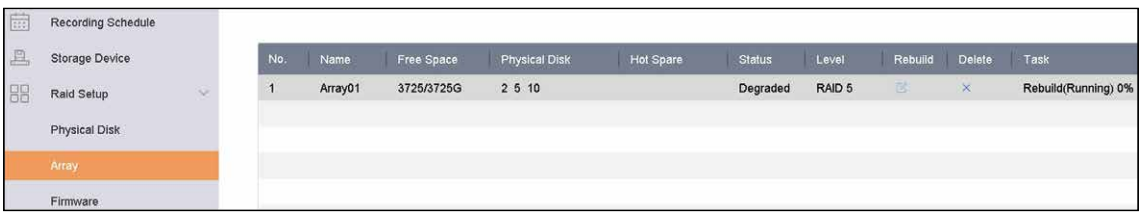


図 9-7 アレイリスト

9.2.2 アレイを再構築する

アレイのステータスは、Functional、Degraded、Offline があります。アレイに保存されたデータの高い安全性と信頼性を確保するために、アレイのステータスに応じて迅速かつ適切なメンテナンスを行ってください。

Functional

アレイのディスクロスはありません。

Offline

失われたディスクの数が上限を超えました。

Degraded

アレイのいずれかの HDD に障害が発生した場合、アレイが劣化します。アレイの再構築で Functional ステータスに戻します。

ホットスペアディスクの設定

ホットスペアディスクは、ディスクアレイの自動再設定に必要です。

ステップ

1. 次の順に進みます。**Storage → RAID Setup → Physical Disk**

No.	Capacity	Array	Type	Status	Model	Hot Spare	Task
1	1863.02GB	Array01	Array	Functional	ST2000VX000-1CU164	-	None
2	2794.52GB		Normal	Functional	ST3000VX000-9YW166		None
5	1863.02GB	Array01	Array	Functional	ST2000VX000-1CU164	-	None
9	2794.52GB		Normal	Functional	ST3000VX000-1CU166		None
10	1863.02GB	Array01	Array	Functional	ST2000VX000-1CU164	-	None

図 9-8 物理ディスク

2. 使用できる HDD の をクリックし、ホットスペアディスクとして設定します。

アレイを自動で再構築

本機は、ホットスペアディスクを使用して、劣化したアレイを自動的に再構築することができます。

ご使用の前に

ホットスペアディスクを作成します。詳しくは**ホットスペアディスクの設定**を参照してください。

ステップ

1. 次の順に進みます。**Storage → RAID Setup → Array**

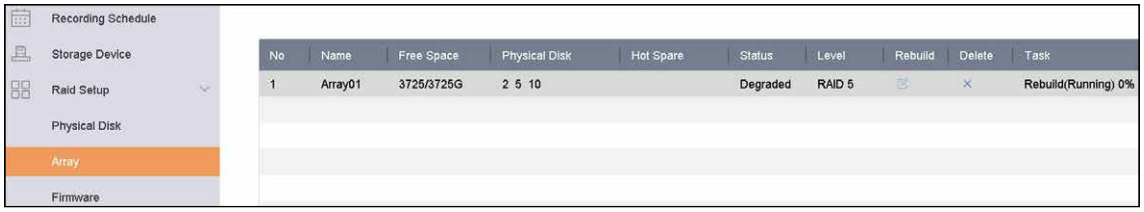


図 9-9 アレイリスト

手動でアレイを再構築する

ホットスペアディスクが設定されていない場合、劣化したアレイを手動で再構築します。

ご使用の前に

アレイを再構築するには、少なくとも 1 つの利用可能な物理ディスクが必要となります。

ステップ

1. 次の順に進みます。**Storage → RAID Setup → Array**
2. 劣化したアレイの をクリックします。

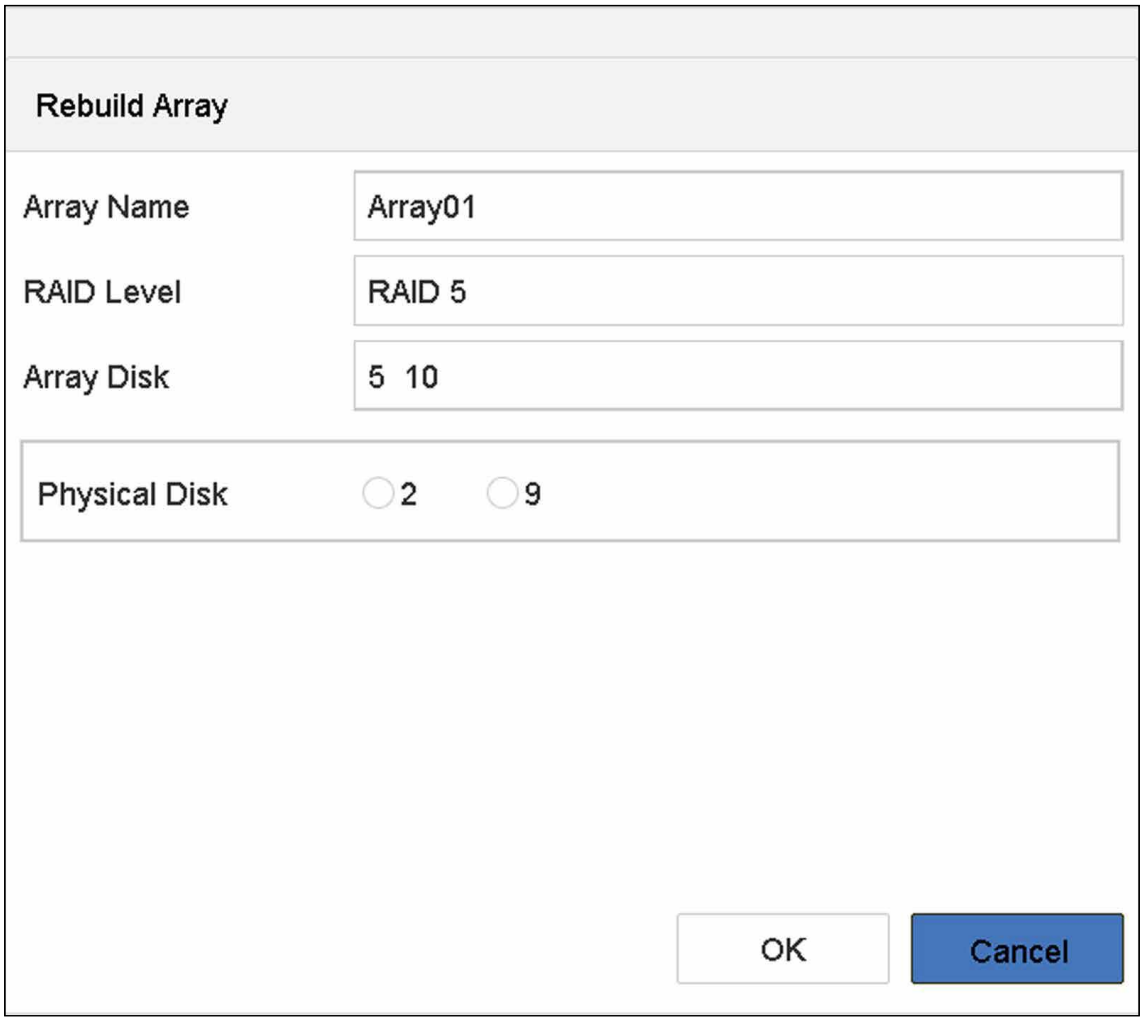


図 9-10 アレイの再構築

3. 利用可能な物理ディスクを選択します。
4. **OK** ボタンをクリックします。
5.「Do not unplug the physical disk when it is under rebuilding.」のポップアップメッセージボックスで **OK** をクリックします。

第 10 章 ネットワーク設定

10.1 DDNS の設定

ネットワークアクセスに Dynamic DNS サービスを設定することができます。異なる DDNS モードが利用できます。DynDNS、PeanutHull、NO-IP の 3 つです。

ご使用の前に

DDNS の設定を行う前に、DynDNS、PeanutHull、NO-IP の各サービスを ISP に登録する必要があります。

ステップ

1. 次の順に進みます。**System → Network → TCP/IP → DDNS**

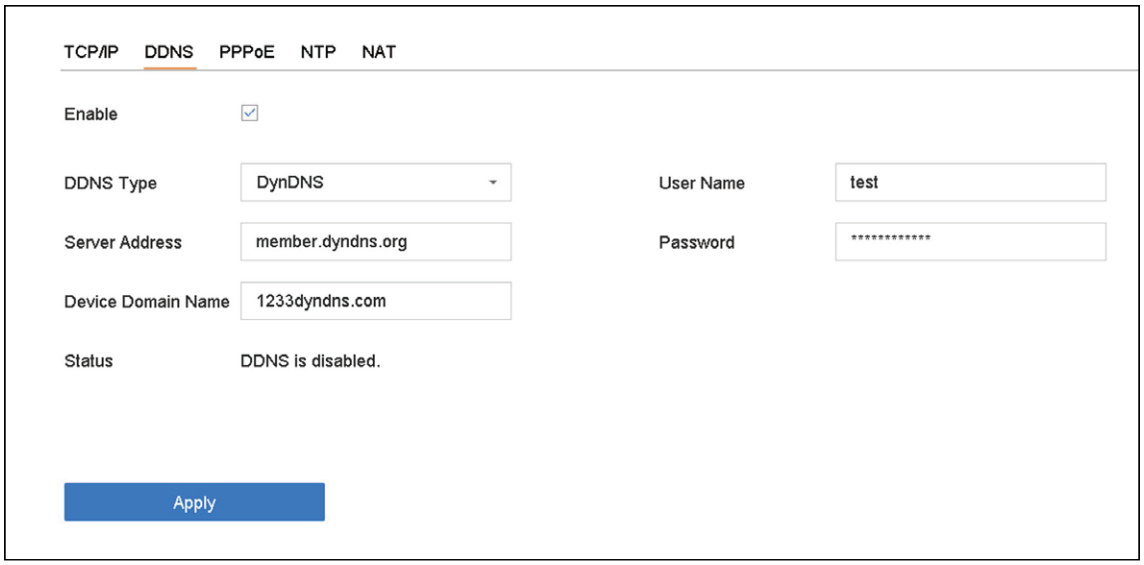


図 10-1 DDNS 設定

2. **Enable** にチェックを入れます。
3. **DDNS Type** は DynDNS を選択します。
4. DynDNS の Server Address を入力します。（例：members.dyndns.org）
5. Device Domain Name に、DynDNS ウェブサイトから取得したドメイン名を入力します。
6. DynDNS のウェブサイトに登録されている **User Name** と **Password** を入力します。
7. **Apply** をクリックします。

10.2 PPPoE の設定

本機が PPPoE でインターネットに接続されている場合、ユーザー名とパスワードを **System → Network → TCP/IP → PPPoE** で設定する必要があります。
PPPoE サービスの詳細については、ご利用のインターネットサービスプロバイダーにお問い合わせください。

10.3 ポートマッピング (NAT) の設定

クロスセグメントネットワークによるリモートアクセスを可能にするために、UPnP™ とマニュアルマッピングの 2 種類のポートマッピングがあります。

ご使用の前に

本機の UPnP™ 機能を有効にする場合は、本機が接続されているルーターの UPnP™ 機能を有効にする必要があります。本機のネットワーク動作モードがマルチアドレスに設定されている場合、本機のデフォルトルートは、ルーターの LAN IP アドレスと同じネットワークセグメントにある必要があります。
ユニバーサルプラグアンドプレイ（UPnP™）は、ネットワーク上の他のネットワーク機器の存在をシームレスに検出し、データ共有、通信などのための機能的なネットワークサービスを確立することを可能にします。UPnP™ 機能を使用すると、ポートマッピングなしでルーターを介してデバイスの WAN への高速接続することができます。

ステップ

1. 次の順に進みます。**System → Network → TCP/IP → NAT**

図 10-2 ポートマッピングの設定

2. **Enable** にチェックを入れます。
3. **Mapping Type** は **Manual** または **Auto** を選択します。
   – 自動：**Auto** を選択した場合、ポートマッピングの項目は読み取り専用で、外部ポートはルーターが自動的に設定します。
   – 手動：**Manual** を選択した場合、**External Port Settings** をクリックして有効にし、必要に応じて外部ポートを編集することができます。

メモ

- ポート番号はデフォルトで使用することもできますが、実際の要件に応じて変更することができます。
- External Port は、ルーターのポートマッピングのためのポート番号を示します。
- RTSP ポート No. は 554 または 1024 ～ 65535、その他のポートは 1 ～ 65535 で、それぞれ異なる値である必要があります。同じルーターで複数の機器を UPnP™ 設定する場合、各機器のポート番号は固有である必要があります。

4. ルーターの仮想サーバー設定画面に入り、**Internal Source Port** の欄に内部ポートの値、**External Source Port** の空欄に外部ポートの値、その他必要な内容を入力します。

メモ

- 各項目は、サーバーポート、http ポート、RTSP ポート、https ポートなど、本機のポートに対応している必要があります。
- 以下の仮想サーバーの設定インターフェースは参考値で、ルーターの製造元により異なる場合があります。仮想サーバーの設定に問題がある場合は、ルーターの製造元にお問い合わせください。

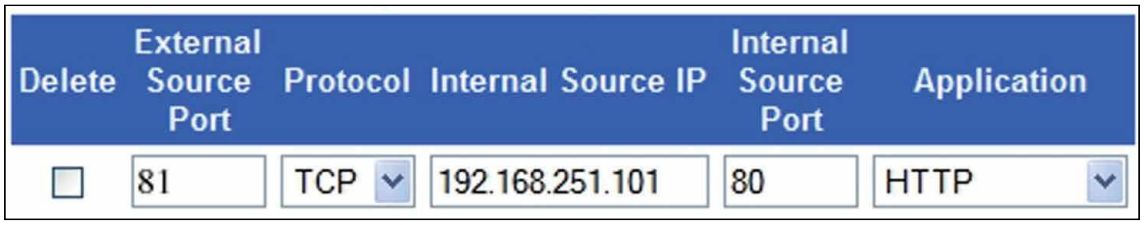


図 10-3 仮想サーバー項目の設定

10.4 Wi-Fi の設定

Wi-Fi ドングルを使って、本機を無線ネットワークに接続することができます。この機能は一部の機種のみ対応しています。

ご使用の前に

Wi-Fi ドングルを用意し、リアパネルの USB インターフェースに挿入します。

ステップ

1. 次の順に進みます。**System → Network → TCP/IP → Wi-Fi**

図 10-4 ワイヤレスネットワークに接続

2. **Enable Wi-Fi** にチェックを入れます。
3. ワイヤレスネットワークに接続します。

自動的に検索されたワイヤレスネットワークに接続する

1. リストから任意の無線 LAN をダブルクリックします。
2. ワイヤレスネットワークのパラメーターを設定します。
3. **OK** ボタンをクリックします。

カスタマイズされたワイヤレスネットワークへの接続

1. **Custom Adding** をクリックします。
2. ワイヤレスネットワークのパラメーターを設定します。
3. **OK** ボタンをクリックします。

WPS（Wi-Fi Protected Setup）でワイヤレスネットワークに接続する

1. **WPS Settings** をクリックします。
2. **Enable WPS** にチェックを入れます。
3. ワイヤレスネットワークのパラメーターを設定します。
4. **Apply** をクリックします。

利用可能なワイヤレスネットワークに接続した後、**Connection Status** で接続結果を見ることができます。

4. 次の順に進みます。**System → Network → TCP/IP → TCP/IP**
5. **NIC** と**デフォルトルート**を **WLAN0** として設定します。
6. 他のネットワークパラメータを設定します。
7. **Apply** をクリックします。

10.5 SNMP の設定

SNMP の設定を行うことで、デバイスのステータスやパラメータ情報を取得できます。

ご使用の前に

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の情報を受信します。トラップアドレスとポートを設定することで、本機はアラームイベントと異常メッセージを監視センターに送信できるようになります。

ステップ

1. 次の順に進みます。**System → Network → Advanced → SNMP**

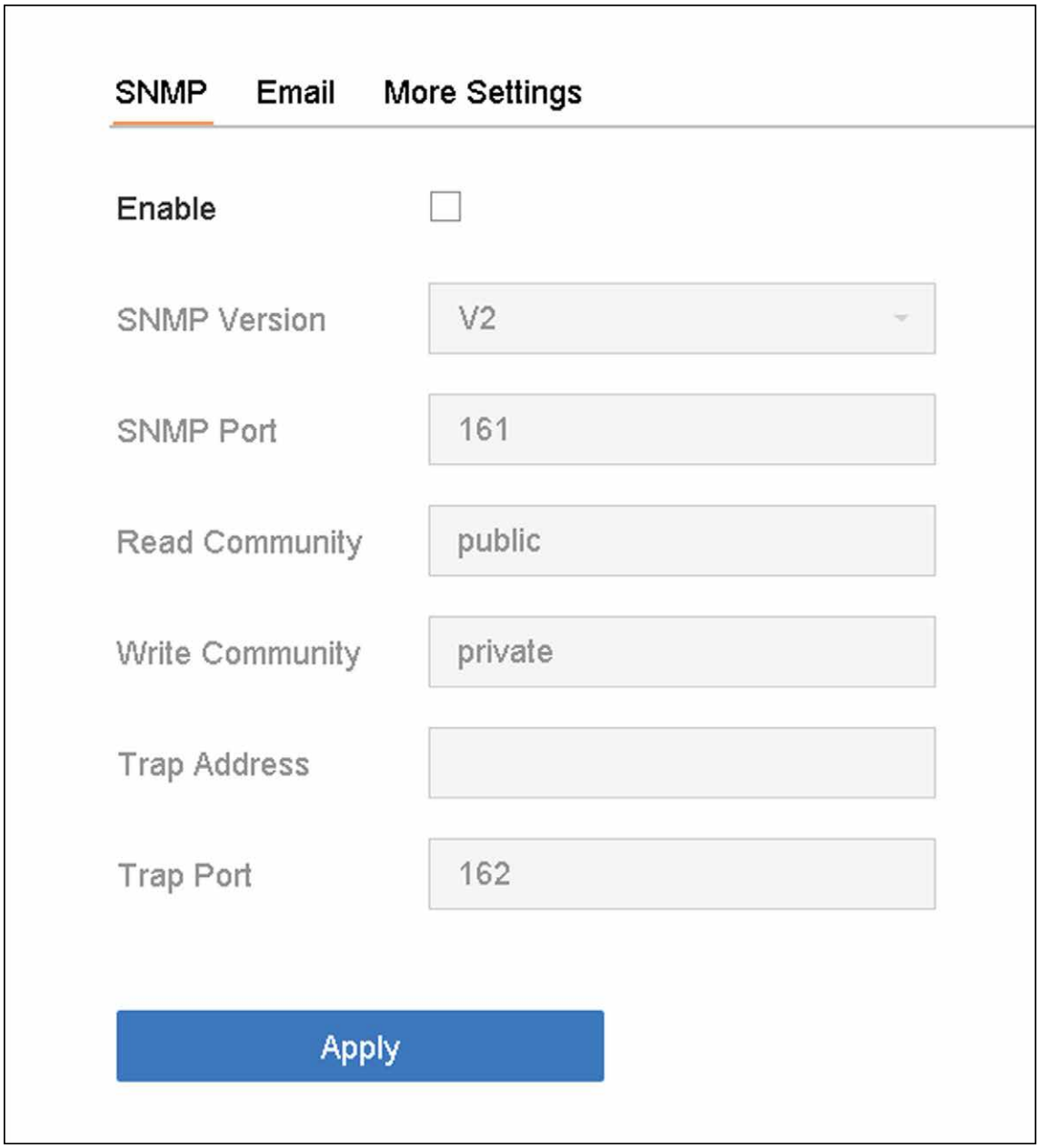


図 10-5 SNMP 設定

2. **Enable** にチェックを入れます。セキュリティリスクの可能性を通知するメッセージがポップアップ表示されます。**Yes** をクリックして続けます。
3. 必要に応じて、SNMP の設定を行ってください。

Trap Address

SNMP ホストの IP アドレスです。

Trap Port

SNMP サーバーのポートです。

4. **Apply** をクリックします。

メモ

Configuration → System → Advanced Settings → SNMP で、Web ブラウザから SNMP v2 および SNMP v3 のパラメータを設定することができます。

10.6 電子メールの設定

このシステムは、アラームや動体イベントを検知したとき、管理者パスワードを変更したとき、指定したイベントが発生したとき等に、指定したユーザー全員に電子メールで通知するよう設定することができます。

ご使用の前に

本機が SMTP メールサーバーがあるローカルエリアネットワーク（LAN）に接続されている必要があります。また、通知を送信するメールアカウントの場所によって、イントラネットまたはインターネットに接続されている必要があります。

ステップ

1. 次の順に進みます。**System → Network → Advanced → Email**
2. 電子メールの設定をします。

Server Authentication

SMTP サーバーがユーザー認証を必要とする場合、この機能を有効にするようチェックを入れ、ユーザー名とパスワードを適宜入力してください。

SMTP Server

SMTP サーバーの IP アドレスまたはホスト名（例：smtp.263xmail.com）です。

SMTP Port

SMTP ポートです。SMTP に使用される TCP/IP ポートのデフォルトは 25 です。

Enable SSL/TLS

SMTP サーバーで必要な場合、SSL/TLS を有効にするようチェックを入れます。

Sender

送信者の名前です。

Sender's Address

送信者のアドレスです。

Select Receivers

受信者を選択します。受信者は最大 3 名まで設定可能です。

Receiver

受信者の名前です。

Receiver's Address

通知するユーザーの電子メールアドレスです。

Attached Image

アラーム画像を添付してメール送信する場合はチェックを入れます。インターバルは、後続の 2 つのアラーム画像を送信する間の時間です。

Interval

添付画像をキャプチャーする時間間隔です。

3. オプション：代替 SMTP を有効にし、代替 SMTP に必要なパラメータを設定します。優先 SMTP が無効な場合、本機は代替 SMTP を使用してメールを送信します。
4. オプション：**Test** をクリックして、テストメールを送信してください。
5. **Apply** をクリックします。

10.7 ポートの設定

関連する機能を有効にするために、異なるタイプのポートを設定することができます。

ステップ

1. **次の順に進みます。System → Network → Advanced → More Settings**

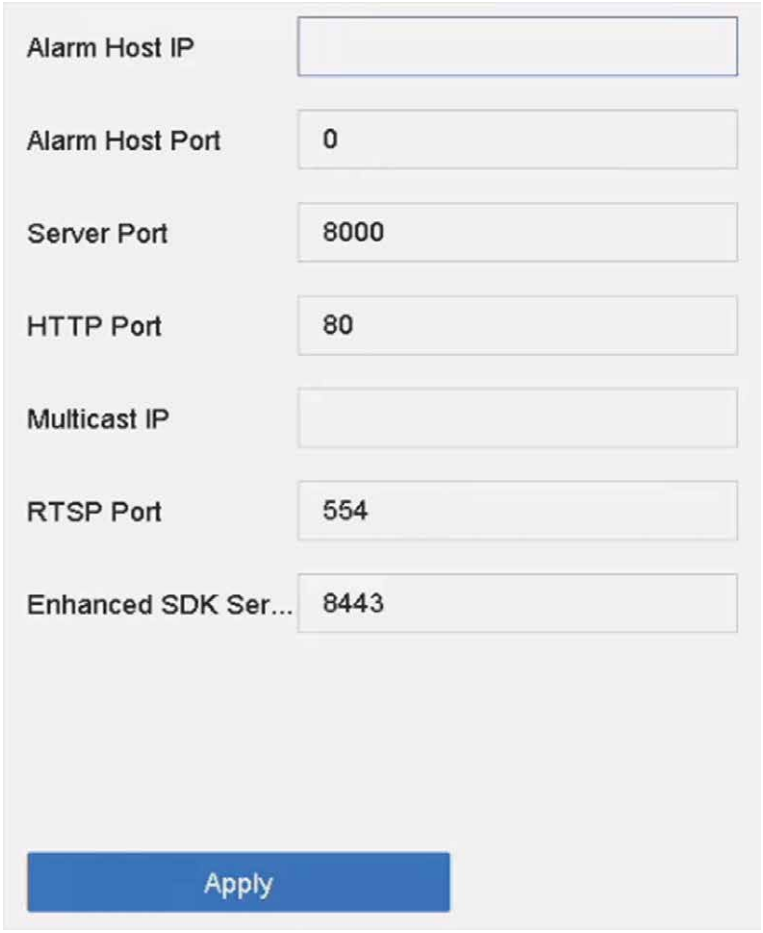


図 10-6 ポートの設定

2. 必要に応じて、ポートの設定を行います。

アラームホストの IP/ ポート

リモートアラームホストを設定すると、本機はアラームが作動されたとき、アラームイベントまたは異常メッセージをホストに送信します。リモートアラームホストには、クライアント管理システム（CMS）ソフトウェアがインストールされている必要があります。アラームホスト IP とは、CMS ソフトウェア（例：iVMS-4200）がインストールされているリモート PC の IP アドレスを指し、アラームホストポート（デフォルトでは 7200）は、ソフトウェアで設定したアラーム監視ポートと同じである必要があります。

Server Port

サーバーポート（デフォルトでは 8000）は、リモートクライアントソフトウェアのアクセス用に設定する必要があり、その有効範囲は 2000 から 65535 です。

HTTP Port

HTTP ポート（デフォルトでは 80）は、リモート Web ブラウザーのアクセス用に設定されている必要があります。

Multicast IP

マルチキャストは、ネットワークで許可された最大数を超えるカメラのライブビューを有効にするために設定することができます。マルチキャスト IP アドレスは、IPv4 と IPv6 の両方が使用できます。IPv4 では、224.0.0.0 ～ 239.255.255.255 の Class-D IP をカバーしており、239.252.0.0 ～ 239.255.255.255 の IP アドレスを使用することが推奨されます。CMS ソフトウェアに機器を追加する場合、マルチキャストアドレスは機器のものと同じである必要があります。

RTSP Port

RTSP（Real Time Streaming Protocol）は、ストリーミングメディアサーバーを制御するために設計されたネットワーク制御プロトコルです。ポートはデフォルトで 554 です。

Enhanced SDK Service Port

拡張 SDK サービスは、より安全なデータ転送を提供する SDK サービス上で TLS プロトコルを採用しています。ポートはデフォルトで 8443 です。

3. **Apply** をクリックします。

10.8 ONVIF の設定

ONVIF プロトコルにより、他社製カメラとの接続が可能です。追加されたユーザーアカウントは、ONVIF プロトコル経由で他の機器を接続する権限を持ちます。

ステップ

1. 次の順に進みます。**Maintenance → System Service → ONVIF**
2. **Enable ONVIF** にチェックを入れて、ONVIF アクセス管理を有効にします。

メモ

ONVIF プロトコルはデフォルトでは無効になっています。

3. **Add** をクリックします。
4. **User Name** と **Password** を入力します。

メモ

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

5. **Level** は **Media User**、**Operator** または **Admin** を選択します。
6. **OK** ボタンをクリックします。

第 11 章 ユーザー管理とセキュリティ

11.1 ユーザーアカウントの管理

管理者のユーザー名は admin で、パスワードは初回起動時に設定されます。管理者は、ユーザーの追加と削除、およびユーザーのパラメータを設定する権限を持っています。

11.1.1 ユーザーを追加する

ステップ

1. 次の順に進みます。**System → User**
2. **Add** をクリックして、操作許可インターフェースに入ります。
3. 管理者パスワードを入力し OK をクリックします。
4. 「ユーザーの追加」インターフェースで、新しいユーザーの情報を入力します。

メモ

強力なパスワードの推奨—製品のセキュリティを高めるため、お客様ご自身で強力なパスワード（大文字、小文字、数字、特殊文字のうち少なくとも 3 つを含む 8 文字以上）を設定することを強くお勧めします。また、定期的にパスワードを再設定することをお勧めします。特にセキュリティの高いシステムでは、毎月または毎週パスワードをリセットすることで、製品をより安全に保護することができます。

User Level

ユーザーレベルを Operator または Guest に設定します。ユーザーレベルによって操作権限が異なります。

- Operator：Operator ユーザーレベルは、デフォルトで Remote Configuration の Two-way Audio 権限と Camera Configuration のすべての操作権限を持っています。
- Guest：Guest ユーザーには、Remote Configuration での Two-way Audio 権限はなく、Camera Configuration でのローカル / リモート再生の権限のみがデフォルトで与えられています。

User's MAC Address

本機にログオンするリモート PC の MAC アドレスです。設定され有効になっている場合、この MAC アドレスを持つリモートユーザーのみが本機にアクセスできるようになります。

5. **OK** ボタンをクリックします。
ユーザー管理インターフェイスでは、追加された新しいユーザーがリストに表示されます。

11.1.2 管理者ユーザーを編集する

管理者ユーザーアカウントでは、パスワードとロック解除パターンを変更できます。

ステップ

1. 次の順に進みます。**System → User**
2. リストから管理者ユーザーを選択します。
3. **Modify** をクリックします。

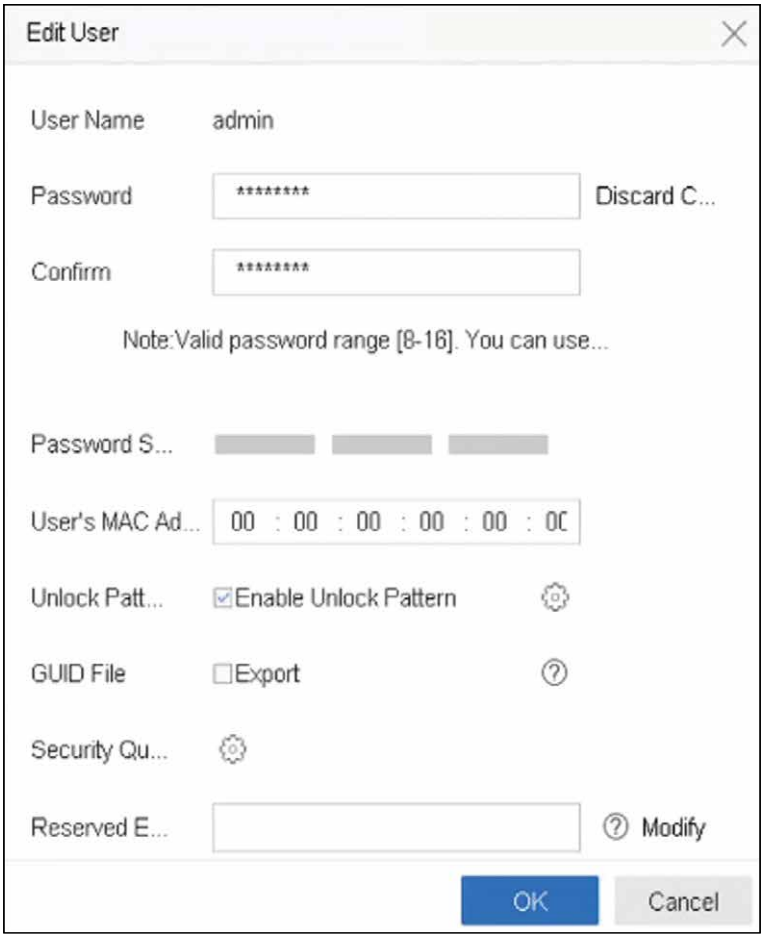


図 11-1 ユーザー（管理者）の編集

4. 新しい管理者パスワード（強力なパスワードが必要です）や MAC アドレスなど、管理者ユーザー情報を必要に応じて編集してください。
5. 管理者ユーザーアカウントのロック解除パターンを編集します。
   1）**Enable Unlock Pattern** にチェックを入れると、本機にログインする際にロック解除パターンを使用できるようになります。
   2) マウスで画面上の 9 つのドットの間にパターンを描画し、パターンが完成したらマウスを離します。

6. **GUID File** の **Export** をクリックして管理者ユーザーアカウントの GUID ファイルをエクスポートします。

> **メモ**
>
> 管理者パスワードを変更した場合、将来のパスワード再設定のために、Import/Export インターフェースで新しい GUID を接続した USB フラッシュドライブにエクスポートしてください。

7. パスワード再設定のためのセキュリティ質問を設定します。
8. パスワード再設定用の予約メールを設定します。
9. **OK** ボタンをクリックして、設定を保存します。

11.1.3 Operator/Guest User を編集する

ユーザー名、パスワード、権限レベル、MAC アドレスなどのユーザー情報を編集することができます。

ステップ

1. 次の順に進みます。**System → User**
2. リストからユーザーを選択し **Modify** をクリックします。

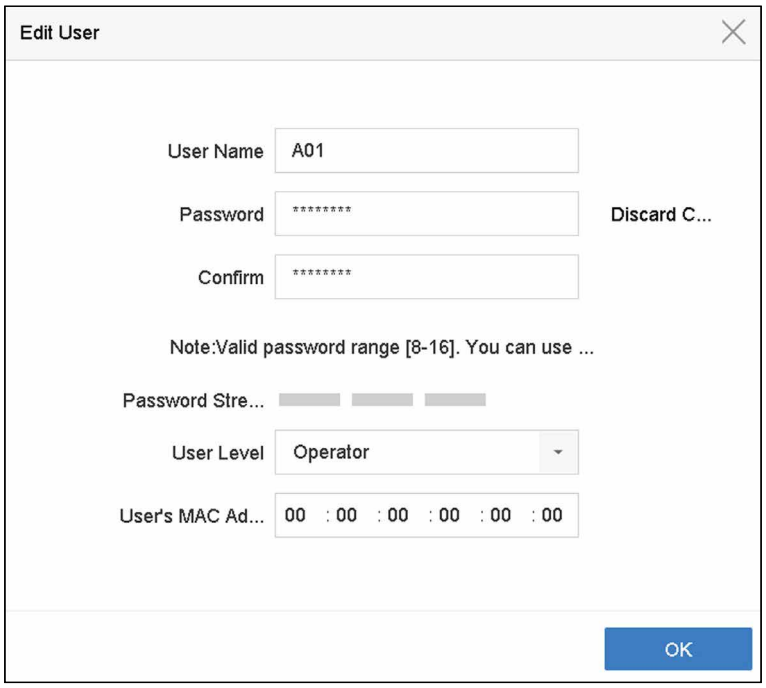


図 11-2 ユーザー（Operator/Guest）の編集

3. 新しいパスワード（強力なパスワードが必要です）、MAC アドレスなど、ユーザー情報を必要に応じて編集してください。
4. **OK** ボタンをクリックします。

11.2 ユーザー権限の管理

11.2.1 ユーザー権限を設定する

追加されたユーザーには、本機のローカルおよびリモート操作など、さまざまな権限を割り当てることができます。

ステップ

1. 次の順に進みます。**System → User**
2. 一覧からユーザーを選択し をクリックして、権限設定のインターフェースに入ります。

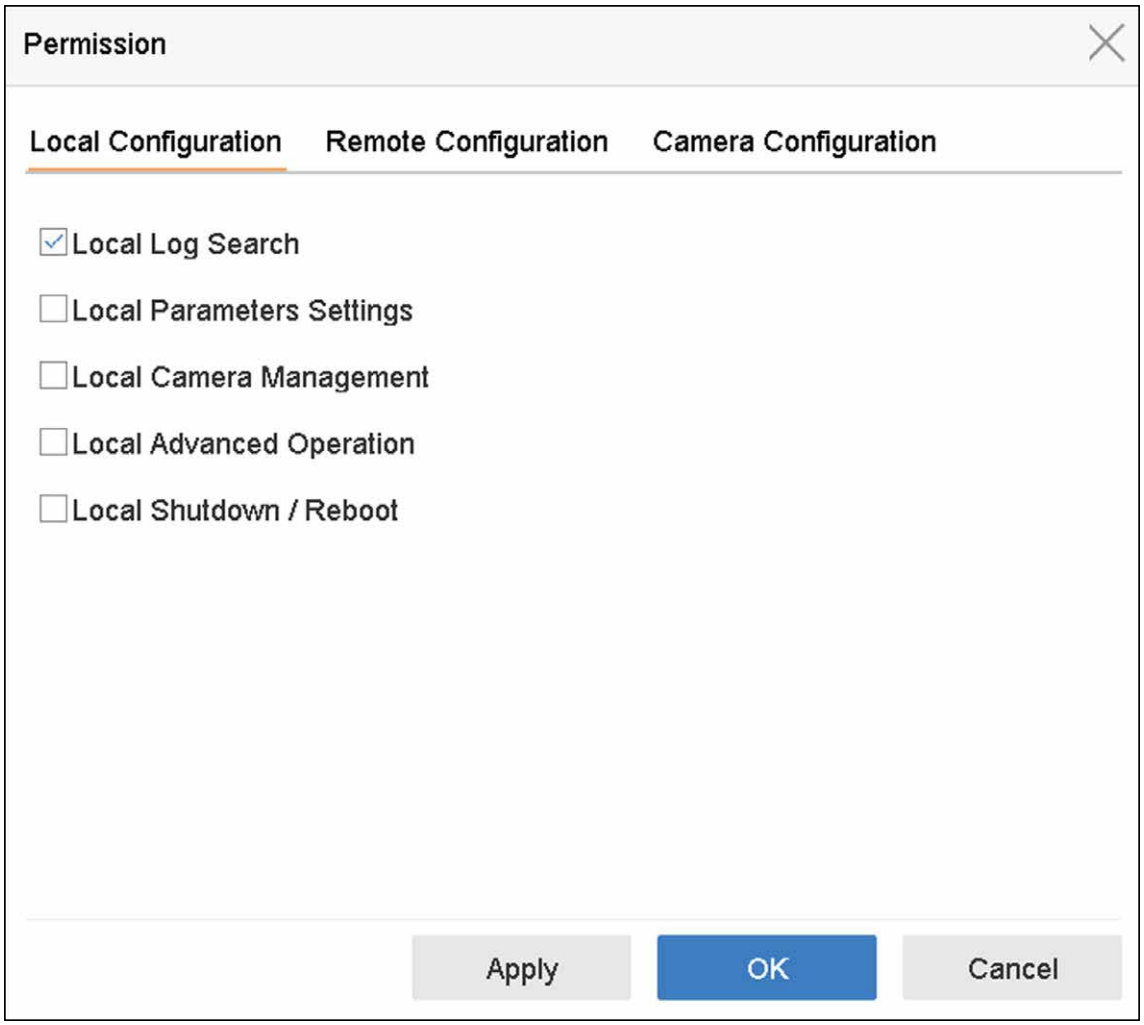


図 11-3 ユーザー権限設定インターフェース

3. **Local Configuration、Remote Configuration、Camera Configuration** のユーザー操作権限を設定します。
   1）ローカル設定を行います。

   Local Log Search

   本機のログやシステム情報を検索したり閲覧することができます。

   Local Parameters Settings

   パラメータの設定、工場出荷時のパラメータの復元、設定ファイルのインポート / エクスポートを行います。

   Local Camera Management

   IP カメラの追加、削除、編集を行います。

   Local Advanced Operation

   HDD 管理（HDD の初期化、HDD のプロパティ設定）、システムファームウェアのバージョンアップ、I/O アラーム出力のクリアを行います。

   Local Shutdown Reboot

   本機のシャットダウンまたは再起動を行います。

   2）リモート設定を行います。

   Remote Log Search

   本機に保存されているログをリモートで閲覧することができます。

   Remote Parameters Settings

   リモートでのパラメータ設定、工場出荷時のパラメータへの復元、設定ファイルのインポート / エクスポートを行います。

   Remote Camera Management

   IP カメラのリモート追加、削除、編集を行います。

   Remote Serial Port Control

   RS-232、RS-485 のポート設定に関する設定を行います。

   Remote Video Output Control

   リモートボタン制御信号を送信します。

   Two-Way Audio

   リモートクライアントと本機の間の双方向無線を行います。

   Remote Alarm Control

   リモートでアーミング（リモートクライアントにアラームと異常メッセージを通知）およびアラーム出力の制御を行います。

   Remote Advanced Operation

   HDD 管理（HDD 初期化、HDD プロパティ設定）、システムファームウェアのバージョンアップ、I/O アラーム出力のクリアをリモートで行います。

   Remote Shutdown/Reboot

   リモートで本機のシャットダウンや再起動を行います。

3) カメラの設定を行います。

Remote Live View

選択したカメラ（複数可）のライブ映像を遠隔で見ることができます。

Local Manual Operation

選択したカメラの手動録画およびアラーム出力をローカルで開始 / 停止することができます。

Remote Manual Operation

選択したカメラの手動録画およびアラーム出力を遠隔で開始 / 停止することができます。

Local Playback

選択したカメラの録画ファイルをローカルで再生します。

Remote Playback

選択したカメラの録画ファイルをリモートで再生する。

Local PTZ Control

選択したカメラの PTZ 動作をローカルで制御します。

Remote PTZ Control

選択したカメラ（複数可）の PTZ 動作を遠隔で操作します。

Local Video Export

選択したカメラ（複数可）の録画ファイルをローカルでエクスポートします。

Local Live View

選択したカメラ（複数可）のライブ映像をローカルで表示します。

4. **OK** ボタンをクリックして、設定を保存します。

11.2.2 ロック画面のライブビューの権限を設定する

管理者ユーザーは、端末の画面ロックステータスで、特定のカメラにライブビューの権限を設定することができます。

- 管理者ユーザーは、ユーザーアカウントに対してこの権限を設定することができます。
- 一般ユーザー（オペレーターまたはゲスト）に特定のカメラに対するローカルライブビュー権限がない場合、ロック画面ステータスでの当該カメラのライブビュー権限を設定することはできません（デフォルトでライブビューは許可されていません）。

ステップ

1. 次の順に進みます。**System → User**
2. **Live View Permission on Lock Screen** をクリックします。
3. 管理者パスワードを入力し **Next** をクリックします。

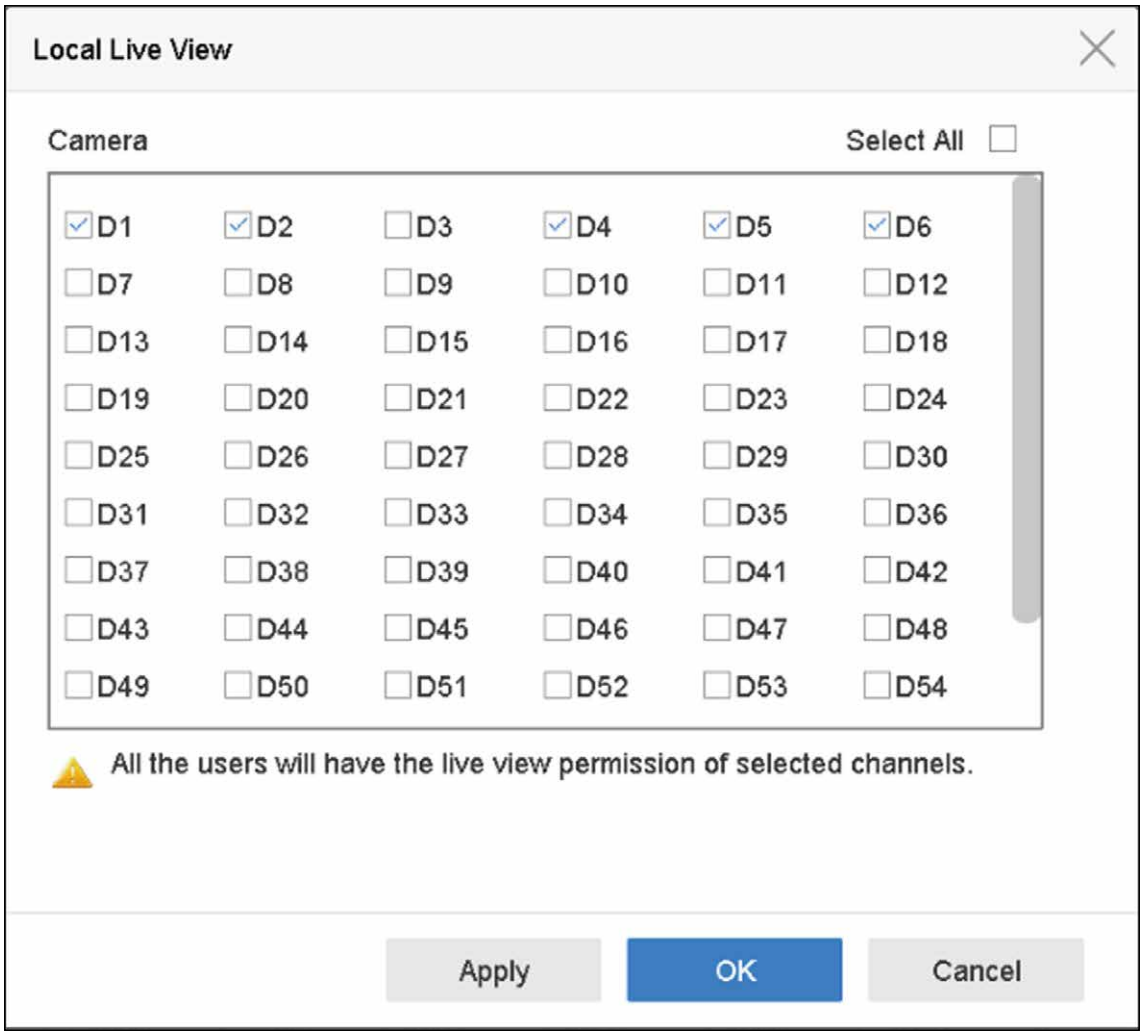


図 11-4 ロック画面のライブビューの権限設定

4. 権限を設定します。現在のユーザーアカウントがログアウトのステータスのとき、ライブビューを許可するカメラ（複数可）を選択します。
5. **OK** ボタンをクリックします。

11.3 パスワードセキュリティの設定

11.3.1 GUID ファイルをエクスポートする

GUID ファイルは、パスワードを忘れたときに、パスワードをリセットするのに役立ちます。Web ブラウザーから GUID ファイルをエキスポートすことができます。GUID ファイルは適切に保管してください。

ご使用の前に

本機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。

ステップ

1. 次の順に進みます。**Configuration → System → User Management → User Management**
2. 管理者ユーザーを選択します。
3. **Account Security Settings** をクリックします。
4. **Modify** をクリックします。

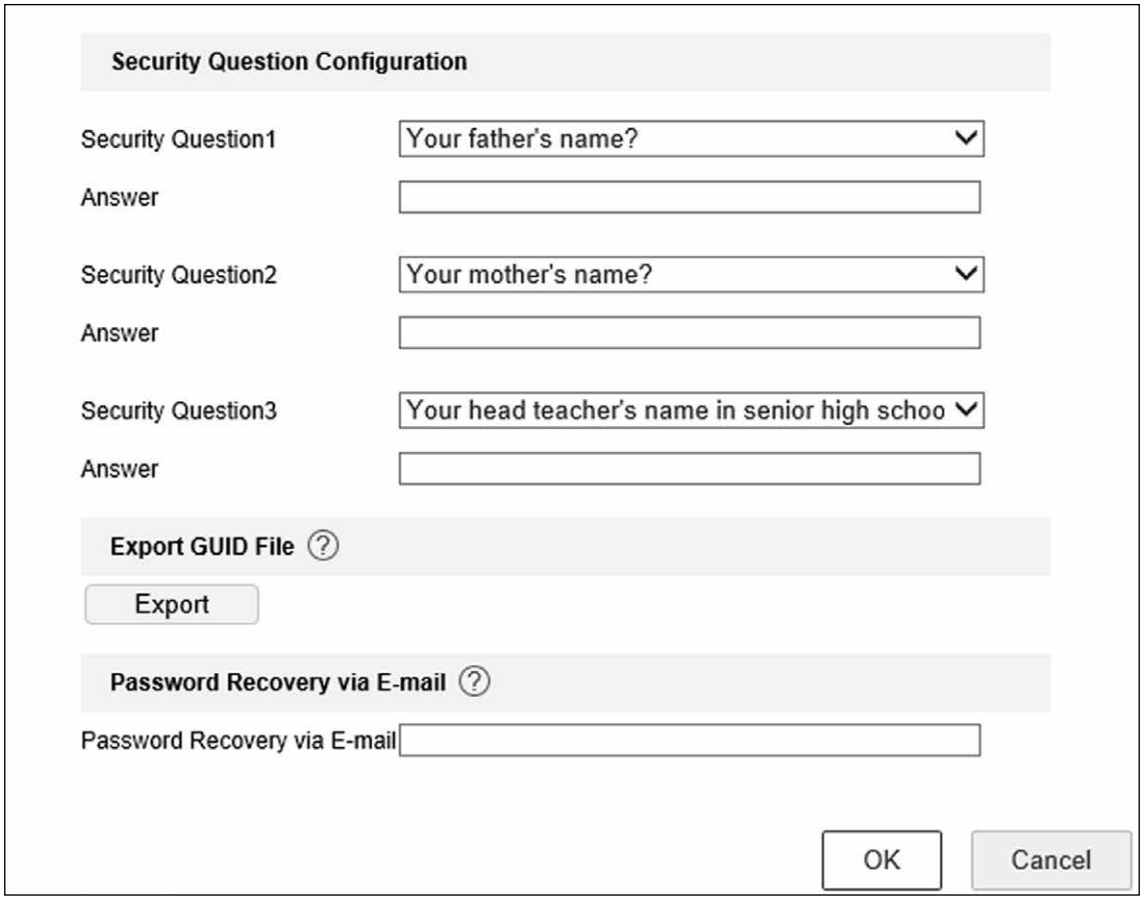


図 11-5 GUID ファイルをエクスポートする

5. **Export GUID File** の **Export** をクリックします。
6. 管理者パスワードを入力します。
7. GUID ファイルを任意のディレクトリに保存します。

11.3.2 セキュリティに関する質問を設定する

セキュリティに関する質問は、パスワードを忘れたときやセキュリティ上の問題が発生したときに、パスワードをリセットするのに役立ちます。Web ブラウザーから セキュリティに関する質問を設定することができます。

ご使用の前に

本機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。

ステップ

1. 次の順に進みます。**Configuration → System → User Management → User Management**
2. 管理者ユーザーを選択します。
3. **Account Security Settings** をクリックします。
4. **Modify** をクリックします。

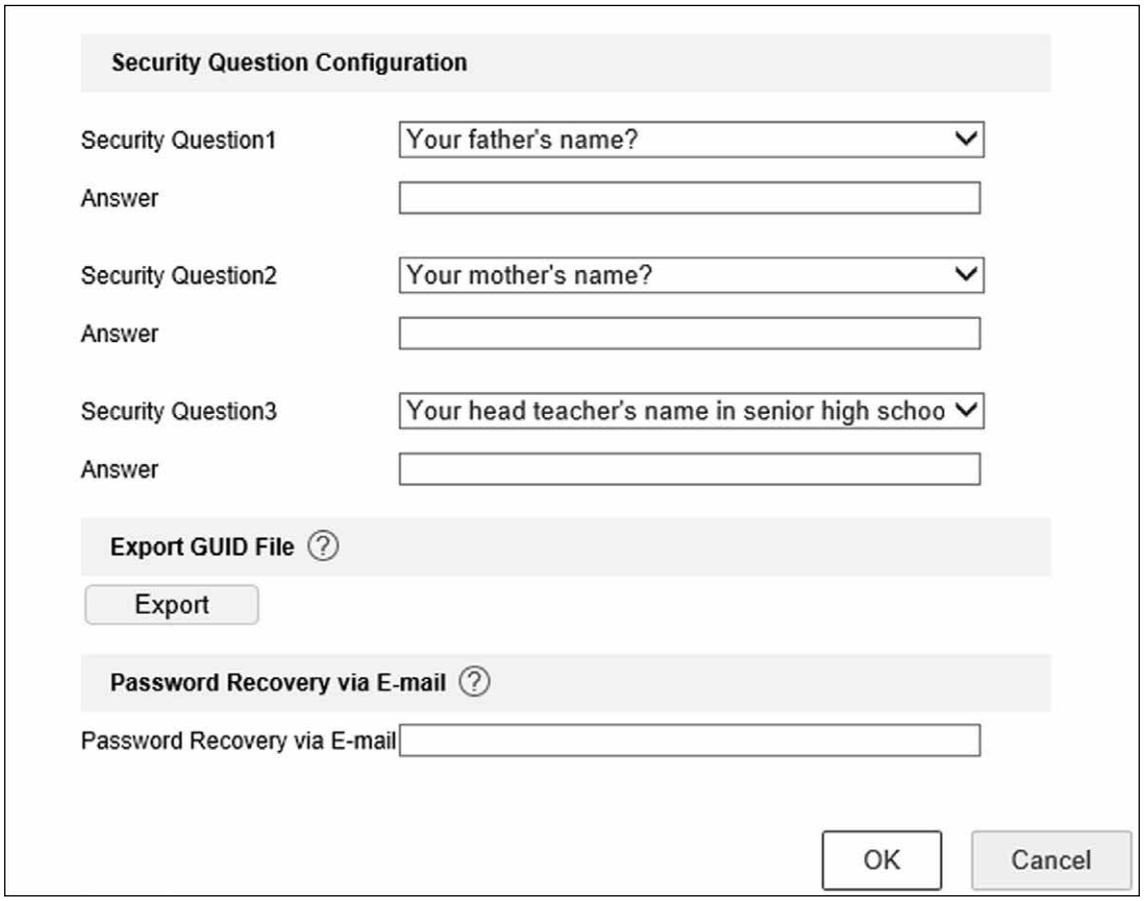


図 11-6 セキュリティに関する質問の設定

5. セキュリティに関する質問を設定します。
6. **OK** ボタンをクリックします。
7. 管理者パスワードを入力します。
8. **OK** ボタンをクリックします。

11.3.3 予約メールの設定

予約メールは、パスワードを忘れたときにパスワードをリセットするのに役立ちます。

ステップ

1. 本機を起動する場合は **Reserved E-mail** にチェック入れ、管理者ユーザーアカウントを編集する場合は **Modify** をクリックします。
2. 予約メールのアドレスを入力します。

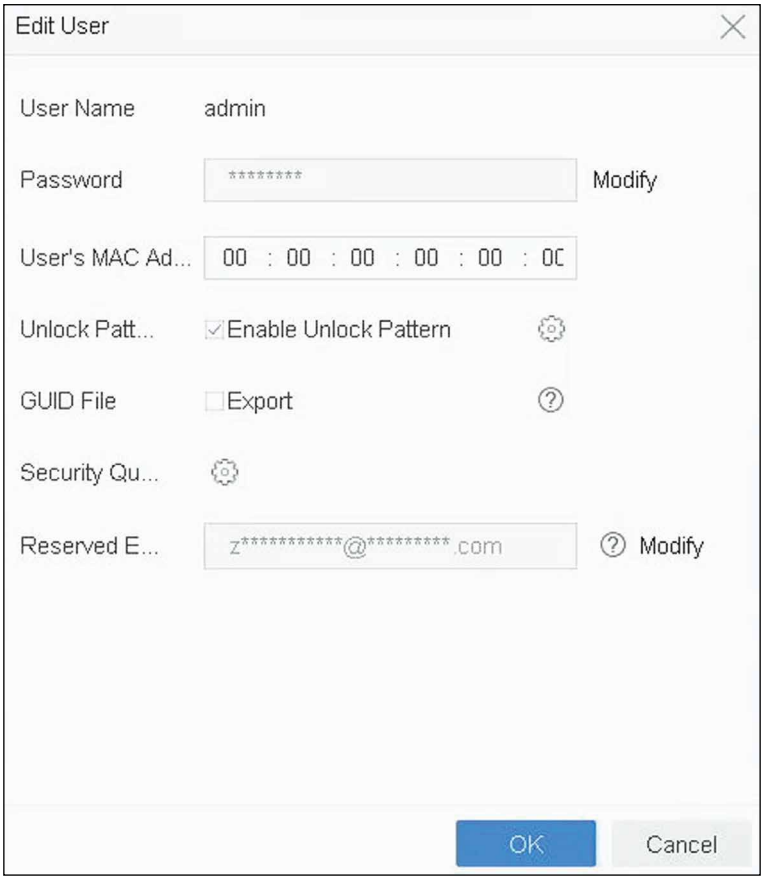


図 11-7 予約メールの設定

3. **OK** ボタンをクリックします。

11.4 パスワードのリセット

管理者パスワードを忘れた場合、GUID ファイルのインポート、セキュリティに関する質問への回答、予約メールからの認証コードの入力により、パスワードをリセットすることができます。

11.4.1 GUID でパスワードをリセットする

GUID によるパスワードのリセットは、Web ブラウザーから行えます。

ご使用の前に

正しい GUID ファイルがあることを確認してください。

ステップ

1. ユーザーログインのインターフェイスで **Forgot password** をクリックします。
2. **Verification Mode** は **GUID File Verification** を選択します。
3. **Browse** をクリックして、GUID ファイルを探します。
4. **Next** をクリックします。
5. 新しいパスワードを入力します。

メモ

製品の安全性を高めるため、お客様ご自身で強力なパスワード（8 文字以上、大文字、小文字、数字、特殊文字の 3 種類以上）を設定することを強くお勧めします。また、定期的にパスワードを変更することをお勧めします。特にセキュリティの高いシステムでは、毎月または毎週パスワードを変更することで、製品をより安全に保護することができます。

6. 新しいパスワードを確認してください。
7. **Next** をクリックします。

11.4.2 セキュリティ質問でパスワードをリセットする

Web ブラウザーからセキュリティ質問に答えてパスワードをリセットできます。

ご使用の前に

本機を起動する場合、または管理者ユーザーアカウントを編集する場合は、セキュリティに関するの質問を設定していることを確認してください。

ステップ

1. ユーザーログインのインターフェイスで **Forgot password** をクリックします。
2. **Verification Mode** は **Security Question Verification** を選択します。
3. 各設問の答えを入力してください。
4. **Next** をクリックします。
5. 新しいパスワードを入力します。

メモ

製品の安全性を高めるため、お客様ご自身で強力なパスワード（8 文字以上、大文字、小文字、数字、特殊文字の 3 種類以上）を設定することを強くお勧めします。また、定期的にパスワードを変更することをお勧めします。特にセキュリティの高いシステムでは、毎月または毎週パスワードを変更することで、製品をより安全に保護することができます。

6. **Next** をクリックします。

11.4.3 Hik-Connect でパスワードをリセットする

ご使用の前に

本機が Hik-Connect を有効にし、登録された Hik-Connect アカウントと紐付いていることを確認してください。

ステップ

1. ユーザーログインのインターフェイスで **Forgot Password** をクリックします。
2. パスワードリセットタイプのインターフェースで **Verify by Hik-Connect** を選択します。
3. 本機に紐付いているアカウントで Hik-Connect アプリにログインしてください。
4. Hik-Connect を使って QR コードを読み取ってください。その後、Hik-Connect から認証コードが届きます。
5. 認証コードを入力してください。
6. **OK** ボタンをクリックします。

11.4.4 予約メールでパスワードをリセットする

ご使用の前に

本機の起動または管理者ユーザーアカウントの編集を行う際に、予約メールを設定したことを確認してください。詳しくは**予約メールの設定**を参照してください。

ステップ

1. ユーザーログインのインターフェイスで **Forgot Password** をクリックします。
2. パスワードリセットタイプのインターフェースで **Verify by Reserved Email** を選択してください。
3. **OK** ボタンをクリックします。
4. 法的免責事項に同意される場合は **Next** をクリックしてください。スマートフォンで QR コードを読み取り、法的免責事項をお読みください。
5. 認証コードを取得してください。認証コードを取得する方法は 2 つあります。
   – Hik-Connect アプリで QR コードを読み取ってください。
   – QR コードをメールサーバーに送信してください。
      1. USB フラッシュメモリーを本機に挿入してください。
      2. **Export** をクリックすると、QR コードを USB メモリにエキスポートできます。
      3. ***Pw_recovery@hikvision.com*** に、QR コードを添付してメールで送信してください。
6. 予約メールにチェックを入れると、5 分以内に認証コードが届きます。
7. 認証コードを入力してください。
8. **OK** ボタン をクリックして、新しいパスワードを設定します。

第 12 章 システム管理

12.1 デバイスの設定

ステップ

1. 次の順に進みます。**System → General**
2. 以下の設定を行ってください。

Language

デフォルトで使用される言語は英語です。

Output Standard

出力規格を NTSC または PAL に設定し、ビデオ入力規格と同じにしてください。

Resolution

ビデオ出力の解像度を設定します。

Device Name

デバイス名を編集します。

Device No.

デバイスのシリアル番号を編集します。Device No. は 1 ～ 255 の範囲で設定可能で、デフォルトは 255 です。この番号は、リモコンやキーボードの操作に使用されます。

Auto Logout

メニューの非アクティブ時のタイムアウト時間を設定してください。例：タイムアウト時間を 5 分に設定した場合、メニューが 5 分間操作されないと、現在のオペレーションメニューからライブビュー画面に移行します。

Mouse Pointer Speed

マウスポインターの速度を設定します。4 段階の設定が可能です。

Enable Wizard

デバイス起動時のウィザードの有効 / 無効を設定します。

Enable Password

ログインパスワードの使用を有効 / 無効にします。

3. **Apply** をクリックして、設定を保存します。

12.2 時間の設定

12.2.1 手動時刻同期

ステップ

1. 次の順に進みます。**System → General**
2. 日付と時刻を設定します。
3. **Apply** をクリックして、設定を保存します。

12.2.2 NTP を同期する

NTP（Network Time Protocol）サーバーへの接続は、システムの日付と時刻の正確性を確保するために、デバイス上で設定することができます。

ステップ

1. 次の順に進みます。**System → Network → TCP/IP → NTP**
2. **Enable** にチェックを入れます。
3. 必要に応じて、NTP の設定を行ってください。

   Interval (min)

   NTP サーバーとの時刻同期を 2 回行う場合の時間間隔です。

   NTP Server

   NTP サーバーの IP アドレスです。

   NTP Port

   NTP サーバーのポートです。
4. **Apply** をクリックします。

12.2.3 DST を同期する

DST（夏時間）とは、1 年のうちで時計を 1 時間進める期間のことです。このため世界には、最も気温の高い月の夕方に日照時間が増える地域があります。
夏時間が始まると時計を一定期間（設定した夏時間バイアスによって異なる）進め、標準時に戻る時同じ期間だけ時間を戻します。

ステップ

1. 次の順に進みます。**System → General**
2. **Enable DST** にチェックを入れます。
3. **DST mode** は **Auto** または **Manual** を設定します。

Auto

ローカル DST ルールに従って、デフォルトの DST 期間を自動的に有効にします。

Manual

夏時間の期間の開始時刻と終了時刻、および夏時間バイアスを手動で設定します。

4. DST バイアスを設定します。標準時からオフセット時間（30/60/90/120 分）を設定します。
5. **Apply** をクリックして、設定を保存します。

12.3 ネットワークの検知

12.3.1 ネットワークトラフィックをモニタリングする

ネットワークトラフィックモニタリングとは、ネットワークのパフォーマンス、可用性、セキュリティに影響を与えるような異常やプロセスがないかどうかを確認、分析し、管理するプロセスです。

ステップ

1. 次の順に進みます。**Maintenance → Network → Traffic**
2. MTU（最大伝送単位）、ネットワークスループットなど、ネットワークのトラフィック状況をリアルタイムで確認することができます。

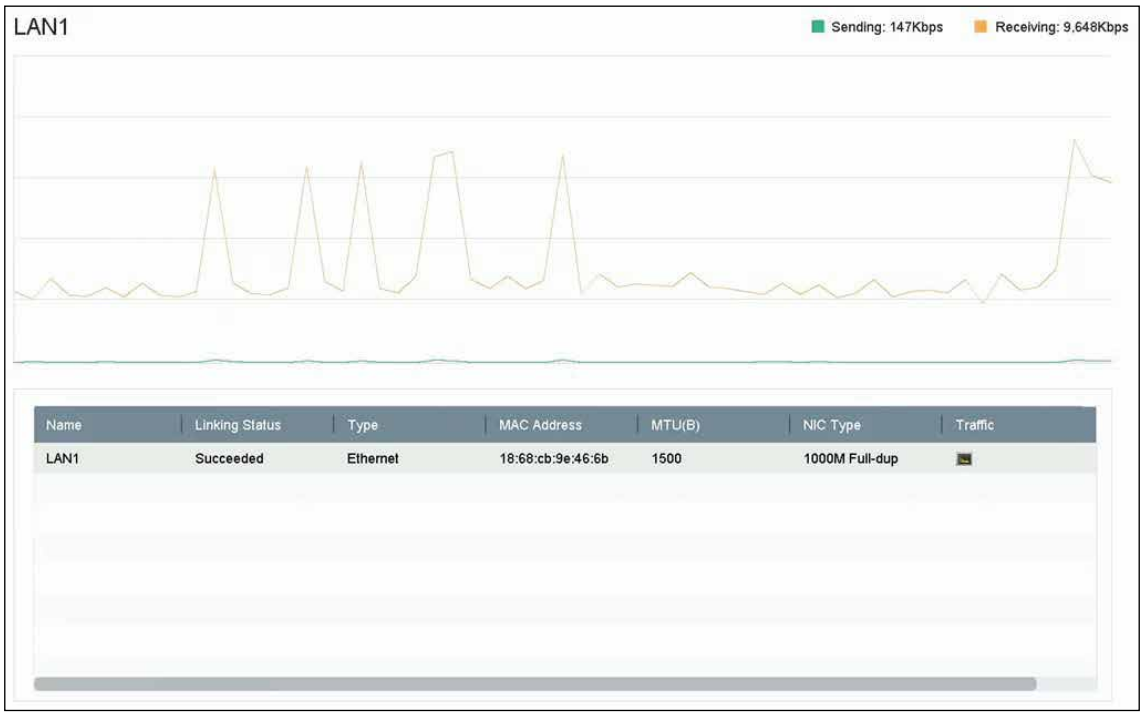


図 12-1 ネットワークトラフィック

12.3.2 ネットワーク遅延とパケットロスをテストする

ネットワーク遅延は、TCP/IP などのネットワークプロトコルで、送信時にデータ情報の大きさが制限されない場合に、機器の応答が遅くなることで発生します。パケットロステストは、ネットワークのパケットロス率（送信されたデータパケットの総数に対して失われたデータパケットの割合）をテストするためのものです。

ステップ

1. 次の順に進み、**Maintenance → Network → Detection**
2. **Select NIC** でネットワークカードを選択します。
3. **Destination Address** に送信先 IP アドレスを入力します。
4. **Test** をクリックします。

図 12-2 ネットワーク遅延とパケットロスをテストする

12.3.3 ネットワークパケットをエクスポートする

本機がネットワークにアクセスした後、USB メモリーを使用してネットワークのパケットをエクスポートすることができます。

ご使用の前に

ネットワークパケットをエキスポートするための USB メモリーを用意します。

ステップ

1. USB フラッシュメモリーを挿入します。
2. 次の順に進み、**Maintenance → Network → Detection**
3. **Select NIC** でネットワークカードを選択します。
4. **Device Name** で USB フラッシュメモリーを選択します。接続されているローカルバックアップデバイスが表示されない場合は、**Refresh** をクリックします。

図 12-3 ネットワークパケットのエクスポート

5. オプション：**Status** をクリックすると、ネットワークのステータスが表示されます。
6. **Export** をクリックします。

メモ

デフォルトでは、1 回につき 1MB のデータをエクスポートします。

12.3.4 ネットワークリソースの統計情報

Web ブラウザーやクライアントソフトウェアを含むリモートアクセスは、出力帯域を消費します。リアルタイムで帯域の統計情報を見ることができます。

ステップ

1. 次の順に進みます。**Maintenance → Network → Stat**

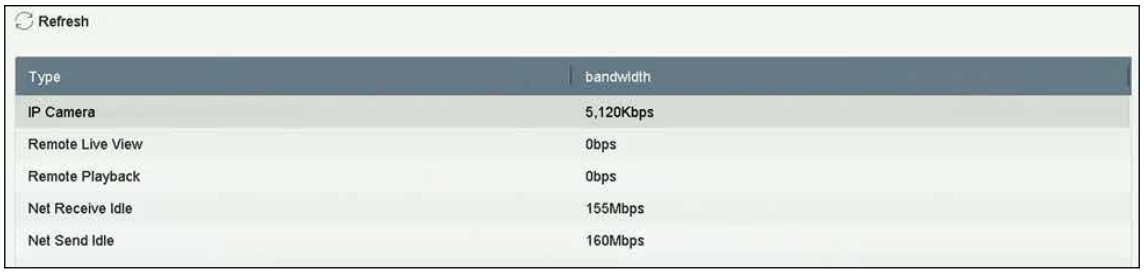


図 12-4 ネットワークリソースの統計情報

2. 次のような帯域の統計情報を表示します。**IP Camera**、**Remote Live View**、**Remote Play**、**Net Total Idle** など。
3. オプション：**Refresh** をクリックすると、最新データを取得できます。

12.4 ストレージデバイスのメンテナンス

12.4.1 不良セクターを検知する

ステップ

1. 次の順に進みます。**Maintenance → HDD Operation → Bad Sector Detection**
2. ドロップダウンリストで、設定したい HDD 番号を選択します。
3. 検知タイプとして **All Detection** または **Key Area Detection** を選択します。
4. **Self-Test** をクリックすると検知を開始します。

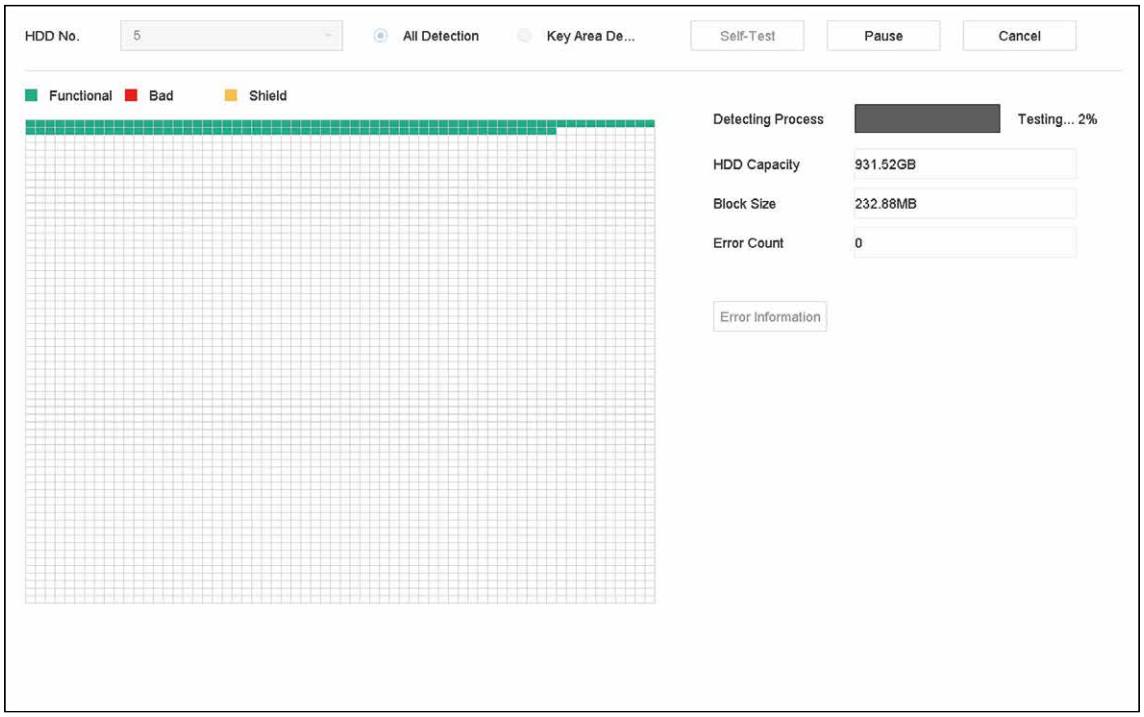


図 12-5 不良セクター検知

メモ

- 検知の一時停止 / 再開、キャンセルができます。
- テストが完了したら Error information をクリックして、詳しいダメージ情報を見ることができます。

12.4.2 S.M.A.R.T. 検知

S.M.A.R.T. および Bad Sector Detection 技術の採用などの HDD 検知機能です。S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology）は故障の予知を行い、さまざまな信頼性指標を検知する HDD 監視システムです。

ステップ

1. 次の順に進みます。**Maintenance → HDD Operation → S.M.A.R.T.**
2. HDD を選択すると、その S.M.A.R.T. 情報リストが表示されます。
3. **Self-Test Type** を設定します。
4. **Self-Test** をクリックして S.M.A.R.T.HDD の自己評価を開始します。

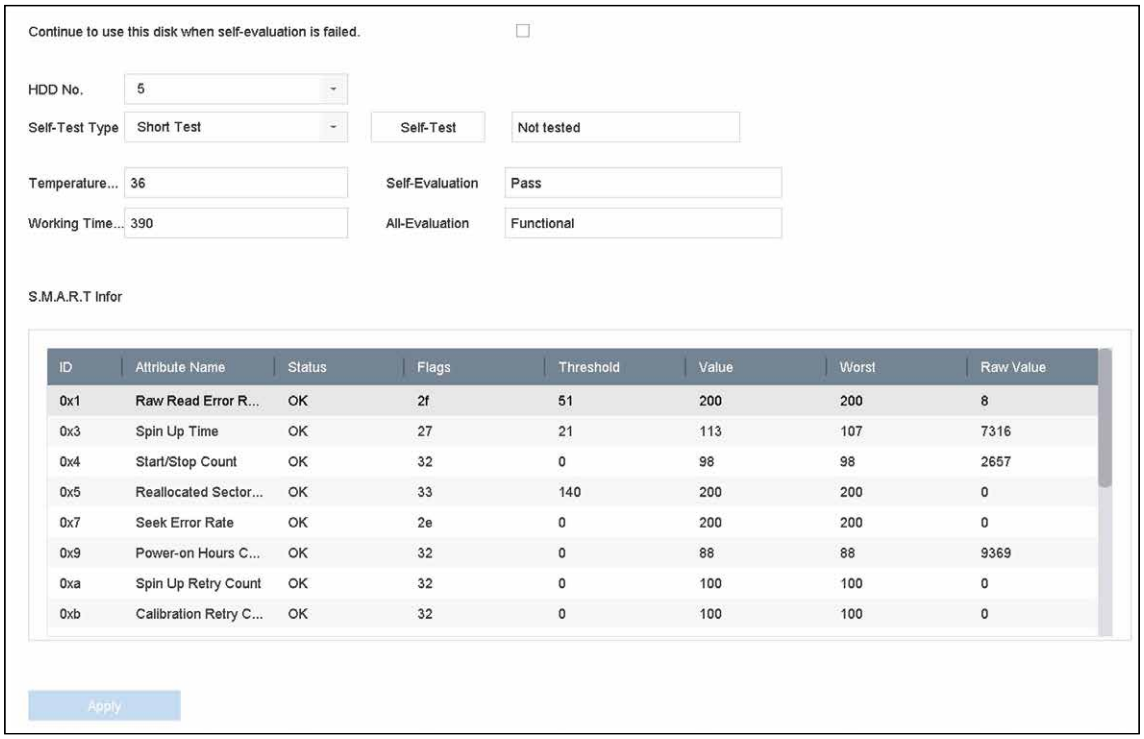


図 12-6 S.M.A.R.T. 設定インターフェイス

メモ

S.M.A.R.T. チェックに失敗しても、HDD を使用するには **Continue to use the disk when self-evaluation is failed.** にチェックを入れてください。

S.M.A.R.T. の関連情報が表示され、HDD のステータスを確認することができます。

12.4.3 HDD のヘルスステータス検知

2017 年 10 月 1 日以降に製造された 4TB ～ 8TB の Seagate 製 HDD のヘルスステータスを確認することができます。この機能は、HDD のトラブルシューティングに役立ちます。ヘルス検知は、S.M.A.R.T. 機能よりも詳細な HDD のステータスを表示する機能です。

ステップ

1. 次の順に進みます。**Maintenance → HDD Operation → Health Detection**

図 12-7 ヘルスステータス検知

2. HDD をクリックすると、詳細が表示されます。

12.4.4 ディスククローンを設定する

eSATA HDD にクローンする HDD を選択します。

ご使用の前に

本機に eSATA ディスクを接続します。

ステップ

1. 次の順に進みます。**Maintenance → HDD Operation → HDD Clone**

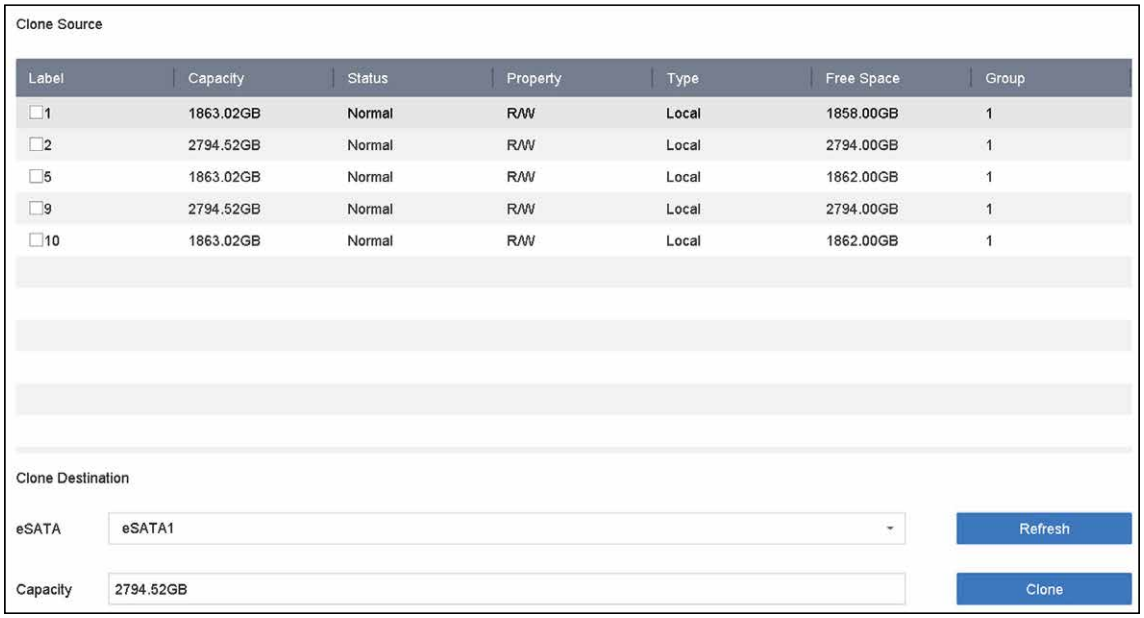


図 12-8 HDD クローン

2. クローンを作成する HDD にチェックを入れます。選択した HDD の容量がクローン先の容量と一致する必要があります。
3. **Clone** をクリックします。
4. ポップアップメッセージの **Yes** をクリックすると、クローンを作成することができます。

12.4.5 データベースを修復する

データベースの修復は、すべてのデータベースを再構築します。アップグレード後のシステム速度を改善するのに役立つ可能性があります。

ステップ

1. 次の順に進みます。**Storage → Storage Device**
2. ドライブを選択します。
3. **Repair Database** をクリックします。
4. **Yes** をクリック します。

メモ

- データベースの修復は、すべてのデータベースを再構築します。既存のデータに影響はありませんが、処理中はローカルの検索・再生機能が使えなくなります。Web ブラウザーやクライアントソフトなどを使って、リモートで検索・再生をすることができます。
- 途中でドライブを抜いたり、機器をシャットダウンしたりしないでください。

Status で修理の進捗状況を見ることができます。

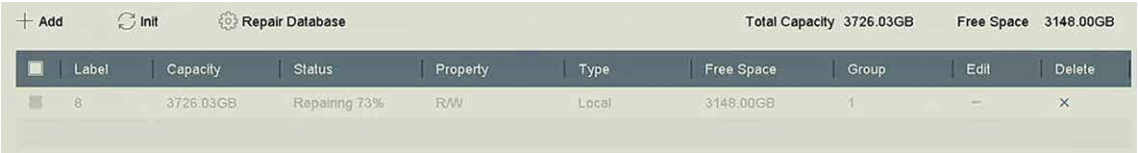


図 12-9 データベースの修復

12.5 本機のアップグレード

本機のファームウェアは、ローカルのバックアップデバイスまたはリモートの FTP サーバーを使用してアップグレードすることができます。

12.5.1 ローカルバックアップデバイスによるアップグレード

ご使用の前に

ファームウェアのアップデートファイルが保存されているローカルストレージに本機を接続します。

ステップ

1. 次の順に進みます。**Maintenance → Upgrade**
2. **Local Upgrade** をクリックして、ローカルアップグレードインターフェースに入ります。

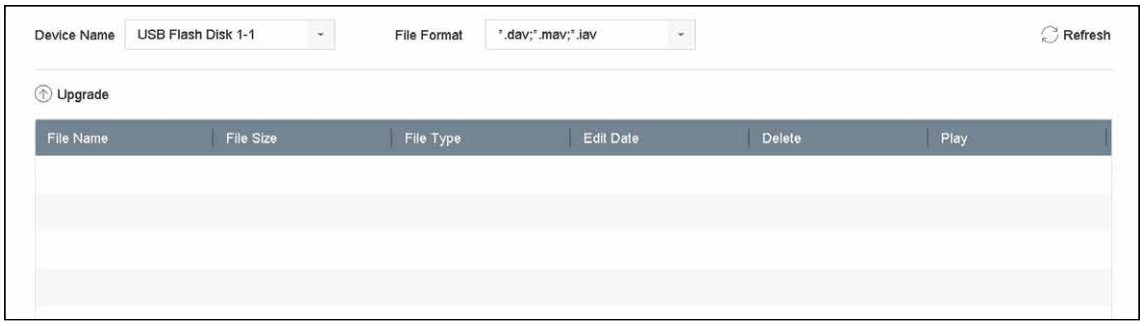


図 12-10 ローカルアップグレード

3. ストレージデバイスからファームウェアアップデートファイルを選択します。
4. **Upgrade** をクリックし、アップグレードを開始します。
   バージョンアップが完了すると自動的に本機が再起動し、新しいファームウェアが有効になります。

12.5.2 FTP によるアップグレード

ご使用の前に

PC（FTP サーバーを起動中）と本機のネットワーク接続が有効で適切あることを確認してください。PC で FTP サーバーを起動し、ファームウェアを PC の対応するディレクトリにコピーしてください。

ステップ

1. 次の順に進みます。**Maintenance → Upgrade**
2. **FTP** をクリックして、ローカルアップグレードインターフェースに入ります。

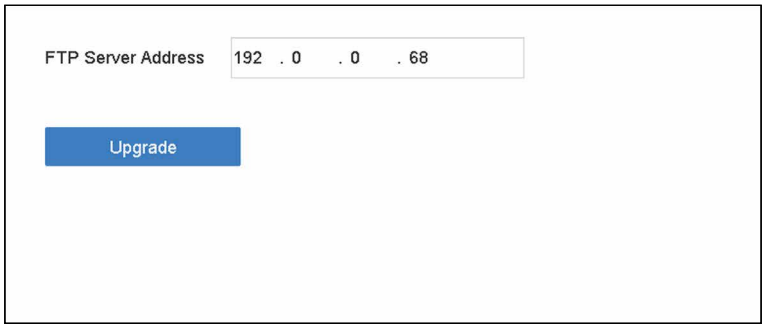


図 12-11 FTP アップグレード

3. **FTP Server Address** を 入力します。
4. **Upgrade** をクリックし、アップグレードを開始します。
5. アップグレードが完了したら、本機を再起動して新しいファームウェアを有効にしてください。

12.5.3 Web ブラウザーによるアップグレード

Web ブラウザーで本機のアップグレードが可能です。
Web ブラウザーで端末にログイン後、次の順に進みます。**Configuration → System → Maintenance → UpgradeBrowse** をクリックしてファームウェアをアップロードし、本機をアップグレードします。

12.5.4 Hik-Connect によるアップグレード

本機は Hik-Connect にログインした後、定期的に Hik-Connect からの最新ファームウェアを確認します。バージョンアップ用ファームウェアがある場合は、ログイン時に本機に通知されます。また、手動で最新のファームウェアを確認することもできます。

ご使用の前に

本機が Hik-Connect に正常に接続されていることを確認し、ファームウェアのダウンロードのために最低 1 台の読み書き可能な HDD を接続する必要があります。

ステップ

1. 次の順に進みます。**Maintenance → Upgrade → Online Upgrade**
2. **Check Upgrade** をクリックして手動で確認し、Hik-Connect から最新のファームウェアをダウンロードしてください。

   メモ

   本機は 24 時間ごとに最新のファームウェアを自動的に確認します。アップグレード可能なファームウェアを検出した場合、ログイン時に通知されます。

3. オプション：**Download Latest Package Automatically** をオンにすると、最新のファームウェアパッケージが自動的にダウンロードできます。
4. **Upgrade Now** をクリックします。

12.6 機器設定ファイルのインポート / エクスポート

機器設定ファイルをローカル機器にエクスポートしてバックアップしたり、1 つの機器の設定ファイルを複数の機器にインポートして同じパラメータで設定したりすることができます。

ご使用の前に

本機にストレージデバイスを接続してください。設定ファイルをインポートするには、ストレージデバイスにそのファイルが入っている必要があります。

ステップ

1. 次の順に進みます。**Maintenance → Import/Export**

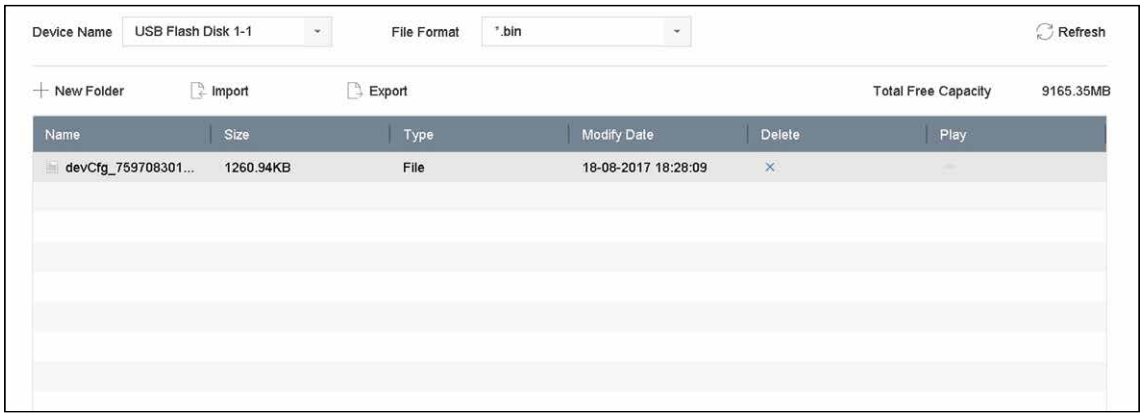


図 12-12 インポート / エクスポート設定ファイル

2. 機器設定ファイルをエクスポートまたはインポートします。
   – **Export** をクリックすると、選択したローカルバックアップデバイスに設定ファイルをエクスポートします。
   – 設定ファイルをインポートするには、選択したバックアップデバイスからファイルを選択し **Import** をクリックします。

メモ

設定ファイルのインポートが終了すると、本機が自動的に再起動します。

12.7 ログの管理

メモ

このセクションの機能は、特定のモデルでのみ使用できます。

12.7.1 ログを保存する

ログ保存ディスクとログ保存期間をカスタマイズすることができます。

ステップ

1. 次の順に進みます。**Storage → Advanced**

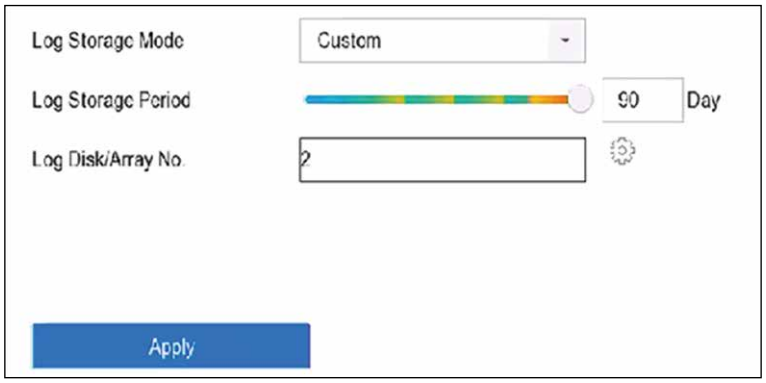


図 12-13 ログの保存

2. **Log Storage Mode** を設定します。
   System Default 各ディスクには、6 ヶ月間のログを保存するための一定の容量が割り当てられます。6 ヶ月を過ぎると、古いログは上書きされます。
   Custom **Log Storage Period** を設定して、ログ保存用の Log Disk を割り当てます。ログディスクが満杯になると、期間を超えたログは上書きされます。
3. **Apply** をクリックします。

12.7.2 ログファイルの検索とエキスポート

機器の動作、アラーム、異常、情報をログファイルとして保存し、いつでも閲覧、出力することができます。

ステップ

1. 次の順に進みます。**Maintenance → Log Info**

図 12-14 ログ検索インターフェース

2. 時刻、メジャータイプ、マイナータイプなどのログ検索条件を設定します。
3. **Search** をクリックすると、ログファイルの検索を開始します。
4. 以下のように、一致したログファイルが一覧で表示されます。

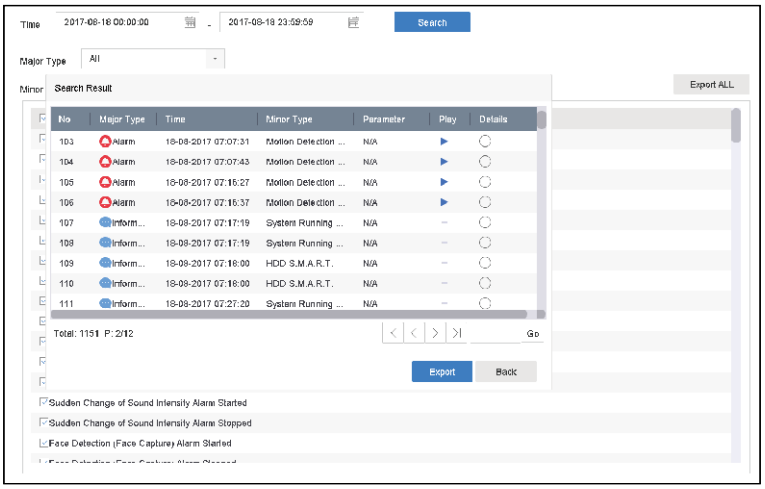


図 12-15 ログ検索結果

メモ

1 回に表示できるログファイルの数は最大 2,000 件です。

5. 関連する操作：

	クリックまたはダブルクリックすると、詳細情報が表示されます。
	クリックすると、関連する動画ファイルが表示されます。
Export/Export ALL	クリックすると、すべてのシステムログがストレージデバイスにエクスポートされます。

12.7.3 サーバーへログをアップロードする

システムログをサーバーにアップロードし、バックアップすることができます。

ステップ

1. 次の順に進みます。**System → Network → Advanced → Log Server Settings**

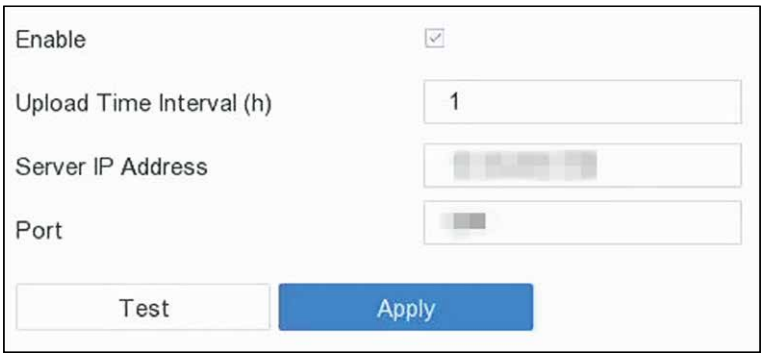


図 12-16 ログサーバーの設定

2. **Enable** にチェックを入れます。
3. **Upload Time**、**Server IP Address**、**Port** を設定します
4. オプション：**Test** をクリックして、パラメータが有効であるかどうかをテストします。
5. **Apply** をクリックします。

12.7.4 一方向認証

CA 証明書（サーバーのもの）を本機にインストールし、Web ブラウザーでサーバーを認証することができます。ログ通信の安全性を向上させることができます。

ご使用の前に

- サーバーから CA 証明書をダウンロードします。
- ログサーバーのパラメータが有効であることを確認してください。

ステップ

1. 次の順に進みます。**Configuration → Network → Advanced Settings → Log Server Configuration**

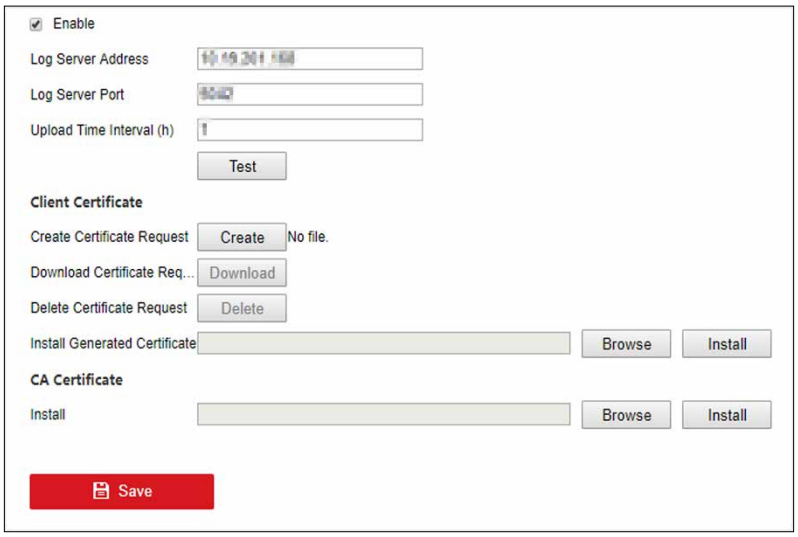


図 12-17 一方向認証

2. **CA Certificate** に CA 証明書をインストールします。
3. オプション：**Test** をクリックして、接続が有効であるかどうかをテストします。
4. **Save** をクリックします。

12.7.5 双方向認証

CA 証明書（サーバー側）を本機にインストールしてサーバーを認証したり、証明書（本機側）を作成してサーバーから本機を認証したりすることができます。これにより、ログ通信の安全性を向上させることができます。Web ブラウザーで双方向認証の設定が可能です。

ご使用の前に

- サーバーから CA 証明書をダウンロードします。
- ログサーバーのパラメータが有効であることを確認してください。

ステップ

1. 次の順に進みます。**Configuration → Network → Advanced Settings → Log Server Configuration**

図 12-18 双方向認証

2. **CA Certificate** に CA 証明書をインストールします。
3. **Client Certificate** の **Create** をクリックし、ポップアップに従って証明書を作成します。
4. **Download** をクリックして、証明書ファイルを任意の場所にダウンロードします。
5. ダウンロードした証明書ファイルをサーバーにアップロードすると、サーバーから証明書キーが返送されます。
6. 証明書をテキストファイルで開き、サーバーが返した証明書キーで修正します。
7. **Client Certificate** に変更した証明書をインストールします。
8. オプション：**Test** をクリックして、接続が有効であるかどうかをテストします。
9. **Save** をクリックします。

12.8 初期設定への復元

ステップ

1. 次の順に進みます。**Maintenance → Default**

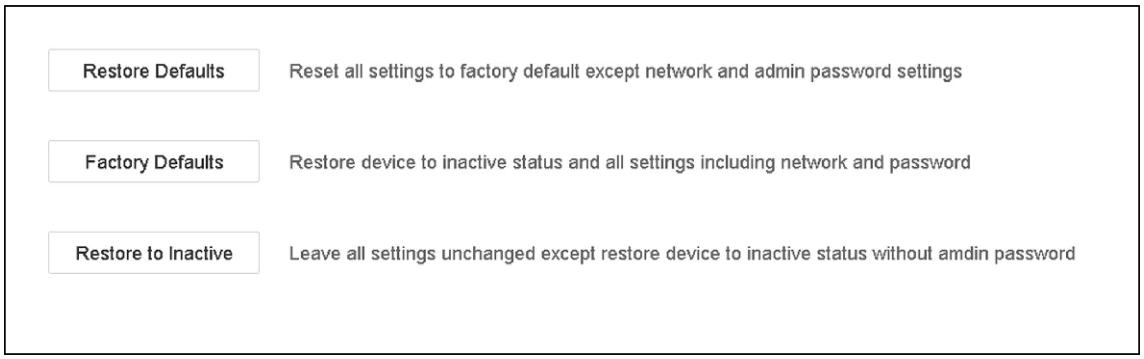


図 12-19 初期設定への復元

2. 復元の種類を次の 3 つから選択します。

Restore Defaults

ネットワーク（IP アドレス、サブネットマスク、ゲートウェイ、MTU、NIC ワーキングモード、デフォルトルート、サーバーポートなど）とユーザーアカウントのパラメータを除くすべてのパラメータを、工場出荷時の設定に戻すことができます。

Factory Defaults

すべてのパラメータを工場出荷時の設定に戻します。

Restore to Inactive

本機を非アクティブステータスに戻します。

メモ

初期設定に戻した後、本機は自動的に再起動します。

12.9 セキュリティ管理

メモ

このセクションの機能は、特定のモデルでのみ使用できます。

12.9.1 ONVIF を設定する

ONVIF プロトコルにより、他社製カメラとの接続が可能です。追加されたユーザーアカウントは、ONVIF プロトコル経由で他の機器を接続する権限を持ちます。

ステップ

1. 次の順に進みます。**Maintenance → System Service → ONVIF**
2. **Enable ONVIF** にチェックを入れて、ONVIF アクセス管理を有効にします。

メモ

ONVIF プロトコルはデフォルトでは無効になっています。

3. **Add** をクリックします。
4. **User Name** と **Password** を入力します。

メモ

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

5. **Level** は **Media User**、**Operator** または **Admin** を選択します。
6. **OK** ボタンをクリックします。

12.9.2 IP/MAC アドレスフィルター

アドレスフィルターは、特定の IP/MAC アドレスが本機にアクセスすることを許可または禁止するかどうかを決定します。

ステップ

1. 次の順に進みます。**Maintenance → System Service → Address Filter**

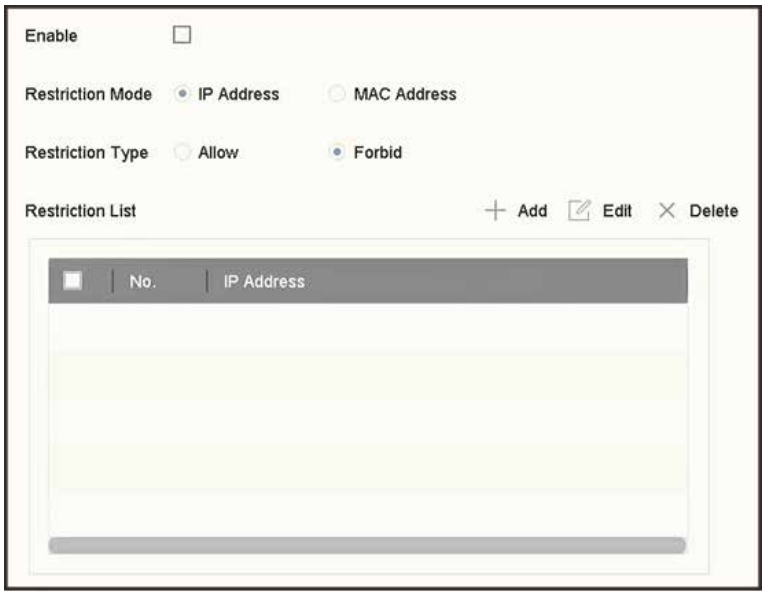


図 12-20 アドレスフィルター

2. **Enable** にチェックを入れます。
3. **Restriction Mode** を選択します。IP アドレスまたは MAC アドレスでフィルタを選択します。
4. **Restriction Type** を選択します。本機が特定の IP/MAC アドレスからのアクセスを許可または禁止するかどうかを決定します。
5. オプション：**Restriction List** を設定します。アドレスの追加、編集、削除ができます。
6. **Apply** をクリックして、設定を保存します。

12.9.3 RTSP 認証

RTSP 認証を設定することで、ライブビューのストリームデータのセキュリティを精密に確保することができます。

ステップ

1. 次の順に進みます。**Maintenance → System Service → System Service**

図 12-21 RTSP 認証

2. **RTSP Authentication Type** を選択します。

メモ

digest を選択した場合、2 種類の認証が選択可能です。 この場合ダイジェスト認証されたリクエストのみが、IP アドレス経由で RTSP プロトコルによりビデオストリームにアクセスすることができます。セキュリティ上、認証タイプとして **digest** を選択することを推奨します。

3. **Apply** をクリックします。
4. 設定を反映させるには、本機を再起動してください。

12.9.4 RTSP ダイジェストアルゴリズム

RTSP ダイジェストアルゴリズムは、RTSP プロトコルに基づき、ユーザー認証のダイジェスト認証を行うアルゴリズムです。Web ブラウザーから RTSP ダイジェストアルゴリズムを設定することができます。
Web ブラウザーで次の順に進み、必要な RTSP ダイジェストアルゴリズムの種類を選択します。
Configuration → System → Security → Authentication

12.9.5 ISAPI サービス

ISAPI (Internet Server Application Programming Interface) は HTTP をベースとしたオープンプロトコルで、システム機器（ネットワーク・カメラ、NVR など）間の通信を可能にすることができます。本機はサーバーとして機能し、このシステムは本機を検索して接続します。

ステップ

1. 次の順に進みます。**Maintenance → System Service → System Service**
2. **Enable ISAPI** にチェックを入れます。
3. **Apply** をクリックします。
4. 設定を反映させるには、本機を再起動してください。

12.9.6 HTTP 認証

HTTP サービスを有効にする必要がある場合は、HTTP 認証を設定することで、アクセスのセキュリティを強化することができます。

ステップ

1. 次の順に進みます。**Maintenance → System Service → System Service**

図 12-22 HTTP 認証

2. **Enable HTTP** にチェックを入れます。
3. **HTTP Authentication Type** を選択します。

メモ

2 種類の認証が選択可能ですがセキュリティ上、認証の種類として digest を選択することをお勧めします。

4. **Apply** をクリックして、設定を保存します。
5. 設定を反映させるには、本機を再起動してください。

12.9.7 HTTP/ ウェブダイジェストアルゴリズム

HTTP/ ウェブダイジェストアルゴリズムは、HTTP プロトコルに基づき、ユーザー認証のダイジェスト認証を行うアルゴリズムです。HTTP/ ウェブダイジェストのアルゴリズムは、Web ブラウザーから設定することができます。

Web ブラウザーで次の順に進み、必要なダイジェストアルゴリズムの種類を選択します。**Configuration → System → Security → Authentication**

12.9.8 画像 URL ダイジェスト認証

SDK がアップロードした画像を HTTP プロトコルでダウンロードする際、画像の URL のダイジェスト認証を必要とするかどうかを制御します。Web ブラウザーで画像 URL ダイジェスト認証を設定することができます。

Web ブラウザーで次の順に進み、画像 URL ダイジェスト認証の有効・無効を設定することができます。**Configuration → System → Security → Security Service**

12.9.9 SADP サービスの無効化

信頼されないネットワーク環境にいる場合など、アクセスセキュリティを強化するために SADP サービスを無効にすることができます。

次の順**System → System Service → System Service** に進んで、**Enable SADP** のチェックを外し、このサービスを無効にします。

第 13 章 付録

13.1 適用可能な電源アダプターのリスト

電源アダプターは、下記のものだけをご使用ください。

電源アダプターモデル	仕様	メーカー
ADS-26FSG-12 12024EPG	12 V、2 A	Shenzhen Honor Electronic Co., Ltd.
MSA-Z3330IC12.0-48W-Q	12 V、3.33 A	Moso Power Supply Technology Co., Ltd.
MSA-C1500IC12.0-18P-DE	12 V、1.5 A	0000201935 MOSO Technology Co., Ltd.
ADS-25FSG-12 12018GPG	CE、100 ～ 240 VAC、12 V、1.5 A、18 W、Φ 5.5 × 2.1 × 10	0000200174 Shenzhen Honor Electronic Co., Ltd.
MSA-C1500IC12.0-18P-US	12 V、1.5 A	0000201935 MOSO Technology Co., Ltd.
TS-A018-120015AD	100～240 VAC、12 V、1.5 A、18 W、Φ 5.5 × 2.1 × 10	0000200878 Shenzhen Transin Technologies Co., Ltd.
MSA-C2000IC12.0-24P-DE	12 V、2 A	0000201935 MOSO Technology Co., Ltd.
ADS-24S-12 1224GPG	CE、100 ～ 240 VAC、12 V、2 A、24 W、Φ 2.1	0000200174 Shenzhen Honor Electronic Co., Ltd.
MSA-C2000IC12.0-24P-US	US、12 V、2 A	0000201935 MOSO Technology Co., Ltd.
ADS-26FSG-12 12024EPCU	US、12 V、2 A	0000200174 Shenzhen Honor Electronic Co., Ltd.
KPL-040F-VI	12 V、3.33 A、40 W	0000203078 Channel Well Technology Co., Ltd.
MSA-Z3330IC12.0-48W-Q	12 V、3.33 A	0000201935 MOSO Technology Co., Ltd.
MSP-Z1360IC48.0-65W	48 V、1.36 A	0000201935 MOSO Technology Co., Ltd.
KPL-050S-II	48 V、1.04 A	0000203078 Channel Well Technology Co., Ltd.

13.2 用語集

Dual-Stream

デュアルストリームとは、高解像度の画像をローカルに記録し、低解像度のストリームをネットワーク上に送信するために使用される技術です。2 つのストリームは DVR によって生成され、メインストリームは最大解像度 1080P、サブストリームは最大解像度 CIF となります。

DVR

デジタルビデオレコーダーの略称です。DVR は、アナログカメラからの映像信号を受信し、信号を圧縮してハードディスクに保存することができる装置です。

HDD

Hard Disk Drive の略称です。磁気面を有するプラッターにデジタル符号化されたデータを格納する記憶媒体です。

DHCP

DHCP（Dynamic Host Configuration Protocol）は、インターネットプロトコルネットワークで動作するための設定情報を取得する機器（DHCP クライアント）が使用するネットワークアプリケーションプロトコルです。

HTTP

Hypertext Transfer Protocol 略称です。ネットワーク上のサーバーとブラウザーの間で、ハイパーテキストのリクエストや情報を転送するためのプロトコルです。

PPPoE

PPPoE（Point-to-Point Protocol over Ethernet）は、PPP（Point-to-Point Protocol）フレームをイーサネットフレーム内にカプセル化するためのネットワークプロトコルです。主に、個々のユーザーがイーサネット上の ADSL トランシーバー（モデム）に接続する ADSL サービスや、プレーンメトロイーサネットネットワークで使用されます。

DDNS

ダイナミック DNS とは、ルーターやインターネットプロトコルスイートを使用するコンピュータシステムなどのネットワーク接続機器が、DNS に格納されているホスト名、アドレスなどの設定されたアクティブな DNS の設定をリアルタイム（アドホック）で変更するようドメインネームサーバーに通知する機能を提供する方法、プロトコル、ネットワークサービスです。

Hybrid DVR

ハイブリッド DVR は、DVR と NVR を組み合わせたものです。

NTP

Network Time Protocol 略称です。ネットワーク上のコンピュータのクロックを同期させるために設計されたプロトコルです。

NTSC

National Television System Committee の略称です。NTSC は、アメリカや日本などで使用されているアナログテレビの規格です。NTSC 信号の各フレームには、60Hz で 525 本の走査線が含まれます。

NVR

ネットワークビデオレコーダーの略称です。NVR は、IP カメラ、IP ドーム、その他の DVR の集中管理およびストレージに使用される PC ベースまたは組み込みシステムです。

PAL

Phase Alternating Line の略称です。PAL もまた、世界の多くの地域で放送用テレビシステムに使用されているビデオ規格の一つです。PAL 信号は 50Hz で 625 本の走査線が含まれています。

PTZ

Pan、Tilt、Zoom の略称です。PTZ カメラはモーター駆動により、カメラを左右にパン、上下にチルト、ズームイン・ズームアウトすることができるシステムです。

USB

Universal Serial Bus の略称です。USB は、ホストコンピュータにデバイスを接続するためのプラグアンドプレイのシリアルバス規格です。

13.3 通信マトリクス

下記の QR コードを読み取ると、コミュニケーションマトリクス資料が表示されます。

図 13-1 通信マトリックス

13.4 デバイスコマンド

以下の QR コードを読み取ると、デバイスコマンドのドキュメントが表示されます。

図 13-2 デバイスコマンド

13.5 よくある質問

13.5.1 マルチ画面ライブビューで、一部のチャンネルが「No Resource」と表示されたり、画面が黒くなったりするのはなぜですか？

原因

1. サブストリームの解像度またはビットレート設定が不適切です。
2. サブストリームの接続に失敗しました。

解決方法

1. 次の順に進みます。**Camera → Video Parameters → Sub-Stream**。チャンネルを選択し、解像度と最大ビットレートを下げます（解像度は 720p 以下、最大ビットレートは 2048Kbps 以下）。

   メモ

   本機がこの機能をサポートしていない場合、カメラにログインし、Web ブラウザーでビデオパラメータを調整することができます。

2. サブストリームの解像度と最大ビットレート（解像度は 720p 以下、最大ビットレートは 2048Kbps 以下）を適切に設定し、チャンネルを削除して再度追加してください。

13.5.2 ネットワークカメラを追加した後、ビデオレコーダーが危険なパスワードを通知するのはなぜですか？

原因

カメラのパスワードが弱すぎます。

解決方法

カメラのパスワードを変更してください。

警告

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

13.5.3 ビデオレコーダーがストリームの種類をサポートしていないと通知するのはなぜですか？

原因

カメラのエンコード形式がビデオレコーダーと一致していません。

解決方法

カメラが H.265/MJPEG でエンコードしているが、ビデオレコーダーが H.265/MJPEG に対応していない場合、カメラのエンコード形式をビデオレコーダーと同じ形式に変更します。

13.5.4 再生画質を向上させる方法は？

原因

録画パラメーター設定が不適切です。

解決方法

次の順に進みます。**Camera → Video Parameters**。解像度と最大ビットレートを上げて、もう一度試してみてください。

13.5.5 アナログチャンネルのライブビューに「NO VIDEO」が表示されるのはなぜですか？

原因

1. ビデオ入力コネクターが緩んでいるため、ビデオ信号が弱くなっています。
2. ビデオ入力 / 出力規格の不一致です。
3. 送信距離が長すぎます。
4. ケーブルの損傷により、ビデオ信号が弱くなっています。
5. ビデオレコーダーのビデオ入力コネクターが壊れています。

解決方法

1. コネクターがしっかりと接続されていることを確認してください。
2. 次の順に進みます。**System → General** 出力規格が正しいことを確認してください。
3. アナログカメラとビデオレコーダーの距離が制限値を超えていないことを確認してください。
4. ケーブルが損傷していないことを確認してください。
5. 他の BNC コネクタが正常に動作している場合は、他の BNC コネクタをお試しください。

13.5.6 ビデオレコーダーが H.265 で画像を録画していることを確認する方法は？

解決方法

ライブビューツールバーのエンコードタイプが H.265 になっているか確認してください。

13.5.7 再生時のタイムラインが一定でないのはなぜですか？

原因

1. 本機がイベント録画を使用している場合、イベントが発生したときのみ動画を録画します。そのため、動画が連続しないことがあります。
2. デバイスオフライン、HDD エラー、録画異常、ネットワークカメラオフラインなどの異常の発生です。

解決方法

1. 録画タイプが連続録画であることを確認してください。
2. 次の順に進み、**Maintenance → Log Information**、ビデオ時間帯のログファイルを検索します。HDD エラー、録画異常など、予期せぬ事象が発生していないか確認してください。

13.5.8 ネットワークカメラの追加時に、ビデオレコーダーがネットワークに到達できないことを通知するのはなぜですか？

原因

1. ネットワークカメラの IP アドレスまたはポートが正しくありません。
2. ビデオレコーダーとカメラの間のネットワークが切断されています。

解決方法

1. 次の順に進み、**Camera → Camera → IP Camera**、選択したカメラの をクリックし、その IP アドレスとポートを編集します。 ビデオレコーダーとカメラが同じポートを使用していることを確認してください。
2. 次の順に進み、**Maintenance → Network → Detection**、**Destination Address** にネットワークカメラの IP アドレスを入力し、**Test** をクリックして、ネットワークに到達可能かどうかを確認します。

13.5.9 ネットワークカメラの IP アドレスが自動的に変更されるのはなぜですか？

原因

ネットワークカメラとビデオレコーダーが同じスイッチを使用しているが、サブネットが異なる場合、ビデオレコーダーはネットワークカメラの IP アドレスをそのビデオレコーダーと同じサブネットに変更します。

解決方法

カメラを追加する場合は **Custom Add** をクリックして、カメラを追加します。

13.5.10 ビデオレコーダーが IP 競合を通知しているのはなぜですか？

原因

ビデオレコーダーが、他の機器と同じ IP アドレスを使用しています。

解決方法

ビデオレコーダーの IP アドレスを変更してください。他の機器と同じでないことを確認してください。

13.5.11 シングルまたはマルチチャネルのカメラで再生すると、画像が固まるのですが？

原因

HDD の読み書きの異常です。

解決方法

画像をエクスポートして、他のデバイスで再生してください。他のデバイスで正常に再生される場合は、HDD を交換し、再度試しください。

13.5.12 ビデオレコーダーが起動すると、ビープ音が鳴るのですが？

原因

1. フロントパネルが固定されていない（フロントパネルが取り外し可能な機器の場合）。
2. HDD エラー、または HDD が装着されていない。

解決方法

1. ビープ音が鳴り続け、機器のフロントパネルが取り外し可能な場合、フロントパネルが固定されていることを確認してください。
2. 非連続的なビープ音（長音 3、短音 2）が鳴る場合は、HDD エラーを例にとり、HDD が装着されているかどうかを確認します。そうでない場合は、次の順に進み、**System → Event → Normal Event → Exception**、**Event Hint Configuration** のチェックを外して HDD エラーイベントヒントを無効にします。
   HDD が初期化されているか確認してください。そうでない場合は、Storage → Storage Device に進んで HDD を初期化します。
   HDD が壊れていないか確認してください。HDD を変えて再試行してください。

13.5.13 動体検知を設定しても、録画された動画がないのはなぜですか？

原因

1. 録画予約に誤りがあります。
2. 動体検知イベントの設定が間違っています。
3. HDD の異常です。

解決方法

1. 録画 / キャプチャースケジュールの設定に記載されている手順で、録画スケジュールが正しく設定されます。
2. 動体検知エリアが正しく設定されています。チャンネルは動体検知で作動されています（「動体検知の設定」を参照）。
3. HDD が搭載されているかを確認してください。
   HDD が初期化されているか確認してください。そうでない場合は、Storage → Storage Device に進んで HDD を初期化します。
   HDD が壊れていないか確認してください。HDD を変えて再試行してください。

13.5.14 PTZ カメラをコアキトロン経由で制御できないのはなぜですか？

原因

1. このカメラはコアキトロンには対応していません。
2. コアキトロンのプロトコルが間違っています。
3. ビデオ光トランシーバーの影響を受ける信号です。

解決方法

1. ビデオ入力信号が HDTVI であること、カメラがコアキトロンに対応していることを確認してください。
2. ボーレートやアドレスなど、コアキシトロンプロトコルのパラメータが正しいか確認してください。
3. ビデオ光トランシーバーを取り外して、再度お試しください。

13.5.15 RS-485 経由で PTZ が応答しないように見えるのはなぜですか？

原因

1. RS-485 ケーブルが正しく接続されていません。
2. RS-485 インターフェースが壊れています。
3. 制御プロトコルが正しくありません。

解決方法

1. RS-485 ケーブルが正しく接続されているか確認してください。
2. RS-485 インターフェースを変えて、再度お試しください。
3. 制御プロトコルが Pelco であることを確認してください。

13.5.16 動画の音質が良くないのですが？

原因

1. オーディオ入力デバイスの集音効果が良くない。
2. 伝送に支障をきたしています。
3. オーディオパラメータが正しく設定されていません。

解決方法

1. 音声入力機器が正常に動作しているか確認してください。別の音声入力機器に変えて、もう一度試してみてください。
2. オーディオの伝送路を確認してください。すべての線が適切に接続または溶接されていること、および電磁波の干渉がないことを確認してください。
3. 環境や音声入力機器に応じて、音声の音量を調整してください。


See Far, Go Further