ネットワークビデオレコーダー

ユーザーマニュアル

対応機種

Y4988　V6391　D5196　D3252
H3054　V4724　E1686 C8959
M9744　D5010

R0594　X1129　G7135　F4688
L4837　X6323　C5113
T3729　C0758　F5372

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、当社ウェブサイトでご確認ください。
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

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。当社は、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。当社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、当社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、当社はサイバー攻撃、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、当社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

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-9600NI-I8(B)	DS-9608NI-I8(B)
	DS-9616NI-I8(B)
	DS-9632NI-I8(B)
	DS-9664NI-I8(B)
DS-9600NI-I16(B)	DS-9616NI-I16(B)
	DS-9632NI-I16(B)
	DS-9664NI-I16(B)
DS-9600NI-I8	DS-9608NI-I8
	DS-9616NI-I8
	DS-9632NI-I8
	DS-9664NI-I8
DS-9600NI-I16	DS-9616NI-I16
	DS-9632NI-I16
	DS-9664NI-I16
DS-8600NI-I8	DS-8608NI-I8
	DS-8616NI-I8
	DS-8632NI-I8
	DS-8664NI-I8
DS-8600NI-I8/24P	DS-8632NI-I8/24P
DS-7600NI-I2	DS-7608NI-I2
	DS-7616NI-I2
	DS-7632NI-I2
DS-7600NI-I2/P	DS-7608NI-I2/8P
	DS-7616NI-I2/16P
	DS-7632NI-I2/16P

シリーズ	モデル
DS-7700NI-I4	DS-7708NI-I4
	DS-7716NI-I4
	DS-7732NI-I4
DS-7700NI-I4(B)	DS-7716NI-I4(B)
	DS-7732NI-I4(B)
DS-7700NI-I4/P	DS-7708NI-I4/8P
	DS-7716NI-I4/16P
	DS-7732NI-I4/16P
DS-7700NI-I4/P(B)	DS-7716NI-I4/16P(B)
	DS-7732NI-I4/16P(B)
DS-7800NI-I2	DS-7808NI-I2
	DS-7816NI-I2
	DS-7832NI-I2
DS-7800NI-I2/P	DS-7808NI-I2/8P
	DS-7816NI-I2/16P
	DS-7832NI-I2/16P
DS-7900NI-I4	DS-7916NI-I4
	DS-7932NI-I4
DS-7900NI-I4/P	DS-7916NI-I4/16P
	DS-7932NI-I4/16P
	DS-7932NI-I4/24P
DS-7608NI-M2	R0594 / X1129 / G7135 / F4688
	L4837 / X6323 / C5113
	T3729 / C0758 / F5372
DS-7600NI-M2/P	Y4988 / V6391 / D5196 / D3252
	H3054 / V4724 / E1686
DS-7700NI-M4	DS-7716NI-M4
	DS-7732NI-M4

シリーズ	モデル
DS-7700NI-M4/P	DS-7708NI-M4/8P
	DS-7716NI-M4/16P
	C8959 / M9744 / D5010
DS-9600NI-M8	DS-9616NI-M8
	DS-9632NI-M8
	DS-9664NI-M8
DS-9600NI-M8/R	DS-9616NI-M8/R
	DS-9632NI-M8/R
	DS-9664NI-M8/R
DS-9600NI-M16	DS-9616NI-M16
	DS-9632NI-M16
	DS-9664NI-M16
DS-9600NI-M16/R	DS-9616NI-M16/R
	DS-9632NI-M16/R
	DS-9664NI-M16/R

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。
- 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。
- ロウソク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。

記述について

記述を簡略化するため、以下の規約をお読みください。

- レコーダーやデバイスは、主にビデオレコーダーを指します。
- IP 機器とは、主にネットワークカメラ（IP カメラ）、IP ドーム（スピードドーム）、DVS（デジタルビデオサーバー）、NVS（ネットワークビデオサーバー）などを指します。
- チャンネルとは、主にビデオレコーダーの映像チャンネルを指します。

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	商品説明
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を提供します。

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 4
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 ネットワークカメラの追加 9
1.4.1 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 10
1.4.2 ネットワークカメラを手動で追加する 10
1.4.3 PoE 経由でネットワークカメラを追加する 12
1.4.4 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
1.5 プラットフォームへの接続 15
1.5.1 ISUP を設定する 15
1.5.2 Guarding Vision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 カメラの時刻同期 21
2.5 ネットワークカメラ認証のインポート 22
2.6 IP カメラの設定ファイルのインポート / エクスポート 23
2.7 カメラ VCA データの保存 23
2.8 IP カメラのアップグレード 23
第 3 章 ライブビュー 25
3.1 ライブビューの開始 25
3.1.1 ライブビューを設定する 26
3.1.2 ライブビューレイアウトを設定する 27

3.1.3 メイン / 補助ポートを切り替える 28
3.2 デジタルズーム 28
3.3 フィッシュアイビュー 29
3.4 3D ポジショニング 30
3.5 チャンネルゼロエンコーディングの設定 30
3.6 PTZ コントロール 31
3.6.1 PTZ パラメーターを設定する 31
3.6.2 プリセットを設定する 32
3.6.3 プリセットを呼び出す 33
3.6.4 パトロールを設定する 33
3.6.5 パトロールを呼び出す 35
3.6.6 パターンを設定する 36
3.6.7 パターンを呼び出す 37
3.6.8 リニアスキャンリミットの設定 37
3.6.9 ワンタッチパーク 38
第 4 章 録画と再生 39
4.1 録画 39
4.1.1 録画パラメーターを設定する 39
4.1.2 H.265 ストリームアクセスを有効にする 41
4.1.3 ANR 41
4.1.4 手動で録画する 41
4.1.5 録画スケジュールを設定する 42
4.1.6 休日録画を設定する 43
4.2 再生 44
4.2.1 インスタント再生 44
4.2.2 通常の動画を再生する 45
4.2.3 スマート検索された動画を再生する 46
4.2.4 カスタム検索されたファイルを再生する 47
4.2.5 タグファイルを再生する 47
4.2.6 サブピリオドで再生する 48
4.2.7 外部ファイルを再生する 49

4.3 再生操作 49
4.3.1 ビデオクリップを編集する 49
4.3.2 サムネイルビュー 49
第 5 章 画像キャプチャー 50
5.1 パラメータを設定する 50
5.2 録画のスケジュールを設定する 50
5.3 休日録画のスケジュールを設定する 51
第 6 章 イベント 52
6.1 通常イベントアラーム 52
6.1.1 動体検知アラームの設定 52
6.1.2 ビデオロスアラームを設定する 52
6.1.3 ビデオタンパリングアラームの設定 53
6.1.4 センサーアラームを設定する 53
6.1.5 異状アラームを設定する 53
6.1.6 コンバインドアラームの設定 54
6.2 VCA イベントアラーム 55
6.2.1 温度スクリーニング 56
6.2.2 トランスペアレント伝送 56
6.2.3 ハードハット検知 57
6.2.4 フェイスキャプチャー 57
6.2.5 ラインクロッシング検知 58
6.2.6 侵入検知 60
6.2.7 領域入口検知 61
6.2.8 領域退去検知 63
6.2.9 車両検知 64
6.2.10 マルチターゲットタイプ検知 64
6.2.11 建物から投げ出された対象 65
6.2.12 ロイタリング検知 66
6.2.13 人の密度検知 68
6.2.14 高速移動検知 69
6.2.15 パーキング検知 70
6.2.16 不審手荷物の検知 71

6.2.17 対象物持ち出し検知 72
6.2.18 音声異常検知 74
6.2.19 デフォーカス検知 75
6.2.20 突然のシーンチェンジ検知 76
6.2.21 PIR アラーム 76
6.2.22 サーマルカメラ検知 77
6.2.23 キューマネージメント 78
6.3 ターゲット検知 78
6.4 アーミングスケジュールの設定 79
6.5 リンケージアクションの設定 80
6.5.1 フルスクリーンモニタリング自動切替えを設定する 80
6.5.2 ブザーを設定する 81
6.5.3 サーベイランスセンターへ通知する 81
6.5.4 メールリンケージを設定する 82
6.5.5 オーディオアラートを設定する 82
6.5.6 アラーム出力を作動する 82
6.5.7 オーディオとライトアラームリンケージを設定する 83
6.5.8 PTZ リンケージを設定する 83
第 7 章 IoT 84
7.1 IoT デバイスの追加 84
7.1.1 アクセス管理デバイスを追加する 84
7.1.2 アラームデバイスを追加する 85
7.2 リンケージアクションとアーミングスケジュールの設定 87
7.3 OSD の設定 88
7.4 IoT レコードの検索 89
7.5 IoT ビデオ / ピクチャー 90
7.5.1 イベント録画 / イベントキャプチャを設定する 90
7.5.2 IoT 動画を検索する 92
第 8 章 スマートレポート 94
8.1 人数カウント 94
8.2 ヒートマップ 94

第 9 章 ファイル管理 96
9.1 ファイル検索 96
9.2 ファイルのエクスポート 96
9.3 クイックバックアップ 97
9.4 スマートサーチ 97
9.4.1 顔画像検索 97
9.4.2 ヒト検索 98
9.4.3 車両検索 99
第 10 章 ストレージ 100
10.1 ストレージデバイスの管理 100
10.1.1 ローカル HDD を管理する 100
10.1.2 ネットワークディスクを追加する 102
10.1.3 クラウドストレージを設定する 103
10.1.4 eSATA を管理する 104
10.1.5 録画書込みバッファの動的調整 106
10.2 ディスクアレイ 107
10.2.1 ディスクアレイを作成する 107
10.2.2 アレイを再構築する 110
第 11 章 ホットスペアデバイスバックアップ 113
11.1 稼働デバイスの設定 113
11.2 ホットスペアデバイスの設定 114
11.3 ホットスペアシステムの管理 114
第 12 章 ネットワーク設定 117
12.1 DDNS の設定 117
12.2 PPPoE の設定 117
12.3 SNMP の設定 118
12.4 電子メールの設定 120
12.5 ポートマッピング (NAT) の設定 121
12.6 ポートの設定 122
12.7 ONVIF の設定 124

第 13 章 POS 設定 125
13.1 POS 接続の設定 125
13.2 POS テキストオーバーレイの設定 128
13.3 POS アラームの設定 130
第 14 章 ユーザー管理とセキュリティ 131
14.1 ユーザーアカウントの管理 131
14.1.1 ユーザーを追加する 131
14.1.2 管理者ユーザーを編集する 132
14.1.3 Operator/Guest User を編集する 133
14.2 ユーザー権限の管理 134
14.2.1 ユーザー権限を設定する 134
14.2.2 ロック画面のライブビューの権限を設定する 136
14.2.3 管理者ユーザー以外の二重認証権限の設定 137
14.3 パスワードセキュリティの設定 138
14.3.1 GUID ファイルをエクスポートする 138
14.3.2 セキュリティに関する質問を設定する 139
14.3.3 予約メールの設定 140
14.4 パスワードのリセット 141
14.4.1 GUID でパスワードをリセットする 141
14.4.2 セキュリティ質問でパスワードをリセットする 142
14.4.3 予約メールでパスワードをリセットする 142
14.4.4 Guarding Vision でパスワードをリセットする 143
第 15 章 システム管理 144
15.1 デバイスの設定 144
15.2 時間の設定 144
15.2.1 手動で時刻を合わせる 145
15.2.2 NTP を同期する 145
15.2.3 DST を同期する 145
15.3 オーディオの管理 146
15.4 エンハンスド SVC モードの設定 146
15.5 ネットワークの検知 147
15.5.1 ネットワークトラフィックをモニタリングする 147

15.5.2 ネットワーク遅延とパケットロスをテストする 147
15.5.3 ネットワークパケットをエクスポートする 148
15.5.4 ネットワークリソースの統計情報 148
15.6 ストレージデバイスのメンテナンス 149
15.6.1 バッドセクターを検知する 149
15.6.2 S.M.A.R.T. 検知 150
15.6.3 HDD のヘルス検知 151
15.6.4 ディスククローンを設定する 151
15.6.5 データベースを修復する 152
15.7 本機のアップグレード 153
15.7.1 ローカルバックアップデバイスによるアップグレード 153
15.7.2 FTP によるアップグレード 153
15.7.3 Guarding Vision によるアップグレード 154
15.8 機器設定ファイルのインポート / エクスポート 154
15.9 ログの管理 155
15.9.1 ログを保存する 155
15.9.2 ログファイルの検索とエキスポート 156
15.9.3 サーバーへログをアップロードする 157
15.9.4 一方向認証 158
15.9.5 双方向認証 158
15.10 初期設定の復元 159
15.11 自動メンテナンス 160
15.12 セキュリティ管理 161
15.12.1 ONVIF を設定する 161
15.12.2 IP/MAC アドレスフィルター 161
15.12.3 RTSP 認証 162
15.12.4 RTSP ダイジェストアルゴリズム 163
15.12.5 ISAPI サービス 163
15.12.6 HTTP 認証 163
15.12.7 HTTP/ ウェブダイジェストアルゴリズム 164
15.12.8 画像 URL ダイジェスト認証 164
15.12.9 シリアルポート認証サービス 164

第 16 章 付録 165
16.1 用語集 165
16.2 通信マトリクス 166
16.3 デバイスコマンド 167
16.4 よくある質問 167
16.4.1 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？ 167
16.4.2 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？ 168
16.4.3 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？ 168
16.4.4 再生画質を向上させる方法は？ 168
16.4.5 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？ 168
16.4.6 再生時のタイムラインが一定でないのはなぜですか？ 169
16.4.7 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？ 169
16.4.8 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？ 169
16.4.9 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？ 170
16.4.10 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？ 170
16.4.11 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？ 170
16.4.12 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？ 171
16.4.13 動画の音質が良くないのですが？ 171

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. 本機に接続されているネットワークカメラを起動するためのパスワードを入力します。
3. **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。

次は

ウィザードに従って、基本的なパラメータを設定します。

- パスワードを忘れたときはパスワードをリセットできます。起動後、少なくとも 1 つのパスワードをリセット用に設定しておく必要があります。
- Guarding Vision の設定について、詳しくは **Guarding Vision を設定する**を参照してください。

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。

本機を使用する前に

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。

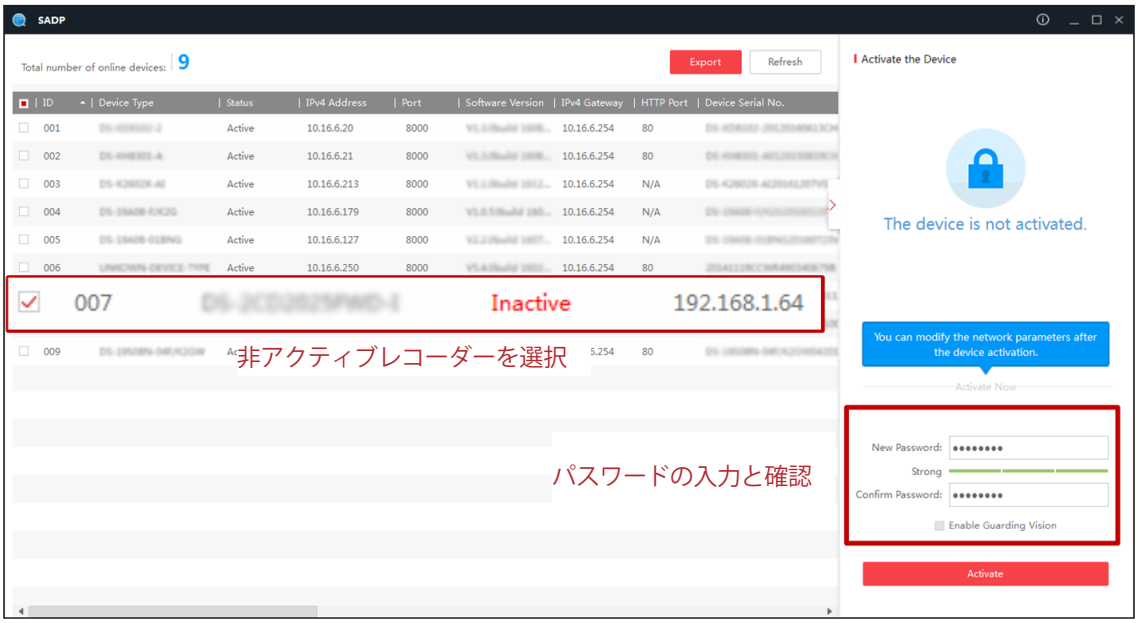

図 1-2 SADP による起動

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。

本機を使用する前に

弊社ホームページからクライアントソフトウェア（Windows用遠隔閲監視用ソフトGuarding Vision）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。

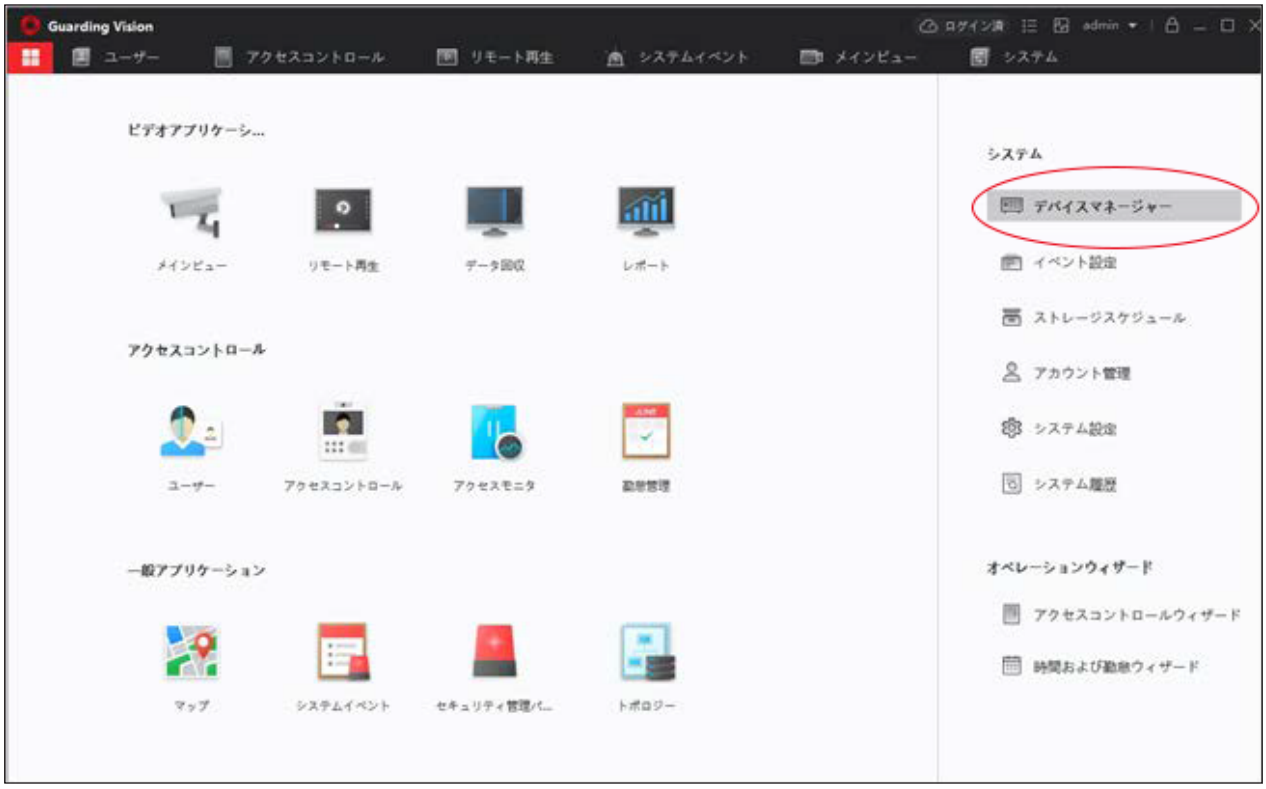

図 1-3 操作パネル

2. **デバイスマネージャー**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。

   オンラインデバイス をクリックすると画面下部にオンラインの機器一覧が表示されます。

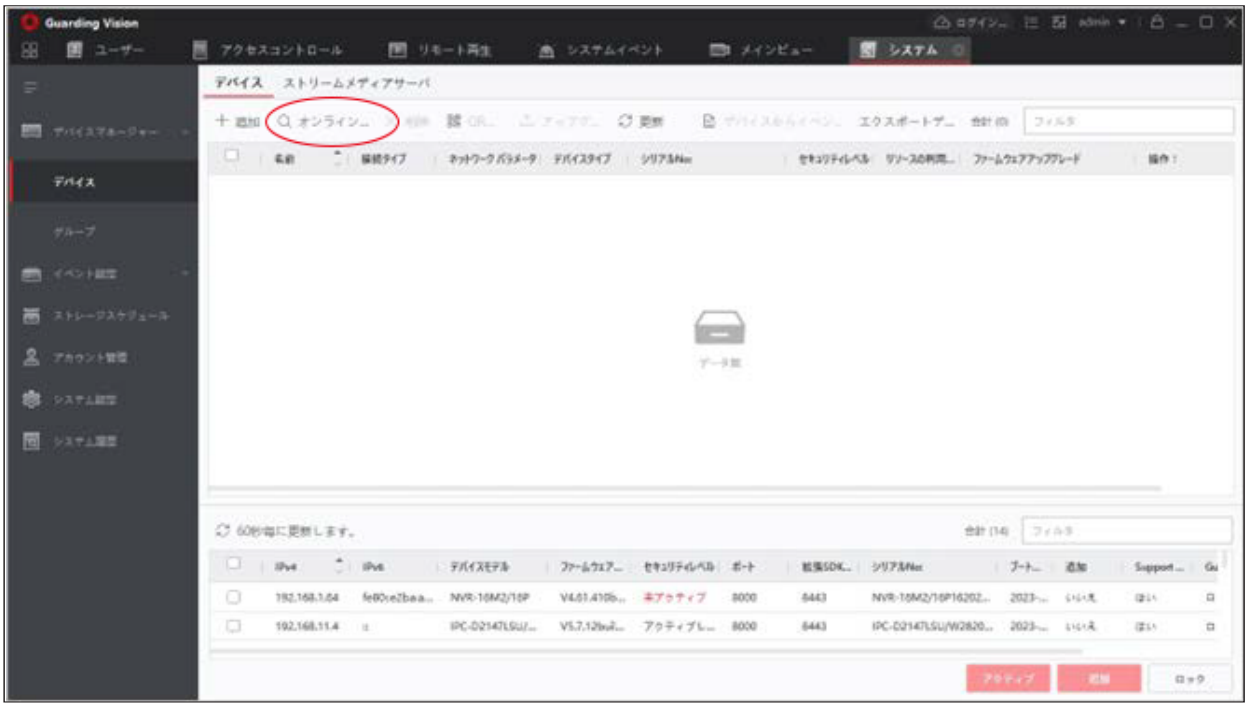

図 1-4 デバイス管理インタフェース

3. 機器一覧から非アクティブのレコーダーを選択し、本機の □ にチェックを入れます。
4. **アクティブ**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. **機器一覧の本機の右端の** 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。**IP設定** ☐ **DHCP** の☐ にチェックを入れてください。
9. パスワードを入力し、OKをクリックすると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。

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。工場出荷時の IP アドレスは 192.168.1.64 です。

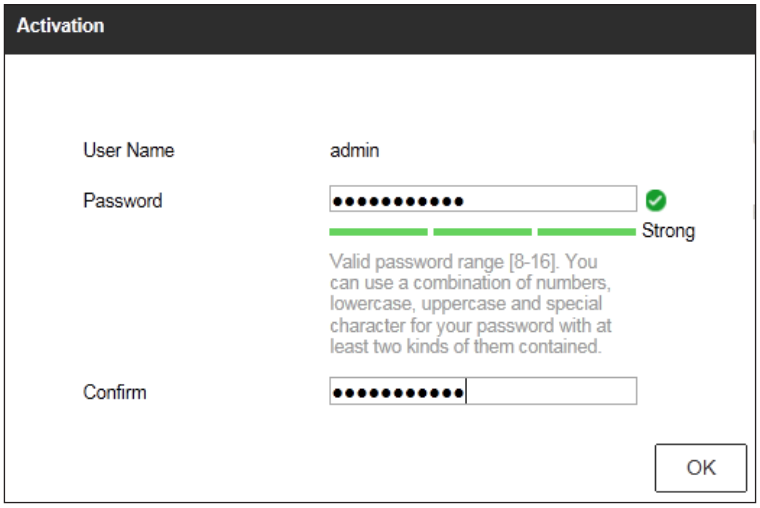

図 1-7 Web ブラウザーの起動

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。

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**

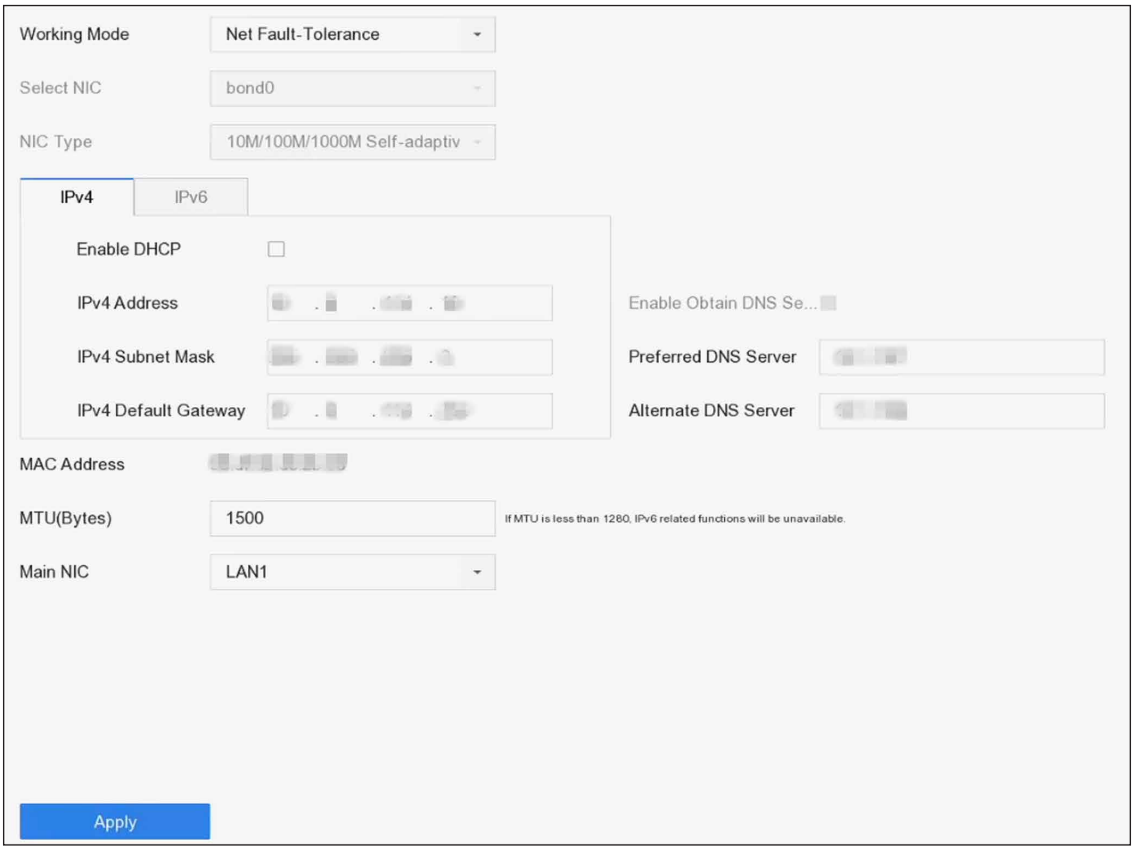

図 1-8 TCP/IP の設定

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　（HDDは、装着済みです）

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 ネットワークカメラの追加

ライブ動画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。

本機を使用する前に

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。

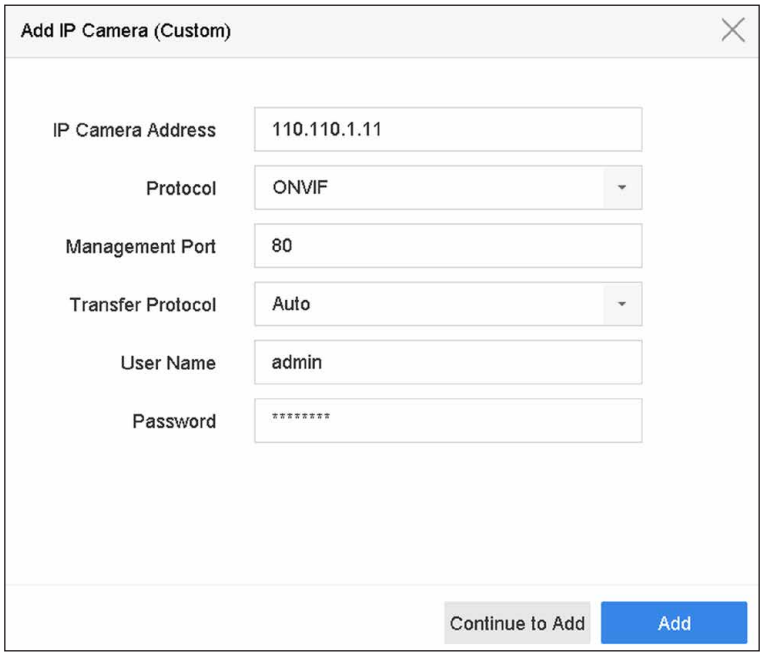

図 1-9 IP カメラの追加

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。

1.4.1 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。

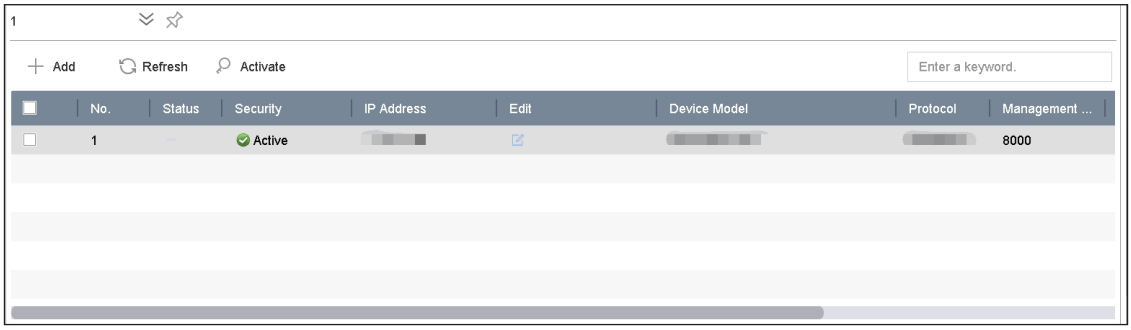

図 1-10 自動検索されたオンラインネットワークカメラの追加

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。

1.4.2 ネットワークカメラを手動で追加する

ライブ動画を表示したり、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。

本機を使用する前に

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。

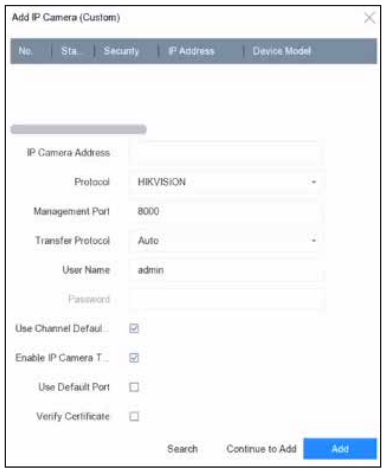

図 1-11 ネットワークカメラの追加

4. オプション：カメラの追加に工場出荷時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：接続した IP カメラの時刻を自動的に同期させる場合は、**Enable IP Camera Time Sync** にチェックを入れます。詳しくは **IP カメラの時刻同期**を参照してください。
6. オプション：工場出荷時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、工場出荷時のポート値は 8000 です。拡張 SDK サービスの場合、工場出荷時値は 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。

7. 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**ネットワークカメラ認証のインポート**を参照してください。

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。

8. オプション：**Search** をクリックすると、他のネットワークカメラを検索することができます。
9. オプション：**Continue to Add** をクリックすると、他のネットワークカメラを追加できます。
10. **Add** をクリックします。

1.4.3 PoE 経由でネットワークカメラを追加する

PoE インターフェースにより、デバイスシステムは、接続された PoE カメラにイーサネットケーブルでデータとともに安全に給電することができます。対応する PoE カメラ番号はデバイスモジュールによって異なります。PoE インターフェースを無効にすると、オンラインのネットワークカメラにも接続できるようになります。また、PoE インターフェースは Plug-and-Play 機能をサポートしています。

PoE カメラの追加

ステップ

1. 次の順に進みます。**Camera → Camera → PoE Settings**
2. **Long Distance** または **Short Distance** を選択して、長距離ネットワークケーブルモードを有効または無効にします。

   Long Distance

   PoE インターフェースによる長距離（100 ～ 300m）ネットワーク伝送が可能です。

   Short Distance

   PoE インターフェースによる短距離（100m 未満）ネットワーク伝送が可能です。

メモ

- PoE ポートは、デフォルトで短距離モードが有効になっています。
- 長距離ネットワークケーブル（100 ～ 300m）で PoE 接続された IP カメラの帯域は、6MP を超えることはできません。
- IP カメラの機種やケーブルの材質によっては、最大許容長が 300m を下回る場合があります。
- 伝送距離が 100 ～ 250m になる場合は、CAT5E または CAT6 ネットワークケーブルで PoE インターフェースと接続する必要があります。
- 伝送距離が 250 ～ 300m になる場合は、CAT6 ネットワークケーブルで PoE インターフェースと接続する必要があります。

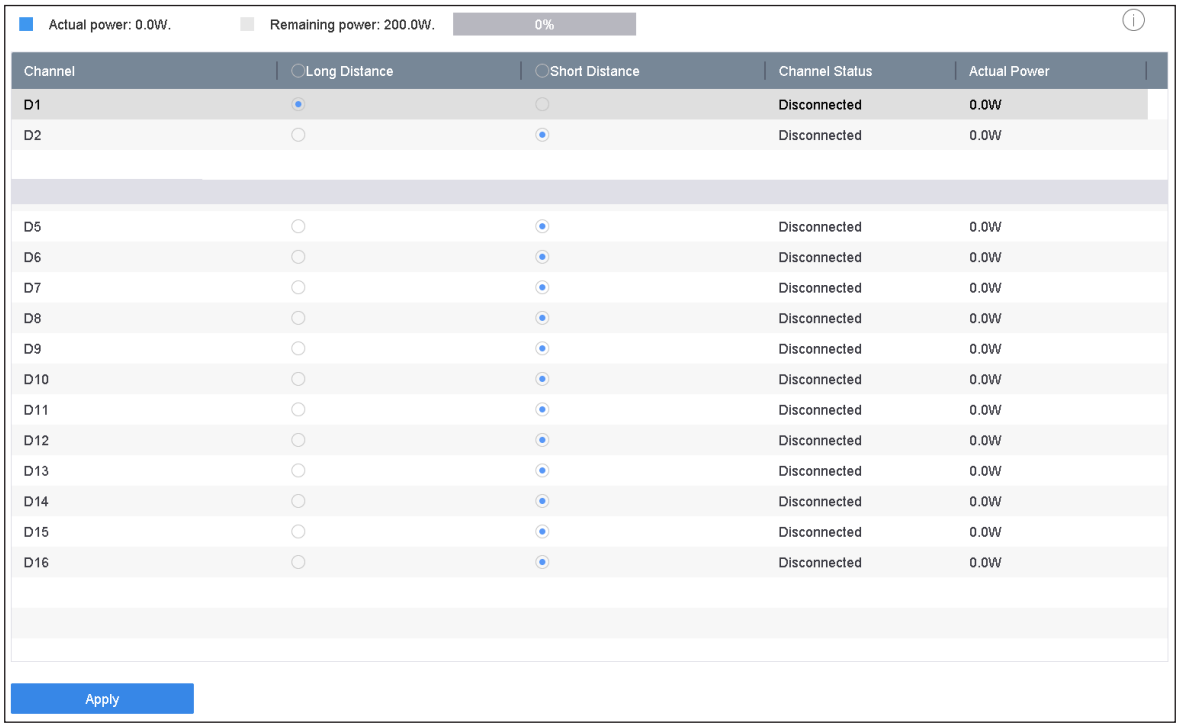

図 1-12 PoE カメラの追加

3 **Apply** をクリックします。
4. PoE カメラと機器の PoE ポートをネットワークケーブルで接続します。
5. **Camera → Camera → IP Camera** の順に進むと、カメラの画像や情報が表示されます。

非 PoE ネットワークカメラの追加

現在のチャンネルを通常のチャンネルとして使用しながら、Manual を選択することで PoE インターフェースを無効にすることができ、パラメータの編集も可能です。

ステップ

1. 次の順に進みます。**Camera → Camera → IP Camera**
2. ネットワークカメラがリンクされていないウィンドウにカーソルを合わせ、 をクリックします。

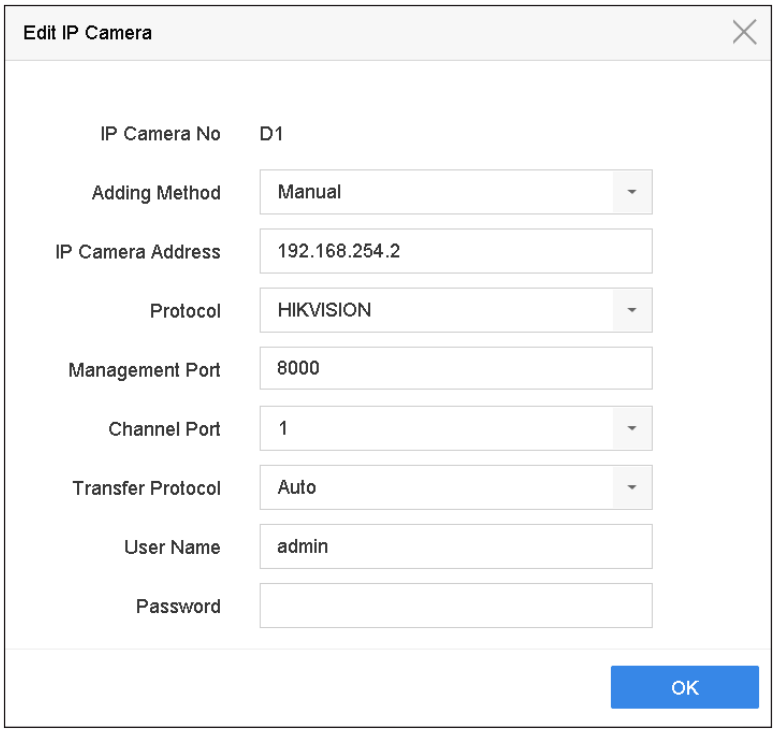

図 1-13 ネットワークカメラの編集

3. **Adding Method** は **Manual** を選択します。

   Plug-and-Play

   カメラは PoE インターフェースに物理的に接続されています。パラメータを編集することはできません。**System → Network → TCP/IP** の順に進んで、PoE ポートの IP アドレスを変更します。

   Manual

   ネットワーク経由で物理的に接続することなく、IP カメラを追加することができます。
4. **IP address**、**User Name**、**Password** を入力します。
5. **OK** ボタンをクリックします。

1.4.4 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. メインメニューバーの をクリックします。
2. 次の順に進みます。**More Settings → Protocol**

メモ

3. 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。

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

1.5 プラットフォームへの接続

1.5.1 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

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

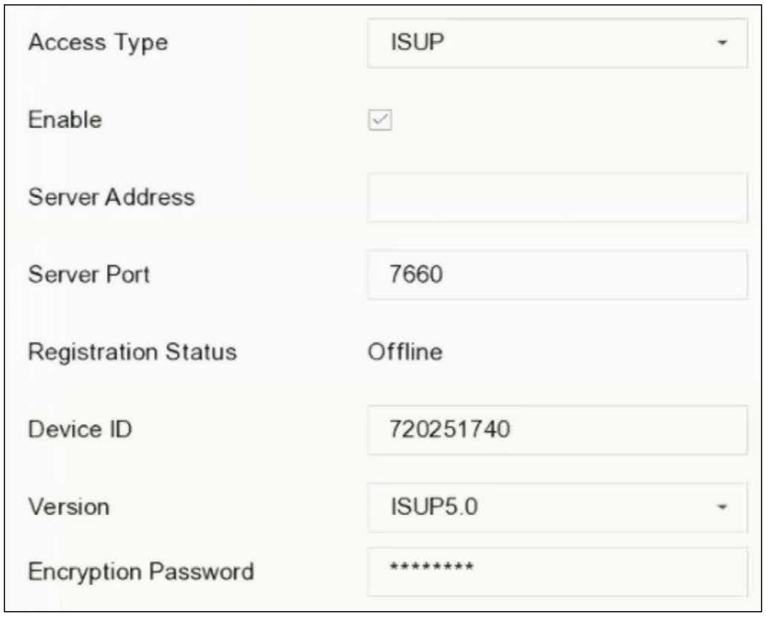

図 1-14 ISUP 設定

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

ISUP プロトコルバージョン、V5.0 のみ使用可能です。

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。

1.5.2 Guarding Vision を設定する

Guarding Vision 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）**Guarding Vision 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稈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

- デフォルトでは Guarding Vision 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 Guarding Vision で時刻を同期します。
4. 本機を Guarding Vision 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、Guarding Vision アプリをダウンロードします。

   https://ho-tu.net/cam/ からダウンロードすることもできます。詳しくは **Guarding Vision 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。

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。

5. **Apply** をクリックします。

次は

Guarding Vision 経由で本機にアクセスすることができます。

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。

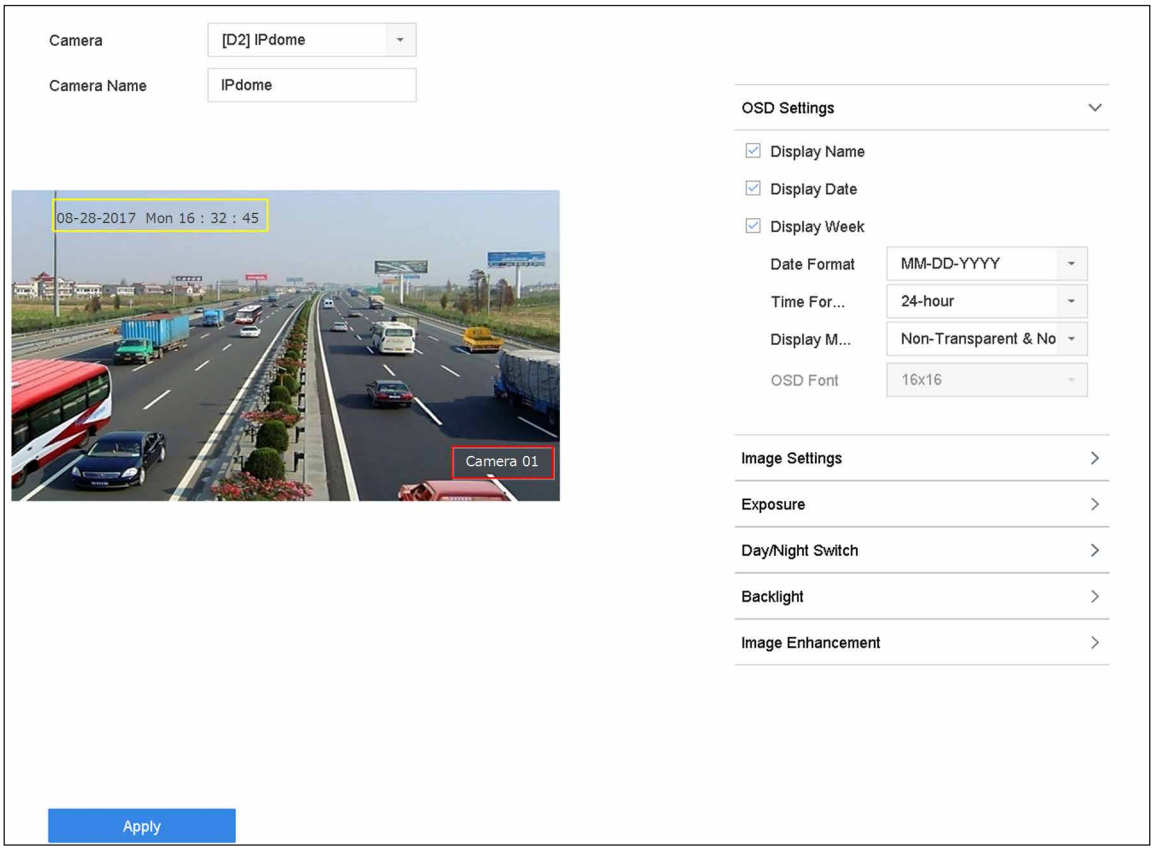

図 2-1 OSD 設定

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。

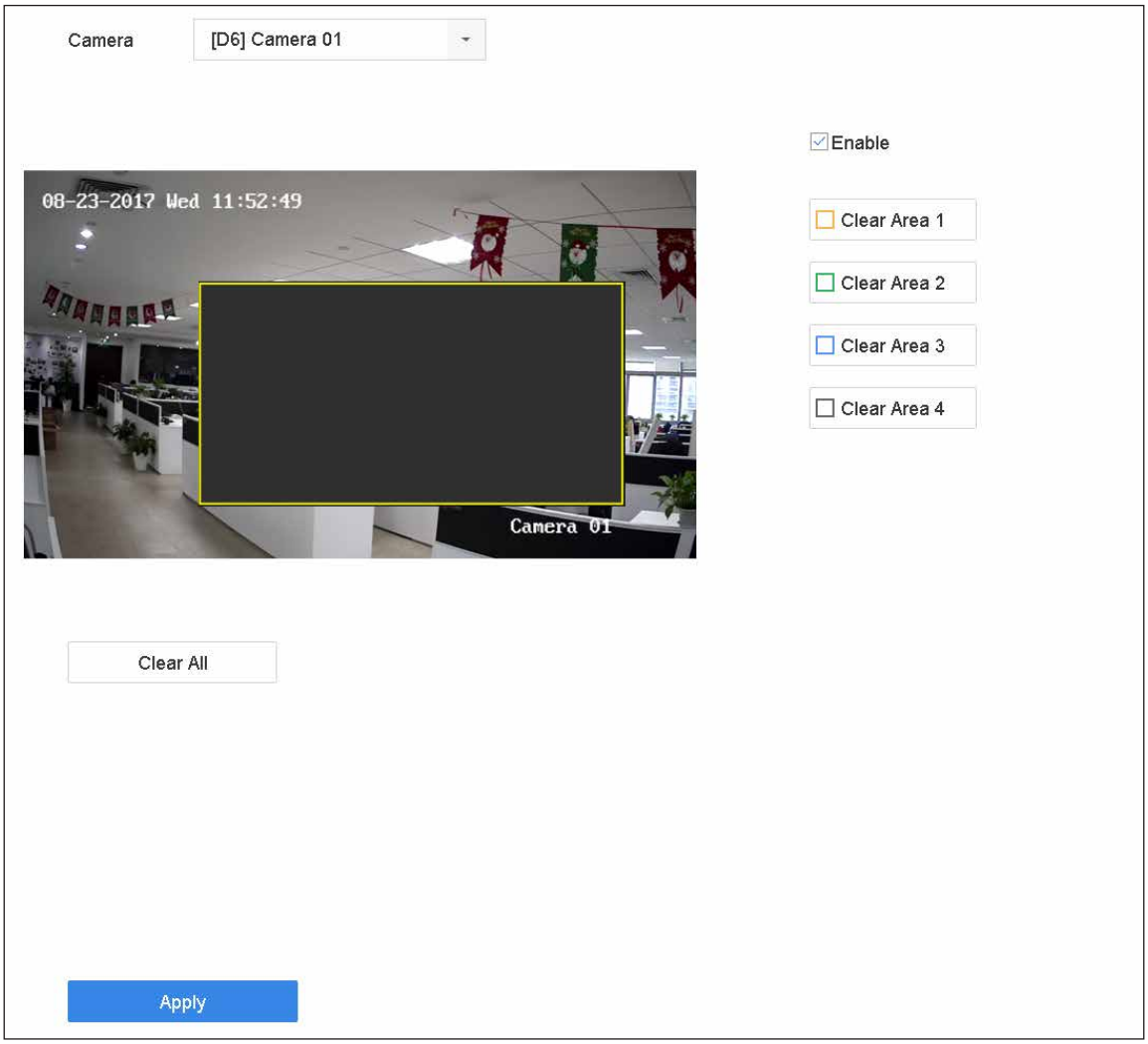

図 2-2 プライバシーマスクの設定

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

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。
5. オプション：すべての IPC チャンネルをショートカットで有効 / 無効にすることができます。
   1）次の順に進みます。**Maintenance → System Service → More Settings**
   2）**Time Sync Configuration** をクリックし、**Enable IPC Time Sync** か **Disable IPC Time Sync** を選択、すべての IPC/IoT チャネルのスケジュール時刻同期を有効 / 無効にします。

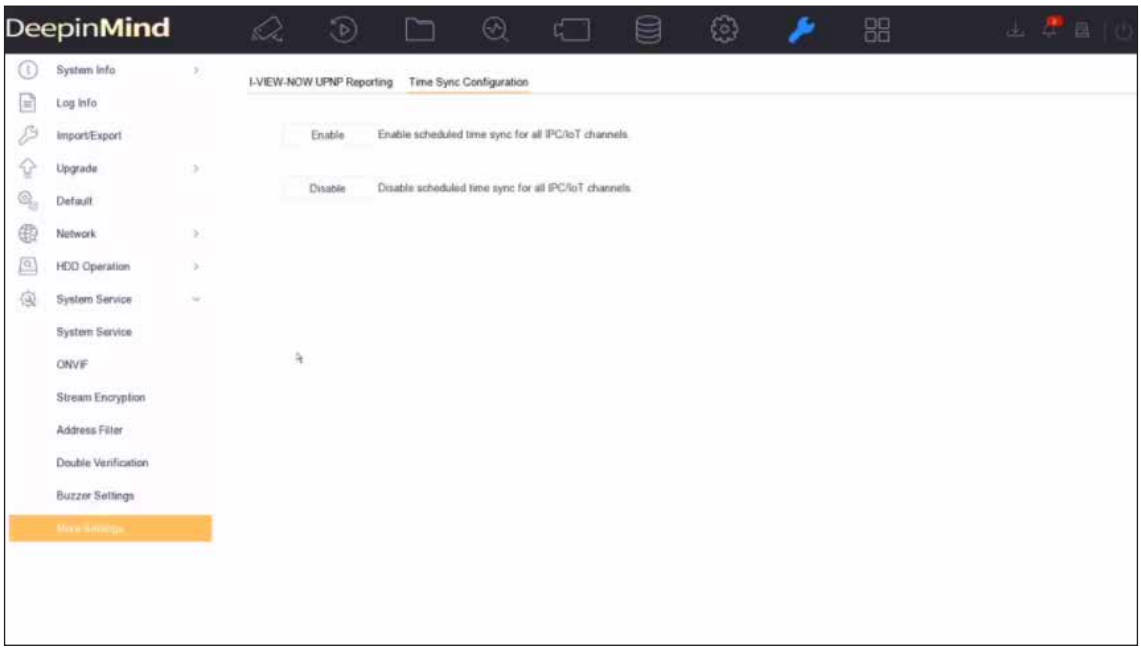

図 2-3 IP カメラの時刻同期

メモ

この機能は、管理者ユーザーだけが使用できます。

2.5 ネットワークカメラ認証のインポート

ネットワークカメラ認証を本機にインポートします。

ステップ

1. Web ブラウザーでネットワークカメラにログインします。
2. Web ブラウザー上で次の順に進み **Configuration → Network → Advanced Settings → HTTPS**、その認証をエクスポートします。
3. **Export Certificate** の **Export** をクリックして、認証を保存します。
4. Web ブラウザーで本機にログインします。
5. 次の順に進みます。**Configuration → System → Security → Trusted Root Certification Authorities → Import**
6. **Import** をクリックして、ネットワークカメラの認証をインポートします。

2.6 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。

本機を使用する前に

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。

2.7 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。

2.8 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。

ステップ

1. 次の順に進みます。**Camera → Camera → IP Camera → More Settings → Upgrade**

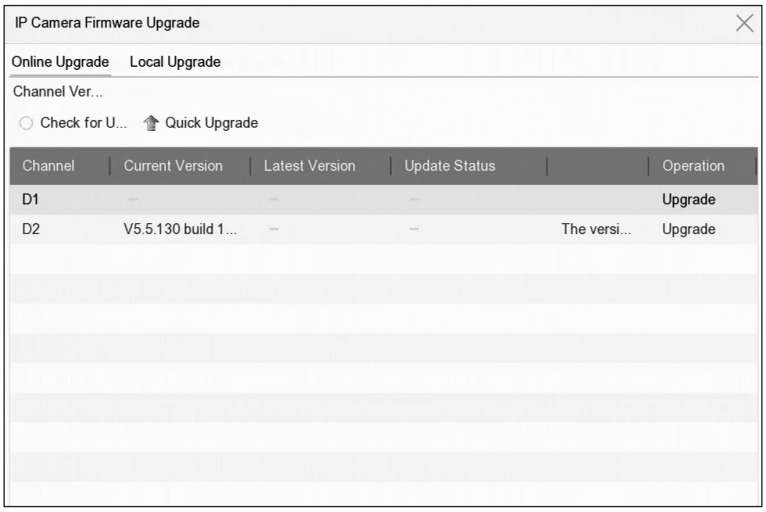

図 2-4 IP カメラのアップグレード

2. カメラのアップグレード方法を選択します。

Online Upgrade

Online Upgrade をクリック、次に **Check for Updates** か **Quick Upgrade** をクリックしてカメラのアップグレードを行います。

メモ

本機が Guarding Vision に正しく接続されていることが必要です。

Local Upgrade

ファームウェアを格納した USB メモリーを本機に接続します。**Local Upgrade** をクリックし、アップグレードするカメラとファームウェアファイルを選択します。

アップグレード後、IP カメラは自動的に再起動します。

3. **Upgrade** をクリックします。

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、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。

メモ

右下角の をクリックすると、終日連続録画が停止します。

- 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。
- をシングルクリックすると、VCA 情報表示が有効になります。 をダブルクリックすると、VCA 情報表示が無効となります。

メモ

右下の をクリックすると、全チャンネルの VCA 情報表示の有効 / 無効を切り替えることができます。最大 16ch の VCA 情報が取得可能です。

- 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。

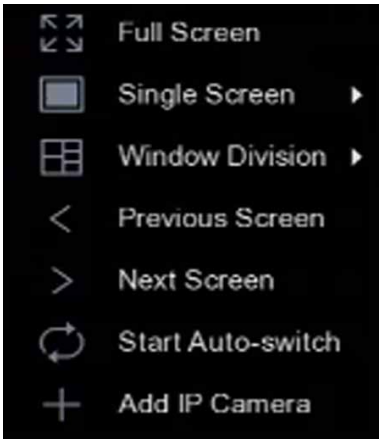

図 3-1 ショートカットメニュー

メモ

異状が発生した場合は、画面にエラー情報が表示されます。 をクリックして、別のチャンネルのパラメータを編集します。

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**

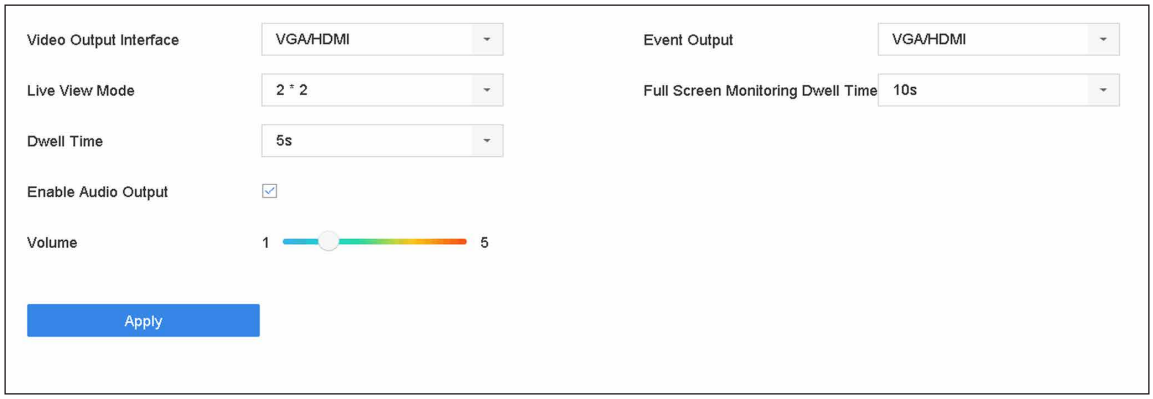

図 3-2 ライブビュー - ゼネラル

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 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。

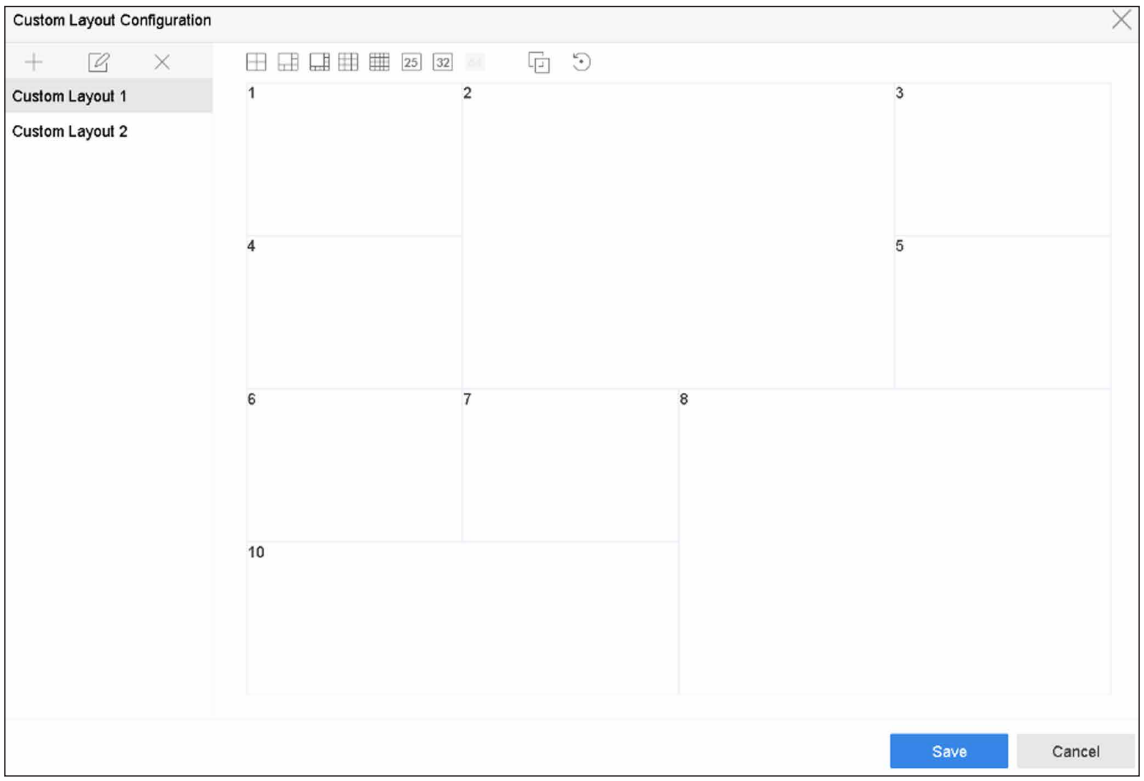

図 3-3 ライブビューのレイアウト設定

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。

3.1.3 メイン / 補助ポートを切り替える

メインポートに表示されている映像のみ、メインメニューに入ることができ、機器の操作ができます。
ライブビューモードでをクリックするか、**System → Live View → General** に進むと、メイン / 補助ポートの切り替えができます。
本機が 2 つの HDMI と 2 つの VGA のインターフェースを持つ場合。HDMI1、VGA1 がメインポートで、映像出力も同時に行います。HDMI2、VGA2 は補助ポートで、映像出力も同時に行います。

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）に映像を拡大・縮小することができます。

図 3-4 デジタルズーム

3.3 フィッシュアイビュー

本機はライブビューや再生モードでの魚眼レンズカメラの拡大に対応しています。

本機を使用する前に

- 魚眼レンズ拡大表示機能は、一部の機種のみ対応しています。
- 接続するカメラが魚眼レンズの表示に対応している必要があります。

ステップ

1. ライブビューを開始し をクリックすると、魚眼拡大モードになります。
2. 拡大表示モードを選択します。

表 3-1 フィッシュアイビューアイコンの説明

アイコン	説明	アイコン	説明
180°パノラマ ( )	ライブビュー画像を 180° パノラマビューに切り替えます。	360°パノラマ ( )	ライブビュー画像を 360° パノラマビューに切り替えます。

アイコン	説明	アイコン	説明
PTZ 拡大 ( )	PTZ 拡大は、フィッシュアイビューやパノラマ拡大で定義された領域のクローズアップ映像です。e–PTZとも呼ばれる電子PTZ 機能をサポートしています。	放射状拡大 ( )	放射状拡大モードでは、魚眼レンズカメラの広角視野全体が表示されます。この表示モードは、魚の凸面の目の見え方に似ていることから、フィッシュアイビューと呼ばれています。このレンズは、映像内の物体の遠近感や角度を歪めながら、広い面積の曲線的な映像を作り出します。

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

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 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。

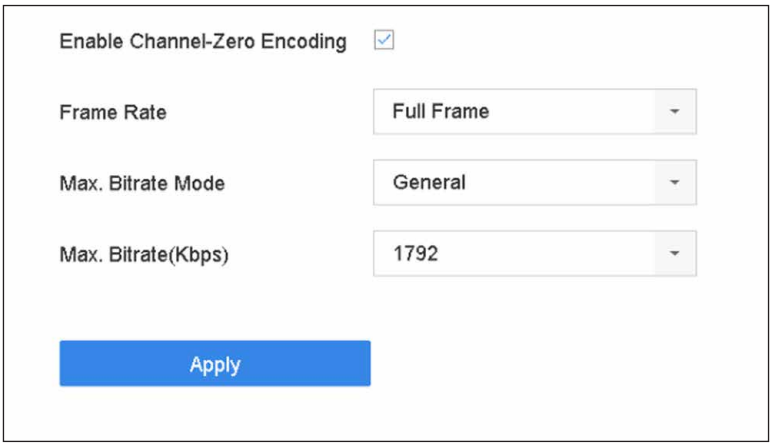

図 3-5 チャネルゼロエンコーディング

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。

3.6 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。

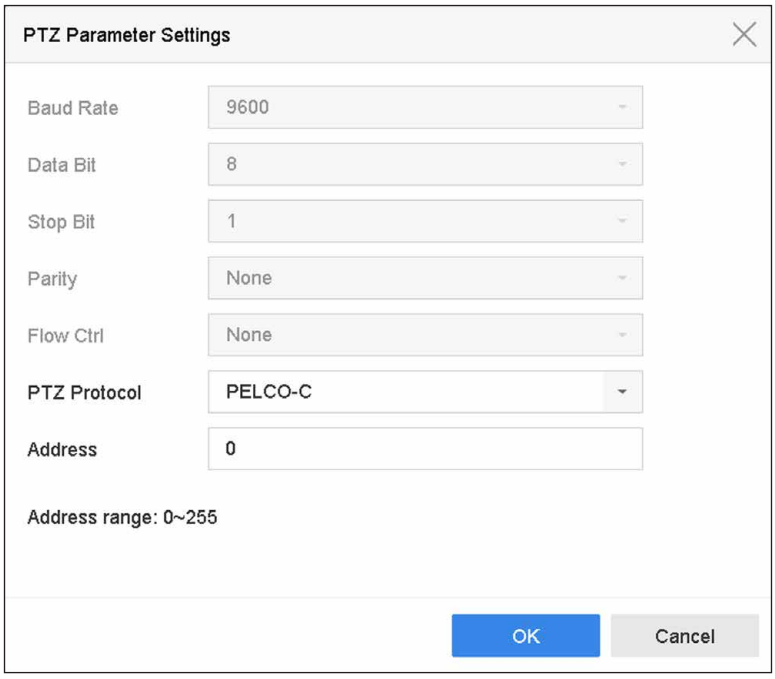

図 3-6 PTZ パラメータの設定

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** 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 3-7 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角にある 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 3-8 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 3-9 プリセットを呼ぶ出す (1)

図 3-10 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 3-11 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

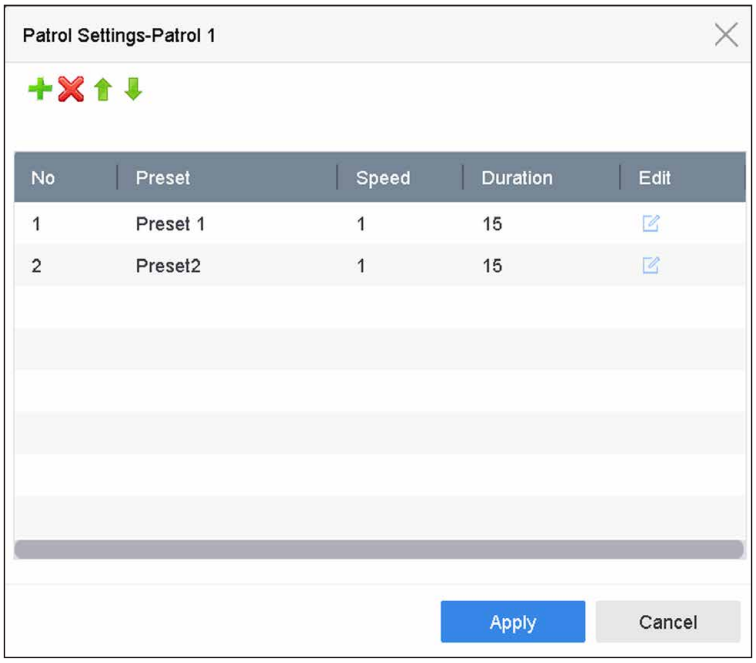

図 3-12 パトロールの設定

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。

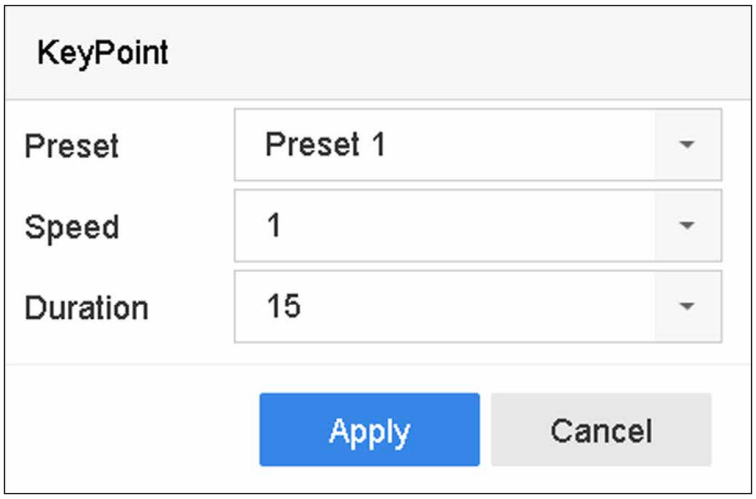

図 3-13 キーポイントの設定

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 3-2 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 3-14 パトロールの設定

3. パトロールを選択します。
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。

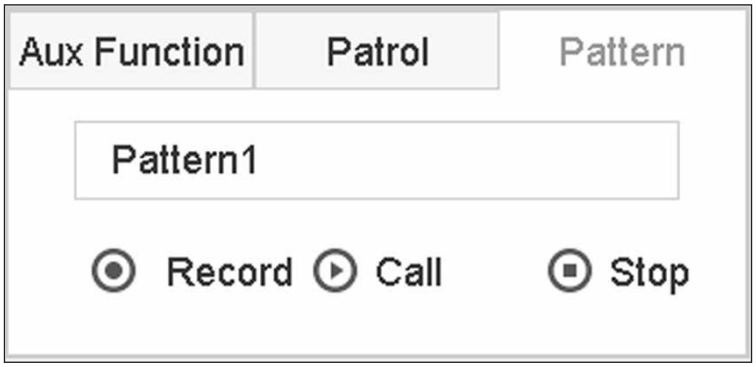

図 3-15 パターン設定

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 3-16 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。

本機を使用する前に

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。

本機を使用する前に

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)**（**プリセット 1**）をクリックしてパークアクションを無効にできます。

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

ビデオパラメータの設定

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 秒間に撮影するフレーム数です。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便利です。

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 Type

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。可変と定数の 2 種類あります。

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.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ドのことです。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。

Video Quality

必要に応じて、ビデオの画質を設定します。映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。

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。

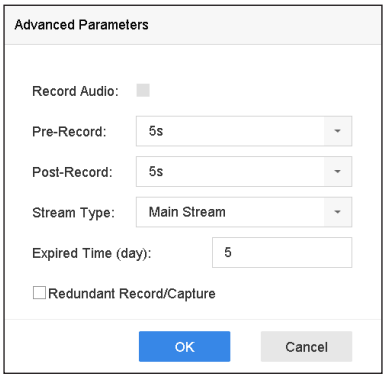

図 4-1 高度な録画設定

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 ANR

ANR（Automatic Network Replenishment）は、ネットワークが切断された状態で、ネットワークカメラの SD カードを自動的に有効にして映像を保存し、ネットワーク回復後にデータを同期させることができます。

本機を使用する前に

- 本機とネットワークカメラの間のネットワーク接続が有効で正しいことを確認してください。
- ネットワークカメラに SD カードが装着されていることを確認してください。

ステップ

1. Web ブラウザーで本機にログインし、次の順に進みます。**Configuration → Storage → Schedule Settings → Advanced**
2. **Enable ANR** にチェックを入れます。
3. **OK** ボタンをクリックします。

4.1.4 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。

4.1.5 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。

本機を使用する前に

- 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された **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。

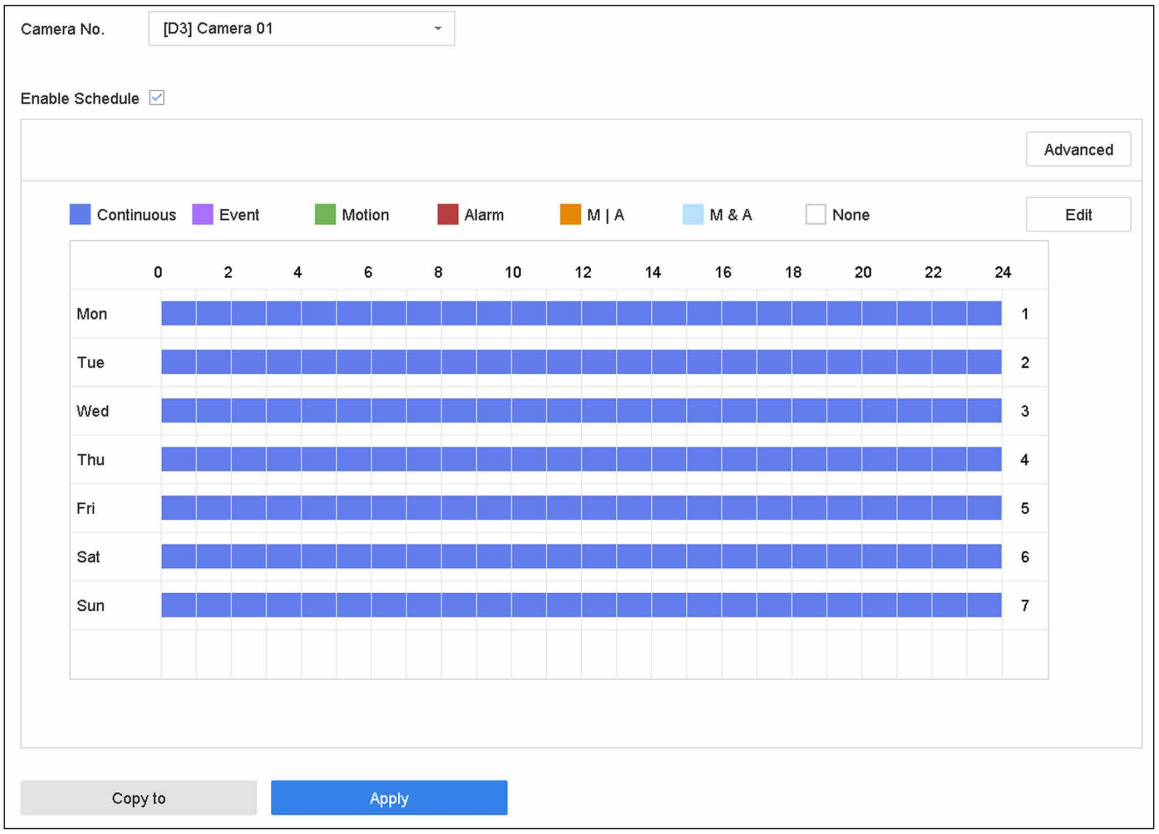

図 4-2 録画スケジュール

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。

4.1.6 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。

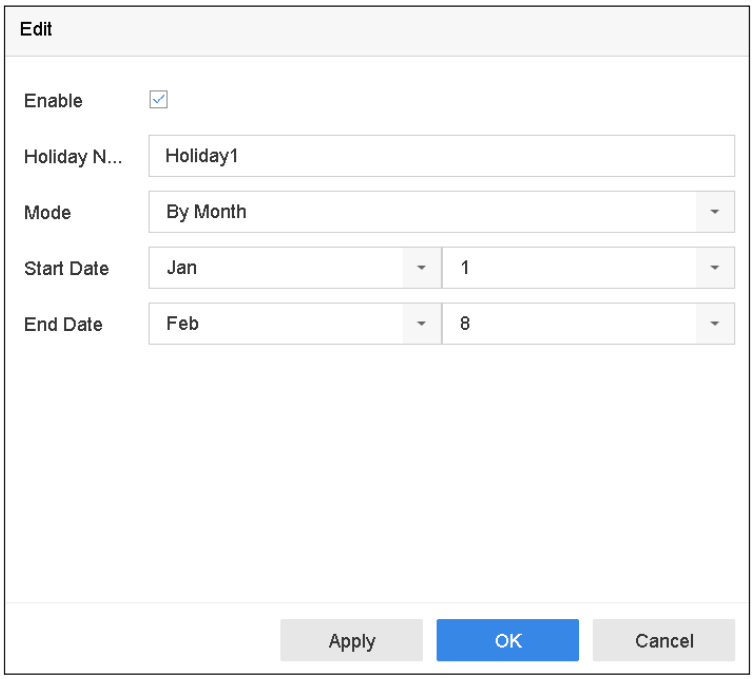

図 4-3 休日設定の編集

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. 休日録画の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**を参照してください。

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 4-4 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 4-5 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、動きや線、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 4-6 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

カスタム検索て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：**Search by Appearance** 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. 左下角の **Custom Search** をクリックします。
3. **Search by Tag** をクリックします。
4. 時間やタグのキーワードを含む検索条件を設定します。
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ます。選択したチャンネルの検索結果が表示されます。
7. をクリックして動画を再生します。
8. 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）**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。

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 HH 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 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。

本機を使用する前に

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 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。

4.3.2 サムネイルビュー

再生インタ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 4-7 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。

第 5 章 画像キャプチャー

メモ

この章は、一部の機種にのみ適用されます。

5.1 パラメータを設定する

画像は、連続録画またはイベント録画で撮影されたライブ画像のことを指します。
Storage → Schedule → Capture → Advanced でピクチャーパラメーターを編集することができます。

Resolution

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。高画質化にはより多くの記憶容量が必要です。

Interval

ライブ映像の撮影間隔です。

Capture Delay Time

画像を撮影する時間です。

5.2 録画のスケジュールを設定する

スケジュールに従って、自動的に撮影を行います。

本機を使用する前に

HDD を設置したこと、またはストレージとしてネットワークディスクを追加したことを確認します。

ステップ

1. 次の順に進みます。**Storage → Schedule → Capture**
2. カメラを選択します。
3. 撮影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。

5.3 休日録画のスケジュールを設定する

1 年のうち、休日録画のスケジュールを設定することができます。本機は、休日の間は録画の優先順位に従って録画プランを決定します。

本機を使用する前に

HDD を設置したこと、またはストレージとしてネットワークディスクを追加したことを確認します。

ステップ

1. 次の順に進みます。**System → Holiday**
2. リストからひとつの休日を選択し をクリックします。
3. **Enable** にチェックを入れます。
4. 名前、モード、日付など、休日のパラメータを編集します。

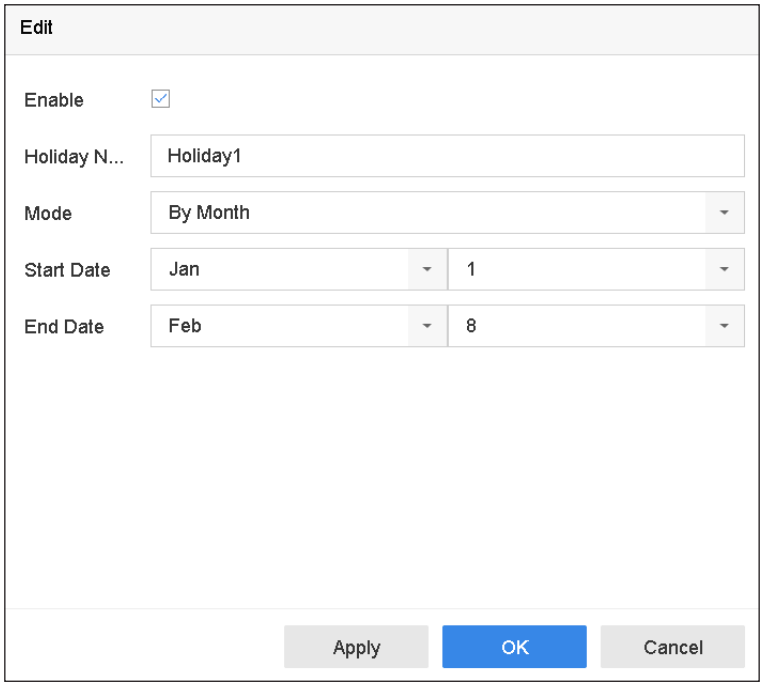

図 5-1 休日設定の編集

5. **OK** ボタンをクリックします。
6. 休日の録画影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。

第 6 章 イベント

6.1 通常イベントアラーム

6.1.1 動体検知アラームの設定

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. 動体検知ルールを設定します。

カメラに人体検知と車両検知の機能がある場合	**Draw Area** をクリックして、プレビュー画面上に検出領域を描画します。**Detection Target** を **Human** または **Vehicle** に設定して、人体または車両によって作動しないアラームを削除します。
カメラに人体検知、車両検知の機能がない場合	**Full screen** をクリックして全画面を検出範囲に設定するか、プレビュー画面上をドラッグしてカスタマイズした検出範囲を描画します。

5. **Sensitivity** を設定します。

Sensitivity

Sensitivity は 0 から 100 の範囲です。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。

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。

6.1.2 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知し、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。

6.1.3 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。

6.1.4 センサー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。

6.1.5 異状アラームを設定する

異状イベントは、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状の種類を選択します。

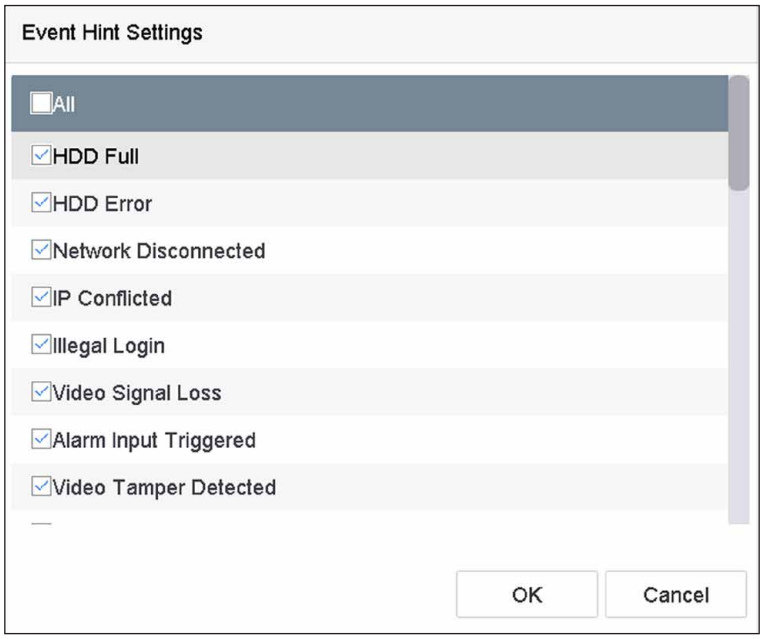

図 6-1 イベントヒントの設定

3. 異状の種類を選択します。

図 6-2 例外処理

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。

6.1.6 コンバインドアラームの設定

コンバインドアラームは、アラーム入力のあるイベントを結合したものです。コンバインドアラームは、アラーム入力とイベントの両方からアラームを受信したときに作動します。イベントの種類には、動体検知、ビデオタンパリング検知、その他ラインクロス検知、侵入検知などのスマートイベントがあります。

本機を使用する前に

チャンネルにイベントアラームが設定されていること、およびアラーム入力が設定されていることを確認してください。(**センサーアラームを設定する**を参照してください。)

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. **Input** として **Settings** を選択します。

4. **Combined Alarm** をクリックします。
5. 見たいチャンネルを選択します。
6. **Combined Alarm Event** を選択します。
7. **Apply** をクリックします。

メモ

コンバインドアラームアーミングスケジュールとリンケージアクションは、選択したイベント（複数可）と同じです。

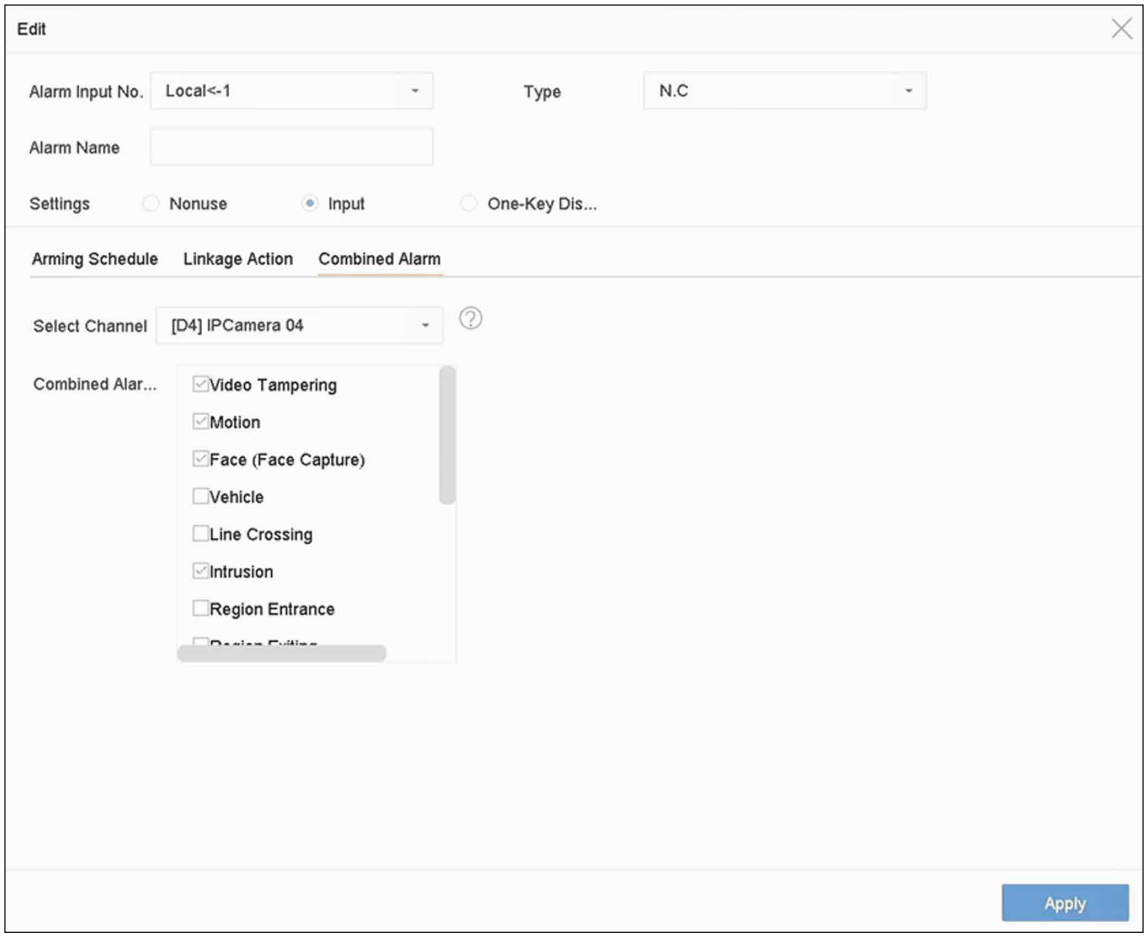

図 6-3 コンバインドアラーム

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 温度スクリーニング

指定のサーモグラフィーカメラを接続すると、温度測定結果を表示したり、正常な温度や異常な温度を検出した場合に音声で通知したりすることができます。

本機を使用する前に

お使いのサーモグラフィーカメラがこの機能をサポートしているか、また正しく設定されているかを確認してください。

ステップ

1. 次の順に進みます。**System → Event → Smart Event**
2. サーモグラフィーカメラの光学チャンネルを選択します。
3. **Face Capture** をクリックします。
4. 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画像が保存されます。
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。サーモグラフィーカメラが異常な温度を検知したときだけリンケージアクションを行う必要がある場合は、**Rule Settings** の **Abnormal Body Temperature** にチェックを入れてください。

   メモ

   サーモグラフィーカメラで異常温度を検知し、定義します。

7. **Apply** をクリックします。

次は

- ライブビューの **Target** にチェックを入れると、検知結果が表示されます。
- **File Management → Smart Search → Search by Appearance** の順に進むと検知結果を検索できます。

6.2.2 トランスペアレント伝送

トランスペアレント伝送により、多種多様なイベントを設定でき、カメラからのイベントアラームも直接伝送できます。スマートイベントに掲載されていないイベントについては、トランスペアレント伝送リストに掲載されます。リストには、接続されているカメラが対応しているイベントのみが表示されます。イベントの説明文は必要に応じてカスタマイズできます。トランスペアレント伝送は Web ブラウザーで設定可能です。

本機を使用する前に

トランスペアレント伝送に対応したカメラが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. 次の順に進みます。**Configuration → Event → More Events → Transparent Transmission Configuration**
   利用可能なイベントは **Event Description List** に掲載されます。
2. **Template List** をクリックすると、テンプレートリストファイルをエクスポートします。

メモ

テンプレートリストは、あくまで参考です。削除や編集はできません。

3. お使いのカメラとテンプレートリストに合わせて Event Description を編集します。

   Event Type

   イベントのタイプは、カメライベントと同じである必要があります。

   Event Description

   イベントの説明をカスタマイズすることができます。イベントのタイプを認識した後、本機はイベントの説明をイベント名として表示します。
4. **Save** をクリックします。

次は

次の順に進んで **Configuration → Event → Smart Event → More Events** をクリックし、イベントを設定します。

6.2.3 ハードハット検知

ハードハット検知は、ヘルメットを着用していない人を検知します。アーミングスケジュールとリンケージアクションを設定することができます。ハードハット検知は、Web ブラウザーで設定できます。

6.2.4 フェイスキャプチャー

フェイスキャプチャーは、監視映像に現れる顔を検知し、録画するものです。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。**Smart Analysis → Smart Event Settings → Facial Recognition**
2. **Face Capture** をクリックします。

図 6-4 フェイスキャプチャー

3. 設定するカメラを選択します。
4. **Enable Face Capture** 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。

メモ

感度の範囲 [1 - 5]。値が高いほど、顔が検知されやすくなります。

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 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。**Smart Analysis → Smart Event Settings → Perimeter Protection**
2. カメラを選択します。
3. **Line Crossing** をクリックします。

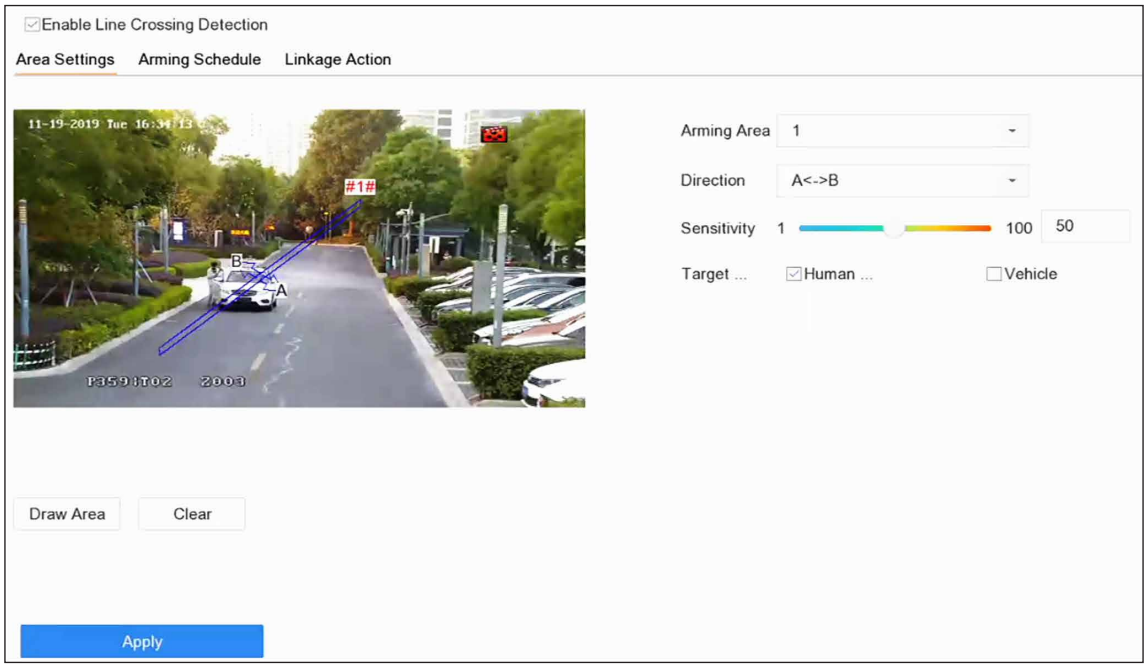

図 6-5 ラインクロッシング検知

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）エイ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知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知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、検知アラームが出やすくなります。
   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. オプション：ターゲットの最大サイズ / 最小サイズを描画します。

メモ

ラインクロッシング検知が作動するのは、最大サイズから最小サイズまでのターゲットのみです。

1）**Max. Size/Min. Size** をクリックします。
2) プレビューウィンドウに領域を描画します。
3）**Stop Drawing** をクリックします。

8. オプション：人体や車両で作動しないアラームを削除するため、**Detection Target** は **Human** または **Vehicle** を選択します。
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** をクリックします。

6.2.6 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。**Smart Analysis → Smart Event Settings → Perimeter Protection**
2. カメラを選択します。
3. **Intrusion** をクリックします。

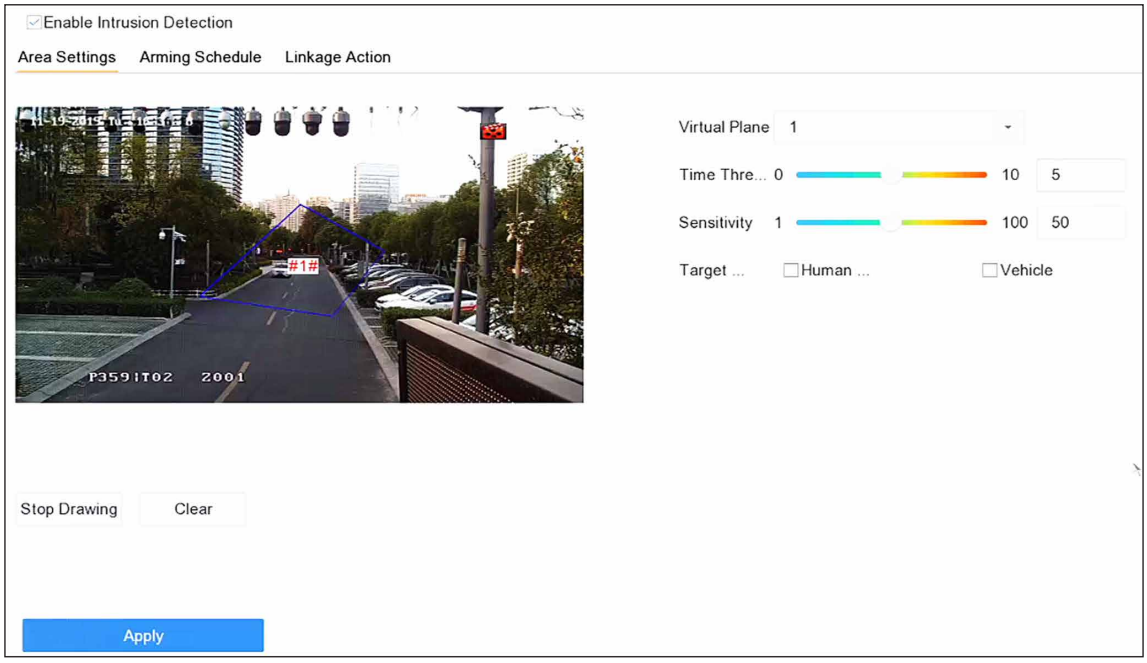

図 6-6 侵入検知

4. **Enable Intrusion 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、キャプチャーした侵入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）**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

   Sensitivity とは、アラームを作動させることができる物体の大きさです。Sensitivity 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画します。
7. オプション：ターゲットの最大サイズ / 最小サイズを描画します。

メモ

最大サイズから最小サイズまでのターゲットのみが侵入検知を作動します。

   1）**Max. Size/Min. Size** をクリックします。
   2) プレビューウィンドウに領域を描画します。
   3）**Stop Drawing** をクリックします。
8. オプション：**Detection Target** を **Human** または **Vehicle** に設定して、人体または車両によって作動しないアラームを削除します。
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** をクリックします。

6.2.7 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。**Smart Analysis → Smart Event Settings → Perimeter Protection**
2. カメラを選択します。
3. **Region Entrance Detection** をクリックします。

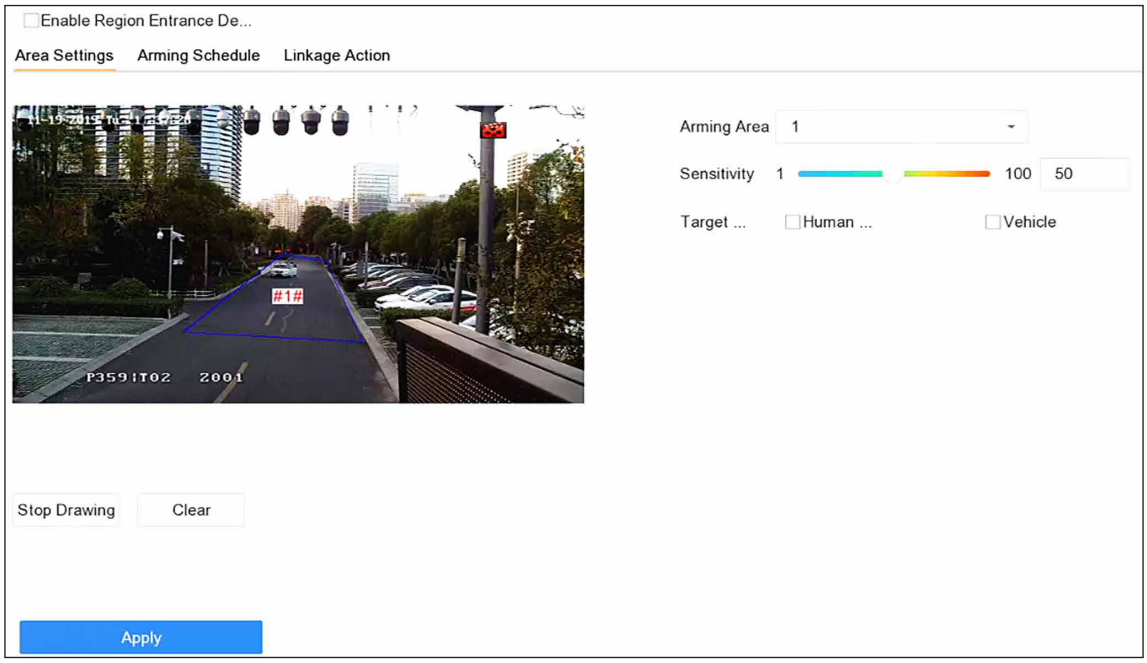

図 6-7 領域入口検知

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。

   メモ

   最大 4 つまで領域が選択できます。

   2）**Sensitivity** を設定します。

   Sensitivity

   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. オプション：ターゲットの最大サイズ / 最小サイズを描画します。ラインクロッシング検知が作動するのは、最大サイズから最小サイズまでのターゲットのみです。
   1）**Max. Size/Min. Size** をクリックします。
   2) プレビューウィンドウに領域を描画します。
   3）**Stop Drawing** をクリックします。
8. オプション：**Detection Target** を **Human** または **Vehicle** に設定して、人体または車両によって作動しないアラームを削除します。
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** をクリックします。

6.2.8 領域退去検知

領域退去検知は、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。**Smart Analysis → Smart Event Settings → Perimeter Protection**
2. カメラを選択します。
3. **Region Exiting** をクリックします。

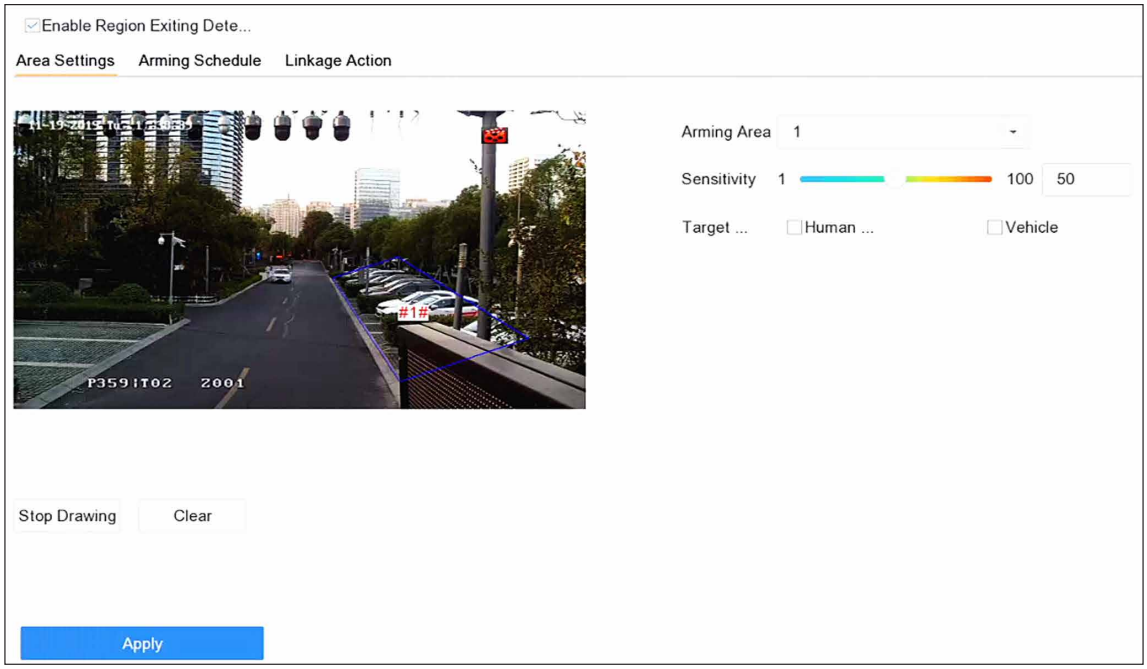

図 6-8 領域退去検知

4. **Enable Region Exiting Detection** にチェックを入れます。
5. オプション：**Save VCA Picture** をにチェックを入れると、キャプチャーされた領域退去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. オプション：ターゲットの最大サイズ / 最小サイズを描画します。ラインクロッシング検知が作動するのは、最大サイズから最小サイズまでのターゲットのみです。
   1）**Max. Size/Min. Size** をクリックします。
   2) プレビューウィンドウに領域を描画します。
   3）**Stop Drawing** をクリックします。
8. オプション：**Detection Target** を **Human** または **Vehicle** に設定して、人体または車両によって作動しないアラームを削除します。
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** をクリックします。

6.2.9 車両検知

道路交通モニタリングで利用できる車両検知は、多くが車両を検知し、同時にそのナンバープレートを捕捉します。

ステップ

1. 次の順に進みます。**Smart Analysis → Smart Event Settings → Vehicle Detection**
2. 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. **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。
7. **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。

8. 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。
9. 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。

6.2.10 マルチターゲットタイプ検知

マルチターゲットタイプの検知では、映像内の顔、人体、車両を同時に検知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 Event Settings → Video Structuralization**
2. カメラを選択します。
3. **Enable Multi-Target-Type Detection** にチェックを入ます。
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. 検知領域を設定します。
   1）**Draw Area** をクリックします。
   2）画像上の赤枠を調整し、検知領域を描画します。デフォルトはフルスクリーンになっています。
   3）**Stop Drawing** をクリックします。
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。

6.2.11 建物から投げ出された対象

この機能により、建物から物を投げる対象を識別し、本来の標的を特定することができます。

本機を使用する前に

お使いのカメラがこの機能をサポートしていることを確認してください。

ステップ

1. Web ブラウザー経由で次の順に進みます。**Configuration → VCA → Object Thrown from Building**
2. カメラを選択します。
3. **Enable Object Thrown from Building** にチェックを入れます。
4. **Area Settings** をクリック、次にルール領域を描画するため をクリックします。

メモ

1. をクリックして描画を開始、画面上で毎回左クリックで頂点決定、右クリックで描画を停止します。描画された多角形の内側が遮蔽領域となります。間違えてしまった場合は をクリックすると再描画できます。
2. 画面内の建物の外形に合わせて検知領域を描くことをお勧めします。

5. **Rule Name** を入力します。デフォルトの名前は、rule 1 です。
6. 検知パラメータを設定します。

Sensitivity

明らかに建物から投げ出されたものでないことを確認し、フィルタリングするために使用します。数値が高いほど誤アラームの可能性が高くなります。初期値として 50 を推奨します。

Detection Confidence

検知領域内の不審物を検出する際に使用します。値が小さいほど、映像中の対象を検知しやすく、判定もしやすくなります。初期値として 50 を推奨します。

Target Confidence

建物から投げられた対象が本物かどうかを判断するために使用します。値が小さいほど、映像内で検知された対象が建物から投げられたものと判断されやすくなり、誤アラームの可能性が高くなります。初期値として 50 を推奨します。

メモ

最初はデフォルト値を推奨します。動作中に誤アラームが頻発する場合は、調整が可能です。ターゲット信頼度は最初に調整し、音声検出結果が提供されない場合は検知信頼度を後で調整することを推奨します。それでも明らかな効果がない場合は、sensitivity を調整してください。

7. **Save** をクリックします。
8. **Arming Schedule** をクリックします。**アーミングスケジュールの設定**を参照してください。

9. **Linkage Method** をクリックします。**リンケージアクションの設定**を参照してください。
10. **Shield Region** を設定します。
    1）**Shield Region** をクリックします。
    2）領域を描画します。

メモ

1. 画面の一部（検出エリア内または外）に、検知する必要のない部分（光が時々飛ぶ、葉っぱがよく流れて誤報を誘発する、など）がある場合、シールド領域として描画することが可能です。
2. をクリックして描画を開始、画面上で毎回左クリックで頂点決定、右クリックで描画を停止します。描画された多角形の内側が遮蔽領域となります。間違えてしまった場合は をクリックして再描画を行います。
3. 8 つのシールドリージョンに対応しています。

11. **Save** をクリックします。

6.2.12 ロイタリング検知

ロイタリング検知は、ターゲットが設定された時間以上、指定されたエリア内に滞在しているかどうかを検知し、連動してアラームを作動するために使用されます。

ステップ

1. 次の順に進みます。**Smart Analysis → Smart Event Settings → Other Events**
2. カメラを選択します。
3. **Loitering Detection** をクリックします。

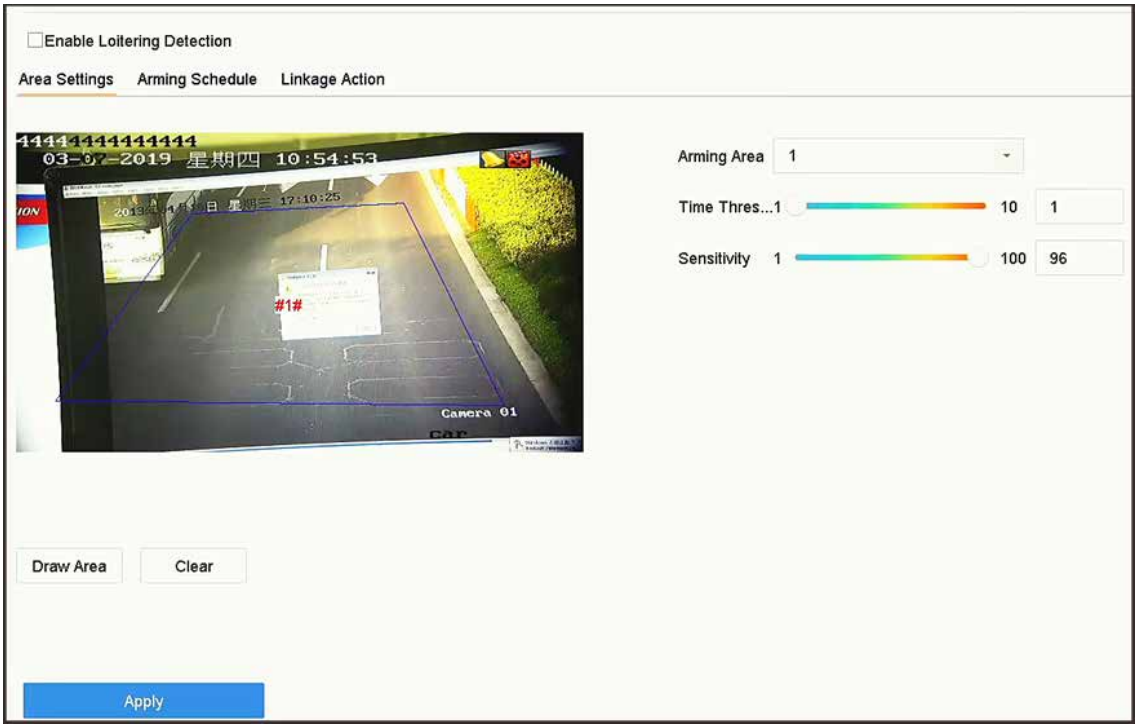

図 6-9 ロイタリング検知

4. **Enable Loitering 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、キャプチャーしたロイタリング検知画像を保存します。
6. ロイタリング検知パラメータを設定します。
   1）**Arming Area** を選択します。

   メモ

   最大 4 つまでエリアの選択が可能です。

   2）**Time Threshold** 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 10 秒間領域内に留まった後、アラームを作動します。時間の範囲は [1-10] です。

   3）**Sensitivity** を設定します。

   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。
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。

6.2.13 人の密度検知

人の密度検知は、指定したエリア内の人の密度が設定値を超えているかどうかを検知し、アラームを作動させて連動したアクションを行うものです。

ステップ

1. 次の順に進みます。**Smart Analysis → Smart Event Settings → Other Events**
2. カメラを選択します。
3. **People Gathering** をクリックします。

図 6-10 人の密度検知

4. **Enable People Gathering 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 People gathering 検知画像を保存します。
6. People gathering 検知のパラメータを設定します。
   1）**Arming Area** を選択します。

   メモ

   最大 4 つまでエリアの選択が可能です。

   2）**Draw Area** をクリックし領域の 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。
   3）**Percentage** を設定します。

   Percentage

   エリア内の人の密度しきい値を超えると、本機はアラームを作動します。

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。

6.2.14 高速移動検知

高速移動検知は、不審な走行や追跡、オーバースピード、高速移動の検知に使用されます。これは、対象が高速で移動しているときにアラームを作動し、必要なアクションを事前に取ることができるように、アーミングホストに通知を送信します。

ステップ

1. 次の順に進みます。**Smart Analysis → Smart Event Settings → Other Events**
2. カメラを選択します。
3. **Fast Moving** をクリックします。

図 6-11 高速移動検知

4. **Enable Fast Moving** 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、キャプチャーした高速移動検知画像を保存します。
6. 高速移動検知パラメータを設定します。
   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）**Draw Area** をクリックし領域の 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。
   3）**Sensitivity** を設定します。

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。

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。

6.2.15 パーキング検知

パーキング検知は、高速道路や一方通行の道路、指定した領域での駐車違反を検知するために使用されます。

ステップ

1. 次の順に進みます。**Smart Analysis → Smart Event Settings → Other Events**
2. カメラを選択します。
3. **Parking** をクリックします。

図 6-12 パーキング検知

4. **Enable Parking 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、キャプチャーしたパーキング検知画像を保存します。
6. パーキング検知のパラメータを設定します。
   1）**Arming Area** を選択します。

メモ

最大 4 つまでエリアの選択が可能です。

2）**Time Threshold** を設定します。

Time Threshold

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

3）**Sensitivity** を設定します。

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。

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。

6.2.16 不審手荷物の検知

不審手荷物の検知は、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。**Smart Analysis → Smart Event Settings → Other Events**
2. カメラを選択します。
3. **Unattended Baggage** をクリックします。

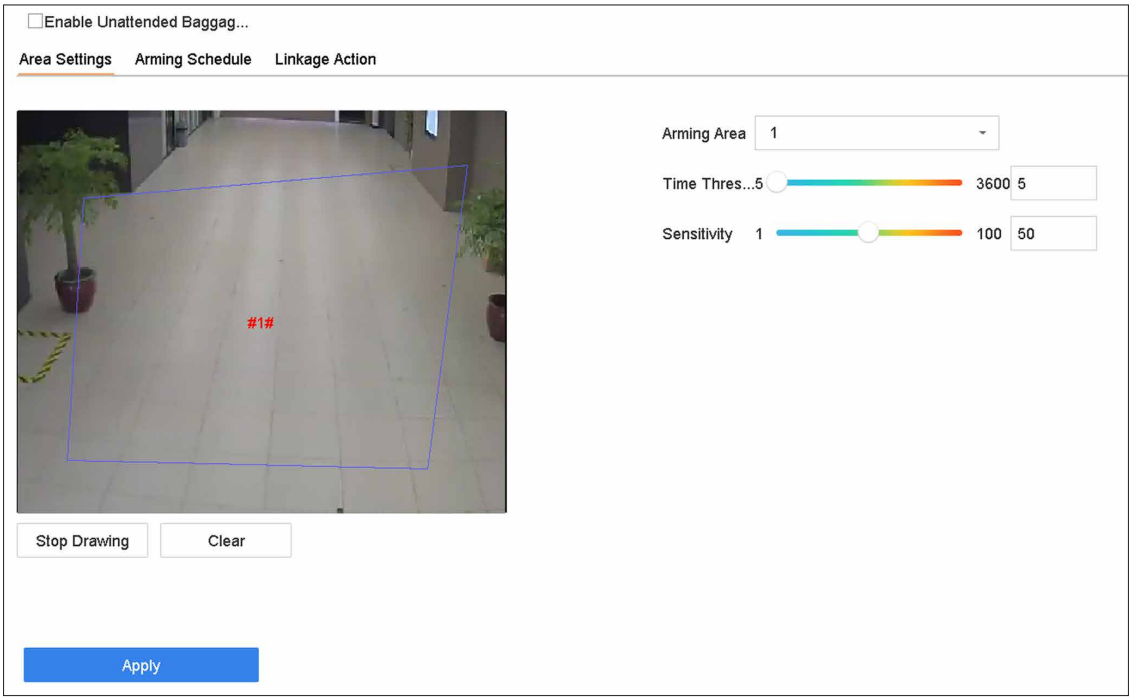

図 6-13 不審手荷物の検知

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、キャプチャーした不審手荷物の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 Area** を選択します。

   メモ

   最大 4 つまでエリアの選択が可能です。

   2) マウスをドラッグして **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 秒間放置された後、アラームが作動します。時間の範囲は [5-20] 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。

6.2.17 対象物持ち出し検知

対象物持ち出し検知機能は、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。**Smart Analysis → Smart Event Settings → Other Events**
2. カメラを選択します。
3. **Object Removable** をクリックします。

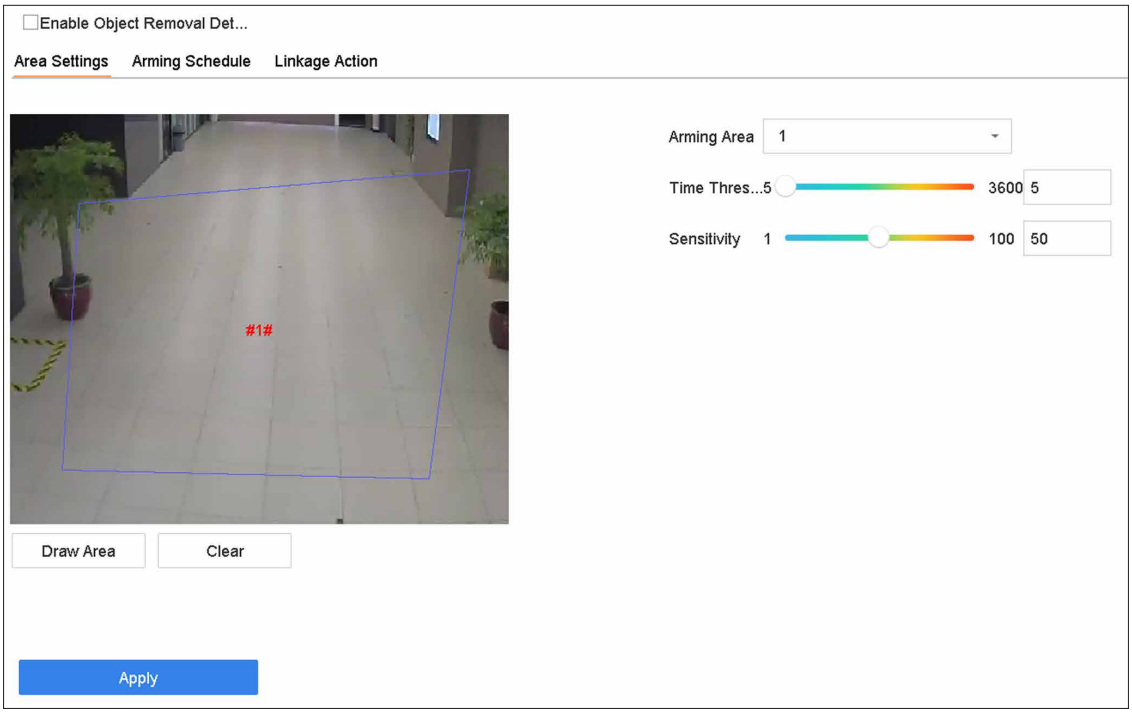

図 6-14 対象物持ち出し検知

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、キャプチャーした対象物持ち出し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 Area** を選択します。

   メモ

   最大 4 つまでエリアの選択が可能です。

   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。時間の範囲は [5-20] です。

   Sensitivity

   背景画像の類似度です。感度が高ければ、その領域から取り出した非常に小さな物体でも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。

6.2.18 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。**Smart Analysis → Smart Event Settings → Other Events**
2. カメラを選択します。
3. **Audio Exception** をクリックします。

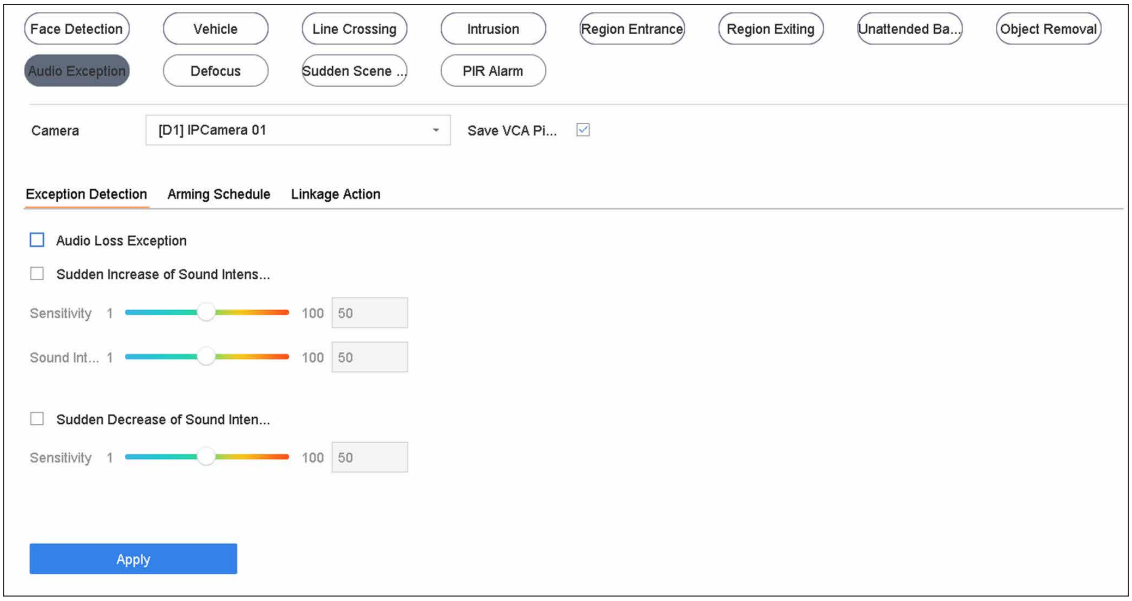

図 6-15 音声異常検知

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。急激な音の立ち上がりに対応するため **Sensitivity** と **Sound Intensity Threshold** を設定します。

   Sensitivity

   値が小さいほど、その変化をより厳格に検知します。検知の範囲は [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。音の範囲は [1-100] です。

   Sudden Decrease of Sound Intensity Detection

   監視シーンで急な音の落ち込みを検知します。検知感度の範囲は [1-100] です。

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。

6.2.19 デフォーカス検知

レンズデフォーカスによる画像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。**Smart Analysis → Smart Event Settings → Other Events**
2. カメラを選択します。
3. **Defocus** をクリックします。

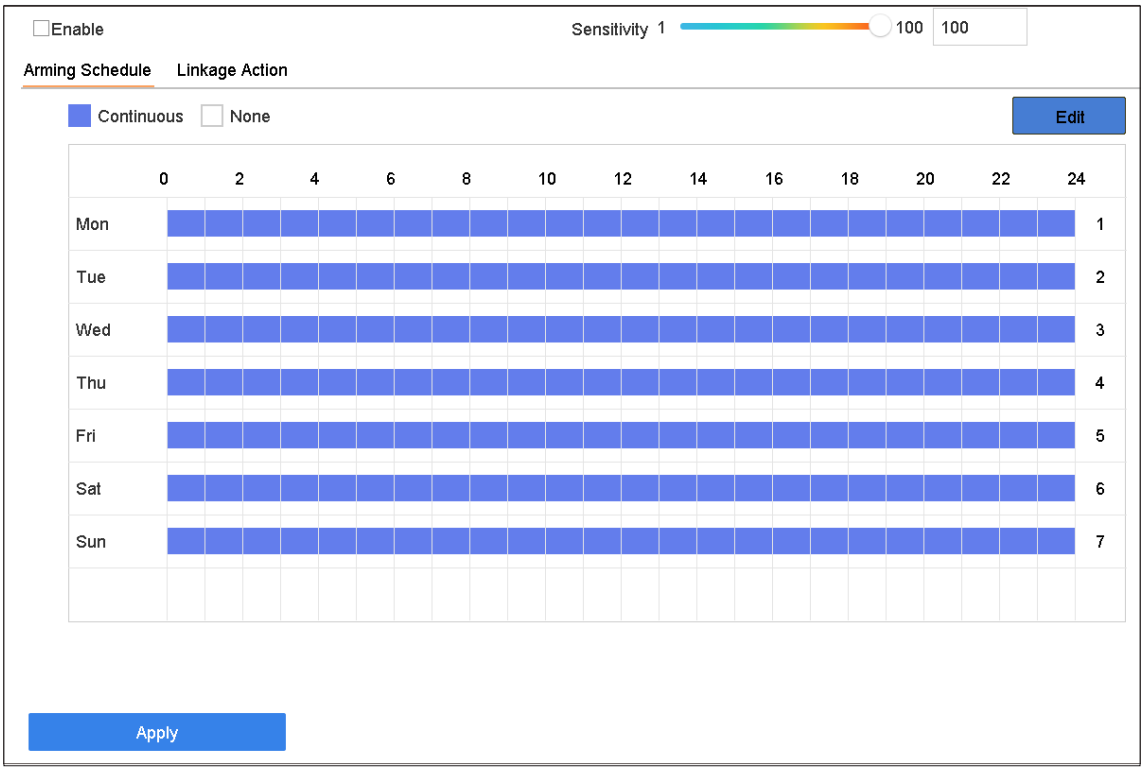

図 6-16 デフォーカス検知

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. 検知感度を設定します。

   Sensitivity

   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。

6.2.20 突然の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。**Smart Analysis → Smart Event Settings → Other Events**
2. カメラを選択します。
3. **Sudden Scene Change** をクリックします。

図 6-17 突然のシーンチェンジ検知

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然のシーンチェンジ検知の画像を保存します。
6. 検出感度を設定します。

   Sensitivity

   1 ～ 100 の範囲で設定でき、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。

6.2.21 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。**Smart Analysis → Smart Event Settings → Other Events**
2. カメラを選択します。
3. **PIR Alarm** をクリックします。

図 6-18 PIR アラーム

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。

6.2.22 サーマルカメラ検知

NVR は、サーマルネットワークカメラのイベント検知モード（火災・煙検知、温度検知、温度差検知など）をサポートします。

本機を使用する前に

サーマルネットワークカメラを本機に追加し、カメラが起動していることを確認します。

ステップ

1. 次の順に進みます。**Smart Analysis → Smart Event Settings → Other Events**
2. サーマルカメラを選択します。
3. オプション：**Save VCA Picture** にチェックを入れると、キャプチャーした検知画像を保存します。
4. イベント検知（Temperature Measurement Alarm など）を選択します。
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。

6.2.23 キューマネージメント

キューマネージメントカメラと接続後、キューマネージメントのアーミングスケジュールとリンケージアクションを設定することができます。

本機を使用する前に

本機がキューマネージメントカメラに接続されていることを確認します。

ステップ

1. 次の順に進みます。**Smart Analysis → Smart Event Settings → Other Events**
2. キューマネージメントカメラを選択します。
3. オプション：**Save VCA Picture** にチェックを入れると、キャプチャーした検知画像を保存します。
4. アーミングスケジュールを設定します。詳しくは**アーミングスケジュールの設定**を参照してください。
5. リンケージアクションを設定します。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。
6. **Apply** をクリックします。

6.3 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

1. 建物からの投下物を検知するため、スマート検知 がチェックされていることを確認してください。ターゲットが特定されると、左側に検知された画面が表示されます。一方、ボックスには検知された対象が表示されます。(不審なターゲットがある場合、放物線は緑色に変化します。リアルターゲットがあり、アラームが作動した場合、放物線は赤色になります。)
2. 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. をクリックして、アラーム設定を行います。
   1) IP カメラと IoT チャンネルを選択し、アクセスコントロールイベントの表示設定を完了します。

      Display Pop-Up

      この機能を有効にすると、アラームが作動したときに、人のタイプ情報、体温、マスク装着状態（オプション）を含むポップアップが表示されます。

      Mask Not Wearing Event

      検知したターゲットの摂氏、華氏などの温度単位を設定することができます。この機能を有効にすると、ターゲットがマスクを着用していない場合、ポップアップが黄色で表示されます。一方、ターゲットが異常な体温を持っている場合、ポップアップが赤くなります。
4. 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。

6.4 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。

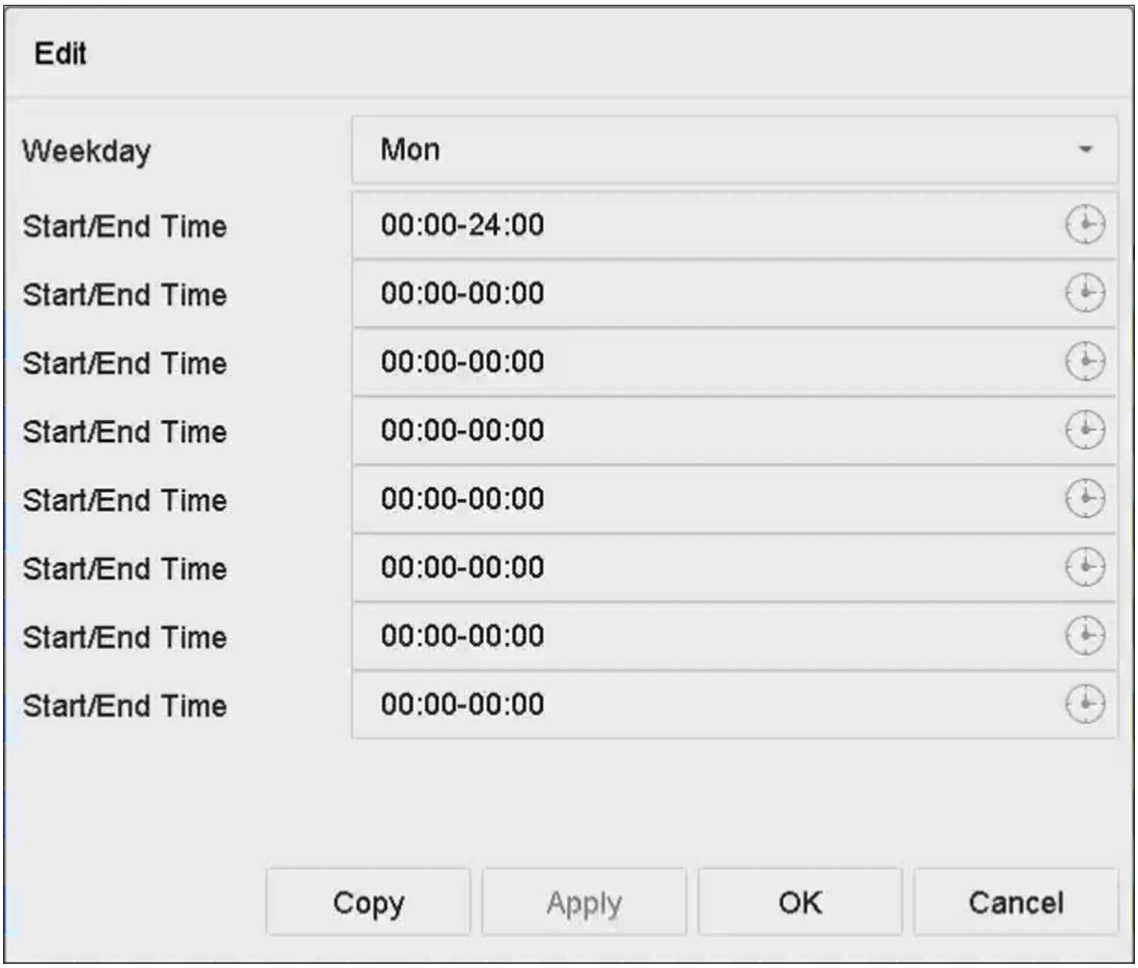

図 6-19 アーミングスケジュールの設定

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。

6.5 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。

6.5.1 フルスクリーンモニタリング自動切替えを設定する

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

   イベント動画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）を選択します。

6.5.2 ブザーを設定する

アラームを検知すると、ブザーがビープ音を発生します。

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。

6.5.3 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（Guarding Vision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。

6.5.4 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。

6.5.5 オーディオアラートを設定する

アラームが発生すると、リンケージアクションとして音声ファイルが再生されます。オーディオファイルはカスタマイズすることができます。詳しくは**オーディオの管理**を参照してください。

本機を使用する前に

オーディオファイルが本機にインポートされていることを確認してください。

ステップ

メモ

このリンケージアクションは、特定のイベントでのみ利用可能です。

1. **Normal Linkage** の **Audio Alert** にチェックを入れます。
2. をクリックして、オーディオファイルを選択します。
3. オーディオファイルを選択します。
4. アーミングスケジュールを設定します。
5. **OK** ボタンをクリックします。
6. **Apply** をクリックします。

6.5.6 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** インターフェースに進んでください。（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** 領域で、作動するアラーム出力を選択します。
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。

メモ

本機にアラーム出力が 8 個ある場合、Ctrl 12V 電源はアラーム出力 9 で制御されます。プラス極を Ctrl 12V の A に、マイナス極を Ctrl 12V の B に接続します。アラーム出力が作動すると、電源が入ります。

6.5.7 オーディオとライトアラームリンケージを設定する

一部のネットワークカメラでは、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。

本機を使用する前に

- 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. 希望する **Audio and Light Alarm Linkage** を設定してください。
3. **Apply** をクリックします。

6.5.8 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。

本機を使用する前に

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。

第 7 章 IoT

IoT（モノのインターネット）機能により、本機とアクセス制御や警報デバイスなどの IoT 機器との接続を構築することができます。本機は、接続された IoT 機器からのアラームを受信します。IoT アラーム発生時に、録画や全画面監視を作動するなどのリンケージアクションを設定することができます。

7.1 IoT デバイスの追加

メモ

IoT チャンネルの最大数は、本機の最大ネットワークカメラ数の半分です。

7.1.1 アクセス制御デバイスを追加する

アラームを受信するために、Hikvision アラームホストとビデオインターカムデバイスを追加します。アラーム発生時の録画や全画面監視の作動などのリンケージアクションを設定することができます。

本機を使用する前に

アクセス制御デバイスを設置します。アクセス制御デバイスと本機の間のネットワーク通信が良好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。**Business Application → IoT → Access Control → Device Management**
2. **Add** をクリックします。

図 7-1 アクセス制御

3. アクセス制御デバイス情報を入力します。**Device IP**、**Port**、**Transfer Protocol**、**User Name**、**Password** は、アクセス制御デバイスと同じである必要があります。
4. オプション：希望する **Enable IoT Time Sync** にチェックを入れます。

メモ

すべての IoT チャンネルをショートカットで有効 / 無効にすることができます。

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

Time Sync Configuration をクリックして、**Enable IoT Time Sync** または **Disable IoT Time Sync** を選択し、すべての IoT チャンネルのスケジュール時刻同期を有効 / 無効にします。

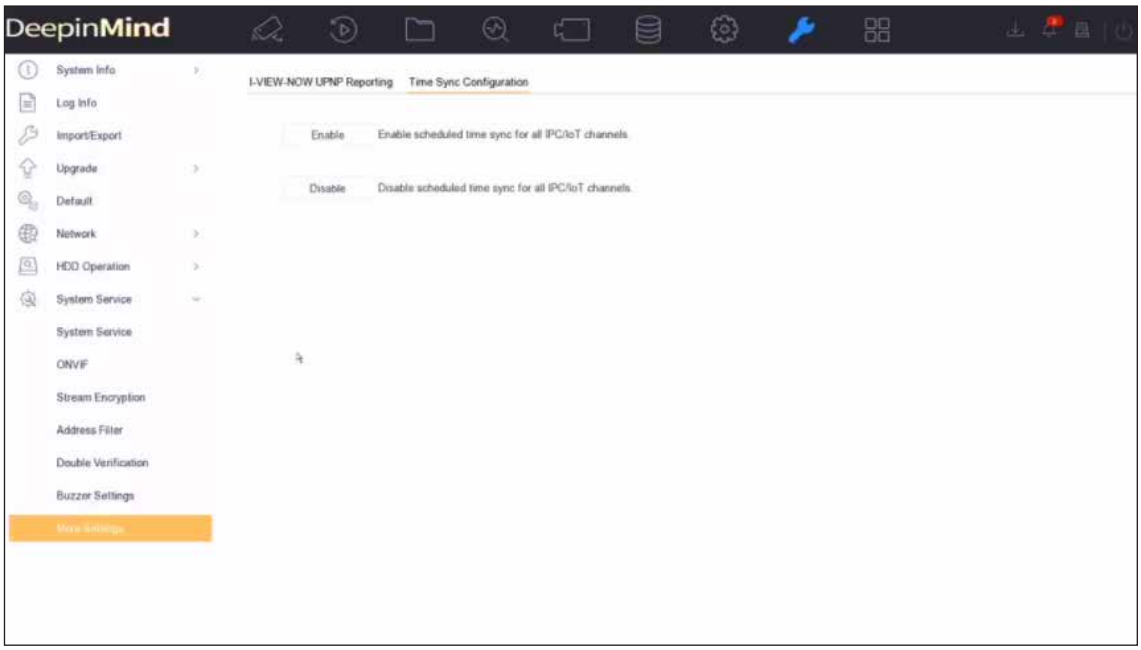

図 7-2 IoT 時刻同期

この機能は、管理者ユーザーだけが使用できます。

5. **Add** をクリックします。

7.1.2 アラームデバイスを追加する

アラームを受信する様々のメーカーのアラームデバイスを追加します。アラーム発生時の録画や全画面監視の作動などのリンケージアクションを設定することができます。

本機を使用する前に

アラームデバイスを設置します。アラームデバイスと本機の間のネットワーク通信が良好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。**Business Application → IoT → Alarm → Device Management**
2. **Add** をクリックします。

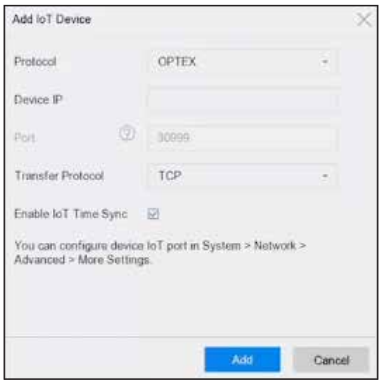

図 7-3 アラームデバイス

3. アクセス制御デバイス情報を入力します。追加するアラームデバイスと同じ情報である必要があります。
4. オプション：希望する **Enable IoT Time Sync** にチェックを入れます。

メモ

すべての IoT チャンネルをショートカットで有効 / 無効にすることができます。

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

Time Sync Configuration をクリックして、**Enable IoT Time Sync** または **Disable IoT Time Sync** を選択し、すべての IoT チャンネルのスケジュール時刻同期を有効 / 無効にします。

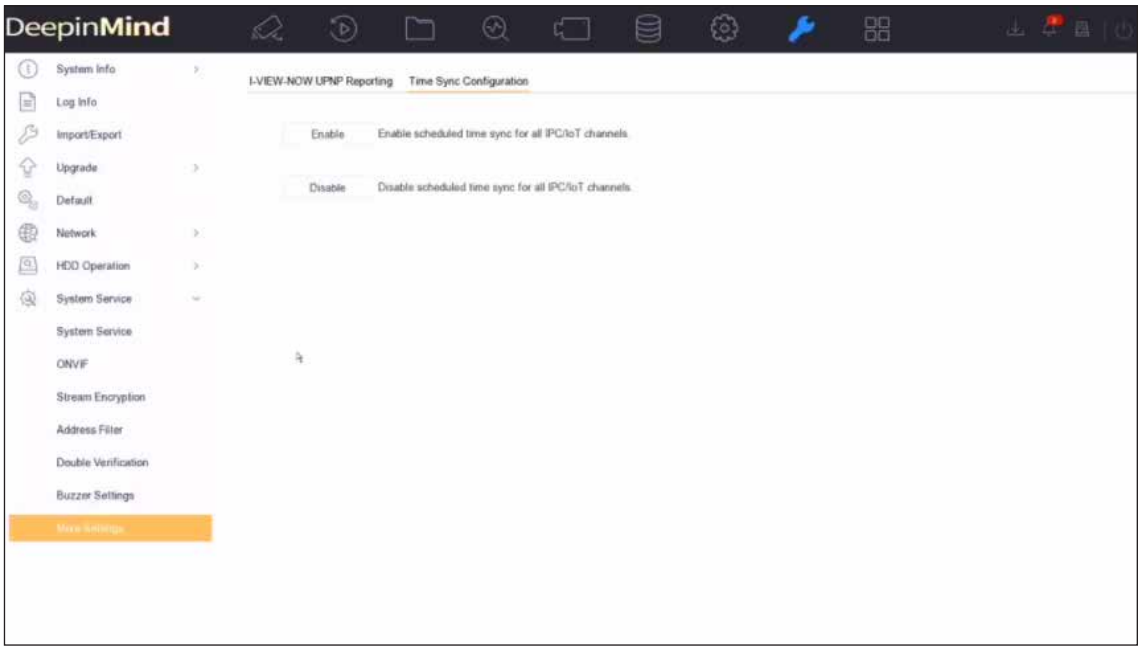

図 7-4 IoT 時刻同期

この機能は、管理者ユーザーだけが使用できます。

5. **Add** をクリックします。

7.2 リンケージアクションとアーミングスケジュールの設定

アクセス制御またはアラームデバイスのリンケージアクションとアーミングスケジュールを設定します。指定されたアラームが発生すると、リンケージアクションが作動します。

ステップ

1. 追加された IoT デバイスの をクリックします。

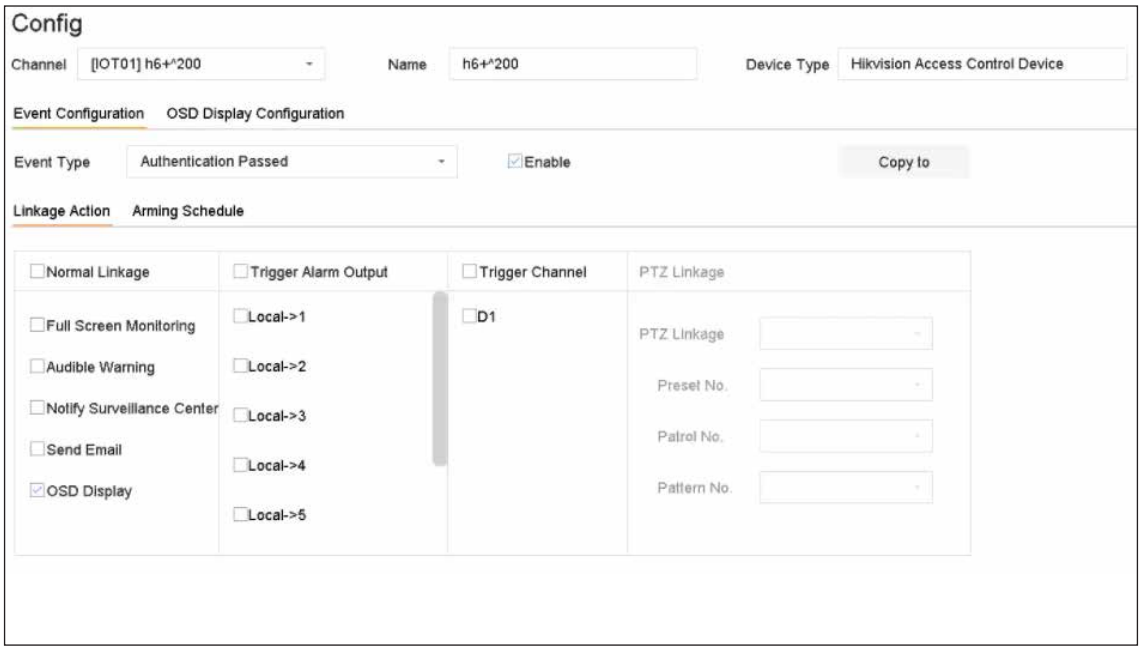

図 7-5 IoT の設定

2. **Event Type** を選択します。以下の設定は、選択したイベントタイプに対してのみ有効です。
3. **Enable** にチェックを入れます。
4. 希望するリンケージアクションにチェックを入れてください。詳細な手順については、**リンケージアクションの設定**を参照してください。

メモ

Full Screen Monitoring と **OSD Display** は選択された **Trigger Channel** のみ有効です。

5. **Arming Schedule** をクリックします。
6. アーミングスケジュールを設定します。詳細な手順については、**アーミングスケジュールの設定**を参照してください。リンケージアクションは、設定されたスケジュールの間のみ有効です。
7. **Apply** をクリックします。

7.3 OSD の設定

IoT デバイスから受信したアラーム情報をライブビュー画像に表示することができます。

ステップ

1. 追加された IoT デバイスの をクリックします。
2. イベント設定インターフェースの **OSD Display** にチェックを入れてください。
3. **Trigger Channel** を選択してください。
4. **OSD Display Configuration** をクリックしてください。

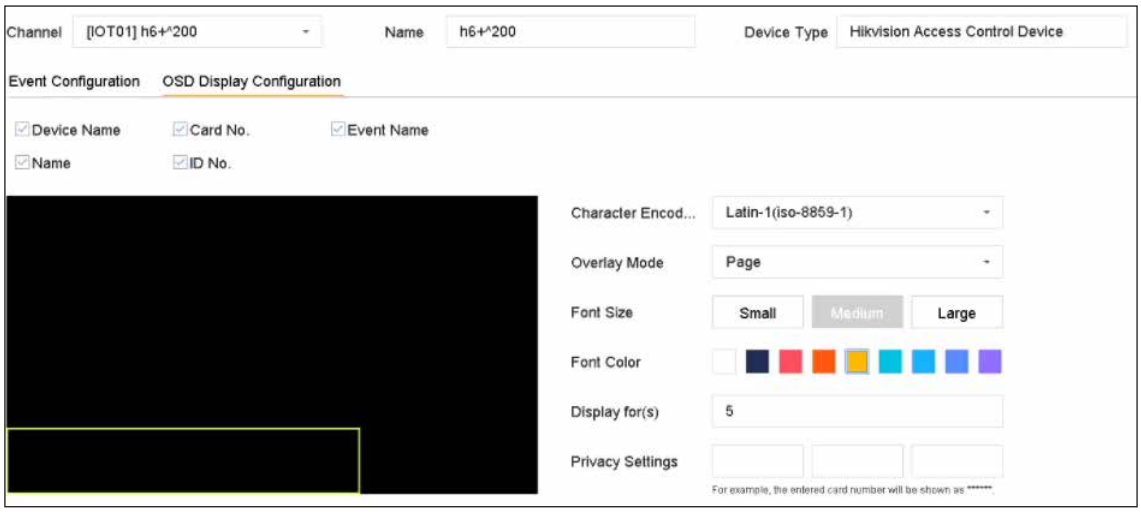

図 7-6 OSD の設定

5. ライブビュー画像に表示する **Device Name**、**Card No.**、**Event Name**、**Name**、**ID No.** などの項目を選択します。この項目は、アクセス制御デバイスのみです。
6. OSD のプロパティを設定します。

   Overlay Mode - Scroll

   この OSD は自動的にスクロールし、新しいアラーム情報を表示します。

   Overlay Mode - Page

   現在の OSD がアラーム情報を表示しきれない場合、自動的に新しいページに切り替わります。

   Privacy Settings

   隠したいプライバシー情報を入力します。隠されたプライバシー情報は、* に置き換えられます。個人情報には **Event**、**Device**、**Card**、**Name**、**ID** が含まれます。
7. IoT OSD のサイズと位置を調整するために、プレビューウィンドウの黄色い枠の四角形を調整してください。
8. **Apply** をクリックします。

7.4 IoT レコードの検索

アラームを時間別、イベントタイプ別、チャンネル別で検索できます。

ステップ

1. イベントレコードインターフェースに進みます。
   - アクセス制御：次の順に進みます。**Business Application → IoT → Access Control → Card Swiping Record**
   - アラームデバイス：次の順に進みます。**Business Application → IoT → Alarm → Search Data**

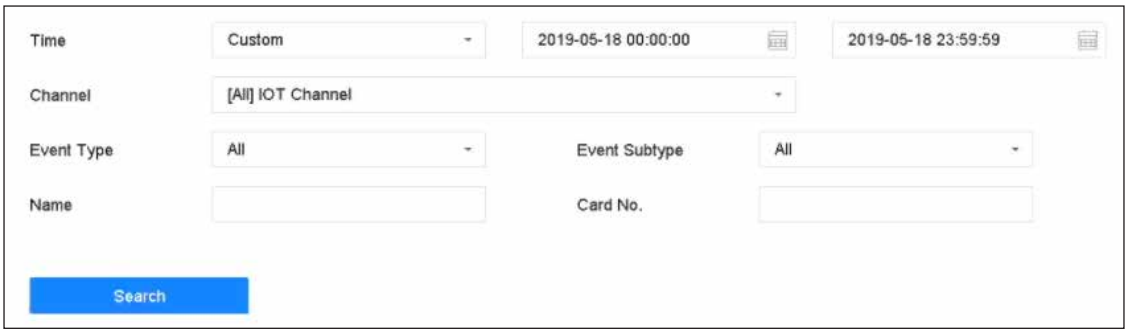

図 7-7 イベントレコードの検索（アクセス制御）

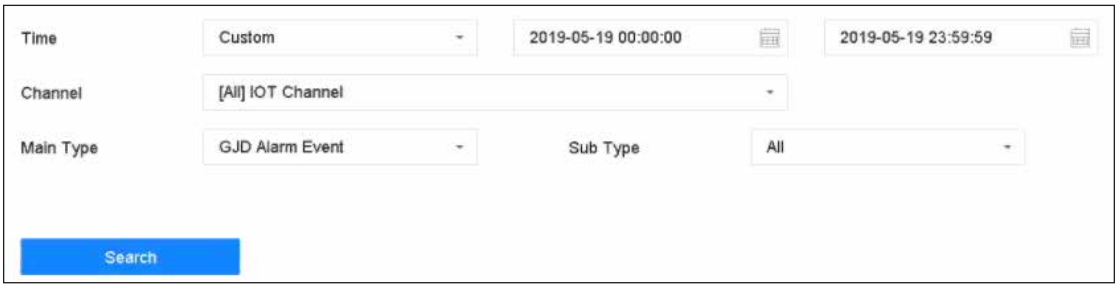

図 7-8 イベントレコードの検索（アラームデバイス）

2. 検索条件を指定します。

メモ

Name/Card No.：カードスワイプイベントが起こると、アクセス制御デバイスはビデオ記録にカード名とカード番号をアップロードします。カード名やカード番号からイベントを検索することができます。

3. **Search** をクリックします。

No.	Event Type	Name	Card No.	Card Type	Time	Event Source	View
1	Time Sync. Event				05-18-2019 14:04:39	IOT01	
2	Time Sync. Event				05-18-2019 14:05:39	IOT01	
3	Time Sync. Event				05-18-2019 14:06:39	IOT01	
4	Time Sync. Event				05-18-2019 14:07:39	IOT01	
5	Time Sync. Event				05-18-2019 14:08:39	IOT01	
6	Time Sync. Event				05-18-2019 14:09:35	IOT01	
7	Time Sync. Event				05-18-2019 14:09:40	IOT01	
8	Time Sync. Event				05-18-2019 14:10:39	IOT01	
9	Time Sync. Event				05-18-2019 14:11:40	IOT01	
10	Time Sync. Event				05-18-2019 14:12:40	IOT01	
11	Time Sync. Event				05-18-2019 14:13:39	IOT01	
12	Time Sync. Event				05-18-2019 14:14:40	IOT01	
13	Time Sync. Event				05-18-2019 14:14:41	IOT01	
14	Time Sync. Event				05-18-2019 14:15:40	IOT01	
15	Time Sync. Event				05-18-2019 14:16:40	IOT01	
16	Time Sync. Event				05-18-2019 14:17:40	IOT01	
17	Time Sync. Event				05-18-2019 14:18:40	IOT01	
18	Time Sync. Event				05-18-2019 14:19:40	IOT01	
19	Time Sync. Event				05-18-2019 14:19:46	IOT01	
20	Time Sync. Event				05-18-2019 14:20:40	IOT01	

Total: 22 P: 1/1 Go

図 7-9 検索結果 (アクセス制御)

No.	Channel	Time	Main Type	Sub Type	Status	Data	View
1	IOT03	05-18-2019 14:49:56	GJD Alarm Event	PIR Detection alarm			

図 7-10 検索結果（アラームデバイス）

7.5 IoT ビデオ / ピクチャー

選択したトリガーチャンネルのイベント録画またはキャプチャーのスケジュールを設定すると、IoT アラームが発生したときにチャンネルは自動的にビデオ録画または画像キャプチャーを行います。

7.5.1 イベント録画 / イベントキャプチャを設定する

本機は、IoT のアラーム発生時に動画を録画したり、画像をキャプチャーしたりすることができます。

ステップ

1. 追加された IoT デバイスの をクリックします。
2. 希望する **Event Type** を選択します。
3. **Enable** にチェックを入れます。
4. アラーム発生地、イベントを動画録画または画像キャプチャーをするには **Trigger Channel** にチェックを入れます。

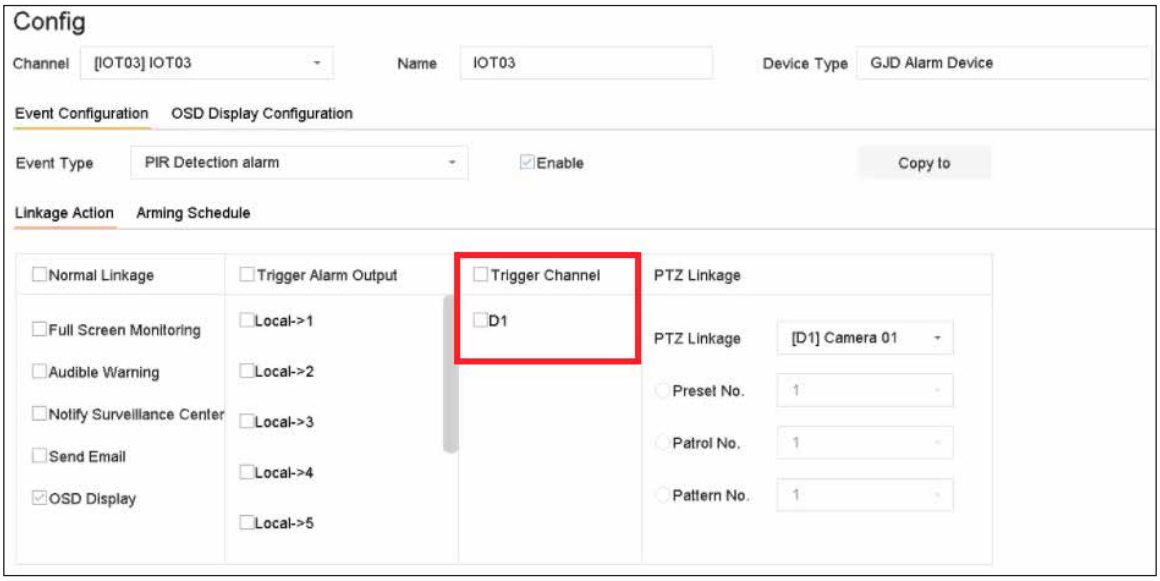

図 7-11 トリガーチャンネル

5. **Apply** をクリックします。
6. イベントの録画または画像キャプチャーのスケジュールを設定します。ここでは、イベントレコーディングの設定を例に、その手順を説明します。
   1）次の順に進みます。**Storage → Schedule → Record**
   2）**Camera No.** を選択して **Enable Schedule** にチェックを入れます。カメラは、手順 4 で選択したカメラである必要があります。
   3) 録画の種類は **Event** を選択します。
   4) 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。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。
   5) **OK** ボタンをクリックしてください。

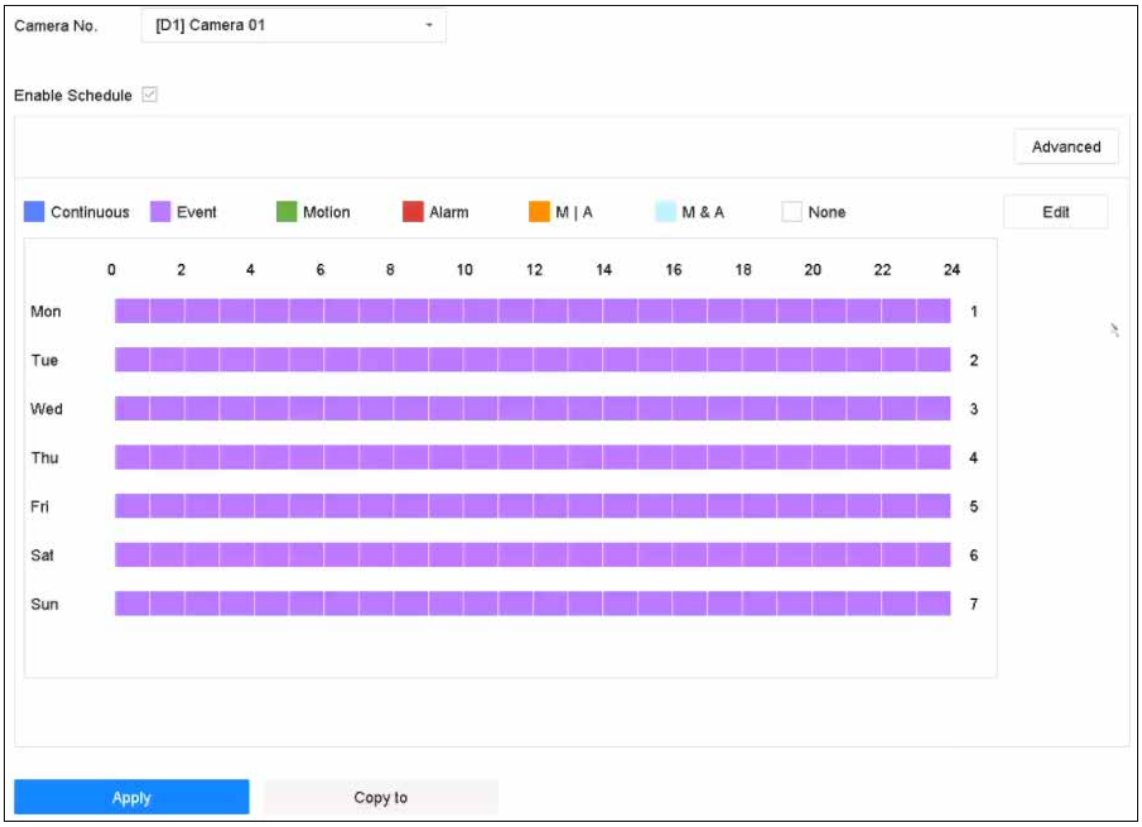

図 7-12 イベント録画

結果

アラームが発生すると、選択したトリガーチャンネルがイベント録画を開始します。

7.5.2 IoT 動画を検索する

IoT イベントトリガー動画を検索します。

ステップ

1. 次の順に進みます。**File Management → Video → Search by Event**

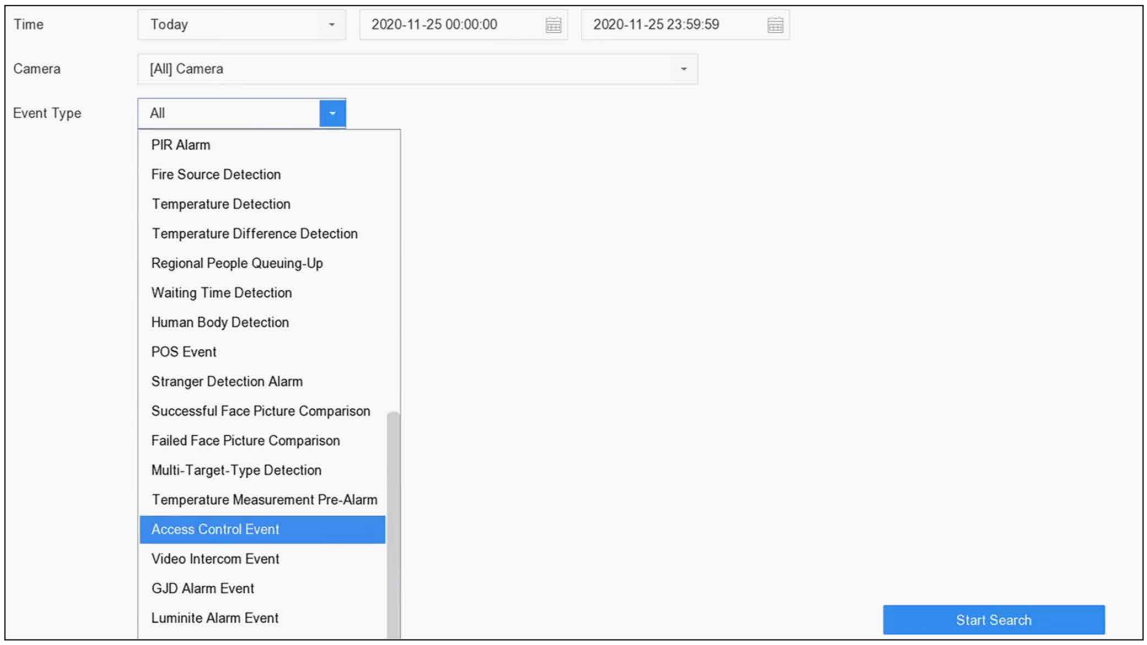

図 7-13 イベント動画検索

2. 検索条件を設定します。

Camera

IoT リンケージアクション設定の選択されたトリガーチャンネルとして選択します。

Event Type

希望する IoT イベントを選択します。

3. **Start Search** をクリックします。

第 8 章 スマートレポート

8.1 人数カウント

人数カウントは、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. 次の順に進みます。**Smart Analysis → Smart Report → Counting**
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。

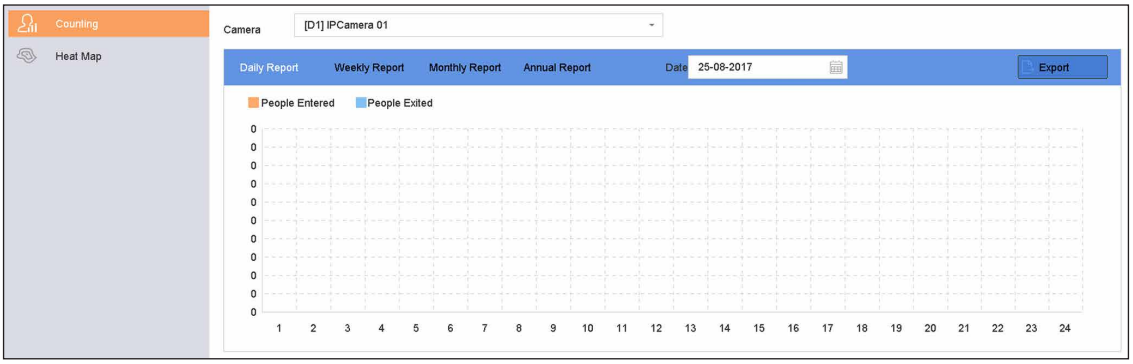

図 8-1 人数カウント

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。

8.2 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。

本機を使用する前に

接続された IP カメラがこの機能に対応しており、対応するパラメータが設定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。**Smart Analysis → Smart Report → 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。

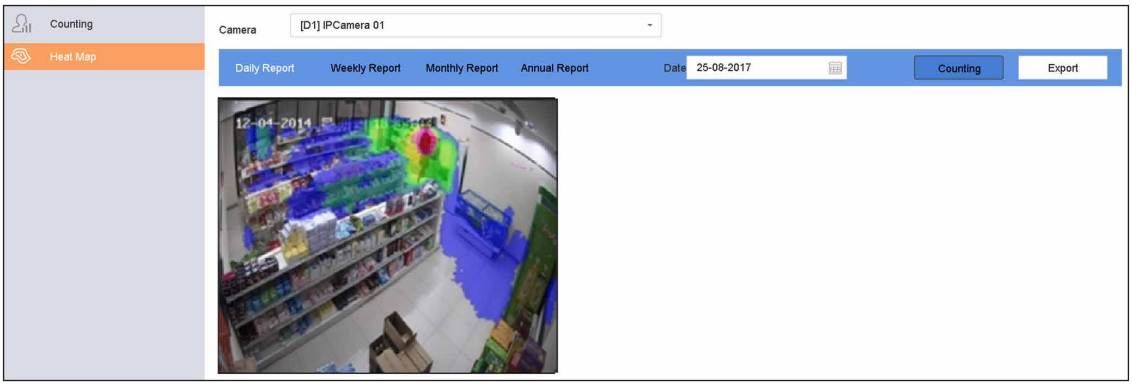

図 8-2 ヒートマップ

5. **Counting** をクリックします。

メモ

上図のように、赤のカラーブロック（255, 0, 0）は人の往来の多いエリア、青のカラーブロック（0, 0, 255）は人の往来の少ないエリアを表しています。

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。

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 9 章 ファイル管理

9.1 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 → Video** または **File Management → Picture**
2. 検索方法を選択します。例：**Search by Appearance** または **Search by Event** で検索します。
3. 時間やカメラなど、細かい条件を指定します。
4. **Start Search** をクリックします。
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. オプション： または をクリックしてビューモードを切り替えます。
7. オプション： または を別のビューモードでクリックすると動画をロックします。ロックされた動画は上書きされません。
8. 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）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。

9.2 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 にエクスポートすることができます。

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** を選択して **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。

9.3 クイックバックアップ

すべての動画をショートカットでバックアップできます。

ステップ

1. 次の順に進みます。**File Management → Video**
2. アピアランス、イベント、タグなどの条件を指定して、動画を検索することができます。
3. **Quick Backup** をクリックします。

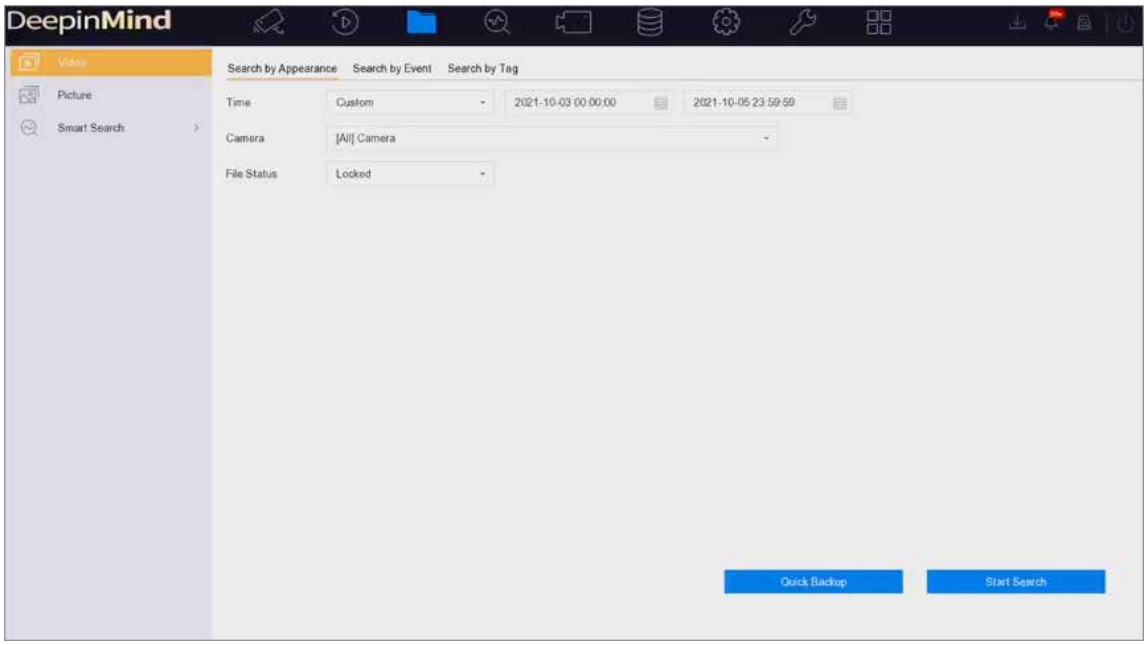

図 9-1 クイックバックアップ

9.4 スマートサーチ

9.4.1 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。**File Management → Smart Search → Face → 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を表示します。

次は

検索結果の表示を参照してください。

Search by Appearance

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。**File Management → Smart Search → Face → 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、お好みの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を表示します。

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。
- **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。

9.4.2 ヒト検索

人体検知アラームで画像を検索します。

ステップ

1. 次の順に進みます。**File Management → Smart Search → Human → 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 **Human Body Alarm** 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を表示します。
7. 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）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。

9.4.3 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。**File Management → Smart Search → Vehicle**
2. 検索方法を選択します。例：**Search by Appearance** または **Search by Event** で検索します。
3. 車両検索用の IP カメラを選択します。
4. 検索条件を設定します。
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を表示します。
7. 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。

第 10 章 ストレージ

10.1 ストレージデバイスの管理

10.1.1 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。

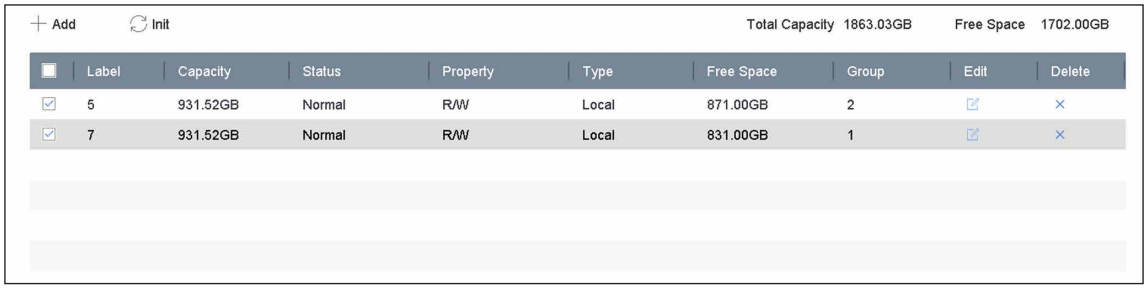

図 10-1 ストレージデバイス

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

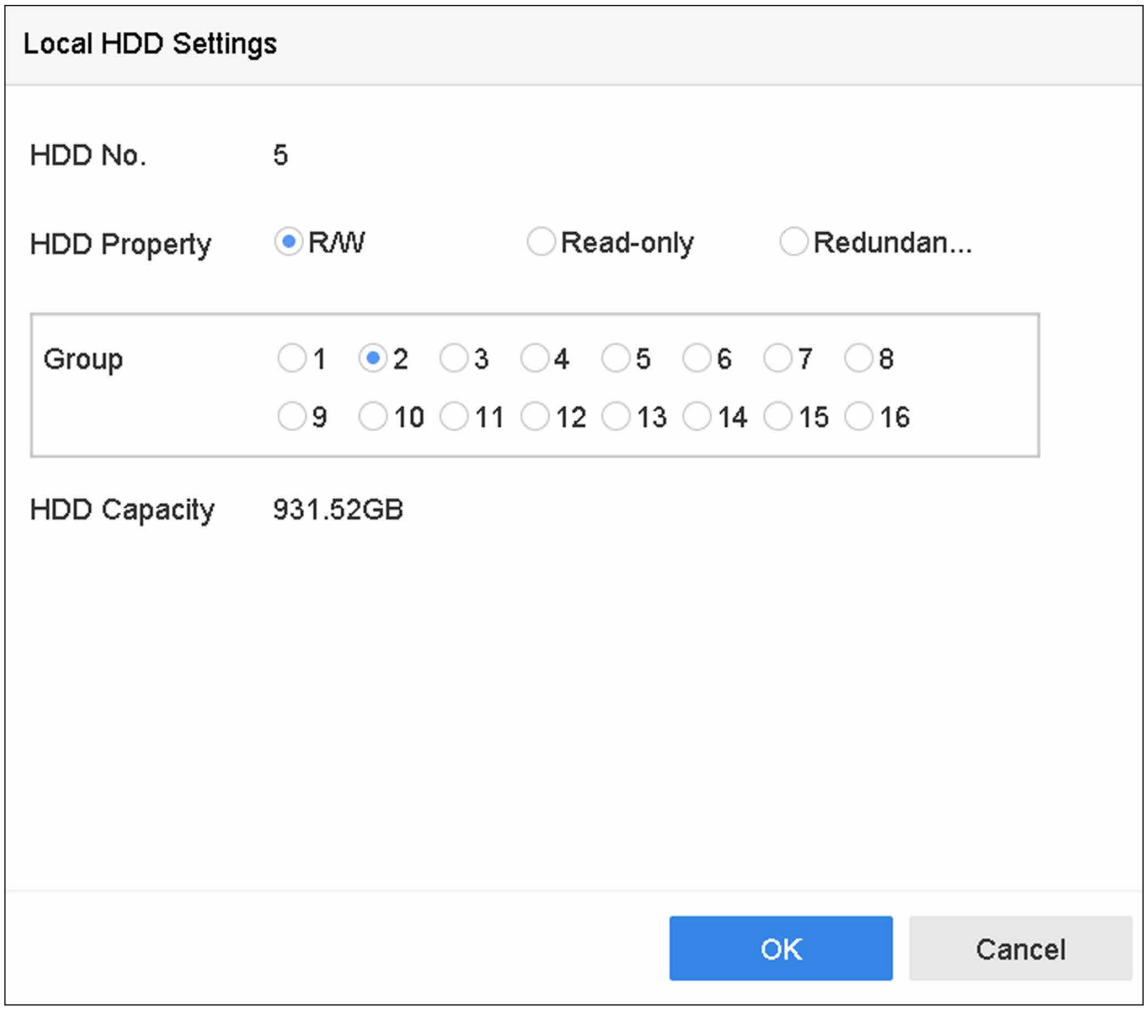

図 10-2 ローカル HDD の設定

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。

本機を使用する前に

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。

10.1.2 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。

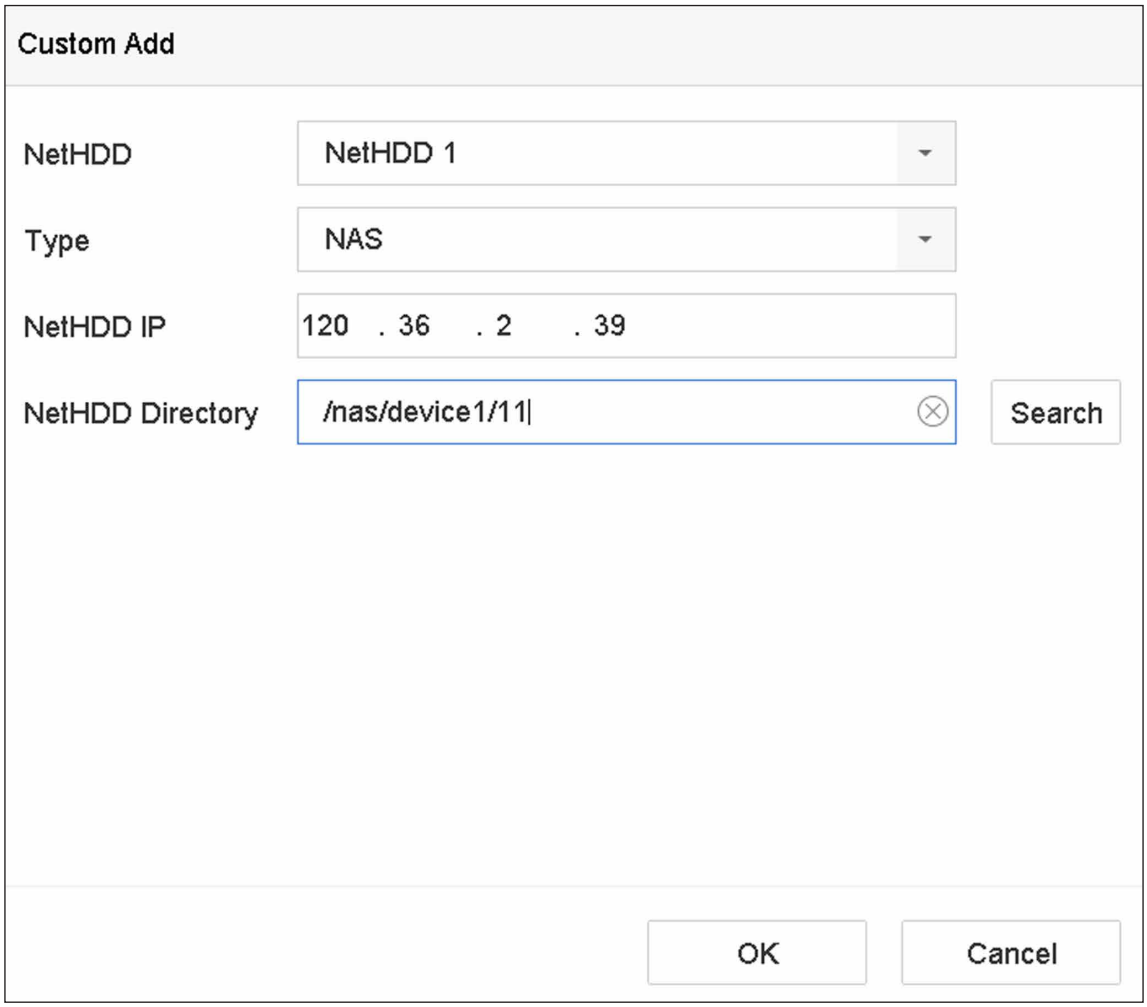

図 10-3 NetHDD の追加

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。

10.1.3 クラウドストレージを設定する

クラウドストレージ機能により、本機からクラウドサーバーに動画をアップロードすることができます。ローカル HDD の容量を節約できるだけでなく、より便利に動画にアクセスすることができます。Web ブラウザーからクラウドストレージを有効にすることができます。

本機を使用する前に

本機がインターネットに正しく接続され、正しいクラウドストレージ情報を取得してい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 → Storage → Storage Management → Cloud Storage**

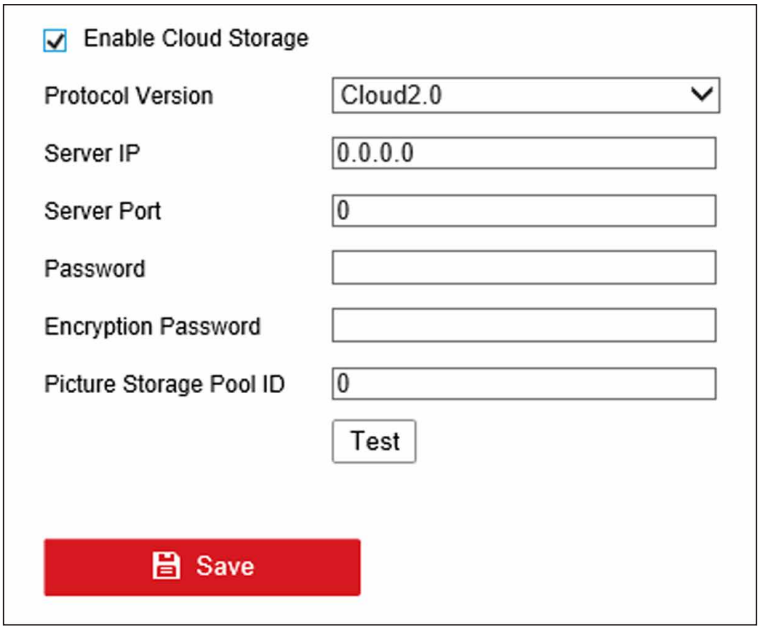

図 10-4 クラウドストレージ

2. **Enable Cloud Storage** にチェックを入れます。
3. クラウドストレージサーバーのパラメーターを設定します。

メモ

クラウドストレージサーバーには、複数のプールがあります。プールは HDD のようなもので、ファイルを保存するために使用されます。各プールは ID を持っているので、ストレージサーバーからプール ID を取得する必要があります。

4. **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. **Save** をクリックします。

10.1.4 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 10-5 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。

本機を使用する前に

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。

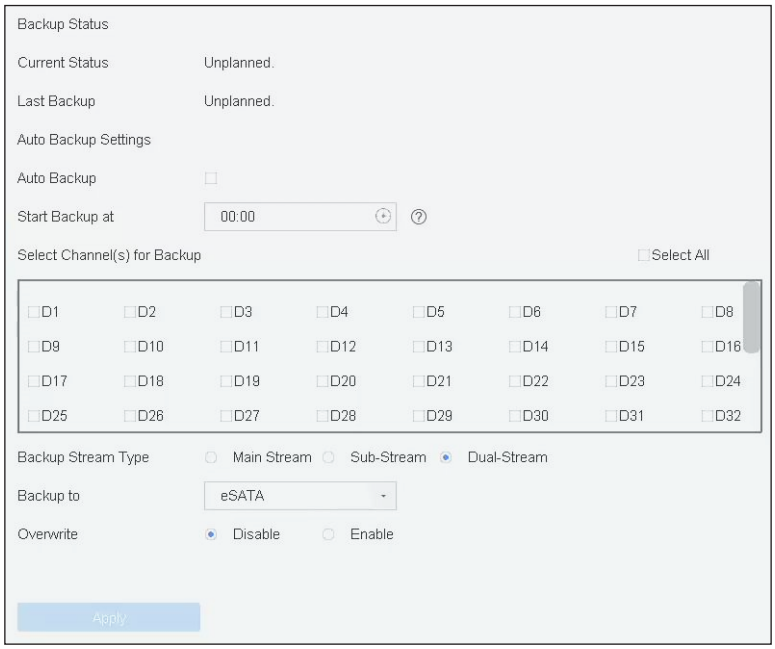

図 10-6 自動バックアップの eSATA の設定

10.1.5 録画書込みバッファの動的調整

Dynamically adjust recording writing buffer は、ビットレートが制限を超えた場合に、バッファメモリを動的に調整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. **Dynamically Adjust Recording Writing Buffer** にチェックを入れ、ビットレートが 4Mbps 以上の時ビデオロスを防ぎます。

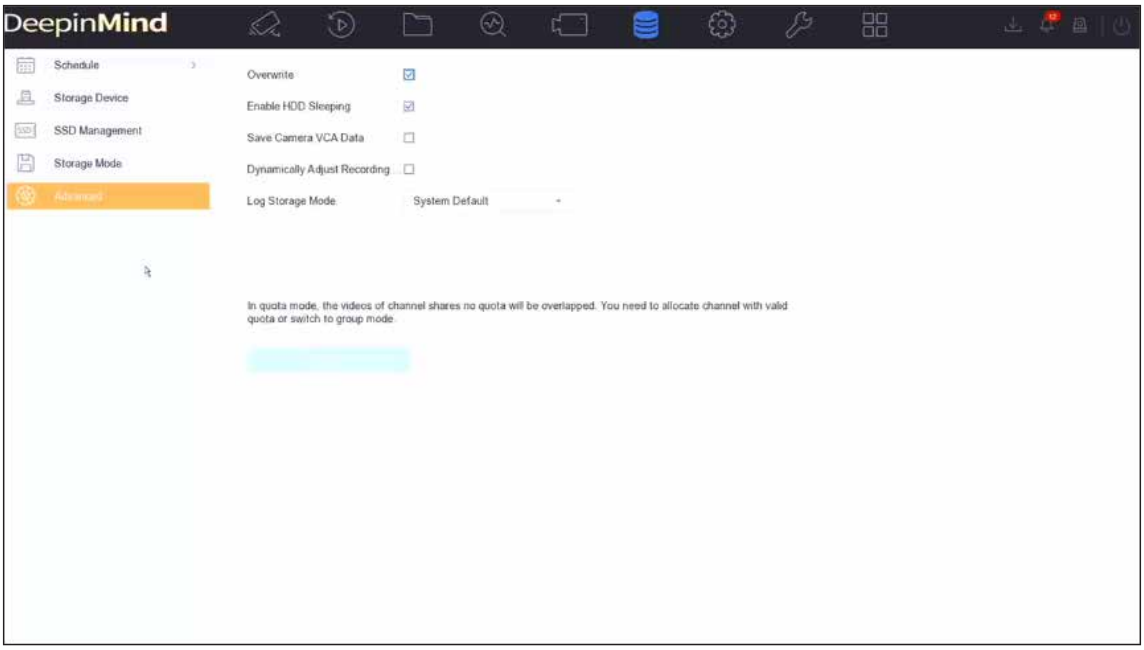

図 10-7 録画書込みバッファの動的調整

メモ

この機能を使用すると、メモリの使用量が多くなります。機能の有効化 / 無効化を行った後、本機を再起動してください。

10.2 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。

10.2.1 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。

本機を使用する前に

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。

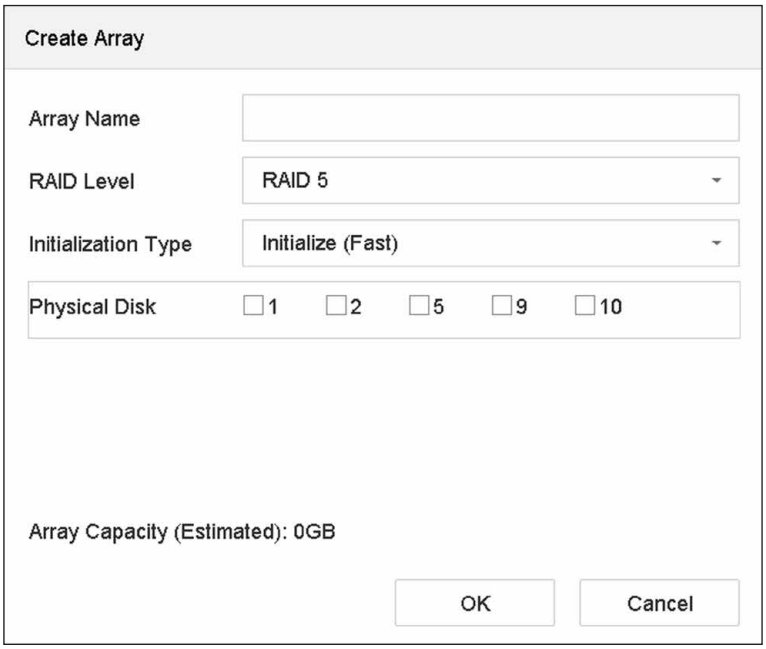

図 10-8 アレイの作成

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 10-1 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。

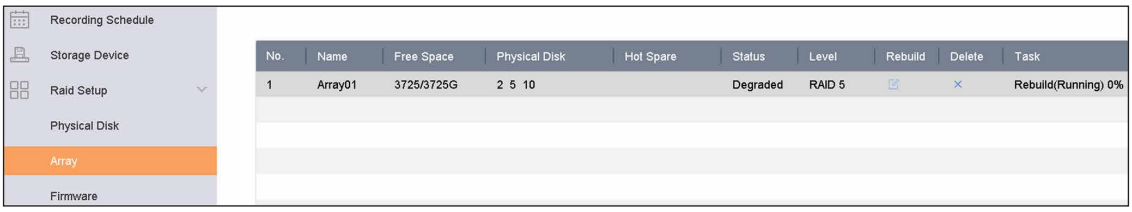

図 10-9 アレイリスト

10.2.2 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 10-10 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。

本機を使用する前に

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**

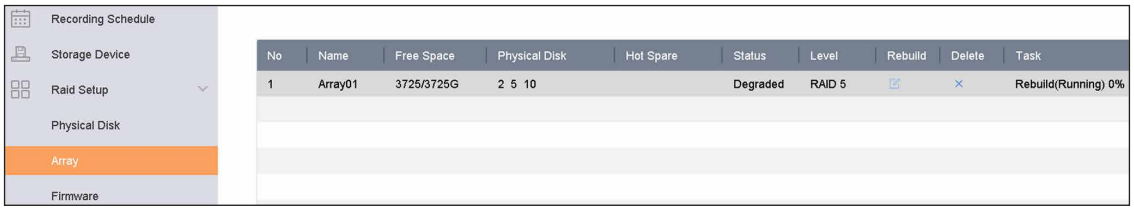

図 10-11 アレイリスト

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。

本機を使用する前に

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。

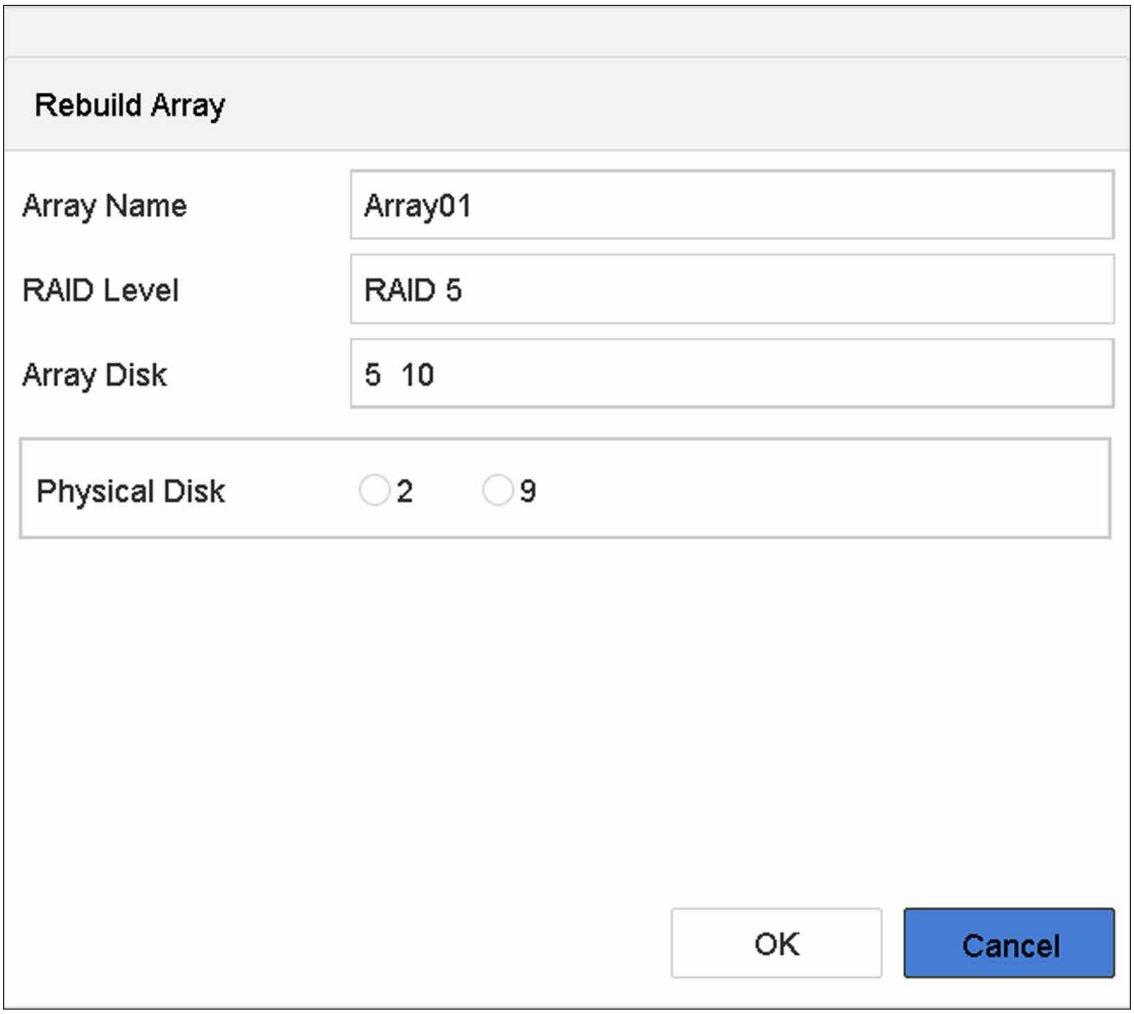

図 10-12 アレイの再構築

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 11 章 ホットスペアデバイスバックアップ

本機は、N+M のホットスペアシステムを構成することができます。このシステムは、複数の稼働中のビデオレコーダーと少なくとも 1 台のホットスペアのビデオレコーダーで構成されています。稼働中のビデオレコーダーが故障した場合、ホットスペアのビデオレコーダーに切り替えて稼働させることで、システムの信頼性を高めることができます。
ホットスペアビデオレコーダーと稼働中のビデオレコーダーの間には、下図のような双方向の接続が必要です。

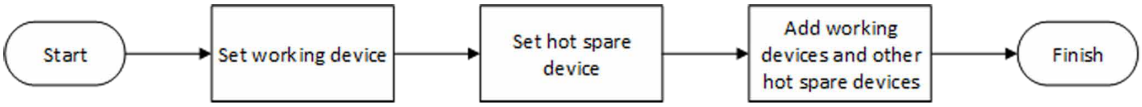

図 11-1 ホットスペアシステムの構築

メモ

- 稼働デバイスは最大 32 台、ホットスペアデバイスは最大 32 台まで許容されます。
- 互換性を保つため、すべてのデバイスを同じモデルで使用することをお勧めします。ホットスペア機能対応機種の詳細については、販売店にお問い合わせください。

11.1 稼働デバイスの設定

ステップ

1. 次の順に進みます。**System → Hot Spare**
2. **Work Mode** は **Normal Mode** を設定します。

メモ

Normal Mode はデフォルトで設定されています。

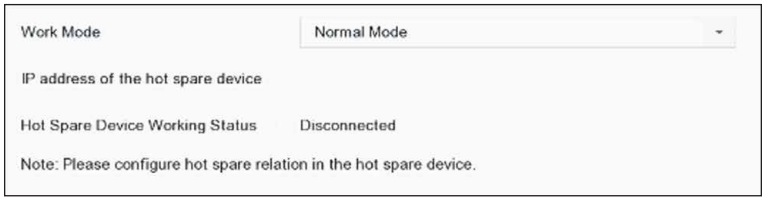

図 11-2 稼働レコーダーの設定

3. **Apply** をクリックします。

メモ

上記手順を繰り返し、他の稼働デバイスを設定します。

11.2 ホットスペアデバイスの設定

ホットスペアデバイスは、稼働デバイスに障害が発生した場合に、稼働デバイスのタスクを引き継ぎます。

ステップ

1. 次の順に進みます。**System → Hot Spare**
2. **Work Mode** は **Hot Spare Mode** を設定します。

図 11-3 ホットスペア

3. **Apply** をクリックします。
4. ポップアップで **Yes** をクリックします。本機が自動的に再起動します。

メモ

- ホットスペアモードで動作する場合、カメラ接続は無効となります。
- ホットスペアデバイスの作業モードを通常モードに切り替えた後、その後の正常な動作を確保するために、デバイスをデフォルトに戻すことを強く推奨します。

11.3 ホットスペアシステムの管理

ステップ

メモ

- ホットスペアシステムでは、最大 32 台の稼働デバイスと 32 台のホットスペアデバイスを使用することができます。
- 稼働デバイスや他のホットスペアデバイスを追加できるのは、1 台のホットスペアデバイスのみです。ホットスペアデバイスの IP アドレスは、稼働中のデバイスから確認することができます。

1. ホットスペアデバイスを経由して、次の順に進みます。**System → Hot Spare**

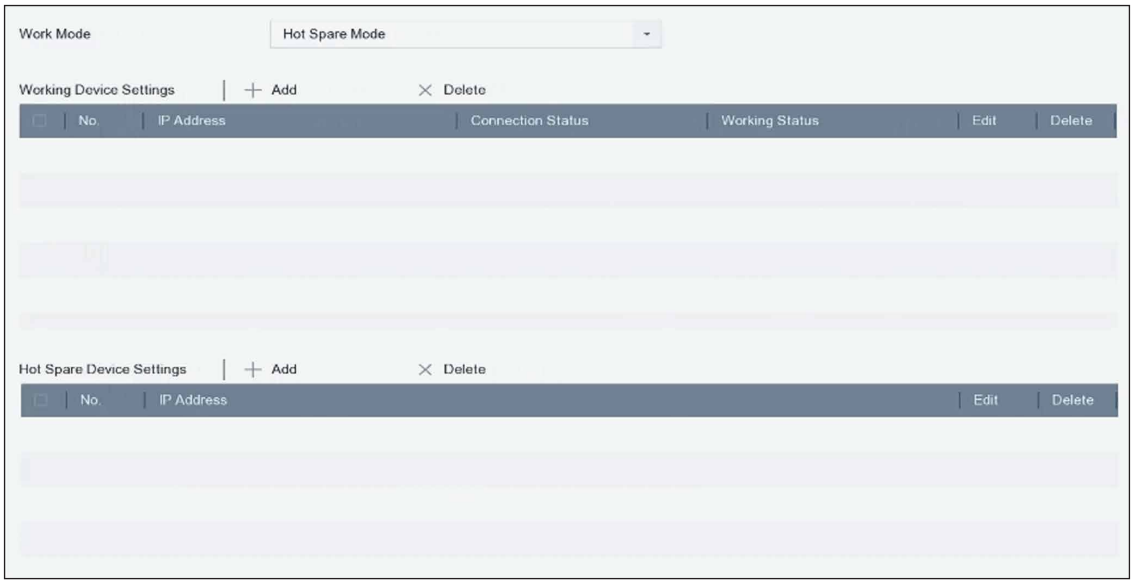

図 11-4 稼働デバイスの追加

2. **Working Device Settings** で **Add** をクリックして、ホットスペアシステムに稼働デバイスを追加します。インターフェイスの更新後、ホットスペアデバイスのインターフェイスから稼働中のデバイスの作業ステータスを確認することができます。また、ホットスペアデバイスの稼働ステータスや IP アドレスは、稼働デバイスインターフェースから確認することができます。

表 11-1 稼働デバイスの作業ステータス

作業ステータス	説明
Monitoring	稼働中のデバイスは正常に動作しています。
No need for backup	稼働中のデバイスはオフラインになり、これまで一度もモニターされたことがありません。
Backing up	稼働中のデバイスは以前からモニターされていますが、オフラインになっています。ホットスペアデバイスは、稼働中のデバイスを引き継ぎ、稼働中のデバイスに接続されたネットワークカメラの映像を録画します。ビデオバックアップ機能は、1 台の稼働デバイスに対して同時に有効にすることができます。
Waiting for synchronization	稼働中のデバイスはオンラインに戻り、ホットスペアデバイスが動画を同期するのを待ちます。
Synchronizing	ホットスペアデバイスは、稼働中のデバイスに動画を復元しています。同期機能は、1 台の稼働デバイスに対して同時に有効にすることができます。
Synchronization finished	動画は稼働中のデバイスに復元されます。稼働デバイスが回復しました。

3. **Hot Spare Device Settings** で **Add** をクリックして、ホットスペアデバイスをホットスペアシステムに追加します。
4. オプション：**Delete** をクリックすると、稼働中のデバイスやホットスペアデバイスを自由に削除することができます。

第 12 章 ネットワーク設定

12.1 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。

本機を使用する前に

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**

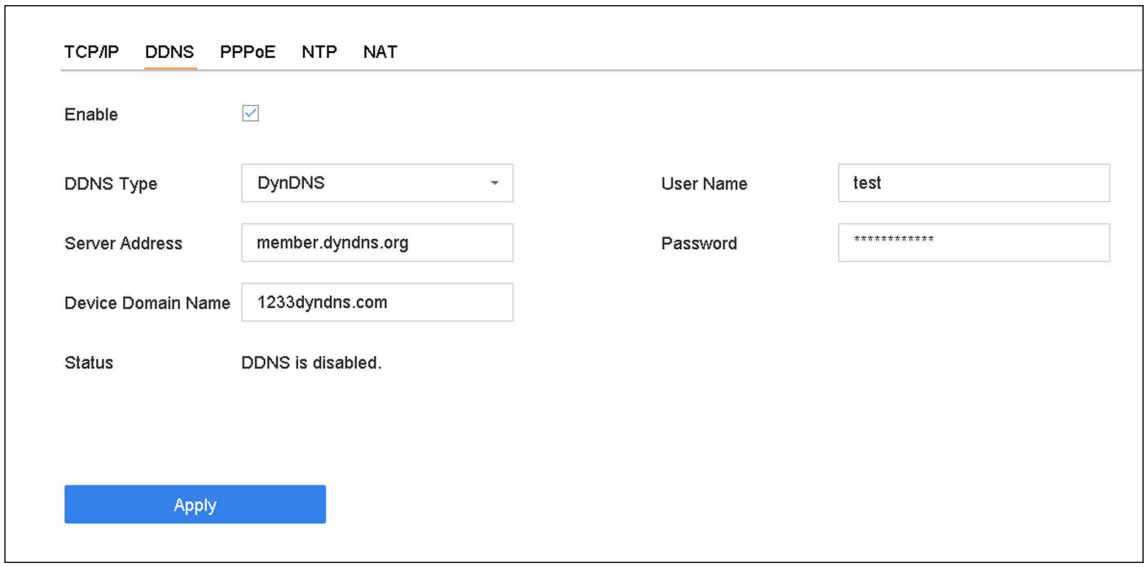

図 12-1 DDNS 設定

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。

12.2 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以下のように設定する必要があります。**System → Network → TCP/IP → PPPoE**
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。

12.3 SNMP の設定

SNMP（SNMP v2 および SNMP v3）の設定を行い、Web ブラウザー経由でデバイスのステータスやパラメータ情報を取得することができます。SNMP v3 は、SNMP v2 に暗号化セキュリティを追加し、認証とプライバシーによるセキュリティを提供します。

本機を使用する前に

SNMP ソフトウェアをダウンロードし、SNMP ポート経由でデバイス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. Web ブラウザー経由で次の順に進みます。**Configuration → Network → Advanced Settings → SNMP**

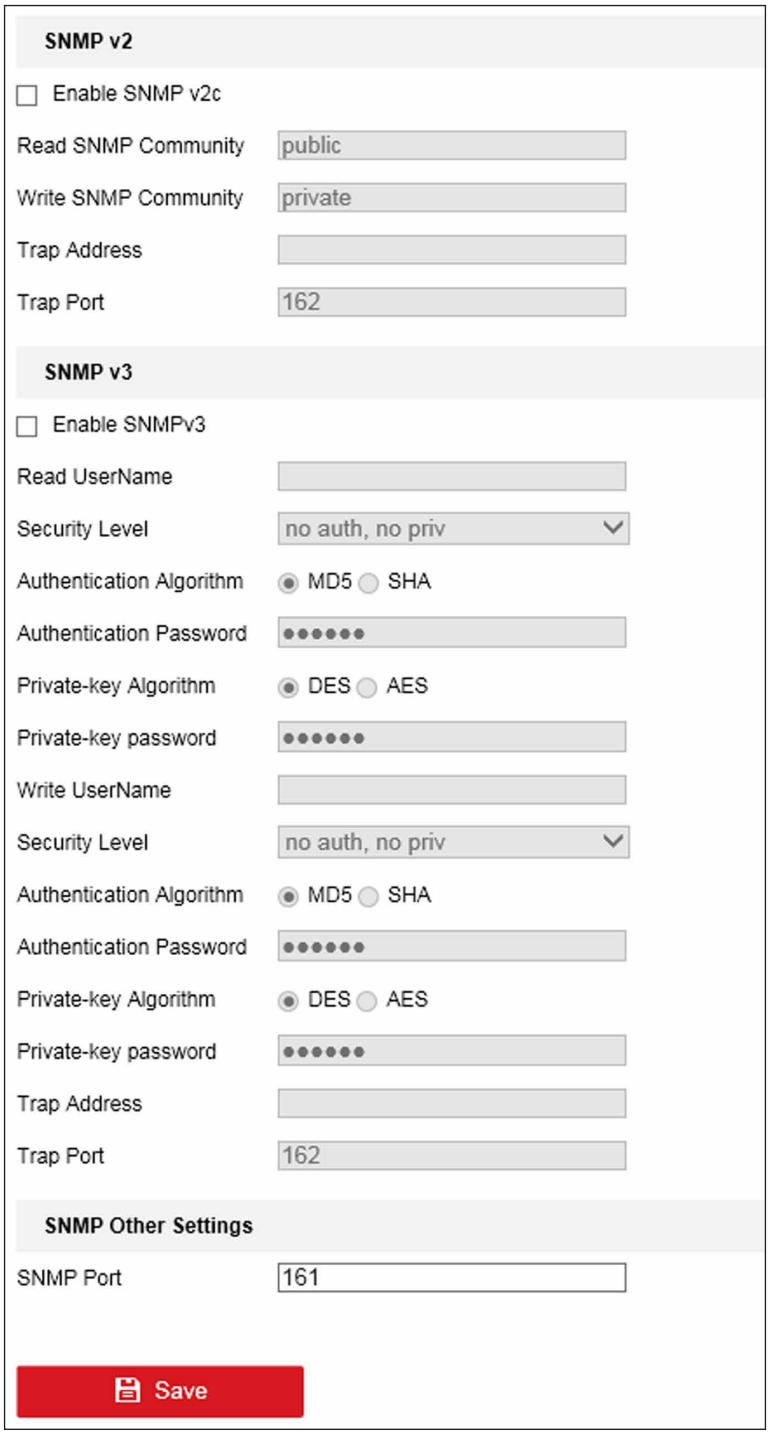

図 12-2 SNMP 設定

2. 希望する SNMP v2 または SNMP v3 を有効にしてください。
3. 関連するパラメーターを設定します。
4. **SNMP Port** を設定します。
5. **Save** をクリックします。

12.4 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。

本機を使用する前に

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。

12.5 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。

本機を使用する前に

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 12-3 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。

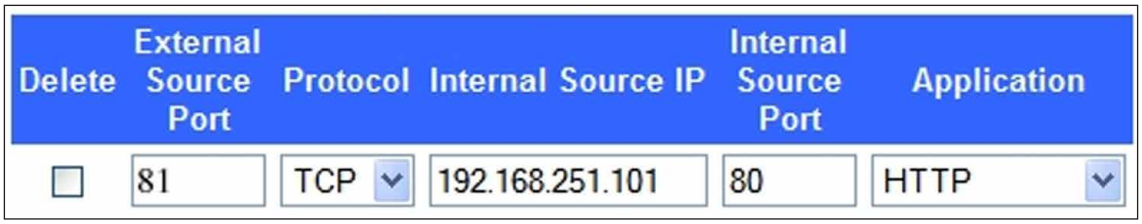

図 12-4 仮想サーバー項目の設定

12.6 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 12-5 ポートの設定

2. 必要に応じて、ポートの設定を行います。

Alarm Host IP/Port

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：Guarding Vision）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。

12.7 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。

注意

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 13 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。

13.1 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。

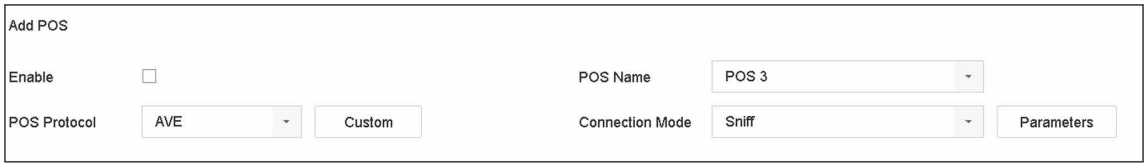

図 13-1 POS 設定

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。

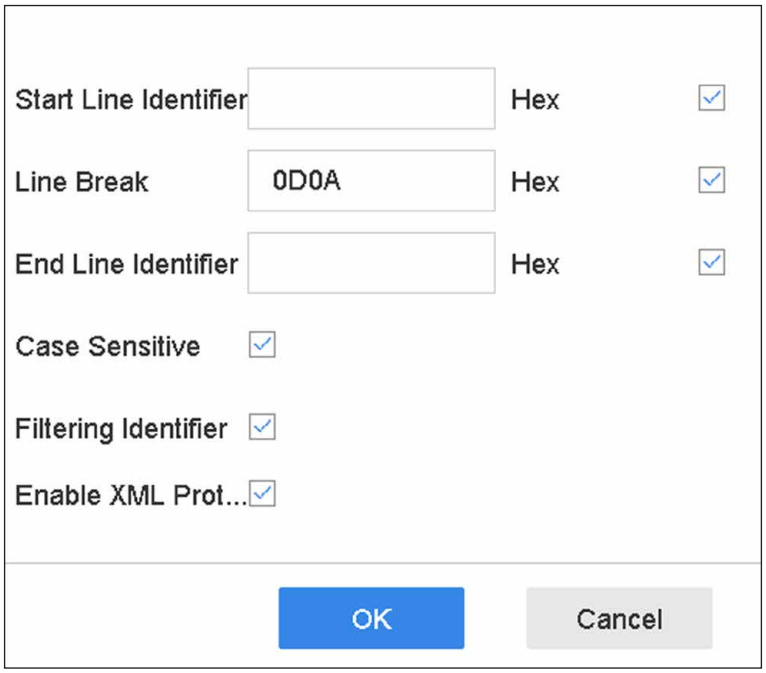

図 13-2 ユニバーサルプロトコルの設定

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** 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、Flow Ctrl）を設定します。

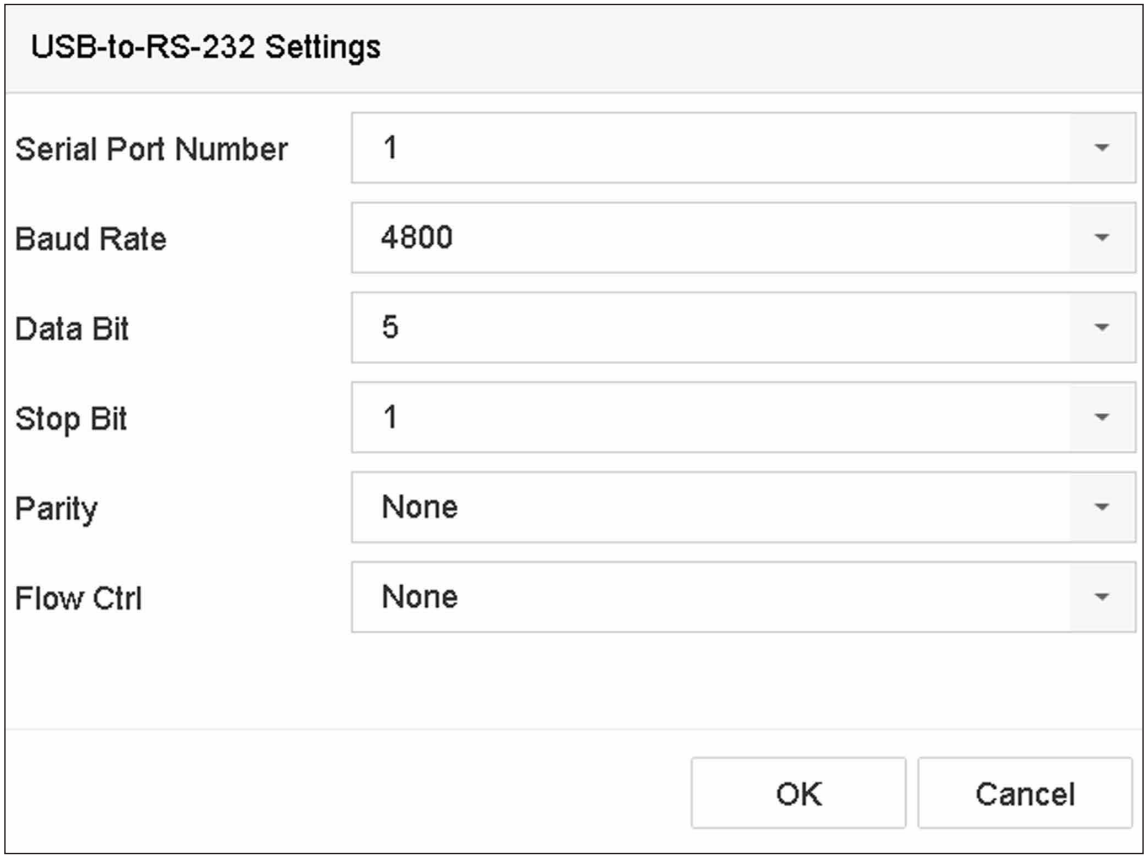

図 13-3 USB-to-RS-232 の設定

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。

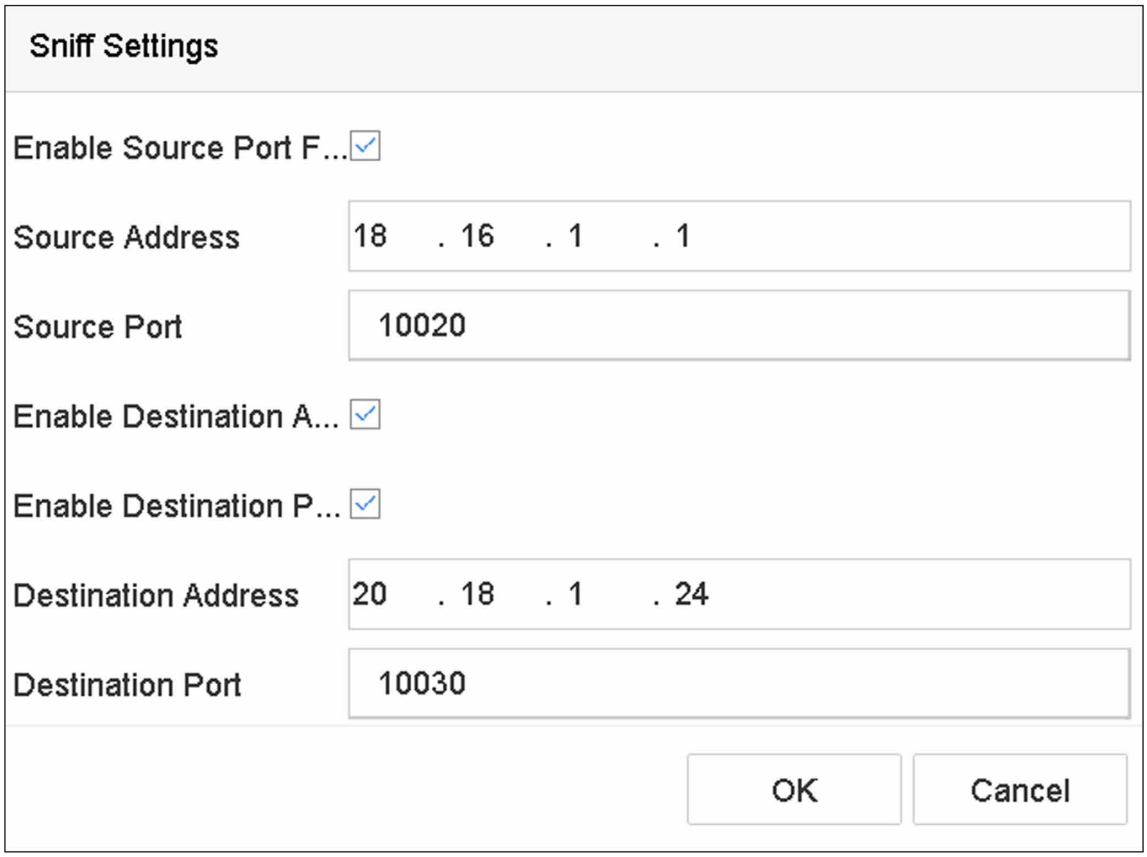

図 13-4 Sniff の設定

13.2 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。

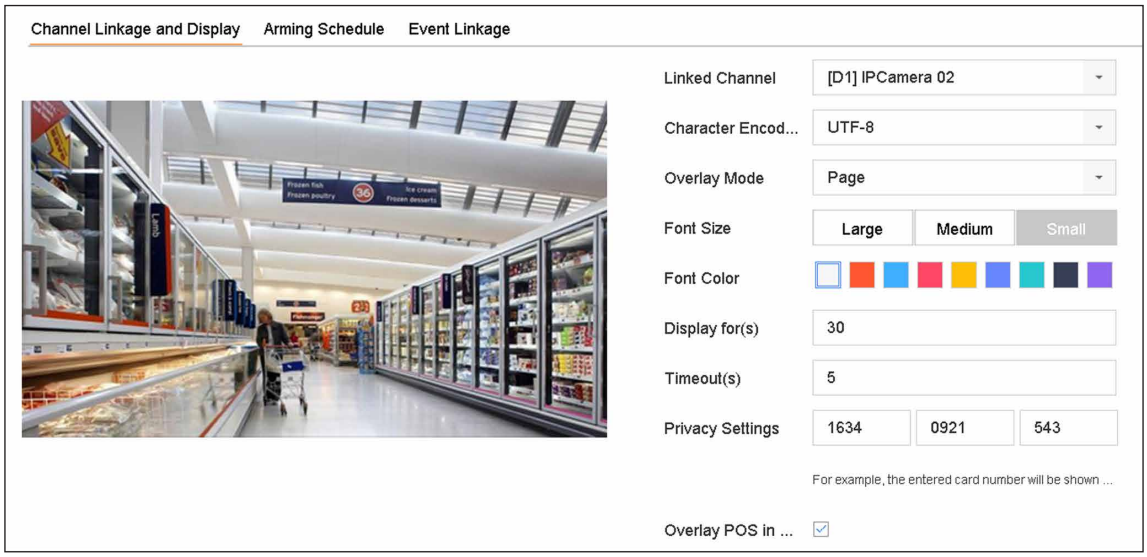

図 13-5 オーバーレイ文字設定

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、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。

13.3 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。

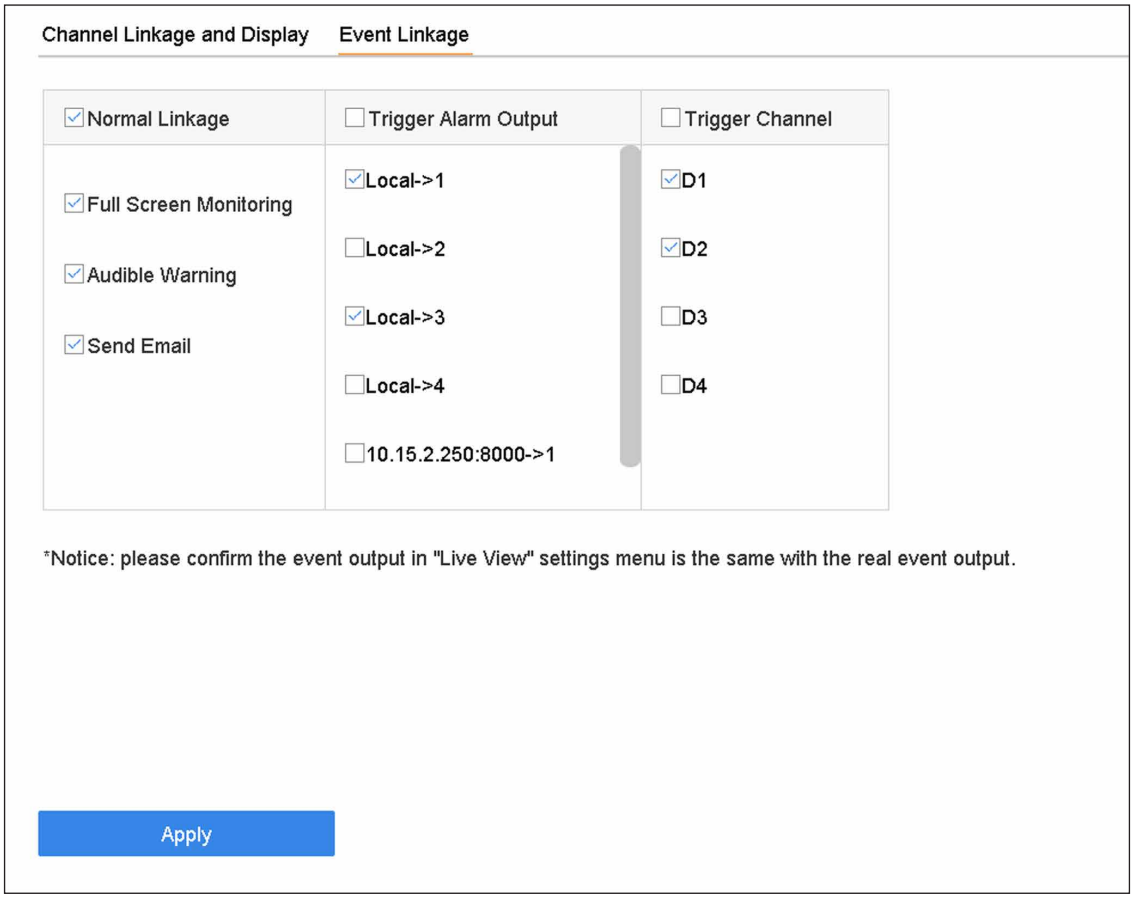

図 13-6 POS のカメラ作動の設定

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 14 章 ユーザー管理とセキュリティ

14.1 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。

14.1.1 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** ボタンをクリックします。
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。

注意

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。

14.1.2 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。

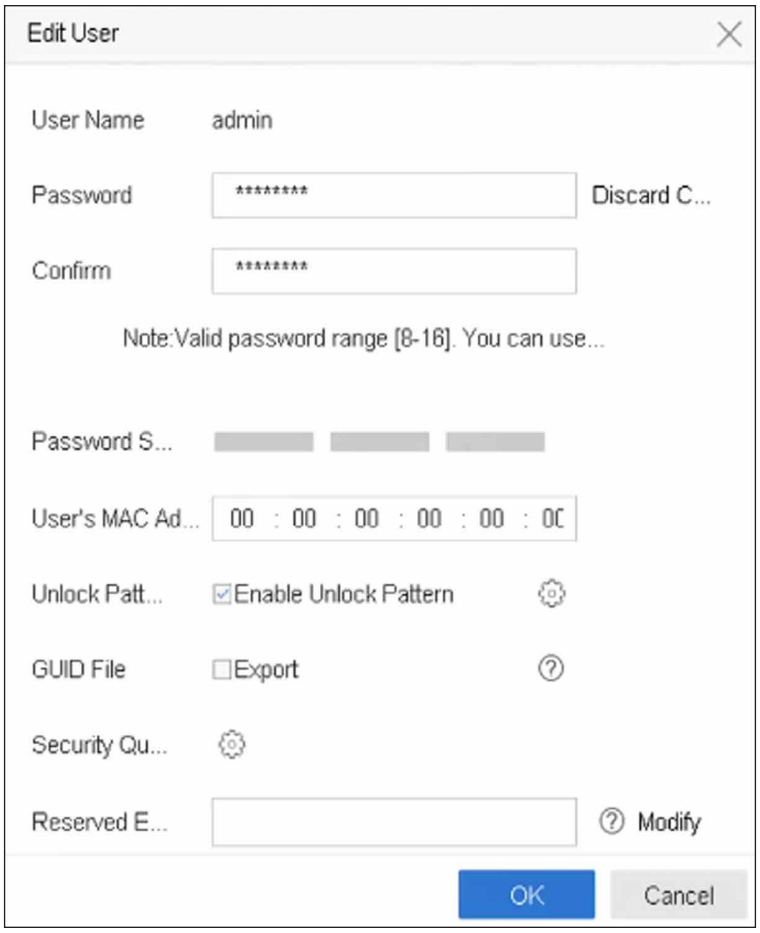

図 14-1 ユーザー（管理者）の編集

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、今後パスワードを再設定する時のために、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。

14.1.3 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。

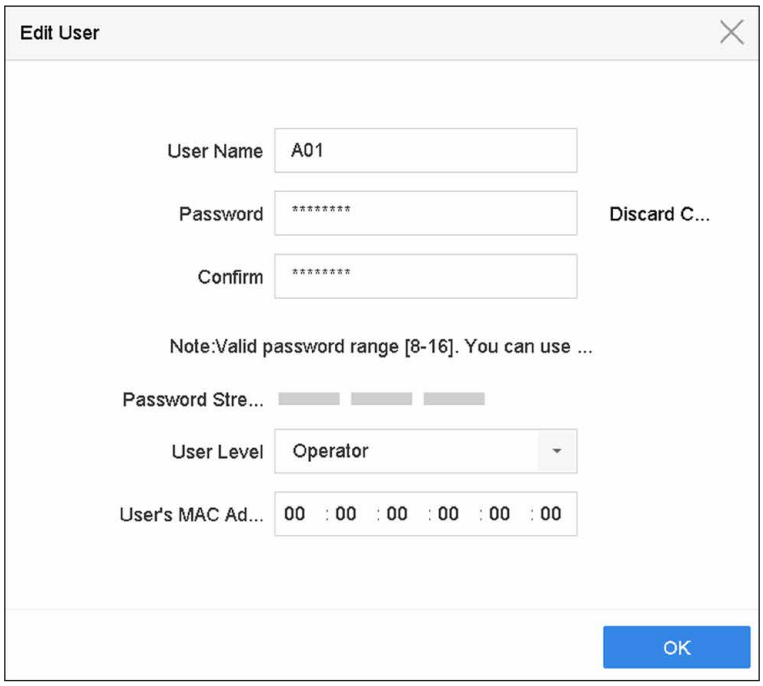

図 14-2 ユーザー（Operator/Guest）の編集

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。

14.2 ユーザー権限の管理

14.2.1 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。

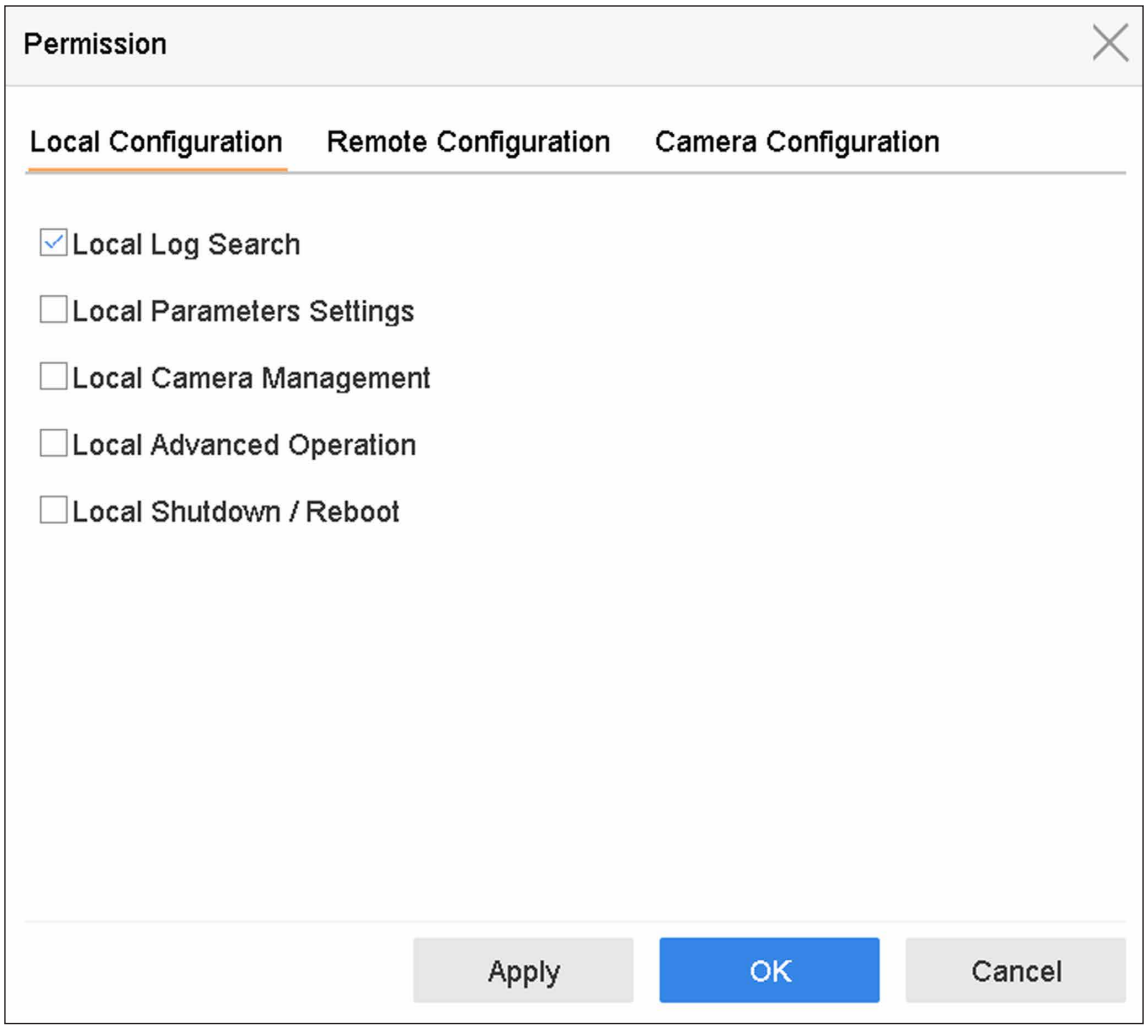

図 14-3 ユーザー権限設定インタフェース

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）のライブ動画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 動作を遠隔で制御します。

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）のライブ動画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。

14.2.2 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。

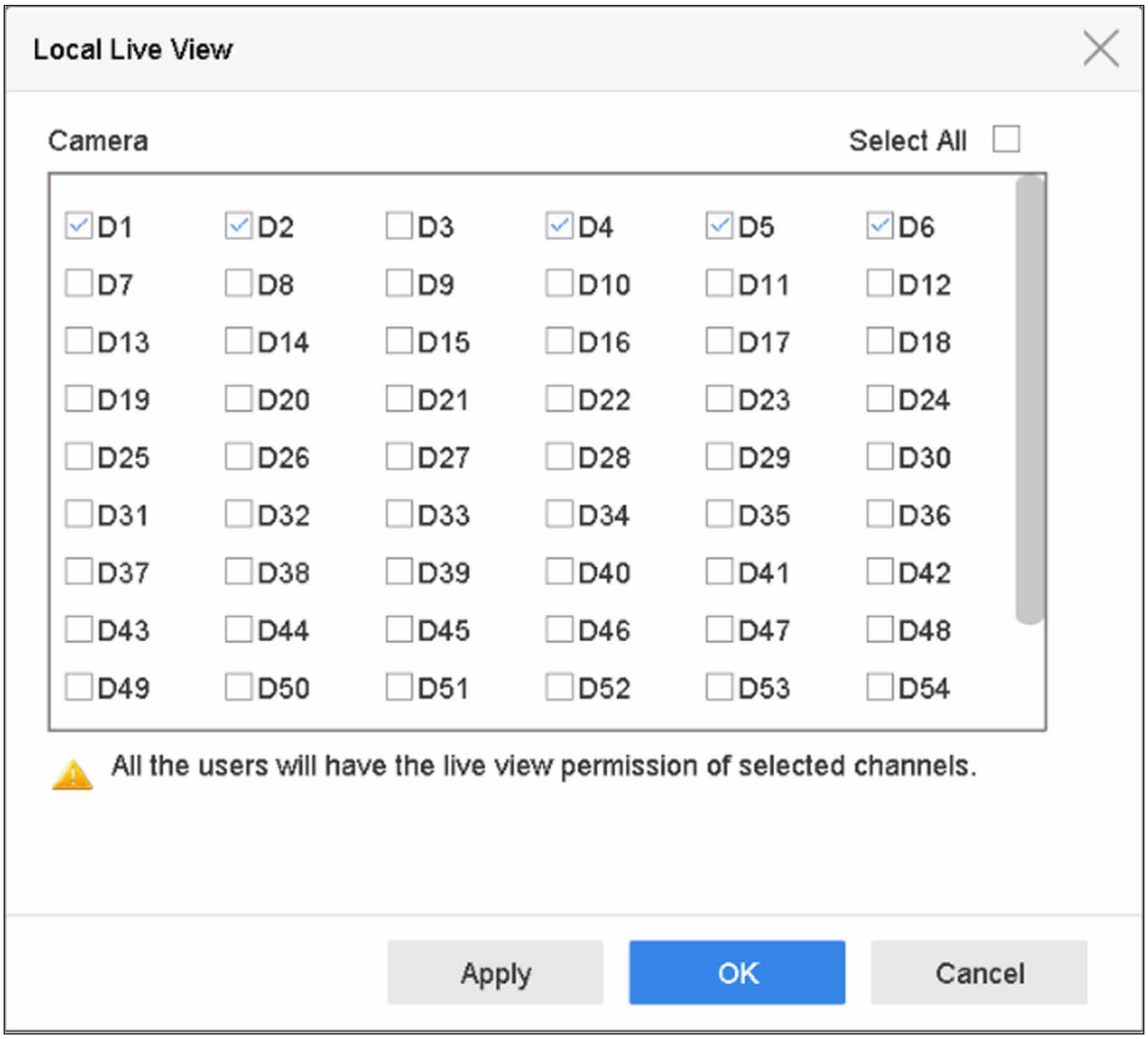

図 14-4 ロック画面のライブビューの権限設定

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。

14.2.3 管理者ユーザー以外の二重認証権限の設定

チャンネルで二重認証を有効にした後、管理者ユーザー以外が権限を得るには、権限のあるユーザーによって認証される必要があります。二重認証の設定は、管理者のみが行うことができます。

ステップ

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

図 14-5 二重認証ユーザーの設定

2. **Enable Double Verification** にチェックを入れます。
3. 二重認証ユーザーを設定します。二重認証ユーザーはシステムユーザーとは異なります。二重認証のユーザーは最大 8 名まで追加できます。
   1）**Add** をクリックして、二重認証ユーザーを追加します。
   2）管理者パスワードを入力します。
   3) ユーザー名、パスワード、カメラ権限などのユーザーパラメータを設定します。
   4) **OK** ボタンをクリックしてください。
4. **Apply** をクリックします。
5. 管理者ユーザー以外に対する権限を設定します。
   1）次の順に進みます。**System → User**
   2）をクリックして、ユーザー権限を編集します。
   3）**Camera Permission** を選択します。**Local Playback**、**Remote Playback/Download**、**Local Video Export** だけが二重認証できます。
   4) 二重認証が必要なチャンネルを選択します。
   5) **OK** ボタンをクリックしてください。

14.3 パスワードセキュリティの設定

14.3.1 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。

本機を使用する前に

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。

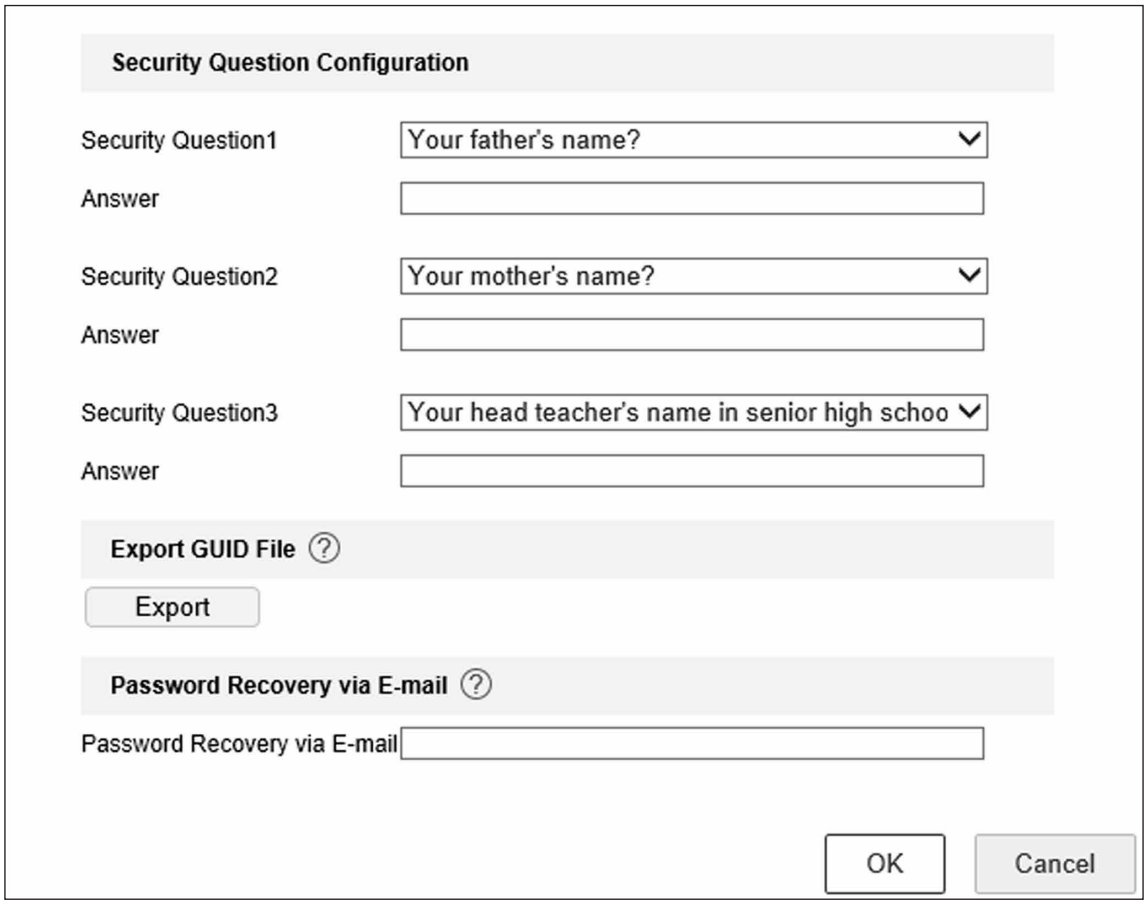

図 14-6 GUID ファイルをエクスポートする

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。

14.3.2 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。

ステップ

1. 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 **Security Question Configuration** をクリックします。
2. セキュリティに関する質問と答えを設定します。

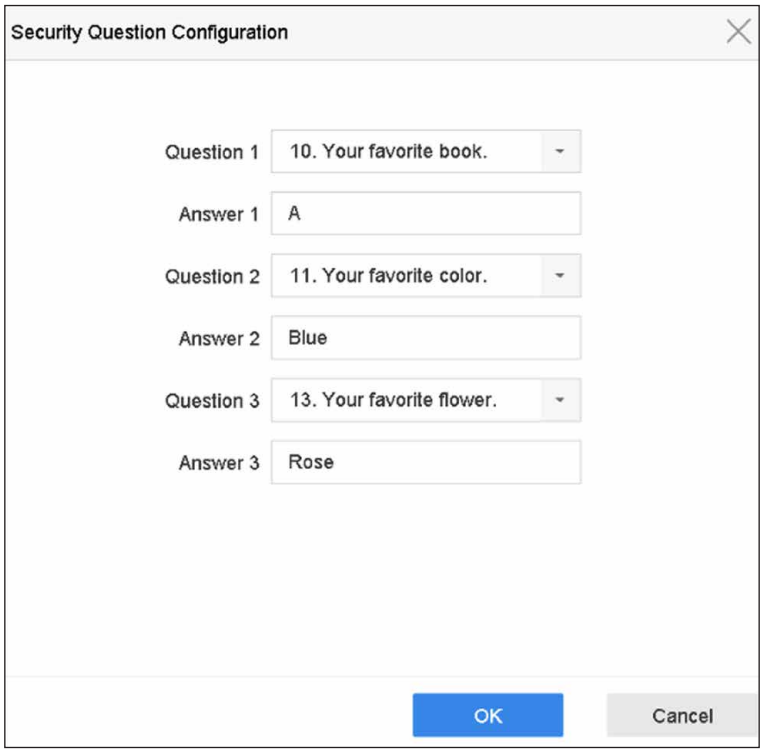

図 14-7 セキュリティに関する質問の設定

3. **OK** ボタンをクリックします。

14.3.3 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。

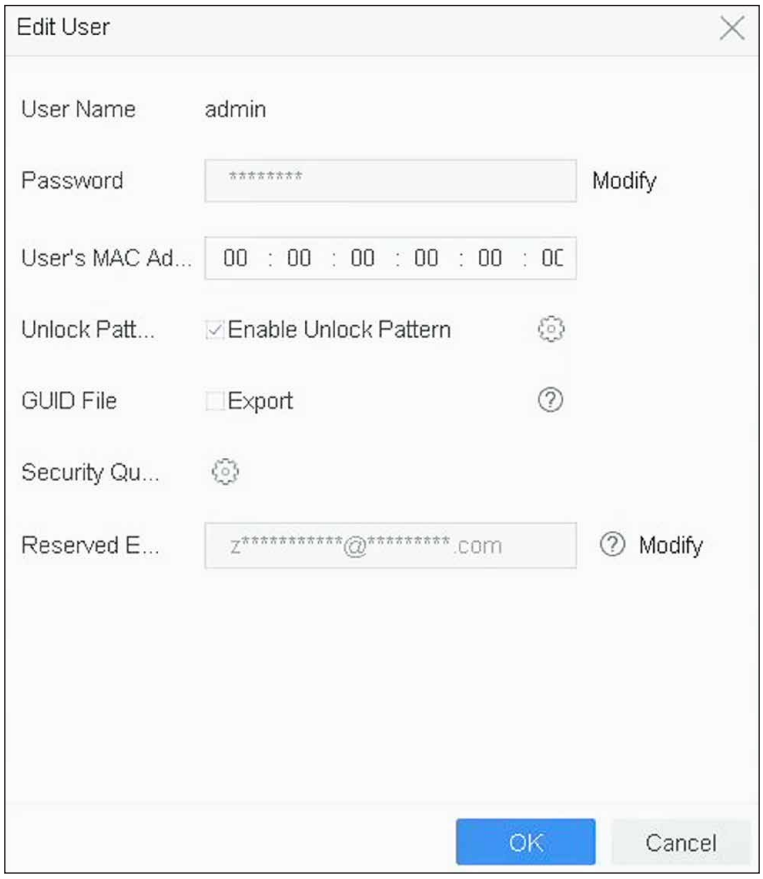

図 14-8 予約メールの設定

3. **OK** ボタンをクリックします。

14.4 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。

14.4.1 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。

本機を使用する前に

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。

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。

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。

14.4.2 セキュリティ質問でパスワードをリセットする

本機を使用する前に

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ます。

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. **password resetting type** は **Verify by Security Question** を選択します。
3. 3 つのセキュリティに関する質問の正しい答えを入力してください。
4. **OK** ボタンをクリックします。
5. Reset Password インターフェースで新しい管理者パスワードを作成します。

14.4.3 予約メールでパスワードをリセットする

本機を使用する前に

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。（**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。
   - Guarding Vision 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. QR コードを添付して ***pw_recovery@hikvision.com*** に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。

14.4.4 Guarding Vision でパスワードをリセットする

本機を使用する前に

本機が Guarding Vision を有効にし、登録された Guarding Vision 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 Guarding Vision** を選択します。
3. 本機に紐付いているアカウントで Guarding Vision アプリにログインしてください。
4. Guarding Visionを使って QR コードを読み取ってください。その後、Guarding Vision 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。

第 15 章 システム管理

15.1 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。

15.2 時間の設定

15.2.1 手動で時刻を合わせる

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。

15.2.2 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。

15.2.3 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。

15.3 オーディオの管理

音声ファイルはアラームリンケージに使用されます。
System → Audio Management でオーディオファイルをインポートし、管理することができます。

メモ

音声ファイルをインポートする前に、音声ファイルが入ったバックアップデバイスを用意します。

15.4 エンハンスド SVC モードの設定

ライブビューや再生時には、動画のフレームを抽出するエンハンスト SVC モードを設定することができ、より優れたデコード能力を発揮することができます。一部の機種のみ対応しています。
System → General に進むと、このモードを有効にすることができます。

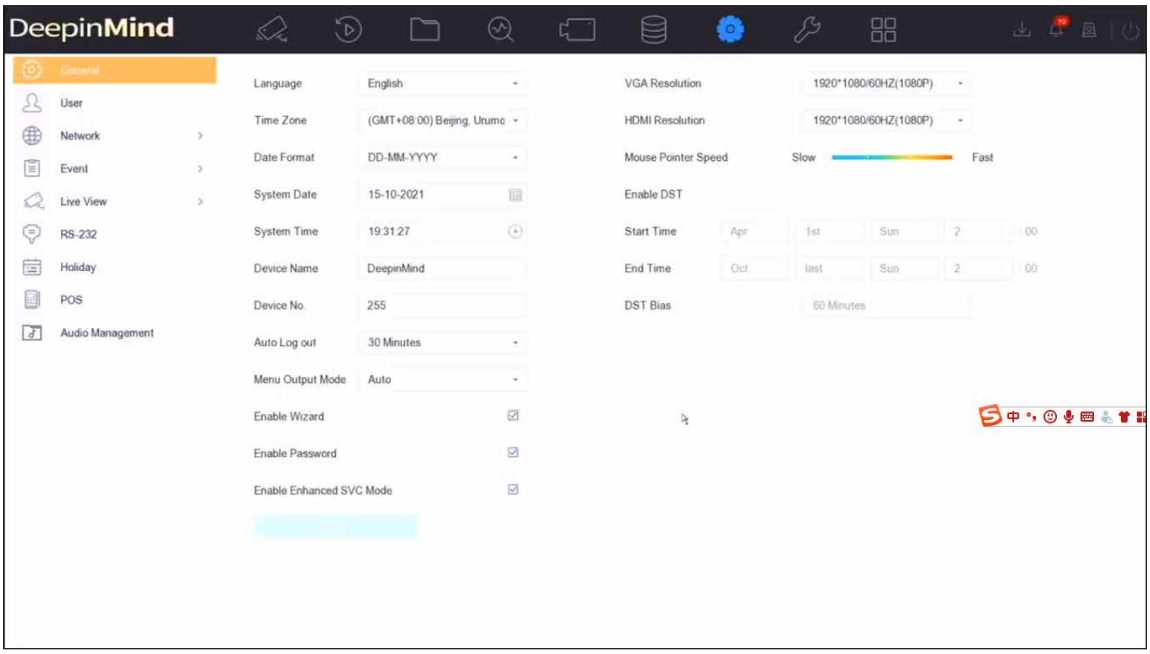

図 15-1 エンハンスド SVC モード

メモ

本機のエンハンスド SVC モード設定がうまくいかない場合は、カメラの Web ページでエンハンスド SVC モードを有効にしてください。

15.5 ネットワークの検知

15.5.1 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。

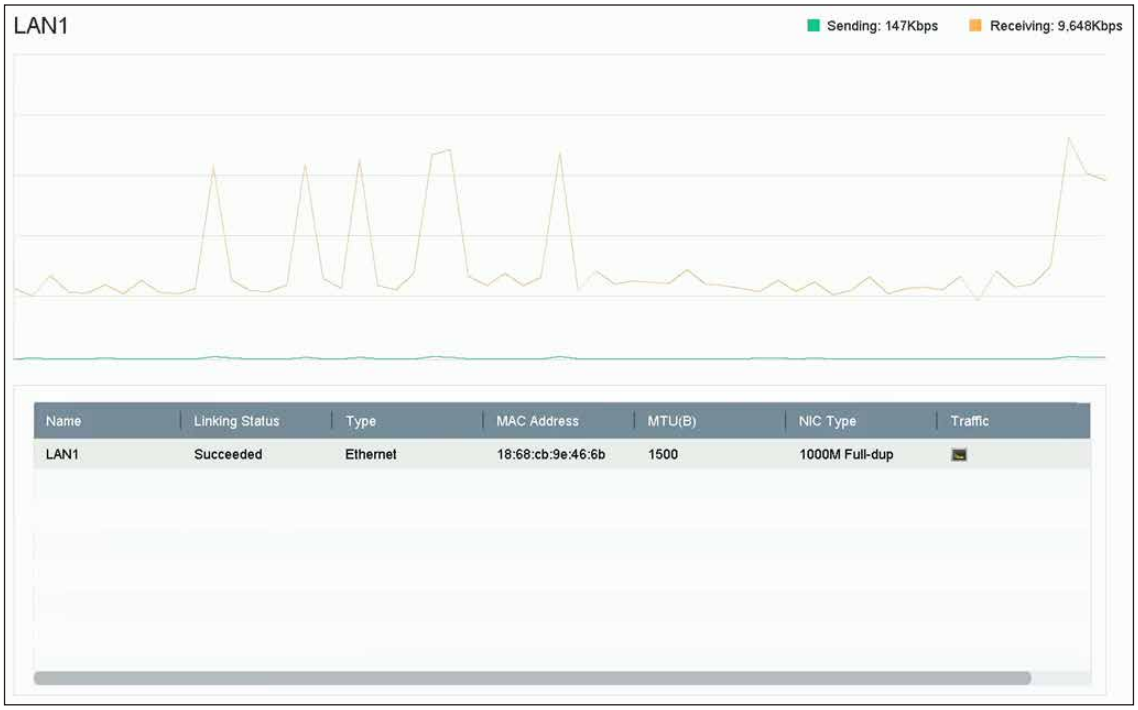

図 15-2 ネットワークトラフィック

15.5.2 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. 次の順に進みます。**Maintenance → Network → 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 15-3 ネットワーク遅延とパケットロスをテストする

15.5.3 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。

本機を使用する前に

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. 次の順に進みます。**Maintenance → Network → 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 15-4 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。

15.5.4 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 → Network Stat**

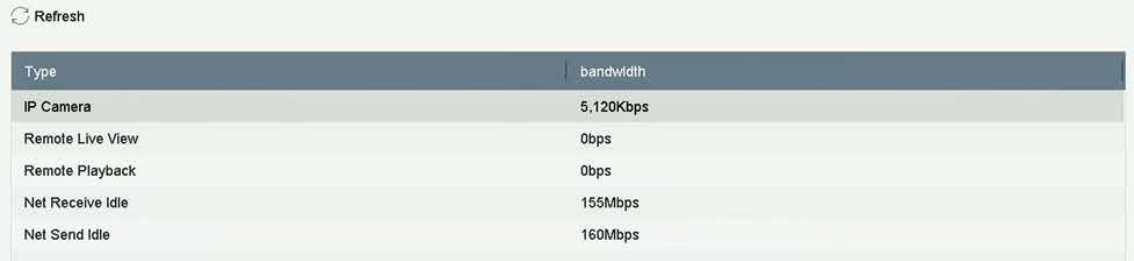

図 15-5 ネットワークリソースの統計情報

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。

15.6 ストレージデバイスのメンテナンス

15.6.1 バッド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。

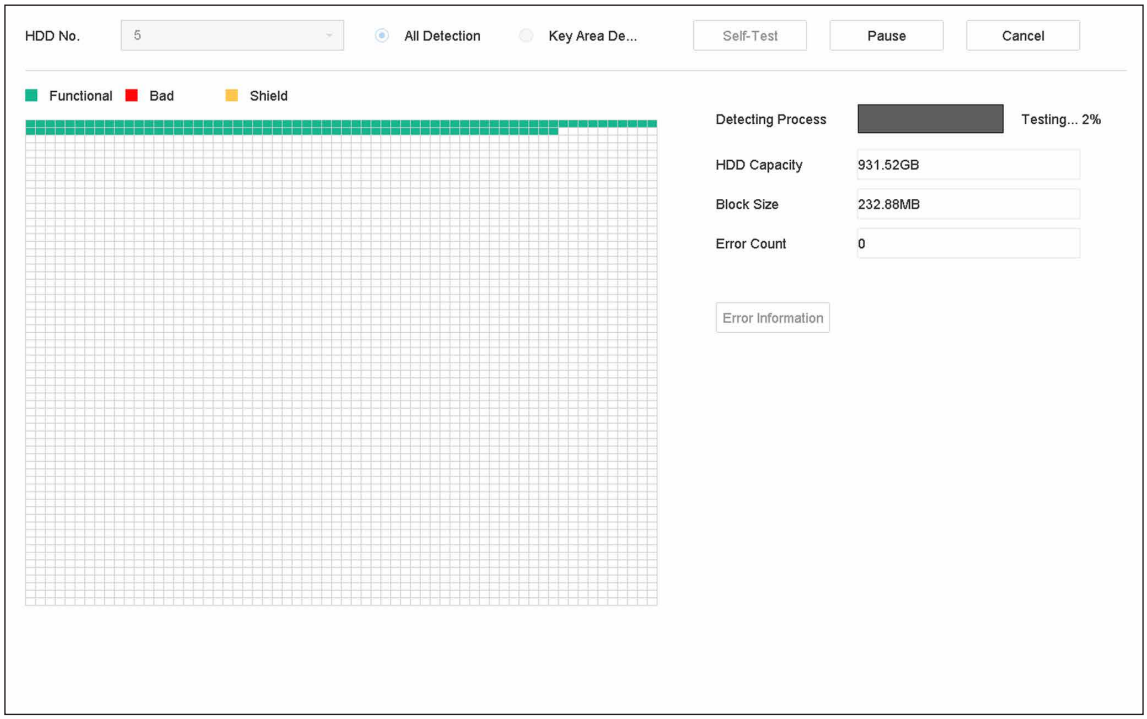

図 15-6 バッドセクター検知

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。

15.6.2 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** をクリックすると S.M.A.R.T. HDD self-evaluation を開始します。

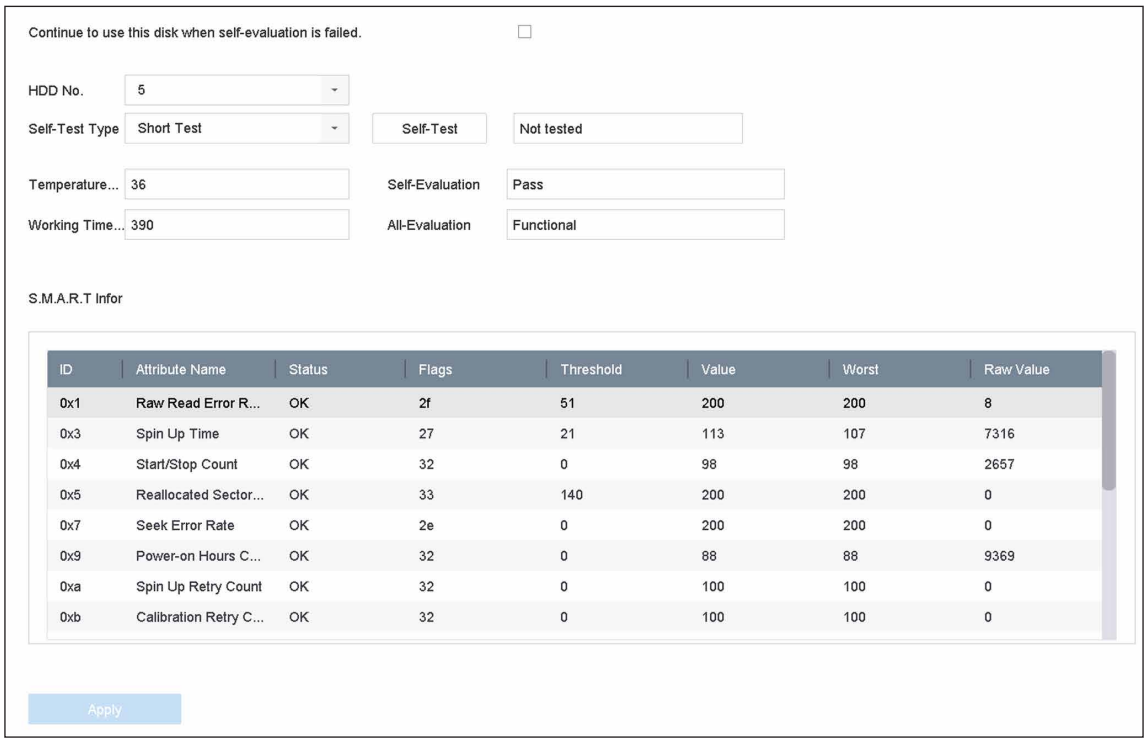

図 15-7 S.M.A.R.T. 設定インターフェース

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。

15.6.3 HDD のヘルス検知

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 15-8 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。

15.6.4 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。

本機を使用する前に

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**

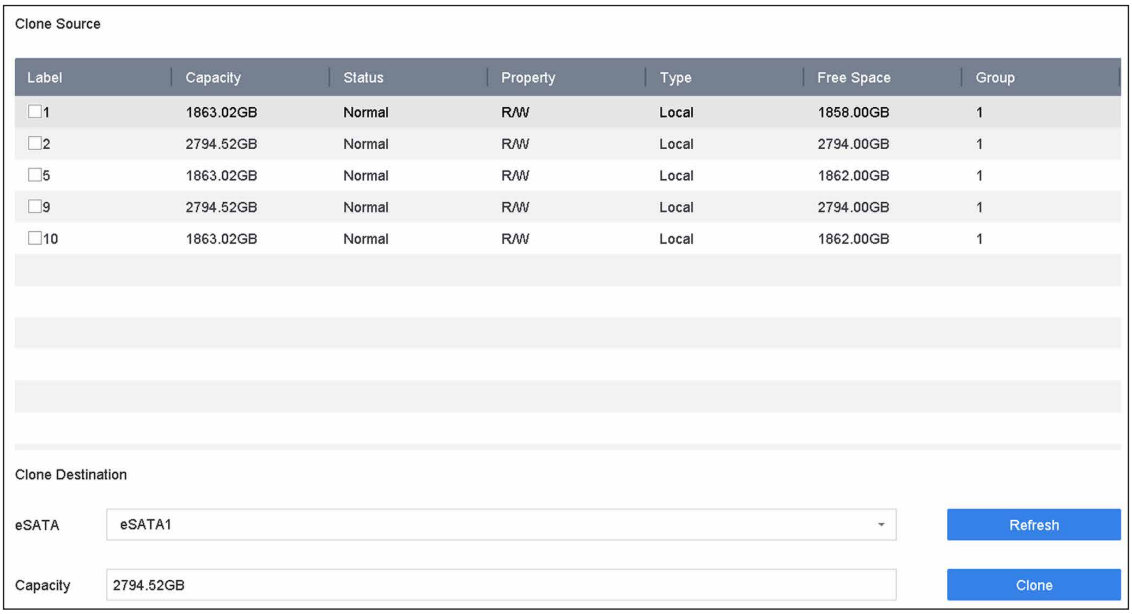

図 15-9 HDD クローン

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。

15.6.5 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。

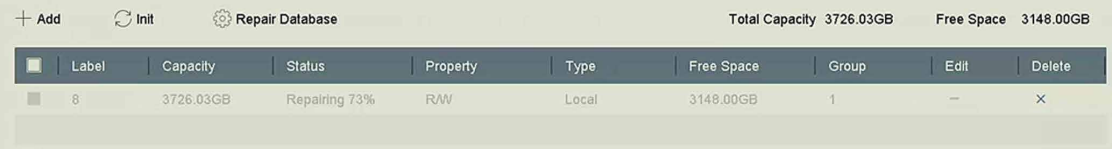

図 15-10 データベースの修復

15.7 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。

15.7.1 ローカルバックアップデバイスによるアップグレード

本機を使用する前に

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。

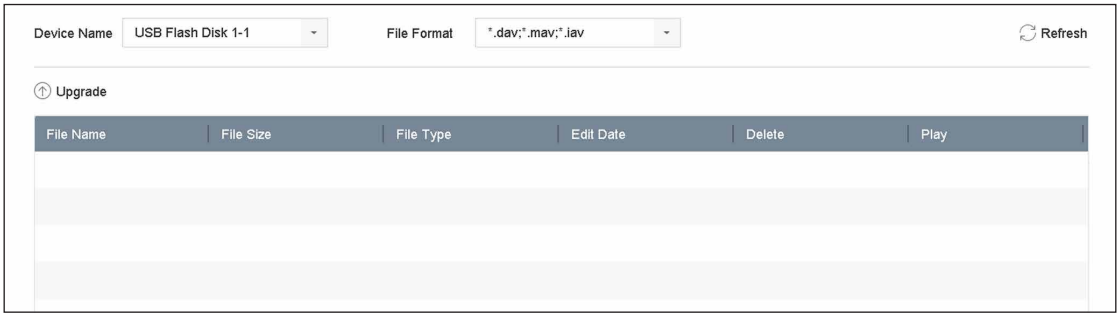

図 15-11 ローカルアップグレード

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。

15.7.2 FTP によるアップグレード

本機を使用する前に

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。

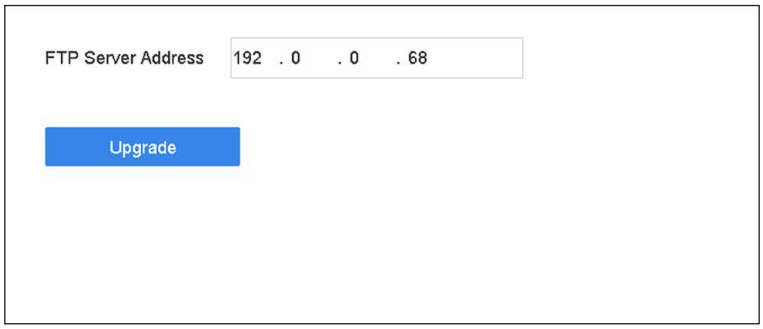

図 15-12 FTP アップグレード

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。

15.7.3 Guarding Vision によるアップグレード

本機は Guarding Vision にログインした後、定期的に Guarding Vision 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。

本機を使用する前に

本機 Guarding Vision 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、Guarding Vision 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。

15.8 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。

本機を使用する前に

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**

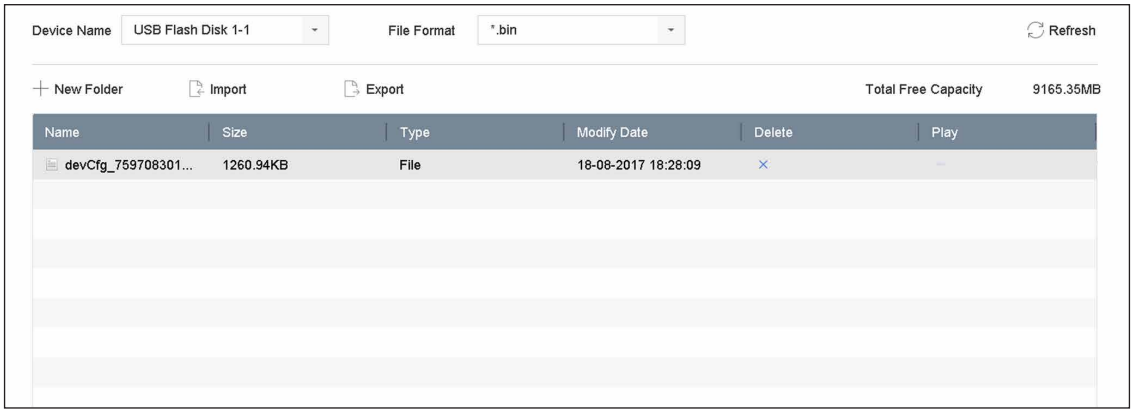

図 15-13 インポート / エクスポート設定ファイル

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。

15.9 ログの管理

15.9.1 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**

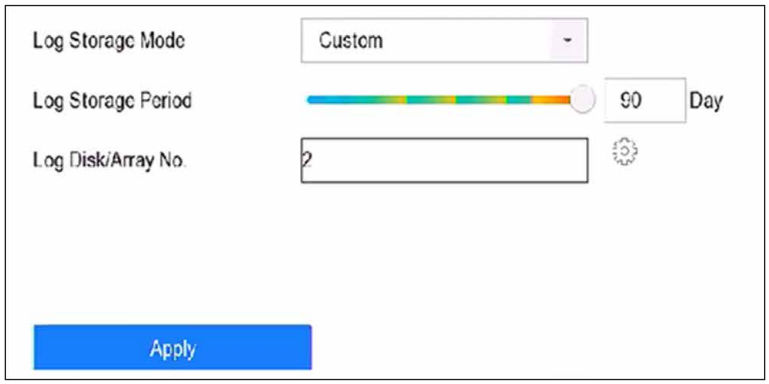

図 15-14 クラウドストレージ

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。

15.9.2 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 15-15 ログ検索インタフェース

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。

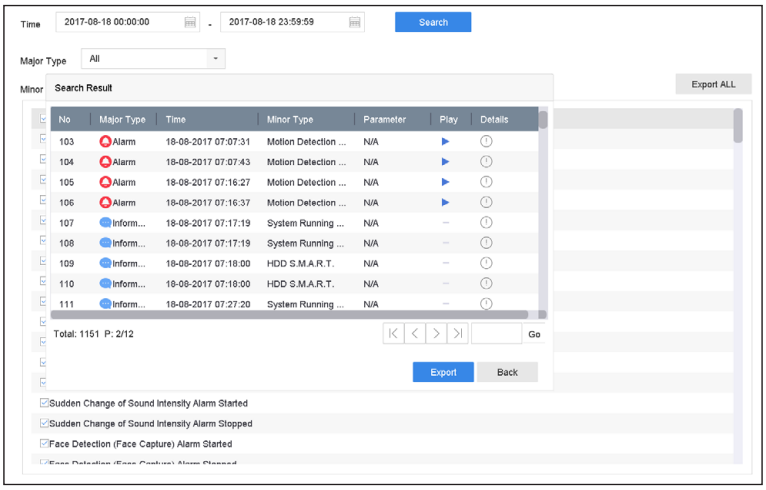

図 15-16 ログ検索結果

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。

15.9.3 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**

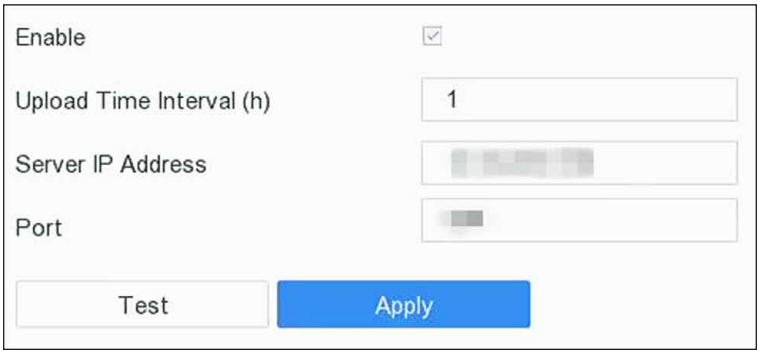

図 15-17 ログサーバーの設定

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。

15.9.4 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。

本機を使用する前に

- 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**

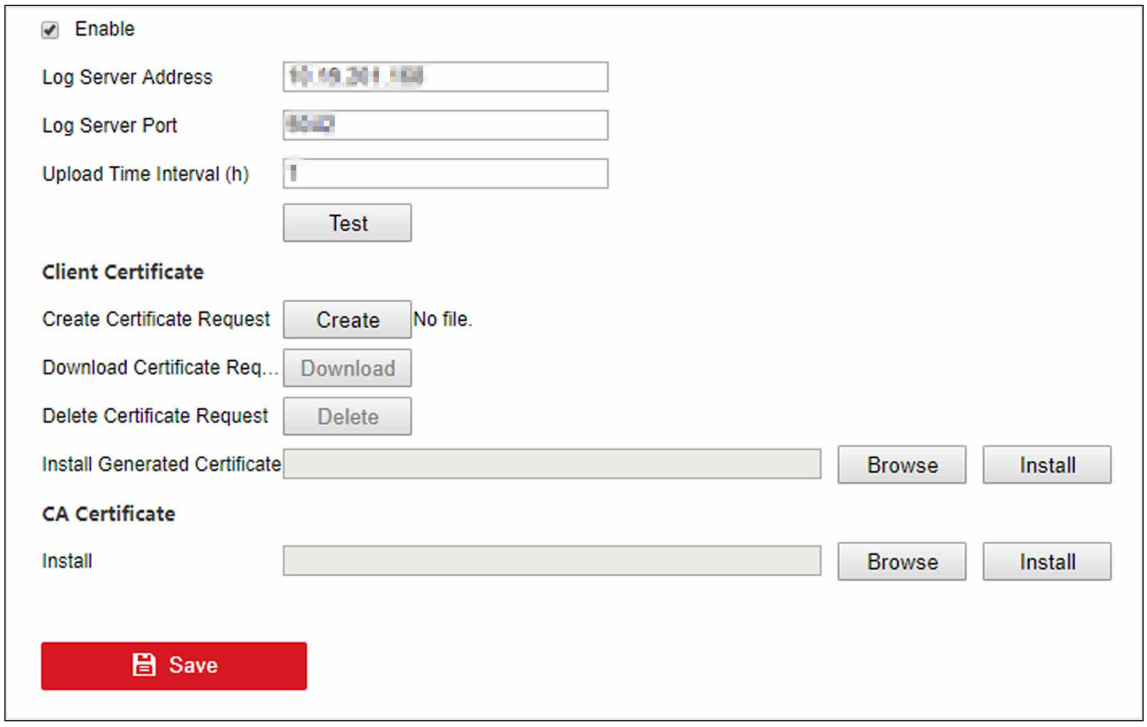

図 15-18 一方向認証

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。

15.9.5 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。

本機を使用する前に

- 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**

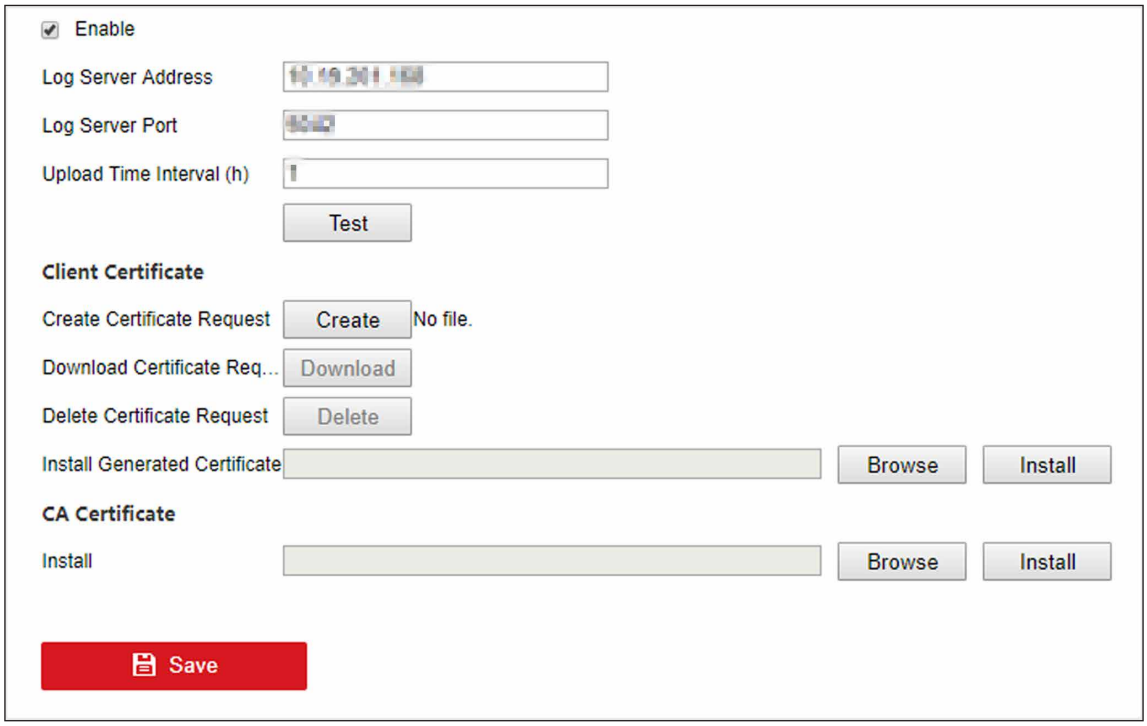

図 15-19 双方向認証

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。

15.10 初期設定の復元

ステップ

1. 次の順に進みます。**Maintenance → Default**

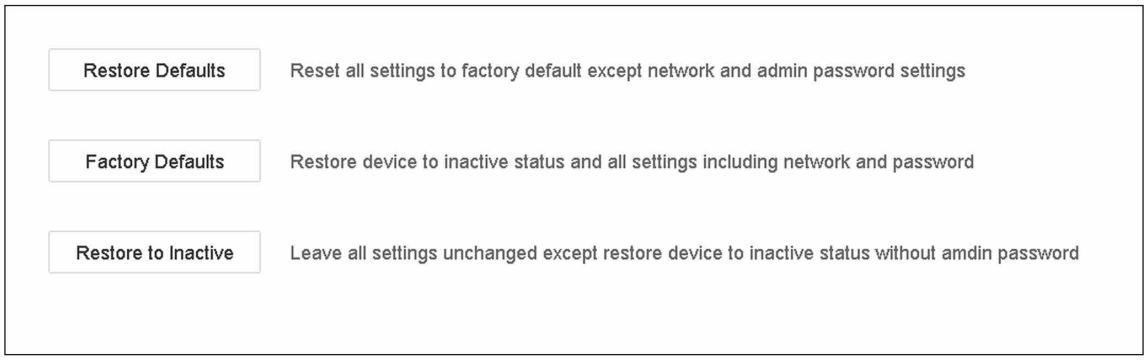

図 15-20 初期設定の復元

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。

15.11 自動メンテナンス

本機はメンテナンスプランにしたがって、自動的に再起動します。

ステップ

1. 次の順に進みます。**Maintenance → System Service → System Service → Device Auto Maintenance**
2. **Enable** にチェックを入れます。
3. **Maintenance Time** を設定します。

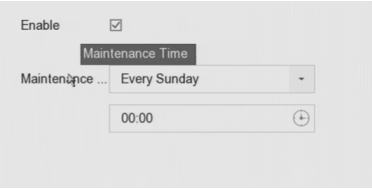

図 15-21 自動メンテナンス

4. **Apply** をクリックします。

15.12 セキュリティ管理

15.12.1 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** クリックして、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。

注意

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。

15.12.2 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**

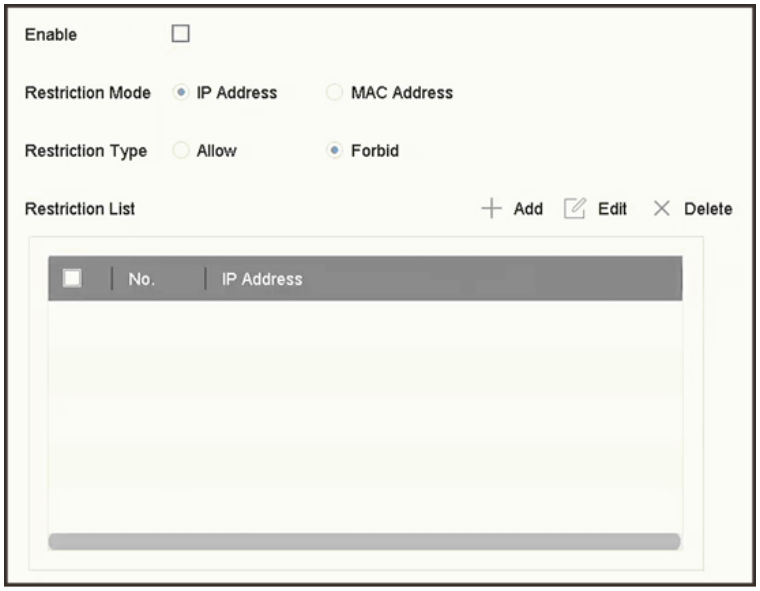

図 15-22 アドレスフィルター

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。

15.12.3 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 15-23 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。

15.12.4 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

15.12.5 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。

15.12.6 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**

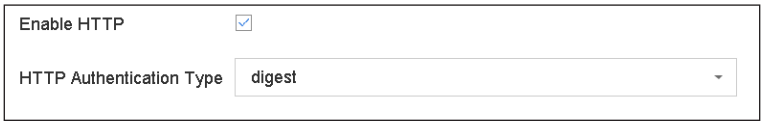

図 15-24 HTTP 認証

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。

15.12.7 HTTP/ ウェブダイジェストアルゴリズム

HTTP/Web digest algorithm 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/web digest 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

15.12.8 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 ブラウザーから画像 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

15.12.9 シリアルポート認証サービス

シリアルポートで機器情報の取り込みや本機の制御が可能です。シリアルポート認証サービスは、シリアルポートを使用する際の認証を提供するサービスです。
Web ブラウザーで次の順に進み、シリアルポート認証サービスの有効 / 無効を設定します。
Configuration → System → Security → Security Service

Service Close Time

シリアルポート認証サービスを一定期間停止します。例：**Service Close Time** が 30 と設定され場合、シリアルポート認証サービスは 30 日間停止されます。また、30 日経過すると、シリアルポート認証サービスが有効になります。

第 16 章 付録

16.1 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。

16.2 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 16-1 通信マトリックス

16.3 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 16-2 デバイスコマンド

16.4 よくある質問

16.4.1 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？

理由

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。

16.4.2 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？

理由

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。

16.4.3 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？

理由

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。

16.4.4 再生画質を向上させる方法は？

理由

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。

16.4.5 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。

16.4.6 再生時のタイムラインが一定でないのはなぜですか？

理由

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。

16.4.7 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？

理由

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。

16.4.8 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？

理由

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ます。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。

16.4.9 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？

理由

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る。

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。

16.4.10 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？

理由

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。

16.4.11 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？

理由

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 3、短 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。

16.4.12 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？

理由

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。

16.4.13 動画の音質が良くないのですが？

理由

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