



ネットワークビデオレコーダー

ユーザーマニュアル

法的情報

©2023 Hangzhou Hikvision Digital Technology Co. Ltd.がすべての権利を保有しています。

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。本マニュアルの最新版は、Hikvisionのウェブサイトからご覧ください。(<https://www.hikvision.com/>)。

本製品をサポートする訓練を受けた専門家の指導と支援を受けながら、本マニュアルを使用してください。

商標について

HIKVISION およびその他のHikvisionの商標およびロゴは、さまざまな管轄区域におけるHikvisionの財産です。

その他、記載されている商標およびロゴは、それぞれの所有者の財産です。

HDMITM
HIGH-DEFINITION MULTIMEDIA INTERFACE

: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、「現状のまま」かつ「すべての欠陥および誤りを含む」状態で提供されています。Hikvisionは、商品性、満足のいく品質、特定目的への適合性を含むがこれに限定されない、明示または黙示の保証を一切行いません。本製品の使用は、お客様ご自身の責任において行われるものとします。Hikvisionがそのような損害や損失の可能性を知らされていたとしても、本製品の使用に関連し、特に事業利益の損失、事業の中断、またはデータの損失、システムの破損、文書の損失に対する損害など、契約違反、不法行為（過失を含む）、製品責任、またはその他のいずれに基づいても、いかなる特別、必然、付随的、間接損害についても、Hikvisionがお客様に責任を負うことはないものとします。

お客様は、インターネットの性質上、固有のセキュリティリスクがあることを認め、Hikvisionはサイバー攻撃、ハッカー攻撃、ウイルス感染、またはその他のインターネットセキュリティリスクに起因する異常動作、プライバシー漏洩またはその他の損害について一切の責任を負いません。ただし、Hikvisionは必要に応じて適時に技術サポートを提供します。

お客様は、本製品をすべての適用法に従って使用することに同意し、お客様の使用が適用法に適合していることを確認する責任を負うものとします。

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を推奨されます。

- 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



本製品および（該当する場合）付属のアクセサリには「CE」のマークが付いており、EMC指令2014/30/EU、LVD指令2014/35/EU、RoHS指令2011/65/EUの下でリストされた該当する整合欧州規格に準拠しています。



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。

シリーズ	モデル
DS-7100NI-Q1	DS-7104NI-Q1
	DS-7108NI-Q1
DS-7100NI-Q1/P	DS-7104NI-Q1/4P
	DS-7108NI-Q1/8P
DS-7100NI-Q1/M	DS-7104NI-Q1/M
	DS-7108NI-Q1/M
DS-7100NI-Q1/P/M	DS-7104NI-Q1/4P/M
	DS-7108NI-Q1/8P/M
DS-7600NI-K1	DS-7604NI-K1
	DS-7608NI-K1
	DS-7616NI-K1
DS-7600NI-K1/P	DS-7604NI-K1/4P
	DS-7608NI-K1/8P
DS-7600NI-Q1	DS-7604NI-Q1
	DS-7608NI-Q1
	DS-7616NI-Q1
DS-7600NI-Q1/P	DS-7604NI-Q1/4P
	DS-7608NI-Q1/8P
DS-7600NI-Q2	DS-7608NI-Q2
	DS-7616NI-Q2
DS-7600NI-Q2/P	DS-7608NI-Q2/8P
	DS-7616NI-Q2/16P
DS-7600NI-K2	DS-7608NI-K2
	DS-7616NI-K2
	DS-7632NI-K2

ネットワークビデオレコーダー ユーザーマニュアル

シリーズ	モデル
DS-7600NI-K2/P	DS-7608NI-K2/8P
	DS-7616NI-K2/16P
	DS-7632NI-K2/16P
DS-7700NI-K4	DS-7708NI-K4
	DS-7716NI-K4
	DS-7732NI-K4
DS-7700NI-K4/P	DS-7708NI-K4/8P
	DS-7716NI-K4/16P
	DS-7732NI-K4/16P
DS-7700NI-Q4	DS-7708NI-Q4
	DS-7716NI-Q4
DS-7700NI-Q4/16P	DS-7708NI-Q4/8P
	DS-7716NI-Q4/16P
DS-8600NI-Q8	DS-8608NI-Q8
	DS-8616NI-Q8

記号について

本書で使用する記号は、次のように定義されています。

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

安全上のご注意

- すべてのパスワードおよびその他のセキュリティセ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。
- 本機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、異音が生じたらすぐに電源を切り、電源ケーブルを抜いて、サービスセンターへご連絡ください。
- UPSと併用し、HDDはなるべく工場出荷時の推奨品を使用してください。
- 本機には、コイン/ボタン電池が使用されています。電池を飲み込むと、わずか2時間で体内に重度の火傷を負い、死に至る可能性があります。
- 本機は、子供がいる可能性のある場所での使用には適していません。
- 注意：異なる種類の電池と交換した場合、爆発する危険性があります。
- 異なる種類の電池と交換すると、安全装置が無効になることがあります（例：一部のリチウム電池の場合）。
- バッテリーを火や高温のオープンに入れたり、機械的に押しつぶしたり、切断したりすると、爆発する恐れがあります。
- 爆発や引火性液体・気体の漏洩の恐れがあるため、極端に高温の場所に電池を放置しないでください。
- 電池を極端に低い気圧の場所に置くと、爆発したり、可燃性の液体やガスが漏れたりすることがありますのでご注意ください。
- 使用済みの電池は、説明書に従って廃棄してください。
- ファンブレードやモーターに体の一部を近づけないでください。修理の際は、電源を切ってください。
- モーターに近づかないでください。修理の際は、電源を切ってください。

予防と注意点

機器を接続し操作する前に、以下の注意事項をご確認ください。

- 本機は屋内専用です。風通しがよく、ほこりのない、液体のない環境に設置してください。
- レコーダーがラックや棚に正しく固定されていることを確認してください。落下などにより大きな衝撃を受けると、レコーダー内の精密電子機器を破損させる原因となります。
- 機器に水滴や水がかからないようにしてください。また、花瓶など、液体の入った物を機器の上に置かないでください。
- ろうそくなどの火を機器の上に置かないでください。
- 新聞紙、テーブルクロス、カーテンなどで換気口を覆い、換気を妨げないでください。ベッド、ソファ、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、電池ホルダ内の電池（複数）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示します。
- - 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示します。
- 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 Dongle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でください。
- 本機が45℃以上で動作している場合、またはS.M.A.R.T.のHDD温度が記載値を超えている場合は、本機を涼しい環境で動作させるか、HDDを交換してS.M.A.R.T.のHDD温度を記載値以下にするようにしてください。

目次

第 1 章 スタートアップ	1
1.1 本機の起動	1
1.2 ログイン	2
1.2.1 アンロックパターンの設定	2
1.2.2 アンロックパターンでログイン	3
1.2.3 パスワードでログイン	3
第 2 章 ライブビュー	5
2.1 GUIの紹介	5
2.2 PTZコントロール	6
2.2.1 PTZパラメータの設定	6
2.2.2 PTZコントロールパネルの紹介	8
2.2.3 プリセットのカスタマイズ	8
2.2.4 パトロールのカスタマイズ	8
2.2.5 パターンのカスタマイズ	9
第 3 章 再生	10
3.1 GUIの紹介	10
3.2 通常再生	10
3.3 イベント再生	12
3.4 バックアップクリップ	13
第 4 章 ファイル検索	14
第 5 章 設定（イージーモード）	15
5.1 システム設定	15
5.1.1 全般	15
5.1.2 ユーザー	16
5.1.3 異常	18

5.2 ネットワーク設定	19
5.2.1 全般	19
5.2.2 Hik-Connect	19
5.2.3 電子メール	21
5.3 カメラの管理	22
5.3.1 ネットワークカメラ	22
5.3.2 OSDの設定	26
5.3.3 イベント	27
5.4 録画管理	29
5.4.1 ストレージデバイス	29
5.4.2 録画スケジュールの設定	30
5.4.3 録画パラメータの設定	32
第 6 章 設定（エキスパートモード）	33
6.1 システム設定	33
6.1.1 全般	33
6.1.2 ライブビュー	35
6.1.3 ユーザー	37
6.2 ネットワーク設定	37
6.2.1 TCP/IP	37
6.2.2 DDNS	38
6.2.3 NAT	39
6.2.4 NTP	40
6.2.5 ログサーバーの設定	40
6.2.6 ポート（その他の設定）	42
6.2.7 ISUP	44
6.2.8 Hik-Connect	45
6.2.9 電子メール	45
6.3 カメラの管理	45

6.3.1 ネットワークカメラ	45
6.3.2 ディスプレイの設定	53
6.3.3 プライバシーマスク	54
6.4 イベント設定	55
6.4.1 通常イベント	55
6.4.2 境界保護	59
6.4.3 その他のイベント	62
6.4.4 アーミングスケジュールの設定	62
6.4.5 アラームリンケージアクションの設定	63
6.5 録画管理	66
6.5.1 録画スケジュールの設定	66
6.5.2 録画パラメータの設定	68
6.5.3 ストレージデバイス	69
6.5.4 ストレージモードの設定	71
6.5.5 高度な設定	72
第 7 章 メンテナンス	73
7.1 初期設定を復元する	73
7.2 ログを検索する	73
7.3 システムサービス	73
7.4 デバイスマンテナンス	74
7.4.1 スケジュールの再起動	74
7.5 アップグレード	75
7.5.1 ローカルアップグレード	75
7.5.2 オンラインアップグレード	75
第 8 章 アラーム	76
8.1 イベントヒントの設定	76
8.2 アラームセンターでアラームを見る	76

第 9 章 Webオペレーション	77
9.1 紹介	77
9.2 ログイン	77
9.3 ライブビュー	78
9.4 再生	78
9.5 設定	79
9.6 ログ	79
第 10 章 付録.....	80
10.1 用語集	80
10.2 通信マトリックス	81
10.3 デバイスコマンド	81

第 1 章 スタートアップ

1.1 本機の起動

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、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。

ご使用の前に

本機に電源を入れます。

ステップ

1. 言語を選択します。
2. **Apply**をクリックします。
3. **Password**と**Confirm Password**に同じパスワードを入力してください。



警告

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。

4. 本機に接続されているネットワークカメラ（複数可）を起動します。
 - **Use the Device Password**にチェックを入れ、本機のパスワードを使用して、非アクティブなネットワークカメラ（複数可）を有効にすることができます。
 - **Camera Activation Password**にパスワードを入力して、ネットワークカメラ（複数可）を起動します。
5. **Activate**をクリックします。

The screenshot shows a web interface for setting up the device. It has a dark background with light-colored text. The fields are as follows:

- *User Name: admin
- *Password: [text input field]
- *Confirm Password: [text input field]
- *Camera Activation Password: [text input field]
- Below the Camera Activation Password field is a checkbox labeled "Use the Device Password" which is checked.

図 1-1 起動

次に行うことは

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場合、パスワード再設定メール、Hik-Connect、セキュリティ質問の3つの方法で再設定することができます。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。詳しくは[パスワード再設定メールの設定](#)と[Hik-Connect](#)を参照してください。
- ・ アンロックパターンについて、詳しくは[アンロックパターンの設定](#)を参照してください。
- ・ 全般的なシステムパラメータについて、詳しくは[全般](#)を参照してください。
- ・ 全般的なネットワークパラメータについて、詳しくは[全般](#)を参照してください。
- ・ ストレージデバイスの設定について、詳しくは[ストレージデバイス](#)を参照してください。
- ・ ネットワークカメラの追加について、詳しくは[ネットワークカメラ](#)を参照してください。
- ・ プラットフォームの設定について、詳しくは[Hik-Connect](#)を参照してください。

1.2 ログイン

1.2.1 アンロックパターンの設定

管理者ユーザーは、アンロックパターンを使用してログインできます。本機の起動後にアンロックパターンの設定ができます。

ステップ

1. マウスを使って、画面上の9つのドットの間にパターンを描画します。パターンが完成したらマウスを離します。



メモ

- ・ パターンでは、少なくとも4つのドットを使用します。
- ・ 各ドットは一度しか結ぶことができません。

2. もう一度同じパターンを描画して確認します。

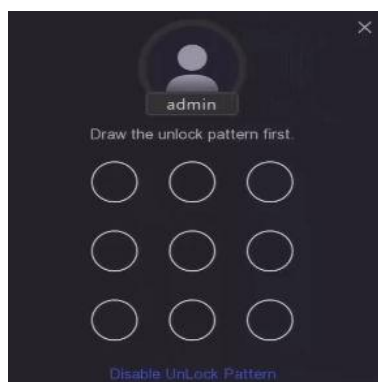


図 1-2 アンロックパターンの設定

2つのパターンが一致すると、そのパターンは正常に設定されます。

1.2.2 アンロックパターンでログイン

ステップ

1. ライブビュー上でマウスを右クリックします。

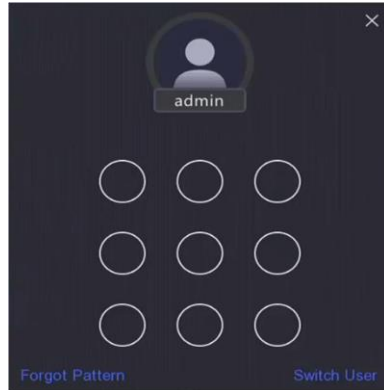


図 1-3 アンロックパターンの描画

2. あらかじめ設定されたパターンを描いて、メニュー操作に入ります。

メモ

- パターンを忘れてしまった場合、**Forgot My Pattern**または**Switch User**をクリックして、パスワードでログインします。
 - 間違ったパターンを5回以上描画した場合、自動的に通常のログインモードに切り替わります。
-

1.2.3 パスワードでログイン

本機がログアウトしている場合、メニューなどの操作を行う前にログインする必要があります。

ステップ

1. **User Name**を選択します。

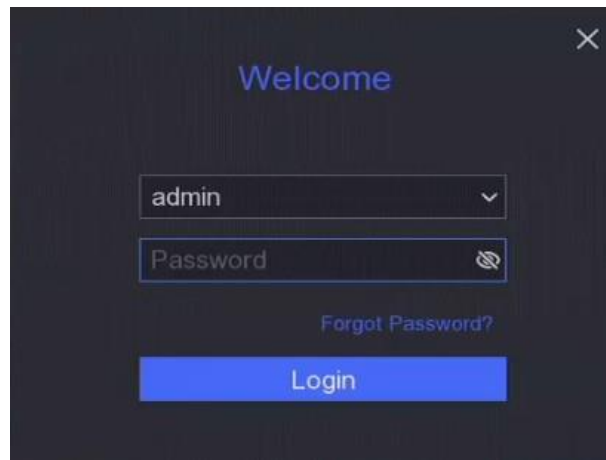


図 1-4 ログインインターフェース

2. パスワードを入力します。
3. **Login**をクリックします。



メモ

- 管理者パスワードを忘れてしまったときは**Forgot Password**をクリックすると、パスワードがリセットされます。
- 間違ったパスワードを7回入力すると、現在のユーザーアカウントは60秒間ロックされます。

第2章 ライブビュー

2.1 GUIの紹介

- 左上の隅にある**Target Detection**をクリックし、またはを選択すると、指定したライブターゲット検知結果を表示します。結果の詳細については、**View More**をクリックしてください。

メモ

- Target Detection**は一部の機種のみ対応しています。
- Target Detection**はHDD装着時に有効です。
- は、動体検知、ラインクロッシング検知、侵入検知、顔検知で有効です。
- 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。
- をクリックするとフルスクリーンモードになります。
- カメラ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。
- カメラのライブビュー画面を、ある画面から目的の画面へドラッグして変更できます。
- 上下にスクロールすると、前画面／次画面に切り替わります。
- カメラにカーソルを合わせると、ショートカットメニューが表示されます。



図 2-1 ショートカットメニュー

表 2-1 ショートカットメニューの説明

ボタン	説明
	直近の5分間に録画した動画の再生を開始します。
	デジタルズームズームイン時間を調整し、目的のエリアを表示します。
	このボタンをクリックしてPTZコントロールモードに入ります。
	ライブビューオーディオのオン／オフを切り替えます。
	ビデオストリームを切り替えます。
	ルールフレームとターゲットフレームを表示します。
	画面サイズに応じて、画像表示効果を調整する。

- ライブビューのインターフェースでは、各カメラの画面右上にアイコンが表示され、カメラの録画ステータスやアラームステータスが表示されます。

表 2-2 アイビューアイコンの説明

アイコン	説明
	アラーム（通常イベント、スマートイベント）
	録画

- マウスを右クリックすると、ショートカットメニューが表示されます。

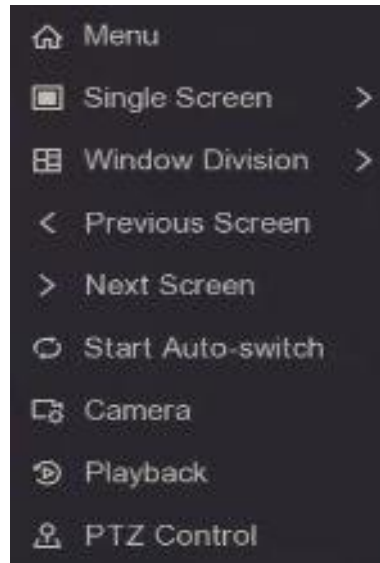


図 2-2 右クリックのショートカットメニュー

2.2 PTZコントロール

2.2.1 PTZパラメータの設定

PTZカメラを制御する前に、PTZパラメータを設定する必要があります。

ステップ

- ライブビューでカメラをプレビューし、ショートカットメニューの  をクリックします。



図 2-3 PTZ設定

2. をクリックします。
3. PTZカメラのパラメーターを設定します。

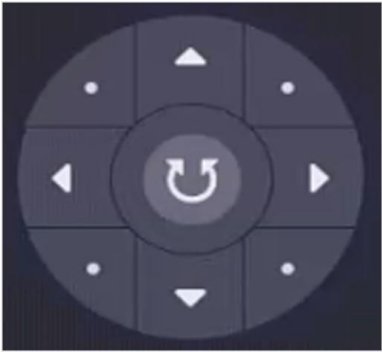
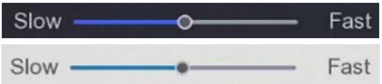
メモ

すべてのパラメータは、PTZカメラと同じにする必要があります。

4. **OK** をクリックします。

2.2.2 PTZコントロールパネルの紹介

表 2-3 PTZパネルの説明

アイコン	説明
	方向ボタン、オートサイクルボタン。
	PTZの移動速度。
	ズーム-/+
	フォーカス-/+
	アイリス-/+

2.2.3 プリセットのカスタマイズ

イベント発生時にPTZカメラが指し示す場所をあらかじめ設定します。

ステップ

1. ライブビューでカメラをプレビューし、ショートカットメニューのをクリックします。
2. プリセットリストの中から、目的のプリセットを選択します。
3. 方向ボタンを使用してカメラを任意の場所に移動することができます。ズームやフォーカスは任意に調整します。
4. をクリックします。

次に行うことは

プリセットリストのプリセットをダブルクリックすると、そのプリセットを呼び出すことができます。

2.2.4 パトロールのカスタマイズ

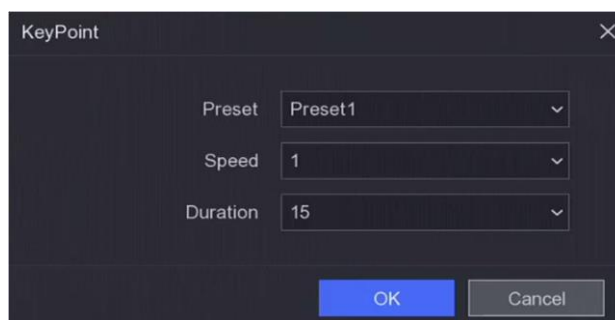
パトロールとは、指定された順序で一連のプリセットから構成される経路です。複数のプリセットをモニタリングするためのダイナミックライブイメージを表示します。

ステップ

1. ライブビューでカメラをプレビューし、ショートカットメニューのをクリックします。

2. **Patrol**をクリックします。
3. 目的のパトロールのをクリックします。
4. をクリックします。
5. キーポイントNo.や1つのキーポイントに留まる時間、パトロールのスピードなどのキーポイントのパラメーターを設定します。このキーポイントはプリセットに対応しています。Preset番号はパトロールで移動中、PTZが従う順序を決めます。**Duration**とは対応するキーポイントに留まる時間を指します。**Speed**ではPTZが1つの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。

図 2-4 パトロールの設定



6. **OK**をクリックします。
7. **Save**をクリックします。

次に行うことは

パトロールを選択しをクリックして呼び出します。PTZカメラは、あらかじめ設定されたパトロール経路に従って移動します。

2.2.5 パターンのカスタマイズ

1つのパターンは、ある位置での移動経路と滞留時間を記録します。パターンを呼び出すと、記録された経路に従ってPTZカメラが動きます。

ステップ

1. ライブビューでカメラをプレビューし、ショートカットメニューのをクリックします。
2. **Pattern**をクリックします。
3. パターンを選択します。
4. をクリックします。
5. 方向ボタン使用してカメラを任意の場所に移動することができます。ズームやフォーカスは任意に調整します。
6. をクリックします。前回のPTZカメラの移動経路がパターンとして記録されます。

次に行うことは

パターンを選択し、をクリックすると呼び出すことができます。あらかじめ設定されたパターンに従って、PTZカメラが移動します。

第 3 章 再生

3.1 GUIの紹介

Playbackに進みます。



図 3-1 再生

表 3-1 再生インターフェースの説明

ボタン	操作	ボタン	操作
	30秒早戻し		30秒早送り
	全画面表示		再生を開始します。
	スロー再生		ファスト再生
	再生スピード		



図 3-2 タイムライン

- ・ タイムライン上にカーソルを置き、タイムラインをドラッグして特定の時刻を設定します。
- ・ 青いバーが表示されている期間は、映像が含まれています。赤いバーは、期間中の映像がイベント映像であることを示します。
- ・ 上下にスクロールすると、タイムラインの拡大・縮小ができます。

3.2 通常再生

通常映像を再生します。

ステップ

1. **Playback**に進みます。
2. カメラリストから1つのカメラを選択します。
3. 再生するカレンダー上の日付を選択します。

メモ

カレンダーの日付の隅にある青い三角形は、利用可能な映像があることを示します。例えば、 は映像あり、 は映像なしを意味します。

4. オプション：再生画面にカーソルを置くと、コントロールバーが表示されます。



図 3-3 コントロールバー

表 3-2 ボタンの説明

ボタン	説明	ボタン	説明
    	ウィンドウ分割、チャンネルをグループ化して再生します。		再生映像をズームイン/ズームアウトします。
	オーディオをオン／オフに切り替えます。		タグを追加します。
	映像のロック／アンロックします。		映像をクリップします。
	人物を含む映像を表示します。		車両を含む映像を表示します。
通常映像をスキップ	  にチェックを入れると、本機は他の映像は非表示にし、再生時に人物や車両を含む映像のみを表示・再生することができます。		ルールフレームとターゲットフレームを表示します。
	画面サイズに応じて、画像表示効果を調整します。		

3.3 イベント再生

イベント再生モードを選択すると、動体検知、ラインクロッシング検知、侵入検知の情報を含む映像を解析してマークします。

ご使用の前に

- カメラのDual-VCAが有効になっていることを確認します。**Configuration → Video/Audio → Display Info. on Stream**の順に進み、カメラのWebブラウザインターフェースからDual-VCAを有効にすることができます。
- 本機のSave VCA Dataが有効になっていることを確認します。**Configuration → Record → Advanced**の順に進み、Save VCA Dataを有効にすることができます。

ステップ

1. **Playback**に進みます。
2. **Event**をクリックします。
3. カメラを選択します。



図 3-4 イベント再生

4. 再生画面にカーソルを置くと、コントロールバーが表示されます。

表 3-3 ボタンの説明

ボタン	説明	ボタン	説明
	タグを追加します。		再生映像をズームイン/ズームアウトします。
	映像をクリップします。		映像のロック／アンロックします。
	検知領域を設定します。		オーディオをオン／オフに切り替えます。

5. をクリックして、ラインクロッシング検知、侵入検知、動体検知の検知エリアを設定します。
6. をクリックして映像を検索します。検知ルールを満たす映像は、赤色でマークされます。
7. をクリックすると、再生ストラテジーを設定します。

Do not Play Normal Videos

この機能を有効にすると、スマート情報のない映像は再生されません。

Normal Video

通常再生速度を設定します。**Do not Play Normal Videos**がチェックされていない場合のみ有効なオプションです。

Play Speed of Smart/Custom Video

スマート情報付き映像の再生速度を設定します。**Do not Play Normal Videos**が有効の場合のみ機能するオプションです。

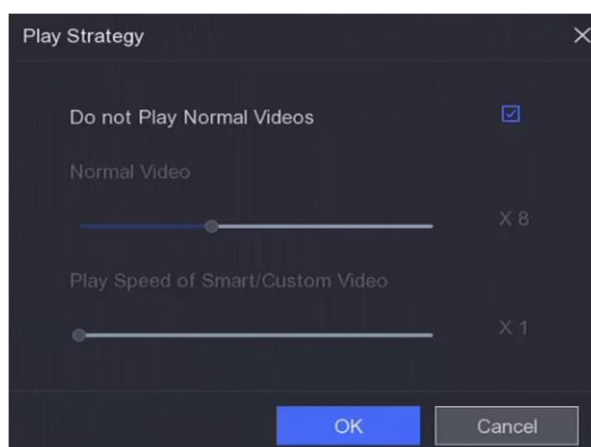


図 3-5 ストラテジーの再生

3.4 バックアップクリップ

再生中に映像をクリップできます。映像クリップをバックアップデバイス（USBメモリーなど）に書き出すことができます。

ご使用の前に

本機にバックアップデバイスを接続してください。

ステップ

1. 再生を開始します。詳しくは通常再生を参照してください。
2.  をクリックします。
3. 開始時刻と終了時刻を設定します。また、タイムバー上のカーソルを調整して、期間を設定することもできます。
4. **Save** をクリックします。
5. バックアップデバイスとフォルダを選択します。
6. **Save** をクリックして、クリップした映像をバックアップデバイスにエクスポートします。

第 4 章 ファイル検索

ステップ

1. **Search**に進みます。

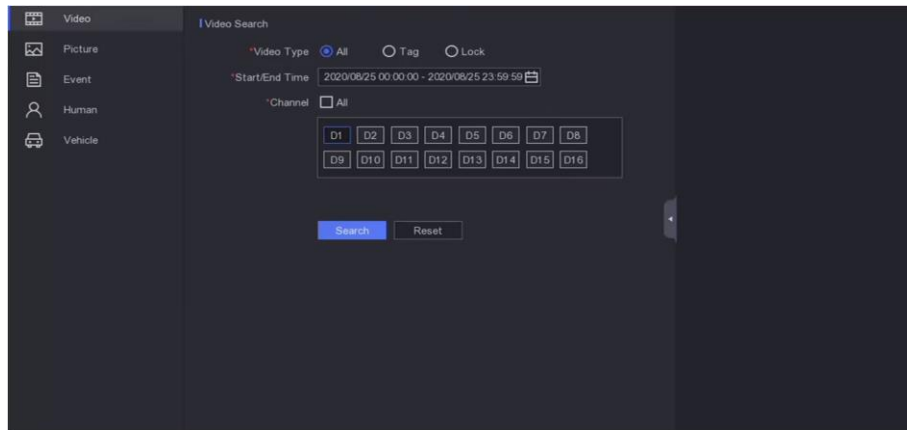


図 4-1 検索

2. 検索タイプ（映像、画像、イベントなど）を選択します。

3. 検索条件を設定します。

4. **Search**をクリックします。

-  をクリックして映像を再生します。
-  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。
- ファイル（複数可）を選択し**Export**をクリックして、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。

第5章 設定（イージーモード）

イージーモードには、基本的な設定が含まれています。**Configuration**に進み、**Easy Mode**をクリックします。

5.1 システム設定

5.1.1 全般

出力解像度やシステム時間などを設定します。

ステップ

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

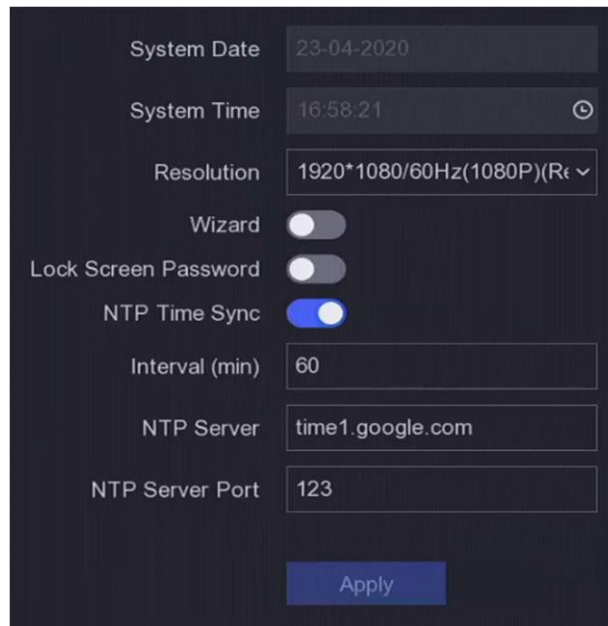


図 5-1 全般設定

2. パラメータは任意に設定します。

Wizard

本機の起動後にウィザードがポップアップします。

Lock Screen Password

画面がロックされている場合は、パスワードの入力が必要です。

NTP Time Sync

Network time protocol (NTP)は、時刻同期のためのネットワーク・プロトコルです。本機をNTP（ネットワークタイムプロトコル）サーバーに接続して、時刻を同期できます。

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。

3. **Apply**をクリックします。

5.1.2 ユーザー

ユーザーの追加

デフォルトのアカウントはAdministratorです。管理者ユーザー名は**admin**です。管理者には、ユーザーの追加、削除、およびユーザーのパラメータを設定する権限があります。ゲストユーザーには、ライブビュー、再生、ログ検索の権限のみあります。

ステップ

1. 次の順に進みます。**Configuration → System → User**
2. **Add**をクリックし、管理者パスワードを確認してください。

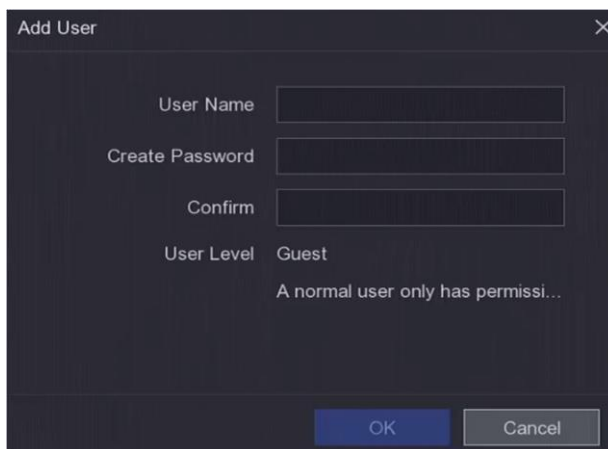


図 5-2 ユーザーの追加

3. ユーザー名を入力します。
4. **Password**と**Confirm**には同じパスワードを入力します。



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。

5. **OK**をクリックします。

  をクリックして、ユーザーを編集／削除することができます。

パスワード再設定用電子メールの設定

ログインパターンやパスワードを忘れた場合、本機は認証コードを含む電子メールをパスワードの再設定に必要な電子メールに送信します。

ステップ

1. 次の順に進みます。 **Configuration → System → User**
2. **Password Resetting Email**をクリックします。
3. 認証のための管理者パスワードを入力します。
4. 電子メールのアドレスを入力します。
5. **OK**をクリックします。

アンロックパターンの編集

管理者ユーザーは、アンロックパターンを使ってログインすることができます。アンロックパターンを変更したり、アンロックパターンを無効にすることができます。

ステップ

1. 次の順に進みます。 **Configuration → User**
2. をクリックします。
3. 管理者パスワードを入力します。
4. **Unlock Pattern**をクリックします。
5. 任意でこの機能のオン／オフを切り替えます。
6. この機能が有効な場合、アンロックパターンを設定します。
 - 1) マウスを使って、画面上の9つのドットの間パターンを描画します。パターンが完成したらマウスを離します。



- ・ パターンでは、少なくとも4つのドットを使用します。
- ・ 各ドットは一度しか結ぶことができません。

- 2) もう一度同じパターンを描画して確認します。
7. **OK**をクリックします。

パスワードの編集

本機のパスワードをお持ちの場合は、新しいパスワードに変更することができます。管理者ユーザーは、他のユーザーのパスワードを変更することができます。

ステップ

1. 次の順に進みます。 **Configuration → User**
2. パスワードを編集します。
 - ゲストユーザーの場合は、旧パスワードと新パスワードを入力します。
 - 管理者ユーザーの場合、をクリックして新しいパスワードを設定します。

3. **OK**をクリックします。



管理者パスワードを変更した場合、以前のアンロックパターンは消去されます。

パスワードのリセット

ログインパターンやパスワードを忘れた場合、パスワードの再設定が可能です。

ステップ

1. パスワードログイン画面の**Forgot Password**をクリックします。
2. プライバシーポリシーに同意される方は、**Next**をクリックしてQRコードをスキャンし、プライバシーポリシーをお読みください。
3. ウィザードに従って、パスワードを再設定します。

5.1.3 異常

アラームセンターの異常イベントのヒントを受信し、異常リンケージアクション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。**Configuration → System → Exception**
2. **オプション**：イベントヒントを設定します。設定したイベントが発生するとアラームセンターにヒントが表示されます。
 - 1) **Event Hint**を有効にします。
 - 2) ローカルメニューの右上にあるをクリックしてアラームセンターに入ります。
 - 3) **Event Type**を選択します。
 - 4) **Set**をクリックして、ヒントとなるイベントを選択します。
3. **Exception Type**を選択します
4. 異常リンケージアクションの**Normal Linkage**と**Trigger Alarm Output**タイプを選択します。

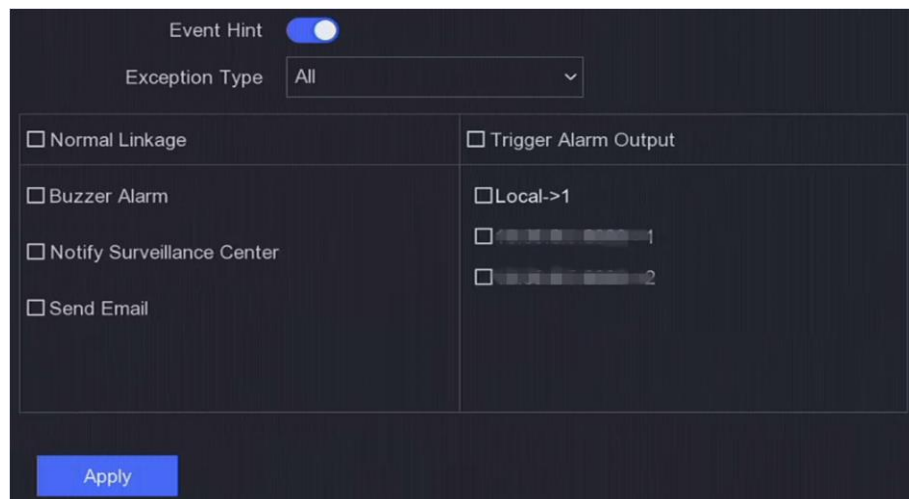


図 5-3 異常

5. **Apply**をクリックします。

5.2 ネットワーク設定

5.2.1 全般

ネットワーク経由で本機を操作する場合は、事前にネットワークの設定を適切に行う必要があります。

ステップ

1. 次の順に進みます。**Configuration → Network → General**

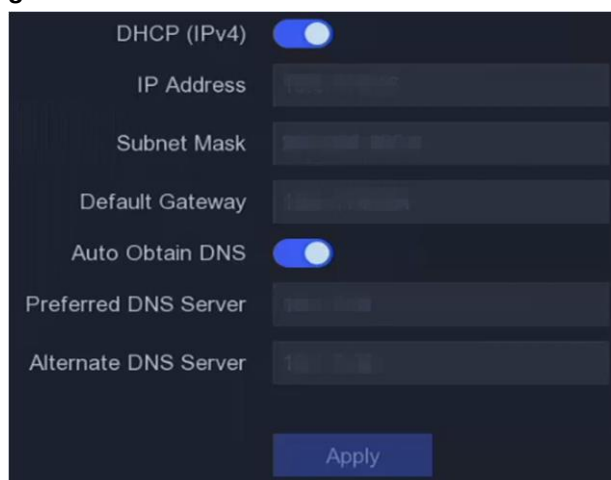


図 5-4 ネットワーク

2. ネットワークパラメータを設定します。

DHCP

DHCPサーバーが利用可能な場合、**DHCP**を有効にして、サーバーからIPアドレスやその他のネットワーク設定を自動的に取得します。

Auto Obtain DNS

DHCPが有効の場合**Auto Obtain DNS**を有効にして、**Preferred DNS Server**と**Alternate DNS Server**を自動的に取得することができます。

3. **Apply**をクリックします。

5.2.2 Hik-Connect

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

ステップ

1. 次の順に進みます。**Configuration → Network → Hik-Connect**
2. **Enable**をオンにします。サービス規約が表示されます。
 - 1) 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。

- 2) 本サービス規約およびプライバシーステートメントに同意される場合、**I have read and agree to Service Terms and Privacy Statement**にチェックを入れます。
- 3) **OK**をクリックします。
3. をクリックして、認証コードを設定します。
4. **オプション：Platform Time Sync**にチェックを入れると、NTPサーバーの代わりにHik-Connectで時刻を同期します。
5. **オプション：Stream Encryption**を有効にします。本機能を有効にすると、リモートアクセスやライブビューで認証コードの入力が必要になります。
6. **オプション：Server IP**を編集します。
7. **オプション：Sub-Stream Self-Adaptive Bitrate**を有効にします。ネットワーク環境が悪い場合は、映像のビットレートを自動的に調整し、スムーズに再生します。
8. 本機をHik-Connectのアカウントで紐づけします。
 - 1) スマートフォンでQRコードを読み取り、Hik-Connectアプリをダウンロードします。
<https://appstore.hikvision.com>からダウンロードすることもできます。または、下記のQRコードを使用します。詳しくはHik-Connectモバイルクライアントユーザーマニュアルを参照ください。



図 5-5 Hik-Connectのダウンロード

- 2) Hik-Connectで本機のQRコードをスキャンして、本機と紐づけします。

メモ

- 本機がすでにアカウントと紐づけされている場合は、**Unbind**をクリックして、現在のアカウントとの紐づけを解除します。
- 左上の隅にある  のQRコードを使用してHik-Connectをダウンロードし、本機と紐づけできます。

9. **Apply**をクリックします。

結果

- 本機がHik-Connectプラットフォームと接続されている場合、**Connection Status**は**Online**となります。
- 本機がHik-Connectのアカウントで紐づけされている場合、**Bind Status**は**Yes**になります。

次に行うことは

Hik-Connect経由で本機にアクセスすることができます。

5.2.3 電子メール

イベント通知を受信する電子メールアカウントを設定します。

ご使用の前に

- 電子メールのSMTPサービスが利用可能であることを確認します。
- ネットワークパラメーターを設定します。詳しくは全般を参照してください。

ステップ

1. 次の順に進みます。**Configuration → Network → Email**

図 5-6 電子メール

2. 電子メールのパラメータを設定します。

Server Authentication

Server Authenticationにチェックを入れ、サーバー認証機能を有効にします。

User Name

SMTPサーバー認証のための電子メール送信者のユーザーアカウントです。

Password

SMTPサーバー認証のための電子メール送信者のパスワードです。

SSL/TLS

(オプション) SMTPサーバーでSSL/TLSが必要な場合、SSL/TLSを有効にします。

Attached Picture

(オプション) イベントが作動した場合、画像をメール添付で送信します。

Sender

送信者の名前です。

Sender's Address

送信者の電子メールアドレスです。

Select Receiver

受信者を選択します。3人まで対応可能です。

Receiver

受信者の名前です。

Receiver's Address

受信者の電子メールアドレスです。



メモ

ネットワークカメラの場合、イベント画像は直接電子メール添付で送信されます。1台のネットワークカメラからは1枚の画像しか送信されません。

3. **オプション** : **Test**をクリックして、テストメールを送信します。
4. **Apply**をクリックします。

5.3 カメラの管理

5.3.1 ネットワークカメラ

デバイスのパスワードでネットワークカメラを追加する

本機と同じパスワードが設定されているネットワークカメラを追加します。

ご使用の前に

- ネットワークカメラが本機と同じネットワークセグメント上にあることを確認します。
- ネットワーク接続が有効で正しいことを確認します。詳しくは**全般**を参照してください。
- ネットワークカメラのパスワードが本機と同じであることを確認します。

ステップ

1. **Configuration** → **Camera** → **IP Camera**の順に進むと、本機と同じネットワークセグメントにあるオンラインカメラが、**Online Device List**に表示されます。

ネットワークビデオレコーダー ユーザーマニュアル

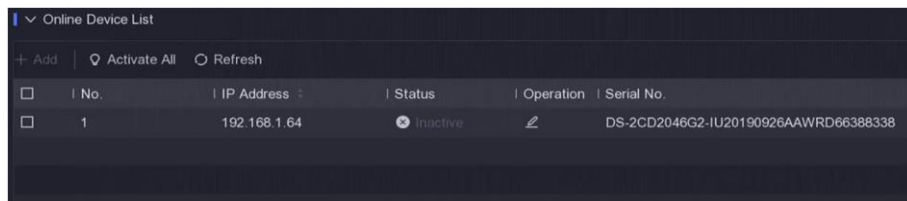


図 5-7 IPカメラ管理インターフェース

2. 目的のネットワークカメラを選択します。
3. **+**をクリックすると、カメラが追加されます。

メモ

カメラが非アクティブの場合、デバイスの起動時に設定したパスワードで、自動的にカメラを起動します。

ネットワークカメラを手動で追加する

ご使用の前に

- ネットワークカメラが本機と同じネットワークセグメントにあることを確認します。
- ネットワーク接続が有効で正しいことを確認します。
- 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. 次の順に進みます。**Configuration → Camera → IP Camera**
2. **Added Device List**の**+**をクリックします。
3. IPアドレス、プロトコル、管理ポートなどのネットワークカメラのパラメータを設定します。
4. **オプション**：**Use Camera Password**を有効にして本機のパスワードを使用すると、ネットワークカメラ（複数可）を追加します。
5. **オプション**：**Add More**をクリックして、ネットワークカメラをもう1台追加します。
6. **Add**をクリックします。

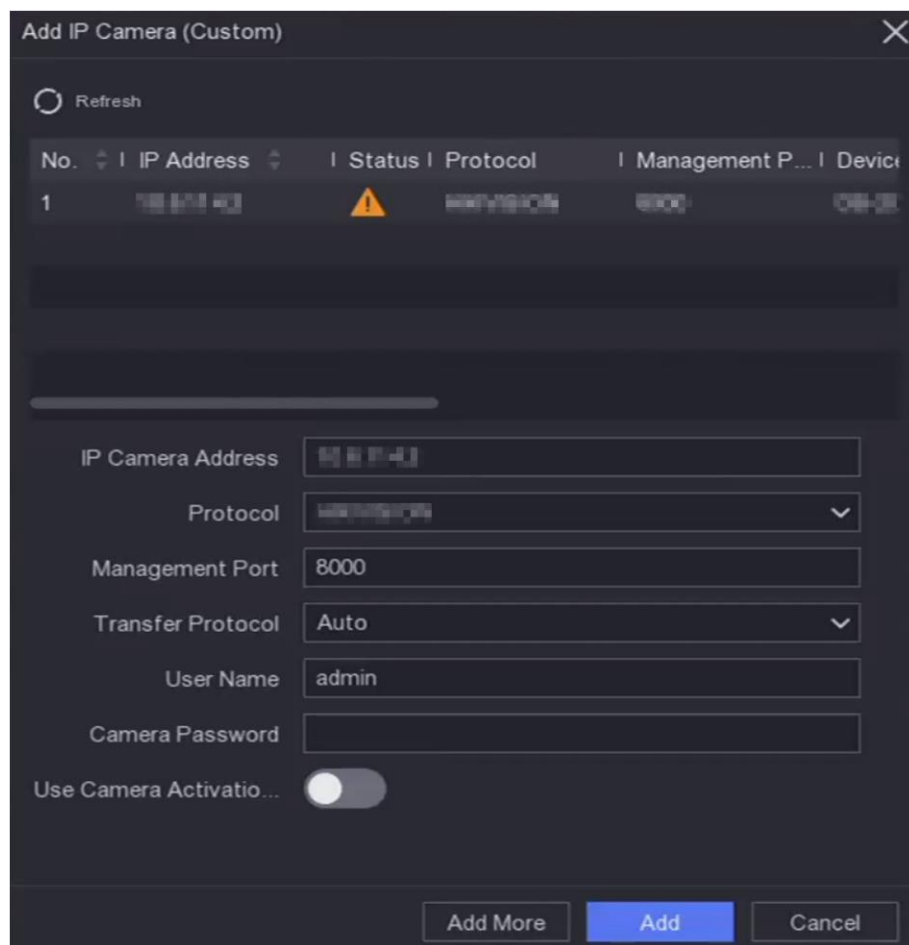


図 5-8 ネットワークカメラの追加

接続されたネットワークカメラを編集する

追加したネットワークカメラのIPアドレスやプロトコル、パラメーターなどを編集できます。

ステップ

1. 次の順に進みます。**Configuration → Camera → IP Camera**
2.  をクリックして、選択したカメラを編集します。

Channel Port

接続機器が複数のチャンネルを持つエンコード機器の場合、チャンネルポート番号を選択すると、接続チャンネルを選択できます。

3. **OK** をクリックします。

チャンネル順の並び換え

チャンネルレイアウトウィンドウは、チャンネル番号順に並んでいます。ウィンドウをドラッグして、カメラ連動チャンネル番号を変更できます。

ステップ

1. 次の順に進みます。**Configuration → Camera → Camera**
2. **Sort Channel**をクリックします。
3. チャンネルウィンドウを任意のチャンネル番号にドラッグします。
4. **Apply**をクリックします。



メモ

チャンネルを振り分けた後、ネットワークカメラに再接続します。

リモート設定

Webブラウザからしか設定できなかったカメラパラメータについては、リモート設定機能により、リモートカメラのパラメータを設定するための操作インターフェースを提供します。

ご使用の前に

カメラが正しく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。**Configuration → Camera → IP Camera**
2. **Remote Settings** をクリックします
3. デバイスリソースが初期化された後、カメラを選択します。
4. カメラのパラメータを設定します。

ネットワークカメラをアップグレードする

ネットワークカメラのアップグレードは、本機から遠隔で行うことができます。

ご使用の前に

- USBフラッシュメモリーを本機に挿入し、ネットワークカメラのアップグレードファームウェアが入っていることを確認してください。
- ネットワークカメラが本機と同じネットワークセグメント上にあることを確認します。
- ネットワーク接続が有効で正しいことを確認します。

ステップ

1. 次の順に進みます。**Configuration → Camera → IP Camera**
2.  をクリックします。
3. **Yes**をクリックして確認します。
4. ストレージデバイスからカメラのアップグレードファームウェアを選択します。

5. **Upgrade**をクリックし、アップグレードを開始します。アップグレードが完了すると、カメラは自動的に再起動します。

高度なカメラのパラメータの設定

カメラのIPアドレス、カメラのパスワードなどの高度なカメラのパラメータを設定できます。

ご使用の前に

- ネットワークカメラが本機と同じネットワークセグメント上にあることを確認します。
- ネットワーク接続が有効で正しいことを確認します。

ステップ

1. 次の順に進みます。**Configuration → Camera → IP Camera**
2. をクリックします。
3. IPアドレス、カメラのパスワードなどのカメラのパラメータを設定します。
4. **Apply**をクリックします。

5.3.2 OSDの設定

カメラのOSD（オンスクリーンディスプレイ）の日时表示形式やカメラ名などの設定ができます。

ステップ

1. 次の順に進みます。**Configuration → Camera → OSD**
2. カメラを選択します。

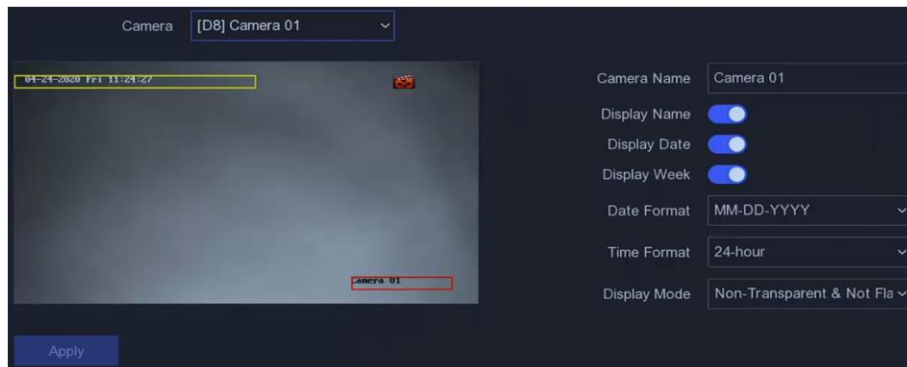


図 5-9 OSD

3. パラメータは任意で設定します。
4. 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の位置を調整できます。
5. **Apply**をクリックします。

5.3.3 イベント

動体検知

動体検知機能により監視領域内の動体を検知し、アラームを発生します。

ステップ

1. 次の順に進みます。**Configuration → Camera → Event → Motion Detection**

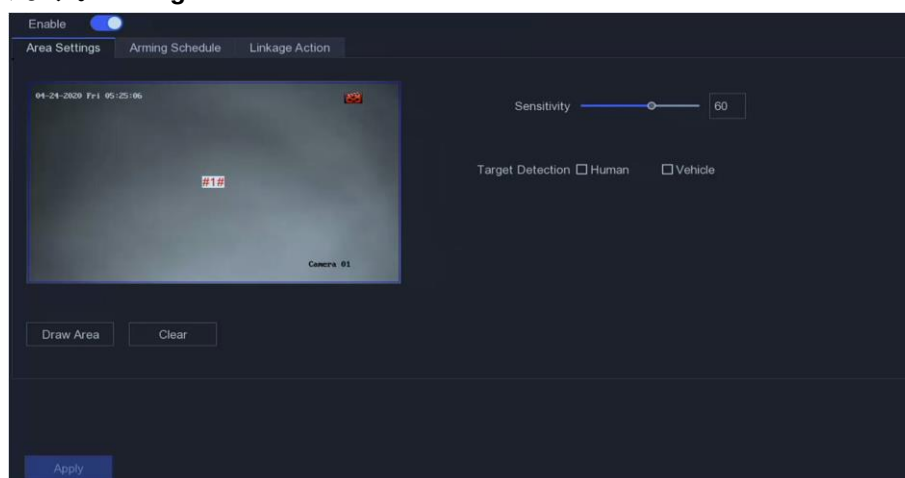


図 5-10 動体検知

2. カメラを選択します。
3. **Enable**をオンにします。
4. 動体検知領域を設定します。
 - **Draw Area**または**Clear**をクリックして、領域を描画したり、クリアしたりできます。最初のエリアは、デフォルトで全画面に設定されています。
 - **Full Screen**をクリックすると動体検知域を全画面に設定できます。プレビューウィンドウ上でドラッグして、動体検知領域を描画できます。
5. **Sensitivity**を調整します。これにより、動体の動きがどの程度でアラームを作動するかをキャリブレーションできます。値が高いほど動体検知しやすくなります。
6. オプション：**Target Detection**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。この機能は一部の機種のみ対応しています。

メモ

本機能は一部の機種のみ対応しています。

7. 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。
8. リンケージアクションを設定します。詳しくは[アラーム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。

アーミングスケジュールの設定

ステップ

1. **Arming Schedule**を選択します。
2. 曜日を選択し、時間帯を設定します。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

時間帯は、繰り返したり、重複したりはできません。

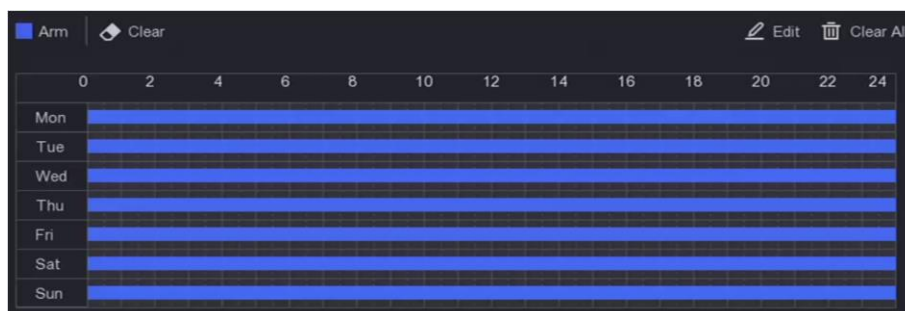


図 5-11 アーミングスケジュールの設定

3. **Apply**をクリックします。

アラームリンケージアクションの設定

アラームリンケージアクションは、アラームや異常が発生したときに起動します。

ステップ

1. **Linkage Action**をクリックします。
2. 通常のリンケージアクション、アラーム出力リンケージアクション、トリガーチャンネルなどを設定します。

Alarm Pop-up Window

アラームが作動すると、ローカルモニターはアラームチャンネルの画像をポップアップ表示します。

Trigger Channelでアラームチャンネル（複数可）を選択する必要があります。

Buzzer Alarm

アラームが作動すると、ビープ音が鳴ります。

Notify Surveillance Center

アラームが作動すると、リモートクライアントソフトウェアに異常信号またはアラーム信号を送信します。

Send Email

アラームが作動すると、アラーム情報を電子メールで送信します。

PTZ Linkage

スマート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）が作動します。

Audio and Light Alarm Linkage

一部のネットワークカメラでは、アラームリンケージアクションを音声アラームまたは点灯アラームに設定できます。



メモ

- 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。
 - 音声や点灯のパラメータを設定する必要がある場合は、Webブラウザでネットワークカメラにログインして設定を行ってください。
-

3. **Apply**をクリックします。

5.4 録画管理

5.4.1 ストレージデバイス

HDDを初期化する

新しく取り付けたハードディスクドライブ（HDD）は、映像や情報の保存に使用する前に初期化する必要があります。

ご使用の前に

本機にHDDを1台以上接続してください。詳しい挿入方法は、クイックスタートガイドを参照してください。

ステップ

1. 次の順に進みます。**Configuration → Record → Storage**
2. HDDを選択します。
3. **Init**をクリックします。

Repair Database

データベースでエラーが発生したHDDを修復します。専門のテクニカルサポートを受けながら操作してください。

ネットワークディスクの追加

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として使用できます。

ステップ

1. 次の順に進みます。**Configuration → Record → Storage**
2. **Add**をクリックします。
3. **NetHDD**を選択します。
4. **Type**は**NAS**または**IP SAN**を設定します。
5. **NetHDD IP**アドレスを入力します。

6. をクリックして、利用可能なディスクを検索します。

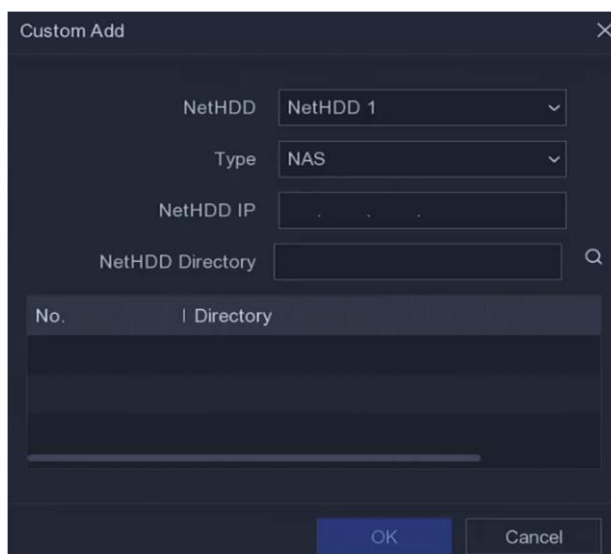


図 5-12 NetHDDの追加

7. リストからNASディスクを選択するか、または手動でNetHDD Directoryに目的のディレクトリまでのパスを入力します。
8. **OK**をクリックします。ストレージデバイス一覧に追加したNetHDDが表示されます。

5.4.2 録画スケジュールの設定

ビデオレコーダーが設定したスケジュールに従って、自動的に録画を開始/停止します。

連続録画を設定する

ステップ

1. 次の順に進みます。**Configuration → Record → Parameter**
2. カメラのメインストリーム／サブストリームの連続録画パラメーターを設定します。
詳しくは[録画パラメーターを設定する](#)を参照してください。
3. 次の順に進みます。**Configuration → Record → Schedule**
4. 録画タイプは**Continuous**を選択します。詳しくは[スケジュールを編集する](#)を参照してください。

イベント録画を設定する

動体検知、ラインクロス検知、侵入検知などで作動する録画を設定します。

ステップ

1. 次の順に進みます。**Configuration → Event → Smart Event**
2. イベント検知を設定し、イベントが発生したときに録画を作動するチャンネル（複数可）を選択します。
3. 次の順に進みます。**Configuration → Record → Parameter**

4. カメラのメインストリーム／サブストリームの連続録画パラメーターを設定します。
詳しくは録画パラメーターを設定するを参照してください。
5. 次の順に進みます。**Configuration → Record → Schedule**
6. 録画の種類は**Event**を選択します。詳しくはスケジュールを編集するを参照してください。

スケジュールを編集する

ステップ

1. 次の順に進みます。**Configuration → Record → Schedule**

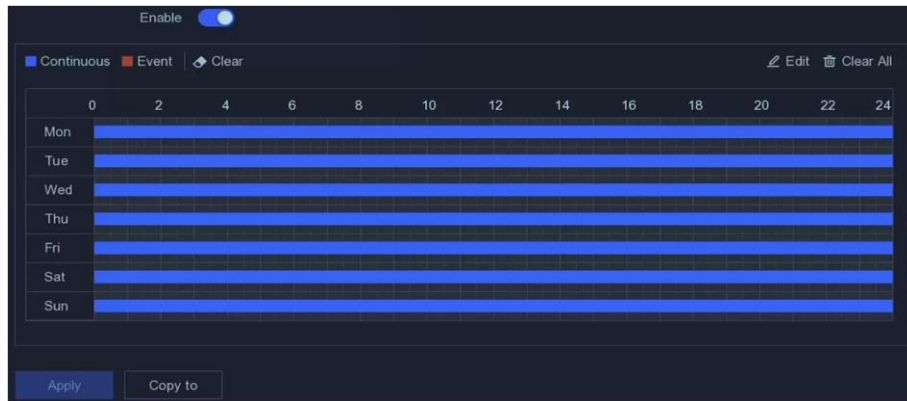


図 5-13 録画スケジュール

Continuous

連続録画が可能です。

Event

イベントで録画が作動します。

2. **Camera No.**でカメラを選択します。
3. **Enable**をオンにします。
4. 録画スケジュールを設定します。

Edit Schedule

- a. **Edit**をクリックします。
- b. **Weekday**で設定する日を選択します。
- c. 終日録画のスケジュールを設定する場合は、**All Day**にチェックを入れ、スケジュールの種類を選択します。
- d. 他のスケジュールを設定する場合は、**All Day**のチェックを外し、**Start/End Time**とスケジュールの種類を設定します。



メモ

1日に最大8つの時間帯を設定できます。その時間帯は互いに重複することはできません。

Draw Schedule

- e. **OK**をクリックすると、設定が保存され、上位メニューに戻ります。
- a. クリックして、スケジュールの種類は**Continuous**または**Event**を選択します。
- b. 表の上で、希望する時間帯にマウスをドラッグしてカラーバーを描画します。

5. **Apply**をクリックします。

5.4.3 録画パラメータの設定

ステップ

1. 次の順に進みます。**Configuration → Record → Parameter**
2. 録画パラメータを設定します。

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、映像の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。

Sub-Stream

サブストリームとは、メインストリームと並行して動作する第二のコーデックのことです。直接録画の画質を落とすことなく、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スマートフォンアプリで独占的に使用されます。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。

Frame Rate

1秒間に何枚のフレームをキャプチャできるかを示します。フレームレートが高いほど、ビデオに動きがある場合に画質を維持するため有利です。

Resolution

画像解像度とは、デジタル画像がどれだけ詳細な情報を保持できるかを示す指標であり、解像度が高いほど詳細な情報が得られます。解像度は、ピクセル列数（幅）×ピクセル行数（高さ）で指定することができます（例：1024×768）。

Bitrate

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



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。

3. **Apply**をクリックします。

第 6 章 設定（エキスパートモード）

Configurationに進み、左下隅にあるExpert Modeをクリックします。

6.1 システム設定

6.1.1 全般

基本設定をする

言語、システム時間、出力解像度、マウスポインターの速度、ロック画面のパスワードなどを設定します。

Configuration → System → General → Basic Settingsの順に進み、任意にパラメータを設定し、Applyをクリックします。

Language

デフォルトの言語はEnglishです。

VGA/HDMI Resolution

出力解像度を選択します。VGA/HDMIディスプレイの解像度と同じである必要があります。

Lock Screen Password

画面がロックされている場合は、認証のためのパスワードの入力が必要です。

Mouse Pointer Speed

マウスポインターの速度を設定します。4つのレベルを設定できます。

Wizard

本機の起動後にウィザードがポップアップします。

Enhanced SVC Mode

Scalable Video Coding（SVC）は、H.264とH.265の規格を拡張したものです。システムのデコード能力が不十分な場合、エンハンストSVCモードでは、オリジナル映像から自動的にフレームを抽出し、映像を表示できます。拡張SVCモードは、SVCに対応したネットワークカメラで有効になります。



メモ

- 拡張SVCモードは、SVCに対応したネットワークカメラで有効になります。
 - 一部のカメラではConfiguration → Camera → Camera → More → Batch Configurationの順に進み、ネットワークカメラのSVC機能を有効にできます。
-

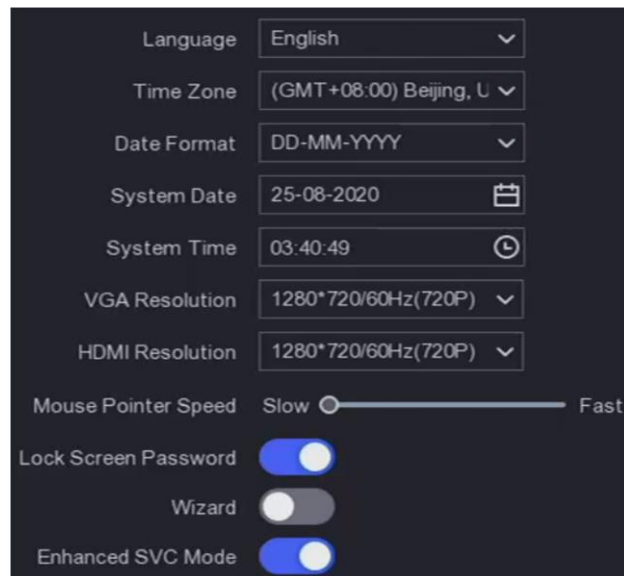


図 6-1 基本設定

DSTを設定する

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。

Configuration → System → General → DST Settingsの順に進み、任意にパラメータを設定し**Apply**をクリックします。

その他の設定をする

デバイス名、ロック画面の時間、出力モードなどを設定します。

Configuration → System → General → More Settingsの順に進み、任意のパラメータを設定し、**Apply**をクリックします。

Device Name

ビデオレコーダー名を編集します。

Device No.

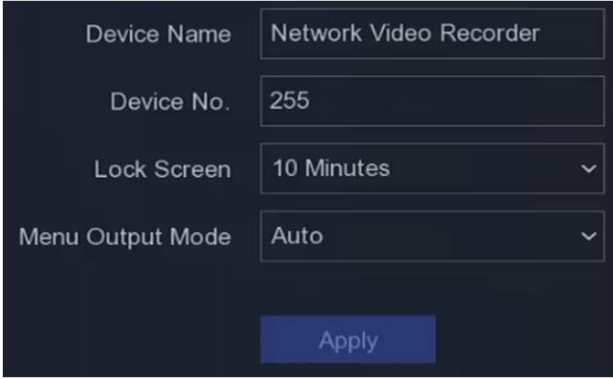
リモコンやネットワークキーボードなどとの接続時に必要な番号です。ビデオレコーダーのシリアルナンバーを編集します。デバイス番号は1～255まであり、初期値は255です。

Lock Screen

ロック画面の終了時間を設定します。

Menu Output Mode

ローカルメニューを表示する出力を選択します。



Device Name	Network Video Recorder
Device No.	255
Lock Screen	10 Minutes
Menu Output Mode	Auto

Apply

図 6-2 その他の設定

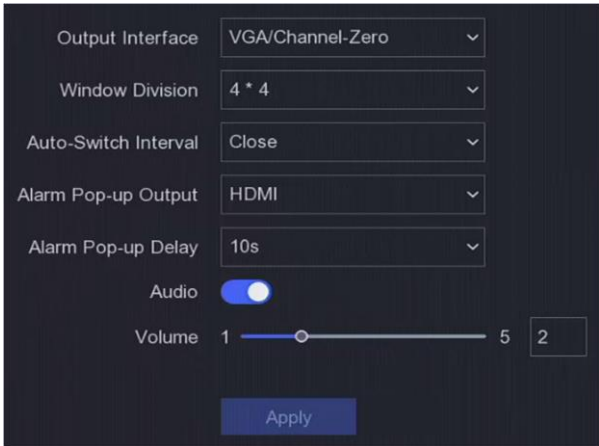
6.1.2 ライブビュー

全般パラメータを設定する

出カインターフェースの設定、音声のミュートやオン、イベント出カインターフェースなどの設定ができます。

ステップ

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



Output Interface	VGA/Channel-Zero
Window Division	4 * 4
Auto-Switch Interval	Close
Alarm Pop-up Output	HDMI
Alarm Pop-up Delay	10s
Audio	☒
Volume	1 <input type="range"/> 5 2

Apply

図 6-3 ライブビュー全般

2. ライブビューのパラメーターを設定します。

Window Division

ライブビューのウィンドウ分割を選択します。

Auto Switch Interval

ライブビューの自動切り替えが有効な場合、次のカメラに切り替えるまでの滞留時間を設定します。

Alarm Pop-up Output

アラーム映像を表示する出力を選択します。

Alarm Pop-up Delay

アラームイベント画像を表示する時間を設定します。

Audio

選択した映像出力の音声出力をオン/オフに切り替えます。

Volume

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

3. **Apply**をクリックします。

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。 **Configuration → System → Live View → View**
2. **Output Interface**を設定します。
3. ウィンドウを選択し、表示したいカメラリストをダブルクリックします。✚は、ウィンドウにカメラが表示されていないことを示します。
4. オプション：  または  をクリックすると、全カメラのライブビューを開始または停止します。
5. **Apply**をクリックします。

チャンネルゼロエンコーディングを設定する

Webブラウザや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。 **Configuration → System → Live View → General**
2. **Video Output Interface**は**Channel-Zero**に設定します。
3. 次の順に進みます。 **Configuration → System → Live View → Channel-Zero**

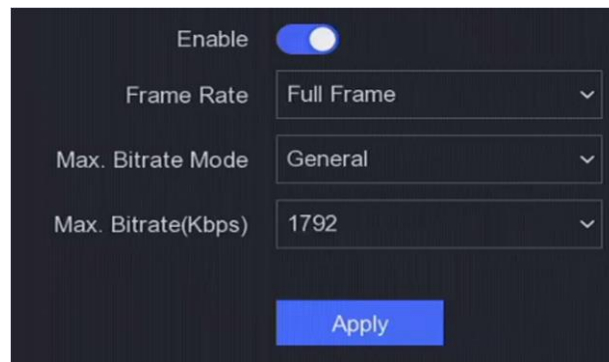


図 6-4 チャンネルゼロ

4. **Enable**をオンにします。
5. **Frame Rate**、**Max. Bitrate Mode**、**Max. Bitrate**を設定します。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。
6. **Apply**をクリックします。

6.1.3 ユーザー

詳しくは[ユーザー](#)を参照してください。

6.2 ネットワーク設定

6.2.1 TCP/IP

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。

ステップ

1. 次の順に進みます。**Configuration → Network → General → TCP/IP**
2. ネットワークパラメータを設定します。

Working Mode

- **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NICタイプ欄で、LAN1またはLAN2を選択します。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。
- **Net-fault Tolerance Mode** : 2枚のNICカードは同じIPアドレスを使用し、Main NICをLAN1またはLAN2に選択します。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します。
- **Load Balance Mode** : 同じIPアドレスを使用し、2枚のNICカードで総帯域の負荷を分担することで、このシステムは2ギガビットのネットワーク容量を提供することが可能です。



Working Modeは一部の機種のみ対応しています。

NICタイプ

任意のNICタイプを選択します。

DHCP

DHCPサーバーが利用できる場合は、**Enable DHCP**にチェックを入れると、そのサーバーからIPアドレスやその他のネットワーク設定を自動的に取得します。

MTU

単一のネットワークトランザクションで通信可能な最大ネットワークレイヤープロトコルデータ単位（MTU）のサイズです。

Obtain DNS Automatically

DHCPにチェックが入っている場合、**Obtain DNS Automatically**にチェックを入れると、**Preferred DNS Server**と**Alternate DNS Server**を取得できます。

3. **Apply**をクリックします。

6.2.2 DDNS

ダイナミックドメインネームサーバー（DDNS）は、動的なユーザーIPアドレスを固定ドメインネームサーバーにマッピングします。

ご使用前に

DynDNS、PeanutHull、NO-IPの各サービスをISPに登録します。

ステップ

1. 次の順に進みます。**Configuration → Network → General → DDNS**

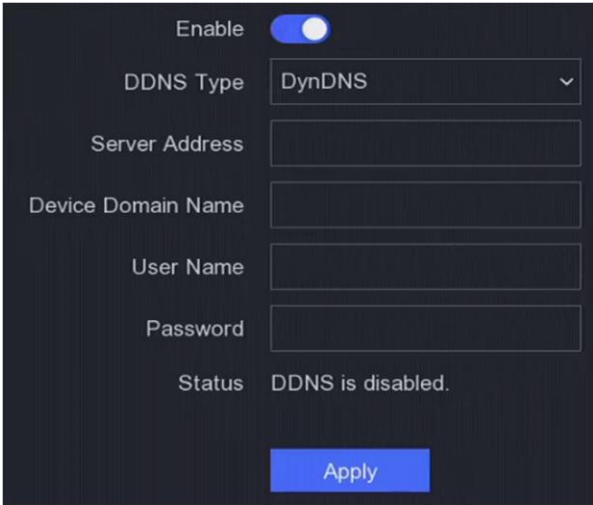


図 6-5 DDNS

2. **Enable**をオンにします。

3. DDNSの種類を選択します。
4. サービスアドレス、ドメイン名などのパラメータを入力します。
5. **Apply**をクリックします。

次に行うことは

StatusでDDNSのステータスを確認します。

6.2.3 NAT

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

ご使用の前に

UPnP™が必要な場合は、ルーターのUPnP™機能を有効にしてください。本機のネットワークワーキングモードがマルチアドレスの場合、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。

ステップ

1. 次の順に進みます。**Configuration → Network → General → NAT**

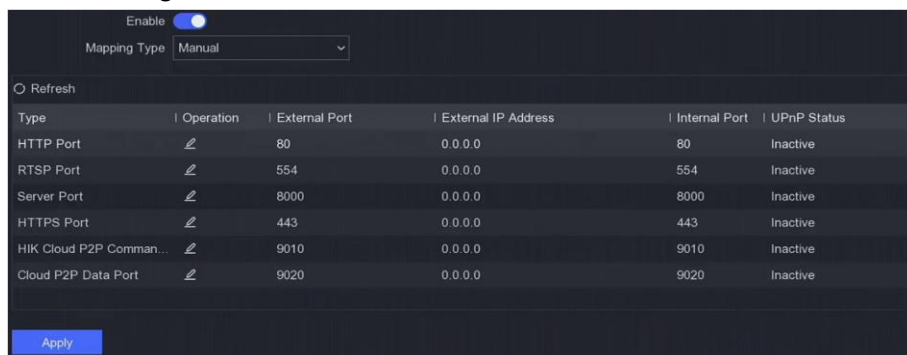


図 6-6 NAT

2. **Enable**をオンにします。
3. **Mapping Type**は**Manual**または**Auto**を選択します。

Auto 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。**Refresh**をクリックすると、ポートマッピングの最新ステータスを取得できます。

Manual 外部ポートの種類を選択します。をクリックして**External Port**を編集します。デフォルトの外部ポート番号を使用できますが、実際の要件に応じて変更できます。**External Port**は、ルーターのポートマッピングのポート番号を示します。

RTSPポート番号は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. 内部ソースポート、外部ソースポートなど、ルーターの仮想サーバーを設定します。仮想サーバーのパラメーターは、お使いのデバイスのポートに対応するものである必要があります。

6.2.4 NTP

お使いのデバイスは、ネットワークタイムプロトコル（NTP）サーバーに接続することで、システムの時刻を正確に把握できます。

ステップ

1. 次の順に進みます。 **Configuration → Network → General → NTP**
2. **Enable**をオンにします。
3. パラメータを入力します。

Interval

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。

4. **Apply**をクリックします。

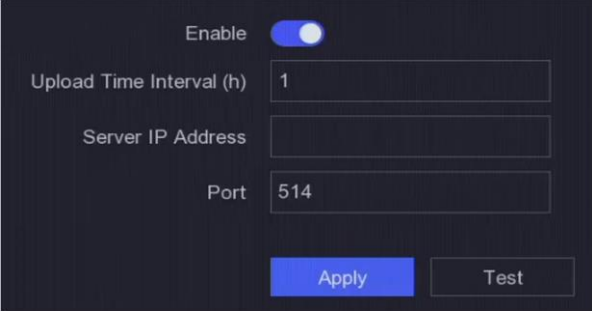
6.2.5 ログサーバーの設定

サーバーにログをアップロード

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。 **Configuration → Network → General → Log Server Settings**



The screenshot shows a configuration window for Log Server Settings. At the top, there is an 'Enable' toggle switch which is currently turned on (blue). Below this, there are three input fields: 'Upload Time Interval (h)' with the value '1', 'Server IP Address' which is empty, and 'Port' with the value '514'. At the bottom of the window, there are two buttons: 'Apply' (highlighted in blue) and 'Test'.

図 6-7 ログサーバーの設定

2. **Enable**をオンにします
3. **Upload Time Interval**、**Server IP Address**、**Port**を設定します。
4. **オプション** : **Test**をクリックして、パラメータが有効かどうかをテストします。
5. **Apply**をクリックします。

一方向認証

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

ご使用の前に

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

ステップ

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

The screenshot shows the 'Log Server Configuration' page. At the top, there's a checkbox labeled 'Enable' which is checked. Below it are three input fields: 'Log Server Address' (containing '192.168.1.100'), 'Log Server Port' (containing '8080'), and 'Upload Time Interval (h)' (containing '1'). A 'Test' button is below these fields. The next section is 'Client Certificate', which includes a 'Create' button (with 'No file.' next to it), a 'Download' button, and a 'Delete' button. Below these is a field for 'Install Generated Certificate' with 'Browse' and 'Install' buttons. The final section is 'CA Certificate', which has an 'Install' button and a 'Browse' button. A large red 'Save' button is at the bottom center of the form.

図 6-8 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をテストします。
4. **Save**をクリックします。

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ブラウザで双方向認証の設定が可能です。

ご使用の前に

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

ステップ

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

The screenshot shows a configuration window for mutual authentication. It includes fields for Log Server Address, Log Server Port, and Upload Time Interval (h). There are buttons for 'Test', 'Create', 'Download', and 'Delete' under the 'Client Certificate' section. There are also 'Browse' and 'Install' buttons for both 'Install Generated Certificate' and 'CA Certificate'. A large red 'Save' button is at the bottom.

図 6-9 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、接続が有効であることをテストします。
9. **Save**をクリックします。

6.2.6 ポート（その他の設定）

さまざまなポートタイプを設定することで、思い通りに関連機能を有効にできます。次の順に進みます。

Configuration → Network → General → More Settings

Alarm Host IP/Port

本機はアラームが作動したとき、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。

Alarm Host IPとは、CMSソフトウェア（例：iVMS-4200）がインストールされているリモートパソコンの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

クライアントソフトウェアのリモートアクセス用です。2000から65535の範囲です。初期値は8000です。

HTTP Port

Webブラウザによるリモートアクセス用です。初期値は80です。

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224.0.0.0～239.255.255.255の範囲のClass-D IPをカバーしており、239.252.0.0～239.255.255.255の範囲の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、エンターテインメントや通信システムで、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。

Output Bandwidth Limit

チェックボックスにチェックを入れると、出力帯域の制限を有効にできます。

Output Bandwidth

出力帯域制限を有効にした後、出力帯域を入力します。



メモ

- 出力帯域の制限は、リモートライブビューや再生に使用されます。
 - デフォルトの出力帯域が上限となります。
-

Alarm Host IP	
Alarm Host Port	0
Server Port	8000
HTTP Port	80
Multicast IP	
RTSP Port	554
<button>Apply</button>	

図 6-10 ポートの設定

6.2.7 ISUP

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、双方向音声、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。**Configuration → Network → Platform Access**
2. **Type**は**ISUP**を設定します。

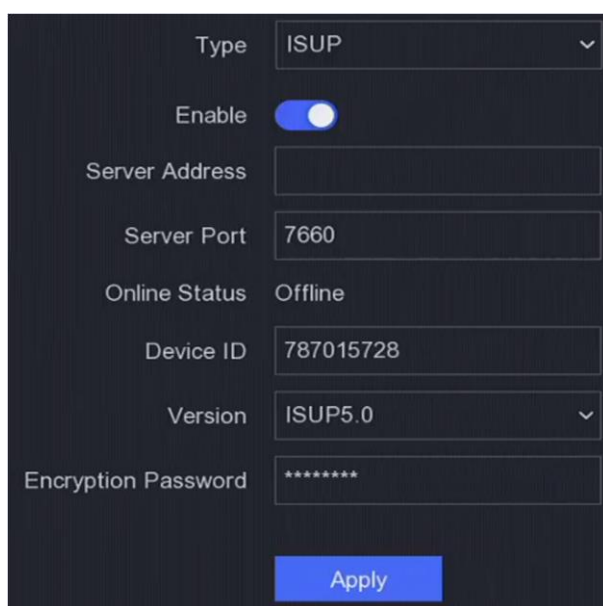


図 6-11 ISUP

3. **Enable**をオンにします。



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ます。

Version

使用可能なISUPプロトコルバージョンは、V5.0のみです。

Encryption Password

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

5. **Apply**をクリックして設定を保存し、本機を再起動します。

次に行うことは

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。

6.2.8 Hik-Connect

Configuration → Network → Platform Accessの順に進みます。詳しくは[Hik-Connect](#)を参照してください。

6.2.9 電子メール

Configuration → Network → Emailの順に進みます。詳しくは[電子メール](#)を参照してください。

6.3 カメラの管理

6.3.1 ネットワークカメラ

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

ネットワークカメラ認証を本機に追加します。

ご使用の前に

- ネットワークカメラが本機と同じネットワークセグメント上にあることを確認します。
- ネットワーク接続が有効で正しいことを確認します。
- ネットワークカメラのパスワードが本機と同じであることを確認します。

ステップ

1. 次の順に進みます。Configuration → Camera → Camera
2. **Online Device List**をクリックします。同じネットワークセグメント上のオンラインカメラがリストに表示されます。

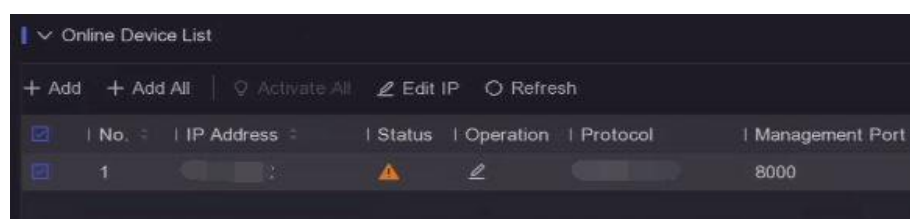


図 6-12 オンラインデバイス

3. **オプション** : **Edit IP**をクリックすると、カメラのIPアドレスを一括で編集できます。選択されたカメラに順番にIPアドレスを割り当てていくシステムです。
-



メモ

選択したカメラが起動していることを確認します。

4. ネットワークカメラを選択し、**Add**をクリックして追加してください。

ネットワークカメラを手動で追加する

ネットワークカメラ認証を本機に追加します。

ご使用の前に

- ネットワークカメラが本機と同じネットワークセグメントにあることを確認します。
- ネットワーク接続が有効で正しいことを確認します。
- 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. 次の順に進みます。**Configuration → Camera → Camera**
2. **+**をクリックします。

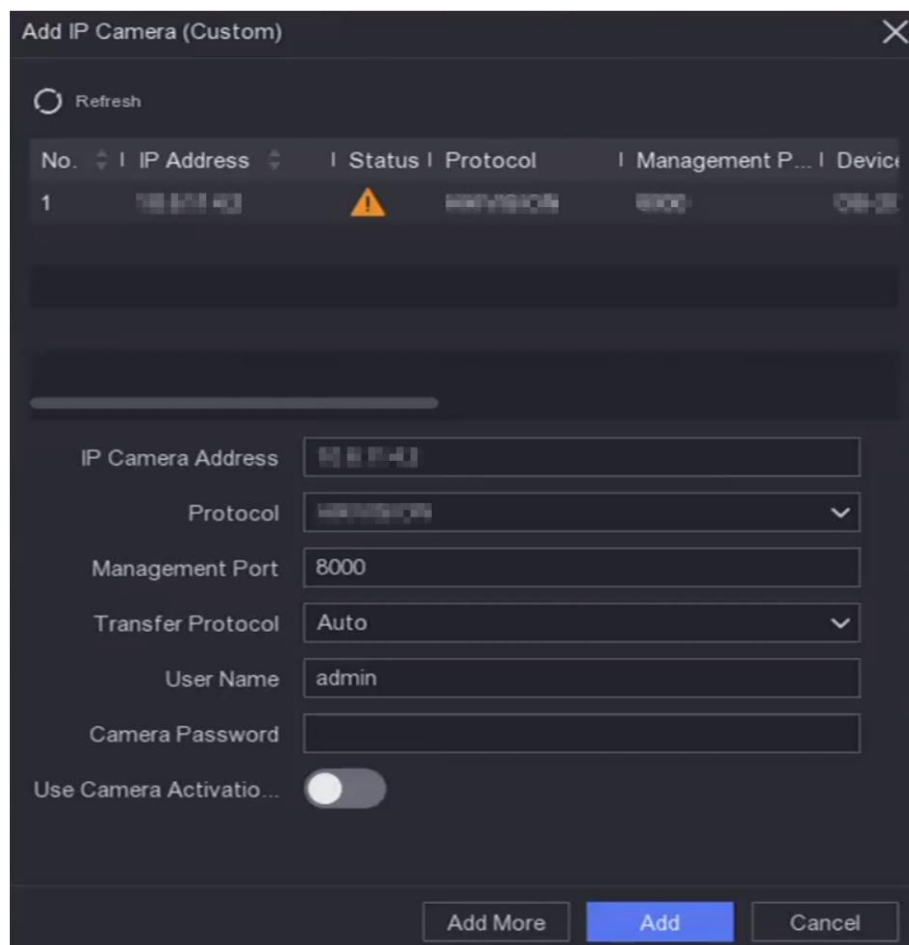


図 6-13 IPカメラの追加

3. ネットワークカメラのパラメータを入力します。

Use Camera Activation Password

有効な場合、本機は設定されたチャンネルのデフォルトパスワードでカメラを追加します。

4. **Add**をクリックします。

異なるネットワークセグメント上にネットワークカメラを追加する

ネットワークカメラが別のネットワークセグメントにある場合、本機はIPアドレスの範囲内でそのIPアドレスを検索し、それを追加します。

ご使用の前に

- ネットワーク接続が有効で正しいことを確認します。
- ネットワークカメラのパスワードが本機と同じであることを確認します。

ステップ

1. 次の順に進みます。**Configuration → Camera → Camera → IP Channel**
2. **Advanced Search**をクリックします。

3. **Network Segment**に入ります。

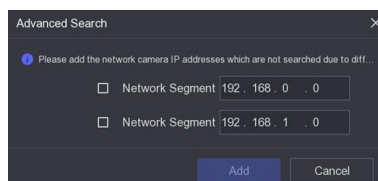


図 6-14 ネットワークセグメントに入る

4. **Add**をクリックします。

プラグアンドプレイでネットワークカメラを追加

非アクティブなネットワークカメラまたはサードパーティのONVIFカメラがネットワークに接続されている場合、本機は自動的にカメラを検出して追加するか、手動で追加するように通知することができます。

ステップ

1. 次の順に進みます。**Configuration → Camera → Camera → IP Channel**
2. **More**をクリックします。
3. **Plug-and-Play**を選択します。
4. **オプション**：**Auto Add Network Camera**を有効にします。本機は、自動的に非アクティブなネットワークカメラまたはサードパーティのONVIFカメラを検出し、追加します。

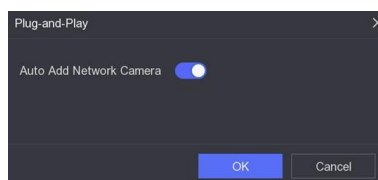


図 6-15 ネットワークカメラの自動追加



メモ

Auto Add Network Cameraをオフにし、非アクティブなネットワークカメラやサードパーティのONVIFカメラがネットワークに接続されると、本機は自動的にそれを検出し、追加するように通知します。

ネットワークカメラを編集する

ネットワークカメラのIPアドレスやプロトコル、パラメーターなどを編集できます。

ステップ

1. 次の順に進みます。**Configuration → Camera → Camera**
2. 追加されたネットワークカメラの  をクリックします。

Channel Port

接続デバイスが複数のチャンネルを持つエンコード機器である場合、ドロップダウンリストのチャンネルポート番号を選択することで、接続するチャンネルを選択できます。

3. **オプション : Edit IP**をクリックすると、カメラのIPアドレスを一括で編集できます。選択されたカメラに順番にIPアドレスを割り当てていくシステムです。
4. **OK**をクリックします。

ネットワークカメラをアップグレードする

ネットワークカメラのアップグレードは、本機から遠隔で行うことができます。

ご使用の前に

- USBフラッシュメモリーを本機に挿入し、ネットワークカメラのアップグレードファームウェアが入っていることを確認してください。
- ネットワークカメラが本機と同じネットワークセグメント上にあることを確認します。
- ネットワーク接続が有効で正しいことを確認します。

ステップ

1. 次の順に進みます。**Configuration → Camera → Camera**
2. をクリックします。
3. **Yes**をクリックして確認します。
4. ストレージデバイスからカメラのアップグレードファームウェアを選択します。
5. **Upgrade**をクリックし、アップグレードを開始します。アップグレードが完了すると、カメラは自動的に再起動します。

高度なカメラのパラメータを設定する

カメラのIPアドレス、カメラのパスワードなどの高度なカメラのパラメータを設定できます。

ご使用の前に

- ネットワークカメラが本機と同じネットワークセグメント上にあることを確認します。
- ネットワーク接続が有効で正しいことを確認します。

ステップ

1. 次の順に進みます。**Configuration → Camera → Camera**
2. をクリックします。
3. IPアドレス、カメラのパスワードなどのカメラのパラメータを設定します。
4. **Apply**をクリックします。

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、接続されたPoEカメラに電力とデータを転送できます。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。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。

PoEカメラの追加

ステップ

1. 次の順に進みます。**Configuration → 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

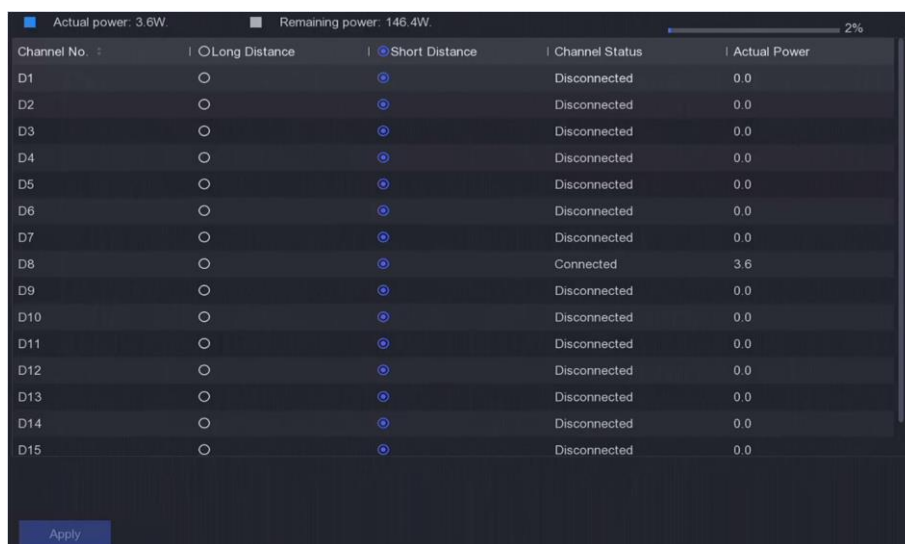
PoEインターフェースによる長距離（100～300m）ネットワーク伝送が可能です。

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、6Mbps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。



Channel No.	Long Distance	Short Distance	Channel Status	Actual Power
D1	☐	☒	Disconnected	0.0
D2	☐	☒	Disconnected	0.0
D3	☐	☒	Disconnected	0.0
D4	☐	☒	Disconnected	0.0
D5	☐	☒	Disconnected	0.0
D6	☐	☒	Disconnected	0.0
D7	☐	☒	Disconnected	0.0
D8	☐	☒	Connected	3.6
D9	☐	☒	Disconnected	0.0
D10	☐	☒	Disconnected	0.0
D11	☐	☒	Disconnected	0.0
D12	☐	☒	Disconnected	0.0
D13	☐	☒	Disconnected	0.0
D14	☐	☒	Disconnected	0.0
D15	☐	☒	Disconnected	0.0

図 6-16 PoEカメラの追加

3. **Apply**をクリックします。
4. PoEカメラと本機のPoEインターフェースをネットワークケーブルで接続します。

次に行うことは

Configuration → Camera → Camera → IP Channelの順に進み、接続されているPoEカメラを表示します。そのステータスをクリックすると、ライブ画像を表示します。

非PoEネットワークカメラの追加

PoEチャンネルリソースを使用して、PoE以外ネットワークカメラを接続することができます。

ステップ

1. 次の順に進みます。**Configuration → Camera → Camera → IP Channel**
2. ネットワークカメラがリンクされていないチャンネルの  をクリックします。
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。追加されたデバイスリストの  をクリックすると、パラメータを編集できます。

Manual

ネットワーク経由で物理的に接続することなく、IPカメラを追加できます。

4. ユーザー名、パスワード、IPアドレスなど、その他のパラメータを設定します。

チャンネルタイプの設定

PoEチャンネルを無効にして、通常のIPチャンネルリソースを追加で増やすことができます。

Configuration → Camera → Camera → PoE Binding Configurationの順に進み、PoEチャンネルを任意に設定します。



図 6-17 PoEバインディングの設定

チャンネル順の並び変え

Configuration → Camera → Cameraの順に進みます。詳しくは[チャンネル順の並び変え](#)を参照してください。

リモート設定

Configuration → Camera → Cameraの順に進みます。詳しくは[リモート設定](#)を参照してください。

IPカメラの設定ファイルのインポート/エクスポート

追加したネットワークカメラのIPアドレス、ポート、管理者のパスワードなどの情報をエクセルファイルに生成し、ローカルデバイスにエクスポートしてバックアップすることができます。エクスポートしたファイルは、パソコン上で内容の追加や削除などの編集ができ、他の機器にエクセルファイルをインポートすることで設定をコピーすることもできます。

ご使用の前に

USBメモリーなどのバックアップデバイスを接続します。

ステップ

1. 次の順に進みます。**Configuration → Camera → Camera**
2. **More**をクリックします。
3. **Export/Import**をクリックすると、接続したバックアップデバイスに設定ファイルをエクスポート/インポートします。
4. バックアップデバイスとフォルダのパスを設定します。
5. **Export/Import**をクリックします。

次に行うことは

インポートの手順が完了したら、本機を再起動する必要があります。

高度な設定

ステップ

1. 次の順に進みます。**Configuration → Camera → Camera**
2. **More**をクリックします。
3. パラメータは任意に設定します。

H.265 Auto Switch Configuration

このオプションを有効にすると、初回アクセス時にネットワークカメラ（H.265ビデオ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。

Upgrade

追加したネットワークカメラをアップグレードします。

Export/Import

追加したネットワークカメラのIPアドレス、ポート、管理者のパスワードなどの情報をエクセルファイルに生成し、ローカルデバイスにエクスポートしてバックアップすることができます。エクスポートしたファイルは、パソコン上で内容の追加や削除などの編集ができ、他の機器にエクセルファイルをインポートすることで設定をコピーすることもできます。

Protocol

標準プロトコルで設定されていないネットワークカメラを接続するために、カスタマイズされたプロトコルを設定できます。このシステムは16つのカスタマイズされたプロトコルを提供します。

Camera Activation Password Settings

ネットワークカメラの起動および追加のためのデフォルトのパスワードを変更します。すでに接続されているネットワークカメラでは、次のポップアップウィンドウで、既存のパスワードをこのパスワードに変更するか、選択できます。

Batch Configuration

本機はSVC機能を有効にしたり、選択したネットワークカメラの時刻を自動的に同期できます。

6.3.2 ディスプレイの設定

OSD（オンスクリーンディスプレイ）、画像設定、露出設定、day/nightの切り替えなどを設定します。

ステップ

1. 次の順に進みます。**Configuration → Camera → Display**
2. **Camera**を設定します。
3. パラメータは任意で設定します。

OSD Settings

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）を行います。

Image Settings

ライブビューや録画効果の明るさ、コントラスト、彩度などの画像パラメーターをカスタマイズします。

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

周囲の明るさやタイムスケジュールに合わせて、デイ、ナイト、オート、スケジュール切り替えモードに設定できます。

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は、WDR値を設定する必要があります。

Image Enhancement

画像のコントラストの強調を最適化するために使用します。

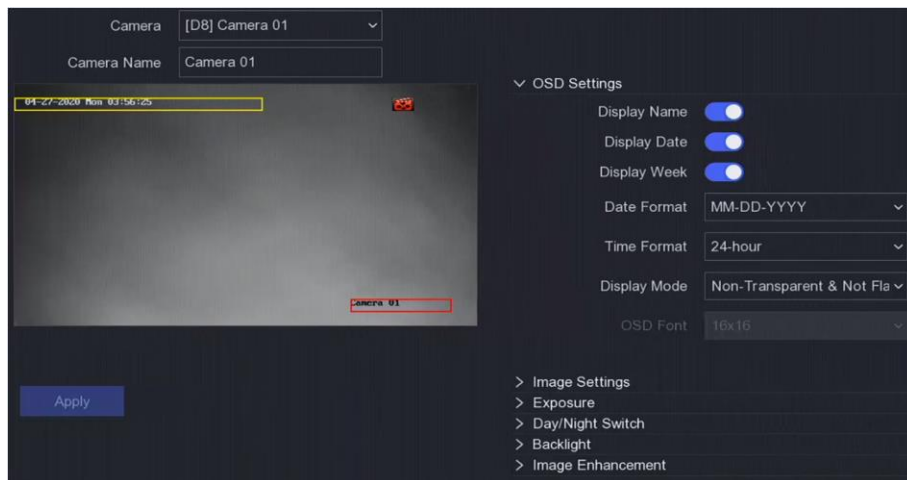


図 6-18 OSD

4. 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の位置を調整できます。
5. **Apply**をクリックします。

6.3.3 プライバシーマスク

閲覧や録画ができないプライバシーマスク領域を設定できます。

ステップ

1. 次の順に進みます。**Configuration → Camera → Privacy Mask**
2. **Camera**を選択します。
3. **Enable**をオンにします。

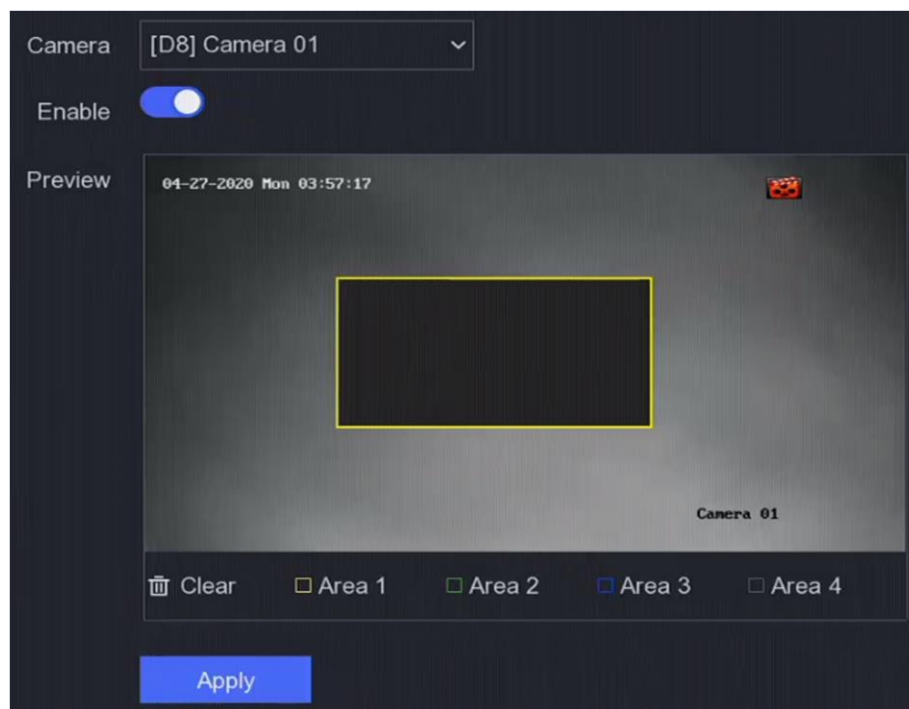


図 6-19 プライバシーマスク

4. ウィンドウにドラッグして領域を描画します。領域の枠は、異なる色で表示されます。



メモ

プライバシーマスクの領域は4箇所まで設定できます。各領域の大きさを調整できます。

5. **Apply**をクリックします。

6.4 イベント設定

6.4.1 通常イベント

動体検知

動体検知機能により監視領域内の動体を検知し、アラームを発生します。詳しくは[動体検知](#)を参照してください。

ビデオタンパリング

カメラレンズが覆われた場合アラームが作動し、アラーム対応アクションを実行します。

ステップ

1. 次の順に進みます。**Configuration → Event → Normal Event → Video Tampering**

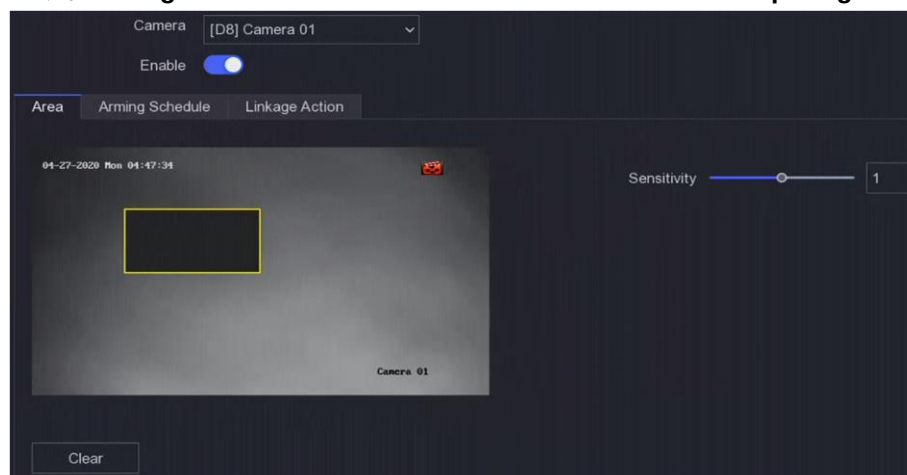


図 6-20 ビデオタンパリング

2. **Camera**を設定します。
3. **Enable**をオンにします。
4. **Sensitivity**を任意に調整します。値が高いほどビデオタンパリングが作動しやすくなります。
5. 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。
6. リンケージアクションを設定します。詳しくは[アラーム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。

ビデオロス

カメラのビデオロスを検知し、アラーム対応アクションを実行します。

ステップ

1. 次の順に進みます。**Configuration → Event → Normal Event → Video Loss**
2. **Camera**を設定します。
3. **Enable**をオンにします。
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[アラーム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。

Alarm Input

外部センサーアラームのリンケージアクションを設定します。

ステップ

1. 次の順に進みます。**Configuration → Event → Normal Event → Alarm Input**

ネットワークビデオレコーダー ユーザーマニュアル

Alarm Input No.	Alarm Name	Alarm Type	Enable	Operation
Local<-1		N.O	No	
Local<-2		N.O	No	
Local<-3		N.O	No	
Local<-4		N.O	No	

図 6-21 アラーム入力

メモ

ローカルアラーム入力：ローカルアラーム入力は、ビデオレコーダの端子台に接続された外部機器によって作動されます。

- 希望するアラーム入力のをクリックします。

図 6-22 アラーム入力の編集

- Alarm Name**をカスタマイズします。
- アラームの種類は**N.O** (normally open)または**N.C** (normally closed)を設定します。
- Settings**は**Input**を設定し、この機能を有効にします。

メモ

Settingsを**Nonuse**に設定すると、アラーム入力は無効となります。**Settings**を**One-Key Disarming**設定すると、選択したアラーム入力のリンク方法（複数可）は無効になります。

- 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。
- リンケージアクションを設定します。詳しくは[アラームリンケージアクションの設定](#)を参照してください。
- Apply**をクリックします。

アラーム出力

アラームが作動すると、アラーム出力を作動します。

ステップ

- 次の順に進みます。**Configuration → Event → Normal Event → Alarm Output**

Alarm Output No.	Alarm Name	Dwell Time	Operation
Local->1		5s	

図 6-23 アラーム出力

- 希望するアラーム出力のをクリックします。
- Alarm Name**をカスタマイズします。
- Dwell Time**を選択します。



図 6-24 アラーム出力の編集

5. **Settings**を**Input**に設定して、この機能を有効にします。
6. 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。
7. **Apply**をクリックします。

異常

異常イベントは、ライブビューウィンドウにイベントヒントを取り込み、アラーム出力やリンケージアクションを作動するように設定します。

ステップ

1. 次の順に進みます。**Configuration → Event → Normal Event → Exception**
2. イベントヒントを設定します。設定したイベントが発生するとアラームセンターにヒントが表示されます。
 - 1) **Event Hint**を有効にします。
 - 2) ヒントとなるイベントを選択します。次から選んでください：
 - **Event Hint Configuration**の をクリックしてイベントを選択します。
 - ローカルメニューの右上の隅にある をクリックしてアラームセンターに入り、イベントを選択します。
3. **Exception Type**を選択して、そのリンケージアクションを設定します。

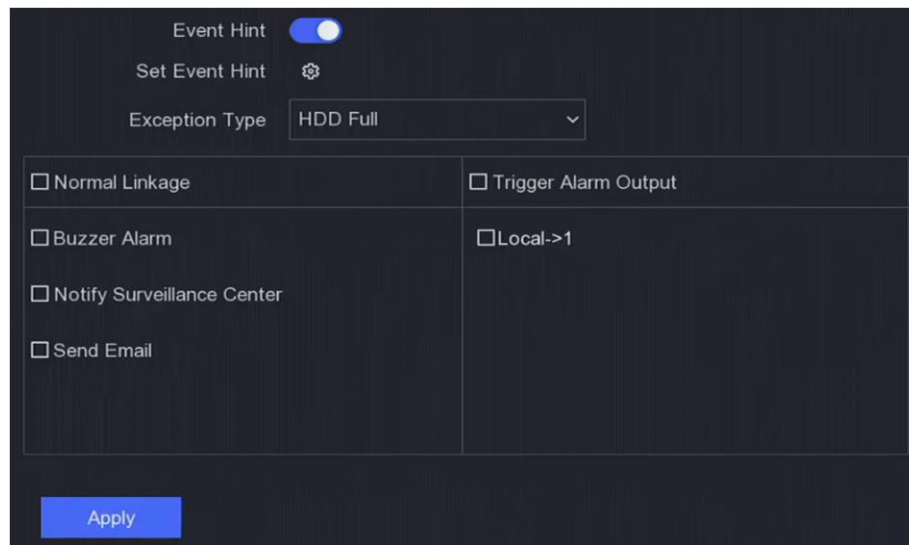


図 6-25 異常

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. **Apply**をクリックします。

6.4.2 境界保護

境界保護はラインクロッシング検知、侵入検知、領域入口検知、領域出口検知などを含みます。



メモ

境界保護は、一部の機種または一部のカメラのモデルにのみ対応しています。

ラインクロッシング検知

ライン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。**Configuration → Event → Smart Event → Line Crossing**
2. **Camera**を設定します。
3. **Enable**をオンにします。
4. **オプション**：**Save VCA Picture**にチェックを入れると、VCA検知のキャプチャ画像が保存されます。
5. 検知ルールと検知エリアを設定します。
 - 1) **Arming Area**を設定します。最大4つまで領域の選択ができます。
 - 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双方向に横切る物体を検知するとアラームが作動します。

A->B

設定されたラインをA側からB側へ横切る対象のみを検知します。

B->A

設定されたラインをB側からA側へ横切る対象のみを検知します。

- 3) **オプション** : **Target Detection**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。



メモ

本機能は一部の機種のみ対応しています。

- 4) **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。
6. 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。
7. リンケージアクションを設定します。詳しくは[アラーム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。

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、不審な往来をする人物や車両などを検知する機能です。

ステップ

1. 次の順に進みます。**Configuration → Event → Smart Event → Intrusion**
2. **Camera**を設定します。
3. **Enable**をオンにします。
4. **オプション** : **Save VCA Picture**にチェックを入れると、VCA検知のキャプチャ画像が保存されます。
5. 検知ルールと検知エリアを設定します。
 - 1) **Arming Area**を設定します。最大4つまで領域の選択ができます。
 - 2) **Time Threshold**と**Sensitivity**を調整します。

Sensitivity

アラームを作動させることができる物体の大きさです。値が高いほど検知アラームが作動しやすくなります。範囲は[1-100]です。

Time Threshold

範囲は[1s-10s]で、対象が領域内を不審な往来している時間のしきい値を示します。定義された検知領域内で対象の滞留時間がしきい値を超えると、アラームが作動します。

- 3) **オプション** : **Target Detection**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。



メモ

本機能は一部の機種のみ対応しています。

- 4) **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。
6. 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。
7. リンケージアクションを設定します。詳しくは[アラーム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。

領域入口検知

領域入口検知機能とは、あらかじめ設定された仮想領域に外部から入って来る人や車両などを検知し、アラームが作動すると何らかのアクションを起こす機能です。

ステップ

1. 次の順に進みます。**Configuration → Event → Smart Event → Region Entrance**
2. **Camera**を設定します。
3. **Enable**をオンにします。
4. **オプション**：**Save VCA Picture**にチェックを入れると、VCA検知のキャプチャ画像が保存されます。
5. 検知ルールと検知エリアを設定します。
 - 1) **Arming Area**を設定します。最大4つまで領域の選択ができます。
 - 2) **Sensitivity**を調整します。**Sensitivity**：範囲は[0-100]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) **オプション**：**Target Detection**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。



メモ

本機能は一部の機種のみ対応しています。

- 4) **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。
6. 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。
7. リンケージアクションを設定します。詳しくは[アラーム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。

領域出口検知

領域出口検知機能とは、あらかじめ定義された仮想領域から退出する人や車両などの対象を検知し、アラームが作動すると何らかのアクションを起こすことができる機能です。

ステップ

1. 次の順に進みます。**Configuration → Event → Smart Event → Region Exiting**
2. **Camera**を設定します。
3. **Enable**をオンにします。

4. オプション：Save VCA Pictureにチェックを入れると、VCA検知のキャプチャ画像が保存されます。
5. 検知ルールと検知エリアを設定します。
 - 1) Arming Areaを設定します。最大4つまで領域の選択ができます。
 - 2) Sensitivityを調整します。Sensitivity：範囲は[0-100]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) オプション：Target Detection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。



メモ

本機能は一部の機種のみ対応しています。

- 4) 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。
6. 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。
7. リンケージアクションを設定します。詳しくは[アラーム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。

6.4.3 その他のイベント

サーマルカメラによる検知

サーマルネットワークカメラのイベント検知モード（火災検知、温度検知など）に対応しています。選択したイベ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します。

ご使用の前に

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。Configuration → Event → Other Events
2. サーマルカメラの検知イベントを選択します。
3. Cameraを設定します。
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[アラーム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。

6.4.4 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. 曜日を1日選択し、時間帯を設定します。1日に最大8つまで時間帯を設定することができます。



時間帯は、繰り返したり、重複したりできません。

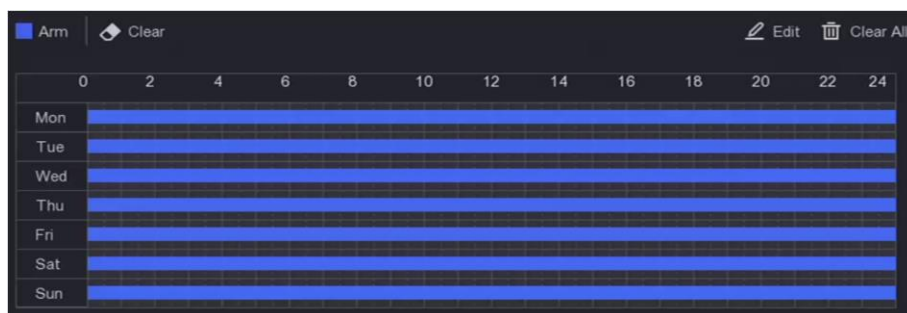


図 6-26 アーミングスケジュールの設定

3. Applyをクリックします。

6.4.5 アラームリンケージアクションの設定

アラームポップアップウィンドウを設定する

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。

ステップ

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

Alarm Pop-up Output

イベント映像を表示する出力を選択します。

Alarm Pop-up Delay

アラームイベント画像を表示する時間を秒単位で設定します。複数のチャンネルで同時にアラームが発生した場合、それらのフルスクリーン画像は10秒間隔（デフォルトの滞留時間）で切り替えます。

3. アラーム検知の**Linkage Action**をクリックします。
4. **Alarm Pop-up Window**アラームリンケージアクションを選択します。
5. トリガーチャンネル設定で、フルスクリーン監視を行いたいチャンネル（複数可）を選択します。



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。

ブザーアラームを設定する

音声警告は、アラームを検知すると本機がビープ音を作動させます。

ステップ

1. 次の順に進みます。 **Configuration → System → Live View → General**
2. **Audio**をオンにして**Volume**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みます。
4. アラームリンケージアクションとして**Buzzer Alarm**を選択してください。

監視センターへの通知

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

ステップ

1. 次の順に進みます。 **Configuration → Network → General → More Settings**
2. **Alarm Host IP**と**Alarm Host Port**を設定します。
3. アラーム検知のリンケージアクションインターフェイスに進みます。
4. **Notify Surveillance Center**を選択します。

電子メールリンケージを設定する

アラームを検知すると、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できます。

ステップ

1. 次の順に進みます。 **Configuration → Network → Email**
2. この設定を行います。
3. アラーム検知のリンケージアクションインターフェイスに進みます。
4. **Send Email**はアラームリンケージアクションを選択します。

アラーム出力の作動

アラーム出力は、ノーマルイベントとスマートイベントで作動できます。

ステップ

1. アラーム検知またはイベント検知の**Linkage Action**インターフェースに進みます。
2. **Trigger Alarm Output**をクリックします。
3. 作動するアラーム出力を選択します。
4. 次の順に進みます。 **Configuration → Event → Normal Event → Alarm Output**
5. リストからアラーム出力の項目を選択します。詳しくは[アラーム出力](#)を参照してください。

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）を作動します。

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みます。
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。

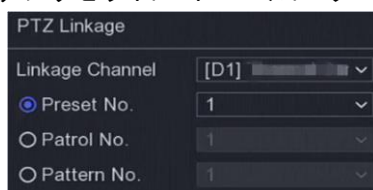


図 6-27 PTZリンケージ



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。

音声と点灯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。

ご使用の前に

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

ステップ

1. **Linkage Action**をクリックします。
2. 音声または点灯を任意に選択します。
3. **Apply**をクリックします。



音声や点灯のパラメータを設定する必要がある場合は、Webブラウザでネットワークカメラにログインして設定を行ってください。

6.5 録画管理

6.5.1 録画スケジュールの設定

ビデオレコーダーが設定したスケジュールに従って、自動的に録画を開始/停止します。

連続録画を設定する

ステップ

1. 次の順に進みます。**Configuration → Record → Parameter**
2. カメラのメインストリーム／サブストリームの連続録画パラメーターを設定します。
3. 次の順に進みます。**Configuration → Record → Schedule**
4. 録画タイプは**Continuous**を選択します。

イベント録画を設定する

ノーマルイベントまたはスマートイベントで作動する録画を設定できます。

ステップ

1. 次の順に進みます。**Configuration → Event**
2. イベント検知を設定し、イベントが発生したときに録画を作動するカメラ（複数可）を選択します。
3. 次の順に進みます。**Configuration → Record → Parameter**
4. カメラのメインストリーム／サブストリームの連続録画パラメーターを設定します。
5. 次の順に進みます。**Configuration → Record → Schedule**
6. 録画の種類は**Event**を選択します。

スケジュールを編集する

ステップ

1. 次の順に進みます。**Configuration → Record → Schedule**

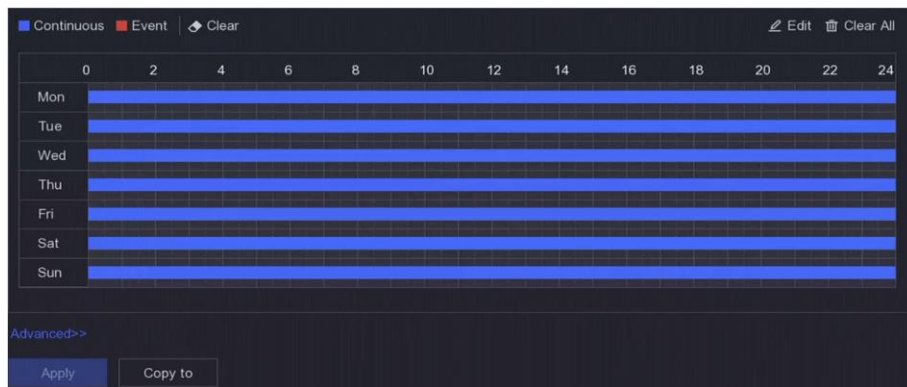


図 6-28 録画スケジュール

Continuous

連続録画が可能です。

Event

すべてのイベントトリガーアラームを作動した録画です。

2. **Camera No.**でカメラを選択します。
3. **Enable**をオンにします。
4. 録画スケジュールを設定します。
 - 1) **Edit** をクリックします。
 - 2) **Weekday**で設定する日を選択します。
 - 3) 終日録画のスケジュールを設定する場合は、**All Day**にチェック入れ、スケジュール**Type**を選択します。
 - 4) 他のスケジュールを設定する場合は、**All Day**のチェックを外し、**Start/End time**とスケジュール**Type**を設定します。

メモ

1日に最大8つの時間帯を設定できます。その時間帯は互いに重複することはできません。

- 5) **OK**をクリックすると、設定が保存され、上位メニューに戻ります。

メモ

スケジュールタイプは**Continuous**または**Event**を選択し、目的の時間帯にカーソルをドラッグして、カラーバーを描画します。

5. **Advanced**をクリックして、高度なパラメータを設定します。

Record Audio

音声は映像ファイルに記録されます。

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：11時にアラームが作動して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。

Video/Picture 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。

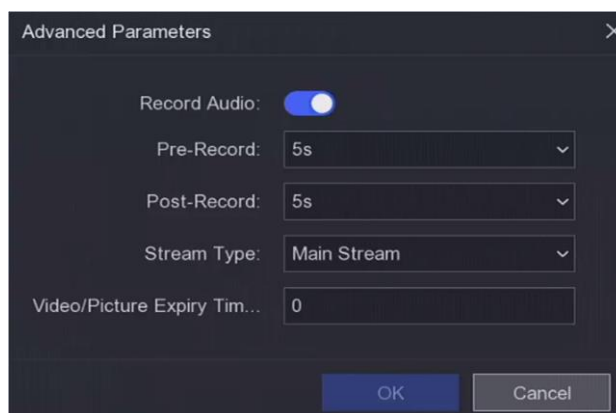


図 6-29 高度なパラメータ

6. OKボタンをクリックして、高度な設定を保存します。
7. Applyをクリックします。

6.5.2 録画パラメータの設定

ステップ

1. Configuration → Record → Parameterの順に進み、カメラのメインストリームとサブストリームのパラメータを設定します。
2. 録画パラメータを設定します。

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、映像の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。

Sub-Stream

サブストリームとは、メインストリームと並行して動作する第二のコーデックのことです。直接録画の画質を落とすことなく、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スマートフォンアプリで独占的に使用されます。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。

Frame Rate

1秒間に何枚のフレームをキャプチャできるかを示します。フレームレートが高いほど、ビデオに動きがある場合に画質を維持するため有利です。

Resolution

画像解像度とは、デジタル画像がどれだけ詳細な情報を保持できるかを示す指標であり、解像度が高いほど詳細な情報が得られます。解像度は、ピクセル列数（幅）×ピクセル行数（高さ）で指定することができます（例：1024×768）。

Bitrate

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

Enable H.264+/Enable H.265+

H.264+/H.265+モードは、低いビットレートで高い映像品質を確保するのに役立ちます。帯域幅やHDDの記憶容量の必要性を効果的に低減します。

Enable Low Bitrate Mode

デバイスの帯域幅やメモリを節約するために、本機はネットワーク状況に応じてカメラビデオのメインストリームのビットレートを自動的に調整します。



メモ

低ビットレートモードは、一部のカメラ機種でのみ対応しています。カメラがこの機能をサポートしている場合、デフォルトで有効になっています。

3. **Apply**をクリックします。

6.5.3 ストレージデバイス

HDDを初期化する

初めてHDDを使用する場合は、接続後に初期化を行ってください。

ご使用前に

本機にHDDを1台以上接続してください。

ステップ

1. 次の順に進みます。**Configuration → Record → Storage**
2. HDDを選択します。
3. **Init**をクリックします。

ネットワークディスクの追加

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として使用できます。

ステップ

1. 次の順に進みます。**Configuration → Record → Storage**
2. **Add**をクリックします。
3. **NetHDD**を設定します。
4. **Type**は**NAS**または**IP SAN**に設定します。
5. NetHDDのIPアドレスを入力します。
6. をクリックして、利用可能なディスクを検索します。

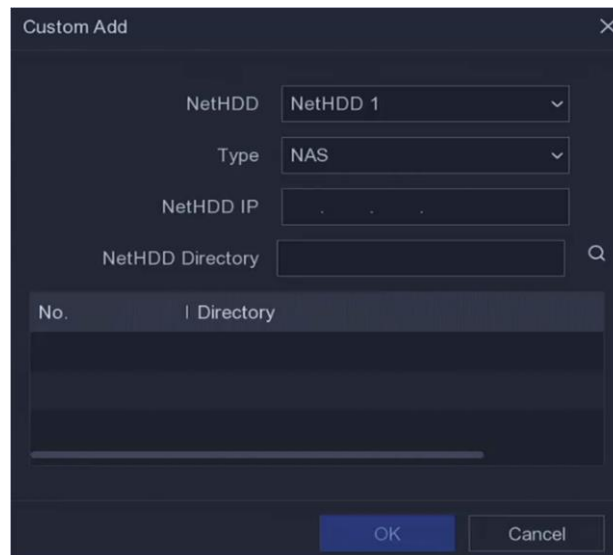


図 6-30 NetHDDの追加

7. リストからNASディスクを選択するか、または手動で**NetHDD Directory**に目的のディレクトリまでのパスを入力します。
8. **OK**をクリックします。



ネットワークディスク1台につき8TBまでの記憶容量が認識されます。

結果

ストレージデバイス一覧に追加したネットワークディスクが表示されます。

6.5.4 ストレージモードの設定

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

メモ

本機能は一部の機種のみ対応しています。

1. 次の順に進みます。**Configuration → Record → Storage Mode**
2. **Mode**は**Group**を選択します。
3. グループ番号を選択する。
4. HDDグループに録画するIPカメラを選択します。

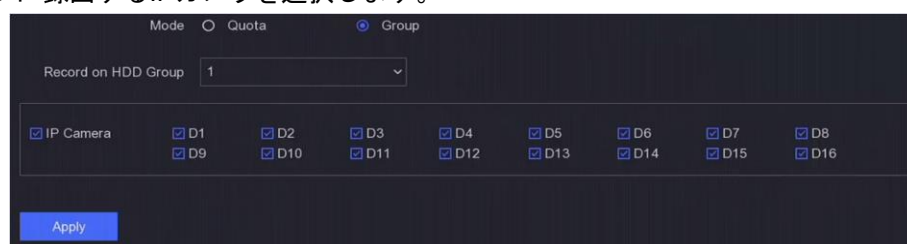


図 6-31 グループ

5. **Apply**をクリックします。
6. 本機を再起動して、新しいストレージモード設定を起動します。
7. 再起動した後、次の順に進みます。**Configuration → Record → Storage**
8. 使用するHDDのをクリックして、グループを設定します。
9. 現在のHDDのグループ番号を選択します。
10. **OK**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。

HDD割り当てを設定する

各カメラには、映像を保存するための割り当て容量を設定できます。

ステップ

メモ

本機能は一部の機種のみ対応しています。

1. 次の順に進みます。**Configuration → Record → Storage Mode**
2. **Mode**は**Quota**を選択します。
3. **Camera**で割り当てを設定するカメラを選択します。
4. **Record Capacity**で保存容量を入力します。

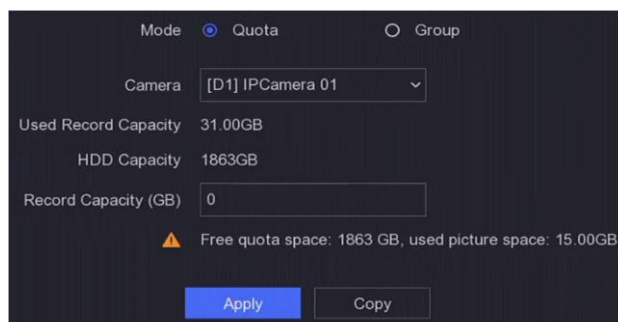


図 6-32 割り当て



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できるようになります。

5. **Apply**をクリックします。
6. 本機を再起動すると、新しい設定が起動します。

6.5.5 高度な設定

ステップ

1. 次の順に進みます。**Configuration → Record → Advanced**
2. パラメータは任意に設定します。

Overwrite

- 無効にする：HDDが一杯になると、書き込みを停止します。
- 有効にする：HDDが一杯になると、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。

Enable HDD Sleeping

長時間動作していないHDDは、スリープ状態になります。

Save Camera VCA Data

カメラVCAのデータは保存されるため、検索できます。

Alarm Storage

HDDの空き容量が不足している場合、無効にすることで容量を確保できますが、本機にアラーム情報が保存されなくなります。

Picture Storage

HDDの空き容量が不足している場合、無効にすることで容量を確保できますが、端末に画像が保存されなくなります。

第 7 章 メンテナンス

7.1 初期設定を復元する

ステップ

1. 右上の隅にあるをクリックします。
2. 復元のタイプを選択します。

Simple Restore

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

デバイスを非アクティブ状態に戻し、ユーザーアカウントの復元を除くすべての設定を変更しないようにします。

3. **Yes**をクリックします。本機は自動的に再起動します。

7.2 ログを検索する

本機の動作、アラーム、異常、情報をログに保存し、いつでも閲覧、出力することができます。

ステップ

1. 右上の隅にあるをクリックします。
2. **More**をクリックします。
3. **Log Information**をクリックします。
4. 検索条件を設定します。
5. **Search**をクリックします。

7.3 システムサービス

ステップ

1. 右上の隅にあるをクリックします。
2. **More**をクリックします。
3. **System Service**をクリックします。
4. パラメータは任意に設定します。

RTSP

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。

RTSP Authentication

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。

ISAPI

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。

HTTP

管理者ユーザーアカウントは、GUIまたはWebブラウザからHTTPサービスを無効化することができます。HTTPを無効にした後、ISAPIやONVIFなどの関連サービスもすべて終了します。

HTTP Authentication

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。2種類の認証方式が選択可能です。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。

Camera Added Detection

ネットワークカメラのステータスを検出する機能です。他のビデオレコーダーでネットワークカメラが追加された場合、ネットワークカメラのステータスは**Online Device**リストに🔥のように表示されます。

5. **Apply**をクリックします。

7.4 デバイスマaintenance

7.4.1 スケジュールの再起動

スケジュールに従って、自動的に再起動を行います。

ステップ

1. 右上の隅にある🔍をクリックします。
2. **More**をクリックします。
3. 次の順に進みます。 **Device Maintenance** → **Schedule Reboot**
4. **Enable**をオンにします。
5. 再起動のスケジュールを設定します。
6. **Apply**をクリックします。

7.5 アップグレード



警告

アップグレード中は、シャットダウンや電源を切らないでください。

7.5.1 ローカルアップグレード

ご使用前に

アップグレードファームウェアをバックアップデバイスに保存し、本機に接続します。

ステップ

1. 右上の隅にあるをクリックします。
2. をクリックします。
3. **Local Upgrade**をクリックします。
4. **Device Name**でバックアップデバイスを選択します。
5. アップグレードファームウェアを選択します。
6. **Upgrade**をクリックします。本機が自動的に再起動します。

7.5.2 オンラインアップグレード

最新のオンラインファームウェアでデバイスをアップグレードしてください。

ご使用前に

Hik-Connectが有効であり、正しく設定されていることを確認してください。詳しくは[**Hik-Connect**](#)を参照してください。

ステップ

1. 右上の隅にあるをクリックします。
2. をクリックします。
3. **Online Upgrade**に進みます。
4. 最新のファームウェアをダウンロードします。

Auto Download 自動的に最新のファームウェアを確認し、ダウンロードします。

Test Upgrade **Test Upgrade**をクリックして、手動で最新のファームウェアを確認し、ダウンロードができます。

5. 新しいバージョンのファームウェアがある場合は、本機をアップグレードしてください。本機は自動的に再起動します。

第 8 章 アラーム

イベントが発生すると、アラームセンターでその詳細を確認することができます。

8.1 イベントヒントの設定

アラームセンターでヒントとなるイベントを選択します。

ステップ

1. 右上の隅にある  をクリックします。
2. **Exception**、**Basic Event**または**Smart Event**を任意で設定します。

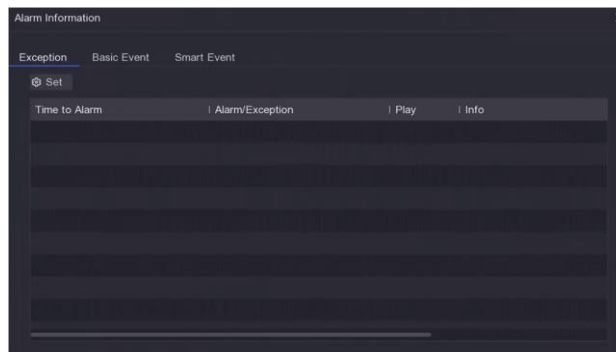


図 8-1 アラームセンター

3.  をクリックしてヒントとなるイベントを選択します。
4. **OK**をクリックします。
選択されたイベントが発生すると、アラーム情報が  (ローカルメニューの右上の隅にあります)に表示されます。

8.2 アラームセンターでアラームを見る

ステップ

1. ローカルメニューの右上の隅にある  をクリックします。
2. **Exception**、**Basic Event**または**Smart Event**をクリックして必要に応じて表示します。

第 9 章 Webオペレーション

9.1 紹介

Webブラウザで本機にアクセスできます。

以下のWebブラウザのいずれかをご利用ください。Internet Explorer 11.0、Apple Safari、Mozilla Firefox、Google Chrome。サポートする解像度は1024×768以上です。

一部の機種では、Webコンポーネントプラグインをダウンロードし、インストールする必要があります。インストールしないと、いくつかの機能が使用できません。ダウンロードアドレスは<http://hikdownload.hs7.com/web/webplugin/windows/WebComponents/standard/WebComponents.exe>です。

9.2 ログイン

お客様は、本製品をインターネットに接続して使用する場合、ネットワークセキュリティリスクの下に置かれる可能性があることを了承するものとします。ネットワーク攻撃や情報漏洩を防ぐため、各自で防御を強化してください。本機が正常に動作しない場合は、お買い上げの販売店または最寄りのサービスセンターまでご連絡ください。

ステップ

1. Webブラウザを開いて本機のIPアドレスを入力し、**Enter**を押します。



HTTPポートを変更した場合は、アドレスバーに<http://IPAddress:HTTP port>を入力します。

例：<http://192.168.1.64:81>。

2. **user name**と**password**をログイン画面に入力します。
3. **Login**をクリックします。

The image shows a login interface within a web browser. There are two text input fields. The first field contains the text 'admin'. The second field contains a series of dots, representing a password. Below these fields is a prominent red button with the word 'Login' in white text.

図 9-1 ログイン

4. インストール画面の指示に従って、プラグインをインストールします。



プラグインのインストールを終了するために、Webブラウザを閉じる必要があります。

9.3 ライブビュー

ログイン後、ライブビューのインターフェイスが表示されます。



図 9-2 ライブビュー

9.4 再生

Playbackをクリックして、再生インターフェースに入ります。

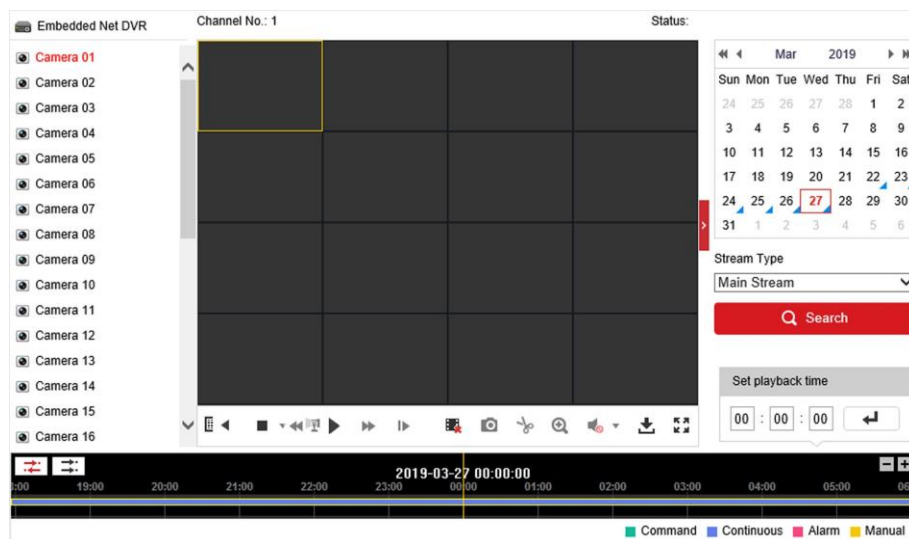


図 9-3 再生

9.5 設定

Configurationをクリックして、コンフィギュレーションインターフェースに入ります。

The screenshot shows the 'Configuration' interface with a sidebar on the left containing menu items: Local, System, Network, Video/Audio, Image, Event, Storage, Vehicle Detection, and VCA. The main content area is divided into three sections:

- Live View Parameters:**
 - Protocol: ☒ TCP, ☐ UDP, ☐ MULTICAST
 - Stream Type: ☒ Main Stream, ☐ Sub-stream
 - Play Performance: ☐ Shortest Delay, ☒ Balanced, ☐ Fluent
 - Rules: ☐ Enable, ☒ Disable
 - Image Size: ☒ Auto-fill, ☐ 4:3, ☐ 16:9
 - Auto Start Live View: ☐ Yes, ☒ No
 - Image Format: ☒ JPEG, ☐ BMP
 - Encryption Key:
- Record File Settings:**
 - Record File Size: ☐ 256M, ☒ 512M, ☐ 1G
 - Save record files to:
 - Save downloaded files to:
- Picture and Clip Settings:**
 - Save snapshots in live view to:
 - Save snapshots when playback to:
 - Save clips to:

図 9-4 設定

9.6 ログ

ステップ

1. 次の順に進みます。Maintenance → System → Maintenance → Log
2. 検索条件を設定します。
3. **Search**をクリックします。

The screenshot shows the 'Log List' interface. The sidebar on the left has 'Maintenance' selected. The main content area has tabs for 'Upgrade & Maintenance', 'Online Upgrade', 'Log', and 'Diagnose'. The 'Log' tab is active, showing search filters and a table of log entries.

Search filters:

- Major Type:
- Minor Type:
- Start Time:
- End Time:
-

Log List table:

No.	Time	Major Type	Minor Type	Channel No.	Local/Remote User	Remote Host IP
Total 0 items << < 0/0 > >>						

図 9-5 ログ

第 10 章 付録

10.1 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の間に、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。

10.2 通信マトリックス

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 10-1 通信マトリックス

10.3 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 10-2 デバイスコマンド

