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

この文書について

- 本書には、本製品の使用および管理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、説明のためのものです。
- 本書に記載されている情報は、ファームウェアの更新やその他の理由により、予告なく変更される場合があります。本書の最新版はHikvisionのウェブサイト(***https://www.hikvision.com***)でご確認ください。別段の合意がない限り、杭州Hikvision Digital Technology Co., Ltd.またはその関連会社(以下「Hikvision」)は、明示または黙示を問わず、いかなる保証も行いません。
- 本書は、本製品のサポートに精通した専門家の指導と支援を受けながら使用してください。

この商品について

- 、購入された国または地域においてのみアフターサービスを受けることができます。
- お選びいただいた商品が映像商品の場合は、以下のQRコードを読み取って「映像商品の利用に関する取り組み」を入手し、よくお読みください。

知的財産権の承認

- Hikvisionは、記載された製品に具現化された技術に関連する著作権および／または特許を所有し、これには第三者から取得したライセンスが含まれる場合があります。
- テキスト、画像、グラフィックス等を含む本書のいかなる部分も、Hikvision に帰属します。書面による許可なく、本書の一部または全部を抜粋、複写、翻訳、改変することを禁じます。
- HIKVISIONおよびその他のHikvisionの商標およびロゴは、様々な管轄区域におけるHikvisionの所有物です。
- その他記載されている商標およびロゴは、各所有者の財産です。
- HDMI™HDMI、HDMI High-Definition Multimedia Interface、および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

- 適用される法律で許可される最大限の範囲において、本書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」、「すべての欠点およびエラーとともに」提供されます。Hikvisionは、明示または黙示を問わず、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、いかなる保証も行いません。お客様による本製品の使用は、お客様自身の責任において行われるものとします。Hikvisionは、契約違反、不法行為（過失を含む）、製造物責任、その他に基づくか否かを問わず、本製品の使用に関連して、事業利益の損失、事業の中断、データの損失、システムの破損、ドキュメンテーションの損失など、特別損害、派生的損害、偶発的損害、または間接的損害について、たとえHikvisionがそのような損害または損失の可能性を知らされていたとしても、いかなる場合も責任を負いません。
- インターネットの性質上、セキュリティ上のリスクが内在しており、Hikvisionはサイバー攻撃、ハッカー攻撃、ウイルス感染、その他のインターネット上のセキュリティ上の起因する異常動作、プライバシー漏洩、その他の損害について一切の責任を負いません。
- お客様は、適用されるすべての法律に従って本製品を使用することに同意し、お客様の使用が適用される法律に適合していることを確認することについては、お客様が単独で責任を負うものとします。特に、お客様は、肖像権、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。大量破壊兵器の開発または生産、化学兵器または生物兵器の開発または生産、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、または人権侵害の支援など、禁止されている最終用途のために本製品を使用してはなりません。
- 本書と適用される法律の間に矛盾がある場合は、後者が優先されます。

規制情報

FCC情報

コンプライアンスに責任を負う当事者によって明示的に承認されていない変更または修正は、装置を操作するユーザーの権限を無効にする可能性がありますのでご注意ください。

FCC準拠：本装置は、FCC 規則パート 15 に従った制限に準拠していることがテストにより確認されています。これらの制限は、住宅用設置において有害な干渉から適切に保護することを目的としています。本装置は、無線周波数エネルギーを発生、使用、放射する可能性があり、説明書に従って設置および使用されない場合、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、特定の設置場所で干渉が発生しないことを保証するものではありません。本装置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（本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つまたは複数によって干渉を修正するよう試みてください：

- 受信アンテナの向きを変えるか、位置を変える。
- 機器と受信機の距離を離す。
- 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ください。
- 販売店または経験豊富なラジオ/テレビ技術者にください。FCC条件

本装置は FCC 規則パート 15 に準拠しています。動作は以下の 2 つに従います。

という条件がある：

- 本装置は有害な干渉を引き起こす可能性はありません。
- このデバイスは、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、受信した干渉を受け入れなければなりません。

EU適合性宣言

本製品および付属品（該当する場合）には「CE」マークが貼付されており、EMC指令2014/30/EU、LVD指令2014/35/EU、RoHS指令2011/65/EUに記載されている該当する整合欧州規格に準拠しています。

2012/19/EU（WEEE指令）：このマークが付いた製品は、欧州連合（EU）では未分別の一般廃棄物として処分できません。適切なリサイクルを行うため、このマークが付いた製品を廃棄する前に、お近くの販売店までご返送ください。

同等の新しい機器を購入するか、指定された回収処分する。詳細は ***http://www.recyclethis.info を***参照。

2006/66/EC（電池指令）：本製品には、欧州連合（EU）で未分別の一般廃棄物として処分できないバッテリーが含まれています。バッテリーの具体的な情報については、製品の説明書を参照してください。バッテリーにはこのシンボルマークが表示されており、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、バッテリーを供給元または指定の回収場所に返却してください。詳細については***http://www.recyclethis.info を***ご覧ください。

対象モデル

本書は以下の機種に対応しています。ただし、各機種とも本書のすべての機能に対応しているわけではありません。

表 1-1 適用モデル

シリーズ	モデル
DS-7600NI-I2	DS-7608NI-I2
	DS-7616NI-I2
	DS-7632NI-I2
DS-7600NI-I2/P	DS-7608NI-2/8P
	DS-7616NI2/16P
	DS-7632NI-II2/16P
DS-7700NI-I4	DS-7708NI-I4
	DS-7716NI-I4
	DS-7732NI-I4
DS-7700NI-I4/P	DS-7708NI-4/8P
	DS-7716NI-4/16P
	DS-7732NI-4/16P
	DS-7732NI-24P
DS-7600NI-M1/P	DS-7604NI-M1/4P
DS-7608NI-M2	DS-7608NI-M2
	DS-7616NI-M2
	DS-7632NI-M2
DS-7600NI-M2/P	DS-7608NI-M2/8P
	DS-7616NI-M2/16P
DS-7700NI-M4	DS-7716NI-M4
	DS-7732NI-M4
	DS-7764NI-M4
DS-7700NI-M4/P	DS-7708NI-M4/8P

シリーズ	モデル
	DS-7716NI-M4/16P
	DS-7732NI-M4/16P
	DS-7732NI-M4/24P
DS-9600NI-M8	DS-9616NI-M8
	DS-9632NI-M8
	DS-9664NI-M8
	DS-96128NI-M8
DS-9600NI-M8/R	DS-9616NI-M8/R
	DS-9632NI-M8/R
	DS-9664NI-M8/R
	DS-96128NI-M8/R
DS-9600NI-M16	DS-9616NI-M16
	DS-9632NI-M16
	DS-9664NI-M16
	DS-96128NI-M16
DS-9600NI-M16/R	DS-9616NI-M16/R
	DS-9632NI-M16/R
	DS-9664NI-M16/R
	DS-96128NI-M16/R
DS-7600NXI-M2/P/VPro	DS-7608NXI-M2/8P/VPro
	DS-7616NXI-M2/16P/VPro
DS-7600NXI-M2/VPro	DS-7608NXI-M2/VPro
	DS-7616NXI-M2/VPro
DS-7700NXI-M4/VPro	DS-7716NXI-M4/VPro
	DS-7732NXI-M4/VPro
DS-7700NXI-M4/16P/VPro	DS-7716NXI-M4/16P/VPro
	DS-7732NXI-M4/16P/VPro
DS-8600NI-M16	DS-86128NI-M16

シリーズ	モデル
DS-9600NXI-M8/VPro	DS-9616NXI-M8/VPro
	DS-9632NXI-M8/VPro
	DS-9664NXI-M8/VPro
	DS-96128NXI-M8/VPro
DS-9600NXI-M8R/VPro	DS-9616NXI-M8R/VPro
	DS-9632NXI-M8R/VPro
	DS-9664NXI-M8R/VPro
	DS-96128NXI-M8R/VPro
DS-9600NXI-M16/VPro	DS-9632NXI-M16/VPro
	DS-9664NXI-M16/VPro
	DS-96128NXI-M16/VPro
DS-9600NXI-M16R/VPro	DS-9632NXI-M16R/VPro
	DS-9664NXI-M16R/VPro
	DS-96128NXI-M16R/VPro
DS-7600NXI-2/S	DS-7608NXI-2/S
	DS-7616NXI2/S
	DS-7632NXI-2/S
DS-7600NXI2/P/S	DS-7608NXI2/8P/S
	DS-7616NXI2/16P/S
	DS-7632NXI2/16P/S
DS-7700NXI-4/S	DS-7716NXI-4/S
	DS-7732NXI-4/S
DS-7700NXI-4/P/S	DS-7716NXI4/16P/S
	DS-7732NXI4/16P/S
DS-8600NXI-I8/S	DS-8616NXI-I8/S
	DS-8632NXI-I8/S
	DS-8664NXI-I8/S
DS-8600NXI-8/24P/S	DS-8632NXI-8/24P/S

シリーズ	モデル
DS-9600NXI-8/S	DS-9616NXI8/S
	DS-9632NXI-8/S
	DS-9664NXI-I8/S
DS-96000NI-H16R	DS-96256NI-H16R
	DS-96256NI-H16R/LCD
DS-96000NI-H20R	DS-96128NI-H20R
	DS-96128NI-H20R/LCD
	DS-96256NI-H20R
	DS-96256NI-H20R/LCD
DS-96000NI-H30R	DS-96128NI-H30R
	DS-96128NI-H30R/LCD
	DS-96256NI-H30R
	DS-96256NI-H30R/LCD
DS-9600NI-G8R	DS-9632NI-G8R
iDS-6700NXI-M1/X	iDS-6704NXI-M1/X
	iDS-6708NXI-M1/X
	iDS-6716NXI-M1/X
iDS-7600NXI-M1/X	iDS-7608NXI-M1/X
	iDS-7616NXI-M1/X
iDS-7600NXI-M2/X	iDS-7608NXI-M2/X
	iDS-7616NXI-M2/X
	iDS-7632NXI-M2/X
iDS-7600NXI-M2/P/X	iDS-7608NXI-M2/8P/X
	iDS-7616NXI-M2/16P/X
iDS-7700NXI-M4/X	iDS-7716NXI-M4/X
	iDS-7732NXI-M4/X
iDS-7700NXI-M4/16P/X	iDS-7716NXI-M4/16P/X
	iDS-7732NXI-M4/16P/X

シリーズ	モデル
iDS-9632NXI-M8/X	iDS-9632NXI-M8/X
	iDS-9664NXI-M8/X
	iDS-96128NXI-M8/X
iDS-9600NXI-M8R/X	iDS-9632NXI-M8R/X
	iDS-9664NXI-M8R/X
	iDS-96128NXI-M8R/X
iDS-9600NXI-M16/X	iDS-9632NXI-M16/X
	iDS-9664NXI-M16/X
iDS-9600NXI-M16R/X	iDS-9632NXI-M16R/X
	iDS-9664NXI-M16R/X
iDS-96000NXI-H16R	iDS-96064NXI-H16R
	iDS-96128NXI-H16R
	iDS-96128NXI-H16R/LCD
iDS-96000NXI-H24R	iDS-96128NXI-H24R
	iDS-96128NXI-H24R/LCD
	iDS-96256NXI-H24R
	iDS-96256NXI-H24R/LCD

安全指導

- すべてのパスワードおよびその他のセキュリティ設定の適切な構成は、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規則を厳守してください。
- プラグを電源ソケットにしっかりと接続してください。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、デバイスの電源を切ってください。
- 感電の危険があります！メンテナンスの前に、すべての電源を切ってください。
- 本機器はアース付きコンセントに接続してください。
- ソケットコンセントは装置の近くに設置し、容易にアクセスできること。
- 危険な通電を示す記号ϟ が付いている装置の場合、端子に接続された外部配線は、指示された人による設置が必要です。
- 装置を不安定な置かないでください。装置が落下し、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に準拠したSELV（安全特別低電圧）およびLPS（制限電源）を満たす必要があります。
- タッチ電流が大きい！電源に接続する前にアースに接続してください。
- 煙、臭い、ノイズが発生した場合は、すぐに電源を切り、電源ケーブルを抜いてから、サービスセンターにご連絡ください。
- デバイスはUPSと併用し、可能であれば工場出荷時に推奨されているHDDを使用してください。
- 本装置は、子供が可能性のある場所での使用には適していません。
- 注意：誤ったタイプのバッテリーに交換すると、爆発する危険があります。
- 電池を飲み込まないでください。化学的火傷の危険性！
- 本製品にはコイン／ボタン電池が内蔵されています。コイン電池を飲み込むとわずか2時間で重度のやけどを負い、死に至る可能性があります。
- 不適切なタイプのバッテリーに交換すると、保護機能が働かなくなることがあります（一部のリチウム電池の場合など）。
- 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しないでください。
- 爆発や可燃性液体・ガスの漏えいの原因となります。
- バッテリーを極端に低い空気圧にさらさないで。爆発や可燃性液体・ガスの漏れの原因となります。
- 使用済みバッテリーは説明書に従って処分してください。
- ファンブレードやモーターに身体の一部を近づけない。整備中は電源を切ってください。
- 身体の一部をモーターに近づけないでください。整備中は電源を切ってください。
- 元のモデルと同じ電源、または同じ電圧と電流のLPS電源のみを使用してください。

予防と注意

デバイスを接続して操作する前に、以下の注意事項をご確認ください：

- 本機は屋内です。換気がよく、ほこりのない、液体のない設置してください。
- レコーダーがラックや棚に適切に固定されていることを確認してください。レコーダーを落下させ、大きな衝撃を与えると、レコーダー内の繊細な電子部品が損傷することがあります。
- また、花瓶のような液体の入ったものを装置の上に置いてはならない。
- 火をつけたロウソクなどの裸火は、本機の上に置かないでください。
- 換気口を新聞紙、テーブルクロス、カーテンなどで覆って換気を妨げてはならない。ベッド、ソファー、敷物、その他同様のものの上に装置を置いて換気口を塞いではならない。
- 一部のモデルでは、AC電源に接続するための端子の配線が正しいことを確認してください。
- モデルによっては、IT配電システムに接続するために、必要な場合、装置を改造して設計されています。
-  は、電池ホルダ自体を識別し、電池ホルダ内のセルの位置を識別する。
- \+ 直流電流と共に使用される、または直流電流を発生させる装置のプラス端子を特定し、 - 直流電流と共に使用される、または直流電流を発生させる装置のマイナス端子を特定する。
- デバイスの電源が切れていたり、置かれていたりすると、コイン電池/ボタン電池の電力が切れることがあります。
- コイン電池/ボタン電池が場合、システム時刻が正しくないので、アフターサービスに連絡して電池を交換してください。
- 十分な換気のため、装置の周囲には最低 200 mm (7.87 インチ) の距離を保ってください。
- 一部のモデルでは、AC電源に接続するための端子の配線が正しいことを確認してください。
- 鋭利な角やエッジには触れないでください。
- デバイスが45 °C (113 °F)を超えて動作している場合、またはS.M.A.R.T.のHDD温度が規定値を超えている場合は、デバイスが涼しい環境で動作していることを確認するか、HDDを交換してS.M.A.R.T.のHDD温度を規定値以下にしてください。
- 山頂、鉄塔、森林などの特殊な条件下では、装置の入口開口部にサージサプレッサを設ける。
- デバイスの電源が切れた後も電気が残っている可能性があるため、むき出しの部品（インレットの金属接点など）には触れず、少なくとも5分間待ちます。
- 本装置のUSBポートは、マウス、キーボード、USBフラッシュドライブ、またはWi-Fiドングルの接続にのみ使用される。接続する機器の電流は0.1A以下でなければならない。
- デバイスのシリアルポートはデバッグのみに使用される。
- 装置の電源出力ポートが限定電源に準拠していない場合、このポートから電源を供給される接続装置は、防火筐体を備えなければならない。
- 電源アダプターが同梱されている場合は、同梱のアダプターのみを使用してください。

-  または  のステッカーが貼られた機器については、以下の注意事項に注意してください：注意：高温の部品です！触れないでください。指を火傷する恐れがあります。30分以上経ってから部品を扱ってください。
- 装置を壁や天井に設置する必要がある場合、
  1. 本マニュアルの指示に従い、デバイスを取り付けてください。
  2. けがを防ぐため、本装置は設置説明書に従って設置面に確実に取り付けてください。
- 使用温度が高い場合（40 °C ～ 55 °）、一部の電源アダプタの電力が低下することがあります。
- 配線、取り付け、分解を行う前に、電源が切断されていることを確認してください。
- デバイスを自分で配線する必要がある場合は、デバイスに表示されている電気パラメータに従って、電力を供給するための対応するワイヤーを選択します。対応する、標準的なワイヤーストリッパーでワイヤーを剥く。重大な結果を避けるため、剥いた電線の長さは適切なものとし、導線が露出しないようにしてください。
- 煙、臭い、ノイズが発生した場合は、直ちに電源を切り、電源ケーブルを抜いて、サービスセンターにご連絡ください。

コンテンツ・コンベンション

説明を簡単にするため、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）を指す。
- チャンネルとは、主にビデオレコーダーのビデオチャンネルを指す。

シンボル規約

本書で使用される記号はように定義されている。

シンボル	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内容を示しています。
 **注意**	回避しなければ、機器の損傷、データ損失、性能低下、または予期せぬ結果を招く可能性のある、潜在的に危険な状況を示します。
 **注**	本文の重要なポイントを強調または補足するための追加情報を提供する。

インジケータとインターフェースの説明

フロントパネル・インジケータ

フロントパネルのインジケータは、デバイスのさまざまな動作状態を示します。

表 1-1 共通インジケータの説明

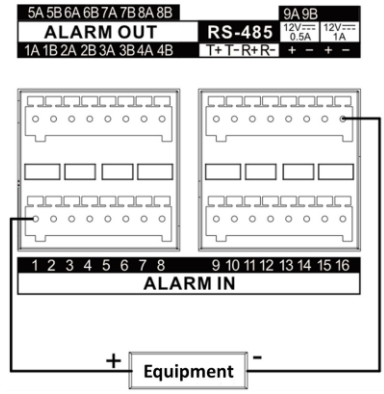
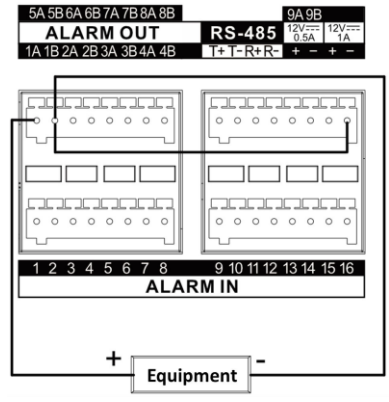
インジケーター	説明
⏻	デバイスに入ると、インジケータが点灯します。
🛢	HDDからデータが読み出されているとき、またはHDDにデータが書き込まれているときに、インジケータが点滅します。
🖧	ネットワーク接続が正常に機能している場合、インジケーターが点滅します。

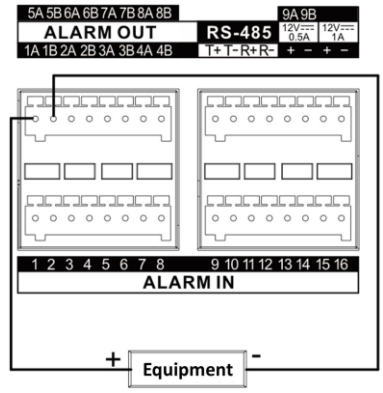
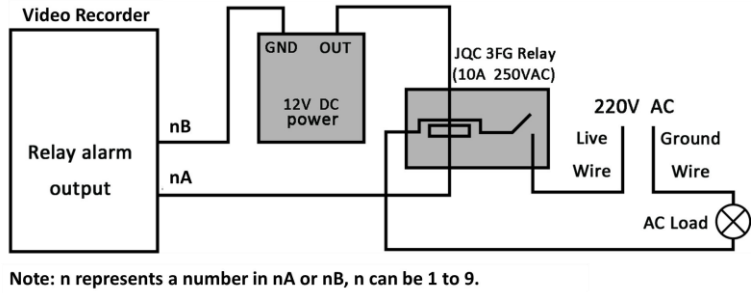
インターフェース

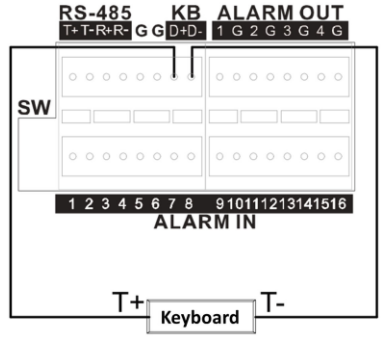
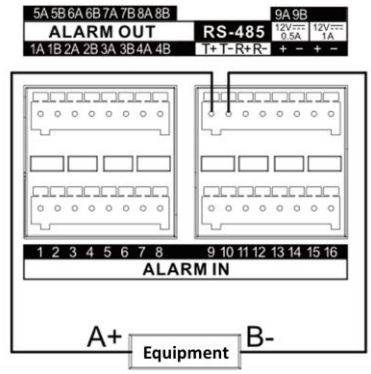
パネル・インターフェースはモデルによって異なります。一般的なインターフェースの説明については、以下の表を参照してください。

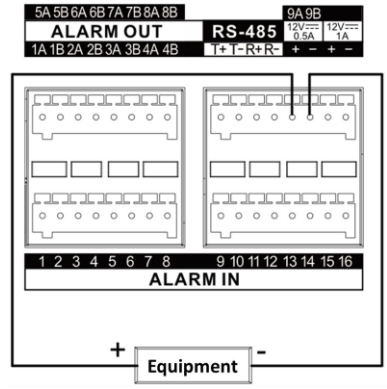
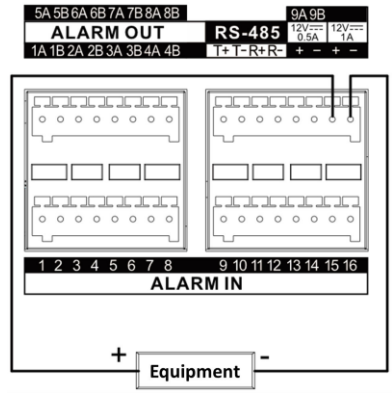
表 1-2 共通インジケータの説明

項目	説明
ビデオ・イン	ターボHDおよびアナログビデオ入力用BNCインターフェース。
ビデオ出力	ビデオ出力用BNCコネクタ。
オーディオ入力	オーディオ入力用RCAコネクター。
オーディオ出力	オーディオ出力用RCAコネクター。
LINE IN	双方向オーディオ入力用RCAコネクター。
USB	追加デバイス用ユニバーサル・シリアル・バス（USB）インターフェース。
ブイジーエー	ローカルビデオ出力およびメニュー表示用DB15コネクタ。
HDMI	ビデオ出力用HDMIインターフェース。
RS-485	パン/チルトユニット、スピードドームなどのためのRS-485シリアルインターフェース。
RS-232	パラメータ設定用RS-232インターフェース、またはトランスペアレント・チャンネル。
LAN	RJ-45自己適応型イーサネットインターフェイス。
eSATA	記録やバックアップのためのストレージおよび拡張インターフェイス。
GND	グラウンド

項目	説明
電源スイッチ	デバイスのオン/オフ用スイッチ。
電源	100～240 VAC、48 VDC、または12 VDC電源。
USIMカード	UIM/SIMカードスロット。
⅄	SMAアンテナインターフェース。
アラームイン	アラーム入力はアラーム入力信号を受信します。機器のプラス端子（＋）は数字に、機器のマイナス端子（-）は "-"または "G "に接続してください。 アラーム入力の接続例として下図を使用します。 
警報出力	アラーム出力はアラーム信号を送出します。 直流電源の場合、プラス端子（＋）は "A "の番号に、マイナス端子（-）は "B "の番号にそれぞれ接続し、"-"または "G "に接続してください。直流機器の警報出力接続例として、下図を参考にしてください。 

項目	説明
	AC電源を使用する機器の場合、プラス端子（＋）は "A "の番号に、マイナス端子（-）は "B "の番号に接続してください。 AC 機器のアラーム出力接続例として下図を使用してください。  注 AC負荷電圧が高くなる可能性があるため、安全のため外部リレーを使用してください。 以下の図を参考にしてください。  **Note: n represents a number in nA or nB, n can be 1 to 9.**
KB	KBはキーボードを表す。D+」とD-」をそれぞれ「T+」と「T-」に接続する。下図を参考にしてください。

項目	説明
	
RS-485	RS-485は、2線式半二重多地点シリアル接続の電気的仕様である。T+」と「T-」をそれぞれ「A+」と「B-」に接続する。 以下の図を参考にしてください。 
コントロール12V $\overset{12V}{\underset{0.5A}{\text{⎓}}}$	外部アラーム装置用の制御可能な12 VDCおよび0.5/1 A電源出力。対応するアラーム出力がトリガーされると電源がオンになります。 以下の図を参考にしてください。

項目	説明
	
DC 12V 12V 1A	DC12V、1Aの電力を出力します。以下の図を参考にしてくださ い。 

HDDの取り付け

お使いのデバイスがHDDのホットスワップに対応していない場合は、ハードディスクドライブ（HDD）を取り付ける前にデバイスから電源を抜いてください。この取り付けには、工場推奨のHDDを使用する必要があります。

下のQRコードをスキャンして、HDDのインストールビデオをご覧ください。

図 1-1 HDD の取り付け

ブラケットの取り付け

ブラケット取り付けは、デバイスカバーを取り外し、内蔵ブラケットにHDDを取り付ける必要がある場合に適用されます。

ステップ

1. 背面のネジを外し、後方に押して取り外します。

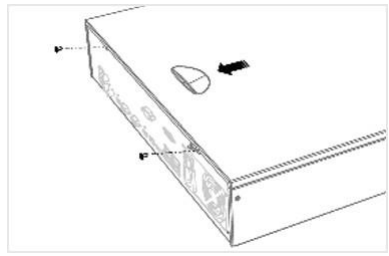


図 1-2 カバーの取り外し

2. HDDをブラケットにネジで固定する。

注

下層ブラケットにHDDを取り付ける前に、まず上層ブラケットをアンインストールしてください。

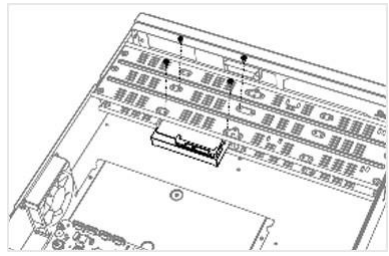


図 1-3 HDD を固定する

3. データケーブルと電源ケーブルを接続する。

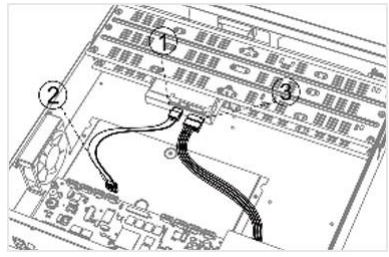


図 1-4 ケーブルの接続

注

他のHDDを取り付けるには、上記の手順を繰り返すことができます。

4. 装置カバーを再び取り付け、ネジを締めます。

フロントパネルのプラグ・プルの取り付け

フロントパネルプラグプルインストールは、キーでデバイスのフロントパネルを開け、HDDを取り付ける必要がある場合に適用されます。

ステップ

1. 取り付け耳をネジでHDDに固定する。

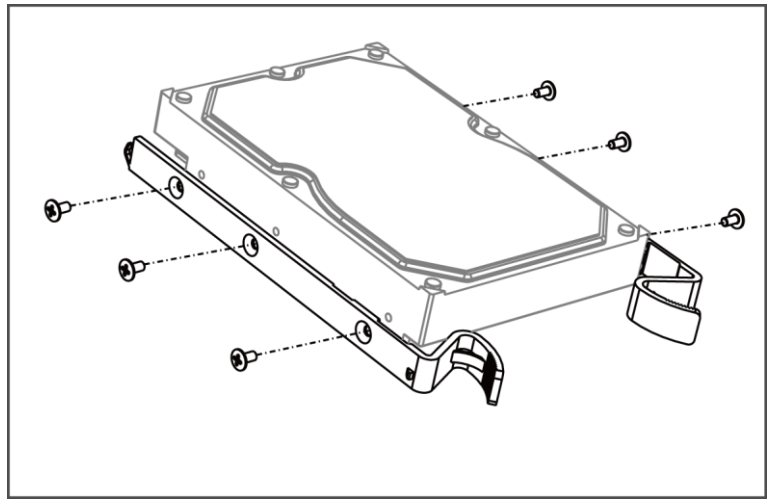


図 1-5 取り付け耳を HDD に固定する

2. 付属のキーでフロントパネルのロックを解除し、フロントパネル両脇のボタンを押して開けます。

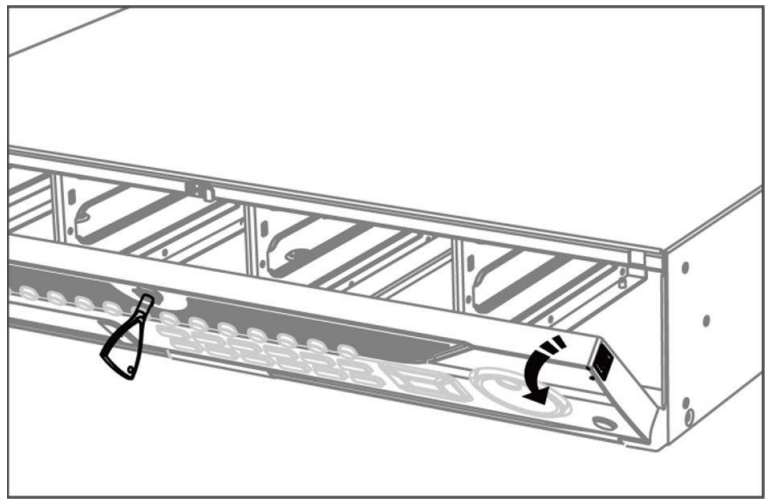


図1-6 オープン・フロント・パネル

3. HDDがしっかりと固定されるまで挿入する。

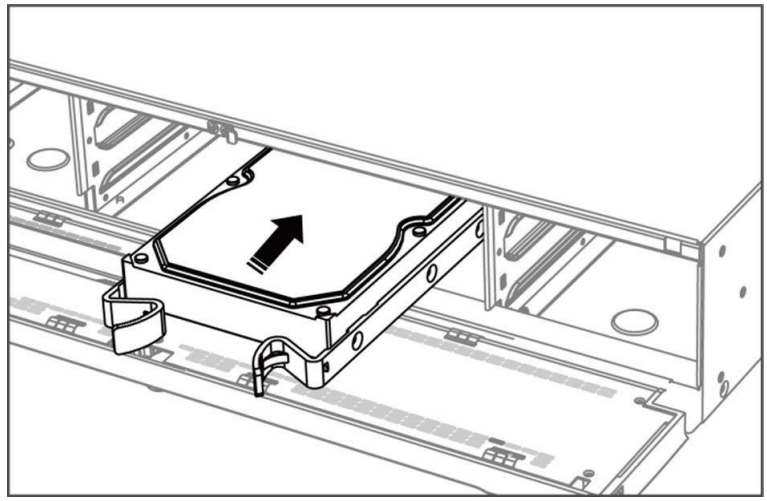


図 1-7 HDD の挿入

4. オプション： 他のHDDを取り付けるには、上記の手順を繰り返します。

5. フロントパネルを閉じ、キーでロックする。

HDDケースの取り付け

HDDケースの取り付けとは、HDDをケースに取り付け、HDDケースをスロットに差し込む方法を指す。

ステップ

1. パネルキーでフロントパネルのロックを解除する。

2. フロントパネルを装置から引き出し、左ハンドルの少し上にする。

注

フロントパネルと装置の角度は10°以内でなければならない。

3. 青いボタンを押してハンドルを跳ね上げ、ハンドルを持ったままHDDケースをスロットから引き抜く。

4. ハードディスクをHDDケースに固定する。

1) HDDをケースに入れる。SATAインターフェイスはケース底面を向いている必要があります。

2) HDDの位置を調整します。ハードディスクの背面がHDDの底面と一致していることを確認します。

3) ドライバーを使い、4本のネジを両側のネジ穴に留める。

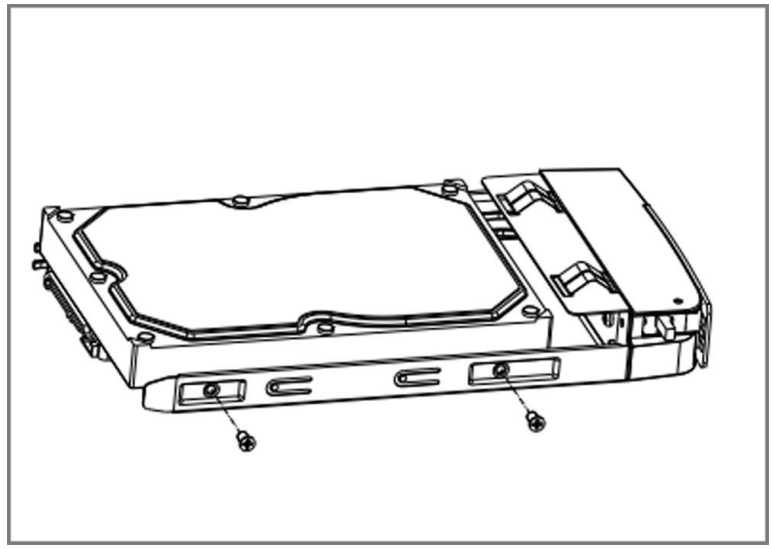


図 1-8 HDD の固定

5. HDDケースをスロットに押し戻す。

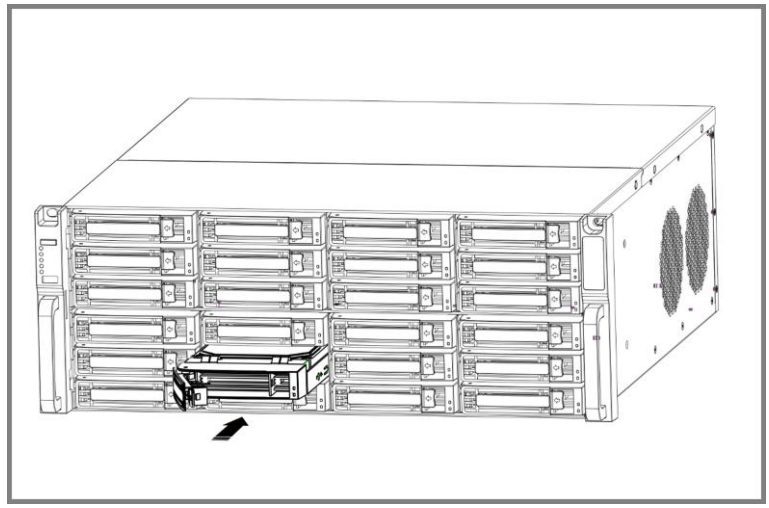


図1-9 HDDケースをスロットに押し込む

6. カチッと音がするまでハンドルを押す。こうしてHDDケースが固定される。上記の手順を繰り返し、残りのハードディスクボックスを取り付ける。
7. フロントパネルを閉じ、パネルキーでロックする。

フィックス・オン・ボトムの取り付け

底面固定設置は、デバイスの底面にHDDを設置して固定する必要がある場合に適用されます。

ステップ

1. パネルのネジを外し、装置からカバーを取り外します。

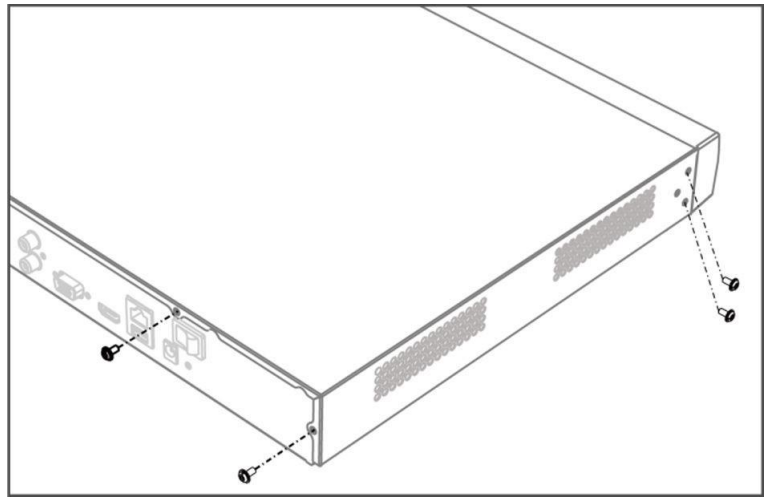


図 1-10 カバーの取り外し

2. データケーブルと電源ケーブルを接続する。

1) データケーブルの一端をデバイスのマザーボードに接続する。

2) データケーブルのもう一方の端をHDDに接続する。

3) 電源ケーブルの一端をHDDに接続する。

4) 電源ケーブルのもう一方の端をデバイスのマザーボードに接続する。

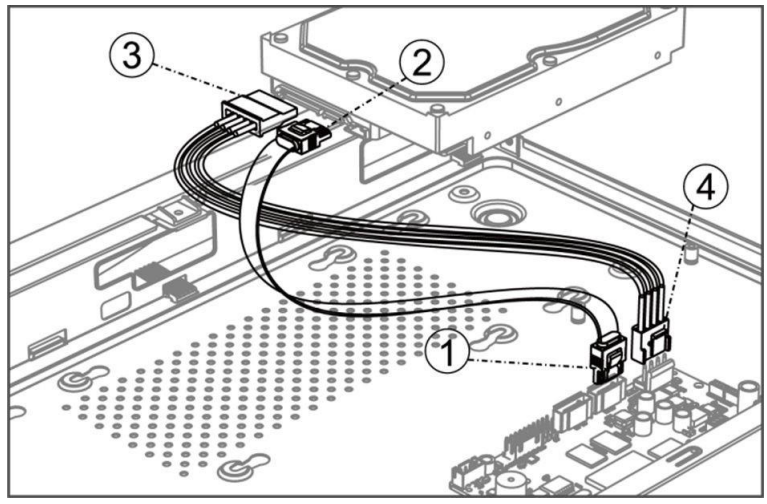


図 1-11 ケーブルの接続

3. デバイスをし、HDDのネジ山とデバイス底面の予約穴を合わせ、HDDをネジで固定する。

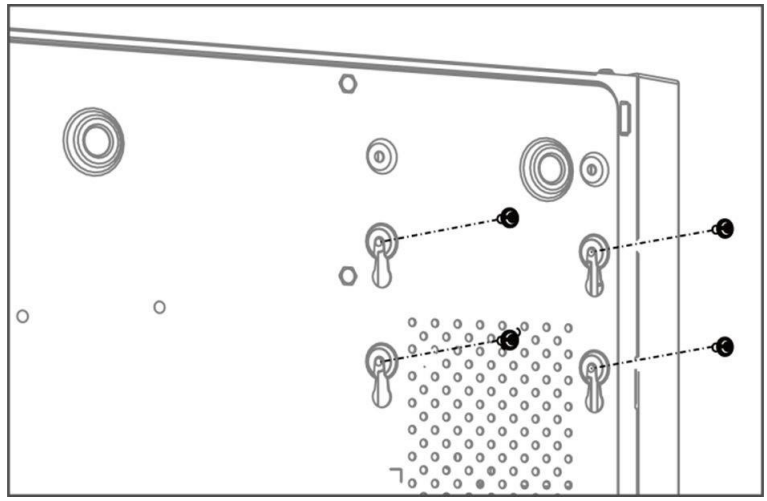


図 1-12 HDD をデバイス底面に固定する

4. オプション：他のHDDを取り付けるには、上記の手順を繰り返します。

5. 装置カバーを再び取り付け、ネジを締めます。

コイン/ボタン電池の交換

コイン電池/ボタン電池は、デバイスの電源が切れていたり、長時間置かれていたりして、システム時間が正しくない場合に交換する必要があります。

始める前に

デバイスの電源を切る。

ステップ

1. デバイスのシャーシカバーを取り外します。
2. マザーボード上のコイン/ボタン電池を探す。
3. 親指をバッテリースロットの外側に置き、人差し指でプラス側のコンタクトスプリングを外側に軽く押します。バッテリーは自動的に飛び出します。

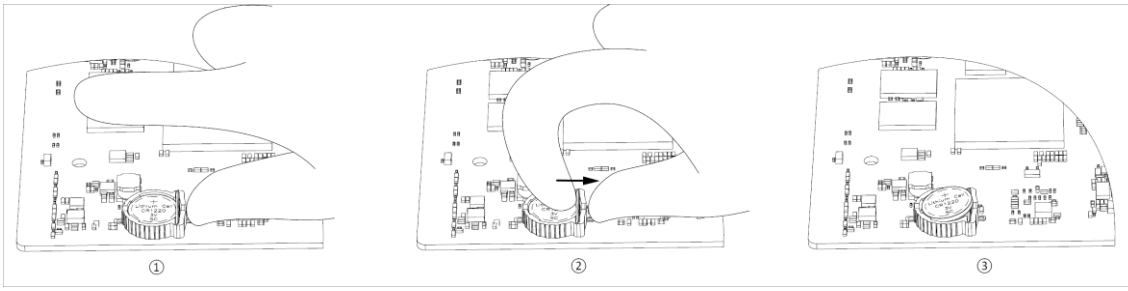


図 1-1 バッテリーの取り外し

注

- バッテリーを取り外す際は、静電気防止手袋を着用してください。
- 外側に押し出す力が強すぎてスプリングが変形している場合は、バッテリーを挿入する前に元の位置に調整する必要があります。

4. プラスチック製のスナップポイントがバッテリースロットにある側に向かって斜めにバッテリーを挿入し、プラス接点バネの近くでバッテリーを押してバネの下にはめ込みます。

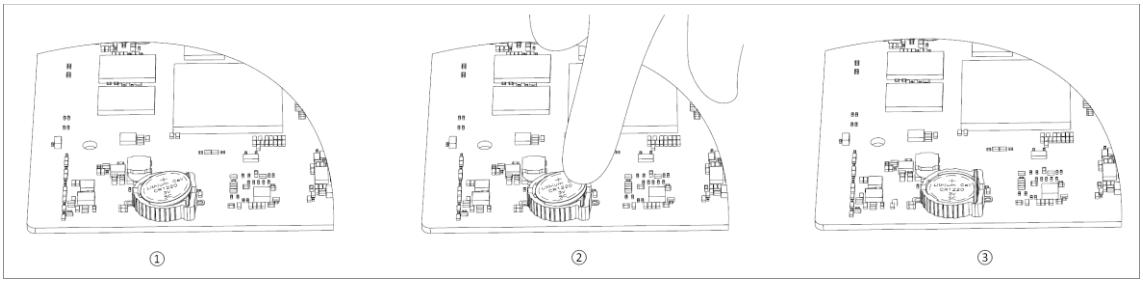


図 1-2 バッテリーの交換

注

バッテリーを交換する際は、静電気防止手袋を着用してください。

5. デバイスのシャーシカバーを再度取り付けます。

次に何をすべきか

システム時刻が正しくない場合は、時刻の設定を行ってください。

内容

第1章 ローカルメニューで起動する

初めてアクセスする場合は、管理者パスワードを設定してデバイスをアクティベートする必要があります。アクティベーション前の操作はできません。ウェブブラウザ、SADP またはクライアントソフトウェアを使用してデバイスをアクティベートすることもできます。

始める前に

モニターとマウスが接続されていることを確認してください。

ステップ

1. デバイスの電源を入れます。
2. 地域またはDST（夏時間）パラメータを設定します。
3. システム言語を選択します。
4. 管理者パスワードを2回入力する。

注意

製品のセキュリティを高めるため、ご自身で選択した強力なパスワード（大文字、小文字、数字、特殊文字の少なくとも3種類を含む、最低8文字を使用）を作成することを強くお勧めします。また、パスワードは定期的に変更することをお勧めします。特にセキュリティの高いシステムでは、毎月または毎週パスワードを変更することで、製品をより確実に保護することができます。

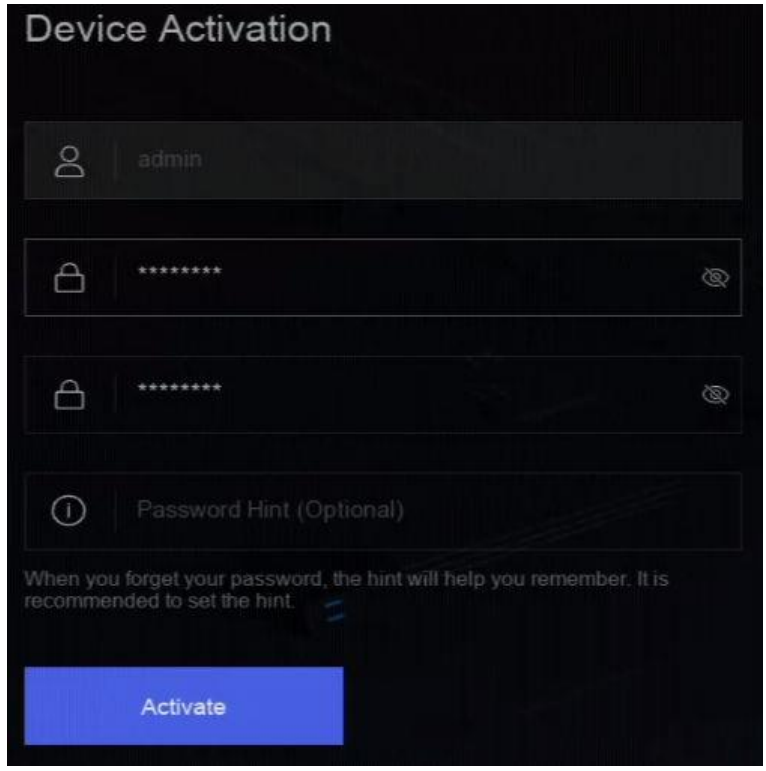


図1-1 ローカルメニューによる起動

5. **オプション：**パスワードのヒントを入力します。パスワードをときに思い出すのに役立ちます。
6. **Activateを**クリックする。

注

デバイスがアクティベートされた後、パスワードを適切に保管する必要があります。

7. **オプション：**ロック解除パターンを描く。
8. 少なくとも1つのパスワード回復設定する。

次に何をすべきか

ウィザードに従って基本パラメータを設定します。

第2章 デバイスにログインする

メニューやその他の機能を操作する前に、デバイスにログインする必要があります。

始める前に

デバイスがアクティベートされていることを確認してください。

ステップ

1. デバイスの電源を入れます。
2. 右クリックでショートカットメニューを表示。
3. 必要に応じて項目を選択する。例えば、**Exit Full Screenを**選択すると、自動的にログインインターフェイスに入ります。

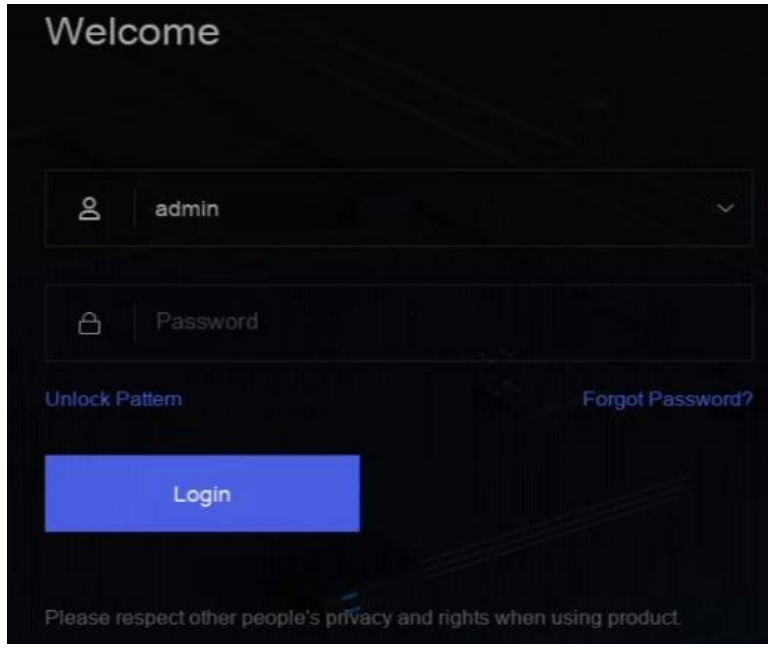


図2-1 ログイン

4. ロック解除パターンを使用してログインするか、**パスワードログインを**クリックしてユーザー名とパスワードでログインします。

注

- アンロックパターンは管理利用可能です。
- ロック解除パターンやログインパスワードを忘れた場合は、パスワードログインインターフェイスで**「パスワードを忘れた場合」を**クリックしてパスワードをリセットするか、パスワードヒントを使用してパスワードを記憶してください。

第3章 ユーザーインターフェースの紹介

電源オン後、デバイスはライブビューインターフェイスに入ります。マウスを右クリックし、ショートカットメニューから**「フルスクリーン終了」を**選択します。

図 3-1 メイン機能ページ

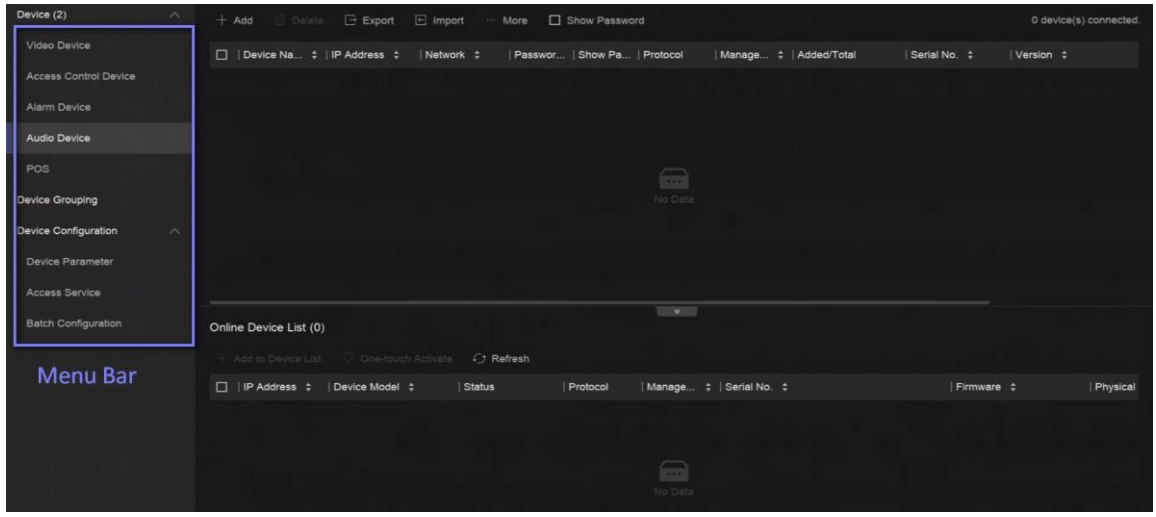


図 3-2 メニュー・バーの例

図3-3 アプリケーションセンターの人・車両検知例 表3-1 インターフェース紹介

インターフェース名	はじめに
タスクバー	開いているアプリケーションはタスク一覧表示されます。各アプリケーションのタブを移動したり閉じたりできます。 アイコン紹介 • :メインメニュー。 • :イベントセンター。イベントアラームの検索、閲覧が可能。 • :各ダウンロードタスクのダウンロードの進捗状況はここで確認できます。 • :デバイスをシャットダウン、ログアウト、または再起動します。
アプリケーション一覧	すべてのアプリケーションがここに表示されます。クリックして設定ことができます。
ナビゲーションバー	クリックすると、システムの各機能を設定できます。
メニューバー	各アプリケーションの設定可能な項目はここにリストアップされている。 注 **アプリケーションセンターの**アプリケーションについては、をクリックするか、右クリックしてメニューバーを表示します。

第4章 ネットワーク設定

ネットワーク・パラメーター、プラットフォーム・アクセス設定、ネットワーク・サービスは設定可能です。

4.1 ネットワーク・パラメーター設定

ネットワークアクセスを必要とする機能を使用する前に、ネットワークパラメータを設定する必要があります。

4.1.1 TCP/IPの設定

ネットワーク経由でビデオレコーダーを操作したり、ネットワーク機器にアクセスする前に、TCP/IPを適切に設定する必要があります。

ステップ

1. システム→ システム設定→ ネットワーク→ ネットワーク→ TCP/IP .

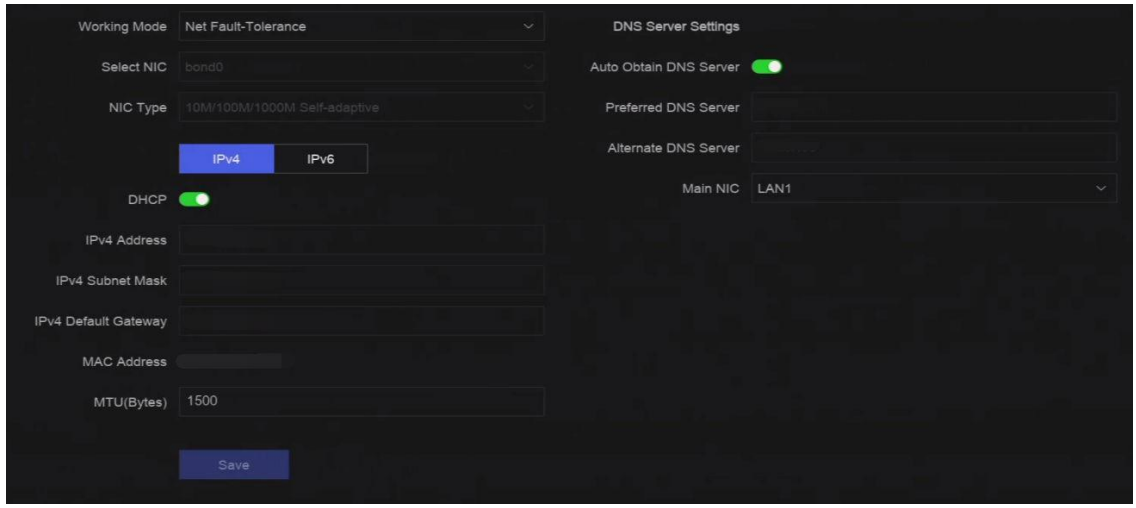


図4-1 TCP/IP設定

2. 作業モードを設定し、**NICを選択**します。**マルチア**

ドレス

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 タイプフィールドで **LAN1** または **LAN2** を選択できます。片方の NIC カードをデフォルトルートとして選択できます。そして、システムはエクストラネットと接続し、データはデフォルトルートを通して転送されます。

ネットフォールトトレランス

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**設定することができます。これにより、一方のNICカードが故障した場合、ビデオレコーダーは自動的にもう一方のスタンバイNICカードを有効にし、システム全体の正常な動作を保証します。

注

作業モードは特定のモデルでのみ利用可能です。

3. ネットワークパラメータを設定する。

- IPv4 DHCP

DHCPサーバーが利用可能な場合は**、DHCPを**有効にして、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することができます。

エムティーユー

最大伝送単位（MTU）とは、1つのネットワークトランザクションで通信できる最大のネットワーク層プロトコルのデータ単位のサイズである。

DNSサーバーの自動取得

DHCPが有効になっている場合。**DNSサーバーの自動取得]**をオンにすると**、優先DNSサーバーを**取得できます。
および**代替DNS**サーバを指定する。

- アイピーブイシックス

ルーター広告

ネットワーク内のルーターがIPv6をサポートしている場合は、このモードをデフォルトとして使用することをお勧めします。

オート

ネットワーク内にDHCPv6デバイスがある場合は、このモードを使用することをお勧めします。

マニュアル設定

IPv6パラメータを手動で入力する場合は、このモードを使用する。

4. 保存をクリックする。

4.1.2 DDNSの設定

ダイナミックドメインネームサーバー（DDNS）は、ダイナミックユーザー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する。

始める前に

DynDNS、PeanutHull、NO-IPサービスをISPに登録していることを確認してください。

ステップ

1. システム→ システム設定→ ネットワーク→ ネットワーク→ DDNS .

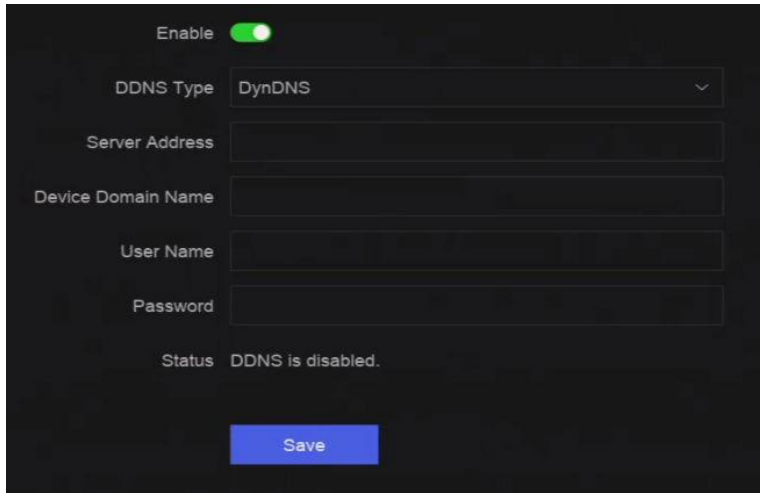


図4-2 DDNS

2. **Enableをオンに**する。
3. DDNSタイプを選択します。
4. サービスアドレス、ドメインパラメータを設定します。
5. **保存を**クリックする。

4.1.3 PPPoEの設定

PPPoEでインターネットに接続する場合はユーザー名とパスワードを設定する必要があります。PPPoEサービスの詳細については、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。

ステップ

1. **システム→ システム設定→ ネットワーク→ ネットワーク→ PPPoE** .

図4-3 PPPoE

2. **Enableをオンに**する。
3. ユーザー名とパスワードを入力してください。
4. **保存を**クリックする。

次に何をすべきか

System→ System Maintenance→ Running Info→ Network Statusにアクセスして、PPPoEのステータスを表示する。

4.1.4 マルチキャストの設定

マルチキャストは、ネットワーク経由で許可される最大数を超えるカメラのライブ表示を有効にするように設定できます。

ステップ

1. **システム→ システム設定→ ネットワーク→ ネットワーク→ その他** .
2. マルチキャストパラメータを設定する。

注

- ネットワークビデオセキュリティクライアントを介してデバイスを追加する場合、マルチキャストグループIPアドレスは、デバイスのマルチキャストIPアドレスと同じでなければなりません。
- IPv4の場合、224.0.0.0から239.255.255.255までのClass-D IPをカバーし、239.252.0.0から239.255.255.255までのIPアドレスを使用することを推奨します。CMSソフトウェアにデバイスを追加する場合、マルチキャストアドレスはデバイスのものと同じでなければなりません。

3. **保存を**クリックする。

4.2 プラットフォーム・アクセス設定

4.2.1 Hik-Connectの設定

Hik-Connectは、ビデオレコーダーにアクセスし、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、ビデオセキュリティシステムへの便利なリモートアクセスを得ることができます。

ステップ

1. **システム→ システム設定→ ネットワーク→ Hik-Connectにアクセスして**ください。

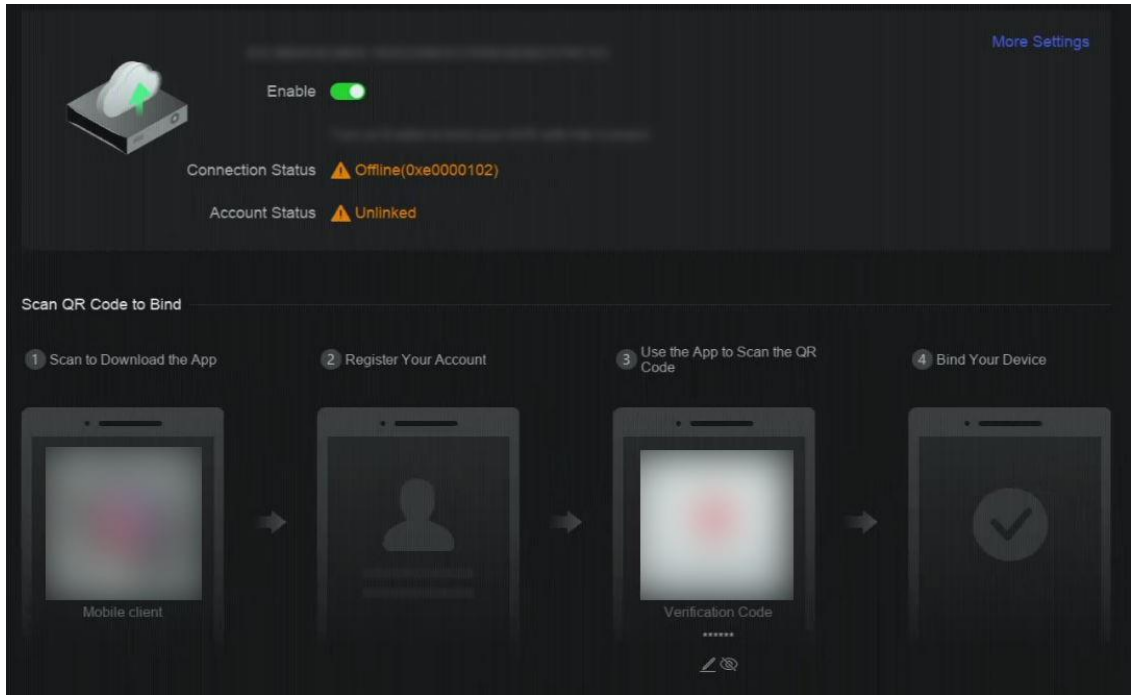


図 4-4 Hik-Connect

2. **Enableをオンに**すると、サービス規約がポップアップ表示されます。
3. サービス同意する。
4. Hik-Connectアプリをダウンロードする。
   - 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。
   - ***https://appstore.hikvision.com*** からアプリをダウンロードする。

図 4-5 Hik-Connect のダウンロード

5. アプリでアカウントを登録する。
6. **オプション：詳細設定]を**クリックして、**ストリーム暗号化**、**プラットフォーム時間同期**、**アダプティブ・ビットレート・ストリーミングを**有効にするか、**サーバーIPアドレスを**編集します。

   ストリーム暗号化

この機能を有効にすると、リモートアクセスとライブビューで認証コードの入力が必要になる。

プラットフォームの時刻同期

デバイスはNTPサーバーの代わりにHik-Connectで時刻を同期します。

アダプティブ・ビットレート・ストリーミング

ネットワーク環境が悪い場合、デバイスは自動的にビデオのビットレートを調整し、流暢な再生を保証する。

サーバーIPアドレス

Hik-ConnectサーバーのIPアドレス。

7. クリックして認証コードを設定する。

8. Hik-Connectアプリを使用してデバイスのQRをスキャンし、Hik-Connectアカウントとデバイスをバインドします。

注

デバイスがすでにアカウントで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でのバインドを解除できます。

結果

- デバイスがHik-Connectで接続されている場合、**接続ステータスはオンラインに**なります。
- 端末がHik-Connectアカウントとバインドされている場合、**アカウントステータスは「Linked」に**なります。

次に何をすべきか

Hik-Connect経由でビデオレコーダーにアクセスできます。

4.2.2 OTAPの設定

OTAP（オープン・シング・アクセス・プロトコル）は、パブリックネットワークおよびプライベートHikVisionプロトコルの統一された統合標準およびプッシュプルモードです。OTAPを有効にした後、他のアプリケーションはこのプロトコルを介してビデオをリモートで見ることができます。

始める前に

デバイス・ネットワークがOTAPを通じてアクセス可能であることを確認する。

ステップ

1. システム→ システム設定→ ネットワーク→ プラットフォーム・アクセス→ OTAP .

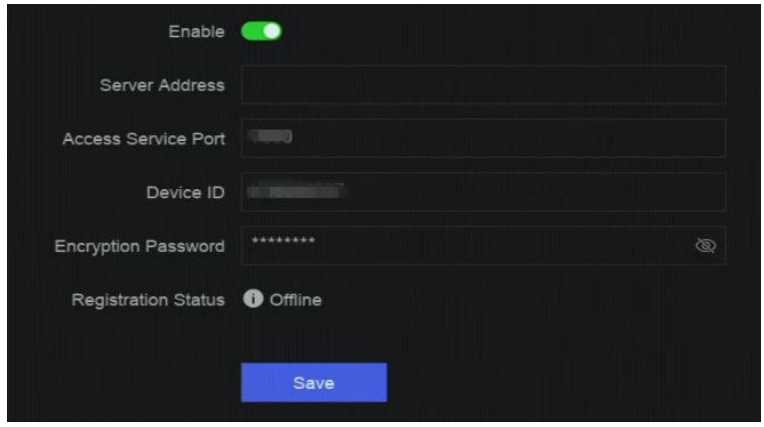


図4-6 OTAP

2. OTAPをオンにする。

3. パラメータを設定する。

4. 保存をクリックする。

4.2.3 ISUPの設定

ISUP (Intelligent Security Uplink Protocol) は、サードパーティ・プラットフォームが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、コマンドを提供します。このプロトコルにより、サードパーティ・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制御などの機能を実現できます。

ステップ

1. システム→ CX→ システム設定→ ネットワーク→ プラットフォーム・アクセス→ ISUP .

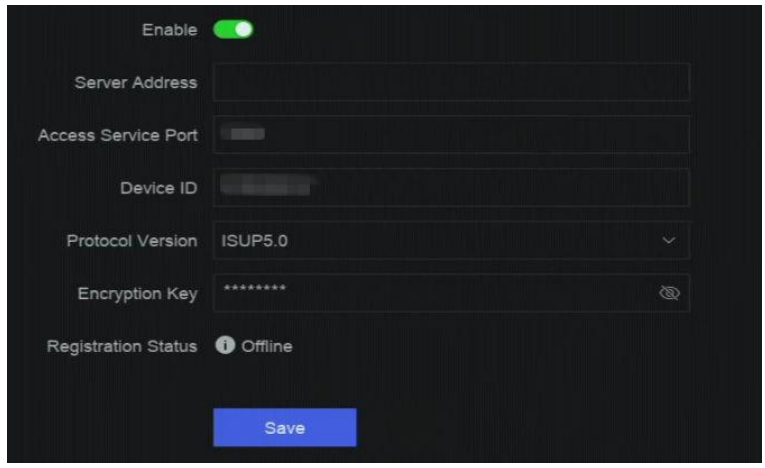


図4-7 ISUP

2. Enableをオンにする。

注

ISUPが有効な場合、Hik-Connectアクセスは自動的に無効になります。

3. 関連するパラメータを設定する。

サーバーアドレス

プラットフォームサーバーのIPアドレス。

アクセスサーバーポート

プラットフォームサーバーポートは、1024から65535の範囲である。実際のポートはプラットフォームが提供する。

デバイスID

デバイスIDはプラットフォームが提供する。

プロトコル・バージョン

ISUP プロトコルのバージョンは ISUP 5.0 。

暗号化キー

暗号化パスワードは ISUP V5.0 バージョンを使用する場合に必要で、デバイスとプラットフォーム間のより安全な通信を提供します。デバイスが ISUP プラットフォームに登録された後、確認のために入力します。空や「ABCDEF」は使用できません。

4. **保存を**クリックする。

デバイスの再起動後、登録状態（オンラインまたはオフライン）を確認できます。

4.2.4 SDKサービスの設定

SDK（ソフトウェア開発キット）サービスは、サードパーティのパートナーがさまざまな機能を統合するために使用されます。強化されたSDKサービスは、SDKサービス上でTLSプロトコルを採用し、より安全なデータ伝送を提供します。

ステップ

1. **System→ System Settings→ Network→ Platform Access→** SDK にアクセスしてください。

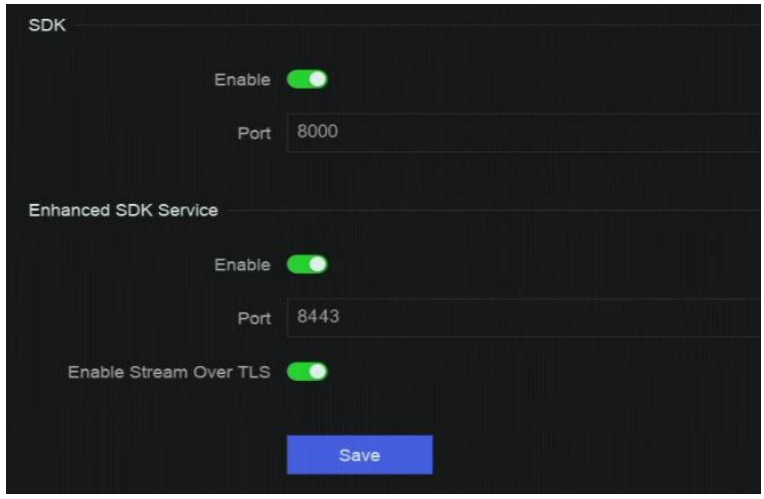


図 4-8 SDK サービス

2. お客様の要件に応じてSDKと**拡張SDKサービスを**設定します。

注

拡張SDKサービスのポートはデフォルトで8443です。

3. オプション：Stream Over TLSを有効にする。Stream over TLS暗号化技術は、より安全なストリーム伝送サービスを提供します。

4. 保存をクリックする。

4.2.5 ISAPIを有効にする

ISAPI (Internet Server Application Programming Interface) はHTTPベースのオープン・プロトコルで、システム・デバイス（ネットワーク・カメラ、NVRなど）間の通信を実現できます。

System→ System Settings→ Network→ Platform Access→ ISAPIにアクセスして機能を有効にする。

4.2.6 ONVIFの設定

ONVIFプロトコルはサードパーティ製カメラとの接続を可能にします。追加されたユーザ・アカウントには、ONVIFプロトコル経由で他のデバイスを接続する権限があります。

ステップ

1. システム→ CX→ システム設定→ ネットワーク→ プラットフォーム・アクセス→ ONVIF .

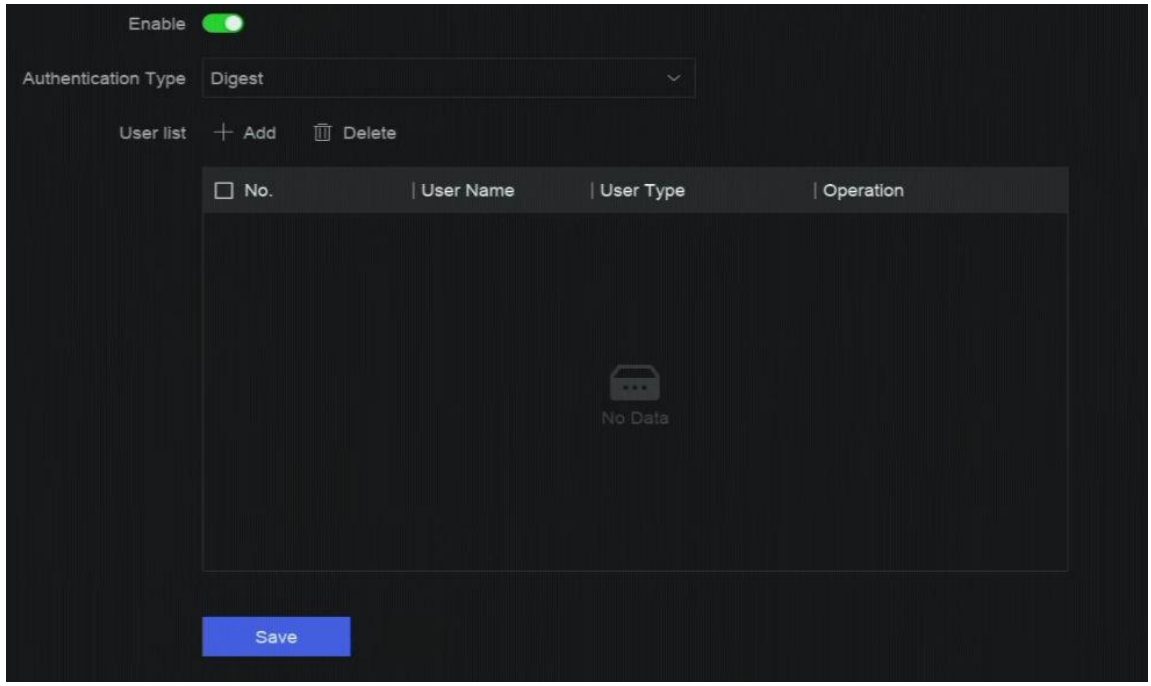


図4-9 ONVIF

2. **Enableをオンに**する。
3. 認証タイプを選択します。
4. ユーザーを追加するには**Addを**クリックします。
5. ユーザー名とパスワードを設定する。

注意

製品のセキュリティを向上させるために、ご自身で選択した強力なパスワード（大文字、小文字、数字、特殊文字のうち少なくとも3つを含む、最低8文字を使用）を作成することを強くお勧めします。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、より製品を保護することができます。

6. **保存を**クリックする。

4.2.7 ログサーバーの設定

ログはバックアップのためにログサーバーにアップロードすることができる。

ステップ

1. **System→ System Settings→ Network→ Platform Access→ Log** Server にアクセスする。

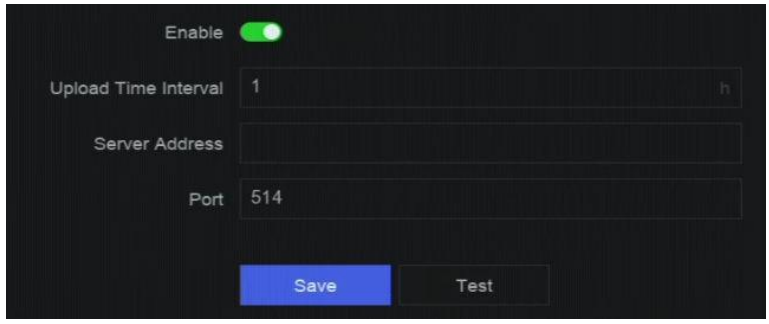


図 4-10 ログ･サーバー

2. **Enableをオンに**する。
3. **アップロードの時間間隔**、**サーバーのIPアドレス**、**ポートを**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チェックする。
5. **保存を**クリックする。

4.3 ネットワークサービス設定

4.3.1 HTTP(S)の設定

HTTP（ハイパーテキスト転送プロトコル）とHTTPS（ハイパーテキスト転送プロトコルセキュア）ポートは、ウェブブラウザを介したリモートアクセスに使用されます。HTTPSプロトコルは、暗号化された転送とID認証を可能にし、リモートアクセスのセキュリティを向上させます。

ステップ

1. **システム→ システム設定→ ネットワーク→ ネットワークサービス→ HTTP(S)**にアクセスします。

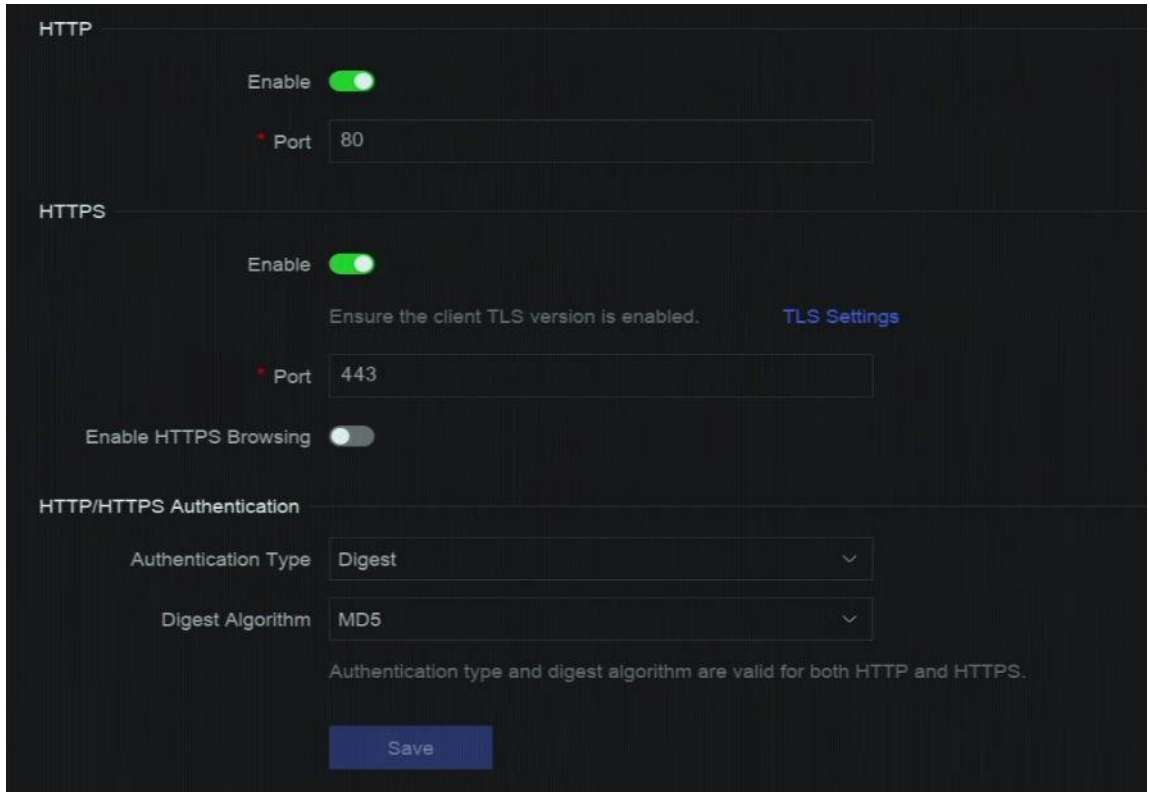


図4-11 HTTP(S)

2. **オプション：**HTTPまたはHTTPSをオンにします。
3. HTTPまたはHTTPSの**ポートを**表示または編集します。
4. **HTTP/HTTPS認証を**設定します。**認証タイプ**

   セキュリティ上の、以下の2つの認証タイプを選択することをお勧めします。
   認証タイプは**ダイジェスト**。

   ダイジェスト・アルゴリズム

   ダイジェスト・アルゴリズムはHTTP/HTTPSに基づくもので、主にユーザー認証のダイジェスト認証に使われる。
5. **保存を**クリックする。

4.3.2 RTSPの設定

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。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を特別に保護することができます。

ステップ

1. **システム→ システム設定→ ネットワーク→ ネットワークサービス→ RTSP** .

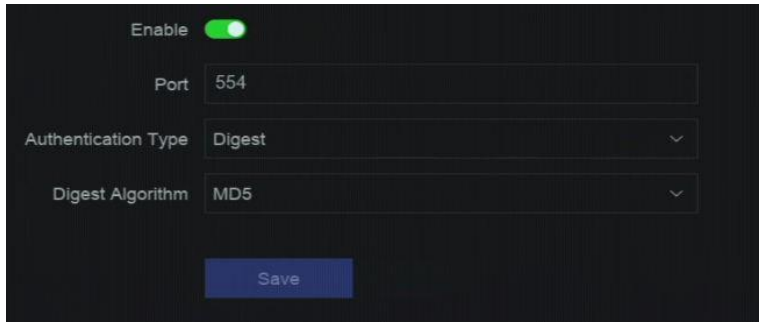


図4-12 RTSP

2. パラメータを設定する。

ポート

ポートはデフォルトで554。

認証タイプ

ダイジェスト認証を選択した場合、ダイジェスト認証を持つリクエストのみがIPアドレス経由でRTSPによるビデオストリームにアクセスすることができます。セキュリティ上の認証タイプは**ダイジェストを**選択することをお勧めします。

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に基づいており、ユーザー認証のダイジェスト認証のためのアルゴリズムです。

3. 保存をクリックする。

4.3.3 WebSocketの設定

TCPをベースにしたWebSocketプロトコルは、ウェブブラウザとサーバー間の全二重通信を提供することを目的としている。双方向のインタラクティブな通信セッションを開くことができる。

ステップ

1. System→ System Settings→ Network→ Network Service→ WebSocket(s) .

2. Enableをオンにする。

3. ポートを設定する。

4. 保存をクリックする。

4.3.4 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経由のリモートアクセスを実現するポートマッピングには、UPnP™（Universal Plug and Play）と手動マッピングの2つの方法が用意されています。UPnP™は、デバイスがネットワーク上の他のネットワークデバイスの存在をシームレスに検出し、データ共有や通信など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経由してデバイスをWANに高速接続できます。

始める前に

デバイスのUPnP™機能を有効にするには、デバイス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。デバイス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、デバイス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. **システム→ システム設定→ ネットワーク→ ネットワークサービス→ NAT** .

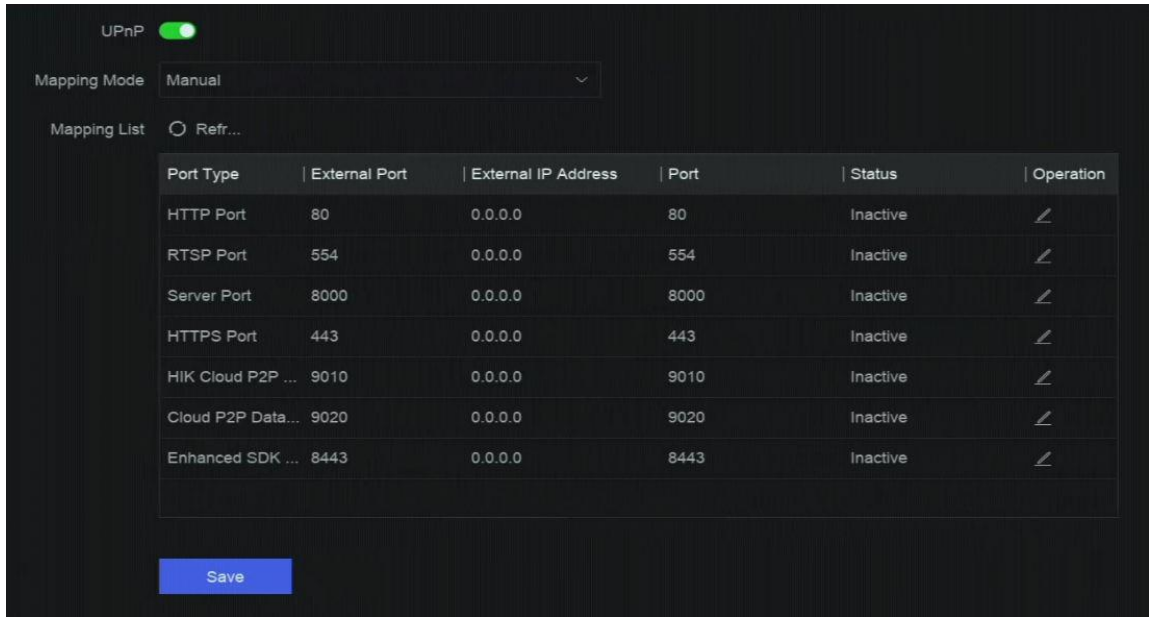


図 4-13 ポートマッピング（NAT）

2. **Enableをオンに**する。
3. **マッピングモードを**設定します。

   オート

   ポートマッピング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する。

   マニュアル

   外部手動で編集できます。

4. **Mapping** Mode**がManualに**選択されている場合は、クリックして対応するポートを編集します。

注

- RTSPポート番号の値は554または1024～65535、その他のポートの値は1～65535で、異なる値でなければなりません。複数のデバイスが同じルーターの下でUPnP™設定されている場合、各デバイスのポート番号の値は一意でなければなりません。
- **外部ポートは**、ルーターのポートマッピング用の内部ポート番号を示します。

5. **保存を**クリックする。

次に何をすべきか

ルーターの仮想サーバー設定画面に入り、内部/外部ソースポートの空欄に内部/外部ポートの値、その他必要な内容を入力します。

4.3.5 IoTの設定

NVRがセキュリティ・コントロール・パネルからのアラームを受信するネットワーク・ポートを設定できます。

System→ System Settings→ Network→ Network Service→ IoT にアクセスして機能を有効にし、ポート番号を設定する。

注

ここで設定したポート番号は、セキュリティコントロールパネルのアラーム送信ポートと同じでなければ。

第5章 ユーザー管理

管理者用のデフォルトアカウントがある。管理者ユーザー名は**admin**です。管理者は、ユーザーを追加、削除、編集する権限を持っています。GuestおよびOperatorユーザは、制限された権限しか持ちません。

システム→ システム設定→ ユーザー管理 にアクセスしてください。

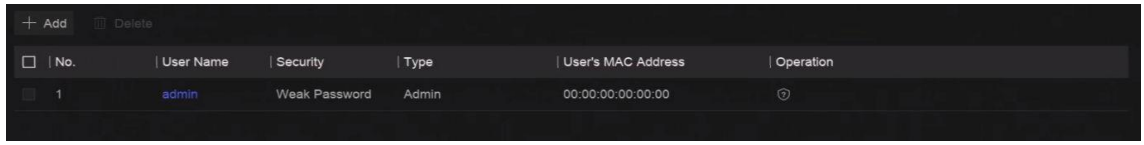


図 5-1 ユーザー管理 表 5-1 アイコン／ボタン

の説明

アイコン/ボタン	説明
	アカウントの設定します。
追加	新しいゲストまたはオペレーターユーザーを追加します。
	選択したユーザーを削除します。

注

操作の前に、管理者パスワードを確認する必要があります。

第6章 デバイス・アクセス

ビデオレコーダーは、ネットワークカメラ、入退室管理装置、アラーム装置など、複数のデバイスタイプにアクセスできる場合があります。ビデオレコーダーのアクセス機能については実際のデバイスを参照してください。

6.1 アクセス・ビデオ・デバイス

ビデオ機器にアクセスする方法はいくつかある。

6.1.1 自動検索されたオンライン・ネットワーク・カメラの追加

同じネットワーク・セグメント上のネットワーク・カメラを自動的に検索し、デバイスに追加できます。

ステップ

1. **System→ Device Access→ Device→ Video Device→ Online Device List** へ。

2. デバイスを選択します。

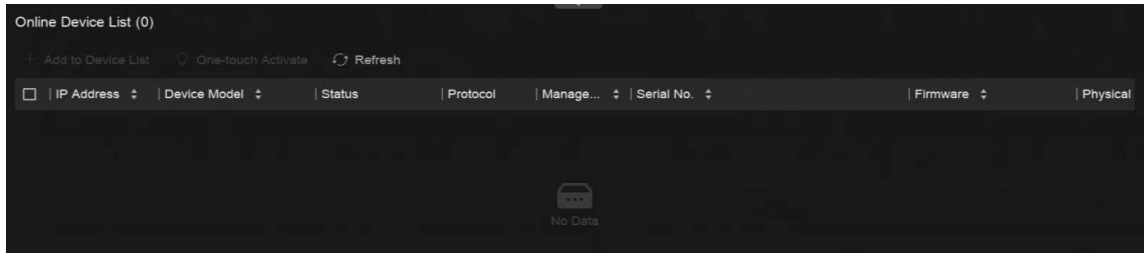


図6-1 自動検索されたオンライン・ネットワーク・カメラの追加

3. **デバイスリストに追加】を**クリックします。

注

- カメラのパスワードがデフォルトのパスワードと同じであることを確認してください。デフォルト・パスワードは**More → Default Password Settingsで**設定できます。
- 検索されたネットワーク・カメラがアクティブになっていない場合、デバイスはデフォルトのパスワードを使用してアクティブになっていないネットワーク・カメラを追加します。デフォルトパスワードは
  →デフォルトのパスワード設定。
- ネットワークカメラが正常に追加されると、ステータスは**オンラインに**なります。
- デバイス名をクリックしてパラメータを追加できます。

6.1.2 ネットワークカメラを手動で追加する

手動でネットワークカメラをビデオレコーダーに追加します。

始める前に

- ネットワークカメラがビデオレコーダーと同じネットワークセグメントにあることを確認してください。
- 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が起動していることを確認します。

ステップ

1. **System→ Device Access→ Device→ Video Device に**アクセスしてください。

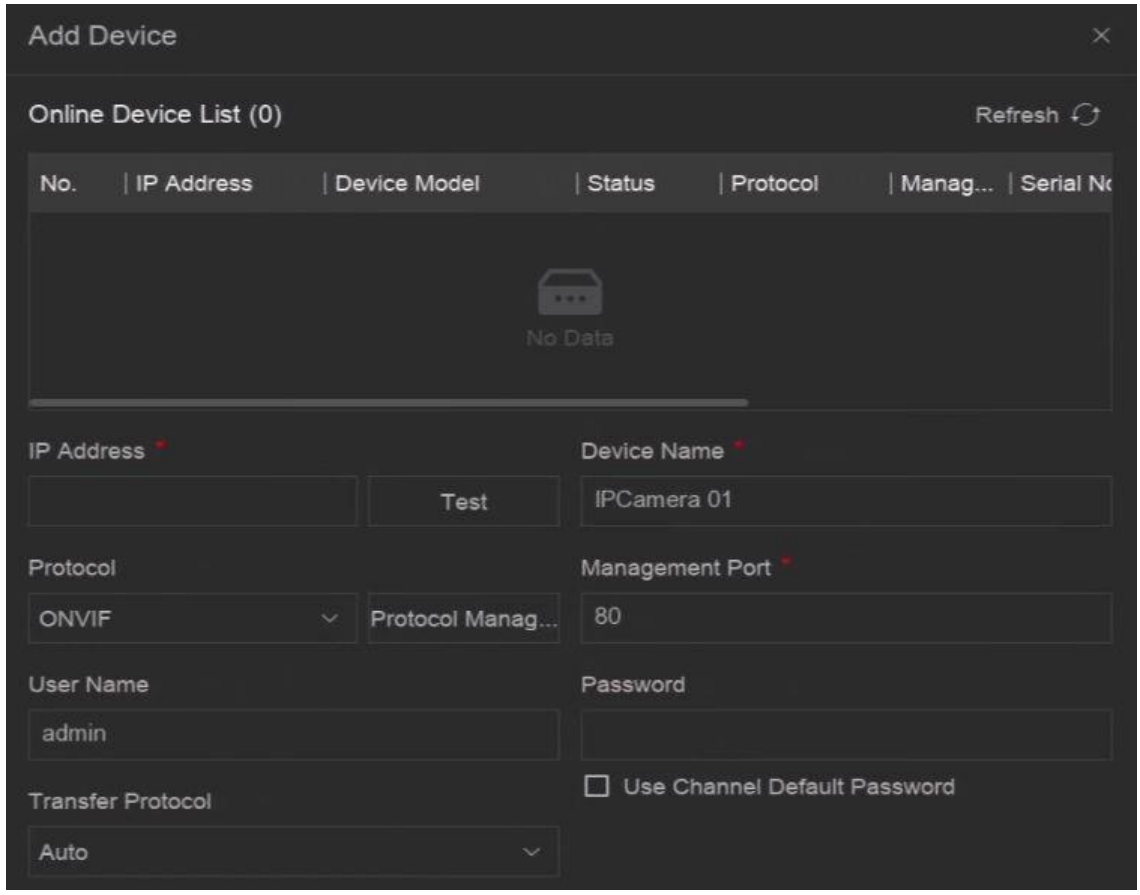


図6-2 手動によるネットワークカメラの追加

2. **追加を**クリックする。

3. ネットワークカメラのパラメータを入力します。

チャンネルのデフォルトパスワードを使用

これが有効な場合、ビデオレコーダーは設定されたチャンネル・デフォルト・パスワードでカメラを追加します。

その他の設定

証明書の検証を有効にして、証明書でカメラを検証できます。証明書はカメラの識別形式であり、より安全なカメラ認証を提供します。この機能を使用するには、まずネットワークカメラの証明書をデバイスにインポートする必要があります。

4. **オプション：**他のネットワーク・カメラを追加するには、**［追加を続行］を**クリックします。
5. **追加を**クリックする。

6.1.3 PoE経由でネットワークカメラを追加

PoE（パワー・オーバー・イーサネット）ネットワークカメラは、背面パネルにあるPoEインターフェイスを介してデバイスに直接接続できます。

ネットワークケーブルを使用してPoEネットワークカメラをデバイスに接続した後、対応するPoEインターフェースを設定する必要があります。詳しくは***PoE（Power over Ethernet）インターフェースの設定を***参照してください。

6.1.4 OTAPプロトコルによるソーラー電源カメラの追加

OTAPプロトコルを介して、ソーラーカメラをデバイスに追加できます。

始める前に

お使いのデバイスとソーラー電源カメラ間のネットワークがOTAPプロトコルでアクセス可能であることを確認してください。

ここにあなたのタスクのコンテキストを入力します（オプション）。

ステップ

1. **System→ Device Access→ Device Configuration→ Access Service→ OTAP Service** に移動します。
2. **Enableをオンに**する。
3. OTAP**サーバーの**ポートと**暗号化キーを**設定します。
4. **オプションIPカメラの自動追加を**有効にします。デバイスのOTAPパラメータが設定された後、（OTAPプロトコルを介して）新しく署名されたネットワークカメラをデバイスに自動的に追加できます。
5. ウェブブラウザでソーラーカメラのOTAPプロトコルパラメータを設定します。詳細については、カメラのユーザーマニュアルを参照してください。

注

太陽電池カメラ OTAP プロトコルパラメータは、デバイスと同じでなければならない。

6. ソーラーカメラをデバイスに追加する。
   - **IPカメラの自動追加を**有効にすると、（OTAPプロトコルを介して）新しく署名されたネットワークカメラが自動的にデバイスに追加されます。
   - **オンラインデバイスリストから**ソーラーカメラを選択し、**クイック追加を**クリックします。
7. **System→ Device Access→ Device→ Video DeviceでAddを**クリックし、Protocolに**OTAPを**選択し、**Addを**クリックします。

次に何をすべきか

- ソーラー・カメラをデバイスに追加すると、カメラを起動したり、バッテリー残量を確認したり、ライブ・ビデオを見たり、ウェブ・ブラウザでパラメーターを設定したりすることができる。
- カメラのANR（自動ネットワーク補充）を設定します。**録画設定 スケジュールの**を参照してください。

6.1.5 カスタムプロトコルによるネットワークカメラの追加

標準プロトコルを使用していないネットワークカメラにはカスタムプロトコルを設定して追加することができます。システムには8つのカスタムプロトコルが用意されています。

始める前に

- ネットワークカメラがRTSPストリーミングに対応していることを確認します。
- ネットワークカメラのメインストリームまたはサブストリームを取得するためのURL（Uniform Resource Locator）を準備します。

ステップ

1. **System→ Device Access→ Device→ Video Device に**アクセスしてください。
2. **More→ Custom Protocol Management** 、または **Add→ Protocol Management** をクリックします。

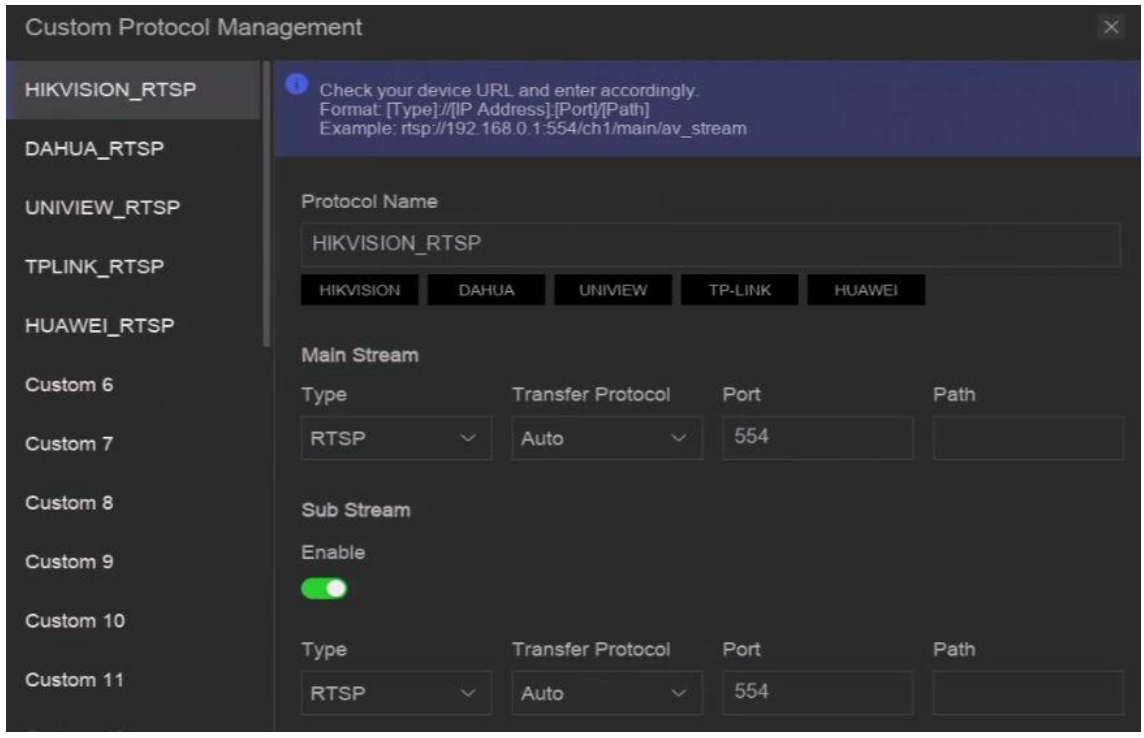


図6-3 カスタマイズされたプロトコルによるネットワークカメラの追加

3. 左側でプロトコルの種類を選択する。
4. プロトコルパラメータを設定する。

タイプ

カスタムプロトコルを採用しているネットワークカメラは、標準の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。

転送プロトコル

Auto、**UDP**、**RTP Over RTSPの**3種類から選択可能。**ポート**

RTSPストリーミング用のポートで、デフォルト値は554。

パス

メインストリーム、サブストリームの取得URL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。一般的な形式は*[Type]:///[IP Address]:[Port]/[Resource Path]*で、例えば*rtsp://192.168.0.1:554/ch1/main/av_stream*のようになります。

注

- 以下のブランド名をクリックすると、**プロトコル**名とパスが自動的に生成されます。
  プロトコル名
- カメラがサブストリームをサポートしていない場合、またはサブストリームを使用する必要がない場合は、サブストリームを無効にできます。

5. OKをクリックする。

6. システム]→ [デバイスアクセス →[デバイス →ビデオデバイス] で **[追加**] をクリックし、ネットワークカメラを手動で追加します。

6.1.6 カメラ設定ファイルによるネットワークカメラの追加

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スポートできます。そして、エクスポートされたカメラ設定ファイルの内容は、コンピュータ上で編集することができます。編集後、ファイルを他のデバイスにインポートして、ファイル内のカメラを追加することもできます。

始める前に

ビデオレコーダーをカメラ設定ファイルのUSBフラッシュドライブに接続します。

ステップ

1. System→ Device Access→ Device→ Video Device にアクセスしてください。

2. インポート]をクリックして、USBフラッシュ内の設定ファイルをインポートします。

3. フォルダパスを設定します。

4. 確認をクリックします。

6.2 アクセス制御装置の追加

アクセス制御デバイスをビデオレコーダーに追加できます。追加方法は、***Access Video Device*** と同様です。

6.3 オーディオデバイスの追加

IPスピーカーやマイクなど、オーディオデバイスをビデオレコーダーに追加できます。

追加手順は***Access Video Device***と同様です。ビデオチャンネルをIPスピーカーとリンクした場合、IPスピーカーは音声放送に使用できます。ビデオチャンネルをマイクとリンクした場合、マイクはビデオ録画用にリンクされたビデオチャンネルの音声入力として使用されます。

6.4 POSデバイスの追加

特定のデバイスモデルでは、POS マシン/サーバーを接続できます。デバイスはPOSマシン/サーバーからトランザクションメッセージを受信し、ビデオトランザクションメッセージをオーバーレイ表示し、POSイベントアラームをトリガーすることができます。

ステップ

1. System→ Device Access→ Device→ POS にアクセスする。

2. Add をクリックして POS デバイスを追加します。

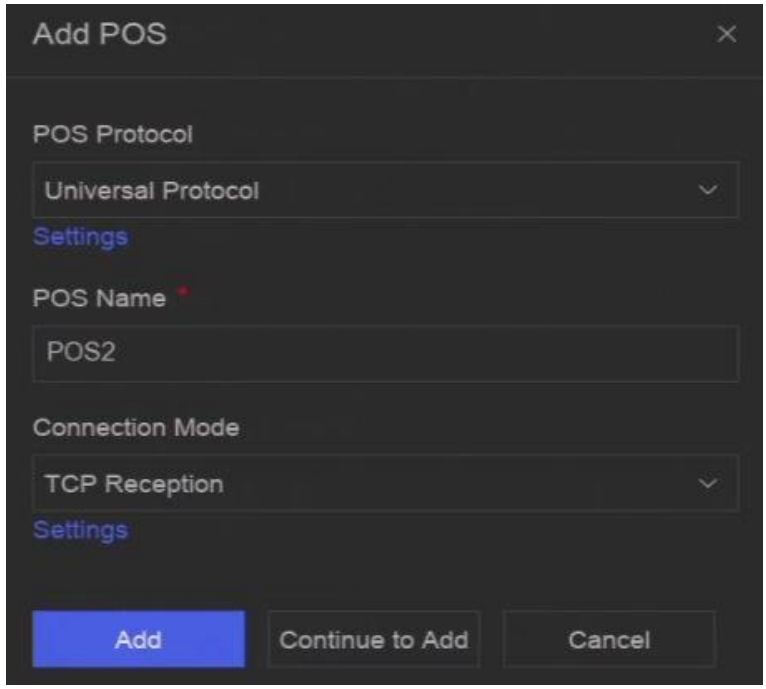


図 6-4 POS デバイスの追加

3. POSデバイスのパラメータを設定します。

POSプロトコル ユニバーサル・

プロトコル

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プロトコルをチェックすることもできます。

エプソン

EPSON プロトコルでは、固定開始行タグと固定終了行タグが使用される。

AVE

AVEプロトコルでは、固定開始行タグと固定終了行タグが使用される。シリアルポートおよび仮想シリアルポート接続タイプに対応。

ヌクレウス

AVEプロトコルでは、固定開始行タグと固定終了行タグが使用される。シリアルポートと仮想シリアルポートの接続が可能です。RS-232接続の通信にはNUCLEUSプロトコルを使用する必要があります。

接続モード TCP接続

TCP接続を使用する場合、ポートは1から65535まで設定する必要があり、各POSマシンのポートは一意でなければなりません。

UDP接続

UDP接続を使用する場合、ポートは1～65535の間で設定する必要があり、各POSマシンのポートは一意でなければなりません。

USB-RS-232接続

ポートのシリアル番号、ボーレート、データビット、ストップビット、パリティを含む、USB-to-RS-232変換器ポートのパラメータを設定します。

RS-232接続

デバイスと POS マシンを RS-232 で接続します。

マルチキャスト接続

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

スニフ・コネクション

Sniff経由でデバイスとPOSマシンを接続します。送信元アドレスと送信先アドレスの設定を行います。

4. **追加を**クリックする。

注

POSデバイスが追加されたら、操作の **を**クリックしてPOSテキストオーバーレイを設定することができま

6.5 チャンネル管理

ビデオデバイスの追加後、チャンネル番号とチャンネル名を表示し、パラメータを管理することができます。この機能は主に複数のチャンネルを持つビデオデバイスに使用します。

ビデオデバイスのチャンネルを管理するには、**システム→ デバイスアクセス→ チャンネルに**アクセスしてください。

第7章 デバイスのグループ化

追加されたデバイスは、さまざまなカスタマイズされた分類することができる。

ステップ

1. System→ Device Access→ Device Grouping にアクセスしてください。

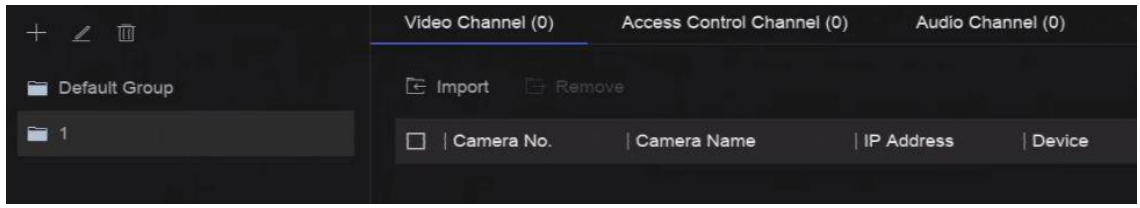


図 7-1 デバイスのグループ化

2. クリックしてグループを追加する。

注

グループが追加されたら / をクリックして/削除できます。

3. 選択したチャンネルを追加するには、**Import** をクリックします。

第8章 ビデオまたはオーディオデバイスの設定

プライバシーマスク、画像パラメータなど、追加したビデオまたはオーディオデバイスを設定できます。

8.1 H.265ストリームアクセスを有効にする

このデバイスは、IP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えて初回アクセスを行います。

ステップ

1. **System→ Device Access→ Device→ Video Device に**アクセスしてください。
2. **More→ Auto Switch to H.265** をクリックする。
3. この機能を有効にする。
4. **保存を**クリックする。

8.2 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、デイナイトスイッチ設定などを行います。

System→ Device Access→ Device Configuration→ Device Parameter→ Video Device → Display Settingsに進みます。カメラを選択し、必要なパラメータを設定します。

OSD設定

カメラのOSD（オンスクリーンディスプレイ）設定（日付／時刻、カメラ名など）。

画像設定

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をカスタマイズできます。

露出時間

カメラの露光時間を設定します（1/10000～1秒）。露出値を大きくすると画像が明るくなります。

デイナイトスイッチ

カメラは、周囲の照明条件に応じて、デイモード、ナイトモード、または自動切り替えモードに設定できます。

バックライト

カメラのワイドダイナミックレンジ（0～100）を設定します。周囲の明るさと被写体の明るさの差が大きい場合は、WDR値を設定します。

画像補正

画像の最適化する。

8.3 ビデオパラメータの設定

ビデオパラメーターはライブビュー画像と録画影響する。

System→ Device Access→ Device Configuration→ Device Parameter→ Video Device → Video Parametersにアクセスしてください。カメラを選択し、必要なパラメータを設定します。

メインストリーム

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、ビデオの画質と画像サイズを直接決定します。サブストリームと比較すると、メインストリームはより高い解像度とフレームレートでより高品質なビデオを提供します。

サブストリーム

サブストリームは、メインストリームと並行して動作する第2のコーデックです。これにより、直接録画の品質を犠牲にすることなく、送信インターネット帯域幅を削減することができます。サブストリームは、ライブビデオを表示するためのスマートフォンアプリケーションでのみ使用されることがよくあります。インターネット速度が制限されているユーザーは、この設定から最も恩恵を受けることができます。

決議

画像の解像度とは、デジタル画像がどれだけのディテールを保持できるかを示す尺度である。解像度が高ければ高いほど、度が高くなる。解像度は、ピクセルの列数（幅）×ピクセルの行数（高さ）で指定することができます（例：1024×768）。

ビットレート・タイプ

ビットレート（kビット/秒またはMビット/秒）はしばしば速度と呼ばれるが、実際には距離/時間単位ではなく、ビット数/時間単位を定義する。可変と定数の2種類がある。

フレームレート

1秒間にキャプチャされるフレームの数を指す。ビデオストリームに動きがある場合、フレームレートが高い方が画質が保たれるため有利である。

Iフレーム間隔

Iフレームはイントラ・ピクチャーとも呼ばれ、GOP（MPEGの映像圧縮技術）の最初のフレームである。圧縮後の画像として見ることができる。I-Frame間隔は、連続する2つのI-Frame間のフレーム量である。

8.4 プライバシーマスクの設定

プライバシーマスクは、ライブビューや録画から画像の一部をマスク領域で隠すことで、個人のプライバシーを保護します。

ステップ

1. System→ Device Access→ Device Configuration→ Device Parameter→ Video Device → Privacy Mask へ。

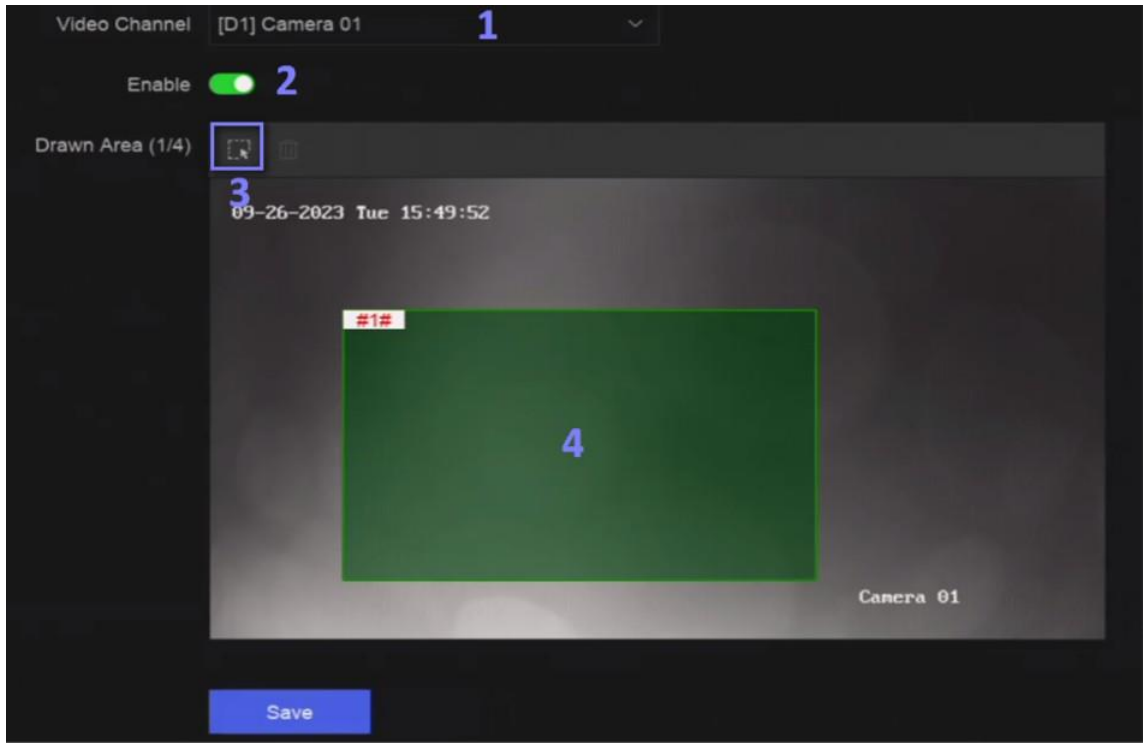


図8-1 プライバシー・マスク

2. カメラを選択します。

3. Enableをオンにする。

4. プレビューマスク領域を描画します。領域は異なるフレーム色でマークされます。

注

最大4つのプライバシーマスク領域を設定でき、各領域のサイズも調整可能。

5. 保存をクリックする。

8.5 オーディオパラメーターの設定

オーディオデバイスが追加されたら、**システム → デバイスアクセス → デバイス設定→ デバイスパラメータ→ オーディオデバイスで**パラメータを設定できます。例えば、IPスピーカーを追加した場合、その名前、音声出力音量、音質を設定できます。

8.6 OTAPサービスの設定

OTAP（オープン・シング・アクセス・プロトコル）は、パブリックネットワークおよびプライベートHikVisionプロトコルの統一された統合標準およびプッシュプルモードです。OTAPを有効にした後、他のアプリケーションはこのプロトコルを介してビデオをリモートで見ることができます。

始める前に

デバイス・ネットワークがOTAPプロトコルでアクセス可能であることを確認する。

ステップ

1. **System→ Device Access→ Device Configuration→ Access Service→ OTAP Service** に移動します。

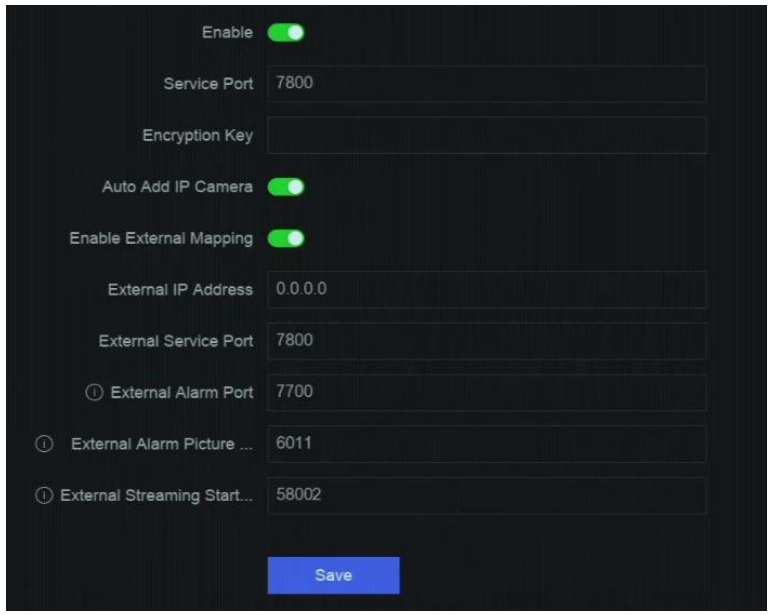


図 8-2 OTAP サービスの構成

2. **Enableをオンに**する。
3. パラメータを設定する。
4. **保存を**クリックする。

8.7 バッチ構成

接続されたデバイスは一括で設定できる。

ステップ

1. **System→ Device Access→ Device Configuration→ Batch Configuration** へ。

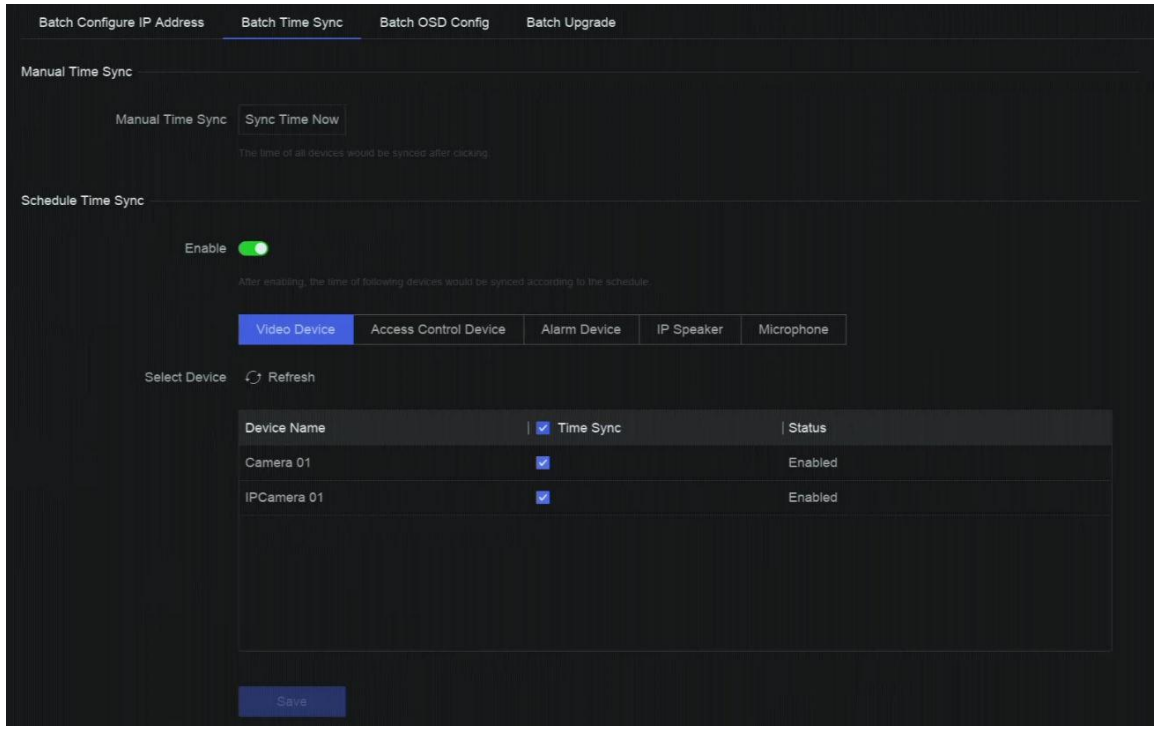


図 8-3 バッチ構成

2. IPアドレス、時刻同期、OSD、ファームウェアのアップグレードをお好みで設定できます。

手動時間同期

接続されているすべてのデバイスの時刻を手動で同期するには、**「今すぐ時刻を同期」**をクリックします。この操作は一度だけです。

スケジュール時刻同期

レコーダーは、固定されたスケジュールに従って、選択したデバイスの時刻を同期する。

3. IPアドレスの設定と時刻同期については、**「保存」**をクリックします。

8.8 PoE（パワー・オーバー・イーサネット）インターフェースの設定

PoEインターフェースは、接続されたPoEデバイスへの電力とデータの転送を可能にします。また、PoEインターフェースはプラグアンドプレイ機能をサポートしています。接続可能なPoEデバイスの数は、デバイスモデ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、オンラインデバイスへの接続にも使用できます。

始める前に

NVRがPoE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. System→ Device Access→ Device Configuration→ PoE にアクセスする。

2. 要件に応じて、PoEインターフェースの**プラグアンドプレイ**機能を有効にします。

3. デバイスのタイプを**IPスピーカー**または**カメラに**選択してください。

4. PoEインターフェースを使ってPoEカメラを接続する場合は、ネットワークケーブルの接続距離を選択します。

長距離

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。

近距離

PoEインターフェースによる近距離（100m未満）ネットワーク伝送。

注

- PoEインターフェースは、デフォルトで短距離モードで有効になっている。
- 長いネットワークケーブル（100～300m）でPoE接続されたIPカメラの帯域幅は、6MPを超えることはできません。
- IPカメラのモデルやケーブルの材質によっては、許容されるネットワークケーブルの最大長が300m未満になる場合があります。
- 伝送距離が100～250メートルの場合は、PoEインターフェースとの接続にCAT5EまたはCAT6ネットワークケーブルを使用する必要があります。
- 伝送距離が250～300mに達した場合、PoEインターフェースとの接続にはCAT6ネットワークケーブルを使用する必要があります。

5. **保存を**クリックする。

次に何をすべきか

PoEデバイスが接続されている場合、各PoEインターフェイスのステータスとパワーを表示できます。

第9章 ストレージ管理

9.1 HDDの管理

新しくインストールされたハードディスクドライブ（HDD）は、使用する前に初期化する必要があります。HDD管理インターフェイスを通じて、HDDのフォーマット、データベースの修復、HDDステータスの閲覧が可能です。

始める前に

HDDがデバイスに正しく取り付けられていることを確認してください。

ステップ

1. System→ Storage Management→ Storage HDD→ Storage HDD にアクセスする。

図 9-1 HDD の管理

2. オプション： お好みで以下の操作を行ってください。

ネットワークHDDの追加	NASまたはIP SANを追加する。
フォーマット	選択したHDDをフォーマットします。
データベースの修復	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の改善に役立つかもしれません。

注

- 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。既存のデータは影響を受けませんが、ローカルの検索・再生機能は処理中に使用できなくなります。ただし、ウェブブラウザ、クライアントソフトウェアなどを使用して、リモートで検索・再生機能を実現することは可能です。
- この中にドライブを引き抜いたり、デバイスをシャットダウンしたりしないでください。

/ HDD の取り外し/ロード。

9.2 RAID構成

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るデータストレージ仮想化技術である。RAID」としても知られるアレイは、複数のHDDにデータを保存し、1台のディスクが故障してもデータを復旧できるよう、十分な冗長性を提供する。データの分散

RAIDレベル」と呼ばれるいくつかの方法の中から、必要とされる冗長性とパフォーマンスに応じて、ドライブを横断する。

注意

RAIDにはエンタープライズレベルのHDDが必要です。

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。同じモデル、同じ容量のHDDを使用することをお勧めします。

RAIDの作成には2つの方法がある。ワンタッチで作成する場合、デフォルトの RAID タイプは RAID5 です。手動で作成する場合は、RAID0、RAID1、RAID5、RAID6、RAID10 を設定できます。

表 9-1 各 RAID タイプの HDD 要件

RAIDタイプ	必要なHDDの数
RAID0	≥2
RAID1	2
RAID5	≥3
RAID6	≥4
RAID10	4または8

注

- この機能は一部のモデルでのみ利用可能です。
- 配列例外イベントが発生した場合、対応するリンクアクションは **システム→ システム設定→ 例外** .

9.2.1 ディスクアレイの作成

ディスクアレイは、アレイモードを有効にした後に作成できる。

始める前に

- **System→ Storage Management→ Storage Mode** で、**Storage Mode** が **Quota に**設定されている。
- 十分なHDDがデバイスに正しくインストールされている。また、アレイ作成用のHDDはAIまたはエンタープライズレベルである。

ステップ

1. **System→ Storage Management→ Storage HDD→ Array Management** に移動する。
2. **Enable Array Mode（アレイモードを有効に**する）をクリックする。

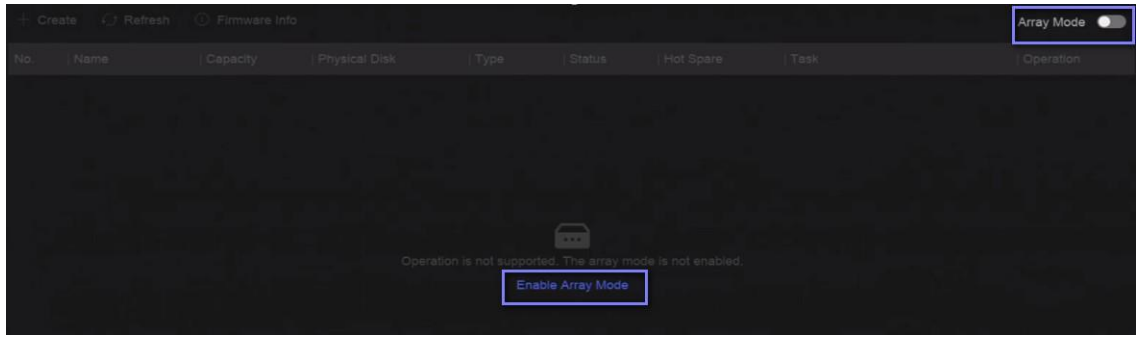


図 9-2 RAID の有効化

3. デバイスの再起動を待つ。

4. **System→ Storage Management→ Storage HDD→ Array Management** に再度アクセスします。

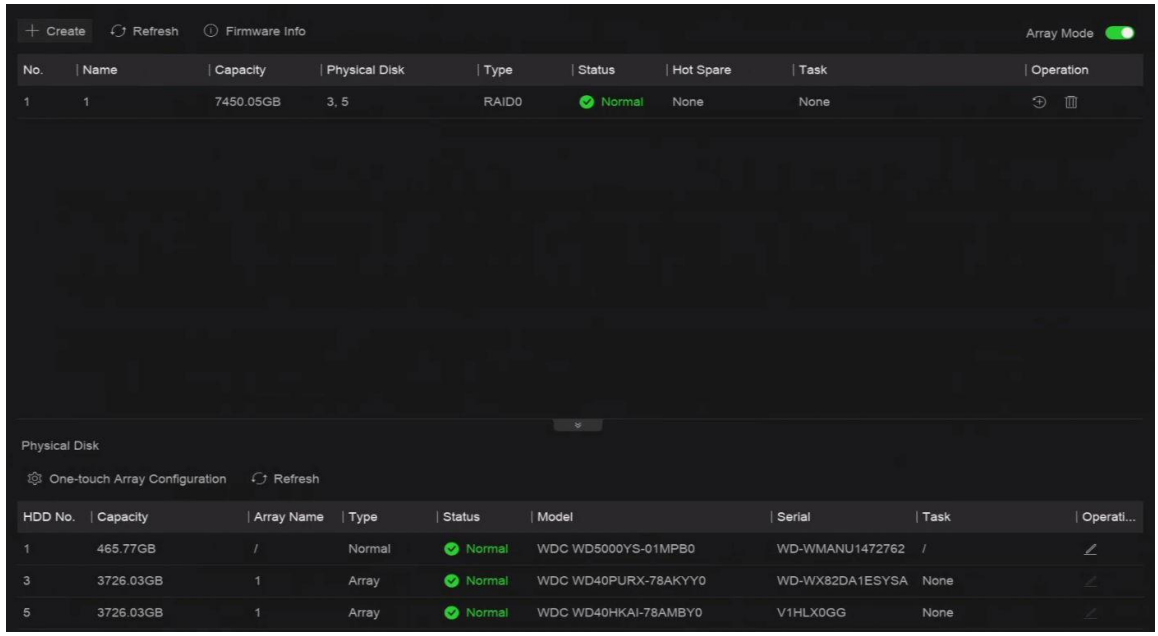


図9-3 アレイ管理

5. 配列を作成する。

作成方法 作成方法

ワンタッチ・アレイ構成 **One-touch Array Configuration**】をクリックします。

注

デフォルトでは、ワンタッチ構成で作成されるアレイはRAID 5です。

手動作成 手動でRAID 0、RAID 1、RAID 5、RAID 6、またはRAID 10アレイを作成するには、**Create** をクリックします。

9.2.2 アレイの再構築

アレイのステータスには、**機能**、**劣化**、**オフラインが**あります。アレイに保存されたデータの高いセキュリティと信頼性を確保するために、アレイの状態に応じて迅速かつ適切なメンテナンスを行う。

ステップ

1. **System→ Storage Management→ Storage HDD→ Array Management** に移動する。

2. アレイを再構築する。

表 9-2 再構築の方法

再建方法	説明
オート・リビルド	アレイにホットスペアディスクがあり、ホットスペアディスクの容量がアレイの最小容量のディスクより小さくないこと。ホットスペアディスクを設定するには、**Physical Disk のOperation** 列で をクリックします。 アレイ内のHDDが動作しない場合、ホットスペアディスクが起動し、アレイが自動的に再構築される。 注 自動終了したら、別のHDDを取り付け、ホットスペアディスクとして設定することをお勧めします。
マニュアル・リビルド	アレイにホットスペアディスクがない場合は手動でアレイを再構築する必要があります。 **システム → ストレージ管理 → ストレージHDD → アレイ管理** と進み、リビルドするホットスペアディスクをリストから選択する。

9.2.3 配列の削除

System→ Storage Management→ Storage HDDに移動し、クリックして選択したアレイを削除します。

9.2.4 ファームウェア情報を見る

アレイファームウェアの情報を表示したり、バックグラウンドタスクの速度を設定することができます。

始める前に

ディスクアレイが有効になっていることを確認する。

ステップ

1. **System→ Storage Management→ Storage HDD→ Array Management** に移動する。
2. **ファームウェア情報を**クリックします。
3. **オプション：バックグランドタスクスピードを**設定する。

9.3 ストレージモードの設定

ステップ

1. **System→ Storage Management→ Storage Mode** に進む。

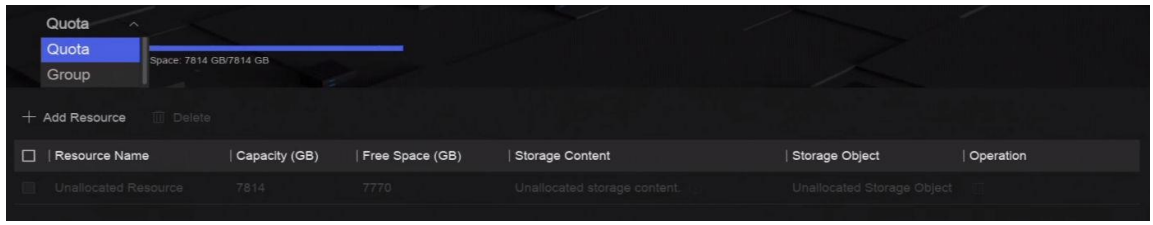


図 9-4 ストレージ・モード

2. **クォータ**またはグループを選択しま
   す。**クォータ**

   各カメラやオーディオデバイスは、ビデオ、写真、またはオーディオを保存するために割り当てられたクォータを設定することができます。

   グループ

   複数のHDDを管理可能。HDDの設定により、指定したチャンネルの映像を特定のHDDグループに録画できる。
3. 対応するパラメータを設定する。
   - **クォータ**：ストレージオブジェクトに領域を割り当てる。
   - **グループ**：チャンネルをHDDグループにリンク。

9.4 その他のストレージパラメータの設定

System→ Storage Management→ Advanced Settings にアクセスする。

表 9-3 パラメータの説明

パラメータ名	説明
HDDスリーピング	HDDのモードを選択します。**パフォーマンスモード**、**バランスモード** **省エネ**モードが選択可能。
上書き	一杯になると、古いファイルを削除して新しいファイルを書き込み続ける。
カメラVCAデータの保存	カメラのVCAデータをデバイスに保存すると、**イベントセンターで**検索できるようになります。
最大ビデオ1本あたりの長さ	これは、デバイスからビデオをエクスポートする際の各ビデオファイルの長さです。
タグ動画ポストレコーディング	タグを追加した後、スケジュールされた時間の後に録画するように設定した時間です。 **注** • ライブビューまたは再生中に クリックしてタグを追加できます。 • タグ動画を検索するには、→**Backup→ By Tagに**アクセスしてください。
eSATA	リアパネルにeSATAインターフェイスを持つデバイス用。
使用方法	eSATAの使用量を設定します。

9.5 マンジェUSBフラッシュ・ドライブ

USBフラッシュ・ドライブをデバイスに挿入すると、残りのストレージ容量を確認したり、コンテンツを管理したり、フォーマットしたりすることができます。

USBフラッシュドライブがデバイスに接続されると、デバイスのアップグレードやバックアップなど、短い操作を実行することができます。その間、右上に新しいアイコン 表示されます。

第10章 スケジュール設定

デバイスはスケジュールに従ってファイルをディスクに保存する。

10.1 スケジュールテンプレートの設定

スケジュールテンプレートが設定されると、そのテンプレートを録画スケジュールとして使用することができます。

ステップ

1. **システム→ システム設定→ テンプレート設定→ 休日スケジュール** .
2. **追加を**クリックする。

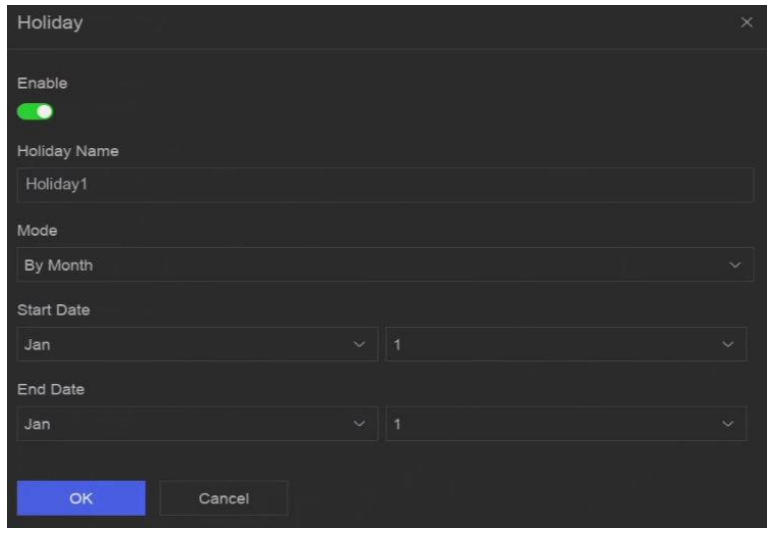


図10-1 休日の追加

3. **Enableをオンに**する。
4. 休日の設定

注

休日を設定すると、休日スケジュールを独自に設定できるようになります。休日スケジュールは通常スケジュール（月～日）よりも優先度が高くなります。

5. **保管スケジュールを**設定する。
   1) **Storage Scheduleを**クリックします。
   2) テンプレート名を選択します。

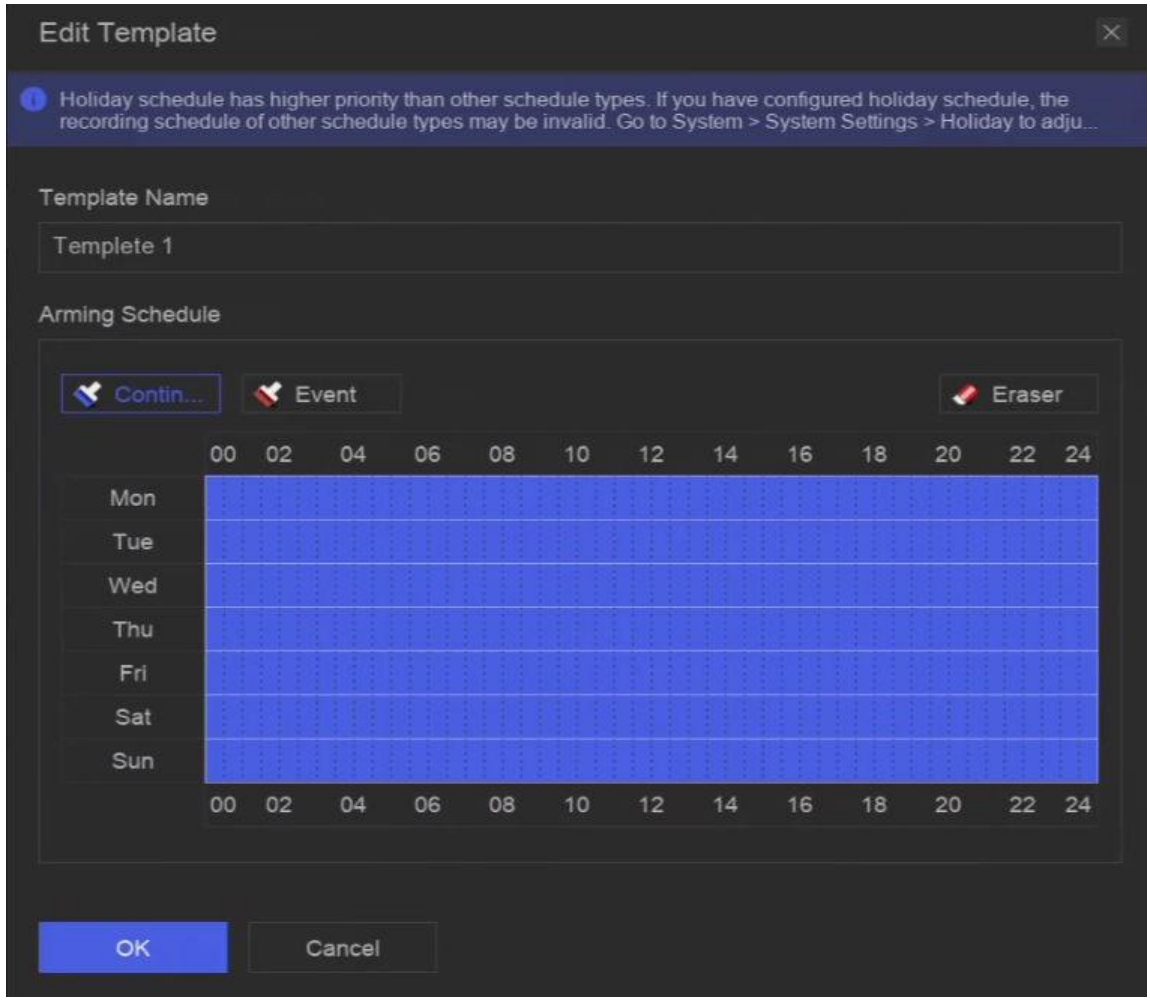


図 10-2 テンプレートの編集

3) 録画タイプを選択します。例えば、**イベント**。

4) タイムバー上でカーソルをドラッグすると、スケジュールが描画されます。

注

- タイムバー上にカーソルを移動した後、00:00-24:00 クリックして、指定したタイムスケジュールを設定することもできます。
- **消しゴムを**クリックするとスケジュールが消去されます。

注

また、**Configure Templateを**クリックして、**System→ Storage Management**でテンプレートを構成することもできます。

→保存スケジュール→ ビデオ録画 / 画像キャプチャー / 音声録音 .

6. OKをクリックする。

10.2 録画スケジュールの設定

カメラは設定された録画スケジュールに従って自動的に録画を開始/停止する。

ステップ

1. **システム→ ストレージ管理→ ストレージスケジュール→ ビデオ録画** .

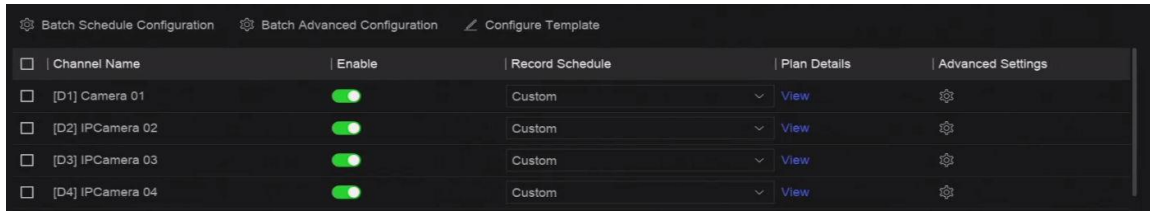


図 10-3 ビデオ録画の設定

2. カメラの**有効**化を**オンに**する。

3. スケジュールタイプを選択します。

注

録画スケジュールをカスタムに設定した場合、タイムバー上でカーソルをドラッグしてカスタマイズした録画スケジュールを設定するか、タイムバー上でカーソルを移動し、00:00-24:00 クリックして指定したタイムスケジュールを設定することができます。

4. スケジュールを表示するには、**「表示」**をクリックします。

図 10-4 スケジュールの表示

5. オプション： その他の詳細パラメータを設定するには、**[Advanced Settings]**の下にある⚙クリックします。

表 10-1 高度なパラメータの説明

パラメータ	説明
オーディオの録音	オーディオ録音を有効または無効にする。 **注** チャンネルにオーディオあるか、オーディオ機器が接続されていること。
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カードが自動的にビデオを保存できるようにし、ネットワークが回復した後にデータを同期することができます。
プレレコード	スケジュールされた時間またはイベントの前に録画するように設定した時間。例えば、アラームにより10:00に録画がトリガされた場合、録画前の時間を5秒に設定すると、カメラは9:59:55に録画します。

パラメータ	説明
ポストレコード	イベントまたはスケジュールされた時間の後に録画するように設定した時間。例えば、アラームが作動して録画が11:00に終了した場合、録画後の時間を5秒に設定すると、11:00:05まで録画されます。
ストリーム・タイプ	**メインストリームの**場合、解像度は通常高い。**サブストリームの**場合、同じストレージ容量でより長時間録画できるが、解像度は低くなる。**デュアルストリームの**場合、デバイスはメインストリームとサブストリームの両方を録画します。
ビデオ/画像有効期限	有効期限はファイルをHDDに保存しておく期間です。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。実際のファイルの保存時間は、HDDの容量に応じて決定してください。

6. **オプション：**リストでチャンネルを選択し、**Batch Schedule Configuration** と **Batch Advanced Settings を**使用して、バッチでチャンネルを設定する。
7. **保存を**クリックする。

10.3 画像キャプチャスケジュールの設定

デバイスはスケジュールに従って自動的にライブ写真を撮影する。

ステップ

1. **System→ Storage Management→ Storage Schedule→ Picture Capture** に移動する。

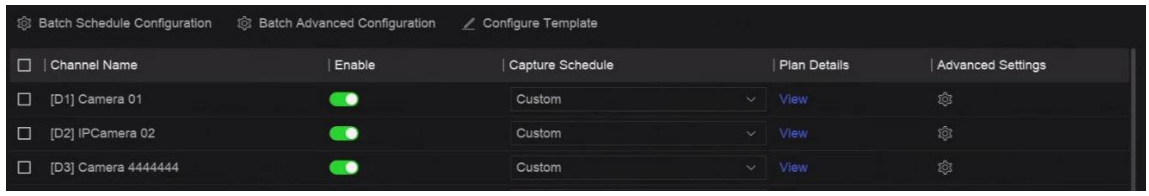


図 10-5 画像キャプチャの構成

2. カメラの**有効**化を**オンに**する。
3. スケジュールタイプを選択します。

注

キャプチャスケジュールをカスタムに設定した場合、タイムバー上でカーソルをドラッグしてカスタマイズした画像キャプチャスケジュールを設定するか、タイムバー上でカーソルを移動し、00:00-24:00 クリックして指定したタイムスケジュールを設定することができます。

4. スケジュールを表示するには、「**表示**」をクリックします。

図 10-6 スケジュールの表示

5. **高度**な画像パラメータを設定するには、**[高度な設定]を**クリックします。

表 10-2 高度なパラメータの説明

パラメータ	説明
キャプチャ遅延	撮影時間。
決議	撮影する画像の解像度を設定します。
画質	画質を低、中、高に設定する。高画質では、より多くのストレージ容量が必要になります。
インターバル	各ライブ画像をキャプチャする時間間隔。

6. **オプション：**リストでチャンネルを選択し、**Batch Schedule Configuration** と **Batch Advanced Settings** を使用して、バッチでチャンネルを設定する。

7. **保存を**クリックする。

10.4 音声録音の設定

このデバイスは、設定された録音スケジュールに従って自動的に音声を録音する。

ステップ

1. **System→ Storage Management→ Storage Schedule→ Audio Recording** へ。
2. チャンネルの**Enableをオンに**する。
3. スケジュールタイプを選択します。

   注

   録画スケジュールをカスタムに設定した場合、タイムバー上でカーソルをドラッグしてカスタマイズした録画スケジュールを設定するか、タイムバー上でカーソルを移動し、00:00-24:00 クリックして指定したタイムスケジュールを設定することができます。
4. スケジュールを表示するには、**「表示」**をクリックします。
5. **オプション：詳細設定]を**クリックして、その他の詳細パラメータを設定します。

表 10-3 高度なパラメータの説明

パラメータ	説明
プレレコード	スケジュールされた時間またはイベントの前に録画するために設定した時間。例えば、アラームが10:00に録画をトリガーする場合、録画前の時間を5秒に設定すると、チャンネルは9:59:55に録画します。
ポストレコード	イベントまたはスケジュールされた時間の後に録画するように設定した時間。例えば、アラームが作動して録画が11:00に終了した場合、録画後の時間を5秒に設定すると、11:00:05まで録画されます。

6. **オプション：**リストでチャンネルを選択し、**Batch Schedule Configuration** と **Batch Advanced Settings を**使用して、バッチでチャンネルを設定する。
7. **保存を**クリックする。

第11章 ライブビュー

11.1 ライブビューのレイアウトを設定する

ライブビューは、各カメラの映像をリアルタイムで表示します。

ステップ

1. **ライブビューへ。**
2. 右 をクリック。
3. ウィンドウの分割タイプを選択するか、**カスタムを**クリックして新しいタイプをカスタマイズします。
4. **ViewのDefault Viewに**カーソルを合わせる。
5. **表示」の**右側にある 」をクリックする。
6. ステップの説明に従って、ライブビュー画像の出力インターフェイスを調整します。ユーザーインターフェースに記載されている2つの方法以外に、1つのウィンドウから別のウィンドウにチャンネルをドラッグすることができます。
7. クリックする。

11.2 GUIの紹介

ライブ画像の表示、ライブ音声の再生、画像のキャプチャ、インスタント再生の実行などができる。

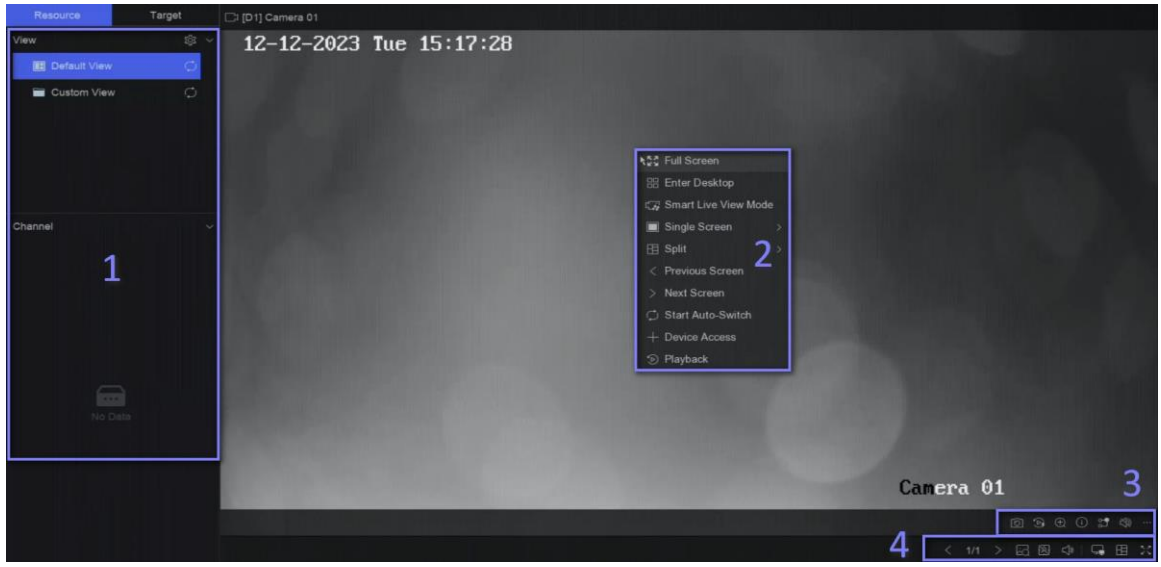


図 11-1 ライブビュー（タイプ 1）

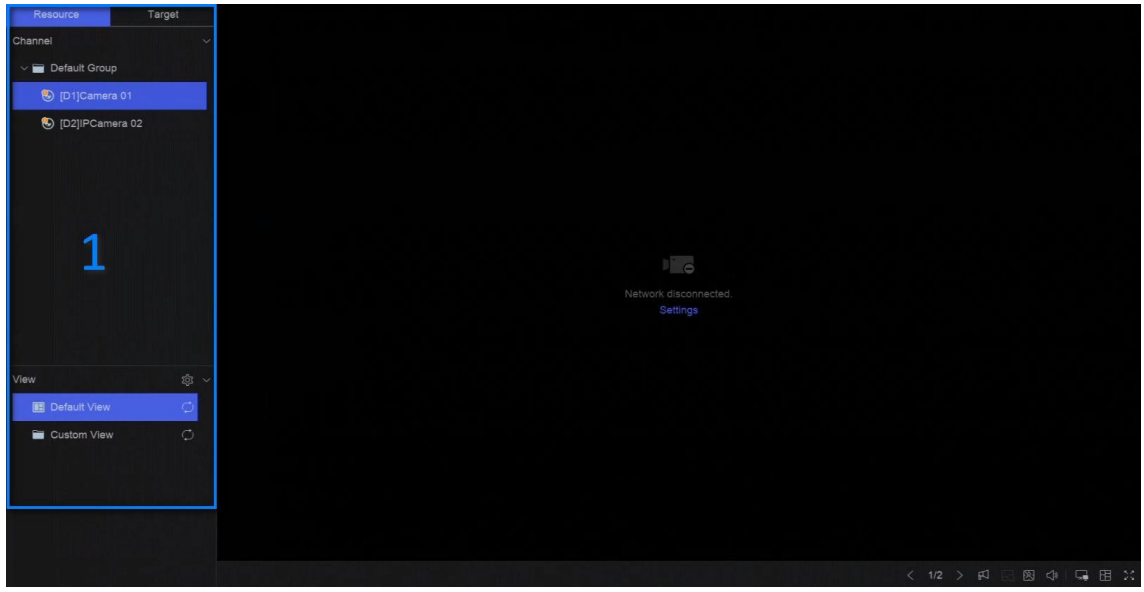


図 11-2 ライブビュー（タイプ 2） 表 11-1 イ

ンタフェース説明

いや。	説明
1	チャンネルリスト、PTZコントロールパネル、ターゲット検出リスト。チャンネルリストからチャンネルを選択すると、対応するウィンドウにリダイレクトされます。**ターゲット】 を**クリックすると、リストでライブターゲット検出結果を表示でき、] をクリックして対応する設定を行います。
2	右クリックのショートカットメニュー。画像エリア上でカーソルを右クリックすると表示されます。
3	チャンネルツールバー • タグを追加するには、クリックしてください。追加後、→**Backup→ By** Tagからタグ別に動画を検索できます。 • →**Show VCA Info** を選択すると、ルールが表示されます。 フレーム。
4	ライブビューのツールバー。**ボイスブロードキャスト、VCA情報表示、出力切替などの**機能をここで実行できる。

注

- マウスを上下にスクロールさせることで、前後の画面を切り替えることができる。
- チャンネル画像表示の例外が発生した場合、対応するウィンドウにエラーメッセージが表示され、テキスト（青色）を直接クリックしてデバイス設定を編集することができます。

11.3 PTZコントロール

PTZとは、Pan（パン）、Tilt（チルト）、Zoom（ズーム）の頭文字をとったものです。PTZカメラをデバイスに追加すると、デバイスは左右にパン、上下にチルト、ズームイン・ズームアウトできるようになる。

PTZカメラを選択し、あるPTZコントロールメニューを消費します。

表 11-2 PTZ 操作

タスク	説明	オペレーション
プリセット	プリセットはPTZ位置とズーム、フォーカス、アイリスなどの状態を記録します。プリセットを呼び出すと、カメラを事前に設定した位置にすばやく移動できます。	プリセットを設定する： 1. プリセットを選択する。 2. 方向ボタンで画像を調整する。 3. クリックする。
		プリセットを呼び出す：クリッ . ク
パトロール	パトロールは、PTZをキーポイントに移動させ、次のキーポイントに移動する前に、設定された時間、そこに留まるように設定することができます。キーポイントはプリセットに対応しています。	パトロールを設定する： 1. パトロールを選択する。 2. クリックする。 3. パトロール用のプリセットを追加する。 4. **OKを**クリックする。
		パトロールを呼ぶクリック .
パターン	PTZの動きを記録して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、PTZを事前に定義された経路に従って移動させることができます。	パターンを決める： 1. クリックする。 2. 方向ボタンを使って画像を調整すると、デバイスがその動きを記録します。 3. 録音を停止する。
		パターンを呼び出す：クリック .

注

PTZパネルが使用できない場合は をクリックして設定を確認してください。

第12章 再生

12.1 GUIの紹介

ビデオオーディオファイルを再生することができます。

図12-1 再生 表12-1 インターフェ

ース説明

そうだ。	説明
1	再生タイプを選択するエリア。
2	チャンネルリスト。
3	カレンダーで時間選択。
4	チャンネルツールバー • チャンネルにタグを追加するには、をクリックします。追加後、→**Backup**→ **By** Tagからタグ別に動画を検索できます。 • クリックしてロックします。ビデオがロックされると は上書きされません。ロックした後、→ **バックアップ** → **タグで**ロック別にビデオを検索できます。

そうだ。	説明
	• →**Dual-VCA を**選択して、対応するイベントルールをトリガーできるビデオを検索します。各イベントタイプの詳細については、イベント設定の手順を参照してください。 **注** この機能を使用するには、**[設定]→[デバイスアクセス]→[デバイス設定]→[デバイスパラメータ]→[Display Info. on Scream]で[**ウェブブラウザ経由で**デュアルVCAを有効にする]**をオンにし、[**システム**]→[ストレージ管理]→[詳細設定]**で[ローカルGUIインターフェース経由で**カメラVCAデータを保存する]を**オンにします。 • →**Show VCA Info** を選択すると、ルールフレームを表示できます。
5	再生タイムライン。 • 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間に合わせる。 • 青いバーで示された期間はビデオを含む。赤いバーは、その期間のビデオがイベントビデオであることを示します。 • タイムラインをズームアウト/ズームインするには、上下にスクロールします。
6	再生ツールバー。 • クリックして、通常ビデオとスマートビデオ（スマートデータを含むビデオ）の再生戦略を設定する。 • （スマートサーチ）をクリックし、ポップアップのイベントルールを描き、対応するイベントルールをトリガーできるビデオを検索する。操作はDual-VCA機能と同様です。 • AcuSearch機能を実行するには、をクリックする。参照詳細は***AcuSearch***。 • / をクリックすると、人間／乗り物を含むビデオが表示されます。 **注** この機能を使用するには、特定のイベントタイプで**検出ターゲットを人間**または**車両に**設定していることを確認してください。

12.2 通常再生

チャンネルの動画を再生する。デバイスによっては、複数のチャンネルで同期再生が可能な場合があります。

ステップ

1. **Playback** →へ。
2. リストからチャンネルを選択します。

   注

   グループ再生：リストからグループを選択し、グループ内のチャンネルを再生することができます。

3. カレンダーで日付を選択します。

   注

   カレンダーの日付の隅にある青い三角形は、利用可能なあることを示します。

4. **オプション：**人間や車両をターゲットにしたビデオを再生する。
   - :人間を含む動画は赤で表示されます。
   - :車両を含む動画は赤で表示されます。

12.3 イベント再生

イベント再生モードを選択すると、システムは動体検知、踏切検知、または侵入検知情報を含むビデオを分析し、マークを付けます。

始める前に

- カメラが**デュアルVCAを**有効にしていることを確認します。カメラのウェブブラウザのインターフェースで**設定** → **ビデオ/オーディオ** → **ストリームの表示情報で**有効にできます。
- ビデオレコーダーが**ストレージ管理でカメラVCAデータの保存を**有効にしていることを確認してください → **詳細設定** .

ステップ

1. **Playback** →を選択する。
2. カレンダーで日付を選択します。

   注

   カレンダーの日付の隅にある青い三角形は、利用可能なあることを示します。

3. をクリックします。 →をクリックしてイベントタイプを選択します。各イベントタイプの詳細については、イベント設定の手順を参照してください。
4. **検索を**クリックする。

   検出ルールの要件を満たす動画は赤で表示されます。

5. クリックして、通常ビデオとスマートビデオ（スマートデータを含むビデオ）の再生戦略を設定する。

注

デュアルVCAが使用されていない場合、プログレスバーの赤いセグメントは、スマートビデオが元のイベントによって生成されていることを意味します。

12.4 スライス再生

ビデオをスライスに分割して再生する。

ステップ

1. **Playback** →へ。
2. カメラカメラを選択します。
3. カレンダーの日付を選択します。
4. **検索を**クリックする。

   検索された映像は1時間ごとに分割されて再生される。
5. **オプション：**1時間のスライスを選択し、をクリックすると、再生用に1分のスライスに分割されます。

12.5 サブピリオド再生

ビデオファイルは、上で同時に複数のサブ期間で再生することができます。

ステップ

1. **Playback** →へ。
2. カメラを選択します。
3. 開始時刻と終了時刻を設定する。
4. **検索を**クリックする。

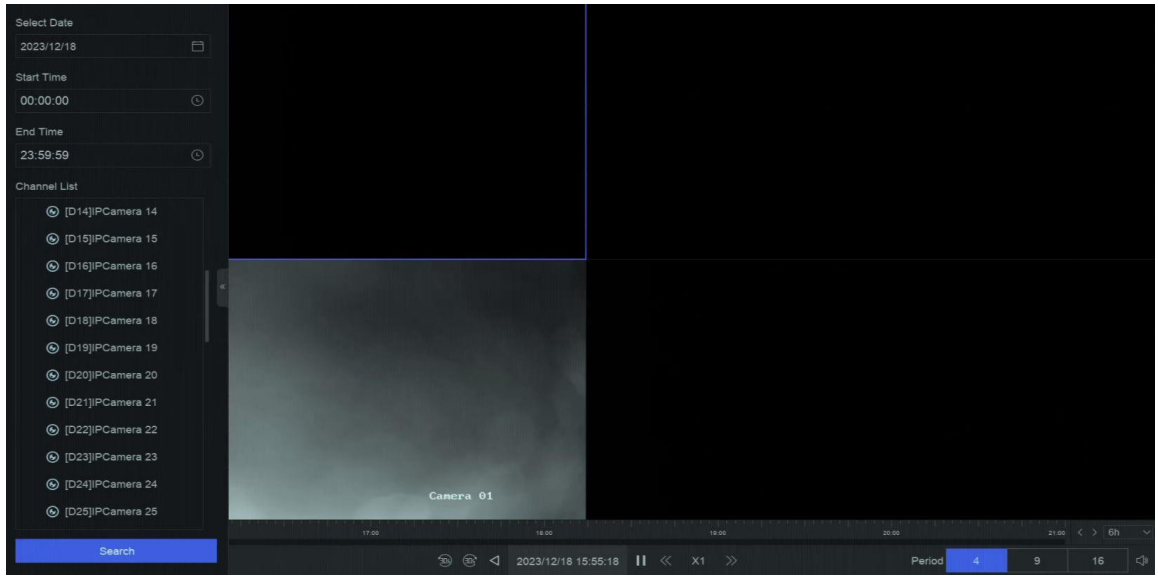


図12-2 サブピリオド再生

5. 右ピリオドを選択する。

注

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分割して再生することができる。例えば、16:00から22:00の間にビデオファイルが存在し、6画面表示モードが選択された場合、各画面で同時に1分のビデオファイルを再生することができます。

チャプター13イベントセンター

13.1 イベント設定

13.1.1 ベーシック／ジェネリック・イベント

ステップ

1. **イベントセンターへ →⚙→イベント設定→ 基本イベント / 汎用イベント** .

2. チャンネルを選択する。

3. イベントの種類を選択してください。

4. **Enableをオンに**する。

5. ルールを設定するには、**[ルール設定]を**クリックします。

表 13-1 通常のイベント

イベント名	イベント内容	ルール構成	
モーション検知	動体検知は、監視エリア内の動く物体を検知します。	画像上部のツールバーを使って検出エリアを描画する。 • **NVRによるAI**：動体検知イベントはNVRによって分析される。このデバイスは人間と車両を含むビデオを分析できます。選択されたタイプ（人間または車両）のターゲットのみがアラームをトリガーするため、他のオブジェクトによって引き起こされる誤報を減らすことができます。 • **カメラによるAI**：動体検知イベントはカメラによって分析されます。 • **検出ターゲット**：人間とが選択可能で、誤報は別として、唯一の	感度を設定することで、動きがアラームをトリガーしやすいかどうかを調整できます。値が高いほど、動体検知をトリガーしやすくなります。

イベント名	イベント内容	ルール構成	
		選択したターゲットにアラームをトリガーすることができます。	
ビデオ改ざん検知	ビデオ改ざん検出は、カメラレンズが覆われたときにアラームをトリガーし、アラーム対応アクションを実行します。	画像上部のツールバーを使って検出エリアを描画する。	
ビデオロス検出	ビデオロス検出は、チャンネルのビデオロスを検出し、アラーム応答アクションを実行します。	-	
オーディオ例外検出	オーディオ例外検出は、音の強度が急激に増加/減少するなど、シーン内の異常な音を検出。	-	
デフォーカス検出	レンズデフォーカスによる画像ブレを検出できる。	-	
突然のシーンチェンジ検出	シーン変化検出は、カメラの意図的な、外的要因に影響されるビデオセキュリティ環境の変化を検出します。	-	

6. **アーミング・スケジュールを**クリックして、アーミング・スケジュール・タイプを選択します。

注

Arming Schedule**をCustomに**設定した場合、タイムバー上でカーソルをドラッグしてカスタマイズしたアーミングスケジュールを設定するか、タイムバー上でカーソルを移動し、00:00-24:00 クリックして指定したタイムスケジュールを設定することができます。

7. リンケージ設定するには、**リンケージ方法を**クリックします。

表 13-2 リンケージ方法の説明

リンケージ方式	説明
監視センターに通知	イベントがすると、デバイスは例外またはアラーム信号をリモートアラームホストに送信できます。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たPCを指します。
アラームポップアップウィンドウ	アラームがトリガーされると、ローカルモニターはアラームポップアップウィンドウを表示します。
ブザー	アラームを検知すると、ブザーがビープ音を発します。
メール送信	システムは、アラームが検出されると、アラーム情報を含む電子メールをユーザーまたはユーザーに送信できます。
アラーム出力	アラーム出力は、アラーム入力、モーション検知、ビデオ改ざん検知、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トリガーすることができます。
記録	アラームが検出されると、選択したチャンネルがビデオを録画する。 注 ビデオ録画スケジュールはチャンネルに対して有効でなければならない。**システム → ストレージ管理→ ストレージスケジュール→ ビデオ録画** でビデオ録画スケジュールを設定できます。

8. 保存をクリックする。

13.1.2 周辺保護

境界保護イベントには、ライン交差検出、侵入検出、領域入口検出、領域出口検出が含まれる。

踏切検出の設定

ラインクロス検出は、設定された仮想横切る人、車両、物体を検出する。検出方向は、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

注

以下の手順の一部は、特定のNVRまたはカメラ・モデルでのみ使用できます。

1. Event Center →⚙→Event Configuration→ Perimeter Protectionにアクセスしてください。

2. カメラを選択します。
3. **オプション：セカンダリ分析を**オンにします。対応するデバイスエンジンは、誤報を減らすためにこのイベントを2回目分析します。

注

少なくとも 1 つのデバイス エンジンで **Secondary Analysis for Perimeter Protection** アルゴリズムを実行する必要があります。右側の［**Allocate Engine（エンジンの割り当て）**］をクリックしてエンジンをすばやく割り当てるか、［**System（システム）**］→［**Smart Settings（スマート設定）**］→［**Algorithm Configuration（アルゴリズム設定）**］→［**Algorithm Management（アルゴリズム管理）**］で**Secondary Analysis for Perimeter Protection（境界保護アルゴリズムの二次解析）を**有効にします。

4. **オプション：NVRのAIを**オンにします。対応するデバイス・エンジンがビデオを分析し、カメラはビデオ・ストリームのみを送信します。

少なくとも1つのデバイスエンジンが**Perimeter Protection**アルゴリズムを実行する必要があります。右側の「**Allocate Engine」を**クリック

注

してエンジンを素早く割り当てるか、「**System → Smart Settings → Algorithm Configuration→ Algorithm Management**」で**Perimeter Protection**アルゴリズムを有効にします。

5. **ライン・クロッシングを**選択する。
6. **Enableをオンに**する。

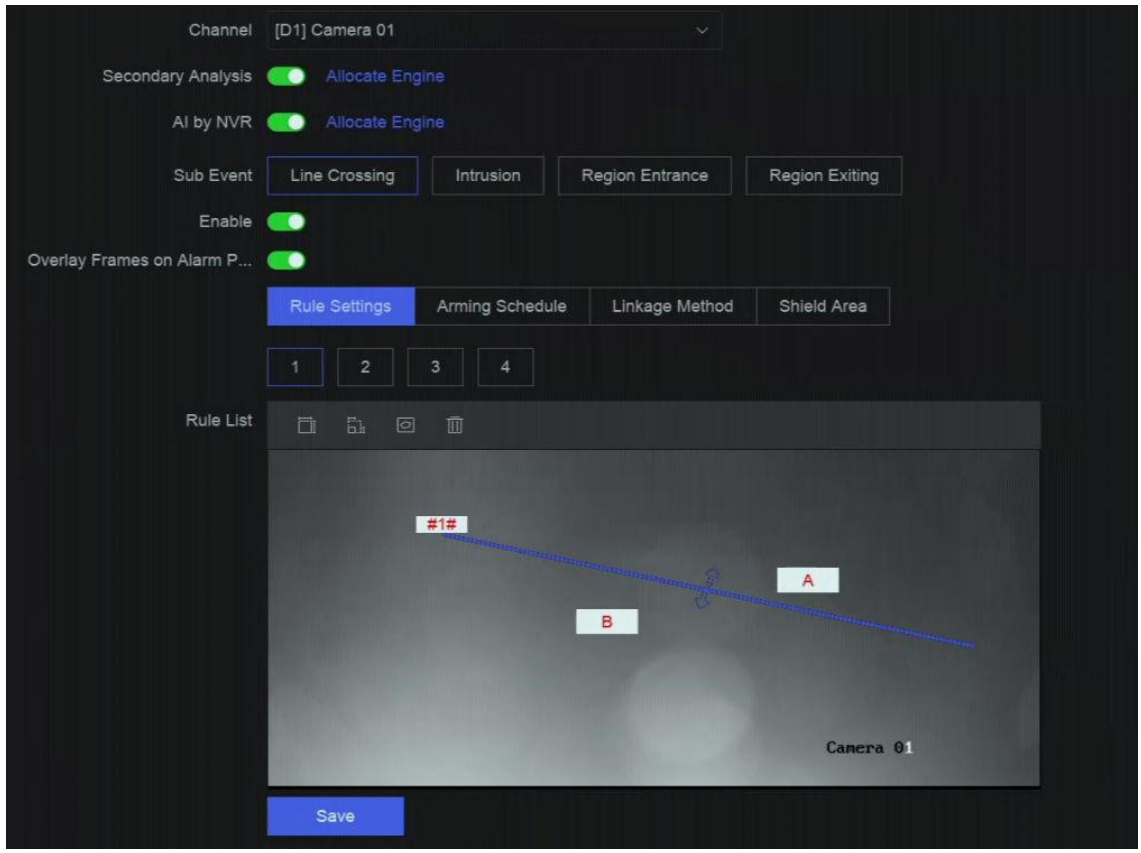


図13-1 ライン・クロッシング検出

7. ルールを検出するには、**[ルール設定]を**クリックします。

1) ルール番号を選択する。例えば、**1を**選択する。

2) をクリックし、画像上をそれぞれ2回クリックして、検出線の始点と描きます。

3) **方向**、**感度**、**検出目標を**設定します。**A<->B**

B側の矢印のみが表示されます。物体が設定されたラインを両方向に横切ると検出され、アラームが作動します。

A->B

A側からB側へ設定されたラインを横切る物体のみを検出することができる。

B->A

B側からA側に設定されたラインを横切る物体のみを検出することができる。

感度

数値が高いほど、検知アラームが作動しやすくなる。

検出ターゲット

検出ターゲットを人間または**車両に**選択すると、人間または車両によってトリガーされなかったアラームが破棄されます。**検出**対象は特定のモデルでのみ使用できます。

4) **オプション：** / をクリックして、**最大サイズまたは最小**サイズを描画します。または**Min.サイズ**。サイズ要件を満たすターゲットのみがアラームをトリガーできます。

5) **オプション：**さらに引くには、上記の手順を繰り返します。最大4つのルールがサポートされています。

8. **アーミング・スケジュールを**クリックして、アーミング・スケジュール・タイプを選択します。

注

Arming Scheduleを**Customに**設定した場合、タイムバー上でカーソルをドラッグしてカスタマイズしたアーミングスケジュールを設定するか、タイムバー上でカーソルを移動し、00:00-24:00 クリックして指定したタイムスケジュールを設定することができます。

9. リンケージ設定するには、**リンケージ方法を**クリックします。

表 13-3 リンケージ方法の説明

リンケージ方式	説明
監視センターに通知	イベントがすると、デバイスは例外またはアラーム信号をリモートアラームホストに送信できます。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たPCを指します。
アラームポップアップウィンドウ	アラームがトリガーされると、ローカルモニターはアラームポップアップウィンドウを表示します。
ブザー	アラームを検知すると、ブザーがビープ音を発します。
メール送信	システムは、アラームが検出されると、アラーム情報を含む電子メールをユーザーまたはユーザーに送信できます。

リンケージ方式	説明
アラーム出力	アラーム出力は、アラーム入力、モーション検知、ビデオ改ざん検知、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トリガーすることができます。
記録	アラームが検出されると、選択したチャンネルがビデオを録画する。 注 ビデオ録画スケジュールはチャンネルに対して有効でなければならない。**システム → ストレージ管理→ ストレージスケジュール→ ビデオ録画** でビデオ録画スケジュールを設定できます。

10. **オプション：NVR による AI** が有効な場合、**シールド・エリアを**設定します。シールド・エリアが設定されると、デバイスはエリア内のターゲットの行動を分析しないため、エリア内で境界保護イベントがトリガーされることはありません。
11. **保存を**クリックする。

次に何をすべきか

ライブビューに移動し、**ターゲットを**クリックしてリアルタイムのアラームを表示できます。

侵入検知の設定

侵入検知機能は、あらかじめ定義された仮想領域内に侵入したり、うろついたりする人や車両などを検知します。アラームがトリガーされると、特定のアクションを実行できます。

ステップ

注

以下の手順の一部は、特定のNVRまたはカメラ・モデルでのみ使用できます。

1. **Event Center →⚙→Event Configuration→ Perimeter Protectionに**アクセスしてください。
2. カメラを選択します。
3. **オプション：セカンダリ分析を**オンにします。対応するデバイスエンジンは、誤報を減らすためにこのイベントを2回目分析します。

   注

   少なくとも 1 つのデバイス エンジンで **Secondary Analysis for Perimeter Protection** アルゴリズムを実行する必要があります。右側の［**Allocate Engine（エンジンの割り当て）**］をクリックしてエンジンをすばやく割り当てるか、［**System（システム）**］→［**Smart Settings（スマート設定）**］→［**Algorithm Configuration（アルゴリズム設定）**］→［**Algorithm Management（アルゴリズム管理）**］で**Secondary Analysis for Perimeter Protection（境界保護アルゴリズムの二次解析）を**有効にします。
4. **オプション：NVRのAIを**オンにします。対応するデバイス・エンジンがビデオを分析し、カメラはビデオ・ストリームのみを送信します。

注

少なくとも1つのデバイスエンジンが**Perimeter Protection**アルゴリズムを実行する必要があります。右側の「**Allocate Engine**」をクリックしてエンジンを素早く割り当てるか、「**System → Smart Settings → Algorithm Configuration→ Algorithm Management**」で**Perimeter Protection**アルゴリズムを有効にします。

5. **侵入を**選択する。
6. **Enableをオンに**する。

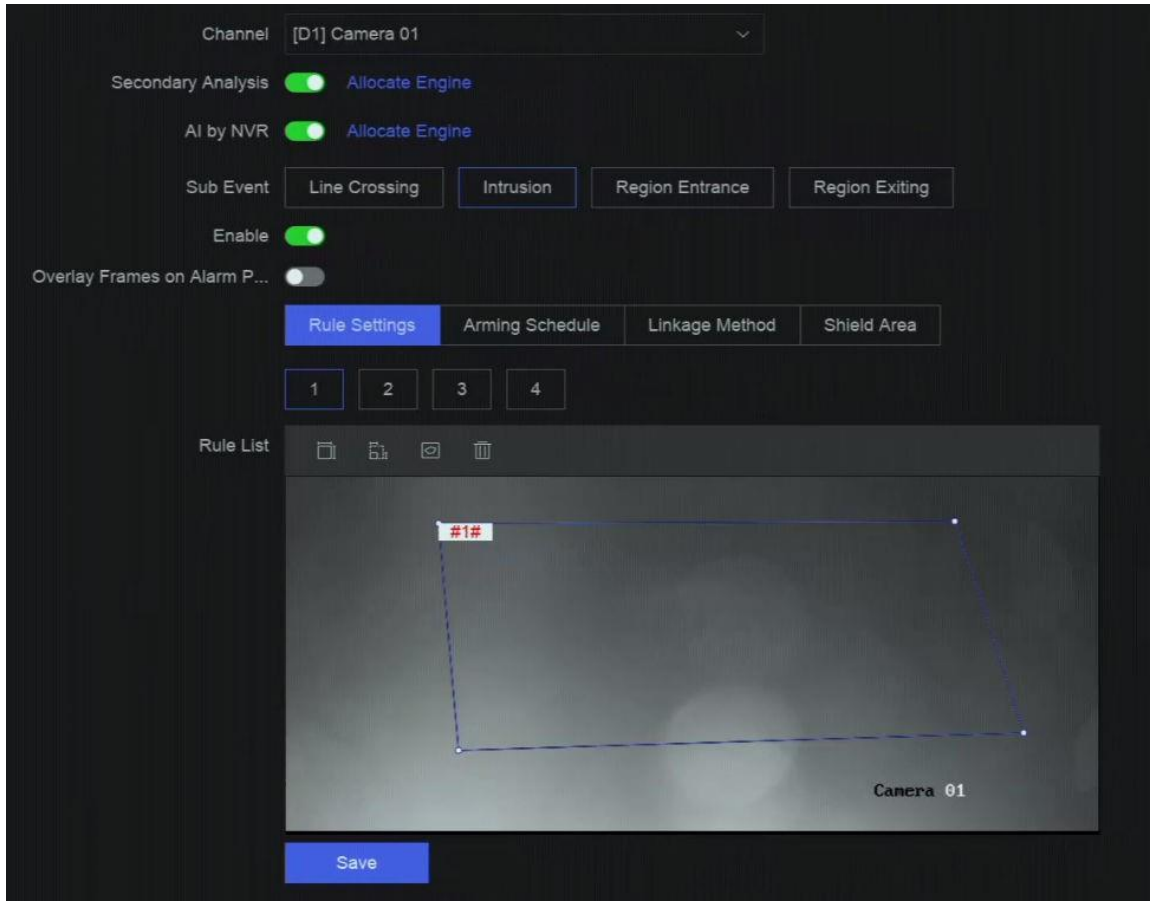


図 13-2 侵入検知

7. ルールを検出するには、**[ルール設定]を**クリックします。
   1) ルール番号を選択する。例えば、**1を**選択する。
   2) クリックし、画像をそれぞれ4回クリックして四角形領域の各点を描く。
   3) **時間しきい値**、**感度**、**検出目標を**設定します。**時間しきい値**

      オブジェクトが領域内をうろうろしている時間。定義された検出領域内の物体の持続時間が閾値を超えると、デバイスはアラームをトリガーします。

      感度

数値が高いほど、検知アラームが作動しやすくなる。

検出ターゲット

検出ターゲットを人間または**車両に**選択すると、人間または車両によってトリガーされなかったアラームが破棄されます。**検出**対象は特定のモデルでのみ使用できます。

4) **オプション：** / をクリックして、**最大サイズまたは最小**サイズを描画します。または**Min.サイズ**。サイズ要件を満たすターゲットのみがアラームをトリガーできます。

5) **オプション：**さらに引くには、上記の手順を繰り返します。最大4つのルールがサポートされています。

8. アーミング・スケジュールをクリックして、アーミング・スケジュール・タイプを選択します。

注

Arming Scheduleを**Customに**設定した場合、タイムバー上でカーソルをドラッグしてカスタマイズしたアーミングスケジュールを設定するか、タイムバー上でカーソルを移動し、00:00-24:00 クリックして指定したタイムスケジュールを設定することができます。

9. リンケージ設定するには、**リンケージ方法を**クリックします。

表 13-4 リンケージ方法の説明

リンケージ方式	説明
監視センターに通知	イベントがすると、デバイスは例外またはアラーム信号をリモートアラームホストに送信できます。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たPCを指します。
アラームポップアップウィンドウ	アラームがトリガーされると、ローカルモニターはアラームポップアップウィンドウを表示します。
ブザー	アラームを検知すると、ブザーがビープ音を発します。
メール送信	システムは、アラームが検出されると、アラーム情報を含む電子メールをユーザーまたはユーザーに送信できます。
アラーム出力	アラーム出力は、アラーム入力、モーション検知、ビデオ改ざん検知、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トリガーすることができます。
記録	アラームが検出されると、選択したチャンネルがビデオを録画する。 注 ビデオ録画スケジュールはチャンネルに対して有効でなければならない。**システム → ストレージ管理→ ストレージスケジュール→ ビデオ録画** でビデオ録画スケジュールを設定できます。

10. オプション：NVR による AI が有効な場合、**シールド・エリアを**設定します。シールド・エリアが設定されると、デバイスはエリア内のターゲットの行動を分析しないため、エリア内で境界保護イベントがトリガーされることはありません。

11. 保存をクリックする。

次に何をすべきか

ライブビューに移動し、**ターゲットを**クリックしてリアルタイムのアラームを表示できます。

リージョン入口検出の設定

領域入口検出は、事前に定義された仮想領域に入るオブジェクトを検出します。

ステップ

注

以下の手順の一部は、特定のNVRまたはカメラ・モデルでのみ使用できます。

1. **Event Center →⚙→Event Configuration→ Perimeter Protectionに**アクセスしてください。
2. カメラを選択します。
3. **オプション：セカンダリ分析を**オンにします。対応するデバイスエンジンは、誤報を減らすためにこのイベントを2回目分析します。

   注

   少なくとも 1 つのデバイス エンジンで **Secondary Analysis for Perimeter Protection** アルゴリズムを実行する必要があります。右側の **［Allocate Engine（エンジンの割り当て）］** をクリックしてエンジンをすばやく割り当てるか、**［System（システム）］→［Smart Settings（スマート設定）］→［Algorithm Configuration（アルゴリズム設定）］→［Algorithm Management（アルゴリズム管理）］でSecondary Analysis for Perimeter Protection（境界保護アルゴリズムの二次解析）を**有効にします。
4. **オプション：NVRのAIを**オンにします。対応するデバイス・エンジンがビデオを分析し、カメラはビデオ・ストリームのみを送信します。

   少なくとも1つのデバイスエンジンが**Perimeter Protection**アルゴリズムを実行する必要があります。右側の「**Allocate Engine」を**クリック

   注

   してエンジンを素早く割り当てるか、「**System → Smart Settings → Algorithm Configuration→ Algorithm Management**」で**Perimeter Protection**アルゴリズムを有効にします。
5. **地域入口を**選択する。
6. **Enableをオンに**する。

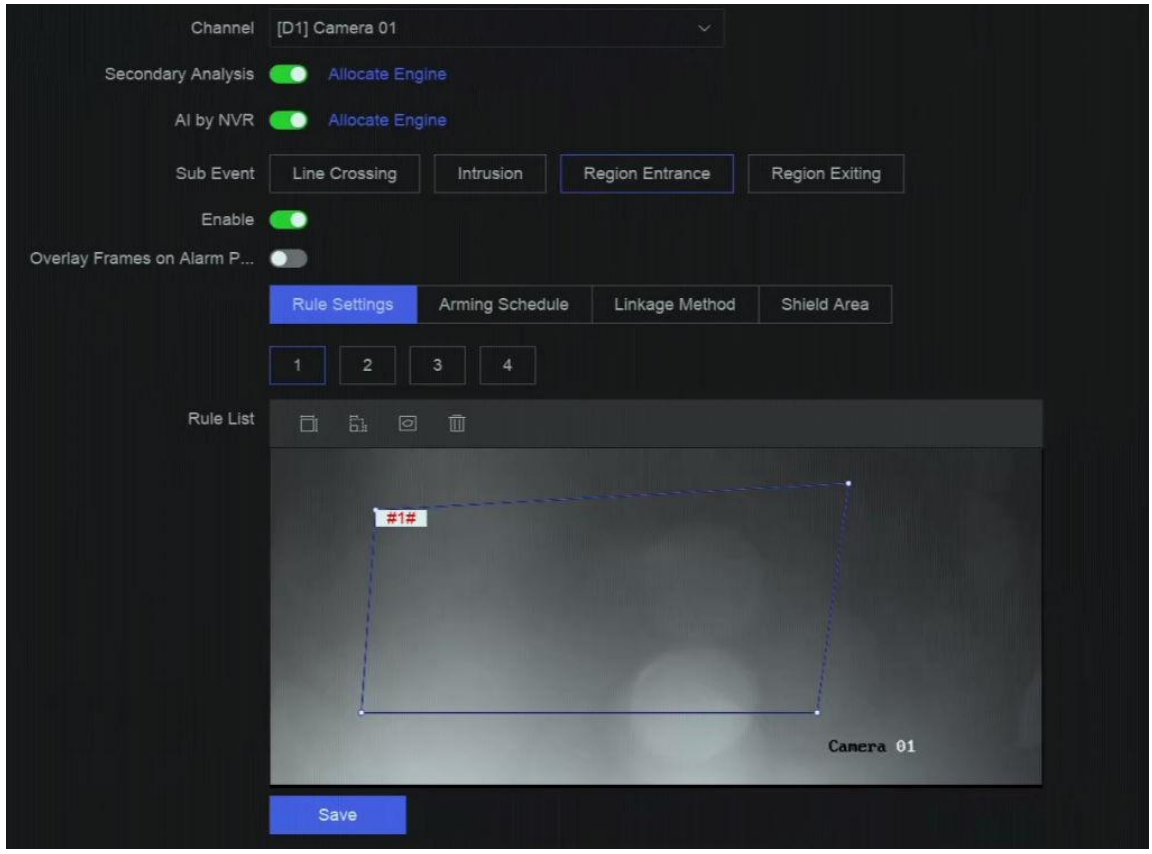


図13-3 領域入口検出

7. ルールを検出するには、**[ルール設定]を**クリックします。

1) ルール番号を選択する。例えば、**1を**選択する。

2) クリックし、画像をそれぞれ4回クリックして四角形領域の各点を描く。

3) 感度と**検出目標を**設定します。**感度**

数値が高いほど、検知アラームが作動しやすくなる。

検出ターゲット

検出ターゲットを人間または**車両に**選択すると、人間または車両によってトリガーされなかったアラームが破棄されます。**検出**対象は特定のモデルでのみ使用できます。

4) **オプション：**さらに引くには、上記の手順を繰り返します。最大4つのルールがサポートされています。

8. アーミング・スケジュールをクリックして、アーミング・スケジュール・タイプを選択します。

注

Arming Schedule**をCustomに**設定した場合、タイムバー上でカーソルをドラッグしてカスタマイズしたアーミングスケジュールを設定するか、タイムバー上でカーソルを移動し、00:00-24:00 クリックして指定したタイムスケジュールを設定することができます。

9. リンケージ設定するには、**リンケージ方法を**クリックします。

表 13-5 リンケージ方法の説明

リンケージ方式	説明
監視センターに通知	イベントがすると、デバイスは例外またはアラーム信号をリモートアラームホストに送信できます。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たPCを指します。
アラームポップアップウィンドウ	アラームがトリガーされると、ローカルモニターはアラームポップアップウィンドウを表示します。
ブザー	アラームを検知すると、ブザーがビープ音を発します。
メール送信	システムは、アラームが検出されると、アラーム情報を含む電子メールをユーザーまたはユーザーに送信できます。
アラーム出力	アラーム出力は、アラーム入力、モーション検知、ビデオ改ざん検知、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トリガーすることができます。
記録	アラームが検出されると、選択したチャンネルがビデオを録画する。 注 ビデオ録画スケジュールはチャンネルに対して有効でなければならない。**システム → ストレージ管理→ ストレージスケジュール→ ビデオ録画** でビデオ録画スケジュールを設定できます。

10. **オプション：NVR による AI** が有効な場合、**シールド・エリアを**設定します。シールド・エリアが設定されると、デバイスはエリア内のターゲットの行動を分析しないため、エリア内で境界保護イベントがトリガーされることはありません。
11. **保存を**クリックする。

次に何をすべきか

ライブビューに移動し、**ターゲットを**クリックしてリアルタイムのアラームを表示できます。

リージョン退出検出の設定

領域抜け検出は、あらかじめ定義された仮想領域から抜けるオブジェクトを検出する。

ステップ

注

以下の手順の一部は、特定のNVRまたはカメラ・モデルでのみ使用できます。

1. **Event Center →⚙→Event Configuration→ Perimeter Protectionに**アクセスしてください。
2. カメラを選択します。

3. **オプション：セカンダリ分析を**オンにします。対応するデバイスエンジンは、誤報を減らすためにこのイベントを2回目分析します。

注

少なくとも 1 つのデバイス エンジンで **Secondary Analysis for Perimeter Protection** アルゴリズムを実行する必要があります。右側の［**Allocate Engine（エンジンの割り当て）**］をクリックしてエンジンをすばやく割り当てるか、［**System（システム）**］→［**Smart Settings（スマート設定）**］→［**Algorithm Configuration（アルゴリズム設定）**］→［**Algorithm Management（アルゴリズム管理）**］で**Secondary Analysis for Perimeter Protection（境界保護アルゴリズムの二次解析）を**有効にします。

4. **オプション：NVRのAIを**オンにします。対応するデバイス・エンジンがビデオを分析し、カメラはビデオ・ストリームのみを送信します。

少なくとも1つのデバイスエンジンが**Perimeter Protection**アルゴリズムを実行する必要があります。右側の「**Allocate Engine」を**クリック

注

してエンジンを素早く割り当てるか、「**System → Smart Settings → Algorithm Configuration→ Algorithm Management**」で**Perimeter Protection**アルゴリズムを有効にします。

5. **地域を**選択**する**。
6. **Enableをオンに**する。

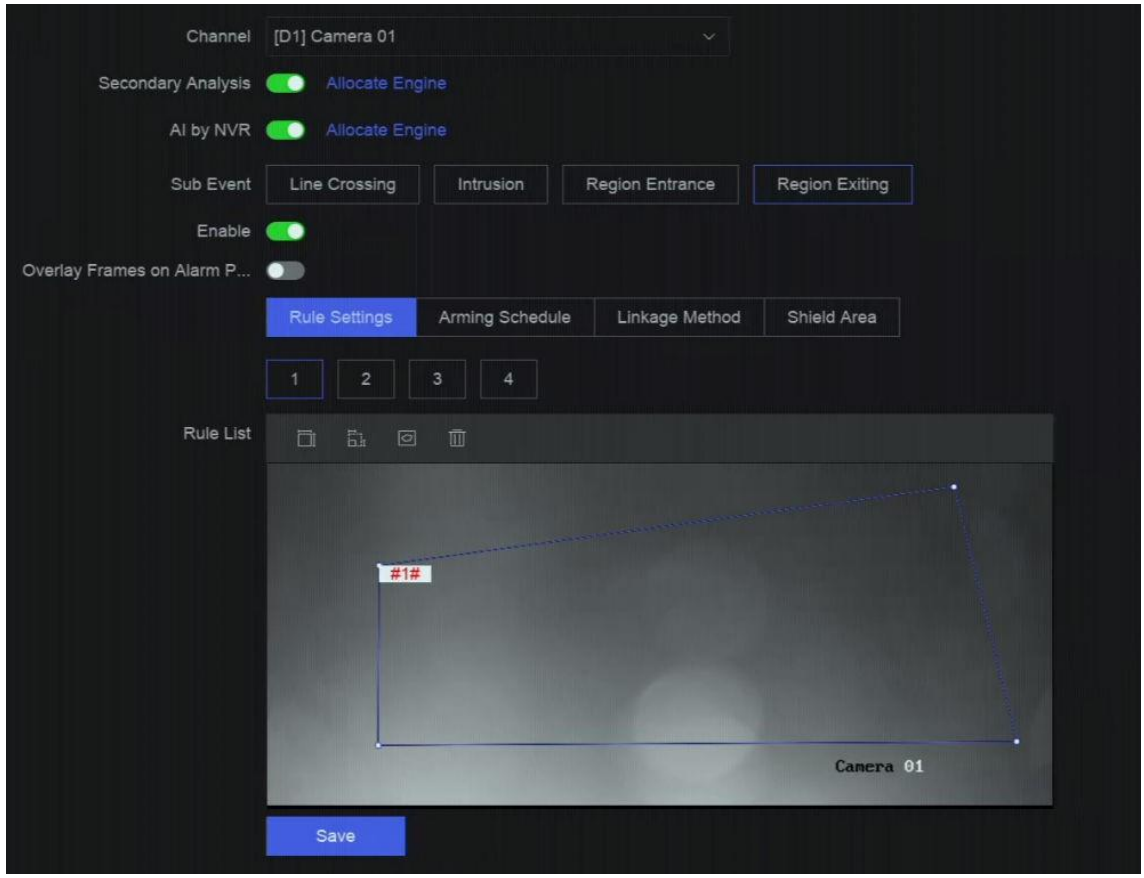


図 13-4 リージョン退出検出

7. ルールを検出するには、**[ルール設定]を**クリックします。

1) ルール番号を選択する。例えば、**1を**選択する。

2) クリックし、画像をそれぞれ4回クリックして四角形領域の各点を描く。

3) 感度と**検出目標を**設定します。**感度**

数値が高いほど、検知アラームが作動しやすくなる。

検出ターゲット

人間または車両によってトリガーされなかったアラームを破棄するには、**検出ターゲットを人間**または**車両として**選択します。**検出**対象は特定のモデルでのみ使用できます。

4) **オプション：**さらに引くには、上記の手順を繰り返します。最大4つのルールがサポートされています。

8. **アーミング・スケジュールを**クリックして、アーミング・スケジュール・タイプを選択します。

注

Arming Scheduleを**Customに**設定した場合、タイムバー上でカーソルをドラッグしてカスタマイズしたアーミングスケジュールを設定するか、タイムバー上でカーソルを移動し、00:00-24:00 クリックして指定したタイムスケジュールを設定することができます。

9. リンケージ設定するには、**リンケージ方法を**クリックします。

表 13-6 リンケージ・メソッドの説明

リンケージ方式	説明
監視センターに通知	イベントがすると、デバイスは例外またはアラーム信号をリモートアラームホストに送信できます。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たPCを指します。
アラームポップアップウィンドウ	アラームがトリガーされると、ローカルモニターはアラームポップアップウィンドウを表示します。
ブザー	アラームを検知すると、ブザーがビープ音を発します。
メール送信	システムは、アラームが検出されると、アラーム情報を含む電子メールをユーザーまたはユーザーに送信できます。
アラーム出力	アラーム出力は、アラーム入力、モーション検知、ビデオ改ざん検知、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トリガーすることができます。
記録	アラームが検出されると、選択したチャンネルがビデオを録画する。 注 ビデオ録画スケジュールがそのチャンネルで有効になっている必要があります。→

リンケージ方式	説明
	ストレージ管理→ ストレージスケジュール→ ビデオ録画 ビデオ録画スケジュールを設定する。

10. **オプション：NVR による AI** が有効な場合、**シールド・エリアを**設定します。シールド・エリアが設定されると、デバイスはエリア内のターゲットの行動を分析しないため、エリア内で境界保護イベントがトリガーされることはありません。

11. **保存を**クリックする。

次に何をすべきか

ライブビューに移動し、**ターゲットを**クリックしてリアルタイムのアラームを表示できます。

13.1.3 異常行動イベント

始める前に

カメラがこのサポートしていることを確認してください。

ステップ

1. **イベントセンターへ →⚙→イベント構成→ 異常動作イベント** .

2. カメラの選択

3. イベントの種類を選択してください。

4. **Enableをオンに**する。

5. ルールを設定するには、**[ルール設定]を**クリックします。

表 13-7 異常動作イベント

イベント名	イベント内容	ルール構成
徘徊検知	ロイタリング検出は、ターゲットが設定された時間より長く指定された領域内に滞在しているかどうかを検出し、リンクされたアクションのためのアラームをトリガする使用されます。	a. ルール番号を選択する。 b. 画像上部のツールバーを使って検出線を引く。 c. **時間しきい**値と**感度を**設定します。**時間しきい値** ターゲットが領域内に滞在する時間。値が 10 の場合、ターゲットが領域内に 10 秒間滞在した後にアラームがトリガーされる：[1-10]. **感度** 背景画像と対象物の類似度。値が大きいほど
駐車検知	駐車違反の、高速道路や一方通行の道路に適用されます。	
無人手荷物検知	手荷物、財布、危険物など、事前に定義された領域に残された物体を検出し、一連のアクションを実行します。	

イベント名	イベント内容	ルール構成
	アラームがトリガーされたときに取ることができる。	検出アラームが作動します。 d.オプション：上記の手順を繰り返して、別のものを設定する。
オブジェクト除去検出	対象物除去検知機能は、展示物などあらかじめ設定された領域から対象物が除去されたことを検知し、アラームが作動した場合に一連の動作を行うことができる。	
高速移動検出	高速移動検出は、不審な走行や追跡、速度超過高速移動を検出するために使用されます。それは必要な処置を前もって取るできるように目的が速く動くとき警報を誘発し、武装のホストに通知を送ります。	
人集め検知	人集り、特定エリア内の人体密度が設定値を超えたかどうかを検知し、アラームを発して連動動作を行うもの。	a. ルール番号を選択する。 b. 画像上部のツールバーを使って検出線を引く。 c. **パーセンテージを**設定する。パーセンテージはエリア内の人体密度です。閾値を超えた場合、アラームが作動します。 d. オプション：上記の手順を繰り返して、別のものを設定する。

6. **アーミング・スケジュールを**クリックして、アーミング・スケジュール・タイプを選択します。

注

Arming Scheduleを**Customに**設定した場合、タイムバー上でカーソルをドラッグしてカスタマイズしたアーミングスケジュールを設定するか、タイムバー上でカーソルを移動し、00:00-24:00 クリックして指定したタイムスケジュールを設定することができます。

7. リンケージ設定するには、**リンケージ方法を**クリックします。

表 13-8 連結方法の説明

リンケージ方式	説明
監視センターに通知	イベントがすると、デバイスは例外またはアラーム信号をリモートアラームホストに送信できます。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たPCを指します。
アラームポップアップウィンドウ	アラームがトリガーされると、ローカルモニターはアラームポップアップウィンドウを表示します。
ブザー	アラームを検知すると、ブザーがビープ音を発します。
メール送信	システムは、アラームが検出されると、アラーム情報を含む電子メールをユーザーまたはユーザーに送信できます。
アラーム出力	アラーム出力は、アラーム入力、モーション検知、ビデオ改ざん検知、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トリガーすることができます。
記録	アラームが検出されると、選択したチャンネルがビデオを録画する。 注 ビデオ録画スケジュールはチャンネルに対して有効でなければならない。**システム** → **ストレージ管理**→ **ストレージスケジュール**→ **ビデオ録画** でビデオ録画スケジュールを設定できます。

8. **保存を**クリックする。

13.1.4 対象イベント

始める前に

接続されたカメラがこの機能をサポートしているか、デバイスエンジンが**イベントセンター**→ **イベント設定**→ **スマート設定** → **アルゴリズム設定** → **アルゴリズム管理** で**ターゲット認識**または**ビデオ構造化**アルゴリズムを有効にしていることを確認してください。

ステップ

1. **イベントセンターへ** →⚙→**イベント設定**→ **対象イベント** .

2. カメラを選択します。

3. イベントを選択してください。

4. **Enableをオンに**する。

5. イベントルールを設定する。

イベント名	イベント内容	ルール構成
フェイス・キャプチャー	顔キャプチャは、シーンに現れる顔を検出してキャプチャする。人の顔が検出されると、連動アクションをトリガーすることができる。	-
顔写真の比較	検出された顔画像を指定されたリストライブラリと比較します。比較に成功するとアラームを発生します。	• ターゲットの等級設定をサポート。ターゲットのグレードが比較要件（瞳孔距離が設定されたしきい値より大きく、チルト角とパン角が設定されたしきい値より小さい）を満たすと、顔画像の比較が開始されます。 • 比較に失敗した場合と成功した場合のプロンプトの設定をサポート。
ストレンジャー・ディテクション	ビデオに登場するリストライブラリにない顔は、見知らぬ人と識別される。	• ターゲットの等級設定をサポート。ターゲットのグレードが比較要件（瞳孔距離が設定されたしきい値より大きく、チルト角とパン角が設定されたしきい値より小さい）を満たすと、顔画像の比較が開始されます。 • 見知らぬ人を検出するプロンプトの設定をサポート。
マルチ・ターゲット・タイプ検出	マルチターゲットタイプ検出により、シーン内の顔、人体、車両を同時に検出することができる。	-

6. **アーミング・スケジュールを**クリックして、アーミング・スケジュール・タイプを選択します。

注

Arming Scheduleを**Customに**設定した場合、タイムバー上でカーソルをドラッグしてカスタマイズしたアーミングスケジュールを設定するか、タイムバー上でカーソルを移動し、00:00-24:00 クリックして指定したタイムスケジュールを設定することができます。

7. リンケージ設定するには、**リンケージ方法を**クリックします。

表 13-9 連結方法の説明

リンケージ方式	説明
監視センターに通知	イベントがすると、デバイスは例外またはアラーム信号をリモートアラームホストに送信できます。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たPCを指します。
アラームポップアップウィンドウ	アラームがトリガーされると、ローカルモニターはアラームポップアップウィンドウを表示します。
ブザー	アラームを検知すると、ブザーがビープ音を発します。
メール送信	システムは、アラームが検出されると、アラーム情報を含む電子メールをユーザーまたはユーザーに送信できます。
アラーム出力	アラーム出力は、アラーム入力、モーション検知、ビデオ改ざん検知、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トリガーすることができます。
記録	アラームが検出されると、選択したチャンネルがビデオを録画する。 注 ビデオ録画スケジュールはチャンネルに対して有効でなければならない。**システム → ストレージ管理→ ストレージスケジュール→ ビデオ録画** でビデオ録画スケジュールを設定できます。

8. 保存をクリックする。

13.1.5 サーマルカメラ検出

NVRは、サーマルネットワークカメラのイベント検出モード（火災および煙検出、温度検出、温度差検出など）をサポートしています。

始める前に

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

ステップ

1. イベントセンターへ →⚙→イベント構成→ サーマルイベント .

2. カメラを選択します。

3. イベントの種類を選択してください。

4. Enableをオンにする。

5. ルールを設定するには、**[ルール設定]を**クリックします。

表 13-10 サーマル・イベント

イベント名	イベント内容
火災検知	武装エリア内で火災が検知されると、アラームが作動する。
温度検出	温度がしきい値を超えるとアラームが作動する。
周辺保護	境界保護イベントには、ライン交差検出、侵入検出、領域入口検出、領域出口検出が含まれる。

6. **アーミング・スケジュールを**クリックして、アーミング・スケジュール・タイプを選択します。

注

Arming Scheduleを**Customに**設定した場合、タイムバー上でカーソルをドラッグしてカスタマイズしたアーミングスケジュールを設定するか、タイムバー上でカーソルを移動し、00:00-24:00 クリックして指定したタイムスケジュールを設定することができます。

7. リンケージ設定するには、**リンケージ方法を**クリックします。

表 13-11 リンク方法の説明

リンケージ方式	説明
監視センターに通知	イベントがすると、デバイスは例外またはアラーム信号をリモートアラームホストに送信できます。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たPCを指します。
アラームポップアップウィンドウ	アラームがトリガーされると、ローカルモニターはアラームポップアップウィンドウを表示します。
ブザー	アラームを検知すると、ブザーがビープ音を発します。
メール送信	システムは、アラームが検出されると、アラーム情報を含む電子メールをユーザーまたはユーザーに送信できます。
アラーム出力	アラーム出力は、アラーム入力、モーション検知、ビデオ改ざん検知、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トリガーすることができます。
記録	アラームが検出されると、選択したチャンネルがビデオを録画する。 注 ビデオ録画スケジュールがそのチャンネルで有効になっている必要があります。→

リンケージ方式	説明
	ストレージ管理→ ストレージスケジュール→ ビデオ録画 ビデオ録画スケジュールを設定する。

8. 保存をクリックする。

13.1.6 アラーム入力イベント

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. イベントセンターへ →→イベント設定→ アラーム入力イベント .

2. アラーム入力名を選択します。

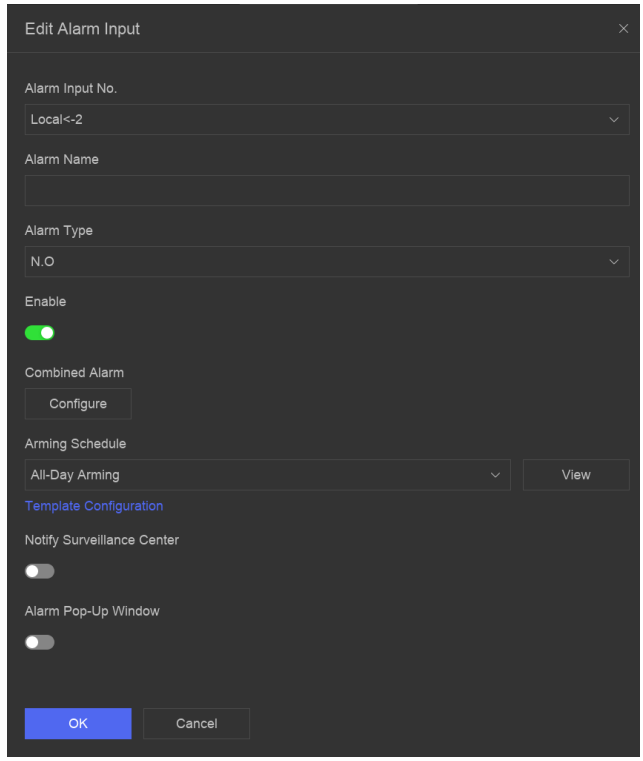


図 13-5 アラーム入力の構成

注

例えば、**Local<-1は**、装置背面パネルのアラーム入力番号が1であることを表す。

3. アラーム名を編集する。

4. アラームの種類を設

定します。**N.O**

接点が自然電源がオフのとき、2つの接点がオフであればノーマルオープンと呼ぶことができる。

N.C

接点が自然電源が切れているとき、2つの接点が導通していればノーマルクローズと呼ぶことができる。

5. **Enableをオンに**する。

6. **オプション：**ステップ**Local<-**1を選択した場合は、処理方法を選択する。

- **プロセスアラーム**入力を選択し、対応するアーミングスケジュール、リンク方法などを設定します。

注

以下の操作はすべて、この処理選択した場合に利用できます。

- **クイック解除を**選択すると、すべてのイベントのリンク方法が無効になる。

7. **Configure] を**クリックして、複合アラームを設定します。

1) チャンネルを選択する。

2) 動体検知やビデオ改ざん検知などの複合アラームイベントを選択します。

3) **OKを**クリックする。

複合アラームは、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トリガーされます。

8. **アーミング・スケジュールを**クリックして、アーミング・スケジュール・タイプを選択します。

注

Arming Scheduleを**Customに**設定した場合、タイムバー上でカーソルをドラッグしてカスタマイズしたアーミングスケジュールを設定するか、タイムバー上でカーソルを移動し、00:00-24:00 クリックして指定したタイムスケジュールを設定することができます。

9. リンケージ設定するには、**リンケージ方法を**クリックします。

表 13-12 連結方法の説明

リンケージ方式	説明
監視センターに通知	イベントがすると、デバイスは例外またはアラーム信号をリモートアラームホストに送信できます。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たPCを指します。
アラームポップアップウィンドウ	アラームがトリガーされると、ローカルモニターはアラームポップアップウィンドウを表示します。
ブザー	アラームを検知すると、ブザーがビープ音を発します。
メール送信	システムは、アラームが検出されると、アラーム情報を含む電子メールをユーザーまたはユーザーに送信できます。

リンケージ方式	説明
アラーム出力	アラーム出力は、アラーム入力、モーション検知、ビデオ改ざん検知、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トリガーすることができます。
記録	アラームが検出されると、選択したチャンネルがビデオを録画する。 注 ビデオ録画スケジュールはチャンネルに対して有効でなければならない。**システム → ストレージ管理→ ストレージスケジュール→ ビデオ録画** でビデオ録画スケジュールを設定できます。

10. **保存を**クリックする。

13.1.7 オーディオ分析イベント

ステップ

1. **イベントセンターへ →⚙→イベント構成→ 音声分析** .

2. チャンネルを選択する。

3. イベントの種類を選択してください。

4. **Enableをオンに**する。

5. ルールを設定するには、**[ルール設定]を**クリックします。

表 13-13 オーディオ分析イベント

イベント名	イベント内容	ルール構成
オーディオ例外検出	オーディオ例外検出は、音の強度が急激に増加/減少するなどシーン内の異常な音を検出します。	**急激な音の**増加を**検出**します。**音量の急減検出** シーン内の急な音の落ち込みを検出する。 **感度** 数値が高いほど、検知アラームが作動しやすくなる。 **音の強さのしきい値** 環境音をフィルターすることができる。環境の音が大きければ大きいほど、この値は高くなるはずです。環境に合わせて調整してください。

6. **アーミング・スケジュールを**クリックして、アーミング・スケジュール・タイプを選択します。

注

Arming Scheduleを**Customに**設定した場合、タイムバー上でカーソルをドラッグしてカスタマイズしたアーミングスケジュールを設定するか、タイムバー上でカーソルを移動し、00:00-24:00 クリックして指定したタイムスケジュールを設定することができます。

7. リンケージ設定するには、**リンケージ方法を**クリックします。

表13-14 リンケージ方法の説明

リンケージ方式	説明
監視センターに通知	イベントがすると、デバイスは例外またはアラーム信号をリモートアラームホストに送信できます。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たPCを指します。
アラームポップアップウィンドウ	アラームがトリガーされると、ローカルモニターはアラームポップアップウィンドウを表示します。
ブザー	アラームを検知すると、ブザーがビープ音を発します。
メール送信	システムは、アラームが検出されると、アラーム情報を含む電子メールをユーザーまたはユーザーに送信できます。
アラーム出力	アラーム出力は、アラーム入力、モーション検知、ビデオ改ざん検知、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トリガーすることができます。
記録	アラームが検出されると、選択したチャンネルがビデオを録画する。 注 ビデオ録画スケジュールはチャンネルに対して有効でなければならない。**システム → ストレージ管理→ ストレージスケジュール→ ビデオ録画** でビデオ録画スケジュールを設定できます。

8. 保存をクリックする。

13.2 リンケージ構成

イベントリンクのパラメータを設定する。

ステップ

1. **Event Center →⚙→Event Configuration→ Linkage Configuration** または **System→ Event Configuration →⚙ → Event Configuration → Linkage Configuration** へ。

2. 電子**メール**パラメータを設定するには、**［電子メール］を**クリックします。

表13-15 Eメール・リンケージ

項目	説明
サーバー認証	**SMTPサーバーがユーザー認証を必要とする場合は有効にし、ユーザー名とパスワードを適宜入力する。**
SMTPサーバー	SMTPサーバーのIPアドレスまたはホスト名（例：smtp.263xmail.com）。
SMTPポート	SMTPポート。SMTPに使用されるデフォルトのTCP/IPポートは25です。
SSL/TLSを有効にする	SMTPサーバーにSSL/TLSの要件がある場合は、SSL/TLSを有効にする。
送信者	送信者名。
送信者の住所	送信者の住所。
レシーバーの選択	受信機を選択します。受信機は3台まで設定できます。
添付画像	アラーム画像を添付したメールを送信する。
周囲保護のための3つの添付画像を有効にする	境界保護イベントがトリガーされると、デバイスは3つのアラーム画像を添付した電子メールを送信する。
インターバル	添付画像をキャプチャする時間間隔。

注

3. アラームリンク用のオーディオファイルを管理するには、**［オーディオ管理］を**クリックします。

リストには削除できないデフォルトのオーディオファイルが3つあります。USBメモリーからオーディオファイルをインポートすることができます。ファイルはAACまたはMP3フォーマットで、各ファイルのサイズは1MB以内でなければなりません。

4. IPスピーカーを接続している場合は、**［IPスピーカー］を**クリッ クして、選択したIPスピーカーに音声ファイルをインポートし、 アラーム連動させます。

注

- このリンクアクションは、いくつかのイベントタイプでのみ利用可能である。
- アップロードする音声ファイルはMP3、WAV、ACCのいずれかのフォーマットで、ファイルサイズは1MB以下でなければなりません。

5. アラーム出力］をクリックして、アラーム出力パラメータを設定します。

注

- 各アラーム出力の名前をクリックして編集します。
- アラーム出力 No.は、機器背面パネルの No.と同じです。例えば、**Local->1**
  とは、装置背面パネルのアラームアウト No.

遅延

アラーム信号の継続時間。

アラーム状況

トリガーをクリックしてステータスを切り替える。

6. 音声およびライトカメラを接続している場合は、**[カメラ音声およびライト設 定**] をクリックして、アラームリンク用のカメラ点滅ライトおよびカメ ラ・スピーカーのパラメータを設定します。

注

このリンクアクションは、いくつかのイベントタイプでのみ利用可能である。

7. セキュリティコントロールパネルをクリックして、接続されているセキュリティコントロールパネルのパラメータを設定します。

13.3 解除設定

解除テンプレートが設定されると、テンプレートを使用してチャンネルを一括で解除できます。**解除を許可]**が有効になっているチャンネルは、解除テンプレートに従ってアラームリンク項目をトリガーしません。

ステップ

1. Event Center →⚙**→Event Configuration→ Linkage Configuration** または **System→ Event Configuration →**⚙ **→ Event Configuration → Linkage Configuration** へ。

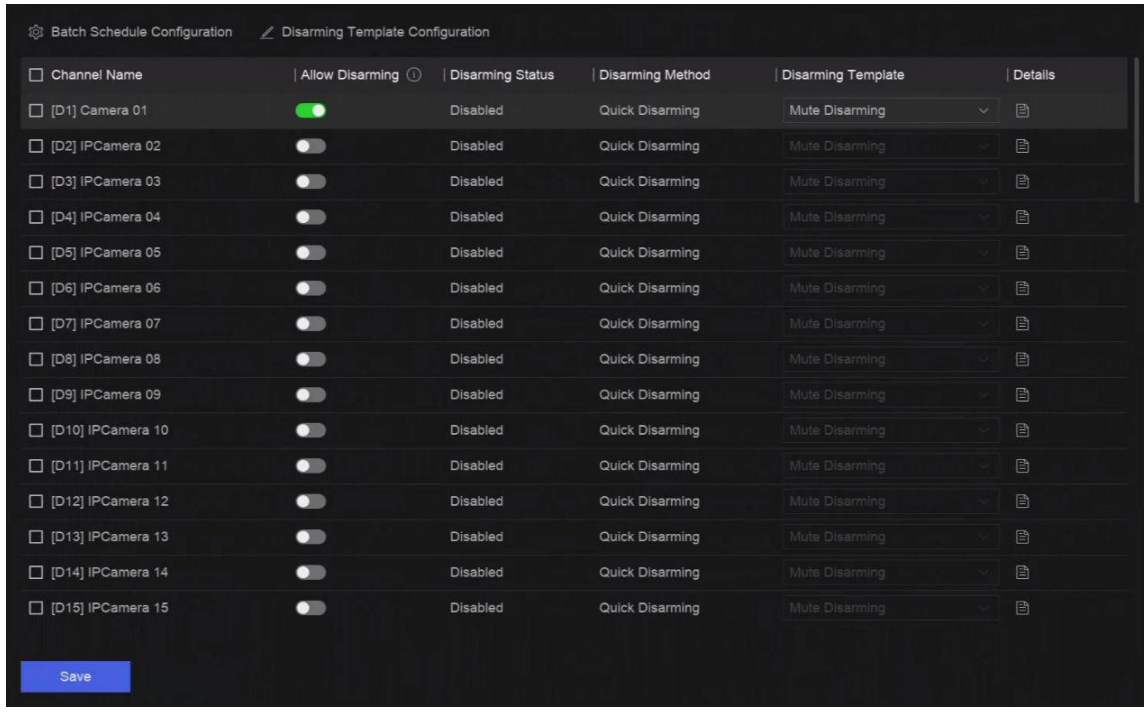


図 13-6 武装解除の構成

2. 解除を許可するチャンネルを選択します。

3. Batch Schedule Configuration] をクリックします。

4. 有効にする。

5. 解除テンプレートを選択します。利用可能なのは以下の2種類のみです。

注

現在、利用可能なテンプレートは2種類のみで、各テンプレートのパラメーターは設定できない。

6. **OK**をクリックする。

13.4 バッチ構成

リストされたイベントと**Notify Surveillance Center**の対応するリンクアクションは、**Event Center** → →**Event Configuration** → **Batch Configuration**または**System** → **Event Configuration** → → **Event Configuration** → **Batch Configuration** で一括して有効または無効に。イベントが有効になったら、**[イベント構成に移動]** をクリックしてルールを設定します。

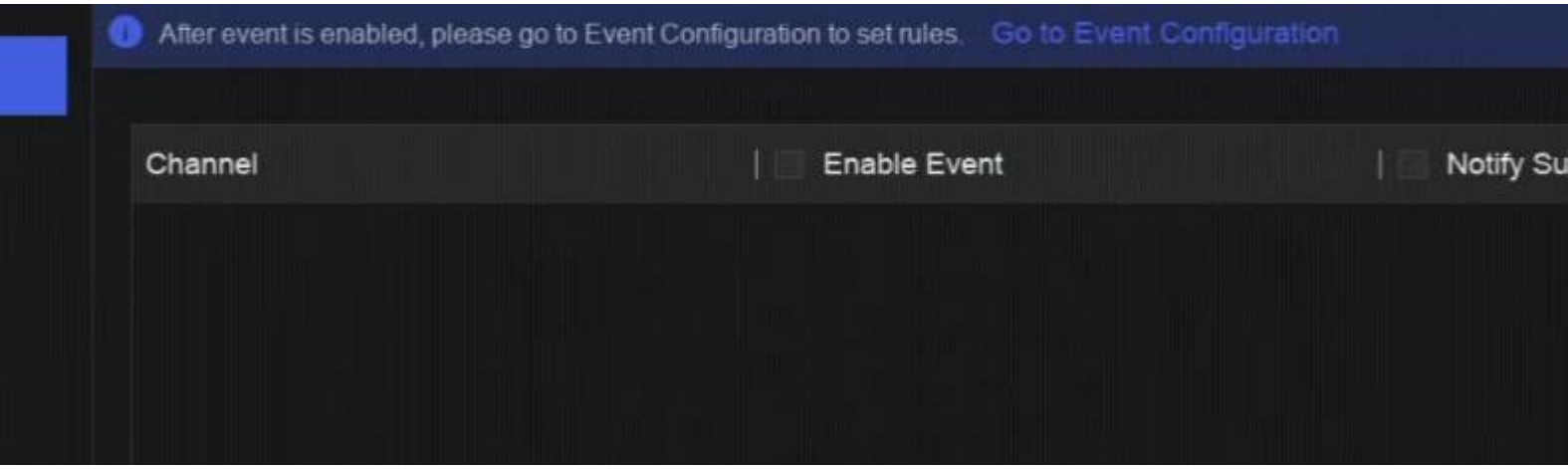


図 13-7 バッチ構成

13.5 イベント検索

動画や写真などのイベントファイルを検索条件に合わせて検索することができます。

ステップ

1. **イベントセンター** → へ。

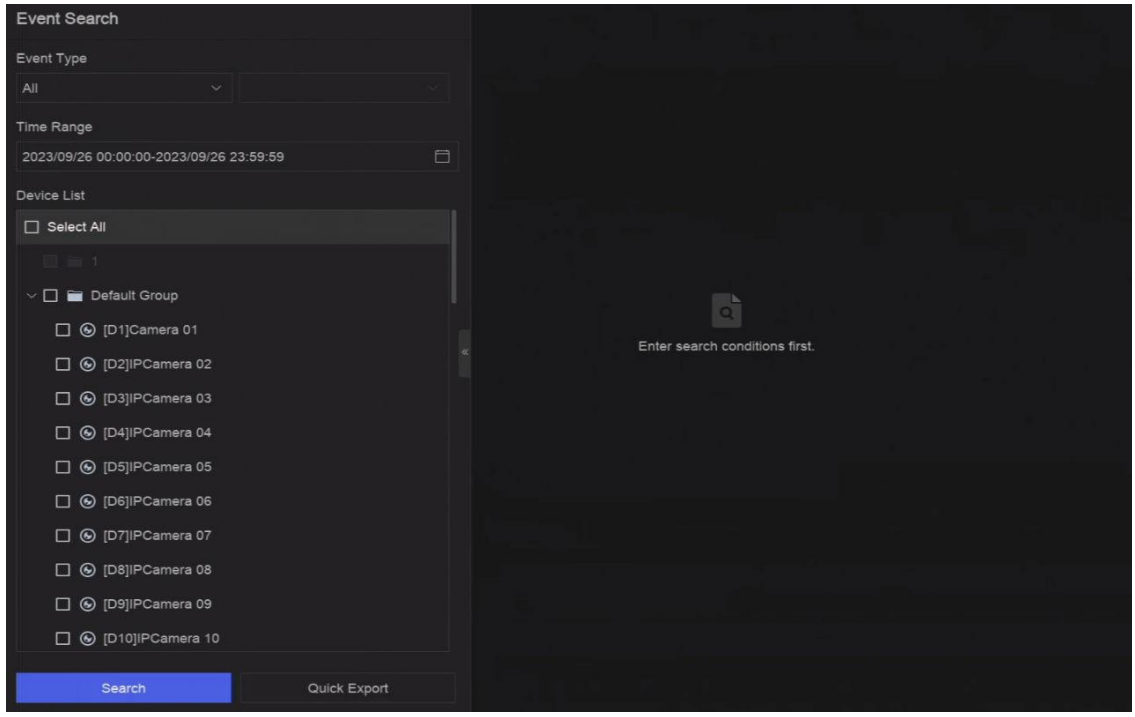


図 13-8 イベント検索

2. イベントの種類、時間、チャンネルなど、詳細な条件を指定します。
3. **検索を**クリックする。

   選択したチャンネルの検索結果が表示されます。

次に何をすべきか

結果リストから項目を選択し、バックアップのためにエクスポートします。

13.6 アラームを見る

アラームのビデオや写真をリアルタイムで見たり、再生できる。

ステップ

1. **イベントセンター** →へ。
2. **リアルタイムアラームを**クリックします。
3. リストからアラームを選択します。

   アラームの数が多すぎる場合は、**［フィルタ］を**クリックしてアラームを検索します。
4. **再生」を**クリックすると、アラーム録画ビデオが再生される。
5. あるアラーム画像を見る。利用可能な写真の数が表示されます。

第14章 検索とバックアップ

ファイルタイプ、イベントタイプ、時間、タグなど、さまざまな検索条件に従ってファイルを検索できます。検索結果はUSBメモリなど別のデバイスにエクスポートできます。

始める前に

HDDが正しく取り付けられ、録画パラメータが適切に設定されていることを確認する。

ステップ

1. **バックアップ**に行く。

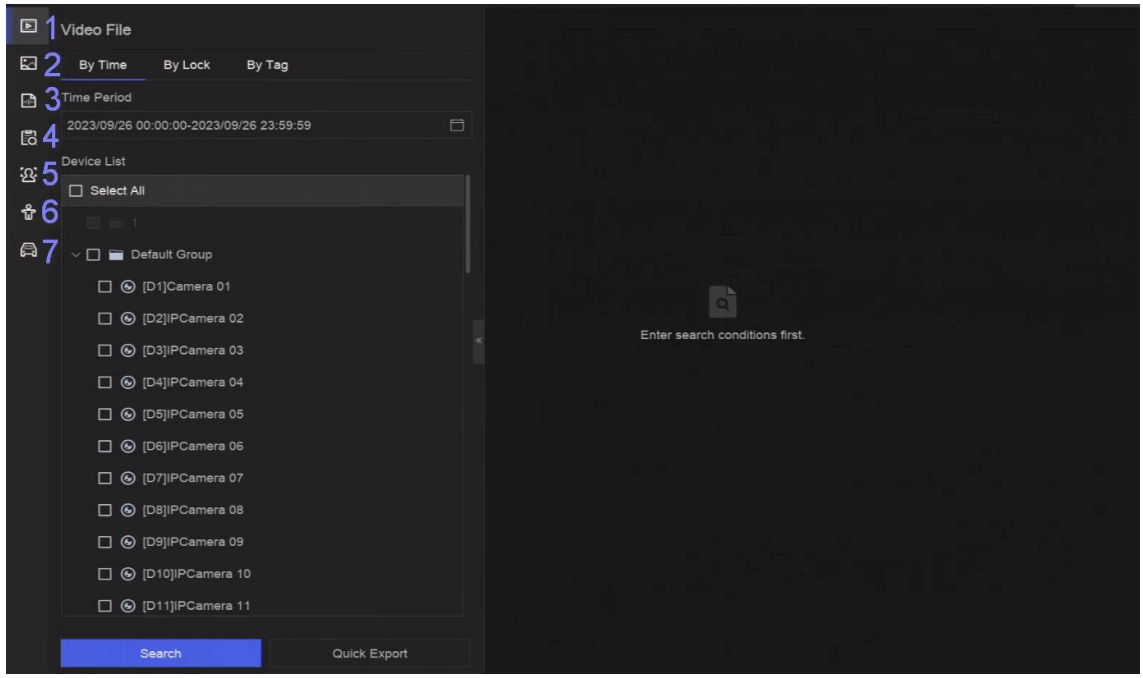


図14-1 検索とバックアップ

2. 左側から検索方法を選べます。

注

検索条件は、選択した検索方法によって異なる。

3. 検索条件を設定する。
4. **検索を**クリックする。

図 14-2 検索結果

5. オプション：以下の操作を行う。

1 クリックしてファイルを選択します。

2 クリックするとファイルがロックされます。ロックされたファイルは上書きされません。

3 ファイルをエクスポートするにはクリックしてください。

4 上部のツールバーを使用して、チャンネル別に結果をフィルタリングします。

5 上部のツールバーで表示切り替える。

6 異なる結果ページに移動する。

7 インターフェイスを拡大または縮小します。結果ビデオを選択した後、あなたはすぐにそれを再生することができるでしょう。

6. バックアップ用のUSBフラッシュドライブをデバイスに挿入する。

7. USBフラッシュドライブにファイルをエクスポートします。

- 結果リストでファイルを選択し、**エクスポートを**クリックします。
- **すべての**エクスポートするには、**「すべてエクスポート」**をクリックします。

第15章 AcuSearch

AcuSearch機能は、まずライブビュー中または再生中のビデオシーンから人の顔や体の画像を抽出し、次に抽出された画像と録画されたビデオを比較し、最終的にターゲットが含まれているビデオを検出します。

始める前に

お使いのデバイスまたはカメラがこのサポートしていることを確認してください。

ステップ

1. **System→ Smart Settings→ Algorithm Configuration→ Algorithm** Managementにアクセスして、AcuSearchアルゴリズムを有効にする。
   - **カメラによるAI**：カメラがAcuSearch分析を行う。
   - **NVRによるAI**：デバイスがAcuSearch分析を実行し、分析にはエンジン・リソースが必要です。
2. ライブビューまたはプレイバックに移動し、ビデオ再生中に左下隅の をクリックします。

   注
   - 再生中にターゲットを見つけるのが難しい場合は、**スマートサーチ**( )を使ってターゲットを含むシーンを見つけることをお勧めします。
   - 人間の顔や体は異なる色で縁取られるだろう。
   - また、 をクリックした後、画像上でカーソルをドラッグしてターゲットを手動でフレームに収めたり、フレーム領域を手動で調整することもできます。
3. クリック をクリックする。

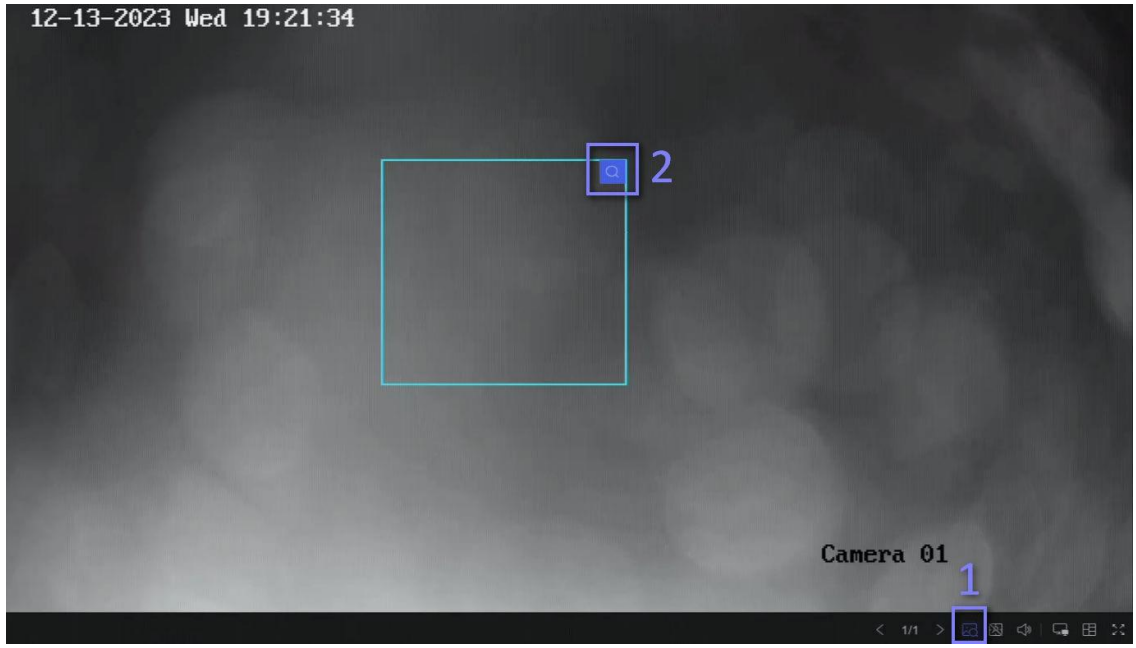


図15-1 AcuSearch

比較されたビデオが見つかった場合、デバイスはAcuSearchインターフェイスにリダイレクトされます。

4. 検索結果を見る

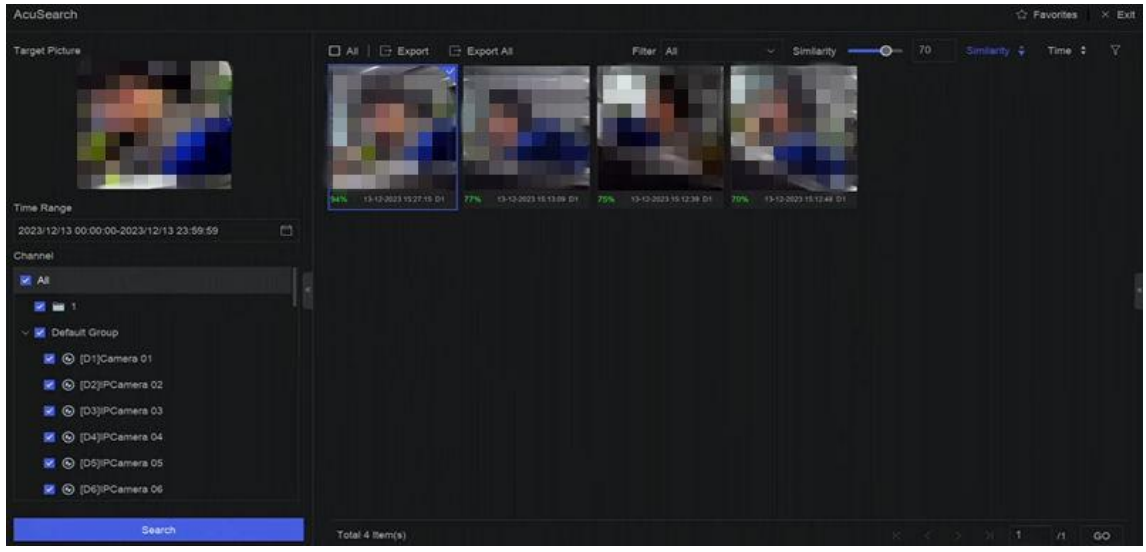


図 15-2 AcuSearch の結果

5. オプション： 結果が望ましくない場合は、**時間範囲**、**チャンネル**、または以下のようなパラメータを調整することができます。
また検索に似て**いる**。

6. オプション： 結果リストから項目を選択し、その対応するビデオは右側で再生され、赤い色でマークされます。ツールバーのアイコンをクリックして機能を実行することができます。

第16章 スマートセッティング

16.1 アルゴリズム管理

アルゴリズムは、さまざまなスマート・ファンクションを分析するためのデバイス・エンジンに使用される。スマートファンクションは、対応するアルゴリズムをエンジンに割り当てた後に使用できるようになります。

システム → イベント設定 → イベント設定 → スマート設定 → アルゴリズム管理、または**イベントセンター → イベント設定 → スマート設定 → アルゴリズム管理に**進みます。利用可能なアルゴリズムが一覧表示され、必要なアルゴリズムをエンジンをリンクすることができます。

AcuSearchアルゴリズムをサポートする特定のモデルでは、AcuSearchアルゴリズムを実行するカメラ（**AI by Camera**）またはNVR（**AI by NVR**）を選択できます。

16.2 エンジンの状態

走行状態、温度、アルゴリズム名など、エンジンの状態を見ることができます。

System→ Event Configuration→ Event Configuration→ Smart Settings→ Engine Statusまたは**Event Center→ Event Configuration→ Smart Settings→ Engine Statusに**アクセスしてください。アルゴリズムを切り替える必要がある場合は、**アルゴリズム管理** を参照してください。

16.3 タスクプラン管理

タスクのステータスはタスク確認できます。スマート解析結果は、人体や乗り物の写真を検索する際のフィルタリングに使用されます。

システム → イベント構成 → イベント構成 → スマート設定 → タスクプラン管理、または**イベントセンター → イベント構成 → スマート設定 → タスクプラン管理へ**進んでください。**非リアルタイム目標**比較では、各日の進捗状況を確認することができます。

タスクのステータスには主に3つの状態がある：**無効**、**待機中**、**有効**。**無効**

カメラで分析タスクが有効になっていない。

待機中

カメラの解析タスクが有効になっています。デバイスはデータ解析を待機しています。

有効

カメラの解析タスクが有効になっており、デバイスがカメラのデータを解析している。

16.4 リストライブラリ管理

リストライブラリは主にターゲット画像の保存とターゲット比較に使用されます。**見知らぬ人用**ライブラリは、見知らぬ人の写真を保存するために使用され、削除することはできません。

16.4.1 リストライブラリの追加

ステップ

1. **システム→ イベント設定→ イベント設定→ データ・アーカイブ→ リスト・ライブラリ** または **イベントセンター→ イベント設定→ データアーカイブ→ リストライブラリ**.
2. **追加を**クリックする。
3. ライブラリ名を入力してください。
4. **確認を**クリックします。

注

- リストライブラリの後、ライブラリ上でカーソルを動かすと編集や削除ができる。
- **一括削除]**をクリックすると、選択したライブラリを削除したり、選択したライブラリのすべてのピクチャを消去したりできます。

16.4.2 顔写真をライブラリにアップロードする

ターゲット画像の比較は、ライブラリ内のターゲット画像に基づいています。単一のターゲット画像をアップロードすることも、複数のターゲット画像をライブラリにインポートすることもできます。

始める前に

- 画像形式がJPEGまたはJPGであることを確認してください。
- すべての写真をあらかじめバックアップデバイスにインポートしておく。

ステップ

1. リストダブルクリックする。
2. **オプション：**写真にタグを追加するには、**カスタムタグを**クリックします。タグは、個人情報、組織、役職など、ご希望に応じて編集できます。
3. **追加**または**インポートを**クリックする。
4. 輸入写真
   - **追加**写真を1枚ずつアップロードする。写真に複数のターゲットがある場合は、それらの中から1つを選択する必要があります。
   - **インポート**：一度に複数の画像をインポートすることができます。デバイスはファイル名を画像名として使用し、他の属性は空のままにするか、または指定されたルールに従って画像ファイルをインポートします。画像内に複数のターゲットがある場合、デバイスはデフォルトで中央のターゲットを選択します。
5. **オプション：**以下の操作を行う。

ライブラリから写真を削除する	• 写真を選択して削除。 • 写真を選択し、**一括削除を**クリックすると、選択した写真が削除されます。
で写真を検索 図書館	 をクリックしてください。 をクリックしてください。
写真を別のライブラリにコピーする	写真を選択し、**「コピー」を**クリックすると、現在のライブラリのアップロードされた写真が別のライブラリにコピーされます。
写真の編集	写真名をクリックし、その属性を編集します。
写真のエクスポート	写真を選択し、**エクスポートを**クリックしてUSBフラッシュにエクスポートします。 ドライブ

16.5 セルフラーニングの設定

自己学習技術はアルゴリズムの精度を最適化し、ユーザーの手動介入を最小限に抑える。自己学習機能が有効な場合、デバイスは自動的に誤報材料を収集し、収集された材料を使用して、対応するアルゴリズムを常に訓練し、最適化する。

System→ Event Configuration→ Event Configuration→ Smart Settings→ Algorithm Managementまたは**Event Center → Event Configuration → Smart Settings → Algorithm** Managementにアクセスして、**Self-Learning**アルゴリズムを有効にしてください。

注

- このサポートしているのは一部のモデルのみです。
- 現在、自己学習機能を採用できるのは、境界保護イベントのみである。
- デバイスにエンジンが1つしかない**場合は、NVRによる**AIを無効にし、カメラが検出ターゲットの解析を実行する必要があります。デバイスに2つ以上のエンジンしかない場合は、**NVRによるAIを**有効にして、検出ターゲットの分析に1つのエンジンを使用し、別のエンジンを使用して自己学習アルゴリズムを実行できます。

16.5.1 自己学習タスク管理

自己学習アルゴリズムが実行された後、自己学習タスクも有効にする必要がある。

システムへ→ イベント構成→ イベント構成→ 自己学習→ タスク管理
または**Event Center→ Event Configuration→ Self-Learning→ Task** Managementでタスクを有効にしてください。

利用可能なタスクがリストアップされ、タスクのステータスとプログレスバーを見ることができる。素材集めに時間がかかる。

タスクが完了すると、自己学習アルゴリズムは自動的に更新されます。あなたは
更新時間を設定する**自動更新設定**。

注

- 自己学習アルゴリズムが更新中の場合境界保護イベントが利用できなくなる。
- フォース・トレーニングは技術サポートにのみ使用される。

16.5.2 モデル・マネージメント

自己学習アルゴリズムのモデルバージョンは、要件に応じて設定することができます。**システムへ→ イベント設定→ イベント設定→**

自己学習→ モデル

管理または**イベントセンター→ イベント設定→ 自己学習→ モデル管理** モデルバージョンを設定します。

以前のバージョンに戻す

モデルを前のバージョンに戻す。

デフォルトバージョンに戻す

モデルを工場出荷時のバージョンに戻す。

16.5.3 スマートステータス

System→ Event Configuration→ Event Configuration→ Self-Learning→ Smart Status または **Event Center→ Event Configuration → Self-Learning → Smart Status で**、各チャンネルの自己学習アルゴリズ ムのパフォーマンス・ステータスを見ることができます。

第17章 アプリケーション・センター

17.1 人と車両の検出

選択されたチャンネルの人と車両の情報がリアルタイムで表示される。

人と車両の検知は事前に設定しておく必要がある。**イベントセンター** →⚙で設定してください。

図17-1 人と車の検出 表17-1 人と車の検出 説明

そうだ。	説明
1	右クリックのショートカットメニュー。
2	人と車両の検出設定。レイアウト、比較成功プロンプト、リソースチャンネルを設定できます。
3	フルスクリーンに入る／出る。

17.2 チェックイン

チェックインタスクが追加されると、ライブチェックイン情報を表示したり、チェックイン結果を検索したりすることができます。

17.2.1 チェックイン・タスクの追加

チェックインを開始する前に、対応するタスクが適切に設定されている必要があります。

始める前に

- チェックイン用のカメラがきちんと接続されている。
- **System→ Smart Settings→ Algorithm Configuration→ Algorithm Management** にアクセスしてください。少なくとも1つのエンジンに**ターゲット認識を**割り当てます。
- チェックイン比較用のリストライブラリが正しく設定されています。詳細については、**リスト・ライブラリの追加を**参照してください。

ステップ

1. **チェックインを**クリック**する**。
2. 右クリックするとメニューが表示されます。
3. クリックする。
4. **追加を**クリックする。

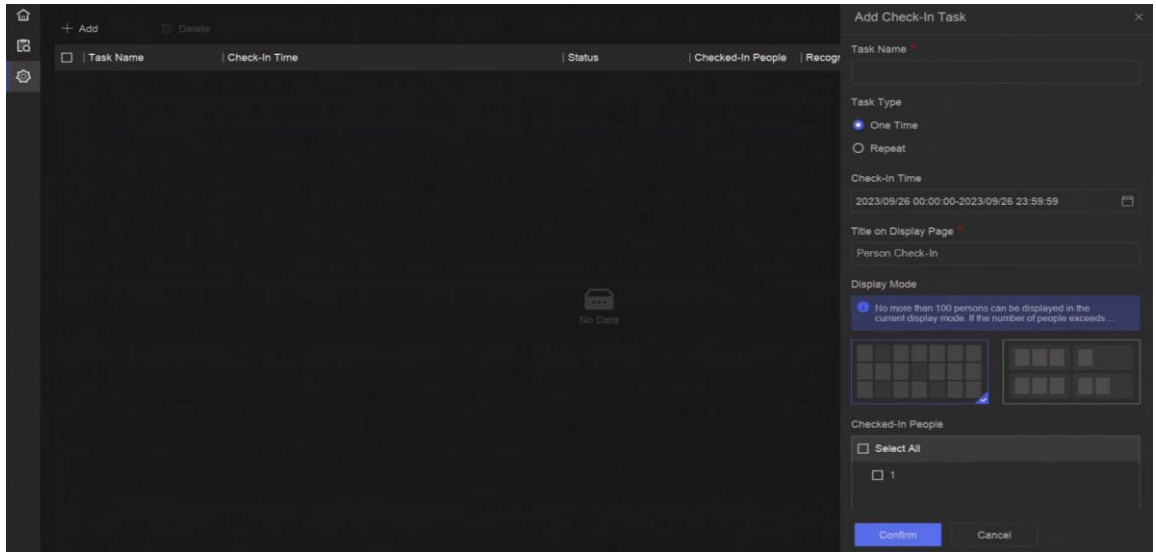


図 17-2 チェックイン・タスクの追加

5. **タスクを**設定

   する**ワンタイム**

   タスクの使用は1限り。

   リピート

   このタスクは何繰り返される。
6. **タスク名**、**チェックイン時間**、**認識**チャンネルなど、その他のパラメータを設定します。
7. **確認を**クリックします。

17.2.2 チェックイン記録の検索

チェックイン・タスクの設定後、記録を日または月単位で検索することができます。

始める前に

チェックインタスクが設定されていることを確認する。

ステップ

1. **チェックインへ** .
2. 右クリックするとメニューが表示されます。
3. クリックする。

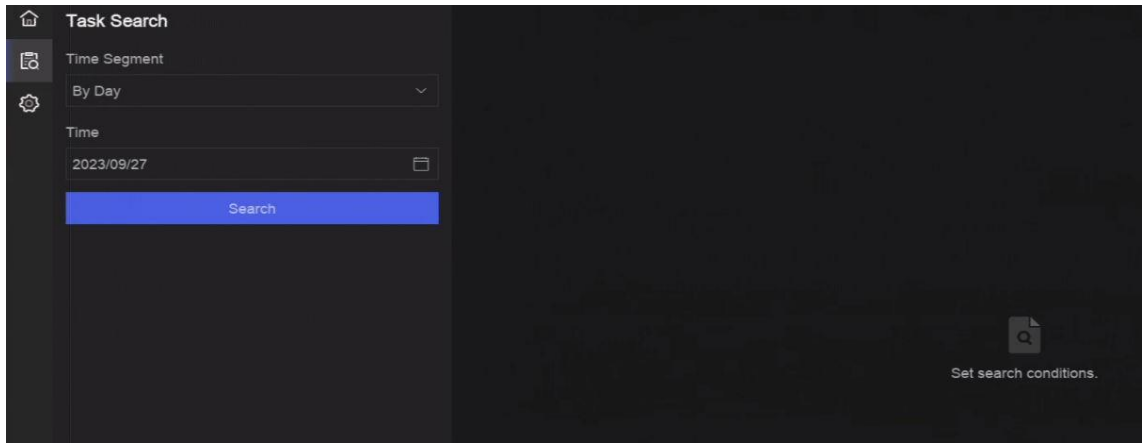


図 17-3 チェックイン記録の検索

4. セットタイム。
5. **検索を**クリックする。

17.3 統計レポート

集計レポートやヒートマップを見ることができる。

表 17-2 統計レポートの紹介

機能名	アイコン	コンディション	説明
人数のカウント		• 接続するIPサポートしている機能であること。例えば	ピープルカウンティングは、特定の設定されたエリアに出入りする人の数を計算し、分析のための日次/週次/月次/年次レポートを作成します。

機能名	アイコン	コンディション	説明
		カメラがデバイスに接続されています。 • カメラの統計データは、デバイスのHDDに保存することができます。	
ヒートマップ		• 接続するIPカメラがこの機能をサポートしている必要があります。 • カメラの統計データは、デバイスのHDDに保存することができます。	ヒートマップとは、データをグラフ化したもの。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します。

第18章 システム･パラメーター設定

システムパラメータには、デバイス名、地域、時間、ロック画面時間、含まれます。**システム→システム設定→システム**構成でパラメータを設定する。

表 18-1 パラメータの説明

タイプ	パラメータ名	説明
基本情報	画面ロック時間	指定された時間カーソルが動かないと画面がロックされる。
	ロック画面でのライブビュー許可	画面がロックされた後、デバイスはこの許可を持っているカメラのライブ画像を再生する。
地域と時間の設定	時間同期モード	**NTP時間同期** **NTP Time Syncを**選択し、**NTP Server**、**NTP Server Port**、**NTP Client Port**、**Intervalを**設定できます。Interval は、NTP サーバー内の 2 つの同期アクション間の時間間隔です。デバイスがパブリックネットワークに接続されている場合は、時刻同期機能を持つNTPサーバーを使用する必要があります。デバイスがカスタマイズされたネットワークに設定されている場合、NTPソフトウェアを使用して時刻同期用のNTPサーバーを確立することができます。 **手動時間同期** 手動でシステム時刻を設定する。 **Hik-Connectサーバーの時刻同期** デバイスはNTPサーバーのHik-Connectで時刻を同期します。
	民主党	DST（サマータイム）とは、1年のうちで時計が1日期間のこと。世界の一部の地域では、気候が最も暖かくなる月の夕方に、日照時間が増える効果がある。 夏時間の開始時に時計を一定期間進め（設定した夏時間のバイアスによって異なる）、標準時（ST）に戻るときに同じ期間戻す。

タイプ	パラメータ名	説明
メニュー出力	補助ポート自動切り替え	リアパネルに2台以上のモニターを接続した場合、そのうちの1台がメインメニューに入れない補助出力になることがあります。補助出力ウィンドウの画像は、間隔に従って自動的に次の画像に切り替わります。
チャンネル・ゼロ	-	バーチャル・知られるチャンネル・ゼロは、デバイスの全チャンネルのライブ画像を表示できるため、伝送帯域幅を節約できる。
RS-232	使用方法	**コンソール** コンバーターでPCに接続した後、PCはデバイスのパラメーターを設定できる。 **透明チャンネル** シリアルデバイスに直接接続します。PCはネットワーク経由でシリアルデバイスにリモートアクセスできます。

第19章 ホットスペアデバイスのバックアップ

ビデオレコーダーは、N+Mホットスペアシステムを形成することができる。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台のホットスペアビデオレコーダーで構成される。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が動作に切り替わるため、システムの信頼性が向上する。ホットスペアビデオレコーダーと作業用ビデオレコーダーの間には、下図のような双方向接続が必要である。

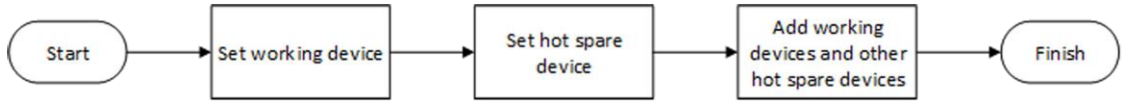


図 19-1 ホットスペア・システムの構築

注

- 最大32台のワーキングデバイスと32台のホットスペアデバイスが使用可能。
- 互換性のため、すべてのデバイスを同じモデルで使用することを推奨します。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。
- このサポートしているのは一部のモデルのみです。

19.1 作業デバイスの設定

ステップ

1. **System→ System Management→ N+M Hot Spare** にアクセスしてください。
2. **作業**モードを**通常モードに**設定する。
3. **Enableをオンに**する。
4. **保存を**クリックする。
5. **オプション：ホットスペアデバイスのIP**アドレスと**ホットスペアデバイスの動作ステータスを**表示します。

19.2 ホットスペア・デバイスの設定

ホットスペアデバイスは、作業デバイスが故障したときに、作業デバイスのタスクを引き継ぎます。

ステップ

1. **System→ System Management→ N+M Hot Spare** にアクセスしてください。
2. **作業モードをホットスペアモードに**設定する。
3. **保存を**クリックします。デバイスが自動的に再起動します。

注

- デバイスがホットスペアモードで動作している場合、カメラ接続は無効になります。
- 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保証するために、デバイスのデフォルトを復元することを強く推奨します。

4. **System→ System Management→ N+M Hot** Spareに再度アクセスしてください。
5. 作業デバイスをホットスペアシステムに追加する。
6. ホットスペアシステムにホットスペアデバイスを追加する。
7. **保存を**クリックする。

第20章 例外イベントの設定

例外イベントは、ライブ・ビュー・インターフェースのイベント・ヒントを取り、アラーム出力およびリンク・アクションをトリガーするように設定できます。

ステップ

1. **システム→ システム設定→ 例外** .

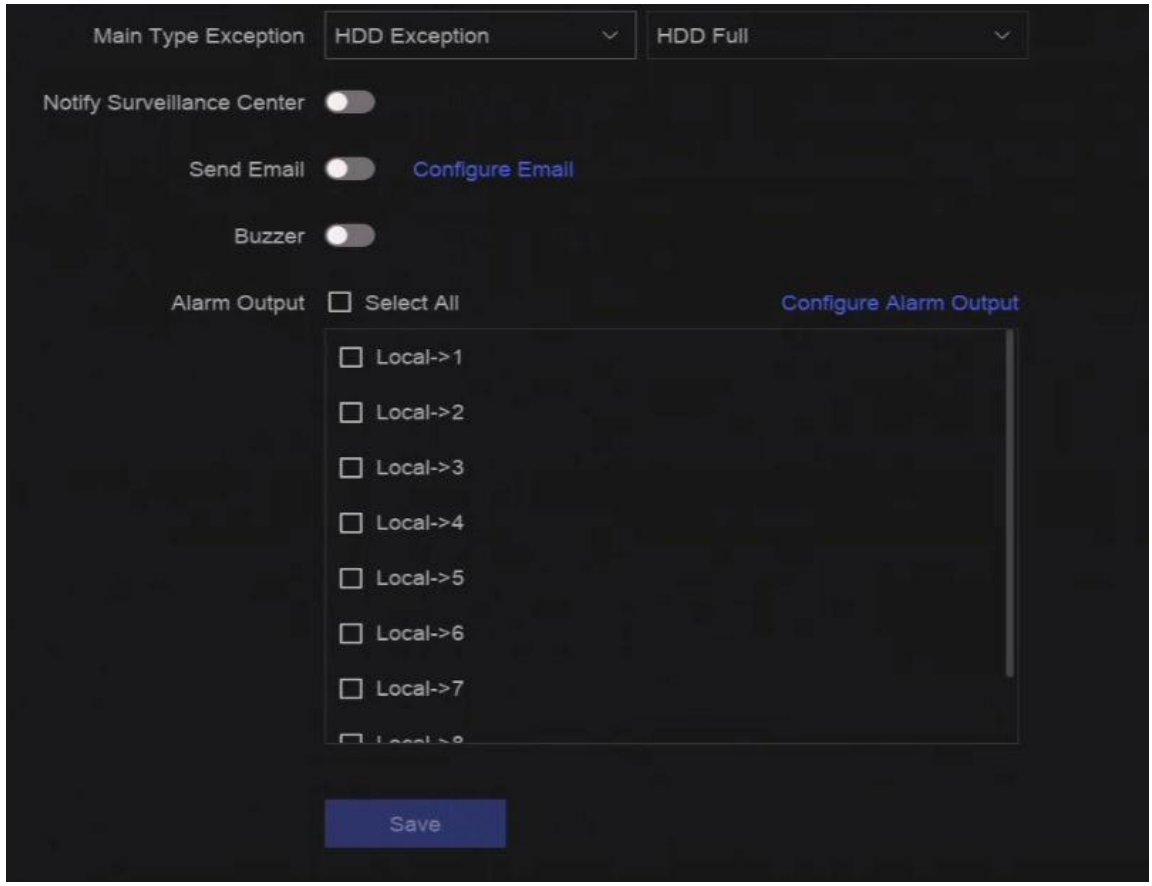


図 20-1 例外イベントの構成

2. 例外の種類を選択します。

3. 連結方法を設定する。

表 20-1 リンケージの説明

リンケージ方式	説明
監視センターに通知	イベントがすると、デバイスは例外またはアラーム信号をリモートアラームホストに送信できます。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たPCを指します。
ブザー	アラームを検知すると、ブザーがビープ音を発します。
メール送信	システムは、アラームが検出されると、アラーム情報を含む電子メールをユーザーまたはユーザーに送信できます。
アラーム出力	アラーム出力は、アラーム入力、モーション検知、ビデオ改ざん検知、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トリガーすることができます。

注

例外イベントが発生すると、右上の 。

4. **保存を**クリックする。

第21章 システム情報の表示

システム → システムメンテナンス → 稼働情報 → システム情報 で、録画情報、HDD情報、ネットワーク情報、ライブビューやビデオ再生のストリーム情報、時刻同期診断情報などのシステム情報を見ることができます。

デバイスの例外が発生した場合、例えば、時刻同期例外が発生し、RTC（コイン電池/ボタン電池）の電池が切れた場合、ビデオの録画や再生に影響を与える可能性がありますので、できるだけ早く例外を解決してください。

第22章 システムメンテナンス

システムメンテナンス機能には、ログ検索、スケジュール再起動、アップ含まれます。

22.1 スケジュール再起動

デバイスはスケジュールに従って自動的に再起動します。

System→ System Maintenance→ Maintenance→ Schedule Rebootにアクセスして機能を有効にし、再起動スケジュールを設定する。

22.2 アップグレード装置

デバイスシステムは、ローカルのUSBフラッシュドライブ、リモートのFTPアップグレードできます。

System→ System Maintenance→ Maintenance→ Upgrade にアクセスして、デバイスをアップグレードします。

22.3 バックアップと復元

System→ System Maintenance→ Maintenance→ Backup and Restore にアクセスして、システムパラメーターを復元またはバックアップします。

設定ファイルのインポート/エクスポート

デバイスのコンフィギュレーション・ファイルは、バックアップのためにローカル・デバイスにエクスポートすることができ、1つのデバイスのコンフィギュレーション・ファイルは、同じパラメータでコンフィギュレーションする場合、複数のデバイスにインポートすることができます。

シンプルリストア

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作業モード、デフォルトルート、サーバーポートなどを含む）とユーザーアカウントパラメーターを除くすべてのパラメーターを工場出荷時のデフォルト設定に戻す。

工場出荷時設定

すべてのパラメーターを工場出荷時の設定に戻す。

非アクティブに戻す

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。

22.4 ログ情報

システム→ システムメンテナンス→ メンテナンス→ ログを検索し、ログ情報をエクスポートします。

期限切れ時間設定

ログディスクがいっぱいになると、期間を超えたログは上書きされる。

22.5 ログサーバーの設定

システムログをサーバーにアップロードしてバックアップすることができます。

ステップ

1. **システム→ CX→ システム設定→ ネットワーク→ ネットワーク→ ログサーバー** .
2. **Enableをオンに**する。
3. **アップロード時間**、**サーバーIPアドレス**、**ポートを**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する。
5. **保存を**クリックする。

22.6 メンテナンスツール

S.M.A.R.T.検出や不良セクタ検出など、システムメンテナンスのためのツールが複数用意されている。

始める前に

HDDが正しく取り付けられていることを確認する。

ステップ

1. **システム→ システムメンテナンス→ メンテナンス→ メンテナンスツール** .
2. お客様のツールをお選びください。

表 22-1 ツールの説明

ツール名	説明
ネットワーク・データ 監視	ネットワーク・データ・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可能性のある異常やプロセスについて、ネットワーク・データをレビュー、分析、管理するプロセスである。
ネットワーク・パケット・キャプチャ	**ピン** pingテストは、宛先IPアドレスが到達可能かどうかを検出するために使用される。 **NICパケットキャプチャ**

ツール名	説明
	レコーダーがネットワークにアクセスした後、USBフラッシュ・ドライブを使用してネットワーク・パケットをキャプチャし、エクスポートすることができます。
HDDステータス検出	2017年10月1日以降に生成された4 TB～8 TBのシーゲイトHDDの健康状態を表示できます。この機能を使用して、HDD の問題のトラブルシューティングを支援します。健全性検出は、S.M.A.R.T.機能よりも詳細なHDDステータスを表示します。
S.M.A.R.T.ディテクション	S.M.A.R.T.（自己監視、分析、報告技術）は、故障の予期を期待して、さまざまな信頼性指標を検出するHDD監視システムである。
不良セクタ検出	HDDに不良セクタが多すぎる場合、HDDを交換することをお勧めします。そうしないと、HDD内のファイルが失われる可能性があります。
HDDクローン	eSATAインターフェイスを介してHDD内のデータを別のものに対応する。

注

テクニカルサポートの助けを借りてメンテナンスツールを使用することをお勧めします。

22.7 ソフトパワーオフ設定

ソフトパワーオフ機能は、POWER-AC（AC電源例外）、POWER-UPS（UPS例外）、POWER-UPSL（UPS低電力）アラーム出力（実パネル）を持つデバイスでのみ使用可能です。デバイスはこれらのアラームを受信し、記録することができます。POWER-AC および POWER-UPSL アラームの両方がトリガーされると、デバイスはプリセット時間に従って自動的に電源がオフになります。POWER-AC または POWER-UPSL アラームのいずれかがトリガーされない場合、デバイスは自動的に電源がオンになります。

ステップ

1. **System→ System Maintenance→ Maintenance→ Soft Power Off Configuration に**アクセスする。

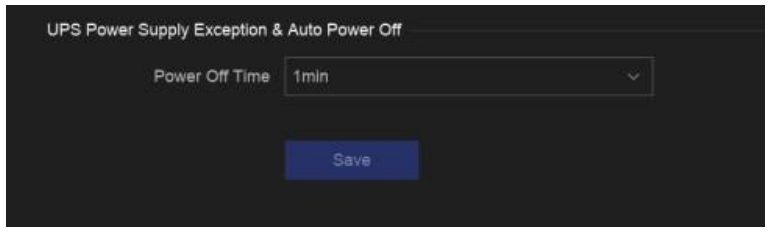


図 22-1 ソフト・パワー・オフの構成

2. **電源オフ時間の**設定。対応するアラームがトリガーされると、プリセット時間後にデバイスの電源が自動的にオフになります。
3. **保存を**クリックする。

例

例えば、**Power Off Time** が **1min** に設定されている場合、POWER-AC（AC 電源例外）アラームと POWER-UPSL（UPS電源低下）アラームの両方がトリガーされると、デバイスは 1 分後に自動的に電源を切ります。

第23章 セキュリティ管理

23.1 アドレスフィルター

アドレスフィルターは、特定のIP/MACアドレスがあなたのデバイスにアクセスすることを許可するか禁止するかを決定します。

始める前に

管理者アカウントでログインする。

ステップ

1. **システム→ システムメンテナンス→ セキュリティ管理→ アドレスフィルター** .
2. **Enableをオンに**する。
3. **フィルタリングの種類を**設定します。IPアドレスまたはMACアドレスによるフィルタリングを選択します。
4. **制限タイプを**設定します。デバイスのメカニズムは、特定のIP/MACアドレスがデバイスにアクセスすることを許可または禁止します。
5. **オプション：制限リストを**設定します。アドレスの追加、編集、削除ができます。
6. **保存を**クリックする。

23.2 ストリーム暗号化

ストリーム暗号化を有効にすると、リモートライブ視聴、リモート再生、ダウンロードした動画に暗号化キーが必要になる。

ステップ

1. **システム→ システムメンテナンス→ セキュリティ管理→ ストリーム暗号化** .
2. **Enableをオンに**する。
3. **暗号化キーを**設定する。

注

ストリームの暗号化キーは、Hik-Connectサービスの認証コードと同期しています。暗号化コードを有効にすると、Hik-Connectのストリームが強制的に暗号化されます。

4. **保存を**クリックする。

23.3 TLSバージョンの選択

TLSの設定は、HTTP(s)と拡張SDK有効です。より安全なストリーム伝送サービスを提供します。**システム → システムメンテナンス → セキュリティ管理** → TLSでTLSバージョンを選択します。

第24章 付録

24.1 適合電源アダプター一覧

下記の電源アダプター以外は使用しないでください。

電源アダプター モデル	仕様	メーカー
ADS-26FSG-12 12024EPG	12V、2A	深セン誉電子有限公司
MSA-Z3330IC12.0-48W-Q	12V、3.33A	(株)モソパワーサプライテクノロジー
MSA-C1500IC12.0-18P-DE	12V、1.5A	0000201935 MOSOテクノロジー株式会社
ADS-25FSG-12 12018GPG	CE、100～240 VAC、12 V、1.5 A、18 w、φ5.5× 2.1× 10	0000200174 深セン誉電子有限公司
MSA-C1500IC12.0-18P-US	12V、1.5A	0000201935 MOSOテクノロジー株式会社
TS-A018-120015AD	100～240VAC、12V、1.5A、18インチ w、φ5.5× 2.1× 10	0000200878 深圳市トランシン・テクノロジーズ有限公司
MSA-C2000IC12.0-24P-DE	12V、2A	0000201935 MOSOテクノロジー株式会社
ADS-24S-12 1224GPG	CE、100～240 VAC、12 V、2 A、24 W、.1	0000200174 深セン誉電子有限公司
MSA-C2000IC12.0-24P-US	US、12 V、2 A	0000201935 MOSOテクノロジー株式会社
ADS-26FSG-12 12024EPCU	US、12 V、2 A	0000200174 深セン誉電子有限公司
KPL-040F-VI	12V、3.33A、40W	0000203078 チャンネルウェルテクノロジー（株
MSA-Z3330IC12.0-48W-Q	12V、3.33A	0000201935 MOSOテクノロジー株式会社
MSP-Z1360IC48.0-65W	48V、1.36A	0000201935 MOSOテクノロジー株式会社
KPL-050S-II	48V、1.04A	0000203078 チャンネル・ウェル・テクノロジー（株

24.2 用語集

デュアルストリーム

デュアルストリームは、高解像度のビデオをローカルに録画し、低解像度のストリームをネットワーク経由で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、メインストリームの最大解像度は1080P、サブストリームの最大解像度はCIFです。

DVR

Digital Video Recorderの略。DVRは、アナログカメラからのビデオ信号を受信し、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ある。

HDD

ハードディスク・ドライブの略。デジタル符号化されたデータを磁性体表面のプラッタに保存する記憶媒体。

ディーエイチシーピー

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ために、デバイス（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

ハイパーテキスト・トランスファー・プロトコルの略。ハイパーテキストのリクエストや情報を、ネットワークを介してサーバーとブラウザーの間で転送するためのプロトコル。

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ある。主に、個々のユーザーがイーサネット経由で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る。

ディーディーエヌエス

ダイナミックDNSとは、インターネット・プロトコル・スイートを使用するルータやコンピュータ・システムなどのネットワーク接続されたデバイスが、DNSに保存されている設定済みのホスト名、アドレス、その他の情報のアクティブなDNSコンフィギュレーションをリアルタイム（アドホック）で変更するようにドメインネームサーバに通知する機能を提供する方法、プロトコル、またはネットワークサービスのことである。

ハイブリッドDVR

ハイブリッドDVRは、DVRとNVRを組み合わせたものです。

エヌティーピー

Network Time Protocolの略。ネットワーク上のコンピューターの時計を同期させるために設計されたプロトコル。

NTSC

National Television System Committeeの略。米国や日本などで使われているアナログテレビ規格。NTSC信号の各フレームには、60Hzで525本の走査線が含まれる。

NVR

Network Video Recorderの略。NVRは、IPカメラ、IPドーム、その他のDVRの集中管理と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。

パル

Phase Alternating Lineの略。PALもまた、世界の大部分で放送テレビシステムに使用されているビデオ規格である。PAL信号は50Hzで625本の走査線を含む。

PTZ

パン、チルト、ズームの頭文字。PTZカメラはモーター駆動のシステムで、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ます。

USB

Universal Serial Bus（ユニバーサル・シリアル・バス）の略。USBは、デバイスとホスト・コンピュータ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。

24.3 よくある質問

24.3.1 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の設定が不適切。
2. サブストリームの接続に失敗しました。

ソリューション

1. **カメラ → ビデオパラメーター → サブストリーム** 。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）。

   注

   ビデオレコーダーがこのサポートしていない場合は、ウェブブラウザでカメラにログインし、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を適切に設定し（解像度は720p以下、最大ビットレートは2048Kbps以下）、チャンネルを削除して再度追加する。

24.3.2 ネットワークカメラが追加された後、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る。

ソリューション

カメラのパスワードを変更する。

警告

製品のセキュリティを向上させるために、ご自身で選択した強力なパスワード（大文字、小文字、数字、特殊文字のうち少なくとも3つを含む、最低8文字を使用）を作成することを強くお勧めします。特にセキュリティの高い、毎月または毎週パスワードをリセットすることで、より製品を保護することができます。

24.3.3 なぜビデオレコーダーはストリームタイプがサポートされていないと通知するのですか？

理由

カメラのエンコード形式がビデオレコーダーと不一致。

ソリューション

カメラがエンコードにH.265/MJPEGを使用しているが、ビデオレコーダーがH.265/MJPEGをサポートしていない場合は、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てください。

24.3.4 ビデオレコーダーがH.265を使っていることを確認するには？

ソリューション

ライブビューのツールバーのエンコーディングタイプがH.265になっているか確認してください。

24.3.5 ビデオレコーダーがIP競合を通知するのはなぜですか？

理由

ビデオレコーダーは他の機器と同じIPアドレスを使用します。

ソリューション

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

24.3.6 シングルまたはマルチチャンネルカメラで再生すると画像が固まるのはなぜですか？

理由

HDDの読み書き例外。

ソリューション

ビデオをエクスポートし、他のデバイスで再生してください。他の正常に再生される場合は、HDDを交換してもう一度試してください。

24.3.7 同軸ケーブル経由でPTZカメラを制御できないのはなぜですか？

理由

1. カメラはコアキシトロンに対応していません。
2. コアキシトロンのプロトコルが間違っている。
3. 信号はビデオ光トランシーバーの影響を受ける。

ソリューション

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

24.3.8 RS-485経由でPTZが反応しないように見えるのはなぜですか？

理由

1. RS-485ケーブルが正しく接続されていない。
2. RS-485インターフェースが壊れている。
3. 制御プロトコルが正しくない。

ソリューション

1. RS-485ケーブルが正しく接続されているか確認してください。
2. RS-485インターフェイスを変更し、再試行してください。
3. 制御プロトコルがPelcoであることを確認する。

24.3.9 ビデオの良くないのはなぜですか？

理由

1. オーディオ入力デバイスの集音効果が悪い。
2. 送信の妨害。
3. オーディオパラメータが正しく設定されていない。

ソリューション

1. オーディオ入力デバイスが正しく動作しているか確認してください。別の音声入力デバイスに変更して、再度お試しください。
2. オーディオ伝送ラインをチェックします。すべてのラインが適切に接続または溶接され、電磁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。

24.4 腐食性ガスに関する通知

データセンター以外の部屋ではIEC 60721-3-3:2002の化学活性物質3C2レベルの要件を満たす腐食性ガス濃度限度を推奨する。

表 24-1 腐食性ガス濃度限度

腐食性ガス・カテゴリー	平均値 (mg/m^3)	最大値値 (mg/m^3)
SO_2（二酸化硫黄）	0.3	1.0
H_2S (硫化水素)	0.1	0.5
Cl_2（塩素）	0.1	0.3
HCl（塩化水素）	0.1	0.5
HF（フッ化水素）	0.01	0.03
NH_3（アンモニア）	1.0	3.0
O_3（オゾン）	0.05	0.1
NO_X (窒素酸化物)	0.5	1.0

注

- 上表の平均値は、機械室環境における腐食性ガスの典型的な管理限界値である。一般的に、腐食性ガスの濃度が平均値を超えることは推奨されません。
- 最大値とは、限界値またはピーク値を指す。腐食性ガス濃度が最大値に達するまでの時間は、1日あたり30分以内とする。

表 24-2 腐食性ガスの一般的な分類と発生源

カテゴリー	一次資料
H_2S (硫化水素)	地熱排出、微生物活動、石油製造、木材腐食、廃水処理など。
SO_2(二酸化硫黄)、$SO_{(3)}$(三酸化硫黄)	石炭燃焼、石油製品、自動車排気ガス、鉱石製錬、硫酸製造、タバコ燃焼など。
S（硫黄）	鋳造工場、硫黄製造工場など
HF（フッ化水素）	肥料製造、アルミニウム製造、セラミック製造、鉄鋼製造、電子機器製造、鉱物燃焼など。
NO_X (窒素酸化物)	自動車排気ガス、石油燃焼、微生物活動、化学工業など
NH_3（アンモニア）	微生物活動、下水、肥料製造、地熱排出など。
CO（一酸化炭素）	燃焼、自動車排気ガス、微生物活動、樹木の腐朽など。
Cl_2(塩素)、ClO_2(二酸化塩素)	塩素製造、アルミニウム製造、亜鉛製造、廃棄物分解など
HCl（塩化水素）	自動車排気ガス、燃焼、森林火災、海洋プロセスポリマー燃焼など。
HBr（臭化水素酸）、HI（ヨウ化水素酸）	自動車の排気ガスなど
O_3（オゾン）	大気光学プロセス（主に一酸化窒素と過酸化水素を含む）など。
C_nH_n (アルカン)	自動車の排気ガス、タバコの燃焼、動物の排泄物、下水、樹木の腐敗など。


See Far, Go Further