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

- この文書には、製品の使用および管理に関する手順が記載されています。本文中に含まれる図、表、画像およびその他の情報は、説明および参考目的のみを目的としています。
- この文書に記載されている情報は、ファームウェアの更新またはその他の理由により、予告なしに変更される場合があります。最新のバージョンは、Hikvisionのウェブサイト（***https://www.hikvision.com***）でご確認ください。別途合意がない限り、杭州Hikvision デジタルテクノロジー株式会社またはその関連会社（以下「Hikvision」といいます）は、明示的または黙示的ないかなる保証もいたしません。
- 本ドキュメントは、製品をサポートする専門家の指導と支援を受けてご使用ください。

本製品について

- この製品は、購入された国または地域でのみアフターサービスサポートを受けることができます。
- 選択された製品がビデオ製品の場合、以下のQRコードをスキャンして「ビデオ製品の利用に関する取り組み」を取得し、必ずお読みください。

知的財産権の承認

- 本ドキュメントに記載される製品に組み込まれた技術に関する著作権および/または特許権は、Hikvisionが所有しています。これには、第三者から取得したライセンスを含む場合があります。
- 本文書の一部（テキスト、画像、グラフィックなど）はすべてヒクビジョンに帰属します。本文書のいかなる部分も、書面による許可なしに、全部または一部を問わず、引用、複製、翻訳、改変を行うことはできません。
- HIKVISIONおよびその他のヒクビジョンの商標およびロゴは、各管轄区域においてヒクビジョンの財産です。
- 本文書に記載されているその他の商標およびロゴは、それぞれの所有者の財産です。
- HDMIおよびHDMI High-Definition Multimedia Interface、ならびにHDMIロゴは、米国およびその他の国において、HDMI Licensing Administrator, Inc.の商標または登録商標です。

法的免責事項

- 適用される法律で許される最大限の範囲において、本文書および記載された製品（ハードウェア、ソフトウェア、ファームウェアを含む）は「現状有姿」かつ「一切の瑕疵およびエラーを含む」状態で提供されます。HIKVISIONは、明示的または黙示的な一切の保証（商品性、満足のいく品質、または特定の目的への適合性を含むがこれらに限定されない）を一切提供しません。本製品の使用は、お客様の責任において行われます。いかなる場合においても、HIKVISIONは、特別損害、間接損害、付随的損害、または派生損害（事業利益の損失、事業の中断、データの損失を含むがこれらに限定されない）について、契約違反、不法行為（過失を含む）、製品責任、またはその他の理由に基づく場合であっても、一切の責任を負いません。システム障害、または文書の喪失を含む損害について、契約違反、不法行為（過失を含む）、製品責任、またはその他の理由に基づくものであっても、製品の使用に関連して生じた損害について、HIKVISIONは一切の責任を負いません。これは、HIKVISIONがそのような損害または損失の可能性について事前に通知を受けていた場合でも同様です。
- あなたは、インターネットの性質上、内在するセキュリティリスクが存在することを承認します。HIKVISIONは、サイバー攻撃、ハッカー攻撃、ウイルス感染、またはその他のインターネットセキュリティリスクに起因する異常な動作、プライバシー漏洩、またはその他の損害について一切の責任を負いません。ただし、必要に応じて適切な技術サポートを提供します。
- お客様は、本製品を適用されるすべての法律に準拠して使用することに同意し、その使用が適用される法律に準拠していることを確保する責任はお客様にのみあります。特に、あなたは、第三者の権利（パブリシティ権、知的財産権、データ保護権その他のプライバシー権を含むがこれらに限定されない）を侵害しない方法で本製品を使用する責任を負います。お客様は、大量破壊兵器の開発または製造、化学兵器または生物兵器の開発または製造、核爆発または安全でない核燃料サイクルに関連するいかなる活動、または人権侵害を支援する目的での使用は、一切禁止されます。
- 本文書と適用される法律との間に矛盾が生じた場合、後者が優先されます。

規制情報

FCCに関する情報

変更または改変が、適合責任者によって明示的に承認されていない場合、ユーザーの機器の操作権限が無効になる可能性があります。FCC 準拠: この機器は、FCC 規則の第15部に準拠する制限値を満たすことを確認するための試験を受けています。これらの制限値は、住宅環境での使用において有害な干渉から合理的な保護を提供するよう設計されています。この機器は、無線周波数エネルギーを発生、使用し、放射する可能性があります。指示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、特定の設置環境において干渉が発生しないことを保証するものではありません。この機器がラジオまたはテレビの受信に有害な干渉を引き起こす場合（機器の電源をオン/オフすることで確認できます）、ユーザーは次の措置の1つまたは複数を試すよう推奨されます：

- 受信アンテナの方向を変更するか、移動させる。
- 機器と受信機との距離を離す。
- 機器を、受信機が接続されている回路とは異なる回路のコンセントに接続する。
- 販売店または経験豊富なラジオ/テレビ技術者に相談してください。FCCの条件

この装置はFCC規則の第15部に準拠しています。動作は次の2つの条件に準拠しています。

条件に準拠しています：

- この装置は有害な干渉を引き起こしてはなりません。
- この装置は、受信した干渉（不要な動作を引き起こす可能性のある干渉を含む）をすべて受け入れる必要があります。

EU適合宣言

この製品および適用される場合、付属品も「CE」マークが付与されており、したがって、EMC指令2014/30/EU、LVD指令2014/35/EU、RoHS指令2011/65/EUに定める適用される調和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、欧州連合において一般廃棄物として処分できません。適切なリサイクルのため、この製品は、

同等の新品を購入する際、または指定の回収場所に廃棄してください。詳細については、***http://www.recyclethis.info*** をご覧ください。

規則（EU）2023/1542（電池規則）：この製品には電池が含まれており、規則（EU）2023/1542に準拠しています。この電池は、欧州連合において一般廃棄物として処分できません。製品のドキュメントで詳細なバッテリー情報を確認してください。バッテリーには、カドミウム（Cd）または鉛（Pb）を示す文字が記載されたこのマークが付けられています。適切なリサイクルのため、バッテリーを販売店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。

適用モデル

このマニュアルは、以下のモデルに適用されますが、このマニュアルに記載されているすべての機能が各モデルでサポートされ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-I2/8P
	DS-7616NI-I2/16ポート
	DS-7632NI-I2/16ポート
DS-7700NI-I4	DS-7708NI-I4
	DS-7716NI-I4
	DS-7732NI-I4
DS-7700NI-I4/P	DS-7708NI-I4/8P
	DS-7716NI-I4/16ポート
	DS-7732NI-I4/16P
	DS-7732NI-I4/24ポート
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-M2/16ポート
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-I2/S	DS-7608NXI-I2/S
	DS-7616NXI-I2/S
	DS-7632NXI-I2/S
DS-7600NXI-I2/P/S	DS-7608NXI-I2/8P/S
	DS-7616NXI-I2/16P/S
	DS-7632NXI-I2/16P/S
DS-7700NXI-I4/S	DS-7716NXI-I4/S
	DS-7732NXI-I4/S
DS-7700NXI-I4/P/S	DS-7716NXI-I4/16P/S
	DS-7732NXI-I4/16P/S
DS-8600NXI-I8/S	DS-8616NXI-I8/S
	DS-8632NXI-I8/S
	DS-8664NXI-I8/S
DS-8600NXI-I8/24P/S	DS-8632NXI-I8/24P/S

シリーズ	モデル
DS-9600NXI-I8/S	DS-9616NXI-I8/S
	DS-9632NXI-I8/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
DS-7600NXI-I2/VPro	DS-7608NXI-I2/VPro
	DS-7616NXI-I2/VPro
	DS-7632NXI-I2/VPro
DS-7600NXI-I2/16P/VPro	DS-7632NXI-I2/16P/VPro
	DS-7616NXI-I2/16P/VPro
DS-7700NXI-I4/16P/VPro	DS-7716NXI-I4/16P/VPro
	DS-7732NXI-I4/16P/VPro
DS-7700NXI-I4/VPro	DS-7716NXI-I4/VPro
	DS-7732NXI-I4/VPro
DS-7600NXI-I2/8P/VPro	DS-7608NXI-I2/8P/VPro
DS-9600NXI-I16R/VPro	DS-9632NXI-I16R/VPro

シリーズ	モデル
	DS-9664NXI-I16R/VPro
DS-9600NXI-I16/VPro	DS-9632NXI-I16/VPro
	DS-9664NXI-I16/VPro
DS-9600NXI-I8R/VPro	DS-9616NXI-I8R/VPro
	DS-9632NXI-I8R/VPro
	DS-9664NXI-I8R/VPro
DS-9600NXI-I8/VPro	DS-9616NXI-I8/VPro
	DS-9632NXI-I8/VPro
	DS-9664NXI-I8/VPro
DS-8600NXI-I8/VPro	DS-8616NXI-I8/VPro
	DS-8632NXI-I8/VPro
	DS-8664NXI-I8/VPro

安全注意事項

- 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設定は、インストール担当者および/またはエンドユーザーの責任です。
- 本製品の使用に際しては、当該国および地域の電気安全規格に厳格に従う必要があります。
- 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または取り外す前に、必ず機器の電源を切ってください。
- 感電の危険！メンテナンスを行う前に、すべての電源を遮断してください。
- 機器は接地された電源ソケットに接続する必要があります。
- コンセントは機器の近くに設置し、容易にアクセスできる位置に配置してください。
- ϟ の表示がある危険な帯電箇所を有する機器の場合、端子に接続される外部配線は、指示を受けた者によって設置する必要があります。
- 装置を不安定な場所に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（安全低電圧）およびLPS（限定電源）の要件を満たす必要があります。
- 高接触電流！電源に接続する前に、必ず接地してください。
- 装置から煙、臭い、または異常な音が発生した場合は、直ちに電源を切り、電源ケーブルを抜き、サービスセンターまでご連絡ください。
- UPSと組み合わせて使用し、可能な場合は工場推奨のHDDを使用してください。
- この機器は、子供が立ち入る可能性のある場所での使用には適していません。
- 注意：バッテリーを誤ったタイプのものと交換すると、爆発の危険があります。
- 電池を飲み込まないでください。化学やけどの危険があります！
- この製品にはコイン型/ボタン型電池が含まれています。コイン型/ボタン型電池を誤飲した場合、2時間以内に重度の内部やけどを引き起こし、死亡する可能性があります。
- 誤った種類の電池に交換すると、安全装置が機能しなくなる可能性があります（例：一部のリチウム電池タイプの場合）。
- バッテリーを火の中や熱いオーブンに捨てたり、機械的に潰したり切断したりしないでください。これにより爆発の危険があります。
- バッテリーを極端に高温の環境下に放置しないでください。爆発や可燃性液体またはガスの漏洩を引き起こす可能性があります。
- 電池を極端に低い気圧にさらさないでください。爆発や可燃性液体またはガスの漏洩を引き起こす可能性があります。
- 使用済みのバッテリーは、指示に従って処分してください。
- ファンブレードやモーターから身体の一部を離してください。メンテナンス中は電源を切断してください。
- 身体の部位をモーターから離してください。メンテナンス中は電源を遮断してください。
- 元のモデルと同じ電源装置を使用するか、同じ電圧と電流のLPS電源装置を使用してください。

予防措置と注意事項

装置を接続および操作する前に、以下の注意事項をご確認ください：

- この装置は室内専用です。液体がない、換気の良い、ほこりのない環境に設置してください。
- レコーダーがラックや棚に適切に取り付けられていることを確認してください。レコーダーを落とした際に生じる大きな衝撃や振動は、レコーダー内の敏感な電子部品に損傷を与える可能性があります。
- 装置は水滴や飛沫にさらされないようにし、花瓶などの液体入りの容器を装置の上に置かないでください。
- 点火したキャンドルなどの裸火源を装置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、カーテンなどの物で覆って換気を妨げないでください。装置をベッド、ソファ、ラグ、または類似の表面の上に置かないでください。
- 特定のモデルでは、AC電源に接続する際の端子接続が正しく行われていることを確認してください。
- 一部のモデルでは、必要に応じてIT電源分配システムへの接続に対応するため、機器が設計または改造されています。
-  バッテリーホルダー自体を識別し、バッテリーホルダー内のセルの位置を識別します。
- \+ 直流を使用する、または生成する装置の正極端子（複数ある場合はすべて）を識別し、- 直流を使用する、または生成する装置の負極端子（複数ある場合はすべて）を識別します。
- デバイスが電源を切られたり、長時間放置された場合、コイン型/ボタン型電池の電池が切れる可能性があります。
- コイン型/ボタン型電池の電池が切れた場合、システム時間が正しく表示されなくなります。電池の交換が必要な場合は、アフターサービスまでご連絡ください。
- 機器の周囲に十分な換気のため、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電源に接続する際、端子の配線を正しく行ってください。
- 鋭利な部分や角に触れないでください。
- デバイスが45°C（113°F）を超える温度で動作している場合、またはS.M.A.R.T.におけるHDD温度が指定値を超える場合、デバイスを冷却された環境で動作させるか、HDDを交換してS.M.A.R.T.におけるHDD温度を指定値以下に低下させてください。
- 山岳地帯、鉄塔、森林など特殊な環境下では、デバイスの入力端子にサージプロテクターを装着してください。
- 電源を切った後でも電気残留の可能性があるため、裸の部品（入力端子の金属部分など）に触れないでください。少なくとも5分間お待ちください。
- 機器の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ドングル接続専用です。接続された機器の電流は0.1Aを超えてはいけません。
- デバイスのシリアルポートはデバッグ専用です。
- デバイス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デバイスには防火ケースを装備する必要があります。
- デバイスパッケージに電源アダプターが同梱されている場合、同梱のアダプターのみを使用してください。

-  または  のステッカーが貼付されたデバイスについては、以下の注意点を遵守してください：注意：高温部です！触れないでください。部品を扱う際に指がやけどするおそれがあります。電源を切ってから30分以上経過し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. このマニュアルの指示に従って、デバイスをインストールしてください。
  2. 怪我を防ぐため、この装置は取り付け面に確実に固定してください。
- 高温環境（40 °C（104 °F）から55 °C（131 °F））では、一部の電源アダプターの出力が低下する可能性があります。
- 配線、取り付け、または分解を行う前に、必ず電源を切断してください。
- デバイスを自分で配線する必要がある場合、デバイスに表示されている電気的仕様に従って、適切な電源供給用の配線を選択してください。標準のワイヤーストリッパーを使用して、指定された位置で配線の被覆を剥がしてください。重大な事故を防止するため、剥がした配線の長さは適切にし、導体が露出しないようにしてください。
- デバイスから煙、臭い、または異常な音が発生した場合は、直ちに電源を切り、電源ケーブルを抜き、サービスセンターまでご連絡ください。

内容の規約

説明を簡素化するため、以下の規約をご確認ください。

- レコーダーまたはデバイスは主にビデオレコーダーを指します。
- IPデバイスは主に、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）、またはNVS（ネットワークビデオサーバー）を指します。
- チャネルは主にビデオレコーダー内のビデオチャネルを指します。

記号の規約

この文書で用いられる記号は、以下のとおり定義されます。

記号	説明
 危険	危険な状況を示し、回避しない場合、死亡または重大なけがを引き起こす可能性があります。
 注意	回避しない場合、機器の損傷、データ損失、性能の低下、または予期しない結果を引き起こす可能性がある危険な状況を示します。
 注意	本文の重要なポイントを強調したり補足したりするための追加情報を提供します。

インジケーターとインターフェースの説明

前面パネルのインジケーター説明

フロントパネルのインジケーターは、デバイスの異なる動作状態を表示します。

表1-1 共通インジケーターの説明

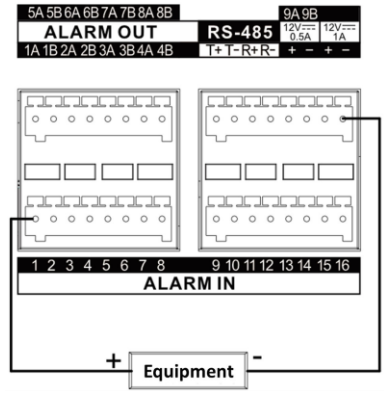
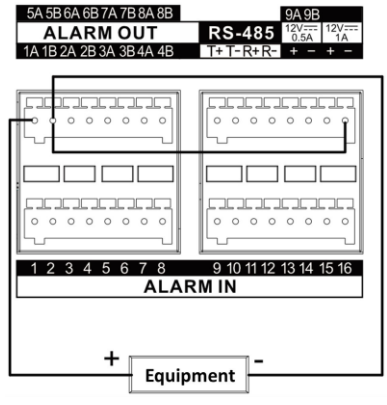
インジケーター	説明
⏻	インジケーターは、デバイスが電源投入時に点灯します。
🛢	HDDからデータを読み込み中または書き込み中時に、インジケーターが点滅します。
品	ネットワーク接続が正常に機能している際に、インジケーターが点滅します。

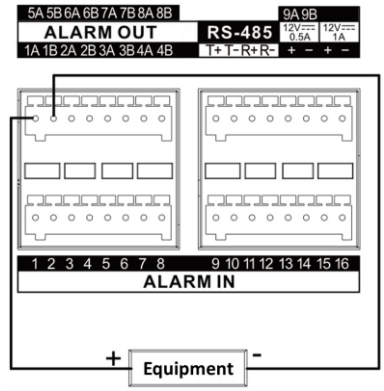
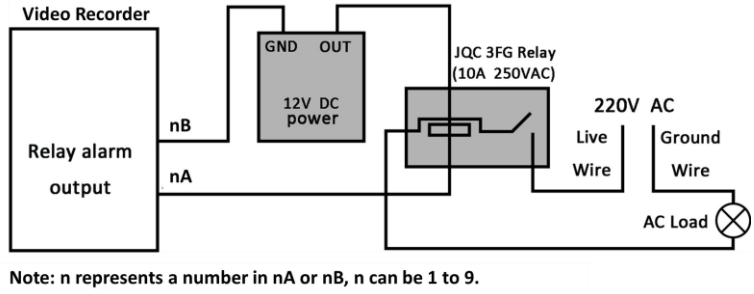
インターフェース説明

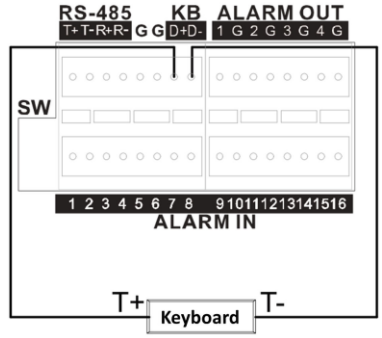
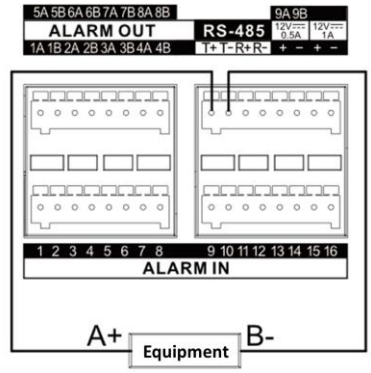
パネルのインターフェースはモデルによって異なります。一般的なインターフェースの記述については、以下の表を参照してください。

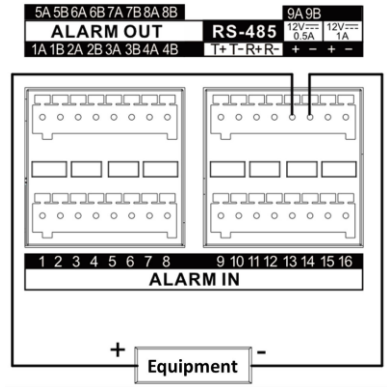
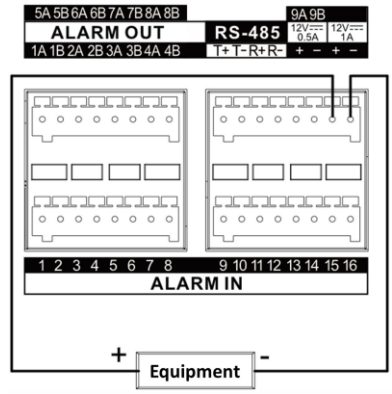
表1-2 共通インジケーターの説明

項目	説明
VIDEO IN	Turbo HDおよびアナログビデオ入力用のBNCインターフェース。
ビデオ出力	ビデオ出力用のBNCコネクタ。
オーディオ入力	RCAコネクタ（オーディオ入力用）。
オーディオ出力	RCAコネクタ（オーディオ出力用）。
ライン入力	RCAコネクタ（双方向オーディオ入力用）。
USB	追加デバイス用のユニバーサルシリアルバス（USB）インターフェース。
VGA	DB15コネクタ（ローカルビデオ出力およびメニュー表示用）
HDMI	HDMIインターフェース（ビデオ出力用）。
RS-485	RS-485シリアルインターフェース（パン/チルトユニット、スピードドームなど用）。
RS-232	RS-232インターフェース（パラメーター設定用またはトランスペアレントチャネル用）。
LAN	RJ-45自己適応型イーサネットインターフェース。
eSATA	記録またはバックアップ用のストレージおよび拡張インターフェース。
GND	接地。

アイテム	説明
電源スイッチ	デバイスの電源をオン/オフするスイッチ。
電源	100～240 VAC、48 VDC、または12 VDCの電源。
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。
アラーム入力	アラーム入力はアラーム入力信号を受信します。機器の正極端子（+）は番号に接続し、機器の負極端子（-）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、以下の図を参照してください。 
アラーム出力	アラーム出力はアラーム信号を出力します。 機器が直流電源を使用する場合、その正極端子（+）は「A」が付いた番号に接続し、負極端子（-）は「B」が付いた対応する番号に接続し、その後「-」または「G」に接続する必要があります。直流機器のアラーム出力接続例として、以下の図を参照してください。 

項目	説明
	交流電源を使用する機器の場合、その正極端子（+）は「A」の番号に接続し、負極端子（-）は対応する「B」の番号に接続します。 以下の図を、AC機器の警報出力接続例として使用してください。  **注意** 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。 以下の図を参考として使用してください。  **Note: n represents a number in nA or nB, n can be 1 to 9.**
KB	KBはキーボードを表します。「D+」と「D-」をそれぞれ「T+」と「T-」に接続してください。以下の図を参考として使用してください。

項目	説明
	
RS-485	RS-485は、2線式、半二重、多点接続の電気的仕様です。「T+」と「T-」をそれぞれ「A+」と「B-」に接続してください。 以下の図を参考にしてください。 
Ctrl 12V/ 12V 0.5A	外部アラーム装置用の制御可能な12 VDCおよび0.5/1 Aの電源出力。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。 以下の図を参考にご確認ください。

項目	説明
	
DC 12V/ $\frac{12V⎓}{1A}$	12 VDCおよび1 Aの電源出力を提供します。以下の図を参照 してください。 

HDDの取り付け

デバイスがHDDのホットスワップに対応していない場合、ハードディスクドライブ（HDD）をインストールする前に、デバイスの電源を切断してください。このインストールには、メーカー推奨のHDDを使用してください。

以下のQRコードをスキャンして、HDDの取り付け動画を表示してください。

図1-1 HDDの取り付け

ブラケットの取り付け

ブラケットの取り付けは、デバイスカバーを取り外す必要があり、HDDを内部ブラケットに取り付ける場合に適用されます。

手順

1. 背面のネジを緩め、カバーを後ろに押して取り外します。

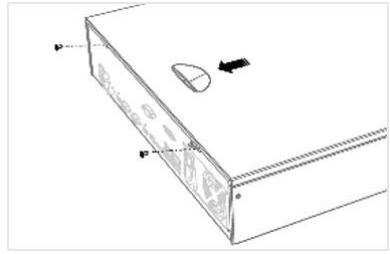


図1-2 カバーの取り外し

2. ネジでHDDをブラケットに固定します。

注意

HDDを下のブラケットに取り付ける前に、まず上のブラケットを取り外してください。

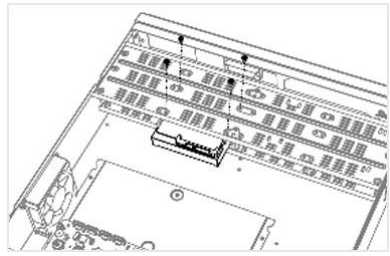


図1-3 HDDの固定

3. データケーブルと電源ケーブルを接続します。

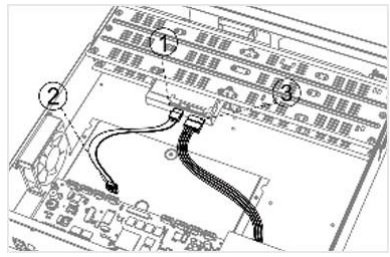


図1-4 ケーブルの接続

注

上記のステップを繰り返し、他のHDDをインストールできます。

4. デバイスカバーを再取り付けし、ネジを締め付けます。

フロントパネルのプラグ引き抜き取り付け

フロントパネルのプラグ引き抜き取り付けは、デバイスのフロントパネルを鍵で開けてHDDをインストールする必要がある場合に適用されます。

手順

1. HDDにマウント耳をネジで固定します。

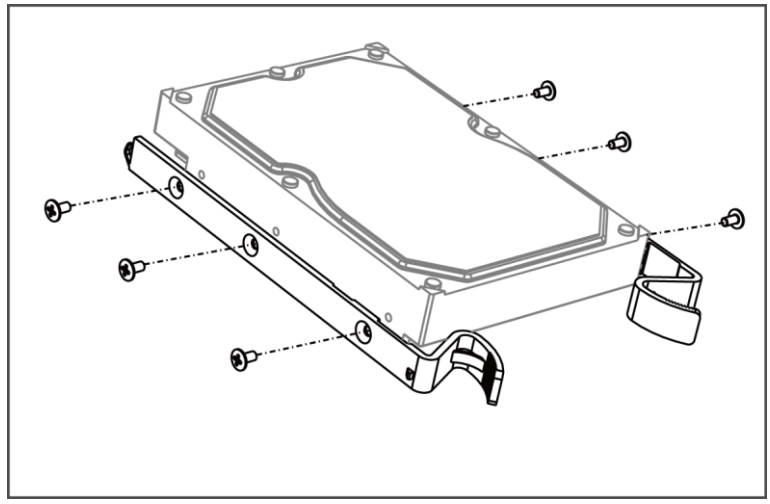


図1-5 HDDにマウント耳を固定する

2. 付属の鍵でフロントパネルのロックを解除し、フロントパネルの両側のボタンを押して開きます。

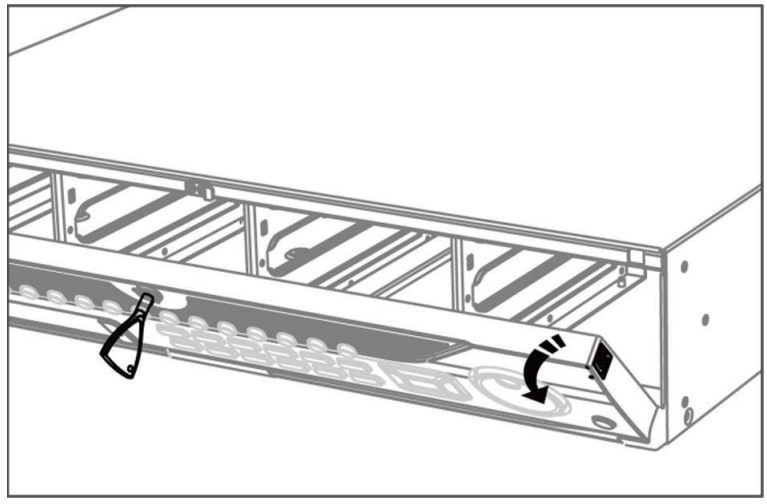


図1-6 フロントパネルの開け方

3. HDDをしっかりと固定されるまで挿入してください。

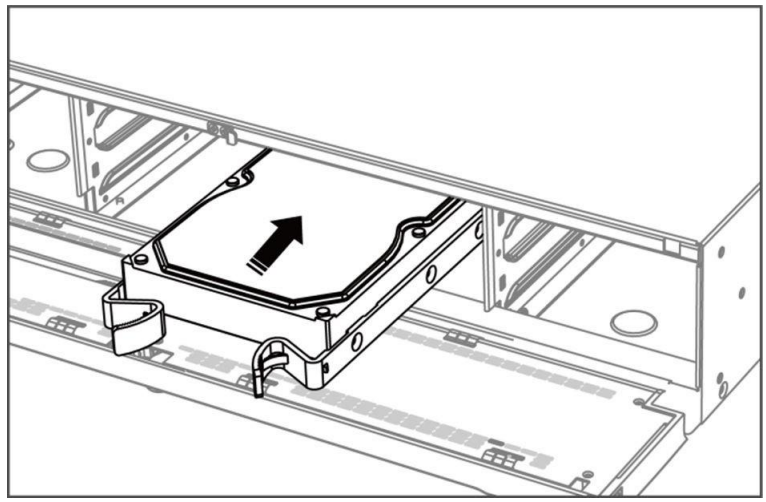


図1-7 HDDの挿入

4. オプション：他のHDDをインストールする場合は、上記のステップを繰り返し実行してください。

5. フロントパネルを閉じて、鍵でロックします。

HDDケースの取り付け

HDDケースの取り付けとは、HDDをケースにインストールし、その後HDDケースをスロットに接続する方法を指します。

手順

1. パネルキーで前面パネルのロックを解除します。

2. 前面パネルをデバイスから引き出し、左のハンドルより少し上部に位置させます。

注意

前面パネルとデバイスとの角度は10°以内にしてください。

3. 青いボタンを押してハンドルをポップアップさせ、ハンドルを握ってHDDケースをスロットから引き出します。

4. HDDケースにハードディスクを固定します。

1) HDDをケースに挿入します。SATAインターフェースはケースの底面に向ける必要があります。

2) HDDの位置を調整してください。ハードディスクの背面がHDDの底面と一致するようにしてください。

3) ドライバーを使用して、両側のネジ穴に4本のネジを締め付けます。

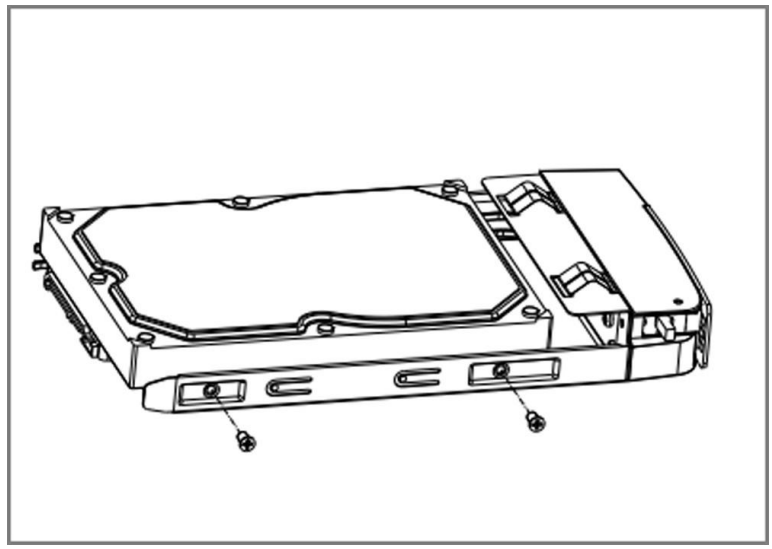


図1-8 HDDの固定

5. HDDケースをスロットに戻します。

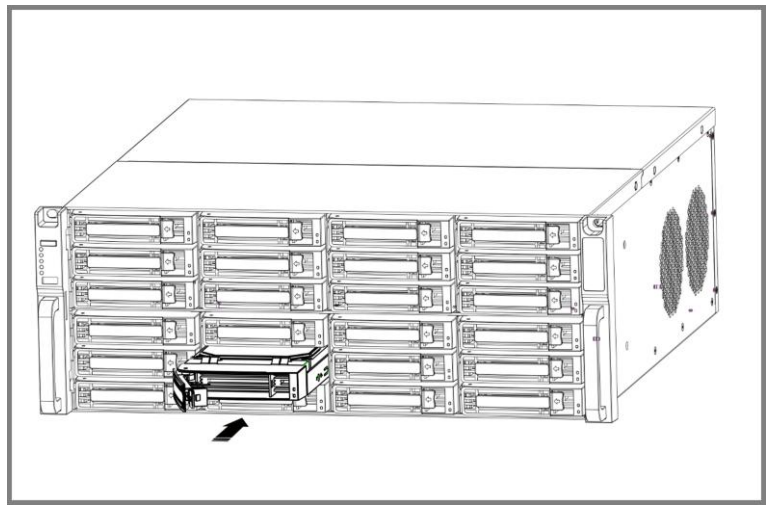


図1-9 HDDケースをスロットに押し込む

6. ハンドルを押し込み、カチッという音がするまで押します。これにより、HDDケースが固定されます。上記のステップを繰り返し、残りのハードディスクボックスをインストールします。

7. 前面パネルを閉じて、パネルキーでロックしてください。

底面固定取り付け

底面固定取り付けは、HDDをデバイスの底面に固定して取り付ける必要がある場合に適用されます。

手順

1. パネルのネジを緩めて、デバイスからカバーを取り外します。

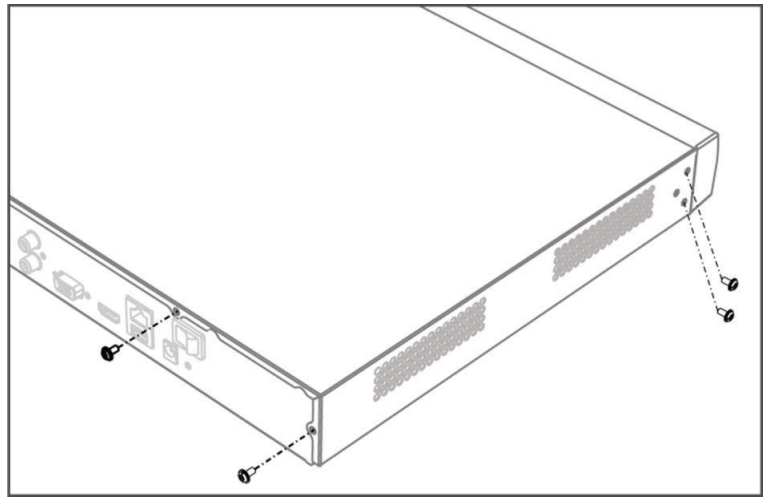


図1-10 カバーの取り外し

2. データケーブルと電源ケーブルを接続します。

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します。

2) データケーブルのもう一方の端をHDDに接続します。

3) 電源ケーブルの一端をHDDに接続します。

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します。

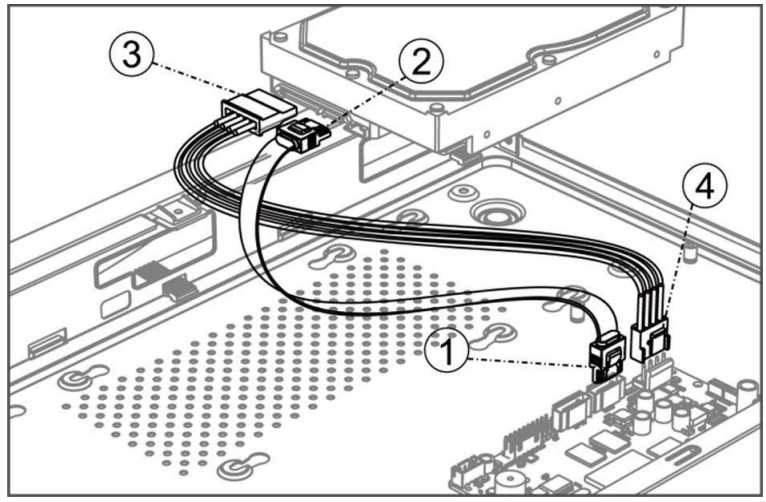


図1-11 ケーブルの接続

3. デバイスを設置し、HDDのネジ山をデバイスの底面の予約された穴と合わせ、ネジでHDDを固定します。

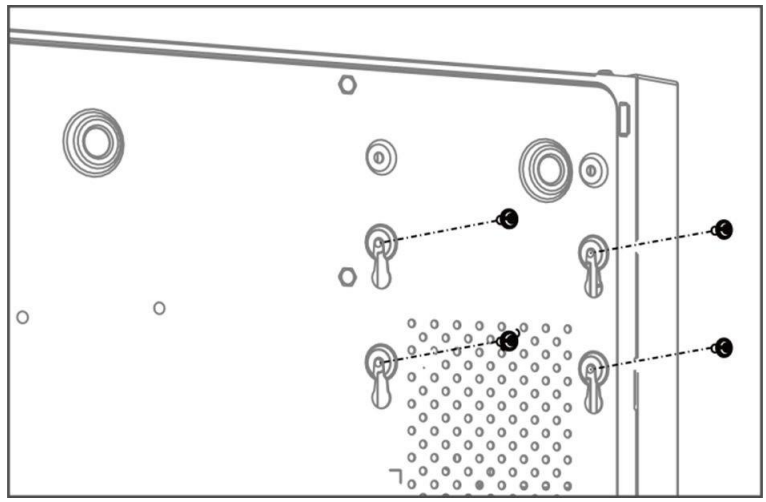


図1-12 HDDをデバイス底面に固定

4. オプション：他のHDDをインストールする場合は、上記のステップを繰り返し実行します。

5. デバイスカバーを再取り付けし、ネジを締め付けます。

コイン/ボタン型電池の交換

コイン型/ボタン型電池は、デバイスが電源を切られた後または長時間放置された後、システム時間が正しくない場合に交換してください。

開始前に

デバイスを電源オフにしてください。

手順

1. デバイスのシャーシカバーを外します。
2. マザーボード上のコイン型/ボタン型電池を探します。
3. 親指を電池スロットの外側に置き、人差し指で正極の接点スプリングを優しく外側に押します。電池が自動的に飛び出します。

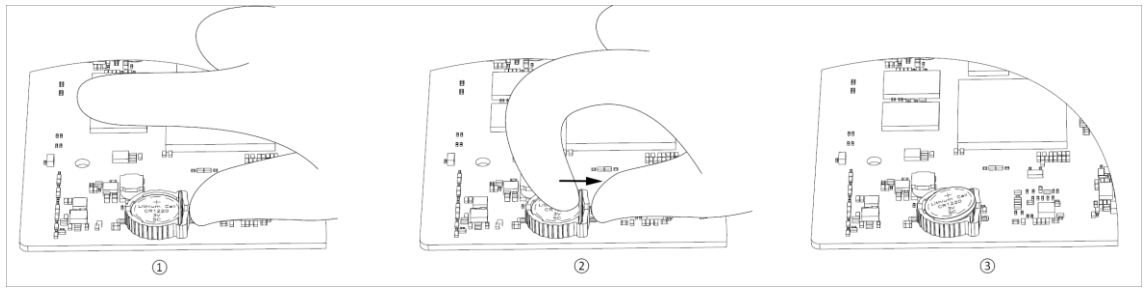


図1-1 電池の取り外し

注意

- 電池を取り外す際は、静電気防止手袋を着用してください。
- スプリングが外側に押し出す際に過度の力によって変形した場合、バッテリーを挿入する前に、スプリングを元の位置に戻して調整する必要があります。

4. バッテリーを、バッテリースロットのプラスチックのスナップポイントがある側に向かって斜めに挿入し、その後、正極の接触スプリングの近くを押して、スプリングの下にスナップさせるようにします。

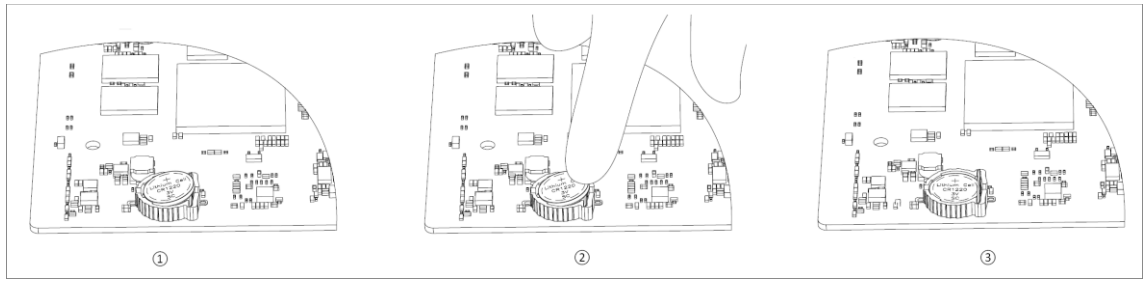


図1-2 バッテリーの交換

注意

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. デバイス筐体カバーを再取り付けます。

次にやるべきこと

システム時間が正しくない場合は、時間設定を行ってください。

内容

第1章 ローカルメニューからアクティベート

初回アクセス時は、デバイスをアクティベートするために管理者パスワードを設定する必要があります。アクティベート完了前は、いかなる操作も行うことができません。デバイスはウェブブラウザ、SADP、またはクライアントソフトウェア経由でもアクティベート可能です。

開始前に

デバイスがモニターとマウスに接続されていることを確認してください。

手順

1. デバイスを電源オンにします。
2. 地域またはDST（夏時間）の設定を行います。
3. システム言語を選択してください。
4. 管理者パスワードを2回入力してください。

注意

私たちは、製品のセキュリティを強化するため、ご自身で選択した強固なパスワード（8文字以上で、大文字、小文字、数字、特殊文字の少なくとも3種類を含む）を設定することを強くおすすめします。また、特に高セキュリティシステムでは、パスワードを定期的に変更することをおすすめします。月次または週次でのパスワード変更は、製品の保護をさらに強化します。

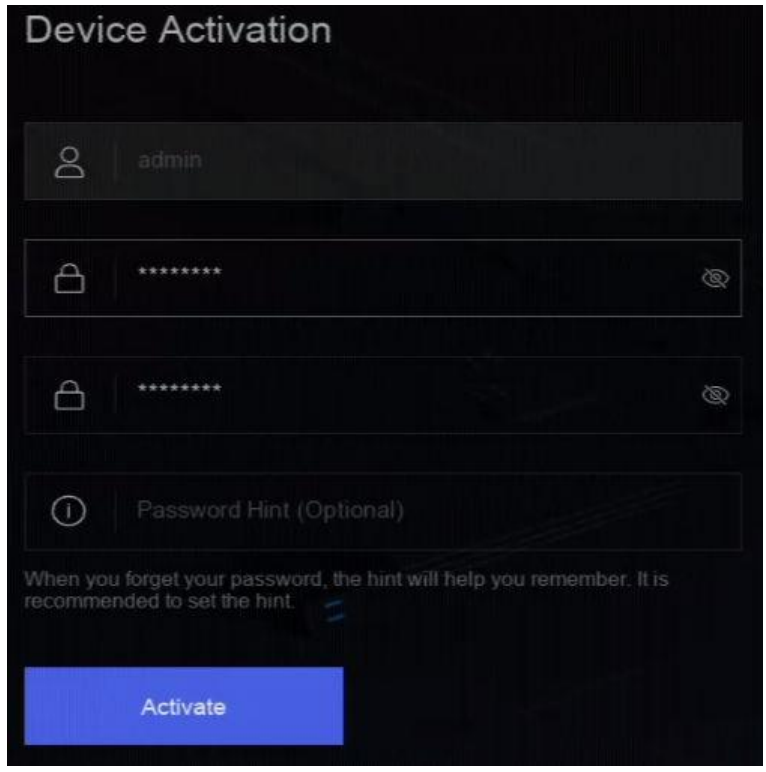


図1-1 ローカルメニューからアクティベート

5. **オプション：**パスワードのヒントを入力してください。パスワードを忘れた際に思い出せるように役立ちます。
6. **「有効化」**をクリックしてください。

注意

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管理してください。

7. **オプション：**ロック解除パターンを描いてください。
8. 少なくとも1つのパスワード回復方法を設定してください。

次に実行する操作

ウィザードに従って基本パラメーターを設定してください。

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使用する前に、デバイスにログインする必要があります。

開始前に

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。

手順

1. デバイスを起動します。
2. 右クリックしてショートカットメニューを表示します。
3. 必要に応じて項目を選択します。例えば、「**フルスクリーンを終了**」を選択すると、自動的にログイン画面が表示されます。

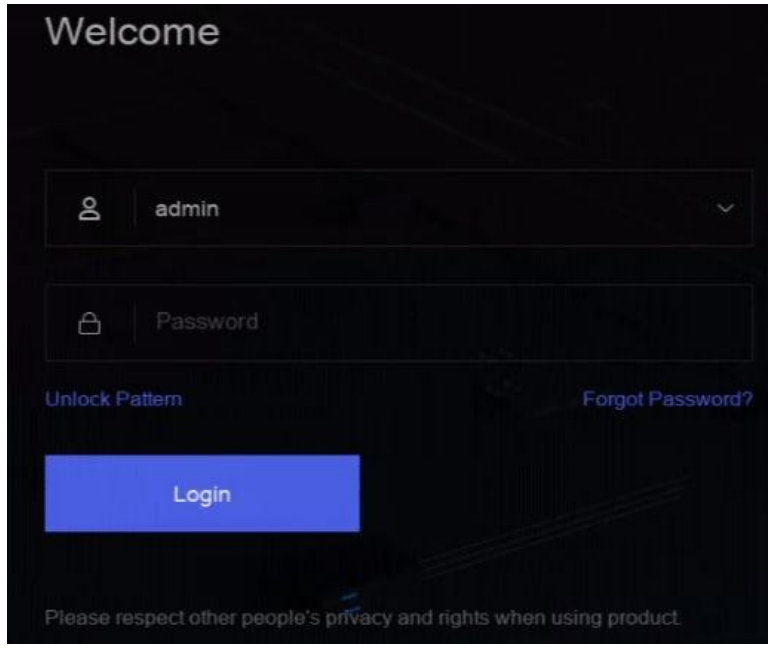


図2-1 ログイン

4. ロック解除パターンを使用してログインするか、ユーザー名とパスワードでログインするには「**パスワードログイン**」をクリックしてください。

注

- アンロックパターンは管理者ユーザーのみ利用可能です。
- アンロック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画面の「**パスワードを忘れた場合**」をクリックしてパスワードをリセットするか、パスワードヒントを使用して思い出してください。

第3章 ユーザーインターフェースの紹介

デバイスを起動すると、ライブビューインターフェースが表示されます。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**」を選択してください。

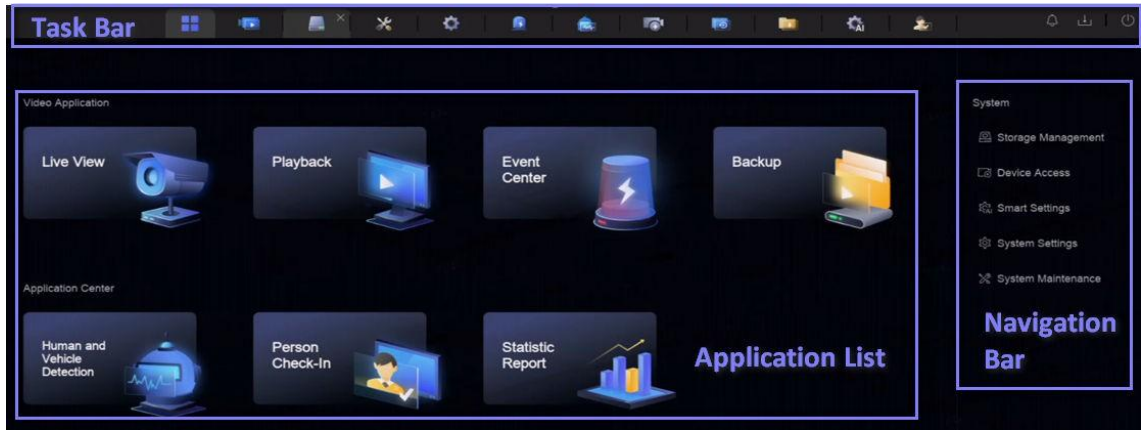


図3-1 メイン機能ページ

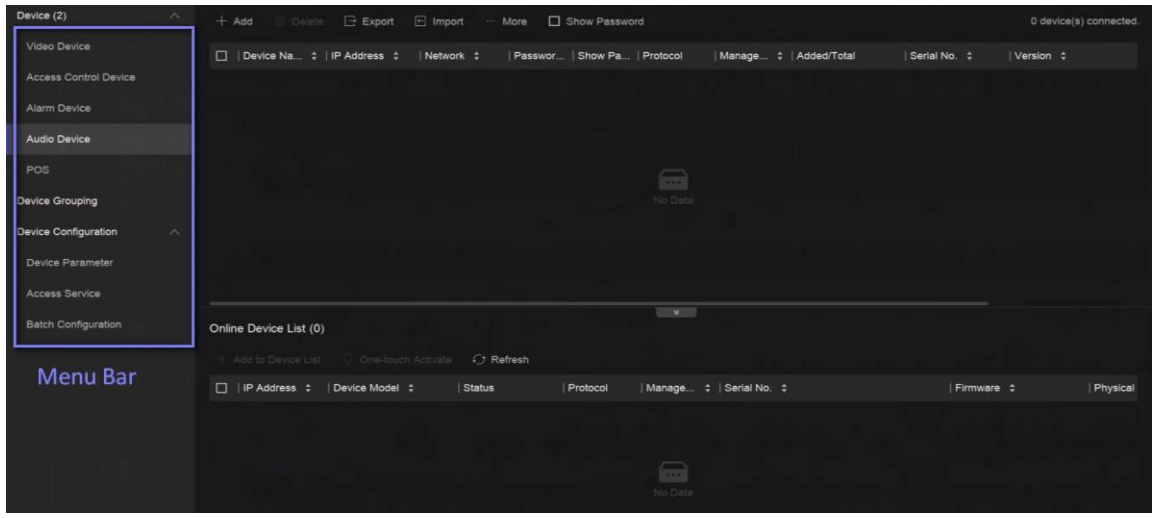


図3-2 メニューバーの例

図3-3 アプリケーションにおける人物と車両の検出例表3-1 インターフェースの概要

インターフェース名	概要
タスクバー	開いているアプリケーションがタスクバーに一覧表示されます。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。 アイコンの説明： • : メインメニュー。 • : イベントセンター。イベントのアラームを検索して表示できます。 • : 各ダウンロードタスクのダウンロード進捗を確認できます。 • : デバイスのシャットダウン、ログアウト、または再起動を行います。
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。クリックすると設定が可能です。
ナビゲーションバー	各システムの機能を設定するには、クリックしてください。
メニューバー	各アプリケーションの設定可能な項目が一覧表示されます。 **注意** **アプリケーションセンター**内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できます。

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、およびネットワークサービスが設定可能です。

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ー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、ネットワークデバイスにアクセスしたりする前に、TCP/IPを適切に設定する必要があります。

手順

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** へ移動します。

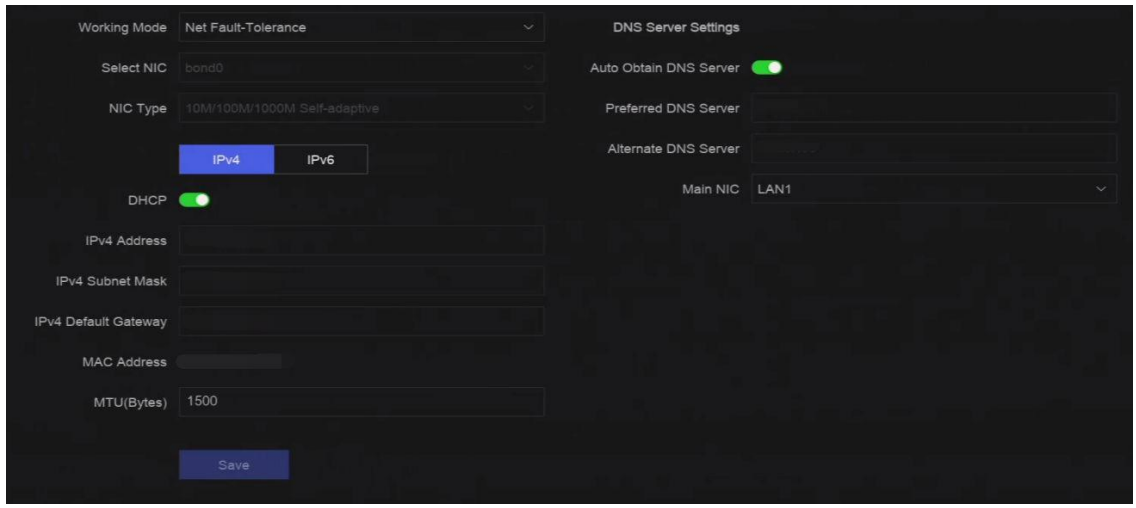


図4-1 TCP/IP設定

2. **動作モード**を設定し、**NICを選択します。マルチアドレス**

2つのNICカードのパラメーターは独立して設定可能です。パラメーター設定時に、NICタイプフィールドで**LAN1**または**LAN2**を選択できます。デフォルトルートとして1つのNICカードを選択できます。その後、システムはエクストラネットに接続され、データはデフォルトルート経由で転送されます。

ネットワーク障害耐性

2つの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**に設定できます。これにより、1つのNICカードが故障した場合、ビデオレコーダーは自動的に別のスタンバイNICカードを有効化し、システムの正常な動作を保証します。

注意

動作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ーを設定します。

- IPv4 DHCP

DHCPサーバーが利用可能な場合、**DHCPを**有効にすることで、そのサーバーからIPアドレスその他のネットワーク設定を自動的に取得できます。

MTU

最大伝送単位（MTU）は、単一のネットワーク取引で送信可能な最大のネットワーク層プロトコルデータ単位のサイズです。

DNSサーバーの自動取得

DHCPが有効になっている場合、**自動取得DNSサーバーを**有効にすると、**優先DNSサーバー**

および**代替DNSサーバーを取得できます**。

- IPv6

ルーター広告

ネットワーク内のルーターがIPv6に対応している場合、このモードをデフォルトとして使用することをおすすめします。

自動

ネットワーク内にDHCPv6対応デバイスが存在する場合、このモードを使用することをおすすめします。

手動設定

IPv6パラメーターを手動で入力する場合、このモードを使用してください。

4. **保存**をクリックしてください。

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、動的なユーザーIPアドレスを固定のドメインネームサーバーにマッピングします。

開始前に

DynDNS、PeanutHull、および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。

手順

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

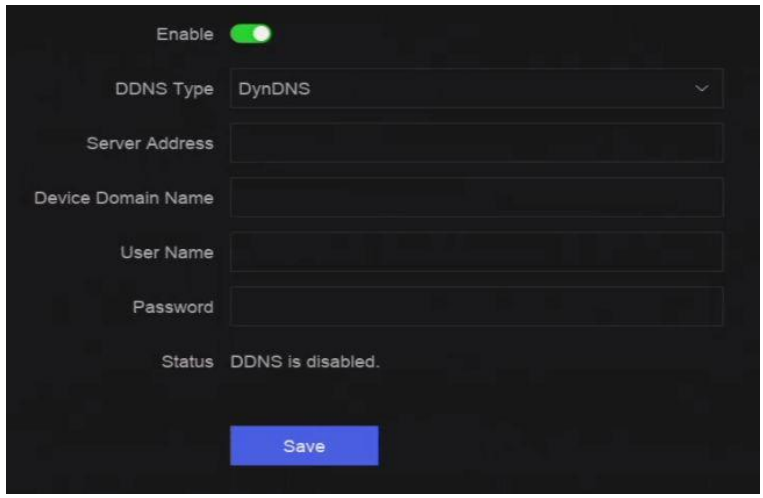


図4-2 DDNS

2. **「有効」**をオンにします。
3. DDNS タイプを選択します。
4. サービスアドレス、ドメイン名など、パラメーターを設定します。
5. **保存**をクリックします。

4.1.3 PPPoEを設定します

デバイスがPPPoE経由でインターネットに接続されている場合、ユーザー名とパスワードを適切に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。

手順

1. **システム→ システム設定→ ネットワーク→ ネットワーク→ PPPoE** へ移動します。

図4-3 PPPoE

2. **「有効」**をオンにします。
3. ユーザー名とパスワードを入力します。
4. **「保存」**をクリックします。

次に実行する操作

システム→ システムメンテナンス→ 実行情報→ ネットワーク状態 に移動し、PPPoEの状態を確認します。

4.1.4 マルチキャストを設定します。

マルチキャストを設定することで、ネットワーク経由で許可されている最大数を超えるカメラのライブビューを有効にできます。

手順

1. **システム→ システム設定→ ネットワーク→ ネットワーク→ その他の設定**。
2. **マルチキャスト**パラメーターを設定します。

注

- ネットワークビデオセキュリティクライアント経由でデバイスを追加する際、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アドレスと一致する必要があります。
- IPv4の場合、Class-D IPアドレス（224.0.0.0から239.255.255.255）が対象となり、239.252.0.0から239.255.255.255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際は、マルチキャストアドレスはデバイスのマルチキャストアドレスと一致する必要があります。

3. **保存**をクリックします。

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て管理するためのモバイルアプリ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可能にします。

手順

1. **システム→ システム設定→ ネットワーク→ Hik-Connect** を選択します。

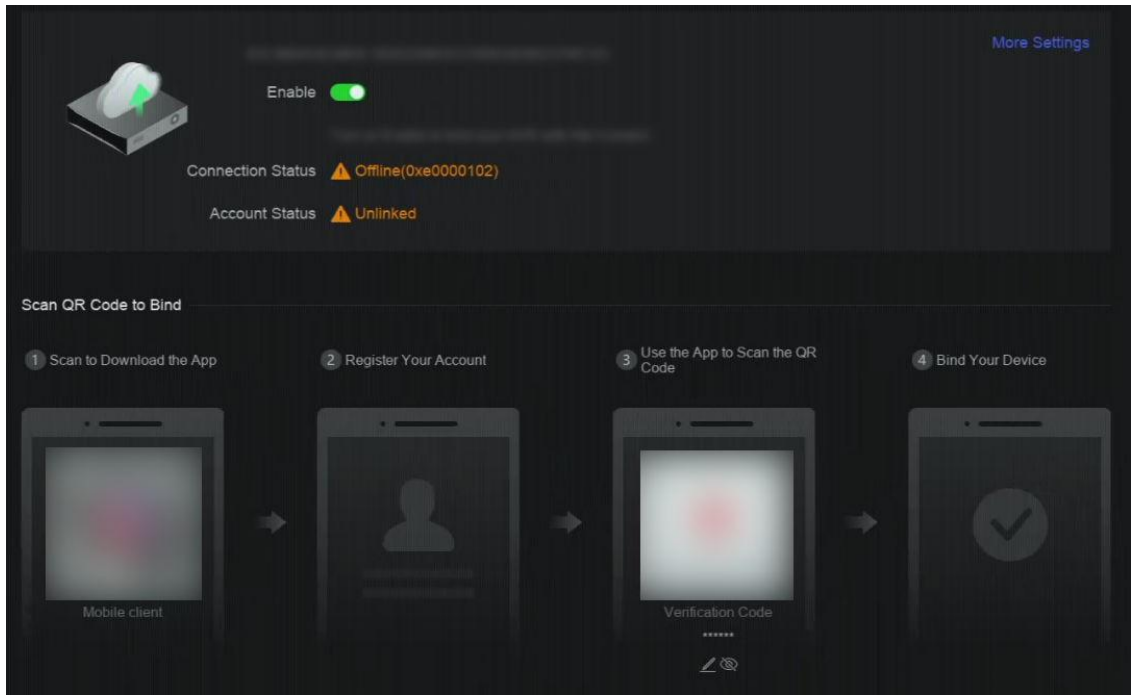


図4-4 Hik-Connect

2. **「有効にする」**をオンにすると、サービス利用規約が表示されます。
3. サービス利用規約に同意してください。
4. Hik-Connect アプリをダウンロードしてください。
   - スマートフォンでQRコードをスキャンし、Hik-Connectアプリをダウンロードしてください。
   - ***https://appstore.hikvision.com*** からアプリをダウンロードしてください。

図4-5 Hik-Connectのダウンロード

5. アプリ内でアカウントを登録してください。
6. **オプション：詳細設定**をクリックし、**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**有効にしたり、**サーバーIPアドレスを**編集したりできます。

   ストリーム暗号化

この機能有効化後、リモートアクセスおよびライブビュー時に検証コードの入力が必要です。

プラットフォーム タイムシンク

デバイスはNTPサーバーではなくHik-Connectと時間を同期します。

適応型ビットレートストリーミング

ネットワーク環境が不良の場合、デバイスは自動的に動画のビットレートを調整し、再生の滑らかさを確保します。

サーバーIPアドレス

Hik-ConnectサーバーのIPアドレスです。

7. 「」をクリックして検証コードを設定してください。

8. Hik-Connectアプリを使用してデバイスのQRコードをスキャンし、デバイスをHik-Connectアカウントに紐付けます。

注意

デバイスが既にアカウントとリンクされている場合、**[リンク解除]** をクリックして現在のアカウントとのリンクを解除できます。

結果

- デバイスがHik-Connectに接続されている場合、**接続状態は「オンライン」**になります。
- デバイスがHik-Connectアカウントとリンクされている場合、**アカウントステータスは「リンク済み」**になります。

次にやるべきこと

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を設定してください。

OTAP（Open Thing Access Protocol）は、パブリックネットワークとプライベートネットワークにおける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を有効にすると、他のアプリケーションがこのプロトコルを介してリモートで動画を閲覧できるようになります。

開始前に

デバイスがOTAP経由でネットワークにアクセス可能であることを確認してください。

手順

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** を選択します。

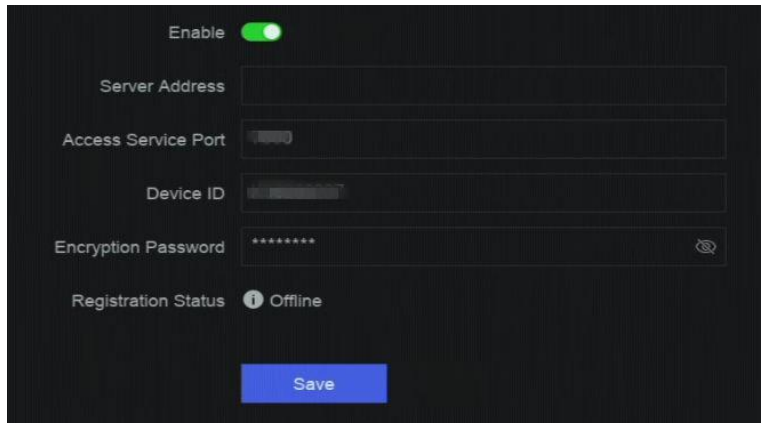


図4-6 OTAP

2. **OTAP を**有効にします。
3. パラメーターを設定します。
4. **保存**をクリックします。

4.2.3 ISUP を設定します。

ISUP（Intelligent Security Uplink Protocol）は、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、さまざまなデバイスにアクセスするためのAPI、ライブラリファイル、コマンドを第三者プラットフォームに提供します。このプロトコルにより、第三者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装できます。

手順

1. **システム**に移動→ **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** .

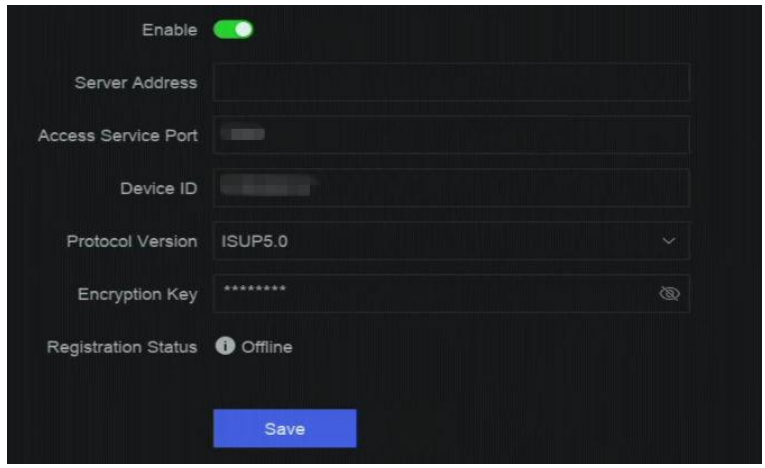


図4-7 ISUP

2. **「有効」**をオンにします。

注

ISUP が有効に設定されると、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ーを設定します。

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のポート番号は、1024から65535の範囲です。実際のポート番号はプラットフォームによって指定されます。

デバイスID

デバイスIDはプラットフォームによって提供されます。

プロトコルバージョン

ISUPプロトコルバージョンは、ISUP 5.0のみが利用可能です。

暗号化キー

ISUP V5.0バージョンを使用する場合、暗号化パスワードが必要です。これにより、デバイスとプラットフォーム間の通信がより安全になります。デバイスをISUPプラットフォームに登録後に、確認のために入力してください。空欄にしたり、「ABCDEF」と入力したりしないでください。

4. **保存**をクリックしてください。

デバイスを再起動後、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 サービスを設定します。

SDK（ソフトウェア開発キット）サービスは、第三者のパートナーが異なる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。

手順

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→ SDK**。

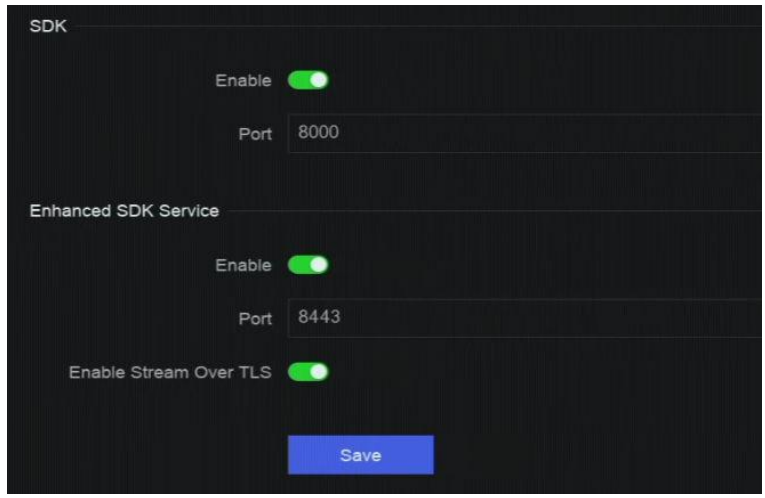


図4-8 SDKサービス

2. 要件に応じて**SDK**と**強化されたSDKサービスを**設定します。

注意

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: TLS 経由のストリームを**有効化します。TLS 暗号化技術を使用したストリーム伝送サービスにより、より安全なストリーム伝送が実現します。
4. **保存**をクリックします。

4.2.5 ISAPI を有効化します。

ISAPI（Internet Server Application Programming Interface）は、HTTPを基盤としたオープンプロトコルで、システムデバイス（例：ネットワークカメラ、NVRなど）間の通信を実現できます。

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→ ISAPI を有効にします。

4.2.6 ONVIFを設定

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。追加されたユーザーアカウントは、ONVIFプロトコル経由で他のデバイスに接続する権限を有します。

手順

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**。

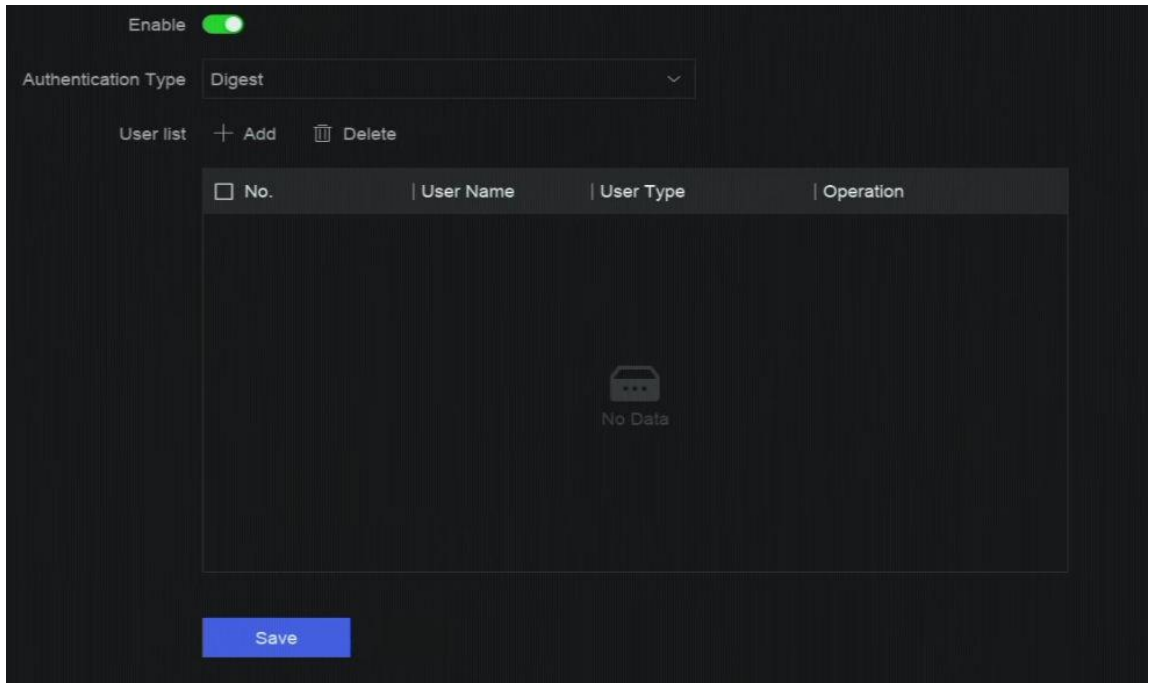


図4-9 ONVIF

2. **「有効」**をオンにします。
3. 認証タイプを選択します。
4. **「追加」**をクリックしてユーザーを追加します。
5. ユーザー名とパスワードを設定します。

注意

製品のセキュリティを強化するため、ご自身で選択した強固なパスワード（8文字以上で、大文字、小文字、数字、特殊文字の少なくとも3つを含む）を設定することを強くおすすめします。また、特に高セキュリティシステムでは、パスワードを定期的に変更することをおすすめします。月次または週次でのパスワード変更は、製品の保護をさらに強化します。

6. **「保存」**をクリックしてください。

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できます。

手順

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→ ログサーバー**。

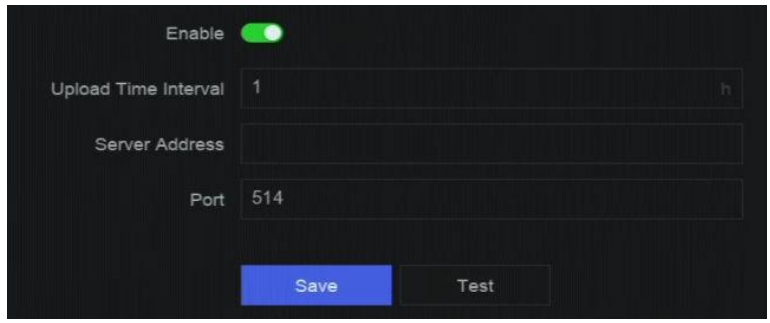


図4-10 ログサーバー

2. **「有効」**をオンにします。
3. **アップロード間隔**、**サーバーのIPアドレス**、および**ポート**を設定します。
4. **オプション：テスト**をクリックしてパラメーターが有効かどうかを確認します。
5. **保存**をクリックします。

4.3 ネットワークサービス設定

4.3.1 HTTP(S)の設定

HTTP（Hyper Text Transfer Protocol）およびHTTPS（Hypertext Transfer Protocol Secure）ポートは、ウェブブラウザ経由の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通信と身分認証を可能にし、リモートアクセスのセキュリティを向上させます。

手順

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)** に移動します。

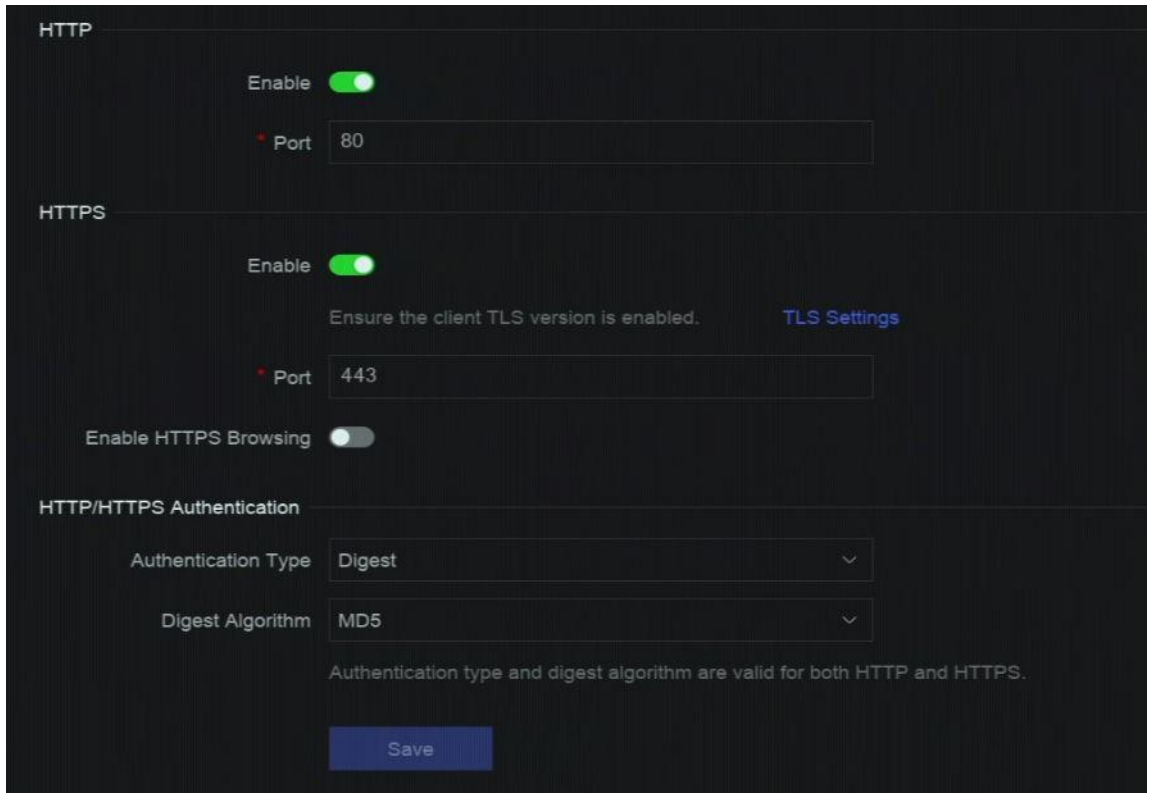


図4-11 HTTP(S)

2. **オプション：**HTTPまたはHTTPSを有効にします。
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**

   セキュリティ上の理由から、2つの認証タイプから選択可能です。セキュリティを優先する場合は、

   Digest を選択することを推奨します。

   ダイジェストアルゴリズム

   Digest アルゴリズムはHTTP/HTTPSを基盤としており、主にユーザー認証のダイジェスト認証に使用されます。
5. **保存**をクリックします。

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の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具体的に保護できます。

手順

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** へ移動します。

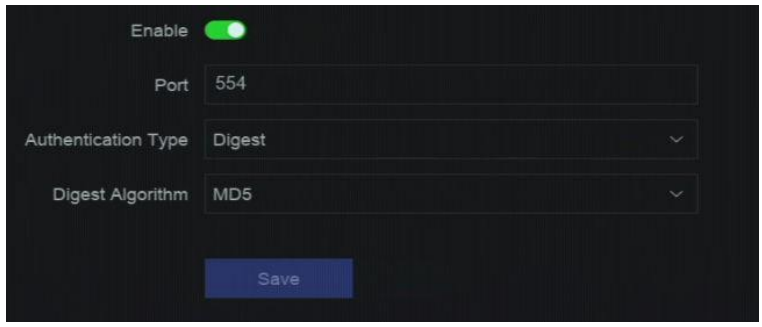


図4-12 RTSP

2. パラメーターを設定します。

ポート

ポートはデフォルトで554です。

認証タイプ

2つの認証タイプから選択可能です。**Digest**を選択した場合、RTSP経由でIPアドレスから動画ストリームにアクセスできるのは、Digest認証を使用したリクエストのみです。セキュリティ上の理由から、認証タイプとして**Digest**を選択することを推奨します。

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を基盤としたもので、ユーザー認証のダイジェスト認証用のアルゴリズムです。

3. **保存**をクリックしてください。

4.3.3 WebSocketの設定

WebSocketプロトコルはTCPを基盤とし、ウェブブラウザとサーバー間の双方向通信を提供することを目的としています。これにより、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可能です。

手順

1. **→→→→システム**に移動し、**システム設定を開きます。 システム設定を開き、システム設定を開きます。 システム設定を開き、システム設定を開きます。 システム設定を開き、システム設定を開きます。 システム設定を開き、システム設定を開きます。 システム設定**

2. **有効にするを**オンにします。

3. **ポート**を設定します。

4. **保存**をクリックします。

4.3.4 ポートマッピングの設定 (NAT)

リモートアクセスをクロスセグメントネットワーク経由で実現するための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つの方法が提供されています。UPnP™ は、ネットワーク上の他のネットワークデバイスを自動的に検出し、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経由でデバイスをWANに高速接続できます。

開始前に

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内に配置する必要があります。

手順

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** へ移動します。

図4-13 ポートマッピング（NAT）

2. **「有効」**をオンにします。
3. **マッピングモード**を設定します。**自動**

   ポートマッピング項目は読み取り専用であり、外部ポートはルーターによって自動的に設定されます。

   手動

   外部ポートを手動で編集できます。
4. **マッピング モードが手動**に設定されている場合、対応するポートを編集するには「」をクリックします。

注

- RTSP ポート番号の値は 554 または 1024 から 65535 の範囲内である必要があります。その他のポートの値は 1 から 65535 の範囲内であり、各ポートの値は互いに異なる必要があります。同じルーターの下で UPnP™ 設定が複数のデバイスに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ある必要があります。
- **外部ポートは、**ルーターで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**をクリックします。

次にやるべきこと
ルーターの仮想サーバー設定ページに移動し、内部/外部ソースポートの空白に内部/外部ポート値を入力し、その他の必要な内容を記入します。

4.3.5 IoTを設定します

NVRがセキュリティ制御パネルから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。

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→ IoT を選択し、機能を有効化し、ポート番号を設定します。

注意
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一致する必要があります。

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用意されています。管理者のユーザー名は「**admin**」です。管理者はユーザーを追加、削除、編集する権限を有します。ゲストとオペレーターユーザーは限定された権限のみを有します。

システム→ システム設定→ ユーザー管理 .

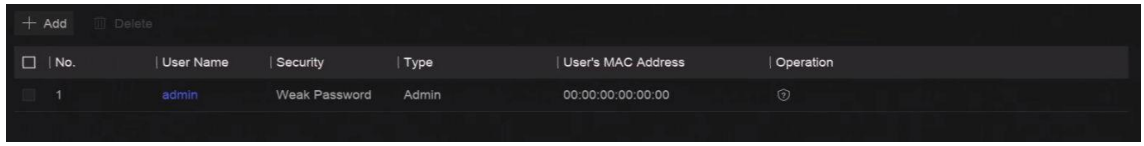


図5-1 ユーザー管理 表5-1 アイコン/ボタン説明

アイコン/ボタン	説明
	アカウントのセキュリティを設定します。
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

操作を行う前に、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、アクセス制御装置、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、実際のデバイスをご確認ください。

6.1 ビデオデバイスへのアクセス

ビデオデバイスにアクセスする方法はいくつかあります。

6.1.1 自動的に検索されたオンラインネットワークカメラを追加する

同じネットワークセグメント内のネットワークカメラは、自動的に検索され、デバイスに追加されます。

手順

1. **システム→ デバイスアクセス→ デバイス→ ビデオデバイス→ オンラインデバイス一覧** へ移動します。

2. リストからデバイスを選択します。

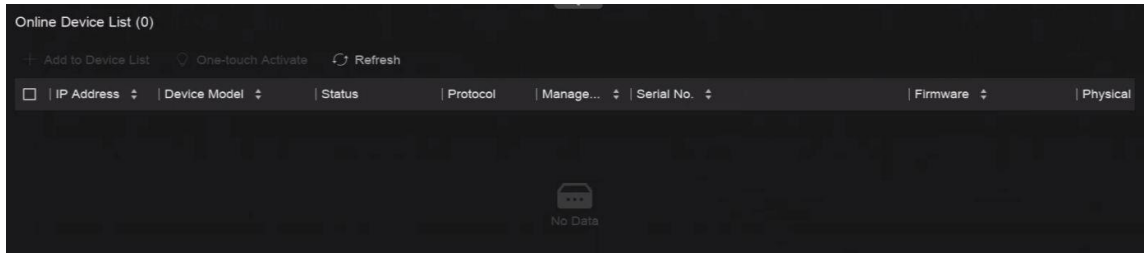


図6-1 自動的に検出されたオンラインネットワークカメラの追加

3. **「デバイス一覧に追加」**をクリックします。

注

- デバイスはデフォルトのパスワードを使用してネットワークカメラを追加します。カメラのパスワードがデフォルトのパスワードと一致していることを確認してください。デフォルトのパスワードは**「設定」→「デフォルトパスワード設定」**で設定できます。
- 検索したネットワークカメラがアクティブでない場合、デバイスはデフォルトのパスワードを使用して非アクティブなネットワークカメラをアクティブ化し、追加します。デフォルトのパスワードは**「詳細」**

  →デフォルトパスワード設定で設定できます。
- ネットワークカメラが正常に追加されると、そのステータスは**「オンライン」**になります。
- デバイス名をクリックすると、そのパラメーターを追加できます。

6.1.2 ネットワークカメラを手動で追加する

ネットワークカメラをビデオレコーダーに手動で追加します。

開始前に

- 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接続されてい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有効になっていることを確認してください。

手順

1. **システム→ デバイスアクセス→ デバイス→ ビデオデバイス** を選択します。

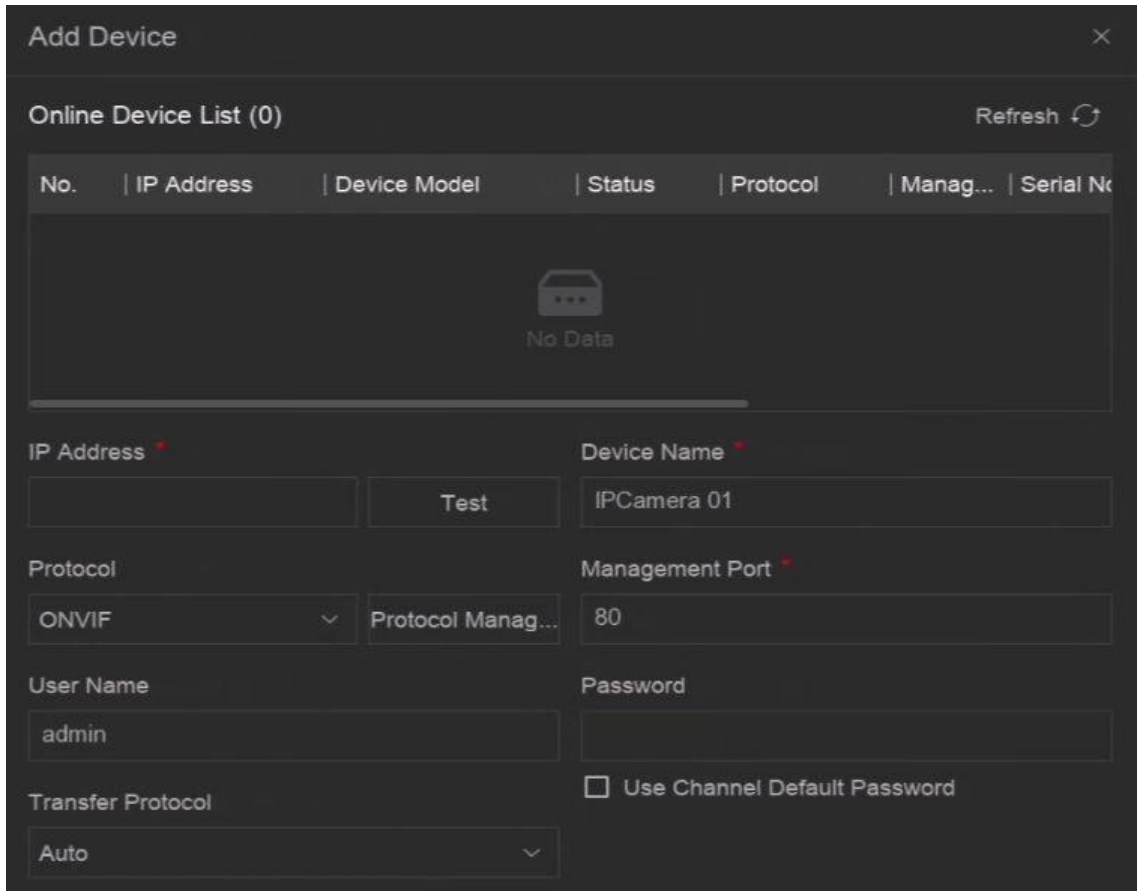


図6-2 ネットワークカメラを手動で追加

2. **「追加」**をクリックします。
3. ネットワークカメラのパラメーターを入力します。

チャンネルのデフォルトパスワードを使用する

この設定が有効になっている場合、ビデオレコーダーは設定されたチャンネルのデフォルトパスワードを使用してカメラを追加します。

詳細設定

「証明書を確認」を有効にすると、証明書を使用してカメラを検証できます。証明書はカメラの識別手段であり、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際は、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、**[続行]**をクリックして**[追加]**をクリックします。
5. **「追加」**をクリックします。

6.1.3 PoE経由でネットワークカメラを追加

PoE（Power over Ethernet）対応のネットワークカメラは、背面パネルのPoEインターフェー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対応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。詳細については、*「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プロトコルを使用してソーラーパワーカメラを追加する

ソーラー電源カメラは、OTAPプロトコルを使用してデバイスに追加できます。

開始前に

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

タスクのコンテキストを入力してください（任意）。

手順

1. **システム**に移動し、→を選択します**。デバイス アクセス→ デバイス設定→ アクセス サービス→ OTAP サービス**。
2. **有効にするを**オンにします。
3. OTAP **サーバー 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 パラメーターが設定されると、OTAP プロトコル経由で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。
5. ウェブブラウザ経由でソーラーパワーカメラのOTAPプロトコルパラメーターを設定します。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。

注意

ソーラー電源カメラのOTAPプロトコルパラメーターは、デバイスと同一にする必要があります。

6. デバイスに太陽光発電式カメラを追加してください。
   - **「自動追加IPカメラ」を**有効にしている場合、OTAPプロトコル経由で新規に接続されたネットワークカメラは自動的にデバイスに追加されます。
   - **オンラインデバイス一覧から**太陽光発電カメラを選択し、**クイック追加**をクリックします。
7. **システム→ デバイスアクセス→ デバイス→ ビデオデバイス**を選択し、**プロトコルをOTAPに設定**し、**追加**をクリックします。

次にやるべきこと

- 太陽電池式カメラをデバイスに追加すると、カメラを起動、バッテリー残量を確認、ライブ動画を視聴、ウェブブラウザ経由で設定を調整するなど、さまざまな操作が可能です。
- カメラにANR（自動ネットワーク補充）を設定します。詳細については*「録画スケジュールの設定」*を参照してください。

6.1.5 カスタムプロトコルを使用してネットワークカメラを追加する

標準プロトコルを使用していないネットワークカメラの場合、カスタムプロトコルを設定して追加できます。システムでは8つのカスタムプロトコルが提供されています。

開始前に

- 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てください。
- 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。

手順

1. **システム**に移動し、**→デバイスアクセス、→デバイス、→ ビデオデバイスを選択します**。
2. **「詳細」**をクリックし、**「→ カスタムプロトコル管理」**を選択するか、**「→ プロトコル管理」を追加します**。

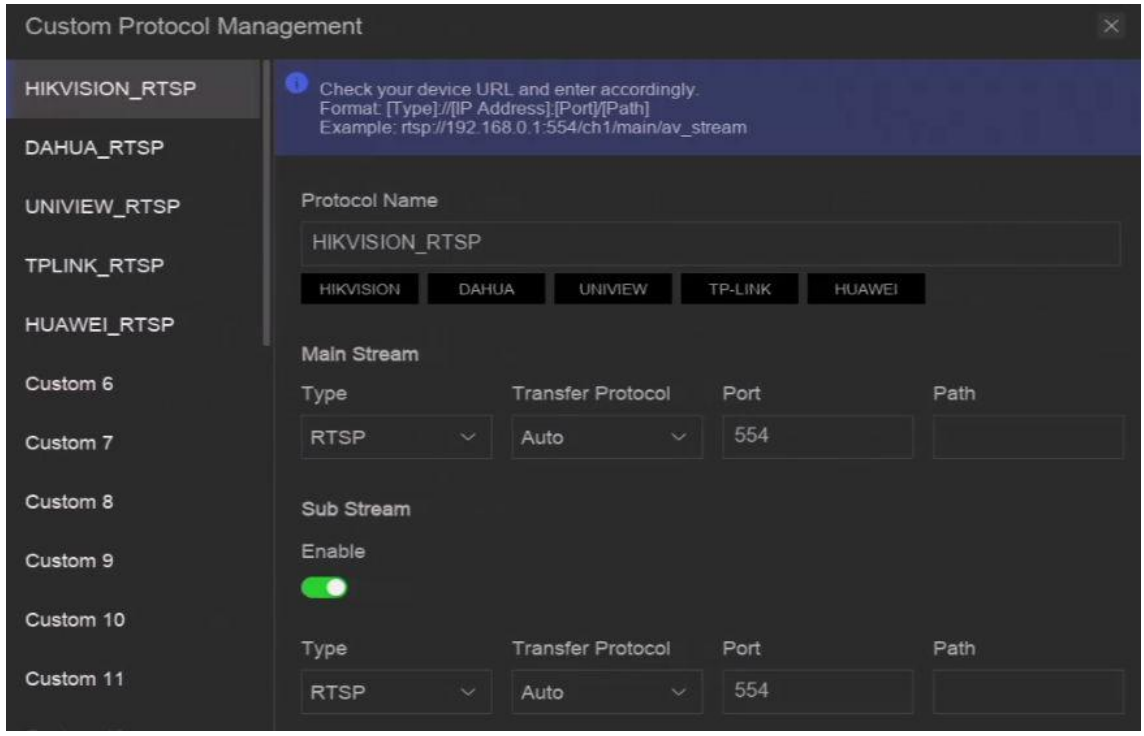


図6-3 カスタマイズされたプロトコルを使用してネットワークカメラを追加

3. 左側でプロトコルタイプを選択します。
4. プロトコルパラメーターを設定します。

タイプ

カスタム プロトコルを採用するネットワーク カメラは、標準の RTSP 経由でストリームを取得できる必要があります。

転送プロトコル

3種類から選択可能です：**Auto**、**UDP**、**およびRTP Over RTSP**。**ポート**

RTSP ストリーミング用のポート番号です。デフォルト値は 554 です。

パス

ネットワークカメラの製造元に、メインストリームとサブストリームのURLを確認してください。一般的な形式は *[Type]://[IP アドレス]:[ポート]/[リソースパス]* です。例：*rtsp://192.168.0.1:554/ch1/main/av_stream*。

注意

- プロトコル名**とパスは**、以下のブランド名をクリックすると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に対応していない場合、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**をクリックしてください。
6. **システム→ デバイスアクセス→ デバイス→ ビデオデバイスを**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経由でネットワークカメラを追加する

追加したネットワークカメラの情報（IPアドレス、ポート、管理者のパスワードなど）をエクスポートできます。エクスポートしたカメラ設定ファイルの内容は、コンピュータ上で編集可能です。編集後、ファイルを他のデバイスにインポートすることで、ファイル内のカメラを追加できます。

開始前に

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

手順

1. **システム→ デバイス アクセス→ デバイス→ ビデオ デバイス** .
2. USB フラッシュドライブに保存された設定ファイルをインポートするには、**[インポート]** をクリックします。
3. フォルダーのパスを設定します。
4. **「確認」**をクリックします。

6.2 アクセス制御デバイスを追加します

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。追加手順は「*アクセスビデオデバイス*」と類似しています。

6.3 セキュリティコントロールパネルを追加

手順

1. **システム**に移動し、**→デバイス、→デバイス、→セキュリティコントロールパネルを選択します**。
2. **「追加」**をクリックします。
3. **オプション:** プロトコルを選択してください。
4. デバイスのIPアドレス、名前、およびIoTサービスポートを入力してください。
5. **オプション：** プロトコルタイプとして**OPTEX**を選択した場合、転送プロトコルを選択してください。
6. **オプション：** 操作列の「」をクリックして、文字エンコード、オーバーレイモード、フォントサイズなどのOSDパラメーターを設定します。

注意

リンクされたチャンネルは編集できません。リンクされたチャンネルを編集するには、**イベントセンター →→ → イベント設定 →→ → イベント設定 → セキュリティコントロールパネル → イベント**に移動してください。

設定した OSD 情報は、動画画像に表示されます。

6.4 オーディオデバイスを追加

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

追加手順は「***Access Video Device***」と類似しています。ビデオチャンネルをIPスピーカーとリンクすると、その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すると、そのマイクはリンクされたビデオチャンネルの音声入力として動画記録に使用されます。

6.5 POSデバイスの追加

一部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。このデバイスは、POSマシン/サーバーから取引メッセージを受信し、動画画像に取引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できます。

手順

1. **システム**に移動し、**→デバイスアクセス、→デバイス、→POSを選択します**。
2. **「追加」**をクリックして POS デバイスを追加します。

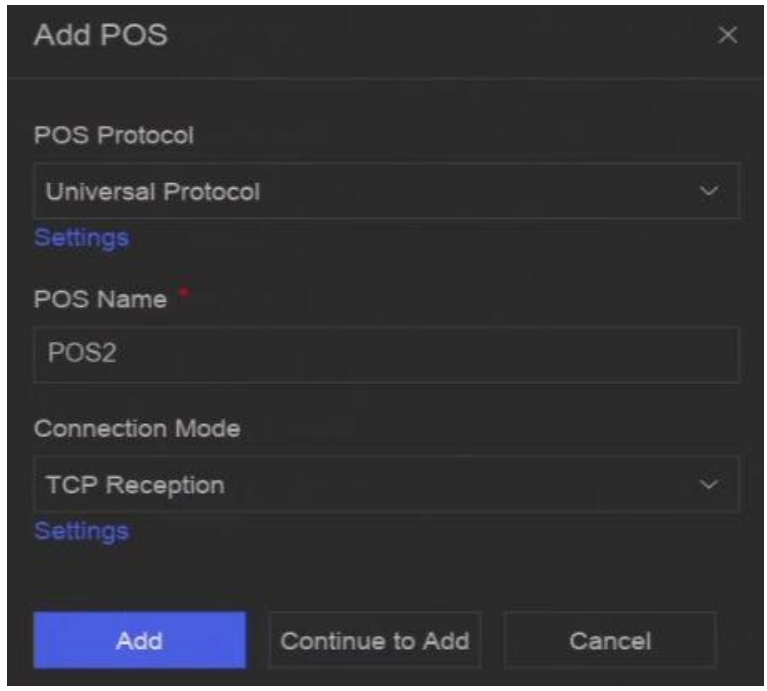


図6-4 POS デバイスを追加

3. POS デバイスのパラメーターを設定します。

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、終了行タグを設定できます。また、文字の大文字小文字区別プロパティを設定できます。オプションでフィルタリング識別子とXMLプロトコルを選択できます。

EPSON

EPSONプロトコルでは、固定の開始行タグと終了行タグが使用されます。

AVE

固定の開始ラインタグと終了ラインタグは、AVEプロトコルで使用されます。シリアルポートと仮想シリアルポートの接続タイプがサポートされています。

NUCLEUS

固定の開始行と終了行のタグはAVEプロトコルで使用されます。シリアルポートと仮想シリアルポートの接続タイプがサポートされています。RS-232接続通信では、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、ポート番号は1から65535の範囲で設定し、各POSマシンごとにポート番号をユニークに設定する必要があります。

UDP接続

UDP接続を使用する場合、ポート番号は1から65535の範囲で設定する必要があります。また、各POS端末のポート番号は一意である必要があります。

USBからRS-232への接続

USB-RS-232変換器のポートパラメーターを設定します。これには、ポートシリアル番号、ボーレート、データビット、ストップビット、パリティが含まれます。

RS-232接続

デバイスとPOSマシンをRS-232経由で接続します。

マルチキャスト接続

マルチキャストプロトコルを使用してデバイスとPOSマシンを接続する場合、マルチキャストアドレスとポートを設定します。

スニフ接続

デバイスとPOS端末をSniff経由で接続します。ソースアドレスとデスティネーションアドレスの設定を行います。

4. **「追加」**をクリックします。

注意

POSデバイスを追加した後、 **をクリックして、**POSテキストオーバーレイを設定できます。

6.6 チャンネル管理

ビデオデバイスを追加した後、そのチャンネル番号とチャンネル名を確認し、パラメーターを管理できます。この機能は、複数のチャンネルを含むビデオデバイスに対して主に使用されます。

システムに移動し、**→デバイスアクセス→ を選択し、**ビデオデバイスのチャンネルを管理するチャンネルを選択します。

第7章 デバイスグループ化

追加されたデバイスは、異なるカスタムグループに分類できます。

手順

1. **システム**に移動し、**→**、**デバイスアクセス**、**→**、**デバイスグループ化を選択します**。

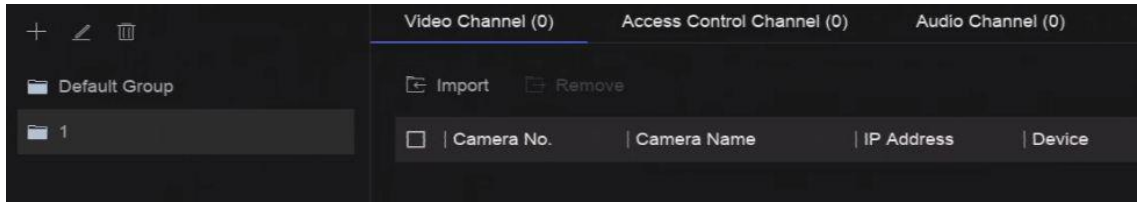


図7-1 デバイスグループ化

2. 「＋」をクリックしてグループを追加します。

注

グループを追加した後、クリックできます / をクリックして編集/削除できます。

3. **「インポート」**をクリックして、選択したグループにチャンネルを追加します。

第8章 ビデオまたはオーディオデバイスの設定

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

8.1 H.265 ストリームへのアクセスを有効にする

デバイスは、IPカメラ（H.265動画形式に対応しているもの）への初回アクセス時に、自動的にH.265ストリームに切り替わります。

手順

1. **システム→ デバイスアクセス→ デバイス→ ビデオデバイス** を選択します。
2. **「詳細」**をクリックし、**「→」→「Auto Switch to H.265」**を選択します。
3. この機能を有効にします。
4. **「保存」**をクリックします。

8.2 ディスプレイ設定の構成

OSD（画面表示）設定、画像設定、露出設定、昼夜切り替え設定などを行います。

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ー→ ビデオデバイス → ディスプレイ設定。カメラを選択し、ご希望の設定を行います。

OSD設定

カメラのOSD（画面表示）設定（日付/時刻、カメラ名など）を設定します。

画像設定

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

露出時間

カメラの露出時間を設定します（1/10000秒から1秒）。露出値が大きいほど、画像が明るくなります。

昼/夜切り替え

カメラは、周囲の照明条件に応じて、昼、夜、または自動切替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（WDR）を0から100の範囲で設定します。周囲の照明と被写体の明るさに大きな差がある場合、WDR値を設定してください。

画像強化

画像のコントラストを最適化して強化します。

8.3 ビデオパラメーターの設定

ビデオパラメーターは、ライブビュー画像と記録ファイルに影響を与えます。

システム→ デバイス アクセス→ デバイス 設定→ デバイス パラメーター→ ビデオ デバイス → ビデオ パラメーター。カメラを選択し、ご希望の設定を行います。

メインストリーム

メインストリームは、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であり、動画の品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して、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高品質な動画を提供します。

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2つ目のコーデックです。これにより、直接記録の品質を犠牲にすることなく、インターネットの送信帯域幅を削減できます。サブストリームは、スマートフォンアプリでライブ動画を視聴するために主に使用されます。インターネット速度が限られているユーザーはこの設定から最も恩恵を受ける可能性があります。

解像度

画像の解像度は、デジタル画像が保持できる詳細の量を示す指標です。解像度が高いほど、詳細のレベルが高くなります。解像度は、ピクセルの列数（幅）とピクセルの行数（高さ）の組み合わせで指定されます。例えば、1024 × 768 などです。

ビットレートタイプ

ビットレート（kbit/sまたはMbit/s）は「速度」と呼ばれることがありますが、実際には時間単位あたりのビット数を表し、距離単位あたりの時間ではありません。可変と定数の2種類があります。

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します。動画ストリームに動きがある場合、フレームレートが高いほど、画像品質を維持できます。

Iフレーム間隔

I-フレーム（イントラピクチャーとも呼ばれる）は、MPEGの動画圧縮技術であるGOP（グループオンピクセル）の最初のフレームです。圧縮後の画像として表示可能です。I-フレーム間隔は、連続する2つのI-フレーム間のフレーム数です。

8.4 プライバシーマスクの設定

プライバシーマスクは、ライブビューまたは録画時に画像の一部をマスク領域で隠すことで、個人情報を保護します。

手順

1. **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ー→ ビデオデバイス → プライバシーマスク**。

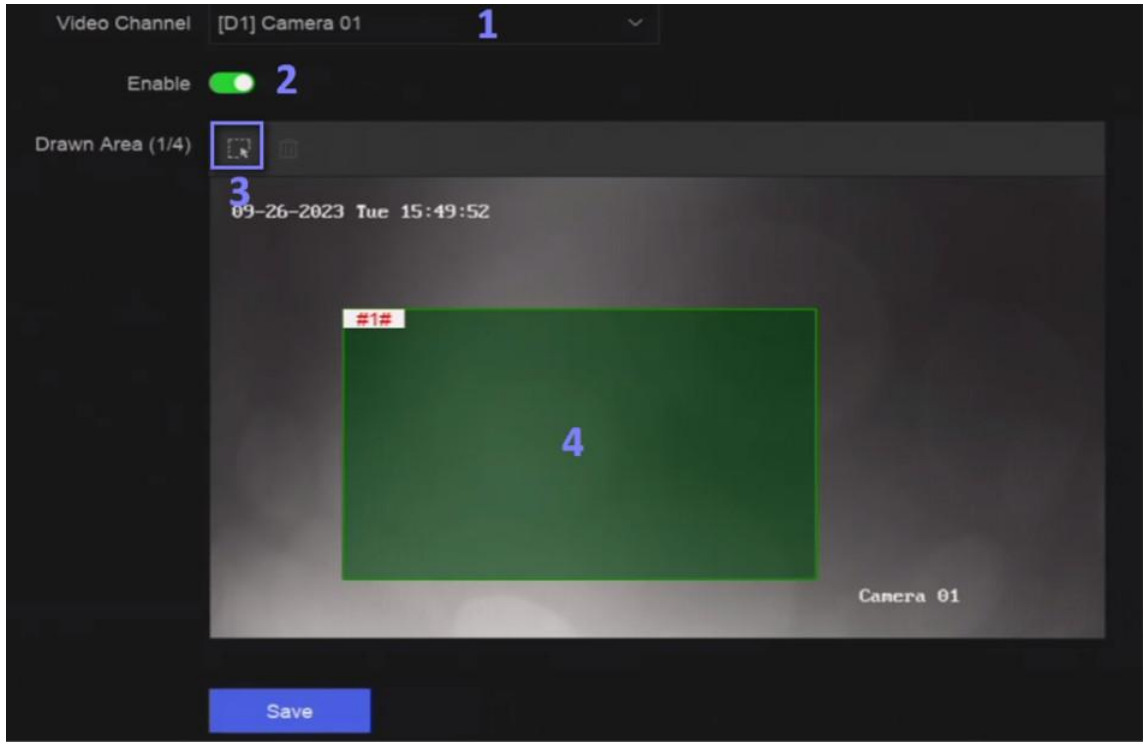


図8-1 プライバシーマスク

2. カメラを選択します。

3. **「有効」**をオンにします。

4. プレビュー ウィンドウに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、各領域のサイズを調整できます。

5. **保存**をクリックしてください。

8.5 プライバシー保護の設定

この機能は、動画映像内の特定の領域（人間の顔、人体、車両など）を自動的にぼかしたり、隠したりすることで、個人情報の保護や機密情報の保護を実現します。

開始前に

この機能はカメラでサポートされている必要があります。

手順

1. **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ー→ ビデオデバイス → プライバシー保護** を選択します。

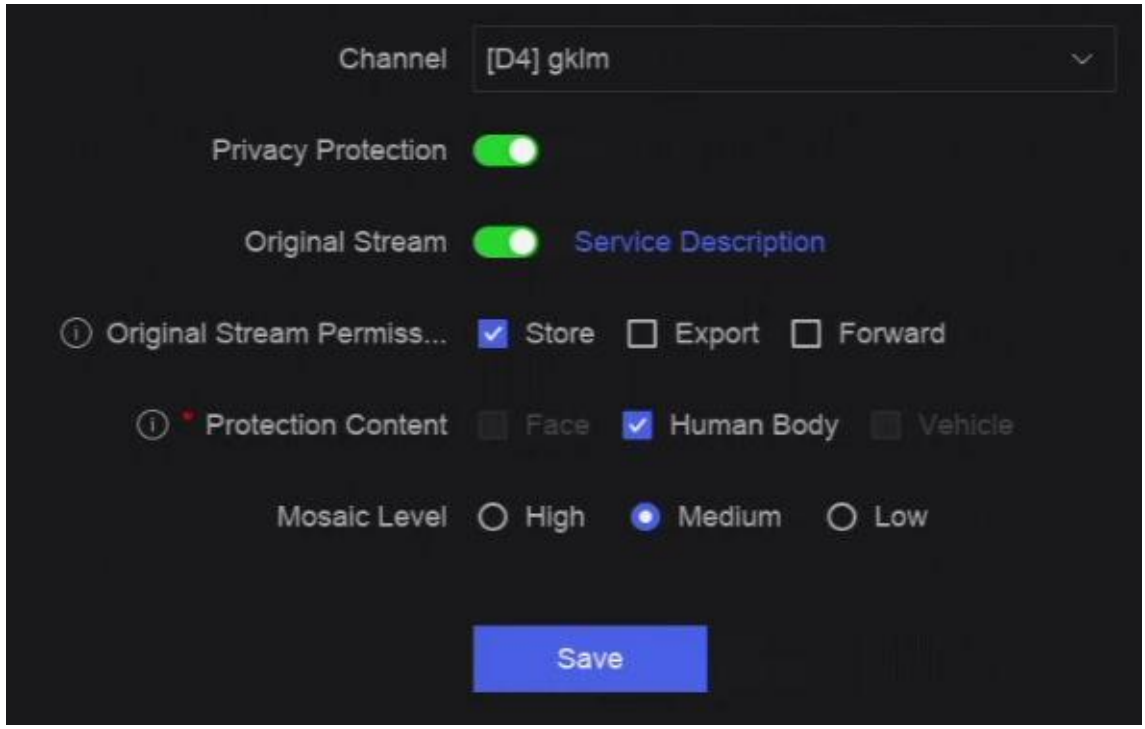


図8-2 プライバシー保護

2. カメラを選択してください。
3. **プライバシー保護を**有効にします。
4. **オプション：オリジナルストリームを**有効にし、ストリームの権限を設定してください。

注意

オリジナルストリームとは、モザイク処理が施されていない動画ストリームを指します。

保存

オリジナルストリームを保存できます。オリジナルストリームを保存すると、ストレージ容量が増加するか、チャンネルの録画保存期間が短縮されます。オリジナルストリームのビットレートはカメラと同じで、設定できません。

エクスポート

チャンネルのオリジナルストリームをエクスポートできます。

転送

元のストリームを転送できます。

注意

エクスポートおよび/または転送の権限を確認する前に、ストアの権限を確認してください。

5. **保護コンテンツ**を設定します。選択した保護コンテンツは、ライブビューと再生時にぼかされます。
6. **モザイクレベル**を設定します。レベルが高いほど、対象画像のぼかしが強くなります。
7. **保存**をクリックします。

8.6 オーディオパラメーターの設定

→オーディオデバイスを追加した後、**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ー → オーディオデバイスで**パラメーターを設定できます。例えば、IPスピーカーを追加した場合、その名前、オーディオ出力音量、オーディオ品質を設定できます。

8.7 OTAP サービスを設定します。

OTAP（Open Thing Access Protocol）は、パブリックネットワークとプライベートネットワークにおける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を有効にすると、他のアプリケーションがこのプロトコルを介してリモートで動画を閲覧できるようになります。

開始前に

デバイスがOTAPプロトコル経由でネットワークにアクセス可能であることを確認してください。

手順

1. **システム→ デバイスアクセス→ デバイス設定→ アクセスサービス→ OTAPサービス**。

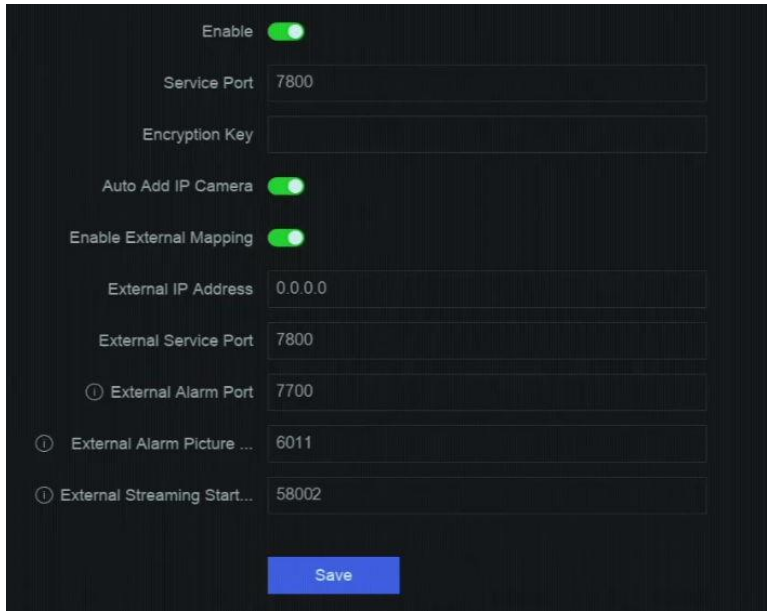


図8-3 OTAPサービスの設定

2. **「有効」**をオンにします。
3. パラメーターを設定します。
4. **保存**をクリックします。

8.8 バッチ設定

接続されたデバイスをバッチで設定できます。

手順

1. **システム→ デバイス アクセス→ デバイス 構成→ バッチ 構成** .

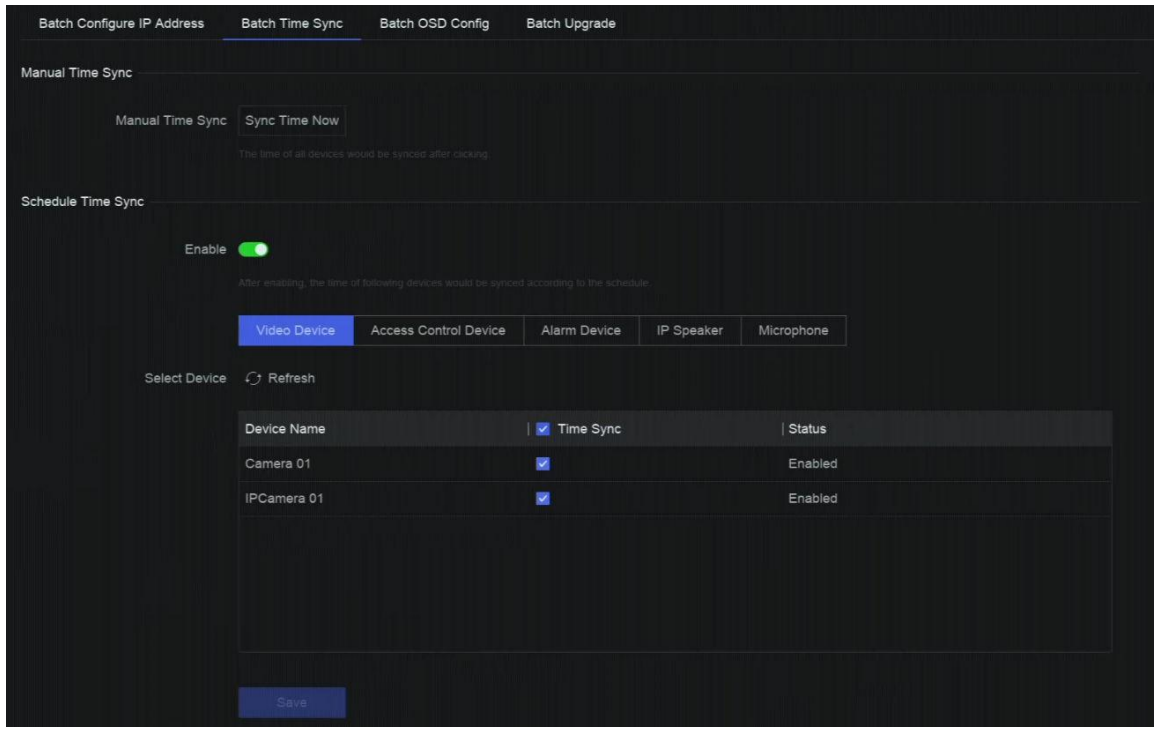


図8-4 バッチ設定

2. IP アドレス、時間同期、OSD、またはファームウェアのアップグレードを必要に応じて設定します。

手動時間同期

「Sync Time Now」をクリックして、接続されているすべてのデバイスの時間を手動で同期します。この操作は一度だけです。

スケジュールされた時間同期

レコーダーは、選択したデバイスの時間を固定されたスケジュールに従って同期します。

3. IPアドレスの設定と時刻同期を行うには、**[保存]** をクリックします。

8.9 PoE（Power over Ethernet）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デバイスに電気電源とデータを転送する機能を提供します。また、PoEインターフェースはプラグアンドプレイ機能に対応しています。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、そのインターフェースをオンラインデバイスへの接続にも使用できます。

開始前に

NVRがPoE機能に対応していることを確認してください。

手順

1. **システム→ デバイスアクセス→ デバイス設定→ PoE** へ移動します。
2. 必要に応じて、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. デバイス種類を**IPスピーカー**または**カメラ**を選択してください。
4. PoEカメラをPoEインターフェースで接続する場合、ネットワークケーブルの接続距離を選択してください。

   長距離

   PoE インターフェース経由で 100 ～ 300 メートルの長距離ネットワーク伝送。

   短距離

   PoE インターフェース経由の短距離（100 メートル未満）ネットワーク伝送。

注意

- PoEインターフェースは、デフォルトで短距離モードが有効になっています。
- PoE経由で長距離ネットワークケーブル（100～300メートル）に接続されたIPカメラの帯域幅は、6MPを超えてはなりません。
- 許可される最大長ネットワークケーブルは、IPカメラのモデルやケーブルの材質によっては300メートル未満になる場合があります。
- 伝送距離が100～250メートルに達した場合、PoEインターフェースに接続するには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250～300メートルに達した場合、PoEインターフェースに接続するには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**をクリックしてください。

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インターフェースの状態と電源状態を確認できます。

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、使用前に初期化する必要があります。HDD管理インターフェースを通じて、HDDのフォーマット、データベースの修復、およびHDDの状態を確認できます。

開始前に

HDDがデバイスに正しく接続されていることを確認してください。

手順

1. **システム→ ストレージ管理→ ストレージ HDD→ ストレージ HDD** を選択します。

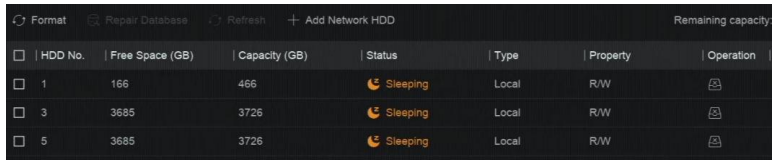


図9-1 HDDの管理

2. **オプション:** 必要に応じて以下の操作を実行してください。

ネットワーク HDD の追加	NASまたはIP SANを追加します。
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。アップグレード後にシステム速度の向上が期待できます。

注意

- 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、修復中はローカルでの検索や再生機能が利用できません。ただし、ウェブブラウザやクライアントソフトウェアなど経由でリモートから検索や再生機能を利用することは可能です。
- プロセス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/取り付け。

9.2 RAID構成

ディスクアレイは、複数の物理的なディスクドライブを単一の論理ユニットに統合するデータストレージ仮想化技術です。RAID（Redundant Array of Independent Disks）とも呼ばれるアレイは、複数のHDDにデータを分散して格納し、1つのディスクが故障した場合でもデータを復旧できる十分な冗長性を提供します。データは

複数の方法（RAIDレベル）でドライブに分散されます。これは、必要な冗長性とパフォーマンスに応じて選択されます。

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利用可能です。同じモデルと容量のHDDを使用することをおすすめします。

RAIDを作成する方法は2つあります。ワンタッチ作成の場合、デフォルトのRAIDタイプはRAID5です。手動作成の場合、RAID0、RAID1、RAID5、RAID6、およびRAID10を設定できます。

表9-1 各RAIDタイプごとのHDD要件

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

注

- この機能は特定のモデルでのみ利用可能です。
- アレイ例外イベントが発生した場合、対応するリンク動作は **システム→ システム設定→ 例外で設定できます**。

9.2.1 ディスクアレイの作成

アレイモードを有効にした後に、ディスクアレイを作成できます。

開始前に

- **ストレージモードは、システム→ ストレージ管理→ ストレージモードで「クォータ」**に設定されています。
- デバイスに十分な数のHDDが正しくインストールされています。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す。

手順

1. **システム→ ストレージ管理→ ストレージ HDD→ アレイ管理** に移動します。
2. **「アレイモードを有効にする」**をクリックするか、**アレイモードを**有効にします。

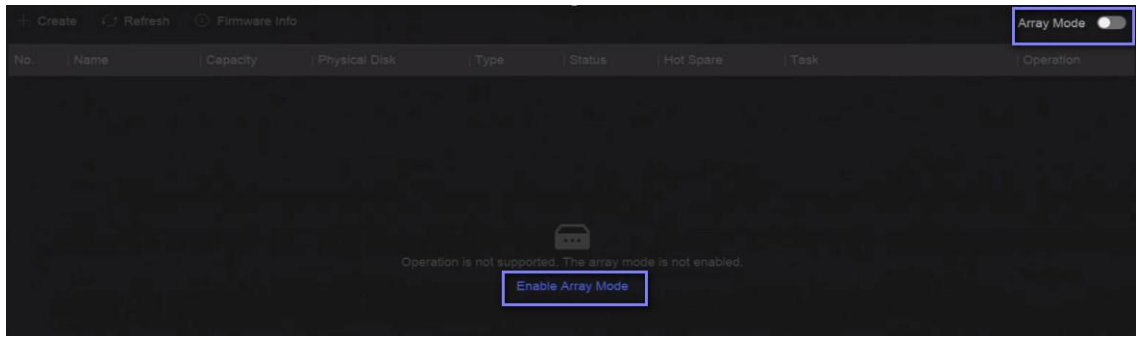


図9-2 RAIDを有効にする

3. デバイスが再起動するまで待ちます。

4. **システム→ ストレージ管理→ ストレージ HDD→ アレイ管理**を再度選択します。

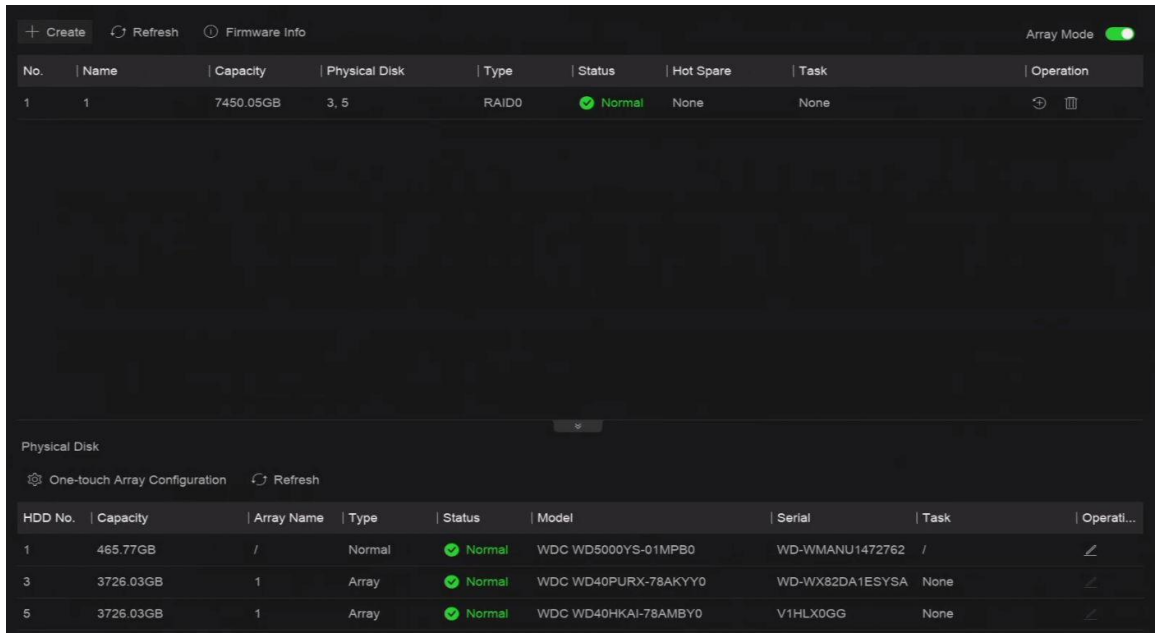


図9-3 アレイ管理

5. アレイを作成します。

作成方法	説明
ワンタッチ アレイ構成	**ワンタッチ配列構成**をクリックします。 **注意** ワンタッチ設定で作成される配列のタイプは、デフォルトでRAID 5です。
手動作成	**「作成」**をクリックして、RAID 0、RAID 1、RAID 5、RAID 6、またはRAID 10アレイを手動で作成します。

9.2.2 アレイの再構築

アレイの状態には、**機能正常**、**機能低下**、および**オフライン**が含まれます。アレイに格納されたデータの高度なセキュリティと信頼性を確保するため、アレイの状態に応じて適切なメンテナンスを速やかに実施してください。

手順

1. **システム→ ストレージ管理→ ストレージ HDD→ アレイ管理** へ移動します。

2. アレイを再構築します。

表9-2 再構築方法

再構築方法	説明
自動再構築	アレイ内にホットスペアディスクが存在し、その容量はアレイ内の最小容量のディスクの容量以上である必要があります。**物理ディスクの「操作」**列で「 」をクリックして、ホットスペアディスクを設定します。 アレイ内のHDDが故障した場合、ホットスペアディスクがアクティブ化され、アレイが自動的に再構築されます。 **注意** 自動再構築が完了した後、別のHDDをインストールし、ホットスペアディスクとして設定することをおすすめします。
手動再構築	アレイにホットスペアディスクがない場合、アレイを手動で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** に移動し、リストから再構築するホットスペアディスクを選択します。

9.2.3 アレイの削除

→→システム → ストレージ管理 → ストレージHDD → ストレージHDD管理に移動し、 を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の表示

配列のファームウェア情報を表示し、バックグラウンドタスクの速度を設定できます。

開始前に

ディスクアレイが有効になっていることを確認してください。

手順

1. **システム→ ストレージ管理→ ストレージ HDD→ アレイ管理** を選択します。
2. **ファームウェア情報を**クリックします。
3. **オプション: バックグラウンド タスクの速度**を設定します。

9.3 ストレージモードを設定します。

手順

1. **システム**に移動し、**→ストレージ管理→ ストレージ モードを選択します**。

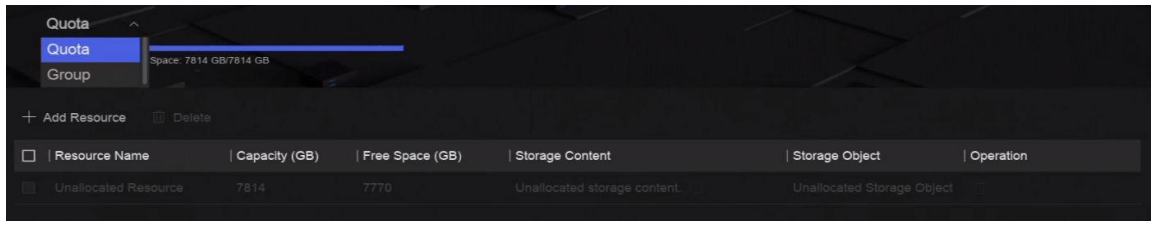


図9-4 ストレージモード

2. **クォータ**または**グループ**を選択します。**クォータ**

   各カメラまたはオーディオデバイスには、動画、画像、または音声の保存用に割り当てられたクォータを設定できます。

   グループ

   複数のHDDをグループとして管理できます。HDD設定を通じて、指定したチャンネルの動画を特定のHDDグループに記録できます。
3. 対応するパラメーターを設定します。
   - **クォータ**：ストレージオブジェクト用のスペースを割り当てます。
   - **グループ**: チャンネルをHDDグループにリンクします。

9.4 その他のストレージパラメーターを設定します

システム→ ストレージ管理→ 詳細設定に移動します。

表9-3 パラメーター説明

パラメーター名	説明
HDD スリープ	HDDのモードを選択してください。**パフォーマンスモード**、**バランスモード**、および**省電力モード**が選択可能です。
上書き	HDDが満杯になった場合、最も古いファイルを削除して新しいファイルの書き込みを継続します。
カメラのVCAデータを保存	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**で検索可能になります。
動画ごとの最大長さ	デバイスから動画をエクスポートする際、各動画ファイルの再生時間です。
動画のタグ付け（録画後）	動画にタグを追加した後、設定した録画開始時間です。 **注意** • ライブ視聴中または再生中に「」をクリックしてタグを追加できます。 • タグ付き動画を検索するには、にアクセスしてください。**→→をタグでバックアップ**。
eSATA	背面パネルにeSATAインターフェースを搭載したデバイス用です。
使用	eSATA の使用設定を行います。

9.5 USB フラッシュドライブの管理

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できます。

USBフラッシュドライブをデバイスに初めて接続した際、デバイスアップグレードやバックアップなどの簡易操作が可能です。同時に、画面の右上部に新しいアイコン「」が表示されます。

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します。

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を設定すると、そのテンプレートを録画スケジュールとして使用できます。

手順

1. →**システム**に移動し、**システム設定を開きます。 システム設定を開き、システム設定を開**きます。→ **テンプレート設定を開きます。 テンプレート設定を開きます。→ 休日**
2. **「追加」**をクリックします。

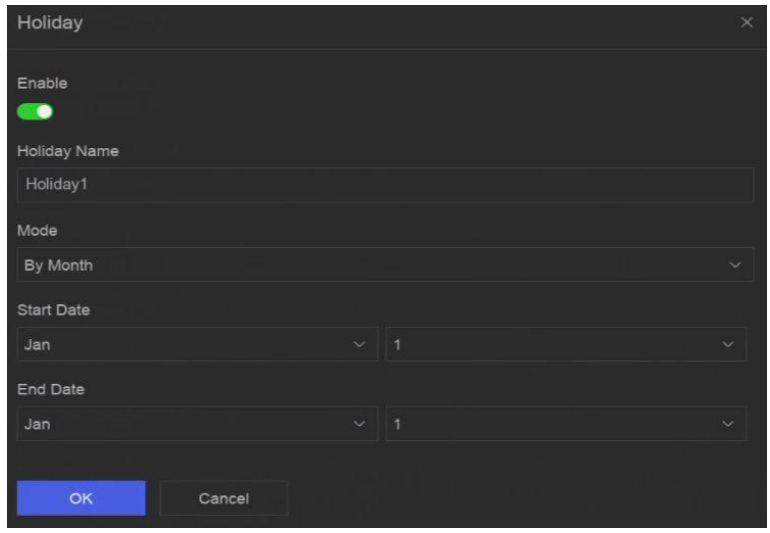


図10-1 休日を追加

3. **有効化を**オンにします。
4. 休日を設定します。

注

休日を設定すると、休日スケジュールを通常スケジュール（月曜日から日曜日）とは独立して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よりも優先されます。

5. **ストレージスケジュールを**設定します。
   1) **ストレージスケジュールを**クリックします。
   2) テンプレート名を選択します。

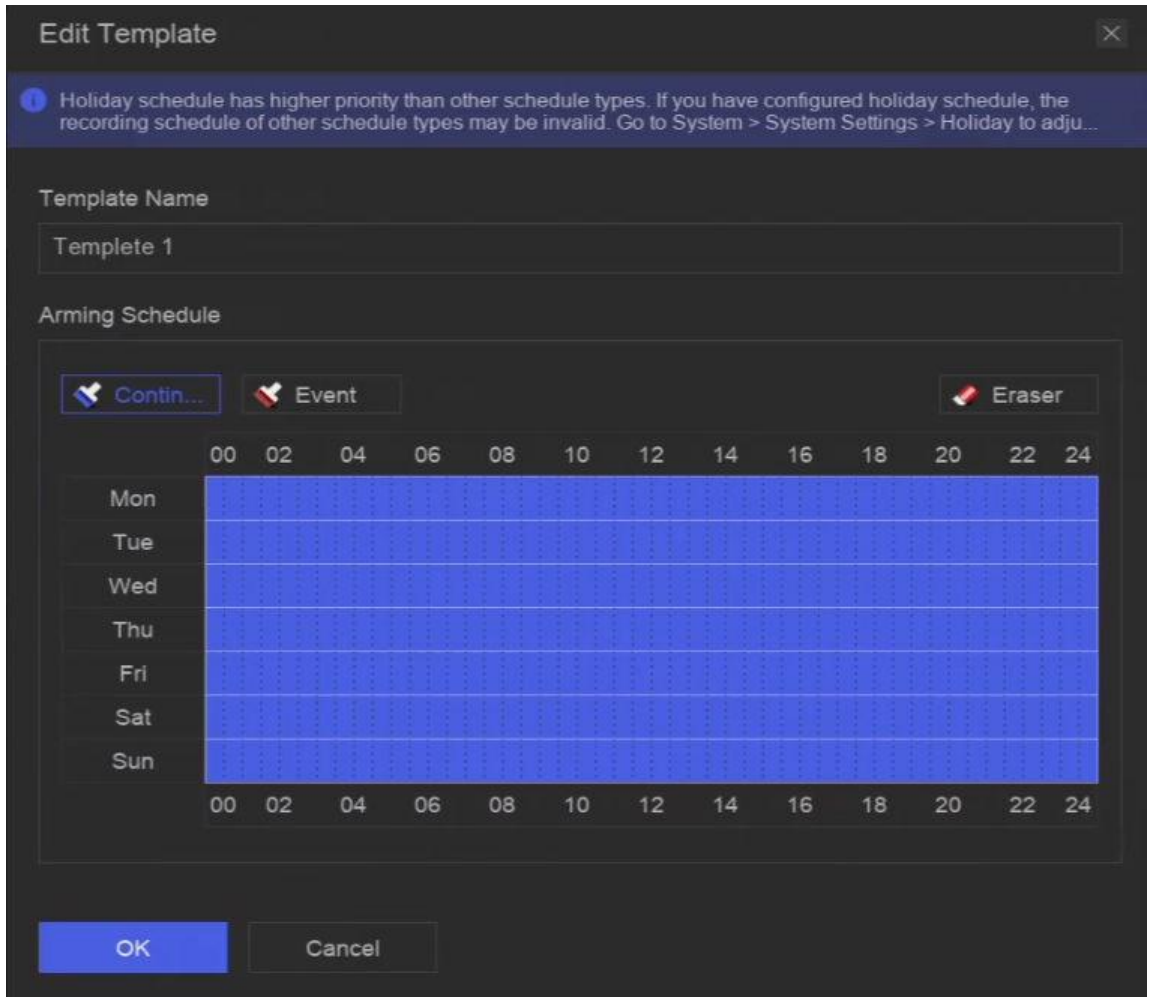


図10-2 テンプレート編集

3) 記録タイプを選択します。例：**イベント**。

4) 時間バー上でカーソルをドラッグしてスケジュールを描画します。

注

- タイムバー上でカーソルを移動させた後、[00:00-24:00] をクリックして指定した時間スケジュールを設定できます。
- スケジュールを削除するには、**消しゴムアイコン**をクリックしてください。

注

「**Configure Template**」をクリックして、**システム設定**でテンプレートを設定できます。**→ストレージ管理 →ストレージ スケジュール→ ビデオ録画 / 画面キャプチャ / 音声録画。**

6. OKをクリックします。

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/停止します。

手順

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** .

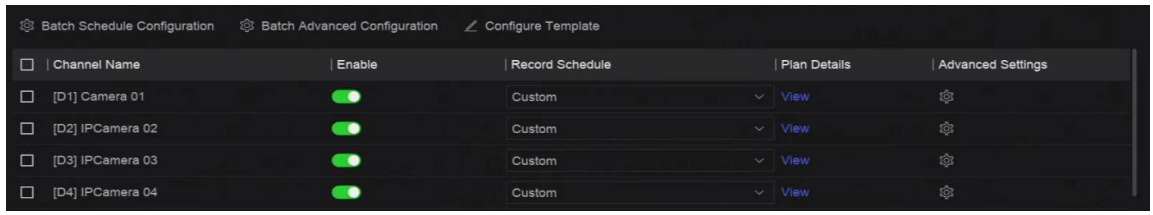


図10-3 ビデオ録画設定

2. カメラの「**有効**」をオンにします。

3. スケジュールタイプを選択します。

注

「**Record 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ム録画スケジュールを設定できます。または、タイムバー上のカーソルを移動し、「00:00-24:00」をクリックして指定した時間スケジュールを設定できます。

4. 「**表示**」をクリックしてスケジュールを表示します。

図10-4 スケジュールを表示

5. オプション：詳細設定の「⚙」をクリックして、その他の詳細パラメーターを設定できます。

表10-1 高度なパラメーター説明

パラメーター	説明
音声の記録	音声の録音のオン/オフを切り替えます。 **注** チャンネルには音声機能があるか、または音声デバイスが接続されている必要があります。
ANR	ANR（自動ネットワーク補充）は、ネットワーク接続が切断された場合にネットワークカメラのSDカードを自動的に有効化し、動画を保存します。ネットワークが回復した後、データを同期します。
事前録画	スケジュールされた時間またはイベントの前に録画を開始する時間です。例えば、アラームが10:00に録画を開始する場合、プレレコーディング時間を5秒に設定すると、カメラは9:59:55に録画を開始します。

パラメーター	説明
事後録画	イベントまたはスケジュールされた時間後に録画を開始する時間です。例えば、アラームがトリガーして録画が11:00に終了する場合、ポスト録画時間を5秒に設定すると、11:00:05まで録画が続きます。
ストリームタイプ	**メインストリームの場合**、解像度は通常より高くなります。**サブストリーム**の場合、同じストレージ容量でより長い時間録画できますが、解像度は低くなります。**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。
動画/画像の有効期限	有効期限は、ファイルがHDDに保存される期間です。有効期限が切れると、ファイルは削除されます。有効期限を0に設定すると、ファイルは削除されません。ファイルの実際の保存期間は、HDDの容量によって決定されます。

6. **オプション：**リストからチャンネルを選択し、**バッチスケジュール**設定と**バッチ詳細設定**を使用して、チャンネルをバッチで設定します。
7. **保存**をクリックします。

10.3 画像キャプチャ スケジュールを設定

デバイスはスケジュールに従って自動的にライブ画像をキャプチャします。

手順

1. **システム→ ストレージ管理→ ストレージ スケジュール→ ピクチャー キャプチャ** .

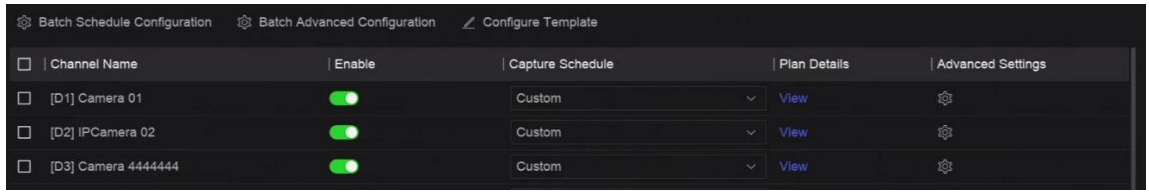


図10-5 画像キャプチャの設定

2. カメラの「**有効**」をオンにします。
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ム画像キャプチャスケジュールを設定できます。または、タイムバー上のカーソルを移動し、「00:00-24:00」をクリックして指定した時間スケジュールを設定できます。

4. **「表示」**をクリックしてスケジュールを確認します。

図10-6 スケジュールを表示

5. **詳細設定**をクリックして、詳細な画像パラメーターを設定します。

表10-2 高度なパラメーター説明

パラメーター	説明
キャプチャ遅延	画像の撮影にかかる時間。
解像度	キャプチャする画像の解像度を設定します。
画像品質	画像の画質を低、中、高から選択します。高画質を選択すると、より多くのストレージ容量が必要です。
間隔	各ライブ画像の撮影間隔を設定します。

6. **オプション：**リストからチャンネルを選択し、**バッチスケジュール**設定と**バッチ詳細設定**を使用して、チャンネルをバッチで設定します。
7. **保存**をクリックします。

10.4 音声記録の設定

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オーディオを録音します。

手順

1. **システム→ ストレージ管理→ ストレージ スケジュール→ オーディオ 記録**.
2. チャンネルの「**有効**」をオンにします。
3. スケジュールタイプを選択します。

注

「**Record 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ム記録スケジュールを設定できます。または、タイムバー上のカーソルを移動し、「00:00-24:00」をクリックして指定した時間スケジュールを設定できます。

4. 「**表示**」をクリックしてスケジュールを表示します。
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ーを設定できます。

表10-3 高度なパラメーター説明

パラメーター	説明
事前録音	スケジュールされた時間またはイベントの前に設定する録画開始時間。例えば、アラームが10:00に録画を開始するように設定した場合、プレ録画時間を5秒に設定すると、チャンネルは9:59:55に録画を開始します。
事後録画	イベントまたはスケジュールされた時間後に録画を開始する時間です。例えば、アラームがトリガーして録画が11:00に終了した場合、ポスト録画時間を5秒に設定すると、11:00:05まで録画が続きます。

6. **オプション：**リストからチャンネルを選択し、**バッチスケジュール**設定と**バッチ詳細設定**を使用して、チャンネルをバッチで設定します。
7. **保存**をクリックします。

第11章 ライブビュー

11.1 ライブビューレイアウトの設定

ライブビューは、各カメラの動画画像をリアルタイムで表示します。

手順

1. **ライブビュー**に移動します。
2. 画面の右下にある「」をクリックします。
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自由にカスタマイズします。
4. **「表示」**内の**「デフォルト表示」**にカーソルを移動します。
5. 「**View**」の右側にある「」をクリックします。
6. 手順の説明に従って、ライブビュー画像の出力インターフェースを調整します。ユーザーインターフェースに表示されている2つの方法に加え、チャンネルを1つのウィンドウから別のウィンドウへドラッグすることもできます。
7. 「」をクリックします。

11.2 GUI 概要

ライブ画像を表示、ライブ音声を再生、写真を撮影、即時再生を行うなど、さまざまな操作が可能です。

図11-1 ライブビュー（タイプ1）

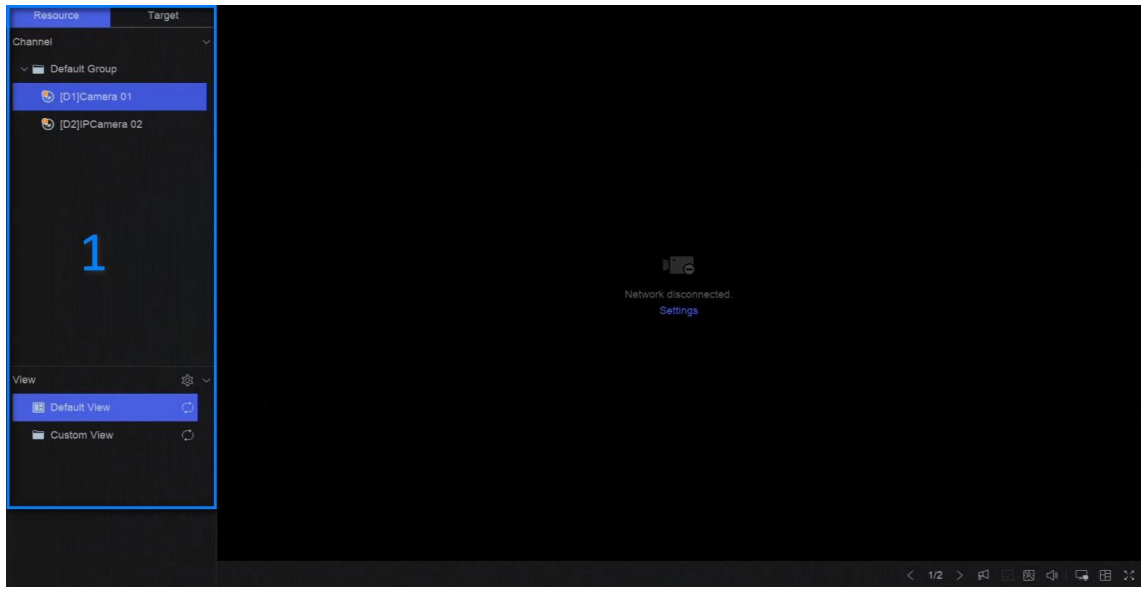


図11-2 ライブビュー（タイプ2）表11-1 インタ

ーフェース説明

番号	説明
1	チャンネルリスト、PTZコントロールパネル、および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、デバイスは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、リストに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構成できます。
2	右クリックショートカットメニュー。画像領域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。 • をクリックして、チャンネルにタグを追加します。追加後、 にアクセスし、→ **を選択し、→ By Tag** をクリックして、タグで動画を検索できます。 • を選択し、→ **で「VCA 情報表示」**を選択すると、ルールフレームを表示します。
4	ライブビューツールバー。**音声放送、VCA情報表示、出力切り替えなどの**機能が利用可能です。

注

- マウスを上下にスクロールすることで、前の画面/次の画面に移動できます。
- チャンネル画像の表示に異常が発生した場合、対応するウィンドウにエラーメッセージが表示され、青い文字のテキストを直接クリックしてデバイス設定を編集できます。

11.3 PTZ制御

PTZは「パン（水平移動）、チルト（垂直移動）、ズーム」の略称です。PTZカメラをデバイスに追加すると、そのデバイスは左右にパン、上下にチルト、ズームイン/ズームアウトが可能になります。

PTZカメラを選択し、画面左下にあるPTZコントロールメニューを展開します。

表11-2 PTZ操作

タスク	説明	操作
プリセット	プリセットは、PTZの位置とズーム、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ことで、カメラを事前に定義された位置に素早く移動させることができます。	プリセットを設定する: 1. プリセットを選択します。 2. 方向ボタンを使用して画像を調整します。 3. 「」をクリックします。
		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、設定された時間滞在した後、次のキーポイントに移動するように設定できます。キーポイントはプリセットに対応しています。	パトロールを設定: 1. パトロールを選択します。 2. 「」をクリックします。 3. パトロール用のプリセットを追加します。 4. OKをクリックします。
		パトロールを呼び出す: をクリックします。
パターン	パターンは、PTZの動作を記録することで設定できます。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沿って移動させることができます。	パターンを設定する: 1. クリック。 2. 方向ボタンを使用して画像の位置を調整し、デバイスが動きを記録します。 3. 記録を停止します。
		パターンを呼び出す: をクリックします。

注意

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 概要

動画または音声ファイルを再生できます。

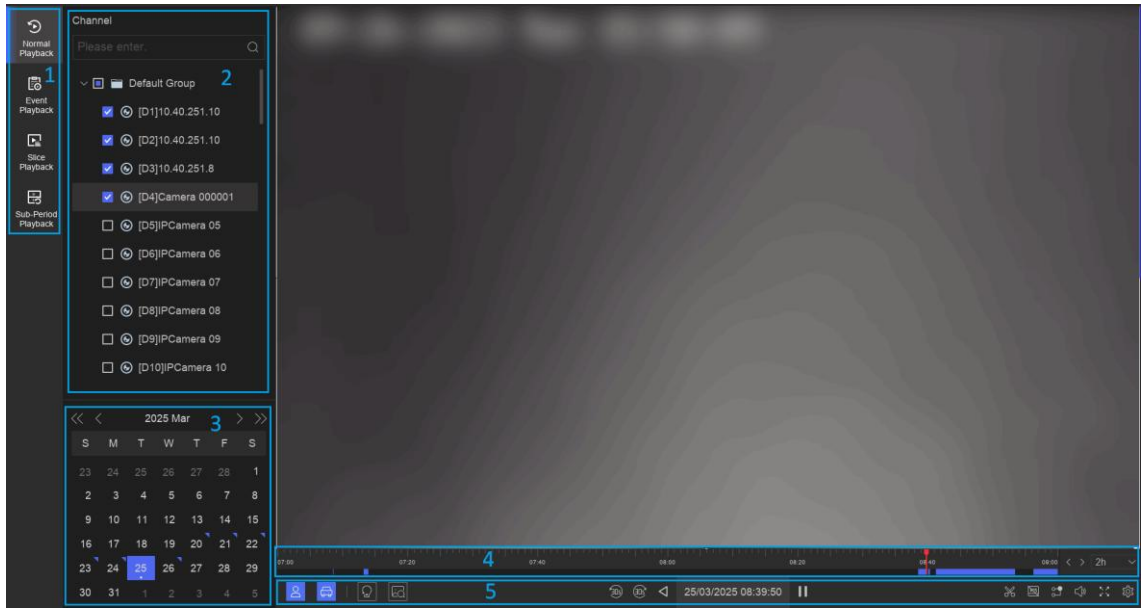


図12-1 再生 表12-1 インターフェー

スの説明

番号	説明
1	再生タイプを選択する領域。
2	チャンネル一覧。
3	時間選択用のカレンダー。
4	再生タイムライン。 • タイムライン上にカーソルを配置し、タイムラインをドラッグして特定の時間に移動します。 • 青色のバーでマークされた期間に動画が含まれています。赤色のバーは、その期間内の動画がイベント動画であることを示します。 • タイムラインを上下にスクロールして、ズームアウト/ズームインできます。
5	再生ツールバー。

番号	説明
	• 「 （スマート検索）」をクリックし、表示されるポップアップのヒントに従ってイベントルールを描画し、対応するイベントルールをトリガーする動画を検索します。操作はデュアルVCA機能と類似しています。 • 「」をクリックしてAcuSearch機能を実行します。詳細については ***AcuSearch*** を参照してください。 • / をクリックして、人間/車両を含む動画を表示します。 **注意** この機能を使用するには、特定のイベントタイプに対して**検出対象を「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。 • にアクセスし、チャンネルを選択し、指定した期間内の選択したチャンネルで動画をクリップするための開始時間と終了時間を設定します。 • 「」をクリックし、通常の動画とスマート動画（スマートデータを含む動画）の再生戦略を設定します。

12.2 通常再生

チャンネルの動画を再生します。一部のデバイスでは、複数のチャンネルの同期再生が許可される場合があります。

手順

1. **再生 →** に移動します。
2. 左側のリストからチャンネルを選択します。

   注意

   グループ再生: リストからグループを選択すると、そのグループ内のチャンネルを再生できます。

3. カレンダーから日付を選択します。

   注

   カレンダーの日付の角にある青い三角形は、再生可能な動画があることを示します。

4. **オプション:** 追加の操作を実行できます。

   キャプチャ 再生中に画面をキャプチャするには、 をクリックしてください。

   デジタルズーム をクリックして、動画画像の特定の部分をズームインします。

	にアクセスして、チャンネルにタグを追加します。追加後、 → **Backup** → **By Tag** に移動し、タグで動画を検索できます。
	をクリックして動画をロックします。ロックされた動画は上書きされなくなります。ロック後、 → **Backup**→ **By Tag** に移動し、ロック状態の動画を検索できます。
デュアルVCA	「」を選択し、→ 「**Dual-VCA**」を選択して、対応するイベントルールをトリガーする動画を検索します。各イベントタイプの設定手順は、イベント設定の手順を参照してください。
	注意 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ー**→ **ディスプレイ情報を**画面に表示 をオンにします。次に、**システム** → **ストレージ管理**→ **詳細設定** に移動し、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** をオンにします。
VCA 情報を表示	「」を選択し、→ **Show VCA Info** を有効にすると、ルールフレームを表示できます。
プライバシー保護を無効にする	プライバシー保護が有効になっている場合、画像にモザイクが表示される可能性があります。プライバシー保護のストレージ権限が有効になっている場合、 → **Display Privacy Protection** を選択すると、元の動画（モザイクなし）を表示できます。プライバシー保護機能の詳細については、***Configure Privacy Protection*** を参照してください。

12.3 イベント再生

イベント再生モードを選択すると、システムは動画内に動作検出、線越え検出、または侵入検出の情報を含む動画を分析し、マークします

開始前に

- カメラで**デュアルVCAが**有効になっていることを確認してください。カメラのウェブブラウザ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から**有効にできます。
- ビデオレコーダーで「**ストレージ管理** → **詳細設定**」の「**カメラVCAデータを保存**」が有効になっていることを確認してください。

手順

1. **再生**→ を選択します。
2. カレンダーから日付を選択します。

注意

カレンダーの日付の隅にある青い三角形は、利用可能な動画があることを示しています。

3. 再生画像の右下にある「」をクリックします。再生画像の右下にある**「→ Dual-VCA」**をクリックして、イベントの種類を選択します。各イベントの種類の詳細については、イベント設定の手順を参照してください。
4. **「検索」**をクリックします。

   検出ルールを満たす動画は赤色でマークされます。
5. 「」をクリックして、通常動画とスマート動画（スマートデータを含む動画）の再生戦略を設定します。

注意

デュアルVCAを使用しない場合、進行バーの赤いセグメントは、スマート動画が元のイベントから生成されていることを示します。

12.4 スライス再生

動画をスライスに分割し、再生します。

手順

1. **再生**に移動→。
2. カメラリストからカメラを選択します。
3. カレンダーから日付を選択します。
4. **検索**をクリックします。

   取得した動画は、再生用に1時間単位のセグメントに分割されます。
5. **オプション:** 1時間の区間を選択し、[ ]をクリックして、再生用に1分間の区間に分割します。

12.5 サブ期間再生

動画ファイルは画面上で複数のサブ期間を同時に再生できます。

手順

1. **再生 →** を選択します。
2. カメラを選択します。
3. 開始時間と終了時間を設定します。
4. **検索**をクリックします。

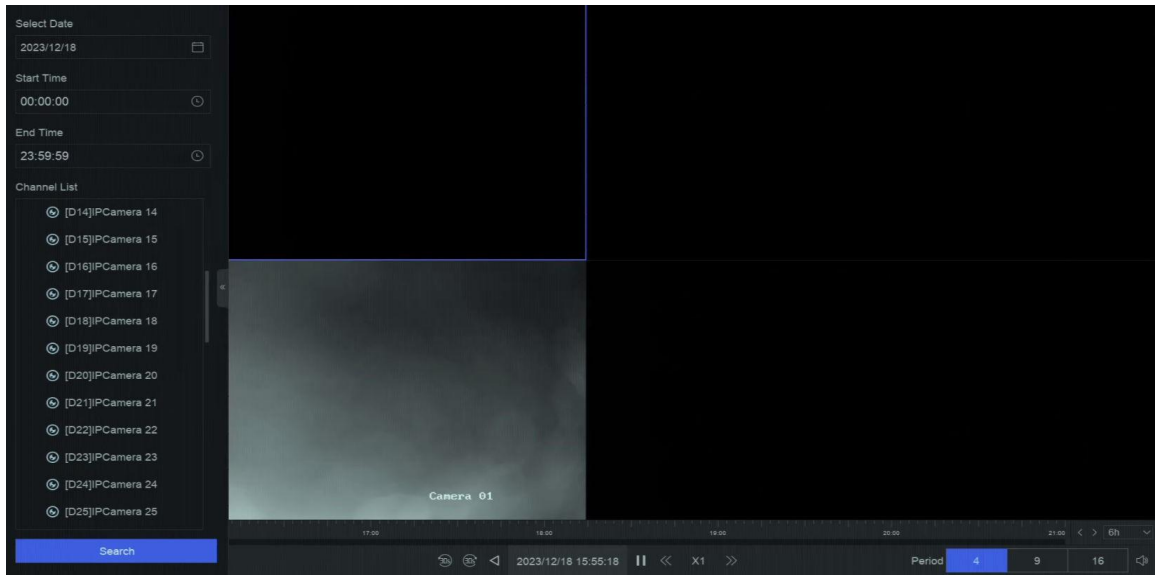


図12-2 サブ期間再生

5. 画面の右下にある期間を選択します（例：4）。

注

定義された分割画面の数に応じて、選択した日付の動画ファイルを再生用に平均的なセグメントに分割できます。例えば、16:00から22:00までの動画ファイルが存在し、6画面表示モードが選択されている場合、各画面で1時間分の動画ファイルを同時に再生できます。

第13章 イベントセンター

13.1 イベント設定

13.1.1 基本/汎用イベント

手順

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

2. チャンネルを選択します。

3. イベントの種類を選択します。

4. **「有効」**をオンにします。

5. **ルール設定**をクリックしてルールを設定します。

表13-1 通常イベント

イベント名	イベント説明	ルール設定	
モーション検出	モーション検出は、監視領域内の移動する物体を検出します。	画像の上部にあるツールバーを使用して、検出領域を描画します。 • **NVRによるAI**: モーション検出イベントはNVRによって分析されます。このデバイスは、人間と車両を含む動画を分析できます。選択したタイプ（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、他の物体による誤報を削減できます。 • **カメラによるAI**: モーション検出イベントはカメラによって分析されます。 • **検出対象**：人間と**車両**が選択可能です。誤報を除き、	感度設定で、動きがアラームをトリガーする容易さを調整できます。値が高いほど、動き検出がより敏感になります。

イベント名	イベント説明	ルール設定	
		選択された対象がアラームをトリガーします。	
動画改ざん検出	カメラのレンズが覆われた際に動画改ざん検出がアラームをトリガーし、アラーム対応措置を実行します。	画像の上部にあるツールバーを使用して、検出領域を描画します。	
動画損失検出	動画損失検出は、チャンネルの動画損失を検出し、アラーム対応措置を実行します。	-	
音声異常検出	音声異常検出は、シーン内の異常な音（例えば、音量の急激な増加/減少など）を検出します。	-	
焦点外れ検出	レンズのボケによる画像のボケを検出できます。	-	
急激なシーン変更検出	シーン変更検出は、カメラの意図的な回転など、外部要因によるビデオセキュリティ環境の変化を検出します。	-	

6. **「アラーム設定スケジュール」**をクリックして、アラーム設定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ム武装スケジュールを設定するか、タイムバー上のカーソルを移動し「00:00-24:00 」をクリックして指定した時間スケジュールを設定できます。

7. **「リンク方法」**をクリックして、リンク方法を設定します。

表13-2 リンク方法の説明

リンク方法	説明
監視センターへの通知	デバイスは、イベントが発生した際に、リモートアラームホストに例外またはアラーム信号を送信できます。アラームホストとは、クライアントソフトウェア（例：iVMS-4200、iVMS-5200）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、ローカルモニターにアラームポップアップウィンドウが表示されます。
ブザー	アラームが検出されると、ブザーが音で鳴ります。
メール送信	アラームが検出された場合、システムはアラーム情報をユーザーまたは複数のユーザーにメールで送信できます。
アラーム出力	アラーム出力は、アラーム入力、動作検出、ビデオ改ざん検出、顔検出、ラインクロス検出、およびその他のすべてのイベントによってトリガーされます。
記録	アラームが検出された場合、選択されたチャンネルが動画を記録します。 **注意** 動画記録スケジュールがチャンネルで有効化されていない場合、この連携は無効になります。動画記録スケジュールを設定するには、**システム → ストレージ管理 →→ ストレージスケジュール →→ 動画記録**に移動してください。

8. **保存**をクリックします。

13.1.2 周辺保護

周辺保護イベントには、線越え検出、侵入検出、領域進入検出、領域退出検出が含まれます。

線越え検出の設定

線越え検出は、設定された仮想線を越える人、車両、物体を検出します。検出方向は双方向、左から右、または右から左に設定できます。

手順

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利用可能です。

1. **イベントセンター**に移動します。**→** **→イベント設定→ 周辺保護**。

2. カメラを選択します。
3. **オプション：セカンダリ分析を**有効にします。対応するデバイスエンジンがこのイベントを再分析し、誤報を削減します。

注

周辺保護アルゴリズム**に対しては**、少なくとも1つのデバイスエンジン**でセカンダリ分析**を実行する必要があります。右側の「**エンジンを割り当てる**」をクリックしてエンジンを迅速に割り当てるか、**システム → スマート設定 → アルゴリズム設定 → アルゴリズム管理**に移動し、**周辺保護**アルゴリズム**に対してセカンダリ分析を**有効化してください。

4. **オプション: NVRでAIを**有効にします。対応するデバイスエンジンが動画を分析し、カメラは動画ストリームのみを送信します。

注意

少なくとも1つのデバイスエンジンで「**周辺保護**アルゴリズム」を実行する必要があります。右側の「**エンジンを割り当てる**」をクリックしてエンジンを迅速に割り当てるか、**システム → スマート設定 → アルゴリズム設定 → 「→アルゴリズム管理」**に移動して「**周辺保護**アルゴリズム」を有効化してください。

5. **「ラインクロス」**を選択します。
6. **「有効」**をオンにします。

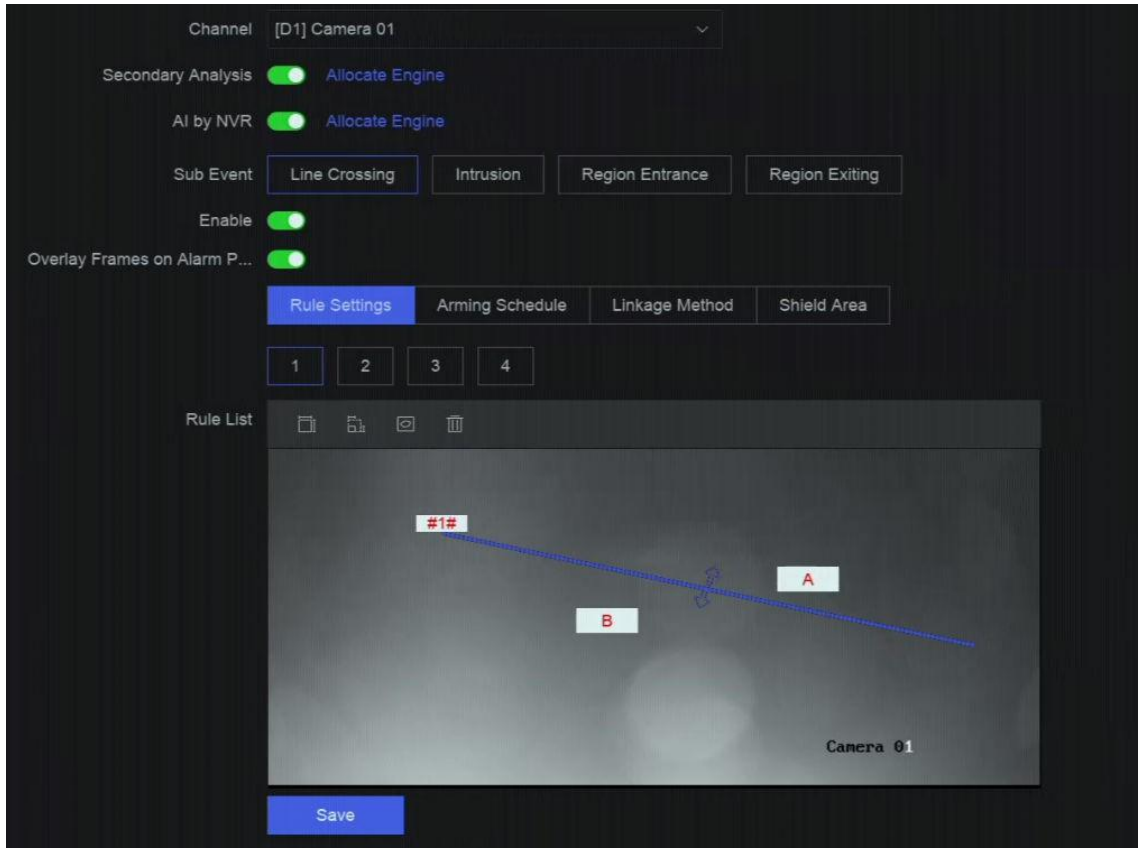


図13-1 ラインクロス検出

7. **「ルール設定」**をクリックして検出ルールを設定します。

1) ルール番号を選択します。例：**1**を選択します。

2) 「  」をクリックし、検出線の開始点と終了点をそれぞれ画像上で2回クリックして描画します。

3) **方向**、**感度**、**検出対象**、および**対象信頼度**を設定します。**A<->B**

B側の矢印のみが表示されます。対象物が設定された線を通過すると、両方向で検出されアラームがトリガーされます。

A->B

A側からB側へ設定された線を横切るオブジェクトのみが検出されます。

B->A

B側からA側へ設定されたラインを横切る対象物のみが検出可能です。

感度

値が高いほど、検出アラームがより容易にトリガーされます。

検出対象

検出対象を「人間」または**「車両」**に設定することで、人間や車両によってトリガーされないアラームを無視できます。**検出対象は、**一部のモデルでのみ利用可能です。

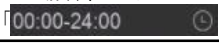
ターゲット信頼度

線越えイベントの検出における確実性または信頼性のレベルを示すために使用されます。信頼性レベルを高く設定すると、高信頼性の検出のみがイベントをトリガーし、誤報を削減します。

4) **オプション:** 「  」または「  」をクリックして、**最大サイズ**または**最小サイズ**を設定します。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します。

5) **オプション：**上記のステップを繰り返し、追加のルールを描画します。最大**4**つのルールまでサポートされています。

8. **「Arming Schedule」**をクリックして、アラームのスケジュールタイプを選択します。

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ム武装スケジュールを設定するか、タイムバー上のカーソルを移動して「  」をクリックし、指定した時間スケジュールを設定できます。

9. **「リンク方法」**をクリックしてリンク方法を設定します。

表13-3 リンク方法の説明

リンク方式	説明
監視センターへの通知	デバイスは、イベントが発生した際に、リモートアラームホストに例外またはアラーム信号を送信できます。アラームホストとは、クライアントソフトウェア（例：iVMS-4200、iVMS-5200）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た場合、ローカルモニターにアラームポップアップウィンドウが表示されます。

連携方法	説明
ブザー	アラームが検出されると、ブザーが音で鳴ります。
メール送信	アラームが検出された場合、システムはユーザーまたは複数のユーザーにアラーム情報を記載したメールを送信します。
アラーム出力	アラーム出力は、アラーム入力、動作検出、ビデオ改ざん検出、顔検出、ライン越え検出、およびその他のすべてのイベントによってトリガーされます。
記録	アラームが検出された場合、選択されたチャンネルが動画を記録します。 **注意** チャンネルの動画記録スケジュールが有効になっていない場合、この連携は無効になります。動画記録スケジュールを設定するには、**システム → ストレージ管理 →→ ストレージスケジュール →→ 動画記録** へ移動してください。

10. **オプション：NVRのAI**機能が有効な場合、**シールドエリア**を設定できます。シールドエリアを設定すると、そのエリア内の対象物の動作分析が行われなくなり、エリア内での周辺保護イベントがトリガーされなくなります。
11. **保存**をクリックします。

次にやるべきこと

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確認できます。

侵入検知の設定

侵入検知機能は、事前に定義された仮想領域内に侵入し、滞留する人、車両、またはその他の物体を検知します。アラームがトリガーされた際に、特定のアクションを実行できます。

手順

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利用可能です。

1. **イベントセンターに移動→ → イベント設定→ 周辺保護**。
2. カメラを選択します。
3. **オプション: セカンダリ分析を**有効にします。対応するデバイスエンジンがこのイベントを再分析し、誤報を削減します。

注

少なくとも1つのデバイスエンジン**で「周辺保護**アルゴリズム」**のセカンダリ分析**を実行する必要があります。右側の「**エンジンを割り当てる**」をクリックしてエンジンを迅速に割り当てるか、**システム → スマート設定 → アルゴリズム設定 → アルゴリズム管理**に移動し、「**周辺保護**アルゴリズム」**のセカンダリ分析を**有効にします。

4. **オプション：NVRによるAIを**有効にします。対応するデバイスエンジンが動画を分析し、カメラは動画ストリームのみを送信します。

注意

少なくとも1つのデバイスエンジンで「**Perimeter Protection**」アルゴリズムを実行する必要があります。右側の「**エンジンを割り当てる**」をクリックしてエンジンを迅速に割り当てるか、**システム → スマート設定 → アルゴリズム設定 → 「→」アルゴリズム管理**に移動して「**Perimeter Protection**」アルゴリズムを有効化してください。

5. 「**侵入**」を選択します。
6. 「**有効**」をオンにします。

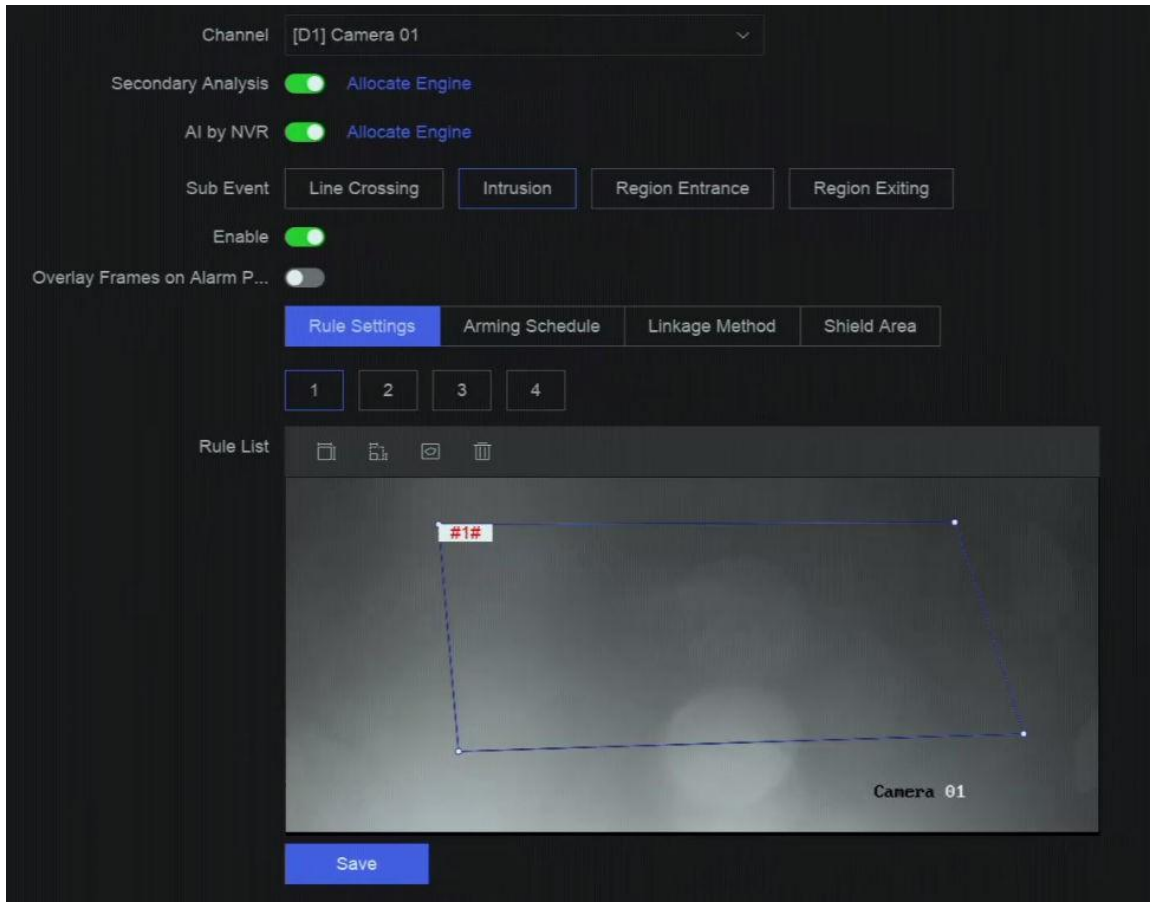


図13-2 侵入検出

7. 「**ルール設定**」をクリックして検出ルールを設定します。
   1) ルール番号を選択します。例：**1**を選択します。

2) 「」をクリックし、四角形または十角形の領域の各点を描くために、それぞれ4回ずつ画像をクリックします。

3) **時間閾値**、**感度**、**検出対象**、および**対象信頼度**を設定します。**時間閾値**

対象物が領域内に滞在する時間です。対象物が定義された検出領域内に滞在する時間が閾値を超えると、デバイスがアラームをトリガーします。

感度

値が高いほど、検出アラームがより簡単にトリガーされます。

検出対象

検出対象を「人間」または**「車両」**に設定し、人間または車両によってトリガーされないアラームを無視します。**検出対象は、**一部のモデルでのみ利用可能です。

ターゲット信頼度

侵入イベントの検出における確実性または信頼性のレベルを示すために使用されます。信頼度を高く設定すると、高信頼性の検出のみがイベントをトリガーし、誤報を削減します。

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。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します。

5) **オプション：**上記のステップを繰り返し、追加のルールを描画できます。最大4つのルールがサポートされています。

8. **「武装スケジュール」**をクリックして、武装スケジュールの種類を選択してください。

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ム武装スケジュールを設定できます。または、タイムバー上でカーソルを移動し、「00:00-24:00」をクリックして指定した時間スケジュールを設定できます。

9. **「リンク方法」**をクリックして、リンク方法を設定します。

表13-4 リンク方法の説明

リンク方法	説明
監視センターに通知	デバイスは、イベントが発生した際にリモートアラームホストに例外またはアラーム信号を送信できます。アラームホストとは、クライアントソフトウェア（例：iVMS-4200、iVMS-5200）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、ローカルモニターにアラームポップアップウィンドウが表示されます。
ブザー	アラームが検出されると、ブザーが音で鳴ります。
メール送信	システムは、アラームが検出された際に、ユーザーまたは複数のユーザーにアラーム情報を記載したメールを送信できます。

連携方法	説明
アラーム出力	アラーム出力は、アラーム入力、動作検出、動画改ざん検出、顔検出、線越え検出、およびその他のすべてのイベントによってトリガーされます。
記録	アラームが検出されると、選択されたチャンネルで動画が記録されます。 **注意** チャンネルに動画記録スケジュールが有効になっていない場合、この連携は無効になります。動画記録スケジュールを設定するには、**システム → ストレージ管理 →→ ストレージスケジュール →→ 動画記録**に移動してください。

10. **オプション: NVRによるAI**が有効になっている場合、**シールド領域**を設定します。シールド領域を設定すると、デバイスはその領域内のターゲットの動作を分析しなくなるため、その領域内で周辺保護イベントがトリガーされなくなります。
11. **保存**をクリックします。

次にやるべきこと

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確認できます。

地域入口検出の設定

領域進入検出は、事前に定義された仮想領域に進入するオブジェクトを検出します。

手順

注意

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利用可能です。

1. **イベントセンター**に移動 → → **イベント設定→ 周辺保護**。
2. カメラを選択します。
3. **オプション：セカンダリ分析を**有効にする。対応するデバイスエンジンがこのイベントを再分析し、誤報を削減します。

   注

   周辺保護アルゴリズム**に対してセカンダリ分析**を実行するデバイスエンジンが少なくとも1つ必要です。右側の「**エンジンを割り当てる**」をクリックしてエンジンを迅速に割り当てるか、**システム → スマート設定 → アルゴリズム設定 → アルゴリズム管理**に移動し、**周辺保護**アルゴリズム**に対してセカンダリ分析を**有効化してください。
4. **オプション：NVRによるAIを**有効にします。対応するデバイスエンジンが動画を分析し、カメラは動画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で**Perimeter Protection**アルゴリズムを実行する必要があります。右側の「**エンジンを割り当てる**」をクリックしてエンジンを迅速に割り当てるか、**システム → スマート設定 → アルゴリズム設定 →→ アルゴリズム管理**に移動し、**Perimeter Protection**アルゴリズムを有効にします。

5. 「**Region Entrance**」を選択します。
6. 「**有効**」をオンにします。

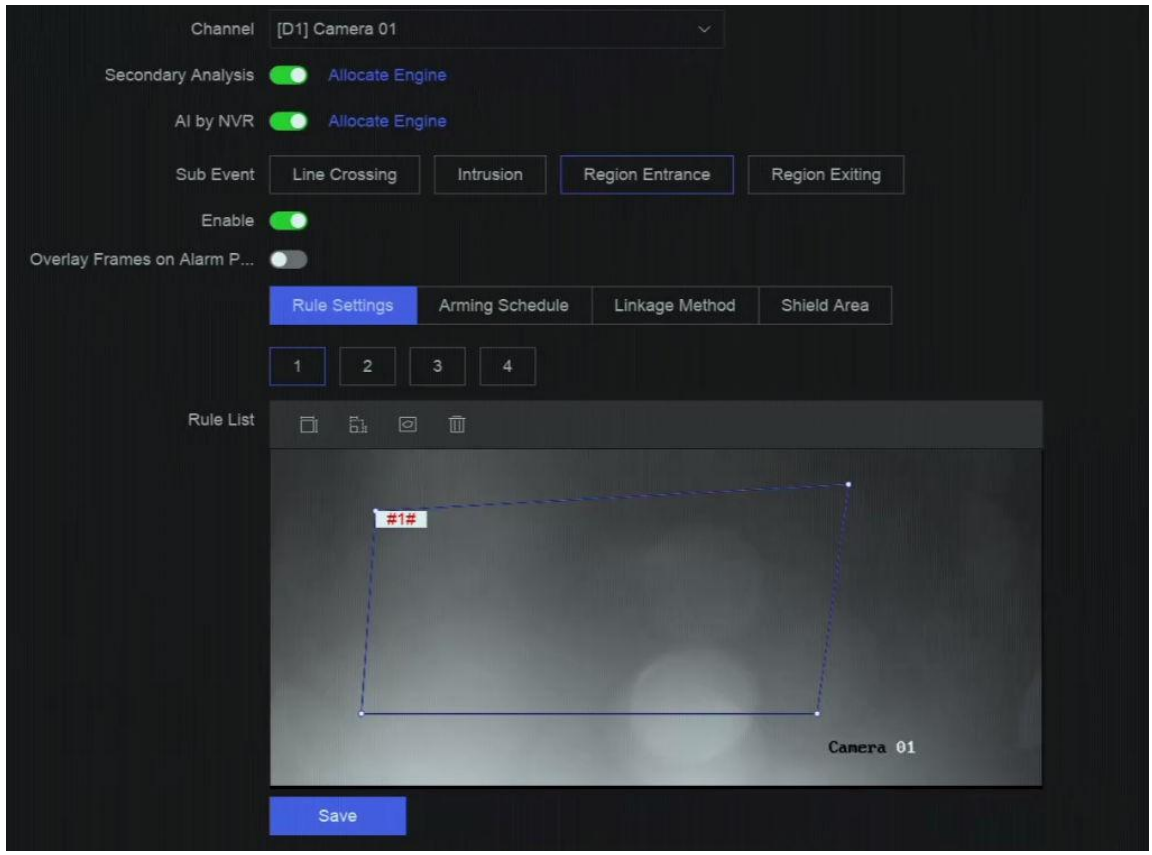


図13-3 地域入口検出

7. 「**ルール設定**」をクリックして検出ルールを設定します。
   1) ルール番号を選択します。例：**1**を選択します。
   2) 「 」をクリックし、四角形または十角形の領域の各点を描くために、画像に**4**回ずつクリックします。
   3) **感度**、**検出対象**、および**対象信頼度**を設定します。**感度**

      値が高いほど、検出アラームがより簡単にトリガーされます。

      検出対象

      検出対象を「人間」または**「車両」**に設定することで、人間や車両によってトリガーされないアラームを無視できます。**検出対象は、**一部のモデルでのみ利用可能です。

ターゲット信頼度

検出領域への進入イベントの検出精度や信頼性を示す指標です。信頼度を高く設定すると、高信頼性の検出のみがイベントをトリガーし、誤報を削減します。

4) **オプション:** 上記の手順を繰り返し、追加のルールを描画します。最大4つのルールまでサポートされています。

8. **「武装スケジュール」**をクリックして、武装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ム武装スケジュールを設定できます。または、タイムバー上でカーソルを移動し、「00:00-24:00」をクリックして指定した時間スケジュールを設定できます。

9. **「リンク方法」**をクリックしてリンク方法を設定します。

表13-5 リンク方法の説明

リンク方法	説明
監視センターに通知	デバイスは、イベントが発生した際にリモートアラームホストに例外またはアラーム信号を送信できます。アラームホストとは、クライアントソフトウェア（例：iVMS-4200、iVMS-5200）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、ローカルモニターにアラームポップアップウィンドウが表示されます。
ブザー	アラームが検出されると、ブザーが音で鳴ります。
メール送信	アラームが検出された場合、システムはアラーム情報をユーザーまたは複数のユーザーにメールで送信できます。
アラーム出力	アラーム出力は、アラーム入力、動作検出、ビデオ改ざん検出、顔検出、ラインクロス検出、およびその他のすべてのイベントによってトリガーされます。
録画	アラームが検出された場合、選択されたチャンネルで動画を記録します。 **注意** チャンネルに動画記録スケジュールが有効になっていない場合、この連携は無効になります。動画記録スケジュールを設定するには、**システム → ストレージ管理 →→ ストレージスケジュール →→ 動画記録**に移動してください。

10. **オプション：NVRによるAI**が有効になっている場合に**シールド領域**を設定します。シールド領域を設定すると、デバイスはその領域内のターゲットの動作を分析しなくなるため、その領域内で周辺保護イベントがトリガーされなくなります。

11. **保存**をクリックします。

次にやるべきこと

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確認できます。

領域退出検出の設定

領域退出検出は、事前に定義された仮想領域から退出するオブジェクトを検出します。

手順

注意

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利用可能です。

1. **イベントセンター**に移動 → → **イベント設定**→ **周辺保護**。
2. カメラを選択します。
3. **オプション：セカンダリ分析を**有効にする。対応するデバイスエンジンがこのイベントを再度分析し、誤報を削減します。

   注

   周辺保護アルゴリズム**に対してセカンダリ分析**を実行するデバイスエンジンが少なくとも1つ必要です。右側の**「エンジンを割り当てる」**をクリックしてエンジンを迅速に割り当てるか、**システム → スマート設定 → アルゴリズム設定 → アルゴリズム管理**に移動し、**周辺保護**アルゴリズム**に対してセカンダリ分析を**有効化してください。
4. **オプション：NVRによるAIを**有効にします。対応するデバイスエンジンが動画を分析し、カメラは動画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で**Perimeter Protection**アルゴリズムを実行する必要があります。右側の「**エンジンを割り当てる**」をクリックしてエンジンを迅速に割り当てるか、**システム → スマート設定 → アルゴリズム設定 →→ アルゴリズム管理**に移動し、**Perimeter Protection**アルゴリズムを有効にします。
5. **「Region Exiting」**を選択します。
6. **「有効」**をオンにします。

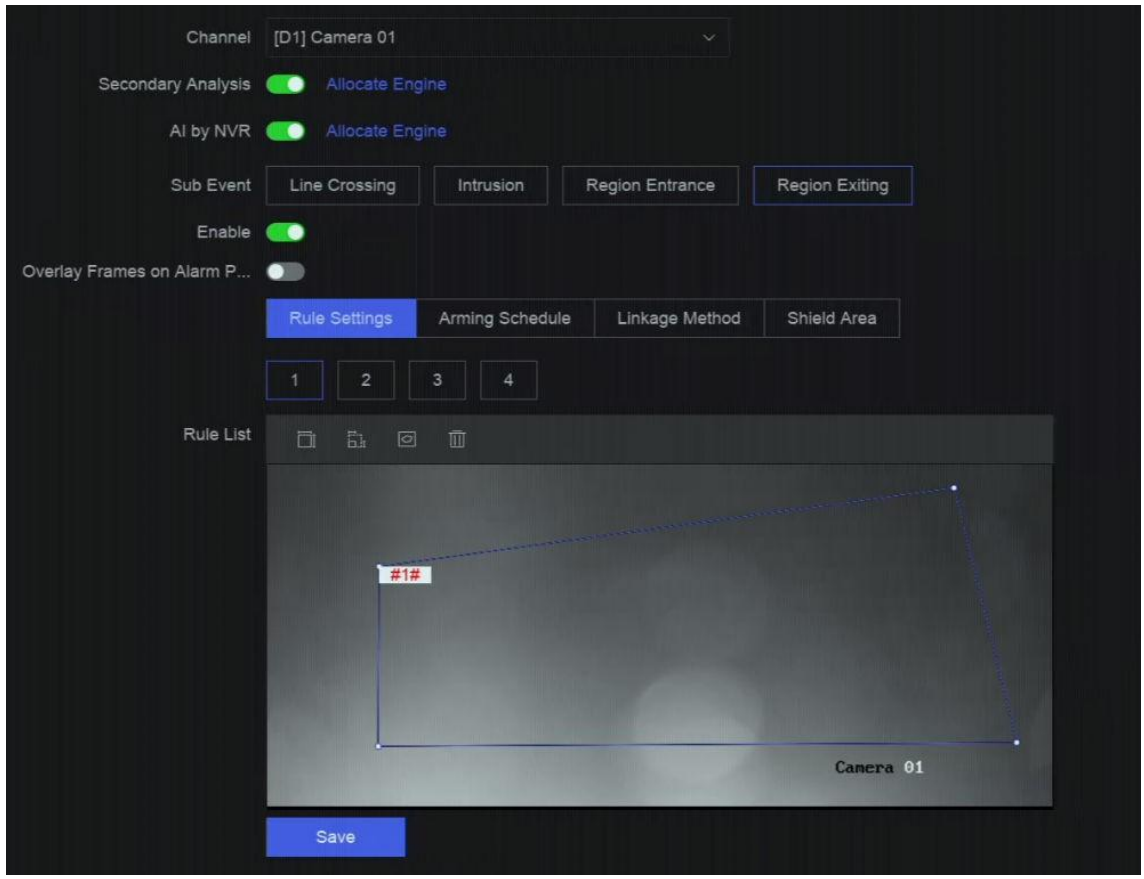


図13-4 地域退出検出

7. **「ルール設定」**をクリックして検出ルールを設定します。

1) ルール番号を選択します。例：**1**を選択します。

2) 「 」をクリックし、画像上で**4**回クリックして、四角形または十角形の領域の各点をそれぞれ描画します。

3) **感度**、**検出対象**、および**対象信頼度**を設定します。**感度**

値が高いほど、検出アラームがより容易にトリガーされます。

検出対象

検出対象を「人間」または**「車両」**に設定することで、人間や車両によってトリガーされないアラームを無視できます。**検出対象は、**一部のモデルでのみ利用可能です。

ターゲット信頼度

検出領域からのイベント検出の確実性または信頼性を示すために使用されます。信頼度を高く設定すると、高信頼性の検出のみがイベントをトリガーし、誤報を削減します。

4) **オプション：**上記のステップを繰り返し、追加のルールを作成できます。最大**4**つのルールがサポートされています。

8. **「武装スケジュール」**をクリックして、武装スケジュールタイプを選択します。

注意

「**Arming Schedule**」を「**Custom**」に設定すると、タイムバー上でカーソルをドラッグしてカスタムの武装スケジュールを設定できます。または、タイムバー上でカーソルを移動し、「00:00-24:00」をクリックして指定した時間スケジュールを設定できます。

9. 「**リンク方法**」をクリックして、リンク方法を設定します。

表13-6 リンク方法の説明

リンク方法	説明
監視センターに通知	デバイスは、イベントが発生した際にリモートアラームホストに例外またはアラーム信号を送信できます。アラームホストとは、クライアントソフトウェア（例：iVMS-4200、iVMS-5200）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、ローカルモニターにアラームポップアップウィンドウが表示されます。
ブザー	アラームが検出されると、ブザーが音で鳴ります。
メール送信	アラームが検出された場合、システムはアラーム情報をユーザーまたは複数のユーザーにメールで送信できます。
アラーム出力	アラーム出力は、アラーム入力、動作検出、ビデオ改ざん検出、顔検出、ライン越え検出、およびその他のすべてのイベントによってトリガーされます。
録画	アラームが検出された場合、選択されたチャンネルで動画を記録します。 **注意** チャンネルに動画記録スケジュールが有効になっていない場合、この連携は無効になります。動画記録スケジュールを設定するには、**システム → ストレージ管理 →→ ストレージスケジュール →→ 動画記録**に移動してください。

10. **オプション：NVRによるAI**が有効になっている場合、**シールド領域**を設定します。シールド領域を設定すると、デバイスはその領域内のターゲットの動作を分析しなくなるため、その領域内で周辺保護イベントがトリガーされなくなります。

11. **保存**をクリックします。

次にやるべきこと

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確認できます。

13.1.3 異常行動イベント

開始前に

カメラがこの機能に対応していることを確認してください。

手順

1. **イベントセンター**に移動します。→ → **イベント設定**→ **異常動作イベント**。
2. カメラを選択
3. イベントの種類を選択します。
4. **「有効」**をオンにします。
5. **ルール設定**をクリックしてルールを設定します。

表13-7 異常動作イベント

イベント名	イベントの説明	ルール設定
滞留検出	滞留検出は、ターゲットが指定された領域内に設定された時間を超えて滞在しているかどうかを検出し、関連するアクションをトリガーするアラームを発動します。	a. ルール番号を選択してください。 b. 画像の上部にあるツールバーを使用して、検出ラインを描画します。 c. **時間閾値**と**感度**を設定します。**時間閾値** 対象物が領域内に滞在する時間です。値が10の場合、対象物が領域内に10秒間滞在するとアラームがトリガーされます。範囲：[1-10]。 **感度** 背景画像と対象物の類似度。値が高いほど、検出アラームがより簡単にトリガーされます。 d. オプション：上記のステップを繰り返し、別の設定を設定します。
駐車検知	駐車検知は、高速道路や一方通行道路などにおいて駐車違反を検知するために使用されます。	
無人荷物検知	無人荷物検知は、手荷物、バッグ、危険物など、事前に定義された区域内に放置された物体を検知し、アラームがトリガーされた際に一連の措置を実行できます。	
物体除去検知	物体除去検出機能は、展示物など事前に定義された領域から除去された物体を検出します。アラームがトリガーされた際に、一連のアクションを実行できます。	
高速移動検出	高速移動検出は、不審な走り回りや追跡、速度超過、高速移動を検出するために使用されます。対象物が高速で移動した場合、アラームをトリガーし、武装ホストに通知を送信します。	

イベント名	イベント説明	ルール設定
	これにより、必要な措置を事前に講じることができます。	
人集まり検出	人集まり検出は、指定されたエリア内の人体の密度が設定値を超えた場合に、関連するアクションをトリガーするアラームを発生させるために使用されます。	a. ルール番号を選択してください。 b. 画像の上部にあるツールバーを使用して、検出ラインを描画します。 c. **パーセンテージ**を設定します。パーセンテージは、領域内の人体の密度を表します。閾値を超えると、デバイスがアラームを発生します。 d. オプション：上記のステップを繰り返し、別の設定を追加できます。

6. **「アラームスケジュール」**をクリックして、アラームスケジュールの種類を選択します。

注意

「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ム武装スケジュールを設定するか、タイムバー上のカーソルを移動し「00:00-24:00」をクリックして指定した時間スケジュールを設定できます。

7. **「リンク方法」**をクリックしてリンク方法を設定します。

表13-8 リンク方法の説明

リンク方法	説明
監視センターに通知	デバイスは、イベントが発生した際にリモートアラームホストに例外またはアラーム信号を送信できます。アラームホストとは、クライアントソフトウェア（例：iVMS-4200、iVMS-5200）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た場合、ローカルモニターにアラームポップアップウィンドウが表示されます。
ブザー	アラームが検出されると、ブザーが音で鳴ります。
メール送信	アラームが検出された場合、システムはアラーム情報をユーザーまたは複数のユーザーにメールで送信できます。
アラーム出力	アラーム出力は、アラーム入力、動作検出、ビデオ改ざん検出、顔検出、線越え検出、およびその他のすべてのイベントによってトリガーされます。
記録	アラームが検出された場合、選択されたチャンネルが動画を記録します。

リンク方法	説明
	注意 チャンネルの動画記録スケジュールが有効になっていない場合、この連携は無効になります。動画記録スケジュールを設定するには、**システム → ストレージ管理 →→ ストレージスケジュール →→ 動画記録**に移動してください。

8. **保存**をクリックします。

13.1.4 対象イベント

開始前に

→接続されたカメラがこの機能に対応していることを確認するか、デバイスエンジンで**イベントセンター（→）**の**「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「動画構造化アルゴリズム」が有効になっていることを**確認してください**。

手順

1. **イベントセンター**に移動し、**→→ →→ →イベント設定 →→ →ターゲットイベントを選択します**。

2. カメラを選択します。

3. イベントを選択します。

4. **有効化を**オンにします。

5. イベントルールを設定します。

イベント名	イベントの説明	ルール設定
顔検出	顔検出機能は、シーン内に表示される顔を検出・キャプチャします。人間の顔が検出された際に、連携アクションを実行できます。	-
顔画像比較	この機能は、検出された顔画像と指定されたリストライブラリ内の画像と比較します。比較が成功した場合、アラームをトリガーします。	• ターゲットのグレード設定をサポートします。顔画像比較は、ターゲットのグレードが比較要件を満たした際に開始されます（瞳孔距離が設定された閾値より大きく、傾き角度とパン角度が設定された閾値より小さい場合）。 • 比較に失敗した場合と成功した場合のメッセージ設定をサポートします。

イベント名	イベント説明	ルール設定
不審者検出	動画内にリストライブラリにない顔が表示された場合、その顔をストレンジャーとして検出します。	• ターゲットのグレード設定をサポートしています。ターゲットのグレードが比較要件を満たした時点で顔画像の比較が開始されます（瞳孔距離が設定された閾値より大きく、傾き角度とパン角度が設定された閾値より小さい場合）。 • 見知らぬ人を検出する際の通知メッセージの設定をサポートしています。
マルチターゲット検出	マルチターゲットタイプ検出は、シーン内で顔、人体、車両を同時に検出する機能です。	-

6. **「武装スケジュール」**をクリックして、武装スケジュールの種類を選択してください。

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ム武装スケジュールを設定できます。または、タイムバー上でカーソルを移動し、「00:00-24:00 」をクリックして指定した時間スケジュールを設定できます。

7. **「リンク方法」**をクリックして、リンク方法を設定します。

表13-9 リンク方法の説明

リンク方法	説明
監視センターに通知	デバイスは、イベントが発生した際に、リモートアラームホストに例外またはアラーム信号を送信できます。アラームホストとは、クライアントソフトウェア（例：iVMS-4200、iVMS-5200）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た場合、ローカルモニターにアラームポップアップウィンドウが表示されます。
ブザー	アラームが検出されると、ブザーが音で鳴ります。
メール送信	アラームが検出された場合、システムはアラーム情報をユーザーまたは複数のユーザーにメールで送信できます。
アラーム出力	アラーム出力は、アラーム入力、動作検出、動画改ざん検出、顔検出、線越え検出、およびその他のすべてのイベントによってトリガーされます。
録画	アラームが検出された場合、選択されたチャンネルで動画を記録します。

連携方法	説明
	注意 チャンネルで動画記録スケジュールが有効になっていない場合、この連携は無効になります。動画記録スケジュールを設定するには、**システム → ストレージ管理 →→ ストレージスケジュール →→ 動画記録**に移動してください。

8. **保存**をクリックします。

13.1.5 熱画像カメラ検出

NVRは、熱画像ネットワークカメラのイベント検出モードに対応しています：火災検出、煙検出、温度検出、温度差検出など。

開始前に

熱画像ネットワークカメラをデバイスに追加し、カメラが有効になっていることを確認してください。

手順

1. **イベントセンター**に移動**します→** **→イベント設定→ 熱イベント**。

2. カメラを選択します。

3. イベントの種類を選択します。

4. **「有効」**をオンにします。

5. **ルール設定**をクリックしてルールを設定します。

表 13-10 熱イベント

イベント名	イベント説明
火災検出	火災が武装区域で検出された場合にアラームが作動します。
温度検知	温度が閾値を超えた場合にアラームが鳴動します。
周辺保護	周辺保護イベントには、線越え検出、侵入検出、区域進入検出、および区域退出検出が含まれます。

6. **「武装スケジュール」**をクリックして、武装スケジュールタイプを選択してください。

注

武装スケジュールを「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ム武装スケジュールを設定するか、タイムバー上のカーソルを移動し「00:00-24:00」をクリックして指定した時間スケジュールを設定できます。

7. **「リンク方法」**をクリックしてリンク方法を設定します。

表13-11 リンク方法の説明

リンク方法	説明
監視センターへの通知	デバイスは、イベントが発生した際に、リモートアラームホストに例外またはアラーム信号を送信できます。アラームホストとは、クライアントソフトウェア（例：iVMS-4200、iVMS-5200）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、ローカルモニターにアラームポップアップウィンドウが表示されます。
ブザー	アラームが検出されると、ブザーが音で鳴ります。
メール送信	アラームが検出された場合、システムはアラーム情報をユーザーまたは複数のユーザーにメールで送信できます。
アラーム出力	アラーム出力は、アラーム入力、動作検出、ビデオ改ざん検出、顔検出、ラインクロス検出、およびその他のすべてのイベントによってトリガーされます。
記録	アラームが検出された場合、選択されたチャンネルが動画を記録します。 **注意** 動画記録スケジュールがチャンネルで有効になっていない場合、この連携は無効になります。動画記録スケジュールを設定するには、**システム → ストレージ管理 →→ ストレージスケジュール →→ 動画記録**に移動してください。

8. **保存**をクリックします。

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アクションを設定します。

手順

1. **イベントセンター →** **→ イベント設定→ アラーム入力イベント** を選択します。

2. アラーム入力の名前を選択します。

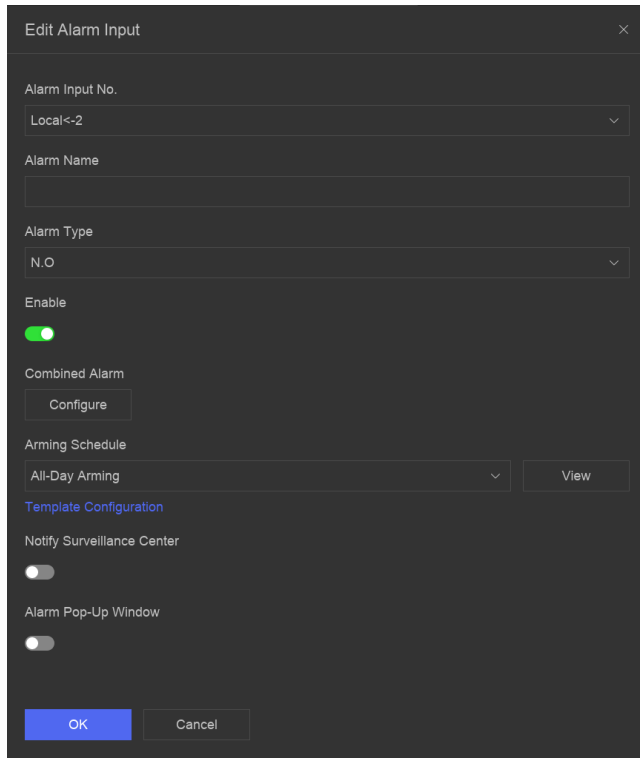


図13-5 アラーム入力の設定

注

例えば、**Local<-1 は、**デバイス背面パネルの警報入力番号が 1 であることを表します。

3. **アラーム名を**変更します。
4. **アラームタイプ**を設
   定します。**N.O**
   接点が自然状態かつ電源オフ状態のとき、2つの接点がオフの場合、それらをノーマルオープンと呼ぶことができます。
   N.C
   接点が自然状態かつ電源オフの状態において、2つの接点が導通している場合、それらを常閉と呼びます。
5. **有効化を**オンにします。
6. **オプション：**ステップ2で**「Local<-1」**を選択した場合、処理方法を選択してください。
   - **プロセスアラーム入力**を選択し、その後、対応するアラーム設定スケジュール、連動方法などを設定できます。

     注

     以下の操作は、この処理方法を選択した際にすべて利用可能です。
   - **クイック解除**を選択すると、すべてのイベントの連携方法が無効になります。
7. **「設定」**をクリックして、複合アラームを設定します。

1) チャンネルを選択します。

2) モーション検出やビデオ改ざん検出などの複合アラームイベントを選択します。

3) 「**OK**」をクリックします。

両方のアラーム入力とイベントからアラームを受信した際に、複合アラームがトリガーされます。

8. 「**アラームスケジュール**」をクリックして、アラームスケジュールタイプを選択します。

注意

「**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ム武装スケジュールを設定するか、タイムバー上のカーソルを移動し「00:00-24:00」をクリックして指定した時間スケジュールを設定できます。

9. 「**リンク方法**」をクリックしてリンク方法を設定します。

表13-12 リンク方法の説明

リンク方法	説明
監視センターに通知	デバイスは、イベントが発生した際にリモートアラームホストに例外またはアラーム信号を送信できます。アラームホストとは、クライアントソフトウェア（例：iVMS-4200、iVMS-5200）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、ローカルモニターにアラームポップアップウィンドウが表示されます。
ブザー	アラームが検出されると、ブザーが音で鳴ります。
メール送信	アラームが検出された場合、システムはアラーム情報をユーザーまたは複数のユーザーにメールで送信できます。
アラーム出力	アラーム出力は、アラーム入力、動作検出、ビデオ改ざん検出、顔検出、ラインクロス検出、およびその他のすべてのイベントによってトリガーされます。
記録	アラームが検出された場合、選択されたチャンネルが動画を記録します。 **注意** 動画記録スケジュールがチャンネルで有効化されていない場合、この連携は無効になります。動画記録スケジュールを設定するには、**システム → ストレージ管理 →→ ストレージスケジュール →→ 動画記録**に移動してください。

10. **保存**をクリックします。

13.1.7 音声分析イベント

手順

1. **イベントセンター**に移動し、**→ → → →→ → イベント設定 →→ → オーディオ分析を選択します。**

2. チャンネルを選択します。

3. イベントの種類を選択します。

4. **「有効」**をオンにします。

5. **ルール設定**をクリックしてルールを設定します。

表13-13 オーディオ分析イベント

イベント名	イベント説明	ルール設定
オーディオ例外検出	音声異常検出は、シーン内の異常な音（例えば、音の強度の急激な増加/減少）を検出します。	**音の強度急上昇検出**シーン内の急激な音の**強度**上昇を検出します。**音の強度急低下検出** シーン内の急激な音の低下を検出します。 **感度** 値が高いほど、検出アラームがトリガーされやすくなります。 **音量閾値** 環境内の音をフィルタリングします。環境音が大きいほど、値を高く設定する必要があります。環境に応じて調整してください。

6. **「武装スケジュール」**をクリックして、武装スケジュールの種類を選択します。

注意

「Arming Schedule」を**「Custom」**に設定すると、タイムバー上でカーソルをドラッグしてカスタムの武装スケジュールを設定できます。または、タイムバー上でカーソルを移動し、「00:00-24:00」をクリックして指定した時間スケジュールを設定できます。

7. **「リンク方法」**をクリックして、リンク方法を設定します。

表13-14 リンク方法の説明

リンク方法	説明
監視センターに通知	デバイスは、イベントが発生した際にリモートアラームホストに例外またはアラーム信号を送信できます。アラームホストとは、クライアントソフトウェア（例：iVMS-4200、iVMS-5200）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た場合、ローカルモニターにアラームポップアップウィンドウが表示されます。
ブザー	アラームが検出されると、ブザーが音で鳴ります。
メール送信	システムは、アラームが検出された際に、ユーザーまたは複数のユーザーにアラーム情報を記載したメールを送信できます。

連携方法	説明
アラーム出力	アラーム出力は、アラーム入力、動作検出、動画改ざん検出、顔検出、線越え検出、およびその他のすべてのイベントによってトリガーされます。
記録	アラームが検出されると、選択されたチャンネルが動画を記録します。 **注意** チャンネルに動画記録スケジュールが有効になっていない場合、この連携は無効になります。動画記録スケジュールを設定するには、**システム → ストレージ管理 →→ ストレージスケジュール →→ 動画記録**に移動してください。

8. **保存**をクリックします。

13.2 リンク設定

イベントリンクのパラメーターを設定します。

手順

1. **イベントセンター**に移動 →⚙ → **イベント設定**→ リンク設定または**システム**→ **イベント設定** →⚙ → **イベント設定** → **リンク設定**。

2. **メール**をクリックしてメールパラメーターを設定します。

表13-15 メール連携

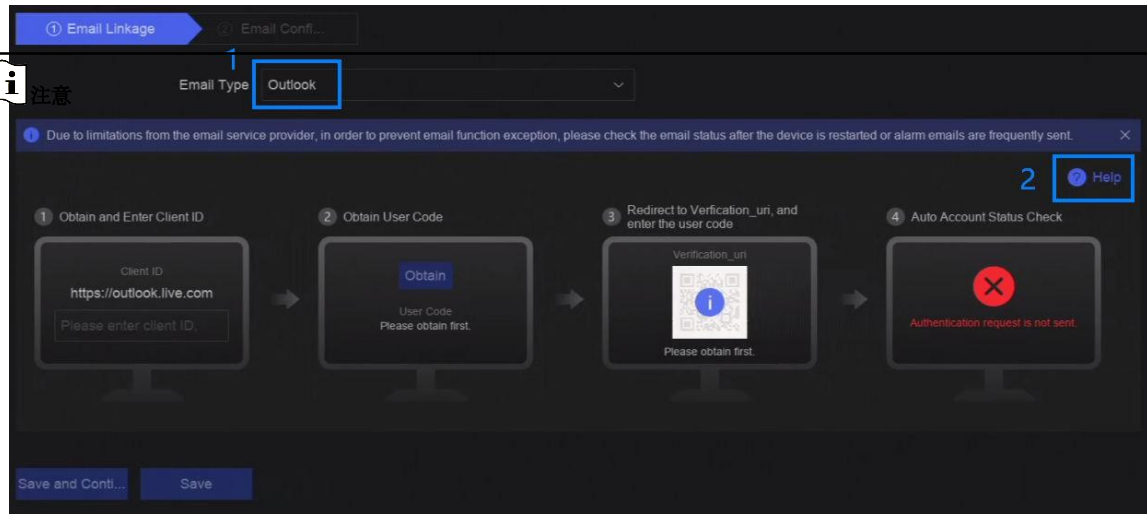
項目	説明
サーバー認証	SMTP サーバーがユーザー認証を要求する場合に有効にし、ユーザー名とパスワードを適切に入力してください。
SMTP サーバー	SMTP サーバーの IP アドレスまたはホスト名（例：smtp.263xmail.com）。
SMTP ポート	SMTP ポート。SMTP で使用されるデフォルトの TCP/IP ポートは 25 です。
SSL/TLSを有効にする	SMTP サーバーが SSL/TLS を要求する場合、SSL/TLS を有効にします。
送信者	送信者の名前。
送信者のアドレス	送信者のアドレス。
受信者を選択	受信者を選択します。最大3件の受信者を設定できます。
添付画像	アラーム画像を添付してメールを送信します。

アイテム	説明
周辺保護用に3つの添付画像有効化	周辺保護イベントがトリガーされた場合、デバイスは3つの添付アラーム画像を含むメールを送信します。
間隔	添付画像の撮影間隔。

注

Outlookメールアカウントを使用している場合は、**メールの種類を「Outlook」**に設定し、右側の**「ヘルプ」**をクリックして設定手順を確認し、画面の指示に従って設定を完了してください。

図13-6 Outlookメール設定



注意

3. アラーム連携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」**をクリックしてください。

   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フラッシュドライブからオーディオファイルをインポートできます。ファイルはAACまたはMP3形式で、各ファイルのサイズは1MB以内である必要があります。

4. IPスピーカーが接続されている場合、**IPスピーカー**をクリックして、選択したIPスピーカーにアラーム連携用のオーディオファイルをインポートします。

注意

- この連携機能は、一部のイベントタイプでのみ利用可能です。
- アップロードするオーディオファイルはMP3、WAV、またはACC形式で、ファイルサイズは1MB未満である必要があります。

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ーを設定します。

注意

- 各アラーム出力の名前をクリックして編集します。
- アラーム出力番号は、デバイス背面パネルの番号と同一です。例えば、**Local->1**

  は、デバイス背面パネルのアラーム出力番号**1**を意味します。

遅延

アラーム信号の持続時間です。

アラーム状態

トリガーをクリックしてステータスを切り替えます。

6. オーディオとライトカメラを接続している場合、カメラのフラッシュライトとカメラスピーカーのパラメーターをアラーム連携用に設定するには、**「カメラ オーディオとライト設定」**をクリックします。

注意

この連携機能は、一部のイベントタイプでのみ利用可能です。

7. セキュリティ制御パネルが接続されている場合は、**セキュリティ制御パネル**をクリックして、IPアドレスやポート番号などのパラメーターを設定してください。

13.3 解除設定

解除テンプレートを設定すると、そのテンプレートを使用してチャンネルをバッチ処理で解除できます。**解除を許可している**チャンネルは、解除テンプレートに従ってアラーム連携項目をトリガーしません。

手順

1. **イベントセンター**に移動し、→→→→ **Event Configuration** →→ → **Linkage Configuration** または **System** →→ → **Event Configuration** → → **Event Configuration** → **Linkage Configuration** を選択します。

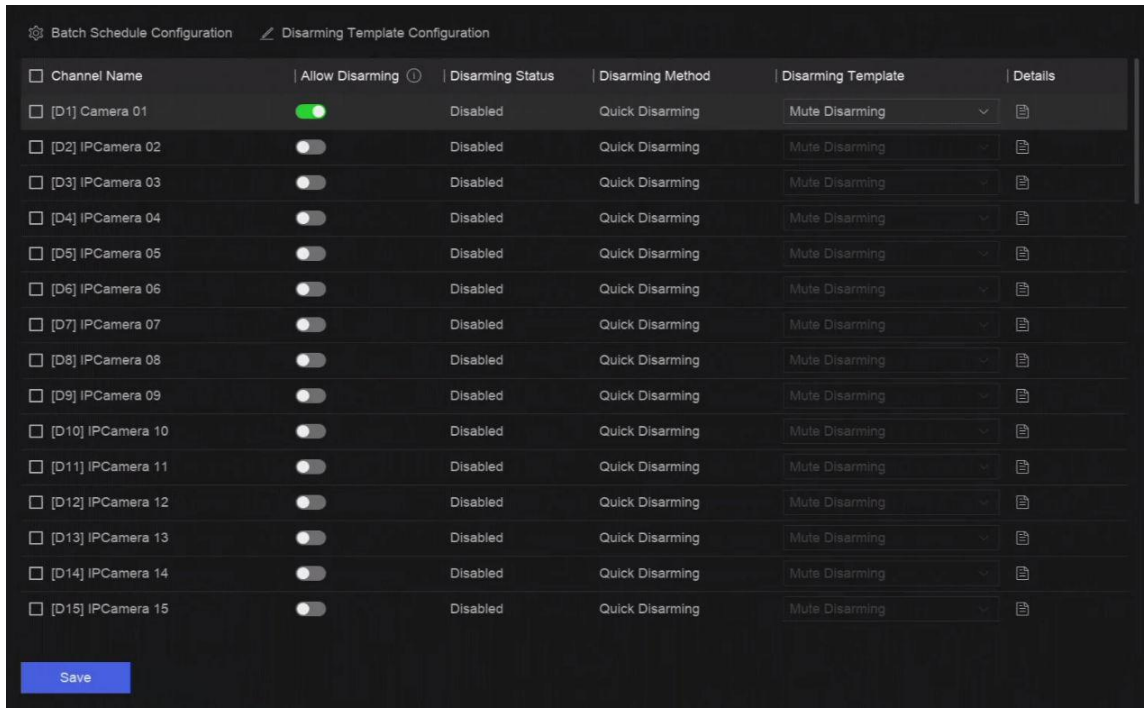


図13-7 解除設定

2. 解除を許可するチャンネルを選択します。
3. **バッチ スケジュール設定**をクリックします。
4. **「有効」を**オンにします。
5. **無効化テンプレート**を選択してください。利用可能なタイプは2種類のみです

注意

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

6. **OK**をクリックしてください。

13.4 バッチ設定

イベントセンター（→ ）の**「→」→「Event Configuration」→「Batch Configuration」**または**「System」→「Event Configuration」→「」→「Event Configuration」→「Batch Configuration」**から、一覧表示されたイベントと対応する**「Notify Surveillance Center」**のリンクアクションをバッチ処理で有効/無効に設定できます。イベントを有効にした後、ルールを設定するには**「Go to Event Configuration」**をクリックしてください。

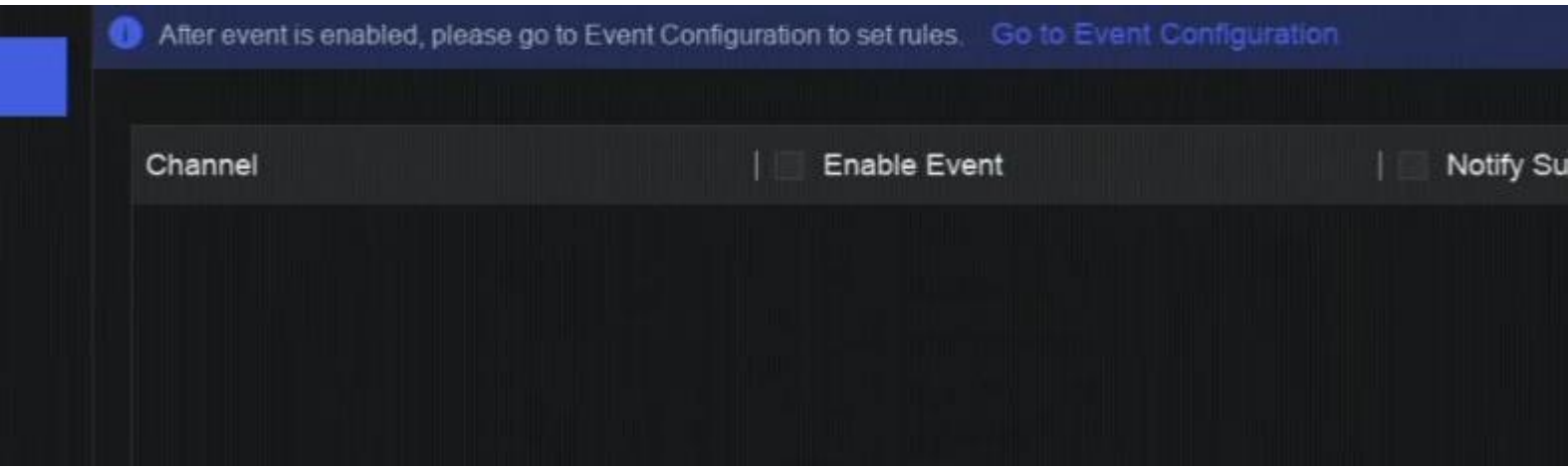


図13-8 バッチ設定

13.5 イベント検索

動画や画像などのイベントファイルを、検索条件に応じて検索できます。

手順

1. **イベントセンター**に移動します→。

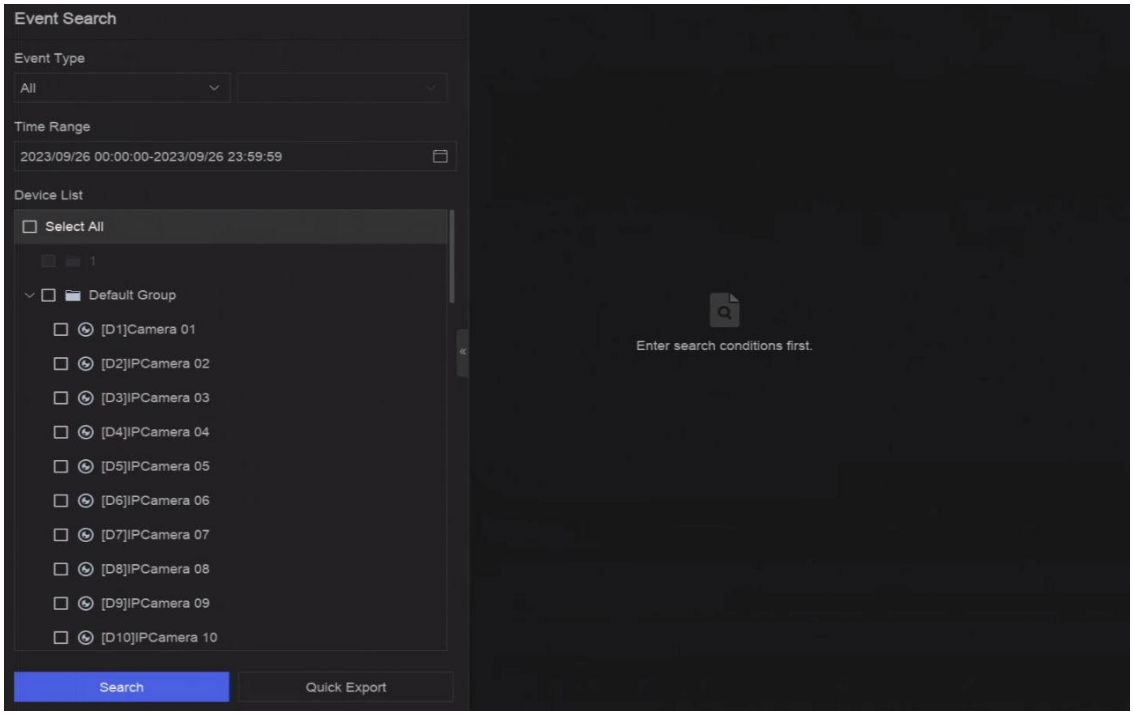


図13-9 イベント検索

2. イベントの種類、日時、チャンネルなど、詳細な条件を指定します。
3. **検索**をクリックします。
   選択したチャンネルの検索結果が表示されます。

次に実行する操作

結果リストからアイテムを選択し、バックアップ用にエクスポートします。

13.6 アラームを表示

リアルタイムのアラーム動画と画像を確認し、再生することができます。

手順

1. **イベントセンター**に移動→  。
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。
   アラームが多数ある場合は、**フィルター**をクリックして検索し、アラームを見つけてください。
4. **「再生」**をクリックすると、アラームの録画動画が再生されます。
5. 右側にアラームの画像が表示されます。利用可能な画像の数が一覧表示されます。

第14章 検索とバックアップ

ファイルは、ファイルの種類、イベントの種類、日時、タグなど、さまざまな検索条件に基づいて検索できます。検索結果は、USB フラッシュドライブなどの別のデバイスにエクスポートできます。

開始前に

HDDが正しくインストールされており、記録パラメーターが適切に設定されていることを確認してください。

手順

1. **バックアップ**に移動します。

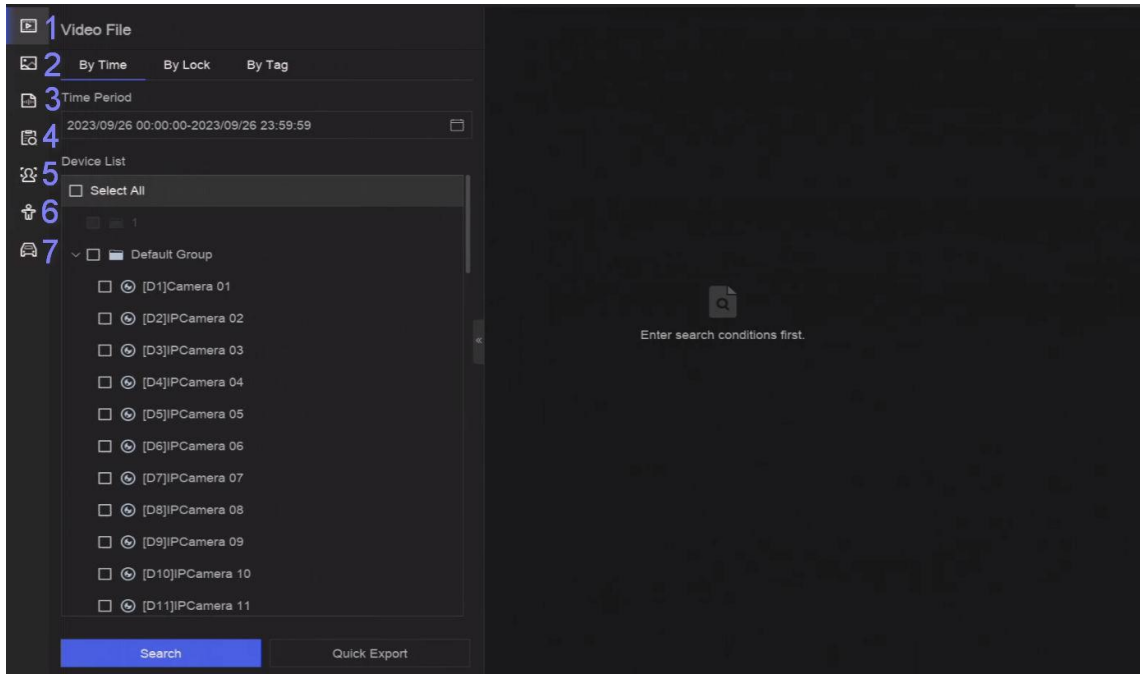


図14-1 検索とバックアップ

2. 左側の検索方法からご希望のものを選択してください。7種類がサポートされています。

注意

検索条件は、選択した検索方法によって異なります。

3. 検索条件を設定します。
4. **検索**をクリックします。

図14-2 検索結果

5. オプション：以下の操作を実行します。

1 ファイルを選択します。

2 ファイルをクリックしてロックします。ファイルがロックされると、上書きされなくなります。

3 ファイルをエクスポートするにはクリックします。

4 上部ツールバーを使用して、結果をチャンネルでフィルタリングします。

5 上部のツールバーを使用して、表示効果を切り替えます。

6 異なる結果ページに移動します。

7 インターフェースを展開または折りたたみます。結果リストから動画を選択すると、すぐに再生できます。

6. バックアップのためにUSBフラッシュドライブをデバイスに挿入します。

7. ファイルをUSBフラッシュドライブにエクスポートします。

- 結果リストからファイルを選択し、[**エクスポート**]をクリックします。
- 「**すべてエクスポート**」をクリックしてすべてのファイルをエクスポートします。

第15章 AcuSeek

AcuSeekは、関連するテキスト説明を入力するだけで、希望の画像や動画クリップを効率的かつ正確に検索できます。

開始前に

- AcuSeekに対応したカメラを追加し、カメラの録画スケジュールを設定していることを確認してください。
- AcuSearchエンジンを設定していることを確認してください。***AcuSearch***を参照してください。

手順

1. **イベントセンターに移動→ イベント設定→ スマート設定→ アルゴリズム管理 → スマート検索**を選択し、対応するチャンネルのターゲット分析にチェックを入れます。

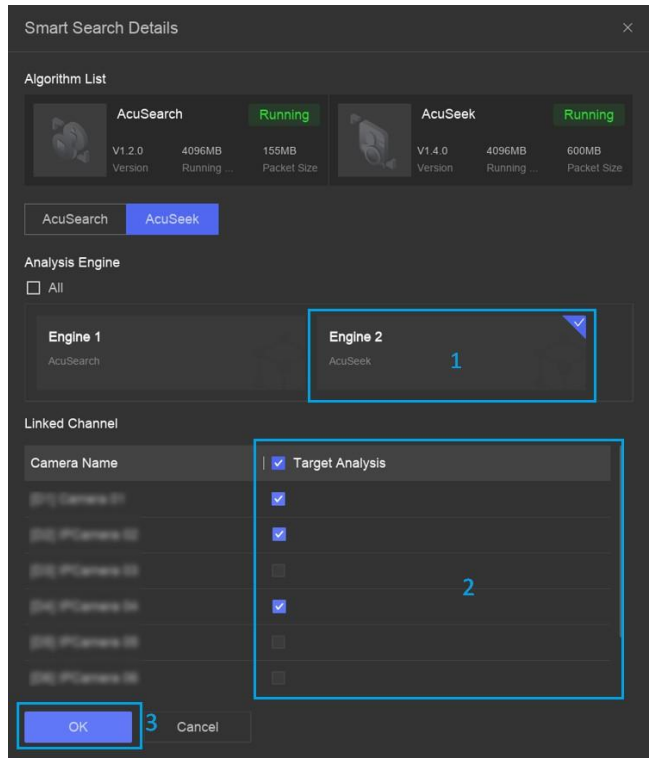


図15-1 AcuSeekエンジンを設定する

2. GUI のメインページで **AcuSeek** をクリックし、実際の要件に応じて条件を設定します。

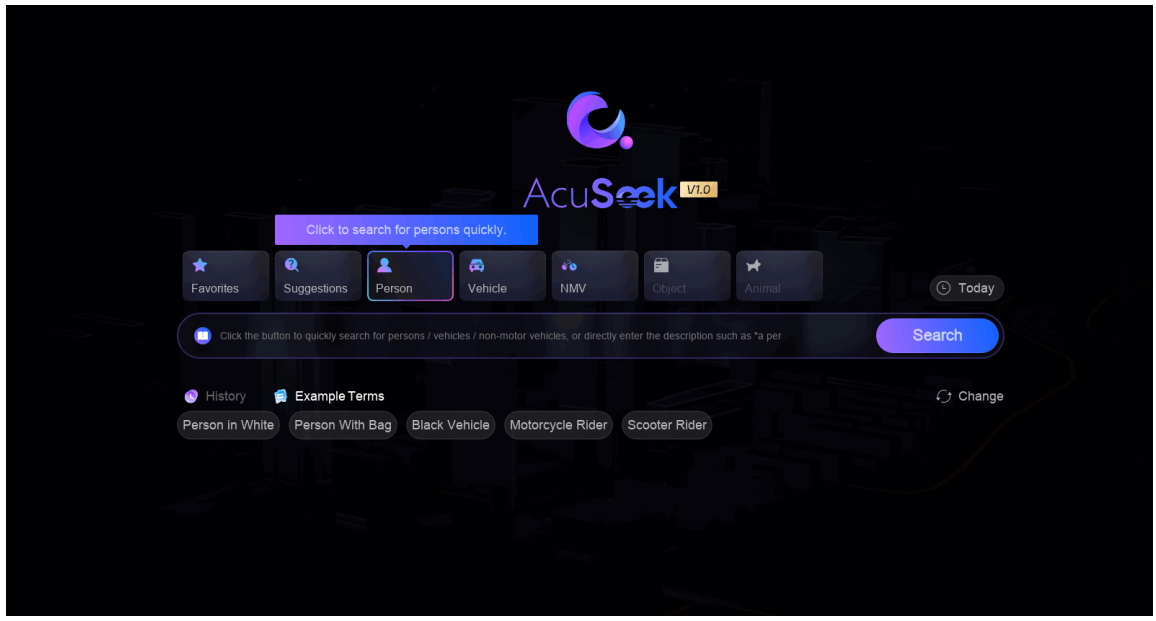


図15-2 検索条件の設定

- (推奨) 「**提案**」をクリックし、**人**、**車両**、**またはNMV**を選択し、事前定義された条件から選択します。人または車両を検索する際は、複数の観点から条件を選択できます。例えば、黄色のトップス、青のボトムス、帽子を着用している人を検索できます。
- 検索ボックスに条件を入力します。
- 「**お気に入り**」をクリックして、お気に入りから条件を選択します。
  カスタムをクリックして、お気に入りに用語を追加できます。
- 「**今日**」をクリックし、検索対象の期間（3日、7日、カスタム）を定義します。
- 検索ボックスの下にある履歴検索条件または例示用語をクリックしてください。履歴検索条件を「お気に入り」に追加するには、「☆」をクリックしてください。

3. 「**検索**」をクリックして検索結果を表示し、以下の図に従って追加の操作を実行してください。

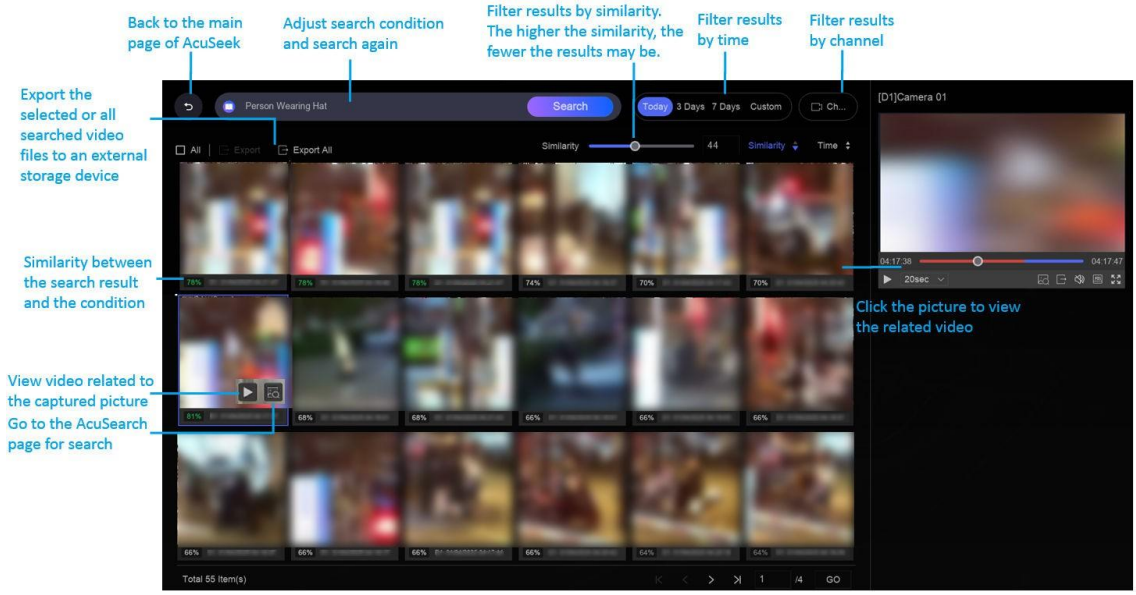


図15-3 AcuSeek 検索結果

第16章 AcuSearch

AcuSearch機能は、ライブビューまたは再生中に動画シーンから人間の顔や体の画像を抽出します。その後、抽出された画像と記録された動画を比較し、最終的にターゲットを含む動画を検出します。

開始前に

デバイスまたはカメラがこの機能に対応していることを確認してください。

手順

1. →**システム設定**に移動し、**システム設定 > スマート設定 >→ アルゴリズム設定 >→ アルゴリズム管理に移動**し、AcuSearch アルゴリズムを有効にします。
   - **カメラによる AI**: カメラが AcuSearch 分析を実行します。
   - **AI by NVR**: 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再生画面に移動し、動画再生中に画面左下にある「  」をクリックします。

注意

- 再生中にターゲットが探しにくい場合は、ターゲットを含むシーンを検索するために**「スマート検索」**（）を使用することをおすすめします。
- 人間の顔と体は異なる色で枠で囲まれます。
-  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したりすることもできます。

3. クリック  をクリックします。

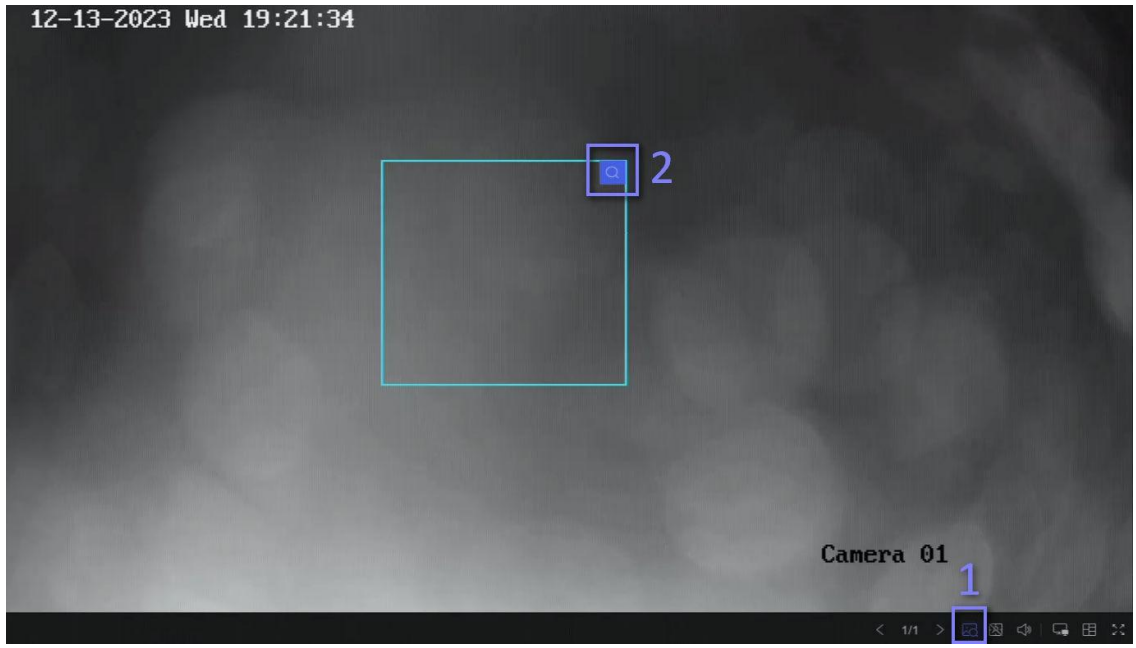


図16-1 AcuSearch

比較対象の動画が見つかった場合、デバイスはAcuSearchインターフェースにリダイレクトされます。

4. 検索結果を表示します。

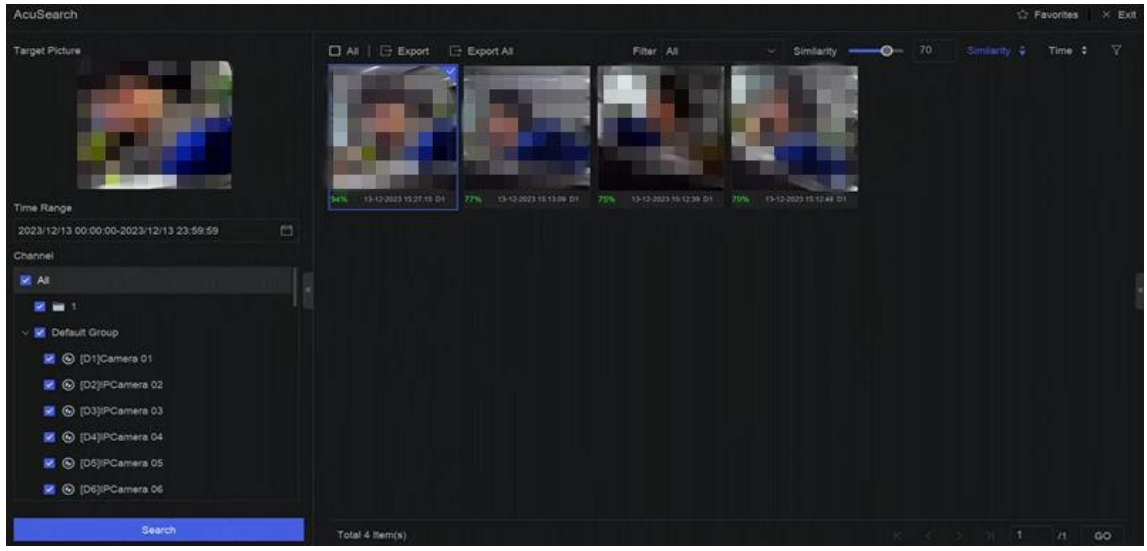


図16-2 AcuSearch 検索結果

5. オプション：検索結果が希望と異なる場合、**時間範囲**、**チャンネル**、または**類似度**を調整して再検索できます。

6. **オプション：**結果リストからアイテムを選択すると、対応する動画が右側に再生され、赤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実行が可能です。

第17章 スマート設定

17.1 アルゴリズム管理

アルゴリズムは、デバイスエンジンがさまざまなスマート機能を分析するために使用されます。スマート機能は、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可能になります。

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** を選択します。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クリックしてエンジンにリンクできます。

一部のモデルでは、AcuSearchアルゴリズムに対応している場合、カメラ（**AI by Camera**）またはNVR（**AI by NVR**）を選択してAcuSearchアルゴリズムを実行できます。

17.2 エンジン状態

エンジンの状態（実行状態、温度、アルゴリズム名）を確認できます。

システム設定に移動し、**→ イベント設定→ イベント設定→ スマート設定→ エンジン**状態または**イベントセンター→ イベント設定→ スマート設定→ エンジン状態**。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。

17.3 タスク計画管理

タスクのステータスはタスク設定で確認できます。スマート分析結果は、興味のある人体や車両の画像を検索する際の画像フィルタリングに利用されます。

システム → イベント設定 → イベント設定 → スマート設定 → タスク計画管理 または **イベントセンター → イベント設定 → スマート設定 → タスク計画管理** へ移動します。**非リアルタイム対象の比較では**、各日の進捗状況を確認できます。

タスクの状態は主に3つの条件で構成されます：**無効**、**待機中**、**有効**。**無効**

カメラで分析タスクが有効化されていません。

待機

カメラの分析タスクが有効化されています。デバイスはデータ分析を待機中です。

有効

カメラの分析タスクが有効化されており、デバイスはカメラのデータを分析中です。

17.4 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。**ストレンジャーズ**ライブラリは、知らない人の画像を保存するために使用され、削除することはできません。

17.4.1 リストライブラリを追加する

手順

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」**をクリックします。
3. ライブラリ名を入力します。
4. **確認**をクリックします。

注

- ライブラリ一覧を表示した後、編集または削除したいライブラリにカーソルを移動できます。
- **バッチ削除**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内のすべての画像を削除したりできます。

17.4.2 ライブラリに顔写真をアップロードする

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行われます。単一のターゲット画像をアップロードするか、複数のターゲット画像をライブラリにインポートできます。

開始前に

- 画像形式がJPEGまたはJPGであることを確認してください。
- 事前にすべての画像をバックアップデバイスにインポートしてください。

手順

1. リストライブラリをダブルクリックします。
2. **オプション：カスタムタグ**をクリックして画像にタグを追加します。タグは自由に編集可能です。例：個人情報、組織、役職など。
3. **「追加」**または**「インポート」**をクリックします。
4. 画像をインポートします。
   - **追加**：[ ]をクリックして、1枚ずつ画像をアップロードします。画像に複数のターゲットがある場合は、その中から1つを選択する必要があります。
   - **インポート**: 複数の画像を一度にインポートできます。デバイスはファイル名を画像名として使用し、他の属性を空のままにします。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。画像に複数のターゲットが含まれる場合、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:** 以下の操作を実行します。

ライブラリから画像を削除	• 画像を選択し、削除します。 • 画像を選択し、**バッチ削除**をクリックして選択した画像を削除します。
画像を検索する ライブラリ	クリック  ツールバーの「検索」をクリックして画像を検索します。
画像を別のライブラリにコピー	画像を選択し、**「コピー先」**をクリックして、現在のライブラリにアップロードされた画像を別のライブラリにコピーします。
画像の編集	画像の名前をクリックし、その属性を編集します。
画像をエクスポート	画像を選択し、**エクスポート**をクリックしてUSBフラッシュドライブにエクスポートします。 ドライブにエクスポートします。

17.5 自己学習設定

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ます。自己学習機能が有効になっている場合、デバイスは自動的に誤報データを収集し、収集したデータを使用して対応するアルゴリズムを継続的に訓練し最適化します。

→→→→システム設定→ 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**に移動し、**自己学習**アルゴリズムを有効にします。

注意

- この機能は一部のモデルのみに対応しています。
- 現在、自己学習機能は周辺保護イベントにのみ適用可能です。
- デバイスにエンジンが**1**つしかない場合、**NVRのAI**機能を無効化し、カメラが検出対象の分析を実行する必要があります。デバイスにエンジンが**2**つ以上ある場合、**NVRのAI機能を**有効化し、**1**つのエンジンで検出対象の分析を実行し、もう**1**つのエンジンで自己学習アルゴリズムを実行できます。

17.5.1 自己学習タスク管理

自己学習アルゴリズムが実行中である場合、自己学習タスクも有効にする必要があります。

システムに移動**→ イベント設定→ イベント設定→ 自己学習→ タスク管理**

または**イベントセンター→ イベント設定→ 自己学習→ タスク管理** を選択し、タスクを有効にします。

利用可能なタスクが一覧表示され、タスクの状態と進捗バーを確認できます。材料の収集には時間がかかります。

タスクが完了すると、自己学習アルゴリズムが自動的に更新されます。クリックできます

Auto Update Config をクリックして**更新時間を**設定できます。

注意

- 自己学習アルゴリズムが更新中の場合、周辺保護イベントに対して自己学習アルゴリズムが利用できない場合があります。
- **強制トレーニングは**技術サポート専用です。

17.5.2 モデル管理

自己学習アルゴリズムのモデルバージョンを要件に応じて設定できます。**システム→ イベント設定→ イベント設定→ 自己学習→ モデル管理で**モデルバージョンを設定します。

以前のバージョンに復元

このバージョンよりも前のバージョンにモデルを復元します。

デフォルトバージョンに復元

モデルを工場出荷時のデフォルト設定に戻します。

17.5.3 スマートステータス

→各チャネルの自己学習アルゴリズムのパフォーマンス状態は、**システム設定 → イベント設定 → 自己学習→ イベント設定→ 自己学習→ スマートステータス**または**イベントセンター→ イベント設定 → 自己学習 → スマートステータスで確認**できます。

第18章 アプリケーションセンター

18.1 人間と車両の検出

選択し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ます。

人間と車両の検出は事前に設定する必要があります。設定するには、**イベントセンター（→）**にアクセスし、に移動して設定を行ってください。

図18-1 人と車両の検出表18-1 人と車両の検出説明

番号	説明
1	右クリックショートカットメニュー。
2	人間と車両の検出設定。レイアウト、比較成功時の通知、およびリソースチャネルを設定できます。
3	フルスクリーン表示の切り替え。

18.2 人物チェックイン

チェックインタスクを追加すると、リアルタイムのチェックイン情報を確認したり、チェックイン結果を検索したりできます。

18.2.1 チェックインタスクの追加

人件費のチェックインを開始する前に、対応するタスクを適切に設定する必要があります。

開始前に

- 人顔認証用のカメラが正しく接続されています。
- **システム→ Smart Settings→ Algorithm Configuration→ Algorithm Management** に移動し、**ターゲット認識を**少なくとも1つのエンジンに割り当ててください。
- チェックイン比較用のリストライブラリが適切に設定されています。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。

手順

1. **「人チェックイン」**をクリックします。
2. 左側のメニューを表示するために右クリックします。
3. 「」をクリックします。
4. **「追加」**をクリックします。

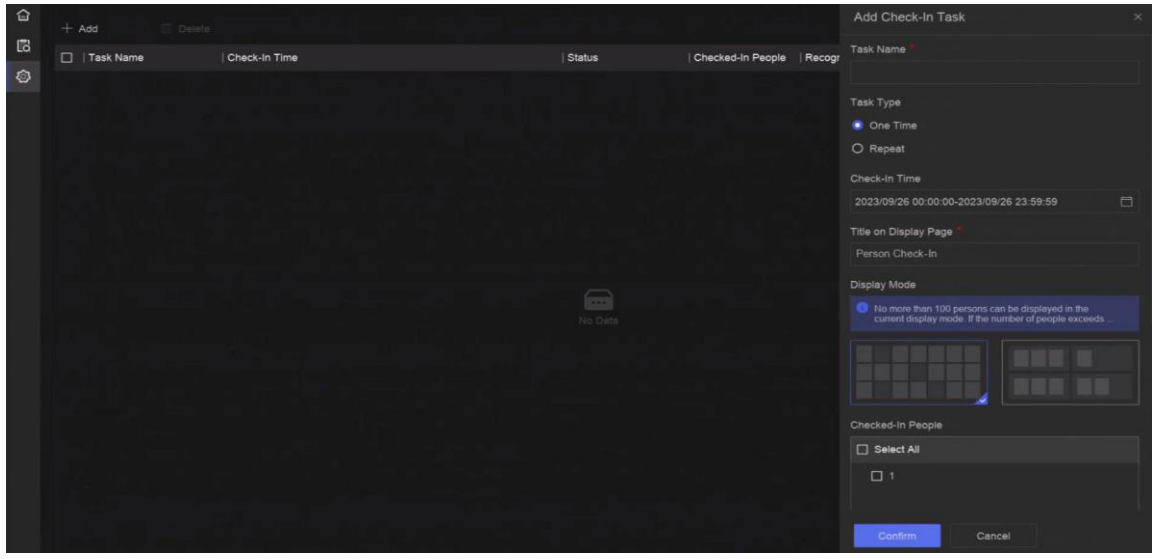


図18-2 チェックインタスクの追加

5. **タスク**を設定します。 **1回**

   限り

   このタスクは1回のみ使用されます。

   繰り返し

   タスクは複数回使用され、繰り返し実行されます。
6. **タスク名**、**チェックイン時間**、**認識チャネル**など、その他のパラメーターを設定します。
7. **確認**をクリックします。

18.2.2 チェックイン記録の検索

チェックインタスクを設定後、日または月単位で記録を検索できます。

開始前に

チェックインタスクが設定されていることを確認してください。

手順

1. 「**Person Check-In**」に移動します。
2. 右クリックして左側にメニューを表示します。
3. 「」をクリックします。

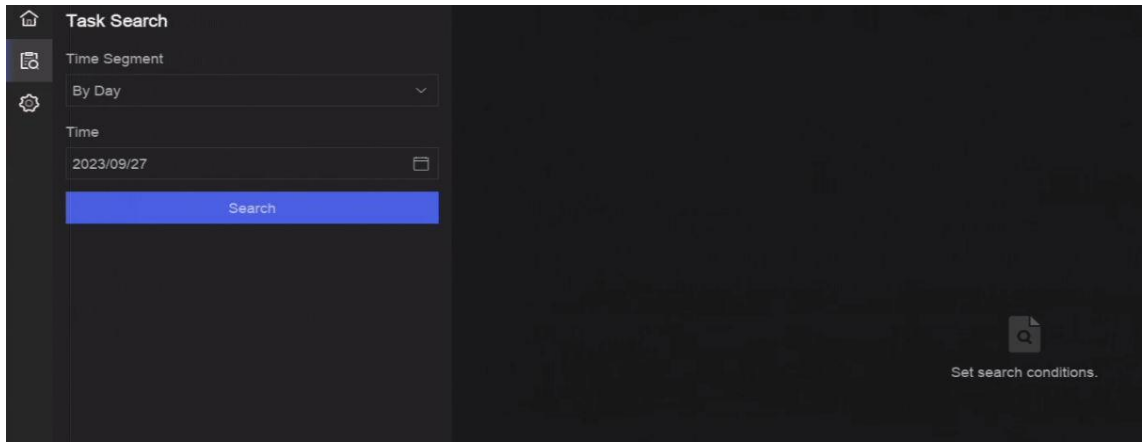


図18-3 チェックイン記録の検索

4. 時間を設定します。
5. **検索**をクリックします。

18.3 統計レポート

人数の集計レポートとヒートマップを表示できます。

表18-2 統計レポートの概要

機能名	アイコン	条件	説明
人数のカウント		• この機能は接続されたIPカメラでサポートされている必要があります。例えば、人数のカウント	人数のカウントは、設定された特定のエリアに出入りする人の数を計算し、分析用に日次/週次/月次/年次のレポートを作成します。

機能名	アイコン	条件	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に保存できます。	
ヒートマップ		• この機能は接続されたIPカメラでサポートされ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に保存できます。	ヒートマップはデータのグラフ表示です。ヒートマップ機能は、特定のエリアに訪れた人や滞在した人の数を分析するために使用されます。

第19章 システムパラメーター設定

システムパラメーターには、デバイス名、地域、時間、ロック画面時間、言語などが含まれます。**システム → システム設定 → システム構成**に移動してパラメーターを設定します。

表19-1 パラメーター説明

タイプ	パラメーター名	説明
基本情報	ロック画面時間	指定した時間、カーソルが動かない場合に画面がロックされます。
	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、この権限を持つカメラのライブ映像が再生されます。
地域と時間の設定	タイムゾーンのロック	この操作には管理者パスワードが必要です。**タイムゾーン**がロックされると、ウェブブラウザ経由のウェブインターフェースを含む他のプラットフォームやインターフェースから、デバイスのタイムゾーン情報をリモートで変更できなくなります。 **タイムゾーンの**ロックまたはロック解除は、ローカルGUIインターフェース経由でのみ可能です。
	タイムシンクモード	• **NTP タイム同期**: **NTP タイム同期**を選択し、**NTP サーバー**、**NTP サーバーポート**、**NTP クライアントポート**、および**間隔**を設定できます。間隔は、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、選択可能なサーバーアドレスにリストされているような、時間同期機能を備えたNTPサーバーを使用する必要があります。デバイスがカスタム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間同期用のNTPサーバーを構築できます。 • **手動タイムシンク**：システム時間を手動で設定します。 • **Hik-Connect サーバー時間同期**: デバイスは NTP サーバーではなく Hik-Connect と時間を同期します。 • **Guarding Vision サーバー時間同期**: デバイスはNTPサーバーではなく Guarding Visionと時間を同期します。
	DST	DST（夏時間）は、時計を1時間進める期間を指します。世界の一部地域では、最も暖かい月の夕方に日照時間を延長する効果があります。

タイプ	パラメーター名	説明
		DSTの開始時に、設定したDSTバイアスに応じて時計を一定期間進めます。標準時間（ST）に戻るときには、同じ期間分時計を戻します。
メニュー出力	補助ポート自動切り替え	後部パネルに2つ以上のモニターが接続されている場合、そのうち1つがメインメニューに入れない補助出力として設定される場合があります。補助出力ウィンドウに表示されている画像は、設定された間隔ごとに自動的に次の画像に切り替わります。
チャンネルゼロ	-	チャンネルゼロ（仮想チャンネル）は、デバイスのすべてのチャンネルのライブ画像を表示でき、伝送帯域幅を節約します。
RS-232	使用	**コンソール** コンバーターを使用してPCに接続すると、PCでデバイスのパラメーターを設定できます。 **透過チャネル** シリアルデバイスに直接接続されています。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20章 ホットスペアデバイスバックアップ

ビデオレコーダーはN+Mのホットスペアシステムを構成できます。このシステムは、複数の動作中のビデオレコーダーと少なくとも1つのホットスペアビデオレコーダーで構成されます。動作中のビデオレコーダーが故障した場合、ホットスペアビデオレコーダーが動作を開始し、システムの信頼性が向上します。図に示すような双方向接続を、ホットスペアビデオレコーダーと動作中のビデオレコーダーの間で構築する必要があります。

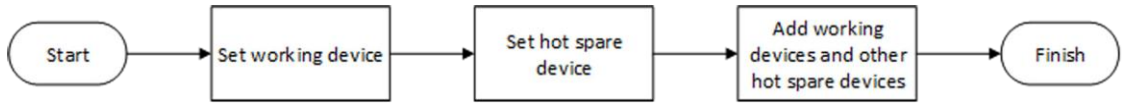


図20-1 ホットスペアシステムの構築

注

- 最大32台の動作デバイスと32台のホットスペアデバイスが許可されています。
- 互換性を確保するため、同じモデルのデバイスを使用することをおすすめします。ホットスペア機能に対応するモデルの詳細については、販売店にお問い合わせください。
- この機能は一部のモデルのみに対応しています。

20.1 作業用デバイスを設定する

手順

1. **システム→ システム管理→ N+M Hot Spare** を選択します。
2. **動作モードを「通常モード」**に設定します。
3. **有効を**オンにします。
4. **保存**をクリックします。
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 デバイスの動作状態**を確認します。

20.2 ホットスペアデバイスを設定します。

ホットスペアデバイスは、動作中のデバイスが故障した場合に、そのデバイスのタスクを引き継ぎます。

手順

1. **システム→ システム管理→ N+M Hot Spare** へ移動します。
2. **動作モードを「ホットスペアモード」**に設定します。
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。

注意

- デバイスがホットスペアモードで動作中は、カメラ接続が無効になります。
- ホットスペアモードの動作モードを通常モードに戻した後は、正常な動作を保証するため、デバイスのデフォルト設定を復元することを強く推奨します。

4. **システム**に移動し、**システム管理（→）を選択し、システム管理（→）を選択し、N+M ホットスペア（N+M Hot Spare）**を再度選択します。
5. 動作中のデバイスをホットスペアシステムに追加します。
6. ホットスペアデバイスをホットスペアシステムに追加します。
7. **保存**をクリックします。

第21章 例外イベントの構成

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トリガーとしてアラーム出力と連動動作を実行するように設定できます。

手順

1. **システム→ システム設定→ 例外** へ移動します。

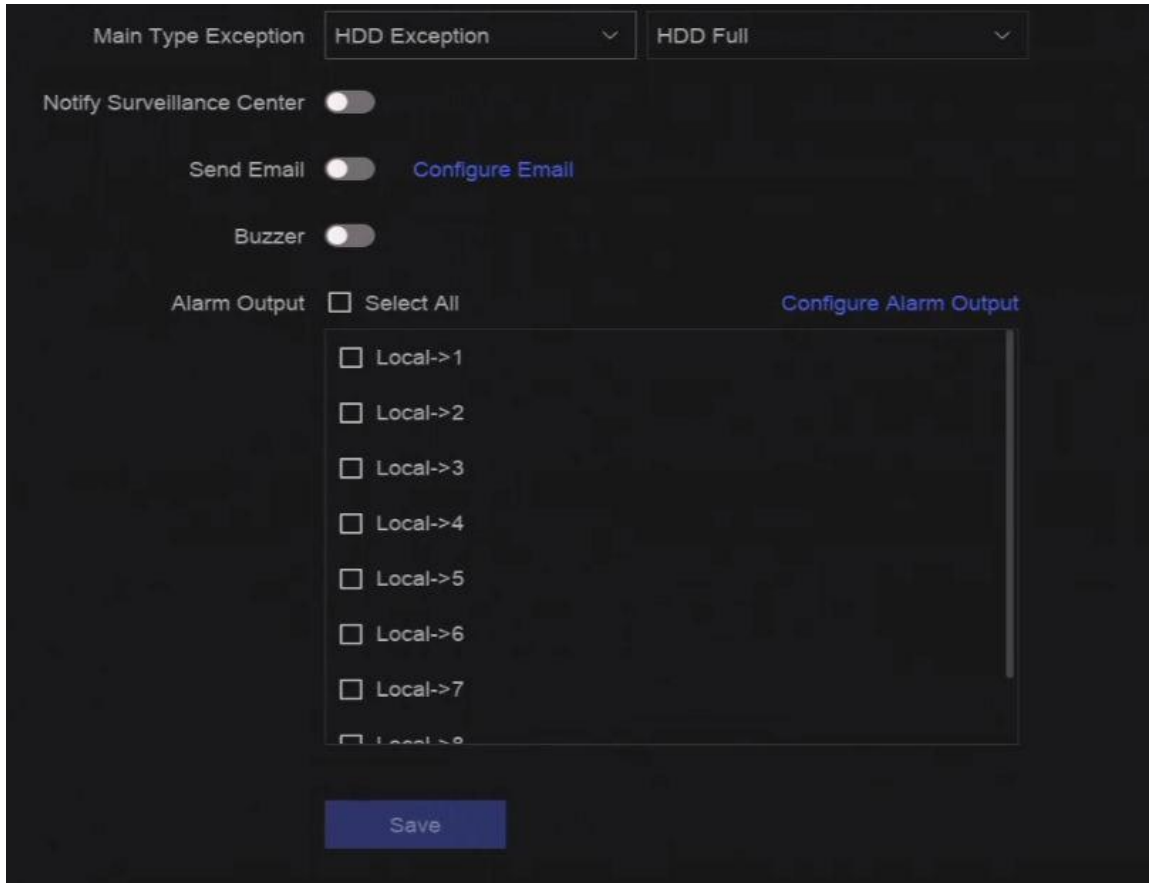


図21-1 例外イベントの設定

2. 例外の種類を選択します。

3. 連携方法を設定します。

表21-1 リンク説明

リンク方法	説明
監視センターへの通知	デバイスは、イベントが発生した際に、リモートアラームホストに例外またはアラーム信号を送信できます。アラームホストとは、クライアントソフトウェア（例：iVMS-4200、iVMS-5200）がインストールされたPCを指します。
ブザー	アラームが検出されると、ブザーが音で鳴ります。
メール送信	アラームが検出された場合、システムはアラーム情報をユーザーまたは複数のユーザーにメールで送信できます。
アラーム出力	アラーム出力は、アラーム入力、動作検出、ビデオ改ざん検出、顔検出、ラインクロス検出、およびその他のすべてのイベントによってトリガーされます。

注意

例外イベントが発生した場合、画面右上にある「」が通知し、をクリックして詳細を確認できます。

4. **「保存」**をクリックします。

第22章 システム情報の表示

システム → システムメンテナンス → 実行情報 → システム情報 に移動し、動画記録情報、HDD情報、ネットワーク情報、ライブビューまたは動画再生のストリーム情報、タイムシンク診断情報など、システム情報を確認できます。

デバイス異常が発生した場合（例：時間同期異常が発生し、RTC（コイン/ボタン電池）の電池が切れた場合）、動画の録画や再生に影響を与える可能性があります。異常をできるだけ早く解決してください。

第23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、アップグレードなどが含まれます。

23.1 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。

システム設定に移動し、**システムメンテナンス（→）**を選択し、**メンテナンス（→）を選択**し、**スケジュール再起動（→）**を選択して機能を有効にし、再起動スケジュールを設定します。

23.2 デバイスのアップグレード

デバイスシステムは、ローカルUSBフラッシュドライブ、リモートFTPサーバーなどからアップグレード可能です。

システム→ システムメンテナンス→ メンテナンス→ アップグレードを選択し、デバイスをアップグレードします。

23.3 バックアップと復元

→システム設定に移動し、**システムメンテナンスを選択します。→ メンテナンス→ バックアップと復元**を選択し、システムパラメーターの復元またはバックアップを行います。

設定ファイルのインポート/エクスポート

デバイス設定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でき、同じパラメーターで設定する複数のデバイスに、1つのデバイスの設定ファイルをインポートできます。

簡易復元

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動作モード、デフォルトルート、サーバーポートなど）および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設定に復元します。

工場出荷時設定

すべてのパラメーターを工場出荷時のデフォルト設定に戻します。

非アクティブ状態に復元

デバイスを非アクティブ状態に復元し、ユーザーアカウントの復元を除き、すべての設定を変更せずに保持します。

23.4 ログ情報

システム→ システムメンテナンス→ メンテナンス→ に移動し、ログを検索してエクスポートします。

有効期限設定

ログディスクが満杯になると、期間を超えたログが上書きされます。

23.5 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を取ることができます。

手順

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. **「有効」**をオンにします。
3. **アップロード時間**、**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: [テスト]** をクリックしてパラメーターが有効かどうかを確認します。
5. **保存**をクリックします。

23.6 メンテナンスツール

システムメンテナンス用に複数のツールが提供されています。例えば、S. M. A. R. T. 検出や不良セクタ検出などです。

開始前に

HDDが正しくインストールされていることを確認してください。

手順

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** を選択します。
2. 必要に応じてツールを選択してください。

表23-1 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監視は、ネットワークのパフォーマンス、可用性、または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を検出するために、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す。
ネットワークパケットキャプチャ	**Ping** Pingテストは、目的の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ます。 **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接続された後、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、エクスポートできます。
HDDステータス検出	2017年10月1日以降に製造された4 TBから8 TBのSeagate HDDの健康状態を確認できます。この機能はHDDの問題をトラブルシューティングするのに役立ちます。Health Detectionは、S.M.A.R.T.機能よりも詳細なHDDの状態を表示します。
S.M.A.R.T. 検出	S.M.A.R.T.（Self-Monitoring, Analysis, and Reporting Technology）は、HDDの信頼性指標を検出することで故障を予知するための監視システムです。
不良セクタ検出	HDDに不良セクタが過度に存在する場合、HDDの交換を推奨します。そうでない場合、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	HDD内のデータをeSATAインターフェース経由で別のHDDにコピーします。

注意

技術サポートの支援を受けてメンテナンスツールを使用することをおすすめします。

23.7 ソフト電源オフ設定

ソフト電源オフ機能は、POWER-AC（AC電源異常）、POWER-UPS（UPS異常）、およびPOWER-UPSL（UPS低電力）アラーム出力（実機パネル上）を備えたデバイスでのみ利用可能です。デバイスはこれらのアラームを受信し記録します。POWER-ACとPOWER-UPSLの両方のアラームがトリガーされた場合、デバイスは事前設定された時間に自動的に電源が切断されます。POWER-ACまたはPOWER-UPSLのどちらかのアラーム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。

手順

1. **システム→ システムメンテナンス→ メンテナンス→ ソフトパワーオフ設定**に移動します。

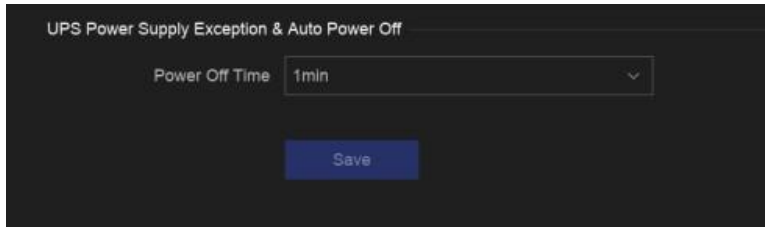


図23-1 ソフト電源オフ設定

2. **電源オフ時間を**設定します。対応するアラームがトリガーされた場合、設定した時間後にデバイスが自動的に電源オフになります。
3. **保存**をクリックします。

例

例えば、**電源オフ時間が1分に設定されている場合**、POWER-AC（AC電源異常）とPOWER-UPSL（UPS低電力）の両方のアラームがトリガーされた場合、デバイスは1分後に自動的に電源が切れます。

第24章 セキュリティ管理

24.1 アドレスフィルター

アドレスフィルターは、特定のIP/MACアドレスがデバイスにアクセスを許可するか拒否するかを決定します。

開始前に

管理者アカウントでログインしてください。

手順

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. **有効化を**オンにします。
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アドレスで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。デバイスは、指定したIP/MACアドレスへのアクセスを許可または拒否します。
5. **オプション: 制限リスト**を設定します。アドレスを追加、編集、または削除できます。
6. **保存**をクリックします。

24.2 ストリーム暗号化

ストリーム暗号化を有効にすると、リモートライブビュー、リモート再生、およびダウンロードした動画に暗号化キーが必要になります。

手順

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. **「有効」**をオンにします。
3. **暗号化キー**を設定します。

注意

ストリーム暗号化キーはHik-Connectサービスの検証コードと同期されます。暗号化を有効にすると、Hik-Connectストリームは強制的に暗号化されます。

4. **保存**をクリックします。

24.3 TLS バージョンを選択

TLS設定はHTTP(s)および強化されたSDKサービスに適用されます。より安全なストリーム送信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**に移動し、TLSバージョンを選択してください。

第25章 付録

25.1 適用可能な電源アダプターのリスト

以下のリストに載っている電源アダプターのみを使用してください。

電源アダプターモデル	仕様	製造元
ADS-26FSG-12 12024EPG	12 V、2 A	深セン・ホノル・エレクトロニクス株式会社
	12 V、3.33 A	モソ・パワー・サプライ・テクノロジー株式会社
	12 V、1.5 A	0000201935モソ・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・オナー・エレクトロニック株式会社
	12 V、1.5 A	0000201935 モソ・テクノロジー株式会社
TS-A018-120015AD	100～240 VAC、12 V、1.5 A、18 W、Φ5.5× 2.1× 10	0000200878 深セン・トランシン・テクノロジー株式会社
	12 V、2 A	0000201935 モソ・テクノロジー株式会社
ADS-24S-12 1224GPG	CE、100～240 VAC、12 V、2 A、24 W、Φ2.1	0000200174 深セン・オナー・エレクトロニック株式会社
	米国、12 V、2 A	0000201935 モソ・テクノロジー株式会社
ADS-26FSG-12 12024EPCU	米国、12 V、2 A	0000200174 深セン・オナー・エレクトロニック株式会社
KPL-040F-VI	12 V、3.33 A、40 W	0000203078 チャネルウェルテクノロジー株式会社
	12 V、3.33 A	0000201935 MOSO Technology Co., Ltd.
MSP-Z1360IC48.0-65W	48 V、1.36 A	0000201935 MOSO Technology Co., Ltd.
KPL-050S-II	48 V、1.04 A	0000203078 チャネルウェルテクノロジー株式会社

25.2 用語集

デュアルストリーム

デュアルストリームは、高解像度動画をローカルに記録しながら、ネットワーク経由で低解像度のストリームを送信する技術です。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

デジタルビデオレコーダーの略称。DVRは、アナログカメラから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装置です。

HD

ハードディスクドライブ（HDD）の略称。磁気表面を持つプラッタにデジタル形式でデータを記録する記憶媒体。

DHCP

ダイナミックホスト構成プロトコル（DHCP）は、インターネットプロトコル（IP）ネットワーク内で動作するための構成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

ハイパーテキスト転送プロトコルの略称。ネットワークを介してサーバーとブラウザ間でハイパーテキストのリクエストと情報を転送するためのプロトコル。

PPPoE

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

DDNS

ダイナミックDNS（Dynamic DNS）は、インターネットプロトコルスイート（IPスイート）を使用するルーターやコンピュータシステムなどのネットワーク接続デバイスが、ドメインネームサーバー（DNSサーバー）に通知し、DNSに格納されたホスト名、アドレス、その他の情報をリアルタイム（アドホック）で変更する機能を提供する手法、プロトコル、またはネットワークサービスです。

ハイブリッドDVR

ハイブリッドDVRは、DVRとNVRを組み合わせたシステムです。

NTP

ネットワーク タイム プロトコル（Network Time Protocol）の略称。ネットワーク上のコンピュータの時計を同期させるために設計されたプロトコルです。

NTSC

National Television System Committeeの略称。NTSCは、アメリカ合衆国や日本などにおいて使用されるアナログテレビ放送の規格です。NTSC信号の1フレームには、60Hzで525本の走査線が含まれます。

NVR

ネットワークビデオレコーダーの略称。NVRは、IPカメラ、IPドーム、その他のDVRの集中管理と保存に用いられるPCベースまたは組み込みシステムです。

PAL

Phase Alternating Lineの略称。PALは、世界の大部分で放送テレビシステムで使用される別のビデオ規格です。PAL信号は、50Hzで625本の走査線を含みます。

PTZ

パン、チルト、ズームの略語。PTZカメラは、モーター駆動システムで、カメラを左右にパン、上下にチルト、ズームイン/ズームアウトが可能。

USB

USB（ユニバーサル・シリアル・バス）の略称。USBは、ホストコンピュータとデバイスを接続するためのプラグアンドプレイ対応のシリアルバス規格です。

25.3 よくある質問

25.3.1 マルチスクリーンライブビューで、一部のチャンネルに「リソースなし」と表示されたり、画面が黒くなるのはなぜですか？

原因

1. サブストリームの解像度またはビットレート設定が適切ではありません。
2. サブストリームの接続に失敗しました。

解決方法

1. **カメラ → ビデオパラメーター → サブストリーム** へ移動します。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未満、最大ビットレートは2048 Kbps未満に設定してください）。

   注意

   ビデオレコーダーがこの機能に対応していない場合、カメラにログインし、ウェブブラウザ経由でビデオパラメーターを調整できます。

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てください（解像度は720p未満、最大ビットレートは2048 Kbps未満）。その後、チャンネルを削除し、再度追加してください。

25.3.2 ネットワークカメラを追加した後、ビデオレコーダーが「危険なパスワード」と表示されるのはなぜですか？

原因

カメラのパスワードが弱すぎます。

解決方法

カメラのパスワードを変更してください。

警告

私たちは、製品のセキュリティを強化するため、ご自身で選択した強固なパスワードを設定することを強くおすすめします（最低8文字以上で、大文字、小文字、数字、特殊文字の少なくとも3つのカテゴリーを含む）。また、特に高セキュリティシステムでは、パスワードを定期的に変更することをおすすめします。月次または週次でのパスワード変更は、製品の保護をさらに強化します。

25.3.3 ビデオレコーダーが「ストリームタイプがサポートされていません」と通知する理由はなぜですか？

原因

カメラのエンコード形式がビデオレコーダーと一致していません。

解決方法

カメラがH.265/MJPEGでエンコードしている場合、ビデオレコーダーがH.265/MJPEGに対応していない場合は、カメラのエンコード形式をビデオレコーダーと同じに設定してください。

25.3.4 ビデオレコーダーがH.265で動画を記録していることを確認する方法は？

解決方法

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

25.3.5 ビデオレコーダーがIP衝突を通知する理由は？

原因

ビデオレコーダーが他のデバイスと同一のIPアドレスを使用しています。

解決方法

ビデオレコーダーのIPアドレスを変更してください。他のデバイスと同一のIPアドレスにならないようにしてください。

25.3.6 単一または複数チャンネルのカメラで再生時に画像が止まるのはなぜですか？

原因

HDDの読み取り/書き込み例外。

解決方法

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

25.3.7 なぜデバイスはコアクシトロン経由でPTZカメラを制御できないのですか？

原因

1. カメラはコアクシトロンに対応していません。
2. コアクシトロンプロトコルが正しくない。
3. 信号はビデオ光トランシーバーの影響を受けています。

解決方法

1. ビデオ入力信号がHDTVIであることを確認し、カメラがコアクシトロンに対応していることを確認してください。
2. コアクシトロンプロトコルのパラメーター（ボーレートやアドレスなど）が正しいことを確認してください。
3. ビデオ光トランシーバーを削除し、再度試してください。

25.3.8 RS-485経由でPTZが反応しないのはなぜですか？

原因

1. RS-485ケーブルが正しく接続されていません。
2. RS-485 インターフェースが故障しています。
3. 制御プロトコルが正しくない。

解決方法

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

25.3.9 動画の音質が悪いのはなぜですか？

原因

1. 音声入力デバイスが音の収集に十分な効果を発揮していません。
2. 伝送中の干渉が発生しています。
3. オーディオパラメーターが適切に設定されていません。

解決方法

1. オーディオ入力デバイスが正常に動作しているか確認してください。別のオーディオ入力デバイスに切り替えて、再度お試しください。
2. オーディオ伝送ラインを確認してください。すべてのラインが適切に接続または溶接されており、電磁干渉がないことを確認してください。
3. 環境とオーディオ入力デバイスに応じてオーディオの音量を調整してください。

25.4 腐食性ガスに関する注意事項

データセンター以外の部屋では、腐食性ガスの濃度限界は、IEC 60721-3-3:2002の化学活性物質3C2レベルに準拠するように推奨されます。

表25-1 腐食性ガス濃度限界値

腐食性ガス分類	平均値（mg/m³）	最大値（mg/m³）
SO_2（二酸化硫黄）	0.3	1.0
H_2S（水素硫化物）	0.1	0.5
Cl_2 (塩素)	0.1	0.3
HCl（塩酸）	0.1	0.5
HF（フッ化水素）	0.01	0.03
NH_3（アンモニア）	1.0	3.
O_3 (オゾン)	0.05	0.1
NO_x (窒素酸化物)	0.5	1.0

注

- 上記の表の平均値は、機械室環境における腐食性ガスの典型的な制御限界値です。一般に、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。
- 最大値は、限界値またはピーク値を指します。腐食性ガスの濃度が最大値に達するまでの時間は、1日あたり30分を超えてはなりません。

表25-2 腐食性ガスの一般的な分類と発生源

分類	主な発生源
H_2S（硫化水素）	地熱排出物、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、鉱石の溶融、硫酸製造、タバコの燃焼など。
S（硫黄）	鋳物工場、硫黄製造など。
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、鋼鉄製造、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、地熱排出物など。
CO（一酸化炭素）	燃焼、自動車排気ガス、微生物の活動、樹木の腐敗など。
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（塩酸）	自動車排気ガス、燃焼、森林火災、海洋プロセスにおけるポリマー燃焼など。
HBr（臭化水素酸）、HI（ヨウ化水素酸）	自動車排気ガス、など。
O_3 (オゾン)	大気中の光化学反応（主に一酸化窒素と過酸化水素を含む）、など。
$C_n H_n$ (アルカン)	自動車排気ガス、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