デジタルビデオレコーダー

※初期設定は別途付属のかんたんガイドをご覧ください※

- ・本機のシリーズはiDS-7200HQHI-M1/S、iDS-7200HQHI-M2/S、iDS-7200HUHI-M1/S、iDS-7200HUHI-M2/S に該当します
- •HDDの交換を行った場合は保証の対象外となります

法的情報

本書について

本マニュアルには、本製品を使用および管理するための説明書が含まれる。以下、写真、チャート、画像、その他の情報は、単に説明のためのものである。本マニュアルに記載されている情報は、ファームウェアの更新その他の理由により、予告なく変更される場合があります。本マニュアルの最新版は、当社ウェブサイトでご確認ください。本マニュアルは、製品のサポートについて訓練を受けた専門家の指導と援助を受けて使用してください。

商標の確認

記載された商標およびロゴは、それぞれの所有者の特性である。

法的免責事項

適用される法律によって許可される最大限の範囲まで、本マニュアルおよび記載される本製品は、そのハードウエア、ソフトウエアおよび会社とともに、「現状のまま」および「すべての障害およびエラーを伴って」提供される。当社は、明示かまたは黙示かを問わず、特定目的に対する商品性、満足できる品質または適合性を含め、いかなる保証も行わない。貴社による本製品の使用は、貴社自身のリスクである。いかなる場合にも、当社は、特に、契約違反、不法行為(過失を含む)、本製品の使用に関連して、たとえ当社がかかる損害または損失の可能性について通知を受けていたとしても、契約違反、不法行為(過失を含む)、本製品の責任またはその他に基づくかを問わず、事業利益の喪失、事業の中断またはデータの喪失、システムの腐敗または文書の喪失、破損に対する損害を含む、特別損害、派生的損害、付随的損害または間接的損害につき、貴社に対して責任を負わない。

INTERNETの本質的なセキュリティリスクがあり、当社は、CYBER-ATTACK、HACKER ATTACK、VIRUS INSPECTION、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操作、プライバシーリーケージ、またはその他の損害に対して一切責任を負わないことをご承知おきください。ただし、当社は、必要に応じて、タイムリーな技術サポートを提供します。

お客様は、本製品をすべての適用される法律に準拠して使用することに同意し、お客様の使用が適用される法律に準拠することを保証する単独の責任を負います。特に、貴社は、制限を設けることなく、出版権、知的財産権、またはデータ保護およびその他のプライバシー権を含め、第三者の権利を侵害しない方法で本製品を使用することに責任を負う。貴殿は、本製品を、大量破壊兵器の開発または製造、化学兵器または生物兵器の開発または製造、核爆発性または危険性のある核燃料サイクルに関連する文章内の活動、または人権侵害の支援を含む、いかなる禁止された最終用途にも使用しないものとします。

本マニュアルと適用される法律との間に矛盾が生じた場合、後者が優先する。

規制情報

FCC情報

コンプライアンス責任者が明示的に承認していない変更または修正は、装置を操作するユーザ の権限を無効にする可能性があることに注意してください。

FCCコンプライアンス:この装置は、FCC規則のパート15に従って、クラスAデジタル装置の限界に適合することが試験され、見出されています。これらの制限は、本装置を商業地域で運用する場合に限り、電波障害に対する適切な保護措置が行われるように設計されています。本装置は電波エネルギーを発生、使用、放射し、ユーザーズマニュアルに従って設置、使用しない場合は無線装置に干渉する可能性もあります。住宅エリアでのこの装置の動作は、有害な干渉を引き起こす可能性があり、その場合、ユーザは、自分の費用で干渉を補正する必要がある。

FCC条件

本装置は、FCC規制のパート15に適合しています。運用は、以下の二つの条件に依存します。

- 1. 本デバイスが有害な干渉を引き起こすことはありません。
- 2. このデバイスが、望ましくない操作の原因となる妨害を含め、被った妨害を受け入れる必要があること

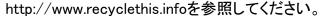
EU適合性宣言



本製品、および、該当する場合、供給される付属品も「CE」でマークされており、したがって、EMC指令2014/30/EU、RoHS指令2011/65/EUに記載されている、該当する調和された欧州規格に準拠している。



2012/19/EU (WEEE指令):この記号でマークされた製品は、欧州連合では、 未選別の都市廃棄物として処分することができない。適切なリサイクルの ために、同等の新設備を購入したら、この製品を地元の供給業者に返却す るか、または指定された回収地点で処分する。詳細については、





2006/66/EC (バッテリー指令): 本製品には、欧州連合で分別されていない 一般廃棄物として廃棄できないバッテリーが含まれています。特定のバッテリー情報については、製品のマニュアルを参照してください。電池は、カドミウム(Cd)、鉛(Pb)、または水銀(Hg)を示す文字を含むことができるこの記号でマークされている。適切なリサイクルを行うためには、電池をサプライヤーまたは指定された回収場所に戻してください。詳細については、

http://www.recyclethis.infoを参照してください。

カナダ産業ICES-003準拠

この装置は、CAN ICES-3(A)/NMB-3(A)規格要件を満たす。

適応機種

本取扱説明書は、以下の機種に適用されます。

表1-1 適用可能なモデル

シリーズ	型式
DS-7200HGHI-K1	DS-7216HGHI-K1
	DS-7216HGHI-K2
DS-7200HGHI-K2	DS-7224HGHI-K2
	DS-7232HGHI-K2
	DS-7104HQHI-K1
DS-7100HQHI-K1	DS-7108HQHI-K1
	DS-7116HQHI-K1
	DS-7204HQHI-K1
DS-7200HQHI-K1	DS-7208HQHI-K1
	DS-7216HQHI-K1
DS-7200HQHI-K1/SSD	DS-7204HQHI-K1/SSD(512G)
D3-7200HQHI-K1/33D	DS-7204HQHI-K1/SSD(1T)
	DS-7208HQHI-K2
DS-7200HQHI-K2	DS-7216HQHI-K2
D3-7200HQHI-KZ	DS-7224HQHI-K2
	DS-7232HQHI-K2
	DS-7204HQHI-K1/P
DS-7200HQHI-K/P	DS-7208HQHI-K2/P
	DS-7216HQHI-K2/P
	DS-7304HQHI-K4
	DS-7308HQHI-K4
DS-7300HQHI-K4	DS-7316HQHI-K4
	DS-7324HQHI-K4
	DS-7332HQHI-K4

シリーズ	型式
DS-8100HQHI-K8	DS-8124HQHI-K8
	DS-8132HQHI-K8
DO 700011111 1/1	DS-7204HUHI-K1
DS-7200HUHI-K1	DS-7208HUHI-K1
	DS-7204HUHI-K2
DS-7200HUHI-K2	DS-7208HUHI-K2
	DS-7216HUHI-K2
DS-7200HUHI-K2/SSD	DS-7208HUHI-K2/SSD
	DS-7204HUHI-K1/P
DS-7200HUHI-K/P	DS-7208HUHI-K2/P
	DS-7216HUHI-K2/P
	DS-7304HUHI-K4
	DS-7308HUHI-K4
DS-7300HUHI-K4	DS-7316HUHI-K4
DS-7300HUHI-K4	DS-7324HUHI-K4
	DS-7332HUHI-K4
	DS-8108HUHI-K8
	DS-8116HUHI-K8
DS-8100HUHI-K8	DS-8124HUHI-K8
	DS-8132HUHI-K8
	DS-9008HUHI-K8
DC 0000111111 I/O	DS-9016HUHI-K8
DS-9000HUHI-K8	DS-9024HUHI-K8
	DS-9032HUHI-K8
DS-7200HTHI-K1	DS-7204HTHI-K1
DC 7000UTUL 1/2	DS-7204HTHI-K2
DS-7200HTHI-K2	DS-7208HTHI-K2
DS-7200HTHI-K2/SSD	DS-7204HTHI-K2/SSD

シリーズ	型式
DS-7300HTHI-K4	DS-7316HTHI-K4
DS-8100HTHI-K8	DS-8116HTHI-K8
DS-9000HTHI-K8	DS-9016HTHI-K8
iDS-7200HQHI-K1/2S	iDS-7204HQHI-K1/2S
iDS-7200HQHI-K/4S	iDS-7208HQHI-K1/4S
	iDS-7216HQHI-K1/4S
iDS-7200HQHI-K/4S	iDS-7208HQHI-K2/4S
	iDS-7216HQHI-K2/4S
	iDS-7204HQHI-K1/2S(B)
iDS-7200HQHI-K1/S(B)	iDS-7208HQHI-K1/4S(B)
	iDS-7216HQHI-K1/4S(B)
iDS-7200HQHI-K2/4S(B)	iDS-7208HQHI-K2/4S(B)
	iDS-7216HQHI-K2/4S(B)
iDS-7200HQHI-K2/4S(B) iDS-7200HUHI-K/4S	iDS-7204HUHI-K1/4S
:DC_7000HIHI_K /4C	iDS-7208HUHI-K1/4S
iDS-7200HUHI-K/4S	iDS-7204HUHI-K2/4S
	iDS-7208HUHI-K2/4S
	iDS-7204HUHI-K1/4S(B)
:DS=7200H1HIT=K /AS(B)	iDS-7208HUHI-K1/4S(B)
iDS-7200HUHI-K/4S(B)	iDS-7204HUHI-K2/4S(B)
	iDS-7208HUHI-K2/4S(B)
iDS-7300HUHI-K4/16S	iDS-7316HUHI-K4/16S
iDS-9000HUHI-K8/16S	iDS-9016HUHI-K8/16S
	Y4661 / M1855
iDS-7200HQHI-M1/S	F5174 / X4933
	R2108 / H4028
:DC 7000HOUR M41 /FA	iDS-7204HQHI-M1/FA
iDS-7200HQHI-M1/FA	iDS-7208HQHI-M1/FA

シリーズ	型式
	iDS-7216HQHI-M1/FA
iDS-7200HQHI-M2/S	iDS-7208HQHI-M2/S
IDS-7200HQHI-M2/S	H8802 / Q9833
iDS-7200HQHI-M2/FA	iDS-7208HQHI-M2/FA
100 7200 NGTIL WIZ/TA	iDS-7216HQHI-M2/FA
iDS-7200HUHI-M1/S	T6325 / V4036
103 7200110111 W173	J9452 / B0650
iDS-7200HUHI-M1/FA	iDS-7204HUHI-M1/FA
IDS-7200HUHI-IMT/FA	iDS-7208HUHI-M1/FA
iDS-7200HUHI-M2/S	N5433 / H6781 / R9743
:DC 700011111 M2 /FA	iDS-7204HUHI-M2/FA
iDS-7200HUHI-M2/FA	iDS-7208HUHI-M2/FA

シンボル条約

本明細書で見られる記号は、以下のように定義される。

記号	説明
<u></u> 危険	取扱いを誤った時に、死亡もしくは重傷を負う可能性が想定されるも のをいいます。
注意	回避しないと、装置の損傷、データの損失、性能の劣化、または予期しない結果を招く可能性のある危険な状況を示します。
jì注	本文の重要なポイントを強調または補足するための追加情報を提供します。

安全上のご注意

- すべてのパスワードおよびその他のセキュリティ設定を適切に構成することは、設置者および/ またはエンドユーザーの責任となります。
- ◆ 本製品の使用にあたっては、国・地域の電気安全規制を厳守しなければなりません。
- プラグを電源ソケットにしっかり接続します。1台の電源アダプタに複数のデバイスを接続しないでください。付属品・周辺機器の着脱は、装置の電源を切ってから行ってください。
- ショックハザード!メンテナンスの前に、すべての電源を切断してください。
- 装置は、アースされた電源コンセントに接続する必要があります。
- サンケットコンセントは、装置の近くに設置され、容易にアクセス可能でなければならない。
- 1 危険な通電状態を示し、端子に接続された外部配線には、指示を受けた人が設置する必要があります。
- 不安定な場所には絶対に置かないでください。装置が落下し、人が重傷を負ったり、死亡したりすることがあります。
- 入力電圧は、IEC62368 に準拠したSELV(安全特別低電圧)およびLPS(制限電源)を満た す必要があります。
- ハイタッチ電流!電源に接続する前にアースに接続してください。
- ◆ 本装置から発煙、異臭、異音が発生した場合は、一旦電源を切り、電源ケーブルのプラグを抜いてから、サービスセンターにご連絡ください。
- デバイスはUPS と併用し、可能であれば工場推奨のHDD を使用してください。
- ◆ 本機のリモコンにはボタン型電池が使用されています。電池を飲み込んだ場合、2時間で重度の内部熱傷を引き起こし、死に至ることがある。
- この装置は、子供がいる可能性のある場所での使用には適していない。
- 注意: バッテリーを正しくないタイプと交換すると、爆発する危険があります。
- 不適切なタイプのバッテリーを不適切に交換すると、予防措置が無効になる可能性があります (リチウムバッテリーの種類によっては、そのような場合など)。
- また、機械的に破砕したり、電池を切ったりすると、爆発する恐れがあります。
- 爆発、可燃性の液体・気体の漏れの原因となるような、電池の周囲の温度が極めて高い場所に放置しないでください。
- バッテリーに極端に低い空気圧をかけないでください。爆発したり、可燃性の液体やガスが漏れたりする恐れがあります。
- 使用済みのバッテリを廃棄する場合は、指示に従ってください。
- ファンの羽根やモーターに身体部品を近づけないでください。保守点検時には、電源を切断してください。
- 車体部分はモーターから離しておいてください。保守点検時には、電源を切断してください。

予防的・警戒的ヒント

装置を接続して操作する前に、以下のヒントをお知らせください:

- ◆ 本装置は屋内専用です。通風性が良く、粉塵のない環境で、液体を使用せずに設置してください。
- レコーダーがラックまたはシェルフに正しく固定されていることを確認します。落としたりすると、 本機に大きな衝撃や衝撃が加わり、本機内部の高感度電子機器が損傷する恐れがあります。
- ●機器は、滴下や飛散にさらされてはならず、液体で満たされた物体は、花瓶などの機器に置かないものとします。
- 照明されたろうそくのような裸の火炎源は、装置上に置かなければならない。
- 通気は、通気口を新聞、テーブルクロス、カーテン等の物品で覆うことによって妨げられるべきではない。開口部は、ベッド、ソファ、ラグ、または他の同様の表面上に装置を置くことによって、決して塞がれてはならない。
- 特定のモデルでは、AC 主電源に接続するための端子の正しい配線を確認してください。
- ある種のモデルでは、必要に応じて、IT配電システムに接続するように装置を設計した。
- 任二 バッテリホルダ 自体を識別し、バッテリホルダ内のセルの位置を特定します。
- + 直流で使用される、または直流を生成する機器の正端子を識別します。+ 直流で使用される、または直流を生成する機器の負端子を識別します。
- 換気を十分に行うため、装置の周囲には最低200mm(7.87inch)の距離を保ってください。
- 特定のモデルでは、AC 主電源に接続するための端子の正しい配線を確認してください。
- 取扱説明書または取扱説明書に記載されている電源のみをご使用ください。
- ◆ 本器の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ドングルのみに接続するために使用します。
- 取扱説明書または取扱説明書に記載されている電源のみをご使用ください。
- 鋭利な角や角には触れないでください。
- デバイスが45°C (113°F)を超えて動作しているとき、またはS.M.A.R.T.のHDD温度が規定値 を超えているときは、デバイスが寒い環境で動作していることを確認するか、HDDを交換して S.M.A.R.T.のHDD温度を規定値以下にしてください。

目次

第1章基本操作	1
1.1 デバイスのアクティブ化	1
1.1.1 デフォルトのユーザーとIP アドレス	1
1.1.2 ローカルメニューから起動	1
1.1.3 SADP 経由で有効化	2
1.1.4 クライアントソフトウェア経由での有効化	3
1.1.5 Web ブラウザ経由で有効化	6
1.2 IP設定を設定する	6
1.3 HDD 設定	
1.4 信号入力の設定	7
1.5 拡張IP モードの設定	8
1.6 PoCカメラの接続	8
1.7 ネットワークカメラの追加	9
1.7.1 自動検索オンラインネットワークカメラの追加	10
1.7.2 ネットワークカメラを手動で追加する	11
1.7.3 カスタマイズプロトコルの設定	12
1.8 5 MP 長距離伝送の設定	13
1.9 プラットフォームアクセス	14
1.9.1 ガーディングビジョンの設定	
第 2 章カメラの設定	16
2.1 イメージパラメータの設定	16
2.2 OSD 設定の構成	16
2.3 プライバシーマスクの設定	17
2.4 IPカメラ設定ファイルのインポート/エクスポート	
2.5 IPカメラのアップグレード	19
第 3 章ライブビュー	20
3.1 ライブビューの開始	20
3.1.1 ライブビュー設定の構成	20

	3.1.2 カメラのオートスイッチの設定	21
	3.1.3 ライブビューレイアウトの設定	21
	3.1.4 Channel-Zero Encoding の設定	23
	3.1.5 補助モニターを使用する	23
	3.2 デジタルズーム	24
	3.3 ライブビュー戦略	24
	3.4 顔面認知	25
	3.5 PTZ制御	27
	3.5.1 PTZ パラメータの設定	27
	3.5.2 プリセットを設定する	28
	3.5.3プリセットを呼び出す	29
	3.5.4 パトロールの設定	29
	3.5.5パトロールを呼び出す	31
	3.5.6 パターンの設定	32
	3.5.7パターンを呼び出す	32
	3.5.8 リニアスキャンリミットの設定	33
	3.5.9 ワンタッチ公園	33
	3.5.10 補助関数	34
第	4 章録音と再生	35
	4.1 記録	35
	4.1.1 記録パラメータの設定	35
	4.1.2 H.265 ストリームアクセスの有効化	37
	4.1.3 手動録音	38
	4.1.4 計画レコーディングの構成	38
	4.1.5 連続録音の設定	39
	4.1.6 動き検出トリガ記録の設定	40
	4.1.7 イベントトリガー記録の設定	40
	4.1.8 アラーム起動記録の設定	40
	4.1.9 画像キャプチャの設定	41
	4.1.10 ホリデイレコーディングの設定	41

		4.1.11 冗長録画とキャプチャの設定	42
		4.1.12 1080p ライトモードの設定	43
	4.2	再生	43
		4.2.1 インスタント再生	43
		4.2.2 通常の動画を再生	44
		4.2.3 スマート検索動画を再生する	44
		4.2.4 カスタム検索ファイルの再生	45
		4.2.5 タグファイルの再生	46
		4.2.6 サブピリオド別再生	48
		4.2.7 ログファイルの再生	48
		4.2.8 外部ファイルの再生	49
	4.3	再生操作	49
		4.3.1 通常/重要/カスタムビデオ	49
		4.3.2 重要/カスタムモードでの再生方法の設定	49
		4.3.3 ビデオクリップの編集	50
		4.3.4 メインストリームとサブストリームの切り替え	50
		4.3.5 サムネイルビュー	50
		4.3.6 高速表示	50
		4.3.7 デジタルズーム	51
第	5 章	スマート分析	52
	5.1	エンジン構成	52
	5.2	タスク設定	52
	5.3	拡張VCA モードの設定	53
	5.4	顔画像の比較	54
		5.4.1 顔面検出	54
		5.4.2 顔画像ライブラリ管理	55
		5.4.3 顔画像比較の設定	56
		5.4.4 顔画像検索	57
	5.5	周辺保護	60
		5.5.1 侵入検知	60

5.5.2 ライン交差検出	6
5.5.3 領域入口検出	6
5.5.4 領域終了検出	6
5.6 人体検出	6
5.6.1 人体検出	6
5.6.2 人体探索	6
5.7 動き検出	6
5.8 車両検知	6
5.8.1 車両検出の設定	6
5.8.2 車両探索	6
5.9 ターゲット検出	7
5.10 人数	7
5.11 ヒートマップ	7
第 6 章イベント	7
6.1 通常イベントアラーム	7
6.1.1 ビデオロスアラームの	設定7
6.1.2 ビデオ・タンパリング・	アラームの設定 7
6.1.3 センサアラームの設定	፪7
6.1.4 例外アラームの設定.	7
6.2 VCA イベントアラーム	7
6.2.1 無人手荷物検知	7
6.2.2 物体除去検出	7
6.2.3 オーディオ例外検出	7
6.2.4 デフォーカス検出	7
6.2.5 突然のシーン変化検	出7
6.2.6 PIRアラーム	8
6.3 Arming Schedule の設定	8
6.4 リンケージアクションの設定.	8
6.4.1 自動スイッチ全画面監	き視の設定 8
6.4.2 オーディオ警告の設定	₹8

6.4.3 通知サーベイランスセンター	83
6.4.4 メール連動の設定	83
6.4.5 トリガアラーム出力	84
6.4.6 PTZ 連携の設定	84
6.4.7 Audio and Light Alarm Linkage の設定	84
第 7 章ファイル管理	86
7.1 ファイルの検索	86
7.2 ファイルのエクスポート	86
7.3 スマートサーチ	87
第 8 章 POS 設定	88
8.1 POS 接続の設定	88
8.2 POS テキストオーバーレイの設定	91
8.3 POSアラームの設定	92
第 9 章ストレージ	94
9.1 ストレージデバイス管理	94
9.1.1 ローカルHDD の管理	94
9.1.2 ネットワークディスクの追加	96
9.1.3 eSATA の管理	97
9.2 ディスクアレイ	99
9.2.1 ディスクアレイを作成する	99
9.2.2 アレイの再構築	101
第10章ネットワーク設定	104
10.1 DDNS の設定	104
10.2 Configure PPPoE	104
10.3 ポートマッピング(NAT) の設定	105
10.4 Wi−Fi の設定	106
10.5 SNMP の設定	108
10.6 電子メールの設定	109
10.7 ポートの設定	110
10.8 ONVIF の設定	112

第 11 章ユーザー管理とセキュリティ	113
11.1 アカウントを管理する	113
11.1.1 ユーザーの追加	113
11.1.2 管理者ユーザーの編集	114
11.1.3 オペレータ/ゲストユーザの編集	115
11.2 権限付与を行なう	115
11.2.1 ユーザー権限の設定	115
11.2.2 Live View Permission on Lock画面の設定	118
11.3 パスワードセキュリティの設定	119
11.3.1 GUID ファイルのエクスポート	119
11.3.2 セキュリティ質問の設定	120
11.3.3 予約メールの設定	121
11.4 パスワードのリセット	122
11.4.1 GUID によるパスワードのリセット	122
11.4.2 セキュリティ質問によるパスワードのリセット	123
11.4.3 Guarding Vision によるパスワードのリセット	123
11.4.4 予約メールによるパスワードのリセット	124
第 12 章システム管理	125
12.1 デバイスの設定	125
12.2 時間の設定	126
12.2.1 手動時間同期	126
12.2.2 NTP同期	126
12.2.3 DST 同期	126
12.3 ネットワーク検出	127
12.3.1 ネットワークトラフィックの監視	127
12.3.2 ネットワーク遅延とパケット損失のテスト	128
12.3.3 ネットワークパケットのエクスポート	128
12.3.4 ネットワークリソース統計	129
12.4 ストレージデバイスのメンテナンス	
12.4.1 不良セクター検出	

	12.4.2 S.M.A.R.T.検出	130
	12.4.3 HDD Health Detection	131
	12.4.4 ディスククローンの設定	132
	12.4.5 修復データベース	133
12.5	アップグレードデバイス	133
	12.5.1 ローカルバックアップデバイスによるアップグレード	133
	12.5.2 FTPによるアップグレード	134
	12.5.3 Webブラウザによるアップグレード	134
	12.5.4 Guarding Visionによるアップグレード	135
12.6	デバイス設定ファイルのインポート/エクスポート	135
12.7	ログファイルの検索とエクスポート	136
12.8	デフォル設定に戻す	137
12.9	セキュリティ管理	138
	12.9.1 RTSP認証	138
	12.9.2 HTTP 認証	138
	12.9.3 SADP サービスの無効化	139
第13章付	録	140
13.1	適用可能な電力アダプター覧	140
13.2	用語集	141
13.3	よくある質問	142
	13.3.1 ライブビューのマルチ画面で「リソースなし」を表示したり、黒画面になったりで チャンネルがあるのはなぜですか?	
	13.3.2 なぜ、ビデオレコーダはネットワークカメラを追加した後に、危険なパスワード 通知するのか?	
	13.3.3 なぜ、ビデオレコーダがストリームタイプをサポートしていないことを通知するか。	
	13.3.4 再生画質を向上させるにはどうすればよいでしょうか。	143
	13.3.5「NO VIDEO」をライブビューにオーバーレイしたアナログチャンネルはなぜでか?	
	13.3.6 ビデオレコーダーがH.265 を使ってビデオを録画していることを確認するには	t? 144

13.3.7 再生時のタイムラインが一定でないのはなぜか?	144
13.3.8 ネットワークカメラを追加する場合、ビデオレコーダは、ネットワークに到達ないことを通知する。	
13.3.9 ネットワークカメラのIPアドレスが自動的に変更されるのはなぜですか?	145
13.3.10 ビデオレコーダがIP競合を通知するのはなぜか?	145
13.3.11 ビデオレコーダーがシングルカメラまたはマルチチャンネルカメラで再生さいるときに、なぜ画像が動かなくなっているのか?	
13.3.12 ブート後、なぜ私のビデオレコーダーがビープ音を鳴らすのでしょうか?	146
13.3.13 モーション検出を設定した後、なぜ録画された映像がないのでしょうか?	146
13.3.14 なぜ同軸トロンを介してPTZカメラを制御できないのでしょうか?	147
13.3.15 なぜPTZはRS-485を介して応答しないように見えますか?	147
13.3.16 なぜ映像を録画するのに音質が良くないのだろうか。	147

第1章基本操作

1.1 デバイスのアクティブ化

1.1.1 デフォルトのユーザーとIP アドレス

- デフォルトの管理者アカウント: admin。
- デフォルトIPv4 アドレス: 192.168.1.64。

1.1.2 ローカルメニューから起動

初めてアクセスする場合は、管理者パスワードを設定してデバイスをアクティブ化する必要があります。起動前は操作できません。Web ブラウザ、SADP、またはクライアントソフトウェアを使用してデバイスをアクティベートすることもできます。

手順

1. 管理者パスワードを2回入力します。

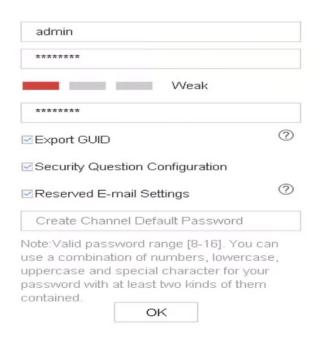


図1-1 ローカルメニューからの起動

警告

製品のセキュリティを高めるために、自分で選択した強力なパスワード(大文字、小文字、数字、特殊文字の3種類以上のカテゴリを含む、最低8文字を使用)を作成することを強くお勧めします。また、パスワードは定期的に変更することをお勧めします。特に高セキュリティシステムでは、毎月または毎週パスワードを変更すると、製品の保護が向上します。

- 2. パスワードを入力して、IPカメラを起動します。
- 3. オプション: GUID のエクスポート、セキュリティ質問の設定、または予約された電子メール設定をチェックします。
- 4. [OK]をクリックします。

[i]注

- デバイスがアクティブ化されたら、パスワードを適切に保持する必要があります。
- デフォルトのプロトコルで接続されているIPカメラにパスワードを複製することができます。

次に何をするか

- エクスポートGUID を有効にしたら、今後のパスワードリセットのために、GUID ファイルをUSB フラッシュドライバに引き続きエクスポートします。
- Security Question Configuration(セキュリティ質問の設定)を有効にしたら、今後のパスワード リセットのために引き続きセキュリティ質問を設定します。
- Reserved E-mail Settings(予約済み電子メール設定)を有効にした場合は、今後のパスワード リセットのために予約済み電子メールの設定を続行します。

1.1.3 SADP 経由で有効化

SADPソフトウェアは、オンラインデバイスの検出、デバイスのアクティブ化、およびパスワードのリセットに使用されます。

開始前に

付属のディスクまたは公式Web サイトからSADP ソフトウェアを入手し、プロンプトに従ってSADP をインストールします。

手順

- 1. ビデオレコーダーの電源をコンセントに接続し、電源を入れます。
- 2. SADP ソフトウェアを実行して、オンラインレコーダーを検索します。
- 3. デバイスリストからレコーダーの状態を確認し、非アクティブなレコーダーを選択します。

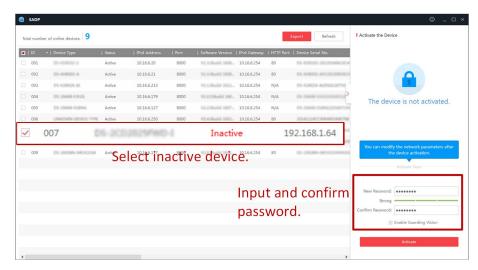


図1-2 SADP 経由での有効化

4. パスワードフィールドに新しいパスワードを作成して入力し、パスワードを確認します。

[i]注

製品のセキュリティを高めるために、自分で選択した強力なパスワード(大文字、小文字、数字、特殊文字の3種類以上のカテゴリを含む、最低8文字を使用)を作成することを強くお勧めします。また、パスワードは定期的に変更することをお勧めします。特に高セキュリティシステムでは、毎月または毎週パスワードを変更すると、製品の保護が向上します。

5. アクティブ化をクリックします。

1.1.4 クライアントソフトウェア経由での有効化

クライアントソフトウェアは、複数の種類のデバイスに対応する多用途のビデオ管理ソフトウェアです。

開始前に

付属のディスクまたは公式ウェブサイトからクライアントソフトウェアを入手し、プロンプトに従って ソフトウェアをインストールします。

手順

クライアントソフトウェアを実行すると、ソフトウェアのコントロールパネルがポップアップ表示されます。

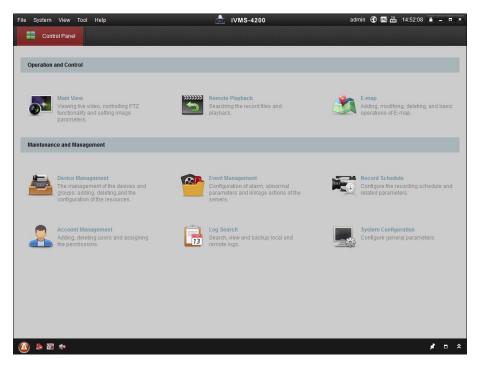


図 1-3 コントロールパネル

2. Device Management(デバイス管理)をクリックして、次のようにデバイス管理インタフェースに入ります。

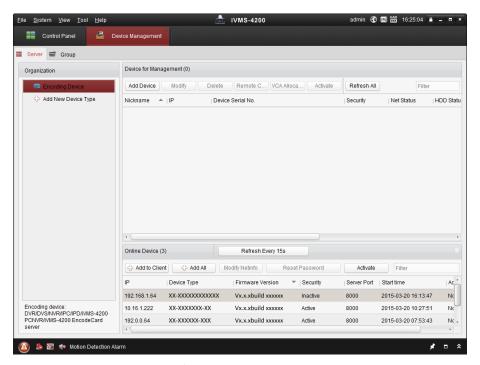


図1-4 デバイス管理インタフェース

- 3. デバイスリストからレコーダーのステータスを確認し、非アクティブなレコーダーを選択します。
- 4. Activate をクリックして、Activation インターフェースをポップアップ表示します。
- 5. パスワードを作成し、パスワードフィールドにパスワードを入力し、パスワードを確認します。

〔i注

製品のセキュリティを高めるために、自分で選択した強力なパスワード(大文字、小文字、数字、特殊文字の3種類以上のカテゴリを含む、最低8文字を使用)を作成することを強くお勧めします。また、パスワードは定期的に変更することをお勧めします。特に高セキュリティシステムでは、毎月または毎週パスワードを変更すると、製品の保護が向上します。

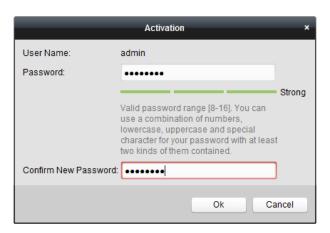


図1-5 起動

- 6. OK をクリックしてアクティベーションを開始します。
- 7. 「Modify Netinfo」をクリックすると、以下に示すように「Network Parameter Modification」インターフェースがポップアップ表示されます。

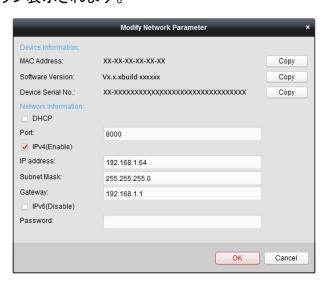


図1-6 ネットワークパラメータの変更

- 8. レコーダのIPアドレスを、お使いのコンピュータと同じサブネットに変更します。
- IP アドレスを手動で変更します。DHCPを有効にするをチェックします。
- 9. IP アドレスの変更を有効にするには、パスワードを入力します。

1.1.5 Web ブラウザ経由で有効化

Webブラウザからレコーダにアクセスできます。Internet Explorer 6.0 以降、Apple Safari、Mozilla Firefox、Google Chrome のいずれかのWeb ブラウザを使用できます。サポートする解像度は1024*768 以上です。

手順

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

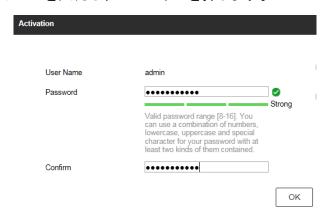


図1-7 Web ブラウザのアクティブ化

2. admin ユーザーアカウントのパスワードを設定します。

[]i注

製品のセキュリティを高めるために、自分で選択した強力なパスワード(大文字、小文字、数字、特殊文字の3種類以上のカテゴリを含む、最低8文字を使用)を作成することを強くお勧めします。また、パスワードは定期的に変更することをお勧めします。特に高セキュリティシステムでは、毎月または毎週パスワードを変更すると、製品の保護が向上します。

3. [OK]をクリックします。

1.2 IP設定を設定する

デバイスをネットワーク経由で動作させるには、TCP/IP 設定が適切に構成されている必要があります。

手順

1. システム→ネットワーク→ TCP/IP に移動します。

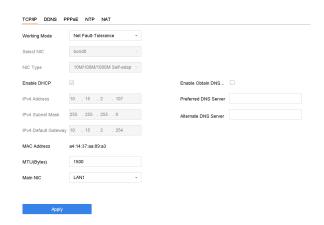


図1-8 TCP/IP 設定

2. Working Mode as Net-Fault Tolerance or Multi-Address Mode を選択します。

正味故障耐性

2 枚のNIC カードは同じIP アドレスを使用し、メインNIC をLAN1 またはLAN2 に選択できます。このように、一方のNIC カードに障害が発生した場合、デバイスはもう一方のスタンバイNIC カードを自動的に有効にして、システムの正常な稼働を保証します。

マルチアドレスモード

2 枚の NIC カードのパラメータは、個別に設定できます。パラメータ設定の「NIC の選択」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 カードを選択します。システムがエクストラネットに接続すると、データはデフォルトルートを介して転送されます。

- 3. 必要に応じて、その他のIP 設定を構成します。
- 4. 適用をクリックします。

[ji 注

- ネットワーク上にDHCP サーバがある場合は、「DHCP を有効にする」をオンにすると、IP 設定が自動的に取得されます。
- 有効なMTU値範囲は500~9676です。

1.3 HDD 設定

ビデオレコーダーの記録メディアが正しいことを確認します。少なくとも1 つのHDD を取り付けて初期化するか、RAID を作成して初期化することができます。

1.4 信号入力の設定

アナログおよびIP信号の入力タイプを設定できます。1つのアナログチャネルを無効にすると、1つ

のIPチャネルを追加できます。

手順

1. Camera → Camera → Analog に移動します。

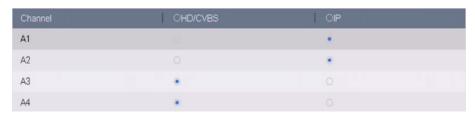


図1-9 信号入力の種類

2. 各チャンネルのHD/CVBSまたはIPとして信号入力タイプを選択します。

HD/CVBS

Turbo HD、AHD、HDCVI、およびCVBSを含む4つのタイプのアナログ信号入力を、チャネルのためにランダムに接続することができる。

ΙP

チャンネルにはネットワークカメラを接続できます。

3. 適用をクリックします。ネットワークカメラの最大アクセス可能数を最大で表示できます。IPカメラ番号。

1.5 拡張IP モードの設定

拡張IPモードを有効にすると、最大数のカメラに接続できますが、2K/4K出力解像度は無効になり、周辺保護機能、動き検出の人間または車両検出機能、顔検出機能、顔画像比較機能はアナログチャネルでは使用できません。

→ユーティリティ全般に移動し、拡張 IP モードを確認します。

1.6 PoCカメラの接続

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

開始前に

- お使いのデバイスがPoC (Power over Coaxitron)カメラ接続に対応していることを確認してください。
- PoC カメラをDVR に接続します。

手順

- 1. 「→カメラの→ PoCの状態」に移動します。
- 2. 希望に応じて、チャンネルのPoCをオンにします。

- 3. 接続したPoCカメラの状態を確認してください。
 - DVRの消費電力がAFカメラよりも低い場合、AFカメラやATカメラが接続されているときは映像がなく、ライブビュー画像に「PoC用電源不足」が重畳されます。
 - DVR の消費電力がAF カメラよりも高く、AT カメラよりも低い場合は、AF カメラを接続すると正常に電源が入ります。AT カメラを接続すると、電源が入ってから電源が切れます。ビデオがなく、ライブビュー映像に「PoC 用電源不足」が重ね合わされます。
 - DVRの消費電力がATカメラの消費電力よりも大きい場合、AFカメラまたはATカメラが接続されているときには、DVRは正常に電源が投入される。
- 4. 接続しているAFまたはATカメラ番号と接続可能なカメラ番号を確認してください。

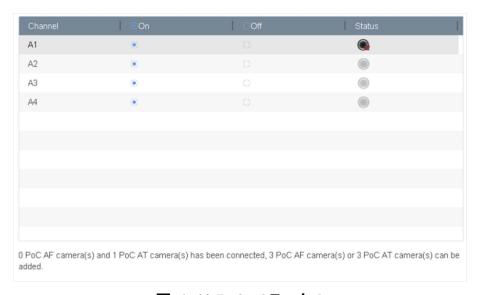


図 1-10 PoC ステータス

li注

- 指定されたPoCカメラのみがサポートされています。
- 接続できるAT/AFカメラの最大台数は、機種によって異なります。

警告

PoCに対応していないカメラや、同一メーカーのカメラが製造していない場合は、PoC機能をOFFにしてください。PoC 機能をオフにすると、カメラまたはDVR に回復不能な損傷を与える可能性があります。

1.7 ネットワークカメラの追加

ライブビデオを取得したり、ビデオファイルを記録したりする前に、ネットワークカメラをデバイスの

接続リストに追加する必要があります。

開始前に

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

手順

- 1. メインメニューバーのをクリックします。
- 2. タイトルバーの「カスタム追加」タブをクリックします。

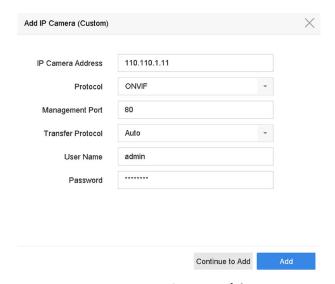


図 1-11 IP カメラの追加

- 3. 追加するIPアドレス、プロトコル、管理ポート、その他のIPカメラ情報を入力します。
- 4. IPカメラのログインユーザ名とパスワードを入力します。
- 5. 「追加」をクリックして、IPカメラの追加を終了します。
- 6. オプション: Continue to Addをクリックして、追加のIPカメラを追加し続けます。

1.7.1 自動検索オンラインネットワークカメラの追加

手順

- メインメニューをクリックします。□
- 2. 下部のNumber of Unadded Online Device をクリックします。
- 3. 自動的に検索されたオンラインネットワークカメラを選択します。
- 4. 「追加」をクリックして、ビデオレコーダと同じログインパスワードを持つカメラを追加します。

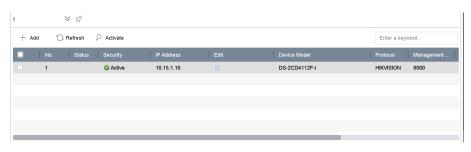


図 1-12 自動検索オンラインネットワークカメラの追加

[ji 注

追加するネットワークカメラが有効になっていない場合は、カメラ管理インタフェースのネットワークカメラー覧で有効にできます。

1.7.2 ネットワークカメラを手動で追加する

ライブビデオまたは録画ビデオファイルを表示する前に、ネットワークカメラをデバイスに追加する必要があります。

開始前に

ネットワーク接続が有効で正しいことを確認し、ネットワークカメラを起動します。

手順

- 1. メインメニューをクリックします。
- 2. カスタム追加をクリックします。
- 3. IP Camera Address、Protocol、Management Port、Transfer Protocol、User Name、Password を設定します。管理ポートの範囲は1 ~ 65535 です。

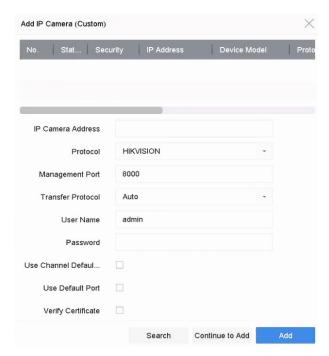


図 1-13 ネットワークカメラの追加

- 4. オプション: Channel Default Password を使用して、デフォルトのパスワードを使用してカメラを追加します。
- 5. オプション: デフォルトポートを使用して、デフォルト管理ポートを使用してカメラを追加します。 SDK サービスの場合、デフォルトのポート値は8000 です。拡張SDKサービスの場合、デフォルト値は8443です。

[ji 注

この機能は、HIKVISIONプロトコルを使用している場合にのみ使用できます。

6. オプション: 証明書を確認して、証明書付きカメラを確認します。証明書は、より安全なカメラ認証を提供するカメラの識別の形式です。この機能を使用する場合は、最初にネットワークカメラ証明書をデバイスにインポートする必要があります。詳細は参照。

山注

この機能は、HIKVISIONプロトコルを使用している場合にのみ使用できます。

- 7. 追加をクリックします。
- 8. オプション:「追加を続ける」をチェックして、他のネットワークカメラを追加します。

1.7.3 カスタマイズプロトコルの設定

標準プロトコルで設定されていないネットワークカメラを接続するには、カスタマイズしたプロトコ

ルを設定します。システムは16のカスタマイズされたプロトコルを提供します。

手順

1. その他の設定→プロトコールに移動します。

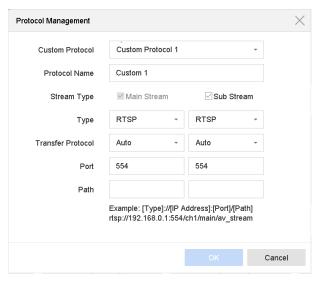


図1-14 プロトコル管理

2. プロトコルパラメータを設定します。

種類

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RTSPを介したストリームの取得をサポートしなければならない。

経路

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

[i]注

プロトコルタイプおよび転送プロトコルは、追加するためにネットワークカメラによってサポートされなければならない。

3. [OK]をクリックします。 カスタマイズしたプロトコルを追加すると、「プロトコル」に表示されます。

1.8 5 MP 長距離伝送の設定

HUHIシリーズおよびHTHIシリーズのDVRでは、信号入力ステータスインタフェースで5 MP長距離

送信を設定できます。

手順

- 1. Camera → Camera → Analog に移動します。
- 2. クリックして、5 MP 長距離伝送設定インターフェースに入ります。 💮

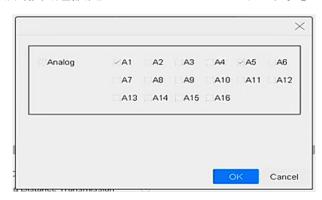


図 1-15 5 MP 長距離伝送設定

- 3.5 MP Long Distance Transmission を有効にするには、チャネルを選択します。
- 4. [OK]をクリックします。
- 5. 適用をクリックします。

1.9 プラットフォームアクセス

1.9.1 ガーディングビジョンの設定

Guarding Vision を使用すると、携帯電話アプリケーションとサービスプラットフォームページ (dev.guardingvision.com) で接続されたNVR にアクセスして管理できるため、監視システムへの 便利なリモートアクセスが提供されます。

手順

- 1. →ユーティリティネットワークシステムの詳細→プラットフォームシステムに移動します。
- 2. 有効をオンにすると、機能が有効になります。すると、サービス条件がポップアップします。
 - 1) 認証コードを入力します。
 - 2) QRコードをスキャンして、サービス利用規約とプライバシーに関する声明を読みます。
 - 3) Guarding Visionサービスを確認するには、インターネットへのアクセスが必要です。サービス 条件とプライバシーステートメントに同意している場合は、サービスを有効にする前に、サー ビス条件とプライバシーステートメントを参照してください。
 - 4) [OK]をクリックします。

[ji]注

- デフォルトでは、Guarding Vision は無効になっています。
- 確認コードはデフォルトでは空です。それは6から12の文字または数字を含まなければなら

ず、大文字と小文字を区別する。

- 3. オプション: 次のパラメータを設定します。
 - 「カスタム」をオンにし、必要に応じて「サーバアドレス」を入力します。
 - ●「ストリーム暗号化を有効にする」をオンにすると、リモートアクセスとライブビューに検証コードが必要になります。
 - ビデオレコーダーが現在のGuarding Visionアカウントとのバインドを解除する必要がある場合は、「バインド解除」をクリックします。
- 4. 適用をクリックします。

次にどうするか

ビデオレコーダーには、Guarding Vision アプリまたはdev.guardingvision.com からアクセスして管理できます。

第 2 章カメラの設定

2.1 イメージパラメータの設定

「カメラ→画面」では、昼夜切り替え、バックライト、コントラスト、彩度などのパラメータをカスタマイズできます。

画像設定

輝度、コントラスト、および彩度を含む画像パラメータをカスタマイズします。

露光

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

デイ/ナイトスイッチ

時刻や周囲の照明状況に応じて、昼夜、オートスイッチのモードに設定します。夜間に光量が 少なくなると、高画質の白黒画像でナイトモードに切り替わります。

バックライト

カメラのワイドダイナミックレンジ(0 ~100)を設定します。周囲の照明や対象物の明るさの差が大きい場合に、WDR 値を設定して画像全体の明るさレベルのバランスを取ることができます。

画像強調

ビデオストリームのノイズを軽減する、最適化されたイメージコントラスト強調のためのものです。

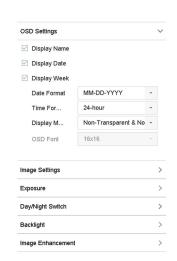
2.2 OSD 設定の構成

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

手順

- 1. カメラ→画面に移動します。
- 2. 希望に応じてカメラを選択します。
- 3. カメラ名で名前を編集します。
- 4. 表示名、表示日、表示週を確認して、画像の情報を表示します。
- 5. 日付形式、時刻形式、表示モードを設定します。





Apply

図2-1 OSD 設定インターフェイス

- 6. プレビューウィンドウ上のテキストフレームをドラッグして、OSD 位置を調整します。
- 7. 適用をクリックします。

2.3 プライバシーマスクの設定

プライバシーマスクは、画像の一部をキイブビューから隠すことによって、またはマスクされた領域で記録することによって、個人のプライバシーを保護する。

手順

- 1. カメラ→プライバシーマスクに移動します。
- 2. プライバシーマスクを設定するカメラを選択します。
- 3. 有効をチェックします。
- 4. ウィンドウにゾーンを描画します。ゾーンは、異なるフレーム色によってマークされる。

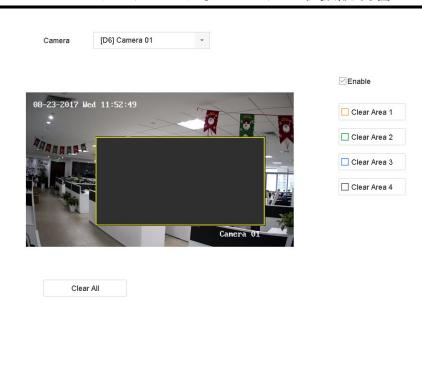


図2-2 プライバシーマスク設定インターフェース

[ji 注

- 4つまでのプライバシーマスクゾーンを設定でき、各エリアのサイズを調整できます。
- ウィンドウの右側にある対応するクリアゾーン1 ~4 アイコンをクリックするか、すべてのゾーンをクリアするには、Clear All(すべてクリア)をクリックします。
- 5. 適用をクリックします。

2.4 IPカメラ設定ファイルのインポート/エクスポート

IP アドレス、管理ポート、管理者パスワードなどのIP カメラ情報をMicrosoft Excel 形式で保存し、ローカルデバイスにバックアップできます。エクスポートしたファイルは、コンテンツの追加や削除、Excel ファイルをインポートして他のデバイスにコピーするなど、PC で編集できます。

開始前に

設定ファイルをインポートする場合は、設定ファイルを含むストレージデバイスをデバイスに接続します。

手順

1. 「カメラ→カメラインポート/エクスポート」に移動します。

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

Lii注

インポート処理が完了したら、デバイスを再起動して設定を有効にする必要があります。

2.5 IPカメラのアップグレード

IPカメラは、装置を介して遠隔でアップグレードすることができる。

開始する前に

USB フラッシュドライブがデバイスに挿入されており、IP カメラのアップグレードファームウェアが含まれていることを確認します。

- 1. カメラ管理インタフェースで、カメラを選択します。
- 2. バージョンアップ→のその他の設定に進みます。
- 3. USB フラッシュドライブからファームウェアアップグレードファイルを選択します。
- 4. アップグレードをクリックします。 アップグレードが完了すると、IPカメラが自動的にリブートします。

第 3 章ライブビュー

ライブビューは、各カメラから得られるビデオ画像をリアルタイムで表示する。

3.1 ライブビューの開始

メインメニューバーをクリックしてライブビューに入ります。

- ウィンドウを選択し、リストからカメラをダブルクリックして、選択したウィンドウでカメラからビデオを再生します。
- 再生ウィンドウの下部にあるツールバーを使用して、キャプチャ、即時再生、オーディオのオン/オフ、デジタルズーム、ライブビューストラテジ、ショー情報、録画の開始/停止などを実現します。

3.1.1 ライブビュー設定の構成

ライブビューの設定はカスタマイズできます。出力インターフェース、画面表示の滞留時間、音声のミュートやオン、チャンネルごとの画面番号などを設定できます。

手順

1. 「→ライブビュー→全般」に移動します。



図 3-1 ライブビュー一般

2. ライブビューのパラメータを設定します。

ビデオ出力インターフェイス

設定するビデオ出力を選択します。

ライブビューモード

「Live View」の表示モード(2*2、1*5など)を選択します。

滞留時間

ライブビューでオートスイッチを使用しているときに、カメラの切り替えを待機する時間(秒)。

オーディオ出力を有効にする

選択したビデオ出力のオーディオ出力を有効/無効にします。

体積

選択した出力インタフェースのLive View音量、再生、双方向オーディオを調整します。

イベント出力

イベントビデオを表示する出力を選択します。

フルスクリーン監視休止時間

アラームイベント画面を表示する時間を秒単位で設定します。

3. [OK]をクリックします。

3.1.2 カメラのオートスイッチの設定

カメラのオートスイッチを、異なる表示モードで再生するように設定できます。

手順

- 1. 「→ライブビュー→全般」に移動します。
- 2. ビデオ出カインタフェース、ライブビューモード、ドウェル時間を設定します。

ビデオ出力インターフェイス

ビデオ出力インターフェイスを選択します。

ライブビューモード

ライブビューの表示モード(2*2、1*5など)を選択します。

滞留時間

オートスイッチを有効にしたとき、カメラの切り替えが滞留するまでの時間(秒)。5~300秒の範囲です。

- 3. 表示設定に移動して、ビューレイアウトを設定します。
- 4. 設定を保存するには、OKをクリックします。

3.1.3 ライブビューレイアウトの設定

ライブビューは、各カメラから得られるビデオ画像をリアルタイムで表示する。

カスタムライブビューレイアウトの設定

- 1. 「システム→ライブビュー→ビュー」に移動します。
- 2. カスタムレイアウトの設定をクリックします。
- 3. Custom Layout Configuration インターフェースをクリックします。
- 4. レイアウト名を編集します。

5. ツールバーからウィンドウ分割モードを選択します。

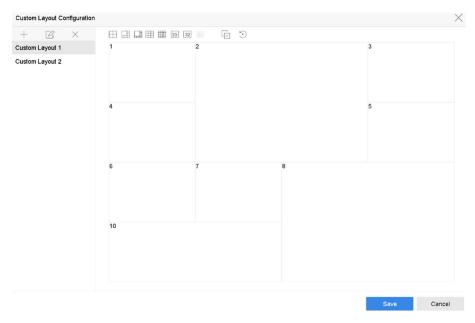


図3-2 ライブビューレイアウトの設定

- 6. 複数のウィンドウを選択し、クリックしてウィンドウを結合します。選択したウィンドウは矩形領域にある必要があります。 🖸
- 7. 保存をクリックします。 正常に設定されたレイアウトがリストに表示されます。
- 8. 必要に応じて、リストからライブビューレイアウトを選択し、をクリックして名前を編集するか、をクリックして名前を削除します。 ②×

ライブビューモードの設定

手順

- 1. 「システム→ライブビュー→ビュー」に移動します。
- 2. ビデオ出力インターフェイスを選択します。
- 3. ツールバーからレイアウトまたはカスタムレイアウトを選択します。
- 4. 分割ウィンドウを選択し、リスト内のカメラをダブルクリックして、カメラをウィンドウにリンクします。

迎注

- カメラの順序を設定するには、Live Viewインタフェースの目的のウィンドウにカメラをクリックアンドドラッグすることもできます。
- テキストフィールドに数字を入力して、リストからカメラを迅速に検索することもできます。
- 5. 適用をクリックします。

6. 必要に応じて、クリックしてすべてのチャンネルのライブビューを開始するか、クリックしてすべてのライブビューチャンネルを停止します。□□

3.1.4 Channel-Zero Encoding の設定

画像の質に影響を及ぼさずにバンド幅の必要性を減らすために、ウェブ・レーザーやCMS (Client Management System)ソフトウェアから多くのチャネルをリアルタイムで遠隔視野に入れる必要がある場合は、チャネルーゼロ符号化を有効にします。

手順

- 1. 「システム→ライブビュー→チャンネルゼロ」に移動します。
- 2. Enable Channel-Zero Encodingをチェックします。



図 3-3 チャネルゼロ符号化

- 3. フレームレート、最大を設定します。Bitrate Mode(ビットレートモード)およびMax(最大)。硝酸塩。より高いフレームレートおよびビットレートは、より高い帯域幅を必要とする。
- 4. 適用をクリックします。
 CMS またはWeb ブラウザを介して、すべてのチャンネルを1 つの画面に表示できます。

3.1.5 補助モニターを使用する

また、Auxモニターにあるときに、Live Viewの特定の機能を使用することもできます。特徴は以下の通りである:

シングルスクリーン

選択したカメラのフルスクリーン表示に切り替えます。ドロップダウンリストからカメラを選択できます。

マルチ画面

異なる表示レイアウトオプションを切り替えます。レイアウトオプションはドロップダウンリストから選択できます。

次画面

「Live View」で最大数未満のカメラを表示する場合は、この機能をクリックすると次の表示に切り替わります。

再生

再生モードに入ります。

PTZ制御

PTZ制御モードに入ります。

メインモニタ

Main operation modeを入力します。

〕注

メイン出力モニタのライブビューモードでは、Aux出力モード中はメニュー操作ができません。

3.2 デジタルズーム

デジタルズームは、異なる倍率(1×~16×)でライブ画像にズームインします。

手順

- 1. ライブビューを開始し、ツールバーからをクリックします。 ⊕
- 2. スライドバーを動かすか、マウスホイールをスクロールして、画像を異なる倍率(1×~16×)に ズームイン/ズームアウトします。



図3-4 デジタルズーム

3.3 ライブビュー戦略

- ライブビューモードでクリックすると、デジタルズーム操作インタフェースはフルスクリーンモードになります。
- 2. リアルタイム、バランス、またはフルエンシーにライブビューストラテジを選択します。

3.4 顔面認知

顔認識インターフェイスを入力すると、リアルタイムの顔認識と見知らぬ人の認識結果を表示できます。

開始前に

顔検出機能と顔画像比較機能を設定していることを確認するには、詳細を参照してください。

手順

- 1. ライブビューインターフェイスに移動し、ツールバーでをクリックします。 🖸
- 2. またはをクリックして、ウィンドウ分割を設定します。
- 3. 任意のウィンドウを選択します。
- 4. 左下のカメラ一覧からカメラをダブルクリックします。



図3-5 顔の認識

- 5. 「レコード」をクリックして、選択したカメラのリアルタイム顔認識レコードを表示します。レコード は右側のウィンドウにも表示されます。合計数、成功数、失敗数を含めて、顔検出数を上から 見ることができます。
- 6. オプション:登録されていない顔画像の場合は、レコードリストでダブルクリックして顔画像ライブラリーに追加できます。

[ji注

ゲストユーザおよびオペレータユーザの場合、顔写真ライブラリに未登録の顔写真を追加するには、ローカルパラメータ設定権限が必要です。

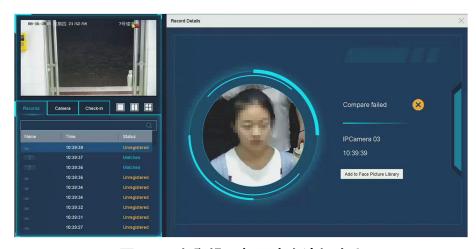


図 3-6 未登録の顔写真を追加する

- 7. オプション:「チェックイン」をクリックして、「合計番号」、「チェックイン」、「未チェックイン」などの 顔画像ライブラリのチェックインレコードを表示します。
- 8. オプション:右上隅をクリックして、必要に応じて表示設定を構成します。 🔯

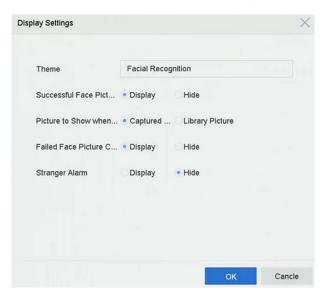


図 3-7 顔認識表示設定

- 9. (オプション) 右上隅をクリックして、レコードを検索およびエクスポートします。 🔞
 - 1) 必要に応じて検索パラメータを設定します。
 - 2) 検索をクリックします。
 - 3) 「アテンダンスレコードのエクスポート」または「チェックインレコードのエクスポート」をクリックします。

迎注

- エクスポートする前に、USB フラッシュドライブが挿入されていることを確認してください。
- レコードをクリックして、カレンダー内のこの個人の出席情報を確認できます。
- ゲストおよびオペレータのユーザの場合、レコードを検索してエクスポートするには、「ローカルビデオエクスポート許可」(「カメラ許可」)が必要です。



図 3-8 顔認識検索レコード

3.5 PTZ制御

3.5.1 PTZ パラメータの設定

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

- 1. PTZカメラのライブビューのクイック設定ツールバーをクリックします。 🖺
- 2. PTZ Parameters Settings をクリックして、PTZ パラメータを設定します。

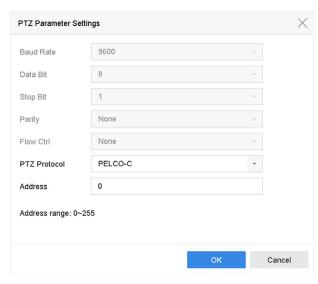


図3-9 PTZ パラメータの設定

3. PTZ パラメータを編集します。

[i]注

全てのパラメータは、PTZカメラパラメータと正確に一致しなければならない。

4. 設定を保存するには、OKをクリックします。

3.5.2 プリセットを設定する

PTZ位置、ズーム、フォーカス、アイリスなどの状態をプリセットで記録します。プリセットを呼び出して、カメラをすばやく定義済みの位置に移動させることができます。

- 1. PTZカメラのライブビューのクイック設定ツールバーをクリックします。≤
- 2. 方向ボタンをクリックして、カメラを場所にホイールします。
- 3. ズーム、フォーカス、アイリスの状態を調整します。
- 4. ライブビューの右下隅にあるをクリックして、プリセットを設定します。



図 3-10 プリセット設定

- 5. ドロップダウンリストからプリセット番号(1~255)を選択します。
- 6. プリセット名を入力します。
- 7. 「適用(Apply)」をクリックしてプリセットを保存します。
- 8. オプション:「キャンセル」をクリックすると、プリセットの位置情報がキャンセルされます。
- 9. 必要に応じて、ライブビューの右下隅にあるをクリックして、設定済みのプリセットを表示します。

 ■



図3-11 設定済みのプリセットの表示

3.5.3プリセットを呼び出す

プリセットは、イベントが発生したときに、カメラがウィンドウのような指定された位置を指示することを可能にする。

手順

- 1. PTZカメラのライブビューのクイック設定ツールバーをクリックします。 \(\times \)
- 2. ライブビューの右下隅にあるをクリックして、プリセットを設定します。
- 3. ドロップダウンリストからプリセットNo.を選択します。
- 4. 「呼び出し」をクリックして呼び出すか、ライブビューの右下隅にあるをクリックして、設定済みのプリセットをクリックして呼び出します。 ■



図 3-12 コールプリセット(1)



図 3-13 コールプリセット(2)

3.5.4 パトロールの設定

パトロールは、PTZをキーポイントに移動させ、次のキーポイントに移動する前に、設定された持続時間の間そこに留まるように設定することができる。キーポイントはプリセットに対応しています。

- 1. PTZカメラのライブビューのクイック設定ツールバーをクリックします。 🖺
- 2. パトロールをクリックしてパトロールを設定します。



図 3-14 パトロールの設定

- 3. パトロールNo.を選択します。
- 4. 設定をクリックします。

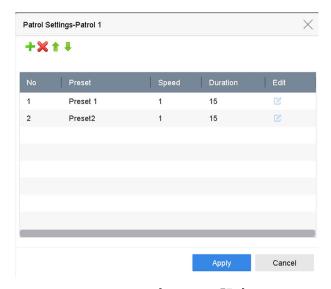


図 3-15 パトロール設定

5. クリックして、パトロールにキーポイントを追加します。+

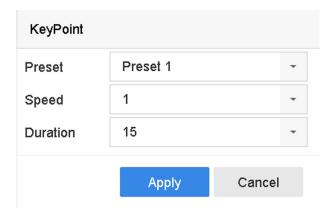


図3-16 キーポイントの構成

1) キーポイントパラメータを設定します。

プリセット

パトロールを循環しながらPTZが従う順序を決定する。

速度

PTZ があるキーポイントから次のキーポイントに移動する速度を定義します。

期間

該当するキーポイントに滞在する時間を指します。

- 2) 適用をクリックして、パトロールにキーポイントを保存します。
- 6. その他の動作は以下の通りである。

表3-1 動作説明

操作	説明	操作	説明
×	削除するキーポイン トを選択します。		追加したキーポイン トを編集します。
t	キーポイントの順序 を調整します。		キーポイントの順序 を調整します。

7. 「適用」をクリックして巡回設定を保存します。

3.5.5パトロールを呼び出す

パトロールを呼び出すと、PTZは所定のパトロール経路に従って移動する。

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



図 3-17 パトロールの設定

- 3. パトロールを選択します。
- 4. Call(呼び出し)をクリックしてパトロールを開始します。
- 5. 必要に応じて、「停止」をクリックしてパトロールを停止します。

3.5.6 パターンの設定

パターンは、PTZの動きを記録することによって設定することができる。パターンを呼び出すと、定義済みのパスに従ってPTZ を移動させることができます。

手順

- 1. PTZカメラのライブビューのクイック設定ツールバーをクリックします。 ≗
- 2. パターンを設定するには、パターンをクリックします。



図 3-18 パターン構成

- 3. パターンNo.を選択します。
- 4. パターンを設定します。
 - 1) 録音を開始するには、録音をクリックします。
 - 2) コントロールパネルの対応するボタンをクリックして、PTZカメラを移動します。
 - 3)「停止」をクリックして録画を停止します。PTZ移動はパターンとして記録される。

3.5.7パターンを呼び出す

手順に従って、定義済みのパターンに従ってPTZ カメラを移動します。

- 1. PTZカメラのライブビューのクイック設定ツールバーをクリックします。 🖺
- 2. パターンを設定するには、パターンをクリックします。

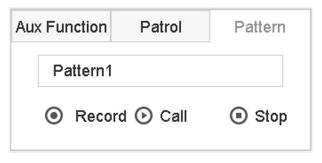


図 3-19 パターン構成

- 3. パターンを選択します。
- 4. 「呼び出し」をクリックしてパターンを開始します。
- 5. (オプション)「停止(Stop)」をクリックしてパターンを停止します。

3.5.8 リニアスキャンリミットの設定

リニアスキャンは、所定の範囲内で水平方向のスキャンをトリガする。

Before You Start

接続されているIPカメラがPTZ機能をサポートし、正しく接続されていることを確認します。

[i];

この関数は、一部のモデルでのみサポートされています。

手順

- 1. PTZカメラのライブビューのクイック設定ツールバーをクリックします。 🕹
- 2. 方向ボタンをクリックしてカメラをある場所にホイールし、「左限界」または「右限界」をクリックして、その場所を対応する限界にリンクします。

[ji注

速度ドームのリニアスキャンは、左限界から右限界まで行われ、左限界を右限界の左側に設定する必要があります。また、左側の限界から右側の限界までの角は、180°以下でなければならない。

3.5.9 ワンタッチ公園

ある速度ドームモデルは、不活動期間(駐車時間)の後に、自動的に所定の駐車動作(スキャン、 プリセット、パトロールなど)を開始するように構成することができる。

開始前に

この機能を動作させる前に、接続されているカメラがリニアスキャンに対応しており、HIKVISIONプロトコルになっていることを確認してください。

手順

- 1. PTZカメラのライブビューのクイック設定ツールバーをクリックします。 ≗
- 2. パーク(クイックパトロール)、パーク(パトロール1)、またはパーク(プリセット1)をクリックして、パークアクションを有効にします。

公園(クイックパトロール)

ドームは、駐車時間の後、所定のプリセット1からプリセット32まで順番にパトロールを開始する。未定義のプリセットはスキップされます。

公園(パトロール1)

ドームは、駐車時間の後、所定のパトロール1経路に従って移動を開始する。

パーク(プリセット1)

ドームは、駐車時間の後、予め定められた予め設定された1つの位置に移動する。

门i注

駐車時間は、スピードドーム構成インターフェースを介してのみ設定することができる。デフォルト値は、デフォルトでは5 秒です。

3. オプション: Stop Park (クイックパトロール)、Stop Park (パトロール1)、Stop Park (プリセット1) をクリックして無効にします。

3.5.10 補助関数

可視光、ワイパー、3D ポジショニング、PTZ コントロールパネルの中央を含む補助機能を操作できます。

開始前に

接続されているIPカメラがPTZ機能をサポートしており、正しく接続されていることを確認します。

手順

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



図 3-20 Aux Function Configuration

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

 アイコン
 説明

 ライトのオン/オフ
 ワイパーのオン/オフ

 ③①
 3Dポジショニング

 中央

表3-2 Aux 機能アイコンの説明

第 4 章録音と再生

4.1 記録

4.1.1 記録パラメータの設定

「カメラ→のビデオパラメータ」に移動します。

メインストリーム

メインストリームとは、ハードディスクドライブに記録されたデータに影響を与え、記録品質や画像サイズを直接決定するプライマリストリームのことです。

サブストリームと比較して、メインストリームは、より高い解像度およびフレームレートを有するより高品質のビデオを提供することができる。

フレームレート(FPS - Frames per Second)

これは、毎秒いくつのフレームが捕捉されるかを指す。より高いフレームレートは、ビデオストリームに動きがあるときに、全体を通して画質を維持するので有利である。

解像度

画像解像度は、デジタル画像がどれだけのディテールを保持することができるかの尺度である。解像度が大きいほど、細部のレベルは大きくなる。解像度は、ピクセル列の数(幅)×ピクセル行の数(高さ)、例えば1024×768として指定することができる。

硝酸塩

ビットレート(kbit/sまたはMbit/s)は、しばしば速度と呼ばれるが、実際には、距離/時間単位ではなく、ビット/時間単位の数を定義する。

H.264+を有効にする

H. 264+は、インテリジェント分析技術を予測符号化、雑音抑圧、および長期ビットレート制御と組み合わせて、より低いビットレートを実現し、これは、記憶コストの削減において重要な役割を果たし、投資のためのより高いリターン値を提供する。

H.265+を有効にする

H. 265+は、標準H.265/HEVC圧縮に基づく最適化された符号化技術である。H.265+では、ビデオ品質は、H.265/HEVCとほぼ同じであるが、必要とされる伝送帯域幅および記憶容量がより少ない。

オーディオ

オーディオ入力信号源。

[i]注

- 解像度、フレームレート、ビットレートを高く設定すると、ビデオ品質が向上しますが、より多くのインターネット帯域幅が必要になり、ハードディスクドライブのストレージ容量が増えます。
- H. 264+またはH.265+コード化技術は、特定のモデルについてのみ利用可能である。
- DS-7100HQHI-K、DS-7204/7208/7216HQHI-K、DS-710HUHI-K、DS-7200HUHI-K、DS-7200HUHI-K、DS-7200HTHI-K、iDS-7200HQHI-K1/S(B)、iDS-7200HQHI-K2/4S(B)、iDS-7200HUHI-K/4S(B)、iDS-7200HQHI-M、iDS-7200HQHI-M、iDS同軸ケーブル経由でオーディオを送信します。
- Audio as Camera を選択する前に、カメラがオーディオを同軸ケーブルを介して送信するのをサポートしていることを確認してください。
- ●「Audio as Camera」を選択した場合、ローカルオーディオ入力信号は使用不可になります。

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実行される2 番目のコーデックです。これにより、 ダイレクトレコーディングの品質を犠牲にすることなく、送信インターネット帯域幅を削減すること ができます。

サブストリームは、多くの場合、ライブビデオを見るためにアプリによって専ら使用される。制限されたインターネット速度を有するユーザは、この設定から最も利益を得ることができる。

ピクチャ

ピクチャは、連続またはイベント記録タイプのライブピクチャキャプチャを指す。(→取り込み予定 →の詳細

画質

画質を低、中、高に設定します。より高い画質は、より多くの記憶空間要件をもたらす。

間隔

ライブ画像を撮影する間隔。

キャプチャ遅延時間

ピクチャの撮影時間。

高度な録音パラメータの設定

- 1. 保存→予定→レコードに移動します。
- 2. 「スケジュールを有効にする」をオンにすると、予約録音が有効になります。
- 詳細パラメータを設定するには、詳細をクリックします。

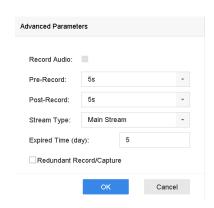


図 4-1 詳細レコード設定

録音

オーディオ録音を有効または無効にします。

プリレコード

予約時刻またはイベントの前に録音するように設定した時刻。たとえば、10:00にアラームが鳴った場合、録画前時刻を5秒に設定した場合、カメラは9:59:55に録画します。

ポストレコード

イベント後またはスケジュールされた時刻に記録するように設定した時刻。たとえば、アラームトリガー録画が11:00に終了し、録画後時刻を5秒に設定すると、11:00:05まで録画されます。

ストリームタイプ

メインストリームおよびサブストリームは、記録のために選択可能である。サブストリームを 選択すると、同じ保存領域でより長い時間録画できます。

期限切れ

有効期限は、記録されたファイルがHDDに保存される期間である。期限に達すると、ファイルは削除されます。期限切れ時間を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持時間は、HDDの容量によって決定されるべきである。

冗長レコード/キャプチャ

冗長録画またはキャプチャを有効にすると、録画とキャプチャ画像が冗長HDD に保存されます。

4.1.2 H.265 ストリームアクセスの有効化

デバイスは、初期アクセスのために(H.265ビデオフォーマットをサポートする)IPカメラのH.265ストリームに自動的に切り替えることができる。

「カメラ→詳細設定」→ H.265「自動切替設定」に移動して、機能を有効にします。

4.1.3 手動録音

ライブビューで動画の録画を手動で開始/停止するには、クリックします。 🗂

4.1.4 計画レコーディングの構成

設定した録画スケジュールに従って、カメラが自動的に録画を開始/停止します。

開始する前に

- ビデオファイル、画像、ログファイルを保存する前に、HDD をデバイスにインストールしたか、 ネットワークディスクを追加したことを確認します。
- Motion, Alarm, M | を有効にする前にA(モーションまたはアラーム)、M & A(モーションおよびアラーム)、イベントトリガ記録およびキャプチャを有効にする前に、モーション検出設定、アラーム入力設定、その他のイベントも設定する必要があります。詳細は参照。

手順

- 1. 保存→予定→レコードに移動します。
- 2. カメラを選択します。
- 3. 「スケジュールを有効にする」をチェックします。
- 4. 録画タイプを選択します。

連続

予約録画

イベント

すべてのイベント・トリガー・アラームによってトリガーされた記録。

モーション

動き検出をトリガとした記録。

アラーム

アラームを契機とした録音

M/A

記録は、動き検出またはアラームのいずれかによってトリガされる。

M&A

モーション検出とアラームによってトリガーされる録画。

POS

POS、アラームを契機とした録音

5. タイムバーのカーソルをドラッグして、録画スケジュールを設定します。

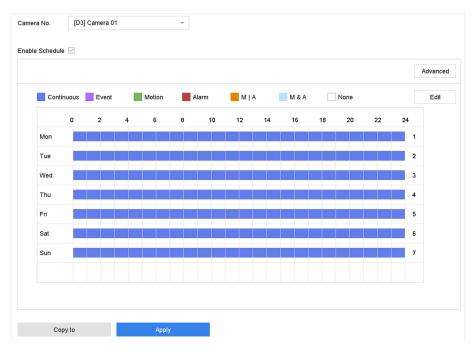


図 4-2 記録スケジュール

〔i注

- 上記の手順を繰り返して、曜日ごとにスケジュール録画またはキャプチャを設定できます。
- 連続記録はデフォルトで毎日適用されます。
- 6. オプション: 録画スケジュールを他のカメラにコピーします。
 - 1) コピー先をクリックします。
 - 2) 同じスケジュール設定で重複するカメラを選択します。
 - 3) [OK]をクリックします。
- 7. 適用をクリックします。

4.1.5 連続録音の設定

装置は、設定された時間スケジュール内でビデオを連続的に記録することができる。

- 1. カメラ→符号化パラメータ→記録パラメータに進む。
- 2. カメラの連続主流/副流記録パラメータを設定します。
- 3. 「保存→記録予定」に移動します。
- 4. タイムバー上でマウスをドラッグして、連続録画スケジュールを設定します。詳細については、「プラン記録の設定」を参照してください。

4.1.6 動き検出トリガ記録の設定

モーション検出イベントによってトリガーされる録画を設定できます。

手順

- 1. →事象→正常事象→動き検知に進む。
- 2. モーション検出を設定し、モーションイベントが発生したときに記録をトリガーするチャネル(複数可)を選択します。詳細については、「リンクアクションの設定」を参照してください。
- 3. カメラ→符号化パラメータ→記録パラメータに進む。
- 4. カメラのイベントメインストリーム/サブストリーム記録パラメータを設定します。
- 5. 「保存→記録予定」に移動します。
- 6. 「モーション」の録画タイプを選択します。
- 7. タイムバー上でマウスをドラッグして、モーション検出録画スケジュールを設定します。詳細については、「プラン記録の設定」を参照してください。

4.1.7 イベントトリガー記録の設定

動き検出、動き検出、アラーム、顔検出、車両検出、ラインクロス検出などをトリガーに録音を設定できます。

手順

- 1.「システム→イベント」に進みます。
- 2. イベント検出を設定し、イベント発生時に記録をトリガするチャネルを選択します。詳細はイベントを参照してください。
- 3. カメラ→符号化パラメータ→記録パラメータに進む。
- 4. カメラのイベントメインストリーム/サブストリーム記録パラメータを設定します。
- 5.「保存→記録予定」に移動します。
- イベントする録音タイプを選択します。
- 7. タイムバーの上でマウスをドラッグして、イベント検出録画スケジュールを設定します。詳細については、「プラン記録の設定」を参照してください。

4.1.8 アラーム起動記録の設定

動き検出、顔検出、車両検出、ラインクロス検出などをトリガーに録音を設定できます。

- 1. →事象→正常事象→アラーム入力に進む。
- 2. アラーム入力を設定し、アラームが発生したときに録音をトリガするチャンネルを選択します。 詳細はイベントを参照してください。
- 3. カメラ→符号化パラメータ→記録パラメータに進む。
- 4. カメラのイベントメインストリーム/サブストリーム記録パラメータを設定します。
- 5.「保存→記録予定」に移動します。

- 6. アラームに録音する種類を選択します。
- 7. タイムバー上でマウスをドラッグすると、アラーム録音スケジュールが設定されます。詳細については、「プラン記録の設定」を参照してください。

4.1.9 画像キャプチャの設定

ピクチャは、連続またはイベント記録タイプのライブピクチャキャプチャを指す。この機能をサポートするのは、特定のモデルのみです。

手順

- 1. 取り込み→に「カメラ→符号化パラメータ」に移動します。
- 2. ピクチャパラメータを設定します。

解像度

撮影する画像の解像度を設定します。

画質

画質を低、中、高に設定します。より高い画質は、より多くの記憶空間要件をもたらす。

間隔

ライブ画像を撮影する間隔。

- 3.「保存→取り込みスケジュール」に移動します。
- 4. カメラを選択して写真撮影を設定します。
- 5. 撮影スケジュールを設定する。詳細については、「プラン記録の設定」を参照してください。

4.1.10 ホリデイレコーディングの設定

休日に録画する予定が異なる場合もありますので、年間の休日の録画予定を設定できます。

- 1.「システム→休暇」に移動します。
- 2. 一覧から休日項目を選択します。
- 3. クリックして、選択した休日を編集します。 🗹
- 4. 有効をチェックします。

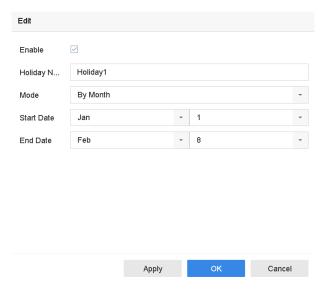


図4-3 休日設定の編集

- 5. ホリデー名、モード、開始日、終了日を設定します。
- 6. [OK]をクリックします。
- 7. ホリデー録音のスケジュールを設定します。詳細については、「プラン記録の設定」を参照してください。

4.1.11 冗長録画とキャプチャの設定

R/W HDDのみならず、冗長HDDにも記録ファイルや撮影画像を保存することを意味する冗長記録・キャプチャを可能にすることで、データの安全性・信頼性を効果的に高めることができる。

開始前に

HDD プロパティを Redundancy(冗長性)に設定する前に、ストレージモードを Group(グループ) に設定する必要があります。詳細については、「HDD グループの構成」を参照してください。少なくとも、読み取り/書き込みステータスの別のHDD がある必要があります。

- 1. Storage → Storage Device に移動します。
- 2. リストからHDD を選択し、をクリックしてローカルHDD 設定インターフェイスに入ります。☑
- 3. HDD プロパティをRedundancy に設定します。
- 4. 保存→スケジュール設定→録画スケジュール/キャプチャスケジュールに移動します。
- 5. [詳細設定]をクリックして、カメラの記録パラメータを設定します。

Advanced Parameters				
Record Audio:				
Pre-Record:	5s		~	
Post-Record:	5s		•	
Stream Type:	Main Stream		•	
Expired Time (day):		5		
Redundant Record/Capture				
	ок	Can	icel	

図4-4 レコードパラメータ

- 6. Redundant Record/Captureをチェックします。
- 7. OK をクリックして設定を保存します。

4.1.12 1080p ライトモードの設定

1080P Lite Mode を有効にすると、1080P Lite でのエンコード解像度(リアルタイム)がサポートされます。そうでない場合は、最大1080P(非リアルタイム)がサポートされています。 1080Pライトモードを有効または無効にするには、「ストレージ→アドバンスト」に移動します。

4.2 再生

4.2.1 インスタント再生

インスタント再生では、過去5分間に録画された録画ビデオファイルを再生できます。ビデオが見つからない場合、これは、最後の5分間に記録がないことを意味する。

ライブビューでカメラを選択した後、カーソルをウィンドウ下部に移動してツールバーにアクセスし、をクリックしてインスタント再生を開始できます。♡



図4-5 再生インターフェイス

4.2.2 通常の動画を再生

再生に進み、日付とカメラを選択し、下部のツールバーを使用して再生操作を実行します。再生操作を参照してください。カメラをクリックすると、複数のカメラを同時に再生できます。

[ji注

256倍の再生速度がサポートされています。



図4-6 通常のビデオインターフェイスの再生

4.2.3 スマート検索動画を再生する

スマート再生モードでは、デバイスは、動き、線、または侵入検出情報を含むビデオを分析し、そ

れらを赤色でマークすることができる。

再生に移動し、スマートをクリックしてから、下部のツールバーでラインクロス検知()や侵入検知()などの検知イベントを選択し、目的に応じてビデオを再生します。 🔍 🗌

人間と車両の動き検出を可能にした特定のアナログカメラでは、人間と車両のターゲットをクリックしたり、検索したりすることができます。人間または車両のターゲットを含むビデオを再生しているとき、デバイスは、ビデオ(人間または車両のターゲットを含む)を使用して、ラインクロス検出()または侵入検出()の二重分析を適用することができません。

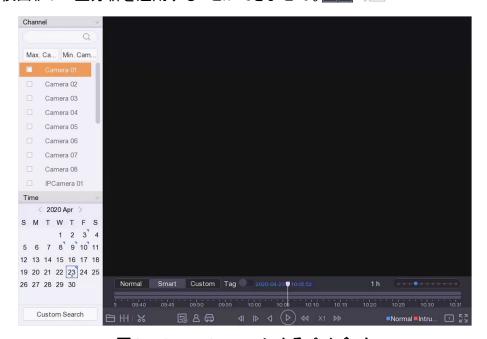


図4-7 Smart Search によるペイパック

4.2.4 カスタム検索ファイルの再生

検索条件をカスタマイズして動画を再生できます。

- 1. 再生に移動します。
- 2. リストからカメラを選択します。
- 3. 左下のカスタム検索をクリックします。
- 4. 時間、ファイルステータス、イベントタイプなどの検索条件を入力します。

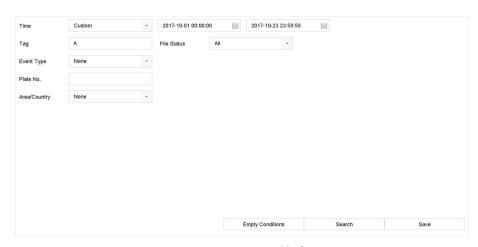


図4-8 カスタム検索

5. 検索をクリックします。

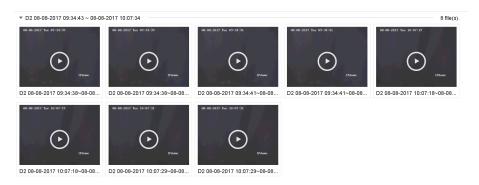


図4-9 カスタム検索ビデオファイル

6. ファイルを選択し、検索結果インターフェイスでビデオの再生を開始します。

4.2.5 タグファイルの再生

ビデオタグを使用すると、再生中に、特定の時点の人や場所などの情報を記録できます。ビデオタグを使用して、ビデオファイルや位置のタイムポイントを検索できます。

タグファイルの追加

- 1. 再生に移動します。
- 2. 動画ファイルを検索して再生します。
- 3. クリックしてタグを追加します。
- 4. タグ情報を編集します。
- 5. [OK]をクリックします。

[_i注

1 つのビデオファイルに最大64 個のタグを追加できます。

タグファイルの再生

手順

- 1. 再生に移動します。
- 2. 左下のカスタム検索をクリックします。
- 3. 時刻とタグキーワードを含む検索条件を入力します。

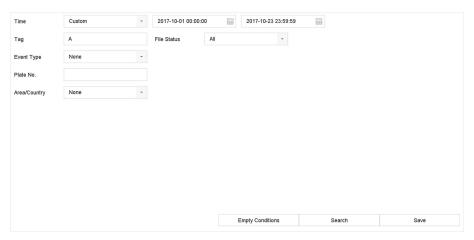


図4-10 タグ検索

4. 検索をクリックします。

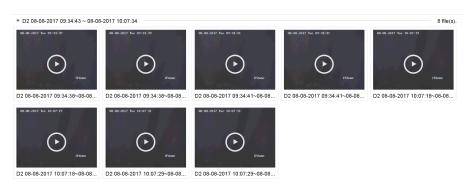


図4-11 検索タグファイル

5. タグファイルを選択し、検索結果インターフェイスでビデオを再生します。

4.2.6 サブピリオド別再生

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. 再生に移動します。
- 2. 左下隅にあるをクリックします。 日日
- 3. カメラを選択します。
- 4. 動画を検索する開始時刻と終了時刻を設定します。
- 5. 右下隅の別のマルチピリオド(4ピリオドなど)を選択します。

[i注

分割画面の定義数に従って、選択した日付のビデオファイルを平均セグメントに分割して再生できます。たとえば、16:00 ~22:00 の間に既存のビデオファイルがあり、6 画面表示モードが選択されている場合、各画面で同時に1 時間のビデオファイルを再生できます。

4.2.7 ログファイルの再生

システムログを検索した後、チャンネルに関連付けられた録画ファイルを再生します。

手順

- 1. 保守→履歴情報に移動します。
- 2. ログ検索をクリックします。
- 3. 検索時間とタイプを設定し、「検索」をクリックします。

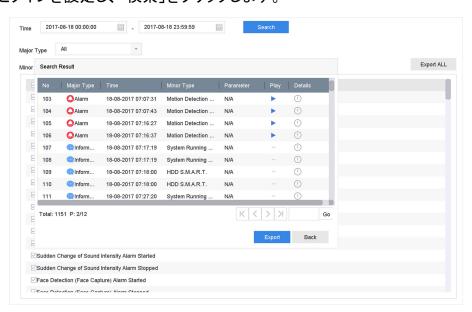


図4-12 システムログ検索インタフェース

4. ビデオファイルのあるログを選択し、をクリックしてログファイルの再生を開始します。

4.2.8 外部ファイルの再生

外部記憶装置からファイルを再生できます。

開始前に

ストレージデバイスをビデオファイルとデバイスに接続します。

手順

- 1. 再生に移動します。
- 2. 左下隅にあるをクリックします。
- 3. ファイルをクリックするか、ダブルクリックして再生します。>

4.3 再生操作

4.3.1 通常/重要/カスタムビデオ

再生中に、次の3つのモードを選択して動画を再生できます。

通常

連続録画からのビデオファイル。

重要

イベントおよびアラーム録画からのビデオファイルが録画をトリガしました。

カスタム

カスタム条件で検索されたビデオファイル。

4.3.2 重要/カスタムモードでの再生方法の設定

スマートまたはカスタムビデオ再生モードになっているときは、通常のビデオとスマート/カスタムビデオに別々に再生速度を設定することも、通常のビデオをスキップするように選択することもできます。

スマート/カスタムビデオ再生モードで、をクリックして再生ストラテジーを設定します。 🗟

- 通常動画を再生しないことを確認すると、通常動画をスキップし、スマート(モーション/ラインクロス/イントルージョン)動画とカスタム(検索動画)を通常速度(X1)でのみ再生します。
- 「通常のビデオを再生しない」がチェックされていない場合、通常のビデオの再生速度をスマート/カスタムビデオに個別に設定できます。速度範囲はX1~XMAXです。

[ji]注

シングルチャンネル再生モードでのみ速度を設定できます。

4.3.3 ビデオクリップの編集

再生中にビデオクリップを切り取り/書き出しできます。

手順

- 1. 再生に進む
- 2. 下部のツールバーでをクリックします。※
- 3. 開始時刻と終了時刻を設定します。クリックして期間を設定するか、タイムバーに時間セグメントを設定できます。Ы
- 4. ビデオクリップをストレージデバイスに保存する場合にクリックします。 🗎

4.3.4 メインストリームとサブストリームの切り替え

再生中にメインストリームとサブストリームを切り替えることができます。

アイコン	説明
Ç—;	ビデオをメインストリームで再生します。
Ĉ-j	ビデオをサブストリームで再生します。

[ji注

主流と副流のための符号化パラメータは、保存→符号化パラメータの中で構成されることがある。

4.3.5 サムネイルビュー

再生インターフェイスのサムネイルビューを使用すると、タイムバーで必要なビデオファイルを簡単に見つけることができます。

再生モードで、タイムバーにカーソルを置くと、プレビューサムネイルが表示されます。

図4-13 サムネイルビュー

サムネイルをクリックすると、フルスクリーン再生に入ることができます。

4.3.6 高速表示

マウスを押したままタイムバーをドラッグすると、ビデオファイルがすばやく表示されます。 ビデオ再生モードで、再生タイムバーをマウスでホールド&ドラッグすると、ビデオファイルが高速 に表示されます。

フルスクリーン再生に入るには、必要な時点でマウスを放します。

4.3.7 デジタルズーム

デジタルズームは、異なる倍率(1×~16×)でライブ画像にズームインします。

- 1. ライブビューを開始し、ツールバーからをクリックします。 ⊕
- 2. スライドバーを動かすか、マウスホイールをスクロールして、画像を異なる倍率 $(1 \times \sim 16 \times)$ に ズームイン/ズームアウトします。



図4-14 デジタルズーム

第 5 章スマート分析

5.1 エンジン構成

各エンジンは、その動作モードとして指定されたVCAタイプを処理する。必要に応じて、エンジンの作業モードを設定できます。

手順

i注

この章は、iDSシリーズの特定のモデルでのみ使用できます。

- 1. Smart Analysis → Smart Analysis → Engine Configurationに進みます。
- 2. 各エンジンの使用を設定します。各機能のエンジン温度とリンクされたチャネル状態を表示できます。

li注

エンジンがチャネルにバインドされている場合、スイッチングエンジン動作モードは、エンジンおよびチャネルのバインドを解除し、チャネルの関連するスマートイベントをキャンセルする。

3. [適用] をクリックして、設定を保存します。

5.2 タスク設定

タスク設定でタスクステータスを表示できます。スマート分析結果は、関心のある人体および車両の画像を検索するときに画像をフィルタリングするために使用される。

開始前に

人体検知/車両検知、線路横断検知、侵入検知、領域入口、または領域出口については、VCA Picturesを保存を確認してください。

手順

道注

この章は、iDSシリーズの特定のモデルでのみ使用できます。

1. Smart Analysis → スマート解析タスクコンフィギュレーションに移動します。

- 2. カメラをチェックして、対応する解析モードを有効にします。選択した分析モードでエンジンが使用可能であることを確認します。
- 3. 自動分析を有効にします。

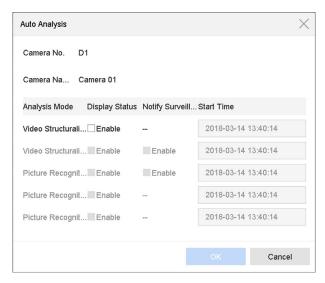


図5-1 自動解析

- 1) 編集をクリックします。
- 2) オプション: Display Status とNotify Surveillance Center のEnable をチェックします。
- 3) 分析するビデオの開始時刻を設定します。
- 4) [OK]をクリックします。
- 4. カメラを確認し、「Enabled」をクリックして分析を開始します。

タスクステータスには、Disabled、Waiting、およびEnabled の3 つの条件があります。

- Disabled: カメラで分析タスクが有効になっていません。
- 待機中:カメラの分析タスクが有効になります。デバイスはデータの分析を待機しています。
- Enabled: カメラの分析タスクが有効になり、デバイスがカメラのデータを分析しています。
- 5. オプション: 非リアルタイム顔画像比較分析モードの場合、記録の表示をクリックして毎日の進 行状況を表示します。

5.3 拡張VCA モードの設定

強化されたVCAモードをイネーブルすることは、回線交差検出および侵入検出のための接続可能なチャネル番号を最大にする。ただし、HUHI-Kシリーズでは、2K/4K HDMI出力解像度と4 MP/5 MP/8 MP信号入力を無効にします。また、HQHI-Kシリーズでは、CVBS出力およびチャネルゼロ符号化を無効にします。

「システム→全般」に進み、「拡張VCAモード」を確認します。

5.4 顔画像の比較

デバイスは、顔認識機能に基づいて、接続されたカメラの顔画像比較アラームおよび顔キャプチャをサポートします。

Smart Analysis → Smart Analysis → Engine Configurationに進みます。Facial Recognition として少なくとも1 つのエンジン使用量を設定します。詳細は、「エンジン構成」を参照してください。

〔〕 注

この章は、iDSシリーズの特定のモデルでのみ使用できます。

5.4.1 顔面検出

顔検出は、監視シーンに現れる顔を検出する。リンク動作は、人間の顔が検出されたときにトリガすることができる。

- 1. →ユーティリティのイベント→スマートイベントに移動します。
- 2. 「Face Detection」をクリックします。

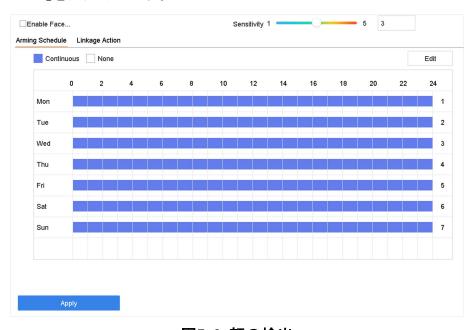


図5-2 顔の検出

- 3. 設定するカメラを選択します。
- 4. Enable Face Detectionをチェックします。
- 5. オプション: Save VCA Picture(VCA ピクチャの保存)をチェックして、キャプチャした顔検出のピクチャを保存します。
- 6. 検出感度を設定します。感度範囲:[1-5]値が高いほど、顔が検出されやすくなる。
- 7. アーミングスケジュールを設定します。Configure Arming Scheduleを参照してください。

- 8. リンクアクションを設定します。「リンクアクションの設定」を参照してください。
- 9. 適用をクリックします。

5.4.2 顔画像ライブラリ管理

顔画像ライブラリは、主に顔画像記憶および顔画像比較に使用される。

顔画像ライブラリーを追加する

ローカルGUI またはGuarding Vision アプリを使用して顔画像ライブラリを作成できます。ここでは、ローカルGUI での操作を例に説明します。

手順

- 1. Smart Analysis → Face Picture Database に移動します。
- 2. クリック +
- 3. 顔写真ライブラリ名を入力します。
- 4. [OK]をクリックします。

[i]注

またはをクリックして、ライブラリー名を編集したり、ライブラリーを削除したりできます。

顔写真をライブラリにアップロードする

顔画像の比較は、ライブラリ内の顔画像に基づく。1枚の顔写真をアップロードしたり、複数の顔写真をライブラリにインポートすることができます。

開始前に

- 画像形式が JPEG または JPG であることを確認します。
- 各ピクチャについて、1つの顔しか持っていないことを確認します。あらかじめすべてのピクチャをバックアップデバイスにインポートしておきます。

画像はJPEG またはJPG 形式である必要があります。

手順

- 1. リストから顔写真ライブラリを選択します。
- 2. 顔画像ライブラリの追加またはインポートをクリックします。
- 3. ピクチャをインポートします。

追加:取り込む画像を選択し、「読み込む」をクリックします。 顔画像ライブラリの読み込み:読み込む画像を複数選択し、「読み込む」をクリックします。

次に何をするか

● 画像を選択し、Copy(コピー)をクリックして、現在のライブラリのアップロードされた画像を他のライブラリにコピーします。

- 画像を選択し、「編集」をクリックして画像情報を変更します。
- リストから画像を選択し、「削除」をクリックして画像を削除します。
- ライブラリを選択し、「顔画像ライブラリの書き出し」をクリックして、ライブラリをバックアップデバイスに書き出します。
- またはをクリックすると、図または一覧で表示できます。 □ □

5.4.3 顔画像比較の設定

検出された顔画像を特定の顔画像ライブラリと比較する。比較が成功したときにアラームをトリガ します。

手順

1. →ユーティリティイベントスマートイベント→顔画像の比較に移動します。

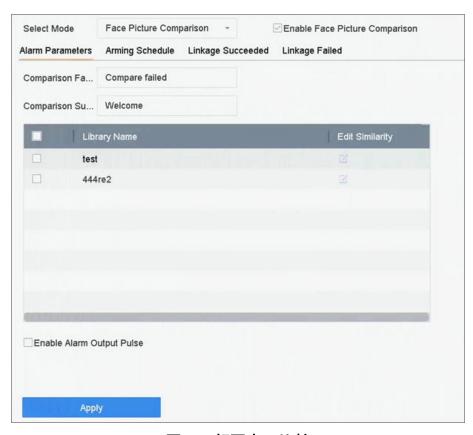


図5-3 顔写真の比較

- 2. カメラを選択します。
- 3. 顔画像の比較としてモードを選択します。
- 4.「顔画像の比較を有効にする」をチェックします。
- 5. オプション: 比較失敗プロンプトの設定、比較成功プロンプトの設定、およびアラーム出力パルスの有効化。

比較失敗プロンプト

顔画像の比較に失敗した場合、ライブビューのターゲット検出(顔検出がチェックされている) または顔認識でプロンプトが表示されます。ライブビューでをクリックすると、顔認識インターフェースに入ることができます。 **○**

比較成功例

顔画像の比較に成功すると、顔認識のプロンプトが表示されます。ライブビューでをクリックすると、顔認証のインターフェースに入ることができます。 ☑

アラーム出力パルスを有効にする

それは、通常、ゲートと連結されている。人がゲートを通過すると、比較が成功した場合は、 パルスをトリガしてゲートを開く。パルスは100~900msである。システム→イベント→通常イ ベント→アラーム出力で、アラーム出力パルス(ms) を設定できます。

- 6. 顔画像ライブラリを選択し、類似度を設定します。
- 7. アーミングスケジュールを設定します。「Configure Arming Schedule」を参照してください。
- 8. 顔画像の比較に成功した場合と失敗した場合の連携動作を設定します。「リンクアクションの 設定」を参照してください。
- 9. [適用] をクリックして、設定を保存します。

5.4.4 顔画像検索

顔画像比較イベントで検索する

顔画像の比較結果を顔画像ごとに検索する。

手順

- 1. Smart Analysis → Smart Search → Face Search → Search by Event に移動します。
- 2. 開始時刻と終了時刻を設定します。
- 3. チャンネルを選択します。
- 4. 顔画像の比較としてイベントタイプを選択します。
- 5. 検索の開始をクリックします。検索結果一覧に1チャンネル表示されます。
- 6. 「チャンネル(Channel)」をクリックして、任意のチャンネルを選択します。選択したチャンネルの検索結果が表示されます。

次にどうするか

検索結果の表示を参照してください。

アップロードした画像で検索

アップロードした写真から顔写真を検索できます。

手順

1. スマート解析→スマート検索→顔検索→画像検索に移動します。

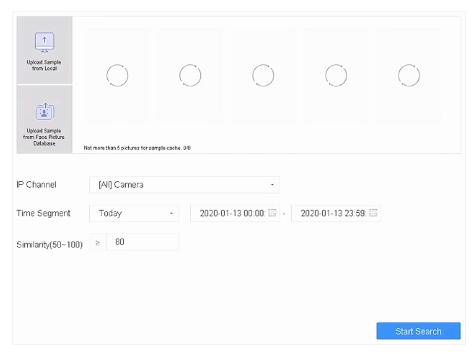


図5-4 アップロード画像による検索

- 2. チャンネルを選択します。
- 3. 検索する顔写真を選択します。
 - ローカルからサンプルをアップロードをクリックし、ローカルディレクトリから顔画像を選択します。
 - 「顔画像データベースからサンプルをアップロード」をクリックし、作成した顔画像ライブラリから顔画像を選択します。
- 4. 開始時刻と終了時刻を設定します。
- 5. 類似度値(範囲:0~100)を設定します。装置は、ライブラリ内のサンプルと顔画像との間の類似性を分析し、その類似性が集合よりも高い画像を示す。
- 6. 検索の開始をクリックします。検索結果一覧に1チャンネル表示されます。
- 7. 「チャンネル(Channel)」をクリックして、任意のチャンネルを選択します。選択したチャンネルの検索結果が表示されます。

次にどうするか

検索結果の表示を参照してください。

個人名による検索

個人名で顔写真を検索します。

手順

1. スマート解析→スマート検索→顔検索→名前による検索に移動します。

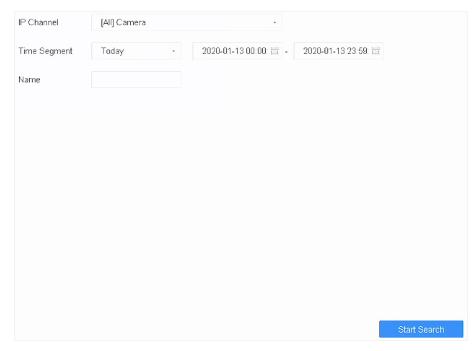


図5-5 個人名による検索

- 2. 検索する顔画像の開始時刻と終了時刻を設定します。
- 3. チャンネルを選択します。
- 4. 名前を入力します。
- 5. 検索の開始をクリックします。検索結果一覧に1チャンネル表示されます。
- 6. 「チャンネル(Channel)」をクリックして、任意のチャンネルを選択します。選択したチャンネルの 検索結果が表示されます。

次にどうするか

検索結果の表示を参照してください。

外観による検索

顔写真を見た目で検索します。

手順

- 1. Smart Analysis → Smart Search → Face Search → Search by Appearance に移動します。
- 2. 検索条件を設定します。
- 3. 検索の開始をクリックします。検索結果一覧に1チャンネル表示されます。
- 4. 「チャンネル(Channel)」をクリックして、任意のチャンネルを選択します。選択したチャンネルの検索結果が表示されます。

次にどうするか

検索結果の表示を参照してください。

検索結果の表示

- ファイルをダブルクリックすると、関連するビデオが表示されます。
- 顔データベースに追加をクリックして、選択したファイルを顔画像ライブラリに追加します。
- Add to Sample(サンプルに追加)をクリックして、選択したファイルをサンプル画像として追加します。サンプルピクチャを使用して、他のピクチャを検索できます。アップロードした画像で検索を参照してください。
- エクスポートをクリックして、選択したファイルをバックアップデバイスにエクスポートします。 Select All(すべて選択)をクリックして、すべてのファイルを選択できます。

[ji 注

- クリックすると、エクスポートの進行状況を表示できます。
- クリックすると、検索インターフェースに戻ることができます。

5.5 周辺保護

iDSシリーズの特定のモデルについては。Smart Analysis → Smart Analysis → Engine Configurationに進みます。Perimeter Protection として、少なくとも1 つのエンジン使用量を設定します。詳細は、「エンジン構成」を参照してください。

5.5.1 侵入検知

侵入検出機能は、予め定義された仮想領域に入り、そこを飛び越える人、車両、または他の物体 を検出する。アラームがトリガされると、特定のアクションをとることができる。

- 1. →ユーティリティのイベント→スマートイベントに移動します。
- 2. 「Intrusion」をクリックします。

デジタルビデオレコーダー取扱説明書

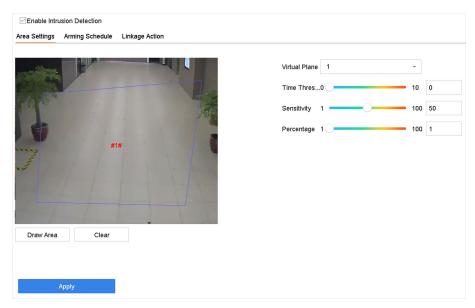


図5-6 侵入検出

- 3. Intrusion Detection を有効にするをチェックします。
- 4. オプション: VCA ピクチャの保存をチェックして、取り込んだ侵入検出ピクチャを保存します。
- 5. 検出ルールと検出エリアを設定します。
 - 1) 仮想パネルを選択します。4つまでの仮想パネルを選択できます。
 - 2)「時間しきい値」と「感度」を設定します。

時間しきい値

領域内の物体ロータの時間。定義された検出領域内の物体の持続時間が閾値を超えると、デバイスはアラームをトリガする。

感度

アラームを起動できるオブジェクトのサイズ。値が大きいほど、検出アラームがトリガされ やすくなります。

- 3) Draw Area をクリックします。
- 4) プレビューウィンドウに四角形を描画します。
- 6. アーミングスケジュールを設定します。「Configure Arming Schedule」を参照してください。
- 7. リンクアクションを設定します。「リンクアクションの設定」を参照してください。
- 8. 適用をクリックします。

li注

iDS-7200シリーズでは、「ターゲット検出」を「人間」または「車両」に設定できます。選択したタイプのターゲットのみがアラームをトリガします。

5.5.2 ライン交差検出

交差線検出は、設定された仮想線を横切る人、車両、および物体を検出する。検出方向は、左

から右へ、または右から左への双方向として設定することができる。

手順

- 1. →ユーティリティのイベント→スマートイベントに移動します。
- 2. 線の交差をクリックします。

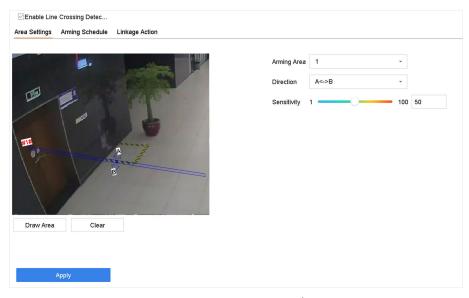


図5-7 ラインクロッシング検出

- 3. カメラを選択します。
- 4.「回線交差検出を有効にする」をチェックします。
- 5. オプション: Save VCA Picture(VCA ピクチャの保存)をチェックして、取り込んだラインクロス検出のピクチャを保存します。
- 6. 検出ルールと検出エリアを横切る線を設定します。
 - 1) アーミングエリアを選択します。
 - 2) 方向をA<->B、A->B、またはA<-B として選択します。

A<->B

B側の矢印のみが示されている。物体が構成された線を両方向に横切ると、検出することができ、アラームがトリガされる。

A→B

A側からB側に構成線を横切る物体のみを検出することができる。

B->A

B側からA側に構成線を横切る物体のみを検出することができる。

- 3) 検出感度を設定します。値が高いほど、検出アラームをトリガーしやすくなります。
- 4) Draw Region をクリックします。
- 5) プレビューウィンドウに仮想線を描画します。
- 7. アーミングスケジュールを設定します。「Configure Arming Schedule」を参照してください。
- 8. リンクアクションを設定します。「リンクアクションの設定」を参照してください。

9. 適用をクリックします。

[i]注

iDS-7200シリーズでは、「ターゲット検出」を「人間」または「車両」に設定できます。選択したタイプのターゲットのみがアラームをトリガします。

5.5.3 領域入口検出

領域入口検出は、所定の仮想領域に入る物体を検出する。

- 1. システムマネジメント→イベント設定→スマートイベントに移動します。
- 2. Region Entrance Detectionをクリックします。

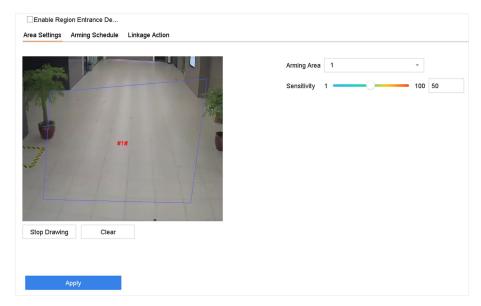


図5-8 領域入口検出

- 3. カメラを選択します。
- 4. Enable Region Entrance Detectionをチェックします。
- 5. オプション: Save VCA Picture(VCA ピクチャの保存)をチェックして、取り込んだリージョンエントランス検出ピクチャのピクチャを保存します。
- 6. 検出ルールと検出エリアを設定します。
 - 1) Arming Region を選択します。4つまでの領域が選択可能である。
 - 2) 感度を設定します。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。範囲は[0-100]です。
 - 3) Draw Region をクリックし、プレビューウィンドウで四角形を描画します。
- 7. アーミングスケジュールを設定します。「Configure Arming Schedule」を参照してください。
- 8. リンクアクションを設定します。「リンクアクションの設定」を参照してください。
- 9. 適用をクリックします。

5.5.4 領域終了検出

領域出口検出は、事前定義された仮想領域から出るオブジェクトを検出します。

手順

- 1. →ユーティリティのイベント→スマートイベントに移動します。
- 2. Region Exiting をクリックします。

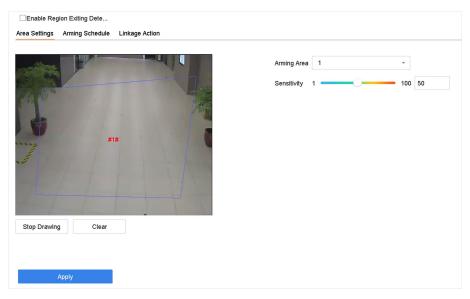


図5-9 リージョン終了検出

- 3. カメラを選択します。
- 4. Enable Region Exiting Detectionをチェックします。
- 5. オプション: Save VCA Picture(VCA ピクチャの保存)をチェックして、検出ピクチャを出るキャプチャされた領域を保存します。
- 6. 以下の手順に従って、検出ルールと検出エリアを設定します。
 - 1) Arming Region を選択します。4つまでの領域が選択可能である。
 - 2) 感度を設定します。値が大きいほど、検出アラームがトリガされやすくなります。範囲は[0-100]です。
 - 3) Draw Region をクリックし、プレビューウィンドウで四角形を描画します。
- 7. アーミングスケジュールを設定します。「Configure Arming Schedule」を参照してください。
- 8. リンクアクションを設定します。「リンクアクションの設定」を参照してください。
- 9. 適用をクリックします。

5.6 人体検出

Smart Analysis → Smart Analysis → Engine Configurationに進みます。少なくとも1 つのエンジン使用量を「画像認識 - 人体」として設定します。詳細は、「エンジン構成」を参照してください。
Smart Analysis → Smart Analysis → Task Configuration に移動して、カメラのタスクを有効にします。詳細はタスク構成を参照してください。

[ji 注

この章は、iDSシリーズの特定のモデルでのみ使用できます。

5.6.1 人体検出

人体検出により、監視シーンに現れる人体を検出し、人体画像を撮像することができる。

開始前に

接続したカメラが人体検知に対応しています。

- 1. →ユーティリティのイベント→スマートイベントに移動します。
- 2. Human Body をクリックします。
- 3. オプション: IP カメラが人体検出に対応していない場合は、[Enable Local Human Body Detection] をチェックします。次いで、装置は、人体検出を実行するためにその復号化資源を消費する。機能を有効にする前に、スマート分析→スマート分析→エンジン構成に進んで、少なくとも1つのエンジンをビデオストラクチュラライゼーションリアルタイムとして選択します。
- 4. 機能を有効にすると、カメラでサポートされているスマートイベントが変更されます。
- 5. カメラを選択して、人体検出を設定します。
- 6. VCA Pictureの保存を確認し、撮影した人体検出画像を保存します。
- 7. 対象(人体)をチェックし、人体検出によってトリガされない人体以外の写真およびビデオを破棄 する。この特徴は、局所的な人体検出にのみ利用可能である。
- 8. 検出領域を設定します。

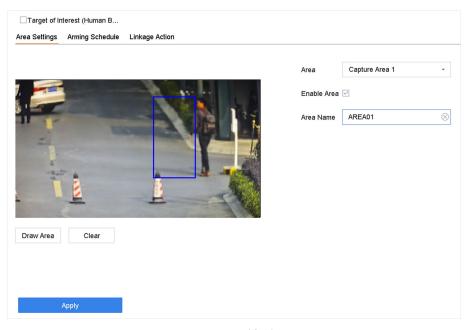


図5-10 人体検出

- 1) 「エリア」ドロップダウンリストから設定する検知エリアを選択します。検出エリアは8つまで選択できます。
- 2) [Enable Area]をチェックして、選択した検出エリアを有効にします。
- 3) シーン名でエリア名を編集します。シーン名は最大32 文字です。
- 4) Draw Area をクリックしてプレビューウィンドウに四角形を描画し、Stop Drawing をクリックします。
- 9. アーミングスケジュールを設定します。「Configure Arming Schedule」を参照してください。
- 10. リンクアクションを設定します。「リンクアクションの設定」を参照してください。
- 11. 設定値を有効にするには、[Apply](適用) をクリックします。

5.6.2 人体探索

外観による検索

手動で指定した検索条件で人体の画像を検索します。

手順

- 1. スマート解析→スマートサーチ→ 外観別人体検知→サーチに進む。
- 2. 検索条件を指定します。
- 3. 検索の開始をクリックします。検索結果一覧に1チャンネル表示されます。
- 4. 「チャンネル(Channel)」をクリックして、任意のチャンネルを選択します。選択したチャンネルの検索結果が表示されます。
- 5. オプション: 検索結果をエクスポートします。
 - 1) 検索結果インターフェースから結果ファイルを選択するか、「すべて選択」をオンにしてすべてのファイルを選択します。
 - 2) エクスポートをクリックして、選択したファイルをバックアップデバイスにエクスポートします。

〕注

クリックすると、エクスポートの進行状況を表示できます。クリックすると、検索インターフェースに 戻ることができます。
■ ▼ ▼ ▼ ▼ ▼ ▼

アップロードした画像で検索

検索精度を上げるには、1人の人物の複数の写真をアップロードし、撮影した人体の写真と比較 してください。

開始前に

USBフラッシュドライブに人体の写真を取り込み、デバイスに接続します。

手順

li注

- 同じピクチャ内に複数のターゲットが存在する場合には、30枚までのターゲットピクチャを解析して表示することができる。
- 最大許容画像サイズは3840*2160である。
- 画像はJPG またはJPEG 形式である必要があります。
- ピクチャ名(サフィックス付き)は64 文字以内にしてください。
- ▼アップロードした写真がクリアで認識可能であることを確認します。
- 1. 画像によるスマート解析→スマートサーチ→人体検知→サーチに進む。
- 2. チャンネルを選択します。
- 3. Upload Sample をクリックします。
- 4. 「Upload Sample from Local」をクリックし、ローカルディレクトリから顔写真を選択します。
- 5. 開始時刻と終了時刻を設定します。
- 6. USB フラッシュドライブの画像を選択し、「読み込み」をクリックします。
- 7. 関連画像を選択し、「アップロード」をクリックします。
- 8. 検索条件を指定します。

類似性

装置は、ライブラリ内のサンプルと顔画像との間の類似性を分析し、その類似性が集合より も高い画像を示す。

- 9. 検索の開始をクリックします。検索結果一覧に1チャンネル表示されます。
- 10. オプション: 検索結果をエクスポートします。
 - 1) 検索結果インターフェースから結果ファイルを選択するか、「すべて選択」をオンにしてすべてのファイルを選択します。
 - 2) エクスポートをクリックして、選択したファイルをバックアップデバイスにエクスポートします。

[ji 注

クリックすると、エクスポートの進行状況を表示できます。クリックすると、検索インターフェースに 戻ることができます。

Sample PictureとしてSearch Resultを追加する

検索した人体画像をサンプル画像として追加できます。そして、サンプル画像により人体画像を 検索する。

- 1. 人体の写真を検索します。
- 2. 検索結果インターフェースで、をクリックして画像を選択し、「Add to Sample」をクリックします。
- 3. 検索条件設定画面に戻り、選択したサンプルが一覧表示されます。

5.7 動体検知

動き検出は、デバイスが、監視領域内の移動物体を検出し、アラームをトリガすることを可能にする。

手順

- 1. ①→イベント→通常イベント→動体検知録画
- 2. カメラを選択します。
- 3. 有効をチェックします。
- 4. 検出エリアとルールを設定します。
 - 1) Draw Area(エリアの描画)をクリックして、プレビュー画面に検出エリアを描画します。
 - 2) マウスを右クリックし、「描画停止」をクリックして描画を終了します。
 - 3) 感度(0~100)を設定します。感度により、移動がアラームをトリガーする度合いを校正できます。より高い値は、動き検出をより容易にトリガする結果となる。
 - 4) オプション: 特定のアナログPIR カメラでは、誤警報フィルタをチェックして、警報を減らします。
 - 5) オプション: 特定のiDS M およびiDS K(B) シリーズデバイスでは、人間と車両を含むアナログカメラビデオを解析できます。アナログカメラで人や車両を確認してください。選択されたタイプのターゲットのみがアラームをトリガし、他のオブジェクトによって引き起こされる誤ったアラームを低減することができる。

[ji注

- 動作検出のターゲット検出はPIR アラームと競合するため、誤警報フィルタと人と車両のターゲット検出を同時に有効にすることはできません。
- 動き検出のターゲット検出は、強化されたIPモード、および顔検出、顔画像比較、周辺保護 (線交差検出および侵入検出)などのスマートイベントと競合することもある。
- 5. アーミングスケジュールを設定します。「Configure Arming Schedule」を参照してください。
- 6. リンクアクションを設定します。「リンクアクションの設定」を参照してください。
- 7. 適用をクリックします。

5.8 車両検知

道路交通監視には車両検知が利用可能である。車両検知では、通過した車両を検知し、そのナンバープレートの絵を捉えることができる。警報信号を送信して監視センターに通知することができます。

5.8.1 車両検出の設定

道路交通モニタリングのために車両検知が利用可能である。車両検知では、通過した車両を検

知し、そのナンバープレートの写真を撮影することができます。

手順

- 1. →ユーティリティのイベント→スマートイベントに移動します。
- 2. 設定するカメラを選択します。
- 3. 「車両」をクリックします。
- 4. 車両検出を有効にすることを確認します。
- 5. オプション: VCA Picture の保存をチェックして、取り込んだ車両検出画像を保存します。
- 6. アーミングスケジュールを設定します。Configure Arming Scheduleを参照してください。
- 7. リンクアクションを設定します。「リンクアクションの設定」を参照してください。
- 8. エリア設定、画像、オーバーレイコンテンツ、ブロックリスト、許可リストなどのルールを設定します。

エリア設定

4レーンまで選択できます。

ブロックリストと許可リスト

最初にファイルを書き出してその形式を確認し、編集してデバイスに読み込むことができます。

9. 適用をクリックします。

〔〕 注

車両検出の詳細については、『ネットワークカメラユーザーマニュアル』を参照してください。

5.8.2 車両探索

マッチした車両画像を検索して見ることができます。

手順

- 1. スマート解析→スマートサーチ→ビークルサーチに進む。
- 2. 車両探索用のIPカメラを選択します。
- 3. 検索条件を設定します。

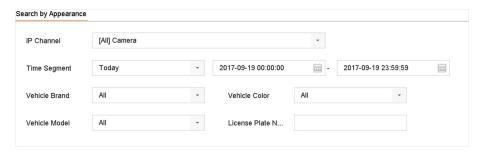


図5-11 車両検索

4. 検索の開始をクリックします。検索結果一覧に1チャンネル表示されます。

- 5. 「チャンネル(Channel)」をクリックして、任意のチャンネルを選択します。選択したチャンネルの検索結果が表示されます。
- 6. 検索結果をエクスポートします。
 - 1) 検索結果インターフェースから結果ファイルを選択するか、「すべて選択」をオンにしてすべてのファイルを選択します。
 - 2) エクスポートをクリックして、選択したファイルをバックアップデバイスにエクスポートします。

[i]注

クリックすると、エクスポートの進行状況を表示できます。

5.9 ターゲット検出

ライブビューモードでは、目標検出機能は、最後の5秒間およびその後の10秒間に、スマート検出、顔検出、車両検出、および人体検出を達成することができる。

手順

- 1. [Live View]モードで、[Target Detection]をクリックして、[Target Detection]インターフェースに入ります。
- 2. スマート検出()、車両検出()、顔検出()、人体検出()の異なる検出タイプを選択します。 🖬 🖨 🖫
- 3. ヒストリカル分析()またはリアルタイム分析()を選択して、結果を取得します。 ③ 🔍

[ji注

検出のスマートな分析結果は、リストに表示される。関連するビデオを再生するには、結果リストをクリックします。

5.10 人数

カウンティングは、特定の構成されたエリアに出入りする人の数を計算し、分析のために日次/週次/月次/年次レポートを作成します。

- 1. スマートアナリシス→カウントに進みます。
- 2. カメラを選択します。
- 3. レポートタイプを選択します。
- 4. 分析する日付を設定します。人数計算グラフィックが表示されます。

デジタルビデオレコーダー取扱説明書

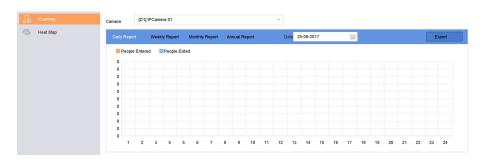


図5-12 People Counting Interface

5. 必要に応じて、「エクスポート」を選択して、レポートをMicrosoft Excel 形式でエクスポートします。

5.11 ヒートマップ

ヒートマップは、データのグラフ表示である。ヒートマップ関数は、特定の地域に何人の人が訪れ、滞在したかを分析するために使用される。

開始前に

接続されているIPカメラでヒートマップ機能をサポートし、対応する設定を行う必要があります。

手順

- 1. スマート解析→ヒートマップに移動します。
- 2. カメラを選択します。
- 3. レポートタイプを選択します。
- 4. 分析する日付を設定します。



図 5-13 ヒートマップインタフェース

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

[i]注

上の図に示すように、赤色ブロック(255、0、0)は最も人気のない領域を示し、青色ブロック(0、0、255)は人気の低い領域を示す。

デジタルビデオレコーダー取扱説明書

必要に応じて します。	·、「エクスポー	ト」を選択して、	統計レポートを	Microsoft Excel	形式でエクスポート

第 6 章イベント

6.1 通常イベントアラーム

6.1.1 ビデオロスアラームの設定

ビデオ損失検出は、チャネルのビデオ損失を検出し、アラーム応答アクションを取る。

手順

- 1. →ユーティリティイベント→通常イベント ビデオロスに移動します。
- 2. カメラを選択します。
- 3. 有効をチェックします。
- 4. アーミングスケジュールを設定します。「Configure Arming Schedule」を参照してください。
- 5. リンクアクションを設定します。「リンクアクションの設定」を参照してください。

6.1.2 ビデオ・タンパリング・アラームの設定

ビデオ改ざん検出は、カメラレンズがカバーされるとアラームをトリガーし、アラーム応答アクションを実行しました。

手順

- 1. →事象→通常事象→ビデオタンパリングに進む。
- 2. カメラを選択します。
- 3. 有効をチェックします。
- 4. ビデオ改ざん領域を設定します。プレビュー画面上でドラッグして、カスタマイズしたビデオ改 ざん領域を描きます。
- 5. 感度(0-2)を設定します。3つのレベルが利用可能である。感度は、動きがどの程度容易にアラームをトリガするかを較正する。より高い値は、ビデオ改竄検出をより容易にトリガする。
- 6. アーミングスケジュールを設定します。「Configure Arming Schedule」を参照してください。
- 7. リンクアクションを設定します。「リンクアクションの設定」を参照してください。

6.1.3 センサアラームの設定

外部センサアラームの処理動作を設定します。

- 1. →事象→正常事象→アラーム入力に進む。
- 一覧からアラーム入力項目を選択し、クリックします。

- 3. アラーム入力の種類を選択します。
- 4. アラーム名を編集します。
- 5. 入力を確認します。
- 6. アーミングスケジュールを設定します。「Configure Arming Schedule」を参照してください。
- 7. リンクアクションを設定します。「リンクアクションの設定」を参照してください。

6.1.4 例外アラームの設定

例外イベントは、Live Viewウィンドウ内のイベントヒントを取得し、アラーム出力およびリンケージアクションをトリガするように構成することができる。

手順

- 1. →ユーティリティイベント→正常イベント 除外に移動します。
- 2. オプション:イベントヒントを有効にして、ライブビューウィンドウに表示します。
 - 1) イベントヒントの有効化をオンにします。
 - 2) クリックして、イベントヒントを取得する例外タイプを選択します。

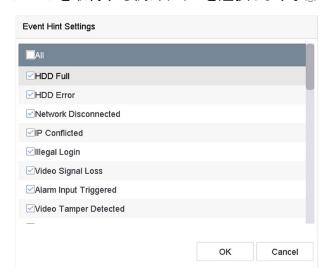


図6-1 イベントヒントの設定

3. 例外タイプを選択します。



図6-2 例外処理

4. リンクアクションを設定します。「リンクアクションの設定」を参照してください。

6.2 VCA イベントアラーム

デバイスは、接続されたIPカメラによって送信されたVCA検出の受信をサポートする。IPカメラ設定インタフェースで最初にVCA検出を有効にし、設定します。

[ji注

- VCA検出は、接続されたIPカメラによってサポートされなければならない。
- 詳細なVCA検出方法については、ネットワークカメラのユーザーマニュアルを参照してください。

6.2.1 無人手荷物検知

無人手荷物検出は、手荷物、財布、危険物などの所定の領域に残された物体を検出し、アラームがトリガされたときに一連の動作を行うことができる。

- 1. →ユーティリティのイベント→スマートイベントに移動します。
- 2. 無人荷物をクリックします。

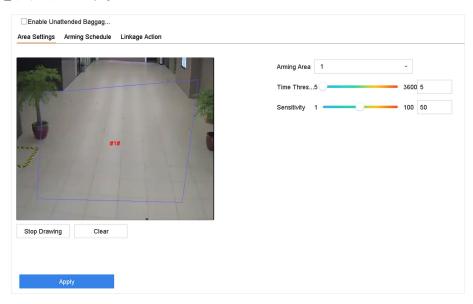


図6-3 無人手荷物検出

- 3. カメラを選択します。
- 4. 無人荷物検出を有効にすることを確認します。
- 5. オプション: VCA Pictureの保存をチェックして、キャプチャされた無人の手荷物検出画像を保存します。
- 6. 検出ルールと検出エリアを設定します。
 - 1) Arming Region を選択します。4つまでの領域が選択可能である。
 - 2) スライダをドラッグして、「Time Threshold」と「Sensitivity」を設定します。

時間しきい値

オブジェクトの時間はリージョンに残されます。値が10である場合、対象物が残され、領域内に10秒間留まった後に、アラームがトリガされる。その範囲は[5s-20s]である。

感度

2.対象物に対する背景画像の類似性。値を高くするほど、検出アラームがトリガーされやすくなります。

- 3) Draw Region をクリックし、プレビューウィンドウで四角形を描画します。
- 7. アーミングスケジュールを設定します。「Configure Arming Schedule」を参照してください。
- 8. リンクアクションを設定します。「リンクアクションの設定」を参照してください。
- 9. 適用をクリックします。

6.2.2 物体除去検出

物体除去検出機能は、ディスプレイ上の展示物のような所定の領域から除去された物体を検出し、アラームがトリガされたときに一連の動作を行うことができる。

- 1. →ユーティリティのイベント→スマートイベントに移動します。
- 2. Object Removable をクリックします。

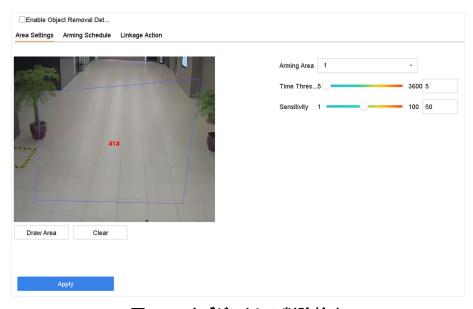


図 6-4 オブジェクトの削除検出

- 3. 設定するカメラを選択します。
- 4. Enable Object Removable Detectionをチェックします。
- 5. オプション: Save VCA Picture(VCA ピクチャの保存)をチェックして、取り込んだオブジェクトの リムーバブル検出ピクチャを保存します。
- 6. 以下の手順に従って、検出ルールと検出エリアを設定します。
 - 1) Arming Region を選択します。4つまでの領域が選択可能である。

2) スライダをドラッグして、「Time Threshold」と「Sensitivity」を設定します。

時間しきい値

領域から削除されたオブジェクトの時刻。値が10の場合、対象が領域から10秒間消えた後にアラームがトリガされます。その範囲は[5s-20s]です。

感度

背景画像の類似度。感度が高い場合には、領域から取り出された非常に小さな物体が警報をトリガする。

- 3) Draw Area をクリックし、検出領域の4 つの頂点を指定して、プレビューウィンドウに四角形を描画します。
- 7. アーミングスケジュールを設定します。「Configure Arming Schedule」を参照してください。
- 8. リンクアクションを設定します。「リンクアクションの設定」を参照してください。
- 9. 適用をクリックします。

6.2.3 オーディオ例外検出

音声例外検出は、音の強さの突然の増加/減少のような、監視シーンにおける異常な音を検出する。

- 1. →ユーティリティのイベント→スマートイベントに移動します。
- 2. オーディオ除外をクリックします。

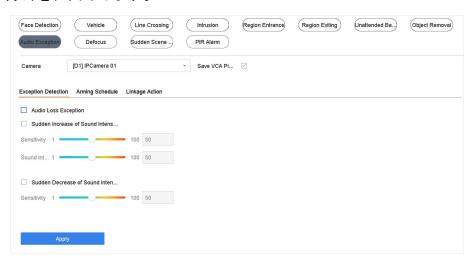


図 6-5 オーディオ例外検出

- 3. 設定するカメラを選択します。
- 4. オプション: VCA Picture の保存をチェックして、キャプチャしたオーディオ例外検出ピクチャを保存します。
- 5. 検出ルールの設定:
 - 1) 例外検出を選択します。

2) 音声喪失例外、音量検出の突然の増加、および/または音量検出の突然の減少をチェックする。

オーディオ損失例外

監視シーンで急峻な音の立ち上がりを検出します。急峻な音の立ち上がりの検出感度としきい値は、感度しきい値と音の強さしきい値を設定することで設定できます。

感度

値が小さければ小さいほど、検出をトリガするために変化がより厳しくなければならない。 範囲「1-100」.

音響強度しきい値

それは、環境中の音をフィルタリングすることができる。環境音が大きければ大きいほど、 その値は高くなければならない。環境に合わせて調整してください。範囲[1-100].

音量検出の急激な低下

監視シーンで急峻な音の低下を検出します。検出感度を[1-100]に設定する必要があります。

- 6. アーミングスケジュールを設定します。「Configure Arming Schedule」を参照してください。
- 7. リンクアクションを設定します。「リンクアクションの設定」を参照してください。
- 8. 適用をクリックします。

6.2.4 デフォーカス検出

レンズの焦点ぼけによる画像のボケを検出できます。

- 1. →ユーティリティのイベント→スマートイベントに移動します。
- 2. Defocusをクリックします。

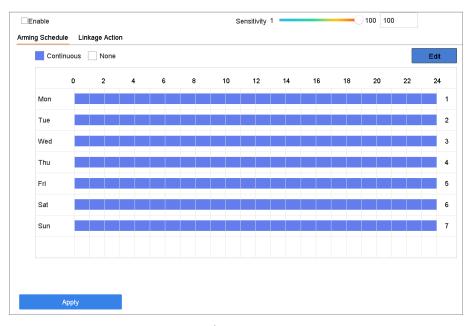


図6-6 デフォーカス検出

- 3. 設定するカメラを選択します。
- 4. 有効をチェックします。
- 5. オプション: Save VCA Pictureをチェックして、取り込んだデフォーカス検出画像を保存します。
- 6. 感度スライダをドラッグして検出感度を設定します。

[ji 注

感度範囲:[1-100]。値が高いほど、デフォーカス画像が検出されやすくなる。

- 7. アーミングスケジュールを設定します。「Configure Arming Schedule」を参照してください。
- 8. リンクアクションを設定します。「リンクアクションの設定」を参照してください。
- 9. 適用をクリックします。

6.2.5 突然のシーン変化検出

シーン変化検出は、カメラの意図的な回転などの外部要因によって影響を受ける監視環境の変化を検出する。

- 1. →ユーティリティのイベント→スマートイベントに移動します。
- 2. 「Sudden Scene Change」をクリックします。

デジタルビデオレコーダー取扱説明書

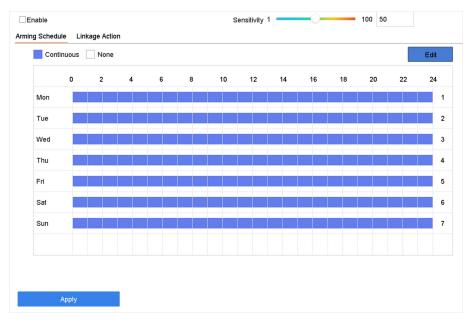


図6-7 急激なシーンの変化

- 3. 設定するカメラを選択します。
- 4. 有効をチェックします。
- 5. オプション: Save VCA Picture(VCA ピクチャの保存)をチェックして、取り込んだ突然のシーンチェンジ検出ピクチャを保存します。
- 6. 感度スライダをドラッグして検出感度を設定します。

[i注

感度範囲:[1-100]。値が高いほど、場面の変化がより容易にアラームをトリガすることができる。

- 7. アーミングスケジュールを設定します。「Configure Arming Schedule」を参照してください。
- 8. リンクアクションを設定します。「リンクアクションの設定」を参照してください。
- 9. 適用をクリックします。

6.2.6 PIRアラーム

侵入者が検出器視野内を移動すると、PIR (受動赤外線)アラームがトリガーされます。ヒトまたはイヌ、ネコなどの任意の他の温血生物によって放散される熱エネルギーを検出することができる。

- 1. →ユーティリティのイベント→スマートイベントに移動します。
- 2. PIRアラームをクリックします。



図6-8 PIR アラーム

- 3. 設定するカメラを選択します。
- 4. PIR アラームを確認します。
- 5. オプション: 撮影したPIRアラーム画像を保存するには、VCA画像の保存を確認します。
- 6. アーミングスケジュールを設定します。「Configure Arming Schedule」を参照してください。
- 7. リンクアクションを設定します。「リンクアクションの設定」を参照してください。
- 8. 適用をクリックします。

6.3 Arming Schedule の設定

手順

- 1. Arming Schedule をクリックします。
- 2. 編集をクリックします。
- 3. 曜日を選択し、期間を設定します。1日8回まで設定できます。

Di注

期間を繰り返したり、重複したりすることはできません。

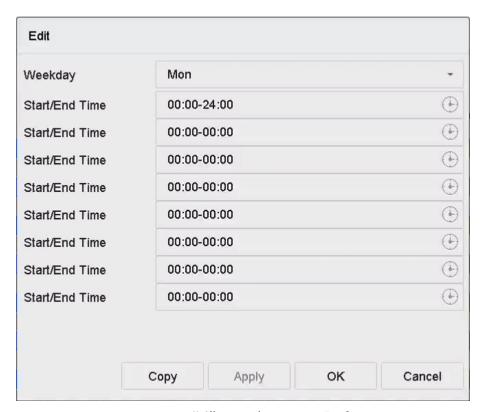


図 6-9 準備スケジュールの設定

- 4. 「コピー」をクリックすると、当日のアーミングスケジュール設定を他の日にコピーできます。
- 5. [適用] をクリックして、設定を保存します。

6.4 リンケージアクションの設定

アラームリンクアクションは、イベントヒント表示、フルスクリーンモニタリング、可聴警告(ブザー)、 監視センター通知、トリガアラーム出力、および電子メール送信を含む、アラームまたは例外が 発生したときに起動される。

6.4.1 自動スイッチ全画面監視の設定

アラームがトリガされると、ローカルモニタは、フルスクリーン監視のために構成されたアラームチャネルからのビデオ画像をフルスクリーンで表示する。また、複数のチャネルで同時にアラームがトリガされる場合は、自動スイッチのドウェル時間を設定する必要があります。

[i]注

アラームが停止すると、オートスイッチは終了し、ライブビューインタフェースに戻ります。

手順

1. 「→ライブビュー→全般」に移動します。

2. イベント出力とドウェル時間を設定します。

イベント出力

出力を選択してイベントビデオを表示します。

フルスクリーン監視休止時間

アラームイベント画面を表示する時間を秒単位で設定します。いくつかのチャネルで同時にアラームがトリガされる場合、それらのフルスクリーン画像は、10秒の間隔(デフォルト滞留時間)で切り替えられる。

- 3. アラーム検出(例えば、動き検出、ビデオ改ざん、顔検出など)の連係動作インターフェースに 進む。
- 4. 「全画面監視アラームリンク」アクションを選択します。
- 5. Trigger Channel でチャンネルを選択し、フルスクリーンでモニタリングします。

6.4.2 オーディオ警告の設定

音声警告は、アラームが検出されたときに可聴ビープ音をトリガするシステムを有する。

手順

- 1. →ユーティリティビュー→全般に移動します。
- 2. 音声出力を有効にし、音量を設定します。
- 3. アラーム検出(例えば、動き検出、ビデオ改竄、顔検出等)の連係動作インタフェースに進む。
- 4. 「Audio Warning alarm linkage action」を選択します。

6.4.3 通知サーベイランスセンター

デバイスは、イベントが発生したときに、例外信号またはアラーム信号をリモートアラームホストに送信することができる。アラームホストとは、クライアントソフトウェア(iVMS-4200、iVMS-5200など)がインストールされているPCをいう。

手順

- 1. →ユーティリティネットワーク 詳細→詳細設定に移動します。
- 2. アラームホストIPとアラームホストポートを設定します。
- 3. アラーム検出(例えば、動き検出、ビデオ改竄、顔検出等)の連係動作インタフェースに進む。
- 4. [Notify Surveillance Center] を選択します。

6.4.4 メール連動の設定

システムは、アラームが検出されると、アラーム情報を有する電子メールをユーザに送信することができる。

手順

1. →ネットワーク→先進→メールへ。

- 2. 電子メールパラメータを設定します。
- 3. 適用をクリックします。
- 4. アラーム検出(例えば、動き検出、ビデオ改ざん、顔検出など)の連係動作インターフェースに 進む。
- 5. Send Email alarm linkage action を選択します。

6.4.5 トリガアラーム出力

アラーム出力は、アラーム入力、モーション検出、ビデオ改ざん検出、顔検出、ライン交差検出、 その他すべてのイベントによってトリガできます。

手順

- 1. アラーム検出(動き検出、顔検出、線交差検出、侵入検出等)の連携動作インタフェースに進む。
- 2. Trigger Alarm Outputs Area で、トリガするアラーム出力(s) を選択します。
- 3. →事象→正常事象→アラームアウトプットに進む。
- 4. 一覧からアラーム出力項目を選択します。

6.4.6 PTZ 連携の設定

システムは、アラームイベントまたはVCA検出イベントが発生したときに、PTZアクション(例えば、コールプリセット/パトロール/パターン)をトリガすることができる。

開始前に

接続されているPTZまたはスピードドームがPTZリンクを支持していることを確認します。

手順

- 1. アラーム入力またはVCA検出(例えば、顔検出、線交差検出、侵入検出など)の連係動作インタフェースに進む。
- 2. PTZリンクを選択します。
- 3. PTZアクションを実行するカメラを選択します。
- 4. アラーム発生時に呼び出すプリセット/パトロール/パターン番号を選択します。

[ji 注

リンクアクションのPTZ タイプは、その都度1 つだけ設定できます。

6.4.7 Audio and Light Alarm Linkage の設定

特定のカメラでは、アラーム連動アクションをオーディオアラームまたはライトアラームとして設定

できます。

開始前に

- お使いのカメラがオーディオと可視光のアラーム連動に対応していることを確認してください。
- オーディオ出力と音量が正しく設定されていることを確認します。

- 1. アラーム検出(例えば、動作検出)のリンク動作インタフェースに進む。
- 2. Audio and Light Alarm Linkage を希望通りに設定します。
- 3. 適用をクリックします。

第 7 章ファイル管理

7.1 ファイルの検索

動画・写真を検索する際の詳細条件を設定します。

手順

- 1. File Management → All Files/Human Files/Vehicle Files に移動します。
- 2. 時間、カメラ、イベントタイプなどの詳細な条件を指定します。

[i]注

- 「すべてのファイル」で、「時間」、「カメラ」、「ファイルタイプ」、「イベントタイプ」を選択します。
- ヒューマンファイルの場合は、「時間」、「カメラ」、「ファイルの種類」を選択して検索します。
- 車両ファイルの場合は、時間、カメラ、ファイルタイプ、プレート番号、エリア/国を選択します。
- 3. 検索をクリックして結果を表示します。一致したファイルが表示されます。
- 4. メニューバーの「ターゲット画像」または「ソース画像」を選択すると、関連画像のみが表示されます。
 - Target Picture:車両クローズアップの検索結果を表示します。
 - Source Picture:カメラで撮影したオリジナル画像の検索結果を表示します。

7.2 ファイルのエクスポート

バックアップ目的でファイルをUSB デバイス、またはeSATA HDD にエクスポートします。

- 1. ファイルの検索。詳細については、「ファイルの検索」を参照してください。
- 2. ファイルを選ぶ。
- 3. エクスポートをクリックします。
- 4. オプション: 車両ファイルの場合は、バックアップライセンスプレート統計情報をチェックして、 後でライセンスプレート統計情報をエクスポートします。
- 5. Video and log としてエクスポートするファイルを選択し、OK をクリックします。
- 6. バックアップデバイスとフォルダパスを選択します。
- 7. [OK]をクリックします。

7.3 スマートサーチ

ファイルマネージメント→スマートサーチで人体ファイル、顔ファイル、車両を検索できます。詳細は「人体探索顔画像探索」、「車両探索」を参照してください。

第 8 章 POS 設定

デバイスは、POSマシン/サーバに接続され、Live Viewまたは再生中に画像上にオーバーレイするためのトランザクションメッセージを受信し、POSイベントアラームをトリガすることができる。

8.1 POS 接続の設定

手順

- 1.「システム→ POS」に進む。
- 2. 追加をクリックします。



図8-1 POS 設定

- 3. ドロップダウンリストからPOS デバイスを選択します。
- 4. 有効をチェックします。

[i]注

各デバイスによってサポートされるPOSデバイスの数は、そのチャネルの数の半分であり、例えば、DS-9616NI-I8モデルに対して8つのPOSデバイスがサポートされる。

5. POS Protocol を選択します。

〔〕 注

新しいプロトコルが選択されたら、デバイスを再起動して新しい設定を有効にします。

ユニバーサル・プロトコル

ユニバーサルプロトコルを選択するときに詳細設定を展開するには、詳細をクリックします。 POS オーバーレイ文字の開始行識別子、改行タグ、終了行タグ、および文字の大文字と小文字を区別する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 プロトコルを確認することもできます。

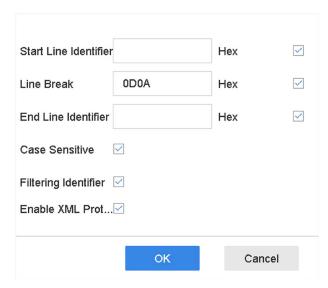


図8-2 ユニバーサルプロトコル設定

エプソン

固定開始および終了ラインタグは、EPSONプロトコルのために使用される。

AVE

固定開始および終了ラインタグは、AVEプロトコルのために使用される。シリアルポートと仮想シリアルポートの接続タイプがサポートされています。

「カスタム」をクリックして、AVE 設定を構成します。ルールをVSI-ADD またはVNET として選択します。送信するPOSメッセージのアドレスビットを設定します。設定を保存するには、OKをクリックします。

核

Custom(カスタム)をクリックして、NUCLEUS 設定を構成します。

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

[i]注

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。

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

TCP 接続

TCP 接続を使用する場合、ポートは1 ~65535 に設定する必要があり、各POS マシンのポートは一意である必要があります。

POS メッセージを送信する機器のAllowed Remote IP Address を設定します。

UDP接続

UDP 接続を使用する場合は、ポートを1 ~65535 に設定し、各POS マシンのポートを一意

にする必要があります。

POS メッセージを送信する機器のAllowed Remote IP Address を設定します。

USB-to-RS-232 接続

ポートのシリアル番号、ボーレート、データビット、ストップビット、パリティ、フローctrl など、USB-to-RS-232 コンバータのポートパラメータを設定します。

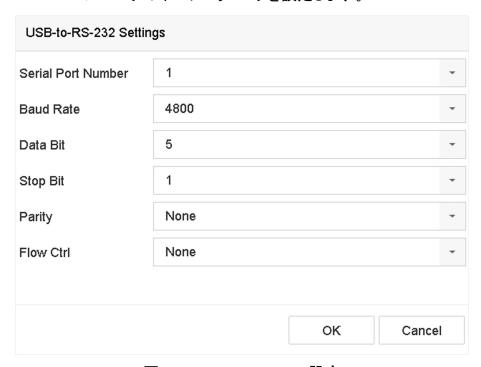


図8-3 USB-to-RS-232 設定

RS-232 接続

RS-232を介してデバイスとPOSマシンを接続します。RS-232 設定は、メニュー→設定 RS-232 で設定できます。UsageはTransparent Channelに設定する必要があります。

マルチキャスト接続

デバイスとPOS マシンをマルチキャストプロトコルで接続する場合は、マルチキャストアドレスとポートを設定します。

Sniff 接続

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

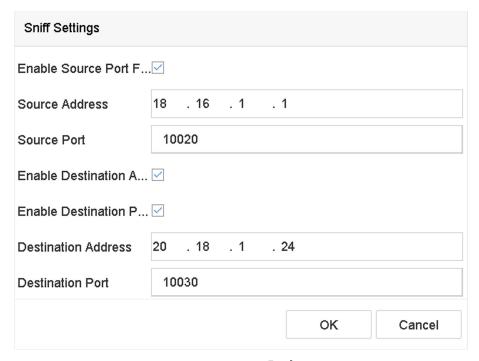


図8-4 Sniff 設定

8.2 POS テキストオーバーレイの設定

- 1.「システム→ POS」に進む。
- 2.「チャンネル連動と表示」をクリックします。

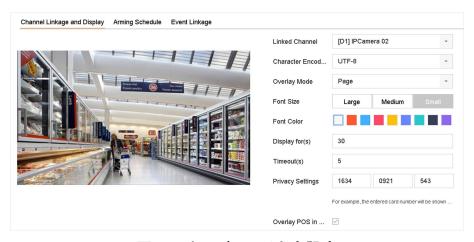


図8-5 オーバーレイ文字設定

- 3. POSキャラクターを重ね合わせるには、リンクされたチャンネルを選択します。
- 4. 有効なPOS の文字オーバーレイを設定します。
 - ◆ 文字エンコーディング形式: 現在Latin-1 形式が使用可能です。
 - スクロールやページモードで表示する文字のオーバーレイモード

- 文字サイズと文字色
- 文字の表示時間(秒)値は5~3600秒の範囲である。
- POS イベントのタイムアウト。値は5~3600秒の範囲である。デバイスが定義された時間内にPOSメッセージを受信しなかった場合、トランザクションは終了します。
- 5. プライバシー設定で、カード番号、ユーザー名など、画像に表示されないようにPOSプライバシー情報を設定します。
 - 定義されたプライバシー情報は、代わりにイメージ上の***を使用して表示されます。
- 6. 「Live View」で「Overlay POS」をチェックします。この機能を有効にすると、POS 情報がライブ ビュー画像にオーバーレイされます。

〕注

フレームをドラッグして、POS設定インターフェースのプレビュー画面でテキストボックスのサイズと位置を調整します。

7. 設定値を有効にするには、[Apply](適用) をクリックします。

8.3 POSアラームの設定

POSイベントは、チャンネルをトリガして録画を開始するか、またはフルスクリーンモニタリングまたは音声警告をトリガして、監視センタに通知し、電子メールを送信するなどすることができる。

- 1.「保存→記録予定」に移動します。
- 2. POSイベントのアーミングスケジュールを設定します。
- 3.「システム→ POS」に進む。
- 4. POS の追加または編集インターフェースで「イベント連携」をクリックします。

デジタルビデオレコーダー取扱説明書

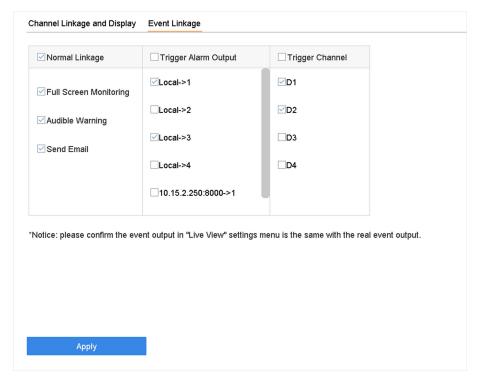


図8-6 POS のトリガカメラの設定

- 5. 通常のリンクアクションを選択します。
- 6. トリガする1つ以上のアラーム出力を選択します。
- 7. POSアラームがトリガーされたときに、録画またはフルスクリーンモニタリングになる1つ以上の チャンネルを選択します。
- 8. [適用] をクリックして、設定を保存します。

第 9 章ストレージ

9.1 ストレージデバイス管理

9.1.1 ローカルHDD の管理

HDD グループの構成

複数のHDDをグループで管理できます。HDD設定により、指定したチャンネルの映像を特定のHDDグループに記録することができます。

手順

- 1. ストレージ→ストレージモードに移動します。
- 2. グループとしてモードを選択します。
- 3. 適用をクリックします。
- 4. Storage → Storage Device に移動します。
- 5. HDDを選択します。



図9-1 ストレージデバイス

6. クリックして、ローカルHDD 設定インターフェースに入ります。

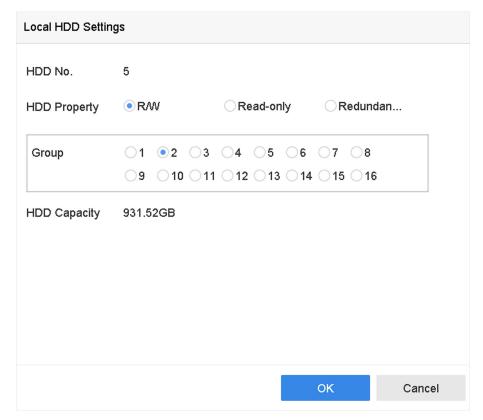


図9-2 ローカルHDD 設定

- 7. HDDのグループ番号を選択します。
- 8. [OK]をクリックします。

[i]注

HDDグループ番号が変更された場合は、HDD用カメラを再グループ化します。

- 9. ストレージ→ストレージモードに移動します。
- 10. リストからグループ番号を選択します。
- 11. 関連するカメラを選択すると、HDDグループに動画や画像が保存されます。
- 12. 適用をクリックします。

HDD プロパティの設定

HDDプロパティは、R/W、Read-only、Redundantに設定できます。

開始前に

ストレージモードをグループに設定します。詳細な手順については、「HDD グループの構成」を参照してください。

手順

1. Storage → Storage Device に移動します。

- 2. 目的のHDD をクリックします。 🗹
- 3. HDD Property を選択します。

R/W

HDD は読み取りと書き込みの両方をサポートします。

読み取り専用

読み取り専用HDDのファイルは上書きされません。

冗長

R/W HDDのみならず、冗長HDDにも動画を保存します。これは、データの安全性および信頼性を効果的に向上させる。リード/ライト状態の別のHDD が存在することを確認してください。

4. [OK]をクリックします。

HDD クォータの設定

各カメラは、ビデオまたはピクチャを記憶するための割り当てられた割当量で構成することができる。

手順

- 1. ストレージ→ストレージモードに移動します。
- 2. クォータとしてモードを選択します。
- 3. クォータを設定するカメラを選択します。
- 4. Max(最大)のテキストフィールドにストレージ容量を入力します。記録容量(GB)と最大。画像の容量(GB)。
- 5. 「コピー」をクリックして、現在のカメラのクォータ設定を他のカメラにコピーします。
- 6. 適用をクリックします。

[ji]注

- クォータ容量が0に設定されている場合、すべてのカメラは、ビデオおよびピクチャのために HDDの総容量を使用する。
- ビデオレコーダーを再起動して、新しい設定を有効にします。

9.1.2 ネットワークディスクの追加

割り当てられたNAS またはIP SAN ディスクをデバイスに追加し、ネットワークHDD として使用できます。

- 1. Storage → Storage Device に移動します。
- 2. 追加をクリックします。

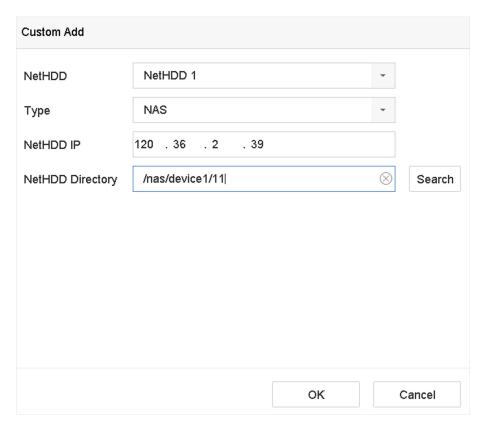


図9-3 NetHDD の追加

- 3. NetHDDタイプを選択します。
- 4. NetHDD IP アドレスを入力し、「検索」をクリックして使用可能なNetHDD を検索します。
- 5. 目的のNetHDD を選択します。
- 6. [OK]をクリックします。
- 7. 追加したNetHDDがHDD一覧に表示されます。新しく追加したNetHDD を選択し、「Init」をクリックします。

9.1.3 eSATA の管理

データストレージ用のeSATA の設定

ビデオレコーダに外部eSATAデバイスが接続されている場合、データストレージとしてeSATA使用量を設定し、eSATAを管理できます。

手順

- 1. 「保存→の詳細」に移動します。
- 2. eSATA Usage as Export または Record/Capture を選択します。

エクスポート

バックアップにはeSATA を使用します。

記録/取り込み

eSATA を録画/キャプチャに使用します。操作方法については、以下の手順を参照してください。



図9-4 eSATA モード

次にどうするか

eSATA の使用が Record/Capture(記録 / キャプチャ)として設定されている場合は、ストレージデバイスのインタフェースを入力して、そのプロパティを編集するか、初期化します。

自動バックアップ用のeSATA の設定

自動バックアッププランを作成した場合、ビデオレコーダは、バックアップ開始時間の24時間前にローカルビデオをeSATAにバックアップします。

開始前に

デバイスが外付けeSATAハードドライブに正しく接続されており、その使用タイプがエクスポートとして設定されていることを確認します。詳細については、「eSATA の管理」を参照してください。

手順

- 1. 記憶域→の自動バックアップに移動します。
- 2. Auto Backupをチェックします。
- 3. バックアップ開始時刻を「バックアップ開始時刻」に設定します。

[ji]注

その日にバックアップが失敗した場合、ビデオレコーダは、翌日のバックアップ開始時間の48時間前にビデオをバックアップする。

- 4. バックアップするチャネルを選択します。
- 5. 必要に応じて「バックアップストリームタイプ」を選択します。
- 6. 上書きタイプを選択します。
 - Disable: HDD がフルの場合、書き込みを停止します。
 - 有効:HDDが一杯になると、一番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。
- 7. 適用をクリックします。

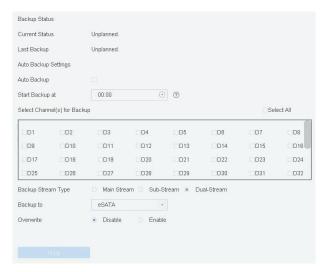


図9-5 自動バックアップ用のeSATA の構成

9.2 ディスクアレイ

ディスクアレイは、複数の物理ディスクドライブを 1 つの論理ユニットにまとめたデータストレージ 仮想化テクノロジです。アレイは「RAID」とも呼ばれ、1 台のディスクに障害が発生した場合にデータを復元できるように、複数のHDD にデータを保存し、必要な冗長性とパフォーマンスに基づいて、「RAID レベル」と呼ばれる複数の方法のいずれかでドライブにデータを分散します。

9.2.1 ディスクアレイを作成する

ビデオレコーダは、ソフトウェアベースのディスクアレイをサポートする。必要に応じてRAID機能を有効にし、各HDD容量が4TB以上であることを確認します。アレイを作成するには、ワンタッチ構成とマニュアル構成の2つの方法があります。

ワンタッチクリエイション

ワンタッチ構成でディスクアレイを作成します。デフォルトでは、ワンタッチ構成で作成される配列タイプはRAID 5 です。

開始前に

3 台以上のHDD を取り付けます。HDD が10 台以上取り付けられている場合は、2 つのアレイが作成されます。HDDの信頼性と安定性を維持するために、同じモデルと容量の企業レベルの HDDを使用することが推奨される。

- 1.「保存→の詳細」に移動します。
- 2. RAID を有効にするをチェックします。
- 3. 設定を有効にするには、Apply(適用)をクリックし、デバイスを再起動します。

- 4. 再起動後、Storage → RAID 設定→物理ディスクに移動します。
- 5. ワンタッチ設定をクリックします。
- 6. アレイ名を編集し、OK をクリックして設定を開始します。

[ji 注

- 4 台以上のHDD を取り付けると、アレイを再構築するためのホットスペアディスクが作成されます。
- 7. オプション: ビデオレコーダは、作成されたアレイを自動的に初期化します。Storage → RAID 設定→アレイに移動して、作成されたアレイの内容を表示します。

マニュアル作成

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

- 1.「保存→の詳細」に移動します。
- 2. RAID を有効にするをチェックします。
- 3. 設定を有効にするには、Apply(適用)をクリックし、デバイスを再起動します。
- 4. 再起動後、Storage → RAID 設定→物理ディスクに移動します。
- 5. 作成をクリックします。

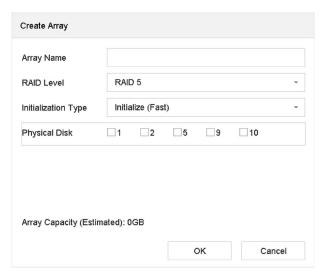


図9-6 アレイの作成

- 6. アレイ名を入力します。
- 7. 必要に応じてRAID レベルを選択します。
- 8. アレイを構成する物理ディスクを選択します。

表9-1	必要なHDD	数
	20'50'01'00	

RAID レベル	必要なHDD 数	
RAID 0	2 台以上のHDD。	
RAID 1	2 台以上のHDD。	
RAID 5	3 台以上のHDD。	
RAID 6	4 台以上のHDD。	
RAID 10	HDD の数は、4 ~16 の偶数の範囲にする必要があります。	

- 9. [OK]をクリックします。
- 10. オプション: ビデオレコーダは、作成されたアレイを自動的に初期化します。Storage → RAID 設定→アレイに移動して、作成されたアレイの内容を表示します。



図9-7 アレイ一覧

9.2.2 アレイの再構築

アレイのステータスには、Functional、Degraded、および Offline が含まれます。配列に格納されているデータの高いセキュリティと信頼性を確保するために、配列のステータスに応じて、配列を迅速かつ適切に保守します。

機能

アレイにディスク損失がない。

オフライン

失われたディスクの数が制限を超えました。

劣化

アレイ内のいずれかの HDD に障害が発生すると、アレイは劣化します。アレイを再構築することで、機能ステータスに復元します。

ホットスペアディスクの設定

ホットスペアディスクは、ディスクアレイの自動再構築に必要です。

手順

1. Storage → RAID 設定→物理ディスクに移動します。

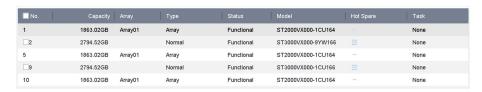


図9-8 物理ディスク

2. 使用可能なHDD をクリックして、ホットスペアディスクとして設定します。 ☑

アレイを自動的に再構築する

ビデオレコーダは、ホットスペアディスクを用いて、劣化したアレイを自動的に再構築することができる。

開始前に

ホットスペアディスクを作成します。詳細については、「ホットスペアディスクの設定」を参照してください。

手順

1. Storage → RAID 設定→アレイに移動します。



図9-9 アレイ一覧

アレイを手動で再構築する

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

開始前に

アレイを再構築するには、少なくとも 1 台の使用可能な物理ディスクが存在する必要があります。

- 1. Storage → RAID 設定→アレイに移動します。
- 2. 劣化アレイのクリック。 🗹

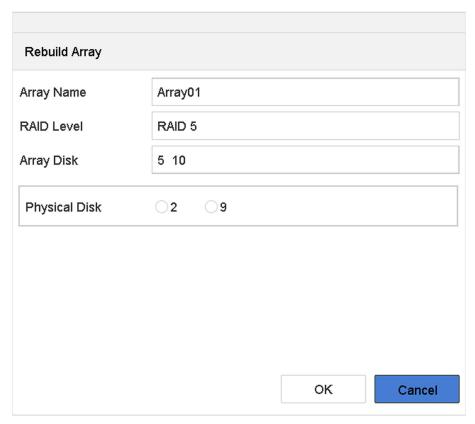


図9-10 アレイの再構築

- 3. 使用可能な物理ディスクを選択します。
- 4. [OK]をクリックします。
- 5. ポップアップ・メッセージ「再構築中の物理ディスクを切り離さない」をクリックすると、OKが表示されます。

第10章ネットワーク設定

10.1 DDNS の設定

ネットワークアクセスにダイナミックDNS サービスを設定できます。さまざまなDDNS モード (DynDNS、PeanutHull、およびNO-IP) を使用できます。

開始前に

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

手順

1. →ユーティリティネットワーク TCP/IP → DDNS に移動します。

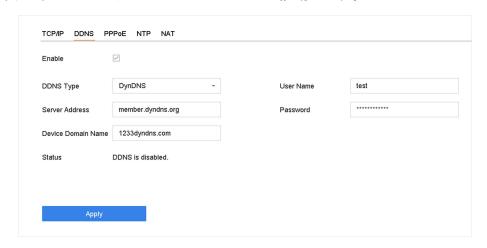


図10-1 DDNS 設定

- 2. 有効をチェックします。
- 3. DynDNSとしてDDNSタイプを選択します。
- 4. DynDNS のサーバアドレス(members.dyndns.org) を入力します。
- 5. Device Domain Name(デバイスドメイン名)に、DynDNS ウェブサイトから取得したドメイン名を入力します。
- 6. DynDNS Webサイトに登録されているユーザー名とパスワードを入力します。
- 7. 適用をクリックします。

10.2 Configure PPPoE

機器がPPPoE 経由でインターネットに接続されている場合は、→ユーティリティのTCP/IP → PPPoE でユーザ名とパスワードを適宜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にお問い合わせください。

10.3 ポートマッピング(NAT) の設定

クロスセグメントネットワークを介したリモートアクセスを実現するために、2つの方法、UPnP(商標)および手動マッピングがポートマッピングのために提供される。

開始前に

デバイスのUPnP™機能を有効にする場合は、デバイスが接続されているルータのUPnP™機能を有効にする必要があります。装置のネットワーク作業モードをマルチアドレスに設定する場合は、装置のDefault Route はルータのLAN IP アドレスと同じネットワークセグメントにある必要があります。

Universal Plug and Play (UPnP™)は、デバイスがネットワーク上の他のネットワークデバイスの存在をシームレスに検出し、データ共有、通信などのための機能的なネットワークサービスを確立することを可能にします。UPnP™機能を使用すると、ポートマッピングなしでデバイスをルータ経由でWAN に高速接続できます。

手順

1. \rightarrow ユーティリティネットワーク TCP/IP \rightarrow NAT に移動します。

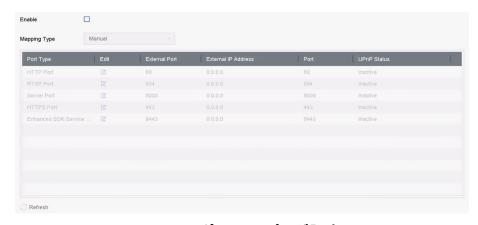


図10-2 ポートマッピング設定

- 2. 有効をチェックします。
- 3. Mapping Type as Manual or Autoを選択します。
 - Auto: Auto を選択すると、ポートマッピング項目は読み取り専用になり、外部ポートはルータによって自動的に設定されます。
 - Manual(手動):Manual(手動)を選択すると、External Port Settings(外部ポート設定)をクリックしてアクティブにすることで、需要に応じて外部ポートを編集できます。

注

● デフォルトのポート番号を使用するか、実際の要件に従って変更できます。

- External Port は、ルータ内のポートマッピング用のポート番号を示します。
- RTSPポート番号の値は554または1024~65535で、他のポートの値は1~65535で、値は互いに異なっている必要があります。同一ルータ下のUPnP™設定に複数の機器が設定されている場合、各機器のポート番号の値は一意である必要があります。
- 4. ルータの仮想サーバ設定ページを入力します。内部ソースポートの空白に内部ポート値、外部ソースポートの空白に外部ポート値、およびその他の必要な内容を入力します。

[ji注

- 各項目は、サーバーポート、http ポート、RTSP ポート、https ポートなどのデバイスポート に対応している必要があります。
- 下記の仮想サーバ設定インタフェースは参考用であり、ルータの製造元によって異なる場合があります。仮想サーバの設定に問題がある場合は、ルータの製造元にお問い合わせください。



図10-3 仮想サーバ項目の設定

10.4 Wi-Fi の設定

Wi-Fi ドングルを使用して、デバイスをワイヤレスネットワークに接続できます。

開始前に

適切なWi-Fiドングルを準備し、背面パネルのUSBインターフェイスに挿入します。

手順

1. →ネットワーク→ TCP/IP → Wi-Fiに行く。



図10-4 ワイヤレスネットワークへの接続

- 2. Wi-Fi を有効にするをチェックします。
- 3. ワイヤレスネットワークに接続します。

ヤレスネットワークへ

- **自動検索されたワイ** 1. 必要に応じて、リストからワイヤレスネットワークをダブルクリック します。
- の接続
- 2. ワイヤレスネットワークのパラメータを設定します。
- 3. [OK]をクリックします。

カスタマイズしたワイ 1. カスタム追加をクリックします。

ヤレスネットワークへ 2. ワイヤレスネットワークのパラメータを設定します。

の接続

3. [OK]をクリックします。

WPS (Wi-Fi

1. WPS 設定をクリックします。

Protected Setup)で

2. WPS を有効にするをチェックします。

ワイヤレスネットワー 3. ワイヤレスネットワークのパラメータを設定します。

クに接続する

4. 適用をクリックします。

利用可能なワイヤレスネットワークに接続した後、接続結果を Connection Status(接続ステー タス)で表示することができます。

- $4. \rightarrow \Delta$ ーティリティネットワーク TCP/IP \rightarrow TCP/IP に移動します。
- 5. 「NIC」と「既定のルート」を「WLANO」に設定します。
- 6. その他のネットワークパラメータを設定します。
- 7. 適用をクリックします。

10.5 SNMP の設定

SNMP 設定を構成して、デバイスのステータスとパラメータ情報を取得できます。

開始する前に

SNMP ソフトウェアをダウンロードして、SNMP ポート経由でデバイス情報を受信します。トラップアドレスおよびポートを設定することによって、デバイスは、警報イベントおよび例外メッセージを監視センタに送信することが可能になる。

手順

1. 「システム→網→先進→ SNMP」へ。

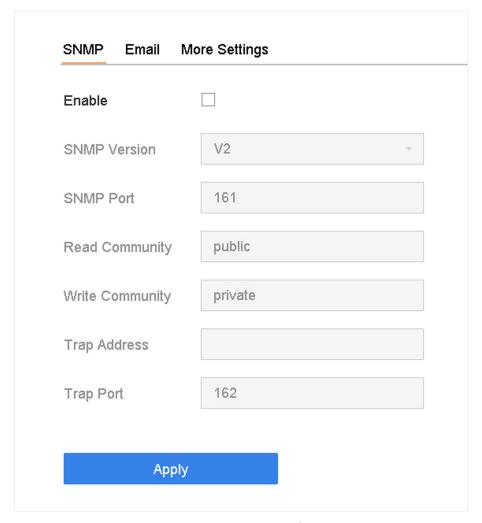


図10-5 SNMP 設定

- 2. 有効をチェックします。メッセージがポップアップして、セキュリティリスクの可能性を通知します。 [はい] をクリックして続行します。
- 3. 必要に応じてSNMP 設定を構成します。

トラップアドレス

SNMP ホストのIP アドレス。

トラップポート

SNMP ホストのポート。

4. 適用をクリックします。

10.6 電子メールの設定

システムは、アラームまたはモーションイベントが検出されたとき、または管理者パスワードが変更されたときなど、指定されたイベントが発生したときに、すべての指定されたユーザに電子メール通知を送信するように構成することができる。

開始前に

デバイスは、SMTP メールサーバを含むローカルエリアネットワーク(LAN) に接続する必要があります。また、通知を送信する電子メールアカウントの場所に応じて、ネットワークがイントラネットまたはインターネットに接続されている必要があります。

手順

1. →ネットワーク→先進→メールへ。

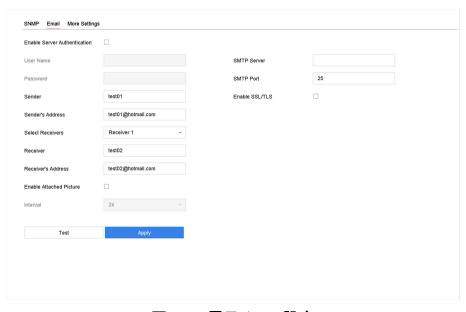


図10-6 電子メール設定

2. 電子メール設定を構成します。

サーバー認証の有効化

SMTP サーバーがユーザー認証を必要とするかどうかをチェックして機能を有効にし、それに応じてユーザー名とパスワードを入力します。

SMTPサーバー

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

SMTP ポート

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

SSL/TLS を有効にする

SMTP サーバーで必要な場合は、SSL/TLS を有効にします。

送信者

送信者の名前。

送信者の住所

送信者のアドレス。

受信者の選択

受信側を選択します。3台まで設定できます。

レシーバ

受信者の名前。

受信者の住所

通知されるユーザーの電子メールアドレス。

添付画像を有効にする

アラーム画像を添付したメールを送信することを確認してください。間隔は、2つの後続のアラーム画像を送信する間の時間である。

- 3. 適用をクリックします。
- 4. 必要に応じて、「テスト」を選択してテストメールを送信します。

10.7 ポートの設定

さまざまなタイプのポートを設定して、関連する機能を有効にできます。

手順

1. →ユーティリティネットワーク 詳細→詳細設定に移動します。

Alarm Host IP	
Alarm Host Port	0
Server Port	8000
HTTP Port	80
Multicast IP	
RTSP Port	554
Enhanced SDK Ser	8443
Apply	

図10-7 ポート設定

2. 必要に応じてポート設定を構成します。

アラームホストIP/ポート

リモートアラームホストが構成されている場合、デバイスは、アラームがトリガされると、アラームイベントまたは例外メッセージをホストに送信する。リモートアラームホストには、クライアント管理システム(CMS) ソフトウェアがインストールされている必要があります。アラームホストIP は、CMS ソフトウェア(iVMS-4200 など) がインストールされているリモートPC のIP アドレスを参照し、アラームホストポート(デフォルトは7200) は、ソフトウェアに設定されているアラーム監視ポートと同じである必要があります。

サーバーポート

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

HTTP ポート

HTTP ポート(デフォルトでは80) は、リモートWeb ブラウザアクセス用に設定する必要があります。

マルチキャストIP

マルチキャストは、ネットワークを介して許可される最大数を超えるカメラのライブビューを有効にするように構成することができる。マルチキャストIP アドレスは224.0.0.0 ~ 239.255.255.255 の範囲のClass-D IP をカバーし、239.252.0.0 ~239.255.255.255 の範囲のIP アドレスを使用することをお勧めします。CMS ソフトウェアにデバイスを追加する場

合、マルチキャストアドレスはデバイスのアドレスと同じである必要があります。

RTSPポート

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

拡張SDKサービスポート

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

3. 適用をクリックします。

10.8 ONVIF の設定

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

手順

- 1. 保守→システムサービス→ ONVIFに移動します。
- 2. ONVIF アクセス管理を有効にするには、ONVIF を有効にするをチェックします。

山注

ONVIF プロトコルはデフォルトで無効になっています。

- 3. 追加をクリックします。
- 4. ユーザー名、パスワードの入力

製品のセキュリティを高めるために、独自に選択した強力なパスワードを作成することを強くお勧めします(大文字、小文字、数字、特殊文字の3 つ以上を含む8 文字以上の使用)。また、高セキュリティシステムでは、特に毎月または毎週パスワードをリセットすることで、製品の保護を向上させることができるため、パスワードを定期的にリセットすることをお勧めします。

- 5. Media User、Operator、またはAdmin としてLevel を選択します。
- 6. [OK]をクリックします。

第 11 章ユーザー管理とセキュリティ

11.1 アカウントを管理する

Administrator ユーザー名はadmin で、パスワードはデバイスを初めて起動するときに設定されます。管理者には、ユーザーの追加と削除、およびユーザーパラメータの設定を行う権限があります。

11.1.1 ユーザーの追加

手順

- 1.「システム→ユーザ」へ。
- 2. 「追加」をクリックして、操作許可インターフェースに入ります。
- 3. 管理者パスワードを入力し、OK をクリックします。
- 4. 「ユーザの追加」インターフェースで、新しいユーザの情報を入力します。

企注意

強力なパスワードの推奨-製品のセキュリティを高めるために、独自に選択した強力なパスワードを作成することを強くお勧めします(大文字、小文字、数字、特殊文字の3 つ以上のカテゴリを含む8 文字以上を使用)。また、パスワードを定期的にリセットすることをお勧めします。特に、高セキュリティシステムでは、毎月または毎週パスワードをリセットすることで、製品を保護することができます。

ユーザーレベル

ユーザーレベルをオペレータまたはゲストに設定します。ユーザーレベルによって操作権限が異なります。

- オペレータ:オペレータユーザレベルには、Remote Configuration の「2 ウェイオーディオ」 権限と、デフォルトでCamera Configuration のすべての操作権限があります。
- ゲスト:ゲストユーザには、リモート設定での双方向オーディオの権限はなく、デフォルトではカメラ設定でのローカル/リモート再生のみがあります。

ユーザーのMACアドレス

デバイスにログオンするリモートPC のMAC アドレス。設定されて有効になっている場合、こ

のMAC アドレスを持つリモートユーザーのみがデバイスにアクセスできます。

5. [OK]をクリックします。

User Management インターフェースで、追加された新しいユーザーがリストに表示されます。

11.1.2 管理者ユーザーの編集

admin ユーザーアカウントの場合は、パスワードとロック解除パターンを変更できます。

- 1.「システム→ユーザ」へ。
- 2. リストから管理者ユーザーを選択します。
- 3. 変更をクリックします。



図11-1 ユーザーの編集(Admin)

- 4. 新しい管理者パスワード(強力なパスワードが必要)やMAC アドレスなど、必要に応じて管理者ユーザー情報を編集します。
- 5. admin ユーザーアカウントのロック解除パターンを編集します。
 - 1) デバイスへのログイン時にロック解除パターンの使用を有効にするには、ロック解除パターンを有効にするをオンにします。
 - 2) マウスを使用して画面上の9 つのドットの中からパターンを描き、パターンが終了したらマウスを放します。
- 6. GUID ファイルのエクスポートをオンにすると、admin ユーザーアカウントのGUID ファイルがエクスポートされます。

[i]注

管理者パスワードが変更されたら、今後のパスワードリセットのために、Import/Export インタフェースで接続されたUSB フラッシュドライブに新しいGUID をエクスポートします。

- 7. パスワードリセットのセキュリティ質問を設定します。
- 8. パスワードリセット用の予約メールを設定します。
- 9. 設定を保存するには、OKをクリックします。

11.1.3 オペレータ/ゲストユーザの編集

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

手順

- 1.「システム→ユーザ」へ。
- 2. リストからユーザーを選択し、「変更」をクリックします。

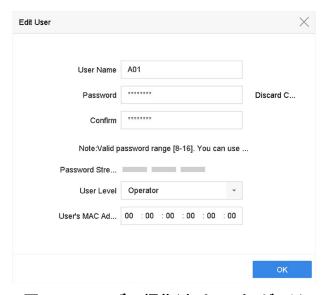


図11-2 ユーザの編集(オペレータ/ゲスト)

- 3. 新しいパスワード(強力なパスワードが必要)やMACアドレスなど、必要に応じてユーザー情報 を編集します。
- 4. [OK]をクリックします。

11.2 権限付与を行なう

11.2.1 ユーザー権限の設定

追加されたユーザーには、デバイスのローカル操作やリモート操作など、さまざまな権限を割り当

てることができます。

手順

- 1.「システム→ユーザ」へ。
- 2. リストからユーザーを選択し、をクリックして権限設定インターフェースに入ります。 🤡

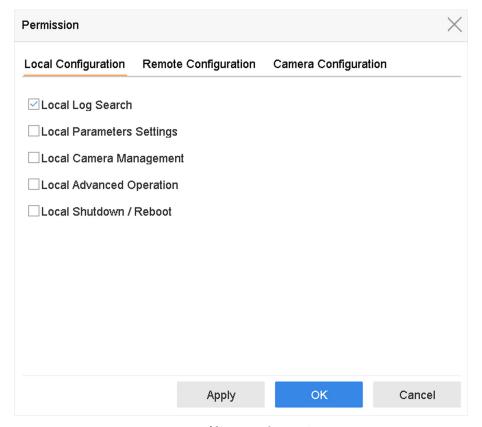


図11-3 ユーザ権限設定インタフェース

- 3. ユーザーのローカル設定、リモート設定、カメラ設定に対するユーザーの操作権限を設定します。
 - 1) ローカル設定の設定
 - ローカルログ検索

デバイスのログとシステム情報の検索と表示。

ローカルパラメータ設定

パラメータの設定、工場出荷時のデフォルトパラメータの復元、設定ファイルのインポート/エクスポート。

ローカルカメラ管理

IPカメラの追加・削除・編集

ローカル・アドバンスド・オペレーション

HDD管理の操作(HDDの初期化、HDDプロパティの設定)、システムファームウェアのアップグレード、I/Oアラーム出力のクリア

ローカルシャットダウン再起動

デバイスのシャットダウンまたはリブート。

2) リモート設定の設定

リモートログ検索

デバイスに保存されているログをリモートで表示します。

リモートパラメータ設定

パラメータのリモート設定、工場出荷時のデフォルトパラメータの復元、設定ファイルのインポート/エクスポート。

リモートカメラ管理

IPカメラのリモート追加、削除、編集

リモートシリアルポート制御

RS-232 およびRS-485 ポートの設定を行います。

リモートビデオ出力制御

遠隔ボタン制御信号を送信します。

双方向オーディオ

リモートクライアントとデバイスとの間で双方向無線を動作させる。

リモートアラーム制御

リモートアーミング(リモートクライアントにアラームおよび例外メッセージを通知する)およびアラーム出力の制御。

リモートアドバンスト操作

HDD管理の遠隔操作(HDDの初期化、HDDプロパティの設定)、システムファームウェアのアップグレード、I/Oアラーム出力のクリア

リモートシャットダウン/再起動

デバイスをリモートでシャットダウンまたは再起動する。

3) カメラ設定

リモートライブビュー

選択したカメラのライブビデオをリモートで表示します。

ローカルマニュアル操作

選択したカメラの手動録画およびアラーム出力をローカルで開始/停止します。

リモートマニュアル操作

選択したカメラの手動録画とアラーム出力をリモートで開始/停止します。

ローカル再生

選択したカメラの録画ファイルをローカル再生します。

リモート再生

選択したカメラの録画ファイルをリモート再生します。

ローカルPTZ制御

選択したカメラのPTZ 移動をローカルで制御します。

リモートPTZコントロール

選択したカメラのPTZ 移動をリモートコントロールします。

ローカルビデオエクスポート

選択したカメラの記録ファイルをローカルにエクスポートします。

ローカルライブビュー

ローカルで選択したカメラのライブビデオを表示します。

4. 設定を保存するには、OKをクリックします。

11.2.2 Live View Permission on Lock画面の設定

管理者ユーザは、デバイスの画面ロック状態において、特定のカメラのライブビュー許可を設定することができる。

- 管理者ユーザーは、この権限をユーザーアカウントに設定できます。
- 通常のユーザ(オペレータまたはゲスト)が特定のカメラのローカルライブビュー許可を持っていない場合、ロック画面ステータス上のそのようなカメラのライブビュー許可は設定できません(デフォルトではライブビューは許可されません)。

- 1.「システム→ユーザ」へ。
- 2. ロック画面でライブビュー権限をクリックします。
- 3. 管理者パスワードを入力し、次へをクリックします。

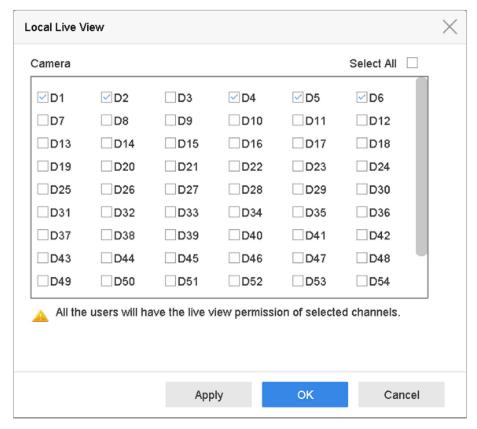


図11-4 ロック画面でのライブビューの許可の設定

- 4. 権限を設定します。現在のユーザアカウントがログアウト状態にあるときに、カメラを選択して ライブビューを許可します。
- 5. [OK]をクリックします。

11.3 パスワードセキュリティの設定

11.3.1 GUID ファイルのエクスポート

GUID ファイルは、パスワードを忘れたときにパスワードをリセットするのに役立ちます。適切に保管してください。

- 1. エクスポートをオンにし、OK をクリックして、デバイスをアクティブ化するときにGUID ファイルをエクスポートするか、admin ユーザーアカウントを編集します。
- 2. デバイスに USB フラッシュドライブを挿入し、GUID 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。

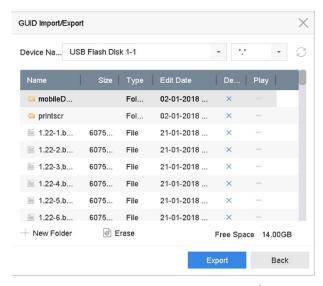


図11-5 GUID ファイルのエクスポート

- 3. デバイスを選択します。
- 4. デバイス上のディレクトリを選択します。
- 5. エクスポートをクリックします。

11.3.2 セキュリティ質問の設定

セキュリティ上の質問は、パスワードを忘れた場合やセキュリティ上の問題が発生した場合に、 パスワードをリセットするのに役立ちます。

- 1. デバイスをアクティブ化するとき、または管理者ユーザーアカウントを編集するときは、「セキュリティ質問の設定」を選択します。
- 2. ドロップダウンリストから3つのセキュリティ質問を選択し、回答を入力します。

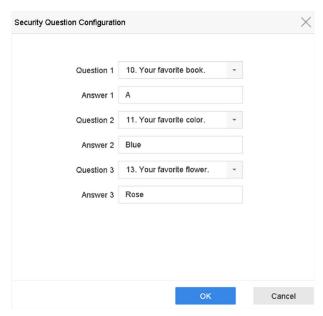


図11-6 セキュリティの質問の設定

3. [OK]をクリックします。

11.3.3 予約メールの設定

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

- 1. デバイスをアクティブ化するときに予約済みの電子メールをオンにするか、admin ユーザーアカウントを編集するときに「変更」をクリックします。
- 2. 予約メールアドレスを入力します。

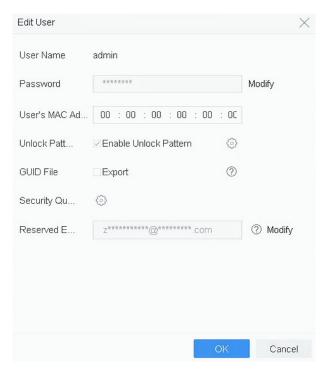


図11-7 予約電子メールの設定

3. [OK]をクリックします。

11.4 パスワードのリセット

管理者パスワードを忘れた場合は、GUID ファイルのインポート、セキュリティ上の質問への回答、または予約された電子メールからの確認コードの入力を行うことで、パスワードをリセットできます。

11.4.1 GUID によるパスワードのリセット

開始前に

GUID ファイルは、デバイスをアクティブ化した後、またはadmin ユーザーアカウントを編集した後に、エクスポートしてUSB フラッシュドライブに保存する必要があります。

手順

- 1. ユーザーログインインターフェースで、「パスワードを忘れました」をクリックします。
- 2. Password Reset Type で、Verify by GUID を選択します。

[ji]注

パスワードをリセットする前に、GUID ファイルに保存されているUSB フラッシュドライブをデバイスに挿入してください。

3. USB フラッシュドライブからGUID ファイルを選択し、Import(インポート)をクリックしてファイルをデバイスにインポートします。

[ji注

間違ったGUID ファイルを7 回インポートした場合、パスワードを30 分間リセットすることはできません。

- 4. GUID ファイルが正常にインポートされたら、リセットパスワードインタフェースを入力して新しい管理者パスワードを設定します。
- 5. OK をクリックして、新しいパスワードを設定します。今後のパスワードのリセットのために、新しいGUID ファイルをUSB フラッシュドライブにエクスポートできます。

[ji 注

新しいパスワードが設定されると、元のGUID ファイルは無効になります。新しいGUID ファイルは、今後のパスワードリセットのためにエクスポートする必要があります。また、User → User Management と入力して、管理者ユーザーを編集し、GUID ファイルをエクスポートすることもできます。

11.4.2 セキュリティ質問によるパスワードのリセット

開始前に

デバイスをアクティブ化するとき、またはadmin ユーザーアカウントを編集するときに、セキュリティ質問を設定しておきます。(17.3.2 セキュリティ質問の設定を参照)。

手順

- 1. ユーザーログインインターフェースで、「パスワードを忘れました」をクリックします。
- 2. セキュリティ質問による検証としてパスワードリセットタイプを選択します。
- 3.3つのセキュリティ質問の正解を入力します。
- 4. [OK]をクリックします。
- 5. 「パスワードのリセット」インターフェースで新しい管理者パスワードを作成します。

11.4.3 Guarding Vision によるパスワードのリセット

開始前に

デバイスがGuarding Vision を有効にし、登録済みのGuarding Vision アカウントにバインドされていることを確認します。

- 1. ユーザーログインインターフェースで、「パスワードを忘れました」をクリックします。
- 2. パスワードリセットタイプのインターフェースで、「視覚の保護による検証」を選択します。

- 3. デバイスにバインドされているアカウントでGuarding Vision アプリにログインします。
- 4. QRコードを読み取るには、Guarding Visionを使用します。その後、Guarding Visionから検証コードがあります。
- 5. 確認コードを入力します。
- 6. [OK]をクリックします。

11.4.4 予約メールによるパスワードのリセット

開始前に

デバイスをアクティブ化するとき、またはadmin ユーザーアカウントを編集するときに、予約済みの電子メールが設定されていることを確認します。(予備電子メールを参照 toConfigure reserved email)

- 1. ユーザーログインインターフェースで、「パスワードを忘れました」をクリックします。
- 2. パスワードリセットタイプのインターフェースで、「予約済み電子メールによる確認」を選択します。
- 3. [OK]をクリックします。
- 4. 法的免責事項を受け入れる場合は、「次へ」をクリックします。スマートフォンを使用してQRコードをスキャンし、正当な免責事項を読み取ることができます。
- 5. 確認コードを取得します。確認コードを取得するには、2 つの方法があります。
 - QRコードを読み取るには、Guarding Visionアプリを使用します。
 - QR コードを電子メールサーバーに送信します。
 - 1. USB フラッシュドライブをデバイスに挿入します。
 - 2. Export(エクスポート)をクリックして、QR コードを USB フラッシュドライブにエクスポートします。
 - 3. QRコードを添付としてpw_recovery@device-service.comにメールで送信します。
- 6. 予約済みの電子メールを確認すると、5 分以内に確認コードが届きます。
- 7. 確認コードを入力します。
- 8. OK をクリックして、新しいパスワードを設定します。

第 12 章システム管理

12.1 デバイスの設定

手順

- 1.「システム→全般」に移動します。
- 2. 以下の設定を行います。

言語

使用されるデフォルト言語は英語である。

出力規格

出力規格をNTSC またはPAL に設定します。これは、ビデオ入力規格と同じである必要があります。

解像度

ビデオ出力解像度を設定します。

デバイス名

デバイス名を編集します。

装置番号

デバイスのシリアル番号を編集します。デバイス番号は1~255の範囲で設定でき、初期値は255です。リモコンとキーボードのコントロールには番号が使用されます。

自動ログアウト

メニュー非アクティブ時のタイムアウト時間を設定します。例えば、タイムアウト時間が5分に設定されると、システムは、メニューの非アクティブ状態が5分間続いた後、現在の操作メニューからライブビュー画面に戻ります。

マウスポインタ速度

マウスポインタの速度を設定します。4 つのレベルを設定できます。

ウィザードの有効化

デバイスの起動時にウィザードを有効/無効にします。

パスワードの有効化

ログインパスワードの使用を有効/無効にします。

3. [適用] をクリックして、設定を保存します。

12.2 時間の設定

12.2.1 手動時間同期

手順

- 1.「システム→全般」に移動します。
- 2. 日付と時刻を設定します。
- 3. [適用] をクリックして、設定を保存します。

12.2.2 NTP同期

ネットワークタイムプロトコル(NTP)サーバへの接続は、システムの日付と時刻の正確性を確保するために、デバイスで設定できます。

手順

- 1. システム→網→ TCP/IP → NTPに移動します。
- 2. 有効をチェックします。
- 3. 必要に応じてNTP 設定を構成します。

間隔(min)

NTP サーバとの2 つの時刻同期間の時間間隔

NTPサーバ

NTP サーバのIP アドレス

NTP ポート

NTPサーバのポート

4. 適用をクリックする

12.2.3 DST 同期

DST (daylight saving time)は、クロックが1周期先に移動される年の期間を指す。世界中のいくつかの地域では、これは、天候が最も暖かい数ヶ月間の夕方により多くの日照時間を作り出す効果を有する。

DSTの開始時には、時計を一定期間(設定したDSTバイアスによって決まります)先に進め、標準時間(ST)に戻すのと同じ期間に戻します。

- 1.「システム→全般」に移動します。
- 2. DST を有効にするをチェックします。

3. DSTモードを「自動」または「手動」に設定します。

自動

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

マニュアル

DST期間の開始時刻と終了時刻、DSTバイアスを手動で設定します。

- 4. DSTバイアスを設定します。標準時間から時間(30/60/90/120分)オフセットを設定します。
- 5. 「適用」をクリックして、設定を保存します。

12.3 ネットワーク検出

12.3.1 ネットワークトラフィックの監視

ネットワークトラフィックの監視とは、ネットワークのパフォーマンス、可用性、セキュリティに影響を与える可能性のある異常またはプロセスについて、ネットワークトラフィックを確認、分析、管理するプロセスのことです。

- 1. 保守→網→トラヒックに移動します。
- 2. MTU (Maximum Transmission Unit)やネットワークスループットなど、リアルタイムのネットワークトラフィックステータスを表示できます。

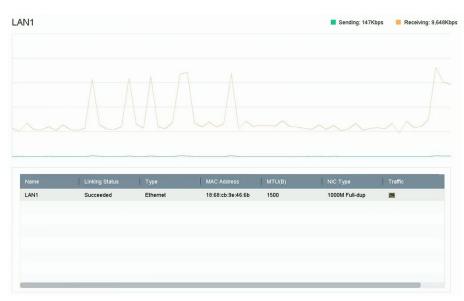


図12-1 ネットワークトラフィック

12.3.2 ネットワーク遅延とパケット損失のテスト

ネットワーク遅延は、特定のネットワークプロトコル(TCP/IP など)で送信中に過剰サイズのデータ情報が制限されない場合に、デバイスの応答が遅くなることによって発生します。パケット損失試験は、失われたデータパケットと送信されたデータパケットの総数との比であるネットワークパケット損失率を試験するためのものである。

手順

- 1. 保守→網→検知に進む。
- 2. NIC の選択でネットワークカードを選択します。
- 3. 「宛先アドレス」に宛先IP アドレスを入力します。
- 4. 「テスト」をクリックします。



図12-2 ネットワーク遅延とパケット損失のテスト

12.3.3 ネットワークパケットのエクスポート

レコーダーがネットワークにアクセスしたら、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エクスポートできます。

開始前に

ネットワークパケットをエクスポートするUSB フラッシュドライブを準備します。

- 1. USB フラッシュドライブを挿入します。
- 2. 保守→網→検知に進む。
- 3. NIC の選択でネットワークカードを選択します。
- 4. Device Name(デバイス名)でUSB フラッシュドライブを選択します。接続されたローカルバックアップデバイスが表示できない場合は、Refresh(更新)をクリックできます。



図12-3 ネットワークパケットのエクスポート

- 5. オプション:「状況」を選択して、ネットワーク状況を表示します。
- 6. エクスポートをクリックします。

[i]注

デフォルトでは、毎回1MB のデータがエクスポートされます。

12.3.4 ネットワークリソース統計

Webブラウザやクライアントソフトウェアを含むリモートアクセスは、出力帯域幅を消費します。リアルタイムの帯域幅統計を表示できます。

手順

1. 保守→網→統計に移動します。



図12-4 ネットワークリソース統計

- 2. IPカメラ、リモート・ライブ・ビュー、リモート・プレート、ネット・トータル・アイドルなどを含む帯域 幅統計を表示します。
- 3. (オプション)最新のデータを取得するには、「更新」を選択します。

12.4 ストレージデバイスのメンテナンス

12.4.1 不良セクター検出

- 1. 保守→ HDD 動作→ 不良セクタ検知に進みます。
- 2. ドロップダウンリストから設定したいHDD No.を選択します。
- 3. 検出タイプとして「すべて検出」または「キーエリア検出」を選択します。
- 4. Self-Test をクリックして検出を開始します。

デジタルビデオレコーダー取扱説明書

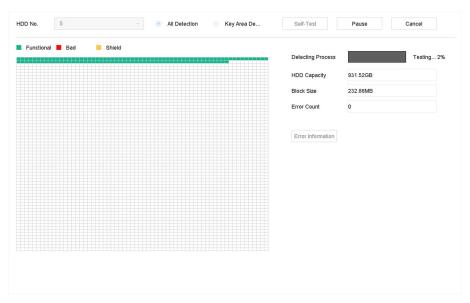


図12-5 セクタ検出不良

〔〕注

検出を一時停止/再開またはキャンセルできます。テストが完了したら、エラー情報をクリックして 詳細な損傷情報を確認できます。

12.4.2 S.M.A.R.T.検出

S.M.A.R.T.やBad Sector Detection技術の採用などのHDD検出機能S.M.A.R.T. (自己監視、分析、報告技術)は、故障を予測するために様々な信頼性指標を検出するHDD監視システムである。

- 1. 保守→ HDD 動作→ S.M.A.R.T に進みます。
- 2. HDD を選択すると、そのS.M.A.R.T. 情報リストが表示されます。
- 3. Self-Test Type を設定します。
- 4. Self-Test をクリックしてS.M.A.R.T を起動します。HDD自己評価

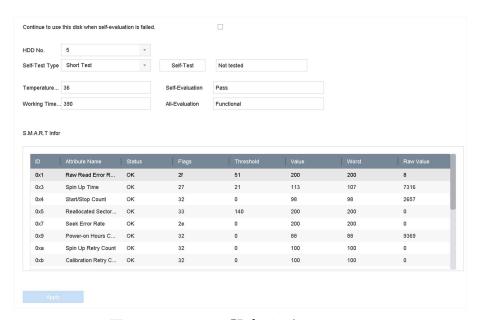


図12-6 S.M.A.R.T.設定インターフェース

Di注

S.M.A.R.T.チェックに失敗してもHDDを使用する場合は、自己評価に失敗したときにディスクを使用し続けるをチェックします。

S.M.A.R.T.の関連情報が表示され、HDDの状態を確認できます。

12.4.3 HDD Health Detection

平成29年10月1日以降に発生した4TB~8TB Seagate HDDの健康状態を確認できます。この機能を使用して、HDD の問題のトラブルシューティングに役立ててください。Health Detectionは、S.M.A.R.T.機能よりも詳細なHDDステータスを示します。

手順

1. 保守→ HDD オペレーション・→・ヘルス・ディテクションに進みます。

デジタルビデオレコーダー取扱説明書

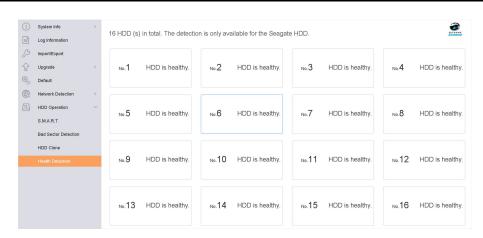


図12-7 健康状態の検出

2. 詳細を表示するには、HDD をクリックします。

12.4.4 ディスククローンの設定

eSATA HDD にクローンを作成するHDD を選択します。

開始前に

eSATA ディスクをデバイスに接続します。

手順

1. 保守→ HDD 運用→ HDD 複製に移動します。

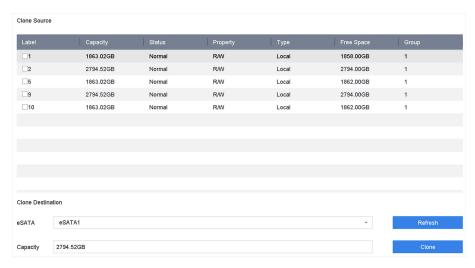


図12-8 HDD クローン

- 2. HDDのクローンを確認します。選択したHDDの容量は、クローン先の容量と一致している必要があります。
- 3. クローンをクリックします。
- 4. ポップアップ・メッセージ・ボックスで「はい」をクリックして、クローンを作成します。

12.4.5 修復データベース

データベースを修復すると、すべてのデータベースが再構築されます。これは、アップグレード後にシステム速度を向上させるのに役立つ可能性があります。

手順

- 1. Storage → Storage Device に移動します。
- 2. ドライブを選択します。
- 3. データベースの修復をクリックします。
- 4. はいをクリックします。

[i];

- データベースを修復すると、すべてのデータベースが再構築されます。既存のデータは影響を受けませんが、処理中はローカルの検索/再生機能は利用できません。Webブラウザやクライアントソフトウェアなどを介して、リモートで検索/再生機能を実現することができます。
- ▶ ドライブを引き抜いたり、装置をシャットダウンしたりしないでください。

修理の進捗状況はStatusに表示されます。



図12-9 修理データベース

12.5 アップグレードデバイス

デバイスのファームウェアは、ローカルバックアップデバイスまたはリモートFTP サーバでアップグレードできます。

12.5.1 ローカルバックアップデバイスによるアップグレード

開始前に

ファームウェアアップデートファイルを含むローカルストレージデバイスにデバイスを接続します。

- 1. 保守→のアップグレードに進みます。
- 2. ローカルアップグレードをクリックして、ローカルアップグレードインタフェースに入ります。



図12-10 ローカル・アップグレード・インタフェース

- 3. ストレージデバイスからファームウェアアップデートファイルを選択します。
- 4. アップグレードをクリックしてアップグレードを開始します。 アップグレードが完了すると、デバイスが自動的に再起動し、新しいファームウェアがアクティ ブになります。

12.5.2 FTPによるアップグレード

開始前に

PC(FTPサーバを実行している)とデバイスのネットワーク接続が有効で正しいことを確認します。 PC でFTP サーバを実行し、ファームウェアをPC の対応するディレクトリにコピーします。

手順

- 1. 保守→のアップグレードに進みます。
- 2.「FTP」をクリックして、ローカルアップグレードインターフェイスに入ります。



図12-11 FTP アップグレードインターフェイス

- 3. FTP サーバアドレスを入力します。
- 4. アップグレードをクリックしてアップグレードを開始します。
- 5. アップグレードが完了したら、デバイスを再起動して新しいファームウェアをアクティブにします。

12.5.3 Webブラウザによるアップグレード

Web ブラウザでデバイスをアップグレードできます。

ウェブブラウザから本機にログイン後、→ユーティリティの保守→の設定に進みます。参照をクリックしてファームウェアをアップロードし、デバイスをアップグレードします。

12.5.4 Guarding Visionによるアップグレード

デバイスをGuarding Vision にログインすると、デバイスはGuarding Vision から最新のファームウェアを定期的にチェックします。アップグレード用のファームウェアが利用可能な場合、ログイン時にデバイスから通知されます。最新のファームウェアを手動で確認することもできます。

開始する前に

デバイスがGuarding Vision に正常に接続されていることを確認し、ファームウェアのダウンロード用に少なくとも1 つの読み取り/書き込みHDD をインストールする必要があります。

手順

- 1. 保守→のアップグレード→のオンラインアップグレードに移動します。
- 2. Check Upgrade(アップグレードの確認)をクリックして、Guarding Vision から最新のファームウェアを手動で確認し、ダウンロードします。

[i]注

デバイスは24 時間ごとに自動的に最新のファームウェアをチェックします。利用可能なアップグレードファームウェアが検出されると、ログイン時にデバイスから通知されます。

- 3. オプション:「最新のパッケージを自動的にダウンロード」をオンに切り替えて、最新のファームウェアパッケージを自動的にダウンロードできます。
- 4. 今すぐアップグレードをクリックします。

12.6 デバイス設定ファイルのインポート/エクスポート

装置構成ファイルは、バックアップのためにローカル装置にエクスポートすることができます。また、同じパラメーターで構成する場合は、1つの装置の構成ファイルを複数の装置にインポートすることができます。

開始前に

ストレージデバイスをデバイスに接続します。設定ファイルをインポートするには、ストレージデバイスにファイルが含まれている必要があります。

手順

1. 保守→のインポート/エクスポートに移動します。

デジタルビデオレコーダー取扱説明書



図12-12 構成ファイルのインポート/エクスポート

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

[]i注

設定ファイルのインポートが完了すると、デバイスは自動的に再起動します。

12.7 ログファイルの検索とエクスポート

デバイス動作、アラーム、例外、および情報は、ログファイルに格納することができ、ログファイルは、いつでも閲覧およびエクスポートすることができる。

手順

1. 保守→履歴情報に移動します。



図12-13 ログ検索インタフェース

- 2. 時間、メジャー・タイプ、マイナー・タイプなどのログ検索条件を設定します。
- (検索)をクリックして、ログ・ファイルの検索を開始します。
- 4. 一致したログファイルは、以下に示すようにリストに表示されます。

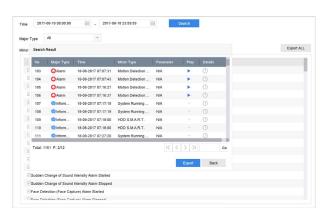


図12-14 ログ検索結果

〔〕注

毎回最大2000 個のログファイルを表示できます。

- 5. 関連操作:
 - 詳細情報を表示するには、クリックまたはダブルクリックします。
 - クリックすると、関連するビデオファイルが表示されます。

ALLのエクスポート/ クリックすると、すべてのシステムログがストレージデバイスにエクス**エクスポート** ポートされます。

12.8 デフォル設定に戻す

手順

1. 保守→初期値に移動します。

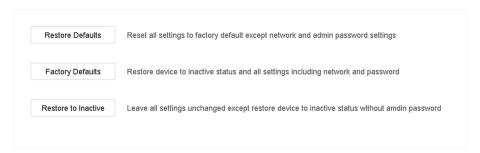


図12-15 デフォルト設定の復元

2. 次の3 つのオプションから復元タイプを選択します。

デフォルトの復元

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作業モード、デフォルトル

ート、サーバポートなど)とユーザアカウントパラメータを除くすべてのパラメータを工場出荷時のデフォルト設定に復元します。

Factory Defaults

すべてのパラメータを工場出荷時のデフォルト設定に戻します。

非アクティブに復元する

レコーダーを非アクティブ状態に戻します。

li注

デフォルトの設定に戻った後、レコーダーは自動的にリブートします。

12.9 セキュリティ管理

12.9.1 RTSP認証

RTSP認証を設定することで、ライブビューのストリームデータを特に保護できます。

手順

1. System → System Service → System Service に移動します。



図 12-16 RTSP 認証

2. RTSP 認証タイプを選択します。

[ji 注

ダイジェストを選択すると、ダイジェスト認証を使用した要求のみがIP アドレス経由でRTSP プロトコルによってビデオストリームにアクセスできるようになり、2 つの認証タイプを選択できます。セキュリティ上の理由から、認証タイプとしてダイジェストを選択することをお勧めします。

- 3. 適用をクリックします。
- 4. 設定を有効にするには、デバイスを再起動します。

12.9.2 HTTP 認証

HTTP サービスを有効にする必要がある場合は、HTTP 認証を設定してアクセスセキュリティを

強化できます。

手順

1. 保守→システムサービス→システムサービスに移動します。

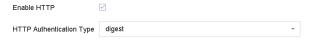


図 12-17 HTTP 認証

- 2. HTTP を有効にするをチェックします。
- 3.「HTTP 認証種別」を選択します。

[i]注

- 2 つの認証タイプを選択できます。セキュリティ上の理由から、認証タイプとしてダイジェストを選択することをお勧めします。
- 4. [適用] をクリックして、設定を保存します。
- 5. 設定を有効にするには、デバイスを再起動します。

12.9.3 SADP サービスの無効化

SADPサービスを無効にすると、信頼できないネットワーク環境にいる場合など、アクセスセキュリティを強化できます。

System → System Service → System Service に移動し、SADP の有効化をオフにしてサービスを無効にします。

第13章付録

13.1 適用可能な電力アダプター覧

以下に示す電源アダプタのみを使用してください。

電源アダプタモデル	仕様	製造業者	
MSA-C1500IC12.0-18P-DE	12 V, V, 1.5 A	0000201935 (株)モソテクノロ ジー	
ADS-25FSG-12 12018GPG	CE、100 ~ 240 VAC、12 V、 1.5 A、18 W、Φ5.5 × 2.1 × 10	0000200174 深セン名誉電子 (株)	
MSA-C1500IC12.0-18P-US	12 V, V, 1.5 A	0000201935 (株)モソテクノロ ジー	
TS-A018-120015AD	100 ~ 240 VAC, 12 V, 1.5 A, 18 W, Φ5.5 × 2.1 × 10	0000200878 深セントランスイ ンテクノロジーズ(株)	
MSA-C2000IC12.0-24P-DE	12 V, V, 2 A	0000201935 (株)モソテクノロ ジー	
ADS-24S-12 1224GPG	CE、100 ~ 240 VAC、12 V、 2 A、24 W、Φ2.1	0000200174 深セン名誉電子 (株)	
MSA-C2000IC12.0-24P-US	US, 12 V, 2 A	0000201935 (株)モソテクノロ ジー	
ADS-26FSG-12 12024EPCU	US, 12 V, 2 A	0000200174 深セン名誉電子 (株)	
KPL-040F-VI	12 V, V, 3.33 A, 40 W	0000203078 チャンネルウェ ルテクノロジー(株)	
MSA-Z3330IC12.0-48W-Q	12 V, V, 3.33 A	0000201935 (株)モソテクノロ ジー	
MSP-Z1360IC48.0-65W	48 V, V, 1.36 A	0000201935 (株)モソテクノロ ジー	
KPL-050S-II	48 V, V, 1.04 A	0000203078 チャンネルウェ ルテクノロジー(株)	

13.2 用語集

デュアルストリーム

デュアルストリームは、ネットワークを介して低解像度ストリームを送信しながら、高解像度ビデオをローカルに記録するために使用される技術である。2つのストリームはDVRによって生成され、主ストリームは1080Pの最大解像度を有し、サブストリームはCIFの最大解像度を有する。

DVR

Digital Video Recorderの略。DVR は、アナログカメラからのビデオ信号を受け取り、信号を圧縮してハードドライブに保存できるデバイスです。

HDD

Hard Disk Drive(ハードディスクドライブ)の略語。磁気表面を有するプラッター上にデジタル符号化されたデータを記憶する記憶媒体。

DHCP

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

HTTP

Hypertext Transfer Protocol の略。ネットワーク経由でサーバとブラウザ間でハイパーテキスト要求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、Ethernet フレーム内にPoint-to-Point Protocol (PPP)フレームをカプセル化するためのネットワークプロトコルです。これは、主に、個々のユーザがイーサネット経由でADSLトランシーバ(モデム)に接続するADSLサービスや、プレーンメトロイーサネットネットワークで使用されます。

DDNS

ダイナミックDNS は、インターネットプロトコルスイートを使用するルータやコンピュータシステムなどのネットワークデバイスが、設定されたホスト名、アドレス、またはDNS に保存されているその他の情報のアクティブなDNS 設定をリアルタイム(アドホック) で変更するようにドメインネームサーバに通知する機能を提供する方法、プロトコル、またはネットワークサービスです。

ハイブリッドDVR

ハイブリッドDVRは、DVRとNVRとの組み合わせである。

NTP

Network Time Protocolの略。ネットワーク上で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。

NTSC

National Television System Committeeの略。NTSCは、米国や日本などの国で使用されているアナログテレビ規格である。NTSC 信号の各フレームには、60Hz で525 本の走査線が含まれます。

NVR

ネットワークビデオレコーダーの頭文字。NVRは、IPカメラ、IPドーム、および他のDVRのための集中管理および記憶のために使用される、PCベースの、または組み込みシステムであり得る。

PAL

Phase Alternating Lineの略。PALはまた、世界の大部分の放送テレビシステムで使用されているもう一つのビデオ規格である。PAL 信号には50Hz で625 本の走査線が含まれています。

PTZ

Pan、Tilt、Zoomの略。PTZ カメラは、モーター駆動のシステムで、カメラを左右にパンしたり、上下に傾けたり、拡大/縮小したりすることができます。

USB

Universal Serial Bus(ユニバーサルシリアルバス)の略語。USB は、デバイスをホストコンピュータにインターフェイスするためのプラグアンドプレイシリアルバス規格です。

13.3 よくある質問

13.3.1 ライブビューのマルチ画面で「リソースなし」を表示したり、黒画面になったりするチャンネルがあるのはなぜですか?

理由

- 1. サブストリームの解像度やビットレートの設定が不適切です。
- 2. サブストリームの接続に失敗しました。

ソリューション

1. サブストリームの→に「カメラ→ビデオパラメータ」に移動します。チャンネルを選択し、解像度と最大ビットレート(解像度は720p以下、最大ビットレートは2048 Kbps以下)を下げます。

[i]注

ビデオレコーダがこの機能をサポートしていないと通知した場合は、カメラにログインし、Webブラウザを介してビデオパラメータを調整できます。

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

13.3.2 なぜ、ビデオレコーダはネットワークカメラを追加した後に、危険なパスワードを通知するのか?

理由

カメラのパスワードが弱すぎる。

ソリューション

カメラのパスワードを変更します。

警告

製品のセキュリティを高めるために、独自に選択した強力なパスワードを作成することを強くお勧めします(大文字、小文字、数字、特殊文字の3つ以上を含む8文字以上の使用)。また、高セキュリティシステムでは、特に毎月または毎週パスワードをリセットすることで、製品の保護を向上させることができるため、パスワードを定期的にリセットすることをお勧めします。

13.3.3 なぜ、ビデオレコーダがストリームタイプをサポートしていないこと を通知するのか。

理由

カメラのエンコードフォーマットがビデオレコーダーと不一致です。

ソリューション

カメラがエンコードにH.265/MJPEG を使用しているが、ビデオレコーダーがH.265/MJPEG 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変更してください。

13.3.4 再生画質を向上させるにはどうすればよいでしょうか。

理由

記録パラメータの設定が不適切です。

ソリューション

「カメラ→のビデオパラメータ」に移動します。解像度と最大ビットレートを上げ、もう一度試してください。

13.3.5 「NO VIDEO」をライブビューにオーバーレイしたアナログチャンネ

ルはなぜですか?

理由

- 1. ビデオ入力コネクタが緩んでいるため、ビデオ信号が弱くなっています。
- 2. ビデオ入力/出力標準の不一致。
- 3. 伝送距離が長すぎる。
- 4. ケーブルが損傷すると、ビデオ信号が弱くなります。
- 5. ビデオレコーダーのビデオ入力端子が壊れています。

ソリューション

- 1. コネクタがしっかりと接続されていることを確認します。
- 2. 「システム→全般」に移動します。出力規格が正しいことを確認します。
- 3. アナログカメラとビデオレコーダーの間の距離が制限を超えていないことを確認します。
- 4. ケーブルが損傷していないことを確認します。
- 5. 正常に動作している場合は、他のBNCコネクタを試してください。

13.3.6 ビデオレコーダーがH.265 を使ってビデオを録画していることを確認するには?

ソリューション

ライブビューツールバーのエンコーディングタイプがH.265であるかどうかを確認します。

13.3.7 再生時のタイムラインが一定でないのはなぜか?

理由

- 1. ビデオレコーダがイベント録画を使用している場合、イベントが発生したときにのみビデオを 録画します。したがって、ビデオは連続的でないことがある。
- 2. デバイスオフライン、HDDエラー、レコード例外、ネットワークカメラオフラインなどの例外が発生します。

ソリューション

- 1. 記録タイプが連続記録であることを確認します。
- 2. 保守→履歴情報に移動します。ビデオの時間帯にログファイルを検索します。HDD エラー、レコード例外などの予期しないイベントが発生していないかどうかを確認します。

13.3.8 ネットワークカメラを追加する場合、ビデオレコーダは、ネットワー

クに到達できないことを通知する。

理由

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

ソリューション

- 1. 「→カメラ」→「IPカメラ」に移動します。選択したカメラをクリックし、その IP アドレスとポートを 編集します。ビデオレコーダーとカメラが同じポートを使用していることを確認します。☑
- 2. 保守→網→検知に進む。「送信先アドレス」にネットワークカメラのIP アドレスを入力し、「テスト」をクリックしてネットワークに到達可能かどうかを確認します。

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

理由

ネットワークカメラとビデオレコーダが同じスイッチを使用しているが、サブネットが異なる場合、ビデオレコーダは、ネットワークカメラのIPアドレスをそれ自体と同じサブネットに変更する。

ソリューション

カメラを追加する場合は、「カスタム追加」をクリックしてカメラを追加します。

13.3.10 ビデオレコーダがIP競合を通知するのはなぜか?

理由

ビデオレコーダは、他の装置と同じIPアドレスを使用する。

ソリューション

ビデオレコーダーのIPアドレスを変更します。他のデバイスと同じでないことを確認します。

13.3.11 ビデオレコーダーがシングルカメラまたはマルチチャンネルカメラで再生されているときに、なぜ画像が動かなくなっているのか?

理由

HDD 読み取り/書き込み例外。

ソリューション

ビデオをエクスポートし、他のデバイスで再生します。他の機器で正常に再生された場合は、

HDDを交換してから再度操作してください。

13.3.12 ブート後、なぜ私のビデオレコーダーがビープ音を鳴らすのでしょうか?

理由

- 1. フロントパネルは固定されていません(フロントパネルが取り外し可能な装置の場合)。
- 2. HDDエラー、またはHDDがありません。

ソリューション

- 1. 連続的なビープ音が鳴り、装置のフロントパネルが取り外し可能な場合は、フロントパネルが 固定されていることを確認します。
- 2. 不連続なビープ音(長さ3、短さ2)が発生した場合は、HDDエラーを例にとり、HDDがインストールされているかどうかを確認してください。取り付けられていない場合は、システム→イベント正常イベント→例外に移動し、イベントヒント設定のチェックを外して、HDD エラーイベントヒントを無効にできます。

HDDが初期化されているか確認してください。そうでない場合は、「Storage」>「Storage Device」と選択して、HDDを初期化します。

HDDが破損していないか確認してください。それを変更して、もう一度試してみることができます。

13.3.13 モーション検出を設定した後、なぜ録画された映像がないのでしょうか?

理由

- 1. 録画予約が間違っています。
- 2. 動き検出イベントの設定が間違っています。
- 3. HDD 例外。

ソリューション

- 1. 録画スケジュールは、「録画/キャプチャスケジュールの設定」に記載されている手順に従って 正しく設定されます。
- 2. 動き検出領域は正しく構成されている。モーション検出のためにチャネルがトリガーされています(「モーション検出の設定」を参照)。
- 3. デバイスにHDDがインストールされているかどうかを確認します。
 HDDが初期化されているか確認してください。そうでない場合は、「Storage」>「Storage Device」と選択して、HDDを初期化します。
 - HDDが破損していないか確認してください。それを変更して、もう一度試してみることができます。

13.3.14 なぜ同軸トロンを介してPTZカメラを制御できないのでしょうか?

理由

- 1. カメラは同軸トロンに対応していません。
- 2. 同軸トロンのプロトコルが間違っている。
- 3. 信号はビデオ光トランシーバの影響を受けます。

ソリューション

- 1. ビデオ入力信号がHDTVIで、カメラが同軸トロンに対応していることを確認します。
- 2. ボーレートおよびアドレスなどのコアキシトロンプロトコルパラメータが正しいことを確認します。
- 3. ビデオ光トランシーバを取り外し、もう一度試してください。

13.3.15 なぜPTZはRS-485を介して応答しないように見えますか?

理由

- 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切断されています。
- 3. 制御プロトコルが正しくない。

ソリューション

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

13.3.16 なぜ映像を録画するのに音質が良くないのだろうか。

理由

- 1. 音声入力装置は、集音に効果がない。
- 2. 伝送の干渉。
- 3. オーディオパラメータが正しく設定されていません。

ソリューション

- 1. オーディオ入力デバイスが正常に動作しているかどうかを確認します。別のオーディオ入力 デバイスを変更して、もう一度やり直すことができます。
- 2. 音声伝送路を確認してください。すべてのラインが十分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ます。
- 3. 環境や音声入力機器に合わせて音量を調整します。