アイリスオーヤマ

ネットワークカメラ Sシリーズ

# 取扱説明書

本書は、アイリスオーヤマの所有物であり、事前にアイリスオーヤマに書面で承諾を得た場合を除き、いかなる場合によっても複製、変更、翻訳、または配布することはできません。アイリスオーヤマは、本書に明示的に記載されていない限り、本書に含まれる情報について、いかなる保証・補償・責任を負いません。

# 取扱説明書について

本書には、本機の使用および管理に関する説明が含まれています。写真・図表・画像およびその他の情報は、説明のための情報です。また、本書に記載されている情報は、ファームウェアのアップデートなどにより予告なく変更される場合があります。

このマニュアルは、製品のサポートについてトレーニングを受けた専門家のガイダンスとサポートとともに使用してください。

# 商標について

- IRIS OHYAMA の商標は、アイリスオーヤマのさまざまな管轄区域における所有物です。
- 記載されているその他の商標およびロゴは、それぞれの所有者の所有物です。
- **H⊇mi** HDMI、High-Definition Multimedia Interface、及び HDMI ロゴ は、米国 及びその他の国における HDMI Licensing Administrator, Inc. の商標または、 登録商標です。

# 法的免责事項

本書及び本製品(ハードウェア、ソフトウェア、ファームウェアを含む)は関連する法律によって許される最大限の範囲で「現状有姿」又は「瑕疵があってもそれらを含む状態」で提供されます。

アイリスオーヤマは、商品性(良好な品質、特定目的適合性を含むがこれらに限定されない)について、明示的にも黙示的にも保証いたしません。

本製品の使用については、お客様自身の責任に基づいて行ってください。

いかなる場合においてもアイリスオーヤマは、契約不履行・不法行為(過失を含む)・ 製造物責任などに基づくかを問わず、本製品の使用に関連して発生する特別損害・派生的損害・間接損害(これら損害には事業利益の損失、事業の中断、データの喪失、システムの破損、文書の喪失を含む)について、責任を負いません。

アイリスオーヤマに上記のような損害・喪失の可能性を通知されていたとしても同様に責任を負いません。

インターネットの性質上、内在する安全上のリスクが存在することを認識していただき、サイバーアタック・ハッカーによる攻撃・ウイルスの感染等に起因する異常な動作・個人情報の漏洩・その他の損害についてアイリスオーヤマは責任を負いません。しかしながらアイリスオーヤマは必要があれば技術的なサポートをタイムリーに提供いたします。

お客様は関連する法令を遵守して本製品を使用することに同意するものとし、お客様にはその使用態様について関連する法律に準拠することをお客様自身で確認する責任を負います。

特に、第三者の権利(パブリシティー権、知的財産権、データ保護、その他のプライバシー権を含むがこれらに限定されない)を侵害することのない方法で本製品を使用する責任を負います。

本製品を禁止された用途(大量破壊兵器・生物化学兵器の製造・開発、核爆発物または核燃料の不正な再利用に関するあらゆる活動、または人権侵害を支援する活動を含むがこれらに限られない)に使用しないものとします。

本書と関連する法令との間に矛盾がある場合は、法令が優先されます。

# 安全上のご注意

これらの指示は、危険や所有物の損失を防止し、製品を正しく使用できることを目的としています。

安全上の注意は「警告」と「注意」に分かれています。

警告: これらの警告を無視すると、重傷または死亡につながる可能性があります。

注意: これらの注意を無視すると、けがや装置の損傷を引き起こす可能性があります。





**警告**: 重傷または死亡を防ぐために、 指示に従ってください。 注意: 怪我や物的損害を防ぐため に、指示に従ってください。



#### 警告:

- 安全特別低電圧(SELV)規格に適合した電源アダプタを使用し、IEC60950-1 および制限電源規格に準拠した 12 V DC または 24 V AC (モデルにより異なる) の電源電圧で使用してください。
- 火災や感電の危険を避けるため、本機を雨や湿気にさらさないでください。
- ◆ 本機の設置は、資格のあるサービス業者が行い、地域のすべての規制に準拠している必要があります。
- カメラが天井に固定されている場合、固定している天井面の強度を確認してください。
- 製品が正常に動作しない場合は、販売店またはサポートコールにお問い合わせください。ご自分でカメラを分解しないでください。(無断の修理・メンテナンスによるトラブルについては、一切の責任を負いかねます。)



# 注意:

- カメラを使用する前に、電源電圧が正しいことを確認してください。
- カメラを落としたり衝撃を与えないでください。

- センサーモジュールを指で触らないでください。清掃が必要な場合は、薄めた中性洗剤を含ませた清潔な布で軽く拭いてください。そのあと、洗剤が残らないように水拭きしてください。カメラを長期間使用しないときは、センサーを汚さないようにレンズキャップを装着してください。
- カメラのレンズを太陽や白熱灯などの強い光に向けないでください。強いライトはカメラに致命的な損傷を与える恐れがあります。
- レーザー光によりセンサーが焼損する恐れがありますので、レーザー機器を使用する場合は、センサーの表面にレーザー光が当たらないようにしてください。
- カメラを高温、低温(作業温度については製品仕様をご確認ください)、ほこりや 湿気の多い環境に設置しないでください。また、高電磁放射にさらさないでくだ さい。
- 蓄熱による高温を避けるために、換気のよい環境に設置してください。
- ◆ 本機を水や液体がかかる場所には取り付けないでください。
- バッテリーを誤って使用または交換すると、爆発の危険があります。メーカーが 推奨するタイプのバッテリーを使用してください。

#### お知らせ:

IR(赤外線)に対応しているカメラでは、IR反射を防ぐために、次の点に注意してください。

- ドームカバーにほこりや油脂が付着すると、赤外線が反射します。取り付けが 終わるまでドームカバーフィルムをはがさないでください。ドームカバーにごみ やグリスが付着している場合は、清潔な柔らかい布でドームカバーを清掃してく ださい。
- 設置場所のすぐ近くに反射する物体がないことを確認してください。カメラからの赤外線がレンズに反射することがあります。

# 目次

第1章	動作環境	10
第2章	ネットワーク接続	11
2.1	LAN経由でのネットワークカメラの設定	11
2.1	.1 LAN 経由の配線	12
2.1	.2 カメラの起動	13
2.1	.3 セキュリティ質問の設定	17
2.2	WAN経由でのネットワークカメラの設定	17
2.2	2.1 固定IP 接続	17
2.2	2.2 動的IP 接続	18
第3章	ネットワークカメラにアクセス	21
3.1	Webブラウザによるアクセス	21
3.2	クライアントソフトウェアによるアクセス	22
第4章	Wi-Fi設定	24
4.1	管理モードおよびアドホックモードでのWi-Fi接続の設定	24
4.2	WPS機能付き簡単Wi−Fi接続	29
4.3	ワイヤレスネットワーク接続のIPプロパティ設定	
第5章	ライブビュー	34
5.1	ライブビューページ	34
5.2	ライブビューの開始	36
5.2	2.1 ライブ動作	36
5.2	2.2 プラグインのインストール	37
5.3	手動で録画/撮影する	38
5.4	クイックセットアップ	39
5.5	PTZ コントロールの操作	40
5.5	5.1 PTZ コントロールパネル	41
5.5	5.2 プリセットの設定/呼び出し	42
5.5	5.3 パトロールの設定/呼び出し	43
第6章	ネットワークカメラ設定	45
6.1	ローカルパラメータの設定	45
6.2	システム設定	47
6.2	2.1 基本情報の設定	47

# ネットワークカメラ Sシリーズ 取扱説明書

6.2.2 時間設定	48
6.2.3 RS232 設定	50
6.2.4 RS485 設定	51
6.2.5 DST 設定	52
6.2.6 外部デバイスの設定	53
6.2.7 VCA リソースの設定	
6.2.8 メタデータ設定	
6.2.9 オープンソース・ソフトウェア・ライセンス	56
6.3 メンテナンス	56
6.3.1 アップグレードとメンテナンス	
6.3.2 ログ	
6.3.3 システムサービス	
6.3.4 セキュリティ監査ログ	59
6.4 セキュリティ設定	61
6.4.1 認証	61
6.4.2 IPアドレスフィルタ	
6.4.3 セキュリティサービス	
6.4.4 高度なセキュリティ	64
6.5 ユーザー管理	65
6.5.1 ユーザー管理	65
6.5.2 セキュリティに関する質問	
6.5.3 オンラインユーザー	69
第7章 ネットワーク設定	70
7.1 基本設定	70
7.1.1 TCP/IP 設定	70
7.1.2 DDNS 設定	72
7.1.3 PPPoE 設定	74
7.1.4 ポート設定	75
7.1.5 NAT (ネットワークアドレス変換) 設定	76
7.1.6 マルチキャストの設定	78
7.2 詳細設定	79
7.2.1 SNMP設定	79
7.2.2 FTP 設定	81
7.2.3 Eメール設定の指定	84
7.2.4 プラットフォームアクセス	87
7.2.5 ワイヤレスダイヤル	87
7.2.6 HTTPS 設定	90
7.2.7 QoS 設定	94
7.2.8 802.1X の設定	95

	7.2.9	9 統合プロトコル	96
	7.2.1	10 帯域幅適応	97
		11 ネットワークサービス	
	7.2.1	12 スムーズなストリーミング	98
第	8章	ビデオ/オーディオ設定	100
	8.1	ビデオ設定	100
	8.1.1		
	8.1.2	2 カスタムビデオ	105
	8.2	オーディオ設定	106
	8.3	ROIエンコーディングの設定	108
	8.4	ストリーム上の情報表示	110
	8.5	ターゲットクロッピングの設定	110
第	9章	画像設定	111
	9.1	ディスプレイ設定	111
	9.2	OSD 設定	116
	9.3	プライバシーマスクの設定	117
	9.4	画像オーバーレイの設定	119
	9.5	画面切り換えパラメータの設定	120
第	10章	イベント設定	121
	10.1	基本イベント	121
	10.1	.1 モーション検出の設定	121
	10.1	.2 ビデオ改ざんアラームの設定	128
	10.1	.3 アラーム入力の設定	129
		.4 アラーム出力の設定	
		.5 例外アラームの設定	
		.6 アラームライト出力の点滅の設定	
		.7 音声アラーム出力の設定	
	10.1	.8 その他のアラームの設定	134
		スマートイベント	
		.1 オーディオ例外検出の設定	
		.2 デフォーカス検出の設定	
		.3 シーンチェンジ検出の設定	
	100	.4 顔検出の設定	142
	10.2	.5 侵入検知の設定	

10.2.7 領域進入検出の設定	149
10.2.8 領域退出検出の設定	151
10.2.9 無人手荷物検出の設定	154
10.2.10 オブジェクトの退出検知の設定	156
10.3 VCA 設定	158
10.3.1 挙動解析	158
10.3.2 フェイスキャプチャ	166
10.3.3 人数カウント	170
10.3.4 カウント	174
10.3.5 ヒートマップ	176
10.3.6 道路交通	178
10.3.7 キュー管理	179
第11章 ストレージ設定	183
11.1 レコードスケジュールの設定	183
11.2 キャプチャスケジュールの設定	187
11.3 ネットHDD の設定	189
11.4 メモリーカード検出	192
11.5 Liteストレージの設定	194
第12章 再生	195
第13章 ピクチャー	198
第14章 アプリケーション	200
14.1 フェイスキャプチャ統計	200
14.2 人数統計	201
14.3 ヒートマップ統計	201
14.4 カウント統計	203
14.5 キュー管理統計	203
14.5.1 キューイングアップ時間解析	204
14.5.2 キューステータス解析	205
14.5.3 元データ	206
14.6 オープンプラットフォーム	207
付録	210
付録1 SADP ソフトウェアの概要	210
付録2 ポートマッピング	213

# 第1章 動作環境

# オペレーティングシステム

Microsoft Windows 10、Mac OS X 10.8以降のバージョン

### **CPU**

Intel corei5以上

#### **RAM**

8GB以上

# ディスプレイ

1024×768 解像度以上

# Webブラウザ

# プラグインフリーライブビュー対応のカメラの場合

〈Windowsの場合〉

Internet Explorer 8.0以降のバージョン、Mozilla Firefox 30.0以降

およびGoogle Chrome 31.0以降のバージョン

〈MACの場合〉

Apple Safari 16.0以降のバージョン、Mozilla Firefox 52.0以降

およびGoogle Chrome 57.0以降のバージョン

# お知らせ:

Google Chrome 57 以降またはMozilla Firefox 52 以降のプラグインフリーバージョンでは、「ピクチャー」および「プレイバック」機能は非表示になります。

Webブラウザで上記機能を使用する場合は、下位バージョンに変更するか、またはInternet Explorer 8.0以降に変更します。

# プラグインフリーライブビューに対応していないカメラの場合

〈Windowsの場合〉

Internet Explorer 8.0以降のバージョン、Mozilla Firefox 30.0以降

およびGoogle Chrome 31.0以降のバージョン

〈MACの場合〉

Apple Safari 16.0以降のバージョン、Mozilla Firefox 52.0以降

およびGoogle Chrome 57.0以降のバージョン

# 第2章 ネットワーク接続

## お知らせ:

- インターネットアクセスを伴う本機の使用には、ネットワークセキュリティリスクの下にある可能性があります。ネットワーク攻撃や情報漏洩を回避するために、お客様のセキュリティ対策を強化してください。正常に動作しない場合は、お買い上げの販売店またはサポートコールにご連絡ください。
- ネットワークカメラのネットワークセキュリティを確保するために、ネットワークカメラの評価とメンテナンスを確実に行うことを推奨します。このようなサービスが必要な場合は、弊社までご連絡ください。

# 準備:

- LAN (Local Area Network)経由でネットワークカメラを設定する場合は、「2.1 LAN 経由でのネットワークカメラの設定」を参照してください。
- WAN (Wide Area Network) 経由でネットワークカメラを設定する場合は、「2.2 WAN 経由でのネットワークカメラの設定」を参照してください。

# 2.1 LAN経由でのネットワークカメラの設定

#### 目的:

LAN 経由でカメラを表示および設定するには、同じサブネット内のネットワークカメラをコンピュータと接続し、ネットワークカメラのIP を検索および変更するため ICSADP またはiVMS-4200 ソフトウェアをインストールする必要があります。

お知らせ: SADPの詳細な導入については、付録1を参照してください。

# 2.1.1 LAN 経由の配線

ネットワークカメラとパソコンのケーブル接続の2つの方法を下図に示します:

# 目的:

- ネットワークカメラをテストするには、図 2-1 のようにネットワークケーブルでネットワークカメラとコンピュータを直接接続します。
- 図2-2 を参照して、スイッチまたはルーターを介してLAN 経由でネットワークカメラを 設定します。

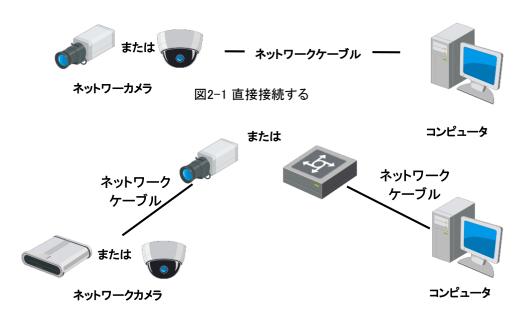


図2-2 スイッチまたはルーター経由の接続

# 2.1.2 カメラの起動

カメラを使用する前に、まずカメラに安全性の高いパスワードを設定してカメラを有効にする必要があります。

Webブラウザによる起動、SADPによる起動、クライアントソフトウェアによる起動 すべてサポートされています。

# ❖ Webブラウザによる起動

### 手順:

- 1. カメラの電源を入れ、ネットワークに接続します。
- 2. WebブラウザのアドレスバーにIPアドレスを入力し、クリックしてアクティベーション画面を入力します。

# お知らせ:

- カメラのデフォルトIP アドレスは192.168.1.64 です。
- コンピュータとカメラは同じサブネットに属している必要があります。
- カメラのデフォルトでDHCP を有効にするには、SADP ソフトウェアを使用してIP アドレスを検索する必要があります。

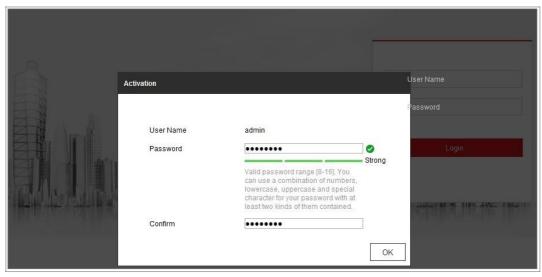


図2-3 Web ブラウザによる起動

3. パスワードを作成し、パスワードフィールドに入力します。 ユーザー名を含むパスワードは許可されません。



# 強力なパスワードを推奨

製品のセキュリティを強化するために、独自に強力なパスワードを作成することを強く推奨します(大文字、小文字、数字、特殊文字のカテゴリを少なくとも3つ含む8 文字以上を使用)。

また、パスワードを定期的に変更することを推奨します。特に高セキュリティシステムでは、パスワードを月単位または週単位で変更すると製品のセキュリティが向上します。

- 4. パスワードを確認します。
- 5. 「OK」をクリックしてパスワードを保存し、ライブビュー画面に入ります。
- ❖ SADPソフトウェアによる起動

SADPソフトウェアは、オンラインデバイスの検出、カメラの起動、パスワードの変更に使用します。

公式ウェブサイトから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。カメラを起動する手順に従います。

# 手順:

1. SADP ソフトウェアを実行して、オンラインデバイスを検索します。

2. デバイス一覧からデバイスの状態を確認し、停止中のデバイスを選択します。

図2-4 SADP画面

# お知らせ:

SADPソフトウェアは、カメラの一括起動をサポートします。

3. パスワードフィールドにパスワードを作成して入力し、パスワードを確認します。ユーザー名を含むパスワードは許可されません。



# 強力なパスワードを推奨

製品のセキュリティを強化するために、独自に強力なパスワードを作成することを強く推奨します(大文字、小文字、数字、特殊文字のカテゴリを少なくとも3つ含む8 文字以上を使用)。

また、パスワードを定期的に変更することを推奨します。特に高セキュリティシステムでは、パスワードを月単位または週単位で変更すると製品のセキュリティが向上します。

4. 「Active」をクリックして起動を開始します。

起動が完了したかどうかは、ポップアップウィンドウで確認できます。

有効化に失敗した場合は、パスワードが要件を満たしていることを確認してから、 もう一度試してください。 5. IP アドレスを手動で変更するか、「Enable DHCP」チェックボックスをオンにし、デバイスのIP アドレスをコンピュータと同じサブネットに変更します。



図2-5 IP アドレスの変更

6. 「Admin Password」を入力し、「Modify」をクリックしてIP アドレスの変更を有効にします。

バッチIP アドレスの変更は、SADP でサポートされています。

# 2.1.3 セキュリティ質問の設定

管理者ユーザーがパスワードを忘れた場合、セキュリティ質問を使用して管理者パスワードを変更します。

管理者ユーザーはポップアップウィンドウに従い、カメラのアクティベーション中にセキュリティ質問を設定できます。または、管理者ユーザーは「User Management」に移動して設定できます。

# 2.2 WAN経由でのネットワークカメラの設定

### 目的:

ここのセクションでは、ネットワークカメラを固定IP または変動IP を使用してWAN に接続する方法について説明します。

# 2.2.1 固定IP 接続

# 準備:

ISP (Internet Service Provider) から固定IP を適用してください。固定IP アドレスを使用すると、ネットワークカメラをルーター経由で接続したり、WAN に直接接続したりできます。

● ルーター経由でネットワークカメラを接続する

# 手順:

- 1. ネットワークカメラをルーターに接続します。
- 2. LAN IP アドレス、サブネットマスク、およびゲートウェイを割り当てます。ネットワークカメラのIPアドレス設定の詳細は、「2.1.2 カメラの起動」を参照してください。
- 3. ルーターに固定IP を保存します。

4. ポートマッピング(80、8000、554ポートなど)を設定します。ポートマッピング の手順は、ルーターによって異なります。ポートマッピングのサポートについ ては、ルーターの製造元にお問い合わせください。

**お知らせ:** ポートマッピングの詳細については、付録2 を参照してください。

5. Webブラウザまたはインターネット上のクライアントソフトウェアを介して、ネットワークカメラにアクセスします。



図2-6 固定IPルーターを経由したカメラへのアクセス

# ● 固定IP でネットワークカメラを直接接続する

また、固定IP をカメラに保存し、ルーターを使用せずに直接インターネットに接続することもできます。ネットワークカメラのIPアドレス設定の詳細は、「2.1.2 カメラの起動」を参照してください。



図2-7 固定IP を使用したカメラへの直接アクセス

# 2.2.2 動的IP 接続

### 準備:

ISP から動的IP を適用してください。ダイナミックIPアドレスを使用して、ネットワークカメラをモデムまたはルーターに接続できます。

# ● ルーター経由のネットワークカメラの接続

# 手順:

ネットワークカメラをルーターに接続します。カメラで、LAN IP アドレス、サブネット マスク、ゲートウェイを割り当てます。ネットワークカメラのIPアドレス設定の詳細 は、「2.1.2 カメラの起動」を参照してください。

- 1. ルーターで、PPPoE ユーザー名、パスワードを設定し、パスワードを確認します。
- 2. ポートマッピングを設定します。例:80、8000、554ポート。ポートマッピングの手順は、ルーターによって異なります。

ポートマッピングのサポートについては、ルーターの製造元にお問い合わせください。

**お知らせ:** ポートマッピングの詳細については、付録2 を参照してください。

- 3. ドメインネームプロバイダからドメイン名を適用します。
- 4. ルーターの設定画面でDDNS を設定します。
- 5. 適用したドメイン名を介してカメラを接続します。

# ● モデム経由でネットワークカメラを接続する

### 目的:

本機はPPPoEオートダイヤルアップ機能に対応しています。カメラは、モデムに接続された後、ADSLダイヤルアップによってパブリックIPアドレスを取得します。ネットワークカメラのPPPoE パラメータを設定する必要があります。詳しい設定については、「7.1.3 PPPoE 設定」を参照ください。



図2-8 動的IP を使用したカメラへのアクセス

お知らせ: 取得したIP アドレスはPPPoE経由で動的に割り当てられるため、カメラの再起動後は必ずIP アドレスが変更されます。動的IPの不便さを解決するには、DDNS プロバイダ(例: DynDns.com) からドメイン名を取得する必要があります。通常のドメイン名の解像度とプライベートドメイン名の解像度については、以下の手順に従って問題を解決してください。

◆ 通常のドメイン名の解像度



図2-9 通常のドメイン名の解像度

# 手順:

- 2 ドメインネームプロバイダからドメイン名を適用します。
- 3 ネットワークカメラのDDNS設定画面でDDNS設定を設定します。詳細については、「7.1.2 DDNS設定」を参照してください。
- 2 適用したドメイン名を介してカメラを接続します。

# 第3章 ネットワークカメラにアクセス

# 3.1 Webブラウザによるアクセス

# お知らせ:

特定のカメラモデルでは、HTTPS がデフォルトで有効になっており、カメラは署名されていない証明書を自動的に作成します。カメラに初めてアクセスすると、Webブラウザは証明書の発行に関する通知を促します。

通知をキャンセルするには、署名付き証明書をカメラにインストールしてください。 詳しい操作については、「7.2.6 HTTPS 設定」を参照してください。

# 手順:

- 1. Webブラウザを開きます。
- 2. ブラウザアドレスバーで、ネットワークカメラのIPアドレスを入力し、Enterキーを押してログイン画面を入力します。

#### お知らせ:

デフォルトの IP アドレスは 192.168.1.64 です。IP アドレスは、お使いのコンピュータと同じサブネットに変更することを推奨します。

3. ユーザー名とパスワードを入力し、ログインをクリックします。

管理者ユーザーは、デバイスアカウントとユーザー/オペレーター権限を適切に設定する必要があります。不要なアカウントとユーザー/オペレーターの権限を削除します。

# お知らせ:

管理者がユーザー名/パスワードの入力を7回(オペレーター/ユーザーの場合は5回)失敗すると、IP アドレスからのログインが拒否されます。



図3-1 ログイン画面

- 4. 「Login」をクリックします。
- 5. ライブビデオを見てカメラを操作する前に、プラグインをインストールします。インストール・プロンプトに従って、プラグインをインストールします。

### お知らせ:

プラグインフリーライブビューに対応しているカメラの場合、Google Chrome 45 以上のバージョン、またはMozilla Firefox 52以上のバージョンを使用している場合は、プラグインのインストールは不要です。ただし、ピクチャー機能、プレイバック機能は非表示になります。Webブラウザで上記機能を使用する場合は、下位バージョンへの変更、またはInternet Explorer 8.0以降への変更を行います。

# 3.2 クライアントソフトウェアによるアクセス

製品CD には、iVMS-4200 クライアントソフトウェアが含まれています。ライブビデオを閲覧したり、ソフトウェアでカメラを管理したりすることができます。

インストールの指示に従って、ソフトウェアをインストールします。以下は、iVMS-4200クライアントソフトウェアのコントロールパネルとライブビュー画面です。

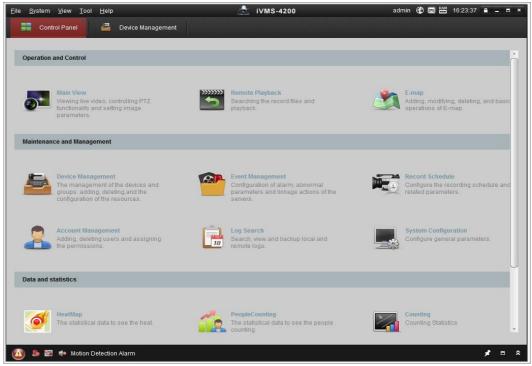


図3-2 iVMS-4200 コントロールパネル

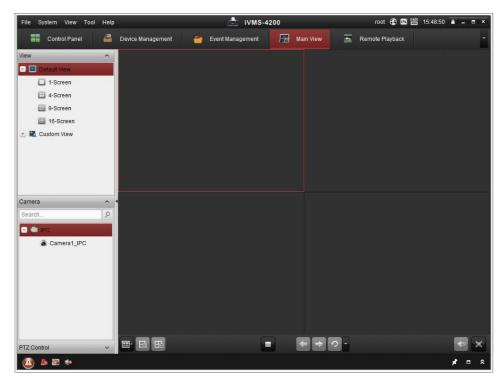


図3-3 iVMS-4200 のメインビュー

# 第4章 Wi-Fi設定

# 目的:

ワイヤレスネットワークに接続することで、ネットワーク接続にケーブルを使用する 必要がなくなり、実際の監視アプリケーションに非常に便利です。

**お知らせ**: この章は、内蔵Wi-Fi モジュールを搭載したカメラにのみ適用されます。

# 4.1 管理モードおよびアドホックモードでのWi-Fi接続 の設定

# 目的:

本機は2つの接続モードに対応しています。モードを選択し、Wi-Fi を設定する手順を実行してください。

# 管理モードでのワイヤレス接続

# 手順:

- 1. 「Configuration」 > 「Network」 > 「Advanced Settings」 > 「Wi-Fi」を選択します。
- 2. 「Search」をクリックして、オンラインのワイヤレス接続を検索します。

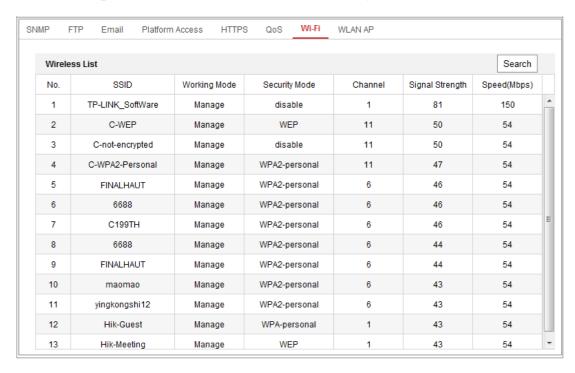


図4-1 Wi-Fi リスト

3. リストでワイヤレス接続をクリックして選択します。

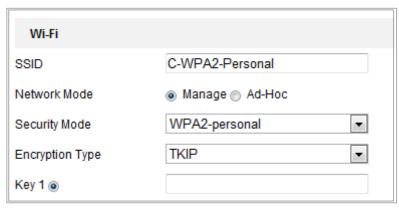


図4-2 Wi-Fi 設定管理モード

- 4. ラジオボタンをチェックして「Network Mode」を「Manage」として選択します。ワイヤレスネットワークを選択すると、ネットワークのセキュリティモードが自動的に表示されます。手動で変更しないでください。 *お知らせ*: これらのパラメータは、ルーターのパラメータとまったく同じです。
- 5. キーを入力してワイヤレスネットワークに接続します。キーは、ルーター に設定したワイヤレスネットワーク接続のキーにする必要があります。

# アドホックモードでの無線接続

アドホックモードを選択した場合は、ルーターを介してワイヤレスカメラを接続する必要はありません。シナリオは、カメラとPCを直接ネットワークケーブルで接続した場合と同じです。

#### 手順:

1. アドホックモードを選択します。

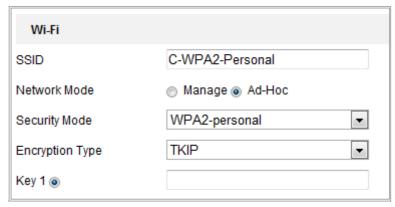


図4-3 Wi-Fi 設定アドホック

- 2 カメラのSSID をカスタマイズします。
- 3. ワイヤレス接続のセキュリティモードを選択します。
- 4. パソコンの無線接続機能を有効にしてください。
- 5. PC 側でネットワークを検索すると、表示されているカメラのSSID が確認できます。



図4-4 アドホック接続ポイント

6. SSID を選択して接続します。

# セキュリティモードの説明:

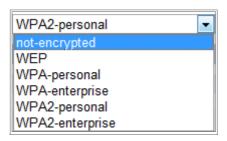


図4-5 セキュリティモード

セキュリティモードは、非暗号化、WEP、WPA-personal、WPA-enterprise、WPA2-personal、およびWPA2-enterprise から選択できます。

### WEPモード:

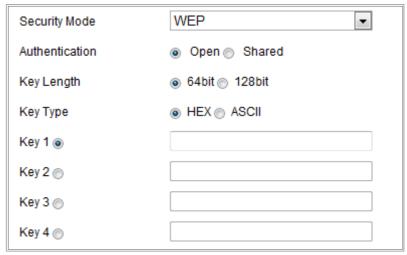


図4-6 WEP モード

- 「Authentication」-アクセスポイントで使用する方式に応じて、「Open」または「Shared」を選択します。すべてのアクセスポイントにこのオプションがあるわけではありません。その場合は、オープンシステムを使用します。これはSSID 認証と呼ばれることもあります。
- 「Key length」- ワイヤレス暗号化に使用されるキーの長さを設定します(64 ビットまたは 128 ビット)。暗号化キーの長さは、40/64 および104/128 と表示されることがあります。
- 「Key Type」-使用可能なキーの種類は、使用するアクセスポイントによって 異なります。以下のオプションがあります:

HEX - 16 進数キーを手動で入力できます。

ASCII -このメソッドでは、文字列は64 ビットWEP の場合は5 文字、128 ビットWEP の場合は13 文字である必要があります。

WPA パーソナルおよび WPA2 パーソナルモード:

アクセスポイントに必要な事前共有キーを16 進数またはパスフレーズで入力します。

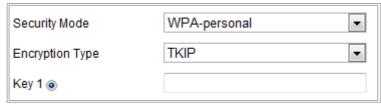


図4-7 セキュリティモードWPA パーソナル

WPA エンタープライズおよびWPA2 エンタープライズモード:

アクセスポイントで使用されているクライアント/サーバー認証のタイプ(EAP-TLS またはEAP-PEAP)を選択します。

EAP-TLS



図4-8 EAP-TLS

- 「Identity」 ネットワークに提示するユーザーID を入力します。
- 「Private key password」 ユーザーID のパスワードを入力します。
- 「EAPOL version」-アクセスポイントで使用するバージョン(1または2)を選択します。
- 「CA Certificates」 認証のためにアクセスポイントに提示するCA 証明書をアップロードします。

#### EAP-PEAP:

- 「User Name」 ネットワークに表示するユーザー名を入力します。
- 「Password」 ネットワークのパスワードを入力します。
- 「PEAP version」- アクセスポイントで使用するPEAP バージョンを選択します。
- 「Label」-アクセスポイントが使用するラベルを選択します。
- 「EAPOL version」-アクセスポイントで使用するバージョンに応じて、バージョン(1または2)を選択します。
- 「CA Certificates」 認証のためにアクセスポイントに提示するCA 証明書をアップロードします。



● プライバシーを守り、セキュリティリスクからシステムを保護するために、すべて の機能およびネットワークデバイスに強力なパスワードを使用することを強く推 奨します。パスワードは、製品のセキュリティを強化するために、8 文字以上 (大文字、小文字、数字、特殊文字の3つ以上を含む)に設定してください。

# 4.2 WPS機能付き簡単Wi-Fi接続

### 目的:

ワイヤレスネットワーク接続の設定は簡単ではありません。ワイヤレス接続の複雑な設定を回避するには、WPS 機能を有効にします。

WPS (Wi-Fi Protected Setup)とは、デバイスとワイヤレスルータ間の暗号化された接続を簡単に設定する手法です。WPSを使用すると、長いパスフレーズを入力することなく、既存のネットワークに新しいデバイスを簡単に追加できます。WPS接続には、PBCモードとPINモードの2つのモードがあります。

**お知らせ:** WPS 機能を有効にすると、暗号化タイプなどのパラメータを設定する必要がなく、ワイヤレス接続のキーを知る必要もありません。

# 手順:

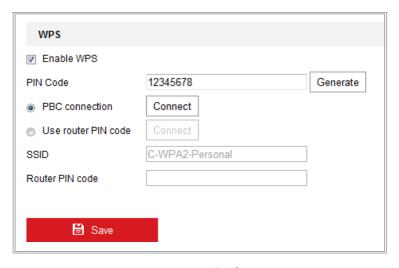


図4-9 Wi-Fi 設定- WPS

### PBCモード:

PBC とは、アクセスポイント(およびネットワークのレジストラ)と新しいワイヤレスクライアントデバイスの両方で、実際のボタンまたは仮想ボタン(IE ブラウザの設定画面上の Connect ボタンとして)を押す必要があるプッシュボタン設定のことです。

- 2. 接続モードをPBC として選択します。



*お知らせ:* このモードのサポートは、アクセスポイントと接続デバイスの両方で必須です。

3. Wi-Fi ルーターにWPS ボタンがあるかどうかを確認します。WPS ボタンがある場合、ボタンを押してください。ボタンの近くのインジケータが点滅し、ルーターのWPS機能が有効になります。詳しい操作方法については、ルーターの取扱説明書を参照してください。

- 4. カメラのWPSボタンを押して、カメラの機能を有効にします。 カメラにWPSボタンがない場合は、仮想ボタンをクリックして、Web画面の PBC機能を有効にすることもできます。
- 接続ボタンをクリックします。
   ルーターとカメラの両方でPBCモードが有効になると、カメラとワイヤレスネットワークが自動的に接続されます。

#### PINモード:

PIN モードでは、新しいワイヤレスデバイスのステッカーまたはディスプレイから 個人識別番号(PIN)を読み取る必要があります。その後、このPIN を入力してネットワーク(通常はネットワークのアクセスポイント)に接続する必要があります。

# 手順:

- 1. リストでワイヤレス接続を選択すると、SSID が自動的にロードされます。
- 2. 「Use route PIN code 」を選択します。

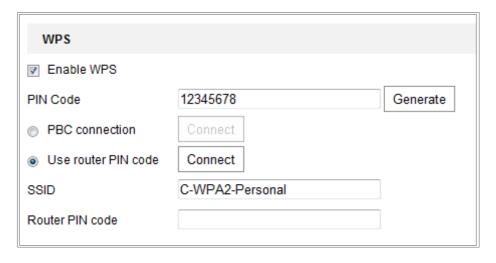


図4-10 PIN コードの使用

ルーター側からPINコードが生成された場合は、ルーター側から取得した PINコードを「Router PIN code」フィールドに入力する必要があります。 3. 「Connect」をクリックします。

### または

カメラ側でPINコードを生成できます。また、PINコードの有効期限は120秒です。

1. 「Generate」をクリックします。



2. この例では、ルーターにコードを入力し、ルーターに48167581 を入力します。

# 4.3 ワイヤレスネットワーク接続のIPプロパティ設定

ワイヤレスネットワーク画面コントローラのデフォルトIPアドレスは192.168.1.64です。 ワイヤレスネットワークに接続すると、デフォルトIP を変更できます。

# 手順:

- 1. 「Configuration」 > 「Network」 > 「Basic Settings」 > 「TCP/IP」を選択します。
- 2. 「WLAN」タブを選択します。

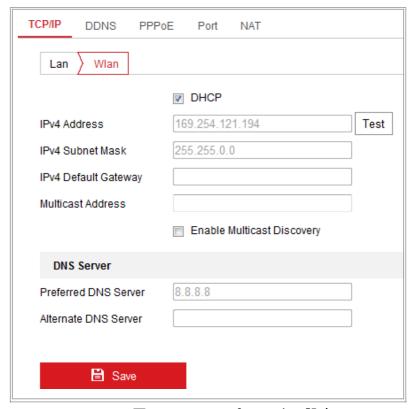


図 4-11 WLAN パラメータの設定

3. IPv4 アドレス、IPv4 サブネットマスク、およびデフォルトゲートウェイをカスタマイズします。設定手順はLAN と同じです。

IP アドレスを割り当てる場合は、チェックボックスをオンにしてDHCP を有効にします。

# 第5章 ライブビュー

# 5.1 ライブビューページ

# 目的:

ライブビューページでは、リアルタイムビデオの表示、画像のキャプチャ、PTZ 制御の実現、プリセットの設定/コール、ビデオパラメータの設定を行うことができます。 ネットワークカメラにログインしてライブビューページを開くか、メインページのメニューバーにあるライブビューをクリックしてライブビューページを開きます。

# ライブビューページの説明:



図5-1 ライブビューページ

### メニューバー:

各タブをクリックして、ライブビュー、再生、画像、アプリケーション、設定ページをそれぞれ開きます。

# ライブビューウィンドウ:

ライブビデオを表示します。

### ツールバー:

ツールバーでは、ライブビューウィンドウのサイズ、ストリームの種類、およびプラ グインを調節できます。また、ライブビューページでの操作を処理することができ ます。例えば、ライブビューの開始/停止、キャプチャ、録画、オーディオのオン/ オフ、双方向オーディオ、デジタルズームの開始/停止などです。

IE (Internet Explorer)ユーザの場合、ウェブコンポーネントとしてのプラグインおよびクイックタイムが選択可能です。また、非IEユーザーの場合、ウェブコンポーネント、クイックタイム、VLC、またはMJPEGは、それらがウェブブラウザによってサポートされている場合、選択可能です。

## お知らせ:

プラグインフリーライブビューに対応しているカメラの場合、Google Chrome 57以上のバージョン、またはMozilla Firefox 52以上のバージョンを使用しているときは、プラグインのインストールは必要ありません。ただし、ピクチャー機能、プレイバック機能は非表示になります。Webブラウザで上記機能を使用する場合は、下位バージョンへの変更、またはInternet Explorer 8.0以上のバージョンへの変更を行います。

# PTZコントロールパネル:

カメラのパン、チルト、ズーム操作を行います。ライトとワイパーを制御します(PTZ 機能をサポートするカメラでのみ使用できます)。

# プリセット/パトロール設定:

PTZ カメラのプリセットまたはパトロールを設定/呼び出し/削除します。

# 5.2 ライブビューの開始

# 5.2.1 ライブ動作

図 5-1 のようなライブビューウィンドウで、ツールバーの ▶ をクリックしてカメラ のライブビューを開始します。

■ - t<sub>0</sub> - 0 - 0 - 0 - 1. ► 10 1 • 0 • 1.

図5-2 ライブビューツールバー

*お知らせ:* アイコンは、モデルによって異なります。 表5-1 ツールバーの説明

アイコン	説明
▶/■	ライブビューの開始/停止。
4:3	4:3 ウィンドウサイズ。
16:9	16:9 ウィンドウサイズ。
IX	オリジナルのウィンドウサイズ。
	自己適応ウィンドウサイズ。
	オリジナルレシオのウィンドウサイズ。
	さまざまなビデオストリームを使用したライブビュー。
រ៉ៃក្លុំ រ៉ៃក្លុំ	対応するビデオストリームは、モデルによって異なります。
to <sub>0</sub>	10 ストリームをサポートするカメラモデルの場合は、「Video
等	/Audio」>「Custom」を選択してストリームを追加します。
	サードパーティ製プラグインをクリックして選択します。
0	写真を手動で撮影します。
<b>/</b>	手動で録画を開始/停止します。
<b>◆</b> ) ▼ / <b>◆</b>	オーディオをオンにして、音量/ミュートを調整します。
<b>⅓</b> / <b>⅓</b>	マイクのオン/オフを切り替えます。
<b>Q</b> / <b>Q</b>	デジタルズーム機能を開始/停止します。
'L]. /'L].	ピクセルカウンタの開始/停止
	クリックすると、カメラで撮影した画像が表示されます。
<u> </u>	<i>お知らせ:</i> この機能は、フェイスキャプチャをサポートする特定の
	カメラモデルでのみ使用できます。

### ピクセルカウンタ:

### 手順:

- 1. 「Start Pixel Counter」をクリックして機能を有効にします。
- 2. 画像上でマウスをドラッグして、目的の領域を選択します。ウェブの下部に幅 ピクセルと高さピクセルが表示されます。
- 3. 機能を停止するには、もう一度ボタンをクリックします。

### お知らせ:

ピクセルカウンタはメインストリームの下でのみサポートされ、1つの長方形のみが サポートされます。

### フルスクリーンモード:

ライブビデオをダブルクリックすると、現在のライブビューをフルスクリーンに切り替えたり、フルスクリーンから通常モードに戻ったりできます。

### 5.2.2 プラグインのインストール

操作システムやウェブブラウザによっては、カメラ機能の表示や動作が制限される場合があります。通常の表示と動作を確保するには、プラグインをインストールするか、特定の設定を完了する必要があります。

運用体制	Webブラウザ	動作
Windows	● Internet Explorer 8+ ● Google Chrome 57以前のバージョン ● Mozilla Firefox 52以前のバージョン	ポップアッププロンプトに従っ て、プラグインのインストールを 完了します。
	<ul><li>Google Chrome 31+</li><li>Mozilla Firefox 30+</li></ul>	♣ Download Plug-in をクリックしてプラ グインをダウンロードし、インスト ールします。
Mac OS	<ul> <li>Google Chrome 57+</li> <li>Mozilla Firefox 52+</li> <li>Apple Safari 16+</li> </ul>	● プラグインインストールは不要です。 通常のライブビューを表示するには、「WebSocket」または「WebSockets」を有効にします(「Configuration」〉「Network」〉「Advanced Settings」〉「Network Service」)。 一部の機能の表示・操作に制限があります。たとえば、「Playback」や「Picture」は使用できません。制限機能の詳細については、実機を参照してください。

### お知らせ:

このカメラはWindowsおよびMac OSシステムのみをサポートし、Linuxシステムはサポートしていません。

# 5.3 手動で録画/撮影する

ライブビュー画面で、ツールバーの 🔯 をクリックしてライブピクチャを

撮影するか、 **▲** をクリックしてライブビューを録画します。撮影した画像やクリップの保存経路は、「Configuration」>「Local」画面で設定できます。リモートスケジュール録画を設定するには、「6.1 ローカルパラメータの設定」を参照してください。

*お知らせ:*撮影した画像は、パソコンにJPEGファイルまたはBMPファイルとして保存されます。

### 5.4 クイックセットアップ

ライブビューページで画像/ビデオ関連のパラメータを素早くセットアップできます。 *手順:* 

- ライブビューウィンドウの右側にある をクリックすると、PTZコントロールパネルが表示されます。
   をクリックすると非表示になります。
- 2. PTZ、ディスプレイ、OSD、ビデオ/オーディオ、およびVCA リソースパラメータを指定します。詳細設定については、「Configuration」 > 「Image and Configuration」 > 「Video/Audio」を選択します。

### 「Display Settings」

- 「Scene」: 実際の設置環境に合わせてシーンを選択します。(特定のカメラモデルのみをサポートします。)
- 「WDR」: WDR (ワイドダイナミックレンジ)機能は、逆光の状況でもカメ ラが鮮明な画像を提供するのに役立ちます。視野内に非常に明るい 領域と非常に暗い領域の両方が同時に存在する場合、WDRは画像 全体の明るさレベルを調節し、細部まで鮮明な画像を提供します。 WDR 機能を有効または無効にしたり、レベルを設定したりできます。
- 「HLC」: ハイライト補正により、カメラは通常シーン全体でフレアになる強い光源を識別して抑制します。これにより、通常隠れてしまうようなイメージの細部を確認することができます。

### FOSD (On Screen Display) ↓

画面に表示する文字情報を設定します。配置調整は、テキストオーバー レイで使用できます。設定後に設定を保存します。

#### ∇ideo/Audio I

解像度と最大ビットレートは調整可能です。 **は は** をクリックしてストリームを変更します。

### ● 「VCA Resource」

VCAリソース は、特定のVCA 機能を有効にし、他の機能を隠すオプションを提供します。必要な機能により多くのリソースを割り当てるのに役立ちます。VCA リソースを設定した後は、再起動が必要です。

### お知らせ:

- VCAリソース機能は、モデルによって異なります。
- VCAオプションは相互に排他的です。
- サポートされる機能は、モデルによって異なります。

## 5.5 PTZ コントロールの操作

#### 目的:

ライブビュー画面では、PTZコントロールボタンを使用して、カメラのパン/チルト/ズームコントロールを実現できます。

*お知らせ:* PTZ 制御を実現するには、ネットワークに接続されたカメラがPTZ 機能をサポートするか、カメラにパン/チルトユニットを取り付ける必要があります。「6.2.4 RS-485の設定」を参照し、RS485設定画面からPTZパラメータを適切に設定してください。

### 5.5.1 PTZ コントロールパネル

ライブビューページで、ライブビューウィンドウの右側の横にある ► をクリックしてPTZコントロールパネルを表示します。 ► をクリックすると非表示になります。 方向ボタンをクリックして、パン/チルトの動きをコントロールします。



図5-3 PTZコントロールパネル

ズーム/フォーカス/アイリスボタンをクリックして、レンズコントロールします。

### お知らせ:

操作パネルには、8つの方向矢印(△、▽、▽、▽、▽、▽、▽、△、△)があります。矢印をクリックすると、相対位置での調整をします。

● レンズの動きだけに対応しているカメラの場合、方向ボタンは無効です。表5-2 PTZ コントロールパネルの説明

アイコン	説明
α α	拡大/縮小
7	遠近フォーカス
0	アイリス+/-
4	PTZ速度調整
· <b>.</b>	ライトのオン/オフ
•	ワイパーのオン/オフ
3:0	補助焦点
<b>9</b>	レンズ初期化
≡	パン/チルト動作の速度を調整する
[9]	手動トラッキング開始
30	3D ズームの開始

### 5.5.2 プリセットの設定/呼び出し

- プリセットの設定:
- 1. PTZコントロールパネルで、プリセットリストからプリセット番号を選択します。



図5-4 プリセットの設定

- 2. PTZコントロールボタンを使用して、レンズを希望の位置に移動します。
  - カメラを右または左にパンします。
  - カメラを上下に傾けます。

- ズームインまたはズームアウトします。
- レンズに焦点を当てます。
- をクリックすると、現在のプリセットの設定が終了します。
- 4. 🧝 をクリックすると、プリセットを削除できます。
- プリセットの呼び出し:

この機能を使用すると、カメラは手動で、またはイベントが発生したときに、指定したプリセットシーンを指すことができます。

定義したプリセットは、いつでも任意のプリセットシーンに呼び出すことができます。 PTZコントロールパネルで、リストから定義済みのプリセットを選択し、<sup>™</sup>をクリックしてプリセットを呼び出します。

または、プリセット画面にマウスを置き、プリセット番号を入力してプリセットを呼び出して、対応するプリセットを呼び出すこともできます。



図5-5 プリセットの呼び出し

### 5.5.3 パトロールの設定/呼び出し

#### お知らせ:

パトロールを設定する前に、2つ以上のプリセットを設定する必要があります。

### 手順:

- 1. 2 をクリックして、パトロール設定を起動します。
- 2. パス番号を選択し、 
  をクリックして設定済みのプリセットを追加します。

- 3. プリセットを選択し、パトロール継続時間とパトロール速度を入力します。
- 4. 「OK」をクリックして、最初のプリセットを保存します。
- 5. 上記の手順に従って、他のプリセットを追加します。



図5-6 パトロールパスの追加

- 6. 「OK」をクリックしてパトロールを保存します。
- 7. ▶ をクリックするとパトロールを開始し、 をクリックすると停止します。
- 8. ×をクリックして、パトロールを削除します。

# 第6章 ネットワークカメラ設定

## 6.1 ローカルパラメータの設定

#### 目的:

ローカル設定は、ライブビュー、録画ファイル、キャプチャ画像のパラメータを参照します。

録画ファイルとキャプチャされた写真は、Webブラウザを使用して録画およびキャプチャしたものであり、ブラウザを実行しているPC上に保存パスがあります。

### 手順:

- 1. 「Configuration」 > 「Local」を選択します。
- 2. 以下の設定をします:
- **ライブビューパラメータ**:プロトコルタイプとライブビューパフォーマンスを設定します。
  - ◆ 「Protocol Type」:「TCP」、「UDP」、「MULTICAST」、「HTTP」から選択できます。

「TCP」: ストリーミングデータの完全な配信とビデオ品質を確保しますが、リアルタイム転送は影響を受けます。

「UDP」: リアルタイムのオーディオおよびビデオストリームを提供します。

「HTTP」: 一部のネットワーク環境では、特定のポートをストリーミング用に設定することなく、TCP と同じ品質を実現します。

「MULTICAST」: マルチキャスト機能を使用する場合は、MCAST タイプを選択することを推奨します。マルチキャストの詳細については、「7.1.1TCP/IP 設定」を参照してください。

◆ 「Play Performance」: ライブビューパフォーマンスを「Shortest Delay」、
「Balanced」、「Fluent」、「Custom」に設定します。「Custom」では、ライブビューのフレームレートを設定できます。

◆ 「Rules」: ローカルブラウザのルールを参照し、モーション検出、顔検 出、または侵入が検出されたときに色付きマークを表示するかどうかを 選択して、有効または無効にします。

たとえば、ルールとして有効になり、顔検出も有効になります。顔が検出されると、ライブビューに緑の長方形がマークされます。

◆ 「Display POS Information」: この機能を有効にすると、検出されたターゲットのフィーチャー情報がライブ画像のターゲット付近に動的に表示されます。各機能の機能情報は異なります。たとえば、キュー管理のID と待機時間、人数計算の高さなどです。

#### お知らせ:

POS情報の表示は、特定のカメラモデルでのみ使用できます。

◆ 「Image Format」: 画像取り込みの画像形式を選択します。

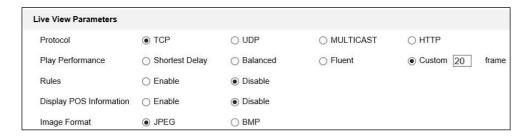


図6-1 ライブビューのパラメータ

- 「Record File Settings」: 録画されたビデオファイルの保存パスを設定します。Webブラウザで録画した録画ファイルに有効です。
  - ◆ 「Record File Size」: 手動で録画/ダウンロードした動画ファイルの圧縮サイズを256M/512M/1Gから選択します。選択後、最大レコードファイルサイズは選択した値になります。
  - ◆ 「Save record files to」: 手動で録画したビデオファイルの保存先を設定します。
  - ◆ 「Save snapshots when playback to」: 再生モードでダウンロードした動画 ファイルの保存先を設定します。

- 「Save clips to」: 撮影した写真やクリップしたビデオファイルの保存経路を設定します。Webブラウザで撮影する画像に有効です。
  - ◆ 「Save snapshots in live view to」:: 手動で撮影した画像のライブビューモードでの保存先を設定します。
  - ◆ 「Save snapshots when playback to」: 再生モードで撮影した画像の保存 経路を設定します。
  - ◆ 「Save clips to」: 再生モードでクリップされた動画ファイルの保存先を設定します。

お知らせ: 「Browse」をクリックしてクリップと画像を保存するディレクトリを変更し、「Open」をクリックしてクリップと画像の保存先フォルダを開きます。

3. 「Save」をクリックし、設定を保存します。

### 6.2 システム設定

### 目的:

システム設定、メンテナンス、セキュリティ、ユーザー管理などのシステム設定を 行うには、以下の手順に従ってください。

### 6.2.1 基本情報の設定

「Configuration」 > 「System」 > 「System Settings」 > 「Basic Information」を選択します。

「Basic Information」画面では、「Device Name」と「Device No」を編集できます。モデル、シリアル番号、ファームウェアバージョン、エンコーディングバージョン、チャネル数、HDD数、アラーム入力数、アラーム出力数など、ネットワークカメラのその他の情報が表示されます。このメニューで情報を変更することはできません。今後のメンテナンスや改造の参考になります。

### 6.2.2 時間設定

### 目的:

このセクションの指示に従って、時刻同期およびDST 設定を行います。

#### 手順:

1. 「Configuration」>「System」>「System Settings」>「Time Settings」を選択します。

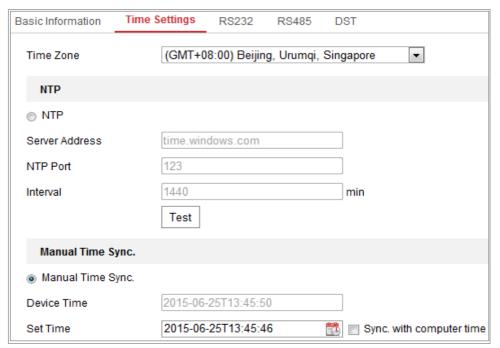


図6-2 時間設定

- 2. ドロップダウンメニューから場所のタイムゾーンを選択します。
- 3. NTP 設定をします。
  - (1)「NTP」チェックボックスをオンにしてNTP機能を有効にします。
  - (2) 以下の設定をします:

「Server Addres」: NTP サーバーのIP アドレス。

「NTP Port」: NTP サーバーのポート。

「Interval」: NTP サーバーとの2つの同期アクション間の時間間隔。

(3) 「Test」をクリックすると、NTPサーバーを介してタイム同期機能をテストすることができます。



図6-3 NTP サーバーによる時刻同期

お知らせ: カメラがパブリックネットワークに接続されている場合は、National Time Center (IP Address: 210.72.145.44) のサーバーなど、時刻同期機能を備えたNTP サーバーを使用する必要があります。カスタマイズされたネットワークでカメラが設定されている場合、NTP ソフトウェアを使用して、時刻同期用のNTP サーバーを確立することができます。

- 手動時刻同期を設定します。
  - (1)「Manual Time Sync.」チェックボックスをオンにすると、手動時刻同期機能が有効になります。
  - (2) **型**アイコンをクリックして、ポップアップカレンダーから日付と時刻を選択します。

(3) 「Sync. with computer time」チェックボックスをオンにして、デバイスの時刻をローカルPCの時刻と同期させることができます。



図6-4 手動による時刻同期

● 「Save」をクリックして設定を保存します。

### 6.2.3 RS232 設定

RS232 ポートは2 つの方法で使用できます:

- Consolo: シリアルポートを介してコンピュータをカメラに接続します。デバイスパラメータは、ハイパーターミナルなどのソフトウェアを使用して設定できます。シリアルポートパラメータは、カメラのシリアルポートパラメータと同じである必要があります。
- 透過チャンネル:シリアルデバイスをカメラに直接接続します。シリアルデバイスは、ネットワークを介してコンピュータによってリモートで制御されます。

### 手順:

1. 「Configuration」 > 「System」 > 「System Settings」 > 「RS232」を選択します。

2. ボーレート、データビット、ストップビット、パリティ、フロー制御、および使用方法 を設定します。

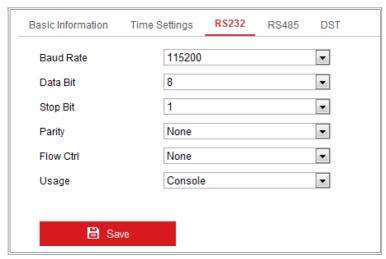


図6-5 RS232 設定

*お知らせ:* RS232 ポートでカメラを接続する場合、RS232 のパラメータはここで 設定したパラメータとまったく同じになるはずです。

3. 「Save」をクリックし、設定を保存します。

### 6.2.4 RS485 設定

### 目的:

RS485シリアルポートは、カメラのPTZを制御するために使用します。PTZ パラメータの設定は、PTZ ユニットを制御する前に行ってください。

### 手順:

1. 「Configuration」>「System」>「System Settings」>「RS485」を選択します。

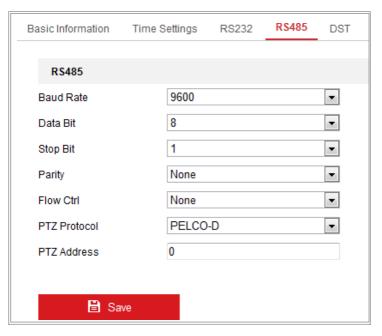


図6-6 RS-485の設定

2. RS485 パラメータを設定し、「Save」をクリックして設定を保存します。 デフォルトでは、ボーレートは9600 bps、データビットは8、ストップビットは1、 パリティおよびフロー制御はNone に設定されています。

お知らせ: ボーレート、PTZ プロトコル、およびPTZ アドレスのパラメータは、PTZ カメラのパラメータとまったく同じである必要があります。

### 6.2.5 DST 設定

### 目的:

サマータイム(DST)とは、夏の数カ月間に時計を1時間進め、秋には再び時刻を合わせることで、自然光をよりうまく利用する方法です。 必要に応じてDSTを設定してください。

### 手順:

1. 「Configuration」 > 「System」 > 「System Settings」 > 「DST」を選択します。



図6-7 DST 設定

- 2. 開始時刻と終了時刻を選択します。
- 3. DSTバイアスを選択します。
- 4. 「Save」をクリックして、設定を有効にします。

### 6.2.6 外部デバイスの設定

### 目的:

ハウジング上のワイパーやLEDライトなど、デバイスサポートの外部デバイスでは、Webブラウザを介して制御できます。カメラの機種により、外部デバイスは異なります。

### 手順:

1. 「Configuration」 > 「System」 > 「System Settings」 > 「External Device」を選択します。

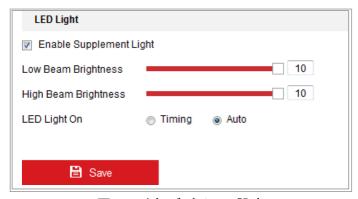


図6-8 外部デバイスの設定

- 2. 「Enable Supplement Light」チェックボックスをオンにすると、LED Light が有効になります。
- 3. スライダーを動かして、ロービームの明るさとハイビームの明るさを調整します。
- 4. LEDライトのモードを選択します。タイミング、オートが選択可能です。
  - 「Timeing」: 設定したスケジュールでLEDが点灯します。開始時間と終了時間を設定する必要があります。

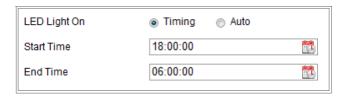


図6-9 セットスケジュール

- 「Auto」: 環境照明に応じてLEDが点灯します。
- 5. 「Save」をクリックし、設定を保存します。

### 6.2.7 VCA リソースの設定

### 目的:

VCA リソースには、複数のVCA 機能が使用可能な場合に、必要に応じて特定の VCA 機能を有効にするオプションが用意されています。これは、必要な機能によ り多くのリソースを割り当てるのに役立ちます。

### 手順:

- 1. 「Configuration」 > 「System」 > 「System Settings」 > 「VCA Resource」を選択します。
- 2. 任意のVCA の組み合わせを選択します。使用可能なVCA の組み合わせは、モデルによって異なります。
- 3. 「Save」をクリックし、設定を保存します。VCA リソースを設定した後は、再起動が必要です。

### お知らせ:

- VCA の組み合わせは相互に排他的です。1 つの組み合わせをアクティブにすると、その他は非表示になります。
- カメラの機種によっては、対応していないことがあります。

### 6.2.8 メタデータ設定

### 目的:

メタデータは、アルゴリズム処理前にカメラが収集する元データです。侵入検知、 ライン交差検知、領域進入検知、領域退出検知、無人手荷物検知、物体除去、 待ち行列管理およびフェイスキャプチャのメタデータをアップロードできます。有 効にすると、対応するイベントのメタデータがユーザーに提供され、さまざまなデータ使用の可能性が調査されます。

### 手順:

- 1. 「Configuration」>「System」>「System Settings」>「metadata Settings」を選択します。
- 2. 対応する関数のチェックボックスにチェックを入れて、メタデータ関数を有効に します。
- スマートイベントのメタデータには、ターゲットID、ターゲット座標、および時間 情報が含まれます。
- キュー管理のメタデータには、ルール情報、領域ID、ターゲットID、ターゲット 座標、および時間情報が含まれます。初期設定では、カメラが画像全体を検出します。キュー管理設定でリージョンを設定した場合、カメラは設定された リージョンを検出します。
- フェイスキャプチャのメタデータには、ルール情報、ターゲットID、ターゲット座標、顔のグレーディング、および時間情報が含まれます。初期設定では、カメラが画像全体を検出します。フェイスキャプチャ設定で領域が設定されている場合、カメラは設定された領域を検出します。

### 6.2.9 オープンソース・ソフトウェア・ライセンス

必要に応じて、IP カメラに適用されるオープンソースソフトウェアに関する情報を確認できます。「Configuration」 > 「System」 > 「About」を選択してください。

### 6.3 メンテナンス

### 6.3.1 アップグレードとメンテナンス

### 目的:

アップグレード&メンテナンス画面から、再起動、一部の復元、デフォルトへの復元、設定ファイルの エクスポート/インポート、デバイスのアップグレードなどの操作を処理できます。

「Configuration」>「System」>「Maintenance」>「Upgrade & Maintenance」を選択します。

- 「Reboot」: デバイスを再起動します。
- 「Restore」: IP パラメータとユーザー情報を除くすべてのパラメータをデフォルト設定にリセットします。
- 「Default」: すべてのパラメータを工場出荷時のデフォルトに戻します。

#### お知らせ:

- 初期設定を復元すると、IPアドレスも初期設定のIPアドレスに復元されますので、この対処には十分ご注意ください。
- Wi-Fi、ワイヤレスダイヤル、wlan 機能に対応したカメラの場合、Restore アクションでは、上記の機能の関連設定は初期設定に戻りません。

#### 「Information Export」

「Device Parameters」: クリックして、カメラの現在の設定ファイルをエクスポートします。この操作を続行するには、管理者パスワードが必要です。エクスポートしたファイルに対しては、暗号化パスワードも作成する必要があります。暗号化パスワードは、ファイルを他のカメラにインポートするときに必要です。

「Diagnose Information」: クリックしてログとシステム情報をダウンロードします。

### • 「Import Config. File」

カメラの一括設定には、設定ファイルを使用します。

### 手順:

- 1. 「Browse」をクリックして、保存した設定ファイルを選択します。
- 2. 「Import」をクリックして、エクスポート時に設定した暗号化パスワードを 入力します。

*お知らせ:* 設定ファイルをインポートした後、カメラを再起動する必要があります。

● 「Upgrade」: デバイスを特定のバージョンにアップグレードします。

### 手順:

- ファームウェアまたはファームウェアディレクトリを選択して、アップグレードファイルを見つけます。ファームウェア:アップグレードファイルの正確なパスを見つけます。
  - ファームウェアディレクトリ:アップグレードファイルが属するディレクトリのみが必要です。
- 2. 「Browse」をクリックしてローカルアップグレードファイルを選択し、「Upgrade」 をクリックしてリモートアップグレードを開始します。

*お知らせ:* アップグレード処理には1~10分かかります。処理中はカメラの電源を切断しないでください。アップグレード後、カメラは自動的に再起動します。

### 6.3.2 ログ

### 目的:

カメラの操作、アラーム、例外、情報をログファイルに保存できます。必要に応じてログファイルをエクスポートすることもできます。

### 準備:

カメラにネットワークストレージを設定するか、カメラにSDカードを挿入してください。

### 手順:

1. 「Configuration」 > 「System」 > 「Maintenance」 > 「Log」を選択します。

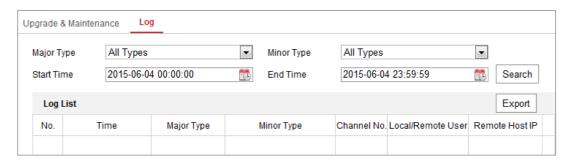


図6-10 ログ検索画面

- 2. 「Major Type」、「Minor Type」、「Start Time」、「End Time」など、検索を指定 するためのログ検索条件を設定します。
- 3. 「Search」をクリックして、ログファイルを検索します。一致したログファイルがログリスト画面に表示されます。

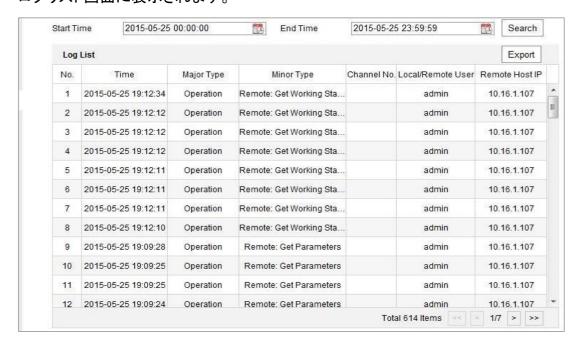


図6-11 ログ検索

4. ログファイルをエクスポートするには、「Export」をクリックしてログファイルを保存します。

### 6.3.3 システムサービス

#### 目的:

システムサービス設定は、カメラがサポートするハードウェアサービスを参照します。 対応する機能はカメラによって異なります。カメラがIR Light、ABF (Auto Back Focus)、Auto Defog、またはStatus LEDをサポートしている場合、実際の需要に応じて対応するサービスを有効または無効にするように選択できます。

「ABF」: ABF 機能を有効にすると、PTZ コントロールパネルの Se をクリックして補助フォーカスを実現できます。

「Third Stream」: 一部のモデルでは、デフォルトで3 番目のストリームが有効になっていません。この機能を有効にするには、「Enable Third Stream」にチェックを入れます。

「eMMC Protection」: eMMC 保護を有効にすると、eMMC の寿命が表示されます。
「Enable Motion Detection」:チェックを入れると、モーション検出機能が有効になります。

### 6.3.4 セキュリティ監査ログ

### 目的:

セキュリティ監査ログは、セキュリティ操作ログを参照します。カメラのセキュリティーログファイルを検索および分析して、セキュリティイベントの不正侵入およびトラブルシューティングを検出することができます。セキュリティ診断ログは、デバイスフラッシュに保存できます。ログは、デバイスの起動後30分ごとに保存されます。フラッシュの保存領域が限られているため、ログサーバにログを保存することもできます。

「Advanced Settings」でサーバー設定をします。

### ● ログの検索

### 手順:

1. 「Configuration」 > 「System」 > 「Maintenance」 > 「Security Audit Log」を選択します。

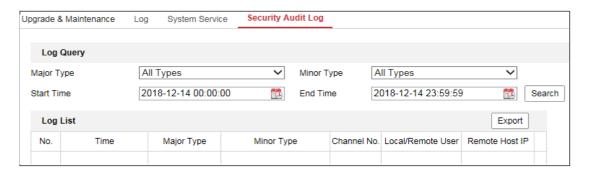


図6-12 セキュリティ監査ログ検索画面

- 2 「Major Type」、「Minor Type」、「Start Time」、「End Time」など、検索を指定する ためのログ検索条件を設定します。
- 3. 「Search」をクリックして、ログファイルを検索します。一致したログファイルがログリスト画面に表示されます。

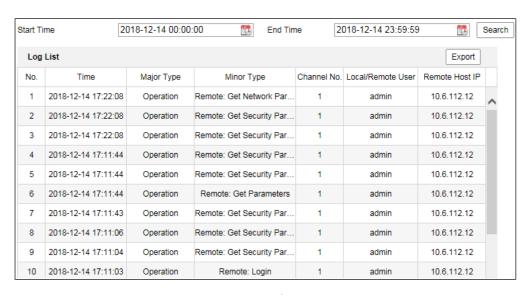


図6-13 ログ検索

4. ログファイルをエクスポートするには、「Export」をクリックしてログファイルを保存します。

### ログサーバの設定

### 手順:

1. 「Enable Log Upload Server」をオンにします。

- 2. ログサーバIP とログサーバポートを入力します。
- 3. 「Test」をクリックして設定をテストします。
- 4. 証明書をインストールします。クライアント証明書とCA 証明書が必要です。
  - 「Client Certificate」
  - (1)「Create」をクリックして、証明書要求を作成します。ポップアップウィンドウで必要な情報を入力します。
  - (2)「Download」をクリックして証明書要求をダウンロードし、署名のために 信頼できる認証局に送信します。
  - (3) 署名済み証明書をデバイスにインストールします。
  - 「CA Certificate」 デバイスにCA 証明書をインストールします。

### 6.4 セキュリティ設定

セキュリティ画面からの認証、IP アドレスフィルタ、セキュリティサービスなどのパラメータを設定します。

### 6.4.1 認証

#### 目的:

ライブビューのストリームデータを明示的に保護することができます。

### 手順:

1. 「Configuration」 > 「System」 > 「Security」 > 「Authentication」を選択します。



図6-14 認証

2. RTSP 認証とWEB 認証の認証方式を設定します。

### お知らせ:

ダイジェストは、データセキュリティを高めるために推奨される認証方法です。 認証方法としてbasic を採用する場合は、リスクに注意する必要があります。

3. 「Save」をクリックし、設定を保存します。

### 6.4.2 IPアドレスフィルタ

### 目的:

この機能により、アクセス制御が可能になります。

### 手順:

1. 「Configuration」 > 「System」 > 「Security」 > 「IP Address Filter」を選択します。



図6-15 IP アドレスフィルタ画面

- 2 「Enable IP Address Filter」チェックボックスをオンにします。
- 3. ドロップダウンリストでIPアドレスフィルタのタイプを選択し、「Forbidden」と「Allowed」を選択できます。
- 4. IP アドレスフィルタリストを設定します。
  - IPアドレスを追加する

### 手順:

(1) IP を追加するには、「Add」をクリックします。

(2) IP Adreess を入力します。



図6-16 IP の追加

- (3)「OK」をクリックして追加を終了します。
- IP アドレスの変更

### 手順:

- (1) フィルタリストからIP アドレスを左クリックして、「Modify」をクリックします。
- (2) テキストボックスでIP アドレスを変更します。



図6-17 IP の変更

- (3)「OK」をクリックして変更を終了します。
- IP アドレスまたはIP アドレスを削除します。
  IP アドレスを選択し、「Delete」をクリックします。
- 5. 「Save」をクリックし、設定を保存します。

### 6.4.3 セキュリティサービス

リモートログインを可能にし、データ通信セキュリティを向上させるために、カメラはより良いユーザエクスペリエンスのためにセキュリティサービスを提供します。

### 手順:

1. 「Configuration」 > 「System」 > 「Security」 > 「Security Service」を選択します。

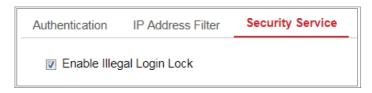


図 6-18 セキュリティサービス

2. 「Enable Illegal Login Lock」チェックボックスをオンにします。

「Illegal Login Lock」: ユーザーのログイン試行を制限するために使用されます。 管理者がユーザー名/パスワードの入力を7回(オペレーター/ユーザーの場合は5回)失敗すると、IP アドレスからのログインが拒否されます。

*お知らせ:* IP アドレスが拒否された場合は、30 分後にデバイスへのログインを 試みることができます。

### 6.4.4 高度なセキュリティ

### 目的:

高度なセキュリティは、デバイスのより多くのネットワークセキュリティ設定を管理 するオプションを提供します。

「Security Reinforce」

チェックボックスにチェックを入れると、機能が有効になります。セキュリティ強化は、ネットワークセキュリティを強化するための方法です。この機能を有効にすると、危険な機能、プロトコル、デバイスのポートが無効になり、より安全な代替機能、プロトコル、ポートが有効になります。

「Control Timeout Settings」

この機能を有効にしてタイムアウト時間を設定すると、設定したタイムアウト時間(ライブ画像の閲覧、再生は含まれません)の間、ウェブブラウザから本機に操作を行わないとログアウトします。

### 「Algorithm」

現在アクティブなダイジェストアルゴリズムを表示します。Security Reinforce が有効になっている場合、MD5 は無効になり、代わりにSHA256 が有効になります。

### 6.5 ユーザー管理

### 6.5.1 ユーザー管理

### ● 管理者として

管理者ユーザーは、ユーザーアカウントを追加、削除、または変更したり、さまざまな権限を付与したりできます。ユーザーの勘定と許可を適切に管理することを強く推奨します。

「Configuration」 > 「System」 > 「User Management」を選択します。

#### お知らせ:

ユーザーアカウントの追加と変更が必要な場合は、管理者パスワードが必要です。

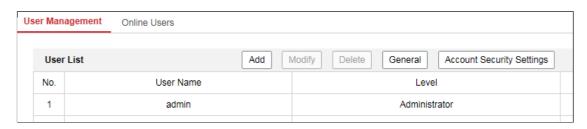


図6-19 ユーザー管理画面

### ● ユーザーの追加

管理者 ユーザーはデフォルトですべての権限を持ち、他のアカウントを作成/変更/削除できます。

管理者ユーザーは削除できず、管理者パスワードのみを変更できます。

### 手順:

- 1. 「Add」をクリックしてユーザーを追加します。
- 「Admin Password」、「User Name」を入力し、「Level」を選択して「Password」を入力します。

### お知らせ:

- ユーザーアカウントは31 個まで作成できます。
- 異なる「Level」のユーザーは、異なるデフォルト権限を所有します。オペレーターとユーザーを選択できます。

### 強力なパスワードを推奨-



製品のセキュリティを強化するために、独自に強力なパスワードを作成することを強く推奨します(大文字、小文字、数字、特殊文字のカテゴリを少なくとも3つ含む8文字以上を使用)。

また、パスワードを定期的に変更することを推奨します。特に高セキュリティシステムでは、パスワードを月単位または週単位で変更すると製品のセキュリティが向上します。

- 3. 新しいユーザーの権限をチェックまたはチェック解除できます。
- 4. 「OK」をクリックして、ユーザーの追加を終了します。
- ユーザーの変更

#### 手順:

1. 左クリックしてリストからユーザーを選択し、「Modify」をクリックします。

2. 「UserName」、「Level」、「Password」を変更します。



### 強力なパスワードを推奨-

製品のセキュリティを強化するために、独自に強力なパスワードを作成することを強く推奨します(大文字、小文字、数字、特殊文字のカテゴリを少なくとも3つ含む8文字以上を使用)。

また、パスワードを定期的に変更することを推奨します。特に高セキュリティシステムでは、パスワードを月単位または週単位で変更すると製品のセキュリティが向上します。

- 3. 権限をチェックまたはチェック解除できます。
- 4. 「OK」をクリックして、ユーザーの変更を終了します。
- ユーザの削除

### 手順:

- 1. 削除するユーザーをクリックして選択し、「Delete」をクリックします。
- 2. 表示された画面を確認の上「OK」をクリックし、削除します。
- 同時ログインの設定

### 手順:

- 1. 「General」をクリックします。
- 2. スライドバーをスライドさせて、同時ログインを設定します。不正なログイン 試行回数が設定したしきい値を超えると、アクセスが拒否されます。
- オペレーターまたはユーザーとして

オペレーターまたはユーザーはパスワードを変更できます。このアクションには 古いパスワードが必要です。

### 6.5.2 セキュリティに関する質問

### 目的:

セキュリティに関する質問は、管理者ユーザーがパスワードを忘れた場合に管理者 パスワードを復元するために使用されます。

### アカウントセキュリティの設定:

カメラ起動中にセキュリティの質問を設定できます。または、ユーザー管理画面で機能を設定することもできます。

カメラを復元すると、セキュリティの質問設定はクリアされません(デフォルトではありません)。

### 手順:

- 1. 「Configuration」>「System」>「User Management」>「User Management」を選択します。
- 2. 「Account Security Settings」をクリックします。
- 3. 質問を選択し、回答を入力します。
- 4. パスワード復旧の確認コードを受信するEメールアドレスを入力します。
- 5. 「OK」をクリックし、設定を保存します。

### 管理者パスワードの変更:

### 準備:

パスワードの変更に使用するPC およびカメラは、同じLAN の同じIP アドレスセグメントに属している必要があります。

● 管理者パスワードを変更される場合は、当社営業またはサポートコールまでご 相談ください。

### 6.5.3 オンラインユーザー

### 目的:

この画面を通してデバイスを訪問している現在のユーザーを確認できます。ユーザーリストには、ユーザー名、レベル、IPアドレス、操作時間などのユーザー情報が表示されます。

「Refresh」をクリックしてリストを更新します。



図6-20 オンラインユーザーの表示

# 第7章 ネットワーク設定

### 目的:

この章の指示に従って、基本設定と詳細設定をします。

# 7.1 基本設定

### 目的:

このセクションの指示に従って、TCP/IP、DDNS、PPPoE、ポート、NAT などのパラメータを設定できます。

### 7.1.1 TCP/IP 設定

### 目的:

ネットワーク経由でカメラを操作する前に、TCP/IP設定を適切に設定する必要があります。カメラはIPv4 とIPv6 の両方に対応しています。

両方のバージョンは互いに競合せずに同時に設定でき、少なくとも1つのIP バージョンを設定する必要があります。

### 手順:

1. 「Configuration」 > 「Network」 > 「Basic Settings」 > 「TCP/IP」を選択します。

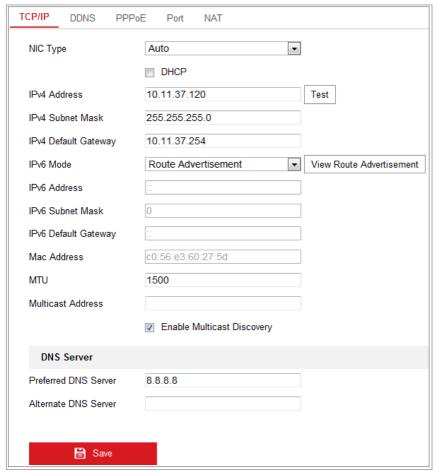


図7-1 TCP/IP 設定

- 2. NIC タイプ、IPv4 またはIPv6 アドレス、IPv4 またはIPv6 サブネットマスク、 IPv4 またはIPv6 デフォルトゲートウェイ、MTU 設定、およびマルチキャストアド レスを含む基本的なネットワーク設定をします。
- 3. 「Enable Multicast Discovery」チェックボックスをオンにすると、LAN 内のプライベートマルチキャストプロトコルを介して、オンラインネットワークカメラをクライアントソフトウェアで自動的に検出できます。
- 4. DNSサーバーを設定します。「Preferred DNS Server」と「Alternate DNS Server」を入力します。
- 5. 「Save」をクリックして、設定を保存します。

#### お知らせ:

- MTU の有効な値の範囲は1280 から1500 です。
- ▼ルチキャストは、マルチキャストグループアドレスにストリームを送信し、マルチキャストグループアドレスからのコピーを要求することによって、複数のクライアントが同時にストリームを取得できるようにします。この機能を使用する前に、ルーターのマルチキャスト機能を有効にする必要があります。
- 設定を有効にするには、再起動が必要です。

### 7.1.2 DDNS 設定

### 目的:

お使いのカメラがデフォルトのネットワーク接続としてPPPoE を使用するように設定されている場合は、ネットワークアクセスにダイナミックDNS (DDNS) を使用できます。

#### 準備:

カメラのDDNS 設定をする前に、DDNSサーバーでの登録が必要です。

#### 手順:

- 1. 「Configuration」 > 「Network」 > 「Basic Settings」 > 「DDNS」を選択します。
- 2. この機能を有効にするには、「Enable DDNS」チェックボックスをオンにします。
- 3. DDNSタイプを選択します。DDNS には、DynDNS とNO-IP の2 種類があります。
  - 「DynDNS」:

#### 手順:

- (1) DynDNS のサーバアドレス(members.dyndns.org など) を入力します。
- (2) 「Domain」欄に、DynDNS Web サイトから取得したドメイン名を入力します。
- (3) 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。

(4)「Save」をクリックし、設定を保存します。

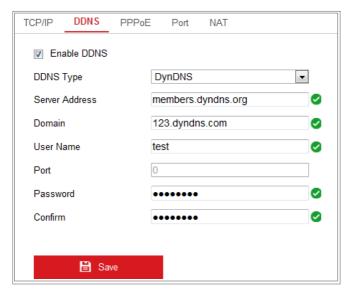


図7-2 DynDNS 設定

「NO-IP」:

### 手順:

(1) NO-IP としてDDNS タイプを選択します。



図7-3 NO-IP DNS 設定

- (2) サーバーアドレスをwww.noip.com と入力します。
- (3) 登録したドメイン名を入力します。
- (4) ユーザー名とパスワードを入力します。

(5)「Save」をクリックすると、ドメイン名のカメラを表示できます。

**お知らせ**: 設定を有効にするには、デバイスを再起動します。

### 7.1.3 PPPoE 設定

### 手順:

1. 「Configuration」 > 「Network」 > 「Basic Settings」 > 「PPPoE」を選択します。

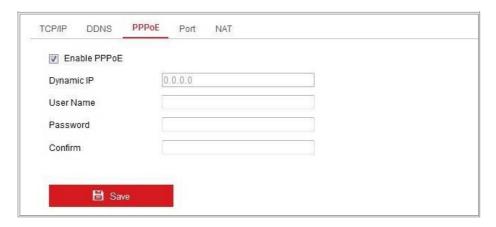


図7-4 PPPoE の設定

- 2. この機能を有効にするには、「Enable PPPoE」チェックボックスをオンにします。
- 3. PPPoE にアクセスするためのユーザー名、パスワード、およびパスワードの確認を入力します。

*お知らせ:* ユーザー名とパスワードは、ISP が割り当てる必要があります。



- プライバシーを守り、セキュリティリスクからシステムを保護するために、すべて の機能およびネットワークデバイスに強力なパスワードを使用することを強く推 奨します。パスワードは、製品のセキュリティを強化するために、8 文字以上(大 文字、小文字、数字、特殊文字の3つ以上を含む)に設定してください。
- 4. 「Save」をクリックして、画面を保存して終了します。

**お知らせ**: 設定を有効にするには、再起動が必要です。

### 7.1.4 ポート設定

### 目的:

カメラのポート番号(HTTPポート、RTSPポート、HTTPSポートなど)を設定できます。

### 手順:

1. 「Configuration」 > 「Network」 > 「Basic Settings」 > 「Port」を選択します。

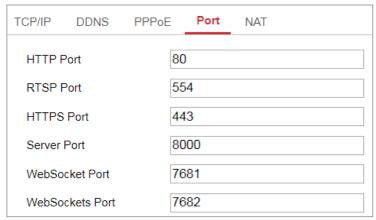


図7-5 ポート設定

2. カメラのポートを設定します。

「HTTP Port」: デフォルトのポート番号は80で、占有されていない任意のポート番号に変更できます。

「RTSP Port」: デフォルトのポート番号は554であり、1から65535までの任意のポート番号に変更することができます。

「HTTPS Port」: デフォルトのポート番号は443で、占有されていない任意のポート番号に変更できます。

「Server Port」: デフォルトのサーバーポート番号は8000 で、2000 ~65535 の任意のポート番号に変更できます。

#### お知らせ:

クライアントソフトウェアを使用してカメラにアクセスし、サーバーポート番号を変更した場合は、ログイン画面に正しいサーバーポート番号を入力してカメラにアクセスする必要があります。

「WebSocket Port」: デフォルトのポート番号は7681 です。1~65535の任意のポートNo.に変更できます。

「WebSockets Port」: デフォルトのサーバーポート番号は7682 です。1~65535の任意のポートNo.に変更できます。

#### お知らせ:

WebSocket および WebSockets プロトコルは、プラグインフリーのライブビューに使用されます。詳細は、「7.2.11 ネットワークサービス」を参照してください。

3. 「Save」をクリックし、設定を保存します。

**お知らせ**: 設定を有効にするには、再起動が必要です。

### 7.1.5 NAT (ネットワークアドレス変換) 設定

### 目的:

NAT設定では、UPnP™パラメータを設定できます。

ユニバーサルプラグアンドプレイ(UPnP™)は、ネットワーク機器、ソフトウェア、およびその他のハードウェアデバイス間の互換性を提供するネットワークアーキテクチャです。UPnP プロトコルを使用すると、デバイスがシームレスに接続でき、ホームおよび企業環境でのネットワークの実装を簡素化できます。

この機能を有効にすると、ポートごとにポートマッピングを設定する必要がなくなり、 カメラはルーター経由でワイドエリアネットワークに接続されます。

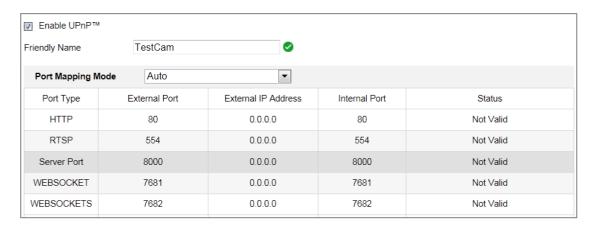


図7-6 UPnP の設定

### 手順:

- 1. 「Configuration」 > 「Network」 > 「Basic Settings」 > 「NAT」を選択します。
- 2 チェックボックスをオンにすると、UPnP™機能が有効になります。

### お知らせ:

UPnP™機能が有効な場合のみ、カメラのポートがアクティブになります。

- 3. カメラのフレンドリーな名前を選択するか、デフォルトの名前を使用できます。
- 4. ポートマッピングモードを選択します。「Manual」または、「Auto」が選択可能です。

### お知らせ:

自動を選択した場合は、ルーターでUPnP™機能を有効にする必要があります。「Manual」を選択すると、外部ポートの値をカスタマイズし、ルーターのポートマッピング設定を手動で完了できます。

5. 「Save」をクリックして設定を保存します。

### 7.1.6 マルチキャストの設定

### 目的:

マルチキャストは、デバイスグループに同時にデータ送信が可能なグループ通信です。アクティブなマルチキャストを設定すると、送信元から複数のデバイスに効率的に送信できます。

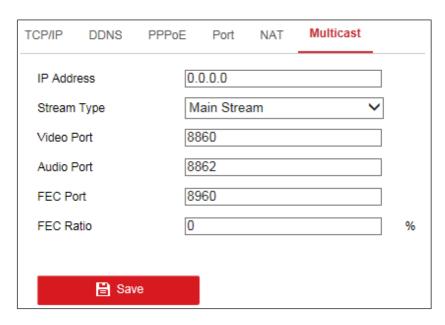


図7-7 マルチキャストの設定

### 手順:

- 1. 「Configuration」 > 「Network」 > 「Basic Settings」 > 「Multicast」を選択します。
- カメラの「IP Address」、「Stream Type」、「Video Port」、「Audio Port」、「FEC Port」、「FEC Ratio」を設定します。

#### お知らせ:

- IP Address は、マルチキャストのアドレスを表します。
- 各カメラチャンネルおよび各ビデオストリームのビデオポートとオーディオポートは、「Video Stream」でストリームを選択し、「Video Port」と「Audio Port」でポート番号を入力して指定します。
- 3. 「Save」をクリックします。

# 7.2 詳細設定

#### 目的:

SNMP、FTP、Eメール、HTTPS、QoS、802.1xなどのパラメータは、このセクションの手順に従って設定できます。

### 7.2.1 SNMP設定

### 目的:

SNMP 機能を設定して、カメラステータス、パラメータ、およびアラーム関連情報を取得し、ネットワークに接続されているときにカメラをリモート管理できます。

### 準備:

SNMP を設定する前に、SNMP ソフトウェアをダウンロードし、カメラ情報をSNMP ポート経由で受信するように管理してください。トラップアドレスを設定することで、カメラはアラームイベントと例外メッセージを監視センターに送信できます。

お知らせ: 選択するSNMPバージョンは、SNMPソフトウェアのバージョンと同じである必要があります。また、必要なセキュリティレベルに応じて異なるバージョンを使用する必要があります。SNMP v1はセキュリティが非対応ですが、SNMP v2はアクセスにパスワードを必要です。また、SNMP v3は暗号化をサポートしているため、v3を使用する場合は、HTTPSプロトコルを有効にしなければなりません。



● プライバシーを守り、セキュリティリスクからシステムを保護するために、すべて の機能およびネットワークデバイスに強力なパスワードを使用することを強く推 奨します。パスワードは、製品のセキュリティを強化するために、8 文字以上(大 文字、小文字、数字、特殊文字の3つ以上を含む)に設定してください。

### 手順:

1. 「Configuration」 > 「Network」 > 「Advanced Settings」 > 「SNMP」を選択します。

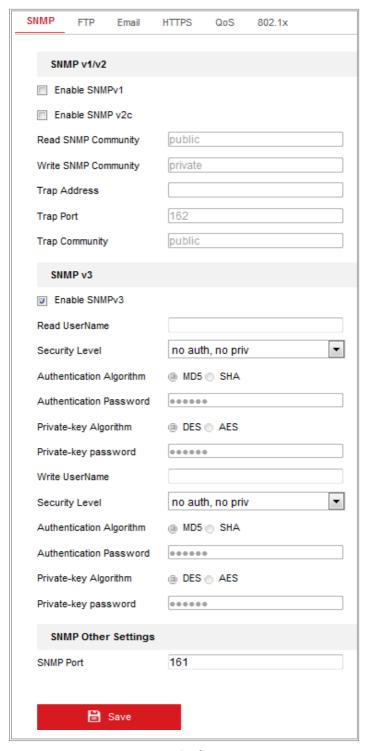


図7-8 SNMP 設定

- 2. 「Enable SNMPv1」、「Enable SNMP v2c」、「Enable SNMPv3」チェックボックスをオンにし、それぞれの機能を有効にします。
- 3. SNMPの設定を行います。

*お知らせ:* SNMPソフトウェアの設定は、ここで設定する内容と同じにする必要があります。

4.「Save」をクリックして設定を保存し、終了します。

### お知らせ:

- 設定を有効にするには、再起動が必要です。
- 情報漏洩のリスクを軽減するために、SNMP v1 またはv2 ではなくSNMP v3 を有効にすることを推奨します。

### 7.2.2 FTP 設定

### 目的:

取り込んだ画像をFTP/SFTP サーバーにアップロードできるように、FTP/SFTP サーバー関連の情報を設定できます。キャプチャされた画像は、イベントまたはタイミングスナップショットタスクによってアップロードされます。

### 手順:

1. 「Configuration」>「Network」>「Advanced Settings」>「FTP」を選択します。

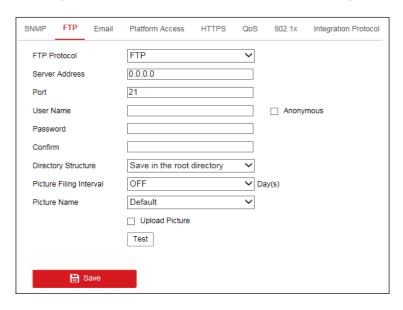


図7-9 FTP 設定

- 2 「FTP Protocol」を選択します。
- 3. サーバーのアドレスとポートを入力します。
- 4. FTP/SFTP 設定をします。サーバーへのログインには、ユーザー名とパスワードが必要です。



- プライバシーを守り、セキュリティリスクからシステムを保護するために、すべての機能およびネットワークデバイスに強力なパスワードを使用することを強く推奨します。パスワードは、製品のセキュリティを強化するために、8 文字以上(大文字、小文字、数字、特殊文字の3つ以上を含む)に設定してください。
- 5. 「Directory Structure」と「Picture Filing Interval」を設定します。

「Directory Structure」: ルートディレクトリ、親・子ディレクトリを選択できます。親ディレクトリを選択すると、ディレクトリ名にデバイス名、デバイス番号、デバイスIP を使用するオプションがあり、子ディレクトリを選択すると、カメラ名またはカメラ番号をディレクトリ名として使用できます。

「Picture Filing Interba;」:画像を管理しやすくするために、画像ファイル間隔を1日から30 日まで設定できます。同じ時間間隔で撮影した画像は、時間間隔の開始日付と終了日付のあとに名前が付けられた1つのフォルダに保存されます。

「Picture Name」: キャプチャした画像ファイルの命名規則を設定します。ドロップダウンリストで「Default」を選択すると、既定のルールを使用できます。

IP address\_channel number\_capture time\_event type.jpg
(例: 10.11.37.189\_01\_20150917094425492\_FACE\_DETECTION.jpg)

または、デフォルトの命名ルールにカスタムプレフィックスを追加してカスタマイズすることもできます。

6. 「Upload Picture」チェックボックスをオンにし、機能を有効にします。

「Upload Picture」: キャプチャした画像のFTP サーバーへのアップロードを有効にします。FTP サーバへの匿名アクセス(この場合、ユーザー名とパスワードは必要ありません): 「Anonymous」チェックボックスをオンにし、FTP サーバへの匿名アクセスを有効にします。

お知らせ: 匿名アクセス機能は、FTPサーバーでサポートする必要があります。

7. 「Save」をクリックし、設定を保存します。

### 7.2.3 Eメール設定の指定

### 目的:

このシステムは、警報事象が検出された場合に、全ての指定された受信者に電子メールの通知を送るように設定することができます。例えば、動き検出イベント、ビデオ損失、ビデオ改ざんなど。

### 準備:

電子メール機能を使用する前に、「Configuration」 > 「Network」 > 「Basic Settings」 > 「TCP/IP」でDNS サーバーの設定を行ってください。

### 手順:

 「Configuration」>「Network」>「Basic Settings」>「TCP/IP」を選択して、 IPv4 アドレス、IPv4 サブネットマスク、IPv4 デフォルトゲートウェイ、および 優先DNS サーバを設定します。

お知らせ: 詳細については、「7.1.1 TCP/IP 設定」を参照してください。

- 2. 「Configuration」 > 「Network」 > 「Basic Settings」 > 「Email」を選択します。
- 3. 以下の設定を行います。

「Sender I: メール送信者の名前

「Sender's Address」: 送信者の電子メールアドレス

「SMTP Server」: SMTP サーバーのIP アドレスまたはホスト名

(例: smtp.263xmail.com)

「SMTP Port」: SMTP のデフォルトのTCP/IP ポートは25 です(セキュアではありません)。SSL SMTP ポートは465 です。

「Email Encryption」:「None」、「SSL」、「TLS」を選択できます。SSL またはTLSを選択し、STARTTLSを無効にすると、SSL またはTLSで暗号化された後に電子メールが送信されます。SMTPポートは、この暗号化方法のために465として設定する必要があります。SSL またはTLSを選択し、STARTTLSを有効にすると、STARTTLSで暗号化された電子メールが送信され、SMTPポートは25に設定されます。

お知らせ: STARTTLS を使用する場合は、お使いの電子メールサーバーでプロトコルがサポートされていることを確認してください。プロトコルが電子メールサーバーでサポートされていない場合に「STARTTLS を有効にする」チェックボックスをオンにすると、電子メールは暗号化されません。

「Attached Image」: アラーム画像が添付されたメールを送信する場合は、添付画像のチェックボックスにチェックを入れます。

「Interval」: 添付画像を送信する2つのアクションの間の時間

「Authentication」: 電子メールサーバーで認証が必要な場合は、このチェックボックスをオンにし、認証を使用してこのサーバーにログインし、ログインユーザー名とパスワードを入力します。



● プライバシーを守り、セキュリティリスクからシステムを保護するため に、すべての機能およびネットワークデバイスに強力なパスワードを 使用することを強く推奨します。パスワードは、製品のセキュリティを 強化するために、8 文字以上(大文字、小文字、数字、特殊文字の3 つ以上を含む)に設定してください。 「Receiver」テーブル: メールの送信先の受信者を選択します。最大3つの受信者を設定できます。

「Receiver」: 通知するユーザーの名前

「Receiver's Address」: 通知するユーザーのメールアドレス

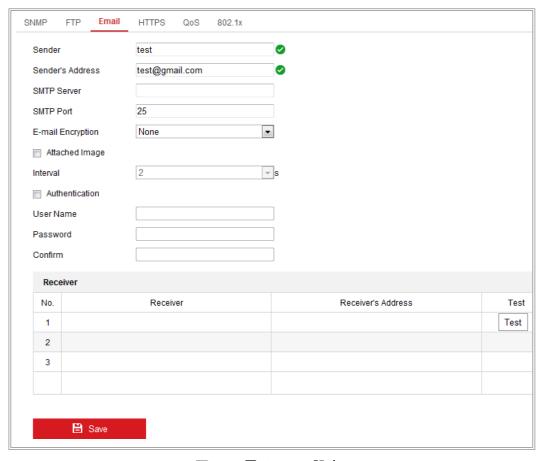


図7-10 電子メール設定

4. 「Save」をクリックし、設定を保存します。

### 7.2.4 プラットフォームアクセス

### 目的:

プラットフォームアクセスには、プラットフォーム経由でデバイスを管理するオプションがあります。

### 手順:

- 1. 「Configuration」>「Network」>「Advanced Settings」>「Platform Access」を選択します。
- 2. 「Enable」チェックボックスをオンにし、デバイスのプラットフォームアクセス機能を有効にしてください。
- 3. 「Platform Access Mode」を選択します。

「Platform Access Mode」を「Ehome」として選択した場合は、

- 1) 「Enable」チェックボックスをオンにします。
- 2) サーバーアドレス、ポート、デバイスID、およびキーを入力します。
- 4. 「Save」をクリックし、設定を保存します。

### 7.2.5 ワイヤレスダイヤル

### 目的:

音声、映像およびデータストリームは、3G/4G ワイヤレスネットワーク経由で転送できます。

### お知らせ:

- 特定のモデルのみがこの機能をサポートしています。
- ワイヤレスダイヤル対応のカメラは、PPPoEに対応していません。

### 手順:

- 1. 「Configuration」〉「Network」〉「Advanced Setting」〉「Wireless Dial」を選択します。
- 2. チェックボックスをオンにし、ワイヤレスダイヤル設定を有効にします。
- 3. ダイヤルパラメータを設定します。
  - 1) ドロップダウンリストからダイヤルモードを選択します。自動と手動を選択できます。「Auto」が選択されている場合は、ダイヤリングのアーミングスケジュールを設定できます。「Manual」が選択されている場合は、オフライン時間と手動ダイヤリングパラメータを設定できます。
  - 2) アクセス番号、ユーザー名、パスワード、APN、MTU、検証プロトコルを設定します。また、これらのパラメータを空白のままにしておくと、他のパラメータを 設定した後に、デバイスはダイヤル用のデフォルト設定を採用します。
  - 3) ドロップダウンリストからネットワークモードを選択します。オート、3G、4G が選択可能です。「Auto」を選択した場合、ネットワーク選択の優先順位は4G > 3G > 有線ネットワークの順になります。
  - 4) ダイヤルモードで「Manual」を選択した場合は、オフライン時間を入力します。
  - 5) UIM番号(携帯電話番号)を入力します。
  - 6) 「Auto」がダイヤルモードとして選択されている場合は、「Edit」をクリックして アーミングスケジュールを設定します。
  - 7)「Save」をクリックし、設定を保存します。

- 4. ダイヤルの状態を表示します。
  - 1) 「Refresh」をクリックすると、リアルタイムモード、UIMステータス、信号強度などを含むダイヤルステータスが表示されます。
  - 2) ダイヤルモードとして「Manual」を選択した場合は、ワイヤレスネットワークを手動で接続/切断することもできます。
- 5. ホワイトリストを設定します。ホワイトリストの携帯電話番号は、デバイスから アラームメッセージを受信し、SMS 経由でデバイスを再起動できます。
  - 1) 「Enable SMS Alarm」チェックボックスをオンにします。
  - 2) ホワイトリストで項目を選択し、Editボタンをクリックします。
  - 3) ホワイトリストの携帯電話番号を入力し、Reboot via SMSのチェックボックスをオンにし、SMSプッシュのアラームを選択して「OK」をクリックします。 お知らせ: SMS 経由でデバイスを再起動するには、デバイスに「reboot」というメッセージを送信します。デバイスは、再起動が成功した後に「reboot success」というメッセージを返します。
  - 4) 「Send Test SMS」をクリックして、テスト用のメッセージを携帯電話に送信できます。
  - 5) 「Save」をクリックし、設定を保存します。

### 7.2.6 HTTPS 設定

### 目的:

HTTPS は、中間者攻撃からウェブサイトを保護し、関連するウェブサーバーの認証を提供します。

### お知らせ:

- プラグインフリーライブビューに対応しているカメラの場合、HTTPSを使用してカメラを操作するときは、ライブビュー用のWebsocketsを有効にする必要があります。「Configuration」>「Network」>「Advanced Settings」>「Network Service」を選択します。
- デフォルトでHTTPS が有効になっている場合、カメラは自動的に符号なし証明書を作成します。HTTPS経由でカメラをご覧になると、Webブラウザから証明書発行のお知らせが出されます。通知を取り消すために、カメラに署名済み証明書をインストールします。

### 手順:

- 1. 「Configuration」 > 「Network」 > 「Advanced Settings」 > 「HTTP」を選択します。
- 2. HTTP またはHTTPS プロトコル経由でカメラにアクセスするには、「Enable」をオンにします。
- 3. HTTPS プロトコル経由でのみカメラにアクセスするには、「Enable HTTPS Browsing」チェックボックスをオンにします。



図7-11 HTTPS 設定画面

4. 自己署名証明書または認可証明書を作成します。

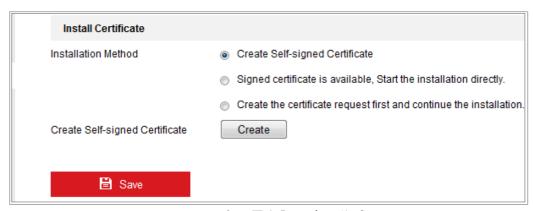


図7-12 自己署名証明書の作成

- 自己署名証明書を作成する
- (1) インストール方法として「Create Self-signed Certificate」を選択します。
- (2)「Create」をクリックして、作成画面を入力します。
- (3) 国、ホスト名/IP、有効性、およびその他の情報を入力します。
- (4)「OK」をクリックし、設定を保存します。

*お知らせ:* すでに証明書がインストールされている場合、「自己署名証明書の作成」はグレー表示になります。

- 要求を作成し、認定証明書をインポートする
- (1) 最初に証明書要求の作成を選択し、インストール方法としてインストールを 続行します。
- (2)「Create」をクリックして、証明書要求を作成します。ポップアップウィンドウで必要な情報を入力します。
- (3)「Download」をクリックして証明書要求をダウンロードし、署名のために信頼できる認証局に送信します。

- (4) 署名された有効な証明書を受け取った後、2つの方法で証明書をインポートすることができます:
  - a) 署名済み証明書が使用可能を選択し、インストールを直接開始します。Browse と Install(参照とインストール)をクリックして、証明書をデバイスにインポートします。

Install Certificate	
Installation Method	Create Self-signed Certificate
	<ul> <li>Signed certificate is available, Start the installation directly.</li> </ul>
	<ul> <li>Create the certificate request first and continue the installation.</li> </ul>
Install Signed Certificate	Browse Install
Save	

図7-13 証明書のインポート(1)

b) 最初に証明書要求の作成を選択し、インストールを続行します。 「Browse」と「Install」をクリックし、証明書をデバイスにインポートします。

Install Certificate	
Installation Method	Create Self-signed Certificate
	<ul> <li>Signed certificate is available, Start the installation directly.</li> </ul>
	<ul> <li>Create the certificate request first and continue the installation.</li> </ul>
Create Certificate Request	Create C=CN, H/IP=10.11.11.111
Download Certificate Request	Download
Delete Certificate Request	Delete
nstall Generated Certificate	Browse Install

図7-14 証明書のインポート(2)

5. 証明書の作成とインストールが正常に完了すると、証明書情報が表示されます。



図7-15 インストール済み証明書

6. デバイスをクライアントソフトウェアに追加するときに、検証のために証明書をエクスポートして保存します。

### お知らせ:

エクスポートした証明書は、PCクライアントにデバイスを追加する前に、クライアントソフトウェアの証明書フォルダに保存する必要があります。

7. 「Save」をクリックし、設定を保存します。

### 7.2.7 QoS 設定

### 目的:

QoS(Quality of Service)は、データ送信の優先順位を設定することにより、ネットワークの遅延や混雑の解決に役立ちます。

### 手順:

1. 「Configuration」 > 「Network」 > 「Advanced Setting」 > 「QoS」を選択します。

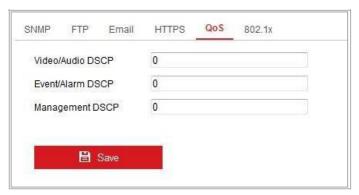


図7-16 QoS 設定

2. 「Video/Audio DSCP」、「Event/Alarm DSCP」、および「Management DSCP」を含むQoS 設定をします。

DSCPの有効値の範囲は0~63です。DSCP値が大きいほど優先度が高くなります。

*お知らせ:* DSCP はDifferentiated Service Code Point を参照し、DSCP 値はIP ヘッダーでデータの優先順位を示すために使用されます。

3. 「Save」をクリックし、設定を保存します。

**お知らせ**: 設定を有効にするには、再起動が必要です。

### 7.2.8 802.1X の設定

### 目的:

IEEE 802.1X 規格はネットワークカメラでサポートされており、機能が有効な場合、IEEE 802.1X で保護されているネットワークにカメラを接続する際に、カメラデータが確保され、ユーザー認証が必要になります。

### 準備:

認証サーバーを設定する必要があります。802.1Xのユーザー名とパスワードをサーバーに登録してください。



● プライバシーを守り、セキュリティリスクからシステムを保護するために、 すべての機能およびネットワークデバイスに強力なパスワードを使用す ることを強く推奨します。パスワードは、製品のセキュリティを強化するた めに、8 文字以上(大文字、小文字、数字、特殊文字の3つ以上を含む) に設定してください。

### 手順:

1. 「Configuration」〉「Network」〉「Advanced Settings」〉「802.1X」を選択します。

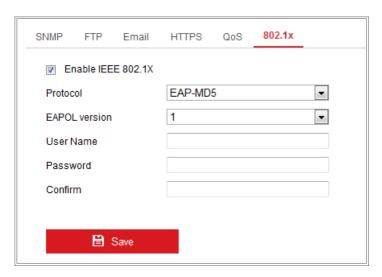


図 7-17 802.1X の設定

2. 「Enable IEEE 802.1X」チェックボックスをオンにし、機能を有効にします。

3. 「Protocol」、「EAPOL version」、「User Name」、「Password」などの802.1Xを設定します。

*お知らせ:* EAPOL versionは、ルーターまたはスイッチのバージョンと同じである必要があります。

- 4. サーバーにアクセスするためのユーザー名とパスワードを入力します。
- 5. 「Save」をクリックし、設定を保存します。

**お知らせ**: 設定を有効にするには、再起動が必要です。

### 7.2.9 統合プロトコル

### 目的:

ONVIFプロトコルを介してデバイスにアクセスする必要がある場合は、この画面で ONVIFユーザーを設定できます。詳細なコンフィギュレーションルールについては、 ONVIF規格を参照してください。

#### ONVIF

#### 手順:

- 1. 「Enable ONVIF」チェックボックスをオンにして、機能を有効にします。 ONVIF ユーザーを追加します。最大32人のユーザーが追加できます。 ユーザー名とパスワードを設定し、パスワードを確認します。ユーザー は、メディアユーザー、オペレーターおよび管理者として設定できます。 お知らせ: ONVIF ユーザーアカウントはカメラユーザーアカウントとは 異なります。ONVIF ユーザアカウントを個別に設定しておきます。
- 2. 設定を保存します。

お知らせ: カメラを復元すると、ONVIF のユーザー設定はクリアされます。

### 7.2.10 帯域幅適応

この機能を有効にすると、カメラのパフォーマンスのうち、ライブビューの品質が優先されます。カメラはビデオ関連のパラメータを自動的に調整し、事前設定されたビデオ関連の設定は無効になります。機能を有効にするには、再起動が必要です。 *お知らせ*: 帯域幅の適応は、特定のカメラモデルでのみ使用できます。

### 7.2.11 ネットワークサービス

カメラが対応している特定のプロトコルのON/OFFを制御できます。

#### お知らせ:

- セキュリティ上の懸念から、使用しない機能はOFFのままにしてください。
- 対応機能はカメラの機種により異なります。

### WebSocket とWebSocketプロトコル

Google Chrome 57以降のバージョンまたはMozilla Firefox 52以降のバージョンを使用してカメラを訪れる場合は、WebSocketまたはWebSocketsプロトコルを有効にする必要があります。ライブビュー、画像キャプチャ、デジタルズーム機能が使用できません。

カメラがHTTP を使用している場合は、WebSocket を有効にします。 カメラがHTTPS を使用している場合は、WebSockets を有効にします。

### SDKサービスと拡張SDKサービス

デバイスをクライアントソフトウェアに追加する場合は、SDK Service または Enhanced SDK Service を有効にする必要があります。

「SDK Service」: SDKプロトコルを使用します。

「Enhanced SDK Service」: SDK over TLS プロトコルが使用されます。デバイスとクライアントソフトウェア間の通信は、TLS (Transport Layer Security)プロトコルを使用して保護されます。

### 「TLS (Transport Layer Security)」

デバイスはTLS 1.1 およびTLS 1.2 を提供します。必要に応じて、1つ以上のプロトコルバージョンを有効にします。

### 7.2.12 スムーズなストリーミング

### 目的:

ネットワークが不安定なときや高品質な映像が必要なときに、スムーズストリーミング機能を有効にすると、クライアントソフトウェアやWeb ブラウザでライブビューをスムーズに見ることができます。

### 準備:

スムーズストリーミング機能を設定する前に、クライアントソフトウェアにデバイスを追加し、クライアントソフトウェアでNPQプロトコルを選択します。

### 手順:

1. 「Configuration」>「Network」>「Advanced Settings」>「Smooth Streaming」を 選択します。

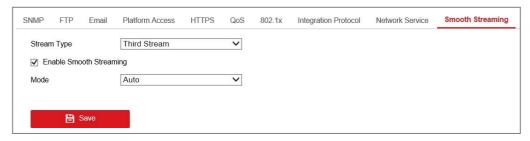


図7-18 スムーズストリーミングの設定

- 2. ストリームタイプを選択します。
- 3. 「Enable Smooth Streaming」をオンにします。

お知らせ: この機能を有効にする前に、「Bitrate Type」が「Constant」として選択され、「SVC」が「OFF」に設定されていることを確認してください。「Configuration」 > 「Video/Audio」 > 「Video」を選択し、パラメータを設定します。

4. スムーズストリーミングのモードを選択します。「Auto」、「Resolution Priority」、「Error Correction」の3 つのモードが選択可能です。

「Auto」:解像度とビットレートが自動的に調整され、解像度が優先されます。これら2つのパラメータの上限は、「Video」画面で設定した値を超えることはありません。「Configuration」>「Video/Audio」>「Video」を選択し、「Resolution」と「Max」を設定します。スムーズストリーミング機能を有効にする前にビットレートを設定します。このモードでは、フレームレートは自動的に最大値に調整されます。

「Resolution Priority」:解像度は「Video」で設定した値のままで、ビットレートは自動的に調整されます。「Configuration」>「Video/Audio」>「Video」を選択し、設定を「Max」にしてください。スムーズストリーミング機能を有効にする前にビットレートを設定してください。このモードでは、フレームレートは自動的に最大値に調整されます。

「Error Correction」: 解像度とビットレートは、「Video」で設定した値と同じになります。帯域幅が十分な場合、送信中にパケットロスやビットエラーが発生し、ビデオデータのエラーや損失につながる可能性があります。このモードは、画像品質を確保するために、転送中のデータエラーを修正するために使用されます。エラー訂正比率は0~100の範囲で設定できます。比率が0の場合、データ再送でデータエラーを修正します。比率が0より大きい場合、ストリームに追加された冗長データとデータ再送信によってエラーデータが修正されます。値が大きいほど、生成される日付の冗長性が高くなり、修正されるデータエラーが増え、必要な帯域幅が大きくなります。比率が100の場合、冗長データは元のデータと同じ大きさになり、帯域幅が2倍必要になります。

*お知らせ:* 「Error Correction」モードでは、帯域幅が十分であることを確認してください。

5. 「Save」をクリックし、設定を保存します。

# 第8章 ビデオ/オーディオ設定

### 目的:

以下の手順で映像設定、音声設定、ROI、ストリームの情報表示などを行います。

# 8.1 ビデオ設定

特定のカメラモデルでは、メインストリーム、サブストリームなど、使用可能なビデオストリームのパラメータを設定できます。さらに必要に応じて、追加のビデオストリームをカスタマイズすることもできます。

- 「Video」画面で、使用可能なビデオストリームを設定します。
- 「Custom Video」画面で、ビデオストリームを追加します。」

### 8.1.1 ビデオ設定

### 手順:

1. 「Configuration」>「Video/Audio」>「Video」を選択します。

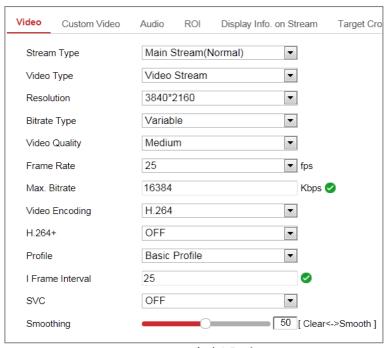


図8-1 ビデオ設定

2. 「Stream Type」を選択します。

サポートされているストリームタイプがドロップダウンリストに表示されます。

#### お知らせ:

- 一部のモデルでは、デフォルトで「Third Stream」が有効になっていません。
   機能を有効にするには、「System」 > 「Maintenance」 > 「System Service」 > 「Software」を選択します。
- メインストリームは通常、良好な帯域幅で録画およびライブビュー用に使用されます。帯域幅が制限されている場合はサブストリームをライブビュー用に使用してください。
- 3. 選択したストリームタイプの次のパラメータをカスタマイズできます。

### 「Video Type」:

ビデオストリーム、またはビデオとオーディオのコンポジットストリームのストリームタイプを選択します。Video Type がVideo & Audio の場合のみ、音声信号が録画されます。

#### Resolution I:

ビデオ出力の解像度を選択します。

### 「Bitrate Type」:

定数または可変にするビットレートタイプを選択します。

#### [Video Quality]:

「Bitrate type」を「Variable」に選択した場合、6 段階の画質を選択できます。

#### Frame Rate J:

フレームレートを設定します。フレームレートは、ビデオストリームが更新され、1秒あたりのフレーム数(fps)で測定される周波数を指定します。ビデオストリームに動きがある場合は、イメージ品質が維持されるため、フレームレートを高くすると便利です。

#### 「Max. Bitrate I:

最大ビットレートを32~16384 Kbps の範囲で設定します。値が大きいほど映像 品質は高くなりますが、帯域幅は高くなります。

*お知らせ:* 最大ビットレート値の最大制限は、さまざまなカメラプラットフォームによって異なります。特定のカメラでは、最大制限は8192 Kbps または12288 Kbps です。

### [Video Encoding]:

本機は、H.264、H.265、MJPEG、MPEG4などの複数のビデオエンコーディングタイプをサポートしています。サポートされるエンコーディングタイプは、ストリームタイプによって異なる場合があります。H.265 は新しいエンコード技術で、H.264 と比べると、同じ解像度・フレームレート・画質でも、伝送ビットレートを低減することができます。

*お知らせ:* 選択可能なビデオエンコードタイプは、異なるカメラモードによって 異なる場合があります。

#### TH.264+ / H.265+: I:

- 「H.264+」: メインストリームをストリームタイプに、H.264 をビデオエンコーディングに設定すると、H.264+が使用可能になります。H.264+は、H.264 に基づく改良された圧縮コーディングテクノロジです。H.264+を有効にすると、ユーザーは最大平均ビットレートでHDD 消費量を見積もることができます。H.264+は、H.264と比較して、ほとんどのシーンで同じ最大ビットレートでストレージを最大50%削減します。
- 「H. 265+」: メインストリームをストリームタイプに、H.265 をビデオエンコーディングに設定すると、H.265+が使用可能になります。H.265+は、H.265 に基づく改良された圧縮コーディングテクノロジです。H.265+ を有効にすると、ユーザーは最大平均ビットレートでHDD 消費量を見積もることができます。H.265+は、H.265 と比較して、ほとんどのシーンで同じ最大ビットレートでストレージを最大50%低減します。

H.264+/H.265+の電源をオンまたはオフにする場合は、カメラを再起動する必要があります。H.264+ からH.265+ に直接切り替えた場合、およびその逆の場合は、システムで再起動は必要ありません。

#### お知らせ:

- 互換性があるためにライブビューや再生が正常に動作しない場合は、ビデオプレーヤーを最新バージョンにアップグレードしてください。
- H.264+/H.265+ を有効にすると、プロファイル、I フレーム間隔、ビデオ品質、 SVC などのパラメータがグレー表示されます。
- H.264+/H.265+を有効にすると、一部の機能はサポートされません。これらの 設定では、対応する画面は非表示になります。
- H.264+/H.265+は、設定された最大平均ビットレートを長期的に実現するために、実際のシーンの要求に応じてビットレート分布を自発的に調整できます。カメラは、固定のモニタリングシーンに適応するために、少なくとも24時間必要です。

### 「Max. Average Bitrate」:

最大ビットレートを設定すると、推奨の最大ビットレート値が最大平均ビットレート欄に表示されます。最大平均ビットレートは、手動で32 Kbps から最大ビットレートの値に設定することもできます。

#### 「Profile 」:

ビデオエンコーディングとしてH.264 またはH.265 を選択した場合、プロファイル を設定できます。選択可能なプロファイルは、モデルによって異なります。

### 「I Frame Interval」:

1 から400 に設定します。

### [SVC]:

SVC(Scalable Video Coding)は、H.264/AVC およびH.265 規格の拡張版です。 SVC 機能を無効/ 有効にするには、OFF/ON を選択します。「Auto」を選択する と、ネットワーク帯域幅が不足した場合に、ビデオから自動的にフレームを抽出します。

### 「Smoothing」:

ストリームの滑らかさを表します。スムージングの値が高いほど、ストリームの流動性は良くなりますが、映像が粗く見える場合があります。

4. 「Save」をクリックし、設定を保存します。

### お知らせ:

ビデオパラメータは、モデルによって異なります。カメラの機能については、実際の表示ページを参照してください。

### 8.1.2 カスタムビデオ

必要に応じて、追加のビデオストリームを設定できます。カスタムビデオストリームの場合、ライブビューできますが、録画や再生はできません。

### お知らせ:

- カスタムビデオ機能にはカメラのサポートが必要です。
- カメラのリストアアクションの後(初期設定に戻さない)、カスタムビデオストリームの数量とその名前は維持されますが、関連するパラメータは復元されます。

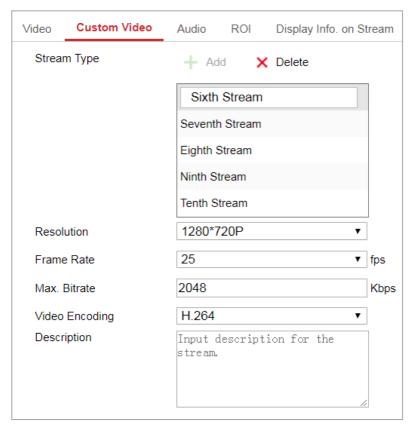


図8-2 カスタムビデオ設定

### 手順:

- 1. 十 をクリックしてストリームを追加します。
- 2. 必要に応じてストリーム名を変更します。

*お知らせ:* ストリーム名には最大32 文字の英字と記号(&、<、>、'、"を除く) を使用できます。

- 3. ストリームパラメータ(解像度、フレーム保持、最大ビットレート、ビデオエンコード)をカスタマイズします。パラメータの導入については、「8.1.1 ビデオ設定」を参照してください。
- 4. ストリームの説明を追加する必要があります。
- 5. カスタムストリームが必要ない場合は、**×**をクリックして削除します。
- 6. 設定を保存します。

## 8.2 オーディオ設定

### 手順:

1. 「Configuration」>「Video/Audio」>「Audio」を選択します。

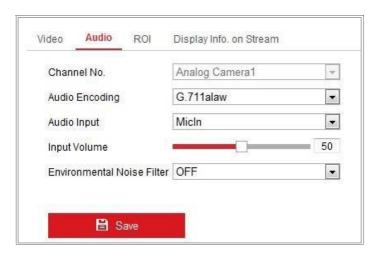


図8-3 オーディオ設定

2. 以下の設定をします。

お知らせ: オーディオ設定は、異なるカメラモデルによって異なります。

「Audio Encoding」: G.722.1、G.711 ulaw、G.711alaw、G.726、MP2L2、PCM、MP3から選択できます。MP2L2では、サンプリングレートとオーディオストリームビットレートを設定できます。PCMの場合、サンプリングレートを設定できます。

「Audio Input」:接続したマイクとピックアップにそれぞれMicIn とLineIn を選択できます。

「Input Volume」: 0~100の間で調整できます。

「Environment Noise Filter」: OFF またはON に設定します。この機能を有効にすると、ある程度環境内のノイズをフィルタリングできます。

3. 「Save」をクリックし、設定を保存します。

# 8.3 ROIエンコーディングの設定

### 目的:

ROI(選択的領域)符号化は、ビデオ圧縮におけるROIと背景情報を識別するのに役立ちます。選択的領域により多くの符号を割り当て、それによりROIの品質を向上させる一方で、背景情報はあまり焦点を絞らないことを意味します。

お知らせ: ROI 機能は、モデルによって異なります。

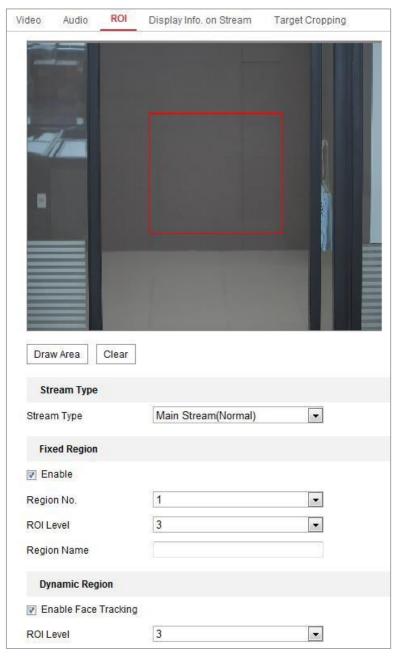


図8-4 ROIエンコーディングの設定

#### 手順:

- 1. 「Configuration」>「Video/Audio」>「ROI」を選択します。
- 2. ROI エンコーディングのストリームタイプを選択します。
- 3. 「Fixed Region」の「Enable」チェックボックスをオンにします。
- 4. ROI の固定領域を設定します。ROI に固定領域を設定します。
  - (1) ドロップダウンリストから地域番号を選択します。
  - (2) 選択した地域のROI 機能を有効にするには、「Enable」チェックボックスをオンにします。
  - (3) 「Drawing]をクリックします。ビュー画面上でマウスをクリックしてドラッグすると、ROI 領域として赤い長方形が描画されます。「Clear」をクリックすると、元の描画をキャンセルできます。終了したら、「Stop Drawing」をクリックします。
  - (4) ROI レベルを選択します。
  - (5) 選択した地域の地域名を入力します。
  - (6)「Save」をクリックし、固定領域の設定を保存します。
  - (7) 上記(1)~(6)を繰り返して、他の固定領域を設定します。
- 5. ROI のダイナミックリージョンを設定します。
  - (1) 顔認識を有効にするには、チェックボックスをオンにします。

*お知らせ:* 顔認識機能を有効にするには、顔検出機能をサポートし、有効にする必要があります。

- (2) ROI レベルを選択します。
- 6. 「Save」をクリックし、設定を保存します。

*お知らせ:* ROI レベルとは、画質を向上させるレベルのことです。値が大きいほど画質が良くなります。

## 8.4 ストリーム上の情報表示

「Enable Dual-VCA」のチェックボックスをオンにすると、オブジェクト(人間や車両など)の情報がビデオストリームにマークされます。その後、接続されたデバイスにルールを設定し、通過・侵入などのイベントを検出できます。



図8-5 ストリーム上の情報表示

## 8.5 ターゲットクロッピングの設定

#### 目的:

ライブビデオのターゲットエリアを指定し、指定したビデオエリアを特定の解像度で3番目のストリーム経由で表示して、必要に応じてターゲットエリアの詳細を表示できます。

お知らせ: ターゲット切り出し機能は、モデルによって異なります。

- 1. 「Target Cropping」設定画面を入力します。
- 2 「Enable Target Cropping」チェックボックスをオンにし、機能を有効にします。
- 3. ストリームタイプとして「Third Stream」を設定します。
- 4. 対象領域のビデオ表示の切り出し解像度を選択します。ライブビデオに赤い 長方形が表示され、ターゲット領域をマークします。この長方形をクリックして ドラッグし、目的のターゲット領域を見つけることができます。
- 5. 「Save」をクリックし、設定を保存します。

# 第9章 画像設定

#### 目的:

この章では、ディスプレイ設定、OSD 設定、プライバシーマスク、画像オーバーレイ、画像パラメータスイッチなどの画像パラメータの設定を説明します。

# 9.1 ディスプレイ設定

#### 目的:

画像調整、露出設定、日中/夜間スイッチ、バックライト設定、ホワイトバランス、画像強調、ビデオ調整およびその他のパラメータをディスプレイ設定で設定します。 *お知らせ:*表示パラメータは、モデルによって異なります。詳細は実際の画面をご

#### 手順:

参照ください。

1. 「Configuration」 > 「Image」 > 「Display Settings」を選択します。



図9-1 ディスプレイ設定

2. シーンを選びます。

3. カメラの画像パラメータを設定します。

#### ● 「Image Adjustment」

「Brightness」は、画像の明るさを表します。値の範囲は1~100です。

「Contrast」は、イメージのコントラストを表します。値の範囲は1~100です。

「Saturation」は、画像カラーの彩度を表します。値の範囲は1~100です。

「Sharpness」は、画像のエッジコントラストを表します。値の範囲は1~100です。

#### ● 「Exposure Settings」

このカメラに固定レンズが搭載されている場合は、「Manual」のみが選択可能で、アイリスモードは設定できません。

「Auto」を選択すると、オートアイリスのレベルを0~100の範囲で設定できます。「Exposure Time」とは、電子シャッター時間のことで、1~1/100,000sの範囲です。実際の輝度条件に合わせて調整してください。

画像の「Gain」は、0~100の範囲で設定することができます。値が大きいほど画像が明るくなり、ノイズが大きく増幅されます。

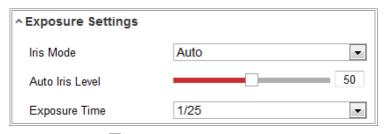


図9-2 Exposure Settings

#### ● 「Focus」

カメラ対応のモーター駆動レンズでは、フォーカスモードを「Auto」、「Manual」、「Semi-Auto」に設定できます。

「Auto」: 実際のモニターシナリオに合わせて、カメラのフォーカスが自動的に調整されます。

「Manual」: ズーム、フォーカス、レンズの初期化および補助フォーカスを手動で調整します。

「Semi-Auto」: ズームを調整すると、カメラは自動的にフォーカスします。

#### ● 「Day/Night Switch」

監視する状況に応じて、昼夜切り換えモードを選択します。デイナイト、オート、スケジュールスイッチ、アラーム入力による動作は、Day/Night Switchで選択することができます。



図9-3 Day/Night Switch

「Day」: カメラは日中モードのままです。

「Night」: カメラは夜間モードのままです。

「Auto」: 自動的に照度に応じて日中モードと夜間モードが切り換わります。感度の範囲は0~7で、値が大きいほどモードが切り換わりやすくなります。「Filtering Time」は、日中/夜間の切り換えのインターバル時間のことで、5秒から120秒で設定できます。

「Scheduled-Switch」: 開始時刻と終了時刻を設定して、日中/夜間モードの期間を設定します。

「Triggered by alarm input」: アラーム入力によりモードが切り換わります。日中または夜間に設定できます。

「Smart Supplement Light」: サプリメントライトON に設定し、ライトモードはオートとマニュアルが選択可能です。

「Auto」を選択すると、補助光が実際の輝度に応じて変化します。例えば、現在のシーンが十分に明るい場合、補助光を低出力に調整し、シーンに十分な明るさがない場合、補助光の出力を高く調整します。

「Manual」を選択すると、距離を調整してサプリメントを設定できます。例えば、物体がカメラの近くにある場合、デバイスは補助光を調整して出力を下げ、物体が遠くにある場合は補助光の出力が高くなります。

#### • 「Backlight Settings」

「BLC Area」: 強いバックライトをかけて物体に焦点を当てると暗すぎて見えにくくなります。BLC は、前面のオブジェクトの光を補正して明瞭にします。

「OFF」、「Up」、「Down」、「Left」、「Right」、「Center」、「Auto」、「Custom」が選択できます。

お知らせ: BLC モードが「Custom」に設定されている場合、ライブビュー画像上にBLC 領域として赤い四角形を描くことができます。

「WDR」: ワイドダイナミックレンジは、シーンの明るい領域と暗い領域のコントラストが高い場合に使用できます。

「HLC」: High Light Compression 機能は、画質に影響するシーンに強いライトがある場合に使用できます。

#### 「White Balance」

環境に応じて色温度を調整するためのカメラの補正機能です。



図9-4 White Balance

#### • 「Image Enhancement」

「Digital Noise Reduction」: DNR はビデオストリームのノイズを低減します。「OFF」、「Normal」、「Expert」が選択可能です。「Normal」モードでは、DNR レベルを0~100の範囲で設定します。「Expert」モードでは、空間DNR レベル[0-100] と時間DNR レベル[0-100] の両方からDNR レベルを設定します。

「Defog Mode」: 環境が曇っていて、画像が不鮮明な場合に、Defog 機能を有効にすることができます。画像がより明確に表示されます。

「EIS (Electrical Image Stabilizer)」: EIS (電気的手ぶれ補正)は、ビデオの振動の影響を軽減します。

「Gray Scale」: グレイスケールの範囲を[0-255] または[16-235] から選択できます。

#### 「Video Adjustment」

れます。

「Mirror」: イメージを反転して見えるように調整します。「Left/Right」、「Up/Down」、「Center」、「OFF」を選択できます。

「Rotate」: 16:9 のアスペクト比を完全に活用するための回転機能取り付けるときは、カメラを 90 度に回すか、3 軸レンズを 90 度に回転させ、回転モードをオンに設定すると、9:16 アスペクト比のシーンの通常のビューが表示され、壁などの不要な情報が無視され、シーンのより意味のある情報が得ら

「Scene Mode」: 実際の環境に応じて、屋内または屋外としてシーンを選択します。

「Video Standard」: さまざまなビデオ規格に応じて「50Hz」と「60Hz」が選択可能です。通常、PAL 規格は50Hz、NTSC 規格は60Hz です。

「Lens Distortion Correction」: モーター駆動レンズを装備したカメラでは、画像がある程度歪んで見えることがあります。この機能を有効にすることで、レンズの歪みを補正することができます。

#### その他

一部のカメラモデルでは、CVBS、SDI、またはHDMI 出力をサポートしています。 ローカル出力のON/OFFは、実機に合わせて設定してください。

## 9.2 OSD 設定

#### 目的:

ライブビューに表示されるカメラ名、時刻/日付の形式、表示モード、OSDサイズをカスタマイズできます。



図9-5 OSD 設定

- 1. 「Configuration」 > 「Image」 > 「OSD Settings」を選択します。
- 2. 目的の「Character Set」を選択します。
- 3. 該当するチェックボックスをオンにすると、必要に応じてカメラ名、日付または 週の表示が選択されます。
- 4. カメラ名のテキストボックスでカメラ名を編集します。
- 5. ドロップダウンリストから時刻形式と日付形式を選択します。
- 6. ドロップダウンリストから選択して、表示モード、OSDサイズ、OSD色を設定します。
- 7. テキストオーバーレイ設定をします。

- (1) テキストボックスの前にあるチェックボックスをオンにすると、オンスクリー ン表示が有効になります。
- (2) テキストボックスに文字を入力します。

**お知らせ**: 最大8つのテキストオーバーレイを設定できます。

- 8. OSD の位置と位置合わせを調整します。
- 9. 選択して文字を揃えることができます。選択して文字を揃えた場合、左右の 余白と上下の余白を設定できます。
  - 0~2文字は使用できません。カスタムを選択すると、マウスを使用してライブビューウィンドウのテキストフレームをクリックしてドラッグし、位置を調整できます。
- 10.「Save」をクリックし、設定を保存します。

## 9.3 プライバシーマスクの設定

#### 目的:

プライバシーマスクを使用すると、ライブビデオの特定の領域をカバーして、監視領域の特定のスポットがライブで表示および録画されるのを防ぐことができます。

- 1. 「Configuration」 > 「Image」 > 「Privacy Mask」を選択します。
- 2 「Enable Privacy Mask」チェックボックスをオンにし、機能を有効にします。
- 3. 「Draw Area」をクリックします。

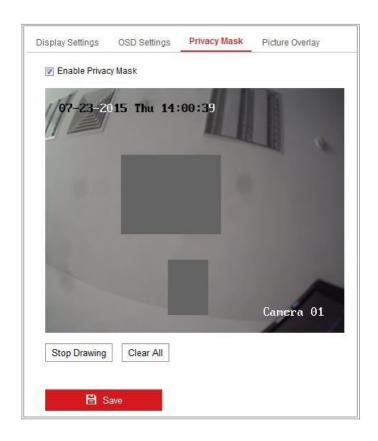


図9-6 プライバシーマスクの設定

- 4. ライブビデオウィンドウでマウスをクリックしてドラッグし、マスク領域を描画します。
- *お知らせ:* 同じ画像上に最大4/8 の領域を描画することができます。サポートされるエリアの数は、モデルによって異なります。
- 5. 「Stop Drawing」をクリックして描画を終了するか、「Clear All」をクリックすると、 設定した領域を保存せずにすべて消去します。
- 6. 「Save」をクリックし、設定を保存します。

## 9.4 画像オーバーレイの設定

#### 目的:

ピクチャーオーバーレイでは、画像に写真を重ねることができます。この機能により、 特定のエンタープライズまたはユーザーは、画像上にロゴをオーバーレイできます。

#### 手順:

1. 「Configuration」 > 「Image」 > 「Picture Overlay」を選択します。

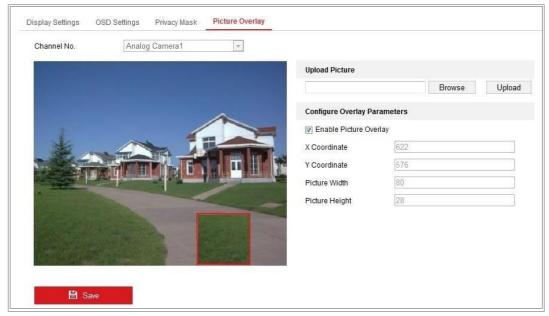


図9-7 ピクチャーオーバーレイ

- 2 「Browse」をクリックして、画像を選択します。
- 3. 「Upload」をクリックしてアップロードします。
- 4. 「Enable Picture Overlay」チェックボックスをオンにし、機能を有効にします。
- 5. 「X Coordinate」と「Y Coordinate」の値を設定すると、画面上の画像の位置を調整できます。画像の幅と高さをお好みのサイズに調整します。
- 6. 「Save」をクリックし、設定を保存します。

*お知らせ:* 画像はRGB24 bmp 形式でなければならず、最大画像サイズは 128\*128 です。

## 9.5 画面切り換えパラメータの設定

#### 目的:

画面切り換えパラメータを使用して、期間とリンクされたシーンを設定できます。また、 対応するチェックボックスをオンにすると、設定した時間内にリンクされたシーンに 移動します。

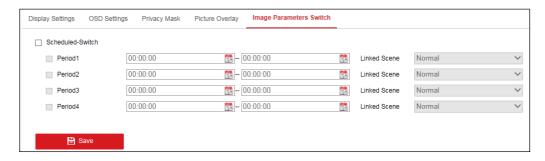


図9-8 画面切り換えパラメータの設定画面

- 1. 「Configuration」 > 「Image」 > 「Image Parameters Switch」を選択します。
- 2. 「Scheduled-Switch」チェックボックスをオンにします。
- 3. 時間周期と連動シーンを設定します。最大4つの周期を設定できます。
- 4. 「Save」をクリックします。

# 第10章 イベント設定

この章では、基本イベントやスマートイベントなどのアラームイベントに対応するようにネットワークカメラを設定する方法について説明します。

## 10.1 基本イベント

モーション検出、ビデオ改ざん、アラーム入力、アラーム出力など、このセクションの指示に従うことで、基本イベントを設定できます。「Notify Surveillance Center」、「Send Email」、「Trigger Alarm Output」などのイベントとの連携方法を設定できます。

*お知らせ:* アラーム発生時にすぐにPC またはモバイルクライアントソフトウェアにアラーム情報を配信する場合は、「Notify Surveillance Center」チェックボックスをオンにします。

### 10.1.1 モーション検出の設定

#### 目的:

モーション検出は、設定された監視領域内の移動物体を検出し、アラーム発生時に 一連のアクションを実行できます。

移動物体を正確に検出し、誤警報率を低減するために、異なる運動検出環境に対して「Normal」設定と「Expert」設定をすることができます。

### ● 「Normal」設定

通常の設定では、昼間と夜間で同じセットの動き検出パラメータを採用します。

#### タスク1: モーション検知領域の設定

#### 手順::

1. 「Configuration」 > 「Event」 > 「Basic Event」 > 「Motion Detection」を選択します。

- 2. 「Enable Motion Detection」チェックボックスをオンにします。
- 3. 検出されたオブジェクトを緑色の四角形でマークする場合は、「Enable Dynamic Analysis for Motion」チェックボックスをオンにします。

*お知らせ:* 検出されたオブジェクトが緑色の長方形で表示されないようにするには、ルールで「無効」を選択します。「Configuration」 > 「Local Configuration」 > 「Live View Parameters-rules」を選択し、ルールで「Disable」を選択します。

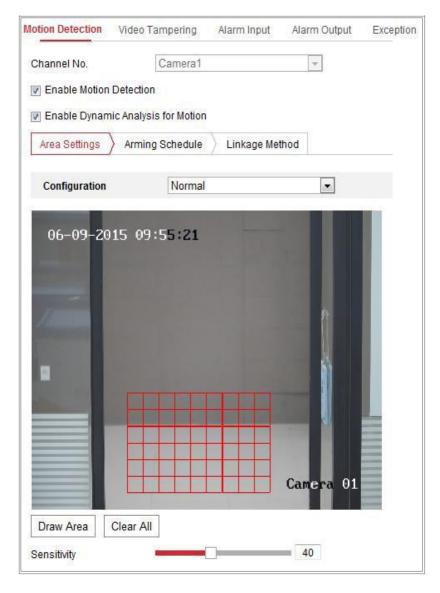


図10-1 モーション検出の有効化

4. 「Draw Area」をクリックします。ライブビデオ上でマウスをクリック・ドラッグして、 モーション検出エリアを描きます。「Stop Drawing」をクリックして、1つの領域の 描画を終了します。

- 5. すべての領域をクリアするには、「Clear All」をクリックします。
- 6. スライダーを動かして、検出の感度を設定します。

#### タスク2: モーション検出のアーミングスケジュールの設定



図10-2 アーミングスケジュール

- 1. 「Arming Schedule」をクリックして、アーミングスケジュールを編集します。
- 2. タイムバーをクリックし、マウスをドラッグして期間を選択します。



図10-3 アーミングスケジュール

お知らせ: 選択した期間をクリックすると、タイムバーを動かすか、正確な期間を入力することによって、期間を希望の時間に調整できます。

- 3. 「Delete」をクリックして現在のアーミングスケジュールを削除するか、「Save」を クリックし、設定を保存します。
- 4. マウスを各日の終わりに動かすと、コピーダイアログボックスがポップアップ 表示され、現在の設定を他の日にコピーできます。
- 5. 「Save」をクリックして設定を保存します。

お知らせ: 各周期の時間は重複できません。1 日に最大8 つの期間を設定できます。

#### タスク3: モーション検出の連携方法の設定

チェックボックスをオンにすると、連動方法を選択できます。音声アラーム、送信メール、監視センター通知、FTP/メモリーカード/NASへのアップロード、トリガ・チャンネル、アラーム出力を選択可能です。イベント発生時の連動方法を指定できます。

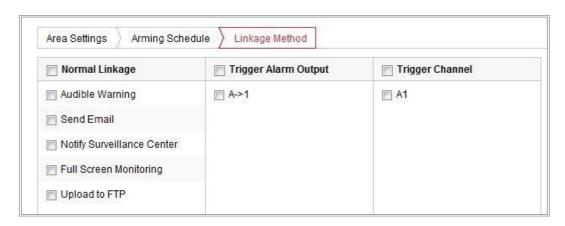


図10-4 連動方法

**お知らせ**: 連動方法は、カメラの機種によって異なります。

#### 「Audible Warning」

アラーム音をローカルで発生させます。また、オーディオ出力を持つデバイスでのみサポートされます。

#### ● 「Send Email」

イベントが発生したときに、アラーム情報を含む電子メールをユーザーに送信します。

お知らせ: イベント発生時に電子メールを送信するには、「7.2.3 Eメール設定の指定」を参照して、事前に電子メールの設定を完了してください。

#### • 「Notify Surveillance Center」

イベントが発生したときに、例外またはアラーム信号をリモート管理ソフトウェア に送信します。

#### ● 「Upload to FTP/Memory Card/NAS」

アラームが発生したときに画像を取り込み、FTPサーバーに画像をアップロードします。

#### お知らせ:

- 最初にFTP アドレスとリモートFTP サーバーを設定します。詳細については、「7.2.2 FTP 設定」を参照してください。
- 「Configuration」>「Storage」>「Schedule Setting」>「Capture」>
  「Capture Parameters」に移動し、イベント連動スナップショットを有効にして、キャプチャ間隔とキャプチャ番号を設定します。
- 取り込んだ画像は、使用可能なSDカードまたはネットワークディスクにアップロードすることもできます。

#### ● 「Trigger Channel」

動きが検出されると、動画が記録されます。この機能を実現するには、録画 スケジュールを設定する必要があります。詳細については、「11.1 レコードス ケジュールの設定」を参照してください。

### • Trigger Alarm Output]

イベントが発生したときに、1つ以上の外部アラームを出力します。

お知らせ: イベント発生時にアラームを出力するには、「10.1.4 アラーム出力の設定」を参照して関連パラメータを設定してください。

### ● 「Expert」設定

「Expert」モードは、主に各エリアのオブジェクトの感度と比率を、異なる日中/夜間で切り換えて設定するために使用されます。

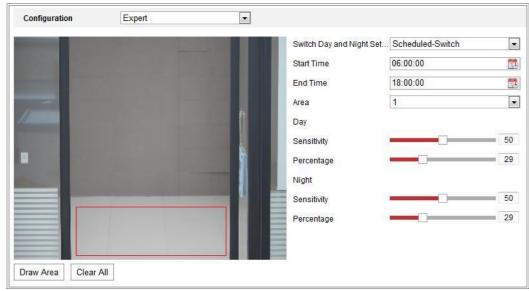


図10-5 モーション検出のExpertモード

#### ● 日中/夜間スイッチOFF

- 1. 通常の設定モードと同様に検出エリアを描画します。最大8つの領域に対応しています。
- 2. 「Switch Day and Night Settings」で「OFF」を選択します。
- 3. エリア番号をクリックしてエリアを選択します。
- 4. カーソルをスライドして、選択した領域のオブジェクトの感度と比率を調整します。
- 5. 通常の設定モードと同様にアーミングスケジュールと連動方法を設定します。
- 6. 「Save」をクリックし、設定を保存します。

#### ● 日中/夜間自動スイッチ

#### 手順:

- 1. 通常の設定モードと同様に、検出エリアを描画します。最大8つの領域に対応しています。
- 2. 「Switch Day and Night Settings」で「Auto-Switch」を選択します。
- 3. エリア番号をクリックしてエリアを選択します。
- 4. カーソルをスライドさせて、昼間の選択したエリアのエリア上のオブジェクト の感度と比率を調整します。
- 5. カーソルをスライドさせて、夜間に選択したエリアのエリア上のオブジェクトの感度と比率を調整します。
- 6. 通常の設定モードと同様にアーミングスケジュールと連動方法を設定します。
- 7. 「Save」をクリックし、設定を保存します。

#### ● 日中/夜間予約スイッチ

- 1. 通常の設定モードと同様に、検出エリアを描画します。最大8つの領域に対応しています。
- 2. 「Switch Day and Night Settings」で「Scheduled-Switch」を選択します。



図10-6 Switch Day and Night Settings

- 3. スイッチタイミングの開始時間と終了時間を選択します。
- 4. エリア番号をクリックしてエリアを選択します。
- 5. カーソルをスライドさせて、昼間の選択したエリアのエリア上のオブジェクト の感度と比率を調整します。
- 6. カーソルをスライドさせて、夜間に選択したエリアのエリア上のオブジェクト の感度と比率を調整します。

- 7. 通常の設定モードと同様にアーミングスケジュールと連動方法を設定します。
- 8. 「Save」をクリックし、設定を保存します。

### 10.1.2 ビデオ改ざんアラームの設定

#### 目的:

レンズが覆われたときにアラームを発し、特定のアラーム応答アクションを実行する ようにカメラを設定できます。

このアラームの検出領域は画面全体です。

- 1. 「Configuration」 > 「Event」 > 「Basic Event」 > 「Video Tampering」を選択します。
- 2 「Enable Video Tampering」チェックボックスをオンにし、機能を有効にします。
- 3. 「Edit」をクリックして、ビデオ改ざんの準備スケジュールを編集します。アーミングスケジュールの設定は、モーション検出のアーミングスケジュールの設定と同じです。「10.1.1 モーション検出の設定」の「タスク2:モーション検知のアーミングスケジュールの設定」を参照してください。
- 4. チェックボックスをオンにすると、映像改ざんにかかる連動方法を選択できます。 「10.1.1 モーション検出の設定」の「タスク3:モーション検知の連動方法の設定」 を参照してください。
- 5. 「Save」をクリックして設定を保存します。

### 10.1.3 アラーム入力の設定

- 1. 「Configuration」 > 「Event」 > 「Basic Event」 > 「Alarm Input」を選択します。
- 2. 「Alam Input NO.」と「Alam Type」を選択します。アラームタイプには、NO (ノーマルオープン)とNC (ノーマルクローズ)があります。名前を編集して、アラーム入力の名前を設定します。

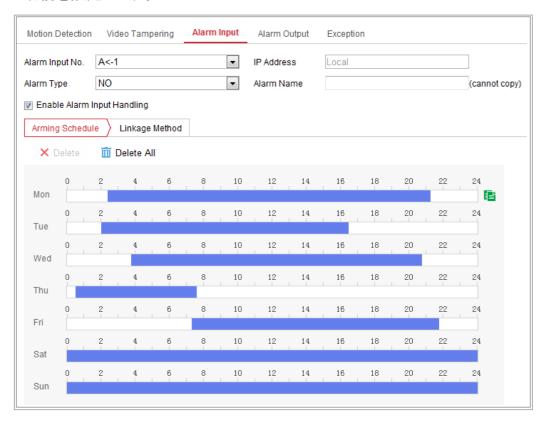


図10-7 アラーム入力の設定

- 3. 「Arming Schedule」をクリックして、アラーム入力のアーミングスケジュールを設定します。「タスク2: モーション検知のアーミングスケジュールの設定」を参照してください。
- 4. 「Linkage Method」をクリックし、チェックボックスをオンにすると、アラーム入力にかかる連動方法を選択できます。「タスク3:モーション検知の連動方法の設定」を参照してください。
- 5. 他のアラーム入力に設定をコピーできます。
- 6. 「Save」をクリックし、設定を保存します。

#### Alarm Output Motion Detection Video Tampering Alarm Input Exception Alarm Output No. A->1 -IP Address Delay 5s Alarm Name Alarm Status OFF Arming Schedule X Delete m Delete All Mon 10 12 Tue 10 Wed 10 18 24 14 16 20 18 20 Fri Sat 10 12 14 16 18 20 Manual Alarm Copy to.

### 10.1.4 アラーム出力の設定

図10-8 アラーム出力の設定

- 1. 「Configuration」 > 「Event」 > 「Basic Event」 > 「Alarm Output」を選択します。
- 2. 「Alarm Output」のドロップダウンリストから、アラーム出力チャンネルを1つ選択します。アラーム出力の名前を設定することもできます。
- 3. ディレイタイムは「5sec」、「10sec」、「30sec」、「1min」、「2min」、「5min」、「10min」、「Manual」のいずれかに設定できます。ディレイ時間とは、アラーム発生後、アラーム出力が継続する時間のことです。
- 4. 「Alarm Schedule」をクリックして、スケジュール時刻の編集画面を表示します。 タイムスケジュールの設定は、モーション検出のアーミングスケジュールの設 定と同じです。「タスク2:モーション検知のアーミングスケジュールの設定」を 参照してください。
- 5. 他のアラーム出力に設定をコピーすることができます。
- 6. 「Save」をクリックし、設定を保存します。

### 10.1.5 例外アラームの設定

想定されることはハードディスクの容量不足および接続 エラー、ネットワーク切断、 複数の端末からの同時ログインおよび不正なログインがあります。

- 1. 「Configuration」 > 「Event」 > 「Basic Event」 > 「Exception」を選択します。
- 2. チェックボックスをオンにし、例外アラームに対して実行されるアクションを設定 します。「タスク3:モーション検知の連動方法の設定」を参照してください。
- 3. 「Save」をクリックし、設定を保存します。

#### Flashing Alarm Light Output Exception Audible Alarm Output Video Tampering 15 Flashing Duration Medium Flashing Frequency 50 Brightness Arming Schedule m Delete All X Delete 14 18 20 24 Mon 2 4 20 12 14 Tue 2 4 6 8 10 12 14 16 18 20 24 Wed 10 14 20 Thu 20 Fri 10 14 18 20 Sat 4 8 10 12 14 18 20 24 Sun

### 10.1.6 アラームライト出力の点滅の設定

図10-9 アラームライト出力の点滅の設定

#### 手順:

- 1. 「Configuration」>「Event」>「Basic Event」>「Flashing Alarm Light Output」を 選択します。
- 「Flashing Duration」: 1回のアラームが発生したときに点滅が続く時間です。
- 「Flashing Frequency」: ライトの点滅速度です。High、Medium、Low が選択可能です。
- 「Brightness」: ライトの明るさです。
- 2. 点滅時間、点滅頻度、明るさを設定します。
- 3. アーミングスケジュールを編集します。
- 4. 「Save」をクリックします。

お知らせ: 特定のモデルのみが機能をサポートします。

#### **Audible Alarm Output** Video Tampering Exception Flashing Alarm Light Output Siren V Alarm Sound Type Alarm Times Sound Volume Arming Schedule × Delete m Delete All Mon Tue Wed Thu Fri Sat

### 10.1.7 音声アラーム出力の設定

図10-10 音声アラーム出力設定

### 手順:

Sun

- 1. 「Configuration」>「Event」>「Basic」>「Event」>「Audible Alarm Output」 を選択します。
- 「Alarm Sound Type」: アラーム音の種類
- 「Alarm Times」: アラームの繰り返し回数
- 2. アラーム音の種類を選択します。
- 3. アラームの時間や音量を設定します。
- 4. アーミングスケジュールを編集します。
- 5. 「Save」をクリックします。

お知らせ: 特定のモデルのみが機能をサポートします。

### 10.1.8 その他のアラームの設定

*お知らせ:* 特定のカメラのみが、ワイヤレスアラーム、PIR (受動赤外線センサー) アラーム、緊急アラームをサポートしています。

#### ● ワイヤレスアラーム

#### 目的:

ワイヤレス・ドア・コンタクトなどの検出器からワイヤレスアラーム信号がカメラに送信されると、ワイヤレスアラームを発信し、一連の応答アクションを実行できます。

#### 手順:

1. 「Configuration」>「Advanced Configuration」>「Basic Event」>「Wireless Alarm」を選択します。

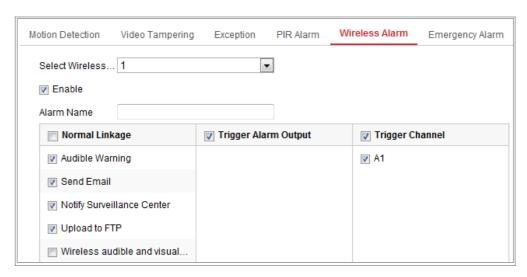


図10-11 ワイヤレスアラームの設定

- 2. ワイヤレスアラーム番号を選択します。 最大8 チャネルの外部ワイヤレスアラーム入力に対応します。
- 3. 「Enable Wireless Alarm」チェックボックスをオンにし、機能を有効にします。
- 4. 必要に応じて、テキストボックスにアラーム名を入力します。
- 5. チェックボックスをオンにすると、ワイヤレスアラームの連動方法を選択できます。

- 6. 「Save」をクリックし、設定を保存します。
- 7. カメラの横にある外部ワイヤレスデバイスを探し、「Configuration」 > 「System」 > 「System Settings」 > 「Remote Control」と選択してカメラをアーミングし、ワイヤレスアラームを調べます。

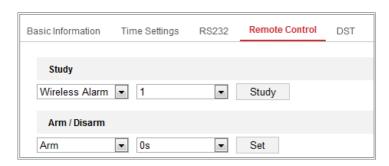


図10-12 ワイヤレスアラームの設定

### ● PIRアラーム

#### 目的:

侵入者が検出器の視野内を移動すると、PIR (受動赤外線)アラームが発動されます。人、または犬や猫などの他の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ます。

#### 手順:

1. 「Configuration」>「Advanced Configuration」>「Basic Event」>「PIR Alarm」を 選択します。

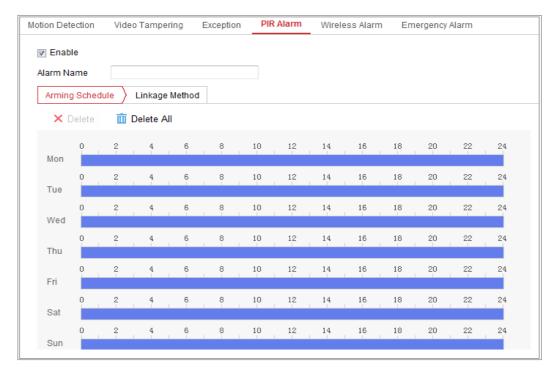


図10-13 PIR アラームの設定

- 2. 「Enable」のチェックボックスをオンにすると、PIR アラーム機能が有効になります。
- 3. 必要に応じて、テキストボックスにアラーム名を入力します。
- 4. チェックボックスをオンにすると、PIR アラームにかかる連動方法を選択できます。
- 5. 「Edit」をクリックして、アーミングスケジュールを設定します。
- 6. 「Save」をクリックし、設定を保存します。
- 7. 「Configuration」>「Advanced Configuration」>「System」>「Remote Control」 の順に選択し、カメラをアームします。

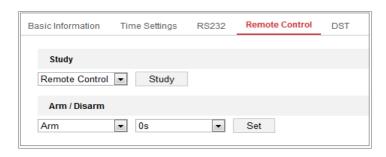


図10-14 PIR アラームのアーミング

### ● 緊急アラーム

#### 目的:

リモコンの緊急ボタンを押すと、緊急時に緊急アラームを通知できます。

お知らせ: 緊急アラームにはリモコンが必要です。まず「Configuration」>

「System」 > 「System Settings」 > 「Remote Control」の順に選択して、リモートコントロールを調べます。

#### 手順:

1. 「Configuration」>「Advanced Configuration」>「Basic Event」>「PIR Alarm」を 選択します。

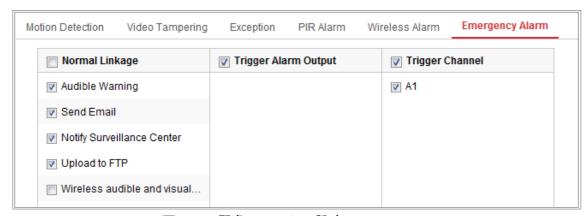


図10-15 緊急アラームの設定

- 2. チェックボックスをオンにすると、緊急アラームの連動方法を選択できます。
- 3. 「Save」をクリックし、設定を保存します。

## 10.2 スマートイベント

オーディオ例外検出、デフォーカス検出、シーンチェンジ検出、侵入検出、ラインクロッシング検出など、このセクションの指示に従ってスマートイベントを設定できます。これらのイベントは、「Notify Surveillance Center」、「Send Email」、「Trigger Alarm Output」などの連携方法を設定できます。

### 10.2.1 オーディオ例外検出の設定

#### 目的:

音声例外検出機能は、サウンド強度の急激な上昇/低下など監視シーンの異常音を検出し、アラームが発生した場合に特定の動作を行うことができる機能です。

**お知らせ:** オーディオ例外検出機能は、モデルによって異なります。

#### 手順:

1. 「Configuration」>「Advanced Configuration」>「Smart Event」>「Audio Exception Detection」を選択します。

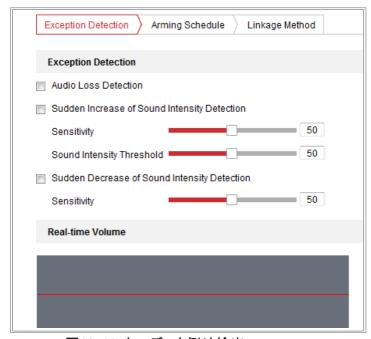


図10-16 オーディオ例外検出

- 2. 「Audio Loss Exception」チェックボックスをオンにし、機能を有効にします。
- 3. 「Sudden Increase of Sound Intensity Detection」チェックボックスをオンにすると、監視シーンのサウンド急上昇を検出します。サウンドの急上昇の検出感度としきい値は設定が可能です。

4. 「Sudden Decrease of Sound Intensity Detection」チェックボックスをオンにすると、監視シーンのサウンドの急激な低下を検出します。サウンドステイプドロップの検出感度としきい値は設定が可能です。

#### お知らせ:

- 「Sensitivity」: 設定範囲[1-100]、値が小さいほど、検出するための変化が 激しくなります。
- 「Sound Intensity Threshold]: 設定範囲[1-100]、環境内の音をフィルタリン グできます。環境音が大きいほど、値を高くする必要があります。実環境に 合わせて調整できます。
- 画面上で音声のリアルタイム音量を確認できます。
- 5. 「Arming Schedule」をクリックして、アーミングスケジュールを設定します。詳細な手順については、「タスク2: モーション検出のアーミングスケジュールの設定」を参照してください。
- 6. 「Linkage Method」をクリックして、音声例外の連動方法(監視センターへの通知、Eメールの送信、FTP/メモリーカード/NAS へのアップロード、トリガ・チャンネル、アラーム出力など)を選択します。
- 7. 「Save」をクリックし、設定を保存します。

### 10.2.2 デフォーカス検出の設定

#### 目的:

レンズの焦点ぼけによって生じる画像ぼけを検出し、アラームが発動されたときに、設定した操作をすることができます。

**お知らせ**: デフォーカス検出機能は、モデルによって異なります。

#### 手順:

1. 「Configuration」>「Advanced Configuration」>「Smart Event」>「Defocus Detection」を選択します。



図10-17 デフォーカス検出の設定

- 2. 「Enable」チェックボックスをオンにし、機能を有効にします。
- スライダーをクリック・ドラッグして、検出感度を設定します。
   感度の値は1~100の範囲で、値が高いほどイメージの焦点がぼけ、アラームが発生しやすくなります。
- 4. 「Notify Surveillance Center」、「Send Email」、「Trigger Alarm Output」など、 デフォーカスの連携方法を選択します。
- 5. 「Save」をクリックし、設定を保存します。

## 10.2.3 シーンチェンジ検出の設定

#### 目的:

シーン変更検出機能は、カメラの意図的な回転などの外部要因の影響を受ける監視環境の変化を検出する機能です。一部のアクションは、アラームが発生したときに実行されます。

お知らせ: シーンチェンジ検出機能は、カメラの機種によって異なります。

#### 手順:

「Configuration」>「Advanced Configuration」>「Smart Event」>「Scene
 Change Detection」を選択します。



図10-18 シーンチェンジ検出

- 2 「Enable」チェックボックスをオンにし、機能を有効にします。
- 3 スライダーをクリック・ドラッグして、検出感度を設定します。 感度の値は1~100の範囲で、値が高いほどシーンの変化でアラームが発生 しやすくなります。
- 4. 「Arming Schedule」をクリックして、アーミングスケジュールを設定します。詳細な手順については、「タスク2:モーション検知のアーミングスケジュールの設定」を参照してください。
- 5. 「Linkage Method」をクリックして、監視センターへの通知、Eメールの送信、FTP/メモリーカード/NASへのアップロード、トリガ・チャンネル、アラーム出力など、シーン変更の連動方法を選択します。
- 6. 「Save」をクリックし、設定を保存します。

### 10.2.4 顔検出の設定

#### 目的:

顔検出機能は、監視シーンに顔が表示されることを検出し、アラームが発生したときに特定のアクションを実行できます。

#### 手順:

- 1. 「Configuration」>「Advanced Configuration」>「Smart Event」>「Face Detection」を選択します。
- 2. 「Enable Face Detection」チェックボックスをオンにし、機能を有効にします。
- 3. 「Enable Dynamic Analysis」チェックボックスをオンにすると、検出された顔がライブビデオで緑の長方形でマークされます。

*お知らせ:* 検出された顔をライブビデオでマークするには、「Configuration」> 「Local」に移動してルールを有効にします。

- 4. スライダーをクリック・ドラッグして、検出感度を設定します。感度の範囲は1~5です。値が大きいほど顔を検出しやすくなります。
- 5. 「Arming Schedule」をクリックして、アーミングスケジュールを設定します。詳細な手順については、「タスク2:モーション検知のアーミングスケジュールの設定」を参照してください。

6. 「Linkage Method」をクリックして、顔検出の連動方法を選択します。 「タスク3:モーション検知の連動方法の設定」を参照してください。

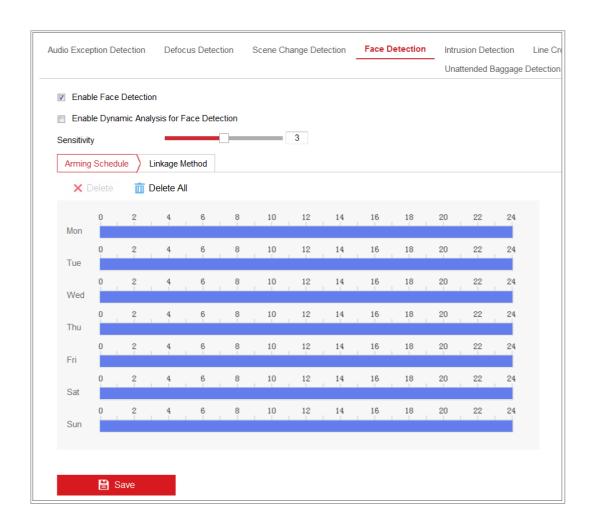


図10-19 顔検出

7. 「Save」をクリックし、設定を保存します。

### 10.2.5 侵入検知の設定

#### 目的:

侵入検知機能は、あらかじめ定義された仮想領域に入ってくる人、車両、その他の 物体を検知し、アラームが発生したときに特定の動作を行うことができます。

お知らせ: 侵入検知機能は、モデルによって異なります。

### 手順:

1. 「Configuration」>「Advanced Configuration」>「Smart Event」>「Intrusion Detection」を選択します。



図10-20 侵入検知

- 2. 「Enable」チェックボックスをオンにし、機能を有効にします。
- 3. 「Region」のドロップダウンリストからリージョン番号を選択します。

「Region」: ライブビュー画像上のあらかじめ定義された頂点領域です。リージョンに出入りする人、車両、その他のオブジェクトなどのターゲットが検出され、設定されたアラームが発生します。

4. 最大値を設定します。サイズと最小有効なターゲットのサイズ。有効なターゲットサイズ より小さいまたは大きいターゲットは、検出できません。ライブ画像内のポイントを開始 点として選択し、最大サイズまたは最小値として長方形を描画します。

「Max. Size」: 有効なターゲットの最大サイズです。より大きなサイズのターゲットは、検出しません。

「Min. Size」: 有効なターゲットの最小サイズです。サイズが小さいターゲットは検出しません。

- 5. 検知領域を設定します。検出領域の4つの頂点を指定するには、ライブビデオ上をクリックします。
- 6. 検出対象を選択します。人間と車両が利用可能です。検出対象が選択されていない場合、検出されたすべてのターゲットが報告されます(人間と車両を含む)。
- 7. 侵入検知の時間しきい値を設定します。

「Threshold」: 設定範囲[0s-10s]、領域内でオブジェクトがロータリングする時間のしきい値です。値を0 に設定すると、領域に入ったオブジェクトの直後にアラームが発生します。

8. スライダーをドラッグして感度値を設定します。

「Sensitivity」: 設定範囲[1-100]。感度とは、あらかじめ定義された領域に入る許容可能なターゲットの身体部分の割合を表します。

感度 = 100 - S1/ST\*100

S1 は、事前定義された領域を横切るターゲットボディパーツを表します。

STは完全な標的本体の略です。

例:値を60 に設定すると、40% のボディパーツがリージョンに入った場合にのみ、 アクションをイントルージョンとしてカウントできます。

*お知らせ:* 検出の感度は、一部のモデルでサポートされています。詳細は実際の表示を参照してください。

- 9. 他のリージョンを設定するには、上記の手順を繰り返します。最大4つの領域を 設定できます。「Clear」をクリックすると、すべての定義済みリージョンをクリアで きます。
- 10. アーミングスケジュールをクリックして、アーミングスケジュールを設定します。

*お知らせ:* 特定のモデルのみが、トリガ・チャンネル、アラーム出力、点滅アラーム、可聴アラームをサポートしています。

12.「Save」をクリックし、設定を保存します。

## 10.2.6 ライン交差検知の設定

#### 目的:

ライン交差検知機能は、事前に定義された仮想線を横切る人、車両、または他の物体を検知し、アラームが発生したときに、いくつかの特定のアクションを取ることができます。

お知らせ: ライン公差検出機能は、カメラの機種により異なります。

### 手順:

1. 「Configuration」>「Advanced Configuration」>「Smart Event」>「Line
Crossing Detection」を選択します。

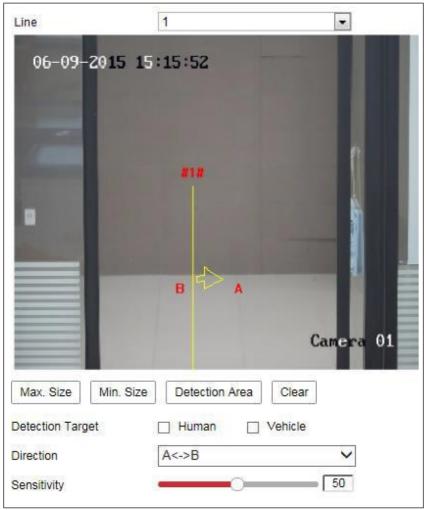


図10-21 ライン交差検出

- 2 「Enable」チェックボックスをオンにし、機能を有効にします。
- 3. ドロップダウンリストから行を選択します。
- 4. 最大値を設定します。サイズと最小有効なターゲットのサイズ。有効なターゲットサイズより小さいか大きいターゲットは検出できません。

「Max. Size」: 有効なターゲットの最大サイズ。より大きなサイズのターゲットは、 検出しません。

「Min. Size」: 有効なターゲットの最小サイズ。サイズが小さいターゲットは検出しません。

- 5. 検出領域を設定します。線をドラッグすると、ライブビデオ上で好きな場所に配置できます。
- 6. 検出対象を選択します。人間と車両が利用可能です。検出対象が選択されていない場合、検出されたすべてのターゲットが報告されます(人間と車両を含む)。
- 線交差検出の方向を選択します。また、A<->B、A->B、B->A の方向を選択 できます。

「A<->B」: 両方向を持つ平面を横切るオブジェクトを検出でき、アラームが通知されます。

「A->B」: A 側からB 側に設定されたラインを横切る物体のみを検出できます。

「B->A」: B 側からA 側に設定されたラインを横切る物体のみを検出できます。

8. スライダーをドラッグして感度値を設定します。

「Sensitivity」: 設定範囲[1-100]。これは、事前定義されたラインを横切る許容可能なターゲットのボディ部分のパーセンテージを表します。

感度 = 100 - S1/ST\*100

S1 は、事前定義されたラインを横切るターゲットボディパーツを表します。 STは完全な標的本体の略です。

例:値を60 に設定すると、40% 以上のボディパーツがラインを横切る場合にのみ、アクションをライン交差アクションとしてカウントできます。

*お知らせ:* 検出の感度は、一部のモデルでサポートされています。詳細は実際の表示を参照してください。

9. 他の回線を設定するには、上記の手順を繰り返します。最大4行まで設定可能です。

「Clear」をクリックすると、定義済みの行をすべてクリアできます。

10. 「Arming Schedule」をクリックして、アーミングスケジュールを設定します。

- 11. 「Linkage Method」をクリックして、侵入検知の連動方法を選択します。これには、通知監視センター、送信メール、FTP/メモリーカード/NASへのアップロード、トリガ・チャンネル、アラーム出力、点滅アラーム、可聴アラームが含まれます。 *お知らせ:* 特定のモデルのみが、トリガ・チャンネル、アラーム出力、点滅アラーム、可聴アラームをサポートしています。
- 12 「Save」をクリックし、設定を保存します。

# 10.2.7 領域進入検出の設定

## 目的:

領域進入検知機能は、外部の場所からあらかじめ定義された仮想領域に入る人、 車両、または他の物体を検知し、アラームが作動したときに、ある種の行動をと ることができます。

### 手順:

1. 「Configuration」>「Advanced Configuration」>「Smart Event」>「Region Entrance Detection」を選択します。



図10-22 領域進入検出

- 2. 「Enable」チェックボックスをオンにし、機能を有効にします。
- 3. 検出設定のドロップダウンリストからリージョンを選択します。
- 4. 最大値を設定します。サイズと最小有効なターゲットのサイズ。有効なターゲット サイズより小さいか大きいターゲットは検出できません。

「Max. Size」: 有効なターゲットの最大サイズ。より大きなサイズのターゲットは、 検出しません。

「Min. Size」: 有効なターゲットの最小サイズ。サイズが小さいターゲットは検出しません。

- 5. 検出領域を設定します。ライブビデオをクリックして検出領域の4つの頂点を指定し、右クリックして描画を完了します。
- 6. 検出対象を選択します。人間と車両が利用可能です。検出対象が選択されていない場合、検出されたすべてのターゲットが報告されます(人間と車両を含む)。

7. スライダーをドラッグして感度値を設定します。

**感度**: 範囲[1-100]。感度とは、あらかじめ定義された領域に入る許容可能なター ゲットの身体部分の割合を表します。

感度 = 100 - S1/ST\*100

S1は、あらかじめ定義された領域STに入るターゲット本体部分を表します。 例:値を60 に設定すると、40% のボディパーツがリージョンに入った場合にの み、リージョンの入口アクションとしてカウントできます。

*お知らせ:* 検出の感度は、一部のモデルでサポートされています。詳細は実際の表示を参照してください。

- 8 他のリージョンを設定するには、上記の手順を繰り返します。最大4つの領域を 設定できます。「Clear」ボタンをクリックすると、すべての定義済みリージョンを クリアできます。
- 9. 「Arming Schedule」をクリックして、アーミングスケジュールを設定します。
- 10. 「Linkage Method」をクリックして、侵入検知の連携方法を選択します。これには、通知監視センター、送信メール、FTP/メモリーカード/NASへのアップロード、トリガ・チャンネル、アラーム出力、点滅アラーム、可聴アラームが含まれます。

*お知らせ:* 特定のモデルのみが、トリガ・チャンネル、アラーム出力、点滅アラーム、可聴アラームをサポートしています。

11. 「Save」をクリックし、設定を保存します。

# 10.2.8 領域退出検出の設定

#### 目的:

領域退出検知機能は、あらかじめ定義された仮想領域から出る人、車両、またはその他の物体を検出し、アラームが発生したときに特定のアクションを実行することができます。

## 手順:

1. 「Configuration」>「Advanced Configuration」>「Smart Event」>「Region Exiting Detection」を選択します。

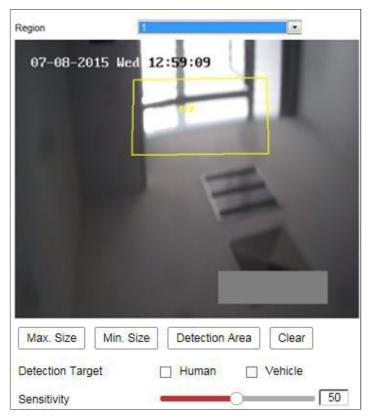


図10-23 領域退出検出

- 2. 「Enable」チェックボックスをオンにし、機能を有効にします。
- 3. 検出設定のドロップダウンリストからリージョンを選択します。
- 4. 最大値を設定します。サイズと最小有効なターゲットのサイズ。有効なターゲットサイズより小さいか大きいターゲットは検出できません。

「Max. Size」: 有効なターゲットの最大サイズ。より大きなサイズのターゲットは、検出しません。

「Min. Size」: 有効なターゲットの最小サイズ。サイズが小さいターゲットは検出しません。

5. 検出領域を設定します。ライブビデオをクリックして検出領域の4つの頂点を 指定し、右クリックして描画を完了します。

- 6. 検出対象を選択します。人間と媒体が利用可能です。検出対象が選択されていない場合は、人および車両を含むすべての検出対象が報告されます。
- 7. スライダーをドラッグして感度値を設定します。

「Sensitivity」: 設定範囲[1-100]。感度は、あらかじめ定義された領域から出る許容可能なターゲットの身体部分のパーセンテージを表します。

感度 = 100 - S1/ST\*100

S1 は、事前定義された領域から出るターゲットボディパーツを表します。ST は完全な標的本体の略です。

例: 値を60 に設定すると、40% のボディパーツがリージョンから出た場合にのみ アクションを終了するリージョンとしてカウントできます。

*お知らせ:* 検出の感度は、一部のモデルでサポートされています。詳細は実際の表示を参照してください。

- 8. 他のリージョンを設定するには、上記の手順を繰り返します。最大4つの領域を設定できます。「Clear」をクリックすると、すべての定義済みリージョンをクリアできます。
- 9. 「Arming Schedule」をクリックして、アーミングスケジュールを設定します。
- 10. 「Linkage Method」をクリックして、侵入検知の連動方法を選択します。これには、通知監視センター、送信メール、FTP/メモリーカード/NASへのアップロード、トリガ・チャンネル、アラーム出力、点滅アラーム、可聴アラームが含まれます。

*お知らせ:* 特定のモデルのみが、トリガ・チャンネル、アラーム出力、点滅アラーム、可聴アラームをサポートしています。

11. 「Save」をクリックし、設定を保存します。

## 10.2.9 無人手荷物検出の設定

## 目的:

手荷物検知機能は、あらかじめ設定した領域内における手荷物、ハンドバッグ、 危険物などの忘れ物を検知します。アラームが発生すると、一連のアクションを 実行します。

## 手順:

1. 「Configuration」>「Event」>「Smart Event」>「Unattended Baggage Detection」を選択します。



図10-24 無人手荷物検出

- 2. 機能を有効にするには、「Enable」チェックボックスをオンにします。
- 3. 検出設定のドロップダウンリストからリージョンを選択します。

- 4. エリア設定をクリックし、エリアの描画をクリックしてエリアの描画を開始します。
- 5. ライブビデオをクリックして検出領域の4つの頂点を指定し、右クリックして描画を完了します。
- 6. 最大値を設定します。サイズと最小有効なターゲットのサイズ。有効なターゲットサイズより小さいか大きいターゲットは検出できません。

「Maz. Size」: 有効なターゲットの最大サイズ。より大きなサイズのターゲットは、検出しません。

「Min. Size」:有効なターゲットの最小サイズ。サイズが小さいターゲットは検出しません。

- 7. 描画が終了したら、「Stop Drawing」をクリックします。
- 8. 無人手荷物検知の時間しきい値と検知感度を設定します。
  「Threshold」: 設定範囲[5-100s]、領域に残っているオブジェクトの時間のしきい値。値を10に設定すると、オブジェクトが放置された後にアラームが発生し、10
  秒間領域に留まります。
- 9. スライダーをドラッグして感度値を設定します。

「Sensitivity」: 設定範囲[1-100]。感度とは、あらかじめ定義された領域に入る許容可能なターゲットの身体部分の割合を表します。

感度 = 100 - S1/ST\*100

S1 は、事前に定義された領域に入るターゲットボディパーツを表します。STは 完全な標的本体の略です。

例:値を60 に設定すると、ターゲットの40% の身体部分が領域に入った場合にのみ、ターゲットを無人手荷物としてカウントすることができます。

*お知らせ:*検出の感度は、一部のモデルでサポートされています。詳細は実際の表示を参照してください。

10. 他のリージョンを設定するには、上記の手順を繰り返します。最大4つの領域を 設定できます。「Clear」をクリックすると、すべての定義済みリージョンをクリアで きます。

- 11. 「Arming Schedule」をクリックして、アーミングスケジュールを設定します。
- 12. 「Linkage Method」をクリックして、連携方法を選択します。
- 13.「Save」をクリックし、設定を保存します。

## 10.2.10 オブジェクトの退出検知の設定

## 目的:

物体退出検知機能は、ディスプレイ上の展示など、あらかじめ定義された領域から除退出する物体を検知し、アラーム発生時に一連の動作を行います。

## 手順:

1. 「Configuration」>「Advanced Configuration」>「Smart Event」>「Object Removal Detection」を選択します。

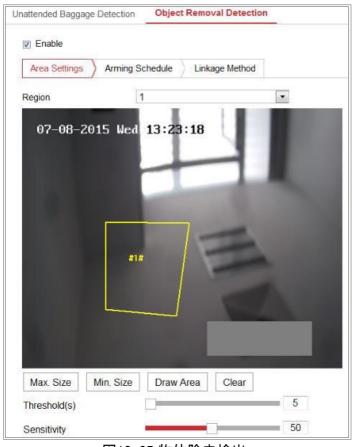


図10-25 物体除去検出

機能を有効にするには、「Enable」チェックボックスをオンにします。

- 3. 検出設定のドロップダウンリストから「Region」を選択します。
- 4. 「Area Settings」をクリックし、「Draw Area」をクリックしてエリア描画を開始します。
- 5. ライブビデオをクリックして検出領域の4つの頂点を指定し、右クリックして描画 を完了します。
- 6. 最大値を設定します。サイズと最小有効なターゲットのサイズ。有効なターゲットサイズより小さいか大きいターゲットは検出できません。

「Maz. Size」: 有効なターゲットの最大サイズです。より大きなサイズのターゲットは、検出しません。

「Min. Size」: 有効なターゲットの最小サイズです。サイズが小さいターゲットは検出しません。

- 7. 描画が終了したら、「Stop Drawing」をクリックします。
- 8. オブジェクト除去検出の時間しきい値を設定します。

「Threshold」: 設定範囲[5-100s]。領域から除去されるオブジェクトの時間のしきい値です。

値を10に設定すると、オブジェクトが領域から10秒間消失した後にアラームが発生します。

9. スライダーをドラッグして感度値を設定します。

「Sensitivity」: 設定範囲[1-100]。これは、あらかじめ定義された領域を離れる、 許容可能なターゲットの身体部分のパーセンテージを表します。

感度 = 100 - S1/ST\*100

S1 は、事前に定義された領域を離れるターゲットボディパーツを表します。ST は完全な標的本体の略です。

例: 値を60 に設定すると、ターゲットの40% のボディ部分が領域から離れる場合にのみ、ターゲットを除去したオブジェクトとしてカウントすることができます。注: 検出の感度は、一部のモデルでサポートされています。詳細は実際の表示を参照してください。

10. 他のリージョンを設定するには、上記の手順を繰り返します。最大4つの領域を設定できます。「Clear」をクリックすると、すべての定義済みリージョンをクリアできます。

- 11. 「Arming Schedule」をクリックして、アーミングスケジュールを設定します。
- 12. 「Linkage Method」をクリックして、連携方法を選択します。
- 13.「Save」をクリックし、設定を保存します。

# 10.3 VCA 設定

## 10.3.1 挙動解析

挙動解析で一連の不審な動きが検出されると、アラームを発信し特定の連動方法が有効になります。

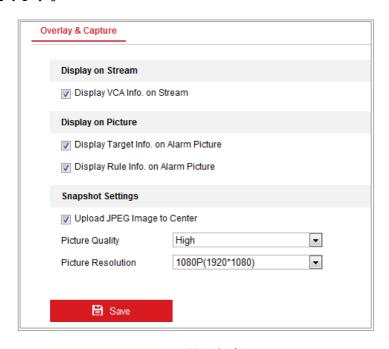


図10-26 挙動解析

### ☆ オーバーレイとキャプチャ

表示情報には、ピクチャー上の表示とストリーム上の表示が含まれます。

「Display VCA info. on Stream」: ライブビューまたは再生中は、緑色のフレームがターゲットに表示されます。

「Display Target info. on Alarm Picture 」: チェックボックスをオンにすると、アップロードされたアラーム画像上のターゲットにフレームが表示されます。

「Display Rule info. on Alarm Picture」: キャプチャされたターゲットと設定された領域がアラームピクチャにフレーム表示されます。

**お知らせ:** ローカル設定でルールが有効になっていることを確認してください。

「Configuration」〉「Local Configuration」〉「Rules」を選択し有効にします。

「Snapshot Setting」: 撮影した画像の画質と解像度を設定します。

「Upload JPEG Image to Center」: チェックボックスをオンにすると、VCAアラームが発生したときに、撮影した画像を監視センターにアップロードします。

「Picture Quality」: 高、中、低が選択できます。

「Picture Resolution」: CIF、4CIF、720P、1080Pから選択できます。

### ❖ 「Camera Calibration」

カメラからの画像を三次元的に測定してクオンタイズし、各ターゲットのサイズを計算するには、次の手順を実行します。カメラキャリブレーションが設定されている場合、VCA検出はより正確になります。

### 手順:

- 1. 「Camera Calibration」チェックボックスをオンにすると、この機能が有効になります。
- 2. 「Input Basic Data」または「Draw on Live View Video」としてキャリブレーションモードを選択します。

「Input Basic Data」: カメラの取り付け高さ、視野角、水平比を手動で入力します。

「Draw on Live View Video」: 「Draw Verification Line (Horizontal) /

(Vertical)」をクリックして、ライブビューに水平/垂直線を描き、実長フィールドに実際の長さを入力します。描かれたリファレンス線とその長さにより、カメラはライブビューに他のオブジェクトが表示されていると判断します。

3. 水平照合 / 垂直照合 **1** をクリックして、ライブビデオに水平/垂直線を描き、「Start Verifing」 をクリックして線の長さを計算します。計算したライン長と実際の長さを比較して、設定したキャリブレーション情報を検証します。 *お知らせ:* ライブビューが停止している場合、カメラキャリブレーションは無効です。



図10-27「Draw on Live View」画面

- 4. ▼ をクリックすると、描かれた線を削除できます。
- 5. 「Save」をクリックし、設定を保存します。

## ❖ 「Shield Region」

シールド領域では、ビヘイビア一解析が機能しない特定の領域を設定できます。最大4つのシールド領域がサポートされます。

## 手順:

- 1. 「Shield Region」をクリックして、シールド領域設定画面を表示します。

#### お知らせ:

- 最大10辺のポリゴン領域に対応しています。
- 図をクリックすると、描画した領域を消去します。
- ライブビューが停止している場合、シールド領域を描画できません。
- 3. 「Save」をクリックし、設定を保存します。

## ❖ 「Rule」

挙動解析は、線交差検出、侵入、領域進入、および領域退出などを含む一連の挙動をサポートしています。

お知らせ: 各動作の詳細情報については、各章を参照してください。

### 手順:

- 1. 「Rule」をクリックして、ルール設定画面を表示します。
- 2. 「Rule」のチェックボックスをオンにし、動作分析のルールを有効にします。

3. ルールの種類を選択し、フィルターの種類を設定してから、ルールのライブ ビデオに線/エリアを描画します。

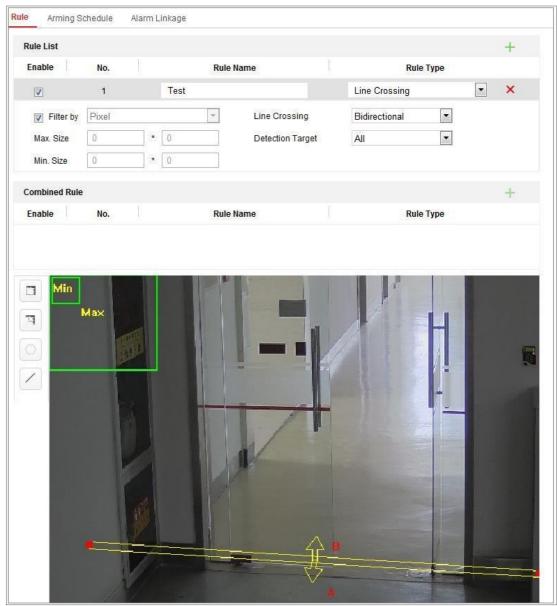


図10-28 ルールの設定

「Filter type」: 「Pixels」と「Actual Size」を選択できます。「Pixels」を選択した場合は、各ルールのライブビデオに最大サイズと最小サイズの領域を描画します。「Actual Size」を選択した場合は、最大サイズと最小サイズの長さと幅を入力します。ターゲットのサイズが最小値と最大値の間にある場合にのみアラームが発生します。

*お知らせ*: 実際のサイズが選択されている場合は、カメラキャリブレーションが 設定されていることを確認してください。 「Detection Target」: 検知対象として「Human」または「Vehicle」を選択します。すべてを選択して、すべてのオブジェクトをターゲットとして検出することもできます。

「Draw line/area」: 線の交差検出には、線を描く必要があります。交差方向を選択します。交差方向は、双方向、A-to-B、またはB-to-A です。

侵入、リージョンの入口・出口、その他のイベントについては、ライブビデオを 左クリックしてエリアの終点を設定し、右クリックしてエリアの描画を終了する 必要があります。

*お知らせ:* ライブビューを停止すると、検出エリア/ラインを描くことができず、ルールを設定できません。

- 4. 組み合わせルールのチェックボックスをオンにし、動作分析のルールを 有効にします。
- 5. 結合されたルールのルールA とルールB として2つの設定された単ールールを選択し、2つの単ールールの最小時間間隔と最大時間間隔を設定してから、アラームフィルタリングの単ールールの動作順序を選択します。

#### お知らせ:

- ルールタイプを「None」として選択した場合、ルールオプションは無効になり、動作分析を設定できません。
- 最大8つの単一ルールと2つの結合ルールを設定できます。また、結合 ルールに対して、ライン交差、侵入、領域退出および領域進入をサポートされています。
- 6. 「Save」をクリックし、設定を保存します。
- 7. 「Arming Schedule」をクリックして、アーミングスケジュールを設定し、「Save」クリックしして設定を保存します。
- 8. 「Linkage Method」をクリックして、各ルールに対応する連携方法のチェックボックスをオンにし、「Save」をクリックして設定を保存します。

### ❖ 詳細設定

「Behavior Analysis Version」: アルゴリズムライブラリのバージョンを一覧表示します。

#### 「Parameter」

以下のパラメータを設定して、設定を詳細化します。

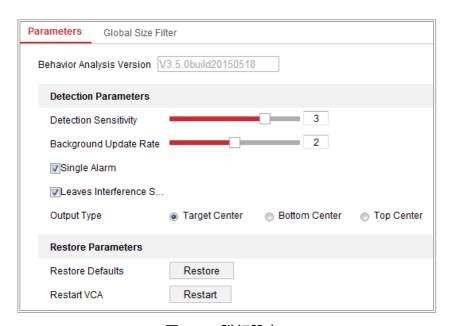


図10-29 詳細設定

Detection Sensitivity: 設定範囲[0~4]、カメラがターゲットを検出する感度を指します。値が大きいほどターゲットを認識しやすくなり、誤情報が多くなります。デフォルト値の3を推奨します。

「Background Update Rate」: 設定範囲[0~4]、新しいシーンの速度を参照し、前のシーンに置き換わります。デフォルト値の3 を推奨します。

「Single Alarm」: 選択されている場合、設定されているエリアのターゲットは、1回だけアラームが発生します。チェックを入れないと、同じターゲットが同じ設定エリアで連続アラームを発生します。

「Leave Interference Suppression」: このチェックボックスをオンにすると、設定したエリアのリーフによって発生する干渉を停止します。

「Output Type」: フレームの位置を選択します。ターゲット中心、ボトム中心、トップ中心が選択可能です。例えば、ターゲット中心が選択されている場合、ターゲットはフレームの中心になります。

「Restore Default」: クリックすると設定したパラメータがデフォルトに戻ります。
「Restart VCA」: 挙動解析のアルゴリズムライブラリを再起動します。

「Global Size Filter I

*お知らせ:* 各ルールを対象とするフィルターと比べ、グローバルサイズフィルターはすべてのルールを対象としています。

### 手順:

- 1. 「Global Size Filter」チェックボックスをオンにし、機能を有効にします。
- 2. 「Filter Type」を「Actual Size」または「Pixel」として選択します。

「Actual Size」: 最大サイズと最小サイズの両方の長さと幅を入力します。 ターゲットのサイズが最小値と最大値の間にある場合のみ、アラームが 発生します。

### お知らせ:

- 実際のサイズでフィルターを選択した場合は、カメラキャリブレーションを設定する必要があります。
- 最大サイズの長さは最小サイズの長さよりも長く、幅も長くする必要があります。

「Pixel」:「Minimum Size」をクリックして、最小の長方形を描画します。ライブビューのサイズです。「Maxmum Size」をクリックすると、最大サイズの長方形がライブビューに描画されます。ターゲットが最小より小さいまたは最大より大きい場合にフィルタリングされます。

## お知らせ:

- ライブビューが停止している場合は、グローバルサイズフィルターは設定できません。
- 最大サイズの長さは最小サイズの長さよりも長く、幅も長くする必要があります。
- 3. 「Save」をクリックし、設定を保存します。

## 10.3.2 フェイスキャプチャ

設定したエリアに表示される顔を撮影でき、撮影した画像にも顔情報がアップロード されます。

### ☆ オーバーレイとキャプチャ

「Display VCA info. on Stream」: ライブビューまたは再生中は、緑色のフレームがターゲットに表示されます。

「Display Target info. on Alarm Picture」: チェックボックスをオンにすると、アップロードされたアラーム画像上のターゲットにフレームが表示されます。

## [Snapshot Settings]:

- Target Picture Settings J
  - a. 撮影する画像のサイズを設定します。カスタム、ヘッドショット、ハーフボディショット、フルボディショットの4種類を用意しています。カスタムを選択した場合は、必要に応じて幅、ヘッド高さ、ボディ高さをカスタマイズできます。
  - b. 固定値をチェックして、画像の高さを設定します。
- 「Background Upload I:
  - a. 背景の確認:アップロードして、背景画像をアップロードします。
  - b. ドロップダウンリストから画質と解像度を選択します。

*お知らせ:* バックグラウンドアップロードは、フェイスキャプチャカメラでのみ使用できます。

### 「Camera Information」:

撮影した画像に重ねて表示できるカメラのデバイス番号とカメラ情報を設定します。

#### Text Overlay Information J:

撮影した画像に表示されるように、設定したい項目を確認したり、順序を調整したりできます。

### ❖ シールド領域

シールド領域では、フェイスキャプチャが機能しない特定の領域を設定できます。最大4つのシールド領域がサポートされます。

## 手順:

1. 六角形のサイン ( をクリックし、ライブビューウィンドウでシールド領域を 左クリックしてエンドポイントを描画し、右クリックで領域描画を終了します。

#### お知らせ:

- ポリゴン領域(4~10辺)の辺に対応しています。
- ※ をクリックして描画した領域を消去します。
- ライブビューが停止している場合、シールド領域を描くことはできません。



図10-30 シールド領域の描画

2. 「Save」をクリックし、設定を保存します。

#### ❖ ルール

## 手順:

- 1. フェイスキャプチャのルールを有効にするには、「Rule」をオンにします。
- 2. 長方形の符号 □ をクリックして最小瞳孔間距離を描画します。ライブビューの下のボックスに、描写した瞳孔の距離が表示されます。瞳孔間距離の最小化とは、2つの瞳孔間の領域で構成される最小正方形サイズのことで、カメラがターゲットを識別するための基本的な標準です。

#### お知らせ:

- ポリゴン領域(4~10辺)の辺に対応。
- ライブビューが停止している場合は、設定した領域を描くことはできません。
- 4. 「Save」をクリックして設定を保存します。

#### ❖ 詳細設定

「Face Capture Version」:アルゴリズムライブラリのバージョンが一覧表示されます。実際の環境に応じて、以下のパラメータを設定します。

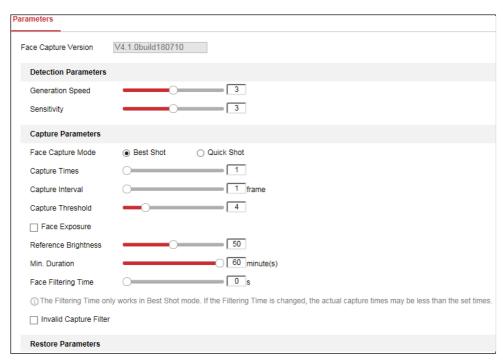


図10-31 詳細設定

## 「Detection Parameters」:

「Generation Speed」[1~5]: ターゲットを識別するための速度です。値を高くするほど、ターゲットの認識速度が速くなります。値を極端に低く設定すると、最初から設定したエリアに顔があった場合、この顔はキャプチャされません。壁画やポスターの顔の誤情報を減らすことができます。デフォルト値の3を推奨します。

「Sensitivity」[1~5]: ターゲットを識別するための感度です。値が大きいほど顔を認識しやすくなり、誤情報の可能性が高くなります。デフォルト値の3を推奨します。

## [Capture Parameters]:

「Face Capture Mode」: ベストショット、クイックショットが利用できます。

「Best Shot」: ターゲットが検出領域を離れた後のベストショット。
 「Capture Times」[1~10]: 設定したエリアに顔が留まっている間に、顔がキャプチャされる時間を指します。デフォルト値は1です。

「Capture Interval」[1~255 Frame]: 写真をキャプチャするフレーム間隔。 デフォルト値を1に設定すると、カメラがすべてのフレームで顔をキャプチャすることを意味します。

「Capture Threshold」: キャプチャとアラームが発生する顔認識精度を表します。値を大きくすると、キャプチャおよびアラーム発生のために、より高い精度を満たす必要があることを意味します。

• 「Quick Shot」: クイックショットのしきい値と最大キャプチャ間隔を定義できます。

「Quick Shot Threshold」: クイックショットをする顔認識精度を表します。

「Face Exposure」:チェックボックスをオンにすると、顔の露出が有効になります。「Reference Brightness」[0~100]:顔露出モード時の顔の基準となる明るさです。顔を検出すると、設定した値に応じてカメラが顔の明るさを調整します。値を高くするほど、顔が明るくなります。

「Minimum Duration」[1~60min]: カメラが顔を露光する最小の持続時間です。初期値は1分です。

*お知らせ:* 顔の露出が有効になっている場合は、WDR機能が無効になっており、手動アイリスが選択されていることを確認してください。

「Face Filtering Time」:カメラが顔を検出してからキャプチャアクションを実行するまでの時間間隔を意味します。検出された顔が設定したフィルタリング時間未満シーンにとどまると、キャプチャされません。たとえば、顔のフィルタリング時間を5 秒に設定すると、顔が5 秒間シーンに留まったままになったときに、カメラが検出された顔をキャプチャします。

お知らせ: 顔のフィルタリング時間(0 秒より長い) は、実際のキャプチャ時間が上記の設定値よりも短くなる可能性を増やします。

「Invalid Capture Filter」: チェックボックスをオンにすると、無効なキャプチャフィルタが有効になります。有効にすると、無効な撮影顔画像がフィルタリングされます。

「Restore Default」: 「Restore」をクリックして、詳細設定のすべての設定を工場出荷時のデフォルトに復元します。

## 10.3.3 人数カウント

## 目的:

人数カウント機能は、特定の設定されたエリアに出入りした人数を計算するのに役立ち、出入り口に広く使用されます。

### お知らせ:

できるだけ入口/出口の真上にカメラを設置し、カウント精度を上げるために水平になるようにすることを推奨します。

## 手順:

1. 「Configuration」>「Counting」を選択します。

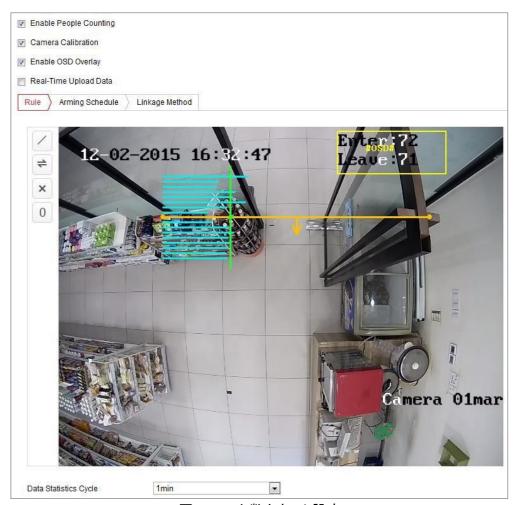


図10-32 人数カウント設定

- 2. 「Enable People Counting」チェックボックスをオンにし、この機能を有効にします。
- 3. 検出ラインを設定します。

ライブ映像上で検出ラインと名付けたオレンジ色のラインを設定でき、ラインを 通って出入りするオブジェクトを検出してカウントします。

- ライブビュー映像の左側にある をクリックします。画像にオレンジ色の線が表示されます。
- 検出ラインをドラッグして位置を調整します。
- 検出ラインの黄色の終点をドラッグして、その長さを調整します。

### お知らせ:

- 検出ラインはカメラ直下の位置に引かれ、出入り口全体を覆うようにしてく ださい。
- 人が残る可能性のある場所に線を引かないでください。
- \*\*をクリックして検出ラインを削除します。
- をクリックして方向を変更します。黄色の矢印は入る方向を示します。
- 4. 「Camera Calibration」チェックボックスをオンにし、カメラキャリブレーションを有効にします。ライブビュー映像には、キャリブレーション線(緑色の縦線)と 青色の横線が数本表示されます。

「Camera Calibration」: カウントする人の幅(通常は肩の幅)を設定します。 十分に設定されたキャリブレーションパラメータは、カウント精度を高めるの に役立ちます。

「Blue Horizontal Lines」: 青色の線が1 本ある場合、通過している人物の検出された幅(通常は肩の幅)が示されます。検出ラインの両側には、最大8 本の青い線を表示できます。これらの線は、キャリブレーション設定の基準となります。

「Calibration Line (Green Vertical Line)」: 左端点からキャリブレーションラインまでの距離(キャリブレーションライン幅)は、人物の設定幅を示します。 青色のライン分布に従って距離を調整するために、キャリブレーションラインをドラッグできます。

「Advanced」: 検知ラインとキャリブレーションラインの位置とサイズを正確に調整できます。

- カーソルをドラッグするか、テキストボックスに値を入力して、検知ライン 開始点と検知ライン終了点を設定します。
- 2) C をクリックしてシステムが自動的に計算した推奨キャリブレーションラインの幅を更新します。

3) カーソルをドラッグするか、値を入力してキャリブレーションを設定します。任意の値を設定することも、実際のニーズに応じて設定することもできます。

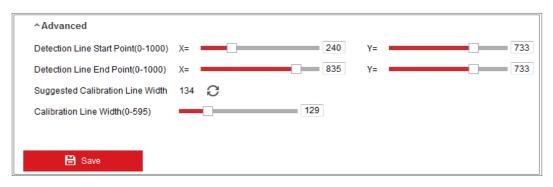


図10-33 人数カウント設定-高度

- 5. カウントデータの設定と表示
  - 1) 「Enable OSD Overlay」チェックボックスをオンにすると、出入りした人のリアルタイム数がライブビデオに表示されます。
  - 2) OSDテキストフレームをドラッグして、実際のニーズに合わせて位置を調整できます。
  - 3) リアルタイムのカウントデータをアップロードする必要がある場合は、「Real-Time Upload Data」チェックボックスをオンにします。
  - 4) カウントサイクルを手動で設定する場合は、「Data Statistics Cycle」から目的の期間を選択します。
  - 5) カウンターをリセットするには、ライブビュー画像の左側にある <sup>0</sup> ボタンを クリックします。
- 6. 「Arming Schedule」をクリックして、アーミングスケジュールを設定します。「タスク2:モーション検知のアーミングスケジュールの設定」を参照してください。
- 7. 「Linkage Method」をクリックして、連携方法を選択します。「タスク3:モーション検知の連動方法の設定」を参照してください。
- 8. 「Save」をクリックし、設定を保存します。

#### お知らせ:

人数統計は、アプリケーションタブで計算されます。「Application」に進み、人数カウント統計を確認します。

## 10.3.4 カウント

カウント機能は、ある設定されたエリアに出入りする人の数を計算するのに役立ち、 出入り口に広く適用されます。

iDSカメラ対応の人数カウント機能と比較して、カウント機能はカメラキャリブレーションを必要としません。

## お知らせ:

できるだけ入口/出口の真上にカメラを設置し、カウント精度を上げるために水平になるようにすることを推奨します。

## 手順:

1. 「Configuration」 > 「Counting」を選択します。

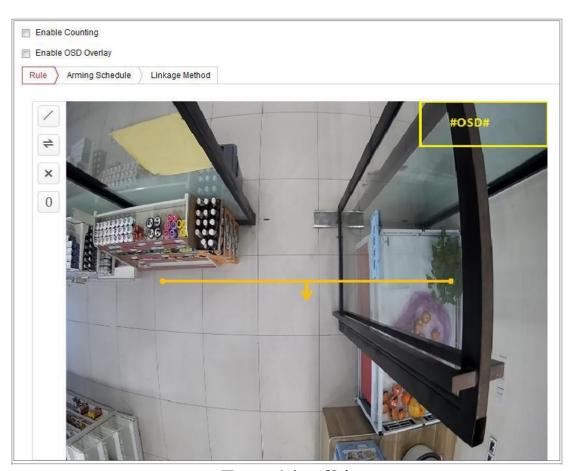


図10-34 カウント設定

- 2. この機能を有効にするには、「Enable Counting」チェックボックスをオンにします。
- 3. 「Enable OSD Overlay」チェックボックスをオンにすると、ライブビデオに映った人のリアルタイム数が表示されます。

4. 検波ラインを設定します。

ライブ映像上で検知ラインと名付けたオレンジ色のラインを設定でき、ラインを通って出入りするオブジェクトを検知してカウントします。

1) をクリックすると検出ラインが描画され、画像上にオレンジ色の検出ラインが表示されます。

### お知らせ:

- 検出ラインはカメラ直下の位置に引かれ、出入り口全体を覆うようにしてください。
- あまり人がいない位置に検知線を引きます。
- 2 検出ラインをクリック・ドラッグして、その位置を調整します。
- 3 検出ラインの2つの終点をクリック・ドラッグして、その長さを調整します。
- 4) \*\* をクリックして検出ラインを削除します。
- 5. 0 ボタンをクリックすると、出入りした人数が0にクリアされます。
- 6. 「Arming Schedule」をクリックしてアーミングスケジュール画面に入り、タイムバー上でマウスをクリックしてドラッグし、時間を設定します。
- 7. 「Linkage Method」をクリックして、連携方法を選択します。
- 8. 「Save」をクリックし、設定を保存します。

#### お知らせ:

カウント統計はアプリケーションタブで計算されます。

「Application」に移動して、カウント統計をチェックします。

# 10.3.5 ヒートマップ

ヒートマップは、色で表されるデータをグラフで表したものです。カメラのヒートマップ機能は、設定されたエリア内の顧客の訪問時間と滞在時間の分析に使用されます。

## 手順:

1. 「Configuration」>「Heat Map」を選択します。

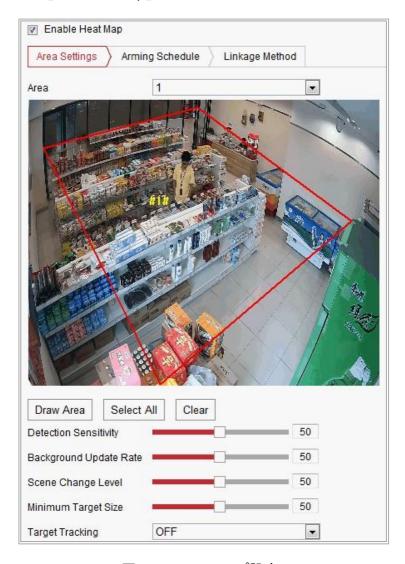


図10-35 ヒートマップ設定

- 2. 「Enable Heat Map」チェックボックスをオンにすると、機能が有効になります。
- 3. 「Area Settings」に進み、検出エリアを描画します。
  ライブビューウィンドウで端点を左クリックして領域を描き、右クリックして領域を描きを終了します。最大8つの領域を設定できます。

*お知らせ:* 「Select All」をクリックすると、ライブビューウィンドウ全体を設定領域として選択できます。または、「Delete」をクリックして、現在の描画領域を削除します。

4. 描画領域のパラメータを設定します。

「Detection Sensitivity」[0~100]: カメラがターゲットを識別する感度を指します。感度が高すぎると、誤情報を引き起こす可能性があります。デフォルト値を50に設定することを推奨します。

「Bckground Update Rate」 [0~100]: :新しいシーンの速度を参照して前のシーンを置き換えます。例: キャビネットの前では、キャビネット以外の人物は、キャビネットからモノが移動した場合はダブルカウントされ、カメラはキャビネット(グッドが削除されたキャビネット)を新しいシーンとして扱います。デフォルト値を50に設定することを推奨します。

「Scene Change Level」[0~100]: 動的な環境、例えば揺れるカーテンに対するカメラの反応のレベルを指します。揺れているカーテンをターゲットとして扱う場合があります。レベルを適切に設定することで、誤情報を回避できます。デフォルト値を50に設定することを推奨します。

「Minimum Target Size」[0~100]: ターゲットを特定するカメラのサイズを指します。実際の環境に合わせて目標サイズを設定することができます。デフォルト値を50に設定することを推奨します。

「Target Track」: ON またはOFF を選択して、ターゲットのトラッキングを有効または無効にします。

- 5. 「Arming Schedule」をクリックしタイムバー上でマウスをクリック・ドラッグして、アーミングスケジュールを設定します。
- 6. 「Linkage Method」をクリックして、監視センターに通知するチェックボックスをオンにして連携方法を選択します。
- 7. 「Save」をクリックし、設定を保存します。

#### お知らせ:

ヒートマップ統計は、「Application」で計算されます。「Application」に進み、ヒートマップ統計を確認します。

## 10.3.6 道路交通

#### 目的:

道路交通モニタリングは、「Vehicle Detection」と「Mixed-traffic Detection」の利用可能です。「Vehicle Detection」では、通過した車両を検知し、ナンバープレートの写真を撮影することができます。また、車両の色や車両ロゴなどの情報を自動認識することができます。「Mixed-traffic Detection」では、歩行者、自動車、非自動車を検知し、対象物(ナンバープレートなしの歩行者/非自動車/自動車用)やナンバープレート(ナンバープレートのある自動車)を把握します。アラーム信号を送信して監視センターに通知し、キャプチャした画像をFTP サーバーにアップロードできます。

お知らせ: 道路交通機能は、モデルによって異なります。

#### ● 検出設定

#### 手順:

- 1. リストから検出タイプを選択します。車両検知と混合交通検知が選択可能です。 *お知らせ:* 道路交通の検知タイプを切り替える場合は、デバイスを再起動して新 しい設定をアクティブにします。
- 2 「Enable」のチェックボックスをオンにし、検出機能を有効にします。
- 3. 対応するドロップダウンリストでレーン番号を選択します。最大4つのレーンを選択できます。
- 4. レーンラインをクリック・ドラッグして位置を設定するか、ラインエンドをクリック・ドラッグしてラインの長さと角度を調整します。
- 5. 映像中の車両の大きさが赤枠の大きさに近くなるように、カメラのズーム倍率を 調整します。赤枠の位置のみ調整可能です。
  - *お知らせ:*レーンごとに一度にキャプチャできるナンバープレートは1 つだけです。
- 6. ナンバープレートの属性が認識できない場合は、ドロップダウンリストからそれ ぞれの略称を選択します。

- 7. アーミングスケジュールを設定します。
  - 1) 「Arming Schedule」をクリックします。
  - 2) タイムバーをクリックし、マウスをドラッグして期間を選択します。設定した スケジュールを削除するには、削除またはすべて削除をクリックします。
  - 3) マウスを各日の終わりに動かすと、コピーダイアログボックスがポップアップ表示され、現在の設定を他の日にコピーできます。
  - 4) 「Save」をクリックし、設定を保存します。

お知らせ: 各期間の時間を重ねることはできません。1 日に最大8つの期間を 設定できます。

- 8. 連携方法を設定します。監視センターに通知し、FTP/メモリーカード/NASにアップロードすることができます。
  - 「Notify Surveillance Center」:イベントが発生した場合に、例外またはアラーム信号をリモート管理ソフトウェアに送信します。
  - 「Upload to FTP/Memory Card/NAS」: アラームが発生したときに画像をキャプチャし、画像をFTPサーバーにアップロードします。画像をローカルSDカードまたは接続されたNASに保存します。
- 9. 「Save」をクリックして、設定を有効にします。

## 10.3.7 キュー管理

キュー管理は、各人のキューイングアップ人数と待ち時間を検出する機能です。 また、カメラは、異なるキューイングアップの効率を比較し、1つのキューの変化 状況を表示するためのレポートを生成します。

機能を使用するには、まず検出ルールを設定する必要があります。キュー管理 の統計を表示するには、アプリケーションに移動します。

## お知らせ:

特定のモデルのみがこの機能をサポートしています。

## ルール設定

本機は、「Regional People Queuing-Up」、「Waiting Time Detection」、「Real-time Upload」をサポートしています。チェックボックスをオンにすると、目的の機能が有効になります。

「Regional People Queuing-Up]: 定義されたリージョンでキューイングアップする 人物を検出して計算し、アラームしきい値条件とアラーム発生の両方が満たされるとアラームを通知します。

「Waiting Time Detection」: 検出エリアに入った各人の待ち時間を検出して演算し、アラームしきい値条件とアラーム発生の両方が成立したときにアラームを通知します。

「Real-time Upload」: ルールリージョンに出入りする人物を検出し、アラームを通知します。

## 手順:

## 1. エリア設定

a) 領域を追加します。最大3つの領域がサポートされます。

領域とは、検出がアクティブである定義された領域です。

領域を描画する場合、ターゲットの有効な領域入力アクションは、その領域 に自分の頭部と肩が入ることに注意してください。

#### 手順:

- a-1 「Add Region」をクリックします。
- a-2 色ドロップダウンリストからリージョンの色を選択します。
- a-3 右クリックしてリージョンを描画し、リージョンの境界を決定します。リージョンでは、最大10 のエッジがサポートされます。

「Move the region」: リージョンを選択してドラッグします。

「Adjust the region boundary」: 領域を選択し、領域の端の終点をドラッグします。

「Delete the region」: リージョンを選択し、「Delete」をクリックします。

#### お知らせ:

- リージョンを描画するときは、リージョンが重ならないようにします。
- 領域は、待ち行列がとることのできるだけのスペースをカバーする 必要があります。

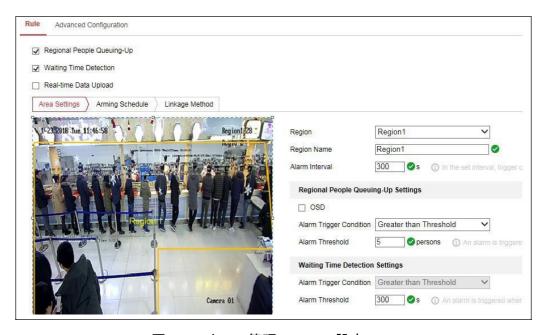


図10-36 キュー管理ルールの設定

- b) 追加したリージョンのパラメータを設定します。
  - b-1 地域名とアラーム間隔を設定します。

「Region Name」: OSD 情報として表示されます。

「Alarm Interval」: 設定したアラーム間隔では、同じ種類のアラームを1回だけ通知します。

b-2 リージョンのキューイングアップ設定を行います。

「OSD」をチェックして、地域名とそのリアルタイムキューイングアップの人数を表示します。

「Alarm Trigger Condition」: 領域内の人数が設定したしきい値より大きい、小さい、等しい、または等しくない場合、アラームが発生します。

「Alarm threshold」: アラームしきい値条件が満たされると、アラームが発生します。

b-3 待ち時間検出の設定をします。

「Alarm Trigger Condition」: 領域内の人数が設定したしきい値より大きい、小さい、等しい、または等しくない場合、アラームが発生します。

「Alarm threshold」: アラームしきい値条件が満たされると、アラームが発生します。

- c) 必要に応じて上記の手順を繰り返して、他の領域を設定します。最大3つの 領域がサポートされます。
- 2. アーミングスケジュール

機能のアーミングスケジュールを設定します。設定期間中は機能が有効です。 「タスク2:モーション検知のアーミングスケジュールの設定」を参照してください。

3. 連動方法を設定します。

発生したアラーム情報の転送や、他のアクションを行うための連携方法を設定することができます。「タスク3:モーション検知の連動方法の設定」を参照してください。

#### 4. 詳細設定

キュー管理バージョンを確認し、フィルターパラメータを設定します。

*お知らせ:* この機能は、キュー管理の検出範囲と感度を変更します。一般的な状況では、フィルター設定は変更されません。必要に応じて、フィルターパラメータの設定について当社営業またはサポートコールにお問い合わせください。

# 第11章 ストレージ設定

#### 準備:

録画設定の前に、ネットワークストレージデバイスまたはローカルストレージデバイスが設定されていることを確認してください。

# 11.1 レコードスケジュールの設定

#### 目的:

カメラの録画には、手動録画とスケジュール録画の2種類があります。このセクションでは、手順に従ってスケジュール録画を設定できます。デフォルトでは、スケジュールされた録画の録画ファイルはローカルストレージまたはネットワークディスクに保存されます。

#### 手順:

1. 「Configuration」>「Storage」>「Schedule Settings」>「Record Schedule」を選択します。

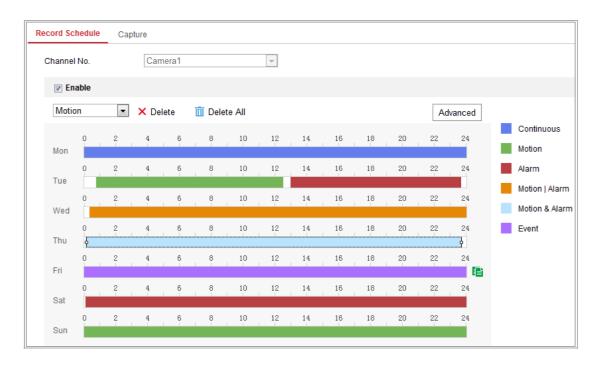


図11-1 録画スケジュール画面

- 2 「Enable」チェックボックスをオンにし、スケジュール録画を有効にします。
- 3. 「Advanced」をクリックして、カメラ録画パラメータを設定します。

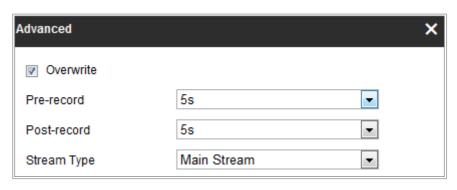


図11-2 レコードパラメータ

● 「Pre-record」: スケジュール時刻またはイベントの前に録画を開始するように設定した時間です。例えば、アラームが10:00 で録画をセットし、録画前の時間が5 秒に設定されている場合、カメラは9:59:55 で録画を開始します。 プリレコード時間は、録画なし、5 秒、10 秒、15 秒、20 秒、25 秒、30 秒または制限なしが設定できます。

「Post-record」: スケジュール時刻またはイベント後に録画を停止するように設定した時間です。例えば、アラーム連動録画が11:00 に終了し、録画後の時間が5 秒に設定されている場合、カメラは11:00:05 まで録画します。 **録画後**の時間は、5 秒、10 秒、30 秒、1 分、2 分、5 分、10 分のいずれかに設定できます。

● 「Stream Type」: 録画するストリームタイプを選択します。

**お知らせ**: 録画パラメータの設定は、モデルによって異なります。

4. 「Record Type」を選択します。録画タイプには、連続、モーション検出、アラーム、モーション|アラーム、モーション&アラーム、イベントがあります。

#### ● 連続

「Continuous」を選択すると、スケジュールの時間に応じてビデオが自動的に 録画されます。

#### ● モーション検出による録画

「Motion Detection」を選択すると、動きが検出されたときに動画が記録されます。

記録スケジュールの設定に加えて、モーション検出エリアを設定し、モーション検出設定画面の連動方法でトリガ・チャンネルのチェックボックスをオンにする必要があります。

詳細については、「10.1.1モーション検出の設定」の「タスク1: モーション検知領域の設定」を参照してください。

#### ● アラームによる録画

「Alarm」を選択すると、外部アラーム入力チャンネルを介してアラームが発生したときにビデオが記録されます。

録画スケジュールの設定に加えて、アラーム入力設定画面の連動方法で、「Alarm Type」を設定し、「Trigger Channel」のチェックボックスをオンにする必要があります。詳細は、「10.1.3 アラーム入力の設定」を参照してください。

#### ● モーション検出とアラームによる録画

「Motion & Alarm」を選択すると、モーション検出とアラーム発生が同時に起きたときに録画を開始されます。

録画スケジュールの設定に加えて、「Motion Detection」と「Alarm Input Settings」の設定が必要です。詳細は、「10.1.1 モーション検出の設定」および「10.1.3 アラーム入力の設定」を参照してください。

#### ● モーション検出による録画 | アラーム

「Motion | Alarm」を選択すると、モーション検出時またはアラーム発生時に 録画を開始されます。

録画スケジュールの設定に加えて、モーション検出およびアラーム入力の 設定を行う必要があります。詳細は、「10.1.1 モーション検出の設定」および「10.1.3 アラーム入力の設定」を参照してください。

### ● イベントによる録画

「Event」を選択した場合、いずれかのイベントが有効になると、録画が開始されます。録画スケジュールの設定に加えて、イベントの設定も必要です。

- 5. 録画タイプを選択し、タイムバー上でマウスをクリック・ドラッグして、レコード スケジュールを設定します。
- 6. 「Save」をクリックし、設定を保存します。

## 11.2 キャプチャスケジュールの設定

#### 目的:

スケジュール設定されたスナップショットとイベント連携スナップショットを設定できます。 撮影した画像は、ローカルストレージまたはネットワークストレージに保存できます。 *手順:* 

1. 「Configuration」>「Storage」>「Storage Settings」>「Capture」を選択します。

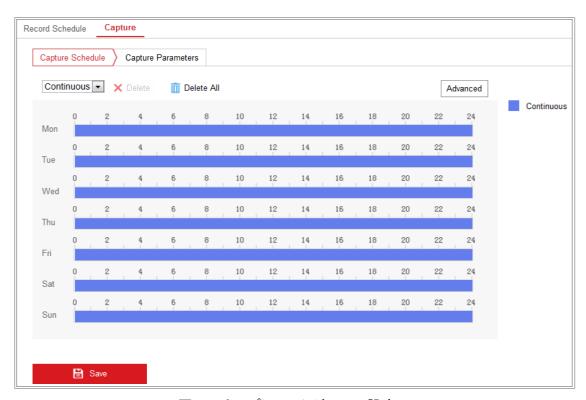


図11-3キャプチャスケジュール設定

2 「Capture Schedule」画面から、タイムバー上でマウスをクリック・ドラッグしてキャプチャスケジュールを設定します。各タイムバーの右側にある緑色のコピーアイコンをクリックすると、レコードスケジュールを他の日にコピーできます。

3. 「Advanced」をクリックして、ストリームタイプを選択します。

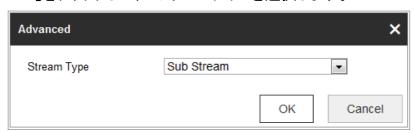


図11-4 キャプチャスケジュールの詳細設定

- 4. 「Save」をクリックし、設定を保存します。
- 5. キャプチャパラメータを設定するには、「Capture Parameters」タブに移動します。
  - (1) 「Enable Timing Snapshot」チェックボックスをオンにし、連続スナップショットを有効にします。
  - (2) キャプチャする画像の「Format」、「Resolution」、「Quality」、「Interval」を選択します。
  - (3) 「Enable Event-triggered Snapshot」チェックボックスをオンにし、イベント連携スナップショットを有効にします。
  - (4)「Format」、「Resolution」、「Quality」、「Interval」、「Capture Number」を選択 します。

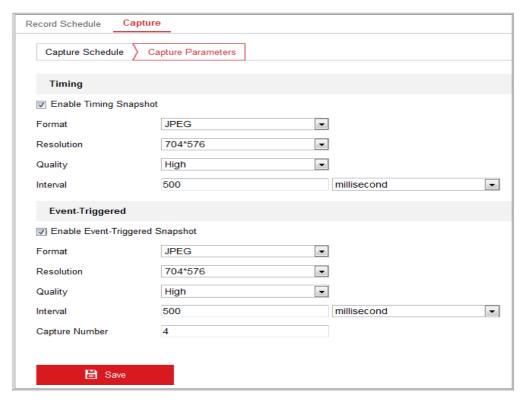


図11-5 キャプチャパラメータの設定

- 6. 2枚の静止画の時間間隔を設定します。
- 7. 「Save」をクリックし、設定を保存します。

### 11.3 ネットHDD の設定

#### 準備:

ネットワークディスクは、ネットワーク内で使用可能であり、記録されたファイル、ログファイル、画像などを保存するように適切に設定されている必要があります。 *手順:* 

- 1. Net HDDを追加します。
  - (1)「Configuration」>「Storage」>「Storage Management」>「Net HDD」を 選択します。



図11-6 ネットワークディスクの追加

- (2) ネットワークディスクのIP アドレスを入力し、ファイルパスを入力します。
- (3) mounting typeを選択します。NFS およびSMB/CIFS が選択可能です。また、SMB/CIFS が選択されている場合は、セキュリティを保証するためにユーザー名とパスワードを設定できます。

*お知らせ:* ファイルパスの作成については、NAS ユーザーマニュアルを参照してください。



- プライバシーを守り、セキュリティリスクからシステムを保護するために、すべての機能およびネットワークデバイスに強力なパスワードを使用することを強く推奨します。パスワードは、製品のセキュリティを強化するために、8 文字以上(大文字、小文字、数字、特殊文字の3つ以上を含む)に設定してください。
- (4)「Save」をクリックして、ネットワークディスクを追加します。
- 2. 追加したネットワークディスクを初期化します。
  - (1) 「Configuration」 > 「Storage 」 > 「Storage Management」 > 「HDD Management」を選択し、ディスクの容量、空き容量、ステータス、タイプ、およびプロパティを表示できます。

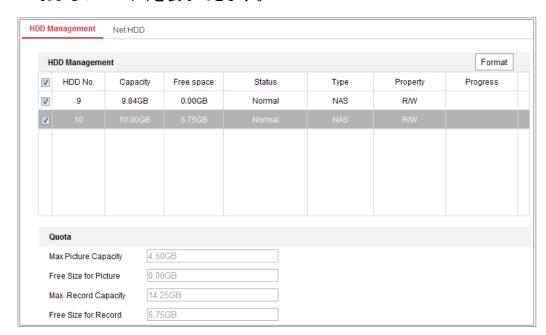


図 11-7 ストレージ管理画面

(2) ディスクのステータスが初期化されていない場合は、対応するチェックボックスをオンにしてディスクを選択し、「Format」をクリックしてディスクの初期化を開始します。

初期化が完了すると、ディスクの状態は正常になります。



図11-8 ディスクステータスの表示

- 3. レコードと写真のクォータを定義します。
  - (1) 画像および記録のクォータパーセンテージを入力します。
  - (2)「Save」をクリックしてブラウザページを更新し、設定を有効にします。

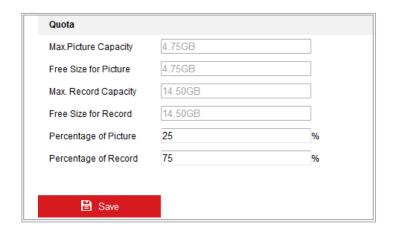


図11-9 クォータ設定

#### お知らせ:

最大 8台の NASディスクをカメラに接続できます。

### 11.4 メモリーカード検出

#### 目的:

メモリーカード検出では、メモリーカードの状態を確認したり、メモリーカードをロック したり、メモリーカードの異常を検出したときに通知を受け取ることができます。

お知らせ: 特定のモデルのみがこの機能をサポートしています。このタブページがWebページに表示されない場合は、カメラがこの機能をサポートしていないか、搭載されているメモリーカードがこの機能に対応していないことを意味しています。機能に対応しているメモリーカードの情報については、販売店にお問い合わせください。

#### 手順:

1. 「Configuration」>「Storage」>「Storage Management」>「Memory Card Detection」を選択します。

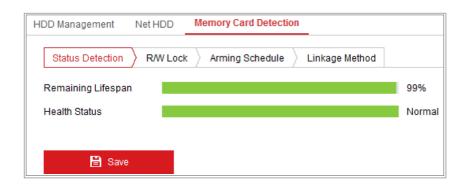


図11-10 メモリーカードの検出

2. 「Status Detection」タブをクリックし、メモリーカードのステータスを表示します。

「Remaining Lifespan」: 空き容量のパーセンテージを示します。メモリーカードの空き容量は、その容量やビットレートなどの要因に左右されます。空き容量が不足している場合は、メモリーカードの交換が必要です。

「Health Status」: メモリーカードの状態を示します。状態の説明には、良好、不良、損傷の3 つがあります。「Arming Schedule」と「Linkage Method」が設定されている場合、ヘルスステータスが良好以外であれば、通知を受け取ります。

*お知らせ:* ヘルスステータスが良好でない場合は、メモリーカードを変更することを推奨します。

3. 「R/W Lock」をクリックして、メモリーカードにロックを追加します。
R/Wロックを追加すると、メモリーカードはロック解除時にのみ読み書きできます。

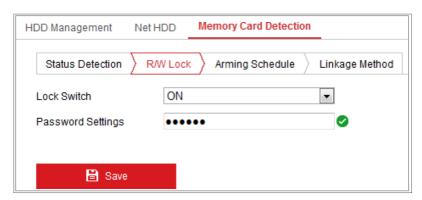


図11-11 R/W ロック設定

#### ● ロックの追加

- (1)「Lock Switch」をオンに設定します。
- (2) パスワードを入力します。
- (3)「Save」をクリックし、設定を保存します。

#### ● ロック解除

- (1) ロックしているカメラでメモリーカードを使用すると、自動的にロック解除が行われ、ユーザーの方々にはロック解除の手順は一切必要ありません。
- ② 別のカメラでメモリーカード(ロック付き)を使用する場合は、「HDD Management」に進み、メモリーカードのロックを手動で解除することができます。メモリーカードを選択し、「Format」ボタンの横にある「Unlock」をクリックします。次に、正しいパスワードを入力してロックを解除します。

#### お知らせ:

- メモリーカードは、ロックが解除されている場合にのみ読み書きできます。
- メモリーカードにロックをかけたカメラを工場出荷時の状態に戻した場合は、「HDD Management」画面からメモリーカードのロックを解除できます。

#### ● ロックの取り外し

- (1)「Lock Switch」をオフに設定します。
- (2)「Password Settings」欄に正しいパスワードを入力します。
- (3)「Save」をクリックし、設定を保存します。
- 4. メモリーカードのヘルスステータスが良好でない場合に通知を受け取りたい場合は、「Arming Schedule」と「Linkage Method」を設定します。「タスク2:モーション検知のアーミングスケジュールの設定」および「タスク3:モーション検知の連動方法の設定」を参照してください。
- 5. 「Save」をクリックして設定を保存します。

### 11.5 Liteストレージの設定

#### 目的:

監視シナリオに動体がない場合は、ビデオストリームのフレームレートとビットレートを下げて、メモリーカードの記憶時間を長くすることが可能です。

#### お知らせ:

- Liteストレージの機能は、カメラの機種によって異なります。
- Liteストレージモードで録画されたビデオファイルは、フルフレームレート (25fps/30fps)で再生されるため、再生処理が速くなります。。
- 1. 「Configuration」>「Storage」>「Storage Management」>「Lite Storage」を選択します。
- 2. 「Enable」チェックボックスをオンにし、Liteストレージ機能を有効にします。
- 3. テキストボックスに保存時間を入力します。SD カードの空き容量は、ページで確認できます。
- 4. 「Save」をクリックし、設定を保存します。

# 第12章 再生

#### 目的:

ここでは、ネットワークディスクやSDカードに保存されているリモート録画映像ファイルを見る方法を説明します。

#### 手順:

1. メニューバーの「Playback」をクリックして再生画面に入ります。

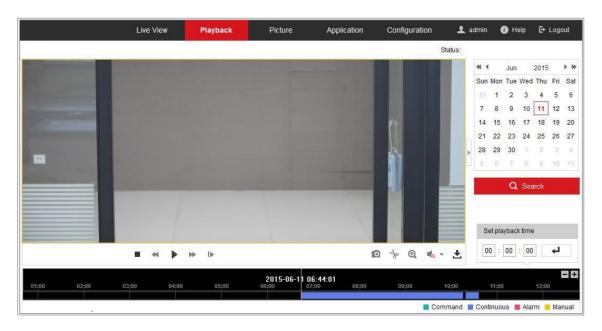


図12-1 再生画面

2. 日付を選択し、「Search」をクリックします。



図12-2 サーチ画面

3. ▶ をクリックしてこの日付にあるビデオファイルを再生します。

再生画面の下部にあるツールバーを使用し、再生プロセスをコントロールできます。



図12-3 再生ツールバー表 12-1 ボタンの説明

ボタン	動作	ボタン	動作
•	再生	0	写真を撮影する
П	一時停止	* / *	ビデオの開始/停止 ファイル
•	停止	<b>*</b>	ボリューム調整 ボリュームON/OFF
*	巻戻し	Ŧ	ダウンロード
₩	早送り	I►	フレーム単位で再生
<b>Q</b> / <b>Q</b>	有効/無効 デジタルズ 一ム		

*お知らせ:* ローカル設定画面では、ダウンロードした再生ビデオファイルと画像のファイルパスをローカルで選択できます。

時間を入力して ◆ をクリックすると、「Set playback time」フィールドで再生ポイントを見つけることができます。また、 ◆ をクリックしてプログレスバーを縮小/拡大することもできます。

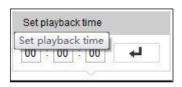


図12-4 再生時間の設定



図12-5 プログレスバー

プログレスバーのビデオの異なる色は、さまざまなビデオタイプに対応しています。

■ Command ■ Continuous ■ Alarm ■ Manual 図12-6 映像の種類

# 第13章 ピクチャー

「Picture」をクリックして、ピクチャー検索画面に入ります。ローカルストレージまたはネットワークストレージに保存されている画像を検索、表示、ダウンロードできます。

#### お知らせ:

- 画像検索を処理する前に、HDD、NAS、またはメモリーカードが正しく設定されていることを確認してください。
- キャプチャスケジュールが設定されていることを確認します。「Configuration」>
  「Storage」>「Schedule Settings」>「Capture」を選択して、取り込みスケジュールを設定します。

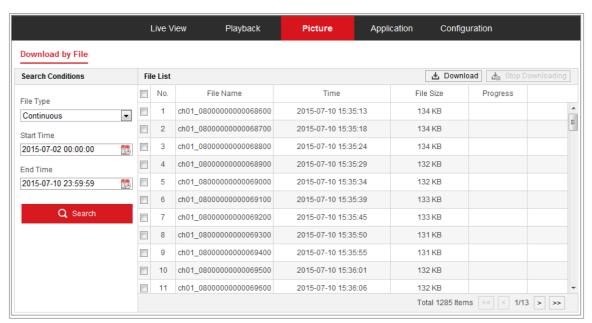


図13-1 ピクチャー・サーチ・画面

#### 手順:

- ドロップダウンリストから「File Type」を選択します。連続、モーション、アラーム、モーション|アラーム、モーション&アラーム、ラインクロッシング、侵入検知、シーンチェンジ検知が選択できます。
- 2. 「Start Time 」と「End Time 」を選択します。
- 3. 「Search」をクリックして、一致する画像を検索します。

4. 画像のチェックボックスをオンにし、「Download」をクリックして選択した画像を ダウンロードします。

### お知らせ:

一度に最大4000枚まで表示できます。

# 第14章 アプリケーション

「Application」をクリックして、統計カウント画面を表示します。ローカルまたはネットワーク上のストレージに保存されているカウントデータを検索、表示、ダウンロードできます。

お知らせ: アプリケーション機能は、モデルによって異なります。

## 14.1 フェイスキャプチャ統計

フェイスキャプチャ機能を有効にすると、キャプチャした顔データをアプリケーションタブから表示およびダウンロードできます。より視覚的な結果を導くために、さまざまなチャートでデータを表示することができます。



図14-1 アプリケーション画面:

#### 手順:

- 1. レポートタイプを選択します。日報、週報、月報、年報を選択可能です。
- 2. 統計の種類を選択します。
- 3. 開始時刻を選択し、「Counting」をクリックします。

集計結果は、統計結果領域に表示されます。「Table」または「Pie chart」をクリックして、結果をさまざまな方法で表示します。

*お知らせ:* カウント結果をテーブルにリストすると、データをエクセルファイルにエクスポートできます。

## 14.2 人数統計

人数計算機能を有効にすると、人数計算データをアプリケーションタブから表示 およびダウンロードできます。より視覚的な計算結果を導くために、さまざまなチャートでデータを表示することができます。

#### 手順:

- 1. レポートタイプを選択します。日報、週報、月報、年報を選択できます。
  - お知らせ: 日次レポートは選択した日付のデータを計算し、週次レポートは選択した日付が属する週のデータを計算し、月次レポートは選択した日付が属する月のデータを計算し、年次レポートは選択した日付が属する年のデータを計算します。
- 2. 統計の種類を選択します。「People Entered」および「People Exited」を選択できます。
- 3. 開始時刻を選択し、「Counting」をクリックします。

集計結果は、統計結果領域に表示されます。「Table」、「Bar」、「Bar Chart」、「Line Chart」をクリックして、結果をさまざまな方法で表示します。

お知らせ: 統計を表示するテーブルを選択すると、エクセルファイルにデータをエクスポートするための「Export」ボタンが表示されます。

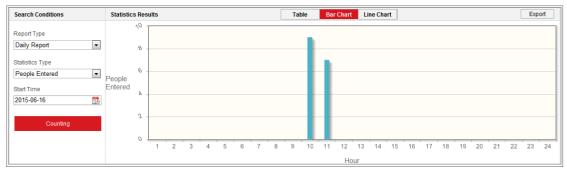


図14-2 人数カウント

# 14.3 ヒートマップ統計

ヒートマップ機能を有効にすると、アプリケーションタブからヒートマップデータを表示してダウンロードできます。より視覚的な結果を導くために、さまざまなチャートでデータを表示することができます。

#### 手順:

- 1. レポートタイプを選択します。日報、週報、月報、年報を選択可能 お知らせ: 日次レポートは選択した日付のデータを計算し、週次レポートは選択 した日付が属する週のデータを計算し、月次レポートは選択した日付が属する 月のデータを計算し、年次レポートは選択した日付が属する年のデータを計算します。
- 2. 開始時刻を選択し、「Counting」をクリックしてヒートマップデータを一覧表示します。
- 3. 「Space Heat Map」または「Time Heat Map」を選択して結果を表示します。 タイムヒートマップを選択して統計を一覧表示すると、エクセルファイルにデータをエクスポートするための「Export」ボタンが表示されます。

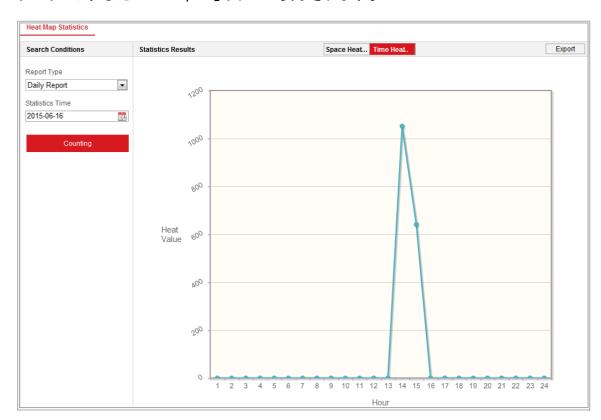


図14-3 時間ヒートマップ

#### お知らせ:

取り付け完了後は電子レンズの調整を行わないことを推奨します。データの精 度不良を引き起こす可能性があります。

### 14.4 カウント統計

カウント機能を有効にすると、アプリケーションタブからカウントデータを表示および ダウンロードできます。より視覚的な結果を導くために、さまざまなチャートでデータ を表示することができます。

#### 手順:

- 1. レポートタイプを選択します。日報、週報、月報、年報を選択可能です。 お知らせ: 日次レポートは選択した日付のデータを計算し、週次レポートは選択 した日付が属する週のデータを計算し、月次レポートは選択した日付が属する 月のデータを計算し、年次レポートは選択した日付が属する年のデータを計算します。
- 2. 統計の種類を選択します。進入者、退出者の選択が可能です。
- 3. 開始時刻を選択し、「Counting」をクリックしてヒートマップデータを一覧表示します。
- 4. 結果を表示するには、表、棒グラフ、または折れ線グラフを選択します。

表を選択して統計をリストすると、エクセルファイルにデータをエクスポートするための「Export」ボタンが表示されます。

### 14.5 キュー管理統計

#### 目的:

キュー管理は、複数のディメンションからのデータ解析およびレポート出力をサポートします。

#### よく使うデータ解析

キュー/リージョン内の特定の待ち時間レベルの人数をキューイングアップするには、キューイングアップ時間分析を使用して、ターゲットリージョンを確認し、 待ち時間レベルを設定します。

- 複数のキュー/リージョンで、特定の待ち時間レベルのキューイングアップ人数を比較するには、キューイングアップ時間分析を使用し、対象領域を確認して、待ち時間レベルを設定します。
- 複数のキュー/リージョン内の異なる待ち時間レベルのキューイングアップ人数を比較するには、キューイングアップ時間分析を使用し、ターゲットリージョンをチェックして、待ち時間レベルを設定します。
- ・ キュー/リージョン内でキューが一定の長さを保持している時間と期間を確認するには、キューステータス分析を使用してターゲットリージョンを確認し、キューの長さレベルを設定します。
- キューが複数のキュー/リージョンで一定の長さを保持している時間と期間を 比較するには、キューステータス分析を使用し、対象領域を確認してキュー の長さレベルを設定します。
- キューが複数のキュー/リージョンで異なる長さに留まっている時間と継続時間を比較するには、キューステータス分析を使用して、ターゲットリージョンを確認し、キューの長さレベルを設定します。

### 14.5.1 キューイングアップ時間解析

#### 目的:

キューイングアップ時間解析は、さまざまな待機時間レベルの人数を計算します。 地域比較と複数の待ち時間レベルの比較が可能です。

#### 手順:

1. 「Statistic Type」を選択します。

「Regional Comparison」: 異なる地域のキューイングアップ人数を比較します。

a) 1つまたは複数のリージョンをチェックします。

b) 待機時間レベルを設定します。希望の時間範囲ラジオボタンと入力値を確認します。

たとえば、10分を超えて待機する人数を表示する場合は、3番目のラジオボタンをオンにして、対応するテキストボックスに600を入力します。

「Multi-Level Comparison」: 待ち行列を作る人数を、待ち時間レベルの違いによって比較します。

- a) 1つまたは複数のリージョンをチェックします。
  - a-1 待機時間レベルを設定します。1つまたは複数の希望する時間範囲の チェックボックスと入力値をチェックします。
  - a-2 例えば、待機時間が10分を超え、待機時間が3分未満の人数を比較する場合は、最初と3番目のラジオボタンを確認し、対応するテキストボックスに600と180を入力します。
- 2. 「Report Type」を選択します。日報、週報、月報、カスタムに対応しています。
- 3. 「Statistics Time」を選択します。
- 4. 「Counting」をクリックしてレポートを生成します。
- 5. 右上隅にある「Export」をクリックして、目的の形式(.txt または xls.が選択可能)でデータをエクスポートします。

### 14.5.2 キューステータス解析

#### 目的:

キューステータス分析は、キューが特定の長さを維持する時間と期間を計算します。 地域比較と複数のキューの長さレベル比較がサポートされています。

#### 手順:

1. 「Statistic Type」を選択します。

「Regional Comparison」:キューが異なる地域の特定の長さに留まる時間と期間を比較します。

- a) 1つ以上の領域をチェックします。
- b) キューの長さレベルを設定します。

ここでのキュー長とは、リージョン内の人数を意味します。

たとえば、キューが1つのリージョンに10人を超える人数を保持している時間を確認するには、3番目のラジオボタンをオンにして、対応するテキストボックスに10を入力します。

「Multi-Level Comparison」: 異なるキューの長さレベルでキューの時間と継続時間を比較します。

- a) 1 つまたは複数のリージョンをチェックします。
- b) キューの長さレベルを設定します。1つまたは複数の希望する範囲のチェックボックスと入力値をチェックします。
- 2. 「Report Type」を選択します。日報、週報、月報、カスタムに対応しています。
- 3. 「Statistics Time Iを選択します。
- 4. 「Counting」をクリックしてレポートを生成します。
- 5. 右上隅にある「Export」をクリックして、目的の形式(.txt またはxls.が選択可能)でデータをエクスポートします。

### 14.5.3 元データ

#### 元データの保存

キュー管理の未処理データは、デバイスのローカルストレージに保存されます。 内蔵メモリーカードを装着すると、最大1口分のデータを保存できます。メモリーカードを装着していない場合は、1週間分のデータしか保存できません。

#### 元データのエクスポート

待ち行列管理の元データ輸出は、ウェブブラウザでは利用できません。詳細な分析のために、RTSP プロトコルを介してデータを取得することができます。

## 14.6 オープンプラットフォーム

#### 目的:

オープンプラットフォームでは、サードパーティの機能開発用のアプリケーションをインストールすることができます。

#### お知らせ:

- 特定のモデルのみが機能をサポートしており、実際の表示はお使いのカメラモ デルによって異なる場合があります。
- オープンプラットフォーム機能を使用する場合、IPアドレスとカメラIPアドレスを 192.168.252.Xに設定することは推奨されません。

#### 手順:

1. 「Configuration」>「Open Platform」を選択し、「Record Schedule Settings」画面を表示します。

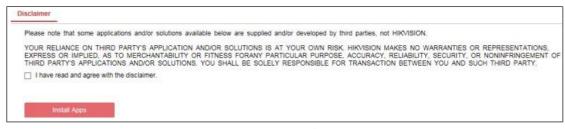


図14-4 免責事項

- 2. 免責事項を読み、チェックボックスをオンにします。
- 3. 「Install Apps」をクリックします。

4. 「Browse」をクリックして、インポートしたアプリケーションパッケージを選択します。

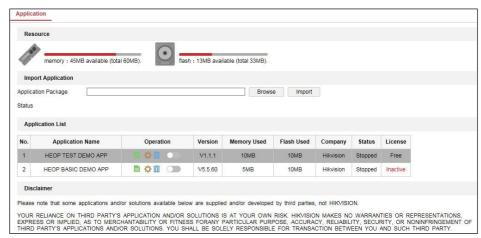


図14-5 オープンプラットフォーム

- 5. 「Import」をクリックすると、アプリケーションがインストールされます。
- 6. インストールされているアプリケーションとその関連情報(バージョン、使用メモリ、フラッシュメモリ、会社、ステータス、ライセンスなど)がリストに表示されます。

「操作(Operation)」リストで■ をクリックしてログをエクスポートし、 をクリック し権限を設定します。 で をクリックしてアプリケーションを削除し、 をクリックしてアプリケーションを有効または無効にします。

#### お知らせ:

☆ をクリックすると、「Get Video Stream」と「Camera Setting Authorization」の2つのチェックボックスがあります。

- 他社製アプリケーションでビデオストリームを取得する必要がある場合は、「Get Video Stream」チェックボックスをオンにして機能を有効にします。
- サードパーティ製のアプリケーションでカメラパラメータを取得または設定する 必要がある場合は、「Camera Setting Authorization」チェックボックスをオンに し、機能を有効にします。

7. アプリケーションをインストールしている場合は、目的のアプリケーションを選択してライセンスを表示するか、「Browse」をクリックして各アプリケーションのライセンスをインポートできます。ライセンスステータスには、無料、無効、有効、有効期限切れの4つがあります。無料とは、アプリケーションが無償で使用されており、ライセンスキーをインポートする必要がないことを意味します。無効とは、アプリケーションを使用する前にライセンスキーをインポートする必要があることを意味します。

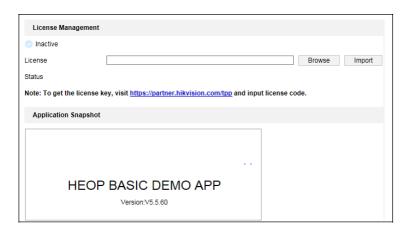


図14-6 インポートライセンス

#### お知らせ:

アプリケーションパッケージをインポートする前に、以下の要件が満たされていることを確認してください。

- インポートしたアプリケーションに同じ名前を付けることはできません。
- インポートしたアプリケーションのフラッシュメモリサイズは、デバイスの空きフラッシュメモリより小さくしてください。
- インポートするアプリケーションのメモリサイズは、デバイスの空きメモリより小さくする必要があります。

# 付録

### 付録1 SADP ソフトウェアの概要

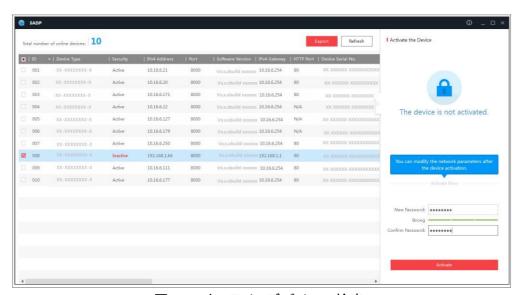
#### ● SADPの説明

SADP (Search Active Devices Protocol)は、ユーザーフレンドリーでインストールのないオンラインデバイス検索ツールです。サブネット内のアクティブなオンラインデバイスを検索し、デバイスの情報を表示します。このソフトウェアを使用して、デバイスの基本的なネットワーク情報を変更することもできます。

### ● アクティブなデバイスをオンラインで検索

#### ♦ オンラインデバイスの自動検索

SADP ソフトウェアを起動すると、コンピュータが検出したサブネットから15秒 ごとにオンラインデバイスが自動的に検索されます。オンラインデバイス画面で検索されたデバイスの総数と情報が表示されます。デバイスの種類、IP アドレス、ポート番号などのデバイス情報が表示されます。



図A.1.1 オンラインデバイスの検索

#### お知らせ:

デバイスは、オンラインになってから15秒後に検索してリストに表示できます。 オフラインになってから45秒後にリストから削除されます。

#### ♦ オンラインデバイスの手動検索

オンラインデバイスリストを手動で更新するには、Refresh をクリックします。 新しく検索されたデバイスがリストに追加されます。

▶ をクリックしてデバイステーブルを展開し、右側のネットワークパラメータパネルを非表示にするか、 ▼ をクリックしてネットワークパラメータパネルを表示します。

### ● ネットワークパラメータの変更

#### 手順:

- 1. デバイスリストで変更するデバイスを選択すると、右側の「Modify Network Parameters」パネルにデバイスのネットワークパラメータが表示されます。
- 2 IPアドレスやポート番号など、変更可能なネットワークパラメータを編集します。
- 3. 「Admin Password」欄にデバイスの管理者アカウントのパスワードを入力し、

Modify をクリックして変更を保存します。



● プライバシーを守り、セキュリティリスクからシステムを保護するために、 すべての機能およびネットワークデバイスに強力なパスワードを使用す ることを強く推奨します。パスワードは、製品のセキュリティを強化するた めに、8 文字以上(大文字、小文字、数字、特殊文字の3つ以上を含む) に設定してください。



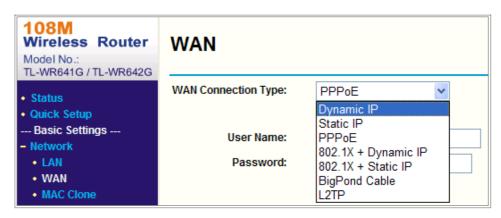
図A.1.2 ネットワークパラメータの変更

## 付録2 ポートマッピング

TP-LINKルータ(TL-WR641G)の設定は以下のとおりです。設定は、ルーターのモデルによって異なります。

#### 手順:

1. 次のように、「WAN Connection Type」を選択します:



図A.2.1 WAN 接続タイプの選択

2 IPアドレスやサブネットマスクの設定など、ルーターのLANパラメータを次の図のように設定します。



図A.2.2 LAN パラメータの設定

3. 「Forwarding」の仮想サーバーでポートマッピングを設定します。デフォルトでは、カメラはポート80、8000、554 を使用します。これらのポートフォリオ価値は、ウェブブラウザまたはクライアントソフトウェアで変更できます。

#### 例:

カメラが同じルーターに接続されている場合、IP アドレス192.168.1.23 でカメラのポートを80、8000、554、8200 に、別のカメラのポートをIP 192.168.1.24 で81、8001、555、8201 に設定できます。以下の手順を参照してください:

#### 手順:

- 1. 上述の設定として、ネットワークカメラのポート80、8000、554、8200を 192.168.1.23でマップします
- 2 ネットワークカメラのポート81、8001、555、8201 を192.168.1.24 にマップします。
- 3. 「ALL」または「TCP」プロトコルを有効にします。
- 4. 「Enable」チェックボックスをオンにし、「Save」をクリックし、設定を保存します。



図A.2.3 ポートマッピング

*お知らせ:* ネットワークカメラのポートは、他のポートと競合できません。たとえば、ルーターのWeb 管理ポートの一部は80 です。管理ポートと同じ場合は、カメラポートを変更します。

# アイリスオーヤマ株式会社

#### ■ 新規購入・導入をご検討のお客様へ

当社営業もしくは下記窓口までご相談ください。

IOTソリューション事業部 TEL **03-5843-7747** (受付時間)平日9:00~17:00

■ 製品の設置・施工・アフターサービスについてのお問い合わせ

サポートコール 0800-111-5300 (通話料無料)

〈受付時間〉平日9:00~17:00、土·日·祝日9:00~12:00/13:00~17:00 (年末年始·夏期休業期間·会社都合による休日を除く)