アイリスオーヤマ

AI カメラ　AG シリーズ

取扱説明書

UD18644B

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。
- 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。

法的免責事項

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 12

2.1.3 セキュリティ質問の設定 16

2.2 WAN 経由でのネットワークカメラの設定 17

2.2.1 固定 IP 接続 17

2.2.2 動的 IP 接続 18

第 3 章 ネットワークカメラへのアクセス 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 23

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 23

4.2 WPS 機能付き簡単 Wi-Fi 接続 28

4.3 ワイヤレスネットワーク接続の IP プロパティ設定 30

第 5 章 ライブビュー 32

5.1 ライブビューページ 32

5.2 ライブ操作 33

5.3 手動で 録画/撮影する 35

5.4 クイックセットアップ 35

5.5 PTZ コントロールの操作 36

5.5.1 PTZ コントロールパネル 36

5.5.2 プリセットの設定/呼び出し 37

5.5.3 パトロールの設定/呼び出し 39

5.6 プラグインのインストール 40

第 6 章 ネットワークカメラの設定 41

6.1 ローカルパラメータの設定 41

6.2 システム設定 43

6.2.1 基本情報の設定 43

6.2.2 時間設定 43

6.2.3 RS-232 設定 45

6.2.4 RS-485 設定 46

6.2.5 DST 設定 47

6.2.6 外部デバイスの設定 48
6.2.7 VCA リソースの設定 49
6.2.8 メタデータ設定 49
6.2.9 オープンソース・ソフトウェア・ライセンス 50

6.3 メンテナンス 50
6.3.1 アップグレードとメンテナンス 50
6.3.2 ログ 52
6.3.3 システムサービス 53
6.3.4 セキュリティ監査ログ 53

6.4 セキュリティ設定 55
6.4.1 認証 55
6.4.2 IP アドレスフィルタ 57
6.4.3 セキュリティサービス 58
6.4.4 高度なセキュリティ 59
6.4.5 証明書管理 60

6.5 ユーザー管理 62
6.5.1 ユーザー管理 62
6.5.2 セキュリティ問題 65
6.5.3 オンラインユーザー 66

第 7 章 ネットワーク設定 67

7.1 基本設定 67
7.1.1 TCP/IP 設定 67
7.1.2 DDNS 設定 69
7.1.3 PPPoE 設定 70
7.1.4 ポート設定 71
7.1.5 NAT（ネットワークアドレス変換）設定 73
7.1.6 マルチキャストの設定 74

7.2 詳細設定 75
7.2.1 SNMP 設定 75
7.2.2 FTP 設定 77
7.2.3 E メール設定の指定 79
7.2.4 プラットフォームアクセス 81
7.2.5 ワイヤレスダイヤル 82
7.2.6 HTTPS 設定 83
7.2.7 QoS 設定 84
7.2.8 802.1X の設定 86
7.2.9 統合プロトコル 87
7.2.10 帯域幅適応 88
7.2.11 ネットワークサービス 88
7.2.12 スムーズストリーミング 89
7.2.13 HTTP リスニングの設定 91
7.2.14 SRTP 設定 92

7.2.15 アラームサーバーの設定 92
第 8 章 ビデオ/オーディオ設定 94
8.1 ビデオ設定 94
8.1.1 ビデオ設定 94
8.1.2 カスタムビデオ 98
8.2 オーディオ設定 99
8.3 ROI エンコーディングの設定 100
8.4 ストリーム上の情報表示 102
8.5 ターゲットクロッピングの設定 103
第 9 章 画像設定 104
9.1 ディスプレイ設定 104
9.2 OSD 設定 109
9.3 プライバシーマスクの設定 110
9.4 画像オーバーレイの設定 112
9.5 画面切り換えパラメータの設定 113
第 10 章 イベント設定 114
10.1 基本イベント 114
10.1.1 モーション検出の設定 114
10.1.2 ビデオ改ざんアラームの設定 121
10.1.3 アラーム入力の設定 121
10.1.4 アラーム出力の設定 123
10.1.5 例外アラームの設定 123
10.1.6 アラームライト出力の点滅の設定 124
10.1.7 ビデオのパラメータの設定 125
10.1.8 ビデオ品質診断 126
10.1.9 振動検出 127
10.1.10 音声アラーム出力の設定 128
10.1.11 その他のアラームの設定 129
10.2 スマートイベント 132
10.2.1 オーディオ例外検出の設定 132
10.2.2 デフォーカス検出の設定 134
10.2.3 シーンチェンジ検出の設定 135
10.2.4 顔検出の設定 136
10.2.5 侵入検知の設定 137
10.2.6 ライン交差検知の設定 140
10.2.7 領域進入検出の設定 142
10.2.8 領域退出検出の設定 144
10.2.9 無人手荷物検出の設定 146

10.2.10 オブジェクトの退出検知の設定 148
10.3 VCA 設定 150
10.3.1 フェイスキャプチャ 150
10.3.2 カウント 154
10.3.3 道路交通 156
10.3.4 キュー管理 160
10.3.5 ヘルメット検出 163
10.3.6 顔の比較とモデリング 164
10.3.7 マルチターゲット型検出 168
10.3.8 顔カウント 172
第 11 章 ストレージ設定 177
11.1 レコードスケジュールの設定 177
11.2 キャプチャスケジュールの設定 180
11.3 HDD 管理の設定 183
11.4 Net HDD の設定 184
11.5 メモリカード検出 186
11.6 Lite ストレージの設定 188
11.7 クラウドストレージの設定 189
第 12 章 再生 190
第 13 章 ピクチャー 192
第 14 章 アプリケーション 193
14.1 フェイスキャプチャ統計 193
14.2 人数統計 194
14.3 カウント統計 194
14.4 顔画像比較統計 195
14.5 キュー管理統計 196
14.5.1 キューイングアップ時間解析 196
14.5.2 キューステータス分析 198
14.5.3 元データ 199
第 15 章 スマートディスプレイ 200
付録 201
付録 1 SADP ソフトウェアの概要 201
付録 2 ポートマッピング 204

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

表示

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:

- 本機をインターネットにアクセスして使用する場合、ネットワークセキュリティ上のリスクが生じる可能性があることを必ずご確認ください。ネットワーク上の攻撃や情報漏洩を防ぐために、ご自身でネットワークセキュリティを強化してください。本機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。
- 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保守を推奨します。このようなサービスが必要な場合は、弊社までお問い合わせください。

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、ネットワークカメラをコンピュータと同じサブネットに接続し、SADP または iVMS-4200 ソフトウェアをインストールしてネットワークカメラの IP を検索および変更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

以下の図は、ネットワークカメラとコンピュータの 2 つのケーブル接続方法を示しています。

目的:

- ネットワークカメラをテストするには、図 2-1 に示すように、ネットワークケーブルを使用してネットワークカメラをコンピュータに直接接続します。
- スイッチまたはルータを経由して LAN 経由でネットワークカメラを設定するには、図 2-2 を参照してください。

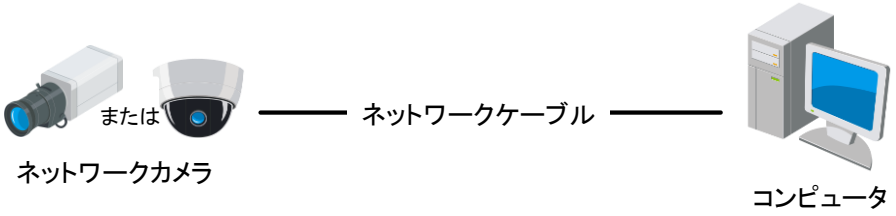


図 2-1 直接接続

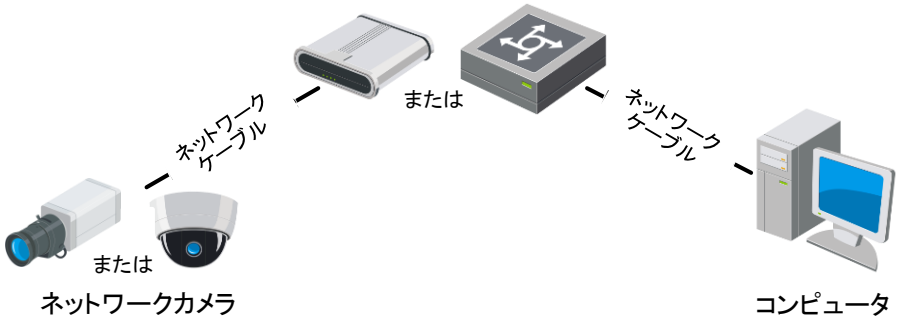


図 2-2 スイッチまたはルータ経由の接続

2.1.2 カメラの起動

カメラを使用する前に、強力な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、SADP、クライアントソフトウェアのいずれからも起動することができます。

お知らせ:

クライアントソフトウェアのアクティベーションの詳細については、クライアントソフトウェアの取扱説明書を参照してください。

❖ 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欄に IP アドレスを入力し、クリックして「Activation」画面を表示します。

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。

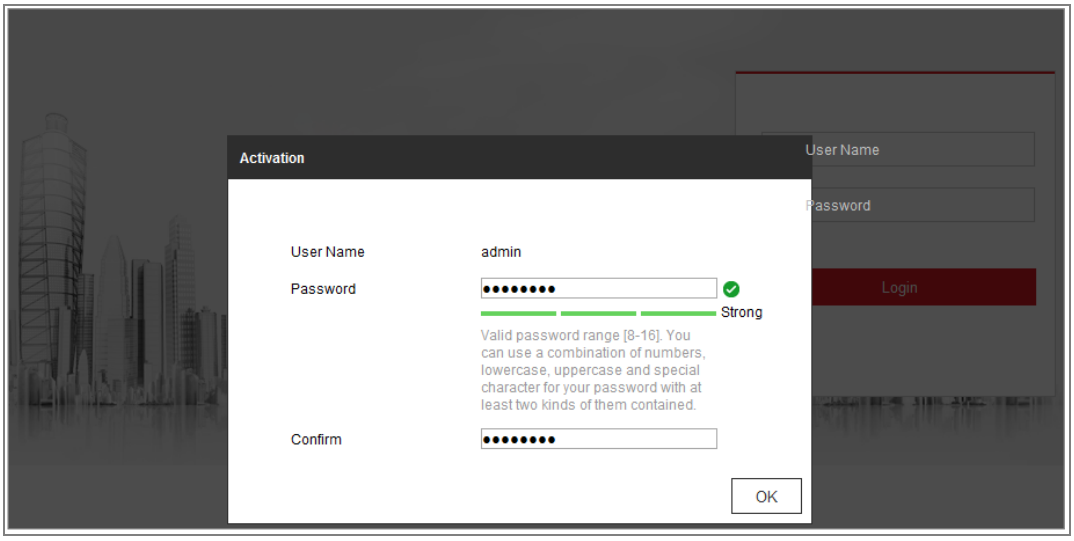


図 2-3 Web ブラウザによる起動

3. パスワードを作成し入力します。

   ユーザー名を含むパスワードは入力できません。

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」をクリックしパスワードを保存し、ライブビュー画面を表示します。

❖ 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、およびパスワードの変更に使用されます。

公式ウェブサイトから SADP ソフトウェアを入手し、画面の表示に従って 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ています。

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。起動に失敗した場合は、パスワードが要件を満たしていることを確認し、再度お試してください。

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。

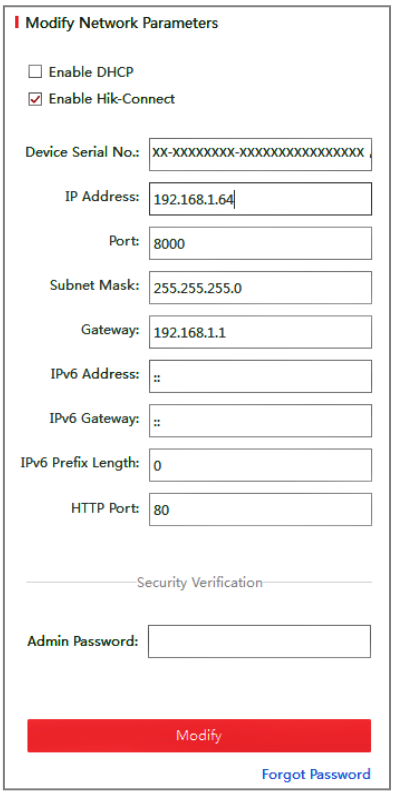


図 2-5 IP アドレスの変更

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:

このセクションでは、ネットワークカメラを固定 IP または動的 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経由で接続したり、WAN に直接接続したりできます。

- **ルータ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については、「2.1.2 カメラの起動」を参照してください。
3. ルータに固定 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、ルータによって異なります。ポートマッピングについては、ルータ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経由して、ネットワークカメラにアクセスします。

図 2-6 固定 IP を使用したルータ経由の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については、「2.1.2 カメラの起動」を参照してください。

図 2-7 固定 IP でカメラに直接アクセスする

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。動的 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に接続できます。

- **ルータ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に接続します。
2. カメラで、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については、「2.1.2 カメラの起動」を参照してください。
3. ルータで、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。

4. 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、ルータによって異なります。ポートマッピングについては、ルータ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. 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。
6. ルータの設定画面で DDNS を設定します。
7. 適用されたドメイン名でカメラにアクセスします。

- **モデム経由でネットワークカメラを接続する**

目的:

このカメラは PPPoE オートダイヤルアップ機能に対応しています。カメラがモデムに接続されると、カメラは 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。詳細な設定については、「7.1.3 PPPoE の設定」を参照してください。

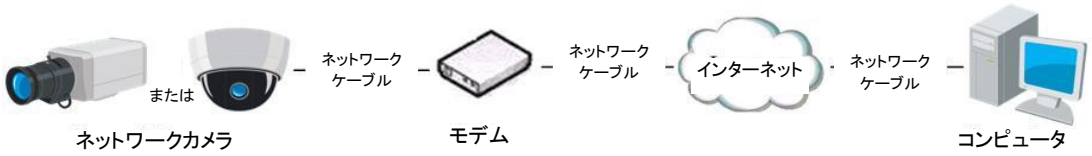


図 2-7 動的 IP でカメラにアクセスする

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 の不都合を解決するには、DDNS プロバイダ（DynDns.com など）からドメイン名を取得する必要があります。通常のドメイン名解決とプライベートドメイン名解決を行うには、以下の手順に従って問題を解決してください。

♦ 通常のドメイン名解決

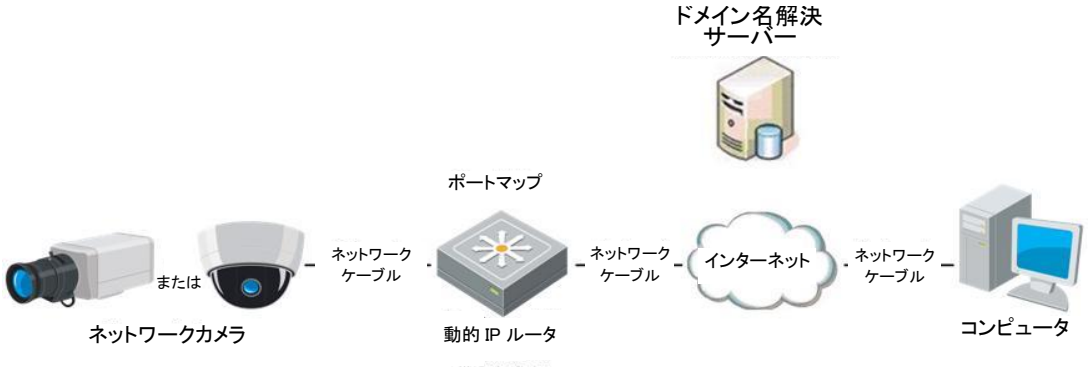


図 2-8 通常のドメイン名解決

手順:

1. 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。
2. ネットワークカメラの「DDNS Settings」画面で DDNS 設定を行います。詳細な設定については、「7.1.2DDNS 設定」を参照してください。
3. 適用されたドメイン名でカメラにアクセスします。

第3章　ネットワークカメラへのアクセス

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表示します。

   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、「Login」をクリックします。

   管理者は、デバイスアカウントおよびユーザー/オペレーター権限を適切に設定する必要があります。不要なアカウントおよびユーザー/オペレーターの権限は削除してください。

お知らせ:

管理者/ユーザー/オペレーターがパスワード入力を 7 回失敗すると、IP アドレスがロックされます。

図 3-1 ログイン画面

4. 「Login」をクリックします。

5. ライブビデオを表示し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:

プラグインフリーのライブビューに対応しているカメラで、Google Chrome 57 以降または Mozilla Firefox 52 以降を使用している場合は、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/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。

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、Wi-Fi モジュールが内蔵されている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

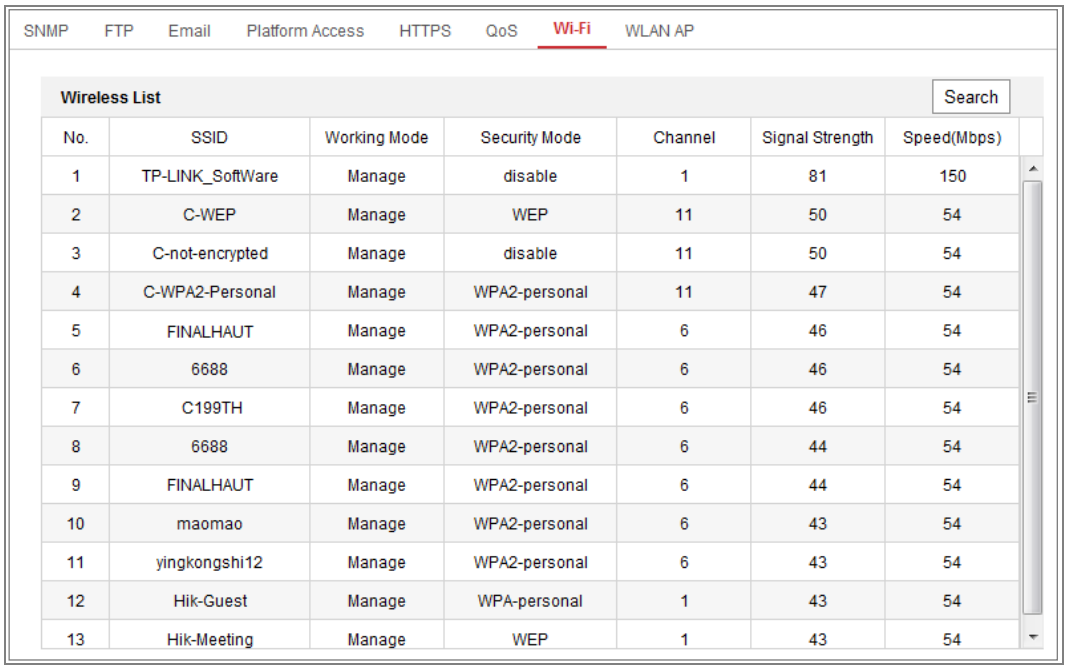
目的:

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。



No.	SSID	Working Mode	Security Mode	Channel	Signal Strength	Speed(Mbps)
1	TP-LINK_SoftWare	Manage	disable	1	81	150
2	C-WEP	Manage	WEP	11	50	54
3	C-not-encrypted	Manage	disable	11	50	54
4	C-WPA2-Personal	Manage	WPA2-personal	11	47	54
5	FINALHAUT	Manage	WPA2-personal	6	46	54
6	6688	Manage	WPA2-personal	6	46	54
7	C199TH	Manage	WPA2-personal	6	46	54
8	6688	Manage	WPA2-personal	6	44	54
9	FINALHAUT	Manage	WPA2-personal	6	44	54
10	maomao	Manage	WPA2-personal	6	43	54
11	yingkongshi12	Manage	WPA2-personal	6	43	54
12	Hik-Guest	Manage	WPA-personal	1	43	54
13	Hik-Meeting	Manage	WEP	1	43	54

図 4-1Wi-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。

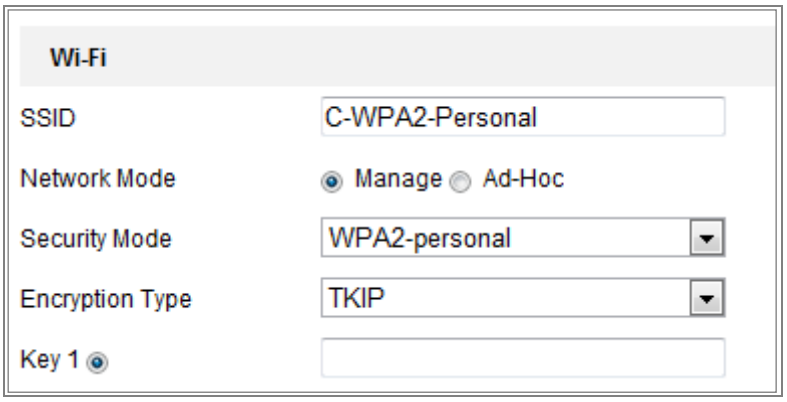


図 4-2 Wi-Fi 設定管理モード

4. ラジオボタンをチェックして「Network Mode」の「Manage」を選択します。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ワイヤレス接続

「Ad-Hoc」モードを選択した場合、ワイヤレスカメラをルータ経由で接続する必要はありません。この手順は、ネットワークケーブルを使用してカメラと PC を直接接続する場合と同じです。

手順:

1. 「Ad-Hoc」モードを選択します。

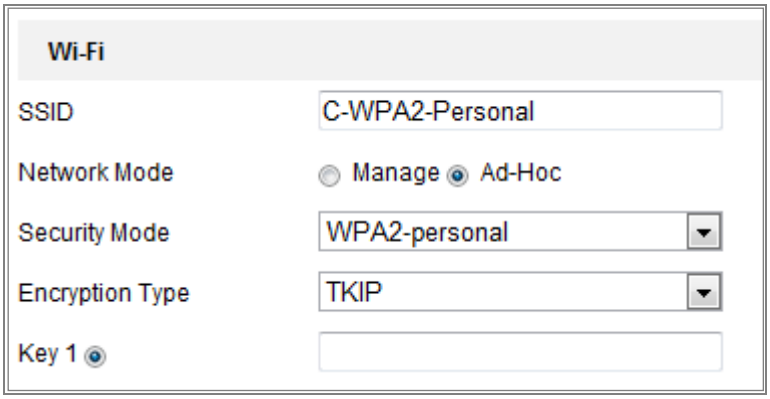


図 4-3 Wi-Fi 設定-アドホックモード

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、カメラの SSID が一覧表示されます。

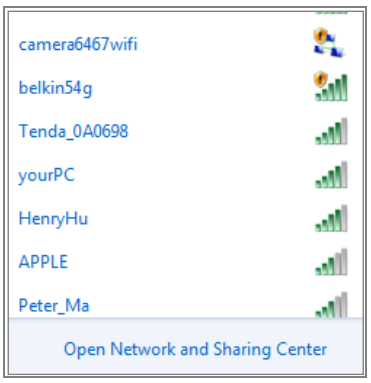


図 4-4 アドホック接続ポイント

6. SSID を選択して接続します。

セキュリティモードの説明:

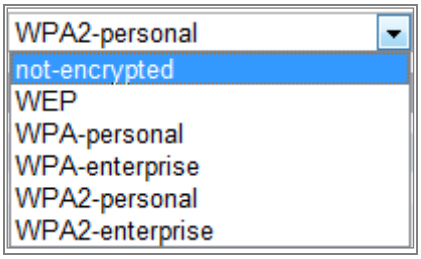


図 4-5 セキュリティモード

「Security Mode」は、「not-encrypted」、「WEP」、「WPA-personal」、「WPA-enterprise」、「WPA2-personal」、「WPA2-enterprise」から選択できます。

WEP モード:

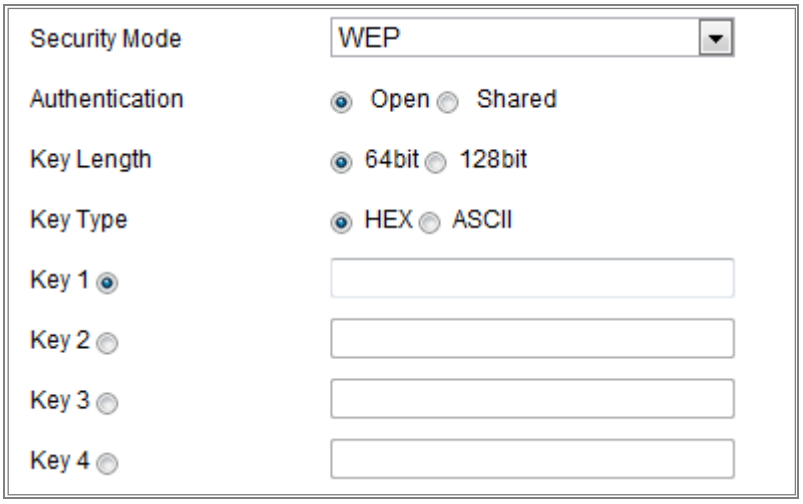


図 4-6 WEP モード

- 「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てください。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 – この方法では、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-personal」および「WPA2-personal」モード:

アクセスポイントに必要な共有鍵を 16 進数またはパスフレーズで入力します。

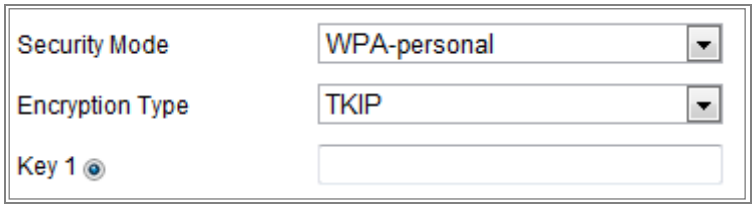


図 4-7 セキュリティモード –「WPA-personal」

「WPA-enterprise」および「WPA2-enterprise」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:

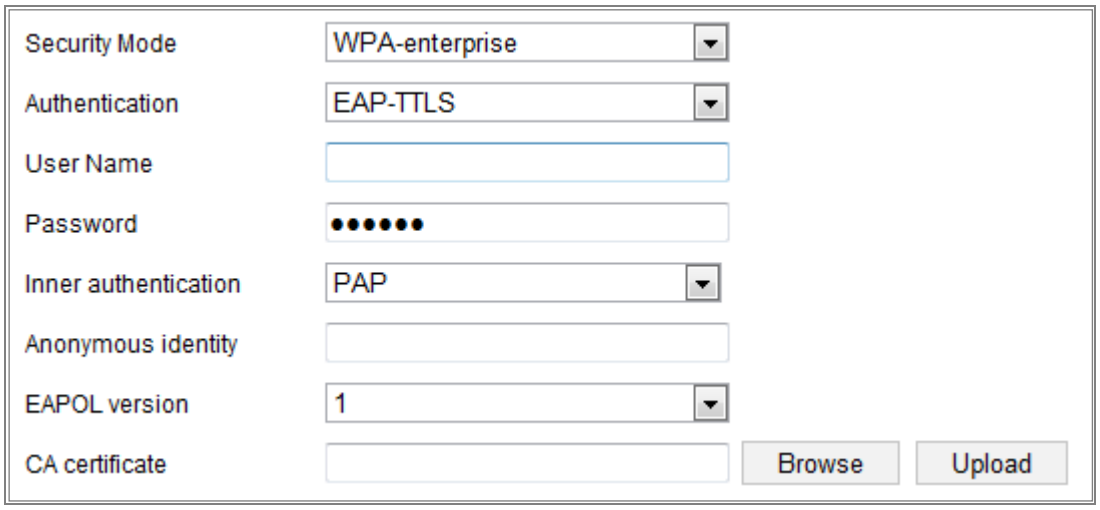


図 4-8 EAP-TLS

- 「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 機能を活用にします。

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:

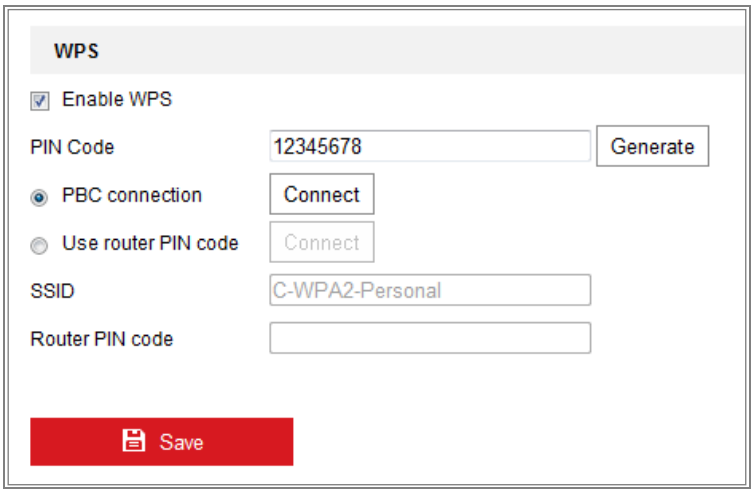
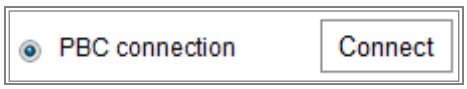


図 4-9 Wi-Fi 設定 -「WPS」

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）を押すだけのプッシュボタン設定のことです。

1. チェックボックス ☑ Enable WPS をオンにすると、WPS が有効になります。
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。
5. 「Connect」をクリックします。
   ルータとカメラの両方で PBC モードを有効にすると、カメラと無線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に表示（ステッカーまたはディスプレイ）されている個人識別番号（PIN）を読み取ってください。その後、その 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）に接続します。

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。

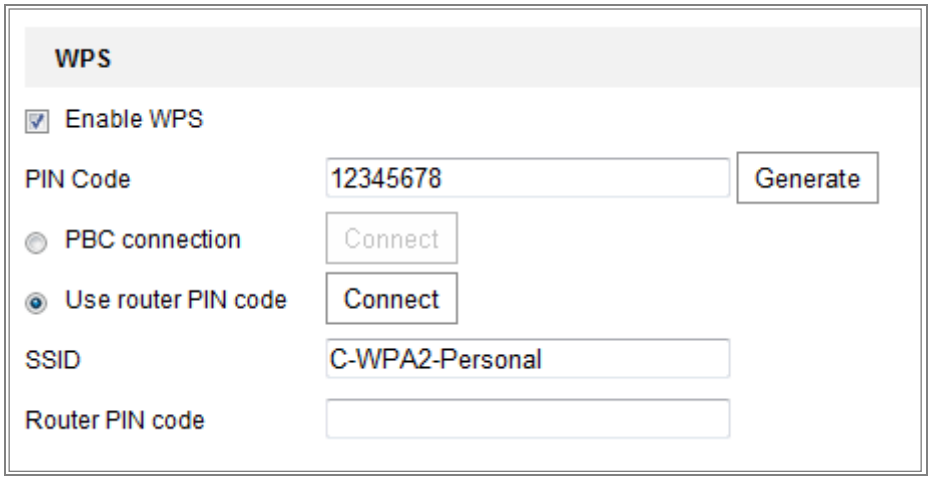


図 4-10 暗証番号の使用

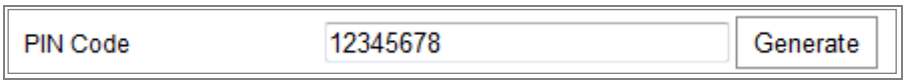
ルータ側から PIN コードが生成された場合は、ルータ側から取得した PIN コードを「Router PIN code」に入力してください。

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、ルータにコードを入力し、ルータに 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設定画面のデフォルト 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、デフォルトの IP アドレスを変更できます。

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。

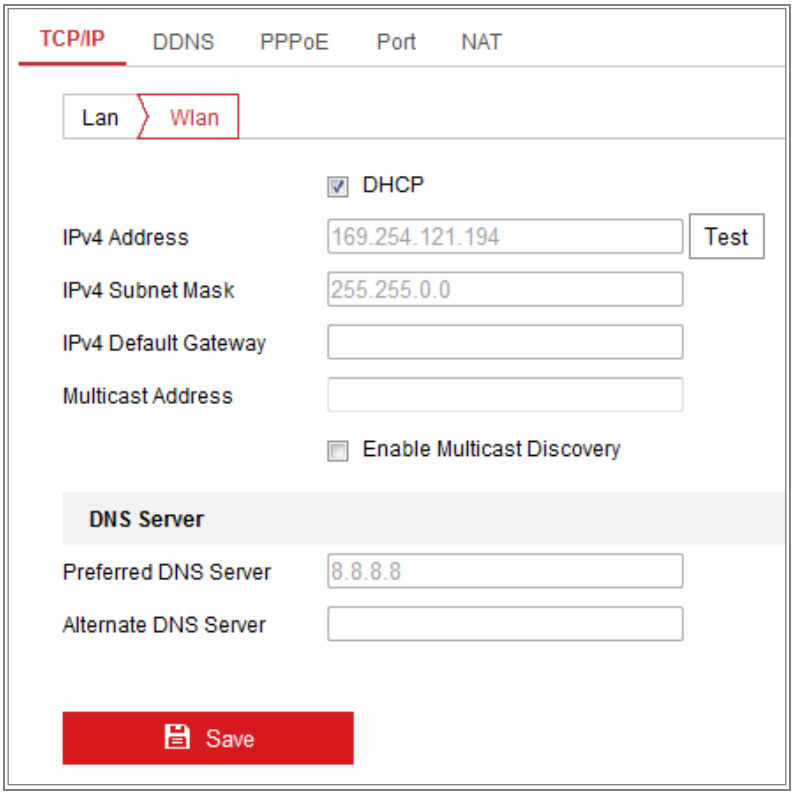


図 4-11 WLAN パラメータの設定

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すると DHCP を有効にできます。

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、ビデオの録画、PTZコントロール、ディスプレイ設定、OSD設定、ビデオ/オーディオ設定、VCA設定、プリセットの設定/呼び出し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:

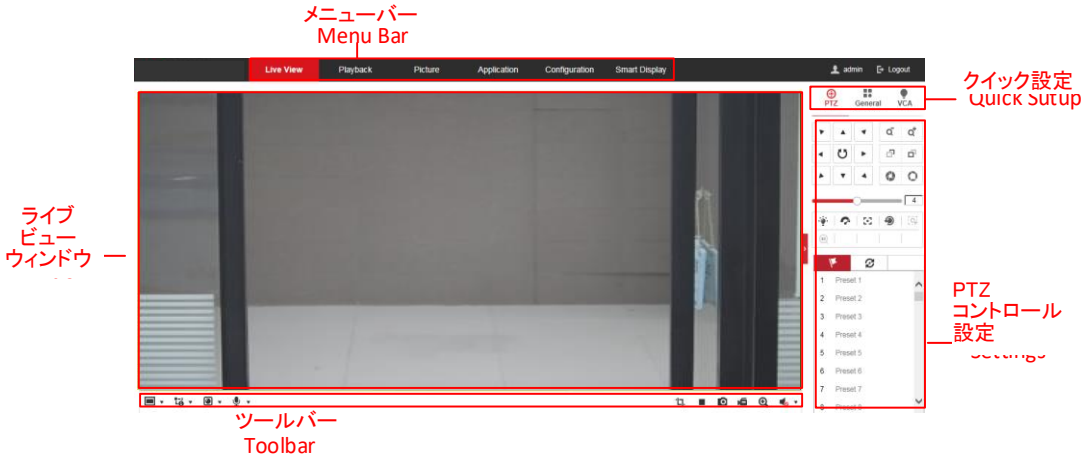


図 5-1 ライブビューページ

- **メニューバー**

各タブをクリックして、ライブビュー、プレイバック、ピクチャー、アプリケーション、コンフィギュレーション、スマートディスプレイの各ページを開きます。

- **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(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)も可能です。

IE （Internet Explorer）ユーザーの場合、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、IE ユーザーでない場合でも、ウェブコンポーネント、クイックタイム、VLC または MJPEG は、ウェブブラウザがサポートしている場合には選択が可能です。

お知らせ:

プラグインフリーのライブビューに対応しているカメラでは、Google Chrome 57 以降または Mozilla Firefox 52 以降を使用している場合、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/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 およびその上のバージョンへの変更を行います。

- **クイックセットアップ**

ライブビューページで、PTZ コントロール、画像、ビデオ/オーディオ設定および VCA 設定を素早くセットアップできます。

- **PTZ コントロール設定**

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）。PTZ カメラのプリセットや監視を設定/呼び出し/削除します。

5.2 ライブ操作

図 5-1 に示す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。

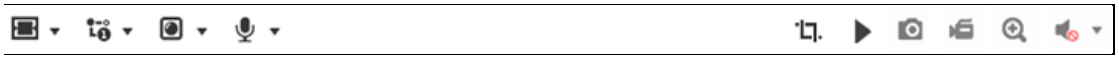


図 5-2 ライブビューツールバー

表 5-1 ツールバーの説明

アイコン	説明
▶/■	ライブビューを開始/停止します。
4:3	4:3 ウィンドウサイズ
16:9	16:9 ウィンドウサイズ
1×	元のウィドウサイズ
	自己適応型ウィンドウサイズ
	元の比率ウィンドウのサイズ
,,,など	さまざまなビデオストリームを含むライブビュー サポートされるビデオストリームはカメラモデルによって異なります。 10 ストリームをサポートするカメラモデルの場合は、「Video /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。
	画像を手動でキャプチャします。
/	録画を手動で開始/停止します。
/	オーディオをオンにして、音量/ミュートを調整します。
/	マイクのオン/オフを切り換えます。
/	デジタルズーム機能を開始/停止します。
/	ピクセルカウンタを開始/停止します。
	ボタンをクリックすると、カメラで撮影した画像が表示されます。 ***お知らせ:*** この機能は、顔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。

お知らせ: アイコンは、モデルによって異なります。

- **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でのみ、選択された領域のみをカウントします。

- **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換えたり、フルスクリーンから通常モードに戻ったりできます。

5.3 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キャプチャするか、  をクリックしてライブビューを録画します。キャプチャされた画像とクリップの保存パスは、「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は、ディスプレイ設定、OSD、およびビデオ/オーディオに素早くアクセスできます。

手順:

1. ライブビューウィンドウの右側  をクリックすると、クイックセットアップ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. ディスプレイ設定、OSD、およびビデオ/オーディオを設定します。

   PTZパラメータ設定については、「5.5PTZ コントロールの操作」を参照してください。

   ディスプレイ設定については、「9.1ディスプレイ設定」を参照してください。

   OSD設定については、「9.2 OSD設定」を参照してください。

   ビデオ/オーディオ設定については、「第8章 ビデオ/オーディオ設定」を参照してください。

   VCAリソースの設定については、「6.2.7VCA リソースの設定」を参照してください。

お知らせ: クイックセットアップ機能は、モデルによって異なります。

5.5 PTZ コントロールの操作

5.5.1 PTZ コントロールパネル

目的:

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が可能です。

お知らせ: PTZ 制御をするには、ネットワークに接続されたカメラが PTZ 機能をサポートしているか、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」を参照して、RS-485 設定ページの PTZ パラメータを正しく設定してください。

方向ボタンをクリックして、パン/チルトの動きを制御します。

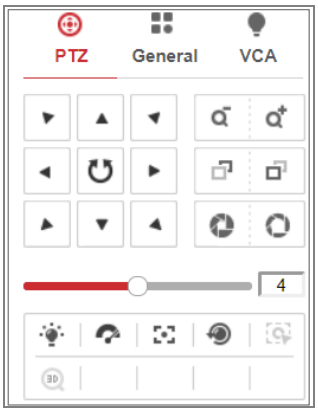


図 5-3 PTZ コントロールパネル

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を制御します。

お知らせ:

- コントロールパネルには、8 つの方向矢印(△、▽、◁、▷、▽、◁、△、◁)があります。矢印をクリックして、位置を調整します。
- レンズの動きのみをサポートするカメラでは、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
	拡大/縮小
	近/遠フォーカス
	アイリス+/−
4	PTZ 速度調整
	ライトオン/オフ
	ワイパーオン/オフ
	補助フォーカス
	レンズ初期化
	パン/チルト動作の速度の調整
	手動トラッキングの開始
	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。

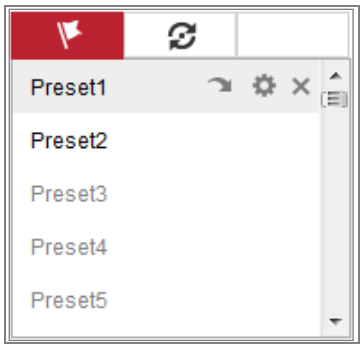


図 5-4 プリセットの設定

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。
   - カメラを左右にパンします。
   - 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。
3. 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、プリセットが削除されます。

- **プリセットの呼び出し:**

指定したプリセットを手動またはイベント発生時に自動的に呼び出すことができます。

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、をクリックしてプリセットを呼び出します。

また、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。

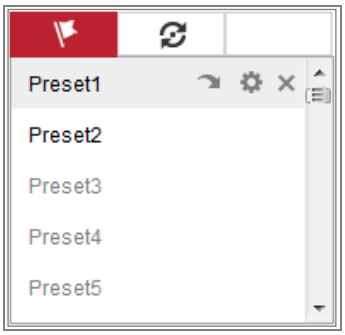


図 5-5 プリセットの呼び出し

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. をクリックして、パトロール設定画面を開きます。
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. 上記の手順を繰り返し、他のプリセットを追加します。

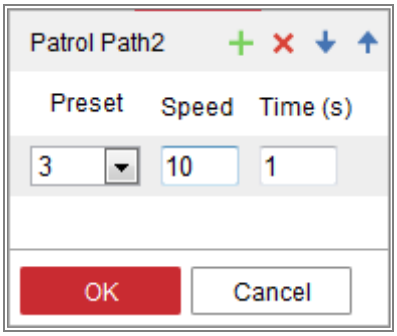


図 5-6 パトロールパスの追加

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。

5.6 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。

オペレーティングシステム	Web ブラウザ	操作
Windows	Internet Explorer 8+	ポップアップ画面に従って、プラグインのインストールを完了します。
	● Google Chrome 31+ ● Mozilla Firefox 30+	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。
マック OS	● Google Chrome 57+ ● Mozilla Firefox 52+ ● Apple Safari 16+	● プラグインのインストールは必要ありません。 ● 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」）。 特定の機能の表示や操作が制限されています。例えば「Playback」や「Picture」は使用できません。機能制限の詳細については、実際のデバイス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。

第6章　ネットワークカメラの設定

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調整します。録画ファイルとキャプチャ画像は、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。

お知らせ: サポートされる機能は、モデルによって異なります。

手順:

1. 「Configuration」 > 「Local」を選択します。
2. 以下を設定します。

- **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のパフォーマンスの設定**
  - **「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」: ライブビューのパフォーマンスを「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、顔検出または侵入検出が報告されたとき、色付きマークを表示するかどうかを選択・設定します。例えば、ルールが有効で、顔検出も有効になっている場合、顔が検出されると、ライブビューで緑色の長方形が表示されます。**
- **「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。例えば、キュー管理の ID と待機時間、人数計算などです。

  お知らせ:

  Display POS Information 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。**

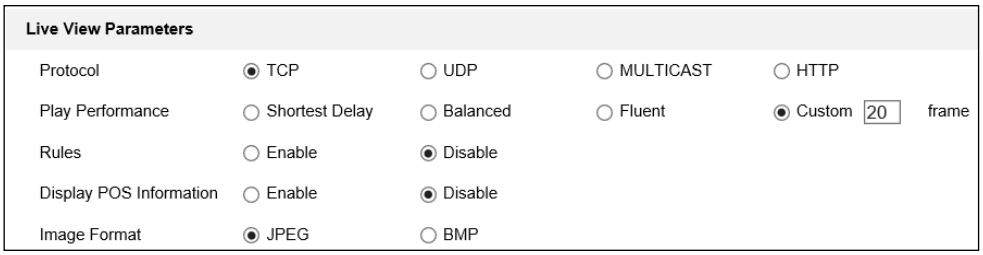


図 6-1 ライブビューパラメーター

- **「Record File Settings」: 録画された録画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。設定すると、最大録画ファイルサイズは選択した値になります。**
  - **録画ファイルの保存先: 手動で録画した録画ファイルの保存先を設定します。**
  - **ダウンロードファイルの保存先: 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 record files to」: キャプチャしたピクチャーとクリップしたビデオファイルの保存パスを設定します。Web ブラウザで撮影する画像に有効です。**
  - **ライブビューでのスナップショットの保存先: 手動でキャプチャ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写真の保存先を設定します。**
- **「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。

お知らせ: サポートされる機能はモデルによって異なります。

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、エンコードバージョン、チャンネル数、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。保守や改良の参考情報で、このメニューで情報を変更することはできません。

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。

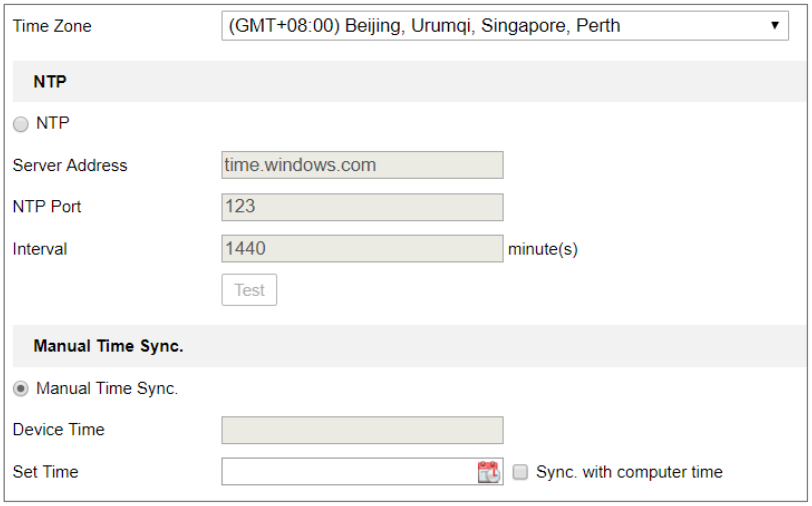


図 6-2 **時間設定**

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 設定を行います。
   (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) 以下の設定を行います。
   「Server Address」: 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。

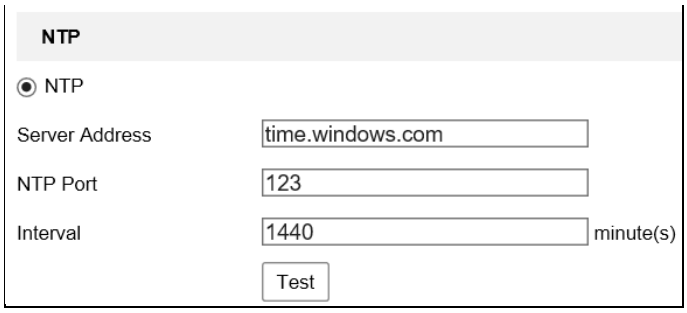


図 6-3 NTP サーバーによる時間同期

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。カメラをカスタマイズしたネットワークに設定すると、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) 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」をオンにできます。デバイスの時刻をローカル PC の時刻と同期させるためのコンピュータ時刻項目が付いています。

図 6-4 手動同期

- 「Save」をクリックし、設定を保存します。

6.2.3 RS-232 設定

RS-232 ポートは 2 つの方法で使用できます。

- 「Console」: コンピュータをシリアルポート経由で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。

- 「Transparent Channel」: 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」 > 「RS-232」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。

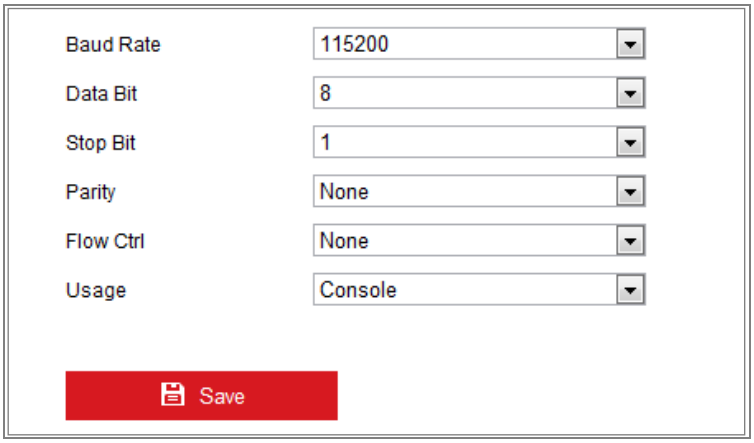


図 6-5 RS-232 設定

お知らせ: RS-232 ポートでカメラを接続する場合、RS-232 のパラメータは、ここで設定したパラメータと同じに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。

6.2.4 RS-485 設定

目的:

RS-485 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」 > 「RS-485」を選択します。

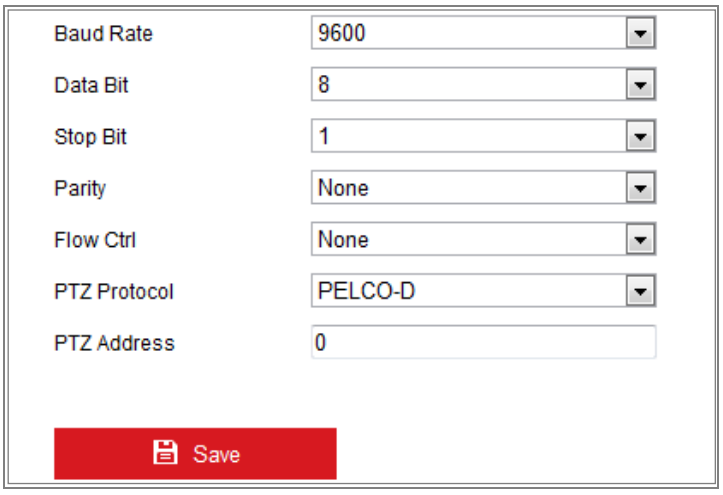


図 6-6 RS-485 設定

2. RS-485 パラメータを設定し、「Save」をクリックし、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 アドレスパラメータは、PTZ カメラ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:

夏時間（DST） は、夏時間の期間に 1 時間早めに設定し夏時間をより有効に活用することができます。

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。

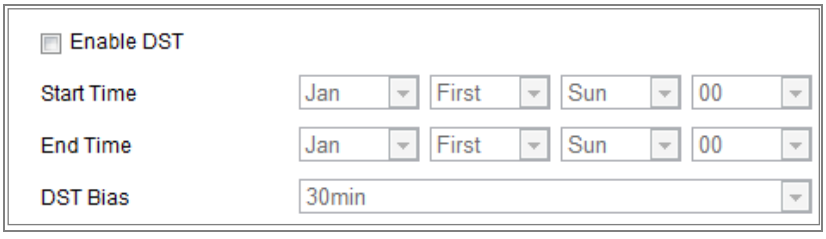


図 6-7 DST 設定

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。

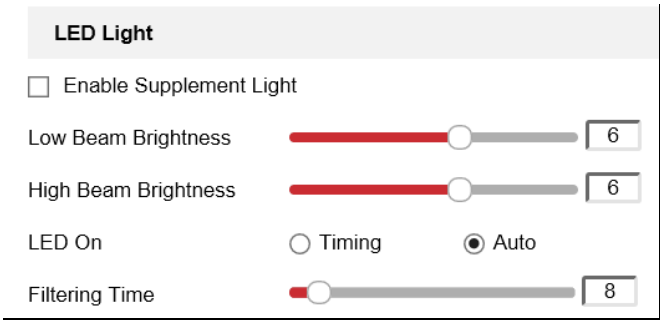


図 6-8 外部デバイス設定

2. 「Enable Supplement Light」のチェックボックスをオンにすると、LED ライトが有効になります。
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。タイミングとオートを選択できます。
   - **「Timing」: 設定したスケジュールで LED が点灯します。「Start Time」と「End Time」を設定する必要があります。**

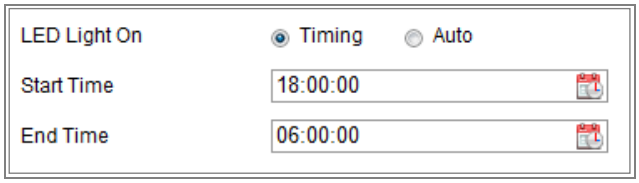


図 6-9 スケジュール設定

   - **「Auto」: 環境照明に応じて LED が点灯します。**
5. スライダーを動かして、フィルタリング時間を調整します。
6. 「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あります。必要な機能に多くのリソースを割り当てることができます。

手順:

1. 「Configuration」>「System」>「System Settings」>「VCA Resource」を選択します。
2. 希望する 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条件となっており、1 つの組み合わせを有効にすると、他の組み合わせは非表示になります。
- 特定のモデルのみがこの機能をサポートしています。

6.2.8 メタデータ設定

目的:

メタデータは、アルゴリズム処理の前にカメラが収集する元データです。侵入検知、回線横断検知、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、顔キャプチャのメタデータをアップロードすることができます。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をオンにし、メタデータ関数を有効にします。

3. 「Enable Stream Rule」チェックボックスをオンにし、ライブイメージにストリームルールを表示させます。ライブビュー上で「Sub-stream」をチェックし選択しておく必要があります。
4. 「Overlay Rule Frame and Target Frame on Background Picture」チェックボックスをオンにし、機能を有効にします。

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。

6.2.9 オープンソース・ソフトウェア・ライセンス

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は、必要に応じて確認できます。「Configuration」 > 「System」 > 「About」を選択してください。

6.3 メンテナンス

お知らせ: サポートされる機能は、モデルによって異なります。

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ができます。

「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設定に戻します。**

  お知らせ:

  - お買い上げ時の設定に戻したあと、IP アドレスもお買い上げ時の IP アドレスに戻りますので、ご注意ください。

- Wi-Fi、ワイヤレスダイヤル、または WLAN 機能に対応しているカメラでは、上記機能の関連設定はお買い上げ時の設定に戻りません。
- デバイスを工場出荷時のデフォルトに復元すると、ビデオ規格は予約済みになります。

- 「Information Export」

  「Device Parameters」: 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、暗号化パスワードの作成も必要です。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になります。

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

  「Import Config. File」

  設定ファイルは、カメラの一括設定に使用されます。

  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: 設定ファイルのインポート後、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:

  1. 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。

     「Firmware」: アップグレードファイルの正確なパスを見つけます。

     「Firmware Directory」: 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: アップグレードプロセスには 1 ～10 分かかります。この処理中はカメラの電源を切らないでください。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:

カメラの動作、アラーム、例外および情報をログファイルに保存することができます。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:

カメラの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。

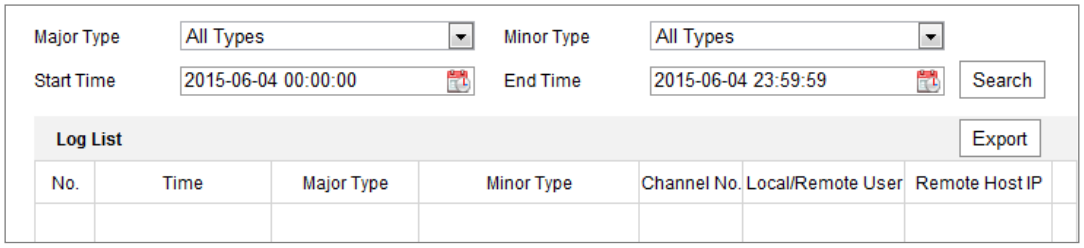


図 6-10 ログ検索画面

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。

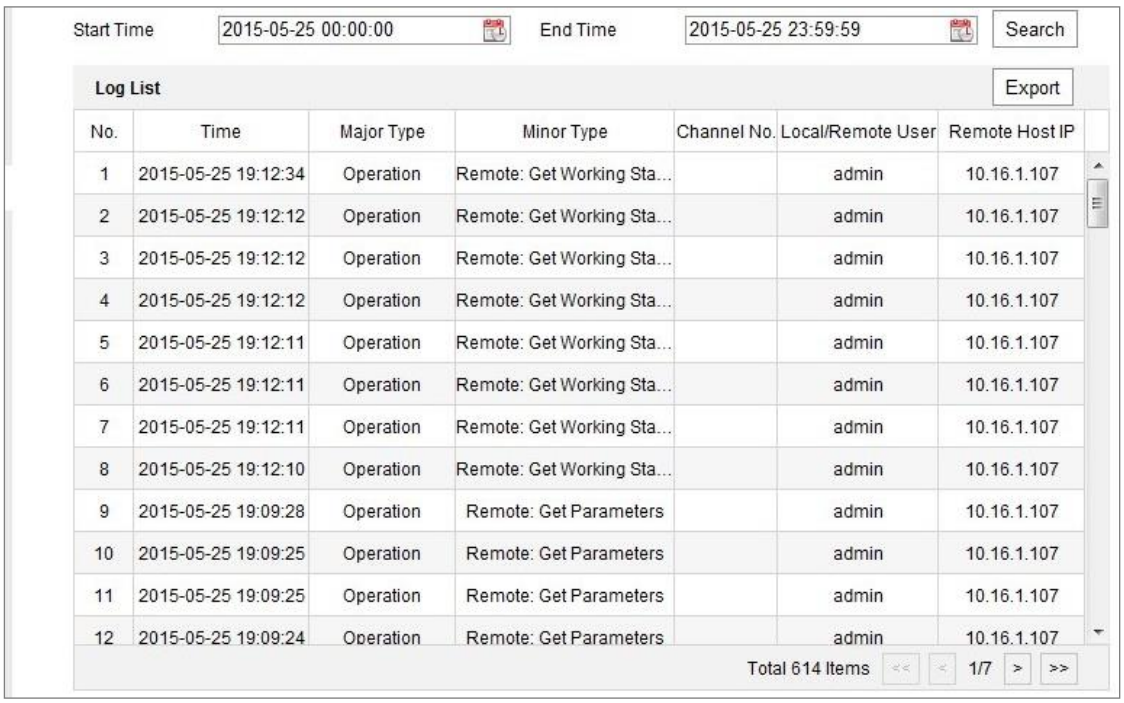


図 6-11 ログ検索

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:

システムサービスの設定は、カメラがサポートするハードウェアサービスを参照してください。カメラによって、サポートする機能が異なります。IR Light、ABF（Auto Back Focus）、Auto Defog または Status LED をサポートするカメラでは、必要に応じてサービスを有効または無効にすることができます。

「Enable IR Light」: チェックボックスをオンにして、機能を有効にします。

「ABF」: ABF 機能が有効な場合、PTZ コントロールパネルの 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無効になっています。3 番目のストリームを有効にする場合は設定をオンにします。

「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」: オンにすると、モーション検知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、セキュリティーイベントの不正侵入やトラブルシューティングを検出することができます。セキュリティ監査ログはフラッシュデバイスに保存できます。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、ログサーバーにログを保存することもできます。「Advanced Settings」でサーバー設定を行います。

- **ログの検索**

手順:

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

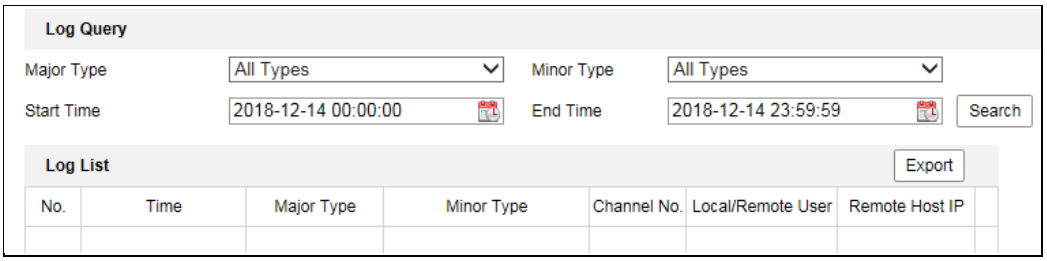


図 6-12 セキュリティ監査ログ検索画面

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。

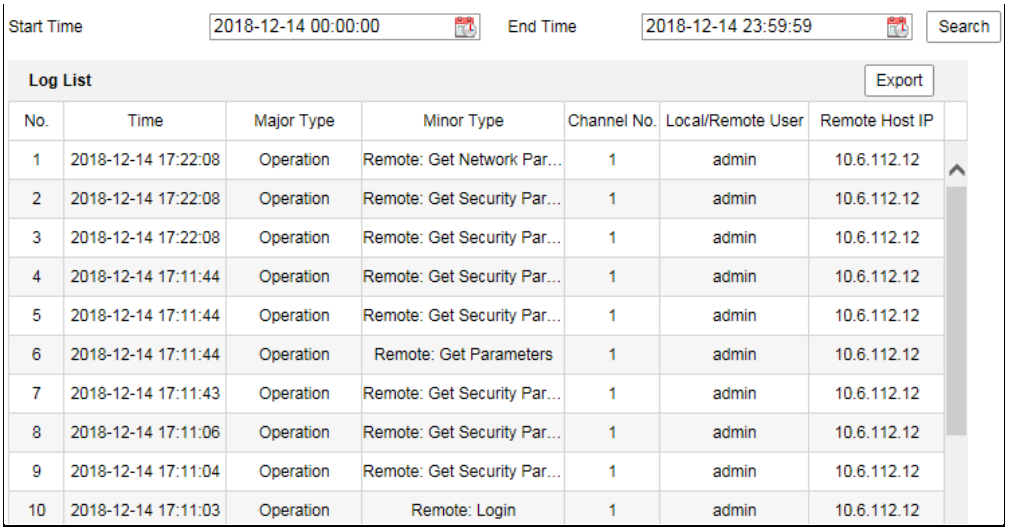


図 6-13 ログ検索

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。

- **ログサーバーの設定**

手順:

1. 「Enable Log Upload Server」をオンにします。
2. 「Enable Encrypted Transmission」をオンにします。証明書管理で証明書がインストールされていることを確認してください。

3. ログサーバーIP とログサーバーポートを入力します。
4. 「Test」をクリックして設定をテストします。
5. 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) 署名付き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。

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。

6.4 セキュリティ設定

セキュリティ設定画面から、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。

お知らせ: サポートされる機能は、モデルによって異なります。

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。

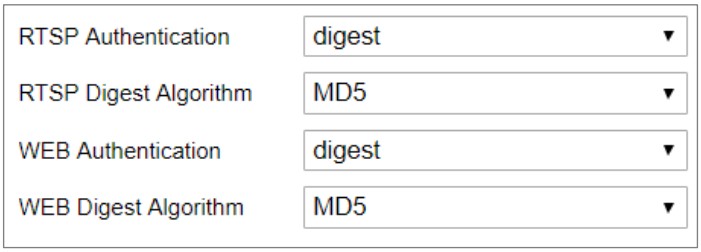


図 6-14 認証

2. RTSP 認証、WEB 認証、RTSP ダイジェストアルゴリズム、WEB ダイジェストアルゴリズムの認証方式を設定します。

   - RTSP 認証

   ダイジェストとダイジェスト/ベーシックがサポートされ、RTSP 要求がデバイスに送信されるときに認証情報が必要になります。ダイジェスト/ベーシックを選択した場合、デバイスがダイジェストまたは基本認証をサポートしていることを意味します。ダイジェストを選択した場合、デバイスはダイジェスト認証のみをサポートしています。

   - RTSP ダイジェストアルゴリズム

   MD5、RTSP 認証の SHA256 および MD5/SHA256 暗号化アルゴリズム。MD5 以外のダイジェストアルゴリズムを有効にすると、互換性があるため、サードパーティプラットフォームがデバイスにログインできなかったり、ライブビューを有効にできなかったりする場合があります。高強度の暗号化アルゴリズムを推奨します。

   - WEB 認証

   ダイジェストとダイジェスト/ベーシックがサポートされ、WEB 要求がデバイスに送信されるときに認証情報が必要になります。ダイジェスト/ベーシックを選択した場合、デバイスがダイジェストまたは基本認証をサポートしていることを意味します。ダイジェストを選択した場合、デバイスはダイジェスト認証のみをサポートしています。

   - WEB ダイジェストアルゴリズム

   MD5、WEB 認証の SHA256 および MD5/SHA256 暗号化アルゴリズム。MD5 以外のダイジェストアルゴリズムを有効にすると、互換性があるため、サードパーティプラットフォームがデバイスにログインできなかったり、ライブビューを有効にできなかったりする場合があります。高強度の暗号化アルゴリズムを推奨します。

   お知らせ:

   認証要件を表示するには、プロトコルの特定の内容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。

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

2. 「Enable IP Address Filter」をオンにします。
3. ドロップダウンリストで「IP Address Filter Type」を選択し、「Forbidden」および「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 または IP セグメントを確認します。

     (3) IP アドレスまたは IP セグメントを入力します。

図 6-16 IP の追加

     (4) 「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

目的:

リモートログインを有効にし、データ通信のセキュリティを向上させ、カメラはユーザーエクスペリエンスを向上させるために、セキュリティサービスを提供します。

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。

手順:

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

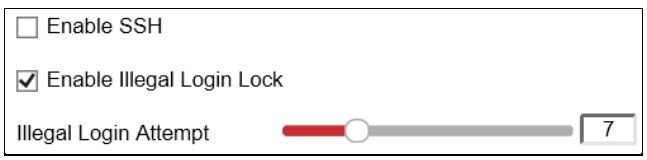


図 6-18 セキュリティサービス

2. 必要に応じて SSH を有効にするには、「Enable SSH」のチェックボックスをオンにします。
3. 「Enable Illegal Login Lock」の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として設定できます。

- 「Security Reinforce」

  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。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。

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。

6.4.5 証明書管理

目的:

サーバー/クライアント証明書と CA 証明書の管理を行い、証明書が期限切れや異常になった場合にアラームを送信します。

- **サーバー/クライアント証明書**
  - **自己署名証明書の作成**

手順:

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

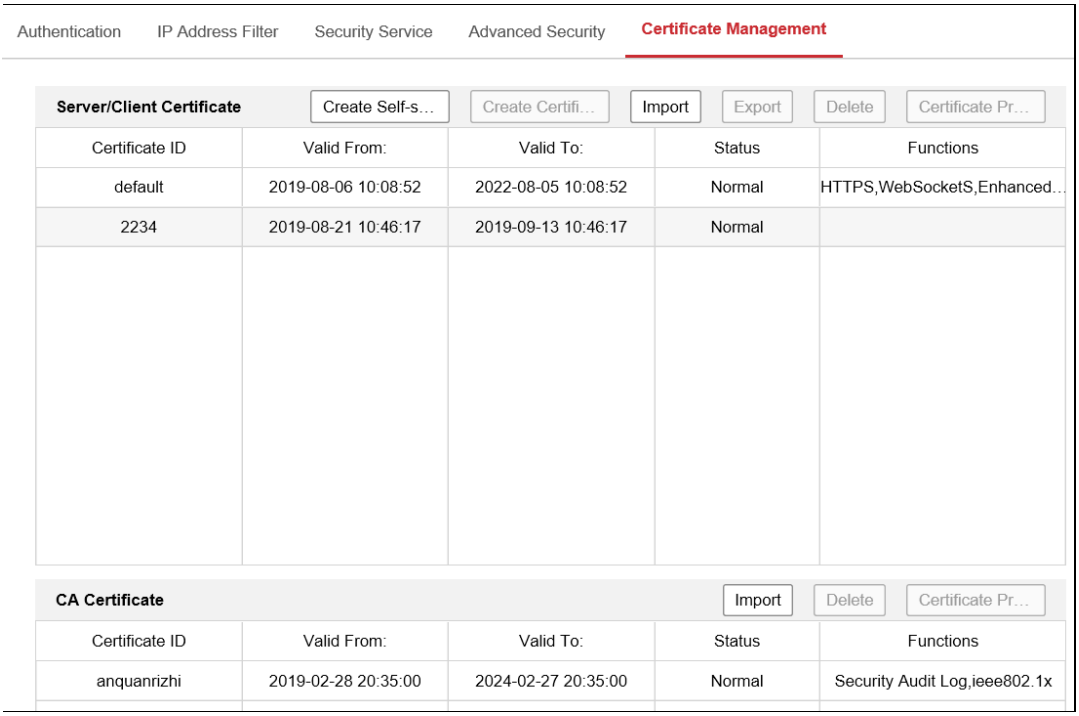


図 6-19「証明書管理」

2. 「Create Self-signed Certificate」をクリックします。
3. 証明書 ID、国、ホスト名/IP、有効性などの情報を入力します。証明書 ID は数字または文字で、64 文字以内にする必要があります。
4. 「OK」をクリックします。
5. 証明書をエクスポートするには、「Export」をクリックします。証明書を削除して証明書を再作成するには、「Delete」をクリックします。証明書の詳細を表示するには、「Certificate Property」をクリックします。

- **証明書要求の作成**

手順:

1. 自己署名証明書を選択します。
2. 「Create Certificate Request」をクリックします。
3. 関連情報を入力します。
4. 「OK」をクリックします。

- **証明書のインポート**

手順:

1. 「Import」をクリックします。
2. 「Create Certificate Request」をクリックします。
3. 「Certificate ID」を入力し、「Browser」をクリックして目的のサーバー/クライアント証明書を選択し、目的のインポート方法を選択して、必要な情報を入力します。
4. 「OK」をクリックします。
5. 証明書をエクスポートするには、「Export」をクリックします。証明書を削除して証明書を再作成するには、「Delete」をクリックします。証明書の詳細を表示するには、「Certificate Property」をクリックします。

お知らせ:

- 最大 16 個の証明書が許可されます。
- 特定の機能が証明書を使用している場合は、削除できません。
- 証明書を使用している関数は、「Functions」列で表示できます。
- 既存の証明書と同じ ID を持つ証明書を作成し、既存の証明書と同じ内容を持つ証明書をインポートすることはできません。

- **CA 証明書**

手順:

1. 「Import」をクリックします。
2. 「Certificate ID」を入力し、「Browser」をクリックして目的のサーバー/クライア
   証明書をエクスポートするには、「Export」をクリックします。証明書
3. 「OK」をクリックします。

お知らせ: 最大 16 個の証明書を使用できます。

- **証明書失効アラームの有効化**

手順:

1. 「Enable Certificate Expiration Alarm」をオンにします。有効にすると、証明書の有効期限が間もなく切れるか、有効期限が切れているか、または異常であることを示す電子メールまたはカメラリンクが監視センターに送信されます。
2. 「Remind Me Before Expiration （day）」、「Alarm Frequency （day）」、「Detection Time （hour）」を設定します。

   お知らせ:

   - 有効期限が切れる前のリマインダー日を 1 日に設定すると、カメラは有効期限の前日を通知します。1～30 日間使用できます。デフォルトのリマインダー日は 7 日間です。
   - 有効期限が切れる前の通知日を 1 日に設定し、検出時間を 10:00 に設定し、証明書の有効期限が翌日の 9:00 に切れた場合、カメラは最初の日の 10:00 に通知します。
3. 「Save」をクリックし、設定を保存します。

6.5 ユーザー管理

お知らせ: サポートされる機能は、モデルによって異なります。

6.5.1 ユーザー管理

- **管理者として**

管理者は、ユーザーアカウントを追加・削除・変更したり、さまざまな権限を付与したりできます。ユーザーアカウントと権限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・変更には、管理者パスワードが必要です。

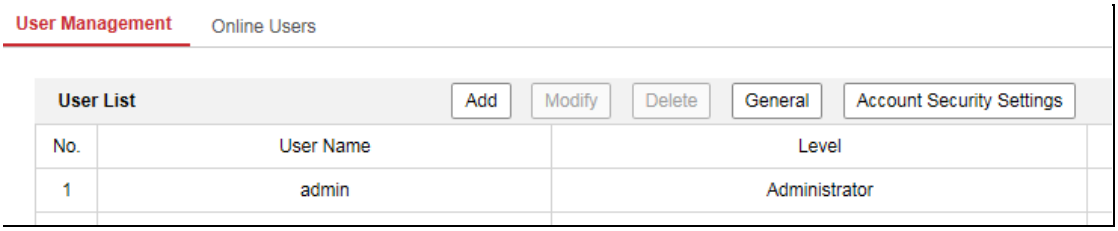


図 6-20 ユーザ管理画面

- **ユーザーの追加**

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

管理者は削除できず、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。
2. 「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の設定・解除ができます。
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. 左クリックからリストのユーザーを選択し、「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. 権限の設定・解除ができます。
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して、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。変更には古いパスワードが必要です。

6.5.2 セキュリティ問題

目的:

セキュリティに関する質問は、管理者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:

カメラ起動時のセキュリティ質問を設定できます。また、ユーザー管理で機能を設定することもできます。

セキュリティ質問の設定は、カメラを復元してもクリアされません（デフォルトには戻りません）。

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 とカメラは、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:

デバイスにアクセスしている現在のユーザーを表示できます。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」をクリックするとリストは更新できます。

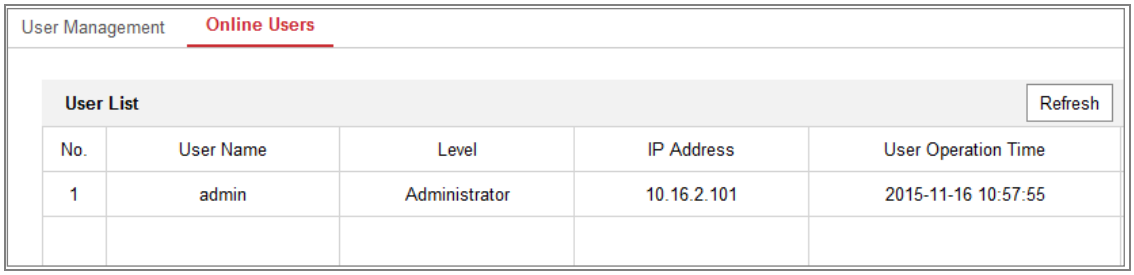


図 6-21 オンラインユーザーの表示

第7章　ネットワーク設定

目的:

この章では、基本設定と詳細設定の方法を説明しています。

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。

お知らせ: サポートされる機能は、モデルによって異なります。

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を正しく設定する必要があります。カメラはIPv4とIPv6の両方をサポートしていますが、両方のバージョンは同時に設定できないため、いずれか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。

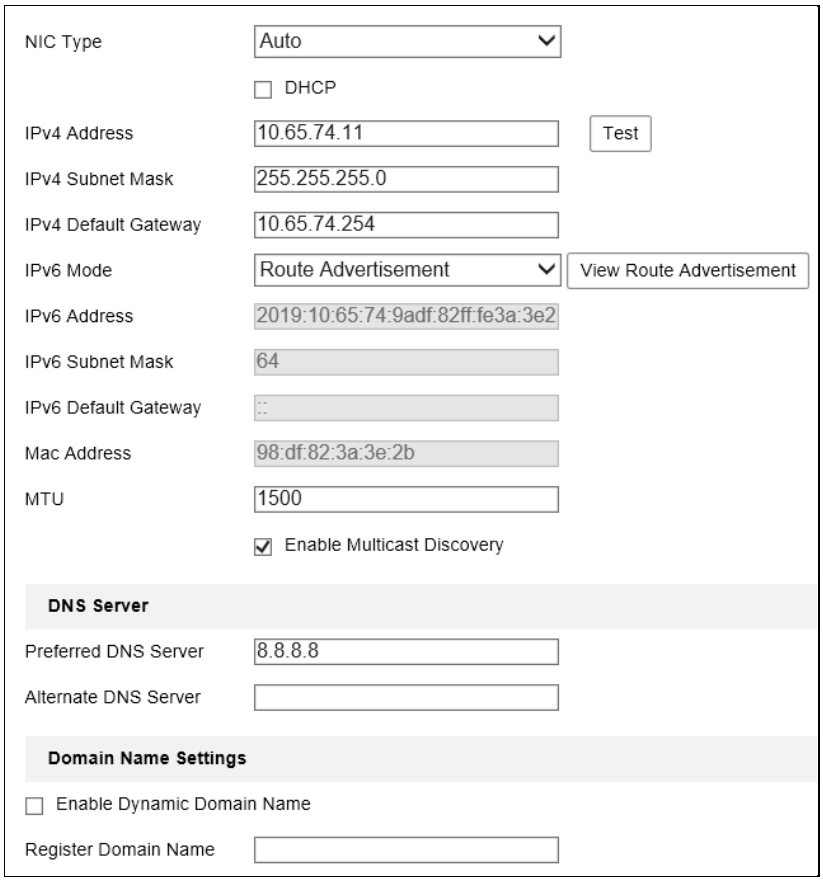


図 7-1 TCP/IP の設定

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行います。
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 serverを設定します。「Preferred DNS Server」と「Alternate DNS Server」を入力します。
5. 「Enable Dynamic Domain Name」チェックボックスをオンにし、「Register Domain Name」を入力します。
6. 「Save」をクリックし、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。
- マルチキャストは、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場合は、ルータ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:

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動的 DNS（DDNS）を使用できます。

準備:

カメラのDDNS 設定を行う前に、DDNS サーバーへの登録が必要です。

手順:

1. 「Configuration」 > 「Network」 > 「Basic Settings」 > 「DDNS」を選択します。
2. 「Enable DDNS」チェックボックスをオンにし、機能を有効にします。
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のサーバーアドレス（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。

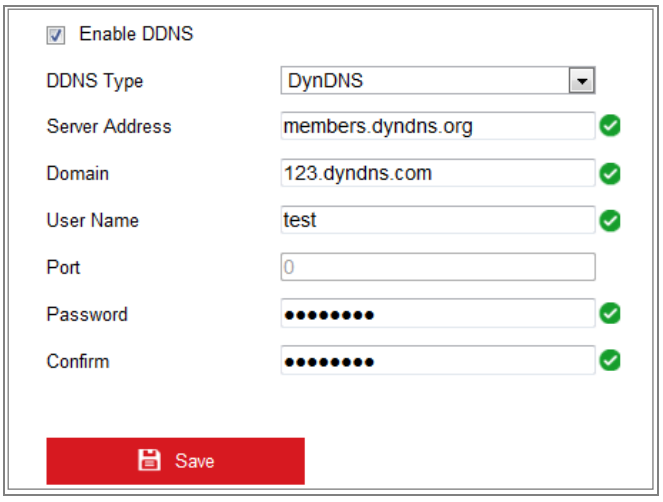


図 7-2 DynDNS 設定

- NO-IP:

手順:

(1)「DDNSタイプ」の「NO-IP」を選択します。

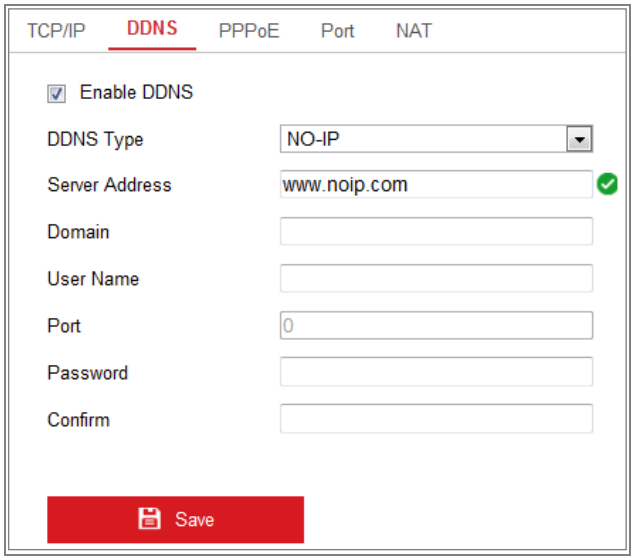


図 7-3 NO-IP DNS 設定

(2)サーバーアドレスをwww.noip.com(Link)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、ドメイン名でカメラを表示できます。

7.1.3 PPPoE 設定

手順:

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

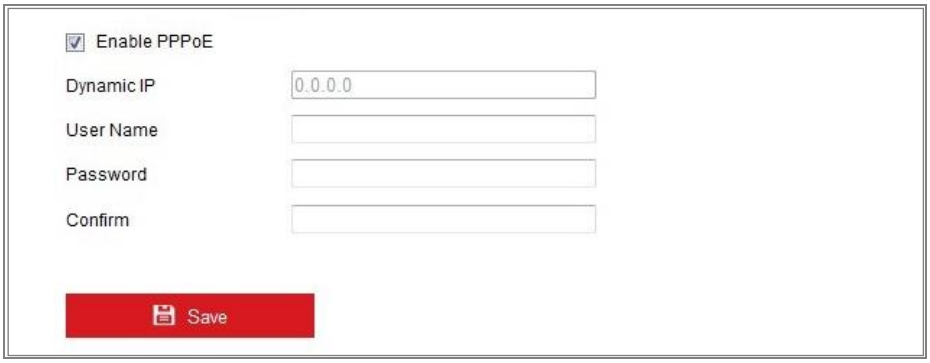


図 7-4 PPPoE Settings

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

3. PPPoEにアクセスするためのユーザー名、パスワードおよび確認用パスワードを入力します。

お知らせ: ユーザー名とパスワードは、ISPによって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、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。

7.1.4 ポート設定

目的:

HTTP ポート、RTSP ポート、HTTPS ポートなど、カメラのポート番号を設定します。

手順:

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

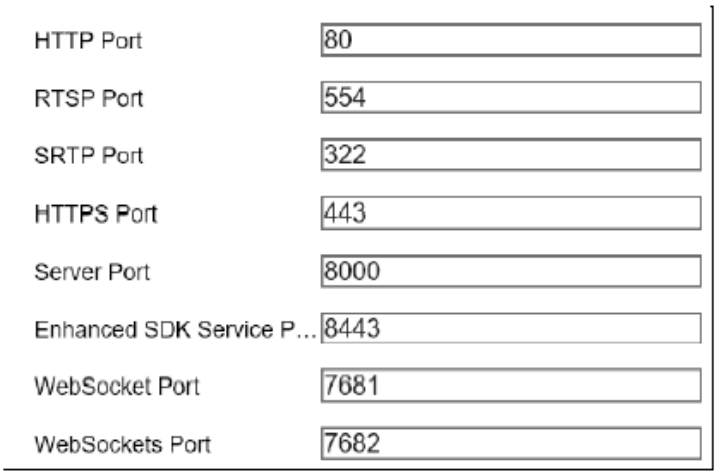


図 7-5 ポート設定

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、1 から 65535 までの任意のポート番号に変更できます。

「SRTP Port」: デフォルトのポート番号は 322 です。

「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。

「Enhanced SDK Service Port」: デフォルトのサーバー番号は 8443 です。これは、クライアントがデバイスを追加するポートを参照します。安全なアクセスを確保するには、証明書の検証が必要です。

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、ログイン画面で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。ポート番号は、2～65534 の範囲で変更できます。

「WebSockets Port」: デフォルトのサーバーポート番号は 7682 です。ポート番号は、2～65534 の範囲で変更できます。

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。詳細については、「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。

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、デバイスをシームレスに接続し、ホームおよび企業環境でのネットワークの構築を簡素化できます。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。

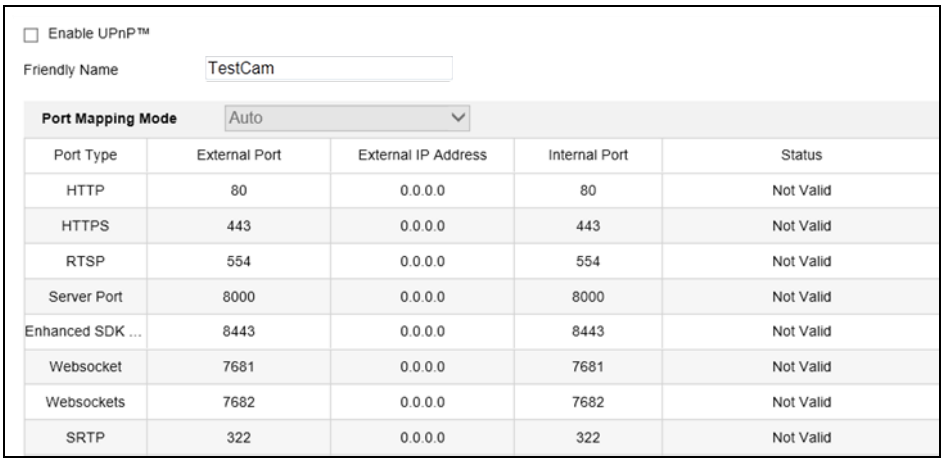


図 7-6 UPnP 設定

手順:

1. 「Configuration」＞「Network」＞「Basic Settings」＞「NAT」を選択します。
2. チェックボックスをチェックすると、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. カメラのわかりやすい名前を選択するか、デフォルトの名前を使用します。
4. ポートマッピングモードを選択します。「Manual」または、「Auto」を選択できます。

   お知らせ:

   自動を選択した場合は、ルータで 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、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。

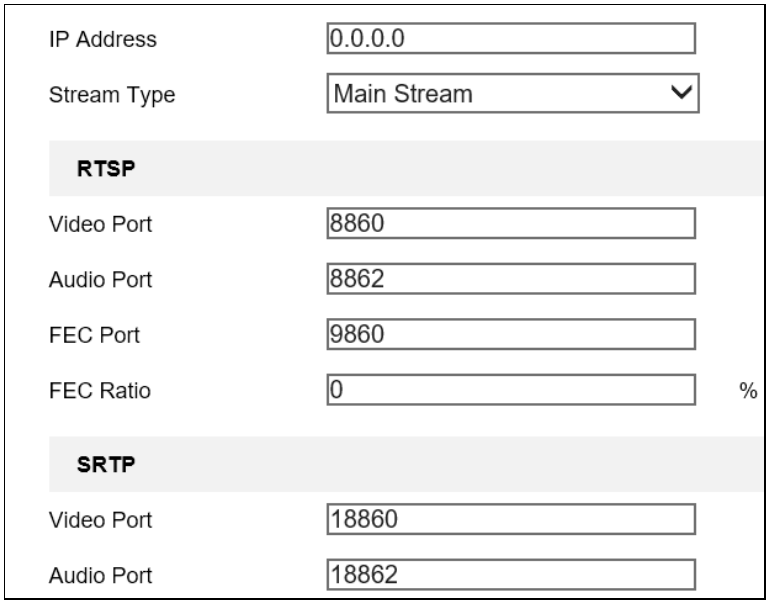


図 7-7 マルチキャストの設定

手順:

1. 「Configuration」 > 「Network」 > 「Basic Settings」 > 「Multicast」を選択します。
2. 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。

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。

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することができます。

お知らせ: サポートされる機能は、モデルによって異なります。

7.2.1 SNMP 設定

目的:

SNMP機能を設定すると、カメラの状態やパラメータ、アラームに関する情報を取得したり、ネットワーク接続時にカメラをリモートで管理したりできます。

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。

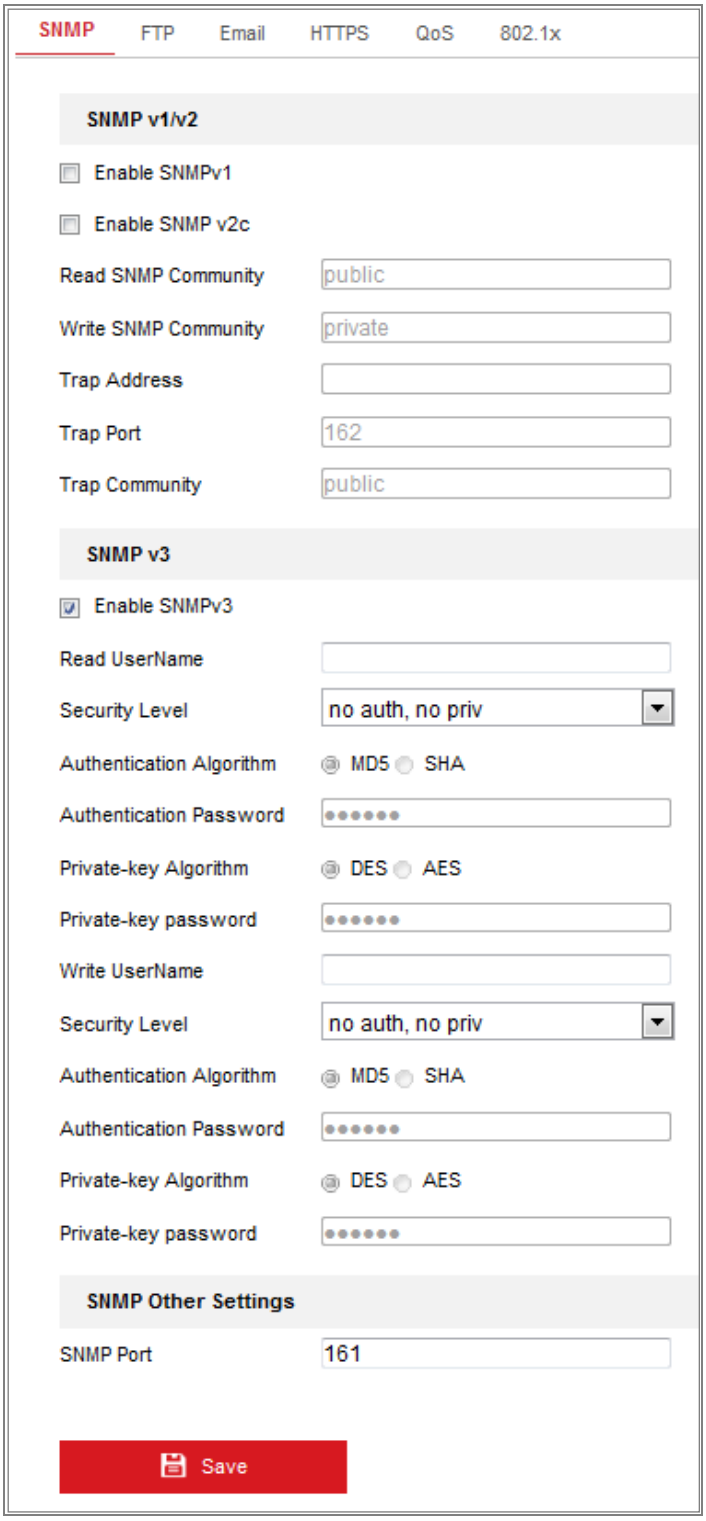


図 7-8 SNMP 設定

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、設定を保存します。

お知らせ: 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 7-9FTP 設定

2. 「FTPProtocol」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 設定を行います。また、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 Interval」: 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。

「Anonymous Access to the FTP Server」(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 サーバー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. 「Enable Automatic Network Replenishment」チェックボックスをオンにします。「Linkage Method」で「Upload to FTP/Memory Card/NAS」と「Enable Automatic Network Replenishment」を同時に有効にする必要があります。
8. 「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:

1. 「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 サーバーを設定します。

   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」: 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、電子メールサーバーがプロトコルをサポートし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「Enable STARTTLS」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」: 通知されるユーザーの名前

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

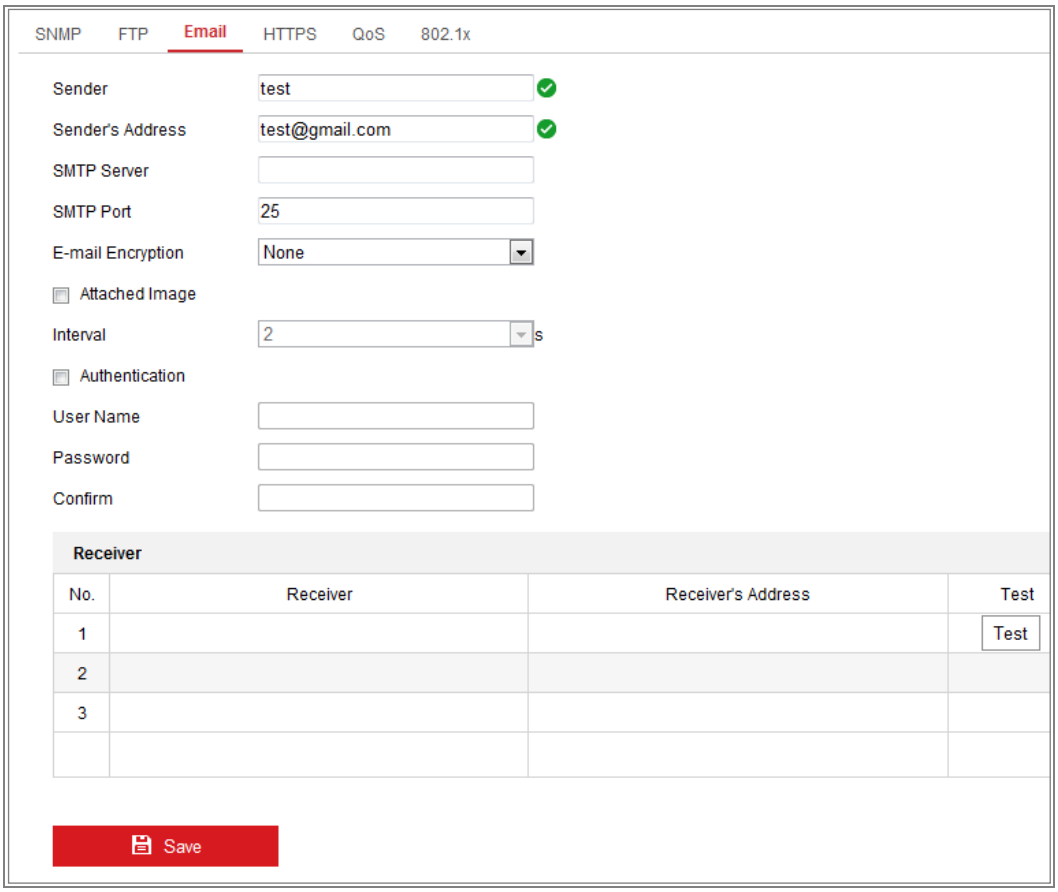


図 7-10 メール設定

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「ISUP」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に対応しているカメラは 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後、ダイヤル用のデフォルト設定が採用されます。
   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 から選択できます。「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、電波強度などの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」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」チェックボックスをオンにし、SM 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」と返信します。

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。

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。

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:

- プラグインフリーのライブビューに対応しているカメラでは、HTTPS を使用してカメラにアクセスするときに、ライブビュー用の WebSocket 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、カメラは署名されていない証明書を自動的に作成します。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. 「Server Certificate」を選択します。
5. 「Save」をクリックし、設定を保存します。

   お知らせ: 正常に機能しない場合は、証明書管理で選択した証明書に異常がないか確認してください。

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。

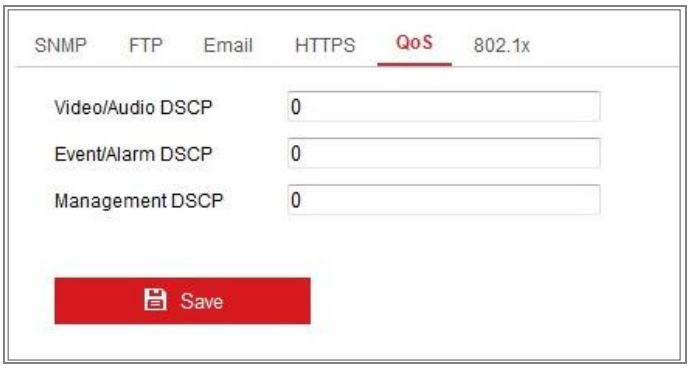


図 7-12 QoS 設定

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

   DSCP の有効値の範囲は 0 ～63 です。DSCP 値が大きいほど、優先順位は高くなります。

   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。

7.2.8 802.1X の設定

目的:

本機は IEEE 802.1X 規格をサポートしています。この機能を有効にすると、カメラのデータが保護されます。IEEE 802.1X によって保護されたネットワークにカメラを接続する場合は、ユーザー認証が必要です。

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。

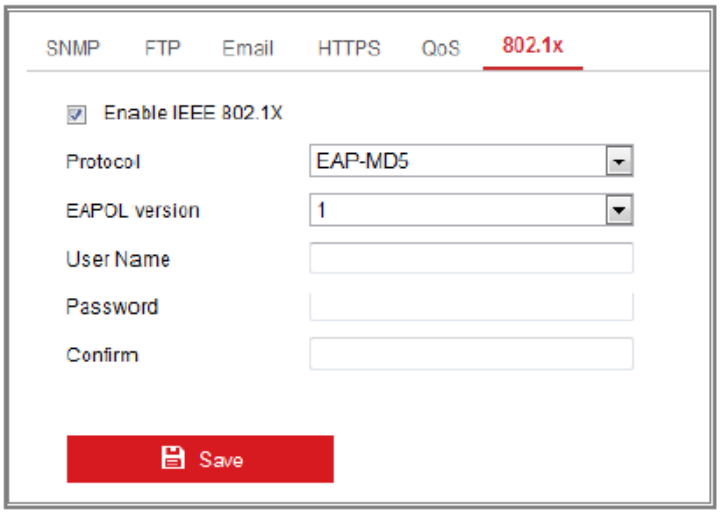


図 7-13 802.1X 設定

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」を選択します。EAP-LEAP、EAP-TLS、EAP-MD5 が選択可能です。

4. 「EAPOL version」を選択します。

   お知らせ: EAPOL version は、ルータ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。

5. 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。
6. 「Protocol」を「EAP-TLS」に設定した場合は、「Client Certificate」と「CA Certificate」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:

   - 設定を有効にするには、再起動が必要です。
   - 正常に機能しない場合は、証明書管理で選択した証明書に異常がないか確認してください。

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、ONVIF ユーザーを設定します。設定ルールの詳細については、ONVIF の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。
  2. 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。
  3. 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:

- セキュリティ対策のため、未使用の機能はオフのままにしておいてください。
- 特定のモデルのみがこの機能をサポートしています。

WebSocket と WebSocket プロトコル

Google Chrome 57 以降または Mozilla Firefox 52 以降を使用してカメラにアクセスする場合は、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、静止画撮影、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、サーバー証明書を選択します。

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 プロトコルが使用されます。

「Enhanced SDK Service」: SDK over TLS プロトコルが使用されます。拡張 SDK サービスを有効にする場合は、サーバー証明書を選択する必要があります。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。

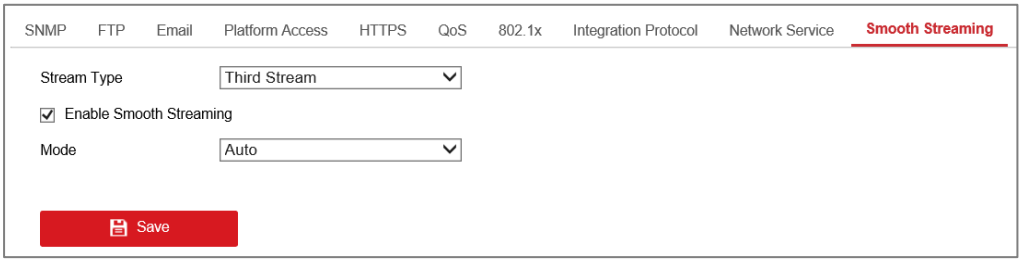


図 7-14 スムーズストリーミング設定

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。

5. 「**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。

6. 「Save」をクリックし、設定を保存します。

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。

7.2.13 HTTP リスニングの設定

目的:

カメラは、HTTP または HTTPS プロトコルを使用して、宛先 IP またはホスト名にアラーム情報を送信することができます。ネットワークが切断されておらず、ネットワーク接続が正常であれば、データを宛先 IP またはホスト名にアップロードできます。

準備:

宛先 IP またはホスト名は、アラーム情報を受信するための HTTP または HTTPS プロトコルをサポートしている必要があります。

手順:

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

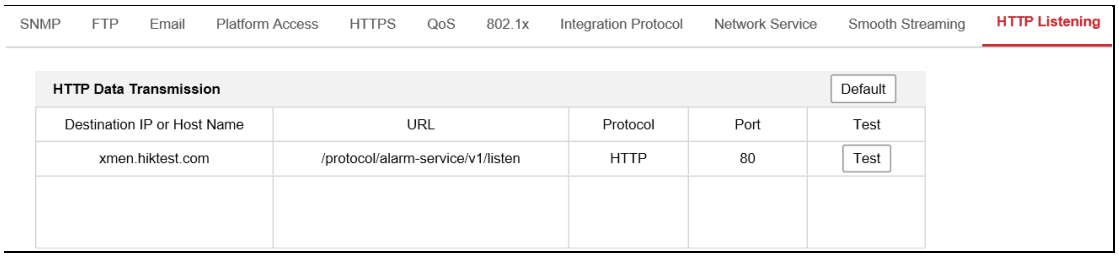


図 7-15 HTTP リスニング

2. 目的の宛先 IP またはホスト名、URL、およびポートを入力します。
3. 「Protocol」を選択します。HTTP と HTTPS が選択できます。
4. 「Test」をクリックして、入力した IP アドレスまたはホスト名が有効かどうかをテストできます。
5. 「Default」をクリックして、宛先 IP またはホスト名をリセットすることもできます。

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。

7.2.14 SRTP 設定

手順:

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

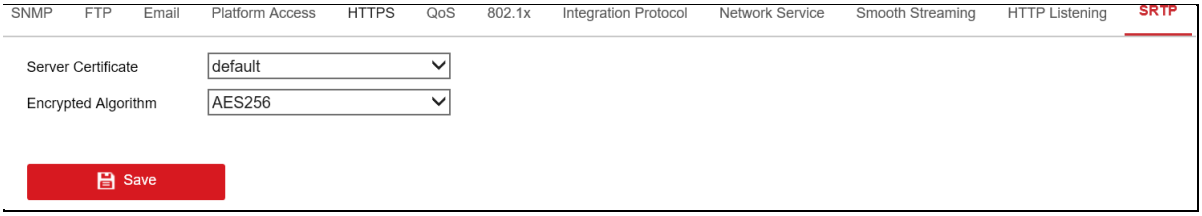


図 7-16 SRTP 設定

2. 「Server Certificate」を選択します。
3. 「Encrypted Algorithm」を選択します。
4. 「Save」をクリックし、設定を保存します。

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。
- 正常に機能しない場合は、証明書管理で選択した証明書に異常がないか確認してください。

7.2.15 アラームサーバーの設定

目的:

カメラは、HTTP、HTTPS、ISUP プロトコルを使用して、宛先 IP またはホスト名にアラーム情報を送信できます。ネットワークが切断されておらず、ネットワーク接続が正常であれば、データを宛先 IP またはホスト名にアップロードできます。

準備:

宛先 IP またはホスト名は、アラーム情報を受信するために HTTP、HTTPS、ISUP プロトコルをサポートする必要があります。

手順:

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

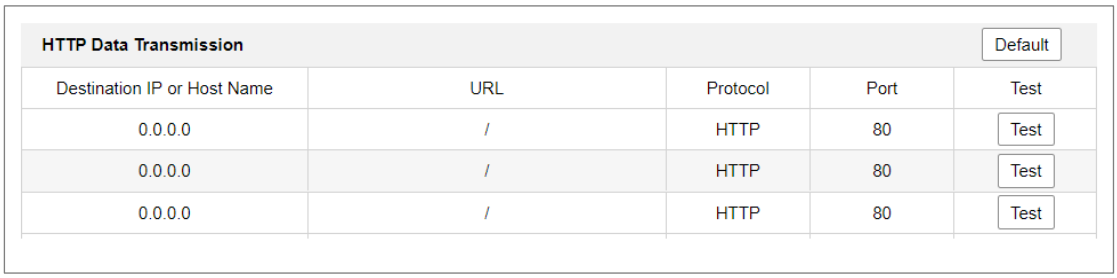


図 7-17 アラームサーバー

2. 目的の宛先 IP またはホスト名、URL、ポートを入力します。
3. 「Test」をクリックして、入力した IP アドレスまたはホスト名が有効かどうかをテストできます。
4. 「Default」をクリックして、宛先 IP またはホスト名をリセットすることもできます。

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。

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。

お知らせ: サポートされる機能は、モデルによって異なります。

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。

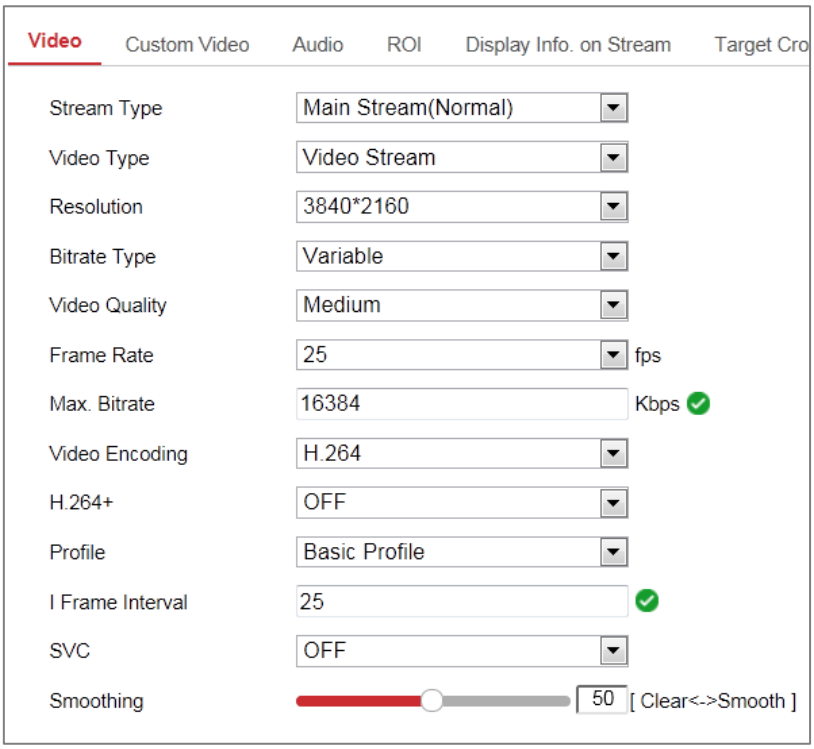


図 8-1 「Video」設定

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。オーディオ信号は、「Video Type」が「Video & Audio」の場合にのみ記録されます。

   「Resolution」:

   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」:

   ビットレートタイプを「Variable」に設定すると、6 段階の映像品質を選択できます。

   「Frame Rate:」:

   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」:

   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、カメラプラットフォームによって異なります。一部のカメラでは、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。サポートす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ディングタイプは、カメラモードによって異なる場合があります。

「H.264+ ／ H.265+:」:

- **「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+をオンまたはオフにするには、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、またはその逆に切り換える場合、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になります。
- H.264+/H.265+ が有効にすると、一部の機能は非対応になります。非対応のメニューは、画面上では非表示になります。
- H.264+/H.265+は、設定し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自発的にビットレート分布を調整します。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 時間かかります。

「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、実際に表示される画面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、ライブビューは可能ですが、録画や再生はできません。

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。
- カメラの復元操作（デフォルト設定に戻さない）をすると、カスタムビデオストリームの数と名前は保持されますが、関連するパラメータは復元されます。

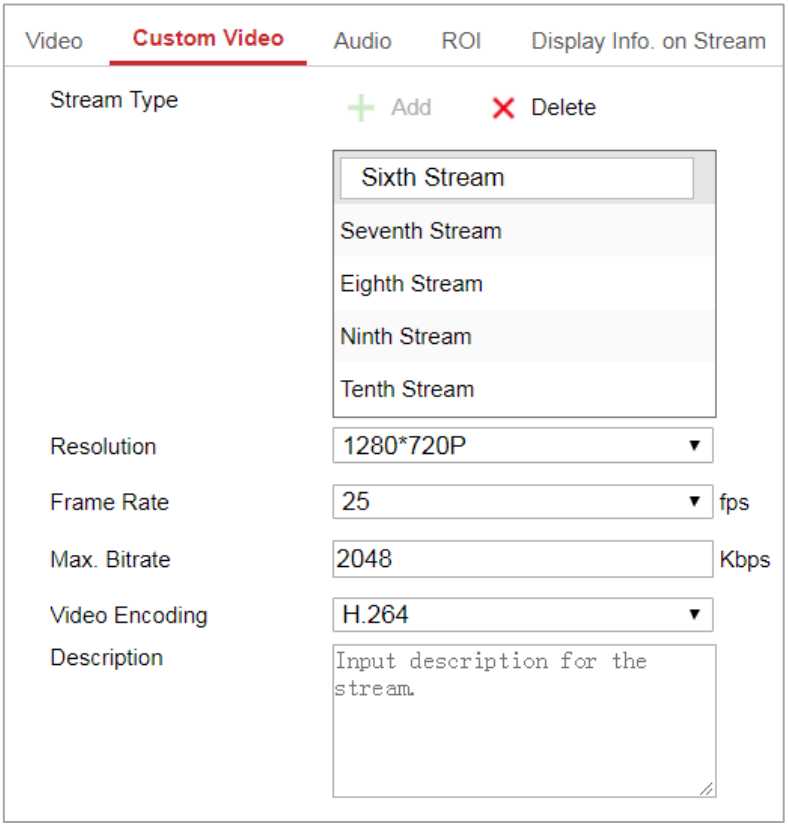


図 8-2 カスタムビデオ設定

手順:

1. ＋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（&、<、>、'、または" を除く）を使用できます。

3. ストリームパラメータ（解像度、フレームリテント、最大ビットレート、ビデオエンコーディング）をカスタマイズします。パラメータの概要については、「8.1.1 ビデオ設定」を参照。
4. 必要に応じてストリームの説明を追加します。
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。

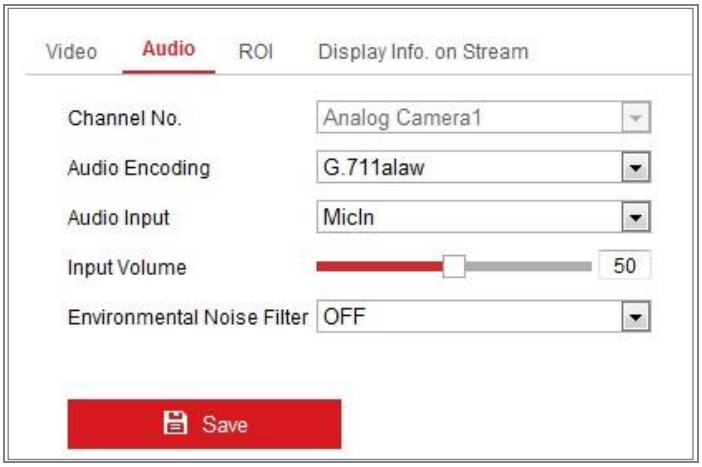


図 8-3 オーディオ設定

2. 以下の設定を行います。

お知らせ: オーディオ設定は、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。

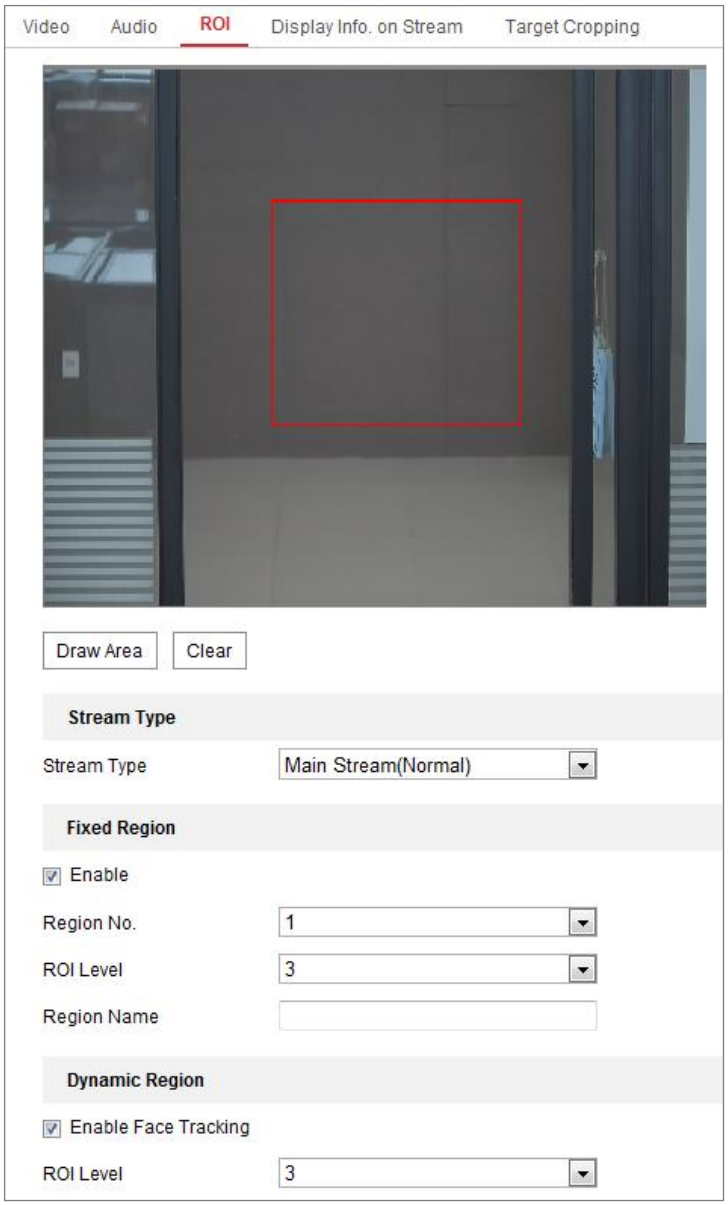


図 8-4 ROI エンコーディングの設定

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。
   (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、画質は良くなります。

8.4 ストリーム上の情報表示

「Enable Dual-VCA」チェックボックスをオンにすると、オブジェクト(人、車両など)の情報がビデオストリームでマークされます。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、必要に応じてターゲットエリアの詳細を表示することができます。

お知らせ: ターゲットクロッピング機能は、モデルによって異なります。

手順:

1. 「Target Cropping」設定画面を選択します。
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. 対象領域の映像表示部のクロップ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。

お知らせ: サポートされる機能は、モデルによって異なります。

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、実際の画面を参照してください。

手順:

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

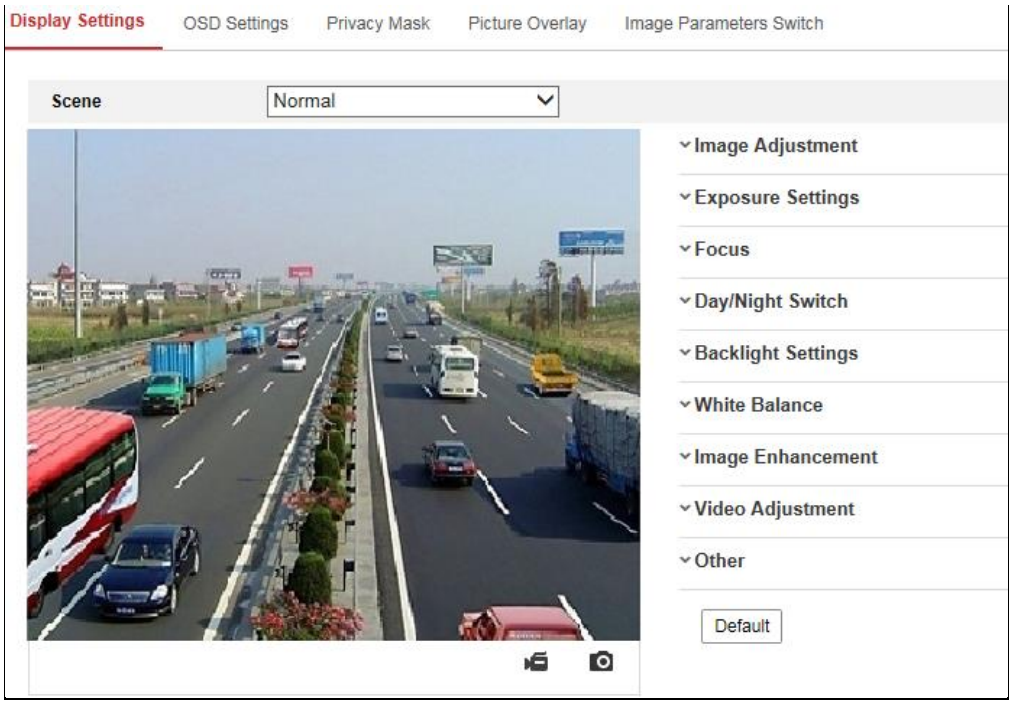


図 9-1 設定を表示する

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。

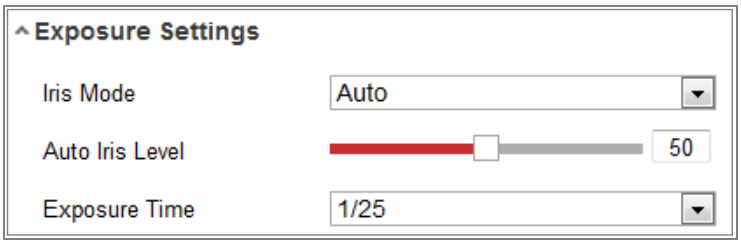


図 9-2 Exposure Settings

- 「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。

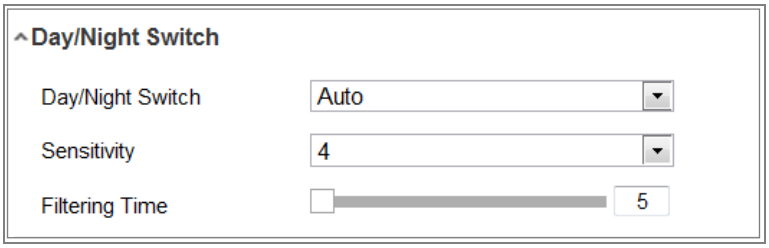


図 9-3 Day/Night Switch

「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」: ハイライトコンプレッション機能は、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。

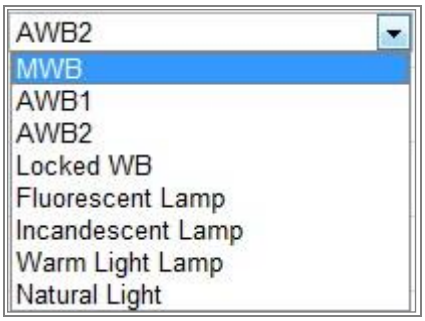


図 9-4 White Balance

- 「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」

「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れます。

「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。

お知らせ: ビデオ調整機能は、デバイスのモデルによって異なります。

- その他

一部のカメラモデルは、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:

ライブビューで OSD 情報をカスタマイズできます。

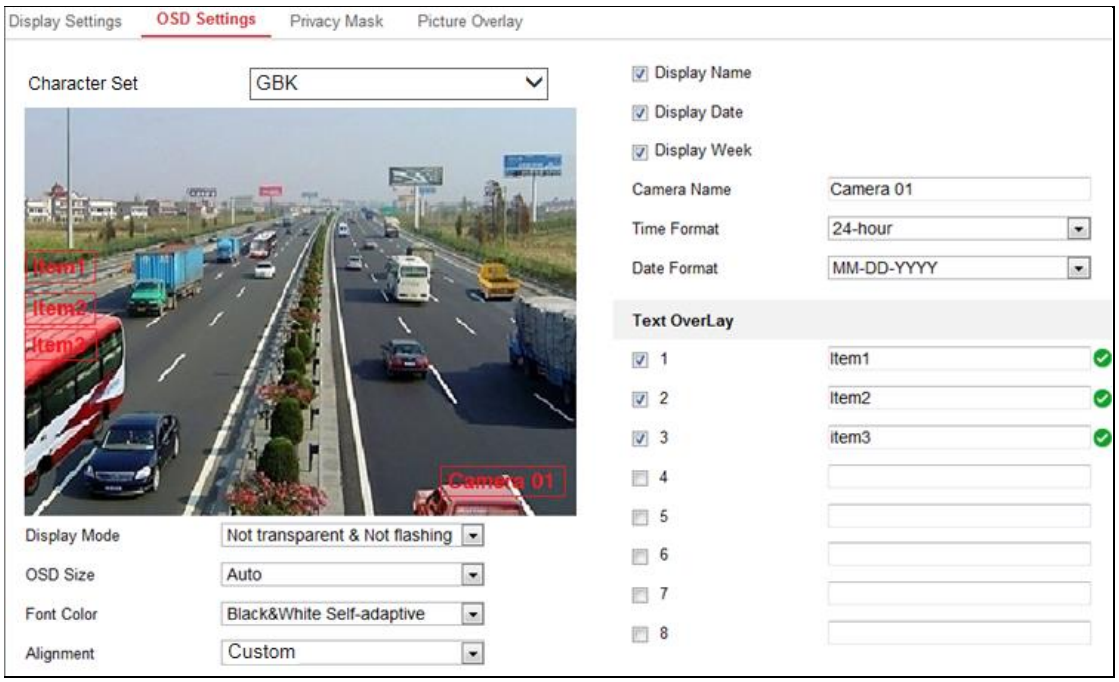


図 9-5 OSD 設定

手順:

1. 「Configuration」 > 「Image」 > 「OSD Settings」を選択します。
2. 目的の「Character Set」を選択します。
3. 対応するチェックボックスをオンにし、カメラ名、日付、または週の表示を選択します（必要な場合）。
4. カメラ名のテキスト欄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行います。
   (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 の位置と配置を調整します。
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、上下左右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ビューおよび録画されないようにすることができます。

手順:

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。

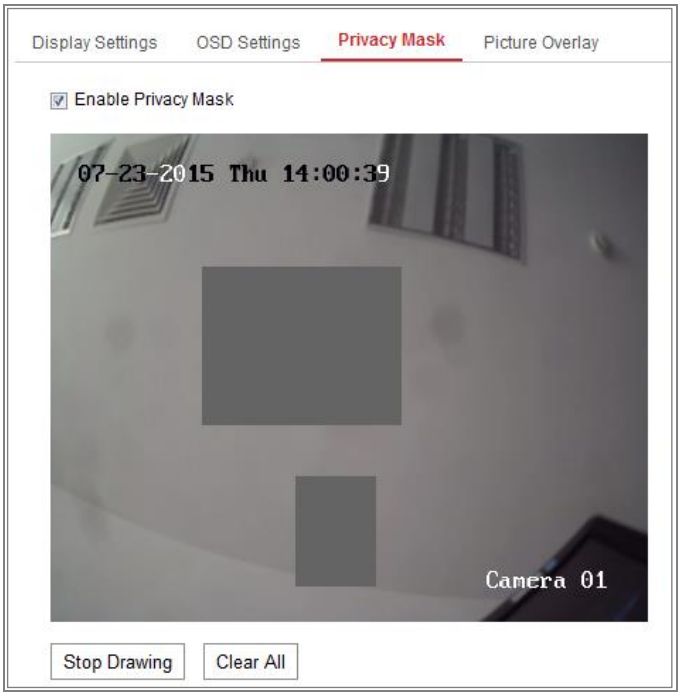


図 9-6 プライバシーマスクの設定

4. ライブビデオウィンドウでマウスをクリック・ドラッグし、マスク領域を描画します。

お知らせ: 同じイメージ上に最大 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. 「Add」をクリックしてプライバシーマスクを追加すると、プライバシーマスクリスト領域に表示されます。
7. マスク設定を変更します。

   「Type」: マスクに黒を指定することも、モザイクとして設定することもできます。

   お知らせ: モザイクオプションは、特定のカメラモデルでのみサポートされます。
8. 「Save」をクリックしてマスクを保存します。
9. 上記の手順を繰り返して、他のマスクを設定します。
10. 保存したマスクを削除するには、リストでマスクを選択し、「Delete」をクリックします。

9.4 画像オーバーレイの設定

目的:

画像オーバーレイを使用すると、画像上に画像をオーバーレイできます。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。

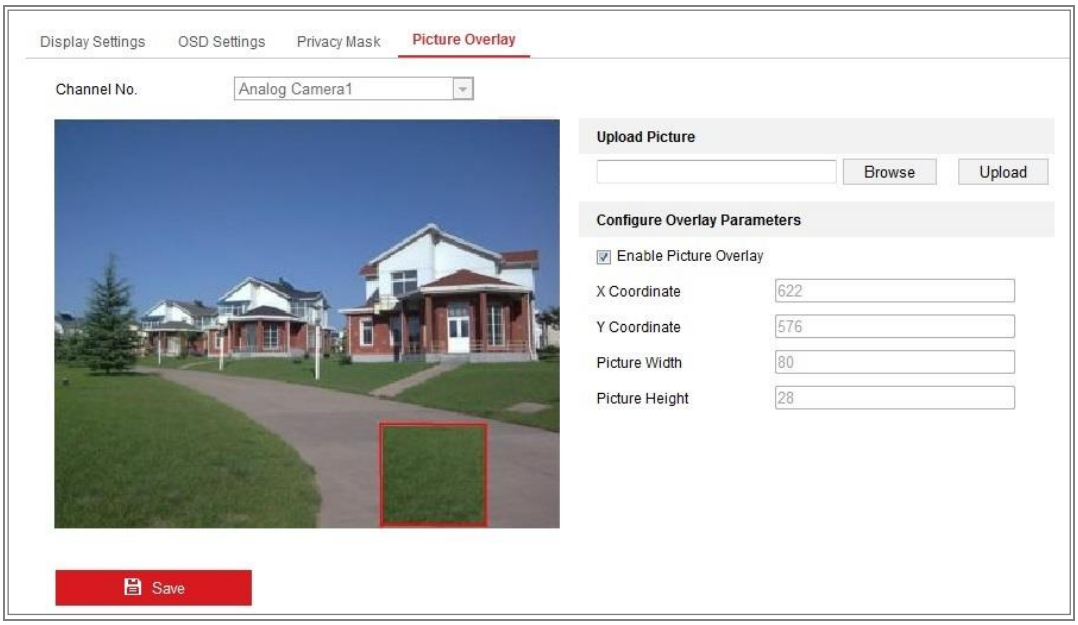


図 9-7 画像オーバーレイ

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。

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。

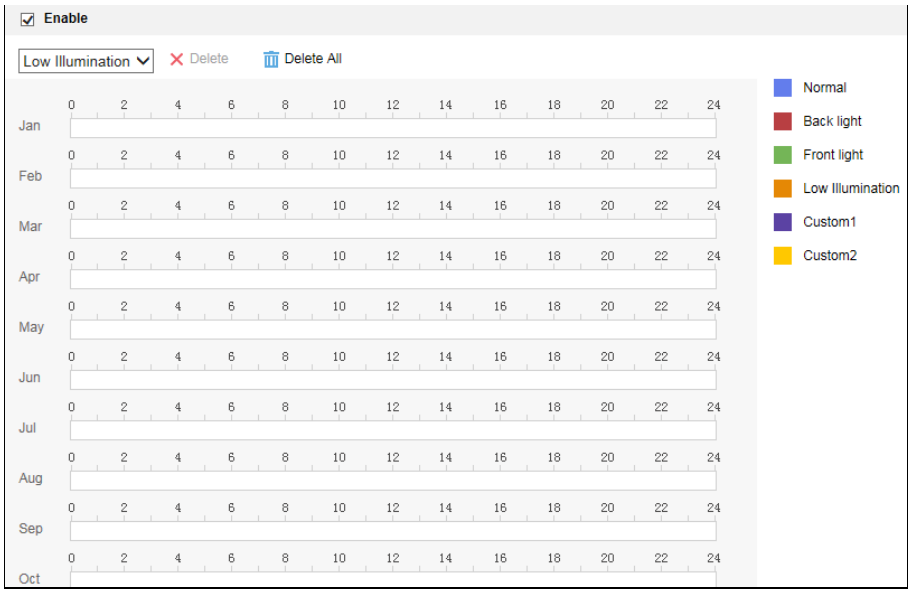


図 9-8 画面切り換えパラメータの設定画面

手順:

1. 「Configuration」 > 「Image」 > 「Image Parameters Switch」を選択します。
2. 「Enable」チェックボックスをオンにします。
3. リンクしたいシーンを選択し、タイムスケジュールに時間を描画します。
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、このセクションの手順に従って基本的な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。
- サポートされる機能は、モデルによって異なります。

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動体を検出し、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を緑色の長方形で表示したくない場合は、「Configuration > 「Local Configuration」 > 「Live View Parameters-rules」を選択し、ルールで「Disable」を選択します。

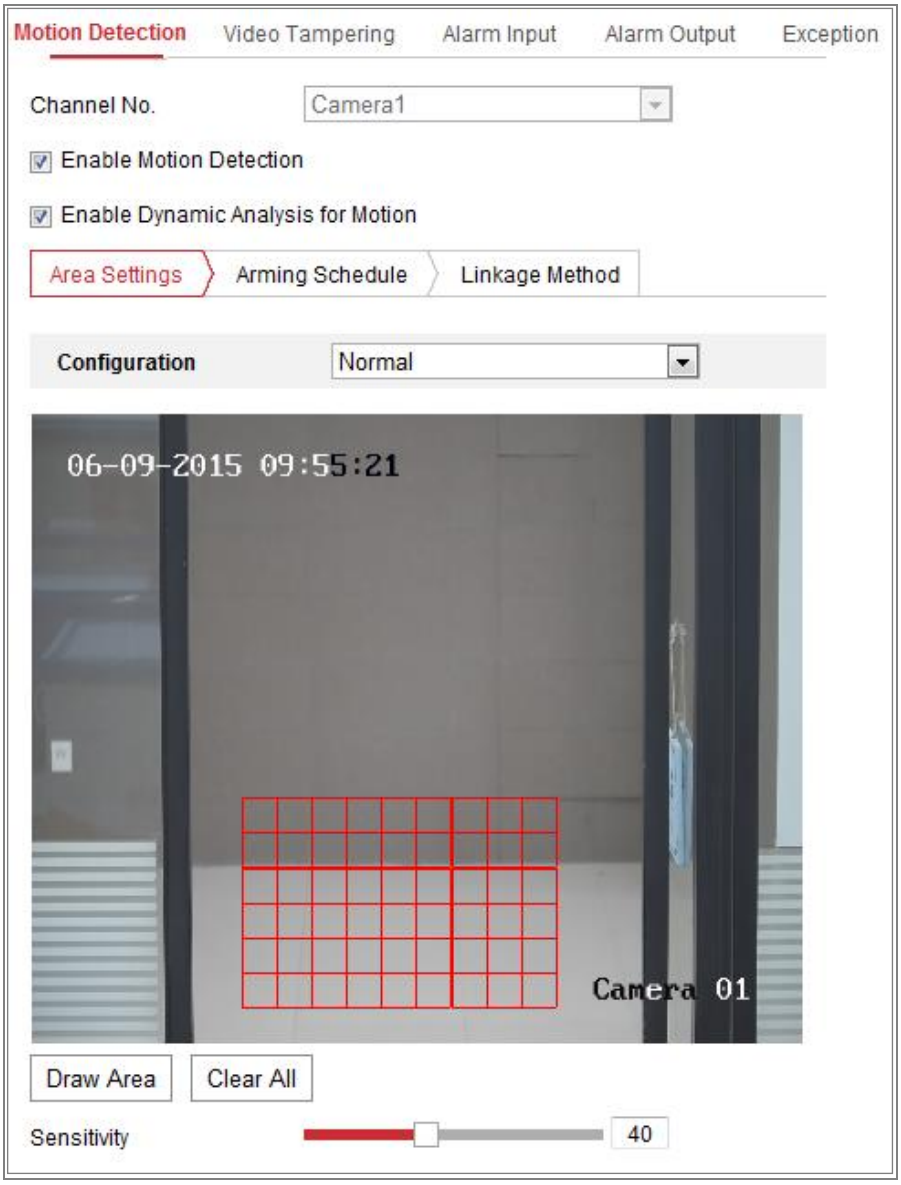


図 10-1 モーション検出の有効化

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

手順:

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。

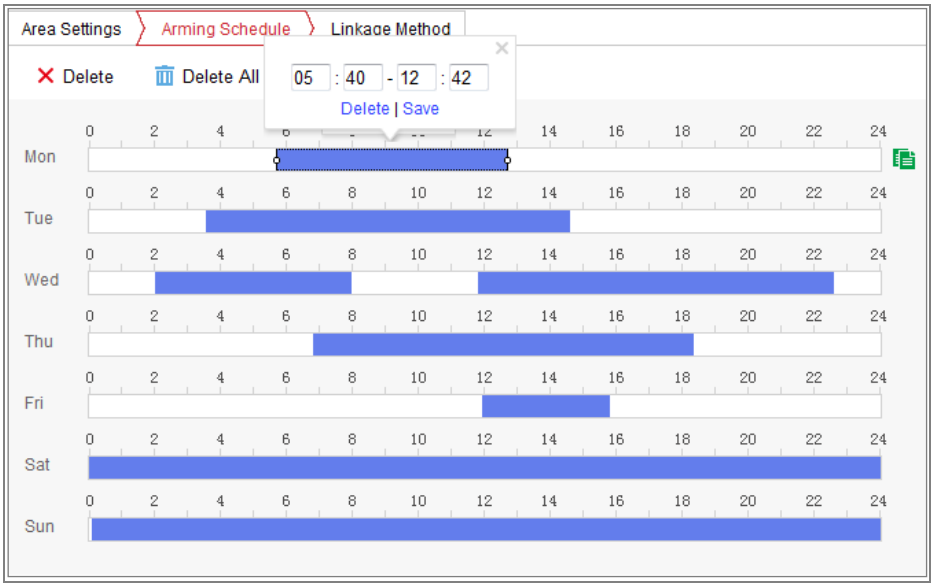


図 10-3 アーミングスケジュール

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移動すると、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、設定を保存します。

お知らせ: 各期間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

チェックボックスにチェックを入れ、連携方法を選択します。アラーム音、E メールの送信、監視センターへの通知、FTP/メモリーカード/NAS へのアップロード、トリガ・チャネル、アラーム出力を選択できます。イベント発生時の連動方法を指定できます。

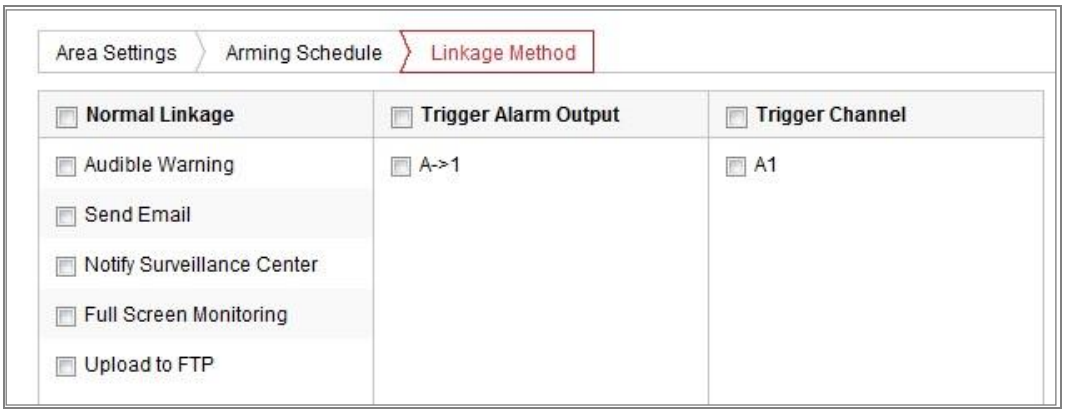


図 10-4 連携方法

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、「7.2.3E 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、リモート管理ソフトウェアに例外またはアラーム信号を送信します。

- 「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、録画が開始されます。この機能を有効にするには、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。

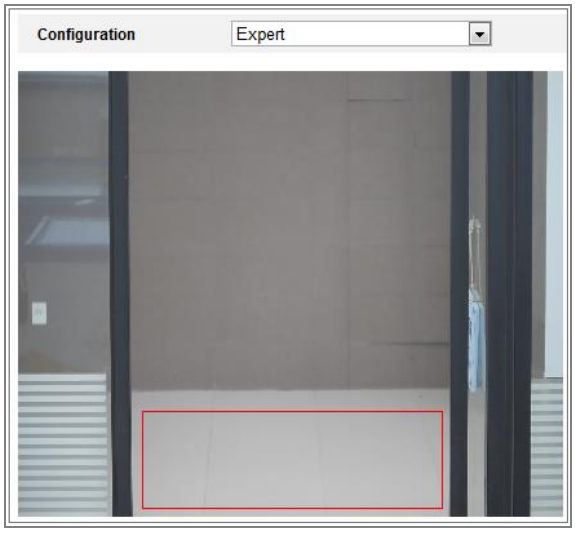


図 10-5 運動検出の Expert モード

- 日中/夜間スイッチ OFF

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「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携方法を設定します。
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して、日中の選択したエリア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して、選択したエリアの夜間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携方法を設定します。
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

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「Scheduled-Switch」を選択します。

図 10-6 Switch Day and Night Settings

3. 切り換えタイミングの開始時刻と終了時刻を選択します。
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して、日中の選択したエリア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して、選択したエリアの夜間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携方法を設定します。
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。

手順:

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し、ビデオの改ざんに使用する連携方法を選択します。「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、設定を保存します。

10.1.3アラーム入力の設定

手順:

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。

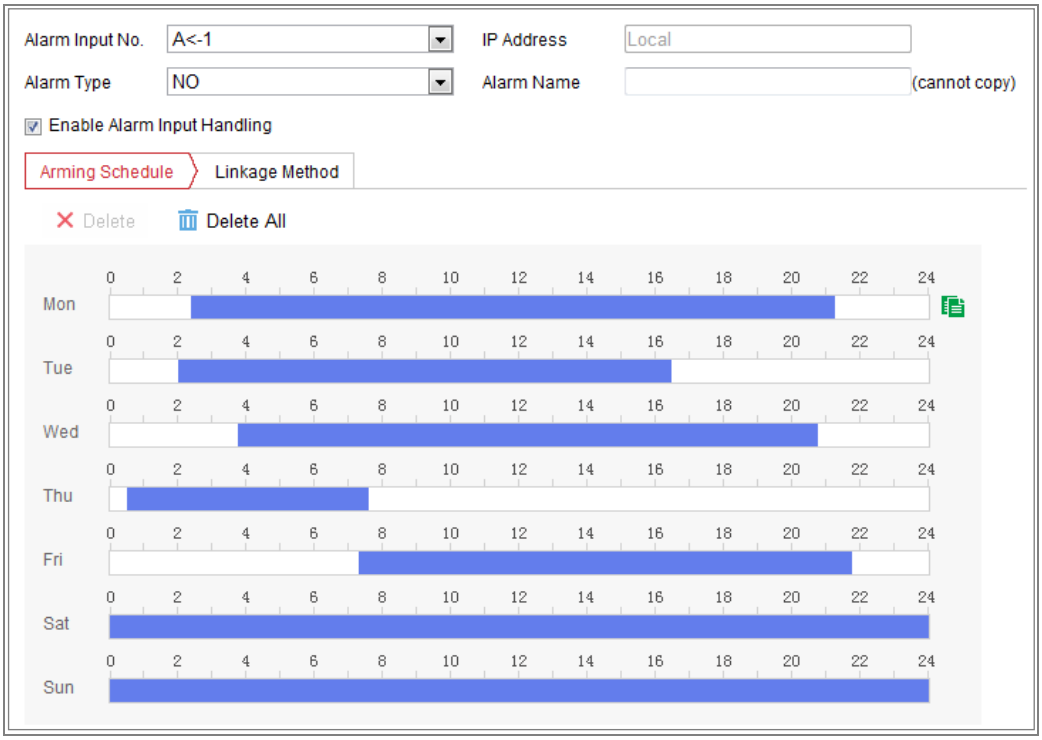


図 10-7 アラーム入力設定

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。「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. 「Linkage Method」をクリックし、チェックボックスをオンにして、アラーム入力の連動方法を選択します。「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. 設定を他のアラーム入力にコピーできます。
6. 「Save」をクリックし、設定を保存します。

10.1.4 アラーム出力の設定

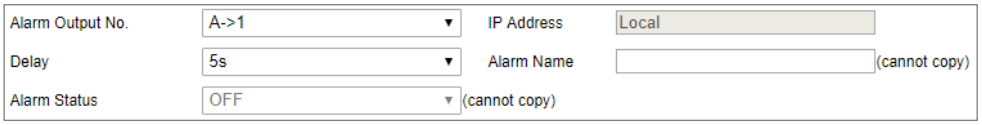


図 10-8 アラーム出力設定

手順:

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. ディレイタイムを設定します。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、「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、モーション検知のアーミングスケジュールの設定と同じです。
5. 設定を他のアラーム出力にコピーできます。
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。

手順:

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。「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。
3. 「Save」をクリックし、設定を保存します。

10.1.6 アラームライト出力の点滅の設定

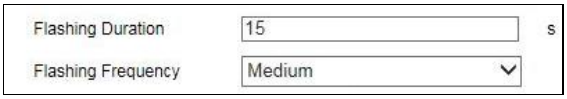


図 10-9 アラームライト出力の点滅の設定

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。高・中・低から選択できます。
- 「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この機能をサポートしています。

10.1.7ビデオのパラメータの設定

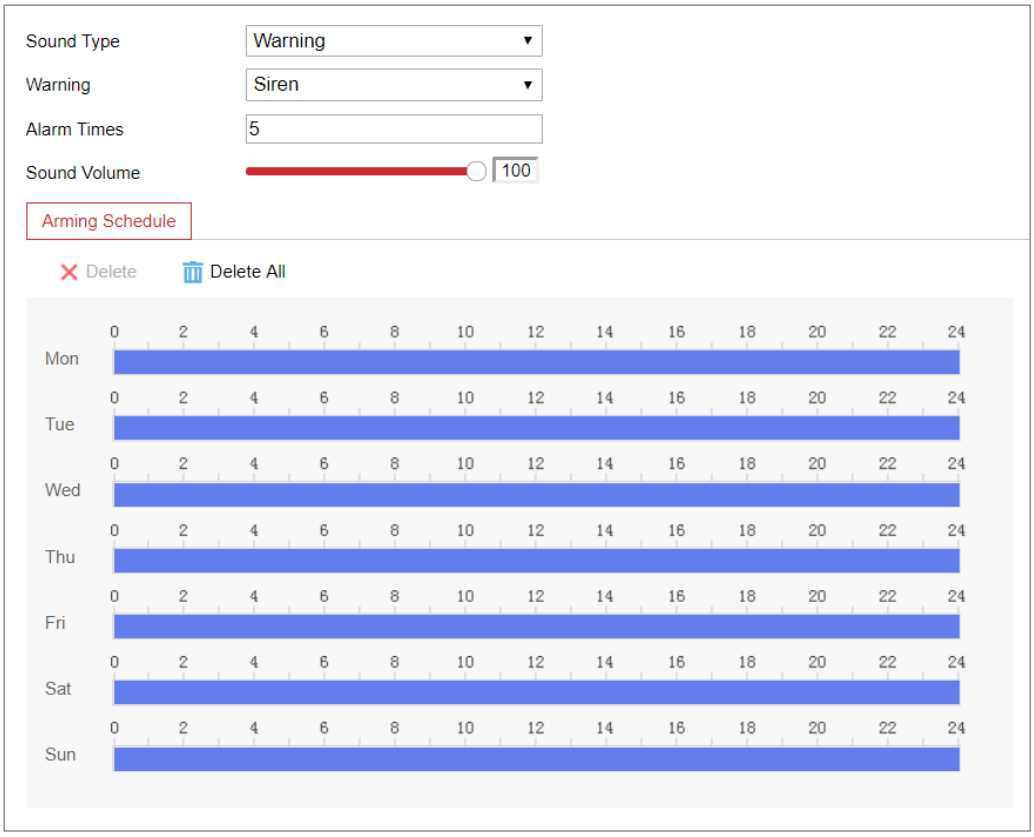


図 10-10 ビデオのパラメータ設定

手順:

1. 「Configuration」 > 「Event」 > 「Basic」 > 「Event」 > 「Audible Alarm Output」を選択します。
2. 診断タイプを選択します。
3. 「Enable Brightness Exception」をチェックします。
4. 対応するパラメータを設定します。

- 「Alarm Detection Level」: 設定範囲 [5～300]
- 「Sensitivity」: 設定範囲 [1～9]、値が大きいほど、例外を検出しやすくなります。
- 「Alarm Delay」: 設定範囲[1～9]、設定された遅延時間に達するとアラームをアップロードします。

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。
6. 「Linkage Method」をクリックして、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: 特定のモデルのみがこの機能をサポートしています。

10.1.8ビデオ品質診断

機器の映像品質に異常があり、アラーム連動が設定されている場合、自動的にアラームが作動します。

手順:

1. 「Diagnosis Type」を選択します。
2. 「Enable Brightness Exception」をオンにします。
3. 対応するパラメータを設定します。
   - **「Alarm Detection Interval」:** 設定範囲[5～300]、初期値は 5 です。
   - **「Sensitivity」:** 設定範囲[1 ～10]、デフォルト値は 5 です。値が大きいほど、例外を検出しやすくなります。
   - **「Alarm Delay」:** 設定範囲[0～100]、初期値は 1 です。アラームが設定された回数に達すると、デバイスはアラームをアップロードします。
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。
5. 「Linkage Method」をクリックして、連携方法を選択します。
6. 「Save」をクリックし、設定を保存します。

お知らせ: 特定のモデルのみがこの機能をサポートしています。

10.1.9 振動検出

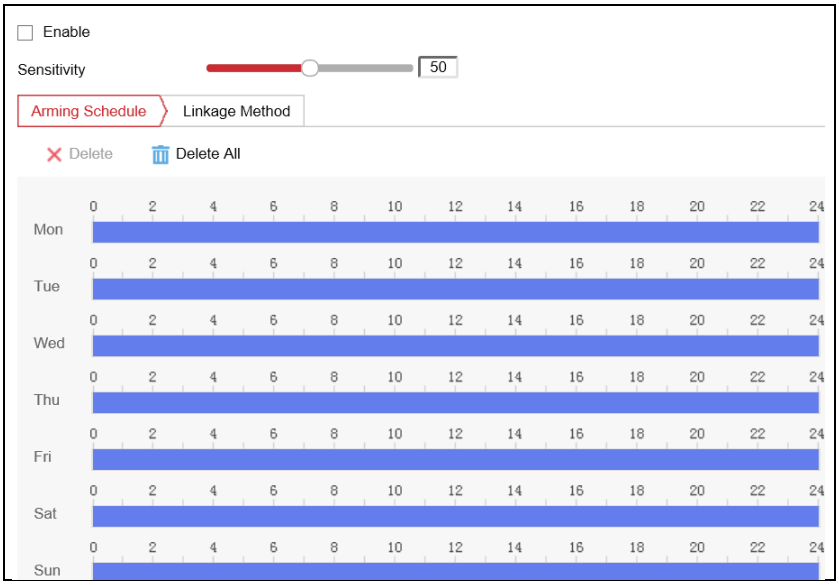


図 10-11 振動検出設定

手順:

1. 「Configuration」 > 「Event」 > 「Basic Event」 > 「Vibration Detection」を選択します。
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。
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。
5. 「Linkage Method」をクリックして、連携方法を選択します。
6. 「Save」をクリックし、設定を保存します。

お知らせ: 特定のモデルのみがこの機能をサポートしています。

10.1.10 音声アラーム出力の設定

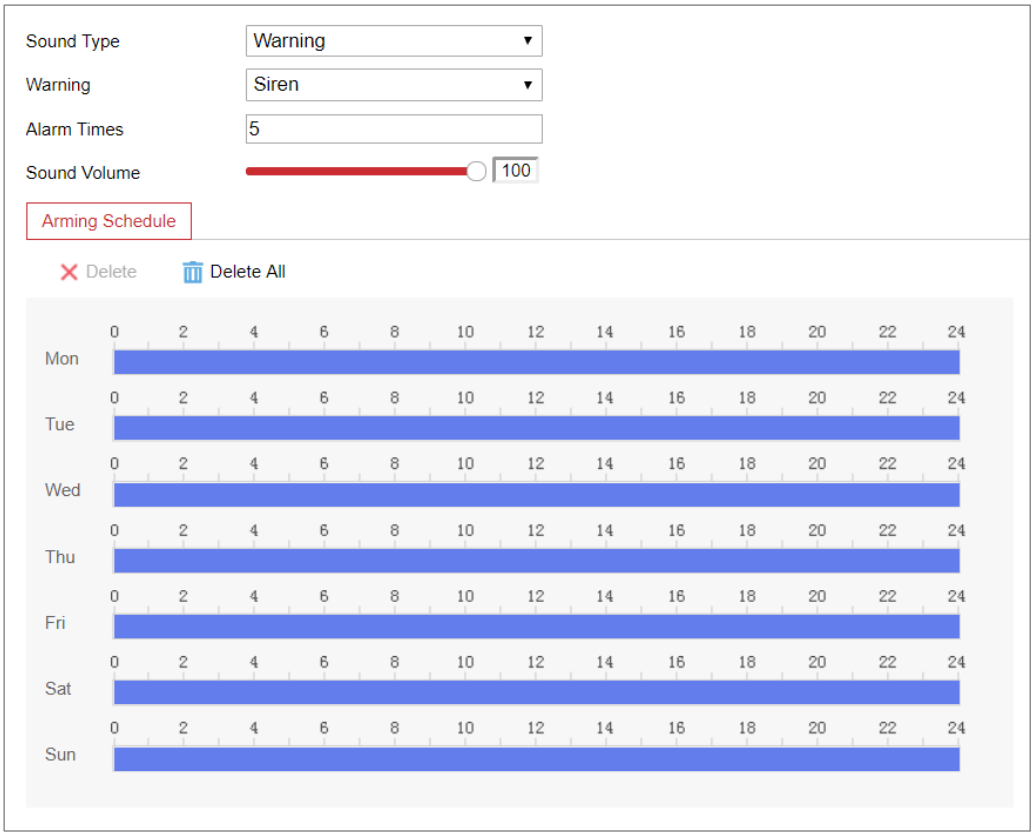


図 10-12 音声アラーム出力設定

手順:

1. 「Configuration」 > 「Event」 > 「Basic Event」 > 「Audible Alarm Output」を選択します。

- 「Sound Type」: アラームとプロンプトを選択できます。
- 「Warning」: アラームの内容
- 「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. アラームの鳴動時間や音量を設定します。
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。
5. 「Save」をクリックし、設定を保存します。

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。

10.1.11 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が発生され、一連の応答アクションを実行します。

手順:

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

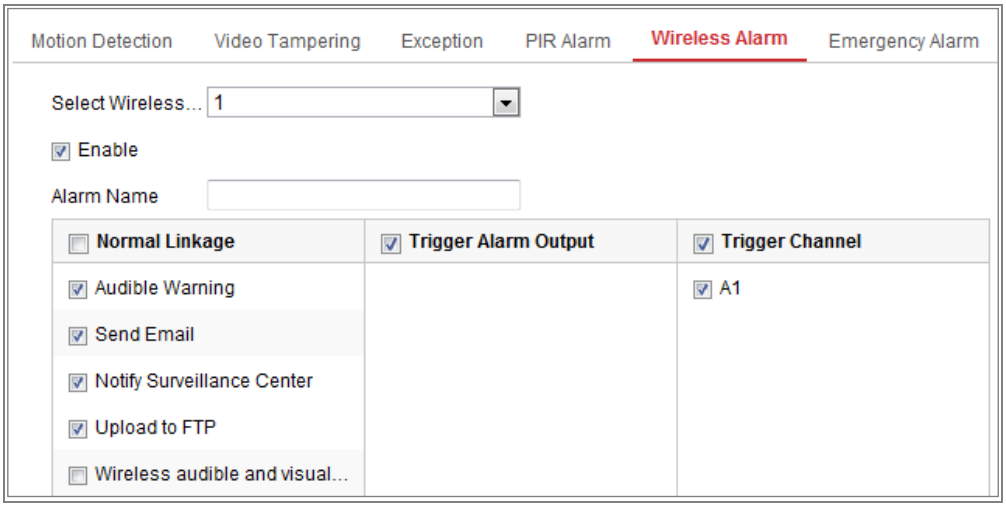


図 10-13 ワイヤレスアラームを設定する

2. ワイヤレスアラーム番号を選択します。

   最大 8 チャンネルの外部ワイヤレスアラーム入力に対応しています。

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、アラーム名を入力します。
5. チェックボックスをオンにし、ワイヤレスアラームの連携方法を選択します。
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。

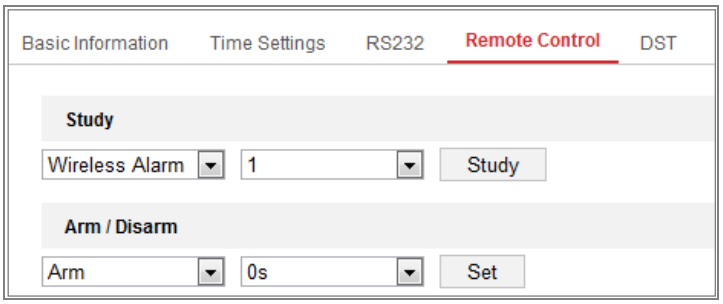


図 10-14 ワイヤレスアラーム設定

● 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。

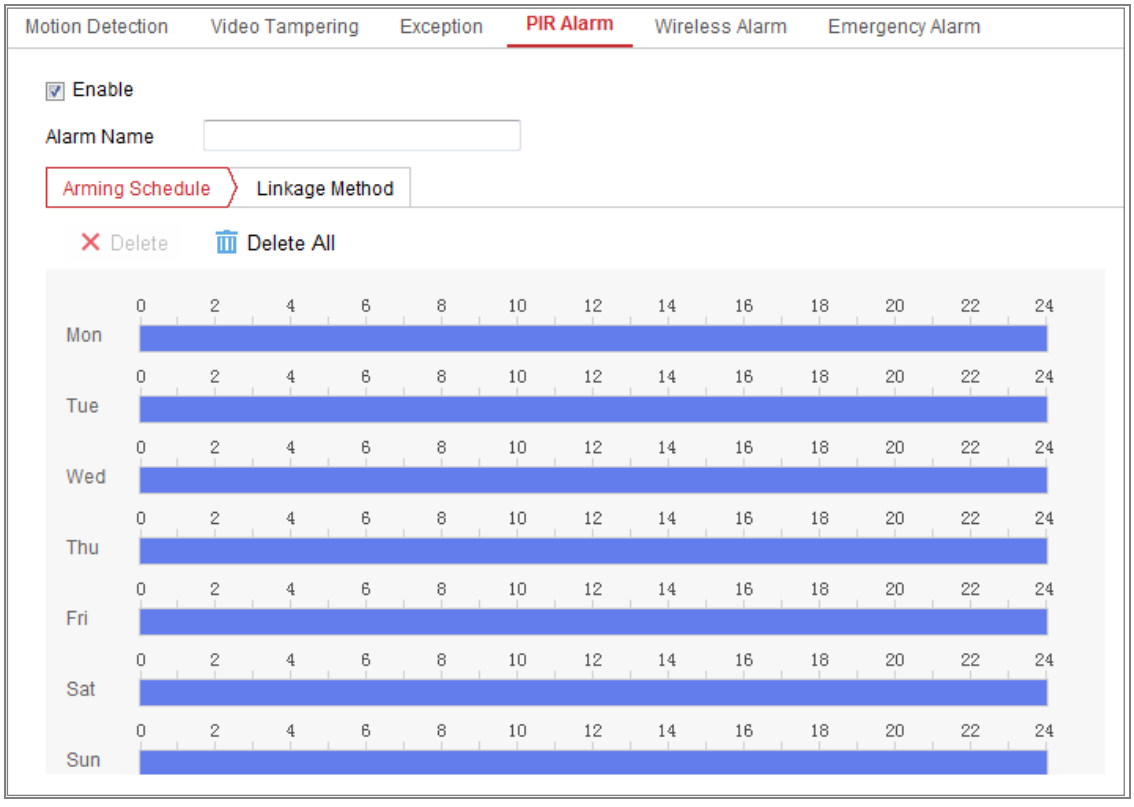


図 10-15 PIR アラームを設定する

2. 「Enable」チェックボックスをオンにすると、PIR アラーム機能が起動します。
3. 必要に応じて、アラーム名を入力します。
4. チェックボックスにチェックを入れ、PIR アラームの連動方法を選択します。
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。

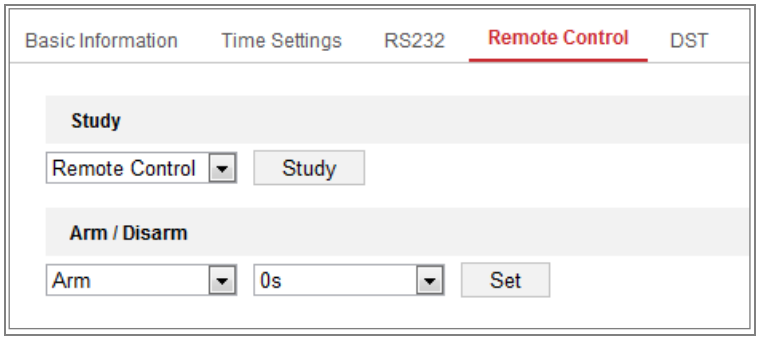


図 10-16 PIR アラームのアーミング

● 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発信できます。

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。

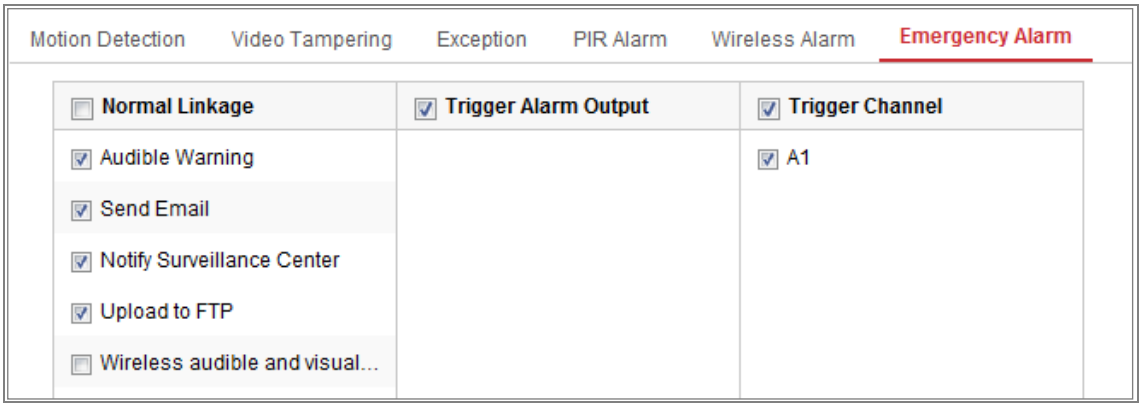


図 10-17 緊急アラームを設定する

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。

お知らせ: サポートされる機能は、モデルによって異なります。

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。

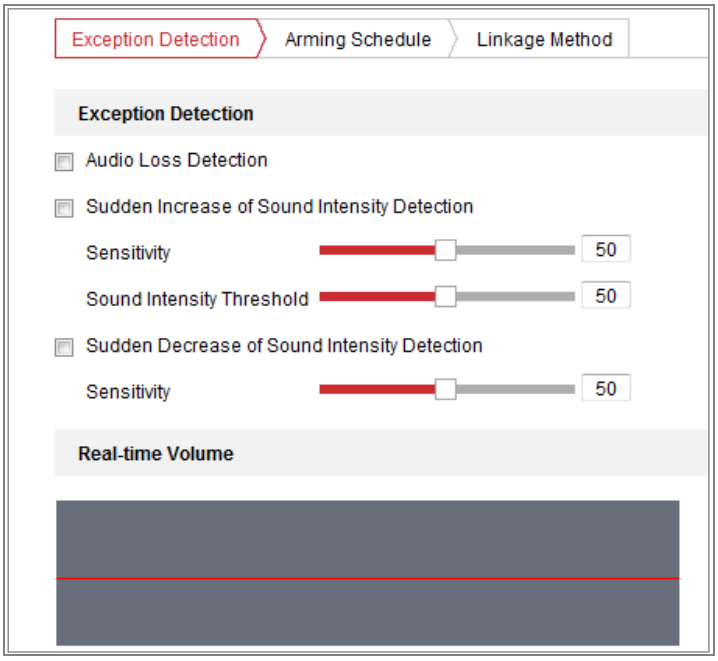


図 10-18 オーディオ例外検出

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変更の重大度が高くなります。
- 「Sound Intensity Threshold」: 設定範囲[1-100] 、環境内のサウンドをフィルタリングし、環境サウンドの音量が大きいほど、値を高くすることができます。実際の環境に合わせて調整します。
- 画面上で音声の実際の音量が表示されます。

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、「10.1.1 モーション検出の設定」の「タスク 2 モーション検知の準備スケジュールを設定する」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。

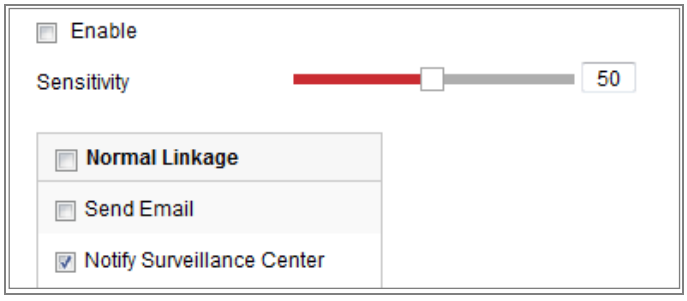


図 10-19 デフォーカス検出の設定

2. 「Enable」チェックボックスをオンにし、機能を有効にします。
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:

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

図 10-20 シーンチェンジの検出

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。感度値は 1 ～100 の範囲で、値が高いほど、シーンの変化によってアラームが発動されやすくなります。
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、「10.1.1 モーション検出の設定」の「タスク 2 モーション検知の準備スケジュールを設定する」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。

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。

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色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、「10.1.1 モーション検出の設定」の「タスク 2 モーション検知の準備スケジュールを設定する」を参照してください。
6. 「Linkage Method」をクリックし、顔検出の連携方法を選択します。「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。

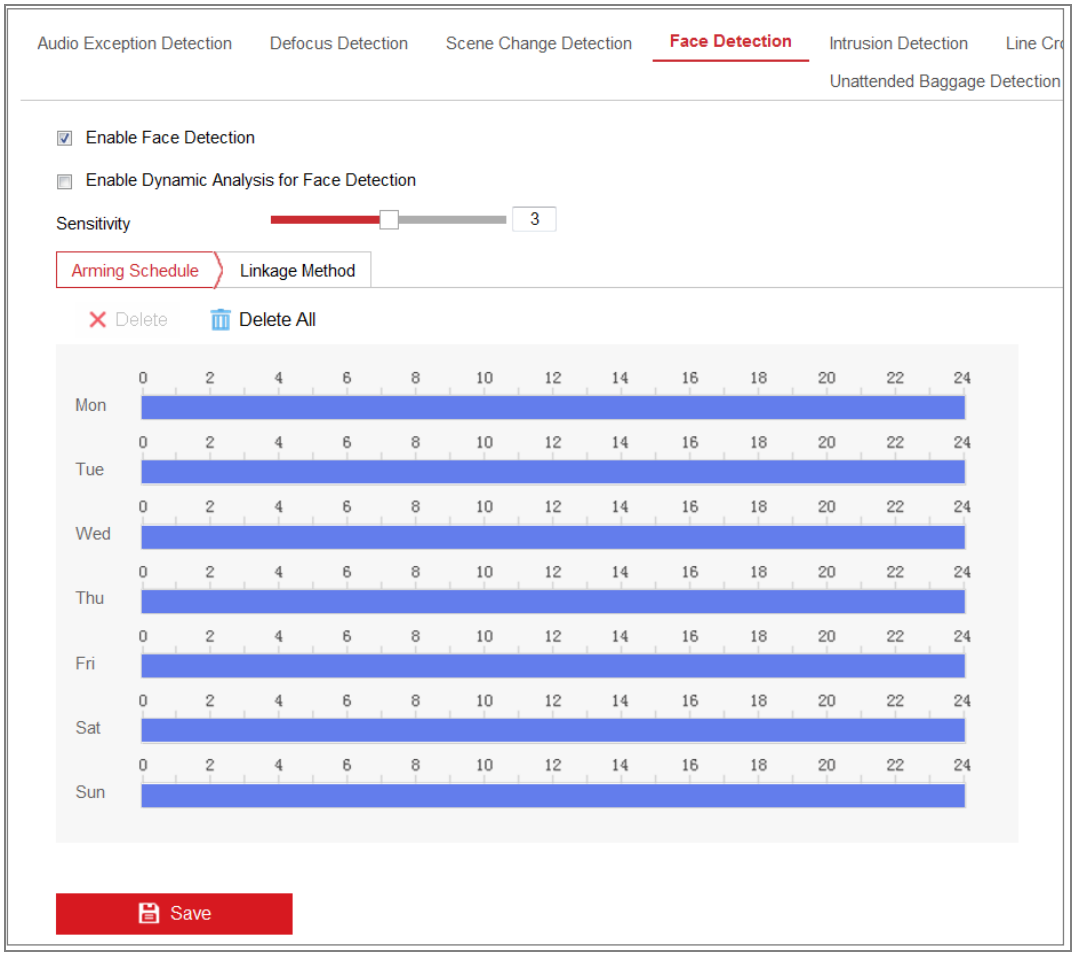


図 10-21 顔検出

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。

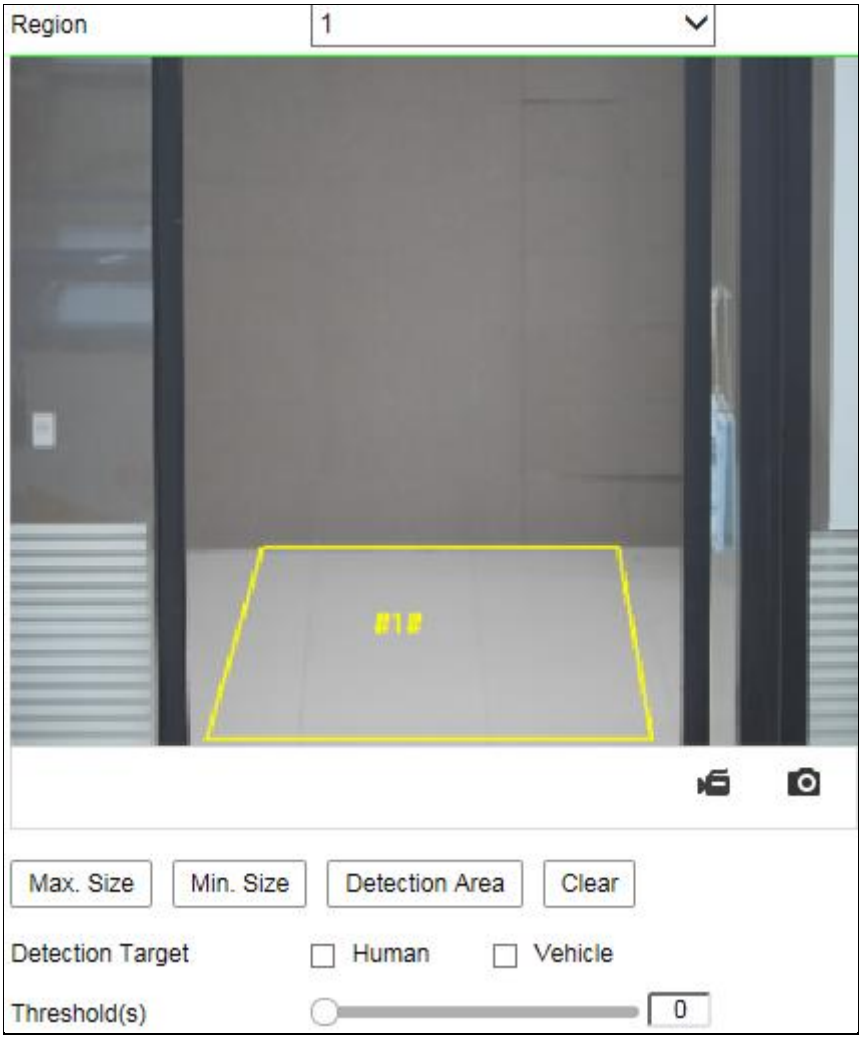


図 10-22 侵入検知

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。サイズが大きい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. 侵入検出の時間しきい値を設定します。

   「Threshold」: 設定範囲[0s-10s]、リージョン内でオブジェクトが繰り返される時間のしきい値です。値を 0 に設定すると、オブジェクトが領域に入った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]、あらかじめ定義された領域内での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 - S_1 /S_T*100

   S_1 は、事前定義されたリージョンを通過するターゲットボディパートを表します。S_T は完全なターゲットボディを表します。

   例: 値を 60 に設定した場合、40 パーセントのボディパートがリージョンに入ったときにのみ、アクションを侵入としてカウントできます。

   お知らせ: 検出の感度は、特定のモデルでサポートされています。
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 つのリージョンを設定できます。「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. 「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、連携方法を選択します。これには、監視センターへの通知、電子メールの送信、FTP/メモリーカード/NAS へのアップロード、トリガ・チャネル、アラーム出力、アラームの点滅、アラーム音が含まれます。

    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。

10.2.6ライン交差検知の設定

目的:

ライン交差検知機能は、あらかじめ設定した仮想ラインを越えた人、車両、その他の物体を検出し、アラームが発生したときの動作を設定できます。

お知らせ: 交差検知機能は、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。

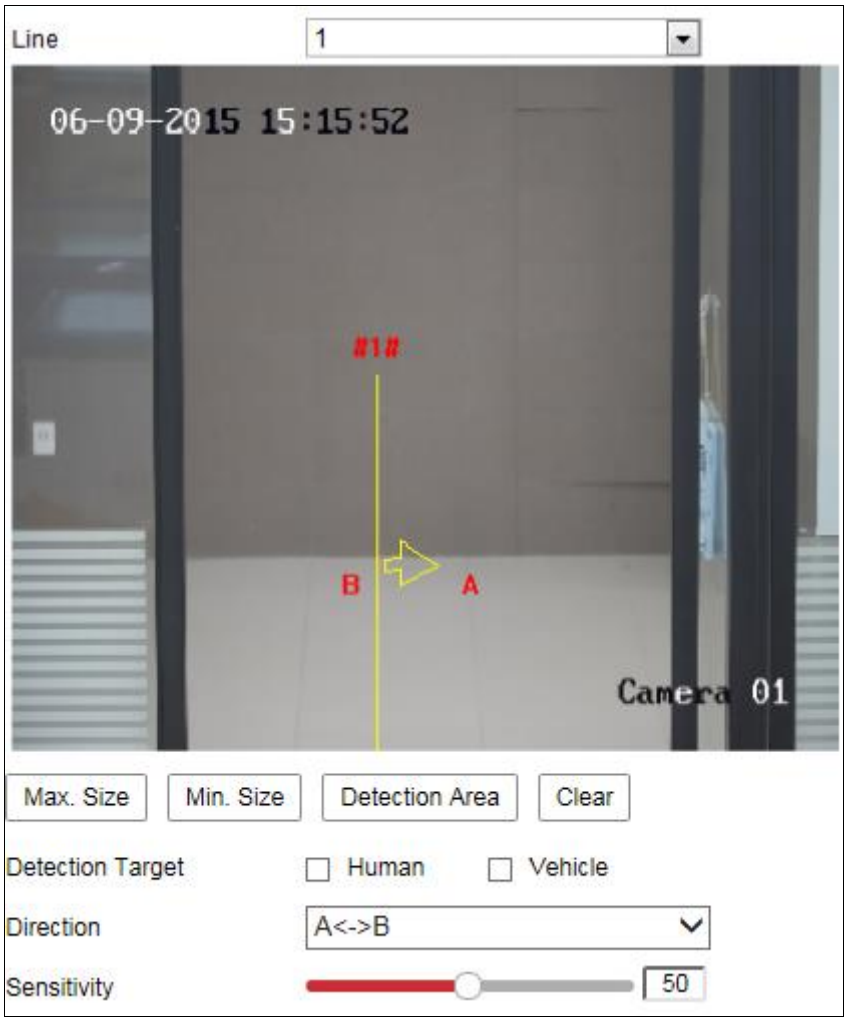


図 10-23 ライン交差検出

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ラインを選択します。

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または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。サイズが大きい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. 検知領域を設定します。ラインをドラッグすると、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. ライン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」: 両方向の平面上を通過する物体を検出し、アラームを発生させます。

   「A→B」: A 側から B 側に設定したラインと交差する物体だけを検出できます。

   「B→A」: B 側から A 側に設定したラインと交差する物体だけを検出できます。

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]、あらかじめ設定したラインを通過する、許容可能なターゲット物のパーセンテージを表します。

   感度= 100 − S_1 /S_T*100

   S_1 は、事前定義された行を通過する対象物を表します。S_T は完全なターゲット物を表します。

   例: 値を 60 に設定中に、40%以上の対象物がラインを交差すると、ライン交差アクションとしてカウントします。

   お知らせ: 検出の感度は、特定のモデルでサポートされています。

9. 他のラインを設定するには、上記の手順を繰り返します。4 行まで設定できます。「Clear」をクリックすると、設定したラインをすべてクリアします。

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、侵入検知の連携方法を選択します。これには、監視センターへの通知、電子メールの送信、FTP/メモリーカード/NAS へ

のアップロード、チャネル、アラーム出力、アラームの点滅、およびアラーム音が含まれます。

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、あらかじめ定義された仮想領域に入る人や車などを外部から検知し、アラーム発生時に特定の動作を行うことができます。

手順:

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

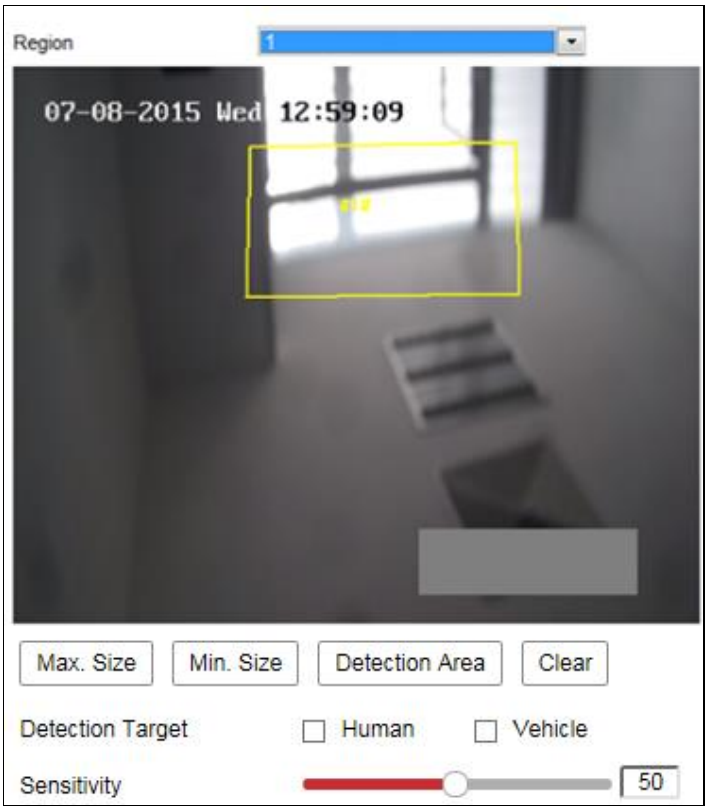


図 10-24 領域進入検出

をサポートしています。

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「Region」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または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。サイズが大きい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、ライブビデオをクリックします。

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]、あらかじめ定義された領域内での許容可能なターゲットのボディ部分のパーセンテージのことを表します。

   感度= 100 - S_1 /S_T*100

   S_1 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 に設定した場合、40% のボディパートがリージョンに入ったときにのみ、アクションをリージョン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、特定のモデルでサポートされています。

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 つのリージョンを設定できます。「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、侵入検知の連携方法を選択します。これには、監視センターへの通知、電子メールの送信、FTP/メモリーカード/NAS へのアップロード、チャネル、アラーム出力、アラームの点滅、およびアラーム音が含まれます。

    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 10-25 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「Region」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または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。サイズが大きい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、ライブビデオをクリックします。

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]、あらかじめ定義された領域内での許容可能なターゲットのボディ部分のパーセンテージのことを表しています。

   感度= 100 - S_1 /S_T*100

   S_1 は、事前定義されたリージョンを出るターゲットボディパートを表します。S_T は完全なターゲットボディを表します。

   例: 値を 60 に設定した場合、40% のボディパートがリージョンから出たときにのみ、アクションをリージョン出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、特定のモデルでサポートされています。
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 つのリージョンを設定できます。「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、侵入検知の連携方法を選択します。これには、監視センターへの通知、電子メールの送信、FTP/メモリーカード/NAS へのアップロード、チャネル、アラーム出力、アラームの点滅、およびアラーム音が含まれます。

    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。

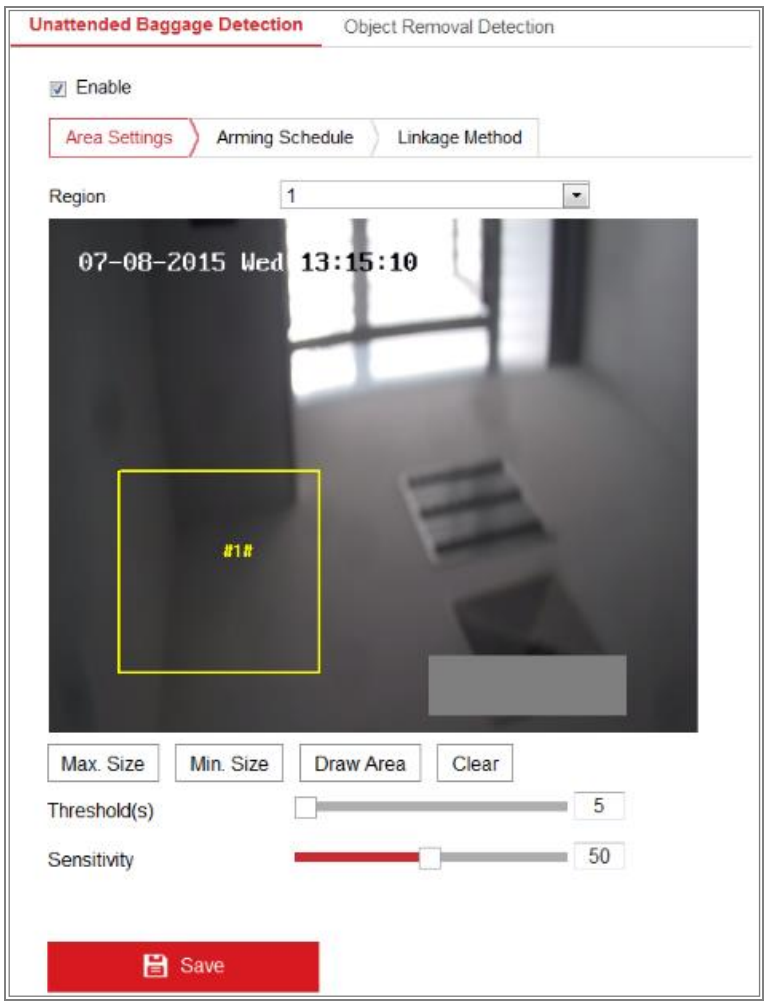


図 10-26 無人手荷物検知

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「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の描画を開始します。

5. 検出領域の 4 つの頂点を指定するには、ライブビデオをクリックします。
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または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。サイズが大きい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]、領域に残されたオブジェクトの時間のしきい値。値を 10 に設定すると、オブジェクトが残った後にアラームが発生し、10 秒間リージョンに留まります。
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]、あらかじめ定義された領域内での許容可能なターゲットのボディ部分のパーセンテージのことを表します。

   感度= 100 - S_1 /S_T*100

   S_1 は、事前定義されたリージョンに入るターゲットボディパートを表します。S_T は完全なターゲットボディを表します。

   例: 値を 60 に設定すると、ターゲットの体の 40% の部分がリージョン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できます。

   お知らせ: 検出の感度は、特定のモデルでサポートされています。
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 つのリージョンを設定できます。「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。

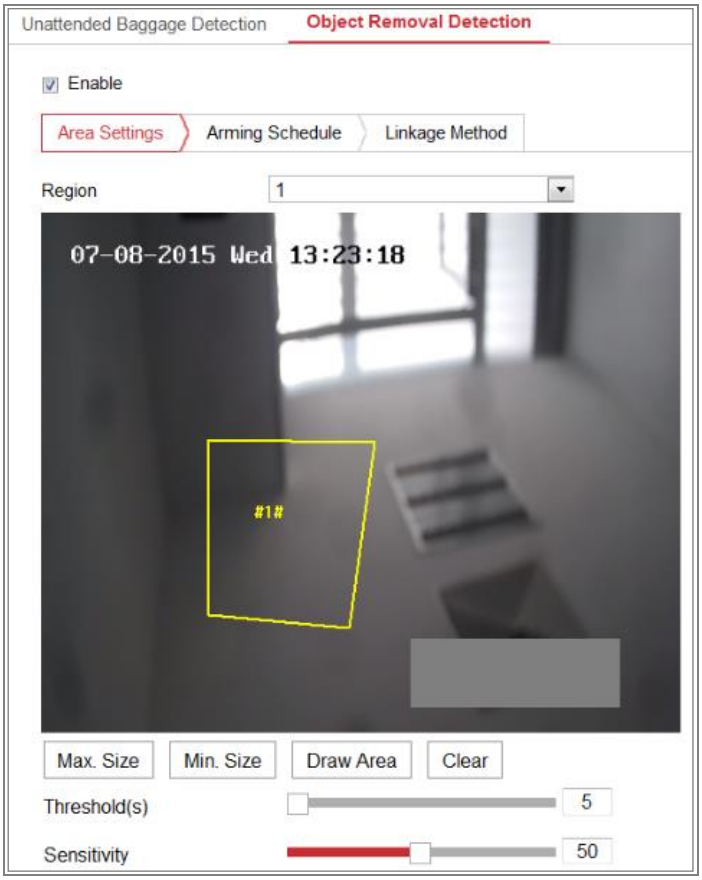


図 10-27 物体除去検出

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「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. 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. 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。

「**Max. Size**」: 有効なターゲットの最大サイズ。サイズが大きい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. オブジェクト退出検知の時間しきい値を設定します。

   「**Threshold**」: しきい値:領域から退出したオブジェクトの時間のしきい値である設定範囲[5～100s]。値を 10 に設定すると、オブジェクトが領域から 10 秒間消え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]**、あらかじめ定義された領域内での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 − S_1 /S_T*100

   S_1 は、事前定義されたリージョンを残すターゲットボディパートを表します。S_T は完全なターゲットボディを表します。

   例: 値を 60 に設定した場合、ターゲットの本体部分の 40% がリージョンを離れた場合にのみ、ターゲットは退出したオブジェクトとしてカウントされる可能性があります。

   お知らせ: 検出の感度は、特定のモデルでサポートされています。
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 つのリージョンを設定できます。「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。

10.3VCA 設定

お知らせ: サポートされる機能は、モデルによって異なります。

10.3.1フェイスキャプチャ

カメラは設定された領域に表示される顔をキャプチャでき、顔情報はキャプチャされた画像とともにアップロードされます。

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。

❖ **オーバーレイとキャプチャ**

「Display VCA info. on Stream」: ライブビューや再生では、赤いフレームがターゲットに表示されます。

「Display Target info. on Alarm Picture」: チェックボックスがチェックされている場合、アップロードされたアラーム画像にターゲット上にフレームがあります。

「Snapshot Settings」:

- 「Target Picture Settings」

a. ターゲットの画像サイズを選択します。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種類があります。「Custom」を選択すると、必要に応じて幅、ヘッドの高さ、ボディの高さをカスタマイズできます。

b. 画像の高さを設定するには、固定値をチェックします。

- 「Background Picture Settings」

a. ドロップダウンリストから「Picture Quality」と「Resolution」を選択します。

b. 「Background Upload」をチェックし、背景画像をアップロードします。

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ることが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」:

撮影した画像に表示したい項目を確認したり、順番を変えたりできます。

❖ 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 つのシールド領域に対応しています。

手順:

1. をクリックしてシールド領域を描画するには、ライブビューウィンドウでエンドポイントを左クリックし、右クリックして領域の描画を終了します。

お知らせ:

- 多角形領域（4 ～10 辺）がサポートされています。
- をクリックして、描画した領域を削除します。
- ライブビューが停止している場合、シールド領域を描画する方法はありません。

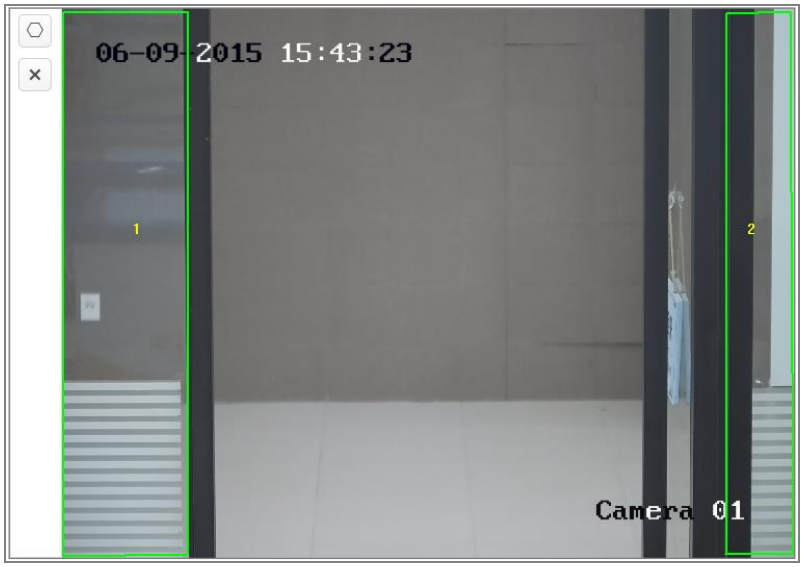


図 10-28 シールド領域の描画

2. 「Save」をクリックします。

❖ 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. 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。
3. をクリックして、最大瞳孔間距離を描画します。

4. をクリックして、顔のキャプチャを有効にする検出領域を描画します。ライブビューウィンドウでエンドポイントを左クリックしてエリアを描画し、右クリックしてエリアの描画を終了します。

   お知らせ:

   - 多角形領域(4 ～10 辺)をサポートしています。
   - ライブビューが停止している場合、設定された領域を描画する方法はありません。

5. 「Save」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、「Save」をクリックし、設定を保存します。
7. 「Alarm Linkage」をクリックし、各ルールに対応する連動方法のチェックボックスにチェックを入れ、「Save」をクリックし、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。

お知らせ: これらの機能は、モデルによって異なります。

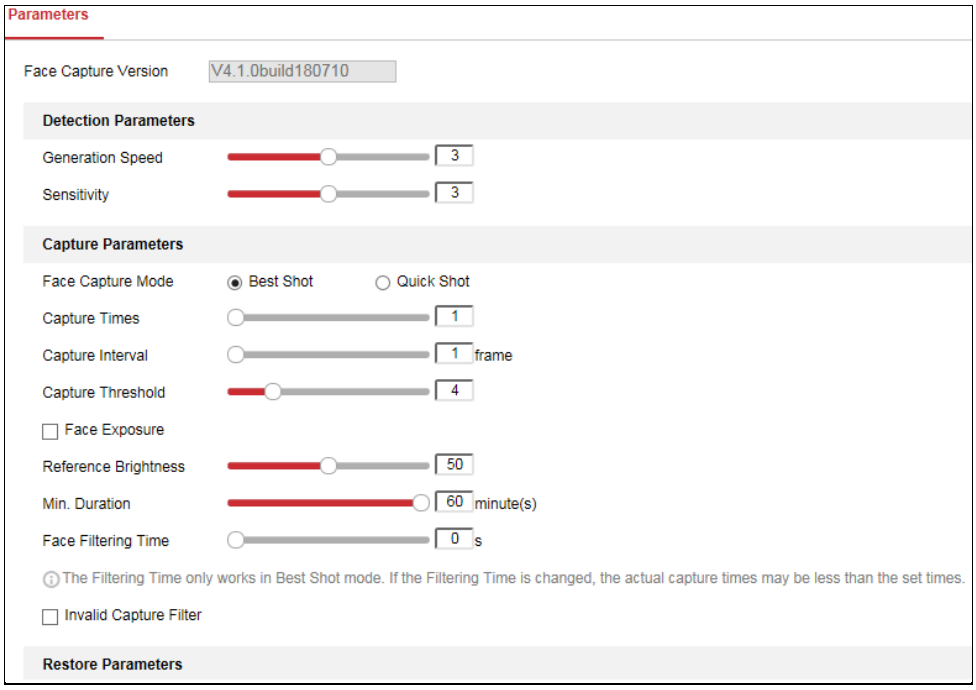


図 10-29 詳細設定

「Detection Parameters」:

「Generation Speed」 [1～5]: ターゲットを識別する速度。値が大きいほど、ターゲットの認識が速くなります。設定値を非常に低く設定し、最初から設定した領域に顔があった場合、その顔はキャプチャされませんが、壁ペイントやポスターの顔の情報ミス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感度。値が高いほど顔が認識しやすくなり、情報ミス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」: ベストショットとクイックショットが利用できます。

- 「Best Shot」: ターゲットが検出エリアから離れた後のベストショット。

  「Capture Times」 [1～3]: 設定された領域にとどまっている間に顔がキャプチャされるキャプチャ時間を表します。デフォルト値は1 です。

  「Capture Interval」 [1～255フレーム]: 画像をキャプチャするフレーム間隔です。値を1（デフォルト値）に設定すると、カメラはすべてのフレームで顔をキャプチャします。

  「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。

  「Capture Times」: 制限および無制限に設定できます。制限値として設定した場合は、[0～100]に設定できます。設定されたエリアにとどまる間に顔がキャプチャされる時間を表します。

「Face Exposure」: チェックボックスをオンにし、顔露出を有効にします。

「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。値が高いほど、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。デフォルト値は 1 分です。

お知らせ: 顔露出が有効な場合は、WDR 機能が無効になっていること、および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です。検出された顔が、設定されたフィルタリング時間より短くシーンに留まっている場合、キャプチャされません。例えば、顔のフィルタリング時間を 5 秒に設定すると、顔が 5 秒間シーンにとどまっているときに、検出された顔がキャプチャされます。

お知らせ: フェイス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少なくなる可能性があります。

「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。この機能を有効にすると、無効な顔画像が取り込まれます。

「Restore Defaults」: 「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。

10.3.2 カウント

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。

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。

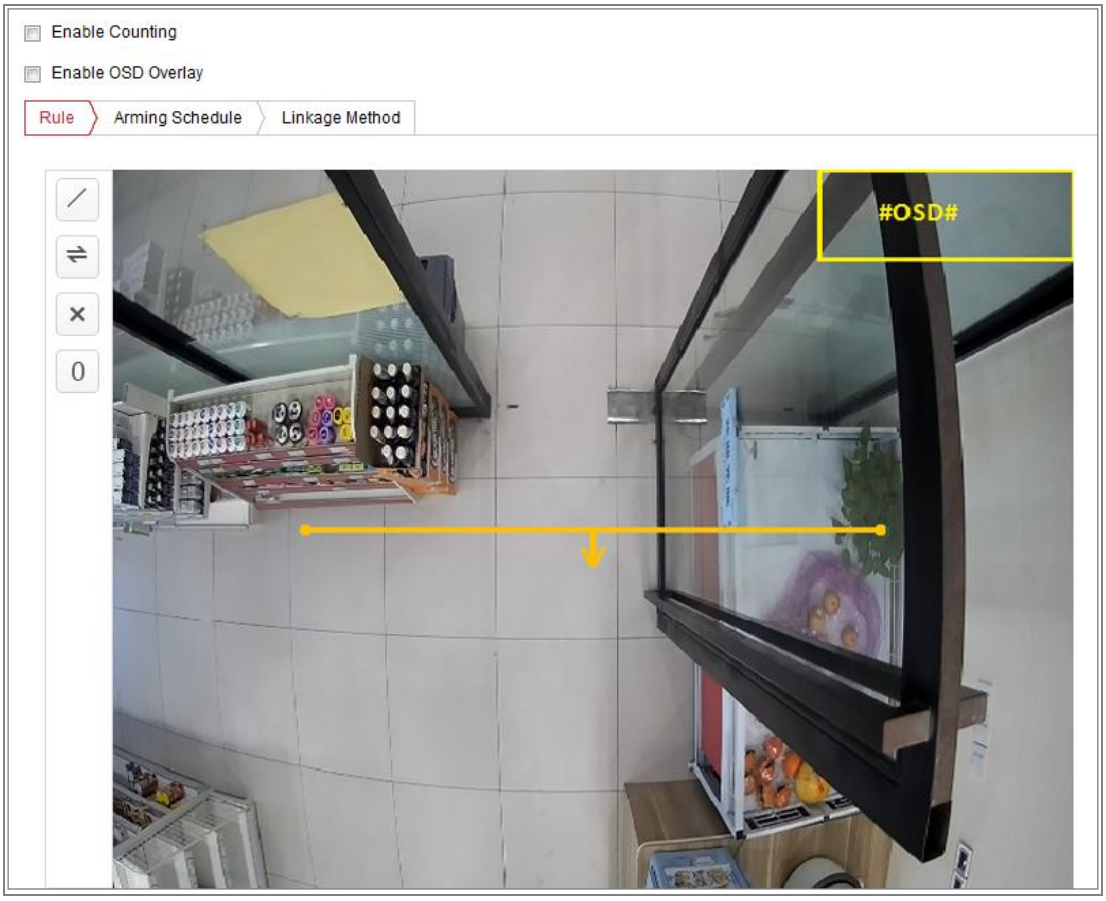


図 10-30 カウント設定

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

   検出ラインと呼ばれるオレンジ色のラインをライブビデオに設定し、ラインを出入りする物体を検出してカウントします。

   1) 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。

      お知らせ:

      - 検出ラインはカメラのすぐ下の位置に引いて、出入り口全体を覆うようにしてください。
      - 残りの人がいない位置に検知ラインを描きます。

2) 検出ラインをクリックしてドラッグし、位置を調整します。

3) 検出ラインの両端をクリックしてドラッグし、長さを調節します。

4) ✕をクリックして検出ラインを削除します。

5) ⇌をクリックして方向を変更します。

5. 0 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、タイムバー上でマウスをクリックしてドラッグし、アーミングスケジュールを設定します。
7. 「Linkage Method」をクリックし、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:

- 特定のモデルのみがこの機能をサポートしています。
- カウント統計はアプリケーションタブで計算されます。アプリケーションに移動して、カウント統計をチェックします。

10.3.3 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: 特定のモデルのみがこの機能をサポートしています。

- **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:

   - 道路交通の検知種別を切り換える場合は、カメラを再起動して新しい設定を有効にしてください。
   - 車両検出と H264+/H265+ は相互に排他条件になります。

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。
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、ラインの終了位置をクリック・ドラッグし、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. 「Region」と「Country/Region」を選択します。
7. 「Select Mode」ドロップダウンリストから、ナンバープレート情報のアップロードモードを選択します。
   - **「Entrance/Exit」:** 検出された車のナンバープレート情報は、車が検出エリアを通過し、出入り口で検出したときにアップロードされます。
   - **「City Street:」:** 検出された車両のナンバープレート情報は、車両が検出エリアを通過し、都市内の道で検出したときにアップロードされます。
   - **「Alarm Input」:** ナンバープレートをキャプチャし、認識アクションを開始します。

   お知らせ:

   - アラーム入力を選択すると、アラーム入力「A<-1」が自動的に車両検知に割り当てられ、そのアラームタイプは常に NO になります。
   - アラーム入力「A<-1」を使用して車両を検出すると、他の基本イベントは使用できません。
   - アラーム入力を選択して保存すると、設定済みの「A<-1」の連動方法は解除されます。

8. エリア設定を保存します。
9. ホワイトリスト、ブラックリストなどを個別に検出するためのアーミングスケジュールと連携方法を設定します。
   1) 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。
   2) マウスを各日の終わりに移動すると、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。
   3) 「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。
   4) 方向を選択します。「Direction」とは、車両の移動方向を意味します。選択された方向に移動している車両があれば、選択済の連携方法を行います。
      - 「Forward」: 車両がカメラに向かって移動します。
      - 「Reverse」: 車両がカメラから離れます。
   5) 連携方法を設定します。
      - 「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。
      - 「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」: アラーム情報が、設定済みの FTP サーバー、NAS、オンボードメモリカードにアップロードされます。
      - 「Trigger Alarm Output」: 受信した信号に対して特定のアクションを実行するように設定されたデバイスにアラーム信号が送信されます。
   6) 現在設定されているアーミングスケジュールと連携方法を他のリストにコピーする場合は、コピー先をクリックし、目的のリストをチェックします。
   7) リストの設定を保存します。

- **画像設定のアップロード**

手順:

1. 「Configuration」 > 「Road Traffic」 > 「Picture」を選択します。
2. 画質オプションボタンを選択し、画質値を調整します。
3. 画像サイズオプションボタンを選択し、サイズを入力します。
4. オーバーレイチェックボックスをオンにし、フォントの色と背景色を設定します。
5. チェックボックスをオンにすると、デバイス番号、キャプチャ時間、方向、プレート番号、カメラ情報、カメラ番号、有効性、車色、ブランドなど、テキストオーバーレイの情報を選択できます。上下 ボタンをクリックして、情報の順序を調整することもできます。
6. 撮影した画像のファイル名を設定します。
   - デフォルト名を使用するには、「Default」をクリックします。
   - 画像名をカスタマイズするには、「Custom」をクリックします。
     - チェックボックスにチェックを入れると、アラームタイプ、カメラ名、キャプチャ時間、プレート番号など、画像名の情報を選択できます。また、上下 ボタンをクリックして情報の順番を調整することもできます。
7. 「Save」をクリックし、設定を保存します。

- **ディスプレイのカメラ情報設定**

目的:

カメラ情報を設定できます。

手順:

1. 「Configuration」 > 「Road Traffic」 > 「Camera」を選択します。
2. デバイス番号、カメラ番号、カメラ情報を入力します。
3. 「Save」をクリックして、設定を有効にします。

- **ブラックリストとホワイトリストの設定**

目的:

必要に応じてブラックリストとホワイトリストをインポートおよびエクスポートし、リストの内容を確認できます。

- **ブラックリストとホワイトリストのインポート**

  1. 「Browse」をクリックして、PC ローカルディレクトリを開きます。
  2. ブラックリストとホワイトリストファイルを検索し、クリックして選択します。「Open」をクリックして確定します。

  お知らせ:

  - インポートするファイルは、カメラに必要なファイルテンプレートに対応している必要があります。空のブラックリストとホワイトリストファイルをカメラからテンプレートとしてエクスポートし、コンテンツに入力することを推奨します。
  - ファイルは".xls"フォーマットで、セルフォーマットは"Text"である必要があります。

  3. 「Import」をクリックして、選択したファイルをインポートします。

- **ブラックリストとホワイトリストのエクスポート**

  1. 「Export」をクリックして、PC のローカルディレクトリを開きます。
  2. PC のローカルディレクトリでディレクトリを選択します。
  3. 「Fine name」欄に名前を入力し、「Save」をクリックして保存します。

10.3.4 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 つのキューの変更ステータスを表示するレポートを生成します。

この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人物のキューイングを検出および計算し、アラームしきい値条件とアラームの両方が満たされるとアラームが発生します。

「Waiting Time Detection」: 検出エリアに入った各人の待ち時間を検出して計算し、アラームしきい値条件とアラーム出力の両方が満たされるとアラームが発生します。

「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) リージョンを追加します。最大 3 つのリージョンがサポートされます。

領域とは、検出がアクティブになっている定義済み領域のことです。

リージョンを描画する場合、ターゲットの有効なリージョン入力アクションは、そのリージョンに自分のヘッドとショルダー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 個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」: リージョンを選択し、リージョンの端をドラッグします。

「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場合は、リージョンの重複を避けてください。
- リージョンは、キューに必要なスペースと同じだけカバーする必要があります。

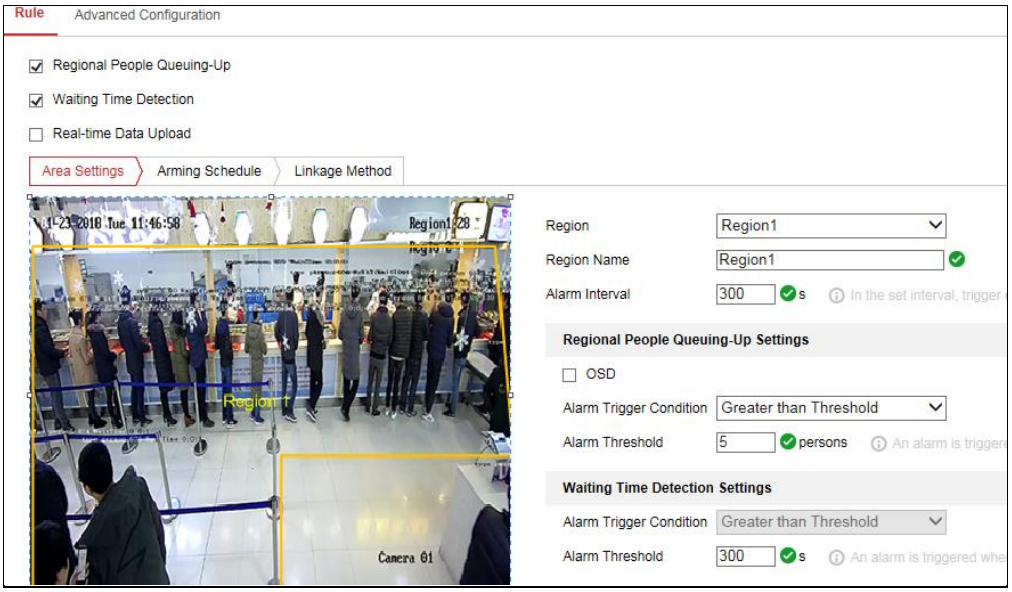


図 10-31 キュー管理ルールの設定

b) 追加したリージョンのパラメータを設定します。

b-1 リージョン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が 1 つだけ通知されます。

b-2 リージョンのキューイング設定を行います。

「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」: リージョン内の人数が設定したしきい値以上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 待ち時間検知の設定を行います。

「Alarm Trigger Condition」: リージョン内の人数が設定したしきい値以上、以下、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リージョンを設定します。最大 3 つのリージョンに対応しています。

2. アーミングスケジュール設定

   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。「10.1.1 モーション検出の設定」のタスク 2 を参照してください。

3. 連携方法

   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。「10.1.1 モーション検出の設定」のタスク 3 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ーを設定します。

   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。

10.3.5 ヘルメット検出

この機能を有効にすると、カメラは、設定された監視領域内の誰かがヘルメットを装着していないことを検出すると、アラームが発生します。

手順:

1. 「Configuration」 > 「Hard Hat Detection」を選択します。
2. 「Enable Hard Hat Detection」をチェックします。
3. 生成速度を設定します。検出領域に入る顔の目標生成速度を指します。値が大きいほど、生成が高速になります。
4. 「Draw Area」をクリックして、検出範囲を設定します。検出範囲内の誰かがヘルメットを装着していないことをカメラが検出すると、アラームが発生します。
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。
6. 「Linked Method」をクリックして連携方法を設定します。
7. 「Save」をクリックします。

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。

10.3.6 顔の比較とモデリング

顔写真ライブラリ

顔写真ライブラリを追加したり、ライブラリの顔写真を管理することができます。

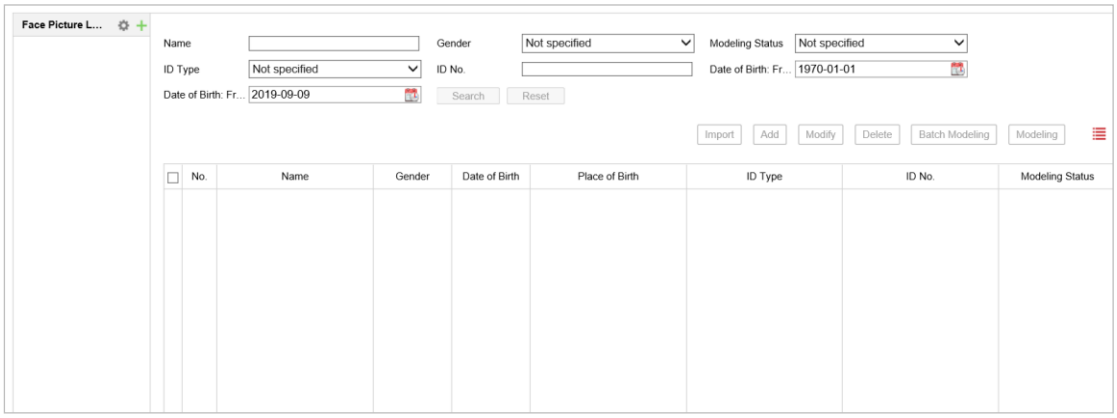


図 10-32 顔写真ライブラリ

- **顔写真ライブラリを追加、修正、削除します。**

手順:

1. ＋をクリックして顔写真ライブラリを追加します。
2. ライブラリ名、しきい値、コメントを入力します。

   「Threshold」: 顔の類似度が設定したしきい値を超えると、顔画像比較アラームがアップロードされます。
3. 「OK」をクリックします。
4. 顔写真ライブラリを変更するには、目的のライブラリを選択し、⚙をクリックして関連パラメータを変更します。
5. 顔写真ライブラリを削除するには、✕をクリックします。

- **ライブラリ内の顔写真を管理します。**

お知らせ:

サポートされるピクチャサイズは、ファイルあたり 300K 以下です。

手順:

1. 顔写真をライブラリに追加します。

   (1) 顔写真ライブラリを選択します。

   (2) 「Add」をクリックします。

(3) 写真をアップロードし、アップロードした顔の詳細情報を指定します。画像フォーマットは JPEG になります。

(4) 「OK」をクリックします。

2. 顔写真を一括で取り込みます。顔写真を一括して取り込むと、顔名として画像名が保存されます。その他の顔情報については、1 つずつ手動で変更する必要があります。

(1) 顔写真ライブラリを選択します。

(2) 「Import」をクリックします。

(3) 画像パスを選択します。

(4) 「OK」をクリックします。

3. 顔情報を修正します。

お知らせ:

修正中に顔写真は変更できません。

(1) 顔写真ライブラリを選択します。

(2) 対象の顔画像を選択します。検索機能を使用して、画像を見つけることができます。

(3) 「Modify」をクリックします。

(4) 詳細情報を編集します。

(5) 「OK」をクリックします。

4. モデリングおよびバッチモデリング。

各顔画像に対して顔モデルを構築・設定します。顔写真の比較を有効にするには、顔モデルが必須です。

「Modeling」: 1 つまたは複数の顔画像を選択し、「Modeling」をクリックします。

「Batch Modeling」: 顔画像ライブラリを選択し、「Batch Modeling」をクリックします。

5. ライブラリ内の顔を検索します。

(1) 名前や性別などの検索条件を入力します。

(2) 「Search」をクリックします。

顔画像比較

目的:

顔画像比較は、キャプチャした画像とライブラリ内の顔画像を比較し、比較結果を出力します。比較結果は、スケジュールと連携方法が設定されている場合に、特定のアクションを連動して発動することがあります。

検出された顔と顔画像ライブラリ内の顔の類似度が一定の閾値に達すると、比較結果と関連するアラーム情報がアップロードされます。

準備:

- 特定のカメラモデルでは、機能を表示するには、「Configuration」 > 「System」 > 「System Settings」 > 「VCA Resource」を選択し、「Face Capture」を有効にする必要があります。
- 最初にフェイスピクチャライブラリを作成し、フェイスピクチャを追加する必要があります。詳しい説明は「Face Picture Library」画面をご覧ください。

手順:

1. 「Configuration」 > 「Comparison and Modeling」 > 「Comparison and Modeling」を選択し、設定画面から「Face Picture Comparison」を選択します。
2. 「Enable Face Picture Comparison」チェックボックスをオンにします。
3. 顔比較のためにアップロードする情報を設定します。
4. 比較モードを選択します。
   - 「Best Comparison」: 顔ターゲットが検出エリアに留まっている場合、デバイスはターゲット顔を継続的にキャプチャして比較し、ターゲット顔がエリアから離れると、最適なスコアの顔画像と関連するアラーム情報をアップロードします。
   - 「Quick Comparison」: デバイスは、顔のグレーディングがキャプチャ用に設定された顔のグレーディングしきい値を超えると、ターゲット顔をキャプチャして比較します。

     「Face Grading Threshold for Capture」: 顔をキャプチャしてアップロードするかどうかを判断するデバイスの顔の等級しきい値です。

「Max. Capture Interval」: ターゲットが検出エリアにあるときの、2 つのキャプチャ間の最大間隔です。顔のグレーディングが設定したしきい値に達していなくても、最大インターバルに達すると撮影されます。

「Quick Setup Mode」: カスタム、フェイスアテンダンス、顔認識を選択できます。実際の使用シナリオに応じて選択します。カスタムモードでは、「Comparison Timeout」と「Comparison Times」を設定できます。

5. 顔写真ライブラリを選択します。
6. 顔比較のアーミングスケジュールを設定します。
7. 顔比較の連動動作を設定します。

お知らせ:

比較結果を表示するには、「Application」画面に移動します。

フェイスモデリング

目的:

顔モデリングは顔の比較の前に行う必要があります。

手順:

1. 設定ページに入り、フェイスモデリングを選択します。

   「Configuration」 > 「Comparison and Modeling」 > 「Face Comparison and Modeling」を選択し、「Face Modeling」設定画面を選択します。
2. 「Enable Face Modeling」チェックボックスをオンにします。
3. モデリングルールを設定します。
   - 「Enable Quick Capture」: この機能を有効にすると、デバイスは、「キャプチャ」に設定された顔の等級しきい値よりも高いスコアの顔を検出するとすぐに顔のモデリングを開始します。
   - 「Enable Quick Capture」: 顔をキャプチャしてアップロードするかどうかを判断するデバイスの顔の等級しきい値です。
   - 「Max. Capture Interval」: ターゲットが検出エリアにあるときの、2 つのキャプチャ間の最大間隔です。顔のグレーディングが設定したしきい値に達していなくても、最大インターバルに達すると撮影されます。

4. 顔モデリングのアーミングスケジュールを設定します。
5. 顔モデリングの連携方法を設定します。

10.3.7 マルチターゲット型検出

「Multi-Target-Type Detection」は、複数のタイプのターゲットのイメージを検出し、キャプチャ、アップロードする機能です。

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。

❖ **オーバーレイとキャプチャ**

「Display VCA info. on Stream」: ライブビューや再生では、赤いフレームがターゲットに表示されます。

アラーム画像に目標情報を表示:チェックボックスがチェックされている場合、アップロードされたアラーム画像にターゲット上にフレームがあります。

「Snapshot Settings」:

- 「Target Picture Settings」

1. ターゲットの画像サイズを選択します。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種類があります。「Custom」を選択すると、必要に応じて幅、ヘッドの高さ、ボディの高さをカスタマイズできます。
2. 画像の高さを設定するには、固定値をチェックします。

- 「Background Picture Settings」

1. ドロップダウンリストから「Picture Quality」と「Resolution」を選択します。
2. 「Background Upload」チェックボックスをオンにして、背景画像をアップロードします。

「Camera Information」:

撮影した画像に重ねることが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」:

撮影した画像に表示したい項目を確認したり、順番を変えたりできます。

❖ 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 つのシールド領域に対応しています。

手順:

1. をクリックしてシールド領域を描画するには、ライブビューウィンドウでエンドポイントを左クリックし、右クリックして領域の描画を終了します。

お知らせ:

- 多角形領域（4 ～10 辺）がサポートされています。
- をクリックして、描画した領域を削除します。
- ライブビューが停止している場合、シールド領域を描画する方法はありません。

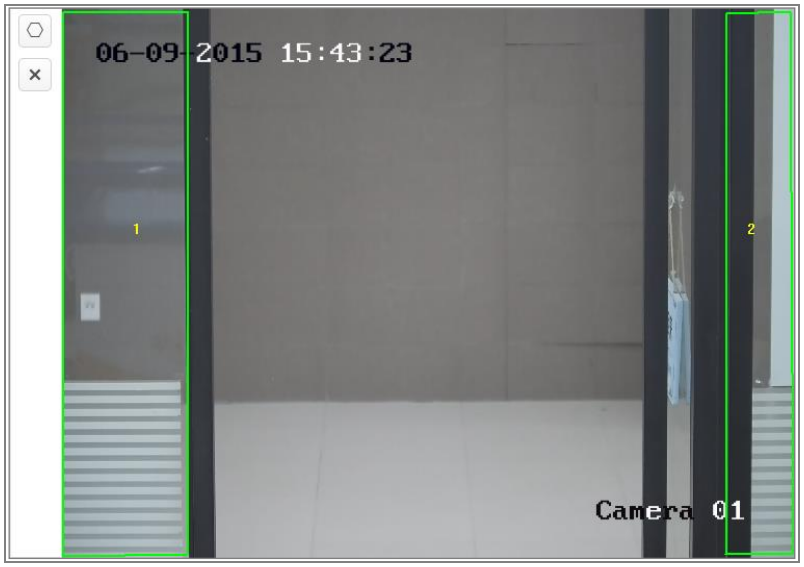


図 10-33 シールド領域の描画

2. 「Save」をクリックします。

❖ ルール

手順:

1. 顔キャプチャのルールを有効にするには、ルールをオンにします。
2. 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、描いた生徒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。

3. をクリックして、顔のキャプチャを有効にする検出領域を描画します。ライブビューウィンドウでエンドポイントを左クリックしてエリアを描画し、右クリックしてエリアの描画を終了します。

   お知らせ:

   - 多角形領域(4 ～10 辺)をサポートしています。
   - ライブビューが停止している場合、設定された領域を描画する方法はありません。

4. 「Save」をクリックします。
5. アーミングスケジュールタブをクリックし、各ルールのスケジュール時間を設定し、「Save」をクリックし、設定を保存します。
6. 「Alarm Linkage」をクリックし、各ルールに対応する連動方法の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。

❖ 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。

お知らせ: これらの機能は、モデルによって異なります。

図 10-34 詳細設定

「Detection Parameters」:

「Generation Speed」 [1～5]: ターゲットを識別する速度。値が大きいほど、ターゲットの認識が速くなります。設定値を最も低く設定し、最初から設定した領域に顔があった場合、その顔はキャプチャされません。壁ペイントやポスターの顔の情報ミス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感度。値が高いほど顔が認識しやすくなり、情報ミス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」: ベストショットが利用できます。

- 「Best Shot」: ターゲットが検出エリアから離れた後のベストショット。

  「Capture Threshold」: キャプチャとアラームを送信する顔の品質を設定します。値を大きくすると、キャプチャおよびアラーム通知するためには、より高い精度が必要になります。

「Face Exposure」: チェックボックスをオンにし、顔露出を有効にします。

「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。値が高いほど、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。デフォルト値は 1 分です。

お知らせ: 顔露出が有効な場合は、WDR 機能が無効になっていること、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です。検出された顔が、設定されたフィルタリング時間より短くシーンに留まっている場合、キャプチャされません。例えば、顔のフィルタリング時間を 5 秒に設定すると、顔が 5 秒間シーンにとどまっているときに、検出された顔がキャプチャされます。

お知らせ: フェイス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少なくなる可能性があります。

「Restore Defaults」:「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。

10.3.8 顔カウント

目的:

顔カウント機能では、重複した顔を削除し、特定の設定領域に出入りしたオブジェクトの数を計算できます。

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。

❖ **オーバーレイとキャプチャ**

「Display VCA info. on Stream 」: フレームは、ライブビューまたは再生時にターゲットに表示されます。

「Display Target info. on Alarm Picture」: チェックボックスがチェックされている場合、アップロードされたアラーム画像にターゲット上にフレームがあります。

「Snapshot Settings」:

- 「Target Picture Settings」

1. ターゲットの画像サイズを選択します。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種類があります。「Custom」を選択すると、必要に応じて幅、ヘッドの高さ、ボディの高さをカスタマイズできます。
2. 画像の高さを設定するには、固定値をチェックします。

- 「Background Picture Settings」

1. ドロップダウンリストから「Picture Quality」と「Resolution」を選択します。
2. 「Background Upload」チェックボックスをオンにし、背景画像をアップロードします。

「People Counting Overlay」:

1. ドロップダウンリストからフローオーバーレイを選択します。
2. ドロップダウンリストから「Daily Reset Time」を選択します。すぐにリセットする場合は、「Manual Reset」をクリックします。

「Camera Information」:

撮影した画像に重ねることが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」:

撮影した画像に表示したい項目を確認したり、順番を変えたりできます。

❖ アラーム設定

開始する前に、「Configuration」 > 「Face Picture Library」と選択し、最初に顔画像ライブラリのパラメータを設定します。

手順:

1. アラームのアップロードの種類を選択します。
2. 顔写真ライブラリを選択します。
3. 重複する人数カウントデータを削除するには、「People Counting Deduplication」をオンにします。
4. キャプチャした顔画像をアラーム情報に追加するには、「Upload Captured Face Image」をオンにします。
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。
6. 「Linkage Method」をクリックし、アラームの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。

❖ ルール

手順:

1. 「People Counting Deduplication Time」を設定します。
2. 最小瞳孔間距離を入力するか、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、描かれ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。
3. 最大瞳孔間距離を入力するか、  をクリックして最大瞳孔間距離を描画します。

4. をクリックして、検出エリアを描画します。ライブビューウィンドウでエンドポイントを左クリックしてエリアを描画し、右クリックしてエリアの描画を終了します。

   メモ: 多角形領域(4 ～10 辺)に対応しています。

5. をクリックして検出ラインを描きます。矢印は入力方向を示し、をクリックして方向を変更できます。
   - ターゲットが入力方向に沿ってカウント領域を横断し、検出ラインと交差する場合は、入力数としてカウントされます。
   - ターゲットが出口方向に沿ってカウント領域を通過し、検出ラインと交差する場合、出口番号としてカウントされます。

6. およびをクリックして、AおよびB領域を描画します。2つの領域が重ならないようにしてください。方向を変更するには、をクリックします。
   - ターゲットがA領域からB領域に入ると、入力番号としてカウントされます。
   - ターゲットがB領域からA領域に進入する場合、退出番号としてカウントされます。

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ます。
8. 「Linkage Method」をクリックし、チェックボックスをオンにして、アラーム入力の連動方法を選択します。
9. 「Save」をクリックし、設定を保存します。

❖ 詳細設定

実際の環境に応じて、以下のパラメータを設定します。

お知らせ: これらの機能は、モデルによって異なります。

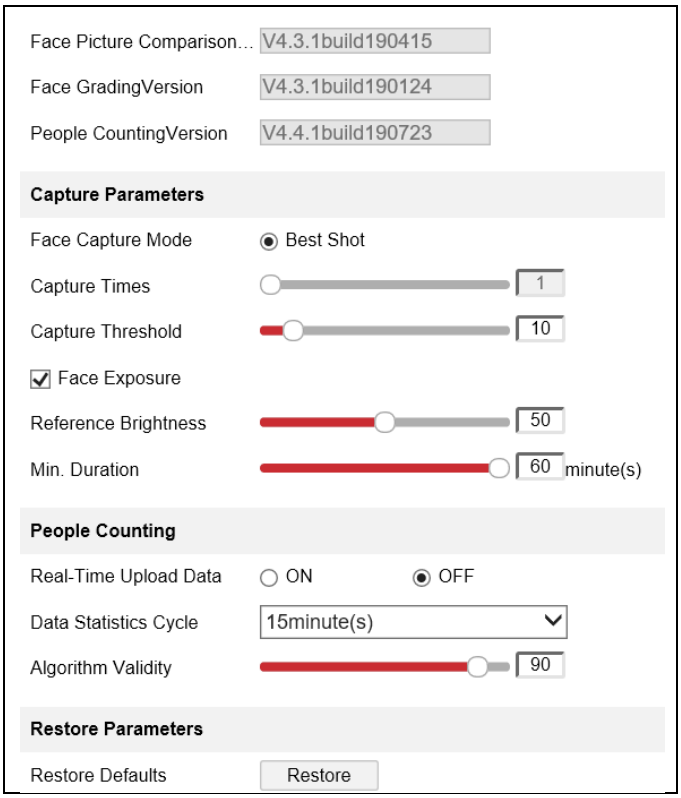


図 10-35 詳細設定

「Capture Parameters」:

「Face Capture Mode」: ベストショットが利用できます。

- 「Best Shot」: ターゲットが検出エリアを離れた後のベストショット。
- 「Capture Times」 [1～3]: 設定されたエリアにいる間に顔がキャプチャされるキャプチャ時間を表します。デフォルト値は1 です。
    - 「Capture Threshold」: キャプチャとアラーム通知する顔認識精度を示します。値を大きくすると、キャプチャおよびアラーム通知するためには、より高い精度が必要になります。

「Face Exposure」: チェックボックスをオンにし、顔露出を有効にします。

「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。値が高いほど、顔が明るくなります。

「Minimum Duration」 [1～60min]: カメラが顔を露出する最小の持続時間です。

お知らせ: 顔露出が有効な場合は、WDR 機能が無効になっていること、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。

「Real-Time Upload Data」: 有効にすると、データをカウントしているリアルタイムユーザーがプラットフォームにアップロードされます。

「Data Statistics Cycle」: 要件に応じて、ドロップダウンリストからデータ統計サイクルを選択します。

「Algorithm Validity」: 値が高いほど、ターゲットの検出が困難になりますが、検出精度は高くなります。

「Restore Defaults」: 「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。

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。

お知らせ: サポートされる機能は、モデルによって異なります。

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する方法を説明しています。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

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。

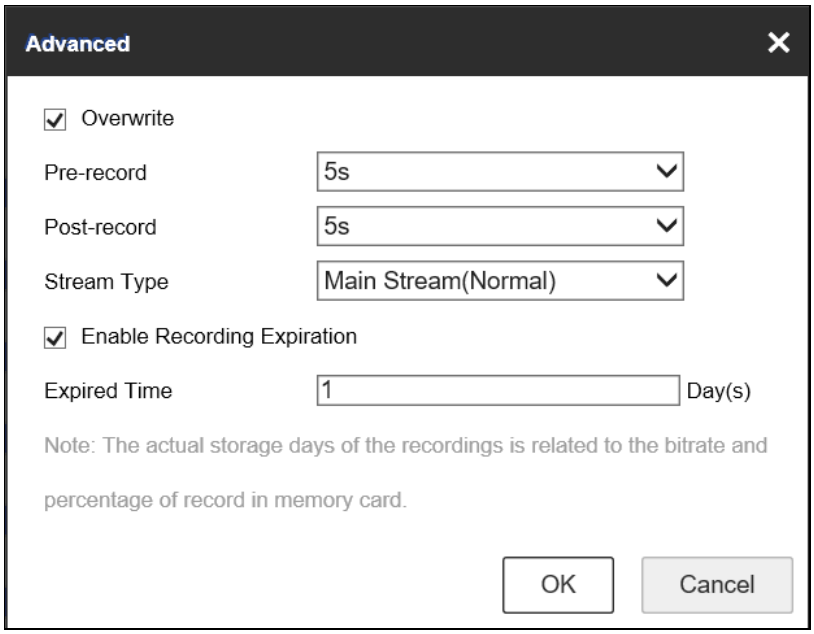


図 11-2 記録パラメータ

- 「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 に録画をセットし、事前録画時間が 5 秒に設定されている場合、カメラは 9:59:55 に録画を開始します。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。
- 「Expired Time」: 有効期限は 1 ～90 日で、7 日はデフォルトの有効期限です。1 月 2 日 8:00 に機能を有効にし、有効期限を 1 日に設定した場合、1 月 1 日 8:30 から 1 月 2 日 8:30 までの間に録画を確認できます。1 月 2 日 8:30 に録画を確認してください。1 月 1 日 8:30 までの録画は削除され、復元できません。

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、モーションとアラーム、イベントがあります。

- **連続録画**

  「Continuous」を選択すると、スケジュールの時刻に従って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、動体が検知されたときに録画を開始されます。

  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から連動方法でトリガ・チャンネルのチェックボックスにチェックを入れる必要があります。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録画を開始されます。

  録画スケジュールの設定に加えて、「Alarm Input Settings」の「Linkage Method」で「Trigger Channel」のチェックボックスにチェックを入れ、「Alarm Type」を設定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動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。

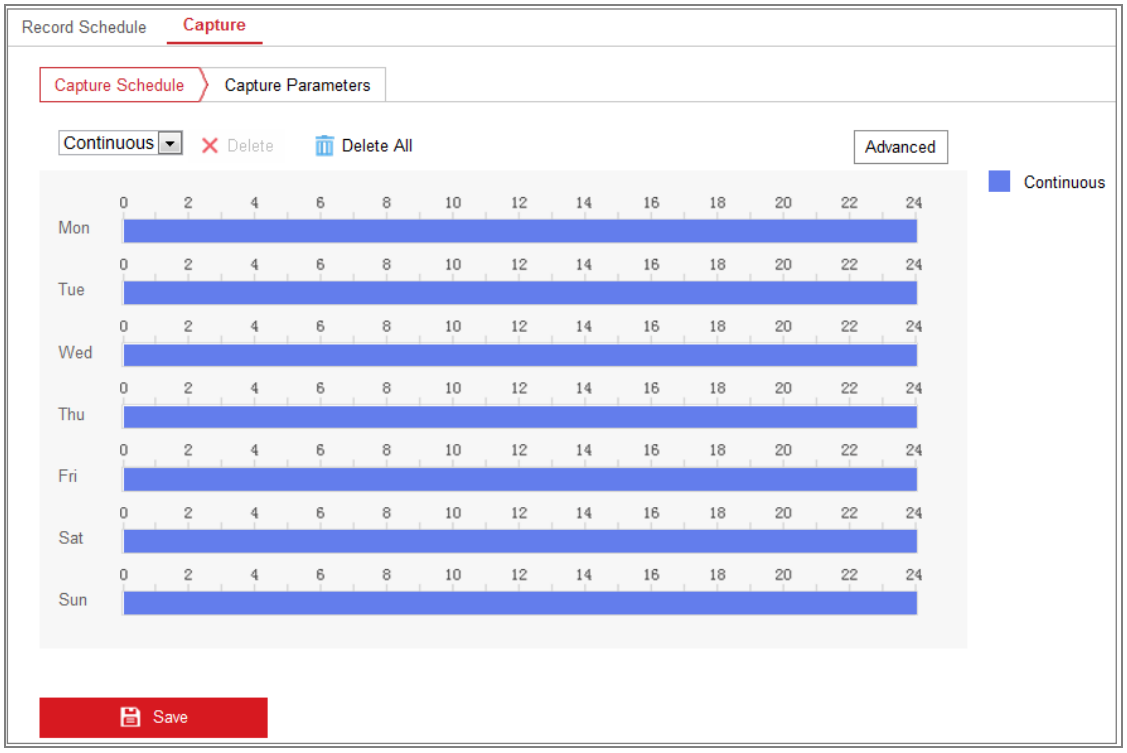


図 11-3 キャプチャスケジュール設定

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。

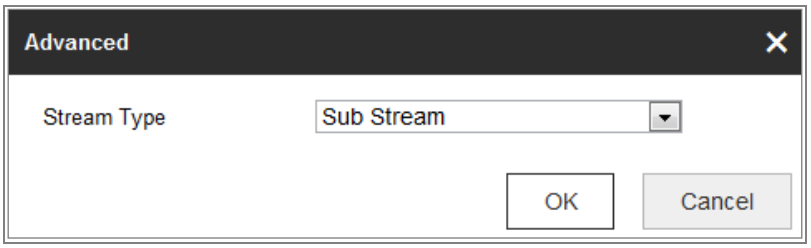


図 11-4 キャプチャスケジュールの詳細設定

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、イベント連動スナップショットを有効にします。

(4) 各イベントと連動するアクションの「Format」、「Resolution」、「Quality」、「Interval」、「Capture Number」を選択します。

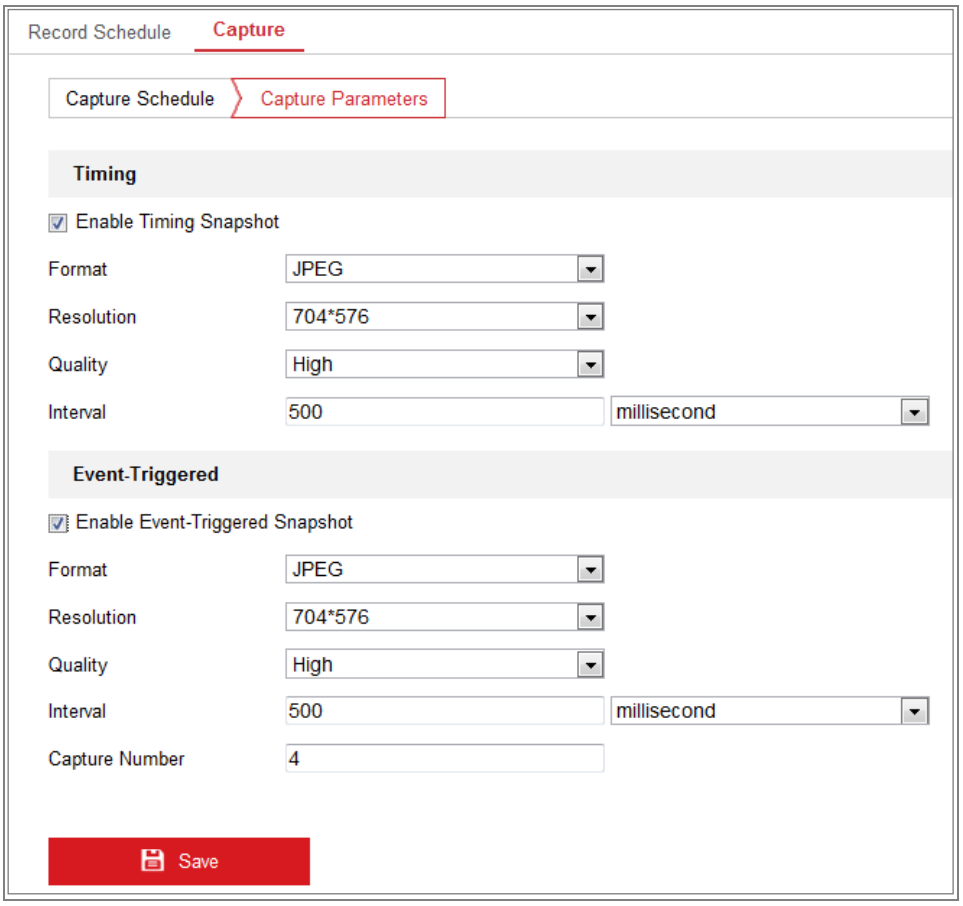


図 11-5 キャプチャパラメータの設定

6. 「Save」をクリックし、設定を保存します。

11.3 HDD 管理の設定

目的:

HDD 管理により、HDD の容量、空き容量、ステータス、暗号化ステータス、タイプ、フォーマットタイプ、プロパティと進捗状況などを表示できます。必要に応じて、選択した HDD をフォーマット、暗号化フォーマット、または検証できます。また、異なるファイルタイプにクォータを割り当てることもできます。

手順:

1. 「Configuration」 > 「Storage」 > 「Storage Management」 > 「HDD Management」を選択します。

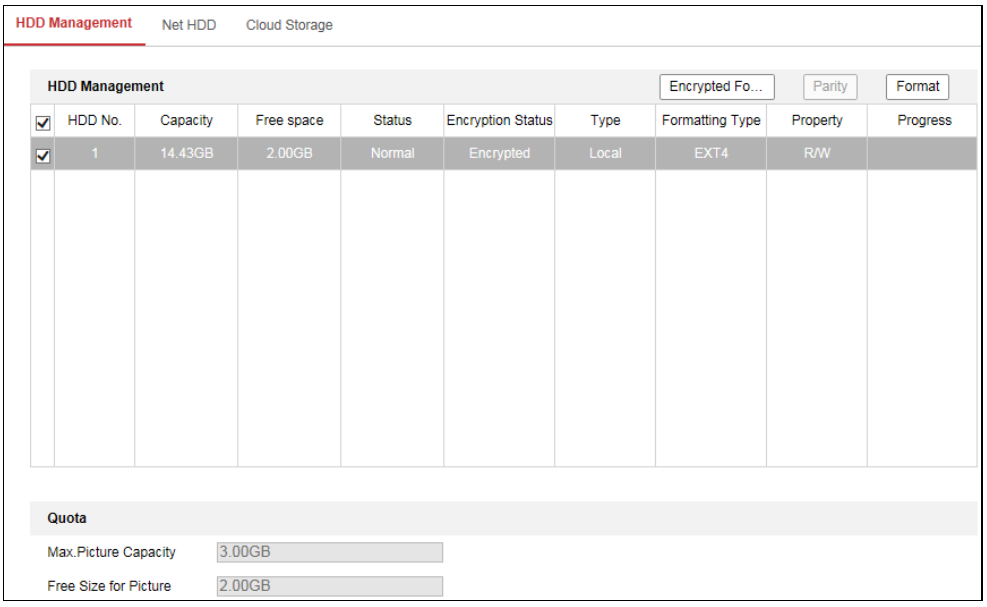


図 11-6 HDD 管理

2. 希望のディスクを選択し、必要に応じて操作します。

(1) ディスクのステータスには、「Uninitialized」と「Normal」が含まれます。

- ディスクのステータスが初期化されていない場合は、フォーマットをクリックしてディスクを初期化できます。初期化が完了すると、ディスクの状態は正常になります。その後、ディスクを通常どおりに使用できます。

(2) ディスクの暗号化ステータスには、「Unencrypted」、「Encrypted」、「Verification Failed」が含まれます。

- ディスクのステータスが「Unencrypted」の場合は、「Format」または「Encrypted Format」をクリックしてフォーマットできます。暗号化フォーマットには暗号化パスワードが必要です。
- 暗号化されたメモリーカードのステータスは、「Encrypted」または「Verification Failed」と表示されます。ディスクのステータスが「Verification Failed」の場合は、「Parity」をクリックして、検証用のパスワードを入力できます。検証に成功すると、ステータスは「Encrypted」に変わります。

3. **録画と画像のクォータを定義します。**

(1) 録画と画像のクォータの割合を入力します。

(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。

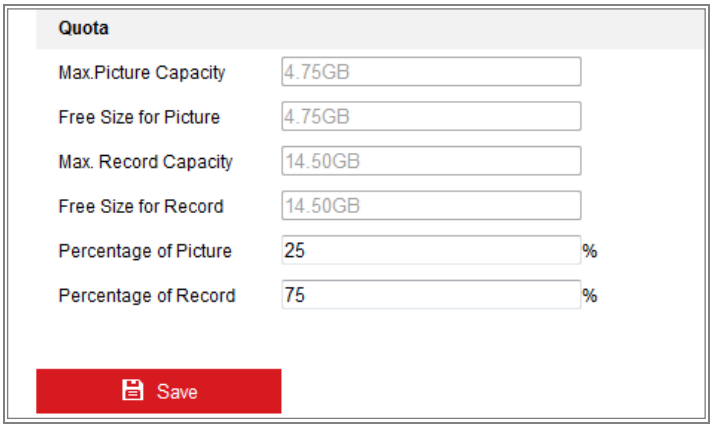


図 11-7 クォータ設定

11.4 Net 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. 「Configuration」>「Storage」>「Storage Management」>「Net HDD」を選択します。

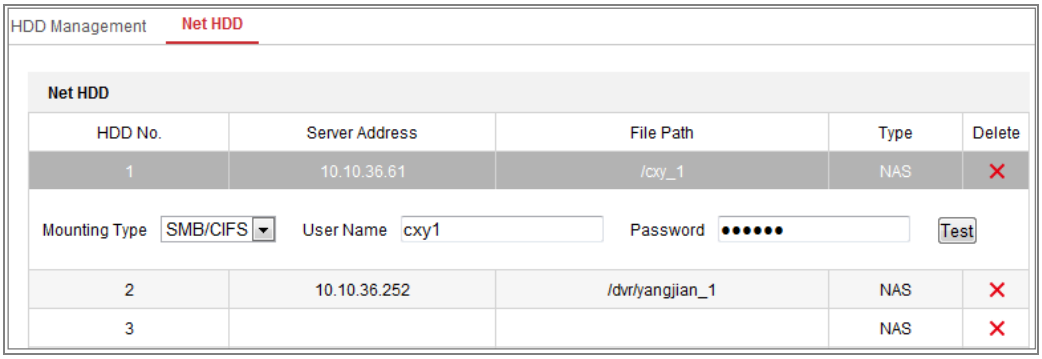


図 11-8 ネットワークディスクの追加

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. マウントタイプを選択します。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 取扱説明書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. 「Test」をクリックして、ネットワークディスクが使用可能かどうかを確認します。
5. 「Save」をクリックします。

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。

11.5 メモリカード検出

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、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。

手順:

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

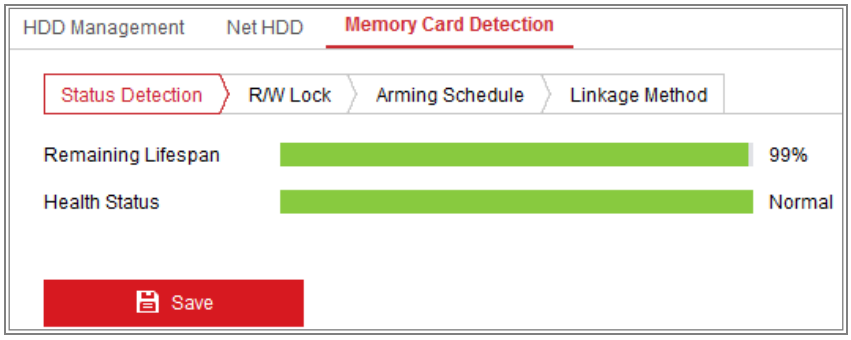


図 11-9 メモリカード検出

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

   「Remaining Lifespan」: 空き容量の割合を示します。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の影響を受けることがあります。空き容量が足りない場合は、メモリーカードを交換する必要があります。

   「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、および損傷の 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。

2. 「R/WLock」タブをクリックし、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。

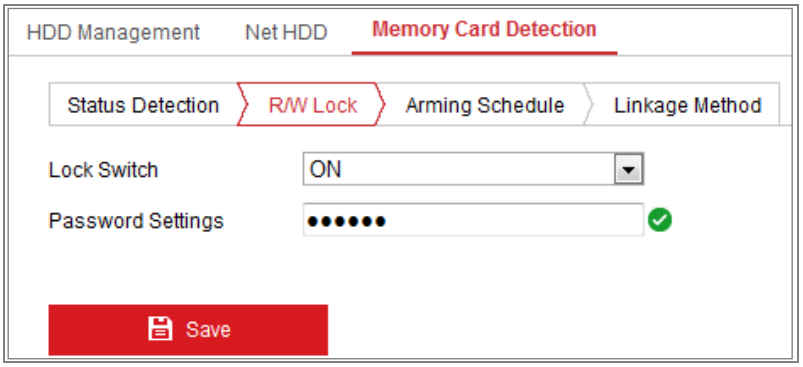


図 11-10R/W ロック設定

- 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) ロックされたメモリーカードをカメラで使用すると、自動的にロックが解除され、ユーザー側でロック解除の操作は必要ありません。

(2) 別のカメラでメモリーカード(ロック付き)を使用すると、「HDD Management」画面からメモリーカードのロックを手動で解除できます。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 Setting」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。

3. 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: モーション検出の準備スケジュールの設定」および「タスク 3: モーション検出の連携方法の設定」（10.1.1 モーション検出の設定）を参照してください。
4. 「Save」をクリックし、設定を保存します。

11.6 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。
- 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、同画面で確認できます。
4. 「Save」をクリックし、設定を保存します。

11.7クラウドストレージの設定

目的:

キャプチャした画像は、機能設定時に Cloud Storage に保存できます。

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。

手順:

1. 「Enable Cloud Storage」チェックボックスをオンにします。
2. プロトコルバージョンを選択します。
3. ストレージサーバーの IP アドレスとポートを入力します。
4. Cloud1.0 としてプロトコルバージョンを選択した場合は、ストレージサーバーの認証に使用するユーザー名、パスワード、および確認パスワードを入力します。

Cloud2.0 としてプロトコルバージョンを選択した場合は、アクセスキーとシークレットキーを入力します。

5. サーバー上のピクチャー・ストレージ・プール ID を入力します。
6. 「Test」をクリックして、クラウドストレージの設定をテストできます。
7. 「Save」をクリックします。

お知らせ:

ストレージ・サーバー・ポートの範囲は 2000 から 65535 で、ピクチャー・ストレージ・プール ID の範囲は 1 から 255 です。

第12章 再生

目的:

この章では、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を表示します。

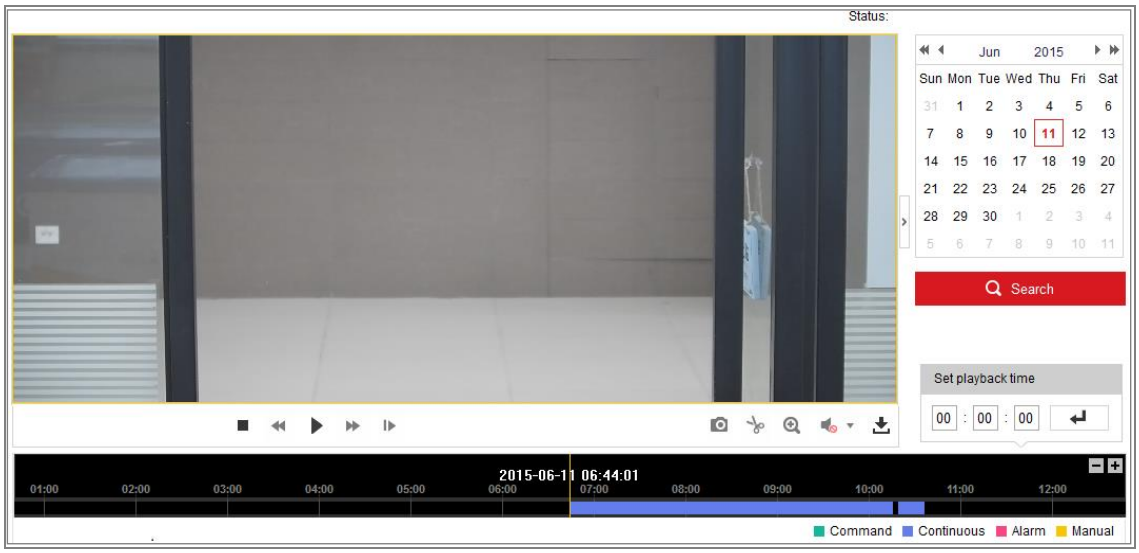


図 12-1 再生画面

2. 日付を選択し、「Search」をクリックします。

図 12-2 動画検索

3. ▶をクリックすると、この日付にあるビデオファイルが再生されます。

再生画面の下部にあるツールバーを使用して、再生操作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	操作	ボタン	操作
▶	再生	📷	画像のキャプチャ
⏸	一時停止	✂ / ✂	ビデオファイルの開始/停止
■	停止	🔊 / 🔇	ボリューム調整 ボリューム ON/OFF
⏪	巻戻し	⬇	ダウンロード
⏩	早送り	⏭	フレーム単位で再生
🔍 / 🔍	デジタルズームの有効化/無効化		

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、プログレスバーの−+をクリックしてズームアウト/インすることもできます。

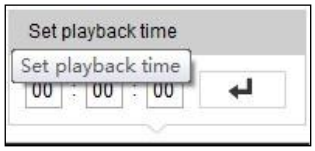


図 12-4 再生時間を設定する

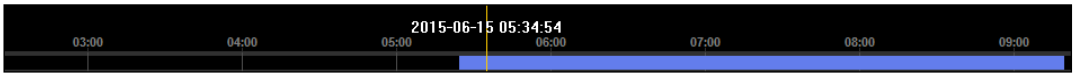


図 12-5 プログレスバー

プログレスバーのビデオのさまざまな色は、さまざまなビデオタイプを表しています。

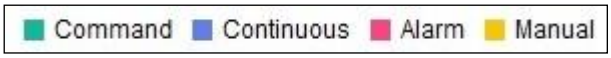


図 12-6 ビデオタイプ

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。

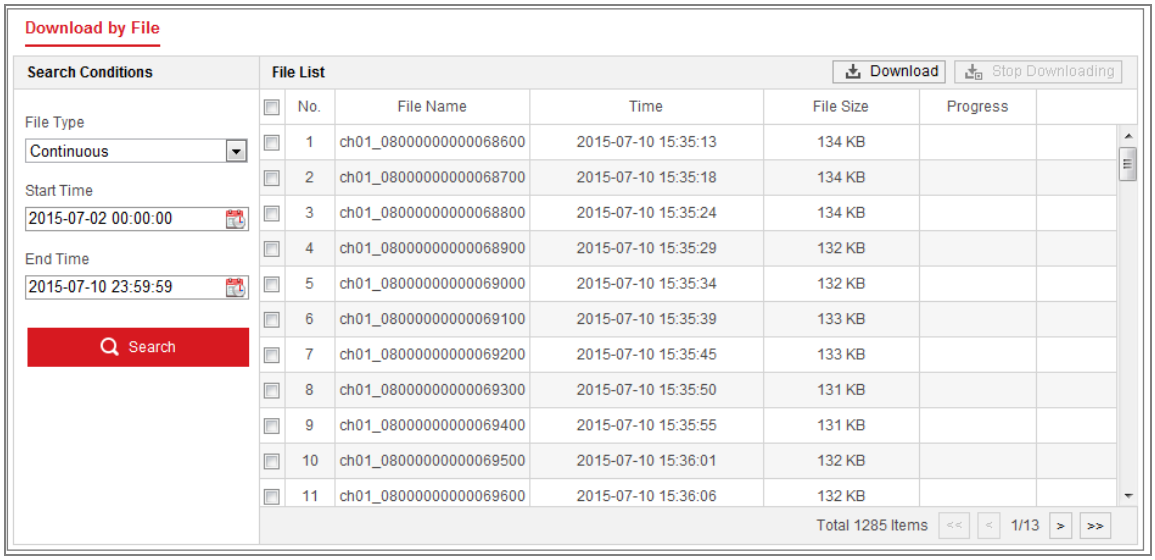


図 13-1 ピクチャー検索画面

手順:

1. ドロップダウンリストから「File Type」を選択します。
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にチェックを入れ、「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: 一度に表示できる画像は 4000 枚までです。

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: 特定のモデルのみがこの機能をサポートしています。

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。

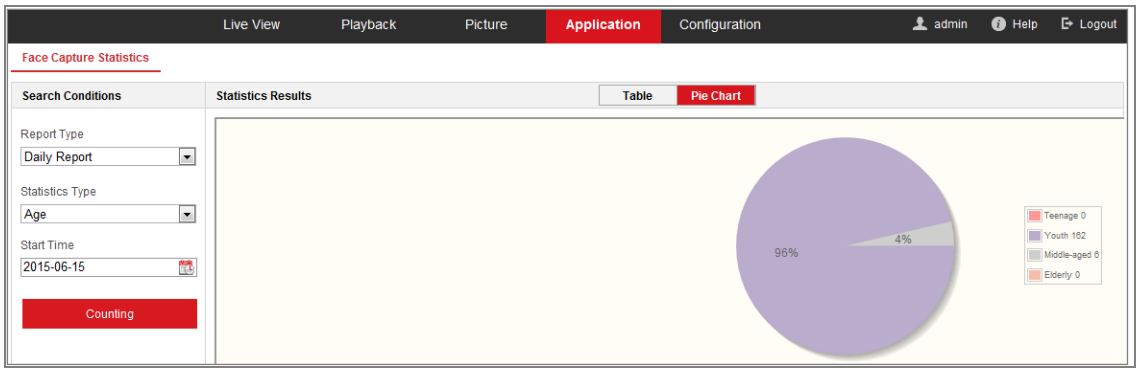


図 14-1 アプリケーション画面

手順:

1. レポートタイプを選択します。日報、週報、月報、年報から選択できます。
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、統計結果エリアに表示されます。「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、年報から選択できます。
   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、統計結果エリアに表示されます。「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。

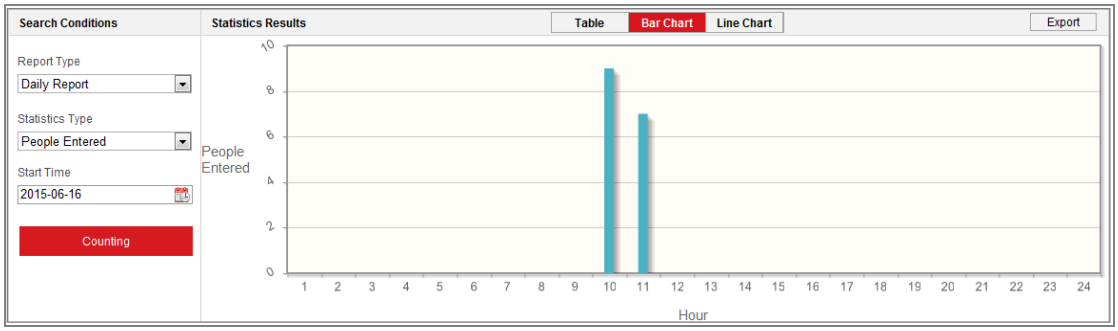


図 14-2 人数カウント

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、年報から選択できます。
   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。進入者、退出者の選択可能です。
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、「Table」、「Bar Chart」、「Line Chart」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。

14.4 顔画像比較統計

目的:

顔画像比較結果を検索・出力します。比較結果を検索する前に、「Face Picture Library」、「Face Comparison and Modeling」を設定する必要があります。

手順:

1. 検索条件を入力します。
2. 「Counting」をクリックします。「Face Picture Comparison Statistics」部に結果が表示されます。
3. アップロードした顔画像をダブルクリックすると、顔の比較結果が表示されます。

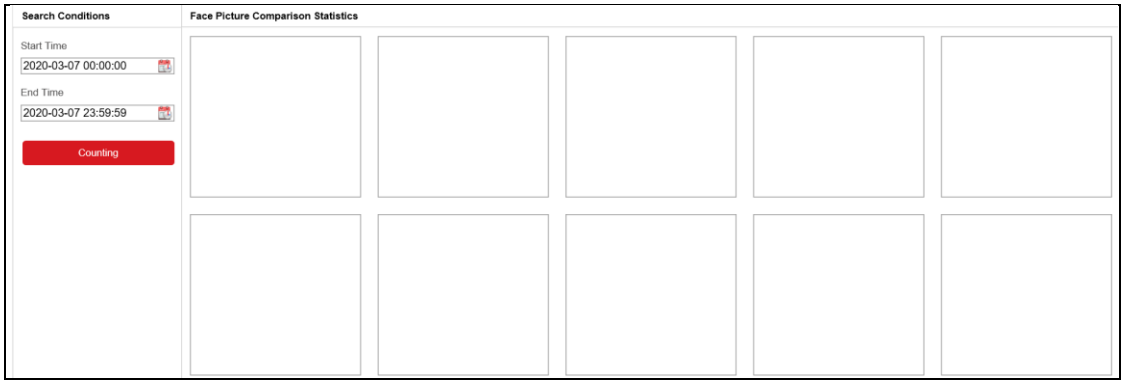


図 14-3 顔画像比較統計

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分析およびレポート出力をサポートします。

一般的なデータ分析

- 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**」: 異なる地域の人数をキューイングアップして比較します。

   a) 1 つまたは複数のリージョンをチェックします。

   b) 待ち時間の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。

   例えば、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。

   b) 待ち時間のレベルを設定します。希望の時間範囲チェックボックスと入力値をチェックします。

   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 キューステータス分析

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。

   ここでのキューの長さは、リージョン内の人数を意味します。

   例えば、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」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 ロ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。

第15章 スマートディスプレイ

目的:

スマート機能中に撮影した画像を表示することができます。

お知らせ: この機能は、特定のカメラモデルでのみサポートされます。

手順:

1. メニューバーの「Smart Display」をクリックします。
2. をクリックし、レイアウトを設定します。

   - **レイアウト**

     レイアウト内の表示内容を確認できます。

   - **検出機能**

     選択した検出対象地物をプレビューすることができます。

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。

● アクティブデバイスのオンライン検索

♦ 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。

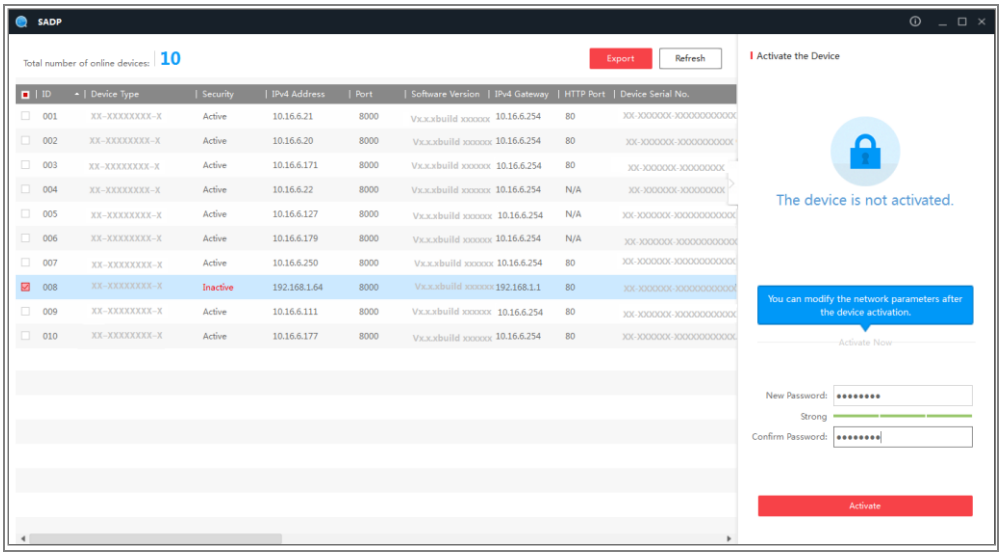


図 A.1.1 オンラインデバイスの検索

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。

NOTE 各列見出しの▲または▼をクリックまたはクリックすると、情報を並べ替えることができます。▶をクリックすると、デバイステーブルが展開され、右側のネットワークパラメータパネルが非表示になります。◀をクリックすると、ネットワークパラメータパネルが表示されます。

● 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。*

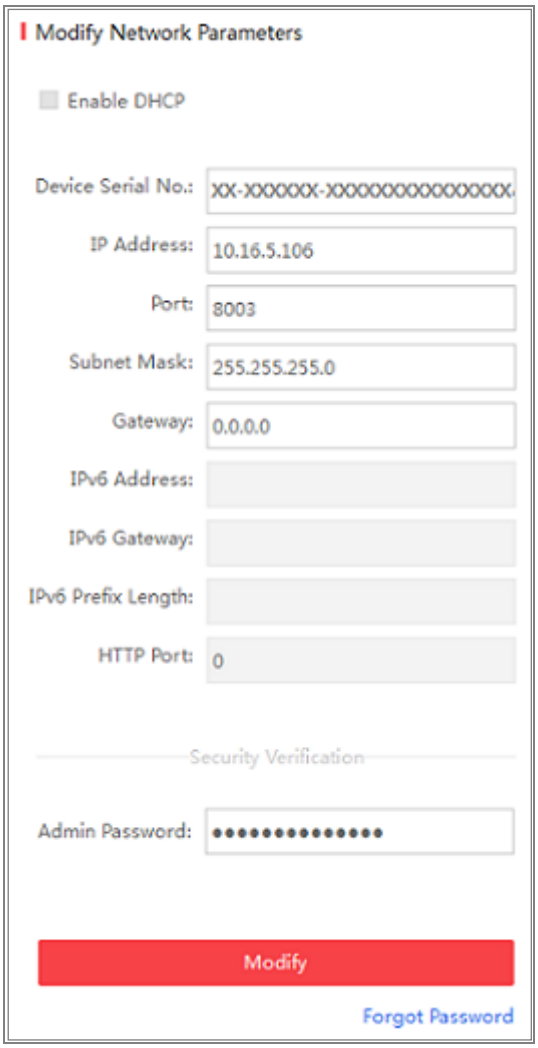


図 A.1.2 ネットワークパラメータの変更

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、ルータのモデルによって異なります。

手順:

1. 以下のように、「WAN Connection Type」を選択します。

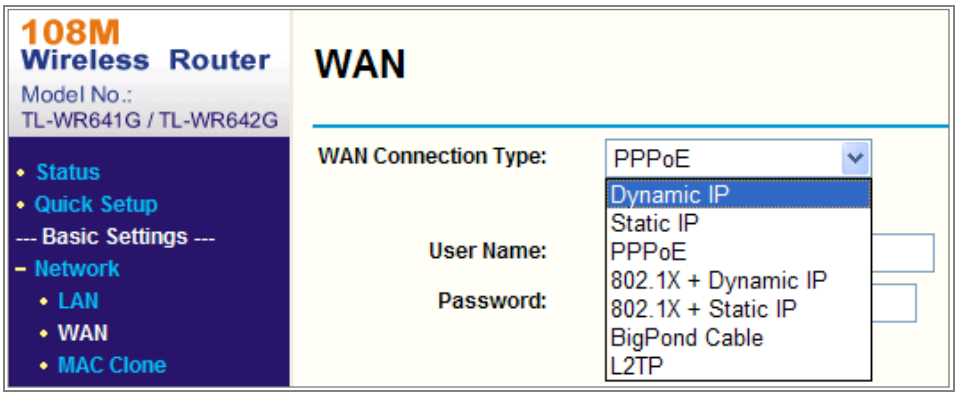


図 A.2.1 WAN 接続タイプの選択

2. IP アドレスやサブネットマスクの設定など、ルータの LAN パラメータを以下のように設定します。

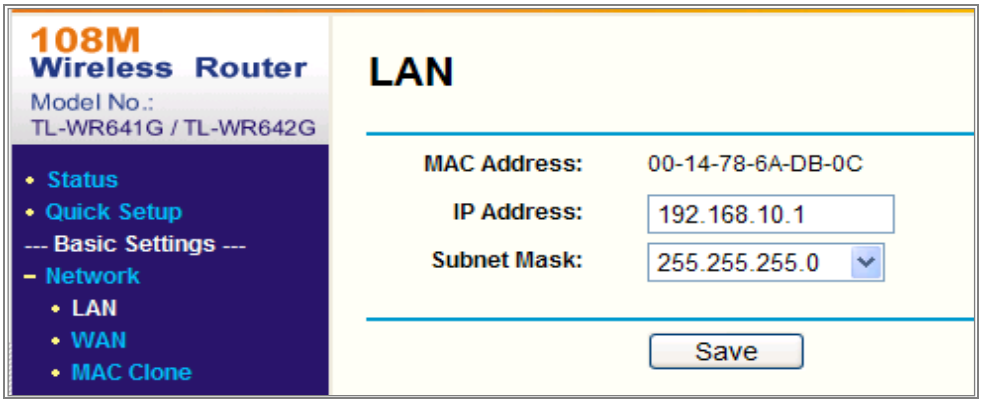


図 A.2.2 LAN パラメータの設定

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、および 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. 前述の設定では、ネットワークカメラのポート 80、8000、554、8200 を 192.168.1.23 にマッピングします。
2. ネットワークカメラのポート 81、8001、555、8201 を 192.168.1.24 にマッピングします。
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。

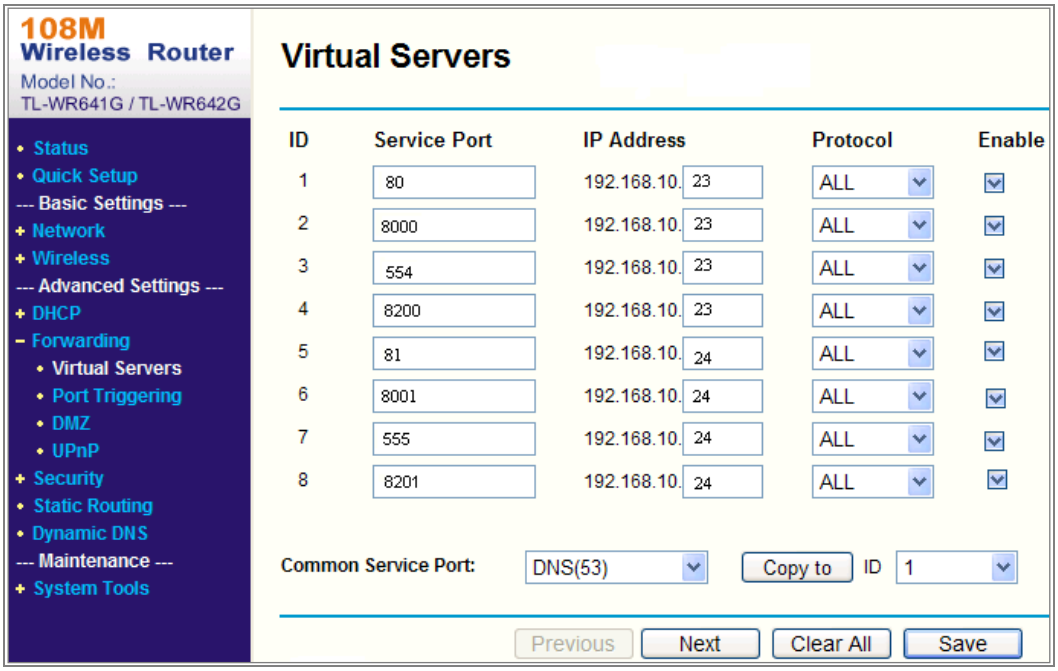


図 A.2.3 ポートマッピング

お知らせ: ネットワークカメラのポートは、他のポートとコンフリクトすることはできません。例えば、ルータの Web 管理ポートの一部は 80 です。カメラポートが管理ポートと同じ場合は変更します。

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)