ネットワークカメラ

ユーザーマニュアル

映像製品の使用に関する取り組み

このたびは、Hikvision製品をお選びいただきありがとうございます。

テクノロジーは私たちの生活のあらゆる場面に影響を与えます。ハイテク企業である当社は、テクノロジーがビジネスの効率や生活の質の向上に果たす役割をますます認識すると同時に、その不適切な使用による潜在的な弊害にも問題があると考えています。例えば、ビデオ製品は、リアルで完全でクリアな映像を記録します。これにより、思い出やリアルタイムの事実の保存に高い価値を提供します。ただし、映像データの不適切な配信、利用、加工が行われた場合、第三者の正当な権利や利益を侵害する可能性もあります。Hikvisionは、「Technology for the Good」の理念のもと、映像技術や映像製品のエンドユーザーの皆様には、より良い社会を共に創るために、適用されるすべての法律や規制、倫理的慣習を遵守していただきたいと考えています。

以下の取り組みをよくお読みください。

- 誰もがプライバシーに対する合理的な期待を抱いており、ビデオ製品の設置はこの合理的な期待に相反するものであってはなりません。従って、公共の場にビデオ製品を設置する場合は、合理的かつ効果的な方法で注意喚起を行い、監視範囲を明確にする必要があります。公共の場以外のエリアについては、映像製品を設置する際に、関係者の同意を得た上で映像製品を設置すること、可視性の高い映像製品を導入しないことなど、第三者の権利と利益が評価されるものとします。
- ビデオ製品の使用目的は、特定の時間と空間において、また特定の条件下での実際の活動を記録することです。従って、ユーザーは第三者の肖像権、プライバシーその他の正当な権利を侵害することのないよう、まずそのような特定の範囲の中で自己の権利を合理的に定めるものとします。
- ビデオ製品の使用中には、大量の生体データ（顔画像など）を含む、実際の場面に由来するビデオ画像データが生成され続け、そのデータはさらに応用されたり、再加工されます。ビデオ製品自体は、撮影した画像だけでデータの使い方の善悪の判断はできません。データ利用の結果は、データ管理者の利用方法と利用目的によって異なります。従って、データ管理者は、適用されるすべての法令およびその他の規範的要件を遵守するだけでなく、国際規範、社会道徳、善良な風俗およびその他の非強制的要件をも尊重し、個人のプライバシー、肖像権およびその他の権利および利益を尊重しなければなりません。
- 映像製品から継続的に発生する映像データを処理する際には、様々な関係者の権利や価値観、その他の要望を常に考慮する必要があります。この点で、製品のセキュリティとデータのセキュリティは極めて重要です。従って、エンドユーザーおよびデータ管理者は、データのセキュリティを確保し、データの漏洩、不適切な開示、不適切な使用を避けるために、アクセス制御の設定、ビデオ製品を接続する適切なネットワーク環境（インターネットまたはイントラネット）の選択、ネットワークセキュリティの確立と継続的な最適化など、あらゆる合理性と必要な措置を行うものとします。
- ビデオ製品は、これまで世界中の社会保障の向上に大きく貢献してきましたが、今後は、より多くの社会生活の場面で積極的な役割を果たすと考えます。ビデオ製品の人権侵害や犯罪行為につながる悪用は、技術革新や製品開発の本来の趣旨に反します。従って、各ユーザーはすべての製品が適切かつ合理的な方法で誠実に使用されることを確かなものにするため、その製品アプリケーションの評価追跡の仕組みを確立する必要があります。

法的情報

このマニュアルについて

このユーザーマニュアルには、本製品の使用および管理方法に関する説明が記載されています。以下、写真、図表、画像、その他すべての情報は、説明および解説のためのものです。本書に記載されている内容は、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ことがあります。本マニュアルの最新版は、Hikvisionのウェブサイトからご覧ください。(***https://www.hikvision.com/***)
本製品をサポートする訓練を受けた専門家の指導と支援を受けながら、本マニュアルを使用してください。

商標について

HIKVISION およびその他のHikvisionの商標およびロゴは、さまざまな管轄区域におけるHikvisionの財産です。
その他、記載されている商標およびロゴは、それぞれの所有者の財産です。

免責事項

適用される法律が許す最大限の範囲において、本マニュアルおよび記載された製品、そのハードウェア、ソフトウェア、ファームウェアは、「現状のまま」かつ「すべての欠陥および誤りを含む」状態で提供されています。Hikvisionは、商品性、満足のいく品質、特定目的への適合性を含むがこれに限定されない、明示または黙示の保証を一切行いません。本製品の使用は、お客様ご自身の責任において行われるものとします。Hikvisionがそのような損害や損失の可能性を知らされていたとしても、本製品の使用に関連し、特に事業利益の損失、事業の中断、またはデータの損失、システムの破損、文書の損失に対する損害など、契約違反、不法行為（過失を含む）、製品責任、またはその他のいずれに基づいても、いかなる特別、必然、付随的、間接損害についても、Hikvisionがお客様に責任を負うことはないものとします。
お客様は、インターネットの性質上、固有のセキュリティリスクがあることを認め、Hikvisionはサイバー攻撃、ハッカー攻撃、ウイルス感染、またはその他のインターネットセキュリティリスクに起因する異常動作、プライバシー漏洩またはその他の損害について一切の責任を負いません。ただし、Hikvisionは必要に応じて適時に技術サポートを提供します。
お客様は、本製品をすべての適用法に従って使用することに同意し、お客様の使用が適用法に適合していることを確認する責任を負うものとします。特に、お客様は、パブリシティ権、知的財産権、データ保護およびその他のプライバシー権を含むがこれらに限定されない第三者の権利を侵害しない方法で本製品を使用する責任を負うものとします。お客様は、本製品を、大量破壊兵器の開発または製造、化学兵器または生物兵器の開発または製造、核爆発物または安全でない核燃料サイクルに関連する活動、あるいは人権侵害の支援を含む、禁止された最終用途に使用してはならないものとします。
本書と適用される法律の間に矛盾がある場合、後者が優先されます。

記号について

本書で使用する記号は、次のように定義されています。

シンボルマーク	説明
危険	この表示を無視して誤った取り扱いをすると、人が死亡または重傷を負う可能性が想定される状況を示しています。
注意	この表示を無視して誤った取り扱いをすると、機器の損傷、データの損失、パフォーマンスの低下、または予期しない結果につながる可能性があり、潜在的に危険な状況を示します。
メモ	本文の重要なポイントを強調または補足するための追加情報を提供します。

安全上のご注意

この取扱説明書は、使用者が製品を正しく使用し、危険や財産上の損失がないようにするためのものです。

法規制について

- 本機は、地域の法律、電気安全規則、火災予防規則を遵守して使用する必要があります。

電気

- 本製品の使用にあたっては、国や地域の電気安全に関する規制を厳守してください。
- 機器に水滴や水がかからないようにしてください。また、花瓶など、液体の入った物を本機の上に置かないでください。
- 山頂、鉄塔、森林などの特殊な条件下では、本機の入口開口部にサージサプレッサを設けてください。
- 注意：火災の危険を減らすため、同じ種類と定格のヒューズのみに交換してください。
- 本機は必ず接地されたコンセントに接続してください。
- 容易にアクセスできる適切な切断装置を機器の外部に組み込む必要があります。
- 建物の仕様を超えない範囲で、適切な過電流保護装置を機器の外部に組み込む必要があります。
- 建物の電気設備には、全極型主電源スイッチを組み込む必要があります。
- AC電源に接続するための端子が正しく配線されていることを確認してください。
- IT配電システムへの接続を前提に設計されており、必要に応じて変更されています。

電池

- 電池を飲み込まないでください。化学物質による火傷の危険性:
- 本機には、コイン/ボタン電池が使用されています。電池を飲み込むと、わずか2時間で体内に重度の火傷を負い、死に至る可能性があります。
- 新しい電池や使用済みの電池は、お子様の手の届かないところに保管してください。
- 電池ボックスが確実に閉まらない場合は、使用を中止し、お子様の手の届かないところに保管してください。
- 電池を飲み込んだり、体の中に入れたりした可能性がある場合は、直ちに医師の診断を受けてください。
- 注意：異なる種類の電池と交換した場合、爆発する危険性があります。使用済みの電池は、説明書に従って廃棄してください。
- 異なる種類の電池と交換すると、安全装置が無効になることがあります（例：一部のリチウム電池の場合）。
- バッテリーを火や高温のオーブンに入れたり、機械的に押しつぶしたり、切断したりすると、爆発する恐れがあります。
- 爆発や引火性液体・気体の漏洩の恐れがあるため、極端に高温の場所に電池を放置しないでください。
- 電池を極端に低い気圧の場所に置くと、爆発したり、可燃性の液体やガスが漏れたりすることがありますのでご注意ください。
- +は直流電流を使用する、あるいは直流電流を発生する機器のプラス端子を示します。
  -は直流電流を使用する、あるいは直流電流を発生する機器のマイナス端子を示します。

火災予防

- ろうそくなどの火を機器の上に置かないでください。
- 機器のシリアルポートは、デバッグのみに使用されます。

高温表面対策

- 

注意：熱い表面部品の取り扱い時に火傷をするおそれがあります。電源を切り30分待ってから、部品を扱ってください。このステッカーが貼られた部品は熱くなる可能性があり、不注意で触れないよう注意喚起すためのものです。このステッカーが貼られたデバイスは、アクセスが制限された場所に設置されることを想定しており、作業は専門業者またはその場所に適用される制限の理由と注意事項についての指示を受けたユーザーによってのみ可能です。

設置

- このマニュアルの指示に従い、本機を設置してください。
- けがをしないように、この機器は設置説明書に従って壁またはラックにしっかりと固定する必要があります。
- 本機を不安定な場所には絶対に設置しないでください。機器が落下して、重大な人身事故や死亡事故を引き起こす可能性があります。

電源

- 入力電圧は、IEC60950-1規格に準拠する必要があります。SELV（Safety Extra Low Voltage）とLimited Power Sourceのことです。詳細な情報については、該当するドキュメントを参照してください。
- 電源はIEC 60950-1またはIEC 62368-1規格に準拠した限定電源またはPS2の要件を満たす必要があります。
- 過負荷によるオーバーヒートや火災を防ぐため、1つの電源アダプターに複数の機器を接続しないでください。
- プラグがコンセントに正しく接続されていることを確認してください。

白色光イルミネーター（対応する場合）

- 本製品から放射される光は危険な可能性があります。
- 動作中の光源を凝視しないでください。目に有害な場合があります。
- カメラの組み立て、設置、メンテナンスの際は、適切な目の保護具を着用するか、白色光を点灯させないでください。

輸送について

- 輸送中は、元の梱包材または類似の梱包材で保管してください。

システムのセキュリティ

- パスワードとセキュリティの設定は、設置者とユーザーの責任で行ってください。

メンテナンス

- 本機が正常に動作しない場合は、お買い上げの販売店または最寄りのサービスセンターまでご連絡ください。
- 無断での修理やメンテナンスによる不具合については、当社は一切の責任を負いません。
- 一部のデバイス部品（電解コンデンサなど）は定期的に交換してください。耐用年数が異なるので、定期的な点検をお勧めします。詳しくは販売店にお問い合わせください。

クリーニング

- 本機のカバーの内側と外側を拭くときは、柔らかい乾いた布を使用してください。アルカリ性の洗剤は使用しないでください。

使用する環境

- レーザー機器を使用するときは、機器のレンズにレーザー光線が当たらないようにしてください。燃え尽きる可能性があります。
- 電磁波の多い場所やほこりの多い場所には置かないでください。
- 屋内専用機の場合は、乾燥した換気のよい場所に設置してください。
- 太陽などの明るい光にレンズを向けないでください。
- 動作環境が本機の要求を満たしていることを確認してください。動作温度は-30 ℃～60 ℃、動作湿度は95%以下（結露しないこと）です。
- 極端に高温、低温、埃や湿気の多い場所に置いたり、強い電磁波にさらさないようにしてください。

緊急時

- 万一本機から煙やにおい、異音がしたらすぐに電源を切り、電源ケーブルを抜いて、サービスセンターへご連絡ください。

時刻同期

- ローカルタイムとネットワークタイムが同期していない場合、初回アクセス時に本機の時刻を手動で設定してください。Webブラウザ/クライアントソフトウェアでデバイスにアクセスし、時間設定のインターフェースに移動します。

反射

- 本機のレンズの近くに反射面がないことを確認してください。本機からの赤外光がレンズに反射して映り込むことがあります。

目次

第 1 章 システム要件

お使いのパソコンが本機に正しくアクセスし、操作できる要件を満たしている必要があります。

オペレーティングシステム	Microsoft Windows XP SP1以上のバージョン
CPU	2.0GHz以上
RAM	1G以上
ディスプレイ解像度	1024×768以上
Webブラウザ	Internet Explorer 8.0以上のバージョン、Mozilla Firefox 30.0〜51、Google Chrome 31〜51

第 2 章 本機の起動とアクセス

ユーザーアカウントとデータのセキュリティとプライバシーを保護するために、ネットワーク経由で本機にアクセスする際には、本機を起動するためのログインパスワードを設定する必要があります。

メモ

クライアントソフトウェアの起動の詳細については、ソフトウェアクライアントのユーザーマニュアルを参照してください。

2.1 SADPで本機を起動する

SADPソフトウェアによるオンラインデバイスを検索し起動します。

ご使用の前に

www.hikvision.comにアクセスして、SADPソフトウェアをインストールしてください。

ステップ

1. ネットワークケーブルで本機をネットワークに接続します。
2. SADPソフトを起動して、オンラインデバイスの検索をします。
3. デバイスの一覧から**Device Status**にチェックを入れ、**Inactive**のデバイスを選択します。
4. 新しいパスワードを作成してパスワード欄に入力し、入力したパスワードを確認してください。

   注意

   本機のセキュリティを高めるため、お客様ご自身で強力なパスワード（大文字、小文字、数字、特殊文字を含む8文字以上）を設定することを強く推奨します。また、定期的にパスワードをリセットすることをお勧めします。特にセキュリティの高いシステムでは、毎月または毎週パスワードをリセットすることで、本機をより安全に保護することができます。
5. **OK**をクリックします。

   Device Statusを**Active**に変更してください。
6. **オプション**：**Modify Network Parameters**で本機のネットワークパラメーターを変更します。

2.2 ブラウザで本機を起動する

ブラウザから本機にアクセスし、起動できます。

ステップ

1. 本機とパソコンをネットワークケーブルで接続します。
2. パソコンと本機のIPアドレスを同じセグメントに変更します。

メモ

工場出荷時のIPアドレスは192.168.1.64です。パソコンのIPアドレスは、192.168.1.2～192.168.1.253（192.168.1.64を除く）の範囲で設定可能です。例えば、パソコンのIPアドレスを192.168.1.100に設定できます。

3. ブラウザに**192.168.1.64**を入力 します。
4. デバイス起動パスワードを設定します。

注意

本機のセキュリティを高めるため、お客様ご自身で強力なパスワード（大文字、小文字、数字、特殊文字のうち少なくとも3つを含む8文字以上）を設定することを強く推奨します。また、定期的にパスワードをリセットすることをお勧めします。特にセキュリティの高いシステムでは、毎月または毎週パスワードをリセットすることで、本機をより安全に保護することができます。

5. **OK**をクリックします。
6. 起動パスワードを入力し、本機にログインします。
7. **オプション**：**Configuration → Network → Basic → TCP/IP**の順に進み、本機のIPアドレスをネットワークと同じセグメントに変更します。

2.3 ログイン

Web ブラウザで本機にログインします。

2.3.1 プラグインのインストール

一部のOSやWebブラウザでは、カメラ機能の表示や操作が制限される場合があります。正常な表示と操作を確認するには、プラグインをインストールしたり、特定の設定を行う必要があります。詳細な制限機能については、実機を確認してください。

オペレーティングシステム	Webブラウザ	操作
Windows	• インターネットエクスプローラー8以上 • Google Chrome 57およびそれ以前のバージョン • Mozilla Firefox 52およびそれ以前のバージョン	ポップアップ表示に従って、プラグインのインストールを完了します。
	• Google Chrome 57以上 • Mozilla Firefox 52以上	Download Plug-in をクリックして、プラグインのダウンロードとインストールをします。
Mac OS	• Google Chrome 57以上 • Mozilla Firefox 52以上 • Mac Safari 16以上	プラグインのインストールは必要ありません。

オペレーティングシステム	Webブラウザ	操作
		Configuration → Network → Advanced Settings → Network Serviceの順に進み、通常表示でWebSocketまたはWebsocketsを有効にします。一部の機能の表示と操作が制限されます。例：PlaybackとPictureは使用できません。詳細な制限機能については、実機を確認してください。

メモ

このカメラはWindowsおよびMac OSにのみ対応し、Linuxには対応していません。

2.3.2 管理者パスワードの復旧

管理者パスワードを忘れた場合は、アカウントのセキュリティ設定を完了した後、ログイン画面の**Forget Password**をクリックしてパスワードをリセットできます。
セキュリティ質問または電子メールを設定することで、パスワードをリセットすることができます。

メモ

パスワードの再設定が必要な場合は、本機とパソコンが同じネットワークセグメント上にあることを確認してください。

セキュリティ質問

起動の際に、アカウントのセキュリティを設定することができます。または、**Configuration → System → User Management**の順に進み、**Account Security Settings**をクリックし、セキュリティ質問を選択して答えを入力してください。
ブラウザから本機にアクセスする場合は、**Forget Password**をクリックしてセキュリティ質問に答えると、管理者パスワードをリセットすることができます。

電子メール

起動の際に、アカウントのセキュリティを設定することができます。または、**Configuration → System → User Management**の順に進み、**Account Security Settings**をクリックし、メールアドレスを入力して復旧操作中に認証コードを受信します。

2.3.3 不正なログインロック

この機能はインターネット経由で本機にアクセスする際のセキュリティ向上に役立ちます。

Configuration → System → Security → Security Serviceの順に進み、**Enable Illegal Login Lock**を有効にします。**Illegal Login Attempts**と**Locking Duration**は設定可能です。

不正なログインの試行

間違ったパスワードでのログイン試行回数が設定回数に達すると、本機がロックされます。

ロッキング時間

設定した時間が経過すると本機がロックを解除します。

第 3 章 ライブビュー

ここでは、ライブビューパラメーター、機能アイコン、送信パラメーター設定について説明します。

3.1 ライブビューパラメーター

対応する機能は機種により異なります。

3.1.1 ライブビューを有効/無効にする

この機能は、全チャンネルのライブビューを素早く有効または無効にするために使用します。

- をクリックすると、全チャンネルのライブビューを開始します。
- をクリックすると、全チャンネルのライブビューを停止します。

3.1.2 アスペクト比を調整する

ステップ

1. **Live View**をクリックします。
2. をクリックして、アスペクト比を選択します。
   - は、4：3のウィンドウサイズです。
   - は、16：9のウィンドウサイズです。
   - は元のウィンドウサイズです。
   - は自己適応ウィンドウサイズです。
   - はウィンドウサイズの元の比率のです。

3.1.3 ライブビューストリームタイプ

用途に応じて、ライブビューストリームの種類を選択します。ストリームタイプ選択の詳細については***ストリームタイプ***を参照してください。

3.1.4 サードパーティプラグインを選択する

特定のブラウザでライブビューが表示できない場合、そのブラウザに応じてライブビュー用のプラグインを変更できます。

ステップ

1. **Live View**をクリックします。
2. をクリックして、プラグインを選択します。

- Internet Explorerでアクセスする場合は、WebcomponentsまたはQuickTimeを選択します。
- その他のブラウザでアクセスする場合は、WebcomponentまたはQuickTime、VLC、MJPEGを選択します。

3.1.5 ウィンドウ分割

- は1×1のウィンドウ分割です。
- は2×2のウィンドウ分割です。
- は3×3のウィンドウ分割です。
- は4×4のウィンドウ分割です。

3.1.6 ライト

をクリックしてイルミネーターの点灯と消灯ができます。

3.1.7 カウントピクセル

ライブビュー画像で選択した領域の高さと幅のピクセルを取得できます。

ステップ

1. をクリックすると、この機能が有効になります。
2. 画像上でマウスをドラッグして、目的の矩形領域を選択します。
   ライブビュー画像の下部に幅ピクセルと高さピクセルを表示します。

3.1.8 デジタルズームを開始する

画像内の任意の領域の詳細情報を確認できます。

ステップ

1. をクリックすると、デジタルズームが有効になります。
2. ライブビュー画像で、マウスをドラッグして目的の領域を選択します。
3. ライブビュー画像内をクリックすると、元の画像に戻ることができます。

3.1.9 補助フォーカス

電動デバイスに使用されます。本機がはっきりを焦点を合わせることができない場合、画像を鮮明にすることができます。
ABF対応機種の場合、レンズの角度を調整し、焦点を合わせてから本機のABFボタンをクリックすると、本機ははっきりと焦点を合わせることができます。

をクリックすると、自動的に焦点を合わせます。

メモ

- 本機が補助フォーカスで焦点合わせができない場合、**レンズの初期化**を使用し、再度補助フォーカスを使用して画像を鮮明にできます。
- 補助フォーカスで本機の焦点がはっきりしない場合は、手動フォーカスを使用します。

3.1.10 レンズの初期化

レンズの初期化は、電動レンズ搭載機で使用します。長時間のズームやフォーカスで画像がぼやけた場合、レンズをリセットする機能です。この機能は機種によって異なります。

手動でのレンズの初期化

をクリックしてレンズを初期化します。

自動でのレンズの初期化

Configuration → System → Maintenance → Lens Correctionの順に進み、この機能を有効にします。アーミングスケジュールを設定することができ、設定した時間帯に自動的にレンズを補正することができます。

3.1.11 クイックセットライブビュー

ライブビューページで、PTZ、ディスプレイ設定、OSD、ビデオ/オーディオ設定、VCAリソース設定が素早くできます。

ステップ

1. をクリックすると、クイックセットアップページが表示されます。
2. PTZ、ディスプレイ設定、OSD、ビデオ/オーディオおよびVCAリソースのパラメーターを設定します。
   - PTZの設定については**レンズパラメーターの調整**を参照してください。
   - ディスプレイ設定については**ディスプレイの設定**を参照してください。
   - OSD設定については**OSD**を参照してください。
   - オーディオ/ビデオ設定については**ビデオ・オーディオ**を参照してください。

メモ

この機能は一部の機種のみ対応しています。

3.1.12 レンズパラメーターの調整

レンズのフォーカス、ズーム、アイリスなどの調整に使用します。

ズーム

- をクリックすると、ズームインします。
- をクリックすると、ズームアウトします。

フォーカス

- をクリックすると、レンズは遠くまで焦点を合わせ、遠くのものが鮮明に見えます。
- をクリックすると、レンズは近くに焦点を合わせ、近くのものが鮮明に見えます。

PTZスピード

- をスライドすると、パン／チルトの動作速度を調整します。

アイリス

- 画像が暗すぎるときはをクリックしてアイリスを大きくします。
- 画像が明るすぎるときはをクリックして、アイリスを絞ります。

3.1.13 3Dポジショニング

3Dポジショニングは、選択した領域を画像中心に再配置することです。

ステップ

1. をクリックするとこの機能が有効になります。
2. ライブ映像の中で、対象エリアを選択します。
   - ライブ画像上のポイントを左クリック：そのポイントがライブ画像の中心に移動します。ズームイン、ズームアウトはありません。
   - マウスを右下の位置までドラッグすると、ライブ画像上の領域を枠で囲むことができます。枠で囲まれた領域は拡大され、ライブ画像の中央に移動します。
   - マウスを左上の位置までドラッグすると、ライブ画像上の領域を枠で囲むことができます。枠で囲んだ領域は縮小され、ライブ画像の中央に移動します。
3. もう一度ボタンをクリックすると、この機能がオフになります。

3.2 送信パラメーターの設定

ネットワーク状況により、ライブビュー映像に異常が表示される場合があります。異なるネットワーク環境では、送信パラメーターを調整することで問題を解決することができます。

ステップ

1. 次の順に進みます。**Configuration → Local**
2. 必要に応じて、送信パラメーターを設定します。

   プロトコル

   TCP

TCPは、ストリーミングデータの完全な配信とより良いビデオ品質を保証しますが、リアルタイム伝送に影響が出ます。安定したネットワーク環境に適しています。

UDP

UDPは、円滑な映像を求めない、不安定なネットワーク環境に適しています。

MULTICAST

MULTICASTは、複数のクライアントが存在する状況に適しています。選択する前に、マルチキャストアドレスを設定する必要があります。

メモ

マルチキャストの詳細については、**マルチキャスト**を参照してください。

HTTP

HTTPは、サードパーティが本機からストリームを取得する必要がある場合に適しています。

プレイパフォーマンス

Shortest Delay

本機は、円滑なビデオ映像よりもリアルなビデオ映像を優先します。

Balanced

本機、はリアルなビデオ映像と円滑なビデオ映像を両立します。

Fluent

本機は、リアルなビデオ映像よりも円滑なビデオ映像を優先します。ネットワーク環境が悪いと、本機はFluentを有効にしていても、円滑なビデオ映像を確保できません。

Custom

フレームレートを手動で設定することができます。劣悪なネットワーク環境でフレームレートを下げて円滑なライブビューを得ることができます。ただし、ルール情報が表示されない場合があります。

3. **OK**をクリックします。

第 4 章 ビデオ・オーディオ

ここでは、ビデオおよびオーディオ関連のパラメーターの設定について説明します。

4.1 ビデオ設定

ここでは、ストリームタイプ、ビデオエンコード、解像度など、ビデオパラメーターの設定について説明します。
設定画面に進みます。**Configuration → Video/Audio → Video**

4.1.1 ストリームタイプ

複数のストリームをサポートするデバイスでは、ストリームタイプごとにパラメーターを設定することができます。

メインストリーム

メインストリームは、本機がサポートする最良のストリーム性能を意味します。メインストリームは通常、本機が使用できる最良の解像度とフレームレートを提供します。ただし、高解像度とフレームレートは通常、より大きなストレージスペースと伝送におけるより高い帯域幅の要件を意味します。

サブストリーム

サブストリームは通常、比較的低解像度のオプションを提供し、より少ない帯域幅とストレージスペースを必要とします。

その他のストリーム

メインストリームとサブストリーム以外のストリームも提供し、カスタマイズして使用することもできます。

4.1.2 ビデオタイプ

このストリームに含みたいコンテンツ（ビデオとオーディオ）を選択します。

ビデオ

このストリームに含まれるのは、ビデオコンテンツのみです。

ビデオ・オーディオ

ビデオコンテンツとオーディオコンテンツは、コンポジットストリームに含まれます。

4.1.3 解像度

必要に応じて、ビデオの解像度を選択します。解像度を上げるには、より高い帯域幅とより大きなストレージが必要です。

4.1.4 ビットレートタイプと最大ビットレート

固定ビットレート

このストリームを圧縮し、比較的一定のビットレートで伝送します。圧縮速度は高速ですが、画像にモザイクがかかる場合があります。

可変ビットレート

Max. Bitrateに設定された下で本機が自動的にビットレートを調整します。圧縮速度は、ビットレートが可変ビットレートよりも低速になります。ただし、可変ビットレートは複雑なシーンの画質を確保します。

4.1.5 ビデオの画質

Bitrate TypeがVariableに設定されている場合、ビデオの画質を設定できます。必要に応じて、ビデオの画質を選択します。ビデオの画質を上げるには、より高い帯域が必要です。

4.1.6 フレームレート

フレームレートは、ビデオストリームが更新される頻度を表すもので、1秒あたりのフレーム数（fps）で測定されます。

フレームレートが高いほど、ビデオに動きがある場合に画質を維持するため有利です。なお、フレームレートを上げるには、より高い帯域幅とより大きなストレージが必要です。

4.1.7 ビデオエンコード

本機がビデオのエンコードに採用する圧縮規格を表します。

メモ

利用可能な圧縮規格は、機器の機種によって異なります。

H.264

H.264は、MPEG-4 Part 10、Advanced Video Codingとしても知られている圧縮規格です。画質を圧縮することなく、MJPEGやMPEG-4 Part 2よりも圧縮率を高め、ビデオファイルのサイズを小さくすることができます。

H.264+

H.264+は、H.264をベースに改良した圧縮コーディング技術です。H.264+を有効にすることで、最大平均ビットレートからHDDの消費量を推定できます。H.264と比較して、H.264+は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%節約できます。

H.264+が有効な場合、**Max. Average Bitrate**を設定できます。本機では、デフォルトで推奨する平均ビットレートを表示します。ビデオの画質を高めたい場合は、パラメーターを高い値に調整することができます。最大平均ビットレートは、最大ビットレート以下にしてください。

メモ

H.264+が有効な場合、**Video Quality**、**I Frame Interval**、**Profile**、**SVC**は設定できません。

H.265

H.265は、High Efficiency Video Coding（HEVC）、MPEG-H Part 2とも呼ばれる圧縮規格です。H.264と比較して同じ解像度、フレームレート、画質でより優れた映像圧縮が可能です。

H.265+

H.265+は、H.265をベースに改良した圧縮コーディング技術です。H.265+を有効にすることで、最大平均ビットレートからHDDの消費量を推定できます。H.265と比較して、H.265+は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%節約できます。

H.265+ は、H.265 をベースに改良した圧縮コーディング技術です。本機では、デフォルトで推奨する平均ビットレートを表示します。ビデオの画質を高めたい場合は、パラメーターを高い値に調整することができます。最大平均ビットレートは、最大ビットレート以下にしてください。

メモ

H.265+ が有効な場合、**Video Quality**、**I Frame Interval**、**Profile**、**SVC**は設定できません。

I-フレームインターバル

I-フレームインターバルは、2つのI-フレーム間のフレーム数です。

H.264やH.265では、Iフレームまたはイントラフレームは、他の画像を参照することなく独立してデコードできる自己完結型のフレームです。Iフレームは、他のフレームよりも多くのビット数が必要です。従って、より多くのIフレーム、つまりIフレーム間隔が小さいビデオは、より大きなのストレージを必要としますが、より安定した信頼性の高いデータビットを生成します。

SVC

Scalable Video Coding（SVC）は、H.264またはH.265ビデオ圧縮規格のAnnex G拡張の名称です。

SVCの標準化の目的は、1つ以上のサブセットビットストリームを含む高品質ビデオビットストリームを、サブセットビットストリームと同じデータ量で、既存のH.264またはH.265設計と同様の複雑さと再構成品質でエンコードできるようにすることです。サブセットビットストリームは、大きなビットストリームからパケットのデータ量を最適化することによって導出されます。

SVCは、古いハードウェアの前方互換性を可能にします。同じビットストリームを、低解像度のサブセットしかデコードできない基本的なハードウェアで消費することができ、より高度なハードウェアは高品質のビデオストリームをデコードできるようになります。

MPEG4

MPEG4とは、MPEG-4 Part 2のことで、Moving Picture Experts Group（MPEG）が開発した動画圧縮フォーマットです。

MJPEG

Motion JPEG（M-JPEGまたはMJPEG）は、フレーム内コード化技術を用いた動画圧縮フォーマットです。MJPEG形式の画像は、個々のJPEG画像として圧縮されます。

プロファイル

この機能は、同じビットレートであれば、プロファイルが複雑なほど高画質となり、ネットワーク帯域の要求も高くなります。

4.1.8 スムージング

このストリームの滑らかさのことです。スムージングの値が高いほど、ストリームの滑らかさが向上しますが、ビデオの画質はよくありません。スムージングの値が小さいほど、ストリームが滑らかでなくなりますが、ストリームの質は高くなります。

4.2 ROI

ROI（Region of Interest）エンコーディングは、画像圧縮においてROIと背景情報を識別するのに役立ちます。この技術では、関心領域に多くのエンコーディングリソースを割り当てることで、ROIの品質を向上させ、背景の情報に焦点を合わせないようにします。

4.2.1 ROIの設定

ROI（Region of Interest）エンコーディングは、関心領域に多くのエンコーディングリソースを割り当てることで、背景の情報に焦点を合わせずROIの品質を向上させます。

ご使用の前に

ビデオコーディングのタイプを確認してください。ROIは、ビデオコーディングタイプがH.264またはH.265の場合にサポートされます。

ステップ

1. 次の順に進みます。**Configuration → Video/Audio → ROI**
2. **Enable**にチェックを入れます。
3. **Stream Type**を選択します。
4. **Fixed Region**の**Region No.**を選択し、ROI領域を描画します。
   1) **Draw Area**をクリックします。
   2) この表示画面でマウスをクリックしてドラッグし、固定領域を描画します。
   3) **Stop Drawing**をクリックします。

   メモ

   調整が必要な固定領域を選択し、マウスをドラッグして位置を調整します。
5. **Region Name**と**ROI Level**を入力します。
6. **Save**をクリックします。

   メモ

   ROIレベルが高いほど、検出された領域の画像は鮮明になります。
7. **オプション**：他の領域No.を選択し、複数の固定領域を描画する必要がある場合は、上記の手順を繰り返してください。

4.3 オーディオ設定

オーディオエンコード、環境ノイズフィルタなどのオーディオパラメーターを設定する機能です。オーディオ設定画面に進みます。**Configuration → Video/Audio → Audio**

メモ

この機能は一部のカメラの機種のみ対応しています。

4.3.1 オーディオエンコード

オーディオエンコード圧縮を選択します。

4.3.2オーディオ入力

メモ

- 必要に応じてオーディオ入力機器を接続します。
- オーディ入力の表示は、デバイスの機種によって異なります。

LineIn	MP3、シンセサイザー、アクティブピックアップなどの出力が大きいオーディオ入力機器と接続した場合は**Audio Input**を**LineIn**に設定します。
MicIn	マイクやパッシブピックアップなどの出力が小さいオーディオ入力機器と接続した場合は**Audio Input**を**MicIn**に設定します。

4.3.3 オーディオ出力

メモ

必要に応じてオーディオ出力機器を接続します。

オーディオ出力デバイスのスイッチです。出力ボリュームは必要に応じて調整できます。これを無効にすると、すべてのデバイスのオーディオ出力ができなくなります。オーディオ出力表示は、本機のモードによって異なります。

4.3.4 環境ノイズフィルタ

環境ノイズフィルタをOFFまたはONに設定します。これを有効にすると、環境中のノイズをある程度フィルタリングすることができます。

4.4ディスプレイの設定

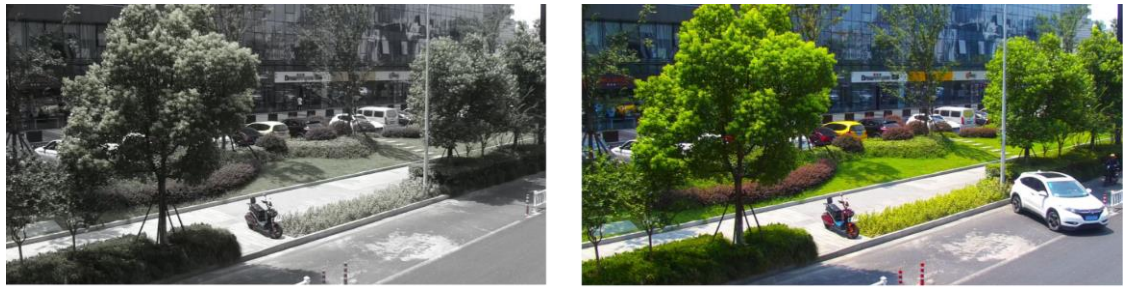
画像の特徴を調整するパラメーター設定を行います。
次の順に進みます。**Configuration → Image → Display Settings**
Defaultをクリックすると設定が復旧されます。

4.4.1 シーンモード

画像パラメーターは、設置環境に応じてあらかじめいくつかのセットが用意されています。実際の設置環境に応じてシーンを選択することで、ディスプレイ設定のスピードアップが図れます。

画像調整

Brightness、**Saturation**、**Hue**、**Contrast**、**Sharpness**を調整して、画像を最適に表示します。



低彩度　　高彩度

図 4-1 彩度

露光設定

露光は、アイリス、シャッター、写真感度の組み合わせでコントロールします。露光パラメーターを設定して、画像効果を調整できます。

マニュアルモードでは、**Exposure Time**、**Gain**、**Slow Shutter**を設定する必要があります。

Day/Nightスイッチ

Day/Nightスイッチ機能により、Dayモードではカラー画像を、Nightモードでは白黒画像を表示します。スイッチモードは設定可能です。

Day

画像は常にカラーで表示されます。

Night

画像は常に白黒で表示されます。

Auto

照度に応じてDayモードとNightモードが自動的に切り替わります。

Scheduled-Switch

Start Timeと**End Time**を設定して、Dayモードの持続時間を決めます。

Triggered by alarm input

Dayと**Night**の2つのトリガーモードがあります。例えばトリガーモードが**Night**の場合、アラーム入力信号を受信すると、画像が白黒になります。

メモ

Day/Nightスイッチの機能は機種により異なります。

Grey Scale

Grey Scaleは[0-255]または[16-235]の範囲で選択できます。

Rotate

この機能を有効にすると、ライブビューは反時計回りに90°回転します。例えば、1280×720は720×1280に回転します。
この機能を有効にすると、垂直方向のモニタリングの有効範囲を変更することができます。

BLC

強い逆光でフォーカスすると、被写体が暗くなってしまいよく見えません。BLC（逆光補正）は、手前の被写体への光を補正し、鮮明にする機能です。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エリアとして赤い四角形を描くことができます。

WDR

WDR（ワイドダイナミックレンジ）機能により、照度差の激しい環境下でも鮮明な映像が得られます。

視野内に非常に明るい部分と非常に暗い部分が同時に存在する場合、WDR機能を有効にしてレベルを設定できます。WDRは画像全体の輝度レベルを自動でバランスをとり、より細部まで鮮明な画像を提供します。

メモ

WDRが有効の時、他の機能がサポートされないことがあります。詳しくは、実機のインターフェースを参照してください。

図 4-2 WDR

HLC

画像の明るい部分が露光オーバー、暗い部分が露光アンダーになっている場合、HLC（High Light Compression）機能を有効にすることで、明るい部分を弱め、暗い部分を明るくして、画像全体の光のバランスを整えることができます。

ホワイトバランス

ホワイトバランスとは、カメラの白色表現機能のことです。この機能は環境に応じて色温度の調整に使用されます。

図 4-3 ホワイトバランス

DNR

デジタルノイズリダクションは画像ノイズを低減し、画質を向上させます。**NormalとExpert**モードが選択できます。

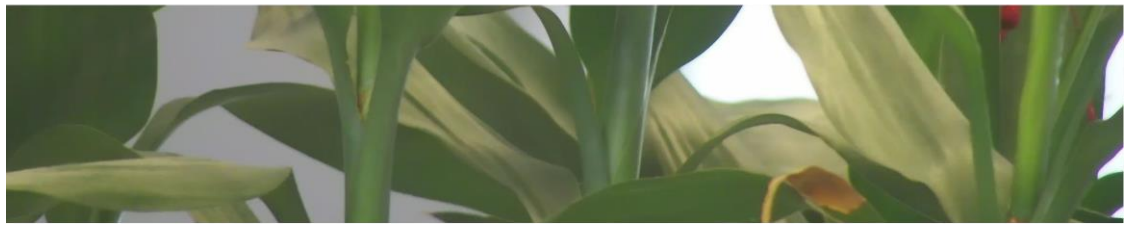
Normal

DNRレベルを設定して、ノイズリダクションの度合いをコントロールします。DNRレベルが高いほど、低減の度合が強くなります。

Expert

空間DNRと時間DNRの両方でDNRレベルを設定し、ノイズリダクションの度合いをコントロールします。DNRレベルが高いほど、低減の度合が強くなります。

DNR Off



DNR On

図 4-4 DNR

デフォッグ

周囲に霧がかかり、映像がモヤモヤしているときに、デフォグ機能を有効にします。微妙なディテールを強調し、画像がより鮮明に見えるようにします。

デフォッグOFF

デフォッグON

図 4-5 デフォッグ

ミラー

ライブビュー画像が実際のシーンと逆になっている場合に、画像を正常に表示する機能です。
必要に応じて、ミラーモードを選択します。

メモ

この機能を有効にすると、ビデオ録画が短時間中断されます。

4.4.2 画像パラメータースイッチ

本機は設定された時間帯で自動的に画像パラメーターを切り換えます。

画像パラメータースイッチの設定画面に進みます。**Configuration → Image → Image Parameters Switch**の順に進み、必要に応じてパラメーターを設定します。

設定スイッチ

一定時間内に画像パラメーターをシーンに合わせて自動で切り替えます。

ステップ

1. **Enable**にチェックを入れます。
2. 対応する時間帯とシーンを選択し、設定します。

   メモ

   シーンの設定は、**シーンモード**を参照してください。
3. **Save**をクリックします。

4.5 ビデオ規格

ビデオ規格とは、表示する色量や解像度を定めたビデオカードやビデオ映像表示デバイスの能力です。一般的に使われているビデオ規格は、NTSCとPALの2種類です。NTSCでは、1秒間に30フレームが送信されます。1フレームは525本の個々の走査線で構成されています。PALでは、1秒間に25フレームが送信されます。1フレームは625本の個々の走査線で構成されています。お住まいの国・地域のビデオ方式に合わせて、ビデオ信号の規格を選択してください。

4.6 OSD

ビデオストリームに表示される機器名、時刻/日付、フォント、色、テキストオーバーレイなどのOSD（On Screen Display）情報をカスタマイズできます。
OSD設定画面に進みます。**Configuration → Image → OSD Settings**で対応するパラメーターを設定し、**Save**をクリックして有効にします。

表示される情報

カメラ名、日付、週、およびそれらに関連する表示形式を設定します。

Text Overlay

画像にカスタマイズしたオーバーレイテキストを設定します。

OSDパラメーター

Display Mode、**OSD Size**、**Font Color**、**Alignment**などのOSDパラメーターを設定します。

4.7 プライバシーマスクの設定

ライバシー保護のため、ライブビューの特定の領域をブロックする機能です。本機がどのように動いても、ブロックされたシーンが見られることはありません。

ステップ

1. プライバシーマスクの設定画面に進みます。**Configuration → Image → Privacy Mask**
2. **Enable Privacy Mask**にチェックを入れます。
3. **Draw Area**をクリックします。ライブビュー内でマウスをドラッグして、閉じた領域を描画します。

Drag the corners of the area	領域の大きさを調整します。
Drag the area	領域の位置を調整します。
Click Clear All	設定した領域をすべてクリアします。

4. **Stop Drawing**をクリックします。
5. **Save**をクリックします。

4.8 オーバーレイ画像

カスタマイズした画像をライブビューに重ねます。

ご使用の前に

オーバーレイする画像は、24bitのBMPフォーマットで、最大画像サイズは128×128ピクセルです。

ステップ

1. 画像オーバーレイ設定画面に進みます。**Configuration → Image → Picture Overlay**
2. **Browse**をクリックして画像を選択し、**Upload**をクリックします。
   アップロードに成功すると、ライブビューに赤い四角がついた画像が表示されます。
3. **Enable Picture Overlay**にチェックを入れます。
4. 画像をドラッグして位置を調整します。
5. **Save**をクリックします。

第 5 章 ビデオ録画と画像キャプチャ

ここでは、ビデオクリップやスナップショットの取り込み、再生、キャプチャしたファイルのダウンロードなどの操作を説明します。

5.1 ストレージの設定

ここでは、いくつかの一般的なストレージパスの設定を説明します。

5.1.1 新しいメモリーカードや暗号化されていないメモリーカードの設定

ご使用の前に

新しいメモリーカードや暗号化されていないメモリーカードを本機に挿入します。詳しい挿入方法は、本機のクイックスタートガイドを参照してください。

ステップ

1. 次の順に進みます。**Configuration → Storage → Storage Management → HDD Management**
2. メモリーカードを選択します。

   メモ

   Unlockが表示されたら、初めにメモリーカードのロックを解除する必要があります。詳しくは**メモリーカードのステータスの検知**をご覧ください。
3. **Format**をクリックして、メモリーカードを初期化します。
   メモリーカードの**Status**が**Uninitialized**から**Normal**に変わるとメモリーカードは使用可能です。
4. **オプション**：メモリーカードを暗号化します。
   1) **Encrypted Format**をクリックします。
   2) 暗号化パスワードを設定します。
   3) **OK**をクリックします。
      Encryption Statusが**Encrypted**に変わるとメモリーカードは使用可能です。

   メモ

   暗号化パスワードは適切に管理してください。暗号化パスワードは、忘れても見つからないようになっています。
5. **オプション**：メモリーカードの**Quota**を定義します。必要に応じて異なるコンテンツの割当率を入力します。
6. **Save**をクリックします。

メモリーカードのステータスの検知

本機はHikvisionメモリーカードのステータスを検知します。メモリーカードの異常を検知したとき、通知を受信します。

ご使用の前に

設定画面は、Hikvisionのメモリーカードが本機に装着されている場合のみ表示されます。

ステップ

1. 次の順に進みます。**Configuration → Storage → Storage Management → Memory Card Detection**
2. **Status Detection**をクリックして、メモリーカードの**Remaining Lifespan**と**Health Status**を確認します。

   Remaining Lifespan

   残りの寿命を表示します。メモリーカードの寿命は、容量やビットレートなどに影響されます。残りの寿命が短い場合は、メモリーカードの交換が必要です。

   Health Status

   メモリーカードの状態を表示します。ステータスの説明には、「good」、「bad」、「damaged」の3つがあります。**Arming Schedule**と**Linkage Method**が設定されていると、ヘルスステータスが「good」以外であれば、通知を受信します。

   メモ

   ヘルスステータスが「good」でない場合は、メモリーカードを交換することをお勧めします。
3. **R/W Lock**をクリックして、メモリーカードへの読み取りと書き込みの認証を設定します。
   - ロックを追加します。
     a. **Lock Switch**を**ON**にします。
     b. パスワードを入力します。
     c. **Save**をクリックします。
   - ロック解除
     - メモリーカードをロックするデバイスでは、ロック解除は自動的に行われ、ユーザー側でのロック解除の操作は不要です。
     - メモリーカード（ロック付き）を別の機器で使用する場合は、**HDD Management**に進み、メモリーカードのロックを手動で解除してください。メモリーカードを選択し、**Unlock**をクリックします。正しいパスワードを入力してロックを解除します。
   - ロックを外す
     a. **Lock Switch**を**OFF**にします。
     b. **Password Settings**にパスワードを入力します。
     c. **Save**をクリックします。

メモ

- **R/W Lock**を設定できるのは管理者ユーザーのみです。
- メモリーカードは、ロックを解除した状態でないと読み書きができません。
- 本機にメモリーカードのロックが追加されていて、本機を工場出荷時に戻す場合、**HDD Management**に進み、メモリーカードのロックを解除できます。

4. アーミングスケジュールとリンケージメソッドを設定します。詳しくは**アーミングスケジュールの設定**と**リンケージメソッドの設定**を参照してください。
5. **Save**をクリックします。

5.1.2 FTPの設定

イベントや定時スナップショットタスクでキャプチャした画像を保存するFTPサーバーを設定します。

ご使用の前に
最初にFTPサーバーのアドレスを取得します。

ステップ
1. 次の順に進みます。**Configuration → Network → Advanced Settings → FTP**
2. **FTP**を設定します。

   FTP Protocol
   FTPとSFTPが選択できます。ファイルのアップロードは、SFTPプロトコルを使用して暗号化されます。

   Server Address and Port
   FTPサーバーのアドレスと対応するポートです。

   User Name and Password
   FTPユーザーには、画像をアップロードする認証が必要です。
   FTPサーバーが匿名ユーザーによる画像アップロードに対応している場合、**Anonymous**にチェックを入れると、アップロード時に端末情報を隠すことができます。

   Directory Structure
   FTPサーバーのナップショットの保存パスです。

   Picture Filing Interval
   画像の管理性を高めるため、画像のファイリング間隔を1日～30日の間で設定できます。同じ時間間隔帯でキャプチャされた画像は、時間間隔帯の開始日と終了日の名前が付いた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のネーミングルールを設定します。ドロップダウンリストから**Default**を選択して、IP アドレス_チャンネルナンバー_キャプチャ時間_イベントタイプ.jpg（例：10.11.37.189_01_20150917094425492_FACE_DETECTION.jpg）というデフォルトルールを使用できます。またはデフォルトのネーミングルールに**Custom Prefix**を追加して、ファイル名をカスタマイズできます。
3. **Upload Picture**にチェックを入れて、FTPサーバーへスナップショットをアップロードします。

4. **Enable Automatic Network Replenishment**にチェックを入れます。

メモ

Linkage Methodの**Upload to FTP/Memory Card/NAS**と**Enable Automatic Network Replenishment**は、両方同時に有効にする必要があります。

5. **Test**をクリックして、FTPサーバーを確認します。
6. **Save**をクリックします。

5.1.3 NASの設定

ネットワークサーバーをネットワークディスクとして、記録ファイルやキャプチャ画像などを保存します。

ご使用の前に

最初にネットワークディスクのIPアドレスを取得します。

ステップ

1. NAS設定画面に進みます。**Configuration → Storage → Storage Management → Net HDD**
2. **HDD No.**をクリックします。ディスクのサーバーアドレスとファイルパスを入力します。

Server Address

ネットワークディスクのIPアドレスです。

File Path

ネットワークディスクのファイルの保存パスです。

Mounting Type

オペレーションシステムに応じて、ファイルシステムのプロトコルを選択します。

SMB/CIFSが選択されている場合、ネットHDDのユーザー名とパスワードを入力してセキュリティを確保します。

3. **Test**をクリックして、ネットワークディスクが利用可能かどうかを確認します。
4. **Save**をクリックします。

5.1.4 eMMCプロテクション

この機能はeMMCのヘルスステータスが悪くなると、記憶媒体としての使用を自動的に停止します。

メモ

eMMCプロテクションは、eMMCハードウェアを搭載した一部の機種のみ対応しています。

次の順に進みます。**Configuration → System → Maintenance → System Service**

eMMCは、embedded multimedia cardの略で、組み込み型の不揮発性メモリシステムです。この機能は本機がキャプチャした画像やビデオを保存します。

本機はeMMCのヘルスステータスを監視し、ステータスが悪くなるとeMMCをオフにします。オンのままで消耗したeMMCを使用すると、デバイスの起動不良につながります。

5.1.5 クラウドストレージの設定

この機能はキャプチャした画像やデータをクラウドにアップロードします。このプラットフォームは、画像用クラウドから直接画像を要求して分析を行います。この機能は一部の機種のみ対応しています。

ステップ

注意

クラウドストレージが有効な場合、画像は最初にクラウドビデオマネージャーに保存されます。

1. 次の順に進みます。**Configuration → Storage → Storage Management → Cloud Storage**
2. **Enable Cloud Storage**にチェックを入れます。
3. 基本的なパラメーターを設定します。

Protocol Version	クラウドビデオマネージャーのプロトコルバージョンです。
Server IP	クラウドビデオマネージャーのIPアドレスです。IPv4アドレスに対応しています。
Serve Port	クラウドビデオマネージャーのポートです。デフォルトのポートを使用することが推奨されます。
AccessKey	クラウドビデオマネージャーにログインするキーです。
SecretKey	クラウドビデオマネージャーに保存されているデータを暗号化するキーです。
User Name and Password	クラウドビデオマネージャーのユーザー名とパスワードです。
Picture Storage Pool ID	クラウドビデオマネージャーの画像保存領域のIDです。ストレージプールIDとストレージリージョンIDが同じであることを確認します。

4. **Test**をクリックして、設定をテストします。
5. **Save**をクリックします。

5.2 ビデオ録画

ここでは、手動/予約録画、再生、録画したファイルのダウンロードの操作を説明します。

5.2.1 自動録画

設定した時間帯に自動的に映像を録画する機能です。

ご使用の前に

Continuousを除く、各レコードタイプのイベント設定を**Trigger Recording**に選択してください。詳しくは**イベントとアラーム**を参照してください。

ステップ

1. 次の順に進みます。**Configuration → Storage → Schedule Settings → Record Schedule**
2. **Enable**にチェックを入れます。
3. 録画の種類を選択します。

メモ

録画の種類は機種によって異なります。

Continuous

この映像はスケジュールに従って、継続的に録画されます。

Motion

動体検知を有効にしてトリガーレコーディングで連携方法を選択すると、対象の動きを録画します。

Alarm

アラーム入力を有効にしてトリガーレコーディングで連携方法を選択すると、外部のアラーム入力機器からアラーム信号を受信後、映像を録画します。

Motion | Alarm

動体検知、または外部アラーム入力機器からのアラーム信号を受信した場合、映像を録画します。

Motion & Alarm

動体検知、外部のアラーム入力機器からアラーム信号を受信した場合のみ、映像を録画します。

Event

設定されたイベントを検知した場合、映像を録画します。

4. 選択した録画タイプのスケジュールを設定します。詳しくは**アーミングスケジュールの設定**を参照してください。
5. **Advanced**をクリックして、高度な設定を設定します。

Overwrite

Overwriteを有効にすると、ストレージ容量がいっぱいになった時、録画映像を上書き保存します。上書き保存しないと、新しい映像を録画することができません。

Pre-record

予定時刻の前に録画するよう設定した時間帯です。

Post-record

予定時刻が過ぎた後に録画を停止するよう設定した時間帯です。

Stream Type

録画するストリームタイプを選択します。

メモ

ビットレートが高いストリームタイプを選択した場合、Pre-recordとPost-recordの実際の時間帯が設定値より短くなることがあります。

Recording Expiration

録画は有効期限を超えると削除されます。有効期限は設定できます。なお、一度削除した録画は元に戻せません。

6. **Save**をクリックします。

5.2.2 手動録画

ステップ

1. 次の順に進みます。**Configuration → Local**
2. 録画したファイルの**Record File Size**と保存先パスを設定します。
3. **Save**をクリックします。
4. ライブビューインターフェースの をクリックすると録画を開始します。をクリックすると録画を停止します。

5.2.3 ビデオの再生とダウンロード

ローカルストレージやネットワークストレージに保存されている映像の検索、再生、ダウンロードができます。

ステップ

1. **Playback**をクリックします。
2. 検索状態を設定し、**Search**をクリックします。

   一致した映像ファイルは、タイミングバーに表示されます。
3. ▶をクリックして映像ファイルを再生します。
   - をクリックすると、映像ファイルをクリップします。
   - をクリックすると、映像ファイルをフルスクリーンで再生します。**ESC**を押すとフルスクリーンが終了します。

メモ

Configuration → Localの順に進み、**Save clips to**をクリックすると、クリップした映像ファイルの保存パスを変更できます。

4. 再生インターフェースの をクリックしてファイルをダウンロードします。
   1) 検索状態を設定し、**Search**をクリックします。
   2) 映像ファイルを選択し、**Download**をクリックします。

メモ

Configuration → Localの順に進み、**Save downloaded files to**をクリックすると、ダウンロードした映像ファイルの保存パスを変更できます。

5.3 キャプチャの設定

本機は手動または自動で画像をキャプチャし、設定した保存パスにそれらの画像を保存します。スナップショットの閲覧やダウンロードができます。

5.3.1 自動キャプチャ

設定した時間帯に自動的に画像をキャプチャする機能です。

ご使用の前に

イベントトリガーによるキャプチャが必要な場合は、イベント設定で関連する連携方法を設定します。イベント設定は**イベントとアラーム**を参照してください。

ステップ

1. 次の順に進みます。**Configuration → Storage → Schedule Settings → Capture → Capture Parameters**
2. キャプチャの種類を設定します。

   Timing

   設定した時間間隔で画像をキャプチャします。

   Event-Triggered

   イベントが作動すると画像をキャプチャします。
3. **Format**、**Resolution**、**Quality**、**Interval**、**Capture Number**を設定します。
4. スケジュール時間の設定は**アーミングスケジュール**の設定を参照してください。
5. **Save**をクリックします。

5.3.2 手動キャプチャ

ステップ

1. 次の順に進みます。**Configuration → Local**
2. **Image Format**とスナップショットの保存パスを設定します。

   JPEG

   このフォーマットの画像サイズは比較的小さく、ネットワーク伝送に適しています。

   BMP

   画質が良い状態で圧縮されます。
3. **Save**をクリックします。
4. ライブビューまたは再生ウィンドウ近くの をクリックして、手動で画像をキャプチャします。

5.3.3 タイミングウェイクの設定

スリープ中は、設定した時間間隔で起動し、画像をキャプチャしてアップロードします。

ステップ

メモ

この機能は一部の機種のみ対応しています。

1. **Configuration → Proactive Mode → Power Consumption Mode**の順に進み、**Sleep Schedule**で、タイムスケジュールをクリックして**Sleep Capture Interval**を設定します。
2. 次の順に進みます。**Configuration → Proactive Mode → Timing Wake**
3. **Enable**にチェックを入れます。
4. **Capture Types**を選択します。
5. リンケージメソッドの設定については**リンケージメソッドの設定**を参照してください。
6. **Save**をクリックします。

結果

設定したスリープキャプチャの間隔で本機が起動し、写真を撮影してアップロードします。

5.3.4 ガーディングスケジュール

ガーディングスケジュールは、設定されたスケジュール内で画像をキャプチャし、センターにアップロードしきます。

ステップ

1. 次の順に進みます。**Configuration → Proactive Mode → Guarding Schedule**
2. **Enable**にチェックを入れます。
3. キャプチャーのスケジュールは、お客様のニーズに合わせて設定してください。詳細な設定については**アーミングスケジュールの設定**を参照してください。

メモ

タイミングウェイクとガーディングスケジュールは、同時に有効にすることはできません。

5.3.5 画像の閲覧とダウンロード

ローカルストレージやネットワークストレージに保存されている画像の検索、閲覧、ダウンロードができます。

ステップ

1. **Picture**をクリックします。
2. 検索状態を設定し、**Search**をクリックします。

   マッチングした画像は、ファイルリストに表示されます。
3. その画像を選択し**Download**をクリックしてダウンロードします。

メモ

Configuration → Localの順に進み、**Save snapshots when playback**をクリックすると、画像の保存パスを変更できます。

第 6 章 イベントとアラーム

ここでは、イベントの設定について説明します。アラームが鳴ったとき、本機は一定の反応をします。

6.1 基本イベント

6.1.1 動体検知の設定

この機能は検知領域内の移動体を検出し、リンケージアクションを作動します。

ステップ

1. 次の順に進みます。**Configuration → Event → Basic Event → Motion Detection**
2. **Enable Motion Detection**にチェックを入れます。
3. **オプション**：ハイライトで画像内の移動体を緑色で表示します。
   1) **Enable Dynamic Analysis for Motion**にチェックを入れます。
   2) 次の順に進みます。**Configuration → Local**
   3) **Rules**を**Enable**に設定します。
4. **Configuration Mode**を選択し、ルール領域とルールパラメーターを設定します。
   - ノーマルモードについては**ノーマルモード**を参照してください。
   - エキスパートモードについては**エキスパートモード**を参照してください。
5. アーミングスケジュールとリンケージメソッドを設定します。アーミングスケジュールの設定については**アーミングスケジュールの設定**を参照してください。リンケージメソッドについては**リンケージメソッドの設定**を参照してください。
6. **Save**をクリックします。

エキスパートモード

必要に応じて、昼と夜で異なる動体検知パラメーターを設定できます。

ステップ

1. **Configuration**でエキスパートモードを選択します。
2. エキスパートモードのパラメーターを設定します。

   Day/Nightスイッチ

   OFF: Day/Nightスイッチは無効です。

   Day/Night自動スイッチ: 環境に応じてDay/Nightモードを自動で切り替えます。昼はカラー画像、夜は白黒画像を表示します。

Day/Nightスケジュールスイッチ: スケジュールに合わせてDay/Nightモードを切り替えます。設定した時間帯はDayモードに、それ以外の時間帯はNightモードに切り替わります。

Sensitivity

Sensitivityの値が高いほど、動体検知の感度が高くなります。感度が0に設定されている場合、動体検知とダイナミック分析は機能しません。

Proportion

描画領域において、移動体が占める比率のことです。対象物の大きさが設定した比率を超えると、動体検知が作動します。

3. **Area**を選択し、**Draw Area**をクリックします。ライブ映像上でマウスをクリックしたままドラッグし、マウスを離すと1つのエリアの描画を終了します。

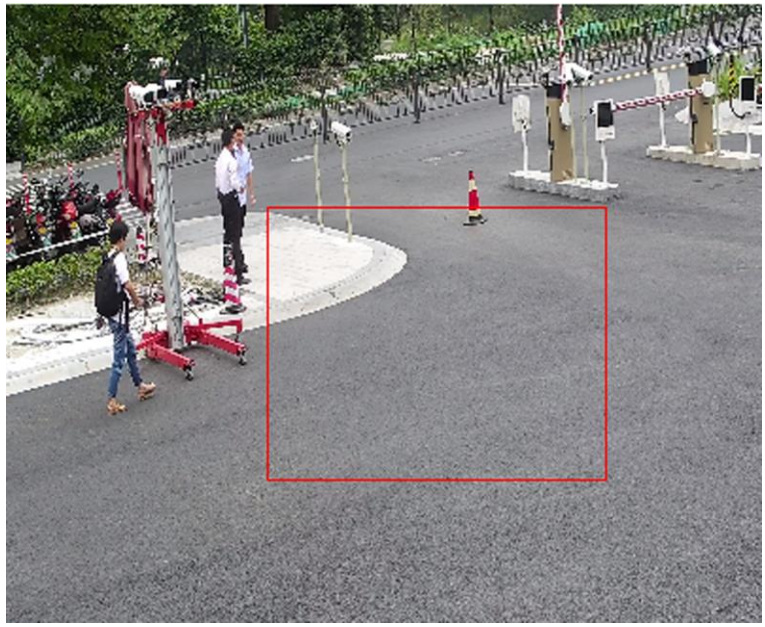


図 6-1 **ルールの設定**

Stop Drawing 1つの領域だけ描画を終了します。

Clear All 全領域を削除します。

4. **オプション**：複数のエリアを設定する場合は、上記の手順を繰り返します。

ノーマルモード

本機のデフォルトパラメーターに従って、動体検知パラメーターを設定できます。

ステップ

1. **Configuration**でノーマルモードを選択します。

2. ノーマルモードの感度を設定します。Sensitivityの値が高いほど、動体検知の感度が高くなります。感度が0に設定されている場合、動体検知とダイナミック分析は機能しません。
3. **Detection Target**を設定します。人物と車両を対象にできます。検知対象が選択されていない場合は、人や車両を含むすべての検知対象が報告されます。
4. **Draw Area**をクリックします。ライブ映像上でマウスをクリックしたままドラッグし、マウスを離すと1つのエリアの描画を終了します。

   Stop Drawing　1つの領域だけ描画を終了します。

   Clear All　全領域を削除します。

5. **オプション**：上記のステップを繰り返して、複数のエリアのパラメーターを設定できます。

6.1.2 ビデオタンパリングアラームの設定

本機は設定されたエリアを監視します。正常に監視できない場合アラームが作動し、特定のアラーム対応アクションを行います。

ステップ

1. 次の順に進みます。**Configuration → Event → Basic Event → Video Tampering**
2. **Enable**にチェックを入れます。
3. **Sensitivity**を設定します。この値が高いほど、エリアのカバーリングが検知しやすくなります。
4. **Draw Area**をクリックし、ライブビュー内でマウスをドラッグしてエリアを描画します。

   Stop Drawing　描画を終了します。

   Clear All　全領域を削除します。

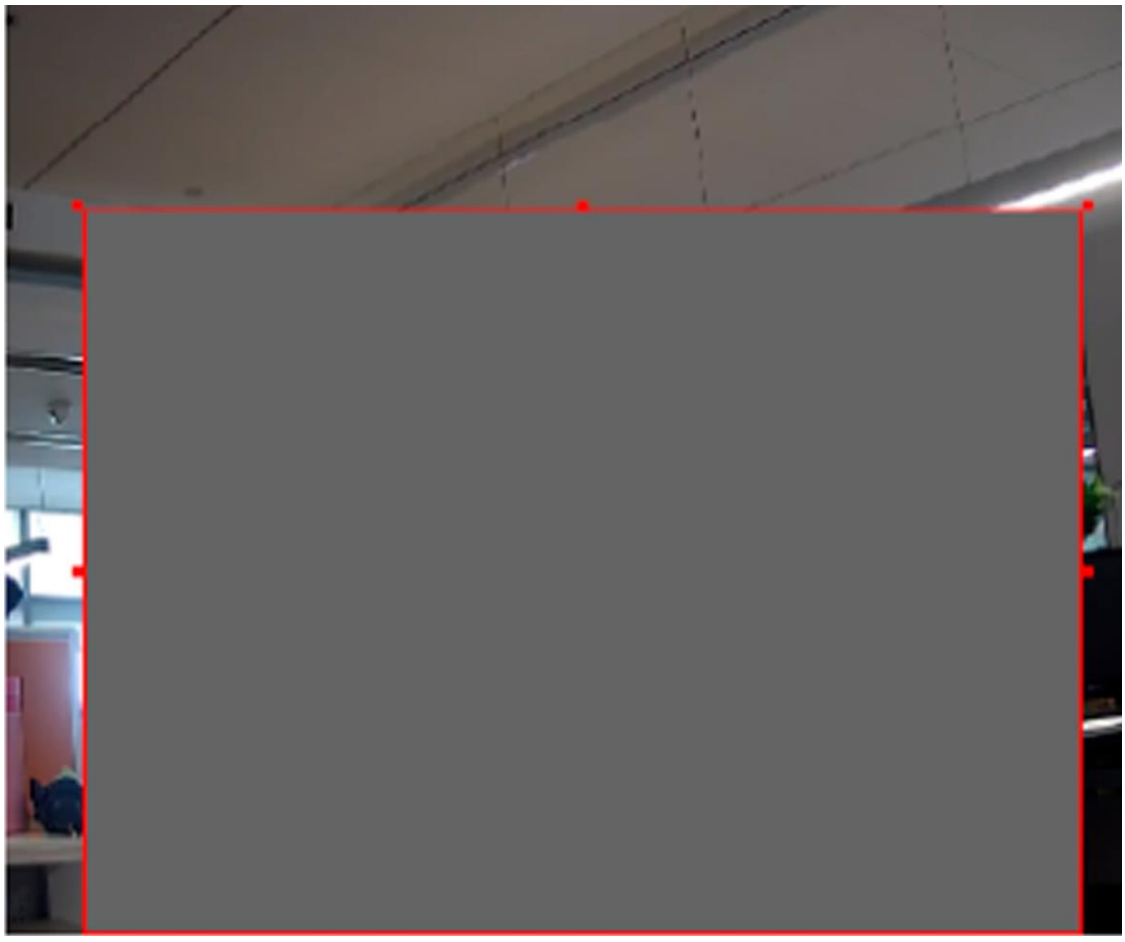


図6-2 ビデオタンパリングエリアの設定

5. スケジュールタイムの設定については**アーミングスケジュールの設定**を参照してください。リンケージメソッドの設定については**リンケージメソッドの設定**を参照してください。
6. **Save**をクリックします。

6.1.3 PIRアラームの設定

侵入者が検知器の視野内に入ると、PIR（受動的赤外線）アラームが作動します。人や犬、猫などの温血動物が放つ熱を検知できます。

ステップ

メモ

この機能は一部の機種のみ対応しています。

1. 次の順に進みます。**Configuration → Advanced Configuration → Basic Event → PIR Alarm**
2. **Enable PIR Alarm**にチェックを入れます。
3. スケジュールタイムの設定については**アーミングスケジュールの設定**を参照してください。リンケージメソッドの設定については**リンケージメソッドの設定**を参照してください。
4. **Save**をクリックします。

6.1.4 角度偏差検出の設定

本機は、傾斜方向と回転方向のデバイスの角度変化を検出することができ、設置面の関連角度変化を示すことができます。

ステップ

1. 次の順に進みます。**Configuration → Event → Basic Event → Angle Deviation Detection**
2. **Enable**にチェックを入れます。
3. **Set**をクリックして、現在の本機の角度を基準角度（回転角度：0°、傾斜角度：0°）として設定します。
   このインターフェースには、リアルタイム角度、リアルタイム角度偏差、基準角度などの角度情報が表示されます。
4. アラームを設定します。
   1) **Real-Time Upload Deviation Angle**にチェックを入れます。
   2) アップロードの間隔は、必要に応じて設定してください。
   3) 傾斜角偏差、回転角偏差を設定します。
   4) **Save**をクリックします。
5. アーミングスケジュールを設定します。**アーミングスケジュールの設定**を参照してください。
6. リンケージメソッドを設定します。**リンケージメソッドの設定**を参照してください。
7. **Save**をクリックします。

6.1.5 異常アラームの設定

ネットワーク切断などの異常が発生した場合、本機は対応するアクションを起します。

ステップ

1. 次の順に進みます。**Configuration → Event → Basic Event → Exception**
2. **Exception Type**を選択します。

HDD Full	HDDのストレージが一杯になっています。
HDD Error	HDDに異常が発生しています。
Network Disconnected	本機はオフラインになっています。
IP Address Conflicted	現在のデバイスのIPアドレスは、ネットワーク内の他のデバイスのIPアドレスと同じです。
Illegal Login	ユーザー名またはパスワードが正しく入力されていません。

3. リンケージメソッドの設定については**リンケージメソッドの設定**を参照してください。
4. **Save**をクリックします。

6.1.6 アラーム入力の設定

外部デバイスからのアラーム信号が、使用中のデバイスの対応するアクションを作動します。

ご使用の前に
外部警報デバイスが接続されていることを確認してください。ケーブルの接続についてはクイックスタートガイドを参照してください。

ステップ

1. 次の順に進みます。**Configuration → Event → Basic Event → Alarm Input**
2. **Enable Alarm Input Handling**にチェックを入れます。
3. **Alarm Input NO.**と**Alarm Type**をドロップダウンリストから選択します。**Alarm Name**を編集します。
4. スケジュールタイムの設定については**アーミングスケジュールの設定**を参照してください。リンケージメソッドの設定については**リンケージメソッドの設定**を参照してください。
5. **Copy to...**をクリックして、他のアラーム入力チャンネルに設定をコピーします。
6. **Save**をクリックします。

6.2 スマートイベント

以下のステップでスマートイベントを設定します。

メモ

- 一部の機種では、はじめに**VCA Resource**画面でスマートイベント機能を有効にして機能設定画面を表示する必要があります。
- この機能は機種によって異なります。

6.2.1 オーディオ異常の検知

オーディオ異常は、音量の急激な増加や減少など、シーン内の異常な音を検知し、対応するためにいくつかの特定のアクションを実行します。

ステップ

1. 次の順に進みます。**Configuration → Event → Smart Event → Audio Exception Detection**
2. オーディオ異常検知の種類を1つまたは複数選択します。

   Audio Loss Exception

   オーディオトラックの突然の喪失を検知します。

   Sudden Increase of Sound Intensity Detection

   音の強さの急激な増加を検知します。**Sensitivity**と**Sound Intensity Threshold**は設定可能です。

メモ

- 感度が低いほど、検知を作動する音の変化が重要になります。
- 音の強度のしきい値は、検知のための音の強度の基準です。周囲の平均的な音の強さを設定することを推奨します。周囲の音が大きい程、値を大きくする必要があります。周囲の環境に応じて調整してください。

Sudden Decrease of Sound Intensity Detection

音の強さの急激な減少を検知します。**Sensitivity**は設定可能です。

3. スケジュールタイムの設定については**アーミングスケジュールの設定**を参照してください。リンケージメソッドの設定については**リンケージメソッドの設定**を参照してください。
4. **Save**をクリックします。

メモ

この機能は機種によって異なります。

6.2.2 シーンチェンジの検知

シーンチェンジ検知機能により、シーンの変化を検知します。アラームが作動した時、特定のアクションを実行します。

ステップ

1. 次の順に進みます。**Configuration → Event → Smart Event → Scene Change Detection**
2. **Enable**にチェックを入れます。
3. **Sensitivity**を設定します。値が高いほどシーンの変化で検知しやすくなります。検知精度は低下します。
4. スケジュールタイムの設定については**アーミングスケジュールの設定**を参照してください。リンケージメソッドの設定については**リンケージメソッドの設定**を参照してください。
5. **Save**をクリックします。

メモ

この機能は機種によって異なります。

6.2.3 侵入検知の設定

この機能はあらかじめ設定された仮想領域に侵入したり、往来する対象を検知します。これを検知すると、本機はリンケージアクションを実行します。

ステップ

1. 次の順に進みます。**Configuration → Event → Smart Event → Intrusion Detection**
2. **Enable**にチェックを入れます。

3. **Region**を選択します。検知領域の設定については**描画領域**を参照してください。
4. ルールを設定します。

Sensitivity 許容される対象の身体の一部が、あらかじめ設定された領域に入る割合を表します。感度＝100 - S1/ST × 100です。S1は、あらかじめ設定された領域を横切る対象の体の部位を表します。STは対象の全身を表します。感度の値が高いほどアラームが作動しやすくなります。

Threshold 対象が領域を往来している時間のしきい値を表します。1つの対象の滞在時間がしきい値を超えた時、アラームが作動します。しきい値の値が大きいほど、アラームの作動時間は長くなります。

図 6-3 ルールの設定

5. **オプション**：上記のステップを繰り返して、複数のエリアのパラメーターを設定できます。
6. アーミングスケジュールの設定については**アーミングスケジュールの設定**を参照してください。リンケージメソッドの設定については**リンケージメソッドの設定**を参照してください。
7. **Save**をクリックします。

6.2.4 ラインクロッシング検知の設定

この機能はあらかじめ設定された仮想線を横切る物体の検知に使用します。これを検知すると、本機はリンケージアクションを実行します。

ステップ

1. 次の順に進みます。**Configuration → Event → Smart Event → Line Crossing Detection**

2. **Enable**にチェックを入れます。
3. 1つの**Line**を選択し、サイズフィルターを設定します。サイズフィルターの設定については**サイズフィルターの設定**を参照してください。
4. **Draw Area**をクリックすると、ライブ映像に矢印のついた線が表示されます。ライブ映像の任意の場所に線をドラッグします。
5. ルールを設定します。

Direction 対象が線を越えていく方向を表します。

A<->B：設定されたラインを対象が両方向に横切った場合、それを検知してアラームが作動します。

A->B：設定されたラインをA側からB側へ横切る対象のみを検知します。

B->A：設定されたラインをB側からA側へ横切る対象のみを検知します。

Sensitivity 許容される対象の体の一部が、あらかじめ設定されたラインを越える割合を表します。感度＝100 - S1/ST × 100です。S1はあらかじめ設定されたラインを横切る対象の体の部位を表します。STは対象の全身を表します。感度の値が高いほどアラームが作動しやすくなります。

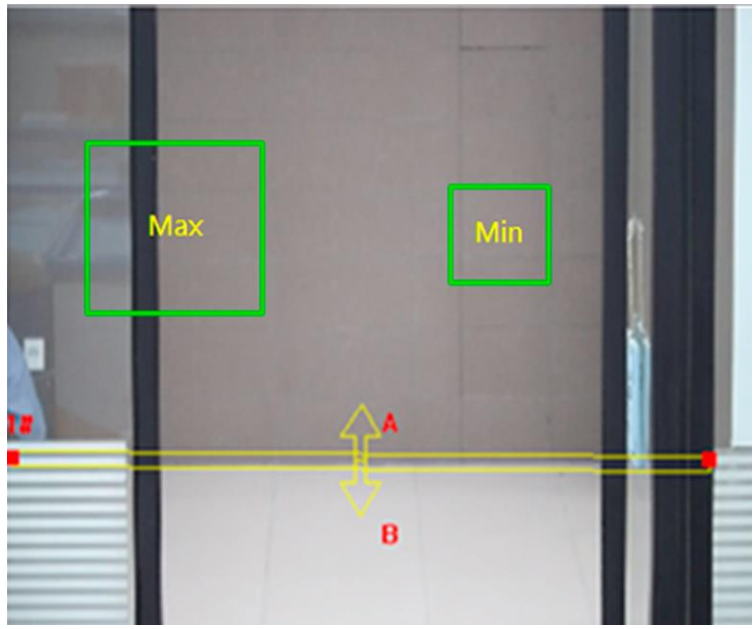


図 6-4 ルールの設定

6. **オプション**：上記のステップを繰り返して、複数のエリアのパラメーターを設定できます。
7. アーミングスケジュールの設定については**アーミングスケジュールの設定**を参照してください。リンケージメソッドの設定については**リンケージメソッドの設定**を参照してください。
8. **Save**をクリックします。

6.2.5 領域入口検知の設定

この機能は外からあらかじめ設定された仮想領域に入る対象を検知します。これを検知すると、本機はリンケージアクションを実行します。

ステップ

1. 次の順に進みます。**Configuration → Event → Smart Event → Region Entrance Detection**
2. **Enable**にチェックを入れます。
3. 1つの**Region**を選択します。領域の設定については**描画領域**を参照してください。
4. **Sensitivity**を設定します。

   Sensitivity 許容される対象の体の一部が、あらかじめ設定されたラインを越える割合を表します。感度＝100 - S1/ST × 100です。S1は、あらかじめ設定された領域を横切る対象の体の部位を表します。STは対象の全身を表します。感度の値が高いほどアラームが作動しやすくなります。

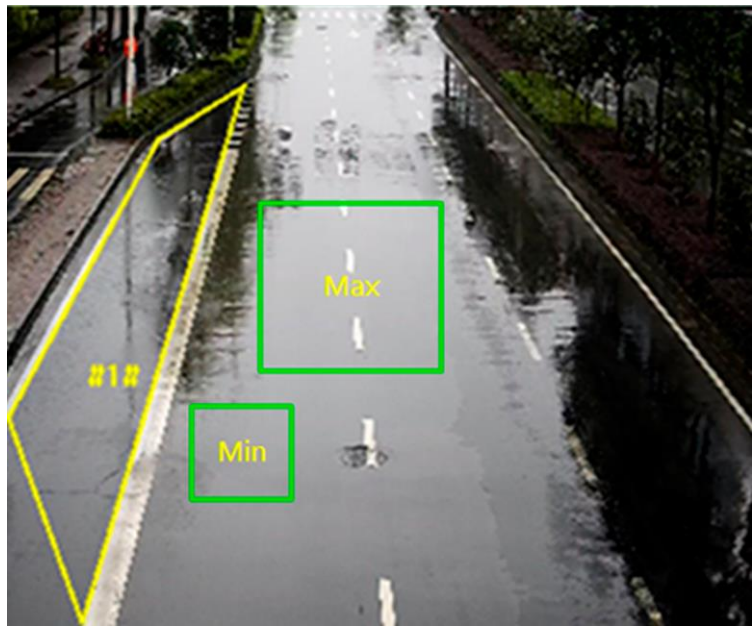


図 6-5 ルールの設定

5. **オプション**：上記のステップを繰り返して、複数のエリアのパラメーターを設定できます。
6. アーミングスケジュールの設定については**アーミングスケジュールの設定**を参照してください。リンケージメソッドの設定については**リンケージメソッドの設定**を参照してください。
7. **Save**をクリックします。

6.2.6 領域出口検知の設定

この機能はあらかじめ設定された仮想領域から退出する対象を検知します。これを検知すると、本機はリンケージアクションを実行します。

ステップ

1. 次の順に進みます。**Configuration → Event → Smart Event → Region Exiting Detection**
2. **Enable**にチェックを入れます。
3. 1つの**Region**を選択します。検知領域の設定については**描画領域**を参照してください。
4. **Sensitivity**を設定します。

Sensitivity 許容される対象の体の一部が、あらかじめ設定されたラインを越える割合を表します。感度＝100 - S1/ST × 100です。S1は、あらかじめ設定された領域を横切る対象の体の部位を表します。STは対象の全身を表します。感度の値が高いほどアラームが作動しやすくなります。

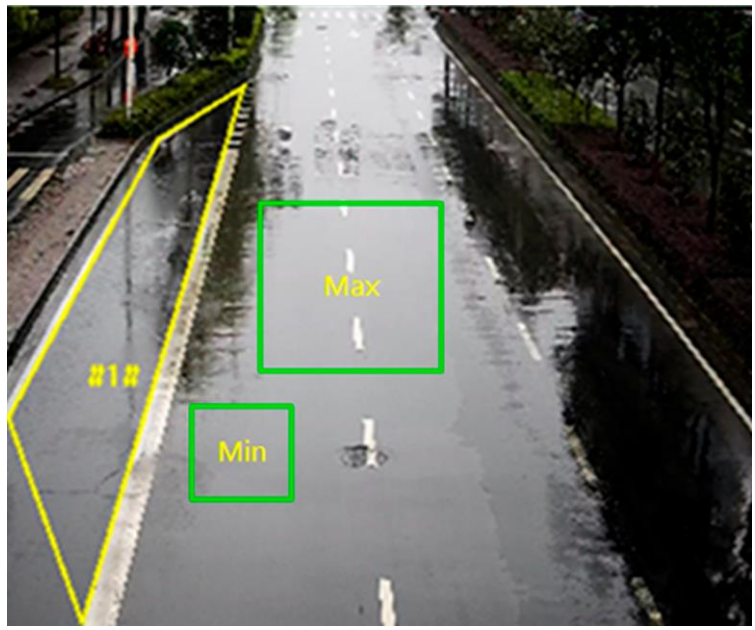


図 6-6 ルールの設定

5. **オプション**：上記のステップを繰り返して、複数のエリアのパラメーターを設定できます。
6. アーミングスケジュールの設定については**アーミングスケジュールの設定**を参照してください。リンケージメソッドの設定については**リンケージメソッドの設定**を参照してください。
7. **Save**をクリックします。

6.2.7 置き去り検知の設定

この機能はあらかじめ設定された領域内に放置された対象を検知します。リンケージメソッドは、対象物がその領域に一定時間放置された後、実行されます。

ステップ

1. 次の順に進みます。**Configuration → Event → Smart Event → Unattended Baggage Detection**
2. **Enable**にチェックを入れます。
3. 1つの**Region**を選択します。検知領域の設定については**描画領域**を参照してください。
4. ルールを設定します。

Sensitivity 許容される対象の身体の一部が、あらかじめ設定された領域に入る割合を表します。感度＝100 - S1/ST × 100です。S1は、あらかじめ設定された領域を横切る対象の体の部位を表します。STは対象の全身を表します。感度の値が高いほどアラームが作動しやすくなります。

Threshold 対象物が指定した領域に放置された時間です。アラームは、対象物がその領域に一定時間放置された後、実行されます。

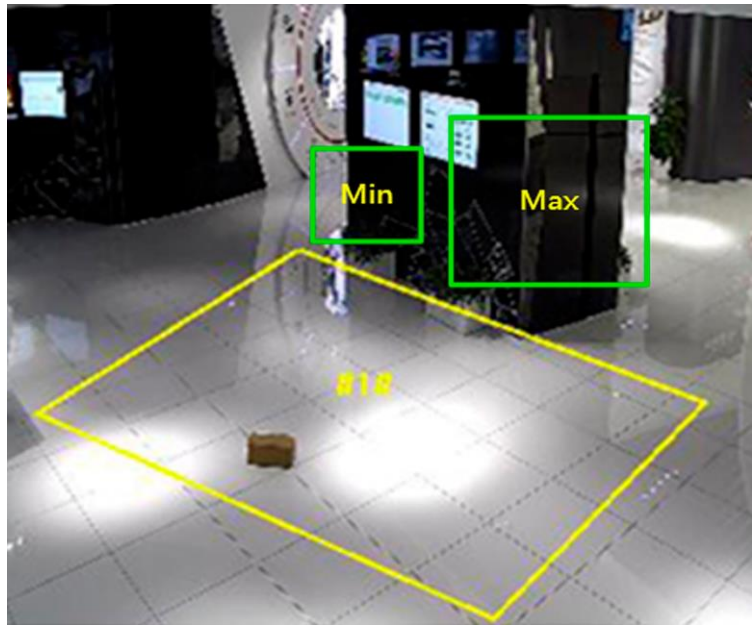


図 6-7 ルールの設定

5. **オプション**：上記のステップを繰り返して、複数のエリアのパラメーターを設定できます。
6. アーミングスケジュールの設定については**アーミングスケジュールの設定**を参照してください。リンケージメソッドの設定については**リンケージメソッドの設定**を参照してください。
7. **Save**をクリックします。

6.2.8 持ち去り検知の設定

この機能は展示されている展示物など、あらかじめ設定された検出領域から対象物が持ち出されたかどうかを検知します。これを検知すると、本機がリンケージアクションを実行し、スタッフが物損を減らす対策を講じることができます。

ステップ

1. 次の順に進みます。**Configuration → Event → Smart Event → Object Removal Detection**
2. **Enable**にチェックを入れます。
3. **Region**を選択します。領域の設定については**描画領域**を参照してください。
4. ルールを設定します。

   Sensitivity 許容される対象の身体の一部が、あらかじめ設定された領域から離れる割合を表します。

   感度＝100 - S1/ST*100です。

   S1は予め設定された領域から離れる対象の身体部位を表します。STは対象の全身を表します。

   例：値を60と設定した場合、対象の40%のボディ部分が領域から出た場合にのみ、対象が領域を離れたとしてカウントします。

   Threshold 領域から対象が持ち出された時刻です。値が10の場合、対象が10秒間領域から消えた後、アラームが作動します。
5. **オプション**：上記手順を繰り返し、他の領域を設定します。
6. アーミングスケジュールの設定については**アーミングスケジュールの設定**を参照してください。リンケージメソッドの設定については**リンケージメソッドの設定**を参照してください。
7. **Save**をクリックします。

メモ

この機能は一部の機種のみ対応しています。ディスプレイは機種によって異なります。

6.2.9 描画領域

ここでは、領域の設定について説明します。

ステップ

1. **Detection Area**をクリックします。
2. ライブビュー上でクリックして検知領域の境界を描き、右クリックで描画を完了します。
3. **Save**をクリックします。

メモ

- **Clear**をクリックすると、選択した領域がクリアされます。
- **Clear All**をクリックすると、あらかじめ設定されたすべての領域をクリアできます。

6.2.10 サイズフィルターの設定

ここでは、サイズフィルターの設定について説明します。サイズが最小値と最大値の間にある対象のみを検出し、アラームを作動させます。

ステップ

1. **Max. Size**をクリックし、ライブビュー内でマウスをドラッグして最大対象のサイズを描画します。
2. **Min. Size**をクリックし、ライブビュー内でマウスをドラッグして最小対象のサイズを描画します。
3. **Save**をクリックします。

第 7 章 ネットワーク設定

7.1 TCP/IP

ネットワーク上で本機を操作する前に、TCP/IPが正しく設定されている必要があります。IPv4、IPv6ともに対応しています。両バージョンは、互いに競合することなく同時に設定できます。

パラメーターの設定は次の順に進みます。**Configuration → Network → Basic Settings → TCP/IP**

NIC Type

ネットワーク状況に応じて、NIC（Network Interface Card）の種類を選択します。

IPv4

IPv4は2つのモードが用意されています。

DHCP

DHCPにチェックを入れると、本機が自動的にネットワークからIPv4パラメーターを取得します。この機能を有効にすると、本機のIPアドレスが変更されます。SADPを使用して、本機のIPアドレスを取得できます。

メモ

本機が接続されるネットワークがDHCP（Dynamic Host Configuration Protocol）に対応している必要があります。

Manual

本機のIPv4パラメーターを手動で設定できます。**IPv4 Address**、**IPv4 Subnet Mask**、**IPv4 Default Gateway**を入力し、**Test**をクリックすると、IPアドレスが使用可能か確認できます。

IPv6

IPv6モードは3種類用意されています。

Route Advertisement

IPv6アドレスは、ルートアドバタイズメントと本機のMacアドレスを組み合わせて生成されます。

メモ

ルートアドバタイズメントモードでは、本機が接続されているルーターからのサポートが必要です。

DHCP

IPv6アドレスは、サーバー、ルーター、ゲートウェイから割り当てられます。

Manual

IPv6 Address、**IPv6 Subnet**、**IPv6 Default Gateway**を入力します。必要な情報はネットワーク管理者にご確認ください。

MTU

Maximum Transmission Unitの略です。単一のネットワーク層トランザクションで通信可能な最大プロトコルデータ単位のサイズです。

MTUの有効な値域は、1280～1500です。

DNS

ドメインネームサーバーのことです。ドメイン名で本機にアクセスする必要がある場合に必要です。一部のアプリケーション（電子メールの送信など）にも必要です。必要であれば、**Preferred DNS Server**と**Alternate DNS server**を適切に設定します。

Dynamic Domain Name

Enable Dynamic Domain Nameにチェックを入れ、**Register Domain Name**を入力します。ローカルエリアネットワーク内での管理を容易にするため、登録されたドメイン名で本機に登録します。

メモ

Dynamic Domain Nameを有効にするには、**DHCP**を有効にする必要があります。

7.1.1マルチキャスト

マルチキャストとは、複数のデバイスに対して同時にデータ送信を行うグループ通信のことです。

マルチキャストの設定は次の順に進みます。**Configuration → Network → Basic Settings → Multicast**

IP Address

マルチキャストホストのアドレスです。

Stream Type

マルチキャストソースとなるストリームタイプ

Video Port

選択したストリームのビデオポートです。

Audio Port

選択したストリームのオーディオポートです。

7.1.2マルチキャストディスカバリー

Enable Multicast Discoveryにチェックを入れ、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、クライアントソフトウェアでオンラインネットワークカメラが自動的に検知されます。

7.2 SNMP

SNMPネットワーク管理プロトコルを設定して、ネットワーク伝送でアラームイベントと異常メッセージを取得できます。

ご使用の前に

SNMPを設定する前に、SNMPソフトウェアをダウンロードし、SNMPポート経由で機器情報を受信できるように管理する必要があります。

ステップ

1. 設定画面へ進みます。**Configuration → Network → Advanced Settings → SNMP**
2. **Enable SNMPv1**、**Enable SNMPv2c**、**SNMPv3**にチェックを入れます。

メモ

選択するSNMPのバージョンは、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う必要があります。SNMP v1は安全ではなく、SNMP v2はアクセスにパスワードが必要です。SNMP v3は暗号化を提供しており、このバージョンを使用する場合、HTTPSプロトコルを有効にする必要があります。

3. SNMPを設定します。
4. **Save**をクリックします。

7.3 SRTPの設定

Secure Real-time Transport Protocol（SRTP）は、Real-time Transport Protocol（RTP）インターネットプロトコルで、ユニキャストとマルチキャストの両方のアプリケーションにおいて、RTPデータの暗号化、メッセージ認証と整合性、リプレイ攻撃防止を提供することを目的としています。

ステップ

1. 次の順に進みます。**Configuration → Network → Advanced Settings → SRTP**
2. **Server Certificate**を選択します。
3. **Encrypted Algorithm**を選択します。
4. **Save**をクリックします。

メモ

- この機能は一部の機種のみ対応しています。
- この機能に異常がある場合は、証明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。

7.4 ポートマッピング

ポートマッピングを設定すると、指定したポートから本機にアクセスできます。

ご使用の前に
本機のポートがネットワーク上のほかのデバイスと同じ場合は、**ポート**を参照して、本機のポートを変更してください。

ステップ
1. 次の順に進みます。**Configuration → Network → Basic Settings → NAT**
2. ポートマッピングモードを選択します。

Auto Port Mapping	詳しくは**オートポートマッピングの設定**を参照してください。
Manual Port Mapping	詳しくは**マニュアルポートマッピングの設定**を参照してください。

3. **Save**をクリックします。

7.4.1 オートポートマッピングの設定

ステップ
1. **Enable UPnP™**にチェックを入れ、カメラのフレンドリーネームを選択するか、デフォルトの名前を使用します。
2. ポートマッピングモードを**Auto**に選択します。
3. **Save**をクリックします。

メモ
ルーターのUPnP™機能を同時に有効にする必要があります。

7.4.2 マニュアルポートマッピングの設定

ステップ
1. **Enable UPnP™**にチェックを入れ、本機のフレンドリーネームを選択するか、デフォルトの名前を使用します。
2. マッピングモードを**Manual**に選択し、外部ポートを内部ポートと同じ設定にします。
3. **Save**をクリックします。

次に行うことは
ルーターのポートマッピング設定インターフェースに進み、ポート番号とIPアドレスを本機のものと同じに設定します。詳しくは、ルーターの取扱説明書を参照してください。

7.4.3 ルーターにポートマッピングを設定

以下はルーターでの設定です。ルーターの機種によって、設定内容は異なります。

ステップ
1. **WAN Connection Type**を選択します。

2. **IP Address**、**Subnet Mask**とその他のルーターのネットワークパラメーターを設定します。
3. **Forwarding → Virtual Severs**の順に進み、**Port Number**と**IP Address**を入力します。
4. **Save**をクリックします。

例：
カメラが同じルーターに接続されている場合、一方のカメラのIPアドレスを192.168.1.23、ポート番号を80、8000、554と設定し、別のカメラのIPアドレスを192.168.1.24、ポート番号を81、8001、555、8201と設定します。

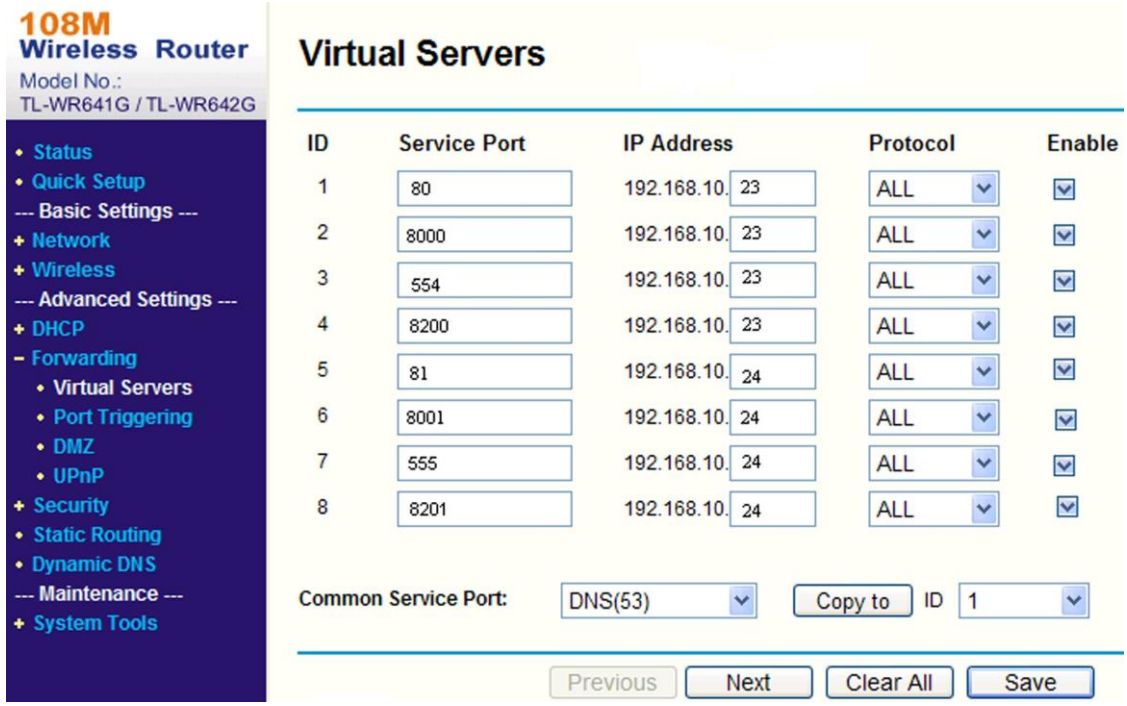


図 7-1 ルーター上のポートマッピング

メモ
ネットワークカメラのポートは他のポートと競合できません。例えば、ルーターのウェブ管理ポートが80の場合です。カメラポートが管理ポートと同じ場合は変更します。

7.5 ポート

ポートの競合により本機がネットワークにアクセスできない場合、本機のポートを変更します。

注意
デフォルトのポートパラメーターを変更すると、本機がアクセスできなくなりますので変更しないでください。

ポート設定は次の順に進みます。**Configuration → Network → Basic Settings → Port**

HTTP Port

ブラウザが本機にアクセスする際のポートです。たとえば、HTTP Portが81に変更されている場合は、ログインのブラウザに**http://192.168.1.64:81**と入力する必要があります。

HTTPS Port

ブラウザが証明書を持つデバイスにアクセスするポートです。安全なアクセスを確保するために、証明書による認証が必要です。

RTSP Port

リアルタイムストリーミングプロトコルのポートです。

SRTP Port

セキュアリアルタイムトランスポートプロトコルのポートです。

Server Port

クライアントがデバイスを追加する際のポートです。

Enhanced SDK Service Port

クライアントがデバイスを追加する際のポートです。安全なアクセスを確保するために、証明書による認証が必要です。

WebSocket Port

TCPベースの全二重通信プロトコルポートで、プラグインフリープレビューが可能です。

WebSockets Port

TCPベースの全二重通信プロトコルポートで、プラグインフリープレビューが可能です。安全なアクセスを確保するために、証明書による認証が必要です。

メモ

- Enhanced SDK Service Port、WebSocket Port、WebSocket Portは一部の機種のみ対応しています。
- その機能に対応した機種では、**Configuration → Network → Advanced Settings → Network Service**の順に進み、ポートを有効にします。

7.6 ドメイン名によるデバイスへのアクセス

Dynamic DNS (DDNS) を使用してネットワークにアクセスですることがきます。本機のダイナミックIPアドレスをドメインネームリゾルーションサーバーにマッピングすることで、ドメイン名によるネットワークにアクセスできます。

ご使用の前に

本機のDDNS設定を行う前に、DDNSサーバーへの登録が必要です。

ステップ

1. DNSパラメーターの設定は**TCP/IP**を参照してください。
2. DDNSの設定画面に進みます。次の順に進みます。**Configuration → Network → Basic Settings → DDNS**
3. **Enable DDNS**にチェックを入れ、**DDNS type**を選択します。

DynDNS

ドメイン名の解決にはDynamic DNSサーバーが使用されます。

NO-IP

ドメイン名の解決にはNO-IPサーバーが使用されます。

4. ドメイン名情報を入力し、**Save**をクリックします。
5. 本機のポートとポートマッピングを確認します。**ポート**を参照し、本機のポートを確認してください。また、ポートマッピングの設定は**ポートマッピング**を参照してください。
6. 本機にアクセスします。

By Browsers	ブラウザのアドレスバーにドメイン名を入力し、本機にアクセスします。
By Client Software	クライアントソフトウェアにドメイン名を追加します。特定の追加方法については、クライアントマニュアルを参照してください。

7.7 PPPoEダイヤルアップ接続によるデバイスへのアクセス

本機は、PPPoEオートダイヤルアップ機能に対応しています。本機はモデムに接続後、ADSLダイヤルアップでパブリックIPアドレスを取得します。本機のPPPoEパラメーターを設定する必要があります。

ステップ

1. 次の順に進みます。**Configuration → Network → Basic Settings → PPPoE**
2. **Enable PPPoE**にチェックを入れます。
3. PPPoEパラメーターを設定します。

Dynamic IP

ダイヤルアップに成功すると、WANのダイナミックIPアドレスが表示されます。

User Name

ダイヤルアップネットワークアクセス用のユーザー名です。

Password

ダイヤルアップネットワークアクセス用のパスワードです。

Confirm

ダイヤルアップパスワードを再度入力します。

4. **Save**をクリックします。
5. 本機にアクセスします。

By Browsers	ブラウザのアドレスバーにWANダイナミックIPアドレスを入力し、本機にアクセスします。
By Client Software	クライアントソフトウェアにWANダイナミックIPアドレスを追加します。詳しくは、クライアントマニュアルを参照してください。

メモ

取得したIPアドレスはPPPoEで動的に割り当てられるため、カメラを再起動すると必ずIPアドレスが変更されます。動的IPの不便さを解消するには、DDNSプロバイダー（例：DynDns.com）からドメイン名を取得する必要があります。詳しくは**ドメイン名によるデバイスへのアクセス**を参照してください。

7.8 ワイヤレスダイヤル

オーディオ、ビデオ、画像のデータを3G/4Gワイヤレスネットワーク経由で転送できます。

メモ

この機能は一部の機種のみ対応しています。

7.8.1 ワイヤレスダイヤルの設定

内蔵のワイヤレスモジュールにより、本機のインターネットへのダイヤルアップ接続ができます。

ご使用の前に

SIMカードを入手し、3G/4Gサービスを起動します。SIMカードを対応するスロットに挿入します。

ステップ

1. 次の順に進みます。**Configuration → Network → Advanced Settings → Wireless Dial**
2. 機能を有効にします。
3. **Dial Parameters**をクリックして、パラメーターを設定し保存します。
4. **Dial Plan**をクリックします。詳しくは**アーミングスケジュールの設定**を参照してください。
5. **Dial Status**をクリックします。

   Click Refresh　ダイヤルステータスをリフレッシュします。

   Click Disconnect　3G/4Gのワイヤレスネットワークを切断します。

   Dial Statusが**Connected**に変わると、ダイヤル設定が成功したことを意味します。
6. ネットワーク上のパソコンの**IP Address**を経由して本機にアクセスします。
   - ブラウザでIPアドレスを入力し、本機にアクセスします。
   - クライアントアプリケーションにデバイスを追加します。**IP/Domain**を選択し、IPアドレスと他のパラメーター入力しすると本機にアクセスします。
7. (オプション）4Gカード情報、ネットワークキャリア情報を**Auxiliary Function**で見ることができます。
   - (オプション）**Re-Camp**をクリックして、ネットワークに再接続できます。本機は機内モードを10秒間維持した後、自動的にネットワークに接続します。

7.8.2 受信許可リストの設定

本機からのアラームメッセージを受信するために、管理者の携帯電話番号を受信許可リストに追加します。

ステップ

1. 受信許可リスト設定画面に進みます。次の順に進みます。**Configuration → Advanced Configuration → Wireless Dial → Allowlist**
2. **Enable SMS Alarm**にチェックを入れます。
3. 受信許可リストの+をクリックします。
   1) アラームメッセージを受信する携帯電話番号を入力します。
   2) **Reboot via SMS**にチェックを入れます。
   3) 特定のイベントを選択すると、そのイベントが発生したときに携帯電話でアラームメッセージを受信することができます。
   4) **Save**をクリックします。
   5) **オプション**：複数の受信者を設定する場合は、上記の手順を繰り返します。

	受信許可リストパラメーターを変更します。
	すでに設定されている受信許可リストを削除します。
Send Test SMS	テスト用に携帯電話にメッセージを送信します。

4. **Save**をクリックします。

7.8.3 ワイヤレスエキスパートの設定

ワイヤレスエキスパート設定は、本機が接続する3G/4Gワイヤレスネットワークの詳細を提供し、専門家が潜在的なネットワーク問題のトラブルシューティングを支援します。

セル無線周波数パラメーター

セル無線周波数パラメーターは、本機が接続されている現在の無線ネットワーク情報を提供します。

Configuration → Network → Basic Settings → Wireless Expert Settingsの順に進むと、セル無線周波数パラメーターが表示されます。

Network Info

現在のセルラーネットワーク情報が表示されます。**Refresh**をクリックすると、異なるセルの周波数情報を見ることができます。

Radio Frequency Fluctuation

過去7日間に本機が接続したセルラーネットワークの変動を記録します。**Export Report**をクリックして、変動報告書を書き出す暗号化パスワードを設定し、確認してください。

周波数の固定

ネットワーク速度を向上させるために、本機がより速いデータレートを得る周波数を固定することができます。

ステップ

1. 次の順に進みます。**Configuration → Network → Basic Settings → Wireless Expert Settings → Advanced Settings → Lock Band**
2. **Enable**にチェックを入れます。
3. **Add**をクリックして、その周波数帯に入ります。

メモ

- 入力する周波数は、B＋数字またはN＋数字にしてください。例えば、B1やN1などを入力します。
- 最大5バンドまで対応しています。

4. **オプション**：をクリックすると選択した周波数が削除されます。**Clear All**をクリックして、そのリストをクリアすることもできます。

キャプチャベースバンドパケット

この機能は、プロトコルの相互作用パケットをキャプチャし、専門家が4Gモジュールと基地局間の通信障害の場所を特定するのに役立ちます。

ステップ

メモ

この機能は、専門家とテクニカルサポートスタッフのために用意されています。

1. 次の順に進みます。**Configuration → Network → Basic Settings → Wireless Expert Settings → Advanced Settings → Maintenance**
2. **Capture Baseband Packet**をクリックして、設定インターフェースに入ります。
3. **Capture Baseband Packet**にチェックを入れます。
4. キャプチャの持続時間と保存パスを設定します。保存パスは、本機の実際の保存方法によって異なります。**Delete Captured Packet Under This Path**をクリックして、キャプチャしたパケットを削除することができます。
5. **Save**をクリックします。
6. **Start Capture**をクリックすると、ベースバンドパケットをキャプチャします。
7. **オプション**：**Stop Capture**をクリックすると、キャプチャ処理を停止します。
8. **Export**をクリックします。
9. **OK**をクリックして、このインターフェースを終了します。

スピードテスト

ステップ

1. 次の順に進みます。**Configuration → Network → Basic Settings → Wireless Expert Settings → Advanced Settings → Maintenance**
2. **Speed Test**をクリックして、設定インターフェースに入ります。
3. デフォルトサーバーを選択するか、サーバーアドレスを入力します。以下の手順で、近くのサーバーアドレスを取得することができます。

   メモ

   以下の手順で、近くのサーバーアドレスを取得することができます。

   a. このサイトにアクセスすると、近くのサーバーのアドレスが表示されます：***https://www.speedtest.net/speedtest- servers-static.php***

   b. 近くのスピードテストステーションのURLを選択して、**Server Address**にコピーします。

4. Speed Testをクリックしてテストを開始します。

   テスト終了後にスピードの詳細を確認することができます。**Export Report**をクリックして確認することもできます。

7.9 トラフィックシェーピング

トラフィックシェーピングは、送信前にビデオデータパケットを整形し、滑らかにするために使用されます。

ネットワークの混雑による遅延やパケットロスを改善し、映像品質も確保することができます。シェーピングレベルは設定可能です。

7.10 データモニタリング

本機で使用しているSIMカードデータや有線ネットワークデータを閲覧・管理することができます。SIMカードのデータはネットワークキャリアが提供するデータサービスで、有線ネットワークのデータは通常4Gルーターを通じて提供されます。

ステップ

1. 次の順に進みます。**Configuration → Network → Advanced Settings → Data Monitoring**
2. **Enable**にチェックを入れます。
3. データプランに応じて、以下のパラメーターを設定します。

   Plan Type

   Daily、**Monthly**或いは**Annually**を選択できます。

   Data Plan

   使用可能なデータ量を入力し、単位を選択します。

   Pre-Alarm Threshold

使用データがデータプランの設定した割合に達すると、本機はアラームメッセージを送信し、OSDまたはポップアップウィンドウに通知を表示します。

4. **Normal Linkage**を選択します。
   Send Emailまたは**Notify Surveillance Center**を選択した場合、使用データがしきい値に達すると、メールまたは監視センターへアラームメッセージを送信します。
5. **Save**をクリックします。

メモ

この機能は機種によって異なります。

7.11 ネットワークサービスの設定

特定のプロトコルのON/OFFステータスを任意にコントロールできます。

ステップ

メモ

この機能は機種によって異なります。

1. 次の順に進みます。**Configuration → Network → Advanced Settings → Network Service**
2. ネットワークサービスを設定します。

WebSocket & WebSockets

Google Chrome 57以上のバージョン、Mozilla Firefox 52以上のバージョンを使用して本機にアクセスする場合、WebSocketまたはWebSocketプロトコルを有効にする必要があります。これらを有効にしないと、ライブビュー、イメージキャプチャ、デジタルズームなどの機能を使用することはできません。
本機がHTTPを使用する場合は、WebSocketを有効にします。
本機がHTTPSを使用する場合は、WebSocketsを有効にします。
WebSocketsを使用する場合は、**Server Certificate**選択します。

メモ

サーバー証明書を選択する前に、証明書管理を完了させてください。詳しくは**証明書の管理**を参照してください。

SDKサービスおよびエンハンストSDKサービス

Enable SDK Serviceにチェックを入れ、SDKプロトコルでクライアントソフトに本機を追加します。
Enable Enhanced SDK Serviceにチェックを入れ、SDK over TLSプロトコルでクライアントソフトに本機を追加します。
エンハンストSDKサービスを使用する場合は、**Server Certificate**を選択します。

メモ

- サーバー証明書を選択する前に、証明書管理を完了させてください。詳しくは**証明書の管理**を参照してください。
- 本機とクライアントソフトウェアの接続を設定する場合、Enhanced SDK Serviceを使用し、データ通信を暗号化するArming Modeで通信することを推奨します。アーミングモードの設定は、クライアントソフトウェアのユーザーマニュアルを参照してください。

TLS (Transport Layer Security)

本機はTLS1.1、TLS1.2、TLS1.3を提供ます。必要に応じて、1つまたは複数のプロトコルのバージョンを有効にしてください。

Bonjour

このチェックを外すと、プロトコルを無効にすることができます。

3. **Save**をクリックします。

7.12 オープンネットワークビデオインターフェースの設定

Open Network Video Interfaceプロトコルで本機にアクセスする必要がある場合は、ユーザー設定を行うことでネットワークセキュリティを強化できます。

ステップ

1. 次の順に進みます。**Configuration → Network → Advanced Settings → Integration Protocol**
2. **Enable Open Network Video Interface**にチェックを入れます。
3. **Add**をクリックして、オープンネットワークビデオインターフェースのユーザーを設定します。

   Delete 選択したオープンネットワークビデオインターフェースのユーザーを削除します。

   Modify 選択したオープンネットワークビデオインターフェースのユーザーを変更します。
4. **Save**をクリックします。
5. **オプション**：上記の手順を繰り返して、さらにオープンネットワークビデオインターフェースのユーザーを追加します。

7.13 アラームサーバーの設定

本機は、HTTP、HTTPS、ISUPプロトコルを介して、宛先IPアドレスやホスト名にアラームを送信できます。目的のIPアドレスまたはホスト名は、HTTP、HTTP、またはISUPのデータ伝送をサポートしている必要があります。

ステップ

1. 次の順に進みます。**Configuration → Network → Advanced Settings → Alarm Server**
2. **Destination IP**、**Host Name**、**URL**、**Port**を入力します。
3. **オプション**：**Enable**にチェックを入れ、ANRを有効にします。
4. **Protocol**を選択します。

メモ

HTTP、HTTPS、ISUPが選択可能です。通信時のデータ転送を暗号化するため、HTTPSの利用を推奨します。

5. **Test**をクリックして、そのIPまたはホストが利用可能かどうか確認します。
6. **Save**をクリックします。

7.14 ISUPの設定

ISUPプラットフォーム（旧Ehome）に本機を登録すると、公衆回線から本機へのアクセス・管理、データ送信、アラーム情報の転送が可能になります。

ステップ

1. 次の順に進みます。**Configuration → Network → Advanced Settings → Platform Access**
2. **ISUP**はプラットフォームアクセスモードに選択します。
3. **Enable**を設定します。
4. プロトコルのバージョンを選択し、関連するパラメーターを入力します。
5. **Save**をクリックします。

   この機能が正しく設定されると、レジスターステータスが**Online**に変わります。

7.15 Hik-Connectでカメラにアクセス

Hik-Connectはモバイル端末向けのアプリケーションです。アプリを使えば、ライブ映像を見たり、アラーム通知などを受け取ることができます。

ご使用の前に

ネットワークケーブルでカメラをネットワークに接続します。

ステップ

1. 以下の手順でHik-Connectアプリケーションを入手し、インストールしてください。
   - ***https://appstore.hikvision.com/***にアクセスして、お使いの携帯電話のシステムに合わせてアプリケーションをダウンロードします。
   - 当社のオフィシャルサイトをご覧ください。次の順に進みます。**Support → Tools → Hikvision App Store**
   - 下記のQRコードを読み取り、アプリケーションをダウンロードしてください。

メモ

インストール時に「Unknown app」などのエラーが発生した場合は2つの方法で問題を解決します。

- ***https://appstore.hikvision.com/static/help/index.html***にアクセスして、トラブルシューティングを参照してください。
- ***https://appstore.hikvision.com/***にアクセスして、インターフェースの右上の**Installation Help**をクリックし、トラブルシューティングを参照してください。

2. アプリケーションを起動し、Hik-Connectのユーザーアカウントを登録します。
3. 登録後、ログインします。
4. アプリで右上の「＋」をタップし、カメラのQRコードを読み取ってカメラを追加します。QRコードは、カメラ本体、または同梱のカメラのクイックスタートガイドの表紙に記載されています。
5. 画面の指示に従って、ネットワーク接続を設定し、カメラをHik-Connectのアカウントに追加します。

詳細については、「Hik-Connect」アプリの取扱説明書を参照してください。

7.15.1カメラのHik-Connectサービスを有効にする

Hik-Connectサービスを利用する前に、カメラ側でHik-Connectサービスを有効にしておく必要があります。SADPソフトウェアまたはWebブラウザからサービスを有効にすることができます。

Webブラウザで Hik-Connectを有効にする

以下の手順に従って、WebブラウザからHik-Connectサービスを有効にします。

ご使用の前に

このサービスを有効にする前に、カメラを起動する必要があります。

ステップ

1. Webブラウザでカメラにアクセスします。
2. プラットフォームアクセス設定インタフェースに入ります。**Configuration → Network → Advanced Settings → Platform Access**
3. **Platform Access Mode**はHik-Connectを選択します。
4. **Enable**にチェックを入れます。
5. ポップアップウィンドウの「Terms of Service」と「Privacy Policy」をクリックして、内容をご確認ください。
6. カメラの認証コードを作成するか、古い認証コードを変更します。

メモ

認証コードは、カメラをHik-Connectサービスに追加する際に必要となります。

7. 設定を保存します。

SADPソフトウェアでHik-Connectサービスを有効にする

ここでは、起動したカメラのSADPソフトウェアからHik-Connectサービスを有効にする方法を説明します。

ステップ

1. SADPソフトを起動します。
2. カメラを選択し、**Modify Network Parameters**ページに入ります。
3. **Enable Hik-Connect**にチェック入れます。
4. 認証コードを作成するか、古い認証コードを変更します。

メモ

認証コードは、カメラをHik-Connectサービスに追加する際に必要となります。

5. 「Terms of Service」と「Privacy Policy」をクリックして、内容をご確認ください。
6. 設定を確認します。

7.15.2 Hik-Connectのセットアップ

ステップ

1. 以下の手順でHik-Connectアプリケーションを入手し、インストールしてください。
   - ***https://appstore.hikvision.com***にアクセスして、お使いの携帯電話のシステムに合わせてアプリケーションをダウンロードします。
   - 当社のオフィシャルサイトをご覧ください。次の順に進みます。**Support → Tools → Hikvision App Store**
   - 下記のQRコードを読み取り、アプリケーションをダウンロードしてください。

メモ

インストール時に「Unknown app」などのエラーが発生した場合は2つの方法で問題を解決します。

- ***https://appstore.hikvision.com/static/help/index.html***にアクセスして、トラブルシューティングを参照してください。
- ***https://appstore.hikvision.com/***にアクセスして、インターフェースの右上の**Installation Help**をクリックし、トラブルシューティングを参照してください。

2. アプリケーションを起動し、Hik-Connectのユーザーアカウントを登録します。
3. 登録後、ログインします。

7.15.3 Hik-Connectにカメラを追加

ステップ

1. モバイル端末をWi-Fiに接続します。
2. Hik-Connectアプリにログインします。
3. ホーム画面で、右上の「＋」をタップして、カメラを追加します。
4. カメラ本体またはクイックスタートガイドの表紙にあるQRコードを読み取ります。

メモ

QRコードがない、またはぼやけていて認識できない場合は、カメラの製造番号を入力して追加することもできます。

5. カメラの認証コードを入力します。

メモ

- 必要な認証コードは、カメラでHik-Connectサービスを有効にしたときに作成または変更したコードです。
- 認証コードを忘れた場合、Webブラウザから**Platform Access**設定ページの現在の認証コードを確認できます。

6. ポップアップインターフェースの**Connect to a Network**をタップします。
7. カメラの機能に応じて**Wired Connection**または**Wireless Connection**を選択します。

Wireless Connection	携帯電話が接続しているWi-Fiのパスワードを入力し、 **Next**をタップするとWi-Fi接続処理を開始します。(Wi-Fi設定時にルーターから3m以内にカメラを設置してください)。
Wired Connection	カメラとルーターをネットワークケーブルで接続し、リザルトインターフェイスの**Connected**をタップします。

メモ

ルーターは、携帯電話が接続されているものと同じでなければなりません。

8. 次のインターフェースの**Add**をタップして追加を終了します。
詳細については、「Hik-Connect」アプリの取扱説明書を参照してください。

第8章 アーミングスケジュールとアラームリンケージ

アーミングスケジュールとは、本機が特定のタスクを実行する時間帯をカスタマイズしたものです。アラームリンケージとは、検知された特定の出来事や対象に対して、予定された時間内に対応することです。

8.1 アーミングスケジュールの設定

本機のタスクの有効時間を設定します。

ステップ

1. **Arming Schedule**をクリックします。
2. タイムバーをドラッグして、希望の有効時間を描画します。

   メモ

   1日に最大8つの時間帯を設定できます。
3. 時間帯を調整します。
   - 選択した時間帯をクリックし、希望の値を入力します。**Save**をクリックします。
   - 選択した時間帯をクリックします。端点をドラッグして時間帯を調整します。
   - 選択した時間帯をクリックし、タイムバー上にドラッグします。
4. **オプション**：**Copy to...**をクリックして、同じ設定を他の日にコピーします。
5. **Save**をクリックします。

8.2 リンケージメソッドの設定

イベントやアラームが発生したとき、リンケージ機能が有効になります。

8.2.1 アラーム出力の作動

本機がアラーム出力デバイスと接続され、アラーム出力番号が設定されている場合、アラームが作動すると、本機は接続されているアラーム出力デバイスにアラーム情報を送信します。

ステップ

メモ

この機能は一部の機種のみ対応しています。

1. 次の順に進みます。**Configuration → Event → Basic Event → Alarm Output**
2. アラーム出力パラメーターを設定します。

   Automatic Alarm　この設定に関する情報は**自動アラーム**を参照してください。

Manual Alarm　　この設定に関する情報は**手動アラーム**を参照してください。

3. **Save**をクリックします。

手動アラーム

アラーム出力を手動で作動できます。

ステップ

1. 手動アラームのパラメーターを設定します。

   Alarm Output No.

   外部アラームデバイスに接続されているアラームインターフェースに応じて、アラーム出力番号を選択します。

   Alarm Name

   アラーム出力の名称を編集します。

   Delay

   Manualを選択します。

2. **Manual Alarm**をクリックすると、手動アラーム出力が有効になります。
3. **オプション**：**Clear Alarm**をクリックすると、手動アラーム出力が無効になります。

自動アラーム

自動アラームパラメーターを設定すると、設定されたアーミングスケジュールで本機がアラーム出力を自動的に作動します。

ステップ

1. 自動アラームのパラメーターを設定します。

   Alarm Output No.

   外部アラームデバイスに接続されているアラームインターフェースに応じて、アラーム出力番号を選択します。

   Alarm Name

   アラーム出力の名前をカスタマイズします。

   Delay

   アラーム発生後、アラーム出力が持続する時間です。

2. アーミングスケジュールを設定します。この設定の情報については**アーミングスケジュールの設定**を参照してください。
3. **Copy to…**をクリックすると、他のアラーム出力チャンネルにパラメーターをコピーできます。
4. **Save**をクリックします。

8.2.2 FTP/NAS/メモリーカードへのアップロード

FTP/NAS/メモリーカードへのアップロードを有効に設定した場合、アラームが作動されると、本機はFTPサーバー、ネットワーク接続ストレージ、メモリーカードにアラーム情報を送信します。

FTPサーバーの設定は**FTPを設定する**を参照してください。

NASの設定は**NASを設定する**を参照してください。

メモリーカードのストレージの設定は**新しいメモリーカードや暗号化されていないメモリーカードの設定**を参照してください。

8.2.3 電子メールの送信

Send Emailにチェックを入れると、本機がアラームイベントを検知したとき、指定されたアドレスにアラーム情報を記載した電子メールを送信します。
電子メールの設定については**電子メールの設定**を参照してください。

電子メールの設定

電子メールが設定され、**Send Email**がリンケージメソッドとして有効な場合、アラームイベントが検知されると、本機は指定されたすべての受信者に電子メールで通知を送信します。

ご使用の前に
電子メール機能を使用する前に、DNSサーバーを設定してください。DNS設定は次の順に進みます。
Configuration → Network → Basic Settings → TCP/IP

ステップ
1. 電子メール設定画面に進みます。**Configuration → Network → Advanced Settings → Email**
2. 電子メールのパラメーターを設定します。
   1) **Sender's Address**、**SMTP Server**、**SMTP Port**を含む、送信者の電子メール情報を入力します。
   2) **オプション**：メールサーバーで認証が必要な場合は、**Authentication**にチェックを入れ、ユーザー名とパスワードを入力してサーバーにログインしてください。
   3) **E-mail Encryption**を設定します。
      - **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、電子メールが送信されます。SMTPポートは465に設定してください。
      - **SSL**、**TLS**、**Enable STARTTLS**を選択した場合、電子メールはSTARTTLSで暗号化された後、送信されます。SMTPポートは25に設定する必要があります。

メモ

STARTTLSを使用する場合、そのプロトコルがメールサーバーでサポートされていることを確認してください。プロトコルがメールサーバーでサポートされていない場合、**Enable STARTTLS**にチェックを入れると電子メールは暗号化されずに送信されます。

4) **オプション**：アラーム画像付きで通知を受け取りたい場合は、**Attached Image**にチェックを入れてください。この通知メールには、イベントに関する3枚のアラーム画像が添付されます。画像のキャプチャ間隔も設定可能です。
5) 受信者の氏名や住所など、受信者情報を入力します。
6) **Test**をクリックして、正しく設定されているか確認します。

3. **Save**をクリックします。

8.2.4 監視センターへの通知

Notify Surveillance Centerにチェックを入れると、アラームイベントが検知されたとき、アラーム情報を監視センターにアップロードします。

8.2.5 トリガーレコーディング

Trigger Recordingにチェックを入れると、検知されたアラームイベントに関する映像を録画します。録画設定については**ビデオ録画と画像キャプチャ**を参照してください。

8.2.6 音声による警告

Audible Warningを有効にし、**Audible Alarm Output**を設定した後、アラームが発生すると、本機の内蔵スピーカーまたは接続した外部スピーカーから警告音が出ます。
音声アラームの出力設定については、**音声アラームの出力設定**を参照してください。

メモ

この機能は一部のカメラ機種のみ対応しています。

音声アラーム出力の設定

本機が検知エリア内で対象を検知すると、警告として音声アラームが作動します。

ステップ

1. 次の順に進みます。**Configuration → Event → Basic Event → Audible Alarm Output**
2. **Sound Type**を選択し、関連するパラメーターを設定します。
   - **Prompt**を選択し、必要なアラーム時間を設定します。
   - **Warning**とその内容を選択します。必要なアラーム時間を設定します。
   - **Custom Audio**を選択します。ドロップダウンリストからカスタムオーディオファイルを選択できます。利用できるファイルがない場合、**Add**をクリックすると、要件を満たした音声ファイルをアップロードできます。オーディオファイルは3つまでアップロードできます。
3. **オプション**：**Test**をクリックして、選択したオーディオファイルを本機で再生します。
4. 音声アラームのアーミングスケジュールを設定します。詳しくは**アーミングスケジュールの設定**を参照してください。
5. **Save**をクリックします。

メモ

この機能は一部の機種のみ対応しています。

第 9 章 システムとセキュリティ

ここでは、システムメンテナンス、システム設定、セキュリティ管理について説明し、関連するパラメーターの設定方法について解説します。

9.1 デバイス情報の表示

デバイス番号、モデル、シリアル番号、ファームウェアバージョンなどのデバイス情報を表示できます。

デバイス情報を見るには、次の順に進みます。**Configuration → System → System Settings → Basic Information**

9.2 ログの検索と管理

ログは、問題の特定とトラブルシューティングに役立ちます。

ステップ

1. 次の順に進みます。**Configuration → System → Maintenance → Log**
2. **Major Type**、**Minor Type**、**Start Time**、**End Time**などの検索条件を設定します。
3. **Search**をクリックします。
   一致したログファイルがログ一覧に表示されます。
4. **オプション**：**Export**をクリックすると、ログファイルをパソコンに保存できます。

9.3 同時ログイン

管理者は、Webブラウザからシステムに同時にログインするユーザーの最大人数を設定できます。

Configuration → System → User Managementの順に進み、**General**をクリックして**Simultaneous Login**を設定します。

9.4 設定ファイルのインポートとエクスポート

同じパラメーターを持つ他のデバイスを素早く設定するのに役立ちます。

Configuration → System → Maintenance → Upgrade & Maintenanceの順に進みます。インポートまたはエクスポートが必要なデバイスのパラメーターを選択し、インターフェースの指示に従って、設定ファイルをインポートまたはエクスポートします。

9.5 診断情報のエクスポート

診断情報には、実行ログ、システム情報、ハードウェア情報などが含まれます。

Configuration → System → Maintenance → Upgrade & Maintenanceの順に進みます。診断したい情報を確認し**Diagnose Information**をクリックして、本機の該当する診断情報をエクスポートします。

9.6 診断

4Gネットワークに対応した機器では、診断により通信パケットや機器の電源・ネットワーク情報を取得し、今後の保守やトラブルシューティングに役立てることができます。

9.6.1 キャプチャーデバイスパケット

この機能は専門家向けに用意されており、問題が発生した時の診断やデバッグのために、機器と外部機器間の通信パケットを取得するために使用されます。

ステップ

メモ

この機能は、専門家とテクニカルサポートスタッフのために用意されています。

1. 次の順に進みます。**Configuration → System → Maintenance → Diagnose**
2. **Capture Device Packet**にチェックを入れると、この機能が有効になります。
3. お客様のニーズに合わせて**Capture Duration**を設定します。
4. パケット保存パスを選択します。

   メモ

   a. 保存パスの選択肢は、本機の実際の保存方法により異なります。
   b. **Delete Captured Packet Under This Path**をクリックすると、保存したパケットファイル（複数可）を削除することができます。
5. NICの種類、IP、ポートを設定します。
6. **オプション**：**Auto Capture**を選択して、ウェイクアップ時にデバイスパケットをキャプチャします。
7. **Save**をクリックします。
8. **Capture Packet Manually**をクリックします。
9. キャプチャが完了したら**Export Report**をクリックして、レポートを保存します。

9.6.2 デバイス情報のエクスポート

Configuration → Network → Basic Settings → Wireless Expert Settingsの順に進み、**Export Report**をクリックして、電圧、電流、電力、4Gデータなどのデバイス情報をエクスポートします。

9.7 再起動

Webブラウザで本機の再起動ができます。

Configuration → System → Maintenance → Upgrade & Maintenanceの順に進み、**Reboot**をクリックします。

9.8 復元と初期設定

復元と初期設定は、本機のパラメーターをデフォルト設定に戻すのに役立ちます。

ステップ

1. 次の順に進みます。**Configuration → System → Maintenance → Upgrade & Maintenance**
2. 必要に応じて、**Restore**または**Default**をクリックします。

Restore	ユーザー情報、IPパラメーター、ビデオフォーマットを除く本機のパラメーターを初期値に戻します。
Default	すべてのパラメーターを工場出荷時の設定に戻します。

メモ

この機能を使用する際はご注意ください。工場出荷状態に戻すと、すべてのパラメーターが初期値になります。

9.9 アップグレード

ご使用の前に

正しいアップグレードパッケージを入手する必要があります。

注意

アップグレード中は電源を切らないでください。アップグレードが終了すると本機は自動的に再起動します。

ステップ

1. 次の順に進みます。**Configuration → System → Maintenance → Upgrade & Maintenance**
2. アップグレードする方法を1つ選びます。

Firmware	アップグレードファイルの正確なパスの位置を示します。
Firmware Directory	アップグレードファイルが属するディレクトリの位置を示します。

3. **Browse**をクリックして、アップグレードファイルを選択します。
4. **Upgrade**をクリックします。

9.10 自動メンテナンス

ステップ

1. **Enable Auto Maintenance**にチェックを入れます。
2. 管理者パスワードを入力し**OK**をクリックします。
3. 再起動を希望する日時を選択します。
4. **Save**をクリックします。

メモ

この機能は一部の機種のみ対応しています。

警告

本機の自動メンテナンスを有効にすると、メンテナンスプランにしたがって自動的に再起動します。再起動中は、本機で映像を録画することはできません。

9.11 オープンソースソフトウェアライセンスの表示

Configuration → System → System Settings → Aboutの順に進み、**View Licenses**をクリックします。

9.12 時刻と日付

タイムゾーン、時刻同期、サマータイム（DST）を設定して、本機の時刻と日付を設定できます。

9.12.1 手動での時刻同期

ステップ

1. 次の順に進みます。**Configuration → System → System Settings → Time Settings**
2. **Time Zone**を選択します。
3. **Manual Time Sync**をクリックします。
4. 時刻を同期する方法を1つ選びます。
   - **Set Time**を選択し、日時を手入力するかポップアップカレンダーから日時を選択します。
   - **Sync. with computer time**にチェックを入れると、本機の時刻をローカルのパソコンの時刻と同期させることができます。
5. **Save**をクリックします。

9.12.2 NTPサーバーの設定

NTPサーバーは、正確で信頼できるタイムソースが必要な場合に使用できます。

ご使用の前に
NTPサーバーを設定したり、NTPサーバーの情報を取得できます。

ステップ
1. 次の順に進みます。**Configuration → System → System Settings → Time Settings**
2. **Time Zone**を選択します。
3. **NTP**をクリックします。
4. **Server Address**、**NTP Port**、**Interval**を設定します。

メモ
サーバーのアドレスは、NTPサーバーのIPアドレスです。
5. **Test**をクリックして、サーバーの接続をテストします。
6. **Save**をクリックします。

9.12.3 サテライトでの時刻同期

メモ
この機能は機器によって異なります。

ステップ
1. 次の順に進みます。**Configuration → System → System Settings → Time Settings**
2. **Satellite Time Sync.**を選択します。
3. **Interval**を設定します。
4. **Save**をクリックします。

9.12.4 DSTの設定

本機が設置されている地域が夏時間を採用している場合、この機能を設定します。

ステップ
1. 次の順に進みます。**Configuration → System → System Settings → DST**
2. **Enable DST**にチェックを入れます。
3. **Start Time**、**End Time**、**DST Bias**を選択します。
4. **Save**をクリックします。

9.13 RS-485の設定

RS-485は、本機と外部デバイスとの接続に使用します。通信距離が長い場合は、RS-485を使用して本機とパソコンや端末の間でデータを伝送できます。

ご使用の前に
本機とパソコンまたは端末をRS-485ケーブルで接続します。

ステップ
1. 次の順に進みます。**Configuration → System → System Settings → RS-485**
2. RS-485のパラメーターを設定します。

メモ
本機とパソコンや端末のパラメーターをすべて同じにする必要があります。
3. **Save**をクリックします。

9.14 RS-232の設定

RS-232は、本機のデバッグや周辺機器へのアクセスに使用します。RS-232は、通信距離が短い場合に、本機とパソコンや端末との通信を行います。

ご使用の前に
本機とパソコンまたは端末をRS-232ケーブルで接続してください。

ステップ
1. 次の順に進みます。**Configuration → System → System Settings → RS-232**
2. RS-232のパラメーターを設定し、パソコンや端末と本機をマッチングさせます。
3. **Save**をクリックします。

9.15 消費電力モード

本機の動作時の消費電力の切り替えに使用します。

メモ
この機能は一部のカメラ機種のみ対応しています。

Configuration → Proactive Mode → Power Consumption Modeの順に進み、目的の電力消費モードを選択します。

Performance Mode
本機はすべての機能を有効にした状態で動作します。

Proactive Mode
本機のDSPは正常に動作します。メインストリームをハーフフレームレートで録画し、リモートログイン、プレビュー、設定をサポートします。

Low Power Sleep
本機の電力が**Threshold of Low Power Sleep Mode**より低い場合、スリープモードになります。

本機の電力が閾値の10%上まで回復すると、本機はユーザー設定モードになります。

Scheduled Sleep

本機が**Scheduled Sleep Time**中の場合スリープモードになり、そのモードでない場合はユーザー設定モードになります。

メモ

計画したスリープのスケジュール設定は**アーミングスケジュールの設定**を参照してください。

本機はタイミングウェイクに対応しています。詳しくは、**タイミングウェイクの設定**を参照してください。

9.16 セキュリティ

セキュリティパラメーターを設定して、システムのセキュリティを向上します。

9.16.1 認証

RTSP認証やWEB認証を設定して、ネットワークアクセスのセキュリティを向上できます。

Configuration → System → Security → Authenticationの順に進み、必要に応じて認証プロトコルや認証方式を選択します。

RTSP認証

ダイジェストとダイジェスト/ベーシックに対応しており、RTSPリクエストを本機に送信する際に認証情報が必要になります。**digest/basic**を選択すると、本機はダイジェスト認証またはベーシック認証をサポートします。**digest**を選択すると、本機はダイジェスト認証のみをサポートします。

RTSPダイジェストアルゴリズム

RTSP認証でのMD5、SHA256、MD5/SHA256の暗号化アルゴリズムです。MD5以外のダイジェストアルゴリズムを有効にすると、サードパーティのプラットフォームは互換性のため、本機へのログインやライブビューができない場合があります。強度の高い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/ベーシックに対応しており、WEBリクエストを本機に送信する際に認証情報が必要になります。**digest/basic**を選択すると、本機はダイジェスト認証またはベーシック認証をサポートします。**digest**を選択すると、本機はダイジェスト認証のみをサポートします。

WEB**ダイジェストアルゴリズム**

WEB認証でのMD5、SHA256、MD5/SHA256の暗号化アルゴリズムです。MD5以外のダイジェストアルゴリズムを有効にすると、サードパーティのプラットフォームは互換性のため、本機へのログインやライブビューができない場合があります。強度の高い暗号化アルゴリズムを推奨します。

メモ

認証要件の表示については、プロトコルの特定内容を参照してください。

9.16.2 IPアドレスフィルタの設定

IPアドレスフィルタはアクセス制御をするためのものです。IPアドレスフィルターを有効にし、特定のアドレスからのアクセスを許可または禁止することができます。

IPアドレスは、IPv4を指します。

ステップ

1. 次の順に進みます。**Configuration → System → Security → IP Address Filter**
2. **Enable IP Address Filter**にチェックを入れます。
3. IPアドレスフィルターの種類を選択します。

   Forbidden　リスト内のIPアドレスは、本機にアクセスできません。

   Allowed　リストに含まれるIPアドレスのみ、本機にアクセスできます。
4. IPアドレスフィルタのリストを編集します。

   Add　新しいIPアドレスまたはIPアドレスの範囲をリストに追加します。

   Modify　リストで選択したIPアドレスまたはIPアドレスの範囲を修正します。

   Delete　リストで選択したIPアドレスまたはIPアドレスの範囲を削除します。
5. **Save**をクリックします。

9.16.3 HTTPSの設定

HTTPSは、暗号化された通信と本人認証を可能にするネットワークプロトコルで、リモートアクセスの安全性を向上させます。

ステップ

1. 次の順に進みます。**Configuration → Network → Advanced Settings → HTTPS**
2. **Enable**にチェックを入れると、HTTPまたはHTTPSプロトコルでカメラにアクセスできます。
3. **Enable HTTPS Browsing**にチェックを入れると、HTTPSプロトコルでのみカメラにアクセスできます。
4. **Server Certificate**を選択します。
5. **Save**をクリックします。

メモ

この機能に異常がある場合は、選択した証明書が正確かどうか、**Certificate Management**で確認してください。

9.16.4 QoSの設定

QoS（Quality of Service）は、データ送信の優先順位を設定することで、ネットワークの遅延やネットワークの混雑を改善できます。

メモ

QoSは、ルーターやスイッチなどのネットワーク機器のサポートが必要です。

ステップ

1. 次の順に進みます。**Configuration → Network → Advanced Configuration → QoS**
2. **Video/Audio DSCP**、**Alarm DSCP**、**Management DSCP**を設定します。

   メモ

   ネットワークは、データ伝送の優先順位を識別します。DSCPの値が大きいほど優先度は高くなります。ルーターでも設定時に同じ値を設定する必要があります。
3. **Save**をクリックします。

9.16.5 IEEE 802.1Xの設定

IEEE 802.1xは、ポートベースのネットワークアクセス制御のことです。LAN/WLANのセキュリティレベルを高めることができます。IEEE 802.1x規格でデバイスがネットワークに接続する場合、認証が必要です。

Configuration → Network → Advanced Settings → 802.1Xの順に進み、この機能を有効にします。ルーター情報に従って、**Protocol**と**EAPOL Version**を設定します。

プロトコル

EAP-LEAP、EAP-TLS、EAP-MD5が選択可能です。

EAP-LEAPとEAP-MD5

EAP-LEAPまたはEAP-MD5を使用する場合は、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あらかじめサーバーに登録しておきます。認証するユーザー名とパスワードを入力します。

EAP-TLS

EAP-TLSを使用する場合は、識別情報、秘密キーのパスワードを入力し、CA証明書、ユーザー証明書、秘密キーをアップロードします。

EAPOLバージョン

EAPOLのバージョンは、ルーターまたはスイッチのバージョンと同一である必要があります。

9.16.6 タイムアウト設定の制御

この機能を有効にすると、設定したタイムアウト時間内にWebブラウザから本機への操作（ライブ映像の視聴を除く）を行わなかった場合、ログアウトされます。

Configuration → System → Security → Advanced Securityの順に進み、設定を完了します。

9.16.7 セキュリティ監査ログの検索

本機のセキュリティログファイルを検索・分析することで、不正侵入の発見やセキュリティイベントのトラブルシューティングが可能です。

ステップ

メモ

この機能は一部の機種のみ対応しています。

1. 次の順に進みます。**Configuration → System → Maintenance → Security Audit Log**
2. ログの種類、**Start Time**と**End Time**を選択します。
3. **Search**をクリックします。

   検索条件に合致したログファイルがログ一覧に表示されます。
4. **オプション**：**Export**をクリックすると、ログファイルをパソコンに保存します。

9.16.8 SSH

Secure Shell（SSH）とは、安全でないネットワーク上でネットワークサービスを操作するための暗号化ネットワークプロトコルです。

Configuration → System → Security → Security Serviceの順に進み、**Enable SSH**にチェックを入れます。
SSH機能はデフォルトでは無効になっています。

注意

この機能の使用には注意が必要です。この機能を有効にした場合、機器内部情報漏洩の危険があります。

9.17 証明書の管理

サーバー/クライアント証明書やCA証明書を管理し、証明書の有効期限が近い場合や、期限切れ/異常の場合にアラームを送信します。

メモ

この機能は一部の機種のみ対応しています。

9.17.1 自己署名証明書の作成

ステップ

1. **Create Self-signed Certificate**をクリックします。
2. 画面の指示に従って、**Certificate ID**、**Country/Region**、**Hostname/IP**、**Validity**、その他のパラメーターに進みます。

メモ

証明書IDは数字または文字で、64文字以内とします。

3. **OK**をクリックします。
4. **オプション**：**Export**をクリックして証明書をエクスポートするか、**Delete**をクリックして証明書を削除し、証明書を再作成するか、または**Certificate Properties**をクリックして、証明書の詳細説明を表示します。

9.17.2 証明書発行依頼の作成

ご使用の前に

自己署名証明書を選択します。

ステップ

1. **Create Certificate Request**をクリックします。
2. 関連情報を入力します。
3. **OK**をクリックします。

9.17.3 証明書のインポート

ステップ

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**を入力します。
4. **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ます。
5. インポート方法を選択し、必要事項を入力します。
6. **OK**をクリックします。
7. **オプション**：**Export**をクリックして証明書をエクスポートするか、**Delete**をクリックして証明書を削除し、証明書を再作成するか、または**Certificate Properties**をクリックして、証明書の詳細説明を表示します。

メモ

- 最大16まで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、削除することはできません。
- 証明書を使用している機能は、機能欄で確認することができます。
- 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。

9.17.4 サーバー/クライアント証明書のインストール

ステップ

1. 次の順に進みます。**Configuration → System → Security → Certificate Management**
2. **Create Self-signed Certificate**、**Create Certificate Request**、**Import**をクリックして、サーバー/クライアント証明書をインストールします。

Create self-signed certificate	**自己署名証明書の作成**を参照してください。
Create certificate request	**証明書発行依頼の作成**を参照してください。
Import Certificate	**証明書のインポート**を参照してください。

9.17.5 CA証明書のインストール

ステップ

1. **Import**をクリックします。
2. **Certificate ID**を入力します。
3. **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ます。
4. インポート方法を選択し、必要事項を入力します。
5. **OK**をクリックします。

メモ

最大16までの証明書が許可されます。

9.17.6 証明書の有効期限切れアラームの有効化

ステップ

1. **Enable Certificate Expiration Alarm**にチェックを入れます。これを有効にすると、証明書がまもなく期限切れになること、または期限切れや異常であることを監視センターへ伝える電子メールまたはカメラリンクを受信します。
2. **Remind Me Before Expiration (day)**、**Alarm Frequency (day)**、**Detection Time (hour)**を設定します。

メモ

- 有効期限前の通知日を1に設定した場合、有効期限日の前日に通知します。1日～30日まで対応可能です。7日間がデフォルトのリマインド日数です。
- 有効期限前の通知日を1、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の場合、カメラは翌日の10:00に通知します。

3. **Save**をクリックします。

9.18 ユーザーとアカウント

9.18.1 ユーザーアカウントと権限の設定

管理者は、他のアカウントの追加、変更、削除、およびユーザーレベルごとに異なる権限を付与することができます。

注意

ネットワーク上で本機を使用する際のセキュリティを高めるため、アカウントのパスワードは定期的に変更してください。パスワードは3ヶ月に1度変更することを推奨します。リスクの高い環境で使用する場合は、1カ月または1週間ごとにパスワードを変更することを推奨します。

ステップ

1. 次の順に進みます。**Configuration → System → User Management → User Management**
2. **Add**をクリックします。**User Name**を入力し、**Level**を選択して**Password**を入力します。必要に応じてユーザーにリモート権限を割り当てます。

   Administrator

   管理者は、すべての操作の権限を持ち、ユーザーやオペレーターの追加、権限の付与ができます。

   User

   ユーザーには、ライブ映像の視聴、PTZパラメーターの設定、パスワードの変更などの権限を付与することができますが、それ以外の操作の権限は付与できません。

   Operator

   オペレーターは、管理者が行う操作とアカウントの作成を除くすべての権限が付与されます。

   Modify　ユーザーを選択し**Modify**をクリックして、パスワードと権限を変更します。

   Delete　ユーザーを選択し**Delete**をクリックします。

   メモ

   管理者は、ユーザーアカウントを最大31個まで追加できます。
3. OKをクリックします。

9.18.2 同時ログイン

管理者は、Webブラウザからシステムに同時にログインするユーザーの最大人数を設定できます。

Configuration → System → User Managementの順に進み、**General**をクリックして**Simultaneous Login**を設定します。

9.18.3 オンラインユーザー

本機にログインしているユーザーの情報が表示されます。

Configuration → System → User Management → Online Usersの順に進むと、オンラインユーザーの一覧が表示されます。

付録A. デバイスコマンド

以下のQRコードを読み取ると、デバイス共通シリアルポートコマンドが取得できます。
なお、コマンドリストには、すべてのHikvisionネットワークカメラでよく使用されるシリアルポートコマンドが含まれています。

付録B. デバイス通信マトリクス

以下のQRコードを読み取ると、デバイス通信マトリックスが取得できます。
なお、マトリックスには、Hikvisionネットワークカメラのすべての通信ポートが含まれています。

付録C. よくある質問

以下のQRコードを読み取ると、本機のよくある質問が表示されます。なお、よくあるご質問の中には、特定の機種にしか該当しないものもあります。


See Far, Go Further