アイリスオーヤマ

ネットワークカメラ Sシリーズ



UD14456B

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。

3

安全上のご注意

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

安全上の注意は「警告」と「注意」に分かれています。

警告: これらの警告を無視すると、重傷または死亡につながる可能性があります。 注意: これらの注意を無視すると、けがや装置の損傷を引き起こす可能性があります。





- 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。)



- 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	
第2章	ネットワーク接続	11
2.1	LAN経由でのネットワークカメラの設定	11
2.1	.1 LAN 経由の配線	12
2.1	.2 カメラの起動	13
2.1	.3 セキュリティ質問の設定	17
2.2	WAN経由でのネットワークカメラの設定	17
2.2	2.1 固定IP 接続	17
2.2	2.2 動的IP 接続	
第3章	ネットワークカメラにアクセス	21
3.1	Webブラウザによるアクセス	21
3.2	クライアントソフトウェアによるアクセス	22
第4章	Wi-Fi設定	24
4.1	管理モードおよびアドホックモードでのWi−Fi接続の設定	24
4.2	WPS機能付き簡単Wi−Fi接続	29
4.3	ワイヤレスネットワーク接続のIPプロパティ設定	32
第5章	ライブビュー	34
5.1	ライブビューページ	34
5.2	ライブビューの開始	
5.2	2.1 ライブ動作	
5.2	2.2 プラグインのインストール	
5.3	手動で録画/撮影する	
5.4	クイックセットアップ	
5.5	PTZ コントロールの操作	40
5.5	5.1 PTZ コントロールパネル	41
5.5	5.2 プリセットの設定/呼び出し	42
5.5	5.3 パトロールの設定/呼び出し	43
第6章	ネットワークカメラ設定	45
6.1	ローカルパラメータの設定	45
6.2	システム設定	47
6.2	2.1 基本情報の設定	47

PHICE	48
RS232 設定	50
RS485 設定	51
DST 設定	52
外部デバイスの設定	53
VCA リソースの設定	54
メタデータ設定	55
オープンソース・ソフトウェア・ライセンス	56
シテナンス	56
アップグレードとメンテナンス	56
ログ	57
システムサービス	59
セキュリティ監査ログ	59
2キュリティ設定	61
忍証	61
IPアドレスフィルタ	62
セキュリティサービス	63
高度なセキュリティ	64
ユーザー管理	65
ユーザー管理	65
セキュリティに関する質問	68
オンラインユーザー	69
ネットワーク設定	70
ネットワーク設定 基本設定	70 70
ドットワーク設定 基本設定 TCP/IP 設定	70 70 70
ネットワーク設定 基本設定 TCP/IP 設定 DDNS 設定	
ネットワーク設定 基本設定 TCP/IP 設定 DDNS 設定 PPPoE 設定	70 70 70 72 74
ネットワーク設定 基本設定 TCP/IP 設定 DDNS 設定 PPPoE 設定 ポート設定	
ベットワーク設定 基本設定 TCP/IP 設定 DDNS 設定 PPPoE 設定 ポート設定 NAT (ネットワークアドレス変換) 設定	
ベットワーク設定 基本設定 TCP/IP 設定 DDNS 設定 PPPoE 設定 ポート設定 NAT (ネットワークアドレス変換) 設定 マルチキャストの設定	
ベットワーク設定 基本設定 TCP/IP 設定 DDNS 設定 PPPoE 設定 ポート設定 NAT (ネットワークアドレス変換) 設定 マルチキャストの設定 ギ細設定	
ベットワーク設定 基本設定 TCP/IP 設定 DDNS 設定 PPPoE 設定 ポート設定 NAT (ネットワークアドレス変換)設定 マルチキャストの設定 SNMP設定	
ベットワーク設定 TCP/IP 設定 DDNS 設定 PPPoE 設定 ポート設定 NAT (ネットワークアドレス変換)設定 マルチキャストの設定 SNMP設定 FTP 設定	
ベットワーク設定 TCP/IP 設定 DDNS 設定 PPPoE 設定 ポート設定 NAT (ネットワークアドレス変換) 設定 マルチキャストの設定 ¥細設定 SNMP設定 FTP 設定	
ベットワーク設定 TCP/IP 設定 DDNS 設定 PPPoE 設定 ポート設定 NAT (ネットワークアドレス変換)設定 マルチキャストの設定 詳細設定 SNMP設定 FTP 設定 Eメール設定の指定 プラットフォームアクセス	
ベットワーク設定 TCP/IP 設定 TCP/IP 設定 DDNS 設定 PPPoE 設定 ポート設定 NAT (ネットワークアドレス変換) 設定 マルチキャストの設定 詳細設定 SNMP設定 FTP 設定 Eメール設定の指定 プラットフォームアクセス ワイヤレスダイヤル	
ベットワーク設定 TCP/IP 設定 DDNS 設定	
×ットワーク設定 基本設定 TCP/IP 設定 DDNS 設定 PPPoE 設定 ポート設定 NAT (ネットワークアドレス変換) 設定 マルチキャストの設定 洋細設定 SNMP設定 FTP 設定 Eメール設定の指定 プラットフォームアクセス ワイヤレスダイヤル HTTPS 設定 QoS 設定	70 70707274757678797979818487879094
	RS485 設定

7.2	9 統合プロトコル	96
7.2	10 帯域幅適応	97
7.2	11 ネットワークサービス	97
7.2	12 スムーズなストリーミング	
第8章	ビデオ/オーディオ設定	100
8.1	ビデオ設定	100
8.1.	1 ビデオ設定	
8.1.	2 カスタムビデオ	
8.2	オーディオ設定	106
8.3	ROIエンコーディングの設定	108
8.4	ストリーム上の情報表示	110
8.5	ターゲットクロッピングの設定	110
第9章	画像設定	111
9.1	ディスプレイ設定	111
9.2	OSD 設定	116
9.3	プライバシーマスクの設定	117
9.4	画像オーバーレイの設定	119
9.5	画面切り換えパラメータの設定	120
第10章	イベント設定	121
10.1	基本イベント	
10.	1.1 モーション検出の設定	
10.	1.2 ビデオ改ざんアラームの設定	
10.	1.3 アラーム入力の設定	
10.	1.4 アラーム出力の設定	
10.	1.5 例外アラームの設定	
10.	1.6 アラームライト出力の点滅の設定	
10.	1.7 音声アラーム出力の設定	
10.1	1.8 その他のアラームの設定	
10.2	スマートイベント	137
10.2 10.3	スマートイベント 2.1 オーディオ例外検出の設定	
10.2 10.3 10.3	スマートイベント 2.1 オーディオ例外検出の設定 2.2 デフォーカス検出の設定	
10.2 10.3 10.3	スマートイベント 2.1 オーディオ例外検出の設定 2.2 デフォーカス検出の設定 2.3 シーンチェンジ検出の設定	
10.2 10.3 10.3 10.3 10.3	スマートイベント 2.1 オーディオ例外検出の設定 2.2 デフォーカス検出の設定 2.3 シーンチェンジ検出の設定 2.4 顔検出の設定	
10.2 10.3 10.3 10.3 10.3	スマートイベント 2.1 オーディオ例外検出の設定 2.2 デフォーカス検出の設定 2.3 シーンチェンジ検出の設定 2.4 顔検出の設定 2.5 侵入検知の設定	

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

第1章 動作環境

オペレーティングシステム

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

CPU

Intel corei5以上

RAM

8GB以上

ディスプレイ

1024×768 解像度以上

Webブラウザ

プラグインフリーライブビュー対応のカメラの場合

<Windowsの場合>

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

およびGoogle Chrome 31.0以降のバージョン

<MACの場合>

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

およびGoogle Chrome 57.0以降のバージョン

お知らせ:

Google Chrome 57 以降またはMozilla Firefox 52 以降のプラグインフリーバー ジョンでは、「ピクチャー」および「プレイバック」機能は非表示になります。 Webブラウザで上記機能を使用する場合は、下位バージョンに変更するか、ま たはInternet Explorer 8.0以降に変更します。

プラグインフリーライブビューに対応していないカメラの場合

<Windowsの場合>

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

およびGoogle Chrome 31.0以降のバージョン

<MACの場合>

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

およびGoogle Chrome 57.0以降のバージョン

第2章 ネットワーク接続

お知らせ:

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

準備:

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

2.1 LAN経由でのネットワークカメラの設定

目的:

LAN 経由でカメラを表示および設定するには、同じサブネット内のネットワークカ メラをコンピュータと接続し、ネットワークカメラのIP を検索および変更するため にSADP またはiVMS-4200 ソフトウェアをインストールする必要があります。 *お知らせ*: SADPの詳細な導入については、付録1を参照してください。

2.1.1 LAN 経由の配線

ネットワークカメラとパソコンのケーブル接続の2つの方法を下図に示します:

目的:

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



図2-2 スイッチまたはルーター経由の接続

2.1.2 カメラの起動

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

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

※ Webブラウザによる起動

手順:

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

お知らせ:

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

	Activation		UserName
			Password
	User Name	admin	
	Password	•••••••• Ø	Login
RAL LA		Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.	Contact of the Alexandrian
	Confirm	•••••	
			ЭК

図2-3 Web ブラウザによる起動

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

	<u>強力なパスワードを推奨</u>
	製品のセキュリティを強化するために、独自に強力なパスワードを作成す
	ることを強く推奨します(大文字、小文字、数字、特殊文字のカテゴリを少な
	くとも3つ含む8 文字以上を使用)。
	また、パスワードを定期的に変更することを推奨します。特に高セキュリテ
	ィシステムでは、パスワードを月単位または週単位で変更すると製品のセ
	キュリティが向上します。

- 4. パスワードを確認します。
- 5.「OK」をクリックしてパスワードを保存し、ライブビュー画面に入ります。

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

公式ウェブサイトからSADP ソフトウェアを入手し、プロンプトに従ってSADP をイン ストールします。カメラを起動する手順に従います。

手順:

1. SADP ソフトウェアを実行して、オンラインデバイスを検索します。

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

illine) at	1.00	100000	1.00.0.0.00	1.2	1.0.0	1.10.4.0.1	1000000		STREET.	
001	1 Device type	Action	10.16.6.20	ROOD	Software Version	10.15.6.254	80	rt Device Sen	ai ruo.	
002	Dis-strength A	Active	10.16.6.21	8000	VLUM-AV 1998	10.16.6.254	80		-	0
003	DS-ROMON-AL	Active	10.16.6.213	8000	VLL Rode 1912.	10.16.6.254	N/A	11-1200	400144.00799	
004	25.18438-1925	Active	10.16,6.179	8000	VL023bald 280.	10.16.6.254	N/A	-	>	The second second second
005	05-18408-01846	Active	10.16.6.127	8000	VED Multi SHET.	10.16.6.254	N/A	The statement		The device is not activated.
006	UNICHINA DEVICE THE	Active	10.16.6.250	8000	VS-ADMAR 2002.	10.16.6.254	80	2040100		
0	07	24-202	2025790	14	Inacti	ive		192.168	.1.64	-
009	15-18189 (M)120W	Active	10.16.6.177	8000	VERIDUAR DEEL	10.16.6.254	80	-	HE CONTRACT	You can modify the network parameters after the device activation.
		停	止中の	ヮディ	バイスを	を選択	2			Adiuste Nove
							•			
							_	184		New Password:
						ハス	.IJ-	ートを	"惟認	confirm Password:

図2-4 SADP画面

お知らせ:

SADPソフトウェアは、カメラの一括起動をサポートします。

3. パスワードフィールドにパスワードを作成して入力し、パスワードを確認し

ます。ユーザー名を含むパスワードは許可されません。

<u>強力なパスワードを推奨</u>
 製品のセキュリティを強化するために、独自に強力なパスワードを作成す
ることを強く推奨します(大文字、小文字、数字、特殊文字のカテゴリを少な
くとも3つ含む8 文字以上を使用)。
また、パスワードを定期的に変更することを推奨します。特に高セキュリテ
ィシステムでは、パスワードを月単位または週単位で変更すると製品のセ
キュリティが向上します。

4.「Active」をクリックして起動を開始します。

起動が完了したかどうかは、ポップアップウィンドウで確認できます。 有効化に失敗した場合は、パスワードが要件を満たしていることを確認してから、 もう一度試してください。 5. IP アドレスを手動で変更するか、「Enable DHCP」チェックボックスをオンに し、デバイスのIP アドレスをコンピュータと同じサブネットに変更します。

Modify Network	Parameters				
Enable DHCP					
Enable Hik-Cor	nnect				
Device Serial No.:	XX-XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX				
IP Address:	192.168.1.64				
Port:	8000				
Subnet Mask:	255.255.255.0				
Gateway:	192.168.1.1				
IPv6 Address:	:				
IPv6 Gateway:	:				
IPv6 Prefix Length:	0				
HTTP Port:	80				
S	ecurity Verification				
Admin Password:					
	Modify				
	Forgot Password				
図2-5 I	っ アドレスの変更				

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

バッチIP アドレスの変更は、SADP でサポートされています。

2.1.3 セキュリティ質問の設定

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

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

2.2 WAN経由でのネットワークカメラの設定

目的:

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

2.2.1 固定IP 接続

準備:

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

● ルーター経由でネットワークカメラを接続する

手順:

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

- ポートマッピング(80、8000、554ポートなど)を設定します。ポートマッピングの手順は、ルーターによって異なります。ポートマッピングのサポートについては、ルーターの製造元にお問い合わせください。
 お知らせ: ポートマッピングの詳細については、付録2を参照してください。
- 5. Webブラウザまたはインターネット上のクライアントソフトウェアを介して、ネットワークカメラにアクセスします。



図2-6 固定IPルーターを経由したカメラへのアクセス

● 固定IP でネットワークカメラを直接接続する

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



2.2.2 動的IP 接続

準備:

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

手順:

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

- ルーターで、PPPoE ユーザー名、パスワードを設定し、パスワードを確認します。
- ポートマッピングを設定します。例:80、8000、554ポート。ポートマッピングの手順は、ルーターによって異なります。
 ポートマッピングのサポートについては、ルーターの製造元にお問い合わせく

ださい。

お知らせ:ポートマッピングの詳細については、付録2を参照してください。

- 3. ドメインネームプロバイダからドメイン名を適用します。
- 4. ルーターの設定画面でDDNSを設定します。
- 5. 適用したドメイン名を介してカメラを接続します。
- モデム経由でネットワークカメラを接続する

目的:

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



図2-8 動的IP を使用したカメラへのアクセス

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

◆ 通常のドメイン名の解像度



図2-9 通常のドメイン名の解像度

手順:

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

第3章 ネットワークカメラにアクセス

3.1 Webブラウザによるアクセス

お知らせ:

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

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

手順:

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

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

ユーザー名とパスワードを入力し、ログインをクリックします。
 管理者ユーザーは、デバイスアカウントとユーザー/オペレーター権限を適切に設定する必要があります。不要なアカウントとユーザー/オペレーターの権限を削除します。

お知らせ:

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



図3-1 ログイン画面

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

お知らせ:

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

3.2 クライアントソフトウェアによるアクセス

製品CD には、iVMS-4200 クライアントソフトウェアが含まれています。ライブビデ オを閲覧したり、ソフトウェアでカメラを管理したりすることができます。 インストールの指示に従って、ソフトウェアをインストールします。以下は、iVMS-4200クライアントソフトウェアのコントロールパネルとライブビュー画面です。



図3-2 iVMS-4200 コントロールパネル



図3-3 iVMS-4200 のメインビュー

第4章 Wi-Fi設定

目的:

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

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

4.1 管理モードおよびアドホックモードでのWi-Fi接続

の設定

目的:

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

管理モードでのワイヤレス接続

手順:

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

SNM	IP F	FTP Email	Platform	Access H	TTPS	QoS	Wi-Fi	WLAN AP			
	Wirele	ess List								Search	
	No.	SSID		Working Mo	de	Security	Mode	Channel	Signal Strength	Speed(Mbps)	
	1	TP-LINK_So	ftWare	Manage		disa	ble	1	81	150	-
	2	C-WEF)	Manage		WE	Р	11	50	54	
	3	C-not-encry	pted	Manage		disa	ble	11	50	54	
	4	C-WPA2-Per	sonal	Manage		WPA2-pe	ersonal	11	47	54	
	5	FINALHA	UT	Manage		WPA2-pe	ersonal	6	46	54	
	6	6688		Manage		WPA2-pe	ersonal	6	46	54	
	7	C199T	H	Manage		WPA2-pe	ersonal	6	46	54	=
	8	6688		Manage		WPA2-pe	ersonal	6	44	54	
	9	FINALHA	UT	Manage		WPA2-pe	ersonal	6	44	54	
	10	maoma	0	Manage		WPA2-pe	ersonal	6	43	54	
	11	yingkongsl	ni12	Manage		WPA2-pe	ersonal	6	43	54	
	12	Hik-Gue	st	Manage		WPA-pe	rsonal	1	43	54	
	13	Hik-Meeti	ng	Manage		WE	Р	1	43	54	-

図4-1 Wi-Fi リスト

3. リストでワイヤレス接続をクリックして選択します。

Wi-Fi	
SSID	C-WPA2-Personal
Network Mode	💿 Manage 💿 Ad-Hoc
Security Mode	WPA2-personal
Encryption Type	TKIP
Key 1 💿	

図4-2 Wi-Fi 設定管理モード

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

アドホックモードでの無線接続

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

手順:

1. アドホックモードを選択します。

Wi-Fi	
SSID	C-WPA2-Personal
Network Mode	💿 Manage 💿 Ad-Hoc
Security Mode	WPA2-personal
Encryption Type	TKIP
Key 1 💿	

図4-3 Wi-Fi 設定アドホック

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

camera6467wifi	٠.
belkin54g	311
Tenda_0A0698	lle.
yourPC	lle.
HenryHu	lle.
APPLE	.all
Peter_Ma	
Open Network and Sharing	Center

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:

WPA2-personal
not-encrypted
WEP
WPA-personal
WPA-enterprise
WPA2-personal
WPA2-enterprise

図4-5 セキュリティモード

セキュリティモードは、非暗号化、WEP、WPA-personal、WPA-enterprise、

WPA2-personal、およびWPA2-enterprise から選択できます。

```
WEPモード:
```

Security Mode	WEP
Authentication	💿 Open 🔘 Shared
Key Length	64bit 128bit
Кеу Туре	HEX ASCII
Key 1 💿	
Key 2 🔘	
Key 3 🔘	
Key 4 🔘	

- 「Authentication」-アクセスポイントで使用する方式に応じて、「Open」または 「Shared」を選択します。すべてのアクセスポイントにこのオプションがあるわけ ではありません。その場合は、オープンシステムを使用します。これはSSID 認 証と呼ばれることもあります。
- 「Key length」 ワイヤレス暗号化に使用されるキーの長さを設定します(64 ビットまたは 128 ビット)。暗号化キーの長さは、40/64 および104/128 と表示されることがあります。
- 「Key Type」-使用可能なキーの種類は、使用するアクセスポイントによって 異なります。以下のオプションがあります:
 HEX - 16 進数キーを手動で入力できます。
 ASCII -このメソッドでは、文字列は64 ビットWEP の場合は5 文字、128 ビット
 WEP の場合は13 文字である必要があります。

図4-6 WEP モード

WPA パーソナルおよび WPA2 パーソナルモード:

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

Security Mode	WPA-personal
Encryption Type	TKIP
Key 1 💿	

図4-7 セキュリティモードWPA パーソナル

WPA エンタープライズおよびWPA2 エンタープライズモード:

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

EAP-TLS

Security Mode	WPA-enterprise	
Authentication	EAP-TTLS	
User Name		
Password	•••••	
Inner authentication	PAP 🔹	
Anonymous identity		
EAPOL version	1	
CA certificate		Browse Upload

図4-8 EAP-TLS

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

EAP-PEAP:

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

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

4.2 WPS機能付き簡単Wi-Fi接続

目的:

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

WPS (Wi-Fi Protected Setup)とは、デバイスとワイヤレスルータ間の暗号化さ れた接続を簡単に設定する手法です。WPSを使用すると、長いパスフレーズを入 力することなく、既存のネットワークに新しいデバイスを簡単に追加できます。 WPS接続には、PBCモードとPINモードの2つのモードがあります。 *お知らせ*: WPS 機能を有効にすると、暗号化タイプなどのパラメータを設定する 必要がなく、ワイヤレス接続のキーを知る必要もありません。

手順:

WPS		
Enable WPS		
PIN Code	12345678	Generate
PBC connection	Connect	
O Use router PIN code	Connect	
SSID	C-WPA2-Personal	
Router PIN code		
🖹 Save		

図4-9 Wi-Fi 設定-WPS

PBCモード:

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

- 1. Enable WPS チェックボックスをオンにすると、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。

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

- 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. 接続ボタンをクリックします。
 ルーターとカメラの両方でPBCモードが有効になると、カメラとワイヤレスネット
 ワークが自動的に接続されます。

PINモード:

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

手順:

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

WPS		
Enable WPS		
PIN Code	12345678	Generate
PBC connection	Connect	
Ose router PIN code	Connect	
SSID	C-WPA2-Personal	
Router PIN code		

図4-10 PIN コードの使用

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

または

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

1. 「Generate」をクリックします。

PIN Code	12345678	Generate

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

4.3 ワイヤレスネットワーク接続のIPプロパティ設定

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

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

TCP/IP DDNS PPP	oE Port NAT
Lan Vilan	
	☑ DHCP
IPv4 Address	169.254.121.194 Test
IPv4 Subnet Mask	255.255.0.0
IPv4 Default Gateway	
Multicast Address	
	Enable Multicast Discovery
DNS Server	
Preferred DNS Server	8.8.8.8
Alternate DNS Server	
🖹 Save	

図 4-11 WLAN パラメータの設定

IPv4 アドレス、IPv4 サブネットマスク、およびデフォルトゲートウェイをカスタマイズします。設定手順はLAN と同じです。
 IP アドレスを割り当てる場合は、チェックボックスをオンにしてDHCP を有効にします。

第5章 ライブビュー

5.1 ライブビューページ

目的:

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



ライブビューページの説明:

図5-1 ライブビューページ

メニューバー:

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

ライブビューウィンドウ:

ライブビデオを表示します。

ツールバー:

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

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

お知らせ:

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

PTZコントロールパネル:

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

プリセット/パトロール設定:

PTZ カメラのプリセットまたはパトロールを設定/呼び出し/削除します。

35

5.2 ライブビューの開始

5.2.1 ライブ動作

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

図5-2 ライブビューツールバー

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

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

手順:

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

お知らせ:

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

フルスクリーンモード:

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

5.2.2 プラグインのインストール

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

運用体 制	Webブラウザ	動作
Windows	 Internet Explorer 8+ Google Chrome 57以前のバ ージョン Mozilla Firefox 52以前の バージョン 	ポップアッププロンプトに従っ て、プラグインのインストールを 完了します。
·	 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。
Mac OS	 Google Chrome 57+ Mozilla Firefox 52+ Apple Safari 16+ 	 プラグインインストールは 不要です。 通常のライブビューを表示 するには、「WebSocket」ま たは「WebSockets」を有効 にします(「Configuration」> 「Network」>「Advanced Settings」>「Network Service」)。 一部の機能の表示・操作に制 限があります。たとえば、 「Playback」や「Picture」は使用 できません。 制限機能の詳細については、実 機を参照してください。

お知らせ:

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

5.3 手動で録画/撮影する

ライブビュー画面で、ツールバーの 🚺 をクリックしてライブピクチャを

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

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

5.4 クイックセットアップ

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

- ライブビューウィンドウの右側にある
 をクリックすると、PTZコントロ
 ールパネルが表示されます。
 をクリックすると非表示になります。
- PTZ、ディスプレイ、OSD、ビデオ/オーディオ、およびVCA リソースパラメー タを指定します。詳細設定については、「Configuration」>「Image and Configuration」>「Video/Audio」を選択します。
- [Display Settings]
 - 「Scene」:実際の設置環境に合わせてシーンを選択します。(特定の カメラモデルのみをサポートします。)
 - 「WDR]: WDR (ワイドダイナミックレンジ)機能は、逆光の状況でもカメ ラが鮮明な画像を提供するのに役立ちます。視野内に非常に明るい 領域と非常に暗い領域の両方が同時に存在する場合、WDRは画像 全体の明るさレベルを調節し、細部まで鮮明な画像を提供します。
 WDR 機能を有効または無効にしたり、レベルを設定したりできます。
 - 「HLC」: ハイライト補正により、カメラは通常シーン全体でフレアになる強い光源を識別して抑制します。これにより、通常隠れてしまうようなイメージの細部を確認することができます。
- 「OSD (On Screen Display)」
 画面に表示する文字情報を設定します。配置調整は、テキストオーバーレイで使用できます。設定後に設定を保存します。
- 「Video/Audio」
 解像度と最大ビットレートは調整可能です。
 は、このです。
 に、たのでのです。

• **[VCA Resource]**

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

お知らせ:

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

5.5 PTZ コントロールの操作

目的:

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

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

5.5.1 PTZ コントロールパネル

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

PTZ				
۲		•	a	Q,
•	Ü	►	ď	ō
•	•	4	0	0
				4
۰.	Ŷ	20	1	≡
163	GD			

図5-3 PTZコントロールパネル

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

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

● レンズの動きだけに対応しているカメラの場合、方向ボタンは無効です。

アイコン	説明
a a	拡大/縮小
5 6	遠近フォーカス
0 0	アイリス+/-
4	PTZ速度調整
.t∰t	ライトのオン/オフ
Ş	ワイパーのオン/オフ
Ξ	補助焦点
(レンズ初期化
	パン/チルト動作の速度を調整す る
6	手動トラッキング開始
Œ	3D ズームの開始

表5-2 PTZ コントロールパネルの説明

5.5.2 プリセットの設定/呼び出し

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



図5-4 プリセットの設定

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

- ズームインまたはズームアウトします。
- レンズに焦点を当てます。
- 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、プリセットを削除できます。
- プリセットの呼び出し:

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

定義したプリセットは、いつでも任意のプリセットシーンに呼び出すことができます。 PTZコントロールパネルで、リストから定義済みのプリセットを選択し、³¹をクリ ックしてプリセットを呼び出します。

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



図5-5 プリセットの呼び出し

5.5.3 パトロールの設定/呼び出し

お知らせ:

パトロールを設定する前に、2つ以上のプリセットを設定する必要があります。 *手順:*

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

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

Preset Speed Time	(s)
3 🔹 10 1	
OK Cancel	

図5-6 パトロールパスの追加

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

第6章 ネットワークカメラ設定

6.1 ローカルパラメータの設定

目的:

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

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

手順:

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

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

「UDP」: リアルタイムのオーディオおよびビデオストリームを提供します。 「HTTP」: 一部のネットワーク環境では、特定のポートをストリーミング用に 設定することなく、TCP と同じ品質を実現します。

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

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

- ◆「Rules」: ローカルブラウザのルールを参照し、モーション検出、顔検出、または侵入が検出されたときに色付きマークを表示するかどうかを 選択して、有効または無効にします。 たとえば、ルールとして有効になり、顔検出も有効になります。顔が検出されると、ライブビューに緑の長方形がマークされます。
- ◆「Display POS Information」:この機能を有効にすると、検出されたター ゲットのフィーチャー情報がライブ画像のターゲット付近に動的に表示 されます。各機能の機能情報は異なります。たとえば、キュー管理の ID と待機時間、人数計算の高さなどです。

お知らせ:

POS情報の表示は、特定のカメラモデルでのみ使用できます。

◆ 「Image Format」: 画像取り込みの画像形式を選択します。

Live View Parameters					
Protocol	TCP	O UDP	○ MULTICAST	⊖ HTTP	
Play Performance	 Shortest Delay 	O Balanced	○ Fluent	Custom 20	frame
Rules	 Enable 	 Disable 			
Display POS Information	 Enable 	 Disable 			
Image Format	JPEG				

図6-1 ライブビューのパラメータ

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

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

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

3. 「Save」をクリックし、設定を保存します。

6.2 システム設定

目的:

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

6.2.1 基本情報の設定

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

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

6.2.2 時間設定

目的:

このセクションの指示に従って、時刻同期およびDST 設定を行います。

手順:

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

ます。

Basic Information	Time Settings	RS232	RS485	DST	
Time Zone	(GMT+0	3:00) Beijin	g, Urumqi,	Singapore	•
NTP					
◎ NTP					
Server Address	time.wind	lows.com			
NTP Port	123				
Interval	1440			min	
	Test				
Manual Time Sy	nc.				
Manual Time Sy	nc.				
Device Time	2015-06-	25T13:45:5	0		
Set Time	2015-06-	25T13:45:4	6	🔁 📄 Sync	. with computer time

図6-2 時間設定

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

「Server Addres」: NTP サーバーのIP アドレス。

「NTP Port」: NTP サーバーのポート。

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

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

Server Address	time.windows.com	
NTP Port	123	
Interval	1440	min

図6-3 NTP サーバーによる時刻同期

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

- 手動時刻同期を設定します。
 - 「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) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2) (3) (4)

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

44 4	E .	May		2015		> >>
Sun	Mon	Tue	Wed	Thu	Fri	Sat
26	27	28	29	30	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2		4	5	6
84	Time [18 :	57	: 36	*	
Ð						ок

図6-4 手動による時刻同期

● 「Save」をクリックして設定を保存します。

6.2.3 RS232 設定

RS232 ポートは2 つの方法で使用できます:

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

手順:

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

 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。

Basic Information	Time Settings	RS232	RS485	DST
Baud Rate	115200			•
Data Bit	8			•
Stop Bit	1			•
Parity	None			•
Flow Ctrl	None			•
Usage	Console)		•
🗎 Sa	ve			

図6-5 RS232 設定

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

3.「Save」をクリックし、設定を保存します。

6.2.4 RS485 設定

目的:

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

手順:

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

Basic Information	Time Settings	RS232	RS485	DST
				-
R\$485				
Baud Rate	9600			•
Data Bit	8			•
Stop Bit	1			•
Parity	None			•
Flow Ctrl	None			•
PTZ Protocol	PELCO	-D		•
PTZ Address	0			
🖹 Sa	ve			

2. RS485 パラメータを設定し、「Save」をクリックして設定を保存します。

デフォルトでは、ボーレートは9600 bps、データビットは8、ストップビットは1、

パリティおよびフロー制御はNone に設定されています。

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

6.2.5 DST 設定

目的:

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

図6-6 RS-485の設定

手順:

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

Basic Information	Time Settings	RS232	RS485	DST	
Enable DST					
Start Time	Jan	▼ First	▼ Sun	- 00	-
End Time	Jan	▼ First	▼ Sun	- 00	-
DST Bias	30min				Ŧ

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。

LED Light							
Enable Supplement Light							
Low Beam Brightness		10					
High Beam Brightness		10					
LED Light On	💿 Timing 💿 A	uto					
🖹 Save							

図6-8 外部デバイスの設定

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

LED Light On	le Timing 💿 Auto	
Start Time	18:00:00	
End Time	06:00:00	1

図6-9 セットスケジュール

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

6.2.7 VCA リソースの設定

目的:

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

手順:

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

お知らせ:

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

6.2.8 メタデータ設定

目的:

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

手順:

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

6.2.9 オープンソース・ソフトウェア・ライセンス

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

6.3 メンテナンス

6.3.1 アップグレードとメンテナンス

目的:

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

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

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

お知らせ:

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

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

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

• [Import Config. File]

カメラの一括設定には、設定ファイルを使用します。

手順:

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

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

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

手順:

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

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

6.3.2 ログ

目的:

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

準備:

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

手順:

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

Upgrade &	Jpgrade & Maintenance Log								
Major Type All Types Minor Type All Types									
Start Time 2015-06-04 00:00:00 📸 End Time 2015-06-04 23:59:59						4 23:59:59	1 Search		
Log Li	ist						Export		
No.	Time	Major Type		Minor Type	Channel No.	Local/Remote User	Remote Host IP		

図6-10 ログ検索画面

- [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。
- 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。

Log	List					Export	
No.	Time	Major Type	Minor Type	Channel No.	Local/Remote User	Remote Host IP	61
1	2015-05-25 19:12:34	Operation	Remote: Get Working Sta.		admin	10.16.1.107	
2	2015-05-25 19:12:12	Operation	Remote: Get Working Sta.		admin	10.16.1.107	
3	2015-05-25 19:12:12	Operation	Remote: Get Working Sta.		admin	10.16.1.107	
4	2015-05-25 19:12:12	Operation	Remote: Get Working Sta.		admin	10.16.1.107	
5	2015-05-25 19:12:11	Operation	Remote: Get Working Sta.	•••	admin	10.16.1.107	
6	2015-05-25 19:12:11	Operation	Remote: Get Working Sta.		admin	10.16.1.107	
7	2015-05-25 19:12:11	Operation	Remote: Get Working Sta.		admin	10.16.1.107	
8	2015-05-25 19:12:10	Operation	Remote: Get Working Sta.		admin	10.16.1.107	
9	2015-05-25 19:09:28	Operation	Remote: Get Parameters		admin	10.16.1.107	
10	2015-05-25 19:09:25	Operation	Remote: Get Parameters		admin	10.16.1.107	
11	2015-05-25 19:09:25	Operation	Remote: Get Parameters		admin	10.16.1.107	
12	2015-05-25 19:09:24	Operation	Remote: Get Parameters		admin	10.16.1.107	

図6-11 ログ検索

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

6.3.3 システムサービス

目的:

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

「ABF」: ABF 機能を有効にすると、PTZ コントロールパネルの № をクリックして補助フォーカスを実現できます。

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

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

6.3.4 セキュリティ監査ログ

目的:

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

「Advanced Settings」でサーバー設定をします。

● ログの検索

手順:

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

Up	grade 8	Maintenance	Log	System Servic	e	Security Au	ıdit Log	_			
	Log	Query									
1	Major T	уре	All T	ypes		~	Minor T	ype 🛛	All Types	~	
:	Start Time		2018	B-12-14 00:00:0	00		End Tin	ne 2	018-12-14 23:59:59	9 📆	Search
	Log List							Export	:		
	No.	Time		Major Type		Minor Typ	е	Channel No	Local/Remote User	Remote Host I	P

図6-12 セキュリティ監査ログ検索画面

- 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。
- 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。

Start Time		2018-12-14 00:00	00 📆 Er	nd Tim	ie 20	018-12-14 23:59:59		Search
Log	List						Export	
No.	Time	Major Type	Minor Type		Channel No.	Local/Remote User	Remote Host IP	
1	2018-12-14 17:22:08	3 Operation	Remote: Get Network	Par	1	admin	10.6.112.12	~
2	2018-12-14 17:22:08	3 Operation	Remote: Get Security	Par	1	admin	10.6.112.12	
3	2018-12-14 17:22:08	3 Operation	Remote: Get Security	Par	1	admin	10.6.112.12	
4	2018-12-14 17:11:44	4 Operation	Remote: Get Security F	Par	1	admin	10.6.112.12	
5	2018-12-14 17:11:44	4 Operation	Remote: Get Security F	Par	1	admin	10.6.112.12	
6	2018-12-14 17:11:44	4 Operation	Remote: Get Parame	eters	1	admin	10.6.112.12	
7	2018-12-14 17:11:43	3 Operation	Remote: Get Security F	Par	1	admin	10.6.112.12	
8	2018-12-14 17:11:06	6 Operation	Remote: Get Security F	Par	1	admin	10.6.112.12	
9	2018-12-14 17:11:04	4 Operation	Remote: Get Security F	Par	1	admin	10.6.112.12	
10	2018-12-14 17:11:03	3 Operation	Remote: Login		1	admin	10.6.112.12	

図6-13 ログ検索

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

ログサーバの設定

手順:

1. 「Enable Log Upload Server」をオンにします。

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

6.4 セキュリティ設定

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

6.4.1 認証

目的:

ライブビューのストリームデータを明示的に保護することができます。

手順:

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

Authentication	IP Addre	ess Filter	Security Service	
RTSP Authentic	ation ation	digest digest		▼

図6-14 認証

2. RTSP 認証とWEB 認証の認証方式を設定します。

お知らせ:

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

3. 「Save」をクリックし、設定を保存します。

6.4.2 IPアドレスフィルタ

目的:

この機能により、アクセス制御が可能になります。

手順:

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

Au	then	tication	IP Address Fi	ilter Security S	Service	
	V E	inable If ddress F	P Address Filter Filter Type F	Forbidden		
	IP Address Filter				Add	Delete
		No.		IP		

図6-15 IP アドレスフィルタ画面

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

手順:

(1) IP を追加するには、「Add」をクリックします。

(2) IP Adreess を入力します。

Add IP Address		×
IP Address	172.6.23.2	0
	ок	Cancel

図6-16 IP の追加

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

手順:

(1) フィルタリストからIP アドレスを左クリックして、「Modify」をクリックします。

(2) テキストボックスでIP アドレスを変更します。

Modify IP Address		×
IP Address	172.6.23.2	
	ок	Cancel

図6-17 IP の変更

(3)「OK」をクリックして変更を終了します。

- IP アドレスまたはIP アドレスを削除します。
 IP アドレスを選択し、「Delete」をクリックします。
- 5.「Save」をクリックし、設定を保存します。

6.4.3 セキュリティサービス

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

手順:

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



```
図 6-18 セキュリティサービス
```

 「Enable Illegal Login Lock」チェックボックスをオンにします。
 「Illegal Login Lock」: ユーザーのログイン試行を制限するために使用されます。
 管理者がユーザー名/パスワードの入力を7回(オペレーター/ユーザーの場合は5回)失敗すると、IPアドレスからのログインが拒否されます。
 お知らせ: IPアドレスが拒否された場合は、30分後にデバイスへのログインを 試みることができます。

6.4.4 高度なセキュリティ

目的:

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

• [Security Reinforce]

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

• [Control Timeout Settings]

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

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

6.5 ユーザー管理

6.5.1 ユーザー管理

・ ・ 管理者として ・

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

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

お知らせ:

ユーザーアカウントの追加と変更が必要な場合は、管理者パスワードが必要 です。

U	ser Mana	gement	Online Users		
	User l	List	Ac	dd N	Indify Delete General Account Security Settings
	No.		User Name		Level
	1		admin		Administrator

図6-19 ユーザー管理画面

ユーザーの追加

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

管理者ユーザーは削除できず、管理者パスワードのみを変更できます。

手順:

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

お知らせ:

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

<u>強力なパスワードを推奨-</u>

製品のセキュリティを強化するために、独自に強力なパスワードを作成 することを強く推奨します(大文字、小文字、数字、特殊文字のカテゴリ を少なくとも3つ含む8 文字以上を使用)。 また、パスワードを定期的に変更することを推奨します。特に高セキュリ ティシステムでは、パスワードを月単位または週単位で変更すると製品

のセキュリティが向上します。

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

手順:

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

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

 <u>強力なパスワードを推奨-</u>

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

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

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

手順:

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

手順:

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

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

6.5.2 セキュリティに関する質問

目的:

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

アカウントセキュリティの設定:

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

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

手順:

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

管理者パスワードの変更:

準備:

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

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

6.5.3 オンラインユーザー

目的:

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

「Refresh」をクリックしてリストを更新します。

User Management O		gement Online Users			
	User List				Refresh
	No.	User Name	Level	IP Address	User Operation Time
	1	admin	Administrator	10.16.2.101	2015-11-16 10:57:55

図6-20 オンラインユーザーの表示

第7章 ネットワーク設定

目的:

この章の指示に従って、基本設定と詳細設定をします。

7.1 基本設定

目的:

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

7.1.1 TCP/IP 設定

目的:

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

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

手順:

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

TCP/IP DDNS PPF	PoE Port NAT	
NIC Type	Auto	•
	DHCP	
IPv4 Address	10.11.37.120	Test
IPv4 Subnet Mask	255.255.255.0	
IPv4 Default Gateway	10.11.37.254	
IPv6 Mode	Route Advertisement	View Route Advertisement
IPv6 Address		
IPv6 Subnet Mask	0	
IPv6 Default Gateway		
Mac Address	c0:56:e3:60:27:5d	
MTU	1500	
Multicast Address		
	Enable Multicast Discovery	
DNS Server		
Preferred DNS Server	8.8.8.8	
Alternate DNS Server		
🖹 Save		

図7-1 TCP/IP 設定

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

お知らせ:

- MTU の有効な値の範囲は1280 から1500 です。
- 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前 に、ルーターのマルチキャスト機能を有効にする必要があります。
- 設定を有効にするには、再起動が必要です。

7.1.2 DDNS 設定

目的:

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

カメラのDDNS 設定をする前に、DDNSサーバーでの登録が必要です。

手順:

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

手順:

- (1) DynDNS のサーバアドレス(members.dyndns.org など) を入力します。
- (2)「Domain」欄に、DynDNS Web サイトから取得したドメイン名を入力します。
- (3) DynDNS Web サイトに登録されているユーザー名とパスワードを入力します。
(4)「Save」をクリックし、設定を保存します。

TCP/IP	DDNS	PPP ₀ E	Port	NAT	
🔽 En	able DDNS				
DDNS	Туре	[DynDNS		•
Server	Address	n	nembers.	dyndns.org	
Domair	ı	1	23.dyndr	is.com	0
User N	ame	te	est		0
Port		0			
Passw	ord	•	•••••		
Confirm	ı	•	•••••		
	🗎 Sav	/e			

図7-2 DynDNS 設定

• 「NO-IP」:

手順:

(1) NO-IP としてDDNS タイプを選択します。

TCP/IP	DDNS	PPP ₀ E	Port	NAT
🔽 En	able DDNS			
DDNS	Туре	N	O-IP	•
Server	Address	wv	w.noip.c	com 🥥
Domair	ı			
User N	ame			
Port		0		
Passw	ord			
Confirm	ı			
	🗎 Sav	/e		

図7-3 NO-IP DNS 設定

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

(5)「Save」をクリックすると、ドメイン名のカメラを表示できます。

お知らせ:設定を有効にするには、デバイスを再起動します。

7.1.3 PPPoE 設定

手順:

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

0.0.0		

図7-4 PPPoE の設定

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

お知らせ: ユーザー名とパスワードは、ISP が割り当てる必要があります。

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

4. 「Save」をクリックして、画面を保存して終了します。

お知らせ:設定を有効にするには、再起動が必要です。

7.1.4 ポート設定

目的:

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

手順:

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

TCP/IP	DDNS	PPPoE	Port	NAT
	Port	8	0	
RTSP F	Port	5	54	
HTTPS	Port	4	43	
Server	Port	8	000	
WebSo	cket Port	7	681	
WebSo	ckets Port	7	682	

図7-5 ポート設定

2. カメラのポートを設定します。

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

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

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

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

お知らせ:

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

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

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

お知らせ:

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

3. 「Save」をクリックし、設定を保存します。

お知らせ:設定を有効にするには、再起動が必要です。

7.1.5 NAT (ネットワークアドレス変換) 設定

目的:

NAT設定では、UPnP™パラメータを設定できます。

ユニバーサルプラグアンドプレイ(UPnP™)は、ネットワーク機器、ソフトウェア、およ びその他のハードウェアデバイス間の互換性を提供するネットワークアーキテクチ ャです。UPnP プロトコルを使用すると、デバイスがシームレスに接続でき、ホーム および企業環境でのネットワークの実装を簡素化できます。 この機能を有効にすると、ポートごとにポートマッピングを設定する必要がなくなり、 カメラはルーター経由でワイドエリアネットワークに接続されます。

Enable UPnP™	и			
Friendly Name	TestCam	0		
Port Mapping N	Node Auto	•		
Port Type	External Port	External IP Address	Internal Port	Status
HTTP	80	0.0.0.0	80	Not Valid
RTSP	554	0.0.0.0	554	Not Valid
Server Port	8000	0.0.0.0	8000	Not Valid
WEBSOCKET	7681	0.0.0.0	7681	Not Valid
WEBSOCKETS	7682	0.0.0.0	7682	Not Valid

図7-6 UPnP の設定

手順:

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

お知らせ:

UPnP™機能が有効な場合のみ、カメラのポートがアクティブになります。

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

お知らせ:

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

5.「Save」をクリックして設定を保存します。

7.1.6 マルチキャストの設定

目的:

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

TCP/IP	DDNS	PPPoE	Port	NAT	Multicast	
IP Add	ress	0.	0.0.0			
Stream	Туре	Μ	ain Stre	am	~	
Video F	Port	88	360			
Audio F	Port	88	362			
FEC P	ort	89	960			
FEC R	atio	0				%
	🖹 Sav	е				

図7-7 マルチキャストの設定

手順:

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

お知らせ:

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

7.2 詳細設定

目的:

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

7.2.1 SNMP設定

目的:

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

準備:

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

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



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

手順:

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

SNMP	FTP	Email	HTTPS	QoS	802.1x
SNI	MP v1/v2				
En En	able SNM	Pv1			
En En	able SNM	P v2c			
Read \$	SNMP Con	nmunity	public		
Write 9	SNMP Con	nmunity	private		
Trap A	ddress				
Trap P	ort		162		
Trap C	community		public		
SNI	MP v3				
👽 En	able SNM	Pv3			
Read I	UserName				
Securi	ity Level		no aut	n, no priv	· -
Auther	ntication A	Algorithm	MD5	SHA	
Authe	ntication P	assword		•	
Private	e-key Algo	orithm	() DES	AES	
Private	e-key pase	sword)	
Write I	UserName				
Securi	ity Level		no auth	n, no priv	· 🔻
Authe	ntication A	lgorithm	MD5	SHA	
Authe	ntication P	assword)	
Private	e-key Algo	orithm	DES	AES	
Private	e-key pas	sword)	
SNI	MP Other	r Settings			
SNMP	Port		161		
	間	Save			

図7-8 SNMP 設定

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

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

4.「Save」をクリックして設定を保存し、終了します。

お知らせ:

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

7.2.2 FTP 設定

目的:

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

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

SNMP FTP Ema	I Platform Access HTTPS	QoS 802.1x Integration Protocol
FTP Protocol	FTP	\checkmark
Server Address	0.0.0.0	
Port	21	
User Name		Anonymous
Password		
Confirm		
Directory Structure	Save in the root directory	\sim
Picture Filing Interval	OFF	V Day(s)
Picture Name	Default	\sim
	Upload Picture	
	Test	
🖹 Save		

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



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

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

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

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

IP address_channel number_capture time_event type.jpg (例: 10.11.37.189_01_20150917094425492_FACE_DETECTION.jpg) または、デフォルトの命名ルールにカスタムプレフィックスを追加してカスタマイ ズすることもできます。

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

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

7. 「Save」をクリックし、設定を保存します。

7.2.3 Eメール設定の指定

目的:

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

準備:

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

手順:

- 「Configuration」>「Network」>「Basic Settings」>「TCP/IP」を選択して、 IPv4 アドレス、IPv4 サブネットマスク、IPv4 デフォルトゲートウェイ、および 優先DNS サーバを設定します。
 お知らせ: 詳細については、「7.1.1 TCP/IP 設定」を参照してください。
- 2. 「Configuration」>「Network」>「Basic Settings」>「Email」を選択します。
- 3. 以下の設定を行います。

「Sender」:メール送信者の名前

「Sender's Address」:送信者の電子メールアドレス

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

(例: smtp.263xmail.com)

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

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

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

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

「Interval」:添付画像を送信する2つのアクションの間の時間 「Authentication」:電子メールサーバーで認証が必要な場合は、このチェッ クボックスをオンにし、認証を使用してこのサーバーにログインし、ログイン ユーザー名とパスワードを入力します。



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

「Receiver」テーブル:メールの送信先の受信者を選択します。最大3つの受

信者を設定できます。

「Receiver」: 通知するユーザーの名前

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

SNMP	FTP	Email	HTTPS	QoS	802.1x					
Sende	er		test							
Sende	er's Addre	SS	test@gm	ail.com						
SMTP	Server									
SMTP	Port		25							
E-mai	l Encrypti	on	None			•				
Att	ached Im	age								
Interva	al		2			▼ S				
🔳 Au	thenticati	ion								
Userl	Name									
Passv	vord									
Confir	m									
Re	ceiver									
No.			Receiv	/er			Receiver's	Address		Test
1										Test
2										
3										
		Save								

図7-10 電子メール設定

4. 「Save」をクリックし、設定を保存します。

7.2.4 プラットフォームアクセス

目的:

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

手順:

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

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

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

7.2.5 ワイヤレスダイヤル

目的:

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

お知らせ:

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

手順:

- 「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。
 - 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。
 - アクセス番号、ユーザー名、パスワード、APN、MTU、検証プロトコルを設定します。また、これらのパラメータを空白のままにしておくと、他のパラメータを 設定した後に、デバイスはダイヤル用のデフォルト設定を採用します。
 - ドロップダウンリストからネットワークモードを選択します。オート、3G、4G が選択可能です。「Auto」を選択した場合、ネットワーク選択の優先順位 は4G > 3G > 有線ネットワークの順になります。
 - 4) ダイヤルモードで「Manual」を選択した場合は、オフライン時間を入力しま す。
 - 5) UIM番号(携帯電話番号)を入力します。
 - 6)「Auto」がダイヤルモードとして選択されている場合は、「Edit」をクリックして アーミングスケジュールを設定します。
 - 7)「Save」をクリックし、設定を保存します。

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

7.2.6 HTTPS 設定

目的:

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

お知らせ:

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

手順:

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



図7-11 HTTPS 設定画面

4. 自己署名証明書または認可証明書を作成します。

Install Certificate	
Installation Method	Create Self-signed Certificate
	Signed certificate is available, Start the installation directly.
	Oreate the certificate request first and continue the installation.
Create Self-signed Certificate	Create
🖹 Save	

図7-12 自己署名証明書の作成

- 自己署名証明書を作成する
- (1) インストール方法として「Create Self-signed Certificate」を選択します。
- (2)「Create」をクリックして、作成画面を入力します。
- (3) 国、ホスト名/IP、有効性、およびその他の情報を入力します。
- (4)「OK」をクリックし、設定を保存します。
 お知らせ:すでに証明書がインストールされている場合、「自己署名証明書の作成」はグレー表示になります。
- 要求を作成し、認定証明書をインポートする
- (1) 最初に証明書要求の作成を選択し、インストール方法としてインストールを 続行します。
- (2)「Create」をクリックして、証明書要求を作成します。ポップアップウィンドウ で必要な情報を入力します。
- (3)「Download」をクリックして証明書要求をダウンロードし、署名のために信頼 できる認証局に送信します。

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

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

図7-13 証明書のインポート(1)

b) 最初に証明書要求の作成を選択し、インストールを続行します。

「Browse」と「Install」をクリックし、証明書をデバイスにインポートします。

Install Certificate						
Installation Method	Create Self-signed Certificate					
	O Signed certificate is available, Start the installation directly.					
	Create the certificate request first and continue the installation.					
Create Certificate Request	Create C=CN, H/IP=10.11.11.11					
Download Certificate Request	Download					
Delete Certificate Request	Delete					
nstall Generated Certificate	Browse Install					

図7-14 証明書のインポート(2)

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

Installed Certificate	C=CN, ST=ZJ, L=HZ, OU=embeddedsofteware,	H/IP=10.	Delete
Property	<pre>Subject: C=CN, ST=ZJ, L=HZ, OU=embeddedsofteware, H/IP=10.13.33.209, EM=com.cn Issuer: C=CN, ST=ZJ, L=HZ, OU=embeddedsofteware, H/IP=10.13.33.209, EM=com.cn Validity: 2015-04-29 14:25:24 ~ 2018-04-28 14:25:24</pre>	*	
		-	

図7-15 インストール済み証明書

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

お知らせ:

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

7. 「Save」をクリックし、設定を保存します。

7.2.7 QoS 設定

目的:

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

手順:

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

Video/	Audio DS	CP	0		
Event/	Alarm DS	CP	0		1
Management DSCP		0			
lanag	gement D	SCP	0		
	P				

図7-16 QoS 設定

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

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

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

3. 「Save」をクリックし、設定を保存します。

お知らせ:設定を有効にするには、再起動が必要です。

7.2.8 802.1Xの設定

目的:

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

準備:

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



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

手順:

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

SNMP FTP Email	HTTPS	QoS	802.1x	
Enable IEEE 802.1X				
Protocol	EAP-MD	5		•
EAPOL version	1			•
User Name				
Password				
Confirm				
🖹 Save				

図 7-17 802.1X の設定

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

「Protocol」、「EAPOL version」、「User Name」、「Password」などの802.1X
 を設定します。
 お知らせ: EAPOL versionは、ルーターまたはスイッチのバージョンと同じであ

る必要があります。

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

お知らせ:設定を有効にするには、再起動が必要です。

7.2.9 統合プロトコル

目的:

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

ONVIF

手順:

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

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

7.2.10 帯域幅適応

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

7.2.11 ネットワークサービス

カメラが対応している特定のプロトコルのON/OFFを制御できます。

お知らせ:

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

WebSocket とWebSocketプロトコル

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

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

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

SDKサービスと拡張SDKサービス

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

「SDK Service」: SDKプロトコルを使用します。

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

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

7.2.12 スムーズなストリーミング

目的:

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

準備:

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

手順:

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

SNMP	FTP	Email	Platform Access	HTTPS	QoS	802.1x	Integration Protocol	Network Service	Smooth Streaming
Stream	п Туре		Third Stream		~				
🗹 En	able Smo	oth Stream	ning						
Mode			Auto		\checkmark				
	8	Save							

図7-18 スムーズストリーミングの設定

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

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

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

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

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

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

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

5. 「Save」をクリックし、設定を保存します。

第8章 ビデオ/オーディオ設定

目的:

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

8.1 ビデオ設定

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

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

8.1.1 ビデオ設定

手順:

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

Video	Custom Video	Audio	ROI	Display Info. on Stream	Target Cro
Strear	n Type	Main S	Stream(N	lormal)	
Video	Туре	Video	Stream	•	
Resol	Resolution		2160	•	
Bitrate	е Туре	Variab	le	•	
Video	Quality	Mediu	m	•	
Frame	Rate	25		▼ fps	
Max. I	Bitrate	16384		Kbps	; 🥑
Video	Encoding	H.264		•	
H.264	+	OFF		•	
Profile	•	Basic	Profile	•	
l Fram	ne Interval	25			
SVC		OFF		•	
Smoo	thing		0	50 [Clea	ar<->Smooth]

図8-1 ビデオ設定

2. 「Stream Type」を選択します。

サポートされているストリームタイプがドロップダウンリストに表示されます。

お知らせ:

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

[Video Type]:

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

[Resolution]:

ビデオ出力の解像度を選択します。

[Bitrate Type]:

定数または可変にするビットレートタイプを選択します。

[Video Quality]:

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

[Frame Rate]:

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、さまざまなカメラプラットフォームによって異なります。特定のカメラでは、最大制限は8192 Kbps または 12288 Kbps です。

[Video Encoding]:

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

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

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

お知らせ:

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

[Max. Average Bitrate]:

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

[Profile]:

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

[I Frame Interval]:

1から400に設定します。

[SVC]:

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

[Smoothing]:

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

4. 「Save」をクリックし、設定を保存します。

お知らせ:

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

8.1.2 カスタムビデオ

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

お知らせ:

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

Video	Custom Video	Audio ROI Display Info.	on Stream
Stream	т Туре	+ Add 🗙 Delete	
		Sixth Stream	
		Seventh Stream	
		Eighth Stream	
		Ninth Stream	
		Tenth Stream	
Resol	ution	1280*720P	¥
Frame	e Rate	25	▼ fps
Max.	Bitrate	2048	Kbps
Video	Encoding	H.264	•
Descr	iption	Input description for the stream.	4

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(&、<、>、'、"を除く)を 使用できます。

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

8.2 オーディオ設定

手順:

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

	el No.	Analog Camera1
Audio E	incoding	G.711alaw
Audio Ir	nput	Micln
Input Ve	olume	50
Environ	mental Noise Filter	OFF

図8-3 オーディオ設定

2. 以下の設定をします。

お知らせ:オーディオ設定は、異なるカメラモデルによって異なります。

「Audio Encoding」: G.722.1、G.711 ulaw、G.711alaw、G.726、MP2L2、PCM、MP3 から選択できます。MP2L2では、サンプリングレートとオーディオストリームビット レートを設定できます。PCMの場合、サンプリングレートを設定できます。 「Audio Input」: 接続したマイクとピックアップにそれぞれMicIn とLineIn を選択で

きます。

「Input Volume」: 0 ~100 の間で調整できます。

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

3. 「Save」をクリックし、設定を保存します。

8.3 ROIエンコーディングの設定

目的:

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

Video	Audio	ROI	Display Info. on Stream	Target Cropping
Drav	W Area	Clear		
Str	eam Type			
Stream	m Type		Main Stream(Normal)	•
Fix	ed Region			
🔽 En	able			
Regio	n No.		1	
ROIL	evel		3	
Regio	n Name			
Dy	namic Reg	ion		
🔽 En	able Face	Tracking		
ROIL	evel		3	

図8-4 ROIエンコーディングの設定
手順:

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

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

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

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

8.4 ストリーム上の情報表示

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



図8-5 ストリーム上の情報表示

8.5 ターゲットクロッピングの設定

目的:

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

お知らせ:ターゲット切り出し機能は、モデルによって異なります。

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

第9章 画像設定

目的:

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

9.1 ディスプレイ設定

目的:

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

手順:

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



図9-1 ディスプレイ設定

2. シーンを選びます。

3. カメラの画像パラメータを設定します。

• [Image Adjustment]

「Brightness」は、画像の明るさを表します。値の範囲は1~100 です。 「Contrast」は、イメージのコントラストを表します。値の範囲は1~100 です。 「Saturation」は、画像カラーの彩度を表します。値の範囲は1~100 です。 「Sharpness」は、画像のエッジコントラストを表します。値の範囲は1~100 です。

• [Exposure Settings]

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

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

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

Exposure Settings	
Iris Mode	Auto
Auto Iris Level	50
Exposure Time	1/25 🔹

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。

Day/Night Switch	
Day/Night Switch	Auto
Sensitivity	4 🔹
Filtering Time	5

図9-3 Day/Night Switch

「Day」: カメラは日中モードのままです。

「Night」: カメラは夜間モードのままです。

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

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

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

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

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

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

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

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

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

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

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

• [White Balance]

環境に応じて色温度を調整するためのカメラの補正機能です。

AWB2	-
MWB	
AWB1	
AWB2	
Locked WB	
Fluorescent Lamp	
Incandescent Lamp	
Warm Light Lamp	
Natural Light	

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。

● その他

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

9.2 OSD 設定

目的:

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



図9-5 OSD 設定

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

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

お知らせ:最大8つのテキストオーバーレイを設定できます。

- 8. OSD の位置と位置合わせを調整します。
- 3. 選択して文字を揃えることができます。選択して文字を揃えた場合、左右の 余白と上下の余白を設定できます。

0~2文字は使用できません。カスタムを選択すると、マウスを使用してライブビュ ーウィンドウのテキストフレームをクリックしてドラッグし、位置を調整できます。

10.「Save」をクリックし、設定を保存します。

9.3 プライバシーマスクの設定

目的:

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

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

/07-23-20	015 Thu 14:	:00:39	B	
	_			
915				
14.1				
			1	
			Camera 01	1
Stop Drawing	Clear All			

図9-6 プライバシーマスクの設定

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

9.4 画像オーバーレイの設定

目的:

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

手順:

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



図9-7 ピクチャーオーバーレイ

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

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

9.5 画面切り換えパラメータの設定

目的:

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

Display Settings	OSD Settings	Privacy Mask	Picture Overlay	Image Parameters Switch	_			
Scheduled-S	witch							
Period1	00	:00:00	<u></u>	00:00:00	*	Linked Scene	Normal	~
Period2	00	:00:00	<u></u>	00:00:00	2	Linked Scene	Normal	~
Period3	00	:00:00		00:00:00	6	Linked Scene	Normal	~
Period4	00	:00:00		00:00:00	1	Linked Scene	Normal	\sim
🗎 Sa	ave							

図9-8 画面切り換えパラメータの設定画面

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

第10章 イベント設定

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

10.1 基本イベント

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

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

10.1.1 モーション検出の設定

目的:

モーション検出は、設定された監視領域内の移動物体を検出し、アラーム発生時に ー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。
- 後出されたオブジェクトを緑色の四角形でマークする場合は、「Enable Dynamic Analysis for Motion」チェックボックスをオンにします。

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

otion Detection Vid	eo Tampering	Alarm Input	Alarm Output	Exception
Channel No.	Camera1		*	
Enable Motion Dete	ction			
Enable Dynamic An	alysis for Motion			
Area Settings 〉 Ar	ming Schedule	Linkage Me	thod	
Configuration	Normal			
			Camera 01	

図10-1 モーション検出の有効化

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

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

タスク2: モーション検出のアーミングスケジュールの設定



図10-2 アーミングスケジュール

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



図10-3 アーミングスケジュール

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

- 「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。
- マウスを各日の終わりに動かすと、コピーダイアログボックスがポップアップ 表示され、現在の設定を他の日にコピーできます。
- 5. 「Save」をクリックして設定を保存します。

お知らせ: 各周期の時間は重複できません。1 日に最大8 つの期間を設定できます。 タスク3: モーション検出の連携方法の設定

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

Normal Linkage	Trigger Alarm Output	Trigger Channel
Audible Warning	A->1	🖻 A1
🖻 Send Email		
Notify Surveillance Center		
Full Screen Monitoring		
Upload to ETP		

図10-4 連動方法

お知らせ:連動方法は、カメラの機種によって異なります。

• [Audible Warning]

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

Send Email

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

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

- 「Notify Surveillance Center」
 イベントが発生したときに、例外またはアラーム信号をリモート管理ソフトウェア
 に送信します。
- [Upload to FTP/Memory Card/NAS]

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

お知らせ:

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

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

• [Trigger Alarm Output]

イベントが発生したときに、1つ以上の外部アラームを出力します。

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

●「Expert」設定



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

図10-5 モーション検出のExpertモード

● 日中/夜間スイッチOFF

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

● 日中/夜間自動スイッチ

手順:

- 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。
- カーソルをスライドさせて、昼間の選択したエリアのエリア上のオブジェクトの感度と比率を調整します。
- 5. カーソルをスライドさせて、夜間に選択したエリアのエリア上のオブジェクトの感 度と比率を調整します。
- 通常の設定モードと同様にアーミングスケジュールと連動方法を設定します。
- 7. 「Save」をクリックし、設定を保存します。
- 日中/夜間予約スイッチ

手順:

- 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。

Switch Day and Night Set.	Scheduled-Switch	
Start Time	06:00:00	1
End Time	18:00:00	

図10-6 Switch Day and Night Settings

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

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

10.1.2 ビデオ改ざんアラームの設定

目的:

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

このアラームの検出領域は画面全体です。

- 1. 「Configuration」>「Event」>「Basic Event」>「Video Tampering」を選択します。
- 2. 「Enable Video Tampering」チェックボックスをオンにし、機能を有効にします。
- 「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。
- チェックボックスをオンにすると、映像改ざんにかかる連動方法を選択できます。
 「10.1.1 モーション検出の設定」の「タスク3:モーション検知の連動方法の設定」
 を参照してください。
- 5. 「Save」をクリックして設定を保存します。

10.1.3 アラーム入力の設定

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。

Motion E	Detection	i V	ideo 1	Tamp	ering	Alar	m Input	Alarm	Output	Except	ion			
Alarm Inp	put No.	A<-	-1				•	IP Addr	ess	Local				
Alarm Ty	pe	NO					-	Alarm N	Name					(cannot copy)
👿 Enabl	le Alarm	Input	Hand	lling										
Arming) Schedu	ile >	Lin	kage	Method	I								
×D)elete	Ē	Dele	te A	I									
Mon	0	2		4	6	8	10	12	14	16	18	20	22	24
Tue	0	2		4	6	. 8	10	12	14	16	18	20	22	24
Wed	0	2		4	6	8	10	12	14	16	18	20	22	24
Thu	0	2		4	6	8	10	12	14	16	18	20	22	24
Fri	0	2		4	6	8	10	12	14	16	18	20	22	24
Sat	0	2		4	6	8	10	12	14	16	18	20	22	24
Sun	0	2		4	6	8	10	12	14	16	18	20	22	24

図10-7 アラーム入力の設定

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

10.1.4 アラーム出力の設定

Motion Det	ection \	/ideo 1	Tampe	ring	A	larm I	nput	Ala	rm Output	Exc	eption				
Alarm Ou	itput No.	A->'	1					-	IP Addres	s	Local				
Default S	tatus	Low	Level					Ŧ	Triggerin	g Status	Pulse				~
Delay		5s						-	Alarm Na	me					(cannot copy)
Alarm Sta	atus	OFF	-					- (Ca	annot copy)					
Arming	Arming Schedule														
×D	elete	亩	Delete	All											
Mon	0	2	4		6		8	10	12	14	16	18	20	22	24
Tue	0	2	4	1	6		8	10	12	14	16	18	20	22	24
Wed	0	2	4		6	1	8	10	12	14	16	18	20	22	24
Thu	0	2	4		6		8	10	12	14	16	18	20	22	24
Fri	0	2	4		6		8	10	12	14	16	18	20	22	24
Sat	0	2	4		6		8	10	12	14	16	18	20	22	24
Sun	0	2	4		6		8	10	12	14	16	18	20	22	24
<u> </u>	Manua	l Alarr	m]			i Cop	y to			B	Save			

図10-8 アラーム出力の設定

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

10.1.5 例外アラームの設定

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

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

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:

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

お知らせ:特定のモデルのみが機能をサポートします。

10.1.7 音声アラーム出力の設定



図10-10 音声アラーム出力設定

手順:

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

お知らせ:特定のモデルのみが機能をサポートします。

10.1.8 その他のアラームの設定

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

● ワイヤレスアラーム

目的:

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

手順:

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

Motion Detection	Video Tampering	Exception	PIR Alarm	Wireless Alarm	Emergency Alarm
Select Wireless	. 1	•			
🗑 Enable					
Alarm Name					
Normal Link	age	👿 Trigger Alar	m Output	👿 Trigger Cl	hannel
🛛 Audible War	ning			✓ A1	
📝 Send Email					
Notify Survei	llance Center				
Vpload to FT	Р				
🔲 Wireless au	dible and visual				

図10-11 ワイヤレスアラームの設定

2. ワイヤレスアラーム番号を選択します。

最大8 チャネルの外部ワイヤレスアラーム入力に対応します。

- 3. 「Enable Wireless Alarm」チェックボックスをオンにし、機能を有効にします。
- 4. 必要に応じて、テキストボックスにアラーム名を入力します。
- 5. チェックボックスをオンにすると、ワイヤレスアラームの連動方法を選択でき ます。

- 6.「Save」をクリックし、設定を保存します。
- 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。

Basic Information	Time Settings	RS232	Remote Control	DST
Study				
Wireless Alarm	• 1	•	Study	
Arm / Disarm				
Arm	▼ Os	•	Set	

図10-12 ワイヤレスアラームの設定

● PIRアラーム

目的:

侵入者が検出器の視野内を移動すると、PIR (受動赤外線)アラームが発動されま す。人、または犬や猫などの他の生物によって放散される熱エネルギーを検出す ることができます。

手順:

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

Motion De	etection	Vide	o Tamper	ring	Exception	PIR	Alarm	Wirel	ess Alarm	En	nergency /	Alarm	
I Ena Alarm I	ble Name												
Armin	ng Schedu Delete		Linkage Delete Al	Method I									
Mon	0	2	4	6	8	10	12	14	16	18	20	22	24
Tue	0	2	4	6	8	10	12	14	16	18	20	22	24
Wed	0	2	4	6	8	10	12	14	16	18	20	22	24
Thu	0	2	4	6	8	10	12	14	16	18	20	22	24
Fri	0	2	4	6	8	10	12	14	16	18	20	22	24
Sat	0	2	4	6	8	10	12	14	16	18	20	22	24
Sun	0	2	4	6	8	10	12	14	16	18	20	22	24

図10-13 PIR アラームの設定

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

Basic Information	Time Settings	RS232	Remote Control	DST
Study				
Remote Control	▼ Study			
Arm / Disarm				
Arm	▼ Os	•	Set	

図10-14 PIR アラームのアーミング

● 緊急アラーム

目的:

リモコンの緊急ボタンを押すと、緊急時に緊急アラームを通知できます。 *お知らせ:* 緊急アラームにはリモコンが必要です。まず「Configuration」> 「System」>「System Settings」>「Remote Control」の順に選択して、リモートコン トロールを調べます。

手順:

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

Motion Detection Video Tampering Exception PIR Alarm Wireless Alarm Emergency Alarm								
	📄 Normal Linkage	🔽 Trigger Ala	rm Output	Trigger	Trigger Channel			
	Variable Warning			☑ A1				
	📝 Send Email							
	Notify Surveillance Center							
	Upload to FTP							
	Mireless audible and visual							

図10-15 緊急アラームの設定

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

10.2 スマートイベント

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

10.2.1 オーディオ例外検出の設定

目的:

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

*お知らせ:*オーディオ例外検出機能は、モデルによって異なります。

手順:

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

Exception Detection Arming Schedule Linkage Method
Exception Detection
Audio Loss Detection
Sudden Increase of Sound Intensity Detection
Sensitivity 50
Sound Intensity Threshold 50
Sudden Decrease of Sound Intensity Detection
Sensitivity 50
Real-time Volume

図10-16 オーディオ例外検出

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

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。サウンドスティプドロップの検出感度としきい値は設定が可能です。

お知らせ:

- 「Sensitivity」: 設定範囲[1-100]、値が小さいほど、検出するための変化が 激しくなります。
- 「Sound Intensity Threshold]: 設定範囲[1-100]、環境内の音をフィルタリン グできます。環境音が大きいほど、値を高くする必要があります。実環境に 合わせて調整できます。
- 画面上で音声のリアルタイム音量を確認できます。
- 「Arming Schedule」をクリックして、アーミングスケジュールを設定します。詳細 な手順については、「タスク2: モーション検出のアーミングスケジュールの設定」 を参照してください。
- 「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:

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

Enable	
Sensitivity	50
📄 Normal Linkage	
🔲 Send Email	
Notify Surveillance Center	

図10-17 デフォーカス検出の設定

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

10.2.3 シーンチェンジ検出の設定

目的:

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

*お知らせ:*シーンチェンジ検出機能は、カメラの機種によって異なります。

手順:

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



図10-18 シーンチェンジ検出

- 2 「Enable」チェックボックスをオンにし、機能を有効にします。
- 3 スライダーをクリック・ドラッグして、検出感度を設定します。

感度の値は1 ~100 の範囲で、値が高いほどシーンの変化でアラームが発生 しやすくなります。

- 「Arming Schedule」をクリックして、アーミングスケジュールを設定します。詳細な手順については、「タスク2:モーション検知のアーミングスケジュールの設定」を参照してください。
- 5. 「Linkage Method」をクリックして、監視センターへの通知、Eメールの送信、 FTP/メモリーカード/NASへのアップロード、トリガ・チャンネル、アラーム出 力など、シーン変更の連動方法を選択します。
- 6.「Save」をクリックし、設定を保存します。

10.2.4 顔検出の設定

目的:

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

- 手順:
- 「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。
- 「Enable Dynamic Analysis」チェックボックスをオンにすると、検出された顔がライ ブビデオで緑の長方形でマークされます。
 お知らせ:検出された顔をライブビデオでマークするには、「Configuration」 > 「Local」に移動してルールを有効にします。
- 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。
- 「Arming Schedule」をクリックして、アーミングスケジュールを設定します。詳細な 手順については、「タスク2:モーション検知のアーミングスケジュールの設定」を 参照してください。

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



図10-19 顔検出

7.「Save」をクリックし、設定を保存します。

10.2.5 侵入検知の設定

目的:

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

手順:

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



図10-20 侵入検知

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

「Region」: ライブビュー画像上のあらかじめ定義された頂点領域です。リージョン に出入りする人、車両、その他のオブジェクトなどのターゲットが検出され、設定 されたアラームが発生します。
最大値を設定します。サイズと最小有効なターゲットのサイズ。有効なターゲットサイズ より小さいまたは大きいターゲットは、検出できません。ライブ画像内のポイントを開始 点として選択し、最大サイズまたは最小値として長方形を描画します。

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

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

- 5. 検知領域を設定します。検出領域の4つの頂点を指定するには、ライブビデオ上 をクリックします。
- 6. 検出対象を選択します。人間と車両が利用可能です。検出対象が選択されていない場合、検出されたすべてのターゲットが報告されます(人間と車両を含む)。
- 7. 侵入検知の時間しきい値を設定します。
 「Threshold」: 設定範囲[0s-10s]、領域内でオブジェクトがロータリングする時間のしきい値です。値を0 に設定すると、領域に入ったオブジェクトの直後に アラームが発生します。
- スライダーをドラッグして感度値を設定します。
 「Sensitivity」: 設定範囲[1-100]。感度とは、あらかじめ定義された領域に入る許

容可能なターゲットの身体部分の割合を表します。

感度 = 100 - S1/ST*100

S1 は、事前定義された領域を横切るターゲットボディパーツを表します。

STは完全な標的本体の略です。

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

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

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

ム、可聴アラームをサポートしています。

12.「Save」をクリックし、設定を保存します。

10.2.6 ライン交差検知の設定

目的:

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

お知らせ: ライン公差検出機能は、カメラの機種により異なります。

手順:

1. $\lceil Configuration \rfloor > \lceil Advanced Configuration \rfloor > \lceil Smart Event \rfloor > \lceil Line$

Crossing Detection」を選択します。

Line	1			•
06-09-	2015 15:15:5	52		
	m			
	B	► <u>A</u>		
Max. Size	Min. Size Det	ection Area	Ca	mera 01
Detection Targ	jet 🗌 Hu	man 🗌	Vehicle	
Direction	A<->[В		~
Sensitivity		0	[50

図10-21 ライン交差検出

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

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

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

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

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

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

8. スライダーをドラッグして感度値を設定します。

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

感度 = 100 - S1/ST*100

S1 は、事前定義されたラインを横切るターゲットボディパーツを表します。

STは完全な標的本体の略です。

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

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

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

「Clear」をクリックすると、定義済みの行をすべてクリアできます。

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

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

10.2.7 領域進入検出の設定

目的:

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

手順:

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

Region	
07-08-2015 W	ed 12:59:09
	-
Max. Size Min.	Size Detection Area Clear
Detection Target	🗌 Human 📋 Vehicle
Sensitivity	50

図10-22 領域進入検出

- 2. 「Enable」チェックボックスをオンにし、機能を有効にします。
- 3. 検出設定のドロップダウンリストからリージョンを選択します。
- 4. 最大値を設定します。サイズと最小有効なターゲットのサイズ。有効なターゲット サイズより小さいか大きいターゲットは検出できません。
 「Max. Size」:有効なターゲットの最大サイズ。より大きなサイズのターゲットは、 検出しません。
 「Mix OS: A ちかなり、ビットの見かせくず、サイズがかさいり、ビットはや出し

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

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

7. スライダーをドラッグして感度値を設定します。

感度: 範囲[1-100]。感度とは、あらかじめ定義された領域に入る許容可能なター

ゲットの身体部分の割合を表します。

感度 = 100 - S1/ST*100

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

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

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

10.2.8 領域退出検出の設定

目的:

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

手順:

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

Region 1
07-08-2015 Wed 12:59:09
Max. Size Min. Size Detection Area Clear
Detection Target 🛛 Human 🗌 Vehicle
Sensitivity 50

図10-23 領域退出検出

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

出しません。

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

- 6. 検出対象を選択します。人間と媒体が利用可能です。検出対象が選択されていない場合は、人および車両を含むすべての検出対象が報告されます。
- スライダーをドラッグして感度値を設定します。
 「Sensitivity」:設定範囲[1-100]。感度は、あらかじめ定義された領域から出る許容可能なターゲットの身体部分のパーセンテージを表します。
 感度 = 100 S1/ST*100
 S1 は、事前定義された領域から出るターゲットボディパーツを表します。ST
 は完全な標的本体の略です。
 例:値を60に設定すると、40%のボディパーツがリージョンから出た場合にのみアクションを終了するリージョンとしてカウントできます。

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

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

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

11.「Save」をクリックし、設定を保存します。

10.2.9 無人手荷物検出の設定

目的:

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

手順:

1. $\lceil Configuration \rfloor > \lceil Event \rfloor > \lceil Smart Event \rfloor > \lceil Unattended Baggage$

Detection」を選択します。

Area Cattinga	Armina	chodula Lin	kana Mathad		
Area Settings	Arming a		kage Method		
Region		1		•	
		I			
07-08-2	2015 Wed	13:15:10			
		-			
			-	-	
			-		
	#1.8				
		_			
			_	-	
Max. Size	Min. Size	Draw Area	Clear		
Max. Size Threshold(s)	Min. Size	Draw Area	Clear	5	
Max. Size Threshold(s)	Min. Size	Draw Area	Clear	50	

図10-24 無人手荷物検出

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

- 4. エリア設定をクリックし、エリアの描画をクリックしてエリアの描画を開始します。
- 5. ライブビデオをクリックして検出領域の4つの頂点を指定し、右クリックして描 画を完了します。
- 6. 最大値を設定します。サイズと最小有効なターゲットのサイズ。有効なターゲットサイズより小さいか大きいターゲットは検出できません。
 「Maz. Size」: 有効なターゲットの最大サイズ。より大きなサイズのターゲットは、検出しません。
 「Min. Size」: 有効なターゲットの最小サイズ。サイズが小さいターゲットは検出しません。
- 7. 描画が終了したら、「Stop Drawing」をクリックします。
- 無人手荷物検知の時間しきい値と検知感度を設定します。
 「Threshold」: 設定範囲[5-100s]、領域に残っているオブジェクトの時間のしきい値。値を10に設定すると、オブジェクトが放置された後にアラームが発生し、10 秒間領域に留まります。
- スライダーをドラッグして感度値を設定します。
 「Sensitivity」:設定範囲[1-100]。感度とは、あらかじめ定義された領域に入る 許容可能なターゲットの身体部分の割合を表します。
 感度 = 100 - S1/ST*100

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

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

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

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

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

10.2.10 オブジェクトの退出検知の設定

目的:

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

手順:

1. $\lceil Configuration \rfloor > \lceil Advanced Configuration \rfloor > \lceil Smart Event \rfloor > \lceil Object$

Removal Detection」を選択します。

Al Fueble	1			
Area Settings	Arming So	chedule / Link	age Method	
Region	1			•
			-11	
	#1#		HIN	

図10-25 物体除去検出

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

- 3. 検出設定のドロップダウンリストから「Region」を選択します。
- 4. 「Area Settings」をクリックし、「Draw Area」をクリックしてエリア描画を開始します。
- 5. ライブビデオをクリックして検出領域の4つの頂点を指定し、右クリックして描画 を完了します。
- 6. 最大値を設定します。サイズと最小有効なターゲットのサイズ。有効なターゲットサイズより小さいか大きいターゲットは検出できません。
 「Maz. Size」:有効なターゲットの最大サイズです。より大きなサイズのターゲットは、検出しません。
 「Min. Size」:有効なターゲットの最小サイズです。サイズが小さいターゲットは検出しません。
- 7. 描画が終了したら、「Stop Drawing」をクリックします。
- オブジェクト除去検出の時間しきい値を設定します。
 「Threshold」: 設定範囲[5-100s]。領域から除去されるオブジェクトの時間のしきい値です。

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

9. スライダーをドラッグして感度値を設定します。

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

感度 = 100 - S1/ST*100

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

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

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

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

10.3 VCA 設定

10.3.1 挙動解析

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

0	verlay & Capture		
	Display on Stream		
	👿 Display VCA Info. on S	tream	
	Display on Picture		
	Display Target Info. on	Alarm Picture	
	👿 Display Rule Info. on A	larm Picture	
	Snapshot Settings		
	👿 Upload JPEG Image to	o Center	
	Picture Quality	High	•
	Picture Resolution	1080P(1920*1080)	•
	🖹 Save		

図10-26 挙動解析

☆ オーバーレイとキャプチャ

表示情報には、ピクチャー上の表示とストリーム上の表示が含まれます。

「Display VCA info. on Stream」: ライブビューまたは再生中は、緑色のフレー

ムがターゲットに表示されます。

「Display Target info. on Alarm Picture」: チェックボックスをオンにすると、アッ

プロードされたアラーム画像上のターゲットにフレームが表示されます。

「Display Rule info. on Alarm Picture」: キャプチャされたターゲットと設定さ れた領域がアラームピクチャにフレーム表示されます。 *お知らせ*: ローカル設定でルールが有効になっていることを確認してください。 「Configuration」 > 「Local Configuration」 > 「Rules」を選択し有効にします。 「Snapshot Setting」: 撮影した画像の画質と解像度を設定します。

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

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

✤ 「Camera Calibration」

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

手順:

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

「Input Basic Data」: カメラの取り付け高さ、視野角、水平比を手動で入力します。 「Draw on Live View Video」: 「Draw Verification Line (Horizontal) / (Vertical)」をクリックして、ライブビューに水平/垂直線を描き、実長フィールドに 実際の長さを入力します。描かれたリファレンス線とその長さにより、カメラはラ イブビューに他のオブジェクトが表示されていると判断します。 水平照合 (小) /垂直照合 (シーンクリックして、ライブビデオに水平/垂直線を 描き、「Start Verifing) (シーンクリックして線の長さを計算します。計算したライン長と実際の長さを比較して、設定したキャリブレーション情報を検証します。
 お知らせ: ライブビューが停止している場合、カメラキャリブレーションは無効です。



図10-27 「Draw on Live View」画面

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

♦ Shield Region ↓

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

手順:

- 1. 「Shield Region」をクリックして、シールド領域設定画面を表示します。
- 六角形のサイン をクリックし、ライブビューウィンドウでシールド領域を左ク リックしてエンドポイントを描画し、右クリックで領域描画を終了します。
 お知らせ:
 - 最大10辺のポリゴン領域に対応しています。
 - ≤をクリックすると、描画した領域を消去します。
 - ライブビューが停止している場合、シールド領域を描画できません。
- 3.「Save」をクリックし、設定を保存します。
- ✤ 「Rule」

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

お知らせ: 各動作の詳細情報については、各章を参照してください。

手順:

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

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

lule List									+
Enable	No.		Rule N	Vame	ų.	Ru	ule Type		
	1		Test			Line Crossing		•	×
Filter by	Pixel		-	Line Crossing		Bidirectional	•		
Max. Size	0	*	0	Detection Targe	t	All	•		
Min. Size	0	* [0						
ombined Rule	n.								+
able	No.	ti -	Rule N	Vame		Ru	ule Type		
Min Min	Max			-		J	H		(
	Max								Ę
	Max								

図10-28 ルールの設定

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

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

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

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

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

- 組み合わせルールのチェックボックスをオンにし、動作分析のルールを 有効にします。
- 5. 結合されたルールのルールA とルールB として2つの設定された単ールー ルを選択し、2つの単ールールの最小時間間隔と最大時間間隔を設定して から、アラームフィルタリングの単ールールの動作順序を選択します。 *お知らせ*:
 - ルールタイプを「None」として選択した場合、ルールオプションは無効になり、動作分析を設定できません。
 - 最大8つの単ールールと2つの結合ルールを設定できます。また、結合 ルールに対して、ライン交差、侵入、領域退出および領域進入をサポ ートされています。
- 6. 「Save」をクリックし、設定を保存します。
- 7. 「Arming Schedule」をクリックして、アーミングスケジュールを設定し、「Save」クリックしして設定を保存します。
- 8. 「Linkage Method」をクリックして、各ルールに対応する連携方法のチェッ クボックスをオンにし、「Save」をクリックして設定を保存します。

✤ 詳細設定

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

• [Parameter]

以下のパラメータを設定して、設定を詳細化します。

Parameters	Global Size Fi	lter		
Behavior An	alysis Version 🛛	/3.5.0build20150518	}	
Detectio	n Parameters			
Detection	n Sensitivity		3	
Backgrou	und Update Rate		2	
Single	Alarm			
Leave	s Interference S			
Output T	ype	Target Center	Bottom Center	Top Center
Restore	Parameters			
Restore	Defaults	Restore		
Restart V	/CA	Restart		

図10-29 詳細設定

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

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

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

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

「Output Type」:フレームの位置を選択します。ターゲット中心、ボトム中心、 トップ中心が選択可能です。例えば、ターゲット中心が選択されている場合、 ターゲットはフレームの中心になります。 「Restore Default」: クリックすると設定したパラメータがデフォルトに戻ります。 「Restart VCA」: 挙動解析のアルゴリズムライブラリを再起動します。

• 「Global Size Filter」

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

手順:

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

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

お知らせ:

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

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

お知らせ:

- 描画領域は、背景アルゴリズムによってピクセルに変換されます。
- ライブビューが停止している場合は、グローバルサイズフィルターは設定できません。
- 最大サイズの長さは最小サイズの長さよりも長く、幅も長くする必要があります。
- 3.「Save」をクリックし、設定を保存します。

10.3.2 フェイスキャプチャ

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

☆ オーバーレイとキャプチャ

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

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

Snapshot Settings]:

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

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

[Camera Information]:

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

[Text Overlay Information]:

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

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

手順:

 六角形のサイン 〇 をクリックし、ライブビューウィンドウでシールド領域を 左クリックしてエンドポイントを描画し、右クリックで領域描画を終了します。

お知らせ:

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



図10-30 シールド領域の描画

- 2.「Save」をクリックし、設定を保存します。
- ◇ ルール

手順:

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

- 六角印 たクリックして、フェイス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左クリックのエンドポイントで領域を描画 し、右クリックして領域の描画を終了します。
 お知らせ:
 - ポリゴン領域(4~10辺)の辺に対応。
 - ライブビューが停止している場合は、設定した領域を描くことはできません。
- 4. 「Save」をクリックして設定を保存します。

✤ 詳細設定

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

Parameters	
Face Capture Version V4.1.0build1	80710
Detection Parameters	
Generation Speed	3
Sensitivity	3
Capture Parameters	
Face Capture Mode Best Sh	ot 🔿 Quick Shot
Capture Times	1
Capture Interval	1 frame
Capture Threshold	4
Face Exposure	
Reference Brightness	50
Min. Duration	60 minute(s)
Face Filtering Time	0 s
() The Filtering Time only works in Bes	t Shot mode. If the Filtering Time is changed, the actual capture times may be less than the set times.
Invalid Capture Filter	
Restore Parameters	

図10-31 詳細設定

「Detection Parameters」:

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

[Capture Parameters]:

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

 「Best Shot」: ターゲットが検出領域を離れた後のベストショット。
 「Capture Times」[1~10]: 設定したエリアに顔が留まっている間に、顔が キャプチャされる時間を指します。デフォルト値は1です。
 「Capture Interval」[1~255 Frame]: 写真をキャプチャするフレーム間隔。
 デフォルト値を1に設定すると、カメラがすべてのフレームで顔をキャプチャすることを意味します。

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

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

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

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

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

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

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

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

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

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

10.3.3 人数カウント

目的:

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

お知らせ:

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

手順:

1. 「Configuration」>「Counting」を選択します。



図10-32 人数カウント設定

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

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

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

お知らせ:

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

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

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

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

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

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

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

^Advanced			
Detection Line Start Point(0-1000)	X= 240	Y=	733
Detection Line End Point(0-1000)	X= 835	Y=	733
Suggested Calibration Line Width	134 📿		
Calibration Line Width(0-595)	129		
🖹 Save			

図10-33 人数カウント設定-高度

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

お知らせ:

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

10.3.4 カウント

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

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

お知らせ:

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

1. 「Configuration」>「Counting」を選択します。



図10-34 カウント設定

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

4. 検波ラインを設定します。

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

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

お知らせ:

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

お知らせ:

カウント統計はアプリケーションタブで計算されます。

「Application」に移動して、カウント統計をチェックします。

10.3.5 ヒートマップ

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

手順:

1. 「Configuration」>「Heat Map」を選択します。



図10-35 ヒートマップ設定

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

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

4. 描画領域のパラメータを設定します。

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

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

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

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

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

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

お知らせ:

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

10.3.6 道路交通

目的:

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

お知らせ:道路交通機能は、モデルによって異なります。

● 検出設定

手順:

- リストから検出タイプを選択します。車両検知と混合交通検知が選択可能です。
 お知らせ: 道路交通の検知タイプを切り替える場合は、デバイスを再起動して新しい設定をアクティブにします。
- 2 「Enable」のチェックボックスをオンにし、検出機能を有効にします。
- 対応するドロップダウンリストでレーン番号を選択します。最大4つのレーンを選択できます。
- 4. レーンラインをクリック・ドラッグして位置を設定するか、ラインエンドをクリック・ド ラッグしてラインの長さと角度を調整します。
- 5. 映像中の車両の大きさが赤枠の大きさに近くなるように、カメラのズーム倍率を 調整します。赤枠の位置のみ調整可能です。

お知らせ:レーンごとに一度にキャプチャできるナンバープレートは1つだけです。

 たンバープレートの属性が認識できない場合は、ドロップダウンリストからそれ ぞれの略称を選択します。

- 7. アーミングスケジュールを設定します。
 - 1) 「Arming Schedule」をクリックします。
 - 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。
 - マウスを各日の終わりに動かすと、コピーダイアログボックスがポップアップ表示され、現在の設定を他の日にコピーできます。
 - 4)「Save」をクリックし、設定を保存します。

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

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

10.3.7 キュー管理

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

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

お知らせ:

特定のモデルのみがこの機能をサポートしています。

ルール設定

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

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

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

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

手順:

- 1. エリア設定
 - a) 領域を追加します。最大3つの領域がサポートされます。
 領域とは、検出がアクティブである定義された領域です。
 領域を描画する場合、ターゲットの有効な領域入力アクションは、その領域
 に自分の頭部と肩が入ることに注意してください。

手順:

- a-1 「Add Region」をクリックします。
- a-2 色ドロップダウンリストからリージョンの色を選択します。
- a-3 右クリックしてリージョンを描画し、リージョンの境界を決定します。リージョンでは、最大10のエッジがサポートされます。
 「Move the region」: リージョンを選択してドラッグします。
 「Adjust the region boundary」: 領域を選択し、領域の端の終点を

ドラッグします。

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

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

Regional People Queuing-Up				
Waiting Time Detection				
Real-time Data Upload				
Area Settings Arming Schedule Linka	age Method			
1-23-2018 Jue 11:46:58	Region1 28	Region	Region1	~
ge here at another	ingia i	Region Name	Region1	0
La Transformer	1 228 09	Alarm Interval	300 S () In the set in	nterval, trigg
		Regional People Queu	ing-Up Settings	
		OSD		
	ATTREAM	Alarm Trigger Condition	Greater than Threshold	~
000	X	Alarm Threshold	5 opersons (i) An :	alarm is trigg
	1	Waiting Time Detection	n Settings	
		Alarm Trigger Condition	Greater than Threshold	\sim

図10-36 キュー管理ルールの設定

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

「Region Name」: OSD 情報として表示されます。

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

b-2 リージョンのキューイングアップ設定を行います。

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

「Alarm Trigger Condition」:領域内の人数が設定したしきい値より大きい、小さい、等しい、または等しくない場合、アラームが発生します。 「Alarm threshold」:アラームしきい値条件が満たされると、アラームが発生します。 b-3 待ち時間検出の設定をします。

「Alarm Trigger Condition」: 領域内の人数が設定したしきい値より大き い、小さい、等しい、または等しくない場合、アラームが発生します。 「Alarm threshold」: アラームしきい値条件が満たされると、アラームが 発生します。

- c) 必要に応じて上記の手順を繰り返して、他の領域を設定します。最大3つの 領域がサポートされます。
- アーミングスケジュール
 機能のアーミングスケジュールを設定します。設定期間中は機能が有効です。
 「タスク2:モーション検知のアーミングスケジュールの設定」を参照してください。
- 連動方法を設定します。
 発生したアラーム情報の転送や、他のアクションを行うための連携方法を設定 することができます。「タスク3:モーション検知の連動方法の設定」を参照してく ださい。
- 4. 詳細設定

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

第11章 ストレージ設定

準備:

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

11.1 レコードスケジュールの設定

目的:

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

手順:

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



図11-1 録画スケジュール画面

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

Advanced		×
Overwrite		
Pre-record	5s	•
Post-record	5s	•
Stream Type	Main Stream	•

図11-2 レコードパラメータ

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

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

● 「Stream Type」:録画するストリームタイプを選択します。

お知らせ、録画パラメータの設定は、モデルによって異なります。

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

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

● モーション検出による録画

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

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

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

アラームによる録画

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

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

● モーション検出とアラームによる録画

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

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

● モーション検出による録画 | アラーム

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

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

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

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

11.2 キャプチャスケジュールの設定

目的:

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

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



図11-3キャプチャスケジュール設定

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。

Advanced			×
Stream Type	Sub Stream		•
		ОК	Cancel

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。
 - キャプチャする画像の「Format」、「Resolution」、「Quality」、「Interval」を選択し ます。
 - (3)「Enable Event-triggered Snapshot」チェックボックスをオンにし、イベント連携スナップショットを有効にします。
 - (4)「Format」、「Resolution」、「Quality」、「Interval」、「Capture Number」を選択 します。

Record Schedule Captu	re	
Capture Schedule	Capture Parameters	
Timing		
Enable Timing Snapsh	ot	
Format	JPEG	•
Resolution	704*576	•
Quality	High	•
Interval	500	millisecond
Event-Triggered		
Enable Event-Triggered	l Snapshot	
Format	JPEG	•
Resolution	704*576	•
Quality	High	•
Interval	500	millisecond
Capture Number	4	
🗎 Save		

図11-5 キャプチャパラメータの設定

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

11.3 ネットHDD の設定

準備:

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

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

н	DD Management Net HI	DD			
	Net HDD				
	HDD No.	Server Address	File Path	Туре	Delete
					×
	Mounting Type SMB/CI	FS Vser Name cxy1	Password •••••	I	est
	2	10.10.36.252	/dvr/yangjian_1	NAS	×
	3			NAS	×

図11-6 ネットワークディスクの追加

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

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



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

HDD N	lanagement	Net HDD								
H	IDD Manageme	ent	Format							
V	HDD No.	Capacity	Free space	Status	Туре	Property	Progress			
V	9	9.84GB	0.00GB	Normal	NAS	R/W				
(Quota									
1	Max.Picture Ca	acity 4.50	GB							
F	Free Size for Pi	cture 0.00	IGB							
	Max. Record Ca	pacity 14.2	25GB							
F	Free Size for Re	ecord 6.75	GB							

図 11-7 ストレージ管理画面

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

初期化が完了すると、ディスクの状態は正常になります。

H)D Manageme	nt					Set	Format
	HDD No.	Capacity	Free space	Status	Туре	Property	1	Progress
1	9	20.00GB	0.00GB	Formatting	NAS	R/W		

図11-8 ディスクステータスの表示

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

Quota		
Max.Picture Capacity	4.75GB	
Free Size for Picture	4.75GB	
Max. Record Capacity	14.50GB	
Free Size for Record	14.50GB	
Percentage of Picture	25	%
Percentage of Record	75	%
🖹 Save		

図11-9 クォータ設定

お知らせ:

最大 8台の NASディスクをカメラに接続できます。

11.4 メモリーカード検出

目的:

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

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

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



図11-10 メモリーカードの検出

 Status Detection」タブをクリックし、メモリーカードのステータスを表示します。
 「Remaining Lifespan」:空き容量のパーセンテージを示します。メモリーカードの 空き容量は、その容量やビットレートなどの要因に左右されます。空き容量が不 足している場合は、メモリーカードの交換が必要です。
 「Health Status」:メモリーカードの状態を示します。状態の説明には、良好、不 良、損傷の3 つがあります。「Arming Schedule」と「Linkage Method」が設定され ている場合、ヘルスステータスが良好以外であれば、通知を受け取ります。 *お知らせ:* ヘルスステータスが良好でない場合は、メモリーカードを変更することを推奨します。

3. 「R/W Lock」をクリックして、メモリーカードにロックを追加します。

R/Wロックを追加すると、メモリーカードはロック解除時にのみ読み書きできます。

HDD Management	Net HDD	Memory Card Detection	_
Status Detection	R/W Lock	Arming Schedule	Linkage Method
Lock Switch	ON		•
Password Settings	••••	••	0
🗎 Save			

図11-11 R/W ロック設定

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

● ロック解除

- (1) ロックしているカメラでメモリーカードを使用すると、自動的にロック解除が行われ、ユーザーの方々にはロック解除の手順は一切必要ありません。
- ② 別のカメラでメモリーカード(ロック付き)を使用する場合は、「HDD Management」に進み、メモリーカードのロックを手動で解除することができます。メモリーカードを選択し、「Format」ボタンの横にある「Unlock」をクリックします。次に、正しいパスワードを入力してロックを解除します。
 お知らせ:
 - メモリーカードは、ロックが解除されている場合にのみ読み書きできます。
 - メモリーカードにロックをかけたカメラを工場出荷時の状態に戻した場合は、「HDD Management」画面からメモリーカードのロックを解除できます。

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

11.5 Liteストレージの設定

目的:

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

お知らせ:

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

第12章 再生

目的:

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

手順:

1. メニューバーの「Playback」をクリックして再生画面に入ります。

Li	ve View	Playback	Picture	Application	Configura	ation 💄	admin	() ⊦	lelp 🖸	► Log	out
						Status:					
								Jur	20	15	▶ ₩
							Sun	Mon Tue	Wed Th	u Fri	Sat
							31	1 2	3 4	5	6
							7	8 9	10 1	12	13
					2 2		14	15 16	17 1	3 19	20
and the second se							21	22 23	24 2	5 26	27
							, 28	29 30	1 1	3	4
the second se							5	6 7		10	11
								Q	Search		1
							-				-
							Se	et plavbac	k time		
		I►			🖸 🤸 🔍	🐀 – 📩	0	00 : 00	: 00	4	
									~		- +
01:00 02:00 03:00	04:00	05:00	2015-06-11 0 06:00 07	6:44:01 7:00 08:00	09:00	10:00		11:00	12	00	
							- 0.44		Alexan		
10 III III III III III III III III III I						Command	Cont	inuous	Alarm	= Ma	inual

図12-1 再生画面

2. 日付を選択し、「Search」をクリックします。

-	(Мау		2015		• •
Sun	Mon	Tue	Wed	Thu	Fri	Sat
26	27	28	29	30	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
21	1	2	3	1	8	63

図12-2 サーチ画面

3. ▶ をクリックしてこの日付にあるビデオファイルを再生します。
 再生画面の下部にあるツールバーを使用し、再生プロセスをコントロールできます。

	-	н	₩	₽	0	s	Ð,	•	\mathbf{t}
--	---	---	---	---	---	---	----	---	--------------

図12-3 再生ツールバー表

12-1 ボタンの説明

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

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

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



図12-4 再生時間の設定

2015-06-15 05:34:54										
03:00	04:00	05:00	06:00	07:00	08;00	09;00				

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



第13章 ピクチャー

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

- 画像検索を処理する前に、HDD、NAS、またはメモリーカードが正しく設定されていることを確認してください。
- キャプチャスケジュールが設定されていることを確認します。「Configuration」> 「Storage」>「Schedule Settings」>「Capture」を選択して、取り込みスケジュー ルを設定します。

		Live V	iew Playback	Picture	Application	Configu	ration	
Download by File								
Search Conditions	Fi	le List				🛓 Downloa	ad 👍 Stop Do	
File Type		No.	File Name	Time		File Size	Progress	
Continuous		1	ch01_0800000000068600	2015-07-10 15:35	5:13	134 KB		^
Start Time		2	ch01_0800000000068700	2015-07-10 15:35	5:18	134 KB		E
2015-07-02 00:00:00		3	ch01_0800000000068800	2015-07-10 15:35	5:24	134 KB		
End Time		4	ch01_0800000000068900	2015-07-10 15:35	5:29	132 KB		
2015-07-10 23:59:59		5	ch01_0800000000069000	2015-07-10 15:35	5:34	132 KB		
		6	ch01_0800000000069100	2015-07-10 15:35	5:39	133 KB		
Q Search		7	ch01_0800000000069200	2015-07-10 15:35	5:45	133 KB		
		8	ch01_0800000000069300	2015-07-10 15:35	5:50	131 KB		
		9	ch01_0800000000069400	2015-07-10 15:35	5:55	131 KB		
		10	ch01_0800000000069500	2015-07-10 15:36	6:01	132 KB		
		11	ch01_0800000000069600	2015-07-10 15:36	6:06	132 KB		~
						Total 1285 Items	s << < 1/13	> >>

図13-1 ピクチャー・サーチ・画面

手順:

- ドロップダウンリストから「File Type」を選択します。連続、モーション、アラーム、モーション|アラーム、モーション&アラーム、ラインクロッシング、侵入検知、シーンチェンジ検知が選択できます。
- 2. 「Start Time」と「End Time」を選択します。
- 3.「Search」をクリックして、一致する画像を検索します。

4. 画像のチェックボックスをオンにし、「Download」をクリックして選択した画像を ダウンロードします。

お知らせ:

一度に最大4000枚まで表示できます。

第14章 アプリケーション

「Application」をクリックして、統計カウント画面を表示します。ローカルまたはネット ワーク上のストレージに保存されているカウントデータを検索、表示、ダウンロード できます。

お知らせ:アプリケーション機能は、モデルによって異なります。

14.1 フェイスキャプチャ統計

フェイスキャプチャ機能を有効にすると、キャプチャした顔データをアプリケーション タブから表示およびダウンロードできます。より視覚的な結果を導くために、さまざま なチャートでデータを表示することができます。

	Live View	Playback	Picture	Application	Configuration	👤 admin	👔 Help	E→ Logout
Face Capture Statistics								
Search Conditions	Statistics Results			Table	Pie Chart			
Report Type Daily Report Statistics Type Age Start Time 2015-06-15					96%	4%	Tri Y M E	eenage 0 outh 162 iiddle-aged 8 Iderly 0
Counting								

図14-1 アプリケーション画面:

手順:

- 1. レポートタイプを選択します。日報、週報、月報、年報を選択可能です。
- 2. 統計の種類を選択します。
- 開始時刻を選択し、「Counting」をクリックします。
 集計結果は、統計結果領域に表示されます。「Table」または「Pie chart」をクリックして、結果をさまざまな方法で表示します。
 お知らせ: カウント結果をテーブルにリストすると、データをエクセルファイルにエクスポートできます。

14.2 人数統計

人数計算機能を有効にすると、人数計算データをアプリケーションタブから表示 およびダウンロードできます。より視覚的な計算結果を導くために、さまざまなチャートでデータを表示することができます。

- 手順:
- レポートタイプを選択します。日報、週報、月報、年報を選択できます。
 お知らせ: 日次レポートは選択した日付のデータを計算し、週次レポートは選択した日付が属する週のデータを計算し、月次レポートは選択した日付が属する月の データを計算し、年次レポートは選択した日付が属する年のデータを計算します。
- 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。
- 開始時刻を選択し、「Counting」をクリックします。
 集計結果は、統計結果領域に表示されます。「Table」、「Bar」、「Bar Chart」、
 「Line Chart」をクリックして、結果をさまざまな方法で表示します。

*お知らせ:*統計を表示するテーブルを選択すると、エクセルファイルにデータを エクスポートするための「Export」ボタンが表示されます。



図14-2 人数カウント

14.3 ヒートマップ統計

ヒートマップ機能を有効にすると、アプリケーションタブからヒートマップデータを表示 してダウンロードできます。より視覚的な結果を導くために、さまざまなチャートでデ ータを表示することができます。 手順:

- レポートタイプを選択します。日報、週報、月報、年報を選択可能 *お知らせ*: 日次レポートは選択した日付のデータを計算し、週次レポートは選択 した日付が属する週のデータを計算し、月次レポートは選択した日付が属する 月のデータを計算し、年次レポートは選択した日付が属する年のデータを計算し ます。
- 2. 開始時刻を選択し、「Counting」をクリックしてヒートマップデータを一覧表示します。
- 3. 「Space Heat Map」 または「Time Heat Map」を選択して結果を表示します。

タイムヒートマップを選択して統計を一覧表示すると、エクセルファイルにデータをエ クスポートするための「Export」ボタンが表示されます。



図14-3 時間ヒートマップ

お知らせ:

取り付け完了後は電子レンズの調整を行わないことを推奨します。データの精 度不良を引き起こす可能性があります。

14.4 カウント統計

カウント機能を有効にすると、アプリケーションタブからカウントデータを表示および ダウンロードできます。より視覚的な結果を導くために、さまざまなチャートでデータ を表示することができます。

手順:

- レポートタイプを選択します。日報、週報、月報、年報を選択可能です。 *お知らせ*: 日次レポートは選択した日付のデータを計算し、週次レポートは選択 した日付が属する週のデータを計算し、月次レポートは選択した日付が属する 月のデータを計算し、年次レポートは選択した日付が属する年のデータを計算し ます。
- 2. 統計の種類を選択します。進入者、退出者の選択が可能です。
- 3. 開始時刻を選択し、「Counting」をクリックしてヒートマップデータを一覧表示します。
- 4. 結果を表示するには、表、棒グラフ、または折れ線グラフを選択します。

表を選択して統計をリストすると、エクセルファイルにデータをエクスポートするため の「Export」ボタンが表示されます。

14.5 キュー管理統計

目的:

キュー管理は、複数のディメンションからのデータ解析およびレポート出力をサポートします。

よく使うデータ解析

キュー/リージョン内の特定の待ち時間レベルの人数をキューイングアップする
 には、キューイングアップ時間分析を使用して、ターゲットリージョンを確認し、
 待ち時間レベルを設定します。

- 複数のキュー/リージョンで、特定の待ち時間レベルのキューイングアップ人数を比較するには、キューイングアップ時間分析を使用し、対象領域を確認して、待ち時間レベルを設定します。
- 複数のキュー/リージョン内の異なる待ち時間レベルのキューイングアップ人数を比較するには、キューイングアップ時間分析を使用し、ターゲットリージョンをチェックして、待ち時間レベルを設定します。
- キュー/リージョン内でキューが一定の長さを保持している時間と期間を確認 するには、キューステータス分析を使用してターゲットリージョンを確認し、キ ューの長さレベルを設定します。
- キューが複数のキュー/リージョンで一定の長さを保持している時間と期間を
 比較するには、キューステータス分析を使用し、対象領域を確認してキュー
 の長さレベルを設定します。
- キューが複数のキュー/リージョンで異なる長さに留まっている時間と継続時間を比較するには、キューステータス分析を使用して、ターゲットリージョンを確認し、キューの長さレベルを設定します。

14.5.1 キューイングアップ時間解析

目的:

キューイングアップ時間解析は、さまざまな待機時間レベルの人数を計算します。 地域比較と複数の待ち時間レベルの比較が可能です。

手順:

1. 「Statistic Type」を選択します。

「Regional Comparison」: 異なる地域のキューイングアップ人数を比較します。

a) 1つまたは複数のリージョンをチェックします。

b) 待機時間レベルを設定します。希望の時間範囲ラジオボタンと入力値を確認します。

たとえば、10分を超えて待機する人数を表示する場合は、3番目のラジオ ボタンをオンにして、対応するテキストボックスに600を入力します。

「Multi-Level Comparison」: 待ち行列を作る人数を、待ち時間レベルの違い によって比較します。

- a) 1つまたは複数のリージョンをチェックします。
 - a-1 待機時間レベルを設定します。1つまたは複数の希望する時間範囲の チェックボックスと入力値をチェックします。
 - a-2 例えば、待機時間が10分を超え、待機時間が3分未満の人数を比較 する場合は、最初と3番目のラジオボタンを確認し、対応するテキスト ボックスに600と180を入力します。
- 2. 「Report Type」を選択します。日報、週報、月報、カスタムに対応しています。
- 3. 「Statistics Time」を選択します。
- 4. 「Counting」をクリックしてレポートを生成します。
- 5. 右上隅にある「Export」をクリックして、目的の形式(.txt または xls.が選択可能) でデータをエクスポートします。

14.5.2 キューステータス解析

目的:

キューステータス分析は、キューが特定の長さを維持する時間と期間を計算します。 地域比較と複数のキューの長さレベル比較がサポートされています。

手順:

 「Statistic Type」を選択します。
 「Regional Comparison」:キューが異なる地域の特定の長さに留まる時間と期間 を比較します。

- a) 1つ以上の領域をチェックします。
- b) キューの長さレベルを設定します。

ここでのキュー長とは、リージョン内の人数を意味します。

たとえば、キューが1つのリージョンに10人を超える人数を保持している時間を確認するには、3番目のラジオボタンをオンにして、対応するテキストボックスに10を入力します。

「Multi-Level Comparison」:異なるキューの長さレベルでキューの時間と継続時間を比較します。

- a) 1 つまたは複数のリージョンをチェックします。
- b) キューの長さレベルを設定します。1つまたは複数の希望する範囲のチェックボックスと入力値をチェックします。
- 2. 「Report Type」を選択します。日報、週報、月報、カスタムに対応しています。
- 3. 「Statistics Time」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。

14.6 オープンプラットフォーム

目的:

オープンプラットフォームでは、サードパーティの機能開発用のアプリケーションをインストールすることができます。

お知らせ:

- 特定のモデルのみが機能をサポートしており、実際の表示はお使いのカメラモ デルによって異なる場合があります。
- オープンプラットフォーム機能を使用する場合、IPアドレスとカメラIPアドレスを 192.168.252.Xに設定することは推奨されません。

手順:

 「Configuration」>「Open Platform」を選択し、「Record Schedule Settings」画 面を表示します。

Disclaimer
Please note that some applications and/or solutions available below are supplied and/or developed by third parties, not HiKVISION.
YOUR RELIANCE ON THIRD PARTY'S APPLICATION AND/OR SOLUTIONS IS AT YOUR OWN RISK. HIKVISION MAKES NO WARRANTIES OR REPRESENTATIONS, EXPRESS OR IMPLIED, AS TO MERCHANTABILITY OR FITNESS FORANY PARTICULAR PURPOSE, ACCURACY, RELIABILITY, SECURITY, OR NONINFRINGEMENT THIRD PARTY'S APPLICATIONS AND/OR SOLUTIONS, YOU SHALL BE SOLELY RESPONSIBLE FOR TRANSACTION BETWEEN YOU AND SUCH THIRD PARTY.
I have read and agree with the disclaimer.
Install Apps

図14-4 免責事項

- 2. 免責事項を読み、チェックボックスをオンにします。
- 3. 「Install Apps」をクリックします。

4. 「Browse」をクリックして、インポートしたアプリケーションパッケージを選択します。



- 5. 「Import」をクリックすると、アプリケーションがインストールされます。
- インストールされているアプリケーションとその関連情報(バージョン、使用メモリ、フラッシュメモリ、会社、ステータス、ライセンスなど)がリストに表示されます。

「操作(Operation)」リストで書をクリックしてログをエクスポートし、ひをクリックし権限を設定します。 立をクリックしてアプリケーションを削除し、 をクリックしてアプリケーションを有効または無効にします。

お知らせ:

☆ をクリックすると、「Get Video Stream」と「Camera Setting Authorization」の2つ のチェックボックスがあります。

- 他社製アプリケーションでビデオストリームを取得する必要がある場合は、
 「Get Video Stream」チェックボックスをオンにして機能を有効にします。
- サードパーティ製のアプリケーションでカメラパラメータを取得または設定する 必要がある場合は、「Camera Setting Authorization」チェックボックスをオンに し、機能を有効にします。

アプリケーションをインストールしている場合は、目的のアプリケーションを選択してライセンスを表示するか、「Browse」をクリックして各アプリケーションのライセンスをインポートできます。ライセンスステータスには、無料、無効、有効、有効期限切れの4つがあります。無料とは、アプリケーションが無償で使用されており、ライセンスキーをインポートする必要がないことを意味します。無効とは、アプリケーションを使用する前にライセンスキーをインポートする必要があることを意味します。

License Manag	ement				
Inactive					
License				Browse	Import
Status					
Note: To get the I	icense key, visit <u>https://parti</u>	ner.hikvision.com/tpj	<u>p</u> and input licen	se code.	
Application Sn	apshot				
н	EOP BASIC DE	EMO APP			

図14-6 インポートライセンス

お知らせ:

アプリケーションパッケージをインポートする前に、以下の要件が満たされていることを確認してください。

- インポートしたアプリケーションに同じ名前を付けることはできません。
- インポートしたアプリケーションのフラッシュメモリサイズは、デバイスの空きフラ ッシュメモリより小さくしてください。
- インポートするアプリケーションのメモリサイズは、デバイスの空きメモリより小 さくする必要があります。

付録

付録1 SADP ソフトウェアの概要

● SADPの説明

SADP (Search Active Devices Protocol)は、ユーザーフレンドリーでインストー ルのないオンラインデバイス検索ツールです。サブネット内のアクティブなオン ラインデバイスを検索し、デバイスの情報を表示します。このソフトウェアを使用 して、デバイスの基本的なネットワーク情報を変更することもできます。

● アクティブなデバイスをオンラインで検索

♦ オンラインデバイスの自動検索

SADP ソフトウェアを起動すると、コンピュータが検出したサブネットから15秒 ごとにオンラインデバイスが自動的に検索されます。オンラインデバイス画 面で検索されたデバイスの総数と情報が表示されます。デバイスの種類、IP アドレス、ポート番号などのデバイス情報が表示されます。

٩	SADP								◎ _ □ ×
To	al numb	er of online devices: 10					1	Export Refresh	Activate the Device
	I ID	• Device Type	Security	IPv4 Address	Port	Software Version IPv4 Gateway	HTTP P	ort Device Serial No.	
	001	XX-XXXXXXXX-X	Active	10.16.6.21	8000	Vica.xbuild 2000000 10.16.6.254	80	X000000000-X000000-X00	
	002	XX-XXXXXXXX-X	Active	10.16.6.20	8000	Vx.x.xbuild x0000x 10.16.6.254	80	30K-300000K-30000000K	4
	003	30X-3000000001-X	Active	10.16.6.171	8000	Vicaciduild iononor 10.16.6.254	80	301-30000001-300000000	
	004	30X-300000002-3	Active	10.16.6.22	8000	Vicacibuild icoccor 10.16.6.254	N/A	301-3000000-300000000	The device is not activated
	005	XX-XXXXXXXXXXXX	Active	10.16.6.127	8000	Vx.x.xbuild x0000x 10.16.6.254	N/A	20000000000-2000000-200	The device is not activated.
	006	XX-XXXXXXXX-X	Active	10.16.6.179	8000	Valaxibuild sosses 10.16.6.254	N/A	201-2000001-2000000-201	
D	007	XX-XXXXXXXX-X	Active	10.16.6.250	8000	Valazbuild access 10.16.6.254	80	301-3000001-300000000000000000000000000	
	008		Inactive	192,168,1.64	8000	Vaxabuild xxxxxx 192,168.1.1	80		You can marify the actuary exception after
	009	XX-XXXXXXX-X	Active	10.16.6.111	8000	Va.a.abuild x00000x 10.16.6.254	80	306-3000006-3000000000	the device activation.
	010	XX-XXXXXXXX-X	Active	10.16.6.177	8000	Valacebuild account 10.16.6.254	80	307-3000007-300000000000	Activata Now
									New Password:
									Confirm Password:
									Activate

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。

▲ 各列の見出しで または をクリックして、情報を並び替える ことができます。

をクリックしてデバイステーブルを展開し、右側のネットワークパラメータ パネルを非表示にするか、 をクリックしてネットワークパラメータパネルを 表示します。

● ネットワークパラメータの変更

手順:

- 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。

Modify Network	Parameters
III Enable DHCP	
Device Serial No.:	30X-300000X-300000000000000000000000000
IP Address:	10.16.5.106
Port:	8003
Subnet Mask:	255.255.255.0
Gateway:	0.0.0.0
IPv6 Address:	
IPv6 Gateway:	
IPv6 Prefix Length:	
HTTP Ports	0
S	ecurity Verification
Admin Password:	******
	Modify
	Forgot Password

図A.1.2 ネットワークパラメータの変更

付録2 ポートマッピング

TP-LINKルータ(TL-WR641G)の設定は以下のとおりです。設定は、ルーターのモ デルによって異なります。

手順:

1. 次のように、「WAN Connection Type」を選択します:

108M Wireless Router Model No.: TL-WR641G / TL-WR642G	WAN		
 Status Quick Setup Basic Settings Network LAN WAN MAC Clone 	WAN Connection Type: User Name: Password:	PPPoE Dynamic IP Static IP PPPoE 802.1X + Dynamic IP 802.1X + Static IP BigPond Cable L2TP	

図A.2.1 WAN 接続タイプの選択

 IPアドレスやサブネットマスクの設定など、ルーターのLANパラメータを次の図の ように設定します。

108M Wireless Router Model No.: TL-WR641G / TL-WR642G	LAN	
Status Original Seture	MAC Address:	00-14-78-6A-DB-0C
Guick Setup Basic Settings Network	Subnet Mask:	192.168.10.1 255.255.255.0
• LAN • WAN • MAC Clone		Save

図A.2.2 LAN パラメータの設定

「Forwarding」の仮想サーバーでポートマッピングを設定します。デフォルトでは、カメラはポート80、8000、554を使用します。これらのポートフォリオ価値は、ウェブブラウザまたはクライアントソフトウェアで変更できます。

例:

カメラが同じルーターに接続されている場合、IP アドレス192.168.1.23 でカメラの ポートを80、8000、554、8200 に、別のカメラのポートをIP 192.168.1.24 で81、8001、 555、8201 に設定できます。以下の手順を参照してください:

手順:

- 1. 上述の設定として、ネットワークカメラのポート80、8000、554、8200を 192.168.1.23でマップします
- 2 ネットワークカメラのポート81、8001、555、8201 を192.168.1.24 にマップします。
- 3.「ALL」または「TCP」プロトコルを有効にします。
- 4. 「Enable」チェックボックスをオンにし、「Save」をクリックし、設定を保存します。

108M Wireless Router Model No.: TL-WR641G / TL-WR642G	Virtu	al Servers			
Status	ID	Service Port	IP Address	Protocol	Enable
Quick Setup	1	80	192.168.10 . 23	ALL 🔽	~
Basic Settings + Network	2	8000	192.168.10 . 23	ALL 🔽	~
+ Wireless	3	554	192.168.10. 23	ALL 🗸	V
+ DHCP	4	8200	192.168.10. 23	ALL 🗸	~
 Forwarding Virtual Servers 	5	81	192.168.10. ₂₄	ALL 🗸	
Port Triggering	6	8001	192.168.10. 24	ALL 🗸	~
• DMZ • UPnP	7	555	192.168.10. 24	ALL 💙	~
+ Security	8	8201	192.168.10. 24	ALL 🗸	~
Static Routing Dynamic DNS Maintenance System Tools	Commo	on Service Port:	DNS(53)	Copy to ID 1	*
		(Previous Next	Clear All	ave

図A.2.3 ポートマッピング

お知らせ: ネットワークカメラのポートは、他のポートと競合できません。たとえば、 ルーターのWeb 管理ポートの一部は80 です。管理ポートと同じ場合は、カメラポ ートを変更します。

アイリスオーヤマ株式会社

■ 新規購入・導入をご検討のお客様へ

当社営業もしくは下記窓口までご相談ください。

IoTソリューション事業部 TEL 03-5843-7747 (受付時間)平日9:00~17:00

■ 製品の設置・施工・アフターサービスについてのお問い合わせ

サポートコール 0800-111-5300 (通話料無料)

〈受付時間〉平日9:00~17:00、土・日・祝日9:00~12:00/13:00~17:00 (年末年始・夏期休業期間・会社都合による休日を除く)