

SHARP

取扱説明書（操作・設定編） 2MP ボックス（マイク内蔵） ネットワークカメラ



専用レンズ：YK-H021AL（別売）を装着した写真です。

形名 YK-H021A （専用レンズ：YK-H021AL）

本書は、YK-H021A の取扱説明書です。

本書をよくお読みのうえ、正しくお使いください。

ご使用前に、『取扱説明書 基本編』の「安全にお使いいただくために」を必ずお読みください。

必要に応じて、説明書を印刷してお使いください。

はじめに

製品概要

本製品は、マイクを内蔵した、約 200 万画素の屋内専用ボックス型ネットワークカメラです。

レンズ（専用レンズ：YK-H021AL）は別売になっています。

取扱説明書について

本製品の取扱説明書は以下のような構成になっています。

- 取扱説明書 基本編：安全上のご注意、使用上、設置上のお願い事項について記載されています。
- 取扱説明書 操作・設定編（本書）：本製品を動かすソフトウェアの操作や設定方法について記載されています。

商標について

- Microsoft、Windows、Internet Explorer は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
- その他、この説明書に記載されている会社名・商品名は、各会社の商標または登録商標です。

著作権について

- 本製品に搭載のソフトウェアは著作物であり、著作権、著作者人格権などをはじめとする著作者等の権利が含まれており、これらの権利は著作権法により保護されています。ソフトウェアの全部または一部を複製、修正、あるいは改変したり、ハードウェアから分離したり、逆アセンブル、逆コンパイル、リバースエンジニアリング等を行わないでください。第三者にこのような行為をさせることも同様です。
- OSS（Open Source Software）ライセンスについて
本製品には、GNU General Public License（GPL）、GNU Lesser General Public License（LGPL）、その他ライセンスに基づくソフトウェアが含まれています。

当該ソフトウェアのライセンスに関する詳細は、商品内の[環境設定] → [システム] → [バージョン情報] → [ライセンスを表示する] にて表示される内容をご参照ください。

個人情報保護について

- 本製品を使用したシステムで撮影された個人を識別できる情報は、「個人情報の保護に関する法律」で定められた「個人情報」に該当します。法律に従って、映像情報を適切にお取扱いください。
- 本製品を使用して記録された情報内容は、「個人情報」に該当する場合があります。本製品、または記録媒体が廃棄、譲渡、修理などで第三者に渡る場合には、その取り扱いを十分に注意してください。

ネットワークのセキュリティについて

ネットワークのセキュリティ対策に関しては、お客様ご自身の責任で十分に行ってください。

セキュリティ対策を行わなかった結果、または、通信仕様上のやむを得ない事情によりデータ漏えいなどネットワークのセキュリティ上の問題が発生した場合、それによって生じたあらゆる損害に対し、弊社は一切の責任を負いかねます。

(対策例)

- ファイアウォールなどで安全性の確保されたネットワーク上で本製品を使用する。
- ユーザー名とパスワードを設定し、ログインできるユーザーを制限する。パスワードは定期的に変更する。
- パソコンが接続されているシステム上で本製品を使用する際は、コンピューターウイルスや不正プログラムの感染に対するチェックや駆除が定期的に行われていることを確認する。

プライバシー・肖像権について

本製品の設置およびご利用につきましては、お客様の責任で被写体のプライバシーの保護や肖像権などに十分配慮してください。被写体となった個人または団体などによるプライバシー侵害などを理由とするいかなる賠償請求やクレームなどに関し、弊社は一切の責任を負いません。

その他

- 本製品は、特定のエリアを対象に監視を行うための映像を得ることを目的に作られたものです。本製品単独で犯罪などを防止するものではありません。
- 本製品や記録メディアの故障もしくは不具合などにより録画ができなかった場合、これにより生じるお客様の損害について、弊社は一切の責任を負いかねます。
- 本製品の故障や不具合を含む何らかの理由または原因により、映像が表示できないことによるお客様の損害、被害について、弊社は一切の責任を負いかねます。
- 記録メディアや外部ストレージなどに記録されたデータの消失および付随的損害（営業損失などの補償）などについて、弊社は一切の責任を負いかねます。
- 本製品を使用したことによるお客様、または第三者からのいかなる請求についても、弊社は一切の責任を負いかねます。

もくじ

第 1 章 システム要件.....	8
第 2 章 ネットワーク接続	9
2.1 LAN 経由のネットワークカメラの設定	9
2.1.1 LAN 経由のケーブル接続.....	9
2.1.2 カメラのアクティベート	10
2.2 WAN 経由のネットワークカメラの設定.....	11
2.2.1 静的 IP アドレスでの接続	12
2.2.2 動的 IP 接続	13
第 3 章 ネットワークカメラへのアクセス	15
3.1 Web ブラウザによるアクセス	15
第 4 章 ライブビュー.....	17
4.1 ライブビューページ	17
4.2 ライブビューの開始	18
4.3 手動の録画および画像のキャプチャ.....	19
第 5 章 ネットワークカメラ設定	20
5.1 ローカルパラメータの設定	20
5.2 システム設定	22
5.2.1 基本情報の設定	22
5.2.2 時間設定	23
5.2.3 RS-232 設定	25
5.2.4 RS-485 設定	25
5.2.5 サマータイム設定	26
5.3 メンテナンス	26
5.3.1 アップグレードとメンテナンス	26
5.3.2 ログ	28
5.4 セキュリティ設定	29
5.4.1 認証	29
5.4.2 IP アドレスフィルタ	30
5.4.3 セキュリティサービス	32
5.5 ユーザー管理	33
5.5.1 ユーザー管理	33
5.5.2 オンラインユーザー	36
第 6 章 ネットワーク設定	37
6.1 基本設定	37
6.1.1 TCP/IP の設定	37

6.1.2	DDNS 設定	39
6.1.3	PPPoE 設定	39
6.1.4	ポート設定	40
6.1.5	NAT(ネットワークアドレス変換) の設定	42
6.2	詳細設定	43
6.2.1	SNMP 設定	43
6.2.2	FTP 設定	46
6.2.3	E メール設定	48
6.2.4	HTTPS 設定	50
6.2.5	QoS 設定	52
6.2.6	802.1X 設定	53
6.2.7	統合プロトコル 設定	55
6.2.8	ネットワークサービス 設定	55
第 7 章	ビデオと音声設定	56
7.1	ビデオ設定	56
7.2	音声設定	60
7.3	ROI エンコーディング設定	61
7.4	複数ストリーム情報表示	63
第 8 章	画像設定	64
8.1	ディスプレイ設定	64
8.1.1	デイ/ナイト自動切替	64
8.1.2	デイ/ナイトスケジュール切替	67
8.2	OSD 設定	69
8.3	プライバシーマスクの設定	70
第 9 章	イベント設定	72
9.1	基本イベント	72
9.1.1	動体検知設定	72
9.1.2	タンパリングアラーム	79
9.1.3	アラーム入力の設定	80
9.1.4	アラーム出力の設定	81
9.1.5	異常への対応処理	82
9.2	スマートイベント	83
9.2.1	オーディオ異常検出の設定	83
9.2.2	焦点ぼけ検出の設定	84
9.2.3	シーン変更検出の設定	85
9.2.4	顔検出の設定	86
9.2.5	エリア侵入検出の設定	87
9.2.6	線のクロス検出の設定	89
9.2.7	領域進入検知	91

9.2.8	領域退出検知	92
9.2.9	放置手荷物検知の設定	93
9.2.10	物体撤去検知の設定	95
第 10 章	ストレージ設定	97
10.1	録画スケジュール設定	97
10.2	キャプチャスケジュール設定	100
10.3	NetHDD の設定	102
10.4	メモリーカード検出の設定	105
第 11 章	再生	108

第1章 システム要件

オペレーティングシステム: Microsoft Windows 7 SP1 またはそれ以上

CPU: 2.0 GHz またはそれ以上

RAM: 1GB またはそれ以上

ディスプレイ: 解像度 1024×768 またはそれ以上

Web ブラウザ: Internet Explorer 11 以降のバージョン

第2章 ネットワーク接続

注意:

- インターネットアクセスを通じて製品を使用した場合、ネットワークのセキュリティリスクがあることを承諾すると見なされます。ネットワーク攻撃や情報漏えいを回避するには、ご自身の保護対策を強化してください。
- 製品が正しく動作しない場合、販売店またはお問い合わせ窓口に連絡してください。

始める前に:

- LAN(ローカルエリアネットワーク) 経由でネットワークカメラを設定したい場合、2.1 節 LAN 経由のネットワークカメラの設定を参照してください。
- WAN(ワイドエリアネットワーク) 経由でネットワークカメラを設定したい場合、2.2 節 WAN 経由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 経由のネットワークカメラの設定

LAN 経由でカメラを閲覧、設定するためには、ネットワークカメラをお使いのコンピューターと同じサブネットに接続してください。

2.1.1 LAN 経由のケーブル接続

以下の図に、ネットワークカメラとコンピューターをケーブルで接続する2つの方法を示します。

- ネットワークカメラをテストする場合、図 2-1 に示すように、ネットワークカメラをコンピューターにネットワークケーブルで直接接続できます。
注意:カメラを動作させるためには PoE 電源が必要です。
- ネットワークカメラをスイッチまたはルーターを経由して LAN 接続する場合、図 2-2 を参照してください。

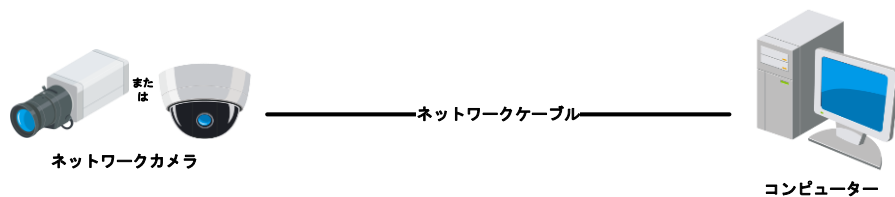


図 2-1 直接接続

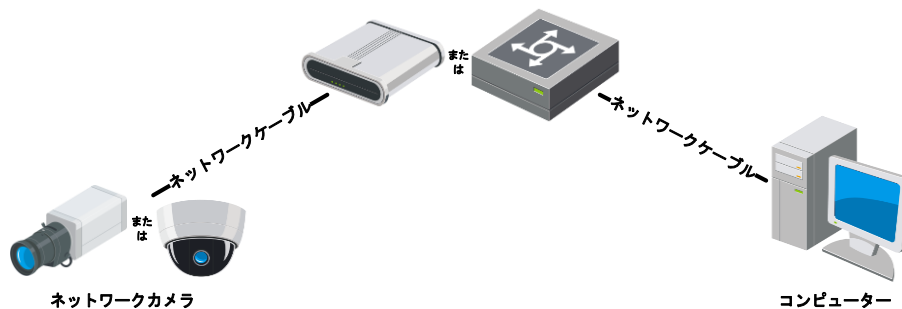


図 2-2 スイッチまたはルーター経由の接続

2.1.2 カメラのアクティベート

カメラを使い始める前に、まず強力なパスワードを設定してカメラをアクティベートする必要があります。

Web ブラウザ経由のアクティベートについて説明します。

❖ Web ブラウザ経由のアクティベート

方法:

1. カメラの電源をオンにし、カメラをネットワークに接続します。
2. Web ブラウザのアドレスバーに IP アドレスを入力し、エンターキーを押してアクティベーションインターフェイスに入ります。

注意:

- カメラのデフォルト IP アドレスは 192.168.1.64 です。



図 2-3 Web ブラウザ経由のアクティベート

3. 新しくパスワードを作り、パスワードフィールドに入力します。



強力なパスワードを推奨-製品のセキュリティを高めるため、ご自分で選択した強力なパスワード (大文字、小文字、数字、特殊記号のうち、少なくとも3つのカテゴリで構成された文字を8文字以上含むパスワード) を設定するよう強くお勧めします。また、定期的にパスワードを再設定し、特に高いセキュリティシステムでは、毎月または毎週パスワードを再設定すると、より安全に製品を保護できます。

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、ライブビューインターフェイスに入ります。

2.2 WAN 経由のネットワークカメラの設定

目的:

この節では静的 IP または動的 IP を用いて、どのようにネットワークカメラを WAN に接続するかを解説します。

2.2.1 静的 IP アドレスでの接続

始める前に:

ISP(インターネットサービス事業者)から静的 IP を取得します。静的 IP アドレスを用いる場合、ネットワークカメラをルーター経由でまたは直接 WAN に接続することができます。

● ルーター経由でのネットワークカメラの接続

方法:

1. ネットワークカメラをルーターに接続してください。
2. 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については 2.1.2 節を参照してください。
3. 静的 IP アドレスをルーターに保存します。
4. 80、8000 および 554 番等、ポートマッピングを設定します。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。ポートマッピングに関するサポートはルーターの製造業者に問い合わせてください。
5. Web ブラウザを利用してインターネット経由でネットワークカメラにアクセスします。



図 2-4 静的 IP を持つルーターを経由したカメラへのアクセス

● 静的 IP アドレスでのネットワークカメラの接続

カメラに静的 IP アドレスを保存し、ルーターを使わずにインターネットに直接接続することもできます。



図 2-5 静的 IP を持つカメラによる直接アクセス

2.2.2 動的 IP 接続

始める前に:

ISP から動的 IP を取得してください。動的 IP アドレスを用いる場合、ネットワークカメラをルーターに接続することができます。

● ルーター経由でのネットワークカメラの接続

方法:

1. ネットワークカメラをルーターに接続してください。
2. カメラ内で 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。
3. ルーター上で、PPPoE ユーザー名、パスワードを設定し、パスワードを確認します。
4. ポートマッピングを設定します。たとえば 80、8000 および 554 番ポートです。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。ポートマッピングに関するサポートはルーターの製造業者に問い合わせてください。
5. ドメインネームプロバイダーからドメインネームを取得します。
6. ルーターの設定インターフェイス上で、DDNS の設定を行います。
7. 取得したドメインネームでカメラにアクセスします。

注意: 取得した IP アドレスは PPPoE 経由で動的にアサインされるものであり、カメラをリブートするたびに変わります。動的 IP による制約を解消するには、DDNS 事業者からドメインネームを取得する必要があります。問題を解決するための通常のドメインネームの解決および、プライベートドメインネームの解決については下記の手順にしたがってください。

◆ 通常のドメイン名の解決

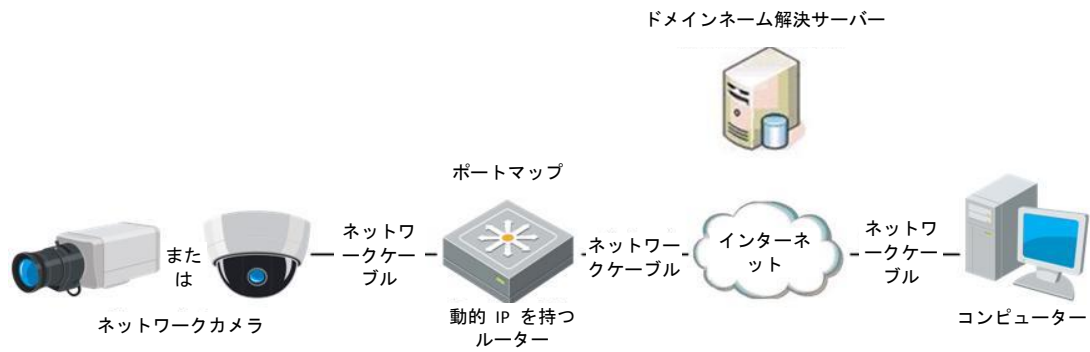


図 2-6 通常のドメイン名の解決

方法:

1. ドメイン名プロバイダーからドメイン名を取得します。
2. ネットワークカメラの **DDNS 設定** インターフェイス上で、DDNS の設定を行います。設定の詳細については 6.1.2 節 **DDNS 設定** を参照してください。
3. 取得したドメイン名でカメラにアクセスします。

第3章 ネットワークカメラへのアクセス

3.1 Web ブラウザによるアクセス

方法:

1. Web ブラウザを開きます。
2. ブラウザのアドレスバーにネットワークカメラの IP アドレスを入力し、
[エンター] キーを押してログインインターフェイスに入ります。
3. 初回利用時には 2.1.2 節の詳細を参照し、ネットワークカメラをアクティベートしてください。

注意:

- デフォルト IP アドレスは 192.168.1.64 です。
 - カメラがアクティベートされていない場合、2.1.2 節にしたがって、
まずカメラをアクティベートしてください。
4. ユーザー名とパスワードを入力して [ログイン] をクリックしてください。

管理ユーザーはデバイスのアカウントおよびユーザー/オペレータの権限を適切に設定する必要があります。必要のないアカウントおよびユーザー/オペレータ権限は削除してください。

注意:

管理ユーザーがパスワード入力に 7 回失敗すると IP アドレスはロックされます(ユーザー/オペレータの場合、5 回)。



図 3-1 ログインインターフェイス

5. ライブビデオの閲覧やカメラの操作の前にプラグインをインストールしてください。インストールの指示に従い、プラグインをインストールします。

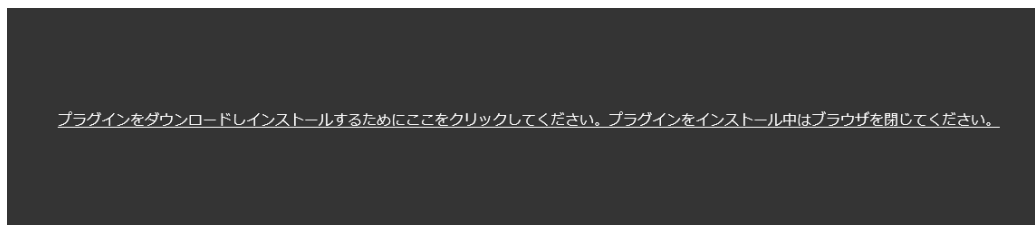


図 3-2 プラグインのダウンロードとインストール

注意: プラグインをインストールするには Web ブラウザを閉じなければならない場合があります。プラグインをインストールした後、Web ブラウザを再度開いて再ログインしてください。

第4章 ライブビュー

4.1 ライブビューページ

目的:

ライブビューページでは、リアルタイムのビデオを表示したり、画像をキャプチャしたり、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に入るか、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に入ります。

ライブビューページの説明:



図 4-1 ライブビューページ

メニューバー:

各タブをクリックすると、それぞれライブビュー、再生、画像および環境設定ページに進みます。

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、ストリーム種別、およびプラグインを調整することができます。また、ライブビューページの操作、たとえばライブビューの開始/停止、キャプチャ、録画、デジタルズームの開始/停止などを行うことができます。

PTZ コントロールパネル:

本製品は手動ズーム、手動フォーカスであり、電動でないため使用しません。



プリセット/パトロール設定:

本製品では使いません。











4.2 ライブビューの開始

図 4-2 に示すライブビューウィンドウで、ツールバー上の ▶ をクリックして、カメラのライブビューを開始します。





図 4-2 ライブビューツールバー

表 4-1 ツールバーの説明

アイコン	説明
	自動調整ウィンドウサイズです。
	メインストリームのライブビューです。
	サブストリームのライブビューです。
	本製品では使用しません。
	双方向音声通話を開始/終了します。 ※AudioOut 端子にスピーカをつなぐことで 双方向通話が可能です。
	ライブビューを開始/停止します。
	画像を手動でキャプチャします。
	録画を手動で開始/停止します。
	デジタルズーム機能を開始/停止します。
	音声をオンにし、ボリュームの調整/ミュートを行います。

4.3 手動の録画および画像のキャプチャ

ライブビューインターフェイスのツールバーにある  をクリックしてライブ画像をキャプチャしたり、 をクリックしてライブビューを録画することができます。キャプチャー画像および動画クリップを保存するパスは、[環境設定]>[ローカル] ページで設定できます。

注意: キャプチャした画像は JPEG または BMP ファイルとしてお使いのコンピュータに保存されます。

第5章 ネットワークカメラ設定

5.1 ローカルパラメータの設定

目的:

ローカル設定とは、ライブビュー、録画ファイルおよびキャプチャ画像のパラメータのことです。録画ファイルとキャプチャ画像は、Web ブラウザを利用して録画するファイルやキャプチャであり、保存するパスはブラウザを実行している PC 上のパスとなります。

方法:

1. ローカル設定インターフェイスに入ります:[環境設定]>[ローカル]。

The screenshot shows the 'Local Settings' interface with the following configurations:

- ライブ画像のパラメーター**
 - プロトコル: TCP, UDP, MULTICAST, HTTP
 - 再生性能: 最短遅延, 均衡, 滑らかさ, カスタマイズ
 - ルール: 有効, 無効
 - POS情報を表示: 有効, 無効
 - 画像フォーマット: JPEG, BMP
- 記録ファイルの設定**
 - 記録ファイルサイズ: 256M, 512M, 1G
 - 保存先: C:\Users\sharp\Web\RecordFiles (ブラウザ) (開く)
 - ダウンロードファイルの...: C:\Users\sharp\Web\DownloadFile (ブラウザ) (開く)
- 画像とクリップの設定**
 - スナップショットを保存: C:\Users\sharp\Web\CaptureFiles (ブラウザ) (開く)
 - スナップショットを保存: C:\Users\sharp\Web\PlaybackPic (ブラウザ) (開く)
 - クリップの保存: C:\Users\sharp\Web\PlaybackFile (ブラウザ) (開く)

A red '保存' (Save) button is located at the bottom left of the interface.

図 5-1 ローカル設定インターフェイス

2. 以下の設定項目を設定します:

- **ライブ画像のパラメータ:**プロトコルタイプおよびライブビューのパフォーマンスを設定します。
- ◆ **プロトコル:**TCP、UDP、MULTICAST および HTTP が選択できます。
TCP: ストリーミングデータの完全な伝送とよりよいビデオ品質を保証しますが、伝送のリアルタイム性が影響を受けます。

UDP: リアルタイムの音声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下でのストリーミング用に特定のポートを設定することなく、TCP と同じ品質を実現します。

MULTICAST: マルチキャスト機能を利用する場合、MCAST タイプを選択してください。マルチキャストについての詳細は、6.1.1 節 **TCP/IP の設定** を参照してください。

- ◆ **再生性能:** 再生性能を最短遅延、均衡または滑らかさに設定します。
- ◆ **ルール:** ローカルブラウザ上で適用されるルールのこと、動体の検知、顔の検出または侵入検知がトリガーされた際の色付きのマークの表示・非表示を有効化ないし無効化します。例えば、ルールが有効化され、かつ、顔の検出が有効化されている場合、顔が検出されるとライブビュー上に緑色の四角形でマーキングされます。
- ◆ **POS 情報を表示:** 本機能は未サポートです。
- ◆ **画像フォーマット:** キャプチャ画像の画像フォーマットを選択します。
- **記録ファイル設定:** 録画したビデオファイルの保存先パスを設定します。Web ブラウザで録画した動画ファイルに関して有効になります。
 - ◆ **記録ファイルサイズ:** 手動録画およびダウンロードされたビデオファイルのパッケージサイズを 256M、512M または 1GB から選択します。選択後、録画されたファイルの最大サイズは選択した値になります。
 - ◆ **保存先:** 手動録画したビデオファイルの保存先パスを設定します。
 - ◆ **ダウンロードファイルの保存:** 再生モード中にダウンロードしたビデオファイルの保存先パスを設定します。
- **画像とクリップの設定:** キャプチャした画像および切り取ったビデオファイルの保存先パスを設定します。Web ブラウザでキャプチャした画像ファイルに関して有効になります。
 - ◆ **上のスナップショットを保存:** ライブビューモード中に手動でキャプチャした画像の保存先パスを設定します。

- ◆ 下のスナップショットを保存: 再生モード中に手動でキャプチャした画像の保存先パスを設定します。
- ◆ クリップの保存: 再生モード中にクリップしたビデオファイルの保存先パスを設定します。

注意: [ブラウザ] をクリックして、クリップと画像を保存するためフォルダを変更し、[開く] をクリックしてクリップおよび画像の保存の設定フォルダを開くことができます。

3. [保存] をクリックして設定を保存します。

5.2 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、ユーザー管理などを含むシステムの設定を行うには、以下の手順に従ってください。

5.2.1 基本情報の設定

デバイス情報インターフェイスに入ります: [環境設定] > [システム] > [システム設定] > [基本的な情報] です。

基本的な情報インターフェイスでは、デバイス名とデバイス番号を編集することができます。

モデル、バージョン No.、ファームウェアバージョン、エンコードバージョン、チャンネルの数、HDD の数、アラーム入力の数、アラーム出力の数などの、ネットワークカメラの他の情報も表示されます。これらの情報はこのメニューでは変更できません。メンテナンスまたは将来の変更のための参考情報です。

基本的な情報	時間設定	サマータイム	RS-232	RS-485	バージョン情報
デバイス名	IP CAMERA				
デバイスNo.	88				
モデル	YK-H021A				
バージョンNo.	XXXXXXXXXX				
ファームウェアバージョン	V5.5.82 build 190312				
エンコードバージョン	V7.3 build 180912				
ウェブバージョン	V4.0.51 build 190130				
プラグインバージョン	V3.0.6.46				
チャンネルの数量	1				
HDDの数量	0				
アラーム入力数	1				
アラーム出力数	1				
ファームウェアバージョ...	B-R-E3-0				


 保存

図 5-2 基本的な情報

5.2.2 時間設定

目的:

時刻同期およびサマータイムの設定を行うには、この節の指示にしたがってください。

方法:

1. 時刻設定インターフェイスに入ります。**[環境設定]** > **[システム]** > **[システム設定]** > **[時間設定]** です。

図 5-3 時刻設定

2. あなたの地域のタイムゾーンをドロップダウンメニューから選択します。
3. NTP 設定を行います。
 - (1) クリックして **NTP** 機能を有効化します。
 - (2) 以下の設定項目を設定します:
 - サーバアドレス:** NTP サーバーの IP アドレス。
 - NTP ポート:** NTP サーバーのポート。
 - インターバル:** NTP サーバーとの同期実行の間の時間間隔です。
 - (3) (オプション) [テスト] ボタンをクリックすると NTP サーバーを利用した時刻同期機能をテストすることができます。

図 5-4 NTP サーバーによる時刻同期

注意: 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には、時刻同期

機能を提供している NTP サーバーを使用する必要があります。カメラがカスタマイズされたネットワークで設定されている場合、NTP ソフトウェアを利用して、時刻同期用の NTP サーバーを立ち上げることができます。


- 手動時刻同期を設定します。
 - (1) **[手動時間同期]** をチェックします。手動時刻同期機能を有効にする項目です。
 - (2)  アイコンをクリックして、日付、時刻をポップアップカレンダーから選択します。
 - (3) (オプション) **[コンピューターの時間と同期します。]** 項目をチェックするとデバイスの時刻をローカル PC の時刻と同期します。



図 5-4 手動時間同期

- **[保存]** をクリックして設定を保存します。

5.2.3 RS-232 設定

一般ユーザーは使用しません。

5.2.4 RS-485 設定

一般ユーザーは使用しません。

5.2.5 サマータイム設定

目的:

サマータイムは、夏の期間に時刻を 1 時間進めることで、自然の日光をよりよく利用するための一手段であり、秋には再度元に戻されます。

実際の必要に応じて サマータイム を設定してください。

方法:

1. サマータイム 設定インターフェイスに入ります:

[環境設定] > [システム] > [システム設定] > [サマータイム]

基本的な情報	時間設定	サマータイム	RS-232	RS-485	バージョン情報
<input type="checkbox"/> サマータイム有効					
開始時間	4月	はじめ	日	02	
終了時間	10月	最終	日	02	
DSTバイアス	30分				
<input type="button" value="保存"/>					

図 5-5 サマータイム設定

2. 開始時間と終了時間を選択します。
3. DST バイアスを選択します。
4. [保存] をクリックして設定を有効化します。

5.3 メンテナンス

5.3.1 アップグレードとメンテナンス

目的:

アップグレードとメンテナンスインターフェイスでは、再起動、部分的復元、デフォルトの復元、設定ファイルのエクスポート/インポートおよびデバイスのアップグレードを含む運用操作を行うことができます。

メンテナンスインターフェイスを開きます:[環境設定]>[システム]>[メンテナンス]>[アップグレードとメンテナンス]。

- **再起動:** デバイスを再起動します。
- **復元:** 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。
- **デフォルト:** すべての設定を工場出荷時のデフォルトに復元します。

注意: デフォルト設定を復元した後は、IP アドレスはデフォルトの IP アドレスに復元されます。このアクションを実行するには十分に注意してください。

- **設定ファイルのエクスポート/インポート:** 設定ファイルは、カメラのバッチ設定に利用されます。設定しなければいけないカメラが多数ある場合に、設定手順を簡素化することができます。

方法:

1. **[デバイスのパラメータ]** をクリックし、現在の設定ファイルをエクスポートして、特定の場所に保存します。
2. **[ブラウザ]** をクリックして、保存された設定ファイルを選択し、**[インポート]** をクリックして設定ファイルのインポートを開始します。

注意: 設定ファイルをインポートした後にカメラを再起動する必要があります。

- **診断情報:** ログ、システム情報、ハードウェア情報をダウンロードします。
- **アップグレード:** デバイスを特定のバージョンにアップグレードします。

方法:

1. ファームウェアを選択するか、またはファームウェアディレクトリを選択し、アップグレードファイルを指定します。
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指定します。
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置かれたフォルダだけを指定してください。
2. **[ブラウザ]** をクリックして、ローカルのアップグレードファイルを選択し、**[アップグレード]** をクリックして遠隔アップグレードを開始します。

注意: アップグレードには 1~10 分かかります。実行中に、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。

5.3.2 ログ

目的:

操作、アラーム、異常、およびカメラの情報はログファイルに保存することができます。必要な場合、ログファイルをエクスポートすることもできます。

始める前に:

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

方法:

1. ログ検索インターフェイスに入ります:[環境設定] > [システム] > [メンテナンス] > [ログ]。

アップグレードとメンテナンス ログ								
メインリスト	すべてのタイプ	サブリスト	すべてのタイプ	開始時間	2019-04-19 00:00:00	終了時間	2019-04-19 23:59:59	検索
ログリスト							エクスポート	
No.	時間	メインリスト	サブリスト	チャンネ...	ユーザー	リモート	ホス...	

図 5-6 ログ検索インターフェイス

2. メインリスト、サブリスト、開始時間、終了時間を含む検索を指定して、ログ検索条件を設定します。
3. [検索] 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インターフェイスに表示されます。

アップグレードとメンテナンス **ログ**

メインリスト サブリスト

開始時間 終了時間

ログリスト							<input type="button" value="エクスポート"/>
No.	時間	メインリスト	サブリスト	チャネル...	ユーザー	リモート ホス...	
1	2018-08-31 14:05:24	操作	リモート：動作状態の取得		admin	192.168.1.10	↑
2	2018-08-31 14:05:18	操作	リモート：動作状態の取得		admin	192.168.1.10	
3	2018-08-31 14:05:17	操作	リモート：動作状態の取得		admin	192.168.1.10	
4	2018-08-31 13:38:10	操作	リモート：パラメータの...		admin	192.168.1.10	
5	2018-08-31 13:38:10	操作	リモート：パラメータの...		admin	192.168.1.10	
6	2018-08-31 13:38:10	操作	リモート：パラメータの...		admin	192.168.1.10	
7	2018-08-31 13:38:10	操作	リモート：パラメータの...		admin	192.168.1.10	
8	2018-08-31 13:38:10	操作	リモート：パラメータの...		admin	192.168.1.10	
9	2018-08-31 13:38:10	操作	リモート：パラメータの...		admin	192.168.1.10	
10	2018-08-31 13:38:10	操作	リモート：パラメータの...		admin	192.168.1.10	
11	2018-08-31 13:38:10	操作	リモート：パラメータの...		admin	192.168.1.10	
12	2018-08-31 13:38:10	操作	リモート：パラメータの...		admin	192.168.1.10	↓

トータル 39 アイテム << < 1/1 > >>

図 5-7 ログ検索中

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

5.4 セキュリティ設定

認証、IP アドレスフィルタおよびセキュリティサービスを含むパラメータをセキュリティインターフェイスから設定します。

5.4.1 認証

目的:

ライブビューのストリームデータを個別に保護することができます。

方法:

1. 認証インターフェイスに入ります: [環境設定] > [システム] > [セキュリティ] > [認証方式]。

認証方式	IPアドレスフィルタ	セキュリティサービス
RTSP認証		digest
ウェブ認証		digest
<input type="button" value="保存"/>		

図 5-8 認証方式

2. ドロップダウンリストから **認証**の種別として **digest** または **digest/basic** を選択します。
3. **[保存]** をクリックして設定を保存します。

5.4.2 IP アドレスフィルタ

目的:

この機能は、アクセス制御を可能にします。

方法:

1. IP アドレスフィルタインターフェイスに入ります:[環境設定] > [システム] > [セキュリティ] > [IP アドレスフィルタ]

IPアドレスフィルタ		追加	変更	削除
<input type="checkbox"/>	No.	IP		

図 5-9 IP アドレスフィルタインターフェイス

2. [IP アドレスフィルタを有効にする] のチェックボックスをチェックします。
3. ドロップダウンリストから IP アドレスフィルタの種別を選択します。禁断と許可されたが選択できます。
4. IP アドレスフィルタリストを設定します。
 - IP アドレスの追加

方法:

- (1) IP アドレスを追加するには、[追加]をクリックします。
- (2) IP アドレスを入力します。

IPアドレスの追加

IPアドレス 192.168.1.65 ✓

OK キャンセル

図 5-10 IP の追加

- (3) [OK] をクリックし、追加を終了します。

- IP アドレスの変更

方法:

- (1) フィルタリストから IP アドレスを左クリックし、[変更] をクリックします。
- (2) テキストフィールド上で IP アドレスを変更します。



図 5-11 IP の変更

(3) [OK] をクリックし、変更を終了します。

- 1 つまたはそれ以上の IP アドレスを削除します。
IP アドレスを選択し、[削除] をクリックします。

5. [保存] をクリックして設定を保存します。

5.4.3 セキュリティサービス

カメラにはセキュリティサービスが備わっており、データ通信のセキュリティを向上させることができます。

方法:

1. セキュリティサービス設定インターフェイスに入ります:[環境設定]>[システム]>[セキュリティ]>[セキュリティサービス]。

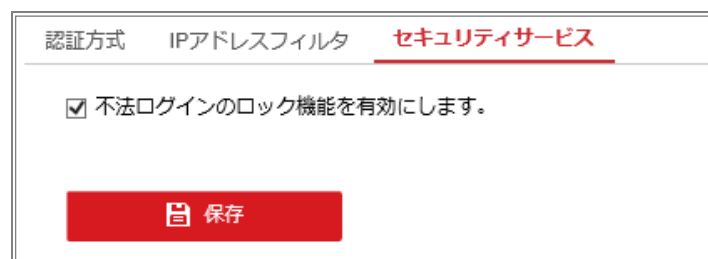


図 5-12 セキュリティサービス

2. [不正ログインのロック機能を有効にします。] チェックボックスをチェックすると、管理ユーザーがユーザー名/パスワード認証に 7 回(オペレータ/ユーザーでは 5 回)失敗した場合、IP アドレスはロックされます。

注意: IP アドレスがロックされた場合は、デバイスは 30 分後にログインを試みることができます。

5.5 ユーザー管理

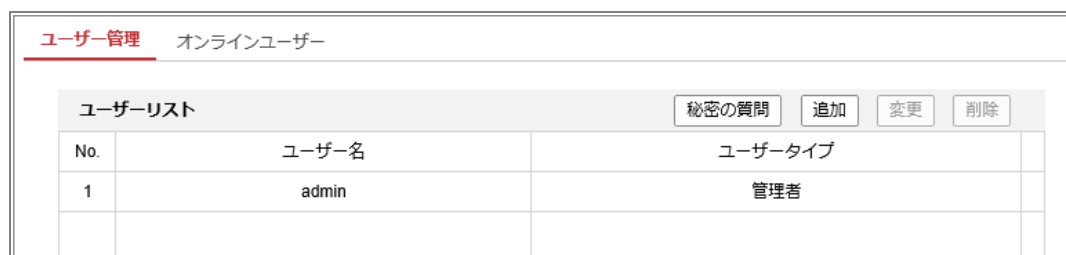
5.5.1 ユーザー管理

目的:

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、異なる権限を付与することができます。ユーザーアカウントとアクセス権は適切に管理することを強くお勧めします。

方法:

1. ユーザー管理インターフェイスに入ります:[環境設定]>[システム]>[ユーザー管理]



The screenshot shows a web interface for user management. At the top, there is a breadcrumb trail: "ユーザー管理" (User Management) and "オンラインユーザー" (Online Users). Below this, there is a section titled "ユーザーリスト" (User List). To the right of this section are four buttons: "秘密の質問" (Secret Question), "追加" (Add), "変更" (Change), and "削除" (Delete). Below the buttons is a table with the following data:

No.	ユーザー名	ユーザータイプ
1	admin	管理者

図 5-13 ユーザー管理インターフェイス

● ユーザーの追加

管理ユーザーは、デフォルトですべての権限を有しており、他のアカウントを作成/変更/削除することができます。

管理ユーザーを削除することはできません。管理パスワードの変更のみが可能です。

方法:

1. [追加] をクリックしてユーザーを追加します。
2. ユーザー名を入力し、レベルを選択してパスワードを入力します。

注意:

- ユーザーアカウントは 31 まで作成できます。
- レベルの異なるユーザーはそれぞれ異なるデフォルトのアクセス権を持っています。オペレータとユーザーが選択できます。



強力なパスワードを推奨-製品のセキュリティを高めるため、ご自分で選択した強力なパスワード (大文字、小文字、数字、特殊記号のうち、少なくとも3つのカテゴリで構成された文字を8文字以上含むパスワード) を設定するよう強くお勧めします。また、定期的にパスワードを再設定し、特に高いセキュリティシステムでは、毎月または毎週パスワードを再設定すると、より安全に製品を保護できます。

3. 新しいユーザーのアクセス権のチェックをオンまたはオフにすることができます。
4. [OK] をクリックし、ユーザー追加を終了します。

図 5-14 ユーザーの追加

● ユーザーの変更

方法:

1. リスト時から左クリックでユーザーを選択し、[変更] をクリックします。
2. ユーザー名、レベルとパスワードを変更します。



強力なパスワードを推奨-製品のセキュリティを高めるため、ご自分で選択した強力なパスワード (大文字、小文字、数字、特殊記号のうち、少なくとも3つのカテゴリで構成された文字を8文字以上含むパスワード) を設定するよう強くお勧めします。また、定期的にパスワードを再設定し、特に高いセキュリティシステムでは、毎月または毎週パスワードを再設定すると、より安全に製品を保護できます。

3. アクセス権のチェックボックスをオンまたはオフにすることができます。
4. [OK] をクリックし、ユーザーの変更を終了します。

ユーザーの修正

ユーザー名: Test

ユーザータイプ: オペレーター

管理者パスワード: []

パスワード: []

確認: []

有効なパスワード範囲は8-16しか、数字で、小文字、大文字、特殊な文字の2種類以上の組み合わせは必要です。

確認

すべてを選択

- リモート: パラメーターの設定
- リモート: ログ検索/動作状態の調査
- リモート: アップグレード/フォーマ...
- リモート: 双方向音声通信
- リモート: シャットダウン/リブート
- リモート: 監視センターに通知/トリ...
- リモートビデオ出力コントロール
- リモートシリアルポートコントロール
- リモートライブ表示
- リモート: 手動記録
- リモートPTZコントロール
- リモート再生

OK キャンセル

図 5-15 ユーザーの変更

- ユーザーの削除

方法:

1. 削除したいユーザーをクリックして選択し、[削除] をクリックします。
2. ポップアップするダイアログボックス上で [OK] をクリックして、削除を確認します。

5.5.2 オンラインユーザー

目的:

このインターフェイスを通じて、現在デバイスにアクセスしているユーザーを確認することができます。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、ユーザーリストに表示されます。

[更新] をクリックして、リストを更新します。



ユーザー管理		オンラインユーザー			
ユーザーリスト					更新
No.	ユーザー名	ユーザータイプ	IPアドレス	ユーザー操作時間	
1	admin	管理者	192.168.1.10	2018-08-31 14:12:21	

図 5-16 オンラインユーザーの表示

第6章 ネットワーク設定

目的:

基本設定および詳細設定を設定するには、この章の手順にしたがってください。

6.1 基本設定

目的:

TCP/IP、DDNS、PPPoE、ポートおよび NAT などを含むパラメータは、この節の手順にしたがって設定することができます。

6.1.1 TCP/IP の設定

目的:

ネットワーク経由でカメラを操作する前に、TCP/IP の設定を適切に行っておく必要があります。カメラは IPv4 と IPv6 の両方をサポートしています。両方のバージョンを合することなく同時に設定可能です。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。

方法:

1. TCP/IP 設定インターフェイスに入ります:[環境設定] > [ネットワーク] > [基本設定] > [TCP/IP]

TCP/IP		DDNS	PPPoE	ポート	NAT
NICタイプ	自動				
	<input type="checkbox"/> DHCP				
IPv4 アドレス	192.168.1.64			テスト	
IPv4サブネットマスク	255.255.255.0				
IPv4デフォルトゲートウ...	192.168.1.1				
IPv6モード	ルートの通知			経路広告を見る	
IPv6 アドレス					
IPv6のサブネットマスク					
IPv6 デフォルトゲートウ...	::				
MACアドレス	94:e1:ac:c9:be:46				
MTU	1500				
マルチキャストアドレス					
	<input checked="" type="checkbox"/> マルチキャスト発見有効				
DNSサーバー					
優先DNSサーバ	8.8.8.8				
代替DNSサーバ					
保存					

図 6-1 TCP/IP 設定

- NIC タイプ、IPv4 または IPv6 アドレス、IPv4 または IPv6 のサブネットマスク、IPv4 または IPv6 の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値を設定します。
- (オプション) [マルチキャスト発見有効] のチェックボックスをチェックすると、LAN 内のプライベートマルチキャストプロトコル経由でクライアントソフトウェアがオンラインのネットワークカメラを自動的に検出できます。
- DNS サーバーを設定します。優先 DNS サーバーおよび代替 DNS サーバーを入力します。
- [保存] をクリックし、上記の設定を保存します。

注意:

- MTU の適正な値の範囲は 1280～1500 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、複数のクライアントがマルチキャストグループアドレスを使用してコピーを要求することで、同時にストリームを取得することを可能にします。この機能を使用する前に、お使いの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。
- 設定を有効にするために再起動する必要があります。

6.1.2 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に 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)を使用することができます。

始める前に:

カメラの DDNS の設定を適用する前に DDNS サーバーへの登録が必要になります。

方法:

1. DDNS 設定インターフェイスに入ります:[環境設定]>[ネットワーク]>[基本設定]>[DDNS]。
2. [DDNS有効] チェックボックスをチェックしてこの機能を有効にします。
3. DDNS タイプを選択します。

6.1.3 PPPoE 設定

方法:

1. PPPoE 設定インターフェイスに入ります:[環境設定]>[ネットワーク]>[基本設定]>[PPPoE]

図 6-2 PPPoE 設定

2. **[PPPoE 有効]** チェックボックスをチェックしてこの機能を有効にします。
3. **ユーザー名、パスワード**を入力して、 PPPoE アクセス用のパスワードを **確認**します。

注意: ユーザー名とパスワードはご利用の ISP によって割り当てられる必要があります。



- 個人情報とお使いのシステムのセキュリティを保持する観点から、すべての機能およびネットワークデバイスに対して強力なパスワードを使用することを強く推奨します。製品のセキュリティを高めるため、ご自分で選択した強力なパスワード (大文字、小文字、数字、特殊記号のうち、少なくとも3つのカテゴリで構成された文字を8文字以上含むパスワード) を設定するようお勧めします。
- すべてのパスワードやその他のセキュリティの適切な設定は、設置者および/またはエンドユーザーの責任です。

4. **[保存]** をクリックしてインターフェイスを閉じます。

注意: 設定を有効にするために再起動する必要があります。

6.1.4 ポート設定

目的:

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

方法:

1. [環境設定]>[ネットワーク]>[基本設定]>[ポート] から、ポート設定インターフェイスに入ります。

TCP/IP	DDNS	PPPoE	ポート	NAT
HTTPポート <input type="text" value="80"/>				
RTSPポート <input type="text" value="554"/>				
HTTPS 端子 <input type="text" value="443"/>				
サーバポート <input type="text" value="8000"/>				
Enhanced SDK Service P... <input type="text" value="8443"/>				
保存				

図 6-3 ポート設定

2. カメラの HTTP ポート、RTSP ポート、HTTPS ポートおよびカメラのサーバーポートを設定します。

HTTP ポート: デフォルトのポート番号は 80 で、占有されていないポート番号であれば何にでも変更できます。

RTSP ポート: デフォルトのポート番号は 554 で、占有されていないポート番号で、1 から 65535 の範囲で変更できます。

HTTPS 端子: デフォルトのポート番号は 443 で、占有されていないポート番号であれば何にでも変更できます。

サーバーポート: デフォルトのポート番号は 8000 で、2000 から 65535 の範囲の、どのポート番号にでも変更できます。

Enhanced SDK Service ポート: 一般ユーザーは使用不可の為、使用しません。

3. [保存] をクリックして設定を保存します。

注意: 設定を有効にするために再起動する必要があります。

6.1.5 NAT(ネットワークアドレス変換) の設定

目的:

NAT インターフェイスでは、UPnP™ パラメータを設定することができます。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 プロトコルは、デバイスをシームレスに接続し、ホームおよび企業環境でのネットワークの実装を簡略化することができます。この機能を有効にすると、各ポートのポートマッピングを設定する必要なく、カメラがルーターを経由で WAN(ワイドエリアネットワーク) に接続されます。

方法:

1. NAT 設定インターフェイスに入ります:[環境設定]>[ネットワーク]>[基本設定]>[NAT]
2. [UPnP™を有効にする] チェックボックスをチェックします。
3. カメラのニックネームを選択するか、デフォルトの名前を使用することができます。
4. ポートマッピングモードを選択します。手動と自動が選択できます。手動ポートマッピングの場合、外部ポートの値をカスタマイズすることができます。
5. [保存] をクリックして設定を保存します。

TCP/IP DDNS PPPoE ポート **NAT**

UPnP™を有効にする
 フレンドリ名

ポートマッピングモード

ポートタイプ	外部ポート	外部IPアドレス	内部ポート	ステータス
HTTP	80	0.0.0.0	80	有効ではない
HTTPS	443	0.0.0.0	443	有効ではない
RTSP	554	0.0.0.0	554	有効ではない
サーバポート	8000	0.0.0.0	8000	有効ではない
Enhanced SDK...	8443	0.0.0.0	8443	有効ではない

図 6-4 UPnP 設定

6.2 詳細設定

目的:

SNMP、FTP、Eメール、HTTPS、QoS、802.1x などを含むパラメータは、この節の手順にしたがって設定することができます。

6.2.1 SNMP 設定

目的:

SNMP 機能を設定することで、カメラのステータス、パラメータ、アラームに関連する情報を取得し、ネットワークに接続されているカメラをリモートで管理を行うことができます。

始める前に:

SNMP の設定の前に、SNMP ソフトウェアをダウンロードし、SNMP ポートを経由してカメラ情報を受信してください。トラップアドレスを設定することで、アラームイベントおよび異常についてのメッセージを監視センターに送信することができます。

注意: SNMP バージョンは SNMP ソフトウェアのバージョンと同じにする必要があります。必要なセキュリティのレベルに応じて、異なるバージョンを使用する必要があります。SNMP v1 はセキュリティを提供しません。SNMP v2 ではアクセスするためのパスワードが必要です。また SNMP v3 は暗号化を提供します。バージョン 3 を使用する場合は、HTTPS プロトコルを有効にする必要があります。



- 個人情報とお使いのシステムのセキュリティを保持する観点から、すべての機能およびネットワークデバイスに対して強力なパスワードを使用することを強く推奨します。製品のセキュリティを高めるため、ご自分で選択した強力なパスワード (大文字、小文字、数字、特殊記号のうち、少なくとも 3 つのカテゴリで構成された文字を 8 文字以上含むパスワード) を設定するようお勧めします。
- すべてのパスワードやその他のセキュリティの適切な設定は、設置者および/またはエンドユーザーの責任です。

方法:

1. SNMP 設定インターフェイスに入ります:[環境設定]>[ネットワーク]>[詳細設定]>[SNMP]

The screenshot shows the SNMP configuration page with the following sections and fields:

- SNMP v1/v2**
 - SNMPv1 有効
 - SNMP v2 c 有効
 - SNMPコミュニティをお...: public
 - SNMPコミュニティを記...: private
 - トラップアドレス: []
 - トラップポート: 162
 - Trap コミュニティ: public
- SNMP v3**
 - SNMPv3 有効
 - ユーザー名の読み込み: []
 - セキュリティレベル: no auth, no priv
 - 認証アルゴリズム: MD5 (selected), SHA
 - 認証パスワード: []
 - プライベートキー: DES (selected), AES
 - プライベートキーパスワ...: []
 - ユーザー名の書き込み: []
 - セキュリティレベル: no auth, no priv
 - 認証アルゴリズム: MD5 (selected), SHA
 - 認証パスワード: []
 - プライベートキー: DES (selected), AES
 - プライベートキーパスワ...: []
- SNMPその他設定**
 - SNMPポート: 161

At the bottom, there is a red button labeled "保存" (Save).

図 6-5 SNMP 設定

2. [SNMP v1有効]、[SNMP v2c有効]、 [SNMP v3有効] のチェックボックスをチェックし、対応する機能を有効にしてください。

3. SNMP の設定

注意: SNMP ソフトウェアの設定は、ここでの設定と同じにする必要があります。

4. [保存] をクリックし、設定を保存して終了します。

注意:

- 設定を有効にするために再起動する必要があります。
- 情報漏洩のリスクを下げるためには、SNMP v1 または v2 の代わりに v3 を有効にすることが推奨されます。

6.2.2 FTP 設定

目的:

キャプチャした画像を FTP サーバーにアップロードを有効にするために FTP サーバーに関連する情報を設定することができます。画像のキャプチャはイベントまたは時間指定のスナップショットタスクによってトリガーされます。

方法:

1. FTP 設定インターフェイスに入ります:[環境設定]>[ネットワーク]>[詳細設定]>[FTP]。

SNMP	FTP	Email	HTTPS	QoS	802.1x	統合プロトコル
サーバアドレス	0.0.0.0					
ポート	21					
ユーザー名						<input type="checkbox"/> 匿名
パスワード						
確認						
ディレクトリ構造	ルートディレクトリに保存し					
画像保存間隔	オフ					日 (秒)
画像の名前	デフォルト					
	<input type="checkbox"/> 画像アップロード					
	テスト					
保存						

図 6-6 FTP 設定

2. FTP のサーバアドレスとポートを入力します。
3. FTP の設定; FTP サーバーへログインするためのユーザー名とパスワードが必要です。



- 個人情報とお使いのシステムのセキュリティを保持する観点から、すべての機能およびネットワークデバイスに対して強力なパスワードを使用することを強く推奨します。製品のセキュリティを高めるため、ご自分で選択した強力なパスワード (大文字、小文字、数字、特殊記号のうち、少なくとも3つのカテゴリで構成された文字を8文字以上含むパスワード) を設定するようお勧めします。
- すべてのパスワードやその他のセキュリティの適切な設定は、設置者および/またはエンドユーザーの責任です。

4. ディレクトリ構造と画像保存の間隔を設定します。

ディレクトリ: [ディレクトリ構造] のフィールドで、ルートディレクトリ、親ディレクトリおよび子ディレクトリを選択できます。親ディレクトリが選択されている場合は、デバイス名、デバイス番号またはデバイスの IP アドレスをディレクトリの名前に利用することができます。子ディレクトリが選択されている場合は、カメラ名またはカメラ番号をディレクトリの名前に使用することができます。

画像保存間隔: 画像をよりよく管理するために、画像保存間隔を 1 日から 30 日の範囲で設定できます。同じ時間間隔でキャプチャした画像はすべて、その時間間隔の開始日と終了日から生成された名前のフォルダに保存されます。

画像の名前: キャプチャした画像ファイルの命名ルールを設定します。ドロップダウンリストでデフォルトのルールを選択すると以下のデフォルトルールを使用できます。

IP アドレス_チャンネル番号_キャプチャ時刻_イベント種別.jpg

(例: 10.11.37.189_01_20150917094425492_FACE_DETECTION.jpg)。

または**カスタムプレフィックス**をデフォルト命名ルールに追加してカスタマイズすることもできます。

5. [画像アップロード] チェックボックスをチェックして機能を有効化します。
画像アップロード: FTP サーバーへのキャプチャ画像のアップロードを有効化します。
FTP サーバーへの匿名アクセス(この場合ユーザー名とパスワードは要求されません): FTP サーバーへの匿名アクセスを有効にするには [匿名] のチェックボックスをチェックします。
注意: 匿名アクセスの機能は、FTP サーバー側でサポートされている必要があります。
6. [保存] をクリックして設定を保存します。

6.2.3 E メール設定

目的:

動体検知イベント、ビデオロス、ビデオ干渉などのアラームイベントが検知された場合に指定されたすべての受信者に E メール通知を送信するようにシステムを設定できます。

始める前に:

電子メール機能を使用する前に、[環境設定]>[ネットワーク]>[基本設定]>[TCP/IP] の下の DNS サーバー設定を行ってください。

方法:

1. TCP/IP 設定 ([環境設定]>[ネットワーク]>[基本設定]>[TCP/IP]) に入り、IPv4 アドレス、IPv4 サブネットマスク、IPv4 デフォルトゲートウェイおよび優先 DNS サーバーを設定してください。
注意: 詳細な設定については 6.1.1 節 **TCP/IP の設定** を参照してください。
2. E メール設定インターフェイスに入ります:[環境設定]>[ネットワーク]>[詳細設定]>[Email]
3. 以下の設定項目を設定します:
差出人: Eメールの送信者の名前です。
差出人アドレス: 送信者の Eメールアドレスです。
SMTP サーバ: SMTP サーバーの IP アドレスまたはホスト名(例:

smtp.263xmail.com) です。

SMTP ポート: SMTP ポートです。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)。また、SSL SMTP ポートは 465 です。

メールの暗号化: なし、SSL および TLS が選択できます。SSL または TLS を選択し、STARTTLS を無効にした場合、E メールは SSL または TLS で暗号化されて送信されます。この暗号化方式では SMTP のポートを 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 を有効にした場合、E メールは STARTTLS で暗号化されて送信され、SMTP ポートは 25 に設定する必要があります。

注意: STARTTLS を使用する場合には、E メールサーバーがプロトコルをサポートしていることを確認してください。[STARTTLS の有効化] チェックボックスをチェックしても、E メールサーバーがプロトコルをサポートしていない場合、E メールは暗号化されません。

添付画像: アラームの画像を E メールに添付して送信したい場合、[画像の添付] チェックボックスをチェックしてください。

間隔: 間隔は、添付画像送信のアクション 2 回の間時間を示します。

認証 (オプション): お使いのメールサーバーが認証を必要とする場合、このチェックボックスをチェックして、サーバーへのログイン認証を利用するようにし、メールアカウントのログインユーザー名とパスワードを入力します。



- 個人情報とお使いのシステムのセキュリティを保持する観点から、すべての機能およびネットワークデバイスに対して強力なパスワードを使用することを強く推奨します。製品のセキュリティを高めるため、ご自分で選択した強力なパスワード (大文字、小文字、数字、特殊記号のうち、少なくとも 3 つのカテゴリで構成された文字を 8 文字以上含むパスワード) を設定するようお勧めします。
- すべてのパスワードやその他のセキュリティの適切な設定は、設置者および/またはエンドユーザーの責任です。

宛先テーブル: E メールが送信される宛先の受信者を選択します。最大 3 人の受信者を設定できます。

宛先: 通知を受けるユーザーの名前です。

宛先アドレス: 通知を受けるユーザーの E メールアドレスです。

宛先			
No.	宛先	宛先アドレス	テスト
1			テスト
2			
3			

図 6-7 E メール設定

4. [保存] をクリックして設定を保存します。

6.2.4 HTTPS 設定

目的:

HTTPS は Web サイトとそれに関連付けられている web サーバに対する認証により、中間者攻撃に対する防護を提供します。次の手順を実行して https のポート番号を設定します。

たとえば、ポート番号として 443、IP アドレスとして 192.168.1.64 を設定する場合、Web ブラウザを通じて `https://192.168.1.64:443` と入力することでデバイスにアクセスすることができます。

方法:

1. HTTPS 設定インターフェイスを開きます。[設定] > [ネットワーク] > [詳細設定] > [HTTPS]
2. [有効化] チェックボックスをチェックして機能を有効化します。

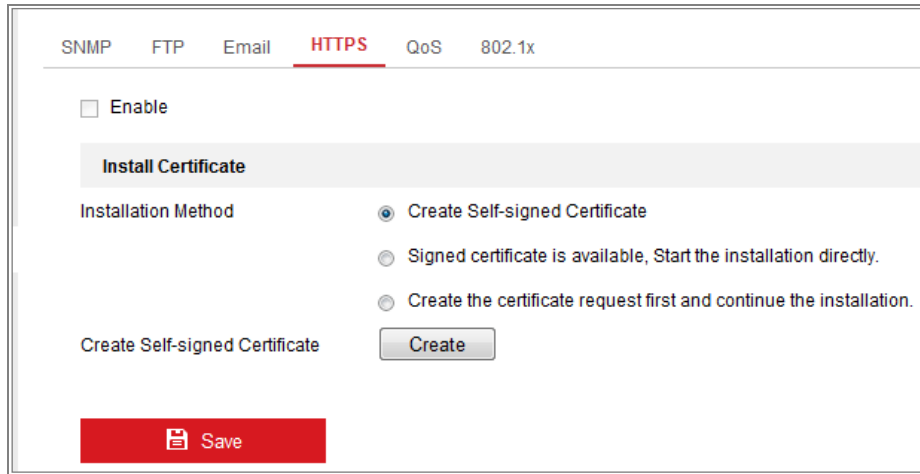


図 6-8 HTTPS 設定インターフェイス

3. 自己署名証明書または権限を付与された証明書を作成します。
 - 自己署名証明書の作成
 - (1) インストール方式として [自己署名証明書の作成] を選択します。
 - (2) [作成] ボタンをクリックして、作成インターフェイスに入ります。

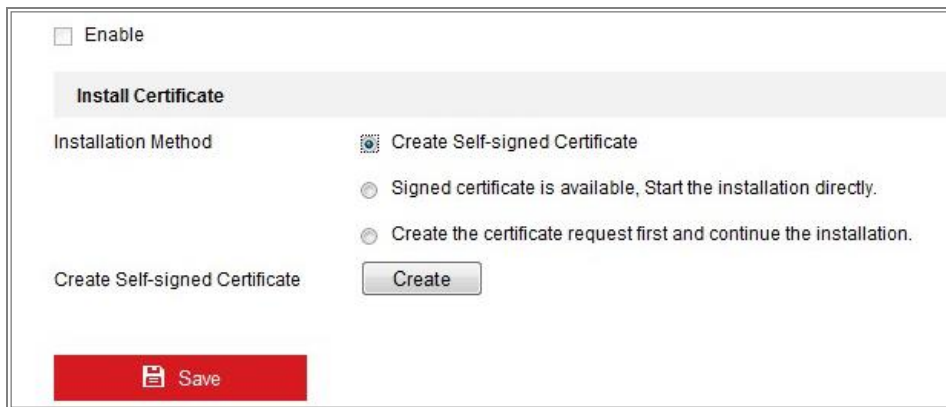


図 6-9 自己署名証明書の作成

- (3) 国、ホスト名/IP、有効期限、その他の情報を入力します。
- (4) [OK] をクリックして設定を保存します。

注意: すでに証明書がインストールされている場合は、[自己署名証明書の作成] はグレーアウトされます。

- 権限を持つ証明書の作成
 - (1) インストール方式として [証明書要求を作成してからインストールを

継続] を選択します。

- (2) **[作成]** ボタンをクリックして、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) 証明書要求をダウンロードして、信頼された認証局に送信して署名してもらいます。
- (4) 署名済みの有効な証明書を受信したら、デバイスに証明書をインポートします。

4. 正常に証明書の作成とインストールが完了すると、証明書情報ができます。

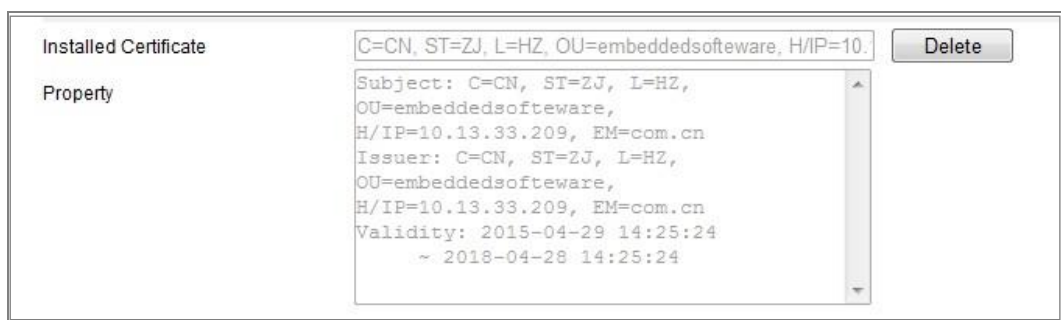


図 6-10 インストールされた証明書

5. **[保存]** ボタンをクリックし、設定を保存します。

6.2.5 QoS 設定

目的:

QoS (サービス品質) はデータ送信の優先順位を設定することによって、ネットワークの遅延やネットワークの輻輳を解決することに役に立ちます。

方法:

1. QoS 設定インターフェイスに入ります: **[環境設定]** > **[ネットワーク]** > **[詳細設定]** > **[QoS]**

SNMP	FTP	Email	HTTPS	QoS	802.1x	統合プロトコル
				ビデオ/音声DSCP	<input type="text" value="0"/>	
				イベント/アラームDSCP	<input type="text" value="0"/>	
				管理DSCP	<input type="text" value="0"/>	
<input type="button" value="保存"/>						

図 6-11 QoS 設定

2. ビデオ/音声 DSCP、イベント/アラーム DSCP および管理 DSCP を含む QoS の設定を行います。

DSCP の適正な値の範囲は 0～63 です。DSCP の値が大きいほど優先度は高くなります。

注意: DSCP は、Differentiated Service Code Point のことで、DSCP 値は、IP ヘッダ内でデータの優先度を指定するために使用します。

3. [保存] をクリックして設定を保存します。

注意: 設定を有効にするために再起動する必要があります。

6.2.6 802.1X 設定

目的:

ネットワークカメラは IEEE 802.1X 標準をサポートしており、機能が有効になっている場合、IEEE 802.1 X で保護されたネットワークへの接続においては、カメラデータの安全性が確保され、ユーザー認証が必要になります。

始める前に:

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



- 個人情報とお使いのシステムのセキュリティを保持する観点から、すべての機能およびネットワークデバイスに対して強力なパスワードを使用することを強く推奨します。製品のセキュリティを高めるため、ご自分で選択した強力なパスワード (大文字、小文字、数字、特殊記号のうち、少なくとも3つのカテゴリで構成された文字を8文字以上含むパスワード) を設定するようお勧めします。
- すべてのパスワードやその他のセキュリティの適切な設定は、設置者および/またはエンドユーザーの責任です。

方法:

1. [環境設定]>[ネットワーク]>[詳細設定]>[802.1x] から、802.1X 設定インターフェイスに入ります。

SNMP	FTP	Email	HTTPS	QoS	802.1x	統合プロトコル
<input checked="" type="checkbox"/> IEEE 802.1X 有効						
プロトコル		EAP-MD5				
EAPOLバージョン		1				
ユーザー名		<input type="text"/>				
パスワード		<input type="password"/>				
確認		<input type="password"/>				
<input type="button" value="保存"/>						

図 6-12 802.1X 設定

2. [IEEE 802.1X 有効] チェックボックスをチェックしてこの機能を有効にします。
3. プロトコル、EAPOL バージョン、ユーザー名、パスワードを含む 802.1X の設定を行い、確認します。
注意: EAPOL バージョンは、ルーターまたはスイッチと同一にする必要があります。
4. サーバーにアクセスするユーザー名とパスワードを入力します。
5. [保存] をクリックして設定を終了します。

注意: 設定を有効にするために再起動する必要があります。

6.2.7 統合プロトコル 設定

目的:

ONVIFプロトコルを通してカメラにアクセスする必要がある場合、ONVIFユーザーを設定することができます。

方法:

1. **[ONVIFを有効化]** チェックボックスをチェックしてこの機能を有効にします。
2. ONVIFユーザーを追加します。最大32ユーザーまで登録できます。
3. **[保存]** をクリックして設定を終了します。

注意: カメラを復元するとONVIFの設定はクリアされます。

6.2.8 ネットワークサービス 設定

一般ユーザーは本機能の設定を変更する必要はありません。

第7章 ビデオと音声設定

目的:

ビデオ設定、オーディオ設定、ROI およびストリーム上での情報表示を設定するには以下の手順にしたがってください。

7.1 ビデオ設定

方法:

1. [環境設定] > [ビデオとオーディオ] > [ビデオ] から、ビデオ設定インターフェイスに入ります。

項目	設定値
ストリームタイプ	メインストリーム (ノーマル)
ビデオタイプ	映像 & 音声
解像度	1920*1080P
ビットレートタイプ	定数
ビデオの品質	中
フレームレート	30 fps
最大ビットレート	8192 Kbps
ビデオエンコーディング	H.264
H.264+	オフ
プロフィール	ミディアム
Iフレーム間隔	50
SVC	オフ
平滑化	50 [クリア<<>平滑]

図 7-1 ビデオ設定

2. カメラのストリームタイプをメインストリーム (ノーマル)、サブストリームから選択します。

注意: メインストリームは通常、良好な帯域幅での録画とライブビューに用いられ、サブストリームは帯域幅が限られている場合のライブビュー表示に用いられます。

3. 選択したストリームタイプについて、次のパラメータをカスタマイズすることができます。

ビデオタイプ:

ビデオストリーム、映像&音声から選択します。

解像度:

ビデオ出力の解像度を選択します。

ビットレートタイプ:

固定または可変のビットレート種別を選択します。

注意: メインストリーム、サブストリームともにビットレートタイプを固定ビットレートを選択、かつ最大ビットレートを高い値に設定すると、両ストリームを同時再生する場合に動作が不安定になる場合があります。その場合は最大ビットレートを下げるか、ビットレートタイプを可変としてください。

ビデオの品質:

ビットレートタイプについて可変が選択されている場合、6段階のビデオ品質が選択できます。

フレームレート:

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る頻度のことで、フレーム/秒 (fps) で計測されます。高いフレームレートは映像品質を一貫して維持するので、ビデオストリーム中に動きがある場合には有利です。

注意: フレームレート以外の設定（最大ビットレート、H.265+/H.264+、動体検知などの検知イベント設定など）次第では、フレームレートが設定を下回る場合があります。

最大ビットレート:

最大ビットレートを 256 から 8192 Kbps まで設定します。高い値にすると、より高品質のビデオとなりますが、より良好な帯域幅が必要です。

ビデオエンコーディング:

ストリームタイプがメインストリームに設定されている場合、H.264 および H.265 が選択可能です。ストリームタイプがサブストリームに設定されている場合、H.264、MJPEG、H.265 が選択可能です。H.265 は、新しいエンコーディング技術です。H.264 と比較して、同じ画質状態を保ったまま、伝送ビットレートが小さくなります。

H.264+ および H.265+:

- **H.264+:** ストリームタイプとしてメインストリームを、そしてビデオエンコーディングに H.264 を設定した場合、H.264+ が使用可能として表示されます。H.264+ は、H.264 をベースに改善された圧縮符号化技術です。H.264+ を有効にすると、その最大平均ビットレートによる、HDD の消費量を見積もることができます。H.264 と比較して、H.264+ はほとんどのシーンで、同じ最大ビットレートで最高 50% のストレージを節約します。
- **H.265+:** ストリームタイプとしてメインストリームを、そしてビデオエンコーディングに H.265 を設定した場合、H.265+ が使用可能として表示されます。H.265+ は、H.265 をベースに改善された圧縮符号化技術です。H.265+ を有効にすると、その最大平均ビットレートによる、HDD の消費量を見積もることができます。H.265 と比較して、H.265+ はほとんどのシーンで、同じ最大ビットレートで最高 50% のストレージを節約します。

H.264+/H.265+ をオンまたはオフにしたい場合は、カメラを再起動する必要があります。H.264+ から H.265+ に直接に切り替えた場合、またはその逆の場合は、システムを再起動する必要はありません。

注意:

- H.264+ または H.265+ を使用したい場合、ビットレートタイプは可変にする必要があります。
- H.264+/H.265+ を有効にし、ビットレートタイプを可変にすると、プロ

ファイル、I フレーム間隔、ビデオの品質、および SVC はグレーアウトされます。

- H.264+/H.265+ を有効にすると、一部の機能がサポートされません。これらの機能については、対応するインターフェイスが非表示になります。
- 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、実際のシーンでの必要性にしたがってビットレート分布を自動的に調整します。カメラを固定された監視シーンに適応させるためには、少なくとも 3 日を必要とします。

最大平均ビットレート:

最大ビットレートを設定した場合、それに対応して推奨される最大平均ビットレートは[最大平均ビットレート] ボックスに表示されます。最大平均ビットレートは 32 Kbps から設定された最大ビットレートまでの範囲で設定できます。

プロフィール:

低、ミディアム、高が選択可能です。

I フレーム間隔:

I フレーム間隔を 1 から 400 までで設定します。

SVC:

スケーラブルビデオコーディングは H.264/AVC の標準機能の拡張です。オフ/オンを選択し、SVC 機能を無効化/有効化します。自動を選択すると、デバイスは、ネットワークの帯域幅が不十分な場合、元のビデオから自動的にフレームを抽出します。

平滑化:

ストリームのスムーズさを指します。スムージングの値が大きいと、ストリームはよりなめらかになりますが、ビデオの品質が十分でない可能性があります。スムージングの値が小さいと、ストリームの品質は向上しますが、なめらかには見えなくなるかもしれません。

4. **[保存]** をクリックして設定を保存します。

7.2 音声設定

方法:

1. 音声設定インターフェイスに入ります: [環境設定] > [ビデオとオーディオ] > [オーディオ]。



図 7-2 オーディオ設定

2. 以下の設定項目を設定します。

音声圧縮: G.722.1、G.711 ulaw、G.711alaw、G.726、MP2L2 および PCM が選択できます。MP2L2 についてはサンプリングレートとオーディオ・ストリーム・ビットレートが設定できます。PCM についてはサンプルレートが設定できます。

音声入力: Lineln で固定されています。

音量入力: 0-100 で調整できます。

環境ノイズフィルター: オフまたはオンに設定できます。この機能が有効の場合、環境中のノイズをある程度フィルターできます。

3. [保存] をクリックして設定を保存します。

7.3 ROI エンコーディング設定

目的:

ROI (関心領域) エンコーディングは関心領域とバックグラウンドの情報を識別してビデオ圧縮を行います。つまり、この技術はエンコーディングリソースを関心領域側により多く割り当て、関心領域の品質を向上し、一方で背景情報に重点を置かないようにします。



ビデオ オーディオ **ROI** 複数ストリーム情報表示

11:28:20.18 Mon 07/25/13

0-312IF

エリアを描く クリア

ストリームタイプ

ストリームタイプ メインストリーム (ノーマル)

固定リージョン

有効

リージョンNo. 1

ROIレベル 3

リージョン名

ダイナミックトラッキング

顔追跡有効

ROIレベル 3

保存

図 7-3 ROI 設定

方法:

1. ROI 設定インターフェイスに入ります:[環境設定] > [ビデオとオーディオ] > [ROI]。
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. 固定領域の項目にある [有効] チェックボックスをチェックします。
4. ROI にする **固定領域** を設定します。
 - (1) ドロップダウンリストから、リージョン No.を選択します。
 - (2) [有効] チェックボックスをチェックして選択した領域の ROI 機能を有効にします。
 - (3) [エリアを描く] をクリックします。マウスをビュー画面上でクリックアンドドラッグして、ROI 領域にする赤い四角形を描きます。[クリア] をクリックすると前に指定した領域をキャンセルできます。完了したら [ドロ-停止] をクリックします。
 - (4) ROI レベルを選択します。
 - (5) 選択した領域に対し、リージョン名を入力します。
 - (6) [保存] をクリックして選択した固定領域の ROI 設定を保存します。
 - (7) 他の固定領域を設定する場合、手順 (1) から (6) を繰り返します。
5. ダイナミックトラッキングを設定します。
 - (1) [顔追跡有効] チェックボックスをチェックします。

注意: 顔追跡機能を有効にするためには顔検知機能を有効にしなければなりません。
 - (2) ROI レベルを選択します。
6. [保存] をクリックして設定を保存します。

注意: ROI レベルは画像品質の向上レベルを意味します。値が大きいほど、画像の品質はよくなります。

7.4 複数ストリーム情報表示

[デュアル VCA 有効にする] チェックボックスをチェックすると、対象(例: 人物、車両など) についての情報がビデオストリーム上にマークされます。さらに、接続された背面デバイスにルールを設定し、ライン横断や侵入などのイベントを検知できます。



ビデオ オーディオ ROI **複数ストリーム情報表示**

デュアルVCA有効にする

 保存

図 7-4 ストリーム上の情報表示

第8章 画像設定

目的:

ディスプレイ設定、OSD 設定、プライバシーマスクの設定を行うにはこの章の指示にしたがいます。

8.1 ディスプレイ設定

目的:

ディスプレイ設定では、画像設定、露光設定、デイ/ナイト切替、逆光設定、ホワイトバランス、画像補正、ビデオ設定、その他のパラメータを設定できます。

8.1.1 デイ/ナイト自動切替

方法:

1. [環境設定]>[画像]>[ディスプレイ設定] から、ディスプレイ設定インターフェイスに入ります。[定期画面設定]において、[スケジュール切替] から [自動切替]に変更すると、画像設定、露光設定、デイ/ナイト切替、逆光設定、ホワイトバランス、画像補正、ビデオ設定、その他のインターフェイスが表示されます。
2. カメラの画像パラメータを設定します。



図 8-1 デイ/ナイト自動切替のディスプレイ設定

- 画像設定

[輝度] は画像の明るさを示し、1 から 100 までの範囲です。

[コントラスト] は画像のコントラストを示し、1 から 100 までの範囲です。

[彩度] は画像の色の鮮やかさを示し、1 から 100 までの範囲です。

[明度] は画像の輪郭の鮮明さを示し、1 から 100 までの範囲です。

- 露光設定

[アイリスモード]は[手動]と[自動]から選択できます。

[自動] が選択された場合、自動絞りレベルは 0 から 100 まで設定することができます。

[露光時間] は電子シャッター速度のことで、1/3 から 1/100,000 の範囲です。実際の光量の状況に応じて調整してください。

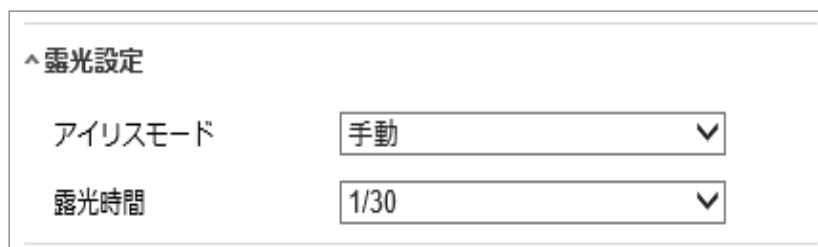


図 8-2 露光設定

- デイ/ナイト切替

個別の監視要件に応じてデイ/ナイト切替モードを選択してください。

デイ/ナイト切替では、日、ナイト、自動、スケジュール切替、またはイベントトリガーが選択できます。



図 8-3 デイ/ナイト切替

日: カメラはデイモードに固定されます。

ナイト: カメラはナイトモードに固定されます。

自動: カメラはデイモードとナイトモードを光量に応じて自動的に切り替えます。感度は 0 から 7 までの範囲で、値が大きいほど切り替えが発生

しやすくなります。フィルタリングタイムはデイ/ナイト切り替えの間の間隔時間を示します。5 秒から 120 秒の間で設定できます。

スケジュール切替: 開始時間と終了時間を設定し、デイ/ナイトモードの継続時間を設定します。

イベントトリガー: アラーム入力によって切り替えがトリガーされます。トリガーされるモードを日またはナイトに設定できます。

- **逆光設定**

BLC エリア: 強い逆光に向かって対象にフォーカスすると、対象は暗くなりすぎて明瞭に見えなくなります。BLC は光を補正して手前の対象を明瞭に見えるようにします。オフ、上、下、左、右、センター、自動が選択できます。

注意: BLC モードがカスタマイズに設定されている場合、BLC 領域としてライブビュー画像上に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画面の明るい部分と暗い部分のコントラスト差が大きい場合に利用できます。

- **ホワイトバランス**

ホワイトバランスはカメラに白を正しく発色させる機能で、環境に応じて色温度を調整することができます。

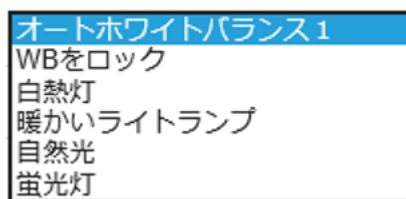


図 8-4 ホワイトバランス

- **画像補正**

ノイズリダクション: DNR はビデオストリームのノイズを低減します。オフ、ノーマル・モード、エキスパート・モードが選択できます。ノーマル・モードでは ノイズ除去レベルを 0 から 100 までで設定します。エキスパート・モードでの DNR レベルは空間 DNR レベル [0-100] と時間 DNR レベル [0-100] の両方で設定します。

- **ビデオ設定**

ミラー反転: 画像を鏡像転回し、反転した状態で見ることができます。左右、上下、センター中央およびオフが選択できます。

廊下モード: 16:9 のアスペクト比を完全に利用するために、カメラを狭い映像領域で使用する場合には回転機能を有効化できます。

設置する際にカメラを 90 度回転させるか、3 軸レンズを 90 度回転させた上で廊下モードをオンに設定すると、シーンの通常画像を 9:16 のアスペクト比で表示させ、壁などの不要な情報は無視し、シーンの中でより意味のある情報だけを取得することができます。

シーンモード: 屋外と屋内から選択できます。

ビデオ標準: 50 Hz および 60 Hz が選択できます。それぞれのビデオ規格に応じて選択してください。通常、PAL 規格では 50 Hz、NTSC 規格では 60 Hz です。

- **その他**

ローカル出力: オンとオフから選択できます。

8.1.2 デイ/ナイトスケジュール切替

デイ/ナイトスケジュール切替設定インターフェイスでは、カメラのパラメータをデイとナイトで個別に設定し、異なる光量下でも画像品質を確保できます。

図 8-5 デイ/ナイトスケジュール切替設定インターフェイス

方法:

1. [環境設定]>[画像]>[ディスプレイ設定] から、ディスプレイ設定インターフェイスに入ります。[定期画面設定]において、[自動切替]から[スケジュール切替]に変更すると、デイ/ナイトスケジュール切替設定インターフェイスが表示されます。
2. デイ/ナイトスケジュール切替インターフェイスのカレンダーアイコンをクリックして切り替えの開始時間と終了時間を選択します。

注意:

- 開始時間と終了時間はデイモードに対して適正な時間を示します。
 - 時間帯は連続した 2 日間にまたがって開始、終了させることができます。例えば、開始時間を 10:00 に設定し、終了時間を 1:00 に設定すると、デイモードは午前 10 時にアクティベートされ、次の日の午前 1 時に終了します。
3. デイ/ナイトスケジュール切替インターフェイスの[ノーマル] タブをクリックし、デイモードとナイトモードで共通して適用されるパラメータ（露光設定、デイ/ナイト切替、ビデオ設定、その他）を設定します。

注意: 各パラメータの詳細については 8.1.1 節 デイ/ナイト自動切替を参照してください。

4. デイ/ナイトスケジュール切替インターフェイスの[日] タブをクリックし、デイモードに適用されるパラメータ（画像設定、露光設定、逆光設定、ホワイトバランス、画像補正）を設定してください。
5. デイ/ナイトスケジュール切替インターフェイスの[ナイト] タブをクリックし、ナイトモードに適用されるパラメータ（画像設定、露光設定、逆光設定、ホワイトバランス、画像補正）を設定してください。

注意: パラメータが変更されると設定は自動的に保存されます。

8.2 OSD 設定

目的:

カメラ名、時刻/日付の表示形式、表示方式、OSD のサイズをカスタマイズできます。

ディスプレイ設定 OSD設定 プライバシーマスク

表示名
 日付表示
 曜日表示

カメラ名 YK-H021A
時間表示方式 24時間
日付の表示形式 XX-XX-XXXX (月日年)

テキストのオーバーレイ

1
 2
 3
 4

表示方式 トランスペアレント&フラッシュ
OSDサイズ 自動
フォント色 ブラック&ホワイトの自適応
位置合わせ カスタマイズ

保存

図 8-6 OSD 設定

方法:

1. OSD 設定インターフェイスに入ります:[環境設定] > [画像] > [OSD 設定]。
2. 必要に応じてカメラ名、日付、曜日を表示するため、対応するチェックボックス（表示名、日付表示、曜日表示）をチェックします。
3. [カメラ名] テキストフィールドにカメラ名を入力します。
4. ドロップダウンリストから時間表示方式と日付の表示形式を選択します。
5. ドロップダウンリストから表示方式、OSD サイズ、フォント色を選択します。

6. テキストオーバーレイを設定します。
 - (1) テキストボックスの前のチェックボックスをチェックしてオンスクリーンディスプレイを有効化します。
 - (2) テキストボックスに文字列を入力します。

注意: テキストオーバーレイは 8 つまで設定できます。
7. テキスト枠の位置と配置を調整します。

左位置合わせ、右位置合わせ、カスタマイズが選択できます。カスタマイズを選択した場合、マウスでライブビューウィンドウ上のテキスト枠をクリックアンドドラッグして位置を調整します。

注意: 配置調整はテキストオーバーレイ項目にのみ適用されます。
8. **[保存]** をクリックして設定を保存します。

8.3 プライバシーマスクの設定

目的:

プライバシーマスクはライブビデオ上の特定のエリアをカバーし、監視エリア中の特定の部分がライブビューで見られたり、録画されたりすることを防止できます。

方法:

1. プライバシーマスク設定インターフェイスに入ります: **[環境設定]** > **[画像]** > **[プライバシーマスク]**。
2. **[プライバシーマスクを有効にする]** チェックボックスをチェックして機能を有効化します。
3. **[エリアを描く]** をクリックします。



図 8-7 プライバシーマスク設定

4. ライブビデオウィンドウ上でマウスをクリックアンドドラッグし、マスク領域を指定します。

注意: 同一画像上で 4 つまでの領域を指定することができます。

5. [ドロー停止] をクリックして指定を完了するか、[すべてクリアー] をクリックして設定した領域をセーブせずにすべて消去することができます。
6. [保存] をクリックして設定を保存します。

第9章 イベント設定

この節ではネットワークカメラが基本イベントとスマートイベントを含む、アラームイベントに反応できるように設定する方法を説明します。

9.1 基本イベント

この節の指示にしたがうことで、動体検知、タンパリング、アラーム入力、アラーム出力、異常などを含む基本イベントを設定することができます。これらのイベントについては監視センター通知、Eメール送信、アラーム出力トリガーなどのリンケージメソッドのトリガーにすることができます。

注意: アラームがトリガーされ次第、アラーム情報を PC またはモバイルクライアントソフトウェアにプッシュ通知したい場合、**[監視センターに通知する]** チェックボックスをチェックします。

9.1.1 動体検知設定

目的:

動体検知機能は、設定された監視シーン内で動く物体を検知し、アラームトリガー時に指定した一連のアクションを実行できます。

動く物体を正確に検知し、アラームの誤発報率を低減するために、異なる動体検知環境向けに、ノーマル・モードとエキスパート・モードが選択できます。

● ノーマル・モード

ノーマル・モードではデイでもナイトでも同じセットの動体検知パラメータを適用します。

タスク 1: 動体検知エリアの設定

方法:

1. 動体検知設定インターフェイスに入ります:**[環境設定]**>**[イベント]**>**[イベント]**>**[動体検知]**。
2. **[動体検知有効]** のチェックボックスをチェックします。

- 検知した対象を緑の四角形でマークしたい場合、[モーションの動的解析を有効] チェックボックスをチェックします。

注意: 検知した対象に緑の四角形を表示させたくない場合、このルールについては無効化を選択してください。[環境設定] > [ローカル] > [ライブ画像のパラメータ] からルールの無効化を選択します。



図 9-1 動体検知の有効化

- [エリアを描く] をクリックします。ライブビデオウィンドウ上でマウスをクリックアンドドラッグし、動体検知領域を指定します。[ドロー停止] をクリックして領域の指定を完了します。
- (オプション) [すべてクリアー] をクリックして領域をすべて消去します。
- (オプション) スライダーを操作して検知の感度を設定します。

タスク 2: 動体検知のアラームスケジュール設定



図 9-2 アラームスケジュール

方法:

1. **アラームスケジュール** をクリックしてアラームスケジュールを編集します。
2. 時間指定バーをクリックアンドドラッグして時間帯を選択します。



図 9-3 アラームスケジュール

注意: 選択した時間帯をクリックすると、時間指定バーを操作するか、正確な時間帯を入力することで、時間帯を調整できます。

3. (オプション) [削除] をクリックして現在のアラームスケジュールを消去するか、[保存] をクリックすることで設定を保存できます。
4. マウスをそれぞれの曜日の最後に移動するとコピーダイアログがポップアップし、現在の設定を他の曜日にコピーすることができます。
5. [保存] をクリックして設定を保存します。

注意: 各時間帯の時間は重複できません。最大 8 件の時間帯を各曜日に設定できます。

タスク 3: 動体検知のリンケージメゾット設定

チェックボックスをチェックしてリンケージメゾットを選択します。Eメールの送付、監視センターに通知する、FTP/メモリーカード/NAS へのアップロード、トリガアラームアウトプットおよび録画をトリガーが選択できます。イベント発生時のリンケージメゾットを指定できます。

リンケージメゾット		
<input type="checkbox"/> ノーマルリンケージ	<input type="checkbox"/> トリガアラームアウトプット	<input type="checkbox"/> 録画をトリガー
<input type="checkbox"/> Eメールの送付	<input type="checkbox"/> A->1	<input type="checkbox"/> A1
<input checked="" type="checkbox"/> 監視センターに通知する		
<input type="checkbox"/> FTP/メモリーカード/NASへ...		

図 9-4 リンケージメゾット

- **監視センターの通知**

イベント発生時に異常またはアラーム信号をリモートの管理ソフトウェアに送信します。

- **Eメールの送付**

イベント発生時にアラーム情報を Eメールでユーザー (複数可) に送信します。

注意: イベント発生時に Eメールを送信する場合、事前に 6.2.3 節 を参照して Eメール設定を完了してください。

- **FTP/メモリーカード/NAS へのアップロード**

アラームがトリガーされた時点で画像をキャプチャし、その画像を FTP サーバーにアップロードします。

注意:

- FTP アドレスとリモート FTP サーバーをまず設定してください。詳細については 6.2.2 節 **FTP 設定** を参照してください。
- **[環境設定]>[ストレージ]>[スケジュール設定]>[キャプチャ]>[キャプチャパラメータ]** ページから、イベントトリガーによるスナップショットを有効化し、キャプチャ間隔とキャプチャ数を設定します。
- キャプチャ画像は利用可能な 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。

- **トリガアラームアウトプット**

イベント発生時、1 つ異常の外部アラーム出力をトリガーします。

注意: イベント発生時にアラーム出力をトリガーする場合、9.1.4 節 **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。

- **録画をトリガー**

動体が検知されると、ビデオが録画されます。この機能を利用する場合、録画スケジュールを設定する必要があります。詳細情報については 10.1 節 を参照してください。

● エキスパート・モード

エキスパート・モードは主に、デイ/ナイト切り替え時の感度や各エリアでの対象の比率を個別に設定するのに使われます。



図 9-5 動体検知のエキスパート・モード

● デイ/ナイト切り替えオフ

方法:

1. ノーマル・モードと同様に検知エリアを指定します。エリアは 8 つまでサポートされています。
2. [定期画像切替] 設定で [オフ] 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. 選択したエリアについて、カーソルをスライドさせて感度とエリア上の対象の比率を設定します。
5. ノーマル設定モードと同様にアラームスケジュールとリンケージメゾットを設定します。
6. [保存] をクリックして設定を保存します。

● デイ/ナイト自動切替

方法:

1. ノーマル・モードと同様に検知エリアを指定します。エリアは 8 つまでサポートされています。
2. [定期画像切替] 設定で [自動切替] 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. 選択したエリアの日の時間帯について、カーソルをスライドさせて感度とエリア上の対象の比率を設定します。
5. 選択したエリアのナイトの時間帯について、カーソルをスライドさせて感度とエリア上の対象の比率を設定します。
6. ノーマル・モードと同様にアラームスケジュールとリンケージメゾットを設定します。
7. **[保存]** をクリックして設定を保存します。

- **デイ/ナイトスケジュール切替**

方法:

1. ノーマル・モードと同様に検知エリアを指定します。エリアは 8 つまでサポートされています。
2. **[定期画像設定]** 設定で **[スケジュール切替]** を選択します。

定期画像設定	スケジュール切替
開始時間	06:00:00
終了時間	18:00:00

図 9-6 日中/夜間スケジュール切り替え

3. 切り替え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. 選択したエリアの日の時間帯について、カーソルをスライドさせて感度とエリア上の対象の比率を設定します。
6. 選択したエリアのナイトの時間帯について、カーソルをスライドさせて感度とエリア上の対象の比率を設定します。
7. ノーマル・モードと同様にアラームスケジュールとリンケージメゾットを設定します。
8. **[保存]** をクリックして設定を保存します。

9.1.2 タンパリングアラーム

目的:

レンズが塞がれた場合にアラームをトリガーし、アラームに対応する特定のアクションを起こすようにカメラを設定することができます。

方法:

1. [環境設定]>[イベント]>[イベント]>[タンパリングアラーム / 或者カメラ妨害アラーム] からタンパリングアラームインターフェイスに入ります。



図 9-7 タンパリングアラーム

2. [有効] チェックボックスをチェックしてタンパリングアラームを有効化します。
3. エリアを設定します。9.1.1 節 **タスク 1: 動体検知エリアの設定** を参照してください。
4. [アラームスケジュール] をクリックし、タンパリングアラームのアラームスケジュールを編集します。アラームスケジュールの設定は動体検知用の

アラームスケジュール設定と同様です。9.1.1 節 **タスク 2: 動体検知エリアのアラームスケジュール設定**を参照してください。

5. チェックボックスをチェックしてタンパリング発生時のリンケージメゾットを選択してください。監視センターに通知する、Eメールおよびトリガアラームアウトプットが選択できます。9.1.1 節の **タスク 3: 動体検知のリンケージメゾット設定** を参照してください。
6. **[保存]** をクリックして設定を保存します。

9.1.3 アラーム入力の設定

方法:

1. アラーム入力設定インターフェイスに入ります:[環境設定]>[イベント]>[イベント]>[アラーム入力]。
2. アラーム入力 No.およびアラームの種類を選択します。アラームの種類は NO (通常時オープン) と NC (通常時クローズ) が設定できます。アラーム名を編集して設定することができます (オプション)。

動体検知 タンパリングアラーム / 或者カメラ妨害アラーム **アラーム入力** アラーム出力 異常検知設定

アラーム入力 No. IPアドレス

アラームの種類 アラーム名 (コピーできません)

アラームインプットを処理します

アラームスケジュール リンケージメゾット

月	0	2	4	6	8	10	12	14	16	18	20	22	24
火曜日	0	2	4	6	8	10	12	14	16	18	20	22	24
水曜日	0	2	4	6	8	10	12	14	16	18	20	22	24
木曜日	0	2	4	6	8	10	12	14	16	18	20	22	24
金曜日	0	2	4	6	8	10	12	14	16	18	20	22	24
土曜日	0	2	4	6	8	10	12	14	16	18	20	22	24
日	0	2	4	6	8	10	12	14	16	18	20	22	24

図 9-8 アラーム入力設定

3. [アラームスケジュール] をクリックしてアラーム入力のアラームスケジュールを設定します。9.1.1 節 **タスク 2: 動体検知エリアのアラームスケジュール設定**を参照してください。
4. [リンケージメゾット] をクリックし、チェックボックスをチェックしてアラーム入力に対応するリンケージメゾットを選択してください。9.1.1 節の **タスク 3: 動体検知のリンケージメゾット設定** を参照してください。
5. 設定を他のアラーム入力にコピーすることができます。
6. [保存] をクリックして設定を保存します。

9.1.4 アラーム出力の設定

The screenshot shows the 'Alarm Output' configuration page. At the top, there are tabs for '動体検知', 'タンパリングアラーム / 或者カメラ妨害アラーム', 'アラーム入力', 'アラーム出力', and '異常検知設定'. The 'アラーム出力' tab is active. Below the tabs, there are several input fields: 'アラーム出力No.' (dropdown menu with 'A->1'), '遅延' (dropdown menu with '5秒'), 'アラーム状態' (dropdown menu with 'オフ'), 'IPアドレス' (text input with 'ローカル'), and 'アラーム名' (text input with '(コピーできません)'). Below these is a section for 'アラームスケジュール' with a calendar grid. The grid shows days of the week and hours from 0 to 24. All days are selected with blue bars. At the bottom, there are three buttons: '⊞ 手動アラーム', '📄 ...にコピーする', and a red '保存' button.

図 9-9 アラーム出力設定

方法:

1. アラーム出力設定インターフェイスに入ります:[環境設定] > [イベント] > [イベント] > [アラーム出力]。
2. [アラーム出力 No.] ドロップダウンリストからアラーム出力チャネルを 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 (オプション)。
3. 遅延時間は 5 秒、10 秒、30 秒、1 分、2 分、5 分、10 分または手動に設定できます。遅延時間はアラーム発生時点からアラーム出力が有効であ

る間の時間を示します。

4. **[アラームスケジュール]** をクリックしてスケジュール時間設定インターフェイスに入ります。時間スケジュールの設定は動体検知用のアラームスケジュール設定と同様です。9.1.1 節 **タスク 2: 動体検知エリアのアラームスケジュール設定**を参照してください。
5. 設定を他のアラーム出力にコピーすることができます。
6. **[保存]** をクリックして設定を保存します。

9.1.5 異常への対応処理

異常検知タイプには HDD フル、HDD エラー、ネットワーク未接続、IP アドレスが競合、不正なログインがあります。

方法:

1. 異常設定インターフェイスに入ります:**[環境設定]** > **[イベント]** > **[イベント]** > **[異常検知設定]**。
2. チェックボックスをチェックして異常アラームに対応するリンケージメゾットを選択してください。9.1.1 節 **タスク 3: 動体検知のリンケージメゾット設定** を参照してください。

異常検知タイプ	
HDDフル	
<input type="checkbox"/> ノーマルリンケージ	<input type="checkbox"/> トリガアラームアウトプット
<input type="checkbox"/> Eメールの送付	<input type="checkbox"/> A->1
<input type="checkbox"/> 監視センターに通知する	

図 9-10 異常設定

3. **[保存]** をクリックして設定を保存します。

9.2 スマートイベント

この節の指示にしたがうことで、シーン変化検知、侵入検知およびライン横断検知などを含むスマートイベントを設定することができます。これらのイベントについては監視センターへの通知、Eメールの送付、トリガアラームアウトプットなどのリンケージメゾットのトリガーにすることができます。

9.2.1 オーディオ異常検出の設定

オーディオの急激な変化を検出する機能です。

このアラームがトリガーされた場合、特定のアクションを行うことができます。

方法:

1. [環境設定] > [イベント] > [Smart 事件] > [オーディオ異常検出] からオーディオ異常検出設定インターフェイスに入ります。

オーディオ異常検出 焦点ぼけ検出 シーン変更検知 顔検出 エリア侵入検出

異常検出 アラームスケジュール リンケージメゾット

異常検出

音声入力異常

音の強く急に上がる検出

感度 50

音響インテンシティ値 50

音の強く急に下がる検出

感度 50

リアルタイム音量

保存

2. 各チェックボックスをチェックして機能を有効化します。
3. スライダーをドラッグアンドドロップし検出感度を設定します。感度の範囲は1から100で、値が高いほどオーディオ異常によるアラームトリガーが発生しやすくなります。

- オーディオ異常に対するリンケージメソッド(監視センターに通知する、Eメールの送信、トリガアラームアウトプットを含む)を選択します。
- [保存] をクリックして設定を保存します。

9.2.2 焦点ぼけ検出の設定

目的:

レンズの焦点ぼけによって起こる画像のぼけを検出する機能です。このアラームがトリガーされた場合、特定のアクションを行うことができます。

方法:

- [環境設定] > [イベント] > [Smart 事件] > [焦点ぼけ検出] から焦点ぼけ検出設定インターフェイスに入ります。

オーディオ異常検知	焦点ぼけ検出	シーン変更検知	顔検出	エリア侵入検出
<input type="checkbox"/> 有効				
感度	50			
<input type="checkbox"/> ノーマルリンケージ	<input checked="" type="checkbox"/> トリガアラームアウトプット			
<input type="checkbox"/> Eメールの送付	<input type="checkbox"/> A->1			
<input type="checkbox"/> 監視センターに通知する				

- [有効] チェックボックスをチェックして機能を有効化します。
- スライダーをドラッグアンドドロップし検出感度を設定します。感度の範囲は1から100で、値が高いほど焦点ぼけによるアラームトリガーが発生しやすくなります。
- 焦点ぼけに対するリンケージメソッド(監視センターに通知する、Eメールの送信、トリガアラームアウトプットを含む)を選択します。
[保存] をクリックして設定を保存します。

9.2.3 シーン変更検知の設定

目的:

シーン変更検知は意図的なカメラの回転など、外的要素の影響による監視環境の変化を検知する機能です。このアラームがトリガーされた場合、特定のアクションを行うことができます。

方法:

1. [環境設定] > [イベント] > [Smart 事件] > [シーン変更検知] からシーン変更検知設定インターフェイスに入ります。



図 9-11 シーン変更検知

2. [有効] チェックボックスをチェックして機能を有効化します。
3. 感度スライダーをクリックアンドドラッグして、検知感度を設定します。感度の値は 1 から 100 の範囲で、値が高いほど、より容易にシーン変更アラームがトリガーされるようになります。
4. [アラームスケジュール] をクリックしてアラームスケジュールを設定します。詳細手順については 9.1.1 節 **タスク 2: 動体検知エリアのアラームスケジュール設定**を参照してください。

5. [リンケージメゾット] をクリックして、シーン変化に対応するリンケージメゾット(監視センターに通知する、Eメールの送信、FTP/メモリーカード/NAS へのアップロード、録画をトリガー、トリガアラームアウトプットを含む)を選択することができます。
6. [保存] をクリックして設定を保存します。

9.2.4 顔検出の設定

目的:

顔検出機能は、監視シーンに表示される顔を検知し、アラーム起動時に特定のアクションを実行できます。

方法:

1. [環境設定] > [イベント] > [Smart 事件] > [顔検出] から顔検出設定インターフェイスに入ります。
2. [顔検知を有効にする] チェックボックスをチェックして機能を有効化します。
3. 顔検出の [顔検知のダイナミック解析を有効にする] チェックボックスをチェックすると、ライブビデオ上で検出した顔が緑の四角形でマークされます。
注意: ライブビデオ上で検出した顔をマークしたい場合、[環境設定] > [ローカル] からライブ画像のパラメーターの[ルール] を有効化します。
4. 感度スライダーをクリックアンドドラッグして、検知感度を設定します。感度は 1 から 5 までです。値が高いほど、顔を検出しやすくなります。
5. [アラームスケジュール] をクリックしてアラームスケジュールを設定します。詳細手順については 9.1.1 節 **タスク 2: 動体検知エリアのアラームスケジュール設定**を参照してください。
6. [リンケージメゾット] をクリックして顔検出に対応するリンケージメゾットを選択します。9.1.1 節 **タスク 3: 動体検知のリンケージメゾット設定** を参照してください。



図 9-12 顔検出

7. [保存] をクリックして設定を保存します。

9.2.5 エリア侵入検出の設定

目的:

エリア侵入検出機能は、事前に定義したバーチャル領域において侵入/徘徊する人物、車両またはその他の対象を検知し、アラームトリガー時に特定のアクションを実行できます。

方法:

1. [環境設定] > [イベント] > [Smart 事件] > [エリア侵入検出] からエリア侵入検出設定インターフェイスに入ります。



図 9-13 エリア侵入検知

2. **[有効]** チェックボックスをチェックして機能を有効化します。
3. 検知設定を行うには、エリアドロップダウンリストから領域を選択します。
4. **[エリア設定]** タブをクリックし、**[エリアを描く]** ボタンを押して領域の指定を開始します。
5. ライブビデオ上でクリックし、検知領域の 4 つの頂点を指定し、右クリックで指定を完了します。
6. 時間限界値、感度およびエリア侵入検出のための対象の比率を設定します。
時間限界値は [0 秒-10 秒] で、対象が範囲内で移動する時間しきい値です。値を 0 に設定すると、領域内に対象が侵入した時点で直ちにアラームをトリガーします。
感度: 範囲は [1-100] です。感度の値は、アラームのトリガーとなりうる対象のサイズを定義します。感度が高い場合、非常に小さい対象でもアラームがトリガーされます。
7. **[クリア]** ボタンをクリックすると、すでに定義されている領域をすべて消去します。
8. **[アラームスケジュール]** をクリックしてアラームスケジュールを設定します。

9. [リンケージメゾット] をクリックして、エリア侵入検出に対応するリンケージメゾット(監視センターに通知する、Eメールの送付、FTP/メモリーカード/NAS へのアップロード、録画をトリガー、トリガアラームアウトプットを含む)を選択することができます。
10. [保存] をクリックして設定を保存します。

9.2.6 線のクロス検出の設定

目的:

線のクロス検出機能は、事前に定義したバーチャルラインを横断する人物、車両またはその他の対象を検知し、アラームトリガー時に特定のアクションを実行できます。

方法:

1. [環境設定] > [イベント] > [Smart 事件] > [線のクロス検出] から線のクロス検出設定インターフェイスに入ります。



図 9-14 ライン横断検知

2. [有効] チェックボックスをチェックして機能を有効化します。
3. [警戒線] ドロップダウンリストからラインを選択します。
4. [エリア設定] タブをクリックし、[エリアを描く] ボタンをクリックすると

ライブビデオ上にバーチャルラインが表示されます。

5. ラインをクリックアンドドラッグし、ライブビデオ上の任意の位置に移動させることができます。ラインをクリックすると、2 つの赤い四角形が両端に表示されます。この赤い四角形をクリックアンドドラッグすることでラインの形状と長さを指定できます。

6. 線のクロス検出の方向を選択します。方向を A<->B、A->B、B->A のいずれかから選択できます。

A<->B: ラインを横断する対象をどちら向きの方でも検知でき、アラームが起動されます。

A->B: 設定されたラインを A サイドから B サイドに横断する対象のみ検知できます。

B->A: 設定されたラインを B サイドから A サイドに横断する対象のみ検知できます。

7. 感度スライダーをクリックアンドドラッグして、検知感度を設定します。
感度: 範囲は [1-100] です。値が高いほど、ラインを横断する行為を検出しやすくなります。

8. **[クリア]** ボタンをクリックすると、すでに定義されているラインを消去します。

9. **[アラームスケジュール]** をクリックしてアラームスケジュールを編集します。

10. **[リンケージメゾット]** をクリックして、線のクロス検出に対応するリンケージメゾット(監視センターに通知する、Eメールの送付、FTP/メモリーカード/NAS へのアップロード、録画をトリガー、トリガアラームアウトプットを含む)を選択することができます。

11. **[保存]** をクリックして設定を保存します。

9.2.7 領域進入検知

目的:

領域進入検知機能は、事前に定義したバーチャル領域に外部から進入する人物、車両またはその他の対象を検知し、アラームトリガー時に特定のアクションを実行できます。

方法:

1. 領域進入検知設定インターフェイスに入ります：
[設定] > [イベント] > [Smart事件] > [検知区域入る]
2. [有効] チェックボックスをチェックして領域進入検知機を有効化します。



図 9-15 領域進入検知設定

3. 検知設定を行うには、ドロップダウンリストから領域を選択します。
4. [エリアを描く] ボタンをクリックし、領域指定を開始します。
5. ライブビデオ上でクリックし、検知領域の 4 つの頂点を指定し、右クリックで指定を完了します。

他の領域を設定する場合、この手順を繰り返してください。最大 4 つの領域を設定できます。[クリア] ボタンをクリックすると、すでに定義されている領域をすべて消去します。

6. [アラームスケジュール] タブをクリックして監視スケジュール設定イ

ンターフェイスに入ります。時間スケジュールの設定は動体検知用の監視スケジュール設定と同様です。9.1.1 節 動体検知設定 のステップ 2 を参照してください。

7. [リンケージメゾット] タブをクリックして領域進入検知に対応するリンク方式を選択します。監視センター通報、E メール送信、FTP アップロード、録画をトリガー、トリガアラームアウトプットが選択できます。9.1.1 節 動体検知設定 のステップ 3 を参照してください。
8. [保存] をクリックして設定を保存します。

9.2.8 領域退出検知

目的:

領域退出検知機能は、事前に定義したバーチャル領域から退出する人物、車両またはその他の対象を検知し、アラームトリガー時に特定のアクションを実行できます。

方法:

1. 領域退出検知設定インターフェイスに入ります：
[設定] > [イベント] > [Smart事件] > [検知区域離れる]
2. [有効] チェックボックスをチェックして領域退出検知機能を有効化します。



図 9-16 領域退出検知設定

3. **【エリアを描く】** ボタンをクリックし、領域指定を開始します。
4. ライブビデオ上でクリックし、検知領域の 4 つの頂点を指定し、右クリックで指定を完了します。

他の領域を設定する場合、この手順を繰り返してください。最大 4 つの領域を設定できます。**【クリア】** ボタンをクリックすると、すでに定義されている領域をすべて消去します。
5. **【アラームスケジュール】** タブをクリックして監視スケジュール設定インターフェイスに入ります。時間スケジュールの設定は動体検知用の監視スケジュール設定と同様です。**9.1.1 節 動体検知設定** のステップ 2 を参照してください。
6. **【リンクージメゾット】** タブをクリックして領域退出検知に対応するリンク方式を選択します。監視センター通報、E メール送信、FTP アップロード、録画をトリガー、トリガアラームアウトプットが選択できます。**9.1.1 節 動体検知設定** のステップ 3 を参照してください。
7. **【保存】** ボタンをクリックし、設定を保存します。

9.2.9 放置手荷物検知の設定

目的:

放置荷物検知機能は、事前に定義した領域に放置された荷物、財布、危険物などの対象を検知し、アラームトリガー時に一連のアクションを実行できます。

方法:

1. **【環境設定】 > 【イベント】 > 【Smart 事件】 > 【放置手荷物検知】** から放置手荷物検知設定インターフェイスに入ります。



図 9-17 放置荷物検知

2. **[有効]**チェックボックスをチェックして機能を有効化します。
3. 検知設定を行うには、エリアドロップダウンリストから**領域**を選択します。
4. **[エリア設定]** をクリックし、**[エリアを描く]** をクリックして領域の指定を開始します。
5. ライブビデオ上でクリックし、検知領域の 4 つの頂点を指定し、右クリックで指定を完了します。
6. 放置手荷物検知の時間限界値と感度を設定します。
時間限界値: 範囲は [5-20 秒] で、対象が範囲内で放置された時間のしきい値です。値を 10 に設定すると、範囲内に 10 秒間、対象が留まった後にアラームをトリガーします。
感度: 範囲は [1-100] です。感度の値は、背景画像との類似の度合いを定義します。通常、感度が高い場合、非常に小さい対象物が範囲内に放置された場合でもアラームがトリガーされます。
7. **[クリア]** ボタンをクリックすると、すでに定義されている領域を消去します。
8. **[アラームスケジュール]** をクリックしてアラームスケジュールを設定します。
9. **[リンケージメゾット]** をクリックしてリンケージメゾットを選択します。

10. [保存] をクリックして設定を保存します。

9.2.10 物体撤去検知の設定

目的:

物体撤去検知機能は、事前に定義した範囲から、展示物などの対象が除去されたことを検知し、アラームトリガー時に一連のアクションを実行できます。

方法:

1. [環境設定] > [イベント] > [Smart 事件] > [物体撤去検知] から物体撤去検知設定インターフェイスに入ります。



図 9-18 物体撤去検知

2. [有効]チェックボックスをチェックして機能を有効化します。
3. 検知設定を行うには、エリアドロップダウンリストから領域を選択します。
4. [エリア設定] をクリックし、[エリアを描く] ボタンを押して領域の指定を開始します。
5. ライブビデオ上でクリックし、検知領域の 4 つの頂点を指定し、右クリックで指定を完了します。
6. 物体撤去検知の時間限界値と感度を設定します。

時間限界値: 範囲は [5-20 秒] で、対象が範囲内で撤去されてからの時間のしきい値です。値を 10 に設定すると、対象が 10 秒間、範囲から離れた後にアラームをトリガーします。

感度: 範囲は [1-100] です。感度の値は、背景画像との類似の度合いを定義します。通常、感度が高い場合、非常に小さい対象物が範囲から離れた場合でもアラームをトリガーできます。

7. **[クリア]** ボタンをクリックすると、すでに定義されている領域を消去します。

8. **[アラームスケジュール]** をクリックしてアラームスケジュールを設定します。

9. **[リンケージメゾット]** をクリックしてリンケージメゾットを選択します。

10. **[保存]** をクリックして設定を保存します。

第10章 ストレージ設定

始める前に:

録画設定を行う前に、ネットワークストレージデバイスか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。

10.1 録画スケジュール設定

目的:

カメラが行う録画には 2 種類あります: マニュアル録画とスケジュール録画です。この節の指示にしたがって、スケジュール録画の設定を行います。デフォルトではスケジュール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。

方法:

1. 録画スケジュール設定インターフェイスに入ります:[環境設定]>[ストレージ]>[スケジュール設定]>[記録スケジュール]。



図 10-1 録画スケジュール設定

2. **[有効]** チェックボックスをチェックしてスケジュール録画を有効化します。
3. **[高度]**をクリックして、カメラの録画パラメータを設定します。

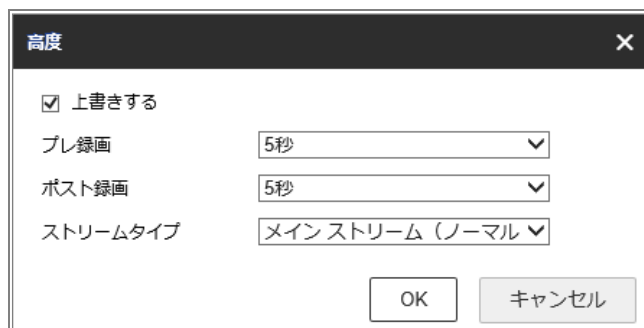


図 10-2 録画パラメータ

- **プレ録画:** スケジュールされた時間またはイベントの前に、録画を開始しておく時間を示します。例えば、アラームが 10 時に録画をトリガーする場合に、事前録画時間が 5 秒に設定されていると録画は 9:59:55 に始まります。
プレ録画時間は、プリ録画しない、5 秒、10 秒、15 秒、20 秒、25 秒、30 秒、限定しないのいずれかに設定できます。
 - **ポスト録画:** スケジュールされた時間またはイベントの後に、録画を停止するまでの時間を示します。例えば、アラームが 11 時に録画停止をトリガーする場合に、ポスト録画時間が 5 秒に設定されていると録画は 11:00:05 に停止します。
ポスト録画時間は、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。
 - **ストリームタイプ:** 録画のストリームタイプはメインストリームで固定されています。
4. **[録画種別]** を選択します。録画種別は、スケジュール録画、動体検知、アラーム、動体検知/アラーム、モーション&アラーム、イベントのいずれかに設できます。
 - **スケジュール録画**
[スケジュール録画] を選択した場合、録画はスケジュールした時間に

したがって自動的に開始されます。

- **動体検知トリガーによる録画**

[**動体検知**] を選択した場合、動体が検知されると、ビデオが録画されます。

録画スケジュールの設定に加えて、動体検知領域を設定し、動体検知のリンケージメゾット設定インターフェイスで [トリガーチャンネル] チェックボックスをチェックする必要があります。詳細情報については 9.1.1 節の **タスク 1: 動体検知エリアの設定** を参照してください。

- **アラームトリガーによる録画**

[**アラーム**] を選択した場合、ビデオは外部アラーム入力チャンネルからアラームがトリガーされた場合に録画されます。

録画スケジュールの設定に加えて、[**アラーム種別**] を設定し、アラーム入力のリンケージメゾット設定インターフェイスで [**録画をトリガー**] チェックボックスをチェックする必要があります。詳細情報については 9.1.3 節を参照してください。

- **モーション& アラームによる録画**

[**モーション& アラーム**] を選択するとビデオは動体が検知され、かつ、アラームが同時にトリガーされた場合に録画されます。

録画スケジュールの設定に加えて、[**動体検知**] および [**アラーム入力設定**] インターフェイスで設定を行う必要があります。詳細情報については 9.1.1 節 と 9.1.3 節を参照してください。

- **動体検知/アラームによる録画**

[**動体検知/アラーム**] を選択するとビデオは外部アラームがトリガーされるか、または動体が検知された場合に録画されます。

録画スケジュールの設定に加えて、[**動体検知**] および [**アラーム入力設定**] インターフェイスで設定を行う必要があります。詳細情報については 9.1.1 節 と 9.1.3 節を参照してください。

- イベントトリガーによる録画

[イベント] を選択した場合、イベントがトリガーされると、ビデオが録画されます。録画スケジュールの設定に加えてイベント設定を行う必要があります。

5. [録画種別] を選択し、時間バーの上でクリックアンドドラッグし、録画スケジュールを設定します。
6. [保存] をクリックして設定を保存します。

10.2 キャプチャスケジュール設定

目的:

スケジュールによるスナップショットとイベントトリガーによるスナップショットを設定することができます。キャプチャされ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管できます。

方法:

1. キャプチャ設定インターフェイスに入ります:[環境設定]>[ストレージ]>[ストレージマネジメント]>[キャプチャー]。



図 10-3 キャプチャ設定

2. **[キャプチャのスケジュール]** タブから時間バーの上でマウスをクリックアンドドラッグし、キャプチャスケジュールを設定します。各時間バーの右にある緑色のコピーアイコンをクリックすることで、キャプチャスケジュールを他の日にコピーすることができます。

注意: 高度ボタンをクリックするとストリームタイプを選択するメニューがでますが、メインストリームで固定されています。

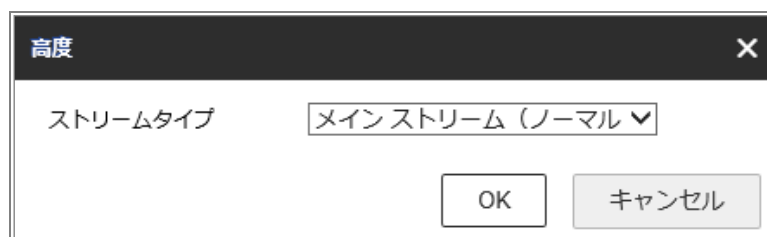


図 10-4 キャプチャスケジュールの高度設定

3. **[保存]** をクリックして設定を保存します。
4. **[キャプチャパラメータ]** タブからキャプチャパラメータを設定します。
 - (1) **[タイミング・スナップショット 有効]** チェックボックスをチェックして継続的なスナップショットを有効にします。
 - (2) フォーマット、解像度、品質および間隔を選択します。
 - (3) **[イベントトリガースナップショット有効]** チェックボックスをチェックしてイベントトリガーによるスナップショットを有効にします。
 - (4) フォーマット、解像度、画質、間隔およびキャプチャ回数(番号をキャプチャ)を選択します。

記録スケジュール **キャプチャー**

キャプチャのスケジュール > **キャプチャパラメータ**

タイミング

タイミング・スナップショット 有効

フォーマット ▼

解像度 ▼

品質 ▼

間隔 ▼

イベントトリガー

イベントトリガースナップショット有効

フォーマット ▼

解像度 ▼

品質 ▼

間隔 ▼

番号をキャプチャ

 保存

図 10-5 キャプチャパラメータ設定

5. **[保存]** をクリックして設定を保存します。

10.3 NetHDD の設定

始める前に:

録画ファイル、ログファイル、画像などを保存するには、ネットワークディスクはネットワーク内で利用可能でかつ、適切に設定されている必要があります。

方法:

1. NetHDD を追加します。
 - (1) **[環境設定]** > **[ストレージ]** > **[ストレージマネジメント]** > **[NetHDD]** から NetHDD 設定インターフェイスに入ります。

HDDマネジメント **NetHDD** メモリーカード検出

NetHDD				
HDD No.	サーバアドレス	ファイルのパス	タイプ	削除
1			NAS	✕
取り付けタイプ <input type="button" value="SMB/CIFS"/> ユーザー名 <input type="text" value="admin"/> パスワード <input type="password" value="....."/> <input type="button" value="テスト"/>				
2			NAS	✕
3			NAS	✕

図 10-6 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 サーバアドレスを入力し、ファイルパスを入力します。
- (3) 取り付けタイプを選択します。NFS および SMB/CIFS が選択できます。SMB/CIFS が選択された場合、セキュリティを確保するためにユーザー名とパスワードを設定できます。



- 個人情報とお使いのシステムのセキュリティを保持する観点から、すべての機能およびネットワークデバイスに対して強力なパスワードを使用することを強く推奨します。製品のセキュリティを高めるため、ご自分で選択した強力なパスワード (大文字、小文字、数字、特殊記号のうち、少なくとも3つのカテゴリで構成された文字を8文字以上含むパスワード) を設定するようお勧めします。
- すべてのパスワードやその他のセキュリティの適切な設定は、設置者および/またはエンドユーザーの責任です。

- (4) **[保存]** をクリックし、ネットワークディスクを追加します。
2. 追加されたネットワークディスクを初期化します。
 - (1) **[環境設定]** > **[ストレージ]** > **[ストレージマネジメント]** > **[HDD マネジメント]** から HDD 設定インターフェイスに入ると、ディスクの最大容量、フリースペース、ステータス、タイプおよびプロパティが確認できます。

HDD Management interface showing a table of HDDs and configuration options for capacity allocation.

HDD No.	容量	フリースペース	ステータス	タイプ	プロパティ	プロセス
<input type="checkbox"/>	1	59.23GB	36.25GB	通常	ローカル	R/W

ハードディスク容量配属

最高画像数: 14.50GB
 画像のための空き容量: 14.50GB
 最高録画容量: 43.75GB
 録画用空き容量: 21.75GB
 画像の比率: 25%
 録画の比率: 75%

保存

図 10-7 ストレージマネジメントインターフェイス

- (2) ディスクのステータスが [未フォーマット] の場合、対応するチェックボックスをチェックしてディスクを選択し、[フォーマット] 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ステータスは [通常] になります。

HDD Management interface showing the status of a disk as '未フォーマット' (Not Formatted).

HDD No.	容量	フリースペース	ステータス	タイプ	プロパティ	プロセス
<input checked="" type="checkbox"/>	1	1.84GB	0.00GB	未フォーマット	ローカル	R/W

保存

図 10-8 ディスクステータスの確認

3. 録画および画像の割り当て容量の比率を定義します。
- (1) 画像の比率および録画の比率割り当てパーセンテージを入力します。
- (2) [保存] をクリックしてブラウザページを更新し、設定をアクティベートします。

HDD Management interface showing the configuration for capacity allocation ratios.

ハードディスク容量配属

最高画像数: 7.00GB
 画像のための空き容量: 7.00GB
 最高録画容量: 21.25GB
 録画用空き容量: 19.75GB
 画像の比率: 5%
 録画の比率: 95%

保存

図 10-9 割り当て容量設定

注意:

最大 8 つまでの NAS ディスクをカメラに接続できます。

10.4 メモリーカード検出の設定

目的:

メモリーカード検出では、メモリーカードのステータスを見たり、メモリーカードをロックしたり、メモリーカードに異常が検出された時に通知を受け取ることができます。

注意:

メモリーカード検出機能は特定のメモリーカードでのみサポートされています。もし本設定が表示されなければ、メモリーカードが本機能をサポートしていません。この機能をサポートするメモリーカード情報については、ディーラーにお問い合わせください。

方法:

1. メモリーカード検出設定インターフェイスに入ります。: [環境設定] > [ストレージ] > [ストレージマネジメント] > [メモリーカード検出]



図 10-10 メモリーカード検出

2. [状態検知] タブにメモリーカードのステータスが表示されます。

残り寿命: 残り寿命のパーセンテージが表示されます。メモリーカードの寿命は容量やビットレートなどの要因によって影響を受ける場合があります。残り寿命が十分でない場合メモリーカードを交換する必要があります。

健全性の状態: メモリーカードの状態が表示されます。アラームスケジュールとリンケージメゾットを設定することで、通常以外の状態になった時に通知を受け取ることができます。

注意: 健全性の状態が“通常”でない時はメモリーカードを変更することを推奨します。

3. [R/W ロック] タブからメモリーカードにロックを加えることができます。

R/W ロックを加えると、メモリーカードはアンロックされた時のみ読み書きができます。



The screenshot shows the 'HDD Management' interface with the 'Memory Card Detection' tab selected. The 'RW Lock' sub-tab is active. The 'Lock Switch' is set to 'On' in a dropdown menu. Below it, there is a 'Password Setting' field with an 'Change' button. At the bottom, there is a red 'Save' button.

図 10-10 RW ロック設定

- ロックを加える
 - (1) ロック切替にオンを選択します。
 - (2) パスワードを入力します。
 - (3) [保存] をクリックして設定を保存します。
- アンロック
 - (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、自動的にアンロックが行われます。ユーザーがアンロックの手順を行う必要はありません。
 - (2) 異なるカメラでロックしたメモリーカードを使用する時、手動でメモリーカードのアンロックを行うために HDD マネジメントインターフェイスに移動することができます。メモリーカードを選択し、アンロックボタンをクリックします。正しいパスワードを入力するとアンロックされます。

注意:

- メモリーカードはアンロックされた時だけ読み書きすることができます。
 - メモリーカードにロックを加えたカメラが工場出荷状態に復元した時、メモリーカードはHDD マネジメントインターフェイスでアンロックしてください。
- ロックを取り除く
 - (1) **ロック切替にオフ**を選択します。
 - (2) **パスワード設定**に正しいパスワードを入力します。
 - (3) **[保存]** をクリックして設定を保存します。
4. アラームスケジュールとリンケージメゾットを設定すると、メモリーカードの健全性の状態が通常でない場合に通知を受け取ることができません。詳細情報については 9.1.1 節 と 9.1.3 節を参照してください。
5. **[保存]** をクリックして設定を保存します。

第11章 再生

目的:

この節ではリモートで録画され、ネットワークディスクや SD カード上に保存されたビデオファイルの閲覧方法を解説します。

方法:

1. メニューバーの再生をクリックして再生インターフェイスを開きます。



図 11-1 再生インターフェイス

2. 日付を選択して [検索] をクリックします。

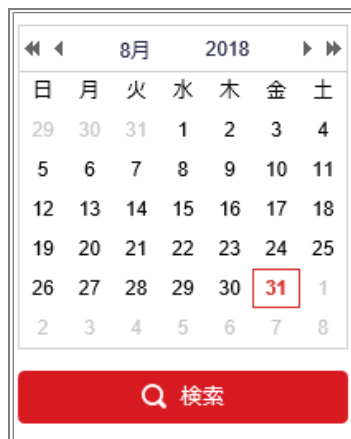


図 11-2 ビデオ検索

3. ▶ をクリックしてその日付で見つかったビデオファイルを再生します。

再生インターフェイスの下部にあるツールバーを使って再生プロセスをコントロールできます。

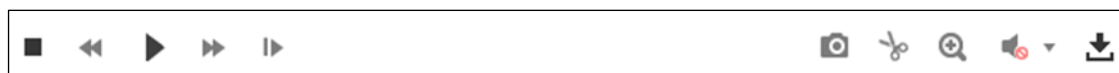


図 11-3 再生ツールバー

表 11-1 ボタンの説明

ボタン	操作	ボタン	操作
▶	再生	📷	画像のキャプチャ
⏸	一時停止	✂️/✂️	ビデオファイルのクリッピングの開始/停止
■	停止	🔍/🔍	デジタルズームの有効化/無効化
◀	スピードダウン	🔊 / 🔇	音声の ONOFF、ボリュームの調整/ミュート
▶	スピードアップ	⬇️	ダウンロード
▶▶	フレームごとの再生		

注意: ローカル設定インターフェイスから、ビデオファイルまたは画像をダウンロードして再生するためのローカルファイルパスを選択できます。

[再生時間のセット] フィールドに時間を入力して をクリックすることで、再生ポイントを位置指定できます。 をクリックするとプログレスバー上でズームイン/アウトができます。



図 11-4 再生時間のセット

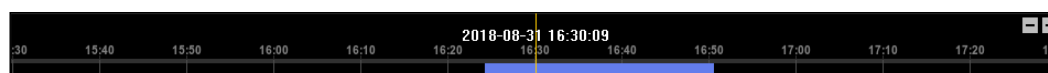


図 11-5 プログレスバー

プログレスバー上の異なる色のビデオは異なるビデオタイプを示します。

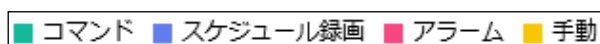


図 11-6 ビデオ種別

シャープ株式会社

ビジネスソリューション事業本部 先進設備事業部
〒581-8581 大阪府八尾市跡部本町4丁目1番33号

YKH021AUSM1904R001