



ファームウェア ユーザー マニュアル
A1D-500-V6.02.03-AC

2013/01/31



免責事項

本書の英語版が汎用の公式ドキュメントです。すべての翻訳版は便宜のために提供されているもので、他言語の翻訳に矛盾または不一致があっても、法的拘束力を伴わないものとします。

目次

免責事項	2
目次	2
推奨 PC 規格.....	4
準備	5
機器の接続.....	5
IP アドレスの構成	5
カメラへのアクセス	9
ライブ ビュー	11
ログイン	11
ライブ ビュー	12
Setup (セットアップ) :.....	15
Setup (セットアップ) ページへのアクセス.....	15
Host (ホスト)	16
Date & Time (日付と時間)	17
ネットワーク	19
IP アドレス フィルタリング.....	19

Port Mapping (ポート マッピング)	21
HTTPS	22
IEEE 802.1X	23
SNMP 設定.....	25
RTP.....	27
Network (ネットワーク) (ToS、UPnP、Bonjour、ONVIF)	28
IP Settings (IP 設定)	31
Connection Type (接続の種類)	31
DNS	33
DDNS.....	34
ビデオ.....	37
Compression (圧縮方式)	38
Motion Detection (動体検知)	40
Day/Night (デイ / ナイト)	45
画像.....	46
Exposure / White Balance (露出/ホワイト バランス)	47
OSD/Privacy Mask (OSD/プライバシー マスク)	51
On-Screen Graphics (オンスクリーン グラフ)	54
音声.....	56
イベント	57
Event Server (イベント サーバー)	57
Event Configuration (イベント構成)	60
Event List (イベント リスト)	66
Manual Event (手動イベント)	69
システム	70
User Account (ユーザー アカウント)	70
System Info (システム情報)	71
Factory Default (工場出荷時設定)	72
Firmware Upload (ファームウェアのアップロード)	73
Save & Reboot (保存して再起動)	74
Logout (ログアウト)	75

Troubleshooting (トラブルシューティング)76

推奨 PC 規格

カメラの構成やテストを行うには、以下の基本仕様を備えた PC が必要です。

CPU	Core2Duo 2.13GHz 以上
メモリ	2 GB 以上
オペレーティング システム	<ul style="list-style-type: none">● Windows XP SP2 以降● Windows 2003● Windows Vista● Windows 2008● Windows 7
ファームウェアのアクセス用ブラウザ	<ul style="list-style-type: none">● Internet Explorer 8.0 以降 (全機能)● VLC インストール済みのその他ブラウザ (一部機能)
ビデオ解像度	1024x768 以上

準備

機器の接続

ご利用の PC からカメラ ファームウェアへの接続を可能にするには、カメラと PC をイーサネット ケーブルを介して接続する必要があります。また、カメラ本体には電源が必要です。PoE カメラの場合は、カメラと PC 間で PoE インジェクタまたはスイッチを使用できます。DC 電源コネクタを備えたカメラは、電源アダプタを使って電源を入れることができます。

カメラのイーサネット ポート LED または電源 LED は、カメラの電源が正常に機能していることを示します。

IP アドレスの構成

ご利用の PC からカメラとの通信を可能にするには、カメラと PC の両方を同じネットワークセグメントに接続する必要があります。大抵の場合、両方の IP アドレスは非常に類似しており、IP アドレスの最後の番号のみが異なります。ローカル エリア ネットワークで IP アドレス管理にアクセスするには、DHCP サーバーまたは手動の 2 通りの方法があります。

DHCP サーバーを使用して IP アドレスを割り当てる

DHCP サーバーが実行中のネットワークにコンピュータとカメラを接続している場合は、IP アドレスを構成する必要は一切ありません。カメラと PC の両方が、DHCP サーバーに自動的に一意の IP アドレスを要求します。この場合、カメラはすぐに PC からアクセスできる状態になりますが、カメラの IP アドレスがまだ不明な場合があります。Web ブラウザーを使用してカメラにアクセスできるようにするには、カメラの IP アドレスを知る必要があります。

ネットワーク上のカメラを検出する最速の方法は、Windows システムに搭載されている最も簡単なネットワーク検索を使用する方法です。弊社カメラは UPnP 機能に対応しているため、「Network (ネットワーク)」アイコンを押すだけで、ローカル エリア ネットワーク上のすべてのカメラが Windows により検出されます。

以下の例では、ネットワークに接続したばかりの **D11** カメラが正常に検出されています。

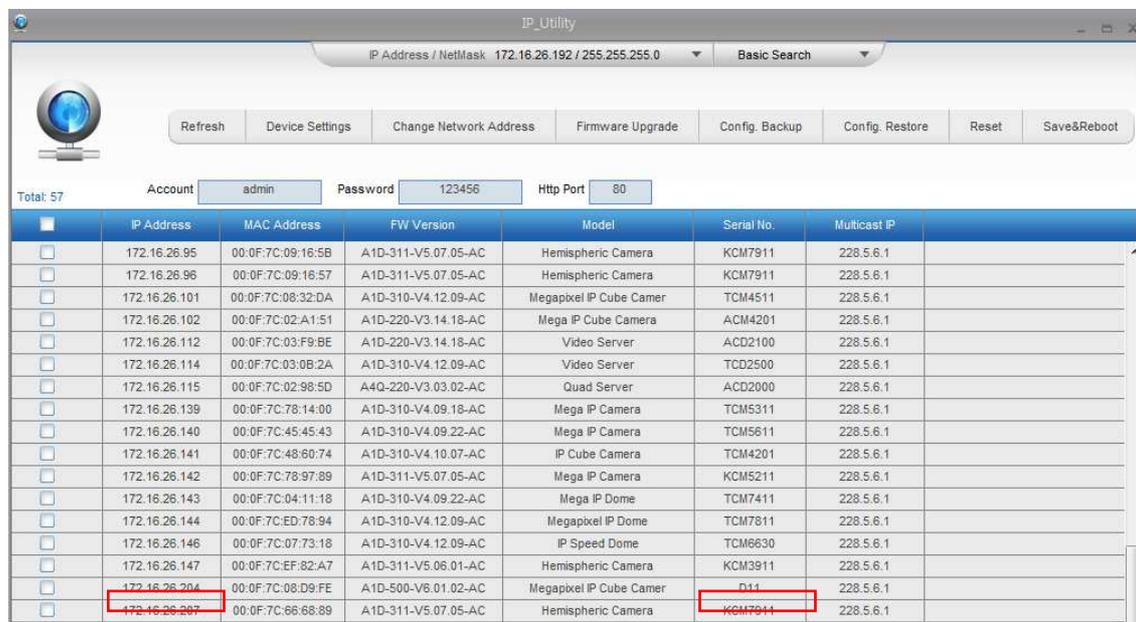


マウスの左ボタンで **D11** をクリックすると、PC の既定ブラウザが自動で起動し、ブラウザのアドレスバーにはターゲットカメラの IP アドレスが入力済みの状態で表示されます。

弊社のカメラを定期的に操作する場合は、ネットワーク上のカメラを検出するためのさらに良い方法があります。IP ユーティリティの使用です。IP ユーティリティは、カメラ検出はもちろん、IP/MAC アドレス、シリアル番号、ファームウェアバージョン等、数多くの大切な情報をリスト表示できると同時に、複数デバイスのクイック構成を可能にするライト版ソフトウェアツールです。

IP ユーティリティは、http://www.acti.com/IP_Utility から無償でダウンロードできます。

わずか 1 回のクリックで、IP ユーティリティを起動し、次のような即時レポートを得ることができます。



IP Address	MAC Address	FW Version	Model	Serial No.	Multicast IP
172.16.26.95	00:0F:7C:09:16:5B	A1D-311-V5.07.05-AC	Hemispheric Camera	KCM7911	228.5.6.1
172.16.26.96	00:0F:7C:09:16:57	A1D-311-V5.07.05-AC	Hemispheric Camera	KCM7911	228.5.6.1
172.16.26.101	00:0F:7C:08:32:DA	A1D-310-V4.12.09-AC	Megapixel IP Cube Camer	TCM4511	228.5.6.1
172.16.26.102	00:0F:7C:02:A1:51	A1D-220-V3.14.18-AC	Mega IP Cube Camera	ACM4201	228.5.6.1
172.16.26.112	00:0F:7C:03:F9:BE	A1D-220-V3.14.18-AC	Video Server	ACD2100	228.5.6.1
172.16.26.114	00:0F:7C:03:0B:2A	A1D-310-V4.12.09-AC	Video Server	TCO2500	228.5.6.1
172.16.26.115	00:0F:7C:02:98:5D	A4Q-220-V3.03.02-AC	Quad Server	ACD2000	228.5.6.1
172.16.26.139	00:0F:7C:78:14:00	A1D-310-V4.09.18-AC	Mega IP Camera	TCM5311	228.5.6.1
172.16.26.140	00:0F:7C:45:45:43	A1D-310-V4.09.22-AC	Mega IP Camera	TCM5611	228.5.6.1
172.16.26.141	00:0F:7C:48:60:74	A1D-310-V4.10.07-AC	IP Cube Camera	TCM4201	228.5.6.1
172.16.26.142	00:0F:7C:78:97:89	A1D-311-V5.07.05-AC	Mega IP Camera	KCM5211	228.5.6.1
172.16.26.143	00:0F:7C:04:11:18	A1D-310-V4.09.22-AC	Mega IP Dome	TCM7411	228.5.6.1
172.16.26.144	00:0F:7C:ED:78:94	A1D-310-V4.12.09-AC	Megapixel IP Dome	TCM7811	228.5.6.1
172.16.26.146	00:0F:7C:07:73:18	A1D-310-V4.12.09-AC	IP Speed Dome	TCM6630	228.5.6.1
172.16.26.147	00:0F:7C:EF:82:A7	A1D-311-V5.06.01-AC	Hemispheric Camera	KCM3911	228.5.6.1
172.16.26.204	00:0F:7C:08:D9:FE	A1D-500-V8.01.02-AC	Megapixel IP Cube Camer	D11	228.5.6.1
172.16.26.287	00:0F:7C:66:68:89	A1D-311-V5.07.05-AC	Hemispheric Camera	KCM7911	228.5.6.1

リストからすぐに **D11** モデルを見つけ出すことができます。IP アドレスをクリックすると、PC の既定ブラウザが自動で起動し、ブラウザのアドレスバーにはターゲットカメラの IP アドレスが入力済みの状態で表示されます。

カメラのデフォルト IP アドレスを使用する

特定のネットワークに DHCP サーバーが存在しない場合は、PC とカメラが同じネットワークセグメントに属するよう、その両方に手で IP アドレスを割り当てる必要があります。

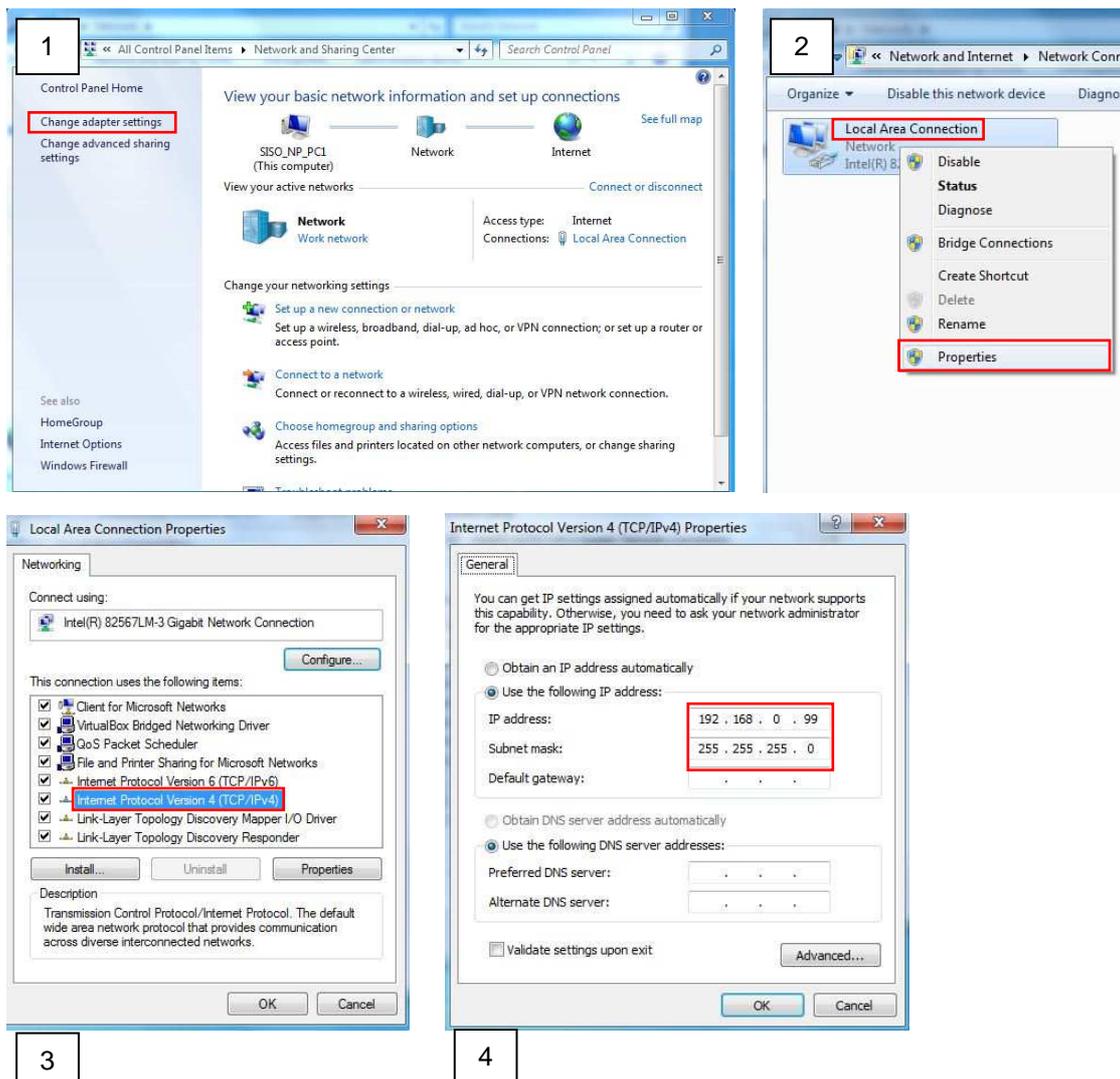
カメラをネットワークに接続した時に DHCP サーバーが検出されない場合、カメラ自体には次のデフォルト IP が自動で割り当てられます。

192.168.0.100

一方、デフォルトのポート番号は **80** です。このカメラにアクセスするには、PC の IP アドレスをカメラのネットワーク セグメントに合わせて構成する必要があります。

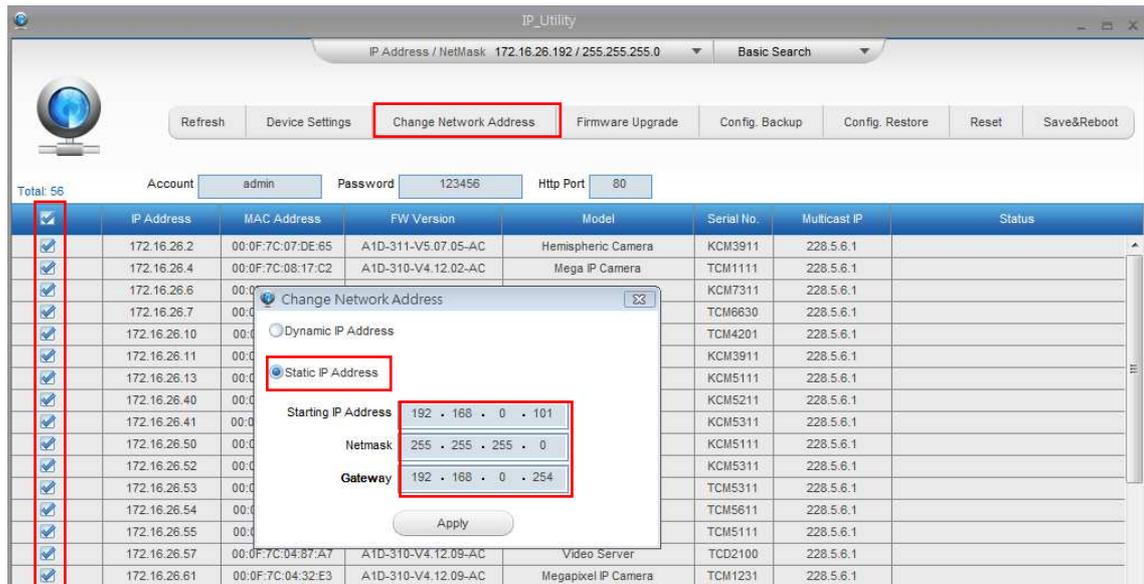
PC の IP アドレスを手動で調整する

次の Windows 7 に基づく例では、以下のステップで IP アドレスを **192.168.0.99** に構成し、Subnet Mask (サブネット マスク) を **255.255.255.0** に設定します。



複数カメラの IP アドレスを手動で調整する

同じローカル エリア ネットワークで使用するカメラが 2 台以上あり、それぞれに一意の IP アドレスを割り当てる DHCP サーバーが存在しない場合、すべてのカメラには初期値の IP アドレス **192.168.0.100** が割り当てられることとなりますが、これはネットワーク デバイスにとって不適切な状況です。つまり、すべての IP アドレスは、それぞれ異なるように設定しなければなりません。複数のカメラに IP アドレスを割り当てる最も簡単な方法は、**IP Utility** (IP ユーティリティ) の使用です。



上記の手順で、すべてのカメラに **192.168.0.101** から始まる一意の IP アドレスが割り当てられます。20 台のカメラを選択した場合、カメラの最後の IP アドレスは **192.168.0.120.20** となります。

後で IP Utility (IP ユーティリティ) の「Refresh (更新)」ボタンを押すと、新しい IP アドレスを持つカメラのリストを表示できます。



Web ブラウザーを使って IP アドレスを手動で変更することも可能です。この場合は、一度に 1 台のカメラのみを接続し、Web ブラウザーを使ってその IP アドレスを変更してから、次のカメラを接続してください。こうすれば、Web ブラウザーが同時に同じ IP アドレスを持つ 2 台のデバイスを混同することはありません。

カメラへのアクセス

これで、カメラと PC の両方が一意の IP アドレスを持ち、同じネットワーク セグメントに接続されたので、PC の Web ブラウザーを使ってカメラにアクセスすることが可能となります。

どのブラウザーでもカメラにアクセスできますが、**Microsoft Internet Explorer** のみが全機能に対応しています。

ブラウザーの機能比較：

機能	Internet Explorer	その他のブラウザー
ライブ映像	○	○*
ライブ映像エリア サイズ変更可能	○	なし
PTZ コントロール	○	○
スナップショットのキャプチャ	○	○
ビデオ オーバーレイ ベースの構成 (動体検知 エリア、プライバシー マスク エリア)	○	なし
その他すべての構成	○	○

* Internet Explorer 以外のブラウザーで、カメラからライブ ビデオ フィードを得られるようにするには、これらのブラウザーを使用する前に、まず基本の **VLC メディア プレーヤー** (<http://www.videolan.org>) を PC にインストールしておく必要があります。これは、フリーかつオープン ソースでクロスプラットフォームのマルチメディア プレーヤーです。

免責事項: VLC プレーヤーはサード パーティー (第三者) ソフトウェアであるため、カメラ・メーカーがこれを搭載したカメラの互換性を保障することはありません。また、サード パーティーは、いかなる時でもユーティリティを変更する権利を有し、これにより互換性が影響を受ける場合があります。この場合は、Internet Explorer のブラウザーを代用してください。

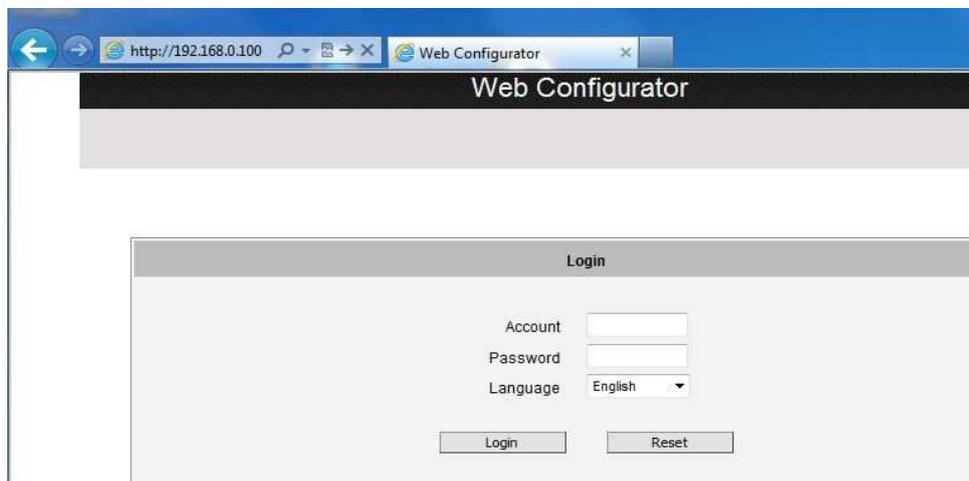
Internet Explorer のブラウザーを使用する際は、ビデオ ストリーム管理用の ActiveX コントロールをカメラから直接ダウンロードします。そのコントロールの使用承諾を促す指示が表示された時に、それに承諾するだけで操作は完了します。この場合、その他サード パーティーのユーティリティをインストールする必要はありません。

本書で紹介する以下の例は、カメラの全機能を取り扱うため、Internet Explorer ブラウザーに基づいて記載しています。

カメラの IP アドレスが **192.168.0.100** である場合、Web ブラウザーを開き、Web ブラウザーのアドレス バーに次のアドレスを入力すると、そのカメラにアクセスできるようになります。

http://192.168.0.100

カメラへの接続が完了すると、**Web Configurator (Web コンフィギュレータ)** と名付けられたユーザー インターフェイスが、ログイン ページと共に表示されます。HTTP ポート番号は IP アドレスの後に追加されていませんが、これはカメラのデフォルト HTTP ポートが、便宜上アドレスから省略可能な 80 番であるためです。



ログインの前に、工場出荷時に設定されているカメラの **Account (アカウント)** と **Password (パスワード)** を知っておく必要があります。

Account (アカウント) : Admin

Password (パスワード) : 123456

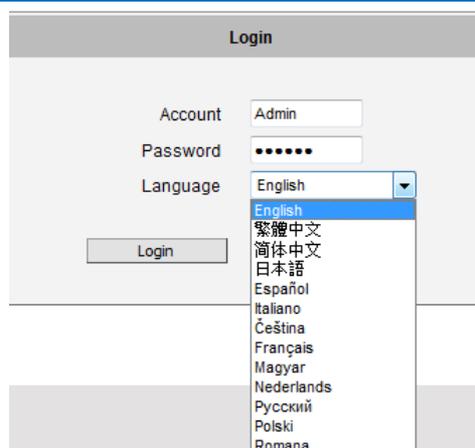
ライブ ビュー

このセクションでは、IP カメラの構成方法を説明します。管理者はすべての設定に無制限にアクセスできますが、通常ユーザーの使用はライブ映像の表示のみに限定されます。

ログイン

最初、カメラには管理者アカウント (**Account: Admin, Password: 123456**) のみが既定されているため、このアカウントを使ってログインする必要があります。必要な場合は、後で制限付きアクセス権のある標準ユーザー アカウントを作成できます。

言語リストからご利用の現地語を自由に選択するか、英語のままに設定しておきます。「Login (ログイン)」を押すと、Web Configurator (Web コンフィギュレータ) のユーザー インターフェースにアクセスできます。

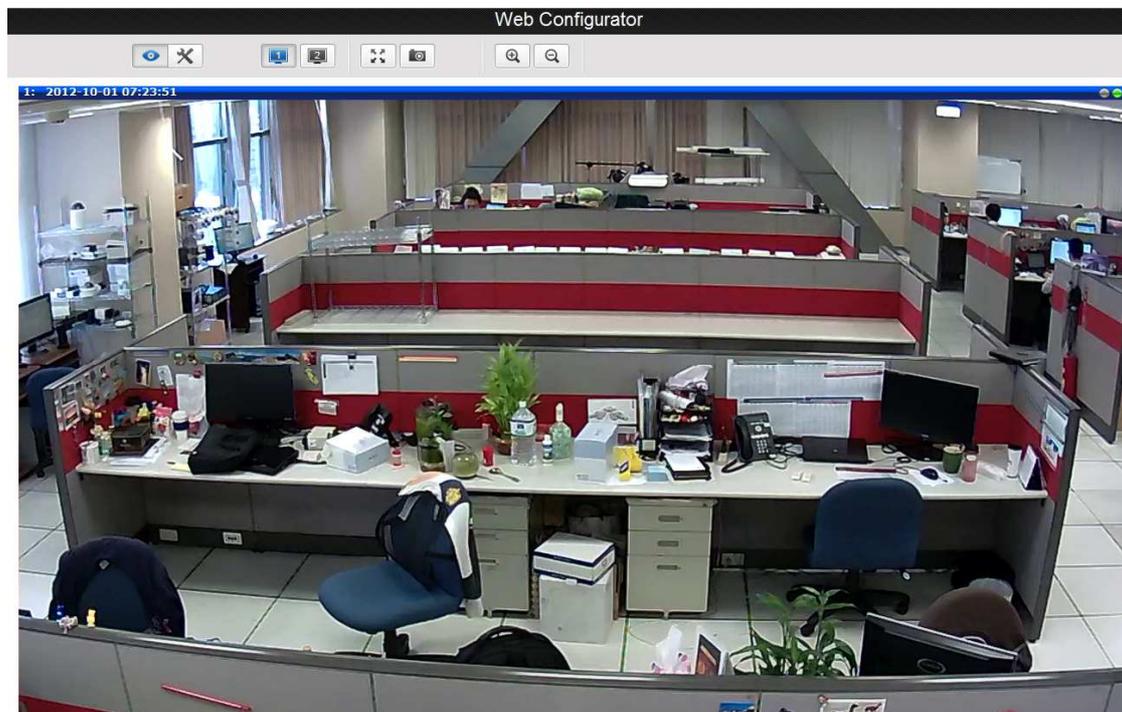


ログインを完了すると、ライブ ビュー ページが表示されます。ブラウザーが **Internet Explorer** の場合、カメラから ActiveX コントロールのインストール許可を促す指示が表示される場合があります。その場合は「Install (インストール)」を押してください。その後間もなくして、ライブ映像が表示されます。



ライブ ビュー

ライブ ビューは自動的に **1280x720** (1MP カメラ) または **1920x1080** (2-5MP カメラ) のビデオ解像度で表示されます。



ライブ ビュー ページを表示したまま、次のアイコンを押すとライブ ビュー アイコンが表示されます。 

ライブ ビュー ページを終了しても、後でこのボタンを押して戻ることができます。

PC のモニター解像度がライブ映像の解像度よりも大きい場合は、フルサイズの映像を表示できませんが、そうでない場合は、最初に映像の一部のみが表示され、スクロール バーを使って残りのビデオ エリアを表示しなければなりません。フル サイズの映像をディスプレイに表示するには、デジタル ズーム ボタンを押して一時的に映像を変更することで、画面によりうまく合わせることができます。

 - ビデオのサイズをデジタル処理で拡大する

 - ビデオのサイズをデジタル処理で縮小する

注意: これらのデジタル ズーム調整が、カメラの実際のビデオ解像度に影響を与えることはありません。デジタル ズーム ボタンを押した後、ディスプレイに表示されるビデオの大きさがどうであっても、カメラの実際のビデオ ストリーム サイズは変わりません。

また、次のアイコンを一度だけクリックすると、ビデオをデジタル処理で変更し、ディスプレイの全画面に合わせるすることができます。

 - 全画面モード

キーボードの **ESC** キーを使って全画面モードを終了することができます。

カメラは **デュアル ストリーム** 機能に対応しています。ストリーム 1 は通常、NVR に録画されるという目的を持つ高解像度のストリームですが、ストリーム 2 は NVR ライブ ビューを目的として NVR PC の計算能力を抑えるために、比較的軽いビデオ構成となっています。どちらのストリームも **Web Configurator (Web コンフィギュレータ)** の **Setup (セットアップ)** ページで構成できます。ストリームそれぞれの表示状態が確認できるように、ライブ ビュー ページにはクイック ボタンが用意されています。

 - ストリーム 1 のビデオを表示する

 - ストリーム 2 のビデオを表示する

ストリーム 2 のボタンを押すと、ライブ ビューは次のような状態に見えます。



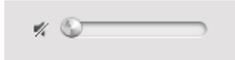
現在のライブ ビューのスナップショットをキャプチャするには、スナップショットボタンを押します。スナップショットは **Pictures (画像)** フォルダーに保存されます。

 - スナップショットを撮る

音声機能を搭載したカメラの場合、ライブ ビュー ページに音声コントロールが表示されます。

カメラのマイクやライン入力デバイスの音声を聞くには、**Web Configurator** (Web コンフィギュレータ) を実行する PC にスピーカーを接続しますが、その音量レベルを調整するには、以下の音声コントロールを使用します。

Audio Muted (音声はミュート状態) :



Audio level adjusted to the maximum (音声レベルを最大に調整) :



この音量コントロールは、**Setup** (セットアップ) ページでカメラの音声入力機能が「**Enabled** (有効)」に設定されている場合にのみ、ユーザー インターフェースに表示されます。

Setup (セットアップ) :

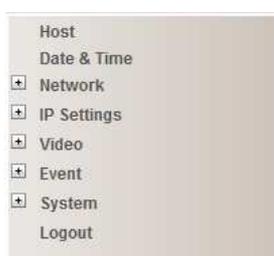
次の章では、カメラの Setup (セットアップ) 機能について説明します。

Setup (セットアップ) ページへのアクセス

カメラの設定を構成するには、ライブ ビュー ページに表示される次のボタンを押して、Setup (セットアップ) メニューに進みます。



- Go to Setup (セットアップに進む)



[Setup (セットアップ)] ページの左側には Setup 項目リストが含まれます。

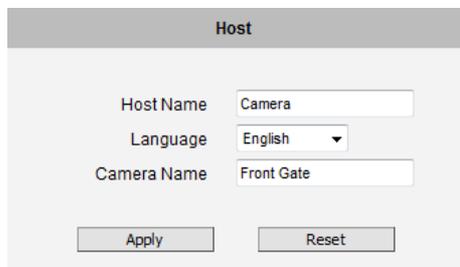
注意: メニュー リストの正確な内容は、各カメラの実際の機能によって異なりますが、本書はあらゆる機能の説明を目的として制作されています。

Setup (セットアップ) ページのいくつかの項目はグループに分けられます (例: Network (ネットワーク)、IP Settings (IP 設定) 等)。[+] ボタンを押すと、グループを展開してサブ項目を表示できます。

本書の次の章では、各 Setup (セットアップ) 項目を個別に説明します。各章は Setup (セットアップ) メニュー項目のリストと同じ順序で記載されています。

Host (ホスト)

Host 「Host (ホスト)」のセクションでは、管理者がカメラ名と好みのユーザー インターフェース言語を定義できます。



名前には **Host Name (ホスト名)** と **Camera Name (カメラ名)** の 2 種類があります。

Host Name (ホスト名) は、DHCP サーバーによるカメラの識別に使用されます。非常に厳格なセキュリティ ポリシーが設けられた一部のネットワークでは、すべてのネットワーク デバイスにホスト名が求められます。デバイスが、DHCP サーバーに IP アドレスを要求してネットワークへアクセスしようとする、DHCP サーバーはそのホスト名が許可されたデバイス内にあるかどうかを確認します。このページで **Host Name (ホスト名)** の編集を行うことができます。実際にカメラから送信される DHCP ディスカバリ パケットにホスト名を追加するには、**IP Settings (IP 設定)** に進み、デバイスが **Dynamic IP Address (動的 IP アドレス)** モードになっていること、また「**Use host name (ホスト名の使用)**」にチェックが入っていることを確認してください。

Camera Name (カメラ名) は、**ビデオ管理システム**または**ソフトウェア ツール**によるデバイスの識別に使用されます。通常、カメラを設置すると、「正門」や「エレベーター 1」といった実際の設置場所が、覚えやすいカメラ名として使用されます。多くの場合、VMS では **Web Configurator (Web コンフィギュレータ)** へのアクセス不要で、そのユーザー インターフェースから直接 **Camera Name (カメラ名)** を変更できます。

Host (ホスト) の下に表示される **Language (言語)** 選択の目的は、**Web Configurator (Web コンフィギュレータ)** のログイン ページに表示されるものと同じです。

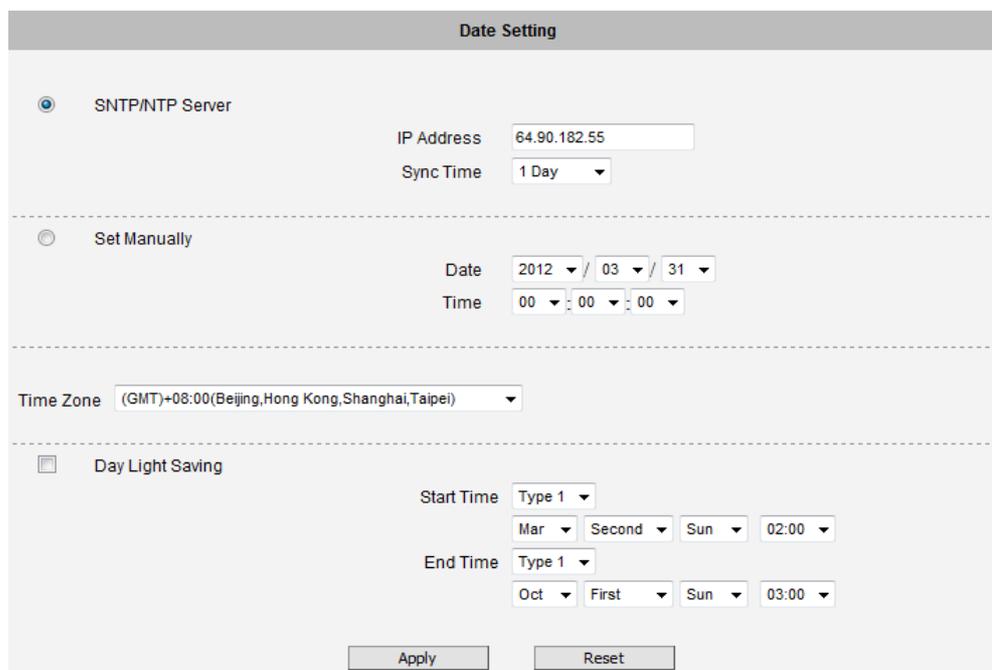
上記項目を変更してから、**Apply (適用)** を押して変更を保存します。**Reset (リセット)** ボタンは、今しがた変更が行われ、まだ適用されていない更新内容を元に戻します。

Date & Time（日付と時間）

各ビデオ フレームにはタイム スタンプが含まれます。タイム スタンプの精度は、事故調査員にとっては大変重要です。そのため、カメラの時計は可能な限り最も正確に合わせておく必要があります。

Date & Time **Date & Time（日付と時間）** セクションでは、カメラの日付と時間を調整するためのオプションが用意されています。

日付と時間の調整には 2 通りの方法があります。**automatically（自動）**により世界中の **NTP サーバー**から定期的に日付と時間を取得する方法、または **manually（手動）**により適切なタイムゾーン、日付、時間を選択する方法です。自動による方法は、カメラが **NTP サーバー**にアクセス可能な場合にのみ使用できます。インターネット アクセスのない、分離されたローカル エリアネットワークを使用している場合は、手動の日付・時間調整モードのみを使用できます。



日付と時間の自動更新のため **SNTP/NTP サーバー**を選択すると、NTP サーバーの IP アドレスと自動時刻同期の時間間隔を入力できるようになります。代わりに NTP サーバーのドメイン名を入力する場合は、DNS サーバーの IP アドレスが **IP Settings（IP 設定）**のセクションで設定されていることを確認してください。設定されていない場合、カメラは NTP サーバーのドメイン名を解決できません。

すべてのカメラで、同じ NTP サーバーから日付と時間を取得すれば、異なるカメラのビデオ クリップを確実に同期化して、後日の比較に役立てることができます。

日付と時間の同期に最適な NTP サーバーを選択するには、NTP サーバーの世界のプール：<http://www.pool.ntp.org/en/> を参照してください。

Set Manually (手動設定) モードを選択すると、選択ボックスで日付と時間を調整できます。適切な **Time Zone (タイムゾーン)** も選択ボックスから選択します。ご自身の居住地がここに表示されていない場合は、GMT が居住地と同じ地域を一覧から選択します。

サマータイム制度を導入している国に合わせて、2 種類の **Day Light Saving (サマータイム)** 機能を用意しています。

Type 1 (タイプ 1) – サマータイム期間の開始時間と終了時間を月の週数 (第 1 週、第 2 週、第 3 週、最終週) によって定義します。

Type 2 (タイプ 2) – サマータイム期間の開始時間と終了時間を月の正確な日付 (1~31) によって定義します。

Type 1 (タイプ 1) と **Type 2 (タイプ 2)** のどちらを選択するかについては、所定国のサマータイム制度を参照してください。

上記項目を変更してから、**Apply (適用)** を押して変更を保存します。**Reset (リセット)** ボタンは、今しがた変更が行われ、まだ適用されていない更新内容を元に戻します。

ネットワーク

Network (ネットワーク) セクションでは、ネットワーク関連の機能とサービスのリストが提供されます。**Network** (ネットワーク) の前に表示される **[+]** マークは、これをクリックすることによりリストを展開できることを示しています。リストを展開後に **[-]** マークをクリックすると、もう一度リストを閉じることができます。

IP アドレス フィルタリング

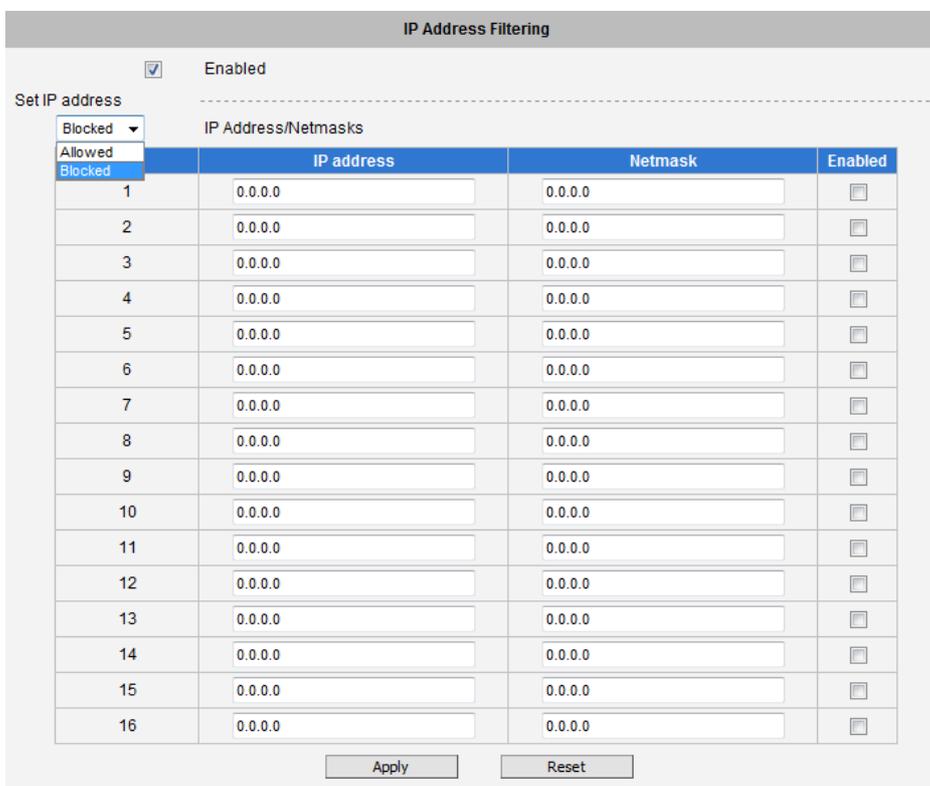
IP Address Filtering (IP アドレス フィルタリング) 機能を使って、このカメラへの接続を許可するデバイス (その IP アドレス) やこのカメラへの接続を禁止するデバイスを定義できます。

IP アドレス フィルタリング機能を起動するには、「**Enabled (有効)**」ボックスにチェックを入れて **Apply (適用)** を押します。



The screenshot shows a control panel titled "IP Address Filtering". It features a checkbox labeled "Enabled" which is currently unchecked. Below the checkbox are two buttons: "Apply" and "Reset".

ここで「**Allowed (許可)**」または「**Blocked (ブロック)**」リストのいずれかを選択して項目を追加し、各行の後方にあるチェックボックスを使って有効にできます。



The screenshot shows the configuration interface for IP Address Filtering. At the top, the "Enabled" checkbox is checked. Below it, a dropdown menu is set to "Blocked". The main area contains a table with 16 rows, each representing a filter rule. Each row has input fields for "IP address" and "Netmask", and a checkbox in the "Enabled" column. All input fields currently contain "0.0.0.0".

	IP address	Netmask	Enabled
1	0.0.0.0	0.0.0.0	<input type="checkbox"/>
2	0.0.0.0	0.0.0.0	<input type="checkbox"/>
3	0.0.0.0	0.0.0.0	<input type="checkbox"/>
4	0.0.0.0	0.0.0.0	<input type="checkbox"/>
5	0.0.0.0	0.0.0.0	<input type="checkbox"/>
6	0.0.0.0	0.0.0.0	<input type="checkbox"/>
7	0.0.0.0	0.0.0.0	<input type="checkbox"/>
8	0.0.0.0	0.0.0.0	<input type="checkbox"/>
9	0.0.0.0	0.0.0.0	<input type="checkbox"/>
10	0.0.0.0	0.0.0.0	<input type="checkbox"/>
11	0.0.0.0	0.0.0.0	<input type="checkbox"/>
12	0.0.0.0	0.0.0.0	<input type="checkbox"/>
13	0.0.0.0	0.0.0.0	<input type="checkbox"/>
14	0.0.0.0	0.0.0.0	<input type="checkbox"/>
15	0.0.0.0	0.0.0.0	<input type="checkbox"/>
16	0.0.0.0	0.0.0.0	<input type="checkbox"/>

At the bottom of the table are "Apply" and "Reset" buttons.

「**Allowed (許可)**」モードは、以下の記載を除くすべての IP アドレスへのアクセスを拒否します。

「**Blocked (ブロック)**」モードは、以下に記載される IP アドレスを除くすべての着信アクセスを受信します。

ネットマスク (サブネット マスク) を使用すれば、全範囲の IP アドレスを一度にフィルタリングするよう設定でき、全 IP アドレスの個別入力は不要となります。ネットマスクの機能がよく分からない場合は、255.255.255.255 を使用してください。各エントリの 1 つの IP アドレスにのみ影響します。また、255.255.255.0 を使用すると、3 つの同じ数字で始まるすべての IP アドレスに、同じ設定が適用されます。

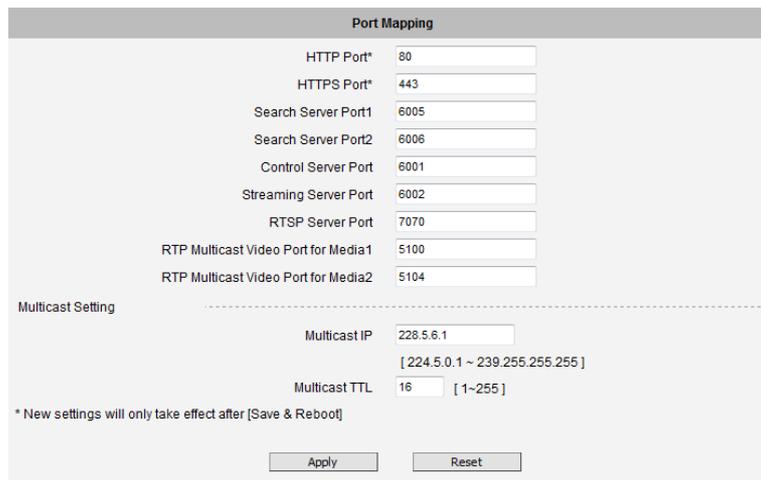
上記項目を変更してから、**Apply (適用)** を押して変更を保存します。**Reset (リセット)** ボタンは、今しがた変更が行われ、まだ適用されていない更新内容を元に戻します。

警告! 誤って接続中の IP アドレスをブロックしないようご注意ください。ブロックしてしまうと、それ以上カメラにアクセスして変更を戻すことが不可能となります。万一手違いでブロックした場合は、ハードウェアのリセットを実行できますが、フィルタリング ルールはすべて消去されます。

Port Mapping (ポート マッピング)

Port Mapping

Port Mapping (ポート マッピング) セクションでは、通信用として固有のポート番号が求められるサービスやプロトコルのリストが提供されます。デフォルトでは、カメラのポートはすべて定義済みとなっています。ポート番号の変更が特に必要な場合には、このページでその変更を行うことができます。ほとんどの場合、ローカル エリア ネットワークとインターネット間のブリッジとして機能するルーターの、覚えやすいポート フォワーディング ルールに合わせて、HTTP ポートは 80 以外の番号に変更されます。



The screenshot shows the 'Port Mapping' configuration page. It includes the following settings:

- HTTP Port*: 80
- HTTPS Port*: 443
- Search Server Port1: 6005
- Search Server Port2: 6006
- Control Server Port: 6001
- Streaming Server Port: 6002
- RTSP Server Port: 7070
- RTP Multicast Video Port for Media1: 5100
- RTP Multicast Video Port for Media2: 5104

Below the port settings is the 'Multicast Setting' section:

- Multicast IP: 228.5.6.1 (Range: [224.5.0.1 ~ 239.255.255.255])
- Multicast TTL: 16 (Range: [1~255])

At the bottom, there are 'Apply' and 'Reset' buttons. A note states: '* New settings will only take effect after [Save & Reboot]'.

パラメータ	説明
HTTP port (HTTP ポート)	HTTP プロトコルのアクセスに割り当てるポートを選択する
Search server port1 (サーバー検出ポート 1)	サーバー検出アプリケーションが、この IP デバイスを検出するために使用する第 1 ポートを選択する。(例: IP ユーティリティ)
Search server port2 (サーバー検出ポート 2)	サーバー検出アプリケーションが、この IP デバイスを検出するために使用する第 2 ポートを選択する。(例: IP ユーティリティ)
Control Server Port (コントロール サーバー ポート)	アプリケーション プログラムがビデオ コントロール機能に対応するために使用するポートを選択する。(例: NVR)
Streaming Server Port (ストリーミング サーバー ポート)	この IP デバイスがビデオ ストリーミング (TCP) に使用するポートを選択する
RTSP Server Port (RTSP サーバー ポート)	RTSP プロトコルのアクセスに割り当てるポートを選択する
RTP Multicast Video Port for Media1 (メディア 1 用 RTP マルチキャスト ビデオ ポート)	RTP プロトコル経由でストリーム 1 のマルチキャスト ビデオ ストリーミングを行うためのポートを選択する
RTP Multicast Video Port for Media2 (メディア 2 用 RTP マルチキャスト ビデオ ポート)	RTP プロトコル経由でストリーム 2 のマルチキャスト ビデオ ストリーミングを行うためのポートを選択する
Multicast IP (マルチキャスト TTL)	マルチキャスト IP を選択します。デフォルト設定は 228.5.6.1 です。
Multicast TTL (マルチキャスト TTL)	マルチキャスト TTL を選択します。デフォルト設定は 255 です。

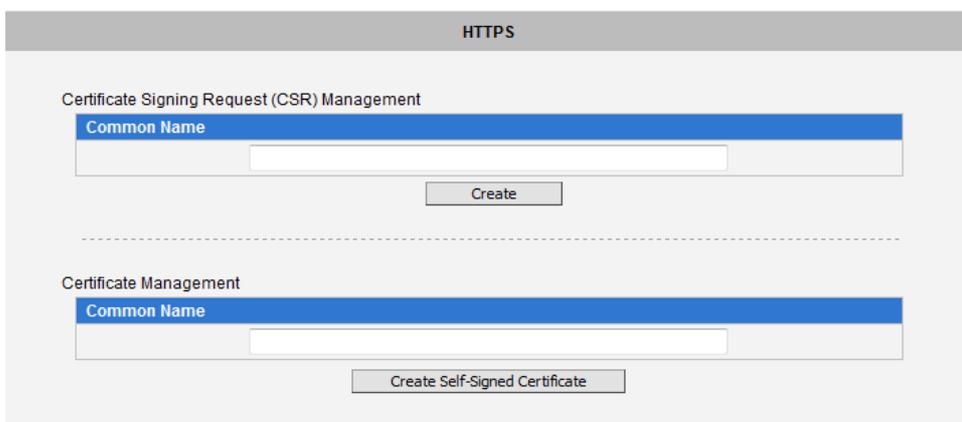
上記項目を変更してから、**Apply (適用)** を押して変更を保存します。**Reset (リセット)** ボタンは、今しがた変更が行われ、まだ適用されていない更新内容を元に戻します。新しいポート設定は、**System (システム) -> Save & Reboot (保存して再起動)** を押して初めて有効となります。

HTTPS

HTTPS

HTTPS プロトコルでは、カメラとその対照物間で送信されるデータを保護するため、安全でないネットワーク上に安全なチャンネルを作成することができます。安全な通信を確保するには 2 つの事項、すなわち暗号化されたデータと検証済みの通信対照物が必要です。メッセージが正当な対照物から送受信されたものかどうかを確認するには、認証が必要となります。

認証の作成には 2 通りの方法があります。**Certificate Signing Request (CSR、証明書署名要求)** および **Self-Signed Certificate (自己署名証明書)** です。



The screenshot shows a web interface for HTTPS configuration. It is divided into two main sections: "Certificate Signing Request (CSR) Management" and "Certificate Management". Both sections have a "Common Name" input field and a "Create" button. The "Certificate Management" section also has a "Create Self-Signed Certificate" button.

Certificate Signing Request (CSR、証明書署名要求)：ユーザーは信頼できる Certification Authority (CA、認証局) により発行される署名済み証明書を使用します。

Self-Signed Certificate (自己署名証明書)：ユーザーが自分で作成し発行した証明書を使用する場合に適用します。

「Create (作成)」または「Create Self-Signed Certificate (自己署名証明書)」ボタンを押し、ポップアップ画面で設定を構成して証明書をインストールします。

新しい設定は、「Save & Reboot (保存して再起動)」後に初めて有効となることにご注意ください。

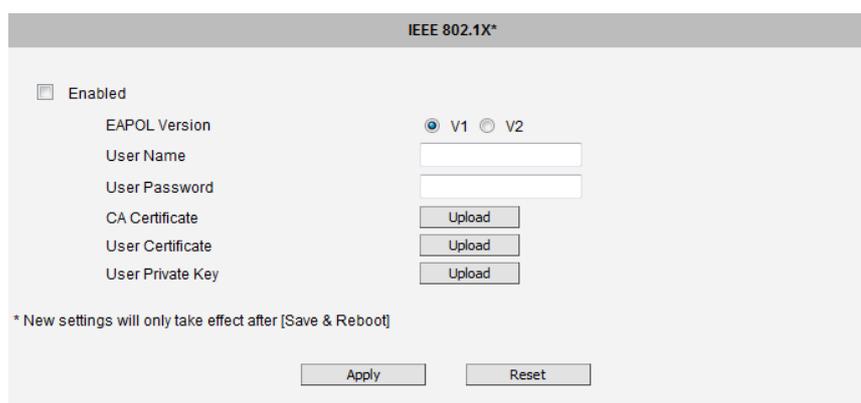
IEEE 802.1X

IEEE 802.1X は、ポートベースのネットワーク アクセス制御に対応する IEEE 規格です。802.1X 認証は、サブリカント、オーセンティケータ、認証サーバーの 3 要素で構成されています。

サブリカントは、LAN/WLAN にアクセスするクライアント デバイス (例 : IP カメラ) です。オーセンティケータは、イーサネット スイッチやワイヤレス アクセス ポイントといったネットワーク デバイスであり、認証サーバーは通常、RADIUS と EAP プロトコル対応のソフトウェアを実行するホストです。

オーセンティケータは、保護されたネットワークに対し警備員のような役割を果たします。サブリカント (例 : クライアント デバイス) は、その ID が検証され承認されるまで、オーセンティケータを介してネットワークの被保護側にアクセスすることを禁じられます。例えて言うなら、空港で有効なパスポートを提示して初めてターミナルへのセキュリティ通過が許可されるようなものです。802.1X ポートベース認証を使って、サブリカントはユーザー名/パスワードやデジタル証明書などの資格情報をオーセンティケータに提供し、オーセンティケータは検証のため、その資格情報を認証サーバーに転送します。認証サーバーによってその資格情報が有効であると判定されると、サブリカント (クライアント デバイス) は、ネットワークの被保護側にあるリソースにアクセスすることを許可されます。

IEEE 802.1x を有効にして、下の画面で設定を構成してください。新しい設定は、「Save & Reboot (保存して再起動)」後に初めて有効となることにご注意ください。



EAPOL Version (EAPOL バージョン) V1 と V2 は 802.1X の通信タイプです。 **User name (ユーザー名)** と **User password (ユーザー パスワード)** は、ユーザーによって作成され、RADIUS サーバーで設定されます。 **Certificates (証明書)** と **Private Key (秘密キー)** は RADIUS サーバーにより提供されます。

証明書や秘密キーがすでに存在する場合は、必要に応じてこれらの項目を削除できるように、その後方に「**Remove (削除)**」ボタンが表示されます。

上記項目を変更してから、**Apply (適用)** を押して変更を保存します。**Reset (リセット)** ボタンは、今しがた変更が行われ、まだ適用されていない更新内容を元に戻します。

SNMP 設定

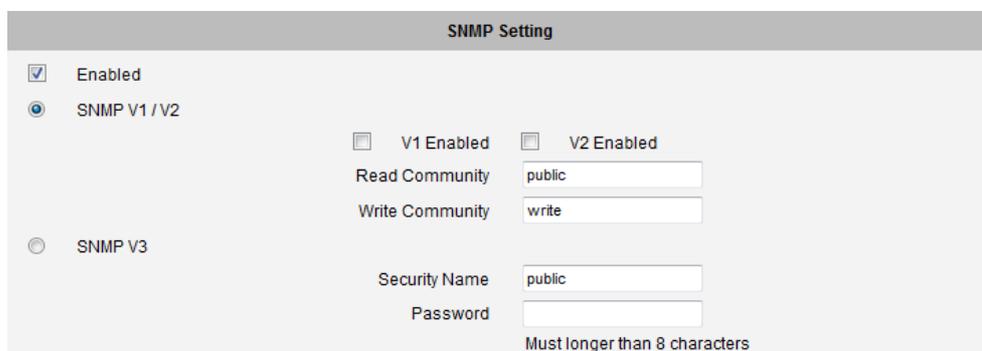
SNMP Setting

SNMP Setting (SNMP 設定) 項目は **SNMP** 構成ページを表示します。

SNMP はネットワーク デバイスの簡単な管理方法を提供します。主な機能は次の通りです。

1. デバイス稼働時間の監視
2. システムの詳細説明。(例：モデル名、モデルの説明、ファームウェアのバージョン。)
3. インターフェース情報の収集。(例：MAC アドレス、インターフェースの速度、ローカル ポート。)
4. ネットワーク インターフェースのスループット測定。

SNMP を使用するには、カメラ (SNMP エージェント) の **SNMP** 機能を有効にし、サーバー (NMS: ネットワーク管理ステーション) の **SNMP** 管理ソフトウェアを実行してデバイスに接続するだけで完了です。



SNMP エージェントは、V1、V2、V3 のバージョンに対応しています。SNMP V1 は、SNMP の初期の実装です。SNMP V2 は、サーバーやデバイスの通信、データ送受信の確認等、管理の性能を向上するために提案されたものです。SNMP V3 の主な追加内容は、セキュリティおよびリモート構成の強化に関わっています。

SNMP V1/V2 では、ID を認証するためのパスワードとして、「Community (コミュニティ)」名を使用します。「Read Community (読み取りコミュニティ)」は、サーバーがデバイスから情報を入手するためのパスワードです。「Write Community (書き込みコミュニティ)」は、サーバーがデバイスで値を編集するためのパスワードです。デフォルトでは、Read Community (読み取りコミュニティ) に「public」、Write Community (書き込みコミュニティ) に「write」が設定されていますが、読み取り/書き込みコミュニティに他のパスワードを設定することも可能です。

V1、V2 またはその両方を有効にできます。セットアップを完了後に「**Apply (適用)**」をクリックします。

SNMP V3 のセキュリティ メソッドでは、認証にアカウント/パスワードを使用します。「Security Name (セキュリティ名)」は、「Password (パスワード)」と併せて使用するアカウント名です。既定のセキュリティ名は「public」で、パスワードは 8 文字以上を設定します。他のセキュリティ名やパスワードを設定することも可能です。セットアップを完了後に「**Apply (適用)**」をクリックします。

これで、SNMP 機能は有効になりました。SNMP 管理ソフトウェアをコンピュータ サーバーにインストールして実行できます。

SNMP トラップの使用方法：

Trap Enabled

Destination IP address

Trap Community

Available Traps
 Cold Start
 Warm Start
 Authentication Failure

SNMP トラップは、デバイスからの通知を有効にします。コールド スタートやウォーム スタート、認証エラー等の重大なイベントが発生した時はすぐに、デバイスから管理サーバーへメッセージが送信されます。管理者は即時に情報を入手し、必要な場合には措置を講じます。

Cold start (コールド スタート) とは、デバイスが電源切断によって再起動することを意味します。**Warm start (ウォーム スタート)** とは、デバイスが電源切断がない状態でファームウェアにより再起動することを意味します。SNMP V1、V2、または V3 を設定した状態で、他パーティーが間違ったセキュリティ パスワードを使ってデバイスに接続しようとする、デバイスから管理サーバー宛てに **authentication failure (認証エラー)** メッセージが送信されます。

カメラの SNMP トラップ機能を有効にするには、SNMP 管理ソフトウェアを実行するコンピュータの IP アドレスを入力し、パスワードとしてトラップ コミュニティを入力すると、サーバーがデバイスからトラップ メッセージを受信できるようになります (既定は public)。使用可能なトラップを選択して「**Apply (適用)**」をクリックします。

カメラの SNMP では以下の情報が提供されます。

グループ	説明
システム	被管理デバイスに関する一般情報を提供します。 例：システム説明、システム名。
インターフェース	物理インターフェースからの一般情報を提供します。 例：インターフェースの速度、MAC アドレス。
アドレス変換	各物理インターフェースのネットワーク アドレスと物理アドレス間のマッピングに関する情報を提供します。 例：被管理デバイスに接続するための IP/MAC アドレス。
IP	ネットワーク層 (レイヤ 3) の状態とオペレーションを提供します。 例：受信/送信パッケージの情報とトラフィック フロー。
ICMP	ICMP の状態と統計情報を提供します。 例：ICMP の受信/エラー メッセージの量。
TCP	TCP プロトコルを使用してトランスポート層 (レイヤ 4) の状態とオペレーションを提供します。 例：Ex: TCP ローカル ポート、着信/発信 TCP セグメント
UDP	UDP プロトコルを使用してトランスポート層 (レイヤ 4) の状態とオペレーションを提供します。 例：UDP ローカル ポート、イン/アウト データグラム。
SNMP	SNMP 経由で関連の統計情報を提供します

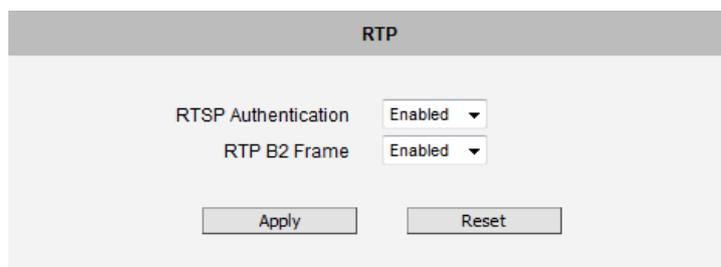
RTP

RTP

RTP セクションでは、RTP 設定を構成できます。

RTSP Authentication (RTSP 認証) が「**Enabled (有効)**」の場合、RTP ストリーミングにはアカウント名とパスワードの認証が必要になります。

RTP B2 Frame (RTP B2 フレーム) が「**Enabled (有効)**」の場合は、追加情報（例：各フレームの動態検知状態、デジタル入力/デジタル出力レベル、パッシブ赤外線状態、他のビデオ インテリジェンス データ、フレーム カウンタ、フレームレート モードとフレームレート、ビットレート、解像度、タイムスタンプ、他多数）を含む B2 フレームが、各ビデオ フレームに追加されます。イベント管理、ストレージ消費量の予測、プレビュー用画像サイズ変更等を含むビデオ データの操作は、ユーザー側で容易に行えます。



RTP

RTSP Authentication Enabled

RTP B2 Frame Enabled

Apply Reset

上記項目を変更してから、**Apply (適用)** を押して変更を保存します。**Reset (リセット)** ボタンは、今しがた変更が行われ、まだ適用されていない更新内容を元に戻します。

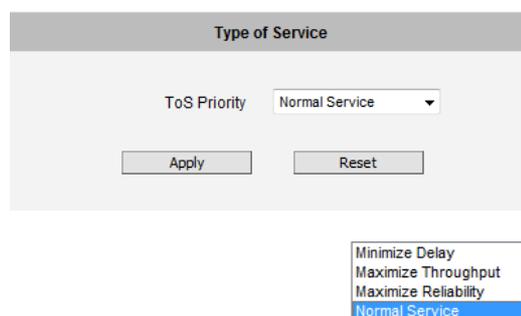
Network (ネットワーク) (ToS、UPnP、Bonjour、ONVIF)

Network Network (ネットワーク) のセクションには次の機能のコントロールが含まれます。

- Type of Service (サービス タイプ)
- UPnP
- Bonjour
- ONVIF

Type of Service (サービス タイプ)

「Type of Service (サービス タイプ)」では、ToS 概念対応のルーターがカメラ データを処理する方法について、その優先順位を定義する 4 つのオプションが提供されます。デフォルトの ToS 優先順位は「Normal Service (標準サービス)」に設定されています。



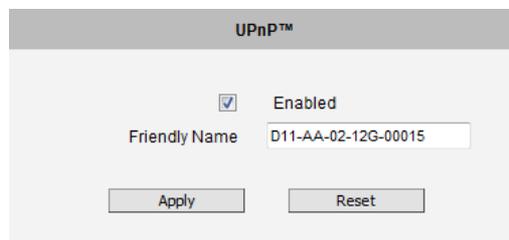
特別な優先順位の並べ替えができるよう、他に 3 つのオプションが用意されています。

- Minimize Delay (遅延最小化)
- Maximize Throughput (スループット最大化)
- Maximize Reliability (信頼性最大化)

上記項目を変更してから、**Apply (適用)** を押して変更を保存します。**Reset (リセット)** ボタンは、今しがた変更が行われ、まだ適用されていない更新内容を元に戻します。

UPnP™

UPnP™ セクションでは、カメラのユニバーサル プラグ アンド プレイ機能を有効または無効にするオプションが提供されます。UPnP™ を有効にすると、ネットワーク上のデバイスが他のネットワーク デバイスに継続的に検出されるようになり、識別やアクセスに便利です。



Friendly Name (フレンドリ名) は、カメラの検出時に表示されるデバイスのヒューマンリーダブルな (人が読み取れる) 名前です。デフォルト設定では、カメラのシリアル番号がフレンドリ名として使用されますが、プロジェクトの必要に応じて名前を変更できます。

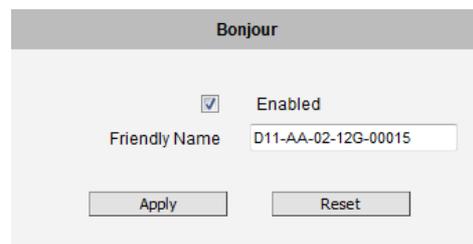
上記項目を変更してから、**Apply (適用)** を押して変更を保存します。**Reset (リセット)** ボタンは、今しがた変更が行われ、まだ適用されていない更新内容を元に戻します。

Windows ベース コンピュータの大半は、UPnP™ 対応デバイスの検出機能を備えています。以下は Windows 7 の例です。**Windows 7** の **Network (ネットワーク)** アイコンをクリックすると、PC ではカメラが直ちに検出されます。



Bonjour

Bonjour セクションでは、アップル社が開発した Bonjour プロトコルを使用し、他のネットワーク デバイスがカメラを検出できるようにする機能を、有効または無効にするオプションが提供されます。**Bonjour** と **UPnP** はどちらも、デバイスを効果的に検出するという同じ目的を果たします。



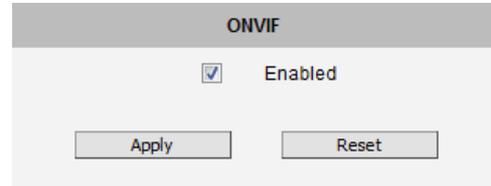
UPnP と同様、ヒューマンリーダブルな **Friendly Name (フレンドリ名)** は、ユーザーによる定義が可能です。カメラがネットワークで検出されると、その名前が表示されます。デフォルトのフレンドリ名はカメラのシリアル番号で設定されていますが、プロジェクトの必要に応じて名前を変更できます。

上記項目を変更してから、**Apply (適用)** を押して変更を保存します。**Reset (リセット)** ボタンは、今しがた変更が行われ、まだ適用されていない更新内容を元に戻します。

ONVIF

既定のファームウェアを搭載した本カメラは、ONVIF 2.2 に対応しています。デフォルトでは、ONVIF 機能は無効に設定されています。

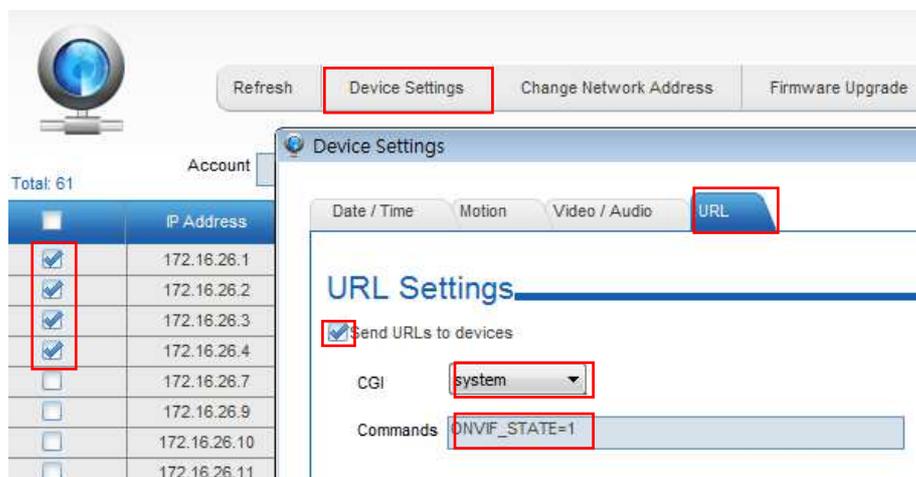
ONVIF 対応を有効にするには、ボックスにチェックを入れて **Apply (適応)** を押します。



ONVIF

Enabled

便宜上、複数のカメラで ONVIF を有効にする必要がある場合は、IP ユーティリティを代用し、**system cgi and ONVIF_STATE=1** を URL コマンドとして使用します。



Refresh **Device Settings** Change Network Address Firmware Upgrade

Total: 61 Account

	IP Address
<input checked="" type="checkbox"/>	172.16.26.1
<input checked="" type="checkbox"/>	172.16.26.2
<input checked="" type="checkbox"/>	172.16.26.3
<input checked="" type="checkbox"/>	172.16.26.4
<input type="checkbox"/>	172.16.26.7
<input type="checkbox"/>	172.16.26.9
<input type="checkbox"/>	172.16.26.10
<input type="checkbox"/>	172.16.26.11

Device Settings

Date / Time Motion Video / Audio **URL**

URL Settings

Send URLs to devices

CGI: **system**

Commands: **ONVIF_STATE=1**

IP Settings (IP 設定)

IP Settings

IP Settings (IP 設定) セクションでは、カメラによる IP アドレス

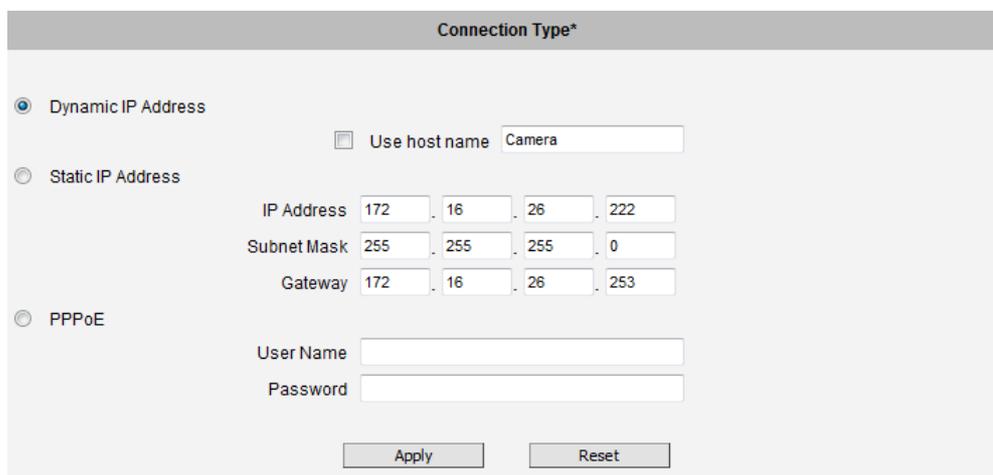
の取得方法と、カメラが接続する DNS サーバーの指定について定義するオプションが提供され、これによりドメイン名を解決します。

Connection Type (接続の種類)

Connection Type

Connection Type (接続の種類) のサブセクションでは、カメラ

の IP アドレスを取得する方法を定義できます。デフォルトでは、カメラは **Dynamic IP Address (動的 IP アドレス)** モードに設定されており、DHCP サーバーから IP アドレスの取得を試行します。この試行が数秒経過して失敗すると（例えば、DHCP サーバーが存在しない場合など）、カメラは **Static IP Address (静的 IP アドレス)** の下に表示されている IP アドレスを自動的に割り当てます。



Host Name (ホスト名) は、DHCP サーバーによるカメラの識別に使用されます。非常に厳格なセキュリティ ポリシーが設けられた一部のネットワークでは、すべてのネットワーク デバイスにホスト名が求められます。デバイスがネットワークへのアクセスを試行し、DHCP サーバーに IP アドレスを要求すると、DHCP サーバーはそのホスト名が許可されたデバイス内にあるかどうかを確認します。このページで **Host Name (ホスト名)** を編集し、ホスト名の有効/無効を設定できます。

大抵の設置プロジェクトには、各カメラ用のクリアなネットワーク トポロジと静的 IP アドレスが含まれています。この場合、カメラを **Static IP Address (静的 IP アドレス)** モードに変更し、**IP Address (IP アドレス)**、**Subnet Mask (サブネット マスク)** および **Gateway (ゲートウェイ)** を修正することができます。

まれに、カメラがインターネット経由でコントロール センターに接続される場合があります。通常、最も費用効果の高い方法は、**PPPoE** による **ADSL** 接続を使用することです。カメラの再起動時にインターネット サービス プロバイダーが不意に **IP** アドレスを変更してしまわないよう、その事態に備えて **DDNS** サービスを有効にし、代わりにコントロール センターがカメラにドメイン名で接続できるように設定しておくことをお勧めします。詳細は、**DDNS** セクションを参照してください。

カメラを **PPPoE** モードに設定するには、ラジオ ボタンを **PPPoE** に合わせ、インターネット サービス プロバイダーから提供される **User Name** (ユーザー名) と **Password** (パスワード) を入力します。

上記項目を変更してから、**Apply (適用)** を押して変更を保存します。**Reset** (リセット) ボタンは、今しがた変更が行われ、まだ適用されていない更新内容を元に戻します。

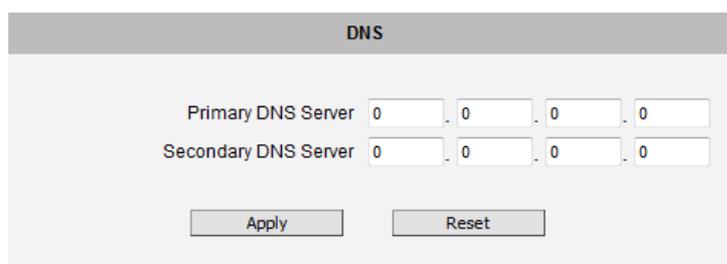
新しい **IP** アドレス設定は **System (システム)** -> **Save & Reboot (保存して再起動)** を押して初めて有効となります。

DNS

DNS セクションでは、カメラのドメイン名サービスを設定できます。データ送信先のドメイン名を解決する必要がある場合に、カメラは DNS サーバーに接続します。

最も一般的な使用法は、Event Handler (イベント ハンドラ) セクションの ftp または E メール サーバーをドメイン名で定義する方法です。DNS サービスが構成されていないと、カメラは FTP または E メール サーバーのドメイン名を解決する方法が分からなくなります。

Primary (プライマリ) / Secondary (セカンダリ) DNS サーバーの両方を構成できます。Secondary DNS Server (セカンダリ DNS サーバー) は、Primary DNS Server (プライマリ DNS サーバー) への接続失敗時に使用されます。



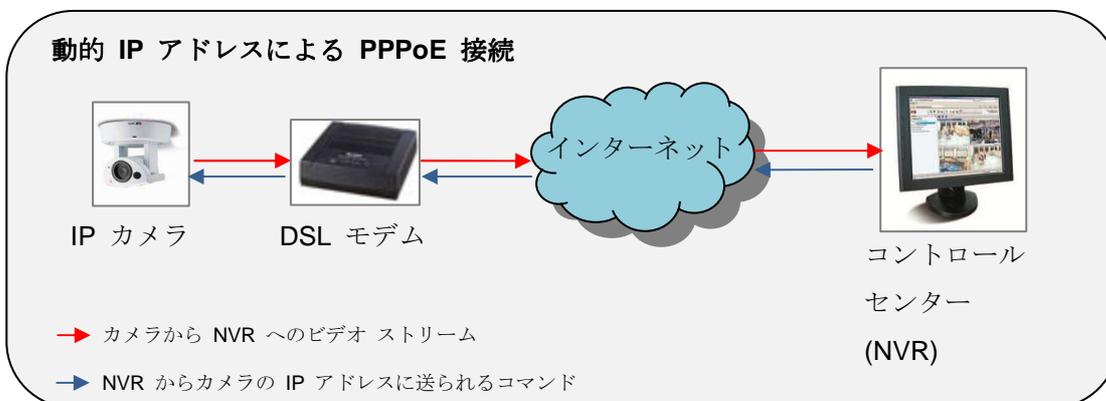
上記項目を変更してから、**Apply (適用)** を押して変更を保存します。**Reset (リセット)** ボタンは、今しがた変更が行われ、まだ適用されていない更新内容を元に戻します。

DDNS

DDNS

監視ソリューションによっては、広範な領域に点在する単一カメラで構成される場合があります。そのため、これらのカメラをそれぞれインターネットに接続して、コントロールセンターにアクセスできるようにしておかなければなりません。例えば、チェーン店、バス停、両替ブース等の場合です。

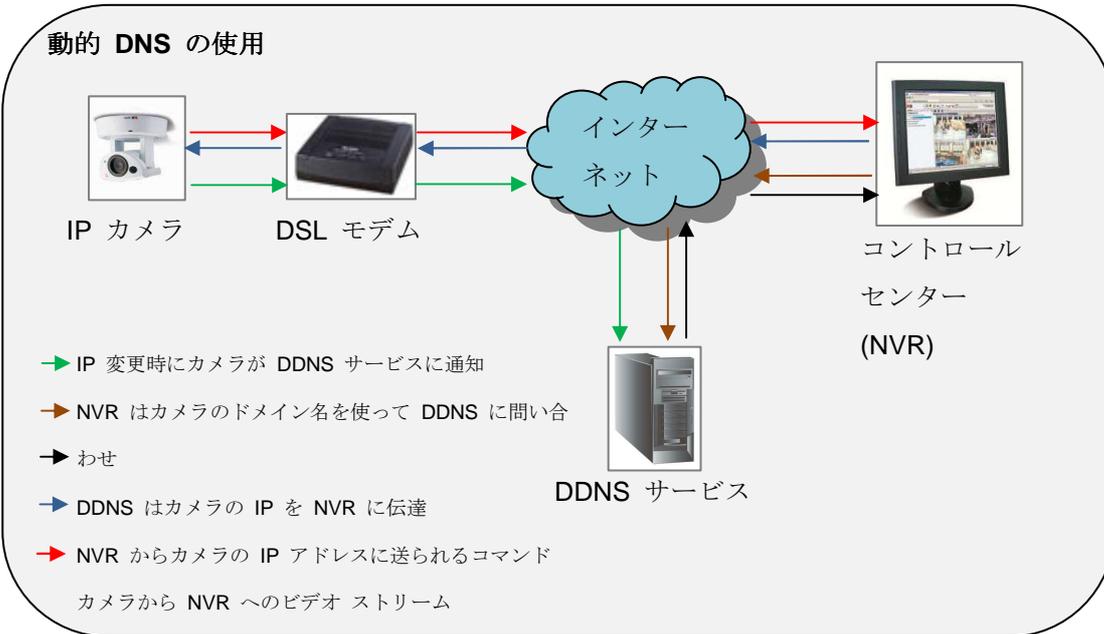
このような場合、実用的なネットワークソリューションの一つが、カメラ側で DSL モデムを使用し、PPPoE 接続により DSL モデム経由でインターネット サービス プロバイダーから動的 IP アドレスを取得できるようにする方法です。これなら静的 IP アドレスを適用するよりも、費用効果がさらに高くなります。



ただし、このソリューションには欠点の一つがあります。コントロールセンターからリモート監視を行うため、コントロールセンターの NVR サーバーは、常時 IP カメラのアドレスを把握し、カメラからビデオ ストリームを取得できるようにしておく必要があります。カメラのネットワーク接続が、何らかの理由でリセットされた場合、カメラは DSL モデム経由で、以前とは異なる新しい IP アドレスを取得することになります。NVR はこの変更が把握できないため、カメラと NVR 間の接続は失敗してしまいます。

ただし、カメラの IP が頻繁に変更しても、NVR が必ずカメラを検出できるようにする解決法があります。弊社のカメラは、しばしば変更する IP を、特定の不変ドメイン名にマッピングできるようにする、**Dynamic DNS (動的 DNS)** または **DDNS** サービスに対応しています。マッピング データベースとその更新エンジンは、Dynamic DNS サーバーの一つにホストされますが、そのほとんどのサーバーが無償で基本サービスを提供しています (例：www.dyndns.org)。

動作の仕組み 下図をご覧ください。



IP カメラは以前と異なる IP を取得するたびに、パブリック DDNS サービスにその変更を通知します。DDNS サービスは直ちに、割り当てドメイン名 (例えば *camera123.dyndns.org*) を新しい IP アドレスにマッピングして、そのデータベースを更新します。NVR 設定では、カメラの識別にドメイン名 (*camera123.dyndns.org*) のみが使用されます。NVR はカメラへの接続が必要になるたびに、DDNS サービスに現在のカメラの IP を問い合わせます。DDNS サービスはすぐに NVR へ応答し、カメラの IP を伝えます。これで、NVR はカメラの IP を使ってカメラに接続し、カメラから NVR へのビデオ ストリームを開始できるようになります。

そのため、カメラの IP アドレスが頻繁に変更しても、NVR は常に IP カメラを検出できるようになるわけです。無償で利用できるパブリック DDNS サービスは数多くありますので、単一カメラの設置場所には、PPPoE ベースの接続が実に優れた低コストのソリューションと言えます。

DDNS

Enabled

As a service / As a protocol reference: members.dyndns.org

Host Name: camera123.dyndns.org

User Name: camera123owner

Password: ●●●●●●●●

Apply
Reset

DDNS を有効にするには、「**Enabled (有効)**」にチェックを入れてください。サーバー リファレンスを選択し、**Host Name (ホスト名)** (DDNS サービスがカメラに与えるドメイン名)、及び DDNS サーバー アカウントの **User Name (ユーザー名)** と **Password (パスワード)** を入力します。

一度 DDNS サービスに登録し、カメラのドメイン名を要求すると、そこから必要なホスト名、ユーザー名、パスワード情報が得られます。

上記項目を変更してから、**Apply (適用)** を押して変更を保存します。**Reset (リセット)** ボタンは、今しがた変更が行われ、まだ適用されていない更新内容を元に戻します。

ビデオ

Video

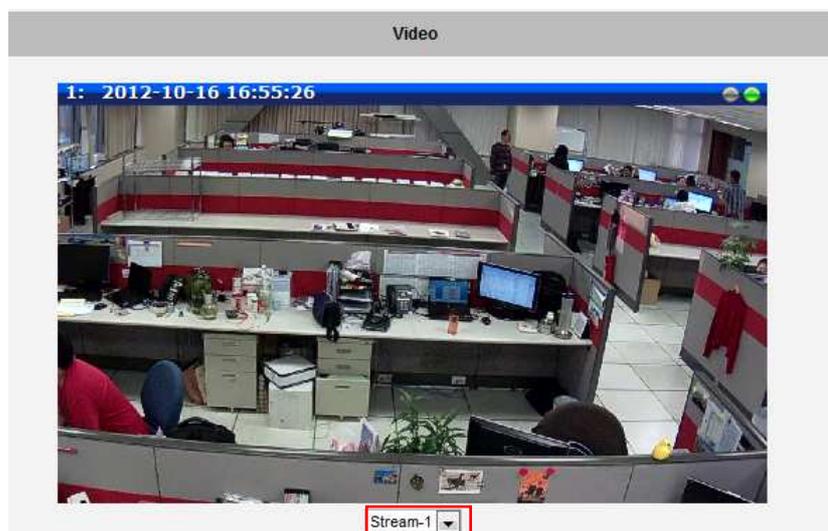
Video (ビデオ) セクションでは、カメラのビデオ画質を調整し、ストリーミングの詳細を構成するためのオプションが提供されます。カメラのデフォルト設定でほとんどの環境に十分対応できるため、ビデオ調整は不要です。次のセクションでは、ビデオ調整が必要になる万一の場合に備え、ビデオ画質またはストリーミングの詳細を構成する方法を説明します。

Video (ビデオ) の前に表示される **[+]** マークは、これをクリックすることによりリストを展開できることを示しています。リストを展開後に **[-]** マークをクリックすると、もう一度リストを閉じることができます。

Video

サブセクションも **Video (ビデオ)** と名付けられています。音声対応カメラの場合は、**Audio (音声)** というサブセクションも表示されます。ビデオ セクションは複数のタブに分かれます。各タブの機能については、以下で個別に説明します。

Video (ビデオ) と名付けられたサブセクションを開くと、カメラの **Stream 1 (ストリーム 1)** のライブ ビューが表示されます。カメラはデュアル ストリーム デバイスであるため、ライブ 映像ウィンドウ下の **Stream-1 (ストリーム-1)** または **Stream-2 (ストリーム-2)** のいずれかを選択することにより、2 つのストリーミング構成それぞれの表示状態を確認できます。



ストリーム-1 は録画用として解像度・フレーム レート共に最大の高画質ビデオになるよう構成されることが多く、ストリーム-2 は大抵の場合、マルチチャンネルのビデオ デコーディング中に VMS の計算能力を抑え、VMS のライブ表示用として提供される、品質が中レベルのストリームです。

Compression (圧縮方式)

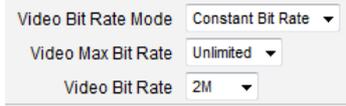
Compression

「Compression (圧縮方式)」では、ビデオ ストリーム 1 とストリーム 2 の圧縮設定を定義できます。圧縮の目的は、帯域幅と VMS ストレージ消費量の低減です。

一般にストリーム 1 は、NVR 録画用として高画質ストリームに構成され、ストリーム 2 は、NVR のライブ表示用として、ビデオ デコーディングに使用する NVR の計算能力を最小化した、基本レベルの品質に構成されます。

Stream 1	Stream 2
Encoder Type: H.264	Encoder Type: MJPEG
VGA Aspect Ratio: Auto Detected	VGA Aspect Ratio: Auto Detected
Resolution: N1280x720	Resolution: N640x360
Frame Rate: 30	Frame Rate: 15
Video Bit Rate Mode: Constant Bit Rate	Quality: 70
Video Max Bit Rate: 2M	
Apply	Reset

パラメータ	説明
Encoder Type (エンコーダー タイプ)	エンコーダーは、H.264 (ハイ プロファイル) と MJPEG の 2 タイプが使用できます。
VGA 縦横比	VGA ストリームの縦横比を定義するために使用します。4:3 比 (640x480) または 16:9 比 (640x360) のいずれかを設定できます。「Auto Detected (自動検出)」を選択すると、VGA ストリームは、ストリーム 1 とストリーム 2 の表示を一致させるため、解像度が比較的高いストリームの比率に合わせます。
解像度	カメラのモデルによって、得られる解像度の数は異なります。カメラにデフォルトで設定されている解像度は、必ずしもカメラの最大解像度であるとは限りません。最大解像度を使用する場合は、このセクションで設定できます。ストリーム 2 で設定可能な最大解像度はストリーム 1 よりも小さい値となります。
Frame rate (フレーム レート)	1 秒当たりのフレーム数を定義します。
Video Bit Rate Mode (ビデオ ビット レート モード) (H.264 のみ)	「Constant Bit Rate (固定ビット レート)」モード (CBR) では、シーンの複雑度に関わらず、カメラは安定したビットレートを保持します。このモードの状態ではビット レート値の設定が低すぎると、画質が変わることがあります。このモードでは、ストレージやネットワーク帯域幅の消費量が、可変ビット レートと比べて予測しやすくなります。 「Variable Bit Rate (可変ビット レート)」モード (VBR) では、カメラの画質が安定しますが、ビット レートはシーンの複雑度によって上下することがあります。

<p>Video Max Bit Rate (ビデオ最大ビット レート) (H.264 のみ)</p>	<p>ビットレートの上限を定義します (CBR モードで使用する場合のみ)。ビットレートはその制限値をわずかに下回って推移します。例えば、制限値が 2M に設定されている場合、ビットレートはおよそ 1.6~2.0 Mbps の範囲で推移します。</p>  <p>Video Max Bit Rate (ビデオ最大ビット レート) で「Unlimited (無制限)」を選択すると、ビット レート レベルを定義する Video Bit Rate (ビデオ ビット レート)」の選択ボックスが表示されます。</p>
<p>Video Bit Rate (ビデオ ビット レート) (H.264 のみ)</p>	<p>CBR モードで、Video Max Bit Rate (ビデオ最大ビット レート) に「Unlimited (無制限)」を選択すると、平均ビット レートを定義できます。例えば、Video Bit Rate (ビデオ ビット レート) に 2M を選択すると、実際のビット レートは時折 2M を上下しますが、長期的に見れば平均ビット レートは 2M に大変近い値となります。このモードで最も正確なストレージを推定できますが、帯域幅を設計する際はビット レートの不定期に見られる最大値を考慮してください。</p>
<p>Quality (品質)</p>	<p>H.264 圧縮方式:</p>  <p>VBR モードでは、ビット レートは変動しますが、画質は安定し、ユーザー設定の品質基準が確保されます。品質は「High (高)」、「Medium (中)」、「Low (低)」のいずれかを選択できます。品質レベルが高いほど、ターゲットの品質を達成するためにカメラが使用するビット レートは高くなります。</p> <p>MJPEG 圧縮方式: 品質を 1 ~ 100 の数値スケールで定義できます。デフォルトでは MJPEG の品質は 60 です。品質レベルが高いほど、ターゲットの品質を達成するためにカメラが使用するビット レートは高くなります。</p>
<p>GOP (H.264 のみ)</p>	<p>VBR モードでは、GOP 長 (I-フレームの出現頻度) を調整できます。デフォルトでは、毎秒 1 I-フレームです。例えば、30fps の場合、デフォルトでは毎秒 1 I-フレームと 29 P-フレームで構成されます。GOP を「5 秒あたり 1 I-フレーム」に変更すると、1 I-フレームの後に 149 P-フレームが続きます。静的シーンの場合、GOP が長いと帯域幅とストレージの消費量をさらに最小化できます。</p>

上記項目を変更してから、**Apply (適用)** を押して変更を保存します。**Reset (リセット)** ボタンは、今しがた変更が行われ、まだ適用されていない更新内容を元に戻します。

Motion Detection (動体検知)

Motion Detection

「Motion Detection (動体検知)」では、カメラのビデオ動体検知システムを構成できます。動体検知領域は、ストリーム 1 に基づいています。デフォルトでは、すべての領域が無効に設定されています。

Region	Enabled	Sensitivity	Trigger Interval [s]	Trigger Threshold
1	<input type="checkbox"/>	70	1	10 %
2	<input type="checkbox"/>	70	1	10 %
3	<input type="checkbox"/>	70	1	10 %

Setup

「Setup (セットアップ)」をクリックして、動体検知領域またはそのパラメータを調整します。

Microsoft Internet Explorer ブラウザーが、動体検知領域の構成に必要となります。

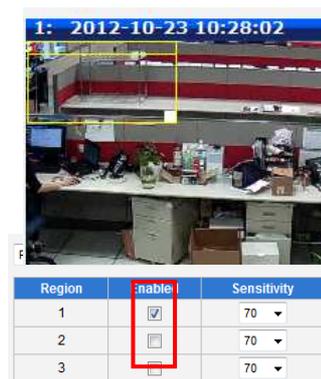
カメラには個別に構成可能な動体検知領域が 3 箇所あります。また、各動体検知領域には 6 つの構成パラメータがあります。

- 有効または無効
- 領域の場所
- 領域のサイズ
- 感度
- トリガーしきい値
- トリガー間隔

有効または無効

3 箇所の動体検知領域はそれぞれ個別に有効/無効に設定できます。例を見ると、領域 1 のみ有効、2 と 3 は無効に設定されています。無効の領域はビデオ表示から消えます。

動体検知領域の番号は、領域の左上隅に記載されることにご注意ください。



領域の場所

画像に表示される動体検知範囲の最上部をドラッグすることにより、動体検知領域を表示フィールドのどこにでも移動できます。好みに合わせて、動体検知領域をオーバーラップさせることも可能です。



領域のサイズ

動体検知領域の右下隅をドラッグすることにより、領域のサイズを変更できます。領域の最大サイズは、全画面の大きさまで拡大可能です。



感度

感度は、実際の移動ターゲット（人、車）と、風にそよぐ木の葉のような、わずかに動く背景との識別に役立つパラメータです。誤認警報を避けるためには、カメラが小さな動作を無視できれば良いと思われます。カメラの感度レベルが高いほど、アラームのトリガーに必要なオブジェクトの移動は小さくなります。例えば、動体検知領域内のオブジェクトが 2 ビデオ フレーム間に 1~3 ピクセル分ほど移動した場合、この小さな動作は感度が低いとカメラに破棄され、感度が高いとアラームをトリガーします。つまり、感度レベルは**真逆の速度規制**と考えられます。感度が小さいほど、動きの速いオブジェクトは検知されずに移動を見逃されます。

動体検知構成で最大の課題は、誤認警報を引き起こさず、同時に実際の侵入を見落とさない設定を見つけ出すことです。目安としては、**誤認警報を引き起こさずに、感度をできる限り高く設定することです**。カメラのデフォルト感度レベルは 70（スケールは 0~100）で、最も標準的な場合に適した設定になっています。

トリガーしきい値

動体検知領域に入り込む移動オブジェクトをご覧ください。大変ゆっくりと移動していますが、モーション アクティビティを引き起こしています。つまり、複数のピクセル範囲で、許可済みの感度「制限速度」(70)よりも速いモーションが報告されたのです。



画像右側の青いグラフは、動体検知領域内の何パーセントのピクセルが「現在移動中」と見なされているかを示しています。

Runtime MD Profile

Region	Enabled	Sensitivity	Trigger Interval [s]	Trigger threshold
1	<input checked="" type="checkbox"/>	70	1	10 %
2	<input type="checkbox"/>	70	1	10 %
3	<input type="checkbox"/>	70	1	10 %

アクティビティ パネル自体がタイムラインとなっており、時点ごとに青色バーの高さが確認できます。ある時点でアクティビティ グラフの最も高いバーがおよそ 25% (アクティビティ パネル全高の 4 分の 1) に到達していることに気づかれるかもしれません。これは、その時点で動体検知領域の 25%が移動ピクセルで埋められていることを意味します。目視観察でも動体検知領域内に立っているオブジェクトが、実際に領域サイズの約 25% を占めていることが確認できます。

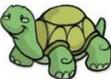
もしオブジェクトが本当に小さく、かなり速く移動するとしたら (現在の感度レベルでトリガーされるのでは) ? 例として、部屋の中を歩く猫ではなく、人を検知したいと考えた場合、人も猫も、モーションをトリガーする速度で移動する可能性はありますが、トリガーされるピクセルのサイズは異なります。例えば、動体検知領域を通過する人は、その領域の 25% のピクセルをトリガーしますが、猫がトリガーするのはわずか 2% に過ぎません。鳥や猫、チョウ、ネズミ等は無視して、人や車が通過した場合に本物のアラームが発生するようにしたいため、本物のアラームと見なすトリガー ピクセルの割合を定義できるフィルターが必要となります。このパラメータが **trigger threshold (トリガーしきい値)** と呼ばれます。トリガーしきい値のデフォルト値は 10% です。すなわち、動体検知領域サイズの 10%より大きく、許可済みの感度レベル (70) よりも速く移動するオブジェクトのみが、実際のアラームを発生させます。

最適なトリガーしきい値レベルの選択方法は? 目安としては、**人や車ではない移動オブジェクトで誤認警報を引き起こさずに、トリガーしきい値をできる限り小さく設定することです。**

感度レベルとトリガーしきい値レベルは、動体検知領域ごとに異なる値に設定できます。

上記の内容をさらに詳しく理解するには、以下の表を参照してください。感度レベルとトリガーしきい値のパーセントを使用した、想定される 4 つの組み合わせ設定を紹介しています。

セルごとに表示されるオブジェクトは、定められた設定でアラームをトリガーします。

	低しきい値 (0-5%)	高しきい値 (5-100%)
低感度 (0-65)	大きくて速い  小さくて速い 	大きくて速い 
高感度 (65-100)	大きくて速い  大きくて遅い  小さくて速い  小さくて遅い 	大きくて速い  大きくて遅い 

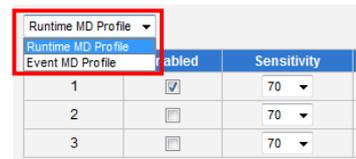
カメラのデフォルト感度は **70** でしきい値は **10%** です。これらのデフォルト値では、ウサギとカメがアラームをトリガーし、チョウとカタツムリは動体検知システムに無視されます。

重要：動体検知領域のサイズを変更すると、しきい値に影響を及ぼすことにご留意ください。同じオブジェクトサイズでモーションをトリガーする場合は、動体検知領域のサイズが大きいほど、しきい値が小さくなります。例えば、動体検知領域を前のサイズの **2** 倍にした場合、しきい値は元の値を半減 (**10%→5%**) することにご留意ください。一方、動体検知領域の位置を変更しても、しきい値には全く影響しません。

トリガー間隔

最後の構成項目はトリガー間隔です。トリガー イベント開始からの期間を示すもので、その間のあらゆるモーション アクティビティはカメラに無視されます。これは、同じ侵入を無駄に繰り返して報告しないように設計されたものです。トリガー間隔が **20** 秒とは、イベント発生時に、カメラが **1** 回限りの特定アクションを起こし、動体検知領域で継続中のアクティビティを **20** 秒間無視することを意味します。**20** 秒経過時に、動体検知領域でなおアクションが検知されると、カメラは新たにアラームを発生させ、再度アクションを起こします。

動体検知構成ページには、上記に説明されていない項目がもう一つあります。動体検知のプロファイルです。それらをプロファイル 1 (Runtime MD Profile、ランタイム MD プロファイル) とプロファイル 2 (Event MD Profile、イベント MD プロファイル) と考えます。これは、2 つの独立したグループから成る動体検知領域 (グループごとに最大 3 箇所のエリア) を構成できることを意味します。通常、プロファイル 1 (Runtime MD Profile、ランタイム MD プロファイル) が、カメラのアクティブ プロファイルとして使用されます。ただし、場合によってはカメラのイベント ハンドラ システムを使用することにより、カメラがプロファイル 2 に切り替わる場合があります。



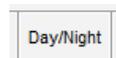
	Runtime MD Profile	Event MD Profile	Enabled	Sensitivity
1			<input checked="" type="checkbox"/>	70
2			<input type="checkbox"/>	70
3			<input type="checkbox"/>	70

通常、プロファイル 1 (Runtime MD Profile、ランタイム MD プロファイル) が、カメラのアクティブ プロファイルとして使用されます。ただし、場合によってはカメラのイベント ハンドラ システムを使用することにより、カメラがプロファイル 2 に切り替わる場合があります。

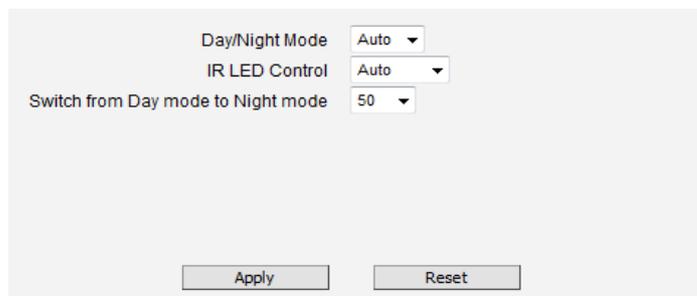
例えば、昼間と夜間の動体検知パラメータは別にした方が良いでしょう。そこで 2 つのプロファイルが実際に役立ってきます。この場合、イベント レスポンス システムの構成に進む前に、両プロファイルの動体検知パラメータを忘れずに構成してください。

上記項目を変更してから、**Apply (適用)** を押して変更を保存します。**Reset (リセット)** ボタンは、今しがた変更が行われ、まだ適用されていない更新内容を元に戻します。

Day/Night (デイ / ナイト)



Day/Night (デイ/ナイト) セクションでは、デイ モードとナイト モード間の切り替えをコントロールできます。このセクションは、デイ/ナイト モデルのみに表示されます。

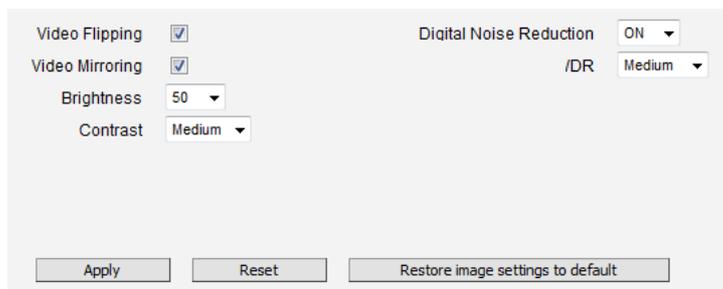


パラメータ	説明
Day/Night mode (デイ / ナイト モード)	<p>3 つのモードがあります。</p> <p>Auto (自動) : 「Switch from Day mode to Night mode (デイ モードからナイト モードへの切り替え)」でユーザーが定義した特定の露出レベルで、デイ モード (カラー) とナイト モード (モノクロ) を自動で切り替えます。</p> <p>Day (デイ) : 露出レベルに関わらず、カメラは常にデイ モード (カラー) に維持されます。</p> <p>Night (ナイト) : 露出レベルに関わらず、カメラは常にナイト モード (モノクロ) に維持されます。</p>
IR LED Control (IR LED コントロール)	<p>この機能は IR LED 搭載のカメラでのみ表示されます。</p> <p>2 つのモードがあります。</p> <p>Auto (自動) : 内蔵 IR LED は昼から夜に切り替わると自動で点灯し、夜から昼に切り替わると消灯します。</p> <p>Disabled (無効) : IR LED はデイ / ナイトモードに関わらず消灯します。</p>
Switch from Day mode to Night mode (デイ モードからナイト モードへの切り替え)	<p>0~100 のスケールで、昼から夜への切り替えが発生する露出レベルを定義できます。値が高くなるほど、デイ モードからナイト モードへの切り替えをトリガーする環境が暗くなります。</p>

画像



Image (画像) セクションでは、ビデオ フレームの特定パラメータをコントロールできます。



パラメータ	説明
Video Flipping (ビデオ フリップング)	このボックスにチェックを入れると、ビデオが上下反転します。通常は 180 度の回転効果を得るために、Video Mirroring (ビデオ ミラーリング) と併用されます。
Video Mirroring (ビデオ ミラーリング)	このボックスにチェックを入れると、ビデオが左右反転します。通常は 180 度の回転効果を得るために、Video Flipping (ビデオ フリップング) と併用されます。
Brightness (明るさ)	輝度値 (0~100) を選択します。値が高いほど画像は明るくなります。
Contrast (コントラスト)	次のオプションからコントラスト レベルを選択します: Lowest (最低)、low (低)、medium (中)、high (高)、highest (最高)。
Digital Noise Reduction (デジタル ノイズ リダクション)	デジタル ノイズ リダクションを ON または OFF にします。ON にすると、ビデオ (特に低照度時) のノイズが低減され、画像がよりスムーズかつクリアに映ります。
WDR	次のオプションから WDR レベルを選択します: Disabled (無効)、low (低)、medium (中)、high (高)、highest (最高)。

上記項目を変更してから、**Apply (適用)** を押して変更を保存します。**Reset (リセット)** ボタンは、今しがた変更が行われ、まだ適用されていない更新内容を元に戻します。

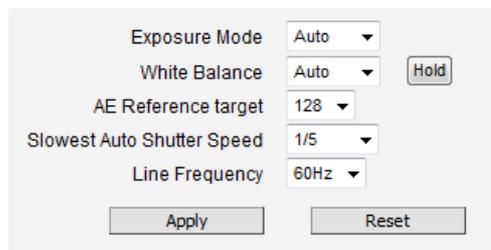
「**Restore image settings to default (画像設定をデフォルトに復元)**」ボタンは、工場出荷時の画像設定を素早く復元する方法です。これにより、カメラ全体を工場出荷時設定にリセットする必要はありません。

Exposure / White Balance (露出/ホワイト バランス)

Exposure/White Balance

Exposure / White Balance (露出/ホワイト バランス)のセクションでは、露出 (シャッター、アイリス、ゲイン コントロール) とホワイト バランス設定をコントロールできます。大抵の場合、デフォルト設定で十分対応できますので、調整の必要はありません。オプションによっては、特定の **Exposure / White balance (露出/ホワイト バランス)** モードでのみ表示されるものがあります。各モードの詳細は以下の通りです。

Exposure Mode - Auto (露出モード-自動)



Exposure Mode	Auto	
White Balance	Auto	Hold
AE Reference target	128	
Slowest Auto Shutter Speed	1/5	
Line Frequency	60Hz	
Apply		Reset

Auto Exposure Mode (自動露出モード) では、AE Reference Target (AE 参照ターゲット) と Slowest Auto Shutter (最低速自動シャッター) の構成により、画像の明るさをコントロールします。

AE Reference Target (AE 参照ターゲット) (自動露出参照ターゲット) は「センサーのターゲット輝度」と考えることができます。カメラは複数の内部パラメータを使用して、このターゲットを基準に最高画質を達成します。この値が高いほど、シーン全体は明るくなりますが、この場合、夜間のノイズは大きくなる可能性があります。AE Reference Target (AE 参照ターゲット) の範囲は、1~255 です。

カメラはシャッター スピード、自動アイリス (利用可能な場合)、シグナル ゲインをコントロールして、ユーザーが設定したターゲット レベルを実現します。自動アイリスが搭載されていない、または最大開口済みにも関わらず、画像がユーザー定義のターゲットより暗い場合、許容範囲 (「最低速自動シャッター スピード」でユーザー設定済み) 内でさらにシャッター スピードを下げて、シグナル ゲインを増加します。

Slowest Auto Shutter Speed (最低速自動シャッター スピード) は、自動シャッターの許容最低速度を決定するユーザー定義のしきい値です。例えば、シャッター スピードが照明条件に応じて 1/5 秒 ~ 1/2000 秒間で変化するようデフォルト設定されている場合、最低速自動シャッター スピードを 1/30 秒に設定すると、自動シャッター範囲が狭められ、1/30 秒~1/2000 秒間で動作するようになります。最低速度のしきい値をユーザーが定義できるようにする目的は、夜間撮影で遅すぎるシャッター スピードに因り発生するモーション ブラーを防ぐことにあります。

また、特定の周波数で点滅する人工光を使用する屋内ソリューションの場合は、シャッター スピードが速すぎると、露出モードに関係なくフリッカー (ちらつき) 効果が発生することがあるため、超高速は避けたほうが良いと知っておくことも重要です。

環境に応じたシャッター スピードの選択:

Shutter Speed (シャッター速度)	1/5	1/13 1/15	1/25 1/30	1/50 1/60	1/100 1/120	1/250	1/500	1/1000	1/2000
屋内	○	○	○	○	○	-	-	-	-
屋外	○	○	○	○	○	○	○	○	○

超低照度条件では、画像により多くの光量を取り込むためにシャッター スピードが落ちますが、ユーザー定義のしきい値を下回ることはありません。

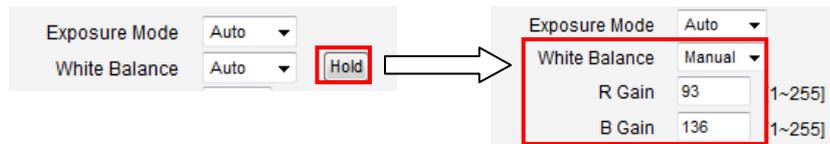
露出時間がフレーム間の時間間隔を超えた（シャッターが遅すぎる）場合（例：1/30 秒）、フレーム レートは自動で低減されます。この値の時間が長いほど、夜間に撮影される動きの遅いオブジェクトではさらに鮮明な画像が得られ、動きの速いオブジェクトではモーション ブラーの発生が多くなります。

White balance (ホワイト バランス) は「トゥルー ホワイト カラー」の意味を理解するカメラの機能を指します。カメラがトゥルー ホワイト カラーを理解すると、他のカラーも正確になります。人の目は、異なる光源に（窓から差し込む日光と室内照明が同時に入るといった混合光源でも）容易に順応しますが、カメラは特定シーンの主光源がどれか、その光源の「ホワイト カラー」がどれかを理解しなければなりません。

デフォルトでは、カメラは **auto white balance (自動ホワイト バランス)** モードに設定されており、光源とその色スペクトルの自動認識を試み、それに基づいて画像を調整します。この機能は背景で継続的に作動し、主光源に変化があるかどうか（例：カーテンを閉じて日光を遮断し、室内照明を点ける等）を確認するために、フレームごとに見直しが行われます。

大抵の場合、自動ホワイト バランスは最適な状態で作動しますので、調整の必要はありません。設置上まれないケース、特に視界に白いオブジェクトがなく、光源が混合する場合などは、カメラがホワイト カラーを識別して他のカラーを微調整することが困難になることがあります。

このような場合、設置者はカメラの前に白いオブジェクト（白紙など）を置き、数秒間視界を覆うことによって、カメラにトゥルー カラーを理解させる「手助け」を行うことができます。白紙がディスプレイ上で実際に白く見えるようになるまで、自動ホワイト バランス システムによるカラー調整が行われます。この時、**Hold (保留)** ボタンを押すことにより、これらのホワイト バランス設定を保持できます。このボタンを押すと、**White Balance (ホワイト バランス)** は、**Auto (自動)** モードから **Manual (手動)** モードに切り替わり、**Hold (保留)** の時点で取り込まれたカラー値が反映されます。これで、白いオブジェクトを視界から外すことができ、特定シーンに適したカラーが保持されます。



上級ユーザー向けに、White Balance（ホワイト バランス）を Auto（自動）モードから **Manual（手動）** モードに直接切り替え、手動で R Gain（R ゲイン）と B Gain（B ゲイン）を入力するオプションも用意されています。

Line Frequency（電力線周波数） は、特定国の人工光源の周波数に合わせてシャッター スピード オプションを調整する機能です。例えば、ヨーロッパでは（照明の電源周波数に因る）光周波数は 50Hz であり、毎秒 50 回点滅します。この場合、電源線周波数を 50Hz に設定することにより、シャッター スピード オプションは光源周波数に対応するようになります（1/25 秒、1/50 秒、1/100 秒など）。

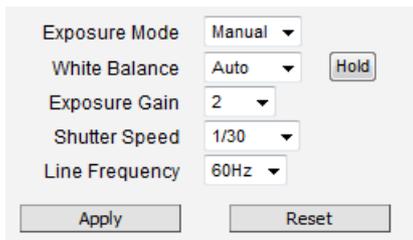
フリッカー効果を防ぐには、カメラの電力線周波数を光源の電源周波数に照らして調整しておく必要があります。

ただし、自然光源（日光）はシームレスな光の流れであるため、自然光にのみさらされるカメラの場合、電力線周波数は対象外の設定となります。

上記項目を変更してから、**Apply（適用）** を押して変更を保存します。**Reset（リセット）** ボタンは、今しがた変更が行われ、まだ適用されていない更新内容を元に戻します。

Exposure Mode - Manual (露出モード-手動)

照明条件が一日 24 時間安定していると、上級ユーザーは手動露出モードを使ってさらに画質を微調整し、特殊なプロジェクト要件を満たそうと考えるかもしれませんが、ほとんどの場合は、カメラを自動露出モードに設定したままにして、カメラのインテリジェント システムにより最適な露出設定を見つけ出せるようにしておくことを強くお勧めします。



手動露出モードでは、シグナル ゲインとシャッター スピードを直接手動で調整できます。White Balance (ホワイト バランス) と Line Frequency (電力線周波数) コントロールについては、前章で説明済みです。

上記項目を変更してから、**Apply (適用)** を押して変更を保存します。**Reset (リセット)** ボタンは、今しがた変更が行われ、まだ適用されていない更新内容を元に戻します。

OSD/Privacy Mask (OSD/プライバシー マスク)

OSD/Privacy Mask

OSD / Privacy Mask (OSD/プライバシー マスク) のセクションでは、ビデオ上で行う 2 種類の操作のいずれかを実行できます。

1. ビデオの上/下左隅にテキストを追加する。この機能は **Text Overlay (テキスト オーバーレイ)** または **On-Screen Display (OSD、オンスクリーン ディスプレイ)** と呼ばれます。カメラ名、日付と時間、IP アドレス、カスタム テキストをテキスト オーバーレイとして表示できます。テキストはできる限り小さいまま保持され、**サイズ変更はできません**。ディスプレイ上でビデオを 1:1 比に拡大すると、テキストが普通に読み取れます。テキストをこれほど小さくする目的は、テキスト オーバーレイが貴重な証拠映像の邪魔にならないよう、ビデオを遮るエリアを可能な限り小さくして、十分な法的証拠を提供できるようにするためです。テキストはビデオに埋め込まれ、再生やエクスポート後に削除することはできません。
2. 管理者のコンピュータ画面や浴室の入口など、カメラがキャプチャする必要のない、ビデオの非公開エリアを隠す。この機能は **Privacy Mask (プライバシー マスク)** と呼ばれます。マスキングは複数の独立したエリアに分けて構成できます。**Microsoft Internet Explorer** ブラウザーが、プライバシー マスクの構成に必要となります。プライバシー マスクはビデオに埋め込まれ、再生やエクスポート後に削除することはできません。

テキスト オーバーレイ (OSD) のセットアップ

最大 4 エリアのテキストを定義できます。1 エリア以上のテキストを **enabled (有効)** にして同じ場所に位置づけると、テキストは下方に 1 行ずつ表示されます。



Region	Enabled	Color	Transparent	Position	Format of Texts
1	<input checked="" type="checkbox"/>	Blue	50	Bottom	Office View %Y%Y%Y%H%M%S
2	<input type="checkbox"/>	Black	0	Bottom	
3	<input type="checkbox"/>	Black	0	Bottom	
4	<input type="checkbox"/>	Black	0	Bottom	

Apply Reset

上記の例では、青色で透明度 50%、左下隅に位置づけ、現在の日付と「Office View」というテキストを含む、という条件の 1 エリアのテキストが有効に設定されています。日付は毎日、カメラの「日付と時間」設定に準じて自動変更されます。この例の構成結果は以下のように表示されます (ライブ ビュー ページ、1:1 スケール) :



以下はテキスト フィールドに使用可能な、特別な意味を持つ文字のリストです。

パラメータ	説明
%YYYY	年は 4 桁形式。例：2008
%YY	年は 2 桁形式。例：08
%MM	月は 2 桁形式。例：1 月は 01、12 月は 12
%DD	日は 2 桁形式。01～31
%hh	時は 2 桁形式。00～23 24 時間表示のみ対応することに注意。
%MM	分は 2 桁形式。00～59
%ss	秒は 2 桁形式。00～59
%H	ハイフン、「-」
%C	コロン、「:」
%X	スラッシュ、「/」
%N	カメラ名を表示（最大 OSD 長を超える場合は切り詰められることがある）

上記項目を変更してから、**Apply（適用）** を押して変更を保存します。**Reset（リセット）** ボタンは、今しがた変更が行われ、まだ適用されていない更新内容を元に戻します。

Privacy Mask Setup（プライバシー マスクのセットアップ）

最大 4 エリアのプライバシー マスクをセットアップできます。プライバシー マスク エリアは、エリアの「Setup」欄下にチェックが入っている場合に調整できます。

Privacy Mask

(Don't overlap privacy mask regions)

Region	Enabled	Color	Setup
1	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
2	<input type="checkbox"/>		<input type="checkbox"/>
3	<input type="checkbox"/>		<input type="checkbox"/>
4	<input type="checkbox"/>		<input type="checkbox"/>



動体検知エリアと同じ方法でサイズ変更とドラッグを実行できます。エリア番号を含む上のバーは、そのエリアをビデオに跨ってドラッグする場合に使用でき、プライバシー マスクの右下隅にある白いボックスは、エリアのサイズ変更を使用できます。

プライバシー マスクには 4 つの定義済みカラーオプションが用意されています。他のカラーを使用する場合は、代わりに URL コマンドでプライバシー マスクをセットアップしてください。そのためには、URL コマンドの使用法について説明のあるガイドを参照してください。

ライブ ビューに戻すと、プライバシー マスクは次のように表示されます。



テキスト オーバーレイ (OSD) とプライバシー マスクは、ストリーム 1 とストリーム 2 の両方で有効になります。

上記項目を変更してから、**Apply (適用)** を押して変更を保存します。**Reset (リセット)** ボタンは、今しがた変更が行われ、まだ適用されていない更新内容を元に戻します。

注意:Apply (適用) を押すと、映像表示上のエリア位置の更新に数秒かかることがあります。

On-Screen Graphics (オンスクリーン グラフ)

On-Screen Graphics (OSG、オンスクリーン グラフ) は、ビデオ上にカスタム画像ファイルをレイヤとして配置できる新しい機能です。例えば、安全のためのウォーターマーク (透かし) として、あるいはブランド ロゴとして、ビデオ画像の隅に入れることができます。

この機能はほとんど使用されないため、**Web Configurator (Web コンフィギュレータ)**内には、オンスクリーン グラフを構成するためのインターフェースがありません。代わりに URL コマンドを使用してこのタスクを完了できます。

画像を OSG として使用可能にするには、カメラにアップロードする前に、YUV 形式 (イメージ ラスター グラフィックス) に変換します。YUV 形式への画像変換に使用できるフリーウェアのコンバータは複数あります。

例えば、YUV コンバータの無料体験版は、以下でダウンロードできます。Sunrayimage.com:

http://www.sunrayimage.com/download/YUVTools_3.0_trial.zip

弊社が、この製品の性能、利用規約、可用性を保証することはありません。ユーザーは最初に利用規約を読んでから、規約に承諾できる場合にインストールを続行する必要があります。

画像は 640x480 ピクセル以下となり、偶数のピクセルが含まれることにご注意ください。一度アップロードした画像のサイズ変更はできないため、カメラにアップロードする前に画像のサイズが正しいことを確認してください。

例えば、YUV に変換済みで、サイズが 204x106 の BMP ロゴがある場合：



画像の準備が完了したら、次の URL コマンドでカメラにアップロードします：

http://192.168.0.100/cgi-bin/cmd/encoder?OSG_IMAGE

ユーザー名とパスワードの入力が完了すると、以下のアップロード ウィンドウが表示されます。コンピュータに準備した yuv ファイルを **Browse (閲覧)** し、Apply (適用) を押します。

OSG_IMAGE :

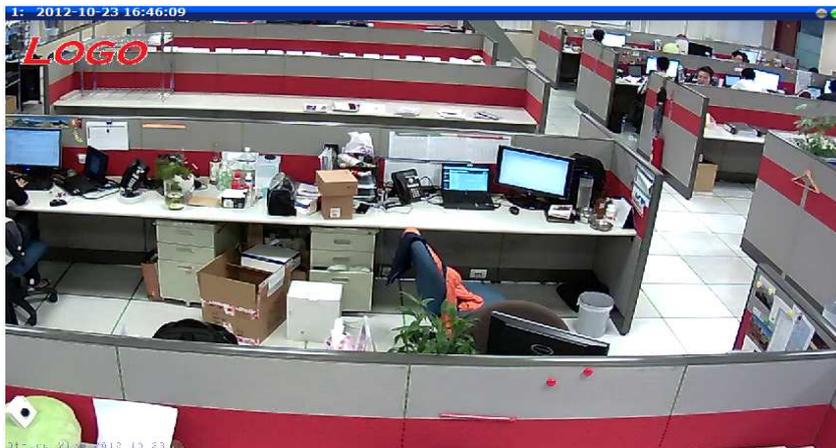
完了したら、別の URL コマンドを使ってその位置を構成します：

**http://192.168.0.100/cgi-bin/cmd/encoder?OSG_CONFIG=
1,0,0,240,106,EB8080,4**

... OSG_CONFIG の後にある 7 つのパラメータは次の内容を示します。

パラメータの位置	説明
1	1 は有効、0 は無効を示す。
2	X 位置
3	Y 位置
4	画像の幅
5	画像の高さ
6	ブレンドされる画像背景色の YYUUVV 値
7	透明度レベル: 0 は 0%、1 は 25%、2 は 50%、3 は 75%、4 は 100% を示す。

結果は以下のように表示されます：

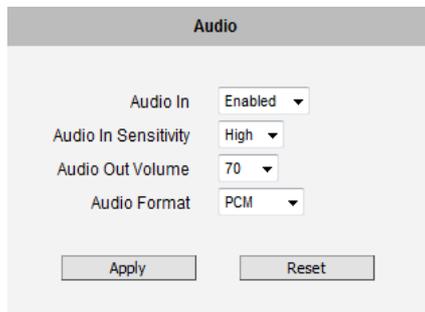


音声

Audio

Audio (音声) セクションは、音声対応モデルのみに適用されます。

オーディオ コントロールのユーザー インターフェースは以下のように表示されます。



パラメータ	説明
Audio in (音声入力)	「Enabled (有効)」オプションは着信音声 (ライン入力または内蔵マイク) を有効にします。「Disabled (無効)」オプションは、着信音声をオフにします。この場合、ビデオ ストリームは音声なしでキャプチャされます。
Audio In Sensitivity (音声入力の感度)	ターゲットがカメラからかなり離れている時は「High (高)」を選択し、ターゲットがカメラの近くにある時は「Low (低)」を選択します。「High (高)」モードでは、信号増幅のレベルが高くなるため、音声ノイズが大きくなる場合があります。
Audio Out Volume (音声出力の音量)	音声出力の音量レベルは、0~100 のスケールで調整できます。カメラに接続されたスピーカーの音量レベルに影響します。
Audio Format (音声形式)	音声の圧縮形式を選択します: PCM、G.711A (A-law) または G.711U (μ -law)。

カメラのマイクやライン入力デバイスの音声を聞くには、Web Configurator (Web コンフィギュレータ) を実行する PC にスピーカーを接続しますが、その音量レベルを調整するには、**Live View (ライブ ビュー)** ページに進み、そこにある音量コントロールを使用します。

Audio Muted (音声はミュート状態) :



Audio level adjusted to the maximum (音声レベルを最大に調整) :



この音量コントロールは、カメラの音声入力機能が「Enabled (有効)」に設定されている場合のみ、ユーザー インターフェースに表示されます。

イベント

このセクションでは、IP デバイスの状況対処法に関わる、イベント ハンドラのセットアップ方法を説明します。IP デバイスごとに最大 10 件のイベント ルールを設定できます。各ルールには、1 つのトリガーと 1 つ以上のレスポンスが含まれます。数種類のレスポンスが設定可能です。またデバイスが情報交換する外部サーバーは複数存在します。

イベント ハンドラのセットアップには、次の 4 つの設定方法があります。Event Server (イベント サーバー)、Event Configuration (イベント構成)、Event Rules (イベント ルール) および Manual Event (手動イベント) です。

⊕ の項目 (Event (イベント) の前) をクリックしてリストを展開します。



Event Server (イベント サーバー)

Event servers (イベント サーバー) は、デバイスのインタラクションの相手を定義します。それらは、ネットワーク上の他のサーバーまたはデバイス、もしくはカメラ本体である場合があります。**Event Configuration** (イベント構成) は、インタラクションの間、相手に伝達する内容のリストを構成します。**Event list** (イベント リスト) は、どのトリガーからどのレスポンスをいつ開始するかについての規則と条件を定めています。**イベント ルールで使用可能なオプションは、イベント サーバーやイベント構成から選択されたものです。**

イベント サーバーは、FTP サーバー、SMTP サーバー、および HTTP サーバーに分類されます。

Event Server			
Type	Network Address	Ports	User Name
FTP Server Configuration	none	21	none
SMTP Server Configuration	none	none	none
HTTP Server 1 Configuration	none	80	none
HTTP Server 2 Configuration	none	80	none

FTP server (FTP サーバー)

FTP サーバーは、イベント ハンドラからレスポンスの一部として発行されるスナップショットやビデオのアップロードを受信することができます。FTP サーバーを 1 つセットアップできます。

FTP Server Configuration

Network Address

Network Port

User Name

User Password

Mode

Max. Connection Time sec. (0~60 sec)

FTP サーバーをセットアップするには、必ず FTP サーバーのネットワーク アドレス、ネットワーク (FTP) ポート、FTP アカウントのユーザー名とパスワード、接続モード (**Passive** または **Active**) およびタイムアウトまでの接続時間を入力してください。

上記項目を変更してから、**Apply (適用)** を押して変更を保存します。**Reset (リセット)** ボタンは、今しがた変更が行われ、まだ適用されていない更新内容を元に戻します。

SMTP server (SMTP サーバー)

SMTP サーバーは、IP デバイスからの要求があり次第、E メールを送信できます。E メールは件名とテキストの簡単なもので、スナップショット / ビデオを添付することができます。2 つの **SMTP サーバー**をセットアップできます。デバイスは最初にプライマリ E メール **SMTP サーバー**経由でメッセージの送信を試みます。最初の試みが失敗すると (最大接続時間の経過後)、デバイスはセカンダリ **SMTP サーバー**経由で送信を試みます。プライマリ **SMTP サーバー**経由による E メール送信が成功した場合、セカンダリ **SMTP サーバー**は使用されません。

SMTP Server Configuration

Primary SMTP Configurations

Enabled

Authentication Type

User Name

User Password

Sender Email Address

Network Address

Network Port

Max. Connection Time sec. (0~300 sec)

Secondary SMTP Configurations

Enabled

SMTP サーバーをセットアップするには、必ず SMTP アカウントを有効にし、正しい認証タイプを選択してください。多くのタイプが使用できます。デフォルトは Login (ログイン) です。Auto Detection (自動検出) の使用をお勧めします。利用可能な認証タイプには、Auto Detection (自動検出)、None (なし)、Login (ログイン)、Plain、Cram MD5、Digest MD5、PoP Relay が含まれます。User Name (ユーザー名)、パスワード、送信者として表示される E メールアドレス (ユーザー名と異なるものも可能)、ネットワーク (SMTP サーバー) アドレス、ネットワーク (SMTP サーバー) ポート番号およびタイムアウトまでの最大接続時間 (秒単位) も入力してください。

上記項目を変更してから、**Apply (適用)** を押して変更を保存します。**Reset (リセット)** ボタンは、今しがた変更が行われ、まだ適用されていない更新内容を元に戻します。

HTTP server (HTTP サーバー)

HTTP CGI サーバー は、Web サイトや複数のデバイスで実行するプログラムです。カスタムプログラムが可能のため、入力に基づき多種多様なアクションを実行できます。ここで、接続する CGI サーバーと、ターゲット サーバーのログインに必要なユーザー / パスワードを定義できます。実際のメッセージ / コマンドは、「Notification messages / URL commands (通知メッセージ / URL コマンド)」のセクションでセットアップします。2 つの個別 CGI サーバーを定義できます。

IP デバイスは CGI サーバーでもあります。つまり、IP デバイスが互いにコマンドを出し合えることで、レスポンスを高度に統合する可能性が無限に広がることを意味します。また、IP デバイスはループバックコマンドを自身に送り、実質的には、ほぼすべての可能な設定を同時に変更することができます。カメラのコントロールに使用するコマンドの詳細については、カスタマーサービス係までお問い合わせください。

このユニークな機能の利用方法をさらにご理解いただくために、例を挙げて説明します。カメラ A を、メインホールに通じる廊下を映す固定カメラだとします。このカメラの動体検知ウィンドウは、廊下が大ホールに接するポイントの傍に、配置されているとします。カメラ B は、ホールに設置された PTZ カメラで、通常はオートツアーパトロール機能が作動中であるとします。動体検知エリアのモーション アクティビティが、カメラ A の MD1 をトリガーすると、それを受けてカメラ A のイベント ルールが作動し、カメラ B にコマンドを發します。次に、カメラ B は廊下が入口に通じる場所に設定されたプリセット ポイントに向けて回転し、より高いビット レートに切り替えて、さらに鮮明な画像を一時的に提供します。イベントが終了すると、カメラ B はビット レートを下げ、通常のルーチンに戻ります。

HTTP Server Configuration - 1

Enabled

User Name

User Password

Network Address

Network Port

Max. Connection Time sec. (0-60 sec)

HTTP サーバーをセットアップするには、必ず HTTP サーバーを有効にし、ユーザー名、ユーザー パスワード、ネットワーク (HTTP サーバー) アドレス、ネットワーク (HTTP サーバー) ポート番号、およびタイムアウトまでの最大接続時間 (秒単位) を入力してください。

上記項目を変更してから、**Apply (適用)** を押して変更を保存します。**Reset (リセット)** ボタンは、今しがた変更が行われ、まだ適用されていない更新内容を元に戻します。

Event Configuration (イベント構成)

Event configurations (イベント構成) は、イベントがトリガーされた時に実行されるレスポンスです。ほとんどのレスポンス タイプで、異なるプリセット レスポンスを複数作成し、それらを混合してイベント ルールに適合させることができます。

構成可能なレスポンスは、**Notification messages (通知メッセージ)**、**Upload Video/Snapshot and Audio (ビデオ/スナップショットと音声のアップロード)**、**Send URL Commands (URL コマンドの送信)** に分類されます。

Event Configurator

Notification message	<input type="button" value="Edit"/>
Upload video/snapshot and Audio	<input type="button" value="Edit"/>
Send URL commands	<input type="button" value="Edit"/>

Notification message (通知メッセージ)

***Pre-requisites: SMTP server / HTTP CGI server setup.**

Notification messages (通知メッセージ) は、E メールまたは HTTP CGI サーバーのどちらかに送信できます。**CGI** サーバーに送信された場合、URL コマンドと同様に機能しますが、イベント終了時に 2 つ目のメッセージは許可されません。最大 **3** つのプリセット メッセージを構成できます。メッセージを構成して、それを無効にすることも可能です。これにより、メッセージを使わない設定保存が可能となり、テストやトラブルシューティングの時に便利です。

Notification message

Notification message 1

Send message to: HTTP CGI 1

CGI Path & Program *
including path of CGI program

URL Command

Message *

Notification message 2

Send message to: E-Mail

E-Mail Recipients *
using ";" for multiple addresses

Subject *

Message *

Notification message 3

* : Fields must be filled in

Notification Messages（通知メッセージ）をセットアップするには、必ず、メッセージを有効にしてから、送信するメッセージのタイプ（HTTP CGI または E メール）を決定します。

CGI サーバーに送信する場合は、CGI パス、URL コマンド自体、オプションのメッセージを入力する必要があります。

E メールを送信する場合は、受信者の E メール アドレス、Eメールの件名、メッセージ本文を入力してください。

上記項目を変更してから、**Apply（適用）** を押して変更を保存します。**Reset（リセット）** ボタンは、今しがた変更が行われ、まだ適用されていない更新内容を元に戻します。

Upload video/snapshot (ビデオ / スナップショットのアップロード)

*前提条件:SMTP サーバー / FTP サーバー / HTTP CGI サーバーのセットアップ。

イベント発生時に、IP デバイスから、選択されているサーバーにビデオ録画 / スナップショットを送信できます。ビデオは .RAW 形式、スナップショットは .JPG ファイルになります。ビデオ / スナップショットのアップロードには、最大 3 グループの設定を定義できます。スナップショットは FTP / HTTP CGI 宛て、および E メール経由で送信できますが、ビデオは FTP または HTTP CGI サーバーへのアップロードのみ可能です。デバイスの音声の有効になっている場合、アップロードされたビデオには音声が含まれます。

この機能のセットアップに必要なパラメータは、タスクの組み合わせによってそれぞれ異なるため (スナップショット / ftp または ビデオ / HTTP... など)、以下に説明します。

有効化						UI
						Upload video/snapshot and Audio 1 <input checked="" type="checkbox"/>
アップロードするメディア タイプ	Snapshot (スナップショット)		Video (ビデオ)			Upload Media Type <input checked="" type="radio"/> Snapshot <input type="radio"/> Video
メディアのアップロード先	Email (E メール)	FTP	CGI	FTP	CGI	Upload Media To <input type="text" value="E-Mail"/>
アップロード期間	<input type="checkbox"/>	Upload Period <input type="text" value="0"/> (0~86400 seconds)				
アップロード期間中の画像	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			Images during Upload Period <input type="text" value="0"/> (Use 0 for maximum number of images)
プリバッファ時間				<input type="checkbox"/>	<input type="checkbox"/>	Pre-Buffer Time <input type="text" value="0"/> (0~10 Second)
画像ファイル名	<input type="checkbox"/>	Image File Name <input type="text" value="Front_Door_%YYYY_%MM_%DD"/>				
アップロードパス	*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Upload Path <input type="text" value="Camera/%N"/>
CGI パス&プログラム			<input type="checkbox"/>		<input type="checkbox"/>	CGI Path & Program <input type="text"/>
E メール受信者	<input type="checkbox"/>					E-Mail Recipients <input type="text"/> using ; for multiple addressed
件名	<input type="checkbox"/>					Subject <input type="text" value="Front Door Snapshot"/>
ビデオ ソース	<input type="checkbox"/>	Video Source <input type="text" value="1"/>				

Upload Video/snapshot and Audio checkbox (ビデオ/スナップショットと音声アップロードのチェックボックス) : これは、このルールを有効にするか無効にするかを決定します。トラブルシューティングの目的で、この設定を有効にしておくとう便利な場合がありますが、無効に設定しておいてください。

Upload Media to (メディアのアップロード先) : これらは目前のタスクを定義し、入力が必要なフィールドを変更します。

Upload Period (アップロード期間) : IP デバイスはここで選択した秒数のビデオ / スナップショットをアップロードします。この時間が経過するとビデオ / スナップショットのアップロードが停止します。このカメラで同時にビデオ管理ソフトによる録画を実行しても、NVR による通常録画は影響を受けることなく、イベントの間やその後も継続されます。ただし、特別なアップロード セッションは、イベント終了時に終了します。

Image during Upload Period (アップロード期間中の画像) : これはスナップショットでのみ使用します。アップロード時間内にカメラがキャプチャするスナップショット数のことです。この値を 0 に設定すると、IP デバイスは可能な限り多くのスナップショットをキャプチャします。デバイスのローディングによっては、キャプチャされるスナップショット数が、指定数に満たない場合があります。

Pre-Buffer Time (プリバッファ時間) : これはビデオでのみ使用します。これを 0 以上に設定すると、IP デバイスは内部メモリでビデオのバッファリングを開始します。最大プリバッファは **10 秒**です。イベントがビデオのアップロードを要求すると、IP デバイスはまずイベント直前に格納したビデオをアップロードし、次にアップロード時間に到達するまで、アップロードを継続します。

Image File Name/ Upload Path (画像ファイル名/アップロードパス) : ファイル名とアップロードパスのルールを指定する必要があります (E メールの場合アップロードパスは不要です。フィールドにスラッシュ「/」を入れるだけで結構です)。ルールにはフレキシブルパラメータが含まれます。一例を挙げると、ルールと対応ファイル名は以下のようになります。

Front_Door_%YYYY_%MM_%DD@%hh%mm%ss

Front_Door_2009_10_12@195037.JPG

アップロードパスフォルダーも同時に名前を付けられます。IP デバイスが FTP と HTTP CGI サーバー上にフォルダーを適切に作成できるようにするには、FTP/CGI アカウントがフォルダー作成の許可を受けている必要があります。オートネーミングのシンタックスについては、オンラインヘルプ、または本セクション文末の挿入ボックスを参照してください。

記号「%」は、ファイル名やアップロードパスの冒頭に付けることはできません。開始文字にはアルファベットまたは数字を使用してください。アップロードパスは、必ず最初と最後にバックスラッシュ「\」を付けてください。例は次の通りです : \Backgate%MM%DD\

CGI path & Program (CGI パス&プログラム) : CGI サーバーによっては特別な情報と設定が必要となる場合があります。本セクションの CGI サーバー デザイナーを参照してください。IP デバイスでは、埋め込み CGI サーバーにスナップショット / ビデオをアップロードできません。

E-Mail Recipient / Subject (E メール受信者/件名) : E メール経由でビデオ/スナップショットをアップロードする時は、これらのフィールドが必要となります。

Video Source (ビデオ ソース) : ビデオ ソースはビデオ 1 またはビデオ 2 から選択します。

ファイルとフォルダー向けのオート ネーミング ルール:

画像やビデオを適切に追跡するには、綿密なネーミング ルールが必要です。固有のネーミング システム設計に使用可能な自動変数は数多くあり、ファイルやフォルダーのどちらにも使用できます。

記号	説明	例
%YYYY	年を示す 4 桁	2009 年は 2009
%YY	4 桁年号の末尾 2 桁	2009 年は 09
%MM	月を示す 2 桁 01~12	1 月を示す 01
%DD	日を示す 2 桁 01~31	月の初日は 01
%hh	時を示す 2 桁 00~23	
%MM	分を示す 2 桁 00~59	
%ss	秒を示す 2 桁 00~59	
%W	空白文字 ''	''
%N	カメラ名	camera-1
%Y	ファイルのシリアル カウンター。アップロードするタスクごとに 1 から開始します。次のアップロード ファイルのカウンターは 1 ずつ増えます。	1,2,3,4,5,...

例

1. 時間が 2009/06/05 22:50:30 の場合、Entrance-%YYYY-%MM-%DD@%hh%mm%ss 。フルネームは Entrance-2009-06-05@225030
2. カメラ名が 'my-camera' で、連続してアップロードしたファイルが 3 つある場合、X_%w-%N_TEST%Y 。

Send URL commands (URL コマンドの送信)

*前提条件: HTTP CGI サーバーのセットアップ。

Send URL commands

Send Command 1 to HTTP CGI 1

Command as event is triggered /cgi-bin/cmd/encoder?PTZ_PRESET_GO=1
including path of CGI program [max. 119 characters]

Command as event becomes inactive /cgi-bin/cmd/encoder?PTZ_PRESET_GO=2
including path of CGI program [max. 119 characters]

Send Command 2 to HTTP CGI 1

Command as event is triggered /cgi-bin/cmd/encoder?VIDEO_BITRATE=3M&VI
including path of CGI program [max. 119 characters]

Command as event becomes inactive /cgi-bin/cmd/encoder?VIDEO_BITRATE=1M&VI
including path of CGI program [max. 119 characters]

Send Command 3 to HTTP CGI 1

イベント発生時に、URL コマンドを HTTP CGI サーバーに送信できます。これにより、イベント発生時に優れたインテリジェント レスポンスを実現する可能性が広がります。IP デバイスとその他多くのデバイスにも、制御可能な埋め込み CGI サーバーが搭載されています。

イベント ハンドラが URL コマンドを送る時は、イベントのトリガー実行時にコマンド一式が送信され、イベントが非アクティブになった時に別のコマンド一式が送信されます。CGI デザインによっては、URL コマンドを併せてひと続きの文字列にし、複数のコマンドを 1 行にして発行する場合があります。

例は、入り口に設置されたアクセス コントロール デバイスが入場を検知すると、このデバイスが PTZ カメラに DI 信号を送り、イベントをトリガーする、という設定を示しています。次にこのイベントは、(カメラ本体の IP を HTTP CGI サーバーとして設定することにより) カメラ本体にループバック コマンドを送ります。続いて PTZ カメラがプリセット ロケーションまで移動して停留し、イベントが終了すると別のロケーションに戻ります。プリセット ロケーションへの移動と同時に、ビットレートは 1M から 3M に、フレーム レートは 4 fps から 8 fps に増加します。ビットレート / fps の変更は、イベント終了時に元の状態に戻ります。

Event List (イベント リスト)

最大 10 件のイベント ルールの定義が可能で、これらは **Event List** (イベントリスト) パネルに短縮形で表示されます。各イベント ID の下には、イベントが有効となる曜日、アクティブ期間の開始時刻と持続時間、トリガー ソースのタイプ、レスポンスに使用するアクションが表示されます。行がグレー表示されている場合は、そのルールが現在無効で非アクティブになっていることを示します。

Event List					
ID	Week Day	Start	Duration	Source	Action
1	1234567	00:00	24:00	MD1	CMD1
2	1234567	00:00	24:00	NONE	NONE
3	1234567	00:00	24:00	NONE	NONE
4	1234567	00:00	24:00	NONE	NONE
5	1234567	00:00	24:00	NONE	NONE
6	1234567	00:00	24:00	NONE	NONE
7	1234567	00:00	24:00	NONE	NONE
8	1234567	00:00	24:00	NONE	NONE
9	1234567	00:00	24:00	NONE	NONE
10	1234567	00:00	24:00	NONE	NONE

リストのイベント ID 番号をクリックすると、新規イベントの作成を開始できます (例 2)。イベント ルールは複数の要素から構成されます:

アクティブになる時間:

ルールの有効/無効を選択できます。イベント ルールが無効の場合でも、設定は内部メモリに保存されます。週サイクルで、このルールとスケジュールがアクティブになる曜日を選択してください。

アクティブ期間の開始時刻と持続時間を決定します。例えば、動体検知をトリガーとしてスナップショットを FTP にアップロードする、というルールが毎日 19:00 以降 12 時間実行されたとします。このルールは、この時間外ではアクティブになりません。

以下の例では、イベント ハンドラ ルールが毎日 24 時間アクティブになります。

Event List 1

Enabled

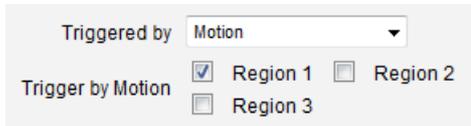
Active on Mon Tue Wed Thr
 Fri Sat Sun

Time 00 : 00

Duration 24 : 00 (max. 168:00 hours)

イベントのトリガー条件:

イベントは複数あるソースのいずれかによってトリガーされます。以下の例では、動体検知領域 1 がイベント トリガーとして使用されます。



Triggered by: Motion

Trigger by Motion: Region 1 Region 2 Region 3

この予定時間の中にイベントが繰り返しトリガーされるよう設定することも可能です。間隔は分単位で決定します。この機能を使用すれば、一定間隔でスナップショットを撮影し、E メール/FTP でアップロードすることも可能です。

Dis: デジタル入力でトリガーできる IP デバイスは選択したモデルに限定されます。

Motion (モーション) : 1 ヶ所以上の動体検知領域でモーション トリガーが発生した場合に、イベントをトリガーできます。いずれの領域のトリガーでもイベントは開始します。イベントの持続時間は、「Video Adjust (ビデオ調整) ページ」の「Motion Detection (動体検知)」セクションで定義されている「MD トリガー長」、または「トリガー間隔」と同じです。

Video Loss (ビデオ ロス) : これはビデオ サーバーでのみ使用できます。アナログ ビデオ入力 が喪失すると、ビデオ状態は「喪失」となり、デバイスがアナログ ビデオ信号を受信して漸く「通常」に戻ります。一般的には、ビデオの喪失時にビデオサーバーが管理者に E メールを送信し、DO 信号を始動して、アナログ信号が復元するまでアラームを発信するといった状況に使用されます。

Switch to Night mode (ナイト モードへの切り替え) : これは選択したモデルのみ使用可能です。カメラがデイ / ナイトモードの切り替えを行うと、埋め込みイベント ハンドラがこの変更を察知し、この情報に基づいて作動します。

動体検知プロファイルを別のイベント MD パラメーター式に変換するといった利用も可能です。昼夜それぞれに合わせて最適化された 2 セットのパラメータを備えることにより、昼夜どちらの状況でも精度を全体的に向上することができます。夜間限定の MD 領域も、場合によってこの方法で作動できます。カメラがデイモードに戻ると、イベント期間は終了し、カメラは元の設定にリセットされます。

Device boots successfully (デバイス正常起動) : デバイスが起動すると、イベント レスポンスをトリガーします。これを使用すれば、デバイス再起動時の記録を E メール経由で保存する通知システムを作成できます。

Reboot device (デバイスの再起動) : デバイスのシャットダウン時に、Web UI 「Save and Reboot (保存して再起動)」経由でイベント レスポンスをトリガーします。これを使用して、デバイス設定編集時の記録を保存します。デバイスの電源が抜かれた場合は、正常なシャットダウンではないため、この機能が有効にならないことにご注意ください。

発生するレスポンスの種類

- Response To
- Send notification message
 - Upload video/snapshots
 - Change Motion Detection Profile
 - Send URL command

Digital Output (デジタル出力) (選択モデルのみ) これは他のデバイスに便利なリンクです。クリックして、本ルールへのレスポンスにこれを追加します。

Send notification Message (通知メッセージの送信) : 「Event Configuration (イベント構成)」セクションでセットアップした 3 つの定義済みメッセージから選択します。同時に複数のメッセージを有効にできます。E メールを送信する場合、受信者はイベント ルール 1 件につき一か所に限定してください。複数の受信者に E メールを送信する必要がある場合は、同じトリガーで作動する個々のイベント ルールを使用してください。

Upload video/snapshots (ビデオ/スナップショットのアップロード) : このレスポンス セットに含めるイベント構成を選択します。E メールでアップロード ビデオを送信し、同時に通知メッセージを送信する場合、システムは自動的に 2 つの E メールを 1 つに結合します。件名と画像は、有効となっているイベント構成の「スナップショットのアップロード」に基づきますが、本文テキストのメッセージは通知メッセージに基づき構成されます。

一般的に、最良のパフォーマンスを得るには、「1 イベント ルールにつき 1 E メール」の制限に従ってください。

Change Motion Detection profile (動体検知プロファイルの変更) : これは、選択した動体検知領域のプロファイルをランタイム プロファイルからイベント プロファイルに切り替えます。プロファイルは、このイベントが終了するとランタイム設定に戻ります。1 つの動体検知領域をランタイム時に無効にするようプログラムできますが、ある状況下でイベント ハンドラを使ってそれを有効にすることができます。

Send URL command (URL コマンドの送信) : レスポンス セットに含める URL コマンドを選択します。イベントのトリガー時とトリガー解除時に、2 つの異なるコマンドが送信されます。

Change to Night Mode (ナイト モードへの変更) (選択モデルのみ) : モデルによっては、カメラにナイト モードを強制適用できます。イベントが終了すると、カメラは (自動または強制適用のデイ/ナイトに関わらず) 前の設定に戻ります。

Go to a preset point (プリセット ポイントに進む) : デバイスが PTZ カメラの場合は、プリセット ポイントが PTZ セットアップ ページで構成済みとなっていますので、Send URL Command (URL コマンドの送信) の方法を使って、イベント ルールのレスポンス セクションにこの機能を含めることができます。イベント終了時に、カメラを別のプリセット ポイントに戻すことができます。

上記項目を変更してから、Apply (適用) を押して変更を保存します。Reset (リセット) ボタンは、今しがた変更が行われ、まだ適用されていない更新内容を元に戻します。

Manual Event (手動イベント)

イベント リスト下にある Manual Event (手動イベント) エリアで、Web ユーザー インターフェース経由にてトリガーするイベントを一つ選択できます。



上記項目を変更してから、Apply (適用) を押して変更を保存します。Reset (リセット) ボタンは、今しがた変更が行われ、まだ適用されていない更新内容を元に戻します。

一度選択すると、ビデオ表示画面のトリガー ボタンがクリック可能になります。クリックして、選択したイベントをトリガーします。これは、イベント ルールのテスト中に役立ちます。

ライブ ビュー パネルは以下のように表示されます。



システム

System

System (システム) セクションでは、カメラの管理に役立つ機能のリストが提供されます。**System (システム)** の前に表示される **[+]** マークは、これをクリックすることによりリストを展開できることを示しています。リストを展開後に **[-]** マークをクリックすると、もう一度リストを閉じることができます。

User Account (ユーザー アカウント)

User Account

User Account (ユーザー アカウント) のセクションでは、次のユーザー管理タスクを実行できます。

1. カメラのフル アクセス権を持つルート アカウントのアカウント名またはパスワードを変更する。
2. ライブ表示と PTZ コントロールのアクセス権のみを持つ一般ユーザーを最大 10 件作成する。
3. ユーザー名とパスワード不要 (匿名ログイン) でライブ表示を見るオプションを有効/無効にする。これは現場のカメラ設置者にとって特に便利な機能です。安全上の理由から、**Web** コンフィギュレータのセットアップ ページに入るとき、また **URL** コマンドでカメラへのアクセスや設定変更を試みる際には、常にアカウント名とパスワードが必要となります。

User Account

Live view without account name and password

User	Account	Password
Root	<input type="text" value="admin"/>	<input type="text" value="123456"/>
User 1	<input type="text"/>	<input type="text"/>
User 2	<input type="text"/>	<input type="text"/>
User 3	<input type="text"/>	<input type="text"/>
User 4	<input type="text"/>	<input type="text"/>
User 5	<input type="text"/>	<input type="text"/>
User 6	<input type="text"/>	<input type="text"/>
User 7	<input type="text"/>	<input type="text"/>
User 8	<input type="text"/>	<input type="text"/>
User 9	<input type="text"/>	<input type="text"/>
User 10	<input type="text"/>	<input type="text"/>

上記項目を変更してから、**Apply (適用)** を押して変更を保存します。**Reset (リセット)** ボタンは、今しがた変更が行われ、まだ適用されていない更新内容を元に戻します。

System Info (システム情報)

System Info

System Info (システム情報) のセクションでは、カメラの状態、設定、ログに関する完全な情報が提供されます。この情報は、カメラの構成、メンテナンス、トラブルシューティングを実行する際に大変役立ちます。

System Information

System Information :

```

Firmware Version = A1D-500-V6.01.03-AC
MAC Address = 00:0F:7C:08:D9:FE
Production ID = D11-AA-02-12G-00015
Factory Default Type = No Audio (0x11)
Company Name = /
Web Site = \
Profile ID = OV9715-DA1_V120308A
Sensor Board = OV9715
    
```

WAN Status :

```

WAN_TYPE='1'
WAN_IP='172.16.26.201'
WAN_NETMASK='255.255.255.0'
WAN_GATEWAY='172.16.26.253'
DNS_PRIMARY='172.16.5.20'
DNS_SECONDARY='172.16.5.19'
MAC='00:0F:7C:08:D9:FE'
BONJOUR_CONFIG='1,D11-AA-02-12G-00015'
    
```

System Log :

```

Mount jffs2 filesystem
Devcap Version D11_20120713_01
Bootloader Version BOOTLOADER-500-V01.04
Loading GetJiffies driver
Initiating factory button ...
Loading System Config files ...
Starting Streaming Core ...
Initial system time manager ...
    
```

Config file:

The unit's parameters and their current settings. Parameter List

Always attach the server report when contacting your support channel. Server Report

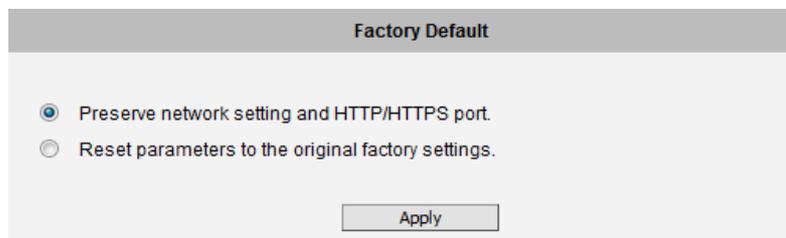
Third party software licenses. Show License

Server Report (サーバー レポート) は、カメラ関連情報をテクニカル サポート チームに送信して、いち早いサービスが受けられるよう、その情報の完全なリストをテキスト形式でエクスポートするための便利な方法です。

Factory Default (工場出荷時設定)

Factory Default

Factory Default (工場出荷時設定) セクションでは、カメラの設定を元の工場出荷時設定にリセットできます。



Factory Default

- Preserve network setting and HTTP/HTTPS port.
- Reset parameters to the original factory settings.

Apply

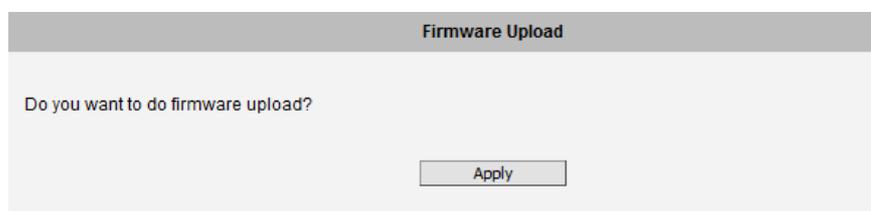
ネットワーク設定を保持し、他の設定を工場出荷時設定に復元する場合は、最初のオプションを選択してください。代わりに 2 番目のオプションを選択すると、工場出荷時設定中にすべての設定が削除され、工場出荷時の既定 IP 設定で本カメラに接続しなければなりません。

Firmware Upload (ファームウェアのアップロード)

Firmware Upload

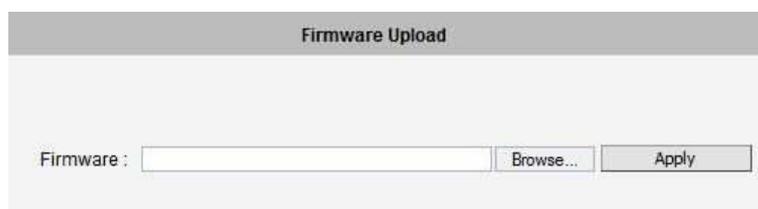
Firmware Upload (ファームウェアのアップロード) セクションでは、カメラのファームウェアをリモートでアップグレード/ダウングレードできます。より新しいバージョンへのアップグレードは、通常新しい機能を手したり、既存のバグや制限を修正したりするために実行します。一方、古いバージョンへのダウングレードは、新規購入したカメラ機種が搭載するファームウェアが、特定プロジェクトのサードパーティ管理システムにサポートされるバージョンより新しい場合など、統合の目的で使用されることがほとんどです。

ファームウェアの画像ファイルは Web サイトからダウンロードできます。ファイルには「.upg」というファイル拡張子が付いています。



The screenshot shows a dialog box titled "Firmware Upload". The main text asks "Do you want to do firmware upload?". At the bottom center, there is a single button labeled "Apply".

Apply (適用) ボタンを押すと、Web コンフィギュレータを実行中のコンピュータにダウンロード済みの、ファームウェアの画像ファイルを開覧できます。



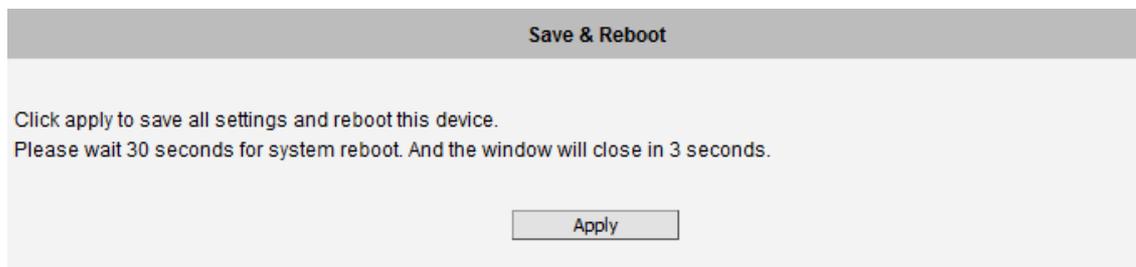
The screenshot shows a dialog box titled "Firmware Upload". It features a text input field labeled "Firmware:" followed by a "Browse..." button and an "Apply" button.

Browse (閲覧) をクリックし、アップロードする画像ファイルを選択します。**Apply (適用)** ボタンをクリックしてアップロードを開始します。
プロセスが終了すると、「OK」のメッセージが表示され、システムが再起動します。

Save & Reboot (保存して再起動)

Save & Reboot

Save & Reboot (保存して再起動) セクションでは、リモートで設定を保存してカメラを再起動できます。保存して再起動しないと有効にならない設定がありますので、この機能は重要です。



Logout (ログアウト)

Logout

この項目をクリックすると IP デバイスからログアウトできます。Web コンフィギュレータを使ってすべてのタスクを完了したら、必ずこの IP デバイスからログアウトしてください。

Troubleshooting (トラブルシューティング)

カメラのデフォルト設定が 9 割の状況に理想的であっても、まれに設定調整やデバイスの検証が必要になる場合があります。次のセクションでは、大抵の場合に対応する簡単なトラブルシューティング ソリューションを提供します。場合によって、特定の環境に合わない製品を選択したために、予期せぬ現象が発生することがあります。

各状況の詳細な説明と指示については、完全な **Troubleshooting Guide (トラブルシューティング ガイド)** を参照してください (http://www.acti.com/kb/detail.asp?KB_ID=KB20130130001)

画質のトラブル シューティング	
問題	解決法
モーション ブラー	シャッター速度を上げる
ぼやけた画像	Auto Focus (自動フォーカス) : Refocus (リフォーカス) ボタン; Manual focus (手動フォーカス) : 手動で調整
DoF が狭すぎる	絞り値を下げて画角を広げる、カメラをオブジェクトからさらに離して設置する
画角が狭すぎる	バリフォーカル レンズ: 画角を広げる; ズーム レンズ: ズームアウト ボタンを押す; 固定レンズ: 広角固定レンズと交換する、または広角レンズ搭載の別モデルを選択する
オブジェクトが小さすぎる	ビデオ解像度を上げる; ズームイン (ズーム レンズ) またはレンズを望遠ポジションに調整 (バリフォーカル); カメラをターゲットにさらに近づけて設置する; 焦点距離がさらに長いレンズに変える; カメラを解像度がさらに高い、または焦点距離がさらに長いモデルに変える
露出不足の画像	自動露出モードを使用して、 AE 参照ターゲット を上げる; 最低速自動シャッター スピードを最低速 (1/5 秒) に設定する; 外部光源を追加して、カメラの撮影範囲を明るくする
露出過度の画像	自動露出モードを使用し、必要な場合は AE 参照ターゲット を下げる
ノイズ	DNR を有効にする; 絞り値を上げる; 自動露出モードの AE 参照ターゲット を下げる; 手動露出モードの露出ゲインを下げる; ビデオ解像度を下げる; 可視光または赤外光をさらに追加する
ブロックノイズ & モザイク	ビットレートを上げる
色違いまたはカラーローリング	白紙と自動ホワイト バランス モードの「 Hold (保留) 」ボタンを使って、手動で色を補正する; カメラの位置と監視方向を調整する; 光源を調整する
真っ暗な画像	十分な光があるか確認する; デイ/ナイト モードと IR LED コントロールがどちらも自動モードになっているか確認する; 「 デイ モードからナイト モードへの切り替え 」が最も極端な値 (100) になっていないことを確認する; 手動アイリス: リングを「 O 」の方に回転してアイリスを開く; 設置の間、レンズの保護キャップを取り外す

赤外光反射	ドーム カバーやバレット カバーがしっかり取り付けられているか確認する; 自動露出モードの AE 参照ターゲットを下げる; 手動露出モードの露出ゲインを下げる
-------	---

ストリーミングの品質に関するトラブルシューティング	
夜間のフレーム レートが低すぎる	自動露出モードで、最低速自動シャッター スピードがフレーム間隔より遅くならないよう設定する; 手動露出モードで、シャッター スピードがフレーム間隔より遅くならないよう設定する
遅延	デュアル ストリームを使用する (ストリーム 1 は録画用、ストリーム 2 はライブ表示用); ビットレートを下げる; 解像度を下げる (ユーザーが承諾できる場合); ケーブルの品質を確認する; 必ず産業グレードのスイッチとルーターを使用する; NVR マニュアルの NVR サーバー & クライアント PC の要件を確認する
ジッタ (ぶれ)	ライブ表示と再生には、ビデオ スムージング アルゴリズム対応の NVR を使用する
欠落フレーム	NVR の再生機能を使用- フレームが欠落しているかを確認するには、ぶれて見える部分にコマ送り検証を使用する; データ スイッチ/ルーターと VMS コンピュータの問題を解決するには、カメラ メーカーのテクニカル サポート チームに相談することも可能です。