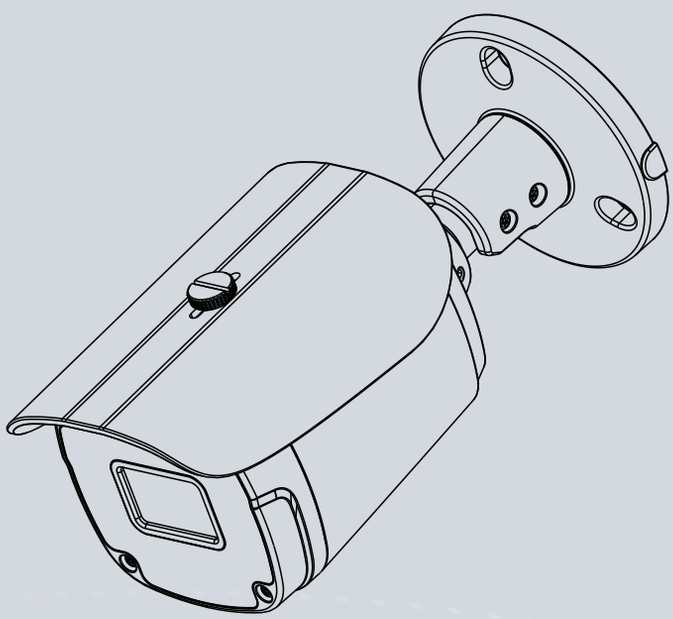
IB9368-HT
IB9388-HT バレット型 ネットワークカメラ

ユーザーズマニュアル

（参考用）

5MP/2MP • 屋外設置• IP66 • IK10 • デイナイト機能 • リモートフォーカス
WDR Pro • スマートストリーム III • SNV • 30M スマート IR



Rev. 1.0

この製品マニュアルは、ビボテックジャパンが日本のお客様向けに日本語で作成した参考用の資料です。
より詳細な内容、最新のバージョンについては、VIVOTEKウェブサイトの製品ページより英語版をダウンロードのうえご参照ください。

目次

安全上のご注意 4
廃棄について 4
概要 4
改定履歴 5
ご使用になる前に 6
内容物のご確認 6
本書中の記号および記述 6
各部の名称 7
ハードウェアのインストール 9
カメラの取り付け 10
ソフトウェアのインストール 16
ネットワークへの接続 22
セットアップ 23
ネットワークカメラに接続 26
ウェブブラウザで接続 26
RTSP プレーヤーで接続 29
3GPP 互換モバイルデバイスで接続 29
VIVOTEK 録画ソフトウェアからのアクセス 31
メインページ 32
クライアントの設定 37
設定 42
System（システム） > General settings（一般設定） 43
System（システム） > Homepage layout（ホーム画面レイアウト） 45
System（システム） > Logs（ログ） 48
System （システム）> Parameters（パラメータ） 50
System > Maintenance 51
Media（メディア） > Image（画像） 55
Media > Video 69
Media > Video 70
Media > Video 71
Network > General settings 80
Network > Streaming protocols 87
Network > DDNS 91
Network > SNMP (Simple Network Management Protocol) 96
Network > FTP 97
Security > User accounts 98
Security > HTTPS (Hypertext Transfer Protocol over SSL) 100
Security > Access List 107
PTZ > PTZ settings 113
Event > Event settings 117
Applications > Motion detection 131
Applications > Tampering detection 134
Applications > Package management - a.k.a., VADP (VIVOTEK Application Development Platform) 135
Recording > Recording settings 138

Local storage > SD card management 143
Local storage > Content management 144
Appendix 147
URL Commands for the Network Camera 147
Technology License Notice 148
VCCI 規制について 149
責任 149
製品の譲渡または売却時のご注意 149

安全上のご注意

- 本機に物を落としたり、強い衝撃を与えないで下さい。
- 本機のカバーの上に物を置かないで下さい。
- 本機から熱や煙が出た場合、ただちに使用をやめ本機からプラグを抜いて下さい。
- 異常がある場合は、お買い上げ取扱店へご連絡ください。
- 本機の分解、部品の取替えは、危険がある為　行わないで下さい。
- 感電の危険性があるため、カバーを外さないで下さい。
- 外観に破損がないかどうか確認してください。破損が見られた場合は使用を中止してください。
- アークや火花が生じる恐れのある場所を避けて使用して下さい。通気口をふさがないで下さい。
- 本機は、乾燥した涼しい風通しの良い空間で保管・使用をして下さい。また、燃えやすい物から離れた場所で保管・使用をして下さい。内部を冷却するためのファンが組み込まれている機器では、本機の前後に物を置かず、スペースを空けて下さい。
- 感電の危険性を減らすことと、腐食の防止のため、屋外設置ができない機器は雨や水しぶきのかかる場所で保管・使用をしないで下さい。
- 本機を使用していない時は、入力 / 出力プラグを取り外して下さい。
- 保証期間内であっても不正改造を発見した場合、保証の対象外とします。

廃棄について

企業でご使用のお客さまは、本製品を産業廃棄物として扱ってください。
本製品を廃棄するときは、地方自治体の条例または規則に従って処理してください。

概要

IB9368、IB9388シリーズは、WDRオンにした状態で、2560×1920の解像度で20 fpsの撮影が可能なバレット型ネットワークカメラです。2MPのIB9368は、1920×1080の解像度で30fpsを実現しています。5MPの解像度でWDR機能を有効にした場合、IB9388のフレームレートは20fpsに若干低下します。最新のVIVOTEK WDR Proテクノロジーを搭載したこのカメラシリーズは、逆光や低照度のシーンでも、高画質映像を実現します。

リモートフォーカスレンズを使えば、気になる部分を自由な距離で撮影することができます。自由な距離範囲で撮影することができます。また、設置のしやすさも実現しています。

カメラは最大120dBの効果でWDR機能に対応しています。このモデルは 万が一、ネットワークが遮断された場合でも、MicroSDカードに保存されているローカルビデオをサポートします。
また、最大5つのプライバシーマスク領域を設定可能な動体検知およびいたずら検知機能を搭載しています。最大5つのプライバシーマスク領域を設定できます。

改定履歴

■ 1.0: 初期リリース

ご使用になる前に

ご使用される国によって、監視デバイスの使用が禁止されている場合があります。ネットワークカメラは高性能のWeb対応カメラであるだけでなくフレキシブルな監視システムの一部でもあります。 本体を取り付ける前に、このような監視デバイスの運用が合法であることをお確かめください。使用する地域の法律に抵触するご使用の結果生じた事故、損害の発生等については、当社は一切の責任を負いかねます。予めご了承ください。

本製品をお使いになる前に、P6[内容物のご確認]に記載されている内容がすべて揃っているかを必ずお確かめください。また、本製品を取り付ける前に、クイックインストレーションガイドの注意事項をお読みください。誤った組立てや取付けによる破損や故障を防止するため、P9[カメラの取付け]の説明に従ってください。

本製品はネットワークデバイスであり、ネットワークに関する基本的な知識があれば簡単に使用することができます。また、ビデオ共有、一般的なセキュリティ/監視などを含む様々なアプリケーション用に設計されています。設定の章では、ネットワークカメラを最大限に活用し、適切な動作を実現する方法を提案します。既存のホーム画面のカスタマイズや現在のWebサーバとの統合については、URL コマンドマニュアルをご参照ください。

内容物のご確認

- IB9368-HT または IB9388-HT
- スクリューパックとサイドカバー。
- 取付ネジ一式。
- クイックインストレーション・ガイド。
- ケーブルグランド。

⚠ 警告：

1.本製品は赤外線を放射します。
2.適切な遮蔽物または眼を保護する器具を使用してください。

本書中の記号および記述

INFORMATION: 誤動作や問題の発生を防止するために役立つ重要なメッセージやアドバイスを提供します。

ノート： 製品を正常に動作させるために必要なガイダンスまたはアドバイスです。

ヒント： インストール、機能、またはプロセスをより円滑に行うための有用な情報です。

警告または重要： 製品または使用者に対して危険または危害が生じ得る状況を示します。

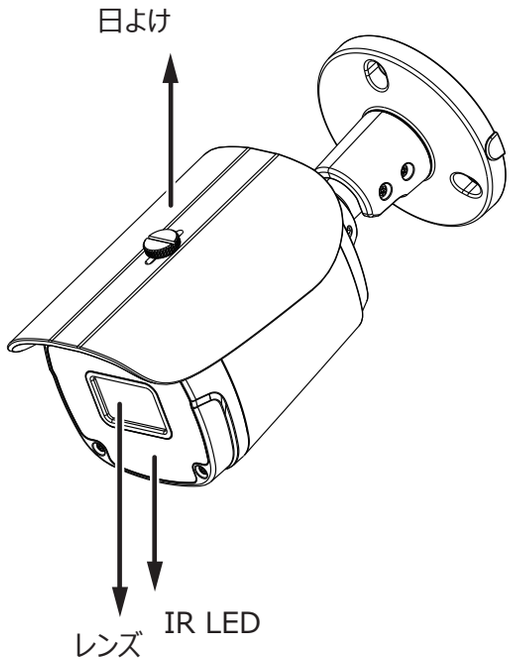
電気的危険： 使用者に高電圧による感電の危険性があるときに表示されます。

⚠ 重要:

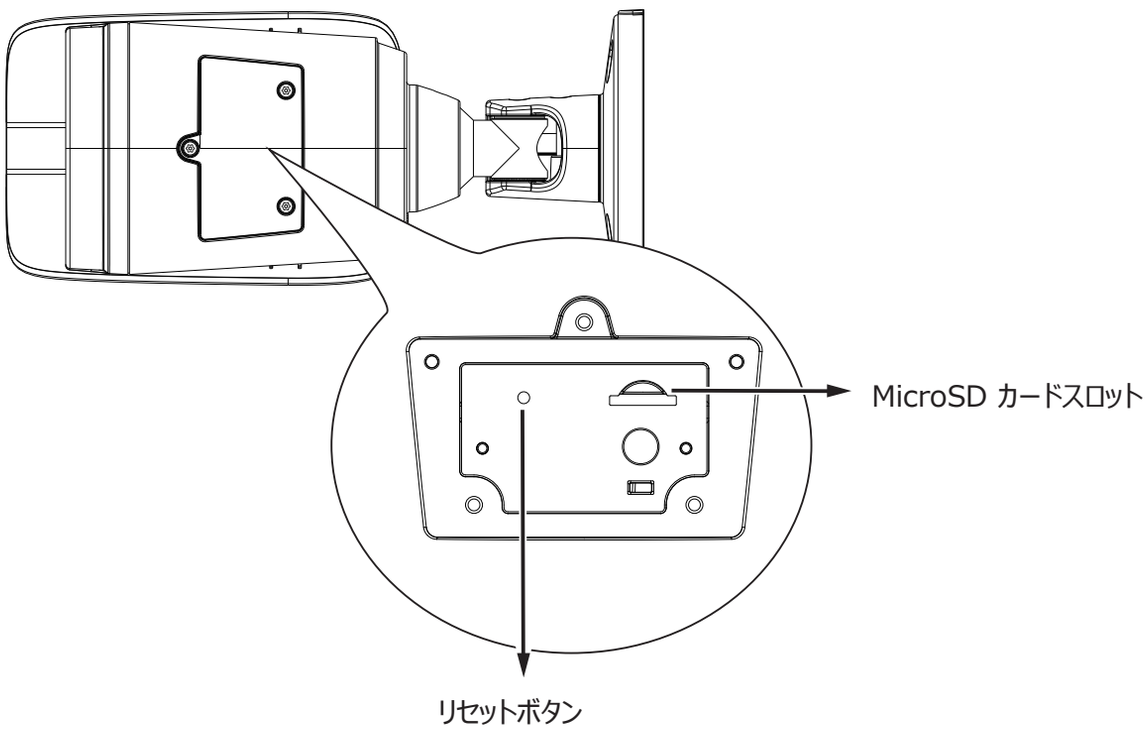
本製品は屋内に配線された PoE ネットワークに接続してください。

製品外観

外側



下部

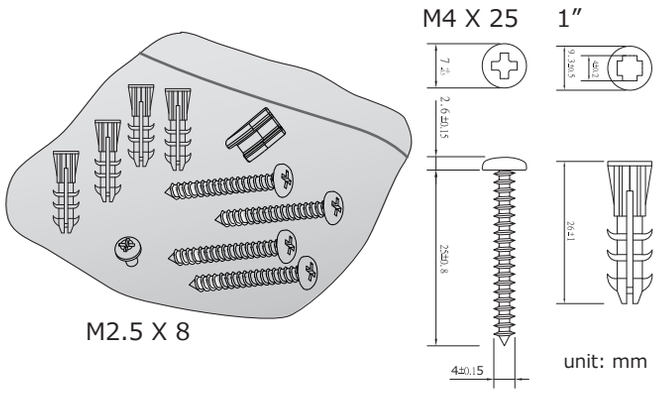


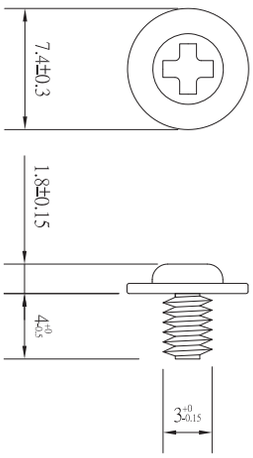
ノート：

モデル名末尾のアルファベットは下記の機能を表します。

E	広範囲な環境温度に対応するためのヒーターを搭載
Fx	焦点距離（x はその値）
T	リモートフォーカスレンズ付きリモートフォーカスレンズ付き
R	PoE リピータ搭載
H	ワイドダイナミックレンジ機能搭載

ネジ

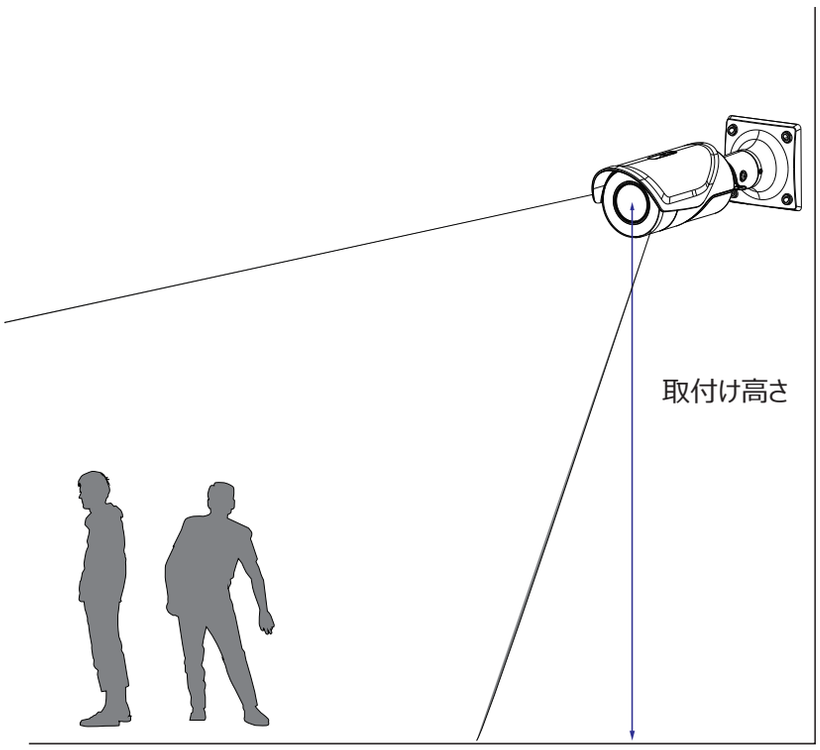




ハードウェアのインストール

⚠ 重要:

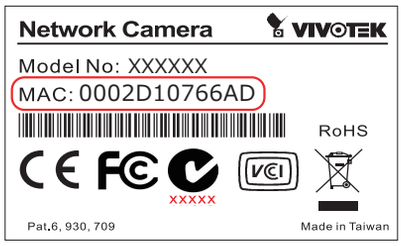
スマートモーション検出、スマート VCA の機能を使用する場合は、必ずカメラの高さを測定してください。高さ情報は映像分析結果の精度にとって重要です。その他の遠近情報は、内蔵のセンサーによって自動的に収集されます。高さ情報をもとに、視野の水平および垂直キーストーン補正を行います。





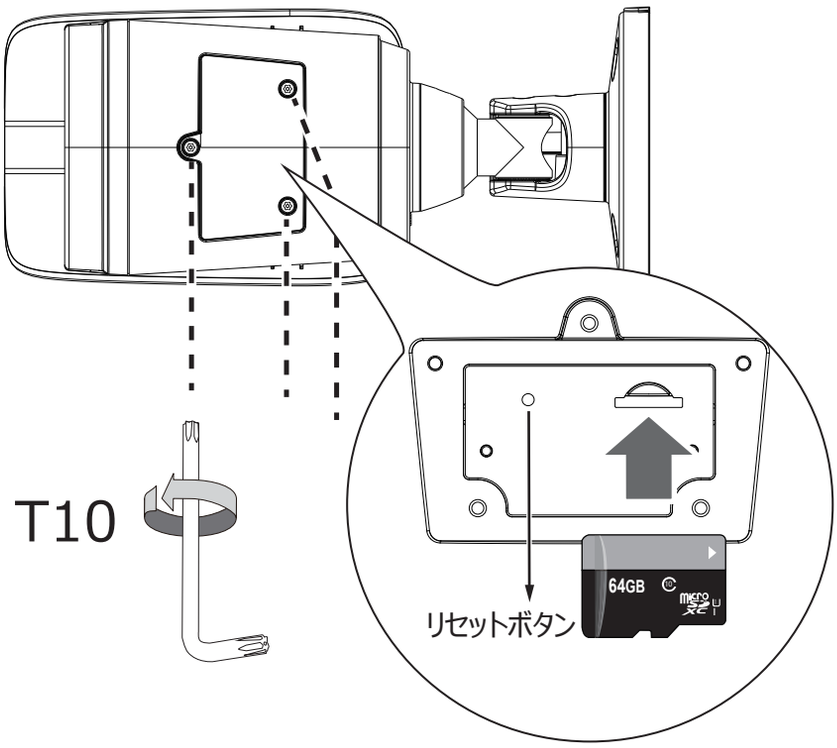
カメラの取り付け

1. 後で参照できるように、カメラの MAC アドレスを書き留めます。

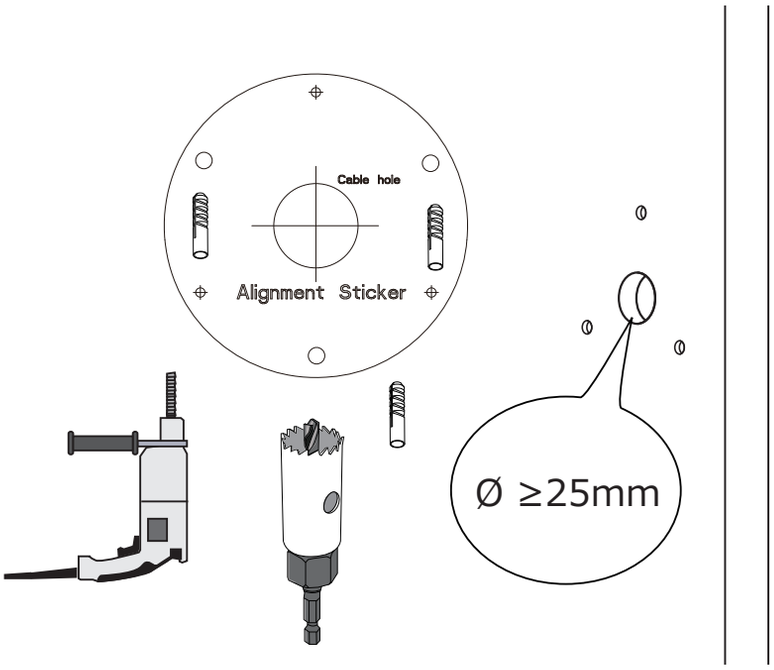




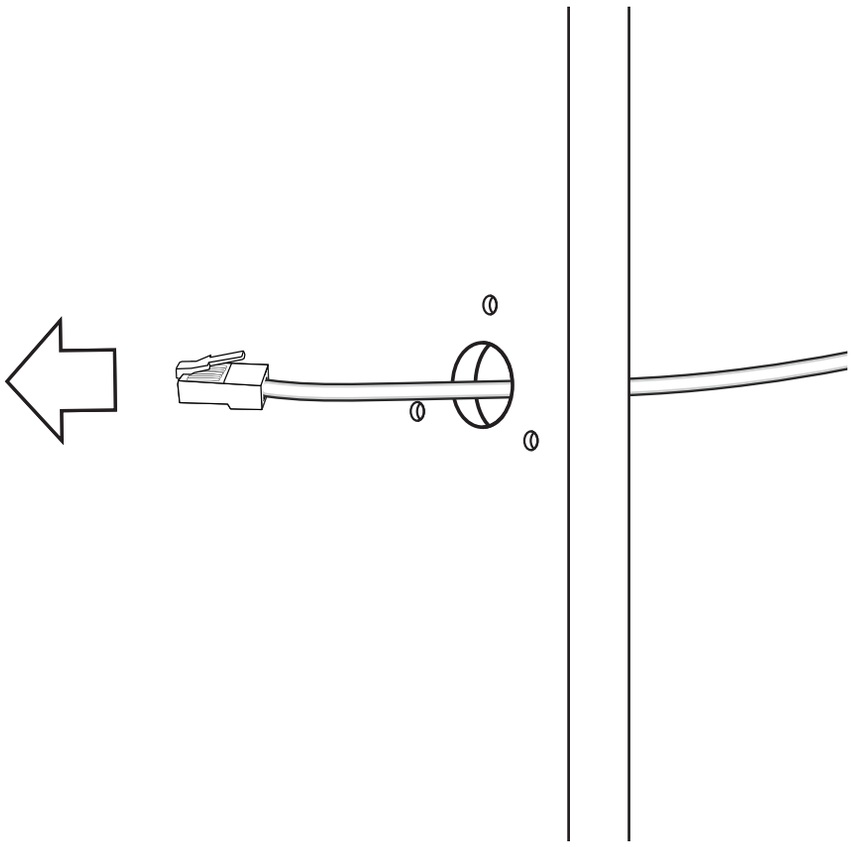
2. SD カードを利用する場合は、T10 のトルクスレンチ（同梱されていません。）でカメラ本体にあるバーをネジを緩めて取り外し、MicroSD カードを挿入してください。



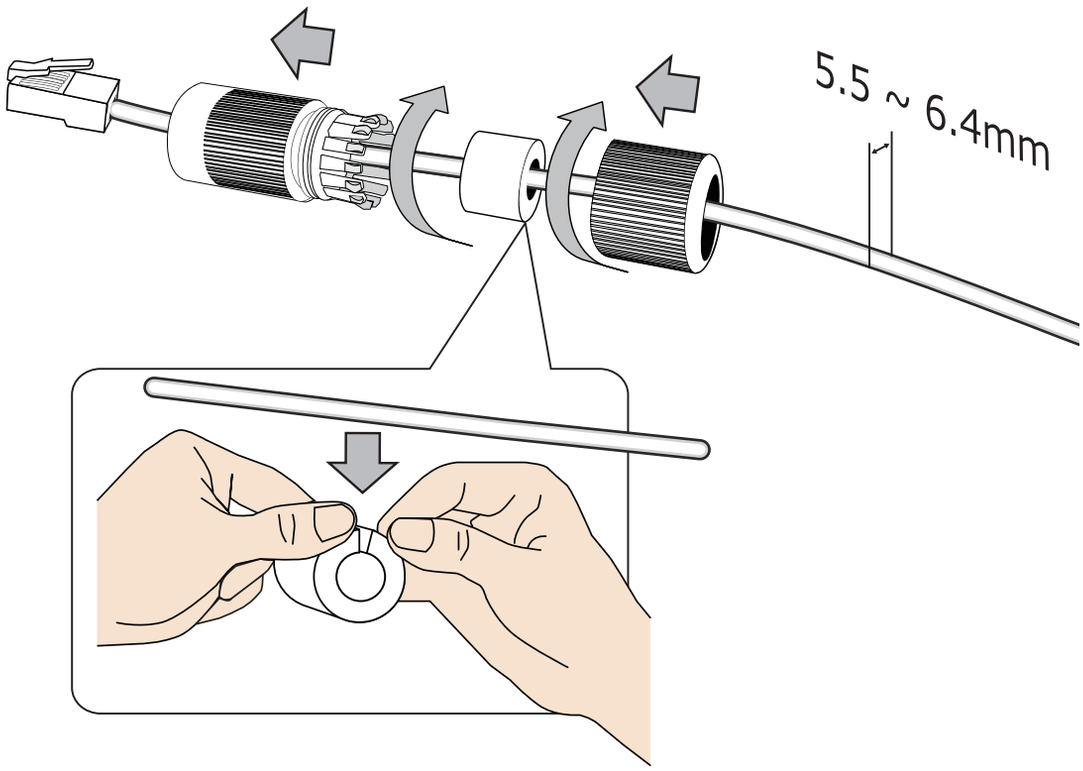
3. アライメントステッカーを使用して、壁にドリルで取付けネジ用の穴を開けます。必要に応じて、さらにケーブル配線穴を開けます。



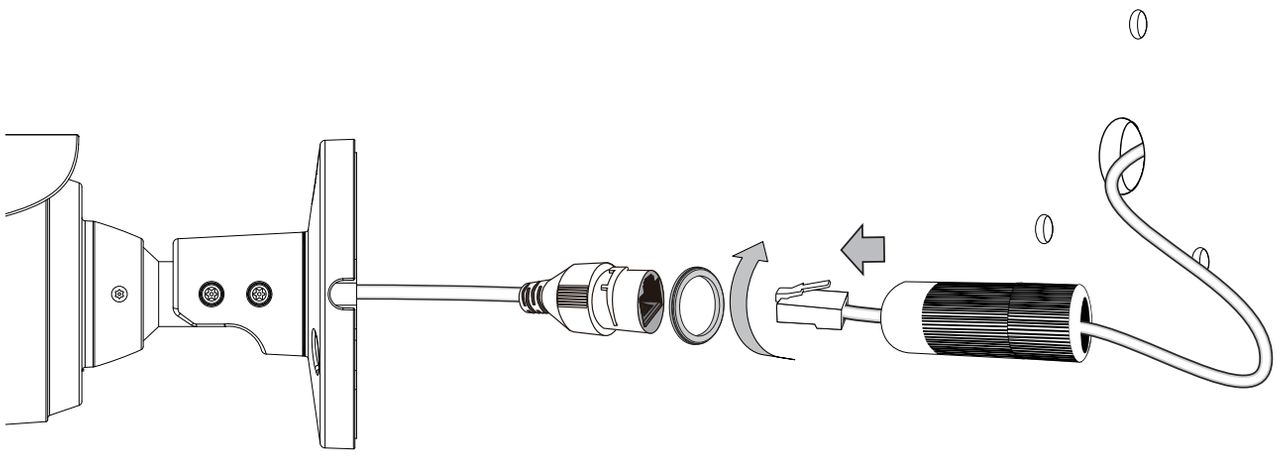
4. ケーブル配線穴にイーサネットケーブルを通します。



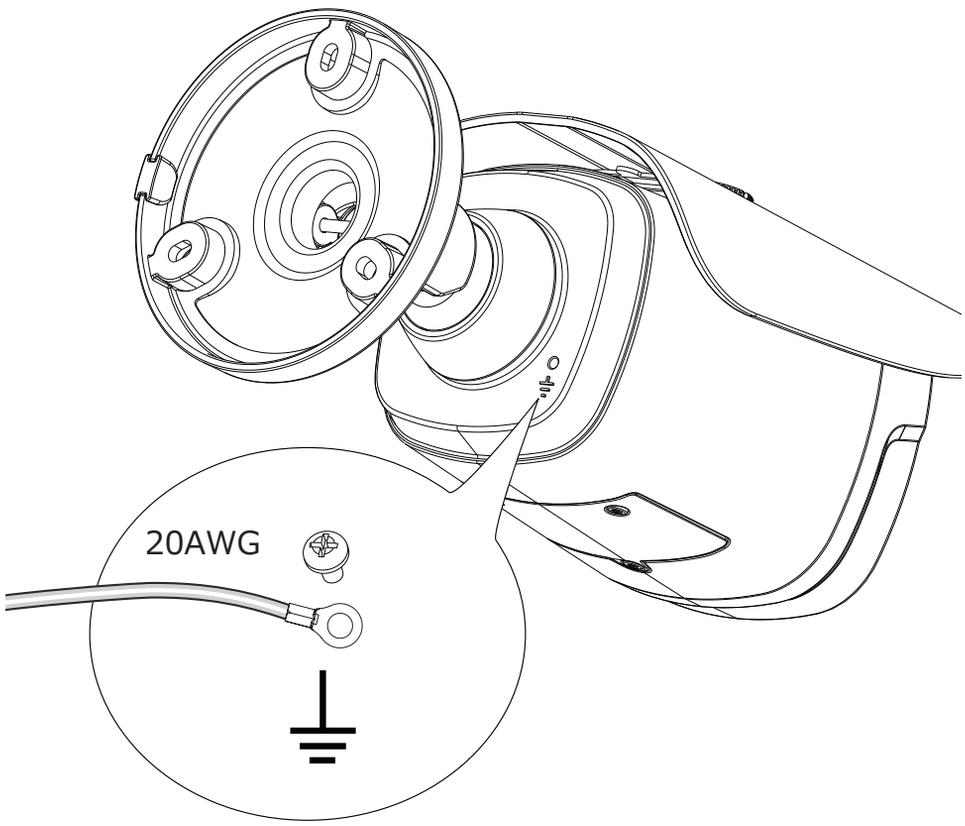
5. イーサネットケーブルを、下図のように、ケーブルグランドの部品に通し、締め付けます。



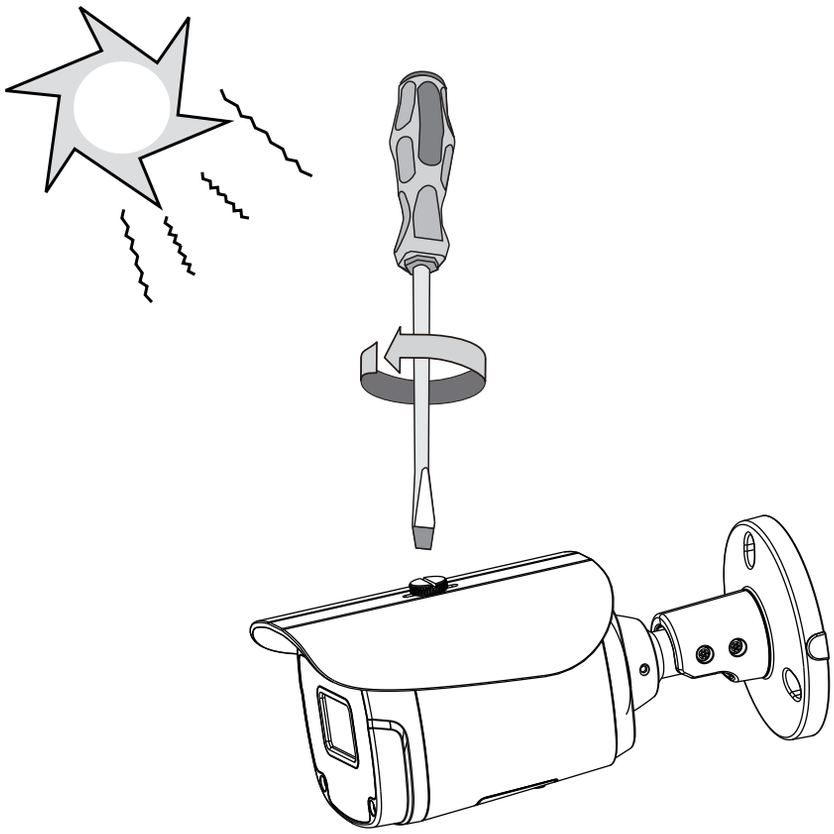
6. シールリングを挟み込んでカメラの RJ-45 コネクタに接続し、防水コネクタを締め付けます。



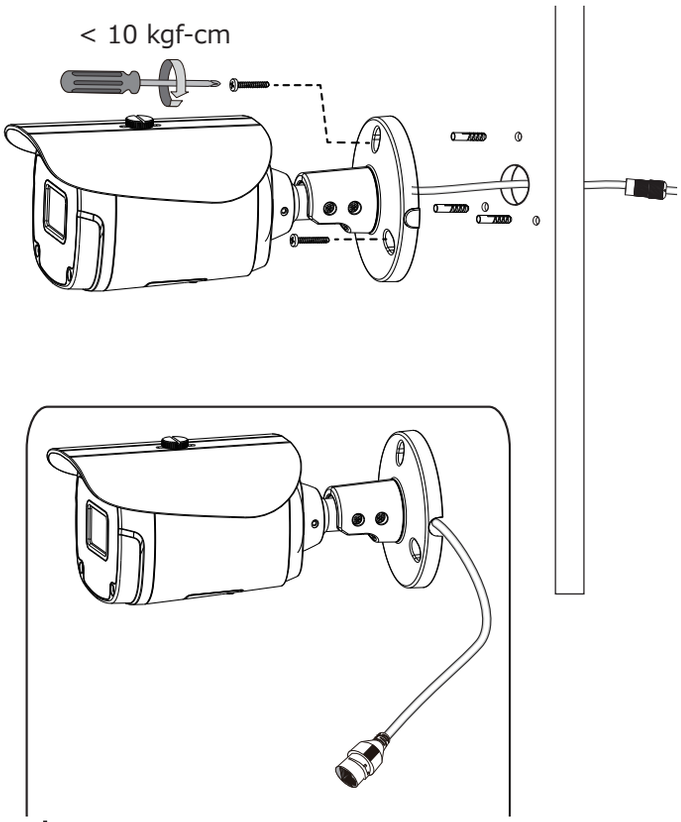
7. 付属のネジを使用して、アース線をカメラ背面のアース位置に接続します。



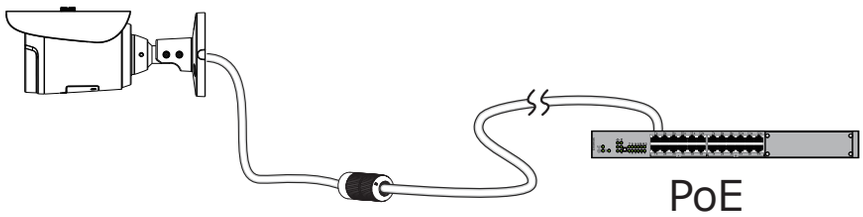
8. ねじをしっかりと締め付けて、日よけを取り付けます。

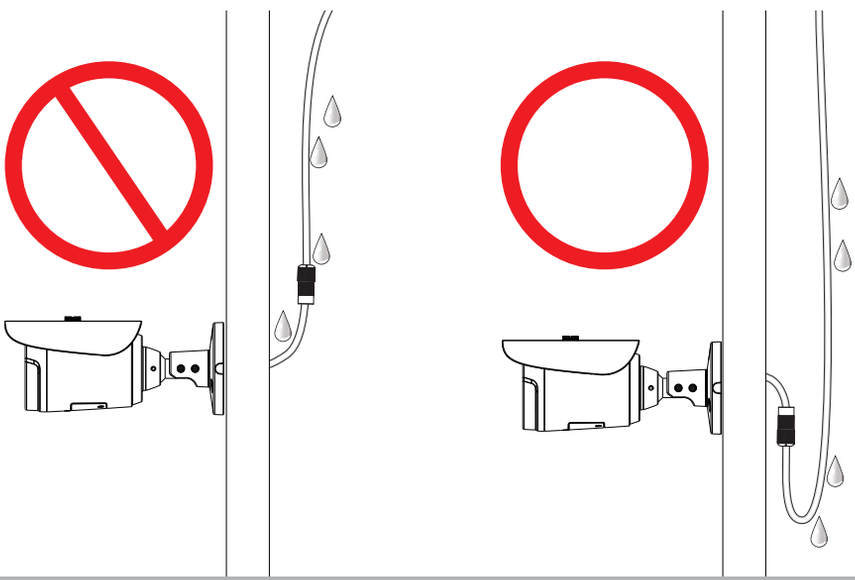


9. 付属のネジ、アンカーを使用してカメラを取り付けます。（取り付ける場所によって付属のネジ、アンカーがご利用できない場合、お客様で最適なネジ、アンカーをご用意ください。）壁に配線穴を開けることができない場合は、取付金具側面の開口部からケーブルを配線することもできます。



配線には下の図のように水切り部を設け、水滴が接続部または本体に接触しないようにしてください。





10. VIVOTEK のウェブサイトにアクセスして、ソフトウェアユーティリティ [Shepherd] をインストールしてください。このプログラムは、同じ LAN 上にあるビデオレシーバー、ビデオサーバー、ネットワークカメラを検索します。

[Shepherd] にあるカメラの MAC アドレスをダブルクリックして、カメラの Web コンソールを開きます。

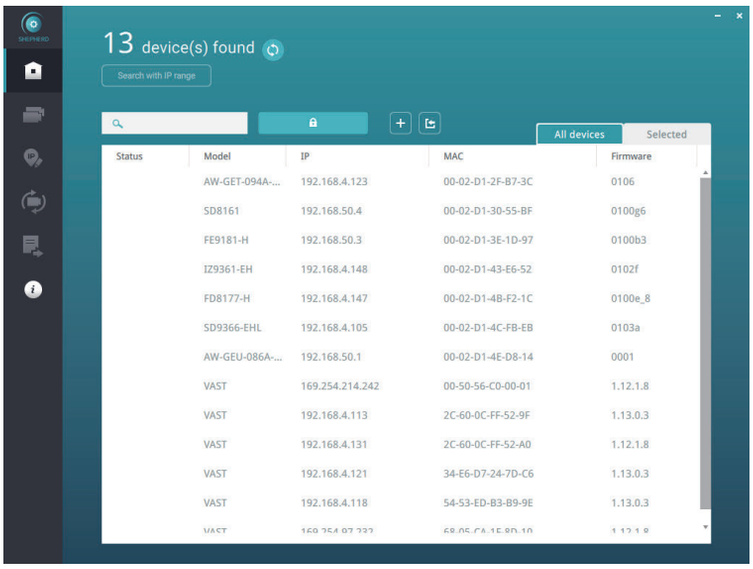


ソフトウェアのインストール

11. Shepherd ユーティリティをインストールします。これは、ローカルネットワークでネットワークカメラを見つけて構成するのに役立ちます。カメラに CD が付属していない場合は、VIVOTEK の Web サイトにアクセスし、[ダウンロード]> [ソフトウェア] ページでユーティリティを見つけます。

11-1. Shepherd ユーティリティを実行します。

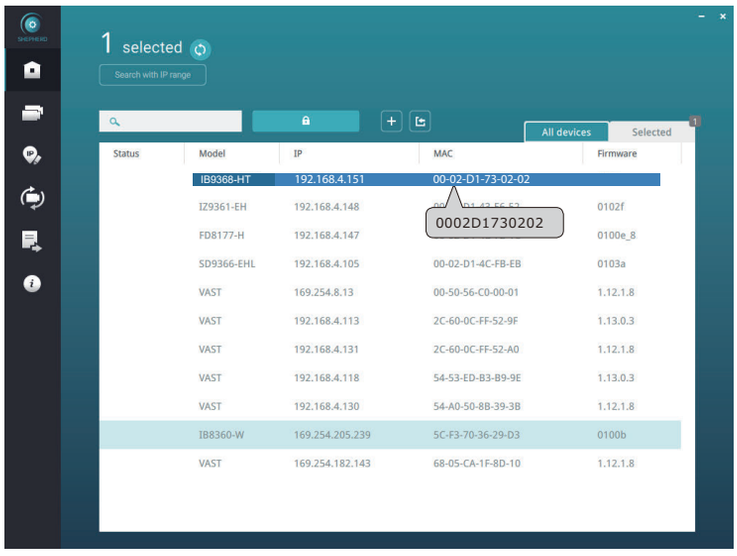
11-2. プログラムは、ネットワーク環境の分析を行います。



11-3. プログラムは、同じ LAN 上のすべての VIVOTEK ネットワークデバイスを検索します。

11-4. 検索が終わると、プログラムのメインウインドウにデバイスのリストが表示されます。製品ラベルに印刷されている MAC とモデル名を確認してアドレスをダブルクリックすると、ネットワークカメラの管理画面が開きます。

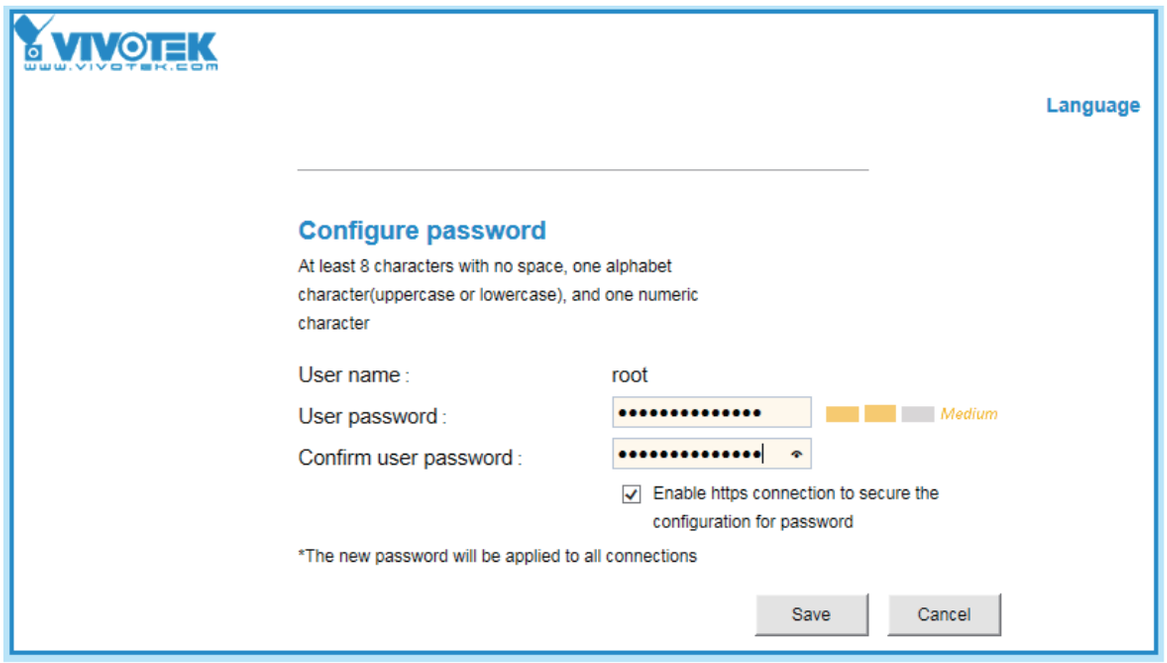




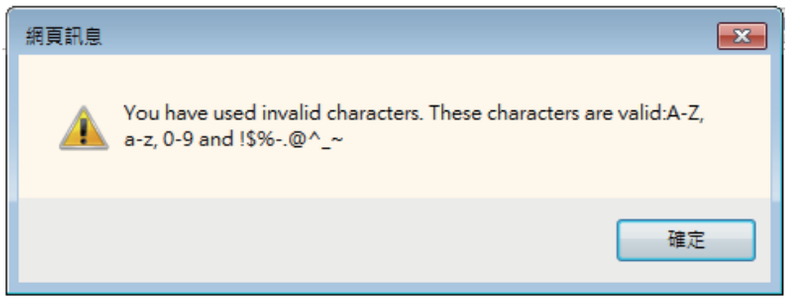
効果的なパスワード設定

12. カメラに初めてログインしたとき、カメラはセキュリティ上の理由からパスワード設定を要求します。

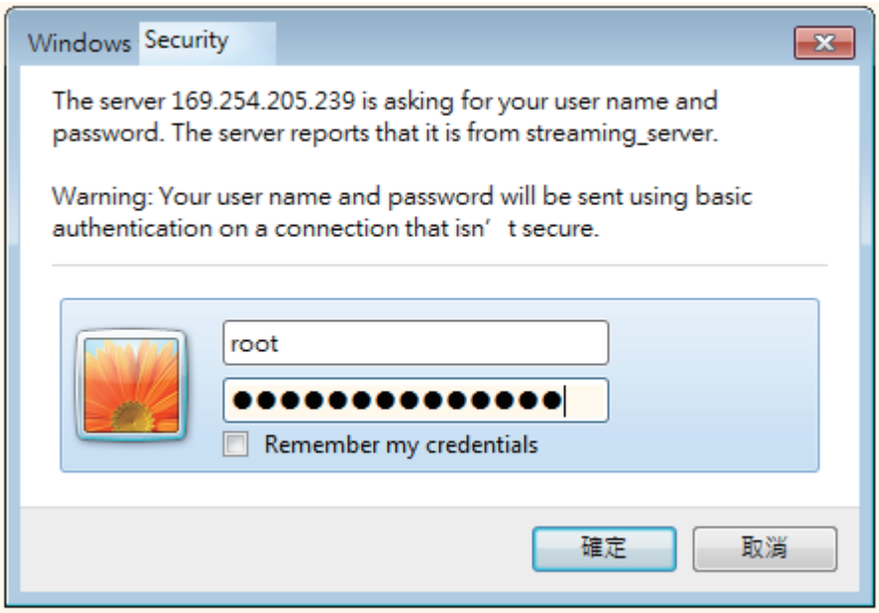
12-1. パスワードの設定画面が表示されますので、より強力なパスワードにするためアルファベットと数字を組み合わせたパスワードを入力します。カメラ管理者のユーザー名は [root] から変更することはできません。



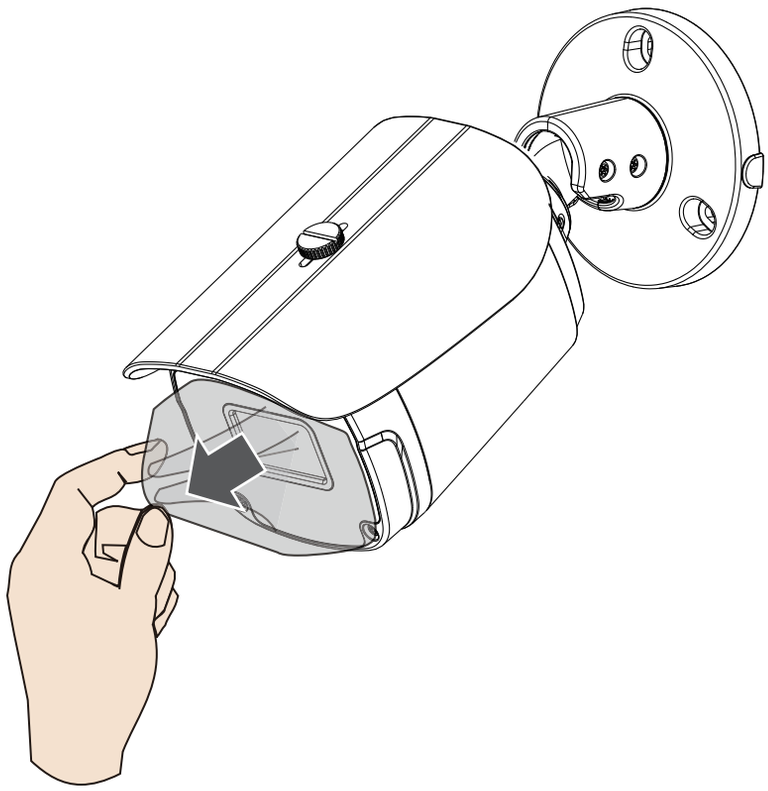
パスワードには、一部の記号（ !, $, %, -, ., @, ^, _, ~）を使用することもできます。



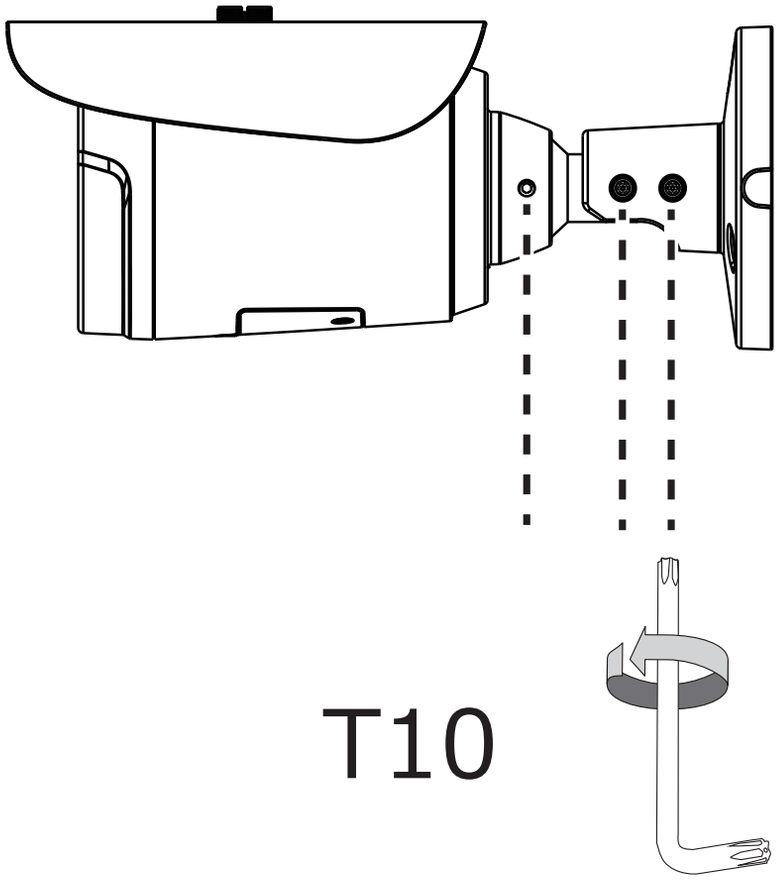
12-2. パスワードの設定が終わると Windows のパスワード入力画面が表示され、ID と設定したパスワードの入力を求められます。ID とパスワードを入力すると、カメラのトップ画面が開き、ライブビューが表示されます。



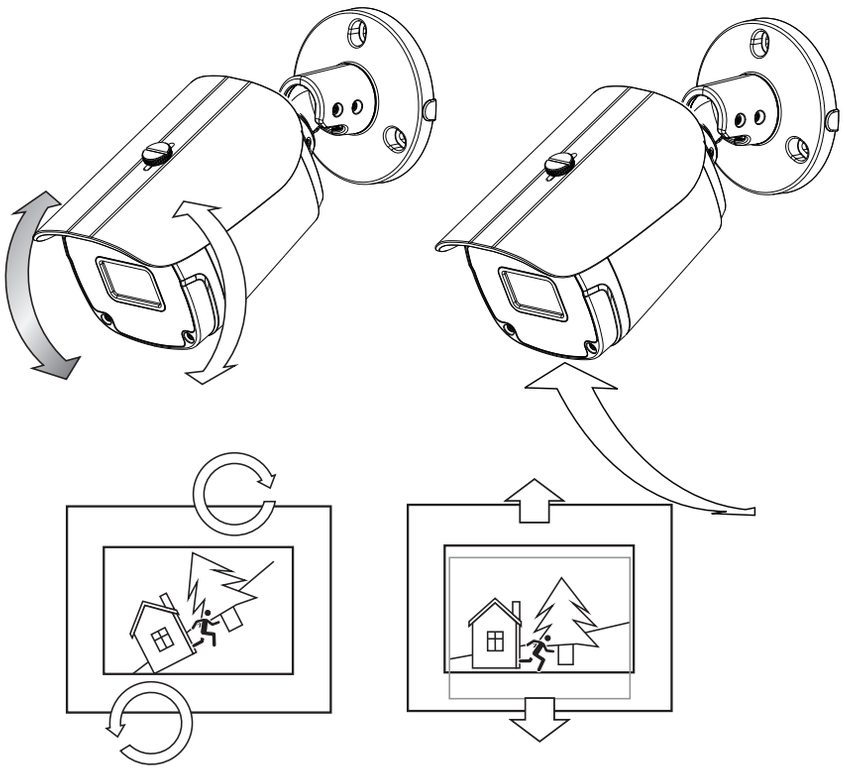
13. レンズの保護シートを剥がします。



14. マウントブラケットの固定ネジを緩めます。



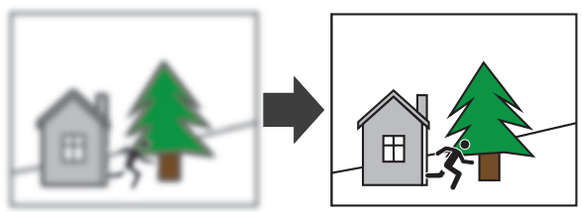
15. コンピュータのライブビュー画面に表示される映像を見ながら、最適な向きになるように調整します。



16. Web コンソールから、ファームウェア構成ページを開きます。[構成]> [メディア]> [イメージ]> [フォーカス] ページに入ります。画面にライブストリームが表示されます。必要に応じて、シーンを拡大できます。「オートフォーカスの実行」機能を使用すると、最適な画像フォーカスに自動的に調整されます。ライブビューをチェックして、イメージに焦点が合っていることを確認します。

構成 > メディア > 画像 > フォーカス





注意：

「T」モデルには電動フォーカスレンズが付属しています。

ハードウェアリセット

リセットボタンは、システムの再起動と出荷時のデフォルト設定に初期化する際に使用します。システムを再起動すると、カメラが初期状態に戻ることがあります。再起動してもシステムの問題が解決しない場合は、出荷時の設定に初期化してから再度システムをインストールしてください。

リセット：リセットボタンを押して離し、ネットワークカメラが再起動するのをお待ちください。

デフォルトの復元：ステータス LED が点滅するまで、リセットボタンを長押ししてください。すべての設定が工場出荷時の設定に復元されます。初期化が成功すると、ステータス LED は緑色が点滅し、通常動作に戻ると赤色が点灯します。

MicroSD/SDHC/SDXC カードの容量

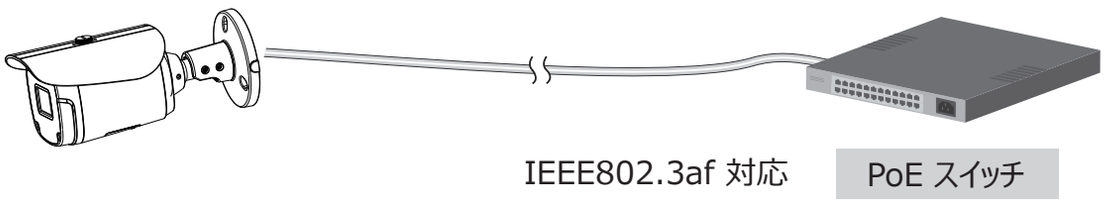
本モデルは **MicroSD/SDHC/SDXC 1TB** までのカード に対応しています。

ネットワークへの接続

通常の接続 (PoE)

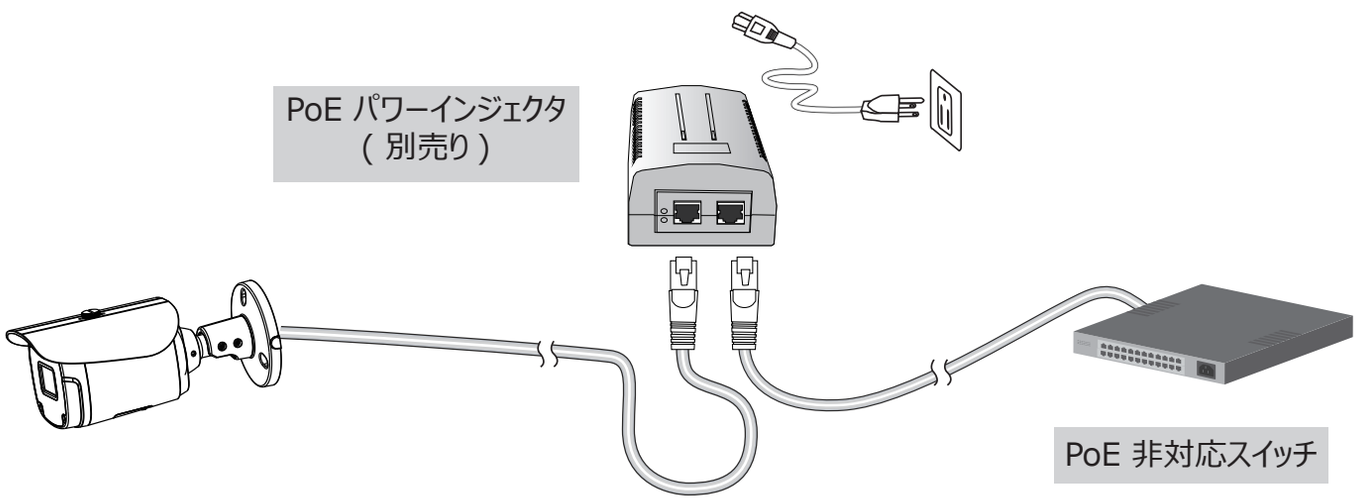
PoE 対応スイッチを使用する場合

本モデルはPoEに対応しており 1 本のイーサネットケーブルで電力とデータを伝送することができます。本モデルをイーサネットケーブルでPoE対応スイッチに接続するには、下図のように接続してください。



PoE 非対応スイッチを使用する場合

PoE パワーインジェクタ（別売り）を使用して、ネットワークカメラと PoE 非対応スイッチを接続してください。



セットアップ

1. ネットワークカメラのブラウザ画面が表示されます。
2. この画面でカメラのライブビデオを見ることができます。複数のカメラで構成されるシステムの場合は、32 チャンネル録画ソフトソフトウェアをインストールすることもできます。インストールの詳細については、VIVOTEK の WEB サイトを参照してください。

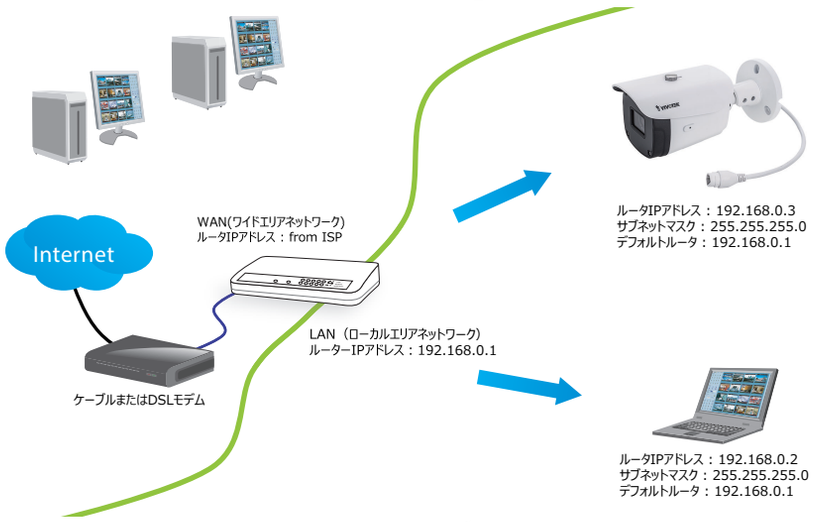


IoT 機器のセキュリティ基準（端末設備等規則第 34 条の 10）
「本製品は電気通信事業者（移動通信会社、固定通信会社、インターネットプロバイダ等）の通信回線（公衆無線 LAN を含む）に直接接続することができません。本製品をインターネットに接続する場合は、必ずルータ等を経由し接続してください。」

ルーター経由のインターネット接続

インターネット経由でネットワークカメラをセットアップする前に、ルーターがあることを確認し、以下の手順に従ってください。

1. ネットワークカメラをルーターの背後に接続します。インターネット環境を以下に示します。 IP アドレスの取得方法については、16 ページの「ソフトウェアのインストール」を参照してください。



2. ここの例の場合、ネットワークカメラの LAN IP アドレスが 192.168.0.3 であり、ルータは以下のポートの通信をネットワークカメラへ転送します。

   - HTTP ポート：default is 80
   - RTSP ポート：default is 554
   - 映像用 RTP ポート：default is 5556
   - 映像用 RTCP ポート：default is 5557

ネットワーク上でポート番号を変更した場合は、それに応じてルータのポートを開いてください。ルータでポートの通信を転送する方法については、ルータのマニュアルを参照してください。

3. ISP (Internet Service Provider) から割り当てられたルータのパブリック IP アドレスを確認し、パブリック IP とセカンダリ HTTP ポートを使用してインターネットからネットワークカメラにアクセスします。詳しくは取扱説明書の P80[Network Type] を参照してください。

固定 IP を使用したインターネット接続

ネットワークカメラに固定 IP を使用する必要がある場合は、この接続タイプを選択してください。詳しくは取扱説明書の P80[LAN] を参照してください。

PPPoE 経由のインターネット接続（ ポイント to ポイント オーバーイーサネット ）

DSL 回線を介してインターネットに接続している場合は、この接続タイプを選択してください。詳しくは取扱説明書の P81[PPPoE] を参照してください。

ルータと IP の設定例

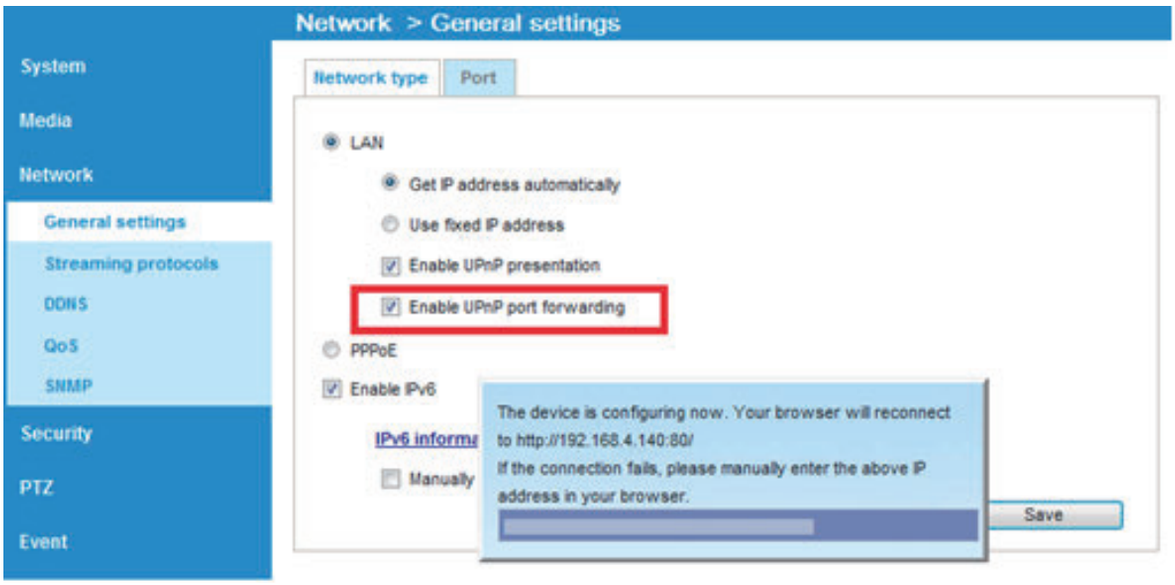
デバイス	IP アドレス：内部ポート	IP アドレス：外部ポート (ルータのマップされたポート)
ルータのパブリック IP	122.146.57.120	
ルータの LAN IP	192.168.2.1	
カメラ 1	192.168.2.10:80	122.146.57.120:8000
カメラ 2	192.168.2.11:80	122.146.57.120:8001
...	...	...

設定済みのポート番号から入力されるすべてのデータをプライベートネットワーク上のネットワークカメラに転送できるように、ルータ、仮想サーバ、またはファイアウォールを設定し、カメラからのデータを同じパスを介してネットワークの外部に送信できるようにします。

ポート番号	転送先
122.146.57.120:8000	192.168.2.10:80
122.146.57.120:8001	192.168.2.11:80
...	...

正しく設定されていれば、次のアドレスを使用してルータのローカル側にあるカメラにアクセスできます。
http://122.146.57.120:8000
ネットワーク設定でポート番号を変更した場合は、それに応じてルータのポートを開いてください。たとえば、ルータを経由してローカルネットワーク内のカメラにアクセスするように設定するには、ルータとの管理セッションを開きます。
ルータの設定に問題がある場合は、ネットワーク管理者に問い合わせてください。

ネットワーク構成オプション (ストリーミングポートなど) の詳細については、取扱説明書の P80[Network（ネットワーク） > General Settings（一般設定）] を参照してください。
また、VIVOTEK はルータが UPnP ポート転送機能に対応する場合に限り NAT トラバーサル機能として自動ポート転送機能を提供します。ポート転送機能を提供します。



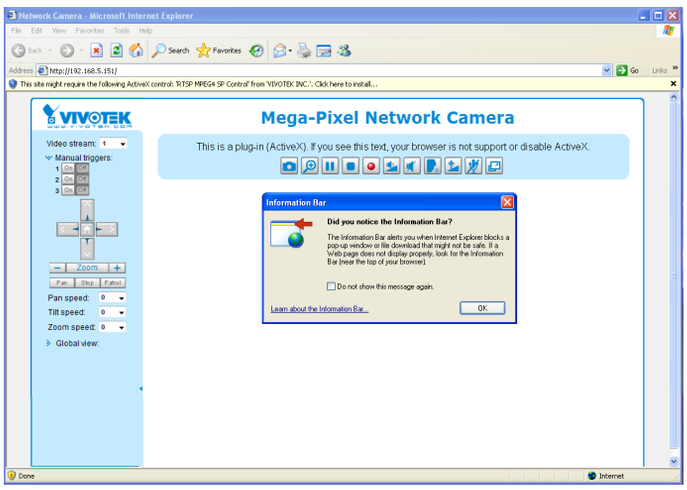
ネットワークカメラに接続

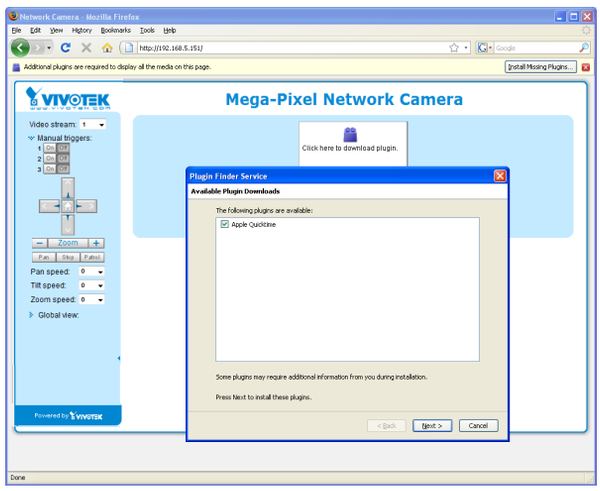
この章では、Webブラウザ、RTSPプレーヤー、3GPP互換モバイルデバイス、VIVOTEK録画ソフトウェアを使ってネットワークカメラにアクセスする方法について説明します。

Webブラウザからのアクセス

Shepherd ユーティリティを使用して、LAN上のネットワークカメラにアクセスします。
ネットワーク環境がLANでない場合は、次の手順に従ってネットワークカメラにアクセスします。

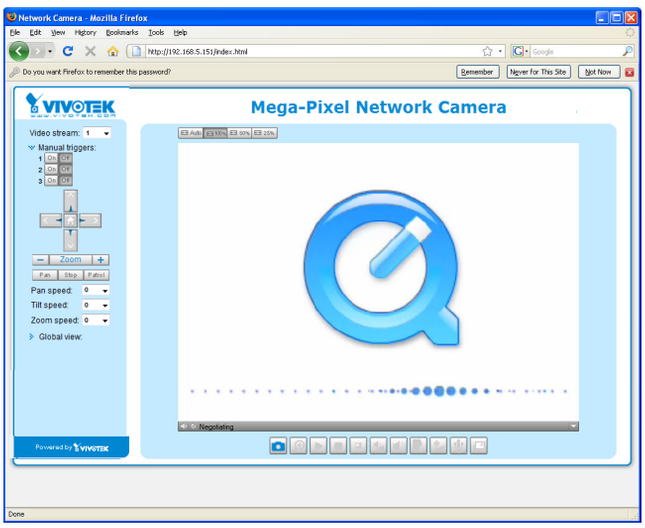
1. Webブラウザを起動します (例： Microsoft® Internet Explorer または Mozilla Firefox)。
2. アドレス欄にネットワークカメラのIPアドレスを入力し[Enter]キーを押します。
3. ライブビデオがWebブラウザに表示されます。
4. VIVOTEKネットワークカメラを初めてインストールする場合は、次のような情報バーが表示されます。指示に従って、必要なプラグインをコンピュータにインストールします。

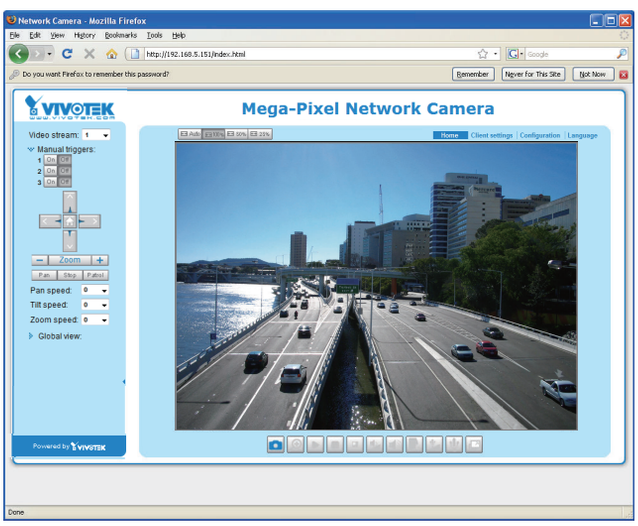




ノート:

► Mozilla Firefox の場合は、ライブビデオのストリーミングには QuickTime を使用します。コンピュータに QuickTime がインストールされていない場合は、QuickTime をインストールしてから Web ブラウザを起動してください。

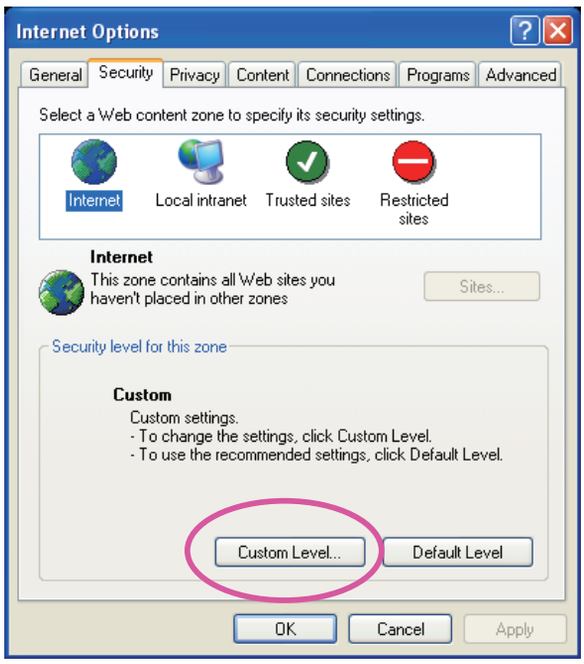




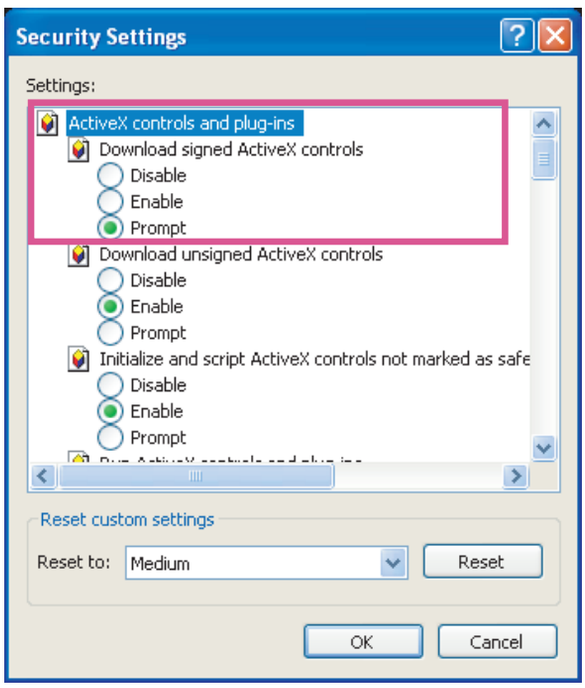
► 初期設定では、ネットワークカメラはパスワード保護されていません。不正アクセスを防ぐために、ネットワークカメラのパスワードを設定してください。取扱説明書の P96[Security] を参照してください。

► セキュリティの設定により ActiveXR コントロールの実行が禁止されていることを示すダイアログボックスが表示された場合は、以下に従ってブラウザの ActiveXR コントロールを有効にしてください。

1. [ツール] > [インターネットオプション]> [セキュリティ] > [レベルのカスタマイズ]を選択します。



2. [署名されたActiveX® コントロールのダウンロード]項目で[有効]または[ダイアログ表示]を選択し[OK]をクリックします。



3. Webブラウザを更新し、ActiveX® コントロールを指示に従ってインストールします。

警告:

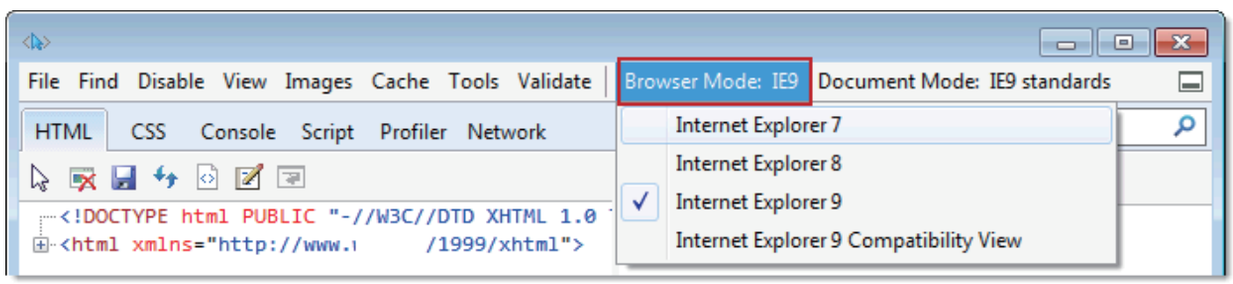
- ネットワークカメラは 32 ビット ActiveX プラグインを使用しています。64 ビット IE ブラウザを使用してカメラの管理 / ビューセッションを開くことはできません。
- 64 ビットのコンピュータを使用する場合、C:¥Windows¥SysWOW64¥Iexpore.exe でプログラムを実行してください。32 ビット IE ブラウザがインストールされます。
- Windows 7 では、下記の場所から 32 ビット Explorer ブラウザにアクセスできます。
  C:¥Program Files (x86)¥Internet Explorer¥iexplore.exe
- Shepherd ユーティリティから Web セッションを開くと 32 ビット IE ブラウザを開くことができます。

ヒント:

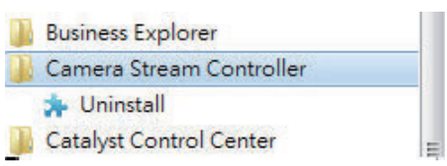
1. 同じ IP アドレス（または同一のカメラが異なるファームウェアバージョンで実行された場合）を使用している別のカメラに PC から接続すると、画面上の Java コントロールが誤動作することがあります。この場合、ブラウザの Cookie を削除すると問題は解決します。
2. 設定メニューまたは UI 項目の表示に問題がある場合は、下図のように IE8 または IE9 の互換表示機能を使用してください。



F12 キーを押して開発者ツールユーティリティを開き、ブラウザのモードを正規の IE8 または IE9 モードに変更しても対応することができます。



- プラグインの互換性の問題が発生した場合は、以前にインストールしたプラグインをアンインストールしてください。



RTSP プレーヤーからのアクセス

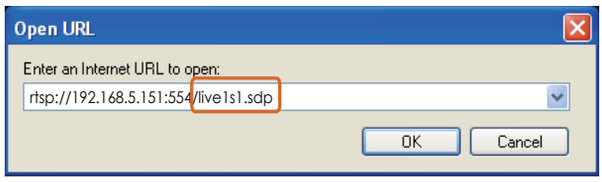
RTSPプレーヤーを使用してストリーミングメディアを表示するには、RTSPストリーミングをサポートする次のいずれかのプレーヤーを使用します。

Quick Time Player

VLC media player

1. RTSP プレーヤーを起動します。
2. [ファイル> URLを開く]を選択します。URLダイアログボックスが表示されます。
3. アドレスの形式は以下です。
   rtsp://<IPアドレス>:<rtspポート>/< stream1 または stream2のRTSPストリーミングアクセス名>
   ほとんどのISPプレーヤーでは、ポート番号554経由のRTSPストリーミングのみが許可されています。RTSPポートを例のように554に設定してください。

   例:



4. ライブビデオが表示されます。RTSPアクセス名の設定方法の詳細については、取扱説明書のP87[RTSP Streaming]を参照 してください。



3GPP 互換モバイルデバイスからのアクセス

3GPP互換モバイルデバイスでストリーミングメディアを表示するには、最初にネットワークカメラにインターネット経由でアクセスできることを確認してください。インターネット経由でネットワークカメラを設定する方法の詳細についてはP22[ネットワークへの接続]を参照してください。

この機能を利用するには、以下の設定を確認してください。

1. 3GPPの携帯電話のプレーヤーはRTSP認証をサポートしていないことが多いので、RTSPストリーミングの認証モードが無効に設定されていることを確認してください。詳細については取扱説明書のP88[RTSP Streaming]を参照してください。

2. 3Gネットワークの帯域幅は限られているため、大きなビデオサイズは使用できません。ビデオストリーミングパラメータを以下のように設定してください。詳細については取扱説明書のP70[Stream settings]を参照してください。

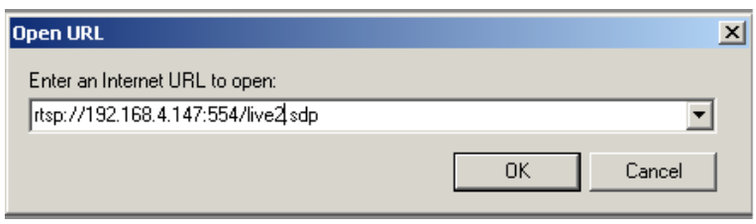
Video Mode	H.264
Frame size	176 x 144
Maximum frame rate	5 fps
Intra frame period	1S
Video quality (Constant bit rate)	40kbps

3. ほとんどのISPやプレーヤーでは、ポート番号554経由のRTSPストリーミングのみが許可されています。RTSPポートを例のように554に設定してください。詳細については取扱説明書のP88[RTSP Streaming]を参照してください。

4. 3GPP互換モバイルデバイス(例:QuickTime)でプレーヤーを起動します。

5. プレーヤーに例図のようにURLコマンドを入力します。
rtsp://<カメラのパブリックIPアドレス>:<rtspポート>/<RTSPストリーミングアクセス名>です。

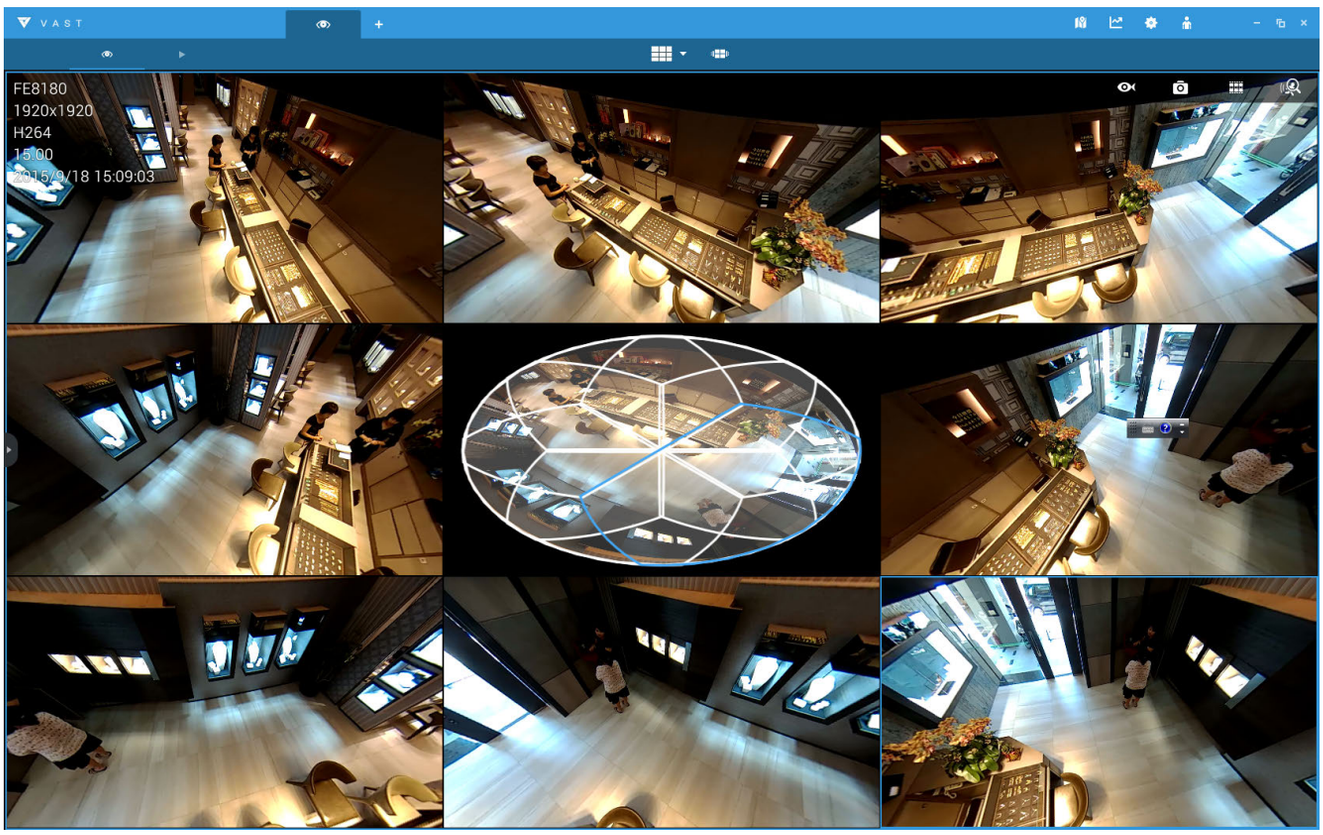
例:



モバイルデバイスでライブ表示するために、ストリーム #2 を上記の推奨ストリーム設定に設定することができます。

VIVOTEK録画ソフトウェアからのアクセス

VIVOTEKのWebサイトからVAST2(監視、録画ソフト)をダウンロードして使用することができます。このソフトウェアを使用すると、複数のネットワークカメラの同時監視とビデオ記録が可能となりますので、ご利用をおすすめします。
ソフトウェアをインストールしてプログラムを起動し、チャンネルリストにネットワークカメラを追加します。ソフトウェアの使用方法の詳細については、ソフトウェアのマニュアルをhttp://www.vivotek.comからダウンロードして参照してください。



ヒント:

1. ライブビューまたはオンスクリーンプラグイン制御に問題が発生した場合は、コンピュータにインストールしたプラグインを削除してみてください。
   C:¥Program Files (x86)¥Camera Stream Controller¥のフォルダを削除します。

2. root (管理者) パスワードを忘れてしまった場合は、リセットボタンを5秒以上押し続けると、カメラを出荷状態へ復元できます。

3. ネットワークでDHCPが有効になっていてもカメラにアクセスできない場合は、Shepherdユーティリティでネットワークを検索してください。デフォルトIP "169.254.x.x" が表示される場合、カメラがローカルネットワークに準拠しない固定IPで設定されている可能性があります。また、それでもカメラが見つからない場合は、カメラのリセットボタンを5秒以上押して初期状態に戻してください。

4. LANカードへの接続を追加するなどネットワークパラメータを変更した場合は、Shepherdユーティリティを再起動してください。

メインページ

この章では、メインページのレイアウトについて説明します。



VIVOTEK ロゴ

ロゴをクリックするとVIVOTEKのWebサイトにリンクします。

ホスト名

ホスト名は必要に応じてカスタマイズすることができます。特に監視環境にカメラが複数ある場合は、ホスト名の変更をおすすめします。詳しくはP43[System]を参照してください。

カラーコントロールエリア

ビデオストリーム: 本モデルは複数のストリーム(ストリーム1,2,3)を同時にサポートしており、いずれかを選択してライブ表示することができます。マルチストリームの詳細については取扱説明書のP70[Stream settings]を参照してください。

手動Trigger: イベントトリガを手動で有効または無効にするときに使用します。この機能を有効にする前に、 アプリケーションページでイベント設定を設定してください。合計3つのイベントを設定できます。

イベント設定の詳細については、取扱説明書のP116を参照してください。この項目を非表示にするには、[Configuration] > [System] > [Homepage Layout] > [General settings] >[Customized button]の順に選択し、[show manual trigger button]のチェックボックスの選択を解除してください。

設定エリア

クライアント設定: このボタンをクリックするとクライアント設定にアクセスすることができます。詳しくはP37[クライアントの設定] を参照してください。.

設定: このボタンをクリックするとネットワークカメラの設定にアクセスすることができます。管理者だけがネットワークカメラを設定できるように、ネットワークカメラにパスワードを設定してください。詳しくはP42[設定] を参照してください。

言語: このボタンをクリックするとユーザインタフェースの言語を選択することができます。言語は、 英語、ドイツ語、スペイン語、フランス語、イタリア語、日本語、ポルトガル語、中国語(簡体/ 繁体)、ロシア語を選択することができます。詳しくはP42[設定] を参照してください。.

非表示ボタン

このボタンをクリックするとコントロールパネルの表示/非表示を切り替えることができます。

リサイズボタン



:

Auto(自動) : クリックするとビデオセルのサイズがモニターに合わせて自動的に変更されます。
100% : クリックすると元の画面サイズで表示されます。
50% : クリックすると元の画面サイズの50%に変更されて表示されます。
25% : クリックすると元の画面サイズの25%に変更されて表示されます。

ライブビデオウインドウ

■ ビデオモードをH.264またはH.265に設定すると、次の画面が表示されます。



ビデオタイトル: ビデオのタイトルを表示します。詳しくは P55[General Settings] を参照してください。

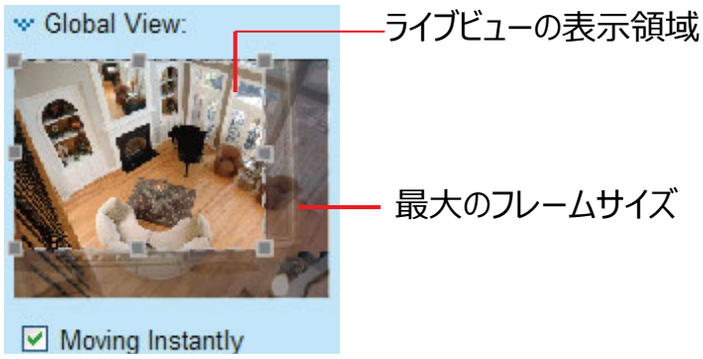
H.264/265 プロトコルとメディアオプション: H.264 またはH.265 ビデオストリーミング用の転送プロトコルおよびメディアオプションを表示します。詳しくはP37[クライアントの設定] を参照してください。

時間: 現在の時刻を表示します。詳しくはP55[Media > Image > General settings] を参照してください。

タイトルと時間: ビデオタイトルと時間は、ストリーミングビデオにスタンプできます。詳しくはP60[Media > Image > General setting] を参照してください。

PTZ パネル：本モデルはデジタルパン/ チルト/ ズーム（e-PTZ）制御に対応しており、ズームインした映像をパン/チルトさせることができます。詳しくは取扱説明書のP113[PTZ > PTZ settings] を参照してください。

グローバルビュー: この項目をクリックするとグローバルビューウインドウを表示することができます。グローバルビューウインドウではフルビューイメージ(キャプチャしたビデオの最大フレームサイズ) とフローティングフレーム（現在のライブビューの表示領域）を選択することができます。フローティングフレームを使用すると、e-PTZ 機能(デジタルパン/ チルト/ ズーム) を制御することができます。詳しくは取扱説明書のP113[PTZ > PTZ settings] を参照してください。また、ビデオストリームの表示領域の設定方法についても同ページを参照してください。

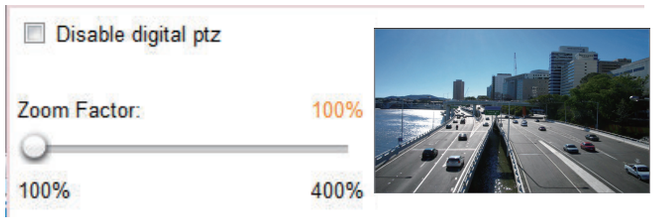


※パネル上の PTZ ボタンは、ズームインされた映像を表示している場合に限り使用できます。ライブビューウインドウにフルビューが表示されている場合、PTZ ボタンは機能しません。

ビデオコントロールボタン: ネットワークカメラの機種やネットワークカメラの設定によっては、利用できないボタンがあります。

 スナップショット: このボタンをクリックすると静止画をキャプチャして保存することができます。キャプチャした画像はポップアップウインドウに表示されますので、画像を右クリックし[名前を付けて画像を保存]を選択してJPEG (*.jpg)、またはBMP (*.bmp) 形式で保存します。

 デジタルズーム: このボタンをクリックして[デジタルズームを無効にする]をオフにするとズーム操作を有効にすることができます。ナビゲーション画面には画像の拡大部分が表示されます。ズームレベルを調整するには、スライダーバーをドラッグします。拡大する別の領域に移動するには、ナビゲーション画面をドラッグします。



 一次停止: ストリーミングメディアの送信を一時停止します。一時停止中に再度ボタンをクリックすると、送信を再開します。

 停止: ストリーミングメディアの送信を停止します。  ボタンをクリックすると転送を続行します。

 MP4録画: このボタンをクリックするとビデオクリップをMP4ファイル形式でコンピュータに録画することができます。  ボタンを押すと録画が終了します。Webブラウザを終了すると、それに応じて録画も停止します。保存先とファイル名を指定するには、P36[MP4 saving options]を参照してください。

 全画面表示: このボタンをクリックすると全画面表示モードに切り替えることができます。Escキーを押すと、通常のモードに戻ります。

■ ビデオモードをMJPEGに設定すると、次の画面が表示されます。



ビデオタイトル: ビデオのタイトルを表示します。詳しくはP60[Media > Image]を参照してください。

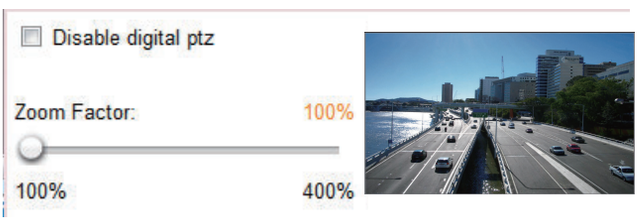
時間: 現在の時刻を表示します。詳しくはP60[Media > Image]を参照してください。

タイトルと時間: ビデオタイトルと時間は、ストリーミングビデオにスタンプできます。詳しくはP60[Media > Image]を参照してください。

ビデオコントロールボタン: ネットワークカメラの機種やネットワークカメラの設定によっては、利用できないボタンがあります。

スナップショット: このボタンをクリックすると静止画をキャプチャして保存することができます。キャプチャした画像はポップアップウインドウに表示されますので、画像を右クリックし[名前を付けて画像を保存]を選択して JPEG (*.jpg) またはBMP (*.bmp) 形式で保存します。

デジタルズーム: このボタンをクリックして[デジタルズームを無効にする]をオフにするとズーム操作を有効にすることができます。ナビゲーション画面には画像の拡大部分が表示されます。ズームレベルを調整するには、スライダーバーをドラッグします。拡大する別の領域に移動するには、ナビゲーション画面をドラッグします。



MP4録画: このボタンをクリックするとビデオクリップをMP4ファイル形式でコンピュータに録画することができます。ボタンを押すと録画が終了します。Webブラウザを終了すると、それに応じて録画も停止します。保存先とファイル名を指定するには、P38[MP4 saving options]を参照してください。

全画面表示: このボタンをクリックすると全画面表示モードに切り替えることができます。Escキーを押すと、通常のモードに戻ります。

クライアントの設定

この章ではローカルコンピュータでストリーム転送モードと保存オプションを選択する方法について説明します。設定が完了したら、設定ページにある[Save]をクリックして設定を有効にしてください。

H.265/H.264 Protocol Options



ネットワーク環境により、H.265/H.264ストリーミングでは次の４つの伝送モードを選択することができます。

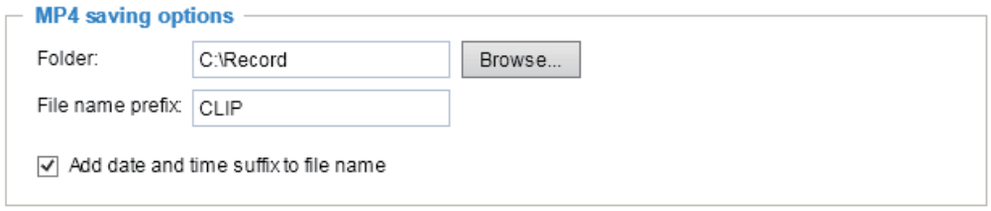
UDP unicast: このプロトコルはよりリアルタイムな音声と映像のストリームを可能にします。ただし、バーストトラフィックによってパケットロスが生じ、画像が破損する場合があります。UDP接続はリアルタイムな応答が必要で映像品質がそれほど重要でない場合に適しています。サーバに接続する各ユニキャストクライアントはそれぞれが帯域幅を使用します。このため、一度にアクセスできるネットワークカメラの数は最大10までとなります。

UDP multicast: このプロトコルを使用すると、マルチキャスト対応のルータはストリーミングメディアを要求するすべてのクライアントにネットワークパケットを転送することができます。これにより、複数のクライアントに同時にサービスを提供しながらもネットワークカメラの転送負荷を軽減することができます。この機能を使用するには、マルチキャストストリーミングを有効にするようにネットワークカメラを設定する必要があります。詳しくは取扱説明書の P88[RTSP ストリーミング] を参照してください。

TCP: このプロトコルはストリーミングデータのより確実な配信と高い映像品質を提供します。ただし、よりリアルタイムなストリーミングには、UDPプロトコルが適しています。

HTTP: Tこのプロトコルは、ある一部のネットワーク環境において、特定のポートを開くことなく TCP プロトコルと同じ品質でストリーミングを行うことができます。ファイアウォール内のユーザーは、このプロトコルを使用してデータのストリーミングを許可することが出来ます。

MP4 Saving Options

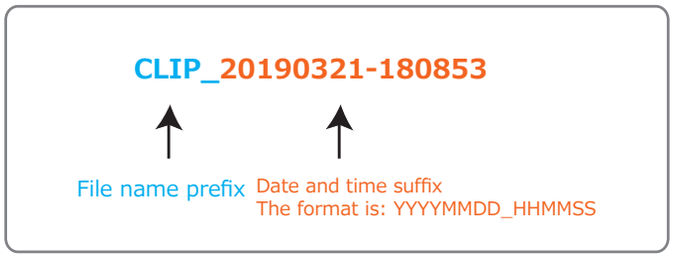


メインページの  ボタンをクリックすると、視聴中のライブビデオを録画することができます。 録画データの保存先とファイル名の指定を行います。

Folder: 録画したビデオファイルの保存先を指定します。保存場所は変更することができます。

File name prefix: ビデオファイル名の前に付加するテキストを入力します。指定したフォルダがローカルのハードディスクに自動的に作成されます。

Add date and time suffix to the file name: このオプションを選択すると、ファイル名の末尾に日付と時刻が追加されます。



Local Streaming Buffer Time



帯域幅が不安定な場合、ライブストリーミングに遅延が生じたり、ビデオストリーミングがスムーズに行われないことがあります。このオプションを有効にすると、ライブストリーミングはPCのキャッシュメモリに一時的に保存され、数ミリ秒後にライブビューウインドウで再生されます。これにより、ストリーミングがよりスムーズに再生されます。例えば、バッファタイムを3,000/ミリ秒に設定すると、ストリーミングは３秒間遅延します。

ジョイスティックセッティング

ジョイスティックを有効にする

ジョイスティックを管理用コンピュータのUSBポートに接続します。対応プラグイン(Microsoft's DirectX)により、Webコンソールのプラグインが読み込まれると、コンピュータに接続されたジョイスティックが自動的に検出されます。ジョイスティックは、他のドライバやソフトウェアをインストールしなくても正常に動作します。

次に、接続されているジョイスティックの設定を行います。設定を有効にするには、次の手順に従ってください。

1. デバイスが複数ある場合は、[Selected joystick]項目から、検出されたジョイスティックを選択します。ジョイスティックが認識されない場合、デバイスに不具合がある可能性があります。
2. [Calibrate]または[Configure]ボタンをクリックして、ジョイスティックの設定を行います。



ノート:

- ジョイスティックにプリセットアクションを割り当てる場合は、あらかじめ[Configuration] >[PTZ]でプリセットの場所を設定しておく必要があります。Windowsでは、メニューの検索機能を使用してゲームコントローラを検索します。
- ジョイスティックが正常に動作していない場合、調整が必要な場合があります。[Calibrate]ボタンをクリックして、Windowsのコントロールパネルにあるウインドウを開き、トラブルシューティングの手順に従ってください。
- ジョイスティックがWindowsのコントロールパネルのゲームコントローラリストに表示されます。デバイスをチェックアウトする場合は、[スタート]→[コントロールパネル]→[ゲームコントローラ]の順に選択します。

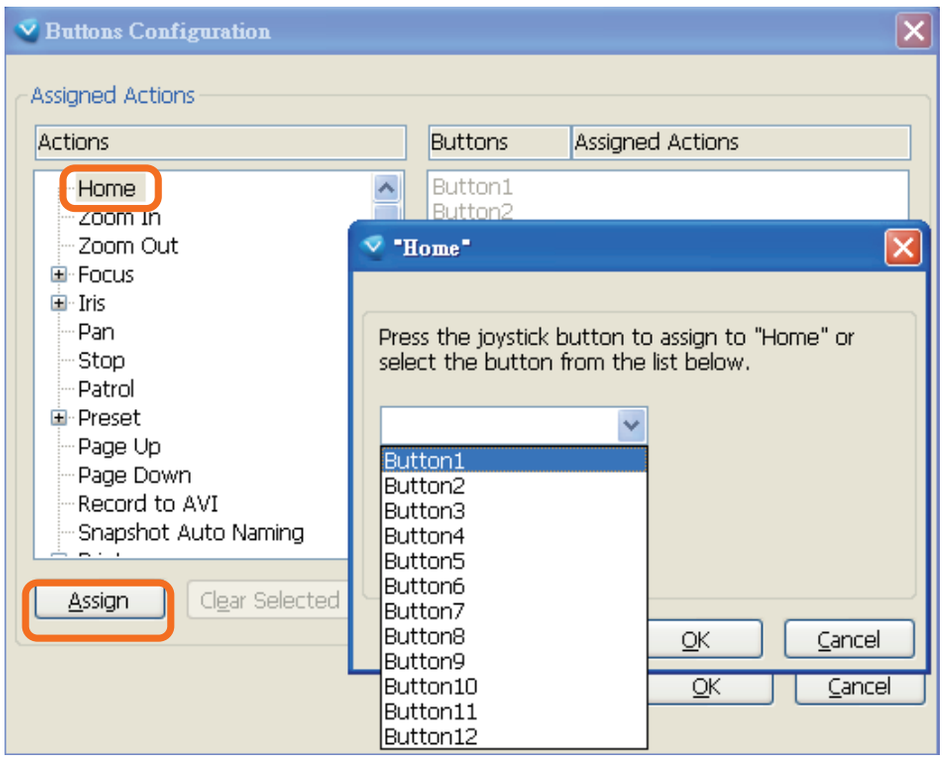


ボタンの設定

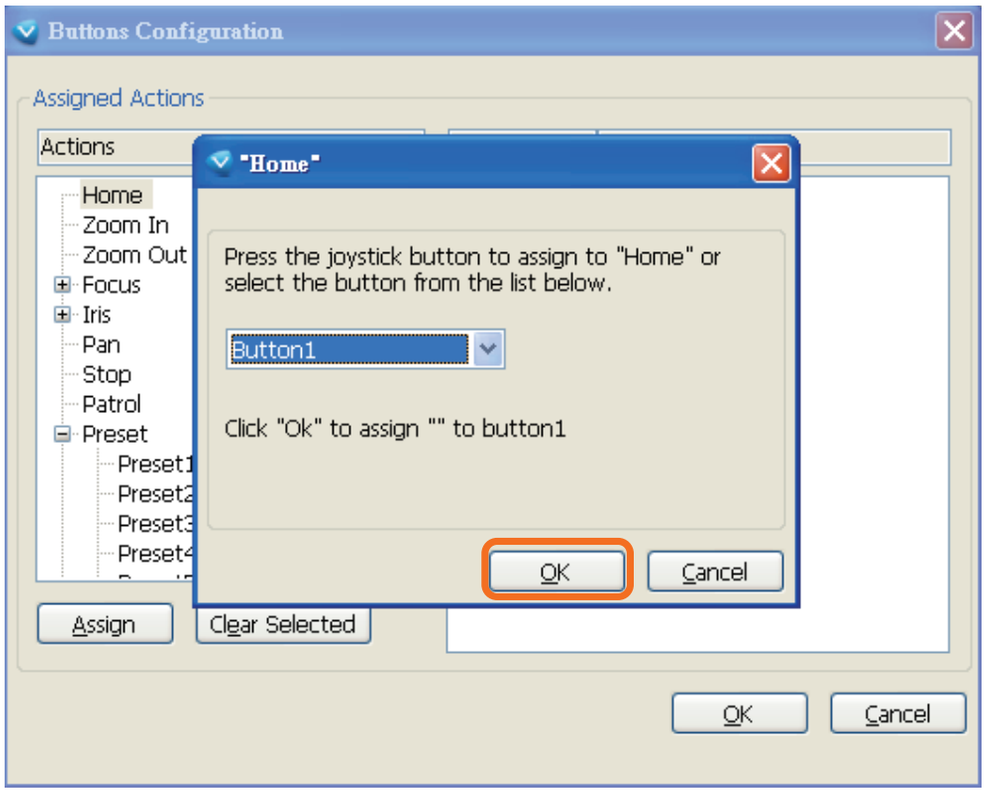
[Button Configuration]ウインドウでは、割り当て可能なアクションが左の列に表示され、機能ボタンと割り当て済みのアクションが右の列に表示されます。ボタンの数はジョイスティックによって異なる場合があります。
次の手順に従ってジョイスティックボタンを設定してください。

1．設定したいアクションを選択して[Assign]をクリックすると、ダイアログボックスが表示されます。ジョイスティックボタンを押すか、ドロップダウンリストからボタンを選択して、このアクションをボタンに割り当てます。

例: [Button 1]に[Home]（ホームポジションに移動する）を割り当てる。



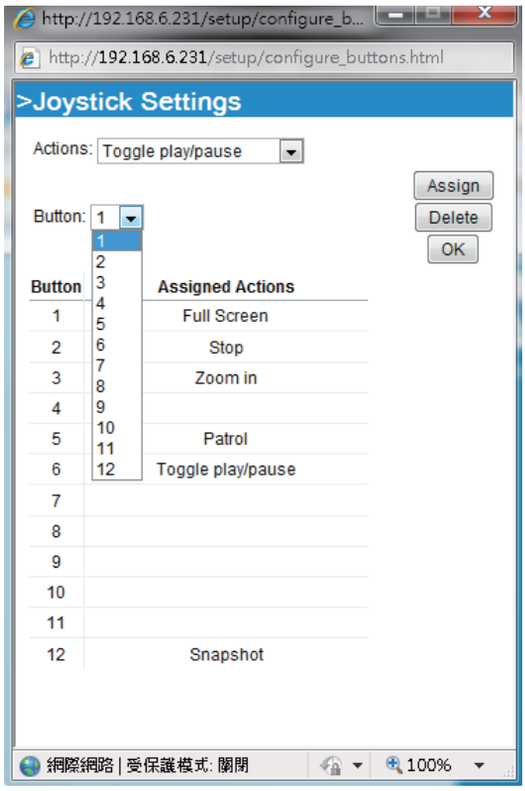
2. [OK]をクリックして設定します。



ボタンの設定

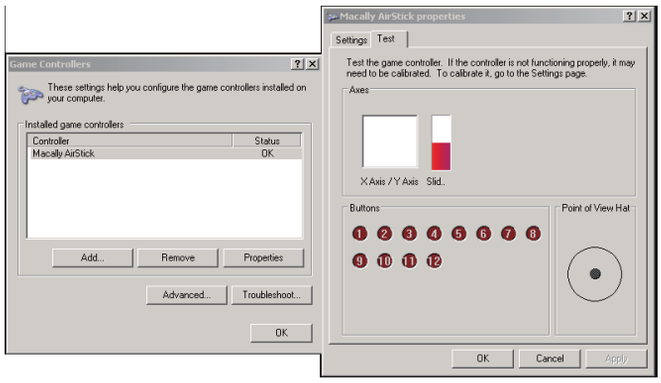
[Configure Buttons]ボタンをクリックすると、下図のようなウインドウが表示され、次の手順でジョイスティックのボタンを設定することができます。

1. [Button]メニューからボタン番号を選択します。



ヒント:

各ボタンの場所がわからない場合は、ゲームコントローラユーティリティのプロパティウインドウで確認してください。



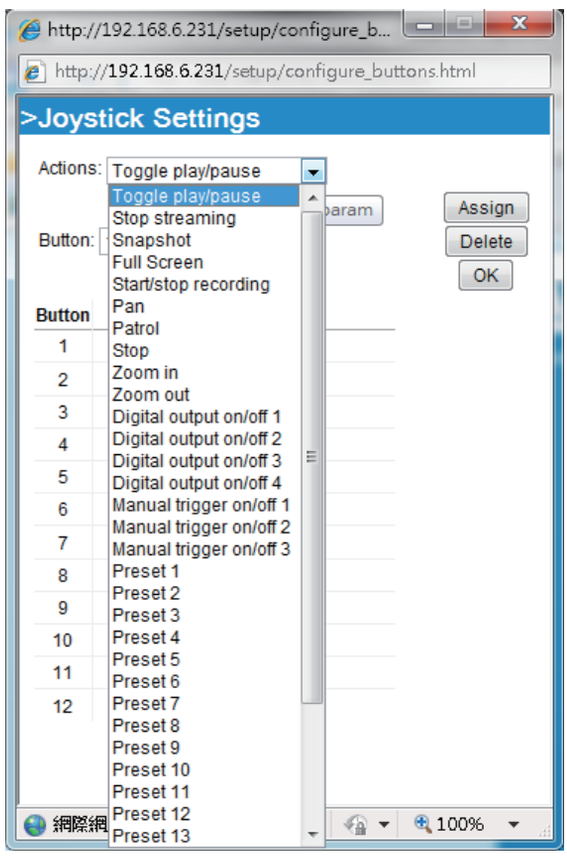
2. [Actions]メニューから[Patrol] や[Preset]などの対応するアクションを選択します。

3. [Assign]ボタンをクリックして、ボタンにアクションを割り当てます。また、ボタン番号を選択して[Delete]ボタンをクリックすると関連付けを削除することができます。

   同様のプロセスを繰り返し、すべてのボタンにアクションを設定します。

   設定したボタンとアクションがボタンリストに表示されます。

4. [Client settings]の[Save]ボタンをクリックして設定を保存してください。

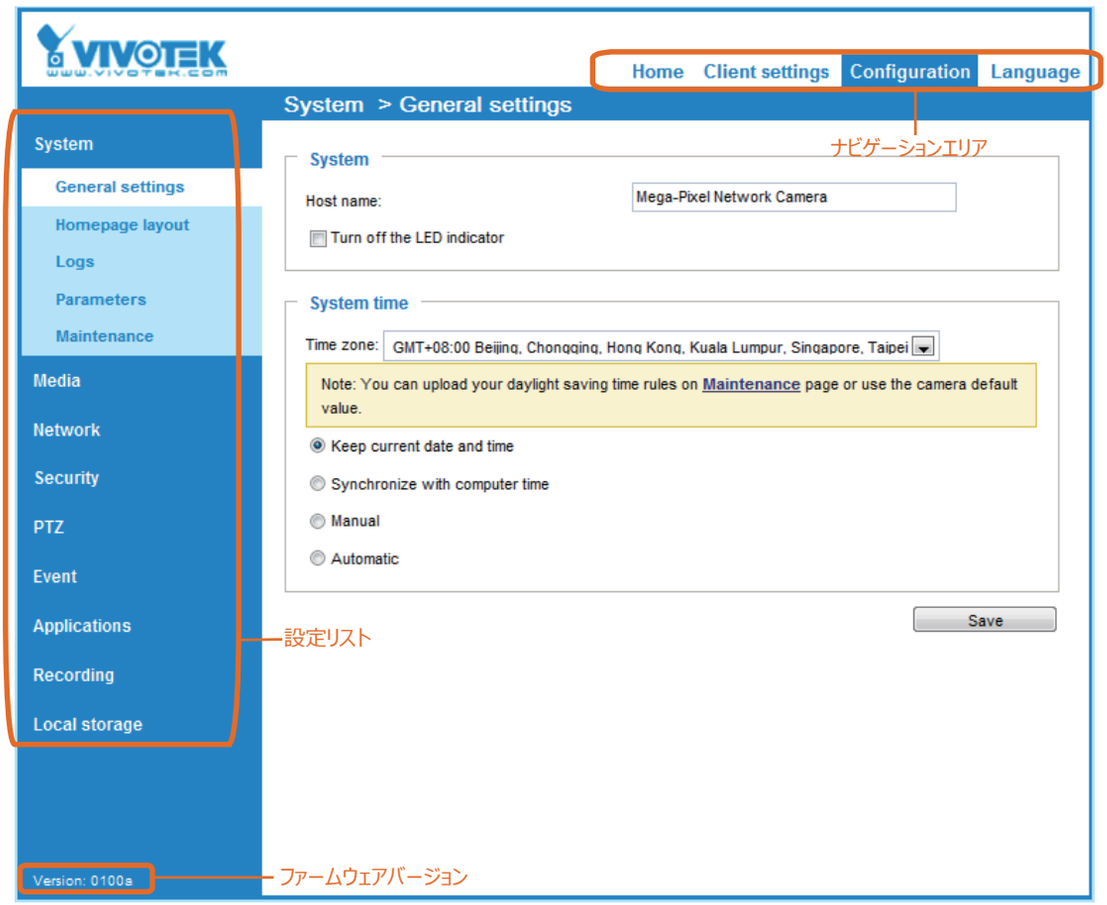


設定

メインページの[Configuration]をクリックすると、カメラの設定を行うことができます。設定ページにアクセスできるのは管理者のみですのでご注意ください。

VIVOTEKのユーザインタフェースでは、最小限の作業でネットワークカメラをセットアップすることができます。設定リストをクリックすると詳細項目が表示されます。また、詳細項目をクリックすると、該当する詳細項目の情報が表示されます。続けて 2 番目の詳細項目をクリックすると、該当する詳細項目の情報が表示され、最初の詳細項目の情報は非表示になります。

設定ページのメイン画面は下図のように表示されます。



次のセクションでは、設定リストの各機能について説明します。

ナビゲーションエリアは固定されており、どの設定項目を開いているときも[Home](ライブビューウインドウ)、[Client settings](クライアント設定ページ)、[Language](言語選択)にアクセスできます。

System（システム） > General settings（一般設定）

ここでは、ホスト名やシステム時刻など、ネットワークカメラの基本設定を行う方法について説明します。[System]と[System Time]の２つの項目があります。いずれも設定が終了したら、ページ下部にある[Save]をクリックして設定を有効にします。

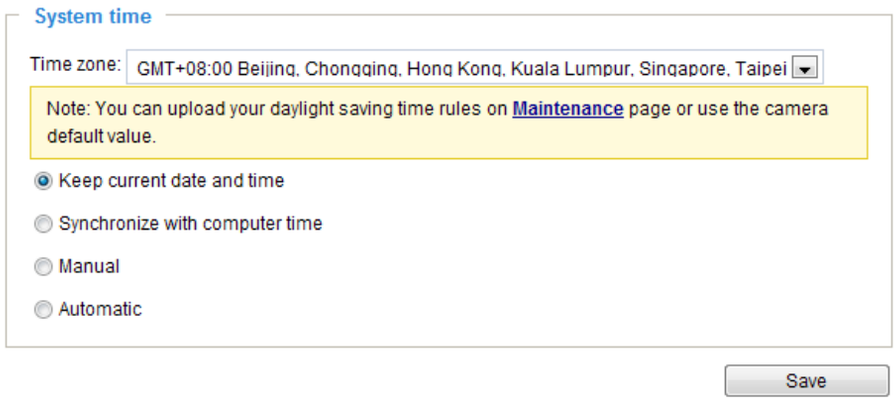
System



Host name: ネットワークカメラの名前を入力します。名前はメインページ上部と、VAST 2 ソフトウェアのビューセルに表示されます。

Turn off the LED indicators: ネットワークカメラが動作していることを人に知られたくない場合は、このオプションを選択してLEDインジケータを消灯できます。

System time



Keep current date and time: 選択すると、ネットワークカメラの現在の設定日時を維持することができます。カメラの内蔵リアルタイムクロックは、システム側の電源を切っても設定日時を保ちます。

Synchronize with computer time: 選択すると、ネットワークカメラの日付と時刻をローカルコンピュータと同期することができます。カメラはPCから読み取った日時に更新されて表示されます。

Manual: 選択すると、日付と時刻を手動で入力することができます。日付と時刻のフォーマットは、 [yyyy/mm/dd] と [hh:mm:ss]です。

Automatic: 選択すると、NTPサーバに定期的に問い合わせてネットワークカメラの時刻を同期化するNetworkTime Protocolを設定します。

NTP server:タイムサーバのIPアドレスまたはドメイン名を割り当てます。 テキストボックスを空白のままにすると、ネットワークカメラがインターネットにアクセスできる場合カメラは既定のタイムサーバに接続されます。

Update interval: 選択すると、NTPサーバを使用して任意の単位（時間/日/週/月）でカメラの時刻を更新することができます。

Time zone ： リストから適切なタイムゾーンを選択することができます。サマータイムルールを適用する場合は取扱説明書のP52[System > Maintenance > Import/ Export files]を参照してください。

System （システム）> Homepage layout （ホーム画面レイアウト）

ここでは、ホーム画面のレイアウトをカスタマイズする方法を説明します。

General settings

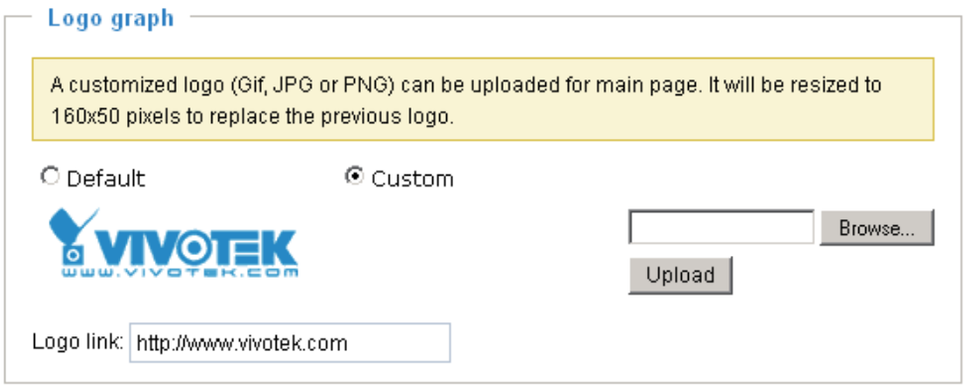
ホーム画面のレイアウトの設定が表示されます。2 番目のタブにある[Theme Options]で背景色とフォントの色を手動で選択することができます。設定はプレビューフィールドに自動的に表示されます。

下図は、工場出荷時の設定を使用したホーム画面を表示しています。



■ Hide Powered by VIVOTEK: この項目をチェックすると、図中枠部分をページから削除することができます。

Logo graph
ホーム画面の上部に表示されるロゴを変更できます。



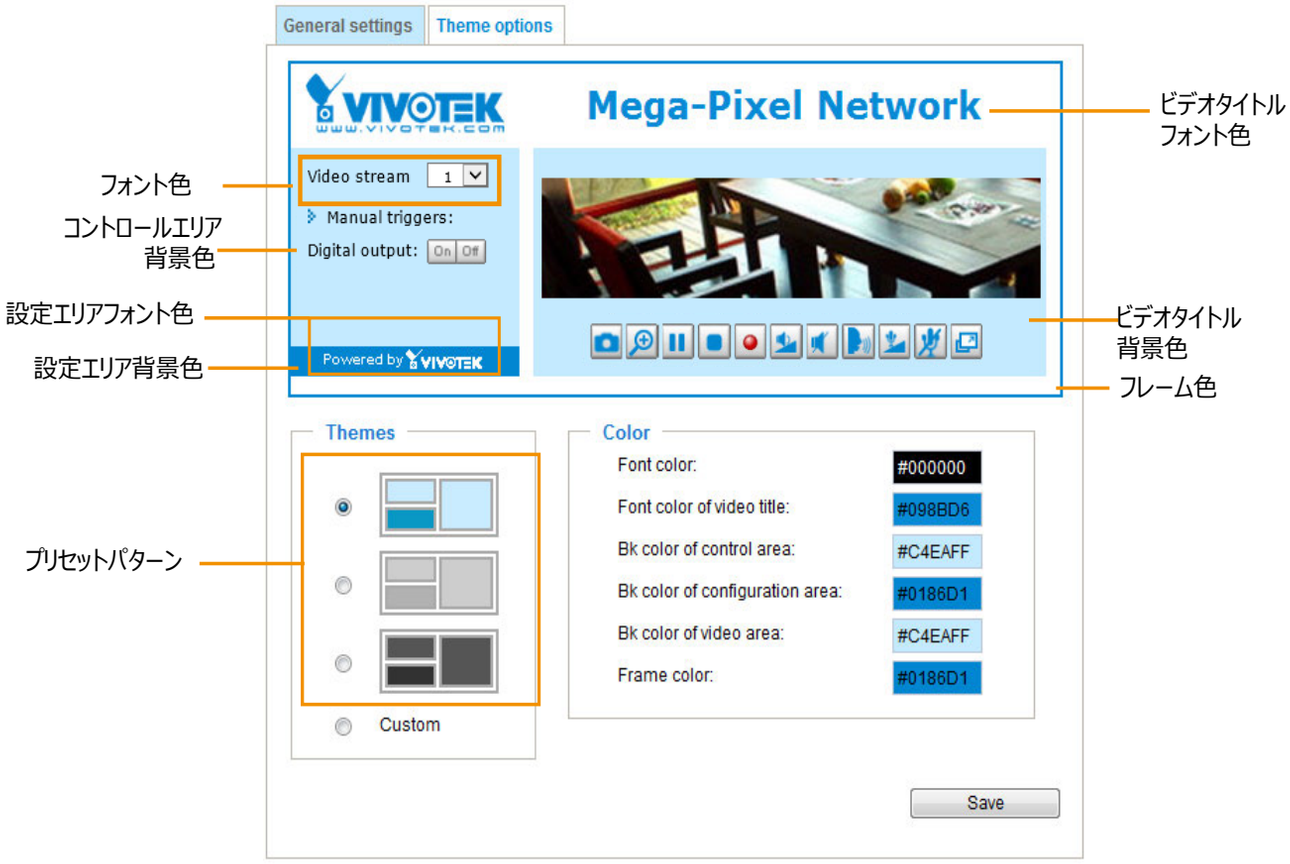
次の手順で新しいロゴをアップロードします。
1. [Custom] を選択すると[Browse]フィールドが表示されます。
2. ファイルからアップロードするロゴを選択します。
3. [Upload]をクリックして、既存のロゴを新しいロゴに置き換えます。
4. 必要に応じてロゴからリンクされるURLを[Logo link]に入力します。
5. [Save]をクリックして設定を有効にします。

Customized button：ホーム画面上の手動トリガーボタンを非表示にしたい場合はチェックをはずしてください。この項目は工場出荷時はオンになっています。



Theme Options

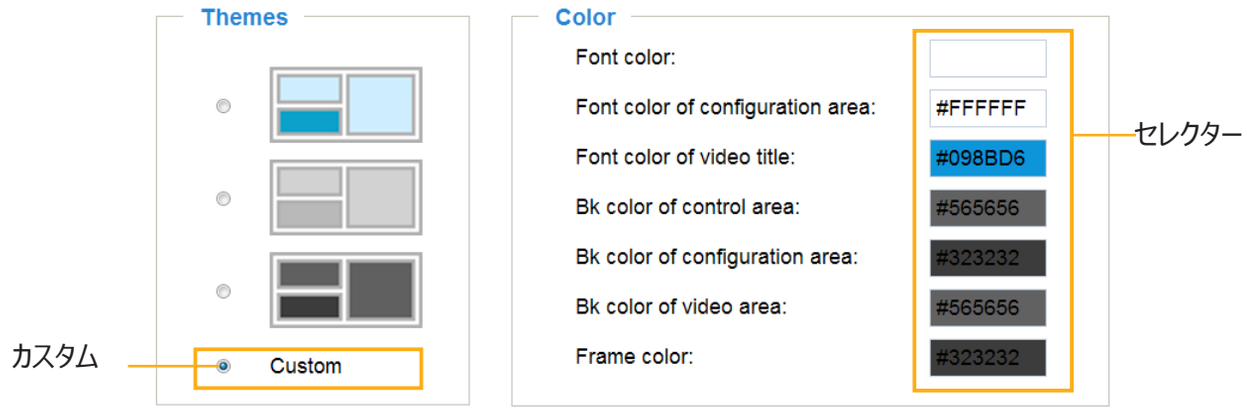
ホーム画面のレイアウトの色を変更することができます。３つのプリセットパターンから１つを選択すると、新しいレイアウトがプレビューフィールドに表示されます。設定が完了したら[Save]をクリックして設定を有効にします。



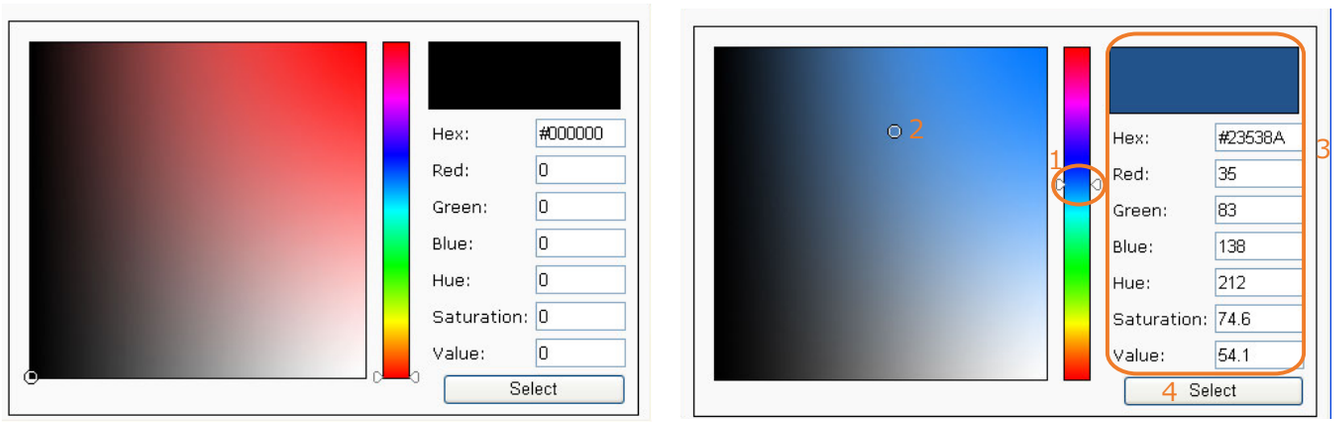




■ 次の手順でホーム画面をカスタマイズすることができます。
1. 左側にある[Custom]を選択します。
2. 右側にある[Color]フィールドの変更したい箇所に該当するセレクターをクリックします。



3. 以下のようなパレットウインドウが表示されます。

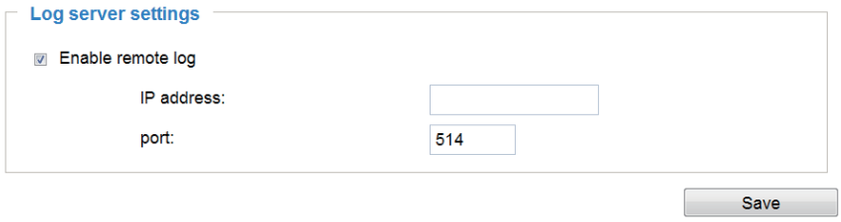


4. スライダーバーをドラッグして調整し、パレットから目的の色を選択します。
5. 選択した色が、対応するフィールドとプレビュー欄に表示されます。
6. [Save]をクリックして設定を有効にします。

System（システム） > Logs（ログ）

ここでは、システムログをバックアップしてリモートサーバに送信するようネットワークカメラを設定する方法を説明します。

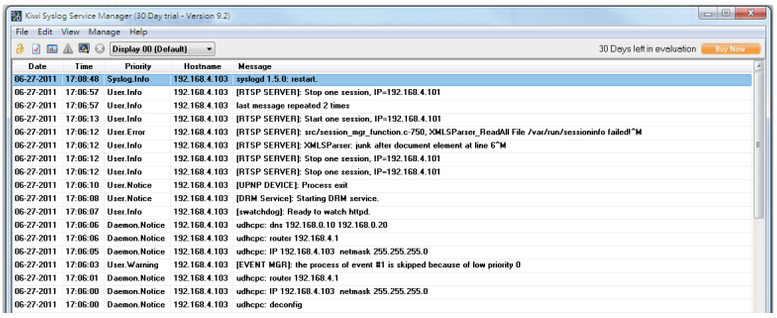
Log server settings



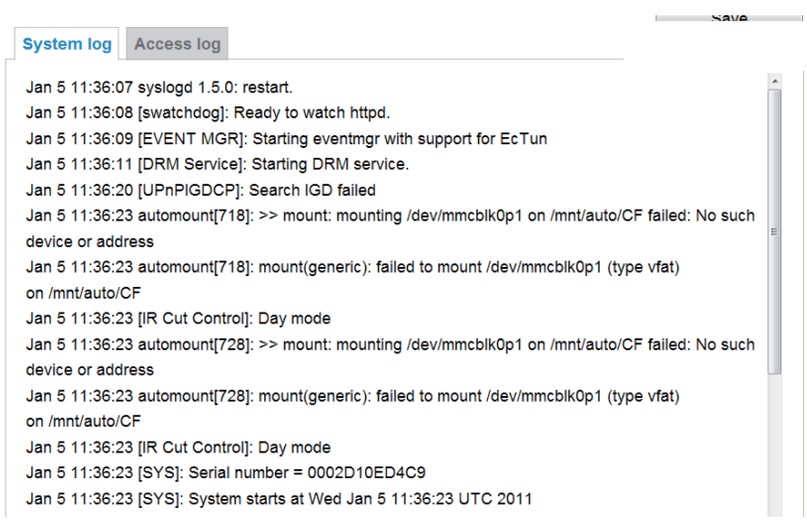
次の手順でリモートログを設定することができます。

1. [Enable remote log]を選択します。
2. [IP address]フィールドにリモートサーバのIPアドレスを入力します。
3. [port]フィールドにリモートサーバのポート番号を入力します。
4. [Save]をクリックして設定を有効にします。

本機能でシステムログファイルをバックアップしてリモートサーバに送信するようネットワークカメラを設定することができます。この機能を使用する前に、Kiwi Syslog Daemonのようなログ記録ツールをインストールして、ネットワークカメラからシステムログメッセージを受信することをお勧めします。
http://www.kiwisyslog.com/kiwi-syslog-daemon-overview/.

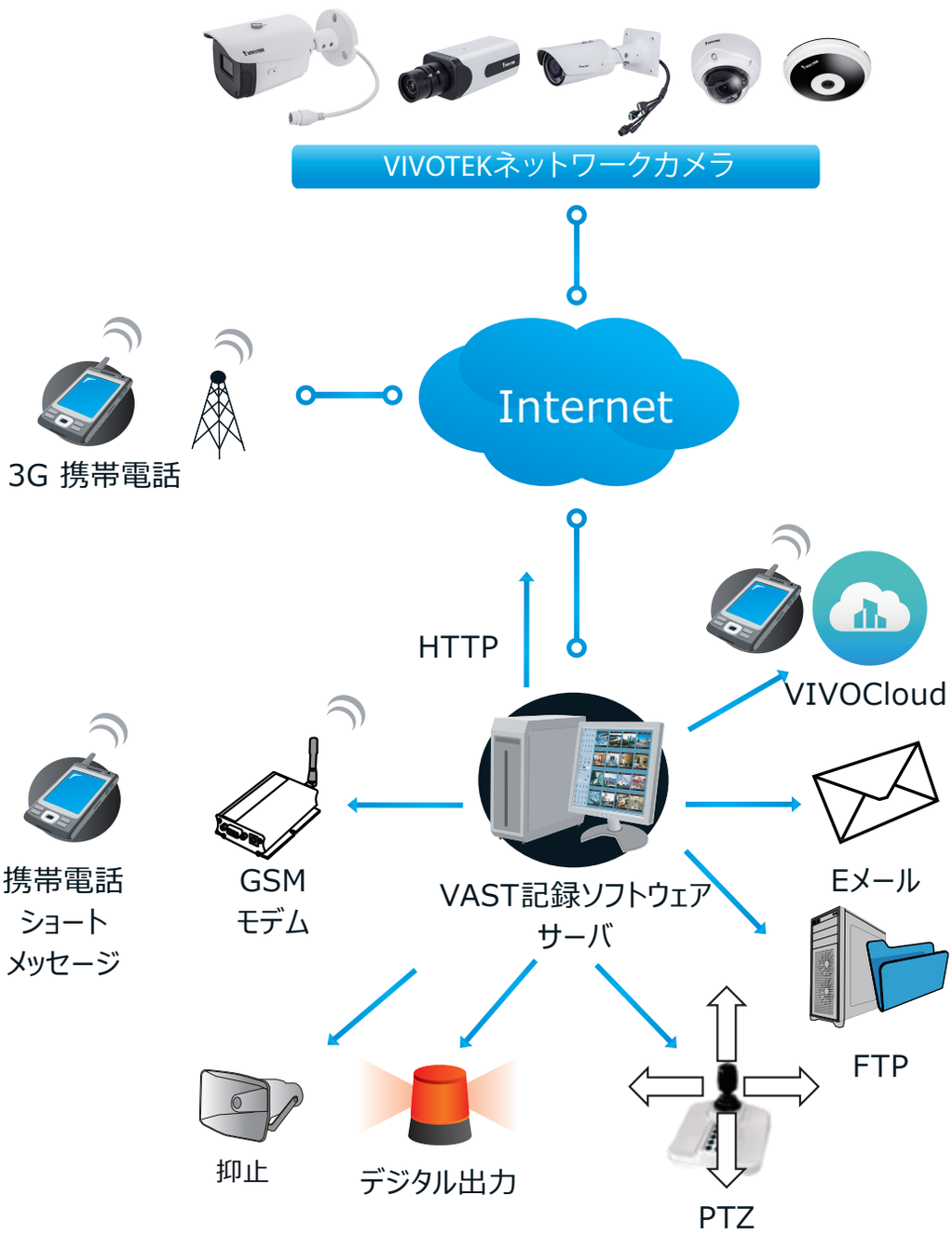


System log

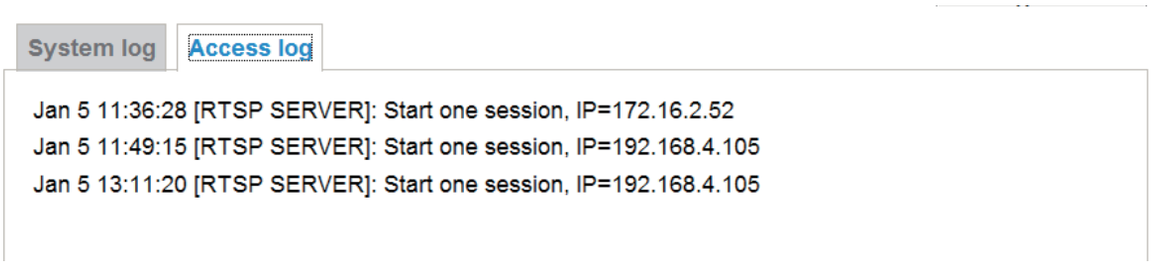


システムログを時系列で表示することができます。システムログはカメラのバッファ領域に保存され、一定の量に達すると上書きされます。

VAST2ソフトウェアをインストールすると、Eメール、GSMショートメッセージ、オンスクリーンイベントパネル、アラームのトリガーなどを使ってイベントメッセージの配信が可能になるイベント管理機能グループをご利用いただけます。詳しくは『VASTユーザーマニュアル』を参照してください。



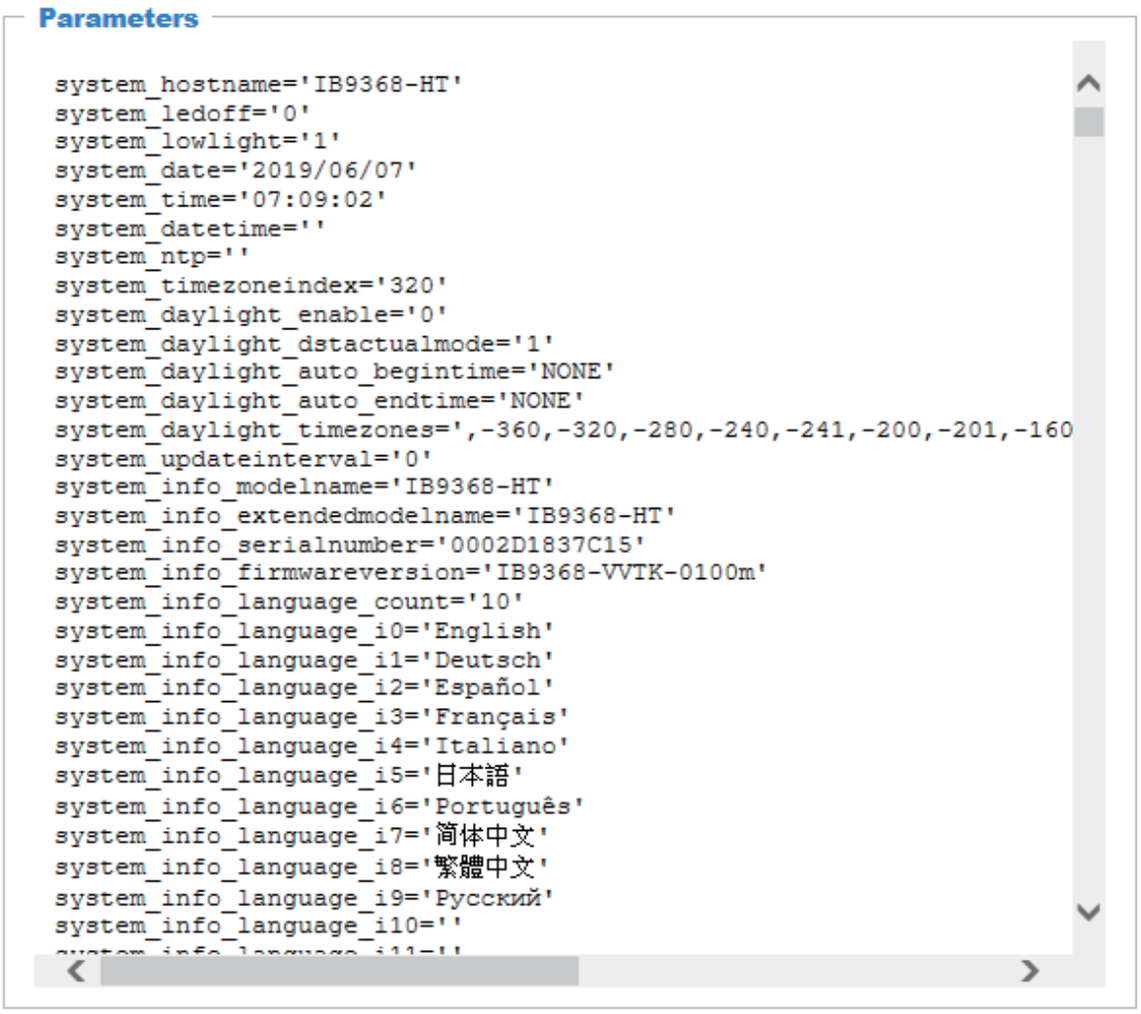
Access log



アクセスログには、すべてのビューア（オペレータと管理者を含む）のアクセス時間とIPアドレスが時系列で表示されます。アクセスログはネットワークカメラのバッファ領域に保存され、一定の量に達すると上書きされます。

System（システム）> Parameters（パラメータ）

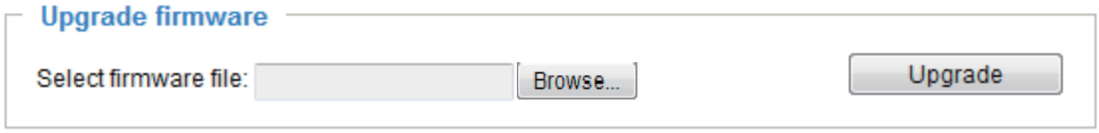
パラメータの表示ページには、システム全体のパラメータが一覧表示されます。技術的なサポートが必要な場合は、このページに表示されている情報を提供してください。



System > Maintenance

ここでは、ネットワークカメラを工場出荷時の設定に戻す方法やファームウェアのバージョンをアップグレードする方法などについて説明します。

General settings > Upgrade firmware

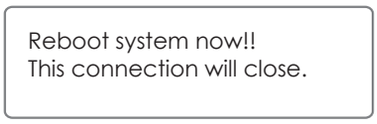


ネットワークカメラのファームウェアをアップグレードすることができます。
処理が完了するまで数分かかります。
注：アップグレードの間は決してネットワークカメラの電源をオフにしないでください。
次の手順でファームウェアをアップグレードすることができます。

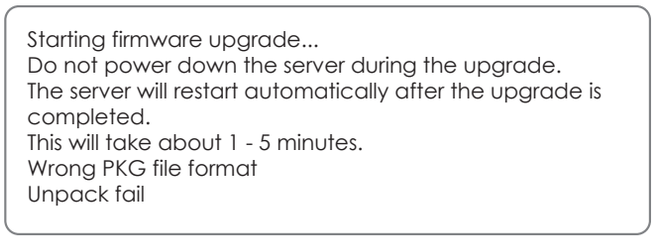
1. VIVOTEKのWebサイトから最新のファームウェアをダウンロードします。
   ファイルはpkgファイル形式で保存されています。
2. [Browse...] をクリックして、ダウンロードしたファームウェアを指定します。
3. [Upgrade] をクリックします。アップグレードが完了するとネットワークカメラは自動的に再起動します。

アップグレードが正常に完了すると、下図のように「今すぐシステムを再起動してください。この接続は閉じられます」と表示されます。その後、ネットワークカメラに再度アクセスします。

アップグレードが成功した際の表示



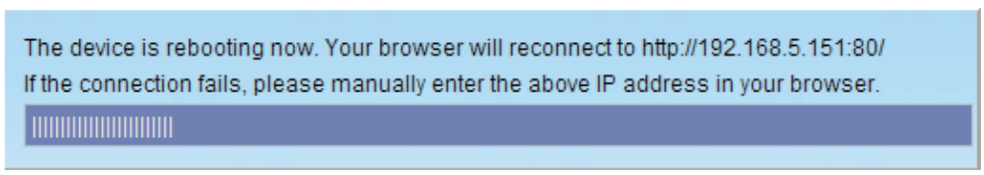
正しくないファームウェアファイルを選択した際の表示



General settings > Reboot

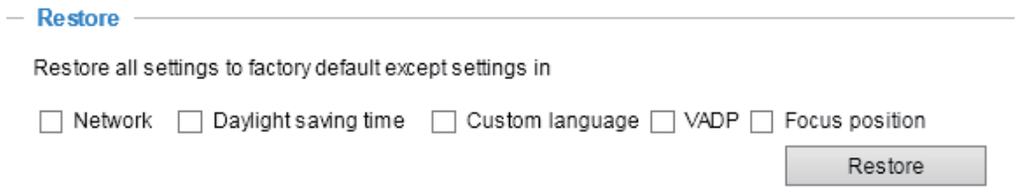


ネットワークカメラを再起動することができます。再起動には約1分かかります。再起動のプロセス中は下図のメッセージが表示されます。再起動が完了すると、ライブビデオページがブラウザに表示されます。



再起動後に接続ができない場合は、[IP address]フィールドにネットワークカメラのIPアドレスを手動で入力して接続してください。

General settings > Restore



ネットワークカメラを工場出荷時の設定に戻すことができます。
Network: このオプションを選択するとネットワークの設定を保持することができます。詳しくはP80[Network Type]を参照してください。

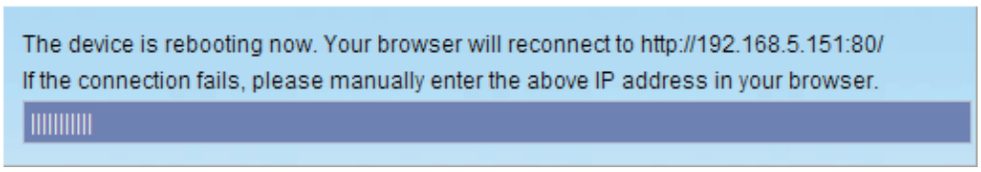
Daylight Saving Time: このオプションを選択するとサマータイムの設定を保持することができます。詳しくは下記の[Import/Export files]を参照してください。

Custom Language: このオプションを選択するとカスタム言語の設定を保持することができます。

VADP: このオプションを選択するとVADPモジュールと関連する設定を保持することができます。

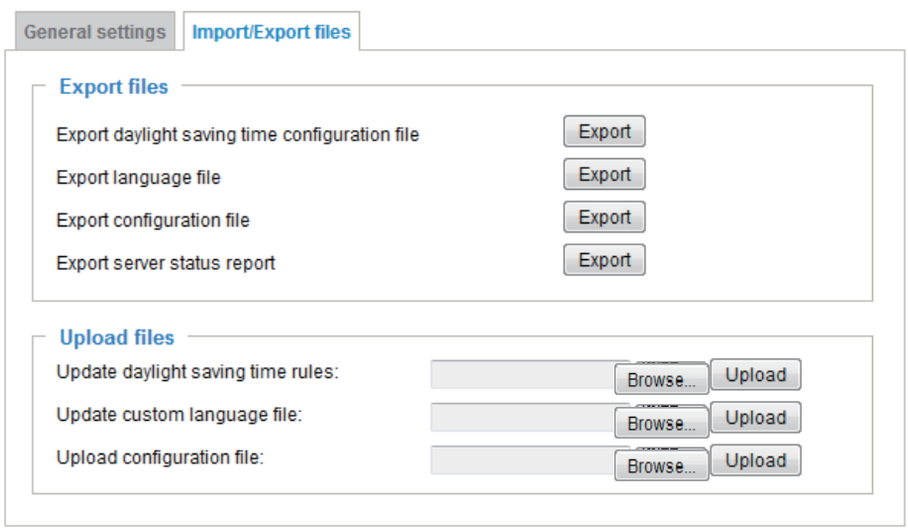
Focus position: このオプションを選択すると以前に保存したレンズの焦点位置を保持することができます。

いずれのオプションも選択されていない場合は、すべての設定が工場出荷時に復元されます。処理中は下図のメッセージが表示されます。



Import/Export files

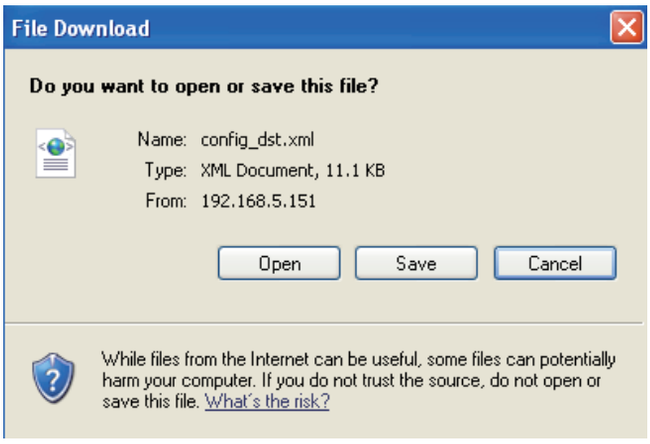
サマータイムルール、カスタム言語ファイル、環境設定ファイル、サーバステータスレポートをエクスポートまたは更新することができます。



Export daylight saving time configuration file: サマータイム(夏時間)の開始と終了時間を設定することができます。

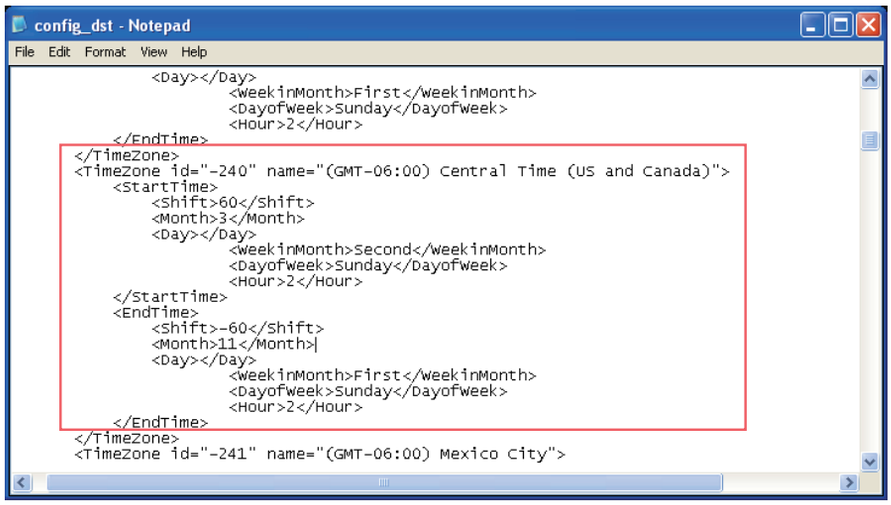
次の手順でデータをエクスポートすることができます。
1. [Export files >Export daylight saving time configuration file]で [Export] をクリックしてサマータイム設定ファイルを取り出します。

2. 下図のようなファイルのダウンロードダイアログが表示されます。[開く] をクリックしてXMLファイルを確認するか、 [保存] をクリックして編集用にファイルを保存します。

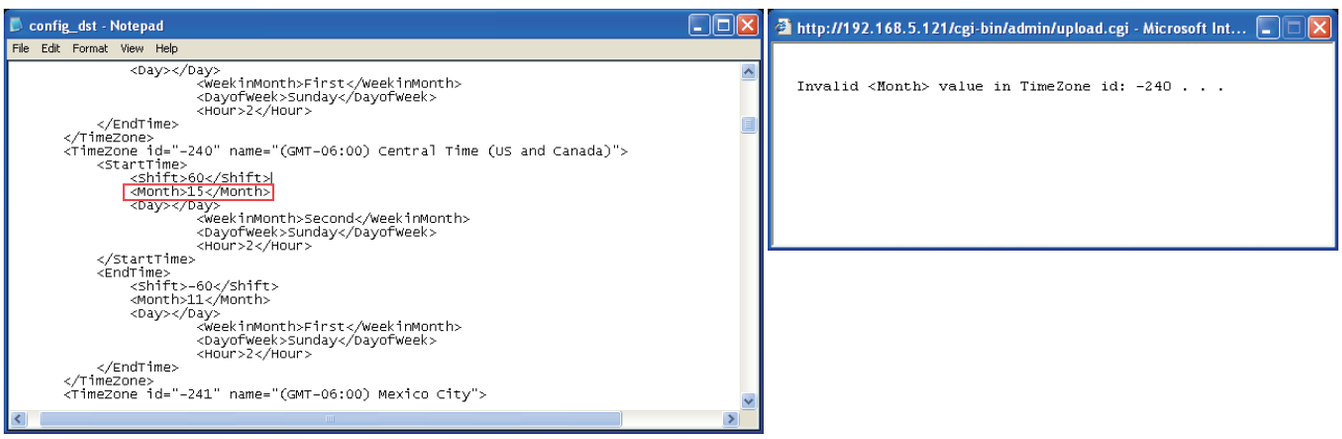


3. Microsoft ® メモ帳でファイルを開き、タイムゾーンを確認し、サマータイムの開始時刻と終了時刻を設定します。設定したら、ファイルを保存してください。

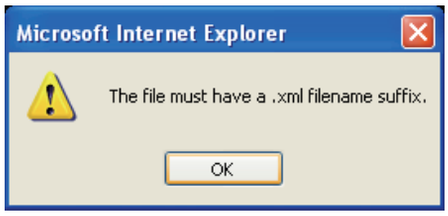
下の例図はサマータイムの設定を「毎年 3 月の第 2 日曜日の 2:00 AM に開始、11 月の第 1 日曜日の 2:00 AM に終了」と設定しています。



Update daylight saving time rules: [Browse...]をクリックし、更新するXMLファイルを指定します。
誤った日時を設定するとファイルをアップロードしたときに下図のような警告メッセージが表示されます。



不正なファイル形式をアップロードしようとすると、次のメッセージが表示されます。



Export language file: クリックすると、言語ファイルがエクスポートされます。英語、ドイツ語、スペイン語、フランス語、イタリア語、日本語、ポルトガル語、中国語(簡体/繁体)、ロシア語の10の言語が提供されています。

Update custom language file: [Browse...]をクリックし、アップロードするカスタム言語ファイルを指定します。

Export configuration file: クリックすると、デバイスおよびユーザー定義スクリプトのすべてのパラメータがエクスポートされます。

Update configuration file: [Browse...]をクリックすると、構成ファイルを更新することができます。デバイスのモデルとファームウェアバージョンが構成ファイルと同じである必要があります。デバイスに固定IPまたはその他の特殊な設定を設定している場合は、構成ファイルを更新しないでください。

Export server staus report: クリックすると、時刻、ログ、パラメータ、プロセスステータス、メモリステータス、ファイルシステムステータス、ネットワークステータス、カーネルメッセージなど、現在のサーバーステータスレポートをエクスポートすることができます。

ヒント:

- ファームウェアのアップグレードが停電などによって中断された場合でも、動作を復元する手段があります。カメラを通常の状態に戻す方法については、以下を参照してください。

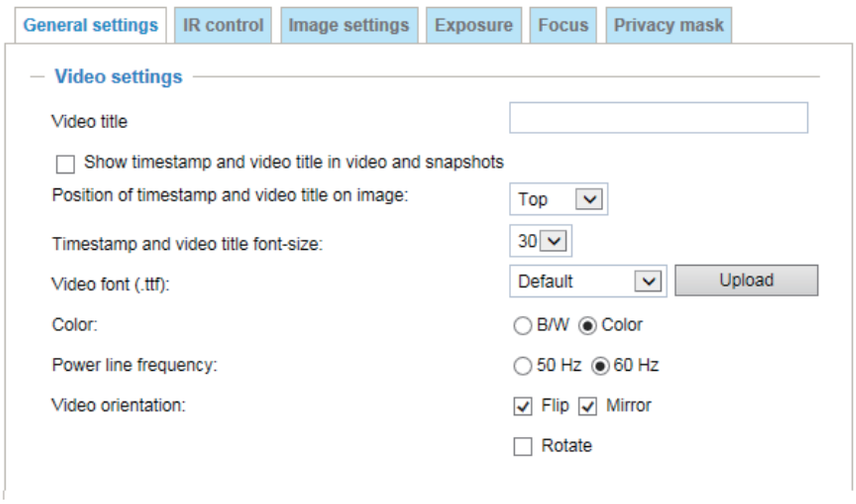
  適用可能シナリオ:
  (a) ファームウェアのアップグレード中に電源が切断された場合。
  (b) LEDステータスが異常を示す原因が不明で、初期化で正常な状態を復元できない場合。

  この場合、下記の方法を使用して、バックアップファームウェアでカメラを正常にすることができます。
  (a) リセットボタンを1分間以上押し続けます。
  (b) 赤のLEDがすばやく点滅するまで、カメラの電源ボタンを押し続けます。
  (c) 起動後、カメラのファームウェアはその前のバージョンに戻ります。
  (この手順は、通常の起動プロセスよりも5~10分長くかかります。)このプロセスが完了すると、LEDのステータスは正常に戻ります。

Media （メディア） > Image（画像）

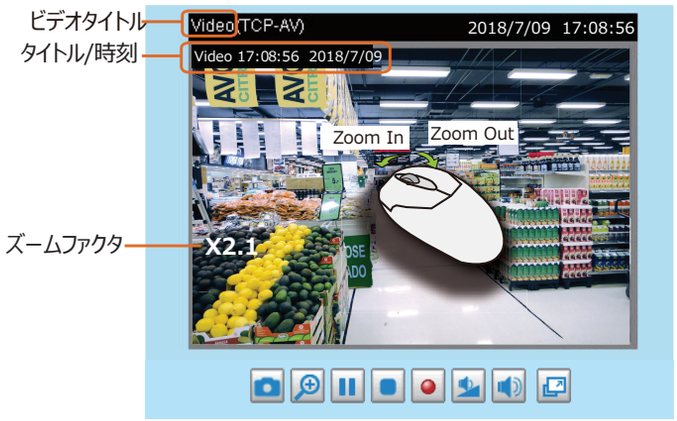
ここでは、ネットワークカメラの画像設定について説明します。このページは、[General settings]、[IR control]、[Image settings]、[Exposure]、[Privacy mask] から構成されています。

General settings



Video title:ライブビデオのタイトルバーに表示される名前を入力することができます。

Show timestamp and video title in video and snapshots: 選択するとライブビデオとスナップショットの画面上にビデオタイトルと時刻をスタンプして表示します。



Position of timestamp and video title on image: タイムスタンプとビデオタイトルを表示する位置を選択します。

Timestamp and video title font size: タイムスタンプとビデオタイトルのフォントサイズを選択します。

Video font (.ttf): True Typeフォントファイルをアップロードすると、そのフォントでビデオタイトルを表示することができます。

Color: ビデオストリームの色（カラー/白黒）を選択します。

Power line frequency: カメラの設置場所と一致する電源周波数を設定して、蛍光灯による画像のちらつきを削減することができます。

Video orientation: ビデオの向きを選択することができます。

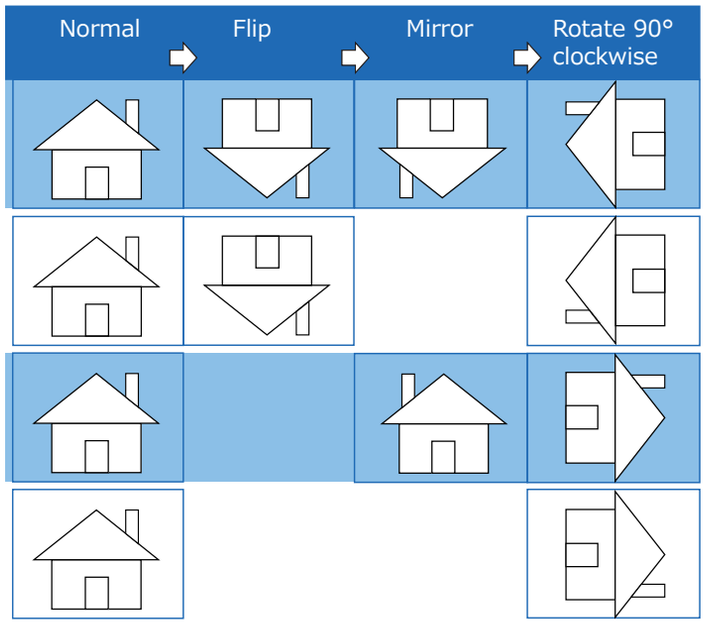
[Flip](反転)：ライブビデオの表示を垂直方向に反転します。
[Mirror](ミラー)：ライブビデオの表示を水平方向に反転します。
ネットワークカメラが上下逆に取付けられている場合は、両方のオプションを選択してイメージの向きを修正します。
[Flip]と[Mirror]の設定後はプリセットした位置情報はクリアされます。

[Rotate](回転)



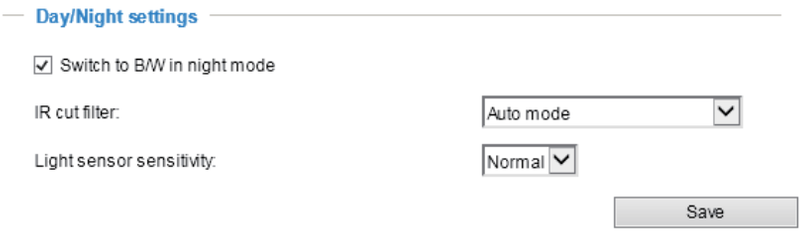
ライブビデオの表示を時計回りに回転します。ローテーションは、[Flip]、[Mirror]の各設定で適用することができ様々な取り付け位置に適応します。

右図は、最左側の４つの図を左から順にフリップ/ミラー/90°回転させた状態を示しています。



カメラは、建物の内部や外部のあらゆる場所に対応するために、垂直面、側面、傾斜面に設置できるようになっています。建物の内部は、廊下など細長い長方形の空間があり、アスペクト比16:9のような従来のHD映像では、こういった縦に長い視界に一致させることができません。しかしライブビデオを回転させることで、このような縦に長い視界をより簡単にカバーすることができます。

Day/Night Settings



Switch to B/W in night mode
選択すると、ネットワークカメラはナイトモード時に自動的に白黒に切り替わります。

IR cut filter
赤外線カットフィルタの自動切換えにより、暗い環境では自動的にIRカットフィルタを取り外し、センサに赤外線領域の光を通すことができます。

- Auto mode
  ([Auto mode]が選択されている場合、[Day/Night Exposure Profile]は使用できません。)
  ネットワークカメラは、周囲の光のレベルを判断してフィルタを自動的に切り替えます。
- Day mode
  [Day mode]では、ネットワークカメラは赤外線カットフィルタを常時オンにして、赤外線領域の光がセンサに入射するのをブロックし、色が歪まないようにします。
- Night mode
  [Night mode]では、ネットワークカメラは赤外線カットフィルタを常時取り外して、センサが赤外線領域の光まで受光できるようにし、低照度時の感度を改善します。
- Synchronize with digital input
  独自の照度センサを持つ外部の赤外線デバイスが接続されている場合、その外部赤外線デバイスにより、デジタル入力を使用してカメラの赤外線カットフィルタの切換えをトリガーできます。これにより、カメラと外部赤外線デバイスの動作を同期させることができます。
- Schedule mode
  [Schedule mode]では、指定されたスケジュールに基づいて[Day mode]と[Night mode]を切り替えることができます。[Day mode]の開始時刻と終了時刻を入力してください。
  なお、時刻形式は24時間表記の[hh:mm]となります。工場出荷時には、[Day mode]の開始時刻と終了時刻は07:00と18:00に設定されています。

Light sensor sensitivity:赤外線カットフィルタが切り替わるときの照明条件を[Low]、[Normal]、[High]の３段階に調整することができます。

設定が完了したら、[Save]をクリックして設定を有効にします。

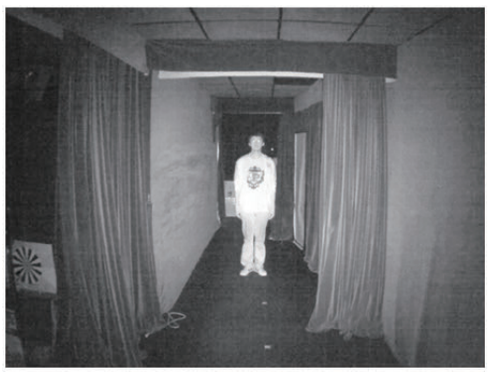
IR control

Turn on built-in IR illuminator in night mode:カメラが低照度状態を検出してナイトモードに入ったときにカメラの内蔵IRイルミネータをオンにする場合に選択します。

Anti-overexposure: この機能を有効にすると、ナイトモードでの露出オーバーを避けるために、カメラが自動的に隣接する物体へのIR投影を調整します。

スマートIR機能は、侵入者のスポットや興味のある対象物がレンズとIRライトの近くにある場合に、より有益です。例えば、3メートルの範囲に侵入者が近づく可能性がある場合、スマートIRは露出オーバーを効果的に抑えることができます。より遠くの監視エリア、例えば5m以上離れた場所では、スマートIR機能は近距離ほど大きな効果をもたらさないかもしれません。

スマートIR無効; 距離: 5M



スマートIR対応; 距離: 5M



スマートIR無効; 距離: 3M



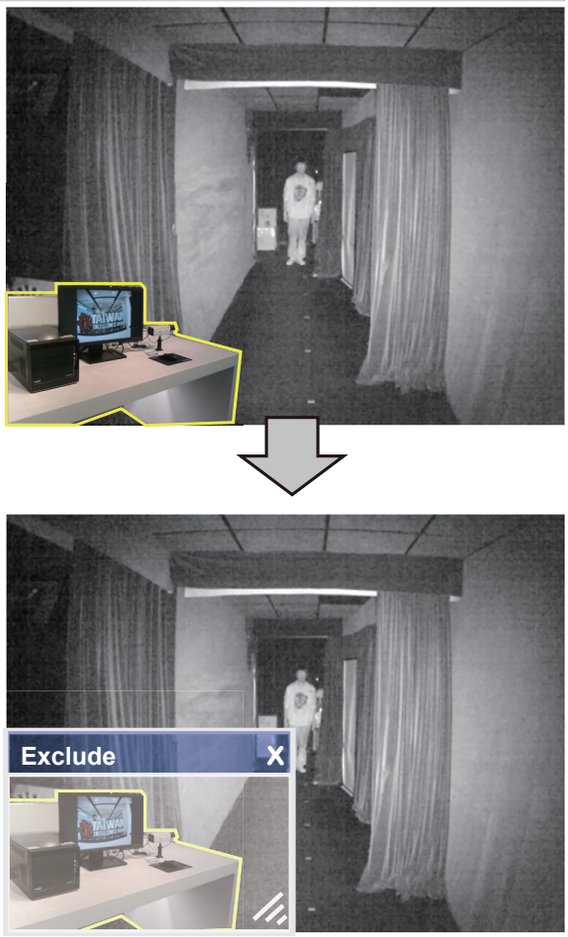
スマートIR対応; 距離: 3M



ヒント:

近くに物体があると、そこから反射してくる赤外線がSmart IRの光量計算を誤らせることがあります。この問題を解決するには、露出設定ウィンドウで、避けられない物体に「露出除外」ウィンドウを配置します。その方法は62ページを参照してください。

また、ナイトモードの「プロファイル」設定で「Exposure Exclude」ウィンドウを設定することで、昼間の設定に影響を与えないようにすることができます。



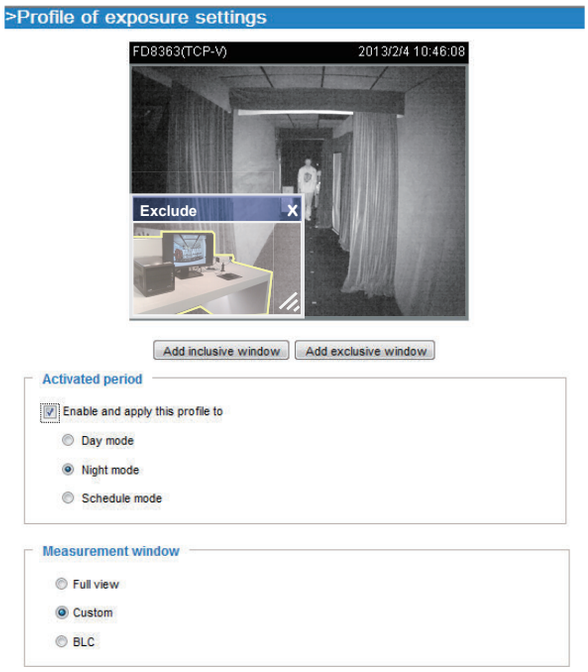


Image settings

この項目では、ホワイトバランスと画像調整を設定できます。



White balance: 最適な色温度に調整します。
■ Auto:光源の変化に対応し、カメラの色温度を自動的に調整します。

■ Fixed Current
特定のホワイトバランス状態に固定させるとき、下記の手順で設定します。
1. ホワイトバランスをAuto(自動)に設定します。
2. 白色の紙を用意し、レンズの前に配置して、ネットワークカメラが自動的に色温度を調整できるようにします。
3. カメラがホワイトバランスを自動的に測定して調整した後、Fixed currentを選択し、設定を確定します。

■Manual: RGainとBGainのスライドバーを動かし、色温度を手動で調整することもできます。

Image Adjustment
スライドバーで数値を変更し、最適な画質に調整します。
■ Brightness：画像の明るさを0%~100%の範囲で調整します。

■ Contrast：画像のコントラストレベルを0%~100%の範囲で調整します。

■ Saturation：色の濃さを0%~100%の範囲で調整します。

■ Sharpness：画像のシャープネスを0%~100%の範囲で調整します。

■ Gamma curve：画像のガンマ曲線を 0.45～1 の範囲で調整します。通常は[Optimize]を選択します。Manual モードを選択してスライドバーのポインターを動かして、画像の暗い箇所と明るい箇所の両方に対し、ガンマ補正を行って高コントラストを選ぶか、詳細を際立たせるために高輝度を選ぶことができます。
WDR機能を有効にしている場合、このオプションは無効です。

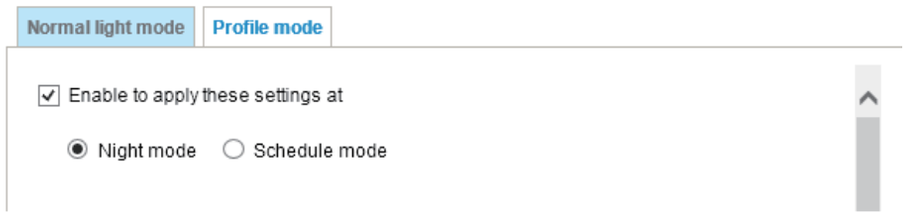
Defog: スモッグ、霧、煙などの悪天候時に、撮影された画像の鮮明度を改善することができます。

Noise reduction

■ 画像のノイズやちらつきを減らす機能です。このカメラには3D Noise Reduction機能が搭載されています。スライドバーを使用して、削減効果を調整します。
3D Noise Reductionは、暗い環境でのノイズの抑制に効果があります。しかし動く被写体を撮影する場合に残像が発生する場合があります。このような場合は強度を下げて使用してください

ノート：

[Image settings]にはプレビューボタンはありません。加えられた変更はすべて画面に直接表示されます。[Restore]を クリックすると、変更を適用せずに元の設定を復元することができます。設定が完了したら、[Save]をクリックして設定を有効にしてください。[Profile mode]では、タブ内のすべての設定を特定のモード時の設定値とすることもできます。



Enable to apply these settings at: プロファイルを適用するモードを[Night mode]、[Schedule mode]から選択することができます。[Schedule mode]を選択する場合は、時間範囲を手動で入力してください。次に[Save]をクリックして設定を有効にします。

Exposure

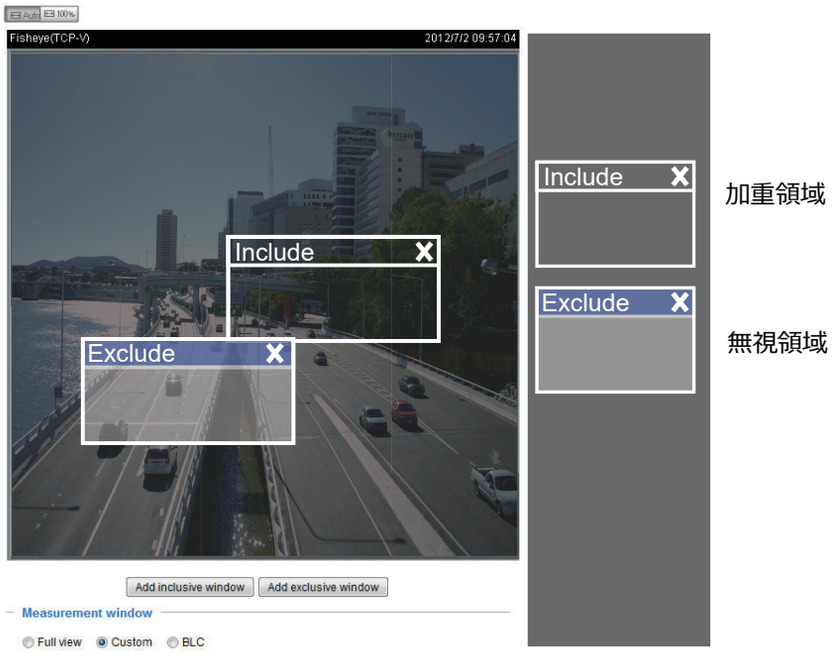
この項目では、露出測定ウインドウ、露出レベル、露出モード、露出時間、ゲインコントロール、デイナイトモードの設定を行います。通常のモード用と[Night mode/Schedule mode]などの特定のモード用の 2 種類の設定を行うことができます。



Exposure strategy:
Measurement window: 露出を計測するための計測ウインドウを設定します。 被写体の背景に非常に明るい光がある場合などに効果があります。たとえば、建物の廊下から差し込む明るい太陽光を除外することができます。

- Full view：画面全体に対して、適切な明るさとなるよう、露出を調整します。
- Custom：このオプションを選択すると、カスタマイズしたウインドウを包含領域または排他領域として手動で追加することができます。合計10個のウインドウを構成できます。詳細は次ページをご参照ください。

インクルーシブウインドウは [weighted window]、エクスクルーシブウインドウは [Ignored window] として認識されます。加重平均法を採用しているため、インクルーシブウインドウの優先順位が高くなります。このウインドウは重ねて表示することができ、インクルーシブウインドウ内にエクスクルーシブウインドウを配置すると、重なったウインドウはエクスクルーシブウインドウとして認識され、残りのインクルーシブウインドウから露出レベルが計算されます。



- BLC (バックライト補正): この機能は、ウインドウの中央に自動的に[weighted region(重み付けした領域]を設定し、適切な露出となるよう動作します。

- HLC: (ハイライト補正): この機能は、カメラが強い光源を検出し、それによる影響を補正して全体の画質を改善します。たとえば、HLCはスポットライトやヘッドライトによってできるにじみを減らすことができます。

Exposure control:

- Exposure level: 露出レベルは-2.0 ～ +2.0(暗い～明るい) の範囲で手動で設定することができます。露出時間とゲインコントロールスライドバーの半円ポインタをクリック＆ドラッグし、最適な画像を得られるよう、カメラが自動的に調整するシャッター速度とゲインの範囲を指定できます。シャッター速度を速くすると光量が減ってしまうため、明るさを増す必要がありますが、動きのある被写体を適切に撮影することができます。

- Flickerless: (WDR Proが無効時に使用可能)
  映像の周波数とAC電源周波数が一致しない状況では、この差によって色ずれや画像のちらつきが発生することがあります。このようなときに、このチェックボックスを選択すると、露出時間(シャッター速度)の範囲はAC電源周波数に合う範囲に制限され、電源周波数が60Hzの場合、シャッター速度は1/120より長くなります。
  固定アイリスレンズを搭載したカメラでは、シャッター速度が 1/120 秒より長くなると、レンズに過度の光量が入力される可能性があります。

- Exposure time :
  ポインタを動かして、露出時間制御の範囲を設定することができます。デフォルトでは1/32000-1/30 です。

- Gain control :
  ポインタを動かして、ゲイン調整の範囲を設定することができます。デフォルトでは0-100% です。

AE Speed Adjustment：この機能は、照明条件が素早く変化する場所を監視する必要がある場合にいます。たとえば、夜間に高速道路の車線や駐車場の入り口をカメラで監視する必要がある場合、ライトを点灯したまま通り過ぎる車によって明るさが急激に変化することがあります。また、カメラが車両に搭載されている場合に、トンネルに出入りする際など急激な明るさの変化に適応する必要がある場合に利用することができます。

WDR：

- Enable WDR Pro：チェックボックスを選択して機能を有効にすると、ワイドダイナミックレンジ(WDR) により、逆光の条件でも明部、暗部の明るさを自動的に調整し、自然な状態で撮影をすることができます。露出時間の異なる2 つの映像を1 つの映像に合成して、ダイナミックレンジの広い映像を撮影することが可能です。

- Enable WDR enhanced：この機能を選択すると、明るい背景（例：入り口など）と被写体とのコントラストが高い場合に、暗い部分の明るさを調整し、画像をより鮮明にとらえることができるようになります。
  [low]、[medium]、[high] の 3 段階から選択し、最適な画質になるように調整してください。

[Restore]をクリックすると、変更を適用せずに元の設定を復元することができます。設定が完了したら、[Save]をクリックして設定を有効にしてください。

[Night mode]、[Schedule mode]用に別の露出設定を行いたい場合は、[Profile mode]をクリックして設定画面を開いてください。

ただし[General settings] > [Day/Night settings] > [IR cut filter]の設定がAuto modeの場合は、このProfile modeは開くことができません。

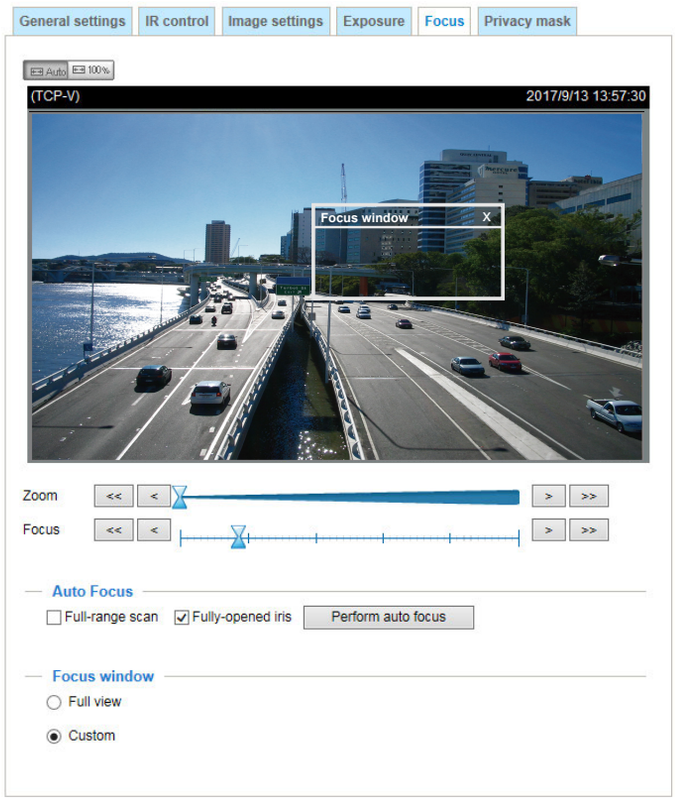
次の手順でプロファイルを設定します:

1. [Profile mode] タブを選択します。
2. [Night mode]、[Schedule mode]のどちらかを選択します。[Schedule mode]を選択する場合は時間範囲を手動で入力してください。
3. 露出設定を行います。詳しくはP64[Exposur econtrol]を参照してください。
4. [Save]をクリックして設定を有効にし、[Close]をクリックしてページを閉じます。



Focus

ここでいうフォーカスとは、ステッピングモーターレンズを搭載したネットワークカメラに搭載されている「リモートフォーカス」のことです。自動フォーカス調整機能により、カメラのフォーカスを物理的に調整する必要はありません。屋外に多数のカメラを設置する場合、数日から数週間後にカメラの焦点が合わなくなったときに、自動焦点調整機能は非常に役立ちます。また、自然の力の影響を受けやすく、例えば、広範囲の使用温度による収縮や膨張、振動などの影響を受けます。



以下は、自動フォーカス機能を実行する手順です。

1. フォーカス調整を全体表示で行うか、カスタムフォーカスウィンドウ内で行うかを、画面下部から選択します。カスタムウィンドウを作成し、画面上の任意の位置にウィンドウをクリック＆ドラッグすることができます。

2. センサーボードのデフォルトのバックフォーカス位置にリセットすることをお勧めします。

3. 全開アイリス」チェックボックス（デフォルト）を使って、アイリスサイズを大きくすることで、より良いピント調整結果を得ることができます。

4. クリックすると、「全開のアイリス」または「フルレンジスキャン」のボタンが選択されます。フルレンジスキャンを選択した場合、カメラの焦点距離全体をフルレンジでスキャンすると、約 30 ～ 80 秒かかります。フルレンジスキャンを選択しない場合、オートフォーカスのスキャンは最適なフォーカスが得られる長さだけを通過し、約 15 ～ 20 秒かかります。理論的には、カメラのアイリスが完全に開いているときにオートスキャンの最良の結果が得られます。

5. スキャンが完了するのを待ちます。しばらくすると、得られた最も鮮明な画像が表示され、最適なフォーカス範囲が得られるはずです。結果に満足できない場合は、側面の矢印マークを使ってフォーカスを微調整してください。画面上のライブ映像によっては、矢印マークを使ってピントを微調整する必要があるかもしれません。">" はワイドからテレ端への移動を意味し、"<" はテレからワイドへの移動を意味します。

ストリーミングウィンドウの左上にある「サイズ変更ボタン」の使い方は、トップページと同じです。

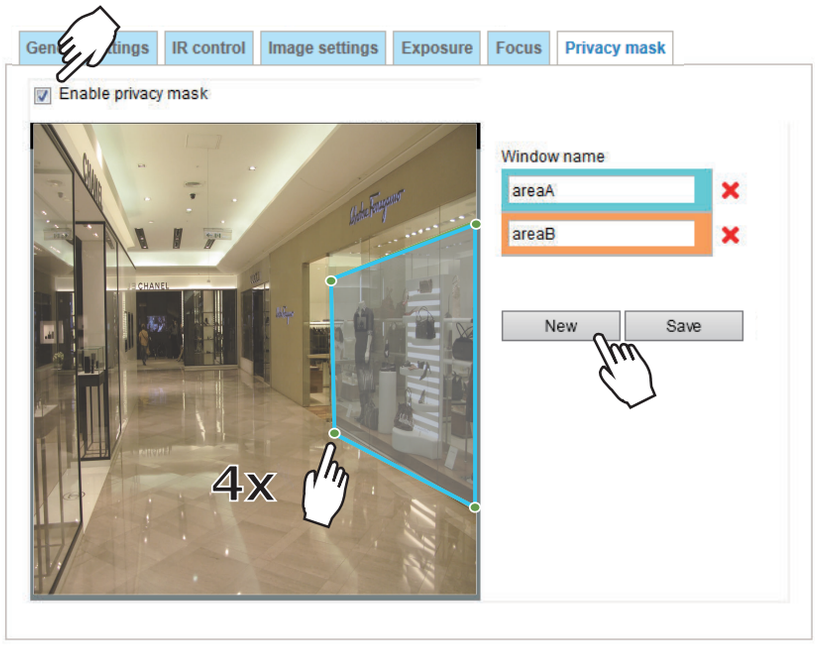
Focus window:
デフォルトでは、フルビューウィンドウに最適なフォーカスが得られます。現在の視野内にカスタムウィンドウを指定して、そのウィンドウから最適なフォーカスを得ることができます。ただし、3m以上離れた廊下など、遠くの背景にフォーカスウィンドウを置くことはできません。フォーカスウィンドウ機能の恩恵を受けることができません。

■ Fフルビュー。フルビュー：フルビューを参照してフォーカスチューニングを行います。

■ カスタム。フォーカスウィンドウを作成して、ビューウィンドウ内の気になる場所にドラッグすることができます。なお、この機能は、一貫した色や質感を持つ立体物をビューウィンドウに表示する場合にのみ使用することをお勧めします。遠くの背景にフォーカスウィンドウを設定した場合、この機能は有効になりません。

Privacy mask

[Privacy Mask]をクリックすると、プライバシーを守るために映像をマスキングする範囲を設定することができます。



■ 次の手順でマスクウインドウを設定します。

1. [New] をクリックして新しいウインドウを追加します。
2. ウインドウを作成したい範囲を囲む四角形を画面上で 4 か所クリックして作成します。作成範囲は実際にカバーする対象物の範囲よりも 2 倍以上（高さ、幅）大きくしてください。
3. [Window Name] を入力し、[Save] をクリックして設定を保存します。
4. [Enable privacy mask] チェックボックスをオンにして、機能を有効にします。

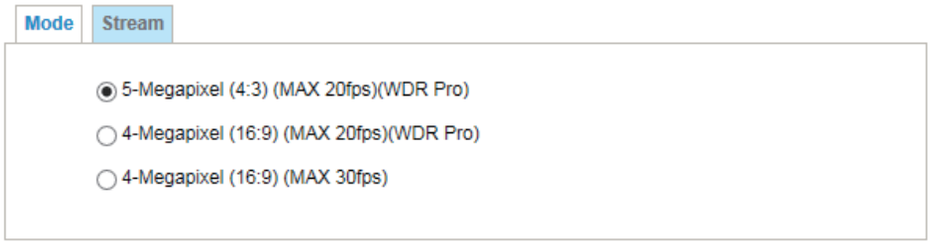
ノート:

► 1 つの画面内では最大 5 つのマスクウインドウを設定することができます。

► プライバシーマスクウインドウを削除するには、[Window name] の右にある [x] マークをクリックしてください。

Media > Video

Mode (IB9388-HT)

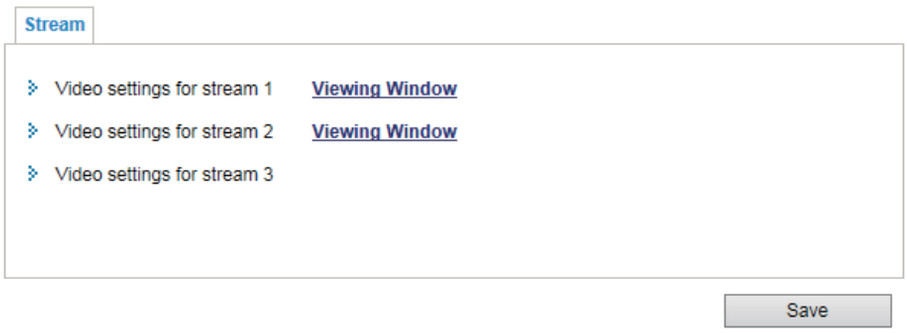


以下のビデオモードを適用することができます。(本項ではIB9388-HTを例に説明します。)

- 5MP (max. 20fps)(WDR Pro): これは、WDR機能を有効にした状態で、画面のアスペクト比が4:3の500万画素のフル解像度です。
- 4MP (16:9) (max. 20fps)(WDR Pro): アスペクト比16:9の場合、WDR機能を有効にすると、使用可能な解像度は4MPに若干低下します。
- 4MP (16:9) (max. 30fps): このモードは、WDR機能を搭載していない4MP解像度のモードです。明るい日差しの中での撮影など、コントラストの高い照明がない場合に使用できます。

Media > Video

Stream settings



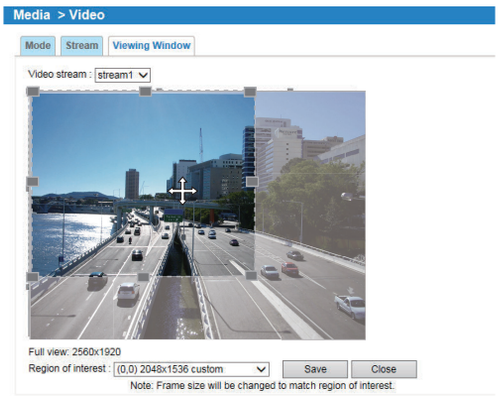
このネットワークカメラは、フレームサイズが480 x 352 ~ 2560 x 1920ピクセルのマルチストリームに対応しています。(本項ではIB9388-HTを例に説明します。)

マルチストリームの定義：

- Stream 1: 「関心領域」と「出力フレームサイズ」を定義することができます。
- Stream 2: 既定のフレームサイズは680 x 480に設定されています。
- Stream 3: 既定のフレームサイズは2560 x 1920に設定されています。

[Viewing Window]をクリックして、表示領域の設定ページを開きます。このページでビデオストリームの関心領域と出力フレームサイズを設定してください。例えば、下図の例では監視対象である駐車場の車だけを表示するようにトリミングして青空の部分を削除し、ビデオストリームの送信に必要な帯域幅を節約することもできます。





次の手順でストリームの設定を行います。

1. 表示領域を設定するストリームを選択します。
2. ドロップダウンリストから関心領域を選択します。カスタマイズした表示領域を設定する場合は、マウスでフローティングフレームサイズを変更し、目的の位置にドラッグすることもできます。
3. モニタリングデバイスのサイズに応じて、フレームサイズのドロップダウンリストから適切な出力フレームサイズを選択します。

ノート:

► 「関心領域」は出力フレームサイズより大きくすることはできません。

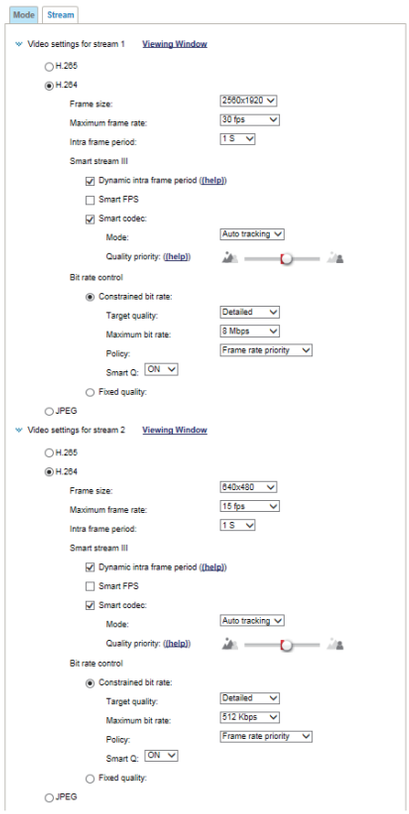
■ マルチストリームのパラメータ

	関心領域	出力フレームサイズ
Stream 1	2560 x 1920 ~ 480 x 352 (選択可)	2560 x 1920 ~ 480 x 352 (S選択可)
Stream 2	2560 x 1920 ~ 480 x 352 (選択可)	2560 x 1920 ~ 480 x 352 (選択可)
Stream 3	既定	既定

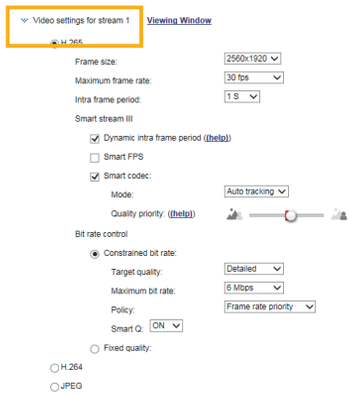
[Viewing Window]の設定が完了したら、[Save]をクリックして設定を有効にし、[Close]でウインドウを閉じてください。選択した出力フレームサイズは、各ビデオストリームのフレームサイズに即時適用されます。その後[e-PTZ function]をテストできます。[e-PTZ function]についてはP113をご参照ください。



[stream item] をクリックすると、詳細情報が表示されます。最大フレームサイズは [Viewing Window] セクションでの設定に従います。



このネットワークカメラはリアルタイムの H.265、H.264、MJPEG 圧縮規格 (トリプルコーデック) に対応します。H.265 または H.264 モードが選択されている場合、映像は RTSP プロトコルでストリーミングされ、ビデオ調整に関する多くのパラメータがあります。



■ Frame size：表示デバイスごとに異なる解像度を設定することができます。携帯電話でのリモート表示では小さいフレームサイズと低いビットレート、NVRのストリーム録画やWebブラウザでのライブ表示では大きいフレームサイズと高いビットレートというような設定が可能です。フレームサイズが大きいほど帯域幅は大きくなります。

■ Maximum frame rate：1秒あたりの最大フレームレートを設定します。フレームレートを高く設定すると、映像の動きが滑らかになり動いている対象物を認識することが容易になります。AC電源周波数を50Hzに設定した場合、フレームレートは1/2/3/5/8/10/12/15fpsおよび最大25fpsまで選択することができます。AC電源周波数を60Hzに設定した場合、フレームレートは1/2/3/5/8/10/12/15fpsおよび最大30fpsまで選択することができます。[Customize]を選択し手動で値を入力することもできます。MD9561-H、MD9581-Hは最大60fpsのフレームレートをサポートしています。

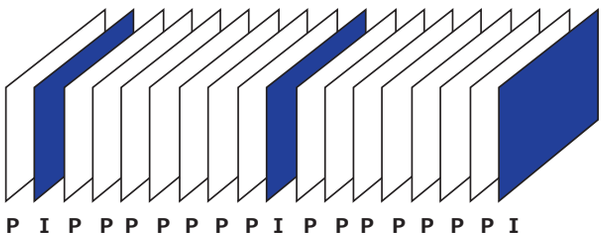
フレームレートはフレームサイズを高くすると減少します。

■ Intra frame period
I フレームを挿入する間隔を決定します。間隔が短いほど画質は向上しますが、ネットワーク帯域幅の消費量は増加します。1/4秒、1/2秒、1秒、2秒、3秒、4秒から選択することができます。

■ Smart stream III

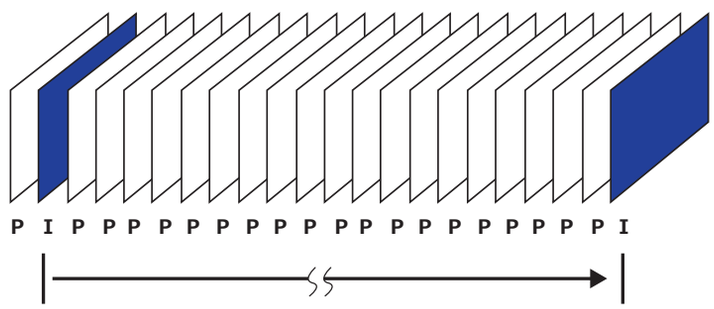
■ Dynamic Intra frame period
H.265などの高品質モーションコーデックは、ビデオフレーム間の冗長性を利用し画質とビットレートのバランスを調整してビデオストリームを配信します。

下図は符号化パラメータを要約したものです。
I フレームはフレーム内すべての情報を保持しており、サイズは大きくなります。一方、P フレームは前方向予測を用いて符号化されたフレームで、エンコーダは冗長性のある画像情報のために前のI フレームを参照します。
図：H.264/265のフレームタイプ



I フレームの挿入間隔を最大10秒まで動的に延長すると、ビデオストリーミングに必要なビットレートを大幅に削減できます。この機能を使用すると、静的シーンの映像をストリーミングする場合、帯域幅を最大53%節約できます。節約される帯域幅の量は、フレーム間の動き予測によっても変わります。シーンに動きがある場合、映像品質維持のためにI フレームの挿入間隔を自動的に短縮します。
一方、暗い場所や夜間のシーンでは、ノイズによりP フレームのサイズが大きくなる傾向があり、帯域幅の節約効果は小さくなります。

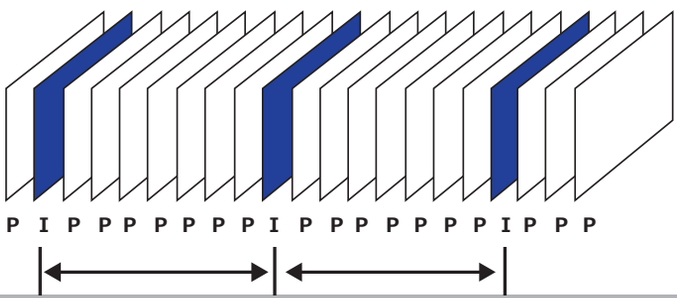
通常、一般的な2MPのストリーミングには、3 ~ 4Mb/秒の帯域幅が必要です。この機能を使用すると、中程度の動きの場面をストリーミングするための帯域幅を2 ~ 3Mb/秒に、動きの少ないシーンでは500kb/秒にまで削減することができます。





静止場面

静止場面での
Dynamic Intra Frame





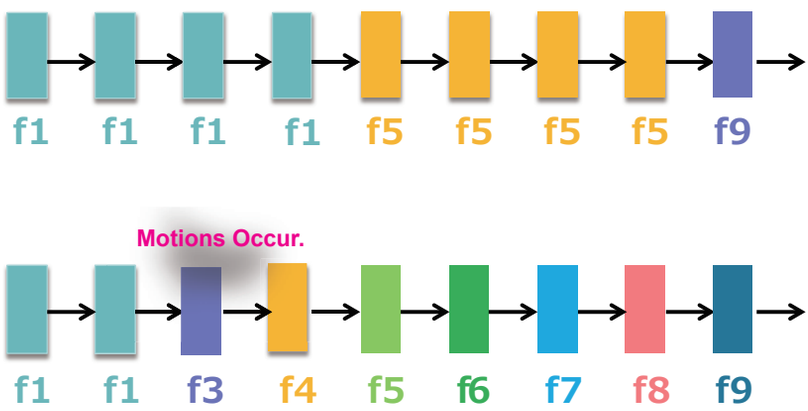
動きのある場面

動きのある場面での
Dynamic Intra Frame

H.265コーデックを使用しDynamic Intra frameをSmart Stream機能と組み合わせると、H.264を使用した場合に比べておよそ80%の帯域幅を節約することができます。

■ Smart FPS

静止場面では、シーン内に動きがない場合、アルゴリズムは古いフレームをキューに入れます。動きがあると、エンコーディングが再度始まりリアルタイムストリーミングを配信します。



静止場面の古いフレームをキューに入れることで、カメラの負荷と P フレームのサイズの両方を削減することができます。またフレームレートを低下させないためにも効果的です。

シーンに動きがあったときに、Smart FPS から通常のエンコーディングに戻すためのフレーム間差分しきい値は 1% です。

ノート:

Smart Stream IIと比較すると、Smart Stream IIIにはSmart QとSmart FPSの2つの設定オプションが追加されました。

- Smart_codec: スマートコーデックは全体または画面上の重要ではない領域の画質を効果的に低下させ、消費される帯域幅を削減します。

  重要な領域（ROI)と重要ではない領域(非ROI)の画質を手動で指定できます。



スマートコーデックを使用するときは下記の動作モードを選択します。

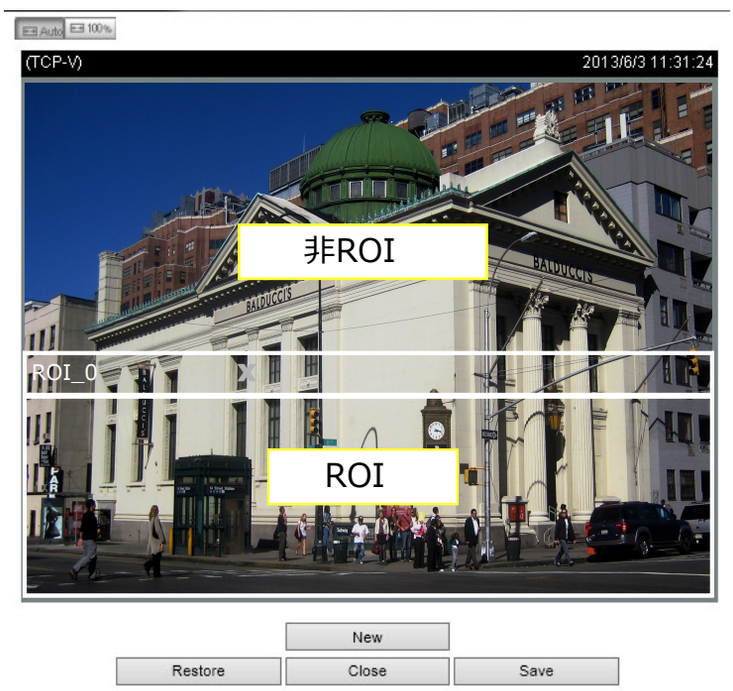
- Auto tracking:

  このモードでは、まず画面全体が非ROI領域に設定されます。画面の一部に動きがあると、動きのある領域が自動的にROI領域に設定され、高画質で伝送されます。そのほか　の領域は低画質のまま伝送されます。

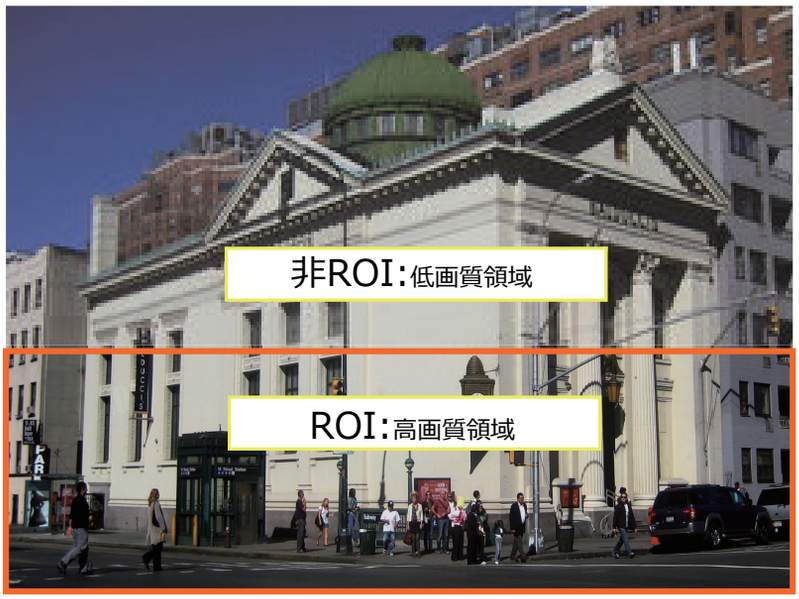
- Manual:

  手動モードでは画面上に3つのROIウインドウを設定できます。ROIウインドウに含まれていない領域は非ROI領域と見なされます。ROI領域は、高画質で送信されます。

下図の例は、画面の上半分は重要ではない領域(非ROI)として、画面の下半分は重要な領域(ROI)として設定した例です。(歩道など)



この結果、画面の下半分は常に高精細に表示され、画面の上半分は低画質で送信されます。上半分の画質は劣りますが、画面全体では一連の映像として何が起きているかを認識することができます。



- Hybrid:

[Manual] モードと[Hybrid]モードの主な違いは次のとおりです。

[Hybrid] モードでは、非ROI領域の被写体に動きがあった場合、対象の被写体とその周囲の画質が自動的に改善されます。

[Manual] モードでは、非ROI領域は内部の被写体に動きがあっても常に低画質で送信されます。



- Quality priority:

ROIと非ROI領域の画質の差をスライドバーで調整することができます。

スライドゲージが右側にあるほど、ROI領域の画質は高くなります。反対に、スライドゲージを左に移動すると、非ROI領域の画質が高くなります。

たとえば、ROIウインドウで保護エリアをカバーして、この機能で画質を調整すれば、ROIウインドウをプライバシーマスクのように設定することができます。その逆の設定も可能です。

スマートストリームの高画質映像と低画質映像の両方の帯域幅消費量を抑制するには、[Maximumbit rate] をプルダウンメニューからしきい値として設定する必要があります。

■ Bit rate control

Constrained bit rate:

複雑なシーンでは一般にファイルサイズが大きくなるため、データ転送に必要な帯域幅が大きくなります。そこで、利用する帯域幅のレベルを選択して設定することが有効です。このモードでは映像品質は変化します。利用する帯域幅は、20/30/40/50/64/128/256/512/768Kbps、または1/2/3/4/6/8/10/12/14/40Mbpsのビットレートの中から選択することができます。
また[Customize]を選択し手動で40Mbpsまでの値を入力して設定することもできます。

- - Target quality:
  [Medium] から [Excellent] の範囲で目標となる画質を選択することができます。

  - Maximum bit rate:
  プルダウンメニューからビットレートを選択することができます。選択できる範囲は20kbps~最大40Mbpsです。ビットレートは平均的な映像における上限のビットレート値になります。ネットワークカメラはビットレートの制限内もしくは制限に沿った形でビデオストリームを配信します。

  - Policy:
  [Frame Rate Priority]を選択すると、ネットワークカメラは1秒あたりのフレームレート数の維持を優先します。画質は低下することがあります。一方、[Image Quarity Priority]を選択すると、ネットワークカメラは画質の維持を優先します。この場合、フレームレート数が低下することがあります。

Smart Q :

ONまたはOFFを選択して、機能の有効化または無効化を行います。Smart Qはシーンを意識しています。Smart Qは、次のような方法でフレームサイズとビットレートの消費を抑えます。

■ 光量の少ないフレームで、輝度の異なるシーンの画質を動的に調整することができます。ノイズが少ないということは、消費する帯域も少ないということです。
■ I フレームとPフレームで異なる品質を裏書きすることで、フレームサイズを小さくすることができます。
■ 1つのフレームを分割して、それぞれに異なる品質を与えること。草木が生い茂っていたり、窓が網戸になっていたり、パターンが繰り返されていたり（壁紙のような複雑な布地のパターン）するような複雑性の高いエリアでは、画質の値を低くしても人間の目にはほとんど影響がありません。

不必要な画質は人間の目には認識されず、ビットレートを浪費します。

Smart Qストリーミングは、異なる照明条件において、同じ画像品質を維持しながら、最大50%から80%の帯域幅を節約することができます。これらの数値は、Smart Stream IIとSmart Stream IIIのストリーミングを比較したものです。.

Fixed quality:

[Fixed quality]を選択すると、すべてのフレームが同じ画質で送信されます。帯域幅はシーンによって変動します。映像画質は[Medium]、[Standard]、[Good]、[Detailed]、[Excellent] の中から設定することができます。また、[Customize]を選択し手動で値を入力することもできます。

Maximum bit rate:

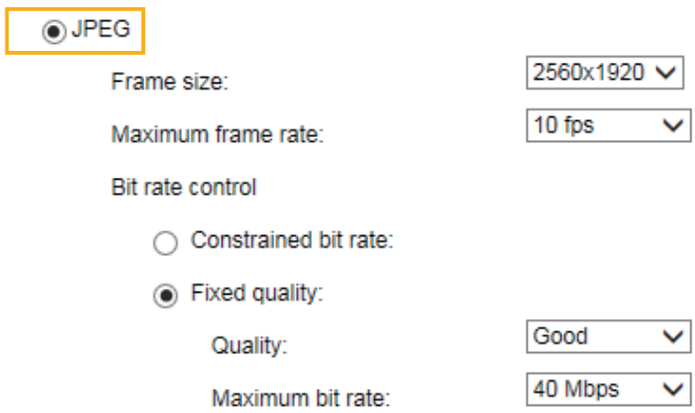
画質優先の場合でも、帯域幅やストレージを考慮してビデオストリームのサイズを制御するビットレートの制限を設定することができます。1Mbps～40Mbpsの間でビットレートを設定することが可能です。

[Fixed quality]で[Maximum bit rate]を設定すると、ネットワーク帯域幅の制限があるとき、設定値を超えないように伝送することができます。[Fixed quality]が適用された低照度のシーンでは、カメラのゲインアップでノイズが発生して、ビデオストリームのデータサイズが大幅に増加する可能性があるので、注意が必要です。

[Customized]オプションを選択して、ビットレート値を手動で入力することもできます。

JPEG

モードを選択すると、連続したJPEG画像をクライアントに送信し、複数の静止画を連続して表示することで動きのある映像として表示することができます。転送されるすべてのJPEG画像は同じ画質となります。また、JPEG画像の組み合わせであるため、オーディオデータはクライアントに送信することができません。JPEGモードでは、ビデオ設定のため3つのパラメータが用意されています。



■ Frame size

表示デバイスごとに異なるビデオ解像度を設定できます。例えば、携帯電話でのリモート表示では小さいビデオサイズと低いビットレート、Webブラウザでのライブ表示では大きいビデオサイズと高いビットレートというような設定が可能です。フレームサイズが大きいほど帯域幅は大きくなります。

■ Maximum frame rate

1秒あたりの最大リフレッシュフレームレートを制限します。フレームレートを高く設定すると、より滑らかな映像品質が得られます。

電源周波数が50Hzの場合（解像度5MPの場合）、フレームレートは1fps、2fps、3fps、5fps、8fps、10fps、15fpsから選択できます。電源周波数が60Hzに設定されている場合、フレームレートは1fps、2fps、3fps、5fps、8fps、10fps、15fpsから選択できます。また、「カスタマイズ」を選択して、手動で値を入力することもできます。高解像度を選択した場合、フレームレートは低下します。

前述のページでは、モーション JPEG の送信時に消費する帯域を制御するために、平均または上限の閾値を設定しています。設定方法は H.264 の場合と同じです。

Constant Bit Rate などの設定については、前ページを参照してください。

ノート:

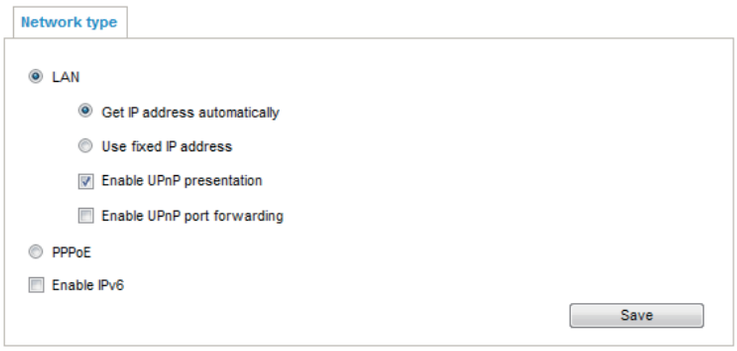
► 一般に圧縮率を小さくすると画質は良くなりますが、データ量は増加します。

► 高品質なビデオ設定は、CPU の負荷を大幅に増加させ、複雑なシーンの映像などでストリーミングの切断やビデオデータの破損が発生するおそれがあります。問題が発生した場合は、ビデオ設定をカスタマイズして解像度を低くしたり、フレームレートを下げてスムーズなビデオを伝送できるようにしてください。

Network > General settings

この項目では、ネットワークカメラの有線ネットワーク接続を設定する方法を説明します。

Network Type

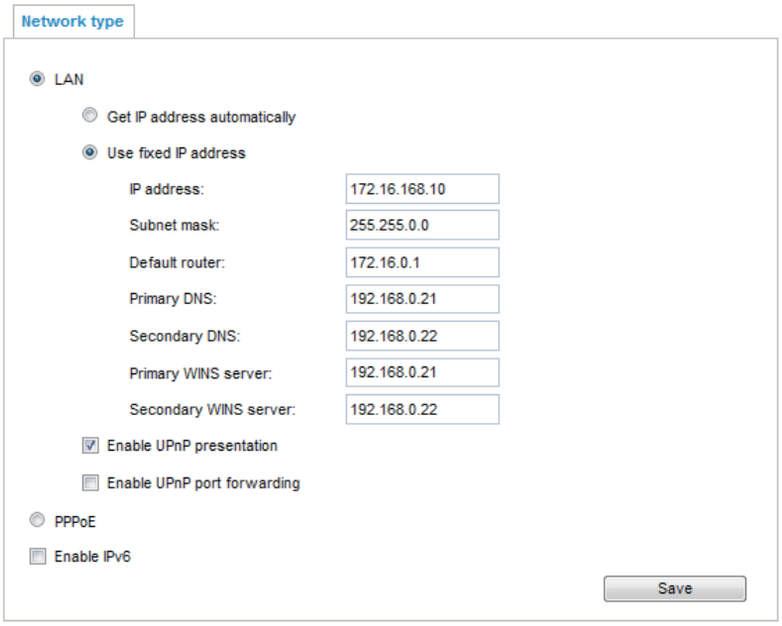


LAN

このオプションを選択すると、ネットワークカメラはローカルエリアネットワーク(LAN)上に展開され、ローカルコンピュータからアクセスすることができるようになります。お買い上げ時の設定はLANになっています。設定が完了したら、[Save] ボタンをクリックしてください。

Get IP address automatically: このオプションを選択すると、カメラはLANに接続されるたびにDHCPサーバーによって割り当てられる使用可能なIPアドレスを取得します。

Use fixed IP address: このオプションを選択すると、ネットワークカメラに固定IPアドレスを手動で割り当てます。



1. VIVOTEK の WEB サイトから Shepherd をインストールして起動すると、ネットワークカメラを LAN に簡単に設定することができます。詳しくは P15[ソフトウェアのインストール] を参照してください。

2. ネットワーク管理者から提供された固定 IP、サブネットマスク、デフォルトルータ、プライマリ DNS を入力してください。

Subnet mask: アドレスが同じサブネット内にあるかどうかを判別するために使用されます。デフォルト値は[255.255.255.0]です。

Default router: 異なるサブネット内のアドレスにフレームを転送するために使用するゲートウェイです。
ルータ設定が無効の場合、異なるサブネット間のアドレスへの転送も無効になります。

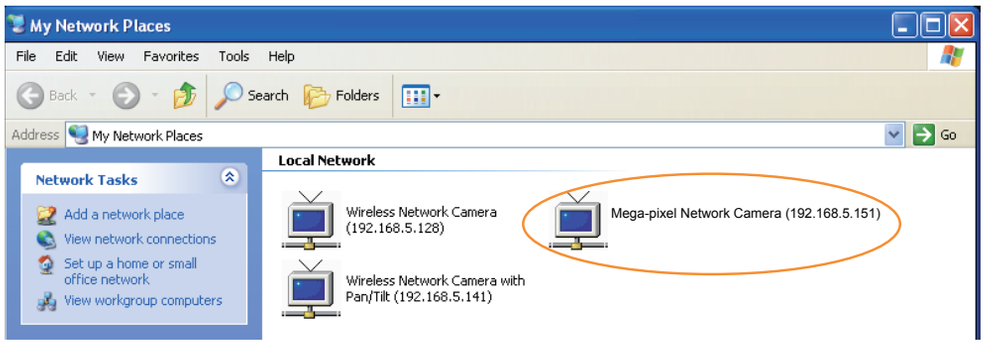
Primary DNS: ホスト名をIPアドレスに変換します。

Secondary DNS: プライマリDNSをバックアップします。

Primary WINS server: コンピュータ名とIPアドレスのデータベースを管理します。

Secondary WINS server: コンピュータ名とIPアドレスのデータベースを管理します。

Enable UPnP™ presentation: このオプションを選択すると、ネットワークのUPnP™プレゼンテーションを有効にすることができます。ネットワークカメラがLANに接続されるたびに、接続されたカメラのショートカットが[My Network Places]に一覧表示されます。ショートカットをクリックすると、Webブラウザにリンクすることができます。現在、UPnP™はWindows XP以降でサポートされており、この機能を使用するには、UPnP™コンポーネントがコンピュータにインストールされている必要があります。



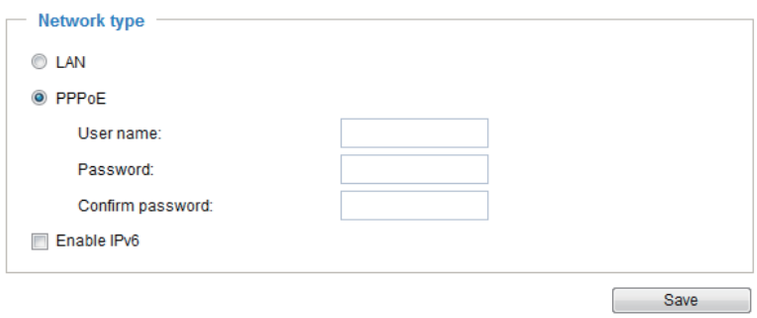
Enable UPnP port forwarding: このオプションを選択すると、インターネットからアクセスしたネットワークカメラが自動的にルータのポートを開いて、LANからビデオストリームを送信することができます。この機能を利用するには、ルータがUPnP™をサポートしており、有効になっている必要があります。

PPPoE (Point-to-point over Ethernet)

このオプションを選択すると、インターネットに接続されていればどこからでもアクセスできるようにネットワークカメラを構成することができます。この機能を利用するには、ISPから提供されたアカウントが必要です。

次の手順でネットワークカメラのパブリックIPアドレスを取得します。

1. LANにネットワークカメラを設定します。
2. [Configuration]>[Event]>[Event settings]>[Add server] (P125[Add server]を参照してください)の順に選択して、新しいメールサーバまたはFTPサーバを追加します。
3. [Configuration]>[Event]>[Event settings]>[Add media] (P130[Add media]を参照してください)の順に選択します。[System log]を選択すると、ネットワークカメラのパブリックIPアドレスを含むTXTファイル形式のシステムログを電子メールまたはFTPサーバで受信することができます。
4. [Configuration]>[Network]>[General settings]>[Network type]>[PPPoE]を選択し、ISPから提供されたユーザー名とパスワードを入力します。[Save]をクリックして設定を有効にします。



5. ネットワークカメラを再起動します。
6. ネットワークカメラの電源を切るときは、LAN環境からカメラを取り除いてください。

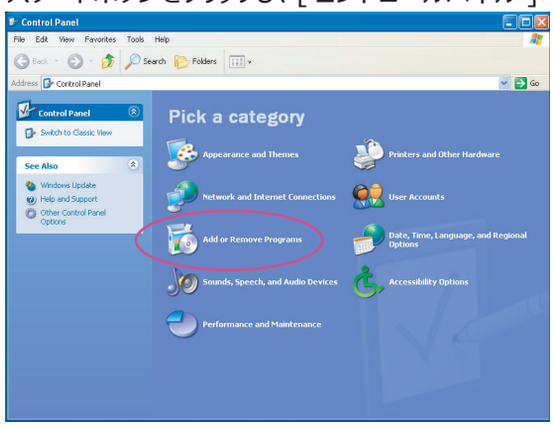
ノート:

► 同じルータに接続されている他のデバイスがすでにデフォルトポートを使用している場合、ネットワークカメラには他のポートを選択します。

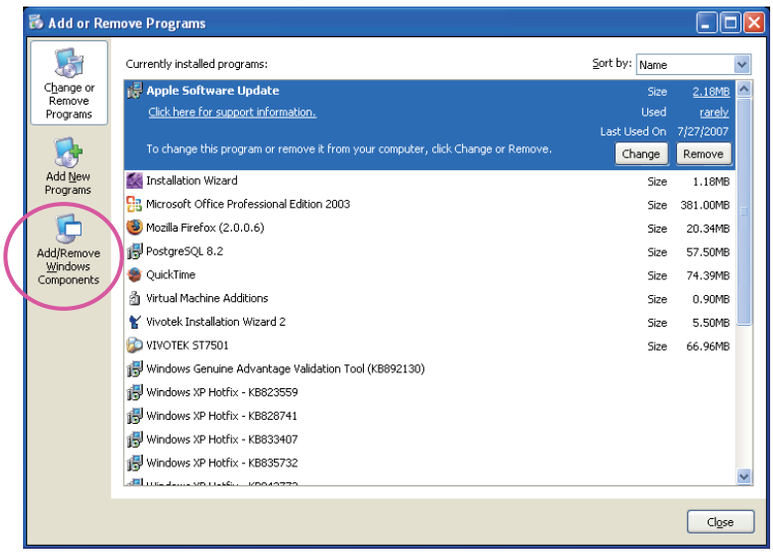
► UPnP ™がサポートされていないルータの場合は、次のメッセージが表示されます。
Error: Router does not support UPnP port forwarding.

► 次の手順でコンピュータから UPnP ™ユーザーインターフェイスを有効にします。
※ UPnP ™コンポーネントをインストールするには、システム管理者としてコンピュータにログオンする必要があります。

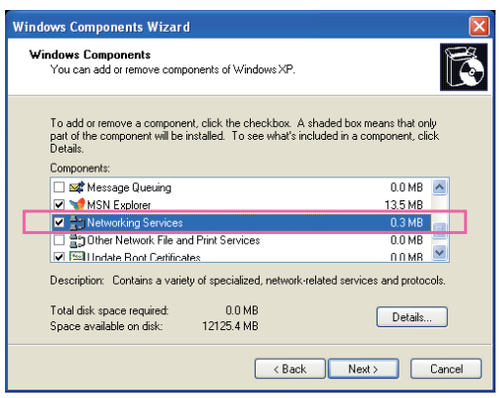
1. スタートボタンをクリックし、[コントロールパネル]>[プログラムの追加と削除] の順に進みます。



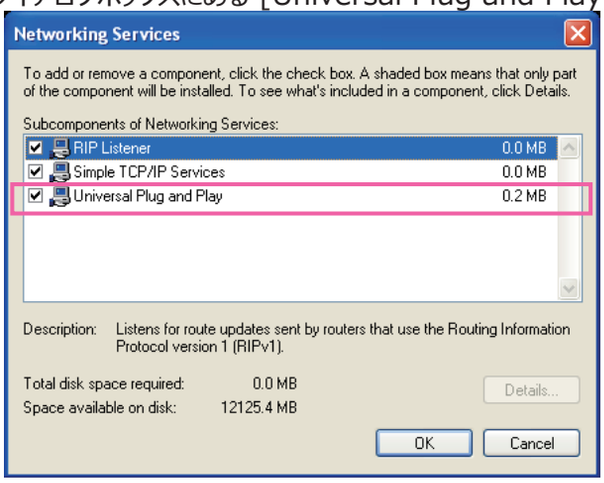
2. ダイアログボックスにある [Windows コンポーネントの追加と削除] をクリックします。



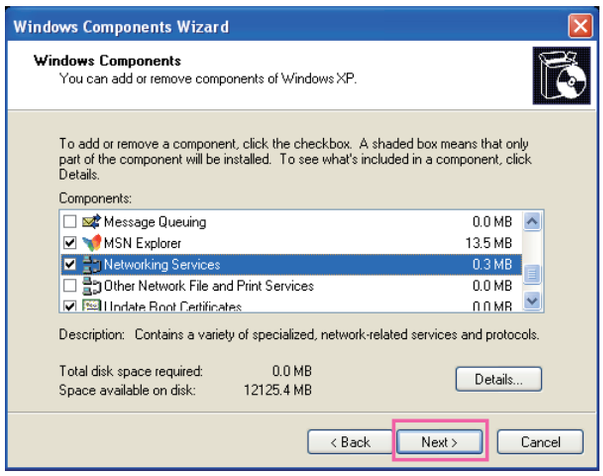
3. [Windows コンポーネントウィザード] ダイアログボックスで [Netowork Services] を選択し、[詳細] をクリックします。



4. ダイアログボックスにある [Universal Plug and Play]を選択し、[OK]をクリックします。



5. 下図のウインドウが表示されますので、[Next]をクリックします。



6. [Finish]をクリックしてUPnP™を有効にします。

► UPnP ™の機能とは？

UPnP ™ネットワークテクノロジーは、ネットワークに追加されたデバイスを検出して相互認識し、自動的に IP を設定することができます。印刷やファイル共有など、ネットワーク接続されたデバイスの機能を、煩雑なネットワーク設定を行う必要なく相互に利用することができます。ネットワークカメラの場合は、[My Network Places] の下にショートカットが表示されます。

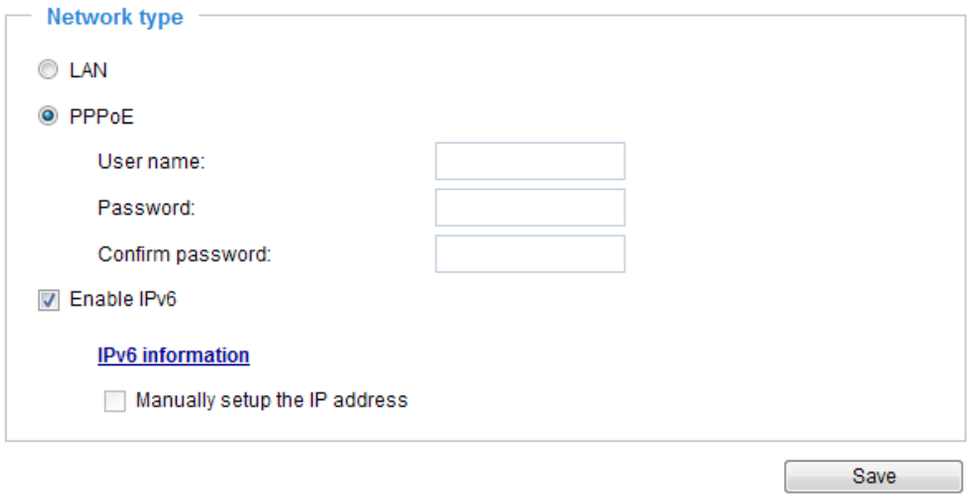
► UPnP ポート転送を有効にすると、ネットワークカメラは HTTP ポートではなく、ルータ上のセカンダリ HTTP ポートを開くことができます。したがって、インターネットからネットワークカメラにアクセスするにはネットワークカメラのパブリックアドレスにセカンダリ HTTP ポート番号を追加する必要があります。たとえば、HTTP ポートが 80 に設定され、セカンダリ HTTP ポートが 8080 に設定されている場合、ネットワークカメラの IP アドレスは次のリストを参照してください。

インターネットLAN	LAN
http://203.67.124.123:8080	http://192.168.4.160 or http://192.168.4.160:8080

► PPPoE 設定が正しく設定されていない場合、またはインターネットアクセスが機能していない場合は、ネットワークカメラを出荷時の設定に初期化します。詳細については、P57[Restore] を参照してください。ネットワークカメラを初期化すると、LAN からアクセスできるようになります。

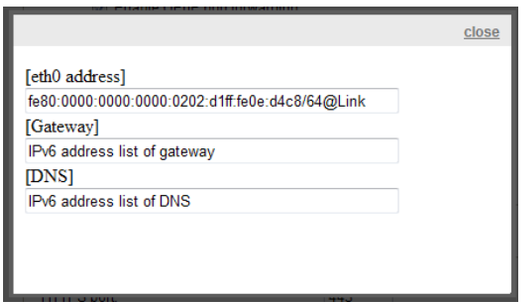
Enable IPv6

このオプションを選択して[Save] をクリックすると、IPv6設定を有効にすることができます。この機能はネットワーク環境およびハードウェア機器がIPv6に対応している場合にのみ動作します。対応ブラウザはMicrosoft® Internet Explorer 6.5、Mozilla Firefox 3.0以上です。

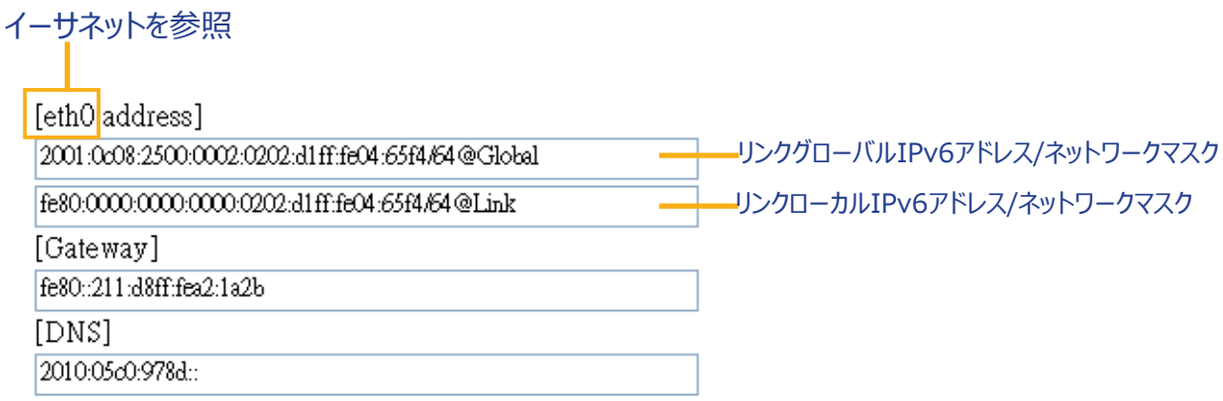


IPv6が有効な場合、デフォルトではネットワークカメラはルーターからのアドバタイジングを受信し、それに応じてリンクローカルIPv6アドレスを割り当てられます。

IPv6 Information: このボタンをクリックすると、次に示すIPv6情報が取得されます。



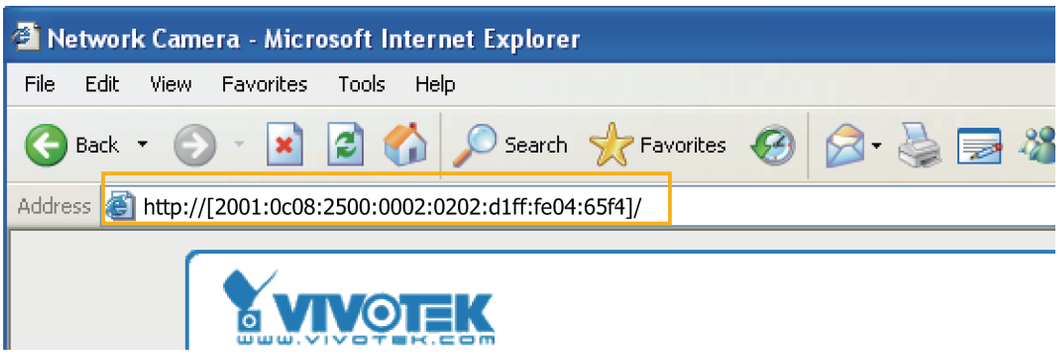
IPv6の設定が完了すると、IPv6アドレスの一覧がポップアップウインドウに表示され、それぞれのIPv6アドレスは次のように表示されます。



次の手順でIPv6アドレスにリンクします。
1. Webブラウザを開きます。
2. Webブラウザのアドレスバーに、リンクグローバルまたはリンクローカルIPv6アドレスを入力します。
3. フォーマットは下記のとおりです。



4. キーボードのEnterキーを押すか、[更新] ボタンをクリックしてWebページを更新します。

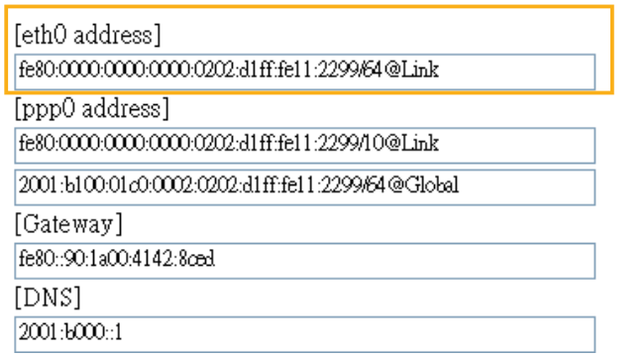


ノート:

► セカンダリ HTTP ポート (デフォルト値：8080) がある場合は、下記のアドレス形式を使用して Web ページにリンクすることもできます。詳しくは P87[HTTP streaming] を参照してください。



► ネットワークタイプとして PPPoE を選択すると、下図のように IPv6 情報欄に [PPP0 アドレス] が表示されます。



Manually setup the IP address: このオプションを選択すると、ネットワーク環境にDHCPv6サーバおよびアドバタイジングが有効なルーターがない場合にIPv6設定を手動でセットアップすることができます。

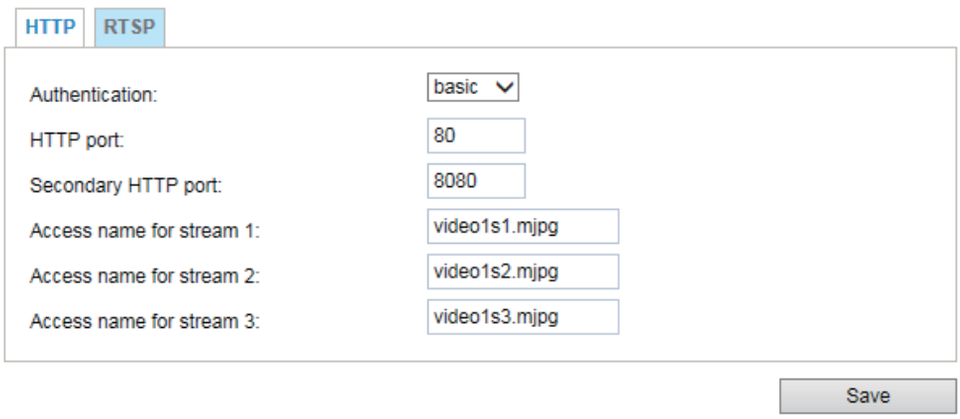
この項目にチェックを入れ、表示される欄に対応する情報を入力します。


Enable IPv6
IPv6 information
Manually setup the IP address
Optional IP address / Prefix length
/ 64
Optional default router
Optional primary DNS

Network > Streaming protocols

HTTP streaming

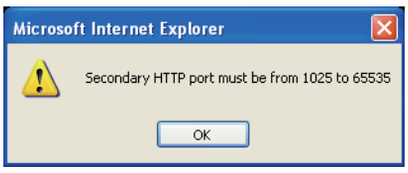
HTTP認証を利用するには、最初にネットワークカメラのパスワードを設定していることを確認してください。詳しくは P97[Security]>[User account]を参照してください。



Authentication: ネットワークカメラにはネットワークのセキュリティ要件に応じたHTTPトランザクションのセキュリティ設定が2種類用意されています。ベーシック認証を選択すると、パスワードはテキスト形式で送信され、傍受される可能性があります。ダイジェスト認証が選択されている場合、ユーザー資格情報はMD 5アルゴリズムを使用して暗号化されるため、不正アクセスに対する保護が強化されます。

HTTP port / Secondary HTTP port: お買い上げ時には、HTTPポートは80、セカンダリHTTPポートは8080に設定されています。これらのポートは1025から65535までのお好みのポート番号に割り当てることもできます。ポートが正しく割り当てられていない場合は、下図のエラーメッセージが表示されます。





HTTPポートとセカンダリHTTPポートの両方を使用してLAN上のネットワークカメラにアクセスすることができます。たとえば、HTTPポートが80に設定され、セカンダリHTTPポートが8080に設定されている場合、ネットワークカメラのIPアドレスは次のリストを参照してください。

LAN
http://192.168.4.160 or http://192.168.4.160:8080

Access name for stream 1 ~ 3: このネットワークカメラは、複数のストリームを同時にサポートすることができます。アクセス名は異なるビデオストリームを識別するために使用します。
[Media]>[Video]>[Stream settings]の順にクリックして、リンクされたストリームの映像品質を設定することができます。映像画質の設定方法について詳しくはP70 [Stream settings]を参照してください。

ビデオモードをJPEGに設定した状態でMozilla Firefoxでネットワークカメラにアクセスすると、連続JPEG画像で構成される映像を受信することができます。この技術は"サーバープッシュ"として知られており、ネットワークカメラはMozilla Firefoxにライブ画像を送ることができます。

URL command -- http://<ip address>:<http port>/<access name for stream 1, 2, 3>
たとえば、ストリーム2のアクセス名がvideo2.mjpgに設定されている場合、次の手順を行います。
1. Mozilla Firefoxを開きます。
2. アドレスバーに上記のURLコマンドを入力し[Enter]を押します。
3. JPEG画像がWebブラウザに表示されます。

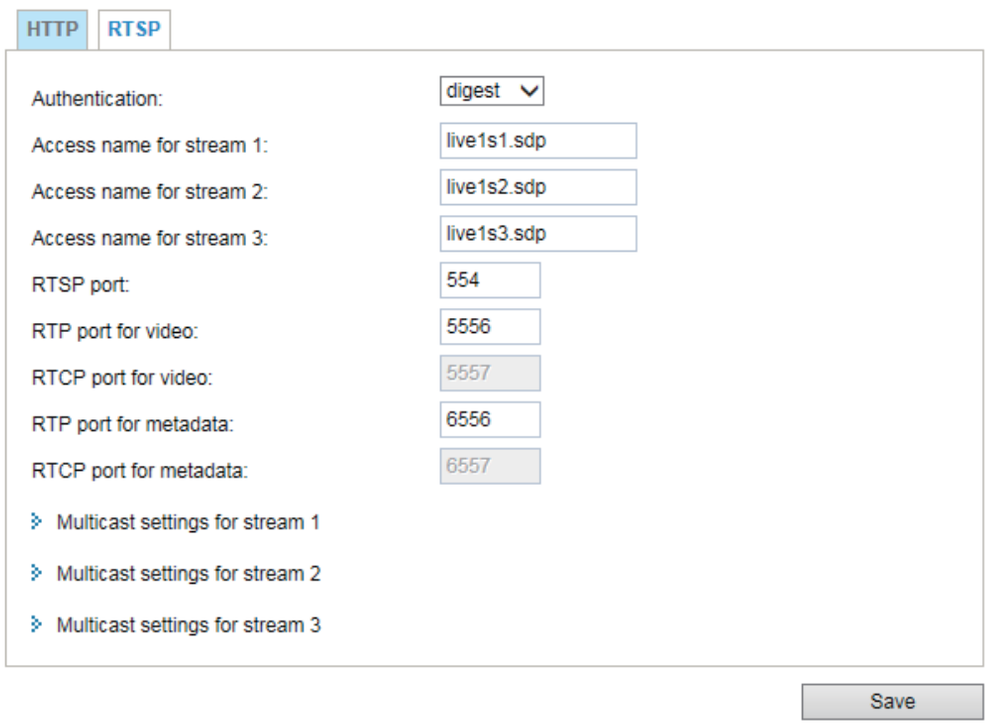


NOTE:

► Microsoft® Internet Explorer はサーバープッシュ技術に対応していないため、http://<ip address>:<http port>/<access name for stream 1, 2, 3> でビデオストリームにアクセスできません。

RTSP Streaming

RTSPストリーミング認証を利用するには、まずビデオストリームへのアクセスを制御するためのパスワードを設定してください。詳しくはP98[Security]>[User account]を参照してください。



Authentication: ネットワークカメラにはネットワークのセキュリティ要件に応じたRSTPプロトコル経由のストリーミング用にセキュリティ設定が3種類用意されています。無効の場合、セキュリティの設定はありません。ベーシック認証を選択すると、パスワードはテキスト形式で送信され、傍受される可能性があります。ダイジェスト認証が選択されている場合、ユーザー資格情報はMD5アルゴリズムを使用して暗号化され、不正アクセスに対する保護が強化されます。それぞれの認証モードで使用できるRTSPストリーミングプレーヤーについては下表をご確認ください。

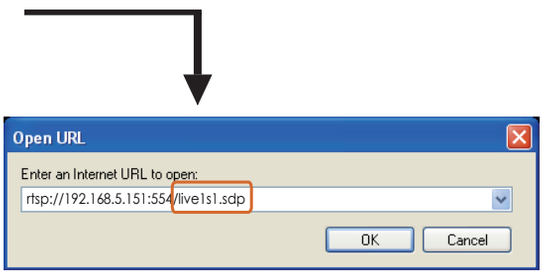
	Quick Time player	VLC
Disable	O	O
Basic	O	O
Digest	O	X

Access name for stream 1 ~ 3: このネットワークカメラは、複数のストリームを同時にサポートすることができます。アクセス名はストリーミングソースを識別するために使用します。RTSPプレーヤーを使用してネットワークカメラにアクセスする場合は、ビデオモードをH.264またはH.265に設定し、次のRTSPURLコマンドを使用してストリーミングデータの送信を要求する必要があります。URLコマンド：rtsp://<ip address>:<rtsp port>/<access name for stream 1 to 3>

たとえば、ストリーム1のアクセス名がlive.sdpに設定されている場合、次の手順を行います。

1. RSTPプレーヤーを起動します。
2. [ファイル]>[URLを開く]を選択します。URLダイアログボックスが表示されます。
3. テキストボックスに上記のURLコマンドを入力します。
4. ライブビデオが下図のようにプレーヤーに表示されます。



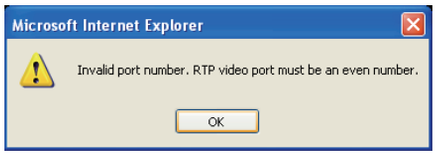


RTSP port /RTP port for video, audio/ RTCP port for video, audio

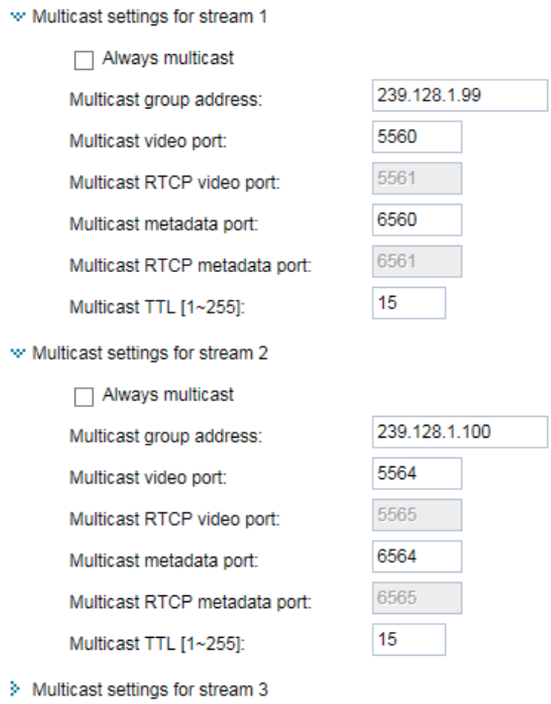
- RTSP(リアルタイムストリーミングプロトコル)はストリーミングメディアの配信を制御します。お買い上げ時ポート番号は554に設定されています。
- RTP(リアルタイム転送プロトコル)はビデオおよびオーディオデータをクライアントに配信するために使用します。お買い上げ時ポートは5556に設定されています。
- RTCP(リアルタイムトランスポート制御プロトコル)を使用すると、ネットワークのトラフィック量をモニターしながらデータを送信することができます。お買い上げ時ポートは5557に設定されています。

ポートは 1025 から 65535 の間のお好みの値に変更することができます。RTP ポートは偶数である必要があり、RTCP ポートは RTP ポート番号に 1 を加えた数になるので、常に奇数となります。RTP ポートが変更されると、それに応じて RTCP ポートも変更されます。

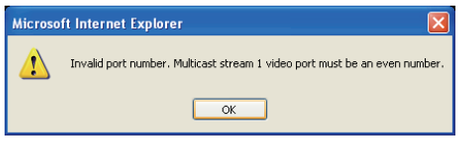
RTP ポートが正しく割り当てられていない場合は、下図のエラーメッセージが表示されます。



Multicast settings for streams: 項目をクリックすると、詳細設定が表示されます。
ビデオストリームのマルチキャストを有効にするには[Always multicast]を選択します。



ユニキャストビデオ伝送では、ポイントツーポイント伝送によってストリームを配信します。一方、マルチキャスト伝送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、そこからのコピーを要求することで、複数のクライアントが同時にストリームを取得できるようにします。よってマルチキャストを有効にすると、インターネットの帯域幅を効果的に節約することができます。
ポートは1025から65535の間のお好みの値に変更することができます。マルチキャストRTPポートは偶数である必要があり、マルチキャストRTCPポートはマルチキャストRTPポート番号に1を加えた数になるので、常に奇数となります。マルチキャストRTPポートが変更されると、それに応じてマルチキャストRTCPポートも変更されます。
RTPポートが正しく割り当てられていない場合は、下図のエラーメッセージが表示されます。



Multicast TTL [1~255]: マルチキャストTTL (生存期間)は、パケットの有効時間で、ルータを通過できる回数です。

Initial TTL	Scope
0	Restricted to the same host
1	Restricted to the same subnetwork
32	Restricted to the same site
64	Restricted to the same region
128	Restricted to the same continent
255	Unrestricted in scope

注意:

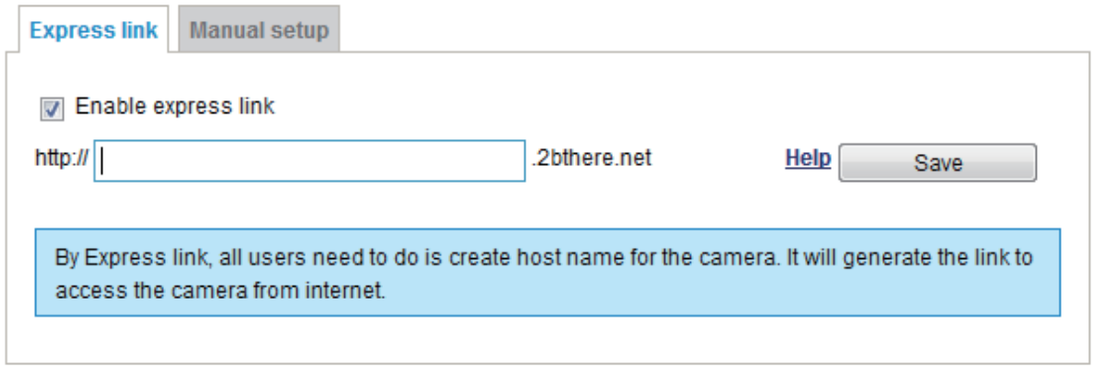
マルチキャストメタデータポートは、VIVOTEK VADPモジュールがビデオ分析結果、PTZストリーム、テキストデータ、イベントメッセージをビデオ分析を行うカメラとクライアント側との間で転送するために利用しています。クライアント側のコンピュータがローカルネットワークの外部にある場合は、ルーターとファイアウォールが関連するTCPポートを開く必要があります。

Network > DDNS

この項目では、ネットワークカメラの動的ドメインネームサービスを設定する方法について説明します。DDNSは、特に動的IPアドレスが割り当てられている場合に、ネットワークカメラが固定のホスト名とドメイン名を持つことを可能にするサービスです。

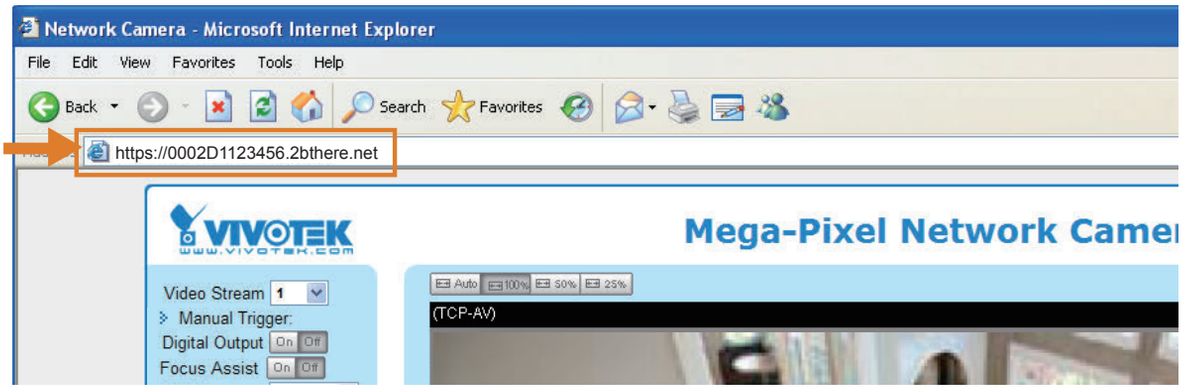
Express link

Express LinkはVIVOTEKサーバが提供する無料のサービスで、ユーザーはネットワークデバイスのドメイン名を登録することができます。1つのURLは1つのMACアドレスにしか関連付けすることができません。このサービスは、ホスト名が有効かどうかを調べ、ルーターのポートを自動的に開くことができます。DDNSを使用する場合は、UPnPポート転送を手動で設定する必要がありますが、Express Linkを使うほうが便利で設定も簡単です。



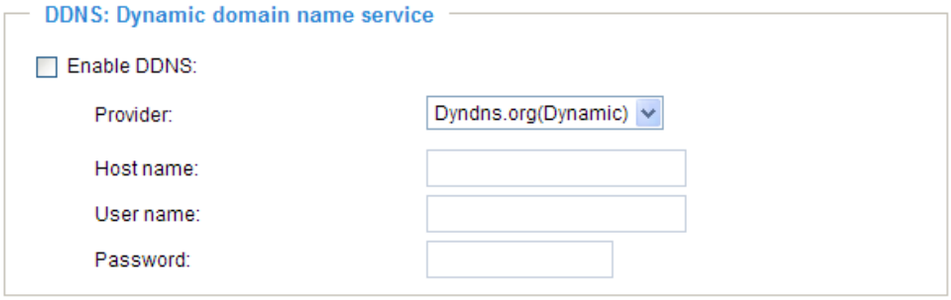
次の手順でExpress Linkを有効にします。
1. ルーターがUPnPポート転送対応であることと、機能が有効になっていることを確認してください。
2. [Enable express link]にチェックを入れます。
3. ネットワークデバイスのホスト名を入力し[Save]をクリックします。ホスト名が別のデバイスで使用されている場合はエラーメッセージが表示されます。ホスト名が有効な場合は下図のメッセージが表示されます。





Manual setup

DDNS: Dynamic domain name service



Enable DDNS: このオプションを選択すると、DDNS設定を有効にすることができます。

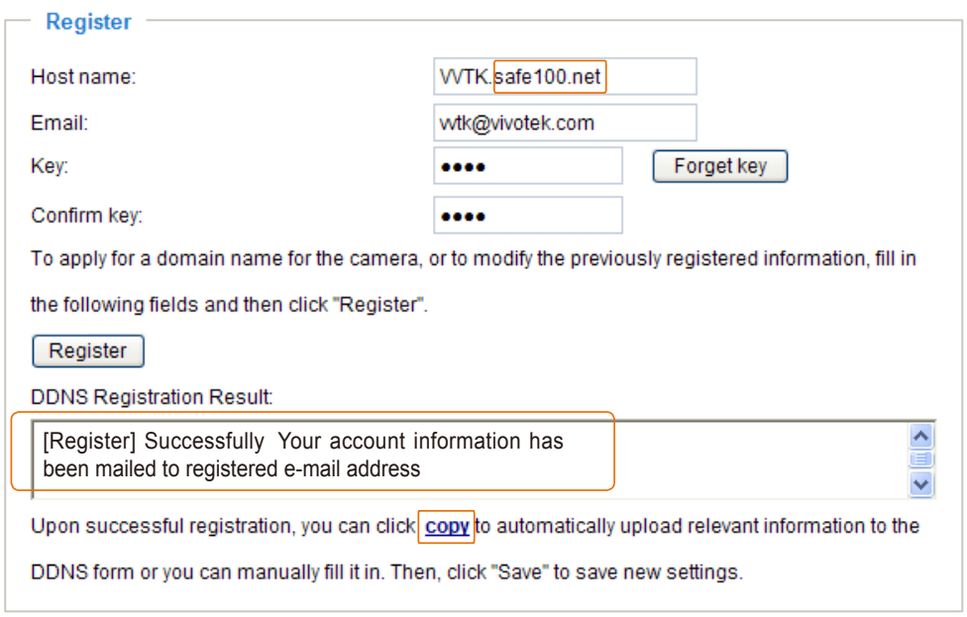
Provider: ドロップダウンリストからDDNSプロバイダを選択します。

DDNS機能を利用する前に、動的ドメインアカウントを申請してください。VIVOTEKは、無料の動的ドメインネームサービスSafe100.netを提供しています。まずはSafe100.netに登録してVIVOTEKのネットワークカメラにアクセスすることをおすすめしています。また、Dyndns.org(Dynamic), Dyndns.org(Custom)など他のDDNSプロバイダも提供しています。

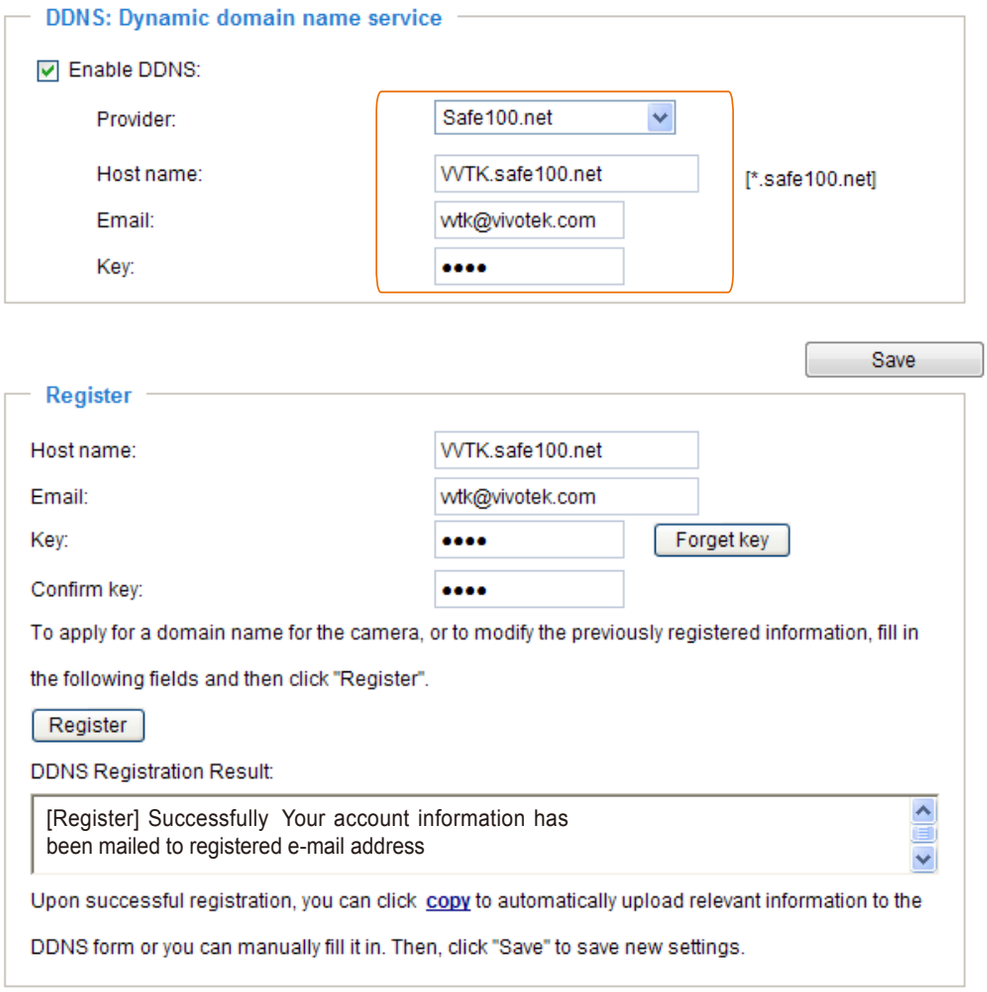
■ Safe100.net

1. [DDNS]列のドロップダウンリストから[Safe100.net]を選択します。サービス契約の条項を確認してから、[I accept](同意します) をクリックします。

2. [Register]列に[Host name(xxxx.safe100.net)]、[Email]、[Key]、[Confirm Key]を入力し、[Register]をクリックします。ホスト名が正常に作成されると、[DDNS Registration Result]列にメッセージが表示されます。



3. [Copy]をクリックすると、登録されているすべての情報が上部の[DDNS]列の対応するフィールドに自動的にアップロードされます。



4. [Enable DDNS]を選択し、[Save]をクリックして設定を有効にします。

■ CustomSafe100

VIVOTEKは、代理店やシステム・インテグレータ向けにCustomSafe100 DDNSサーバを構築するためのドキュメントを提供しています。代理店やシステム・インテグレータがそのようなサービスを提供している場合、CustomSafe100を使用してダイナミック・ドメイン名を登録することができます。

1. [DDNS」欄で、ドロップダウンリストから「CustomSafe100」を選択します。
2. 登録」の欄に、「ホスト名」、「電子メール」、「キー」、「キーの確認」を入力し、「登録」をクリックします。ホスト名が正常に作成されると、「DDNS登録結果」欄に成功メッセージが表示されます。
3. [コピー] をクリックすると、登録されたすべての情報が [DDNS] 列の対応するフィールドにアップロードされます。
4. DDNSの有効化」を選択し、「保存」をクリックすると設定が有効になります。

Forget key: Safe100.netまたはCustomSafe100のキーを忘れた場合は、このボタンをクリックしてください。お客様のアカウント情報がお客様のメールアドレスに送信されます。

その他のDDNSプロバイダを選択して動的ドメインアカウントを適用するには、下記リンクを参照してください。
DDNSプロバイダ：

■ Dyndns.org(Dynamic) / Dyndns.org(Custom): visit http://www.dyndns.com/

Network > QoS (Quality of Service)

Quality of Serviceとは、ネットワーク上のさまざまなサービスに対して一定の品質を保証するリソース予約制御メカニズムのことです。特にリアルタイムストリーミングマルチメディアアプリケーションでは、ネットワーク容量が不十分な場合にQuality of Serviceは重要です。ここでは、保証する品質としてビットレートを維持するレベル、レイテンシの短さ、パケット廃棄防止などを定義しています。

QoS対応ネットワークの主な利点：
- トラフィックに優先順位を付け、データフローに対して一定レベルのパフォーマンスを保証
- 各アプリケーションが使用できる帯域幅の量を制御し、ネットワークの信頼性と安定性を向上

Requirements for QoS

ネットワーク環境でQoSを利用するには、次の要件を満たす必要があります。
- ネットワーク内のすべてのネットワークスイッチとルーターがQoS対応である
- ネットワークで使用するネットワークビデオデバイスはQoS対応である

QoS models

CoS (the VLAN 802.1p model)

IEEE 802.1pはOSIレイヤ2(データリンクレイヤ)でQoSモデルを定義します。これはCoS、Class of Serviceと呼ばれます。VLAN MACヘッダには3ビットの値が追加され、フレームプライオリティレベルは0 (最低)から7(最高)に設定されます。優先順位はネットワークスイッチで設定され、ネットワークスイッチはパケットを転送するために異なるキューイング規則を使用します。下図はCoSの設定列になります。スイッチのVLAN ID(0~4095)を入力し、各アプリケーションの優先順位(0~7)を選択します。



[Video]に最高レベルを割り当てると、スイッチは最初にビデオパケットを処理します。

ノート:

► VLAN スイッチ (802.1p) が必要です。CoS 設定が正しくないと、Web ブラウズが失敗する場合があります。

► Class of Service は帯域幅と配信時間の点ではサービスレベルが保証されません。CoS はおおまかなトラフィック制御、QoS はきめの細かいトラフィック制御と考えることができます。

► CoS は管理が簡単ですが、拡張性は高くありません。また L2 プロトコルベースで、エンドツーエンドの保証は適用できません。

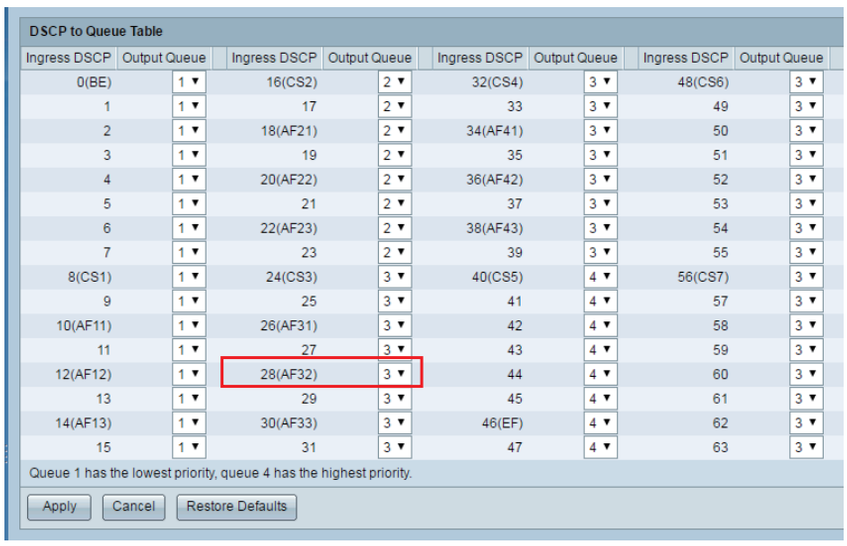
QoS/DSCP (the DiffServ model)

DSCP-ECNは、レイヤ3 (ネットワークレイヤ)でQoSを定義します。これはDifferentiated Services(Diff-Serv)モデルと呼ばれ、パケットマーキングとルータのキューイング規則に基づいてQoSを行います。マーキングはDSCP(差別化サービスコードポイント)と呼ばれる64個の異なるクラスIDを提供する6ビットのフィールドをIPヘッダに追加することによって行われます。特定のパケットの転送方法はPer Hop Behavior(PHB) と呼ばれ、帯域幅、キューイング理論、パケットの破棄の決定に関して、特定のサービスレベルを記述します。各ネットワークノードのルータは、DSCP値に従ってパケットを分類し、たとえば、予約帯域幅の量などに特定の転送処理を行います。

下図はDSCP (DiffServコードポイント)の設定オプションです。各アプリケーションのDSCP値(0~63)を指定することができます。



下図はCisco社製スイッチを使用した場合の対応例となります。ネットワークデバイスベンダーによって設定や実装の方法が異なる場合があります。ネットワークデバイスからの情報に従ってDSCPタグ値を入力してください。



DSCP to Queue Table

Ingress DSCP	Output Queue	Ingress DSCP	Output Queue	Ingress DSCP	Output Queue	Ingress DSCP	Output Queue
0(BE)	1	16(CS2)	2	32(CS4)	3	48(CS6)	3
1	1	17	2	33	3	49	3
2	1	18(AF21)	2	34(AF41)	3	50	3
3	1	19	2	35	3	51	3
4	1	20(AF22)	2	36(AF42)	3	52	3
5	1	21	2	37	3	53	3
6	1	22(AF23)	2	38(AF43)	3	54	3
7	1	23	2	39	3	55	3
8(CS1)	1	24(CS3)	3	40(CS5)	4	56(CS7)	3
9	1	25	3	41	4	57	3
10(AF11)	1	26(AF31)	3	42	4	58	3
11	1	27	3	43	4	59	3
12(AF12)	1	28(AF32)	3	44	4	60	3
13	1	29	3	45	4	61	3
14(AF13)	1	30(AF33)	3	46(EF)	4	62	3
15	1	31	3	47	4	63	3

Queue 1 has the lowest priority, queue 4 has the highest priority.

Apply Cancel Restore Defaults



QoS Baseline/Technical Marketing Classification and Marking Recommendations					
Application	Layer3 Classification			Layer 2 CoS/MPLS EXP	
	IPP	PHB	DSCP		
IP Routing	6	CS6	48	6	
Voice	5	EF	46	5	
Interactive Video	4	AF41	34	4	QoS B
Streaming-Video	4	CS4	32	4	
Locally-defined Mission-Critical Data	3	-	25	3	
Call-signaling	3	AF31/CS3	26/24	3	
Transactional Data	2	AF21	18	2	
Network Management	2	CS2	16	2	
Bulk Data	1	AF11	10	1	

Network > SNMP (Simple Network Management Protocol)

この項目では、ネットワークカメラでSNMPを使用する方法を説明します。SNMP(簡易ネットワーク管理プロトコル)は、ネットワークデバイス間の管理情報の交換を容易にするアプリケーション層プロトコルです。これにより、ネットワーク管理者はネットワークデバイスをリモートで管理し問題を簡単に見つけて解決することができます。

■ SNMPは、次の3つの主要コンポーネントで構成されています。
1. SNMPマネージャ：ネットワーク管理ステーション (NMS) 。管理対象デバイスを監視および制御するアプリケーションを実行するサーバーです。
2. SNMPエージェント：管理対象デバイスのステータスをNMSに転送するデバイス上のネットワーク管理ソフトウェアモジュール。
3. 管理対象デバイス：ネットワーク上のネットワークノード。例：ルーター、スイッチ、ブリッジ、ハブ、コンピュータホスト、プリンタ、IP電話、ネットワークカメラ、Webサーバー、データベースなど。

SNMP設定を構成する前に、必ずNMSを有効にしてください。

SNMP Configuration

Enable SNMPv1, SNMPv2c
このオプションを選択し、NMSの設定に従って[Read/Write community]と[Read Only community]の名前を入力します。



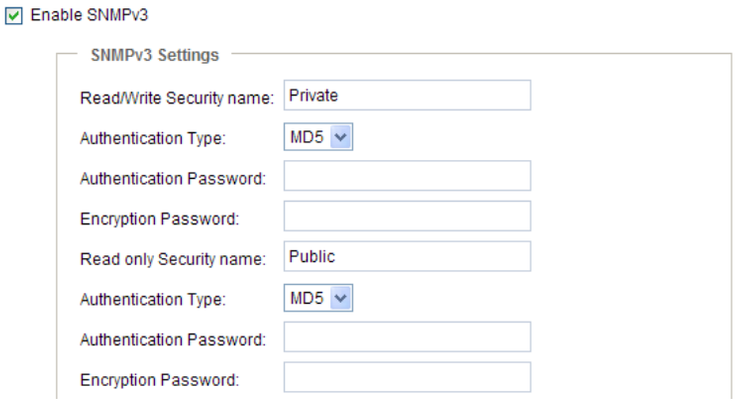
Enable SNMPv3
このオプションを選択すると、より高いセキュリティレベルである暗号化セキュリティが含まれた認証パスワードと暗号化パスワードを設定することができます。

■ Security name: NMSの設定に従って[Read/Write]または[Read Only]のどちらかを選択し、コミュニティ名を入力します。

■ Authentication type: 認証方法として[MD5]または[SHA]のどちらかを選択します。

■ Authentication password: 認証用のパスワードを入力します(最低8文字以上)。

■ Encryption password: 暗号化用のパスワードを入力します(最低8文字以上)。



Network > FTP

このカメラでは、セキュリティ上の理由から工場出荷時は FTP ポートが無効になっています。FTP サーバーサービスを手動で有効にして、FTP 機能を有効にすることができます。FTP サーバー機能は使用していないときは無効にすることもできます。

FTP port: FTPサーバーには、録画したビデオクリップを保存することができます。
工場出荷時FTPポートは21に設定されています。1025から65535までの別のポート番号に割り当てることもできます。

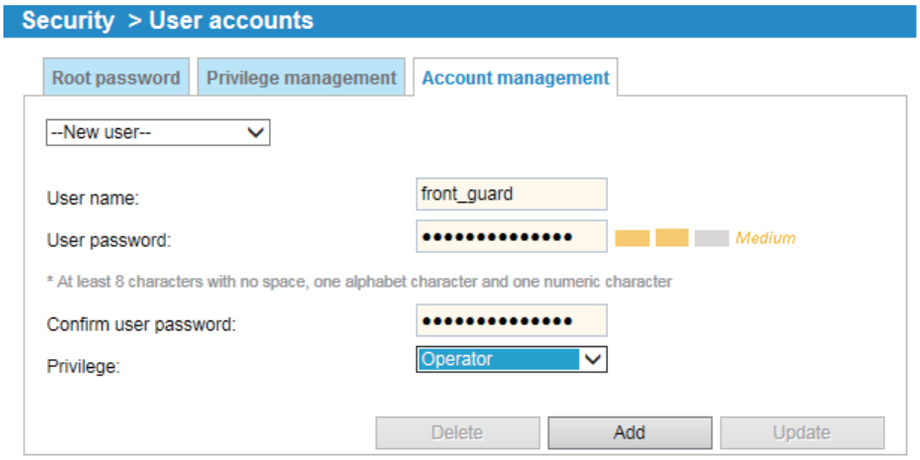
ヒント：

"http://ip/cgi-bin/admin/lsctrl.cgi?cmd=search"というコマンドを使用してSDカードに記録されたファイルを調べることができます。

Security > User accounts

この項目では、パスワード保護を有効にして複数のアカウントを作成する方法について説明します。

Account management



管理者アカウント名は[root]です。これは変更や削除することができません。[Account management]ウインドウでアカウントを追加する場合は、最初に[root]アカウントのパスワードを適用してください。

管理者は最大20個のユーザーアカウントを作成することができます。
新しいユーザーを作成するには次の手順をおこないます。

1. クリックしてプルダウンメニューを展開し、[New user]を選択します。
2. 新しいユーザーの名前とパスワードを入力します。パスワードの安全度の強さが右のゲージに表示されます。パスワードの安全性が十分に強くなるようにアルファベットと数字、大/小文字の組み合わせてください。また、パスワードの設定には、一部の記号 (!, $, %, -, ., @, ^, _, ~)を使用することもできます。[Confirm user password]には設定した同じパスワードを入力してください。
3. 新しいユーザーアカウントの権限レベルを選択し、[Add]をクリックして設定を有効にします。権限レベルは次のとおりです。

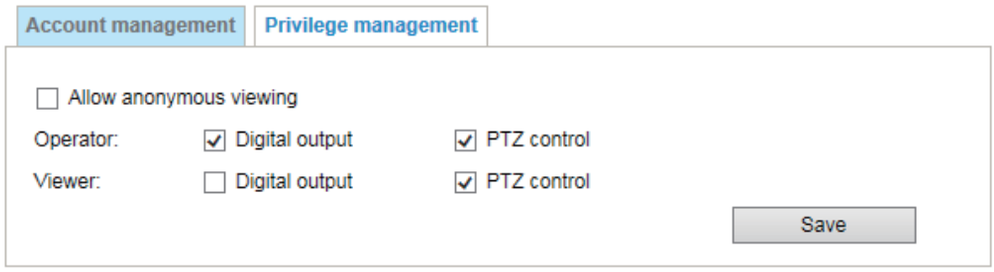
Administrator	すべての権限
Operator	DO 制御、スナップショット、PTZ の操作 ※設定ページにはアクセスできません。
Viewer	DO 制御、スナップショット、画面、音声、PTZ の操作と カメラのインターフェースを介した会話

上記のユーザー権限別にアクセス権は分類されています。カメラの設定ページにアクセスできるのはAdministratorだけです。Operatorは設定ページにアクセスすることはできませんが、URLコマンドを使用してパラメータの値を取得したり設定することができます。Viewerはライブ視聴用のメインページにのみアクセスすることができます。

またユーザーのアクセス権を変更したり、ユーザーアカウントを削除することもできます。

1. 変更する既存のアカウントを選択します。
2. 変更する箇所を入力し直し、[Update]または[Delete]をクリックして設定を有効にします。

Privilege management



Digital Output & PTZ control: 管理権限をオペレーターまたはビューアーとして変更することができます。チェックボックスを選択または選択解除し、［保存］をクリックして設定を有効にします。視聴者に権限を与えた場合、オペレーターもメインページからネットワークカメラを操作することができます。42ページの「設定」を参照）。

Allow anonymous viewing: この項目を選択すると、すべてのクライアントがユーザーIDとパスワードを入力することなくライブストリームにアクセスすることができます。

Security > HTTPS (Hypertext Transfer Protocol over SSL)

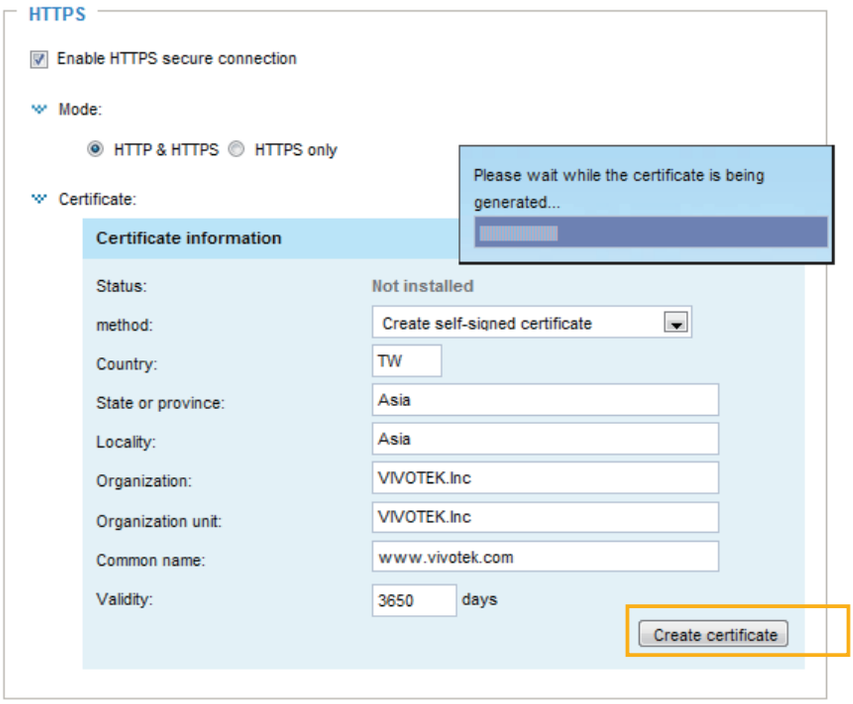
この項目では、SSL(Secure Socket Layer)で認証、暗号化された通信を使用可能にする方法について説明します。これにより、インターネット経由のストリーミングデータ転送をより高いセキュリティレベルで保護できます。

Create and Install Certificate Method

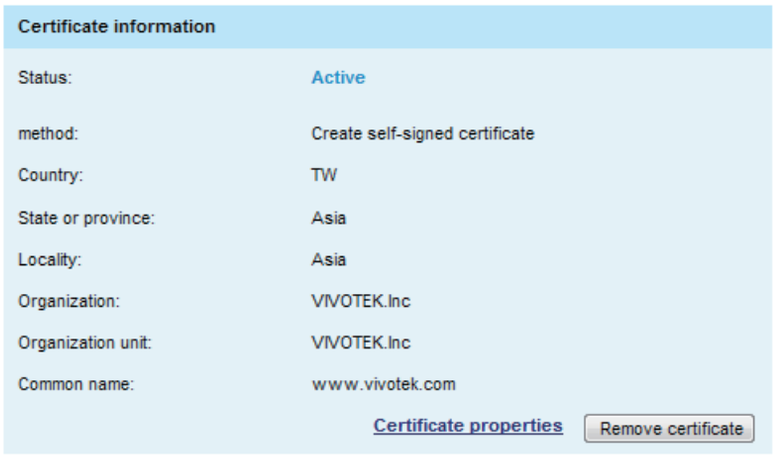
ネットワークカメラとの通信にHTTPSを使用する前に、証明書を作成する必要があります。証明書を作成してインストールするには、次の3つの方法があります。

Create self-signed certificate

1. プルダウンメニューからこのオプションを選択します。
2. [Enable HTTPS secure connection]を選択し、接続オプション[HTTP & HTTPS]または[HTTPS only]を選択します。
3. 証明書を生成するには、[Create certificate]をクリックします。

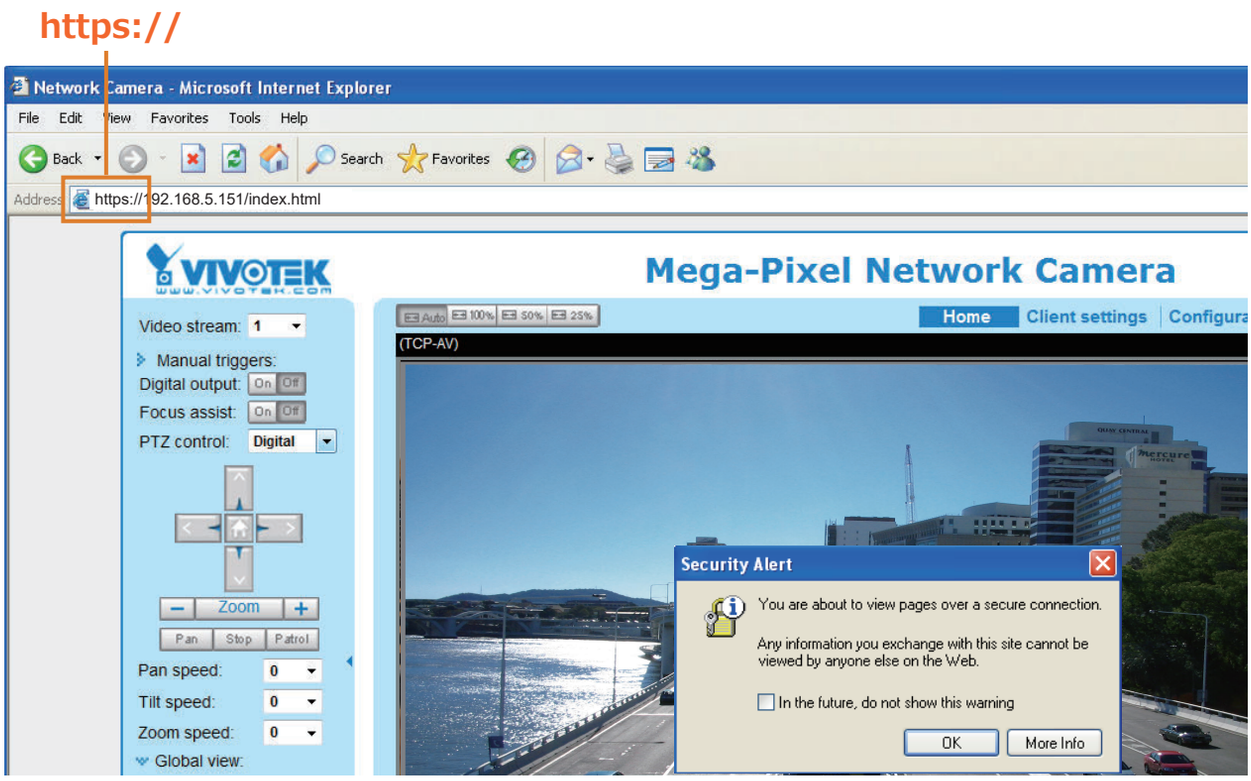


4. 以下のように証明書情報が自動的に表示されます。[Certificate properties] をクリックすると、証明書に関する詳細情報を表示することができます。

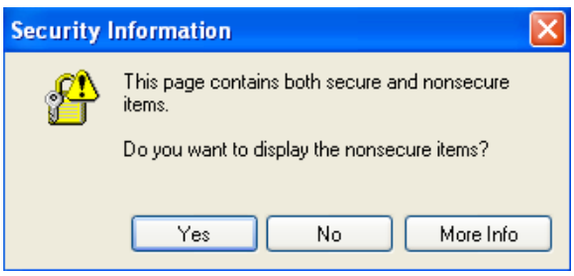


5. [Save]をクリックして設定を保存すると、カメラとの現在のセッションが暗号化された接続に変わります。

6. Webセッションが自動的に暗号化されたHTTPSセッションに変更されない場合は、[Home]をクリックしてメインページに戻り、アドレスバーのURLアドレスを ”http://” から “https://” に変更してキーボードの[Enter]キーを押してください。セキュリティの警告ダイアログが表示されますので、[OK]または[Yes]をクリックして、HTTPSを有効にします。

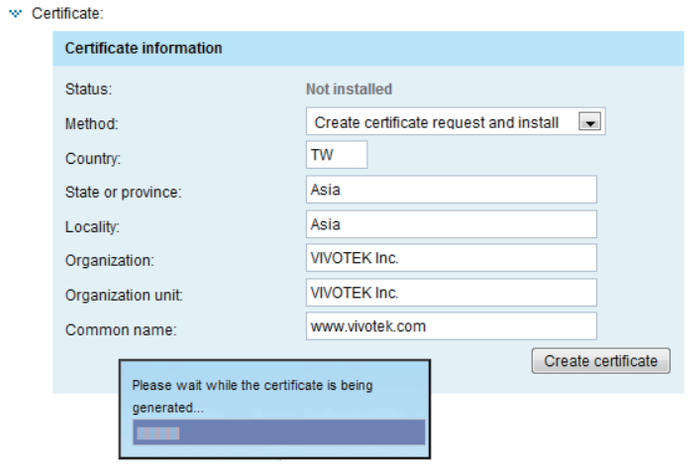




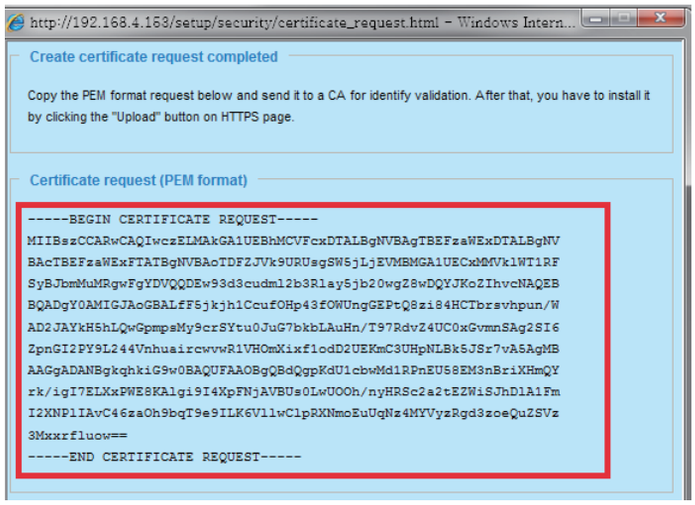


Create certificate request and install

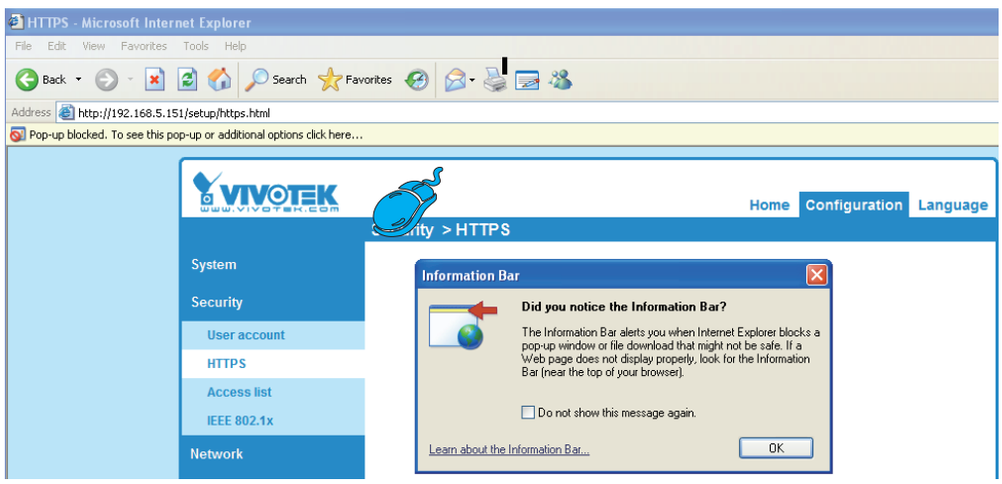
1. [Method]プルダウンメニューからこの項目のオプションを選択します。
2. [Create certificate]をクリックします。
3. [Create]をクリックすると、ポップアップウインドウに下図が表示されます。次に、[Save]をクリックして証明書要求を生成します。



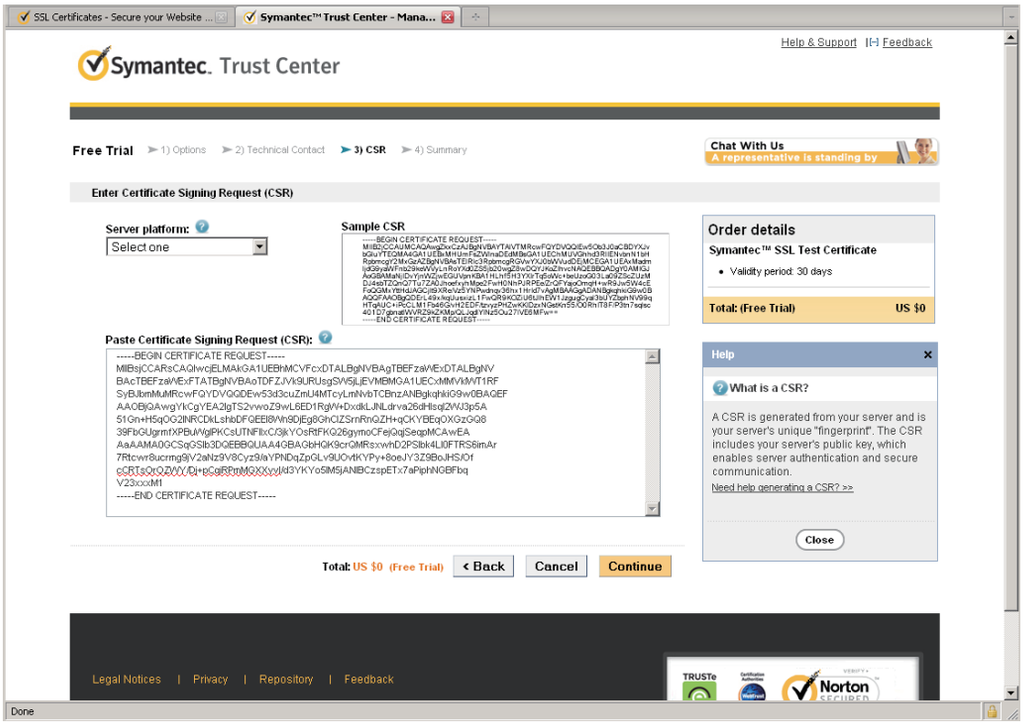
4. [Certificate request]ウインドウが表示されます。



ポップアップウインドウに関する警告メッセージが表示される場合は、メッセージバーをクリックしてポップアップを許可してください。



5. SymantecのVeriSign Authentication Servicesなど、デジタル証明書を発行する信頼できる認証局(CA)にサインインして、SSL証明サービスを購入してください。先ほどのCertificate requestをコピーしてCAの署名要求ウインドウに貼り付けます。続いて記載されている指示に従って、証明書取得の手続きを進めてください。



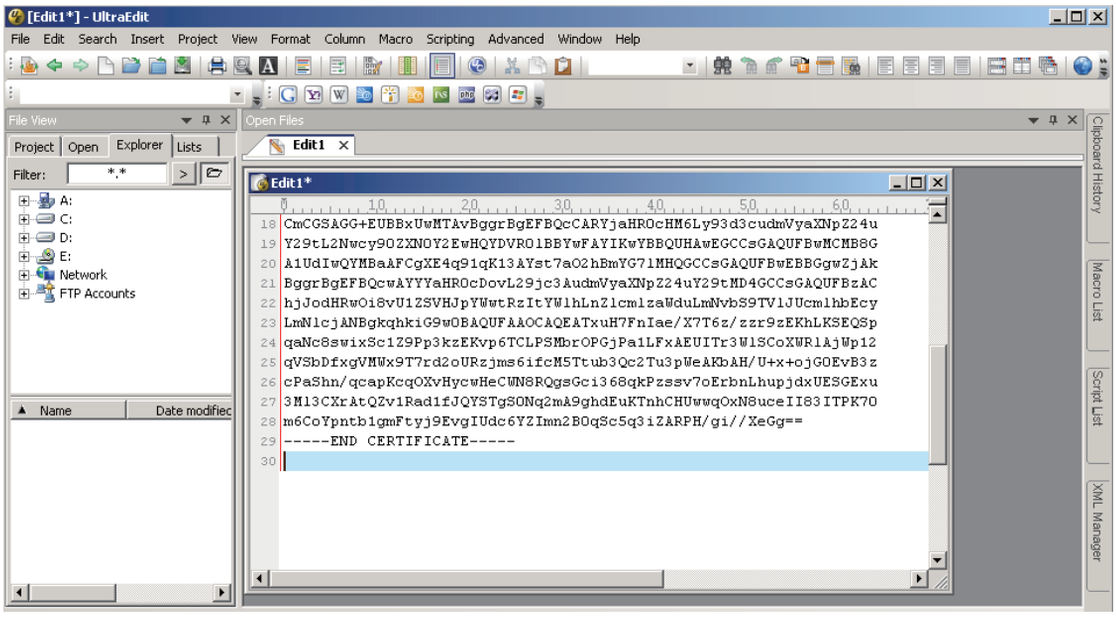
6. 完了したら、SSL証明書が電子メール等で配信されます。証明書の内容をコピーし、IDM Computer SolutionsのUltraEditなどのテキストエディタに貼り付けます。

```
immediately, please dial 866.893.6565 or 650.426.5112 option 3 or send an email to internet-sales@verisign.com

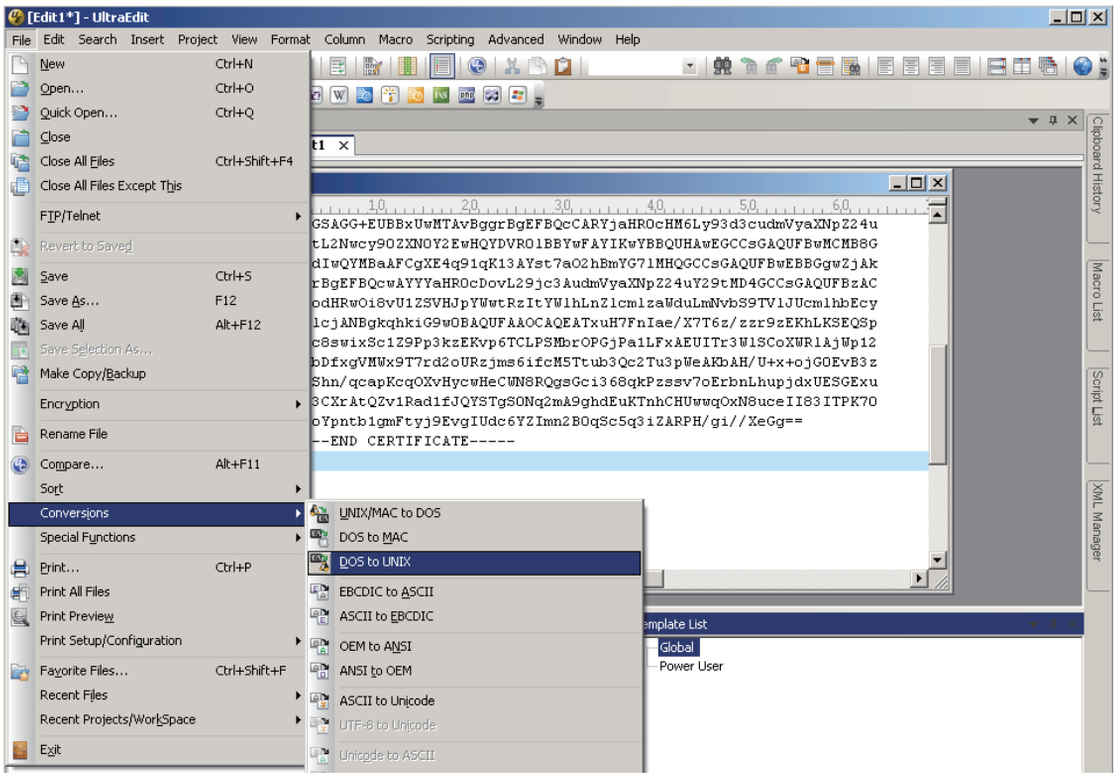
Thank you for your interest in Symantec!

-----BEGIN CERTIFICATE-----
MIIFBDCCA+ygAwIBAgIQFx1Cahn/SeBSit0WQDOBIzANBgkqhkiG9w0BAQUFADCB
yzELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMTAwLgYDVQQL
EydGb3IgVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4xQjBABgNV
BAsTOVRlcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnbi5jb20vY3Bz
L3Rlc3RjYSAoYykwOTEtMCsGA1UEAxMkVmVyaVNpZ24gVHJpYWwgU2VjdXJlIFN1
cnZlciBDQSAtIEcyMB4XDTEyMDcwMzAwMDAwMFoXDTEyMDgwMjIzNTk1OVowga4x
CzAJBgNVBAYTAlRXMQ0wCwYDVQQIEwRBc2lhMQ0wCwYDVQQHFARBc2lhMRUwEwYD
VQQKFAxWSVZPVEVLIEluYy4xFTATBgNVBAsUDFZJVk9URUsgSW5jLjE6MDgGA1UE
CxQxVGVybXMgb2YgdXNlIGF0IHd3dy52ZXJpc2lnbi5jb20vY3BzL3Rlc3RjYSAo
YykwNTEXMBUGA1UEAxQOd3d3LmZlODE3Mi5jb20wgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBANiIE0tr8KGfcC+hA9UYFvg8XZCyTS3a72tunRyLKpdlid6eQOdR
p/h+ajhtpTUQg5C7IWwxUBBCPFp/Q4xIPBoQpWUq50Z0GR/qgimARKjlxskxkPN/R
WxllK5n1zwbloCDygrFEzRSCMQv945GDrEbRSkNuoMpqAhXo0Ko0nqqTAgMBAAGj
ggGBMIIBfTAZBgNVHREEEjAQgg53d3cuZmU4MTcyLmNvbTAJBgNVHRMEAjAAMA4G
A1UdDwEB/wQEAwIFoDBDBgNVHR8EPDA6MDigNqA0hjJodHRwOi8vU1ZSVHJpYWwt
RzItY3JsLnZlcmlzaWduLmNvbS9TV1JUcmlhbEcyLmNybDBKBgNVHSAEQzBBMD8G
CmCGSAGG+EUBBxUwMTAvBggrBgEFBQcCARYjaHR0cHM6Ly93d3cudmVyaXNpZ24u
Y29tL2Nwcy90ZXN0Y2EwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMB8G
A1UdIwQYMBaAFCgXE4q91qK13AYst7aO2hBmYG71MHQGCCsGAQUFBwEBBGgwZjAk
BggrBgEFBQcwAYYYaHR0cDovL29jc3AudmVyaXNpZ24uY29tMD4GCCsGAQUFBzAC
hjJodHRwOi8vU1ZSVHJpYWwtRzItYWlhLnZlcmlzaWduLmNvbS9TV1JUcmlhbEcy
LmNlcjANBgkqhkiG9w0BAQUFAAOCAQEATxuH7FnIae/X7T6z/zzr9zEKhLKSEQSp
qaNc8swixSc1Z9Pp3kzEKvp6TCLPSMbrOPGjPa1LFxAEUITr3WlSCoXWRlAjWp12
qVSbDfxgVMWx9T7rd2oURzjms6ifcM5Ttub3Qc2Tu3pWeAKbAH/U+x+ojG0EvB3z
cPaShn/qcapKcqOXvHycwHeCWN8RQgsGci368qkPzssv7oErbnLhupjdxUESGExu
3Ml3CXrAtQZv1Rad1fJQYSTgS0Nq2mA9ghdEuKTnhCHUwwqOxN8uceII83ITPK70
m6CoYpntb1gmFtyj9EvgIUdc6YZImn2B0qSc5q3iZARPH/gi//XeGg==
-----END CERTIFICATE-----
```

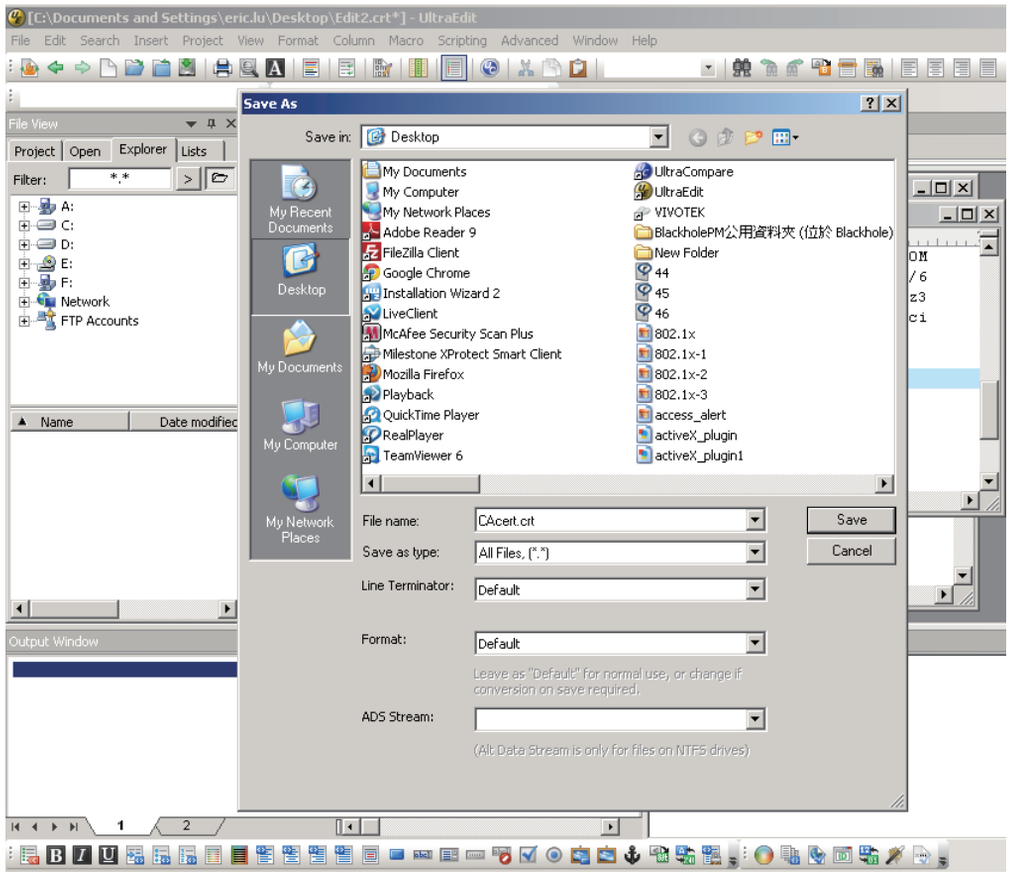
7. 新しい編集画面を開き、証明書の内容を貼り付け、末尾で[Enter]キーを押して空の行を追加します。



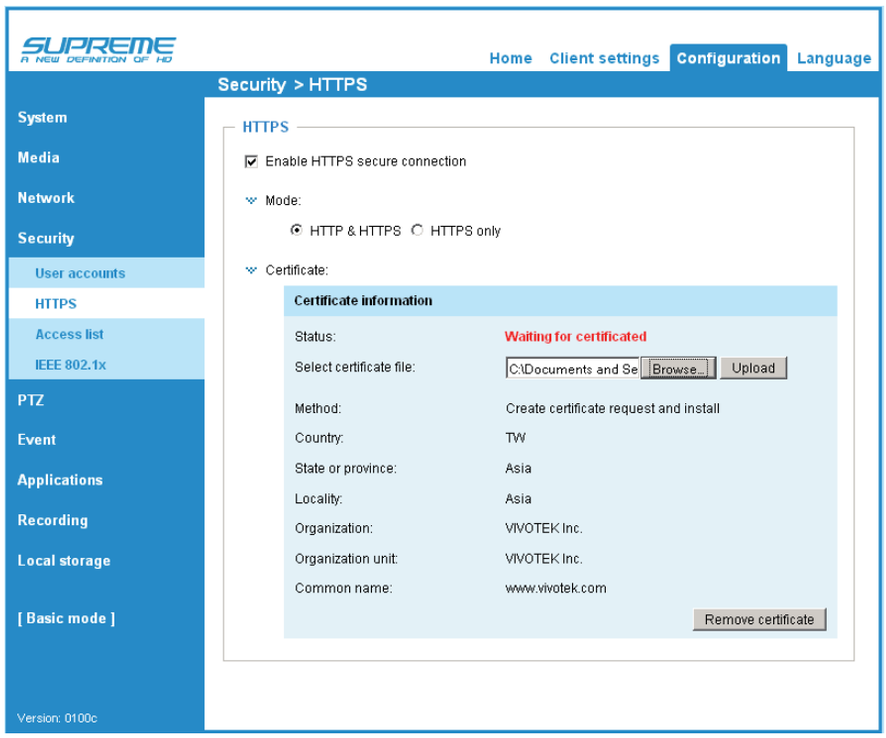
8. ファイル形式をDOSからUNIXに変換します。[File menu] > [Conversions] > [DOS to Unix]を開きます。



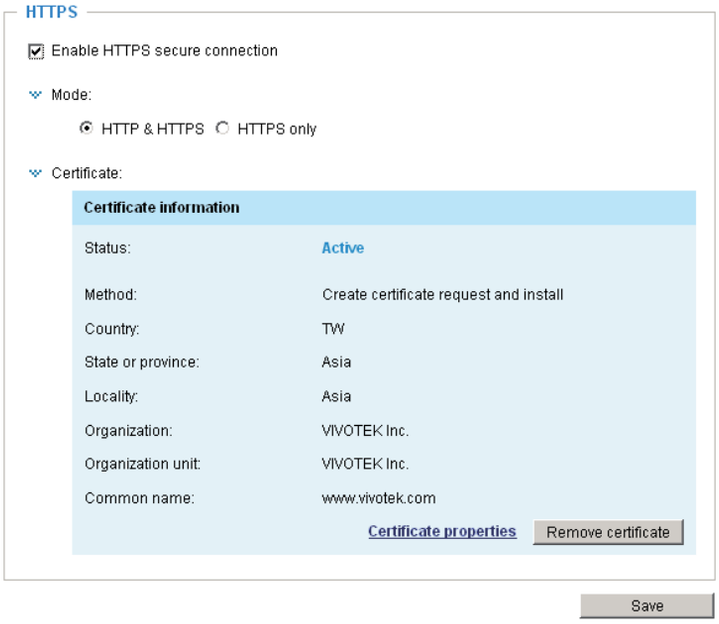
9. “CAcert.crt”のようなファイル名を使用し、“.crt”拡張子を付けて編集を保存します。



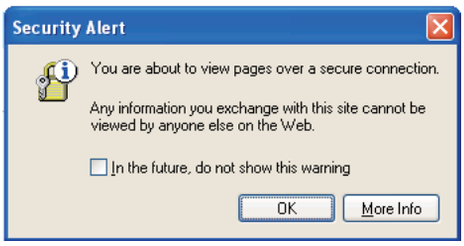
10. 元のカメラの画面に戻ります。[Browse]ボタンを使用してcrt証明書ファイルを指定し、[Upload]をクリックして証明書を有効にします。

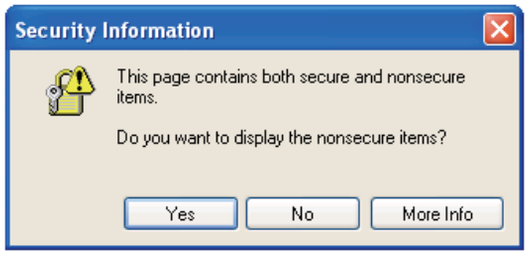


11. 証明書ファイルが正常にアップロードされると、ステータスが[Active]になります。[Save]ボタンをクリックして設定を有効にする前に、必ず証明書がインストールされていることを確認してください。



12. 暗号化されたHTTPSセッションを開始するには、[Home]をクリックしてメインページに戻り、アドレスバーのURLアドレスを ”http://” から “https://” に変更してキーボードの[Enter]キーを押してください。セキュリティの警告ダイアログが表示されますので、[OK] または[Yes]をクリックして、HTTPSを有効にします。



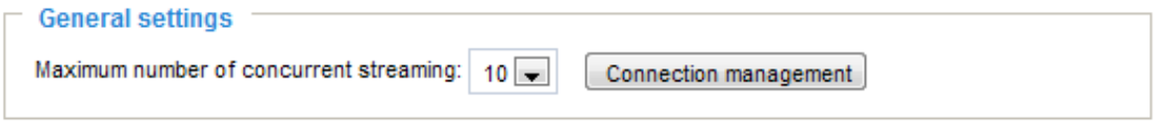




Security > Access List

この項目ではクライアントPCのIPアドレスを確認してアクセス許可を制御する方法について説明します。

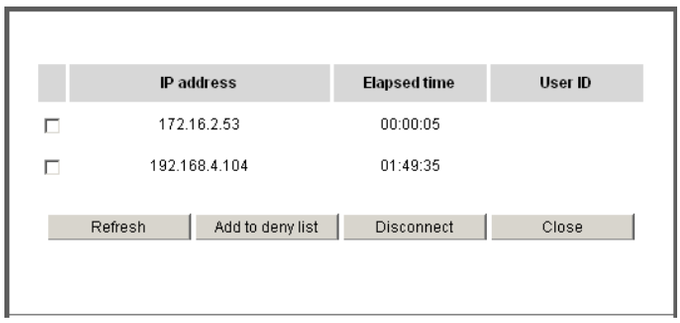
General Settings



Maximum number of concurrent streaming connection(s) limited to: 同時ストリーミング接続の最大数は、10クライアントに制限されています(stream1からstream3までを含む)。デフォルト値は10です。この値を変更して[Save]をクリックすると、現在のすべての接続が切断され、自動的に再リンクが試行されます(IEエクスプローラまたはQuickTimeプレーヤーの場合)。

View Information: クリックすると、現在の接続の一覧を示すステータスウインドウが表示されます。

例：



[View information]の一覧には現在ライブストリーミングを表示しているコンソールだけが表示されます。

- IP address: ネットワークカメラへの現在の接続を見ることができます。
- Elapsed time:クライアントがWebページにアクセスしている時間を見ることができます。
- User ID: 管理者がWebページのパスワードを設定している場合、クライアントはライブビデオにアクセスするためにユーザー名とパスワードを入力する必要があり、このユーザー名が[User ID]に表示されます。管理者がライアントにユーザー名とパスワードなしでWebページにリンクすることを許可した場合、[User ID]は空になります。

クライアントがユーザ名とパスワードなしでライブビデオにアクセスできる場合、下記の状況が考えられます。

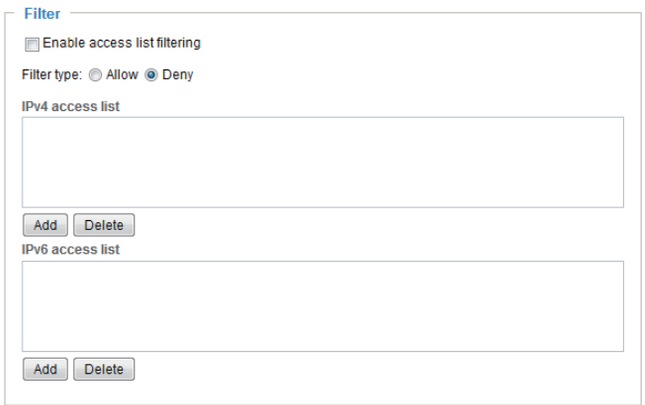
1. 管理者がrootパスワードを設定していない。rootパスワードの設定方法とユーザーアカウントの管理についてはP97[Security] > [User account]を参照してください。
2. rootパスワードは設定されているが、RTSP認証を[disable]にしている。RTSP認証については、P87[RTSP streaming]を参照してください。
3. rootパスワードは設定されているが、[Anonymous Viewing]を許可している。詳しくはP97[Allow anonymous viewing]を参照してください。

- Refresh: クリックすると現在のすべての接続を更新することができます。
- Add to deny list: list : [Connection Status]リストから選択したエントリを拒否リストに追加してアクセスを拒否することができます。追加された接続は一時的に切断され、自動的に再リンクを試みます(IEエクス プローラまたはQuickTimeプレーヤーの場合)。拒否リストを完全に有効にする場合は、[Enable access list filtering]をオンにし、[Save]をクリックします。
- Disconnect: 切断したい接続を選択してこのボタンをクリックすると、現在の接続を切断することができます。選択された接続は一時的に切断され、自動的に再リンクを試みます(IEエクスプローラまたはQuickQuickTimeプレーヤーの場合)。

Filter

Enable access list filtering: この項目をチェックして[Save]をクリックすると、アクセスリストのフィルタリング機能を有効にすることができます。

Filter type: フィルタの種類を選択することができます。[Allow]を選択すると、その下の[Access list]にあるIPアドレスを持つクライアントだけがネットワークカメラにアクセスでき、他のクライアントはアクセスできなくなります。逆に、[Deny]を選択すると、[Access list]にIPアドレスが登録されているクライアントはネットワークカメラにアクセスできなくなり、他のクライアントはアクセスできます。

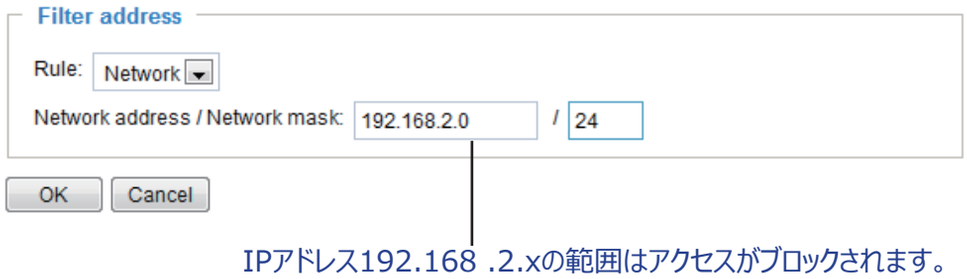


また、[Access list]には規則を追加することもできます。
[IPv6 Access list]はIPv6を有効にしている場合にのみ表示されます。IPv6の設定については、P80 Network> General settings]を参照してください。

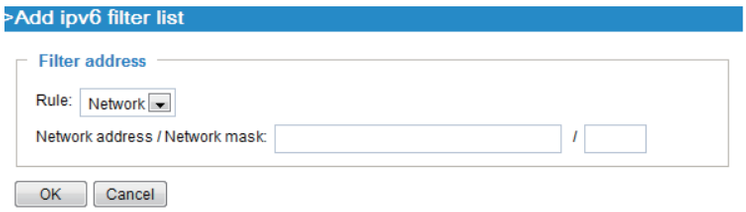
規則には次の3種類があります。
Single: この規則を使用して、IPアドレスを[Allow/Deny]リストに追加することができます。
例:



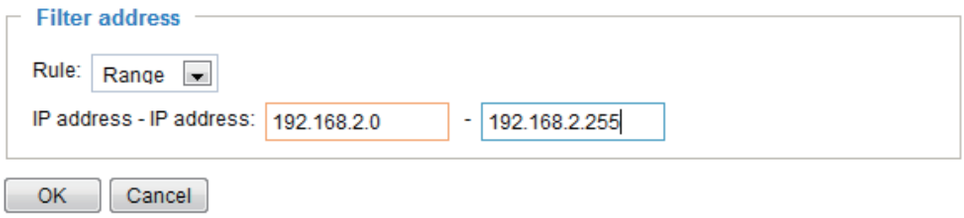
Network: この規則を使用して、ネットワークアドレスと対応するサブネットマスクを[Allow/Deny]リストに割り当てることができます。アドレスとネットワークマスクはCIDR形式で書き込まれます。
例:



IPv6フィルタを使用する場合は、下図のウインドウが表示されます。IPv6アドレスと2桁のプレフィックス長を入力して、構成内のIPアドレスの範囲を指定します。

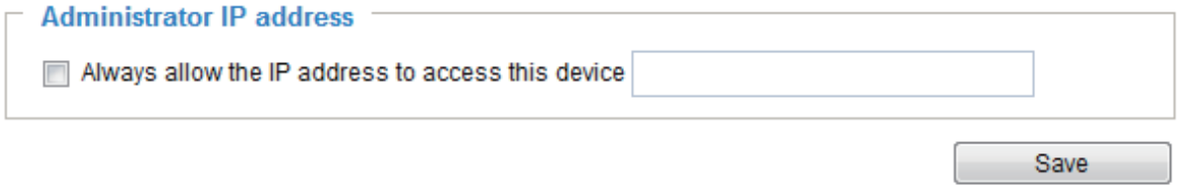


Range: この規則を使用して、[Allow/Deny]リストにIPアドレスの範囲を割り当てることができます。
※この規則はIPv4アドレスにのみ適用されます。
例：



Administrator IP address

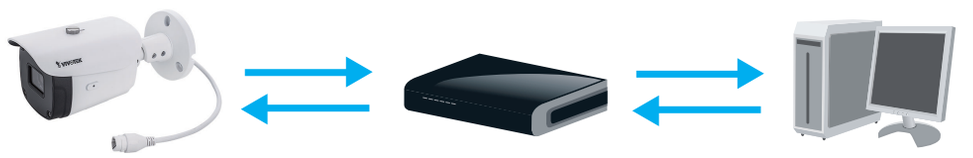
Always allow the IP address to access this device: この項目にチェックを入れ、管理者のIPアドレスを追加すると、管理者が常にデバイスに接続できるかどうかを確認することができます。



Security > IEEE 802.1X

ネットワーク環境でポートベースのネットワークアクセス制御であるIEEE 802.1xを使用している場合はこの機能を有効にします。ネットワークデバイス、中継スイッチ/アクセスポイント/ハブ、RADIUSサーバも802.1xに対応し、設定が有効になっていることを確認してください。802.1x規格はローカルエリアネットワークのセキュリティを強化するために設計されており、ネットワークポート(有線または無線)に接続されたネットワークデバイス (クライアント) に認証を提供します。クライアントとサーバー間のすべての証明書が確認されると、ポイントツーポイント接続が有効になり、認証に失敗した場合そのポートへのアクセスは禁止されます。また802.1xでは、既存のプロトコルである拡張認証プロトコル(EAP)を使用して通信を行います。

■ 802.1 x認証で保護されるネットワークのコンポーネント:



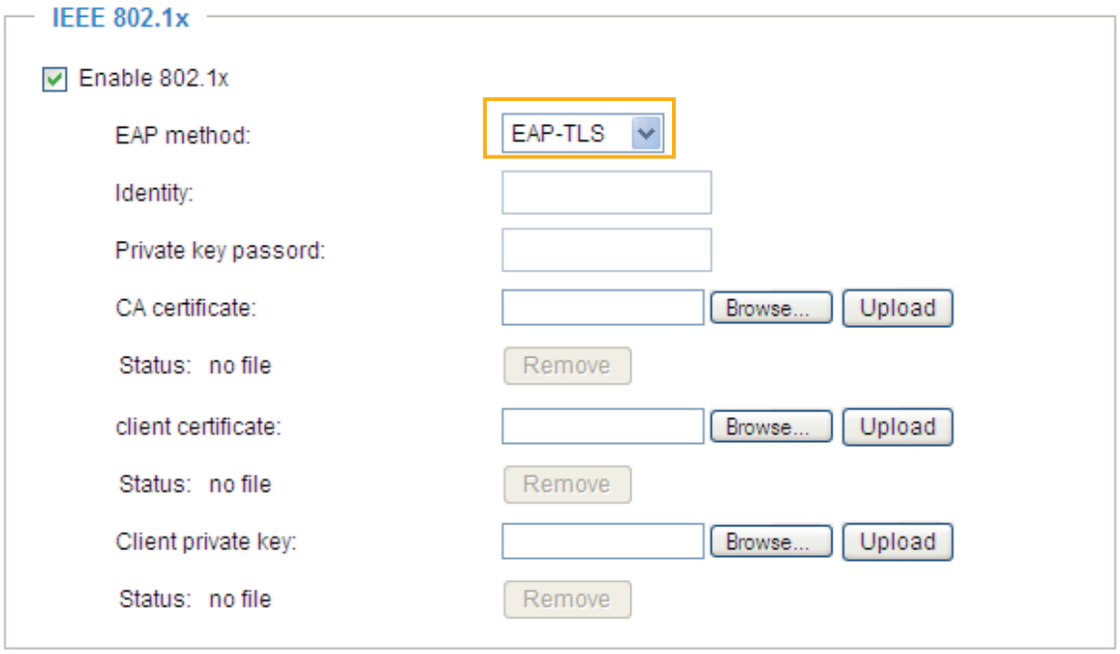
1. サプリカント：認証をリクエストするクライアントエンドユーザー(カメラ)。
2. オーセンティケータ：無許可のエンドユーザーが認証サーバと通信することを制限する仲介者(アクセスポイントやスイッチ)。
3. 認証サーバ：クライアント証明書を確認し、エンドユーザーのアクセス要求を受け入れるかどうかを決定する場所(通常はRADIUSサーバ)。

■ VIVOTEKのネットワークカメラは、認証を実行するEAP方式として、EAP-PEAPとEAP-TLSの2種類をサポートしています。

次の手順で802.1xの設定を有効にします。

1. 802.1xで保護されたネットワークにカメラを接続する前に、RADIUSサーバが確認することができる認証局(ネットワーク管理者)からのデジタル証明書を適用してください。
2. ネットワークカメラを保護ネットワーク外のPCやノートPCに接続し、下図のネットワークカメラの設定画面を開き、[EAP method]で[EAP-PEAP]または[EAP-TLS]のどちらかを選択します。続けて[Identify]、[Password]にそれぞれCAが発行したIDとパスワードを入力し、[CA certificate]欄で関連する証明書をアップロードします。



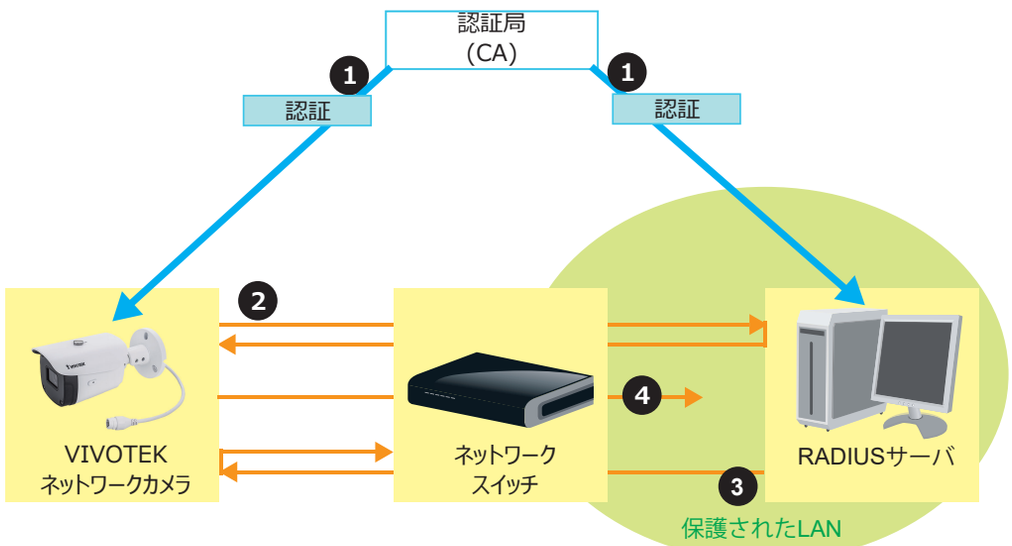


3. すべての設定が完了したら、ネットワークカメラを802.1x対応スイッチに接続して保護ネットワークに移動します。その後、デバイスは自動的に認証を開始します。

ノート:

► 802.1 xの認証プロセス：

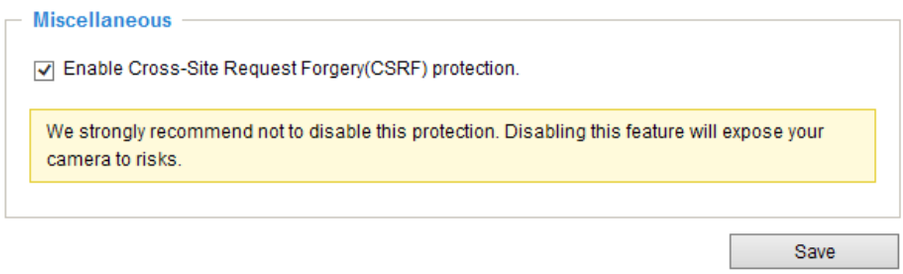
1. 認証局(CA)は必要な署名済み証明書をネットワークカメラ(サプリカント)とRADIUSサーバ(認証サーバ)に提供します。
2. ネットワークカメラはスイッチ(オーセンティケータ)を介して自身のIDとクライアント証明書を提供し、802.1Xを使用して保護ネットワークへのアクセスを要求します。この証明書はスイッチによってRADIUSサーバに転送され、RADIUSサーバはアルゴリズムを使用してネットワークカメラを認証し、受け入れまたは拒否をスイッチに返します。
3. また、スイッチはRADIUSサーバの証明書をネットワークカメラに転送します。
4. すべての証明書が検証されると、スイッチはネットワークカメラの状態を許可に変更し、あらかじめ設定されたポート経由で保護されたネットワークへのアクセスを許可します。



Security > Miscellaneous

組込み済みの TrendMicro ユーティリティによってクロスサイトリクエストフォージェリに対する保護を有効にすることができます。クロスサイトリクエストフォージェリはワンクリック攻撃またはセッションライディングとして知られ、CSRF と呼ばれています。CSRF は Web サイト (この場合はカメラ) に対する悪意ある攻撃の一種です。不正なコマンドを Web アプリケーションが信頼しているユーザーから送信させるのが特徴で、信頼しているユーザーのリクエストに、自身のクッキーを含むリクエストなどを含ませるメカニズムが用いられています。
悪意のある Web サイトがそのようなコマンドを送信するためにさまざまな方法が使用される可能性があります。 それらは、特別に細工されたイメージタグ、非表示フォーム、JavaScript XML Http リクエストなどです。悪意のある攻撃は、ユーザーの操作なしに、あるいはユーザーが知らないうちに発生するおそれがあります。

通常はこの機能を OFF にする必要はありませんが、ブラウザから cgi コマンドでリクエストするときなどは、チェックを外して保存してください。



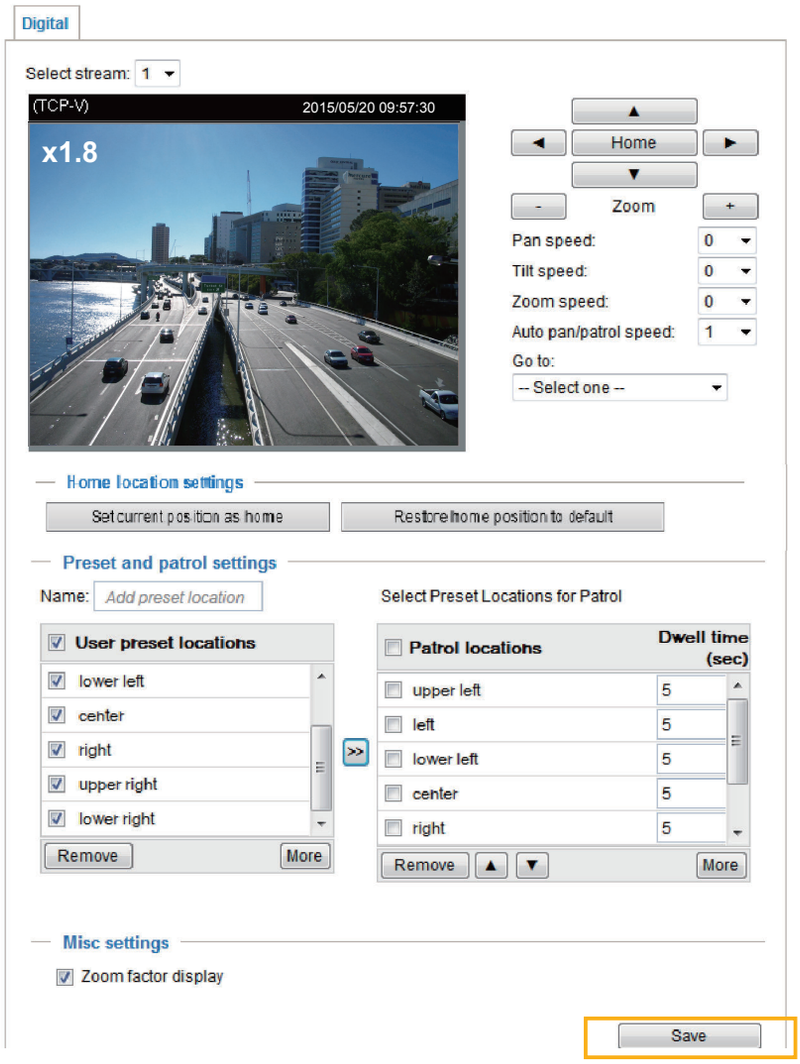
PTZ > PTZ settings

この項目では、ネットワークカメラのパン/チルト/ズーム操作の操作方法について説明します。

Digital: e-PTZ 操作を制御します。撮像範囲内では、カメラを物理的に動かすことなく、焦点をターゲット領域にすばやく移動してクローズアップ表示することができます。

Digital PTZ Operation (E-PTZ Operation)

e-PTZ制御設定セクションは下図のように表示されます。



e-PTZに関する詳細は115ページをご参照ください。

Auto pan/patrol speed: オートパン/パトロール速度制御を設定することができます。速度は1~5(低速/高速)の範囲から選択します。

Zoom factor display
この項目をチェックすると、ライブウインドウを拡大/縮小したときに、上の図のように画面内にズームイを拡大/縮小したときに、上の図のように画面ンジケータを表示することができます。
e-PTZの設定が完了したら、[Save]をクリックして設定を有効にします。

図：E-PTZモードのホームページ



■ ホームページにもe-Preset Positionsが表示されます。ドロップダウンリストからいずれかを選択すると、カメラ映像は選択した位置に移動します。

■ I複数のストリームに異なるプリセット位置を設定した場合は、それぞれのストリームごとに個別のプリセット位置を表示できます。

Global View
e-PTZコントロールパネルを使用するだけでなく、マウスを使用してフローティングフレームをドラッグまたはサイズ変更し、表示領域をパン/チルト/ズームすることもできます。ライブビューウインドウも表示領域に移動します。

Moving Instantly
この項目をチェックすると、フローティングフレームを移動した直後にライブビューウインドウの表示も切り換わります。この項目がチェックされていない場合は、ある位置から別の位置に移動するプロセスが表示されます。

Click on Image
e-PTZ機能は[画像クリック]にも対応しています。グローバルビューウインドウまたはライブビューウインドウのいずれかのポイントをクリックすると、表示領域もそのポイントに移動します。

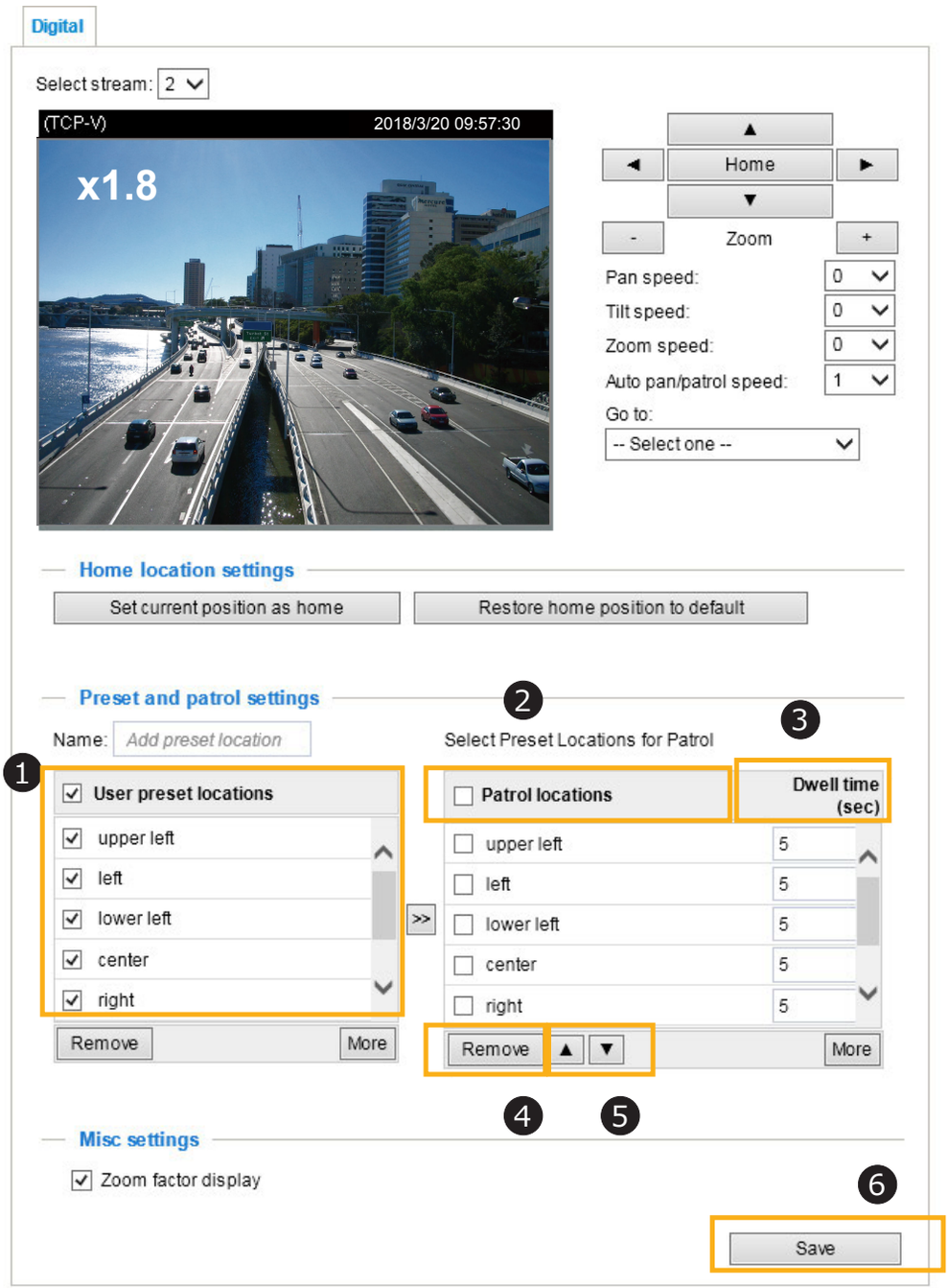
[Click on Image]機能が適用できるのは、最大フレームサイズよりも小さな領域を設定した場合のみです。たとえば、800 x 600ピクセルの領域が設定されている場合などで

Patrol button: このボタンをクリックすると、ネットワークカメラは設定されたプリセット位置を順番に巡回します。

Patrol settings

パトロールするネットワークカメラのプリセット位置を選択することができます。
次の手順でパトロールスケジュールを設定します。

1. リストからプリセットの場所を選択し、 をクリックします。
2. 選択したプリセット位置が[Patrol locations]リストに表示されます。
3. 自動巡回の際の設定位置の滞留時間を設定します。
4. リストからプリセットの位置を削除する場合は、削除位置を選択して[Remove]をクリックします。
5. パトロールの順序を変更するには、ロケーションを選択して をクリックします。
6. リストに保存するパトロール位置を選択し、[Save]をクリックしてパトロール設定を有効にします。
7. パトロールを実行するには、ホームページで[Patrol button]をクリックしてください。

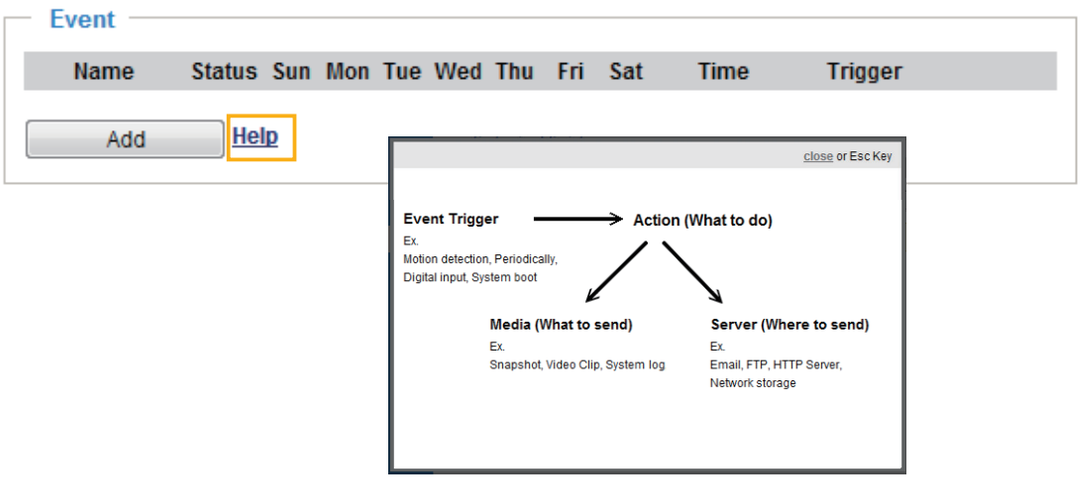


ノート:

- ホームページにもプリセット位置が表示されます。[Go to]メニューから1つ選択すると、カメラは選択したプリセット位置に移動します。
- [Patrol]をクリックすると、ネットワークカメラは選択した位置に沿って繰り返しパトロールをします。

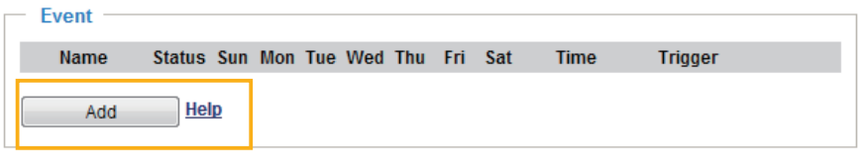
Event > Event settings

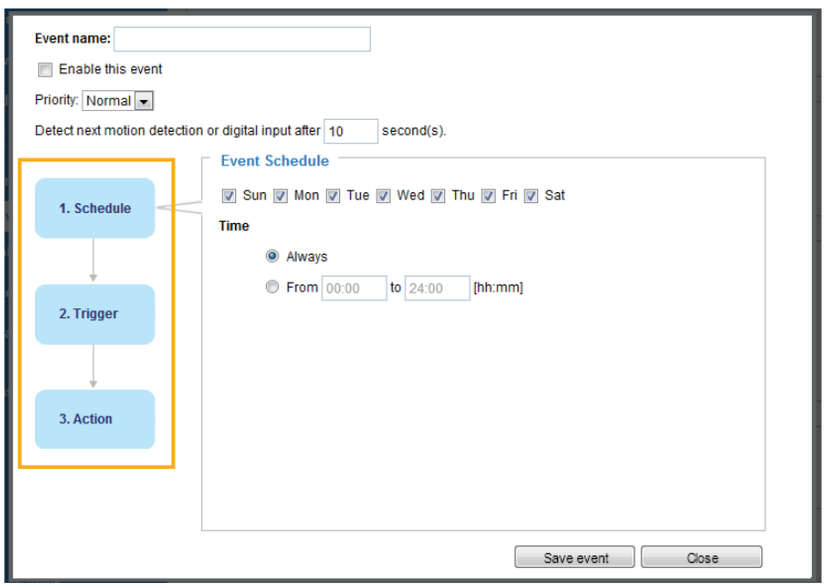
この項目では、特定の状況(イベント)への応答をネットワークカメラに設定する方法を説明します。一般的なアプリケーションでは、たとえば映像に動きが検出されると、ネットワークカメラがバッファされたイメージ通知をFTPサーバや電子メールアドレスに送信します。[Help]をクリックすると、ポップアップウインドウに、動作検出や外部デジタル入力デバイスなどのさまざまなソースによってイベントがトリガされることを説明する図が表示されますので、これをもとに、イベントが発生したときに実行するアクションの種類を指定したり、スナップショットやビデオを電子メールアドレスやFTPサイトに送信するように設定することができます。



Event

ビデオやスナップショットの記録などのイベントを設定するには、そのイベントのトリガが発生したときにネットワークカメラが実行するアクション (メディアファイルを送信するサーバーの設定など) を認識できるようにサーバーとメディアを設定する必要があります。イベント設定ではユーザー定義のトリガーによって開始されるアクションを設定します。[add] をクリックして [Event settings] ウインドウを開き、スケジュール、トリガ、アクションの 3 つの要素を整理してイベントを設定します。合計 3 つのイベントを設定することができます。





- Event name : 設定するイベントの名前を入力します。
- Enable this event: チェックを入れると、設定するイベントを有効にすることができます。
- Priority: このイベントの相対的な重要度を選択することができます。重要度は[High]、[Normal]、[low]から選択します。優先順位が高いイベントが最初に実行されます。

- Detect next motion detection or digital input after □ seconds: モーション検知後、次のモーション検知を一時停止する時間を秒単位で入力します。これにより、モーション検知関連のアクションが頻繁に発生するのを防ぐことができます。

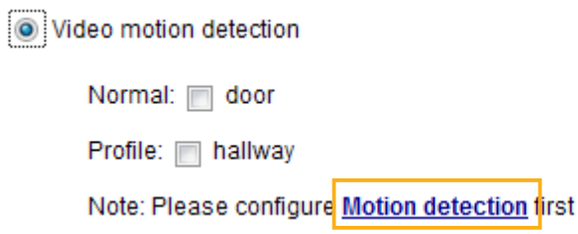
1. Schedule

イベントトリガが有効になる期間を指定することができます。イベント起動スケジュールで曜日と時刻 (24 時間形式) を選択してください。たとえば勤務時間外にのみイベントをトリガするように設定することもできます。

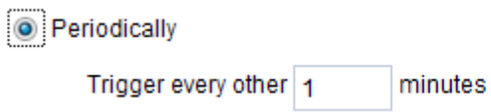
2. Trigger

イベントをトリガする定義を設定することができます。トリガはネットワークカメラのモーション検知や外部デジタル入力を設定することができます。
次に示すように、トリガソースには他にもいくつかの種類があります。設定オプションがある場合には項目を選択してください。

- Video motion detection
  このオプションを選択すると、カメラのモーション検知結果をトリガとして使用します。この機能を有効にするには、最初にモーション検知ウインドウを設定する必要があります。詳しくはP131[MotionDetection]を参照してください。



- Periodically
  このオプションを選択すると、ネットワークカメラは定義された時間おきに定期的にイベントをトリガすることができます。時間は999分まで設定が可能です。

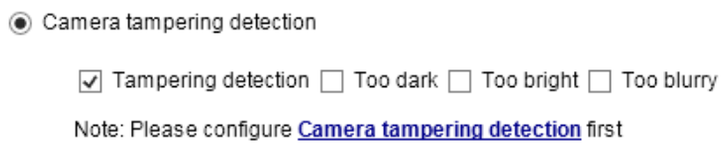


- System boot
  このオプションを選択すると、ネットワークカメラが再起動して再接続されたときにイベントトリガを起動します。

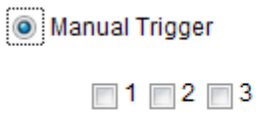
- Recording notify
  このオプションを使用すると、記録ディスクがフルになったとき、またはディスクがフルになった後古いデータが上書きされたときに、イベントトリガを起動します。

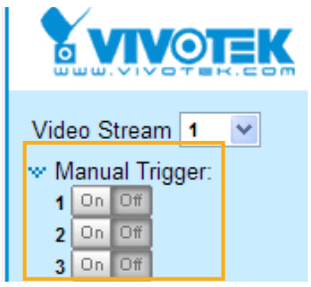
■ このオプションを選択すると、外部マイクを使用したときの音声検知のしきい値をイベントのトリガとして使用することができます。入力がしきい値を超えたか、しきい値を下回った場合トリガされます。音声検知はモーション検知を補完、またはカメラの画像でカバーしきれない領域のイベントを検出する方法として活用することができます。

■ Camera tempering detection
このオプションを選択すると、カメラにいたずらされていることを検出したときにイベントをトリガすることができます。この機能を有効にするには、最初にタンパー検知を設定する必要があります。詳しくはP130をご参照ください。

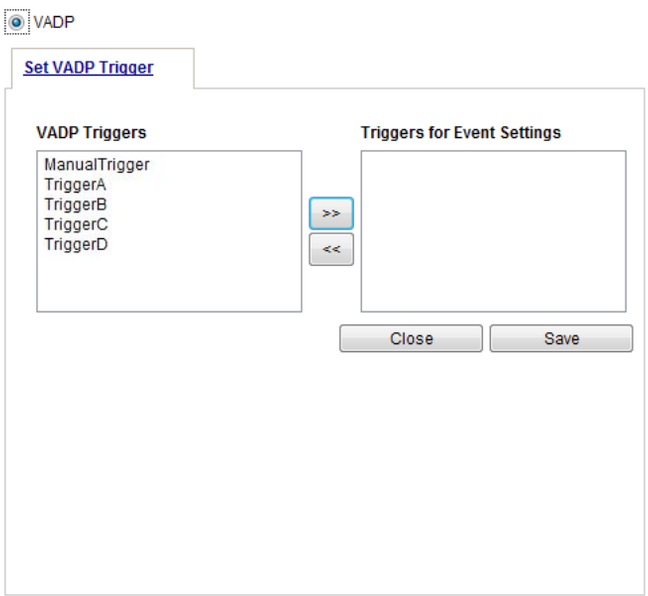


■ Manual Triggers
このオプションを選択すると、ホームページの[On/Off]ボタンをクリックして、イベントトリガを手動で有効にすることができます。この機能を使用する前に、1、2、3にそれぞれあてはまるイベントを設定してください。

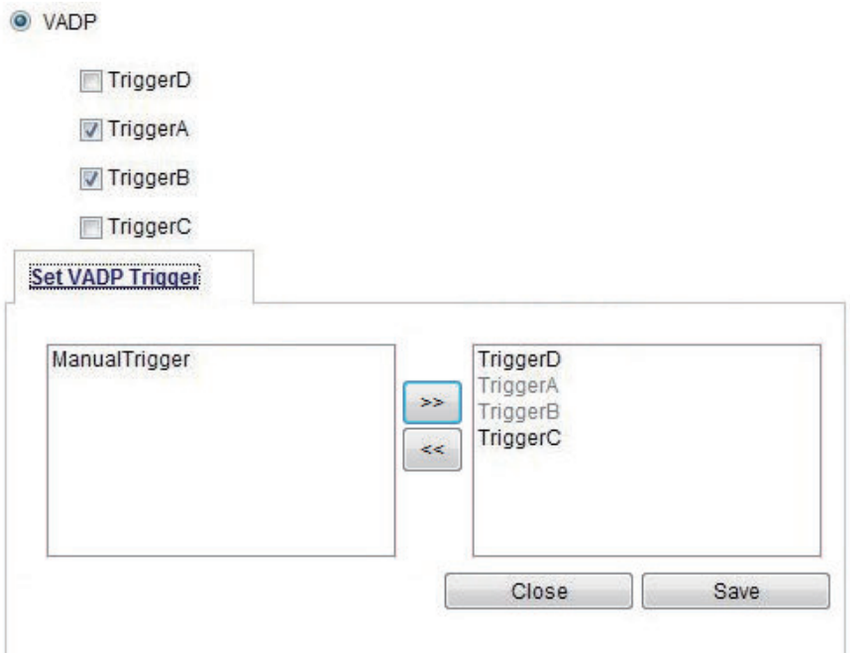




■ VADP
VADPトリガをイベント設定に関連付ける前に、VADPモジュールをカメラにアップロードして機能を有効にしておく必要があります。
[Set VADP Trigger]ボタンをクリックして、VADPセットアップメニューを開きます。VADPと呼ばれるサードパーティ製ソフトウェアモジュールで使用可能なトリガ条件が一覧で表示されます。矢印ボタンを使用して、これらのトリガを選択します。これらのモジュールは、モーション検知のトリガやビデオコンテンツ解析に関連するアプリケーションなど、さまざまな機能が提供されています。VADPモジュールの設定オプションについてはP134を参照してください。

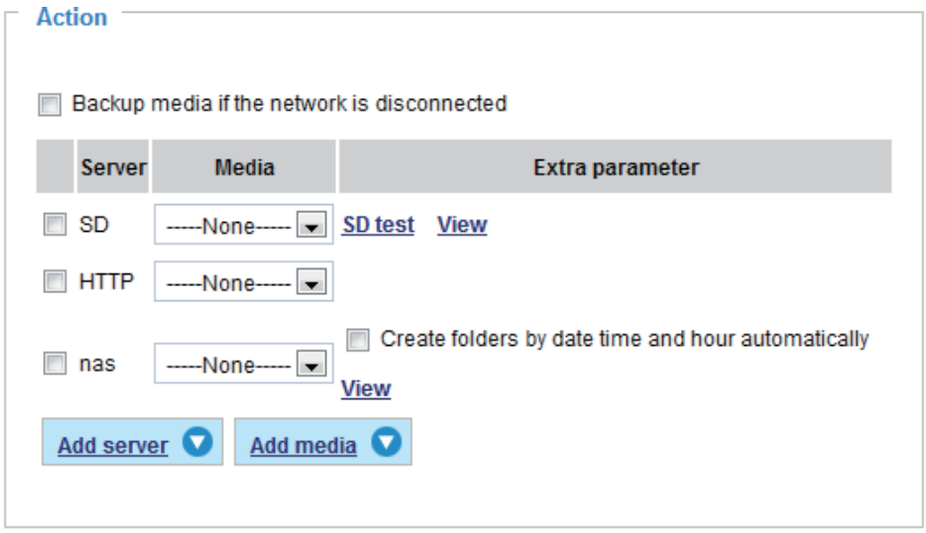


イベントのトリガが設定されると、VADPオプションの下に一覧表示されます。



3. Action

イベントのトリガがアクティブになったときにネットワークカメラが実行するアクションを定義します。



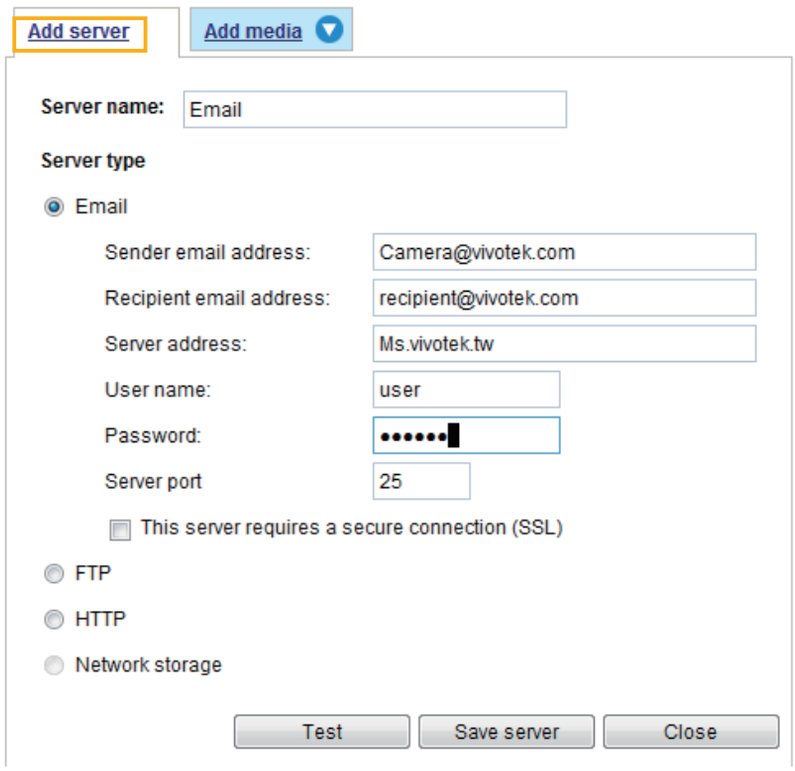
■ Backup media if the network is disconnected

このオプションを選択すると、ネットワークが切断されているときにSDカードにメディアファイルをバックアップすることができます。この機能は、ネットワークストレージ(NAS)をセットアップした後にのみ表示されます。バックアップするメディアには、イベント設定に応じて、スナップショットイメージ、ビデオ、システムログが含まれます。

Add server

トリガがアクティブになったときにネットワークカメラが実行するアクション(メディアファイルを送信するサーバはどれか、など)を認識できるようにサーバとメディアを設定する必要があります。まず、[Add server]をクリックして、サーバの設定画面を開きます。さらにここでは、トリガがアクティブになったときの通知メッセージの送信先を指定することができます。合計5つのサーバを設定することができます。

サーバは電子メール、FTP、HTTP、ネットワークストレージの4つがあります。設定するサーバーを選択してください。



Server type - Email

トリガがアクティブになったときにメディアファイルを電子メールで送信する場合に選択します。

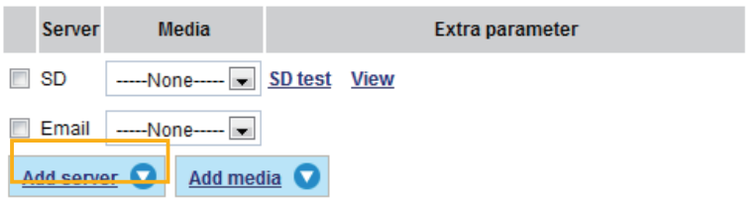
- Server name：設定するサーバの名前を入力します。
- Sender email address：送信者のメールアドレスを入力します。
- Recipent email address：通知を受信するメールアドレスを入力します。
- Server address：メールサーバのドメイン名か IP アドレスを入力します。
- User name：必要に応じて、メールアカウントのユーザー名を入力します。
- Password：必要に応じて、メールアカウントのパスワードを入力します。
- Server port：既定のメールサーバポートは 25 に設定されています。別のポートを手動で設定することもできます。

SMTP サーバがセキュリティで保護された接続 (SSL) を要求する場合は、[This server requires a secure connection(SSL)] を選択します。

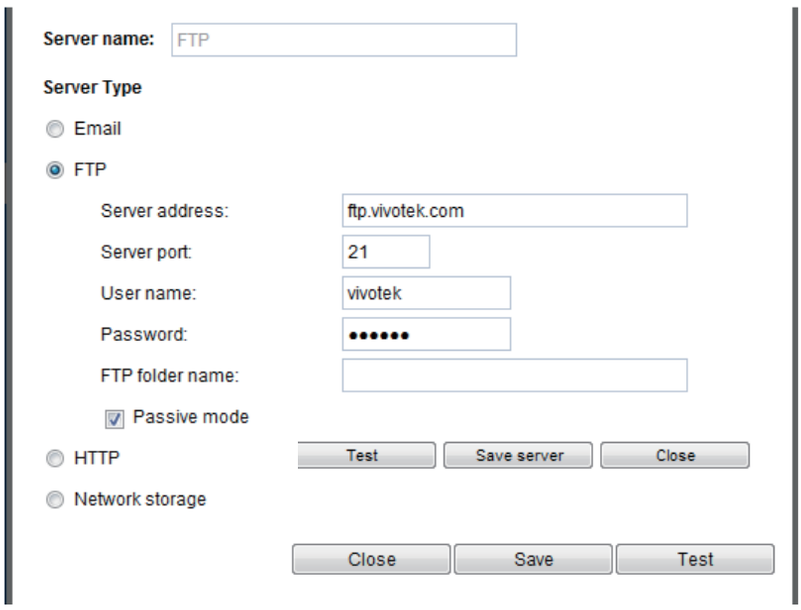
電子メール設定が正しく設定されているかどうかを確認するには[Test]をクリックします。結果がポップアップウインドウに表示されます。成功した場合は、結果を示すメールも送信されます。



[Save server] をクリックして、設定を有効にします。
最初のイベントサーバを設定すると、このサーバは[Server list]に自動的に表示されます。他のサーバオプションを追加する場合は[Add server]を再度クリックしてください。



Server type - FTP
トリガがアクティブになったときにメディアファイルをFTPサーバに送信する場合に選択します。



- Server name：設定するサーバの名前を入力します。
- Server address：FTP サーバのドメイン名か IP アドレスを入力します。
- Server port：既定の FTP サーバポートは 21 に設定されています。1025 から 65535 までの別のポート番号に割り当てることもできます。
- User name：FTP アカウントのユーザー名を入力します。
- Password：FTP アカウントのパスワードを入力します。
- FTP folder name

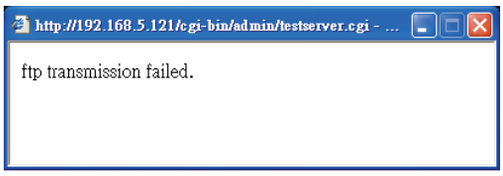
メディアファイルを保存するフォルダを入力します。フォルダが存在しない場合は、カメラによって自動的に FTP サーバ上にフォルダが作成されます。

■ Passive mode

通常ファイアウォールは、外部からの新しい接続を受け入れません。ただしFTPサーバがパッシブモードに対応している場合は、この項目を選択することでパッシブモードFTPを有効にし、データ転送がファイアウォールを通過できるようにすることができます。カメラの工場出荷設定ではこの機能は有効となっています。

FTP設定が正しく設定されているかどうかを確認するには、[Test]をクリックします。下図のようなポップアップウインドウで結果が表示されます。成功した場合は、FTPサーバ上にtest.txtファイルが確認できます。





[Save]をクリックして、設定を有効にします。

Server type - HTTP

トリガがアクティブになったときにメディアファイルをHTTPサーバに送信する場合に選択します。



■ Server name：設定するサーバの名前を入力します。
■ URL：HTTP サーバの URL を入力します。
■ User name：必要に応じてユーザー名を入力します。
■ Password：必要に応じてパスワードを入力します。

HTTP 設定が正しく設定されているかどうかを確認するには、[Test] をクリックします。下図のようなポップアップウインドウで結果が表示されます。成功した場合は、HTTP サーバ上に test.txt ファイルが確認できます。

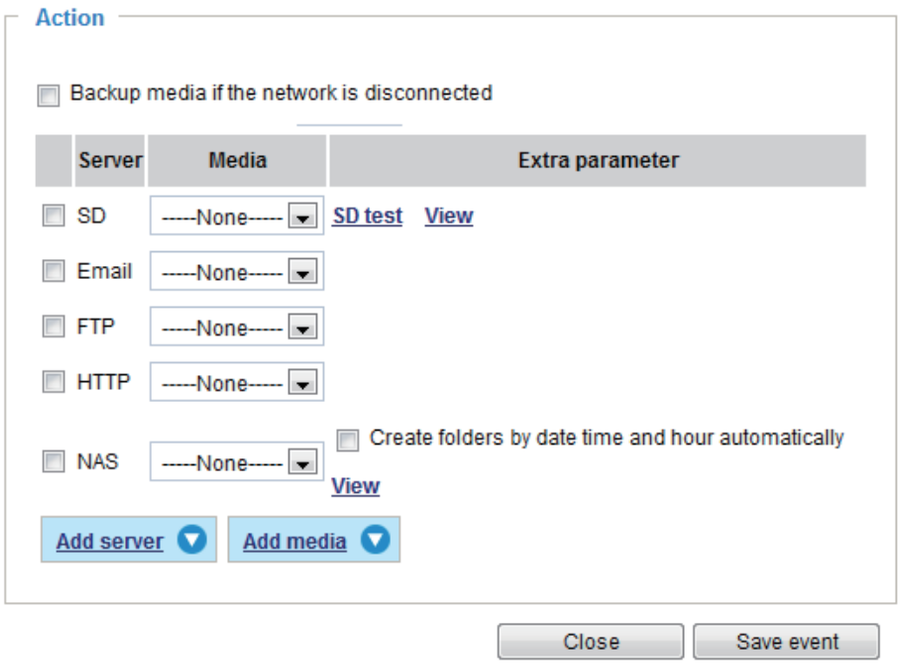




[Save]をクリックして、設定を有効にします。

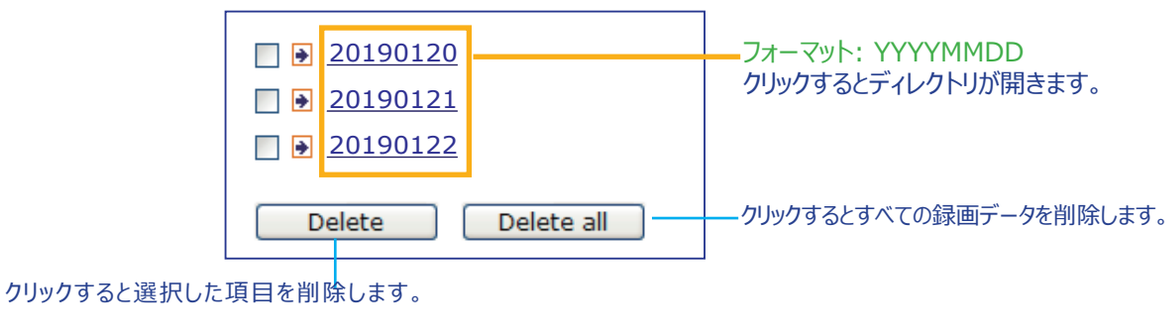
Network storage:
トリガがアクティブになったときにメディアファイルをネットワークストレージに送信する場合に選択します。詳しくは P141[NAS server] を参照してください。設定できる NAS サーバは 1 台のみです。

[Save] をクリックして、設定を有効にします。

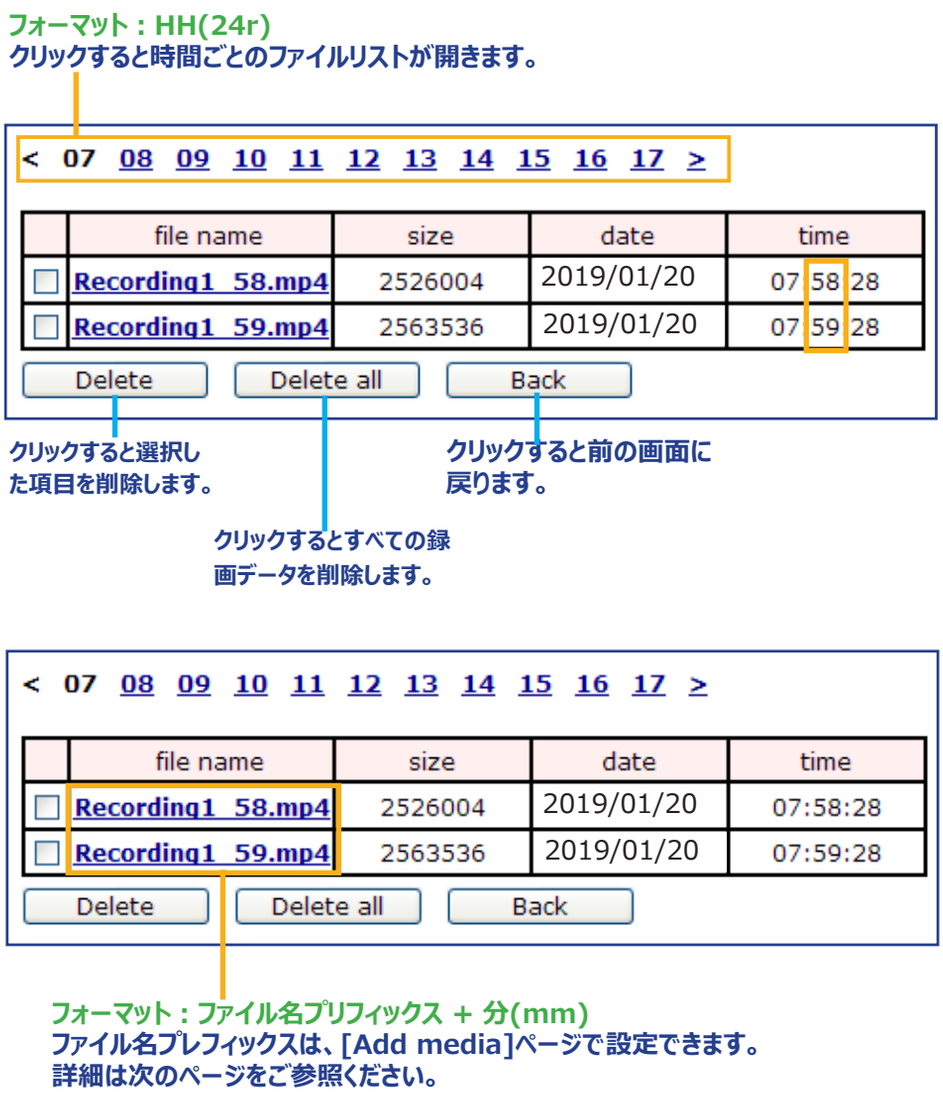


- SD Test：クリックすると SD カードをテストすることができます。テストが完了すると、結果を示すメッセージが表示されます。SD カードをローカルストレージとして使用する場合は、フォーマットしてから使用してください。詳しくは P126 をご参照ください。
- View：クリックするとファイルリストウインドウを開くことができます。この機能は SD カードとネットワークストレージで使用可能です。SD カードの [View] ボタンをクリックすると、ローカルストレージのページが表示され、SD カードに記録されたファイルを管理することができます。ローカルストレージの詳細については P143 を参照してください。ネットワークストレージの [View] ボタンをクリックすると、ネットワークストレージに記録されたデータを表示するためのディレクトリウインドウが表示されます。詳細は次のページをご参照ください。
- Create folders by date, time, and hour automatically：この項目を選択すると、映像がネットワークストレージに保存された日付ごとに自動的にフォルダを作成することができます。

下図はビデオクリップのファイルアドレスの例になります。

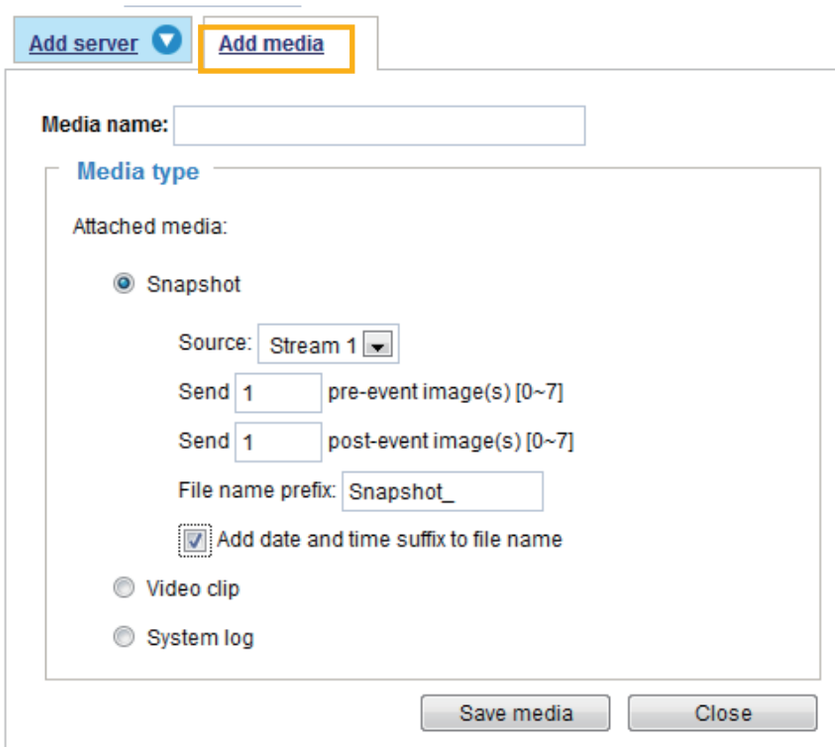


20190120 をクリックしてディレクトリを開くと、下図が表示されます。



Add media

トリガがアクティブになったときに送信されるメディアの種類を指定することができます。[Add media]をクリックして、メディア設定ウインドウを開きます。合計で5つのメディアを[Snapshot]、[Video clip]、[System log]の3種類から選択して設定することができます。メディアを選択して設定してください。

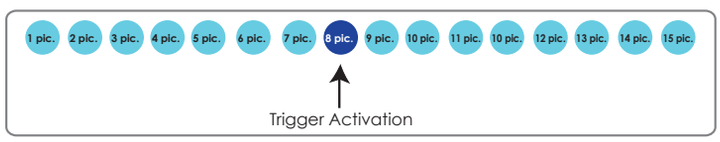


Media type - Snapshot
トリガがアクティブになったときにスナップショットを送信する場合に選択します。

- Media name: メディア設定の名前を入力します。

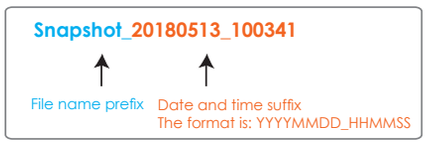
- Source: スナップショットを作成する任意のビデオストリームを選択します。
- Send ☐ pre-event images
  ネットワークカメラには、一定の枚数のイメージを一時的に保持するバッファがあります。トリガがアクティブになる前の画像として保存するイメージの数を指定します。最大7枚まで設定できます。
- Send ☐ post-event images
  トリガがアクティブになった後の画像として保存するイメージの数を指定します。最大7枚まで設定できます。

  例えば、トリガ前イメージとトリガ後イメージの両方が7に設定されている場合、トリガがアクティブになると合計15個のイメージが作成されます。



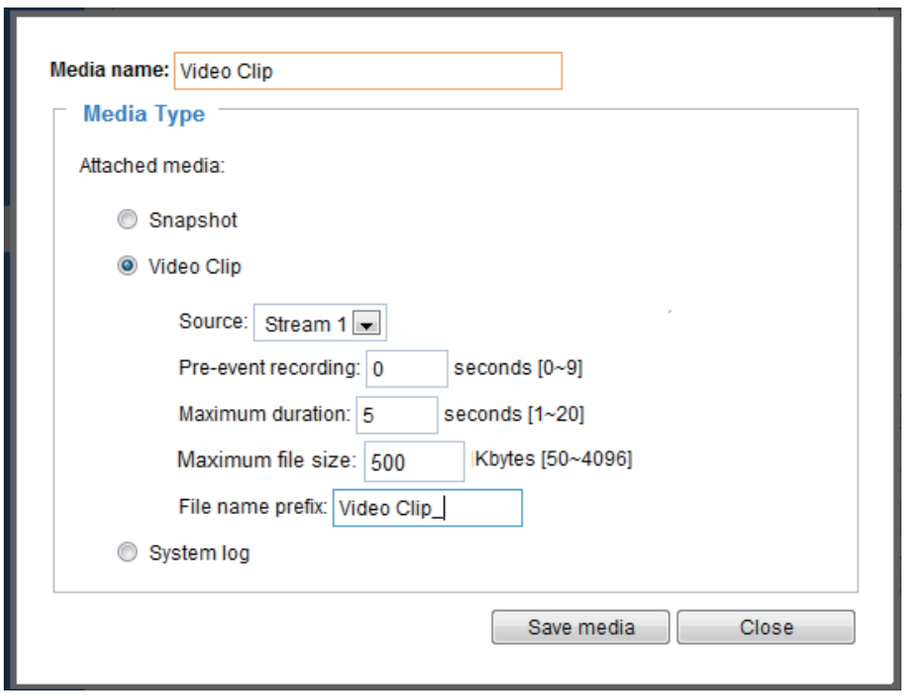
- File name prefix
  ファイル名の前に追加するテキストを入力します。

■ Add date and time suffix to the file name
このオプションを選択すると、ファイル名に日付/時刻のサフィックスを追加することができます。
例：



[Save media] をクリックして、設定を有効にします。
最初のメディアを設定すると、そのメディア名がリストに自動的に表示されます。さらにメディアオプションを追加する場合は、[Add media] を再度クリックします。

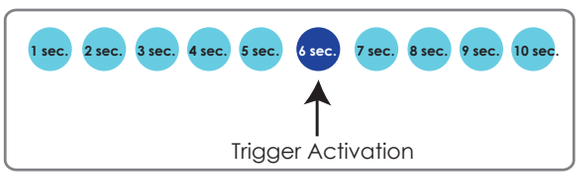
Media type - Video clip
トリガがアクティブになったときにビデオクリップを送信する場合に選択します。



■ Media name: メディア設定の名前を入力します。

■ Source: ビデオクリップを作成する任意のビデオストリームを選択します。
■ Pre-event recording
ネットワークカメラには、一定時間の画像を一時的に保持するバッファがあります。トリガがアクティブになるまでの記録時間を指定できます。最大9秒前まで設定することができます。

■ Maximum duration
最大録画時間を秒単位で指定します。最長時間は10秒です。たとえば、トリガ前の録画を5秒、最大録画時間を10秒に設定した場合、ネットワークカメラはトリガがアクティブになってからさらに4秒間録画を続けます。



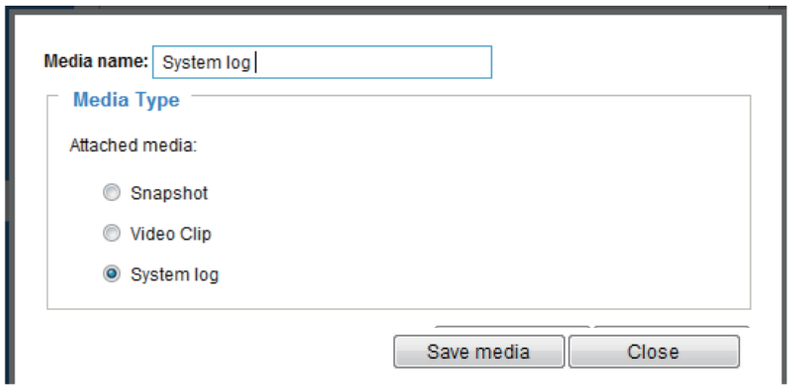
■ Maximum file size
最大ファイルサイズを指定することができます。一部のユーザーにおいては、法的証拠として映像を探してひとつにまとめる際に、ビデオクリップをつなぎ合わせる必要がある場合があります。

■ File name prefix
ファイル名の前に追加するテキストを入力します。
例：

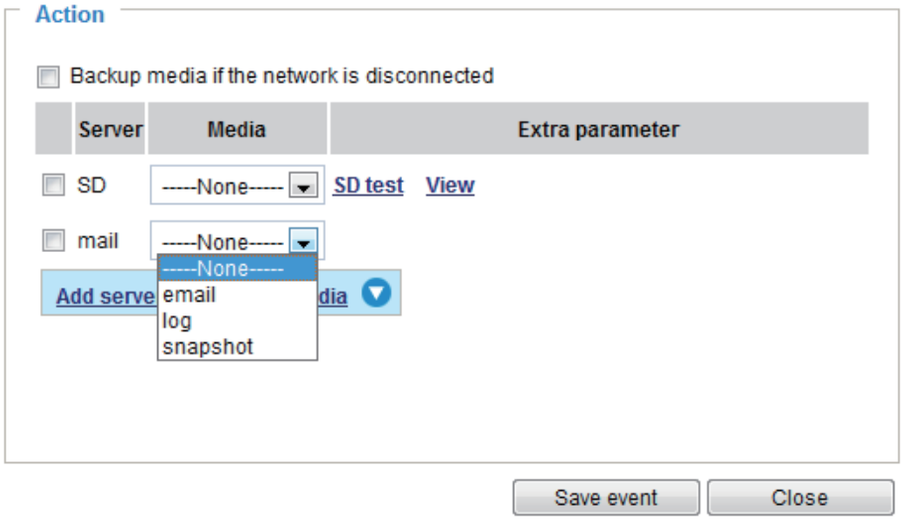


[Save media]をクリックして、設定を有効にします。

Media type - System log
トリガがアクティブになったときにシステムログを送信する場合に選択します。



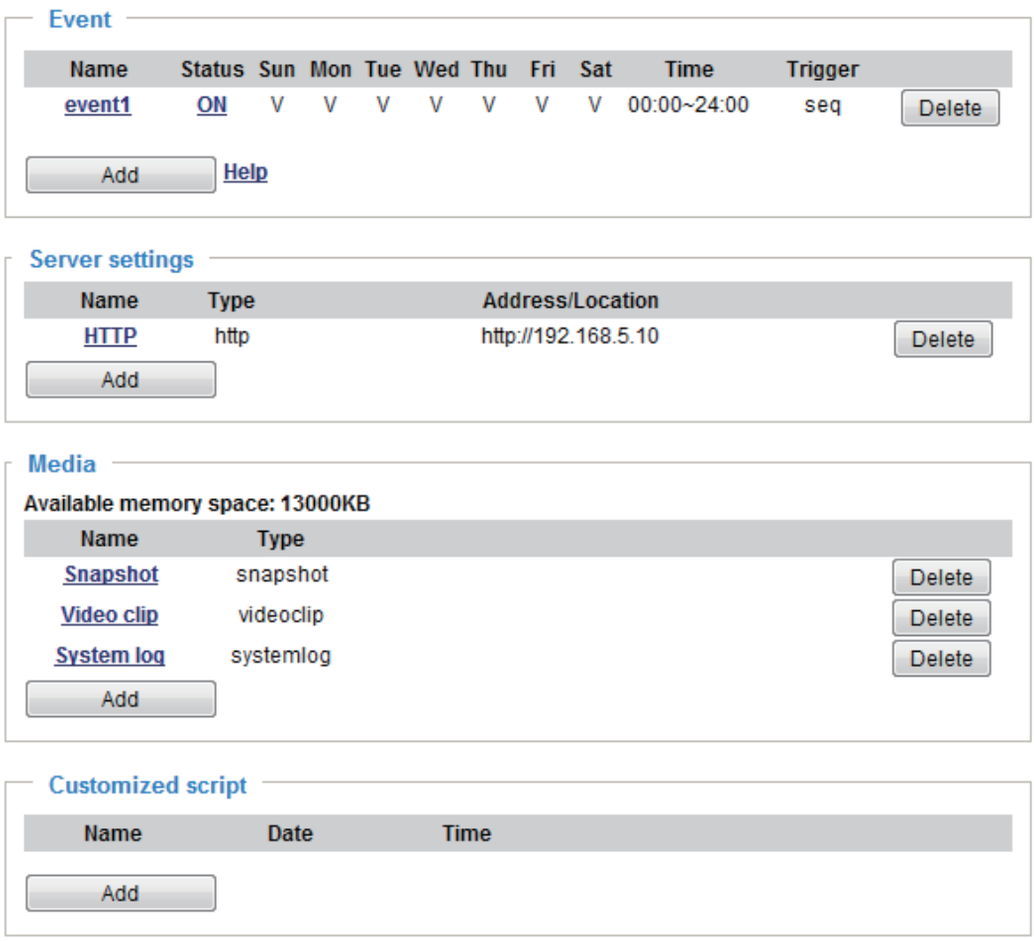
[Save media]をクリックして設定を有効にし、[Close]をクリックして終了します。



[Event settings]に、設定したサーバとメディアが一覧表示されます。イベント起動アクションを有効にするためには、[Event] > [Status]が[ON]になっている必要があります。

完了したら、[Save event]をクリックして設定を有効にし、[Close]をクリックしてページを閉じます。新しいイベント/サーバ設定/メディアが、[Event settings]のドロップダウンリストに表示されます。

下図は設定が完了した[Event settings]の例です。



イベントトリガを停止する場合は、[ON]をクリックしてステータスを[OFF]にするか、[Delete]をクリックしてイベント設定を削除します。

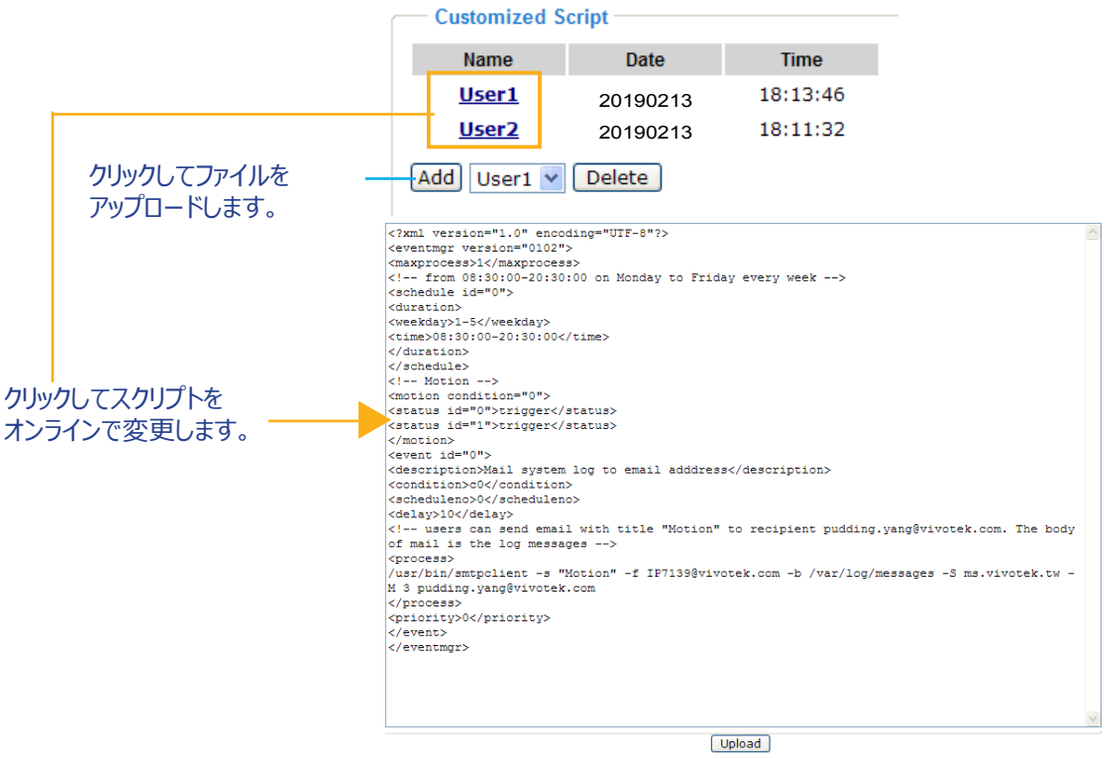
リストからサーバ設定を削除するには、リストのサーバ名横の[Delete]をクリックします。既存のイベント設定に適用されているサーバ設定は削除することができません。

リストからメディア設定を削除するには、リストのメディア名横の[Delete]をクリックします。既存のイベント設定に適用されているメディア設定は削除することができません。
サーバー設定を削除できるのは、既存のイベント設定に適用されていない場合のみです。

Customized Script

この機能を使うと、サンプルスクリプト(.xmlファイル)をカメラにアップロードして、たとえば設定の手間を省くことができます。アップロードできるカスタマイズスクリプトの数には制限がありますので注意してください。カスタマイズスクリプトの件数が上限に達した場合は、警告メッセージが表示されます。

詳しくは、VIVOTEKテクニカルサポートにお問い合わせください。



Applications > Motion detection

ここでは、ネットワークカメラでモーション検知ができるように設定する方法を説明します。モーション検知のウィンドウは全部で5つ設定できます。



モーション検知検知設定 1:
通常の場合

以下の手順でモーション検知を有効にしてください。

1. 「New」をクリックして、新しいモーション検知ウィンドウを追加します。
2. Window Nameのテキストボックスにモーション検知ウィンドウの名前を入力します。

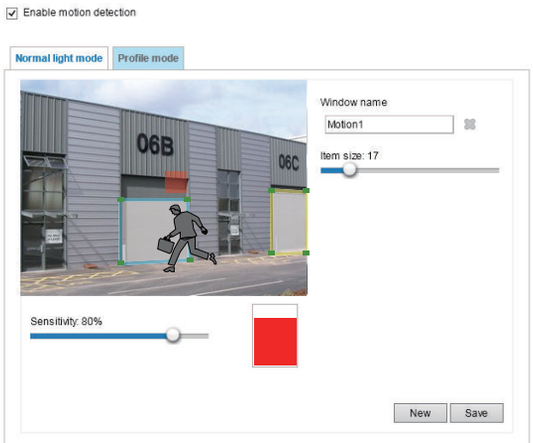
■ マウスを4回クリックして検出ウィンドウを指定します。コーナーマークをお好みの位置にドラッグすることで、ウィンドウの形状を変更することができます。

■ アイテムサイズタブをドラッグして、アラームを作動させるアイテムの最小サイズを変更します。画面中央にアイテムサイズの枠が表示されます（半透明の赤）。侵入してきた物体がアイテムサイズよりも大きいと、アラームが作動します。ライブビューに合わせて、アイテムサイズを変更してください。

■ ウィンドウを削除するには、ウィンドウ名の右にあるXマークをクリックします。

3. 感度のスライドバーを動かして、動く物体に対する感度を設定します。感度を高くすると、光の急激な変化（デイナイトモードの切り替え、照明のオン・オフなど）で誤報が発生しやすくなるので注意が必要です。動きが検出されるためには、動きが0.3秒以上継続する必要があります。
4. 「Save」をクリックすると、設定が有効になります。
5. この機能を有効にするには、「Enable motion detection」を選択します。

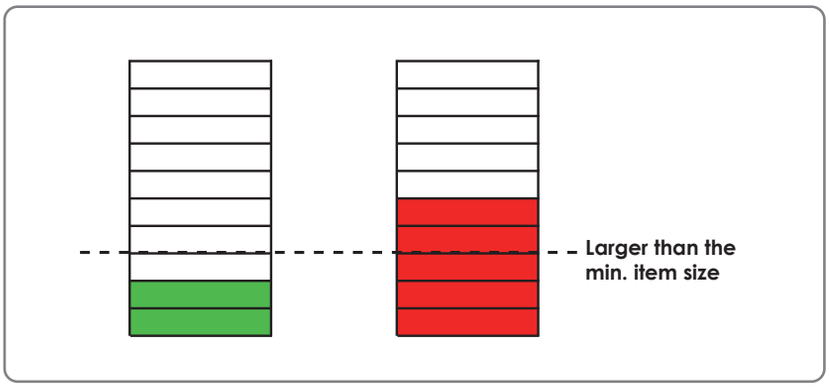
例えば、以下のようになります。



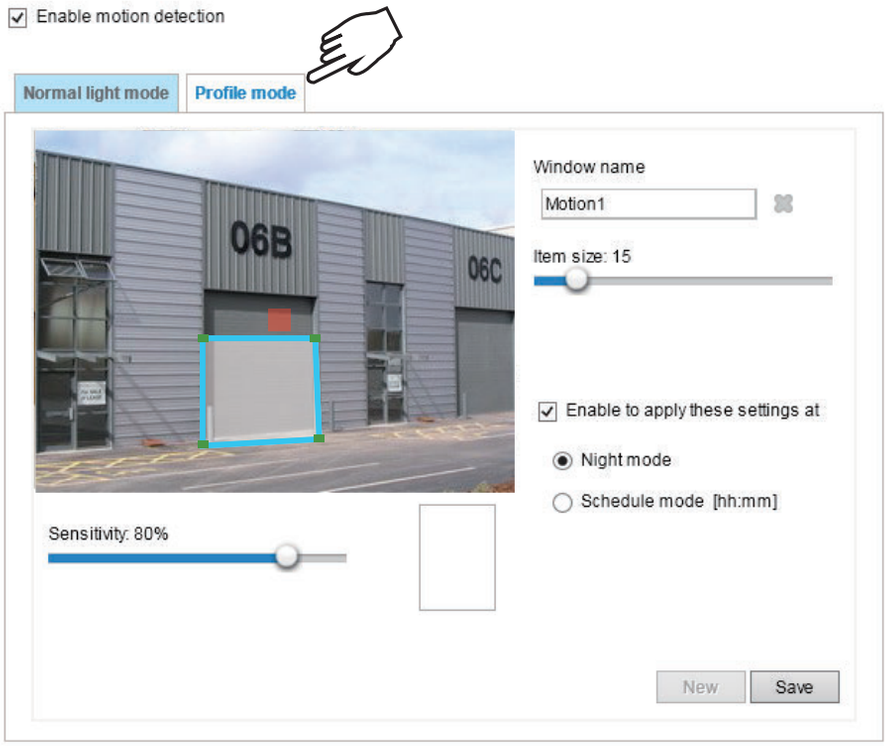
パーセンテージ表示は、連続した画像の変化に応じて上下します。ネットワークカメラで動きが検出され、あらかじめ設定された閾値を超えたと判断されると、赤いバーが上昇します。また、モーション検知ウィンドウは赤で表示されます。

写真やビデオを瞬時に撮影し、リモートサーバー（EメールやFTPサーバー経由）に送信するように設定できます。
イベント設定の詳細については、116ページの「イベント設定」を参照してください。

緑色のバーは、モーションが検出されたにもかかわらず、画像の変動がプリセットされた閾値を下回っているため、
イベントがトリガーされていないことを示しています。



デイ/ナイト/スケジュールモードで他のモーション検知設定を行いたい場合（例：異なる照明条件の場合）は、プロファイルをクリックして、以下のようなモーション検知「Profile」設定ページを開いてください。このページでは、別の3つのモーション検知ウィンドウを設定できます。

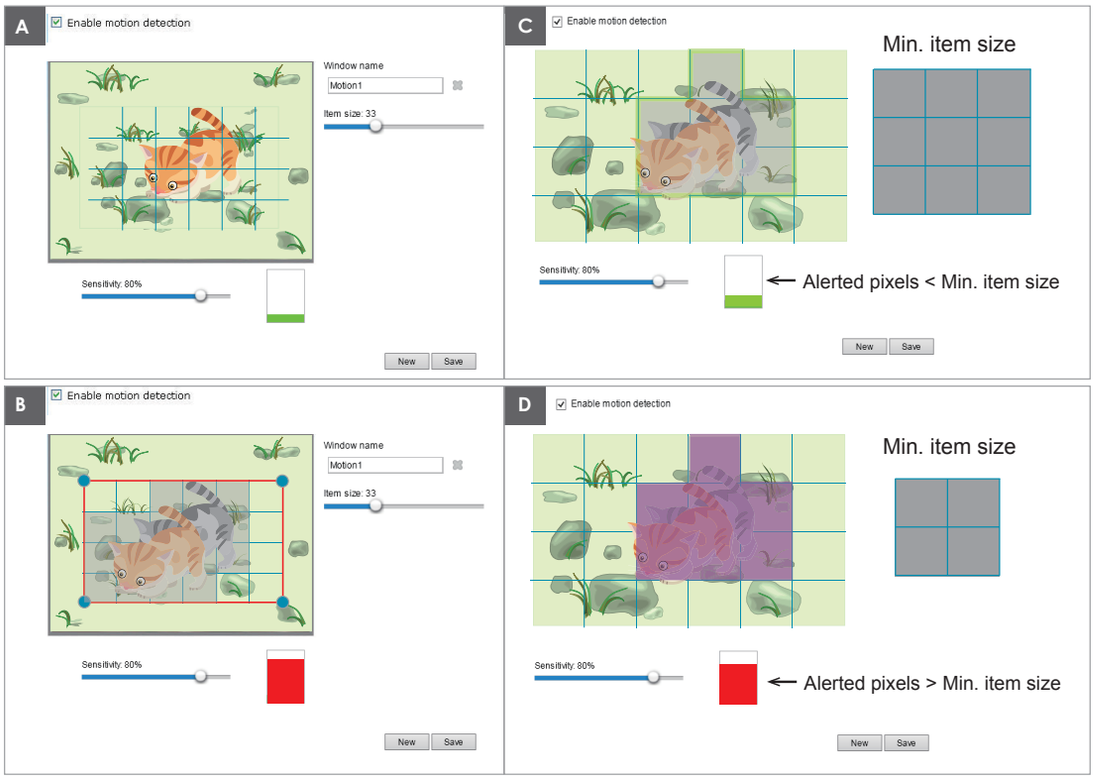


以下の手順でプロファイルを設定してください。
1. 新しいモーションディテクションウィンドウを作成します。
2. 「Profi le mode」タブをクリックします。
3. 該当するスケジュールモードを選択します。時間範囲を手動で入力してください。
4. 「Save」をクリックして設定を有効にし、「Close」をクリックしてページを終了します。

このモーションディテクションウィンドウは、「イベント設定」ページにも表示されます。「イベント」→「イベント設定」→「トリガー」で、トリガーソースとして選択することができます。詳細は126ページをご参照ください。

ノート：

▶動体検知の仕組み：



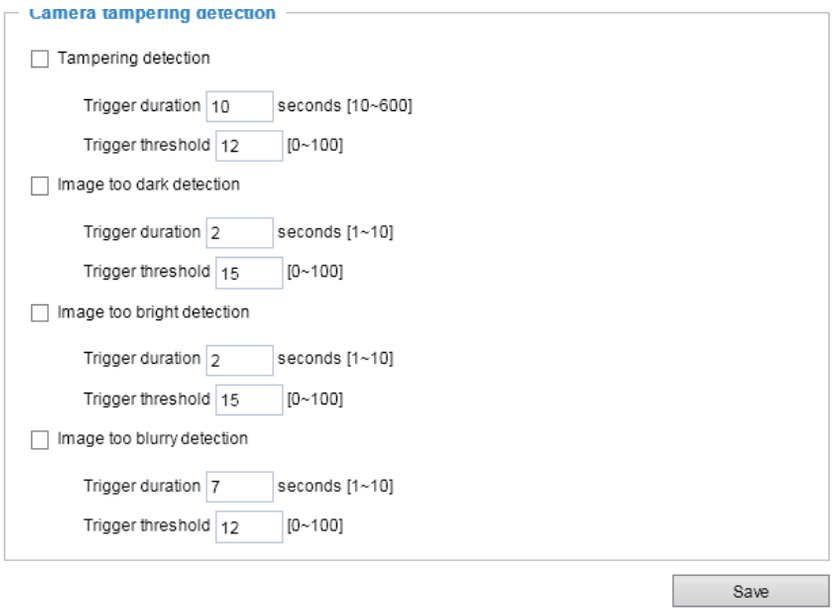
モーション検知のパラメータは 2 つあります。「感度」と「最小値」です。Item Size です。上の図のように、フレーム A とフレーム B は 2 つの連続した画像です。2 つのフレーム間のピクセル差が検出され、感度設定が有効になるグレーで強調表示されます。感度とは、動体に対する感度を表す値です。感度を高く設定すると、カメラはわずかな動きを検出できますが、感度を低く設定すると、動きが無視されます。

最小アイテムサイズは、イベントのトリガーとなる「警告ピクセル」の数を決定するしきい値です。侵入してきた物体のサイズが最小アイテムサイズよりも大きく、その動きが 0.3 秒継続すると、動きが定義された閾値を超えたと判断され、モーションウィンドウが赤の輪郭で表示されます。最小アイテムサイズが大きい場合、フレーム C の移動物体のサイズは最小アイテムサイズよりも小さいとみなされ、モーションアラームはトリガーされません。最小アイテムサイズが小さい場合は、フレーム D の同じ移動物体がアラームを作動させます。

高度なセキュリティ管理を必要とするアプリケーションでは、より高い感度設定を使用することが推奨されます。しかし、感度レベルを高くすると、昼間モードと夜間モードの切り替え、AE スイッチ、照明のオン / オフなどの際の速い光の変化により、誤報が発生する可能性もあります。

Applications > Tampering detection

この項目では、カメラのタンパー検知の設定方法について説明します。本カメラシリーズはタンパー検知機能を備えており、レンズの向きを変える行為、レンズの前に障害物を置く行為、レンズのフォーカスをずらす行為、スプレー塗料を吹き付ける行為などの妨害行為を検出することができます。



次の手順でカメラのタンパー検知機能を設定します。

1. 設定したい条件を[Tampering detection]、[Image too dark]、[Image too bright]、[Image too blurry]の中から選択してチェックボックスをクリックします。チェックした条件のいたずら検出時間を10秒～10分の間で入力します。この設定時間は、いたずらが実際のアラームと見なされるまでの時間を指定します。これにより、一時的な変更でアラームが発生することを回避することができます。

   タンパー検知は、画像の変化要素(現在のフレーム画像と保存済みの画像の違い)がしきい値を超えた場合にのみトリガされます。画像が暗すぎる、明るすぎる、ぼやけすぎる(ピントがぼけている) などの条件もタンパー検知の条件として設定できます。トリガスレッショルドはタンパー検知の条件となるため、この値を小さくすると、トリガは出やすくなります。

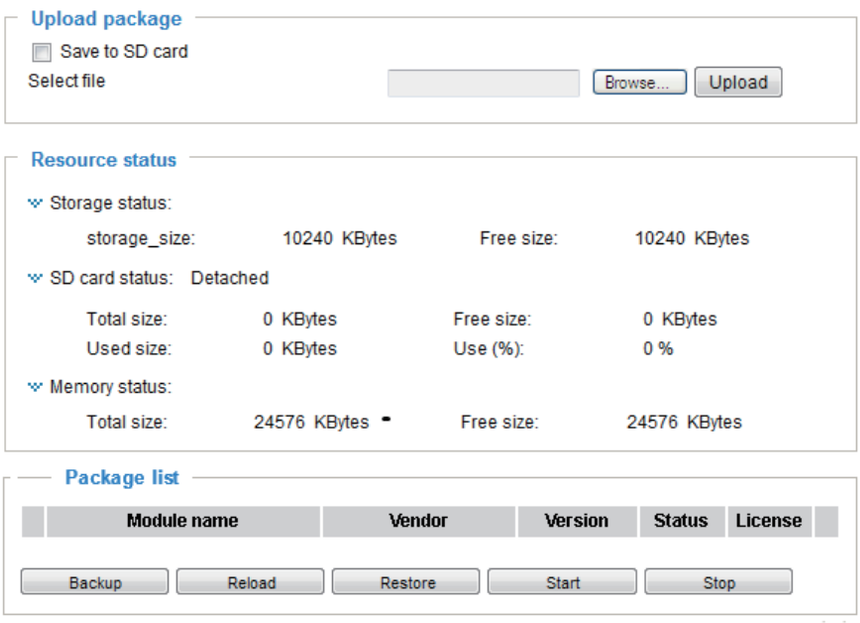
   Too bright: フラッシュライトが光るシーンなどは避け、シーンの平均的な明るさの値が考慮されます。
   Too dark: カメラが覆われたり、ペンキを吹き付けられたときが想定されます。
   Too blurry: 強烈な電波による干渉など、外部からの強い干渉による映像の障害が想定されます。

2. [Event] > Event settings] > [Trigger]では、タンパー検知もトリガの要素としてイベントに設定することができます。たとえば、カメラにいたずらが加えられた場合、イベント前およびイベント後のビデオクリップをネットワーク接続されたストレージデバイスに送信するようにカメラを設定することができます。詳しくはP118をご参照ください。

Applications > Package management - a.k.a., VADP (VIVOTEK Application Development Platform)

カメラによっては、スマートモーション検知機能が提供されます。人の検出と調整可能な時間フィルタを備えたスマートモーション検知は、従来のモーション検出の欠点をカバーし、監視現場での設定をより容易にすることができます。
詳しくは下記URLにある『ユーザーズガイド』を参照してください。

http://download.vivotek.com/downloadfile/solutions/vadp/smart-motion-detection-manual_en.pdf



カメラのフラッシュメモリやSDカードにVIVOTEKやサードパーティ製のソフトウェアモジュールを保存して実行することができます。これらのソフトウェアモジュールは、ナンバープレート認識、オブジェクトカウントなど、インテリジェントなビデオアプリケーションの映像分析に活用することができます。

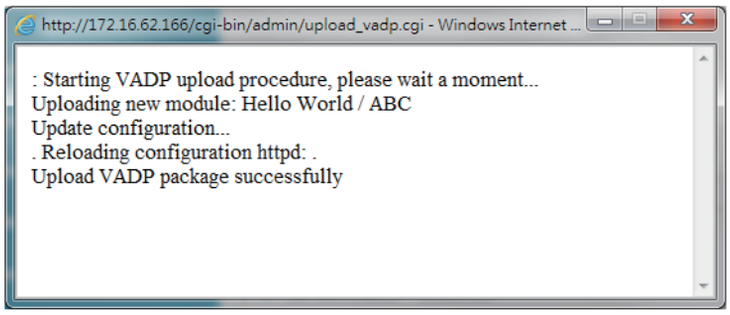
- ソフトウェアパッケージが正常にアップロードされると、モジュール構成(vadp.xml)情報が表示されます。また、モジュールをアップロードすると、カメラはモジュールがVADP要件に適合するかどうかを検査します。含まれているパラメータについては、テクニカルサポートまたはサードパーティ製モジュールのベンダーにお問い合わせください。

- ファームウェア全体を置き換える代わりに、VIVOTEKのVADPパッケージを実行して、更新された機能を利用することもできます。

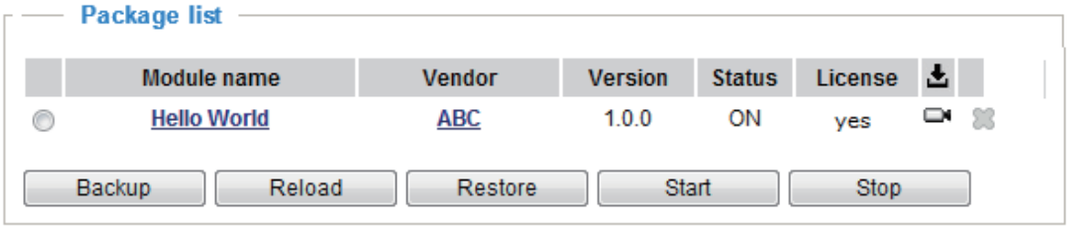
- 一部の製品ではフラッシュの容量が小さいためVADPパッケージを保存できない場合があります。これらの製品は[Save to SD card]ボックスが常に選択され、グレー表示されます。

- SDカード(FAT32)のファイルシステムはソフト(シンボリック)リンクをサポートしていません。モジュールがSDカードにソフトリンクを作成することはできません。

ソフトウェアモジュールを利用するには、ソフトウェアパッケージを取得し、[Browse]と[Upload]をクリックします。アップロードが成功すると、下図のメッセージが表示されます。



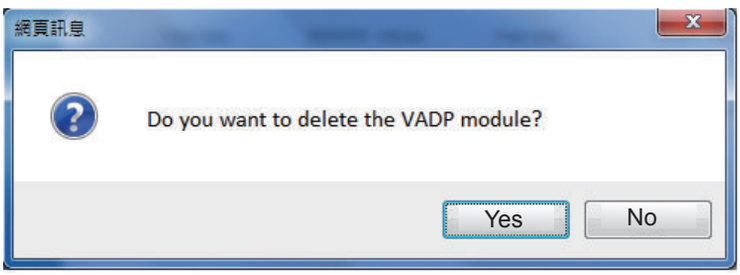
モジュールを開始するには、開始するモジュールをラジオボタンで選択し、[Start]をクリックします。



モジュールを削除する必要がある場合は、削除したいモジュールをラジオボタンで選択し、[Stop] をクリックします。モジュールステータスは [OFF] になり、行の最後に [X] ボタンが表示されますので、この [X] ボタンをクリックしてモジュールを削除します。

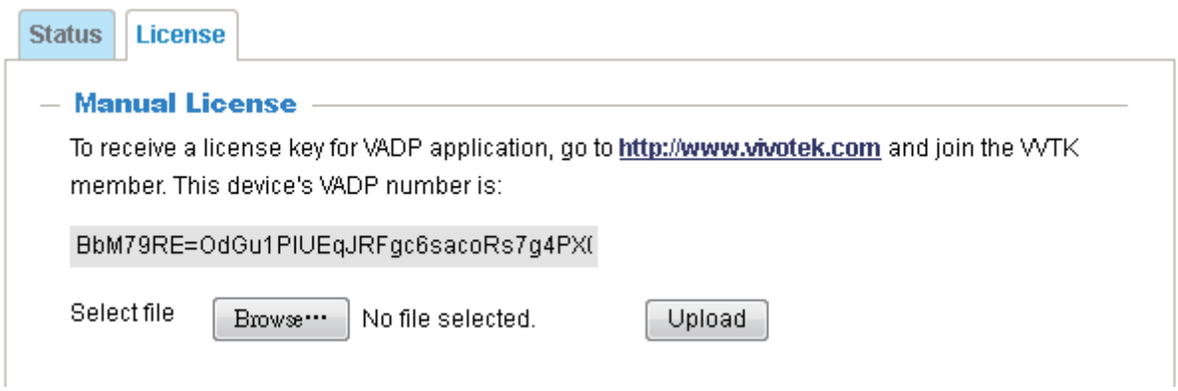


確認メッセージが表示されたら[Yes]をクリックして続行します。



モジュールの動作中に消費される実際のメモリは、メモリステータスフィールドに表示されます。これは、実行中のモジュールがシステムリソースを消費しすぎていないかどうかを判断するのに役立ちます。

[license]ページで、VIVOTEKのVADPモジュールを使用するためのライセンスの登録とアクティベーションを行います。ライセンスキーは別に取得し、手動でネットワークカメラにアップロードする必要があります。登録方法はVIVOTEKのホームページをご確認ください。



Recording > Recording settings

この項目では、ネットワークカメラの録画設定を行う方法について説明します。

Recording Settings

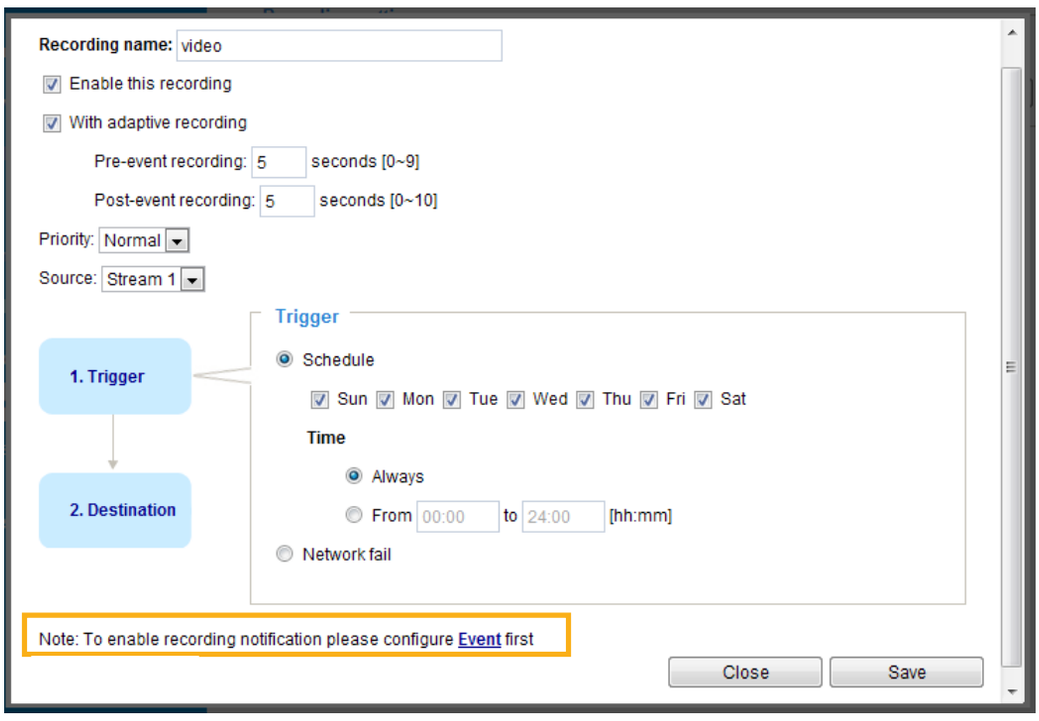


ノート：

► SDカードを初めて使用するときは、カメラのWebコンソールを使用してSDカードを必ずフォーマットしてください。詳しくはP142を参照ください。

Recording Settings

[Add]をクリックして[Recording Settings]ウインドウを開きます。ここでは、アダプティブ録画、録画ソース、スケジュール、容量の定義を2つまで設定することができます。

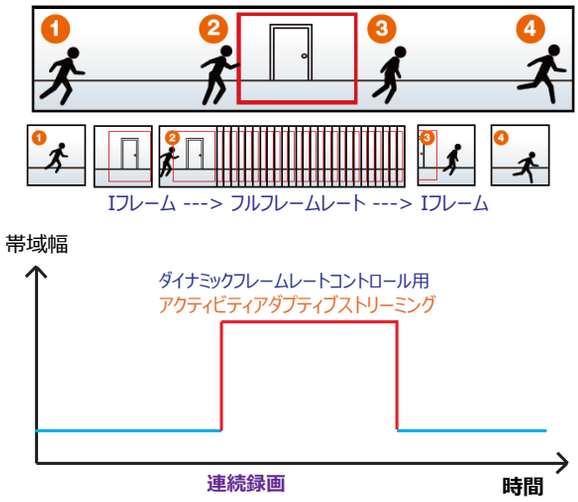


■ Recording name: 録画設定する名前を入力します。

■ Enable this recording: 選択すると、映像録画を有効にすることができます。

■ With adaptive recording:
このオプションを選択すると、イベントトリガによるフレームレート制御を有効にすることができます。
トリガされたイベントが発生すると、フレームレートは[Stream settings]での設定値まで上がります。
詳しくはP72を参照ください。

アダプティブ録画を有効にした場合、カメラAでイベントがトリガされたときにのみ、サーバはフルフレームレートのストリーミングデータを記録します。それ以外の場合、サーバは通常の監視中Iフレームデータのみを要求するため、帯域幅とストレージスペースを効果的に節約することができます



ノート：

- ▶ アダプティブ録画を有効にするには、モーション検知、DI入力、手動トリガなどのトリガソースを必ず設定してください。
- ▶ アラームイベントトリガがない場合：
  - JPEGモード：1秒間に1フレームを記録します。
  - H.264/H.265モード：Iフレームのみを記録します。
- ▶ [Video settings]のIフレーム期間が >1s ので、アダプティブ録画が有効になっていると、カメラはIフレーム期間を強制的に1sに変更します。

イベントトリガはモーション検知や、DI入力などです。詳しくはP121[Event settings]を参照してください。

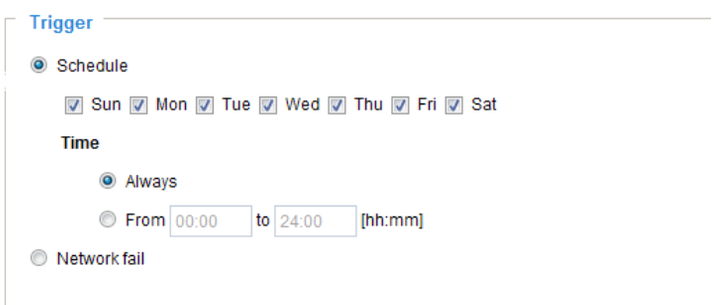
- ■ Pre-event recording and post-event recording
  ネットワークカメラには画像データを一時的に保持するバッファがあります。このオプションを選択しトリガがアクティブになる前と後の記録時間を指定すると、イベントが発生した際に指定した時間だけに撮影された画像を保存することができます。
- ■ Priority: 録画の相対的な重要度を[High]、[Normal]、[Low]の中から選択することができます。優先順位の高い録画が先に実行されます。
- ■ Source: 録画ソースとしてビデオストリームの種類を選択することができます。

ノート：

- ▶ 録画通知を有効にするには、最初にイベントを設定してください。詳しくはP117をご参照ください。

次の手順で録画の詳細を設定します。

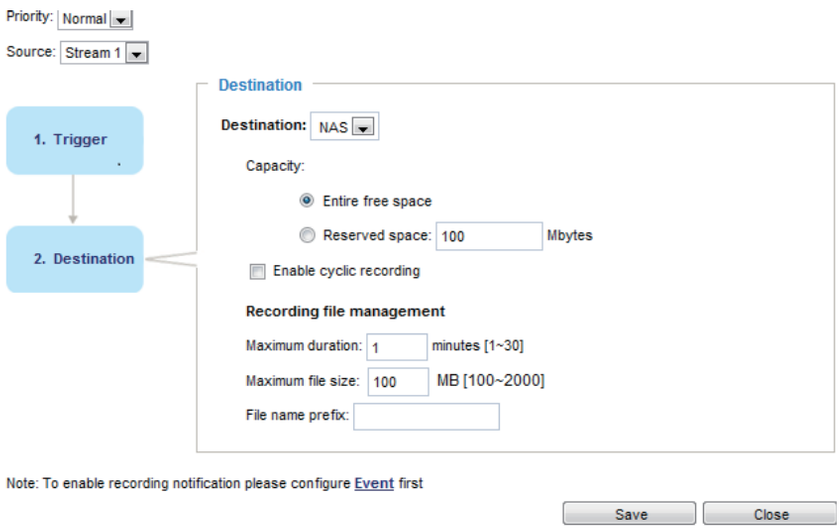
1. Trigger
トリガソースを選択します。



- ■ Schedule: トリガ発生のスケジュールを曜日と時間で設定することができます。サーバはローカルストレージ(SDカード)またはネットワークストレージ(NAS)へのファイルの記録を開始します。
- ■ Network fail: ネットワークの障害発生をトリガに設定することができます。サーバはローカルストレージ(SDカード)にファイルを記録し始めます。

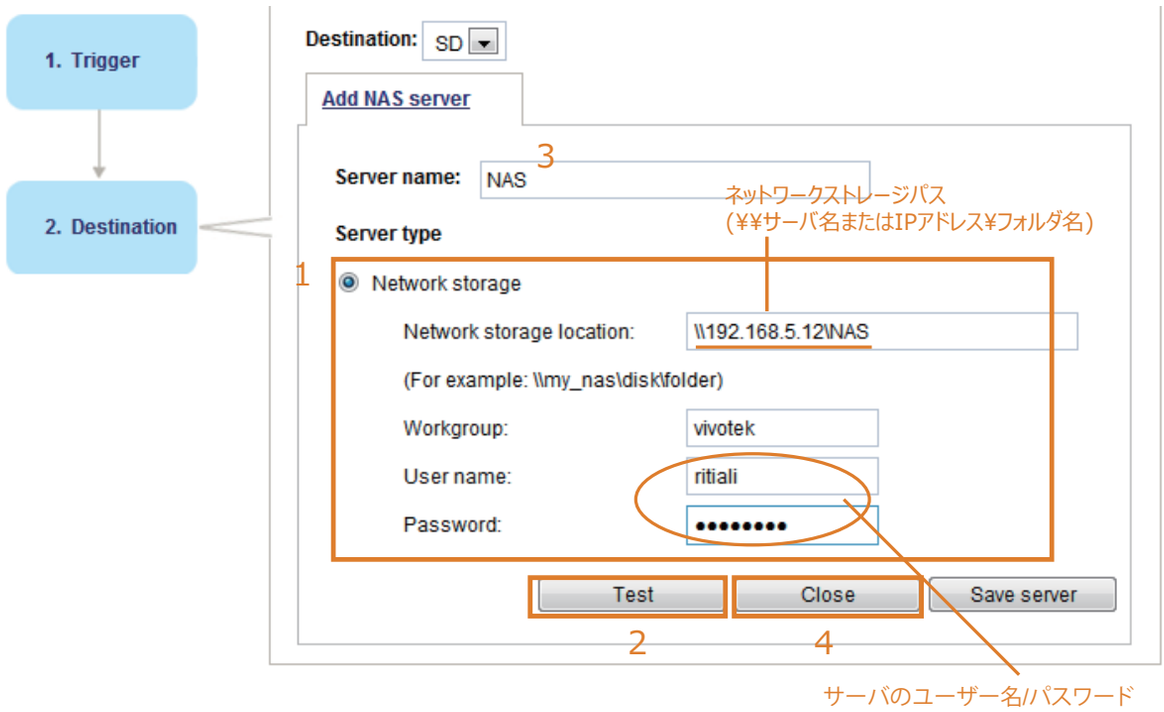
2. Destination

NASサーバーの設定の詳細は、次の項目を参照してください。

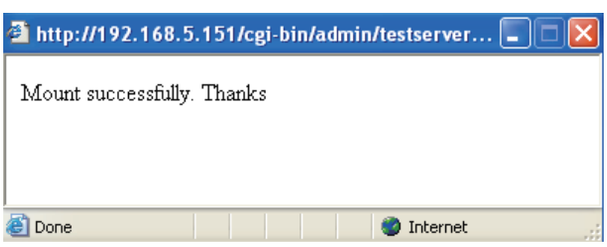


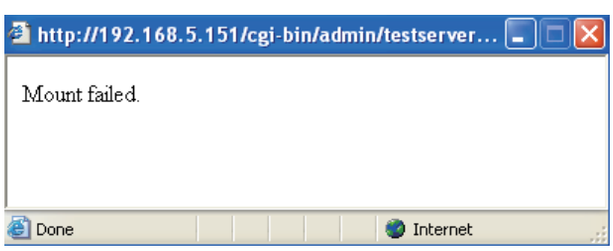
NAS server

[Add NAS server]をクリックして[server settings]ウインドウを開き、次の手順に従って設定します。
1. サーバの情報を入力します。
例：

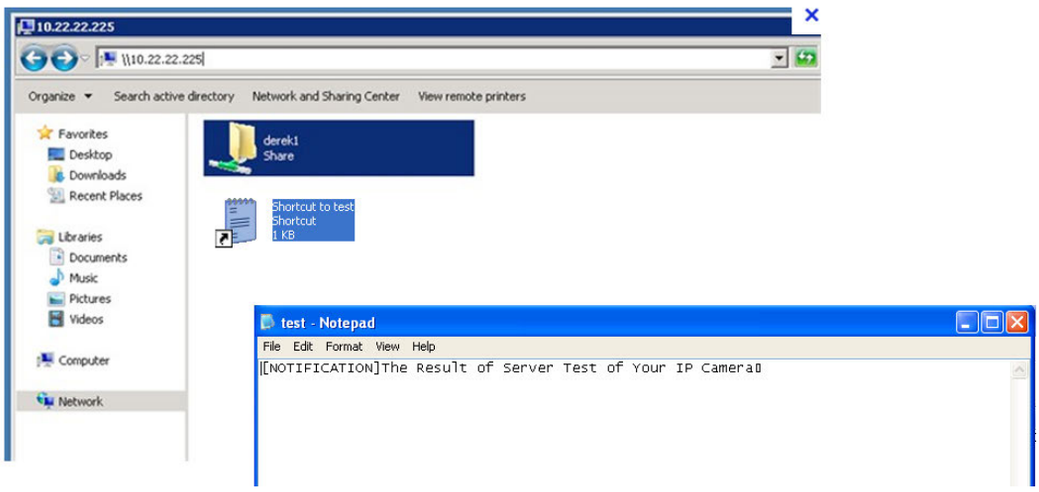


2. [Test]をクリックして設定を確認します。結果はポップアップウインドウに表示されます。

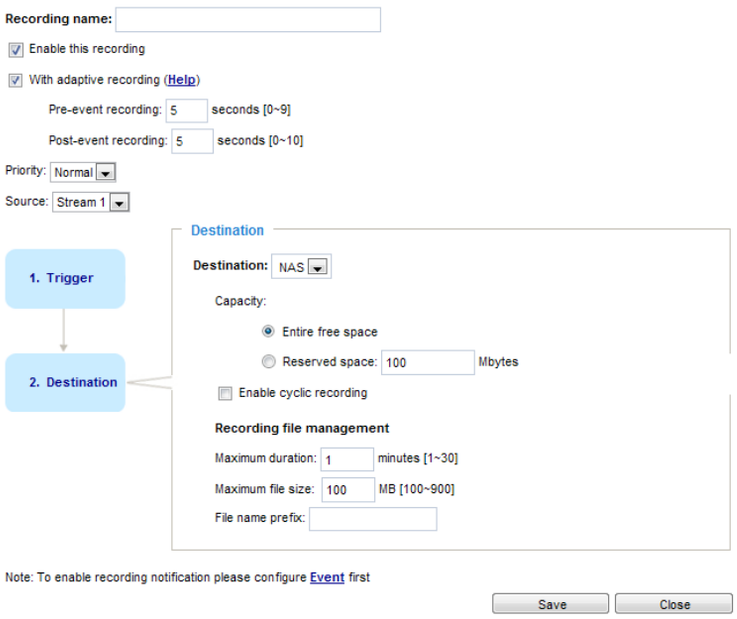




設定が完了すると、ネットワークストレージサーバ上にtest.txtファイルが作成されます。



3. サーバ名を入力します。
4. [Save]をクリックして設定を完了し、 [Close]でページを終了します。



- Capacity: 保存に使用できる領域として、空き領域全体を選択するか、予約済み領域を制限することができます。録画領域の上限は、サイクル録画で使用される領域よりも大きい必要があります。予約済み領域とは、容量が使い切られるかリサイクルされるときにトランザクション処理で使用する少量の領域のことです。

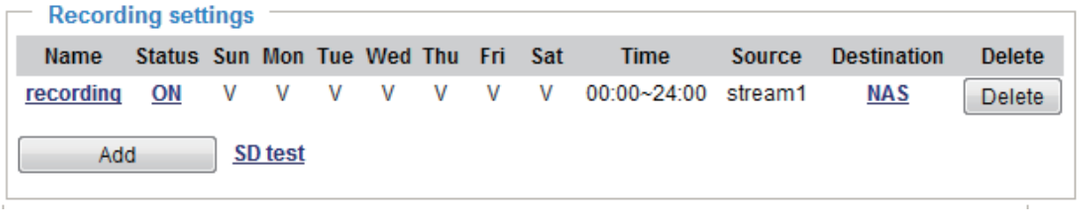
- Enable cyclic recording: この項目を選択すると、録画ファイルが最大容量に達したときに、最も古いファイルから順に上書きして録画することができます。予約済み領域は、ストレージスペースが満杯になり、新しいデータを処理するトランザクション用に確保されます。予約済み領域は15MB以上必要です。

- Recording file management: 各録画ファイルに最大録画時間と最大ファイルサイズを手動で割り当てることができます。必要に応じて、個々のファイルをつなぎ合わせる事も可能です。テキストフィールドに入力して、ファイル名の接頭辞を指定することもできます。

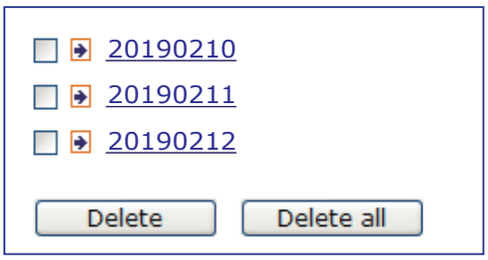
- File name prefix: ファイル名の前に追加するテキストを入力します。

録画通知を有効にするには、[Event]をクリックしてイベントトリガを設定してください。
詳しくはP116[Event] > [Event settings]を参照してください。
設定が終わったら、[Enable this recording]を選択します。[Save]をクリックして設定を有効にし、[Close]でページを終了します。システムは録画を開始すると、録画ファイルをネットワークストレージに送信し、下図のように、録画設定ページのドロップダウンリストに新しい録画が表示されます。

リストから録画設定を削除するには、リストから削除する録画名を選択し、[Delete]をクリックします。



- Click recording (Name): 変更する[Recording Settings] ページが開きます。
- Click ON (Status): ステータスが[OFF]になり、録画が停止します。
- Click NAS (Destination): 下図の録画のファイルリストを開きます。フォルダ名のルールについてはP123を参照ください。



Local storage > SD card management

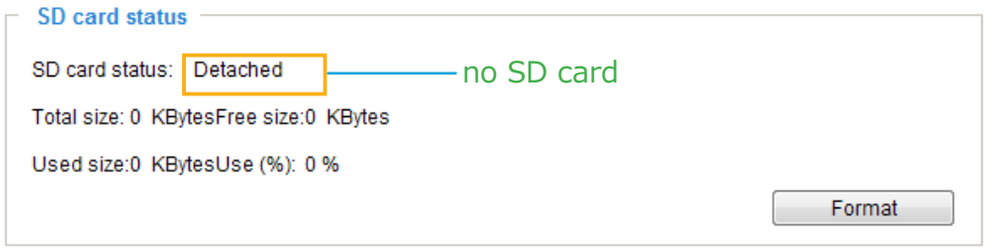
ノート：

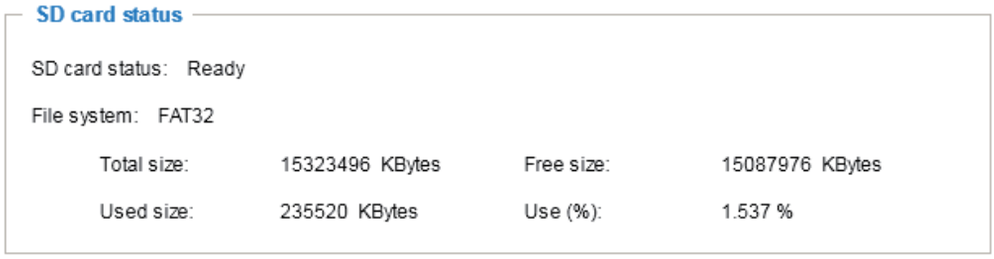
- SD カードをカメラから取り外す前に、録画をオフにしてください。
- SD カードの耐用年数には限りがあります。カードは定期的に新しいものに交換してください。
- カメラのファイルシステムは SD カードの数 MB の領域を専有します。SD カードのすべてのスペースを録画に使用することはできません。
- 他の機器で記録されたデータの入った SD カードは使用しないでください。
- SD カード内のフォルダ名は変更しないでください。カメラの誤動作の原因となります。

この項目では、ネットワークカメラのローカルストレージを管理する方法について説明します。SD カードの状態を表示したり、SD カードの制御を行うことができます。

SD card staus

SD カードのステータスと予約済み領域を表示することができます。初めて SD カードを使用するときは、必ずフォーマットしてください。



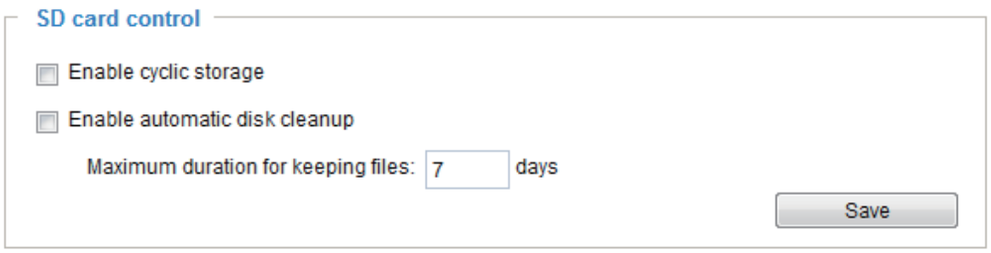


SD card format

EXT4 ファイルは Linux のファイルシステムで、32GB 以上の SD カードに適用可能ですが、Windows のコンピュータでは SD カードの内容に直接アクセスできません。この場合は Windows でサードパーティ製のソフトウェアを使用してください。



SD card control



- この項目をチェックすると、サイクル録画を有効にすることができます。最大容量に達すると、最も古いファイルが最新のファイルで上書きされます。
- Enable automatic disk cleanup: この項目をチェックすると、SDカードに録画ファイルを保存する日数を設定することができます。例えば[7日]と入力すると、録画ファイルはSDカードに7日間保存されます。

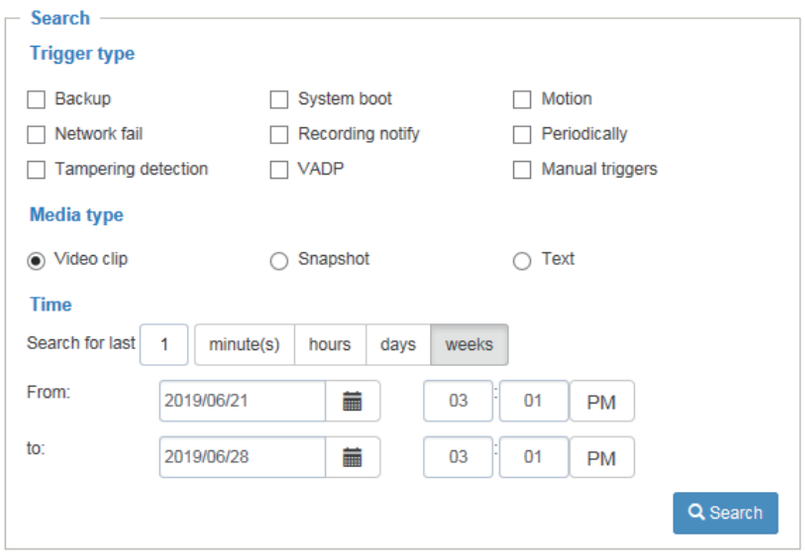
[Save] をクリックして設定を有効にします。SD カードの最小予約済み領域 (トランザクション処理用) の容量は 512 MB、ネットワーク共有の場合は 1GB です。

Local storage > Content management

この項目では、ネットワークカメラで SD カードに録画した画像を管理する方法について説明します。記録済み画像の検索と検索結果の表示、画像の再生とダウンロードをすることができます。

Searching and Viewing the Records

この項目では保存されたファイルの検索条件を設定することができます。選択肢を選ばずに[Search]ボタンをクリックすると、録画されたすべてのファイルからの検索結果が[Search Results]に表示されます。

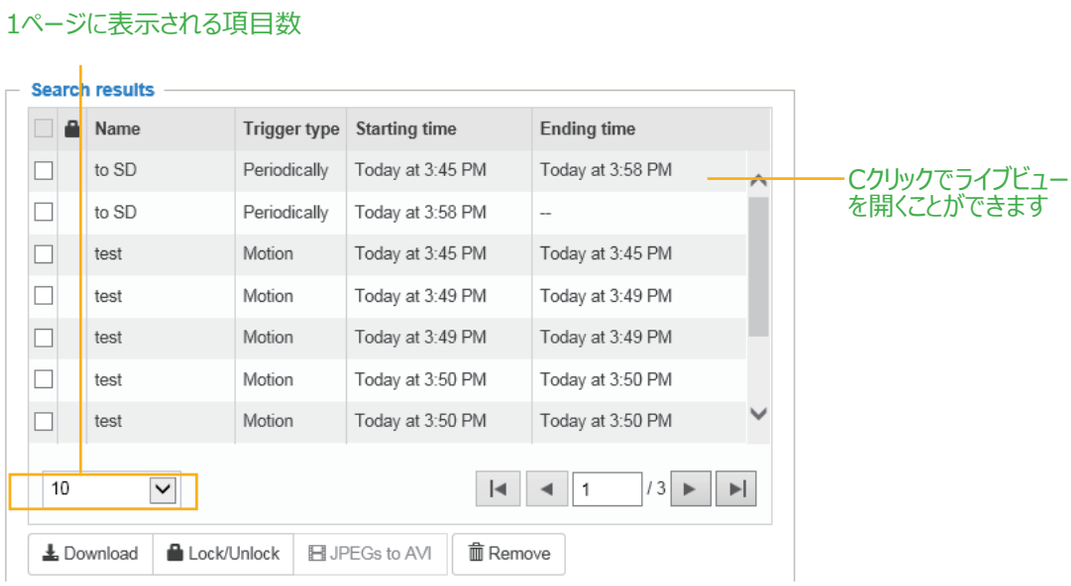


- File attributes: 検索内容として1つ以上の項目を選択します。
- Trigger time: 特定の時間に作成されたファイルの中から検索する場合、時間範囲を手動で入力します。

[Search]をクリックすると、対応する録画ファイルが[Search Results]ウインドウに一覧表示されます。

Search Results

下図は検索結果の例になります。結果の一覧では[Name]、[Trigger type]、[Trigger time]、[Locked]の4つをみることができます。 ⇳ をクリックすると、優先の項目順に検索結果を並べ替えることができます。



■ Play: 検索結果の動画ファイルをすぐに確認することができます。一覧の中からファイルを選択し、検索結果をクリックします。再生ウインドウが上部に表示されます。

例：

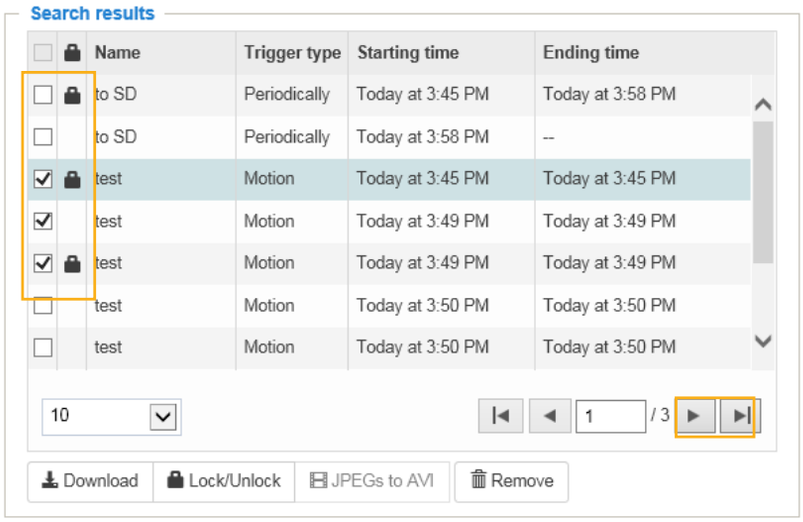


■ Download: 検索結果のファイルをダウンロードすることができます。一覧の中からダウンロードしたい項目を選択し、[Download]ボタンをクリックすると、ファイルのダウンロードウインドウが表示され、ファイルを保存することができます。

■ JPEGs to AVI: 検索結果の一覧の中からスナップショットなど[JPEG]形式のファイルを選択し、ボタンをクリックすると、AVIファイルに変換することができます。

■ Lock/Unlock: 録画ファイルを誤って消去しないようロックをかけることができます。検索結果一覧のチェックボックスでロックしたいファイルを選択し、ボタンをクリックします。チェックした項目は[Locked]になり、サイクル録画中に削除されることはありません。再度ボタンをクリックすると、ロックを解除することができます。

例：



クリックしてページを
切り替えます

■ Remove: 録画ファイルを削除することができます。検索結果一覧の中から削除したいファイルを選択し、ボタンをクリックします。

Appendix

URL Commands for the Network Camera

1. Overview

すでに独自のウェブサイトやウェブコントロールアプリケーションをお持ちのお客様の中には、URL 構文：を使ってネットワークカメラ／ビデオサーバを簡単に統合できる方もいらっしゃると思います。ここでは、HTTP ベースの外部アプリケーション・プログラミング・インターフェースについて説明します。HTTP ベースのカメラインターフェースでは、1 枚の画像の要求、カメラ機能の制御（PTZ、出力リレーなど）、内部パラメータ値の取得および設定などの機能が提供されています。画像や CGI のリクエストは、内蔵の Web サーバーで処理されます。

2. Style Convention

URL 構文：や CGI パラメータの説明では、角括弧内のテキストは、値または文字列に置き換えられるコンテンツを示します。文字列を置き換える際には、角括弧も置き換える必要があります。例えば、以下の URL 構文：の説明で <servername> と表記されているサーバー名の記述が、このページの下の方にある URL 構文：の例では myserver という文字列に置き換えられています。

URL 構文：は、太字で書かれた「Syntax：」という単語と、それに続く以下に示すように参照される語法：のボックスで示されます。 たとえば、サーバーの名前は <servername> と記述されており、実際のサーバーの名前に置き換えることを目的としています。名前には、「mywebcam」や「thecam.adomain.net」などの名前、または 192.168.0.220 などのサーバーの関連 IP アドレスを指定できます。

構文：

```
http://<servername>/cgi-bin/viewer/video.jpg
```

返されたデータの説明は、太字で「Return:」と書かれた後、ボックス内に返されたデータが表示されます。すべてのデータは HTTP フォーマットで返されます。つまり、各行は CRLF（Carriage Return and Line Feed）で区切られ、¥¥ と表示されます。
Return:

```
HTTP/1.0 <HTTP code> <HTTP text>¥r¥n
```

URL 構文の例は、太字で「Example:」と書かれ、その後に短い説明と薄いグレーのボックスで例が示されます。

例：1 枚のスナップショット画像をリクエストします。

```
http://mywebserver/cgi-bin/viewer/video.jpg
```

Technology License Notice

AMR-NB Standard

THIS PRODUCT IS LICENSED UNDER THE AMR-NB STANDARD PATENT LICENSE AGREEMENT. WITH RESPECT TO THE USE OF THIS PRODUCT, THE FOLLOWING LICENSORS' PATENTS MAY APPLY:

TELEFONAKIEBOLAGET ERICSSON AB: US PAT. 6192335; 6275798; 6029125; 6424938; 6058359. NOKIA CORPORATION: US PAT. 5946651; 6199035. VOICEAGE CORPORATION: AT PAT. 0516621; BE PAT. 0516621; CA PAT. 2010830; CH PAT. 0516621; DE PAT. 0516621; DK PAT. 0516621; ES PAT. 0516621; FR PAT. 0516621; GB PAT. 0516621; GR PAT. 0516621; IT PAT. 0516621; LI PAT. 0516621; LU PAT. 0516621; NL PAT. 0516621; SE PAT 0516621; US PAT 5444816; AT PAT. 819303/AT E 198805T1; AU PAT. 697256; BE PAT. 819303; BR PAT. 9604838-7; CA PAT. 2216315; CH PAT. 819303; CN PAT. ZL96193827.7; DE PAT. 819303/DE69611607T2; DK PAT. 819303; ES PAT. 819303; EP PAT. 819303; FR PAT. 819303; GB PAT. 819303; IT PAT. 819303; JP PAT. APP. 8-529817; NL PAT. 819303; SE PAT. 819303; US PAT. 5664053. THE LIST MAY BE UPDATED FROM TIME TO TIME BY LICENSORS AND A CURRENT VERSION OF WHICH IS AVAILABLE ON LICENSOR'S WEBSITE AT HTTP://WWW.VOICEAGE.COM.

HEVCAdvance™
Covered by Patents at patentlist.hevcadvance.com

Notices from HEVC Advance:

THIS PRODUCT IS SOLD WITH A LIMITED LICENSE AND IS AUTHORIZED TO BE USED ONLY IN CONNECTION WITH HEVC CONTENT THAT MEETS EACH OF THE THREE FOLLOWING QUALIFICATIONS: (1) HEVC CONTENT ONLY FOR PERSONAL USE; (2) HEVC CONTENT THAT IS NOT OFFERED FOR SALE; AND (3) HEVC CONTENT THAT IS CREATED BY THE OWNER OF THE PRODUCT. THIS PRODUCT MAY NOT BE USED IN CONNECTION WITH HEVC ENCODED CONTENT CREATED BY A THIRD PARTY, WHICH THE USER HAS ORDERED OR PURCHASED FROM A THIRD PARTY, UNLESS THE USER IS SEPARATELY GRANTED RIGHTS TO USE THE PRODUCT WITH SUCH CONTENT BY A LICENSED SELLER OF THE CONTENT. YOUR USE OF THIS PRODUCT IN CONNECTION WITH HEVC ENCODED CONTENT IS DEEMED ACCEPTANCE OF THE LIMITED AUTHORITY TO USE AS NOTED ABOVE.

H.264

THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM

Electromagnetic Compatibility (EMC)

VCCI 規制について

この装置は、クラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。取扱説明書に従って正しい取扱いをして下さい。 VCCI-B

責任

① 本書の内容は、将来予告なしに変更する場合があります。

② 本書の内容について万全を期して作成いたしましたが、万が一ご不審な点や誤り、記載もれなどお気づきの点がございましたら、お買い求めの販売店にご連絡ください。

③ 製品を運用した結果の影響については②項にかかわらず責任を負いかねますのでご了承ください。

製品の譲渡または売却時のご注意

この製品を第三者に譲渡または売却する場合は、この製品に添付されているすべてのものを譲渡または売却してください。