

**Honeywell**

# Honeywell 35 シリーズ

## IP カメラ

HC35W43R3

HC35W43R2

HC35WB3R3

HC35WB3R2

HC35WE3R3

HC35WE3R2

HC35W45R3

HC35W45R2

HC35WB5R3

HC35WB5R2

HC35WE5R3

HC35WE5R2

HC35W25R3

HC35W48R3

HC35W48R2

HC35WB8R3

HC35WB8R2

HC35WE8R3

HC35WE8R2

HC35WZ2R25

HC35WZ5R30

---

# ユーザーガイド

---

# 推奨事項

この文書およびその他の Honeywell の文書の最新バージョンは、当社の Web サイト <https://buildings.honeywell.com/security> でご確認ください。

# 著作権

© 2022 Honeywell International Inc. All rights reserved. Honeywell の書面による承諾なしに本書の全部または一部を転載することはできません。本書の情報はあらゆる点で正確を期しています。Honeywell は、製品の使用に起因するいかなる結果についても責任を負いません。本書に記載の情報は予告無く変更する場合があります。本書の改訂版や新規作成版には当該の変更を反映するものとします。特許情報については、<https://buildings.honeywell.com/us/en/support/legal/patents> を参照してください。

# 改訂

発行	日付	改訂
A	03/2022	新規文書

# 注意および警告

 <p><b>注意</b> 感電の危険があります 開けないでください。</p>	  <p>このシンボルは、本機器内の電圧には感電の危険性があることを示しています。</p>
<p>注意：感電防止のためカバー（または裏カバー）を取り外さないでください。 内部にはユーザーが修理できる部品はありません。修理は有資格の保守担当者に依頼してください。</p>	 <p>このシンボルは、本機の操作や保守に関する重要事項を示しています。</p>



**警告：** 電気安全規格に準拠するために、地域認定/CSA 認定/UL 規格認定取得済みの LPS またはクラス 2 の電源アダプタが必要です。PoE（パワーオーバーイーサネット）は、IEEE 802.3at の PoE 規格を満たす認定済み情報技術機器によって提供されるものとしします。PoE は、公開されたネットワーク（屋外施設等）に接続することを目的としていません。推奨されるアダプタについては、Honeywell にお問い合わせください。



**注意：** 不可視 LED 照射（850 nm）。光線を見ないでください。

## 規格との適合

### Photobiological safety（フォトバイオロジカルセーフティ）

この製品は、IEC/EN 62471（リスクグループ 1）に準拠した光生物学的安全性の要件を満たしています。

# 一般データ保護規則

この製品には個人データが保存されている場合があります。個人データは、欧州の一般データ保護規則（2016/679）によって保護されているため、個人データの所有者は、この規則により一定の権利を取得しています。

これらの所有者（「データ主体」）の権利、およびこのデータの使用および配布に関して従う必要がある制限事項について十分に理解しておくことを強くお勧めします。

詳細については、EU の GDPR Web サイトを参照してください

# FCC 遵守声明

**使用者のための情報：**本装置は、FCC 規格 Part 15 に基づくクラス A デジタルデバイスの制限に準拠していることが試験で確認されています。これらの規格は、住宅地での有害な電波干渉を防止するためのものです。

本装置は無線周波エネルギーを発生および使用し、場合によっては放射する可能性があります。正しく設置・使用しないと無線通信に干渉する可能性があります。ただし、設置状況によっては干渉が全く起きないという保証はありません。本装置によりラジオやテレビの受信障害が発生した場合（本装置の電源オン/オフで判断できます）、干渉防止のため、以下の対策を試してください。

- 受信アンテナの向きや設置場所を変更する。
- 本装置と受信機との距離を離す。
- 受信機が接続している回路とは別の回路のコンセントに本装置を接続する。
- 取扱店またはテレビやラジオの技術者に問い合わせる。法規遵守の責任当事者による承認のない変更や改造を行うと、本製品を使用する権利を剥奪される場合があります。このクラス A デジタルデバイスはカナダの ICES-003 に準拠しています。

**注記：** 法規制遵守の責任者が明示的に承認していない変更や改造を加えた場合は、本装置を使用する権利を剥奪されることがあります。

# メーカーの適合宣言

## 北米

このガイドが付属する装置は、UL 62368-1 および CSA C22.2 No. 62368-1 に準拠しています。

## 欧州

本メーカーは、このガイドが付属する本製品が、RoHS 3 (2015/863) による改訂の電気・電子機器における特定有害物質の使用制限に関する欧州議会・理事会指令 (2011/65/EU) に準拠し、EMC 指令の必須要求事項 (2014/30/EU)、排出ガスについては EN 55032 規格、イミュニティについては EN 50130-4、電気機器の安全性については EN 62368 の要件に適合していることを宣言します。

# 廃電気・電子機器指令 (WEEE)



本製品の正しい処分 (個別の回収システムを適用している EU と他のヨーロッパ諸国にも該当)

この製品は、耐用年数終了後に、該当する地域の法律、規制、手順に従って処分する必要があります。

# 地域の廃棄物ガイドラインの確認

この製品のコンポーネントは、個別の廃棄物収集が必要です。分類ルールについては、地域の廃棄物ガイドラインを確認してください。

# 安全の手引き

ユニットを設置または操作する前に、すべての指示を読んで従ってください。設置後は、後で参照できるように、安全および操作説明書を保管してください。

1. ご注意ください - 本機および取扱説明書に記載されている警告にすべて従ってください。
2. 設置
  - 製造元の指示に従って取り付けてください。
  - すべての現地法規を遵守して保証を維持するために、設置および修理は資格のある経験豊富な技術者のみによって実施してください。
  - 製品を壁または天井に取り付ける場合は、製造元の指示に従い、製造元が承認または推奨する取り付けキットを使用する必要があります。
  - PTZ カメラは、上下逆に設置できません。
3. 電源 - 本製品は、マーキングラベルに記載されている種類の電源からのみ操作してください。お客様の施設に供給されている電力の種類が不明な場合は、製品販売店または地元の電力会社にお問い合わせください。
4. 取り付けシステム - 製造元が推奨する取り付けシステムを使用するか、製品とともに購入した取り付けシステムのみを使用してください。
5. 付属品/アクセサリ - 製品の製造元が推奨しない付属品/アクセサリを使用しないでください。火災、感電、人身傷害の危険があります。
6. 清掃 - 液体洗剤やスプレー洗剤は使用しないでください。清掃には湿った布を使用してください。
7. 修理 - 本機をお客様自身で修理しようとししないでください。修理の際は必ず資格のある保守担当者に依頼してください。

8. 交換部品 - 交換部品が必要な場合は、修理技術者が、製造元が指定した交換部品、または元の部品と同じ特性を持っている交換部品を使用していることを確認してください。許可されていない部品で代用すると、火災、感電、その他の危険をもたらす可能性があります。元の製造元以外で製造された交換部品またはアクセサリを使用すると、保証が無効になることがあります。

## 保証とサービス

製品保証に記載されている条件に従って、保証期間中、Honeywell は、単独裁量により、送料前払いで返品された不良品を無料で修理または交換します。

Honeywell 製品に問題がある場合は、カスタマーサービスまでご連絡（1.800.323.4576）いただき、サポートを依頼するか、**返品保証（RMA）** 番号をリクエストしてください。

テクニカルサービス担当者にご連絡の際は、問題の内容に加えて、モデル番号、シリアル番号を必ずご確認ください。

すべての返品、交換、または返金については事前の承認が必要です。**明確に識別された返品保証（RMA）** 番号を添付することなく Honeywell に製品を発送すると、拒否される場合があります。

# 目次

<b>1</b>	<b>はじめに.....</b>	<b>1</b>
	概要.....	1
	対応ブラウザ.....	2
	主な機能.....	2
<b>2</b>	<b>カメラへのアクセス.....</b>	<b>4</b>
	Unified Tool のインストール.....	4
	ネットワーク上でのカメラ検出.....	6
	カメラの初期化.....	8
	カメラへの新しい IP アドレスの割り当て.....	9
	IP アドレス設定を構成する.....	10
	DNS サーバーアドレスを構成する.....	10
	カメラのファームウェアのアップグレード.....	10
	Web ブラウザからカメラにアクセスする.....	12
<b>3</b>	<b>ログインとライブビデオの表示.....</b>	<b>13</b>
	Web クライアントからのカメラへのログイン.....	13
	作業を開始する前に.....	13
	カメラへのログイン.....	14
	メインページの使用.....	15
	システムメニュー.....	17
	ストリームプロファイル.....	18

カメラ名.....	18
ライブビューツールバー .....	18
VA イベントリスト.....	19
Language [言語] .....	19
管理者アカウント .....	20
<b>4 カメラ設定の構成.....</b>	<b>21</b>
一般設定の構成.....	21
動画設定の構成.....	21
Mode [モード].....	22
動画ストリーム.....	22
ROI .....	26
オーディオ設定の構成.....	27
画像設定の構成.....	28
画像調整.....	29
シーンモード .....	29
Exposure [露出].....	29
ホワイトバランス (WB) の設定.....	30
デイナイト設定.....	31
ノイズ低減.....	32
画像のエンハンス .....	33
OSD の構成.....	34
プライバシーマスクの設定 .....	34
<b>5 ネットワーク設定の構成.....</b>	<b>36</b>
ネットワークの一般設定の構成.....	36
ストリーミングプロトコルの構成 .....	38
SMTP 設定の構成 .....	41

SNMP 設定の構成 .....	43
QoS 設定の構成.....	45
HTTPS 設定の構成 .....	46
HTTPS.....	46
ファイルのアップロード .....	47
IEEE 802.1x 設定の構成 .....	47
<b>6 ビデオ分析の構成.....</b>	<b>49</b>
モーション検出.....	49
スマートモーション検出.....	50
不正干渉検出 .....	51
侵入検知.....	53
マルチロイタリング .....	54
人数カウンター .....	55
<b>7 アラームとイベントの構成.....</b>	<b>58</b>
アラーム入力とアラーム出力の構成.....	58
アラーム入力.....	59
アラーム出力.....	60
SD カードアラームの構成.....	61
<b>8 ストレージ設定の構成.....</b>	<b>62</b>
SD カード管理.....	62
SD Card Status [SD カードの状態].....	63
SD カードのフォーマット .....	64
コンテンツ管理.....	64
記録の検索と表示 .....	64
検索結果.....	65

録画設定 .....	66
<b>9 システム設定の構成.....</b>	<b>68</b>
システムの一般設定の構成 .....	68
メンテナンス設定の構成.....	69
Upgrading Firmware [ファームウェアのアップグレード] .....	70
カメラの再起動.....	70
Restoring the Camera [カメラの復元] .....	71
ファイルのインポート/エクスポート .....	71
ユーザーアカウント設定の構成.....	74
アカウント管理.....	75
アクセスリスト設定の構成 .....	76
<b>10 PTZ 設定の構成 .....</b>	<b>77</b>
プリセット .....	77
スキャン管理 .....	78
パトロール.....	79
パトロールの録画.....	80
アイドルアクション .....	82
パワーアップアクション.....	83
<b>11 システム情報の表示.....</b>	<b>84</b>
ログ .....	84
操作ログ.....	84
アラームログ .....	85
ログの収集.....	85
バージョン.....	85
<b>12 トラブルシューティング .....</b>	<b>86</b>

一般的な問題のトラブルシューティング ..... 86

**13 付録 .....87**

記号の一覧..... 87



図 1 Unified Tool のインストール	5
図 2 インストールフォルダの選択	5
図 3 インストールの確認	6
図 4 スプラッシュ画面	6
図 5 ネットワークのスキャン	7
図 6 デバイスリスト	7
図 7 初期化の 1 ページ目	8
図 8 初期化の 2 ページ目	9
図 9 IP 割り当て	9
図 10 ファームウェアのアップグレード 1	11
図 11 ファームウェアのアップグレード 2	11
図 12 メインページ	16
図 13 PTZ パネル	17
図 14 ライブビューツールバー	18
図 15 一般設定	21
図 16 モードタブ	22
図 17 ビデオストリーム	23
図 18 ROI 設定	26
図 19 オーディオ設定	27
図 20 画像設定	28
図 21 プライバシーマスク	35
図 22 ネットワークの一般設定	36
図 23 ストリーミングプロトコル-HTTP	38
図 24 ストリーミングプロトコル-RTSP	39
図 25 SMTP 設定	42
図 26 HTTPS 設定	46
図 27 IEEE 802.1x 構成 - EAP-TLS	48
図 28 モーション検出	49
図 29 スマートモーション	51
図 30 不正干渉検出	52
図 31 侵入検知	53
図 32 マルチロイタリング	54
図 33 人数カウンター	56
図 34 アラーム入力とアラーム出力	58
図 35 SD カードなし	63
図 36 SD カードあり	63
図 37 システムの一般設定	68
図 38 プリセット設定	77
図 39 スキャン設定	78
図 40 パトロール設定	79
図 41 パトロールの録画	81
図 42 アイドルアクション	82
図 43 パワーアップアクション	83

# 表

表 1 ライブビューツールバーアイコン.....	19
表 2 カメラ解像度.....	24
表 3 カメラのフレームレート.....	25
表 4 互換性のある SD カード.....	62
表 5 一般的な問題のトラブルシューティング.....	86
表 6 記号の一覧.....	87

# はじめに

この文書では、Honeywell 35 シリーズカメラのアクセス、設定、操作方法について説明します。この文書は、システム設置担当者、管理者、および操作者を対象としています。

## 概要

Honeywell 35 シリーズ IP カメラは、動画データの収集と伝送を組み合わせたネットワークビデオ技術を従来のカメラと統合しています。柔軟性に優れたこれらの高機能カメラは、さまざまな監視アプリケーションに適しています。

このカメラは、最大 60 フレーム/秒で 2 メガピクセルの解像度と最大 30 フレーム/秒で 8 メガピクセルの解像度を実現し、映像圧縮技術を使用して帯域幅とストレージを節約しながら、最高の映像品質を保証します。すべてのカメラは、インテリジェントな IR 機能を備えた True デイナイト機能で、薄暗い照明や夜間での環境下において IPC モデルでは最大 60m、PTZ モデルでは最大 150m の視認可能性を提供します。また、すべてのカメラは最大 120 DB の WDR 機能をサポートしています。各カメラには設定可能なモーション検出とカメラ改ざん検出機能があり、最大 5 つのユーザー定義プライバシー保護領域をサポートしています。12V DC アダプタ (IPC モデル) および 24V AC (PTZ モデル) に加えて、すべての IPC カメラは PoE (パワーオーバーイーサネット) をサポートし、PTZ カメラは POE+ をサポートしているため、別個の電源およびそれに伴う配線が不要です。すべてのモデルは、ネットワークサービス中断時に、装着した 2 つの microSDHC カードへのビデオ録画 (最大 512 GB) もサポートします。

# 対応ブラウザ

**注記：** 35 シリーズカメラは Windows デスクトップシステムをサポートしていますが、モバイルシステムはサポートしていません。

Chrome ブラウザと Edge ブラウザがサポートされています。

ブラウザ	バージョン
Chrome	91.0.4472.164 (公式ビルド) (64 ビット)
Edge	92.0.902.7 (公式ビルド) (64 ビット)

# 主な機能

Honeywell シリーズ 35 IP カメラの主な機能は次のとおりです。

## カメラ

- 最大 8MP (3840 x 2160) のカメラ
- 電子シャッターやゲインなどの録画パラメータの設定
- 映像解析機能：モーション検出、スマートモーション、不正干渉、侵入、マルチロイタリング、人数カウンター
- True WDR (120 dB)
- 着脱式赤外線カットフィルターを使用した True デイ/ナイトモード
- 2D/3D ノイズリダクションによる低照度がスマートコーデックによるストレージと帯域幅を節約
- NDAA に準拠するビデオシステムの一部として使用

## ストレージ

- 中央サーバーバックアップ

- シリーズ 35 カメラは、1 つの SD カードスロットを搭載し、SD カードにファイルを保存

## ネットワーク

- 最大 10 接続
- 以下のネットワークプロトコルとの互換性：IPv4、IPv6、TCP/IP、HTTP、HTTPS、RTSP/RTP/RTCP、IGMP/マルチキャスト、SMTP、DHCP、NTP、DNS、QoS、SNMP、802.1X、UDP、ICMP、ARP、TLS
- サポートしているセキュリティモード：ユーザーアカウントとパスワードの保護、HTTPS、IP フィルター、ダイジェスト認証、TLS1.2 のみ、ストリーム暗号化、AES128/256、SSH/Telnet クローズ、PCI-DSS に準拠
- サポートしている言語：アラビア語、チェコ語、オランダ語、英語、フランス語、ドイツ語、イタリア語、日本語、韓国語、ポーランド語、ポルトガル語（ブラジル）、ロシア語、スペイン語、トルコ語
- イーサネットによるカメラの設定と管理

## イベントと分析

- サポートしているビデオ分析機能タイプ：モーション検出、スマートモーション、不正干渉、侵入、マルチロイタリング、人数カウンター。
- サポートしているイベントタイプ：動画モーション検出、アラーム入力、録画通知、不正干渉
- サポートしているイベントリンケージモード：デジタル出力、電子メール、microSD カードを使用したイベント通知

## ユーザー管理

- 各ユーザーが特定のグループに所属
- グループごとに異なるユーザー権限

## システム管理

- ログ機能
- クライアント PC の IP アドレスを確認することでアクセス許可の制御をサポート

## カメラへのアクセス

この章は以下の項で構成されています。

- [Unified Tool のインストール、ページ 4](#)
- [ネットワーク上でのカメラ検出、ページ 6](#)
- [カメラの初期化、ページ 8](#)
- [カメラへの新しい IP アドレスの割り当て、ページ 9](#)
- [カメラのファームウェアのアップグレード、ページ 10](#)
- [Web ブラウザからカメラにアクセスする、ページ 12](#)

## Unified Tool のインストール

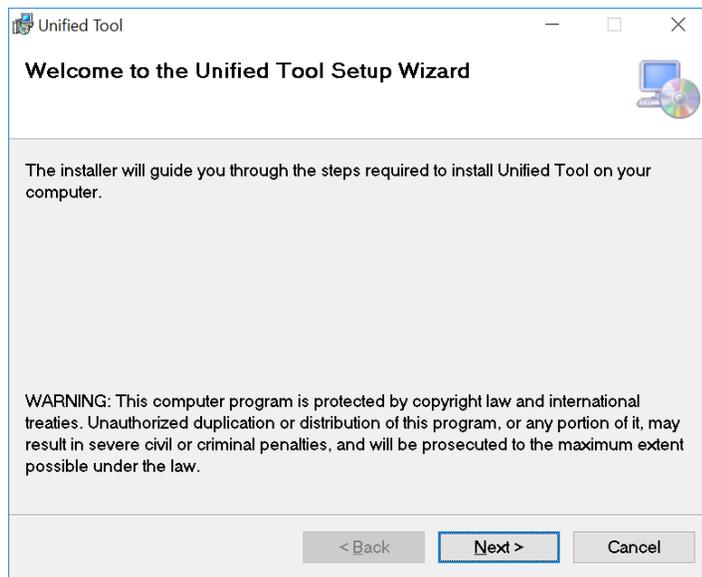
Unified Tool のインストールパッケージを取得するには：

<https://myhoneywellbuildingsuniversity.com/> にアクセスしてログインします。  
**Download Center [ダウンロードセンター]**に移動して、Unified Tool のインストールパッケージを検索してコンピュータにダウンロードします。パッケージを解凍する必要があります。

Unified Tool をインストールするには：

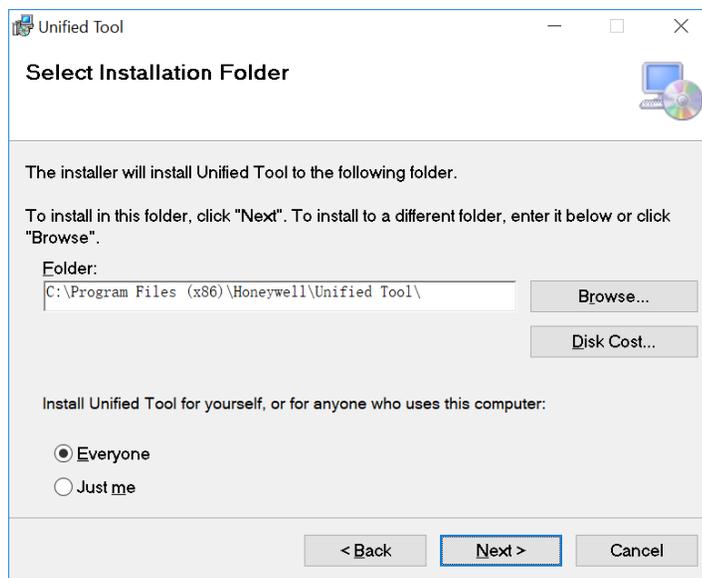
1. インストールパッケージのインストールプログラムをダブルクリックします。

## 図 1 Unified Tool のインストール



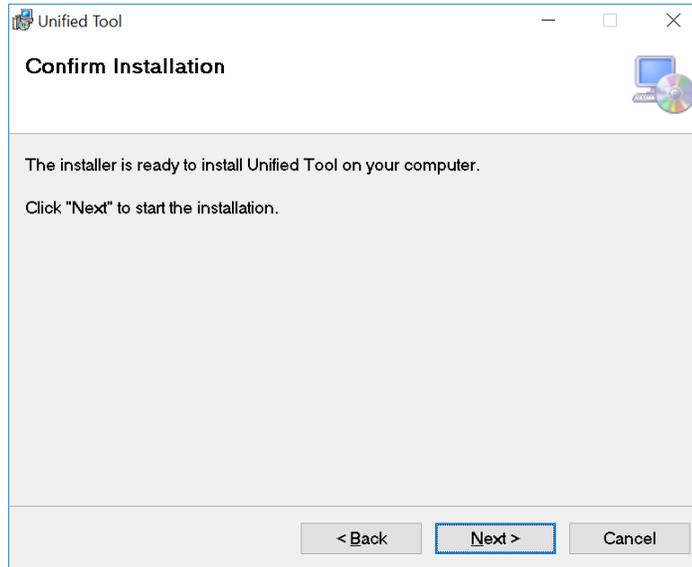
2. Next [次へ]をクリックします。次の図が表示されます。

## 図 2 インストールフォルダの選択



3. 画面の指示に従って設定を行い、Next [次へ]をクリックします。次の図が表示されます。

図 3 インストールの確認



4. Next [次へ]をクリックします。インストールが完了したら、Close [閉じる]をクリックします。Unified Tool のショートカットがデスクトップ上に表示されます。

## ネットワーク上でのカメラ検出

1. デスクトップで  をダブルクリックすると、次の図が表示されます。

図 4 スプラッシュ画面



2. Language [言語] ドロップダウンリストから言語を選択します。現在、サポートされて

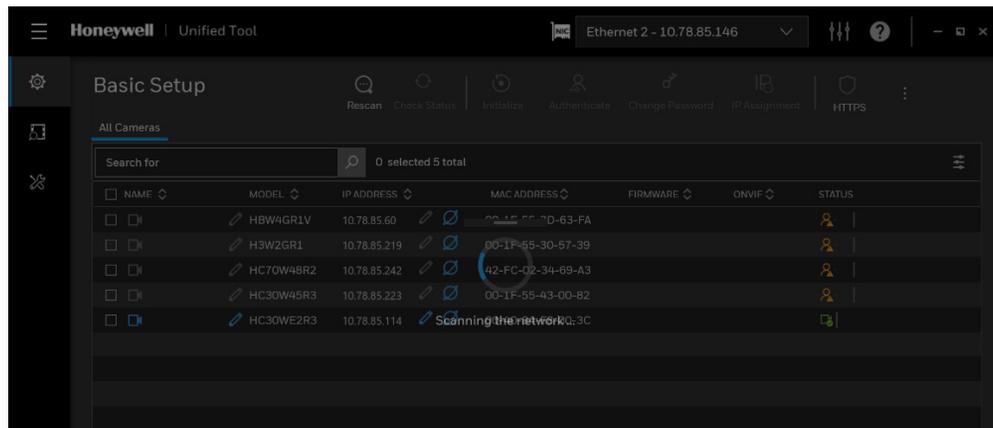
いるのは英語のみです。

3. Don't show the splash window on startup [起動時にスプラッシュウィンドウを表示しない]をオンにすると、次回このページをスキップできます。

スプラッシュウィンドウを再確認する場合は、[図 5](#) に示すように  をクリックし、Show the splash page on startup [起動時にスプラッシュページを表示する]のチェックボックスをオンにします。

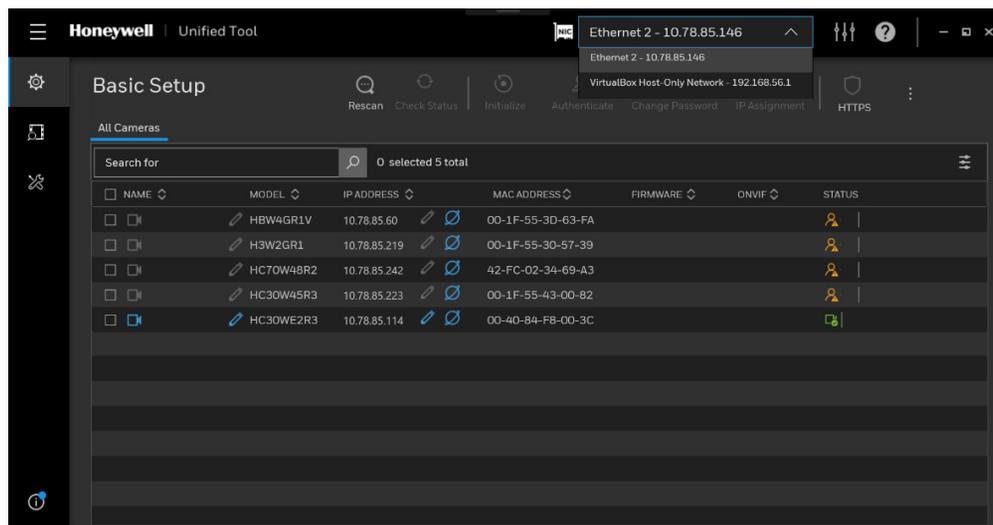
4. CONTINUE [続行]をクリックします。ネットワーク内のデバイスが自動的にスキャンされます。

図 5 ネットワークのスキャン



スキャン後、同じサブネットと異なるサブネットでスキャンされたすべてのデバイスがデバイスリストに表示されます。

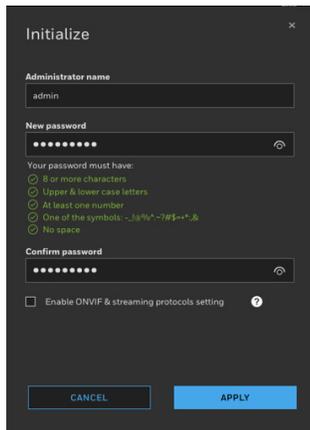
図 6 デバイスリスト



# カメラの初期化

 をクリックして 35 シリーズカメラを初期化することをお勧めします。初期化によって、カメラのパスワードを一括して設定できます。

図 7 初期化の 1 ページ目



Initialize [初期化] ページで、Administrator name [管理者名] と New password [新しいパスワード] を設定します。チェックボックスをオンにして、ONVIF & streaming protocols setting [ONVIF およびストリーミングプロトコルの設定] を有効にします。HTTPS only [HTTPS のみ] を選択します。APPLY [適用] をクリックします。

- 注記：
- Honeywell では HTTPS only [HTTPS のみ] を使用することを強くお勧めしています。Honeywell では、この結果に対する責任を負いません。
  - ONVIF およびストリーミングプロトコルの設定では、35 および 70 シリーズのカメラのみがサポートされます。サポートされていないモデルはスキップされます。

図 8 初期化の 2 ページ目

Initialize

Administrator name  
admin

New password  
••••••••

Your password must have:

- 8 or more characters
- Upper & lower case letters
- At least one number
- One of the symbols: ~!@%\*~?#&+~&
- No space

Confirm password  
••••••••

Enable ONVIF & streaming protocols setting ?

HTTP & HTTPS  HTTPS only

CANCEL APPLY

正常に初期化されたら、カメラを認証し、その他の設定を行うことができます。

## カメラへの新しい IP アドレスの割り当て

カメラの現在の IP アドレスが、デバイスリストの **IP ADDRESS [IP アドレス]**列に表示されます。新しい静的 IP アドレスをカメラに割り当てることができます。

図 5 に示すようにターゲットデバイスを選択し、 **IP Assignment** をクリックします。次の図が表示されます。

図 9 IP 割り当て

IP Assignment

IP address

DHCP  Manual

Start IP address  
192.168.199.244

End IP address  
192.168.199.244

Subnet  
255.255.255.0

Gateway  
192.168.199.100

DNS server address

Prefer DNS server  
192.168.199.100

Alternate DNS server  
0.0.0.0

CANCEL APPLY

## IP アドレス設定を構成する

- IP アドレス、サブネットマスク、およびデフォルトゲートウェイ設定を自動的に取得するには、**DHCP** のチェックボックスをオンにします。
- IP アドレス、サブネットマスク、およびデフォルトゲートウェイ設定を手動で構成するには、**Manual [手動]** のチェックボックスをオンにして設定を入力します。開始 IP アドレスを入力すると、選択したデバイスの数に応じて終了 IP アドレスが自動的に計算されます。
- すべての設定が完了したら、**APPLY [適用]** をクリックします。

## DNS サーバーアドレスを構成する

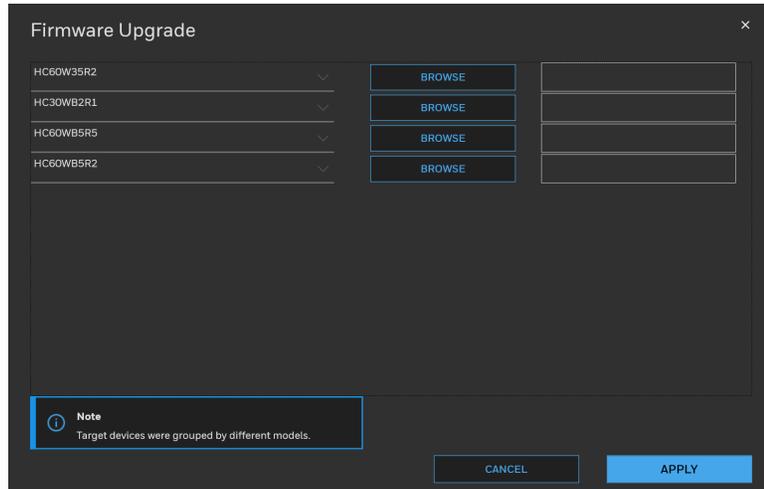
DNS サーバーアドレスを構成し、**Apply [適用]** をクリックします。

## カメラのファームウェアのアップグレード

カメラを使用する前に、最新のファームウェアがインストールされていることを確認してください。1 つまたは複数のカメラを同時にアップグレードできます。

図 5 に示すように、左側のペインから **Maintenance [メンテナンス]** タブを選択し、ターゲットデバイスを選択して  をクリックします。次のウィンドウが表示されます。

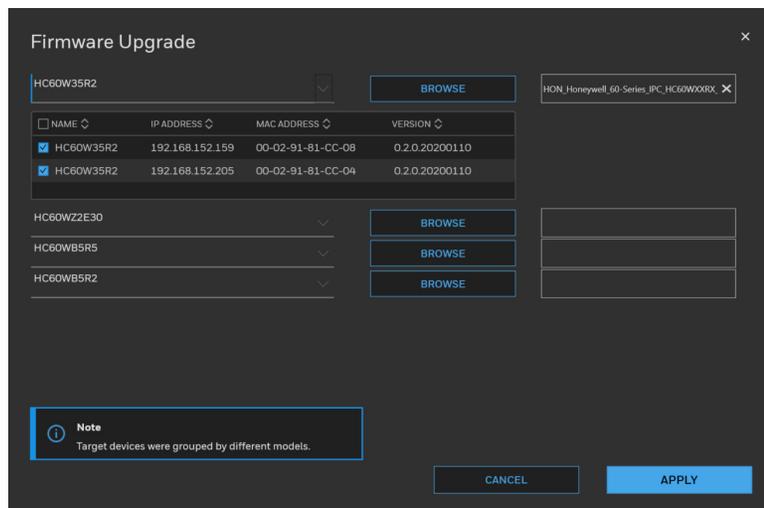
## 図 10 ファームウェアのアップグレード 1



デバイスはモデル別にグループ化されています。ファームウェアをアップグレードするには：

1. モデルの下にあるターゲットデバイスを選択します。
2. BROWSE [参照]をクリックして、コンピュータからアップグレードファイルを選択します。

## 図 11 ファームウェアのアップグレード 2



3. APPLY [適用]をクリックします。デバイスリストで進行状況を確認できます。

# Web ブラウザからカメラにアクセスする

Web ブラウザからカメラにアクセスするには、[図 6](#) に示すようにデバイスの IP アドレスの横にある  をクリックします。

## ログインとライブビデオの表示

この章は以下の項で構成されています。

- [Web クライアントからのカメラへのログイン](#)、ページ 13
- [メインページの使用](#)、ページ 15

## Web クライアントからのカメラへのログイン

Web クライアントを使用すると、ライブビデオを監視し、録画された動画を再生し、カメラ設定を構成することができます。

### 作業を開始する前に

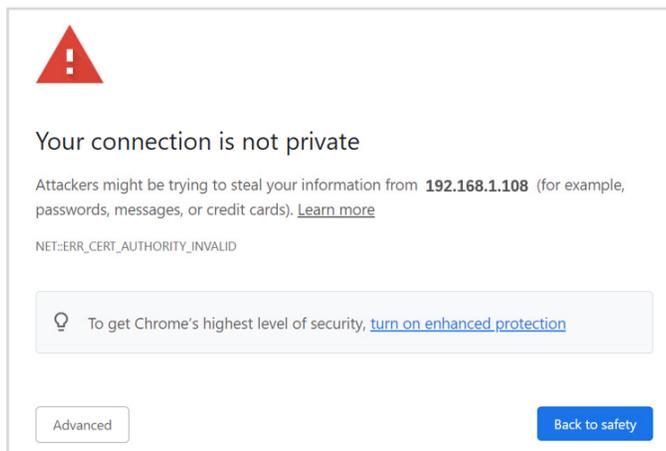
Web クライアントにログインする前に、次の条件が満たされていることを確認してください。

- カメラがネットワークに正しく接続されている。
- カメラの IP アドレスと PC の IP アドレスが同じネットワークセグメントに属する。  
ルーターがある場合は、対応するゲートウェイとサブネットマスクが設定されている。
- ネットワーク接続が確立されている。これを確認するには、カメラの IP アドレスに ping を実行します。（「ping [IP アドレス]」と入力します）。

**注記：** 新しいセキュリティエンハンスでは、カメラの IP アドレスに対して ping を実行できません。

# カメラへのログイン

1. Google Chrome を開いてアドレスバーにカメラの IP アドレスを入力し、Enter キーを押します。たとえば、カメラの IP アドレスが 192.168.1.108 の場合、<https://192.168.1.108> と入力します。
2. 下記のウィンドウが表示されます。Advanced [拡張]をクリックします。



3. 下記のウィンドウが表示されます。Proceed to 192.168.1.108 (unsafe) [192.168.1.108 に進む (安全でない)]をクリックします。

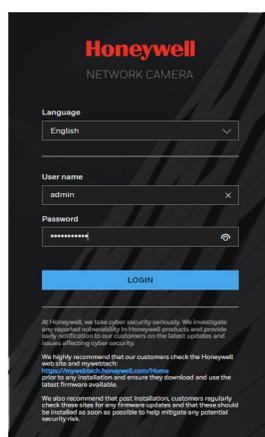


4. セキュリティのために、最初のログイン時に新しい安全なパスワードを作成する必要があります。



パスワードは8文字以上の長さで、少なくとも1つの大文字、1つの小文字、1つの数字、1つの特殊文字（-!@%^.~?#=#+\*;&）を含める必要があります。パスワードを空白にすることはできません。**SAVE [保存]**をクリックします。

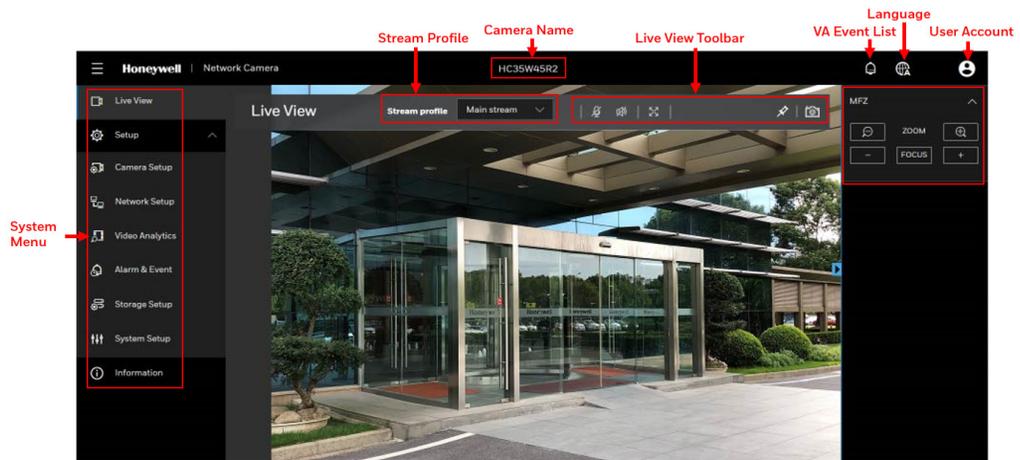
5. ログイン画面が表示されます。管理者のユーザー名とパスワードを入力して **LOGIN [ログイン]**をクリックします。



## メインページの使用

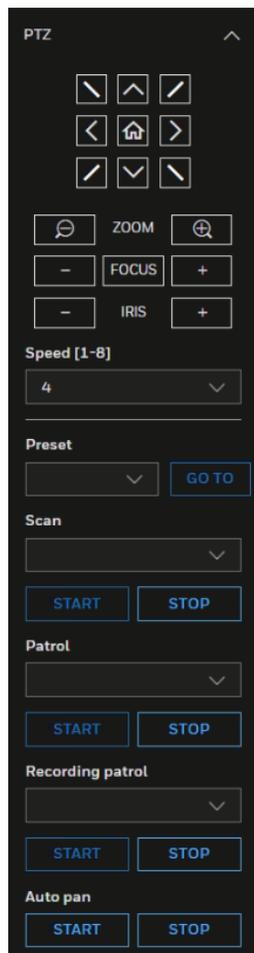
メインページには、システムメニュー、ライブビューツールバー、VA イベントリスト、言語選択、およびユーザーアカウント設定が含まれています。

図 12 メインページ



- MFZ IPC モデルの場合、図 12 に示すように右側の  をクリックすると MFZ パネルにアクセスできます。
- PTZ モデルの場合、図 13 に示すように右側の  をクリックすると PTZ パネルにアクセスできます。

図 13 PTZ パネル



PTZ 操作の詳細については、77 ページの [PTZ 設定の構成](#) を参照してください。

## システムメニュー

Web クライアントを使用してカメラにログインすると、デフォルトでメインページが開きます。セットアップページまたは情報ページにアクセスするには、対応するタブを選択します。

# ストリームプロファイル

ストリームプロファイルを設定するには、**Stream profile** [ストリームプロファイル] リストで **Main stream** [メインストリーム]、**Sub stream** [サブストリーム]、または **Third stream** [サードストリーム] を選択します。

**Main stream** [メインストリーム]：リアルタイムの監視、録画、保存を行う高解像度ビデオを提供します。ほとんどの帯域幅を使用します。

**Sub stream** [サブストリーム]：リアルタイムの監視、録画、保存を行う高解像度ビデオを提供します。ほとんどの帯域幅を使用します。

**Third stream** [サードストリーム]：低解像度ビデオを提供します。

各ストリームタイプのプロパティは、**Setup** [セットアップ] > **Camera Setup** [カメラのセットアップ] > **Video** [ビデオ] ページで構成します（[21 ページの動画設定の構成](#)を参照）。

# カメラ名

必要に応じてカメラ名を変更できます。詳細については、[68 ページのシステムの一般設定の構成](#)を参照してください。

# ライブビューツールバー

ライブビューツールバーを使用すると、スナップショットを作成できます。次の表に、コントロールの詳細を示します。

図 14 ライブビューツールバー



表 1 ライブビューツールバーアイコン

アイコン	説明
	デフォルトでは、このオプションは有効になっています。内蔵カメラを使用して相手に聞こえるように話ができます。クリックするとこのオプションが無効になります。
	クリックすると、監視サイトの音を聞くためのオーディオがオンになります。もう一度クリックすると、オーディオがオフになります。
	クリックして全画面モードに切り替えます。
	クリックすると、ライブビューがツールバーにピン留めされます。ピン留めを外すには、もう一度クリックします。
	クリックしてビデオ画像をキャプチャして保存します。キャプチャされた画像がポップアップウィンドウに表示されます。画像を右クリックして Save picture as [名前を付けて画像を保存]を選択し、JPEG (*.jpg) で保存します。

## VA イベントリスト

VA イベントリストを表示するには、メインページの  アイコンをクリックします。VA アラームが発生すると、 アイコンが点滅します。

**注記：**  をクリックすると最大 100 の VA アラームが表示され、周期的に繰り返してイベント情報が表示されます。Information [情報] > Logs [ログ] > Alarm log [アラームログ] に移動して、さらにアラームログレコードを表示または検索してください。[アラームログ](#) を参照してください。

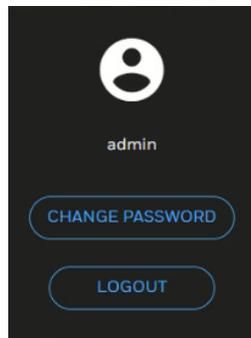
## Language [言語]

言語を切り替えるには、メインページの  アイコンをクリックします。

# 管理者アカウント

**注記：** 管理者のアカウント名とパスワードは、最初のログイン時にユーザーが設定します。

現在のログインユーザーのパスワードを設定したり、現在のユーザーアカウントをログアウトしたりするには、メインページの  アイコンをクリックします。下記のウィンドウが表示されます。



**CHANGE PASSWORD** [パスワードの変更]をクリックして、現在のログインユーザーのパスワードを変更します。

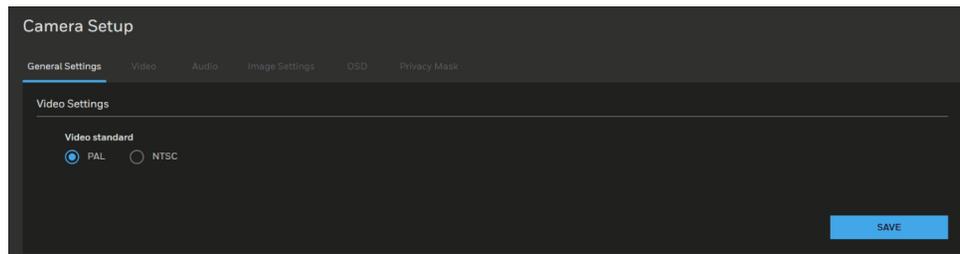
**LOG OUT** [ログアウト]をクリックして、現在のアカウントをログアウトします。

## カメラ設定の構成

### 一般設定の構成

Setup [設定] > Camera Setup [カメラの設定] > General Settings [一般設定]に移動します。  
このページでは、一般的なビデオ設定を構成できます。  
ビデオ規格を変更するには、PAL または NTSC を選択します。SAVE [保存]をクリックします。

図 15 一般設定



### 動画設定の構成

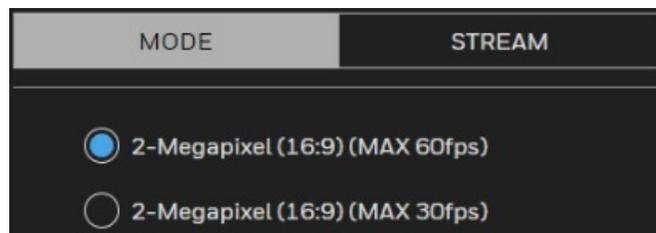
Setup [設定] > Camera Setup [カメラの設定] > Video [動画]に移動します。  
このセクションでは、ビデオストリームと ROI の設定の構成方法について説明します。

## Mode [モード]

Setup [設定] > Camera Setup [カメラの設定] > Video [動画] > MODE [モード]に移動します。

- 注記：
- モード機能は HC35WZ2R25 に適用されます。
  - 動画モードを変更すると、プライバシーマスク、画像設定、モーション、プリセット位置、フォーカスウィンドウの設定がクリアされます。

図 16 モードタブ



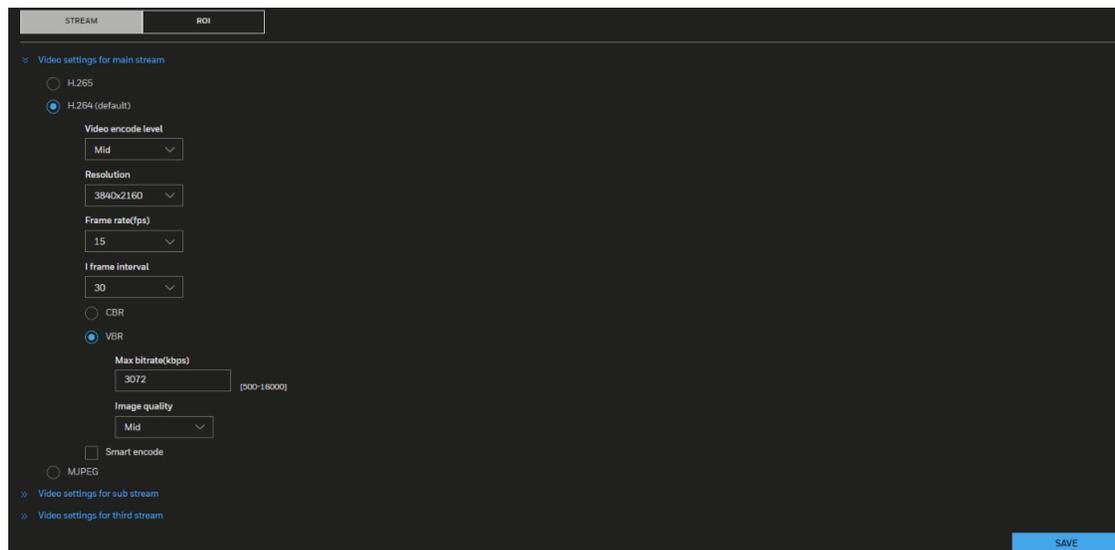
2メガピクセル（16：9）（最大30fps）：これを選択すると、最大解像度は1920x1080になります。

2メガピクセル（16：9）（最大60fps）：これを選択すると、最大解像度は1920x1080になります。これは、非TrueWDRモードではありません。

## 動画ストリーム

Setup [設定] > Camera Setup [カメラの設定] > Video [動画] > STREAM [モード]に移動します。

図 17 ビデオストリーム



H.265、H.264（デフォルト）、または MJPEG を選択し、メインストリーム、サブストリーム、およびサードストリームの動画設定を適用します。

**注記：** MJPEG が適用されている場合は、帯域幅が大きくなるため、5 fps 以下のカメラを使用することをお勧めします。

**Video encode level [ビデオエンコードレベル]：** ドロップダウンリストから値を選択します。

**Resolution [解像度]：** ドロップダウンリストから値を選択します。 解像度が高いほど、画質が向上します。

各モデルの解像度については、次の表を参照してください。

表 2 カメラ解像度

モデル	メインストリーム	サブストリーム	サードストリーム
HC35W43R3/HC35W43R2/ HC35WB3R3/HC35WB3R2 /HC35WE3R3/HC35WE3R 2	2304x1296/1920x 1080/1280x720	704x576 (PAL) /704x480 (NTSC) /640x480/352x288 (PAL) /352x240 (NTSC)	640x480/352x288 (PAL) /352x240 (NTSC) /320x240
HC35W45R3/HC35W45R2/ HC35WB5R3/HC35WB5R2 /HC35WE5R3/HC35WE5R 2/HC35W25R3	2592x1944/2592x 1520/1920x1080/ 1280x720	704x576 (PAL) /704x480 (NTSC) /640x480/352x288 (PAL) /352x240 (NTSC)	1920x1080 (最大 12 fps) /640x480/352x288 (PAL) /352x240 (NTSC) /320x240
HC35W48R3/HC35W48R2/ HC35WB8R3/HC35WB8R2 /HC35WE8R3/HC35WE8R 2	3840x2160/2592x 1944/2592x1520/ 2560x1440/2304x 1296/1920x1080/ 1280x720	704x576 (PAL) /704x480 (NTSC) /640x480/352x288 (PAL) /352x240 (NTSC)	640x480/352x288 (PAL) /352x240 (NTSC) /320x240
HC35WZ2R25	1920x1080/1280x 720	704x576 (PAL) /704x480 (NTSC) /640x480/352x288 (PAL) /352x240 (NTSC)	640x480/352x288 (PAL) /352x240 (NTSC) /320x240
HC35WZ5R30	2592x1944/2592x 1520/1920x1080/ 1280x720	704x576 (PAL) /704x480 (NTSC) /640x480/352x288 (PAL) /352x240 (NTSC)	640x480/352x288 (PAL) /352x240 (NTSC) /320x240

**Frame rate(fps)[フレームレート (FPS) ]:**

これにより、1 秒あたりの最大リフレッシュフレームレートが制限されます。よりスムーズなビデオ品質と視野内の動いているオブジェクトの認識のために、フレームレートを高く設定します。

ビデオ規格が **PAL** に設定されている場合、フレームレートは 1~50 fps から選択できます。ビデオ規格が **NTSC** に設定されている場合、フレームレートは 1~60 fps から選択できます。

より高い解像度を選択すると、フレームレートが低下します。

各モデルのフレームレートについては、次の表を参照してください。

表 3 カメラのフレームレート

メインストリーム	サブストリーム	サードストリーム
MAX 30fps HTTPS で暗号化する場合は最大 15fps  注記：HC35WZ2R25 については、以下のフレームレートを参照してください 最大 30fps (WDR オン) 最大 60fps (WDR オフ) HTTPS で暗号化する場合は最大 15fps	MAX 30fps HTTPS で暗号化する場合は最大 15fps	最大 30fps (暗号化には使用できません)

**I-frame interval [I フレーム間隔]**：ファームウェアが設定する I フレームのフレーム間隔を決定します。期間が短いほど、ビデオの品質が向上する可能性が高くなりますが、ネットワーク帯域幅の消費量が増えます。

**CBR：固定ビットレート**

ビットレートは一定になります（低帯域幅環境に推奨）。MJPEG 圧縮を使用する場合は必須です。

**VBR：可変ビットレート**

ビットレートは、シーンの複雑さに応じて変化します。

**Max bitrate(kbps) [最大ビットレート (kbps)]**：ビットレートの最大値を示します。最大ビットレートに 500～12000 を設定します。

**Image Quality [画質]**：希望の品質を、最低から最大の範囲から選択します。

**Smart encode [スマートエンコード]**：チェックボックスをオンにして、スマートエンコードを有効にします。

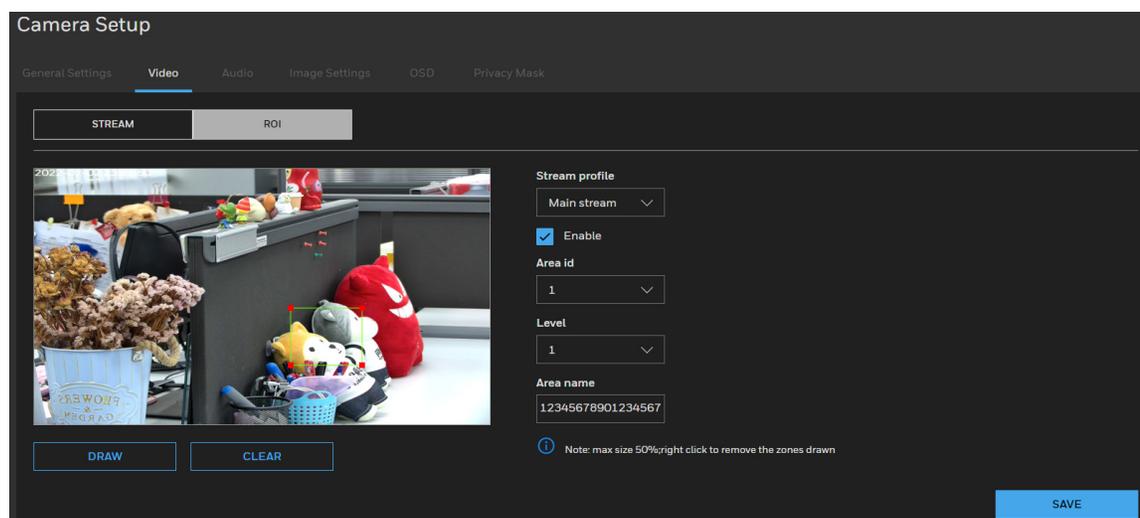
- スマートエンコードには H.264 と H.265 が含まれます。
- スマートエンコードを有効にすると、ストレージ容量が 50%削減されます。
- スマートエンコードをサポートしているのはメインストリームのみです。

# ROI

ROI 機能では、画面上に 8 つの ROI ウィンドウ（ROI 領域、前景品質）を構成できます。いずれの ROI ウィンドウにも含まれていない領域は、非 ROI 領域と見なされます。ROI 領域の詳細は、高品質のビデオ形式で送信されます。ROI ウィンドウを使用して保護された領域を覆い、画面の残りの部分が非 ROI 領域になることにより、ROI ウィンドウをプライバシーマスクとして設定できます。

Setup [設定] > Camera Setup [カメラの設定] > Video [動画] > ROI [モード]に移動します。

図 18 ROI 設定



**Stream profile [ストリームプロファイル]**：Main stream [メインストリーム]、Sub stream [サブストリーム]、または Third stream [サードストリーム]を選択して、ストリームプロファイルを設定します。

**Enable [有効化]**：ROI（関心領域）を有効にするには、チェックボックスをオンにします。

**Area id [エリア ID]**：ドロップダウンリストボックスから値を選択して、ROI 領域 ID を設定します。合計で 8 つのエリアを追加できます。

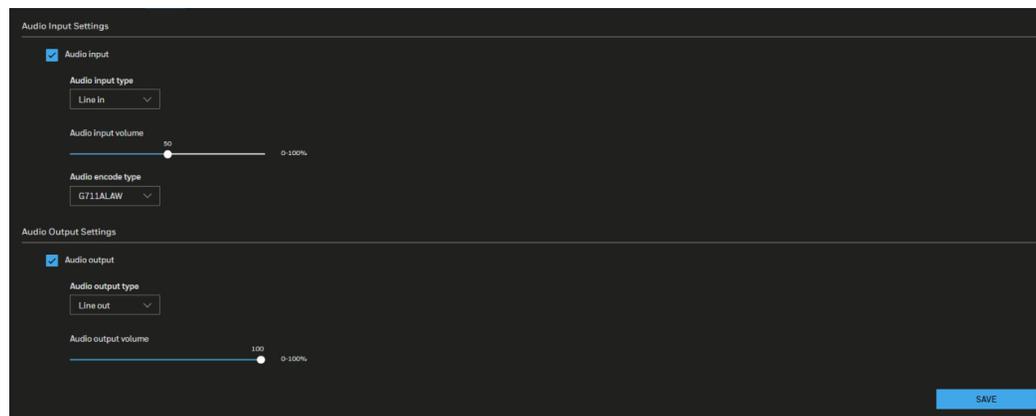
**Level [レベル]**：ドロップダウンリストボックスから値を選択して、ROI の視覚効果を設定します。レベル 1 に設定すると、関心領域内での最高品質のビデオと、非関心領域での最もぼやけたビデオの最適な効果が得られます。

**Area name [エリア名]**：エリアのカスタマイズ名を入力します。最大値は 32 バイトを超えることはできません。

# オーディオ設定の構成

Setup [設定] > Camera Setup [カメラの設定] > Audio [オーディオ]に移動します。

図 19 オーディオ設定



## オーディオ入力設定

**Audio Input [オーディオ入力]**：チェックボックスをオンにして、オーディオ入力を有効にします。

**Audio input type [オーディオ入力タイプ]**：Microphone [マイク]または Line-in [ライン入力]オプションを選択します。

**注記**： Microphone [マイク]オプションは、マイクロドームカメラにのみ適用されます。

**Audio input volume [オーディオ入力音量]**：マイクのゲインまたはライン入力のゲインです。選択したオーディオ入力オプションに従って、マイクのゲインまたはライン入力のゲインのオプションが表示されます。周囲の状況に応じて、外部オーディオ入力のゲインを選択します。ゲインを 0%（最小）から 100%（最大）に調整します。

**Audio encode type [オーディオエンコードタイプ]**：G711ALAW および G711ULAW のオーディオコーデックとビットレートを選択します。

## オーディオ出力設定

**Audio output [オーディオ出力]**：チェックボックスをオンにして、オーディオ出力を有効にします。

**Audio output type [オーディオ出力タイプ]**：Line-out [ライン出力]オプションを選択します。

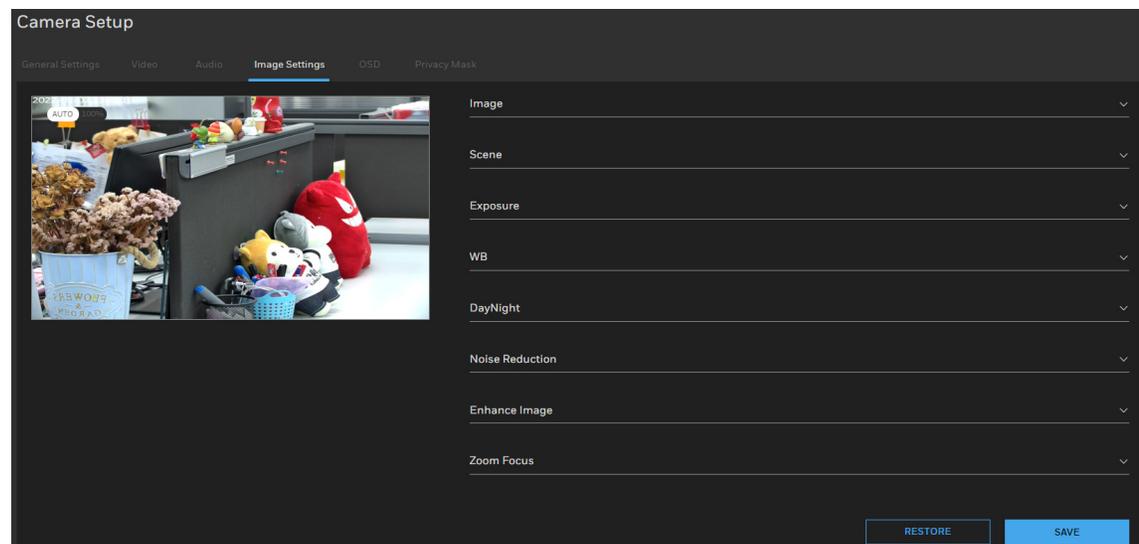
**Audio output volume [オーディオ出力音量]**：ライン出力オプションは、選択したオーディオ出力オプションに応じて表示されます。周囲の状況に応じて、外部オーディオ入力の音量を選択します。音量を 0%（最小）から 100%（最大）に調整します。

このページの設定が完了したら、**SAVE [保存]**をクリックして設定を有効にします。

## 画像設定の構成

Setup [設定] > Camera Setup [カメラの設定] > Image Settings [画像設定]に移動します。このページでは、Image [画像]、Scene [シーン]、Exposure [露光]、WB [ホワイトバランス]、DayNight [デイナイト]、Noise Reduction [ノイズ低減]、Enhance Image [画像のエンハンス]のパラメータを構成できます。

図 20 画像設定



## 画像調整

**Brightness [輝度]**：画像の輝度レベルを調整します（0～100）。

**Saturation [彩度]**：画像の彩度レベルを調整します（0～100）。

**Contrast [コントラスト]**：画像のコントラストレベルを調整します（0～100）。

**Sharpness [シャープネス]**：画像のシャープネスレベルを調整します（0～100）。

## シーンモード

**Scene [シーン]**：シーンモードを変更するには、屋内/屋外を選択します。

**Mirror [ミラー]**：画像をミラーリングするには、Normal [標準]、Horizontal [水平]、Vertical [垂直]、Horizontal + Vertical [水平+垂直]を選択します。

**通路モード**：通路モードが有効な場合、画像は時計回りに 90 度回転します。

- 注記：
- 通路モードが有効で、サブストリームまたはサードストリームが 352\*240 または 320\*240 に設定されている場合は、ストリームアウトできません。
  - 通路モードが有効な場合、人のカウント機能は無効です。

Normal [標準]	Vertical [垂直方向]	Normal [標準]	Horizontal [水平方向]	Normal [標準]	Horizontal + Vertical [水平+垂直]	Aisle [通路]
						

## Exposure [露出]

露光エリアの選択には、**Meter area [メーター領域]**を使用します。エリアの露光設定ごとに、Whole [全体]、Center spot [中央スポット]、Center area [中央エリア]を選択します。

**Exposure Mode [露光モード]**：露光モードには次のものがあります。

- **Auto [自動]**：システムは、監視環境に基づいて自動露出を実行します。

- **Manual [手動]** : **Shutter Setting [シャッター設定]**、**Iris Setting [アイリス設定]**、**Gain Setting [ゲイン設定]**を設定して、最高画質になるように露出レベルを手動で調整します。
- **Shutter priority [シャッター優先]** : 固定シャッターを選択すると、最適な露出レベルに合わせて自動的にゲインとアイリスが調整されます。ゲイン範囲は最大値を下回ります。
- **IRIS priority [アイリス優先]** : IRIS F-number を選択すると、最適な露出レベルに合わせてゲインと露出時間が自動的に調整されます。ゲイン範囲と照射時間は最大値を下回ります。

**Max shutter [最大シャッター]** : 周辺光に基づいてシャッター時間が自動的に最大値設定未満に調整されます。

**Max gain [最大ゲイン]** : 周辺光に基づいてゲインが自動的に最大値設定未満に調整されます。

## ホワイトバランス (WB) の設定

**Mode [モード]** : 最適な色温度の値を調整します。

- **Auto [自動]** : 選択すると、カメラは自動的に色温度を調整します。
- **Tungsten [タングステン]**、**Fluorescent [蛍光灯]**、**Daylight [昼光]**、**Shadow [シャドウ]** : 選択すると、カメラがタングステン/蛍光灯/昼光/シャドウの色温度に変わります。

**注記 :** PTZ モデルでは、タングステン/昼光の色温度がサポートされています。

- **Manual [手動]** : R ゲインと B ゲインのスライダーをドラッグして、色温度を手動で調整できます。

# デイナイト設定

デイナイトモードの設定は、デバイスモデルによって異なります。

**D/N setting [D/N 設定]**：自動、デイモード、ナイトモード、タイミングに設定できます。

- Auto [自動]

カメラは、周囲光のレベルを判断することにより、フィルターを自動的に削除します。

**注記：** 光モードで IR LED [赤外線 LED]を選択すると、ナイトモードで赤外線 LED が点灯します。

- Day mode [デイモード]

デイモードでは、カメラは赤外線カットフィルターを常にオンにして、赤外線がセンサーに届かないようにして、色が歪まないようにします。

- Night mode [ナイトモード]

ナイトモードでは、カメラが赤外線カットフィルターを常にオフにして、センサーが赤外線を受け入れるため、光が弱くても感度を向上させます。

- Timing [タイミング]

カメラは、指定されたスケジュールに基づいて、デイモードとナイトモードを切り替えます。デイモードの開始時刻と終了時刻を入力します。時刻の形式は[hh:mm]で、24 時間制の時刻で表されます。デフォルトでは、デイモード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。

**DTN time [DTN 時間]**：デイモードの時刻をナイトモードに切り替えます

**NTD time [DTN 時間]**：ナイトモードの時間をデイモードに切り替えます

**Delay(s) [遅延]**：カメラが切り替えを検出したときのデイからナイトまたはナイトからデイへの切り替えの遅延時間を設定します。

**D/N switch sensitivity [D/N スイッチの感度]**：デイからナイト/ナイトからデイへの切り替えの感度を設定します。

**Light mode [光モード]**：IR led [赤外線 LED]を選択して、赤外線 LED ライトを有効にします。赤外線 LED ライトを無効にするには、None [なし]を選択します。

### IR led [赤外線 LED] :

- Auto [自動] : 赤外線ランプは、光依存抵抗 (LDR) によって識別される外部環境に基づいて、有効または無効になります。Smart IR [スマート IR]は Auto [自動]でサポートされます。
- Manual [手動] : これを選択して、IR ライトの輝度を手動で制御します。Near [近]、Center [中央]、Far [遠]の距離で IR ライトの輝度を上げるには、スライダーを右にドラッグします。IR ライトの輝度を下げるには、スライダーを距離の分だけ左にドラッグします。

## ノイズ低減

スライダーをドラッグして、低減強度を調整します (低～高)。

**2D NR/3D NR [2D NR/3D NR]** : 画像のノイズを低減します。

**Max Strength [最大強度]** : 3D ノイズリダクションの性能を向上させるには、より高い値を設定してください。

**注記 :** 3D ノイズリダクションは、主に暗い場所で適用されます。高レベルの 3D ノイズリダクションを適用すると、動きの速い物体を含む低光量条件では、遅延やモーションブラーが発生します。この場合は、3D ノイズリダクションで低レベルを選択することをお勧めします

画像設定に加えられたすべての変更は、画面に直接表示されます。変更を組み込まずに元の設定を呼び出すには、**RESTORE [復元]**をクリックします。設定が完了したら、**SAVE [保存]**をクリックします。

# 画像のエンハンス

画像をエンハンスするには、以下の機能を適用して画像を調整できます。

**注記： 機能は、カメラのモデルによって異なる場合があります。**

## **WDR (Wide Dynamic Range)[WDR (ワイド ダイナミック レンジ) ]**

WDR は、最も暗いエリアと最も明るいエリアの両方を同時に明瞭に見ることができるように、最も明るいエリアの輝度を下げて最も暗いエリアの輝度を高めることによって、シーン内の明るさと暗さを調整します。

この値は、1～100 の範囲です。このデフォルト値は 50 です。

## **BLC (逆光補正)**

カメラは自動的に条件に合うように露出を調整し、動画の最も暗い部分が見えるようにします。

この値は、1～100 の範囲です。このデフォルト値は 50 です。

## **HLC (ハイライト補正)**

HLC 機能を有効にすると、カメラは、選択された HLC コントロールレベルに従って、動画の最も明るい部分の輝度を下げることができます。HLC は、ハローの量を減らし、動画画像全体の輝度を低下させることができます。

この値は、1～100 の範囲です。このデフォルト値は 50 です。

**DeFog [霧除去]**：チェックボックスをオンにして、霧除去を有効にします。霧や曇りの環境では画質が低下し、画像の鮮明度を向上させるために霧除去を使用できます。

**Anti-shake [振動防止]**：チェックボックスをオンにして**振動防止**を有効にします。

振動防止を有効にした後では、システムによりスムーズなビデオ（電子画像安定化）が提供されます。画像の品質は、カメラの振動強度の影響を受けます。

**注記： 振動防止機能は、PTZ モデル HC35WZ2R25 と HC35WZ5R30 にのみ適用されます。**

# OSD の構成

**Setup [設定] > Camera Setup [カメラの設定] > OSD [OSD]**に移動します。OSD [OSD] ページが表示されます。

**Time [時間]**：有効にすると、ライブビュー画像に時間情報が表示されます。

**Video title [ビデオタイトル]**：ビデオタイトルを有効にして入力すると、ライブ表示画像にビデオタイトルが表示されます。

**( for PTZ model only ) PTZ coordinates [ (PTZ モデルのみ) PTZ 座標]**：有効にすると、PTZ を移動するときに PTZ 座標が表示されます。

**Position [位置]**：OSD ディスプレイと位置を設定します。

**Font size [フォントサイズ]**：OSD ディスプレイのフォントサイズを設定します。

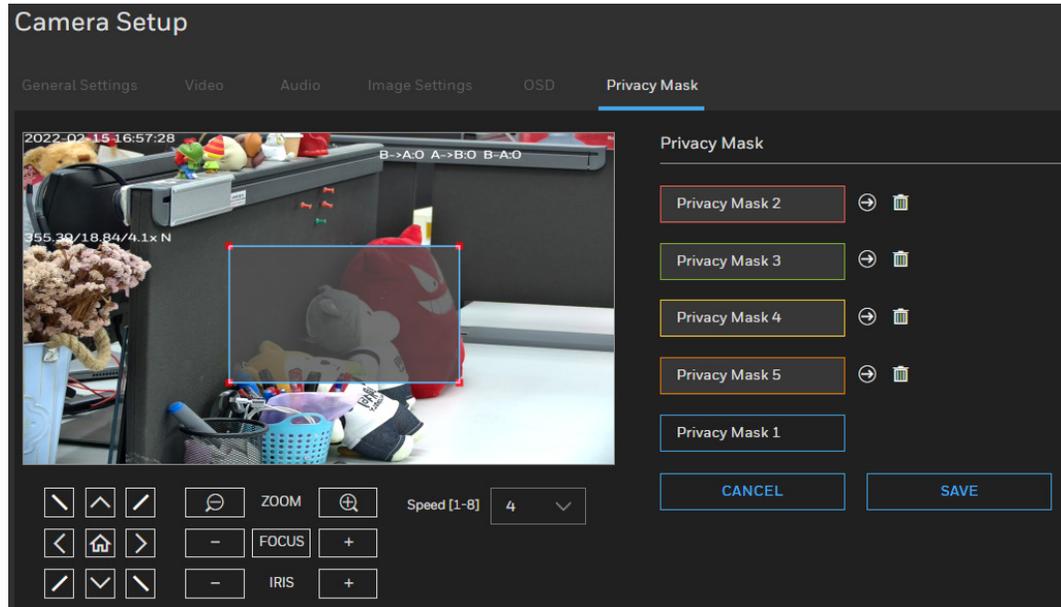
# プライバシーマスクの設定

このページでは、機密性の高い表示領域をブロックして、プライバシーの問題に対処できます。**Setup [設定] > Camera Setup [カメラの設定] > Privacy Mask [プライバシーマスク]**に移動します。

プライバシーマスクを構成する手順は次のとおりです。

1. **ADD MASK [マスクの追加]**をクリックして、ビデオ画面に新しいプライバシーマスクウィンドウを追加します。
2. 長方形の角をドラッグして、新しいマスキングウィンドウを作成します。
3. プライバシーマスクの名前を入力し、**SAVE [保存]**をクリックして設定を有効にします。

図 21 プライバシーマスク



- 注記：
- オブジェクトはビデオ画面の中央に配置し、プライバシーマスクの設定サイズはオブジェクトサイズの 1.5～2.5 倍にする必要があります。
  - IPC/PTZ カメラでは、同じ画面で最大 4/5 のプライバシーマスクウィンドウを構成できます。
  - プライバシーマスクウィンドウを削除する場合は、プライバシーマスクウィンドウ名の右側にある  をクリックします。  をクリックすると、関連のプライバシーマスクの位置に移動します。

## ネットワーク設定の構成

### ネットワークの一般設定の構成

このセクションでは、カメラの有線ネットワーク接続を構成する方法について説明します。

Setup [設定] > Network Setup [ネットワーク設定] > General Settings [一般設定]に移動します。

図 22 ネットワークの一般設定

The screenshot shows the 'Network Setup' configuration page with the 'General Settings' tab selected. The 'Network Type' section is expanded, showing the following settings:

- IP protocol:** A dropdown menu set to 'IPv4'.
- DHCP:** A radio button that is selected.
- DHCP IP:** A text input field containing '192.168.152.207'.
- Fixed IP:** An unselected radio button.
- Preferred DNS server:** A text input field containing '192.168.152.253'.
- Alternate DNS server:** A text input field containing '192.168.152.252'.
- MTU(1280~1500):** A text input field containing '1500'.

IP プロトコルに IPv4/IPv6 を選択します。

IPv4/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アドバタイズメントをリッスンし、それに応じてリンクローカル IPv4/IPv6 アドレスが割り当てられます。

**DHCP**：このオプションを選択して、カメラが 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た使用可能な動的 IP アドレスを取得します。

**Fixed IP [固定 IP]**：このオプションを選択して、静的 IP アドレスをカメラに手動で割り当てます。

**IP address [IP アドレス]**：

ソフトウェア CD の Unified Tool を使用して、LAN でカメラを簡単にセットアップできます。4 ページの[カメラへのアクセス](#)を参照してください。

ISP またはネットワーク管理者から提供された静的 IP、サブネットマスク、デフォルトゲートウェイ、およびプライマリ DNS を入力します。

**Subnet mask [サブネットマスク]**：これは、宛先が同じサブネットにあるかどうかを判断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 gateway [デフォルトゲートウェイ]**：これは、異なるサブネットの宛先にフレームを転送するために使用されるゲートウェイです。無効なルーター設定は、異なるサブネットにわたる宛先への送信を無効にします。

**Preferred DNS Server [優先 DNS サーバー]**：ホスト名を IP アドレスに変換するプライマリドメインネームサーバー。

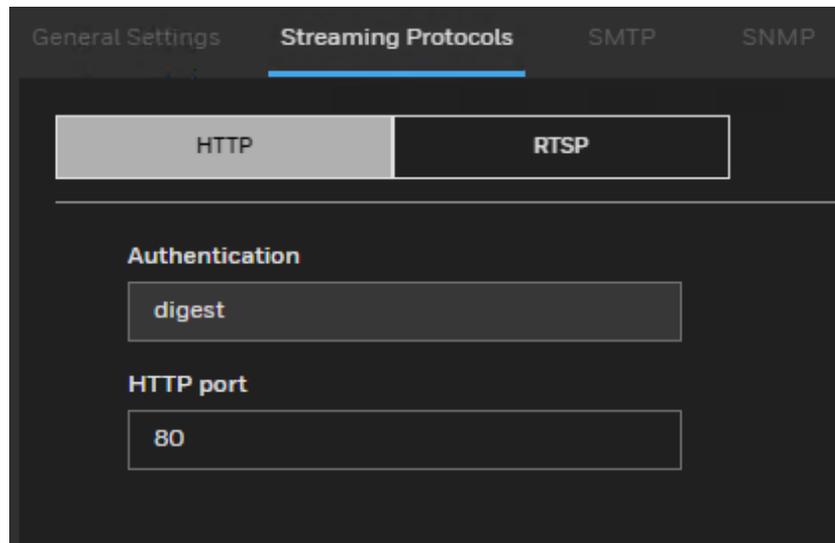
**Alternate DNS Server [代替 DNS サーバー]**：プライマリ DNS をバックアップするセカンダリドメインネームサーバー。

**MTU (1280~1500) [MTU (1280~1500) ]**：ネットワーク送信データパケットの最大値を設定します。

# ストリーミングプロトコルの構成

Setup [設定] > Network Setup [ネットワーク設定] > Streaming Protocols [ストリーミングプロトコル]に移動します。

図 23 ストリーミングプロトコル-HTTP

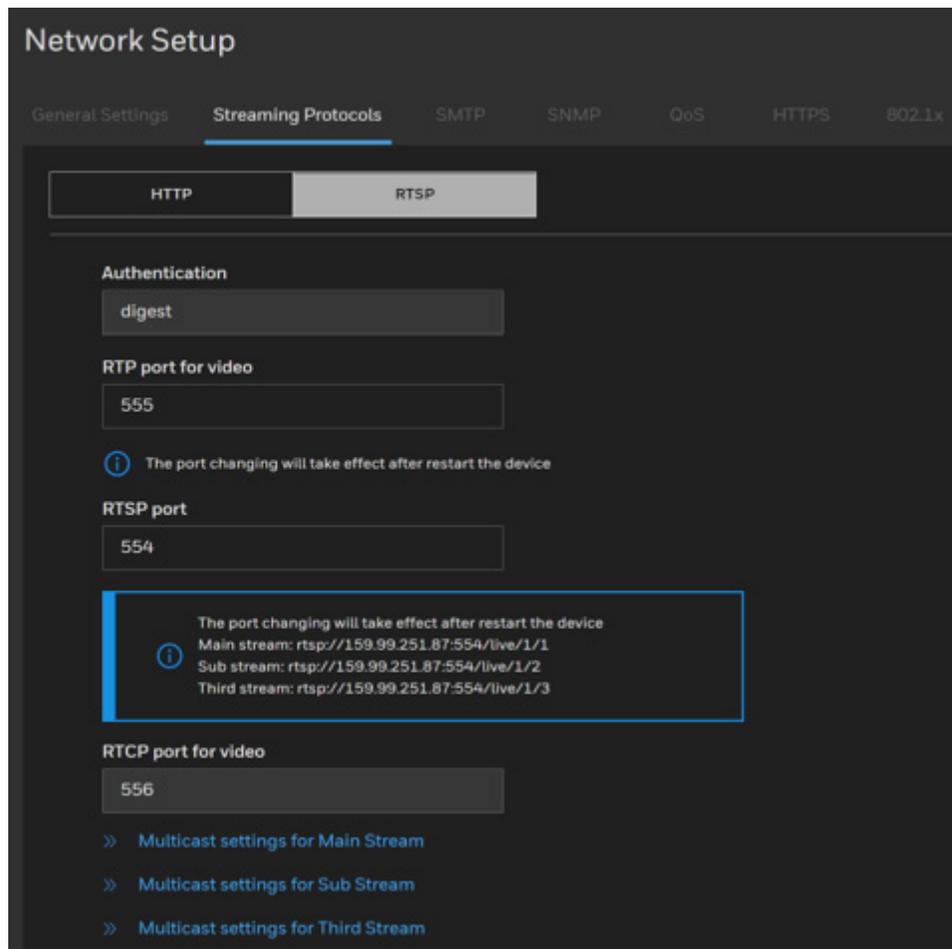


**HTTP** 認証を利用するには、最初にカメラのパスワードを設定してください。詳細については、[74 ページのユーザーアカウント設定の構成](#)を参照してください。

**Authentication [認証]**：ユーザー資格情報は MD5 アルゴリズムで暗号化されており、不正アクセスに対する保護が強化されています。

**HTTP Port [HTTP ポート]**：デフォルトでは、HTTP ポートは 80 に設定されています。また、1025～65535 の別のポート番号に割り当てることもできます。

図 24 ストリーミングプロトコル-RTSP



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。詳細については、[74 ページのユーザーアカウント設定の構成](#)を参照してください。

**Authentication [認証]**：認証により、不正アクセスに対する保護が強化されます。

RTSP プレーヤーを使用して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 RTSP URL 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。

Use rtsp://IP address [rtsp://IP アドレスを使用する]：RTSP ストリーミングをプルするためのポート/ライブ/カメラ ID/ストリーミング ID です。

**注記：**

- IP address [IP アドレス]：デバイスの IP アドレス

- Port [ポート]: RTSP ポート。デフォルトは 554
- Live [ライブ]: デフォルトとしてライブを保持します。
- Camera ID [カメラ ID]: 1
- Streaming ID [ストリーミング ID]: メインストリームは 1、サブストリームは 2、サードストリームは 3 です。

例: RTSP ストリーミングをストリーミングするには、次の手順を実行します。

1. RTSP プレーヤーを起動します。
2. File [ファイル] > Open URL [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. 各ストリームのテキストボックスに次の URL コマンドを入力します。
 

メインストリーム:     rtsp://192.168.0.108:554/live/1/1

サブストリーム:        rtsp://192.168.0.108:554/live/1/2

サードストリーム:     rtsp://192.168.0.108:554/live/1/3
4. ライブビデオがプレーヤーに表示されます。

#### RTSP ポート/ビデオ用の RTP ポート/ビデオ用の RTCP ポート:

- RTP (リアルタイムトランスポートプロトコル) は、ビデオデータをクライアントに配信するために使用されます。デフォルトでは、ビデオの RTP ポートは 555 に設定されています。
- 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。デフォルトでは、RTSP ポート番号は 554 に設定されています。
- RTCP (リアルタイムトランスポートコントロールプロトコル) を使用すると、カメラはインターネットトラフィック量を監視してデータを送信できます。デフォルトでは、ビデオの RTCP ポートは 556 に設定されています。

ポートは、1025~65535 の値に変更できます。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 を加えたものであるため、常に奇数です。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。

**Multicast settings for streams** [ストリームのマルチキャスト設定]：クリックすると、詳細な構成情報が表示されます。

**Multicast group address** [マルチキャストグループアドレス]：マルチキャストグループアドレスを入力します。

**Multicast video port** [マルチキャストビデオポート]：ポートは、1025～65535 の値に変更できます。このデフォルト値は 25330 です。

**Multicast audio port** [マルチキャストオーディオポート]：ポートは、1025～65535 の値に変更できます。このデフォルト値は 25430 です。

**Multicast metadata port** [マルチキャストメタデータポート]：ポートは、1025～65535 の値に変更できます。デフォルト値は 25530

**Multicast TTL** [マルチキャスト TTL]：マルチキャスト TTL (Time To Live) は、パケットを転送できる範囲をルーターに伝える値です。このデフォルト値は 60 です。

**注記：** マルチキャストは、カメラではデフォルトで有効になっています。

## SMTTP 設定の構成

簡易メール転送プロトコル (SMTP) 機能が有効になっている場合、アラームが生成されると、デバイスは指定された電子メールアドレスに JPG イメージとアラーム情報を自動的に送信します。

**Setup** [設定] > **Network Setup** [ネットワーク設定] > **SMTP** [SMTP]に移動します。

図 25 SMTP 設定

The screenshot shows the 'Network Setup' interface with the 'SMTP' tab selected. The configuration fields are as follows:

- SMTP server address \***: An empty text input field.
- SMTP server port \***: A text input field containing '25', with a range indicator '[1 ~ 65535]' to its right.
- User name \***: An empty text input field.
- Password \***: An empty text input field.
- Sender e-mail address1 \***: An empty text input field.
- Recipient e-mail address1 \***: An empty text input field.
- Recipient e-mail address2**: An empty text input field.
- Recipient e-mail address3**: An empty text input field.
- Recipient e-mail address4**: An empty text input field.
- Recipient e-mail address5**: An empty text input field.
- Transport mode**: A dropdown menu currently set to 'No Encrypt'.
- Send interval**: A text input field containing '0', with a range indicator '[0 ~ 60s]' to its right.

**SMTP server address [SMTP サーバーの IP アドレス]**：SMTP サーバーの IP アドレスです。

**SMTP server port [SMTP サーバーポート]**：SMTP サーバーのポート番号です。

**User Name [ユーザー名]**：電子メールを送信するためのメールボックスのユーザー名です。

**Password [パスワード]**：電子メールを送信するためのメールボックスのパスワードです。

**Sender e-mail address1** [送信者の電子メールアドレス 1]：電子メールを送信するためのメールボックスです。

**Recipient\_e-mail\_address1** [Recipient\_e-mail\_address1]：受信者 1 の電子メールアドレスです。

**Recipient\_e-mail\_address2** [Recipient\_e-mail\_address2]：受信者 2 の電子メールアドレスです。

**Recipient\_e-mail\_address3** [Recipient\_e-mail\_address3]：受信者 3 の電子メールアドレスです。

**Recipient\_e-mail\_address4** [Recipient\_e-mail\_address4]：受信者 4 の電子メールアドレスです。

**Recipient\_e-mail\_address5** [Recipient\_e-mail\_address5]：受信者 5 の電子メールアドレスです。

**Transport mode** [トランスポートモード]：電子メール暗号化モードです。このパラメータは、SMTP サーバーでサポートされている暗号化モードに基づいて設定します。

**Send interval** [送信間隔]：送信間隔は 0~60 秒で設定できます。アラームが発生した場合、システムが電子メールを即時に送信することはありません。アラーム、モーション検出またはその他のイベントの発生により電子メールが有効化された場合、ここで指定した間隔で 1 つの電子メールをシステムが送信します。これにより、複数の電子メールが同時に送信されたときの電子メールサーバーの負荷が軽減されます。

## SNMP 設定の構成

**Setup** [設定] > **Network Setup** [ネットワーク設定] > **SNMP** [SMTP]に移動します。

SNMP (Simple Network Management Protocol) は、ネットワーク上の管理対象デバイス間で管理情報を収集、整理、交換するためのプロトコルです。

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。

- **マネージャー**：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

および制御するアプリケーションを実行するサーバー。

- **エージェント**：管理対象デバイスのステータスを NMS に転送する管理対象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。
- **管理対象デバイス**：管理された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、プリンター、IP 電話、ネットワークカメラ、Web サーバー、データベース。

ページで SNMP 設定を構成する前に、まず NMS を有効にします。

**Enable SNMPv1, SNMPv2c [SNMPv1、SNMPv2c の有効化]**：オンにして、SNMPv1、SNMPv2c を有効にします。SNMPv1 および SNMPv2c では、コミュニティを使用して、マネージャーとエージェント間の信頼関係を確立します。エージェントは、3 つのコミュニティ名、書き込みコミュニティ、読み取りコミュニティ、およびトラップをサポートします。

**Write community [書き込みコミュニティ]**：書き込みコミュニティの名前。書き込みコミュニティでは、データのみを変更できます。

**Read community [読み取りコミュニティ]**：読み取りコミュニティの名前です。書き込みコミュニティでは、データの読み取りのみが可能です。

**Trap address [トラップアドレス]**：トラップの IP アドレスです。

**Trap Port [トラップポート]**：トラップからのメッセージを受け入れる管理ポートです。

**Trap community [トラップコミュニティ]**：トラップのコミュニティストリングです。トラップコミュニティストリングを使用すると、マネージャーはエージェントから非同期情報を受信できます。

**Enable SNMPv3 [SNMPv3 の有効化]**：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を含む SNMPv3 を有効にする場合にオンにします。

SNMPv3 ではコミュニティストリングが使用されますが、SNMP マネージャーとエージェント間のセキュアな認証と通信が実現されます。

**Read security name [読み取りセキュリティ名]**：読み取りセキュリティの名前です。

**Write security name [書き込みセキュリティ名]**：書き込みセキュリティの名前です。

**Security level [セキュリティレベル]**：SNMP マネージャーとエージェント間のセキュリティレベルには、次の 3 つのレベルがあります。

- Noauth [認証なし]：認証も暗号化も行われない
- Auth [認証]：認証は行われるが、暗号化は行われない
- Priv [機密]：認証と暗号化が行われる

**Auth algorithm [認証アルゴリズム]**：認証アルゴリズムです。MD5 と SHA を含みます。

**Auth password [認証パスワード]**：認証パスワード。

**Encry Algorithm [暗号化アルゴリズム]**：暗号化アルゴリズムです。DES と AES を含みます。

**Encry Password [暗号化パスワード]**：暗号化パスワードです。

**SNMP Port [SNMP ポート]**：SNMP のポートです。

## QoS 設定の構成

**Setup [設定] > Network Setup [ネットワーク設定] > QoS [QoS]**に移動します。

Quality of Service (QoS) はネットワークセキュリティメカニズムで、ネットワークの遅延や故障の問題を修正します。ネットワークサービスの場合、サービス品質には、伝送帯域幅、遅延、およびパケット損失などが含まれます。QoS を使用すると、パケットの優先順位付けによって伝送帯域幅を保証し、遅延を減らし、データパケットの損失を減らし、伝送品質を向上させることができます。

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およびルーターには、QoS のサポートが含まれている必要があります。
- ネットワークで使用されるネットワークビデオデバイスは、QoS 対応でなければなりません。

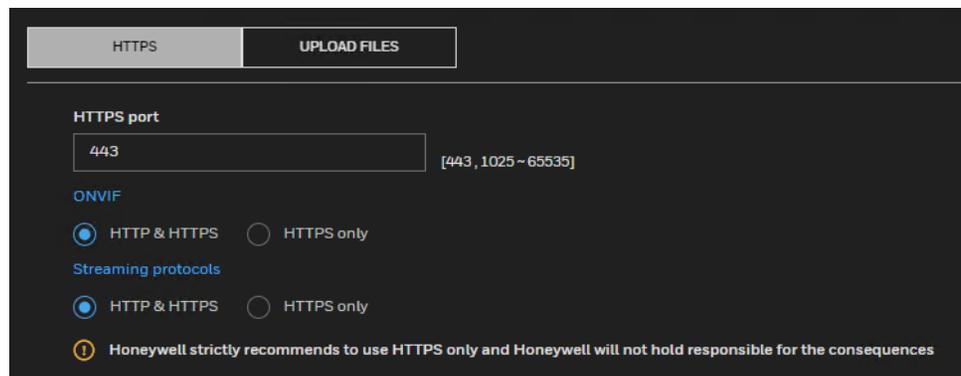
# HTTPS 設定の構成

## HTTPS

Setup [設定] > Network Setup [ネットワーク設定] > HTTPS [HTTPS] > HTTPS [HTTPS]に移動します。

このセクションでは、認証と暗号化通信を有効にする方法について説明します。より高いセキュリティレベルでインターネット上のストリーミングデータ送信を保護するのに役立ちます。

図 26 HTTPS 設定



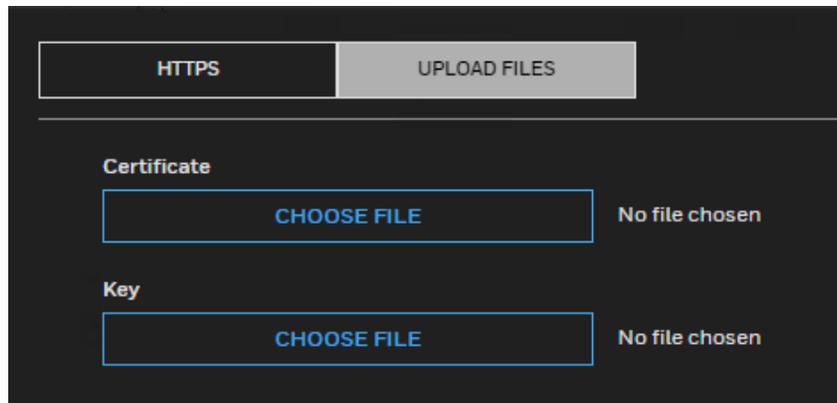
**注記：** Honeywell では、HTTPS only [HTTPS のみ]を使用することを強くお勧めします。

**HTTP & HTTPS：**これを選択すると、HTTP または HTTPS を介して Web ブラウザーにアクセスできます。

**HTTPS only [HTTPS のみ]：**これを選択すると、Web ブラウザーは、より高いセキュリティレベルの HTTPS 経由でのみアクセスできます。

# ファイルのアップロード

Setup [設定] > Network Setup [ネットワーク設定] > HTTPS [HTTPS] > UPLOAD FILES [ファイルのアップロード]に移動します。ここでサードパーティから証明書をインポートできます。



サードパーティから証明書をインポートするには：

1. Certificate [証明書]フィールドで、CHOOSE FILE [ファイルを選択]をクリックして、サードパーティまたは CA ドメインから適用済みの証明書ファイルを選択します。
2. Key [キー]フィールドで、CHOOSE FILE [ファイルの選択]をクリックして、サードパーティまたは CA ドメインから適用済みの証明書キーを選択します。
3. UPLOAD [アップロード]をクリックして、カメラを再起動します。

証明書ファイルが正常にアップロードされた後、証明書を削除する場合は、REMOVE [削除]をクリックします。

- サポートされている証明書の種類：HTTPS プロトコル。
- サポートされている証明書のファイル形式：\*.cert 形式。
- サポートされているキー形式：PEM 形式。

## IEEE 802.1x 設定の構成

Setup [設定] > Network Setup [ネットワーク設定] > 802.1x [802.1x]に移動します。

IEEE802.1xは、ローカルおよびメトロポリタンエリアネットワークのアクセス制御および認証プロトコルで、ポートベースのネットワークアクセス制御プロトコルを使用して、許可されていないユーザーおよび/またはデバイスの LAN へのアクセスを制限します。ネットワークデバイス、中間スイッチ/アクセスポイント/ハブ、RADIUS サーバーは、802.1x 設定をサポートして有効にする必要があります。

IEEE 802.1x 設定を構成するには：

1. カメラを 802.1x で保護されたネットワークに接続する前に、RADIUS サーバーで検証できる認証局（例：ネットワーク管理者）からのデジタル証明書を適用します。
2. カメラを保護された LAN 外の PC またはノートブックに接続します。以下に示すように、カメラの構成ページを開きます。

図 27 IEEE 802.1x 構成 - EAP-TLS

Enable 802.1x

EAP Method  
EAP-TLS

Identity  
[Input field]

Password  
[Input field]

Confirm password  
[Input field]

CA certificate  
[CHOOSE FILE] No file chosen

Client certificate  
[CHOOSE FILE] No file chosen

Client private key  
[CHOOSE FILE] No file chosen

Honeywell strictly recommends not to enable IEEE802.1x and Honeywell won't be responsible for the consequences

**注記：** Honeywell では、IEEE 802.1x を有効にすることはお勧めしません。

EAP 方式として EAP-TLS を選択します。CA が発行した ID とパスワードを入力し、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、カメラを 802.1x 対応スイッチに接続して、保護された LAN に移動します。その後、デバイスは認証を自動的に開始します。

## ビデオ分析の構成

ビデオ分析には、モーション検出、スマートモーション、不正干渉、侵入、マルチロイタリング、人数カウンターなどの機能があります。

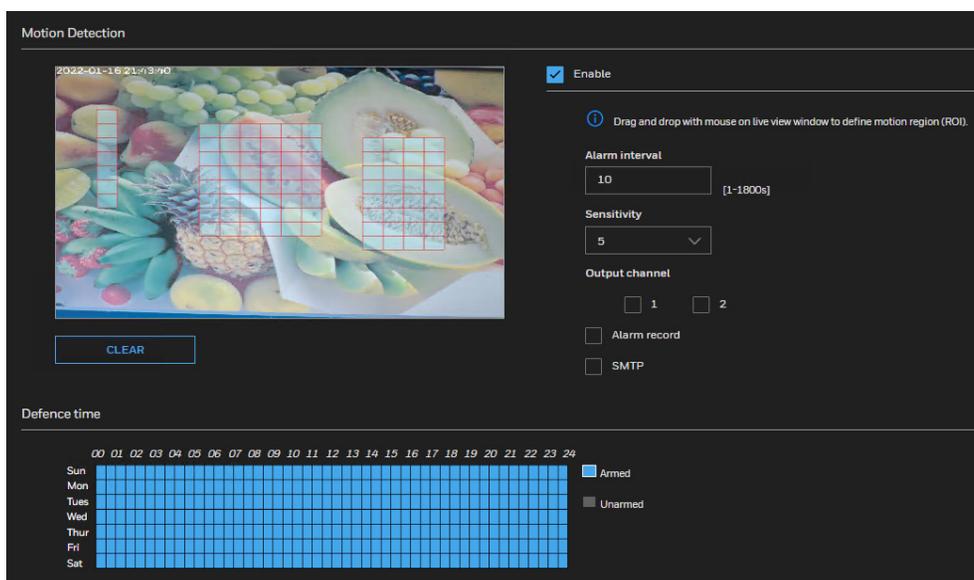
ビデオ分析は、次のオブジェクトの1つまたはグループを検出します。

- 車両
- 人物

## モーション検出

1. Setup [設定] > Video Analytics [ビデオ分析] > Motion Detection [モーション検出] に移動します。

図 28 モーション検出



2. Enable [有効] チェックボックスをオンにして、モーション検出を有効にします。

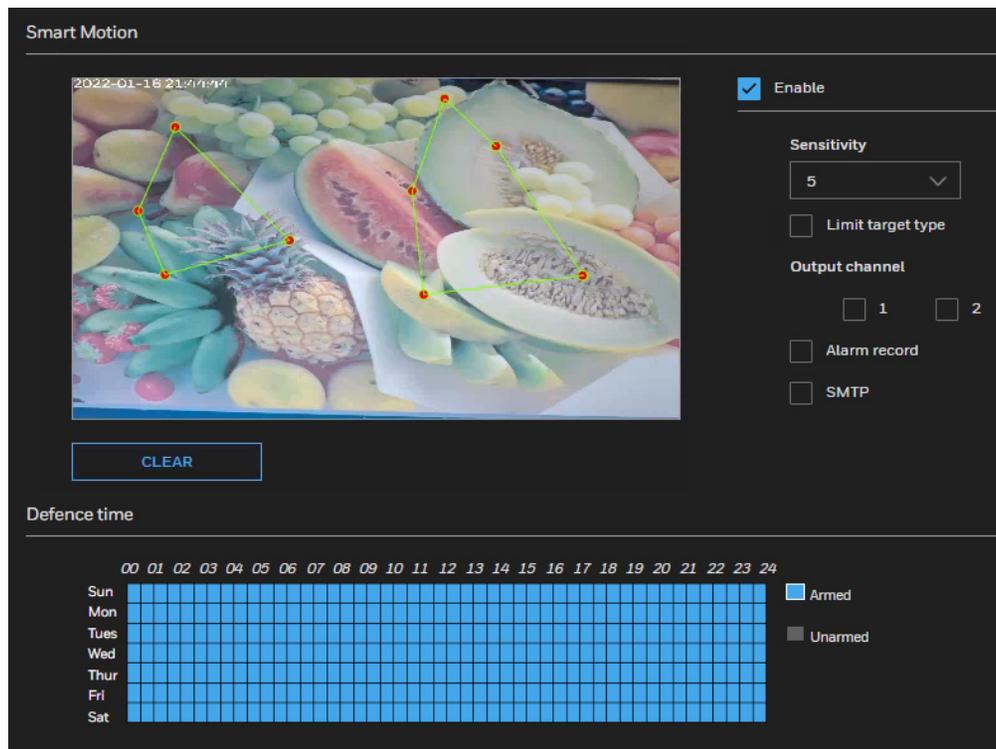
3. Alarm interval [アラーム間隔]と Sensitivity [感度]を構成します。
4. 検出エリアを構成します。
  - 左マウスボタンを押したままビデオエリアをドラッグして、検出エリアを描画します
  - CLEAR [クリア]をクリックして、検出エリアを削除します。
5. Output channel [出力チャンネル]を選択します。
6. チェックボックスをオンにして、アラーム録画と SMTP を有効にします。
7. SAVE [保存]をクリックします。

## スマートモーション検出

スマートモーション検出は、動作中の 1 つまたは複数の検出オブジェクト（人物、PAT、車両）を識別します。適用可能なシナリオには、制限されたエリアでの人物の動作が含まれます。

1. Setup [設定] > Video Analytics [ビデオ分析] > Smart Motion [スマートモーション] に移動します。

図 29 スマートモーション



2. Enable [有効]チェックボックスをオンにして、スマートモーション検出を有効にします。
3. 感度を構成します。
4. 検出エリアを構成します。
  - 左マウスボタンを押したままビデオエリアをドラッグして、検出エリアを描画します
  - CLEAR [クリア]をクリックして、検出エリアを削除します。
5. Output channel [出力チャンネル]を選択します。
6. チェックボックスをオンにして、アラーム録画と SMTP を有効にします。
7. SAVE [保存]をクリックします。

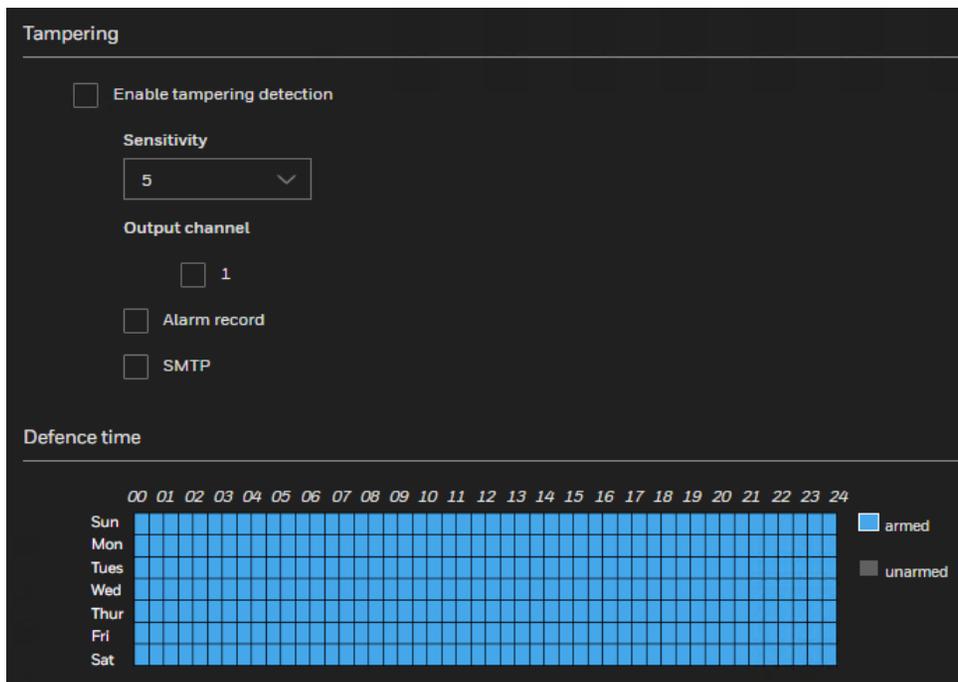
## 不正干渉検出

不正干渉検出は、設定された不正干渉感度の値に基づいてカメラの不正干渉を識別します。

注記： カメラがホーム位置にないため、すべてのVA機能が無効になります。🏠をクリックしてホーム位置に移動してから、不正干渉を設定してください。

1. Setup [設定] > Video Analytics [ビデオ分析] > Tampering [不正干渉]に移動します。

図 30 不正干渉検出



2. Enable [有効]チェックボックスをオンにして、不正干渉検出を有効にします。
3. 感度を構成します。
4. 検出エリアを構成します。
  - 左マウスボタンを押したままビデオエリアをドラッグして、検出エリアを描画します
  - CLEAR [クリア]をクリックして、検出エリアを削除します。
5. Output channel [出力チャンネル]を選択します。
6. チェックボックスをオンにして、アラーム録画と SMTP を有効にします。
7. SAVE [保存]をクリックします。

# 侵入検知

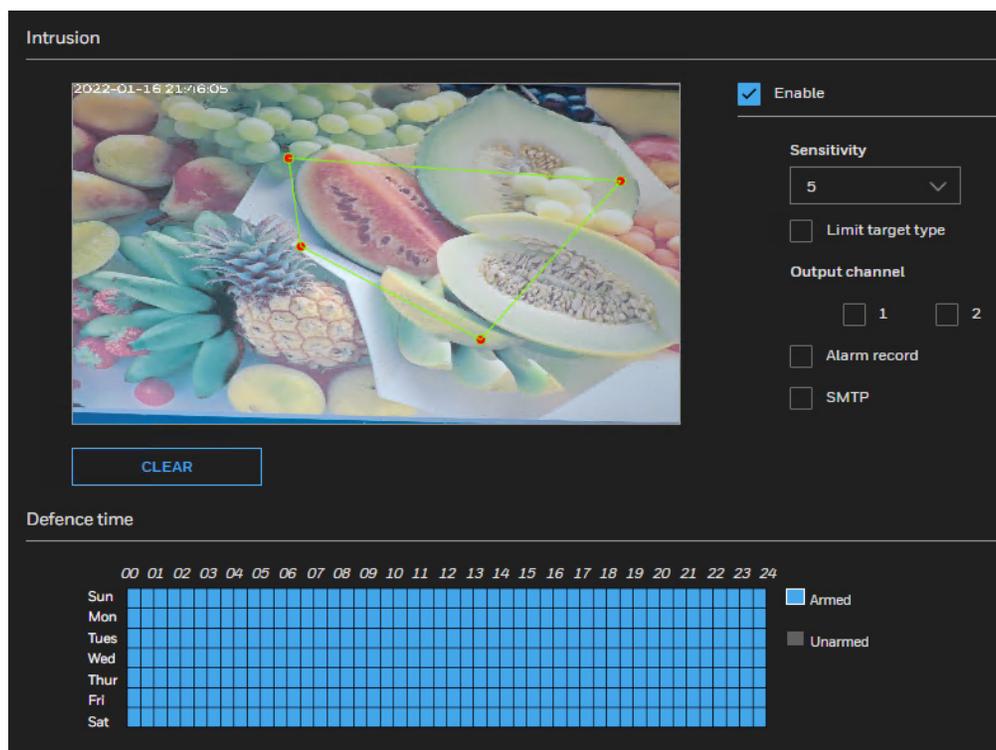
侵入検知を使用して、カメラの視野内で仮想エリアに出入りするオブジェクトを検出できます。

この機能の適用可能なシナリオは次のとおりです。

- 人物が勤務時間後に銀行の金庫室や学校に入ったことを検出します。
- 人物が非常口、非常階段、通常は立ち入り禁止になっている場所から出ることを検出します。

1. Setup [設定] > Video Analytics [ビデオ分析] > Intrusion [侵入]に移動します。

図 31 侵入検知



2. Enable [有効]チェックボックスをオンにして、侵入検知を有効にします。

3. 感度を構成します。

4. 検出エリアを構成します。

- 左マウスボタンを押したままビデオエリアをドラッグして、検出エリアを描画し

ます

- CLEAR [クリア]をクリックして、検出エリアを削除します。
5. Output channel [出力チャンネル]を選択します。
  6. チェックボックスをオンにして、アラーム録画と SMTP を有効にします。
  7. SAVE [保存]をクリックします。

## マルチロイタリング

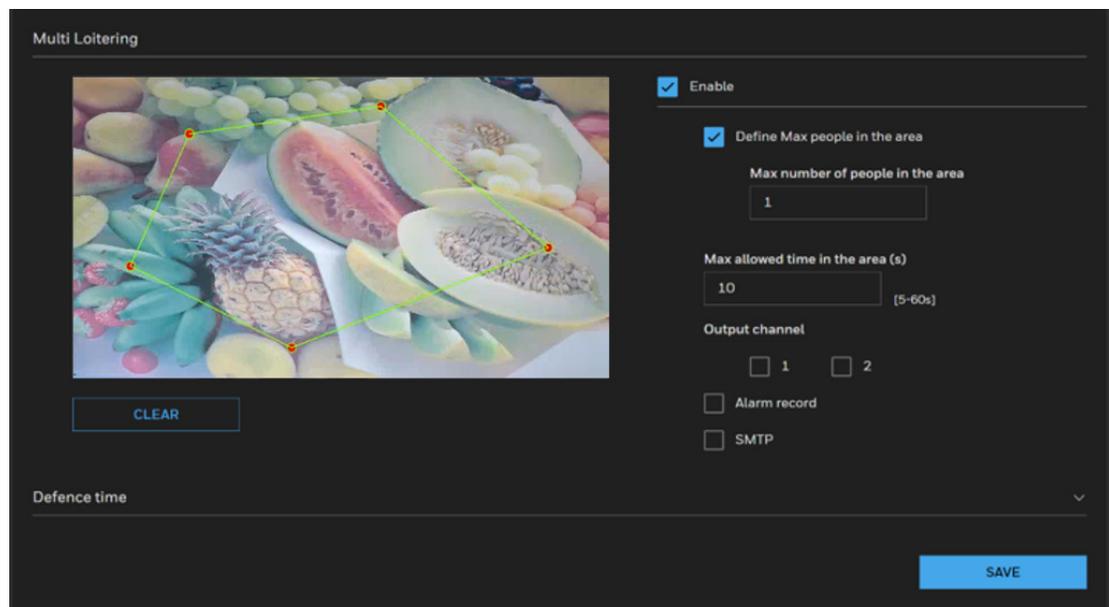
不審行動検出は、事前に設定された時間しきい値よりも長くエリア内に存在する検出オブジェクトまたは検出オブジェクトのグループの検出に使用できます。

この機能の適用可能なシナリオは次のとおりです。

- ATM レーンの接客窓口での人物の不審行動を検出します。
- 店舗の盗難の多いエリアでの人物の不審行動を検出し、破壊行為や侵入を防止します。
- 通常は訪問者がアクセスできないエリアでの人物の不審行動を検出します。

1. Setup [設定] > Video Analytics [ビデオ分析] > Multi Loitering [マルチロイタリング] に移動します。

図 32 マルチロイタリング



2. Enable [有効]チェックボックスをオンにして、マルチロイタリング検出を有効にします。
3. Define Max people in the area [エリア内の最大の人数を定義]のチェックボックスをオンにします。
4. Max number of people in the area [エリア内の最大の人数]を構成します。
5. Max allowed time in the area (s) [エリア内の最大許容時間]を構成します。
6. 検出エリアを構成します。
  - 左マウスボタンを押したままビデオエリアをドラッグして、検出エリアを描画します
  - CLEAR [クリア]をクリックして、検出エリアを削除します。
7. Output channel [出力チャンネル]を選択します。
8. チェックボックスをオンにして、アラーム録画と SMTP を有効にします。
9. SAVE [保存]をクリックします。

## 人数カウンター

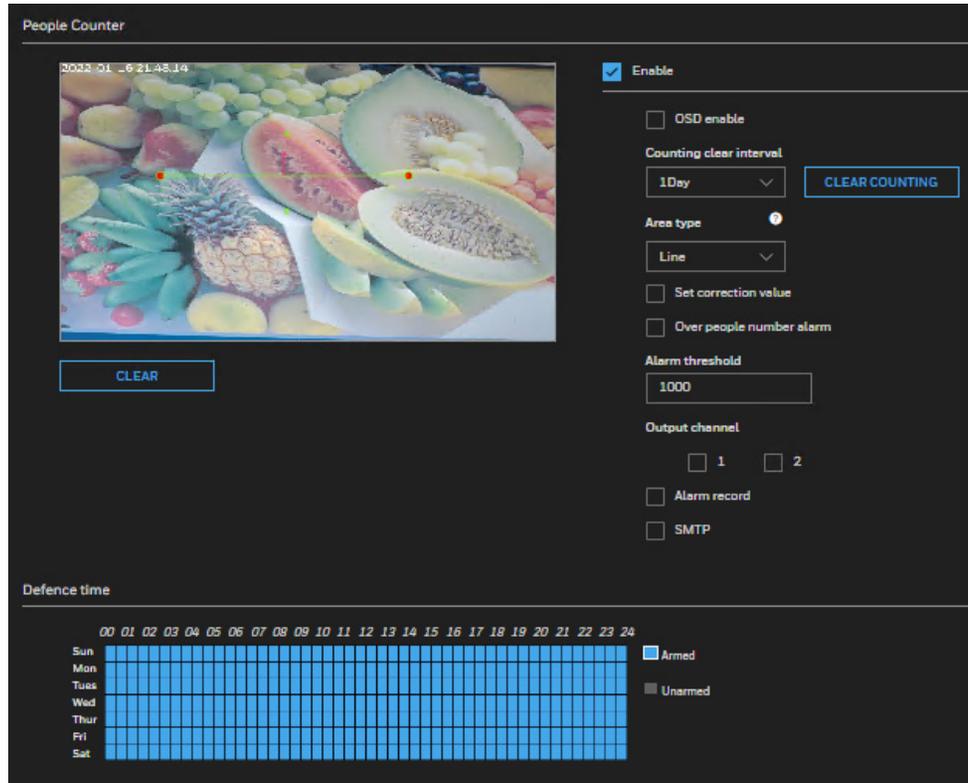
人数カウンターは、視野内に人間の顔が存在することを検出します。この機能の適用可能なシナリオは次のとおりです。

顔の機能を含むビデオフレームにタグを付けることで、管理者は後でこれらの顔が存在するビデオクリップをより効率的に検索できます。何時間も録画を検索する代わりに、顔検出機能を使用すると、録画したビデオのフォレンジック検索を簡単に実行できます。顔の特徴に関係のないオブジェクトは除外されます。

**注記：** 通路モードが有効な場合、人のカウント機能は無効です。

1. Setup [設定] > Video Analytics [ビデオ分析] > People Counter [人数カウンター]に移動します。

図 33 人数カウンター



2. Enable [有効]チェックボックスをオンにして、人数カウンターを有効にします。
3. 検出エリアを構成します。
  - 左マウスボタンを押したままビデオエリアをドラッグして、検出エリアを描画します
  - CLEAR [クリア]をクリックして、検出エリアを削除します。
4. OSD enable [OSD の有効化]チェックボックスをオンにして、人数カウントの OSD 表示を有効にします。
5. Counting clear interval [カウントのクリア間隔]、Area type [エリアタイプ]、Alarm threshold [アラームしきい値]を構成します。
  - a 間隔時間を選択して Counting clear interval [カウントのクリア間隔]を構成すると、カメラは設定された間隔でカウント数をクリアします。現在のカウント数をクリアするには、CLEAR COUNTING [カウントをクリア]をクリックします。
  - b Set correction value [補正値の設定]のチェックボックスをオンにして、インエリアに既に存在するカウント補正を有効にします。すでにインエリアにいる人数を

入力します。

- c Over people number alarm [**人数超過アラーム**]のチェックボックスをオンにして、そこにいる人数が Alarm threshold [**アラームしきい値**]ボックスの人数設定を超えた場合のアラーム機能を有効にします。
6. Output channel [出力チャンネル]を選択します。
7. チェックボックスをオンにして、**アラーム録画**と SMTP を有効にします。
8. SAVE [保存]をクリックします。

## アラームとイベントの構成

ここでは、アラームとイベントの設定について説明します。

### アラーム入力とアラーム出力の構成

Setup [設定] > Alarm & Event [アラームとイベント] > Alarm In and Alarm Out [アラーム入力とアラーム出力]に移動します。

図 34 アラーム入力とアラーム出力

The screenshot displays two configuration sections: "Alarm Input" and "Alarm Output".

**Alarm Input Section:**

- Alarm input
- Name: [Text input field]
- Current mode: [Low] (dropdown menu)
- Output channel:  1
- Alarm record     SMTP
- Defence time: A grid showing days of the week (Sun-Sat) and hours (00-24). The grid is filled with blue squares, indicating the system is armed. A legend on the right shows a blue square for "Armed" and a grey square for "Unarmed".

**Alarm Output Section:**

- Alarm Output
- Name: [Text input field]
- Current signal: [Grounded] (dropdown menu)
- Manual control: [OPEN] [CLOSE] (two buttons)
- Timing alarm output

# アラーム入力

**Alarm input [アラーム入力]**：Alarm input [アラーム入力]のチェックボックスをオンにします。

**Name [名前]**：アラーム入力名を入力します。

**Current mode [現在のモード]**：ドロップダウンリストボックスから現在のモードを選択します。

**Defence time [防護時間]**：次のいずれかの方法を使用して、スケジュールを構成します。

- マウスの左ボタンをクリックして、月曜日から日曜日の 0:00~24:00 の範囲内の任意の時点を選択します。
- マウスの左ボタンを押したままマウスをドラッグして放すと、月曜日から日曜日まで 0:00~24:00 の範囲でスケジュールを選択できます。

**Output channel [出力チャンネル]**：Output channel [出力チャンネル]を選択します。

**Alarm record/SMTP [アラーム録画/SMTP]**：チェックボックスをオンにして、アラーム録画と SMTP を有効にします。

**PTZ linkage [PTZ リンケージ]**：チェックボックスをオンにして、PTZ リンケージを有効にします。

イベントがトリガーされると、システムは設定に従って対応するタイプの移動を実行または停止します。

- **PTZ type [PTZ タイプ]**：Preset [プリセット]、Scan [スキャン]、Patrol [パトロール]、Recording Patrol [録画パトロール]を選択します。
- **Value [値]**：値を選択します。
- **Operate [操作]**：Invoke [起動]、Pause [一時停止]、Continue [続行]を選択します。

**注記：** PTZ リンケージ機能は PTZ モデルにのみ適用されます。

# アラーム出力

**Name [名前]**：アラーム出力名

**Current Signal [現在の信号]**：**Grounded [アース]**または**Open [オープン]**を選択してアラーム出力の正常な状態を定義します。出力ケーブルを外部デバイスに接続すると、カメラはアラームイベント設定に従って現在の信号出力ステータスを報告します。

- **Grounded [アース]**：カメラアラームリレーは**Normal Open [ノーマルオープン]**です。アラームイベントが生成されてトリガーされると、**Grounded/Closed [アース/クローズ]**になります。
- **Open [オープン]**：カメラアラームリレーは**Normal Closed (Grounded) [ノーマルクローズ (アース)]**です。アラームイベントが生成されてトリガーされると、**Open [オープン]**になります。

**注記**： 信号ステータスは、1つのアラーム出力がトリガーされた後に有効になります。

**Manual Control [手動制御]**：アラーム出力信号が発生している場合は、**Close [閉じる]**をクリックしてアラーム出力を無効にするか、**Open [開く]**をクリックしてアラーム出力ステータスを維持します。

アラーム出力信号が発生していない場合は、上記とは逆になります。

**Timing alarm output [タイミングアラーム出力]**：**Timing alarm output [タイミングアラーム出力]**を有効にして、アラーム出力の時間を設定します。選択しているタイムスロットの間、デバイスはアラーム出力をトリガーし続けます。

**注記**： 5M/8M モデル (HC35WX5RX/HC35WX8RX) の場合、アラーム入力とアラーム出力を構成できます。

PTZ モデルの場合、アラーム入力 1/入力 2 およびアラーム出力 1/出力 2 を構成できます。

# SD カードアラームの構成

Setup [設定] > Alarm & Event [アラームとイベント] > SD Card Alarm [SD カードアラーム]に移動します。

**SD card alarm [SD カードアラーム]**：チェックボックスをオンにして SD カードアラームを有効にします。

**Alarm threshold(used space) [アラームしきい値（使用スペース）]**：使用スペースがアラームしきい値に達すると、カメラがアラームを発します。

**Alarm interval [アラーム間隔]**：間隔を設定します。

**Output channel [出力チャンネル]**：チェックボックスをオンにして、出力チャンネルを設定します

## ストレージ設定の構成

### SD カード管理

Setup [設定] > Storage Setup [ストレージ設定] > SD Card Management [SD カード管理] に移動します。

このセクションでは、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。

ここで、SD カードのステータスを表示し、SD カード制御を実装できます。

互換性のある SD カードについては、次の表を参照してください。

表 4 互換性のある SD カード

SD カードブランド	モデル	サイズ
サンディスク	microSDHC A1 C10	16 GB
Kingston	microSDHC V10	16 GB
サンディスク	microSDHC V30	32 GB
サンディスク	microSDXC V30	128 GB
東芝	microSDXC M303 V30	128 GB
Micron	microSDXC A2 C10	128 GB
Samsung	microSDXC C10	256 GB
Kingston	microSDXC V30	256 GB
サンディスク	microSDXC C10	256 GB

- 注記：
- カメラから SD カードを取り外す前に、記録アクティビティをオフにすることをお勧めします。
  - SD カードの寿命は限られています。SD カードの定期的な交換が必要になる場合があります。

- カメラファイルシステムは、数メガバイトのメモリスペースを占有します。ストレージスペースは記録に使用できません。
- 別のデバイスで記録されたデータがすでに含まれている SD カードをこのカメラで使用しないでください。
- SD カード内のフォルダー名を変更または変更しないでください。カメラが誤動作する可能性があります。
- 別のカメラで SD カードを使用する場合は、最初に別のカメラで SD カードをフォーマットします。SD カードをフォーマットする方法については、[64 ページの SD カードのフォーマット](#)を参照してください。

## SD Card Status [SD カードの状態]

このタブには、SD カードのステータスと予約スペースが表示されます。最大 2 枚の SD カードがサポートされています。冗長ストレージモードは、2 枚の SD カードで有効にできます。SD カードを初めて使用するときは、必ず SD カードをフォーマットしてください。[64 ページの SD カードのフォーマット](#)を参照してください。

### 図 35 SD カードなし

SD Card Status			
SD Card Status :	N/A	Total size :	0 MBytes
Free size :	0 MBytes	Used size :	0 MBytes
Alarm threshold(%) :	100%		

### 図 36 SD カードあり

SD Card Status			
SD Card Status :	Usable	Total size :	7360 MBytes
Free size :	2880 MBytes	Used size :	4480 MBytes
Alarm threshold(%) :	50%	File system :	Ext4

SD Card Format	
SD card(s):	<input type="text" value="SD Card 1"/>

## SD カードのフォーマット

SD カードをフォーマットするには、SD カードを選択し、FORMAT [フォーマット]をクリックします。

### SD カードの挿入/取り外し

SD カードをカメラに挿入したり、カメラから取り外したりする際には、次の手順を適用します。



**注意：**フォーマット中はSD カードを取り外さないでください。



**警告：**連続録画などの録画が実行されているかどうかを確認し、SD カードを取り外す前にイベントまたは録画ルールを無効にします。カメラからSDカードを取り外したときに録画がオンになっていた場合は、カメラに再挿入した後にSDカードのステータスが未フォーマットになります。

## コンテンツ管理

Setup [設定] > Storage Setup [ストレージ設定] > Content Management [コンテンツ管理]に移動します。

このセクションでは、カメラで録画したビデオのコンテンツを管理する方法について説明します。ここで、レコードを検索および表示し、検索結果を表示できます。

## 記録の検索と表示

このタブを使用すると、ユーザーは記録されたデータの検索条件を設定できます。条件を選択せずに **SEARCH [検索]**をクリックすると、記録されたすべてのデータが **Search Results [検索結果]**タブに一覧表示されます。

Search

Trigger type

All type

Time Search for last

1

MINUTE(S) HOURS DAYS WEEKS

From / To

01/11/2022 04:43 PM

01/18/2022 04:43 PM

SEARCH

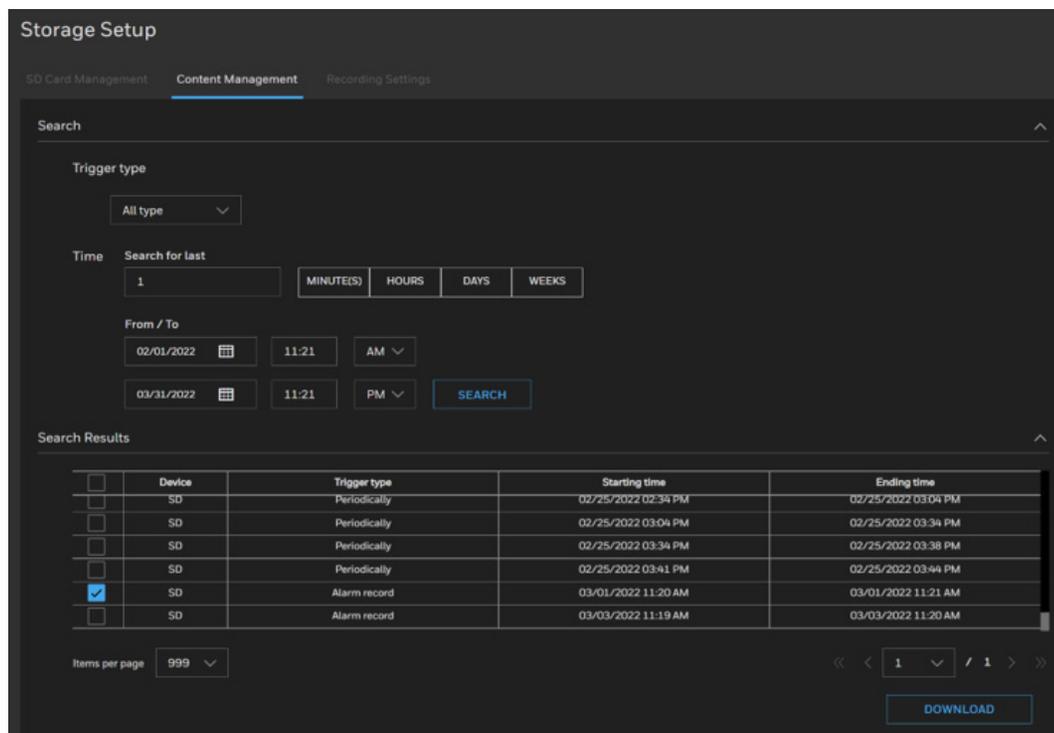
- **Trigger type [トリガータイプ]**：バックアップ、システム起動、アラーム入力、モーション、ネットワーク障害、録画通知、定期的、不正干渉検出、VADP から 1 つ以上のトリガーを選択します。
- **Time [時間]**：特定の時点で作成されたコンテンツを検索する時間範囲を手動で入力します。

**SEARCH [検索]**をクリックすると、検索条件に対応する記録データが **Search Results [検索結果]**タブに一覧表示されます。

## 検索結果

検索結果を並べ替えるには、各列ヘッダーをクリックします。

**Download [ダウンロード]**：検索結果をクリックして **Download [ダウンロード]**をクリックすると、ファイルを保存するためのファイルダウンロードウィンドウが表示されます。VLC プレーヤーでビデオクリップを再生できます。

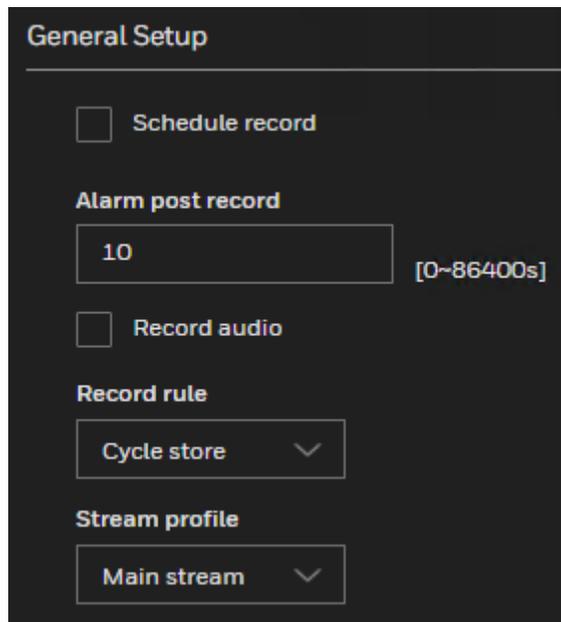


注記： トリガータイプでソートされたアラーム録画は、定期的な録画ではなく、アラームタイプの録画です。これには、モーションアラーム、I/O アラーム、侵入アラーム、マルチロイタリングアラーム、スマートモーションアラーム、カメラ改ざんアラーム、人数しきい値アラームが含まれます。

## 録画設定

Setup [設定] > Storage Setup [ストレージ設定] > Recording Settings [録画設定]に移動します。

このセクションでは、カメラの録画を設定する方法について説明します。



**Schedule record [録画のスケジュール]**：時間ポリシーを構成できる録画のスケジュールを有効にします。

**Alarm post record [アラーム事後録画]**：アラームが生成された後の録画時間（秒単位）です。

**Record audio [オーディオの録音]**：オーディオを録画と一緒に録音するかどうかを示します。

**Record rule [録画ルール]**：録画を保存するためのルールです。オプションは次のとおりです。

Cycle Store [繰り返し保存]：録画を繰り返して保存します。

Save Days [保存日数]：録画を保存する期間（日数）です。期間は最大 99999 日です。値 0 は、録画が上書きされないことを示します。

Stream profile [ストリームプロファイル]：ドロップダウンリストから次を選択します。メインストリーム、サブストリーム、サードストリーム。

**注記：** 上記の設定は、すべてのビデオ録画動作にグローバルに適用されます。

**Defence time [防護時間]**：マウスを左クリックまたはドラッグして、月曜日から日曜日の 0：00～24：00 までの任意の時間を選択します。

## システム設定の構成

### システムの一般設定の構成

Setup [設定] > System Setup [システム設定] > General Settings [一般設定]に移動します。  
このセクションでは、ホスト名やシステム時刻など、カメラの基本設定を構成する方法について説明します。

図 37 システムの一般設定

The screenshot displays the 'System Setup' configuration page. It is divided into two main sections: 'Camera name' and 'System Time'.  
In the 'Camera name' section, there is a text input field containing 'HC35WE5R3' and a 'SAVE NAME' button.  
The 'System Time' section includes:  
- A 'Time zone' dropdown menu set to 'GMT Casablanca, Greenwich Mean Time:Dublin, Edinburgh, Lisbon, London'.  
- An unchecked checkbox for 'Daylight savings time'.  
- A 'SAVE' button.  
- 'Device time' displayed as '2000/01/05 01:12:08'.  
- 'Current PC time' displayed as '2022/01/18 16:59:47' with a 'SYNCHRONIZE' button.  
- A 'Set manually' section with a date input field (2000/1/5), a time input field (01:11:26), and a 'SYNCHRONIZE' button.  
- An unchecked checkbox for 'NTP' and a 'SAVE' button.

**Camera Name [カメラ名]**：カメラの名前を入力します。テキストはメインページの上部に表示されます。

**Time zone [タイムゾーン]**：ドロップダウンリストから適切なタイムゾーンを選択します。夏季時間規則をアップロードする場合は、69 ページのメンテナンス設定の構成を参照してください。

**Daylight savings time [夏季時間]**：夏季時間を有効にし、DST 開始時刻と終了時刻を指定するには、このチェックボックスをオンにします。

- DST 開始時刻になると、デバイスの時刻は自動的に 1 時間先に進みます。
- DST 終了時刻になると、デバイスの時刻は自動的に 1 時間前に戻ります。

**Device time [デバイスの時刻]**：デバイスの表示時間です。

**Current PC time [現在の PC 時間]**：現在の PC の時刻です。

**Set manually [手動設定]**：デバイスの時刻を手動で設定できます。

**NTP [NTP]**：NTP サーバーの IP アドレスまたはドメイン名です。チェックボックスをオンにして、NTP を有効にします。

**NTP server addr [NTP サーバアドレス]**：NTP サーバーの IP です。

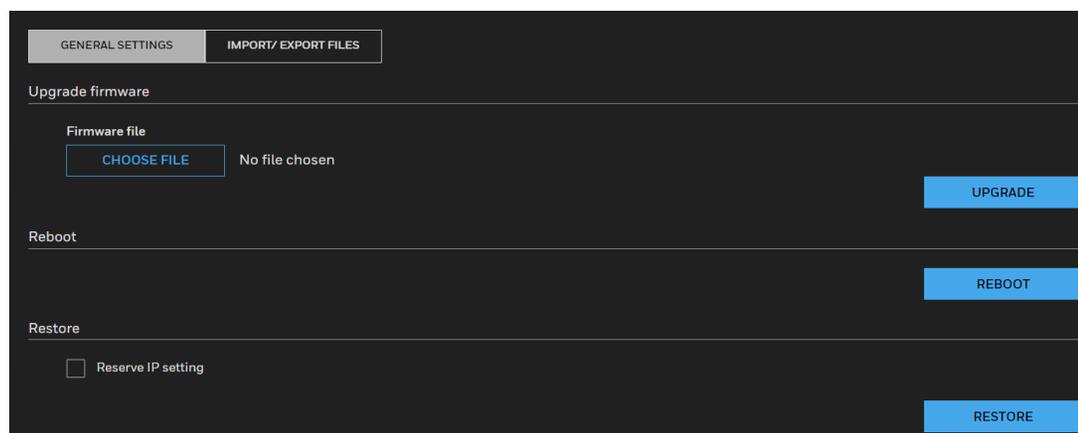
**NTP Port [SNMP ポート]**：NTP サーバーのポート番号です。

**Check the time interval( at least 10 s) [時間間隔 (10 秒以上) を確認]**：デバイスの時刻が NTP サーバーの時刻と同期しているかどうかを確認する時間間隔を設定します。

## メンテナンス設定の構成

**Setup [設定] > System Setup [システム設定] > Maintenance [メンテナンス]**に移動します。

この章では、カメラを工場出荷時のデフォルトに復元する方法、ファームウェア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。



# Upgrading Firmware [ファームウェアのアップグレード]

このページでは、カメラのファームウェアをアップグレードできます。プロセスを完了するには数分かかります。

- 注記：**
- **アップグレード中はカメラの電源を切らないでください。**
  - **カメラで SD カードが使用されている場合、アップグレードの前に必要に応じて SD カードの内容をバックアップしてください。**

以下の手順に従って、ファームウェアをアップグレードします。

1. CHOOSE FILE [ファイルを選択]をクリックして、ファームウェアファイルを見つけます。
  2. UPGRADE [アップグレード]をクリックします。カメラはアップグレードを開始し、アップグレードが完了すると自動的に再起動します。
- カメラで SD カードを使用している場合、アップグレード後に自動的にフォーマットされます。フォーマットには 5~20 分かかる場合があります。
  - SD カードはフォーマット後、暗号化され、そのコンテンツは他のカメラで読み取ることができません。
  - 別のカメラで SD カードを使用する場合は、最初に別のカメラで SD カードをフォーマットします。SD カードをフォーマットする方法については、[64 ページの SD カードのフォーマット](#)を参照してください。
  - カメラに挿入された新しい SD カードも、カメラのアップグレード後に自動的にフォーマットされます。
  - アップグレードが成功すると、「Reboot system now!! This connection will close」 [今すぐシステムを再起動してください!!この接続は解除されます]というメッセージが表示されます。その後、カメラに再度アクセスします。SD カードがカメラに挿入されている場合、SD カードのフォーマットが完了するまで待ちます。

## カメラの再起動

このページで、カメラを再起動できます。完了するには約 1 分かかります。完了すると、ライブビデオページがブラウザーに表示されます。

再起動後に接続に失敗した場合は、アドレスフィールドにカメラの IP アドレスを手動で入力して接続を再開します。

## Restoring the Camera [カメラの復元]

カメラを工場出荷時のデフォルト設定に復元します。

**Network Setup [ネットワーク設定]**：ネットワークタイプの設定を保持する場合にオンにします（[36 ページのネットワークの一般設定の構成](#)を参照）。

**Daylight Saving Time [夏季時間]**：夏季時間の設定を保持する場合はオンにします（[71 ページのファイルのインポート/エクスポート](#)を参照）。

**Focus position [焦点位置]**：オンにして、以前に保存した位置パラメーターを使用して、レンズの焦点位置を保持します。

オプションが選択されていない場合、すべての設定が工場出荷時のデフォルトに復元されます。RESTORE [復元]をクリックすると、カメラが再起動します。

完了すると、ライブビデオページがブラウザーに表示されます。

再起動後に接続に失敗した場合は、アドレスフィールドにカメラの IP アドレスを手動で入力して接続を再開します。

## ファイルのインポート/エクスポート

夏季時間規則、カスタム言語ファイル、構成ファイル、サーバステータスレポートをエクスポート/アップロードします。

GENERAL SETTINGS    IMPORT/ EXPORT FILES

Export Files

CA certificate

EXPORT

Export configuration file

EXPORT

Password for exporting configuration file

Upload Files

Upload configuration file

CHOOSE FILE    No file chosen    UPLOAD

Password for uploading configuration file

*i* The configuration upload is successful, the device will restart

## CA 証明書のエクスポート

カメラは、訪問した Web サイトとサーバーの ID を確認し、クライアントとサーバー間で交換されるデータを暗号化する安全な通信プロトコルである HTTPS を使用します。カメラの Web クライアントに初めてログインすると、一部のブラウザより接続がプライベート/セキュアではないという警告が表示されることがあります。Web クライアントにアクセスするには、Honeywell が署名したセキュリティ証明書をインストールする必要があります。

1. Export [エクスポート]をクリックして、ルート証明書 (ca.crt) をローカルコンピュータに保存します。

2. 証明書を保存したディレクトリに移動し、証明書をダブルクリックします。Certificate [証明書]ウィンドウが開きます。
3. Certificate [証明書]ウィンドウの General [全般]タブで、Install Certificate [証明書のインストール]をクリックして、Certificate Import Wizard [証明書インポートウィザード]を開きます。
4. Next [次へ]をクリックして続行してください。
5. Place all certificates in the following store [すべての証明書を次のストアに配置する]、Browse [参照]、Trusted Root Certification Authorities [信頼されたルート証明機関]の順にクリックし、OK [OK]をクリックします。
6. Next [次へ]をクリックし、Finish [完了]をクリックして Certificate Import Wizard [証明書インポートウィザード]を閉じます。確認ダイアログボックスが表示され、The import was successful [インポートが成功しました]というメッセージが表示されます。
7. OK [OK]をクリックし、もう一度 OK [OK]をクリックして Certificate [証明書]ウィンドウを閉じます。これにより、ブラウザの接続がプライベート/安全ではないという警告は表示されなくなります。

カメラとの安全な通信を確保し、Web ページのナビゲーションの遅延を避けるために、証明書をインストールしてください。

## 構成ファイルのエクスポート

カメラおよびユーザー定義スクリプトのすべてのパラメータをエクスポートするには、EXPORT [エクスポート]をクリックします。

**注記：** ユーザーは、構成ファイルをエクスポートする前にパスワードを指定する必要があります。

## 構成ファイルのアップロード

以下の手順に従って、構成ファイルをアップロードします。

1. 構成ファイルをアップロードするためのパスワードを入力します。パスワードは、エクスポート用に設定した構成ファイルのパスワードと同じである必要があります。そうでない場合、アップロードは失敗します。たとえば、構成ファイル A にパスワード A を設定し、構成ファイル B にパスワード B を設定した場合。構成ファイル B をアップロードするときは、パスワード B を使用する必要があります。
2. CHOOSE FILE [ファイルを選択]をクリックして構成ファイルを見つけ、UPLOAD [アップロード]をクリックして構成ファイルをアップロードします。

デバイスのモデルとファームウェアのバージョンは、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 またはその他の特別な設定を行っている場合、構成ファイルを更新することはお勧めしません。

ファームウェアのアップグレード中に電源が切断されるか、異常な LED ステータスの原因となる不明な理由があるために、復元で正常な動作状態を回復できない場合、次の手順を実行して、バックアップファームウェアでカメラをアクティブ化できます。

- a) リセットボタンを少なくとも 1 分間押し続けます。
- b) 赤い LED がすばやく点滅するまでカメラの電源を入れます。
- c) 起動後、カメラがハングする前にファームウェアが以前のバージョンに戻るはずです。（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 ステータスは正常に戻ります。

## ユーザーアカウント設定の構成

Setup [設定] > System Setup [システム設定] > User Accounts [ユーザーアカウント]に移動します。

このセクションでは、複数のアカウントを作成し、これらのアカウントに特権を付与する方法について説明します。

# アカウント管理

Account Management

– New user –

User name

Password

Confirm password

Privilege

Administrators

ⓘ The password must be between 8 to 20  
ⓘ Upper & lower case letters  
ⓘ At least one number  
ⓘ One of the symbols: ~!@#\$%^&\*~!@#\$%^&  
ⓘ The first character must be a number or letter  
ⓘ No space

DELETE ADD UPDATE

管理者アカウント名は「admin」であり、これは常設で削除できません。

管理者は、最大20個のユーザーアカウントを作成できます。新しいユーザーを作成するには次の手順を実行します。

1. ドロップダウンリストから New user [新しいユーザー]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、パスワードを確認します。すべてではありませんが、一部の特殊な ASCII 文字がサポートされています。パスワードの組み合わせで「!@#\$%&+=\*\_~`~`」を使用できます。
3. 新しいユーザーアカウントの特権レベルを選択します。ADD [追加]をクリックして設定を有効にします。

特権レベルは次のとおりです。

役割	特権
管理者	完全なコントロール
Viewer [ビューワー]	ライブ、言語

アクセス権は、ユーザー特権（管理者、操作者、ビューワー）でソートされます。管理者のみが設定ページにアクセスできます。ビューワーは、ライブビューのメインページにのみアクセスできます。

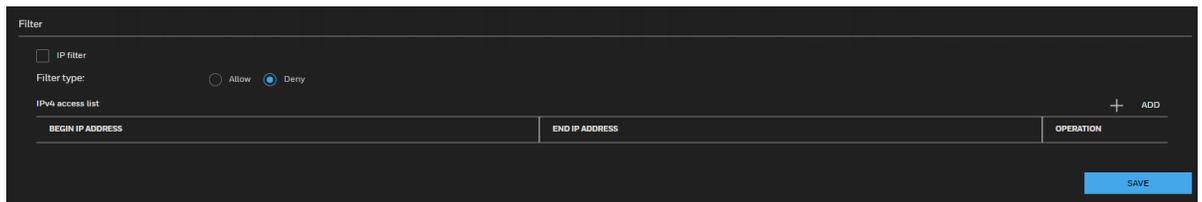
ユーザーのアクセス権を変更するか、ユーザーアカウントを削除するには次の手順を実行します。

1. 既存のアカウントを選択します。
2. 必要な変更を行い、UPDATE [更新]をクリックして設定を有効にするか、DELETE [削除]をクリックしてアカウントを削除します。

# アクセスリスト設定の構成

Setup [設定] > System Setup [システム設定] > Access List [アクセスリスト]に移動します。

このセクションでは、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。



**IP filter [IP フィルター]**：この項目をチェックし、SAVE [保存]をクリックして、IP フィルタリング機能を有効にします。

**Filter type [フィルタータイプ]**：フィルターの種類として **Allow [許可]**または **Deny [拒否]**を選択します。Allow Type [許可タイプ]を選択すると、IP アドレスが以下のアクセスリストにあるクライアントのみが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ません。逆に、Deny Type [拒否タイプ]を選択すると、IP アドレスが以下のアクセスリストにあるクライアントはカメラへのアクセスを許可されず、他のクライアントはアクセスできます。

**ADD [追加]**をクリックすると、フィルタアドレスを追加できます。

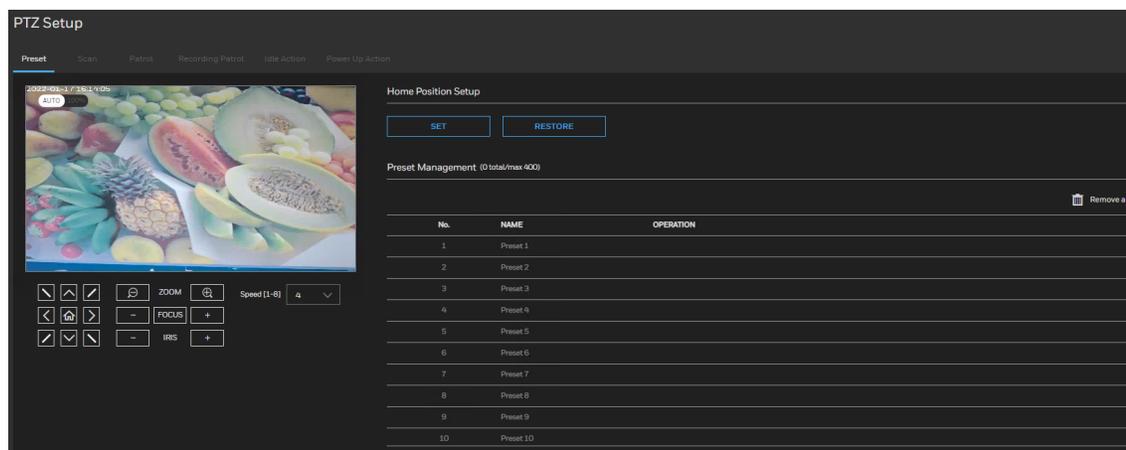
- 注記：**
- Network [ネットワーク]ページで IPv6 を有効にしない限り、IPv6 access list [IPv6 アクセスリスト]列は表示されません。IPv6 設定の詳細については、49 ページの「IPv6 の有効化」を参照してください。
  - Range [範囲]規則は IPv4 アドレスにのみ適用されます。

このセクションでは、カメラのパン/チルト/ズーム操作を制御する方法について説明します。

## プリセット

Setup [設定] → PTZ Setup [PTZ 設定] → Preset [プリセット]に移動します。

図 38 プリセット設定



ボタンをクリックして、ビデオ画像を上/下/左/右/45 度チルトに移動し、 をクリックしてホーム位置に戻ります。

**ZOOM [ズーム]** :  をクリックしてビデオ画像をズームアウトするか、 をクリックしてビデオ画像をズームインします。

**FOCUS [フォーカス]** :  と  をクリックして **Focus [フォーカス]** 設定を調整します。

IRIS [アイリス]：**[-]**と**[+]**をクリックして IRIS [アイリス]設定を調整します。

Speed [1-8] [速度 (1~8) ]：カメラビューの移動速度を選択します。速度の範囲は 1~8 で、デフォルト設定は 5 です。

### ホーム位置の設定

- **SET [設定]**：クリックして、現在位置をホームロケーションとして設定します。
- **RESTORE [復元]**：クリックして、ホーム位置をデフォルトに戻します。

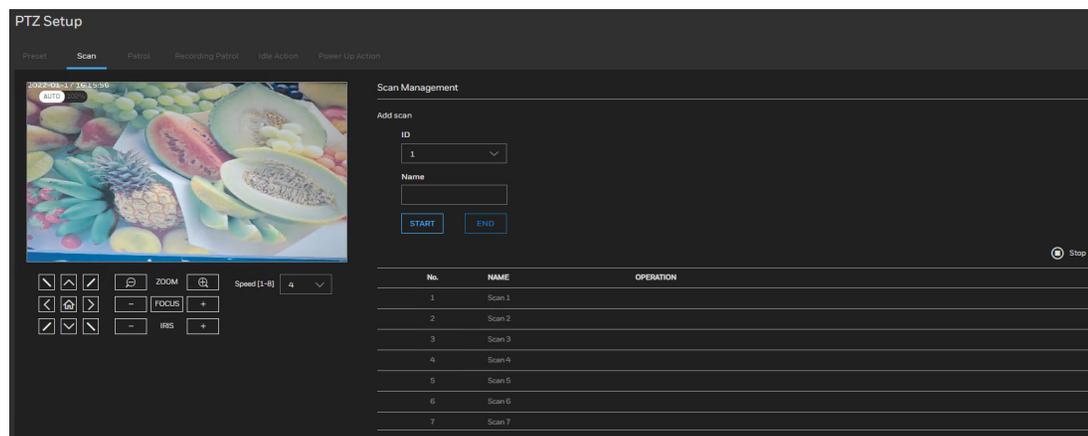
### プリセット管理

- すべてのプリセットリストを削除するには、**Remove all [すべて削除]**をクリックします。
-  をクリックすると、このプリセットに移動します。
-  をクリックすると、このプリセットが現在の位置に置き換えられます。
-  をクリックすると、プリセットが削除されます。

## スキャン管理

Setup [設定] → PTZ Setup [PTZ 設定] → Scan [スキャン]に移動します。

図 39 スキャン設定



ボタンをクリックして、ビデオ画像を上/下/左/右/45 度チルトに移動し、 をクリックしてホーム位置に戻ります。

**ZOOM [ズーム]**：をクリックしてビデオ画像をズームアウトするか、をクリックしてビデオ画像をズームインします。

**FOCUS [フォーカス]**：とをクリックして **Focus [フォーカス]**設定を調整します。

**IRIS [アイリス]**：とをクリックして **IRIS [アイリス]**設定を調整します。

**Speed [1-8] [速度 (1~8)]**：カメラビューの移動速度を選択します。速度の範囲は 1~8 で、デフォルト設定は 5 です。

### スキャン管理

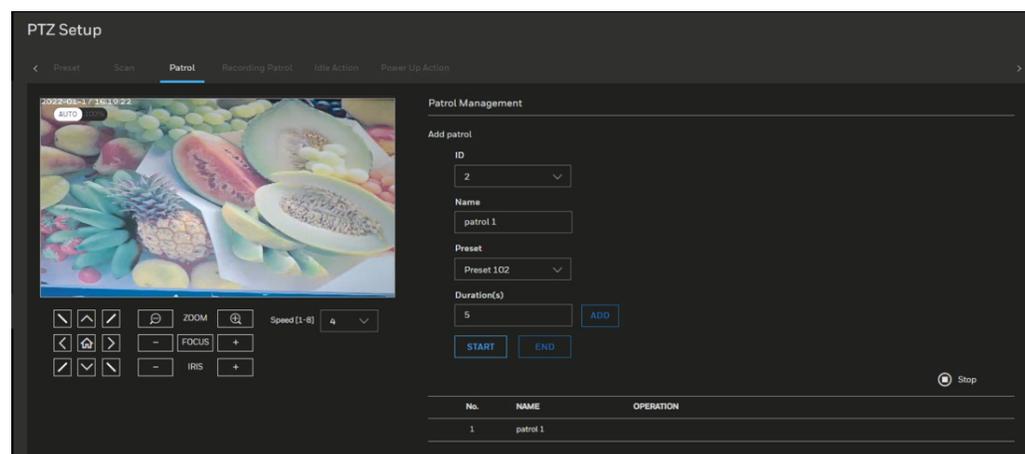
**Add scan [スキャンの追加]**：スキャン ID と名前を設定します。**START [開始]**をクリックして録画を開始します。**END [終了]**をクリックして録画を終了します。

- をクリックすると、このスキャンが開始されます。
- をクリックすると、スキャン設定が停止します。
- をクリックすると、スキャンが削除されます。

## パトロール

Setup [設定] → PTZ Setup [PTZ 設定] → Patrol [パトロール]に移動します。

図 40 パトロール設定



：ボタンをクリックして、ビデオ画像を上/下/左/右/45 度チルトに移動し、をクリックしてホーム位置に戻ります。

**ZOOM [ズーム]**：をクリックしてビデオ画像をズームアウトするか、をクリックしてビデオ画像をズームインします。

**FOCUS [フォーカス]**：とをクリックして **Focus** [フォーカス]設定を調整します。

**IRIS [アイリス]**：とをクリックして **IRIS** [アイリス]設定を調整します。

**Speed [1-8] [速度 (1~8) ]**：カメラビューの移動速度を選択します。速度の範囲は1~8で、デフォルト設定は5です。

### パトロール管理

**Add patrol [パトロールの追加]**：パトロール ID/名前/プリセット/期間を設定します。

**START [開始]**をクリックして録画を開始します。**END [終了]**をクリックして録画を終了します。

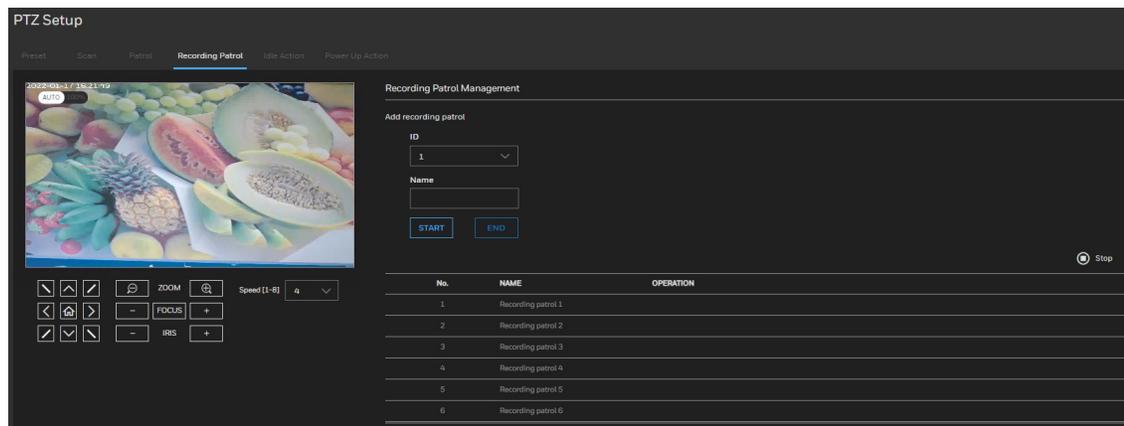
- をクリックして、録画したパトロールをレビューします。
- をクリックして、パトロールのレビューを停止します。
- をクリックして、パトロールを削除します。

このパトロールリストには、構成済みのパトロールが表示されます。一度に1つのパトロールのみ適用できることに注意してください。

## パトロールの録画

**Setup [設定] → PTZ Setup [PTZ の設定] → Recording Patrol [パトロールの録画]**に移動します。

図 41 パトロールの録画



ボタンをクリックして、ビデオ画像を上/下/左/右/45 度チルトに移動し、 をクリックしてホーム位置に戻ります。

**ZOOM [ズーム]** :  をクリックしてビデオ画像をズームアウトするか、 をクリックしてビデオ画像をズームインします。

**FOCUS [フォーカス]** :  と  をクリックして **Focus [フォーカス]** 設定を調整します。

**IRIS [アイリス]** :  と  をクリックして **IRIS [アイリス]** 設定を調整します。

**Speed [1-8] [速度 (1~8) ]** : カメラビューの移動速度を選択します。速度の範囲は 1~8 で、デフォルト設定は 5 です。

### パトロールの録画の管理

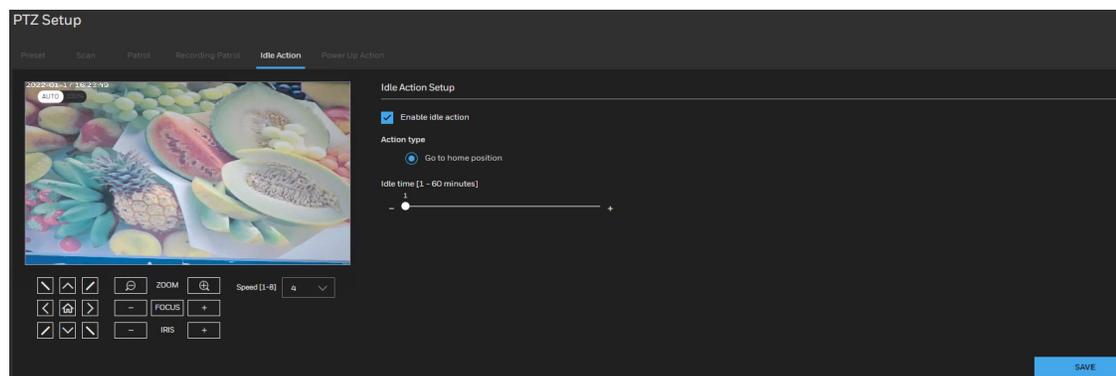
**Add recording patrol [パトロールの録画の追加]** : パトロールの録画 ID と名前を設定します。**START [開始]** をクリックして録画を開始します。**END [終了]** をクリックして録画を終了します。

-  をクリックして、パトロールの録画をレビューします。
-  をクリックして、パトロールの録画のレビューを停止します。
-  をクリックして、パトロールの録画を削除します。

# アイドルアクション

Setup [設定] → PTZ Setup [PTZ の設定] → Idle Action [アイドルアクション]に移動します。

図 42 アイドルアクション



：ボタンをクリックして、ビデオ画像を上/下/左/右/45 度チルトに移動し、 をクリックしてホーム位置に戻ります。

**ZOOM [ズーム]**： をクリックしてビデオ画像をズームアウトするか、 をクリックしてビデオ画像をズームインします。

**FOCUS [フォーカス]**： と  をクリックして **Focus [フォーカス]** 設定を調整します。

**IRIS [アイリス]**： と  をクリックして **IRIS [アイリス]** 設定を調整します。

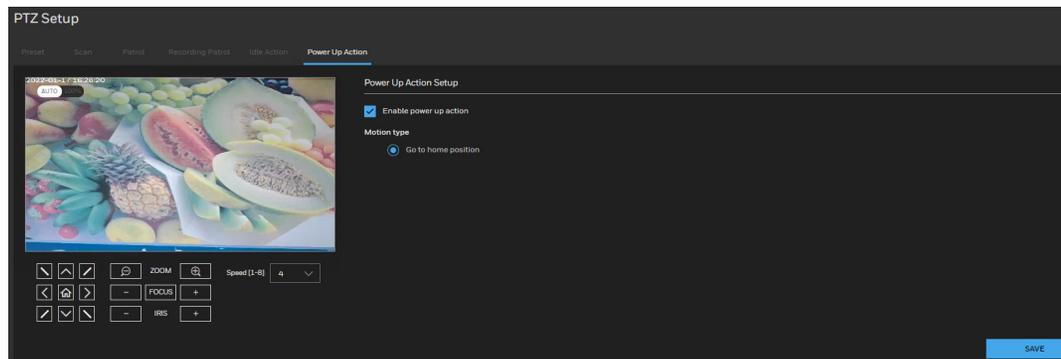
**Speed [1-8] [速度 (1~8)]**：カメラビューの移動速度を選択します。速度の範囲は 1~8 で、デフォルト設定は 5 です。

チェックボックスをオンにして、アイドルアクションを有効にします。アイドル時間を設定します。**SAVE [保存]** をクリックします。

# パワーアップアクション

Setup [設定] → PTZ Setup [PTZ の設定] → Power Up Action [パワーアップアクション]に移動します。

図 43 パワーアップアクション



ボタンをクリックして、ビデオ画像を上/下/左/右/45 度チルトに移動し、 をクリックしてホーム位置に戻ります。

**ZOOM [ズーム]**:  をクリックしてビデオ画像をズームアウトするか、 をクリックしてビデオ画像をズームインします。

**FOCUS [フォーカス]**:  と  をクリックして **Focus [フォーカス]** 設定を調整します。

**IRIS [アイリス]**:  と  をクリックして **IRIS [アイリス]** 設定を調整します。

**Speed [1-8] [速度 (1~8)]**: カメラビューの移動速度を選択します。速度の範囲は 1~8 で、デフォルト設定は 5 です。

チェックボックスをオンにして、パワーアップアクションを有効にします。**SAVE [保存]** をクリックします。

## ログ

Setup [設定] > Information [情報] > Logs [ログ]に移動します。

## 操作ログ

オペレーションログには、デバイスの実行中にユーザー操作とスケジュールされたタスクコマンドが記録されます。オペレーションログは、権限管理、システムメンテナンス、デバイス構成、録画操作、ビデオ制御、リアルタイムビデオのタイプに分類できます。



1. ドロップダウンリストボックスから、クエリーを実行するオペレーションログのタイプを選択します。
2. 必要に応じて開始時刻と終了時刻を設定します。
3. SEARCH [保存]をクリックします。  
操作ログが表示されます。
4. ページの右側にある Download [ダウンロード]をクリックして、オペレーションログをダウンロードします。

## アラームログ

アラームログには、セキュリティ、ディスク、録画アラームなどのデバイスで生成されたアラームに関する情報が記録されます。

1. ドロップダウンリストボックスから、クエリーを実行するアラームログのタイプを選択します。
2. 必要に応じて開始時刻と終了時刻を設定します。
3. SEARCH [保存]をクリックします。
4. アラームログが表示されます。
5. ページの右側にある Download [ダウンロード]をクリックして、オペレーションログをダウンロードします。

## ログの収集

デバイスで発生する可能性のある問題の分析および解決に役立つデバイスに関するログを、1回のクリックで収集できます。

1. COLLECT [収集]をクリックすると、ダウンロードページが表示されます。
2. ログを保存するパスを選択します。

## バージョン

Setup [設定] > Information [情報] > Version [バージョン]に移動します。

Version [バージョン]ページで、ソフトウェアバージョンを表示できます。

## 一般的な問題のトラブルシューティング

パフォーマンスの問題を解決するには、次のガイドラインを参照してください。さらにサポートが必要な場合は、Honeywell テクニカルサポートにご連絡ください（連絡先情報は裏面に記載されています）。

表 5 一般的な問題のトラブルシューティング

問題	解決策
電源が不安定。	UPS 電源の使用を強く推奨します。
カメラの Web ページが異常な表示になる。	ブラウザのキャッシュをクリアします。 <ul style="list-style-type: none"><li>PC 画面の幅が 1366px の場合は、ブラウザを 80%にズームすることをお勧めします。</li><li>PC 画面の幅が 1920px の場合は、ブラウザを 100%にズームすることをお勧めします。</li></ul>

## 記号の一覧

以下は、カメラに表示される可能性のある記号の一覧です。

表 6 記号の一覧

記号	説明
	<p>WEEE 記号。</p> <p>この記号は、エンドユーザーがこの製品を廃棄する場合、回収およびリサイクルのために別の回収施設に送付する必要があることを示しています。この製品を他の家庭用廃棄物と分別することにより、焼却炉や埋立地に送られる廃棄物の量が減り、天然資源が保護されます。</p>
	<p>UL適合ロゴ。</p> <p>このロゴは、製品がテストされ、UL（旧Underwriters Laboratories）によってリストされていることを示します。</p>
	<p>FCC適合ロゴ。</p> <p>このロゴは、製品が連邦通信委員会の適合基準に準拠していることを示しています。</p>
	<p>直流記号。</p> <p>この記号は、製品の電源入出力が直流であることを示しています。</p>
	<p>交流記号。</p> <p>この記号は、製品の電源入出力が交流であることを示しています。</p>

	<p>RCM適合ロゴ。</p> <p>このロゴは、製品がオーストラリアのRCMガイドラインに適合していることを示しています。</p>
	<p>CE適合ロゴ。</p> <p>このロゴは、製品が関連する欧州連合の調和された法令のガイドライン/規格に適合していることを示しています。</p>
	<p>注意記号。</p> <p>この記号は重要な情報を示します。</p>
	<p>保護接地（アース）記号。</p> <p>この記号は、マークされた端子が保護接地/接地線への接続を意図していることを示しています。</p>
	<p>ユーラシア適合性（EAC）RoHS</p>

### Honeywell Building Technologies – Security Americas (Head Office)

Honeywell Commercial Security  
715 Peachtree St. NE  
Atlanta, GA 30308  
Tel: +1 800 323 4576

### Honeywell Building Technologies – Security Mexico

メキシコ : Av.Santa Fe 94, Torre A, Piso 1, Col. Zedec,  
CP 012010, CDMX, México.  
コロンビア : Edificio Punto 99, Carrera 11a.  
98-50, Piso 7, Bogota, Colombia.  
電話 : 01.800.083.59.25

### Honeywell Building Technologies – Security Middle East/N.Africa

Emaar Business Park, Building No. 2, Sheikh Zayed Road  
P.O.Box 232362  
Dubai, United Arab Emirates  
security\_meta@honeywell.com  
電話 : +971 4 450 5800

### Honeywell Building Technologies – Security Europe/South Africa

140 Waterside Road, Hamilton Industrial Park  
Leicester, LE5 1TN, United Kingdom  
電話 : +44 (0) 1928 378005

### Honeywell Building Technologies – Security Northern Europe

Stationsplein Z-W 961, 1117 CE Schiphol-Oost, Netherlands  
電話 : +31 (0) 299 410 200

### Honeywell Building Technologies – Security Deutschland

Johannes-Mauthe-Straße 14  
D-72458 Albstadt  
ドイツ  
電話 : +49 (0) 7431 801-0

### Honeywell Building Technologies – Security France

Immeuble Lavoisier  
Parc de Haute Technologie  
3-7 rue Georges Besse  
92160 Antony, France  
電話 : +33 (0) 1 40 96 20 50

### Honeywell Building Technologies – Security Italia SpA

Via Achille Grandi 22,  
20097 San Donato Milanese (MI), Italy

### Honeywell Building Technologies – Security España

Josefa Valcárcel, 24  
28027 – Madrid, España  
電話 : +34 902 667 800

### Honeywell Building Technologies – Security Россия и СНГ

121059 Moscow,  
Ul, Kiev 7  
Russia  
電話 : +7 (495) 797-93-71

### Honeywell Building Technologies – Security Asia Pacific

Building #1, 555 Huanke Road,  
Zhang Jiang Hi-Tech Park Pudong New Area,  
Shanghai, 201203, China  
電話 : 400 840 2233

### Honeywell Building Technologies – Security and Fire (ASEAN)

Honeywell International Sdn Bhd  
Level 25, UOA Corp Tower, Lobby B  
Avenue 10, The Vertical, Bangsar South City  
59200, Kuala Lumpur, Malaysia  
電子メール : buildings.asean@honeywell.com  
技術サポート (中小企業) :

ベトナム : +84 4 4458 3369

タイ : +66 2 0182439 Indonesia: +62 21 2188 9000

マレーシア : +60 3 7624 1530

シンガポール : +65 3158 6830

フィリピン : +63 2 231 3380

### Honeywell Home and Building Technologies (インド)

HBT India Buildings  
Unitech Trade Centre, 5th Floor,  
Sector – 43, Block C, Sushant Lok Phase – 1,  
Gurgaon – 122002, Haryana, India  
電子メール : HBT-IndiaBuildings@honeywell.com  
フリーダイヤル : 000 800 050 2167  
電話 : +91 124 4975000

### Honeywell Building Technologies – Security and Fire (韓国)

Honeywell Co., Ltd. (韓国)  
5F SangAm IT Tower,  
434, Worldcup Buk-ro, Mapo-gu,  
Seoul 03922, Korea  
電子メール : info.security@honeywell.com  
顧客サポート : HSG-CS-KR@honeywell.com; +82 1522-8779  
電話 : +82-2-799-6114

### Honeywell Building Technologies – Security & Fire (太平洋)

Honeywell Ltd  
9 Columbia Way  
BAULKHAM HILLS NSW 2153  
電子メール : hsf.comms.pacific@Honeywell.com  
技術サポート :  
オーストラリア : 1300 220 345  
ニュージーランド : +64 9 623 5050

# Honeywell

<https://buildings.honeywell.com/security>

+1 800 323 4576 (北米のみ)

文書 800-26904 改訂 A – 03/2022