ViOnyx Web Server
ユーザーガイド

バージョン 1.1.0

日本語
JA 102.00.VQF12-R

suprema
SECURITY & BIOMETRICS

目次

はじめに 5

証明書のインストール 5

パスワードの設定 10

ログイン 11

ユーザーインターフェースの理解 13

メインメニューのショートカット 13

情報とツール 14

ライブ映像を見る 15

ライブビューの基本構成 15

チャンネルとビュー モードを選択する 15

画面の拡大・縮小 17

画面回転 17

画面キャプチャ 17

全画面モード 18

AI表示オプション 18

顔撮影パネルを開く 19

映像が再生されないとき 20

AIイベントの管理 21

ユーザー追跡イベントを設定 21

侵入検知イベントを設定 28

ライン通過検知イベントの設定 35

人数カウントイベントの設定 43

入退室制御イベントを設定する 50

AIイベントの編集と削除 58

AIルールの設定 60

スケジュール管理 66

高度設定 70

カメラを設定する 74

ビデオプロファイルの設定 74

カメラ設定の変更 77

プライバシーとオーバーレイの設定 81

日付と時刻の設定 85

ネットワークを設定 87

RS-485 の設定 98

RTSPおよびONVIF連携 106

ユーザー管理 109

顔認証設定 109

ユーザーの追加 109

ユーザーの編集と削除 116

ユーザーの検索と表示 119

入退室制御管理 123

ドア管理 123

出入レベルの管理性行する 129

出入ドアを制御する 135

出入口ルールの設定 137

システム構成 145

カメラ情報の更新 145

ファームウェアの更新 147

カメラの保守 149

オーディオクリップのアップロード 153

管理者アカウントのパスワードを更新 155

オペレーターの管理 157

システムログの確認 161

システムログの種類 166

付録 175

免責事項 175

著作権に関するお知らせ 176

はじめに

ViOnyxカメラを初めて設置した後、Webブラウザーで初期設定を完了する必要があります。この文書では、証明書のインストール、管理者パスワードの設定、ログインまでに必要なすべての手順を案内します。

> **情報**
> 工場出荷時設定にリセットした後、IPアドレスが割り当てられない場合は、デフォルトIPアドレス（https://192.168.1.100）に変更されます。Webブラウザーでそのアドレスにアクセスしてください。

証明書のインストール

ViOnyx Web Serverは安全なHTTPS接続を使用します。初回アクセス時にセキュリティ警告が表示されますが、これはカメラの自己発行証明書が原因です。証明書をWindowsの信頼済みストアに登録した後、Webサーバーにアクセスすると、警告なしで安全に接続する方法を確認してください。

1 証明書をダウンロード

1. Webブラウザーで、カメラに割り当てたIPアドレス（https://{IP_address}）にアクセスしてください。
2. **この接続ではプライバシーが保護されません** という警告メッセージが表示されたら、下部の **詳細設定** ボタンをクリックしてください。



3. **詳細設定** セクションを展開した後、https://{IP_address} **にアクセスする（安全ではありません）** または同様のリンクをクリックして続行してください。



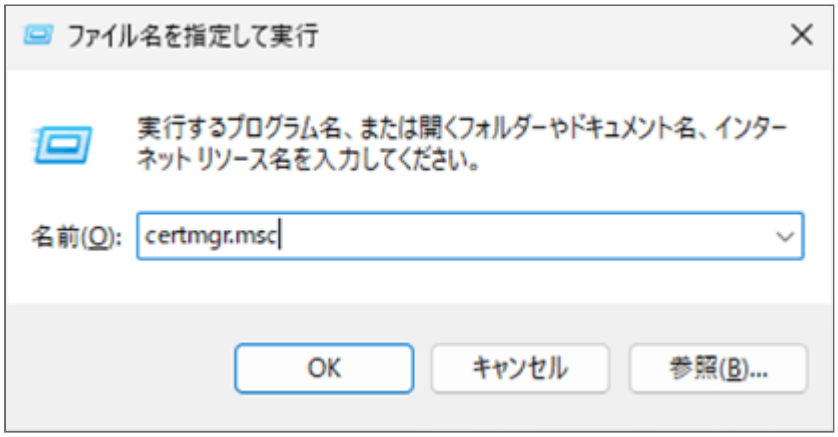
4. パスワード設定画面の下部にある **Suprema ViOnyx Device Root CA** リンクをクリックしてください。



5. 証明書ファイル `Suprema_ViOnyx_Device_{serial-number}_Root_CA.crt` をローカルに保存してください。

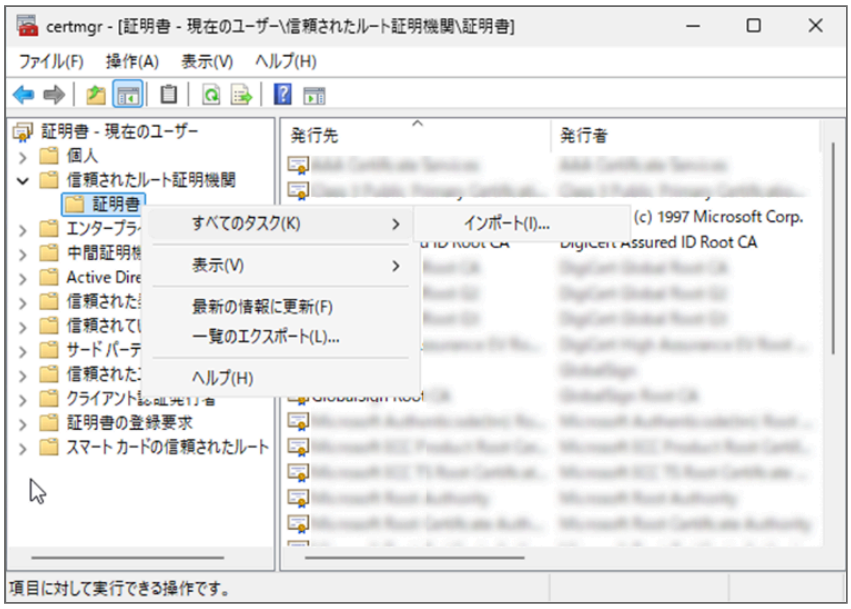
2 Windows管理コンソールを開く

1. 開始 + `R` キーを押して、実行ウィンドウを開いてください。
2. `certmgr.msc` を入力し、`Enter` キーを押して **管理コンソール** を起動してください。

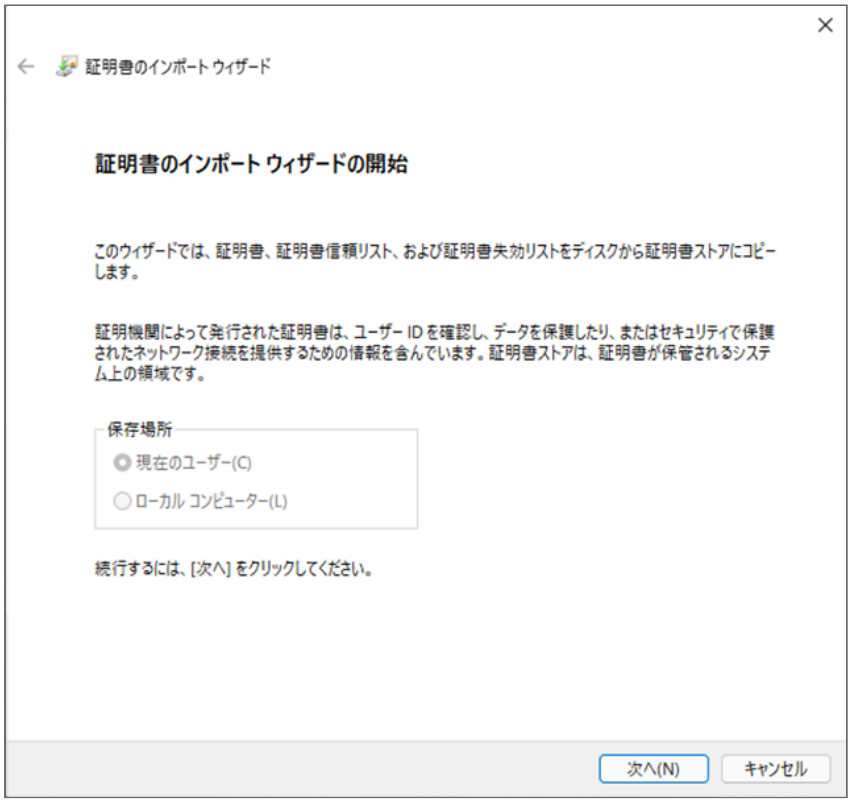


❸ 証明書ウィザードのインポートを実行

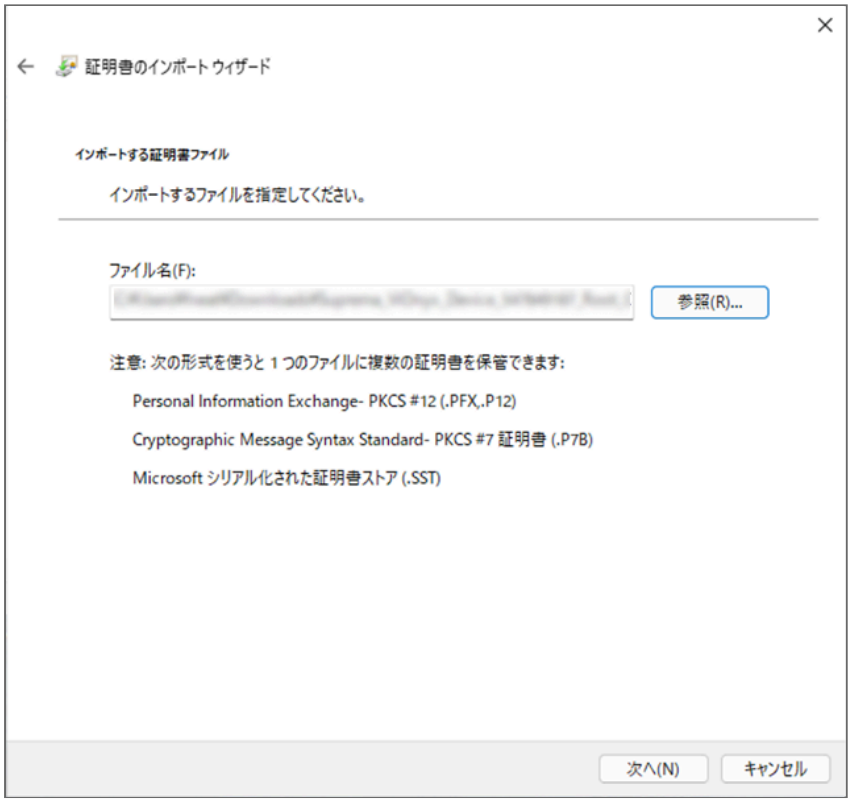
1. **管理コンソール** の左ペインで **信頼されたルート証明機関** を展開してください。
2. 下の **証明書** を右クリックし、**すべてのタスク → インポート** を選択してください。



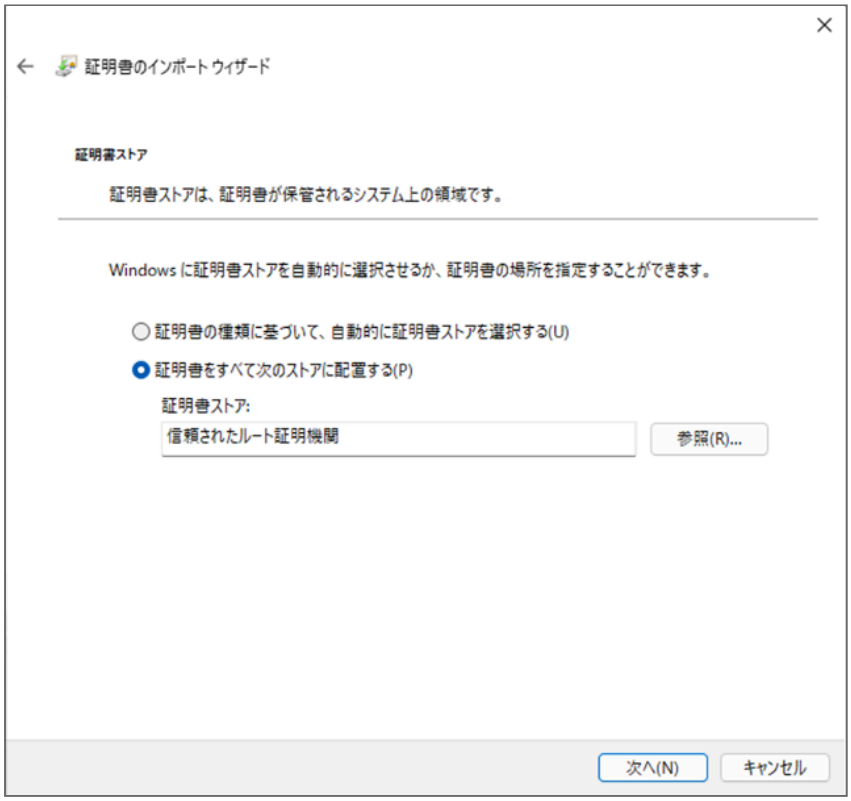
3. 証明書のインポートウィザードで **次へ** ボタンをクリックしてください。



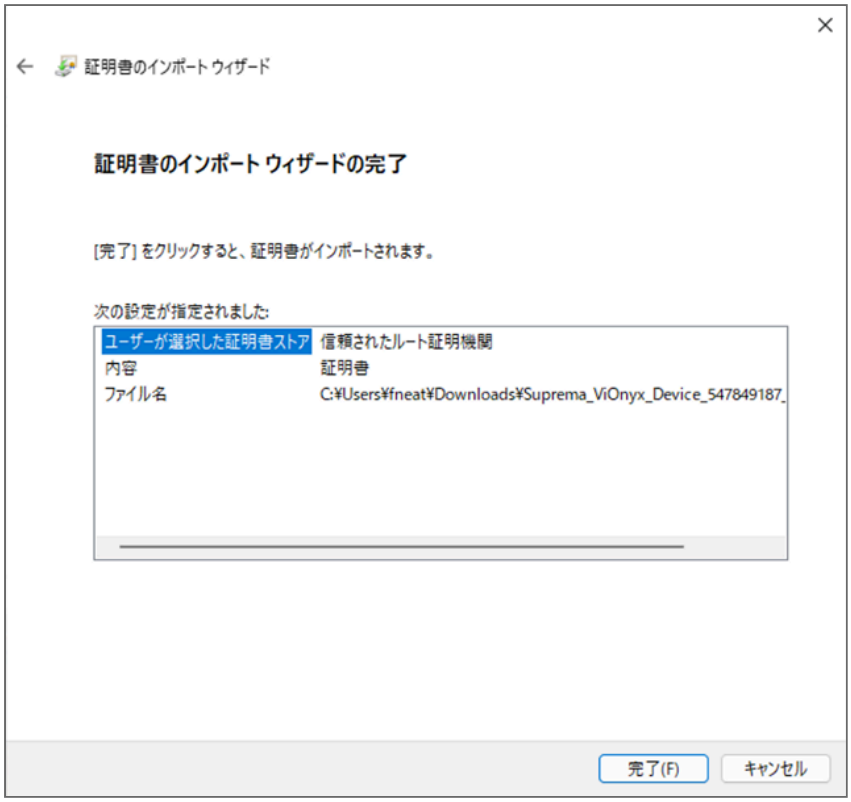
4. 参照 ボタンをクリックして、保存した証明書ファイル Suprema_ViOnyx_Device_547849187_Root_CA.crt を選択してください。



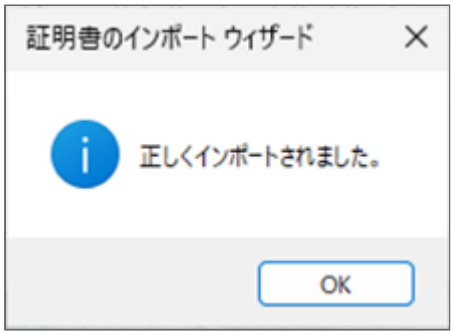
5. **次へ** ボタンをクリックしてください。
6. **証明書をすべて次のストアに配置する** を選択してください。
7. **証明書ストア** が **信頼されたルート証明機関** に設定されていることを確認してください。



8. **次へ** ボタンをクリックしてください。
9. **完了** ボタンをクリックして、証明書のインポートを完了してください。

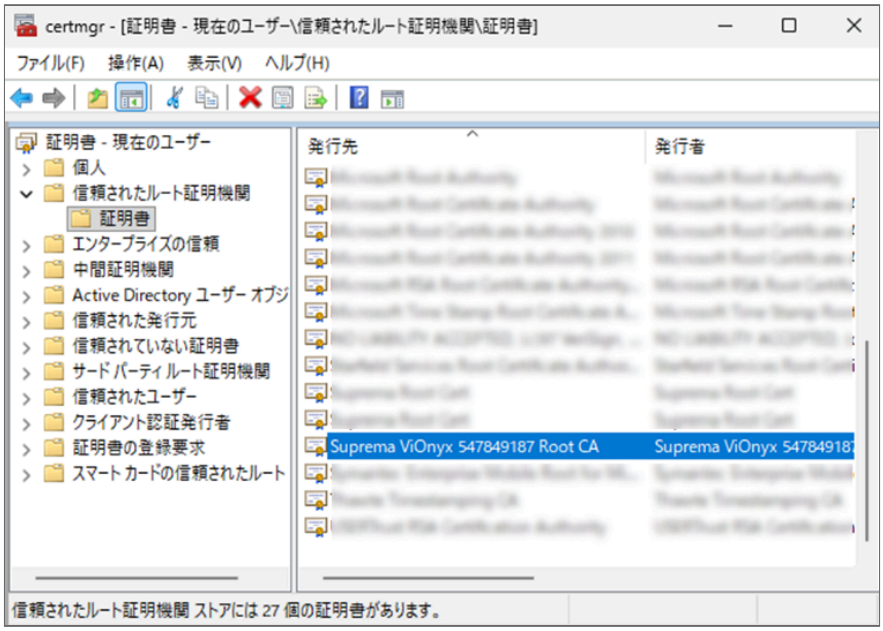


10. セキュリティ警告が表示されたら、**はい** ボタンをクリックしてください。
11. 証明書のインポート成功メッセージが表示されたら、**OK** ボタンをクリックしてください。



4 証明書インストールの確認

管理コンソールで **信頼されたルート証明機関** → **証明書** を選択し、先ほどインポートした証明書が一覧にあることを確認してください。

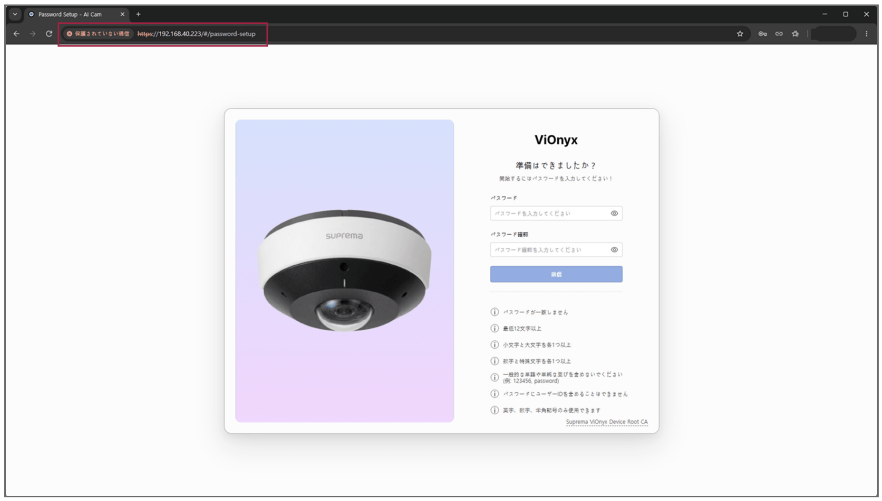


証明書のインストールが完了したら、Webブラウザーを完全に終了して再起動し、カメラのIPアドレスに再度アクセスしてください。これで、セキュリティ警告なしで安全に接続されます。

パスワードの設定

初回ログイン時はセキュリティのため強力なパスワードを設定する必要があります。 ViOnyx は強力なパスワードポリシーを適用してシステムのセキュリティを確保します。

1. Webブラウザーで、カメラに割り当てたIPアドレス（`https://{IP_address}`）にアクセスしてください。



2. パスワード設定ページの **パスワード** 入力フィールドに新しいパスワードを入力してください。
3. **パスワード確認** フィールドに同じパスワードを再入力してください。
4. 入力したパスワードが以下のすべての要件を満たしていることを確認してください。
5. すべての条件が満たされると、**送信** ボタンが有効になります。ボタンをクリックしてパスワードの設定を完了してください。

パスワード要件

パスワードは次のすべての条件を満たす必要があります:

- **パスワード** フィールドと **パスワード確認** フィールドの値が正確に一致する必要があります。
- パスワードは12文字以上にしてください。最大64文字以内です。
- 少なくとも1つの英小文字(`a-z`)と英大文字(`A-Z`)を含める必要があります。
- 少なくとも1つの数字(`0-9`)と特殊文字を含める必要があります。

  > *特殊文字の例:* `\" ! @ # $ % ^ & * ( ) - _ = + [ ] { }`
- `1234` 、 `abcd` のような連続する4文字以上、または同一文字が4回以上含まれていてはいけません。
- 大文字小文字を問わず、IDをパスワードに含めることはできません。

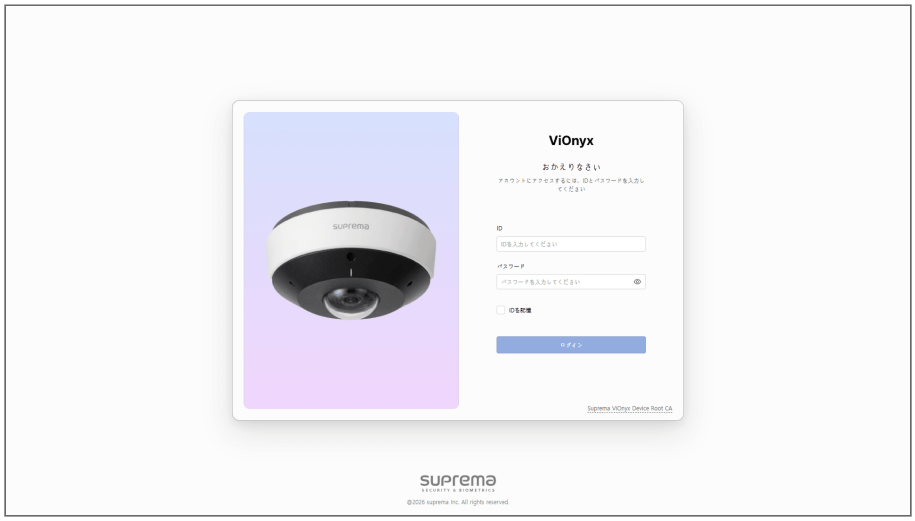
  > *admin, Admin, ADMIN, Admin123! など*
- `password` 、 `qwerty` 、 `123456` など、よく使用されるパスワードパターンは使用できません。
- 使用できるのは英字、数字、英語キーボードの特殊文字のみです。

注意

設定したパスワードは安全な場所に保管してください。パスワードを紛失した場合はカメラを初期化する必要があります。

ログイン

パスワードの設定が完了すると、ログインページへ自動的に移動します。管理者IDと設定したパスワードを入力して、ViOnyx Web Server に接続してください。



1. **ID** 入力フィールドに **admin** を入力してください。
2. **パスワード** 入力フィールドに設定したパスワードを入力してください。
3. **ログイン** ボタンをクリックしてください。

ログインに成功すると、ViOnyx Web Server の **ライブ** ページに移動します。

> **情報**
> 管理者 ID (admin) は **システム** → **アカウント管理** で変更できます。

次のステップ

ライブ メニューの主な機能と使用方法を案内します。
AI イベントを設定して、カメラが検知した特定の状況を監視できます。
カメラの各種設定により、撮影環境に適した最適な映像品質を維持し、ネットワークを構成し、セキュリティおよび個人情報保護ポリシーを適用できます。
ユーザーを登録して、AI顔認識機能を活用できます。
カメラシステムを効果的に管理するために、デバイス情報、ファームウェア、メンテナンス、アカウント、オーディオ、ログを体系的に管理できます。

ユーザーインターフェースの理解

ViOnyx Web Serverにログインすると、上部に主要メニューが表示されます。各メニューから目的の機能へ素早くアクセスできます。このページでは、ウェブサーバーインターフェースの構成と各メニューの役割を説明します。



メインメニューのショートカット

画面左上にはViOnyx Web Serverのロゴと主要メニューのアイコンがあります。各メニューで提供される機能は以下のとおりです。

メニューアイコン	メニュー名	説明
	ライブ	カメラが撮影中の映像をリアルタイムで確認できます。
	設定	カメラとウェブサーバーの設定値を変更できます。
	AI&ルール	AIイベントとルールを設定できます。
	ユーザー	カメラシステムのユーザーを追加・管理できます。
	アクセス	ドア、アクセスレベル、ユーザー権限の体系を連携し、入退室制御を管理できます。このメニューはベータ版です。
	システム	デバイス情報、アカウント、オーディオ、ログなど、システム全体を管理できます。

情報

アクセス メニューはファームウェアバージョン1.1.0以降で利用できます。

情報とツール

画面右上にはカメラ情報、言語選択、ユーザーガイドへのショートカット、ログアウトボタンがあります。

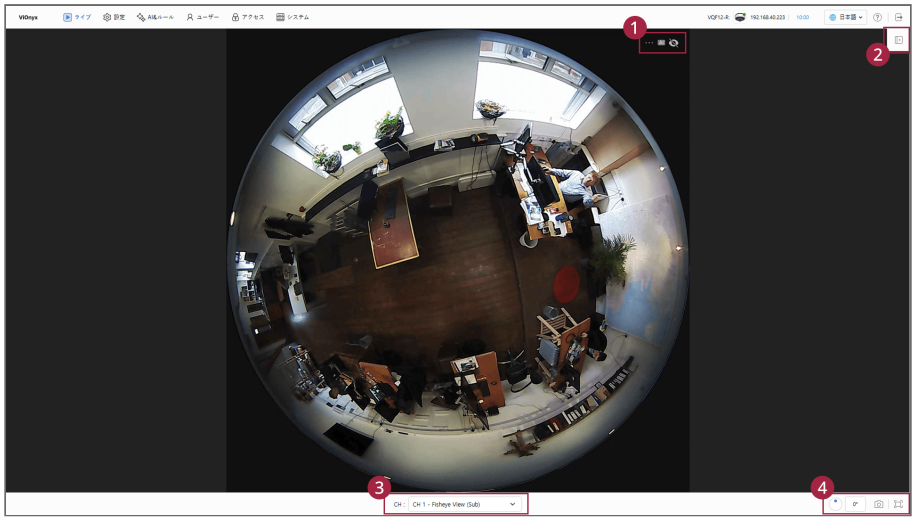
メニューアイコン	メニュー名	説明
	カメラ情報	現在接続中のカメラの名前、状態、IP アドレスを確認できます。 **IPアドレス**をクリックすると、デバイス情報を確認できます。
10:00	セッション時間	現在ログインしている管理者のセッション時間を確認できます。セッション時間を超えると、自動的にログアウトします。
	言語選択	ウェブインターフェースの言語を変更できます。
	ユーザーガイドへのショートカット	ユーザーガイドを確認できます。
	ログアウト	ログアウトできます。

ライブ映像を見る

ViOnyx Web Serverの**ライブ**メニューでは、カメラが撮影している映像をリアルタイムで確認できます。希望するチャンネルとビュー モードを選択し、画面を拡大したり全画面で表示できます。

ライブビューの基本構成

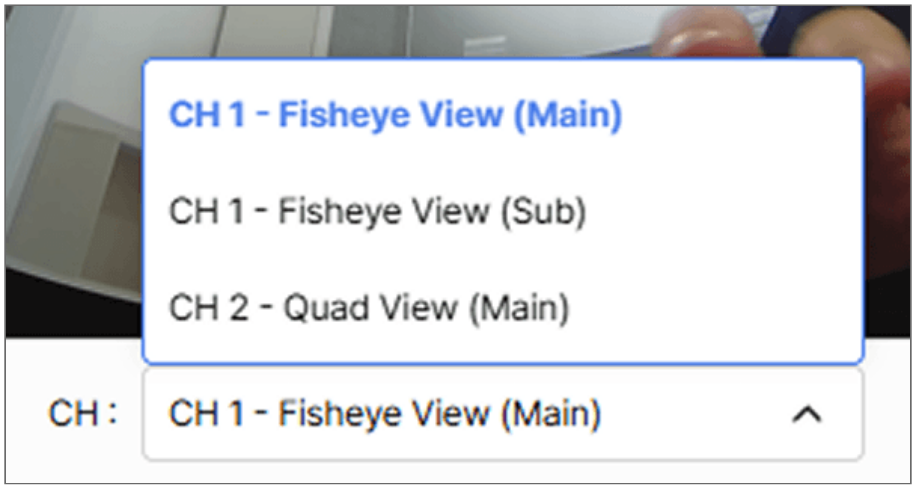
初めて**ライブ**メニューに入ると、映像は次のような初期状態で表示されます。



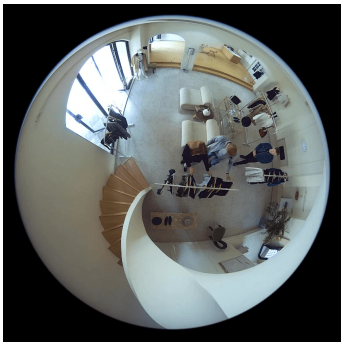
項目	構成要素	説明
1	AI	- AI機能は無効です。アイコンをクリックしてAI機能を有効にできます。 - AIイベントとユーザーボックスを表示または非表示にするには、••• ボタンをクリックして設定を調整してください。
2		**顔撮影**(Face Shot) パネルを開けます。
3	CH	チャンネルごとに利用可能なビュー モードを選択できます。
4		ライブ映像を回転できます。
		ライブ映像をキャプチャできます。
		ライブ映像を全画面で表示できます。

チャンネルとビュー モードを選択する

ViOnyx Web Serverは複数のチャンネルとさまざまなビュー モードを提供します。画面下の**CH**ドロップダウンメニューから目的のチャンネルとビュー モードを選択します。



サポートされているチャンネルとビュー モード

チャンネル	ビュー モード	説明	例
1ch	Fisheye View (Main/Sub)	基本チャンネルのフィッシュアイレンズの原映像	
2ch	Quad View (Main)	パノラマビュー チャンネルの4分割表示	

情報

- 各チャンネルのMainとSubは異なる解像度のストリームを提供します。 Mainは高画質、Subは低画質のストリームです。
- 上の画像は例示用の画面です。実際の画面とは異なる場合があります。

画面の拡大・縮小

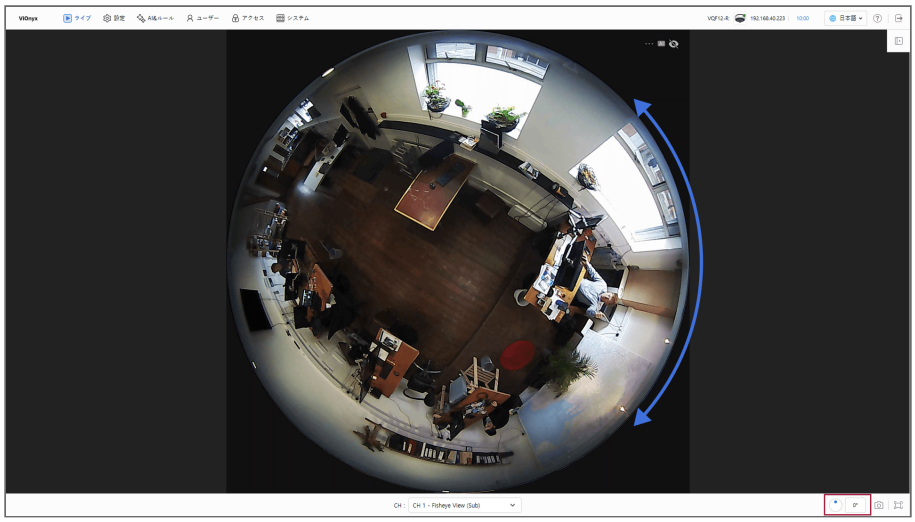
マウスで画面を拡大・縮小できます。

- スクロールアップ（上）：画面拡大（ズームイン）
- スクロールダウン（下）：画面縮小（ズームアウト）
- ダブルクリック：元のサイズに戻る（1倍）

> **情報**
>
> - 1倍 ~ 8倍まで画面を拡大できます。
> - 画面の拡大はデジタルズームのため、高倍率にすると映像がぼやける場合があります。

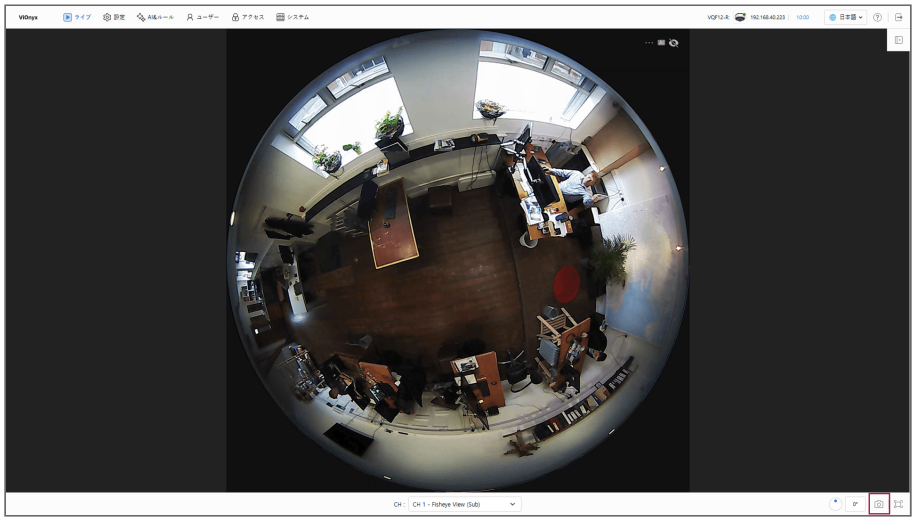
画面回転

ライブ映像を回転するには、 ボタンをクリックしたままドラッグしてください。または、 ボタンの右側の入力フィールドに回転角度を直接入力することもできます。



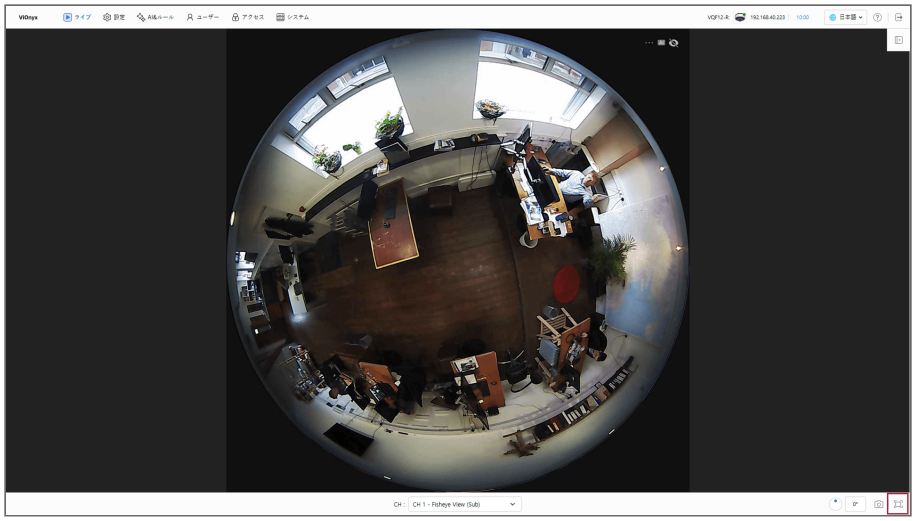
画面キャプチャ

ライブ映像をキャプチャするには、 ボタンをクリックしてください。キャプチャ画像は `capture_{ch1|ch2}_{main|sub}_{YYYY-MM-DDTHH-MM-SS}.jpeg` 形式で保存されます。



全画面モード

大きな映像を確認するには、全画面モードを使用してください。画面右下の ボタンをクリックします。



- 全画面モードでもビュー モードの変更とズーム機能を継続して使用できます。
- 全画面モードを終了するには、 ESC キーを押すか、 ボタンをもう一度クリックします。

AI表示オプション

ライブ映像のAI表示オプションを設定するには、画面右上の ボタンをクリックしてください。



- **イベントボックスポップアップ**: AIイベントが発生すると、ライブ映像の左上にイベントがポップアップ表示されます。
- **ユーザーボックスポップアップ**: AIイベントで顔が検出されると、ライブ映像の右下にユーザーボックスがポップアップ表示されます。
- **基本透明度**：イベントポップアップとユーザーポップアップの透明度を調整できます。
- **基準点**：ライブ映像の人物検知ボックスの上に基準点を表示します。このオプションをオンにすると、映像右上に凡例も表示されます。
  - 水色の点(🔵)：ボックスの中央です。
  - 赤色の点(🔴)：ボックスの長軸に沿って上から80%の位置です。カメラを天井に下向きで設置すると、人の足元付近に表示されます。

> **情報**
>
> - **表示時間** オプションで設定した時間（単位: 秒）の間、ポップアップが表示されます。
> - **基準点** オプションを使用するには、AI機能(AI 👁)をオンにしてください。
> - **基本透明度**、**基準点** オプションはファームウェアバージョン1.1.0以降で利用できます。

顔撮影パネルを開く

AIイベント機能を有効にすると、カメラで検出された顔を確認できます。 **顔撮影**(Face Shot) パネルを開くには、画面右上の ボタンをクリックします。



顔撮影 パネル上部のツールアイコンをクリックして、次の機能を使用できます。

- / : 顔撮影を一時停止または再開できます。
- : 顔撮影結果をフィルタリングできます。
- : **顔撮影** パネルを全画面に拡大できます。

> **情報**
> AIイベントとルール設定の詳細は、AIイベントの管理を参照してください。

映像が再生されないとき

カメラの映像が読み込まれない場合は、次の手順に従ってネットワーク接続を確認してください。

1. カメラとネットワークの接続状態を確認してください。
2. ウェブブラウザで**再読み込み（F5）**ボタンを押してください。
3. システムが自動的に再接続を試みます。

AIイベントの管理

AIイベントとルールを設定すると、カメラが検知した状況に応じて必要な動作を自動で実行します。最初に検知する状況をAIイベントとして作成し、イベント発生時に実行する動作をAIルールに関連付けてください。

AIイベントは、人の動き、エリア侵入、ライン通過、人数カウント、出入口への接近など、監視目的に合わせて作成できます。 AIルールでは、イベント発生時に実行するオーディオ、Webhook、リレー動作を指定し、スケジュールを適用して実行時間帯を制限できます。運用環境に応じて、高度な設定で顔認証関連の詳細オプションを調整してください。

> **情報**
> AIイベントを使用するには、すべてのイベントに共通して適用される顔領域を少なくとも1つ設定する必要があります。

ユーザー追跡イベントを設定

ユーザー追跡イベントを作成して、進入エリアへの出入りを検知します。オプションで顔領域を追加すると、特定の領域で顔を優先的に追跡し、登録済みのユーザーを自動的に顔認証します。

いつ使用しますか？

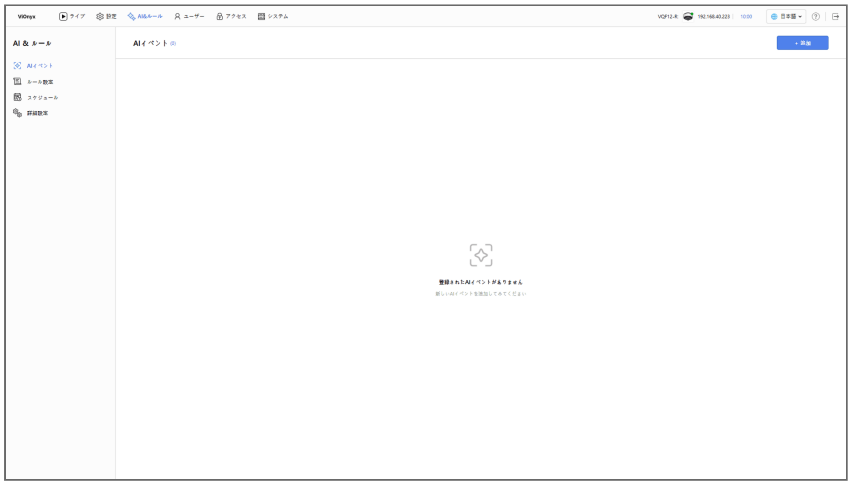
- 進入エリアに登録された社員または顧客の出入り状況の把握
- セキュリティが必要なエリア（会議室、倉庫）へのアクセス監視
- 店舗内の特定コーナー（新商品、イベントゾーン）への来客流入を追跡

ユーザー追跡イベントの作成

ユーザー追跡イベントを作成すると、ライブビューで人の移動をリアルタイムで追跡できます。また、顔領域を設定すると登録済みユーザーを認証して、誰が移動したかを確認できます。

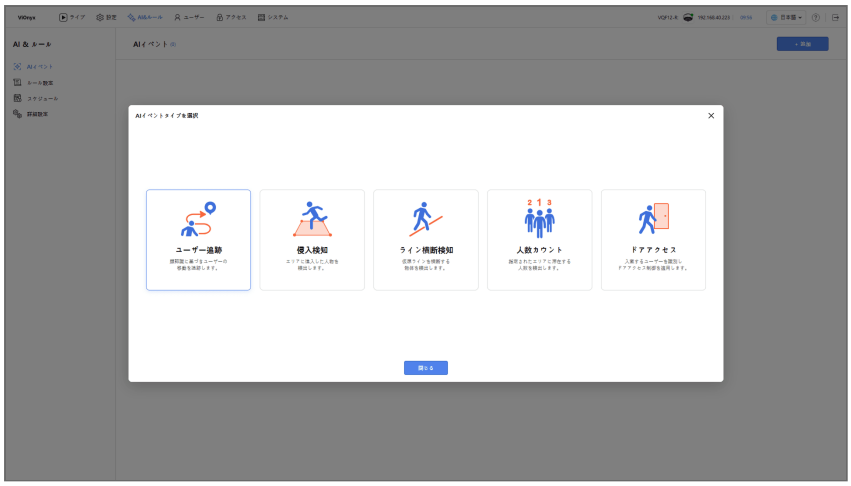
1 イベント作成の開始

1. 画面左上の **AI&ルール** メニューをクリックします。
2. 画面左のサイドバーで **AIイベント** をクリックしてください。

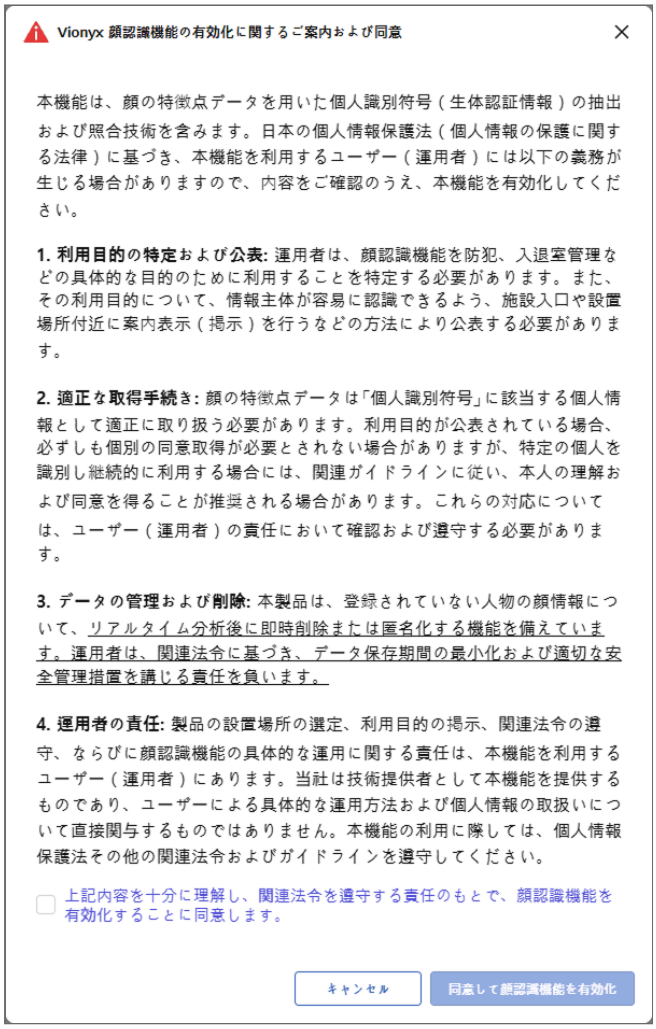


3. 画面右上の**+ 追加**ボタンをクリックしてください。

4. **AIイベントタイプを選択** ウィンドウで **ユーザー追跡** をクリックします。

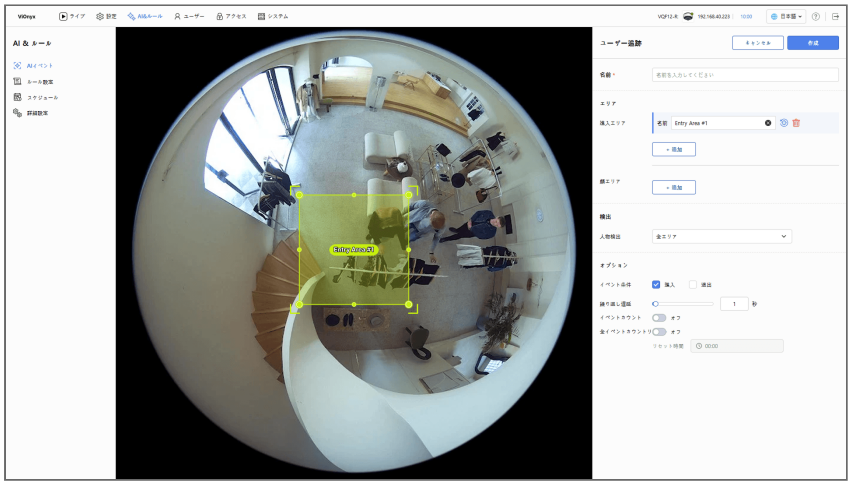


5. **Vionyx 顔認識機能の有効化に関するご案内および同意** ポップアップが表示されたら、内容を確認し、同意チェックボックスをクリックしてから **同意して顔認識機能を有効化** ボタンをクリックします。



- 顔認証機能を使用するには、該当地域の関連法規を遵守する必要があります。同意しない場合は先に進めません。
- 「**Vionyx 顔認識機能の有効化に関するご案内および同意**」ポップアップは初回のみ表示されます。以降、AIイベント作成時は同意済みとみなします。

6. 右側の **ユーザー追跡** パネルで必要な設定を完了してください。

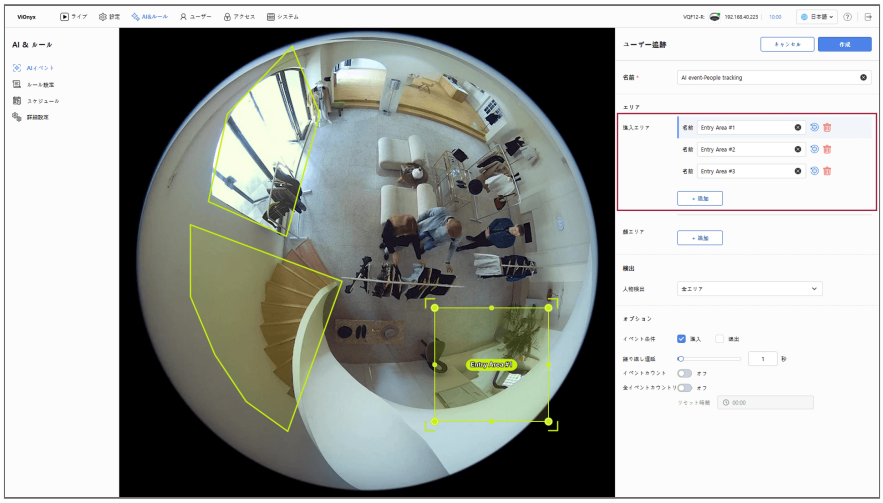


❷ イベント名の設定

名前 入力フィールドに AI イベント名を入力します。名前は最大64文字まで入力できます。

❸ 進入エリアの設定

追跡する進入エリアを設定してください。カメラは設定したエリアの出入りを検知します。最低1本を設定する必要があり、**+ 追加**ボタンをクリックして最大10本まで追加できます。ライブビューに黄色いボックスが表示され、マウスで角または点をドラッグして希望の形状に調整できます。中央の領域をドラッグして位置を移動できます。



- **名前**：進入エリアの名前を編集できます。わかりやすい名前を付けてください。進入エリアの名前はライブビューでマウスオーバーすると表示されます。

> **情報**
>
> - 設定した進入エリアの形状とサイズを初期化するには、ボタンをクリックしてください。
> - 追加した進入エリアを削除するには、ボタンをクリックしてください。

❹ 顔領域の設定（任意）

顔を検知する領域を設定してください。設定すると、当該領域で顔を優先的に追跡します。顔領域は進入エリアを包含するように設定してください。顔領域が進入エリアを包含していないと、カメラは顔を認識できません。**+ 追加**ボタンをクリックして最大10個まで設定できます。ライブビューに青い枠が表示され、マウスで角や点をドラッグして形状を調整できます。中央の領域をドラッグして位置を移動できます。



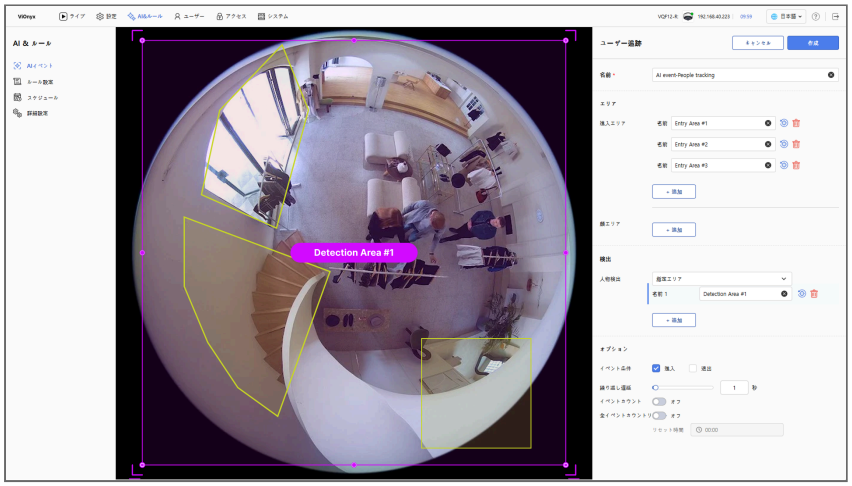
- **名前**：顔領域の名前を編集できます。わかりやすい名前を付けてください。顔領域の名前はライブビューでマウスオーバーすると表示されます。

> **情報**
>
> - 登録済みユーザーは**ライブ**メニューで自動的に識別され、名前が表示されます。登録されていないユーザーは**未認識の顔**として表示されます。
> - 設定した顔領域の形状とサイズを初期化するには、ボタンをクリックしてください。
> - 追加した顔領域を削除するには、ボタンをクリックしてください。
> - カメラ設定で **適応型自動露出** 適応型自動露出オプションを使用する場合は、人が実際に立っている、または通過する際に顔がよく見える位置が顔領域に含まれるように設定してください。

5 人検出の設定（任意）

検出 セクションで、カメラが人を検出する範囲を選択します。検出範囲を必要な場所に絞ると、関心のないエリア（通路の端、窓、反射面など）での誤検出を減らせます。

- **全エリア**：デフォルト値です。画面全体で人を検出します。顔領域の設定に関係なく使用できます。
- **指定エリア**：指定した領域内でのみ人を検出します。顔領域を設定していない場合のみ選択できます。最低1本を設定する必要があり、**+ 追加**ボタンをクリックして最大10本まで追加できます。ライブビューに紫色の枠が表示されます。マウスで角または点をドラッグして希望の形に調整できます。中央の領域をドラッグして位置を移動できます。



  - **名前**：人検出領域の名前を編集できます。

- **顔エリアのみ**：顔領域内でのみ人を検出します。顔領域を設定した場合のみ選択できます。

> **情報**
>
> - **指定エリア**を選択した状態で顔領域を追加すると、**通知** ポップアップが表示されます。 **確認** ボタンをクリックすると、指定した検出領域が解除され、**顔エリアのみ**に変更されます。
> - **顔エリアのみ**を選択した状態で顔領域をすべて削除すると、**全エリア**に自動で変更されます。
> - カメラ設定で **適応型自動露出** オプションを使用する場合は、ディスプレイ、写真、ポスターなど人物が写ったものが検出範囲に含まれないよう、**指定エリア** または **顔エリアのみ** に範囲を絞ってください。
> - 設定した人検出領域の形状とサイズを初期化するには、 ボタンをクリックしてください。
> - 追加した人検出領域を削除するには、 ボタンをクリックしてください。
> - この機能のサポートは、ファームウェアバージョン1.1.0以降に含まれます。

6 イベント発生条件とカウントの設定

オプション セクションでイベント発生条件とイベントカウントを設定してください。



- **イベント条件**：イベントを発生させる動作を選択してください。**進入**と**退出**を両方選択することもできます。

- **繰り返し遅延**：イベントとして認識する最小時間を設定してください。検知状態が設定した時間より長く続く場合にイベントが発生します。最大で60秒まで設定できます。

> イベントが多発する場合は、**繰り返し遅延**の値を増やしてください。設定した時間より短く検知した動きはイベントとして認識しないため、不要なイベントが減ります。

- **イベントカウント**：進入領域に入る、または出る回数をカウントするには、**オン**に設定してください。進入回数と退出回数を別々にカウントし、進入領域が複数ある場合は領域ごとにカウントします。

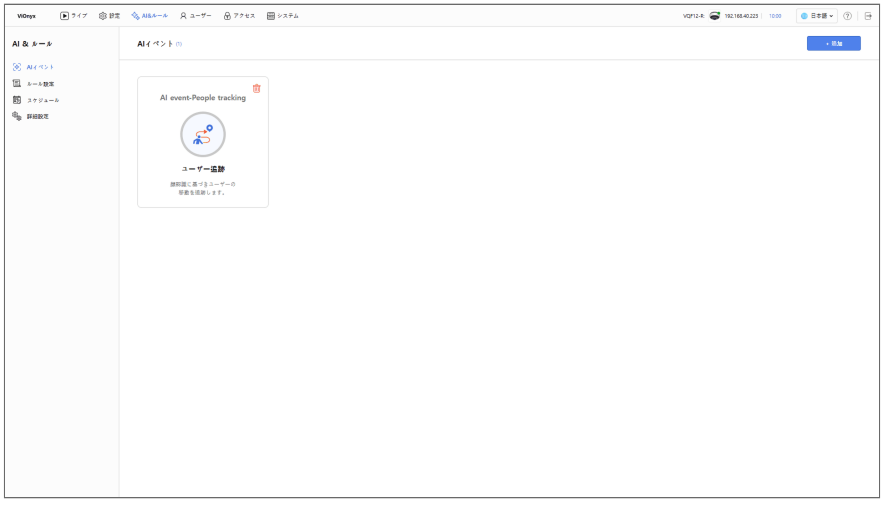
> **イベント条件**で選択した項目のみカウントします。例えば**進入**のみを選択すると、入場回数だけをイベントとして表示し、ログに記録します。

- **全イベントカウントリセット**：すべての進入領域のイベントカウントを毎日指定した時刻に初期化するには、**オン**に設定してください。**リセット時間**で設定した時刻に、すべての進入領域のイベントカウントを初期化します。

> **情報**
>
> - **イベントカウント**を**オン**に設定すると、**ライブ**メニューの映像上で、進入領域ごとに**カウント：N**形式で表示します。イベントカウントを手動で初期化するには、•••ボタンをクリックし、**カウントリセット**を選択してください。
>
> 
>
>
> - ファームウェアバージョン1.1.0以降は、イベントカウント関連オプションをサポートします。

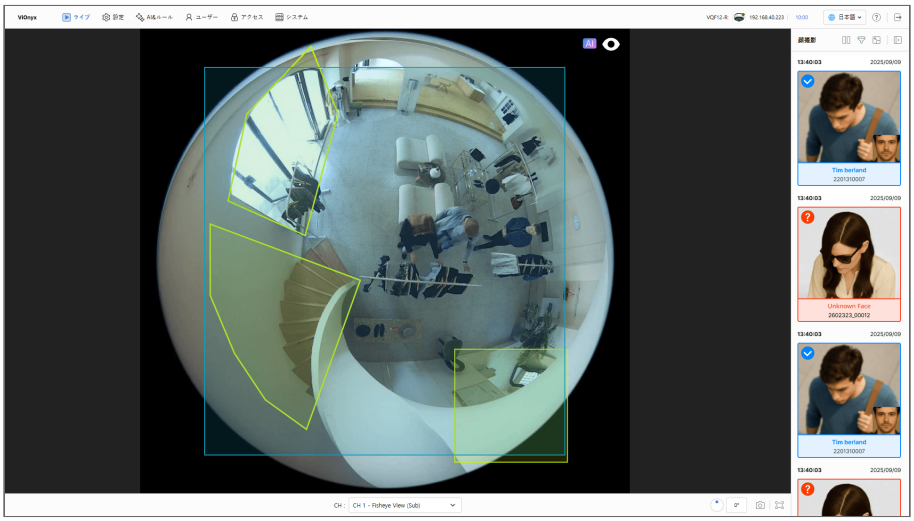
7 設定を保存

すべての設定を完了したら、右上の**作成**ボタンをクリックしてください。前の画面に戻り、新しく作成したAIイベントが一覧に追加されます。



ライブで確認

画面左上の**ライブ**メニューをクリックしてください。カメラ映像の右上にある AI アイコンがオンになっているか確認してください。設定した進入エリアと顔領域が映像にオーバーレイで表示されます。人が進入エリアに入るまたは出るたびにイベントが発生します。顔領域を設定している場合、カメラが当該領域で顔を検知し、登録済みユーザーを自動的に識別して名前を表示します。



情報

- 登録されていないユーザーは**未認識の顔**として表示されます。登録済みユーザーを名前とともに表示します。
- カメラが顔を認識しない場合は、**最小顔サイズ可視化** オプションを有効にしてください。または顔領域を大きく設定するか、カメラ位置を調整してください。
- 照明が不足しているか逆光の場合、カメラが顔を認識できないことがあります。撮影エリアの照明を改善するか、カメラの位置と角度を調整して顔が見えやすくしてください。
- 認識されるには、顔をカメラに向ける必要があります。横顔や後ろ姿は認識が難しい場合があります。
- 進入エリアでイベントが発生しない場合は、顔領域が進入エリアを包含しているか確認してください。

侵入検知イベントを設定

侵入検知イベントを設定すると、管理者が定義した区域に人が出入りするたびにリアルタイムでイベントが発生します。任意で顔領域を追加すると、該当領域で顔を優先的に追跡し、登録済みのユーザーは自動で身元を認証します。監視が必要な区域における不正侵入をすばやく検知し、リアルタイムで通知を受け取れます。

いつ使用しますか？

- セキュリティが必要な区域への不正侵入をリアルタイムで検知
- 業務時間外、または監視が必要な区域にアクセスしたときにリアルタイム通知を受け取る
- 監視区域への未登録者の侵入を検知
- 高リスク区域の出入り状況を記録および追跡する。

情報

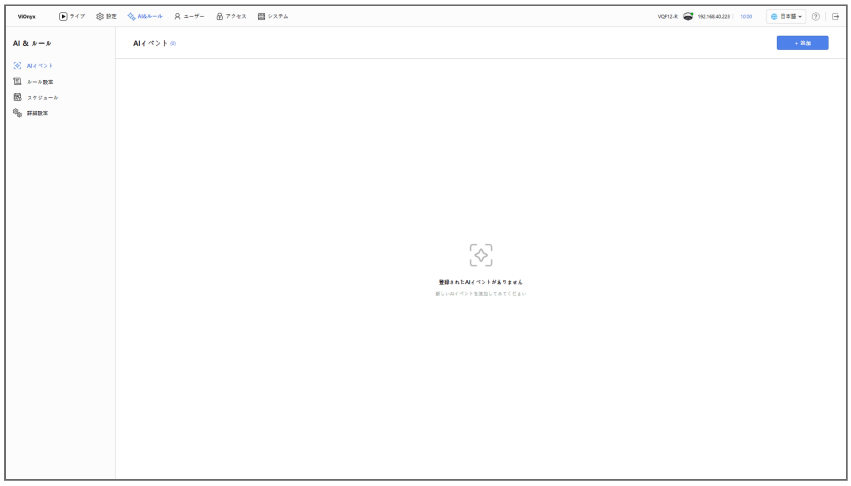
入退室制限以外の用途にも使用でき、カメラで入退室制限の有無を判断しません。

侵入検知イベントの作成

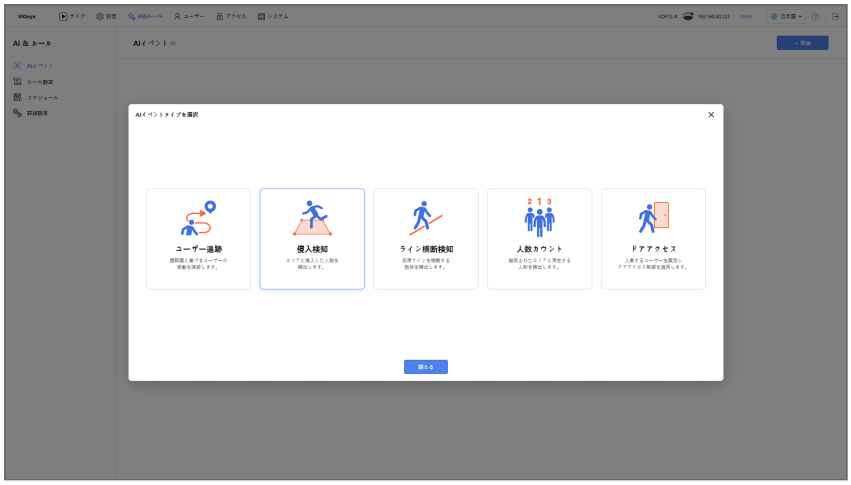
侵入検知イベントを作成すると、**ライブ** メニューで特定区域への人物の侵入を検知してイベントを発生させることができます。また、顔領域を設定すると当該領域で顔を優先的に追跡でき、登録済みユーザーは自動で識別されます。

1 イベント作成の開始

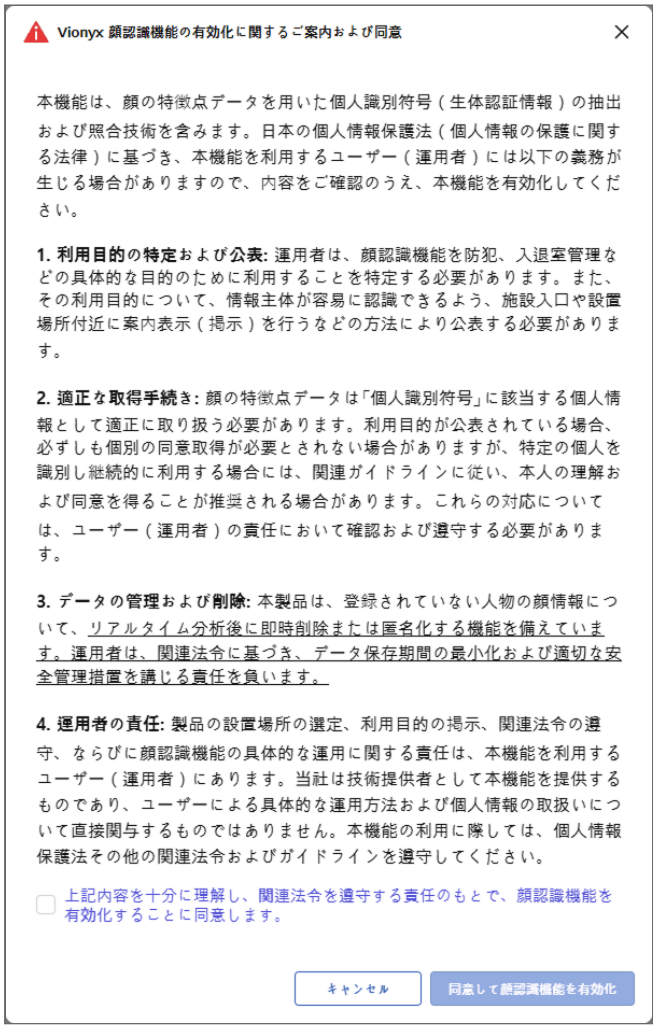
1. 画面左上の **AI&ルール** メニューをクリックします。
2. 画面左のサイドバーで **AIイベント** をクリックしてください。



3. 画面右上の**+ 追加**ボタンをクリックしてください。
4. **AIイベントタイプを選択**ウィンドウで**侵入検知**をクリックします。

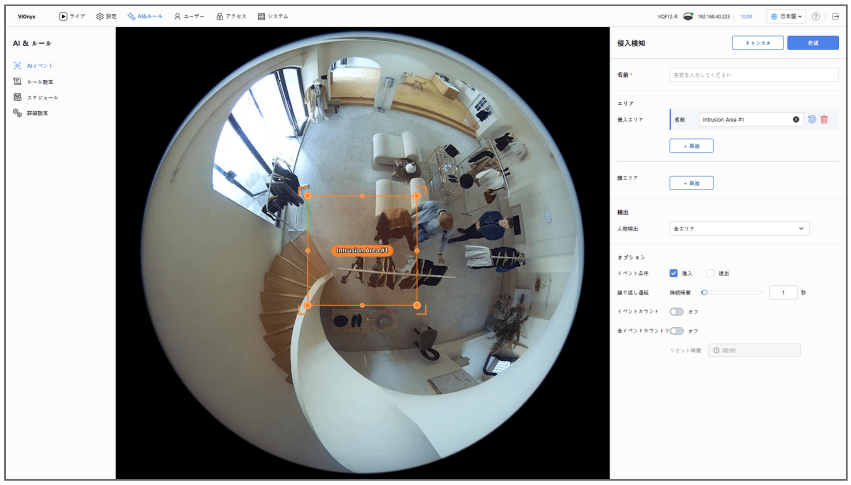


5. **Vionyx 顔認識機能の有効化に関するご案内および同意** ポップアップが表示されたら、内容を確認し、同意チェックボックスをクリックしてから **同意して顔認識機能を有効化** ボタンをクリックします。



- 顔認証機能を使用するには、該当地域の関連法規を遵守する必要があります。同意しない場合は先に進めません。
- 「**Vionyx 顔認識機能の有効化に関するご案内および同意**」ポップアップは初回のみ表示されます。以降、AIイベント作成時は同意済みとみなします。

6. 右側の **侵入検知** パネルで必要な設定を完了してください。

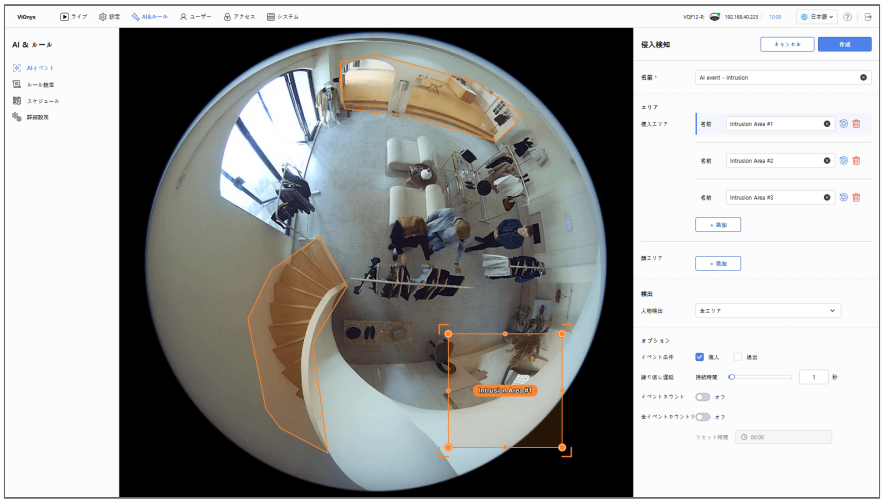


❷ イベント名の設定

名前 入力フィールドに AI イベント名を入力します。名前は最大64文字まで入力できます。

❸ 侵入領域の設定

侵入領域を設定してください。カメラは設定したエリアの出入りを検知します。最低1本を設定する必要があり、**+ 追加**ボタンをクリックして最大10本まで追加できます。ライブビューにオレンジ色の枠が表示されます。マウスで角または点をドラッグして希望の形に調整できます。中央の領域をドラッグして位置を移動できます。

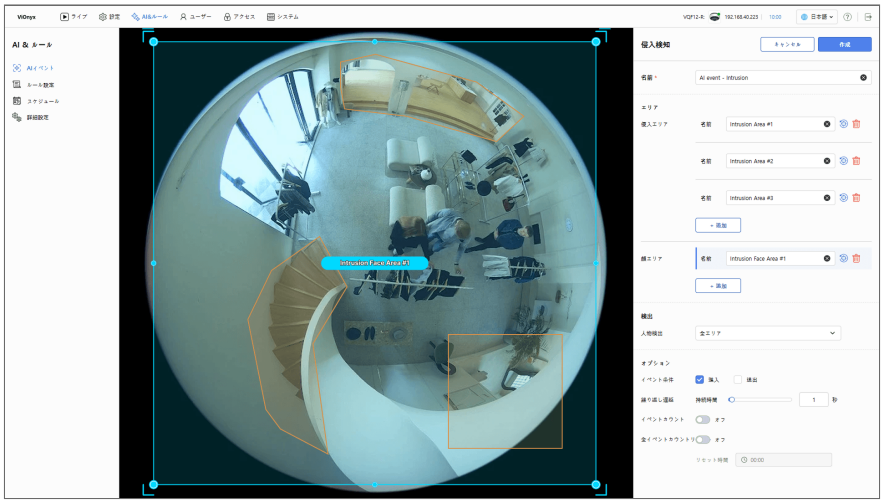


- **名前**：侵入領域の名前を編集できます。わかりやすい名前を付けてください。侵入領域の名前はライブビューでマウスオーバーすると表示されます。

> **情報**
>
> - 設定した侵入領域の形状とサイズを初期化するには、ボタンをクリックしてください。
> - 追加した侵入領域を削除するには、ボタンをクリックしてください。

❹ 顔領域の設定（任意）

顔を検知する領域を設定してください。設定すると、当該領域で顔を優先的に追跡します。顔領域で検出された人物を認証済みユーザーと未承認者に分類することで、承認された出入り者と未許可者を明確に把握できます。顔領域と侵入領域は重ねて設定できます。**+ 追加**ボタンをクリックして最大10個まで設定できます。ライブビューに青い枠が表示され、マウスで角や点をドラッグして形状を調整できます。中央の領域をドラッグして位置を移動できます。



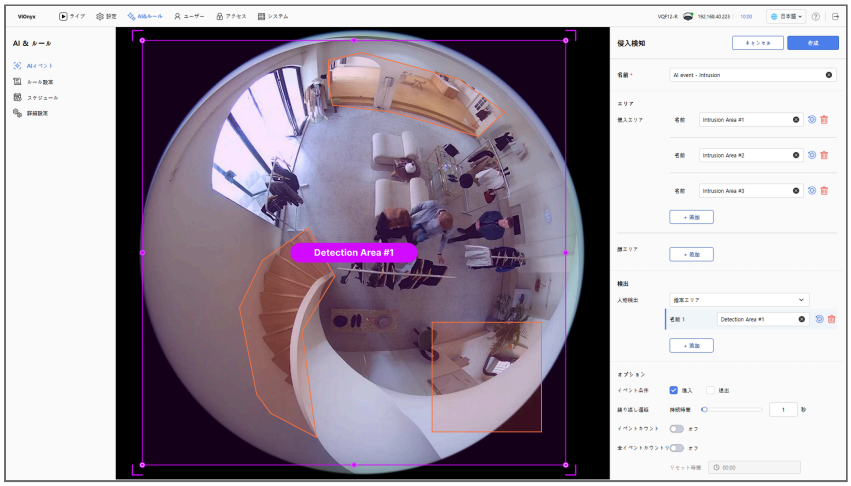
- **名前**：顔領域の名前を編集できます。わかりやすい名前を付けてください。顔領域の名前はライブビューでマウスオーバーすると表示されます。

> **情報**
>
> - 登録済みユーザーは**ライブ**メニューで自動的に識別され、名前が表示されます。登録されていないユーザーは**未認識の顔**として表示されます。
> - 設定した顔領域の形状とサイズを初期化するには、ボタンをクリックしてください。
> - 追加した顔領域を削除するには、ボタンをクリックしてください。
> - カメラ設定で **適応型自動露出** 適応型自動露出オプションを使用する場合は、人が実際に立っている、または通過する際に顔がよく見える位置が顔領域に含まれるように設定してください。

5 人検出の設定（任意）

検出 セクションで、カメラが人を検出する範囲を選択します。検出範囲を必要な場所に絞ると、関心のないエリア（通路の端、窓、反射面など）での誤検出を減らせます。

- **全エリア**：デフォルト値です。画面全体で人を検出します。顔領域の設定に関係なく使用できます。
- **指定エリア**：指定した領域内でのみ人を検出します。顔領域を設定していない場合のみ選択できます。最低1本を設定する必要があり、**+ 追加**ボタンをクリックして最大10本まで追加できます。ライブビューに紫色の枠が表示されます。マウスで角または点をドラッグして希望の形に調整できます。中央の領域をドラッグして位置を移動できます。



  - **名前**：人検出領域の名前を編集できます。

- **顔エリアのみ**：顔領域内でのみ人を検出します。顔領域を設定した場合のみ選択できます。

> **情報**
>
> - **指定エリア**を選択した状態で顔領域を追加すると、**通知** ポップアップが表示されます。 **確認** ボタンをクリックすると、指定した検出領域が解除され、**顔エリアのみ**に変更されます。
> - **顔エリアのみ**を選択した状態で顔領域をすべて削除すると、**全エリア**に自動で変更されます。
> - カメラ設定で **適応型自動露出** オプションを使用する場合は、ディスプレイ、写真、ポスターなど人物が写ったものが検出範囲に含まれないよう、**指定エリア** または **顔エリアのみ** に範囲を絞ってください。
> - 設定した人検出領域の形状とサイズを初期化するには、ボタンをクリックしてください。
> - 追加した人検出領域を削除するには、ボタンをクリックしてください。
> - この機能のサポートは、ファームウェアバージョン1.1.0以降に含まれます。

6 イベント発生条件とカウントの設定

オプション セクションでイベント発生条件とイベントカウントを設定してください。



- **イベント条件**：イベントを発生させる動作を選択してください。**進入**と**退出**を両方選択することもできます。

- **繰り返し遅延**：イベントとして認識する最小時間を設定してください。検知状態が設定した時間より長く続く場合にイベントが発生します。最大で60秒まで設定できます。

> イベントが多発する場合は、**繰り返し遅延**の値を増やしてください。設定した時間より短く検知した動きはイベントとして認識しないため、不要なイベントが減ります。

- **イベントカウント**：侵入領域への入退場回数をカウントするには、**オン**に設定してください。入場回数と退場回数を別々にカウントし、侵入領域が複数ある場合は領域ごとにカウントします。

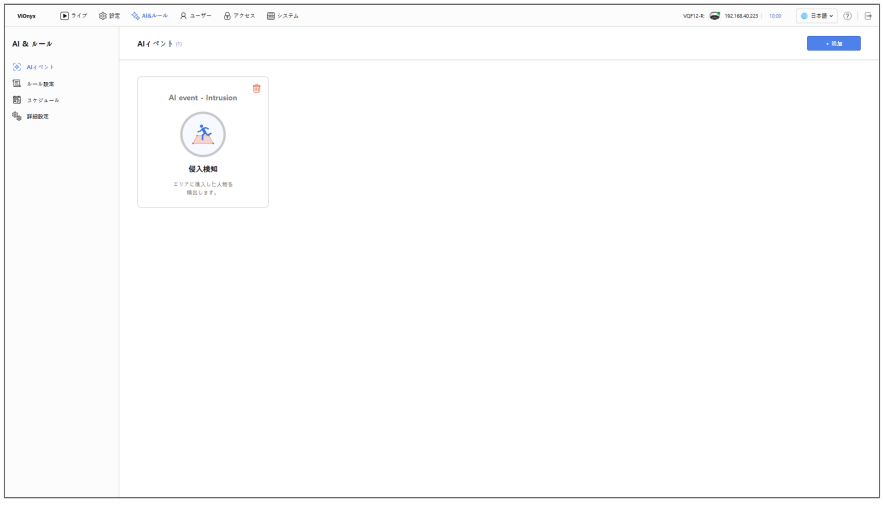
> **イベント条件**で選択した項目のみカウントします。例えば**進入**のみを選択すると、入場回数だけをイベントとして表示し、ログに記録します。

- **全イベントカウントリセット**：すべての侵入領域のイベントカウントを毎日指定した時刻に初期化するには、**オン**に設定してください。**リセット時間**で設定した時刻に、すべての侵入領域のイベントカウントを初期化します。

> **情報**
>
> - **イベントカウント**を**オン**に設定すると、**ライブ**メニューの映像上で、侵入領域ごとに**カウント：N**形式で表示します。イベントカウントを手動で初期化するには、•••ボタンをクリックし、**カウントリセット**を選択してください。
>
> 
>
>
> - ファームウェアバージョン1.1.0以降は、イベントカウント関連オプションをサポートします。

7 設定を保存

すべての設定を完了したら、右上の**作成**ボタンをクリックしてください。前の画面に戻り、新しく作成したAIイベントが一覧に追加されます。



ライブで確認

画面左上の**ライブ**メニューをクリックしてください。カメラ映像の右上にある AI アイコンがオンになっているか確認してください。設定した侵入領域と顔領域が映像にオーバーレイ表示されます。人物が侵入領域に入る、または出るたびにイベントが発生します。顔領域を設定している場合、カメラは当該領域で顔を検知し、登録済みユーザーは自動的に識別され名前が表示されます。



情報

- 登録されていないユーザーは**未認識の顔**として表示されます。登録済みユーザーは名前とともに表示されます。
- 照明が不足しているか逆光の場合、カメラが顔を認識できないことがあります。撮影エリアの照明を改善するか、カメラの位置と角度を調整して顔が見えやすくしてください。
- 顔がカメラに向いている必要があります。横顔や後ろ姿は認識が難しい場合があります。

ライン通過検知イベントの設定

ライン通過検知イベントを設定すると、設定した仮想ラインを通過する人を検知し、リアルタイムでイベントを発生させます。通過方向（A→B、B→A、双方向）を指定して特定の方向の出入りのみを監視できます。任意で顔領域を追加すると、登録済みユーザーを自動で識別します。

いつ使用しますか？

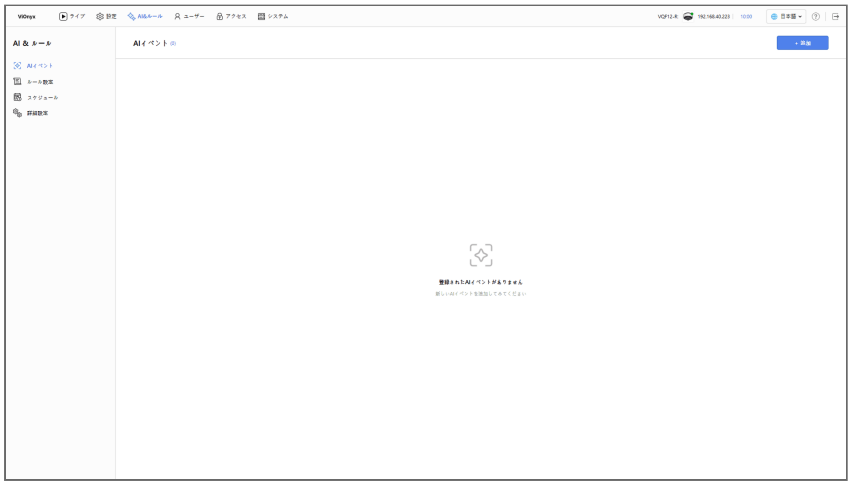
- 出入口の通行量監視およびカウント
- 特定方向への出入りのみを監視（一方向通路の検知）
- 営業時間外の特定エリアへの出入りを検知
- ラインを基準に左右エリアの移動を追跡

ライン通過検知イベントの作成

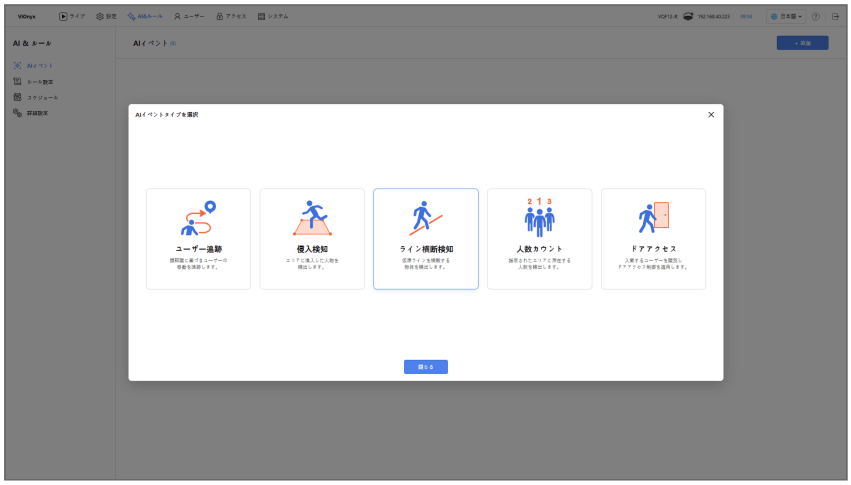
ライン通過検知イベントを作成すると、**ライブ** メニューで特定エリアを人がラインを通過するのを検知してイベントを発生させます。また、顔領域を設定すると当該領域で顔を優先的に追跡でき、登録済みユーザーは自動で識別されます。

1 イベント作成の開始

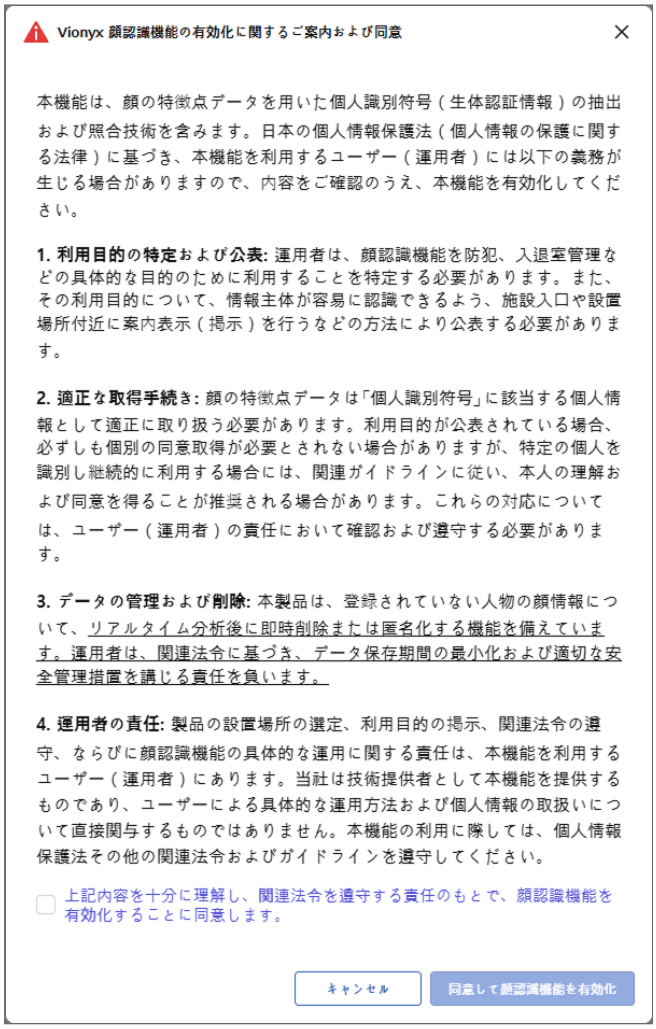
1. 画面左上の **AI&ルール** メニューをクリックします。
2. 画面左のサイドバーで **AIイベント** をクリックしてください。



3. 画面右上の**+ 追加**ボタンをクリックしてください。
4. **AIイベントタイプを選択** 画面で **ライン横断検知** をクリックします。

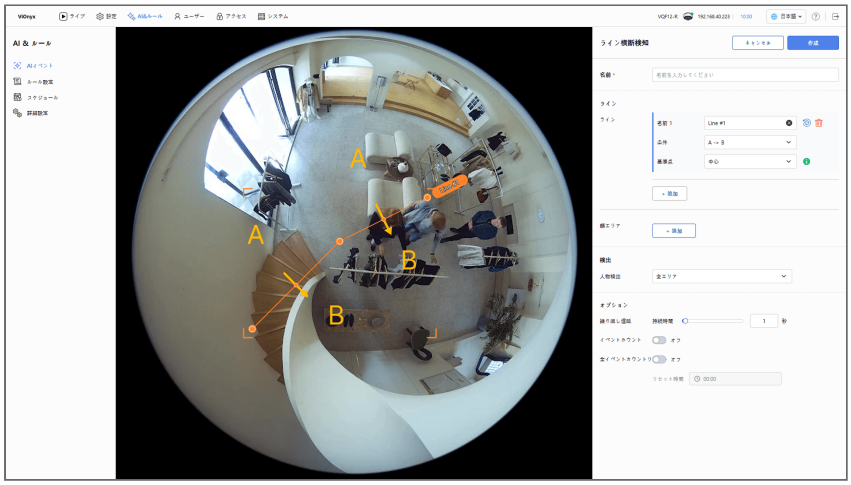


5. **Vionyx 顔認識機能の有効化に関するご案内および同意** ポップアップが表示されたら、内容を確認し、同意チェックボックスをクリックしてから **同意して顔認識機能を有効化** ボタンをクリックします。



- 顔認証機能を使用するには、該当地域の関連法規を遵守する必要があります。同意しない場合は先に進めません。
- 「**Vionyx 顔認識機能の有効化に関するご案内および同意**」ポップアップは初回のみ表示されます。以降、AIイベント作成時は同意済みとみなします。

6. 右側の**ライン横断検知**パネルで必要な設定を完了してください。

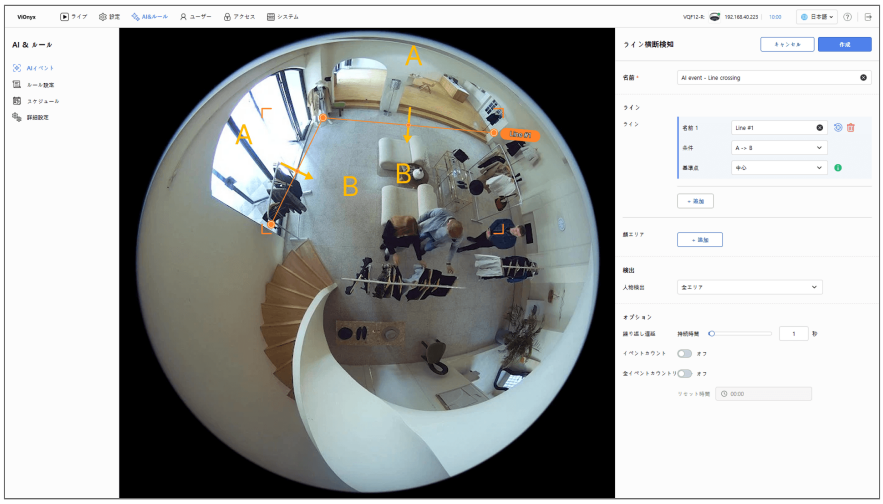


❷ イベント名の設定

名前 入力フィールドに AI イベント名を入力します。名前は最大64文字まで入力できます。

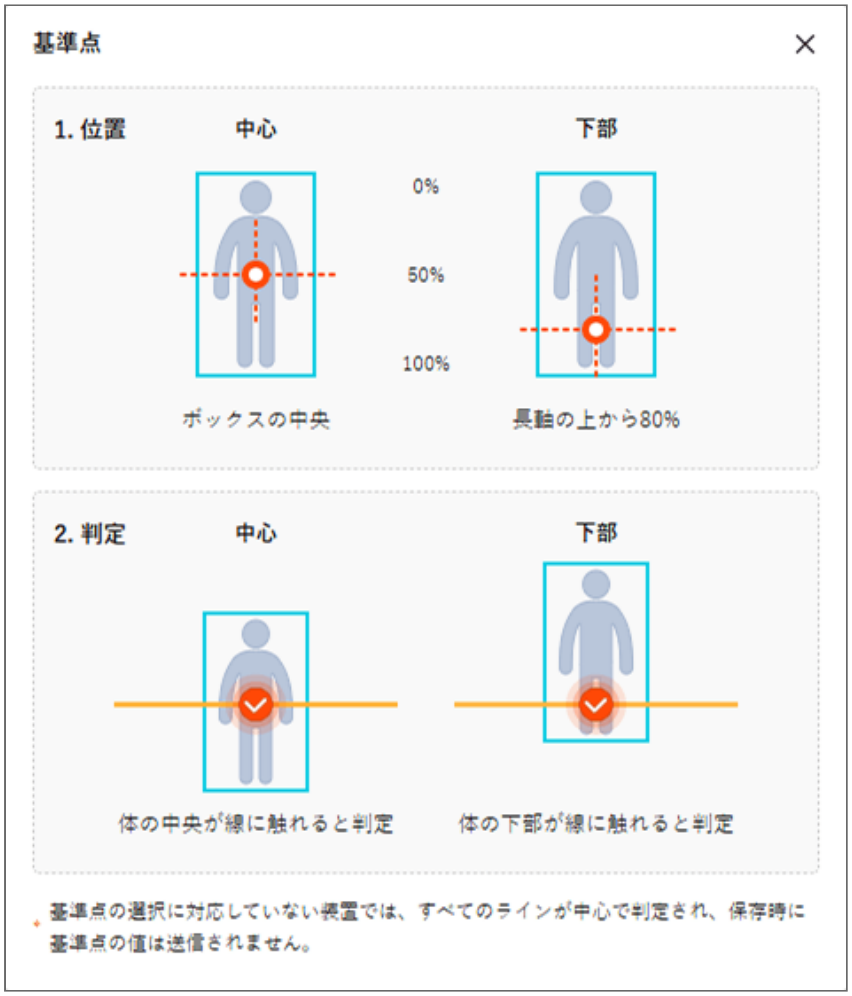
❸ 仮想ラインの設定

ライブビューで仮想ラインを適切な位置に設定してください。カメラに設定した仮想ラインを通過する人を検知してイベントを発生させます。最低1本を設定する必要があり、**+ 追加**ボタンをクリックして最大10本まで追加できます。ライブビューにオレンジ色のラインが表示され、マウスで角や点をドラッグして形状を調整できます。中央の領域をドラッグして位置を移動できます。



- **名前**：仮想ラインの名前を編集できます。わかりやすい名前を付けてください。仮想ラインの名前はライブビューでマウスオーバーすると表示されます。
- **条件**：仮想ラインを通過する条件を設定してください。以下の3つの通過方向オプションからいずれかを選択できます。
  - **A -> B**：AからB方向への通過でイベントが発生します。
  - **B -> A**：BからA方向への通過でイベントが発生します。
  - **A <-> B**：双方向の通過でイベントが発生します。
- **基準点**：人が仮想ラインを通過したかを判定する際に、人検知ボックスのどの位置を基準にするか選択してください。ラインごとに設定でき、デフォルトは **中心** です。
  - **中心**：ボックスの中心を基準に判定します。体の中心がラインに触れると、通過したと判定します。
  - **下部**：ボックスの長軸に沿って上端から 80% の位置を基準に判定します。体の下側がラインに触れると、通過したと判定します。床にラインを描く場合のように、足がラインを越えた時点でイベントを発生させるには、このオプションを選択してください。

基準点 右側の ⓘ アイコンをクリックして、各基準点の位置と判定方法を図で確認してください。



情報

- **基準点** オプションはファームウェア バージョン 1.1.0 以降でサポートします。基準点の選択をサポートしないデバイスでは、すべてのライン通過を **中心** として判定します。
- **下部** は人検知ボックスを基準に計算した位置であり、実際の足位置を検出するものではありません。
- **ライブ** メニューで判定基準点を確認するには、AI 表示オプションで **基準点** オプションをオンにしてください。
- 設定した仮想ラインの形状とサイズを初期化するには、ボタンをクリックしてください。
- 追加した仮想ラインを削除するには、ボタンをクリックしてください。

4 顔領域の設定（任意）

顔を検知する領域を設定してください。設定すると、当該領域で顔を優先的に追跡します。顔領域と仮想ラインは重ねて設定できます。**+ 追加**ボタンをクリックして最大10個まで設定できます。ライブビューに青い枠が表示され、マウスで角や点をドラッグして形状を調整できます。中央の領域をドラッグして位置を移動できます。



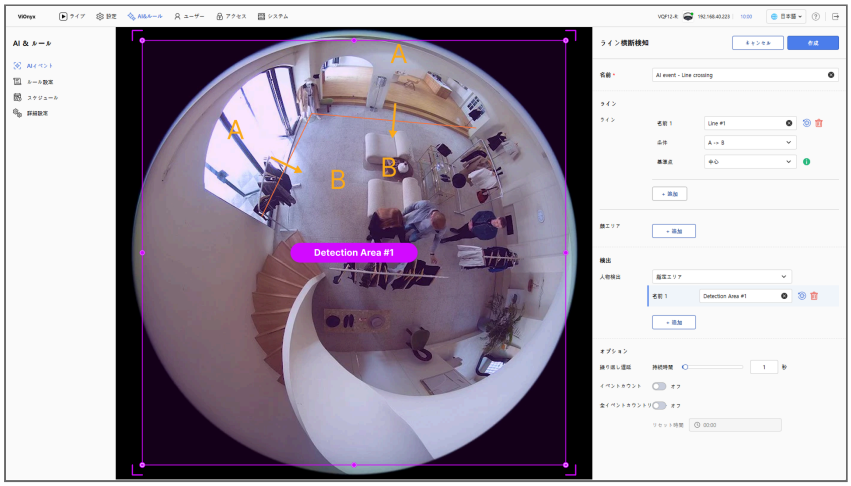
- **名前**：顔領域の名前を編集できます。わかりやすい名前を付けてください。顔領域の名前はライブビューでマウスオーバーすると表示されます。

> **情報**
>
> - 登録済みユーザーは**ライブ**メニューで自動的に識別され、名前が表示されます。登録されていないユーザーは**未認識の顔**として表示されます。
> - 設定した顔領域の形状とサイズを初期化するには、ボタンをクリックしてください。
> - 追加した顔領域を削除するには、ボタンをクリックしてください。
> - カメラ設定で **適応型自動露出** 適応型自動露出オプションを使用する場合は、人が実際に立っている、または通過する際に顔がよく見える位置が顔領域に含まれるように設定してください。

5 人検出の設定（任意）

検出 セクションで、カメラが人を検出する範囲を選択します。検出範囲を必要な場所に絞ると、関心のないエリア（通路の端、窓、反射面など）での誤検出を減らせます。

- **全エリア**：デフォルト値です。画面全体で人を検出します。顔領域の設定に関係なく使用できます。
- **指定エリア**：指定した領域内でのみ人を検出します。顔領域を設定していない場合のみ選択できます。最低1本を設定する必要があり、**+ 追加**ボタンをクリックして最大10本まで追加できます。ライブビューに紫色の枠が表示されます。マウスで角または点をドラッグして希望の形に調整できます。中央の領域をドラッグして位置を移動できます。



  - **名前**：人検出領域の名前を編集できます。

- **顔エリアのみ**：顔領域内でのみ人を検出します。顔領域を設定した場合のみ選択できます。

> **情報**
>
> - **指定エリア**を選択した状態で顔領域を追加すると、**通知** ポップアップが表示されます。 **確認** ボタンをクリックすると、指定した検出領域が解除され、**顔エリアのみ**に変更されます。
> - **顔エリアのみ**を選択した状態で顔領域をすべて削除すると、**全エリア**に自動で変更されます。
> - カメラ設定で **適応型自動露出** オプションを使用する場合は、ディスプレイ、写真、ポスターなど人物が写ったものが検出範囲に含まれないよう、**指定エリア** または **顔エリアのみ** に範囲を絞ってください。
> - 設定した人検出領域の形状とサイズを初期化するには、 ボタンをクリックしてください。
> - 追加した人検出領域を削除するには、 ボタンをクリックしてください。
> - この機能のサポートは、ファームウェアバージョン1.1.0以降に含まれます。

6 イベント発生条件とカウントの設定

オプション セクションでイベント発生条件とイベントカウントを設定してください。



- **繰り返し遅延**：イベントとして認識する最小時間を設定してください。検知状態が設定した時間より長く続く場合にイベントが発生します。最大で60秒まで設定できます。

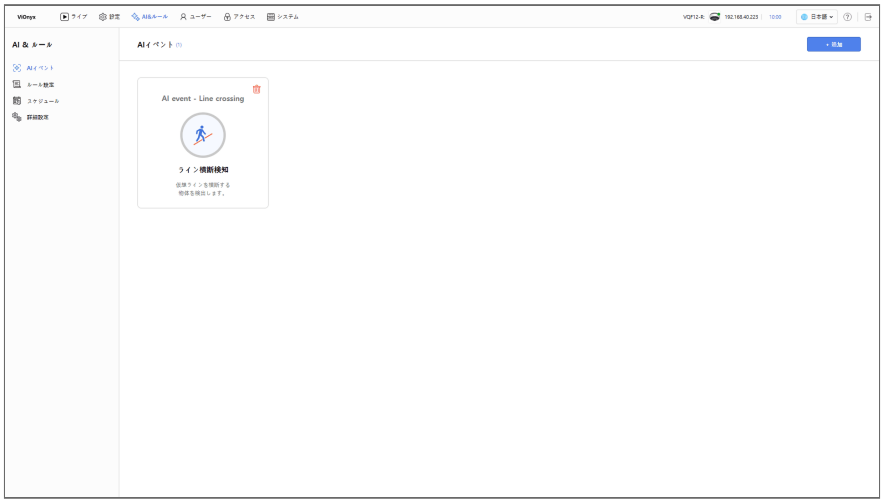
> イベントが多発する場合は、**繰り返し遅延**の値を増やしてください。設定した時間より短く検知した動きはイベントとして認識しないため、不要なイベントが減ります。

- **イベントカウント**：ラインを通過するたびに回数をカウントするには、**オン**に設定してください。ラインが複数ある場合、ラインごとにカウントします。
- **全イベントカウントリセット**：すべてのラインのイベントカウントを毎日指定した時刻に初期化するには、**オン**に設定してください。**リセット時間**で設定した時刻に、すべてのラインのイベントカウントを初期化します。

> **情報**
>
> - **イベントカウント**を**オン**に設定すると、**ライブ** メニューの映像上で、各ラインの上に **カウント : N** の形式で表示します。イベントカウントを手動で初期化するには、•••ボタンをクリックし、**カウントリセット**を選択してください。
>
> 
>
>
> - ファームウェアバージョン1.1.0以降は、イベントカウント関連オプションをサポートします。

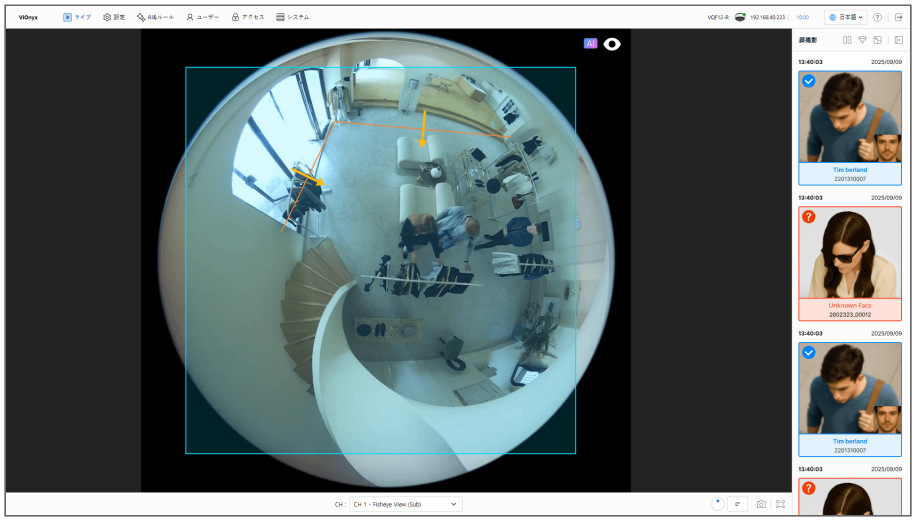
7 設定を保存

すべての設定を完了したら、右上の**作成**ボタンをクリックしてください。前の画面に戻り、新しく作成したAIイベントが一覧に追加されます。



ライブで確認

画面左上の**ライブ**メニューをクリックしてください。カメラ映像の右上にある AI アイコンがオンになっているか確認してください。設定した仮想ラインと顔領域が映像にオーバーレイ表示されます。人が仮想ラインを通過するたびにイベントが発生します。顔領域を設定している場合、カメラは当該領域で顔を検知し、登録済みユーザーは自動的に識別され名前が表示されます。



情報

- 登録されていないユーザーは**未認識の顔**として表示されます。登録済みユーザーは名前とともに表示されます。
- 照明が不足しているか逆光の場合、カメラが顔を認識できないことがあります。撮影エリアの照明を改善するか、カメラの位置と角度を調整して顔が見えやすくしてください。
- 顔がカメラに向いている必要があります。横顔や後ろ姿は認識が難しい場合があります。

人数カウントイベントの設定

人数カウントイベントを設定すると、指定したエリアに滞在する人数を検知できます。任意で顔領域を追加すると、登録済みユーザーを自動で認証します。

いつ使用しますか？

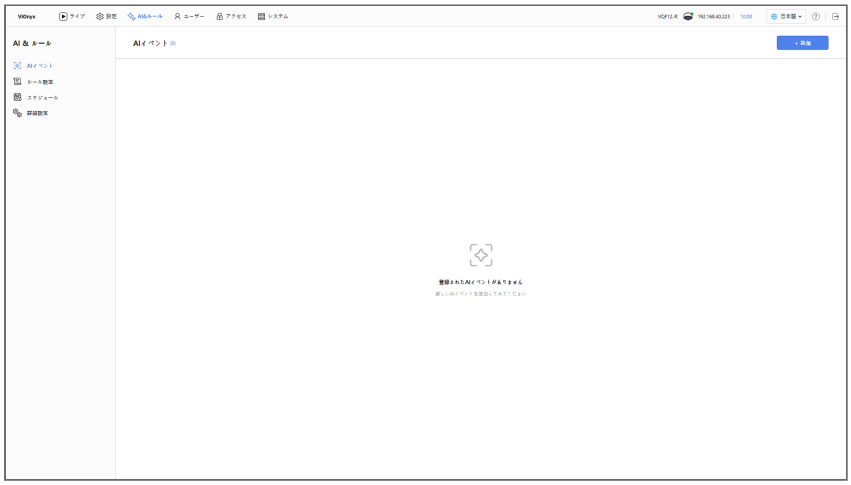
- 小売店または店舗内の特定エリアの訪問者数をリアルタイムで監視したい場合
- 混雑状況の管理のため、特定エリアの人数状況を把握したい場合
- 登録済みの従業員/VIP顧客の入退場状況を追跡したい場合
- セキュリティ目的で特定エリアの入退場統計を管理したい場合

人数カウントイベントの作成

人数カウントイベントを作成すると、**ライブ** メニューで指定したエリアに滞在する人数を検知できます。また、顔領域を設定すると当該領域で顔を優先的に追跡でき、登録済みユーザーは自動で識別されます。

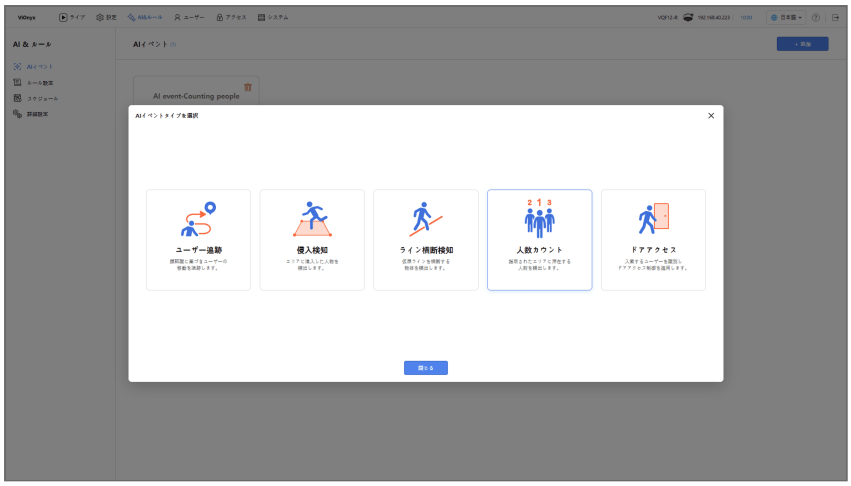
1 イベント作成の開始

1. 画面左上の **AI&ルール** メニューをクリックします。
2. 画面左のサイドバーで **AIイベント** をクリックしてください。

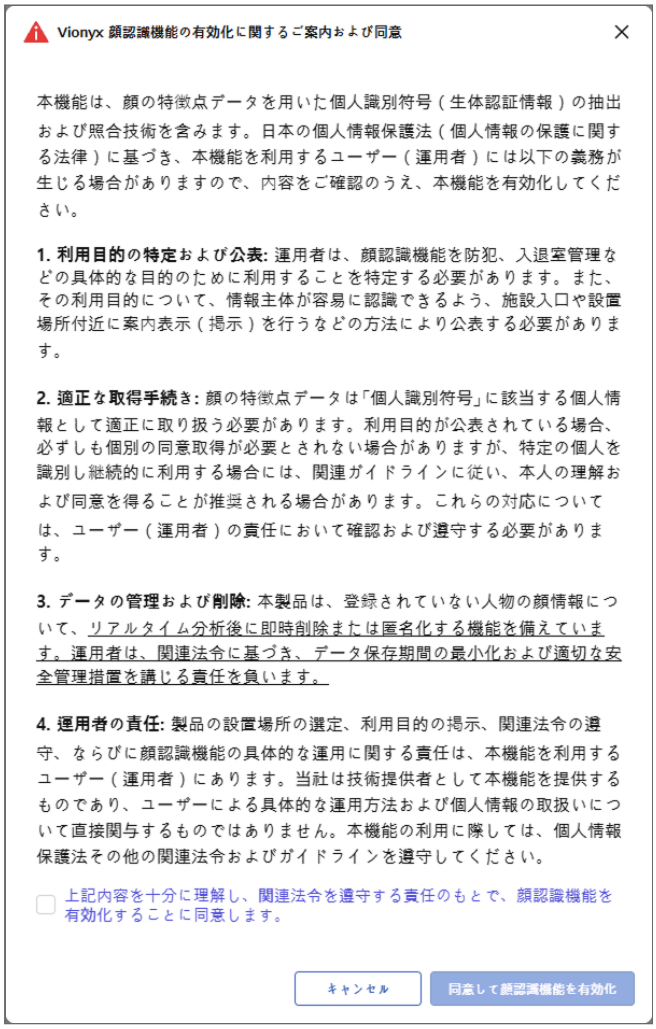


3. 画面右上の**+ 追加**ボタンをクリックしてください。

4. **AIイベントタイプを選択** ウィンドウで **人数カウント** をクリックします。

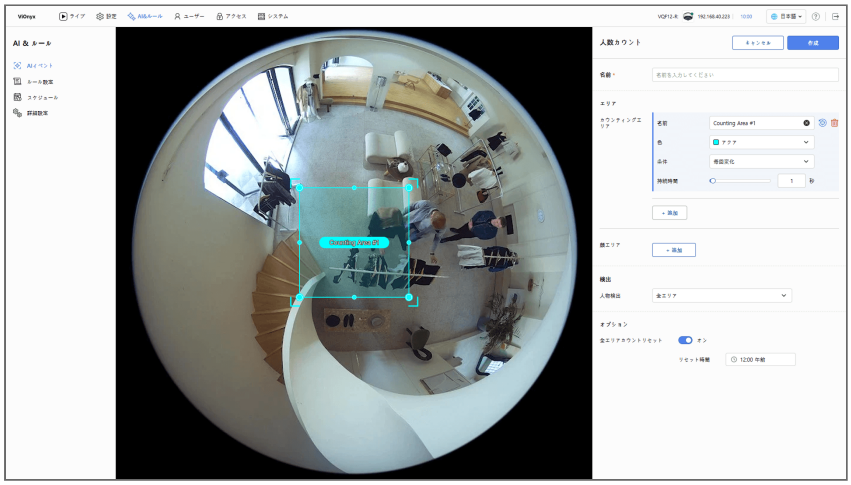


5. **Vionyx 顔認識機能の有効化に関するご案内および同意** ポップアップが表示されたら、内容を確認し、同意チェックボックスをクリックしてから **同意して顔認識機能を有効化** ボタンをクリックします。



- 顔認証機能を使用するには、該当地域の関連法規を遵守する必要があります。同意しない場合は先に進めません。
- 「**Vionyx 顔認識機能の有効化に関するご案内および同意**」ポップアップは初回のみ表示されます。以降、AIイベント作成時は同意済みとみなします。

6. 右側の **人数カウント** パネルで必要な設定を完了します。

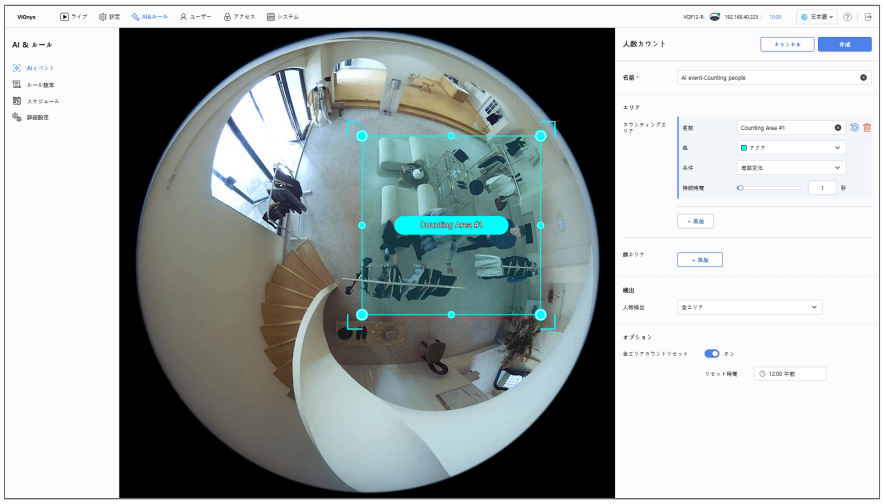


❷ イベント名の設定

名前 入力フィールドに AI イベント名を入力します。名前は最大64文字まで入力できます。

❸ カウント領域の設定

ライブビューでカウント領域を設定します。カメラは設定したカウント領域に滞在する人をリアルタイムでカウントし、イベントを発生させます。最低1本を設定する必要があり、**＋追加**ボタンをクリックして最大10本まで追加できます。ライブビューに表示されるカウント領域ボックスの角または点をマウスでドラッグして、希望の形に調整します。中央の領域をドラッグして位置を移動できます。



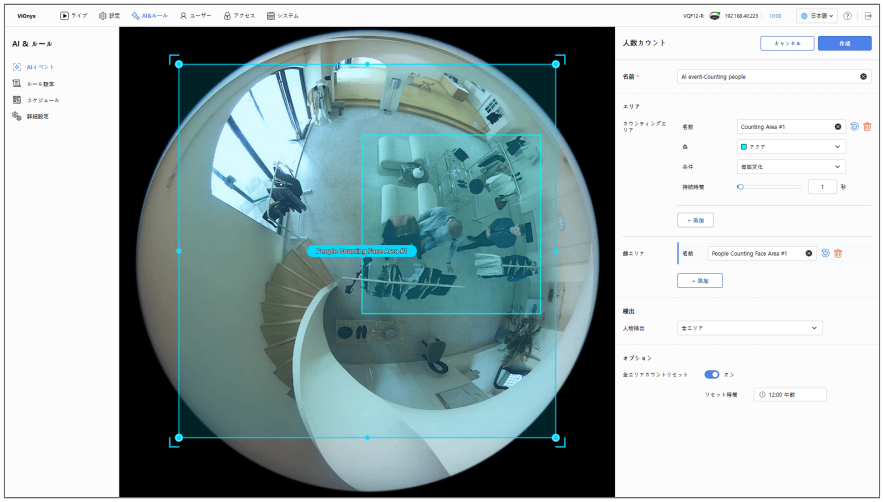
- **名前**：カウント領域の名前を編集できます。わかりやすい名前を付けてください。カウント領域の名前はライブビューでマウスオーバーすると表示されます。
- **色**：カウント領域の色を選択できます。ライブビューでカウント領域が選択した色で表示されます。
- **条件**：イベント発生条件を設定します。
  - **毎回変化**: 人がカウントエリアに入る、または出るたびにイベントが発生
  - **カウント制限**: カウントエリアに滞在する人数が指定数を超えるとイベントが発生します（既定値 10人、最大値 100人）
- **持続時間**：カウント領域に滞在する人数がイベント発生条件を満たすための最小継続時間を設定します。例えば、Duration を 5 秒に設定すると、人物がカウント領域に 5 秒以上滞在した場合にイベントが発生します。最大で60秒まで設定できます。

> **情報**
>
> - 設定したカウント領域の形状とサイズを初期化するには、ボタンをクリックします。
> - 追加したカウント領域を削除するには、ボタンをクリックします。

❹ 顔領域の設定（任意）

顔を検知する領域を設定してください。設定すると、当該領域で顔を優先的に追跡します。顔領域とカウント領域は重ねて設

定できます。**+追加**ボタンをクリックして最大10個まで設定できます。ライブビューに青い枠が表示され、マウスで角や点をドラッグして形状を調整できます。中央の領域をドラッグして位置を移動できます。



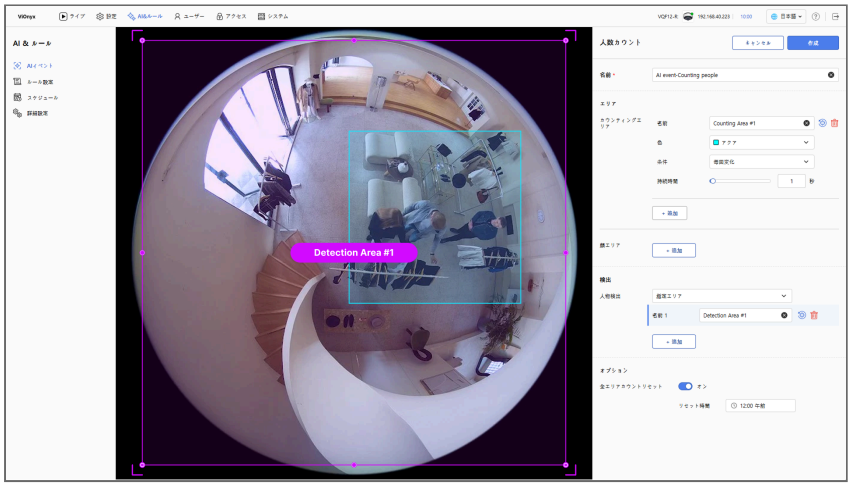
- **名前**：顔領域の名前を編集できます。わかりやすい名前を付けてください。顔領域の名前はライブビューでマウスオーバーすると表示されます。

> **情報**
>
> - 登録済みユーザーは**ライブ**メニューで自動的に識別され、名前が表示されます。登録されていないユーザーは**未認識の顔**として表示されます。
> - 設定した顔領域の形状とサイズを初期化するには、ボタンをクリックしてください。
> - 追加した顔領域を削除するには、ボタンをクリックしてください。
> - カメラ設定で **適応型自動露出** 適応型自動露出オプションを使用する場合は、人が実際に立っている、または通過する際に顔がよく見える位置が顔領域に含まれるように設定してください。

5 人検出の設定（任意）

検出 セクションで、カメラが人を検出する範囲を選択します。検出範囲を必要な場所に絞ると、関心のないエリア（通路の端、窓、反射面など）での誤検出を減らせます。

- **全エリア**：デフォルト値です。画面全体で人を検出します。顔領域の設定に関係なく使用できます。
- **指定エリア**：指定した領域内でのみ人を検出します。顔領域を設定していない場合のみ選択できます。最低1本を設定する必要があり、**+追加**ボタンをクリックして最大10本まで追加できます。ライブビューに紫色の枠が表示されます。マウスで角または点をドラッグして希望の形に調整できます。中央の領域をドラッグして位置を移動できます。



  - **名前**：人検出領域の名前を編集できます。

- **顔エリアのみ**：顔領域内でのみ人を検出します。顔領域を設定した場合のみ選択できます。

> **情報**
>
> - **指定エリア**を選択した状態で顔領域を追加すると、**通知** ポップアップが表示されます。 **確認** ボタンをクリックすると、指定した検出領域が解除され、**顔エリアのみ**に変更されます。
> - **顔エリアのみ**を選択した状態で顔領域をすべて削除すると、**全エリア**に自動で変更されます。
> - カメラ設定で **適応型自動露出** オプションを使用する場合は、ディスプレイ、写真、ポスターなど人物が写ったものが検出範囲に含まれないよう、**指定エリア** または **顔エリアのみ** に範囲を絞ってください。
> - 設定した人検出領域の形状とサイズを初期化するには、 ボタンをクリックしてください。
> - 追加した人検出領域を削除するには、 ボタンをクリックしてください。
> - この機能のサポートは、ファームウェアバージョン1.1.0以降に含まれます。

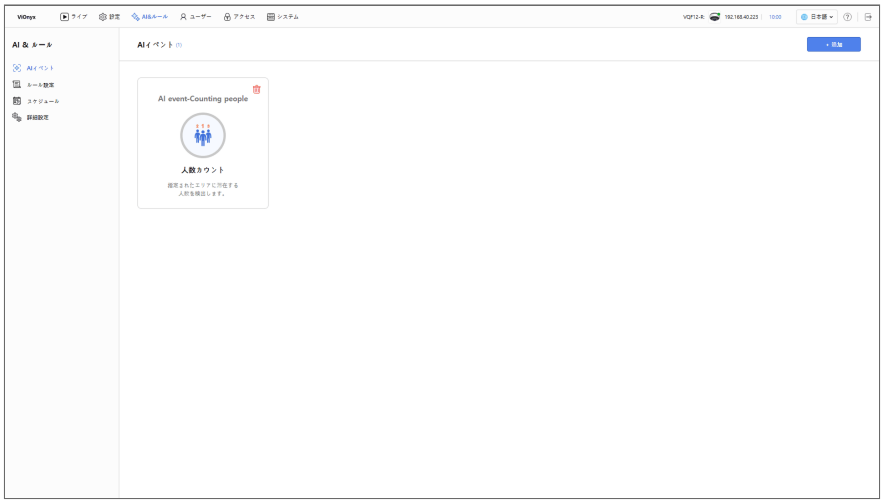
6 カウントの初期化設定

カウント領域に滞在する人数を初期化する条件を設定します。

- **全エリアカウントリセット**：すべてのカウント領域のカウントを定められた時間ごとに初期化するには、**オン** に設定します。 **リセット時間** で設定した時刻に、すべてのカウント領域のカウントが初期化されます。

7 設定を保存

すべての設定を完了したら、右上の**作成**ボタンをクリックしてください。前の画面に戻り、新しく作成したAIイベントが一覧に追加されます。



ライブで確認

画面左上の**ライブ**メニューをクリックしてください。カメラ映像の右上にある AI アイコンがオンになっているか確認してください。設定したカウント領域と顔領域が映像にオーバーレイ表示されます。カウントエリアに滞在する人数を **カウント：N** 形式で表示します。顔領域を設定している場合、カメラは当該領域で顔を検知し、登録済みユーザーは自動的に識別され名前が表示されます。



情報

- カウント値を手動で初期化するには、••• → **カウントリセット** ボタンをクリックします。



- 登録されていないユーザーは**未認識の顔**として表示されます。登録済みユーザーは名前とともに表示されます。
- 照明が不足しているか逆光の場合、カメラが顔を認識できないことがあります。撮影エリアの照明を改善するか、カメラの位置と角度を調整して顔が見えやすくしてください。
- 顔がカメラに向いている必要があります。横顔や後ろ姿は認識が難しい場合があります。

入退室制御イベントを設定する

入退室制御イベントを設定すると、ドアに近づく人を顔認証で識別し、ドア周辺の同行者も検証して入室を許可するか判断できます。認証済みユーザーに続いて未承認者が入室するテールゲーティング（Tailgating）を検知できます。また、ドア内側から出る人を判断対象から除外できます。

> **情報**
> 入退室制御イベントは、ファームウェア バージョン1.1.0以降で利用できます。

いつ使用しますか？

- ドアに近づく人が登録済みユーザーかどうかを顔認証で確認するとき
- 認証済みユーザーに続いて未承認者が入室するテールゲーティングを防止するとき
- ドア内側から出る人を除外し、入ってくる人だけを入退室判断の対象にするとき
- 入退室判断の結果に応じてドアを解錠したり、警告音声を出力したりする後続動作と連動するとき

> **情報**
> 入退室制御イベントは、入室を許可するかを判断するだけで、ドアのリレーを直接制御しません。判断結果に基づいてドアを解錠するには、イベントを作成した後にドアを登録し、イベントに関連付けてください。音声案内やWebhook通知などの追加動作が必要な場合は、ドアルールを設定してください。
>
> - 出入口の登録と管理の詳細については、ドア管理 を参照してください。
> - ドアルールの詳細については、出入口ルールの設定を参照してください。

入退室制御イベントの動作の仕組み

入退室制御イベントは、次の要素を組み合わせて入退室を許可するかどうかを判断します。設定を開始する前に、各要素の役割を確認してください。

構成要素	役割	必須かどうか
検証エリア	入退室制御エリアを囲む、より広いエリアです。このエリア内の人数と識別状態を確認し、テールゲーティングの有無を判断します。	必須
ドアアクセスエリア	ドアのすぐ前のエリアです。人がこのエリアに入ると入退室を試みたとみなし、判断を開始します。	必須
イベント進入ライン	出入口を実際に通過した人を判定するラインです。選択した方向に応じて、入場者、退場者、または両方を判定します。	必須
顔エリア	顔を優先して追跡し、ユーザーを識別するエリアです。	任意

カメラは、エリア内の人を次のいずれかの状態に分類します。

- **識別済み**：顔認証に成功し、登録済みユーザーとして確認された状態です。
- **未識別**：顔認証に失敗した、または登録済みユーザーと一致しない状態です。未登録の人、顔が隠れている人、またはカメラを向いていない人は、ライブメニューで **未認識の顔** と表示されます。

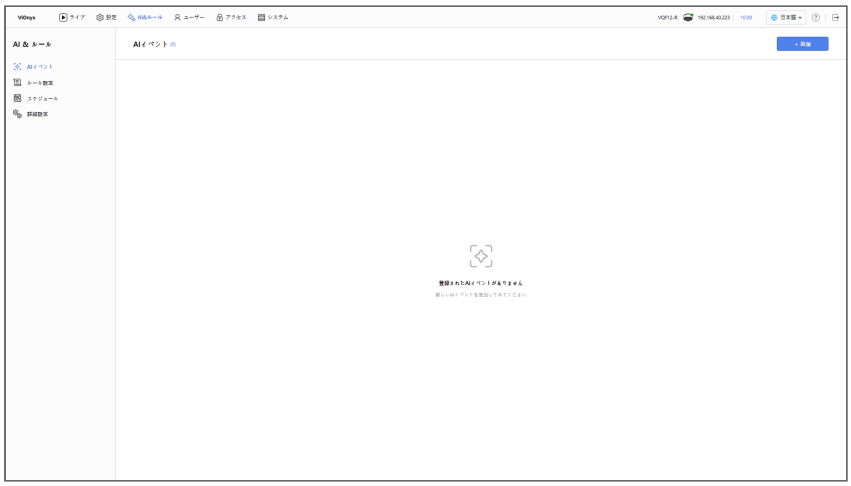
> **注意**
> セキュリティのため、顔を認証できない人を認証済みユーザーとして扱いません。アクセス制御エリアに入った人が未識別状態の場合、入室を許可しません。

アクセス制御イベントの作成

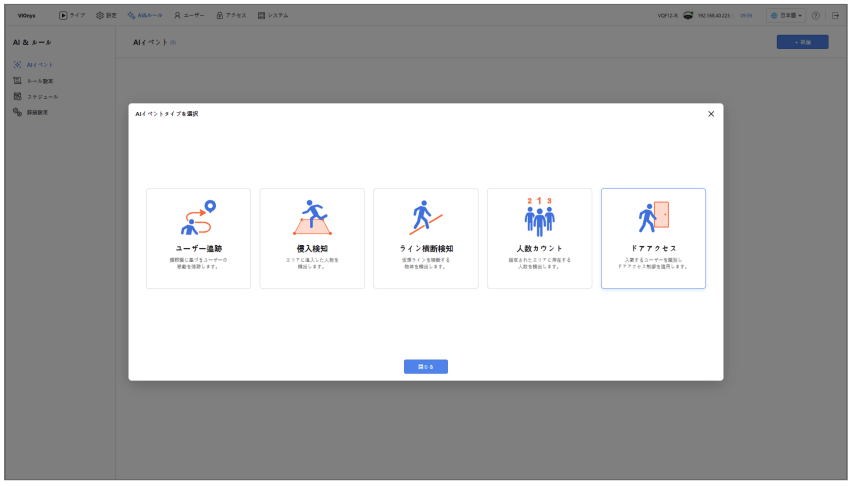
アクセス制御イベントを作成すると、**ライブ** メニューでドアに近づくユーザーを識別し、後から入る人を検証できます。

1 イベント作成の開始

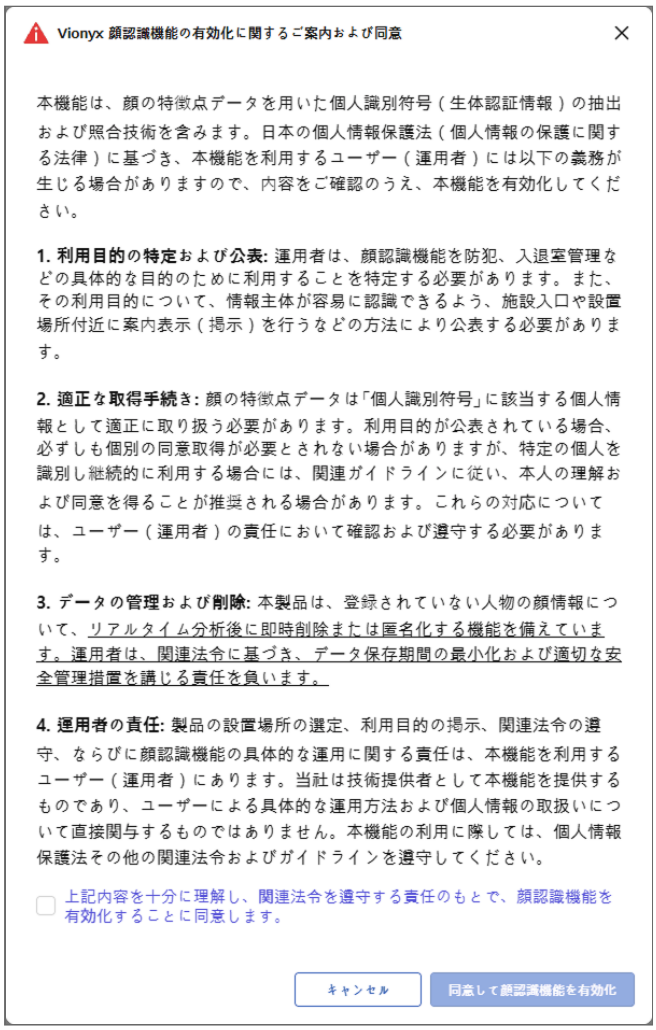
1. 画面左上の **AI&ルール** メニューをクリックします。
2. 画面左のサイドバーで **AIイベント** をクリックしてください。



3. 画面右上の**+ 追加**ボタンをクリックしてください。
4. **AIイベントタイプを選択**ウィンドウで**ドアアクセス**をクリックします。

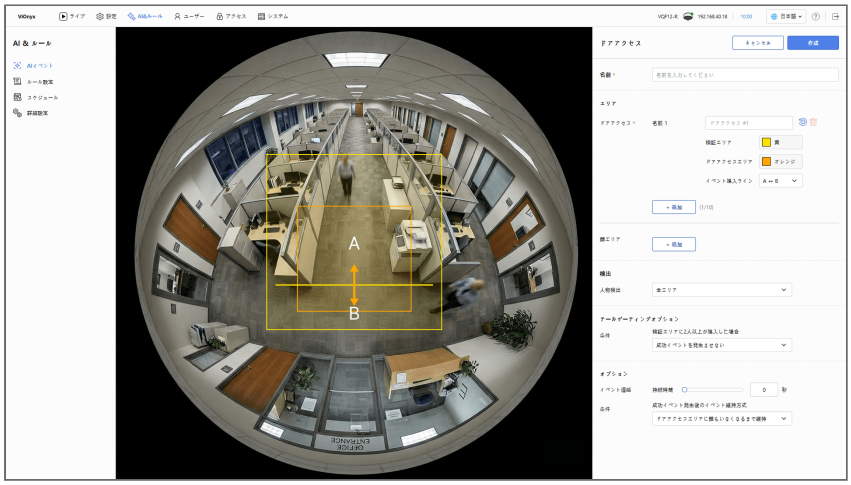


5. **Vionyx 顔認識機能の有効化に関するご案内および同意** ポップアップが表示されたら、内容を確認し、同意チェックボックスをクリックしてから **同意して顔認識機能を有効化** ボタンをクリックします。



> - アクセス制御イベントは顔認証でユーザーを識別するため、顔認証の使用に同意しないと作成できません。
> - 顔認証機能を使用するには、該当地域の関連法規を遵守する必要があります。
> - 「**Vionyx 顔認識機能の有効化に関するご案内および同意**」ポップアップは初回のみ表示されます。以降、AIイベント作成時は同意済みとみなします。

6. 右側の **ドアアクセス** パネルで必要な設定を完了してください。

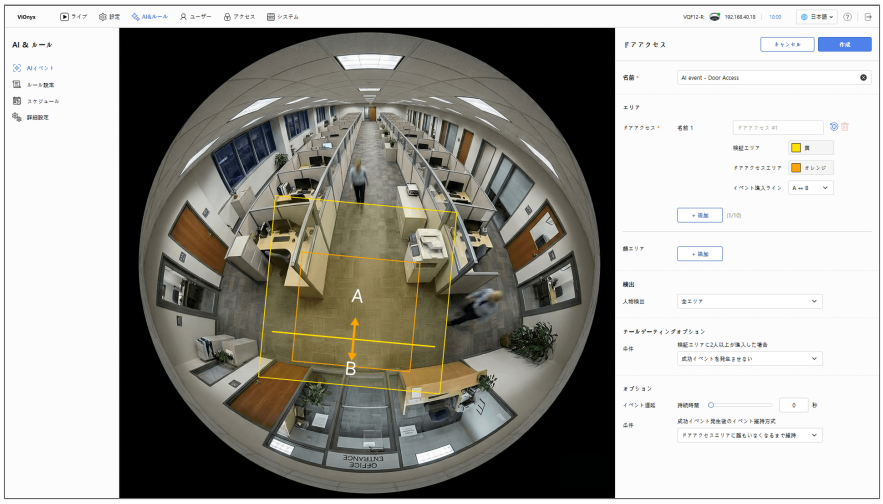


❷ イベント名の設定

名前 入力フィールドに AI イベント名を入力します。名前は最大64文字まで入力できます。

❸ アクセス制御エリアの設定

エリア セクションで、ドアの位置に合わせて検証エリア、アクセス制御エリア、イベント進入ラインを設定してください。最低1本を設定する必要があり、**+ 追加**ボタンをクリックして最大10本まで追加できます。追加するたびに、三つの要素が一つのまとまりとしてライブビューに表示されます。マウスで角または点をドラッグして形状を調整し、中央のエリアをドラッグして位置を移動してください。



- **名前**：アクセス制御エリアの名前を編集できます。ドアの位置など、わかりやすい名前を付けてください。
- **検証エリア**(黄色)：アクセス制御エリアを囲む検証エリアです。急接近する人や追尾する人も確認できるように、アクセス制御エリアより広く設定してください。
- **ドアアクセスエリア**(オレンジ色)：ドアのすぐ前で、入退室しようとする人が必ず通る位置に設定してください。人がこのエリアに入ると、入退室の判定を開始します。
- **イベント進入ライン**：出入口を実際に通過した人を判定するラインです。線の両端の点をドラッグし、入退室する人が必ず通るようにアクセス制御エリアを横切って配置してください。次に、判定する通過方向を選択してください。
  - **A → B**：AからB方向に通過する人だけを判定します。

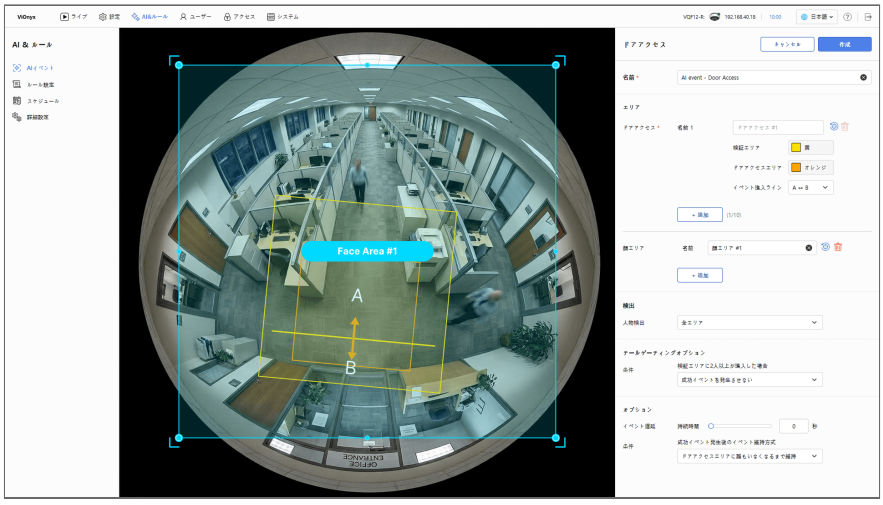
- **B → A**：BからA方向に通過する人だけを判定します。
- **A ↔ B**：両方向を判定します。入場者と退場者を区別して判定します。

入場者または退場者のどちらか一方だけを判定するには、ライブビューでAとBの位置を確認してから、**A → B**または**B → A**を選択してください。

> **情報**
>
> - 検証領域はアクセス制御領域を完全に含む必要があります。アクセス制御領域が検証領域から少しでもはみ出すと、保存できません。
> - イベント進入ラインはアクセス制御領域の外側まで延ばせますが、検証領域の外側には設定できません。
> - 設定した領域の形状とサイズを初期化するには、ボタンをクリックしてください。
> - 追加したアクセス制御領域を削除するには、ボタンをクリックしてください。

4 顔領域の設定（任意）

顔を検知する領域を設定してください。設定すると、当該領域で顔を優先的に追跡し、ユーザーを識別します。出入口に近づく人の顔が正面からよく見える位置に設定してください。顔領域とアクセス制御領域は重ねて設定できます。**+ 追加**ボタンをクリックして最大10個まで設定できます。ライブビューに青い枠が表示され、マウスで角や点をドラッグして形状を調整できます。中央の領域をドラッグして位置を移動できます。



- **名前**：顔領域の名前を編集できます。わかりやすい名前を付けてください。顔領域の名前はライブビューでマウスオーバーすると表示されます。

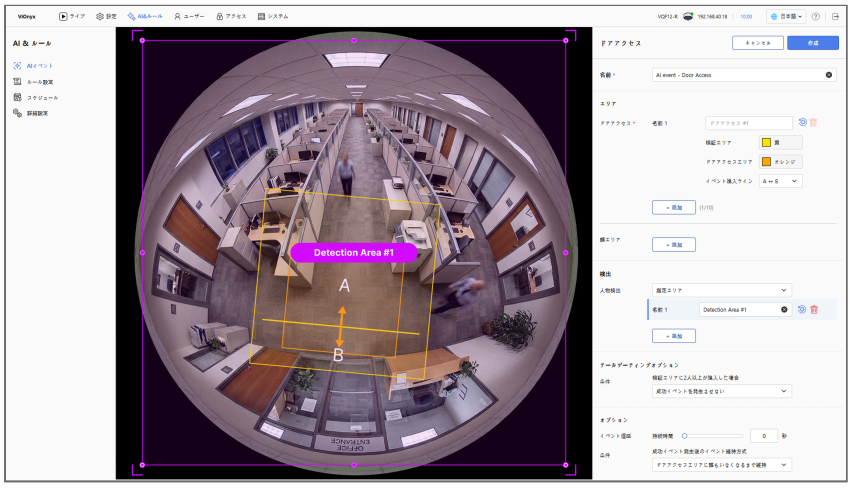
情報

- 登録済みユーザーは**ライブ**メニューで自動的に識別され、名前が表示されます。登録されていないユーザーは**未認識の顔**として表示されます。
- 設定した顔領域の形状とサイズを初期化するには、ボタンをクリックしてください。
- 追加した顔領域を削除するには、ボタンをクリックしてください。
- カメラ設定で **適応型自動露出** 適応型自動露出オプションを使用する場合は、人が実際に立っている、または通過する際に顔がよく見える位置が顔領域に含まれるように設定してください。

5 人検出の設定（任意）

検出 セクションで、カメラが人を検出する範囲を選択します。検出範囲を必要な場所に絞ると、関心のないエリア（通路の端、窓、反射面など）での誤検出を減らせます。

- **全エリア**：デフォルト値です。画面全体で人を検出します。顔領域の設定に関係なく使用できます。
- **指定エリア**：指定した領域内でのみ人を検出します。顔領域を設定していない場合のみ選択できます。最低1本を設定する必要があり、**+ 追加**ボタンをクリックして最大10本まで追加できます。ライブビューに紫色の枠が表示されます。マウスで角または点をドラッグして希望の形に調整できます。中央の領域をドラッグして位置を移動できます。



  - **名前**：人検出領域の名前を編集できます。
- **顔エリアのみ**：顔領域内でのみ人を検出します。顔領域を設定した場合のみ選択できます。

情報

- **指定エリア**を選択した状態で顔領域を追加すると、**通知** ポップアップが表示されます。 **確認** ボタンをクリックすると、指定した検出領域が解除され、**顔エリアのみ**に変更されます。
- **顔エリアのみ**を選択した状態で顔領域をすべて削除すると、**全エリア**に自動で変更されます。
- カメラ設定で **適応型自動露出** オプションを使用する場合は、ディスプレイ、写真、ポスターなど人物が写ったものが検出範囲に含まれないよう、**指定エリア** または **顔エリアのみ** に範囲を絞ってください。
- 設定した人検出領域の形状とサイズを初期化するには、 ボタンをクリックしてください。
- 追加した人検出領域を削除するには、 ボタンをクリックしてください。
- この機能のサポートは、ファームウェアバージョン1.1.0以降に含まれます。

6 テールゲーティングオプションの設定

テールゲーティングオプション セクションで、検証領域に2人以上いる場合に入退室をどのように判断するか選択してください。セキュリティレベルが高いオプションから順に並べました。

- **成功イベントを発生させない**: 検証領域に2人以上いる場合、識別結果に関係なく入退室を許可しません。一度に一人ずつだけ入退室する必要がある場所に適しています。
- **全員が有効な場合のみ成功イベント**: 検証領域にいる全員が登録済みユーザーとして識別された場合にのみ入退室を許可します。一人でも未識別の状態であれば、入退室を許可しません。
- **1人でも有効なら成功イベント**: 検証領域に登録されたユーザーが一人以上いる場合、入退室を許可します。未識別者が一緒でも入退室を許可するため、来訪者の同伴が多い場所に適しています。
- **イベント判定に影響なし**: 検証領域の人数を考慮せず、アクセス制御領域に入った人の識別結果だけで入退室の可否を判断します。

以下は、アクセス制御領域に登録済みユーザーがいて、検証領域に別の人が一緒にいる場合のオプション別の判断結果です。

オプション	入退室権限が有効なユーザーのみがいる場合	入退室権限が無効なユーザーが混在している場合
成功イベントを発生させない	入退室拒否	入退室拒否
全員が有効な場合のみ成功イベント	アクセス許可	入退室拒否
1人でも有効なら成功イベント	アクセス許可	アクセス許可
イベント判定に影響なし	アクセス許可	アクセス許可

ヒント

セキュリティが重要なドアでは、**全員が有効な場合のみ成功イベント** 以上のオプションを使用してください。

7 イベント発生条件の設定

オプション セクションでイベント発生条件を設定します。

- **イベント遅延**：イベントとして認識する最小時間を設定してください。検知状態が設定した時間より長く続く場合にイベントが発生します。最大で60秒まで設定できます。

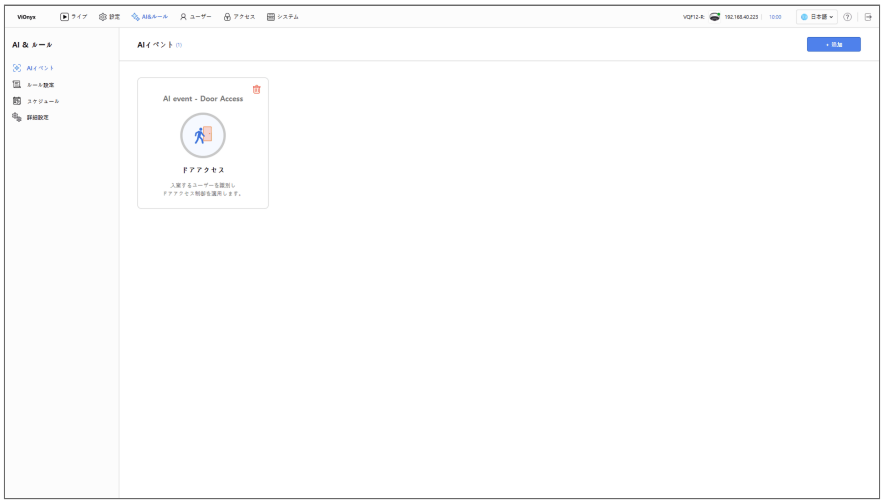
> ドア前を短時間通過する人が原因でイベントが頻繁に発生する場合は、**イベント遅延** の値を増やしてください。設定した時間より短く検知した動きはイベントとして認識しないため、不要なイベントが減ります。

- **条件**：アクセスが許可された後、イベントをいつまで維持するか選択してください。イベントを維持している間、連動動作（例：ドア解錠）も継続します。
  - **ドアアクセスエリアに誰もいなくなるまで維持**：アクセス制御エリアに誰もいなくなるまでイベントを維持します。認証済みユーザーがドアの前にいる間、再認証しなくてもドアの解錠状態を維持します。
  - **エリアが無人になるかテールゲーティング違反時に解除**：アクセス制御エリアに誰もいない場合、または未許可者が検証エリアに入りテイルゲイティングオプション条件に違反すると、直ちにイベントを解除します。ドアが開いている間に未許可者が後に続いて入るのを防げます。
  - **進入時に1回のみ発生（維持なし）**：イベントを維持せず、アクセス制御エリアに入るたびに一度だけイベントを発生させます。

> **情報**
> 登録済みユーザーがドアの前でためらって入れない場合、アクセス制御エリアから出て、再度入るとドアが開きます。この不便を減らしつつセキュリティも維持するには、**エリアが無人になるかテールゲーティング違反時に解除** を選択してください。

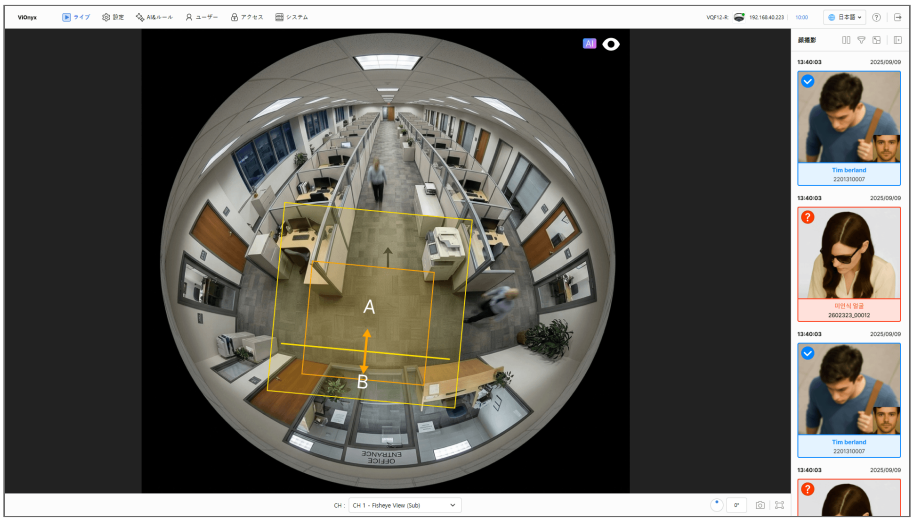
8 設定を保存

すべての設定を完了したら、右上の**作成**ボタンをクリックしてください。前の画面に戻り、新しく作成したAIイベントが一覧に追加されます。



ライブで確認

画面左上の**ライブ**メニューをクリックしてください。カメラ映像の右上にある AI アイコンがオンになっているか確認してください。映像に、設定した検証エリア、アクセス制御エリア、イベント進入ライン、顔領域をオーバーレイ表示します。人がアクセス制御エリアに入ると、識別結果とテイルゲイティングオプションに基づき、アクセス許可またはアクセス拒否イベントが発生します。



> **情報**
>
> - 登録されていないユーザーは**未認識の顔**として表示されます。登録済みユーザーは名前とともに表示されます。
> - 照明が不足しているか逆光の場合、カメラが顔を認識できないことがあります。撮影エリアの照明を改善するか、カメラの位置と角度を調整して顔が見えやすくしてください。
> - 顔がカメラに向いている必要があります。横顔や後ろ姿は認識が難しい場合があります。顔を認識できない人は未識別状態として処理し、アクセスを拒否します。

次のステップ

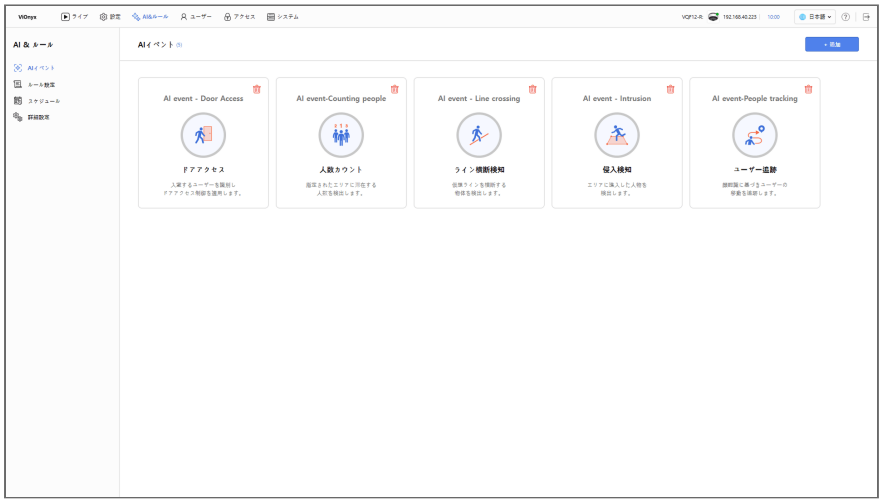
アクセス制御イベントはアクセスの許可/拒否だけを判定します。判定結果に応じて音声案内、Webhook通知、警告灯などの追加動作を実行するには、ドアルールを設定してください。
アクセス制御イベントを作成したら、ドアを登録し、イベントを関連付けてください。アクセスが許可されると、ドアに接続されたリレーが動作し、ドアが開きます。

AIイベントの編集と削除

作成したAIイベントの設定を編集したり、不要になったイベントを削除したりできます。

AIイベント設定の編集

1. 画面左上の **AI&ルール** メニューをクリックします。
2. 画面左のサイドバーで **AIイベント** をクリックしてください。



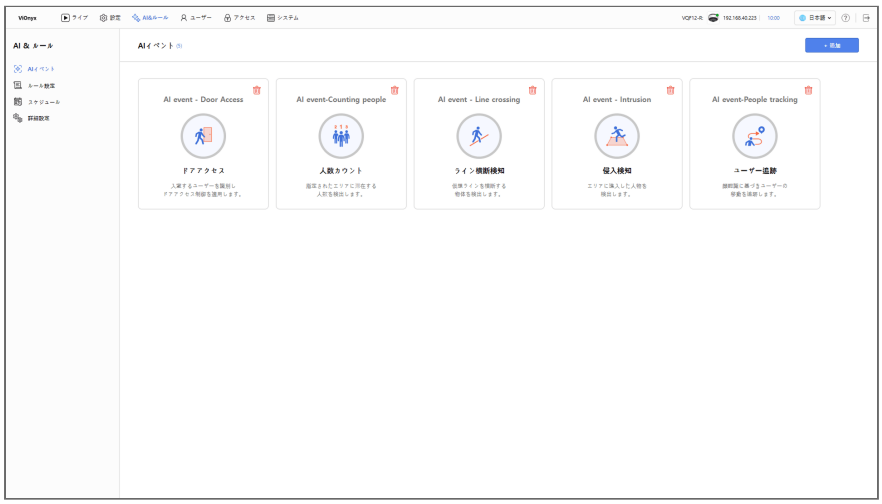
3. 編集するAIイベントをクリックします。
4. 右側のパネルでAIイベントの設定を編集します。
5. すべての設定が完了したら、右上の **更新** ボタンをクリックします。

前の画面に戻り、AIイベント一覧で編集したイベントを確認できます。

> **情報**
> 各イベント設定の詳細については、次のドキュメントを参照してください。
>
> - ユーザー追跡イベントを設定
> - 侵入検知イベントを設定
> - ライン通過検知イベントの設定
> - 人数カウントイベントの設定
> - 入退室制御イベントを設定する

AIイベントの削除

1. 画面左上の **AI&ルール** メニューをクリックします。
2. 画面左のサイドバーで **AIイベント** をクリックしてください。



3. 削除するAIイベントの右側にある  ボタンをクリックします。
4. 警告メッセージが表示されたら内容を確認し、**確認** ボタンをクリックします。

> **情報**
>
> - 削除したAIイベントは復元できません。削除すると、AIイベントに連動するルール（Rule）も削除されます。
> - AIイベントを削除すると、システムログに削除イベントが記録されます。

AIルールの設定

AIルールを使用すると、イベント種類と条件に応じてオーディオ再生、webhook 送信、リレー動作を自動で実行できます。このドキュメントではルールの作成と運用の全手順を案内します。

次のような場合にAIルールを設定してください。

- 特定のAIイベント発生時に外部サーバーへ webhook を送信する場合
- 特定のAIイベント発生時にデバイスでオーディオを再生する場合
- 特定のAIイベント発生時に入退室ドアなどに接続されたリレーを動作させる場合
- イベント種類ごとに異なる後続動作を自動化する場合

開始する前に

ルール設定を開始する前に、以下を確認してください。

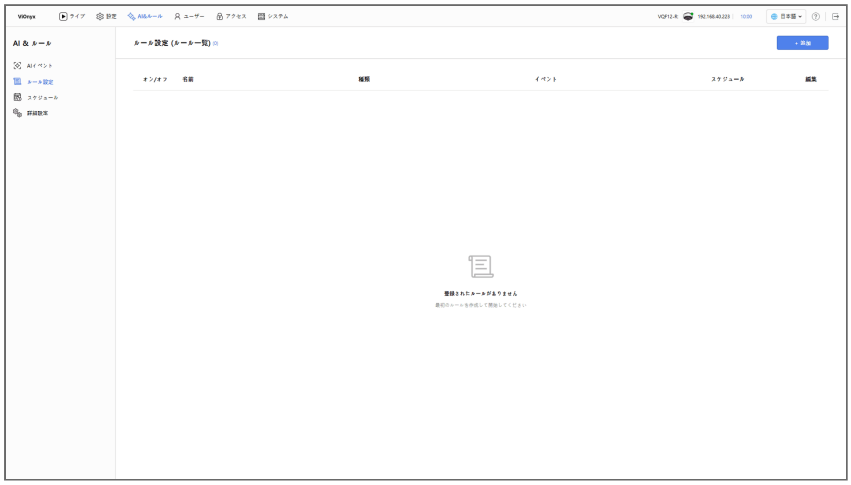
- AIイベントが事前に作成されている必要があります。次のドキュメントを参照してAIイベントを作成してください。
  - ユーザー追跡イベントを設定
  - 侵入検知イベントを設定
  - ライン通過検知イベントの設定
  - 人数カウントイベントの設定
- オーディオを使用する場合は、再生するオーディオクリップを事前に用意してください。
- Webhook を使用する場合は、受信URLを事前に用意してください。
- リレーを使用する場合、デバイスまたはサブデバイスのリレーポートが接続されているか確認してください。
- オーディオ、Webhook、リレーのうち、少なくとも一つの動作を設定する必要があります。

> **情報**
>
> AIイベントのうち **ドアアクセス** は、AIルールの条件として使用できません。

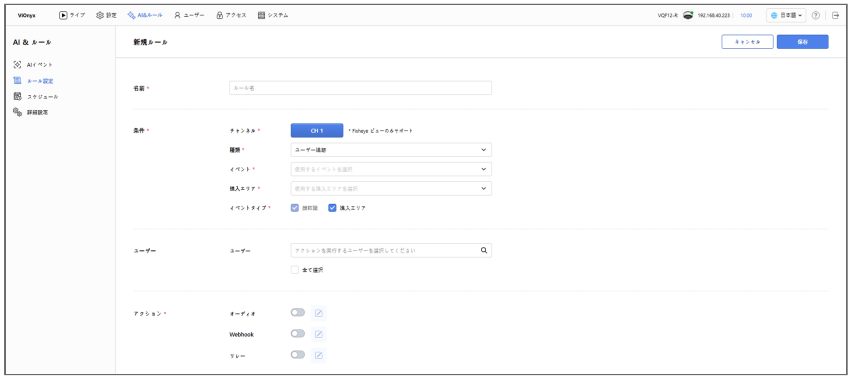
AIルールの作成

1 ルール作成の開始

1. 画面左上の **AI&ルール** メニューをクリックします。
2. 画面左のサイドバーで **ルール設定** をクリックします。



3. 画面右上の**+ 追加**ボタンをクリックしてください。
4. **新規ルール** 画面が表示されたら、ルール名を入力し、条件と動作を設定します。



2 ルール名の入力

名前 入力フィールドにルール名を入力します。ルール名は必須項目です。最大64文字まで入力できます。

3 条件の設定

条件はAIイベント発生時にルールが実行されるかを決定する要素です。 **条件** セクションで案内に従って条件を設定してください。 **種類** と **イベント** オプションは、AIイベント作成時に設定した内容に応じて表示されます。

- **チャンネル**：チャンネルはCH 1に固定されています。 Fisheyeビューのみサポートします。
- **種類**：AIイベントタイプを選択します。次のいずれかを選択できます。
  - **ユーザー追跡**

  - **侵入検知**
  - **ライン横断検知**
  - **人数カウント**

- **イベント**：ルールを実行するAIイベントを選択します。イベント一覧には選択したタイプに該当するAIイベントが表示されます。イベントは (ID:N) event_name 形式で表示されます。
- **進入エリア** / **侵入エリア** / **ライン** / **カウンティングエリア**：選択したイベントタイプに応じて、エリアの条件を追加できます。
- **イベントタイプ**：ルール実行の判定に使うイベントタイプを選択します。選択したイベントタイプに応じてルールが実行されます。

> 少なくとも1つのイベントタイプを選択する必要があります。

4 ユーザー選択

登録済みユーザーから、ルールの実行を判断するユーザーを **ユーザー** セクションで選択してください。選択したユーザーをAIイベントが検知すると、ルールが実行されます。

- 特定のユーザーを選択するには、**アクションを実行するユーザーを選択してください** をクリックしてください。ユーザー一覧が表示されたら、ユーザーを選択し、**保存** ボタンをクリックしてください。
- 登録済みの全ユーザーを選択するには、**全て選択** をクリックしてください。

5 オーディオ動作の設定

オーディオ動作は、AIイベント発生時にカメラでオーディオを再生する機能です。 **アクション** セクションで **オーディオ** トグルボタンをクリックして動作を有効にした後、 ボタンをクリックしてください。オーディオ設定ポップアップが表示されます。



- **オーディオクリップ**：再生するオーディオクリップを選択します。オーディオクリップはシステムにアップロードされた一覧から選択できます。
- **繰り返し**：オーディオの再生回数を設定します。設定した回数だけオーディオクリップを繰り返し再生します。最大 10

回まで設定できます。

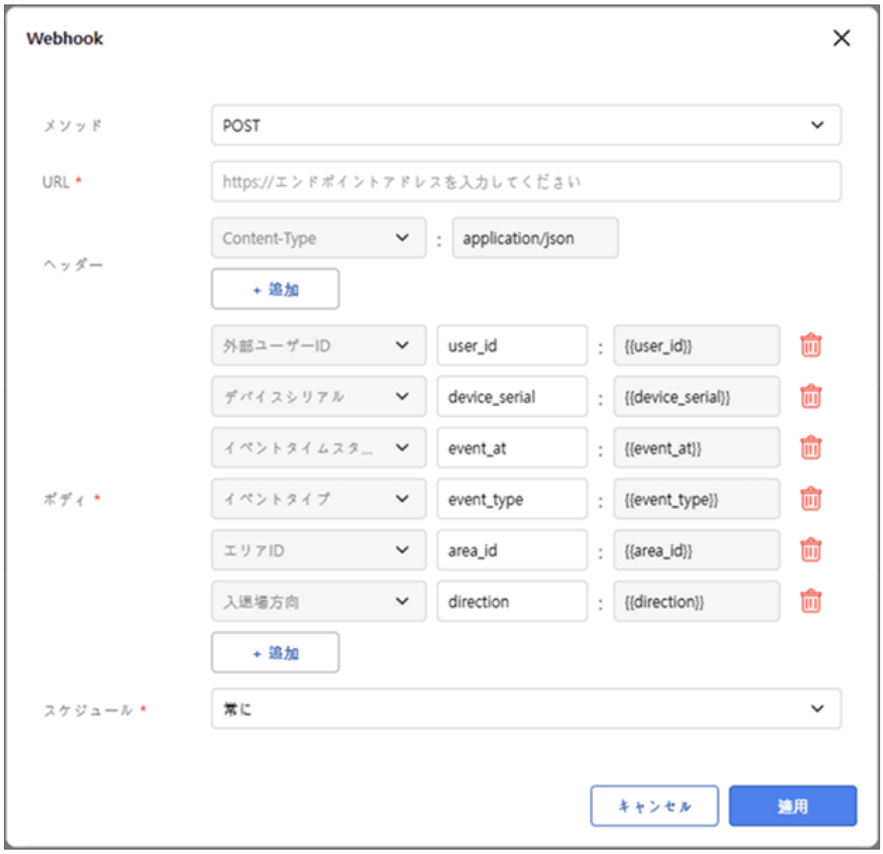
- **スケジュール**：ルールが実行され、オーディオを再生するスケジュールを選択してください。

オーディオ動作の設定を保存するには、**適用** ボタンをクリックします。

> **情報**
>
> - オーディオ動作を設定する前に、オーディオクリップを事前に用意してください。オーディオクリップは **システム** → **オーディオ** メニューでアップロードできます。詳細は オーディオクリップのアップロード を参照してください。
> - スケジュールは **AI&ルール** → **スケジュール** で作成、修正、削除できます。スケジュール管理の詳細は、スケジュール管理をご参照ください。

6 Webhook 動作の設定

Webhook 動作は、AIイベント発生時に外部サーバーへ webhook を送信する機能です。 **アクション** セクションで **Webhook** トグルボタンをクリックして動作を有効にした後、 ボタンをクリックしてください。 webhook 設定ポップアップが表示されます。



- **メソッド**：Webhook の送信方式です。 POST 方式のみサポートします。
- **URL**：Webhookを受信するURLを入力します。 http:// または https:// で始まる有効なアドレスである必要があります。
- **ヘッダー**：Webhook に含めるHTTPヘッダーを設定します。 **+ 追加** ボタンをクリックしてヘッダーを追加できます。各ヘッダーはキーと値のペアで入力します。

- **ボディ**：Webhook に含めるHTTPボディを設定します。 **+ 追加** ボタンをクリックしてボディ項目を追加できます。各ボディ項目はキーと値のペアで入力します。
- **スケジュール**：ルールが実行され、webhook を送信するスケジュールを選択してください。

webhook 動作の設定を保存するには、**適用** ボタンをクリックします。

> **情報**
>
> - Webhook 送信履歴と応答コードは、障害解析のためシステムログで確認できます。
> - スケジュールは **AI&ルール** → **スケジュール** で作成、修正、削除できます。スケジュール管理の詳細は、スケジュール管理をご参照ください。

7 リレー動作の設定

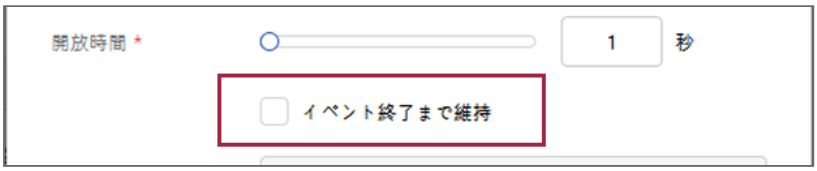
リレー動作は、AIイベント発生時に該当デバイスまたはサブデバイスのリレーを動作させる機能です。例えば、ブラックリストユーザーのイベント発生時にドアのリレーを動作させ、入退室を制限できます。

アクション セクションで **リレー** トグルボタンをクリックして動作を有効にし、 ボタンをクリックします。リレー設定ポップアップが表示されます。



- **ポート**: 動作させるリレーポートを選択してください。デバイス本体のリレーポートと、デバイスに接続された下位デバイスのリレーポートを選択できます。他のルールやドアですでに使用中のポートは、一覧に使用中と表示され、選択できません。
- **開放時間**: リレーを開放状態に保つ時間を設定します。スライダーを動かすか、入力フィールドに値を直接入力できます。 1 秒から 120 秒まで設定できます。

  - **イベント終了まで維持**: 条件の **種類**で **人数カウント**を選択し、**カウント制限**で設定したエリアを条件として指定すると、**イベント終了まで維持** オプションを使用できます。このオプションを選択すると、開放時間に関係なく、カウント制限イベントが解除されるまでリレーが開放状態を維持します。



- **接点タイプ**: リレーの接点タイプを選択してください。リレーポートを選択して設定します。デフォルトは **Normal Close** です。
  - **Normal Open**: 通常は開いており、リレーが動作すると閉じる接点です。
  - **Normal Close**: 通常は閉じており、リレーが動作すると開く接点です。
- **スケジュール**: ルールが実行され、リレーを動作させるスケジュールを選択します。

リレー動作の設定を保存するには、**適用** ボタンをクリックします。

> **注意**
> **接点タイプ**はルールではなく、リレーポートに適用する設定です。 **接点タイプ** を変更すると、そのポートを使用するすべてのルールとドアに直ちに適用されます。ポートが固定施錠または固定解錠の状態で **接点タイプ** を変更すると、出力が反転し、施錠中のドアが開く場合があります。注意してください。

> **情報**
> - この機能のサポートは、ファームウェアバージョン1.1.0以降に含まれます。
> - スケジュールは **AI&ルール** → **スケジュール** で作成、修正、削除できます。スケジュール管理の詳細は、スケジュール管理をご参照ください。

8 ルールを保存

ルール設定をすべて完了してルールを保存するには、画面右上の **保存** ボタンをクリックします。保存したルールはルール一覧で確認できます。ルール一覧では、ルール名、タイプ、イベント、スケジュールを確認できます。



AIルールの有効化/無効化

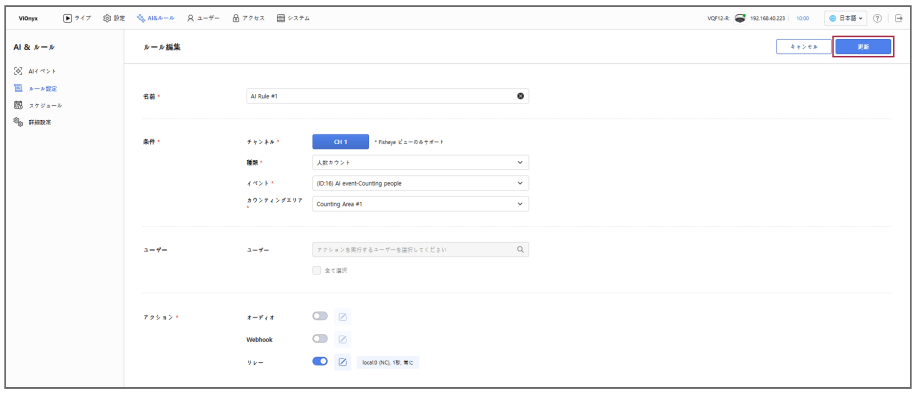
ルール一覧で各ルール項目の最左のトグルボタンをクリックすると、そのルールを有効または無効にできます。有効なルールはAIイベント発生時に設定された動作を実行します。無効なルールはAIイベント発生時でも動作が実行されません。



> **情報**
> ルール一覧で有効/無効の状態をひと目で区別できます。青色のトグルで表示されるルールは有効、灰色のトグルで表示されるルールは無効です。

AIルールの編集

ルール一覧で各ルール項目をクリックすると、ルールの詳細を確認または編集できます。ルール詳細画面で条件と動作を編集した後、変更を保存するには **更新** ボタンをクリックします。



AIルールの削除

ルール一覧で各ルール項目の最右の ボタンをクリックすると、該当ルールを削除できます。削除したルールは復元できません。



スケジュール管理

スケジュールは、曜日と時間帯を組み合わせた週間タイムテーブルです。スケジュールを作成してAIルールの動作に割り当てると、その動作はスケジュールに含まれる時間帯のみ実行されます。作成したスケジュールは複数のAIルールで共有できます。

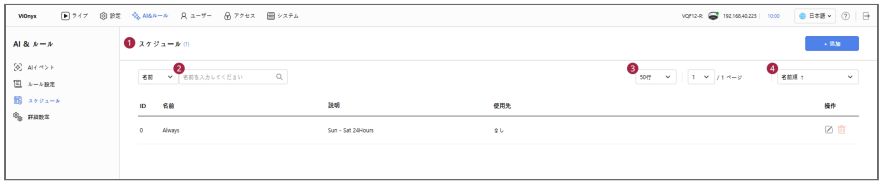
次のような場合にスケジュールを作成してください。

- 平日の業務時間内のみWebhookを送信する場合
- 夜間のみ侵入検知の警告音声を再生する場合
- 週末にリレーが動作しないよう制限する場合

> **情報**
> デバイスには **Always** スケジュールが標準で用意されています。 Alwaysスケジュールは毎日24時間動作し、編集や削除はできません。

スケジュールリストの確認

1. 画面左上の **AI&ルール** メニューをクリックします。
2. 画面左側のサイドバーで **スケジュール** をクリックします。



スケジュールリストで、登録済みスケジュールと各スケジュールを使用するAIルールを確認できます。

- 画面上部の **スケジュール**(1) の横に、登録済みスケジュール数が表示されます。
- 特定のスケジュールを探すには、検索フィールド(2)にスケジュール名またはIDを入力してください。
- 各ページに表示するスケジュール数を変更するには、画面右上の行数リスト(3)で希望の値を選択してください。
- 並べ替え基準を変更するには、**名前順**(4)のリストから希望の基準を選択してください。

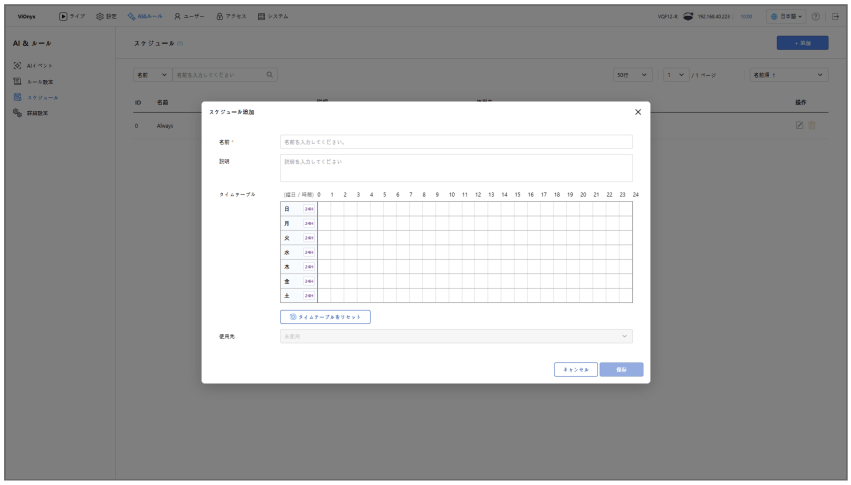
スケジュールリストに表示される項目は次のとおりです。

項目	説明
ID	スケジュールの固有番号です。 Alwaysスケジュールは `0` です。
名前	スケジュール名です。
説明	スケジュールを追加または編集するときに入力した説明です。
使用先	スケジュールを使用するAIルールです。使用中のAIルールがない場合、**なし**と表示されます。 AIルールが複数ある場合、**ほか{count}件** の形式で表示されます。
操作	スケジュールを編集（）または削除（）できます。

スケジュールの追加

1 スケジュールの追加を開始

1. スケジュール一覧画面の右上にある **+ 追加** ボタンをクリックします。
2. **スケジュール追加** ポップアップが開いたら、スケジュール情報を入力します。

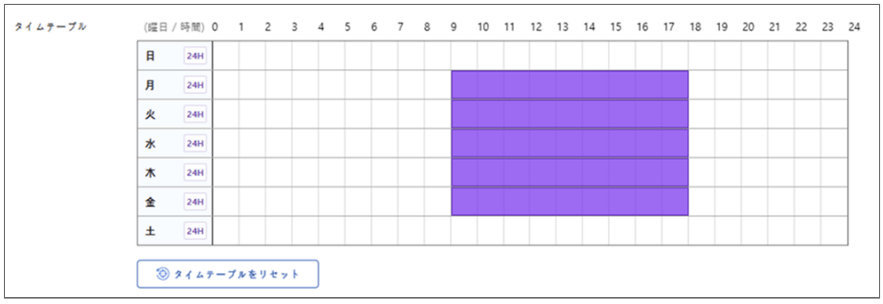


2 名前と説明を入力

- **名前**：スケジュール名を入力します。必須項目で、ほかのスケジュールと同じ名前は使用できません。最大48文字まで入力できます。
- **説明**：スケジュールの説明を入力します。例えば **月-金 09:00-18:00** のように適用時間帯を記載しておくと、ルールでスケジュールを選択するときに区別しやすくなります。

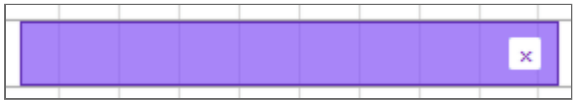
3 タイムテーブルで時間帯を指定

タイムテーブル で、スケジュールが動作する曜日と時間帯を選択します。縦軸は曜日（日曜日~土曜日）、横軸は時間（0時~24時）です。選択した時間帯はブロックで表示されます。



- **時間帯の選択**：目的の曜日行で、開始時刻から終了時刻までマウスでドラッグします。最小10分単位で選択できます。
- **時間帯の移動**：指定したブロックを左右にドラッグすると、別の時間帯に移動できます。
- **24時間の選択/解除**：曜日名の横にある **24H** ボタンをクリックします。その曜日の24時間すべてが選択され、もう一度クリックすると全解除されます。

- **ブロックの削除**：削除するブロックを選択すると、✕ ボタンが表示されます。このボタンをクリックします。



- **全体を初期化**：指定した時間帯をすべて消去して再設定する場合は、**タイムテーブルをリセット** ボタンをクリックします。

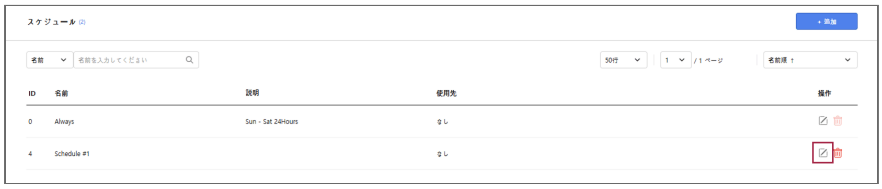
4 スケジュールを保存

すべての設定が完了したら、**保存** ボタンをクリックしてください。保存したスケジュールはスケジュール一覧に追加され、AIルールの動作設定で選択できます。

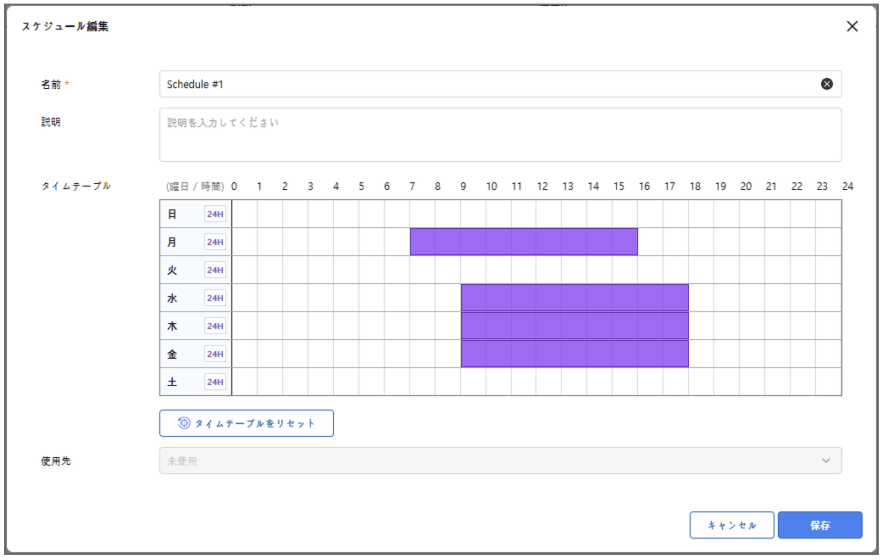
> **情報**
>
> - **使用先** は、スケジュールを使用するAIルールを表示する読み取り専用フィールドです。新しく作成したスケジュールは、まだ使用中のAIルールがないため、**未使用**と表示されます。
> - 保存したスケジュールをAIルールに適用する方法はAIルールの設定を参照してください。

スケジュールの編集

1. スケジュール一覧で編集するスケジュールの右側にある✎ボタンをクリックしてください。



2. **スケジュール編集** ポップアップが表示されたら、名前、説明、タイムテーブルを編集してください。



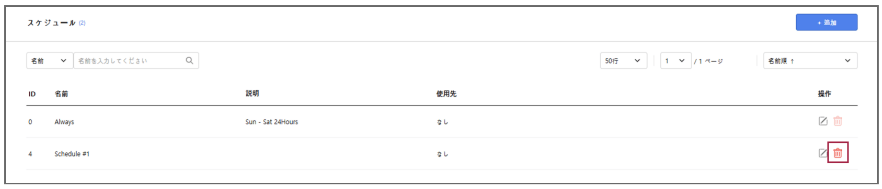
3. 編集内容を保存するには、**保存** ボタンをクリックしてください。

編集したスケジュールは、保存するとすぐに、そのスケジュールを使用するすべてのAIルールに適用されます。

> **情報**
>
> - スケジュールを複数のAIルールで共有する場合、編集前に**使用先**列で影響を受けるAIルールを確認してください。
> - Always スケジュールは基本スケジュールに変更できません。

スケジュールの削除

1. スケジュール一覧で削除するスケジュールの右側にある ボタンをクリックしてください。



2. 確認メッセージが表示されたら内容を確認し、**確認** ボタンをクリックしてください。

削除したスケジュールは復元できません。

> **情報**
>
> - AIルールで使用中のスケジュールは削除できません。**使用先**列に表示されたAIルールで別のスケジュールを選択してから、もう一度削除してください。
> - Always スケジュールは基本スケジュールのため削除できません。

高度設定

高度な設定では、顔の撮影タイプを設定し、顔認証時のユーザーの自動登録と、登録済みユーザーの保存ポリシーを管理できます。

顔の撮影タイプ設定

顔の撮影タイプを上半身のみ撮影するか、全身まで撮影するか設定できます。

1. 画面左上の **AI&ルール** メニューをクリックします。
2. 画面左側のサイドバーで **詳細設定** をクリックします。
3. **撮影タイプ**オプションで希望の撮影タイプを選択し、**保存**ボタンをクリックしてください。



自動登録ユーザ設定

AIイベントで検知した顔をユーザーとして自動登録できます。既定では手動登録モードに設定されており、必要に応じて自動登録モードに切り替えられます。

> **情報**
>
> 自動登録したユーザーも、ユーザー名や説明などの情報を手動で編集できます。ユーザー情報の編集の詳細については ユーザーの編集と削除 をご覧ください。

自動登録モードを有効にする

1. 画面左上の **AI&ルール** メニューをクリックします。
2. 画面左側のサイドバーで **詳細設定** をクリックします。
3. **自動ユーザー登録** セクションでトグルボタンをクリックして自動登録モードを有効にしてください。



次の手順に従って各オプションを設定し、**保存**ボタンをクリックして保存してください。

> **情報**
>
> **自動ユーザー登録**モードを使用すると、低品質の写真（ぼけ、マスク、横顔など）で登録されたユーザーで誤認証が発生する場合があります。

自動登録ユーザー数設定

自動登録ユーザー数オプションで、自動登録できるユーザー数を設定できます。スライダーをドラッグするか、入力欄に数値を直接入力してください。

- 既定値は50,000人で、最大100,000人まで設定できます。
- 自動登録ユーザー数を設定すると、手動登録ユーザーも設定した人数内でのみ登録できます。たとえば、設定ユーザー数が50,000人の場合、自動登録ユーザー数と手動登録ユーザー数を合計して最大50,000人まで登録できます。

> **情報**
>
> - 手動で登録されたユーザーがいる場合、自動登録ユーザー数は増やせません。
> - 自動登録ユーザー数を減らすと、超過分のユーザーは古い順に自動削除されます。

保存処理方法設定

保持処理方式オプションでは、自動登録されたユーザーの保存処理方法を設定できます。ユーザー数の上限に達したときの、自動登録ユーザーの削除方法を選択してください。

- **最も古いものを削除**: 割り当てられたユーザー数を超えると、最も古く登録されたユーザーから自動削除します。

保存期間設定

保持期間（日）オプションでは、自動登録されたユーザーの保存期間を日単位で設定できます。保存期間が終了すると、最も古く登録されたユーザーから自動削除されます。

- **無効**（既定値）: 割り当てられたユーザー数を超えると、最も古く登録されたユーザーから自動削除します。
- **1日**、**3日**、**7日**、**14日**、**30日**、**90日**、**365日**: 選択した期間が経過すると、自動登録されたユーザーを自動削除します。

> **情報**
> 保存期間を設定すると、ユーザー数の上限に達したときに、期間終了を待たずに古いユーザーから即時削除されます。

自動登録ユーザーの確認と管理

ユーザー メニューで確認

自動登録されたユーザーは、**ユーザー** メニューのユーザー一覧で確認できます。

- ユーザーIDは顔認証の順序に従って順番に自動付与されます。
- **説明**列に**自動登録**として表示され、手動登録ユーザーと区別できます。
- **最終更新**列にユーザーが登録された日時が表示されます。

ユーザー詳細情報の編集

1. 画面左上の **ユーザー** メニューをクリックします。
2. ユーザー一覧で自動登録されたユーザーをクリックしてください。

3. ユーザー詳細ポップアップが表示されたら、必要な情報を編集してください。
4. ユーザー情報の編集が完了したら、**適用** ボタンをクリックしてください。

顔認証ログと顔撮影の表示

1. 画面左上の **ユーザー** メニューをクリックします。
2. ユーザー一覧で自動登録されたユーザーをクリックしてください。
3. ユーザー詳細情報のポップアップが表示されたら、**イベントログ**セクションで顔認証ログを確認できます。

- 日付を選択して、特定期間の顔認証ログを確認できます。
- ログの**顔撮影**をクリックすると、該当認証時点の顔写真が表示されます。

カメラを設定する

カメラを設置したら、設置環境と運用目的に合わせて設定してください。このセクションでは、画質とプライバシー保護、時刻とネットワーク構成、外部デバイスおよびシステム連携に必要な設定方法を説明します。必要な設定項目を以下から選択してください。

ビデオプロファイルの設定

ライブ画面に表示される映像品質と保存される録画映像の品質は、ビデオプロファイルの設定により変わります。ビデオプロファイル設定では、チャネルごとにビュー モードとストリームエンコード値を調整できます。また、設置環境に応じて左右反転（Mirror）設定とチャネル設定の初期化機能も提供します。

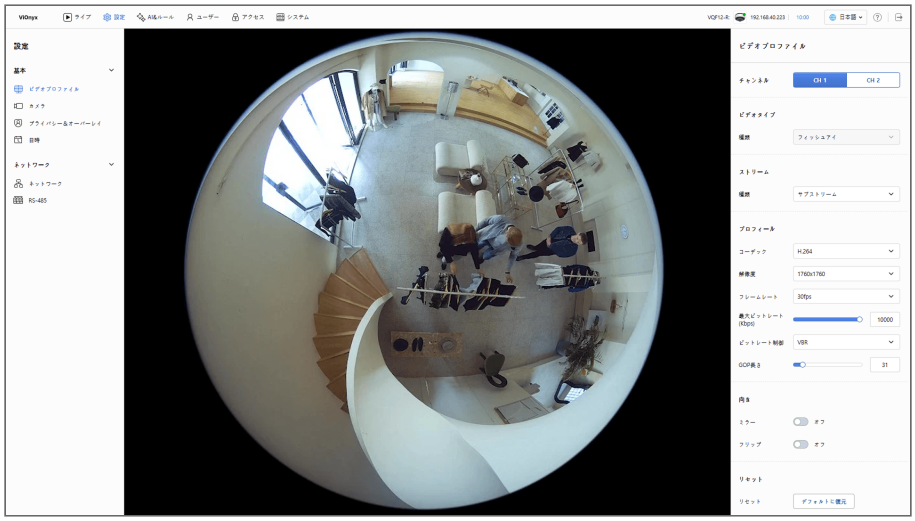
以下の状況ではビデオプロファイルを設定して、映像品質、保存容量、ネットワーク帯域幅の最適なバランスを確保してください。

- 保存容量と画質のバランスを調整したいとき
- ネットワーク帯域に合わせてMain/Subストリームを分離して運用したいとき
- チャネルごとのビュー モードを目的に応じて使用したいとき

> **情報**
> AIイベントを既に運用している場合、左右反転や初期化を行うとAIイベント設定が削除される可能性があります。

ビデオプロファイルの設定

1. 画面左上の **設定** メニューをクリックしてください。
2. 画面左側のサイドバーで **基本** → **ビデオプロファイル** をクリックしてください。



> **情報**
> ビデオプロファイルの設定は、保存ボタンが不要で、変更すると即座にカメラに反映されます。

チャネルの選択とビュータイプの確認

チャネルごとの主な目的は次のとおりです。

- **CH 1**: 物理カメラの元のフィッシュアイ画面を基準に運用するチャンネルです。
- **CH 2**: パノラマや4分割画面などの加工ビューで監視効率を高めて運用するチャンネルです。

カメラのチャネルごとにビデオプロファイルの詳細項目を設定できます。

1. 画面右側の **ビデオプロファイル** パネルの **チャンネル** で **CH 1** または **CH 2** を選択してください。
2. **ビデオタイプ** の **種類** で、選択したチャネルのビュータイプを選べます。

チャネルごとのビュータイプポリシーは以下の通りです。

- **CH 1**: フィッシュアイに固定されており、変更できません。
- **CH 2**: フィッシュアイを除くビュー モードを選択できます。
  - **シングルパノラマ**: フィッシュアイカメラが撮影した映像を補正し、壁面型パノラマ形式で表示するモードです。
  - **ダブルパノラマ**: 360°領域を撮影した映像を歪み補正し、パノラマ形式の上下分割画面で表示するモードです。
  - **クアッドビュー**: 人の視野に適したように歪み補正した4つの特定画面を同時に表示するモードです。

ストリームタイプの選択

ストリーム で設定するストリームを選択してください。メインまたはサブストリームのどちらかを選択し、**プロフィール** セクションで詳細値を調整してください。

- **メインストリーム**: 録画と高画質監視
- **サブストリーム**: 低帯域幅のリモート監視

> **情報**
> **CH 2** チャンネルは **メインストリーム** タイプのみをサポートします。

プロファイル詳細設定

選択したストリームタイプに応じて、コーデック、解像度、フレームレートなどの詳細設定を調整してください。

- **コーデック**：プロファイルに適用するコーデックを選択してください。 **H.264**、**H.265**、**MJPEG** のいずれかを選択できます。

  > H.265コーデックを選択すると、Profile Tが必須で適用されます。

- **解像度**：プロファイルに適用する解像度です。チャンネル、ビデオタイプ、ストリームタイプによって、サポートする解像度が異なります。

チャンネル	ビデオタイプ	ストリームタイプ	サポート解像度
CH 1	**フィッシュアイ**	**メインストリーム**	3520 × 3520
		サブストリーム	1760 × 1760
CH 2	**シングルパノラマ**	**メインストリーム**	2048 × 512、1920 × 480、1280 × 320、704 × 176
	ダブルパノラマ	**メインストリーム**	2048 × 2048、1920 × 1920、1280 × 1280、704 × 704
	クアッドビュー	**メインストリーム**	2048 × 2048、1600 × 1600、1280 × 1280、1024 × 1024

> **CH 2** チャンネルは **メインストリーム** タイプのみをサポートします。

- **フレームレート**：1秒あたりのフレーム数を設定してください。 30、25、20、15、10フレームのいずれかを選択できます。
- **最大ビットレート**: 映像の最大ビットレートを設定できます。
- **ビットレート制御**：映像データの制御方式を選択してください。
  - **VBR**：映像の複雑さに応じてビットレートが可変となるため、ネットワークが安定している場合に高画質を提供します。ネットワーク帯域が十分な環境で推奨します。
  - **CBR**：ビットレートを固定して安定したストリーミングを保証しますが、複雑な画面では画質が低下する場合があります。ネットワーク帯域が制限されている、または一定の環境で推奨します。
- **GOP長さ**：I-Frameの間隔を設定します。 1\~300 の範囲の値を選択できます。 GOVの長さが長いほどデータ量は減少し、短いほど増加します。

> **情報**
>
> - **可変ビットレート**(Variable Bitrate, VBR): フレームのデータサイズを固定せず、最大ビットレート内で映像を送信する方式です。映像の複雑さに応じてビットレートが可変に調整される方式です。一般に高画質を提供しますが、ネットワーク帯域が安定していない環境では映像の途切れが発生する可能性があります。
> - **固定ビットレート**(Constant Bitrate, CBR): フレームのデータサイズを固定して映像を送信する方式です。ネットワーク帯域が一定の環境で安定した映像ストリーミングを提供しますが、映像の複雑さに応じて画質が低下する場合があります。
> - **GOV**(Group of Video): H.264/H.265圧縮で、Iフレームから次のIフレームの直前までのフレーム集合を意味します。GOVには、完全な画像情報を含むI-Frame（キーフレーム）と、前フレームとの差分情報のみを含むP-Frameが含まれます。 GOVの長さが長くなるほどI-Frameの数は減少し映像データ量が減り、短くなるほどI-Frameの数は増加し映像データ量が増えます。

左右反転設定

カメラの設置位置によって、左右または上下反転の設定が必要になる場合があります。

- **ミラー**: 左右反転の設定をオンまたはオフにできます。
- **フリップ**: 上下反転の設定をオンまたはオフにできます。

> **情報**
> AIイベントが設定されている場合、左右反転の変更が制限されることがあります。この場合、案内ポップアップに従いAI設定を削除してから進めてください。

チャネル設定の初期化

設定したチャネルのビュー モードとストリーム設定を工場出荷時の初期値に戻すには、**リセット** セクションで **デフォルトに復元** ボタンをクリックしてください。

> **情報**
> - 選択したチャネルのみ工場出荷時の初期設定に復元されます。
> - フィッシュアイモードでAIイベントが設定されている場合は、AI設定を削除してから進めてください。

カメラ設定の変更

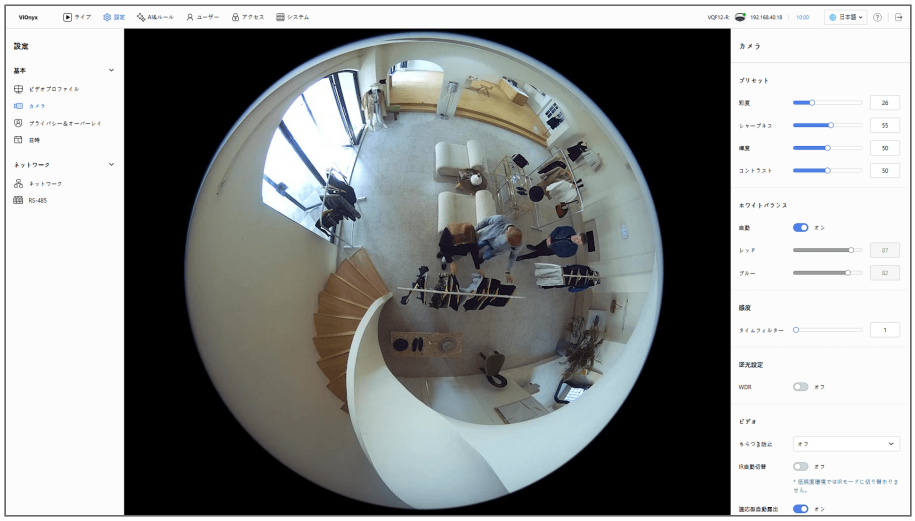
カメラが設置された環境で最適な映像を得られるように、カメラ設定を調整してください。設定を変更するとライブビューにすぐ反映されるため、結果を確認しながら画像品質、ホワイトバランス、感度、逆光補正などを調整できます。また、設置タイプ（天井または壁面）によって使用できるAI機能が異なります。

次のような状況ではカメラ設定を調整してください。

- 撮影環境の明るさや色味に合わせて画像品質を向上させたい場合
- 低照度環境でノイズを最小限にしつつ動作検知を維持したい場合
- 窓や出入口側の強い逆光で被写体が暗く見える場合
- 蛍光灯やLED照明のちらつきを減らしたい場合
- 補助照明がある、またはカラー映像が必要なため、夜間のIR切り替えを無効にする場合
- 外光の影響で顔が暗すぎたり明るすぎたりして、顔認証が難しい場合
- 設置場所に応じてカメラとAI機能を最適化したい場合
- 寒さや湿気でレンズに曇りや霜が付き、映像がぼやける場合

カメラ設定

1. 画面左上の **設定** メニューをクリックしてください。
2. 画面左のサイドバーで **基本** → **カメラ** をクリックしてください。



> **情報**
> カメラ設定の変更は、設定オプションを変更するたびにライブビューにリアルタイムで反映され、変更後は自動で保存されます。

画像品質の調整

撮影環境に合わせて画像品質を調整できます。 **プリセット** セクションの各スライダーを調整すると、プレビュー画面にリアルタイムで反映されます。 1〜100の値で設定できます。

- **彩度**：色の鮮やかさを調整します。（既定値：26）
- **シャープネス**：画像の輪郭の鮮明さを調整します。（既定値：55）
- **輝度**：画像全体の明るさを調整します。（既定値：50）
- **コントラスト**：明るい部分と暗い部分のコントラストを調整します。（既定値：50）

> **情報**
> 各設定はスライダーを操作するたびにプレビュー画面に即時反映され、自動で保存されます。

ホワイトバランス設定

カメラが撮影環境の光色を正しく表現するように、ホワイトバランスを設定してください。 **ホワイトバランス** セクションで **自動** オプションをオン／オフできます。

- **オン**(デフォルト): カメラが色温度を自動で検知して調整します。
- **オフ**: **レッド**と**ブルー**の値を手動で調整して、ホワイトバランスを設定します。

感度設定（タイムフィルタ）

センサーノイズを減らすか、素早い動作検知とのバランスを取るために時間フィルターを調整してください。 **感度** セクションの **タイムフィルター** スライダーを調整すると、ノイズフィルタの強さを設定できます。

- 低（1〜30）：ノイズフィルタが弱くなり、素早く動く物体の検知に有利ですが、低照度環境ではノイズが増える可能性があ

ります。

- 中（31～70）：バランスの取れたフィルタリングで一般的な撮影環境に適しています。
- 高（71～100）：ノイズフィルタが強くなり、低照度環境でノイズを減らすのに有利ですが、素早く動く物体の検知には不利になる場合があります。

> **情報**
> **タイムフィルター**のデフォルト値は1です。

逆光設定

カメラが逆光環境で明るい領域と暗い領域を同時に表現できるよう、WDR（Wide Dynamic Range、逆光補正）を設定してください。 **逆光設定** セクションで **WDR** オプションをオンにすると、逆光補正を有効にできます。（既定値：**オフ**）

> **情報**
> WDR（Wide Dynamic Range）モードは、逆光環境で明るい領域と暗い領域を同時に表現できるように、カメラが自動で露出を調整する機能です。 WDRモードを有効にすると、明るい領域の露出オーバーを防ぎ、暗い領域のディテールをよりよく表現できます。一般的に逆光が強い環境での撮影に有用です。

ちらつき防止設定

撮影環境の照明と周波数の不一致による画面のちらつきを抑えるには、**ビデオ** セクションで **ちらつき防止** オプションを設定してください。

- **オフ**（デフォルト）：ちらつき防止機能を使用しない
- **50HZ**: 50Hzの蛍光灯/LED環境
- **60HZ**: 60Hzの蛍光灯/LED環境

> **情報**
> 撮影環境の照明周波数に一致するオプションを選択してください。誤った設定の場合、画面にちらつきや縞模様が発生することがあります。

IR自動切り替えの設定

周囲が暗くなったときにカメラをIR（夜間）モードへ自動で切り替えるか設定してください。補助照明がある場所やカラー映像が必須の現場では、自動切り替えをオフにできます。 **ビデオ** セクションで **IR自動切替** オプションをオン／オフします。

- **オン**(デフォルト): 照度センサーと映像の明るさを基準に、周囲が暗くなるとIRモードへ自動で切り替えます。
- **オフ**: 低照度環境でもIRモードに切り替えません。

> **情報**
> **IR自動切替** オプションはファームウェア バージョン 1.1.0 以上で利用できます。

適応型自動露出の設定

窓際のように外光が強い場所や、日光が一日の中で大きく変化する場所では、顔が暗すぎたり明るすぎたりして、顔認証が難しい場合があります。この場合は適応型自動露出を使用してください。カメラが顔の出現頻度が高い位置を自動的に学習し、その位置の顔が適切な明るさで見えるように露出を自動調整します。 **ビデオ** セクションで **適応型自動露出** オプションをオン／オフします。

- **オン**(デフォルト)：顔領域の明るさを基準に露出を自動調整します。
  - 外光が強い場合や日光が変化する場合でも、顔領域の明るさを一定に維持します。
  - 人が通り過ぎたり長時間とどまったりしても、衣服の色の影響で画面の明るさが変動しません。
  - 照明をオン／オフすると、変化後の明るさに合わせて露出を再調整します。
- **オフ**：適応型自動露出補正を使用しません。再度オンにすると、補正がに再開します。

> **情報**
>
> - **適応型自動露出** は、AIイベントの顔領域と人物検出範囲を基準に動作します。領域の設定方法については、AIイベントの管理をご参照ください。
> - **適応型自動露出** オプションはファームウェアバージョン 1.1.0 以上で利用できます。

設置タイプ設定

カメラの設置場所に応じて、**設置タイプ** を設定してください。設置タイプによりサポートされるAI機能が決まります。

- **天井**（デフォルト）: 天井に設置した場合に選択してください。すべてのAI機能を使用できます。
- **壁面**: 壁面に設置した場合に選択してください。顔認証AIのみ使用でき、オブジェクト追跡は利用できません。

> **情報**
>
> - **天井から壁面へ変更する場合**、顔認証のみ可能でオブジェクト追跡AIは使用できない旨の確認ポップアップが表示されるため、内容を確認してから進めてください。
> - **壁面から天井へ変更する場合**、即座に変更され、すべてのAI機能が自動で有効になります。

カメラヒーターの設定

気温が低い、または湿度が高い環境では、レンズに曇りや霜が付き、映像がぼやけてAI認識精度が低下することがあります。この場合はカメラヒーターをオンにして、レンズの視界を確保してください。 **ヒーター** セクションで **ヒーター** オプションをオン／オフします。

- **オン**: ヒーターが動作します。 30分後に自動でオフになります。
- **オフ**（デフォルト）: ヒーターの動作を停止します。

情報

- ヒーターは過熱と不要な電力消費を防ぐため、30分間だけ動作した後に自動で停止し、オプションも**オフ**に切り替わります。ヒーターが停止した後もレンズに曇りや霜が残る場合は、オプションをもう一度オンにしてください。
- **ヒーター** オプションはファームウェアバージョン 1.1.0 以上でサポートします。

カメラ設定の初期化

すべてのカメラ設定を工場出荷時の初期値に戻すには、**リセット** セクションで **デフォルトに復元** ボタンをクリックしてください。

プライバシーとオーバーレイの設定

プライバシー＆オーバーレイ 設定を使用するとカメラ映像の機密領域を隠すか、顔を自動でぼかすことができます。また、映像に日付/時刻とカメラ名を表示して、映像の出所と撮影時刻を明確にできます。すべての設定は即座にライブビューに反映されます。

以下のような状況でプライバシーとオーバーレイを設定します。

- プライバシー侵害が懸念される特定の領域をマスクする場合
- 顔の自動ぼかしで個人情報保護方針に準拠する場合
- 録画映像に日付/時刻を表示して映像の追跡性を確保する場合
- 複数カメラを運用する際にカメラ名を表示して映像の出所を明確にする場合

情報

プライバシー設定（マスキング、顔のぼかし）は映像の表示にのみ適用され、AI解析は原画像を基に実行されるためAIの性能には影響しません。

プライバシーとオーバーレイの設定

1. 画面左上の **設定** メニューをクリックしてください。
2. 画面左のサイドバーで **基本** → **プライバシー＆オーバーレイ** をクリックします。



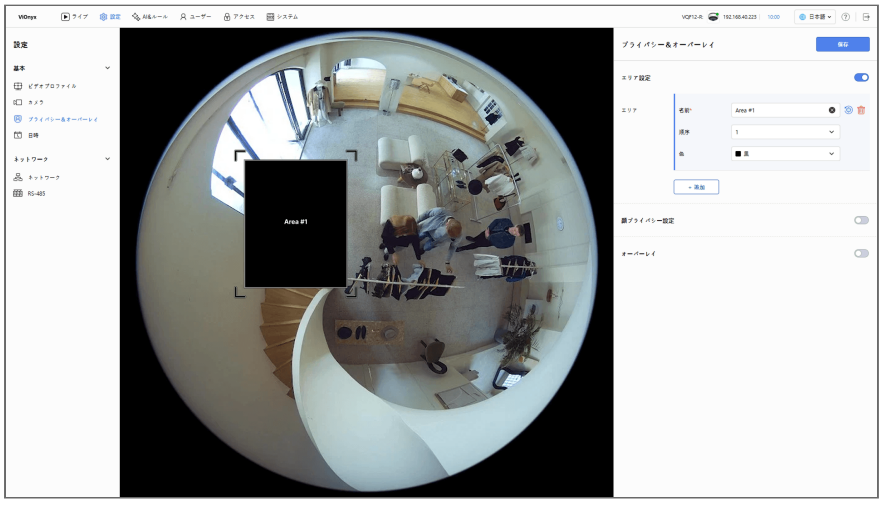
3. 変更内容を保存するには、画面右上の **保存** ボタンをクリックします。

変更は保存後すぐにカメラに反映されます。

プライバシー領域の設定

撮影映像内の非公開領域をマスクできます。最大10領域まで設定でき、各領域は移動せず固定されます。

1. **エリア設定** セクションのトグルボタンをクリックします。
2. **+ 追加** ボタンをクリックします。
3. ライブビューにマスキングする領域が追加されます。領域の角をドラッグしてサイズを調整するか、領域全体をドラッグして位置を移動できます。



4. マスキング領域を作成すると、右側の設定パネルで領域名、順序、色を設定できます。
   - **名前**: マスキング領域名は自動生成され、必要に応じて修正できます。
   - **順序**: マスキング領域が重なる場合に表示順序を調整できます。数字が大きいほど上に表示されます。
   - **色**: マスキング領域の色を選択できます。
5. 追加したマスキング領域を保存するには、画面右上の **保存** ボタンをクリックします。

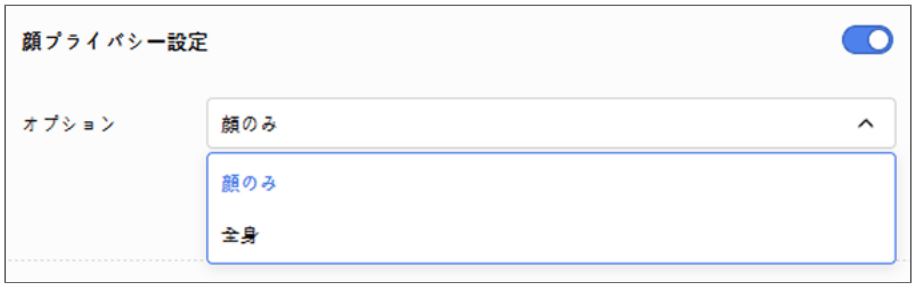
保存したマスキング領域はライブビューと録画映像に反映されます。

情報

- マスキングした領域は、すべての表示モード（フィッシュアイ、シングルパノラマ、ダブルパノラマ、クアッド）に自動適用されます。
- マスク領域の設定を初期化するには、ボタンをクリックします。
- マスク領域を削除するには、ボタンをクリックします。

顔のプライバシー設定

カメラが検出した顔または全身を自動でぼかして個人情報を保護できます。**顔プライバシー設定** オプションを有効にし、ぼかし範囲を選択します。



- **顔のみ**: 検出したすべての顔を自動でぼかします。
- **全身**: 検出した全身を自動でぼかします。

情報

顔または全身がぼかされてもAIの性能には影響しません。カメラがぼかした映像を表示している間も、AI解析は原画像を基に実行されるため、顔認識やオブジェクト追跡などのAI機能は正常に動作します。

オーバーレイ設定

ライブビューに日付/時刻とカメラ名を表示できます。**オーバーレイ** オプションを有効にし、**日付と時刻**、**カメラ名**で詳細設定を調整します。





> **情報**
> 各設定は変更直後に自動保存され、ライブビューにただちに反映されます。

日付と時刻

ライブビューに表示される日付と時刻の形式、サイズ、色を設定できます。ライブビューで日付/時刻の位置を確認し、必要に応じてマウスでドラッグして位置やサイズを調整します。

- **日付** / **時間**：トグルボタンをクリックして日付および時刻のオーバーレイをオンまたはオフにできます。
- **日付形式**：日付形式を選択します。
  - YYYY-MM-DD (既定, 例: 2026-01-12)
  - MM-DD-YYYY (例: 01-12-2026)
  - DD-MM-YYYY (例: 12-01-2026)
- **時刻形式**：時間形式を選択します。
  - HH:MM:SS (既定, 예: 13:45:56)
  - HH:MM (秒を省略, 例: 13:45)
- **フォントサイズ**：ライブビューに表示される文字サイズを選択します。 1〜20から選択してください。
- **色**：ライブビューに表示される文字色を選択します。

> **情報**
> 日付および時刻のオーバーレイはFisheye Viewにのみ表示されます。

カメラ名

ライブビューにカメラ名を表示して映像の出所を明確にできます。ライブビューでカメラ名の位置を確認し、必要に応じてマウスでドラッグして位置やサイズを調整します。

- **表示**：トグルボタンをクリックしてカメラ名オーバーレイをオンまたはオフにできます。
- **名前**：カメラ名を入力します。
- **フォントサイズ**：ライブビューに表示される文字サイズを選択します。 1〜20から選択してください。
- **色**：ライブビューに表示される文字色を選択します。

設定を保存

設定内容はライブビューで即時確認でき、保存するには画面右上の **保存** ボタンをクリックします。保存された設定はカメラに適用され、ライブビューと録画映像に反映されます。

日付と時刻の設定

日付と時刻の設定により、カメラの時刻を正確に保てます。タイムゾーンを選択し、時刻を手動で設定するか、NTPサーバーで自動的に同期します。正確な時刻は映像のタイムスタンプおよびAIイベント記録の信頼性を保証します。

以下のような場合は日付と時刻の設定を確認してください。

- カメラ設置後に運用地域に合わせてタイムゾーンを設定する場合
- 時刻を手動で正確に入力してカメラの時刻を同期する場合
- NTPサーバーで長期間にわたり正確な時刻を自動で維持する場合
- 複数のカメラの時刻を統一して映像解析や追跡を容易にする場合

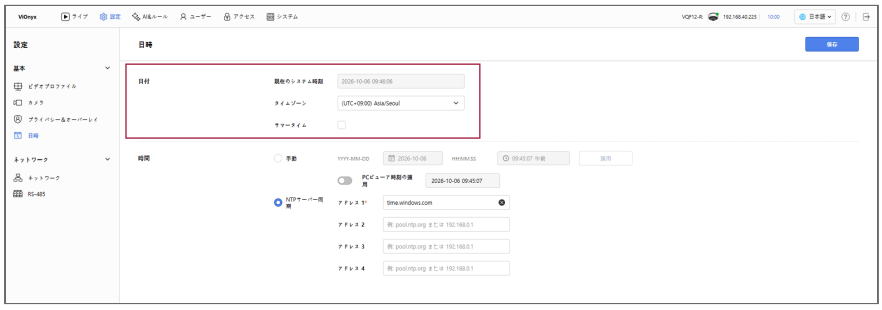
> **情報**
> カメラの時刻が不正確だと、AIイベント記録、ビデオタイムスタンプ、システムログの信頼性が低下します。定期的に時刻設定を確認してください。

タイムゾーンの設定

まずカメラの運用地域のタイムゾーンを設定してください。

1. 画面左上の **設定** メニューをクリックしてください。
2. 画面左側のサイドバーで **基本** → **日時** をクリックしてください。
3. **日付** セクションの **タイムゾーン** で地域を選択してください。

   > *例：* `(UTC+09:00) Asia/Seoul`



4. タイムゾーンに応じてサマータイムを適用するには、**サマータイム** オプションのチェックボックスをクリックしてください。
5. 設定したタイムゾーンを保存するには、画面右上の **保存** ボタンをクリックしてください。

> **情報**
> デフォルト値は `(UTC+09:00) Asia/Seoul` に設定されています。運用地域が異なる場合は必ずタイムゾーンを変更してください。

手動で時刻を設定

カメラの時刻を手動で設定できます。

1. 画面左上の **設定** メニューをクリックしてください。
2. 画面左側のサイドバーで **基本** → **日時** をクリックしてください。
3. **時間** セクションで **手動** を選択してください。



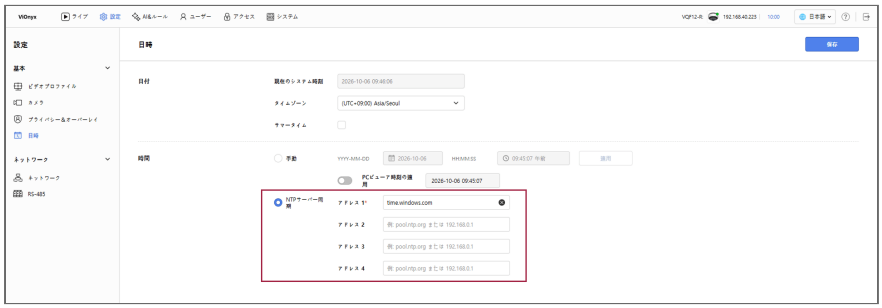
4. 日付フィールドに現在の日付を入力するか、カレンダーアイコンをクリックして日付を選択してください。
5. 時刻フィールドに現在の時刻を入力するか、時計アイコンをクリックして時刻を選択してください。
6. 手動で設定した時刻を適用するには、**適用** ボタンをクリックしてください。
7. 時刻設定を保存するには、画面右上の **保存** ボタンをクリックしてください。

> **情報**
>
> - PCの時刻をカメラに自動適用するには、**PCビューア時刻の適用** オプションを有効にしてください。 Webブラウザーのシステム時刻がカメラに適用されます。
> - 手動モードとNTP自動同期は同時に有効にできません。手動モードを選択するとNTP自動同期は無効になります。

自動同期（NTP）設定

NTPサーバーを通じてカメラの時刻を自動的に正確に維持します。長期間の運用時に推奨されます。

1. 画面左上の **設定** メニューをクリックしてください。
2. 画面左側のサイドバーで **基本** → **日時** をクリックしてください。
3. **時間** セクションで **NTPサーバー同期** を選択してください。



4. **アドレス {n}**(必須) フィールドにNTPサーバーアドレスを入力します。
   - URL形式: time.windows.com、time.nist.gov など
   - IPアドレス: 192.0.2.1 など
5. (オプション) 必要に応じて、**アドレス {n}**、**アドレス {n}**、**アドレス {n}** に追加のNTPサーバーを入力します。

- 最大4つのサーバーを設定できます。
- **アドレス {n}**が応答しない場合、次のサーバーに自動的に切り替わります。

6. 時刻設定を保存するには、画面右上の **保存** ボタンをクリックしてください。

設定完了後、カメラは自動的にNTPサーバーと同期し、定期的に時刻を更新します。

> **情報**
> **推奨NTPサーバー**
> - time.windows.com（Windows 公開NTP）
> - time.nist.gov（NIST 公開NTP）
> - pool.ntp.org（NTP Pool プロジェクト）

ネットワークを設定

ネットワーク設定では、デバイスのIPv4アドレス、サブネット、ゲートウェイ、DNSサーバーを構成し、Web UIとライブ映像ストリーミングで使用するポートを設定します。ネットワーク環境に応じて、自動割り当て（DHCP）または手動設定（Static）のいずれかを選択して構成できます。

また、NVR/VMSがONVIFでデバイスに接続する際に使用するプロファイルを設定し、ユーザー情報を同期するために外部のSuprema CLUeクラウドサービスへ接続できます。 Cloudflare Tunnelを使用すると、外部からデバイスのWeb UIにアクセスできます。

以下の状況ではネットワーク設定を確認してください。

- DHCP対応のネットワークでIPアドレスを自動取得して構成する場合
- 特定のIPアドレスに固定して安定したネットワークアクセスが必要な場合
- デフォルトのポートが他の機器と競合するか、セキュリティ上の理由でポートを変更する場合
- Profile Tに対応しない旧型のNVR/VMSとONVIFで接続する必要がある場合
- Suprema CLUeクラウドサービスとユーザー情報を同期する必要がある場合
- ポートフォワーディングやグローバルIPアドレスなしで、外部からデバイスのWeb UIにアクセスする必要がある場合

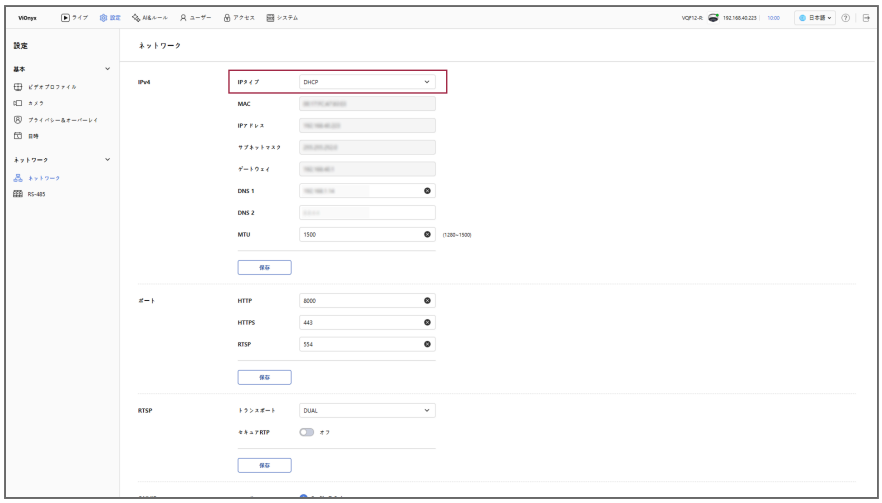
> **情報**
> ネットワーク設定の変更、特にIPアドレスの変更により既存の接続が切断されることがあります。変更後のIPアドレスで再接続してください。

IPアドレス自動設定

DHCPはネットワーク上でIPアドレスを自動割り当てする方式です。ほとんどの一般的なネットワーク環境では、設定なしで自動的に構成されます。

1. 画面左上の **設定** メニューをクリックしてください。
2. 画面左のサイドバーで **ネットワーク** → **ネットワーク** をクリックします。

3. **IPタイプ**で**DHCP**を選択します。



4. DNS サーバーアドレスが必要な場合は、**DNS {n}**および**DNS {n}**入力フィールドに入力します。

5. **MTU**入力フィールドで、MTU（Maximum Transmission Unit）の値を必要に応じて調整します。

   - デフォルトは1500です。
   - 1280〜1500の範囲で設定できます。

6. ネットワーク設定を保存するには、**保存**ボタンをクリックします。

設定が正常に保存されると、自動割り当てされたIPアドレスが**IPアドレス**、**サブネットマスク**、**ゲートウェイ**入力フィールドに表示されます。

> **情報**
> DHCPモードがデフォルトに設定されており、ほとんどの標準的なネットワーク環境では追加設定なしで自動的に動作します。

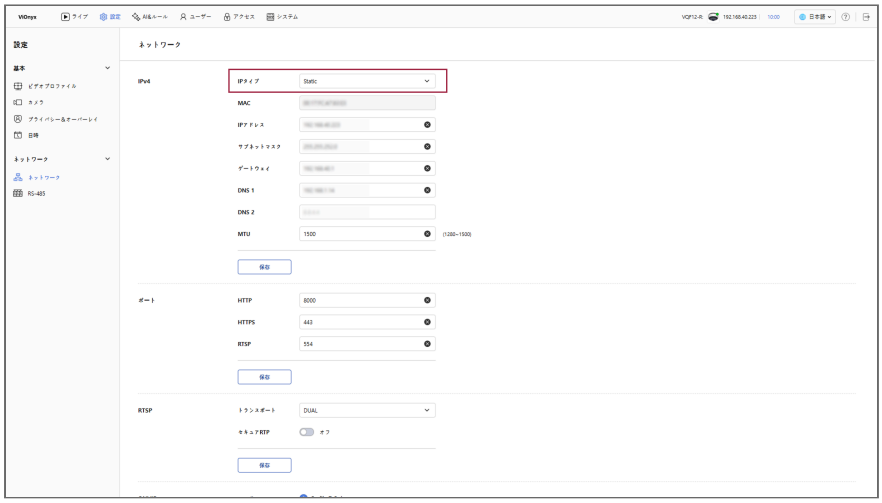
固定IPアドレス設定

ネットワーク環境によっては、特定のIPアドレスに固定して安定したネットワークアクセスが必要なため、手動でIPアドレスを設定できます。

1. 画面左上の **設定** メニューをクリックしてください。

2. 画面左のサイドバーで **ネットワーク** → **ネットワーク** をクリックします。

3. **IPタイプ**で**Static**を選択します。



4. **IPアドレス**入力フィールドに、割り当てられたIPv4アドレスを入力します。

   > *例：192.168.111.11*

5. **サブネットマスク**入力フィールドにサブネットマスクを入力します。

   > *例：255.255.255.0*

6. **ゲートウェイ**入力フィールドにゲートウェイアドレスを入力します。

7. **DNS {n}**および**DNS {n}**入力フィールドに DNS サーバーアドレスを入力します。

8. **MTU**入力フィールドの値を必要に応じて調整します。

   - デフォルトは1500です。
   - 1280〜1500の範囲で設定できます。

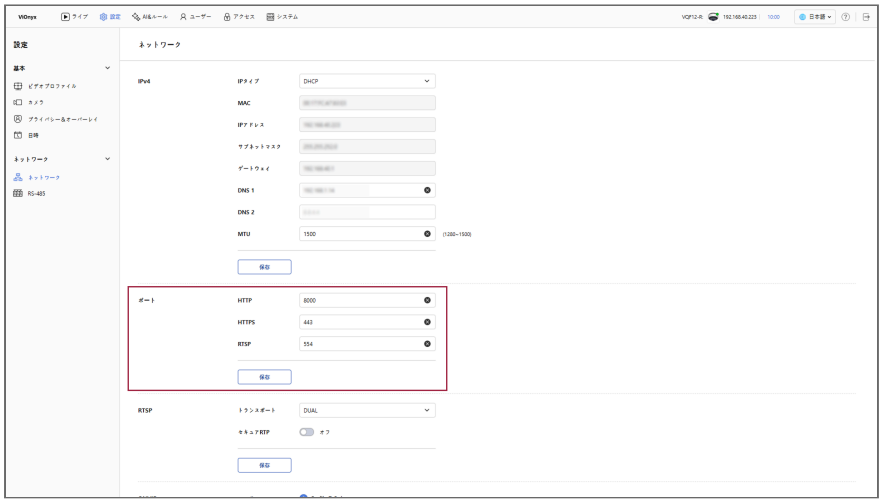
9. ネットワーク設定を保存するには、**保存**ボタンをクリックします。

> 各入力フィールドに正しい形式のアドレスを入力しないと、入力フィールドの周囲に赤い枠が表示され、**保存**ボタンが無効になります。すべての入力フィールドを正しく入力してから、もう一度お試しください。

ポート設定

ポート セクションでは、Web UI接続（HTTP、HTTPS）および映像ストリーミング（RTSP）で使用するポート番号を設定できます。

1. 画面左上の **設定** メニューをクリックしてください。
2. 画面左のサイドバーで **ネットワーク** → **ネットワーク** をクリックします。
3. **ポート** セクションで必要なポートを設定します。



- **HTTP**: Web UIに暗号化せずに接続するポート（既定値: 8000）
- **HTTPS**: Web UIに暗号化して接続するポート（既定値: 443）
- **RTSP**: RTSPプロトコルで映像をストリーミングするポート（既定値: 554）

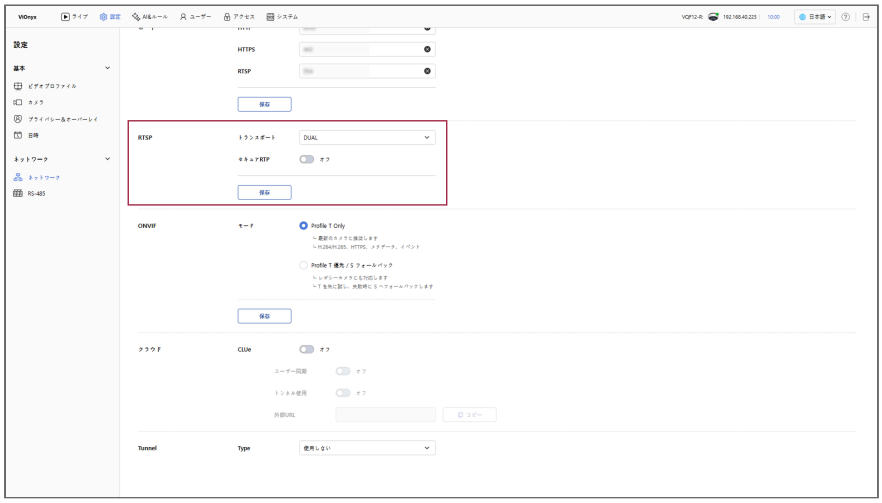
4. ポート設定を保存するには、**保存**ボタンをクリックします。

> **情報**
>
> - 各ポート入力フィールドに 1~65535 の範囲の番号を入力できます。
> - 同じポート番号を複数設定することはできません。各ポートは固有の番号でなければなりません。
> - ポート設定がデフォルトと異なる場合は、Web UIの接続アドレスにポート番号を明記する必要があります。
>
> *例: HTTPSポートが4000の場合:* `https://{ip_address}:4000`

映像転送と暗号化の設定

RTSPセクションでは、映像転送と暗号化の設定を構成できます。

1. 画面左上の **設定** メニューをクリックしてください。
2. 画面左のサイドバーで **ネットワーク** → **ネットワーク** をクリックします。
3. **RTSP**セクションで次のオプションを設定します。



- **トランスポート**: 映像ストリーミングに使用する転送プロトコルを選択します。
  - **UDP**: 高速転送が可能ですが、ネットワーク状態によっては映像の途切れやフレーム損失が発生することがあります。
  - **TCP**: 安定した転送が可能ですが、ネットワーク状態によっては**UDP**より遅延が発生することがあります。
  - **DUAL**: ネットワーク状態に応じてUDPとTCPを自動的に選択してストリーミングします。通常の環境で推奨される既定値です。
  - **TLS**: RTSPストリームをTLS暗号化で送信します。セキュリティを強化しますが、CPU負荷が増加する場合があります。接続先のNVR/VMSがTLSをサポートしているか確認してください。
- **セキュアRTP**: RTSPストリーム暗号化オプションを有効にします。

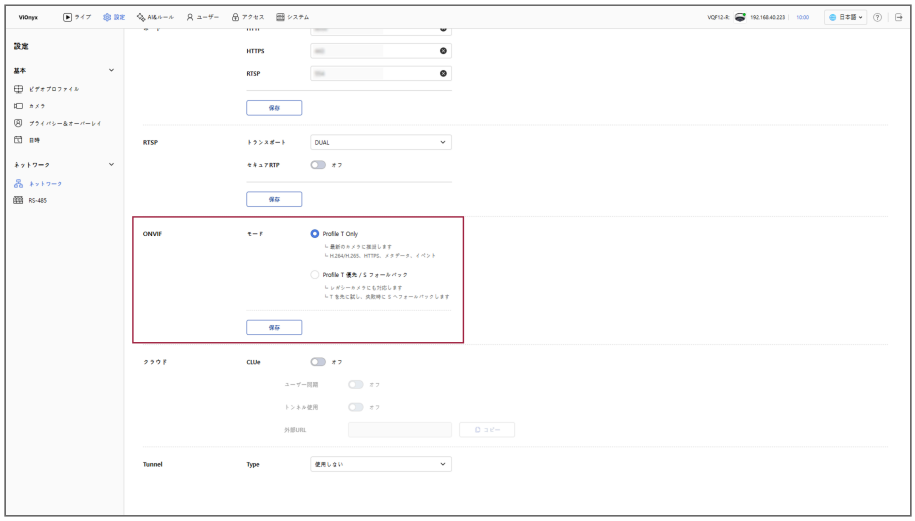
4. 設定を保存するには、**保存**ボタンをクリックします。

> **情報**
> 映像および音声データの暗号化が必要な場合は、**セキュアRTP**オプションを有効にし、接続先のNVR/VMSと互換性があるか確認してください。

> **注意**
> **セキュアRTP**オプションを変更した後は、既存のRTSPセッションを再接続する必要がある場合があります。 NVR/VMSでも、選択した転送方式と互換になるように設定してください。

ONVIFの設定

ONVIFセクションでは、NVR/VMSがONVIFでデバイスに接続する際に使用するプロファイルを設定します。既定ではProfile Tのみを使用します。Profile Tに対応しない旧型のNVR/VMSと接続する場合は、Profile Sのフォールバックを追加で有効にします。



次の2つのモードのいずれかを選択します。

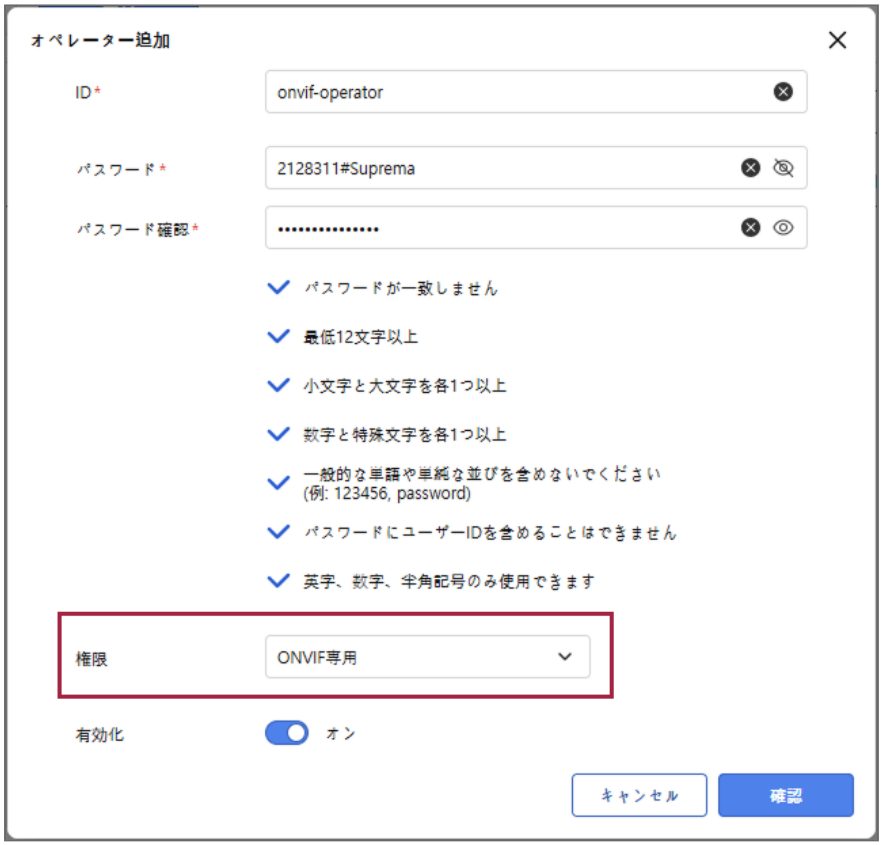
- **Profile T Only**: Profile T（Media2）のみで接続します。 H.264/H.265コーデック、HTTPS、メタデータ、イベントに対応し、最新のNVR/VMS環境で推奨される既定値です。
- **Profile T 優先 / S フォールバック**: NVR/VMSはまずProfile Tでの接続を試行し、Profile Tに対応しない場合はProfile S（Media1）で接続します。 Profile Tに対応するNVR/VMSは、このモードでもProfile Tで接続します。

項目	Profile T (Media2)	Profile S (Media1)
コーデック	H.264, H.265	H.264, MJPEG
暗号化通信	HTTPS対応	非対応（平文通信）
高度な機能	メタデータ、イベント	基本映像ストリーミング
推奨環境	最新のNVR/VMS	Profile Tをサポートしない旧型NVR/VMS

ONVIF専用アカウントの作成

Profile Sフォールバックを有効にする前に、NVR/VMSがONVIFおよびRTSP認証に使用するONVIF専用アカウントが必要です。アカウントなしで設定を保存すると、**Profile Sフォールバックの有効化にはONVIF専用アカウントが必要です** メッセージが表示され、設定は保存されません。

1. 画面左上の **システム** メニューをクリックします。
2. 画面左のサイドバーで **アカウント管理** をクリックします。
3. **オペレーター** セクションで **+ 追加** ボタンをクリックします。
4. **オペレーター追加** ポップアップウィンドウでIDとパスワードを入力し、**権限** で **ONVIF専用** を選択してください。



5. ONVIF専用アカウントを作成するには、**確認** ボタンをクリックしてください。

Profile Sフォールバックの有効化

Profile Sフォールバックを有効にしてください。

1. 画面左上の **設定** メニューをクリックしてください。
2. 画面左のサイドバーで **ネットワーク** → **ネットワーク** をクリックします。
3. **ONVIF** セクションの **モード** で **Profile T 優先 / S フォールバック** を選択してください。
4. **Profile S フォールバックの有効化** ポップアップウィンドウが表示されたら、Profile S使用時の注意事項を確認し、**確認** ボタンをクリックしてください。



5. 設定を保存するには、**保存**ボタンをクリックします。

設定を正常に保存すると、画面右上に成功メッセージが表示されます。 NVR/VMSにデバイスを登録するときは、ONVIF専用アカウントのIDとパスワードを入力してください。

Profile Sフォールバックを無効にするには、**Profile T Only** を選択し、**保存** ボタンをクリックしてください。

> **注意**
> Profile Sは暗号化なしで平文通信するため、ネットワーク攻撃にさらされる可能性があります。また、H.265コーデックとHTTPS/TLSを使用できません。 Profile Tをサポートしない旧型NVR/VMSと接続するときだけ使用してください。

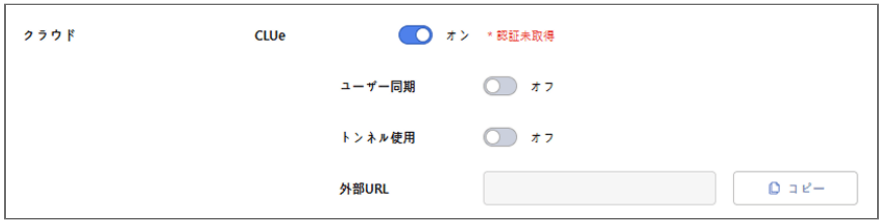
> **情報**
> - ONVIF設定は管理者のみ変更できます。
> - ONVIF専用アカウントはデバイスごとに一つだけ作成できます。 Web UIにログインできません。アカウントを作成すると、IDとパスワードを変更できません。
> - ONVIF専用アカウントは、有効化、無効化、削除のみ行えます。アカウントが無効の場合、Profile Sフォールバックを有効にできません。
> - ONVIF専用アカウントを削除するには、まず **Profile T Only** に変更してください。
> - 変更したONVIF設定は、新しい接続から適用されます。既存の接続済みストリームは、再接続するまで現在の接続方式を維持します。

CLUeクラウド接続

Suprema CLUeはクラウドベースの入退室管理サービスです。 CLUeに接続すると、CLUeクラウドサービスとユーザー情報を同期できます。

1. 画面左上の **設定** メニューをクリックしてください。
2. 画面左のサイドバーで **ネットワーク** → **ネットワーク** をクリックします。

3. **クラウド**セクションの**CLUe**トグルをクリックして有効にします。
4. システムがインターネット接続とCLUeサーバーへの接続を確認します。 **CLUe** トグルの右側に接続状態が表示されます。



- *** 接続中...**: CLUeサーバーに接続しています。
- *** 接続済み**: CLUeサーバーに接続済みです。
- *** 接続に失敗しました**: CLUeサーバーに接続できませんでした。インターネット接続を確認してから再試行してください。
- *** 認証未取得**: デバイスはCLUe認証を受けていません。

5. 必要なオプションを有効にしてください。次のオプションを使用するには、**CLUe** トグルを有効にしてください。
   - **ユーザー同期**: CLUeクラウドサービスとユーザー情報を同期します。
   - **トンネル使用**: CLUeを介して外部からデバイスにアクセスできるトンネルを使用します。トンネルが接続されると、**外部URL** フィールドにURLが表示されます。 **コピー** ボタンをクリックしてURLをコピーしてください。

> **情報**
>
> - 接続に成功すると、**CLUeが有効になりました** メッセージが表示されます。
> - 接続に失敗すると、**CLUeが無効になりました** メッセージが表示されます。インターネット接続を確認してから再試行してください。
> - **CLUe** トグルを無効にするとCLUeサーバーとの接続が切断され、**ユーザー同期**と**トンネル使用**オプションを使用できません。ただし、CLUeサーバー側の登録情報は保持されます。
> - CLUeの接続成功および失敗はシステムログに記録されます。

トンネルの設定

Tunnel セクションでは、Cloudflare Tunnelを使用して外部インターネットからデバイスのWeb UIにアクセスできる外部URLを作成できます。ルーターのポートフォワーディングやグローバルIPアドレスなしでリモートからデバイスにアクセスする場合に使用してください。

Tunnel セクションの **Type** で、次のいずれかを選択できます。

タイプ	説明	必要な情報
使用しない	トンネルを使用しません。既定値です。	なし
Cloudflare Tunnel (Quick)	Cloudflare アカウントなしで一時的な外部URLを発行します。デバイスを再起動するとURLが変わります。	なし

タイプ	説明	必要な情報
Cloudflare Tunnel (Named)	Cloudflare API TokenでTunnelを作成し、ユーザーのドメインに固定した外部URLを使用します。	Cloudflare アカウント、ドメイン
Cloudflare Tunnel (Named, Token)	Cloudflare ダッシュボードで事前に作成したTunnelにConnector Tokenで接続します。	Cloudflare アカウント、ドメイン、Connector Token

ヒント

テストや一時的なリモートアクセスには**Cloudflare Tunnel (Quick)**を使用してください。固定アドレスで継続してアクセスする場合は**Cloudflare Tunnel (Named)**または**Cloudflare Tunnel (Named, Token)**を使用してください。

情報

- Tunnelを使用しない場合は**Type**で**使用しない**を選択してください。
- Tunnelを使用するには、デバイスがインターネットに接続されている必要があります。
- 外部URLを知っている人は誰でも、デバイスのログイン画面にアクセスできます。管理者アカウントとオペレーターアカウントに強力なパスワードを設定し、外部URLは必要な人にのみ共有してください。
- Tunnelモードの変更はシステムログに記録されます。

一時的な外部URLの使用

Cloudflare アカウントなしで一時的な外部URLでデバイスにアクセスできます。

1. 画面左上の **設定** メニューをクリックしてください。
2. 画面左のサイドバーで **ネットワーク** → **ネットワーク** をクリックします。
3. **Tunnel**セクションの**Type**で**Cloudflare Tunnel (Quick)**を選択してください。



4. 一時的な外部URLを発行すると、**外部URL**フィールドに表示します。**コピー**ボタンをクリックしてURLをコピーし、Webブラウザーでアクセスしてください。

注意

Cloudflare Tunnel (Quick)で発行した外部URLは、デバイスを再起動すると変わります。再起動後は**外部URL**フィールドで新しいURLを確認してください。

固定外部URLの使用（API Token）

Cloudflare API Tokenを入力すると、デバイスがCloudflareにTunnelを作成し、指定したホスト名に外部URLを紐付けます。開始

する前に、Cloudflare アカウントとCloudflareに登録したドメインを用意してください。

1. 画面左上の **設定** メニューをクリックしてください。
2. 画面左のサイドバーで **ネットワーク** → **ネットワーク** をクリックします。
3. **Tunnel**セクションの**Type**で**Cloudflare Tunnel (Named)**を選択してください。



4. 次の情報を入力してください。
   - **Cloudflare API Token**: Cloudflare ダッシュボードで発行したAPI Tokenを入力してください。
   - **Account ID**：Cloudflare アカウント ID を入力してください。
   - **Hostname**：外部からアクセスするときに使用するホスト名を入力してください。

     > *例：cam.example.com*

   - **Tunnel Name (Option)**：Cloudflare で Tunnel を区別する名前を入力してください。任意です。
5. 入力した情報が正しいことを確認するには、**検証** ボタンをクリックしてください。
6. 設定を適用するには、**適用** をクリックしてください。

Tunnel が接続されると、**外部URL** フィールドに外部 URL が表示されます。 **コピー** ボタンをクリックすると URL をコピーできます。

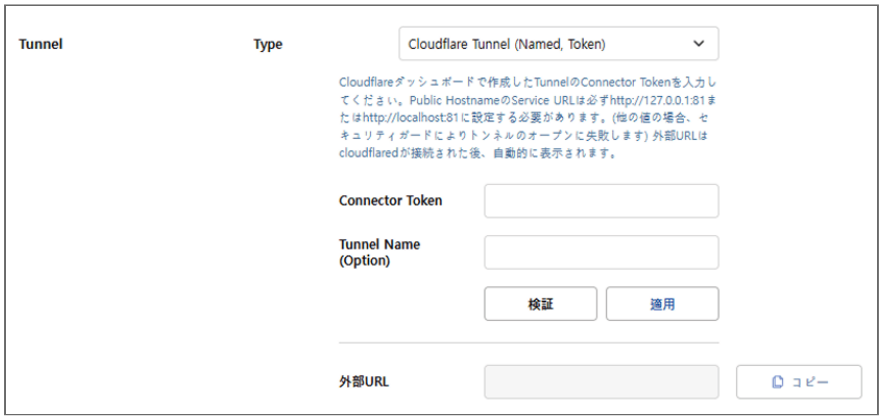
固定外部 URL の使用（Connector Token）

Cloudflare ダッシュボードで作成した Tunnel にデバイスを接続できます。開始する前に、Cloudflare ダッシュボードで次の作業を完了してください。

- Tunnel を作成し、Connector Token をコピーしてください。
- Tunnel の Public Hostname を追加し、Service URL を `http://127.0.0.1:81` または `http://localhost:81` に設定してください。

設定が完了したら、デバイスで次の手順を実行してください。

1. 画面左上の **設定** メニューをクリックしてください。
2. 画面左のサイドバーで **ネットワーク** → **ネットワーク** をクリックします。
3. **Tunnel** セクションの **Type** で **Cloudflare Tunnel (Named, Token)** を選択してください。



4. 次の情報を入力してください。
   - **Connector Token**：Cloudflare ダッシュボードからコピーした Connector Token を入力してください。
   - **Tunnel Name (Option)**：Tunnel を区別する名前を入力してください。任意です。
5. 入力した情報が正しいことを確認するには、**検証** ボタンをクリックしてください。
6. 設定を適用するには、**適用** をクリックしてください。

Cloudflared が接続されると、**外部URL** フィールドに外部 URL が自動的に表示されます。

> **注意**
> Public Hostname の Service URL を `http://127.0.0.1:81` または `http://localhost:81` 以外の値に設定すると、セキュリティポリシーにより Tunnel が開きません。

RS-485 の設定

RS-485 設定では、カメラの RS-485 ポートに接続された Suprema I/O 装置をスレーブ装置として登録し、管理できます。カメラは RS-485 ポートのマスターとして動作し、登録したスレーブ装置のリレーを AI ルールと連動して、扉の解錠や非常灯の作動などの外部装置を制御できます。

以下の状況では **RS-485** 設定を確認してください。

- カメラに I/O 装置を接続して、リレー出力や入力ポートを増やす場合
- AI イベントが発生したとき、スレーブ装置のリレーで外部装置を制御する場合
- スレーブ装置の接続状態を確認するか、ファームウェアを更新する必要がある場合
- 使用しなくなったスレーブ装置を削除する必要がある場合

情報

- ファームウェア バージョン 1.1.0 では、マスターモードのみをサポートします。カメラを他の装置のスレーブとして接続するスレーブモードはサポートしません。
- スレーブ装置は最大 8 台まで登録できます。
- サポートするスレーブ装置は Suprema I/O 装置です。指紋認証装置と顔認証装置はスレーブ装置として接続できません。
  - Secure I/O 2 (SIO2)
  - Door Module (DM-20)
  - Door Interface (DI-24)
  - Output Module (OM-120)
  - Input Module (IM-120)

開始する前に

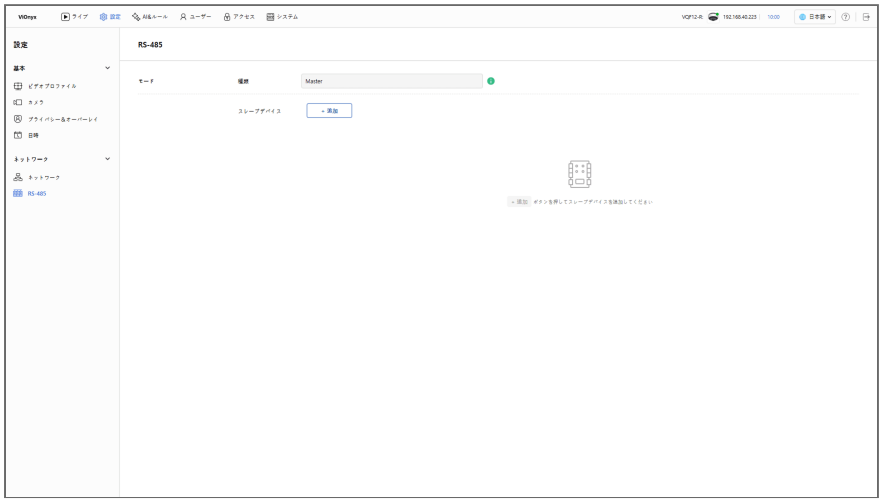
スレーブ装置を追加する前に、次の事項を確認してください。

- スレーブ装置がカメラの RS-485 ポートに正しく配線されているか確認してください。
- スレーブ装置に OSDP ID が割り当てられているか確認してください。 OSDP ID が 0（未割り当て）の装置は登録できません。
- 同じ RS-485 バスに接続された装置間で OSDP ID が重複していないか確認してください。
- スレーブ装置が別のマスター装置に登録されていた場合は、装置を初期化してください。

スレーブ装置の追加

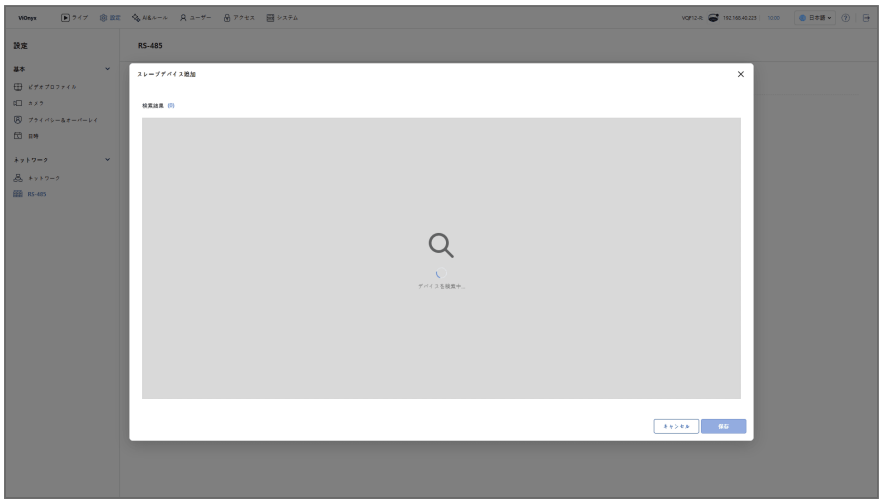
RS-485 ポートに接続されたスレーブ装置を検索して、カメラに登録してください。

1. 画面左上の **設定** メニューをクリックしてください。
2. 画面左のサイドバーで **ネットワーク** → **RS-485**をクリックします。

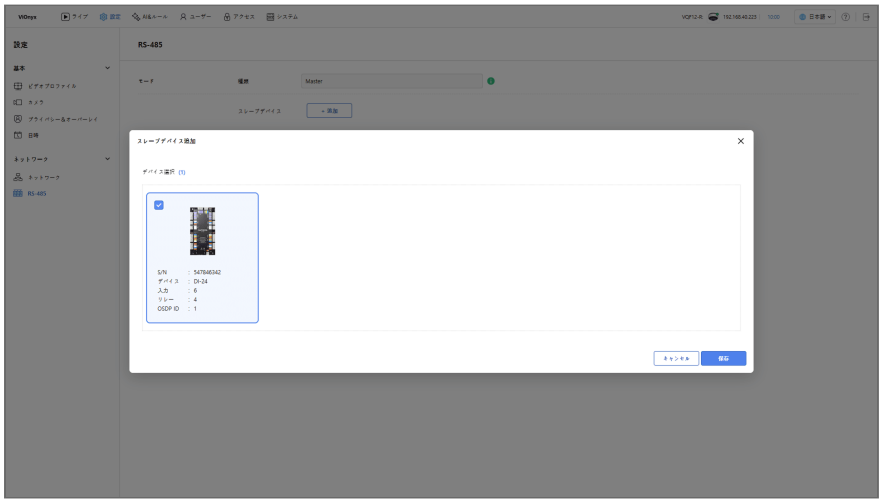


3. **スレーブデバイス** で **+ 追加** をクリックします。

4. **スレーブデバイス追加** ポップアップが表示され、装置検索が自動的に開始されます。検索が終了するまでお待ちください。



5. 検索結果で追加するデバイスのチェックボックスを選択します。複数のデバイスを選択できます。



検索されたデバイスには、以下の情報が含まれます。

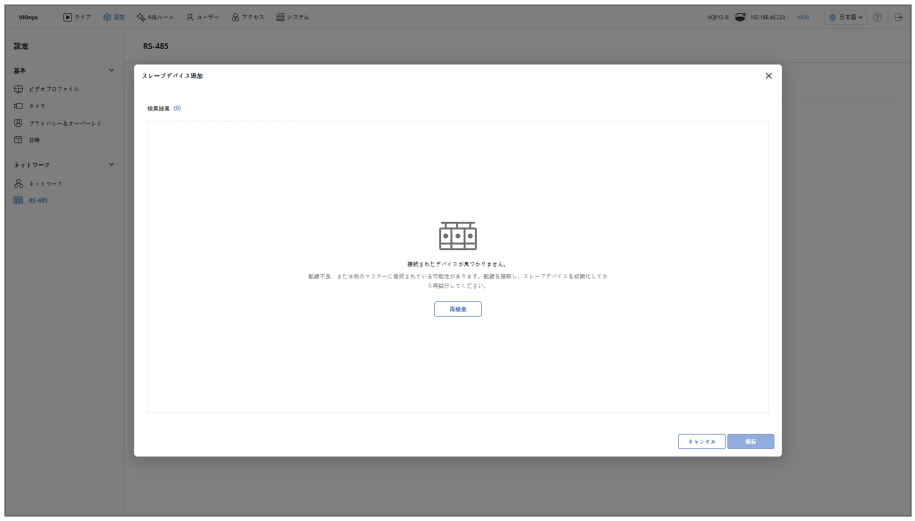
- **S/N**: デバイスのシリアル番号
- **デバイス**: デバイスのモデル名
- **入力**: 入力端子数
- **リレー**: リレー端子数
- **OSDP ID**: デバイスに割り当てられたOSDP ID

6. 選択したデバイスを登録するには、**保存** ボタンをクリックします。一つ以上のデバイスを選択すると、ボタンが有効になります。

デバイスの登録に成功すると、画面右上に成功メッセージが表示されます。**スレーブデバイス**一覧には、デバイスがOSDP ID順に表示されます。デバイス名はシリアル番号で自動設定され、スレーブデバイスの編集で変更できます。

デバイスが見つからない場合

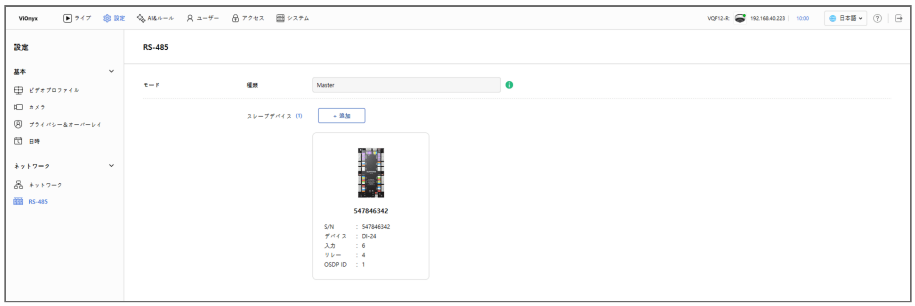
検索結果に**接続されたデバイスが見つかりません。**メッセージが表示されたら、次の事項を確認して**再検索** ボタンをクリックします。



- スレーブデバイスのRS-485配線が正しく接続されていることを確認します。
- スレーブデバイスが別のマスターデバイスに登録されている場合は、デバイスを初期化します。
- スレーブ装置に OSDP ID が割り当てられているか確認してください。

スレーブデバイスの状態確認

スレーブデバイス一覧で、登録したデバイスの情報と接続状態を確認できます。



デバイスとカメラの通信が切断されると、デバイスカードに**切断**表示とともに切断日時が表示されます。デバイスの電源とRS-485配線を確認します。デバイスが再接続されると、表示が消えます。



情報
スレーブデバイスの接続および切断の記録は、システムログで確認できます。詳細については[システムログを確認する]を参照してください。

スレーブデバイスの編集

登録したスレーブデバイスの名前を変更できます。

1. 画面左上の **設定** メニューをクリックしてください。
2. 画面左のサイドバーで **ネットワーク** → **RS-485**をクリックします。
3. 編集するデバイスカードにマウスポインターを合わせ、右上の ボタンをクリックしてください。
4. **スレーブ設定** ポップアップで、**名前** 入力フィールドに新しい名前を入力してください。



5. 変更を保存するには、**適用** ボタンをクリックしてください。

変更が正常に保存されると、画面右上に成功メッセージが表示されます。

> **情報**
> **スレーブ設定** ポップアップでは OSDP ID を確認するだけで、変更できません。

スレーブデバイスのファームウェア更新

スレーブ設定 ポップアップで、スレーブデバイスの現在のファームウェアバージョンを確認し、更新できます。

1. 画面左上の **設定** メニューをクリックしてください。
2. 画面左のサイドバーで **ネットワーク** → **RS-485**をクリックします。
3. 更新するデバイスカードにマウスポインターを合わせ、右上の ボタンをクリックしてください。
4. **スレーブ設定** ポップアップの **FWバージョン** で現在のバージョンを確認し、**更新** ボタンをクリックしてください。



5. ドラッグ＆ドロップするか、**ファイル選択** ボタンをクリックしてファームウェアファイルを選択してください。



6. 更新中のサービス中断に関する案内を確認し、**サービス中断を理解し許可します。** チェックボックスを選択してください。
7. 更新を開始するには **アップロード** ボタンをクリックしてください。

更新中は進行状況と進行率が表示されます。スレーブデバイスのファームウェア更新の成功と失敗の記録は、システムログで確認できます。

> **注意**
>
> - 更新中は、対象デバイスのリレーと入力、およびすべてのスレーブデバイスの入力が停止し、セキュアチャネルが一時的に解除されます。デバイスを使用しない時間帯に更新してください。
> - 更新中はデバイスの電源を切ったり、RS-485 配線を外したりしないでください。
> - 別のファームウェア更新が進行中の場合、更新を開始できません。進行中の更新が完了してから、再試行してください。

スレーブデバイスの削除

使用しなくなったスレーブデバイスを削除できます。デバイスを個別に削除するか、複数のデバイスを選択して一括で削除できます。

> **注意**
>
> AI ルールで使用中のデバイスは削除できません。削除を試みると、そのデバイスを使用しているルール名が表示されます。まず、該当ルールからデバイスのリレー設定を削除し、再試行してください。ルールの修正方法については、AIルールの設定をご参照ください。

デバイスを一台ずつ削除

1. 画面左上の **設定** メニューをクリックしてください。
2. 画面左のサイドバーで **ネットワーク** → **RS-485**をクリックします。
3. 削除するデバイスカードにマウスポインターを合わせ、右上の ボタンをクリックしてください。
   - または ボタンをクリックし、**スレーブ設定** ポップアップウィンドウで **削除** ボタンをクリックしてください。
4. **デバイス削除** ポップアップウィンドウが表示されたら、**適用** ボタンをクリックしてください。

複数のデバイスを一括で削除

1. 画面左上の **設定** メニューをクリックしてください。
2. 画面左のサイドバーで **ネットワーク** → **RS-485**をクリックします。
3. 削除するデバイスカードのチェックボックスをそれぞれ選択してください。 **デバイス選択** の横に、選択したデバイス数が表示されます。



4. **削除** ボタンをクリックしてください。
5. **デバイス削除** ポップアップウィンドウが表示されたら、**適用** ボタンをクリックしてください。

デバイスの削除に成功すると、画面右上に削除成功メッセージが表示されます。

トラブルシューティング

スレーブデバイスを追加、修正、削除するときに、次のエラーメッセージが表示されることがあります。

メッセージ	原因と対処
スレーブデバイスの登録に失敗しました。配線を確認して再試行してください。	デバイスと通信できませんでした。 RS-485 配線を確認してから再試行してください。
スレーブデバイスは最大8台まで登録できます。	すでに8台登録されています。使用していないデバイスを削除してから再度追加してください。

メッセージ	原因と対処
同じシリアル番号のデバイスがすでに登録されています。	同じシリアル番号のデバイスがすでに一覧にあります。一覧を確認してください。
このOSDP IDはすでに使用されています。	別のデバイスが同じ OSDP ID を使用しています。スレーブデバイスで OSDP ID を変更してから再度検索してください。
バス上の他のデバイスとOSDP IDが競合しています。	RS-485 バス上の別のデバイスと OSDP ID が重複しています。スレーブデバイスで OSDP ID を変更してから再度検索してください。
OSDP ID 0（未割当）のデバイスは登録できません。デバイスでアドレスを割り当てて再検索してください。	OSDP ID が 0（未割り当て）のデバイスです。デバイスで OSDP ID を割り当ててから再度検索してください。
デバイス検索がタイムアウトしました。	検索時間内にデバイスが応答しませんでした。配線を確認してから再度検索してください。
スレーブデバイスはルールで使用中です。	デバイスはAIルールで使用中です。該当ルールからデバイスのリレー設定を削除してから再試行してください。
RS-485を初期化しています。しばらくお待ちください。	カメラがRS-485ポートを準備中です。しばらくしてから再試行してください。

RTSPおよびONVIF連携

カメラは、他社NVR(Network Video Recorder)およびVMS(Video Management Software)との標準連携のために、RTSP(Real-Time Streaming Protocol)ストリーミングとONVIF(Open Network Video Interface Forum)プロトコルをサポートします。

次のような場合は、この文書を参照してください。

- 他社NVR/VMSでRTSP経由でカメラ映像を取得したいとき
- ONVIFをサポートするNVR/VMSとカメラを連携したいとき
- RTSP接続先URLやONVIF連携に必要なアカウント情報を確認したいとき

RTSPストリーミング

ポートおよび転送方式

RTSPポートと転送方式は**ネットワーク**設定で変更できます。ポート設定、映像転送、および暗号化設定の詳細は、次の文書を参照してください。

- ポート設定
- 映像転送と暗号化の設定

> **情報**
> RTSPポートをデフォルト値(554)から変更した場合は、下の**Connection URL**の {port} 部分も変更後のポート番号に入力してください。

RTSP Connection URL

他社NVR/VMSでカメラ映像をRTSPで取得するには、チャンネルと解像度に合うConnection URLを登録する必要があります。

チャンネル	ストリーム	Connection URL
Channel 1 - Fisheye(フィッシュアイ映像)	メインストリーム(高解像度)	rtsp://{id}:{passwd}@{IP_address}:{port}/fisheye_primary
Channel 1 - Fisheye(フィッシュアイ映像)	サブストリーム(低解像度)	rtsp://{id}:{passwd}@{IP_address}:{port}/fisheye_secondary
Channel 2 - Dewarp(平面歪み補正映像)	メインストリーム(高解像度)	rtsp://{id}:{passwd}@{IP_address}:{port}/dewarp_primary

- {id}, {passwd}: カメラに接続するアカウントのIDとパスワードを入力します。
- {IP_address}: カメラのIPアドレスを入力します。
- {port}: RTSPポート番号を入力します。デフォルト値は554です。

ONVIF連携

サポート仕様

カメラはONVIF **Profile S**および**Profile T**をサポートします。

ONVIF専用アカウントの準備

セキュリティ標準仕様により、デフォルトの管理者(admin)アカウントではONVIF接続をサポートしません。 ONVIFで連携する前に、ONVIF専用のオペレーターアカウントを追加し、そのアカウント情報でNVR/VMSに接続してください。 ONVIF専用オペレーターアカウントの追加方法はネットワークを設定を参照してください。

連携時の注意事項

- **設定同期保護**

  Web設定エンジンとのデータ整合性を維持し、誤動作を防ぐため、ONVIF経由で解像度、ビットレート、イメージセンサー属性などのカメラ内部設定値を変更する書き込み(Write)操作はサポートしません。

- **VMS自動最適化機能の無効化**

  一部のVMSは、接続時にカメラ設定を自動変更する機能(Video Optimization、Auto Configurationなど)を提供します。この機能がオンだと連携エラーが発生する場合があるため、VMS側でカメラ設定の自動修正/最適化オプションを無効にしてください。

注意

RTSP転送方式を変更すると、既存のRTSPセッションを再接続する必要があります。 NVR/VMSでも、選択した転送方式と互換になるように設定してください。

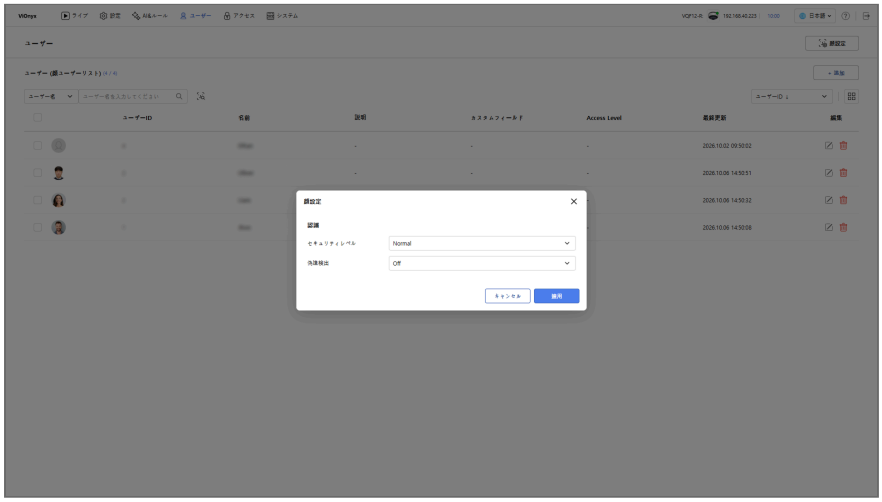
ユーザー管理

ユーザーを登録して、AI顔認識機能を活用できます。新規ユーザーの登録から既存ユーザー情報の管理・参照まで、ユーザーのライフサイクル全体を効率的に管理してください。

顔認証設定

顔認証設定で、認証効率、セキュリティレベル、偽造検知を一度に管理できます。組織のセキュリティポリシーと運用環境に合わせて、適切な値に調整します。

1. 画面左上の **ユーザー** メニューをクリックします。
2. 画面右上の **顔設定** ボタンをクリックします。
3. **顔設定** ウィンドウが表示されたら、必要なオプションを設定します。



- **セキュリティレベル**: セキュリティレベルを設定できます。セキュリティレベルが高いほど、認証はより厳格になります。
- **偽造検出**: 写真などの偽造顔を使ったユーザー認証を防止できます。

4. 設定が完了したら、**適用** ボタンをクリックします。

> **ヒント**
> 高いセキュリティが必要なエリアでは、**セキュリティレベル** オプションを **Most Secure** に設定することを推奨します。

ユーザーの追加

AI顔認証に使用するユーザーを登録できます。ユーザーを追加する際に基本情報を入力し、3つの方法のいずれかで顔写真を登録できます。

次のような場合にユーザーを追加してください。

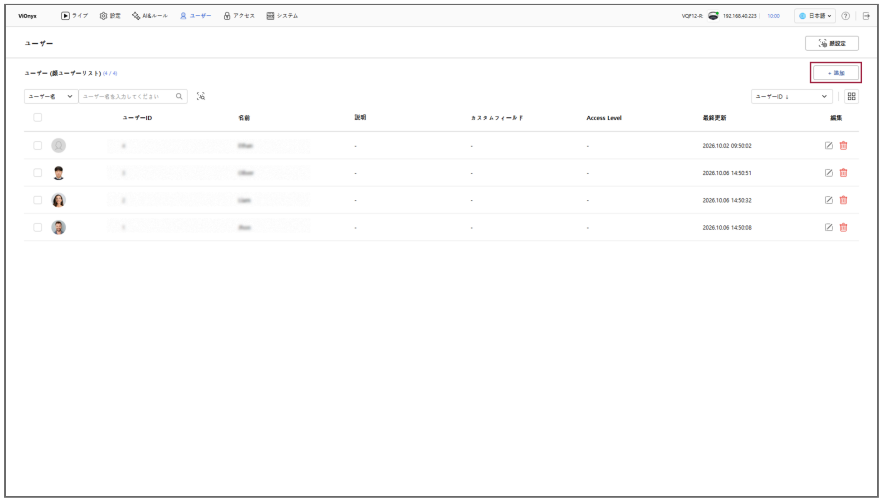
- 組織に新たに入社したユーザーを登録する場合
- ユーザーの顔写真を撮影して顔認証データベースに登録する場合
- 複数のユーザーを一括で追加する場合
- 外部システム（ERP、人事管理システム）と連携するためにユーザーを登録する場合

> **情報**
>
> - 顔認証機能を使用するには、該当地域の関連法規を遵守する必要があります。
> - 初回にユーザーを追加する際、顔認証利用同意のポップアップが表示されます。同意の記録はシステムログに保存され、同意後は再表示されません。
> - AIイベント設定で事前に同意を完了している場合、ユーザー追加時に別のポップアップは表示されません。

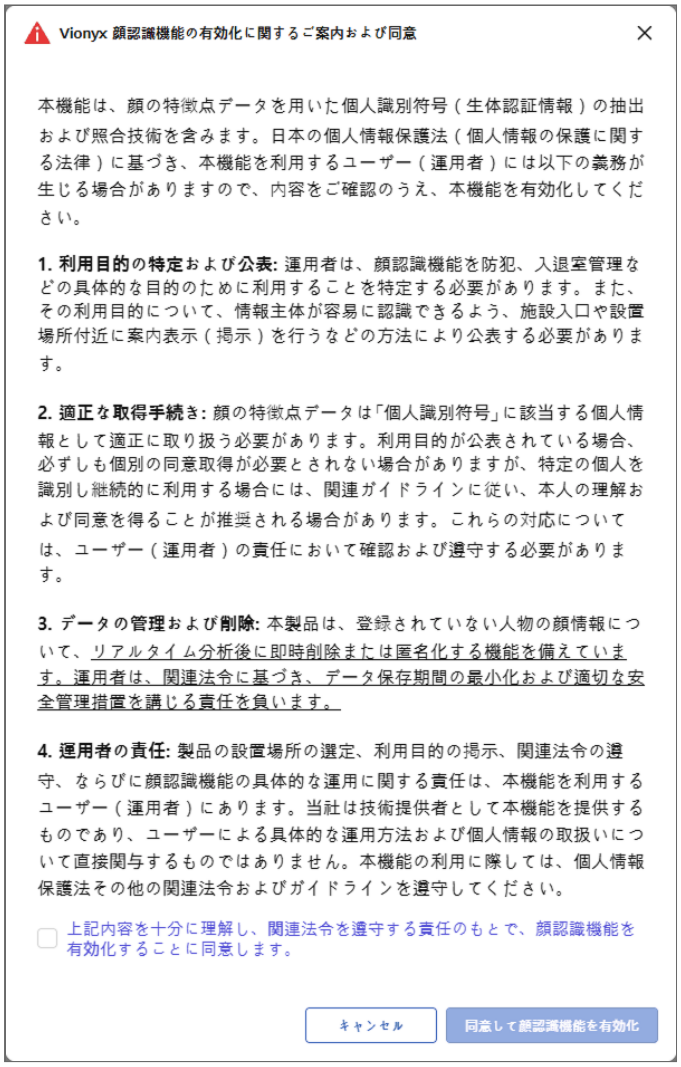
ユーザー基本情報の入力

初回のユーザー追加時に顔認証利用同意のポップアップが表示されたら、内容を確認して進めてください。同意完了後、ユーザー追加ダイアログで基本情報を入力してください。

1. 画面左上の **ユーザー** メニューをクリックします。
2. 画面右上の **追加** ボタンをクリックしてください。

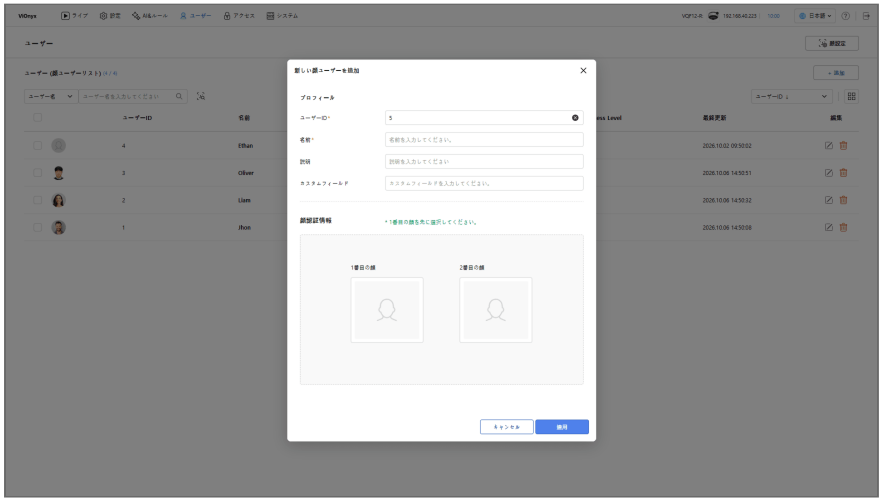


3. 初回ユーザー追加時に **Vionyx 顔認識機能の有効化に関するご案内および同意** ポップアップが表示されたら、内容を確認し、同意チェックボックスをクリックしてから **同意して顔認識機能を有効化** ボタンをクリックしてください。



- 顔認証機能を使用するには、該当地域の関連法規を遵守する必要があります。同意しない場合は先に進めません。
- 「**Vionyx 顔認識機能の有効化に関するご案内および同意**」ポップアップは初回のみ表示されます。

4. **新しい顔ユーザーを追加** ウィンドウが表示されたら、ユーザーの基本情報を入力してください。



5. **ユーザーID** 入力欄にユーザーの固有IDを入力してください。ユーザーIDは他のユーザーと重複できません。

6. **名前** 入力欄にユーザー名を入力してください。
   - 最大64文字まで入力できます。
   - 韓国語、日本語、英大文字・小文字、数字、特殊文字（`#`、`-`、`_`、`.`、`(`、`)`）、文字の途中のスペースを含めることができます。
7. **説明** 入力欄にユーザーの説明を入力してください。最大256文字まで入力できます。
8. **カスタムフィールド** 入力欄では、ユーザー固有の追加情報を最大64文字まで入力できます。たとえば、部署、役職、ユーザーグループなどを英数字形式のメモとして入力できます。
9. ユーザー基本情報を保存するには、**適用** ボタンをクリックしてください。

> **情報**
> 新しいユーザーは顔写真なしで先に作成できます。後でユーザーの詳細ページから顔写真を追加できます。

顔登録

ユーザーを新規追加する際、またはユーザー詳細ページで顔を登録できます。 3つの方法が提供されます。

1. 画面左上の **ユーザー** メニューをクリックします。
2. 画面右上の**追加**ボタンをクリックするか、ユーザー一覧から既存ユーザーをクリックして詳細ページに移動してください。
3. ユーザー追加またはユーザー詳細のポップアップの**顔認証情報**セクションで顔を登録できます。



4. **1番目の顔** にマウスを重ねると、登録オプションが表示されます。



- : ローカルに保存された画像ファイルをアップロードして、顔写真を登録できます。
- : ウェブカメラで顔写真を撮影して登録できます。
- : AIイベントで検出された未認識顔の一覧から、ユーザーに合う顔を選択して登録できます。

> **情報**
> 1番目の顔を先に選択してください。 2番目の顔は任意です。

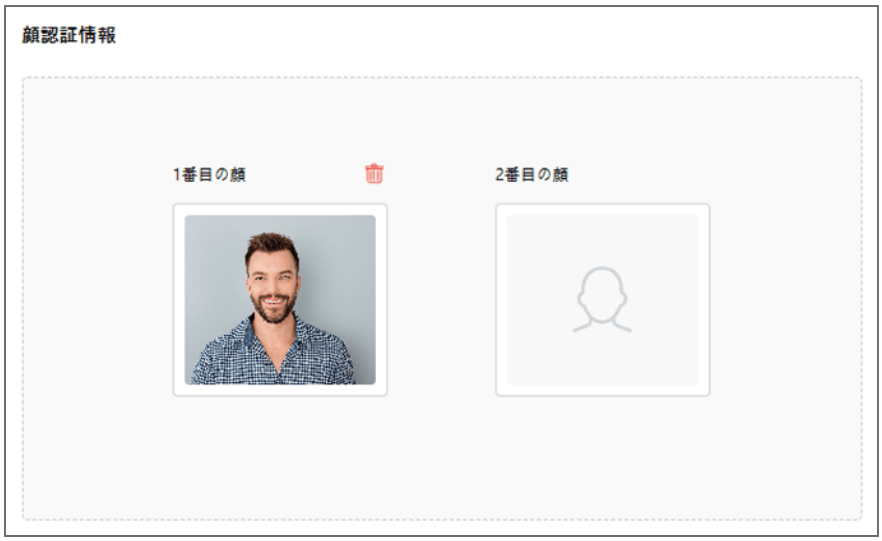
顔写真のアップロード

ローカルに保存された画像ファイルをアップロードして顔写真を登録できます。



1. 以下の方法から希望の方法で顔写真をアップロードしてください。
   - ローカルに保存された画像ファイルをドラッグ＆ドロップで顔領域にドラッグしてください。
   - ローカルに保存された画像ファイルを選択するには、 ボタンをクリックして、目的の画像ファイルを選択してください。

2. 顔が認識されると写真が表示されます。



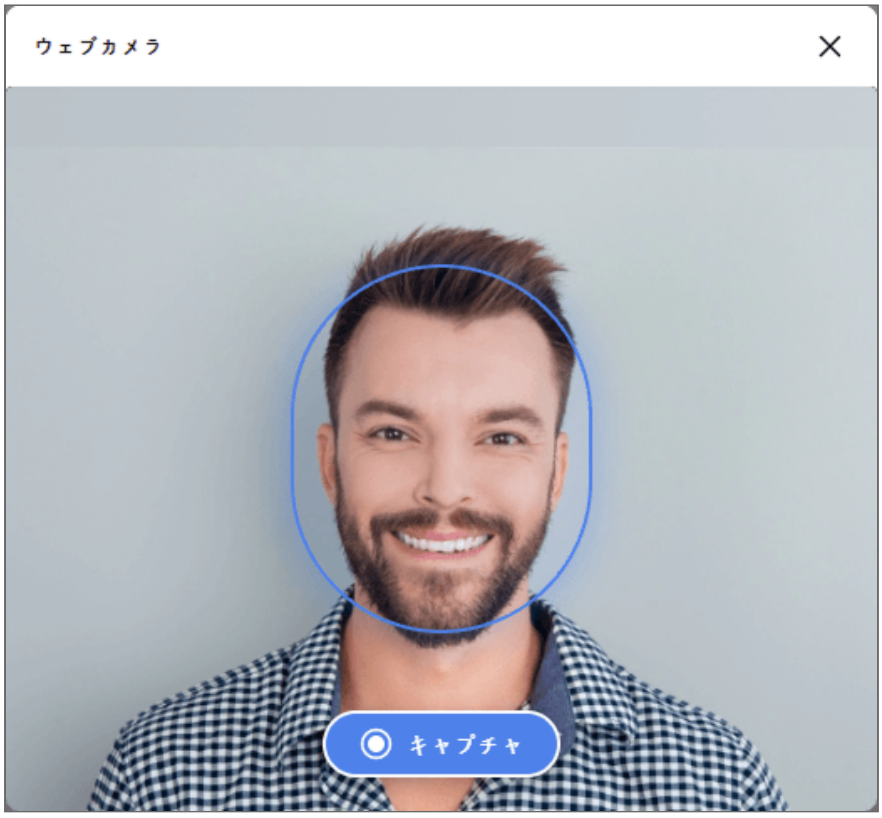
3. アップロードした写真をユーザーに適用するには、下部の **適用** ボタンをクリックしてください。

> **情報**
>
> - 対応する画像ファイル形式はPNG、JPEG、JPGです。
> - 対応する画像ファイルの最大サイズは10MBです。

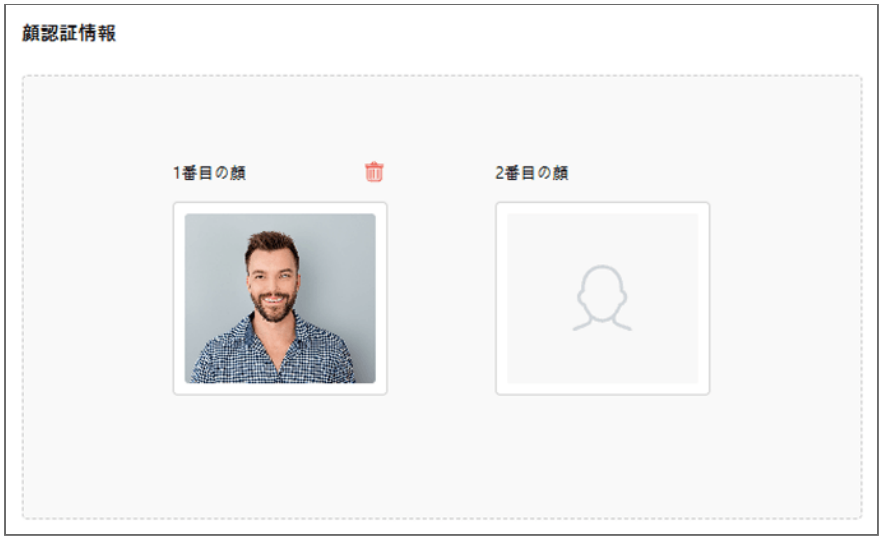
ウェブカメラで顔を登録

ウェブカメラを使用して顔写真を撮影して登録できます。

1. ボタンをクリックしてください。
2. ウェブカメラの撮影画面が表示されたら、顔が画面中央の円内に来るように位置を調整してください。



3. **キャプチャ** ボタンをクリックしてください。



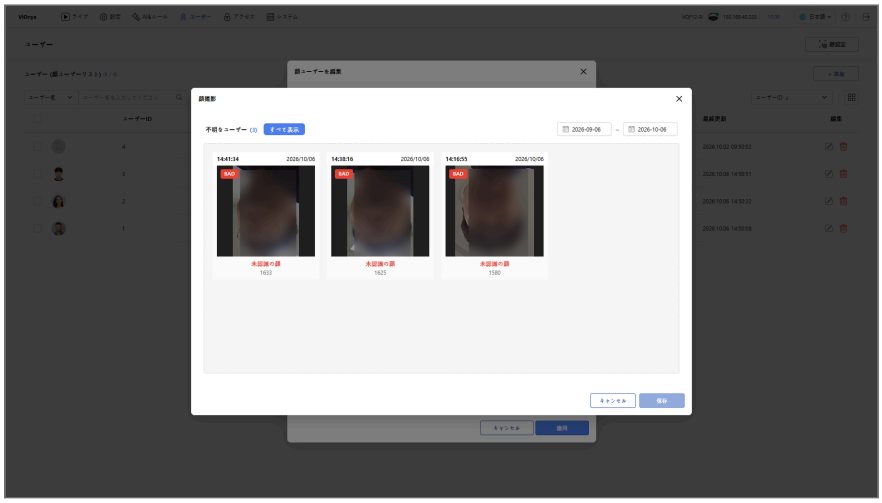
4. 撮影した写真をユーザーに適用するには、**適用** ボタンをクリックしてください。

> **情報**
> 再撮影するには、顔写真をクリックして再度撮影できます。

AI推奨顔登録

AI分析で検出された未エンロールの顔の一覧から、ユーザーに合う顔を選択してエンロールできます。

1. ボタンをクリックしてください。
2. **顔撮影** ポップアップウィンドウに、最近認証された未エンロールの顔の一覧が表示されます。



登録可能な顔 一覧が表示されない場合は、**すべて表示** ボタンをクリックします。未エンロールの顔をすべて確認できます。

3. ユーザーに合う顔を選択してください。一度に1つの顔のみ選択できます。
4. **保存** ボタンをクリックしてください。
5. 選択した顔をユーザーに適用するには、**適用** ボタンをクリックしてください。

ユーザーの編集と削除

登録済みユーザーの情報を編集し、顔を追加・変更できます。また、不要になったユーザーを削除でき、ユーザーの操作履歴をイベントログで確認できます。

以下のような場合にユーザーを編集または削除してください。

- ユーザーの氏名、所属部署などの情報を変更するとき
- ユーザーの顔写真を更新する、または新しい顔を追加するとき
- ユーザーが退職したり、システムから削除する必要があるとき
- ユーザーの認証記録や変更履歴を確認するとき
- 登録済みユーザーで誤認証が発生した場合

> **情報**
>
> - ユーザー情報の編集で高品質の写真をアップロードしても、以前のテンプレートデータが残る場合があるため、ユーザーを削除して再登録することを推奨します。
> - 削除操作は取り消せません。ユーザーを削除する前に必要なデータをバックアップし、慎重に確認してください。

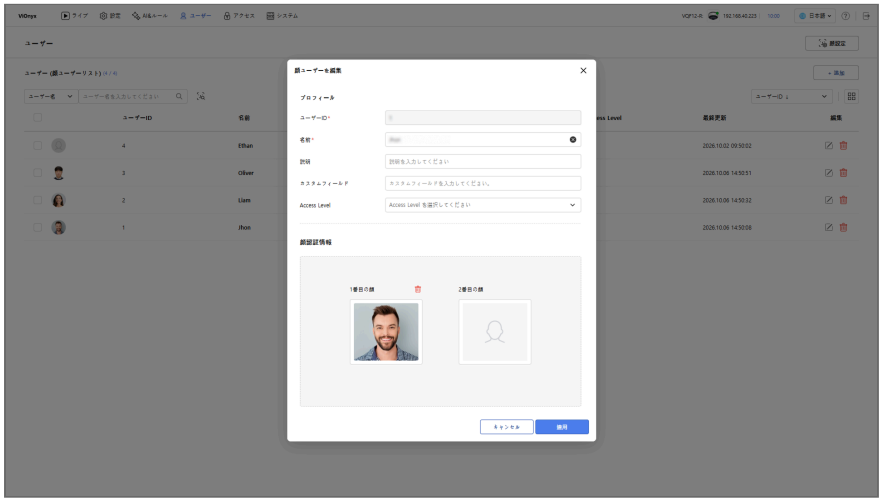
ユーザー情報の編集

登録済みユーザーの情報を編集し、顔を追加・変更できます。

1. 画面左上の **ユーザー** メニューをクリックします。
2. ユーザー一覧で、編集するユーザーの **編集** 列にある ボタンをクリックします。



3. **顔ユーザーを編集** ウィンドウが表示されたら、必要な情報を編集します。



4. ユーザー情報の編集が完了したら、**適用** ボタンをクリックしてください。

編集が完了すると、右上に成功メッセージが表示され、ユーザー一覧に戻ります。

> **情報**
>
> - ユーザーの詳細情報については、ユーザーの追加を参照してください。
> - **ユーザーID**は編集できません。
> - 顔写真は個別に削除できます。該当する顔写真の右上にある 🗑 ボタンをクリックします。

ユーザーの削除

不要になったユーザーを削除できます。

個別ユーザーの削除

1. 画面左上の **ユーザー** メニューをクリックします。
2. ユーザー一覧で削除するユーザーの一番右にある 🗑 ボタンをクリックしてください。



3. 削除確認メッセージが表示されたら、**確認** ボタンをクリックしてください。

画面右上に削除確認メッセージが表示され、ユーザー一覧から該当ユーザーが削除されます。

複数ユーザーの一括削除

1. 画面左上の **ユーザー** メニューをクリックします。
2. ユーザー一覧で削除するユーザーの一番左にあるチェックボックスをクリックしてください。複数のユーザーを選択できます。



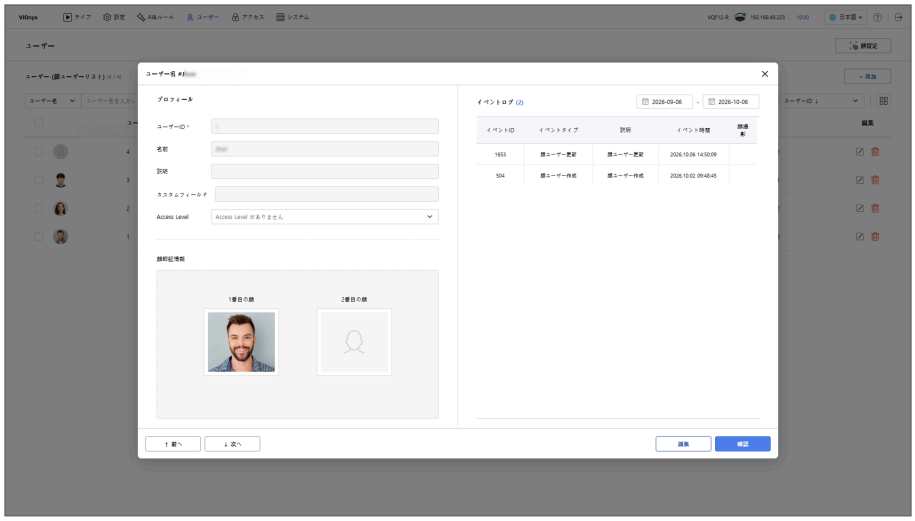
3. 画面右上に削除ボタンが表示されたら、**削除** ボタンをクリックしてください。
4. 削除確認メッセージが表示されたら、**確認** ボタンをクリックしてください。

画面右上に削除確認メッセージが表示され、ユーザー一覧から該当ユーザーが削除されます。

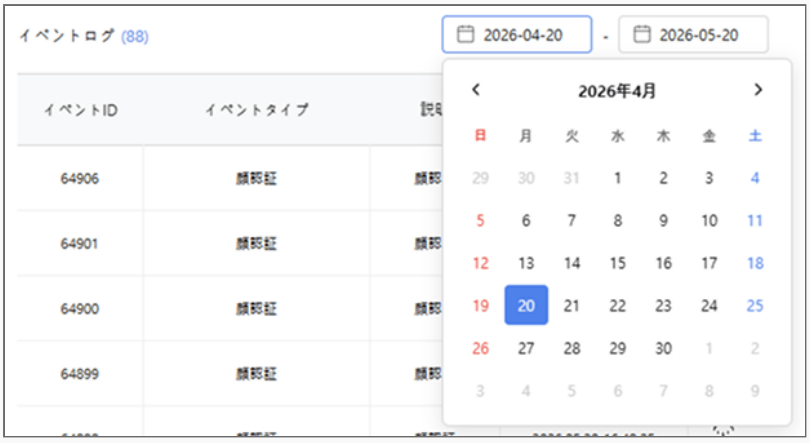
ユーザーイベントログの確認

登録済みユーザーの活動履歴をイベントログで確認できます。

1. 画面左上の **ユーザー** メニューをクリックします。
2. ユーザー一覧でイベントログを確認するユーザーをクリックしてください。
3. ユーザー詳細ポップアップが表示されたら、右側の**イベントログ**でイベント一覧を確認できます。



- 右上のカレンダーアイコンで特定の日付のイベントを表示できます。



- イベントログは自動で記録され、ユーザーの重要なすべての活動を追跡できます。

ユーザーの検索と表示

ユーザー一覧で名前やIDを入力すると、目的のユーザーを素早く見つけられます。必要に応じて、ユーザー情報をテーブル形式またはカード形式で表示できます。

次のような場合に、ユーザーの検索と表示機能を使用してください。

- 多数のユーザーの中から特定のユーザーをすばやく見つける必要があるとき
- カード形式でユーザープロフィールを一目で確認したいとき
- ユーザー一覧を名前、ID、最終更新時刻で並べ替えて確認したいとき

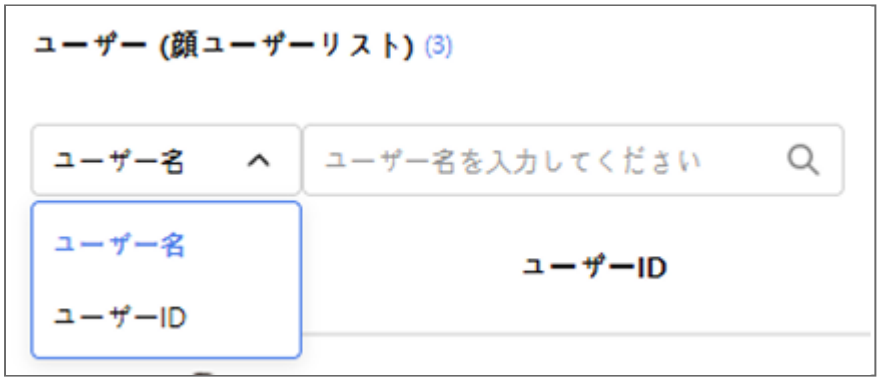
ユーザー検索

目的のユーザーを見つけるための検索機能を提供します。ユーザー名またはIDで検索でき、顔画像から類似したユーザーを検索できます。

キーワード検索

ユーザー一覧で名前またはIDを入力して、目的のユーザーを検索できます。

1. 画面左上の **ユーザー** メニューをクリックします。
2. ユーザー一覧の左上にある検索入力で検索条件を選択します。 **ユーザー名** または **ユーザーID** を選択できます。



3. 検索入力フィールドに検索語を入力します。



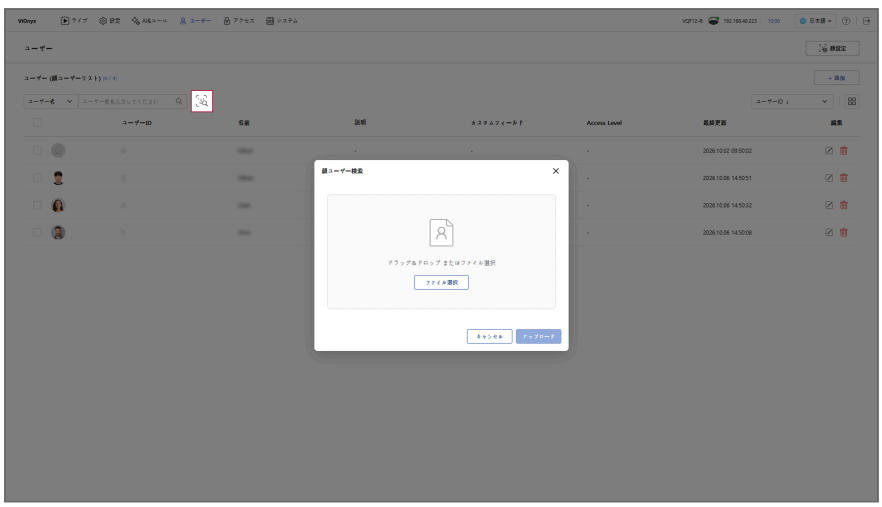
4. 入力したキーワードと一致するユーザーが一覧に表示されます。

> **情報**
>
> - 部分一致検索に対応しています。例えば「Kim」と入力すると、名前に「Kim」を含むすべてのユーザーが表示されます。
> - 検索結果は現在選択されているフィルター条件に従って表示されます。フィルターを変更すると、検索結果も更新されます。

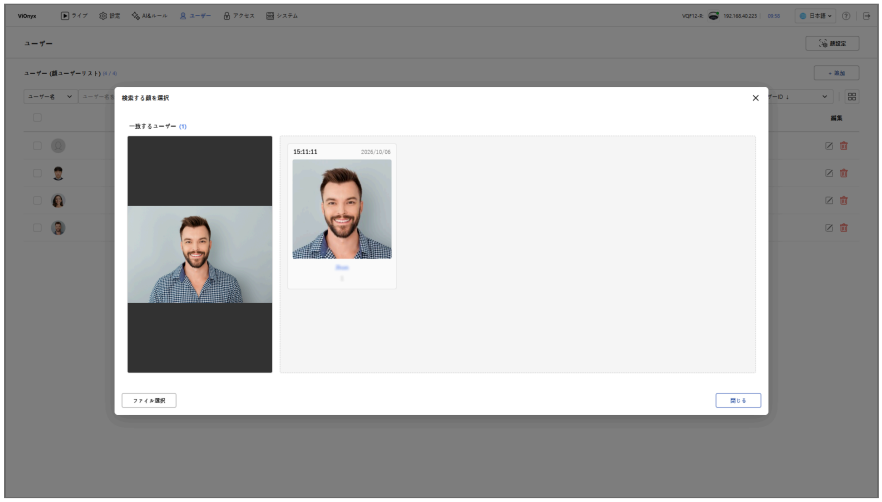
顔画像で検索

顔画像をアップロードして、類似した顔のユーザーを検索できます。

1. 画面左上の **ユーザー** メニューをクリックします。
2. 検索入力フィールド右側の ボタンをクリックします。
3. **顔ユーザー検索** ウィンドウが表示されたら、顔画像をドラッグ＆ドロップするか、**ファイル選択** からアップロードします。



4. 顔画像のアップロードが完了したら、**アップロード** ボタンをクリックします。
5. **検索する顔を選択** ウィンドウが表示されると、アップロードした顔画像に一致するユーザー一覧が表示されます。



- 一致したユーザーの中から目的のユーザーを選択すると、そのユーザーの詳細情報ページに移動できます。
- 別の顔画像でもう一度検索するには、左下の **ファイル選択** ボタンをクリックして、新しい顔画像をアップロードします。

> **情報**
> 顔画像以外の画像をアップロードすると、正しい顔画像ではないというメッセージが表示されます。顔画像で再試行してください。

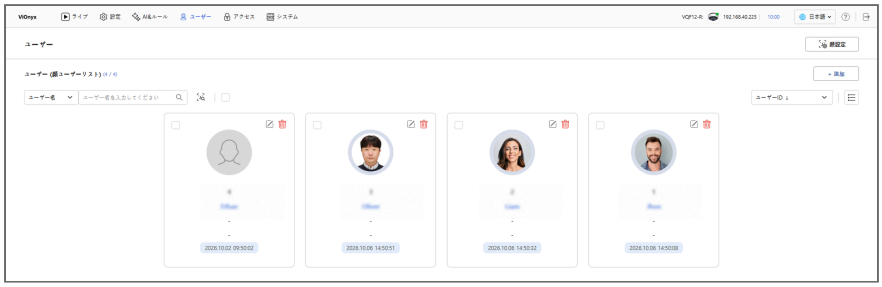
表示モードの変更

ユーザー一覧をテーブル形式またはカード形式で表示できます。ユーザー一覧の右上にある または ボタンをクリックして、表示モードを選択します。

- **リスト表示に切り替え**



- **グリッド表示に切り替え**



> **情報**
>
> **リスト表示に切り替え**, **グリッド表示に切り替え** は、どちらも同じ機能を提供します。表示方法が異なるだけで、検索、フィルター、並べ替えの結果は同じです。

ユーザー一覧の並べ替え

ユーザー一覧をユーザー名、ユーザーID、最終更新時刻の昇順または降順に並べ替えできます。

1. ユーザー一覧の右上にある並べ替えドロップダウンをクリックします。



2. 目的の並べ替え条件を選択します。

入退室制御管理

アクセス メニューでは、カメラに接続された扉を登録し、どのユーザーがいつ入退室できるかを入退室レベルで指定できます。入退室制御イベントが顔認証の結果で許可可否を判定すると、カメラは扉に接続されたリレーを開いて入退室を許可します。扉の状態をリアルタイムで確認し、遠隔で解錠または施錠できます。また、判定結果に応じて音声案内やWebhook通知を実行するよう設定できます。入退室制御を初めて設定する場合は、先に入退室制御イベントを作成し、その後、扉、入退室レベル、扉ルールの順に設定してください。

> **情報**
>
> - **アクセス** メニューはファームウェアバージョン1.1.0以降で利用できます。
> - **アクセス** メニューはベータ版として提供しています。今後のファームウェアアップデートで画面構成や動作が変更される場合があります。

ドア管理

カメラで実際に解錠・施錠するドアを登録できます。ドアを登録するときは、どのアクセス制御イベントで入退室を判定するか、どのリレーで錠前を制御するか、ドアをどれくらい開放するかも指定します。ドアを登録すると、アクセスレベルとドアルールでそのドアを選択できます。

次のような場合は、ドアを登録してください。

- 顔認証で入室が許可されたユーザーに対して、ドアを自動で開ける場合
- 退室ボタンを押して内側からドアを開けられるようにする場合
- センサーでドアの開閉状態を確認する場合
- 営業時間はドアを開放し、夜間は施錠するなど、時間帯ごとにドアを運用する場合

開始する前に

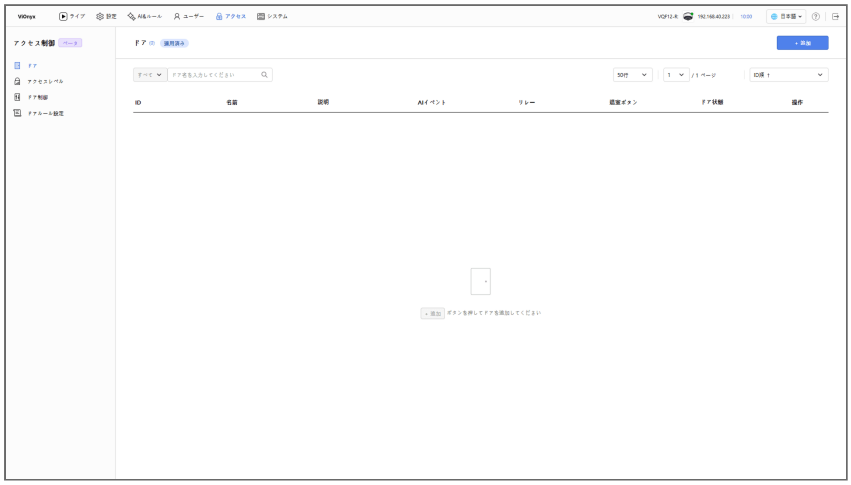
ドアを登録する前に、次の事項を確認してください。

- カメラごとにドアを最大10個まで登録できます。カメラが制御するドア数を事前に確認してください。
- 入退室判定に使用するアクセス制御イベントを先に作成してください。詳しくは、入退室制御イベントを設定するを参照してください。
- ドアの錠前が、カメラまたは下位I/Oデバイスのリレーポートに接続されていることを確認してください。下位I/Oデバイスを使用するには、先にRS-485経由でデバイスを登録してください。詳しくは、RS-485 の設定を参照してください。
- 退室ボタンまたはドア状態センサーを使用するには、該当デバイスが入力ポートに接続されていることを確認してください。
- 開放スケジュールまたは施錠スケジュールを使用するには、事前にスケジュールを作成してください。詳しくは、スケジュール管理を参照してください。

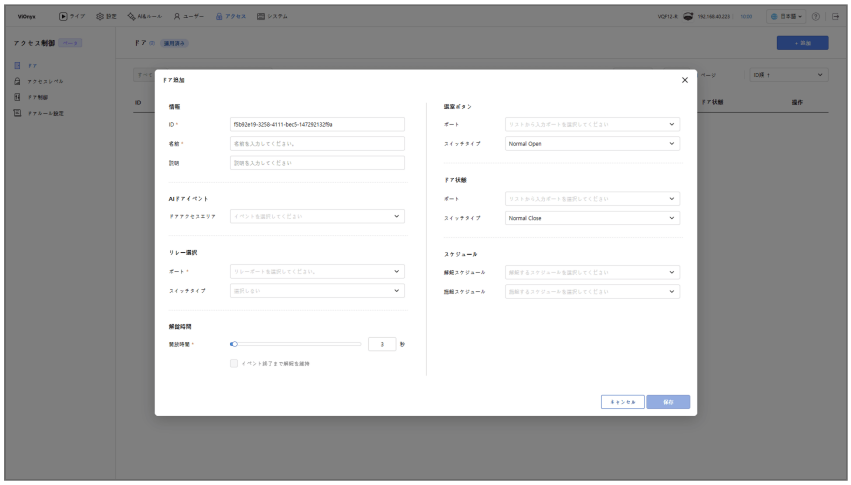
ドアの追加

1 ドアの追加を開始

1. 画面左上の **アクセス** メニューをクリックします。
2. 画面左側のサイドバーで **ドア** をクリックします。



3. 画面右上の**+ 追加**ボタンをクリックしてください。
4. **ドア追加** ポップアップが表示されたら、ドア情報を入力します。必須項目をすべて入力すると、**保存** ボタンが有効になります。



2 基本情報入力

情報 セクションでドアを識別する情報を入力します。

- **ID**：ドアの固有IDです。自動で入力されます。必要に応じて変更できます。ほかのドアと同じIDは使用できません。最大64文字まで入力できます。英数字、ハイフン（`-`）、アンダースコア（`_`）を使用できます。
- **名前**：ドア名を入力します。管理を容易にするために識別しやすい名前を入力してください。必須項目です。他のドアと同じ名前は使用できません。**正面玄関**、**2階オフィス**のように場所が分かる名前を付けると、入退室レベルとルールでドアを簡単に区別できます。

- **説明**：ドアの説明を入力します。

> **情報**
>
> - ドアのIDと名前はシステム内で一意である必要があり、既に使用中の値は使用できません。
> - ドアのIDは一度保存すると変更できません。

3 入退室制御イベントの連携

AIドアイベント セクションの **ドアアクセスエリア** リストで、このドアの入退室判定に使用する入退室制御エリアを選択します。システムは、入退室制御イベントの作成時に設定した入退室制御エリアをリストに表示します。

> **情報**
>
> - 一つの入退室制御エリアは一つのドアにのみ接続できます。他のドアに既に連携されているエリアは選択できません。
> - ドアに連携した入退室制御エリアは、AIイベント画面で削除または変更できません。エリアを変更する前に、まずドアとの連携を解除してください。
> - 入退室制御イベントの作成の詳細は 入退室制御イベントを設定するを参照してください。

4 リレー設定

リレー選択セクションで、ドアのロック装置を制御するリレーを設定します。

- **ポート**：ドアのロック装置が接続されているリレーポートを選択します。必須項目です。カメラのリレーポートと下位I/Oデバイスのリレーポートを選択できます。他のドアまたはAIルールで使用中のポートは選択できません。
- **スイッチタイプ**：ロック装置の接点タイプを選択します。
  - **Normal Open**: 通常は開いており、リレーが動作すると閉じる接点です。
  - **Normal Close**: 通常は閉じており、リレーが動作すると開く接点です。

> **注意**
>
> - **スイッチタイプ**はドアではなく、リレーポートに適用する設定です。ドアを保存すると、そのポートを使用するすべてのドアとルールに適用されます。
> - 使用中のロック装置の仕様を確認し、正しい**スイッチタイプ**を選択します。誤って選択すると、通常時にドアが開いたままになる場合があります。

5 開放時間の設定

解錠時間セクションで、入退室が許可されたときにドアを開けておく時間を設定します。

- **解錠時間**：スライダーを動かすか、入力フィールドに値を直接入力してください。 1 秒から 120 秒まで設定でき、デフォルトは 3 秒です。
- **イベント終了まで解錠を維持**：このオプションを選択すると、解錠時間に関係なく、アクセス制御イベントが終了するまでドアを解錠したままにします。このオプションを使用するには、アクセス制御エリアを選択する必要があります。

> **情報**
> イベントの終了時点は、アクセス制御イベントの **条件** 設定によって異なります。例えば、未承認者が後に続いて入室したときにすぐドアを施錠するには、アクセス制御イベントで **エリアが無人になるかテールゲーティング違反時に解除** を選択してください。詳しくは、入退室制御イベントを設定するを参照してください。

6 退室ボタンの設定（任意）

ドアの内側に退室ボタンを設置した場合は、**退室ボタン** セクションでボタンが接続された入力ポートを設定してください。退室ボタンを押すと、顔認証を行わずにドアが開きます。

- **ポート**：退室ボタンが接続されている入力ポートを選択してください。
- **スイッチタイプ**：退室ボタンの接点タイプを選択してください。デフォルトは **Normal Open** です。
  - **Normal Open**: 通常は開いており、リレーが動作すると閉じる接点です。
  - **Normal Close**: 通常は閉じており、リレーが動作すると開く接点です。

7 ドア状態の設定（任意）

ドアに開閉センサーを設置した場合は、**ドア状態** セクションでセンサーが接続された入力ポートを設定してください。設定すると、**ドア制御** 画面でドアが開いているか閉じているかを確認できます。

- **ポート**：ドアの開閉センサーが接続された入力ポートを選択してください。
- **スイッチタイプ**：センサーの接点タイプを選択してください。デフォルトは **Normal Close** です。
  - **Normal Open**: 通常は開いており、リレーが動作すると閉じる接点です。
  - **Normal Close**: 通常は閉じており、リレーが動作すると開く接点です。

> **情報**
> - 退室ボタンとドア状態センサーは、別々の入力ポートに接続する必要があります。
> - 別のドアで使用中の入力ポートは選択できません。

8 スケジュールの設定（任意）

スケジュール セクションで、時間帯に応じてドアを解錠したままにするか、施錠したままにするかを設定できます。

- **解錠スケジュール**：選択したスケジュールの時間帯では、ドアを解錠したままにします。来訪者が多い業務時間にロビーのドアを解錠しておく場合に使用してください。

- **施錠スケジュール**：選択したスケジュールの時間帯では、ドアを施錠したままにします。この時間帯は登録済みユーザーでも入室できませんが、室内にいる人は退室ボタンを押して出入口ドアを開けて退出できます。

> **情報**
> 開放スケジュールと施錠スケジュールには同じスケジュールを選択できず、両スケジュールの時間帯が重なる場合は保存できません。

9 ドアの保存

すべての設定が完了したら、**保存** ボタンをクリックしてください。保存したドアはドア一覧に追加され、アクセスレベルとドアルールで選択できます。



ドア一覧の確認

ドア一覧で、登録済みのドアと各ドアに接続されたイベントとポートを確認できます。



- 特定のドアを探すには、検索フィールド(1)にドア名を入力します。
- 一ページあたりに表示するドアの数を変更するには、画面右上の行数リスト(2)から希望の値を選択してください。
- 並べ替え基準を変更するには、**ID順**(3)で基準を選択します。

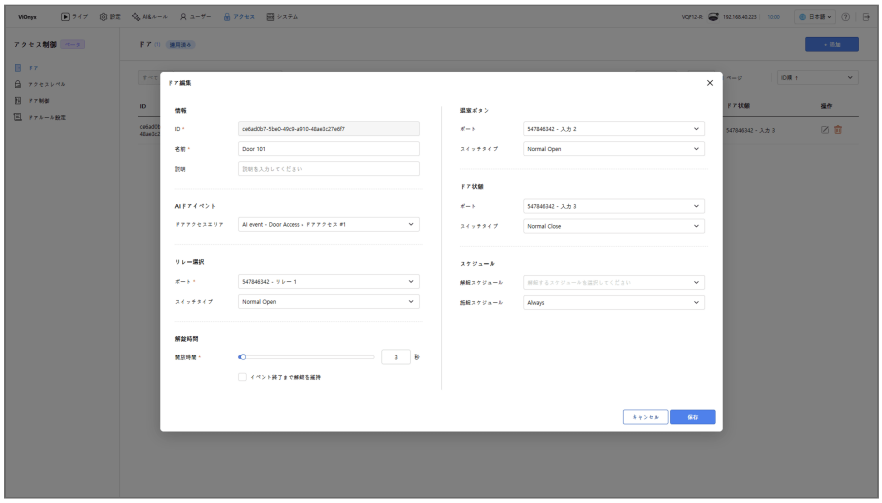
ドア一覧に表示される情報は次のとおりです。

項目	説明
ID	ドアの固有IDです。
名前	ドア名です。
説明	ドアを追加または編集するときに入力した説明です。
AIイベント	ドアに接続されたアクセス制御エリアです。
リレー	ドアの施錠装置を制御するリレーポートです。

項目	説明
退室ボタン	退室ボタンが接続された入力ポートです。
ドア状態	ドア開閉センサーが接続された入力ポートです。
操作	ドアを編集( )または削除( )する機能を提供します。

ドアの編集

1. ドア一覧で編集するドアの右側にあるボタンをクリックしてください。
2. **ドア編集** ポップアップが表示されたら、必要な項目を編集します。



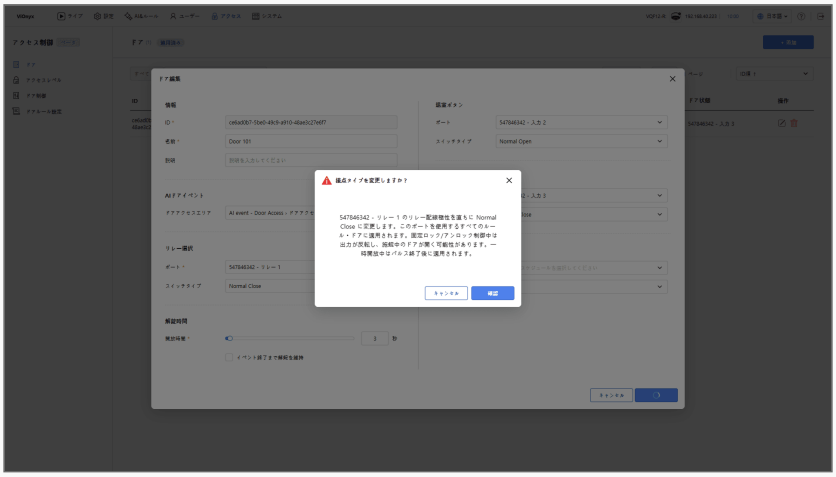
3. 編集内容を保存するには、**保存** ボタンをクリックしてください。

編集内容を保存すると、該当ドアを使用するアクセスレベルとドアルールに直ちに適用されます。

> **注意**
> ドアが手動施錠または手動解錠の状態でリレーの **スイッチタイプ**を変更すると、リレー出力が反転して施錠中のドアが開く場合があります。変更する前に **ドア制御** メニューで手動制御してください。

情報

リレーの **スイッチタイプ**を変更し、**保存** ボタンをクリックすると確認メッセージが表示されます。



- **確認** ボタンをクリックすると確認メッセージが閉じ、変更した接点タイプがリレーポートに直ちに適用されます。該当ポートを使用するすべてのドアとルールにも適用されます。
- **キャンセル** ボタンをクリックすると接点タイプは変更されず、一緒に編集した他の項目のみ保存されます。
- ドアが一時的に開いている間に変更すると、開放時間の終了後に適用されます。

ドアの削除

1. ドア一覧で削除するドアの一番右にある ボタンをクリックしてください。
2. 確認メッセージが表示されたら内容を確認し、**確認** ボタンをクリックしてください。

ドアを削除すると、接続されたアクセス制御イベントとアクセスレベルのリンクが解除されます。削除したドアは **ドア制御** 一覧からも消え、復元できません。

情報

- アクセスレベルやドアルールで使用中のドアを削除すると、アクセスレベルとドアルールも削除されます。
- ドアを追加、修正、削除するには **読み書き** 権限が必要です。権限がない場合は管理者にお問い合わせください。オペレーター権限の詳細については オペレーターの管理 をご覧ください。

次のステップ

ドアを登録したら、アクセスレベルを作成し、どのユーザーがいつ入退室できるかを指定してください。

出入レベルの管理性行する

アクセスレベルは、**どのユーザー**が**どのドア**に**いつ**入退室できるかをまとめたアクセス権限です。アクセス制御イベントで顔認証により識別されたユーザーでも、そのドアのアクセスレベルに割り当てられていない、またはアクセス時間外の場合、入退室でき

ません。

次のような場合にアクセスレベルを作成してください。

- 特定の部署やチームメンバーだけがドアに入退室できるようにする場合
- 平日の業務時間のみ許可するなど、ユーザーグループごとに入退室時間を変える場合
- 夜間勤務者など、特定の時間帯のみ入退室するユーザーに別の権限を付与する場合

開始する前に

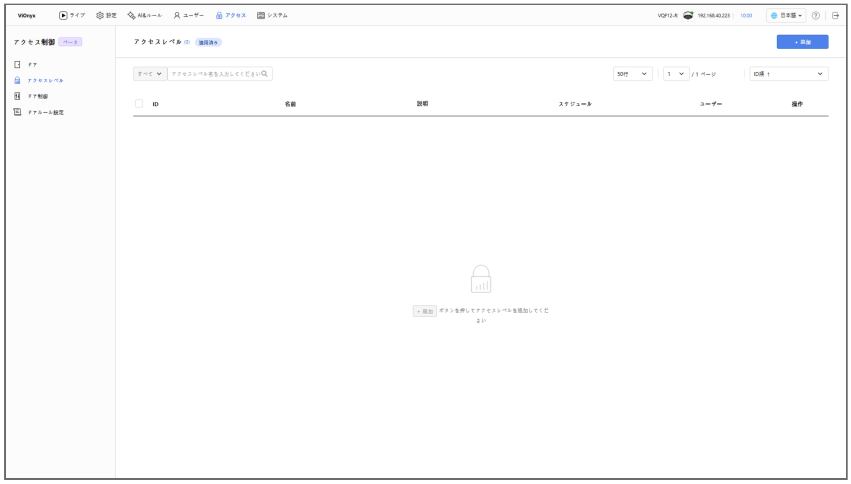
アクセスレベルを作成する前に、次を確認してください。

- アクセスレベルに指定するドアを先に登録してください。詳しくは、ドア管理を参照してください。
- アクセスレベルに割り当てるユーザーを顔ユーザーとして登録してください。詳しくは、ユーザーの追加を参照してください。
- 入退室時間を制限する場合は、スケジュールを事前に作成してください。スケジュールを作成しない場合は、既定のAlwaysスケジュールを使用できます。詳しくは、スケジュール管理を参照してください。

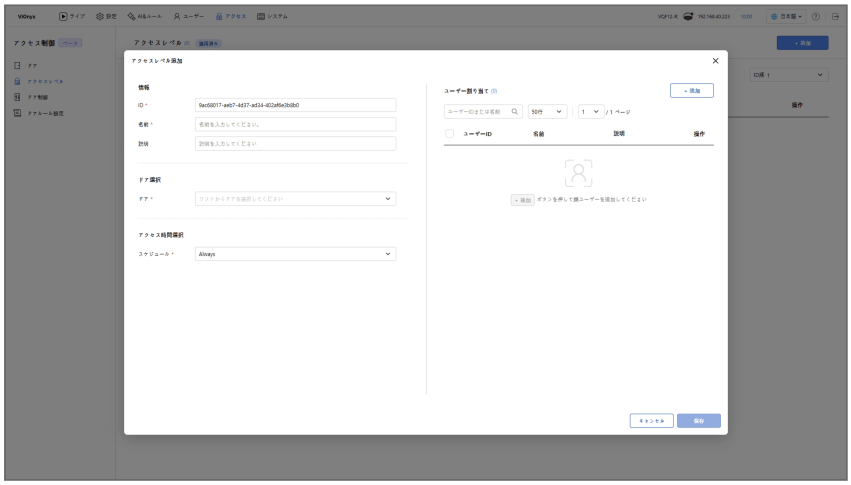
アクセスレベルの追加

1 アクセスレベルの追加を開始

1. 画面左上の **アクセス** メニューをクリックします。
2. 画面左のサイドバーで **アクセスレベル** をクリックします。



3. 画面右上の**+ 追加**ボタンをクリックしてください。
4. **アクセスレベル追加** ポップアップが表示されたら、アクセスレベル情報を入力し、ユーザーを割り当ててください。



❷ 基本情報入力

情報 セクションで、アクセスレベルを識別する情報を入力してください。

- **ID**：アクセスレベルの固有IDです。自動で入力されます。必要に応じて変更できます。他のアクセスレベルと同じIDは使用できません。最大64文字まで入力できます。英数字、ハイフン（-）、アンダースコア（_）を使用できます。
- **名前**：アクセスレベル名を入力します。必須です。他のアクセスレベルと同じ名前は使用できません。**開発チーム 常時入退室、夜間勤務者**のように、対象と時間が分かる名前にしてください。
- **説明**：アクセスレベルの説明を入力します。

❸ 出入口の選択

ドア選択 セクションの **ドア** 一覧で、入退室を許可する出入口を選択します。必須項目です。 1つ以上のドアを選択できます。

> **情報**
> 登録済みの出入口がない場合、一覧で出入口を選択できません。 **アクセス** → **ドア** で、出入口を先に登録してください。出入口の登録の詳細については、ドア管理を参照してください。

❹ アクセス時間の選択

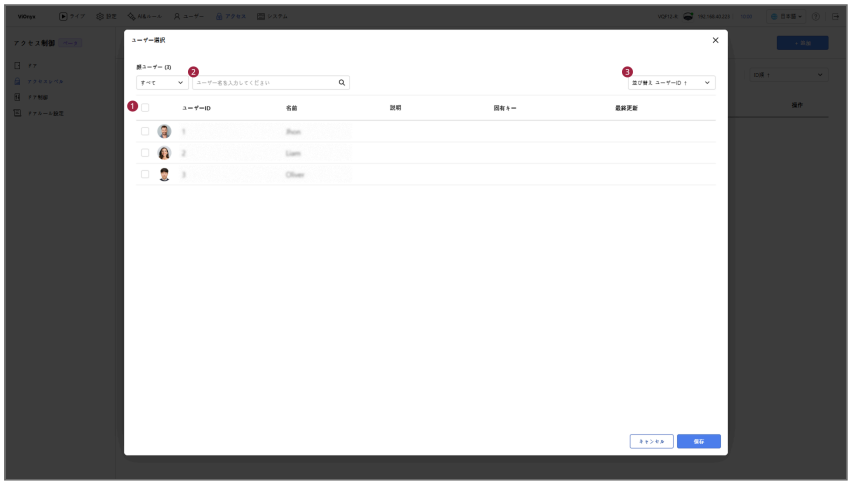
アクセス時間選択 セクションの **スケジュール** 一覧で、入退室を許可するスケジュールを選択します。必須項目で、既定値は **Always** です。選択したスケジュールの時間帯のみ入退室を許可します。その他の時間帯は、登録済みユーザーでも入退室を拒否します。

> **情報**
> スケジュール管理の詳細は、スケジュール管理をご参照ください。

5 ユーザーの割り当て

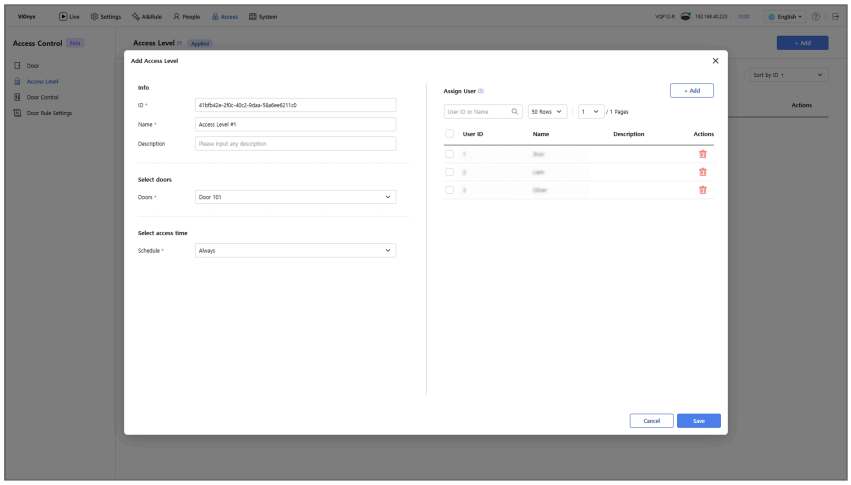
ユーザー割り当て セクションで、アクセスレベルを適用するユーザーを追加してください。

1. **ユーザー割り当て** セクション右上の **+ 追加** ボタンをクリックします。
2. **ユーザー選択** ポップアップが表示されたら、割り当てるユーザーのチェックボックスをクリックします。



- 一覧のすべてのユーザーを選択するには、一覧ヘッダーのチェックボックス(1)を選択します。
- 特定のユーザーを検索するには、検索フィールド(2)にユーザー名を入力します。
- 並べ替え基準を変更するには、並べ替えリスト(3)で目的の基準を選択します。

3. **保存** ボタンをクリックしてください。選択したユーザーが **ユーザー割り当て** 一覧に追加されます。

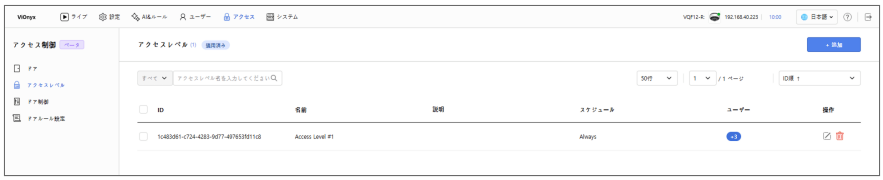


割り当てたユーザーをアクセスレベルから除外するには、**ユーザー割り当て** 一覧で該当ユーザーの  ボタンをクリックします。

> **情報**
>
> - **ユーザー選択** 一覧には、顔ユーザーとして登録されたユーザーのみが表示されます。
> - 一人のユーザーは複数のアクセスレベルに割り当てできます。ユーザーごとに割り当てできるアクセスレベル数には制限があります。

6 アクセスレベルの保存

すべての設定が完了したら、**保存** ボタンをクリックしてください。保存したアクセスレベルはアクセスレベル一覧に追加され、割り当てたユーザーにすぐ適用されます。



アクセスレベル一覧の確認

アクセスレベル一覧で、登録済みのアクセスレベル、各アクセスレベルのアクセス時間、割り当てられたユーザーを確認できます。



- 特定のアクセスレベルを探すには、検索フィールド(1)にアクセスレベル名を入力してください。
- 一ページに表示するアクセスレベル数を変更するには、画面右上の行数リスト(2)で希望の値を選択してください。
- 並べ替え基準を変更するには、**ID順**(3)で基準を選択します。

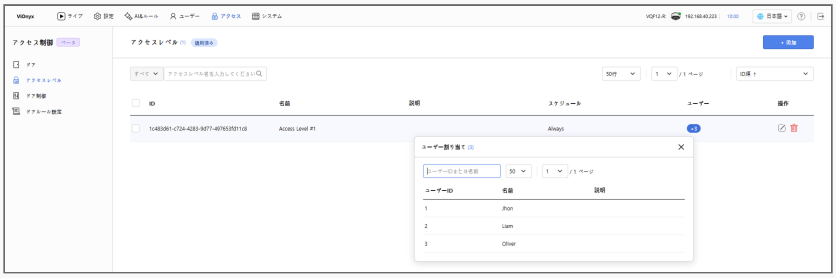
アクセスレベル一覧に表示される項目は次のとおりです。

項目	説明
ID	アクセスレベルの固有IDです。
名前	アクセスレベル名です。
説明	アクセスレベルを追加または編集するときに入力した説明です。
スケジュール	アクセスを許可するスケジュールです。
ユーザー	アクセスレベルに割り当てたユーザー数です。

項目	説明
操作	アクセスレベルを編集( )または削除( )できます。

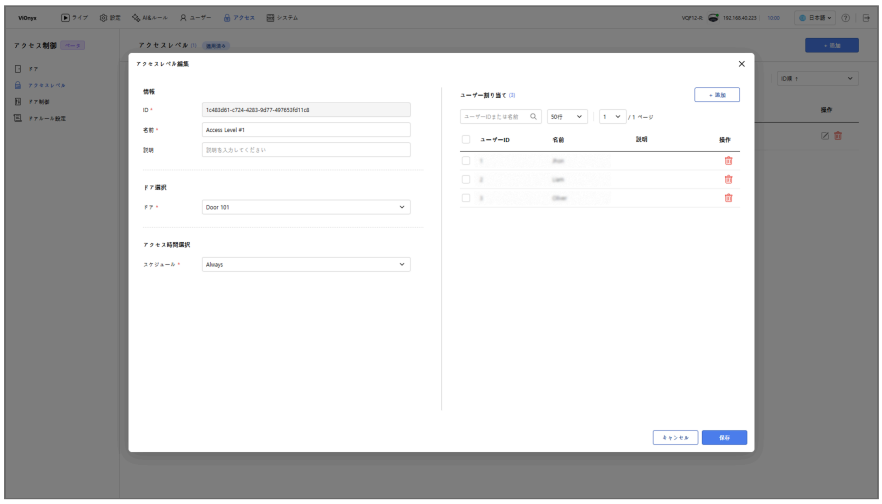
情報

ユーザー項目の数字をクリックすると、割り当てられたユーザー一覧を確認できます。



アクセスレベルの編集

1. アクセスレベル一覧で、編集するアクセスレベルの右側にあるボタンをクリックしてください。
2. **アクセスレベル編集** ポップアップが表示されたら、ドア、アクセス時間、割り当てられたユーザーなどを編集してください。



3. 編集内容を保存するには、**保存** ボタンをクリックしてください。

編集内容は保存するとすぐに、割り当てたすべてのユーザーに適用します。

アクセスレベルの削除

アクセスレベルは一件ずつ削除するか、複数を選択して一度に削除できます。

- **一件ずつ削除:** アクセスレベル一覧で、削除したいアクセスレベルの右側にある ボタンをクリックしてください。
- **複数削除:** アクセスレベル一覧で、削除するアクセスレベルのチェックボックスを選択し、画面右上の **削除** ボタンをクリックしてください。



確認メッセージが表示されたら内容を確認し、**確認** ボタンをクリックしてください。アクセスレベルを削除すると、割り当てたすべてのユーザーから該当のアクセスレベルを解除します。ドアとユーザーは削除しません。削除したアクセスレベルは復元できません。

> **注意**
> アクセスレベルを削除すると、そのアクセスレベルでのみ出入していたユーザーは、以後ドアを出入できません。削除する前に割り当てられているユーザーを確認してください。

次のステップ

アクセス判定結果に応じて、音声案内、Webhook通知、非常灯などの追加動作を実行するには、ドアのルールを設定してください。

出入ドアを制御する

ドア制御 メニューでは、登録されたドアの施錠状態をリアルタイムで確認し、遠隔でドアを開けたり施錠したりできます。

次のような状況では、ドアを直接制御してください。

- 顔が登録されていない来訪者や配送員のために、ドアを一度だけ開けるとき
- イベントや引っ越しなどで、ドアを開けたままにするとき
- 緊急時に、スケジュールに関係なくドアを直ちに施錠する必要があるとき

> **情報**
> - ドアを制御するにはオペレーター権限が必要です。権限がない場合、ドアの状態確認と制御機能を使用できません。オペレーター権限の詳細については オペレーターの管理 をご覧ください。
> - ドアの追加および管理の詳細については ドア管理 をご覧ください。

ドア状態の確認

1. 画面左上の **アクセス** メニューをクリックします。
2. 画面左のサイドバーで **ドア制御** をクリックします。



ドア メニューに登録したドアを一覧に表示します。ドアを追加または削除すると、一覧にもすぐ反映します。

- 特定のドアを探すには、検索フィールド(1)にドア名を入力します。
- 一ページあたりに表示するドアの数を変更するには、画面右上の行数リスト(2)から希望の値を選択してください。
- 並べ替え基準を変更するには、**ID順**(3)で基準を選択します。

ドア一覧に表示される情報は次のとおりです。

項目	説明
ID	ドアの固有IDです。
名前	ドア名です。
説明	ドアを追加または編集するときに入力した説明です。
リレー状態	ドアのロック装置の現在の状態です。
ドアセンサー	ドアセンサーの現在の状態です。ドアに **ドア状態** 入力ポートを設定した場合のみ表示します。
制御	ドアを開けたり、手動で施錠または解錠したりする機能を提供します。

リレー状態

リレー状態 列は、ドアが施錠されているかに加え、その状態を決定した要因を表示します。

状態	説明
施錠	通常は施錠状態です。
解錠	通常は解錠状態です。
スケジュール施錠	ドアは施錠スケジュールに従って施錠した状態です。
スケジュール解錠	ドアは開放スケジュールに従って解錠した状態です。
固定施錠	**手動ロック**で施錠した状態です。
固定解錠	**手動アンロック**で解錠した状態です。

ドア制御

制御 列のボタンをクリックして、ドアを制御してください。

ボタン	動作
ドアを開く	ドアを一度開けます。ドアに設定した開放時間が経過すると、ドアは自動的に施錠します。
手動アンロック	ドアを解錠し、**解除** 機能を実行するまで開放したままにします。
手動ロック	ドアを施錠し、**解除** 機能を実行するまで施錠したままにします。この時間帯は、登録済みのユーザーも入退室できず、退室ボタンも動作しません。
解除	**手動ロック** または **手動アンロック**を終了し、ドアを手動制御前の状態に戻します。

注意

- **手動アンロック** 状態では、顔認証に関係なく誰でも入退室できます。必要な作業が終わったら、必ず **解除** ボタンをクリックしてください。
- **手動ロック**状態では、室内にいる人は退室ボタンで退出できません。**手動ロック**を実行する前に、室内に人が残っていないことを確認してください。

情報

- ドアが手動施錠または手動解錠状態の場合、**ドアを開く** ボタンを無効にし、**解除** ボタンのみを表示します。



- 手動制御は、ドアの開放スケジュールと施錠スケジュールより優先します。例えば、開放スケジュールの時間帯に**手動ロック**を実行すると、ドアは施錠状態を維持します。
- **解除** ボタンをクリックすると、現在時刻に合ったスケジュール状態、または通常状態に戻ります。

出入口ルールの設定

出入口ルールを使用すると、出入口で発生した入退室判定結果に応じて、オーディオ再生、Webhook送信、リレー動作を自動で実行できます。入退室が許可されると、出入口は出入口設定に従って自動で開くため、出入口ルールでは開扉以外の追加動作を設定します。

次のような場合に出入口ルールを設定してください。

- 入退室が許可されたら歓迎音声を、拒否されたら案内音声を再生する場合
- 未認可の人が後から入室したら、非常灯や警告音を作動させる場合
- 入退室記録を外部の入退室制御システムまたは管制サーバーに送信する場合

開始する前に

出入口ルールを設定する前に、以下を確認してください。

- ルールを適用する出入口を先に登録してください。詳しくは、ドア管理を参照してください。
- オーディオを使用するには、再生するオーディオクリップを事前にアップロードしてください。詳細は オーディオクリップのアップロード を参照してください。
- Webhookを使用するには、受信するサーバーのURLを事前に用意してください。
- リレーを使用するには、非常灯、警告音など、動作させる装置がリレーポートに接続されていることを確認してください。外部装置の接続に関する詳細は、ViOnyx インストールガイドを参照してください。

入退室判定結果

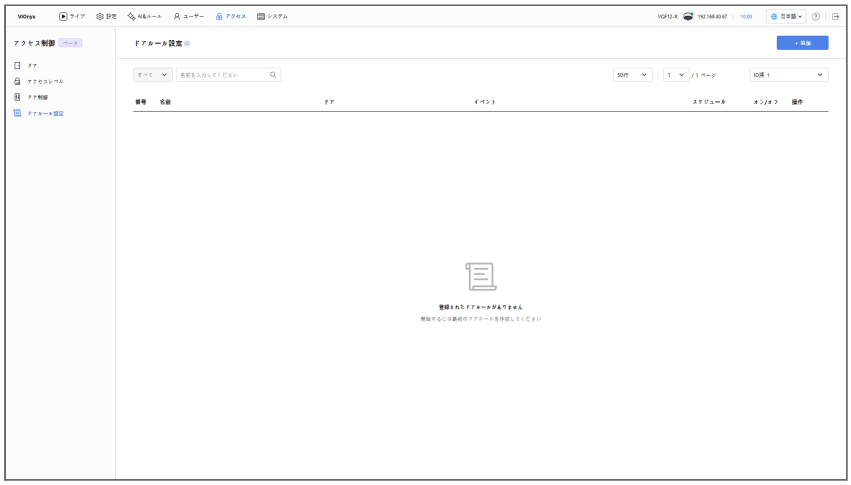
出入口ルールでは、次の入退室判定結果ごとに実行する動作を個別に設定できます。

入退室判定結果	発生条件
入退室許可	入退室レベルがあるユーザーを入退室時間内に識別し、入退室を許可しました。
未識別による入退室拒否	入退室制御エリアに入った人を顔認証で識別できなかった、または未登録の人です。
アクセスレベルによる入退室拒否	登録済みユーザーとして識別しましたが、当該出入口の入退室レベルがない、または入退室時間外です。
ドアモードによる入退室拒否（手動/スケジュールロック）	出入口が手動ロック状態、またはロックスケジュール時間帯のため、入退室を拒否しました。
アンチテールゲーティングによる入退室拒否	検証エリアの人数が入退室制御イベントのテイルゲーティングオプション条件を満たさず、入退室を拒否しました。
認証者の通過（ドアライン）	入退室が許可されたユーザーがイベント進入ラインを通過し、実際に入退室しました。
拒否後の通過（セキュリティイベント）	入退室が拒否された人がイベント進入ラインを通過し、入退室しました。強制入退室が疑われるセキュリティイベントです。

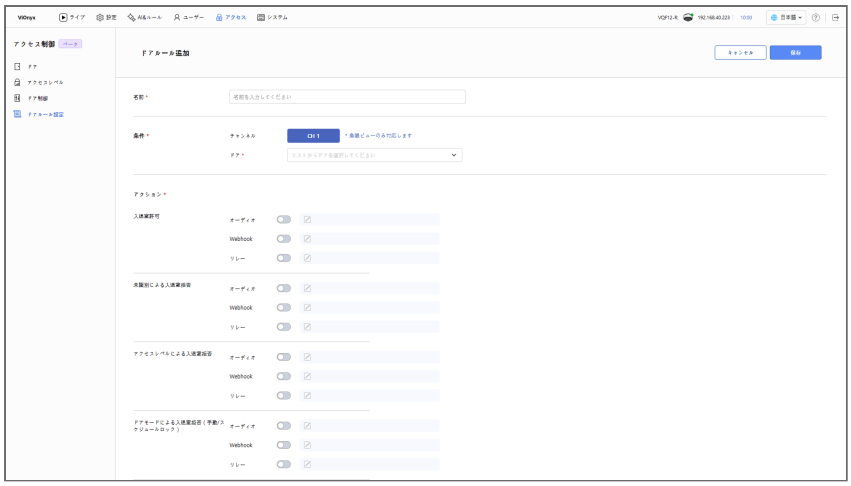
ドアルールの追加

1 ルール追加を開始

1. 画面左上の **アクセス** メニューをクリックします。
2. 画面左のサイドバーで **ドアルール設定** をクリックします。



3. 画面右上の**+ 追加**ボタンをクリックしてください。
4. **ドアルールを追加** 画面が表示されたら、ルール名を入力し、条件と動作を設定します。



❷ ルール名の入力

名前 入力フィールドにルール名を入力します。必須項目です。

❸ 条件の設定

条件セクションで、ルールを適用するドアを選択します。

- **チャンネル**：チャンネルはCH 1に固定されています。フィッシュアイビューのみサポートします。
- **ドア**：ルールを適用するドアを選択します。必須項目です。

❹ 動作設定

アクションセクションでは、入退室判定結果ごとに **オーディオ**、**Webhook**、**リレー** の動作を表示します。動作を実行する入退室判定結果で、目的の動作のトグルをクリックして有効にし、 ボタンをクリックします。動作別の設定ポップアップが開きます。

少なくとも1つの動作を有効にしないと、ルールを保存できません。動作別の設定方法は、以下を参照してください。

> **情報**
> 動作別スケジュールの時間帯でない場合、入退室判定結果が発生してもその動作は実行されません。スケジュールは **AI&ルール** → **スケジュール** で管理できます。詳しくは、スケジュール管理を参照してください。

5 オーディオ動作の設定

入退室判定結果が発生すると、カメラでオーディオクリップを再生します。



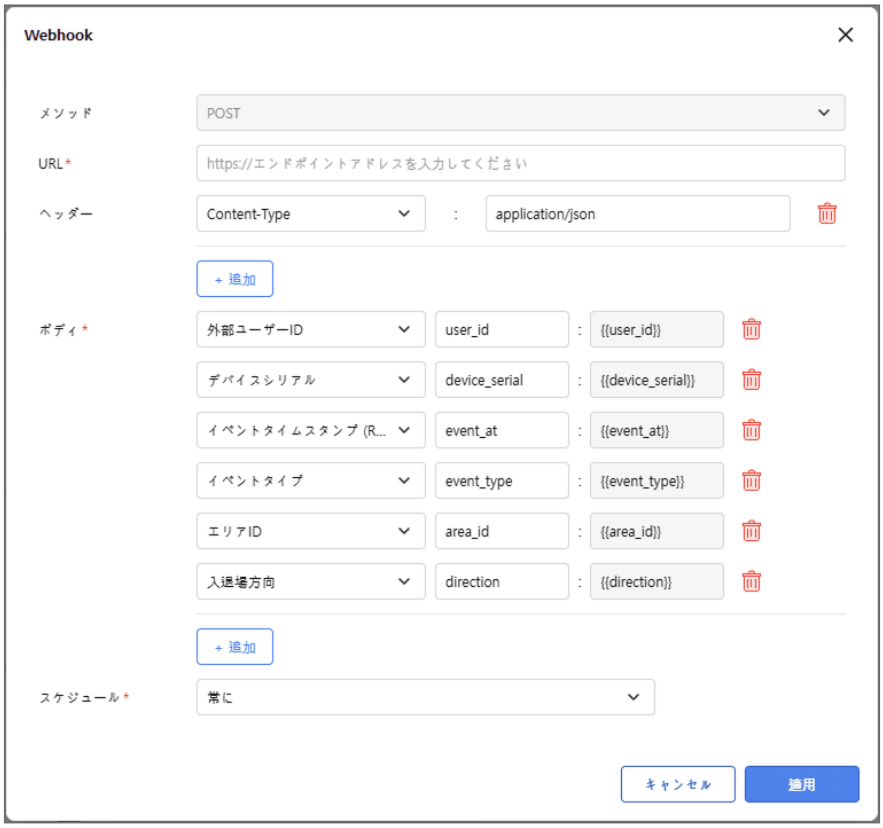
- **オーディオクリップ**：再生するオーディオクリップを選択します。必須項目です。
- **繰り返し**：オーディオクリップを繰り返し再生する回数を選択します。
- **スケジュール**：オーディオを再生するスケジュールを選択します。必須項目で、デフォルト値は **常に** です。

オーディオ動作の設定を保存するには、**適用** ボタンをクリックします。

> **情報**
> オーディオ動作を設定する前に、オーディオクリップを事前に用意してください。オーディオクリップは **システム** → **オーディオ** メニューでアップロードできます。詳細は オーディオクリップのアップロード を参照してください。

6 Webhook 動作の設定

入退室判定結果が発生すると、外部サーバーにWebhookを送信します。



- **メソッド**：Webhook の送信方式です。 POST 方式のみサポートします。
- **URL**：Webhookを受信するURLを入力します。必須項目です。
- **ヘッダー**：Webhook に含めるHTTPヘッダーを設定します。デフォルトで Content-Type: application/json ヘッダーが追加されています。 **+ 追加** ボタンをクリックしてヘッダーを追加できます。同じヘッダー名は重複して使用できません。システムで予約されたヘッダー名も使用できません。
- **ボディ**: Webhook 本文に含める項目を設定してください。必須項目です。各行の左側のリストで送信する情報を選択し、中央のフィールドに JSON キー名を入力してください。右側のフィールドには、イベント発生時に実際の値に置き換わる変数が表示されます。 **+ 追加** ボタンをクリックしてユーザー定義項目を追加します。削除するには、 ボタンをクリックします。本文のサイズは最大64キロバイトです。
- **スケジュール**: Webhook を送信するスケジュールを選択してください。必須項目で、デフォルト値は **常に** です。

設定を保存するには、**適用** をクリックします。

> **情報**
>
> - セキュリティのため、システムは保存後にヘッダーと本文の入力値を画面に再表示しません。ルールを編集しても保存済みの値は保持されます。新しく入力すると既存の値を置き換えます。
> - システムログで Webhook の送信結果を確認できます。詳しくは、システムログの確認を参照してください。

7 リレー動作の設定

入退室判定結果が発生すると、選択したリレーを動作させます。非常灯、警報音、補助ロック装置などを連動させるときに使用してください。



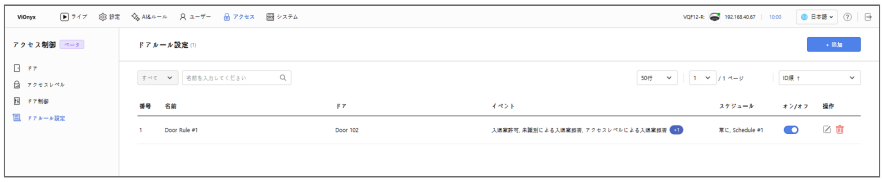
- **ポート**: 動作させるリレーポートを選択してください。必須項目です。ドアロック装置として使用中のリレーポートは選択できません。
- **開放時間**: リレーを動作状態に保持する時間を設定してください。スライダーを動かすか、入力フィールドに値を直接入力できます。 1 秒から 120 秒まで設定でき、デフォルトは 3 秒です。
  - **イベント終了まで維持**: このオプションを選択すると、開放時間に関係なく入退室管理イベントが終了するまでリレーを動作状態に保持します。
- **接点タイプ**: リレーの接点タイプを選択してください。必須項目で、ポートを選択すると設定できます。
  - **Normal Open**: 通常は開いており、リレーが動作すると閉じる接点です。
  - **Normal Close**: 通常は閉じており、リレーが動作すると開く接点です。
- **スケジュール**：リレーを動作させるスケジュールを選択します。必須項目で、デフォルト値は **常に** です。

設定を保存するには、**適用** をクリックします。

> **注意**
> **接点タイプ**はルールではなく、リレーポートに適用する設定です。**接点タイプ**を変更すると、システムが確認メッセージを表示します。**確認** ボタンをクリックすると、該当ポートを使用するすべてのルールとドアに即時適用します。ポートが手動施錠または手動解錠の状態で変更すると、出力が反転し、施錠中のドアが開くことがあります。注意してください。

8 ルールを保存

すべての設定が完了したら、画面右上の **保存** ボタンをクリックします。保存したルールをドアルール一覧に追加し、すぐに適用します。



> **情報**
> ドアルールは最大 20 件まで作成できます。

ドアルール一覧の確認

ドアルール一覧で、登録済みルールと各ルールの適用先を確認できます。



- 特定のドアルールを探すには、検索フィールド(1)にドアルール名を入力します。
- ページあたりに表示するドアルール数を変更するには、画面右上の行数リスト(2)で希望の値を選択してください。
- 並べ替え基準を変更するには、**ID順**(3)で基準を選択します。

ドアルール一覧に表示される項目は次のとおりです。

項目	説明
番号	ルール番号です。
名前	ルール名です。
ドア	ルールを適用するドアです。
イベント	有効な動作が一つ以上ある入退室判定結果です。結果が複数ある場合は、一部のみ表示されます。
スケジュール	ルールに適用したスケジュールです。
オン/オフ	ルールをオンまたはオフに切り替えます。
操作	ルールを編集( )または削除( )する機能です。

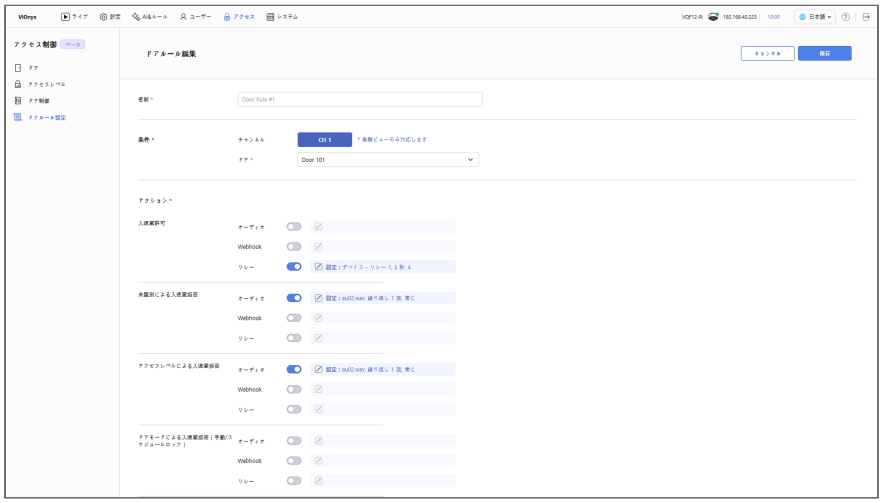
ドアルールの有効化/無効化

ドアルール一覧で **オン/オフ** 列のトグルボタンをクリックして、該当ルールを有効または無効に切り替えます。無効にしたルールは、入退室判定結果が発生しても動作を実行しません。ルールを削除せずに一時停止するときに使用します。



ドアルールの編集

1. 出入口ドアルール一覧で編集するルールの右側にある ボタンをクリックしてください。
2. **ドアルールを編集** 画面が表示されたら、条件と動作を編集してください。



3. 編集した内容を保存するには、画面右上の **保存** ボタンをクリックします。

出入口ドアルールの削除

出入口ドアルール一覧で削除するルールの右側にある ボタンをクリックしてください。確認メッセージが表示されたら **確認** ボタンをクリックします。削除したルールは復元できません。

システム構成

カメラシステムを効果的に管理するために、デバイス情報、ファームウェア、メンテナンス、アカウント、オーディオ、ログを体系的に管理できます。安定かつ安全なカメラ運用のため、各項目を定期的に確認し、更新してください。

カメラ情報の更新

カメラの基本情報を確認し、デバイス名、説明、設置場所情報を入力して組織内の複数台のカメラを効率的に管理できます。

以下の状況でカメラ情報を更新してください。

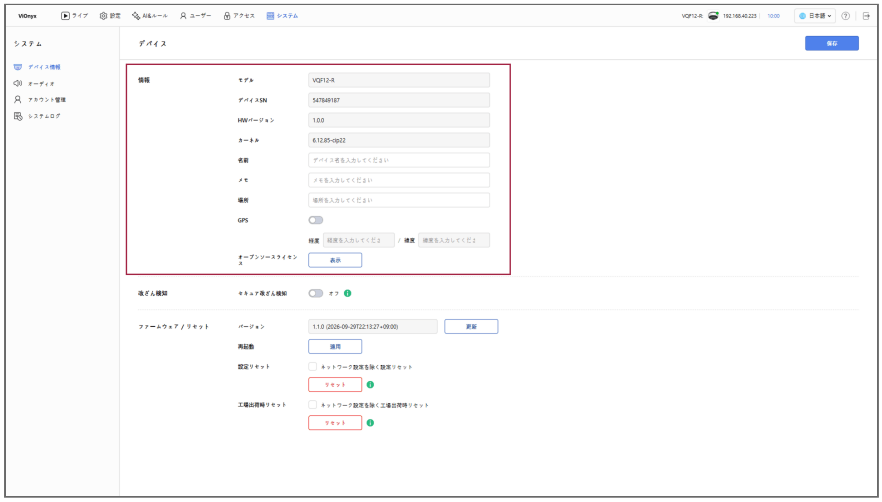
- 設置したカメラの名前を組織内で識別しやすい名称に変更する場合
- カメラの位置や設置場所に関する追加情報を入力する場合
- GPS座標を入力してカメラの正確な位置を記録する場合
- 複数台のカメラを管理する際に、各カメラに特定のメモや説明を追加する場合

> **情報**
>
> - モデル名、シリアル番号、ハードウェアバージョンなどは読み取り専用で編集できません。
> - カメラ名、メモ、位置情報はUnicodeをサポートしており、ハングル、英字、数字、特殊文字を入力できます。

カメラの基本情報を確認

カメラのモデル名、シリアル番号、ハードウェアバージョンなどの基本情報を確認してください。

1. 画面左上の **システム** メニューをクリックします。
2. 画面左のサイドバーで **デバイス情報** をクリックします。



情報 セクションで以下の基本情報を確認できます。読み取り専用で編集できません。

- **モデル**: カメラのモデル名

- **デバイスSN**: カメラのシリアル番号
- **HWバージョン**: ハードウェアバージョン
- **カーネル**: カーネルバージョン
- **オープンソースライセンス**: オープンソースライセンス情報を確認するには、**表示** ボタンをクリックしてください。

カメラ情報の設定

カメラ名、メモ、位置情報を入力して効率的に管理してください。

1. 画面左上の **システム** メニューをクリックします。
2. 画面左のサイドバーで **デバイス情報** をクリックします。

名前の入力

カメラを識別しやすい名前を入力してください。 **名前** 入力フィールドにカメラ名を入力します。

- 最大64文字まで入力できます。
- ハングル、英字、数字、特殊文字（`.`, `-`, `(`, `)`）を含めることができます。

> *例: "入口-1", "会議室-A" など*

> **情報**
> 入力したカメラ名はシステムメニューやWeb UIの複数箇所に表示され、カメラを簡単に識別できます。

メモの追加

カメラに関する追加情報やメモを入力します。 **メモ** 入力フィールドにメモまたは説明を入力します。最大64文字まで入力できます。

> *例: 設置部署、管理者名、設置日など*

位置情報の入力

カメラの設置場所をテキストで入力します。 **場所** 入力フィールドにカメラの設置場所を入力します。最大64文字まで入力できます。

> *例: '1階ロビー入口'、'2階会議室待合室'*

設定を保存

すべての情報を入力したら、画面右上の **保存** ボタンをクリックします。

GPS座標の設定

カメラの正確な地理的位置をGPS座標で入力します。

1. 画面左上の **システム** メニューをクリックします。

2. 画面左のサイドバーで **デバイス情報** をクリックします。
3. GPS設定を有効にするには、**情報** セクションの **GPS** トグルボタンをクリックします。



4. 経度と緯度の情報を入力します。

   > *例: ソウル (37.5665, 126.9780)*

5. 設定を保存するには、画面右上の **保存** ボタンをクリックします。

> **情報**
>
> - GPS座標は10進法（Decimal Degrees, DD）形式で入力する必要があります。
> - GPS設定を無効にするには、**GPS** トグルボタンをもう一度クリックします。

ファームウェアの更新

この機能でカメラのファームウェアを最新バージョンに更新できます。ファームウェア更新で新機能、性能向上、セキュリティパッチを適用できます。

以下の場合はファームウェアを更新してください。

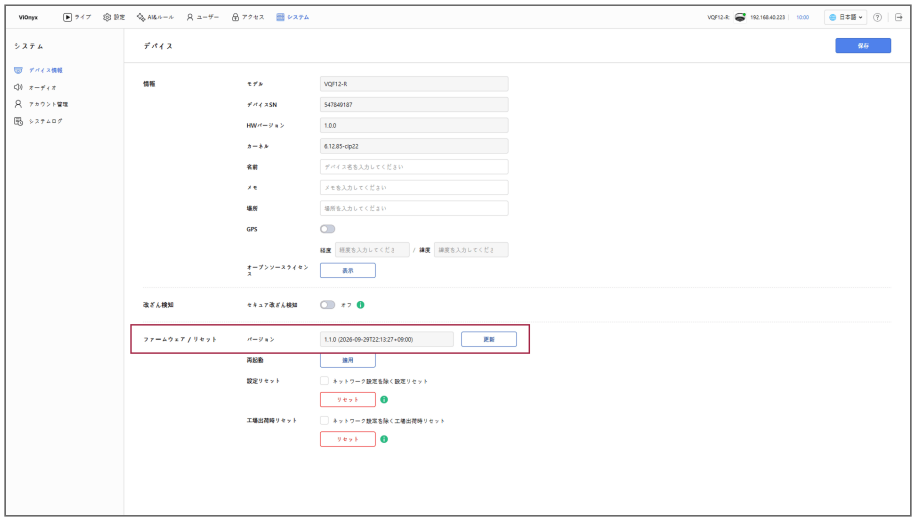
- 新機能を利用する場合
- セキュリティパッチを適用してカメラを保護する場合
- カメラの性能を改善する場合
- 技術サポートが推奨するファームウェアバージョンがある場合

> **情報**
>
> - ファームウェア更新中はカメラが再起動し、この間カメラは使用できません。
> - ファームウェア更新を開始する前に、機器に十分な電源が供給されていることを確認してください。
> - シュプリマ技術サポートが提供する公式のファームウェアファイル(`.bin`)のみを使用してください。

現在のファームウェアバージョンの確認

カメラにインストールされている現在のファームウェアバージョンを確認してください。

1. 画面左上の **システム** メニューをクリックします。
2. 画面左のサイドバーで **デバイス情報** をクリックします。

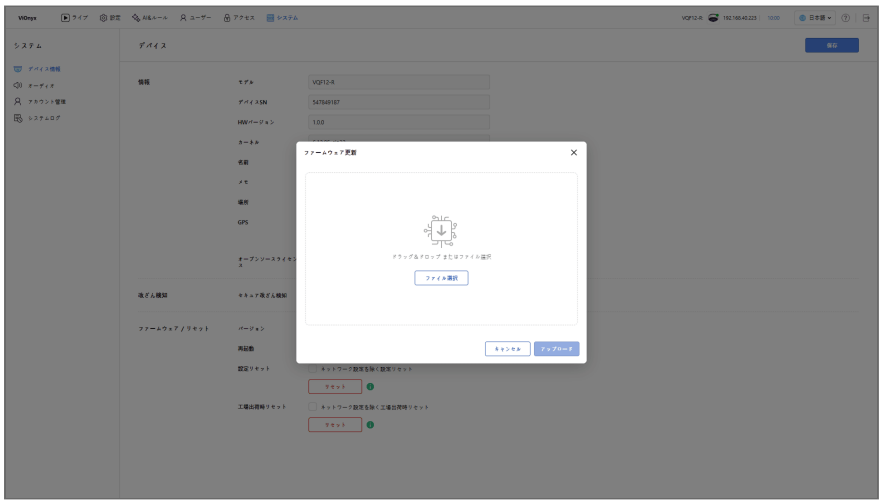


ファームウェア / リセット セクションの **バージョン** で、現在インストールされているファームウェアバージョンを確認できます。

ファームウェアのアップデート

新しいファームウェアファイルを選択して機器を更新してください。

1. 画面左上の **システム** メニューをクリックします。
2. 画面左のサイドバーで **デバイス情報** をクリックします。
3. **ファームウェア / リセット** セクションで **更新** ボタンをクリックしてください。
4. **ファームウェア更新** ポップアップが表示されたら、シュプリマが提供するファームウェアファイル(`.bin` ファイル)を選択してください。



- ファイル拡張子は必ず `.bin` にしてください。
- アップロード領域にファイルをドラッグするか、**ファイル選択** ボタンをクリックしてファイルを選択できます。

5. ファイルを選択すると **アップロード** ボタンが有効になります。
6. ファームウェア更新を進めるには **アップロード** ボタンをクリックしてください。
7. アップロードが完了すると再起動確認のポップアップが表示されます。 **確認** ボタンをクリックしてカメラを再起動し、ファームウェア更新を完了してください。

- カメラが再起動した後、Web UI に再度接続してください。新しいファームウェアバージョンを確認するには、**デバイス情報** に移動してください。
- ファームウェア更新が開始された後はキャンセルできません。更新が完了するまで待ってください。

カメラの保守

カメラを再起動または設定を初期化して、カメラを効果的に管理できます。再起動、設定初期化、工場出荷時リセットの3つの方法を説明します。

次のような状況でカメラの保守機能を使用してください。

- 管理者以外の外部者がカメラのカバーを取り外そうとしたときに、カメラが正常に動作しないようにセキュリティ対策を行いたいとき
- ネットワーク設定を変更した後、新しい設定を適用する場合
- カメラの応答が遅くなる、またはパフォーマンスが低下した場合
- システムが正常に動作しない場合
- カメラの設定をすべてデフォルトに戻す場合
- カメラを他のユーザーに引き継ぐ前に、すべての情報を削除する場合
- システムに問題が発生し、工場出荷時の状態に戻す必要がある場合

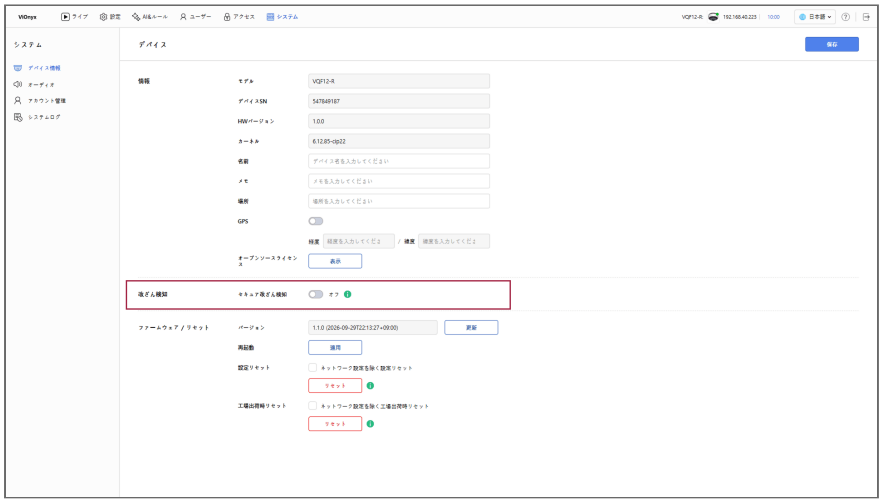
警告

- 再起動または初期化中にカメラの電源を切らないでください。
- **工場出荷時リセット**は、すべてのユーザーデータ、イベント記録、ログを永久に削除します。復元できないため、十分に注意して実行してください。
- 初期化する前に必要なデータをバックアップしてください。

改ざん検知

カメラの**改ざん検知**機能を有効にすると、管理者以外の外部者がカメラのカバーを取り外そうとしたときに、カメラの証明書とキーを削除して、カメラが正常に動作しないようにできます。

1. 画面左上の **システム** メニューをクリックします。
2. 画面左のサイドバーで **デバイス情報** をクリックします。
3. **改ざん検知**セクションのトグルボタンをクリックして、機能を有効にします。



4. 警告メッセージが表示されたら、**確認** ボタンをクリックしてください。

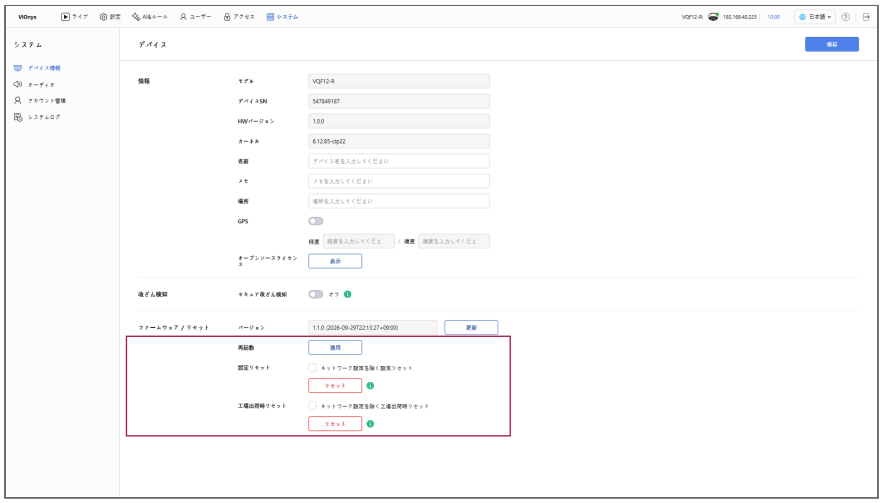
この機能では、**保存**ボタンをクリックしなくても変更内容が自動保存されます。

> **注意**
>
> **改ざん検知**機能を有効にした状態で、管理者がメンテナンスのためにカメラのカバーを取り外す必要がある場合は、**改ざん検知**機能を一時的に無効にしてから作業を進めます。作業完了後は、再度有効にしてセキュリティを維持します。

カメラの再起動

カメラを再起動して、設定の変更を適用するかシステムのパフォーマンスを回復します。再起動は、現在の設定を保持したままシステムを再初期化する方法です。

1. 画面左上の **システム** メニューをクリックします。
2. 画面左のサイドバーで **デバイス情報** をクリックします。
3. **ファームウェア / リセット** セクションの **再起動** で **適用** ボタンをクリックします。



4. 再起動確認のポップアップが表示されたら、**確認** ボタンをクリックします。

情報

- 再起動中はカメラを一時的に使用できません。再起動には最低1〜2分かかります。
- 再起動中にカメラの電源を切らないでください。システムが損傷する可能性があります。
- 再起動後にカメラのIPアドレスが変更された場合、新しいIPアドレスで接続してください。
- 再起動が開始されると、Web UIの接続は自動的に切断されます。これは正常な動作です。

初期化

カメラの設定を初期化するか、工場出荷時の状態に完全に戻せます。 2つの初期化方式が提供され、削除されるデータが異なるため、慎重に選択してください。

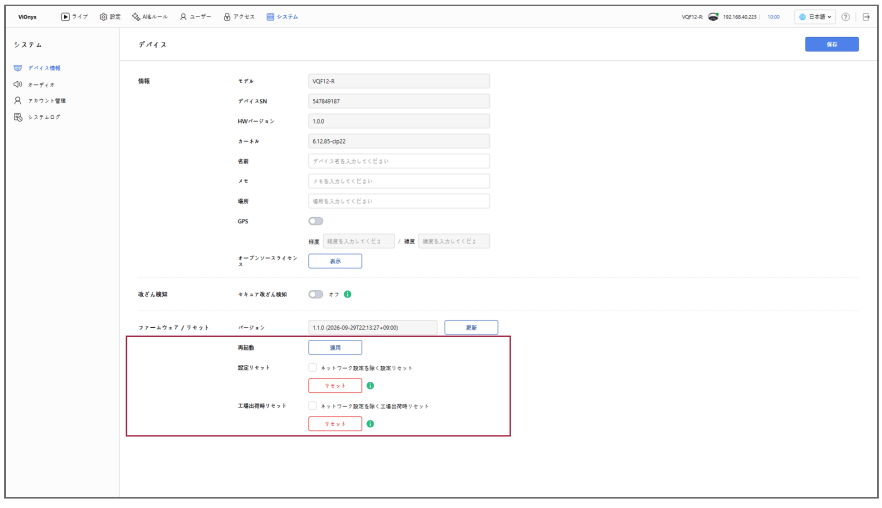
初期化方式の比較

方式	説明	削除対象	保持対象
設定リセット	設定値のみ初期化	カメラ設定、ネットワーク設定（オプション）、ビデオプロファイル、ルール、アカウント	ユーザー情報、顔データ、イベント／ログ
工場出荷時リセット	すべてのデータを削除して工場出荷時の状態に戻す	すべての設定、ユーザー情報、イベント、ログ、アカウント	-

設定リセット

設定値のみを初期化し、ユーザー情報およびログデータは保持します。

1. 画面左上の **システム** メニューをクリックします。
2. 画面左のサイドバーで **デバイス情報** をクリックします。
3. **ファームウェア / リセット** セクションの **設定リセット** で **リセット** ボタンをクリックします。



ネットワーク設定の初期化を除外するには、**ネットワーク設定を除く設定リセット** オプションのチェックボックスをクリックします。

4. 設定初期化の確認ポップアップが表示されたら、**確認** ボタンをクリックします。

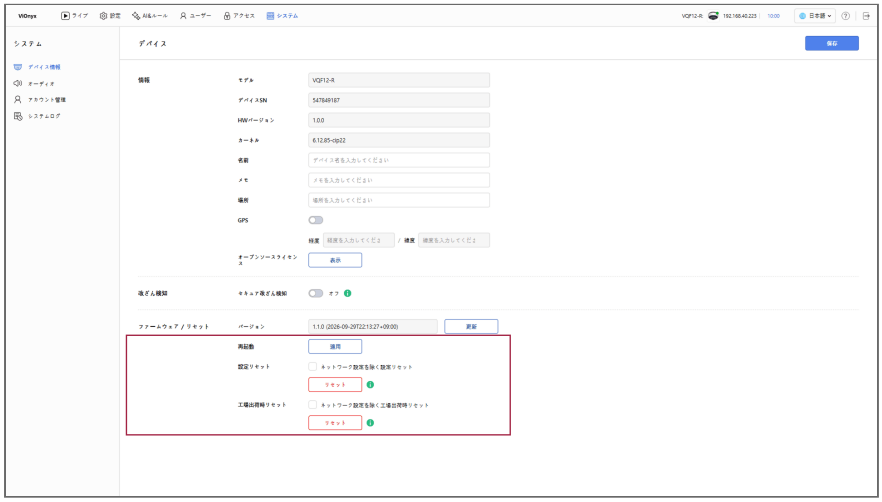
設定初期化が実行されると、カメラは自動的に再起動します。

工場出荷時リセット

カメラを完全に初期化して工場出荷時の状態に戻します。この操作は元に戻せません。

> **警告**
> 工場出荷時リセットは、すべてのデータを完全に削除します。この操作は復元できないため、十分に注意して実行してください。

1. 画面左上の **システム** メニューをクリックします。
2. 画面左のサイドバーで **デバイス情報** をクリックします。
3. **ファームウェア / リセット** セクションの **工場出荷時リセット** で **リセット** ボタンをクリックします。



ネットワーク設定の初期化を除外するには、**ネットワーク設定を除く設定リセット** オプションのチェックボックスをクリックします。

4. 工場出荷時リセットの確認ポップアップが表示されたら、**確認** ボタンをクリックします。
5. 最終確認のポップアップが表示されたら、管理者パスワードを入力してください。
6. **確認** ボタンをクリックします。

> **情報**
> - 工場出荷時リセット完了後、以下の項目がデフォルトに復元されます。
>   - 管理者ID: **admin**
>   - ネットワーク設定: DHCP
>   - すべてのユーザーデータ、イベント、ログ: 削除されます
> - 工場出荷時リセット後、Web UIにアクセスする際に新しい初期パスワードを設定する必要があります。

オーディオクリップのアップロード

カメラで使用するオーディオクリップをアップロードし、警報音や案内音として利用できます。 WAV形式のオーディオファイルをアップロードおよび管理できます。

次のような状況でオーディオクリップをアップロードしてください。

- イベント発生時に再生する警報音をアップロードする場合
- 多言語の案内音を登録する場合
- 特定の状況に合わせた音声メッセージを追加する場合

オーディオ保存容量の確認

1. 画面左上の **システム** メニューをクリックします。
2. 画面左側のサイドバーで **オーディオ** をクリックしてください。
3. **オーディオクリップ** セクションで、オーディオ保存領域の残り容量を確認できます。



オーディオファイルの準備

オーディオクリップをアップロードする前に次の点を確認してください。

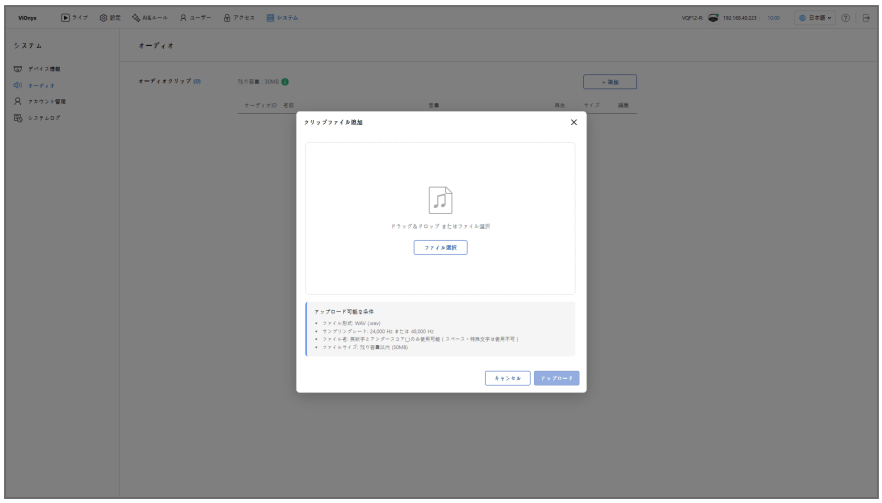
- **ファイル形式:** `.wav` 拡張子のみサポートします。
- **サンプルレート:** 48kHz以上を使用します。
- **ファイル名:** 英字、数字、アンダースコア（`_`）のみ入力でき、最大64文字です。スペースや特殊文字は使用できません。
- **ファイルサイズ:** 残り容量の範囲内でアップロードできます。

オーディオクリップのアップロード

1. 画面左上の **システム** メニューをクリックします。
2. 画面左側のサイドバーで **オーディオ** をクリックしてください。
3. 画面右上の**+ 追加**ボタンをクリックしてください。

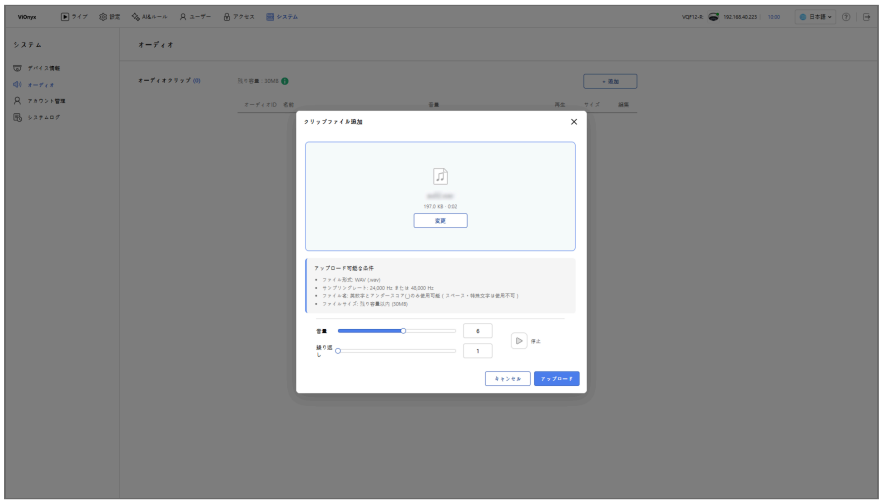


4. **クリップファイル追加** ポップアップが表示されます。



5. アップロード領域にWAVファイルをドラッグ＆ドロップするか、**ファイル選択** ボタンをクリックして、ローカルに保存されたWAVファイルを選択してください。

6. アップロードが完了したら、音量と繰り返し設定オプションを調整してください。



7. オーディオクリップをアップロードするには、**アップロード** ボタンをクリックしてください。

アップロードしたオーディオクリップは一覧で確認してください。



情報

- 音量スライダーを調整して、オーディオクリップの再生音量を設定できます。
- オーディオクリップを再生するには、▶ ボタンをクリックしてください。

オーディオクリップの削除

削除するオーディオクリップの右側にある ボタンをクリックしてください。



> **情報**
>
> - 削除するオーディオクリップがAIルール（Rule）に適用されている場合、AIルール設定から自動的に除外されます。
> - AIルール設定の詳細はAIルールの設定を参照してください。

管理者アカウントのパスワードを更新

管理者アカウントのパスワードを変更して、カメラへのアクセスのセキュリティを強化します。パスワードは定期的に変更することがセキュリティ上の推奨です。

次の場合にパスワードを変更してください。

- 管理者アカウントを初めて設定する際、セキュリティを強化する場合
- 定期的なセキュリティポリシーに従ってパスワードを更新する場合
- パスワードが漏えいしたため、緊急に変更する必要がある場合
- 管理者交代時に新しいパスワードに設定する場合

パスワード要件の確認

パスワードを設定する前に、次のルールを確認してください。すべてのルールを同時に満たす必要があります。

- パスワードは12文字以上にしてください。最大64文字以内です。
- 少なくとも1つの英小文字(`a-z`)と英大文字(`A-Z`)を含める必要があります。
- 少なくとも1つの数字(`0-9`)と特殊文字を含める必要があります。

  > *特殊文字の例:* `\" ! @ # $ % ^ & * ( ) - _ = + [ ] { }`

- `1234`、`abcd` のような連続する4文字以上、または同一文字が4回以上含まれていてはいけません。
- 大文字小文字を問わず、IDをパスワードに含めることはできません。

  > *admin, Admin, ADMIN, Admin123! など*

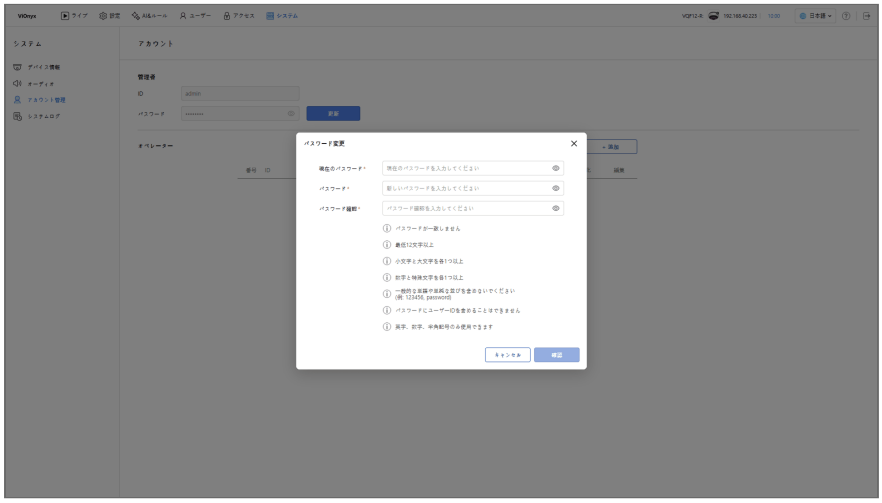
- `password`、`qwerty`、`123456` など、よく使用されるパスワードパターンは使用できません。
- 使用できるのは英字、数字、英語キーボードの特殊文字のみです。

管理者パスワードの変更

1. 画面左上の **システム** メニューをクリックします。
2. 画面左のサイドバーで **アカウント管理** をクリックします。



3. **管理者** セクションで、**更新** ボタンをクリックします。
4. **パスワード変更** ウィンドウが表示されたら、**現在のパスワード** 入力フィールドに現在の管理者パスワードを入力します。



5. **パスワード** と **パスワード確認** 入力フィールドに新しいパスワードを順に入力します。
6. 新しいパスワードに変更するには、**確認** ボタンをクリックします。

成功メッセージが表示されたら、パスワードの変更は完了です。

> **情報**
>
> - パスワード変更後、再ログインが必要になる場合があります。
> - パスワード変更の履歴はシステムログに記録されます。

パスワードを忘れた場合

管理者パスワードを紛失した場合は、次の方法で対処できます。

- **工場出荷時設定へのリセット**: 工場出荷時設定へのリセットを実行すると、管理者アカウントはデフォルト値に復元されます。ただし、すべてのデータが削除されます。工場出荷時設定への初期化方法の詳細は、ViOnyx インストールガイドを参照してください。
- **技術サポートへの連絡**: Suprema グローバル技術サポートチーム に連絡して支援を受けます。

オペレーターの管理

管理者以外に、制限された権限を持つオペレーター（Operator）アカウントを追加、編集、削除できます。オペレーターは管理者に代わってカメラの一部機能を管理できます。

また、NVR/VMSがONVIFおよびRTSP認証に使用するONVIF専用アカウントを追加できます。 ONVIF Profile S フォールバックを有効化するには、ONVIF専用アカウントが必要です。

次のような場合にオペレーターを追加してください。

- カメラ運用の担当者を追加で割り当てるとき
- 特定の権限のみを限定して付与する場合
- 複数名で協力してカメラを管理する必要があるとき
- チームメンバーに読み取り専用または編集権限を付与する場合

> **情報**
>
> - 最大10名までオペレーターを追加できます。
> - オペレーターは他のオペレーターを追加できません。オペレーターを追加できるのは管理者のみです。
> - オペレーターのパスワードは管理者のパスワードと同じルールに従います。詳しくは 管理者アカウントのパスワードを更新 をご参照ください。
> - 各オペレーターは自分のアカウント情報のみ変更できます。

オペレーター権限の種類

オペレーターを追加する際に、次の3つの権限のいずれかを選択します。

- **読み取り専用**：すべてのカメラ設定とログを参照できますが、設定は変更できません。
- **読み書き**：管理者メニューを除くすべてのメニューにアクセスでき、カメラ設定を変更できます。自分のパスワードは変更できますが、他のオペレーターや管理者アカウントのパスワードは変更できません。
- **ONVIF専用**：NVR/VMSがONVIFおよびRTSP認証に使用するデバイス専用アカウントです。 Web UIにはログインできません。ONVIF Profile S フォールバックを有効化する際に必要です。詳しくは、ネットワークを設定を参照してください。

ONVIF専用アカウントの制限事項

ONVIF専用アカウントには、通常のオペレーターアカウントと異なり、次の制限があります。

- デバイスごとに一つだけ作成できます。
- アカウント作成後は、ID、パスワード、権限を変更できません。有効化、無効化、削除のみ行えます。
- アカウントを無効化すると、Profile S フォールバックを有効化できません。
- Profile S フォールバックが有効な場合、アカウントを削除できません。先にONVIFモードを**Profile T Only**に変更してください。

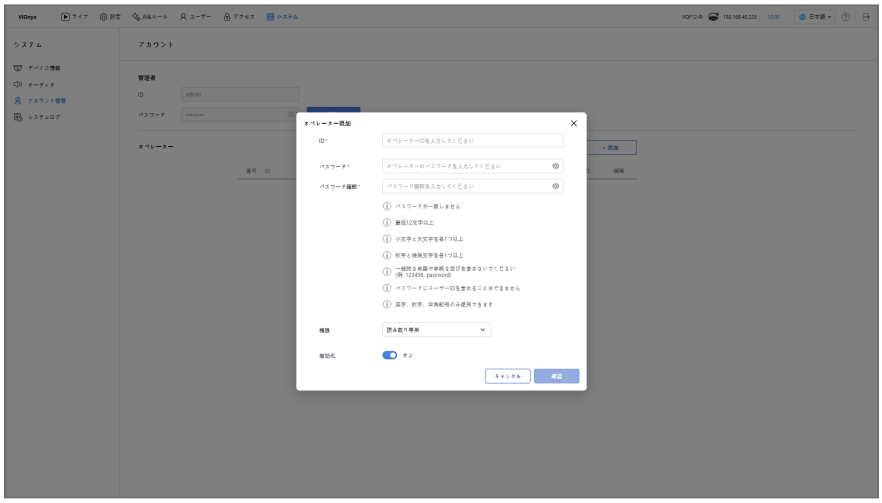
> **注意**
>
> ONVIF専用アカウントは、作成後にIDとパスワードを変更できません。接続するNVR/VMSに入力する情報を事前に決め、アカウント情報を安全に保管してください。パスワードを変更するには、アカウントを削除してから作り直してください。

オペレーターを追加

1. 画面左上の **システム** メニューをクリックします。
2. 画面左のサイドバーで **アカウント管理** をクリックします。



3. **オペレーター** セクションで **+ 追加** ボタンをクリックします。
4. **オペレーター追加** ポップアップが表示されたら、必要な情報を入力します。



- **ID**：オペレーターの固有IDを入力します。
  - 最大64文字まで入力できます。
  - ハングル、英字、数字を含めることができます。
  - 特殊文字（`_`, `.`, `-`, `(`, `)`）を使用できます。
  - 他のオペレーターと重複できません。
- **パスワード**：オペレーターのパスワードを入力します。管理者のパスワードと同じルールに従います。詳しくは 管理者アカウントのパスワードを更新 をご参照ください。
- **パスワード確認**：パスワードを再入力します。
- **権限**：オペレーターの権限を選択します。 ONVIF専用アカウントを作成するには、**ONVIF専用**を選択してください。

- **有効**：オペレーターのアカウントを有効または無効にできます。

5. すべての情報を入力したら、**確認** ボタンをクリックします。

新しいオペレーターを追加すると、一覧に新しいアカウントが表示されます。

> **情報**
>
> - オペレーターを追加したら、そのアカウントでログインして権限が正しく適用されているか確認します。
> - オペレーターのIDとパスワードは安全にオペレーターに伝えてください。

オペレーター権限の変更

追加されたオペレーターの権限を変更できます。

1. 画面左上の **システム** メニューをクリックします。
2. 画面左のサイドバーで **アカウント管理** をクリックします。
3. **オペレーター** セクションで、権限を変更するオペレーターの **権限** 項目をクリックしてください。



4. 選択リストから目的の権限に変更します。

権限の変更に成功すると、画面右上に成功メッセージが表示されます。

> **ヒント**
>
> ボタンをクリックすると、**オペレーター編集** ウィンドウが表示されます。 **権限** 項目で目的の権限に変更した後、**確認** ボタンをクリックしてください。



情報

ONVIF専用アカウントは権限を変更できません。別の権限が必要な場合は、新しいオペレーターアカウントを追加してください。

オペレーターの無効化

オペレーターのアカウントを一時的に無効化できます。アカウントを削除せず、アクセスのみをブロックします。

1. 画面左上の **システム** メニューをクリックします。
2. 画面左のサイドバーで **アカウント管理** をクリックします。
3. **オペレーター** セクションで、無効化するオペレーターの **有効** 項目のトグルボタンをクリックして、アカウントを無効化してください。



無効化に成功すると、画面右上に成功メッセージが表示されます。オペレーターのアカウントが無効化されると、これ以上ログインできなくなります。

ヒント

ボタンをクリックすると、**オペレーター編集** ウィンドウが表示されます。 **有効** 項目でトグルボタンをクリックして、アカウントを無効化してください。変更を保存するには、**確認** ボタンをクリックしてください。



情報

無効化されたアカウントは後で再度有効化できます。

> **注意**
> オペレーターが既にログイン中の場合、次回のログイン試行時にアクセスが拒否されます。

オペレーターの削除

オペレーターアカウントを完全に削除できます。削除したアカウントは復元できません。

1. 画面左上の **システム** メニューをクリックします。
2. 画面左のサイドバーで **アカウント管理** をクリックします。
3. **オペレーター** セクションで、削除するオペレーターの ボタンをクリックしてください。



4. 警告メッセージが表示されたら、**確認** ボタンをクリックしてください。

削除に成功すると、画面右上に成功メッセージが表示されます。オペレーターアカウントが一覧から完全に削除されます。

> **情報**
> **Profile T 優先 / S フォールバック** オプションが有効になっている場合、ONVIF専用アカウントを削除できません。 **設定** → **ネットワーク** → **ネットワーク**でONVIFモードを**Profile T Only**に変更してから、もう一度試してください。詳しくは、ネットワークを設定を参照してください。

システムログの確認

カメラのユーザーアクセス、イベント発生、AI分析、システム運用記録をログとして確認し、管理できます。 Webインターフェースでログの種類、レベル、アクターなどの条件でログをフィルターしたり、CSV形式でエクスポートしたりできます。さらに詳しい分析が必要な場合は、暗号化されたデバイスログをダウンロードできます。

次の場合にログを確認してください。

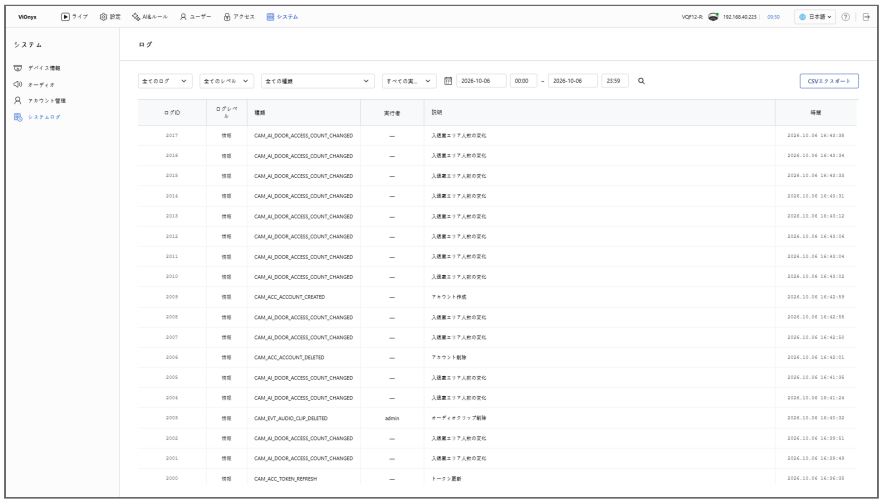
- カメラに誰がいつアクセスしたかを確認したい場合
- 特定のイベント発生記録を追跡したい場合
- カメラの起動・再起動など主要な操作を確認したい場合
- セキュリティ監視のためにアクセス記録を確認したい場合
- トラブルシューティングのためにシステムログを収集したい場合
- ログに残った操作が管理者または運用者の手動操作か、カメラの自動実行かを区別したい場合

情報

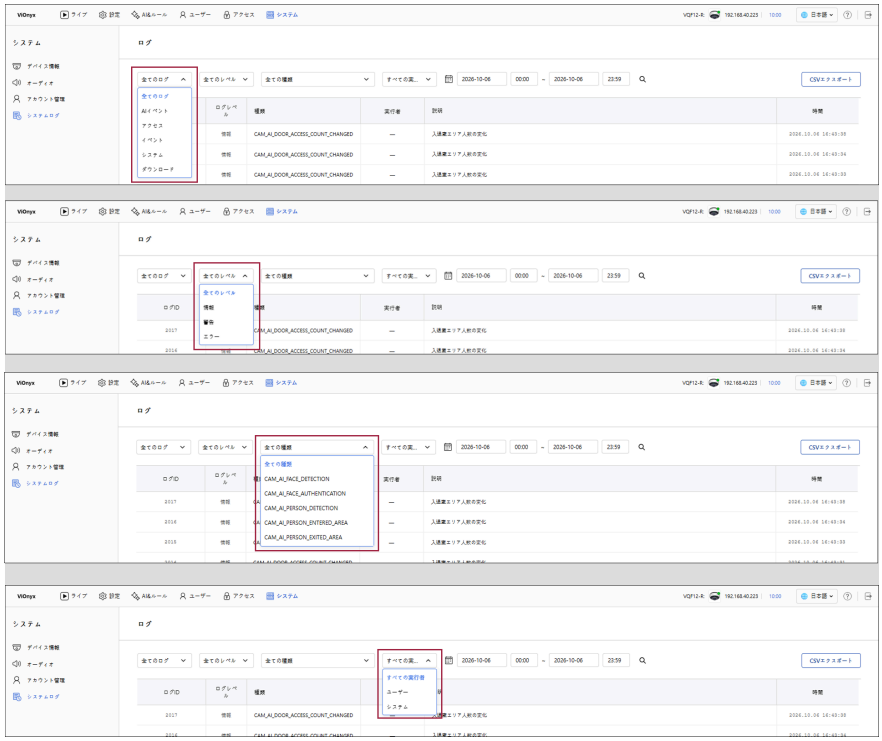
- ログは機器のメモリ容量に応じて自動的に保持されます。
- ログの種類ごとの保持期間は約1か月です。
- メモリが満杯になると、最も古いログから自動的に削除されます。
- **システムログ** メニューは、管理者および読み書き権限を持つ運用者のみが使用できます。ただし、ログの種類のうち **システム** ログは管理者のみが閲覧できます。

ログ確認

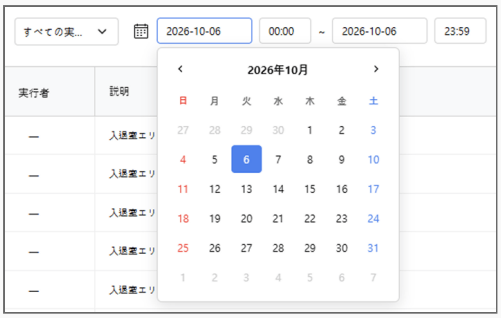
1. 画面左上の **システム** メニューをクリックします。
2. 画面左のサイドバーで **システムログ** をクリックしてください。すべてのログを確認できます。



3. ログの種類、レベル、タイプ、アクターでログをフィルターするには、ログ一覧の左上にある **全てのログ**、**全てのレベル**、**全ての種類**、**すべての実行者** から必要な条件を選択してください。



4. ログ一覧の上部にある 🔍 ボタンをクリックすると、選択した条件でログをフィルターできます。

> **情報**
>
> - 特定期間のログを確認するには、日付と時刻の入力フィールドをクリックしてください。カレンダーと時刻の選択ツールが表示されたら、開始日と時刻を選択してください。終了日と時刻も同じ方法で設定できます。
>
> 
>
>
> - 一覧を下へスクロールすると、ログ一覧を更新しながら過去のログを継続して確認できます。
> - ログ種類の詳細は システムログの種類 を参照してください。

ログ種類

ログは次のように分類できます。

- **AIイベント**: AI分析に関連するイベント記録を確認できます。
- **アクセス**: ログイン、ログアウト、アカウント作成など、ユーザーのアクセスとアカウント関連の記録を確認できます。
- **イベント**: イベント発生、Webhook送信、ルールの実行などの記録を確認できます。
- **システム**: カメラの起動、再起動、初期化などのシステム運用記録を確認できます。このログは**管理者のみが閲覧できます**。

> **情報**
>
> **ダウンロード** を選択すると、デバイスの暗号化されたログファイルをダウンロードできます。詳しくは デバイスログのダウンロード を参照してください。

ログレベル

ログは次のレベルに分類されます。

- **情報**: 一般的な情報メッセージのログを確認できます。
- **警告**: 警告メッセージのログを確認できます。
- **エラー**: エラーメッセージのログを確認できます。

アクター

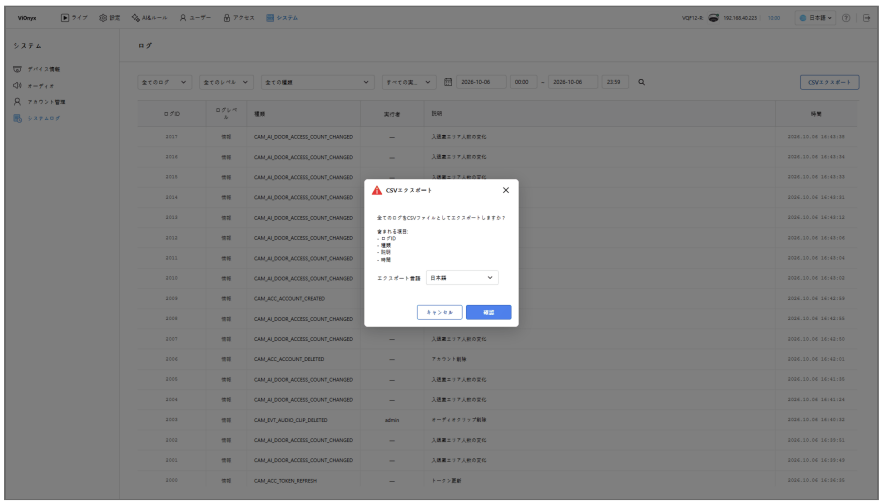
ログを生成した主体をアクターと呼びます。アクターは次のとおり分類されます。

- **ユーザー**: Webインターフェースで操作を直接実行した管理者または運用者です。
- **システム**: AIルールやスケジュールなどに従って操作を自動で実行したカメラです。

ログのエクスポート

ログをCSV形式でダウンロードし、外部で分析または保存できます。

1. 画面左上の **システム** メニューをクリックします。
2. 画面左のサイドバーで **システムログ** をクリックしてください。
3. ログ一覧の左上にある **全てのログ**、**全てのレベル**、**全ての種類**、**すべての実行者** で、エクスポートするログの条件を選択してください。検索期間を設定すると、特定期間のログもエクスポートできます。選択した条件と期間がCSVファイルにそのまま反映されます。
4. 画面右上の **CSVエクスポート** ボタンをクリックしてください。
5. **CSVエクスポート** ポップアップが表示されたら、エクスポートする言語を選択してください。



6. **確認** ボタンをクリックします。

ログ一覧をCSVファイルとしてダウンロードできます。

> **情報**
>
> - CSVファイル名は `system-logs-YYYYMMDD_HHMMSS.csv` 形式です。
>
> *例: system-logs-20240326_153000.csv*
>
> - ウェブブラウザーの既定のダウンロードフォルダーに保存されるか、ユーザーが選択した場所に保存できます。

ログの保管と管理

ログの自動削除

カメラのメモリ容量が満杯になると、最も古いログから自動的に削除されます。

ログの種類	保持期間
AIイベント	約1か月

ログの種類	保持期間
アクセス	約1か月
イベント	約1か月
システム	約1か月

重要なログの保管方法

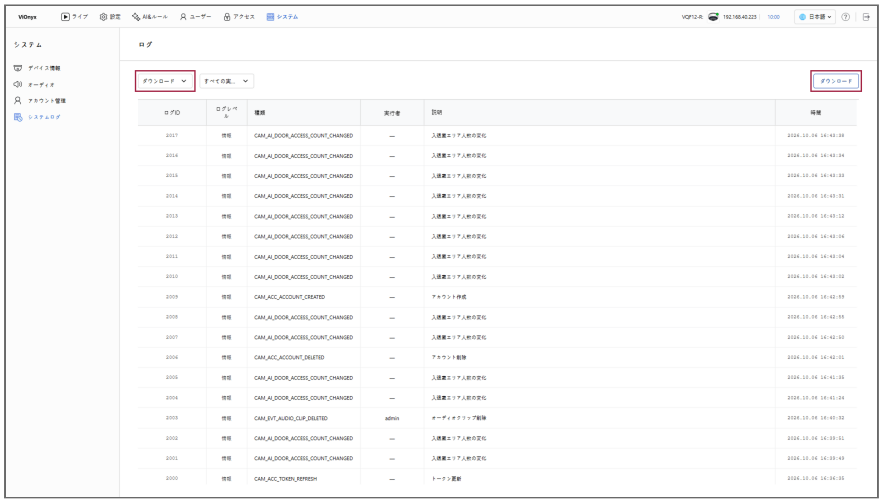
重要なログを長期間保管する場合は、次のようにしてください。

- 定期的にログをCSVでエクスポートしてください。
- エクスポートしたファイルを外部ストレージ（NAS、クラウドストレージなど）に保管してください。
- ファイルにエクスポート日とログの期間を明記してください。

デバイスログのダウンロード

デバイスに保存されたログファイルを暗号化された形式でダウンロードできます。デバイスログは、カメラシステムで発生したすべてのイベントと運用記録を含む詳細ログファイルです。このファイルは暗号化されているため、セキュリティが保たれます。必要に応じて Suprema グローバル技術サポートチーム に提供し、問題解決に活用できます。

1. 画面左上の **システム** メニューをクリックします。
2. 画面左のサイドバーで **システムログ** をクリックしてください。
3. ログ一覧の左上にある **全てのログ** で **ダウンロード** を選択してください。



4. 特定のアクターが生成したログのみをダウンロードするには、**すべての実行者** でアクターを選択してください。選択しない場合は、すべてのアクターのログをダウンロードします。アクターの詳細は アクター を参照してください。
5. ログ一覧の右上にある **ダウンロード** ボタンをクリックしてください。

デバイスログファイルをローカルにダウンロードできます。ファイル名は `device_logs_{device-serial-number}_YYYYMMDDTHHMMSS.zip.enc` 形式です。

> *例: device_logs_1234567890_20240326T153000.zip.enc*

システムログの種類

システムログで確認できるログ種類の情報を案内します。

ログの種類	説明
CAM_AI_FACE_DETECTION	顔検出
CAM_AI_FACE_AUTHENTICATION	顔認証
CAM_AI_PERSON_DETECTION	人物検出
CAM_AI_PERSON_ENTERED_AREA	エリア進入
CAM_AI_PERSON_EXITED_AREA	エリア離脱
CAM_AI_INTRUSION_ENTRY_AREA_APPEARED	侵入検出（進入エリア）
CAM_AI_INTRUSION_EXIT_AREA_APPEARED	侵入検出（離脱エリア）
CAM_AI_PEOPLE_COUNT_CHANGED	人数カウント変更
CAM_AI_PEOPLE_COUNT_LIMIT_REACHED	人数カウント上限到達
CAM_AI_LINE_CROSSED	ライン通過
CAM_AI_FACE_AUTHENTICATION_FAILED	顔認証失敗
CAM_AI_DOOR_ACCESS_EVENT_OFF	入退室イベント終了(在室解消)
CAM_AI_DOOR_ACCESS_SOURCE	入退室判定の下位シグナル
CAM_AI_DOOR_ACCESS_AREA_ENTERED	入退室エリア進入
CAM_AI_DOOR_ACCESS_AREA_EXITED	入退室エリア退出
CAM_AI_DOOR_ACCESS_LINE_CROSSED	ドアラインの通過
CAM_AI_DOOR_ACCESS_COUNT_CHANGED	入退室エリア人数の変化
CAM_EVT_RULE_TRIGGERED	ルールトリガー
CAM_EVT_RULE_CREATED	ルール作成
CAM_EVT_RULE_UPDATED	ルール更新
CAM_EVT_RULE_DELETED	ルール削除

ログの種類	説明
CAM_EVT_RULE_ENABLED	ルール有効化
CAM_EVT_RULE_DISABLED	ルール無効化
CAM_EVT_RULE_USERS_ADDED	ルールのユーザー追加
CAM_EVT_RULE_USERS_REMOVED	ルールのユーザー除外
CAM_EVT_RULE_RELAY_SCHEDULE_BLOCKED	リレー拒否 — スケジュール対象外
CAM_EVT_WEBHOOK_SEND	Webhook送信試行
CAM_EVT_WEBHOOK_SENT	Webhook送信成功
CAM_EVT_WEBHOOK_FAILED	Webhook送信失敗
CAM_EVT_WEBHOOK_CREATED	Webhook作成
CAM_EVT_WEBHOOK_UPDATED	Webhook更新
CAM_EVT_WEBHOOK_DELETED	Webhook削除
CAM_EVT_FACE_USER_CREATED	顔ユーザー作成
CAM_EVT_FACE_USER_UPDATED	顔ユーザー更新
CAM_EVT_FACE_USER_DELETED	顔ユーザー削除
CAM_EVT_FACE_USER_CREATE_FAILED	顔ユーザー作成失敗
CAM_EVT_FACE_USER_UPDATE_FAILED	顔ユーザー更新失敗
CAM_EVT_FACE_USER_DELETE_FAILED	顔ユーザー削除失敗
CAM_EVT_AI_ANALYSIS_CREATED	AI分析イベント作成
CAM_EVT_AI_ANALYSIS_UPDATED	AI分析イベント更新
CAM_EVT_AI_ANALYSIS_DELETED	AI分析イベント削除
CAM_EVT_AI_ANALYSIS_DELETE_STARTED	AI分析イベント削除開始
CAM_EVT_AI_EVENT_SETTINGS_UPDATED	AIイベント設定変更
CAM_EVT_PEOPLE_COUNT_RESET_ALL	カウント全体リセット

ログの種類	説明
CAM_EVT_PEOPLE_COUNT_RESET	カウント手動リセット
CAM_EVT_PEOPLE_COUNT_AUTO_RESET	カウント自動リセット
CAM_EVT_AUDIO_CLIP_UPLOADED	オーディオクリップアップロード
CAM_EVT_AUDIO_CLIP_DELETED	オーディオクリップ削除
CAM_EVT_AUDIO_CLIP_PLAY	オーディオクリップ再生要求
CAM_EVT_AUDIO_CLIP_PLAYED	オーディオクリップ再生成功
CAM_EVT_AUDIO_CLIP_PLAY_FAILED	オーディオクリップ再生失敗
CAM_EVT_AUDIO_CLIP_API_PLAY	APIオーディオクリップ再生要求
CAM_EVT_AUDIO_CLIP_API_STOP	APIオーディオクリップ停止要求
CAM_EVT_RELAY_SENT	リレー信号の送信
CAM_EVT_RELAY_FAILED	リレー通信の失敗
CAM_EVT_RELAY_KEEP_STARTED	リレー状態保持の開始
CAM_EVT_RELAY_KEEP_ENDED	リレー状態保持の終了
CAM_EVT_RELAY_KEEP_REARM_FAILED	リレー状態保持の再設定失敗
CAM_EVT_RELAY_OPENED	リレー一時開放
CAM_EVT_RELAY_LOCKED	リレー固定ロック
CAM_EVT_RELAY_RELEASED	リレー固定制御の解除
CAM_EVT_RELAY_OPEN_REJECTED	リレー開放の拒否(ロック中)
CAM_EVT_RELAY_AUTO_CLOSED	リレー自動再ロック
CAM_EVT_RELAY_STATE_RESTORED	リレー状態の復元
CAM_EVT_RELAY_UNLOCKED	リレー固定開放
CAM_EVT_RELAY_IDLE_STATE_CHANGED	リレー極性設定の変更
CAM_EVT_RELAY_IDLE_STATE_APPLIED	リレー極性の適用完了

ログの種類	説明
CAM_EVT_RELAY_OPEN_FAILED	リレー開放の失敗
CAM_EVT_RELAY_LOCK_FAILED	リレーロックの失敗
CAM_EVT_RELAY_RELEASE_FAILED	リレー解除の失敗
CAM_EVT_RELAY_AUTO_CLOSE_FAILED	リレー自動再ロックの失敗
CAM_EVT_RELAY_STATE_RESTORE_FAILED	リレー状態復元の失敗
CAM_EVT_RELAY_UNLOCK_FAILED	リレー固定開放の失敗
CAM_EVT_RELAY_IDLE_STATE_CHANGE_FAILED	リレー極性設定の失敗
CAM_EVT_RELAY_IDLE_STATE_APPLY_FAILED	リレー極性適用の失敗
CAM_EVT_RELAY_TOKEN_MIGRATED	リレー識別子の移行
CAM_EVT_SCHEDULE_CREATED	スケジュールの作成
CAM_EVT_SCHEDULE_UPDATED	スケジュールの変更
CAM_EVT_SCHEDULE_DELETED	スケジュールの削除
CAM_EVT_SCHEDULE_LEGACY_MIGRATED	スケジュールデータの移行
CAM_EVT_ACCESS_DOOR_CREATED	ドアの作成
CAM_EVT_ACCESS_DOOR_UPDATED	ドアの変更
CAM_EVT_ACCESS_DOOR_DELETED	ドアの削除
CAM_EVT_ACCESS_DOOR_DELETE_STARTED	ドアの削除開始
CAM_EVT_ACCESS_DOOR_DELETE_FAILED	ドアの削除失敗
CAM_EVT_ACCESS_LEVEL_CREATED	アクセスレベルの作成
CAM_EVT_ACCESS_LEVEL_UPDATED	アクセスレベルの変更
CAM_EVT_ACCESS_LEVEL_DELETED	アクセスレベルの削除
CAM_EVT_ACCESS_MEMBERSHIP_UPDATED	アクセスレベルのユーザー割当変更
CAM_EVT_ACCESS_POLICY_APPLY_STARTED	アクセスポリシー適用の開始

ログの種類	説明
CAM_EVT_ACCESS_POLICY_APPLIED	アクセスポリシー適用の完了
CAM_EVT_ACCESS_POLICY_APPLY_FAILED	アクセスポリシー適用の失敗
CAM_EVT_ACCESS_RUNTIME_RECOVERED	アクセスランタイムの復旧成功
CAM_EVT_ACCESS_RUNTIME_RECOVER_FAILED	アクセスランタイムの復旧失敗
CAM_EVT_ACCESS_POLICY_REBUILT_ON_BOOT	起動時のアクセスポリシー再構成
CAM_EVT_ACCESS_RUNTIME_DEGRADED	アクセスランタイムの機能低下
CAM_EVT_ACCESS_DOOR_TRIGGER_CREATED	ドアトリガー紐付けの作成
CAM_EVT_ACCESS_DOOR_TRIGGER_UPDATED	ドアトリガー紐付けの変更
CAM_EVT_ACCESS_DOOR_TRIGGER_DELETED	ドアトリガー紐付けの削除
CAM_EVT_ACCESS_DOOR_PASSED_UNIDENTIFIED	未識別者の通過
CAM_EVT_ACCESS_DOOR_UNLOCK_REQUESTED	認証成功 — ドア開放要求
CAM_EVT_ACCESS_DOOR_ACCESS_DENIED_DOOR_MODE	入退室拒否 — ドアロック中
CAM_EVT_ACCESS_DOOR_ACCESS_DENIED_UNIDENTIFIED	入退室拒否 — 未識別
CAM_EVT_ACCESS_DOOR_ACCESS_GRANTED	入退室許可
CAM_EVT_ACCESS_DOOR_ACCESS_GRANTED_ALREADY_UNLOCKED	入退室許可(開放中)
CAM_EVT_ACCESS_DUAL_AUTH_PENDING	二人認証の待機
CAM_EVT_ACCESS_DUAL_AUTH_TIMEOUT	二人認証のタイムアウト
CAM_EVT_ACCESS_DOOR_SCHEDULE_UNLOCKED	スケジュール開放の開始
CAM_EVT_ACCESS_DOOR_SCHEDULE_LOCKED	スケジュールロックの開始
CAM_EVT_ACCESS_DOOR_SCHEDULE_RELEASED	スケジュール区間の終了
CAM_EVT_ACCESS_DOOR_HOLD_RELEASED	開放保持の解除
CAM_EVT_ACCESS_DOOR_RULE_ACTION_SUCCEEDED	ドアルールアクションの成功
CAM_EVT_ACCESS_DOOR_RULE_ACTION_FAILED	ドアルールアクションの失敗

ログの種類	説明
CAM_EVT_ACCESS_DOOR_RULE_CREATED	ドアルールの作成
CAM_EVT_ACCESS_DOOR_RULE_UPDATED	ドアルールの変更
CAM_EVT_ACCESS_DOOR_RULE_DELETED	ドアルールの削除
CAM_EVT_ACCESS_EXIT_BUTTON_UNLOCKED	退室ボタンによる開放
CAM_EVT_ACCESS_DOOR_EARLY_RELOCKED	ドア閉鎖による早期再ロック
CAM_EVT_ACCESS_EXIT_BUTTON_UNLOCK_FAILED	退室ボタン開放の失敗
CAM_EVT_ACCESS_DOOR_PASSED	認証者の通過
CAM_EVT_ACCESS_DOOR_ACCESS_DENIED_ACCESS_LEVEL	入退室拒否 — 権限なし
CAM_EVT_ACCESS_DOOR_ACCESS_DENIED_TAILGATING	入退室拒否 — 共連れ
CAM_EVT_ACCESS_DOOR_UNLOCK_FAILED	開放失敗(設備)
CAM_EVT_ACCESS_DOOR_PASSED_AFTER_DENIED	拒否後の通過
CAM_EVT_ACCESS_DOOR_RULE_ACTION_RETRYING	ドアルールアクションの再試行
CAM_EVT_ACCESS_DOOR_RULE_MUTATION_REJECTED	ドアルール変更の拒否
CAM_EVT_HEATER_CONTROL_REQUESTED	ヒーター制御の要求
CAM_EVT_HEATER_ENABLED	ヒーターの作動
CAM_EVT_HEATER_DISABLED	ヒーターの停止
CAM_EVT_HEATER_AUTO_DISABLED	ヒーターの自動停止
CAM_EVT_HEATER_CONTROL_FAILED	ヒーター制御の失敗
CAM_EVT_HEATER_STATE_RECONCILED	ヒーター状態の再調整
CAM_EVT_HEATER_BOOT_RECOVERED	ヒーターの起動時復旧
CAM_EVT_HEATER_BOOT_RECOVERY_FAILED	ヒーター起動時復旧の失敗
CAM_EVT_HEATER_FAULT_DISABLED	障害によるヒーター停止
CAM_EVT_INPUT_IDLE_STATE_CHANGED	入力ポート極性の変更

ログの種類	説明
CAM_EVT_INPUT_IDLE_STATE_CHANGE_FAILED	入力ポート極性変更の失敗
CAM_SYS_NETWORK_CHANGE	ネットワーク設定変更
CAM_SYS_NETWORK_DHCP_FALLBACK	DHCP失敗Link-local切替
CAM_SYS_DATETIME_CHANGE	日時設定変更
CAM_SYS_NTP_SYNC_FAILED	NTP同期失敗
CAM_SYS_FIRMWARE_UPGRADE	ファームウェアアップグレード
CAM_SYS_SYSTEM_STARTED	Webサーバー起動
CAM_SYS_FACTORY_RESET	工場初期化
CAM_SYS_CONFIG_RESET	設定初期化
CAM_SYS_SYSTEM_REBOOT	システム再起動
CAM_SYS_CLUE_ENABLED	CLUe有効化成功
CAM_SYS_CLUE_DISABLED	CLUe無効化
CAM_SYS_CLUE_ENABLE_FAILED	CLUe有効化失敗
CAM_SYS_CLUE_USER_SYNC_CHANGED	CLUeユーザー同期の変更
CAM_SYS_CLUE_TUNNEL_CHANGED	CLUeトンネルの変更
CAM_SYS_CONSENT_ENROLLMENT_CHANGED	顔登録同意変更
CAM_SYS_CONSENT_ANALYTICS_CHANGED	顔分析同意変更
CAM_SYS_AI_SETTINGS_CHANGED	AI設定変更
CAM_SYS_AI_LOAD_FAILED	AI機能ロード失敗
CAM_SYS_SECURE_TAMPER_CHANGED	Secure Tamper設定変更
CAM_SYS_TUNNEL_MODE_CHANGED	トンネルモードの変更
CAM_SYS_TUNNEL_SETTING_UPDATED	トンネル設定の変更
CAM_SYS_WEBRTC_SESSION_START	WebRTCセッションの開始

ログの種類	説明
CAM_SYS_WEBRTC_SESSION_END	WebRTCセッションの終了
CAM_SYS_CRYPTO_KEYGEN_FAILED	暗号鍵生成の失敗
CAM_SYS_CRYPTO_OP_FAILED	暗号処理の失敗
CAM_SYS_SLAVE_CONNECTED	RS485スレーブの接続
CAM_SYS_SLAVE_DISCONNECTED	RS485スレーブの切断
CAM_SYS_RS485_SLAVE_FW_UPDATE_SUCCEEDED	スレーブファームウェア更新の成功
CAM_SYS_RS485_SLAVE_FW_UPDATE_FAILED	スレーブファームウェア更新の失敗
CAM_SYS_ONVIF_MODE_CHANGED	ONVIFモードの変更
CAM_SYS_ONVIF_HTTP_PROXY_FAILED	ONVIF HTTPプロキシの失敗
CAM_SYS_API_OPERATION_FAILED	API処理の失敗
CAM_SYS_API_COMPLETION_UNCONFIRMED	API処理の完了未確認
CAM_SYS_API_REQUEST_REJECTED	APIリクエストの拒否
CAM_ACC_LOGIN	ログイン
CAM_ACC_LOGOUT	ログアウト
CAM_ACC_TOKEN_REFRESH	トークン更新
CAM_ACC_PASSWORD_CHANGE	パスワード変更
CAM_ACC_AUTH_FAILURE	認証失敗
CAM_ACC_REFRESH_TOKEN_REUSE	リフレッシュトークン再使用検出
CAM_ACC_SESSION_INVALIDATED	セッション無効化
CAM_ACC_RATE_LIMIT_EXCEEDED	リクエスト制限超過
CAM_ACC_FORBIDDEN_ACCESS	権限のないアクセス
CAM_ACC_PASSWORD_SETUP	初期パスワード設定
CAM_ACC_ACCOUNT_LOCKED	アカウントロック

ログの種類	説明
CAM_ACC_SESSION_EXPIRED	セッション期限切れ
CAM_ACC_ACCOUNT_CREATED	アカウント作成
CAM_ACC_ACCOUNT_UPDATED	アカウント更新
CAM_ACC_ACCOUNT_DELETED	アカウント削除
CAM_ACC_ACCOUNT_DISABLED	アカウント無効化
CAM_ACC_SESSION_KICKED	セッション強制終了
CAM_ACC_LOGIN_FAILED	ログイン失敗
CAM_ACC_PERMISSION_DENIED	権限不足による拒否
CAM_ACC_SESSION_LIMIT_REJECTED	セッション上限超過による拒否
CAM_ACC_ACCOUNT_CREATE_FAILED	アカウント作成の失敗

付録

製品に含まれる法的通知事項を掲載しています。

免責事項

- このウェブサイトは、Suprema製品に関する情報を提供します。
- このウェブサイトは、Supremaの製品使用および販売契約に含まれるSuprema製品にのみ使用できます。 このウェブサイトは、明示的、黙示的、禁反言の原則、またはその他いかなる方法によっても、知的財産権に対するライセンスを付与しません。
- お客様とSupremaとの契約に明示されている場合を除き、Supremaは一切の責任を負わず、特定目的への適合性、商品性、非侵害に関するあらゆる明示的または黙示的保証を否認します。
- 保証が無効となるのは、次の場合です。Suprema製品が 1) 誤って設置される、またはハードウェアのシリアル番号、保証情報、品質保証ステッカーが変更または除去された場合、2) Supremaが許可した方法以外で使用された場合、3) SupremaまたはSupremaが承認した以外の者によって変更、改造、修理された場合、4) 不適切な環境で運用または保守された場合。
- Suprema製品は、製品の故障が負傷や死亡事故につながる可能性のある医療、救命、生命維持などの用途向けに設計されていません。 お客様がこのような用途でSuprema製品を購入または使用する場合、これに起因する負傷または死亡によって発生するすべての請求、費用、損失、支出および合理的な弁護士費用から、Supremaおよびそのメンバー、子会社、関連会社、供給業者を免責するものとします。 製品の設計または製造にSupremaの過失があると主張される場合でも同様です。
- Supremaは、信頼性、機能または設計を向上させるため、予告なくいつでも仕様および製品説明を変更する権利を有します。
- 個人情報は、製品使用時に認証メッセージおよびその他の関連情報の形でSuprema製品に保存されることがあります。 Supremaは、Supremaが直接制御できない、または関連契約に明示されたSuprema製品に保存される個人情報を含むいかなる情報についても責任を負いません。 個人情報を含む保存された情報を使用する場合、製品ユーザーは関連法（例：GDPR）を遵守し、適切に取り扱いおよび処理する責任があります。
- お客様は、いかなる機能の欠如や特性、または"reserved"や"undefined"と表示された説明に依存してはなりません。 Supremaは後日これを定義することができ、後日行われた変更が現行内容と矛盾した場合でも、Supremaは責任を負いません。
- 本サイトに明示的に記載されている場合を除き、Supremaは法律で許容される最大範囲で"現状のまま"販売されます。
- 製品を注文する前に、最寄りのSuprema営業所または代理店に問い合わせ、最新の仕様を確認してください。

著作権に関するお知らせ

本ウェブサイトの著作権は Suprema に帰属します。 その他の製品名、商標、登録商標に関する権利は、それぞれの所有者である個人または団体に帰属します。

Suprema Inc.

17F Parkview Tower, 248, Jeongjail-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 13554, Rep. of KOREA

電話: +82 31 783 4502 | Fax: +82 31 783 4503 | お問い合わせ: sales_sys@supremainc.com

Supremaのグローバル支社の詳細については、
QRコードをスキャンして以下のWebページにアクセスしてください。
https://www.supremainc.com/en/about/contact-us.asp

© 2026 Suprema, Inc. 本書に記載されている Suprema および Suprema 社の製品名および番号は、Suprema, Inc. の登録商標です。Suprema 社以外のすべてのブランドおよび製品名は、それぞれの企業の商標または登録商標です。製品の外観、ビルドステータスおよび/または仕様は、予告なく変更されることがあります。