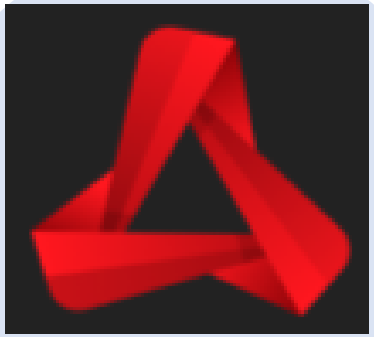
Guarding Vision 簡易マニュアル

ソフト Guarding Vision

本書は、Guarding Vision を利用するための基本設定および基本的な操作方法を
まとめた簡易マニュアルです。
より詳細な設定手順や拡張機能については、取扱説明書または弊社FAQをご参照ください。

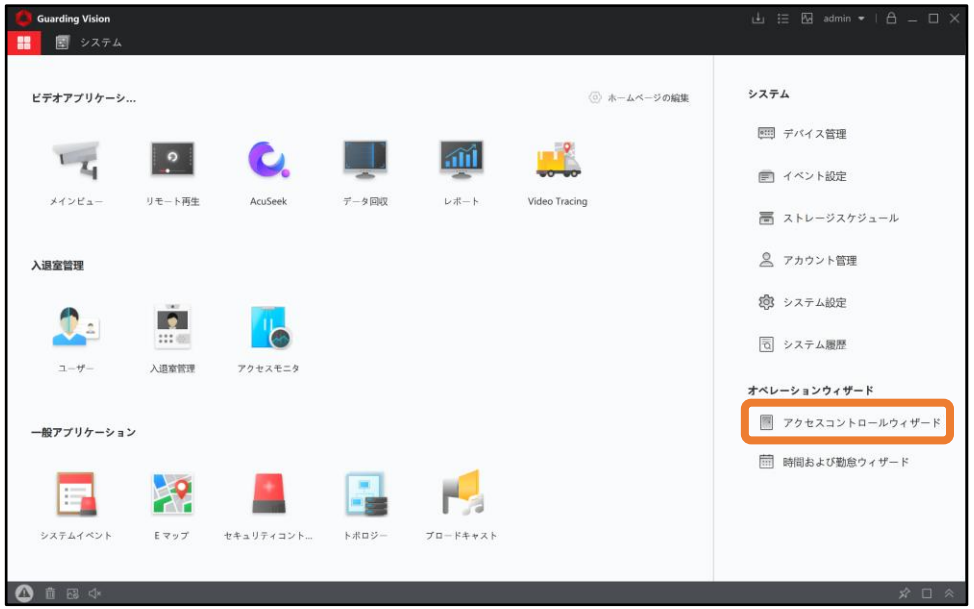
本書で説明する内容は、Guarding Vision ソフトウェアの初歩的な設定・操作に関するもの
となります。
なお、より高度な設定方法や運用方法に関しては本書では扱いません。
必要に応じて、製品ページへ別途掲載されているマニュアルをご確認ください。



●本説明書に記載されている操作画面は開発途中の内容であり、製品の操作画面とは一部異なる場合があります。
●本装置のカメラで撮影顔画像は個人情報保護法における「個人情報」が含まれます。
設置者は、被撮影者に対して、カメラにより自身の個人情報が取得されていることが認識できる処置を講ずる必要があります。
●本装置で取得した顔画像データの6か月以上の保有は、「保有個人データ」となり、本人からの開示、内容の訂正、
利用の停止等の請求に応じる義務が生まれます。6カ月以内に定期的にデータの消去をお願いします。
●本装置を従業員の勤怠、健康管理等に利用する場合、就業規則等に、取得顔画像の利用目的、画像データの管理等についての
規定を設ける必要があります。

2025. 12

アクセスコントロールウィザードについて



ホーム画面右側の「オペレーションウィザード」欄の［アクセスコントロールウィザード］をクリックします。

本簡易マニュアルでは、
アクセスコントロールウィザードを基準に、入退室管理に必要な基本操作を解説します。

目次

目次

ウィザード操作①：ー「デバイス登録手順」ー (1/2)

1 デバイス管理

デバイス（アクセスコントローラー）を登録するために、
ウィザード画面から［デバイス］をクリックしてください。

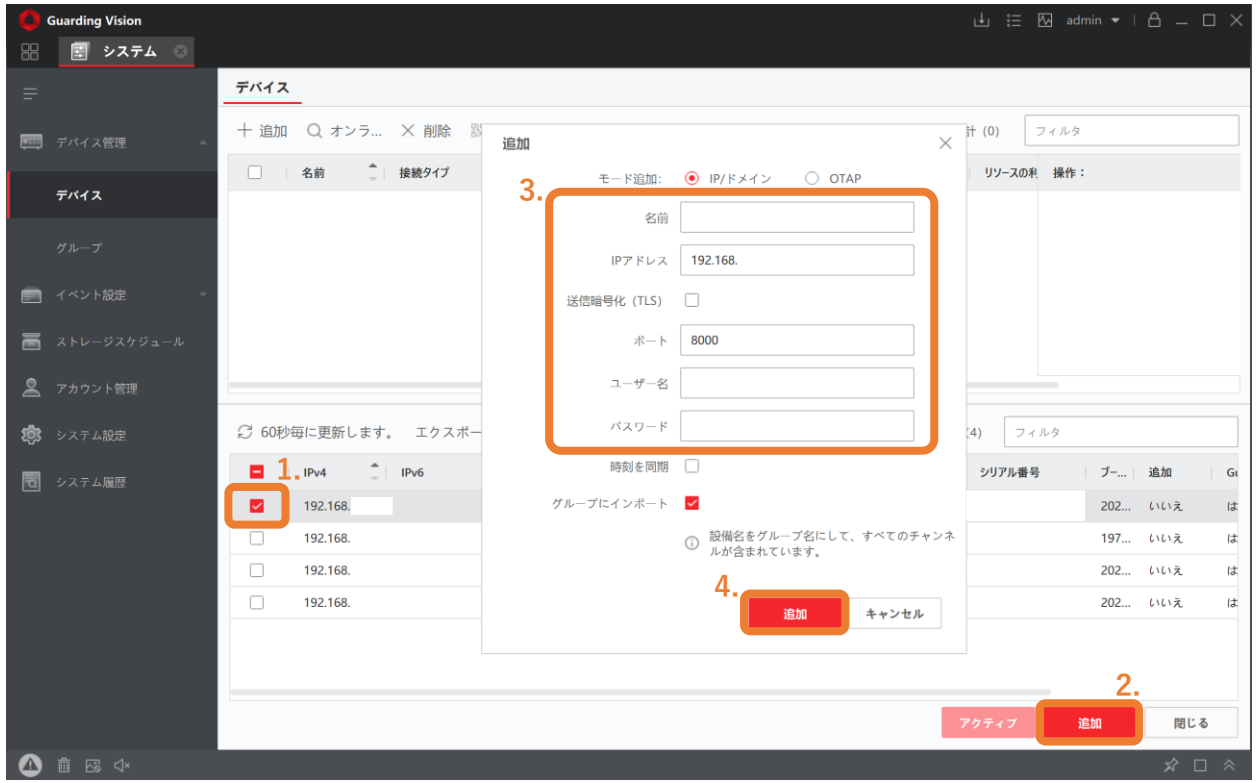
2 オンラインデバイス

デバイス画面で、メニューから［オンラインデバイス］を選択します。

- ネットワーク内で検出された、登録可能なデバイス一覧が表示されます。
- 登録したいデバイスが一覧に表示されていることを確認します。

ウィザード操作①：ー「デバイス登録手順」ー (2/2)

3 デバイス登録の詳細設定



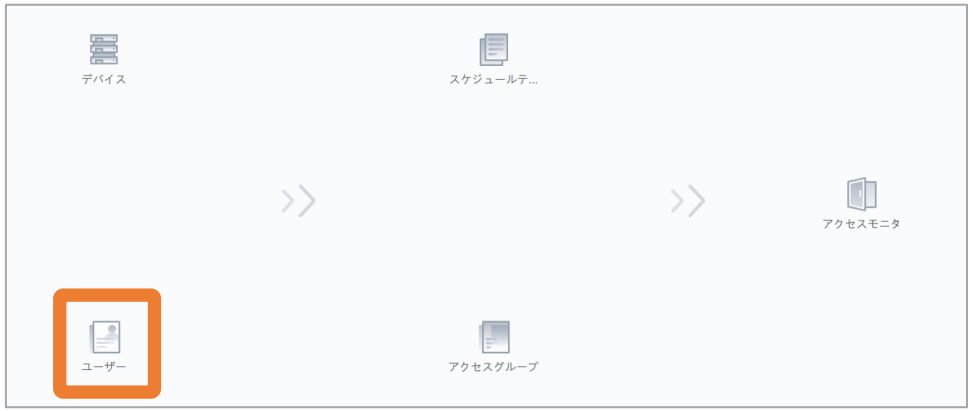
Guarding Vision利用上の注意

Guarding Vision (PC版) はローカル運用のみ対応しているため、ここで行った設定内容は、後のスライドで説明する方法で[デバイスへ適用] する必要があります。

追加したいデバイス端末に [チェック] を入れ、右下の [追加] をクリックするとデバイス情報の入力画面が表示されます。
[名前・ユーザー名・パスワード] を入力し、[追加] をクリックして登録を進めます。

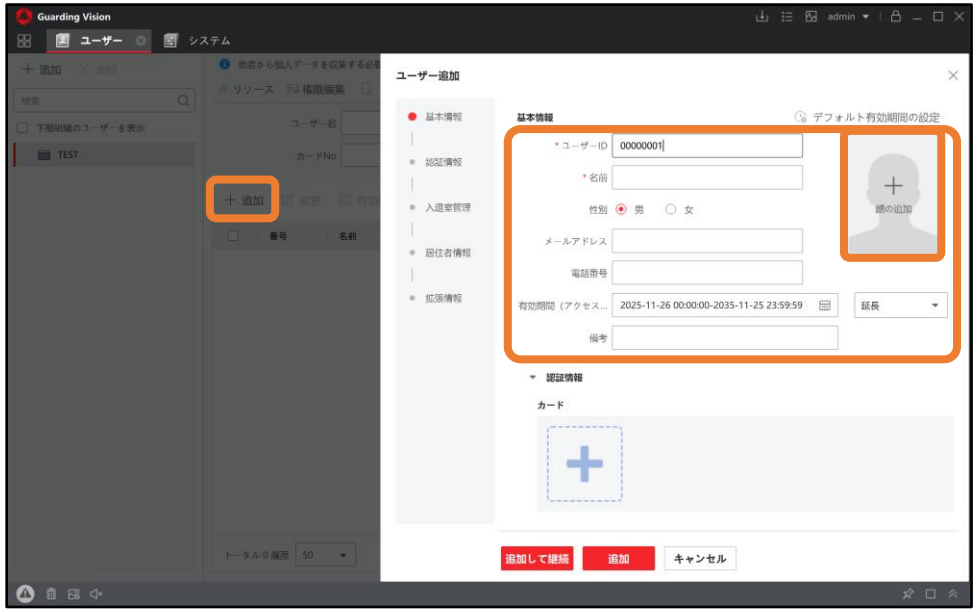
ウィザード操作②：ユーザー登録 (1/9)

1 ユーザー画面の表示



ユーザーの追加や編集を行いたいときは、
ウィザード画面から［ユーザー］をクリックすると
ユーザー管理画面が表示されます。

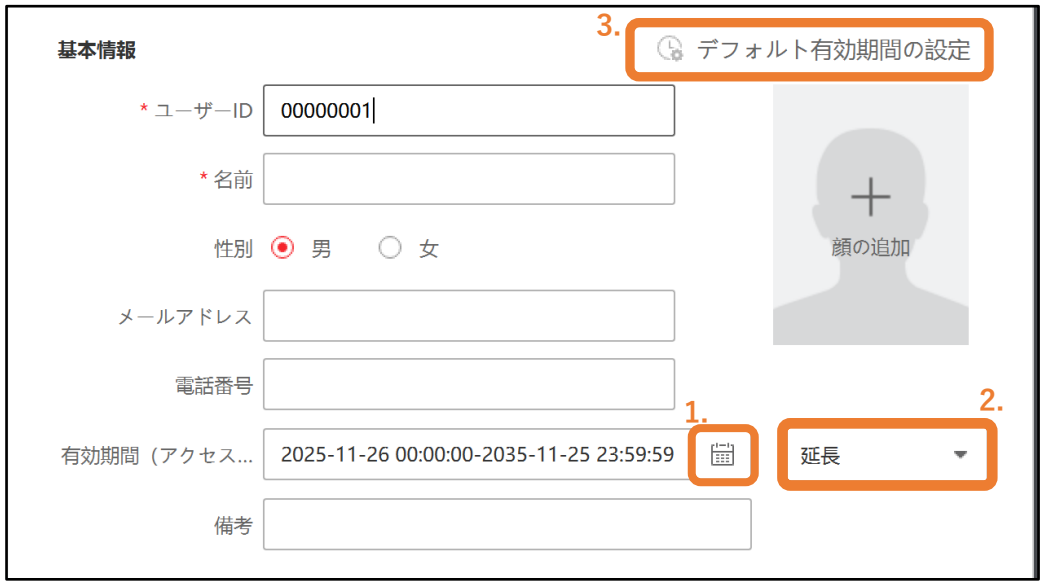
2 新規ユーザーの追加



［追加］をクリックすると、ユーザー追加画面が表示されます。
ユーザーID・名前・性別・メールアドレス（任意）・有効期限など、
必要なユーザー情報を入力します。

顔アイコンの［顔の追加］をクリックして、ユーザーの顔写真を登録します。

3 有効期限の設定について



※有効期限（日付）は2037年までしか設定できません。

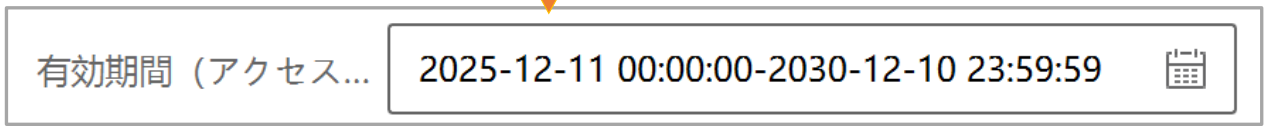
有効期限の概要について

1. カレンダー
   →有効期限をカレンダーから設定できます。

2. [延長]
   →現在設定されている有効期限から［1ヶ月/3ヶ月/6ヶ月/1年］のいずれかを選択し、有効期限を延長できます。

3. [デフォルト有効期限の設定]
   →[1年/3年/5年/10年］のデフォルト期間を設定できます。
   ※初期値10年

例：デフォルト有効期限を5年に設定した場合：



4 顔情報の追加方法

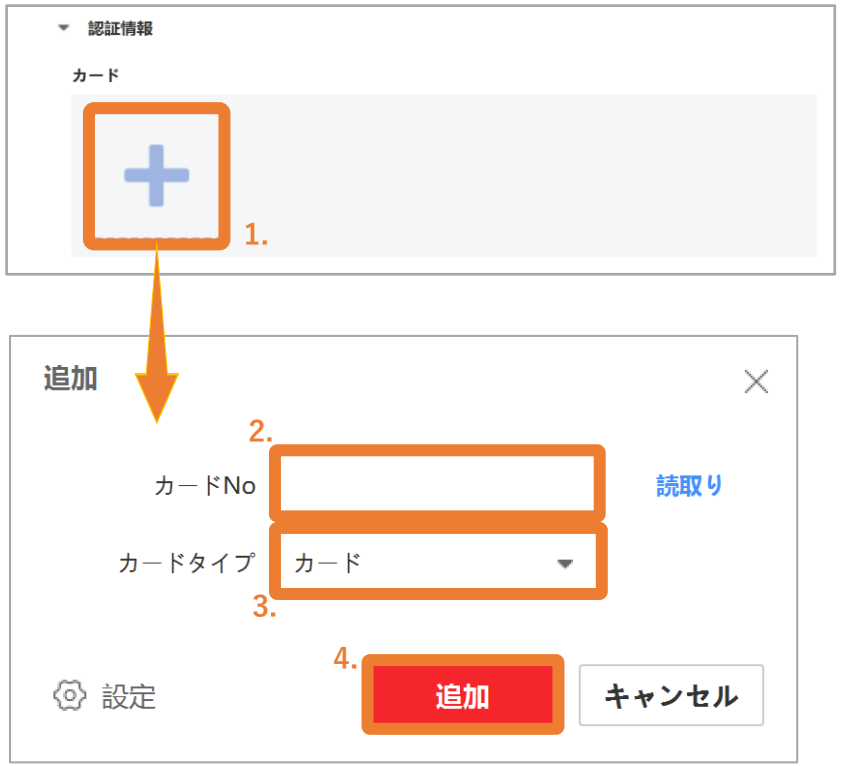
顔情報の登録方法

1. **アップロード**
   →PC内の画像（JPG形式）を選択して登録します。

2. **写真を撮る**
   →PCの内蔵カメラまたはWebカメラで撮影ができます。
   ※カメラが搭載されていないPCでは利用できません。

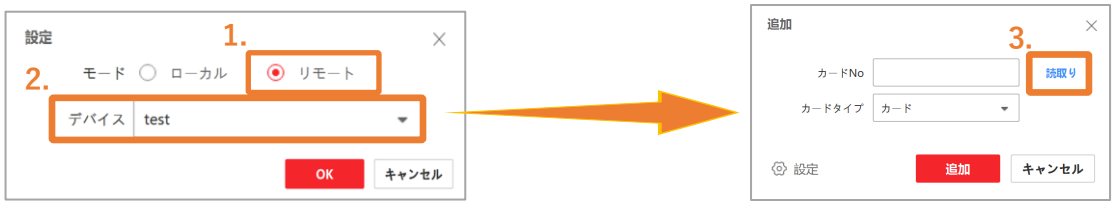
3. **リモートコレクション**
   →Guarding Vision からデバイスへ撮影指示を出し、
   選択したデバイス本体のカメラで顔を撮影して登録する方法です。
   撮影完了後、自動でGuarding Vision に顔画像が取り込まれます。

5 カードの追加手順 (1/)



カード登録時の重要事項

● **デバイスから読み取る方法**
カード追加画面左下の［設定］から［リモート］を選択し、
カードNo.の読み取りに使用する［デバイス］を指定します。



［読取り］を押した状態で、選択したデバイスにカードをかざすと、カード番号が自動で取得されます。
※ここで選択するデバイスは、カード番号を読み取るためのデバイスです。

● **手動で入力する方法**
カード番号を直接入力して登録することも可能です。
※任意のカードNo.でも登録可能です。例:12345
→実在しないカードNo.のため、カードタッチによる認証はできません。

ユーザー追加画面の認証情報内にある カード欄の［+］をクリックします。
カード追加画面が表示されるため、［カードNo.］を読取りし、［カードタイプ］を選択して［追加］を押下します。
※カードNo.は手動入力可能

6 カードタイプ

カードタイプについて

- **カード（通常カード）**
  →通常の入退室認証に使用するカード

- **緊急カード（デュレスカード）**
  →通常の認証動作でドアは解錠されますが、認証時に
  Guarding Vision（P2P登録時）または、ログとして緊急アラーム通知が
  送信されます。

  強要や危険を伴う状況を管理側へ知らせる目的で使用されます。

- **カード拒否** ※非対応
  →当機能は非対応のため、説明対象外とします。

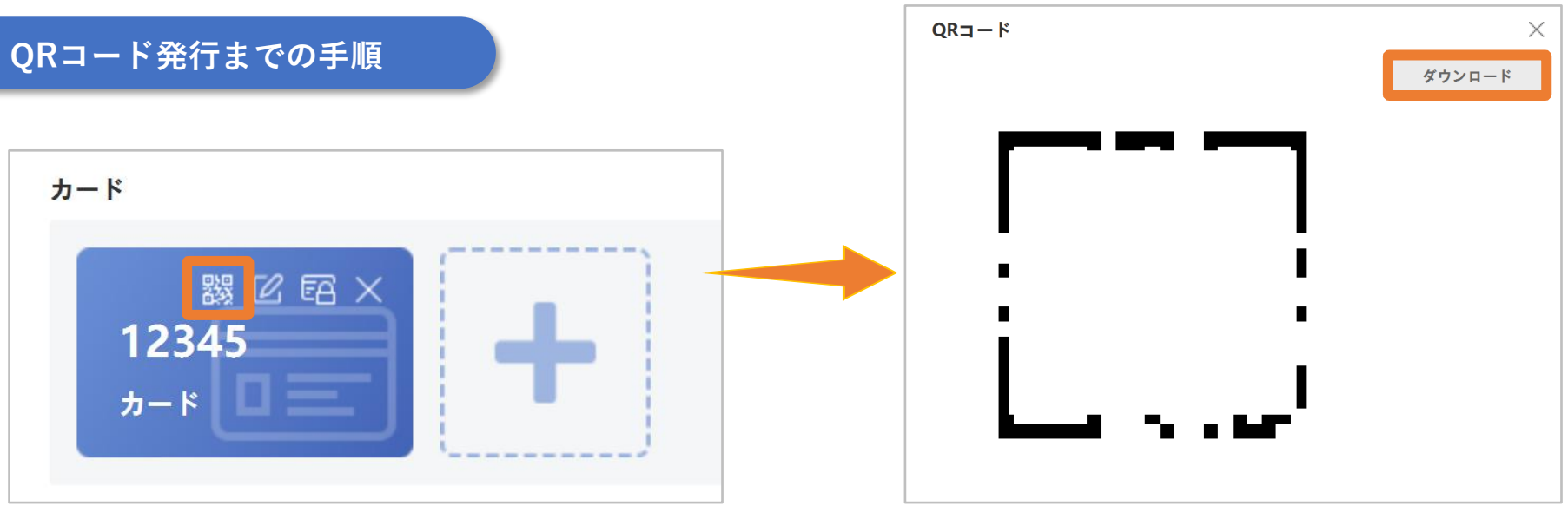
使用するカードタイプを選択し、[追加] を押下すると、カードの追加が完了します。
※カード拒否は非対応のため使用不可です。

7 カード追加後にできる操作

アイコン	内容
QRコード	カード情報からQRコードを発行できます。
編集	カード情報の変更ができます。 (カードNo.／カードタイプ)
カード紛失の報告	カードを一時的にロックします。 ロック中はカードによる入退室はできません。 ※ロックは一時的な措置です。 同じ操作を再度実行することで、ロックを解除できます。
削除	カードを削除します。

カード追加後は、QRコードの発行を含む各種操作が可能です。

8 QRコード発行までの手順



登録済みのカードにカーソルを合わせ、表示される［QRコード］アイコンをクリックします。
QRコードが表示されるため、必要に応じて［ダウンロード］します。

ダウンロードしたQRコードをスマートフォンなどに保存し、
デバイス本体へQRコードをかざすことで、QRコードによる認証が可能です。

※QRコードはユーザー情報に紐づいて発行しています。
　第三者が使用した場合でも、発行元のユーザーとして認証されます。

ウィザード操作②：ユーザー登録　ー「PINについて」ー (8/9)

1 PIN作成

入退室管理の [▶] をタップして項目を展開し、[PINコード]欄からPINを設定します。
[生成] を押すとPINが自動生成され、手動入力も可能です。

※PINコードは 3～8桁の数字で設定してください。
数字以外の入力はできません。

※PINを使用する場合、デバイスのパスワードモードを [プラットフォームパスワード] に設定してください。

1 ユーザーデータの取得

[ユーザー取得]とは、
デバイス本体でユーザー登録を行っている場合、
ユーザー情報をGuarding Visionに取り込むことができます。

[ユーザー取得] をクリックすると、デバイス選択画面が表示されます。

「選択デバイス」から、
ユーザー情報を取得するデバイスを選択します。

ユーザー情報の取得方法を選択して、
[インポート] をクリックすると、ユーザー情報が取得できます。

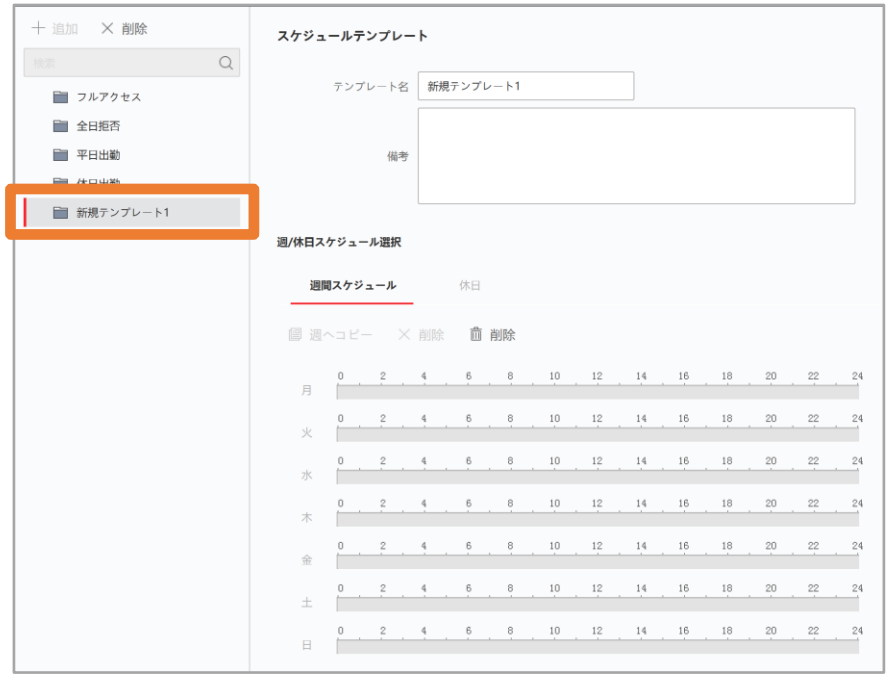
モード取得中について

- すべて取得
  →選択したデバイスのユーザー情報をすべて取得します。
- 従業員IDごと
  →指定した従業員IDのユーザー情報のみを取得します。

ウィザード操作③：スケジュールテンプレート (1/3)

1 スケジュールテンプレート

入退室を許可する時間帯を設定するため、
ウィザード画面から［スケジュールテンプレート］を
クリックします。



スケジュールテンプレート画面の［+追加］をクリックすると、
新しいテンプレートを作成できます。
テンプレート名や備考・スケジュールの時間設定などを設定し、
入退室を許可する時間帯を設定できます。

※注意点
- 「フルアクセス」「全日拒否」は初期状態で作成済みのテンプレートになります。
  →これらのテンプレートは削除できません。

2 スケジュール時間指定

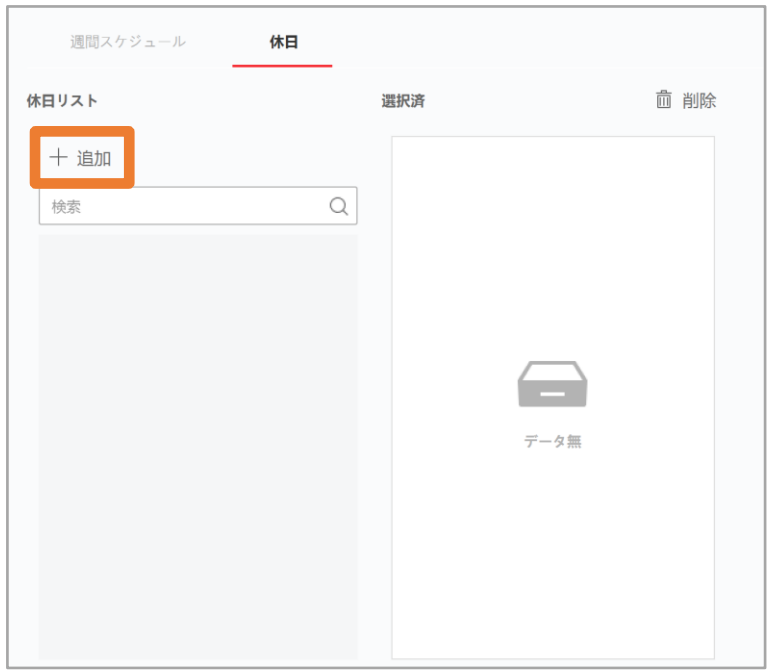
マウスで時間帯をドラッグ（左クリック）をすることで、
入退室を許可する時間を設定できます。

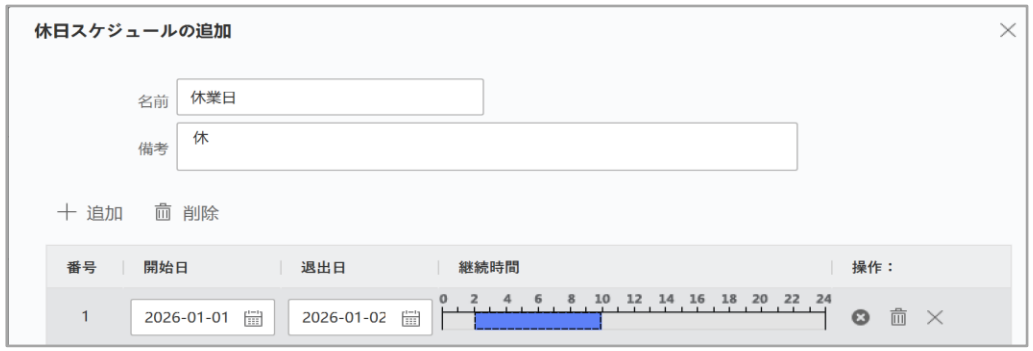
ドラッグ操作では大まかな時間指定となるため、
より正確な時刻を設定したい場合は、
設定済みの時間帯をクリックしてください。

時間帯をクリックすると、詳細設定画面が表示され、
開始時刻・終了時刻を分単位で指定できます。

ウィザード操作③：スケジュールテンプレート　ー「休日について」ー (3/3)

3 休日





[休日スケジュールの追加] 画面では、
- 名前
- 備考（例:正月、休業日など）を設定できます。

開始日・退出日・継続時間などを指定することで、
休日として扱う期間と、入退室を許可する時間帯を設定できます。

[休日] は、祝日や年末年始など、
週間スケジュールとは別に扱いたい特定の日付を設定するための機能です。

休日リストの [+追加] から、休日の追加を行います。

ウィザード操作④：アクセスグループ (1/3)

1 操作手順

アクセスグループを設定するためには、
ウィザード画面から [アクセスグループ] をクリックします。

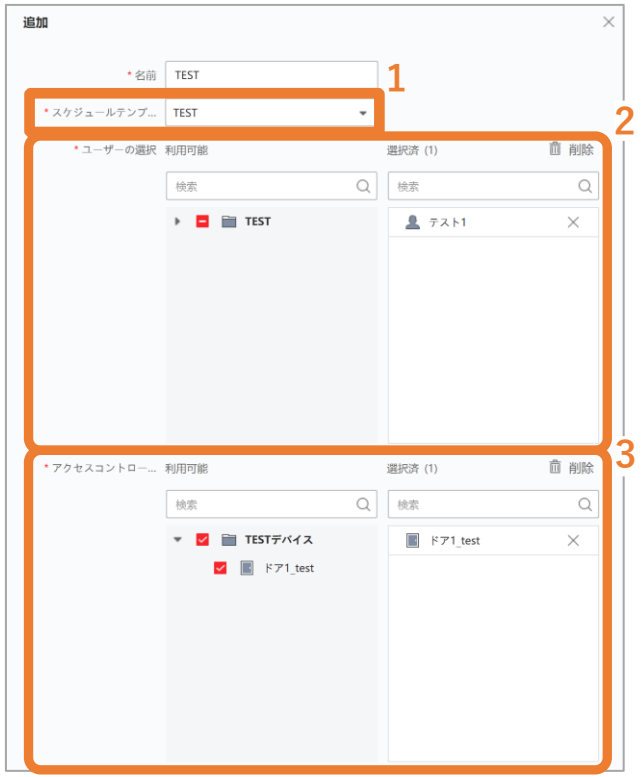
[+追加] から、スケジュール・ユーザー・デバイスを指定し、
アクセスグループの設定を行います。

2 アクセスグループの役割

アクセスグループは、
スケジュール・ユーザー・デバイスを組み合わせて
入退室ルールを設定するための項目です。

ここで設定した内容をデバイスへ適用することで、
設定した入退室ルールが実際のデバイスで有効になります。

3 入退室設定



1. いつ

スケジュールテンプレート

入退室を許可する時間帯（いつ入退室できるか）を指定します。

2. 誰が

ユーザーの選択

入退室を許可するユーザー（誰が入退室できるか）を指定します。

3. どのデバイス

アクセスコントロールポイントの選択

入退室を制御する対象のデバイス（どのデバイスか）を指定します。

[アクセスグループ追加] 画面では、入退室ルールの「いつ・誰が・どのデバイスか」を設定します。
設定後は、次スライドの手順でデバイスを適用します。

ウィザード操作④：アクセスグループ　ー 「設定内容をデバイスへ適用」ー (3/3)

1 デバイスへ適用

アクセスグループやユーザーなどの設定は、
Guarding Vision上で設定・変更しただけでは、
デバイスには反映されません。

設定内容を実際のデバイスに反映させるために、
[デバイスに適用] の操作が必要です。

※ アクセスグループが設定されていない場合、
[デバイスにすべて適用] [デバイスに変更を適用] は使用できません。

適用方法の違い

[デバイスにすべて適用]
→デバイス上の既存ユーザーデータを削除し、
Guarding Vision の設定内容をすべて再適用します。

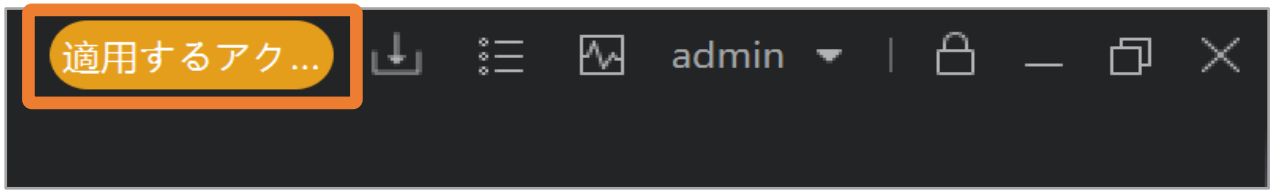
[デバイスに変更を適用]
→Guarding Vision 上で変更した内容のみをデバイスへ反映します。

推奨ケース

[デバイスにすべて適用]
→デバイス側でユーザー設定を変更してしまい、
Guarding Vision の情報と一致しない場合
(※Guarding Vision の設定が反映されます。)

[デバイスに変更を適用]
→Guarding Vision 上でユーザーやアクセスグループを変更した場合

2 適用するアクセスグループ

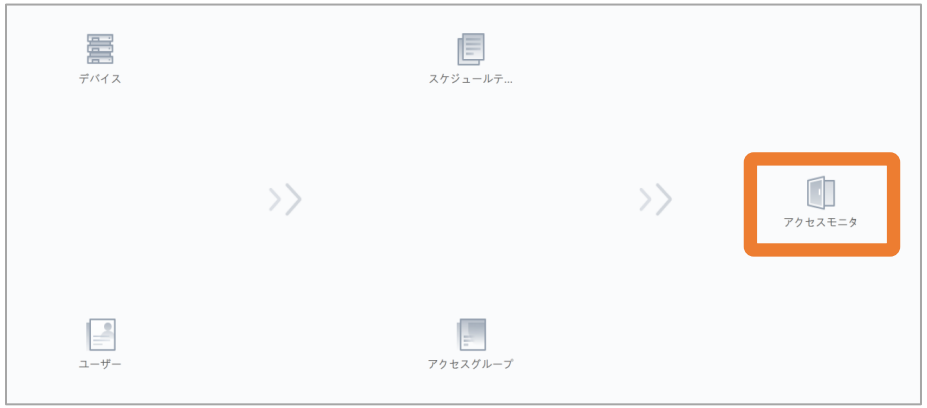


ユーザー情報やアクセスグループなど、デバイスに反映が必要な設定を**変更した**場合、
画面右上に［適用するアクセスグループ］が表示されます。

ここからも、デバイスへの適用操作を行うことができます。
※ アクセスグループ一覧からの運用と、実行される内容は同じです。

ウィザード操作⑤：アクセスモニタ（1/6）

1 操作手順



遠隔での入退室操作をするには、ウィザード画面から［アクセスグループ］をクリックします。

ウィザード操作①で登録したデバイスが表示されるので、
表示されているデバイスを選択し、上部の入退室の操作が可能になります。

ウィザード操作⑤：アクセスモニタ　ー「運用操作について」ー (2/6)

2 機能概要

ドア操作（単体）

開錠 / 施錠
ドアを一時的に開錠、または施錠します。

常時開錠 / 常時施錠
常に開錠/施錠状態を維持します。反対の操作を行うまで解除されません。

重要：常時開錠／施錠について
・"常時開錠を解除する場合" → 通常の「施錠」
・"常時施錠を解除する場合" → 通常の「開錠」

管理操作・確認

管理下
実行するとドアは施錠状態になります（通常は「施錠」と同等）。

キャプチャー
モニター映像を確認・キャプチャー保存可能 / 映像を確認してから遠隔解錠が可能です。

一括操作（全デバイス対象）

一括常時開錠 / 一括常時施錠
登録している全デバイスを常時開錠 / 施錠

その他

ステータス更新
ドア状態を最新情報に更新

3 イベントログについて

ユーザー名	組織	カードNo	イベントタイプ	時刻	ドア	認証タイプ	カードリーダ	マスクを着用
-	-	-	ロック	2026-02-04 11:21:24	入口:入口:ド...	-		不明
-	-	-	退出スイッチOff	2026-02-04 11:21:19	入口:入口:ド...	-		不明
-	-	-	アンロック	2026-02-04 11:21:19	入口:入口:ド...	-		不明
-	-	-	解錠スイッチ	2026-02-04 11:21:19	入口:入口:ド...	-		不明
-	-	-	開扉タイムアウト	2026-02-04 11:20:52	入口:入口:ド...	-		不明
-	-	-	ロック	2026-02-04 11:20:47	入口:入口:ド...	-		不明
-	-	-	アンロック	2026-02-04 11:20:42	入口:入口:ド...	-		不明
テスト1	TEST	3285103430	顔認証成功	2026-02-04 11:20:42	ドア1	カード、顔ま...	入場カードリ...	不明
-	-	-	開扉タイムアウト	2026-02-04 11:19:05	入口:入口:ド...	-		不明

画面下部の左側には、ログ（イベントログ）が表示されます。
ドアの開錠・施錠などの認証結果をリアルタイムで確認するためのログ表示画面です。

※注意点

- 過去ログの検索・CSV出力は［システムイベント］→［イベント検索］から行います。

4 イベントタイプの絞り込み

主な機能

イベントタイプ絞り込み

特定のイベントのみをフィルター表示。

※一部非対応のイベントがあります

イベントログの表示内容をリアルタイムで絞り込み表示することが可能です。

※履歴検索・CSV出力はイベント検索画面を使用します。

5 列表示のカスタマイズ

表示項目の仕様とカスタマイズ

固定表示（変更不可）

- ユーザー名
- イベントタイプ
- 時刻
- 認証タイプ

使用可能（カスタマイズ）

- ✓ 組織
- ✓ カードNo.
- ✓ ドア / カードリーダ
- ✓ マスクを着用

⚠ 設定で「マスク着用顔検出」を有効化しない場合、結果は「不明」となります。

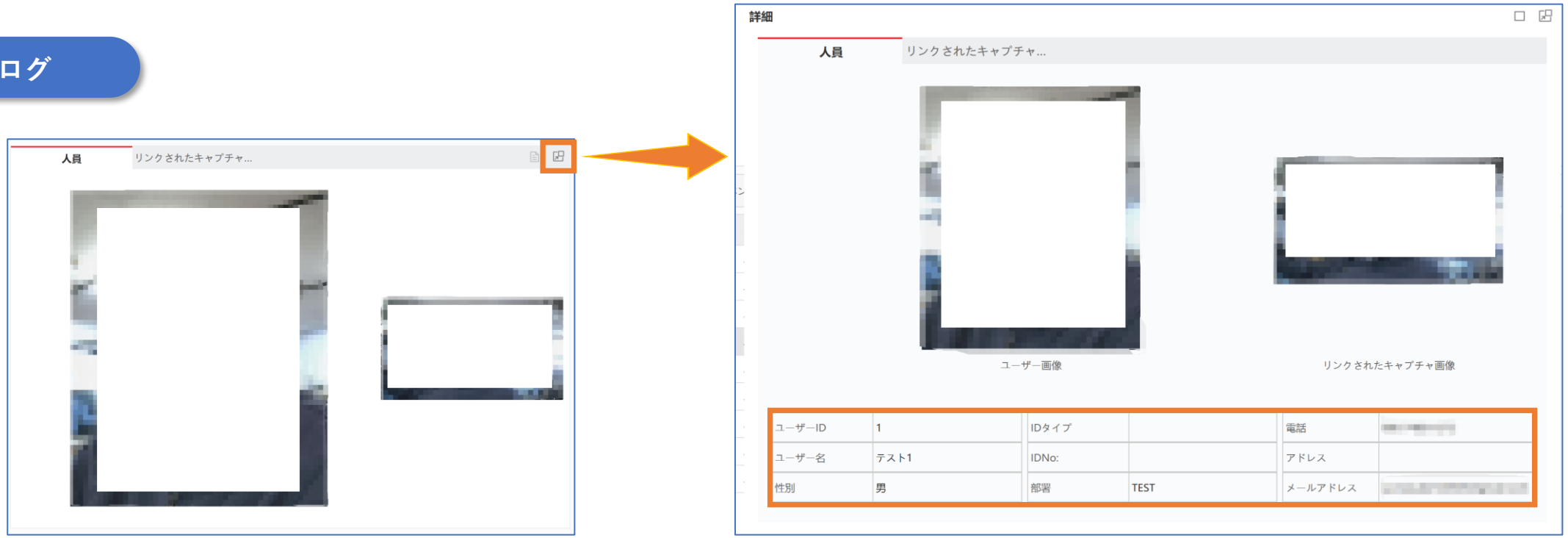
非対応（システム外）

- 温度
- 異常体温
- ヘルメットあり

※設定しても結果は「不明」となるため、非推奨です。

イベントログの表示項目は、運用内容に応じてカスタマイズが可能です。
表示可能な項目や制限事項については、上記に記載されている内容を参照してください。

6 詳細ログ



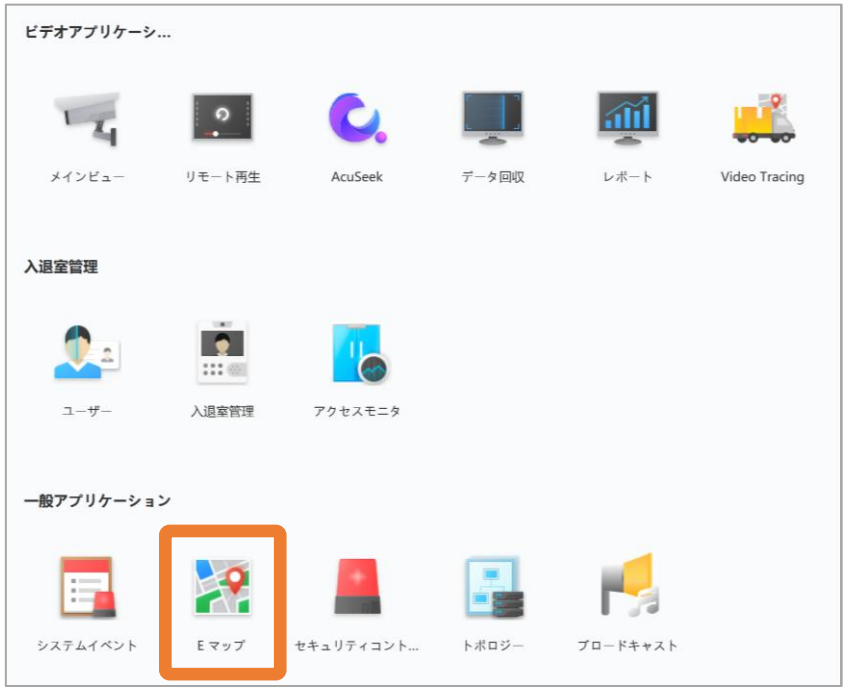
アクセスモニタ画面下部のログを選択すると、認証結果の詳細を確認することができます。
「人員」には、認証したユーザーの**登録時の顔画像（ユーザー画像）**が表示されます。

「リンクされたキャプチャー」には、顔認証で入退室を行った場合に、認証時の顔画像が表示されます。
※カード認証など、顔認証以外で認証した場合は表示されません。

右上の拡大アイコンをクリックすると、
認証したユーザーの詳細情報（ユーザーID、ユーザー名、メールアドレス、電話番号など）を確認することができます。

補足機能：E-map (1/3)

1 E-map



2 マップの追加

E-mapを使用するには、メインメニューから [Eマップ] をクリックします。

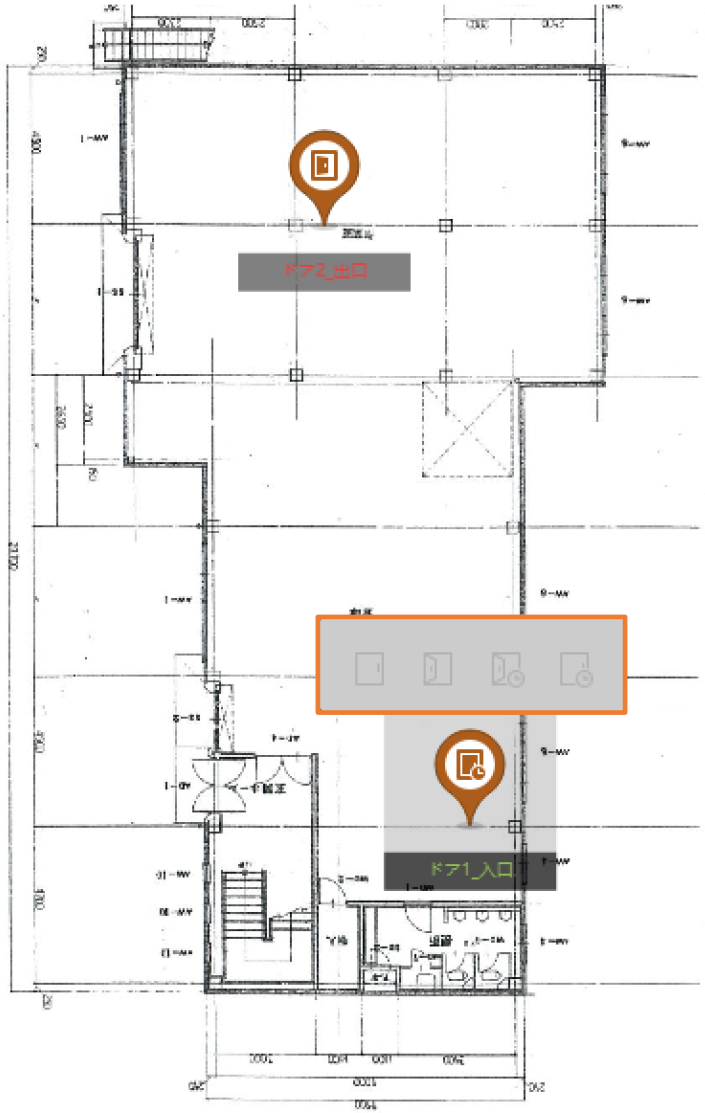
初回起動時はマップが登録されていないため、
画面に表示される [マップを追加します。] をクリックし、マップの追加を行います。

3 デバイスを配置

マップ編集画面で「+ホットスポットを追加します。」をクリックし、
[アクセスコントロールのホットスポット] を選択します。

表示された一覧から、マップ上に配置するデバイスにチェックを入れ、
[OK] をクリックすると、選択したデバイスがマップに追加されます。

追加されたデバイスは、マップ上の任意の位置へ移動して配置することができます。



ドア操作

開錠 / 施錠

ドアを一時的に開錠、または施錠します。

常時開錠 / 常時施錠

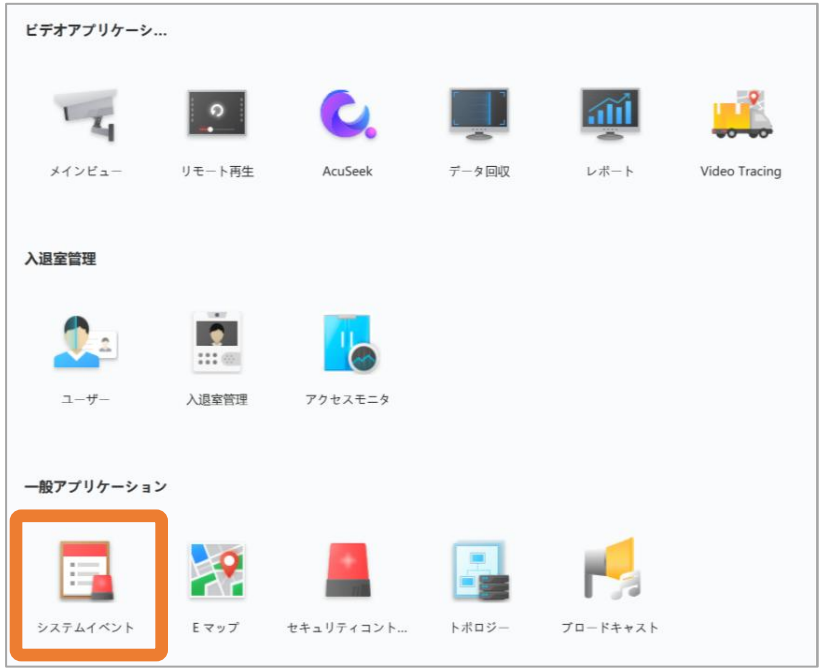
常に開錠/施錠状態を維持します。反対の操作を行うまで解除されません。

重要：常時開錠／施錠について

- "常時開錠を解除する場合" → 通常の「施錠」
- "常時施錠を解除する場合" → 通常の「開錠」

ログの運用パターンについて (1/2)

1 E-map



ログの確認・検索・出力を行うには、
メインメニューの［システムイベント］から行います。

詳細な操作手順や検索条件については、
製品ページに掲載されている「Guarding Vision（PC版）」ログ管理・運用操作マニュアルを参照してください。

次スライドでは、通常運用時と例外運用時におけるログの扱いの違いについて説明します。

ログの運用パターンについて (2/2)

番号	デバイス名	イベントタイプ	時刻	デバイスタイプ	グループ名	オブジェクト名	オブジェ...	優先度	イベント詳細
1	出口	顔認証成功	2026-01-29 11:07:20	アクセスコン...		入場カードリーダ1	アクセ...	カテゴリ無	対象:入場カードリーダ1
2	入口	顔認証成功	2026-01-29 11:07:13	アクセスコン...		入場カードリーダ1	アクセ...	カテゴリ無	対象:入場カードリーダ1

通常運用（オンライン環境）

Guarding Vision によるログ管理

- ✓ デバイスが **LAN / WAN に接続**（オンライン）
- ✓ ログは GVの**自動取得** により収集・蓄積
- ✓ 日常の確認・検索・出力は GV側で完結

補足（重要）

GVが一時的に停止していても、デバイスがオンラインなら
次回GV起動時に **未取得分も自動取得（補完）** される

👉 基本運用はこれが前提
👉 デバイス本体のログ操作は原則不要

例外対応（オフライン・トラブル時）

デバイス本体ログの利用シーン

- ⚠ デバイスが **オフライン**（Wi-Fi / PoE未接続、回線断など）
- ⚠ 自動取得ができない／できなかった状況で履歴が必要
- 🔍 障害調査・証跡保全などで一次データが必要

手順

1. デバイス本体からログをエクスポート
2. 必要に応じて GVへインポート