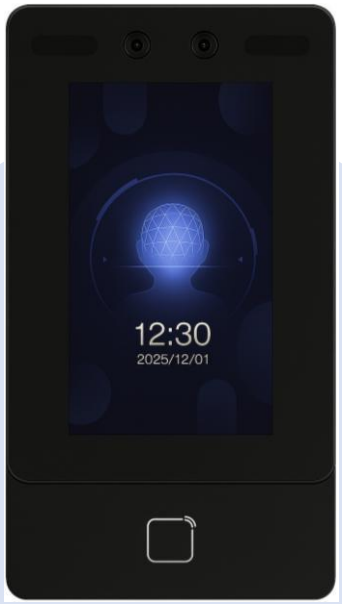
アクセスコントローラー 簡易マニュアル

機種：ASC-F01



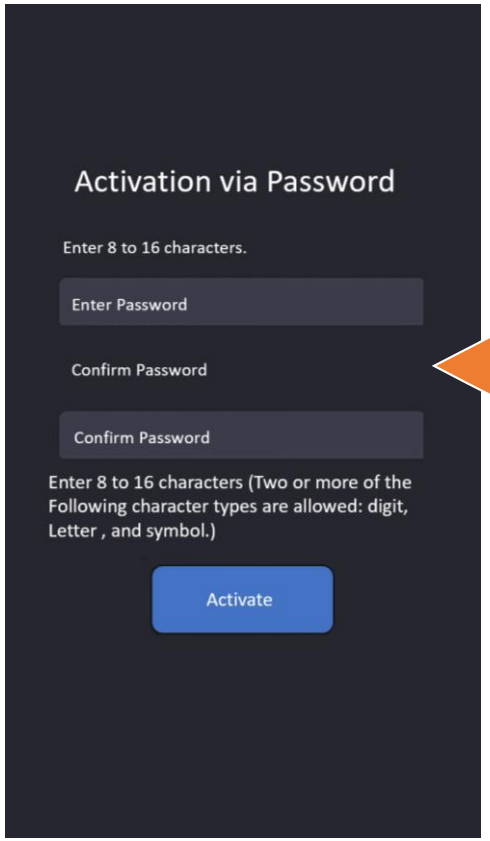
本書は、ASC-F01 の基本的な設定および操作方法をまとめた簡易マニュアルです。
詳細機能についてはユーザーマニュアル・FAQサイトをご参照ください。

ASC-F01 は専用の入退室管理ソフトウェア 「Guarding Vision」に対応しています。
「Guarding Vision」の設定および運用方法については、本書では扱いません。
別途掲載している「Guarding Vision」の簡易マニュアルをご参照ください。

- 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。

初期設定(1/6)

1 パスワードの設定



指でタップすると
キーボードが表示されます。

デバイスの初回起動時に、8～16文字のパスワードを設定してください。
※数字・英字・記号のうち2種類以上を含める必要があります。
同じパスワードを入力し、「Activate」をタッチします。

※初期設定画面は、言語選択前のため英語表記となります。

2 言語の設定

言語を選択してください。
任意の言語を選択し「Next」をタッチします。

※言語選択後、次画面より言語選択した言語へと変更されます。

初期設定(2/6)

3 メールアドレスの設定

● メールアドレスの設定 (推奨)

1. 表示された入力欄にデバイスに登録するメールアドレスを入力します。
2.「次へ」をタップすると、メールアドレスが登録されます。

※登録されたメールアドレス宛に、パスワード変更に必要なリンクが送信されます。
1 から 64文字で入力してください。

● セキュリティ質問の設定

・「セキュリティ質問の変更」をタップします。
・任意の質問を選択し、回答を入力して保存します。

※質問と回答は、パスワード変更をする際に必要になります。
1 から 128文字で入力してください。

初期設定(3/6)

4 ネットワークの設定

● 有線ネットワークを設定する場合

「有線」を選択し、「次へ」をタップします。
1. DHCPを使用する場合は、DHCPをONにします。
   - IPアドレスが自動で割り当てられます。
2. 固定IPアドレスを使用する場合は、「DHCP」をOFFにし、以下の項目を手動で入力します。
   - IPアドレス
   - サブネットマスク
   - ゲートウェイ
3. 入力後、「次へ」をタップします。

● Wi-Fiを設定する場合

「Wi-Fi」を選択し、「次へ」をタップします。
1. 接続したいWi-Fi名称をタップします。
2. パスワードを入力し、接続を完了します。
3. 設定後、「次へ」をタップします。

注意：
・Wi-Fiを使用する場合は、有線LANケーブルを外してから設定してください。
・電波環境により接続が不安定になる可能性があります。

使用環境に応じて「有線」または「Wi-Fi」を選択します。
※通信の安定性を優先する場合は「有線」を推奨。

初期設定(4/6)

5 Guarding Visionへのアクセス

「Guarding Visionへのアクセス」を有効化すると、
確認コードの入力項目が表示されます。

確認コードを入力し、「次へ」をタップします。
※確認コードを入力しないと［コードが無効］と表示され、
次へ遷移できません。

確認コードについて

- **Guarding Vision を使用する場合**
  任意の確認コードを設定できます。
  確認コードを設定すると「デバイスのQRコード」が生成されます。
  ※確認コードは、外部から受け取るものではありません。

- **Guarding Visionを使用しない場合**
  →「Guarding Vision へのアクセス」をOFFのまま
  ［次へ］をタップしてください。

デバイスのQRコードについて

上記に従い、生成された「デバイスのQRコード」は、
Guarding Vision (iOS/Android版)ホーム画面の［+］にある「QRコード/バーコード」
項目から読み取ることで、P2Pでデバイスを登録できます。
※確認コードを入力しないと［コードが無効］と表示され、次へ遷移できません。

初期設定(5/6)

6 プライバシーの設定

プライバシー設定（項目説明）

- **すべてを選択**
  →すべてのプライバシー関連項目を一括で有効化。
- **認証時に画像をアップ**
  →認証時に撮影された画像をGuarding Visionへ自動アップロード。
- **認証時に取得画像を保存**
  →認証時に撮影された画像をデバイス内に保存。
- **登録済み画像を保存**
  →登録された顔画像をデバイスに保存。
- **リンク撮影画像の転送**
  →リンクされたカメラで撮影した画像をGuarding Visionへ転送。
- **通話中に撮影した写真をアップロード]**
  →通話中に撮影した写真をGuarding Visionへ自動アップロード。

画像の保存・アップロードに関する設定を行います。
運用に合わせて適切な項目を選択し、「次へ」をタップします。

初期設定(6/6)

7 管理者の設定

項目説明

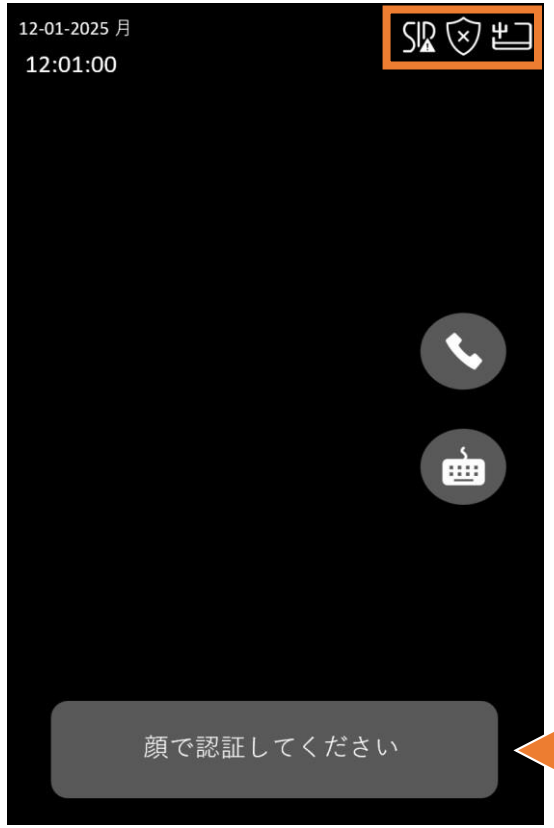
- **1. 管理者情報を入力**
  - ・ユーザーID
  - ・名前
- **2. 認証方法を登録 (任意)**
  - 顔認証を使用する場合
    ・顔を枠内に合わせて撮影します。
  - カード認証を使用する場合 (カードアイコン)
    ・カード番号を入力 or カードをかざして登録します。

運用に合わせて適切な項目を選択し、「次へ」をタップします。

最後に管理者を登録し、初期設定は完了です。

ホーム画面の説明

ホーム画面

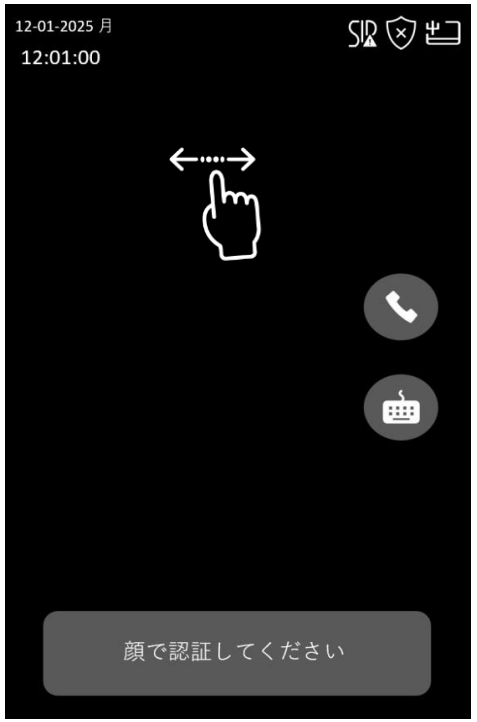


アイコン	内容
	通話や呼び出し機能が正常に接続されていない
	デバイスが Guarding Vision に登録されている/されていない
	有線ネットワーク接続中/未接続/接続不可
	Wi-Fi：接続中/未接続/接続不可
タップ可能	デバイスの部屋番号を入力し、[OK]から電話が可能 タップし、センターに電話が可能
タップ可能	認証するにはPINコードを入力 ※本機能は P13 の設定を行わないとPINコードでの認証ができません。

顔認証が成功すると表示されます。

管理者のログイン方法

1 管理者ログイン

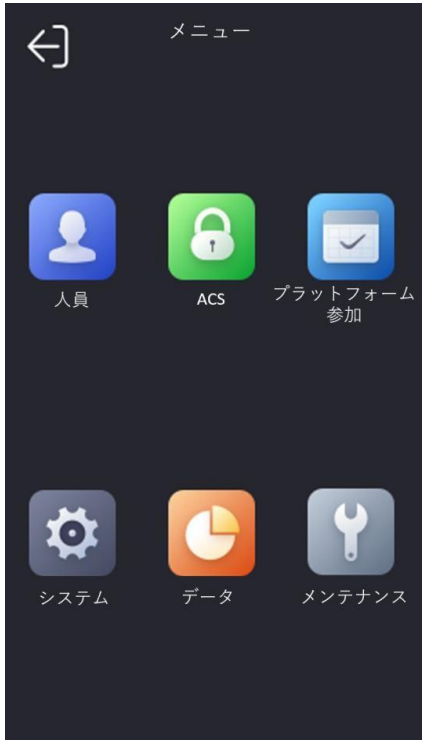


ホーム画面を [3秒間長押し]し、ジェスチャーに従い
[左にスライド]して、管理者認証画面に入ります。

2 管理者認証

「顔」または「カード」認証で、
メインメニューへ遷移します。

3 メインメニュー

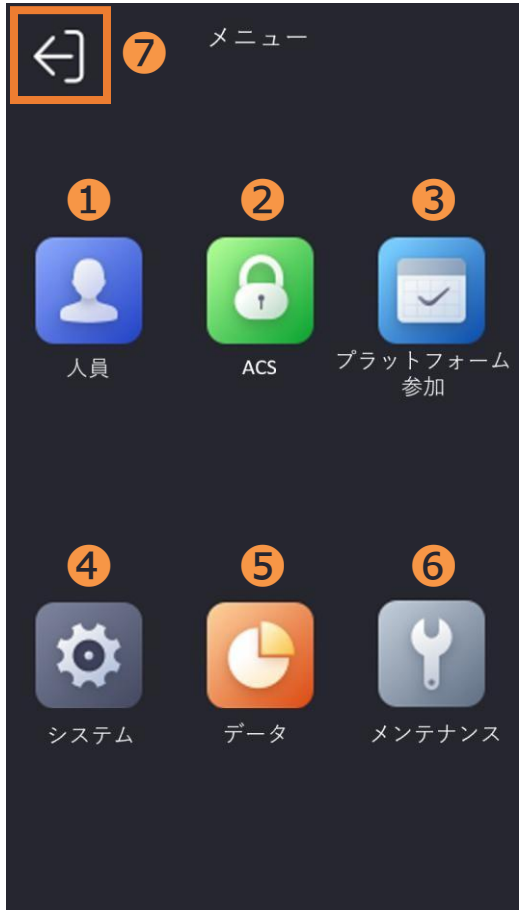


メインメニューが表示されます。

1 パスワード入力で認証も可能。
※カードの認証に 5回失敗した場合、デバイスは 30 分間ロックされます。

メインメニュー画面について

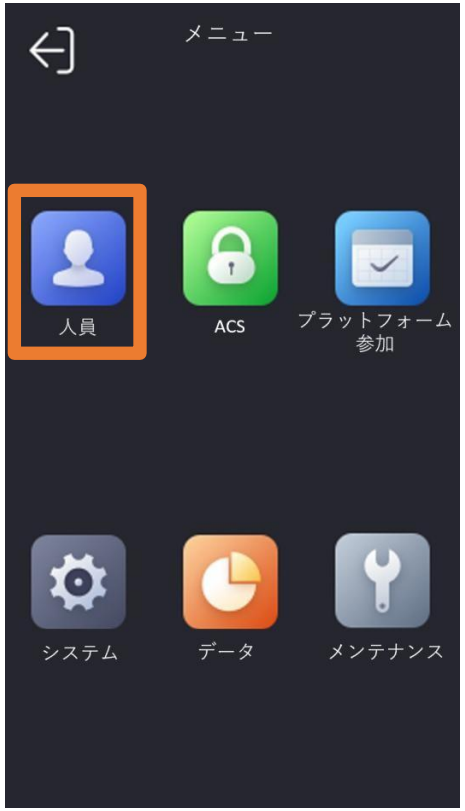
メインメニュー画面



アイコン	内容
❶人員	人員の追加・編集・削除などの操作
❷ASC	ASC（アクセスコントローラー）の詳細設定
❸プラットフォーム参加	出勤に関する設定
❹システム	本体時間、顔認証関連のパラメータの設定
❺データ	USBメモリーを利用したインポート/エクスポート、 FWアップグレード
❻メンテナンス	システム情報や容量確認（人員/顔/カード/イベント） 再起動の実行
❼ホーム	ホームへ戻る

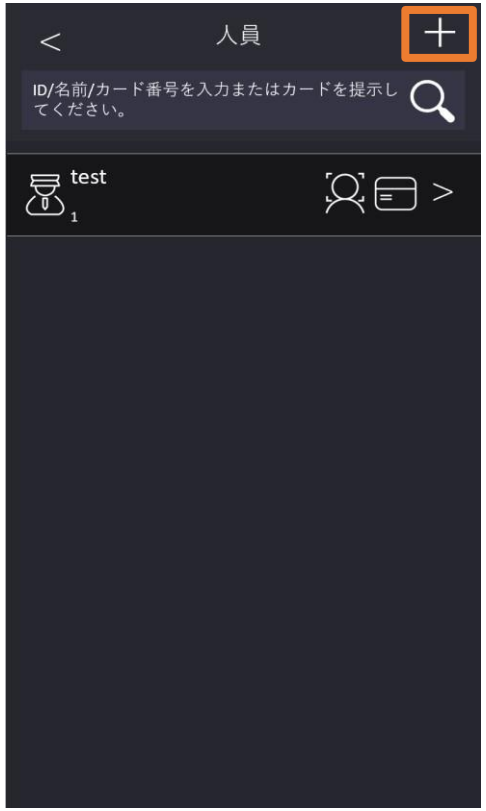
新規ユーザー登録

1 メインメニュー画面



メインメニュー画面で [人員] をタップします。

2 ユーザーの追加



[+] をタップします。

3 ユーザーの追加

[ユーザーID][名前] の [>] をタップし、設定。
認証に必要な[顔画像][カード]等も設定可能です。
※PINの入力はできません。

ユーザーIDの入力条件

- ✓ 最大32文字
- ✓ 小文字/大文字/数字の組み合わせ可
- ✓ IDの重複不可

名前の入力条件

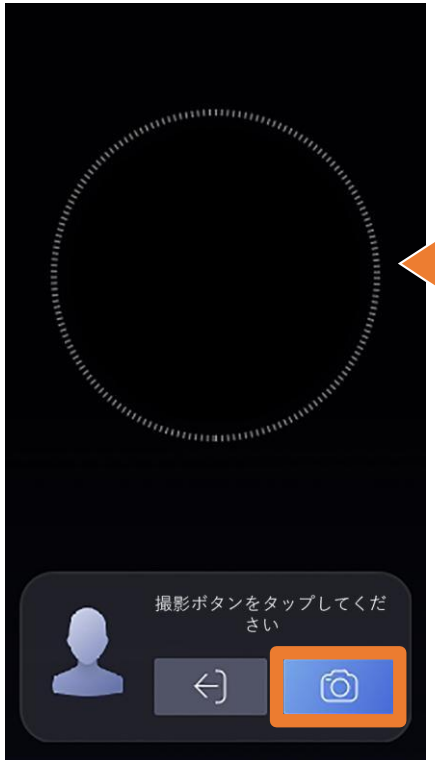
- ✓ 最大32文字
- ✓ 数字/小文字/大文字/特殊文字の使用可
- ✓ 漢字/ひらがな/カタカナは、Guarding Vision（PC版）もしくはWeb設定画面からのみ入力可

新規ユーザー登録（顔）

4 顔の登録

人員を追加画面で [顔画像]を
タップします。

5 撮影



フィールド内に顔全体を映してください。
フィールド内に顔が表示されたら
撮影をタッチして撮影します。

注意事項

- ✓ デバイスから約0.5mの位置に立ち、
  カメラの正面に立ってください。
- ✓ カメラの推奨取付高さは 1.43～1.90mです。
  適切な距離・高さで撮影を行ってください。
- ✓ 顔を近づけすぎたり、離れすぎたりしないでください。
  ※近すぎ/遠すぎは認証精度の低下に繋がります。
- ✓ 髪は顔が見えるように整えてください。
- ✓ メガネ・マスク・帽子・サングラス等、顔を覆うもの
  やアクセサリーは外してください。
  ※装飾品をつけた状態で登録した場合、外した状態
  での認証時にエラーとなる場合があります。
- ✓ 無表情で、真っすぐカメラを見てください。
- ✓ 撮影中は顔の傾き（左右・上下）を避け、数秒間静止
  した状態を保ってください。

新規ユーザー登録(カード)

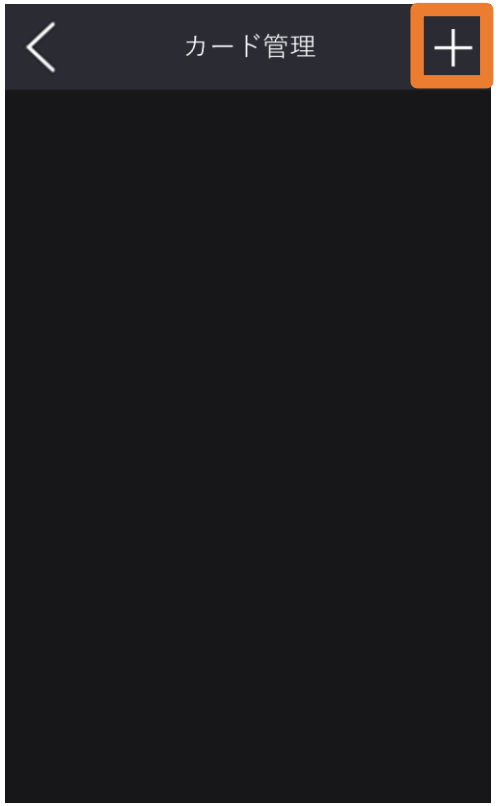
6 カードの追加

人員を追加画面で [カード]をタップします。

1ユーザー 最大50枚

Mifare対応・Felica対応

7 カードの追加



カード追加画面で[+] をタップします。

8 カードの追加

カードNo.の設定

・カード認証エリアにカードをかざしてカード番号を取得します。
(手動入力も可能)

カードタイプ

- **通常カード**
  ホーム画面では認証または、出欠確認のみが可能。
- **デュレスカード**
  通常の認証動作で扉は開きますが、認証時にGuarding Visionへ緊急アラームが通知されます。脅迫や危険と伴う状況を管理側へ密かに知らせるために使用されます。
- **スーパーカード(管理者)**
  通常の勤怠管理機能に加え、権限認証後にメインメニューへアクセスし各種操作が可能。
- **パトロールカード**
  カードをかざすことでログのみを記録。
  警備員の巡回履歴管理や怠慢防止など、巡回状況を確認するための警備管理者向けのカードです。
  ※入退室の解錠は不可

PIN登録(認証用パスワード)

1 PINモードの設定

パスワードモード

PIN（認証用パスワード）の設定方法がモードにより異なります。

- **ローカルパスワード**
  デバイス本体/Web設定画面で設定
- **プラットフォームパスワード（初期値）**
  Guarding Vision（PC版）で設定

1. メインメニュー画面から [ACS] をタッチします。
2. [パスワードモード] から任意のパスワードモードを選択します。

2 PINの設定

PINの入力条件

4～8桁の数字のみ

1. メインメニュー画面から [人員] をタップします。
2. 人員画面で [+] をタップし、[PIN] を選択します。

※パスワードモードが「ローカルパスワード」が選択されていることを確認してください。

認証モードの設定

認証モードの設定

メインメニュー画面から [人員] をタップします。
人員画面で [+] または [>] から[関係者詳細]画面へ遷移します。

・[認証設定] から [デバイスモード] または[カスタム] を選択できます。

❶デバイスモード

- ✓ 認証方式（顔/カード/PIN）を端末全体で統一して運用するモードです。
- ✓ 認証方式はASC側で一括管理され、全てのユーザーに同じ認証条件が適用されます。

❷カスタムモード

- ✓ ユーザー単位で認証方式を自由に設定するモードです。
- ✓ 必要に応じてユーザー単位で異なる認証条件を組み合わせることが可能です。

認証タイプ

- ✓ カスタムモードを選択した場合は、以下の2種類の認証モードから選択します。

  - **シングル認証**
    登録した認証方式のいずれか1つを条件とする認証方式です。
    例）顔のみ / カードのみ / PINのみ

  - **マルチ認証**
    複数の認証方式を組み合わせて運用する認証方式です。
    例）顔＋カード / 顔＋PIN / カード＋PIN