DS-K1T673シリーズ顔認証端末

ユーザーマニュアル

規制情報

FCC情報

適合性責任者によって明示的に承認されていない変更または改造を行った場合、本機器を操作するユーザーの権限が無効になる可能性があります。
FCC適合宣言：本機器は、FCC 規則第 15 部に準拠し、クラス B デジタル機器の制限について試験され、準拠していることが確認されています。これらの制限は、住宅環境における有害な干渉から合理的な保護を提供するように設計されています。本機器は、無線周波エネルギーを発生、使用、および放射するものであり、指示に従って設置および使用されない場合、無線通信に有害な干渉を引き起こす可能性があります。 ただし、特定の設置環境において干渉が発生しない保証はありません。本機器がラジオやテレビの受信に有害な干渉を引き起こしている場合（機器の電源をオフ/オンすることで確認可能）、ユーザーは以下の対策のいずれかまたは複数を試み、干渉の解消に努めてください：

—受信アンテナの方向や設置場所を変更する。

—機器と受信機の間隔を広げてください。
—機器を、受信機が接続されている回路とは異なる回路のコンセントに接続してください。

—販売店または経験豊富なラジオ／テレビ技術者に相談してください。
本機器は、放射器と身体の間に最低20cmの距離を保って設置・操作してください。

FCC条件
本装置はFCC規則第15部に準拠しています。以下の2条件を満たす場合に限り使用できます：

1. 本装置は有害な干渉を引き起こしてはなりません。
2. 本装置は、誤動作を引き起こす可能性のある干渉を含め、受信したいかなる干渉も受け入れなければなりません。

EU適合宣言

CE

本製品および付属品（該当する場合）には「CE」マークが付けられており、EMC指令2014/30/EU、RE指令2014/53/EU、RoHS指令2011/65/EUに基づき、適用される欧州統一規格に準拠しています。

2012/19/EU（WEEE指令）：この記号が付された製品は、欧州連合において一般廃棄物として廃棄できません。適切なリサイクルのため、同等の新品機器購入時に販売店へ返却するか、指定回収拠点で廃棄してください。詳細はwww.recyclethis.infoを参照。

2006/66/EC（電池指令）：本製品に含まれる電池は、欧州連合（EU）域内で一般廃棄物として廃棄できません。電池の詳細情報は製品説明書をご参照ください。電池にはこのマークが付いており、カドミウム（Cd）、鉛（Pb）、水銀（Hg）を示す文字が記載されている場合があります。 適切なリサイクルのため、電池は販売店または指定回収拠点へ返却してください。詳細は以下を参照：www.recyclethis.info

安全に関する注意事項

これらの指示は、ユーザーが製品を正しく使用し、危険や財産の損失を避けることを目的としています。

注意事項は「危険」と「注意」に分類されます：

危険：警告を無視すると、重傷または死亡事故を引き起こす可能性があります。

注意：いずれかの注意を怠ると、けがや機器の損傷を引き起こす可能性があります。

⚠	⚠
危険：重大な負傷や死亡を防ぐため、これらの安全対策に従ってください。	**注意：**潜在的な負傷や物的損害を防ぐため、これらの注意点を遵守してください。

⚠危険：

- すべての電子機器の操作は、お住まいの地域の電気安全規制、防火規制およびその他の関連規制を厳守してください。
- 本機器は、定格DC12V、3Aのクラス2サージ保護電源から給電されることを想定しています。
- 複数の機器を1つの電源アダプターに接続しないでください。アダプターの過負荷により過熱や火災の危険が生じる可能性があります。
- 配線、設置、または分解を行う前に、必ず電源が切断されていることを確認してください。
- 製品を壁や天井に取り付ける場合、装置は確実に固定してください。
- 本機から煙、異臭、異音が発生した場合は、直ちに電源を切り、電源プラグを抜いてください。その後、サービスセンターまでご連絡ください。
- 電池を飲み込まないでください。化学火傷の危険があります。
  本製品にはコイン型電池が含まれています。コイン型電池を飲み込むと、わずか2時間で重度の内部やけどを引き起こし、死に至る可能性があります。
  新しい電池と使用済みの電池は、子供の手の届かない場所に保管してください。電池ケースが確実に閉まらない場合は、製品の使用を中止し、子供の手の届かない場所に保管してください。電池を飲み込んだ、あるいは体内に挿入した可能性がある場合は、直ちに医師の診察を受けてください。
- 製品が正常に動作しない場合は、販売店または最寄りのサービスセンターまでご連絡ください。絶対にご自身で分解しないでください。（無許可の修理やメンテナンスによる問題については、一切の責任を負いかねます。）

⚠ 注意事項：

- 本製品を落下させたり物理的な衝撃を与えたりせず、高電磁波環境下に置かないでください。振動の発生する場所や衝撃を受ける可能性のある場所への設置は避けてください（放置すると機器損傷の原因となります）。
- 極端な高温（詳細な動作温度は製品仕様書参照）・低温・粉塵・湿気の多い場所に設置せず、強い電磁波にさらさないでください。
- 屋内用カバーは雨や湿気を避けて保管してください。
- 機器を直射日光、換気の悪い場所、またはヒーターやラジエーターなどの熱源にさらすことは禁止されています（無知による火災の危険性があります）。
- 本装置を太陽や極端に明るい場所に向けてはいけません。そうすると、ブローム現象やスミアが発生する可能性があります（ただし、これは故障ではありません）。同時に、センサーの耐久性にも影響を与えます。
- 装置カバーを開ける際は付属の手袋を使用し、装置カバーへの直接接触を避けてください。指の酸性汗が装置カバーの表面コーティングを侵食する恐れがあります。
- 装置カバーの内外表面を清掃する際は、柔らかく乾いた布を使用し、アルカリ性洗剤は使用しないでください。
- 開封後は、将来の使用に備えすべての包装材を保管してください。故障が発生した場合、元の包装材と共に製品を工場へ返送する必要があります。元の包装材なしで輸送すると、製品が損傷し追加費用が発生する可能性があります。
- 電池の不適切な使用または交換は爆発の危険を招く恐れがあります。同種または同等品のみと交換してください。使用済み電池は電池メーカーの指示に従って廃棄してください。
- 生体認証製品は、完全ななりすまし防止環境を保証するものではありません。より高いセキュリティレベルが必要な場合は、複数の認証モードを併用してください。
- 動作温度：-30 ℃ 〜 +60 ℃
- 屋内および屋外での使用が可能です。屋内に設置する場合、本装置は照明器具から少なくとも2メートル以上、窓やドアから少なくとも3メートル以上離して設置してください。屋外に設置する場合は、ケーブル配線部分にシリコーンシーラントを塗布し、雨滴の侵入を防いでください。
- 保護等級：IP65

対応モデル

製品名	モデル
顔認証端末	DS-K1T673DX
	DS-K1T673DWX
	DS-K1T673TDX
	DS-K1T673TDWX
	DS-K1T673TDGX
	DS-K1T673TMW
	DS-K1T673TMG
	DS-K1T673TDWX-PROE1
	DS-K1T673TDWX-E1
	DS-K1T673TDX-E1
	DS-K1T673DWX-PROE1
	DS-K1T673DG1X-E1
	DS-K1T673DGX-E1
	DS-K1T673DWX-E1
	DS-K1T673DX-E1

取扱説明書に記載されている電源のみを使用してください：

モデル	メーカー	標準
C2000IC12.0-24P-DE	MOSO Power Supply Technology Co., Ltd.	CEE
C2000IC12.0-24P-GB	MOSO Power Supply Technology Co., Ltd.	BS
KPL-040F-VI	Channel Well Technology Co Ltd.	CEE

法的情報

この文書について

- 本ドキュメントには、製品の使用および管理に関する指示が含まれています。以下に示す図、チャート、画像、その他すべての情報は、説明および解説のみを目的としています。
- 本ドキュメントに記載されている情報は、ファームウェアの更新その他の理由により、予告なく変更される場合があります。最新版はHikvisionウェブサイト（***https://www.hikvision.com***）でご確認ください。別途合意がない限り、杭州海康威視数字技術有限公司またはその関連会社（以下「Hikvision」）は、明示的または黙示的を問わず、一切の保証を行いません。
- 本ドキュメントは、本製品のサポートに関する訓練を受けた専門家の指導および支援のもとでご使用ください。

本製品について

- 本製品は、購入された国または地域でのみアフターサービスサポートを受けることができます。
- お選びいただいた製品が映像製品の場合は、以下のQRコードをスキャンして「映像製品の使用に関する取り組み」を入手し、よくお読みください。

知的財産権の認識

- 本ドキュメントに記載された製品に具現化された技術に関連する著作権および／または特許はHikvisionが所有しており、これには第三者から取得したライセンスが含まれる場合があります。
- 本文書のテキスト、画像、グラフィックなど、その一部または全部は、書面による許可なく、いかなる手段によっても抜粋、複製、翻訳、改変することはできません。
- HIKVISION およびその他の Hikvision の商標およびロゴは、さまざまな法域における Hikvision の所有物です。
- 記載されているその他の商標およびロゴは、それぞれの所有者に帰属します。

法的免責事項

- 適用される法律で許容される最大限の範囲において、本書および記載された製品（ハードウェア、ソフトウェア、ファームウェアを含む）は「現状有姿のまま」かつ「あらゆる欠陥およびエラーを含む状態で」提供されます。HIKVISIONは、

商品性、満足すべき品質、特定目的への適合性を含むがこれらに限定されない、明示または黙示のいかなる保証も行いません。 本製品のご利用はお客様ご自身の責任において行ってください。いかなる場合においても、HIKVISION は、契約違反、不法行為（過失を含む）、製造物責任、その他いかなる法的根拠に基づく場合であっても、本製品の使用に関連して生じた特別損害、結果的損害、付随的損害、または間接損害（事業利益の損失、業務中断、データの損失、システムの破損、文書の喪失等を含むがこれらに限定されない）について、たとえ当該損害または損失の可能性について事前に通知されていた場合であっても、一切責任を負わないものとします。

- お客様は、インターネットの性質上、固有のセキュリティリスクが存在することを認識し、サイバー攻撃、ハッカー攻撃、ウイルス感染、その他のインターネットセキュリティリスクに起因する異常動作、プライバシー漏洩、その他の損害について一切の責任を負いません。ただし、必要に応じてタイムリーな技術サポートを提供します。
- お客様は、本製品を適用されるすべての法令に準拠して使用することに同意し、お客様の使用が適用される法令に準拠していることを確認する責任はお客様のみにあります。 特に、お客様は、パブリシティ権、知的財産権、データ保護およびその他のプライバシー権を含むがこれらに限定されない、第三者の権利を侵害しない方法で本製品を使用することについて責任を負います。 お客様は、大量破壊兵器の開発または製造、化学兵器または生物兵器の開発または製造、 核爆発物または安全でない核燃料サイクルに関連する文脈における活動、または人権侵害を支援する活動を含むがこれらに限定されない。
- 本文書と適用される法律との間に矛盾が生じた場合は、後者が優先する。

データ保護

- データの保護のため、Hikvision製品の開発にはプライバシー・バイ・デザイン原則が組み込まれています。例えば、顔認識機能を備えた製品では、生体認証データは暗号化方式で製品内に保存されます。指紋認証製品では、指紋テンプレートのみが保存され、指紋画像を再構築することは不可能です。
- データ管理者／処理者として、個人データの収集、保存、利用、処理、開示、削除などの処理を行う場合があります。個人データの保護に関連する適用法令（合理的な管理上および物理的なセキュリティ対策の実施、セキュリティ対策の有効性に関する定期的な見直しおよび評価の実施など、個人データを保護するためのセキュリティ対策の実施を含むがこれらに限定されない）に注意を払い、これを遵守することが推奨されます。

記号の表記規則

本書で使用される記号は、以下の通り定義されます。

記号	説明
 危険	回避しなければ死亡または重傷を負う危険な状況を示します。
 注意	回避しなければ、機器の損傷、データの損失、性能の低下、または予期しない結果をもたらす可能性のある潜在的な危険な状況を示します。
 注記	本文の重要な点を強調または補足するための追加情報を提供する。

目次

第1章 インストール

1.1 設置環境

- バックライト、直射日光、間接日光を避けてください。
- 認識精度を高めるため、設置環境内またはその近くに光源があることが望ましい。
- 屋外に設置する場合は、保護シールド（オプション）を取り付けてください。

注意

設置環境の詳細については、「*設置環境に関する注意事項*」を参照してください。

1.2 フラッシュマウント（ギャングボックス付き）

作業前に

デバイスの裏面シートを取り外してください。

手順

1. 壁に配線ボックスが取り付けられていることを確認してください。

注意

ギャングボックスは付属していません。

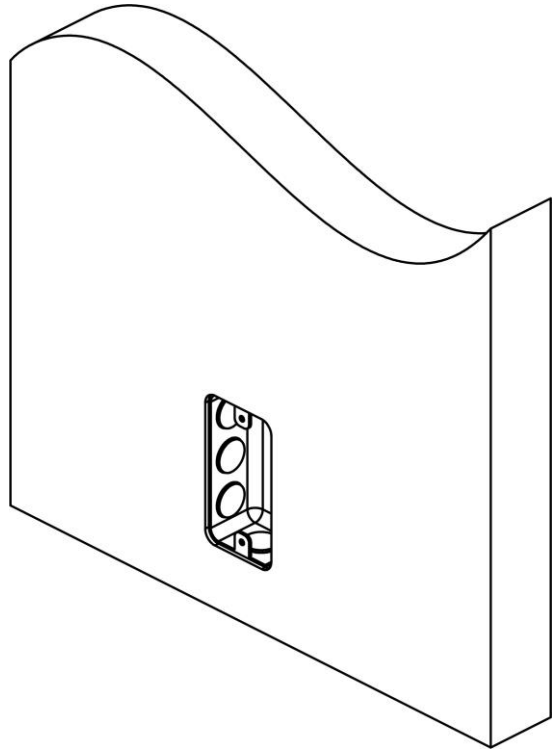


図 1-1 ギャングボックスの取り付け

2. 付属のネジ 2 本（SC-KA4x25-SUS）で、取り付けプレートをギャングボックスに固定します。

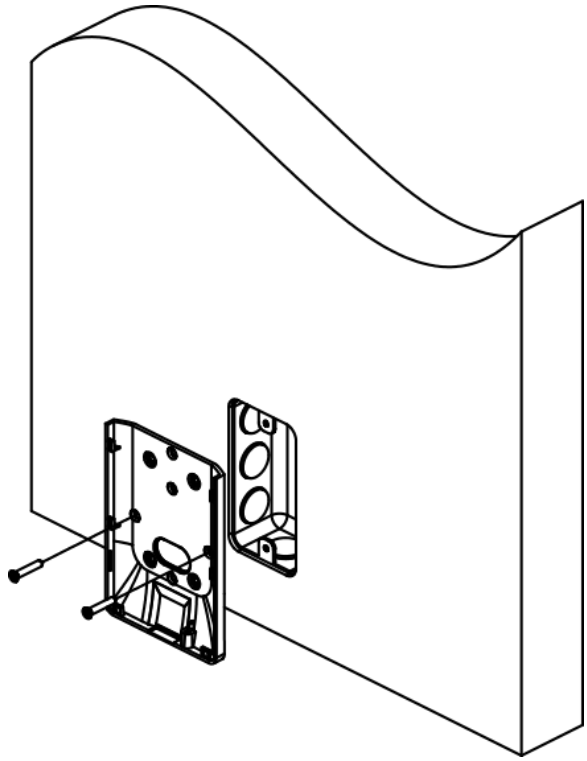


図 1-2 取付プレートの取り付け

3. ケーブルをケーブル穴に通し、配線した後、ギャングボックスに挿入します。

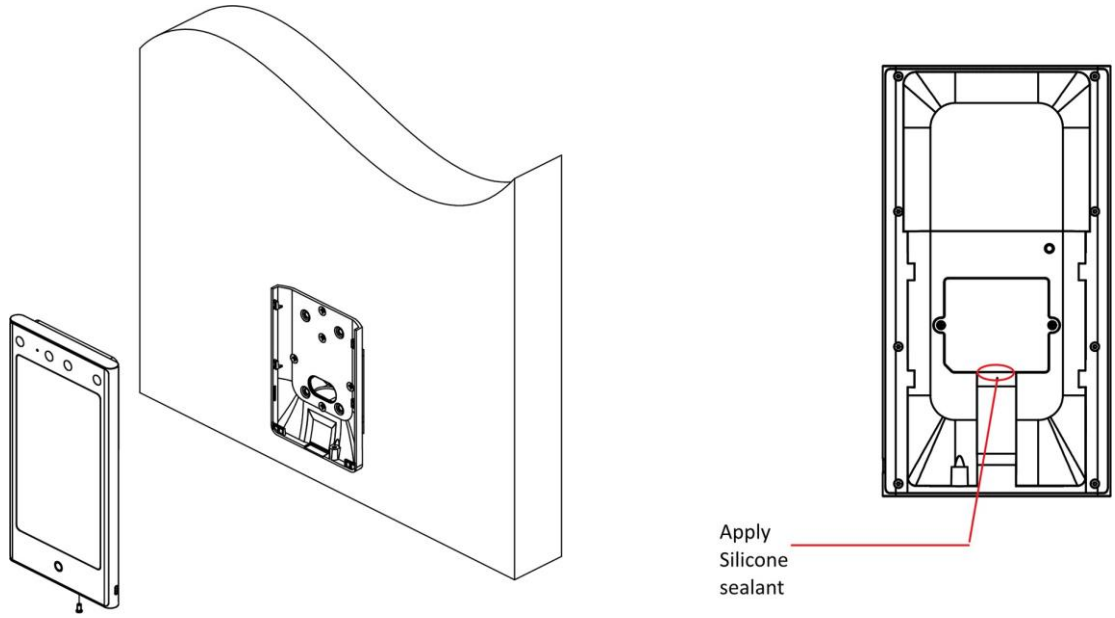


図 1-3 デバイスを固定

注記

ケーブル配線エリアにシリコーンシーラントを塗布し、雨滴の侵入を防止してください。

4. 装置を取付プレートに合わせ、付属のネジ 1 本（SC-KM3X8-T10-SUS-NL）で装置を取付プレートに固定します。

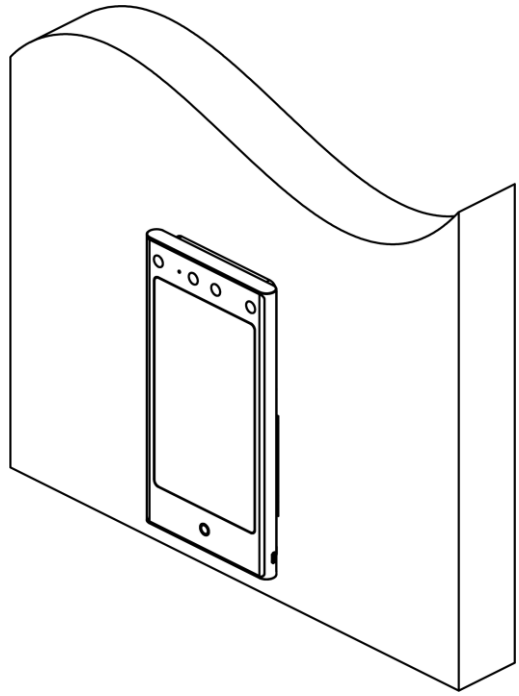


図 1-4 デバイスの固定

5. 取り付け後、デバイスを適切に使用するため（屋外使用）、保護フィルム（付属品の一部）を画面に貼り付けてください。

1.3 表面実装

手順

注記

追加荷重は、機器重量の3倍に等しいものとする。設置中、機器及び関連する取付手段は確実に固定された状態を維持しなければならない。設置後、関連する取付プレートを含む機器に損傷があってはならない。

1. 取り付けテンプレートの基準線に従い、取り付けテンプレートを地面から1.4メートル高い位置の壁面またはその他の表面に貼り付ける。

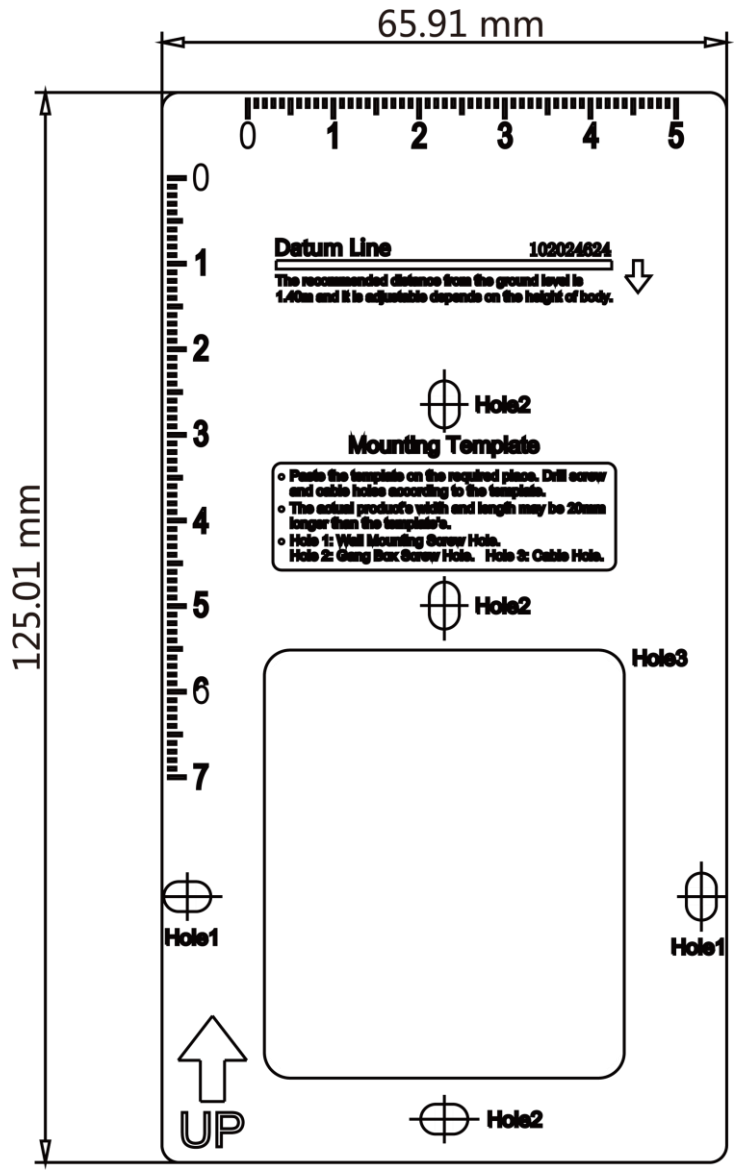


図1-5 取付テンプレート

2. 取り付けテンプレートの穴1の位置に合わせて、壁またはその他の表面に穴を開ける。

3. 工具を使用して取り付けプレートのケーブル穴を開ける。

4. 取り付け穴をマウントプレートに合わせ、付属のネジ2本（SC-KA4x25-SUS）でマウントプレートを壁に固定してください。

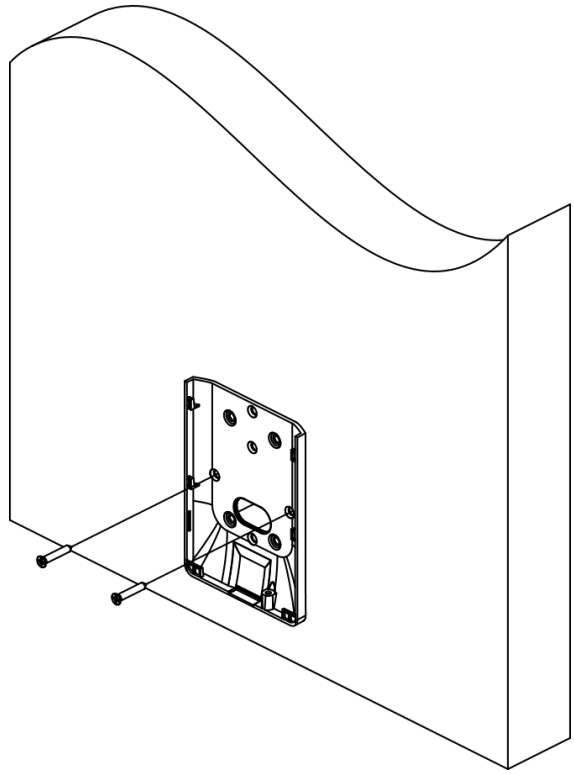


図1-6 取付プレートの取り付け

5. ケーブルをマウントプレートのケーブル穴に通し、対応する周辺機器ケーブルに接続します。

注記

屋外に設置する場合は、配線出口にシリコーンシーラントを塗布し、水の浸入を防止してください。

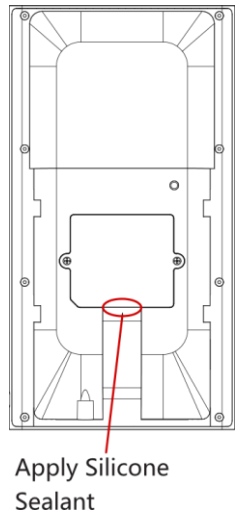


図 1-7 シリコーンシーラントの塗布

6. デバイスを取り付けプレートに合わせ、デバイスを取り付けプレートに吊り下げます。

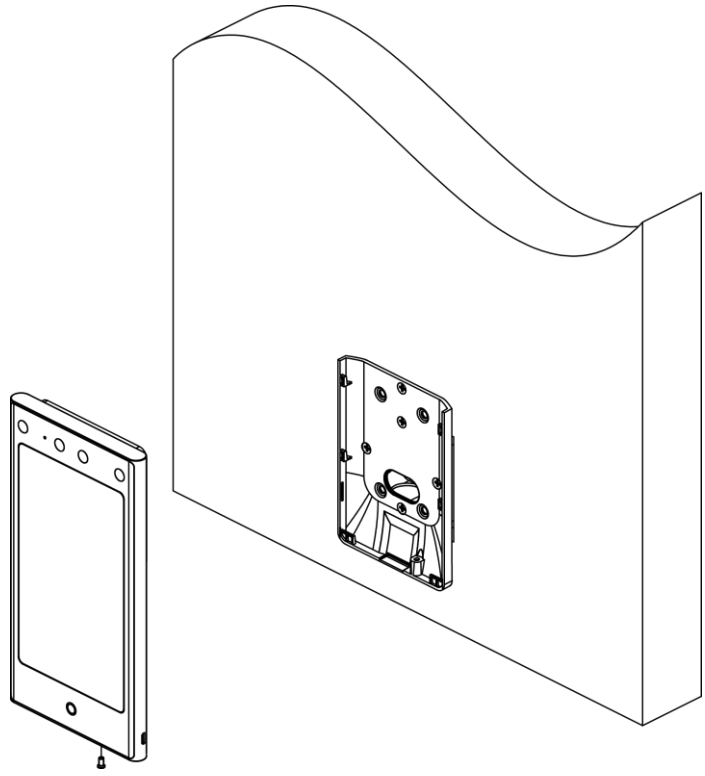


図1-8 デバイスの取り付け

7. 付属のネジ 1 本（SC-KM3X8-T10-SUS-NL）を使用して、デバイスと取り付けプレートを固定します。

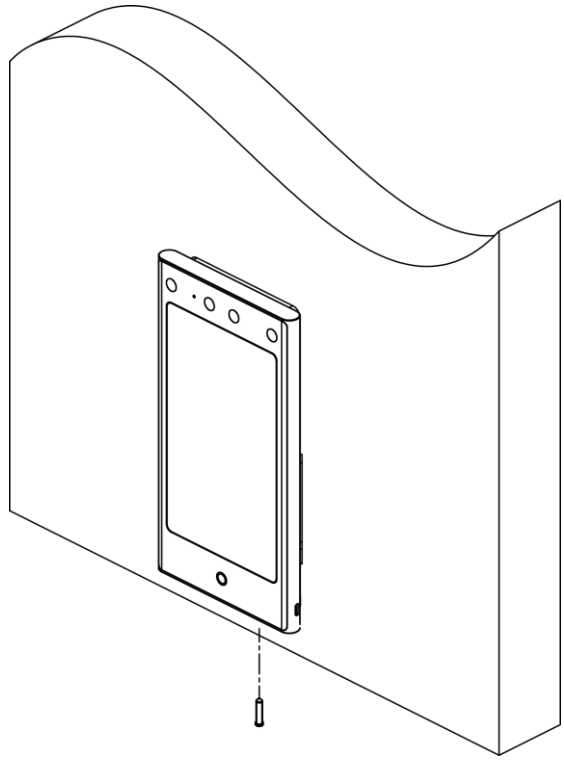


図 1-9 デバイスの固定

8. **オプション：**実際の必要に応じて周辺モジュールを接続してください。
9. 取り付け後、デバイスを適切に使用するため（屋外使用）、保護フィルム（付属モデルの一部）を画面に貼り付けてください。

1.4 ブラケットによる取り付け

1.4.1 ブラケット取付前の準備

手順

1. 下図に示す通り、回転式改札機の表面に穴を開け、防水ナットを取り付けてください。

注意

リベットを圧着した後、はんだ付けを行い、水の侵入を防いでください。

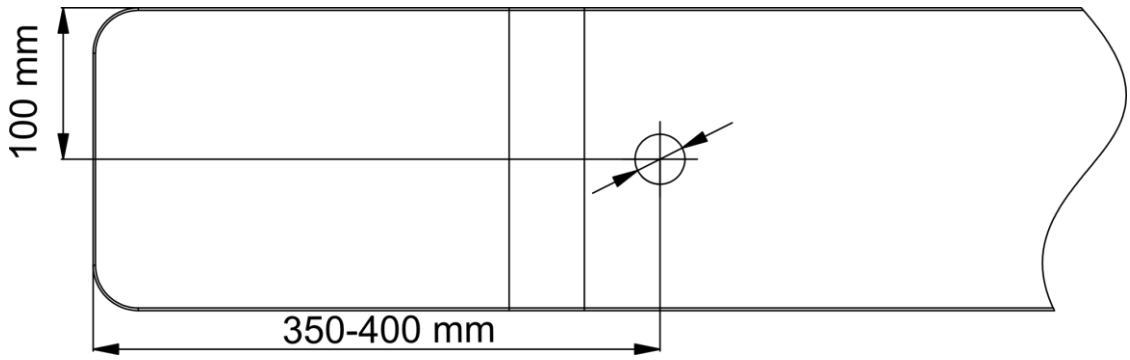


図 1-10 ターンスタイルへの穴あけ

2. 設置角度をターンスタイル本体に対して 180° 垂直にする必要がある場合は、以下の操作が必要です。

1) 下図に示す 3 本のネジを外します。

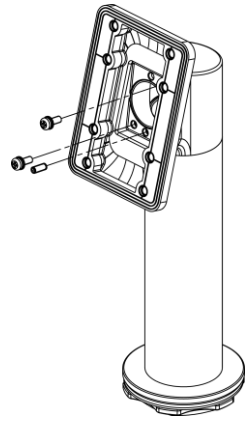


図 1-11 ネジの取り外し

2) 固定部品を180° 回転させ、3本のネジを元に戻して取り付けます。

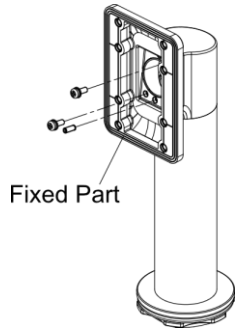


図1-12 固定部の回転

1.4.2 ブラケット取付

取り付け手順

1. ブラケット底部をターンスタイルに通し、付属のナットでターンスタイルに固定します。ブラケットを適切な角度に調整し、レンチでナットをしっかりと固定します。

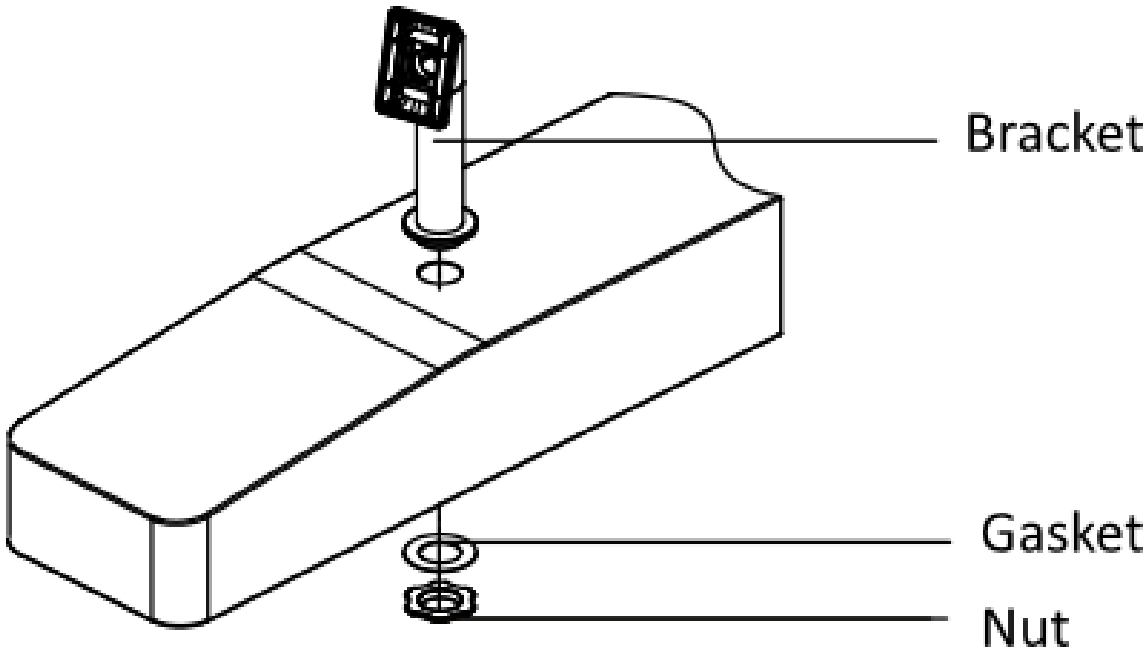


図 1-13 ブラケットの固定

2. 取付プレートをブラケットに 4 本の SC-K1M4×6-SUS ネジで固定します。

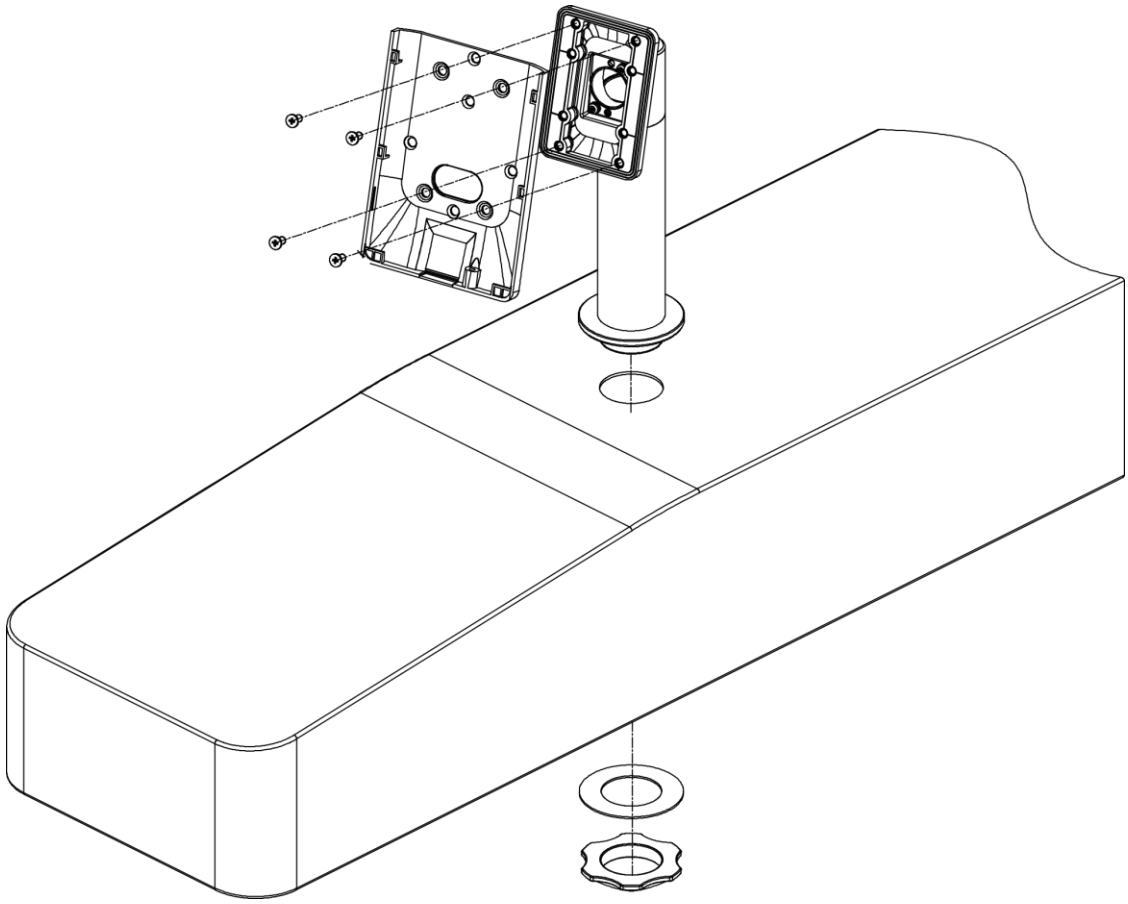


図 1-14 取付プレートの固定

3. 顔認証端末のケーブルをケーブル穴に通し、内側のターンスタイルに挿入します。顔認証端末をSC-KM3X8-T10-SUS-NLネジで取付板に固定します。

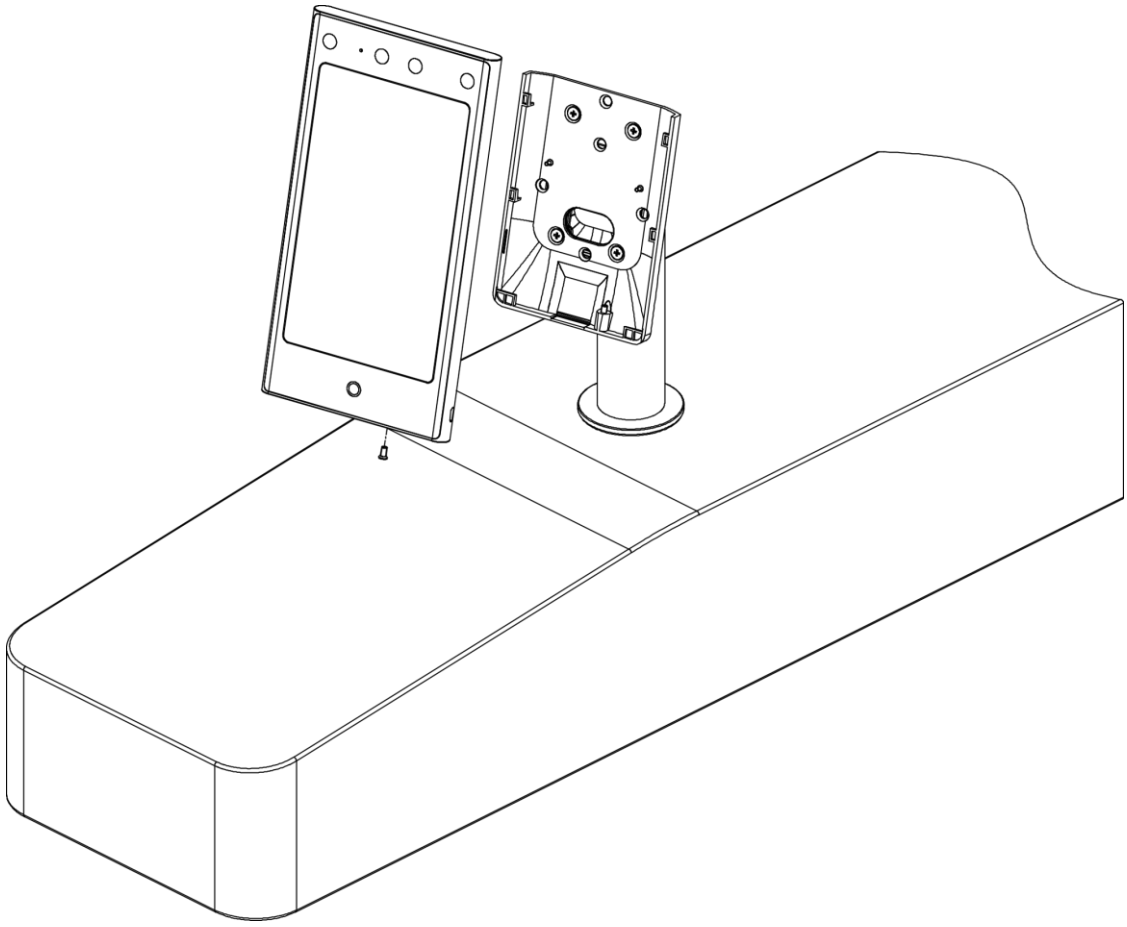


図1-15 固定式顔認証端末

4. 設置後、本装置を適切に使用するため（屋外使用）、保護フィルム（付属品の一部）を画面に貼り付けてください。

1.5 埋め込み設置

手順

1. 埋め込み用ジャンクションボックスを、壁にあらかじめ切られた取り付けスロットに設置します。

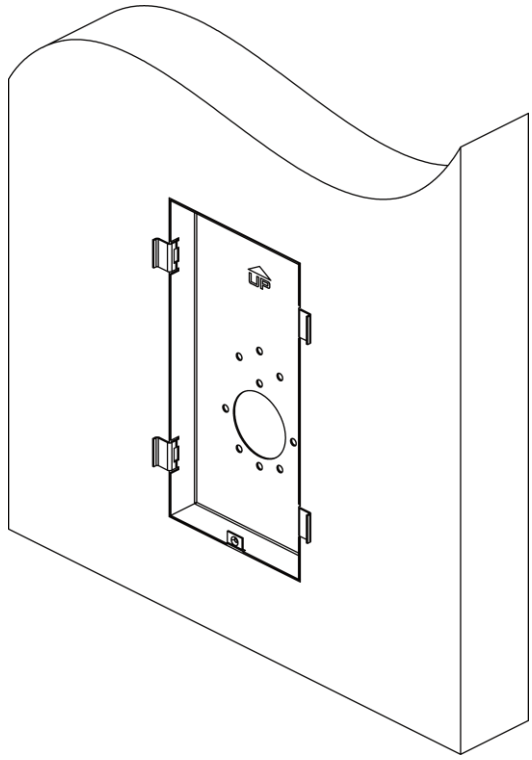


図 1-16 埋め込み型ジャンクションボックスの取り付け

2. 2 本の SC-KA4×25-SUS ネジを使用して、取り付けプレートを埋め込み型ジャンクションボックスに固定します。

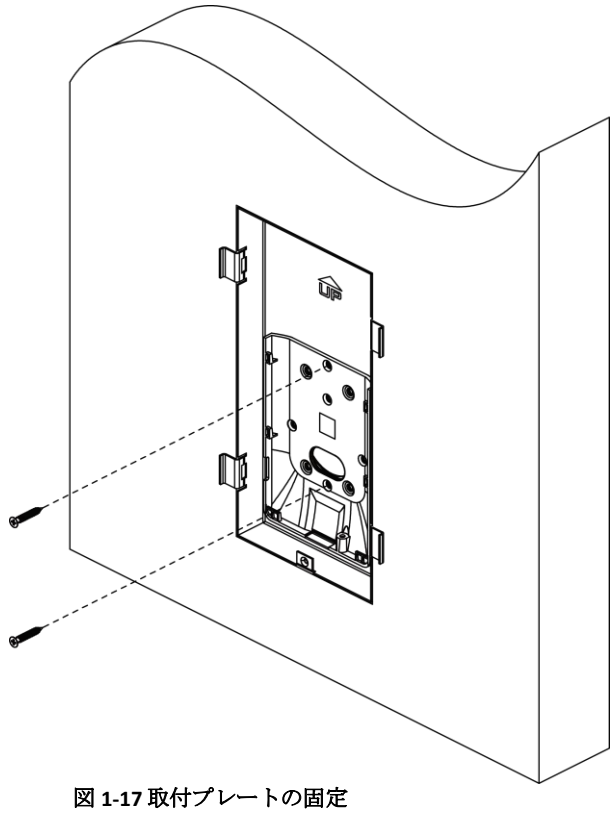


図 1-17 取付プレートの固定

3. 埋め込み型ジャンクションボックスの両側にある取り付け耳を折って外します。ケーブルを接続し、背面インターフェースカバーを再取り付けした後、装置をマウントプレートに上から下へかけて取り付けます。

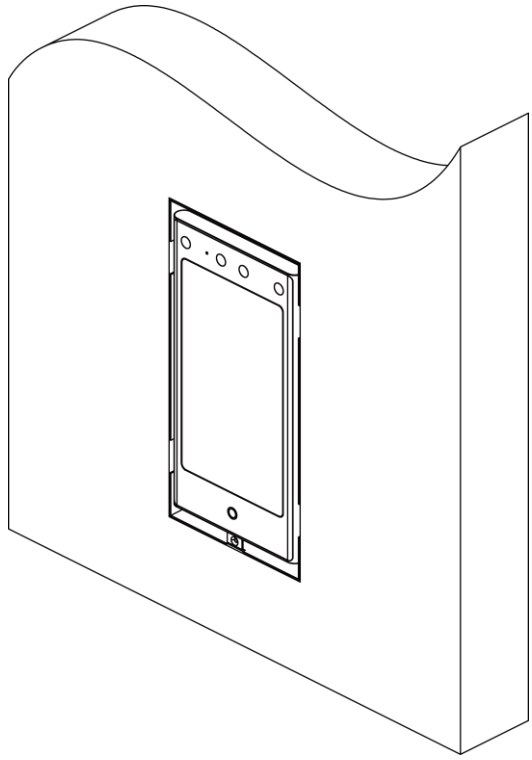


図1-18 取り付け耳の切断とケーブル接続

4. 埋め込み式取り付けパネル上部の2つのフックを、埋め込み式ジャンクションボックス上部の取り付け穴に挿入し、パネルを壁面と面一になるように位置合わせします。

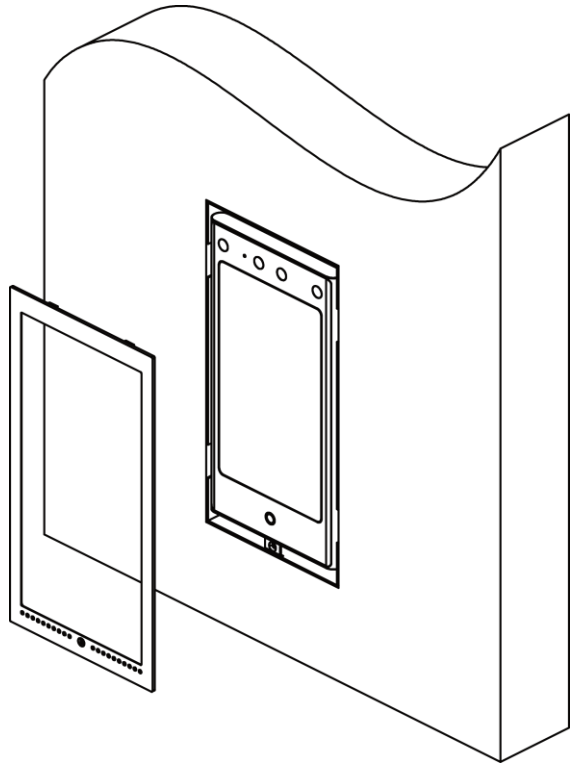


図 1-19 取付パネルのフック挿入

5. 埋め込み型取り付けパネルを埋め込み型ジャンクションボックスに、SC-KM3×6-H2-SUSネジ1本で固定します。

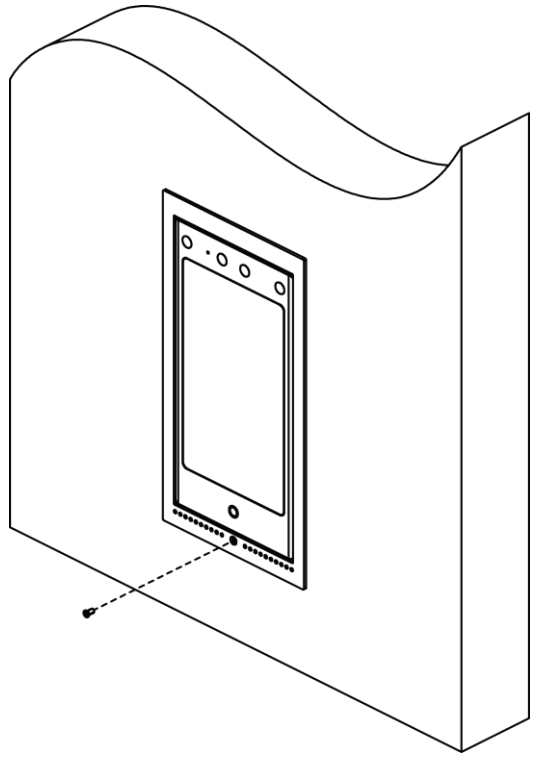


図 1-20 取り付けパネルの固定

6. 取り付け完了。

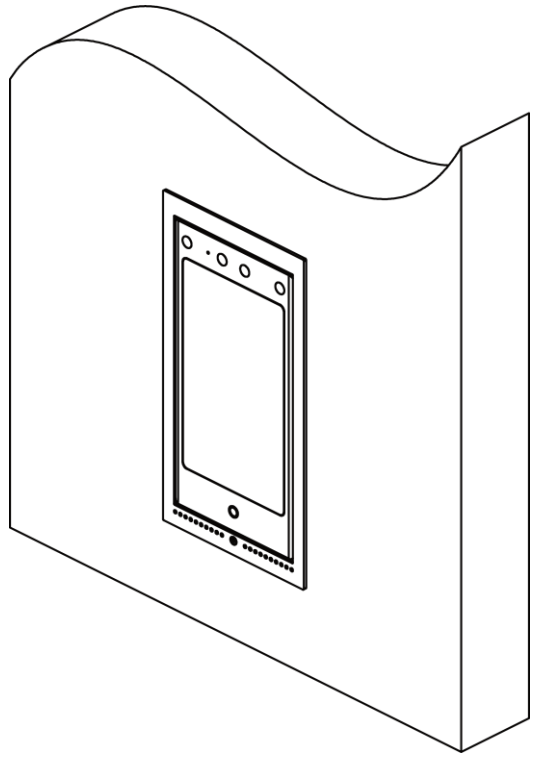


図1-21 完全な設置

第2章 配線

本装置は、RS-485 端末、ドアロック、退出ボタン、警報出力/入力デバイス、ウィーガンドカードリーダー、アクセスコントローラ、および電源への接続に対応しています。以下の説明に従って周辺機器を配線してください。

Wiegandカードリーダーをアクセスコントローラに接続する場合、顔認証端末は認証情報をアクセスコントローラに送信し、アクセスコントローラはドアを開けるかどうかを判断できます。

注意

- ケーブルサイズが18AWGの場合、12Vスイッチング電源を使用してください。また、電源と本装置間の距離は20m以内にしてください。
- ケーブルサイズが15AWGの場合、12Vスイッチング電源を使用してください。また、電源とデバイス間の距離は30mを超えてはいけません。
- ケーブルサイズが12AWGの場合、12Vスイッチング電源を使用してください。また、電源とデバイス間の距離は40mを超えてはいけません。

2.1 端子説明

端子には、電源入力、警報入力、警報出力、RS-485、ウィーガンド出力、ドアロックが含まれます。

端子配置図は以下の通りです：

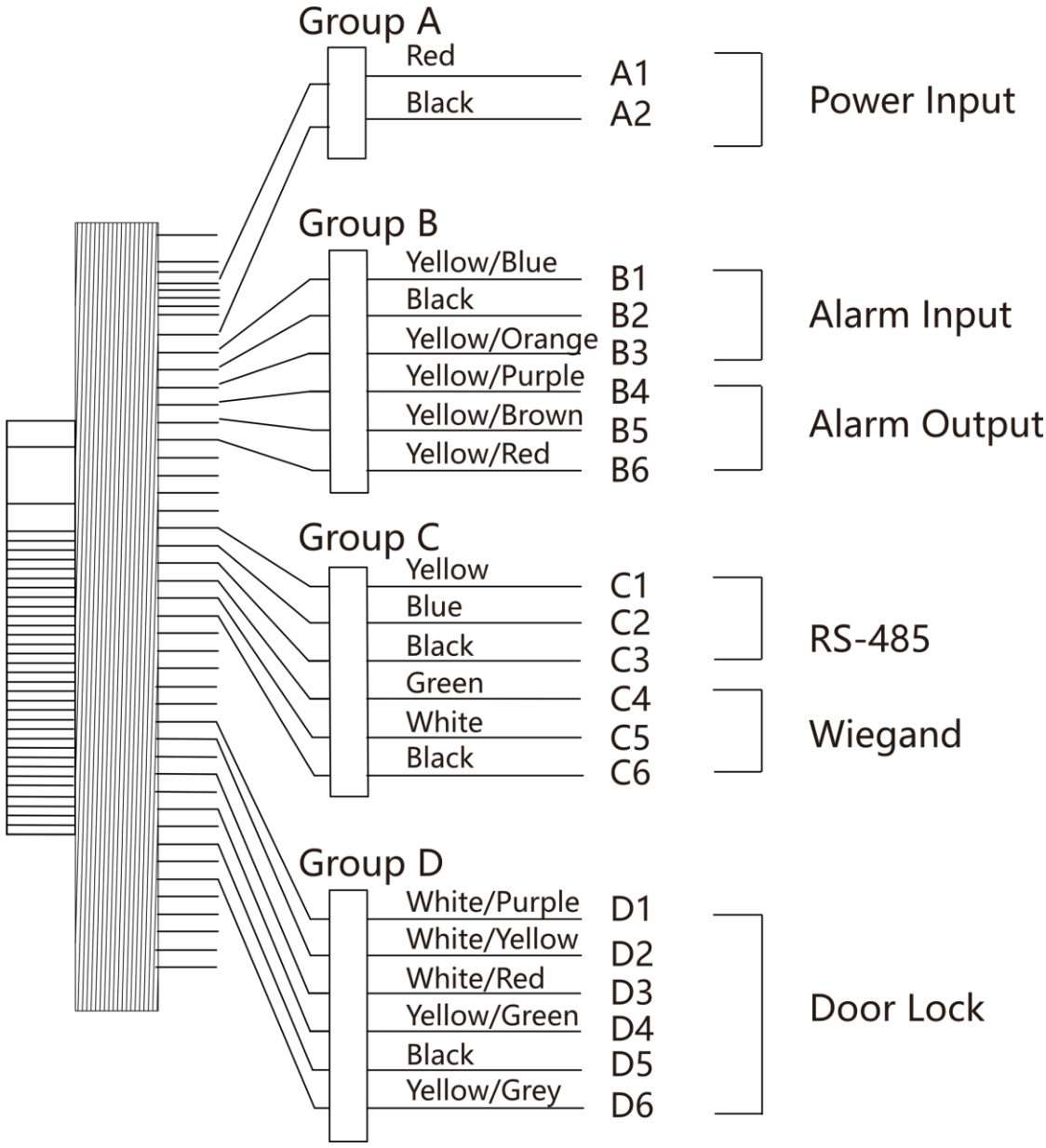


図2-1 端子図

各端子の説明は以下の通りです：

表 2-1 ターミナルの説明

グループ	番号	機能	色	名称	説明
グループ A	A1	入力電力	赤	+12 V	12 VDC 電源
	A2		黒	GND	接地
グループ B	B1	アラーム入力	黄色/青	IN1	警報入力 1
	B2		黒	GND	接地
	B3		黄/オレンジ	IN2	警報入力 2
	B4	警報出力	黄/紫	NC	アラーム出力配線
	B5		黄/茶	COM	
	B6		黄/赤	NO	
グループ C	C1	RS-485	黄色	485+	RS-485 配線
	C2		青	485-	
	C3		黒	GND	接地
	C4	ウィーガンド	緑	W0	ウィーガンド配線 0
	C5		白	W1	ウィーガンド配線 1
	C6		黒	GND	接地
グループ D	D1	ドアロック	白/紫	NC	ロック配線（NC）
	D2		白/黄	COM	共通
	D3		白/赤	NO	ロック配線（NO）
	D4		黄緑	SENSOR	ドアコンタクト
	D5		黒	GND	接地
	D6		黄/灰色	BTN	出口ドア配線

2.2 ワイヤー火災モジュール

2.2.1 電源オフ時にドアが開く配線図

ロックタイプ：陽極ロック、磁気ロック、電気ボルト（NO）

セキュリティタイプ：電源オフ時にドアが開く

シナリオ：消防車アクセスに設置

タイプ1

注記
消防システムがアクセス制御システムの電源を制御します。

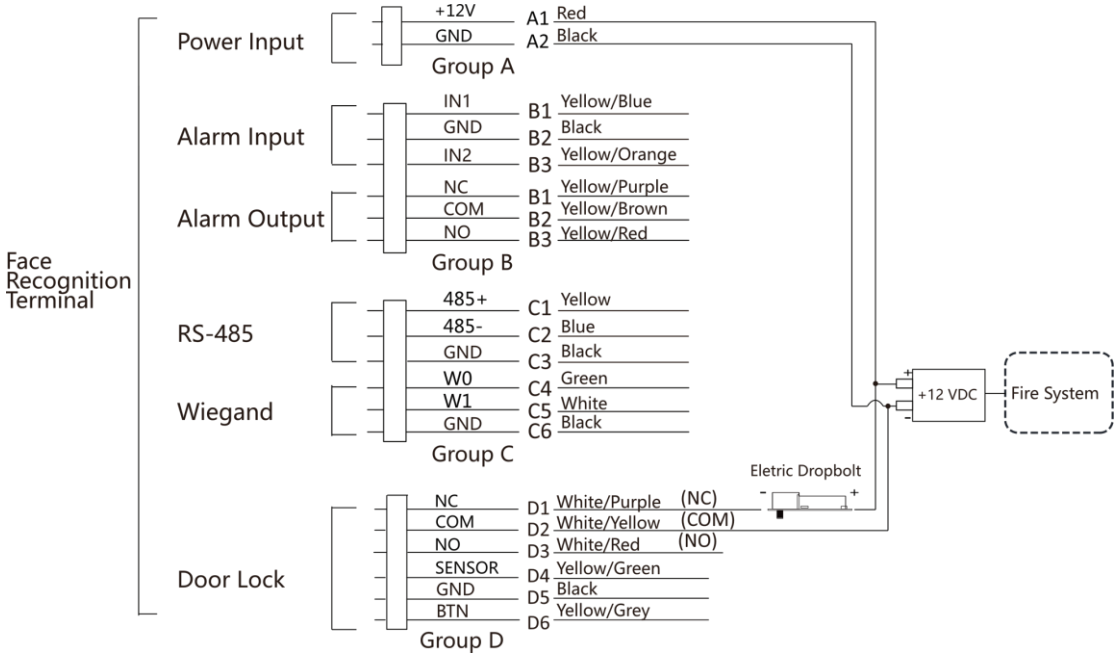


図 2-2 配線装置

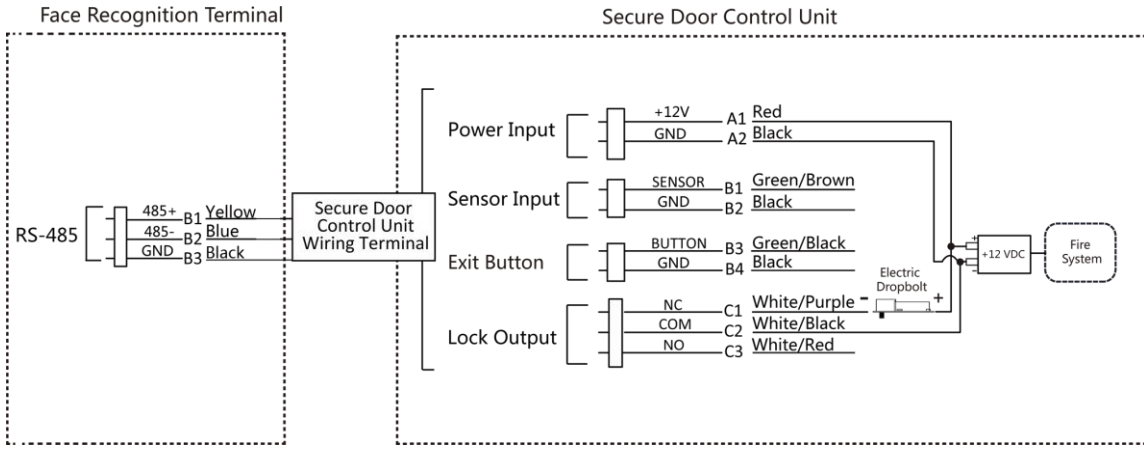


図 2-3 配線式セキュリティドア制御ユニット

タイプ 2

注記

火災システム（NOとCOM、電源オフ時は通常開）は、ロックと電源を直列に接続する。火災警報が作動すると、ドアは開いたままとなる。通常時はNOとCOMは閉状態である。

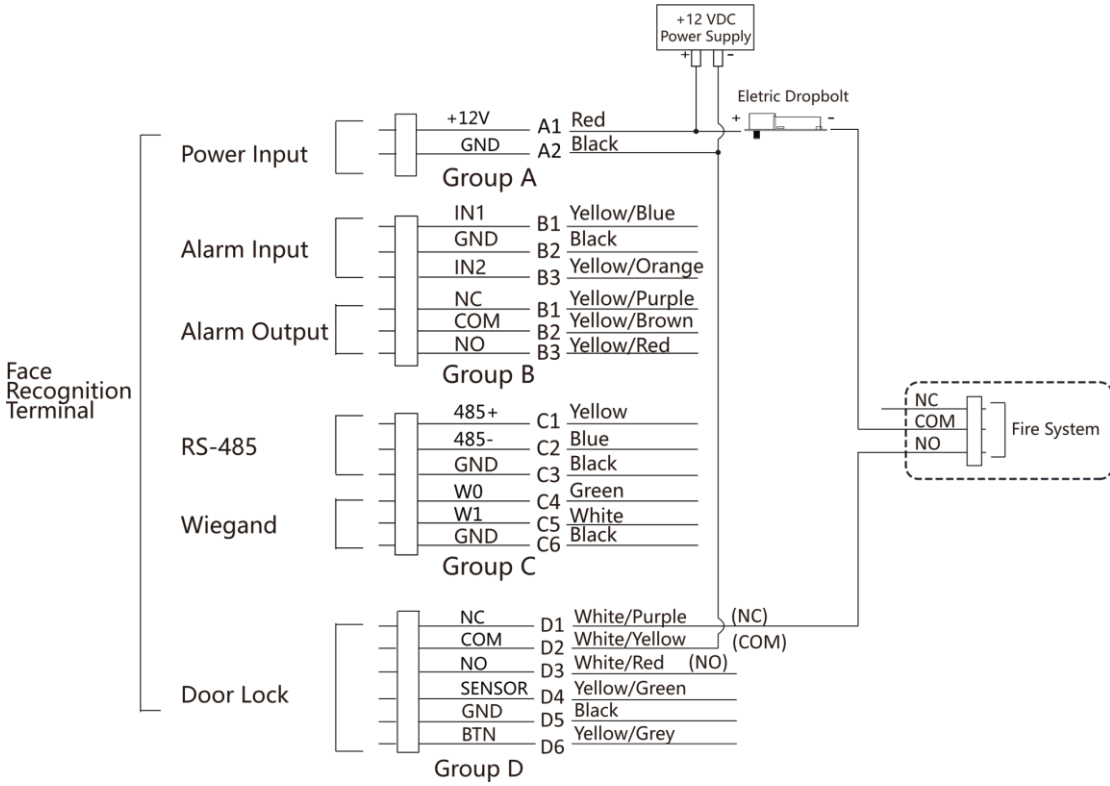


図2-4 配線装置

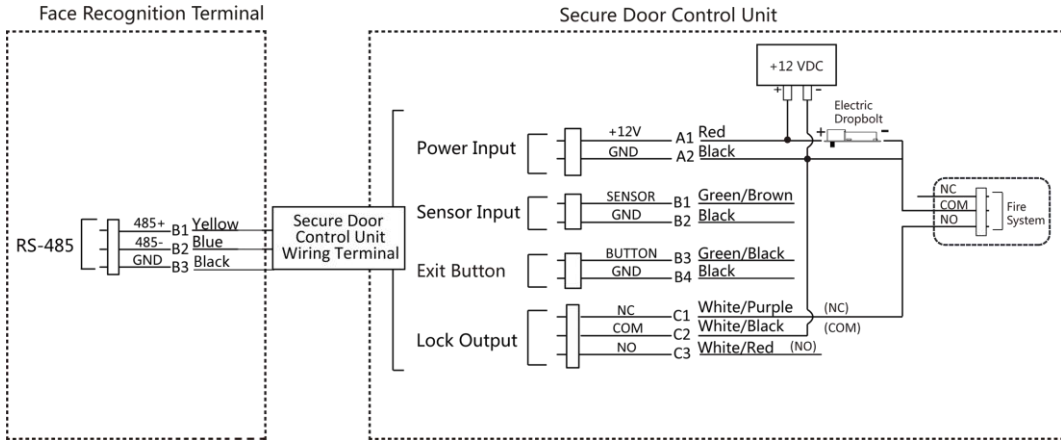


図2-5 セキュアドア制御ユニットの配線

2.2.2 電源オフ時のドアロック配線図

ロックタイプ：カソードロック、電気ロック、電気ボルト（NC）
セキュリティタイプ：電源オフ時にドアロック

シナリオ：火災連動付き出入口への設置

注記

- 無停電電源装置（UPS）が必要です。
- 火災システム（NCとCOM、電源オフ時は通常閉）は、ロックと電源を直列に接続する。火災警報が作動すると、ドアは開いたままとなる。通常時はNCとCOMは開いている。

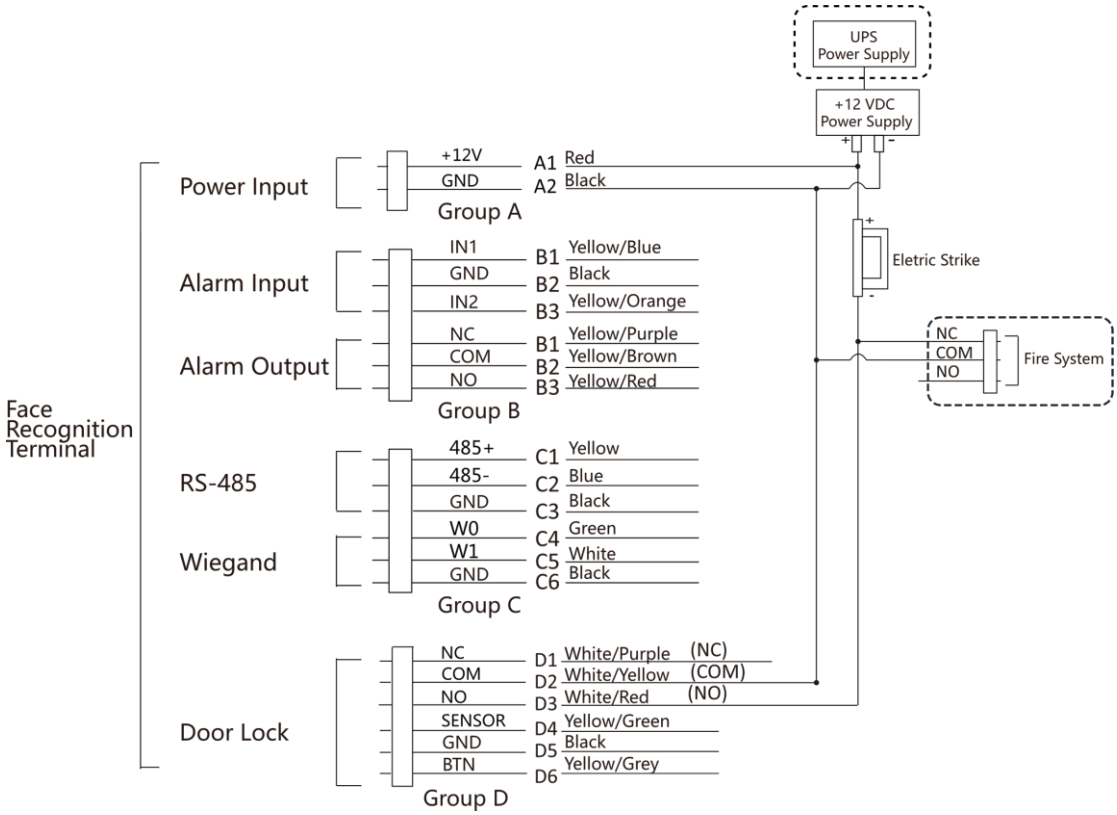


図2-6 装置配線図

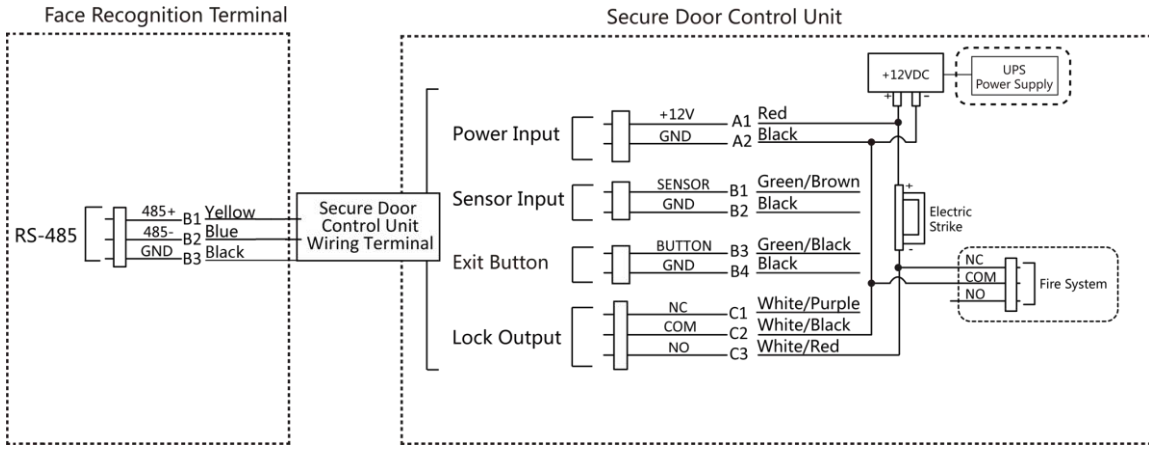

Face Recognition Terminal
Secure Door Control Unit
RS-485
485+
485-
GND
B1
B2
B3
Yellow
Blue
Black
Secure Door Control Unit Wiring Terminal
Power Input
+12V
GND
A1
A2
Red
Black
Sensor Input
SENSOR
GND
B1
B2
Green/Brown
Black
Exit Button
BUTTON
GND
B3
B4
Green/Black
Black
Lock Output
NC
COM
NO
C1
C2
C3
White/Purple
White/Black
White/Red
+12VDC
UPS Power Supply
Electric Strike
NC
COM
NO
Fire System

図2-7 配線図

第3章 手のひら紋様・手のひら静脈認証インジケーターの説明

インジケータ	説明
赤点灯	デバイスがオフラインです。
高速点滅赤	手のひらが近すぎます。
赤（点滅が遅い）	認証に失敗しました。
緑色のライトが3秒間点灯します	認証成功。

第4章 起動

初回ログイン前にデバイスをアクティベートする必要があります。デバイスの電源投入後、システムはデバイスアクティベーションページに切り替わります。

デバイス本体、SADPツール、クライアントソフトウェアによるアクティベーションがサポートされています。デバイスのデフォルト値は以下の通りです：

- デフォルトIPアドレス：192.0.0.64
- デフォルトポート番号：8000
- デフォルトユーザー名：admin

4.1 デバイス経由での起動

デバイスがアクティベートされていない場合、電源投入後にデバイスをアクティベートできます。

デバイスをアクティベートするページで、パスワードを作成し、パスワードを確認します。「**アクティベート**」をタップすると、デバイスがアクティベートされます。

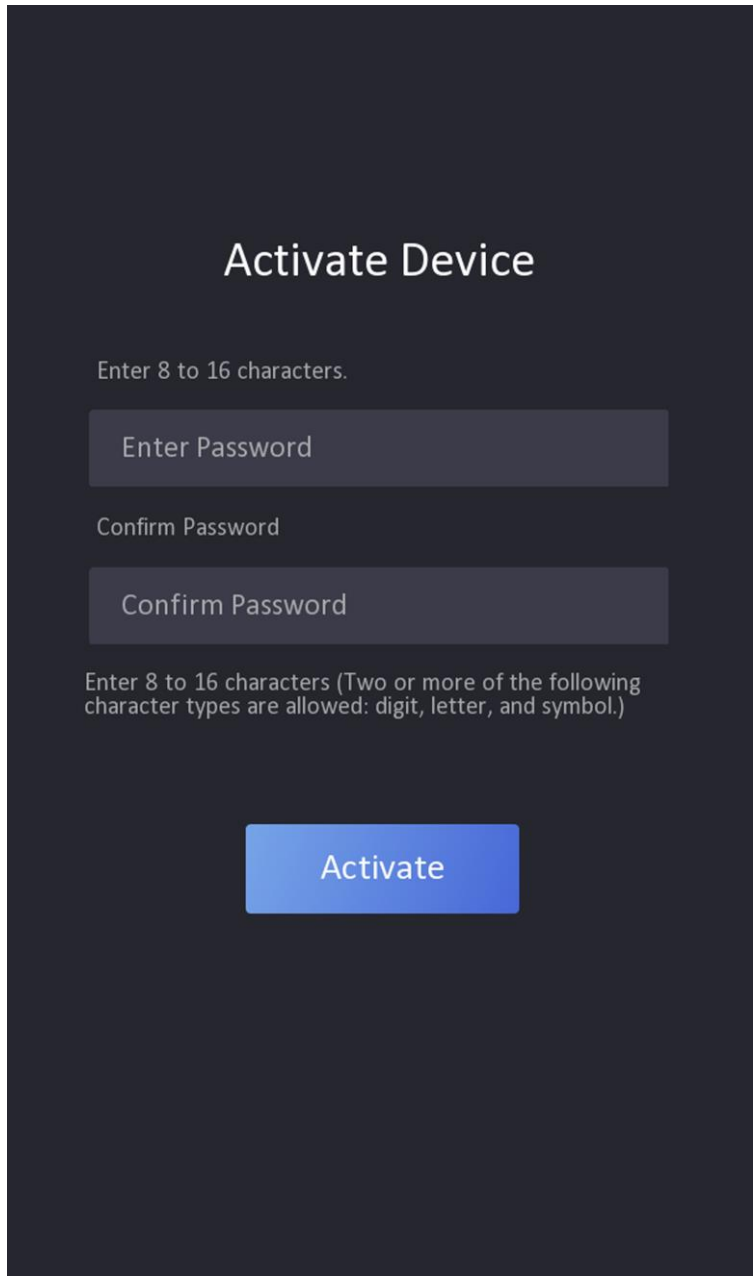


図4-1 起動画面

注意

- 製品のセキュリティを強化するため、デバイスのパスワード強度を自動的にチェックできます。ご自身で選択したパスワード（8文字以上で、大文字、小文字、数字、特殊文字の少なくとも3種類を含む）

に変更することを強く推奨します。また、特に高セキュリティシステムでは、パスワードを定期的に変更することを推奨します。月次または週次での変更により、製品の保護を強化できます。

- すべてのパスワードおよびその他のセキュリティ設定の適切な構成は、サービスプロバイダーおよび／またはエンドユーザーの責任です。
- パスワードには、以下の文字を含めないでください：ユーザー名、123、admin（大文字小文字を区別しない）、4 桁以上の連続した昇順または降順の数字、4 文字以上の連続した繰り返し文字。
- パスワードには、hik、hkws、hikvision などの単語を含めることはできません（大文字と小文字は区別されません）。

4.2 Web ブラウザによる起動

Web ブラウザからデバイスを起動することができます。

手順

1. Web ブラウザのアドレスバーにデバイスのデフォルト IP アドレス (192.0.0.64) を入力し、Enter キーを押します。

Enterキーを押します。

注記

デバイスのIPアドレスとコンピューターのIPアドレスが同じIPセグメントにあることを確認してください。

2. 新しいパスワード（管理者パスワード）を作成し、パスワードを確認してください。

注意

- デバイスのパスワード強度を自動的に確認することができます。製品のセキュリティを強化するため、お客様ご自身で選択したパスワード（大文字、小文字、数字、特殊文字の 3 種類以上を含む 8 文字以上）に変更することを強くお勧めします。また、特にセキュリティレベルの高いシステムでは、パスワードを定期的に変更することをお勧めします。毎月または毎週パスワードを変更することで、製品をより確実に保護することができます。
- すべてのパスワードおよびその他のセキュリティ設定の適切な構成は、サービスプロバイダーおよび／またはエンドユーザーの責任となります。
- パスワードには以下の文字を含めないでください：ユーザー名、123、admin（大文字小文字を区別しない）、4つ以上の連続した昇順または降順の数字、または4つ以上の連続した繰り返し文字。
- パスワードには「hik」、「hkws」、「hikvision」（大文字小文字を区別しない）などの単語を含めることはできません。

3. **[有効化]** をクリックします。

4. デバイスの IP アドレスを編集します。IP アドレスは、SADP ツール、デバイス、およびクライアントソフトウェアを使用して編集できます。

4.3 SADP による起動

SADP は、LAN 上でデバイスの IP アドレスを検出、アクティベート、および変更するためのツールです。

開始前に

- 付属ディスクまたは公式ウェブサイト ***http://www.hikvision.com/en/*** から SADP ソフトウェアを入手し、指示に従って SADP をインストールしてください。
- デバイスとSADPツールを実行するPCは同一サブネット内に配置してください。

以下の手順は、デバイスのアクティベーションと IP アドレスの変更方法を示しています。一括アクティベーションおよび IP アドレスの変更については、*SADP のユーザーマニュアル*を参照してください。

手順

1. SADP ソフトウェアを実行し、オンラインデバイスを検索します。
2. オンラインデバイスリストからご自身のデバイスを探して選択してください。
3. 新しいパスワード（管理者パスワード）を入力し、パスワードを確認してください。

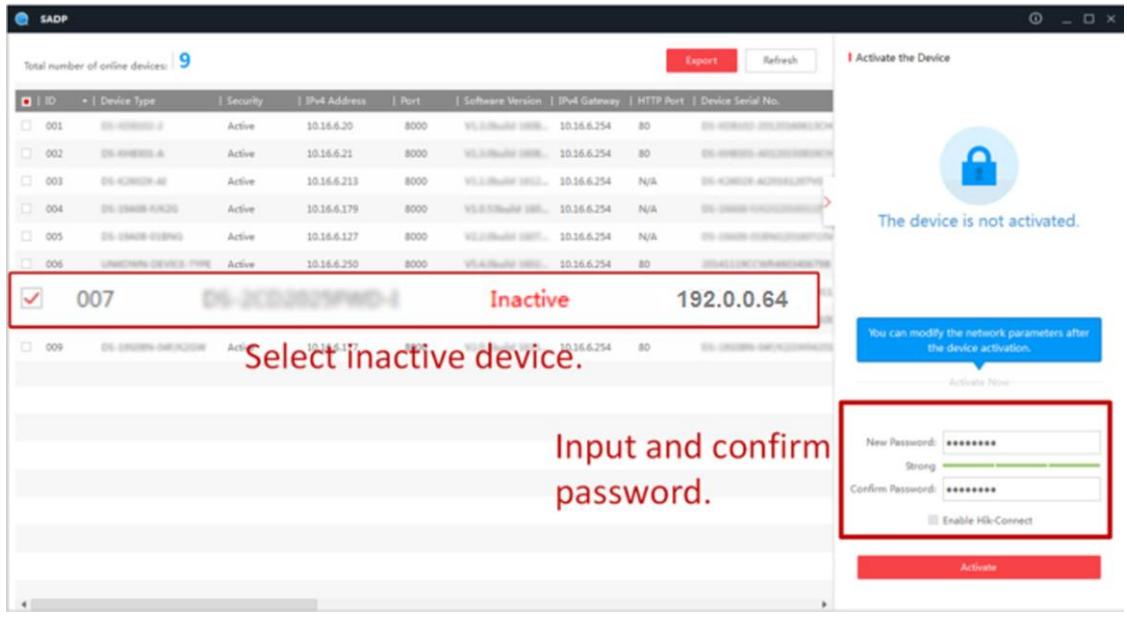
注意

強力なパスワードの使用を推奨 - 製品のセキュリティを強化するため、お客様自身で強力なパスワード（大文字、小文字、数字、特殊文字を含む 8 文字以上）を作成することを強くお勧めします。また、特にセキュリティレベルの高いシステムでは、パスワードを定期的に（毎月または毎週）リセットすることで、製品をより確実に保護することができます。

注記

admin および nimda を含む文字は、アクティベーションパスワードとして設定できません。

4. **アクティベート**をクリックしてアクティベーションを開始してください。



デバイスのステータスは、アクティベーションが成功すると「**アクティブ**」になります。

5. デバイスのIPアドレスを変更します。
   1) デバイスを選択します。
   2) IP アドレスを手動で変更するか、**[DHCP を有効にする]** をチェックして、デバイスの IP アドレスをコンピュータと同じサブネットに変更します。
   3) 管理者パスワードを入力し、「**変更**」をクリックして IP アドレスの変更を有効にします。

4.4 iVMS-4200 クライアントソフトウェアによるデバイスの起動

一部のデバイスでは、iVMS-4200 ソフトウェアに追加して正常に動作させる前に、アクティベート用のパスワードを作成する必要があります。

手順

注
この機能はデバイスでサポートされている必要があります。

1. デバイス管理ページに入ります。
2. **デバイス管理**の右側にある「 」をクリックし、「**デバイス**」を選択します。
3. **オンラインデバイスを**クリックしてオンラインデバイス領域を表示します。検索されたオンラインデバイスがリストに表示されます。
4. デバイスのステータス（セキュリティレベル列に表示）を確認し、非アクティブなデバイスを選択します。
5. 「**アクティベート**」をクリックしてアクティベーションダイアログを開きます。
6. パスワードフィールドにパスワードを入力し、パスワードを確認します。

注意

デバイスのパスワード強度を自動で確認できます。製品のセキュリティ強化のため、ご自身で選択したパスワード（8文字以上で、大文字、小文字、数字、特殊文字の少なくとも3種類を含む）への変更を強く推奨します。また、特に高セキュリティシステムでは、パスワードを定期的に変更することをお勧めします。月次または週次での変更により、製品をより効果的に保護できます。
すべてのパスワードおよびその他のセキュリティ設定の適切な構成は、設置業者および/またはエンドユーザーの責任となります。

注記

admin および nimda を含む文字は、アクティベーションパスワードとして設定できません。

7. **[OK]**をクリックしてデバイスをアクティベートします。

第5章 クイック操作

5.1 言語の選択

デバイスのシステム言語を選択できます。

デバイスのアクティベーション後、デバイスシステムの言語を選択できます。

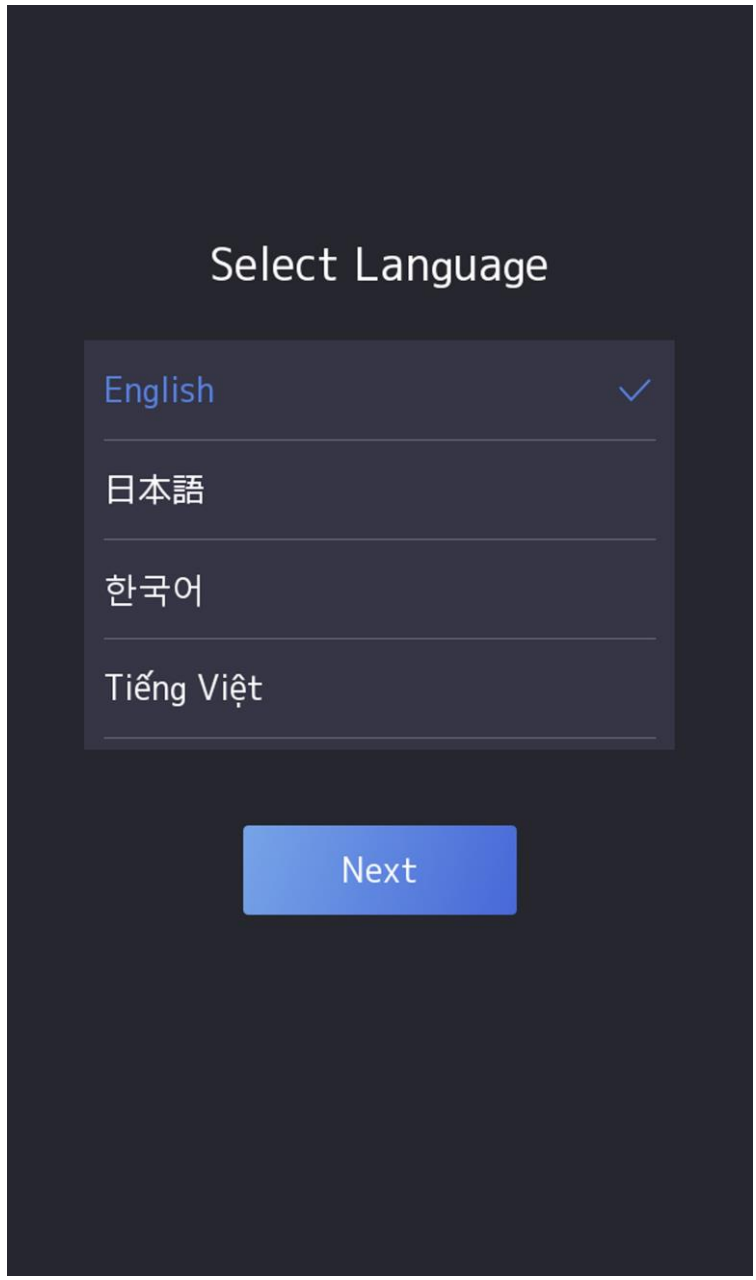


図 5-1 システム言語の選択

デフォルトでは、システム言語は英語です。

注

システム言語を変更すると、デバイスは自動的に再起動します。

5.2 パスワード変更方法の設定

パスワード変更タイプは、登録済みメールアドレスまたはセキュリティ質問として設定できます。デバイスのパスワードを忘れた場合、選択した変更タイプを通じてパスワードを変更できます。

メールアドレス経由でのパスワード変更

予約メールアドレス経由でパスワードを変更する場合は、メールアドレスを入力し、「**次へ**」をタップしてください。

セキュリティ質問による変更

セキュリティの質問でパスワードを変更する必要がある場合は、右隅の「**セキュリティの質問に変更**」をタップしてください。右隅にある「セキュリティ質問に変更」をタップしてください。セキュリティ質問を選択し、回答を入力します。「**次へ**」をタップしてください。

注意

パスワード変更には1種類の方法のみ選択可能です。両方の変更方法を設定する場合は、ウェブページにアクセスしてください。

5.3 ネットワークパラメータの設定

デバイスのネットワークを設定できます。

手順

注意

一部のデバイスモデルはWi-Fi機能をサポートしています。詳細は実際のデバイスをご確認ください。

1. ネットワーク選択画面が表示されたら、実際のニーズに応じて「**有線ネットワーク**」または「**Wi-Fi**」をタップしてください。

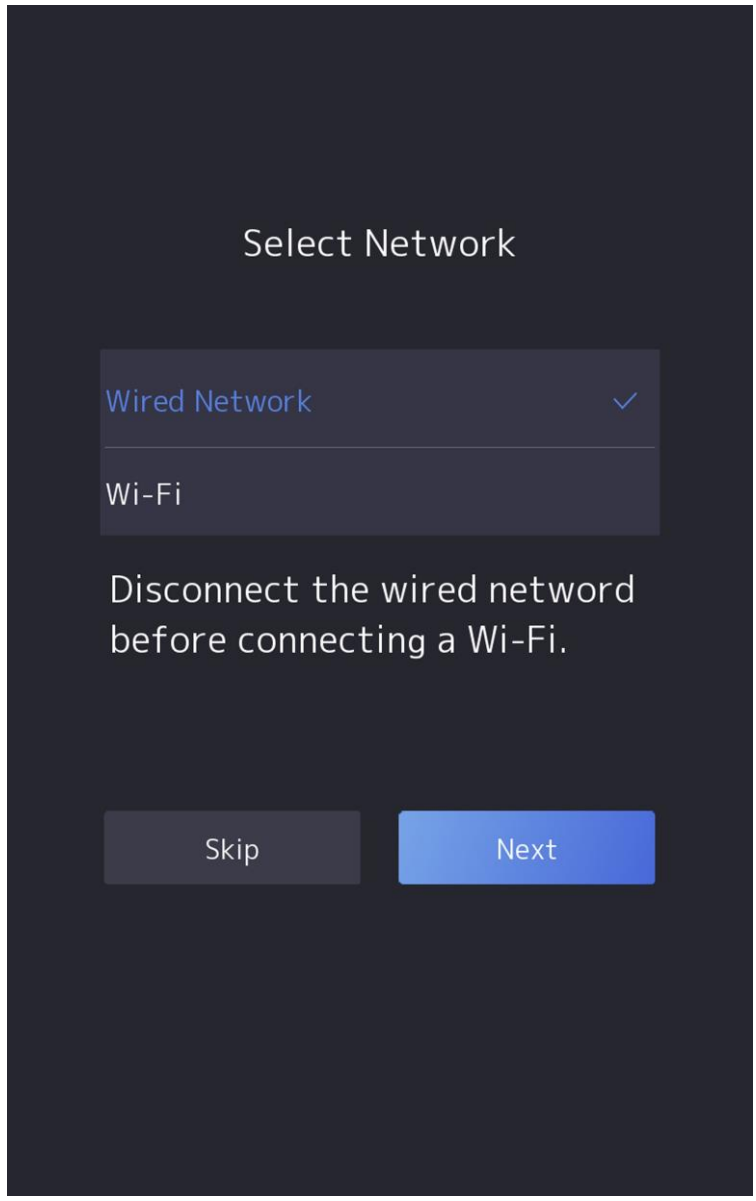


図5-2 ネットワークの選択

注意
Wi-Fi に接続する前に、有線ネットワークを切断してください。

2. **[次へ]** をタップ
   有線ネットワーク

注
デバイスがネットワークに接続されていることを確認してください。

DHCPを有効にすると、システムがIPアドレスやその他のパラメータを自動的に割り当てます。**DHCPを**無効にする場合は、IPアドレス、サブネットマスク、ゲートウェイを設定する必要があります。

Wi-Fi

Wi-Fiを選択し、Wi-Fiのパスワードを入力して接続します。

または「**Wi-Fiを追加**」をタップし、Wi-Fi名とパスワードを入力して接続します。

3. オプション：ネットワーク設定をスキップするには「**スキップ**」をタップします。

5.4 プラットフォームへのアクセス

この機能を有効にすると、デバイスは Hik-Connect 経由で通信できるようになります。デバイスを Hik-Connect モバイルクライアントなどに追加できます。

手順

1. Hik-Connectへのアクセスを有効にし、サーバーIPと認証コードを設定してください。

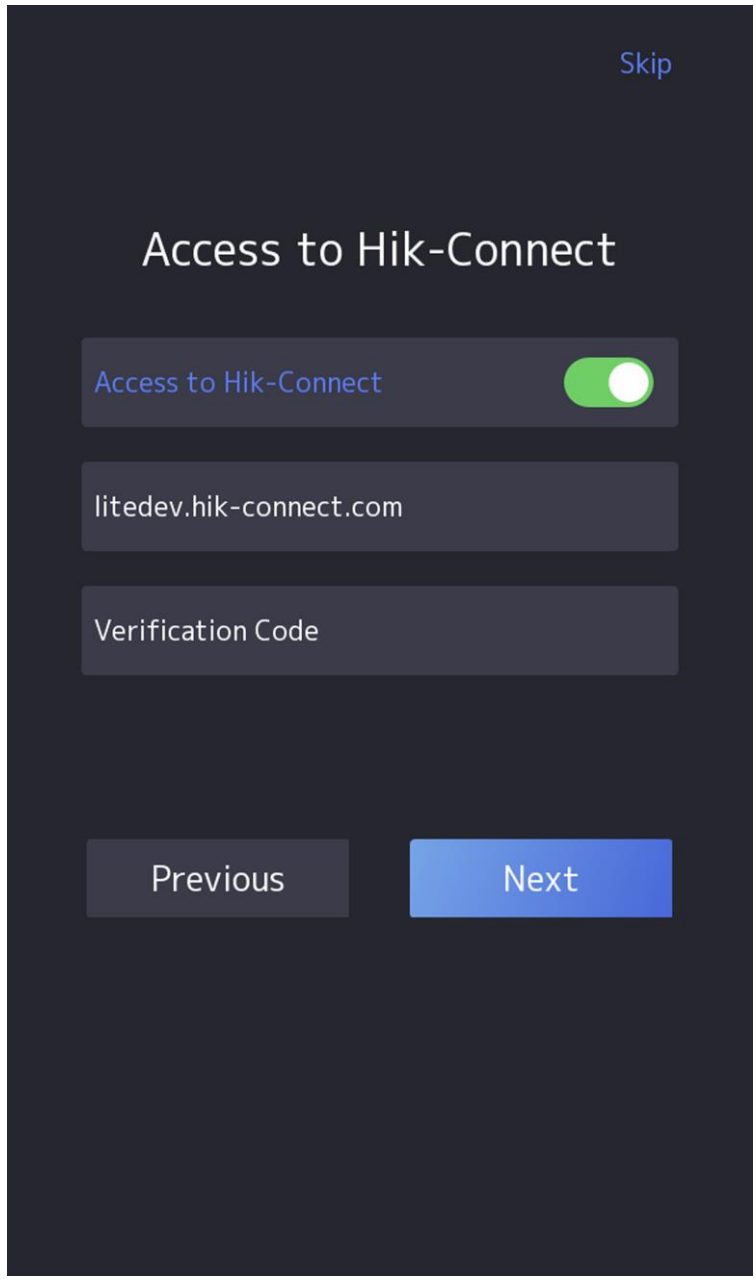


図5-3 Hik-Connectへのアクセス

2. **「次へ」**をタップします。
3. **オプション：**この手順をスキップするには**「スキップ」**をタップします。
4. **オプション：「前へ」**をタップすると前のページに戻ります。

注

前のページに戻るをタップしてWi-Fi設定ページに戻った場合、接続済みのWi-Fiを再度タップするか、別のWi-Fiに接続してプラットフォームページに再度アクセスする必要があります。

5.5 プライバシー設定

起動後、アプリケーションモードの選択、ネットワークの選択を行った後、画像のアップロードや保存など、プライバシーに関するパラメータを設定してください。

実際のニーズに応じてパラメータを選択してください。

認証時に撮影した画像をアップロード

認証時に撮影した画像を自動的にプラットフォームにアップロードします。

認証時に撮影画像を保存（認証時に撮影画像を保存）

この機能を有効にすると、デバイスへの認証時に画像を保存できます。

登録済み画像を保存（登録済み画像を保存）

この機能を有効にすると、登録された顔写真がシステムに保存されます。

リンク撮影後の画像アップロード（リンク撮影後の画像アップロード）

リンクされたカメラで撮影した画像を自動的にプラットフォームにアップロードします。

リンク撮影後の画像保存（リンク撮影後の画像保存）

この機能を有効にすると、リンクされたカメラで撮影した画像をデバイスに保存できます。

通話中の撮影画像をアップロード

通話中に撮影した画像を自動的にプラットフォームにアップロードします。

設定を完了するには「**次へ**」をタップしてください。

5.6 管理者設定

デバイスをアクティベートした後、デバイスのパラメータを管理する管理者を追加できます。

開始前に

デバイスをアクティベートし、アプリケーションモードを選択してください。

手順

1. **オプション：**必要に応じて「**スキップ**」をタップし、管理者の追加をスキップします。
2. 管理者の名前（任意）を入力し、「**次へ**」をタップします。

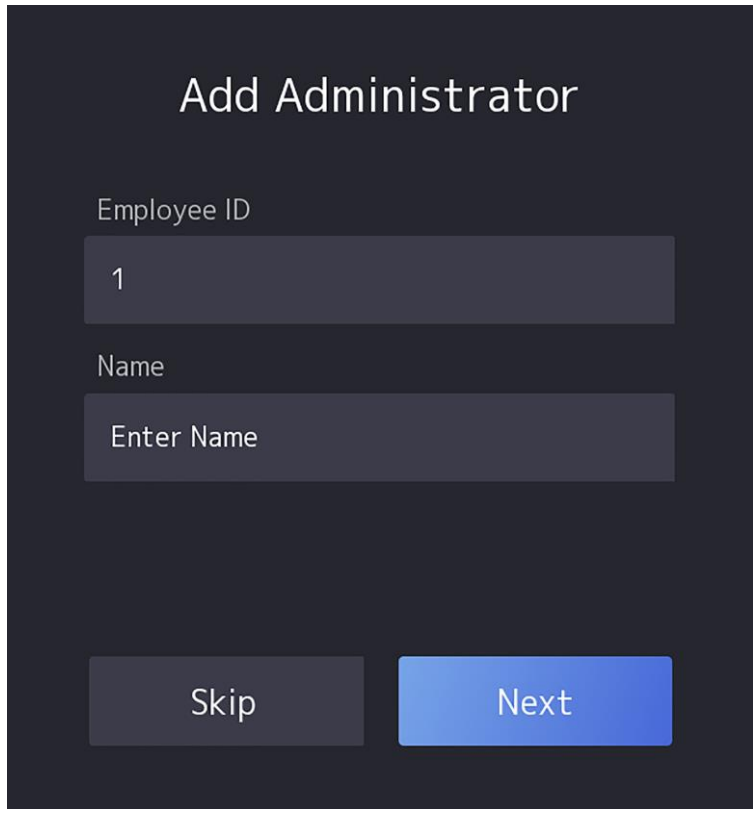


図 5-4 管理者の追加ページ

3. 追加する認証情報を選択します。

注

追加できる認証情報は1つまでです。

- カメラに向かって正面を向いてください。顔が顔認識エリア内にあることを確認してください。をクリックして撮影し、をクリックして確認してください。
- : デバイス画面の指示に従って指を押してください。をクリックして確認します。
- : カード番号を入力するか、カード提示エリアにカードを提示してください。**OK**をクリックしてください。

注意

外部指紋モジュールに接続された端末のみ指紋認証機能をサポートします。

4. **OK**をクリックしてください。

認証ページが表示されます。

5.7 認証ページの手順

認証ページについて

ステータスバーの説明

/

デバイスは武装状態/非武装状態です。

/ /

デバイスのWi-Fiが有効で信号が強い/Wi-Fiは有効だが接続されていない/Wi-FiのIPアドレスが競合している。

/ /

デバイスの有線ネットワークは接続中/未接続/接続失敗。

/ / / /

デバイスのモバイルネットワークは、信号なし/2G 強い信号/3G 強い信号/4G 強い信号/5G 強い信号です。

/

デバイスはVoIPに追加されました/VoIPに追加されませんでした。

/ /

デバイスのSIPサーバーは登録済み/登録失敗/ドアステーションには登録済みだがメインステーションには未登録。

/

掌紋・掌静脈モジュールはオンラインまたはオフラインです。

デュアル周波数カードモジュールはオンライン状態です。

認証ページアイコン

注記

認証ページに表示されるアイコンは制御可能です。詳細は、***デバイス経由でのショートカットキー設定***のショートカットキー***設定***を参照してください。

QRコードをカメラにかざすと、QRコード経由で認証できます。

- 部屋番号を入力し、**OK**をタップして呼び出します。
- をタップしてセンターに電話します。

注意

デバイスはセンターに追加されている必要があります。追加されていない場合、呼び出し操作は失敗します。

認証用の PIN を入力してください。

第6章 基本操作

6.1 ログイン

デバイスの基本パラメータを設定するために、デバイスにログインします。

6.1.1 管理者によるログイン

デバイスに管理者を追加した場合、デバイスの操作には管理者だけがログインできます。

手順

1. 初期画面を3秒間長押しし、ジェスチャーに従って左/右にスライドして管理者ログイン画面に入ります。

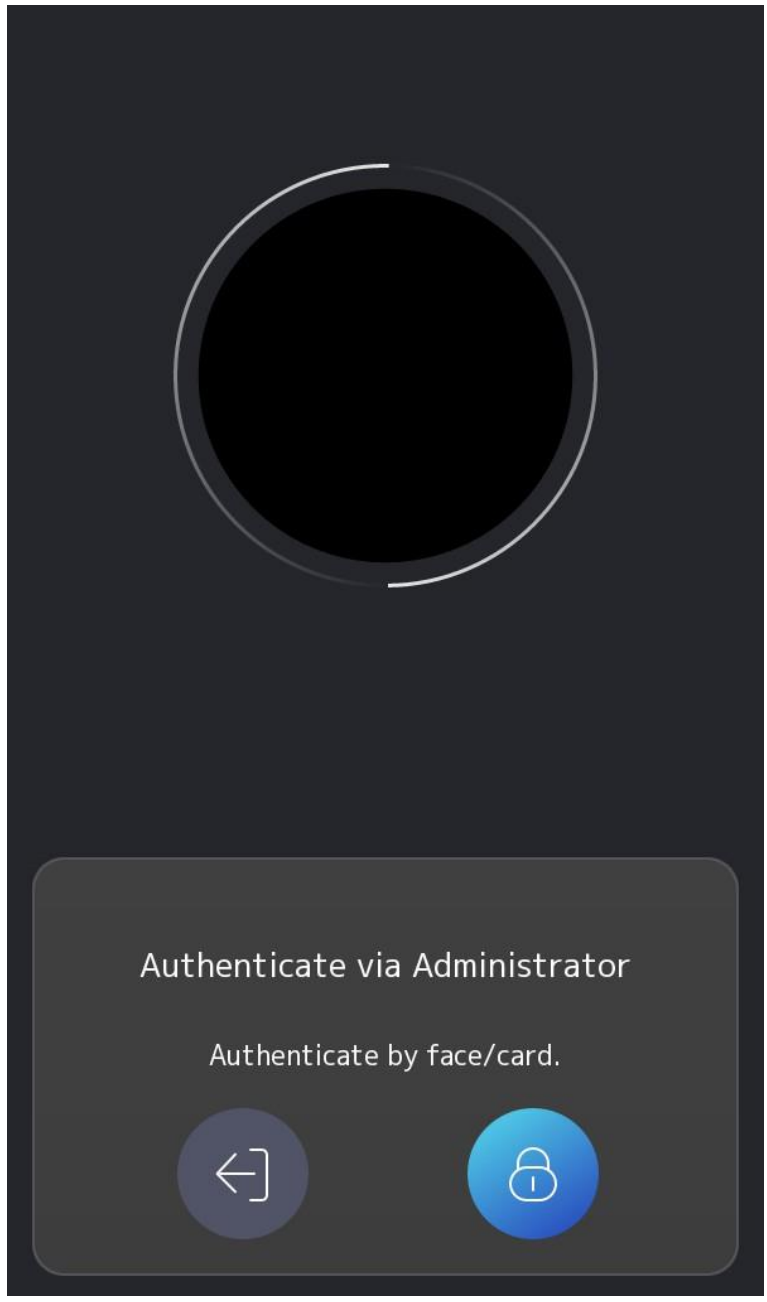


図6-1 管理者ログイン

2. 管理者の顔認証、指紋認証、またはカード認証を行い、ホームページに入ります。

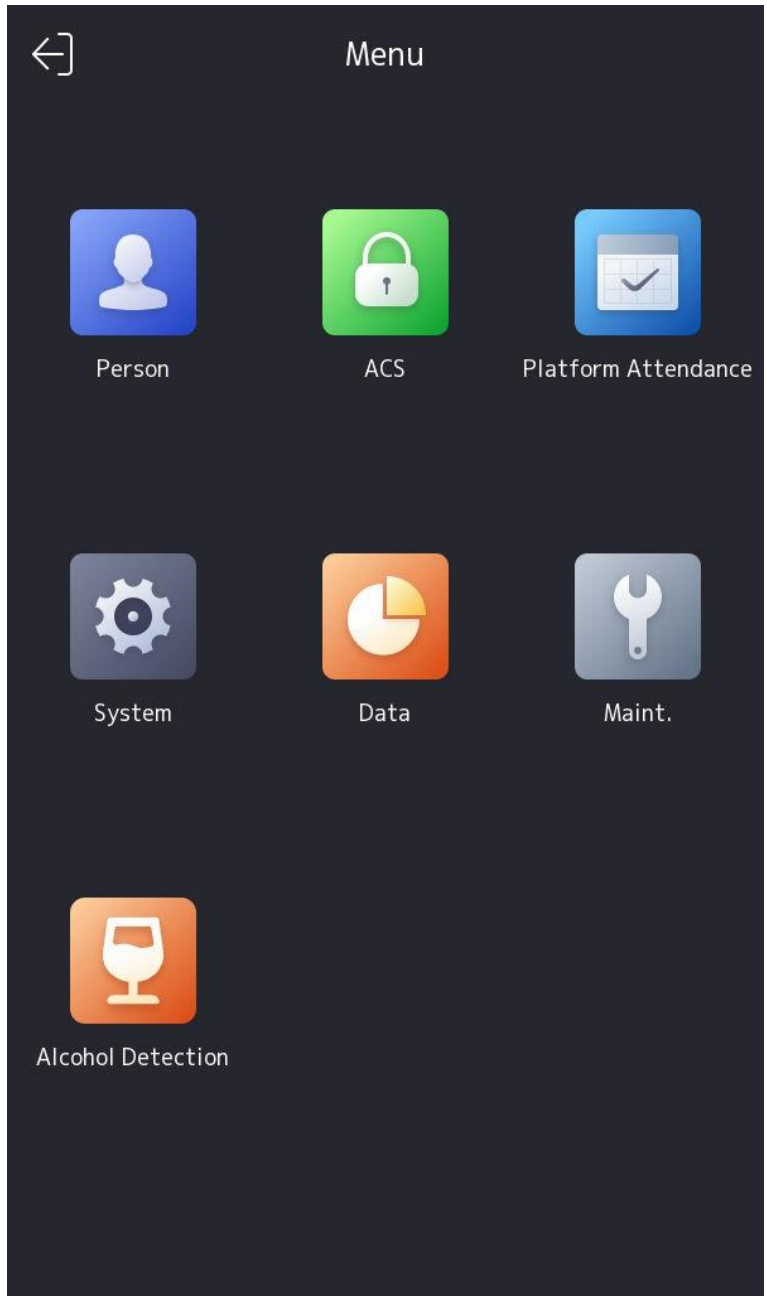


図 6-2 ホームページ

注記
指紋認証またはカード認証の試行が5回失敗すると、デバイスは30分間ロックされます。

3. **オプション：** をタップすると、ログイン用のデバイスアクティベーションパスワードを入力できます。
4. **オプション：** をタップすると、管理者ログインページを終了できます。

6.1.2 起動パスワードによるログイン

他のデバイス操作の前に、システムにログインする必要があります。管理者を設定していない場合は、以下の手順に従ってログインしてください。

手順

1. 初期画面を 3 秒間長押しし、ジェスチャーに従って左/右にスライドしてパスワード入力ページに入ります。
2. パスワードを入力してください。
   - デバイスの管理者を追加している場合は、［ ］をタップし、パスワードを入力してください。
   - デバイスの管理者アカウントを追加していない場合は、パスワードを入力してください。
3. **OK** をタップしてホームページに入ります。

注

パスワードの入力ミスが 5 回続くと、30 分間デバイスのロックがかかります。

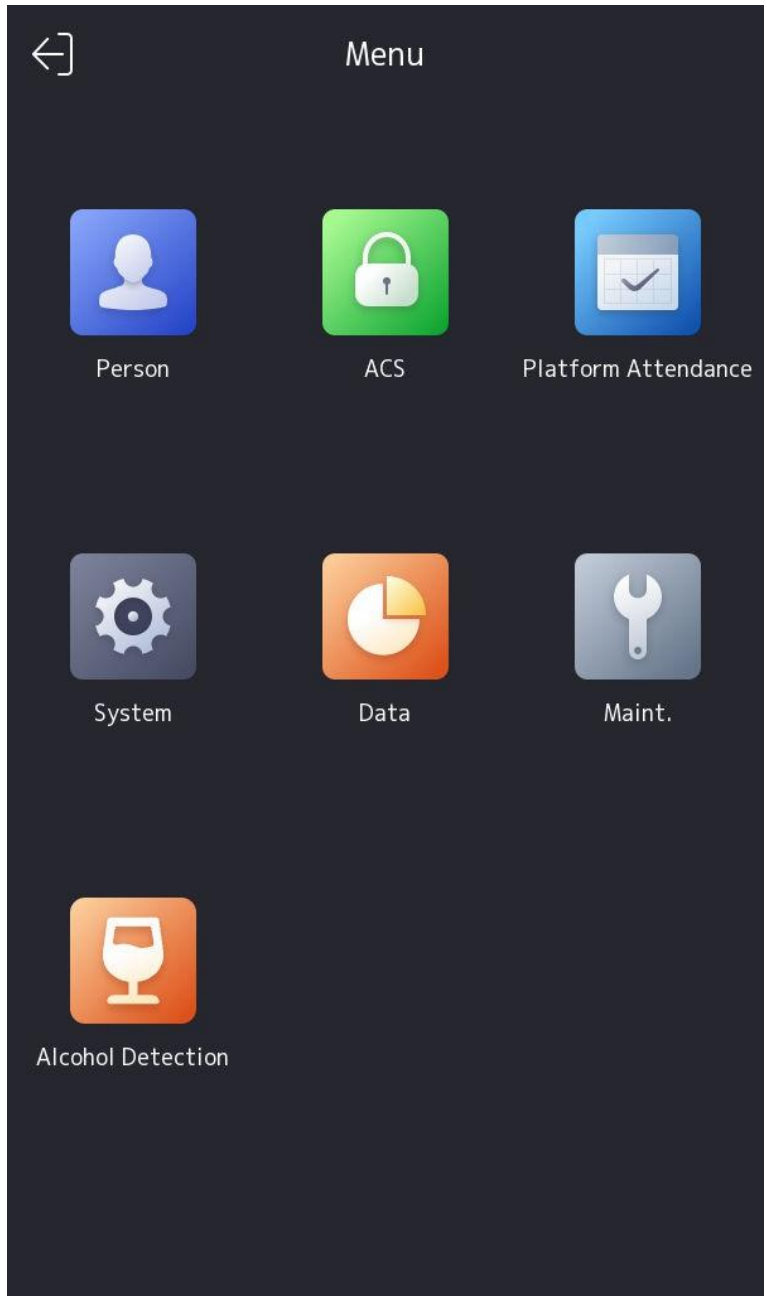


図 6-3 ホームページ

6.1.3 パスワードを忘れた場合

認証中にパスワードを忘れた場合は、パスワードを変更することができます。

手順

1. 最初のページを3秒間押し続け、表示されるジェスチャーに従って左/右にスライドし、ページにログインしてください。
2. **オプション：**管理者設定済みの場合、ポップアップ管理認証画面で「」をタップしてください。
3. **パスワードを忘れた場合は、[パスワードを忘れた場合]**をタップしてください。
4. リストからパスワード変更の種類を選択します。

注

パスワード変更タイプを1つだけ設定している場合は、対応するパスワード変更ページに進み、さらに設定を行います。

5. セキュリティの質問に回答するか、メールアドレスに基づいてパスワードを変更してください。
   - セキュリティ質問： アクティベーション時に設定したセキュリティ質問に回答してください。
   - メールアドレス

   注記

   デバイスがHik-Connectアカウントに追加されていることを確認してください。

   a. Hik-Connectアプリをダウンロードしてください。
   b. **その他 → デバイスのパスワードをリセット** を選択してください。
   c. デバイスのQRコードをスキャンすると、確認コードが表示されます。

   注意

   QRコードをタップすると拡大画像が表示されます。

   d. デバイスページに確認コードを入力してください。
6. 新しいパスワードを作成し、確認してください。
7. **OK**をタップしてください。

6.1.4 デバイスのパスワードを変更する

古いパスワードを入力して、デバイスのパスワードを変更できます。

手順

1. 初期ページを 3 秒間長押しして、ホームページにログインします。**システム → パスワード を**タップします。
2. **「デバイスパスワードの変更」**をタップします。
3. デバイスの古いパスワードを入力します。

注意

パスワードを忘れた場合は、**「パスワードを忘れた場合」**をタップしてパスワードを変更できます。詳細は「*パスワードを忘れた場合*」をご覧ください。

4. 新しいパスワードを入力し、パスワードを確認してください。

注意

デバイスのパスワード強度を自動で確認できます。製品のセキュリティ強化のため、ご自身で選択したパスワード（8文字以上で、大文字、小文字、数字、特殊文字の少なくとも3種類を含む）への変更を強く推奨します。また、特に高セキュリティシステムでは、パスワードを定期的に変更することをお勧めします。月次または週次での変更が製品の保護に効果的です。
すべてのパスワードおよびその他のセキュリティ設定の適切な構成は、設置者および／またはエンドユーザーの責任です。

5. **OK**をタップしてください。

6.2 通信設定

通信設定ページでは、有線ネットワーク、Wi-Fi パラメータ、RS-485 パラメータ、Wiegand パラメータ、ISUP、Hik-Connect へのアクセスを設定できます。

6.2.1 有線ネットワークパラメータの設定

IPv4/IPv6 IP アドレス、サブネットマスク、ゲートウェイ、DNS パラメータなど、デバイスの有線ネットワークパラメータを設定できます。

手順

1. ホームページで「**システム**」→「通信設定」をタップし、通信設定ページに入ります。
2. 通信設定ページで、**有線ネットワーク**をタップします。

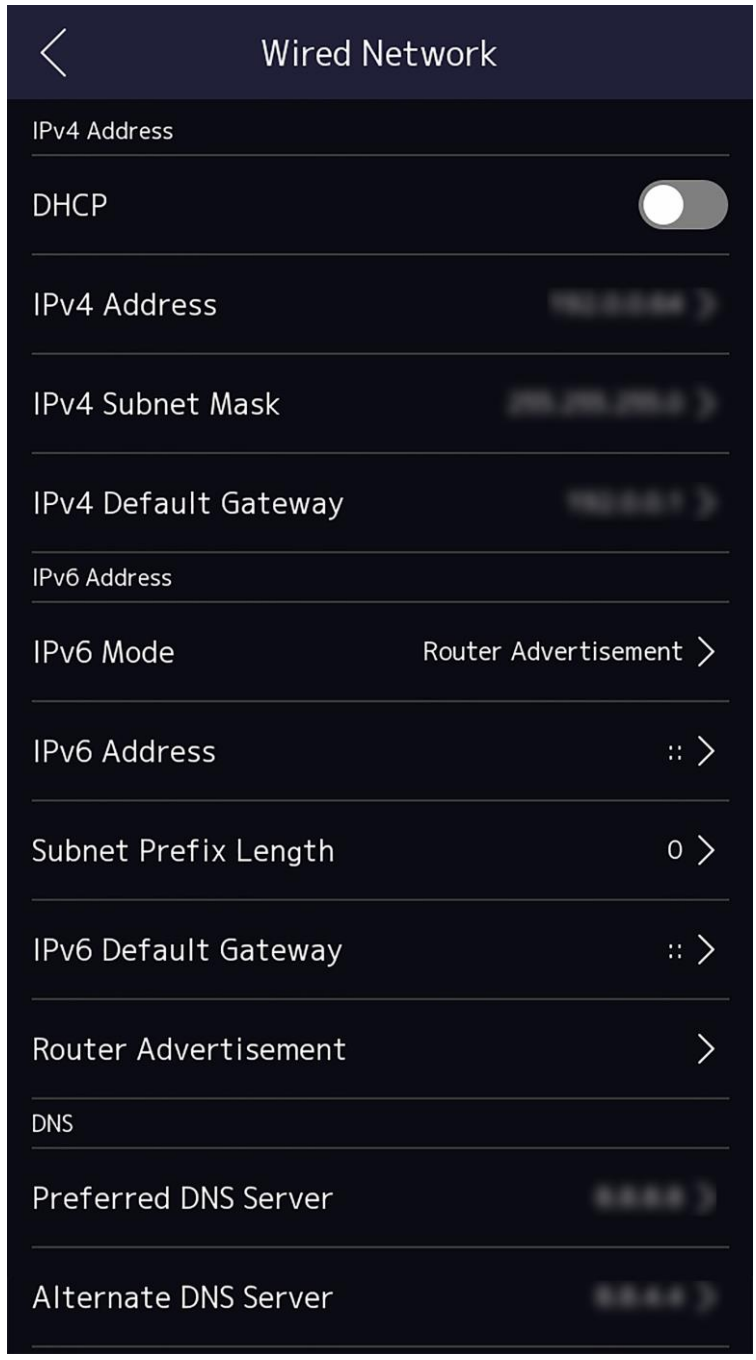


図6-4 有線ネットワーク設定

3. IPv4/IPv6 IP アドレス、サブネット マスク、およびゲートウェイを設定します。

- **DHCPを**有効にすると、システムがIPアドレス、サブネットマスク、ゲートウェイを自動的に割り当てます。
- **DHCP を**無効にする場合は、IP アドレス、サブネット マスク、およびゲートウェイを手動で設定する必要があります。

注

デバイスの IP アドレスとコンピュータの IP アドレスは、同じ IP セグメントにある必要があります。

4. DNSパラメータを設定します。**自動取得DNSを**有効にしたり、優先DNSサーバーと代替DNSサーバーを設定できます。

6.2.2 Wi-Fiパラメータの設定

Wi-Fi機能を有効にし、Wi-Fi関連のパラメータを設定できます。

手順

注意

お使いの端末がこの機能をサポートしている必要があります。

1. ホームページで、[**システム**] → [通信設定] をタップして、通信設定ページに入ります。
2. 通信設定ページで、をタップします。

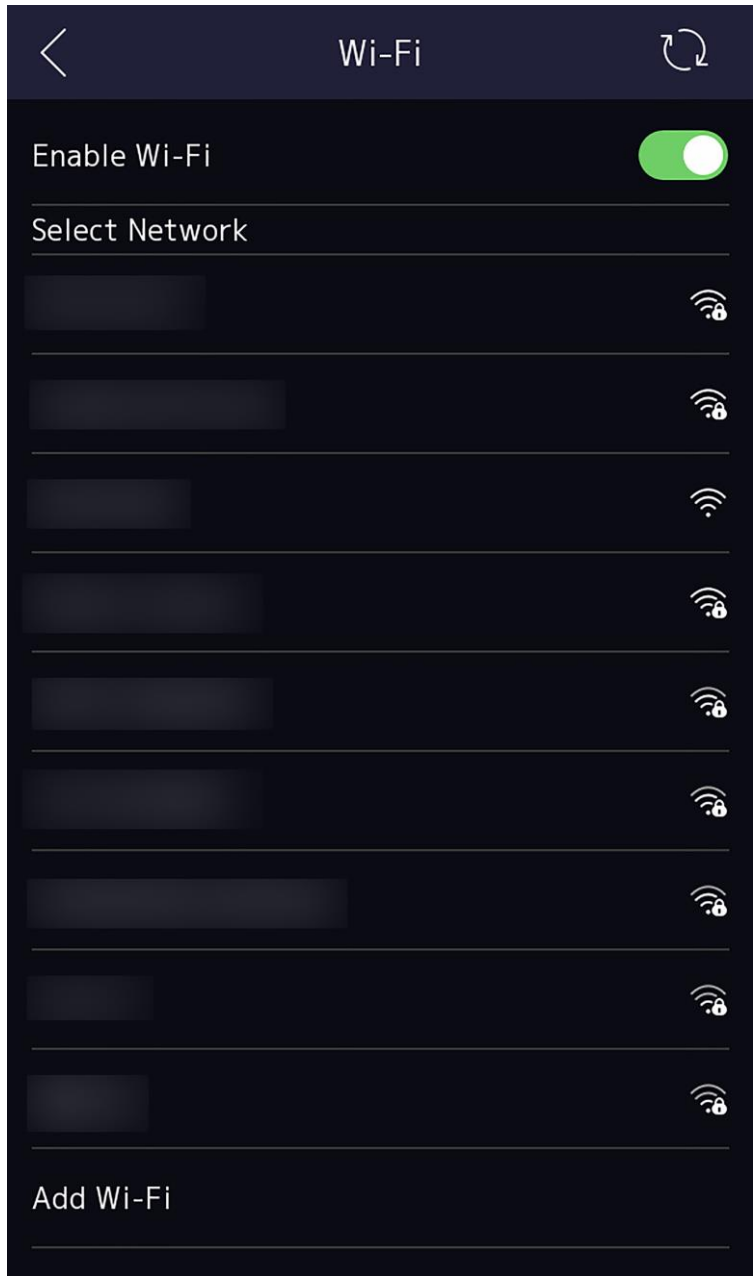


図 6-5 Wi-Fi 設定

3. Wi-Fi 機能を有効にします。

4. Wi-Fiパラメータを設定します。

- リストからWi-Fiを選択し、Wi-Fiのパスワードを入力します。「**OK**」をタップします。
- 対象のWi-Fiがリストにない場合は、「**Wi-Fiを追加**」をタップします。Wi-Fiの名前とパスワードを入力し、「**OK**」をタップします。

注意

パスワードには数字、英字、特殊文字のみ使用可能です。

5. Wi-Fiのパラメータを設定します。
   - デフォルトでは、DHCPが有効になっています。システムは、IPアドレス、サブネットマスク、およびゲートウェイを自動的に割り当てます。
   - DHCPを無効にする場合は、IPアドレス、サブネットマスク、ゲートウェイを手動で入力する必要があります。
6. 設定を保存してWi-Fiタブに戻るには、**[OK]を**タップしてください。
7. をタップしてネットワークパラメータを保存します。

6.2.3 RS-485 パラメータの設定

顔認識端末は、RS-485 端末を介して、外部アクセスコントローラ、セキュリティドア制御ユニット、カードリーダー、または QR コードスキャナに接続できます。

手順

1. ホームページで「**システム**」→「通信設定」をタップし、通信設定ページに入ります。
2. 通信設定ページで、**RS-485**をタップしてRS-485タブに入ります。

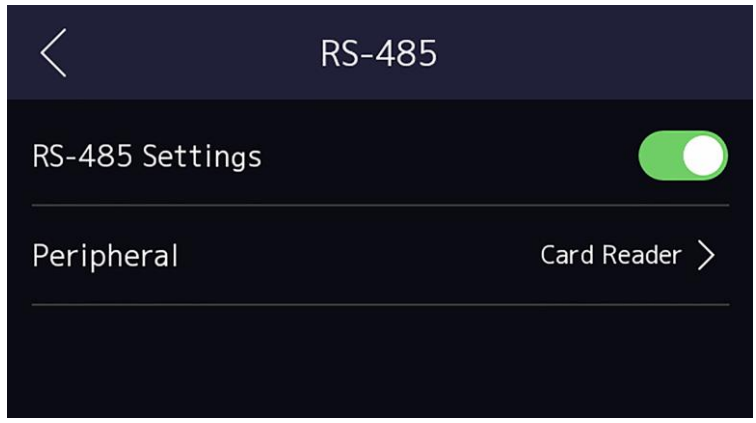


図 6-6 RS-485 パラメータの設定

3. 実際のニーズに応じて周辺機器タイプを選択してください。

注記

アクセスコントローラを選択した場合：RS-485 インターフェースを介してデバイスを端末に接続する場合は、RS-485 アドレスを 2 に設定してください。デバイスをコントローラに接続する場合は、ドア番号に応じて RS-485 アドレスを設定してください。

4. パラメータを変更した場合は、左上の戻るアイコンをタップし、デバイスを再起動してください。

6.2.4 ウィーガンドパラメータの設定

ウィーガンド伝送方向を設定できます。

手順

1. ホーム画面で「**システム**」→「通信設定」をタップし、通信設定ページに入ります。
2. 通信設定ページで、**ウィーガンド**をタップしてウィーガンドタブに入ります。
3. Wiegand機能を有効にします。
4. 送信方向を選択します。
   - 出力：顔認証端末は外部アクセス制御装置に接続できます。両デバイスはWiegand 34経由でカード番号を送信します。
   - 入力：顔認証端末はウィーガンドカードリーダーに接続できます。
5. をタップしてネットワークパラメータを保存します。

注意

外部デバイスを変更し、デバイスパラメータを保存すると、デバイスは自動的に再起動します。

6.2.5 ISUPパラメータの設定

ISUP パラメータを設定すると、デバイスは ISUP プロトコルを介してデータをアップロードできます。

開始前に

お使いのデバイスがネットワークに接続されていることを確認してください。

手順

1. ホームページで、**[システム] → [通信] → [ISUP]**（通信設定）をタップして設定ページに入ります。

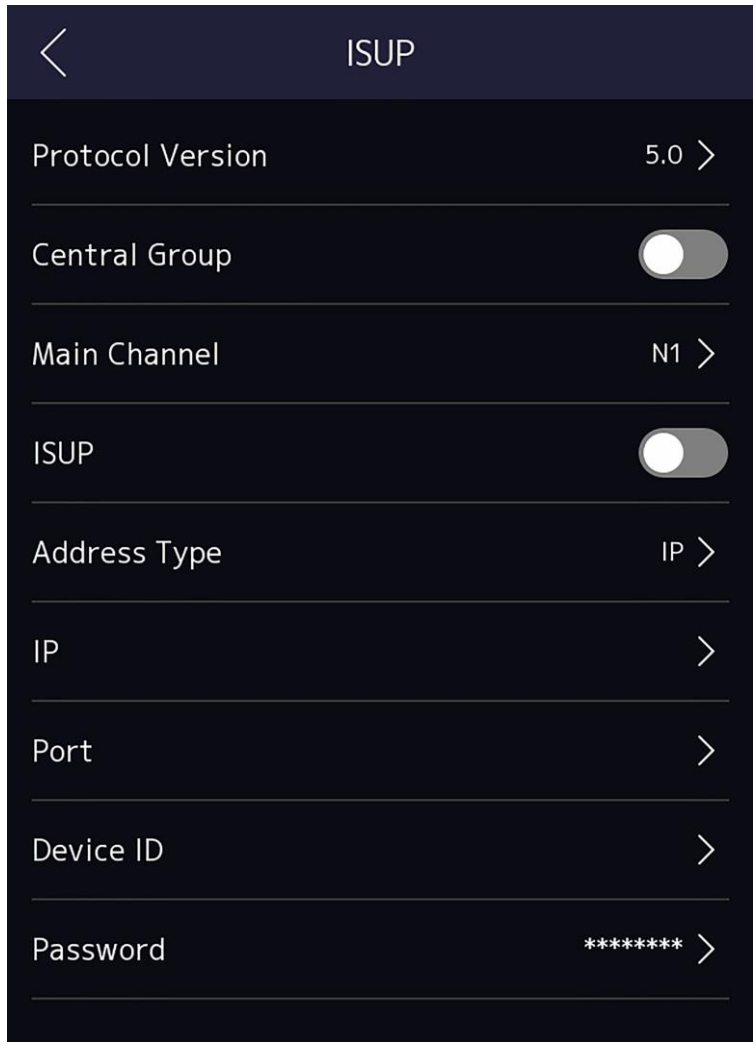


図 6-7 ISUP 設定

2. ISUP機能を有効にし、ISUPサーバーパラメータを設定します。

ISUPバージョン

実際のニーズに応じてISUPバージョンを設定してください。

中央グループ

セントラルグループを有効にすると、データはセントラルグループにアップロードされます。

メインチャネル

N1 または なしをサポートします。

ISUP

ISUP 機能を有効にすると、データは ISUP プロトコルを介してアップロードされます。

アドレスタイプ

実際のニーズに応じてアドレスタイプを選択してください。

IP アドレス

ISUP サーバーの IP アドレスを設定します。

ポート番号

ISUPサーバーのポート番号を設定する

注記

ポート番号の範囲：0～65535。

デバイス ID

デバイスのシリアル番号を設定します。

パスワード

V5.0 を選択した場合は、アカウントと ISUP キーを作成する必要があります。他のバージョンを選択した場合は、ISUP アカウントのみを作成する必要があります。

注

- ISUPアカウントとISUPキーを必ず覚えておいてください。デバイスがISUPプロトコルを介して他のプラットフォームと通信する際には、アカウント名またはキーを入力する必要があります。
- ISUPキーの範囲：8～32文字

6.2.6 プラットフォームアクセス

Hik-Connectモバイルクライアントにデバイスを追加する前に、デバイス認証コードの変更やサーバーアドレスの設定が可能です。

開始前に

デバイスがネットワークに接続されていることを確認してください。

手順

1. ホームページで「**システム**」→「通信設定」をタップし、通信設定ページに入ります。
2. 通信設定ページで、「**Hik-Connectへのアクセス**」をタップします。
3. **Hik-Connectへのアクセスを**有効にする
4. **サーバーIP**を入力してください。
5. **認証コード**を作成し、**Hik-Connect経由で**デバイスを管理する際にはこの認証コードを入力する必要があります。

6.2.7 SNMP設定

SNMP パラメータを設定できます。

手順

1. ホームページで「**システム設定**」→「**通信**設定」をタップし、「通信設定」ページに入ります。

2. 通信設定ページで、**SNMP を**タップします。
3. SNMPを有効にします。
4. トラップコミュニティ文字列を設定します。
5. NMS IP アドレスと **NMS ポート**を設定します。

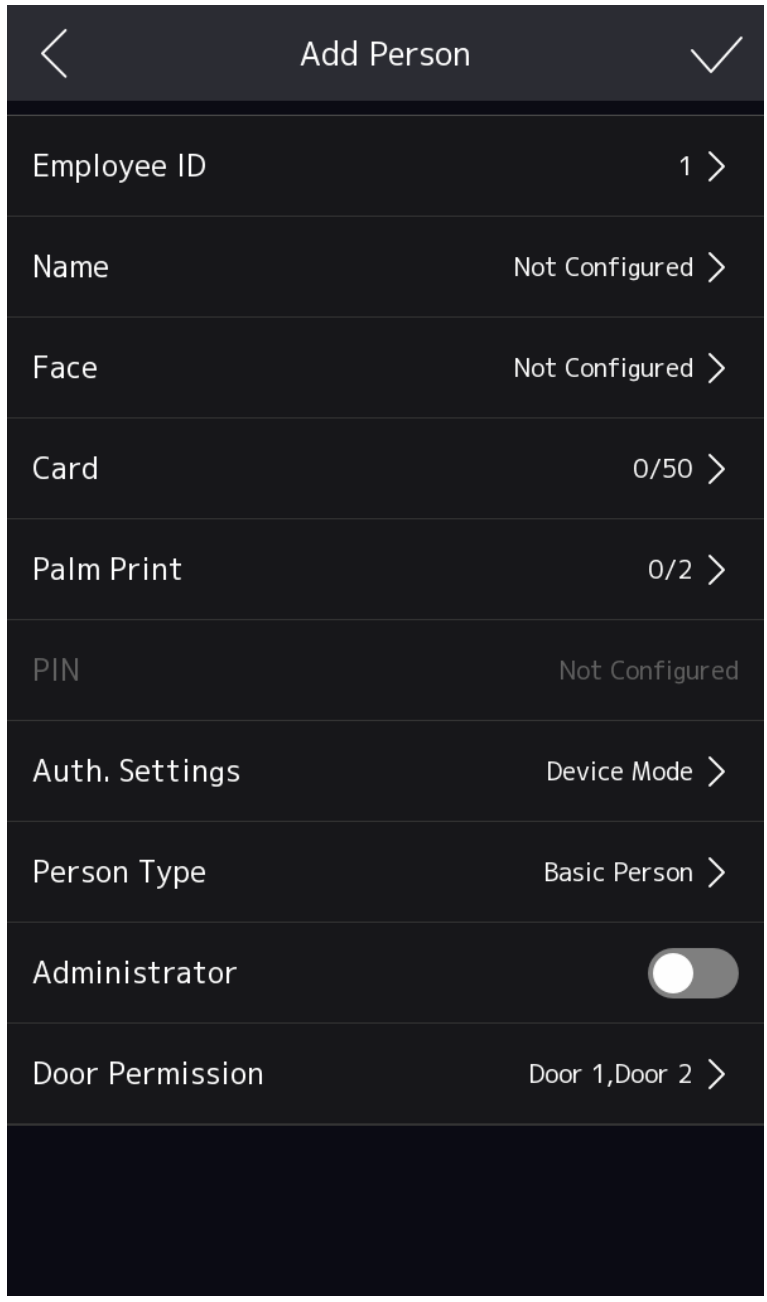
6.3 ユーザー管理

人物管理インターフェースでは、人物の追加、編集、削除、検索が可能です。

6.3.1 管理者の追加

管理者はデバイスのバックエンドにログインし、デバイスパラメータを設定できます。

手順
1. 初期画面を3秒間長押しし、表示されるジェスチャーに従って左右にスライドしてデバイスのバックエンドに入ります。
2. 「**人物**」→「**+**」をタップして人物追加ページに入ります。



3. 従業員IDを編集します。

注

- 従業員IDは32文字未満である必要があります。また、小文字、大文字、数字の組み合わせで構成できます。
- 従業員IDは重複してはいけません。

4. 名前フィールドをタップし、ソフトキーボードで個人名を入力してください。

注記

- 氏名には数字、大文字、小文字、特殊文字の使用が可能です。
- 氏名には最大 32 文字まで入力できます。

5. **オプション：**管理者用に顔写真、指紋、カード、PIN、掌紋、キーフォブを追加。

注記

- 顔写真の追加の詳細***については***、「顔写真の***追加」を***参照してください。
- 指紋の追加については、「***指紋の追加」***を参照してください。
- カード追加の詳細については、「***カード追加」***を参照してください。
- パスワードの追加については、「***PIN コードの表示」***を参照してください。
- キーフォブの追加については、「***キーフォブの追加」***を参照してください。
- 手のひらの登録方法の詳細については、を参照してください。

6. **オプション：**管理者の認証タイプを設定します。

注

認証タイプの設定の詳細については、「***認証モードの設定」***を参照してください。

7. **人物**タイプと**人物の役割**を設定します。

8. 管理者権限機能を有効にします。

管理者権限を有効にする

この人物は管理者です。通常の出席機能に加え、権限認証後にホームページにアクセスして操作できます。

9. 「**出退勤確認のみ**」を有効化できます。有効化後、この人物にはアクセス制御権限が付与されません。

10. **ドアの許可**を設定します。

11. をタップして設定を保存します。

6.3.2 デバイス経由での顔・人物データのバッチインポートとエクスポート

インポートおよびエクスポート機能を使用して、USB フラッシュドライブでデバイス A からデバイス B にデータをインポートすることができます。

開始前に

- ログインデバイス A（データをエクスポートする必要があるデバイス）にログインします。詳細については、***ログインを***参照してください。
- デバイスAにUSBフラッシュドライブを挿入します。

注意

- サポートされているUSBフラッシュドライブのフォーマットはFAT32またはexFATです。
- システムは1GBから256GBのUSBフラッシュドライブをサポートします。USBフラッシュドライブの空き容量が512MB以上であることを確認してください。

手順

1. デバイス A メニューで、**[データ]** をタップして**データ**ページに入ります。

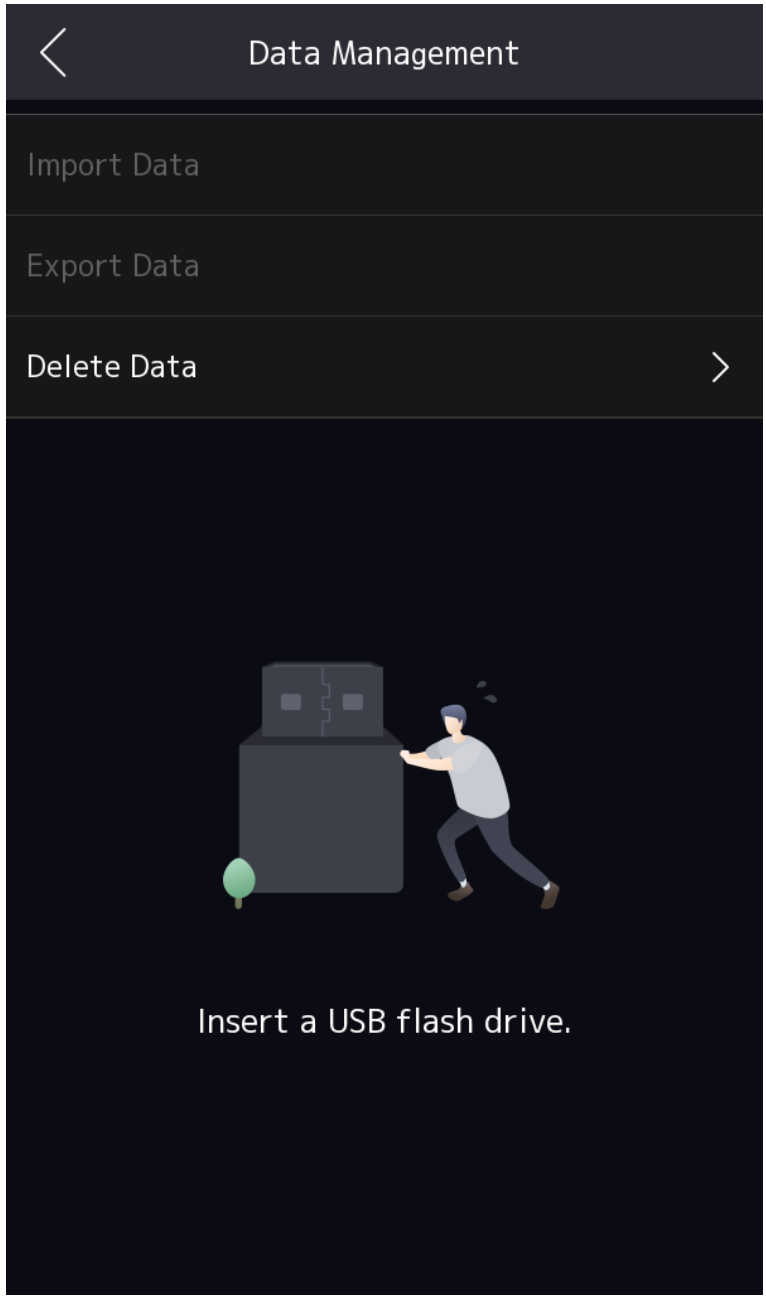


図 6-8 データ管理ページ

2. データ管理ページで「**データのエクスポート**」をタップします。

3. 「**個人データ**」または「**顔データ**」を選択します。

4. **オプション：**エクスポート用のパスワードを作成します。データを別のデバイスにインポートする際には、このパスワードを入力する必要があります。

注意

- パスワードは空欄にできません。パスワードを設定しない場合、エクスポートしたデータをPCで閲覧できます。
- パスワードを設定すると、PCでエクスポートしたデータを閲覧することはできません。
- エクスポートされた人物データはDBファイルであり、編集することはできません。

5. 顔と人物データをインポートする必要があるデバイスBにUSBフラッシュドライブを挿入してください。

注意

2台のデバイスが同じデバイスタイプであることを確認してください。

6. デバイス B のメニューで、[データ] をタップして**データ**ページに入ります。
7. **「データのインポート」**をタップします。
8. **「個人データ」**または**「顔データ」**を選択します。
9. データをエクスポートする際に作成したパスワードを入力します。データをエクスポートする際にパスワードを作成していない場合は、入力ボックスを空白のままにして**「OK」を**タップします。データがUSBフラッシュドライブからインポートされます。

注意

- 手動で画像をインポートする必要がある場合、USBフラッシュドライブのルートディレクトリ（enroll_pic）に画像を保存してください。画像名は以下の規則に従ってください：カード番号_名前_部署_社員ID_性別.jpg性別について、3は男性、6は女性、0はなしを表します。 従業員IDは32文字未満、名前は20文字未満、カード番号は20文字未満である必要があります。
- Enroll_picフォルダには最大10,000枚の画像を保存できます。インポートした画像を全て保存できない場合、ルートディレクトリ下にenroll_pic1、enroll_pic2、enroll_pic3、enroll_pic4という名前のフォルダを追加できます。最大10フォルダまで追加可能です。画像名は命名規則に従ってください。
- 顔写真の要件は以下の規則に従う必要があります：正面をカメラに向けて撮影すること。帽子や頭部を覆うものを着用しないこと。形式はJPEGまたはJPGであること。解像度は640×480ピクセル以上であること。画像サイズは60KB以上200KB以下であること。

6.3.3 顔写真を追加

デバイスに人物の顔写真を追加します。その人物は顔写真を使用して認証できます。

手順

1. 初期画面を3秒間長押しし、表示されるジェスチャーに従って左右にスライドし、バックエンドにログインします。
2. **「人物」→「+」**をタップして「人物追加」ページに入ります。
3. 従業員IDを編集します。

注記

- 従業員IDは32文字未満である必要があります。小文字、大文字、数字の組み合わせで構成できます。
- 従業員IDは重複させてはいけません。

4. 名前フィールドをタップし、ソフトキーボードで人物名を入力してください。

注記

- 氏名には、数字、大文字、小文字、特殊文字を使用できます。
- 提案される人物名は 32 文字以内である必要があります。

5. 顔写真フィールドをタップして、顔写真を追加するページに入ります。

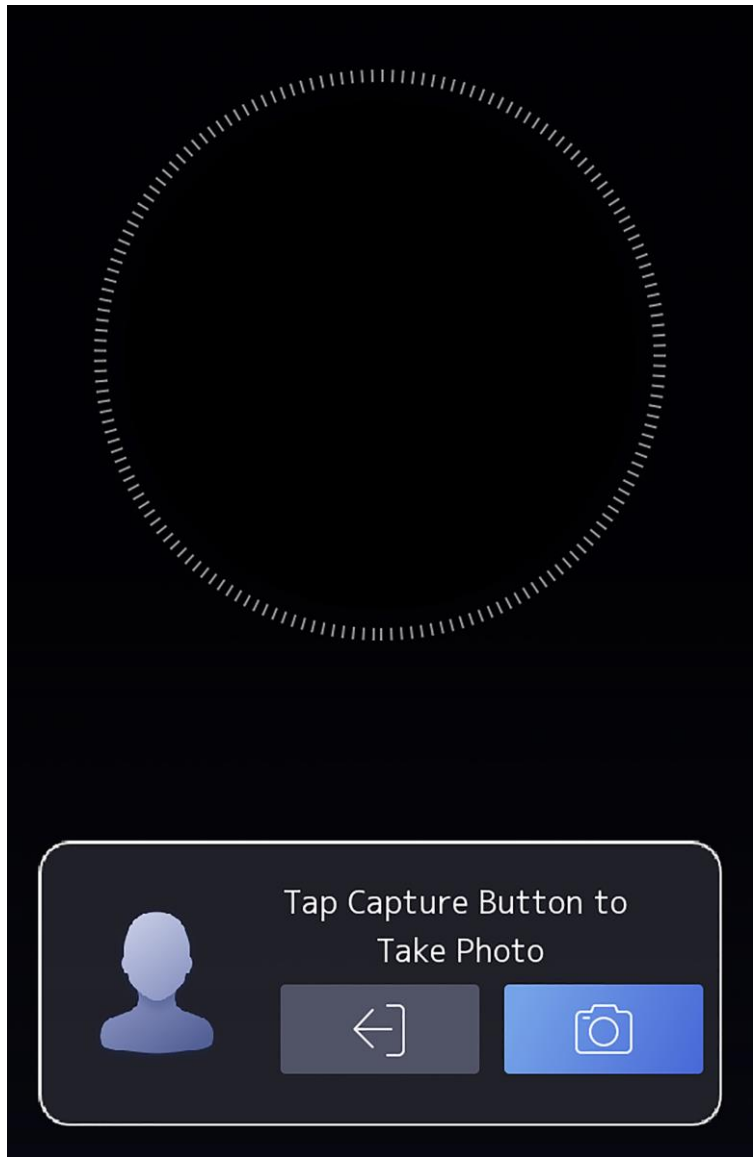


図 6-9 顔写真を追加

6. カメラを見てください。

注

- 顔写真を追加する際は、顔写真が顔写真の枠内に収まっていることを確認してください。
- 撮影した顔写真が高品質で正確であることを確認してください。
- 顔写真の追加手順の詳細については、「***顔写真の収集・照合時の注意点***」を参照してください。

顔写真を完全に追加すると、ページの右上隅に撮影された顔写真が表示されます。

7. **「保存」**をタップして顔写真を保存してください。

8. **オプション：もう一度試す**をタップし、顔の位置を調整して顔写真を再度追加してください。

9. 人物タイプを設定してください。

基本ユーザー

この人物は通常の人物です。この人物は初期ページでの認証または出席確認のみ可能です。管理者機能を有効にすることで、基本人物を**管理者**として設定することもできます。

訪問者

訪問者です。

ブロックリスト登録者

この人物はブロックリストに登録されています。認証を開始すると、イベントがアップロードされます。

カスタムタイプ

カスタム人物タイプを設定します。

10. 設定を保存するには、[✓]をタップしてください。

6.3.4 カードを追加

対象者にカードを追加すると、追加されたカードで認証が可能になります。

手順

注意
各ユーザーは最大50枚のカードを追加できます。

1. 最初のページを3秒間長押しし、表示されるジェスチャーに従って左右にスライドし、バックエンドにログインします。

2. **人→+**をタップして「人物追加」ページに入ります。

3. 配線図に従って外部カードリーダーを接続してください。

4. 従業員IDフィールドをタップし、従業員IDを編集してください。

注記

- 従業員IDは32文字未満である必要があります。小文字、大文字、数字の組み合わせで構成できます。
- 従業員IDは重複してはいけません。

5. 名前フィールドをタップし、ソフトキーボードで人物名を入力します。

注記

- 氏名には数字、大文字、小文字、特殊文字を使用できます。
- 提案される人物名は32文字以内である必要があります。

6. カードフィールドをタップし、**+**をタップします。

7. カード番号を設定する
- カード番号を手動で入力してください。
- カード提示エリアにカードを提示してカード番号を取得する

注意
- カード番号は空欄にできません。
- カード番号は最大20文字まで入力可能です。
- カード番号は重複できません。

8. カードタイプを設定してください。

9. 設定を保存するには、[ ]をタップしてください。

6.3.5 指紋を追加

その人物の指紋を追加すると、追加された指紋で認証できるようになります。

手順

注記
この機能はデバイスがサポートしている必要があります。

1. 初期ページを3秒間長押しし、ジェスチャーに従って左/右にスライドしてデバイスのバックエンドに入ります。

2. **「人物」→「+」**をタップして「人物追加」ページに入ります。

3. 従業員IDフィールドをタップし、従業員IDを編集します。

注記
- 従業員IDは32文字未満である必要があります。また、小文字、大文字、数字の組み合わせで構成できます。
- 従業員IDは0で始まってはならず、重複してはなりません。

4. 名前フィールドをタップし、ソフトキーボードで人物名を入力してください。

注意
- 氏名には数字、大文字、小文字、特殊文字を使用できます。
- 提案される人物名は32文字以内である必要があります。

5. 指紋フィールドをタップして「指紋を追加」ページに入ります。

6. 指示に従って指紋を追加してください。

注意
- 同じ指紋を繰り返し追加することはできません。
- 1 人につき最大 10 個の指紋を追加できます。
- クライアントソフトウェアや指紋リーダーを使用して指紋を記録することもできます。

指紋スキャンに関する詳細な手順については、「*指紋スキャンの注意事項*」をご覧ください。

7. 設定を保存するには、✓ をタップして設定を保存します。

6.3.6 PINコードを表示

対象者にPINコードを追加すると、その対象者はPINコードで認証できます。

手順

1. 初期画面を3秒間長押しし、表示されるジェスチャーに従って左右にスライドし、バックエンドにログインします。

2. 「**人物**」→「**+**」をタップして人物追加ページに入ります。

3. 従業員IDフィールドをタップし、従業員IDを編集します。

注記

- 従業員IDは32文字未満である必要があります。また、小文字、大文字、数字の組み合わせで構成できます。
- 従業員IDは重複してはいけません。

4. 名前フィールドをタップし、ソフトキーボードで人物名を入力してください。

注意

- 氏名には数字、大文字、小文字、特殊文字を使用できます。
- 提案される人物名は 32 文字以内である必要があります。

5. PIN コードをタップすると、PIN コードが表示されます。

注

PINコードは編集できません。プラットフォームによってのみ適用されます。

6. 設定を保存するには ✓ をタップして設定を保存してください。

6.3.7 キーフォブを追加

ユーザー用のキーフォブを追加します。

手順

注

- キーフォブを追加する前に、顔認証端末に対応する周辺機器モジュールを接続する必要があります。WEシリーズキーフォブを追加するにはWEシリーズ周辺機器モジュールを接続し、WBシリーズキーフォブを追加するにはWBシリーズ周辺機器モジュールを接続する必要があります。
- 本機能は端末が対応している必要があります。
- 各ユーザーは最大1つのキーフォブを追加でき、デバイスは最大5,000個のキーフォブを追加できます。

1. 初期画面を3秒間長押しし、表示されるジェスチャーに従って左右にスライドすると、デバイスの管理画面に入ります。

2. **「ユーザー」→「+」**をタップしてユーザー追加ページに入ります。

3. 従業員IDフィールドをタップし、従業員IDを編集します。

注記

- 従業員IDは32文字未満である必要があります。また、小文字、大文字、数字の組み合わせで構成できます。
- 従業員IDは0で始まってはならず、重複してはなりません。

4. 名前フィールドをタップし、ソフトキーボードでユーザー名を入力してください。

注記

- ユーザー名には数字、大文字、小文字、特殊文字を使用できます。
- 提案されるユーザー名は 32 文字以内である必要があります。

5. **キーフォブ**をタップ **→ + → キーフォブシリアル番号**、キーフォブのシリアル番号を入力するか、キーフォブの任意のボタンを押してシリアル番号を取得します。

6. をタップして設定を保存します。

6.3.8 掌紋と掌静脈を追加

その人物の手のひらの指紋を追加すると、追加された指紋で認証が可能になります。

手順

注

- 本機能はデバイスが対応している必要があります。
- 最大10000件の手のひら紋様および手のひら静脈を追加できます。

1. 最初のページを3秒間長押しし、表示されるジェスチャーに従って左右にスライドすると、デバイスのバックエンドに入ります。

2. **「人物」→「+」**をタップして人物追加ページに入ります。

3. 従業員IDフィールドをタップし、従業員IDを編集します。

注記

- 従業員IDは32文字未満である必要があります。小文字、大文字、数字の組み合わせで構成できます。
- 従業員IDは0で始まってはいけません。また重複してはいけません。

4. 名前フィールドをタップし、ソフトキーボードで人物名を入力してください。

注意

- 名前には数字、大文字、小文字、特殊文字を使用できます。
- 提案される人物名は32文字以内である必要があります。

5. **「掌紋」**をタップし、**「+」を**タップして追加ページに入ります。
6. 手のひらを、デバイスの周辺モジュールから 5 ～ 12 cm の距離に置きます。
7. をタップして設定を保存します。

6.3.9 デバイス経由で人物タイプを設定

人物タイプを基本人物、訪問者、ブロックリスト登録者、またはカスタム人物タイプとして設定します。

開始前に

デバイスにログインしてください。詳細は*「ログイン」*を参照してください。

手順

1. **「人物」→「+」**をタップします。

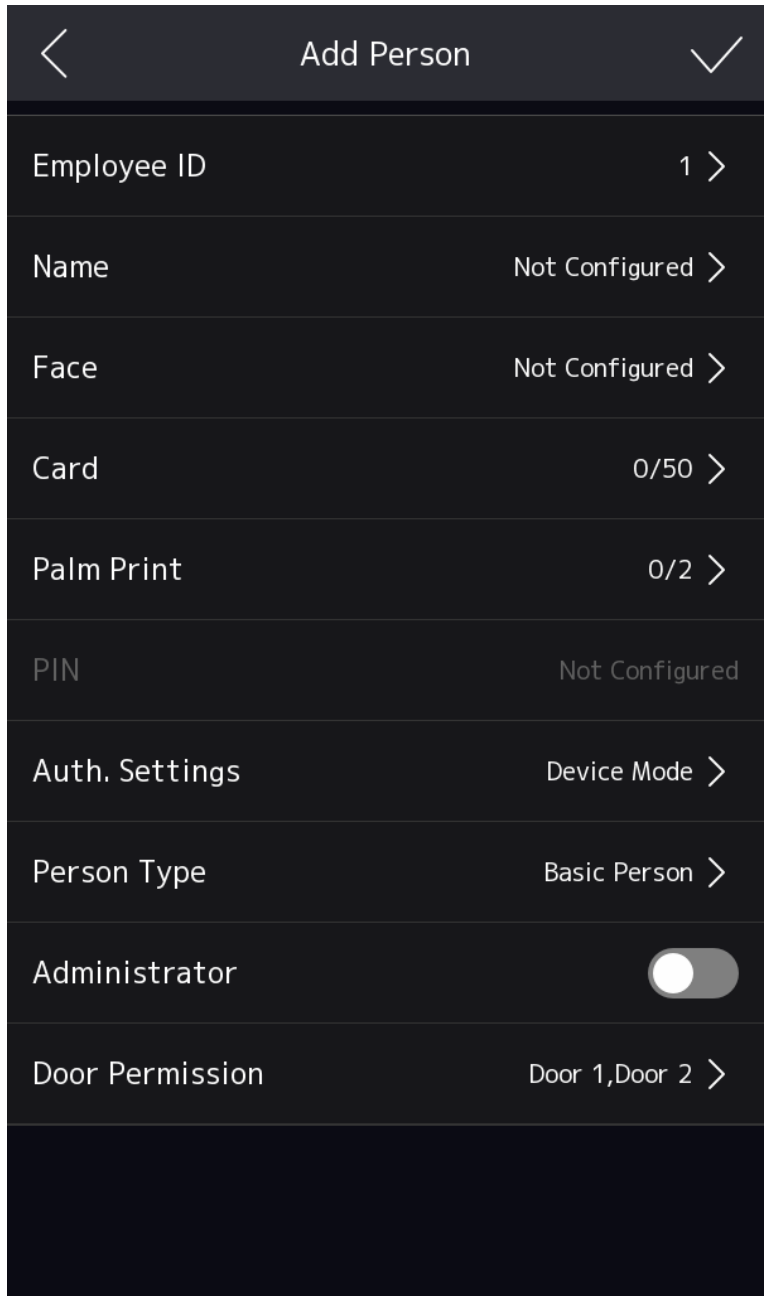


図6-10 人物の追加

2. **従業員ID**をタップすると、従業員IDを編集できます。

注

従業員 ID は 32 文字を超えることはできません。大文字、小文字、数字を組み合わせて使用できます。

3. **名前**をタップして名前を作成します。ポップアップキーボードに従って人物の名前を入力してください。

注意

- 名前には数字、大文字、小文字、特殊文字が使用可能です。
- 名前は128文字以内にしてください。

4. 顔、カード、指紋、掌紋を設定します。

注

- ***顔写真追加***、***カード追加***、***指紋追加***、および顔、カード、指紋、掌紋を追加することを指します。
- 指紋または掌紋モジュールを搭載したデバイスのみが、指紋または掌紋機能をサポートします。

5. **「人物タイプ」**をタップし、タイプを「**基本人物**」「**訪問者**」「**ブロックリストの人物**」「**カスタムタイプ**」のいずれかに設定します。

注記

- 人物を訪問者に設定する場合、管理者を設定できません。人物をブロックリスト登録者に設定する場合、ドアの許可権限を設定できません。
- カスタムタイプの名称はPCウェブ上で設定してください。カスタムタイプに名称を付けると、デバイス上のカスタムタイプは指定された名称に変更されます。詳細な設定については、***人物管理を***参照してください。

6. をタップして設定を保存します。

6.3.10 認証モードを設定する

顔写真、パスワード、その他の認証情報を追加した後、認証モードを設定する必要があります。設定された認証モードを通じて、本人は自身の身元を認証できます。

手順

1. 初期ページを3秒間長押しし、表示されるジェスチャーに従って左右にスライドし、バックエンドにログインします。
2. **「人物」→「人物を追加/編集」→「認証モード」**をタップします。
3. 認証モードとして「デバイス」または「カスタム」を選択します。

   デバイス

   デバイスモードを選択する場合は、まずアクセス制御設定ページで端末認証モードを設定する必要があります。詳細は*「アクセス制御パラメータの設定」*を参照してください。

   カスタム

   実際のニーズに応じて、異なる認証モードを組み合わせて使用できます。

4. をタップして設定を保存します。

6.3.11 人物の検索と編集

人物を追加した後、その人物を検索して編集することができます。

人物を検索

「人員管理」ページで、検索エリアをタップして「人員検索」ページに入ります。ページ左側の「**カード**」をタップし、ドロップダウンリストから検索タイプを選択します。従業員ID、カード番号、または名前を入力して検索します。「  」をタップして検索を実行します。

人物編集

「人員管理」ページで、人員リストから対象者を選択し「人員編集」ページに入ります。***人員管理***の手順に従い、人員パラメータを編集します。「  」をタップして設定を保存します。

注記

従業員IDは編集できません。

6.3.12 デバイス経由での人物ドア権限設定

通常の人物または訪問者のドア通過権限を設定します。

開始前に

デバイスにログインしてください。詳細は*「ログイン」*を参照してください。

手順

1. 「人物」→「+」をタップします。

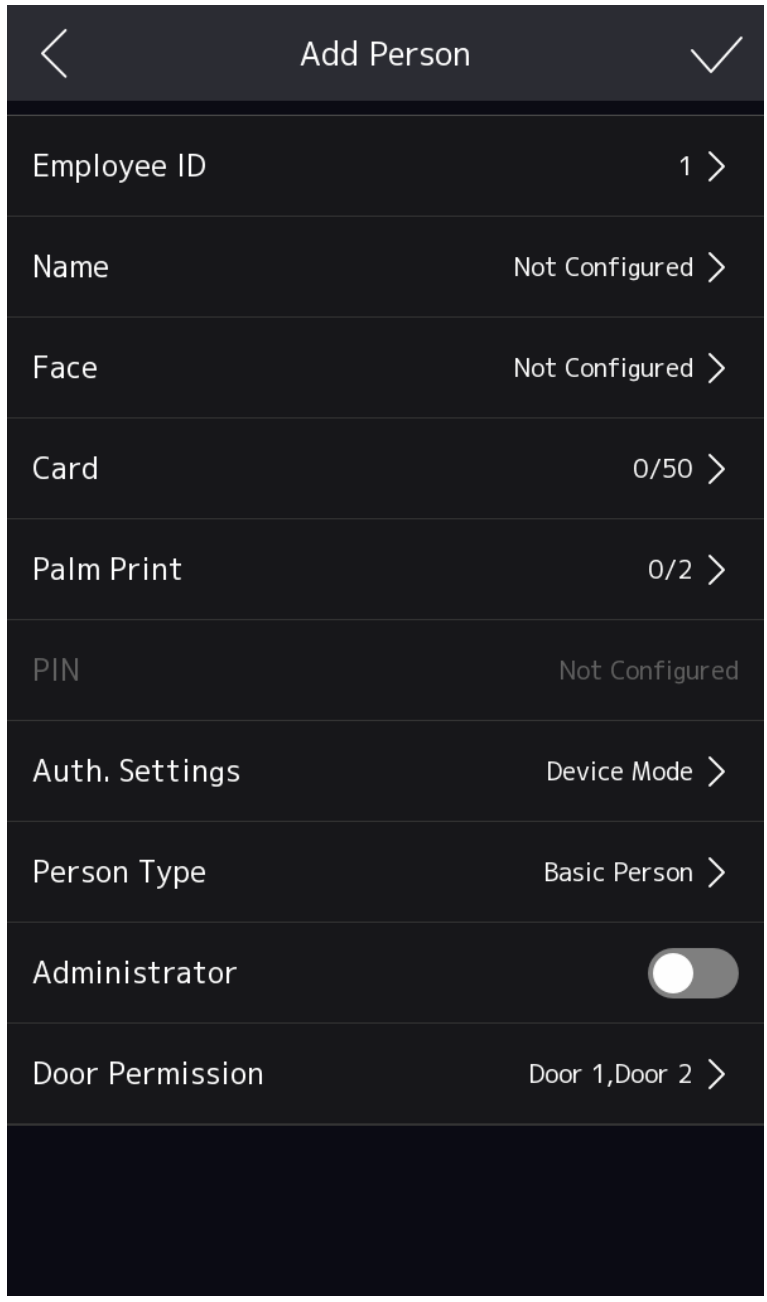


図 6-11 人物の追加

2. **従業員ID**をタップすると、従業員IDを編集できます。

注意

従業員IDは32文字以内である必要があります。大文字、小文字、数字の組み合わせで構成できます。

3. **名前**をタップして名前を作成します。ポップアップキーボードに従って人物の名前を入力してください。

注意

- 名前には数字、大文字、小文字、特殊文字を使用できます。
- 名前は128文字以内にしてください。

4. 顔、カード、指紋、掌紋を設定します。

注記

- ***顔写真の追加***、***カードの追加***、***指紋の追加***、および顔、カード、指紋、掌紋を追加することを指します。
- 指紋または掌紋モジュールを搭載したデバイスのみが、指紋または掌紋機能をサポートします。

5. **「人物タイプ」**をタップし、タイプを「**基本人物**」または「**訪問者**」に設定します。

注

人物を訪問者に設定した場合、管理者を設定できません。人物をブロックリストの人物として設定した場合、その人物に対するドアの許可を設定できません。

6. **ドア許可**をタップし、通行させるドアを選択してください。ドア1は、そのドアがデバイスに接続されていることを意味します。ドア2は、そのドアがセキュアドア制御ユニットに接続されていることを意味します。

注記

リモート認証時、管理者は人物のドア許可権限に基づき開錠するドアを判断できます。

7. をタップして設定を保存します。

6.4 データ管理

データの削除、データのインポート、データのエクスポートが可能です。

6.4.1 データの削除

個人データを削除します。

ホーム画面で、**データ → データ削除 → 個人データを**タップします。デバイスに追加されたすべての個人データが削除されます。

6.4.2 データのインポート

手順

1. USB フラッシュドライブをデバイスに接続します。
2. ホーム画面で、**[データ] → [データのインポート]** をタップします。
3. **「個人データ」**、**「顔データ」**、または**「アクセス制御パラメータ」**をタップします。

注

インポートされたアクセス制御パラメータは、デバイスの設定ファイルです。

4. データエクスポート時に作成したパスワードを入力してください。エクスポート時にパスワードを作成していない場合は、入力欄を空白のままにし、すぐに**「OK」を**タップしてください。

注意

- あるデバイス（デバイスA）から別のデバイス（デバイスB）へ全ての個人情報を転送したい場合、デバイスAからUSBフラッシュドライブへ情報をエクスポートし、その後USBフラッシュドライブからデバイスBへインポートする必要があります。この場合、プロフィール写真をインポートする前に個人データをインポートしてください。
- サポートされているUSBフラッシュドライブのフォーマットはFAT32です。
- インポートした画像はルートディレクトリ内のフォルダ（enroll_pic）に保存し、画像名は以下の規則に従ってください：

  カード番号_氏名_部署名_社員ID_性別.jpg
- インポートした画像をすべて保存できない場合、ルートディレクトリ下に別のフォルダ（enroll_pic1、enroll_pic2、enroll_pic3、enroll_pic4）を作成できます。
- 従業員IDは32文字未満である必要があります。小文字、大文字、数字の組み合わせで構成され、重複せず、0で始まってはいけません。
- 顔写真の要件は以下の規則に従う必要があります：正面を向き、カメラをまっすぐ見据えた状態で撮影すること。顔写真の撮影時には帽子や頭部を覆うものを着用しないでください。形式はJPEGまたはJPGであること。解像度は640×480ピクセル以上であること。画像サイズは60KB以上200KB以下であること。

6.4.3 データエクスポート

手順

1. USBフラッシュドライブをデバイスに接続します。
2. ホームページで、**データ → データのエクスポート** をタップします。
3. **顔データ**、**イベントデータ**、**人物データ**、または**アクセス制御パラメータ**をタップします。

注

エクスポートされたアクセス制御パラメータは、デバイスの設定ファイルです。

4. **オプション：**エクスポート用のパスワードを作成します。これらのデータを別のデバイスにインポートする際には、パスワードを入力する必要があります。

注意

- サポートされているUSBフラッシュドライブのフォーマットはDBです。
- システムは1GBから256GBの容量を持つUSBフラッシュドライブをサポートします。USBフラッシュドライブの空き容量が512MB以上であることを確認してください。
- エクスポートされた人物データはDBファイルであり、編集することはできません。

6.5 人物認証

ネットワーク設定、システムパラメータ設定、ユーザー設定が完了したら、認証のために初期ページに戻ることができます。システムは、設定された認証モードに従って個人を認証します。

6.5.1 シングルクレデンシャルによる認証

認証前にユーザー認証タイプを設定します。詳細については、***認証モードの設定を***参照してください。

顔認証

カメラに向かって顔を向け、顔認証を開始します。

指紋認証

登録済みの指紋を指紋モジュールに置き、指紋による認証を開始します。

掌紋

掌紋認証モジュールに掌を置き、掌紋による認証を開始します。

カード

カードをカード提示エリアに提示し、カードによる認証を開始します。

注意

カードは通常のICカード、または暗号化カードである可能性があります。

QRコード

QRコード認証を行うには、QRコードをデバイスのカメラの前にかざしてください。

注意

- QRコードによる認証は、デバイスがサポートしている必要があります。
- ***設定***でQRコード機能を有効にする***必要があります***。

PIN

PIN による認証を行うには、PIN を入力してください。

キーフォブ

キーフォブのドアオープンボタンを押して認証してください。

認証が完了すると、「認証済み」というプロンプトが表示されます。

6.5.2 複数の認証情報による認証

開始前に

認証前にユーザー認証タイプを設定してください。詳細は「***認証モードの設定***」を参照してください。

手順

1. ライブビューページの指示に従い、任意の認証情報を認証します。

注

- カードは通常のICカード、または暗号化カードのいずれかです。
- QRコードスキャン機能が有効な場合、デバイスカメラの前にQRコードを提示することでQRコード経由で認証できます。

2. 前の認証情報が認証された後、他の認証情報の認証を続行する。

注記

- 指紋スキャンに関する詳細情報は、「*指紋スキャンのヒント*」を参照してください。
- 顔認証の詳細については、「*顔画像収集・比較時のポイント*」を参照してください。

認証が成功すると、「認証済み」というプロンプトが表示されます。

6.6 基本設定

初期ページを 3 秒間長押しし、ジェスチャーに従って左/右にスライドしてデバイスのホームページにログインします。**システム → 基本 を**タップします。

6.6.1 デバイス経由での音声プロンプトの有効化/無効化

音声プロンプト機能を有効/無効にしたり、音声の音量を調整したりできます。デバイスにログインしてください。詳細は「*ログイン*」を参照してください。

システム設定 → 基本 → サウンド設定 をタップします。

音声プロンプト機能を有効にし、音声の音量を調整できます。音声プロンプト機能を有効にすると、音声の音量を設定できます。

6.6.2 デバイス経由でのデバイス時刻設定

デバイスの時刻を設定します。

デバイスにログインします。詳細は*「ログイン」*を参照してください。

システム設定 → 基本 → 時間設定をタップします。

デバイスのタイムゾーン、現在時刻、および夏時間（DST）を設定します。

6.6.3 デバイス経由でスリープ時間を設定

デバイスのスリープ待機時間を設定します。

デバイスにログインしてください。詳細は「*ログイン*」を参照してください。

システム設定 → 基本 をタップし、**スリープ時間を設定**します。
初期画面でスリープ時間を30秒に設定した場合、操作がない状態で30秒後にデバイスがスリープ状態になります。

注意
スリープ時間を0に設定すると、デバイスはスリープモードに入りません。設定可能なスリープ時間は20秒から999秒の間です。

6.6.4 言語を選択

デバイスにログインします。詳細は*「ログイン」*を参照してください。
システム設定 → 基本 をタップします。言語を変更するには「**言語を選択**」をタップします。言語変更後、デバイスは再起動します。

6.6.5 デバイス経由でデバイス番号を設定

本デバイスは、アクセス制御デバイス、ドアステーション、または外部ドアステーションとして使用できます。ビデオインターホン用のデバイス番号を設定できます。

デバイスにログインします。詳細は*「ログイン」*を参照してください。
システム設定 → 基本 をタップします。**コミュニティ番号**、**棟番号**、**部屋番号**を設定します。

6.6.6 デバイス経由でビューティー機能を設定

美容機能を有効にし、滑らかさと白さのパラメータを設定できます。デバイスにログインしてください。

詳細は*「ログイン」*を参照してください。

システム設定 → 基本設定 → 美肌をタップ。
美肌機能を有効にし、滑らかさと白さのパラメータを設定します。**+または-**をタップして効果の強さを調整します。

6.6.7 通話設定

通話パラメータを設定できます。

手順

1. 最初のページを3秒間長押しし、表示されるジェスチャーに従って左右にスライドしてデバイスのホームページにログインします。**システム設定 → 基本 を**タップします。
2. **通話設定**をタップします。
3. 通話パラメータを設定します。
   通話設定

ダイヤル後の自動発信

ダイヤル後自動発信を有効にし、タイムアウト期間を設定できます。

コールセンターボタンの発信先

発信先を選択します。

VoIPサーバー

VoIPサーバーを選択します。

6.6.8 デバイス経由でプライバシーパラメータを設定

画像アップロードパラメータを設定します。

注記

異なるデバイスモデルではサポートされる機能が異なります。実際のモデルを参照してください。

デバイスにログインします。詳細は*「ログイン」*を参照してください。**システム設定 → 基本 → プライバシー**をタップします。

認証設定

名前 / 社員ID / 顔写真

認証時に名前と社員IDを表示する/非表示にする/匿名化するを選択できます。

画像アップロードと保存

写真のアップロードと保存に関する設定を行います。

登録済み画像の保存

この機能を有効にすると、登録された顔写真がシステムに保存されます。

リンクキャプチャ後に画像を保存

この機能を有効にすると、リンクキャプチャ後に画像を保存できます。

リンクキャプチャ後の画像をアップロード

リンクキャプチャ後にキャプチャした画像をアップロードします。

認証時に画像を保存

この機能を有効にすると、デバイスへの認証時に画像を保存できます。

認証時に画像をアップロード

この機能を有効にすると、デバイスへの認証時に画像を保存できます。

掌紋画像を保存

この機能を有効にすると、申請時に画像を保存できます。

通話中に撮影した画像をアップロード

通話中に撮影した画像を自動的にプラットフォームにアップロードします。

6.6.9 ライブ映像の画質設定

ライブビューのビデオ標準を設定します。デバイス
にログインします。詳細は「*ログイン*」を参照して
ください。

システム → 基本設定 → 映像標準 へ移動。
リモートでのライブビュー実行時の動画フレームレートを設定します。標準を変更後は、デバイスを再起動して有効化してください。

PAL (50HZ)

毎秒25フレーム。中国本土、香港（中国）、中東諸国、欧州諸国などに適しています。

NTSC (60HZ)

30フレーム/秒。アメリカ、カナダ、日本、台湾（中国）、韓国、フィリピンなどに適しています。

6.6.10 セキュアドア制御ユニットのパラメータ設定

セキュアドア制御ユニットに合わせて周辺機器を配線できます。セキュアドア制御ユニットの制御にドア1またはドア2を使用するように設定できます。

開始前に

デバイスはRS-485でセキュアドア制御ユニットを配線します。詳細な配線方法については、*配線を*参照してください。

手順

1. デバイスにログインします。詳細は*「ログイン」*を参照してください。
2. **システム → 基本 → セキュアドア制御ユニット** に移動します。
3. ドア番号として「**ドア1**」または「**ドア2**」を選択します。

注意

ドア1を選択すると、そのドアはセキュアドア制御ユニットによって制御されます。ドア2の選択についても同様です。

6.7 フェイスパラメータを設定する

顔認識性能を向上させるため、顔パラメータをカスタマイズできます。

初期画面を3秒間長押ししてホーム画面にログインします。**システム設定 → 生体認証 を**タップします。

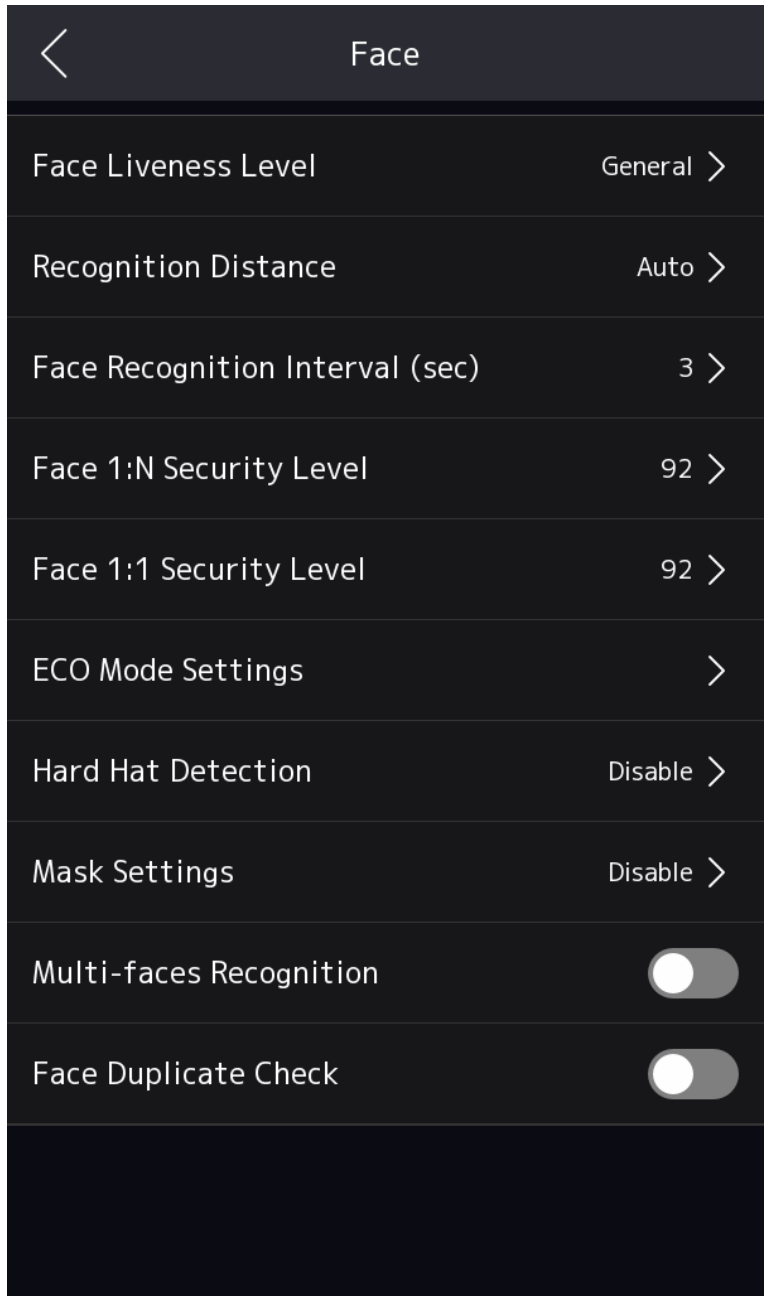


図6-12 顔設定

6.7.1 デバイス経由で顔の生体検知レベルを設定

顔認証の偽装防止機能を有効にした後、生体認証を行う際のセキュリティレベルを設定できます。

デバイスにログインします。詳細については、「*ログイン*」を参照してください。

システム設定 → 生体認証 → 顔 をタップします。顔の生体認
証レベルを選択します。
一般、高度、専門から選択できます。レベルが高いほど、誤検知率は低くなり、誤拒否率は高くなります。

6.7.2 デバイス経由で認識距離を設定

認証時にユーザーとカメラの有効距離を設定します。デバイスにログインしてください。詳細は
「*ログイン*」を参照してください。

システム設定 → 生体認証 → 顔 → 認識距離 をタップします。
認識距離を設定します。

6.7.3 デバイス経由での顔認証間隔設定

認証時の連続した顔認証間の時間間隔を設定します。デバイスにログインしてください。詳細は「*ログイン*」を参照してください。

システム設定 → 生体認証 → 顔 → 顔認識間隔（秒）をタップします。
顔認識の間隔を設定します。

注意
1 から 10 までの数字を入力してください。

6.7.4 デバイス経由で顔認証の1対Nセキュリティレベルを設定

1:N 照合モードによる認証時の照合閾値を設定します。デバイスにログインします。詳細は
「*ログイン*」を参照してください。

システム設定 → 生体認証 → 顔 → 顔認証1:Nセキュリティレベル をタップします。
1:Nマッチングモードによる認証時の照合閾値を設定します。
しきい値の値が大きいほど、顔認証時の誤認許容率は低くなり、誤拒否率は高くなります。最大値は100です。

6.7.5 デバイス経由での顔認証1:1セキュリティレベル設定

1:1照合モードでの認証時の一致閾値を設定します。デバイスにログインしてください。詳細は
「*ログイン*」を参照してください。

システム設定 → 生体認証 → 顔 → 顔1:1セキュリティレベル をタップします。
1:1照合モードによる認証時の照合しきい値を設定します。

しきい値の値が大きいほど、顔認証時の誤認許容率は低くなり、誤拒否率は高くなります。最大値は100です。

6.7.6 デバイス経由でのECOモードの有効化/無効化

ECOモードを有効にすると、低照度または暗所環境においてIRカメラによる顔認証が可能になります。

デバイスにログインします。詳細は*「ログイン」*を参照してください。

システム設定 → 生体認証 → 顔 → ECOモード設定 をタップします。

ECOモードが有効の場合、赤外線カメラを使用して低照度または暗い環境で顔認証が可能です。ECOモードのしきい値、ECOモード（1:N）、ECOモード（1:1）を設定できます。

ECOモードしきい値

ECOモードを有効にした場合、ECOモードのしきい値を設定できます。値が大きいほど、デバイスがECOモードに入りやすくなります。しきい値は照明量と関係があります。

ECOモード（1:1）

ECOモード1:1照合モードによる認証時の照合閾値を設定します。値が大きいほど誤認率（FAA）は低くなりますが、誤拒率（FAR）は高くなります。最大値は100です。

ECOモード（1:N）

ECOモード1:Nマッチングモードによる認証時のマッチング閾値を設定します。値が大きいほど誤認率は低くなりますが、誤拒否率は高くなります。最大値は100です。

6.7.7 デバイス経由でのヘルメット検知の有効化/無効化

ヘルメット検知を有効にした後、デバイスが顔認証を開始すると、システムは被験者がヘルメットを着用しているかどうかを検知します。

デバイスにログインします。詳細は*「ログイン」*を参照してください。

システム設定 → 生体認証 → 顔 → ヘルメット検知 をタップします。

ヘルメット検知

ヘルメット検知機能を有効にした後、ドア開放の戦略を設定できます。

なし

認証時にマスクを着用していない場合、デバイスは通知を表示しません。

着用リマインダー

認証時にヘルメットを着用していない場合、デバイスはポップアップ通知を表示し、ドアは開きます。

着用必須

認証時にヘルメットを着用していない場合、デバイスは警告を表示し、ドアは閉じたままになります。

6.7.8 デバイス経由でのマスク検知の有効化/無効化

マスク着用時の顔認証を有効にすると、システムはマスクを着用した状態で撮影された顔を認識します。

デバイスにログインします。詳細は*「ログイン」*を参照してください。

システム設定 → 生体認証 → 顔 → マスク設定 をタップします。

マスク着用顔検出を有効にすると、システムはマスクを着用した顔画像を認識します。設定可能な項目は、**マスク着用顔＆顔（1:1）**、**マスク着用顔＆顔（1:N）**、**ECOモード（1:1）閾値**、**ECOモード（1:N）閾値**、**およびプロンプト方法です**。

マスク着用顔と顔（1:1）

マスク着用顔と顔の1対1照合しきい値を設定します。値が大きいほど誤認率は低くなりますが、誤拒否率は高くなります。最大値は100です。

マスク着用顔と顔（1:N）

マスク1:Nマッチング閾値を設定します。値が大きいほど誤認率が低くなり、誤拒否率が高くなります。最大値は100です。

ECOモード（1:1）しきい値

ECOモードを有効にした後、マスク付き顔認証機能を設定できます。しきい値を設定可能です。

ECOモード1:1照合モードによる認証時の照合閾値を設定します。閾値の値が大きいほど、顔認証時の誤認率が低くなり、誤拒否率が高くなります。最大値は100です。

ECOモード（1:N）しきい値

ECOモードを有効にした後、マスク機能付き顔認証を設定できます。しきい値を設定可能です。

ECOモード1:Nマッチングモードによる認証時の一致閾値を設定します。閾値の値が大きいほど、顔認証時の誤認率は低くなり、誤拒否率は高くなります。最大値は100です。

戦略

設定：**なし**、**着用リマインダー**、**着用必須**。**なし**

認証時にマスクを着用していない場合、デバイスは通知を表示しません。

着用リマインダー

認証時にマスクを着用していない場合、デバイスが通知を表示し、ドアが開きます。

マスク着用必須

認証時にマスクを着用していない場合、デバイスが通知を表示し、ドアは閉じたままになります。

6.7.9 複数顔認証の有効化/無効化

複数顔認証を有効にすると、複数顔認証がサポートされます。デバイスにログインしてください。詳細は「*ログイン」を*参照してください。

システム設定 → 生体認証 → 顔認証 をタップします。

複数顔認証を有効にする。機能を有効にすると、複数の顔が同時に認証できるようになります。

注意

- 最大5名まで同時に認証可能です。
- 本機能を有効化した後、カードリーダー認証モード、カスタム認証、出勤状況、顔認証による手動認証は使用できません。

6.7.10 デバイス経由の顔重複チェック

顔重複チェック機能を有効にした後、人物の顔を追加する際、システムは重複をチェックします。システム内で重複した顔写真が検出された場合、プロンプトが表示されます。

注意

リモートでの顔写真の追加や一括適用では、この機能はサポートされていません。

デバイスにログインしてください。詳細は*「ログイン」を*参照してください。**システム設定 → 生体認証 → 顔** をタップします。

顔重複チェックを有効にします。機能を有効にした後、人物の顔を追加する際、システムは重複をチェックします。システム内で重複した顔写真が検出された場合、プロンプトが表示されます。

6.7.11 掌紋設定

手のひらの指紋認証タイムアウトしきい値と手のひらの指紋認証間隔を設定できます。デバイスにログインしてください。詳細は「*ログイン」*を参照してください。

システム設定 → 生体認証 → 手のひら認証 をタップします。

手のひら認証タイムアウトしきい値と**手のひら認証間隔**を設定します。

6.8 アルコール検知パラメータ設定

6.8.1 アルコール検知設定

アルコール検出パラメータを設定できます。

手順

1. デバイスにログインします。詳細は*「ログイン」*を参照してください。

2. **「アルコール検知」**をタップします。

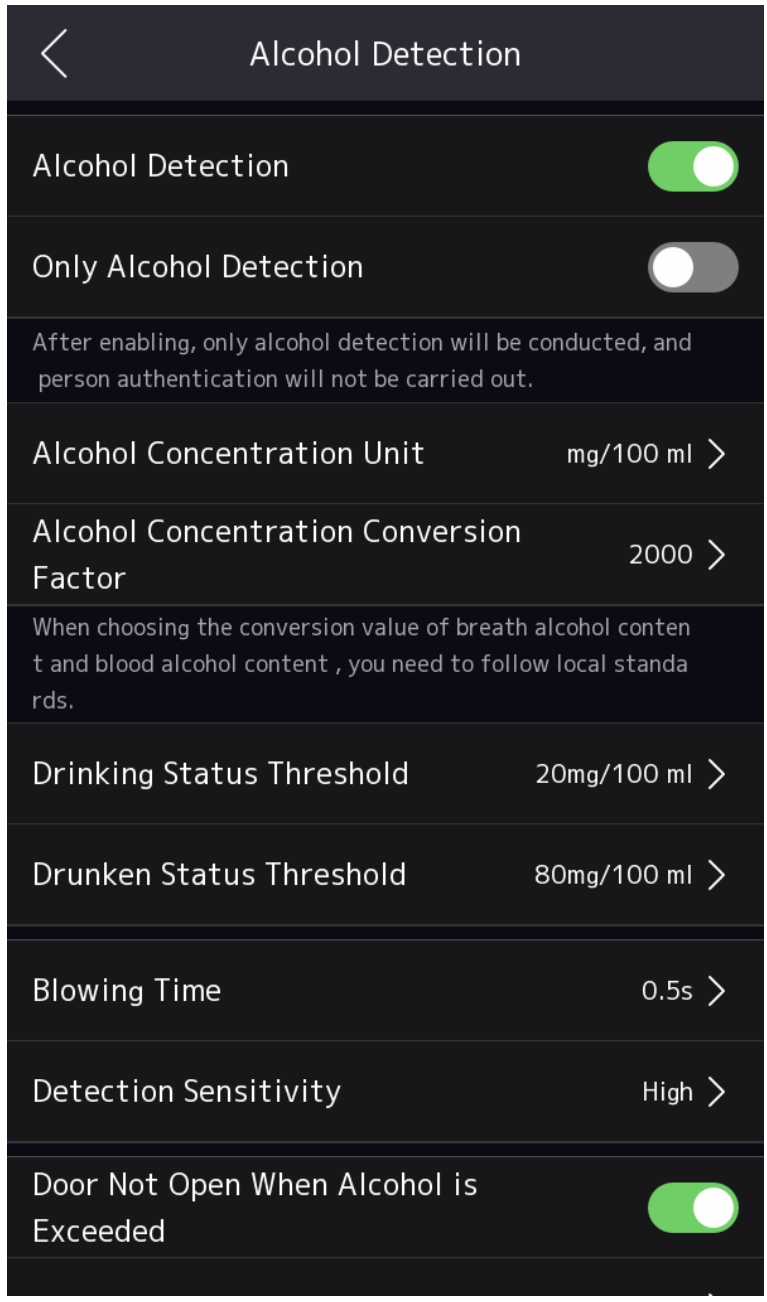


図6-13 アルコール検知

3. アルコール検出パラメータを設定します。

アルコール検知

アルコール検知機能が有効化されている場合、アルコール検知機能が最優先されます。

「体温測定のみ」と「複数人認証」を同時に有効にした場合、通常のアルコール検知機能は利用できなくなります。

アルコール検知のみ

有効化後、デバイスはアルコール検知機能のみをサポートし、その他の許可機能は無効になります。

アルコール濃度単位

濃度の単位はmg/100 mlまたはmg/Lから選択できます。

アルコール濃度換算係数設定

血中アルコール濃度（BAC）と呼気アルコール濃度（BrAC）の換算式：BAC（mg/L）= BrAC（mg/L）× k（kは換算係数）。

飲酒状態閾値／酩酊状態閾値

飲酒状態と酔い状態の閾値濃度を設定でき、濃度がそれ以上であれば「飲酒中」または「酔っている」と判断されます。

検出感度

検出感度を設定できます。感度が高いほど、検出がトリガーされやすくなります。

吹込時間

アルコール検知の吹き込み時間を設定します。

アルコール超過時のドア非開放／ドア非開放設定

アルコール基準超過時のドア開放禁止を有効にすると、検知時にアルコールが基準値を超えた場合、ドアは開放されません。**ドア開放禁止設定は「飲酒時」**または「**酩酊時」**に設定可能です。

6.8.2 アルコール検知モジュールの校正

使用前にアルコール検知モジュールの校正を行ってください。

初期画面を3秒間長押しし、表示されるジェスチャーに従って左右にスライドしてホームページにログインします。**「メンテナンス」→「システム情報」を**タップします。

右隅の「」を長押しし、詳細設定ページに入ります。「**アルコール検知モジュール校正**」をタップします。

1.アルコール検知器の校正プロンプトを表示します。

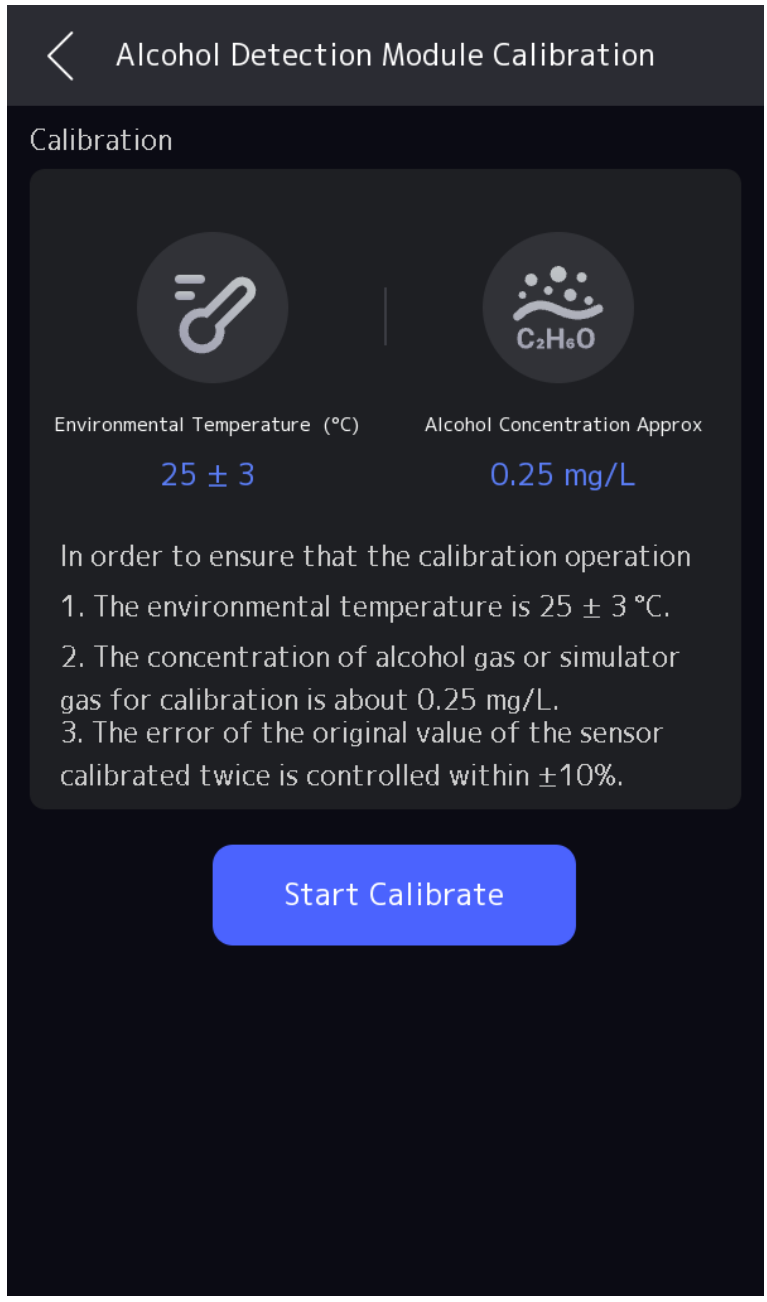


図6-14 アルコール検知器の校正プロンプト

2. **「校正開始」を**タップし、吹込用ピストルに近づけて、音が止まるまで継続的に吹込みます。

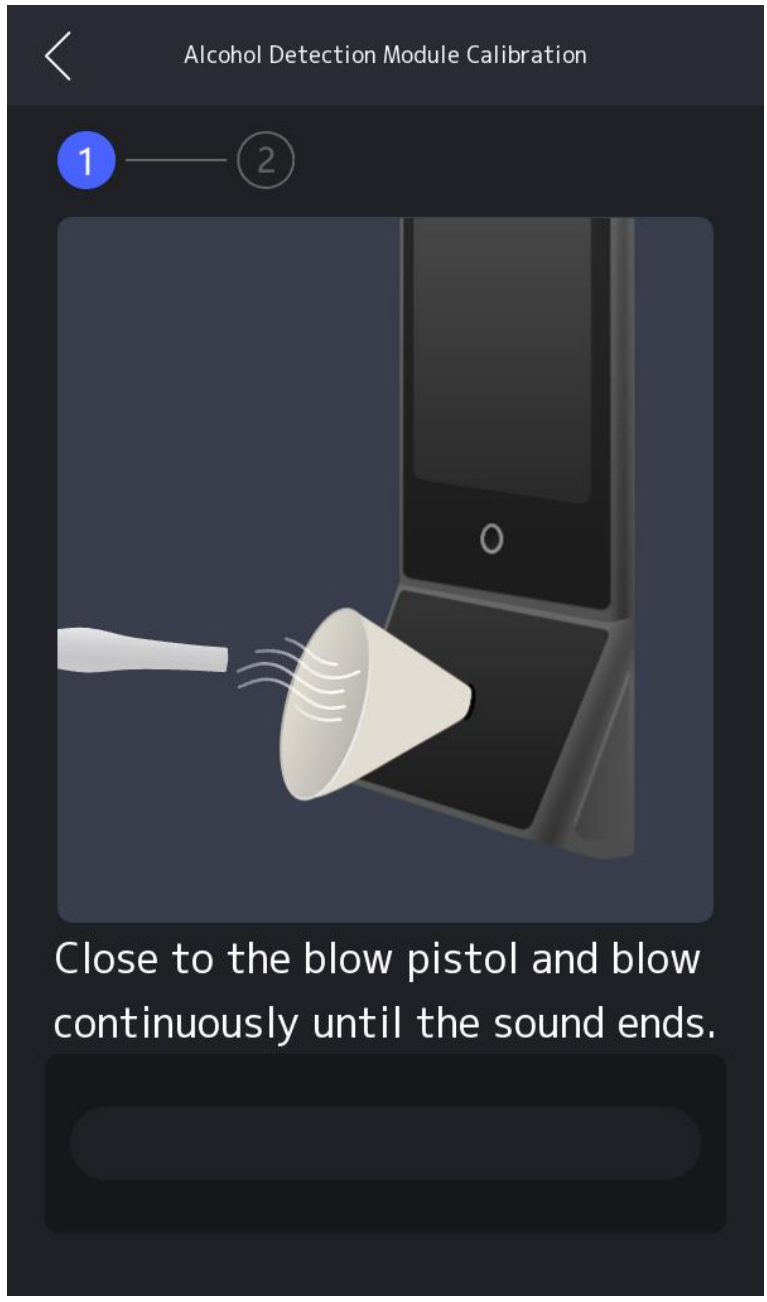


図 6-15 校正を開始

3. 校正結果を表示します。

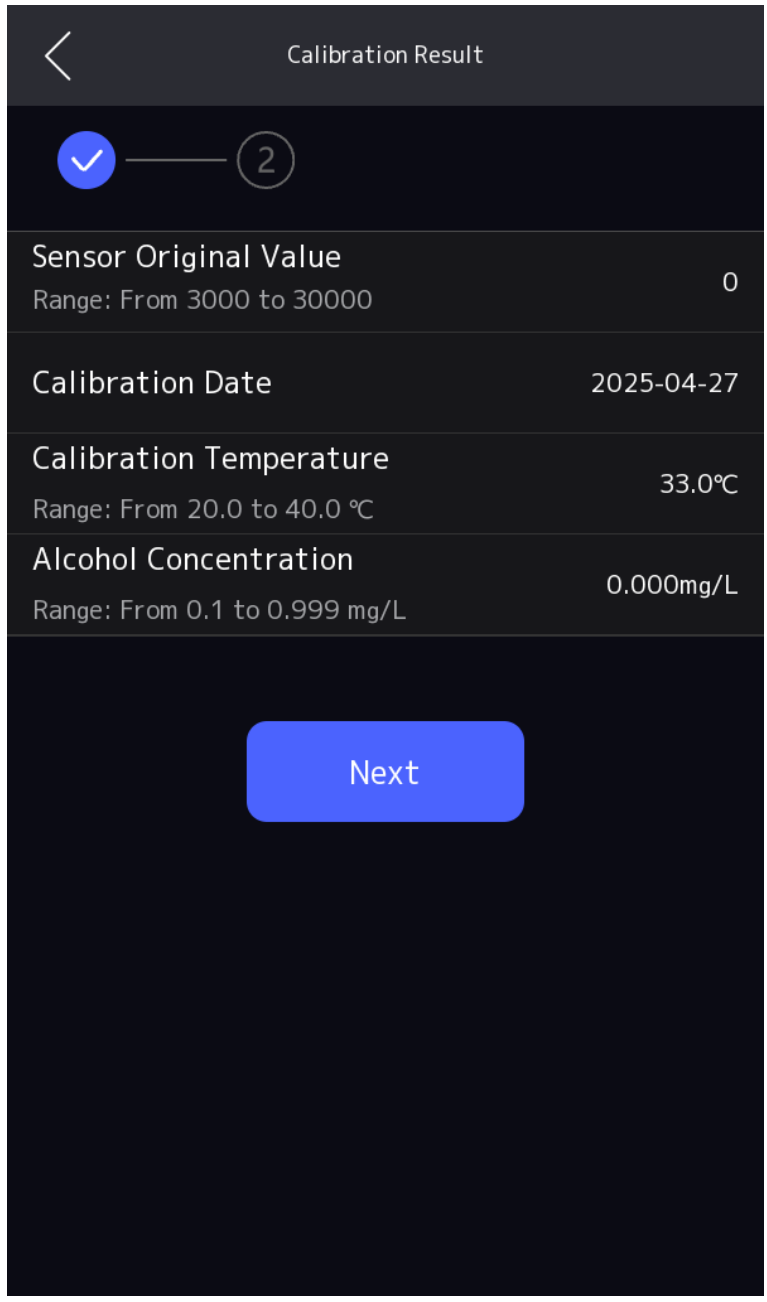


図 6-16 較正結果の表示

4. 校正を繰り返します。
5. 2 つの校正結果を比較します。測定の安定性を確保するには、誤差範囲が ±10% 以内である必要があります。

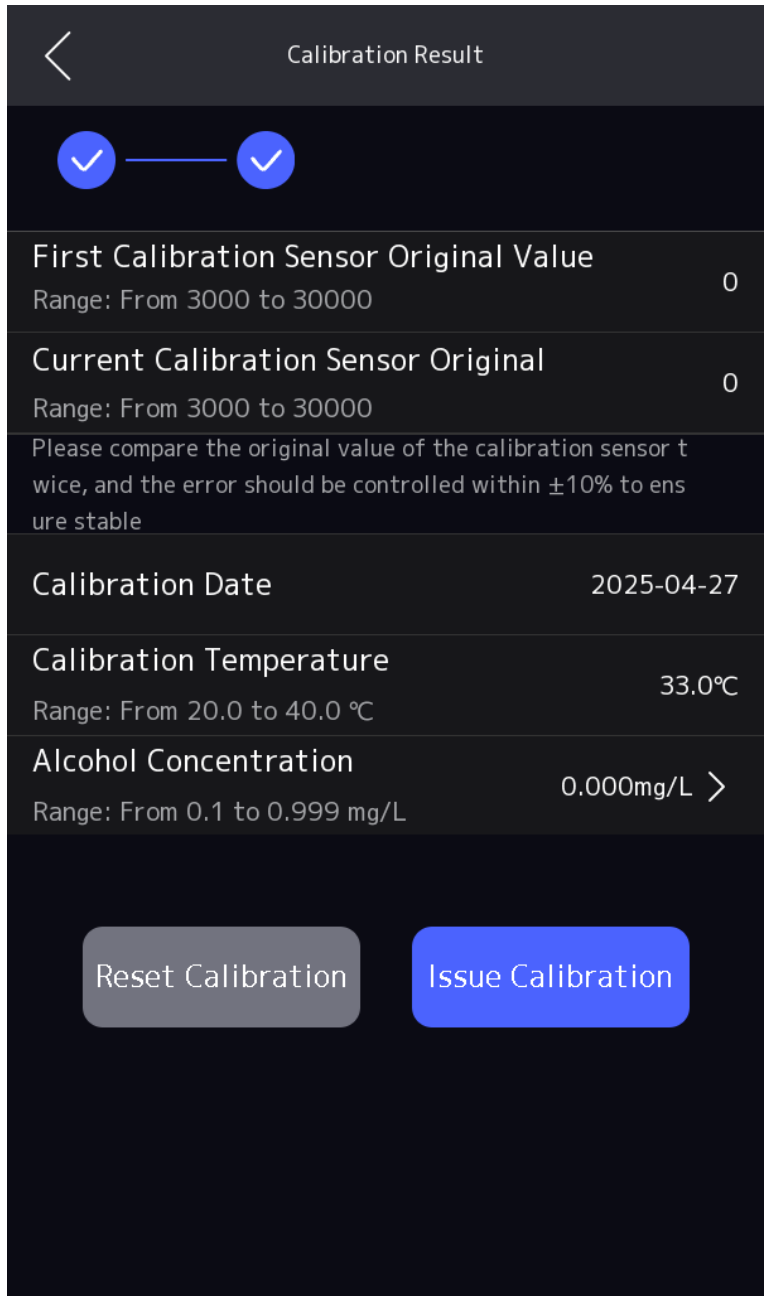


図6-17 2つのキャリブレーション結果の比較

6. **「校正を発行」**をタップします。

6.9 アクセス制御設定

アクセス制御の権限を設定できます。

ホーム画面で**「ACS」を**タップし、設定ページに入ります。

6.9.1 端末認証モードの設定

顔認証端末の認証モードを選択します。認証には異なる組み合わせを選択できます。

端末にログインします。詳細は*「ログイン」を*参照してください。**ACS → 端末認証モード を**タップします。

人物認証の種類と方法を選択し、設定を保存します。

デバイスの認証モードが「**デバイスモード**」に設定されている場合、そのデバイス上のすべてのユーザーはデバイス認証モードを使用します。ユーザー認証モード設定の詳細については、*「認証モードの設定」を*参照してください。

注
指紋モジュール搭載デバイスは指紋認証機能をサポートします。

注意
生体認証製品は、偽装防止環境に完全に対応しているわけではありません。より高いセキュリティレベルが必要な場合は、複数の認証モードを使用してください。

6.9.2 デバイス経由でのリーダー認証モード設定

有線外部リーダーで人物認証タイプを設定します。認証には異なる組み合わせを選択できます。

デバイスにログインします。詳細は*「ログイン」を*参照してください。

ACS → リーダー認証モード をタップします。

本人認証の種類を選択し、設定を保存してください。

人物認証タイプと方法を選択し、設定を保存します。

デバイスの認証モードが「**デバイスモード**」に設定されている場合、そのデバイス上の全ユーザーはデバイス認証モードを使用します。ユーザー認証モード設定の詳細については、*「認証モードの設定」を*参照してください。

注
指紋モジュール搭載デバイスは指紋認証機能をサポートします。

注意
生体認証製品は、偽装防止環境に完全に対応しているわけではありません。より高いセキュリティレベルが必要な場合は、複数の認証モードを使用してください。

6.9.3 PC Web経由で手動に顔認証をトリガーする

顔認証による手動認証を有効にした後、顔認識を行うにはデバイスの画面を手動でタッチする必要があります。

デバイスにログインします。詳細は*「ログイン」*を
参照してください。

ACSをタップします。

「顔認証による手動トリガー認証」を有効にし、「**認証**」を「**シングル**」または「**連続シングル**」に設定します

顔認証を行う前に、認証ページで**認証**をタップして認識を開始する必要があります。

連続

認証をトリガーした後、デバイスがスリープモードに入るまで顔認証が可能です。

6.9.4 NFC カードの有効化/無効化

NFCカード機能を有効/無効にします。

ログイン後、**ACS**をタップしてください。

NFCを有効にするをタップします。有効化後、デバイスはNFCカードを読み取れます。

注意

デュアル周波数カードモジュールが顔認証端末にアクセスする場合、端末でのカードスワイプは無効です。

6.9.5 M1カードの有効化/無効化

M1カード機能を有効または無効にします。

端末にログインします。詳細は*「ログイン」*を参照
してください。ログイン後、**ACS**をタップします。

「**M1カード有効化**」をタップすると、デバイスがM1カードを読み取れます。

M1カードの有効化

有効化後、デバイスはM1カードを読み取ることができます。

M1カード暗号化

M1カード暗号化を有効化すると、デバイスはM1カードのセクターを検証します。プラットフォームでM1カードの暗号化セクターを設定してください。

注意

デュアル周波数カードモジュールが顔認証端末にアクセスする場合、デバイス上でのカードスワイプは無効となります。

6.9.6 キーフォブ設定

キーフォブのパラメータを設定できます。

手順

1. **アクセス制御設定 → キーフォブ設定** をタップします。
2. **認識距離**を選択します。
3. **ドアを開けるにはボタンを押す**を設定します。

6.9.7 リモート認証

リモートプラットフォームによる認証の可否を判断します。デバイスにログインし

ます。詳細は「*ログイン」を*参照してください。

ACSをタップします。

リモート認証を有効化します。認証を行うユーザーがいる場合、リモートプラットフォームが認証の可否を判断します。

デバイス上で認証情報を認証し、プラットフォームで検証します。

「**ローカルでの認証情報の検証**」を有効にすると、検証はデバイス上で実行されます。

6.9.8 デバイス経由で認証間隔を設定

デバイスにログインします。詳細は*「ログイン」*を参照してください。

ACSをタップし、**認証間隔**を設定して保存します。

認証時に同一ユーザーの本認証間隔を設定できます。設定された間隔内で同一ユーザーは1回のみ認証可能です。2回目の認証は失敗します。

利用可能な認証間隔の範囲：0～65535。

6.9.9 デバイス経由で認証結果表示時間を設定

認証時の認証結果表示時間を設定します。デバイスにログインします。詳細は「*ログ*

*イン」*を参照してください。

ACSをタップし、**認証結果表示時間を**設定して保存します。

6.9.10 パスワードモードの設定

パスワードモードを設定し、パスワードを編集する場所（端末／PCウェブ／プラットフォーム）を選択できます。

手順

1. デバイスにログインします。詳細は*「ログイン」*を参照してください。
2. **ACS**をタップします。
3. **「パスワードモード」**をタップし、モードを設定します。

   プラットフォーム適用個人用PIN

   デバイスがプラットフォームにアクセスした後、PIN はプラットフォームによって管理および配布されます。

   デバイス設定個人用PIN

   PIN は、デバイスまたは PC Web で設定されます。
4. 設定を保存するには前のページに戻ってください。

6.9.11 ドアパラメータ設定

ドアのロック解除に関するパラメータを設定します。

デバイス経由でドア番号を設定

デバイス用のドア番号を選択します。

デバイスにログインします。詳細は*「ログイン」*を参照してください。

ログイン後、**ACS**をタップします。

ドア番号をタップします。**ドア1**または**ドア2**を選択します。

ドア1は入口に設置されたデバイスを指します。ドア2は出口に設置されたデバイスを指します。

デバイス経由でドアコンタクトを設定

ドアコンタクトの配線方法に応じてドアコンタクトの状態を選択します。

デバイスにログインします。詳細は*「ログイン」*を参照してください。

ACSをタップします。

実際のニーズに応じて「開いたまま」または「閉じたまま」を選択できます。デフォルトは「閉じたまま」です。

デバイス経由で開扉時間設定

ドアの解錠時間を設定します。

デバイスにログインします。詳細は*「ログイン」*を
参照してください。**ACS**をタップします。
ドアの解錠時間を設定します。設定時間内にドアが開かれない場合、ドアはロックされます。設定可能なドアロック時間範囲：1～255秒。

6.10 プラットフォーム勤怠管理

実際の状況に応じて、出勤モードを「出勤」「退勤」「休憩開始」「休憩終了」「残業開始」「残業終了」から設定できます。

注意

本機能はクライアントソフトウェアの勤怠管理機能と連携してご利用ください。

6.10.1 デバイス経由での出席モード無効化

出勤モードを無効にすると、システムは初期画面に出勤状況を表示しません。

プラットフォーム出席をタップして、T&Aステータスページに入ります。

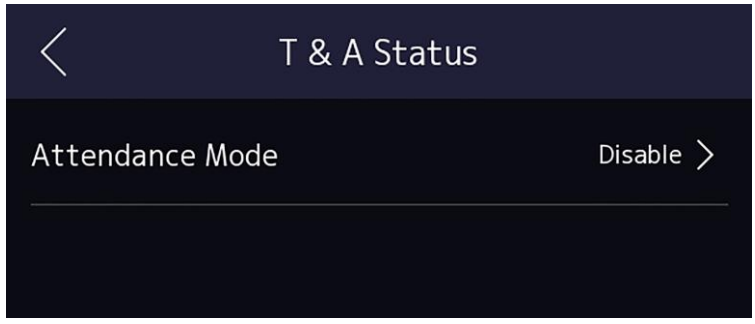


図6-18 勤怠モードを無効にする

出勤モードを「**無効**」に設定します。
初期ページで出勤ステータスを表示または設定することはできません。システムはプラットフォームで設定された出勤ルールに従います。

6.10.2 デバイス経由での手動出席設定

出席モードを手動に設定し、出席を取る際には手動でステータスを選択する必要があります。

開始前に

少なくとも1人のユーザーを追加し、そのユーザーの認証モードを設定してください。詳細は「*ユーザー管理*」を参照してください。

手順

1. **プラットフォーム出席**をタップして、T&Aステータスページに入ります。
2. **出席モード**を「**手動**」に設定します。

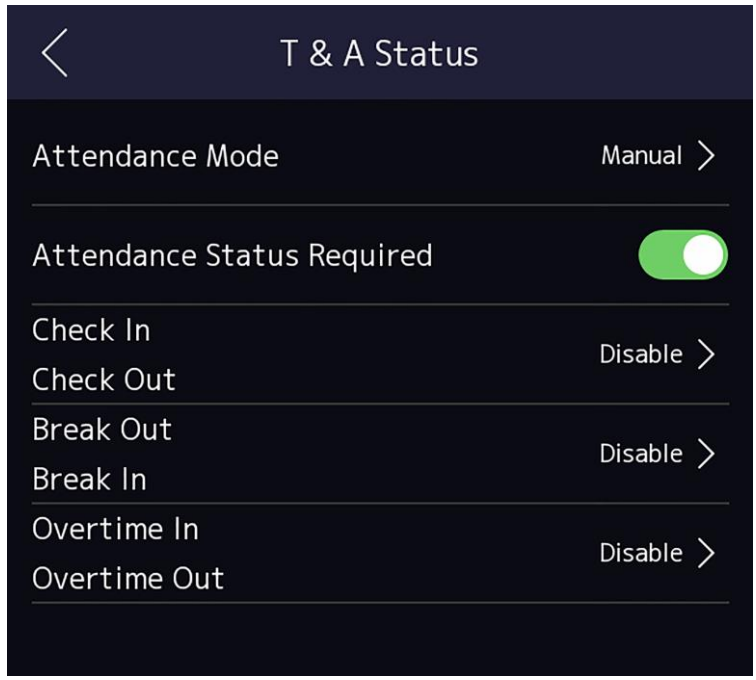


図6-19 手動勤怠モード

3. **「出勤状況必須」**を**有効**にします。
4. 出席ステータスのグループを有効にします。

注記

出席プロパティは変更されません。

5. **オプション：**必要に応じてステータスを選択し、名前を変更してください。
   この名称は、勤怠状況ページおよび認証結果ページに表示されます。

結果

認証後、手動で出勤ステータスを選択する必要があります。

注

ステータスを選択しない場合、認証は失敗し、有効な出勤としてマークされません。

6.10.3 デバイス経由での自動出席設定

出席モードを自動に設定すると、出席ステータスとその利用可能なスケジュールを設定できます。システムは設定されたスケジュールに従って出席ステータスを自動的に変更します。

開始前に

少なくとも1人のユーザーを追加し、ユーザーの認証モードを設定してください。詳細は「*ユーザー管理*」を参照してください。

手順

1. **プラットフォーム出席**をタップして、T&Aステータスページに入ります。
2. **出勤モード**を「**自動**」に設定します。

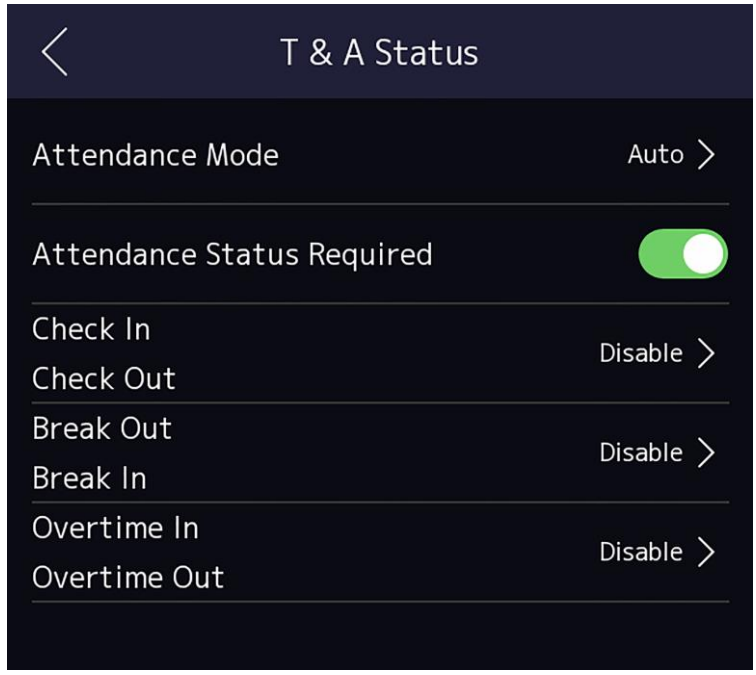


図 6-20 自動勤怠モード

3. **出勤**ステータス機能を有効にします。
4. グループ単位で出勤ステータスを有効にします。

注記

出席プロパティは変更されません。

5. **オプション：**必要に応じてステータスを選択し、名前を変更してください。
   この名称は、勤怠管理ステータスページおよび認証結果ページに表示されます。

6. ステータスのスケジュールを設定します。

1) **出勤スケジュールを**タップします。

2) **月曜日**、**火曜日**、**水曜日**、**木曜日**、**金曜日**、**土曜日**、**日曜日**を選択します。

3) 選択した出勤ステータスのその日の開始時刻を設定します。

4) **確認**をタップします。

5) 実際の必要に応じて、手順1から4を繰り返してください。

注記

設定されたスケジュール内で、出席状況は有効となります。

結果

初期ページで認証を行うと、設定されたスケジュールに基づき、設定された出席ステータスとして認証がマークされます。

例

ブレイクアウトを月曜11:00、**ブレイクイン**を月曜12:00に設定した場合、月曜11:00から12:00までの有効なユーザー認証は休憩としてマークされます。

6.10.4 デバイス経由での手動・自動出席設定

出勤モードを「**手動**」と「**自動**」に設定すると、システムは設定されたスケジュールに従って出勤ステータスを自動的に変更します。同時に、認証後に出勤ステータスを手動で変更することも可能です。

開始前に

少なくとも1人のユーザーを追加し、ユーザーの認証モードを設定してください。詳細は「*ユーザー管理*」を参照してください。

手順

1. プラットフォーム勤怠をタップして勤怠状況ページに入ります。

2. 出勤モードを「手動」と「自動」に設定します。

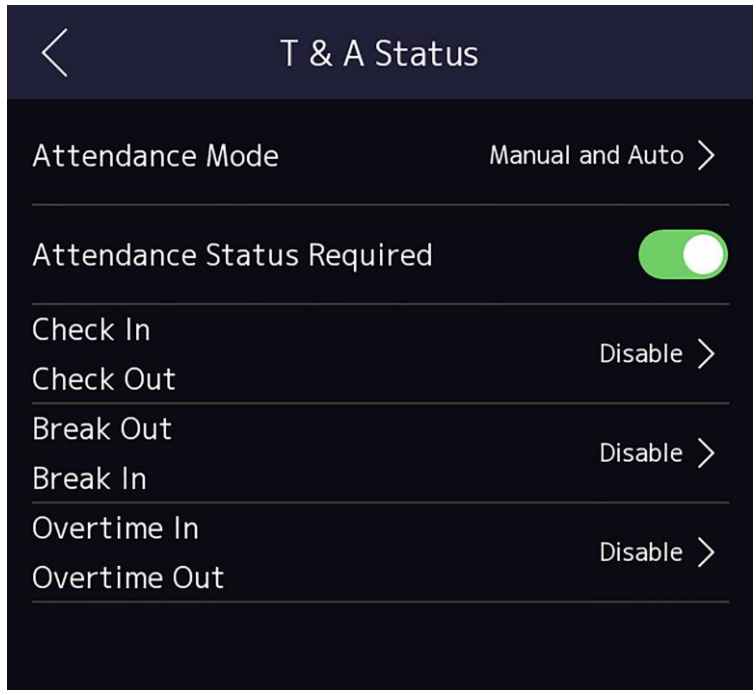


図6-21 手動モードと自動モード

3. **出席**状況機能を有効にする。
4. 出席状況のグループを有効にする。

注記

出席プロパティは変更されません。

5. **オプション：**必要に応じてステータスを選択し、その名前を変更します。

   この名前は、勤怠ステータスページと認証結果ページに表示されます。
6. ステータスのスケジュールを設定します。
   1) **「出勤スケジュール」**をタップします。
   2) **月曜日**、**火曜日**、**水曜日**、**木曜日**、**金曜日**、**土曜日**、または**日曜日**を選択します。
   3) 選択した出席ステータスの当日の開始時刻を設定します。
   4) **OK**をタップします。
   5) 実際の必要に応じて、手順 1 から 4 を繰り返します。

注記

設定されたスケジュール内で出席ステータスが有効になります。

結果

初期ページで認証を行います。スケジュールに基づき、設定された出席ステータスとして認証が記録されます。結果タブの編集アイコンをタップすると、手動で出席ステータスを選択できます。編集した出席ステータスとして認証が記録されます。

例
ブレイクアウトを月曜11:00、**ブレイクイン**を月曜12:00に設定した場合、月曜11:00～12:00の有効なユーザー認証は休憩としてマークされます。

6.11 設定

設定パラメータを構成できます。

手順

1. システム → 設定をタップして設定ページに入ります。

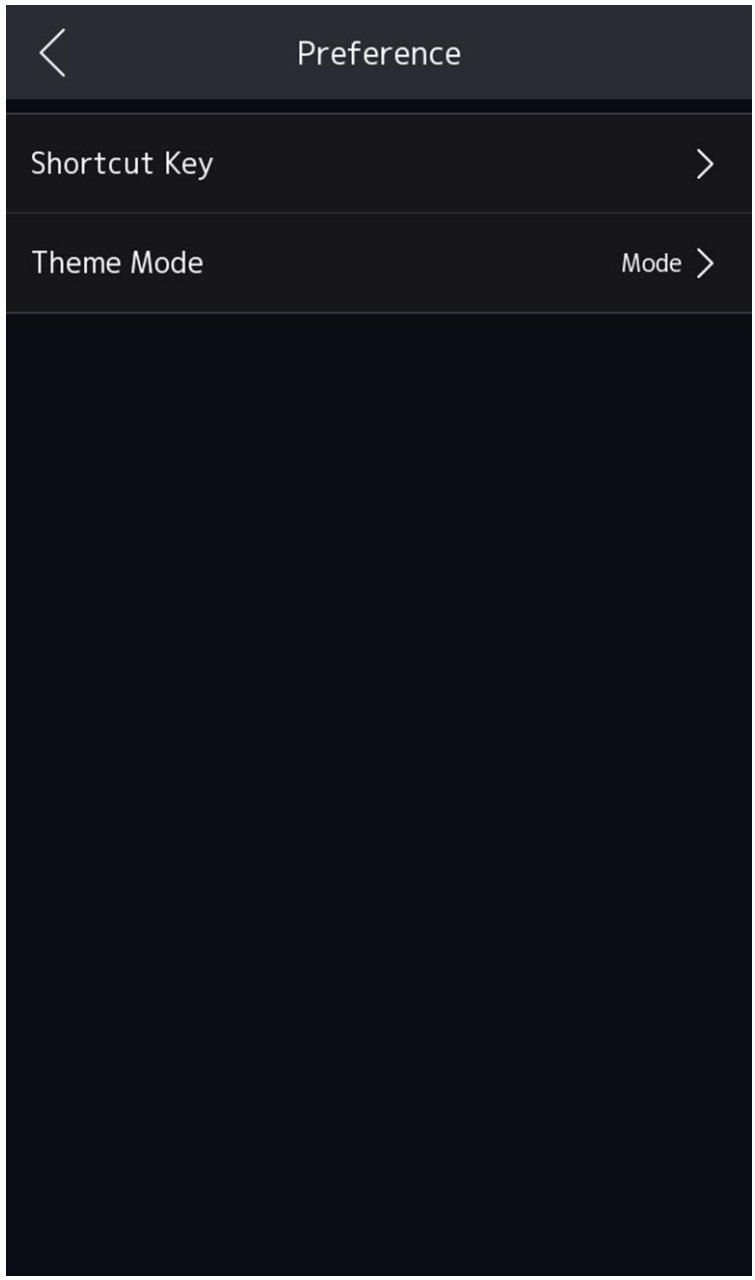


図 6-22 設定

6.11.1 デバイス経由でのショートカットキー設定

認証ページに表示されるショートカットキーを選択します。QRコード機能、通話機能、通話タイプ、パスワード入力機能を含みます。

デバイスにログインします。詳細は*「ログイン」*を参照してください。

システム設定 → 設定 をタップします。

認証ページに表示されるショートカットキーを選択します。QRコード機能、通話機能、通話タイプ、パスワード入力機能などがあります。

パスワード

この機能を有効にすると、パスワードによる認証が可能になります。認証ページで「」をタップして確認してください。

QRコード

認証インターフェースでQRコードスキャン機能をご利用いただけます。デバイスは取得したQRコードに関連付けられた情報をプラットフォームにアップロードします。認証ページで「」をタップして確認してください。

通話

通話タイプとして「通話ルーム」「コールセンター」「指定ルーム通話」「APP通話」から選択可能です。**「指定ルーム通話」**を選択した場合、ルーム番号を入力する必要があります。

認証ページで「」をタップして呼び出します。

屋内ステーション番号を呼び出す

有効化後、認証ページに室内機番号が表示されます。

管理センターへの通話／VoIPセンターへの通話

有効化後、認証ページから管理センターまたはVoIPセンターへ発信できます。

6.11.2 テーマ

異なるテーマを選択すると、認証ページに表示される内容が異なります。デバイスにログインします。詳

細は「*ログイン*」を参照してください。

システム**設定 → 設定**

テーマモードを選択します。

認証

ライブビューが認証画面に表示され、同時に人物名、社員ID、顔写真も表示されます。

広告

本装置の広告表示領域と本人確認認証領域は別々の画面に表示されます。広告表示領域には動画、テキスト、ウェルカムメッセージが表示されます。

インターコムモード

このモードを選択すると、認証ページの下部にショートカットが表示されます。

6.12 システムメンテナンス

初期ページを 3 秒間長押しし、ジェスチャーに従って左/右にスライドしてホームページにログインします。**Maint** をタップします。

6.12.1 システム情報の表示

デバイスのシステム情報を表示します。

初期画面を3秒間長押しし、表示されるジェスチャーに従って左右にスライドしてホームページにログインします。［**メンテナンス**］→［**システム情報**］をタップします。

デバイスのモデル、シリアル番号、バージョン、アドレス、製造データ、QRコード、オープンソースコードライセンスを確認できます。

注意

デバイスモデルによって表示内容が異なる場合があります。詳細は実際の画面を参照してください。

右隅の を長押しすると、詳細設定ページに入ります。生体認証パラメータの設定、デバイスバージョン情報の確認、アルコール検知モジュールのキャリブレーション情報閲覧が可能です。

生体認証パラメータ

カスタム偽装検知顔認証生体検知レベル

顔偽装防止機能を有効にした後、顔の生体認証を行う際の照合セキュリティレベルを設定できます。

偽装検知閾値

値が大きいほど誤認率が低くなり、誤拒否率が高くなります。値が小さいほど誤認率が高くなり、誤拒否率が低くなります。

偽装防止保護のための顔ロック

この機能を有効にすると、なりすまし防止検出が失敗した場合にデバイスが自動的にロックされます。

ロック時間

偽装検出に失敗した場合の**偽装防止保護用ロック顔**認証有効化後のロック時間。

バージョン情報

デバイスの情報を表示できます。

アルコール検知モジュール

アルコール検知モジュールのバージョン情報と校正情報を確認できます。

6.12.2 デバイス経由でデバイス容量を表示

デバイスの容量を確認できます。

初期画面を3秒間長押しし、表示されるジェスチャーに従って左右にスライドしてホームページにログインします。**「メンテナンス」→「容量」を**タップします。

ユーザー数、顔写真、カード、指紋、掌紋、キーフォブ、イベントを確認できます。

注意

指紋モジュールを搭載したデバイスのみが指紋容量の表示をサポートします。

6.12.3 アップグレード

オンラインアップグレード

デバイスをオンラインでアップグレードできます。

初期画面を3秒間長押しし、表示されるジェスチャーに従って左右にスライドしてホームページにログインします。**［メンテナンス］→［デバイスアップグレード］を**タップします。

デバイスがネットワークに接続され、Hik-Connectアプリに追加されている場合、Hik-Connectアプリに更新版があるときは、デバイス上で**「デバイスアップグレード」→**「オンラインアップグレード」をタップしてアップグレードできます。

ローカルアップグレード

デバイスをローカルでアップグレードできます。

初期画面を3秒間長押しし、表示されるジェスチャーに従って左右にスライドしてホームページにログインします。**「メンテナンス」→「デバイスアップグレード」を**タップします。

USBフラッシュドライブを挿入します。**デバイスアップグレード → USB経由で更新**をタップすると、デバイスがUSBフラッシュドライブ内のdigicap.davファイルを読み込み、アップグレードを開始します。

6.12.4 設定の復元

デバイス経由での工場出荷時設定への復元

すべてのパラメータが工場出荷時の設定に復元されます。

初期画面を3秒間長押しし、表示されるジェスチャーに従って左右にスライドしてホーム画面にログインします。**「メンテナンス」→「工場出荷時設定に復元」を**タップします。システムが再起動し設定が有効になります。

デバイス経由でのデフォルト設定への復元

通信設定、リモートでインポートされたユーザー情報を除く全てのパラメータがデフォルト設定に復元されます。

初期画面を3秒間長押しし、表示されるジェスチャーに従って左右にスライドしてホームページにログインします。**「メンテナンス」→「デフォルト設定に復元」を**タップします。システムが再起動し、設定が有効になります。

通信設定を除くすべてのパラメータ、およびリモートでインポートされたユーザー情報は、システムのデフォルト設定に復元されます。デフォルト設定の復元後、システムは再起動します。

デバイスの再起動

デバイスを手動で再起動できます。

初期画面を3秒間長押しし、表示されるジェスチャーに従って左/右にスライドしてホームページにログインします。「**Maint.**」**→「Reboot」を**タップします。

6.13 ビデオインターホン

クライアントソフトウェアにデバイスを追加後、クライアントソフトウェアからデバイスへ発信、デバイスからメインステーションへ発信、デバイスからクライアントソフトウェアへ発信、デバイスから屋内ステーションへ発信、またはデバイスから特定の部屋へ発信が可能です。

6.13.1 デバイスからクライアントソフトウェアへ呼び出し

手順

1. 付属ディスクまたは公式ウェブサイトからクライアントソフトウェアを入手し、指示に従ってインストールしてください。
2. クライアントソフトウェアを実行すると、ソフトウェアのコントロールパネルが表示されます。
3. **「デバイス管理」**をクリックしてデバイス管理インターフェースに入ります。
4. クライアントソフトウェアにデバイスを追加します。

   注意

   デバイスの追加に関する詳細は、「*デバイスの追加*」を参照してください。
5. クライアントソフトウェアを呼び出します。
   1) デバイスの初期ページで「」をタップします。
   2) ポップアップウィンドウに「***0***」を入力します。
   3) をタップしてクライアントソフトウェアを呼び出します。

6. クライアントソフトウェアのポップアップページで**「応答」を**タップすると、デバイスとクライアントソフトウェア間の双方向音声通信を開始できます。

注意
デバイスが複数のクライアントソフトウェアに追加されている場合、デバイスがクライアントソフトウェアを呼び出すと、デバイスを最初に追加したクライアントソフトウェアのみに通話受信ウィンドウが表示されます。

6.13.2 デバイスからのコールセンター

手順

1. 付属ディスクまたは公式ウェブサイトからクライアントソフトウェアを入手し、指示に従ってソフトウェアをインストールしてください。
2. クライアントソフトウェアを実行すると、ソフトウェアのコントロールパネルが表示されます。
3. **「デバイス管理」**をクリックしてデバイス管理インターフェースに入ります。
4. クライアントソフトウェアにメインステーションとデバイスを追加します。

注意
デバイスの追加に関する詳細は、*「デバイスの追加」*を参照してください。

5. リモート設定ページで、メインステーションのIPアドレスとSIPアドレスを設定します。

注
操作の詳細については、メインステーションの取扱説明書を参照してください。

6. センターに電話してください。
   - ***基本設定***でセンターへの通話設定を行っている場合、をタップするとセンターに電話をかけられます。
   - ***基本設定で***センターへの通話が設定されていない場合は、→をタップしてセンターへ電話をかける必要があります。
7. メインステーション経由で応答し、双方向オーディオを開始します。

注意
デバイスは優先的にメインステーションに呼び出しを行います。

6.13.3 クライアントソフトウェアからデバイスを呼び出す

手順

1. 付属ディスクまたは公式ウェブサイトからクライアントソフトウェアを入手し、指示に従ってインストールしてください。
2. クライアントソフトウェアを実行すると、ソフトウェアのコントロールパネルが表示されます。
3. **「デバイス管理」**をクリックしてデバイス管理ページに入ります。
4. クライアントソフトウェアにデバイスを追加します。

デバイスの追加に関する詳細は、「*デバイスの追加*」を参照してください。

5. **ライブ**ビューページに入り、追加したデバイスをダブルクリックしてライブビューを開始します。

注

ライブビューページでの操作の詳細については、クライアントソフトウェアのユーザーマニュアルの「*ライブビュー*」を参照してください。

6. ライブビュー画像を右クリックすると、右クリックメニューが開きます。
7. **双方向オーディオを開始**をクリックすると、デバイスとクライアントソフトウェア間の双方向オーディオが開始されます。

6.13.4 デバイスからルームを呼び出す

手順

1. 付属ディスクまたは公式ウェブサイトからクライアントソフトウェアを入手し、指示に従ってソフトウェアをインストールします。
2. クライアントソフトウェアを実行すると、ソフトウェアのコントロールパネルが表示されます。
3. **「デバイス管理」**をクリックしてデバイス管理インターフェースに入ります。
4. クライアントソフトウェアに室内機とデバイスを追加します。

注意

デバイスの追加に関する詳細は、「*デバイスの追加*」を参照してください。

5. ユーザーを室内機に関連付け、室内機の部屋番号を設定します。
6. その部屋を呼び出します。
   - ***基本設定で***特定の部屋番号を設定している場合、をタップするとその部屋に呼び出しできます。
   - ***基本設定で***特定の部屋番号を設定していない場合は、デバイスの認証ページで をタップしてください。ダイヤル画面で部屋番号を入力し、 をタップして部屋を呼び出します。
7. 屋内機が応答したら、屋内機との双方向音声通信を開始できます。

6.13.5 デバイスからモバイルクライアントを呼び出す

手順

1. 付属ディスクまたは公式ウェブサイトからモバイルクライアントを入手し、指示に従ってソフトウェアをインストールしてください。
2. モバイルクライアントを実行し、デバイスをモバイルクライアントに追加してください。

注記

詳細は、モバイルクライアントのユーザーマニュアルを参照してください。

3. **基本設定 → ショートカットキー** を入力し、**APP 呼び出しを**有効にします。
4. 初期ページに戻り、モバイルクライアントを呼び出します。

1) デバイスの初期画面で、 をタップします。
2) をタップしてモバイルクライアントを呼び出します。

第7章 Webブラウザによる操作

7.1 ログイン

ウェブブラウザまたはクライアントソフトウェアのリモート設定からログインできます。

注記
デバイスがアクティブ化されていることを確認してください。

Web ブラウザ経由でのログイン

Web ブラウザのアドレスバーにデバイスの IP アドレスを入力し、**Enter** キーを押してログインページに入ります。
デバイスのユーザー名とパスワードを入力します。**ログイン**をクリックします。

クライアントソフトウェアのリモート設定によるログイン

クライアントソフトウェアをダウンロードして開きます。デバイスを追加した後、[ ]をクリックして設定ページに入ります。

7.2 パスワードを忘れた場合

ログイン時にパスワードを忘れた場合、メールアドレスまたはセキュリティ質問でパスワードを変更できます。

ログインページで「**パスワードを忘れた場合**」をクリック
します。**確認モード**を選択します。

セキュリティ質問による認証

セキュリティの質問に答えます。

メール認証

1. QRコードをエクスポートし、***pw_recovery@hikvision.com*** 宛に添付ファイルとして送信してください。
2. ご登録のメールアドレスに5分以内に確認コードが届きます。
3. 本人確認のため、確認コード欄に確認コードを入力してください。**次に**進み、新しいパスワードを作成して
確認してください。

7.3 ヘルプ

7.3.1 オープンソースソフトウェアライセンス

オープンソースソフトウェアのライセンスを確認できます。

右上の「 」→「**Open Source Software Statement**」をクリックしてライセンスを表示します。

7.3.2 オンラインヘルプドキュメントを表示

Web 設定のヘルプ文書を表示できます。

→ Webページ右上の「**オンライン文書**」をクリックして文書を表示します。

7.4 ログアウト

アカウントからログアウトします。

admin → Logout → OK をクリックしてログアウトします。

7.5 Webブラウザによるクイック操作

7.5.1 パスワード変更

デバイスのパスワードを変更できます。

ウェブページの右上にある「 」をクリックすると、**パスワード**変更ページが表示されます。ドロップダウンリストからセキュリティの質問を設定し、その回答を入力することができます。

設定を完了するには「**次へ**」をクリックしてください。または、この手順をスキップするには「**スキップ**」をクリックしてください。

7.5.2 言語を選択

デバイスのシステム言語を選択できます。

ウェブページの右上にある「 」をクリックすると、デバイス言語設定ページが表示されます。ドロップダウンリストからデバイスシステムの言語を選択できます。

デフォルトでは、システム言語は英語です。

注意

システム言語を変更すると、デバイスは自動的に再起動します。

7.5.3 時刻設定

ウェブページの右上にある「 」をクリックしてウィザードページに入ります。デバイスの言語を設定した後、「**次へ**」をクリックすると「**時刻設定**」ページに進みます。

タイムゾーン

ドロップダウンリストからデバイスの所在するタイムゾーンを選択します。

時刻同期

NTP

NTP サーバーの IP アドレス、ポート番号、および間隔を設定する必要があります。

手動

デフォルトでは、デバイスの時刻は手動で同期する必要があります。デバイスの時刻を手動で設定するか、**[コンピュータの時刻と同期] を**チェックしてデバイスの時刻をコンピュータの時刻と同期させることができます。

サーバーアドレス/NTP ポート/間隔

サーバーアドレス、NTPポート、間隔を設定できます。

DST

夏時間の開始時刻、終了時刻、およびバイアス時間を表示できます。

[次へ] をクリックして設定を保存し、次のパラメータに進みます。**[スキップ]** をクリックすると、時刻設定をスキップできます。

7.5.4 プライバシー設定

画像のアップロードと保存に関するパラメータを設定します。

ウェブページの右上にある「 」をクリックしてウィザードページに入ります。

画像のアップロードと保存

認証時に画像を保存する

認証時に画像を自動的に保存する。

認証時に画像をアップロード

プラットフォームへの認証時に画像を自動的にアップロードする。

登録済み画像を保存

この機能を有効にすると、登録された顔写真がシステムに保存されます。

リンク撮影後の画像アップロード

リンクされたカメラで撮影した画像を自動的にプラットフォームにアップロードします。

リンク撮影後の画像を保存

この機能を有効にすると、接続したカメラで撮影した画像をデバイスに保存できます。**「次へ」**をクリックして設定を保存し、次のパラメータに進みます。または**「スキップ」**をクリックしてプライバシー設定をスキップします。

7.5.5 管理者設定

手順

1. ウェブページの右上にある「 」をクリックしてウィザードページに入ります。
2. 管理者の従業員IDと名前を入力します。
3. 追加する認証情報を選択します。

注記

少なくとも1つの認証情報を選択する必要があります。

1) **「顔を追加」**をクリックして、ローカルストレージから顔写真をアップロードします。

注意

アップロードする画像は200KB以内、JPG、JPEG、PNG形式である必要があります。

2) カード番号を入力し、カードの属性を選択するには**「カードを追加」**をクリックしてください。

注意

最大50枚のカードをサポートします。

3) 指紋を追加するには、**指紋追加**をクリックしてください。

注

最大10個の指紋が登録できます。

7.5.6 番号およびシステムネットワーク

手順

1. ウェブページの右上にある「 」をクリックしてウィザードページに入ります。前の設定後、**「次へ」**をクリックすると**「No. and Network System Network」**設定ページに入ります。

2. デバイスタイプを設定します。

注意

- デバイス種別を「**ドアステーション**」に設定した場合、**階数**、**ドアステーション番号**、**コミュニティ番号**、**建物番号**、**部屋番号**、**階数**、**ドア**ステーション番号を設定できます。
- デバイスタイプを「**屋外ドアステーション**」に設定した場合、**屋外ドアステーション番号**を設定できます。

コミュニティ番号

デバイスタイプ

このデバイスはドアステーションまたは外部ドアステーションとして使用できます。ドロップダウンリストからデバイスタイプを選択してください。

コミュニティ番号

デバイスのコミュニティ番号を設定してください

建物番号

デバイスの建物番号を設定してください。

ユニット番号

装置ユニット番号を設定

階

設置階を設定

ドアステーション番号

設置されたデバイスのドアステーション番号を設定

注記

メインドアステーション番号は0、サブドアステーション番号は1から16の範囲です。

外ドアステーション番号

設置済みデバイスの外部ドアステーション番号を設定

注記

番号の範囲は 1 から 99 です。

3. ビデオインターホンのネットワークパラメータを設定します。

登録パスワード

通信用メインステーションの登録パスワードを設定します。通信用メインステーションの登録パスワードを設定します。

メインステーションIP

通信に使用するメインステーションのIPアドレスを入力してください。

プライベートサーバーIP

SIPサーバーのIPを指します。通信に使用するメインステーションのIPアドレスを入力してください。この時、メインステーションはSIPサーバーとして使用されます。他のインターコム機器はこのサーバーアドレスに登録することで通信を実現します。

プロトコル1.0を有効化

有効にすると、ドアステーションは旧プロトコルバージョンでメインステーションに登録できます。無効にすると、ドアステーションは新プロトコルバージョンでメインステーションに登録できます。

4. 設定後、**[完了]**をクリックして設定を保存します。

7.6 ユーザー管理

「追加」をクリックし、基本情報、証明書、認証、設定を含む人物情報を追加します。

基本情報の追加

「人物管理」→「追加」をクリックして「人物追加」ページに入ります。
従業員ID、氏名、性別、人物タイプなどの基本情報を追加します。

人物タイプで**「訪問者」**を選択した場合、訪問時間を設定できます。
「カスタムタイプ」を選択した場合、名前を編集できます。変更した名前はデバイスに適用されます。**「人物の役割」**を選択します。

設定を保存するには**「保存」**をクリックします。

許可時間を設定する

「人物管理」→「追加」をクリックして「人物追加」ページに入ります。
長期有効ユーザーを有効にするか、または**長期有効ユーザー**を設定すると、担当者は設定された期間内でのみ権限を持つことができます。実際のニーズに応じて設定してください。
「出退勤確認のみ」を有効化できます。有効化後、この人物にはアクセス制御権限が付与されません。
ドアの権限を設定します。

設定を保存するには「**保存**」をクリックします。

デバイス番号を設定します。

「人物管理」→「人物追加」→「追加」をクリックし、「人物追加」ページに入ります。
階数と**部屋番号**のテキストボックスをクリックし、1から999までの数字を入力して階数と部屋番号を設定してください。

設定を保存するには「**保存**」をクリックしてください。

認証設定

「人物管理」→「追加」をクリックして「人物追加」ページに入ります。認証タイプを設定します。

設定を保存するには「**保存**」をクリックしてください。

カード追加

「人物管理」→「追加」をクリックして「人物追加」ページに入ります。
カード追加をクリックし、**カード番号**を入力して**物件**を選択し、**OK**をクリックしてカードを追加します。**保存**をクリックして設定を保存します。

顔写真を追加

「人物管理」→「追加」をクリックし、「人物追加」ページに入ります。**「+アップロード」**をクリックして、ローカルPCから顔写真をアップロードします。

注意
画像形式はJPG、JPEG、またはPNGとし、サイズは200KB未満である必要があります。

設定を保存するには「**保存**」をクリックします。

指紋を追加

注意
指紋機能をサポートしているデバイスのみが指紋を追加できます。

「人物管理」→「追加」をクリックして「人物追加」ページに入ります。
指紋を追加をクリックし、デバイスの指紋モジュールに指を押し当てて指紋を追加します。

設定を保存するには「**保存**」をクリックします。

掌紋を追加

注意

- 掌紋機能をサポートしているデバイスのみ掌紋を追加できます。
- 最大10000件の手のひら紋様および手のひら静脈を追加できます。

「人物管理」→「掌紋追加」をクリックし、「人物追加」ページに入ります。
デバイスの周辺モジュールから5～12cmの距離に掌を置きます。設定を保存するには**「保存」**をクリックします。

キーフォブを追加

「人物管理」→「追加」をクリックし、「人物追加」ページに入ります。
「+ キーフォブを追加」をクリックし、キーフォブのシリアル番号を入力するか、**「読み取り」**をクリックし、キーフォブの任意のボタンを押してキーフォブのシリアル番号を取得し、**「OK」**をクリックします。

注記

- 各ユーザーは最大1つのキーフォブを追加でき、端末は最大5,000個のキーフォブを追加できます。
- キーフォブを追加する前に、顔認証端末に対応する周辺機器モジュールを接続する必要があります。WEシリーズキーフォブを追加するにはWEシリーズ周辺機器モジュールを接続し、WBシリーズキーフォブを追加するにはWBシリーズ周辺機器モジュールを接続する必要があります。

PINを追加する

PINを設定する前に、そのPINがデバイス設定の個人用PINか、プラットフォーム適用型の個人用PINかを明確にする必要があります。 デバイス設定の個人用PINの場合、デバイスまたはウェブ上で作成・編集が可能であり、他のプラットフォームでは設定できません。プラットフォーム適用型の個人用PINの場合、プラットフォーム上で作成・編集が可能であり、デバイスで使用するには事前に発行する必要があります。デバイスやウェブ上では設定できません。
事前にPINモードを「**デバイス設定型個人PIN**」に設定済みであることを確認してください。ページ上の**「PINモード」**をクリックして設定画面へ移動します。
「人物管理」→「追加」をクリックし、「人物追加」ページに入ります。PINを設定します。または**「自動生成」**をクリックしてPINを自動生成します。**「追加」**をクリックして設定を保存します。

「保存して次へ」をクリックして設定を保存し、次の人の追加を続行します。

デバイス番号設定

「人物管理」→「追加」をクリックし、「人物追加」ページに入ります。
担当者の基本情報を追加します。デバイス番号モジュールに移動します。**追加**をクリックし、担当者が所属する部屋番号と階数を入力します。**追加**または**保存して続行**をクリックします。

人物削除

担当者管理ページで、削除が必要な担当者にチェックを入れ、**「削除」**をクリックします。**「すべてクリア」**をクリックすると、すべての担当者がクリアされます。

人物編集

人物管理ページで、編集が必要な人物を確認します。人物情報を編集するには、をクリックします。

フィルター

担当者管理ページで、従業員ID／氏名／カード番号を入力します。**資格ステータスを選択し**、「**Filter**」をクリックして担当者を絞り込みます。「**Reset**」をクリックするとすべての条件がクリアされます。

7.7 概要

デバイスのライブ映像、リンクされたデバイス、人物情報、ネットワーク状態、基本情報、デバイス容量を確認できます。

をクリックします。

機能説明：

ドア状態

動画画面の をクリックすると、デバイスのライブ映像を視聴できます。

ライブビュー開始時に音量を設定してください。

注意

双方向オーディオ開始時に音量を調整すると、音が繰り返し聞こえる場合があります。

ライブビュー開始時に画像をキャプチャできます。

/ / /

ドアの状態は開いている/閉じている/開いたまま/閉じたままです。

ライブビュー開始時に録画できます。

ライブビュー開始時にストリーミングタイプを選択します。メインストリーム、サブストリーム、サードストリームから選択可能です。

全画面表示。

制御状態

実際のニーズに応じて、ドアを開く、閉じる、開いたままにする、閉じたままにするといった制御が可能です。

リアルタイムイベント

イベントの従業員ID、名前、カード番号、イベントタイプ、時間、操作を確認できます。**「詳細を表示」**をクリックするとイベント検索ページに移動します。イベントタイプを選択し、従業員ID、名前、カード番号、開始時間、終了時間を入力して**「検索」**をクリックできます。結果は右パネルに表示されます。

リンクデバイス

リンク済みデバイスの数量とステータスを確認できます。

人物情報

追加済みおよび未追加の個人認証情報を確認できます。

ネットワーク状態

有線ネットワーク、無線ネットワーク、Hik-Connect、ISUP、OTAP、VoIPの接続状態および登録状態を確認できます。

基本情報

モデル、シリアル番号、ファームウェアバージョンを確認できます。

デバイス容量

人物、顔、指紋、カード、掌紋、キーフォブ、イベントの容量を確認できます。

注記

指紋または掌紋モジュールがインストールされているデバイスのみ、指紋または掌紋の容量を表示できます。

7.8 アクセス制御アプリケーション

7.8.1 アンチパスバック設定

デバイス間のアンチパスバック機能では、設定された経路に従い人員が順次認証を行う必要があります。サブデバイスのみがこの機能をサポートし、認証を伴う片方向通過のみがサポートされます。

手順

1. **アクセス制御 → アクセス制御アプリケーション → クロスデバイスアンチパスバック** をクリックします。
2. 機能を有効にします。
3. アクセスコントローラのパラメータを設定します。これには、**メインデバイスのIPアドレス**、**メインデバイスのポート番号**、**メインデバイスのパスワード**が含まれます。
4. 登録済みデバイスのコードを設定し、**登録ステータスを**確認できます。
5. **カードリーダー**を確認します。チェックされていないカードリーダーは、アンチパスバックのために相互接続できません。

7.8.2 マルチドア連動設定

同一アクセス制御装置の複数ドア間でマルチドア連動を設定します。いずれかのドアを開けるには、他のドアは閉じた状態を維持する必要があります。

手順

1. **アクセス制御 → アクセス制御アプリケーション → クロスデバイスマルチドア連動** をクリックします。
2. 機能を有効にします。
3. **デバイスタイプ**を選択
   - メインデバイスとして設定されたデバイス**にはポート番号**を設定し、「**追加**」をクリックしてアクセスポイントを追加します。「**サブデバイス管理**」をクリックすると、デバイス状態の確認やデバイスの削除が可能です。
   - サブデバイスとして設定されたデバイスには、**メインデバイスのIPアドレス**、**ポート番号**、**パスワード**を含むアクセス制御パラメータの設定が必要です。デバイス登録コードを設定すると、**登録ステータスを**確認できます。**カードリーダー**を確認してください。チェックされていないカードリーダーは、アンチパスバック機能で相互接続できません。
4. **アンチパスバックルールを**設定
   します。**認証ステータスによる**
   カードによる認証で判断されるアンチパスバックルーチン
   実際の通行状況による
   実際のカードによる開錠で判断されるアンチパスバックルーチン。
5. **OK**をクリックします。

7.9 アクセス制御管理

7.9.1 イベント検索

イベント検索をクリックして検索ページに入ります。
検索条件を入力してください。イベントタイプ、従業員ID、名前、カード番号、開始時間、終了時間を含め、**検索**をクリックしてください。
検索結果は右パネルに表示されます。

7.9.2 ドアパラメータ設定

ドアのロック解除に関するパラメータを設定します。

ドア番号を選択

関連パラメータを設定するドアを選択します。

アクセス制御 → パラメータ設定 → ドアパラメータをクリックして設定ページに入ります。

ドア番号を選択してください。通常、ドア1はデバイスに接続されたドア、ドア2はセキュアドア制御ユニットに接続されたドアです。
その他のドアパラメータを設定し、「**保存**」をクリックしてください。

デバイスのオンライン状態を表示

デバイスのステータスを表示および更新します。

アクセス制御 → パラメータ設定 → ドアパラメータをクリックして設定ページに入ります。デバイスのオンラインステータスを確認できます。**更新**をクリックすると、デバイスのステータスが更新されます。

ドア名を設定

ドア名を作成します。

アクセス制御 → パラメータ設定 → ドアパラメータをクリックして設定ページに入ります。**ドア名を**設定し、**保存**をクリックします。

PC Web経由で開錠時間設定

カードをかざした後にドアロックが開く時間を設定できます。

アクセス制御 → パラメータ設定 → ドアパラメータをクリックして設定ページに入ります。
開錠時間（ドアが解錠された後の動作時間）を設定します。設定時間内にドアが開かれない場合、ドアは自動的にロックされます。設定可能時間：1〜255秒。
保存をクリックしてください。

PC Web経由でのドア開放タイムアウトアラーム設定

ロック動作時間に達してもドアが閉じられない場合、アクセス制御ポイントが警報を鳴らします。

アクセス制御 → パラメータ設定 → ドアパラメータをクリックして設定ページに入ります。
ドア開放タイムアウトアラームを設定します。ロック動作時間に達してもドアが閉じられない場合、アクセス制御ポイントが警報を鳴らします。0に設定すると、警報は有効になりません。
保存をクリックします。

ドア閉時ロック設定

ドアが閉まったときにロックを設定できます。

アクセス制御 → パラメータ設定 → ドアパラメータをクリックして設定ページに入ります。「**ドア閉時ロック**」を有効にできます。

「保存」をクリックします。

PC Web経由でのドア磁気センサータイプの設定

配線方法に応じてドア接点タイプを選択できます。

アクセス制御 → パラメータ設定 → ドアパラメータをクリックして設定ページに入ります。磁気センサータイプを閉状態維持または開状態維持から選択します。デフォルトでは**閉状態維持**です（特別な要件を除く）。
保存をクリックします。

PC Web経由での退出ボタン設定

実際の配線方法に応じて、退出ボタンを常時開放または常時閉のどちらかに設定してください。

アクセス制御 → パラメータ設定 → ドアパラメータをクリックして設定ページに入ります。**退出ボタンタイプ**を設定します。デフォルトでは開放状態を維持（特別な必要性がない限り）です。

保存をクリックします。

PC Web経由でドアロックの電源オフ状態を設定

ドアロックの電源オフ時の状態を設定できます。

アクセス制御 → パラメータ設定 → ドアパラメータをクリックして設定ページに入ります。**ドアロック電源オフ状態**を設定します。デフォルトでは閉じたままです。

保存をクリックしてください。

PC Web経由で延長開放時間を設定

延長アクセス権を持つ人物がカードをスワイプした後、適切な遅延を経てドアコンタクトを有効化できます。

アクセス制御 → パラメータ設定 → ドアパラメータをクリックして設定ページに入ります。
延長開放時間を設定します。延長アクセス権を持つ人がカードをスワイプした後、適切な遅延を経てドアコンタクトが有効になります。
保存をクリックします。

PC Webで最初の利用者にドア開放継続時間を設定

最初の人が認証されると、複数人がドアへのアクセスやその他の認証操作を行えるようになります。

アクセス制御 → パラメータ設定 → ドアパラメータをクリックして設定ページに入ります。

最初の人が入室した際のドア開放時間を設定し、「**保存**」をクリックします。

PC Web経由での緊急コード設定

緊急コードを設定後、緊急事態発生時にはコードを入力してドアを開錠します。同時にアクセス制御システムは緊急事態を通知します。

アクセス制御 → パラメータ設定 → ドアパラメータをクリックして設定ページに入ります。緊急コードを設定し、**保存**をクリックします。

注記
緊急コードとスーパーパスワードは重複できません。通常4～8桁で構成されます。

PC Web経由でのスーパーパスワード設定

管理者または指定された人物は、スーパーパスワードを入力してドアを開けることができます。

アクセス制御 → パラメータ設定 → ドアパラメータをクリックして設定ページに入ります。**スーパーパスワード**を設定すると、指定された人物がスーパーパスワードを入力してドアを開けることができます。**保存**をクリックします。

注意
強制コードとスーパーパスワードは重複不可で、通常4～8桁で構成されます。

7.9.3 認証設定

PC Web経由でメインまたはサブカードリーダーを選択

端末を人物認証用に設定します。

アクセス制御 → パラメータ設定 → 認証設定をクリックして設定ページに入ります。端末をメインまたはサブカードリーダーとして選択します。

その他のパラメータを設定し、「**保存**」をクリックします。

PC Web経由で端末タイプとモデルを確認

端末のタイプとモデルを確認できます。

アクセス制御 → パラメータ設定 → 認証設定をクリックして設定ページに入ります。端末タイプと**端末モデル**を確認します。

PC Web経由で認証デバイスを有効化

有効化後、認証端末でカード読み取りが可能になります。

手順

1. **アクセス制御 → パラメータ設定 → 認証設定**をクリックして設定ページに入ります。
2. **認証デバイスを**有効にします。有効化後、端末は通常通りカード読み取りに使用できます。
3. **保存**をクリックします。

PC Web経由での認証設定

認証設定を行う。

アクセス制御 → パラメータ設定 → 認証設定をクリックして設定ページに入ります。

端末としてメインカードリーダーを選択する場合、ドロップダウンリストから認証方式を選択できます。複数の認証方式がある場合、**シングル認証タイムアウト**と**制御初期認証タイプ**を設定する必要があります。

シングル認証情報の認証タイムアウト

各認証の有効期間を設定できます。

注

パスワード認証のタイムアウトはデフォルトで20秒であり、上記の設定による制限を受けません。

制御初期認証タイプ

有効にすると、選択したすべてのタイプを初回認証に使用できます。

端末としてサブカードリーダーを選択する場合、ドロップダウンリストから「認証」を選択できます。

保存をクリックします。

PC Web 画面で顔認証を手動でトリガーする

「顔認証による手動認証のトリガー」を有効にした後、顔認識を行うにはデバイスの画面を手動でタッチする必要があります。

アクセス制御 → パラメータ設定 → 認証設定をクリックして設定ページに入ります。

メインカードリーダーを端末として選択したら、クリックして「**顔認証による手動認証のトリガー」を**有効にし、認証モードを選択してください。

シングル認識

前回の顔認証が完了した後、成功または失敗にかかわらず、画面をタップして次の認証を開始する必要があります。

連続

認証をトリガーした後、デバイスがスリープモードに入るまで顔認証を継続できます。

保存をクリックします。

PC Web による複数人認証を有効にする

有効にすると、複数人が同時に顔認証による本人確認を行えます。

アクセス制御 → パラメータ設定 → 認証設定をクリックして設定ページに入ります。

端末をメインカードリーダーとして選択し、**複数人認証を**有効にして「**保存**」をクリックします。

PC Web経由で認識間隔を設定

認証時に連続する2回の顔認識の間隔を設定します。

アクセス制御 → パラメータ設定 → 認証設定をクリックして設定ページに入ります。端末をメインまたはサブカードリーダーとして選択し、認識間隔を設定して**保存**をクリックします。

注記

1 から 10 までの数字を入力してください。

PC Web経由での認証間隔設定

認証時に同一人物の認証間隔を設定できます。設定された間隔内で同一人物は1回のみ認証可能です。2回目の認証は失敗します。設定間隔内に別の人物が認証した場合、再度認証が可能になります。

アクセス制御 → パラメータ設定 → 認証設定をクリックして設定ページに入ります。端末をメインカードリーダーとして選択し、**認証間隔**を設定して**保存**をクリックします。

PC Web経由での最大失敗試行回数アラームを有効化

設定値に達した際にカード読み取り試行回数のアラームを通知する機能を有効化します。

アクセス制御 → パラメータ設定 → 認証設定をクリックして設定ページに入ります。

端末をメインまたはサブカードリーダーとして選択した場合、**「最大認証失敗回数アラーム」を**スライドで有効にし、**「最大認証失敗回数」を**設定します。

保存をクリックしてください。

PC Web経由での掌紋認証タイムアウト閾値と認証間隔の設定

認証時の掌紋認識タイムアウト閾値と連続掌紋認識間隔を設定します。

アクセス制御 → パラメータ設定 → 認証設定をクリックして設定ページに入ります。

端末をメインまたはサブカードリーダーとして選択する場合、**掌紋認識タイムアウトしきい値**と**掌紋認識間隔**を設定し、「**保存**」をクリックします。

PC Web 経由で改ざん検知を有効/無効にする

改ざん検知を有効にすると、カードリーダーが取り外されたり持ち去られたりした場合に、デバイスが自動的に改ざんイベントを生成します。

アクセス制御 → パラメータ設定 → 認証設定をクリックして設定ページに入ります。

実際のニーズに応じて**改ざん検知**を有効または無効に設定します。機能を有効にした場合、カードリーダーが取り外されたり持ち去られたりすると、デバイスは自動的に改ざんイベントを生成します。機能を無効にした場合、アラームイベントは生成されません。

[保存]をクリックします。

PC Web経由でのカード番号反転の有効化/無効化

カード番号反転機能を有効または無効にできます。

アクセス制御 → パラメータ設定 → 認証設定をクリックして設定ページに入ります。**カード番号反転を**有効にすると、読み取ったカード番号が逆順になります。

保存をクリックします。

サブカードリーダーの位置設定

サブカードリーダーの位置を選択できます。

アクセス制御 → パラメータ設定 → 認証設定をクリックして設定ページに入ります。

サブカードリーダーを端末として選択した場合、サブカードリーダーの位置を「**メインカードリーダーと反対側**」または「**メインカードリーダーと同じ側**」から選択できます。**［保存］をクリックしてください。**

PC Web経由でコントローラとの通信を毎回設定

各サブカードリーダーのコントローラーとの通信間隔を設定できます。設定時間内にカードリーダーがアクセスコントローラーに接続できない場合、カードリーダーはオフライン状態となります。

アクセス制御 → パラメータ設定 → 認証設定 の順にクリックして設定ページに入ります。

端末をサブカードリーダーとして選択したら、「**コントローラーとの通信間隔**」を設定し、「**保存**」をクリックします。

Webクライアント経由のパスワード入力タイムアウト期間の設定

パスワードの2文字入力の最大間隔を設定します。1文字入力後、設定された間隔内に次の文字が入力されない場合、入力された文字はすべて自動的にクリアされます。

アクセス制御 → パラメータ設定 → 認証設定をクリックして設定ページに入ります。
サブカードリーダーを端末として選択した場合、**パスワード入力時の最大間隔**を設定し、**[保存]をクリックできます**。

PC Web経由でOK LED極性とエラーLED極性を設定

OK および ERR インターフェースのダイオードの極性を、実際の配線に応じて選択します（デフォルトは正極性）。

アクセス制御 → パラメータ設定 → 認証設定をクリックして設定ページに入ります。
端末をサブカードリーダーとして選択したら、**OK LED**極性と**エラーLED極性を**設定し、**保存**をクリックしてください。

7.9.4 認証連携設定

認証連携設定を設定できます。

手順

1. **アクセス制御 → パラメータ設定 → 認証設定**をクリックして設定ページに入ります。
2. 連携機能を設定します。

   認証時呼び出し連携

   これを有効にすると、認証に合格した人物がボタン設定の呼び出し先を自動的に呼び出し、遠隔でドアを開けることができます。

   認証失敗時の連動設定

   有効化後、認証失敗回数が設定数に達した場合、自動的にボタン設定の呼び出し先を呼び出し、遠隔でドアを開錠します。
3. **保存**をクリックしてください。

7.9.5 認証プランの設定

認証プランを設定できます。

アクセス制御 → パラメータ設定 → 認証設定をクリックして設定ページに入ります。

認証タイプを選択し、タイムバーで期間をドラッグします。**保存**をクリックします。

7.9.6 顔認証パラメータの設定

Webブラウザ経由での顔認証アンチスプーフィングの有効化/無効化

有効にすると、デバイスは人物が生体かどうかを認識できます。

アクセス制御 → パラメータ設定 → スマートをクリックして設定ページに入ります。**顔偽装防止を**有効にし、**保存**をクリックします。
生体顔検出機能を有効または無効にします。有効にすると、デバイスは人物が生体かどうかを認識できます。生体でない場合、認証は失敗します。

顔重複チェックの有効化/無効化

顔重複チェックを有効化し、人物の顔を追加するたびに、システムは顔の重複をチェックします。重複した顔が検出された場合、プロンプトが表示されます。

注意
リモートでの顔追加や一括顔適用時には本機能はサポートされません。

アクセス制御 → パラメータ設定 → スマートをクリックして設定ページに入ります。**顔重複チェックを**有効にします。

保存をクリックします。

PC Web 経由で偽装検知レベルを設定

顔偽装防止機能を有効にした後、生体認証時の照合セキュリティレベルを設定できます。

アクセス制御 → パラメータ設定 → スマートをクリックして設定ページに入ります。偽装防止検出レベルを選択し、**保存**をクリックします。
一般、高度、専門から選択可能です。レベルが高いほど偽認識率は低くなりますが、拒否率が高くなります。

PC Web経由での認識距離設定

認証ユーザーとデバイスカメラ間の距離を設定できます。**アクセス制御 → パラメータ設定 → スマート**をクリックして設定ページに入ります。

認識距離を選択し、**保存**をクリックします。

PC Web経由でのピッチ角設定

顔認識および認証時にレンズのピッチ角度を設定できます。**アクセス制御 → パラメータ設定 → スマート**をクリックして設定ページに入ります。

注意
モデルによってサポートされるパラメータが異なる場合があります。実際のページを参照してください。

ピッチ角度を設定し、**保存**をクリックします。

PC Web経由でヨー角を設定

顔認識および認証中にレンズのヨー角を設定できます。**アクセス制御 → パラメータ設定 → スマート**をクリックして設定ページに入ります。

注意
モデルによってサポートされるパラメータが異なる場合があります。実際のページを参照してください。

ヨー角を設定し、「**保存**」をクリックしてください。

PC Web経由での適用用顔画像品質グレードを設定

顔認証のグレードは、成功するにはしきい値よりも高くなければなりません。**アクセス制御 → パラメータ設定 → スマート**をクリックして設定ページに入ります。

注意
モデルによってサポートされるパラメータが異なる場合がありますので、実際のページをご参照ください。

適用する顔画像品質グレードを設定します。顔認証のグレードは、成功するにはしきい値よりも高くなければなりません。
保存をクリックします。

PCウェブ経由で1:1フェイスグレード閾値を設定

1:1顔評価閾値を設定します。

アクセス制御 → パラメータ設定 → スマート に移動します。

1:1顔画像グレード閾値を設定し、**保存**をクリックします。

閾値が高いほど、フロントカメラで撮影される画像の品質に対する要求が高くなり、認証失敗が発生しやすくなります。

PC Web 経由で 1:1 顔照合のしきい値を設定

顔1:1照合閾値を設定します。

アクセス制御 → パラメータ設定 → スマートをクリックして設定ページに入ります。顔1:1照合閾値を設定し、**保存**をクリックします。
しきい値の値が大きいほど、顔認証時の誤認率は低くなり、誤拒否率は高くなります。最大値は100です。

PC Web経由での1対N照合しきい値の設定

顔認証の1対Nマッチング閾値を設定できます。

アクセス制御 → パラメータ設定 → スマートをクリックして設定ページに入ります。1:Nマッチングのしきい値を設定し、**保存**をクリックします。
値が大きいほど誤認率が低くなり、誤拒否率が大きくなります。最大値は100です。

ウェブブラウザで顔認識領域を設定する

顔認識および認証時のレンズの認識領域を設定できます。

アクセス制御 → パラメータ設定 → エリア設定をクリックして設定ページに入ります。
プレビュー画面の黄色いボックスをドラッグして、顔認識の有効領域を左右上下に調整します。
またはブロックをドラッグするか数値を入力して有効領域を設定します。「**保存**」をクリックします。

または をクリックしてキャプチャするか、全画面表示に切り替えてください。

PC Web経由での指紋パラメータ設定

デバイスの指紋認証パラメータを設定できます。

アクセス制御 → パラメータ設定 → スマートをクリックして設定ページに入ります。
指紋セキュリティレベルを選択します。レベルが高いほど、偽認識率は低くなり、拒否率は高くなります。
保存をクリックします。

PC Web経由での掌紋認証パラメータ設定

デバイスの掌紋パラメータを設定できます。

アクセス制御 → パラメータ設定 → スマートをクリックして設定ページに入ります。

掌紋偽装検知を有効にします。**掌紋1:1閾値**と**掌紋1:N閾値**を設定します。

注記
値が大きいほど誤認率は低くなりますが、誤拒否率は高くなります。最大値は100です。

保存をクリックします。

PC Web経由でECOモードを有効/無効にする

ECOモードが有効な場合、IRカメラを使用して低照度または暗い環境で顔認証が可能です。

アクセス制御 → パラメータ設定 → スマートをクリックして設定ページに入ります。

ECOモードを有効にすると、IRカメラを使用して低照度または暗所環境での顔認証が可能です。ECOモード（1:N）とECOモード（1:1）を設定できます。

マスク着用顔検出を有効にしている場合、マスク検出パラメータも設定できます。

ECOモード（1:1）のしきい値

ECOモード1:1マッチングモードによる認証時の一致閾値を設定します。値が大きいほど誤認率は低くなりますが、誤拒否率は高くなります。最大値は100です。

ECOモード（1:N）しきい値

ECOモード1:Nマッチングモードによる認証時のマッチングしきい値を設定します。値が大きいほど誤認率が低下し、誤拒率が上昇します。最大値は100です。

マスク着用時の顔認証 1:1 マッチングしきい値 (ECO)

ECOモード1:1マッチングモードでマスク着用時の認証を行う際のマッチングしきい値を設定します。値が大きいほど誤認率が低くなり、誤拒否率が大きくなります。最大値は100です。

マスク着用時の顔認証 1:N マッチングしきい値 (ECO)

ECOモードの1:Nマッチングモードでマスク着用時の認証を行う際のマッチング閾値を設定します。値が大きいほど誤認率は低くなりますが、誤拒否率は高くなります。最大値は100です。

保存をクリック。

PC Web経由でのマスク着用顔検出の有効化/無効化

マスク着用時の顔検出を有効にすると、システムは撮影された顔にマスクが着用されているかどうかを認識します。

アクセス制御 → パラメータ設定 → スマートをクリックして設定ページに入ります。

マスク着用顔検出を有効にした後、以下の設定が可能です：**マスクなし顔戦略**、**マスク着用顔&顔（1:1）**、**マスク着用顔 1:N マッチング閾値（ECO）**、**マスク着用顔 1:1 マッチング閾値**、**マスク着用顔 1:N マッチング閾値（ECO）**。

マスクなし顔戦略

「**なし**」、「**マスク着用リマインダー**」、「**マスク着用必須**」から選択できます。**マスク着用リマインダー**

認証時にマスクを着用していない場合、デバイスがポップアップ表示し、ドアが開きます。

マスク着用必須

認証時にマスクを着用していない場合、端末が警告を表示し、ドアは閉じたままとなります。

マスク着用時の顔認証&顔認証（1:1）

マスク着用時の顔認証において、1:1照合モードで一致判定値を設定します。値が大きいほど誤認率は低くなりますが、誤拒否率は高くなります。最大値は100です。

マスク着用時の顔認証&顔認証（1:N）

マスク着用時の顔認証において、1:N照合モードで設定する照合閾値です。値が大きいほど誤認率は低くなりますが、誤拒否率は高くなります。最大値は100です。

マスク着用顔 1:1 マッチングしきい値 (ECO)

ECOモード1:1照合モードでマスク着用時の顔認証を行う際の一致判定値を設定します。閾値が大きいほど、顔認証時の誤認識率が低下し、拒否率が上昇します。最大値は100です。

マスク着用時の顔認証 1:N マッチングしきい値 (ECO)

ECOモードの1:Nマッチングモードでマスク着用時の顔認証を行う際の一致判定値を設定します。しきい値が大きいほど、顔認証時の誤認識率が低下し、拒否率が上昇します。最大値は100です。

保存をクリックします。

PC Web経由でのヘルメット検出の有効化/無効化

ヘルメット検知を有効にすると、顔認証時に安全帽の着用状態をシステムが認識します。

アクセス制御 → パラメータ設定 → スマートをクリックして設定ページに入ります。**ヘルメット検知を**有効にし、**保存**をクリックします。

ヘルメット検知を有効にする

リマインダー戦略を設定できます。

着用リマインダー

認証時にヘルメットを着用していない場合、デバイスが警告を表示し、ドアが開きます。

着用必須

認証時にヘルメットを着用していない場合、装置は警告を表示し、ドアは閉じたままになります。

アルコール検知設定

アルコール検知パラメータを設定できます。

アクセス制御 → パラメータ設定 → スマートをクリックして設定ページに入ります。アルコール検知パラメータを設定し、**保存**をクリックします。

アルコール検知

アルコール検知を有効にすると、アルコール検知機能が最優先されます。QRコード認証と多要素認証は無効になります。「アルコール検知のみ」と「複数人認証」が有効な場合も、これらの機能は無効になります。

アルコール検知のみ

有効化後、本デバイスはアルコール検知機能のみをサポートし、その他の権限機能は無効となります。

アルコール濃度単位

濃度の単位は、mg/100 ml または mg/L から選択できます。

アルコール濃度換算係数設定

血中アルコール濃度（BAC）と呼気アルコール濃度（BrAC）の換算については、BAC（mg/L）= BrAC（mg/L）*k となります。ここで、k は換算係数です。

飲酒状態閾値／酩酊状態閾値

飲酒状態および酩酊状態の閾値濃度を設定でき、濃度が高ければ「飲酒」または「酩酊」と判断されます。

検出感度

検出感度は設定可能で、感度が高いほど検出結果の精度が高くなります。

吹込時間

アルコール検知の吹込時間を設定します。

アルコール超過時ドア開放禁止/ドア開放禁止設定

アルコール超過時ドアロックを有効にすると、検出時にアルコールが基準値を超えた場合、ドアは開かなくなります。**ドアロック設定は飲酒**時または**酔っ払い時に**設定できます。

7.9.7 キーフォブ設定

キーフォブのパラメータを設定できます。

手順

1. **アクセス制御 → キーフォブ設定** をクリックします。
2. **認識距離**を選択します。
3. **ドアを開けるには、プレスボタンを**押してください。
4. **保存**をクリック。

7.9.8 カード設定

PC Web 経由で NFC 保護を有効/無効にする

有効化後、デバイスは NFC カードを読み取ることができます。

アクセス制御 → パラメータ設定 → カード設定をクリックして設定ページに入ります。

NFC カードを有効にするをクリックし、**保存**をクリックします。有効化後、デバイスは NFC カードを読み取ることができます。アクセス制御デバイスのデータがモバイルデバイスによって取得された場合、認証されていないアクセスが発生する可能性があります。この状況を防ぐために、NFC 機能を無効にすることができます。

Webクライアント経由でのM1カード有効化/無効化

有効化後、デバイスはM1カードを認識し、ユーザーはデバイス経由でM1カードをスワイプできます。**アクセス制御 → パラメータ設定 → カード設定**をクリックして設定ページに入ります。

M1カードを有効にするをクリックします。

M1カード暗号化

M1カード暗号化を有効にすると、入館カードのセキュリティレベルが向上します。これにより、入館カードの複製が困難になります。

セクター

M1 カード暗号化を有効にした後、暗号化セクターを設定する必要があります。

注意
セクター13を暗号化することをお勧めします。

保存をクリックしてください。

Webクライアント経由でのEMカードの有効化/無効化

有効化後、デバイスはEMカードを認識し、ユーザーはデバイスでEMカードをスワイプできます。**アクセス制御 → パラメータ設定 → カード設定**をクリックして設定ページに入ります。

「**EMカードを有効にする**」をクリックし、「**保存**」をクリックします。

注意

- EMカードを読み取れる周辺機器のカードリーダーが接続されている場合、この機能を有効にすると、そのカードリーダーでもEMカードをスワイプできます。
- デュアル周波数カードモジュールが接続されている場合、EMカードとDESfireカードを同時にスワイプできます。ただし、デバイス上でのカードスワイプは無効です。

WebクライアントによるCPUカードの有効化/無効化

有効化後、デバイスはCPUカードを認識可能となり、ユーザーはデバイス経由でCPUカードをスワイプできます。**アクセス制御 → パラメータ設定 → カード設定**をクリックして設定ページに入ります。

クリックして「**CPUカードを読み取る」を有効化**。

CPUカード読み取り内容を有効にするをクリックします。有効化後、デバイスはCPUカードから内容を読み取れます。

「**保存**」をクリックします。

DESFireカードの設定

DESFireカードとDESFireカード内容読み取りを有効化できます。

パラメータ設定 → カード設定をクリックして設定ページに入ります。**DESFire** カードと **DESFire カード**の内容読み取りを**有効にする**を選択し、**保存**をクリックします。

注意

デュアル周波数カードモジュールが接続されている場合、EMカードとDESfireカードを同時にスワイプできます。ただし、デバイス上でカードをスワイプすることは無効です。

FeliCaカードの設定

FeliCaカードを有効にできます。

パラメータ設定 → カード設定をクリックして設定ページに入ります。

FeliCaカード有効化を選択します。

Web経由でのカード番号認証パラメータ設定

端末上でカード認証を行う際のカード読み取り内容を設定します。**アクセス制御 → パラメータ設定 → カード設定** に移動します。

カード認証モードを選択し、「**保存**」をクリックします。

カード番号全体

すべてのカード番号が読み取られます。

3 バイト

デバイスは3バイトを読み取ることでカードを読み込みます。

4 バイト

デバイスは4バイトでカードを読み取ります。

7.9.9 リモート認証の設定

デバイスは、本人の認証情報をプラットフォームにアップロードします。プラットフォームは、ドアを開けるかどうかを判断します。

アクセス制御 → パラメータ設定 → 端末パラメータ に移動します。パラメータ設定後、**保存をクリックします**。

リモート認証

リモート認証を有効にした後、認証時にデバイスは認証情報をプラットフォームにアップロードし、プラットフォームがドアを開けるかどうかを確認します。

人物タイプの遠隔認証

「リモートでの人物タイプ検証」を選択します。

ローカルで認証情報を確認

機能を有効化後、デバイスは権限を確認しますが、プランテンプレートの見積もりは行いません。

リモート検証のタイムアウト期間

リモート検証のタイムアウト期間を設定します。

オフラインリモート検証によるロック解除

オフラインリモート検証によるロック解除を有効にできます。

結果返却モード

結果の返送モードを設定します。

7.9.10 プライバシー設定

PC Webブラウザ経由でのイベント保存タイプ設定

イベント保存タイプを設定できます。

アクセス制御 → パラメータ設定 → プライバシー設定をクリックして設定ページに入ります。

イベント保存タイプは「**古いイベントを定期的に削除**」「**指定時間経過で古いイベントを削除**」「**上書き**」から選択できます。

古いイベントを定期的に削除

ブロックをドラッグするか数値を入力し、イベント削除の期間を設定します。設定された期間に基づき全イベントが削除されます。

指定時間による古いイベント削除

時間を設定すると、設定した時刻にすべてのイベントが削除されます。

上書き

システムが保存済みイベントが全容量の95%を超えたことを検知すると、最も古い5%のイベントが削除されます。

保存をクリックしてください。

PC Web 経由で認証結果を設定

写真、氏名、社員 ID、体温などの認証結果の内容を設定します。**アクセス制御 → アクセス制御 → パラメータ設定 → プライバシー設定** をクリックします。

認証結果に表示される内容（写真、名前、社員IDなど）を確認します。

実際のニーズに応じて、**氏名非識別化**、**ID非識別化**、**体温**、**アルコール濃度**を確認してください。非識別化後、氏名とIDには内容の一部が表示されます。

認証結果表示時間を設定すると、認証結果は設定した時間だけ表示されます。

保存をクリックします。

PC Web経由での画像アップロードと保存を設定

画像アップロードと保存のパラメータを設定できます。

アクセス制御 → パラメータ設定 → プライバシー設定をクリックして設定ページに入ります。

認証時に画像を保存

認証時に画像を自動的に保存する。

認証時に画像をアップロード

プラットフォームへの認証時に画像を自動的にアップロードする。

写真モード

デフォルトとして選択すると、デバイスはパノラマビューを撮影します。最大画像サイズと画像解像度を設定できます。

マット用画像モードとして選択した場合、デバイスは顔のみを撮影します。最大画像サイズを設定できます。

登録済み画像の保存

本機能を有効にすると、登録された顔写真がシステムに保存されます。

リンクしたカメラで撮影した画像を保存

この機能を有効にすると、リンクされたカメラで撮影した画像をデバイスに保存できます。

リンク撮影後の画像アップロード

リンクされたカメラで撮影した画像を自動的にプラットフォームにアップロードします

通話中のキャプチャ画像アップロード

有効にすると、通話中に自動的に画像が撮影され、自動的にアップロードされます。

登録された掌紋画像を保存

これを無効にすると、手のひらのデータのみが保存され、登録された画像は保存されません。

保存をクリックしてください。

PC Web経由でデバイスの画像を消去

登録済み、認証済み、またはキャプチャされた顔写真や画像をすべて消去できます。

アクセス制御 → パラメータ設定 → プライバシー設定をクリックして設定ページに入ります。**クリア**をクリックすると、登録済み、認証済み、キャプチャされた顔写真、または掌紋写真をすべてクリアします。

PC Web 経由で PIN モードを設定する

設定前に、PINがプラットフォーム適用型個人PINかデバイス設定型個人PINかを確認してください。デバイス設定型個人PINの場合、デバイスまたはPC Web上でPINを編集できますが、プラットフォームでは設定できません。プラットフォーム適用型個人PINの場合、デバイスやPC Webではなくプラットフォーム上でPINを設定する必要があります。

アクセス制御 → パラメータ設定 → プライバシー設定 に移動します。

PINモードモジュールでは、以下のパラメータを設定できます。パラメータ設定後、「**保存**」をクリックしてください。

プラットフォーム適用個人用PIN

プラットフォーム上で個人用PINを作成できます。PINはデバイスに適用する必要があります。デバイスやPC Web上ではPINの作成や編集はできません。

デバイス設定個人用PIN

デバイスまたはPC Web上でPINを作成または編集できます。プラットフォーム上ではPINを設定できません。

保存をクリックしてください。

7.9.11 通話設定

Web経由でのデバイス番号設定

本装置はドアステーションまたは外部ドアステーションとして使用できます。使用前にデバイス番号を設定してください。

ビデオインターホン → 通話設定 → デバイス番号 をクリックします。

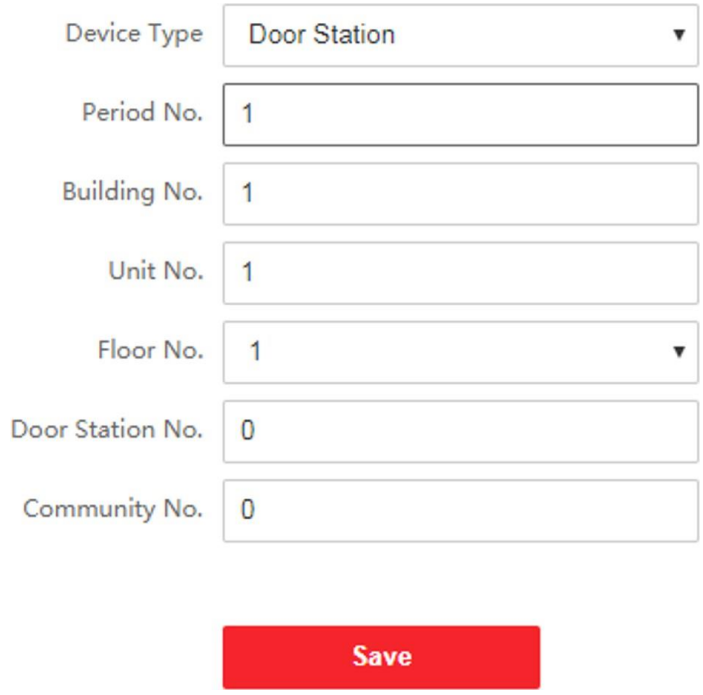


図 7-1 デバイス番号の設定

デバイスタイプを**ドアステーションに**設定した場合、**階数、ドアステーション番号、コミュニティ番号、建物番号、部屋番号**を設定できます。

デバイス種別

本デバイスはドアステーションまたは外部ドアステーションとして使用できます。ドロップダウンリストからデバイス種別を選択してください。

注意

デバイスタイプを変更した場合は、デバイスを再起動してください。

階数

設置階を設定してください。

ドアステーション番号

設置されたデバイスの階数を設定します。

注記

- 番号を変更した場合は、デバイスを再起動してください。
- メインドアステーション番号は0、サブドアステーション番号は1から16の範囲です。

コミュニティ番号

デバイスのコミュニティ番号を設定します。

建物番号

デバイスの建物番号を設定します。

ユニット番号

デバイスのユニット番号を設定

注記

番号を変更した場合は、デバイスを再起動する必要があります。

設定後、**保存**をクリックして設定を保存してください。

デバイスタイプを「**外ドアステーション**」に設定した場合、外ドアステーション番号とコミュニティ番号を設定できます。

外部ドアステーション番号

デバイスタイプとして外部ドアステーションを選択した場合、**1** から 99 の間の番号を入力する必要があります。

99 の間の数字を入力してください。

注記

番号を変更した場合は、デバイスを再起動してください。

コミュニティ番号

デバイスのコミュニティ番号を設定します。

Web ブラウザによるビデオインターホンネットワークパラメータの設定

登録パスワード、メインステーションIP、プライベートサーバーIPを設定でき、実際のニーズに応じてプロトコル1.0を有効にできます。

ビデオインターホン → 呼び出し設定 → ビデオインターホンネットワークをクリックして設定ページに入ります。

登録パスワード

通信用メインステーションの登録パスワードを設定します。通信用メインステーションの登録パスワードを設定します。

メインステーションIP

通信に使用する主機のIPアドレスを入力します。

プライベートサーバーIP

SIPサーバーのIPを指します。通信に使用するメインステーションのIPアドレスを入力してください。この時、メインステーションはSIPサーバーとして使用されます。他のインターコム機器はこのサーバーアドレスに登録することで通信を実現します。

プロトコル1.0を有効にする

有効にすると、ドアステーションは旧プロトコルバージョンでメインステーションに登録できます。無効にすると、ドアステーションは新プロトコルバージョンでメインステーションに登録できます。

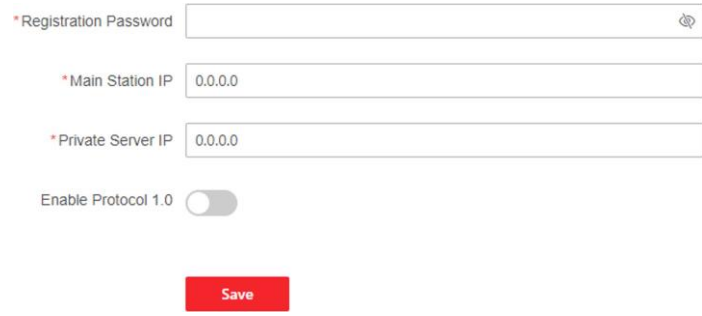


図7-2 ビデオインターコムネットワーク

設定後、アクセス制御デバイスとビデオインターコムのドアステーション、室内機、メインステーション、プラットフォームなどとの間で通信が可能になります。

保存をクリックします。

PC Web 経由で通信時間を設定

最大通信時間を設定します。

ビデオインターホン → 通話設定 → 通話設定 に移動します。

最大通信時間を入力してください。**自動応答**と**外部スピーカーによる応答を**有効にできます。

注意

- 最大通信時間の設定範囲は90秒から120秒です。
- 通話中に外部スピーカーから音声が再生されると、エコーが発生する場合があります。

保存をクリックしてください。

PC Web から通話するにはボタンを押す

手順

1. **アクセス制御 → 通話設定 → ボタンを押して通話**を選択し、設定ページに入ります。

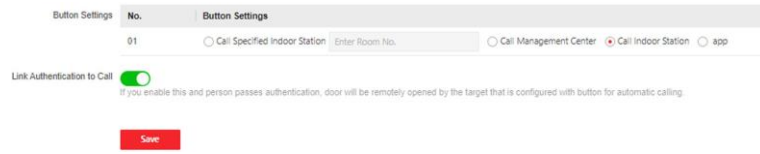


図7-3 ボタンを押して発信

2. 必要に応じて「**指定室内機への通話**」「**管理センターへの通話**」「**室内機への通話**」または「**APPへの通話**」を選択してください。

注記

「**指定室内機を呼び出す**」を選択した場合、室内機の**部屋番号**を入力する必要があります。

---

3. 必要に応じて**リンク認証を有効にしてください**。有効化後、認証を通過した人物が対象のドアに近づくと、自動呼び出しボタンが設定された端末によってドアが遠隔で開錠されます。
4. **保存**をクリックしてください。

通話優先度

呼び出しの優先度を設定できます。

手順

1. **ビデオインターホン → 呼び出し設定 → 呼び出し優先度**をクリックして設定ページに入ります。
2. **通話タイプを確認し**、3つの優先度ごとに**呼び出し音の鳴動時間を**設定します。
3. 設定を有効にするには「**保存**」をクリックします。

注意

レベルが高いほど、呼び出し対象のデバイスは容易になります。呼び出し時間が終了すると、次のレベルの呼び出しがトリガーされます。

PC Web経由での番号設定

部屋のSIP番号を設定します。各部屋はSIP番号を介して相互通信が可能です。

手順

1. **アクセス制御 → 呼び出し設定 → 番号設定** に移動します。

図7-4 番号設定

2. 「**追加**」をクリックし、**ルーム**番号と**SIP1**電話番号を入力します。
3. **オプション：**SIP番号を追加するには「**Add**」をクリック、番号を削除するには「🗑」をクリックしてください。
4. **[保存]**をクリックします。
5. **オプション：[削除]** をクリックすると、部屋番号とその SIP 番号を削除できます。

7.10 デバイス管理

デバイス番号、タイプ、IP、シリアル番号、モデル、バージョン、フロア番号、部屋番号、番号、武装状態、ユーザー名、ネットワーク状態、操作を確認できます。また、デバイス管理ページで屋内ステーションやサブドアステーションを追加したり、デバイスの管理、アップグレード、削除を行うこともできます。

手順

1. 「**デバイス管理**」をクリックします。
2. 「**追加**」をクリックします。
3. **デバイスタイプ**を選択し、**デバイスパスワード**、**登録パスワード**、**シリアル番号**、**IPアドレス**、**IPv4サブネットマスク**、**IPv4デフォルトゲートウェイ**、**ポート**、**階数**を入力してください（屋内ステーションの場合は**階数**と**番号の**入力は不要です）。
4. **保存**をクリックします。
5. **オプション：**以下の操作も実行できます。

デバイスの削除　削除するデバイスを選択し、「**削除**」をクリックします。

デバイスのインポート　デバイス情報を含むUSBフラッシュドライブをデバイスに接続し、**インポート**をクリックしてデバイス情報をインポートします。

デバイスのエクスポート　**エクスポート**をクリックすると、デバイス情報ファイルがUSBフラッシュドライブにエクスポートされます。

7.11 システム構成

7.11.1 PC Web経由でのデバイス情報表示

デバイス名、デバイス番号、言語、モデル、シリアル番号、バージョン、チャンネル数、IO入力、IO出力、ロック、ローカルRS-485番号、レジスタ番号、アラーム入力、アラーム出力、デバイス容量などを表示します。

システムとメンテナンス → システム構成 → システム → システム設定 → 基本情報 をクリックして設定ページに入ります。

デバイス名、デバイス番号、言語、モデル、シリアル番号、バージョン、チャンネル数、IO入力、IO出力、ロック、ローカルRS-485番号、レジスタ番号、アラーム入力、アラーム出力、デバイス容量などを表示できます。

ファームウェアバージョンの「**アップグレード**」をクリックすると、アップグレードページに移動してデバイスをアップグレードできます。

7.11.2 時刻設定

デバイスのタイムゾーン、同期モード、サーバーアドレス、NTP ポート、および間隔を設定します。

システムとメンテナンス → システム構成 → システム → システム設定 → 時刻設定 をクリックします。

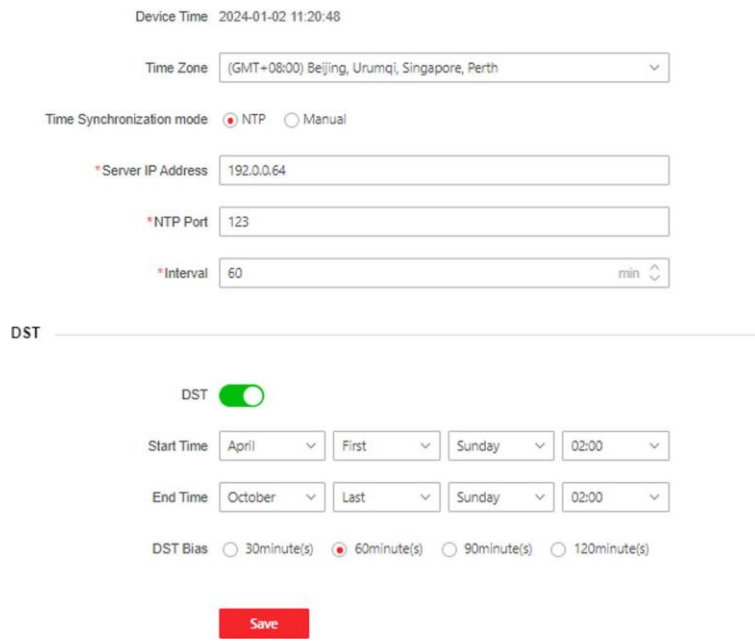


図 7-5 時刻設定

設定後、「**保存**」をクリックして設定を保存します。

タイムゾーン

ドロップダウンリストから、デバイスが所在するタイムゾーンを選択します。

時刻同期

NTP

NTPサーバーのIPアドレス、ポート番号、および間隔を設定する必要があります。

手動

デフォルトでは、デバイスの時刻は手動で同期する必要があります。デバイスの時刻を手動で設定するか、**「コンピュータ時刻と同期」を**チェックしてデバイスの時刻をコンピュータの時刻と同期させることができます。

サーバーアドレスタイプ/サーバーアドレス/NTPポート/間隔

サーバーアドレスタイプ、サーバーアドレス、NTP ポート、および間隔を設定できます。

7.11.3 管理者のパスワードを変更する

手順

1. **システムとメンテナンス → システム構成 → システム → ユーザー管理 → ユーザー管理** をクリックします。
2. をクリックします。
3. 古いパスワードを入力し、新しいパスワードを作成してください。
4. 新しいパスワードを確認してください。
5. **保存**をクリックしてください。

注意

デバイスのパスワード強度を自動的に確認できます。製品のセキュリティを強化するため、ご自身で選択したパスワード（大文字、小文字、数字、特殊文字の少なくとも3種類を含む8文字以上）に変更することを強く推奨します。また、特に高セキュリティシステムでは、パスワードを定期的に変更することを推奨します。月次または週次での変更により、製品をより効果的に保護できます。
すべてのパスワードおよびその他のセキュリティ設定の適切な構成は、設置者および／またはエンドユーザーの責任です。

7.11.4 PC Web経由のアカウントセキュリティ設定

セキュリティの質問と回答、またはデバイスのメールアドレスを変更できます。設定変更後、デバイスパスワードを忘れた場合は、新しい質問に回答するか、新しいメールアドレスを使用してデバイスパスワードをリセットする必要があります。

手順

1. **システムとメンテナンス → システム構成 → システム → ユーザー管理 → ユーザー管理 → アカウントセキュリティ設定** をクリックします。
2. 実際のニーズに応じてセキュリティ質問またはメールアドレスを変更してください。
3. デバイスのパスワードを入力し、変更を確認するために「**OK**」をクリックしてください。

7.11.5 PC Web経由でデバイスの武装/解除情報を表示

デバイスの武装タイプと武装IPアドレスを表示します。

システムとメンテナンス → システム構成 → システム → ユーザー管理 → 警備/解除情報 に移動します。
デバイスの武装/解除情報を表示できます。ページを更新するには「**更新**」をクリックしてください。

7.11.6 PC Web経由で動作モードを設定

デバイスの端末パラメータを設定できます。

注記
一部のモデルのみが本機能をサポートしています。具体的なデバイスをご確認ください。

アクセス制御 → パラメータ設定 → 端末パラメータをクリックして設定ページに入ります。
動作モード
動作モードは、アクセス制御モードまたは許可不要モードに設定できます。
アクセス制御モード
アクセス制御モードはデバイスの通常モードです。アクセスには認証情報の認証が必要です。

7.11.7 ネットワーク設定

PC Web経由で基本ネットワークパラメータを設定

システムとメンテナンス → システム構成 → ネットワーク → ネットワーク設定 → TCP/IP をクリックします。

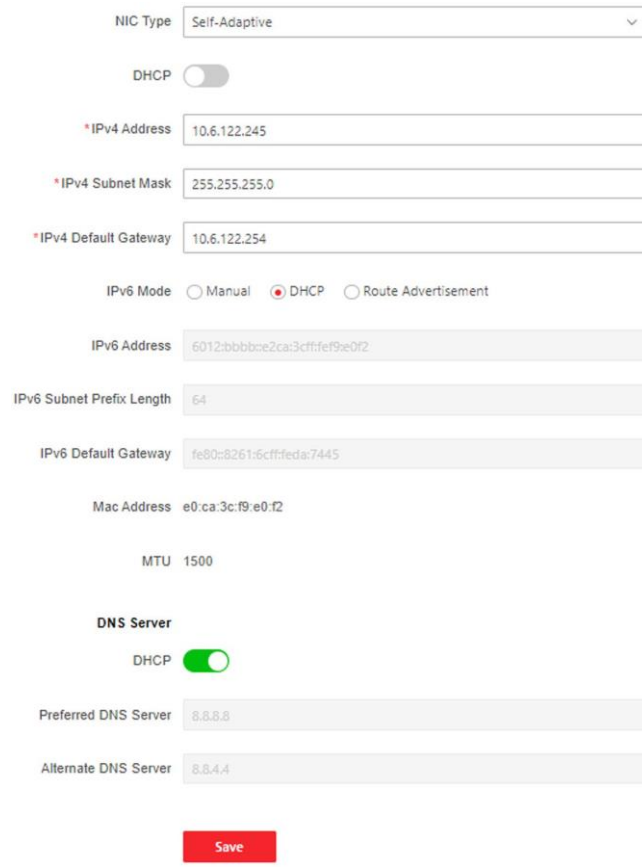


図 7-6 TCP/IP 設定ページ

パラメータを設定し、**[保存]** をクリックして設定を保存します。

NIC タイプ

ドロップダウンリストから NIC タイプを選択します。デフォルトは「**自動**」です。

DHCP

この機能のチェックを外す場合は、IPv4アドレス、IPv4サブネットマスク、IPv4デフォルトゲートウェイ、MACアドレス、およびMTUを設定する必要があります。

この機能をチェックすると、システムは自動的にIPv4アドレス、IPv4サブネットマスク、IPv4デフォルトゲートウェイを割り当てます。

DNSサーバー

実際のニーズに応じて、優先 DNS サーバーと代替 DNS サーバーを設定してください。

Wi-Fi パラメータの設定

デバイスのワイヤレス接続用に Wi-Fi パラメータを設定します。

手順

注意
この機能はデバイスでサポートされている必要があります。

1. **システムとメンテナンス → システム構成 → ネットワーク → ネットワーク設定 → Wi-Fi** をクリックします。

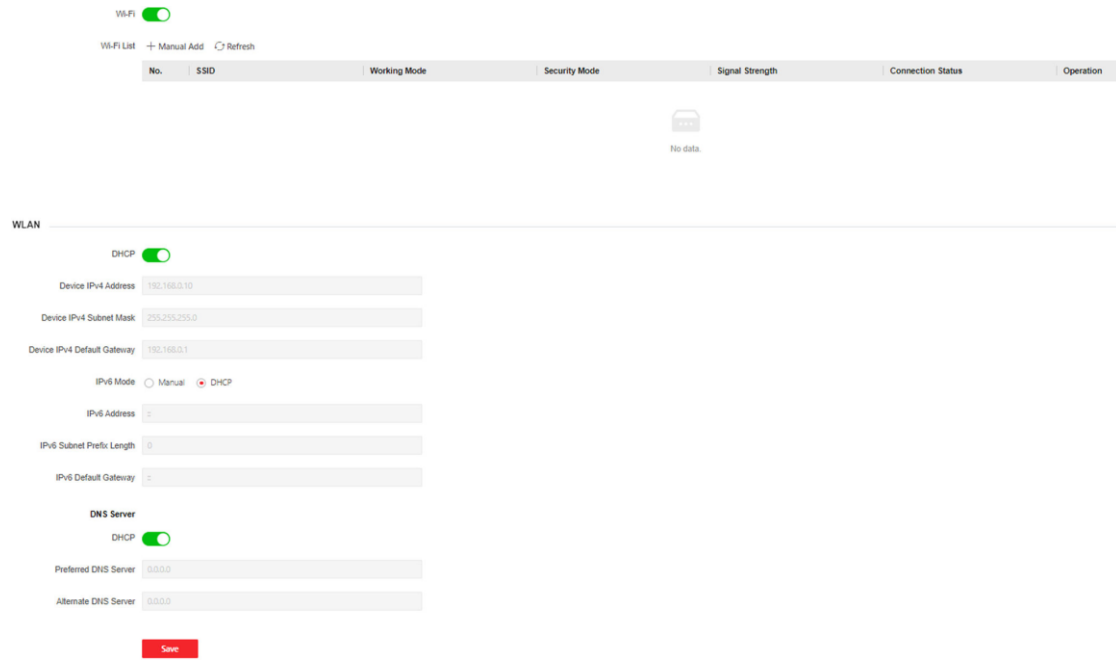


図7-7 Wi-Fi設定ページ

2. **Wi-Fi**を確認してください。

3. Wi-Fiを選択
- リスト内のWi-Fiの「」をクリックし、Wi-Fiパスワードを入力します。
- **[追加]** をクリックし、Wi-Fi の名前、パスワード、暗号化タイプを入力します。**[接続]** をクリックします。Wi-Fi が接続されたら、**[OK]** をクリックします。

4. **オプション：**WLAN パラメータを設定します。
1) IP アドレス、サブネットマスク、およびデフォルトゲートウェイを設定します。または、**DHCP** を有効にすると、システムが IP アドレス、サブネットマスク、およびデフォルトゲートウェイを自動的に割り当てます。

5. **保存**をクリックします。

PC Web 経由で Bluetooth を有効/無効にする

デバイスのBluetoothを有効にして、Bluetoothサウンドを接続できます。

手順

1. **アクセス制御 → システム設定 → ネットワーク → ネットワーク設定 → Bluetooth** の順にクリックし、設定ページに入ります。
2. Bluetoothパラメータ設定セクションで「**有効**」を選択します。
3. **デバイス名**に外部サウンドを入力します。Bluetooth接続後、**保存**をクリックします。

PC Web経由でのポート設定

システムとメンテナンス → システム構成 → ネットワーク → ネットワークサービス に移動します。

HTTP を有効/無効にする

HTTP機能を有効にして、ブラウザの閲覧セキュリティを向上させます。

システムとメンテナンス → システム構成 → ネットワーク → ネットワークサービス → HTTP(S) に移動します。

パラメータ設定後、**[保存]をクリックします**。

HTTPポート

ブラウザでログインする際、アドレスの後に変更したポート番号を追加する必要があります。例えば、HTTPポート番号を81に変更した場合、ブラウザでログインする際にはhttp://

192.0.0.65：81 と入力する必要があります。

HTTPS ポート

ブラウザでアクセスするためのHTTPSポートを設定します。ただし、認証が必要です。

HTTP リスニング

デバイスはHTTPプロトコルにより、アラーム情報を宛先IPまたはドメイン名へ送信します。宛先IPまたはドメイン名はHTTPプロトコルをサポートしている必要があります。宛先IPまたはドメイン名、URL、ポートを入力し、プロトコルタイプを選択してください。

PC Web経由でのRTSPポート表示

RTSPポートはリアルタイムストリーミングプロトコルのポートです。

システムとメンテナンス → システム構成 → ネットワーク → ネットワークサービス → RTSP に移動し、ポートを確認します。

PC Web経由でのWebSocket設定

WebSocketおよびWebSocketsポートを確認します。

システムとメンテナンス → システム構成 → ネットワーク → ネットワークサービス → WebSocket(s) に移動します。

WebSocket と WebSockets ポートを表示します。

SDKサービスを有効にする

SDKサービスを有効にすると、デバイスをSDKサーバーに接続できます。

システムとメンテナンス → システム構成 → ネットワーク → デバイスアクセス → SDKサーバーをクリックして設定ページに入ります。

サーバーポートを入力します。

設定を有効にするには、**保存**をクリックします。

PC Web経由でISUPパラメータを設定する

ISUPプロトコル経由でデバイスにアクセスするためのISUPパラメータを設定します。

手順

注記

この機能はデバイスがサポートしている必要があります。

1. **システムとメンテナンス → システム構成 → ネットワーク → デバイスアクセス → ISUP** をクリックします。
2. **[有効]** をチェックします。
3. ISUP バージョン、サーバーアドレス、デバイス ID、および ISUP ステータスを設定します。

   注記

   バージョンとして 5.0 を選択する場合は、暗号化キーも設定する必要があります。
4. ISUPリスニングパラメータを設定します。これには、ISUPアラームセンターのIPアドレス/ドメイン名、ISUPアラームセンターのURL、およびISUPアラームセンターのポートが含まれます。
5. **保存**をクリックします。

PC Web経由でOTAPを設定

OTAP プロトコルを介してデバイスをプラットフォームに接続し、デバイス情報の取得、動作状況およびアラーム情報のアップロード、デバイスの再起動およびアップグレードを行います。

手順

1. **システムとメンテナンス → システム構成 → ネットワーク → デバイスアクセス → OTAP** をクリックします。

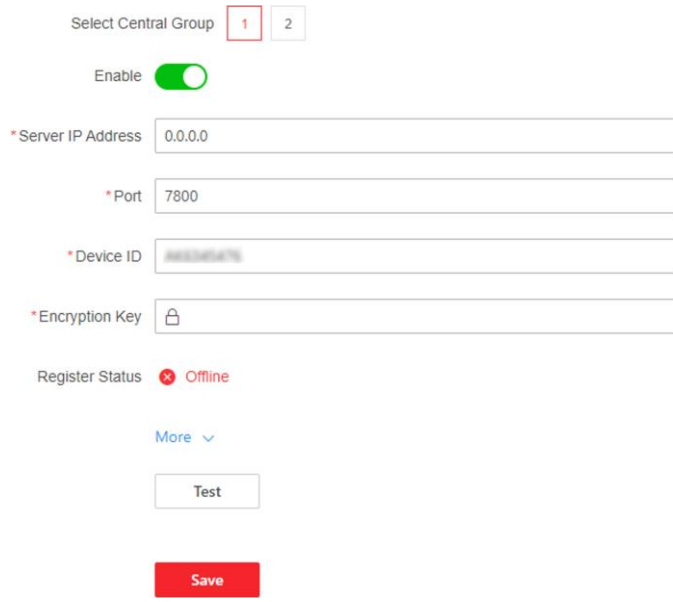


図 7-8 OTAP の設定

2. OTAPを**有効にする**をクリックします。
3. **サーバーIPアドレス**、**ポート**、**デバイスID**、**暗号化キー**を設定します。
4. **テスト**をクリックし、デバイスがサーバーに接続して正常に登録できることを確認してください。ページを更新するかデバイスを再起動して、**登録ステータスを**確認してください。
5. **「詳細」**をクリックしてネットワークタイプとアクセス優先度を確認します。操作アイコンを上下にドラッグしてネットワーク優先度を調整します。
6. **保存**をクリックします。

PC Web経由のプラットフォームアクセス

プラットフォームアクセスでは、プラットフォーム経由でデバイスを管理するオプションが提供されます。

手順

1. **システムとメンテナンス → システム構成 → ネットワーク → デバイスアクセス → Hik-Connect** をクリックして設定ページに入ります。

> **注**
> Hik-Connectはモバイル端末向けアプリケーションです。本アプリでは、デバイスのライブ映像の閲覧やアラーム通知の受信などが可能です。

2. 機能を有効にするには**「有効」**にチェックを入れてください。
3. **オプション：**「**カスタム**」のチェックボックスをオンにすると、サーバーアドレスを自分で設定できます。
4. 認証コードを入力してください。
5. **「表示」**をクリックしてデバイスのQRコードを表示します。QRコードをスキャンしてアカウントを紐付けます。

注意

8文字から32文字（aからz、AからZ）または数字（0から9）で構成され、大文字と小文字が区別されます。8文字以上の英数字の組み合わせを使用することを推奨します。

6. 設定を有効にするには「**保存**」をクリックしてください。

VoIPアカウント設定

ネットワーク経由で音声通話を実現できます。

手順

1. **システムとメンテナンス → システム構成 → ネットワーク → デバイスアクセス → VoIP** に移動します。
2. **通話タイプ**を選択し、VoIP を選択します。
3. **VoIPゲートウェイを**有効にします。
4. **ユーザー名、登録パスワード、サーバーIPアドレス、サーバーポート、有効期限、登録ステータス、番号、表示ユーザー名、センター番号を設定します。**
5. **保存**をクリック。

7.11.8 PC Web経由で映像・音声パラメータを設定

Webブラウザ経由での映像パラメータ設定

デバイスカメラの画質、解像度、その他のパラメータを設定できます。

システムとメンテナンス → システム構成 → ビデオ/オーディオ → ビデオ をクリックして設定ページに入ります。

カメラ名、ストリームタイプ、ビデオタイプ、解像度、ビットレートタイプ、ビデオ品質、フレームレート、最大ビットレート、ビデオエンコーディング、Iフレーム間隔を設定します。

保存をクリックします。

Webブラウザ経由でオーディオパラメータを設定

デバイスの音量を設定できます。

システムとメンテナンス → システム設定 → ビデオ/オーディオ → オーディオ をクリックして設定ページに入ります。

実際のニーズに応じて、ストリームタイプとオーディオエンコーディングを設定します。スライドして入力および出力の音量を設定します。

スライドして音声プロンプト機能を有効にします。

オーディオミキシングを有効にし、**出力サブボリューム**を設定できます。

SIPオーディオエンコーディングを選択します。

保存をクリックします。

7.11.9 画像パラメータ設定

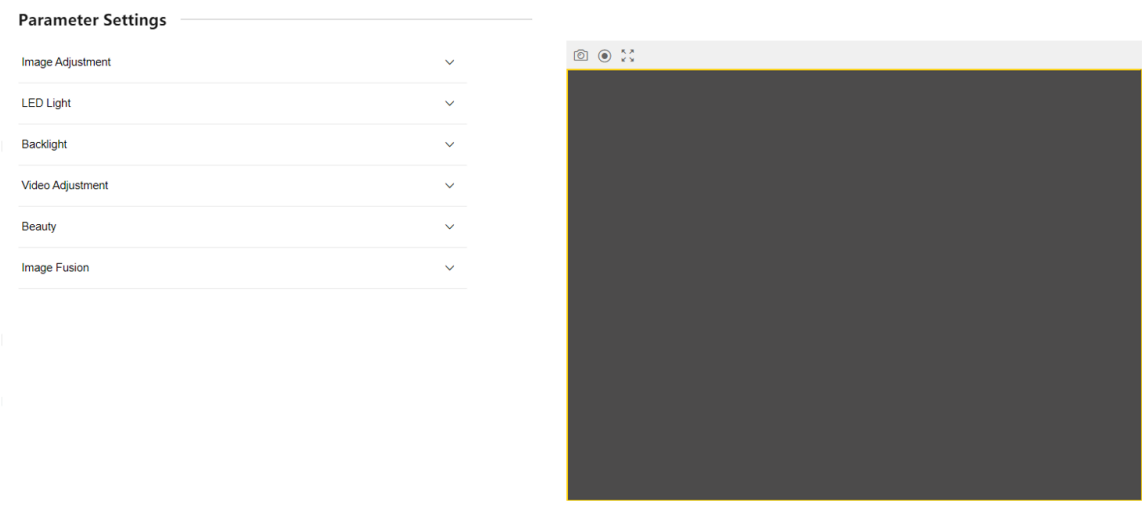


図 7-9 表示設定

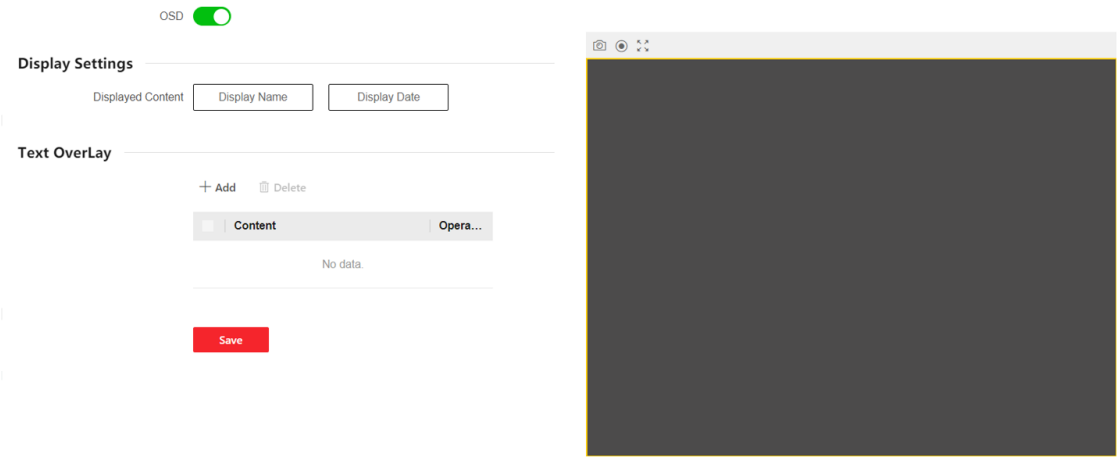


図 7-10 OSD 設定

PC Web 経由で明るさ/コントラスト/彩度/シャープネスを設定

ライブビューページの明るさ、コントラスト、彩度、シャープネスなどの画像情報を設定できます。

システムとメンテナンス → システム構成 → 画像 → 表示設定をクリックして設定ページに入ります。

画像調整

ブロックをドラッグするか数値を入力して、明るさ、コントラスト、彩度、シャープネスを設定します。「**デフォルト設定に戻す**」をクリックするとデフォルト設定に戻ります。

PC Web経由でLEDライトを設定

補助ライトの明るさを調整できます。

手順

1. **システムとメンテナンス → システム構成 → 画像 → ディスプレイ設定**をクリックして設定ページに入ります。
2. 補助ライトのタイプ、モード、明るさを設定します。
3. **オプション: [デフォルト設定に復元]** をクリックすると、デフォルト設定に復元されます。

PC Web経由でWDRを設定する

システムとメンテナンス → システム構成 → イメージ → ディスプレイ設定をクリックして設定ページに入ります。

ワイドダイナミックレンジを有効または無効にします。有効にすると、シーンの明るい部分と暗い部分の両方が同時に鮮明に見えます。

デフォルト設定に戻すをクリックすると、設定がデフォルトに戻ります。

PC Web経由でのビデオ標準設定

ライブビューページのビデオ標準を設定できます。

システムとメンテナンス → システム設定 → 画像 → 表示設定をクリックして設定ページに入ります。

ビデオ調整

リモートプレビュー中のビデオフレームレートを設定します。新しい設定を有効にするには、デバイスの再起動が必要です。

PAL

毎秒25フレーム。中国本土、香港（中国）、中東諸国、ヨーロッパ諸国などに適しています。

NTSC

毎秒30フレーム。アメリカ、カナダ、日本、台湾（中国）、韓国、フィリピンなどに適しています。

デフォルト設定に戻すをクリックすると、デフォルト設定に復元されます。

PC Web経由でビューティーパラメータを設定

有効化後、認証済み画像を美白または滑らかに処理できます。

システムとメンテナンス → システム構成 → イメージ → 表示設定をクリックして設定ページに入ります。
ビューティー機能を有効にし、ブロックをドラッグするか数値を入力して美白・滑らかさのレベルを設定します。
「**デフォルト設定に戻す**」をクリックするとデフォルト設定に復元されます。

PC Web経由で画像融合を設定

画質向上のために画像合成機能を有効にできます。

システムとメンテナンス → システム設定 → 画像 → 表示設定をクリックして設定ページに入ります。
イメージ融合
画像融合を**自動**または**無効**に設定します。ブロックをドラッグするか数値を入力して感度を設定します。
デフォルト設定に戻すをクリックすると、デフォルト設定に復元されます。

PC Web経由でOSDパラメータを設定

ライブビューに表示されるカメラ名、日時形式、表示モード、OSDサイズをカスタマイズできます。

手順
1. **システムとメンテナンス → システム設定 → 画像 → OSD設定**をクリックして設定ページに入ります。
2. **OSDを**有効にします。
3. 必要に応じて、カメラ名、日付、または週の表示を選択するには、対応するチェックボックスを選択してください。
4. **カメラ名**を入力してください。
5. ドロップダウンリストから選択して、**時刻形式**と**日付形式**を設定します。
6. **[追加]** をクリックしてテキストボックスに文字を入力し、OSD の位置と配置を調整します。

7.11.10 PC Web によるアラーム設定

アラーム出力パラメータを設定します。

手順
1. **システムとメンテナンス → システム構成 → イベント → アラーム設定 → アラーム出力を**クリックします。
2. **アラーム**名とアラーム持続時間のモードを設定**します**。

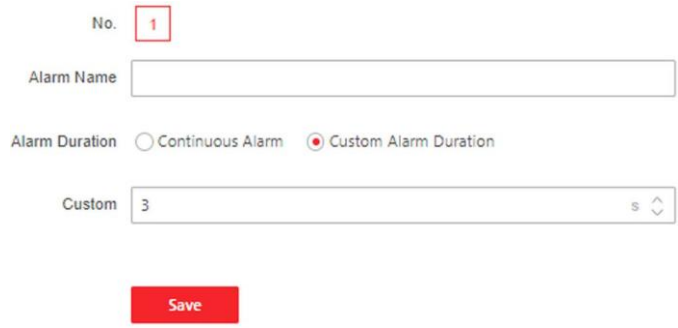


図7-11 アラーム設定

連続アラーム

アラームが作動すると、継続的に警報が鳴ります。

カスタムアラーム持続時間

アラームが作動した際のデバイスのアラーム**持続時間を**設定できます。

7.11.11 連動設定

設定されたイベントが発生した場合、設定された方法に従ってイベント情報を中央プラットフォームにアップロードします。

手順

1. **システムとメンテナンス → システム構成 → イベント → 連携設定**をクリックして設定ページに入ります。
2. **「+」**をクリックします。
3. イベントソースを設定します。リンクタイプを「**イベントリンク**」「**カードリンク**」「**従業員IDリンク**」から選択します。
   - **リンクタイプ**を**イベントリンク**に設定すると、実際のニーズに応じてイベントタイプを選択できます。
   - **連携タイプ**を**カード連携**に選択した場合、**カード番号**を入力し**カードリーダー**を選択します。
   - **連携タイプを**「**従業員IDリンク**」に選択した場合、**従業員ID**を入力し**カードリーダー**を選択します。
4. 連動アクションを設定します。
   1) **ドア連動を**有効にし、ドア動作を確認・選択します。
   2) **リンクされたアラーム出力を**有効にし、アラーム出力アクションを確認して選択してください。
   3) **リンクされたキャプチャを**有効にする。
5. 設定を有効にするには、**[保存] をクリックします**。

7.11.12 設定にアクセス

PC Web経由でRS-485パラメータを設定

周辺機器、アドレス、ボーレートなどの RS-485 パラメータを設定できます。

システムとメンテナンス → システム設定 → アクセス設定 → RS-485 をクリックします。**RS-485 プロトコル**を選択します。

RS-485を有効にするにチェックを入れ、パラメータを設定します。

設定後、**[保存]**をクリックして設定を保存します。

No.

RS-485番号を設定

周辺機器タイプ

実際の状況に応じて、ドロップダウンリストから周辺機器を選択してください。

注記

周辺機器を変更して保存すると、デバイスは自動的に再起動します。

RS-485 アドレス

実際のニーズに応じて RS-485 アドレスを設定してください。

注記

アクセスコントローラを選択した場合：RS-485 インターフェースを介してデバイスを端末に接続する場合は、RS-485 アドレスを 2 に設定してください。デバイスをコントローラに接続する場合は、ドア番号に応じて RS-485 アドレスを設定してください。

ボーレート

デバイスがRS-485プロトコルで通信する際のボーレート。

PC Web経由でのウィーガンドパラメータ設定

Wiegand 伝送方向を設定できます。

手順

注記

一部のデバイスモデルではこの機能をサポートしていません。設定時は実際の製品を参照してください。

1. **システムとメンテナンス → システム設定 → アクセス設定 → ウィーガンド設定** をクリックします。

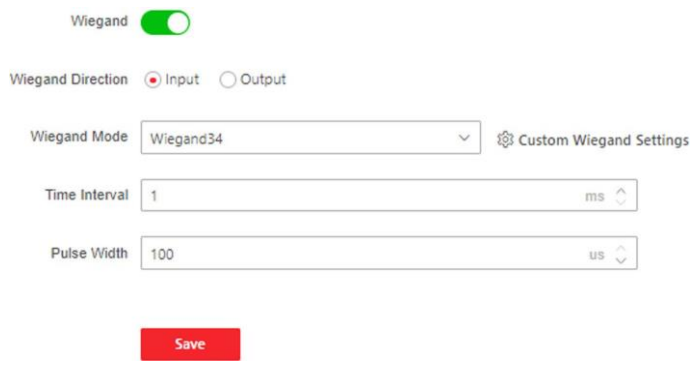


図 7-12 ウィーガンドページ

2. **Wiegand** をチェックして Wiegand 機能を有効にします。
3. 伝送方向を設定します。

入力

このデバイスはウィーガンド方式のカードリーダーを接続できます。

出力

外部アクセスコントローラを接続できます。そして、2つのデバイスはウィーガンド26または34を介してカード番号を送信します。

4. 設定を保存するには「**保存**」をクリックしてください。

注意

周辺機器を変更し、デバイスパラメータを保存すると、デバイスは自動的に再起動します。

PC Web経由でセキュアドア制御ユニットのパラメータを設定

セキュアドア制御ユニットのパラメータを設定できます。

手順

1. **システムとメンテナンス → アクセス設定 → セキュアドア制御ユニット**をクリックしてください。
2. ドアを選択してください。

注記

ドア1を選択すると、そのドアはセキュアドア制御ユニットによって制御されます。ドア2の選択についても同様です。

3. セキュアドア制御ユニットの状態を表示します。
4. **2ドア連動を**有効にできます。

注意

この機能を有効にすると、2つのドアを同時に開けることはできません。

Web経由のエレベーター制御

手順

1. **システムとメンテナンス → システム構成 → エレベーター制御** をクリックします。

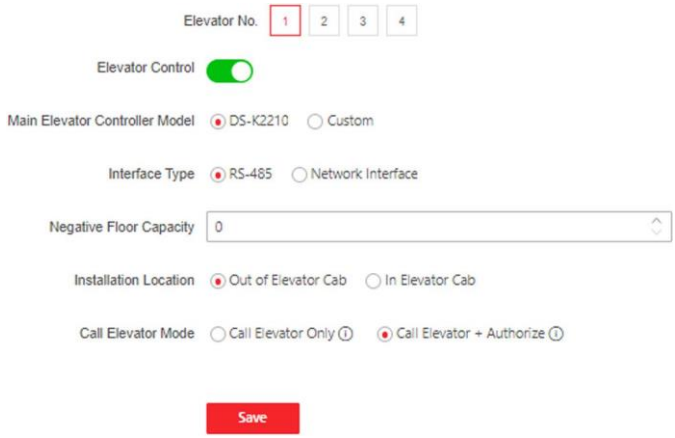


図7-13 エレベーター制御

2. **エレベーター制御を**有効にします。
3. エレベーターのパラメータを設定します。

メインエレベーターコントローラモデル

設定するエレベーター番号を選択します。

インターフェースタイプ

エレベーター通信用の通信タイプをドロップダウンリストから選択してください。

RS-485 を選択する場合は、RS-485 ケーブルでデバイスをエレベーターコントローラに接続していることを確認してください。

ネットワークインターフェースを選択した場合、通信用にエレベーターコントローラのIPアドレス、ポート番号、ユーザー名、パスワードを入力してください。

負の階数設定

負の階数を設定します。

設置場所

設置場所を「**エレベーター外**」または「**エレベーター内**」から**選択**します。

エレベーター呼び出しモード

エレベーター呼び出しモードを選択します。

エレベーター呼び出し専用

認証通過後、デバイスが指定階へエレベーターを呼び出す

エレベーター呼び出し＋認証

本人が認証を通過すると、装置は当該階へエレベーターを呼び出し、本人の部屋と連動した階へのアクセス権限を付与します。対応する階番号を押すことで、目的の階へ移動できます。

注記

- 1台のデバイスに最大4台のエレベーターコントローラーを接続可能。
- 最大10階までの負階を追加できます。
- 同じデバイスに接続されているエレベーターコントローラのインターフェースタイプが一致していることを確認してください。

7.11.13 勤怠設定

従業員の勤務時間、遅刻、早退、休憩、欠勤などを記録したい場合、その従業員をシフトグループに追加し、シフトスケジュール（出勤を定義するルールで、スケジュールの繰り返し方法、シフトタイプ、休憩設定、カード打刻ルールを定義）をシフトグループに割り当て、シフトグループ内の従業員の出勤パラメータを定義できます。

Web経由での出勤モード無効化

勤怠モードを無効にすると、システムは初期画面で勤怠ステータスを表示しなくなります。

手順

1. **システムとメンテナンス → システム設定 → プラットフォーム勤怠**をクリックして設定ページに入ります。
2. **勤怠管理**を無効にします。**結果**

初期画面では出席状況を確認または設定できません。システムはプラットフォームで設定された出席ルールに従います。

Web経由での手動出席設定

出席モードを手動に設定し、出席を取る際に手動でステータスを選択する必要があります。

開始前に

ユーザーを少なくとも1人追加し、ユーザーの認証モードを設定してください。詳細は「*ユーザー管理*」を参照してください。

手順

1. **システムとメンテナンス → システム設定 → プラットフォーム出席**をクリックし、設定ページに入ります。
2. **出席モード**を手**動**に設定します。
3. **出席ステータス必須**を有効にし、出席ステータスの有効期間を設定します。
4. 出席ステータスのグループを有効にします。

注記

出席プロパティは変更されません。

5. **オプション：**必要に応じてステータスを選択し、その名前を変更します。

結果

認証後、手動で出席ステータスを選択する必要があります。

注記

ステータスを選択しない場合、認証は失敗し、有効な出席として記録されません。

Web経由での自動出席設定

出席モードを自動に設定すると、出席ステータスとその有効スケジュールを設定できます。システムは設定されたスケジュールに従って出席ステータスを自動的に変更します。

開始前に

ユーザーを少なくとも1人追加し、そのユーザーの認証モードを設定してください。詳細は「*ユーザー管理*」を参照してください。

手順

1. **システムとメンテナンス → システム構成 → プラットフォーム出席**をクリックして設定ページに入ります。
2. **出席モード**を「**自動**」に設定します。
3. 出席ステータス必須機能を有効にします。
4. 出席ステータスのグループを有効にします。

注記

出席プロパティは変更されません。

5. **オプション：**必要に応じてステータスを選択し、名前を変更します。
6. ステータスのスケジュールを設定します。詳細はを参照してください。

Web経由での手動・自動出席設定

出勤モードを「**手動**」と「**自動**」に設定すると、システムは設定されたスケジュールに従って出勤ステータスを自動的に変更します。同時に、認証後に出勤ステータスを手動で変更することも可能です。

開始前に

少なくとも1人のユーザーを追加し、ユーザーの認証モードを設定してください。詳細は「*ユーザー管理*」を参照してください。

手順

1. **システムとメンテナンス → システム設定 → プラットフォーム出席**をクリックして設定ページに入ります。
2. **出席モード**を「**手動**」と「**自動**」に設定します。
3. 出席状況必須機能を有効にします。
4. 出席ステータスのグループを有効にする。

   注記

   出席プロパティは変更されません。

5. **オプション：**必要に応じてステータスを選択し、名前を変更します。
6. ステータスのスケジュールを設定します。詳細はを参照してください。

結果

初期ページで認証を行います。スケジュールに従い、設定された出席ステータスで認証がマークされます。結果タブの編集アイコンをタップすると、手動で出席を取るステータスを選択でき、認証は編集された出席ステータスでマークされます。

例

ブレイクアウトを月曜11:00に設定し、**ブレイクイン**を月曜12:00に設定した場合、月曜11:00から12:00までの有効なユーザーの認証は休憩としてマークされます。

7.12 設定

7.12.1 PC Web経由で起動画面を設定

起動画像を設定します。

システムとメンテナンス → 設定 → 画面表示 に移動します。

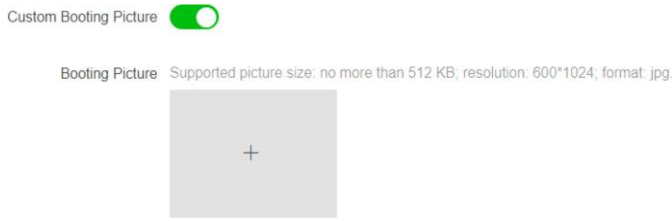


図 7-14 起動画像

カスタム起動画像を使用を有効にし、**+** をクリックしてローカルから起動画像を選択します。

注
サポートされる画像サイズ：512 KB以下；解像度：600*1024；形式：jpg。

保存をクリックしてください。

7.12.2 PC Web経由でスタンバイ画像をセット

スタンバイ画像のパラメータ（スタンバイに入るまでの時間、スクリーンセーバー画像、表示効果、スライドショーの間隔など）を設定します。

システムとメンテナンス → 設定 → 画面表示 に移動します。

スタンバイに入るまでの時間

設定した時間が経過すると、デバイスはスタンバイ画像を表示します。

7.12.3 PC Web経由でスリープ時間を設定

設定した時間が経過すると、デバイスはスリープモードになります。この機能により消費電力が削減されます。

システムとメンテナンス → 設定 → 画面表示 に移動してください。

図7-15 スリープ設定

スリープをスライドしてスリープ時間を設定します。**保存**をクリックします。

7.12.4 通話背景設定

通話のバックグラウンドを設定できます。

手順

1. **システムとメンテナンス → 設定 → 画面表示** に移動します。
2. **カスタム通話背景を**有効にし、**+**をクリックして画像を選択します。
3. **保存**をクリックします。

7.12.5 PC Web経由で認証デスクをカスタマイズ

認証ページ/デスク上のモジュールをカスタマイズします。

手順

1. **システムとメンテナンス → 設定 → カスタムホームページ** に移動します。
2. **アプリケーションモード**を選択します。

   認証モード

   デバイスの認証ページにはライブビューページが表示されます。認証後、人物名、社員ID、顔写真が表示されます。

   フルスクリーン広告

   広告は認証ページの全画面を占めます。スクリーンセーバーやウェルカムメッセージを広告内で再生可能です。

   インターコムモード

   認証インターフェースには、クイック操作領域と認証領域が表示されます。クイック操作領域では、機能ごとにカスタマイズ可能なショートカットキーをサポートしています。

   分割画面での広告

   認証ページには広告領域と認証領域が含まれます。スクリーンセーバーやウェルカムメッセージを広告内で再生できます。
3. **適用**をクリックしてください。

7.12.6 PC Web経由での通知公開設定

デバイスの通知公開を設定できます。

システムとメンテナンス → 設定 → 通知公開 に移動します。

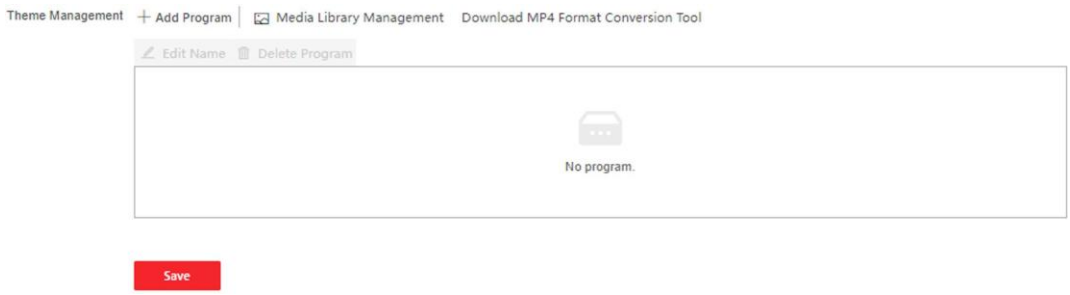


図 7-16 通知公開

MP4 形式変換ツールをダウンロード

フォーマットを変更する必要がある場合は、**「MP4 フォーマット変換ツールをダウンロード」**をクリックできます。

資材管理

「+ テーマを追加」をクリックし、**テーマ名**と**テーマタイプ**を設定できます。

アップロードをクリックし、ローカルPCから画像や動画をアップロードするには**「+」**をクリックします。

注意

現時点では、追加できるテーマは1つだけです。

プログラムを追加

プログラム名を設定し、プログラムタイプを選択することができます。

画像

画像を選択した場合、+をクリックして画像を追加できます。

ウェルカムメッセージ

ウェルカムメッセージを選択すると、メインタイトルとサブタイトルのテンプレート、内容、フォントサイズ、色を設定できます。背景画像もカスタマイズ可能です。

標準

標準を選択すると、背景色と背景画像を設定できます。

プレイスケジュール

テーマを作成後、テーマを選択しタイムライン上にスケジュールを描画できます。描画したスケジュールを選択すると、正確な開始時間と終了時間を編集できます。

描画したスケジュールを選択し、**「削除」**または**「すべて削除」**をクリックすると、スケジュールを削除できます。

スライドショー間隔

ブロックをドラッグするか、数値を入力してスライドショーの間隔を設定します。画像と動画は設定した間隔で切り替わります。

7.12.7 PC Web経由でプロンプトスケジュールを設定

認証成功時と失敗時の出力音声内容をカスタマイズします。

手順

1. **システムとメンテナンス → 設定 → プロンプトスケジュール** に移動します。

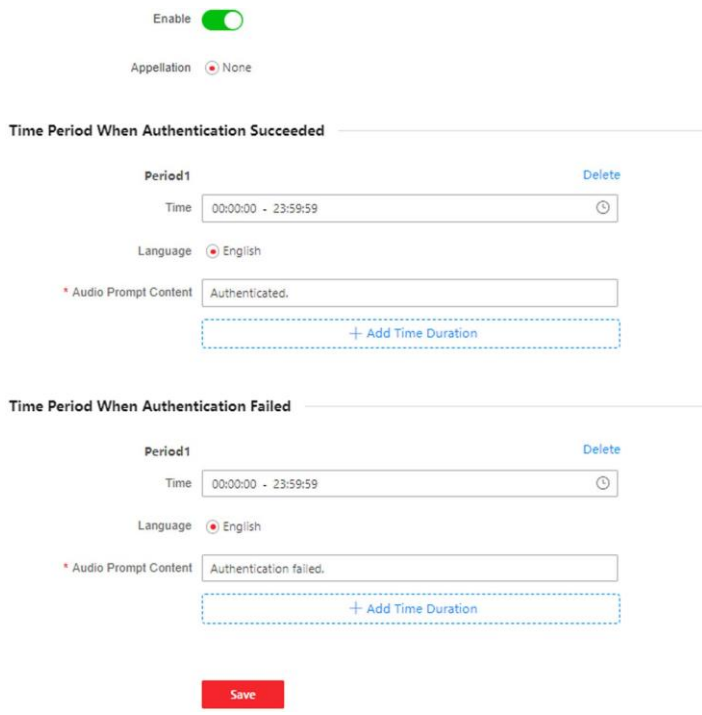


図 7-17 プロンプトスケジュール

2. 機能を有効にします。

3. 呼び出し名を設定します。

4. 時間スケジュールを選択します。

5. 認証が成功した期間を設定します。

1) **「時間範囲を追加」** をクリックします。

2) 時間設定。

注記

設定された時間内に認証が成功した場合、デバイスは設定された内容を放送します。

3) 音声プロンプトの内容を設定します。

4) **オプション：** サブステップ 1 から 3 を繰り返します。

5) **オプション：** をクリックして設定された時間制限を削除します。

6. 認証が失敗した場合の時間設定を行います。

1) 「**Add Time Duration**」をクリックします。
2) 時間設定を設定します。

注

設定された時間内に認証が失敗した場合、デバイスは設定されたコンテンツを放送します。

3) 音声コンテンツを設定します。
4) **オプション:** サブステップ1から3を繰り返します。
5) **オプション：** 設定した時間制限を削除するには、［ ］をクリックします。

7. 設定を保存するには「**保存**」をクリックします。

7.12.8 PC Web経由でのプロンプト音声のカスタマイズ

デバイスのプロンプト音声をカスタマイズできます。

手順

1. **システムとメンテナンス → 設定 → カスタムプロンプト** に移動します。

Custom Type	Importing Status	Operation
Call Center	Not Imported	
Nobody Answered	Not Imported	
Thanks	Not Imported	
Authenticating Failed	Not Imported	
The Door Is Open	Not Imported	
Please Wear the Safety Helmet	Not Imported	
Please Wear the Mask	Not Imported	

図 7-18 カスタムプロンプト

2. 「 」 →「 」 をクリックし、実際のニーズに応じてローカルPCから音声ファイルをインポートします。

注

アップロードする音声ファイルは512KB未満で、WAV形式である必要があります。

7.12.9 PC Web経由で認証結果テキストを設定する

手順

1. **システムとメンテナンス → 設定 → 認証結果テキスト** に移動します。

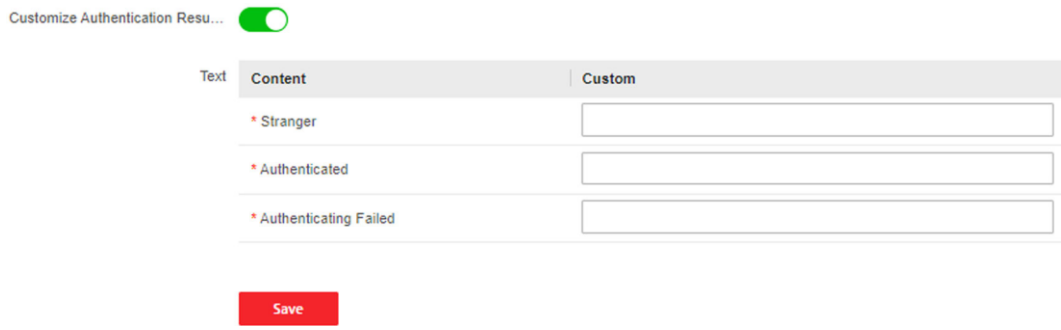


図 7-19 認証結果テキスト

2. **認証結果テキストのカスタマイズを**有効にします。
3. カスタムテキストを入力します。
4. **保存**をクリックします。

7.13 システムとメンテナンス

7.13.1 再起動

デバイスの再起動が可能です。

システムとメンテナンス → メンテナンス → 再起動をクリックして設定ページに入ります。

再起動をクリックするとデバイスが再起動します。

7.13.2 アップグレード

PC Web経由でのローカルアップグレード

デバイスをローカルでアップグレードできます。

システムとメンテナンス → メンテナンス → アップグレードをクリックして設定ページに入ります。

ドロップダウンリストからアップグレードタイプを選択します。をクリックし、ローカルPCからアップグレードファイルを選択します。**アップグレード**をクリックしてアップグレードを開始します。

PC Web経由のオンラインアップグレード

デバイスをオンラインでアップグレードできます。

システムとメンテナンス → メンテナンス → アップグレードをクリックして設定ページに入ります。

更新を確認**をクリックして**更新版があるかどうかを確認します。

デバイスがネットワークに接続され、Hik-Connectアプリに追加されている場合、Hik-Connectアプリに更新版があるときは、デバイス上で**「デバイスアップグレード」→「オンラインアップグレード」**をタップしてアップグレードできます。

キーフォブのアップグレード

注意

- 周辺モジュールがオンライン状態であることを確認してください。
- キーフォブをアップグレードする際は、顔認証端末を1台のみ周囲に置き、キーフォブを移動させないでください。

システムとメンテナンス → メンテナンス → アップグレード をクリックします。アップグレード設定のドロップダウンリストで、**キーフォブ**を選択します。ローカルPCからアップグレードファイルを選択します。**アップグレード → OK** をクリックします。キーフォブの任意のボタンを押してアップグレードを実行します。

7.13.3 復元

Webブラウザ経由での工場出荷時設定への復元

デバイスを工場出荷時の設定に復元できます。

システムとメンテナンス → メンテナンス → バックアップとリセットをクリックして設定ページに入ります。

「すべて復元」をクリックすると、すべてのパラメータが工場出荷時の設定に復元されます。使用前にデバイスをアクティベートする必要があります。

PC Web経由でのデフォルト設定への復元

デバイスの設定をデフォルトに戻すことができます。

システムとメンテナンス → メンテナンス → バックアップとリセットをクリックして設定ページに入ります。

「復元」をクリックすると、デバイスのIPアドレスとユーザー情報を除き、デフォルト設定に復元されます。

7.13.4 PC Web経由でデバイスパラメータをエクスポート

デバイスパラメータをエクスポートします。

システムとメンテナンス → メンテナンス → バックアップとリセット に移動します。

バックアップ

エクスポートをクリックしてデバイスパラメータをエクスポートします。

注記

デバイスパラメータをエクスポートし、それらのパラメータを他のデバイスにインポートします。

7.13.5 PC Web経由でのデバイスパラメータのインポート

設定パラメータをインポートします。

システムとメンテナンス → メンテナンス → バックアップとリセット に移動します。

設定ファイルのインポート

をクリックし、ローカルPCからファイルを選択します。**Import**をクリックします。

7.13.6 デバイスのデバッグ

デバイスのデバッグパラメータを設定できます。

Webブラウザ経由でのSSHの有効化/無効化

リモートデバッグを実行するためにSSHを有効にできます。

システムとメンテナンス → メンテナンス → デバイスデバッグ → デバッグ用ログをクリックします。**SSHを有効にします**

SSHはリモートデバッグに使用されます。このサービスを使用する必要がない場合は、セキュリティ向上のためSSHを無効化することを推奨します。

PC Web経由でデバイスログを印刷

デバイスログを印刷できます。

システムとメンテナンス → メンテナンス → ログをクリックして設定ページに入ります。**エクスポート**をクリックしてデバイスログを印刷します。

PC Web経由でネットワークパケットをキャプチャ

キャプチャパケットの持続時間とサイズを設定し、キャプチャを開始します。キャプチャ結果に基づいてログを確認し、デバッグできます。

システムとメンテナンス → メンテナンス → デバイスデバッグ → デバッグ用ログ に移動します。**キャプチャパケット期間**、**キャプチャパケットサイズ**を設定し、**[キャプチャ開始]**をクリックします。

PC Web経由でのプロトコルテスト

プロトコルアドレスを選択し、テストするプロトコルを入力します。応答ヘッダーと返り値に基づいてデバイスのデバッグが可能です。

システムとメンテナンス → メンテナンス → デバイスデバッグ → プロトコルテスト に移動します。

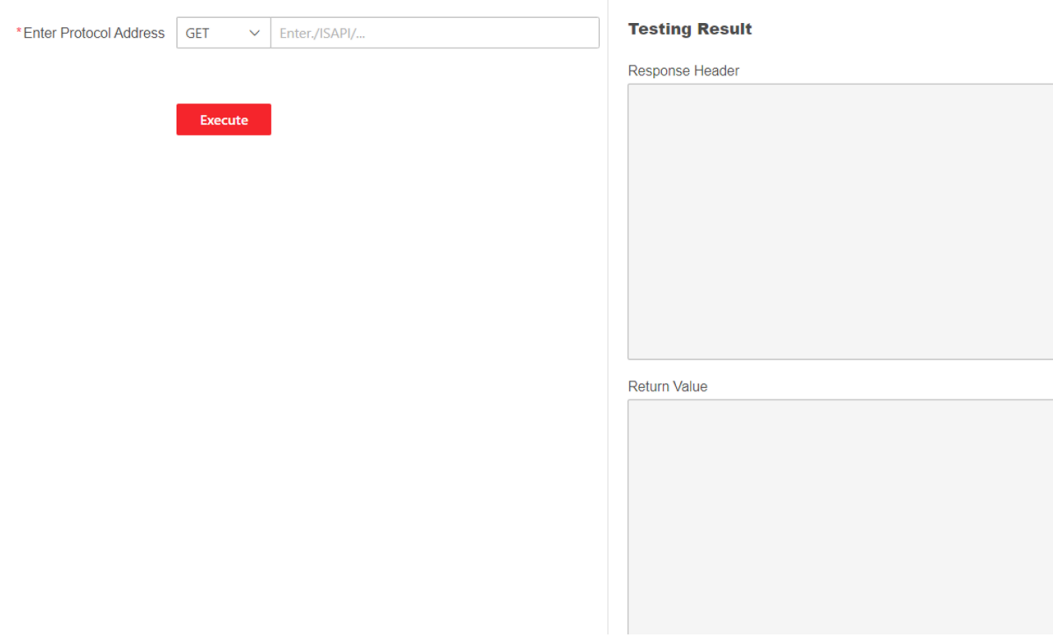


図7-20 プロトコルテスト

プロトコルアドレスを選択し、プロトコルを入力します。**実行**をクリックします。
応答ヘッダーと返り値に基づいてデバイスをデバッグする。

PC Web経由のネットワーク診断

デバイスのIPアドレスまたはドメイン名を入力すると、PING設定を実行できます。PING結果に基づいてネットワークをデバッグします。

システムとメンテナンス → メンテナンス → デバイスデバッグ → ネットワーク診断 に移動します。

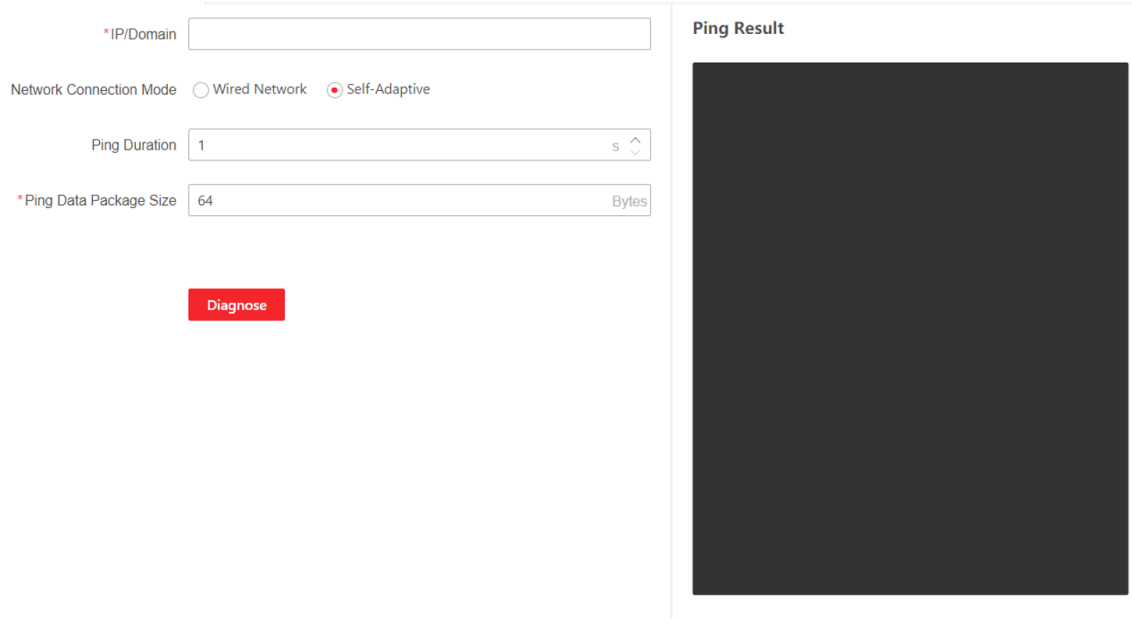


図7-21 ネットワーク診断

PING操作を行うデバイスのIPを入力し、ネットワーク接続モード、PING継続時間、Pingデータパケットサイズを選択します（デフォルトパラメータが推奨されます）。**「診断」**をクリックします。結果は「**PING結果**」に表示されます。

PC Web経由でのネットワーク侵入サービス設定

デバイスがLANに展開されている場合、侵入サービスを活用してデバイス遠隔管理を実現できます。

手順

1. **システムとメンテナンス → メンテナンス → デバイスデバッグ → ネットワークペネトレーションサービス** に移動します。
2. **「侵入サービス有効化」**をスライドします。
3. **サーバーのIP**アドレスと**ポート**を設定します。**ユーザー名**と**パスワード**を作成します。
4. **オプション：ハートビートタイムアウト**を設定できます。設定範囲は1～6000です。
5. **オプション：**ペネトレーションサービスのステータスを確認できます。**「更新」**をクリックするとステータスが更新されます。
6. **保存**をクリックします。

注記

ペネトレーションサービスは48時間後に自動無効化されます。

7.13.7 PC Web経由でログを表示

デバイスのログを検索・閲覧できます。

システムとメンテナンス → メンテナンス → ログ に移動します。

ログタイプのメジャータイプとマイナータイプを設定します。検索の開始時刻と終了時刻を設定し、「**検索**」をクリックします。

検索結果が以下に表示されます。これには、番号、時間、メジャータイプ、マイナータイプ、チャネル番号、ローカル/リモートユーザー情報、リモートホストIPなどが含まれます。

7.13.8 PC Web経由の詳細設定

顔パラメータ、掌パラメータの設定、バージョン情報の確認が可能です。**システムとメンテナンス → メンテナンス → 詳細設定** に移動します。

デバイスのアクティベーションパスワードを入力し、**Enterキー**を押してください。

顔パラメータ

カスタム偽装検出を有効にすると、**偽装検出しきい値 1:1**、**偽装検出しきい値 1:N** を設定できます。
認証用顔ロックを有効にし、**ロック期間**を設定します。偽装検出の失敗回数制限に達すると、設定されたロック期間、顔がロックされます。

保存をクリックします。

掌紋パラメータ

カスタム偽装検出を有効にすると、**偽装検出のしきい値**を設定できます。**保存**をクリックします。

バージョン情報

ここで、さまざまなバージョン情報を確認できます。

7.13.9 セキュリティ管理

PCウェブにログインする際のセキュリティレベルを設定します。

システムとメンテナンス → 安全 → セキュリティサービス に移動します。

セキュリティモード

ログイン時に高いセキュリティレベルを設定し、ユーザー情報を確認します。

互換モード

古いユーザー認証方法と互換性があります。

保存をクリックします。

7.13.10 証明書管理

サーバー/クライアント証明書および CA 証明書の管理に役立ちます。

注
この機能は特定のデバイスモデルでのみサポートされています。

自己署名証明書の作成とインポート

手順

1. **システムとメンテナンス → セキュリティ → 証明書管理** に移動します。
2. **証明書**ファイル領域で、ドロップダウンリストから**証明書タイプ**を選択します。
3. **作成**をクリックします。
4. 証明書情報を入力します。
5. **[OK]** をクリックして証明書を保存およびインストールします。
   作成された証明書は「**証明書の詳細**」領域に表示されます。証明書は自動的に保存されます。
6. 証明書をダウンロードし、ローカルコンピュータの要求ファイルに保存します。
7. 要求ファイルを認証機関に送信し、署名を受け取ります。
8. 署名付き証明書をインポートします。
   1) **[キーのインポート]** 領域で証明書の種類を選択し、ローカルから証明書を選択して **[インポート]** をクリックします。
   2) **通信**証明書のインポート領域で証明書の種類を選択し、ローカルから証明書を選択して**インポート**をクリックします。

その他の認証済み証明書のインポート

認証済み証明書（デバイスで作成されていないもの）を既に持っている場合は、それをデバイスに直接インポートすることができます。

手順

1. **システムとメンテナンス → セキュリティ → 証明書管理** に移動します。
2. 「**キーのインポート**」および「**通信証明書のインポート**」領域で、証明書の種類を選択し、証明書をアップロードします。
3. **インポート**をクリックします。

CA証明書のインポート

開始前に

CA 証明書を事前に準備してください。

手順

1. **システムとメンテナンス → 安全 → 証明書管理** に移動します。
2. **「CA証明書のインポート」**領域でIDを作成します。

   注意

   入力する証明書 ID は既存のものと同じにできません。
3. ローカルから証明書ファイルをアップロードします。
4. **インポート**をクリックします。

第8章 その他の設定プラットフォーム

iVMS-4200クライアントソフトウェアまたはHikCentralアクセス制御を介してもデバイスを設定できます。詳細は各プラットフォームのユーザーマニュアルを参照してください。

iVMS-4200クライアントソフトウェア

リンクをクリック/タップすると、クライアントソフトウェアのユーザーマニュアルが表示されます。

http://enpinfodata.hikvision.com/analysisQR/showQR/ca930247

HikCentral Access Control (HCAC)

リンクをクリック/タップして、HCACのユーザーマニュアルを表示します。

http://enpinfodata.hikvision.com/analysisQR/showQR/f2f6cf42

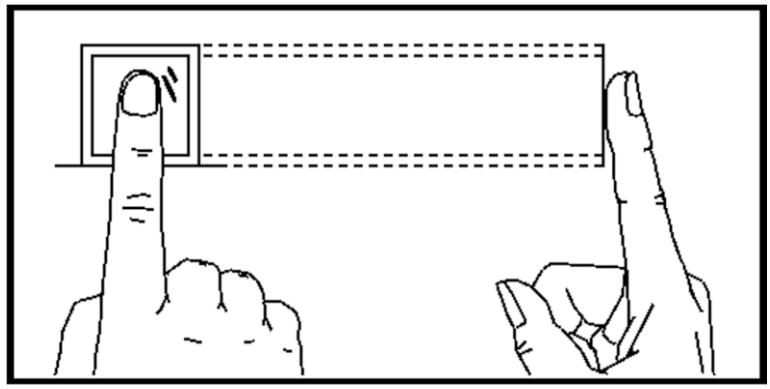
付録 A. 指紋スキャンに関する注意事項

推奨される指

人差し指、中指、または第三指。

正しいスキャン方法

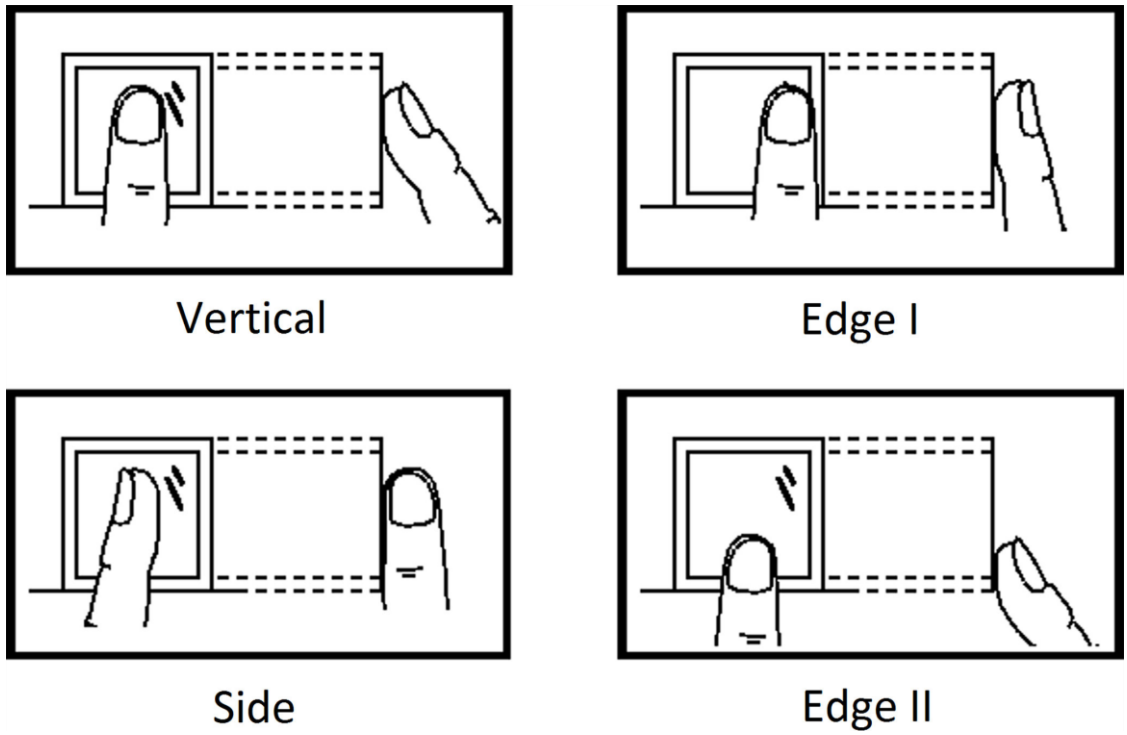
以下の図は指をスキャンする正しい方法です：



指をスキャナーに水平に押し当ててください。スキャンする指の中心がスキャナーの中心と一致するようにしてください。

誤ったスキャン方法

以下の指紋スキャン図は誤った方法です：



環境

スキャナーは直射日光、高温、湿気、雨を避けてください。乾燥している場合、スキャナーが指紋を正常に認識できないことがあります。指を軽く吹きかけ、再度スキャンしてください。

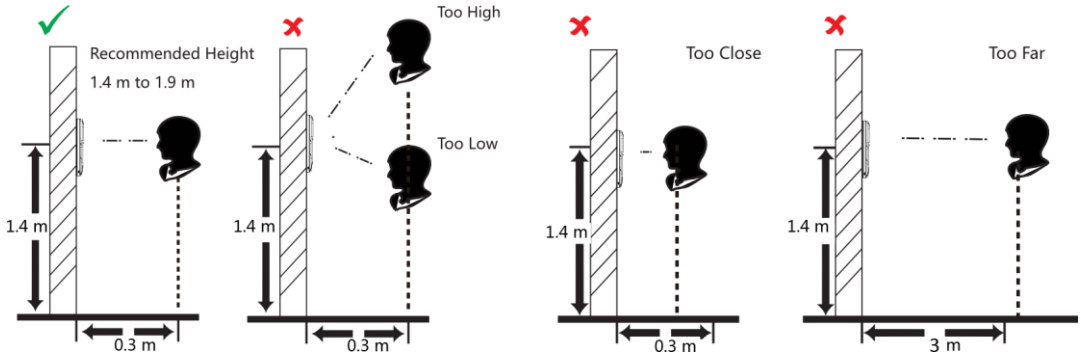
その他

指紋が浅い場合や指紋のスキャンが困難な場合は、他の認証方法のご利用をお勧めします。
スキャンする指に怪我がある場合、スキャナーが認識しない可能性があります。別の指に変更して再度お試しください。

付録B. 顔写真の収集・比較時の注意事項

顔写真の収集または比較時の位置は以下の通りです：

位置（推奨距離：0.3 m）



表情

- 顔写真を収集または比較する際は、下の写真のように自然な表情を保ってください。

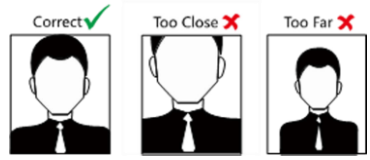
- 帽子、サングラス、その他顔認識機能に影響を与える可能性のあるアクセサリーは着用しないでください。
- 髪が目や耳などを覆わないようにし、濃いメイクは避けてください。

姿勢

高品質で正確な顔写真を撮影するため、顔写真の収集や比較時にはカメラに向かって顔を向けてください。

サイズ

顔は収集ウィンドウの中央に配置してください。



付録C. 手のひら紋様と手のひら静脈の追加の注意事項

- 掌紋および掌静脈を認識する際は、掌の中心をデバイス中心から5～12cmの距離に置き、周辺モジュールと平行に保つよう注意してください。
- 新しい顔認識端末に周辺モジュールを接続する場合、周辺モジュールのデータを消去し、再発行または収集する必要があります。
- 手のひらは汚れが付着しないよう清潔に保ってください。
- 周辺モジュールの表面は、センサーによる誤作動を防ぐため清潔に保つ必要があります。

付録D. アルコール検知の注意事項

- アルコール検知時は、ブローピストルにできるだけ近づけて吹き込み、排気口と平行に保ってください。
- ブローピストルは繰り返し差し込み・抜き差しには対応していません。3回の差し込み/抜き差し後にブローピストルの交換をお勧めします。
- 濃度が2.000mg/Lを超える場合、応答時間とクリア時間がともに増加します。次のユーザーは吹き込み前に20秒間待機する必要があります。
- 温度が30°Cを超える場合、または0°Cを下回る場合、応答時間とクリア時間がともに増加します。
- ブロウピストルに水やアルコールを直接噴射しないでください。ブロウピストルに残留したアルコールは測定精度に影響します。ユーザー自身で拭き取ってください。

付録E. 設置環境に関する注意事項

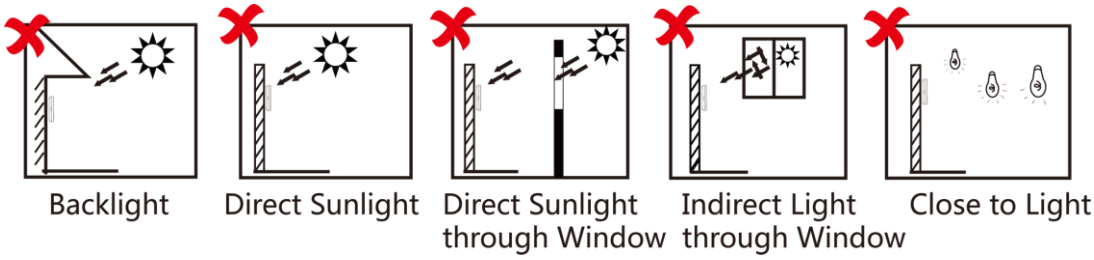
1. 光源の照度基準値

ろうそく：10ルクス

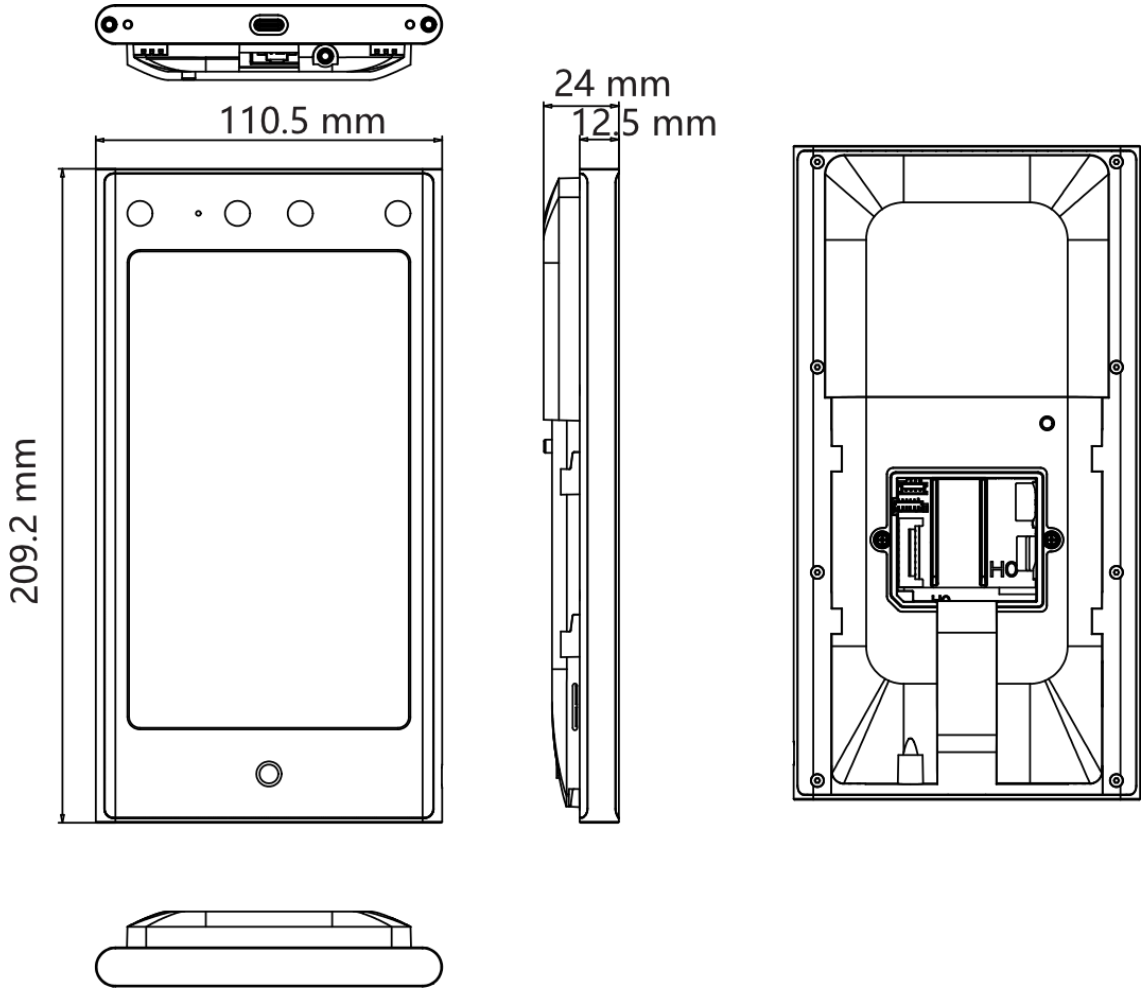
電球：100～850ルクス

太陽光：1200ルクス以上

2. 逆光、直射日光、間接日光を避けてください



付録 F. 寸法



図F-1 寸法