DS-K1T342シリーズ顔認証端末

ユーザーマニュアル

免責事項

本ドキュメントについて

- 本ドキュメントには、製品の使用および管理に関する説明が含まれています。以下に記載されている写真、図表、画像、および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などの理由により、予告なく変更される場合があります。最新バージョンのドキュメントは、Hikvision ウェブサイト（***https://www.hikvision.com***）でご覧ください。別段の合意がない限り、杭州**海康威視数字技術有限公司**およびその関連会社（以下「Hikvision」）は、明示または黙示を問わず、いかなる保証も行いません。
- 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。
- お選びいただいた商品が動画商品の場合、下記のQRコードをスキャンして「動画商品の利用に関する取り組み」を取得し、必ずお読みください。

知的財産権に関する承認

- Hikvision は、本書に記載された製品に組み込まれた技術に関連する著作権および/または特許を所有しており、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、図表等を含む一切の部分は Hikvision に帰属します。書面による許可なく、本文書のいかなる部分も、手段を問わず、抜粋、複製、翻訳、または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、様々な管轄区域において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。

免責事項

- 適用される法律で認められる最大限の範囲において、本書および記載されている製品（そのハードウェア、ソフトウェア、およびファームウェアを含む）は、「現状有姿のまま」かつ「すべての欠陥およびエラーを含むまま」提供されます。HIKVISION は、明示または黙示を問わず、いかなる保証も行いません。明示的、黙示的を問わず、商品性、満足のいく品質、特定目的への適合性を含むがこれらに限定されない一切の保証を否認します。 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、特別損害、結果的損害、付随的損害、間接損害（事業利益の損失、事業中断、データ損失、 システムの破損、または文書の損失を含むがこれらに限定されない損害について、契約違反、不法行為（過失を含む））、製造物責任その他のいかなる法的根拠に基づくものであっても、本製品の使用に関連して生じた場合であっても、HIKVISIONがそのような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、一切の責任を負いません。
- 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、本製品をすべての適用法令を遵守して使用することに同意し、その使用が適用法令に適合していることについて、単独で責任を負うものとします。特に、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第三者の権利を侵害しない方法で本製品を使用する責任を負います。また、本製品を、大量破壊兵器、化学兵器または生物兵器の開発または製造、核爆発装置または安全でない核燃料サイクルに関連する活動、人権侵害を支援する行為など、いかなる禁止用途にも使用してはなりません。
- 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。

記号の定義

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追加情報を提供します。

規制情報

FCC情報

適合性責任者が明示的に承認していない変更または改造は、本機器の操作権限を無効にする可能性があることにご留意ください。

FCC適合性：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値に適合することが試験により確認されています。これらの制限値は、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ため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・使用し、放射する可能性があり、指示に従って設置・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。

—本機器と受信機の間隔を広げる。

—機器は、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. この装置は、望ましくない動作を引き起こす可能性のある干渉を含め、受信したあらゆる干渉を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。電池にはこの記号が刻印されており、カドミウム（Cd）、鉛（Pb）、水銀（Hg）を示す文字が含まれる場合があります。 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

この装置は、カナダ産業省の免許不要RSS規格に準拠しています。動作は以下の2つの条件に従うものとします：

(1) 本装置は干渉を引き起こしてはならず、

(2) 本装置は、装置の意図しない動作を引き起こす可能性のある干渉を含む、あらゆる干渉を受け入れなければなりません。

安全上の注意

本取扱説明書は、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、重傷または死亡の原因となる可能性があります。

注意事項：いずれかの注意事項を怠ると、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、これらの予防措置に従ってください。

⚠危険：

- 本製品の使用にあたっては、国および地域の電気安全規制を厳守してください。
- 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あります。
- 煙、異臭、または騒音が機器から発生した場合は、直ちに電源を切り、電源ケーブルを抜いてください。その後、サービスセンターまでご連絡ください。
- コンセントは機器の近くに設置し、容易にアクセスできる状態にしてください。
- 1. 電池を飲み込まないでください。化学やけどの危険があります！

2. 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。
3. 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。
4. 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。
5. 電池を飲み込んだ、また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。
6. 注意：誤った種類の電池と交換すると爆発の危険があります。
7. 誤った種類の電池への不適切な交換は、安全装置を無効にする可能性があります（例：一部のリチウム電池タイプの場合）。
8. 電池を火の中や高温のオーブンに廃棄したり、機械的に押しつぶしたり切断したりしないでください。爆発の原因となる可能性があります。
9. 電池を極端に高温の環境に放置しないでください。爆発や可燃性液体・ガスの漏出の原因となる可能性があります。
10. 電池を極端に低い気圧にさらさないでください。爆発や可燃性液体・ガスの漏出の原因となる可能性があります。
11. 使用済み電池は指示に従って廃棄してください。

⚠ 注意事項：

- 本装置を落下させたり物理的衝撃を与えたりせず、高電磁波放射環境に曝さないでください。振動する表面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（不注意による装置損傷の原因となります）。
- 本装置を極端に高温（詳細な動作温度は装置の仕様を参照）、低温、ほこりっぽい、または湿気の多い場所に置かないでください。また、強い電磁放射にさらさないでください。
- 直射日光、換気の悪い場所、ヒーターやラジエーターなどの熱源に機器を曝すことは禁止されています（無知は火災の危険を引き起こす可能性があります）。
- 屋内用デバイスカバーは、雨や湿気から保護してください。
- 直射日光、換気の悪い場所、ヒーターやラジエーターなどの熱源に機器をさらすことは禁止されています（無視すると火災の危険があります）。
- デバイスカバーの内側と外側の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。
- 生体認証製品は、完全ななりすまし防止環境には適用されません。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。
- 本装置のシリアルポートはデバッグ専用です。
- 本マニュアルの指示に従って装置を設置してください。怪我を防ぐため、設置指示に従い装置を床/壁に確実に固定してください。
- 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。
- このブラケットは、専用の機器でのみご使用ください。他の機器との併用は不安定な状態を引き起こし、けがの原因となる可能性があります。
- 本装置は専用ブラケットとのみご使用ください。他の台車、スタンド、キャリアなどとの併用は不安定な状態を招き、けがの原因となる可能性があります。

対応モデル

製品名	モデル	ワイヤレス
顔認証端末	DS-K1T342MX DS-K1T342MX-E1	13.56 MHzカード提示周波数
	DS-K1T342MWX DS-K1T342MWX-E1	13.56 MHz カード提示周波数、Wi-Fi (2.4 GHz)
	DS-K1T342MFX DS-K1T342MFX-E1	13.56 MHz カード提示周波数
	DS-K1T342MFWX DS-K1T342MFWX-E1	13.56 MHz カード提示周波数、Wi-Fi (2.4 GHz)
	DS-K1T342EX DS-K1T342EX-E1	125 KHz カード提示周波数
	DS-K1T342EWX DS-K1T342EWX-E1	125 KHz カード提示周波数、Wi-Fi (2.4 GHz)
	DS-K1T342EFWX DS-K1T342EFWX-E1	125 KHz カード提示周波数、Wi-Fi (2.4 GHz)
	DS-K1T342DX DS-K1T342DX-E1	13.56 MHz カード提示周波数
	DS-K1T342DWX DS-K1T342DWX-E1	13.56 MHz カード提示周波数、Wi-Fi (2.4 GHz)

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
ADS-12FG-12N 12012EPG	深セン・オナー電子有限公司	PG

目次

第1章 概要

1.1 概要

顔認識端末は、顔認識によるアクセス制御装置の一種であり、主に物流センター、空港、大学キャンパス、警報センター、住宅などのセキュリティアクセス制御システムに適用されます。

1.2 特徴

- 4.3 インチ LCD タッチスクリーン、272 × 480 画面解像度、最大顔フレームのリアルタイム検出および表示。
- 200万画素広角デュアルレンズ
- 顔認証、指紋認証、カード認証、暗証番号認証、複数認証モードの組み合わせ認証に対応。
- アクセス制御期間制御（プランテンプレート）をサポートし、要求に応じてドアの開放を許可します。
- プラットフォームを介したネットワーク操作および人員権限情報の発行をサポートします。
- データネットワークアップロード機能をサポートし、デバイス比較結果や連動キャプチャ画像をプラットフォームにリアルタイムでアップロードできます。
- デバイスがオフラインの場合、デバイスがプラットフォームに接続された際に生成されたイベントは再度アップロードされます。
- NTP、手動、自動による時刻校正をサポートします。
- デバイス間のビデオインターホンをサポートします。
- RTSPプロトコルによるリモート映像プレビューおよび出力映像ストリームをサポート。
- ウォッチドッグ監視機構、改ざん防止設計をサポートし、デバイスの正常な動作を保証します。
- マスク着用モードのリマインダーやマスク着用必須モードを含むマスク検知モードをサポートします。
- IP65をサポートします。
- 標準PoEによる電源供給と、ドアロック用電源供給（12 VDC/1 A）を同時に行います。

注記

本機能はPoE対応デバイスでのみ利用可能です。

第 2 章 外観

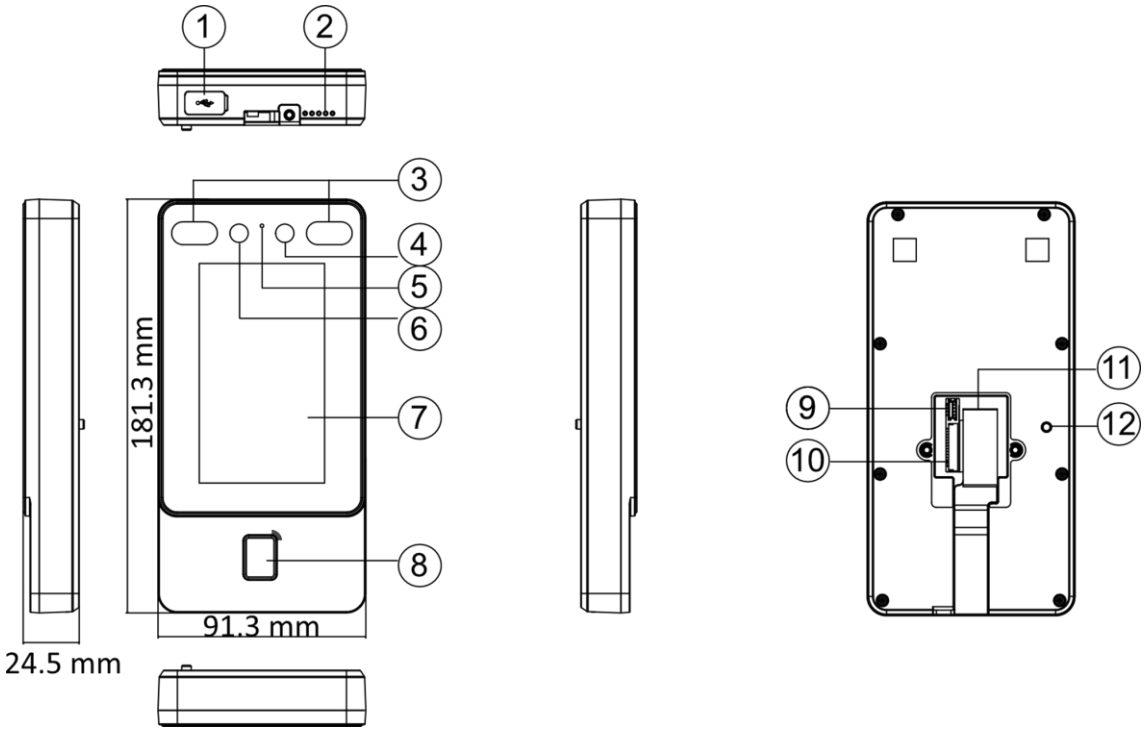


図 2-1 指紋モジュール付き表 2-1 外観の説明

No	名称
1	USB インターフェース
2	スピーカー
3	赤外線発光器
4	カメラ
5	マイク
6	カメラ
7	タッチスクリーン
8	指紋認証エリア/カード提示エリア
9	デバッグ用ポート（デバッグ専用）

No.	名前
10	配線端子
11	ネットワー クインター フェース
12	タンパー

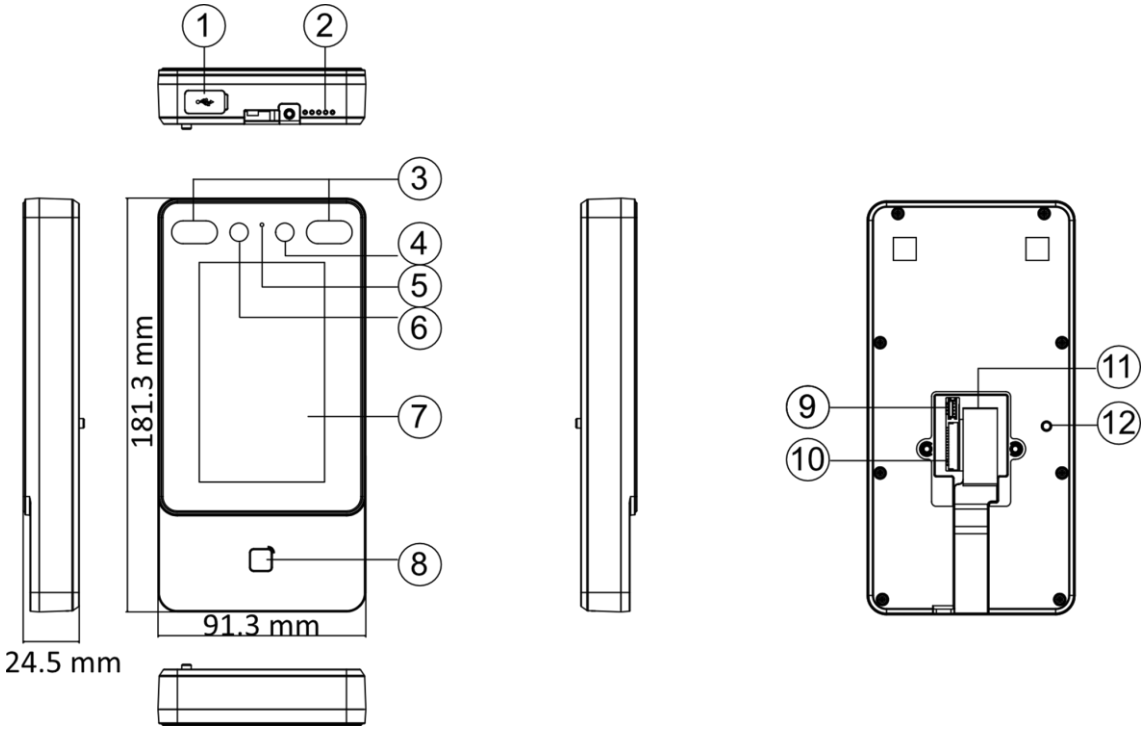


図 2-2 指紋モジュールなし表 2-2 外観の説明

番号	名称
1	USB インターフェース
2	スピーカー
3	赤外線発光器
4	カメラ
5	マイク
6	カメラ

番号	名称
7	タッチスクリーン
8	カード提示エリア
9	デバッグ用ポート（デバッグ専用）
10	配線端子
11	ネットワー クインター フェース
12	タンパー

第3章 設置

3.1 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です。
- 壁面その他の場所の最小支持荷重は、装置重量の3倍以上であること。
- 装置の視野範囲1m以内に、強い反射物（ガラスドア・壁、ステンレス製品、アクリルやその他の光沢プラスチック、漆、セラミックタイルなど）があってはなりません。
- 装置の反射を避けてください。
- 顔認識距離は30cm以上であること。
- カメラを清潔に保ってください。

注記

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。

3.2 ジャンボックス付き設置

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別途購入してください。

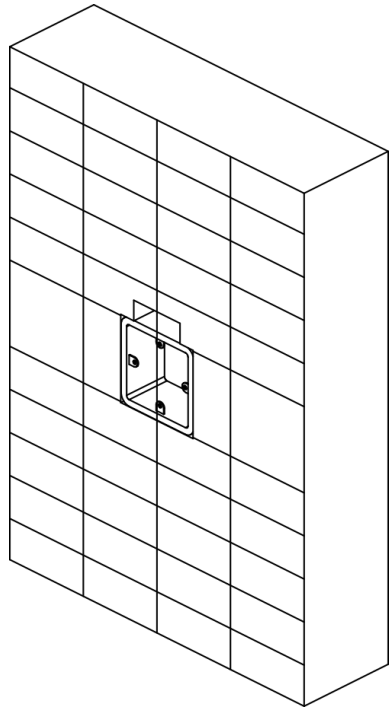


図 3-1 ギャングボックスの取り付け

2. 付属のネジ 2 本（SC-KA4X22）で、取り付けプレートをギャングボックスに固定します。

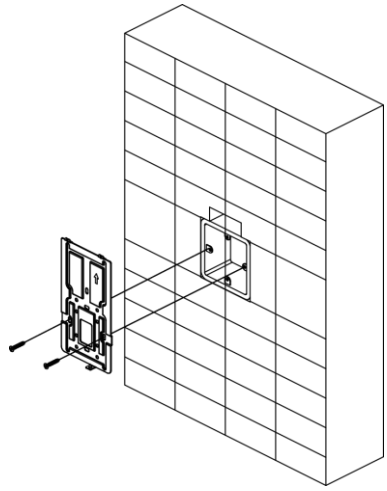


図 3-2 取付プレートの取り付け

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。

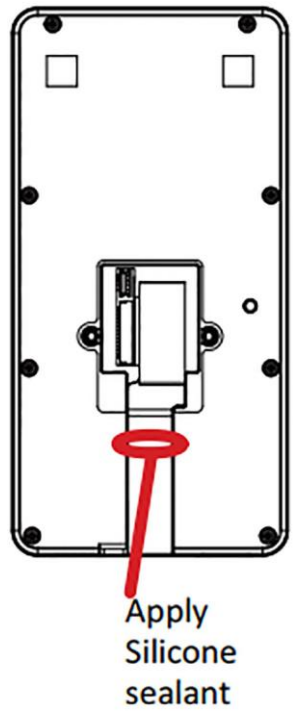


図 3-3 シリコーンシーラントの塗布

4. デバイスを取り付けプレートに合わせ、付属のネジ1本（SC-KM3X6-T10-SUSS）でデバイスをプレートに固定してください。

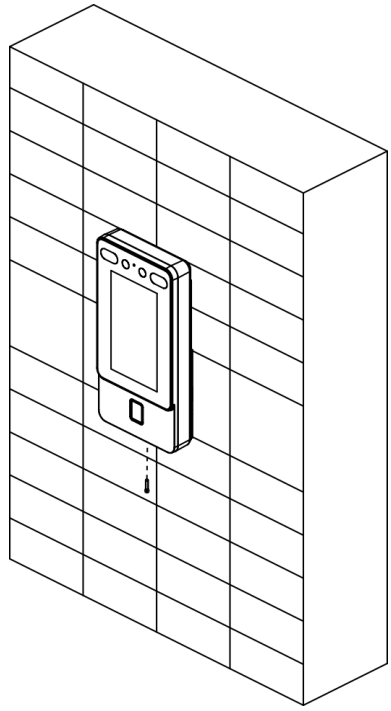


図 3-4 デバイスの固定

3.3 表面実装

手順

1. 取り付けテンプレートの基準線に従って、取り付けテンプレートを地面から 1.45 メートル高い壁またはその他の表面に貼り付けます。

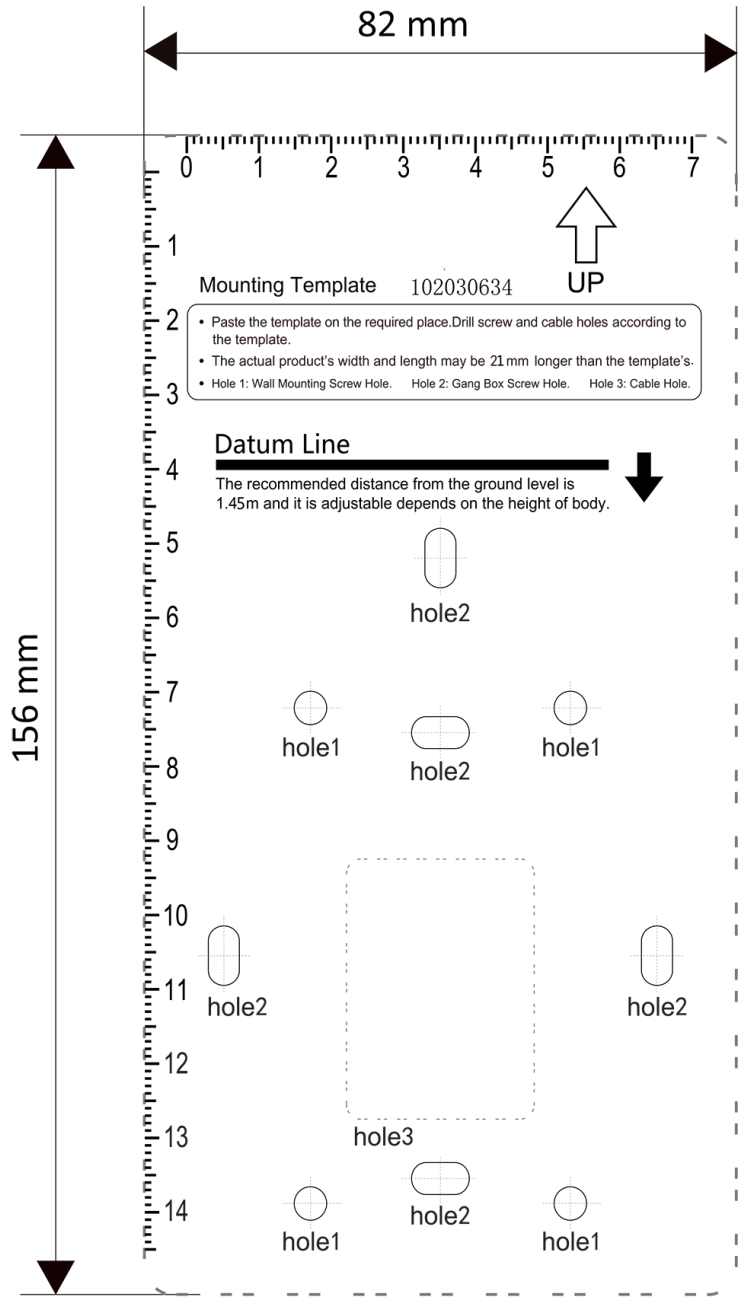


図 3-5 取り付けテンプレート

2. 取り付けテンプレートの穴 1 に従って、壁またはその他の表面に穴を開けます。

3. 拡張ボルトのプラスチック製スリーブを穴に挿入します。

4. 取り付け穴を取付プレートに合わせ、付属のネジ2本（KA4×22-SUS）で取付プレートを壁に固定してください。

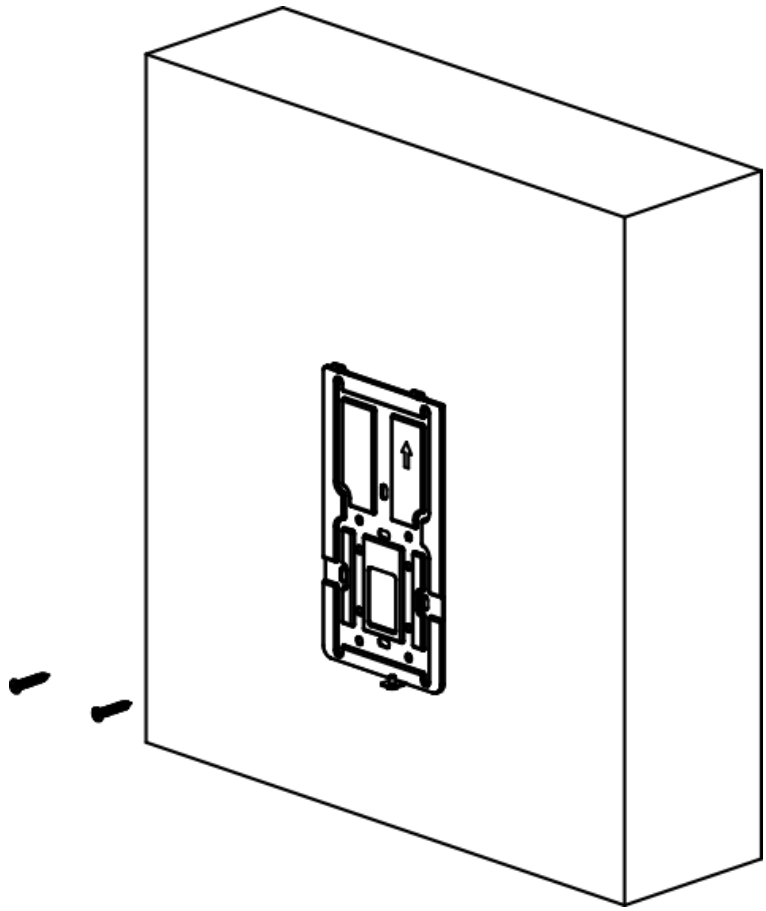


図3-6 取付プレートの取り付け

5. ケーブルを取付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。

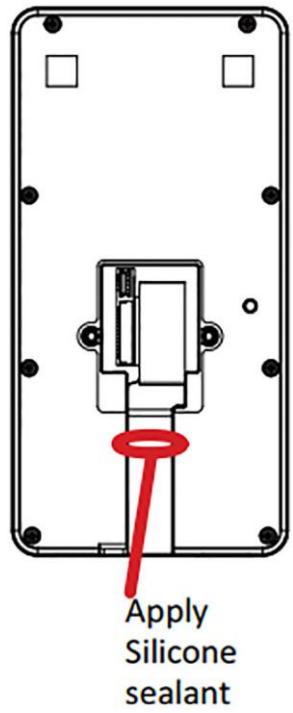


図 3-7 シリコーンシーラントの塗布

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。

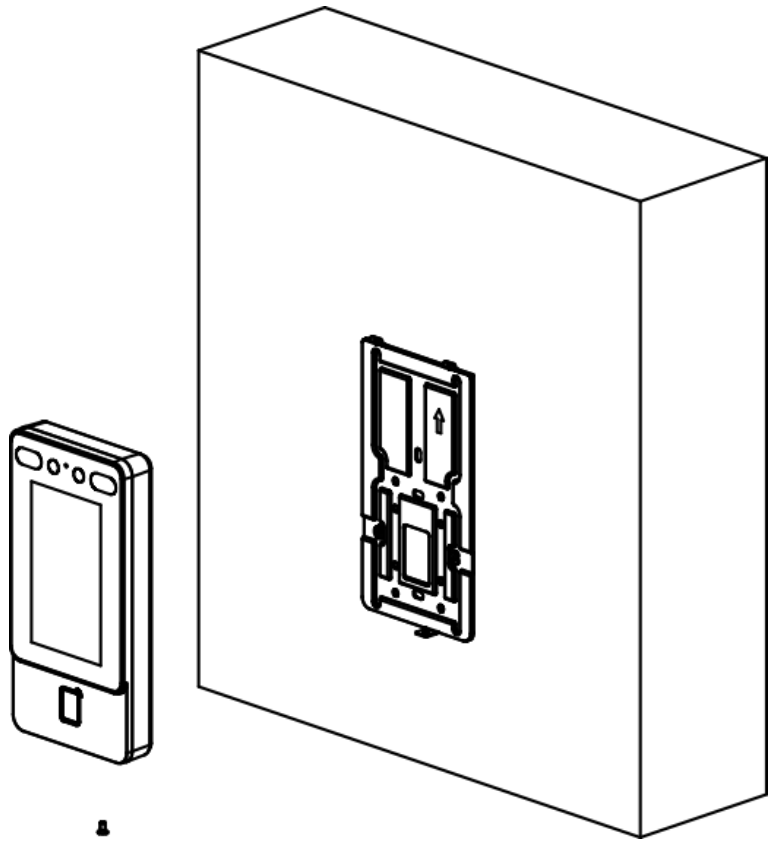


図3-8 デバイスの取り付け

7. 付属のネジ 1 本（KM3×6-SUS）を使用して、デバイスと取り付けプレートを固定します。

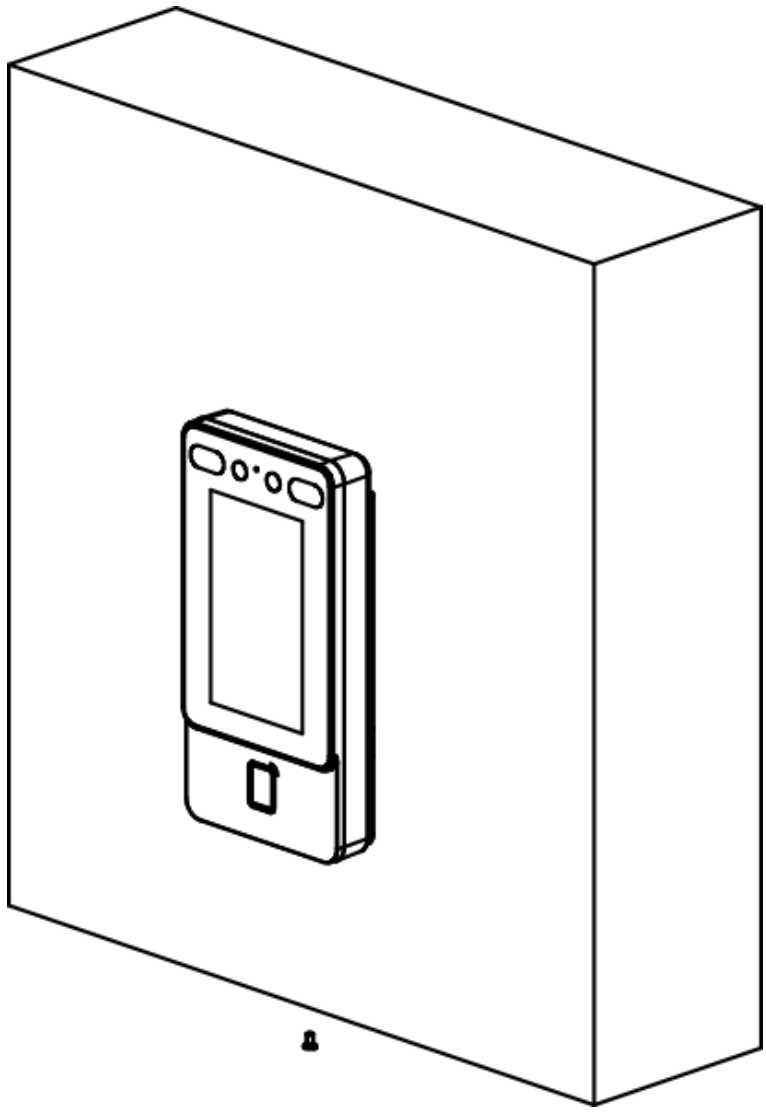


図 3-9 デバイスを固定する

注記

- 推奨設置高さは1.45メートルですが、必要に応じて設置高さを設定できます。
- 付属の取付プレートを使用することをお勧めします。

8. 設置後、本製品を正しく使用するため（屋外使用時）、画面に保護フィルム（付属モデルの一部）を貼付してください。

3.4 ブラケットによる取り付け

3.4.1 ブラケット取付前の準備

手順

1. 下図のように回転式改札機の表面に穴を開けます。防水ナットを取り付けます。

注意
リベットを押し込んだ後、はんだ付けして水の侵入を防ぎます。

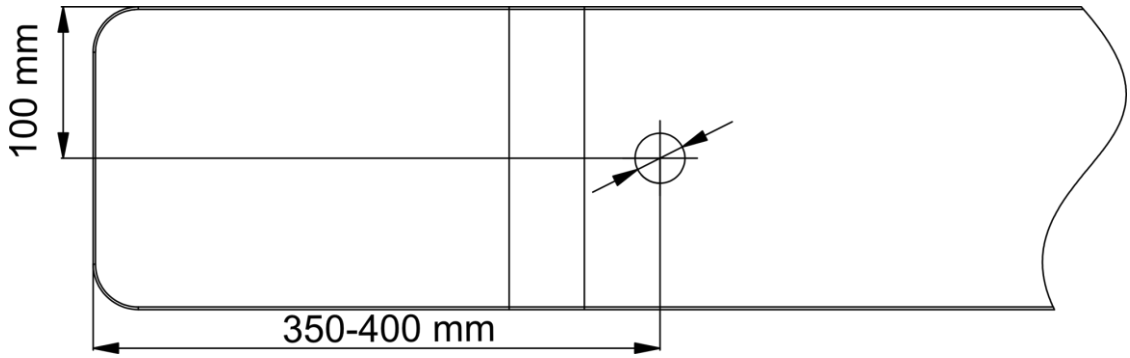


図 3-10 ターンスタイルへの穴あけ

2. ターンスタイル本体に対して180°垂直に設置する必要がある場合、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。

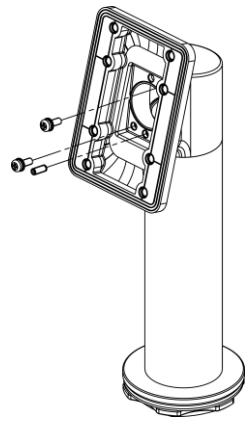


図3-11 ネジを外す

2) 固定部を180°回転させ、3本のネジを再度取り付けます。

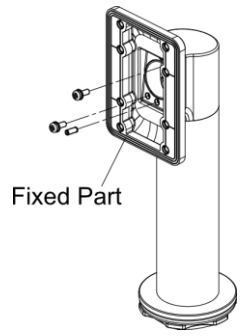


図 3-12 固定部の回転

3.4.2 取付ブラケット

取り付け手順

1. ターンスタイルにベースを取り付けます。

1) ターンスタイルの穴を合わせ、ベースをターンスタイルに設置します。

2) ベースを所定の位置に回転させ、装置が正しい方向を向くことを確認してください。

3) レンチでベースを固定してください。

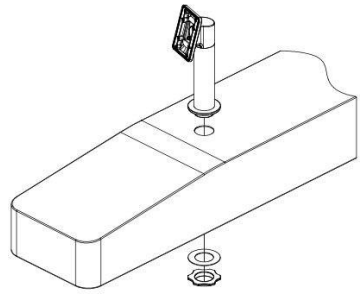


図 3-13 ベースの取り付け

注記

ターンスタイルの前面と背面にシリコンパッドを取り付けます。

2. 付属のネジ 4 本（SC-K1M4×6-SUS）で取り付けテンプレートをブラケットに取り付けます。

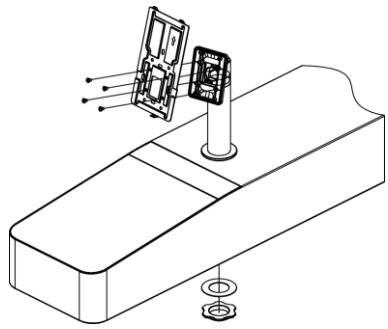


図 3-14 取付テンプレートの固定

3. ケーブルを回転式改札機のケーブル穴に通し、1本のSC-KM3×6-T10-SUSネジで装置を取り付けプレートに固定してください。

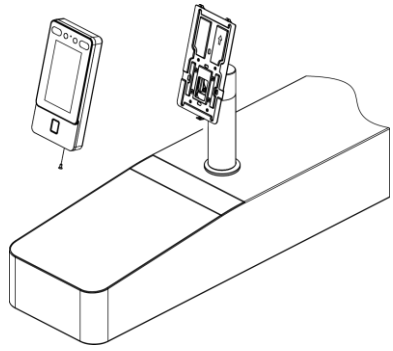


図3-15 装置の固定

4. 設置後、装置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）をスクリーンに貼り付けてください。

3.5 シリンダーブラケットによる取り付け

3.5.1 ブラケットによる取り付け前の準備

ターンスタイルに穴が開いていることを確認してください。穴が開いていない場合は、以下の手順に従って穴を開けてください。

手順

1. ターンスタイルの内側表面に補強板を取り付けるには、フランジナットで固定する4本のネジ（M3またはM4）を使用してください。

注意
回転式改札機と端部の距離は10mm以内にしてください。

2. 下図に従って回転式改札機の内側に穴を開け、防水ナットを取り付けます。

注記

リベットを押し込んだ後、水が侵入しないようはんだ付けしてください。

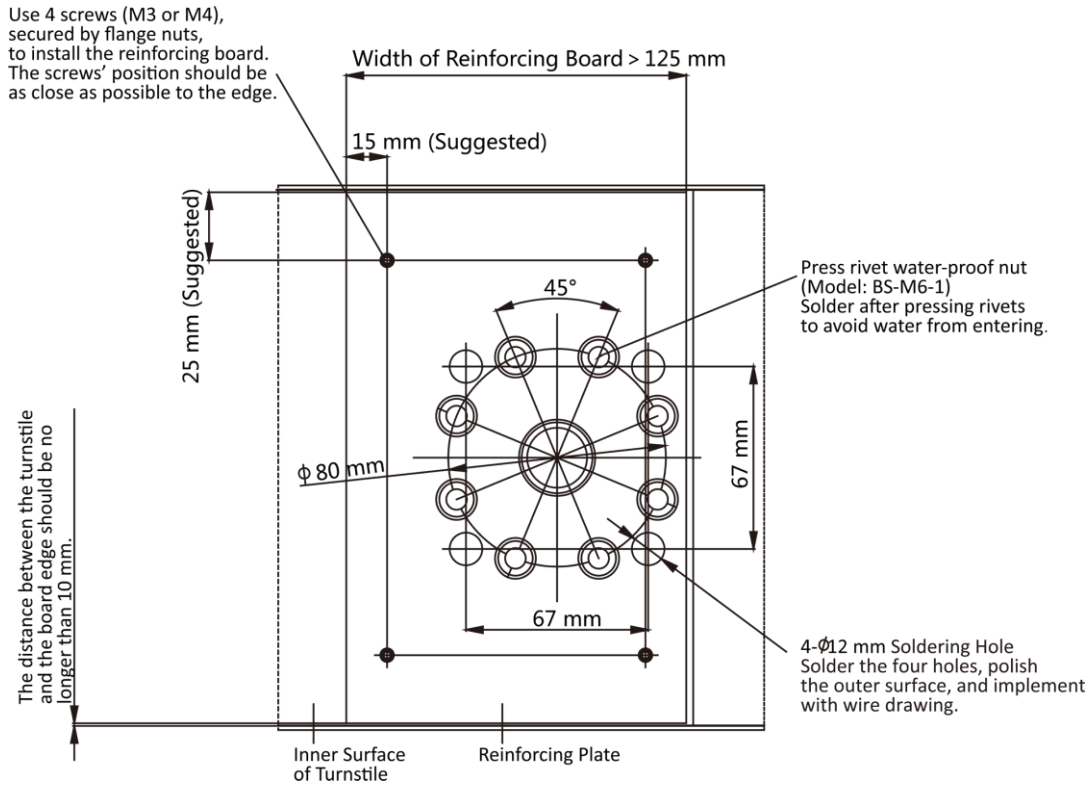


図 3-16 回転式改札機に穴を開ける

3. 残りの4つの穴をはんだ付けし、表面を研磨し、線引きを実施する。

4. 回転式改札機の内側表面に円形チューブをはんだ付けし、水の侵入を防ぐ。

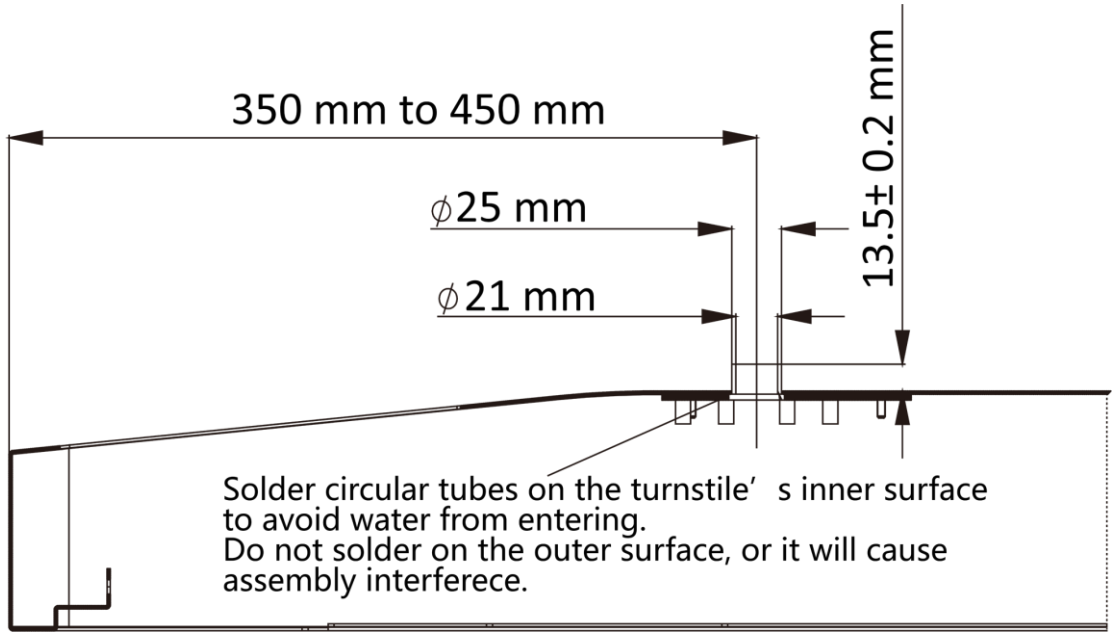


図3-17 チューブのはんだ付け

3.5.2 シリンダーブラケット取付

手順

1. ターンスタイルにベースを取り付ける。

1) ターンスタイルの穴を合わせ、ベースをターンスタイルに設置します。

2) ベースを所定の位置に回転させ、装置が正しい方向を向いていることを確認します。

3) ベースを4本のSC-OM6×12-H-SUSネジで固定してください。

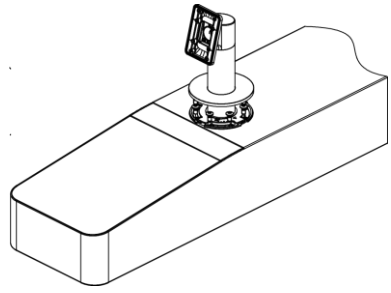


図3-18 ベースの取り付け

2. 取り付け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。

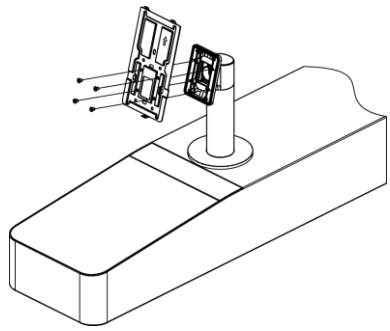


図 3-19 取付プレートの固定

3. ケーブルをターンスタイルのケーブル穴に通します。

4. 顔認識端末を 1 本の SC-KM3×6-H2-SUS ネジで取り付けプレートに固定します。

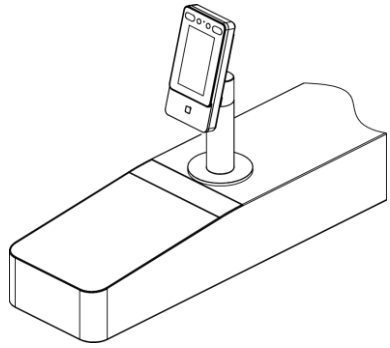


図 3-20 取付プレートの固定

5. 設置後、本機器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。

第4章 配線

RS-485端子をRS-485カードリーダーに接続し、NC/NO端子とCOM端子をドアロックに接続し、SEN端子とGND端子をドアコンタクトに接続し、BTN/GND端子を退出ボタンに接続し、Wiegand端子をアクセスコントローラに接続できます。

WIEGAND端子をアクセスコントローラに接続すると、顔認証端末は認証情報をアクセスコントローラに送信でき、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20m以内にしてください。
- ケーブルサイズが15AWGの場合、12V電源を使用してください。また、電源と機器間の距離は30m以内にしてください。
- ケーブルサイズが12AWGの場合、12V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。
- 外部カードリーダー、ドアロック、退出ボタン、ドア磁気センサーには個別電源が必要です。

4.1 端子説明

端子には電源入力、RS-485、ウィーガンド出力、ドアロックが含まれます。端子の説明は以下の通りです：

表 4-1 端子説明

グループ	No.	機能	色	名前	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	RS-485	黄色	485+	RS-485 配線
	B2		青	485-	
	B3		黒	GND	接地
グループ C	C1	ウィーガンド	緑	W0	ウィーガンド配線 0

グループ	番号	機能	色	名称	説明
	C2		白	W1	ウィーガンド配線 1
	C3		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	ボタン	出口ドア配線

4.2 配線 通常デバイス

端末は通常の周辺機器と接続できます。

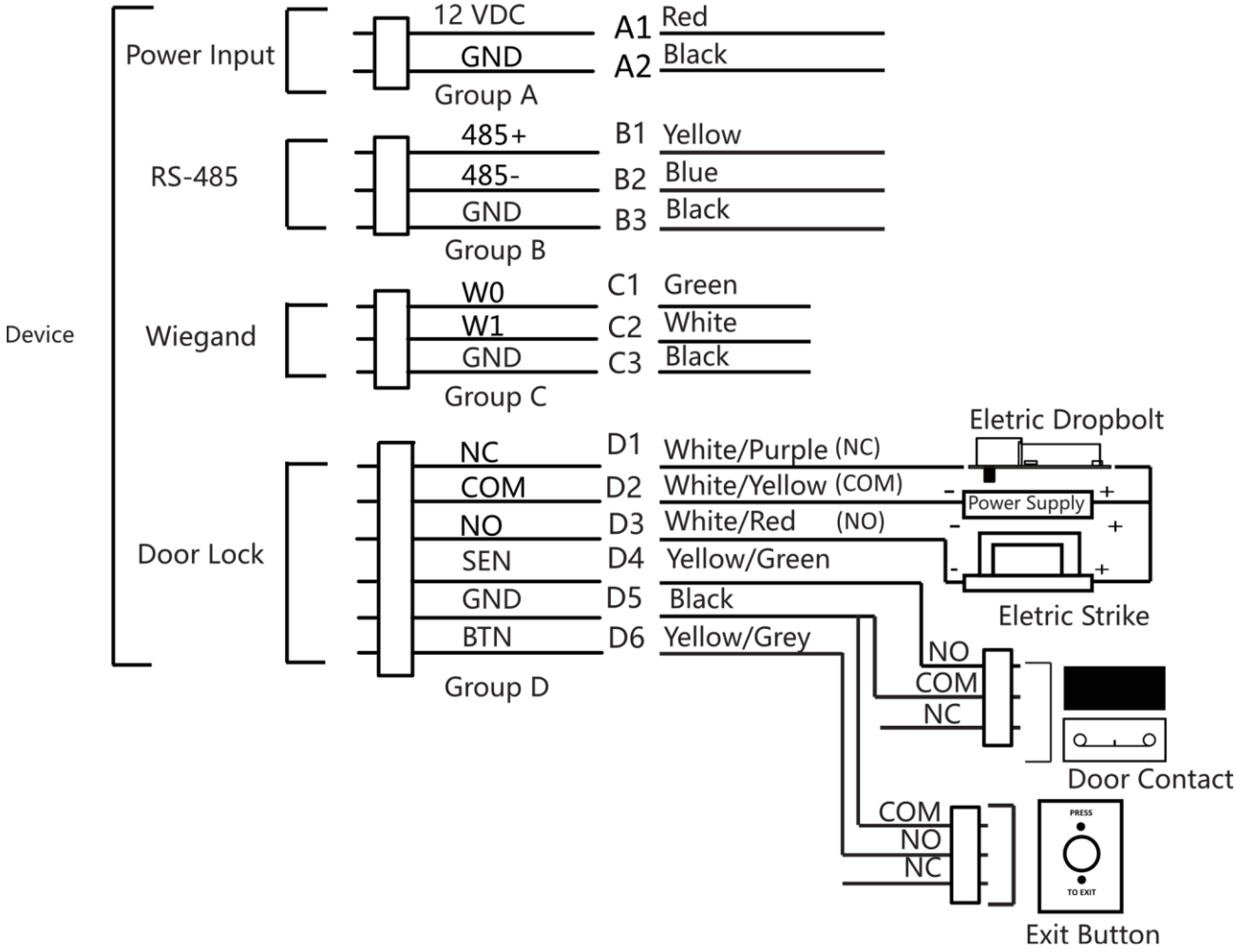


図4-1 デバイス配線

注記

- 顔認証端末のウィーガンド方向は、ウィーガンドカードリーダーに接続する場合は「**入力**」に設定してください。アクセスコントローラに接続する場合は、認証情報をアクセスコントローラに送信するため、ウィーガンド方向を「**出力**」に設定してください。
- Wiegand 方向の設定の詳細については、「***Wiegand パラメータの設定***」を参照してください。
- 本装置を電源に直接配線しないでください。

4.3 セキュアドア制御ユニットの配線

端末をセキュアドア制御ユニットに接続できます。配線図は以下の通りです。

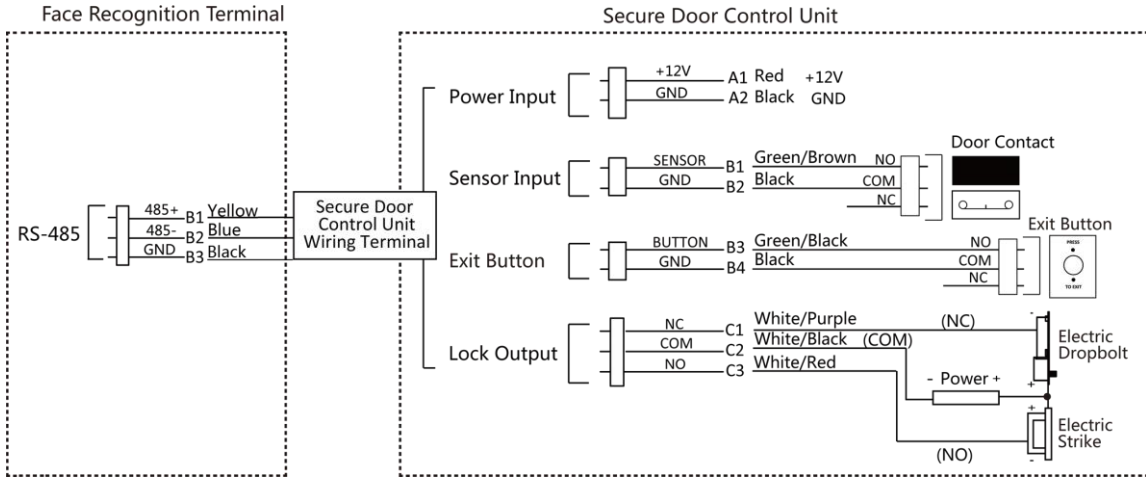


図4-2 セキュアドア制御ユニットの配線

注記

セキュアドア制御ユニットは、外部電源に別途接続する必要があります。推奨される外部電源は12V、0.5Aです。

4.4 ワイヤー火災モジュール

4.4.1 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（常時閉）

セキュリティタイプ：電源オフ時にドアが開く

シナリオ：消防車アクセス用として設置

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する。

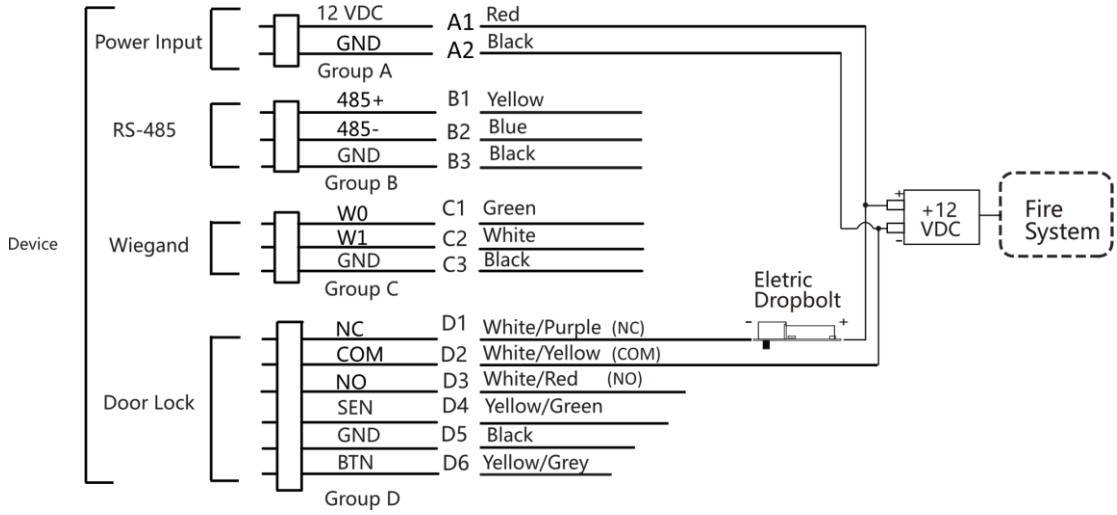


図 4-3 配線デバイス

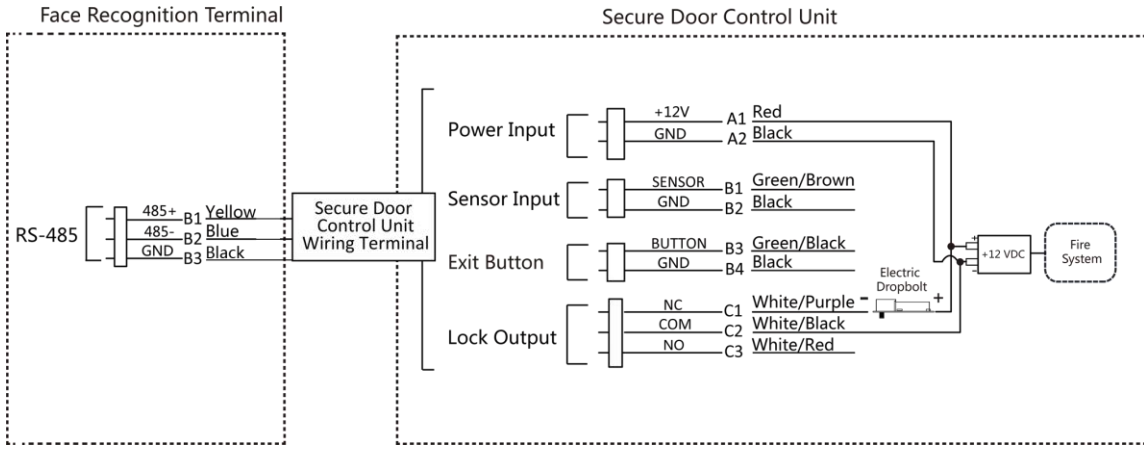


図4-4 ワイヤー式ドア制御ユニット

タイプ2

注記

火災システム（NOおよびCOM、電源オフ時は通常開）は、ロックと電源を直列に接続します。火災警報が作動すると、ドアは開いたままになります。通常時は、NOとCOMは閉じています。

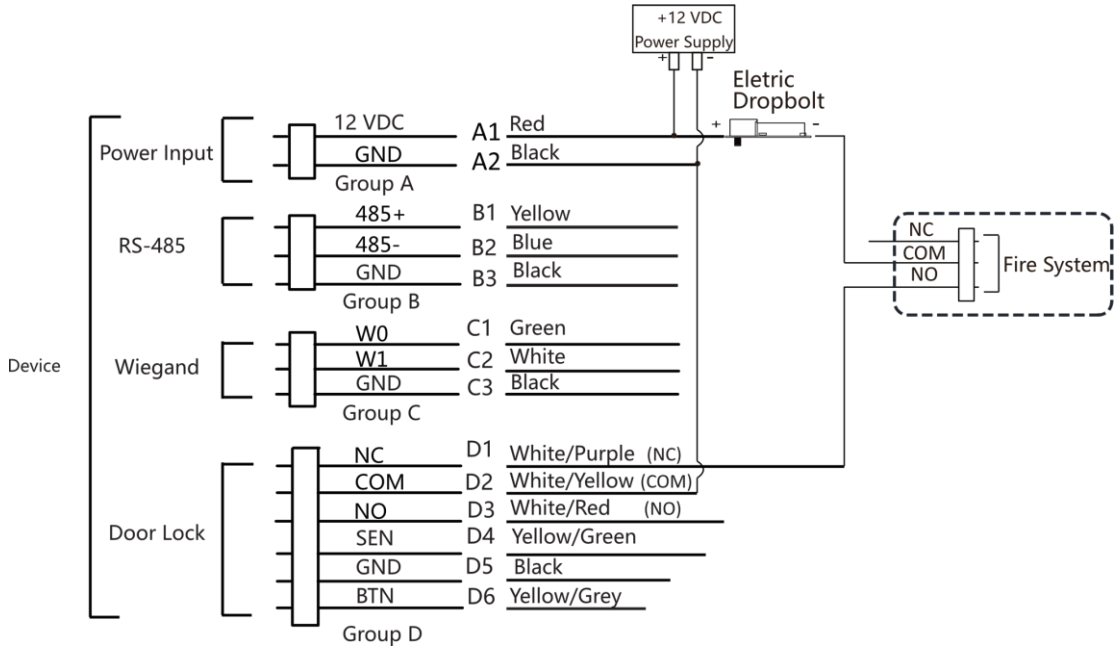


図4-5 配線装置

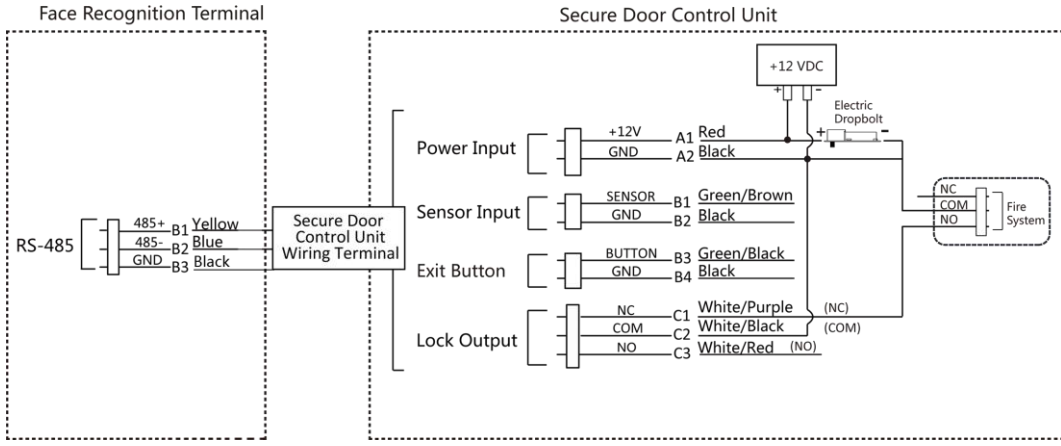


図4-6 配線 セキュアドア制御ユニット

4.4.2 電源オフ時にドアがロックされる配線図

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。

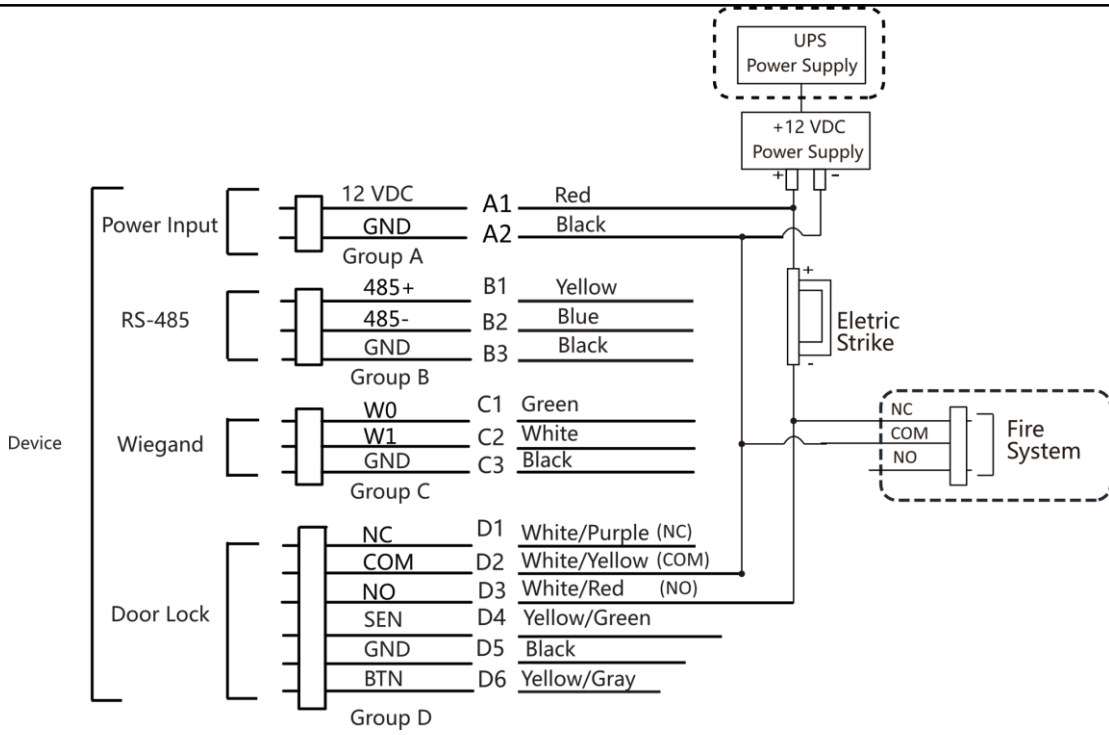


図4-7 装置配線図

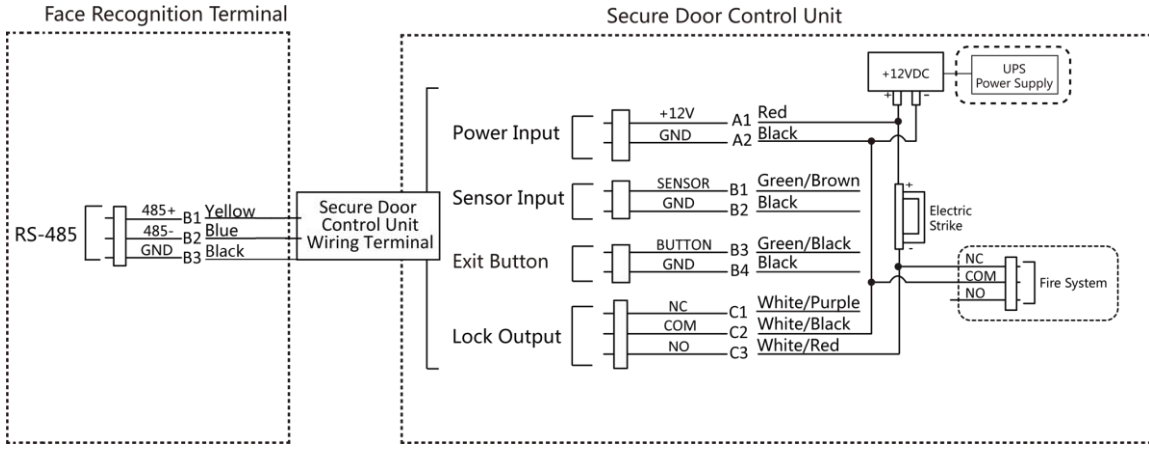


図4-8 配線図

第5章 アクティベーション

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

5.1 デバイス経由でアクティベート

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

「デバイスのアクティベート」ページでパスワードを作成し、確認してください。「**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。

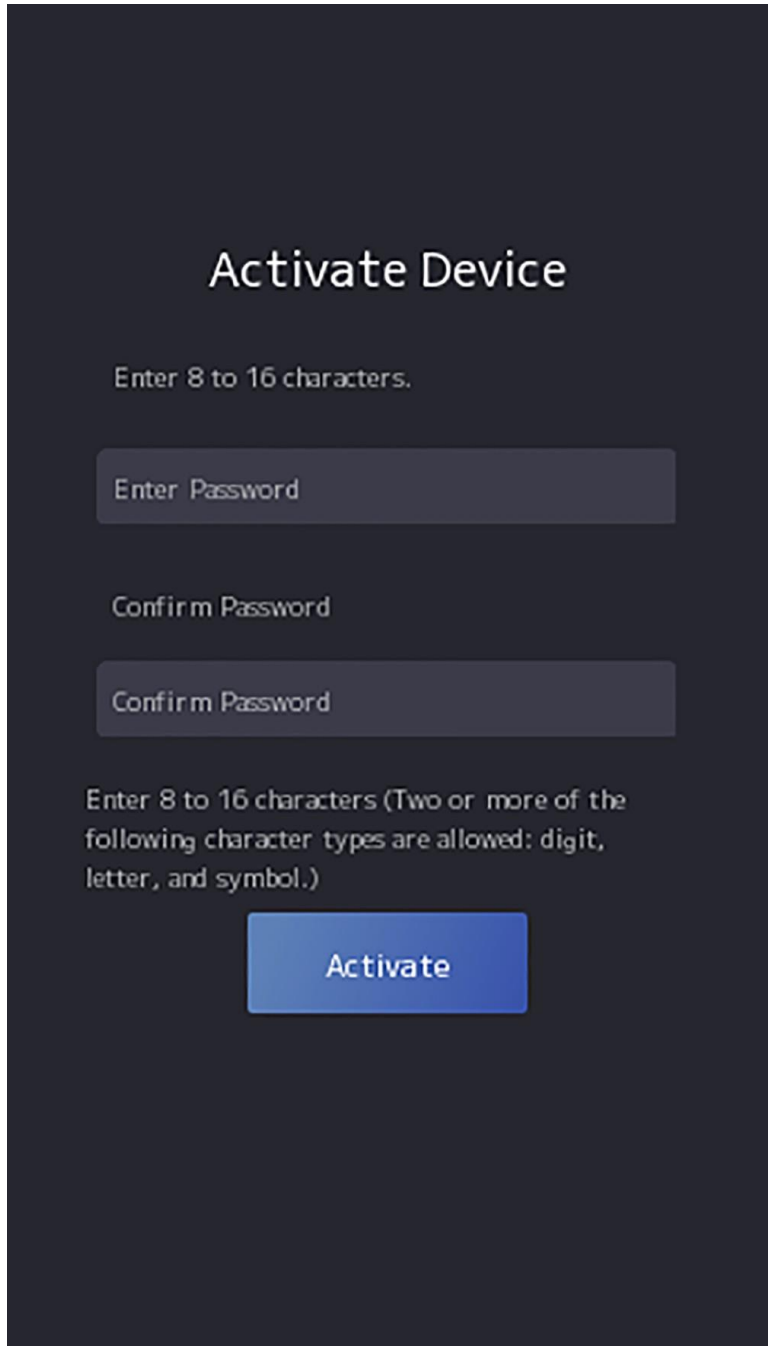


図5-1 アクティベーション画面

注意

デバイスのパスワードの強度については、自動的にチェックすることができます。ご自身で選択したパスワード（最低 8 文字以上、少なくとも

製品のセキュリティ強化のため、パスワードには以下の3種類のカテゴリ（大文字、小文字、数字、特殊文字）を含めることを推奨します。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です。

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、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（大文字小文字区別なし）、4つ以上の連続した昇順/降順の数字、または4つ以上の連続した同一文字。
- 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（大文字小文字は区別しません）。

- アクティベーション後、実際のニーズに応じて言語を選択してください。
- アクティベーション後、アプリケーションモードを選択してください。詳細はを参照してください。
- アクティベーション後、ネットワークを設定する必要があります。詳細は「***ネットワークパラメータの設定***」を参照してください。
- アクティベーション後、デバイスをプラットフォームに追加できます。詳細は「***プラットフォームへのアクセス***」を参照してください。
- アクティベーション後、プライバシー設定が必要な場合は該当項目を確認してください。詳細は「***プライバシー設定***」を参照してください。
- アクティベーション後、デバイスパラメータを管理する管理者追加が必要な場合は、管理者設定を行ってください。詳細は「***管理者の追加***」を参照してください。

5.2 Webブラウザ経由でのアクティベーション

Webブラウザ経由でデバイスをアクティベートできます。

手順

1. ウェブ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

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が自動的にチェックされます。製品のセキュリティを強化するため、お客様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. **[Activate（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。

5.3 SADP によるアクティベート

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。

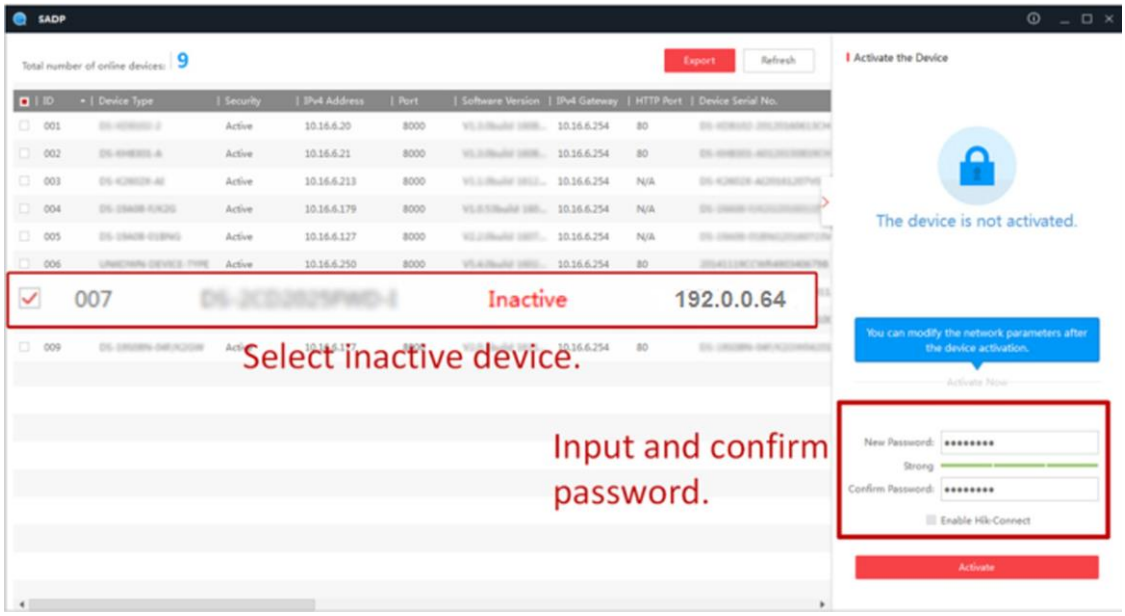
注意

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）を設定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。

注意

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。

5.4 iVMS-4200 クライアントソフトウェアによるデバイスのアクティベート

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的に確認できます。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、設置業者および／またはエンドユーザーの責任となります。

注意

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有効にします。

第6章 クイック操作

6.1 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ト後、デバイスシステムの言語を選択できます。

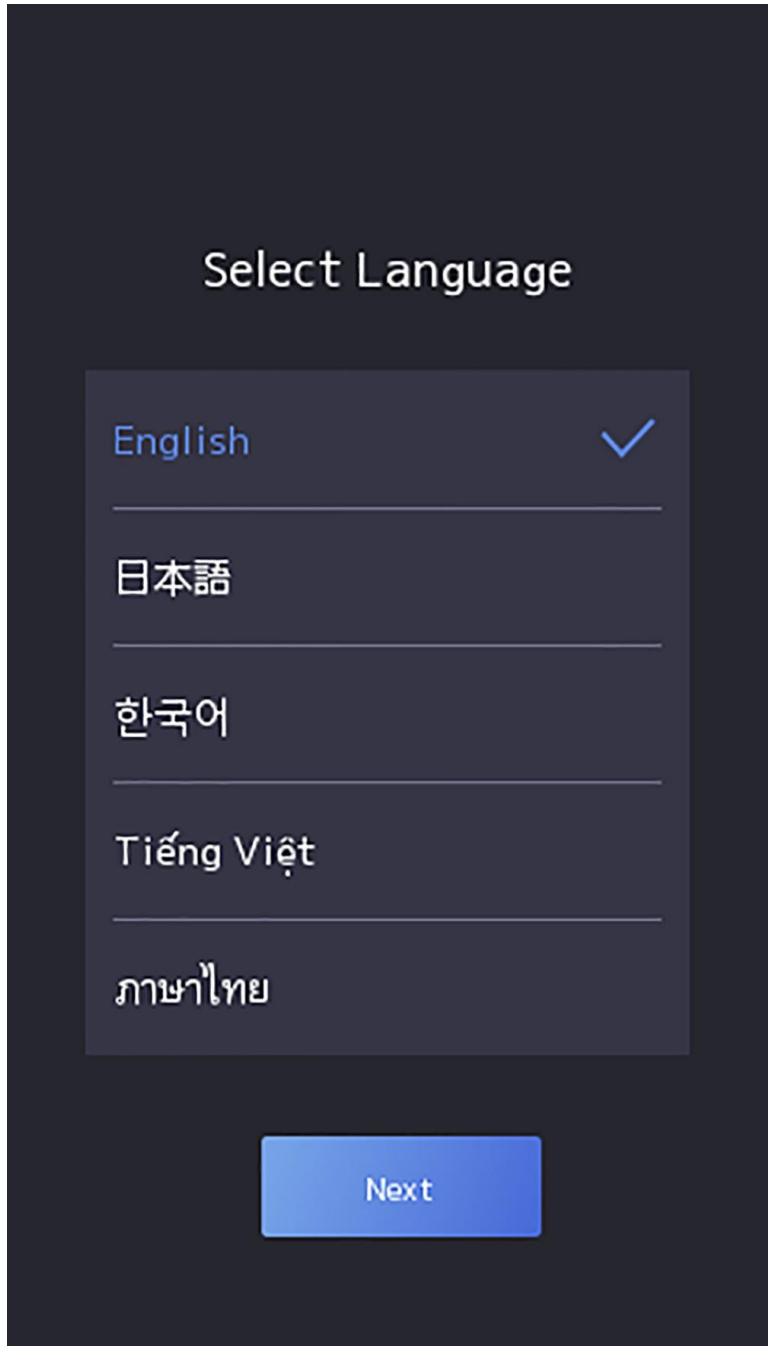


図 6-1 システム言語の選択

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。

6.2 パスワード変更タイプを設定

デバイスをアクティベートした後、パスワード変更方法を登録済みメールアドレスまたはセキュリティ質問に設定できます。デバイスパスワードを忘れた場合、選択した変更方法を通じてパスワードを変更できます。

メールアドレスによるパスワード変更

登録済みメールアドレス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

セキュリティ質問でパスワードを変更する場合は、「**セキュリティ質問に変更」を**タップしてください。

右上の角にあるセキュリティ質問を選択し、回答を入力してください。**次に進む**をクリックしてください。

注記

パスワード変更には**1**つのタイプのみ選択可能です。必要に応じて、両方の変更タイプを設定するウェブページにアクセスできます。

6.3 ネットワークパラメータの設定

アクティベーション後、アプリケーションモードを選択すると、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. ネットワーク選択ページに入ったら、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。

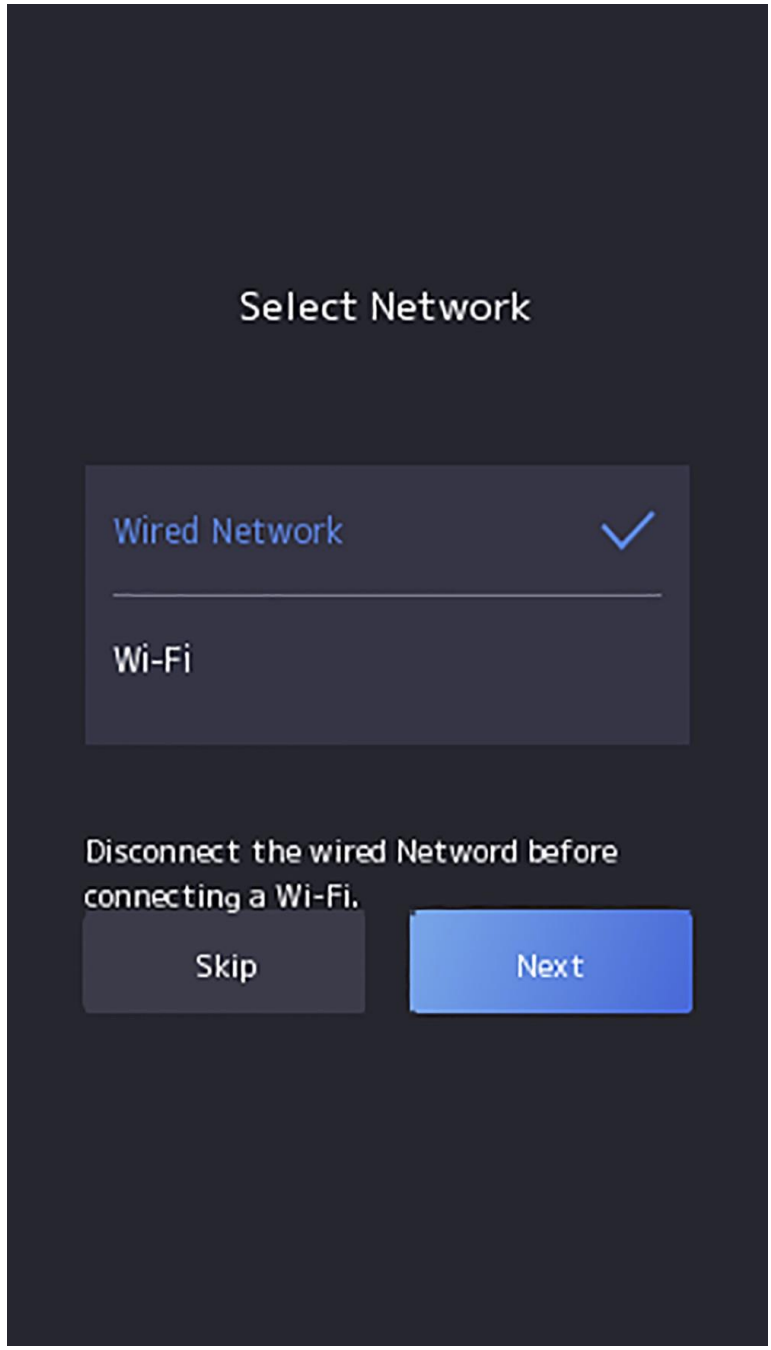


図6-2 ネットワークの選択

注記
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]** をタップします。**有線ネットワーク**

注意

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てください。

または「**Wi-Fiを追加**」をタップし、Wi-Fiの名前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。

6.4 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 および認証コードを設定します。

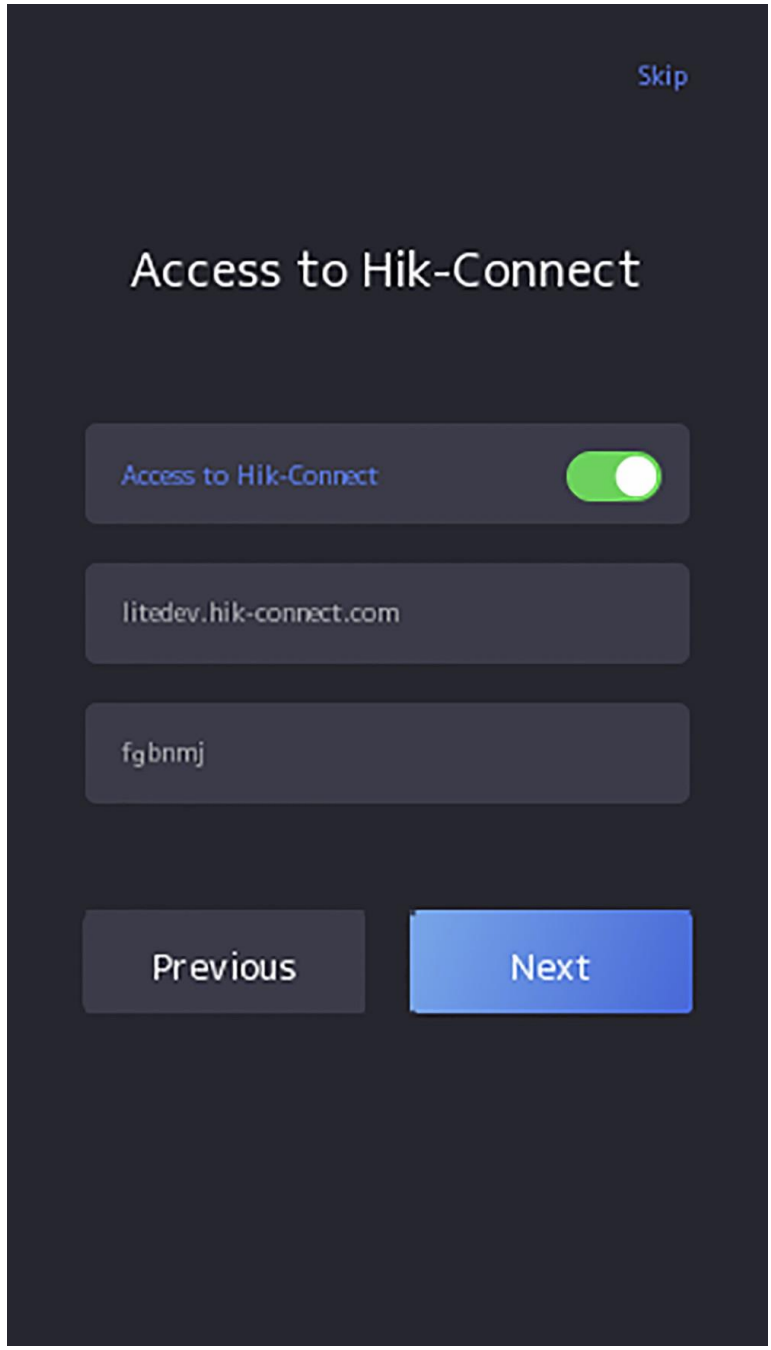


図 6-3 Hik-Connect へのアクセス

2. **「次へ」**をタップします。

注

前の画面に戻るには**「戻る」を**タップしてください。Wi-Fi設定ページに戻る場合、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アクセスする必要があります。

6.5 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

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。

登録画像保存

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、接続されたカメラで撮影した画像を端末に保存できます。

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。

設定を完了するには「**次へ**」をタップしてください。

6.6 管理者設定

デバイスのアクティベーション後、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、管理者追加を省略できます。
2. 管理者の名前を入力（任意）し、「**次へ**」をタップします。

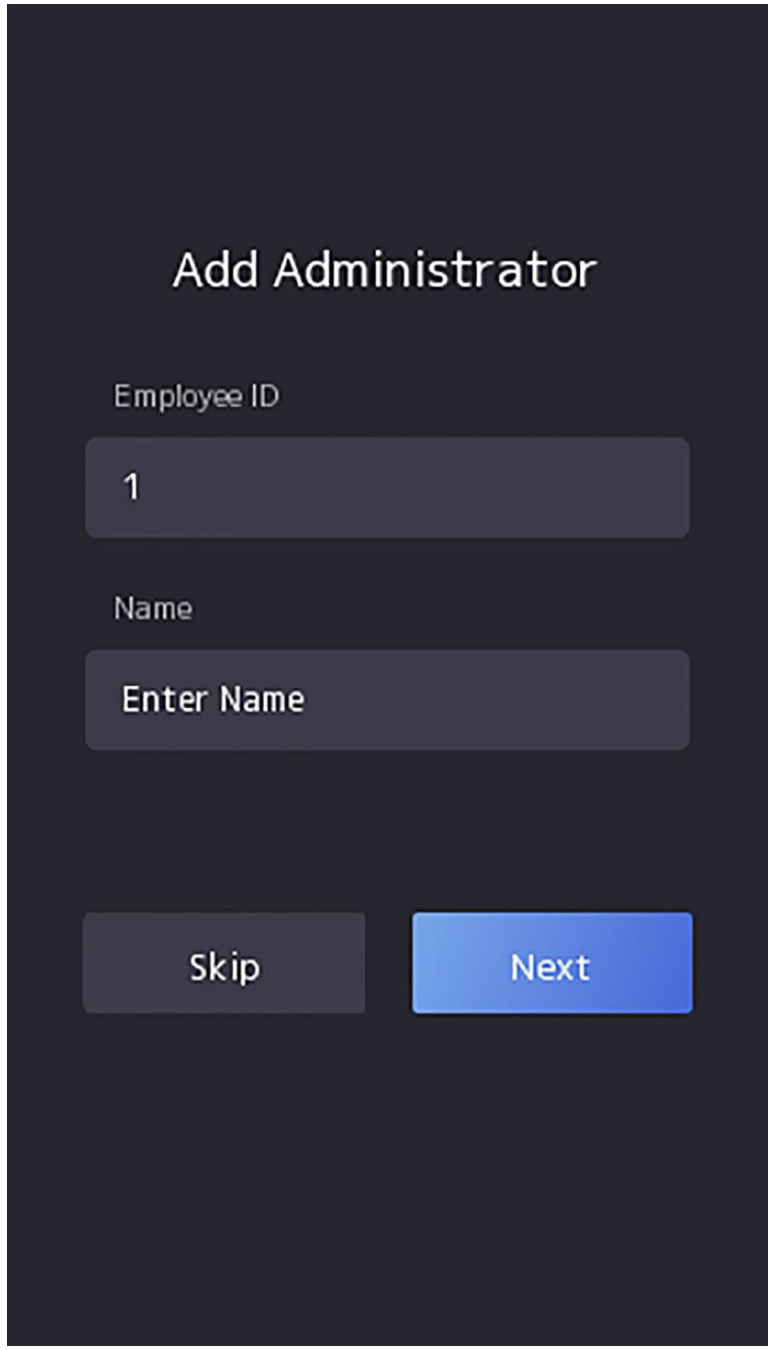


図6-4 管理者追加ページ

3. 追加する認証情報を選択します。

注

認証情報は最大1つまで追加してください。

- : 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ます。
- : 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、カードをカード提示エリアに提示してください。**OK**をクリックしてください。

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。

ステータスアイコンの説明

/

装置が武装状態/非武装状態です。

/

Hik-Connectが有効/無効です。

/ /

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Wi-Fiは有効化され接続済み/未接続/有効化済みだが未接続です。

ショートカットキーの説明

注記

画面に表示されているショートカットキーを設定できます。詳細は***基本設定を***参照してください。

- デバイスルーム番号を入力し、**OK**をタップして呼び出します。
- をタップしてセンターに呼び出します。

注意

センターにデバイスが追加されていない場合、発信操作は失敗します。

認証用の PIN コードを入力してください。

第7章 基本操作

7.1 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。

7.1.1 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、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、管理者ログイン画面に入ります。

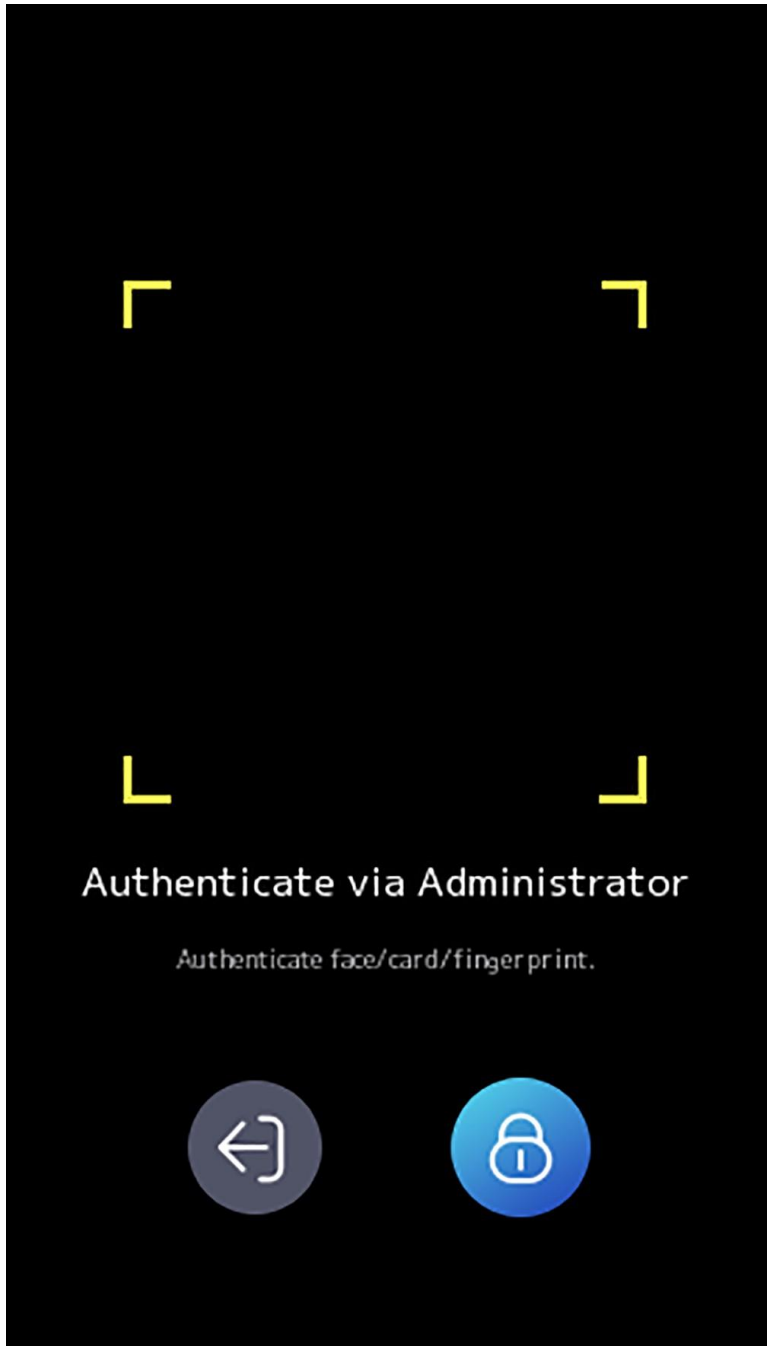


図7-1 管理者ログイン

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。

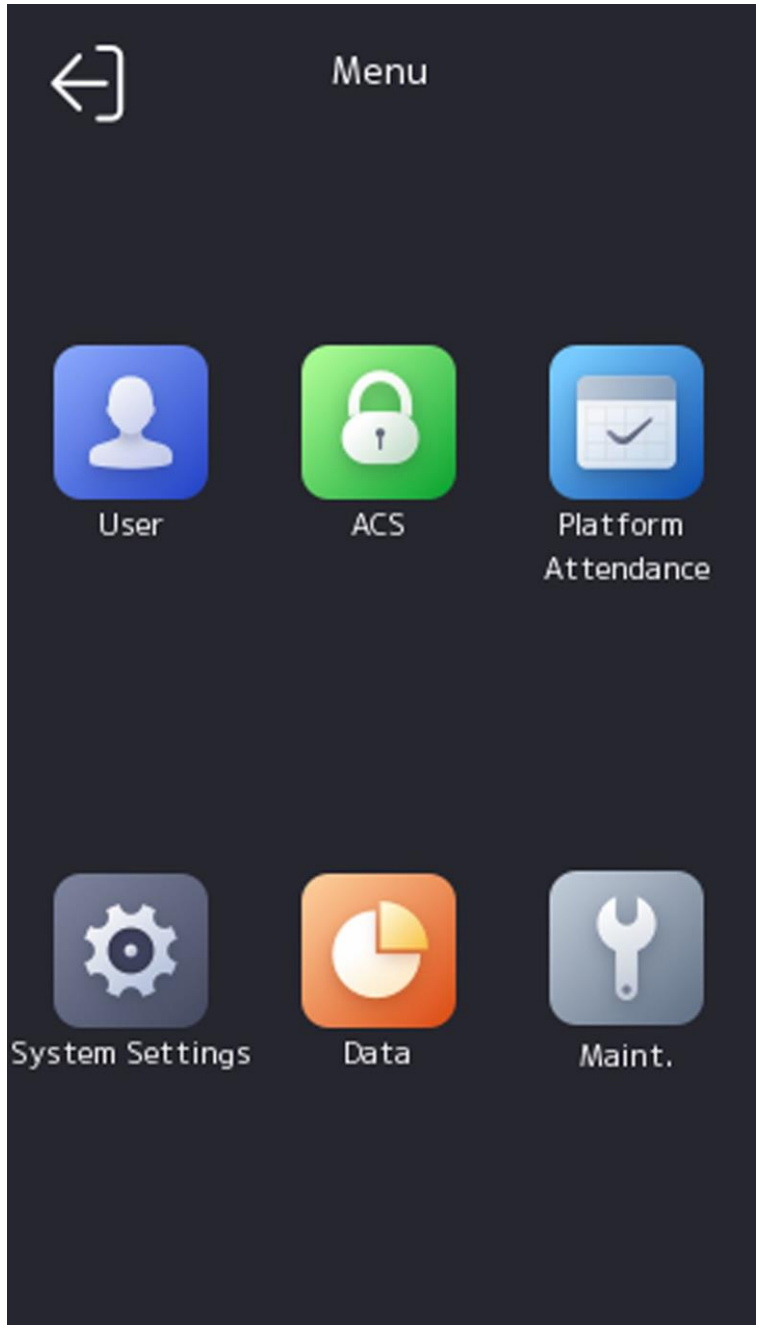


図 7-2 ホームページ

注記
指紋またはカード認証が5回連続で失敗すると、デバイスは30分間ロックされます。

3. **オプション：**タップをタップすると、ログイン用のデバイス起動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。

7.1.2 アクティベーション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. 最初のページを3秒間長押しし、ジェスチャーに従って左/右にスライドすると、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。

注記

パスワードの入力に5回失敗すると、デバイスは30分間ロックされます。

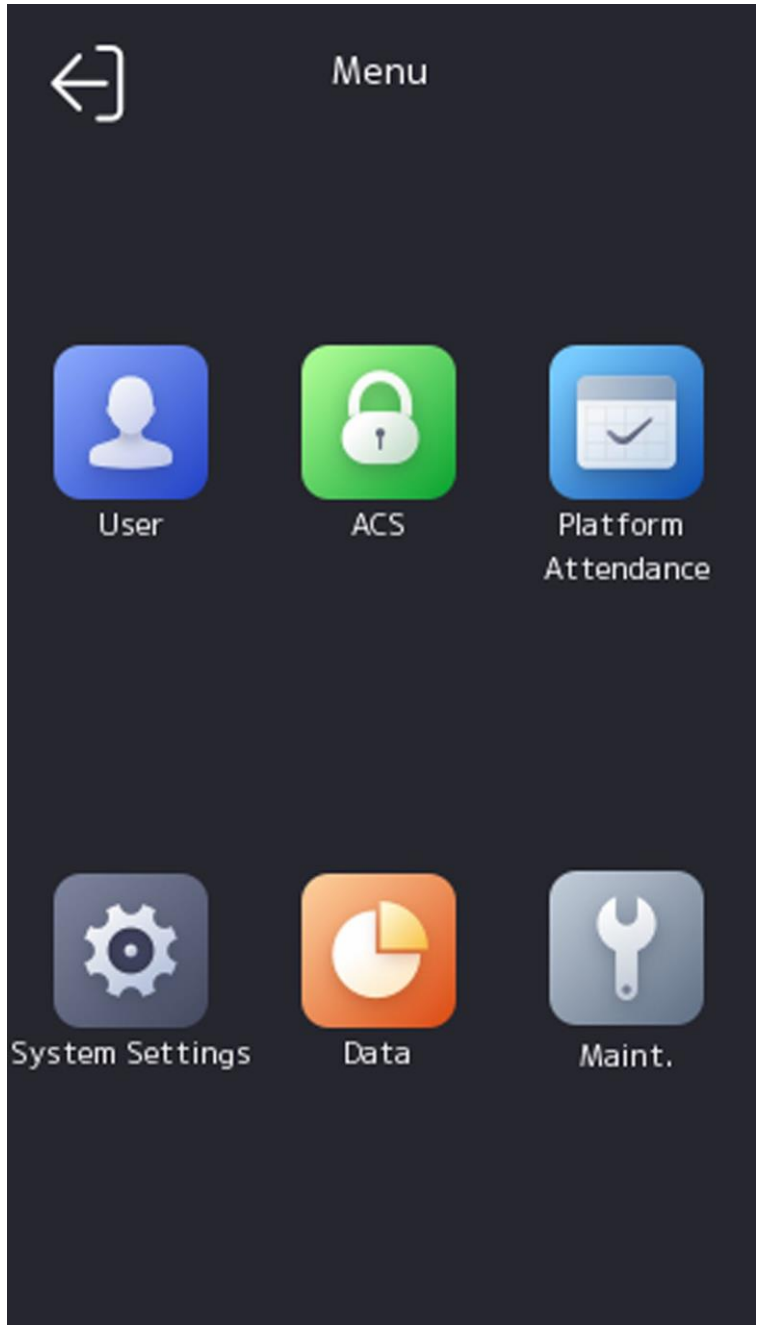


図7-3 ホームページ

7.1.3 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、パスワードを変更できます。

手順

1. 初期ページを3秒間押し続け、ジェスチャーに従って左/右にスライドし、ログインページに進みます。
2. **オプション：**管理者設定がある場合、ポップアップ表示される管理者認証ページで「  」をタップします。
3. **パスワードを忘れた**場合は、
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、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。
   - セキュリティの質問： アクティベーション時に設定したセキュリティの質問に答えてください。
   - 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、認証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. デバイス画面に認証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。

7.2 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。

7.2.1 有線ネットワークパラメータの設定

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

手順

1. ホーム画面で、**[システム設定] →** [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、**「有線ネットワーク」**をタップします。

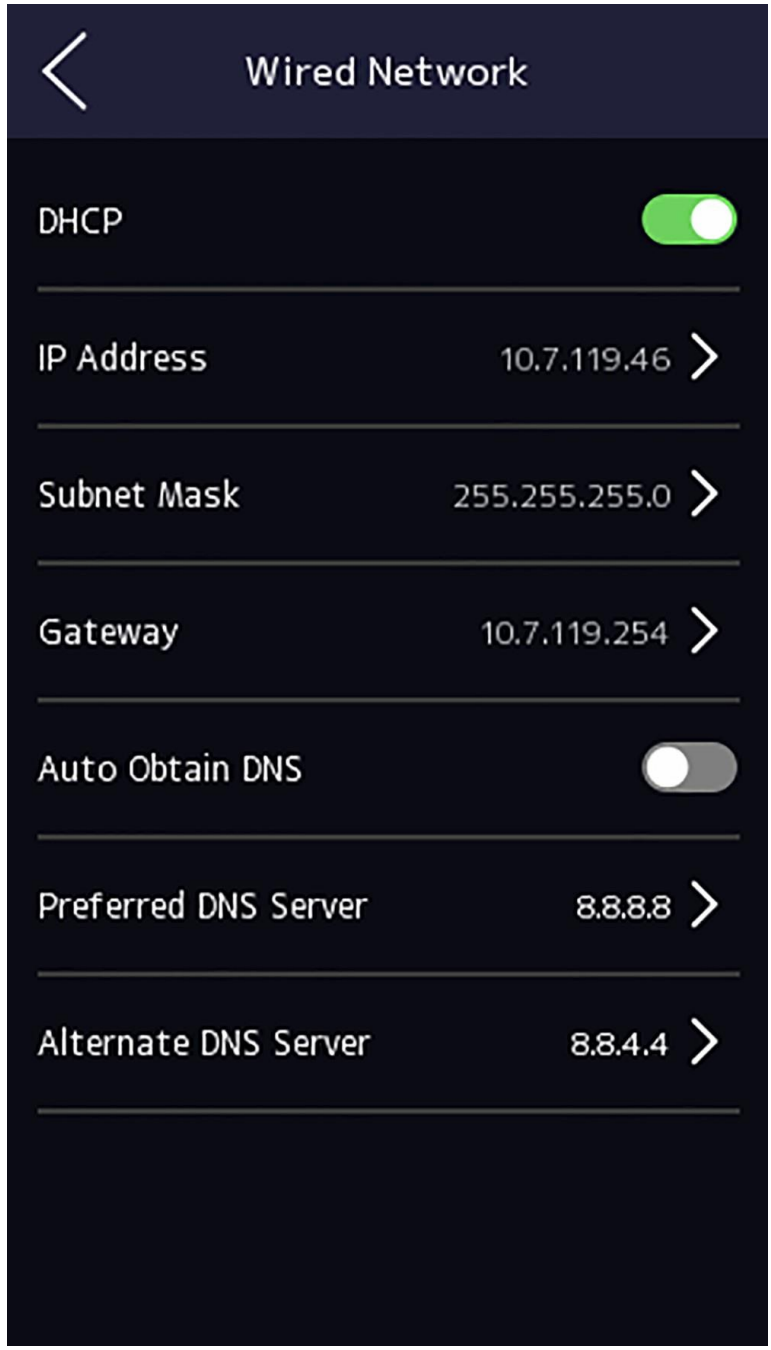


図 7-4 有線ネットワーク設定

3. IP アドレス、サブネットマスク、ゲートウェイを設定します。

- **DHCPを**有効にすると、システムが自動的にIPアドレス、サブネットマスク、ゲートウェイを割り当てます。
- **DHCPを**無効にし、IPアドレス、サブネットマスク、ゲートウェイを手動で設定してください。

注意

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セグメント内にある必要があります。

4. DNS パラメータを設定します。**DNS の自動取得を**有効にしたり、優先 DNS サーバーや代替 DNS サーバーを設定したりできます。

7.2.2 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

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. ホーム画面で［**システム設定**］→［通信設定］をタップし、通信設定画面に入ります。
2. 通信設定ページで、をタップします。

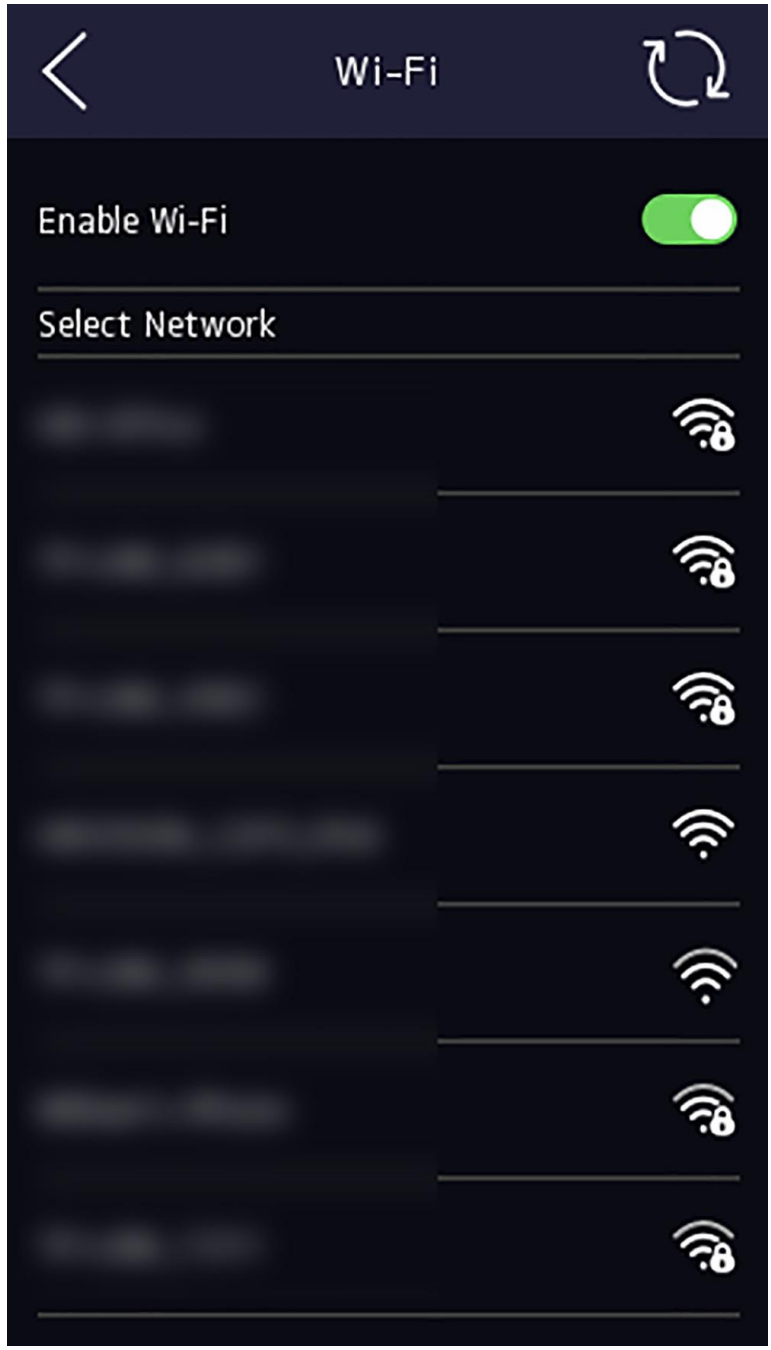


図 7-5 Wi-Fi 設定

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、特殊文字のみ使用できます。

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**タップします。

7. をタップしてネットワークパラメータを保存します。

7.2.3 RS-485 パラメータの設定

顔認識端末は、RS-485端子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、またはカードリーダーに接続できます。

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、**RS-485** をタップして RS-485 タブに入ります。

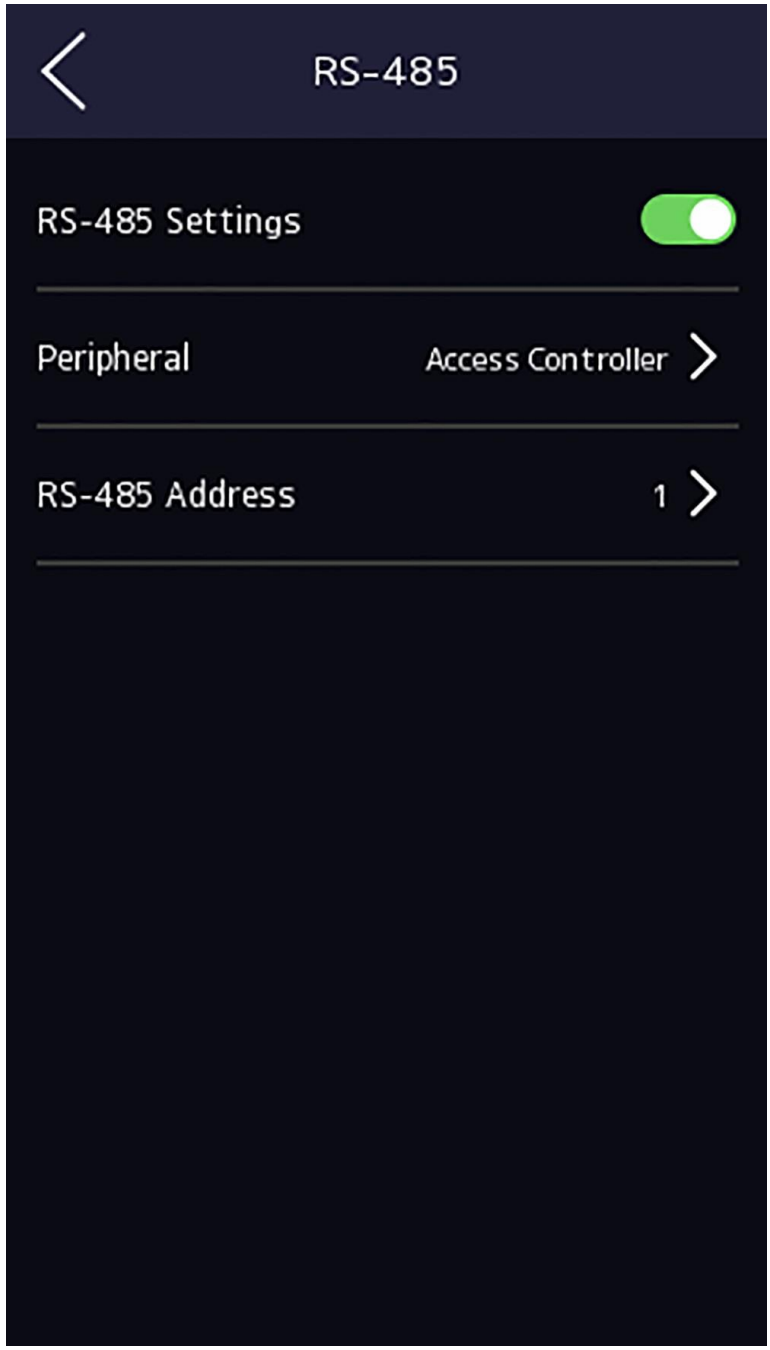


図 7-6 RS-485 パラメータの設定

3. 実際のニーズに応じて周辺機器タイプを選択します。

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 に設定します。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 アドレスを設定します。

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

7.2.4 Wiegandパラメータの設定

Wiegand 伝送方向を設定できます。

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て、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。

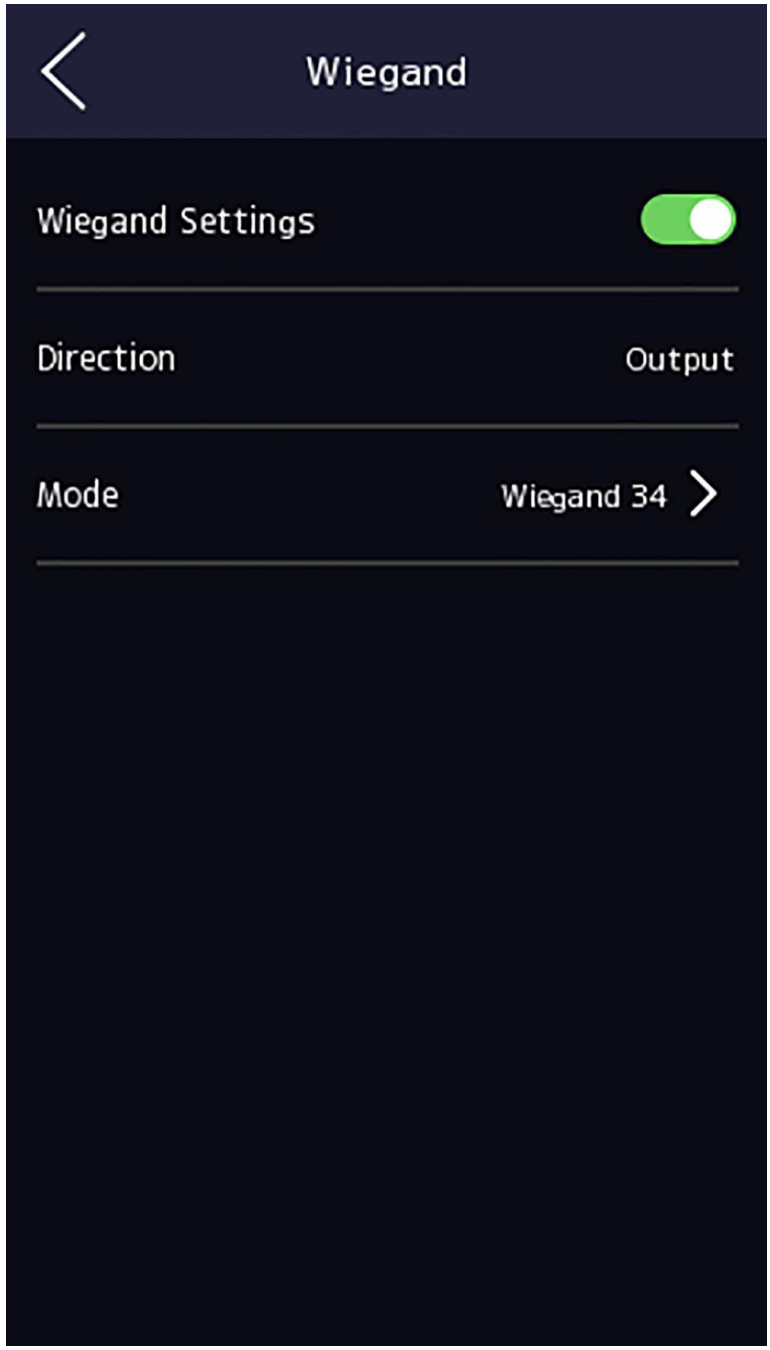


図 7-7 ウィーガンド設定

3. Wiegand 機能を有効にします。
4. Wiegand モードを選択します。
   - 出力：顔認証端末は外部アクセス制御装置に接続可能です。両デバイスはWiegand 26またはWiegand 34経由でカード番号を送信します。
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。

7.2.5 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. ホーム画面で**システム設定 → 通信 → ISUP**（通信設定）をタップして設定画面に入ります。

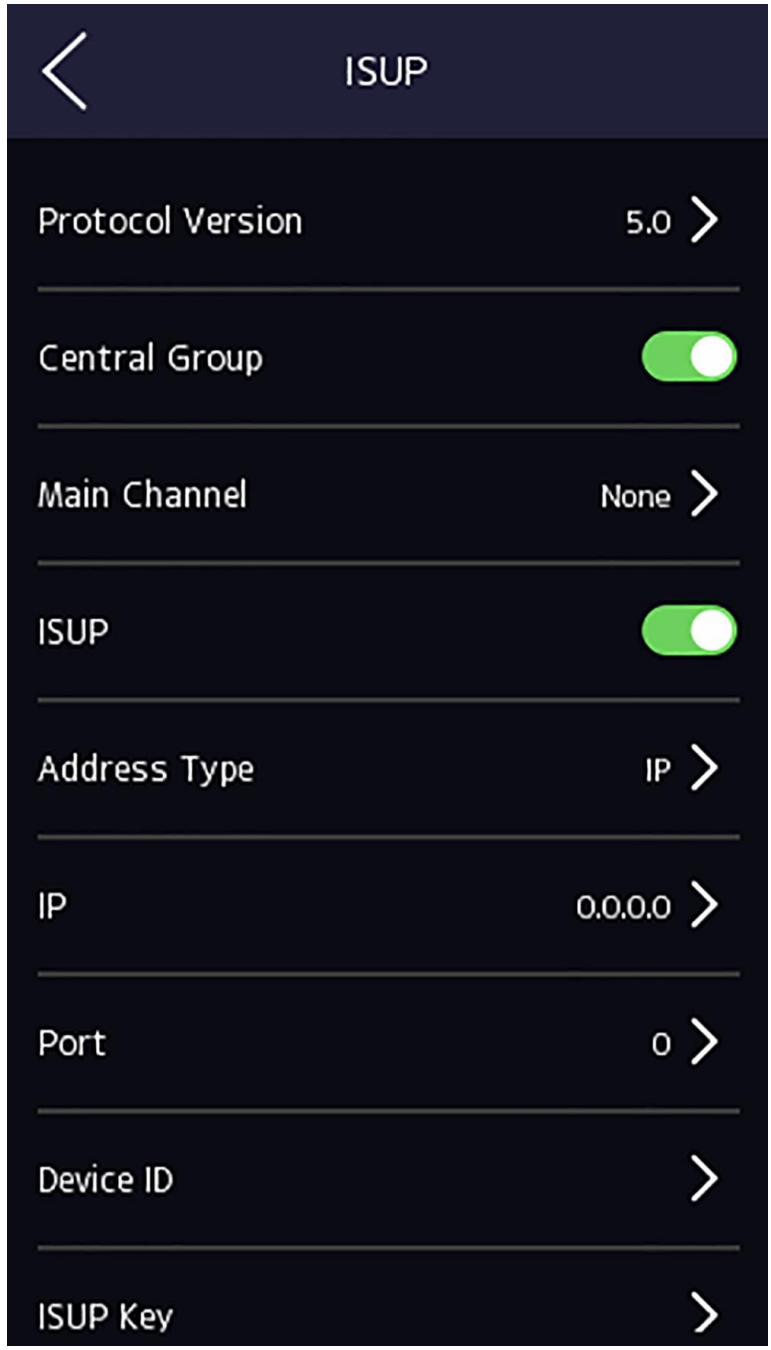


図7-8 ISUP設定

2. ISUP機能を有効にし、ISUPサーバーの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ます。

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 EHome 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します。

注

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キー範囲：8～32文字。

7.2.6 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、デバイス検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

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、「**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。

7.2.7 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。

7.3 ユーザー管理

ユーザー管理インターフェースでは、ユーザーの追加、編集、削除、検索が可能です。

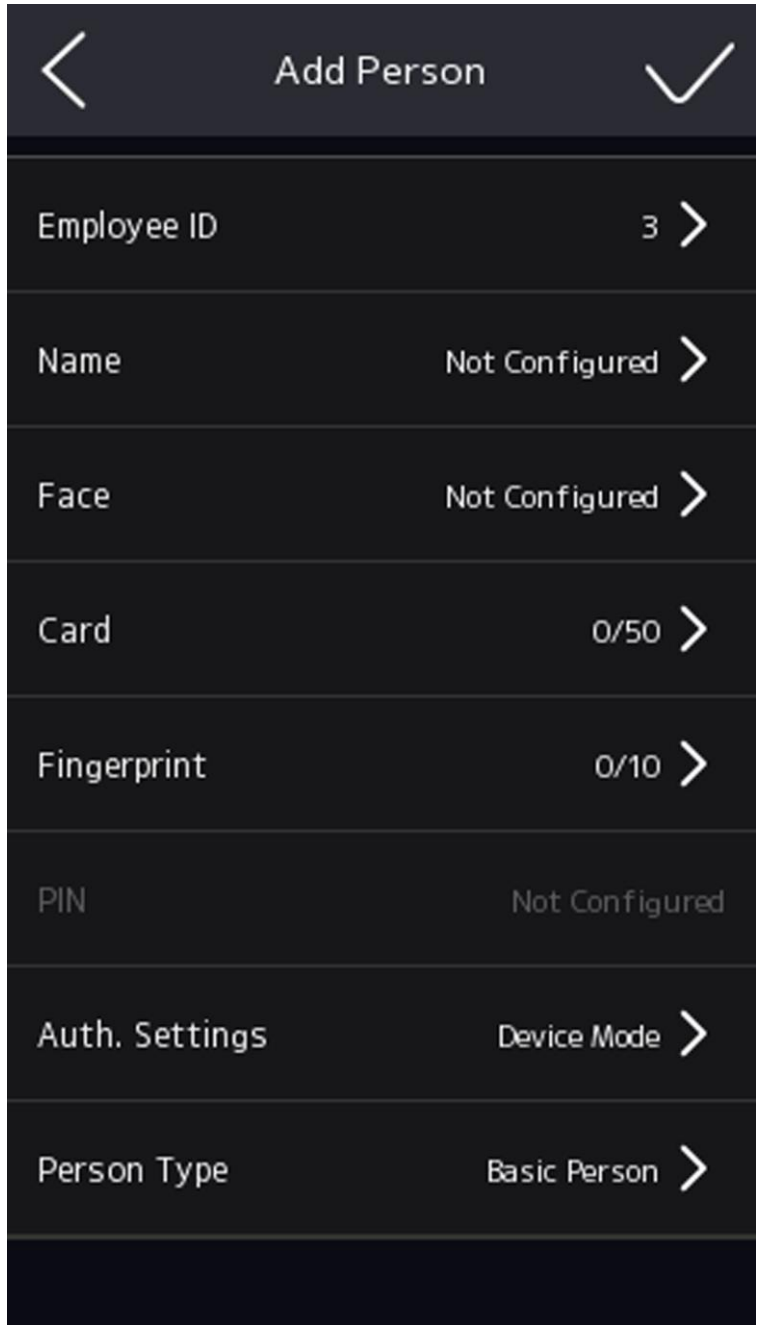
7.3.1 管理者の追加

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. 初期ページを長押しし、バックエンドにログインします。

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ユーザー名を入力して部署を選択してください。

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。
- ユーザー名は最大32文字まで入力可能です。

5. **オプション：**管理者の顔写真、指紋、カード、または PIN を追加します。

注

- 顔写真を追加する方法の詳細については、「***顔写真を追加する」*** を参照してください。
- **注意**
  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、「***カードを追加する」*** を参照してください。
- パスワードの追加については、「***PIN の追加」*** 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。

注記

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

   ユーザーは管理者です。通常の勤怠機能に加え、権限認証後にホームページへアクセスして操作できます。
9. 「**出席確認のみ**」を有効化できます。有効化後、このユーザーにはアクセス制御権限が付与されません。
10. 設定を保存するには「✓」をタップしてください。

7.3.2 顔写真を追加

ユーザーの顔写真をデバイスに追加します。ユーザーは顔写真で認証できます。

手順

注意

最大1500枚の顔写真を追加できます。

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てバックエンドにログインしてください。
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を編集します。

注意

- 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、数字の組み合わせが可能です。
- 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ユーザー名を入力して部署を選択してください。

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. 顔写真フィールドをタップして、顔写真追加ページに入ります。

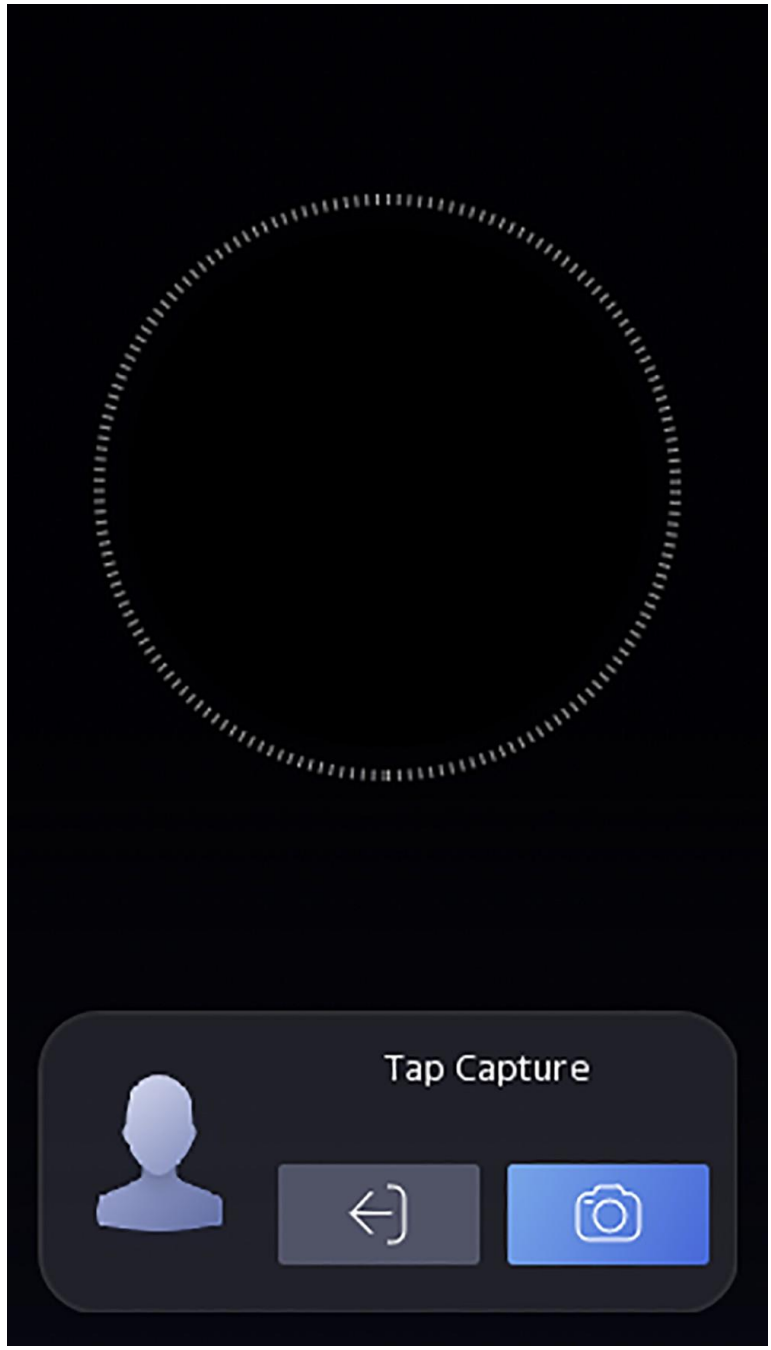


図 7-9 顔写真を追加

6. カメラを見てください。

注意

- 顔写真を追加する際は、必ず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。
- 撮影した顔写真は、画質が良く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・比較時のヒント」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ます。

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. ユーザーロールを設定してください。

管理者

ユーザーは管理者です。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することもできます。

一般ユーザー

ユーザーは一般ユーザーです。ユーザーは初期ページでの認証または出席登録のみ可能です。

10. ✓をタップして設定を保存します。

7.3.3 指紋を追加

ユーザーに指紋を追加すると、ユーザーは追加された指紋で認証できます。

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。
- 最大3000個の指紋を追加できます。

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してデバイスのバックエンドに入ります。

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部署を選択してください。

注記

- ユーザー名には数字、大文字、小文字、特殊文字の使用が許可されています。
    - 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. 指紋フィールドをタップして、指紋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 人のユーザーにつき、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または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、「*指紋スキャンのヒント」*を参照してください。

7. ユーザーの役割を設定
します。

管理者

ユーザーは管理者です。通常の出勤機能に加え、権限認証後にホームページへアクセスして操作することも可能です。

一般ユーザー

ユーザーは一般ユーザーです。ユーザーは初期ページでの認証または出席記録のみ可能です。

8. 設定を保存するには、[ ]をタップしてください。

7.3.4 カード追加

ユーザーにカードを追加すると、追加されたカードで認証できます。

手順

注記

最大3000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てバックエンドにログインしてください。

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. 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。

5. 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部署を選択してください。

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。

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してください

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. ユーザーロールを設定してください。

   管理者

   ユーザーは管理者です。通常の勤怠機能に加え、権限認証後にホームページにアクセスして操作することもできます。

   一般ユーザー

   ユーザーは通常のユーザーです。ユーザーは初期ページでのみ認証または出席確認が可能です。

10. 設定を保存するには、[ ]をタップしてください。

7.3.5 PINを追加

ユーザーに PIN を追加すると、ユーザーは PIN による認証が可能になります。

開始前に

注意

パスワードモードが「**ローカルパスワード**」または「**プラットフォームパスワード**」であることを確認してください。「**ローカルパスワード**」を選択した場合、デバイスまたはWeb上でPINを追加できます。「**プラットフォームパスワード**」を選択した場合、デバイスまたはWeb上でPINを追加できず、代わりにプラットフォーム上でPINを追加する必要があります。パスワードモードの設定の詳細については、***「認証設定」***を参照してください。

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てバックエンドにログインしてください。
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。

注意

- 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、数字の組み合わせが可能です。
- 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ユーザー名を入力して部署を選択してください。

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. PIN コードをタップし、ユーザーの PIN を作成します。

注記

パスワードモードが**ローカルパスワード**であることを確認してください。そうしないと、PIN エリアを編集できません。

6. ユーザーロールを設定します。

管理者

ユーザーは管理者です。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。

一般ユーザー

ユーザーは一般ユーザーです。ユーザーは初期ページでの認証または出席記録のみ可能です。

7. をタップして設定を保存します。

7.3.6 認証モードの設定

ユーザーの顔写真、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。ユーザーは設定された認証モードを通じて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てバックエンドにログインしてください。

2. **ユーザー**をタップ → **ユーザー追加/ユーザー編集** → **認証モード**。

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。

7.3.7 ユーザーの検索と編集

ユーザーを追加した後、そのユーザーを検索して編集できます。

ユーザー検索

ユーザー管理ページで、検索エリアをタップしてユーザー検索ページに入ります。ページの左側にある「**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。検索には従業員ID、カード番号、またはユーザー名を入力します。「  」をタップして検索します。

ユーザーの編集

ユーザー管理ページで、ユーザーリストからユーザーを選択すると、ユーザー編集ページに移動します。***ユーザー管理***の手順に従ってユーザーパラメータを編集してください。設定を保存するには「  」をタップします。

注記
従業員IDは編集できません。

7.4 勤怠ステータス設定

実際の状況に応じて、出勤モードをチェックイン、チェックアウト、休憩開始、休憩終了、残業開始、残業終了に設定できます。

注記
この機能は、クライアントソフトウェア上の勤怠管理機能と連携して使用する必要があります。

7.4.1 デバイス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ません。

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。

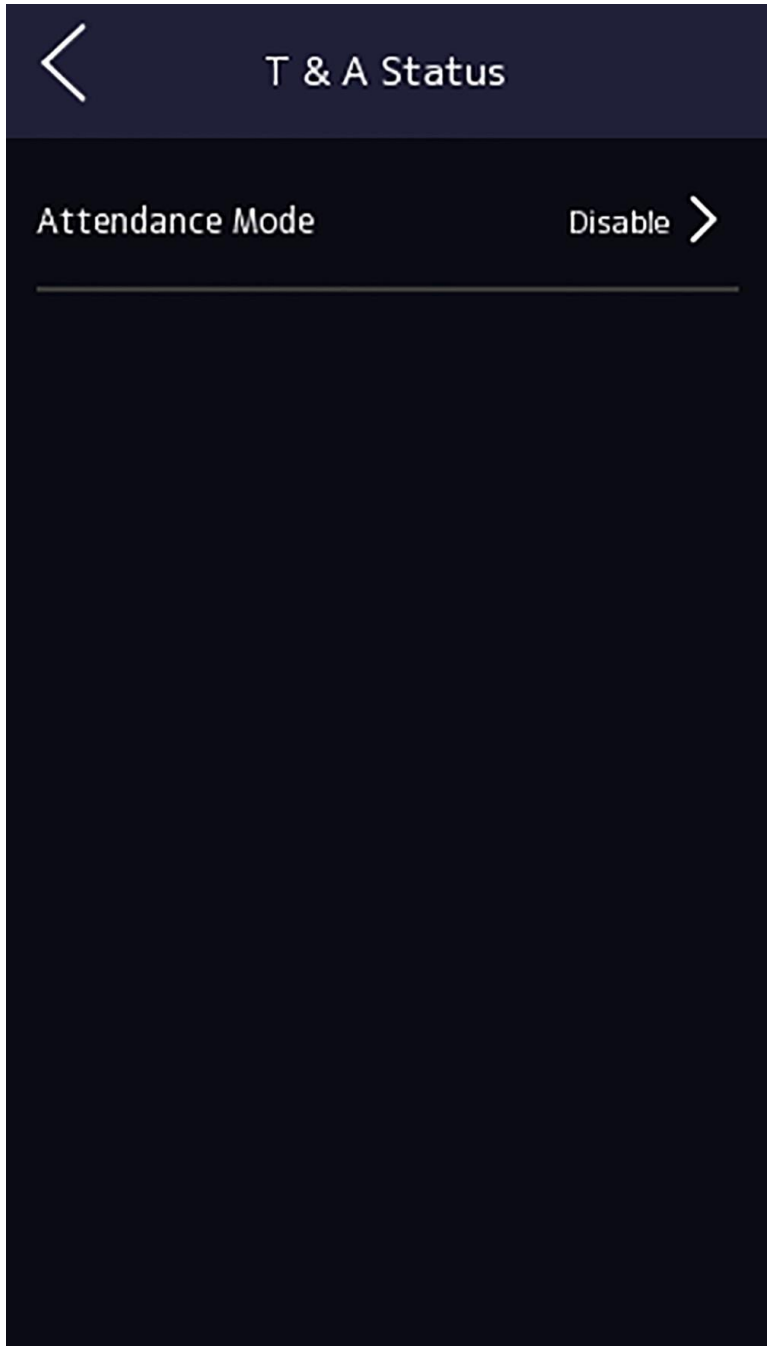


図 7-10 勤怠モードを無効にする

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。

7.4.2 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、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、T&Aステータスページに入ります。
2. **出席モード**を手**動**に設定してください。

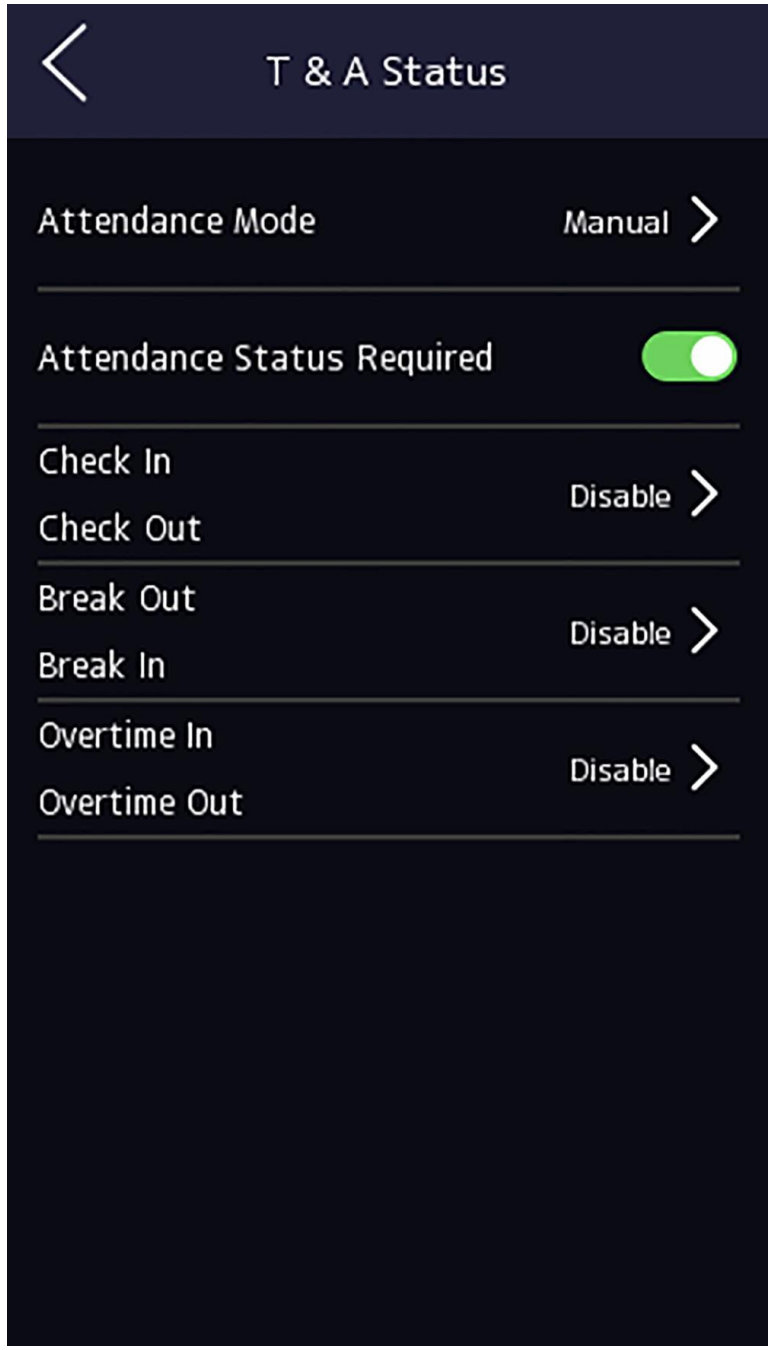


図7-11 手動出席モード

3. **出席ステータス必須**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、名前を変更します。

この名前は、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、有効な出席として記録されません。

7.4.3 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

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、勤怠状況ページに入ります。
2. **出勤モード**を**自動**に設定します。

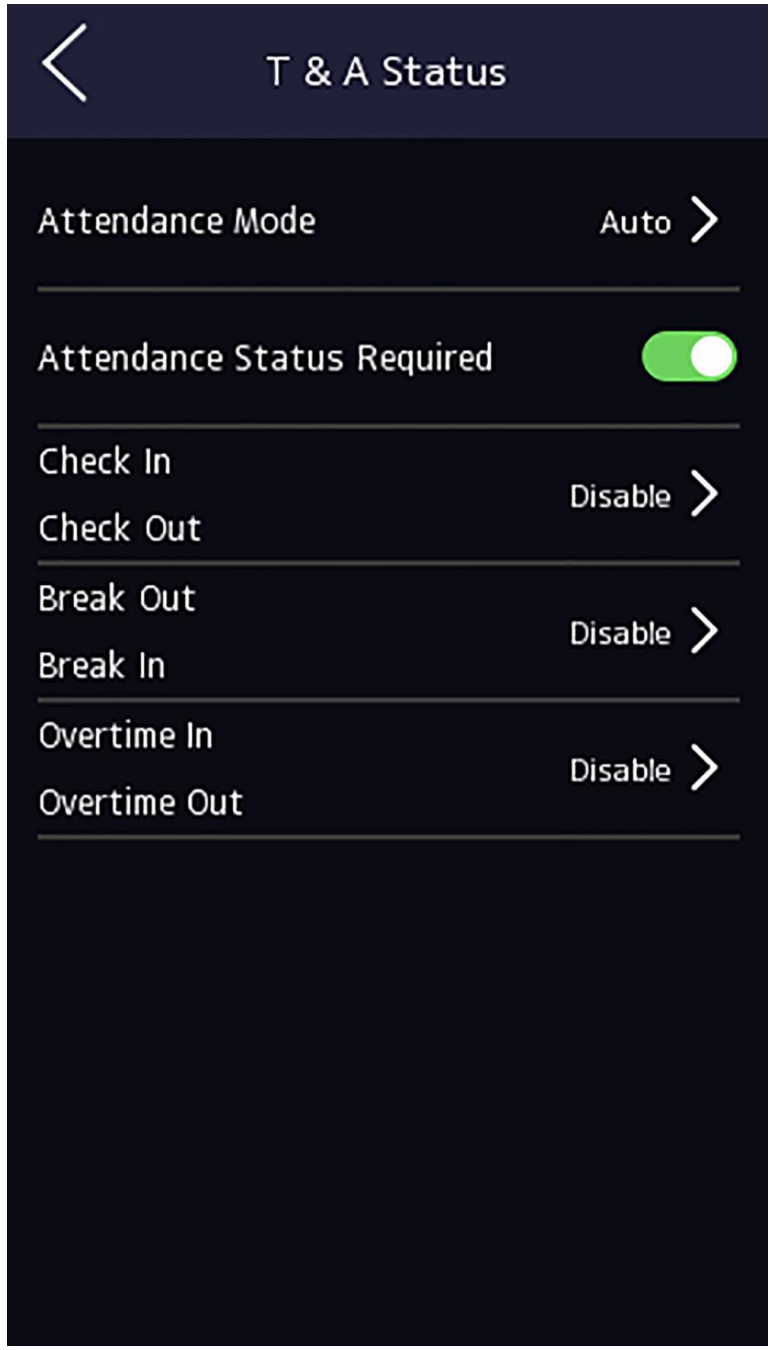


図7-12 自動出席モード

3. **出勤**ステータス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、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**を選択してください。

3) 選択した出勤ステータスの当日の開始時刻を設定します。

4) **確認**をタップしてください。

5) 実際の必要に応じて、手順1から4を繰り返します。

注意

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。

7.4.4 デバイス経由での手動・自動勤怠設定

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、認証後に手動で出勤ステータスを変更することも可能です。

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. **プラットフォームの出勤管理**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。

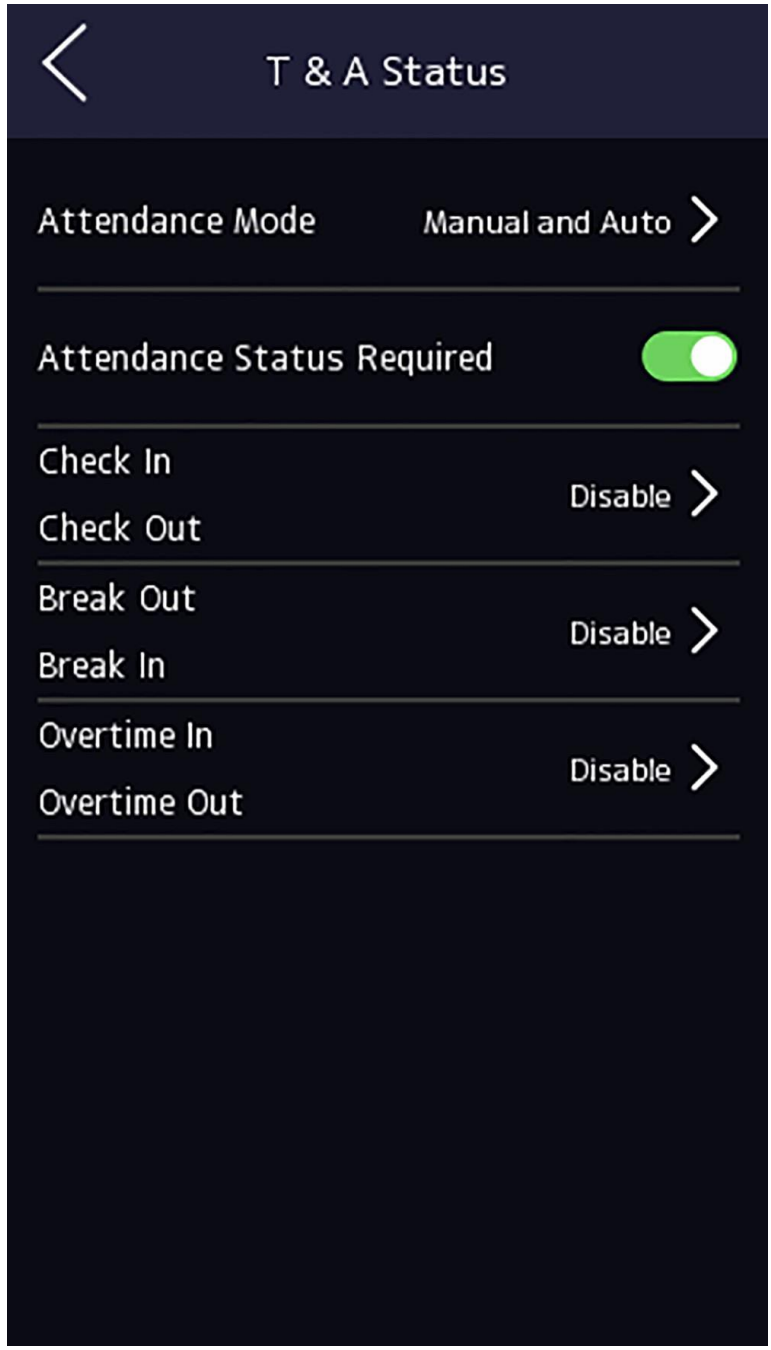


図7-13 手動モードと自動モード

3. **出勤**ステータス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、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) **出席スケジュールを**タップしてください。

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**を選択してください。

3) 選択した出勤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。

7.5 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。

7.5.1 データの削除

ユーザーデータを削除します。

ホームページで、**データ → データの削除 → ユーザーデータを**タップします。デバイスに追加されたすべてのユーザーデータが削除されます。

7.5.2 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. **「ユーザーデータ」**、**「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

インポートする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. データのエクスポート時に作成したパスワードを入力します。データのエクスポート時にパスワードを作成していない場合は、入力ボックスを空白のままにして、すぐに **OK を**タップします。

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）へすべてのユーザー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ユーザー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
- フォルダ「enroll_pic」に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の下に「enroll_pic1」「enroll_pic2」「enroll_pic3」「enroll_pic4」という名前のフォルダを追加作成できます。
- 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可能です。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：正面をカメラに向けて撮影すること。帽子や頭部覆いを着用しないこと。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から200KBの間であること。

7.5.3 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. **フェイスデータ**、**イベントデータ**、**ユーザーデータ**、または**アクセス制御パラメータ**をタップします。

注記

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

- 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1G～32G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512M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ユーザーデータはDBファイルであり、編集することはできません。

7.6 本人認証

ネットワーク設定、システムパラメータ設定、ユーザー設定の後、初期ページに戻って本人認証を行うことができます。システムは設定された認証モードに従って本人を認証します。

7.6.1 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。詳細は「***認証モードの設定***」を参照してください。顔認証、指紋認証、またはカード認証を行います。

顔認証

カメラに向かって正面を向き、顔認証を開始します。

指紋

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てください。

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を使用できます。

PIN

PIN による認証を行うには、PIN コードを入力してください。

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。

7.6.2 複数の認証情報による認証

ご利用開始前に

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。

手順

1. 認証モードが「カードと顔認証」「パスワードと顔認証」「カードとパスワード」「カードと顔認証と指紋認証」の場合、ライブビューページの指示に従いいずれかの認証情報で認証を行ってください。

   注意

   - カードは通常のICカード、または暗号化カードを使用できます。

2. 前の認証手段が認証された後、他の認証手段の認証を続行します。

   注

   - 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。

   認証が成功した場合、「認証されました」というプロンプトが表示されます。

7.7 基本設定

音、時間、スリープ（秒）、言語、コミュニティ番号、建物番号、ユニット番号、プライバシー、ビデオ規格を設定できます。

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。

サウンド設定

音声プロンプト機能の有効化/無効化、および音声音量の調整が可能です。

注意
音声の音量は 0 から 10 まで設定できます。0 は無音です。

時刻設定

タイムゾーン、デバイスの時刻、夏時間を設定します。

スリープ時間 (秒)

デバイスのスリープ待機時間を設定します（分単位）。初期画面でスリープ時間を30分に設定した場合、操作がない状態で30分経過するとデバイスはスリープ状態になります。

注意
スリープ時間を0に設定した場合、デバイスはスリープモードに入りません。

言語の選択

実際のニーズに応じて言語を選択してください。

コミュニティ番号

設置された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

デバイスが設置されている建物の番号を設定してください。

ユニット番号

設置ユニット番号を設定

通話設定

ダイヤル後の自動発信

ダイヤル後の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

発信先を選択してください。

VoIPサーバー

VoIPサーバーを選択します。

プライバシー

名前/従業員ID

認証時に名前と従業員IDを表示する/表示しない/非表示にするかを選択できます。

顔写真

認証時に顔写真を表示するかどうかを選択できます。

登録画像の保存

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。

認証時の画像保存

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

プラットフォームへの認証時に撮影された画像を自動的にアップロードします。

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。

ビデオ標準

リモートでライブビューを行う際の動画フレームレートを設定します。規格を変更した後は、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。

7.8 生体認証パラメータの設定

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。設定可能なパラメータには、顔生体検知レベル、認識距離、顔認識間隔、顔1:Nセキュリティレベル、顔1:1セキュリティレベル、ECOモード設定、マスク検出が含まれます。

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。**システム設定 → 生体認証 を**タップします。

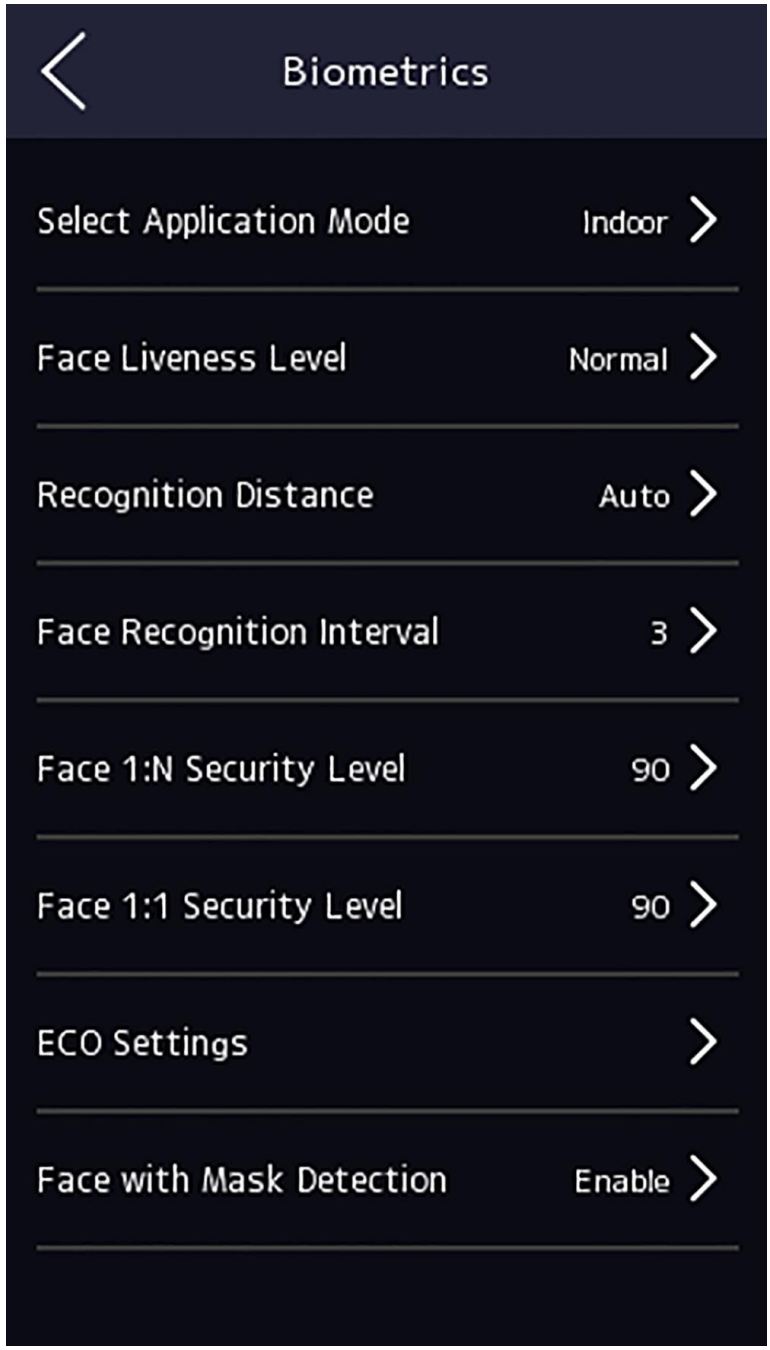


図 7-14 生体認証パラメータページ

表 7-1 顔画像パラメータ

パラメータ	説明
顔生体検知レベル	顔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。
認識距離	認証時にユーザーとカメラの有効な距離を設定します。
顔認識間隔	認証時に連続する2回の顔認識の間隔を設定します。 **注** 1～10の数値を入力できます。
顔1:Nセキュリティレベル	1:N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は低くなりますが、誤拒否率は高くなります。
顔1:1セキュリティレベル	1対1マッチングモードで認証する際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。
ECOモード設定	ECOモードを有効にすると、デバイスは低照度または暗所環境においてIRカメラで顔認証を行います。ECOモードしきい値、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。 **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は低くなりますが、誤拒否率は高くなります。 **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一致閾値を設定します。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
マスク設定	マスク検出機能を有効にすると、システムはマスク画像付きの顔を認識します。**マスク付き顔&顔（1:1）**、**マスク付き顔&顔（1:N）**、**ECO（1:1）しきい値**、**ECOモード（1:N）しきい値**、**およびプロンプト方法を設定できます**。 **マスク着用顔&顔（1:1）**

パラメータ	説明
	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。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。 **マスク着用顔認証&顔認証（1:N）** マスク着用時の顔認証において、1:Nマッチングモードで認証を行う際の一致判定閾値を設定します。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。 **ECOモード（1:1）しきい値** ECOモード1:1マッチングモードでフェイスマスク認証を行う際の一致判定値を設定します。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。 **ECOモード（1:N）しきい値** ECOモード1:Nマッチングモードでフェイスマスク認証を行う際の一致閾値を設定します。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。 **プロンプト方法** **「なし」、「着用リマインダー」、「着用必須」**の戦略を設定します。 **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、通知が表示されドアが開きます。 **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。 **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。

7.9 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 → 設定**をタップして設定ページに入ります。

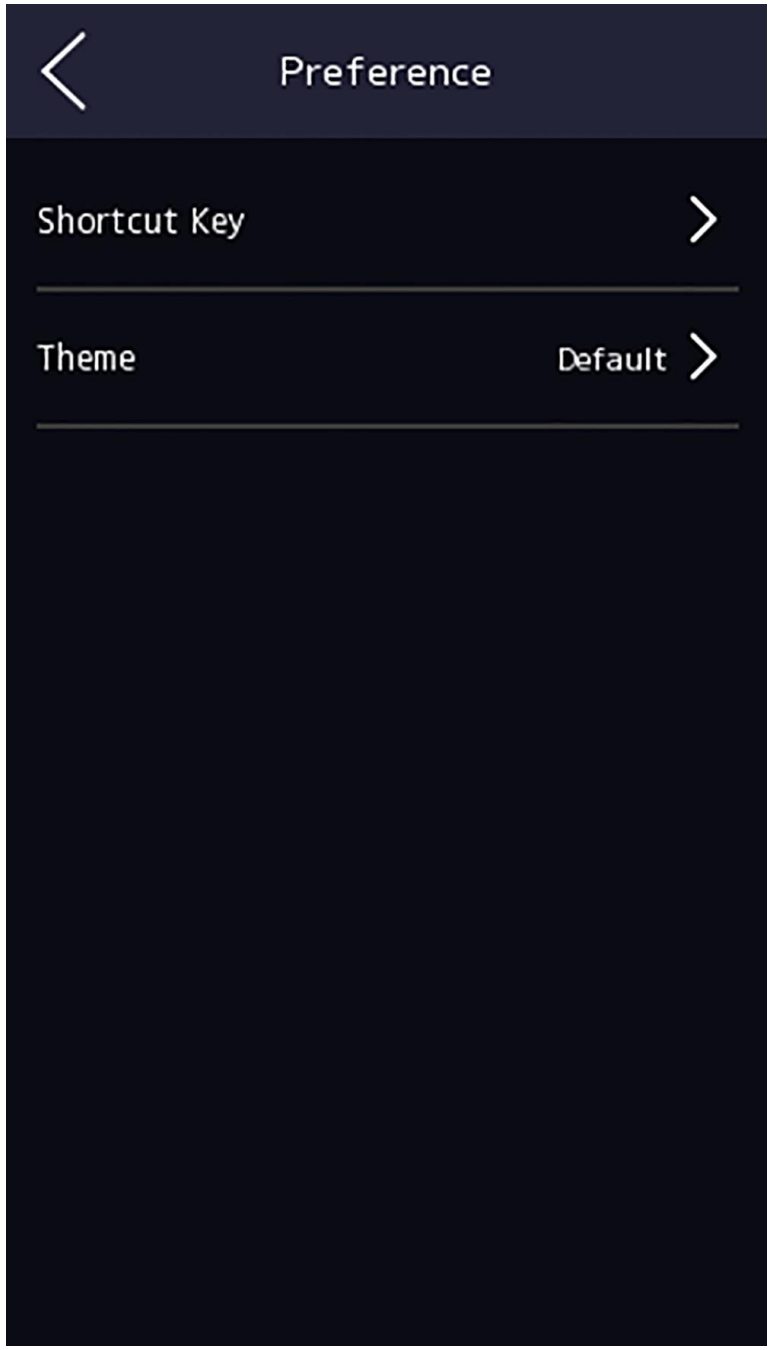


図 7-15 設定

ショートカットキー

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。これには、パスワード入力機能、QRコード機能、通話機能、および通話タイプが含まれます。

注

通話タイプは、**通話ルーム**、**コールセンター**、**指定ルーム番号への通話**、**APPへの通話から**選択できます。**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を行うことができます。

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。

通話ルーム

認証ページで通話ボタンをタップすると、通話する部屋番号をダイヤルする必要があります。

コールセンター

認証ページで通話ボタンをタップすると、センターに直接通話できます。

指定部屋番号への通話

認証ページで通話ボタンをタップすると、設定済みの部屋番号をダイヤルせずに直接呼び出すことができます。

通話アプリ

認証ページで呼び出しボタンをタップすると、デバイスが追加されているモバイルクライアントに呼び出しが行われます。

室内機番号呼び出し

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/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。

テーマ

認証ページのプロンプトウィンドウのテーマを設定できます。

認証用/シンプルをテーマとして選択できます。**認証**

デバイス認証ページで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。

シンプル

このモードを選択すると、認証ページのライブビューは無効化され、同時に人物名、社員ID、顔写真がすべて非表示になります。

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。

チェック時に出席記録を表示する

チェック時に出席記録を表示するを有効にすると、チェック時に出席記録が表示されます。

7.10 デバイスのパスワード変更

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）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。

7.11 認証設定

認証モードの機能、NFC カードの有効化、M1 カードの有効化、ドアコンタクト、開扉時間 (秒)、認証間隔 (秒)、認証結果表示時間 (秒)、パスワードモードなどのアクセス制御権限を設定できます。

ホームページで、**[認証設定]** をタップして設定ページに入ります。

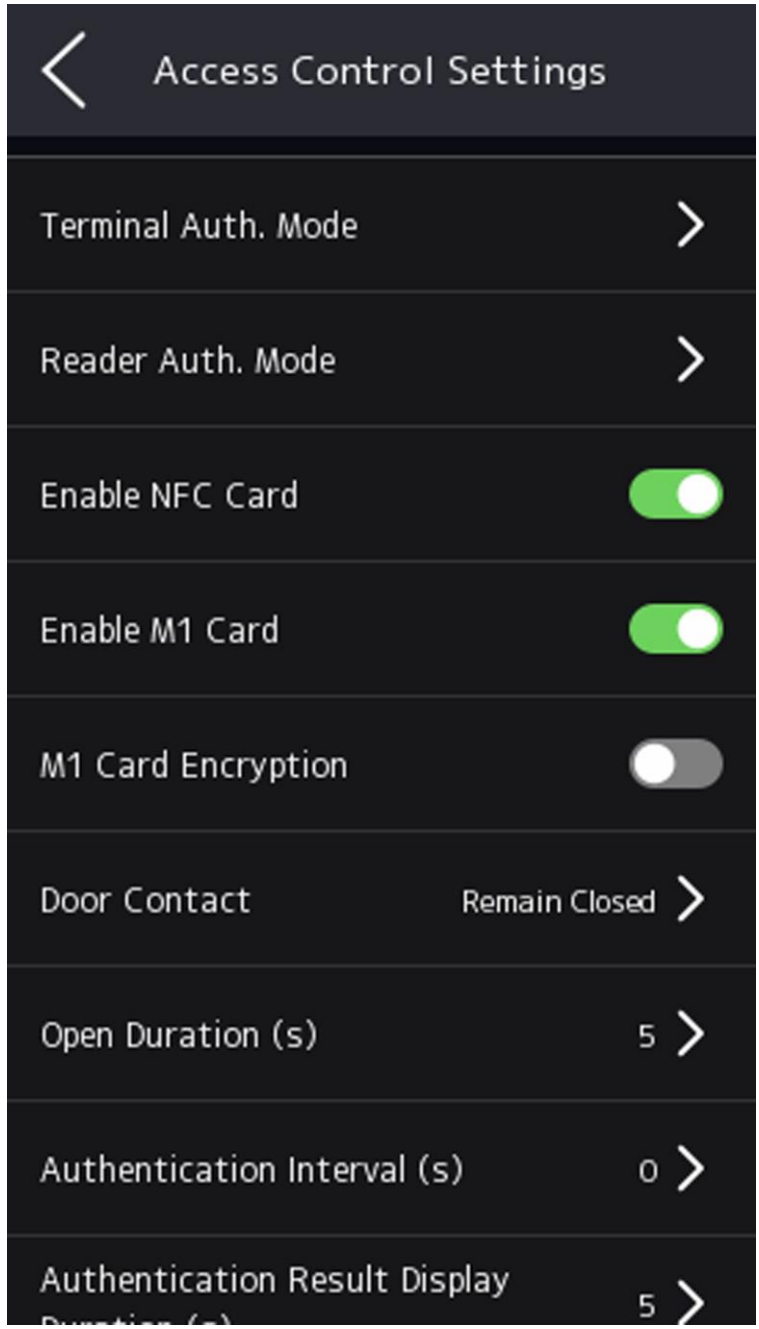


図 7-16 認証設定

利用可能なパラメータの説明は次のとおりです：

表 7-2 アクセス制御パラメータの説明

パラメータ	説明
端末認証モード (Terminal Authentication Mode)	顔認証端末の認証モードを選択します。認証モードをカスタマイズすることも可能です。 **注記** • 指紋モジュールを搭載した端末のみが指紋関連機能をサポートします。 • 生体認証製品は、偽装防止環境に対して完全には適用できません。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。 • 複数の認証モードを採用する場合、顔認証の前に他の認証方法による認証を行う必要があります。
リーダー認証モード（カードリーダー認証モード）	カードリーダーの認証モードを選択します。
NFC カードを有効にする	この機能を有効にすると、NFC カードを提示して認証を行うことができます。
M1 カードの有効化	機能を有効にすると、M1カードを提示して認証できます。
M1カード暗号化	M1カードの暗号化機能を有効にすると、カードのセキュリティレベルが向上します。カードが容易に複製されることはありません。
ドアコンタクト	実際のニーズに応じて「開（開いたまま）」または「閉（閉じたまま）」を選択できます。デフォルトは閉（閉じたまま）です。
開扉時間	ドアの解錠時間を設定します。設定時間内にドアが開かない場合、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。
認証間隔	デバイスの認証間隔を設定します。設定可能な認証間隔の範囲：0～65535秒。
認証結果表示時間 (秒)	認証後の認証結果表示時間を設定します。
パスワードモード	**プラットフォーム適用型個人用PIN** PINはプラットフォームによって管理・配布されます。Web端末ではPINを設定できません。 **デバイス設定個人用PIN**

パラメータ	説明
	PINはデバイスまたはWeb上で設定されます。他のプラットフォームではPINを設定できません。

7.12 システムメンテナンス

デバイスのシステム情報と容量を確認できます。また、デバイスのアップグレード、ユーザーマニュアルの閲覧、工場出荷時設定への復元、デフォルト設定への復元、システムの再起動が可能です。

初期画面を3秒間長押ししてホームページにログインします。「**メンテナンス」を**タップします**。**

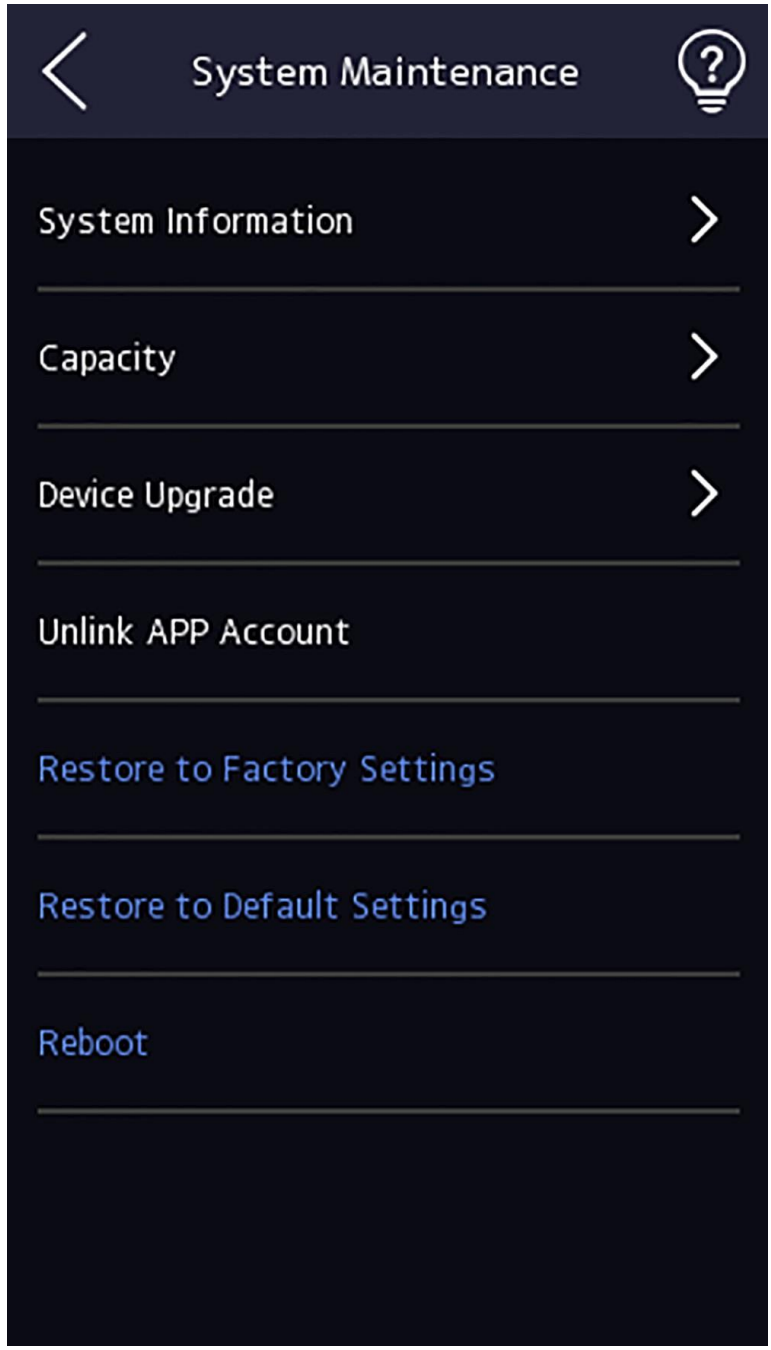


図 7-17 メンテナンスページ

システム情報

デバイスモデル、シリアル番号、ファームウェアバージョン、MACアドレス、製造データ、ライセンスなどのデバイス情報を確認できます。

注意

表示内容はデバイスモデルによって異なる場合があります。詳細は実際の画面をご確認ください。

を長押しし、管理者パスワードを入力してデバイスバージョン情報を表示します。

顔パラメータ

カスタム偽装防止検出顔生体検知レベル

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セキュリティレベルを設定できます。

偽装検出のしきい値

値が大きいほど、誤認率は低くなり、誤拒否率は高くなります。値が小さいほど、誤認率は高くなり、誤拒否率は低くなります。

顔認証ロックによるなりすまし防止

この機能を有効にすると、偽装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に、**偽装防止のためのロック画面を**有効にした後のロック時間。

バージョン情報

デバイスの情報を表示できます。

容量

人物数、顔写真、カード、指紋、イベントの数を表示できます。

注

一部のデバイスモデルでは指紋認証容量の表示に対応しています。詳細は実際のページをご参照ください。

デバイスアップグレー

ドオンライン更新

デバイスがHik-Connectおよびネットワークに接続されている場合、Hik-Connectに新しいインストールパッケージがあるときは、**[デバイスアップグレード] → [オンラインアップデート]**をタップしてデバイスシステムをアップグレードできます。

USB経由での更新

USBフラッシュドライブをデバイスのUSBインターフェースに接続します。**デバイスアップグレード→USB経由の更新**をタップすると、デバイスはUSBフラッシュドライブ内の*digicap*.davファイルを読み取り、アップグレードを開始します。

ユーザーマニュアル

QRコードをスキャンしてデバイスのユーザーマニュアルを表示します。

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。システムは再起動して設定を有効にします。

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すべてのパラメータがデフォルト設定に復元されます。システムは再起動して設定を有効にします。

再起動

確認後、デバイスが再起動します。

第8章 モバイルWebによるデバイスの設定

8.1 ログイン

モバイルブラウザからログインできます。

注

- 一部のモデルではWi-Fi設定をサポートしています。
- デバイスの電源が入っていることを確認してください。
- デバイスと携帯電話が同じWi-Fiに接続されていることを確認してください。

モバイル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へ進みます。
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**をタップします。

8.2 概要

ドアの状態、ネットワーク状態、基本情報を確認し、ショートカット入力でユーザー管理、スマート設定、認証設定、ドアパラメータを設定できます。

機能説明:

ドアの状態

/ / /

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。実際の必要に応じて、タップして開いている/閉じている/開いたまま/閉じたままの状態を選択できます。

ショートカット入力

ショートカット入力により、ユーザー管理、スマート設定、認証設定、ドアパラメータを設定できます。

ネットワーク状態

ネットワークの接続状態と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。

8.3 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**」をタップしてください。

認証モードを選択してください。**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てください。

Eメールによる確認

1. QRコードをエクスポートし、***pw_recovery@hikvision.com*** 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. 確認コードを「確認コード」欄に入力し、本人確認を行ってください。「**次へ**」をクリックし、新しいパスワードを作成して確認してください。

8.4 設定

8.4.1 デバイス情報の表示

デバイス名、言語、モデル、シリアル番号、バージョン、IO入力番号、IO出力番号、ローカルRS-485番号、アラーム入力番号、アラーム出力番号、レジスタ番号、工場情報、デバイス容量などを表示します。

ホーム画面で、 （**システム管理**）→ **System Settings**（**システム設定**）→ **Basic Information**（**基本情報**）をタップします。

デバイス名、言語、モデル、シリアル番号、バージョン、IO 入力番号、IO 出力番号、ローカル RS-485 番号、アラーム入力番号、アラーム出力番号、レジスタ番号、工場情報、デバイス容量などを表示します。

保存をタップします。

8.4.2 時刻設定

タイムゾーン、時刻同期モード、表示時刻を設定します。

→ **System Settings** → **Time Settings** をタップして設定ページに入ります。

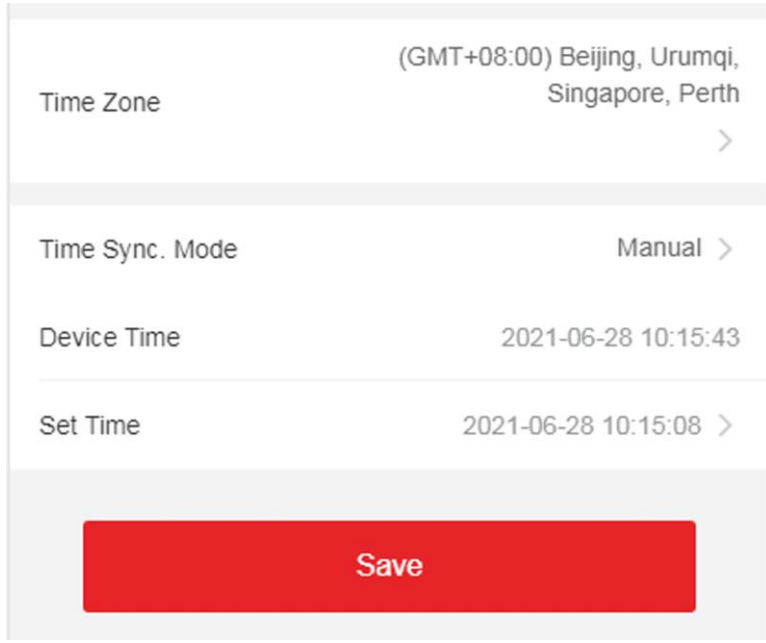


図8-1 時間設定

設定を保存するには「**保存**」をタップしてください。

タイムゾーン

ドロップダウンリストから、デバイスが置かれているタイムゾーンを選択します。

時刻同期モード手動

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。デバイスの時刻は手動で設定できます。

NTP

NTP サーバーの IP アドレス、ポート番号、および間隔を設定します。

8.4.3 夏時間設定

手順

1. → **System Settings** → **Time Settings** をタップし、設定ページに入ります。

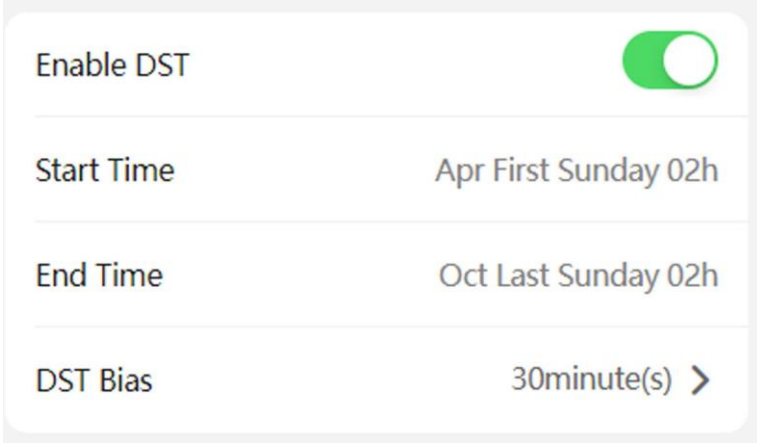


図 8-2 DST

2. **夏時間（DST）を有効にする**をタップします。
3. 開始時刻、終了時刻、およびサマータイムの偏りを設定します。
4. **保存**をタップします。

8.4.4 ユーザー管理

手順

1. 「≡」→**「ユーザー管理」→「ユーザー管理」→「admin」**をタップして設定ページに入ります。
2. 古いパスワードを入力し、新しいパスワードを作成します。
3. 新しいパスワードを確認します。
4. **保存**をタップします。

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（8～16文字で、大文字、小文字、数字、特殊文字の少なくとも2種類を含む）に変更することを強くお勧めします。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。毎月または毎週パスワードを変更することで、製品をより効果的に保護できます。

8.4.5 ネットワーク設定

有線ネットワーク、Wi-Fiパラメータ、およびデバイスポートを設定できます。

有線ネットワーク

有線ネットワークを設定します。

→ **通信設定** → **有線ネットワーク**をタップして設定ページに入ります。

DHCP

この機能を無効にする場合は、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、MTU を設定する必要があります。

機能を有効にすると、システムは 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を自動的に割り当てます。

DNS サーバー

実際の必要に応じて、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

デバイスの無線接続用に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. → **通信設定** → **Wi-Fi** をタップして設定ページに入ります。
2. **Wi-Fi** を有効にします。

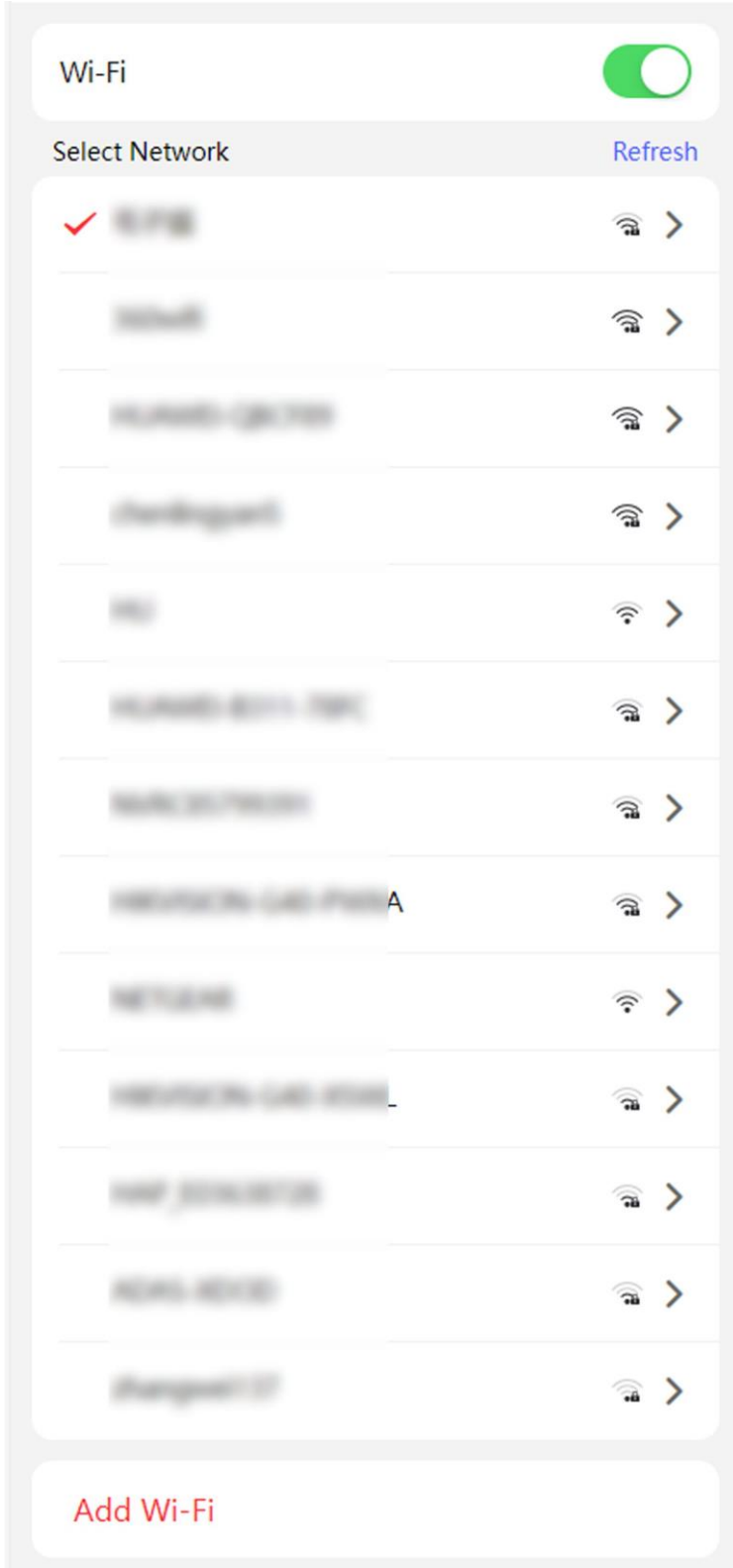


図 8-3 Wi-Fi

3. Wi-Fi を追加します。

1) **Wi-Fi の追加**をタップします。

2) **Wi-Fi** 名と **Wi-Fi パスワード**を入力し、**暗号化タイプ**を選択します。

3) **保存**をタップします。

4. Wi-Fi名を選択し、「**接続**」をタップします。

5. パスワードを入力し、「**保存**」をタップします。

ポートパラメータの設定

ネットワーク経由でデバイスにアクセスする際、実際の必要に応じてHTTPとHTTPSを設定できます。「 」→「**Network Service**」→「**HTTP(S)**」をタップし、設定ページに入ります。

HTTP

ブラウザがデバイスにアクセスする際に使用するポートを指します。例えば、HTTPポートを81に変更した場合、ブラウザでログインするにはhttp://192.0.0.65:81を入力する必要があります。

HTTPS

ブラウザアクセス用のHTTPSを設定します。アクセス時には証明書が必要です。

プラットフォームアクセス

プラットフォームアクセスにより、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. 「 」→「**デバイスアクセス**」→「**Hik-Connect**」をタップして設定ページに入ります。

注意

Hik-Connectはモバイル端末用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「**有効化**」をチェックします。

3. 「**カスタム**」を有効にすると、サーバーアドレスを入力できます。

注意

- 6～12文字（a～z、A～Z）または数字（0～9）、大文字小文字を区別します。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。
- 確認コードは「***123456***」や「***abcdef***」（大文字小文字を区別しない）とすることはできません。

4. **登録状況**と**紐付け状況**を確認できます。

5. **ビデオ暗号化を**有効にし、パスワードを作成して確認してください。

注意

デバイスをアプリに追加後、ライブ映像を視聴するにはビデオ暗号化パスワードの入力が必要です。

6. **アカウントを紐付ける → QRコードを表示 を**タップし、QRコードをスキャンしてアカウントを紐付けます。

7. 設定を有効にするには「**保存**」をタップしてください。

ISUPパラメータの設定

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

注意
デバイスがこの機能をサポートしている必要があります。

1. → **Device Access** → **ISUP** をタップして設定ページに入ります。
2. **ISUP**を有効にします。
3. ISUPバージョン、サーバーアドレス、ポート、デバイスID、暗号化キーを設定します。

注記
バージョンとして5.0を選択した場合、暗号化キーも設定する必要があります。

4. 設定を保存するには、**[保存]** をタップします。

OTAPの設定

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、動作状況やアラーム情報のアップロード、デバイスの再起動やアップグレードを行います。

手順

1. [ ] → **[Device Access]** → **[OTAP]** をタップして設定ページに入ります。
2. 「OTAPを**有効にする**」をタップします。
3. **サーバーアドレス**、**ポート**、**デバイスID**、**暗号化キー**を設定します。
4. **「テスト」を**タップし、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ます。ページを更新するかデバイスを再起動し、**登録ステータスを**確認してください。
5. **保存**をタップします。

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、侵入サービスを有効にしてデバイスのリモート管理を実現できます。

手順

1. [ ] → **[Device Access]** → **[Network Penetration Service]** をタップして設定ページに入ります。
2. **「侵入サービス有効化」**をタップします。
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**をタップします。

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。

8.4.6 ユーザー管理

モバイル Web ブラウザからユーザーの追加、編集、削除、検索を行うことができます。

手順

1. → **人物管理**をタップして設定ページに入ります。

2. ユーザーを追加。

1) + をタップします。

2) 以下のパラメータを設定します。

従業員ID

従業員IDを入力します。従業員IDは0または32文字を超えることはできません。大文字、小文字、数字の組み合わせで構成できます。

名前

名前を入力してください。名前には数字、英字の大文字・小文字、記号が使用可能です。32文字以内が推奨されます。

長期有効ユーザー

ユーザー権限を長期有効に設定します。

開始日/終了日

ユーザー権限の**開始日**と**終了日**を設定します。

ユーザーロール

ユーザーロールを選択してください。

個人ロール

個人としての役割を選択してください。

出席確認のみ

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。

顔

顔写真を追加します。**「顔」を**タップし、**「カメラ」を**タップして顔を追加するか、**「アルバムから選択」**をタップして顔をインポートします。

指紋

指紋を追加します。「**指紋**」をタップし、**「+」**をタップして、指紋モジュールから指紋を追加します。

カード

カードを追加します。**「カード」を**タップし、**「+」を**タップしてカード番号を入力し、カードの種類を選択します。

3) **保存**をタップしてください。

3. ユーザーリストで編集が必要なユーザーをタップして情報を編集します。

4. ユーザーリストで削除が必要なユーザーをタップし、「」をタップしてユーザーを削除します。

5. 検索バーに従業員IDまたは名前を入力してユーザーを検索できます。

8.4.7 イベントを検索

検索をタップ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。従業員ID、名前、カード番号、開始時間、終了時間を含め、**検索**をタップしてください。

注

32桁以内の名前検索に対応しています。

8.4.8 アクセス制御設定 認証パラメータの設定

認証パラメータの設定

手順

1. → **アクセス制御** → **認証設定** をタップします。

2. **保存**をタップします。

設定する端末

設定する端末を選択します。

ターミナルタイプ/ターミナルモデル

端末の説明を取得します。これらは読み取り専用です。

認証デバイスを有効にする

認証機能を有効にします。

認証

実際のニーズに応じて、ドロップダウンリストから認証モードを選択してください。

連続顔認識間隔（秒）

認証中に同一人物の連続認識間隔を設定できます。設定された間隔内では、人物Aは1回のみ認識されます。間隔内に別の人物（人物B）が認識された場合、人物Aは再度認識可能となります。

認証間隔

認証時の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。

最大失敗試行回数アラーム

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

メインインターフェースモード

メインインターフェースモードを**認証モード**または**簡易モード**に設定できます。

改ざん検出を有効にする

カードリーダーの改ざん検知を有効にします。

カード番号反転を有効にする

この機能を有効にすると、カード番号は逆順になります。

ドアパラメータの設定

→ **Access Control** → **Door Parameters** をタップします。

設定後、**保存**をタップして設定を保存します。

ドア名

ドアの名前を作成できます。

開放時間

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。

退出ボタンタイプ

実際のニーズに応じて、退出ボタンを「**開いたまま**」または「**閉じたまま**」に設定できます。デフォルトは「**開いたまま**」です。

最初の入室者によるドア開放持続時間（分）

最初の人が入室した際のドア開放時間を設定します。最初の人が認証されると、複数人の入室やその他の認証操作が可能になります。

ドア開放タイムアウトアラーム

設定時間内にドアが閉じられなかった場合、警報が作動します。

ドアコンタクト

実際のニーズに応じて、ドアコンタクトを「**開いたまま**」または「**閉じたまま**」に設定できます。デフォルトは「**閉じたまま**」です。

ドアロック電源オフ

ドアロック電源オフは、実際のニーズに応じて「**開いたまま**」または「**閉じたまま**」に設定できます。デフォルトは「**閉じたまま**」です。

延長開放時間

延長アクセス権限を持つ者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。

緊急コード

緊急事態発生時には緊急コードを入力することでドアを開錠できます。同時に、クライアントは緊急事態を報告できます。

スーパーパスワード

特定の者はスーパーパスワードを入力することでドアを開けることができます。

注記

緊急コードとスーパーコードは異なるものにする必要があります。また、桁数は4から8桁です。

端末パラメータ

アクセス用の端末パラメータを設定できます。

をタップ → **アクセス制御** → **端末パラメータ**。

アクセス制御モードとして動作モードを設定できます。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。

リモート認証

リモート認証を有効にした後、認証時にはデバイスが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。

ローカルでの認証情報検証

機能を有効にすると、デバイスは許可を確認しますが、プランテンプレートの推定は行いません。

タイムアウト期間

リモート認証のタイムアウト期間を設定できます。

設定後、**保存**をタップして設定を保存します。

カードセキュリティの設定

設定ページに入るには、[ ] → **[Access Control]** → **[Card Security]** をタップします。パラメータを設定し、**[Save]** をタップします。

NFCカードの有効化

携帯電話がアクセス制御のデータを取得するのを防ぐため、NFC カードを有効にしてデータのセキュリティレベルを高めることができます。

M1カードの有効化

M1カードを有効化すると、M1カードの提示による認証が可能になります。

M1カードの暗号化

M1カードの暗号化は、認証のセキュリティレベルを向上させることができます。

セクター

機能を有効化し、暗号化セクターを設定します。デフォルトではセクター13が暗号化されます。セクター13の暗号化を推奨します。

EMカード有効化

EMカードを有効化し、EMカードの提示による認証が可能になります。

注記

EMカードは、EMカードの提示をサポートする周辺機器カードリーダーをデバイスに接続した場合にサポートされます。

DESFireカードの有効化

DESFireカード機能を有効にすると、デバイスはDESFireカードからデータを読み取ることができます。

FeliCaカード機能を有効にする

FeliCa カード機能を有効にすると、デバイスは FeliCa カードからデータを読み取ることができます。

RS-485 パラメータの設定

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。 **（設定）→ Access Control（アクセス制御）→ RS-485** をタップします。

設定後、**[保存]** をタップして設定を保存します。

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。選択可能なのは以下の通りです：**カードリーダー**、**拡張モジュール**、または**アクセスコントローラー**から選択できます。

注意

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 プロトコル プライベート

本デバイスは、RS-485 経由でサードパーティ製デバイスに接続できます。

OSDP

標準 RS-485 プロトコル。

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

アクセスコントローラを選択した場合：RS-485インターフェース経由で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。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

RS-485 プロトコルで通信するときのボーレート。

データビット

RS-485 プロトコルでデバイスが通信するときのデータビット。

ストップビット

デバイスが RS-485 プロトコルを介して通信するときのストップビット。

パリティ/フロー制御/通信モード

デフォルトで有効。

8.4.9 ビデオインターホン設定

デバイス ID 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。使用前に装置番号を設定してください。

手順

1. → **インターコム** → **デバイスID設定 を**タップします。
2. 以下のパラメータを設定します。

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。

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。

期間番号

デバイスの期間番号を設定してください。

建物番号

装置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

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。

フロア番号

設置階を設定してください。

ドアステーション番号

設置階を設定します。

注意

- 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 までの範囲です。

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。

期間番号

デバイスの期間番号を設定します。

セッション設定

ドアステーション、メインステーション、およびビデオインターホンサーバー間の通信を有効にします。

手順

1. → **Intercom** → **Session Settings** をタップします。
2. 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を設定し、プロトコル1.0を有効にします。

   登録パスワード

   メインステーションの起動パスワード。

   メインステーション IP

   メインステーションのIPアドレス。

   プライベートサーバーIP

   プライベートサーバーのIPアドレス。

   プロトコル 1.0 を有効にする

   有効化後、デバイスは従来のプロトコルを通じてメインステーションに登録されます。無効化すると、デバイスは新しいプロトコルを通じてメインステーションに登録されます。
3. **保存**をタップしてください。

通話時間制限設定

最大通話時間を設定します。

→ **Intercom**→ **Call Settings** をタップします。

最大通信時間を設定します。**保存**をタップします。

注意

最大通話時間の設定範囲は90秒から120秒です。

ボタンを押して通話

手順

1. （電話）→ **Intercom（インターコム）→ Press Button to Call**（ボタンを押して通話）をタップします。

2. 必要に応じて「**通話**」または「**コールセンター**」をタップしてください。

番号設定

ルームSIPに電話をかけることで、そのルームに電話をかけることができます。

手順

1. をタップ → **インターコム** → **番号設定**。

2. 「**+**」をタップし、**部屋番号**と**SIP番号**を入力します。

3. **保存**をタップします。

8.4.10 音声設定

手順

1. （インターコム）→ **Audio（音声**）をタップします。

2. **オプション：**入力および出力の音量を設定します。

8.4.11 顔パラメータ設定

顔パラメータを設定します。

顔パラメータ設定

（設定）→ **Smart（スマート）→ Face Recognition Parameters（顔認識パラメータ**）をタップします。

顔認証偽装防止

ライブ顔検出機能を有効または無効にします。機能を有効にすると、デバイスは人物が生きているかどうかを認識できます。

生体顔検出セキュリティレベル

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

1:1照合閾値

1対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は低くなりますが、誤拒否率は高くなります。

1:N照合閾値

1対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。

顔認識タイムアウト値（秒）

顔認識のタイムアウト期間を設定します。顔認識時間が設定値を超えると、デバイスは顔認識タイムアウトを通知します。

指紋パラメータ

→ Smart → Fingerprint Parameters をタップします。

指紋セキュリティレベル

指紋認証のセキュリティレベルを設定できます。設定するセキュリティレベルが高いほど、誤認率（FAR）は低くなります。設定するセキュリティレベルが高いほど、誤拒否率（FRR）は低くなります。

フェイスマスク検出パラメータ

マスク着用顔検出

マスク着用時の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。マスク着用時の顔検出における1対Nマッチングの閾値、ECOモード、および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。

マスク着用時の顔認証と顔認証（1:1）

1:1 照合モードでマスク着用時の顔認証を行う場合、照合値を設定します。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。

マスク着用時の顔 1:N マッチングのしきい値

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。

注記

機能は機種によって異なります。詳細は実際のデバイスを参照してください。

設定を保存するには「**保存**」をタップしてください。

8.4.12 プライバシーパラメータの設定

表示設定、画像アップロード、ストレージパラメータを設定します。 → **Configuration → Security → Privacy Settings** をタップします。

認証設定

写真表示/名前表示/社員ID

写真をタップすると、写真、名前、または社員IDの表示を有効にできます。認証が完了すると、システムは結果に選択した内容を表示します。

名前/IDの匿名化

名前/ID情報はアスタリスクで非表示化されます。

写真のアップロードと保存写真をアップロードして保存できます。

登録済み写真の保存

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。

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。

認証時に撮影した画像をアップロード

プラットフォームへの認証時に撮影された画像を自動的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、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。

8.4.13 パスワードモード

パスワードを設定する前に、そのパスワードがデバイスで設定する個人用 PIN なのか、プラットフォームで適用する個人用 PIN なの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 Web 上で作成または編集でき、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または編集でき、デバイスで使用する前に発行する必要があります。デバイスや Web 上では設定できません。

手順

1. をタップ → **セキュリティ → PINモードデバイス設定の個人用PIN**

デバイスまたはウェブ上で作成または編集でき、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個人用PIN

プラットフォーム上で作成または編集でき、使用前にデバイスに発行されます。デバイスやウェブ上では設定できません。

2. **保存**をタップしてください。

8.4.14 アップグレードとメンテナンス

デバイスの再起動、デバイスパラメータの復元、デバイスバージョンのアップグレード。

デバイスの再起動

（デバイス管理）→ **Restart Device（デバイスの再起動**）をタップします。

「再起動」をタップしてデバイスを再起動します。

アップグレード

をタップ → **アップグレード**。

アップグレードをタップしてデバイスをアップグレードします。

注意

アップグレード中は電源を切らないでください。

パラメータの復元

（デフォルト設定）→ **Default**（デフォルト）をタップします。

デフォルト設定に復元

デバイスの IP アドレスとユーザー情報を除き、デバイスの設定がデフォルトに復元されます。

工場出荷時設定に復元

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。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。

8.4.15 オンラインドキュメントを表示

をタップ → **オンライン文書を表示**。**オンライン文書を表示**をタップすると、携帯電話でQRコードをスキャンして詳細を確認できます。

8.4.16 オープンソースソフトウェアライセンスを表示

設定 → システム → システム設定 → バージョン情報 をタップし、**「ライセンスを表示」**をタップすると、デバイスのライセンスを確認できます。

第9章 Webブラウザによるクイック操作

9.1 パスワードの変更

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「」をクリックして、**パスワード**変更ページに進みます。セキュリティの質問はドロップダウンリストから選択し、回答を入力できます。

「次へ」をクリックして設定を完了します。または**「スキップ」**をクリックしてこの手順を省略できます。

9.2 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「」をクリックして、**デバイス**言語設定ページに入ります。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。

9.3 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、**「Next」**をクリックして**「Time Settings」**ページに入ります。

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、**「コンピューターの時刻と同期する」に**チェックを入れて、デバイスの時刻をコンピューター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、および間隔を設定できます。

夏時間

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。

9.4 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

認証時に画像を自動的に保存します。

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します。

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。**「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。

9.5 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

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てください。

注意

アップロードする画像は、200 K 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、カードの特性を選択するには、**「カードを追加」**をクリックしてください。

注

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。

注記

最大10個の指紋を登録できます。

9.6 番号と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 外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。

4. 設定後、**[完了]**をクリックして設定を保存します。

第10章 Webブラウザによる操作

10.1 ログイン

Web 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
デバイスがアクティベートされていることを確認してください。

Webブラウザ経由でログイン

ウェブ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。

10.2 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、**確認方法**を選択してください。

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てください。

メール認証

1. QRコードをエクスポートし、***pw_recovery@hikvision.com*** 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. 確認コードを「確認コード」欄に入力し、本人確認を行ってください。**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。

10.3 ヘルプ

10.3.1 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。

ライセンスを表示するには、右上の「」→「**Open Source Software Statement**」をクリックしてください。

10.3.2 オンラインヘルプドキュメントの閲覧

Web 設定のヘルプ文書を閲覧できます。

→ **オンラインドキュメント**をクリックすると、ドキュメントを表示できます。

10.4 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。

10.5 ウェブブラウザ経由のクイック操作

10.5.1 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「」をクリックして、**パスワード**変更ページに入ります。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、回答を入力できます。

「**次へ**」をクリックして設定を完了します。または「**スキップ**」をクリックしてこの手順をスキップします。

10.5.2 言語の選択

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「」をクリックして、**デバイス**言語設定ページに入ります。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。

10.5.3 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、「**Next**」をクリックして「**Time Settings**」ページに入ります。

タイムゾーン

ドロップダウンリストからデバイスのタイムゾーンを選択してください。

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。

夏時間

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。

設定を保存して次のパラメータに進むには「**次へ**」をクリックしてください。または時間設定をスキップするには「**スキップ**」をクリックしてください。

10.5.4 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

認証時に画像を自動的に保存します。

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します。

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。

リンクカメラ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

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。**「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。

10.5.5 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と名前を入力してください。

3. 追加する認証情報を選択してください。

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、200 K 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、カードの特性を選択するには、**「カードを追加」**をクリックしてください。

注

最大50枚のカードに対応しています。

3) 指紋を追加するには**「指紋を追加」**をクリックしてください。

注意

最大10個の指紋を登録できます。

10.5.6 番号と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。前の設定が完了したら、**「Next」**をクリックして**「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

- 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**、**ユニット番号**、**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「**外部ドアステーション**」に設定した場合、**外部ドアステーション番号**を設定できます。

コミュニティ番号を設定できます。

デバイス種別

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ます。

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

設置済みドアステーション番号を設定してください

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。

外部ドアステーション番号

設置されたデバイス外ドアステーション番号を設定してください

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サーバーの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。

4. 設定後、「**完了**」をクリックして設定を保存します。

10.6 ユーザー管理

「**追加**」をクリックして、基本情報、証明書、認証設定を含む対象者の情報を追加します。

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すると、名前を編集できます。変更した名前がデバイスに適用されます。**人物の役割**を選択してください。

設定を保存するには「**保存**」をクリックしてください。

許可時間を設定

「ユーザー管理」→「追加」をクリックし、「ユーザー追加」ページに入ります。
長期有効ユーザーを有効にするか、**長期有効ユーザー**を設定すると、実際のニーズに応じて設定された期間内にのみ権限を持つことができます。
「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。
設定を保存するには**「保存」**をクリックしてください。

デバイス番号を設定

「人物管理」→「人物追加」→「追加」をクリックして「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ます。
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]**をクリックします。

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」をクリックして「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

メモ
指紋機能をサポートしている端末のみ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。

PINを追加

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。
PINモードが「**デバイス設定の個人用PIN**」に設定されてい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

人物管理ページで、削除が必要な人物にチェックを入れ、**「削除」**をクリックします。**「すべてクリア」**をクリックすると、すべての人物がクリアされます。

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。

10.7 概要

デバイスのライブ映像、リンクされたデバイス、担当者情報、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。

をクリックしてください。
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できます。

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

接続済みデバイスの数量とステータスを確認できます。

注記

[詳細を表示]をクリックすると、[イベント検索]ページに移動できます。

個人情報の

追加済みおよび未追加の個人認証情報を確認できます。

ネットワークステータス

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、イベントの容量を確認できます。

注意

指紋モジュールを搭載したデバイスのみ、指紋容量を表示できます。

10.8 アクセス制御アプリケーション

10.8.1 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、設定されたルートに従って、担当者が順番に認証を行う必要があります。この機能をサポートしているのはサブデバイスだけで、認証による一方向の通過のみがサポートされています。

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ー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、アンチパスバックのために相互接続できません。

10.8.2 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の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する必要があります。**「サブデバイス管理」**をクリックすると、デバイスのステータスを確認したり、デバイスを削除したりできます。
   - サブデバイスとして設定する場合、アクセスコントローラーのパラメータ（**メインデバイスのIPアドレス**、**ポート番号**、**パスワード**）を設定する必要があります。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、アンチパスバックのために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**

   カード認証によるアンチパスバックルーチンの判定

   実際の通行状況による

   実際のカード開錠によるアンチパスバックルーチンの判定
5. **OK**をクリックしてください。

10.9 アクセス制御管理

10.9.1 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。
イベントタイプ、社員 ID、名前、カード番号、開始時間、終了時間などの検索条件を入力し、「**検索**」をクリックします。
結果が右パネルに表示されます。

10.9.2 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

ドアを選択して関連パラメータを設定します。

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はデバイスと連動するドア、ドア2はセキュリティドア制御ユニットと連動するドアです。
その他のドアパラメータを設定し、「**保存**」をクリックします。

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状態を確認できます。**更新**をクリックするとデバイスの状態が更新されます。

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のドアロックの開放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。

開錠後の動作時間である開放時間を設定します。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。

保存をクリックします。

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た後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警報を設定します。ロック動作時間に達した後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発します。0に設定すると警報は無効になります。

保存をクリックします。

ドア閉時ロック設定

ドア閉時ロック機能を設定できます。

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経由でドア磁気センサータイプを設定

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「閉状態保持」または「開状態保持」から選択します。デフォルトでは**閉状態保持**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状態または常時閉状態に設定します。

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。**退出ボタンタイプ**を設定します。デフォルトでは常時開放（特別な要件を除く）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。

保存をクリックします。

PC Web 経由で延長開放時間を設定する

延長アクセス権限を持つ者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者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。

「保存」をクリックします。

PC Web経由で「最初の利用者によるドア開放継続時間」を設定

最初の人が認証されると、複数人がドアにアクセスしたり、その他の認証操作を行ったりできるようになります。

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不可で、通常4～8桁で構成されます。

PCウェブ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がスーパーパスワードを入力することでドアを開錠できます。

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。

注記
脅迫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。

10.9.3 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する。

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**を表示します。

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、設定ページに入ります。
2. **認証デバイスを**有効化します。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。

メインカードリーダーを端末として選択する場合、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は、**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。

注記
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。

初回認証方式の制御

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方法を選択できます。

保存をクリックします。

PC Webで顔認証を手動でトリガー

「顔認証による手動認証トリガー」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が端末として選択されている場合、**「顔認証による手動認証トリガー」**をクリックして有効にし、認証モードを選択します。

シングル認識

前回の顔認証が完了した後、成功・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

認識を開始すると、デバイスがスリープモードに入るまで顔による認識が可能です。

保存をクリックしてください。

PC Web 経由で認識間隔を設定

認証時に連続する2回の顔認証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経由での改ざん検知の有効化/無効化

改ざん検出を有効にすると、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、**改ざん検出を**有効または無効にします。機能を有効にすると、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。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異なる側またはメインカードリーダーと同じ側**として選択できます。**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、「**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、入力済みの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。

10.9.4 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

   これを有効にし、認証に合格すると、ボタン設定の呼び出し先が自動的に呼び出され、遠隔でドアが開きます。

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。

10.9.5 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、タイムバーで時間枠をドラッグします。

保存をクリックします。

10.9.6 顔認証パラメータの設定

Webブラウザ経由の顔認証偽装防止機能を有効/無効にする

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での顔適用時には、この機能はサポートされていません。

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。偽装検知レベルを選択し、**保存**をクリックします。
一般、上級、プロフェッショナルから選択できます。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。

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のレンズのピッチ角を設定できます。**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。実際のページをご参照ください。

ピッチ角を設定し、「**保存**」をクリックしてください。

PC Web経由でヨー角を設定

顔認識および認証時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**をクリックします。

PC Web経由での適用用顔画像品質グレードの設定

顔認証の判定は、成功するためには閾値よりも高いスコアが必要です。**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。

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。

適用する顔写真の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 Web 経由で 1:1 顔グレードのしきい値を設定

1:1顔認証グレード閾値を設定します。

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、認証失敗の通知が発生しやすくなります。

PC Web経由で顔1:1照合閾値を設定

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。

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、録画、または全画面表示に切り替えます。

PC Web経由での指紋パラメータ設定

デバイスの指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。

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ECOモードの有効化/無効化

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や暗所環境でも顔認証が可能です。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 一致閾値（ECO）**、**マスク着用顔 1:1 一致閾値**、**マスク着用顔 1:N 一致閾値（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、端末は警告を表示し、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照合モードで照合精度値を設定します。値が大きいほど誤認率は低くなりますが、誤拒否率が高くなります。最大値は100です。

マスク着用顔&顔（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が低下し、誤拒否率が上昇します。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。

10.9.7 カード設定

PC Web 経由での NFC 保護の有効化/無効化

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カード有効化」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カードを読み取れます。モバイル端末でアクセス制御デバイスのデータを取得した場合、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、NFC機能を無効化できます。

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るようになります。**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**をクリックしてください。

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、このカードリーダーでEMカードをスワイプすることもできます。
- 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、デバイス上でカードをスワイプすることは無効です。

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 カードを認識し、ユーザーはデバイスで CPU カードをスワイプできるようになります。**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。

CPUカードの有効化をクリックします。

クリック**してCPUカードの内容を読み取る機能を有効にします**。有効化後、デバイスはCPUカードから内容を読み取れます。

保存をクリックしてください。

DESFireカードの設定

DESFireカードとDESFireカードの内容読み取りを有効にできます。

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。**DESFire カードの**有効化と **DESFire カード**の内容読み取りを選択し、**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カードを有効にする**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

カード番号認証パラメータの設定

3 バイト

デバイスは3バイト読み取りでカードを読み取ります。

4 バイト

デバイスは4バイト単位でカードを読み取ります。

10.9.8 リモート検証の設定

デバイスは人物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否かを判断します。

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開門するかどうかを確認します。

遠隔での人物タイプ検証

「リモートでの人物タイプ検証」を選択します。

認証情報をローカルで検証

機能を有効にすると、デバイスは許可を確認しますが、プランテンプレートの推定は行いません。

リモート認証のタイムアウト時間

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。

10.9.9 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として「**古いイベントを定期的に削除**」「**指定時間経過後に古いイベントを削除**」「**上書き保存**」を選択できます。

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て、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、すべてのイベントが削除されます。

指定時刻による古いイベントの削除

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

保存済みイベントが容量の95%を超えた場合、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

認証結果の内容（写真、氏名、社員ID、体温など）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、氏名、社員IDなど）を確認します。
実際の必要に応じて、**名前**非識別化と**ID非識別化**をチェックします。非識別化後、名前とID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、認証結果が設定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の設定

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します。

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します。

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。

マット写真モードを選択すると、デバイスは顔のみを撮影します。最大写真サイズを設定できます。

登録画像の保存

この機能を有効にすると、登録された顔画像がシステムに保存されます。

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

通話中に撮影した画像をアップロード

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

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。プラットフォームではPINを設定できません。

保存をクリックしてください。

10.9.10 通話設定

Web経由でのデバイス番号設定

本機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。

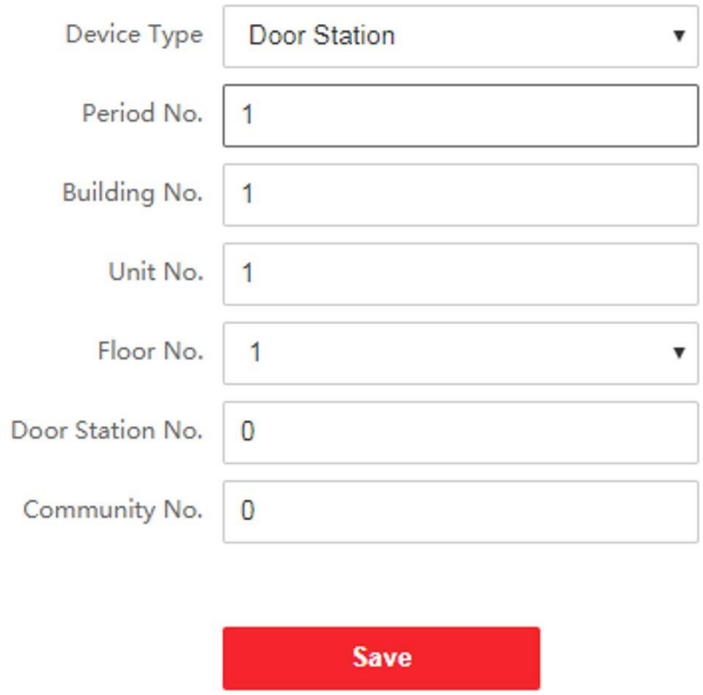


図10-1 デバイス番号設定

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

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。

注記

デバイスタイプを変更した場合は、デバイスを再起動する必要があります。

階数

設置階を設定してください。

ドアステーション番号

設置階を設定してください。

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。
- 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。

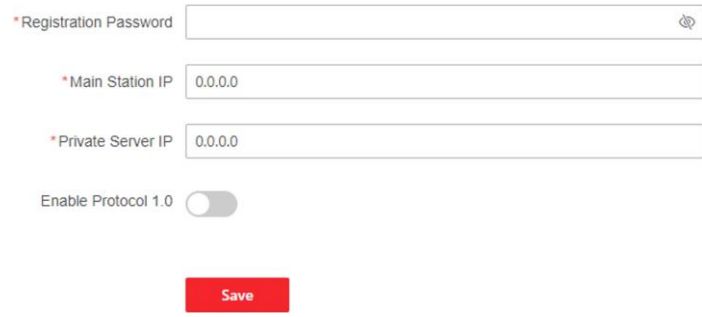


図10-2 ビデオインターコムネットワーク

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。**自動応答を**有効にできます。

注記

最大通信時間の設定範囲は90秒から120秒です。**保存**をクリックします。

PC Webからボタンを押して通話する

手順

1. **アクセス制御 → 通話設定 → ボタンを押して通話** をクリックし、設定ページに入ります。

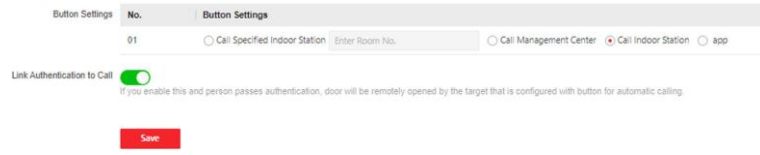


図 10-3 ボタンを押して呼び出し

2. 必要に応じて「**指定室内機を呼び出す**」「**管理センターを呼び出す**」「**室内機を呼び出す**」または「**アプリ**」を選択してください。

注意

「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**「リンク認証による呼び出し」**を有効にしてください。有効にすると、認証を通過した人物が、自動呼び出しボタンが設定された対象によってドアを遠隔操作で開けることができます。
4. **保存**をクリックします。

呼び出し優先度

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、呼び出されるデバイスが優先されます。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 による番号設定

ルームのSIP番号を設定します。ルームはSIP番号を介して相互に通信できます。

手順

1. **アクセス制御 → 通話設定 → 番号設定** に移動します。

図10-4 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：[Add]**をクリックしてSIP番号を追加するか、[ ]をクリックして番号を削除します。
4. **[保存]** をクリックします。
5. **オプション：[Delete]** 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。

10.10 デバイス管理

デバイス番号、タイプ、IPアドレス、シリアル番号、モデル、バージョン、階数、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室内機やサブドアステーションを追加し、デバイスの管理、アップグレード、削除が可能です。

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**、**フロア番号**を入力します（屋内ステーションの場合は**フロア番号**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　USBフラッシュドライブ（デバイス情報を含む）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]**をクリックして、デバイス情報ファイルをUSBフラッシュドライブにエクスポートします。

10.11 システム構成

10.11.1 PC Web経由でデバイス情報を表示

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 → 基本情報の順に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確認できます。

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。

10.11.2 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、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。

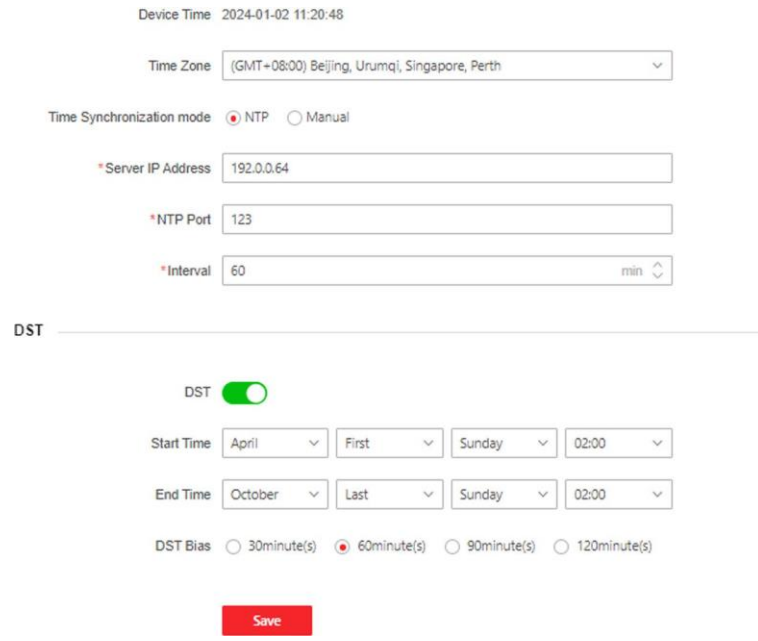


図10-5 時刻設定

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、デバイスが置かれてい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、間隔を設定できます。

10.11.3 管理者のパスワード変更

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ます。

4. 新しいパスワードを確認します。

5. **保存**をクリックします。

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）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、設置業者および／またはエンドユーザーの責任となります。

10.11.4 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. 実際の必要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ます。

3. デバイスのパスワードを入力し、**[OK]**をクリックして変更を確認します。

10.11.5 PC Web経由でデバイスの武装/武装解除情報を表示

デバイスの武装タイプと武装IPアドレスを確認します。

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 → 武装/解除情報 に移動します。

デバイスの武装/解除情報を確認できます。「**更新**」をクリックするとページが更新されます。

10.11.6 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。

注意

一部のモデルのみこの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

動作モードを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。

10.11.7 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。

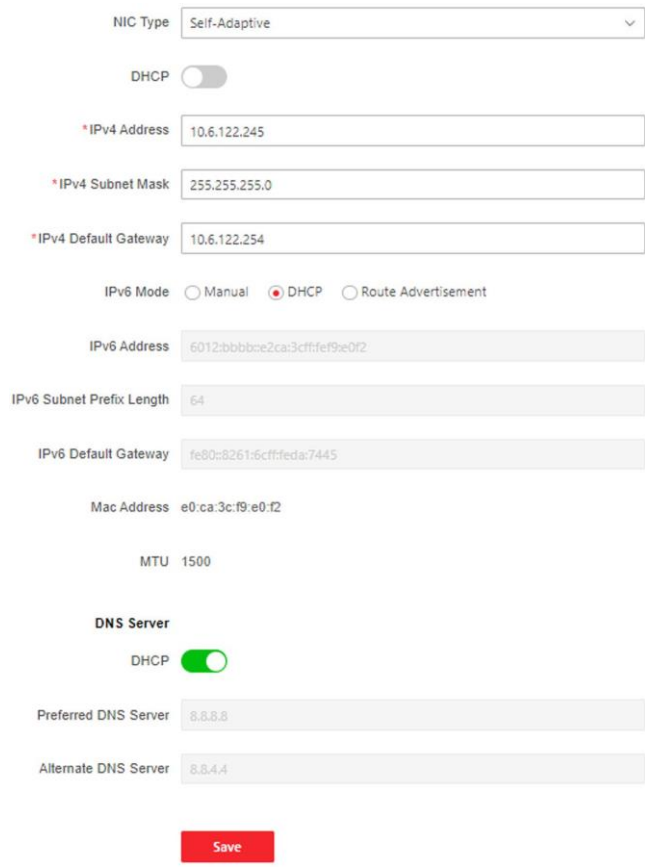


図 10-6 TCP/IP 設定ページ

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タイプを選択してください。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、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 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自動的に割り当てます。

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。

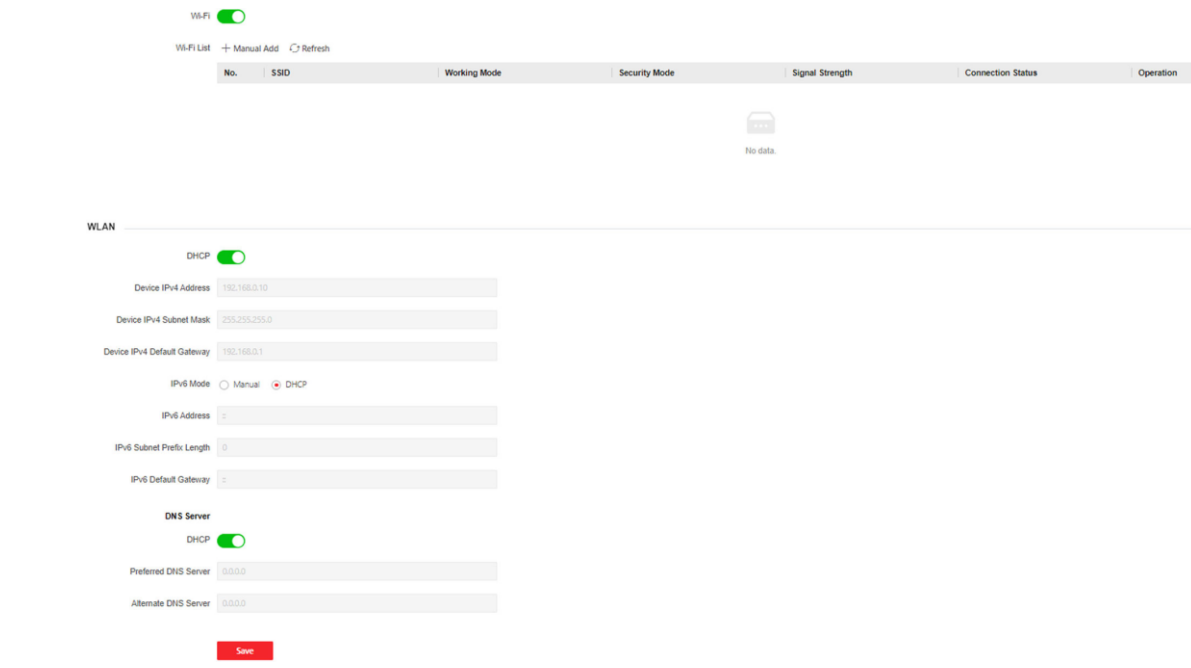


図 10-7 Wi-Fi 設定ページ

2. **Wi-Fi** をチェックします。
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、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、システムが自動的にIPアドレス、サブネットマスク、デフォルトゲートウェイを割り当てます。

5. 保存をクリックします。

PC Web経由でポートを設定

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

HTTPの有効化/無効化

HTTP 機能を有効にして、ブラウザの訪問セキュリティを向上させます。

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

パラメータの設定後、**[保存]をクリックしてください**。

HTTP ポート

ブラウザでログインする際は、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プロトコルでアラーム情報を宛先IPまたはドメイン名に送信します。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 に移動します。ポートを確認します。

PC Web経由でWebSocketを設定

WebSocket と WebSockets ポートを表示します。

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 に移動します。
WebSocket および 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

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. **有効化**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 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、ISUP アラームセンターのポートなど、ISUP リスニングパラメータを設定します。
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。

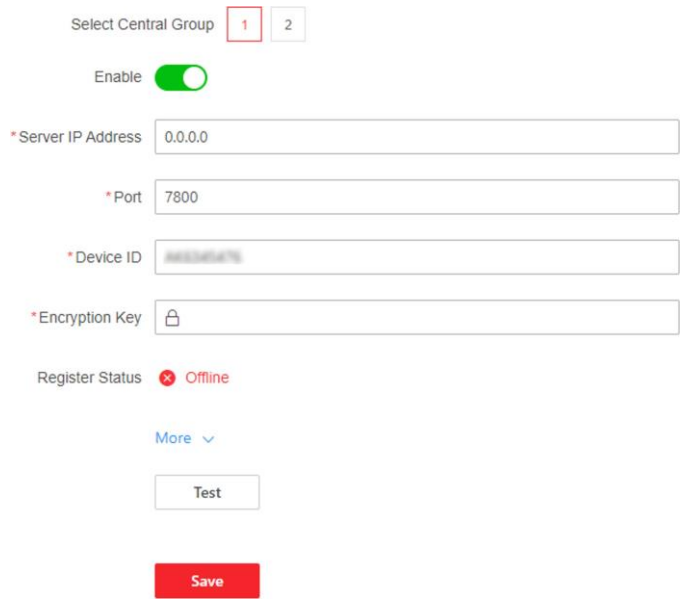


図10-8 OTAPの設定

2. OTAPを**有効にする**にはクリックしてください。
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]** をクリックして、デバイスがサーバーに接続し、正常に登録できることを確認します。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**確認します。
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表示します。操作アイコンを上下にドラッグして、ネットワークの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により、デバイスをプラットフォーム経由で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** の順にクリックし、設定ページに入ります。

注記
Hik-Connectはモバイル端末用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、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**」にチェックを入れます。
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. 確認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

8～32文字（a～z、A～Z）または数字（0～9）、大文字小文字を区別します。8文字以上の英数字の組み合わせの使用をお勧めします。

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**をクリックします。

10.11.8 PC Web 経由でビデオおよびオーディオパラメータを設定

Webブラウザ経由でビデオパラメータを設定

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 の順に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ブラウザ経由でのオーディオパラメータ設定

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てください。入力音量と出力音量はスライドで調整します。

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。

保存をクリックしてください。

10.11.9 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 No. を設定します。

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

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インターフェース経由で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。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

RS-485 プロトコルでデバイスが通信するときのボーレート。

PC Web 経由でウィーガンドパラメータを設定

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 → システム構成 → アクセス構成 → ウィーガンド設定** をクリックします。

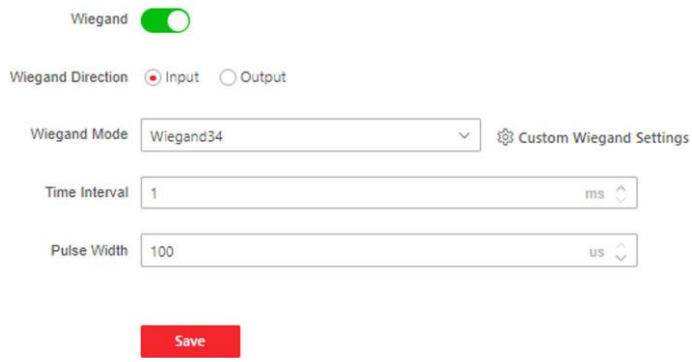


図10-9 ウィーガンド設定ページ

2. **Wiegand** チェックボックスをオンにして Wiegand 機能を有効にします。
3. 送信方向を設定します。

入力

このデバイスは、ウィーガンドカードリーダーに接続できます。

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Wiegand 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。

10.11.10 画像パラメータ設定

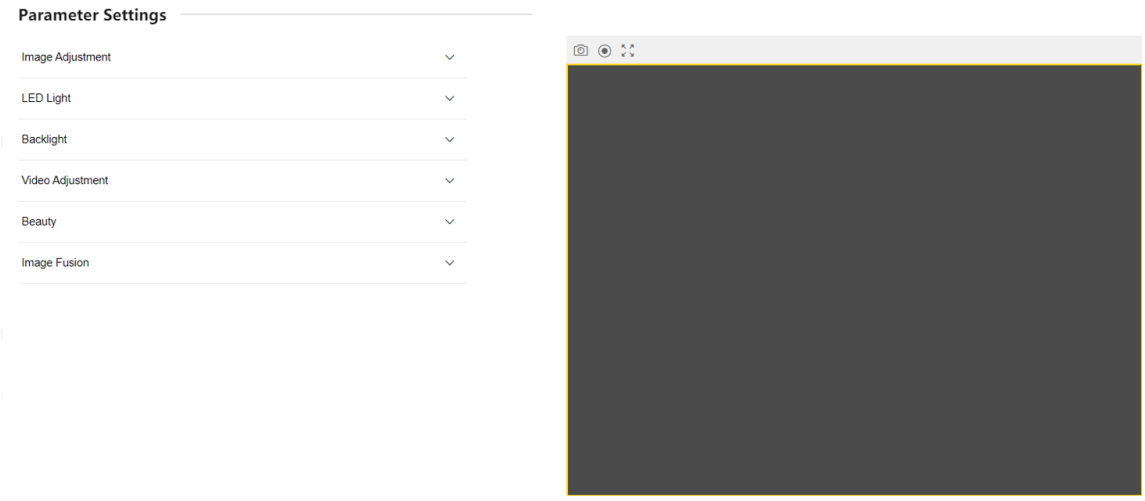


図 10-10 表示設定

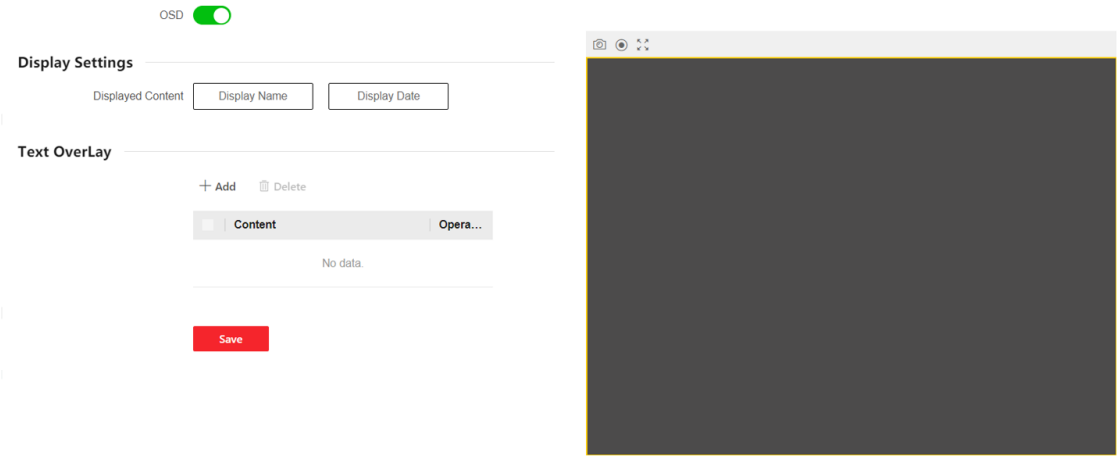


図 10-11 OSD 設定

PC Web 経由で輝度/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経由でビデオ標準を設定する

ライブビューページのビデオ規格を設定できます。

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。

デフォルト設定を復元をクリックしてデフォルトに戻します。

10.11.11 連携設定

設定されたイベントがトリガーされた場合、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。連携タイプとして「**イベント連携**」「**カード連携**」「**従業員ID連携**」のいずれかを選択します。

- **リンクタイプをイベントリンク**として選択すると、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、**カード番号**を入力して**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、**従業員ID**を入力して**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) **リンクキャプチャを**有効にします。

5. 設定を有効にするには、**[保存] をクリックします**。

10.11.12 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（出勤定義のルール：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）をシフトグループに割り当てて、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する。
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、認証は編集後の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。

10.12 設定

10.12.1 PC Web経由でスタンバイ画像を設定

スタンバイ状態に入る時間、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、スタンバイ画像のパラメータを設定します。

システムとメンテナンス → 設定 → 画面表示 に移動します。

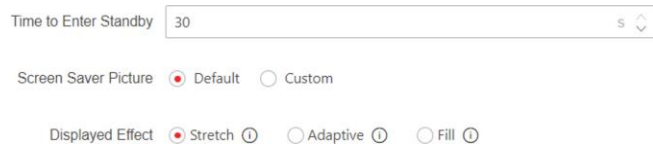


図 10-12 スタンバイ画像設定

スタンバイ画像のパラメータを設定し、［**保存**］をクリックします。

スタンバイに入るまでの時間

設定され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。

スクリーンセーバー画像

スタンバイ画像をデフォルト画像またはカスタム画像として設定します。**カスタム**を選択し、**+**をクリックしてローカルブラウズからスタンバイ画像をアップロードします。

注意
3枚までの画像が許可されます。単一画像サイズ：1024 KB以下、形式：jpg。

表示効果

スタンバイ画像の表示効果を「**引き伸ばし**」、「**自動調整**」、「**塗りつぶし**」から選択します。

スライドショーの間隔

複数の画像を追加した場合、画像の切り替え時間を設定できます。

10.12.2 PC Web経由でスリープ時間を設定

設定時間経過後、デバイスはスリープモードに移行します。この機能により消費電力の削減が可能です。

システムとメンテナンス → 設定 → 画面表示 に移動します。

図10-13 スリープ設定

スリープ時間をスライドで設定し、「**保存**」をクリックします。

10.12.3 PC Web経由での認証デスクのカスタマイズ

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。**アクセスモード**

   デバイス認証ページに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。

   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エリアと認証エリアが表示されます。クイック操作エリアでは機能別のカスタマイズ可能なショートカットキーをサポートします。

シンプル

このモードを選択すると、認証ページのライブビューは無効になります。認証後、人物名、社員ID、顔写真はいずれも非表示になります。

3. **適用**をクリックしてください。

10.12.4 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。

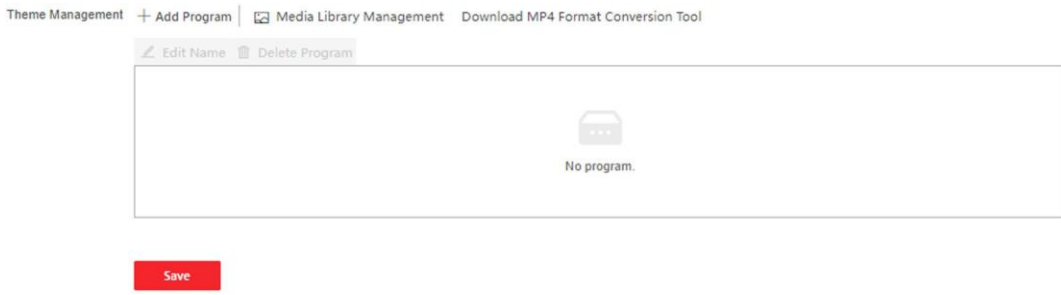


図10-14 通知公開 MP4形式変換ツールのダ

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」**をクリックしてください。

マテリアル管理

「+ 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、**+** をクリックしてローカル PC から画像またはビデオをアップロードします。

注

現時点では、追加できるテーマは1つだけです。

プログラムの追加

プログラム名を設定し、プログラムタイプを選択できます。

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、テンプレート、内容、メインタイトルとサブタイトルのフォントサイズと色を設定できます。背景画像もカスタマイズできます。

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

テーマを作成した後、そのテーマを選択し、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、正確な開始時刻と終了時刻を編集できます。

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。

10.12.5 PC Web経由でのスケジュール設定

認証成功時と失敗時の出力オーディオコンテンツ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。

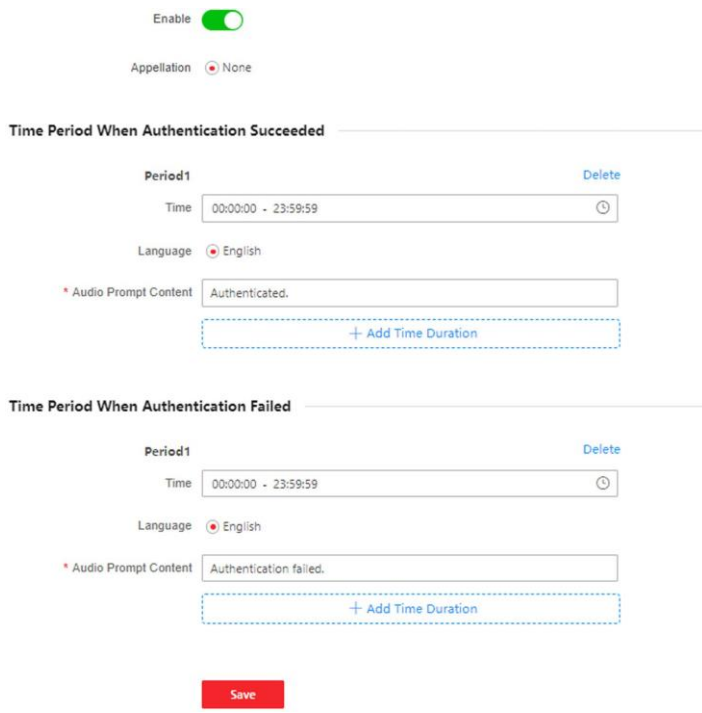


図 10-15 プロンプトスケジュール

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) **時間期間を追加**をクリックします。

2) 時間範囲を設定します。

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1〜3を繰り返します。

5) **オプション:** [ ] をクリックして設定済みの時間制限を削除します。

6. 認証が失敗した際の時間制限を設定します。

1) **「時間制限を追加」**をクリックします。

2) 時間設定を設定します。

注記

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) オーディオ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：**設定した時間範囲を削除するには、をクリックします。

7. [保存] をクリックして設定を保存します。

10.12.6 PC Web経由でプロンプト音声をカスタマイズする

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 10-16 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、WAV 形式で 512 kb 未満である必要があります。

10.12.7 PC Web 経由で認証結果テキストを設定

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。

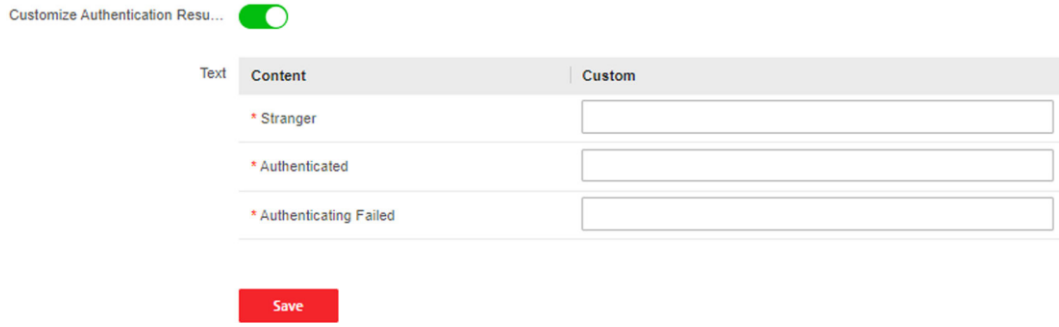


図10-17 認証結果テキスト

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。

10.13 システムとメンテナンス

10.13.1 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**をクリックしてデバイスを再起動します。

10.13.2 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の種類を選択します。「」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**更新バージョン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

- 周辺機器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から**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。

10.13.3 復元

Webブラウザ経由での工場出荷時設定への復元

デバイスの工場出荷時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してください。

PC Web経由でのデフォルト設定への復元

デバイスのデフォルト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。
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。

10.13.4 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。

10.13.5 PC Web経由でデバイスパラメータをインポート

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。

10.13.6 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を有効にする**

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出力

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**をクリックするとデバイスログを印刷できます。

PC Web経由でのネットワークパケットキャプチャ

キャプチャするパケットの期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、デバッグを行うことができます。

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をデバッグできます。

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 → プロトコルテスト に移動します。

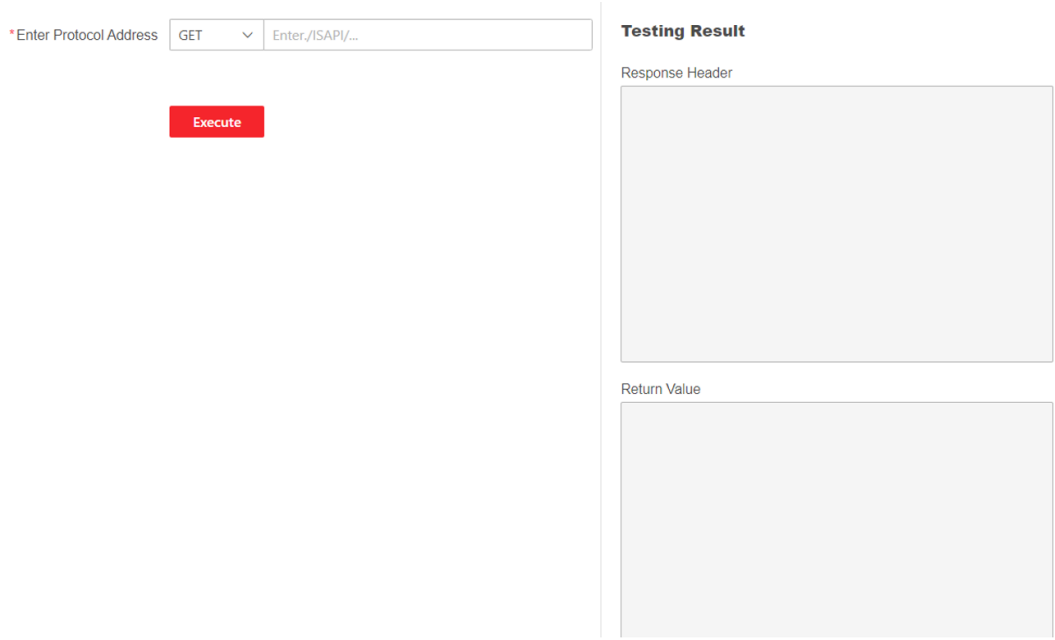


図10-18 プロトコルテスト

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。

レスポンス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。

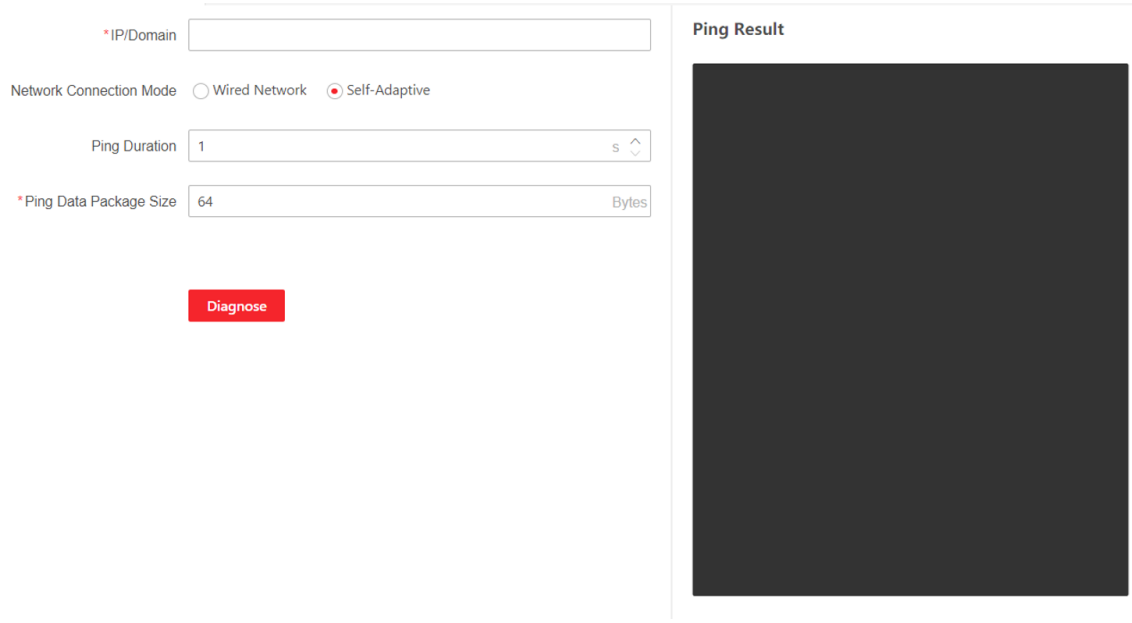


図10-19 ネットワーク診断

PING操作用のデバイス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、ペネトレーションサービスを有効化することで、デバイスのリモート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IP**アドレスと**サーバーポート**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**をクリックしてください。

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。

10.13.7 PC Web経由でログを表示

デバイスのログを検索および表示できます。

システムとメンテナンス → メンテナンス → ログ に移動してください。

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、時刻、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。

10.13.8 PC Web経由の詳細設定

顔認証パラメータ、掌紋認証パラメータの設定、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**をクリックします。

顔認証パラメータ

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** および **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。アンチスプーフィング検出の失敗試行回数制限に達すると、設定されたロック期間中、顔認証がロックされます。

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。

10.13.9 セキュリティ管理

PC Web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

ログイン時およびユーザー情報の確認時に高いセキュリティレベルを適用します。

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。

10.13.10 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. 署名済み証明書をインポートします。
   1) 「**キーのインポート**」領域で証明書タイプを選択し、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**インポート領域で証明書タイプを選択し、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11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

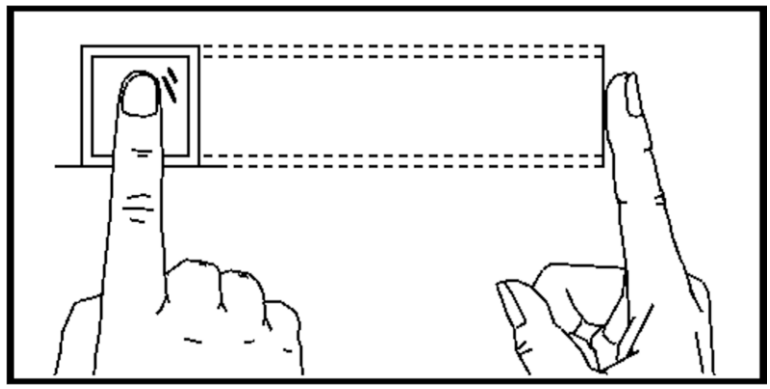
付録 A. 指紋スキャンに関するヒント

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

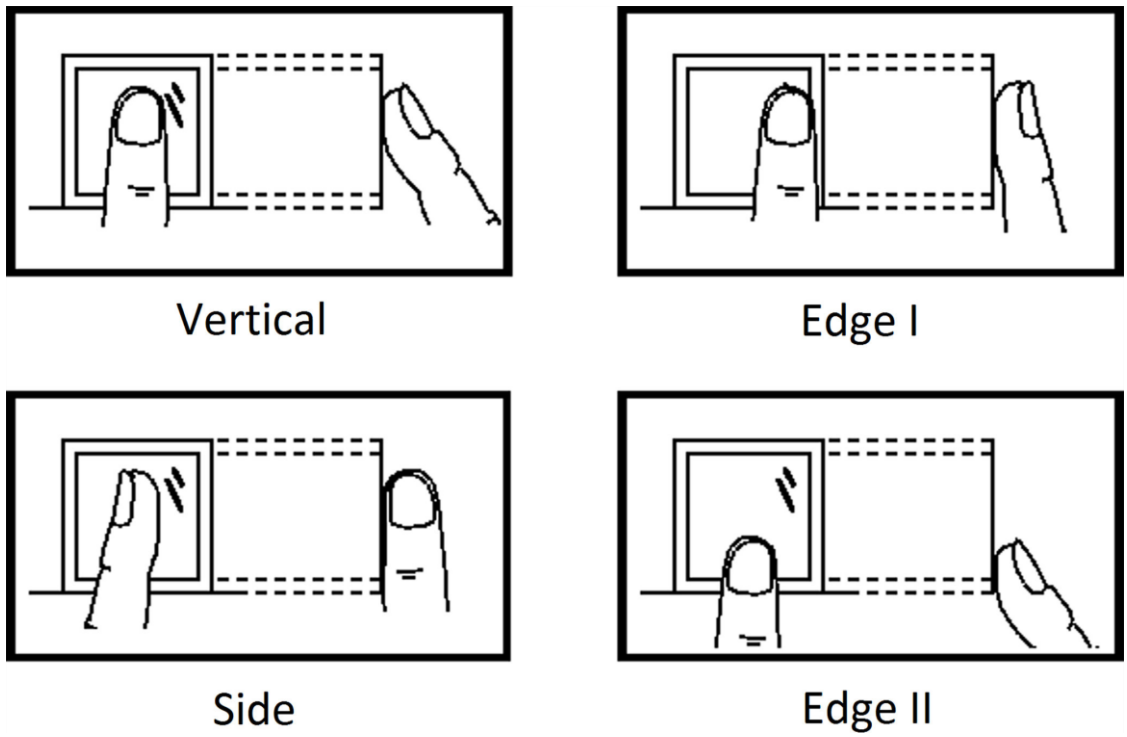
以下の図は指をスキャンする正しい方法です：



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しく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。

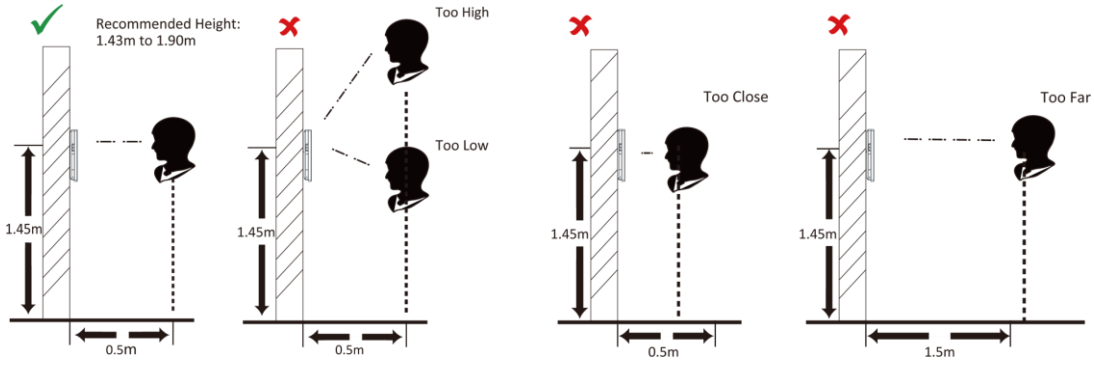
その他

指紋が浅い場合や指紋のスキャンが困難な場合は、他の認証方法の使用をお勧めします。
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・比較時のポイント

顔写真の収集・比較時の位置は以下の通りです：

位置（推奨距離：0.5 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。

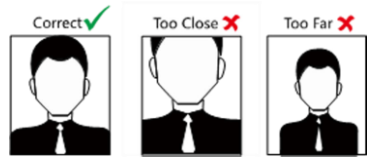
- 帽子、サングラス、その他顔認識機能に影響を与える可能性のあるアクセサリーは着用しないでください。
- 髪が目や耳などを覆わないようにし、濃いメイクは避けてください。

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

顔は撮影範囲の中央に収まるようにしてください。



付録C. 設置環境に関するヒント

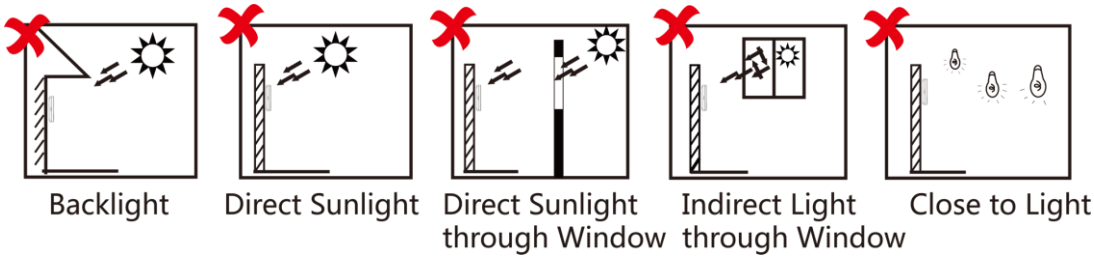
1. 光源の照度基準値

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 D. 寸法

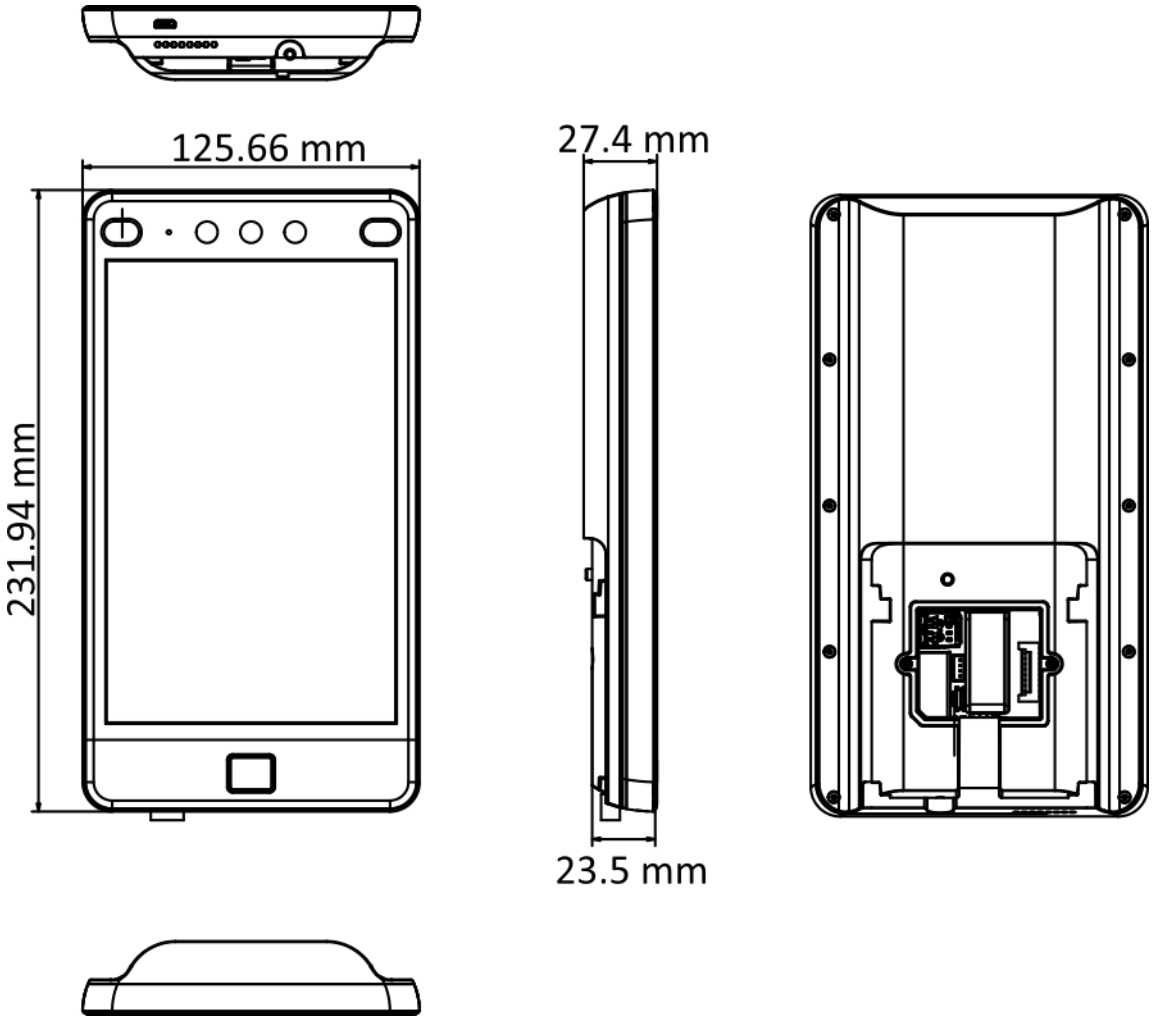


図 D-1 寸法