DS-K3B530X シリーズ スイングバリア

ユーザーマニュアル

法的情報

このドキュメントについて

- この文書には、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、画像、およびその他の情報は、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、ファームウェアのアップデートなどの理由により、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 のウェブサイト (***https://www.hikvision.com***) をご覧ください。別段の合意がない限り、Hangzhou Hikvision Digital Technology Co., Ltd. またはその関連会社 (以下「Hikvision」) は、明示的または黙示的を問わず、いかなる保証も行いません。
- 本ドキュメントは、製品をサポートする専門家の指導と支援を受けてご使用ください。

本製品について

- この製品は、購入し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。
- お選びになった製品がビデオ製品の場合は、以下の QR コードをスキャンして「ビデオ製品の使用に関する取り組み」を入手し、よくお読みください。

知的財産権の承認

- 本ドキュメントに記載される製品に組み込まれた技術に関する著作権および/または特許権は、Hikvisionが所有しています。これには、第三者から取得したライセンスを含む場合があります。
- 本文書の一部（テキスト、画像、グラフィックなど）は、Hikvision に帰属します。本文書のいかなる部分も、書面による許可なく、その全部または一部を、いかなる手段によっても、抜粋、複製、翻訳、または改変することはできません。
- **HIKVISION** およびその他のヒクビジョンの商標およびロゴは、各管轄区域においてヒクビジョンの財産です。
- 本文書で言及されるその他の商標およびロゴは、それぞれの所有者の財産です。

法的免責事項

- 適用される法律で許される最大限の範囲において、本書および本書に記載される製品（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」および「すべての欠陥およびエラーを含む」状態で提供されます。HIKVISION は、明示的または黙示的を問わず、商品性、満足のいく品質、または特定の目的への適合性を含むがこれらに限定されない、いかなる保証も一切行いません。

明示的または黙示的ないかなる保証も提供しません。これには、商品性、満足のいく品質、または特定の目的への適合性に関する保証が含まれますが、これらに限定されません。製品の使用は、お客様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、事業利益の損失、事業の中断、データの損失、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、特別、結果的、偶発的、または間接的な損害について、お客様に対して一切の責任を負いません。システムの破損、または文書の損失を含む損害について、契約違反、不法行為（過失を含む）、製品責任、またはその他の理由に基づくものであっても、製品の使用に関連して生じた場合、HIKVISIONは一切の責任を負いません。これは、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を受けていた場合でも同様です。

- お客様は、インターネットの性質上、セキュリティ上のリスクが内在していることを認識し、サイバー攻撃、ハッカーの攻撃、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な動作、プライバシーの漏洩、その他の損害について、HIKVISION は一切の責任を負わないことを認めます。ウイルス感染、または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な動作、プライバシーの漏洩、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、HIKVISION はタイムリーな技術サポートを提供します。
- あなたは、この製品を適用されるすべての法律に準拠して使用することに同意し、あなたの使用が適用される法律に準拠していることを確保する責任は、あなたのみに帰属します。特に、お客様は、パブリシティ権、知的財産権、データ保護およびその他のプライバシー権を含むがこれらに限定されない、第三者の権利を侵害しない方法で本製品を使用することについて責任を負います。お客様は、大量破壊兵器の開発または製造、化学兵器または生物兵器の開発または製造、核爆発または安全でない核燃料サイクルに関連するいかなる活動、または人権侵害を支援する目的での使用を含みます。
- 本文書と適用法との間に矛盾がある場合は、適用法が優先するものとします。

データ保護

- データを保護するため、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の場合、生体認証データは暗号化方式で製品に保存されます。指紋認証製品の場合、指紋テンプレートのみ保存され、指紋画像を復元することは不可能です。
- データ管理者/処理者として、お客様は、収集、保存、使用、処理、開示、削除など、個人データを処理する場合があります。個人データの保護に関する適用法令を遵守し、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の定期的な見直しおよび評価など、個人データを保護するためのセキュリティ対策を実施することをお勧めします。

規制情報

FCC情報

コンプライアンス責任者が明示的に承認していない変更または修正は、お客様の機器の操作権限を無効にする場合がありますのでご注意ください。

FCC 準拠：この機器は、FCC 規則のパート 15 に準拠したクラス B デジタル機器の制限について試験され、その制限に準拠していることが確認されています。これらの制限は、住宅環境における有害な干渉を合理的に防止するために設定されています。この機器は、無線周波エネルギーを発生、使用、および放射します。指示に従って設置および使用しない場合、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、特定の設置において干渉が発生しないことは保証できません。この機器がラジオやテレビの受信に有害な干渉を与えている場合（機器の電源をオフにして確認してください）、以下のいずれかの方法で干渉を修正してください。

—受信アンテナの向きや位置を変更する。

—機器と受信機との距離を離す。

—機器を、受信機が接続されている回路とは異なる回路のコンセントに接続する。

—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

この機器は、放射器と身体の間に最低20cmの距離を保って設置し、使用してください。

FCC 条件

この装置はFCC規則の第15部に準拠しています。操作は次の2つの条件に準拠する必要があります:

1. この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、受信した干渉（不要な動作を引き起こす可能性のある干渉を含む）をすべて受け入れる必要があります。

EU適合宣言

CE

この製品および付属品（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 に記載された、適用

EMC 指令 2014/30/EU、RE 指令 2014/53/EU、RoHS 指令 2011/65/EU

2012/19/EU（WEEE指令）：このマークが付いた製品は、欧州連合内で分別収集されない一般廃棄物として処分できません。適切なリサイクルのため、同等の新品を購入する際は製品を販売店に返却するか、指定の回収場所に処分してください。詳細情報はwww.recyclethis.infoをご確認ください。

2006/66/EC（電池指令）：この製品には、欧州連合では一般廃棄物として処分できない電池が含まれています。電池の詳細については、製品のドキュメントをご覧ください。電池には、カドミウム（Cd）、鉛（Pb）、水銀（Hg）を示す文字を含むこの記号が記載されています。適切なリサイクルのため、電池を販売店または指定の回収場所に返却してください。詳細については、www.recyclethis.info をご覧ください。

安全に関する指示

これらの指示は、ユーザーが製品を正しく使用し、危険や財産の損失を防止するために用意されています。
予防措置は、危険と注意に分類されます:
危険：警告を無視すると、重大な怪我や死亡事故を引き起こす可能性があります。
注意: 注意を無視すると、けがや機器の損傷を引き起こす可能性があります。

⚠	⚠
危険: 重大な怪我や死亡を防止するため、これらの安全対策を必ず遵守してください。	**注意：**怪我や材料の損傷を防ぐため、これらの注意事項に従ってください。

⚠危険:

- すべての電子操作は、お住まいの地域の電気安全規制、防火規制、およびその他の関連規制を厳守してください。
- 弊社が提供する電源アダプタをご使用ください。消費電力は、必要値以上にしてください。
- 複数の機器を 1 つの電源アダプタに接続しないでください。アダプタの過負荷により、過熱や火災の原因となることがあります。
- デバイスの配線、設置、分解を行う前に、電源が切れていることを確認してください。
  メンテナンスのために上部キャップを開け、装置の電源を入れる場合は、次の点に注意してください。
  1. 操作者が誤って怪我をしないように、ファンの電源を切ってください。
  2. 裸の高電圧部品に触れないでください。
  3. メンテナンス後、スイッチの配線順序が正しいことを確認してください。
- 本製品の配線、設置、分解を行う場合は、必ず電源を切ってください。
- 製品を壁や天井に取り付ける場合は、しっかりと固定してください。
- 本製品から煙、異臭、異音が発生した場合は、直ちに電源を切り、電源コードをコンセントから抜き、サービスセンターにご連絡ください。
- 電池を誤飲しないでください。化学やけどの危険があります。
  この製品にはコイン型/ボタン型電池が含まれています。コイン型/ボタン型電池を誤飲すると、2時間以内に重度の内部やけどを引き起こし、死亡する可能性があります。
  新しい電池や使用済みの電池は、子供の手の届かない場所に保管してください。電池ケースがしっかりと閉まらない場合は、本製品の使用を中止し、子供の手の届かない場所に保管してください。電池を飲み込んだり、体内に挿入したりした場合は、直ちに医師の診断を受けてください。
- 製品が正常に動作しない場合は、販売店または最寄りのサービスセンターまでご連絡ください。絶対に自分で分解しないでください。（不正な修理やメンテナンスによる問題については、当社は一切の責任を負いません。）

⚠注意:

- ステンレス鋼は、一部の条件下で腐食する可能性があります。ステンレス鋼クリーナーを使用して、装置を清掃し手入れしてください。毎月清掃することをおすすめします。
- 装置を落としたり、物理的な衝撃を与えたり、高電磁波放射にさらさないでください。振動する表面や衝撃を受ける場所への設置は避けてください（無視すると装置が損傷する可能性があります）。
- 本装置は、極端な高温（詳細な使用温度については、本装置の仕様書を参照してください）、低温、ほこりや湿気の多い場所に置かないでください。また、強い電磁波にさらさないでください。
- 室内用装置のカバーは、雨や湿気から保護してください。
- 装置を直射日光、換気不良の場所、またはヒーターやラジエーターなどの熱源にさらさないでください（無視すると火災の危険があります）。
- 装置を太陽や極端に明るい方向に向けないでください。そうすると、画像の白化やにじみが発生する可能性があります（これは故障ではありませんが）、同時にセンサーの耐久性に影響を与える可能性があります。
- 装置カバーを開ける際は、付属の手袋を使用してください。指先の汗に含まれる酸が装置カバーの表面コーティングを腐食するおそれがあります。
- デバイスカバーの内外表面を清掃する際は、柔らかく乾いた布を使用し、アルカリ性洗剤は使用しないでください。
- 梱包材は開封後、今後の使用のために保管してください。万一故障が発生した場合は、元の梱包材と共に工場へ返送してください。元の梱包材なしで輸送した場合、デバイスに損傷が生じ、追加費用が発生する可能性があります。
- バッテリーの不適切な使用または交換は、爆発の危険を引き起こす可能性があります。交換する際は、同じまたは同等のタイプのみを使用してください。使用済みのバッテリーは、バッテリー製造元の指示に従って処分してください。
- 生体認証製品は、偽装防止環境に完全に適用できるものではありません。より高いセキュリティレベルが必要な場合は、複数の認証モードを使用してください。
- デバイスが再起動中は、レーン内に留まらないでください。
- 誤ったタイプのバッテリーを交換すると爆発の危険があります。使用済みのバッテリーは、指示に従って処分してください。
- コンクリートまたはその他の不燃性表面への取り付けのみに適しています。
- 取扱説明書には、機器の保護接地導体を設置の保護接地導体に接続することを記載してください。

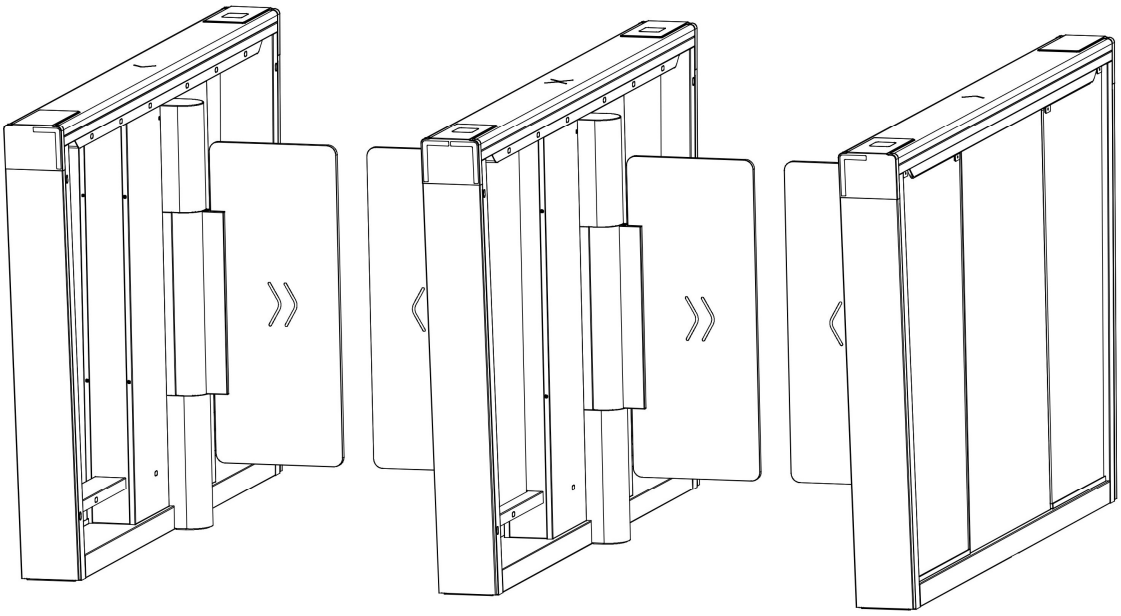
入手可能なモデル

製品名	モデル	説明
スイングバリア		左ペデスタル
	DS-K3B530LX-M/DS-K3B530X- M	中央支柱
		右ペデスタル

内容

第1章 概要

1.1 導入



14個のIRライトを備えたスイングバリアは、不正な入退場を検知するために設計されています。アクセス制御システムと一体型のスイングバリアを採用することで、ICカードやIDカードの読み取り、QRコードの読み取りなどにより、通過する人は認証を受ける必要があります。アトラクション、スタジアム、建設現場、住宅などで広く使用されています。

1.2 主な機能

- 入口と出口の両方向で、制御モード、誘導モード、自由通行モード、常時開モード、常時閉モードをサポートします。
- 強制アクセス防止
  強制アクセスが発生した場合、バリアはソフトモードまたはガードモードに応じて反応します。
- 自己検出、自己診断、および自動アラーム
- 侵入、尾行、逆走、バリアの乗り越えを検知すると、可聴および視覚アラームが作動します。
- LEDは入口/出口と通過状態を表示します
- 火災警報通過
  火災警報器が作動すると、緊急避難のためにバリアが自動的に開きます。
- 有効通過時間設定

有効通過時間内にレーンを通過しない場合、システムは通過許可をキャンセルします。

- 双方向（入口/出口）レーン
  バリアの開閉速度は、来訪者の流れに応じて設定可能です。
- TCP/IP ネットワーク通信
  通信データは、プライバシー漏洩の懸念を軽減するために特別に暗号化されています。
- 権限検証と尾行防止
- キーフォブによるリモートバリアの開閉とスピーカーによる放送（アクセス制御ボードと組み合わせてインストールした場合、カスタム放送コンテキストがサポートされます）。

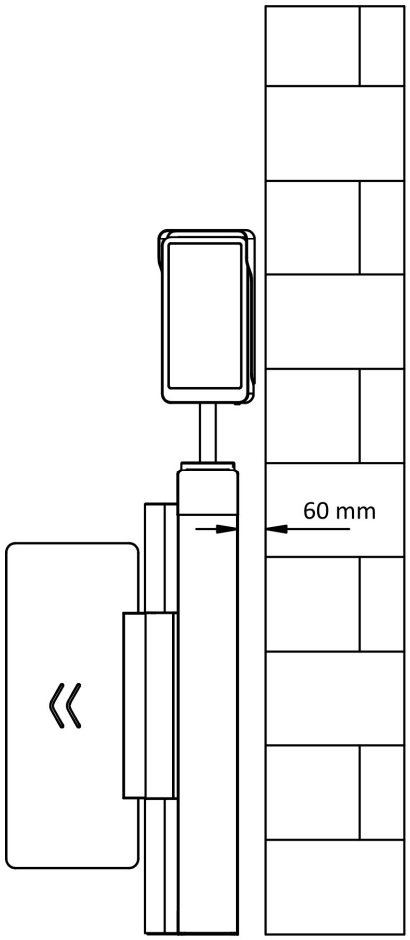
第2章 システム配線

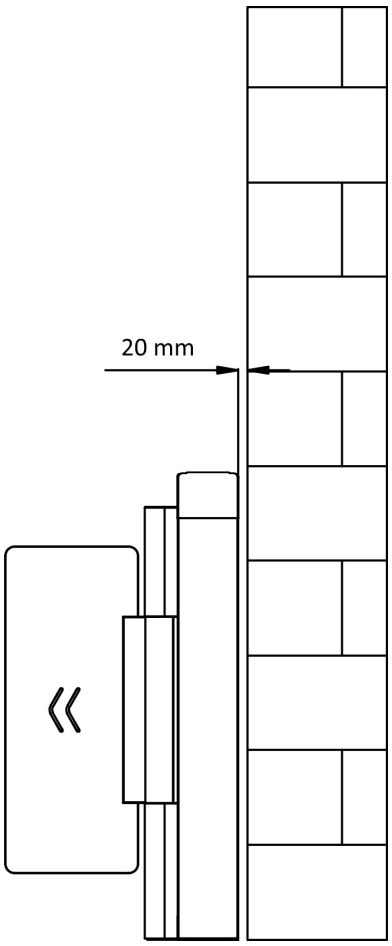
設置前の準備および配線全般。

手順

注

- 装置はコンクリート面または他の平らな不燃性表面に設置する必要があります。
- 設置場所が壁に近すぎる場合は、台座と壁の間の距離を 20 mm 以上（顔認識端末を使用する場合は 60 mm 以上）確保してください。そうしないと、台座の上部パネルを開けなくなったり、機器が損傷したりするおそれがあります。





- 寸法は次のとおりです。

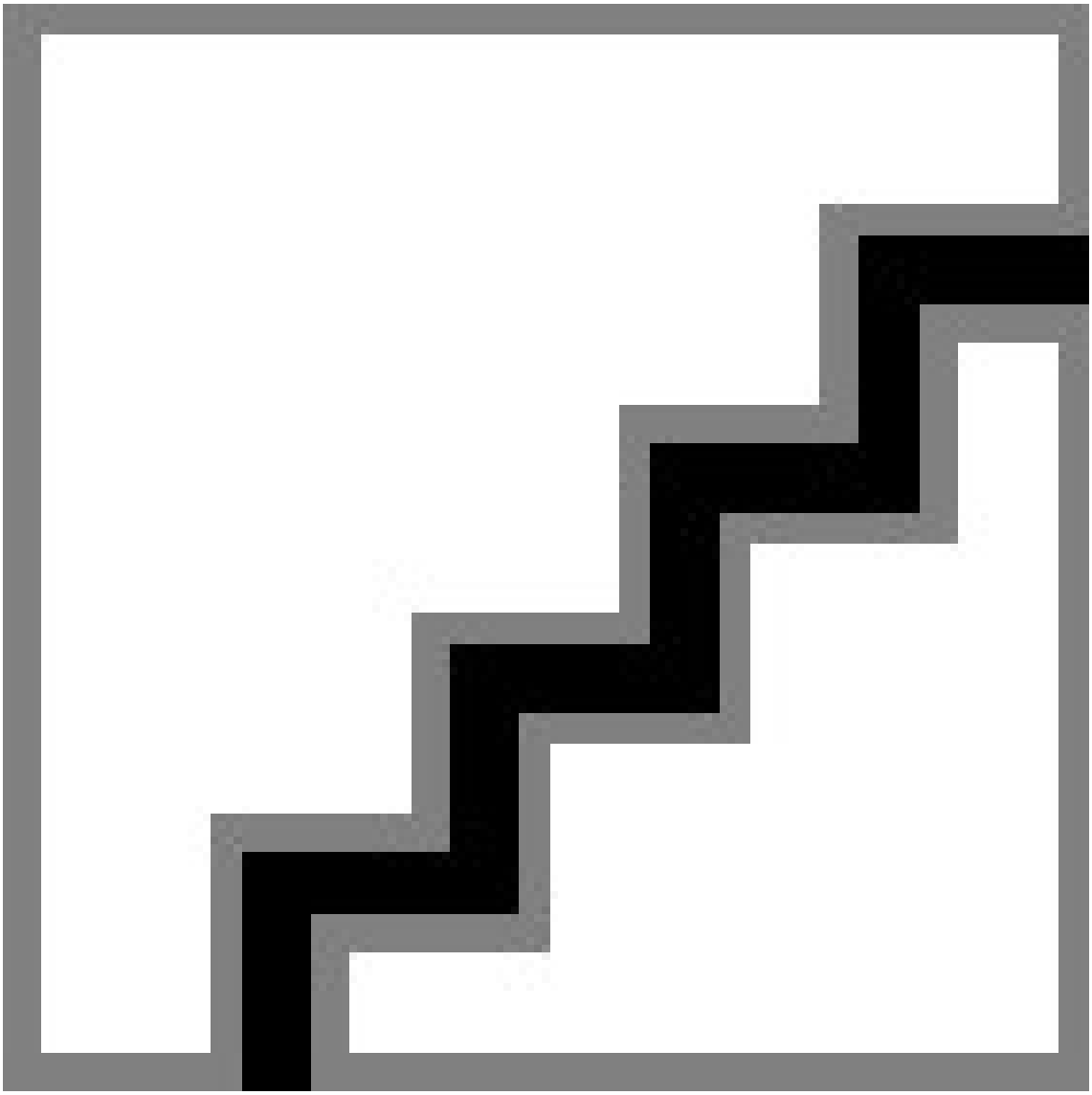


図 2-1 寸法

1. 左または右のペデスタルの設置面に中央線を描きます。

2. 他の台座を設置するための平行な線を引きます。

注意

最寄りの2つの線間の距離はL+ 272 mmです。Lは車線幅を表します。

3. 設置面にスロットを切り、設置穴を掘ります。各支柱にM12×120の拡張ボルトを4本ずつ取り付けます。

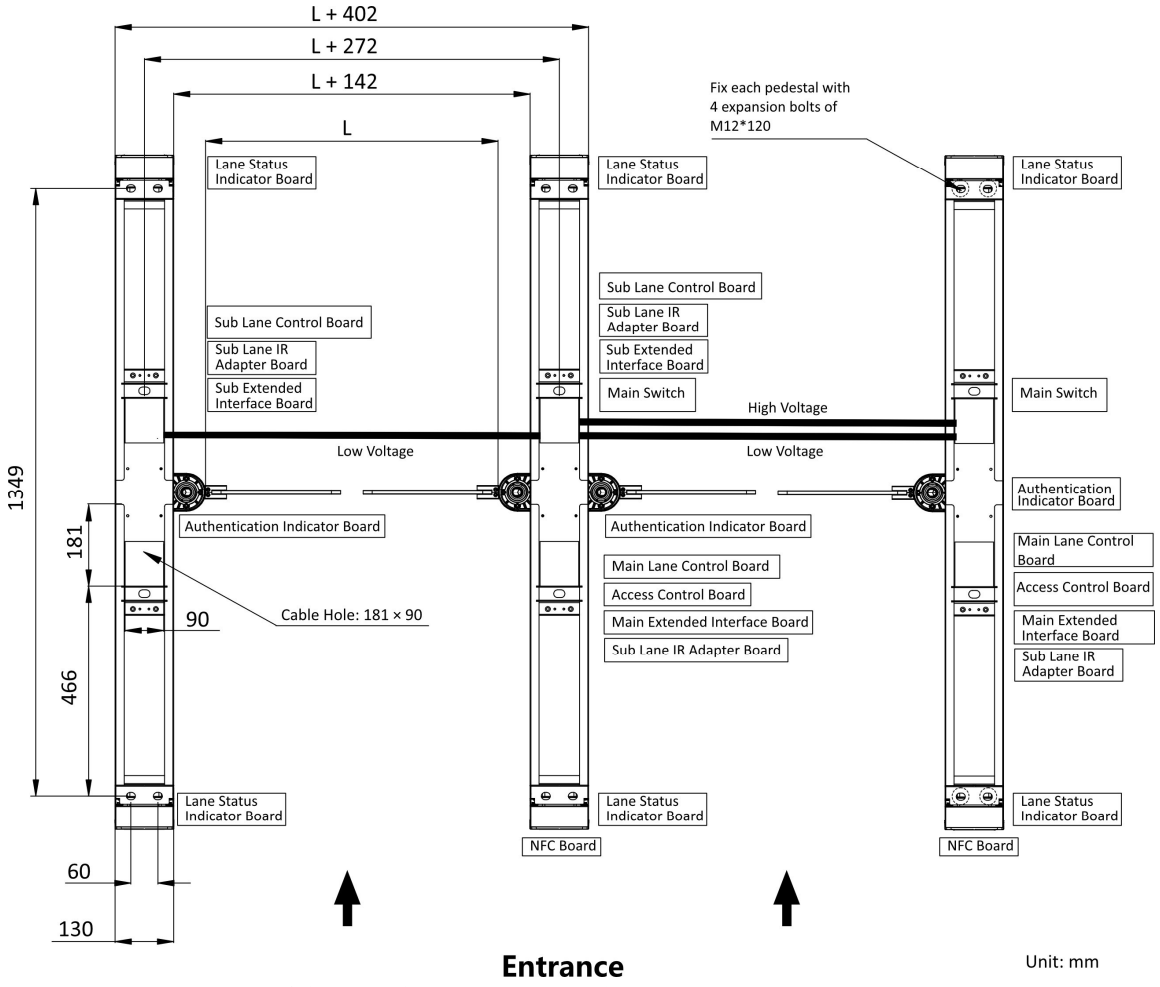


図2-2 穴の位置とシステム配線

4. ケーブルを埋設します。各車線に高圧ケーブル1本と低圧ケーブル1本を埋設します。詳細はステップ3のシステム配線図を参照してください。

注意

- 高電圧：AC 電源入力
  低電圧：相互接続ケーブル（通信ケーブルおよび 24 V 電源ケーブル）およびネットワーク通信ケーブル
- 付属の 24 V 電源ケーブルの長さは 5 m、通信ケーブルの長さは 3 m です。
- 低電圧用配管の内径は30 mm以上を推奨します。
- AC 電源コードと低電圧ケーブルの両方を埋設する場合は、干渉を避けるため、2 本のケーブルは別の導管に入れてください。
- 接続する周辺機器が増える場合は、配管の直径を拡大するか、外部ケーブル用に別の配管を埋設する必要があります。
- 外部 AC 電源コードは二重絶縁のものを使用してください。
- ネットワークケーブルは CAT5e またはそれ以上の性能のネットワークケーブルを使用してください。

第3章 ペデスタルを設置する

作業開始前
設置工具を準備し、装置およびアクセサリーを確認し、設置場所を空けてください。

手順

注意

- デバイスは、コンクリート面または他の平らな不燃性表面に設置してください。
- 設置作業中は、本機の電源がオフになっていることを確認してください。
- インストールツールは、ペデスタルのパッケージ内に収納されています。

1. インストールツールを準備し、部品を確認し、インストールベースの準備を行ってください。

2. 2 つのサイドパネルを固定している 4 本のネジを、各台座から取り外します。

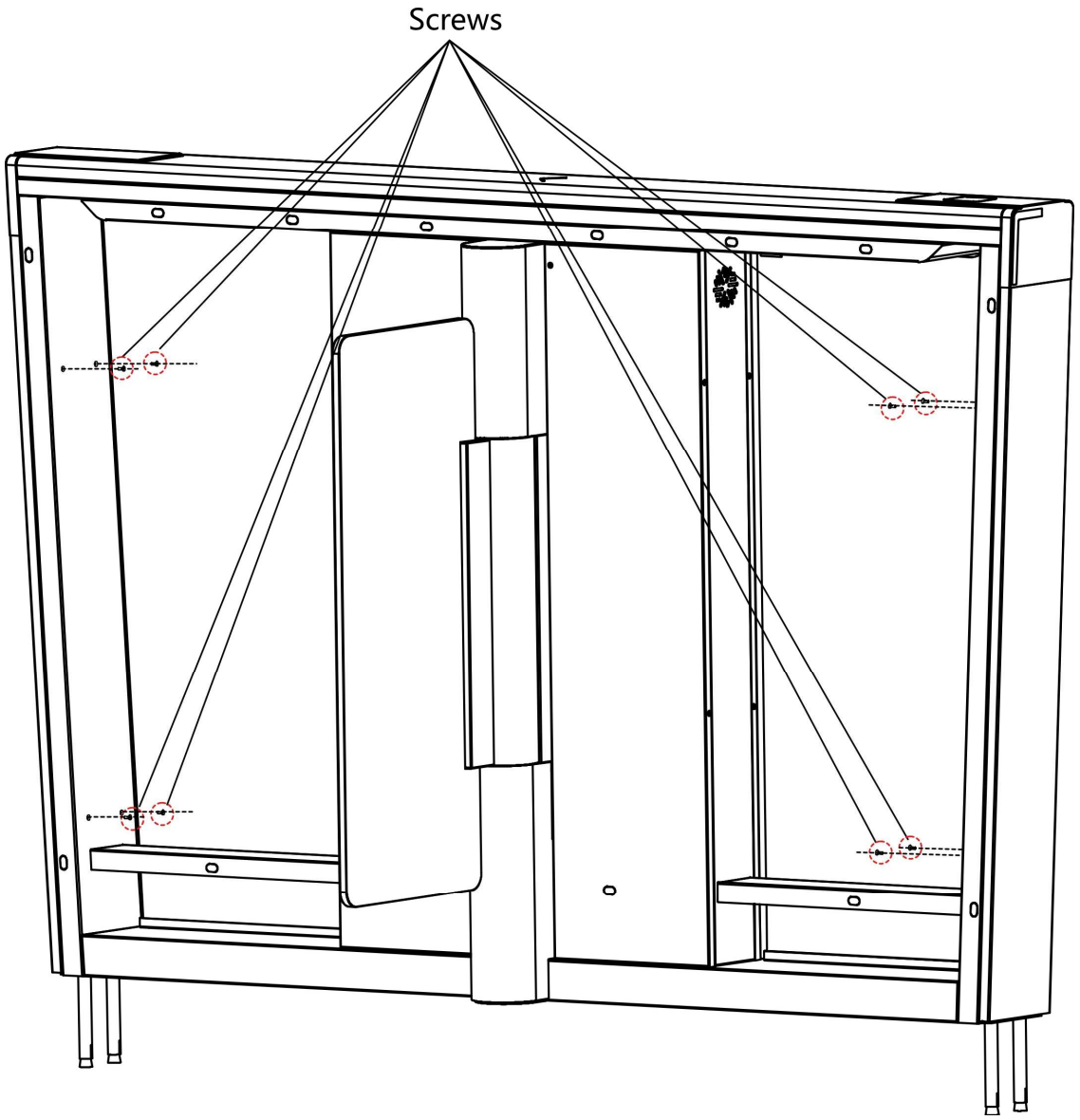


図3-1 側面パネルのネジを外す

3. サイドパネルを取り外し、ペデスタルの入口と出口のマークに従ってペデスタルを対応する位置に移動してください。

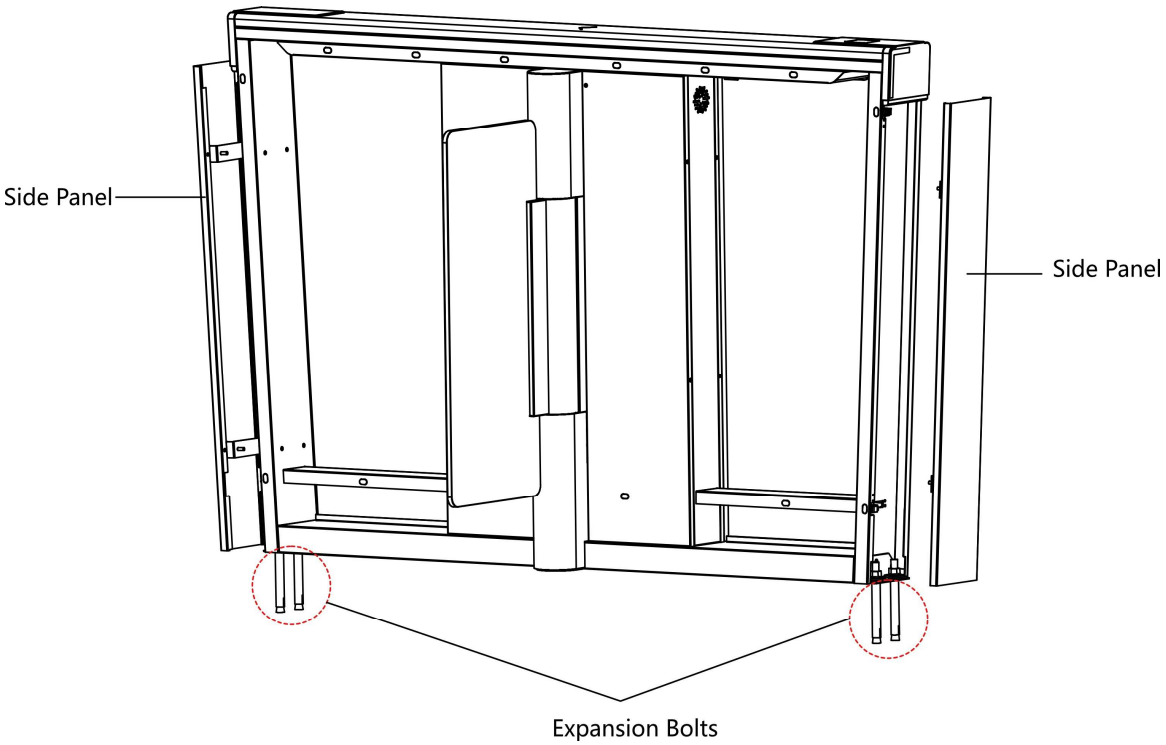


図3-2 サイドパネルのネジを外す

注

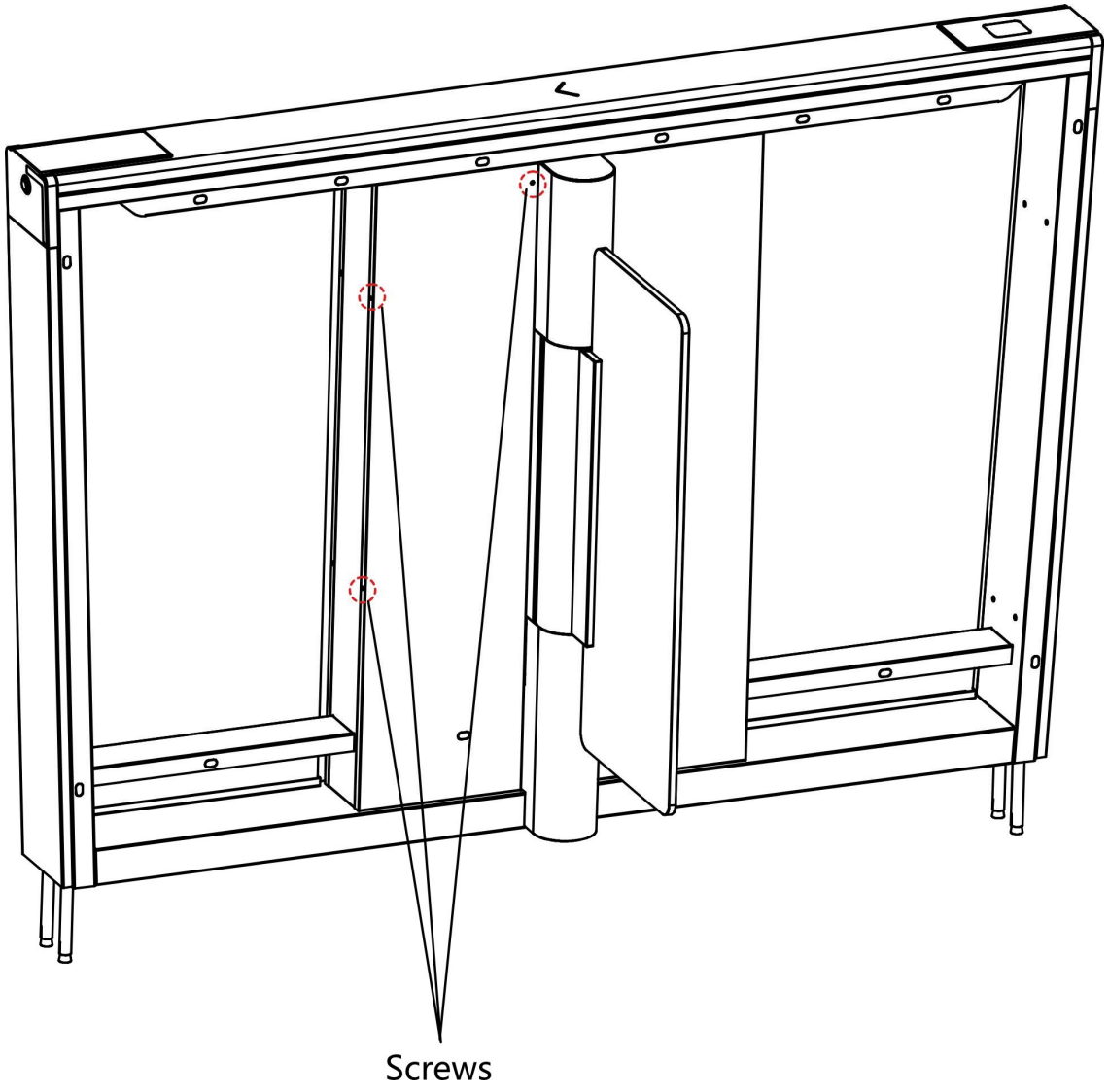
システム配線に関する詳細情報は、***システム配線***をご参照ください。

4. ペデスタルを拡張ボルトで固定し、サイドパネルをネジで元の位置に固定します。

注意

水に浸けないでください。特別な事情がある場合は、浸水高さを 150 mm 以下にしてください。

5. 各メンテナンスドアのケーブル配線のため、3本のネジを外してドアを開けてください。


Screws

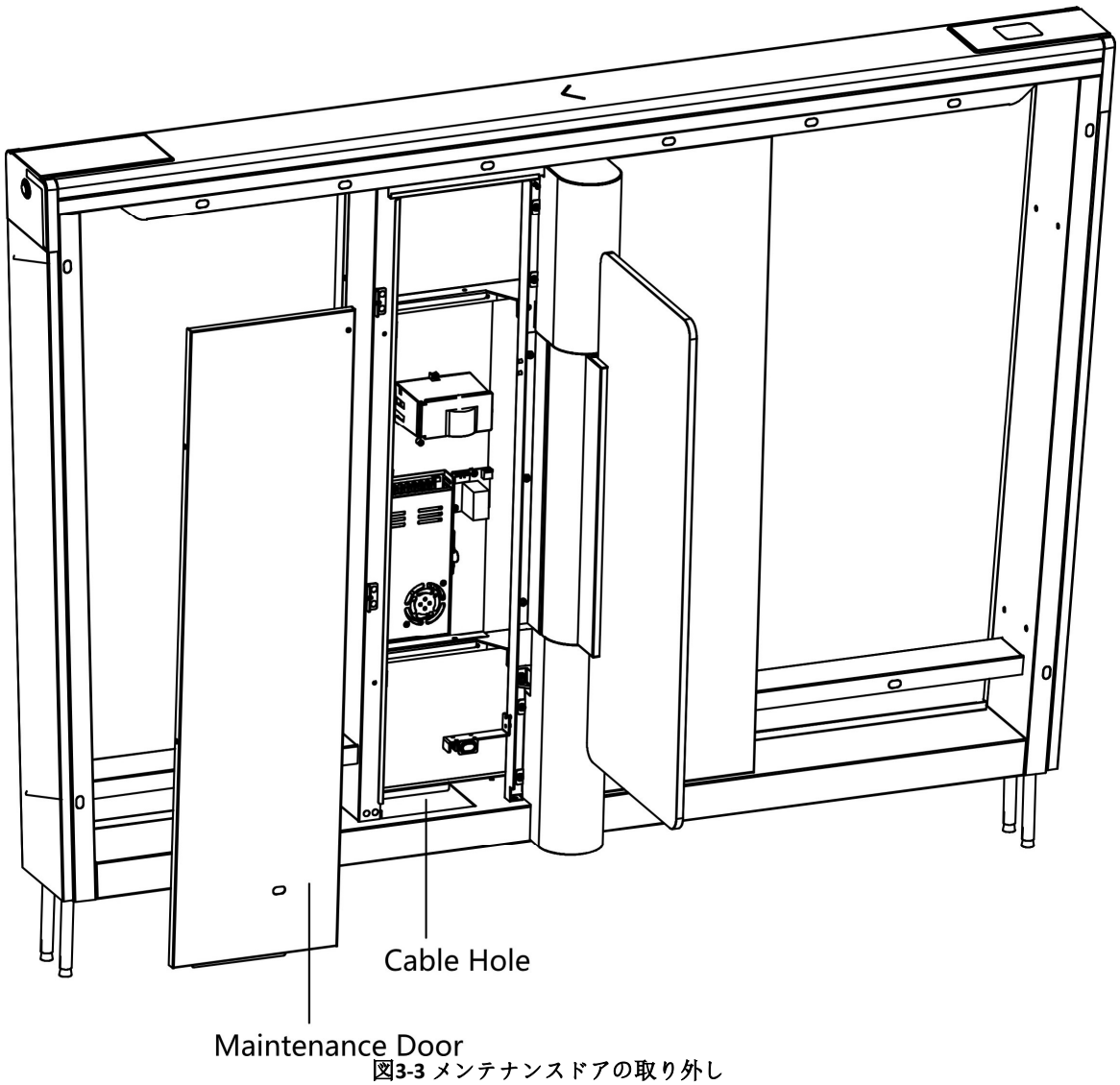


図3-3 メンテナンスドアの取り外し

注意

ケーブルの詳細については、*「配線全般」*を参照してください。

第 4 章 配線全般

注意

- 高電圧モジュールを維持または分解する際は、高電圧モジュール全体を取り外し、ターンスタイルの外でメンテナンスを行ってください。メンテナンス前に、周辺機器に接続されているケーブルを必ず外し、機器の損傷を防止してください。
- 高電圧モジュールを分解する場合は、怪我を防ぐため、電源を切ってください。
- メンテナンスが不要で配線のみが必要な場合は、高電圧モジュールを取り外さないでください。
- スイッチとメインレーン制御基板は既に接続されています。AC電源とスイッチを接続する14 AWGケーブルは別途購入する必要があります。
- 2 本の相互接続ケーブル（24 V 電源ケーブルと通信ケーブル）が付属しています。24 V 電源ケーブル：長さ 5 m、中央と右の台座にあります。

  通信ケーブル：4m長、CAT5e、中央と右のペデスタルに同梱されています。

4.1 コンポーネントの概要

デフォルトでは、ターンスタイルの基本部品はしっかりと接続されています。ペデスタルは、相互接続ケーブルを配線することで通信が可能です。また、ターンスタイルは、システム全体の電源用 AC 電源の配線に対応しています。

注意

入力電圧変動は100 VACから240 VAC、50Hzから60Hzの範囲です。

以下の図は、入口と出口方向のシリアルポートを示しています。

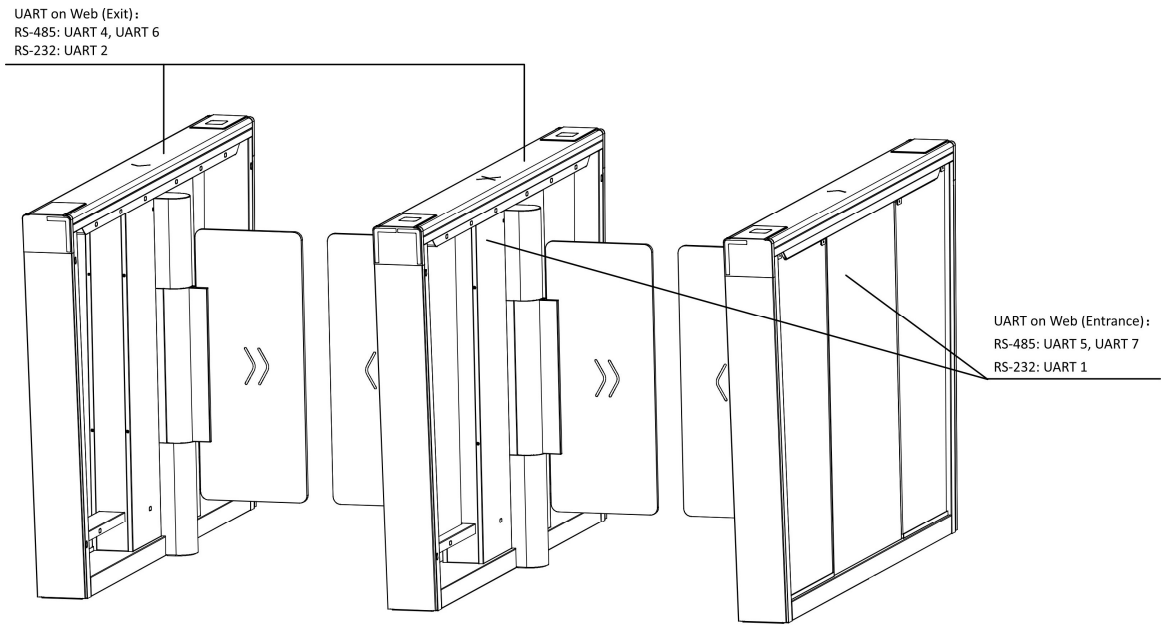


図4-1 シリアルポート

以下の図は、IR送信/受信モジュールと、その対応する番号を台座上に示したものです。

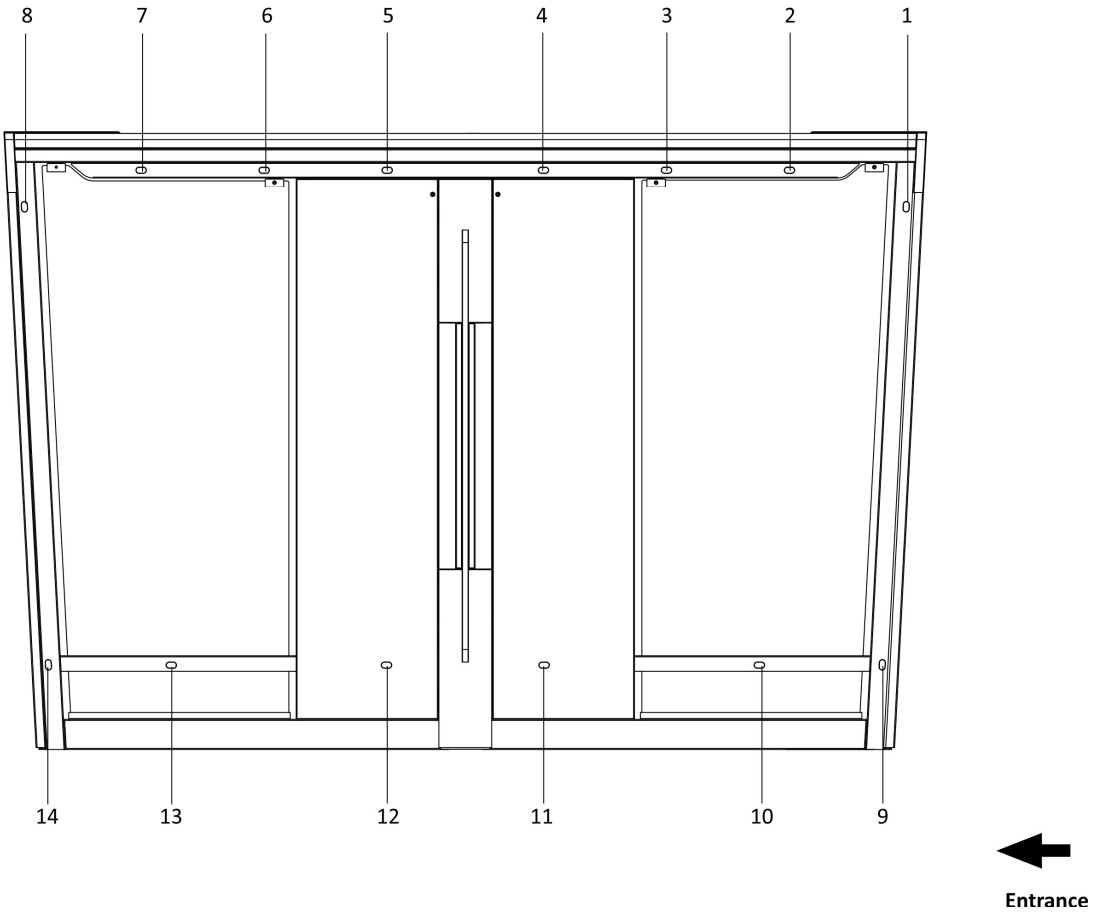


図4-2 IR送信/受信モジュール位置

注

レーンの入り口位置に立っている場合、左側のIRモジュールがIR送信モジュール、右側のIRモジュールがIR受信モジュールです。

4.2 配線

QR コードをスキャンして、ガイドビデオをご覧ください。

4.3 端子説明

4.3.1 全般配線

レーン制御ボード、アクセス制御ボード、拡張インターフェースボードの一般的な配線です。

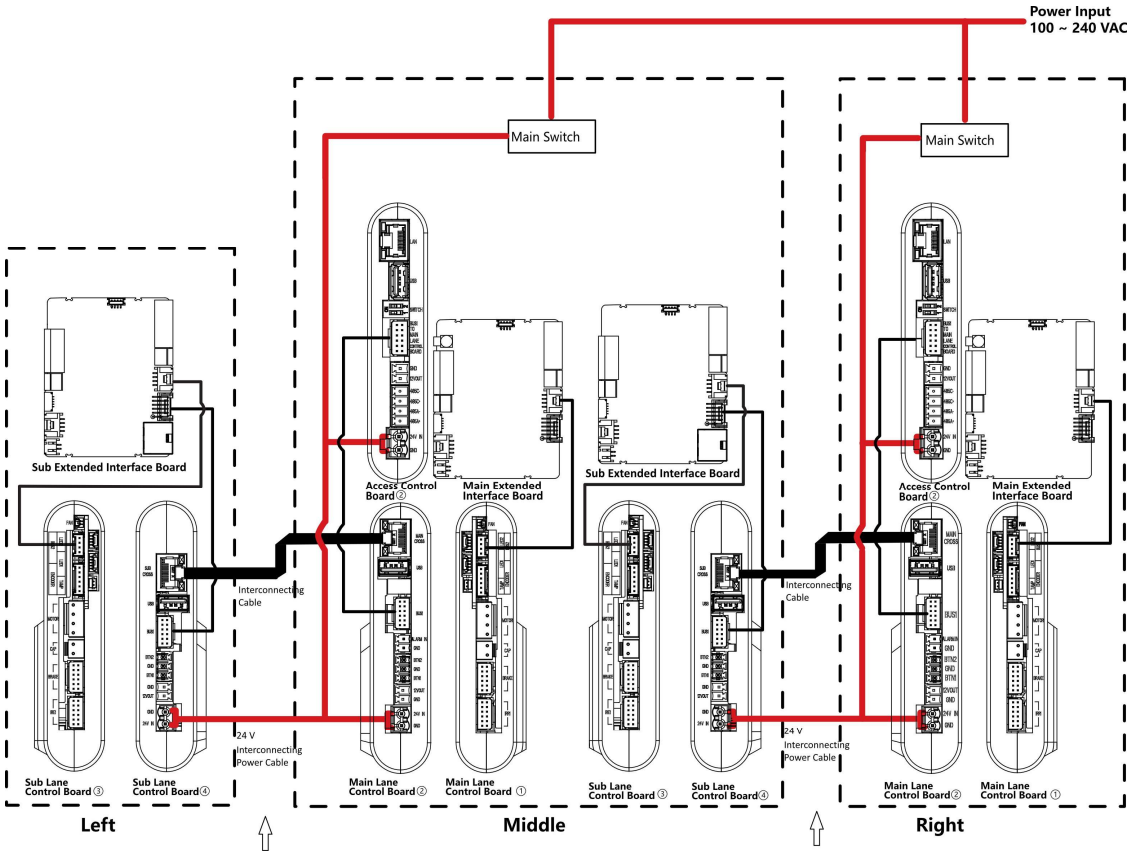


図 4-3 配線全般

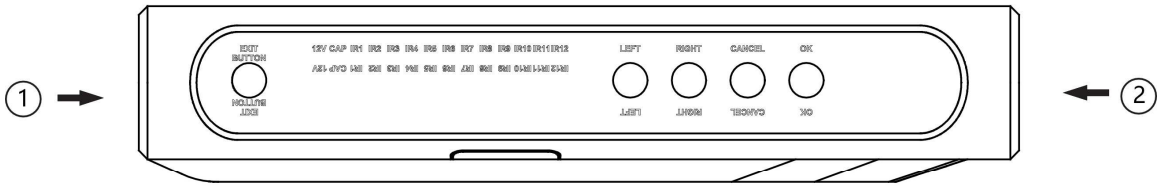
注意

- 電源からメインレーン制御ボードへの電源ケーブルが接続されています。AC 電源入力を電源に接続するための 14AWG 電源ケーブルをご用意ください。
- 付属の2本のインターコネクトケーブルは現場で接続する必要があります:
  1. 14 AWG の 24 V 電源ケーブル。ケーブルの長さは 5 m で、出口の右/中央の台座内に収納されています。
  2. CAT5e通信ケーブル。ケーブルの長さは3mで、右/中央のペデスタルのパッケージ内に配置してください。
- ①と②または③と④は、同じ基板の2つの側面を指します。
- バリアが入り口/出口で開く場合：BTN1/BTN2とGNDに接続してください。

4.3.2 メインレーン制御ボード端子説明

メインレーン制御ボードには、相互接続インターフェース、アクセス制御ボードインターフェース、火災入力インターフェース、出口ボタンインターフェース、12 VDC 出力インターフェース、24 VDC 入力インターフェース、ファンインターフェース、イーサネット端子、エンコーダインターフェース、モーター用電源インターフェース、スーパーキャパシタインターフェース、メインブレーキインターフェース、アダプタインターフェース、およびタンパーインターフェースが含まれています。

以下の図は、メインレーン制御ボードの配線図です。



Main Lane Control Board

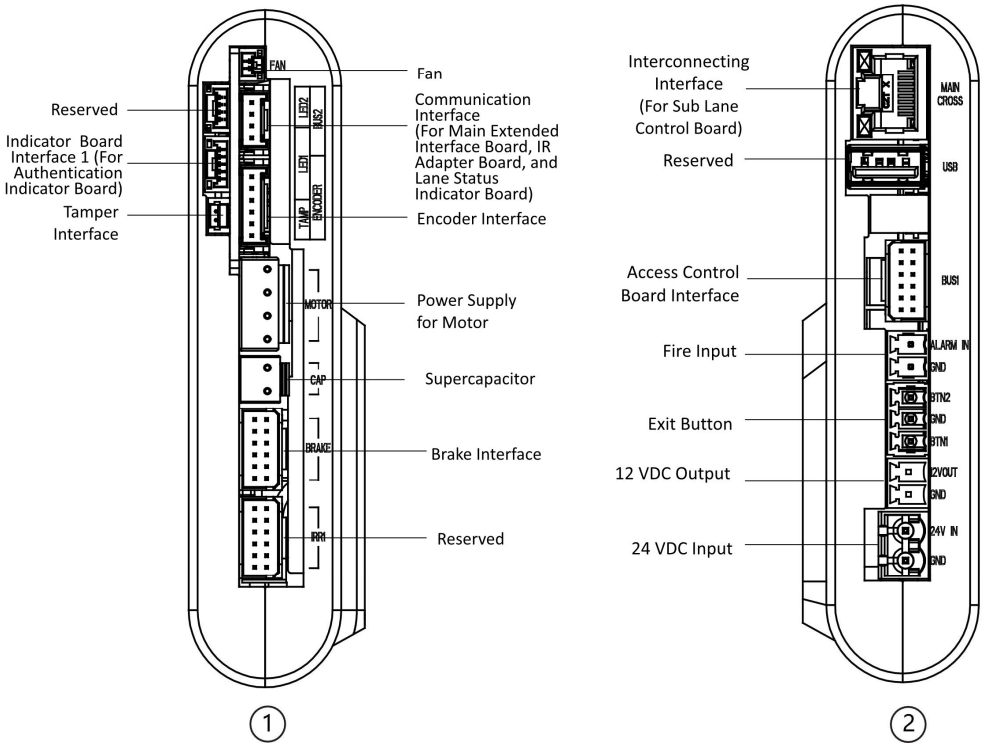


図4-4 メインレーン制御基板端子

4.3.3 サブレーン制御ボード端子説明

サブレーン制御ボードには、相互接続インターフェース、バスインターフェース、出口ボタンインターフェース、12 VDC 出力インターフェース、24 VDC 入力インターフェース、ファンインターフェース、イーサネット端子、エンコーダインターフェース、モーター用電源インターフェース、スーパーキャパシタインターフェース、サブブレーキインターフェース、アダプタインターフェース、およびタンパーインターフェースが含まれています。

以下の図は、サブレーン制御基板の回路図です。

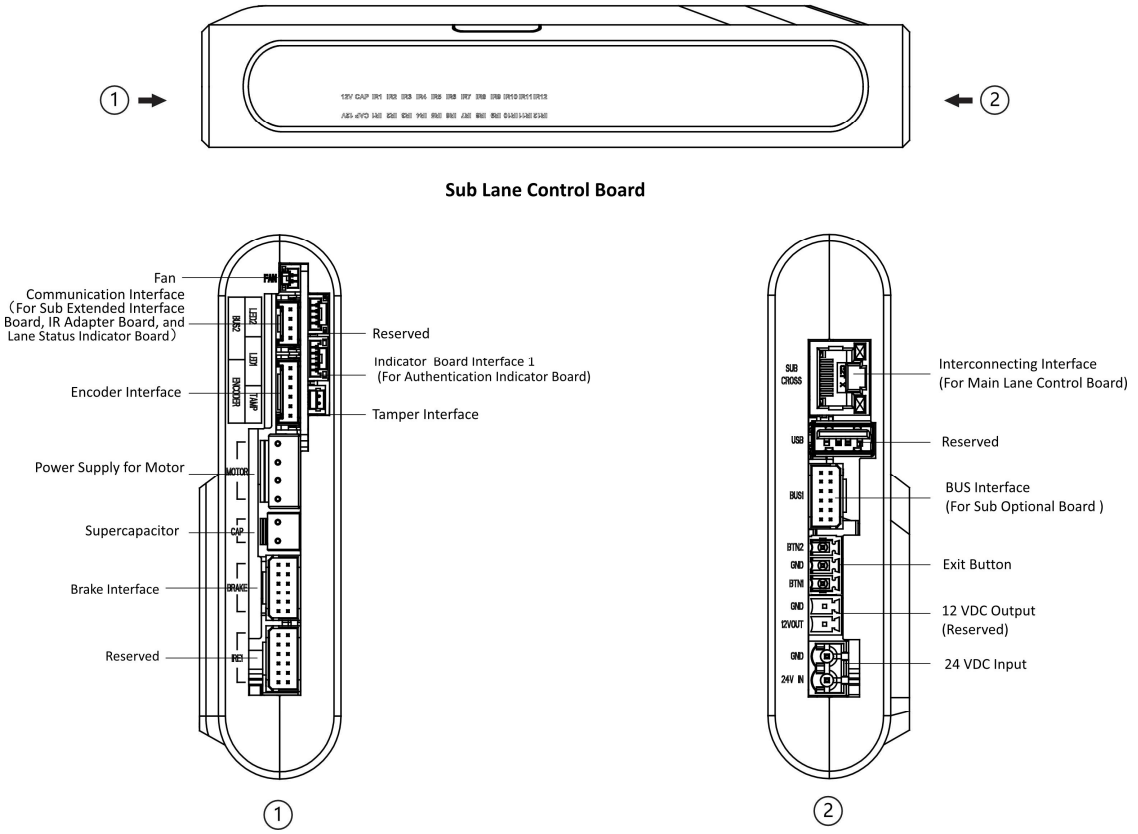


図4-5 サブレーン制御基板の端子

4.3.4 アクセス制御ボード端子説明（オプション

アクセス制御ボードは、主に公安や司法機関などのセキュリティレベルの高い場所での権限識別、外部デバイスへのアクセス、および上位プラットフォームやレーンコントローラとの通信に使用されます。

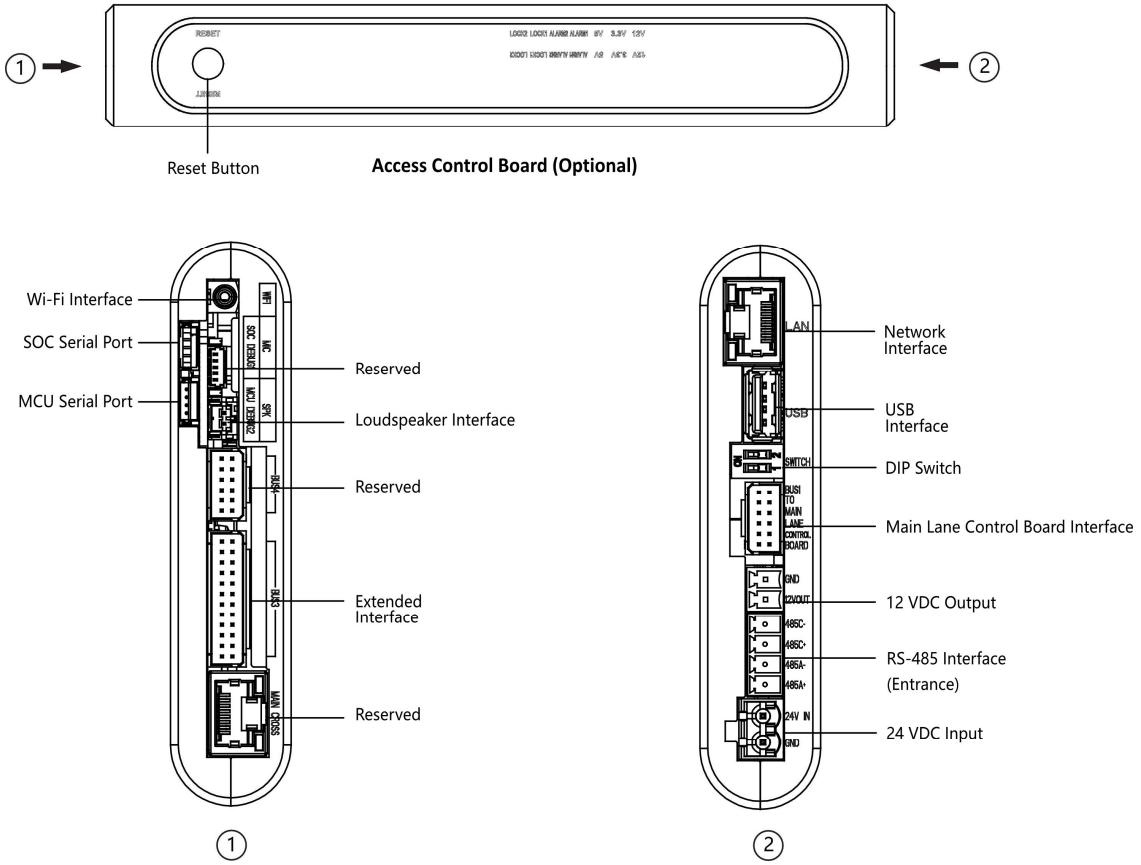


図4-6 アクセス制御ボード

注

- RS-485Aはウェブ上のポート5に対応し、デフォルトで入口のQRコードスキャナー接続用です；RS-485Cはウェブ上のポート7に対応し、デフォルトで入口のカードリーダー接続用です。
- SOCとMCUのシリアルポートは、メンテナンスとデバッグ専用です。
- リセットボタンを5秒間押すと、デバイスが工場出荷時設定に復元されます。
- DIP スイッチは、学習モードの設定およびキーフォブのペアリングに使用します。DIP スイッチの詳細については、*「DIP スイッチの説明」*を参照してください。

アクセス制御ボードの拡張インターフェースの配線図を以下に示します。

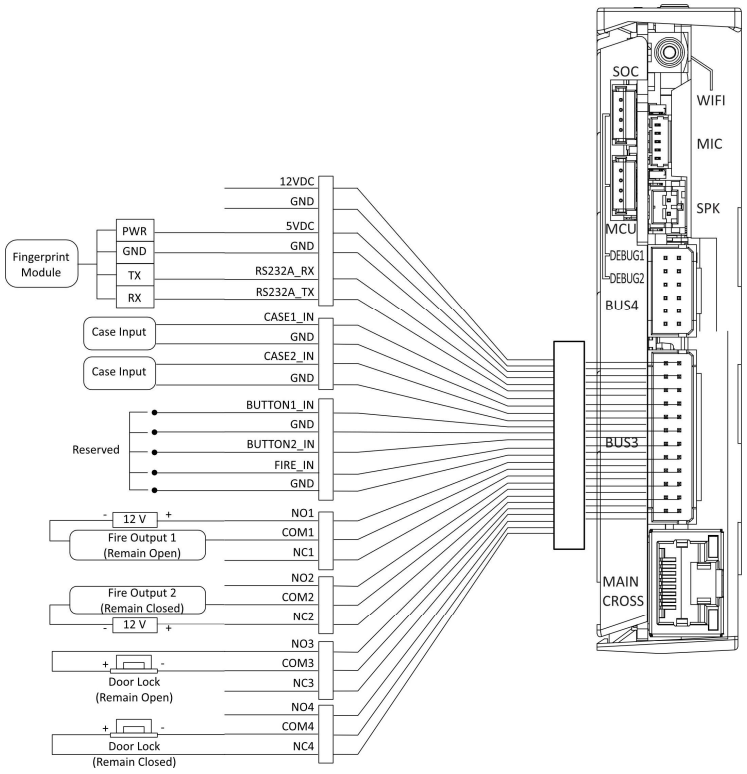


図 4-7 BUS3 インターフェースの配線図

注

RS-232Aはウェブのポート1に対応しています。

4.3.5 メイン拡張インターフェースボード端子説明

メイン拡張インターフェースボードには、サブ 1G アンテナインターフェース、バリアライトインターフェース、スピーカーインターフェース、デバッグポート、ウィーガンド/退出ボタンインターフェース、5 VDC 出力、およびイーサネット端子があります。

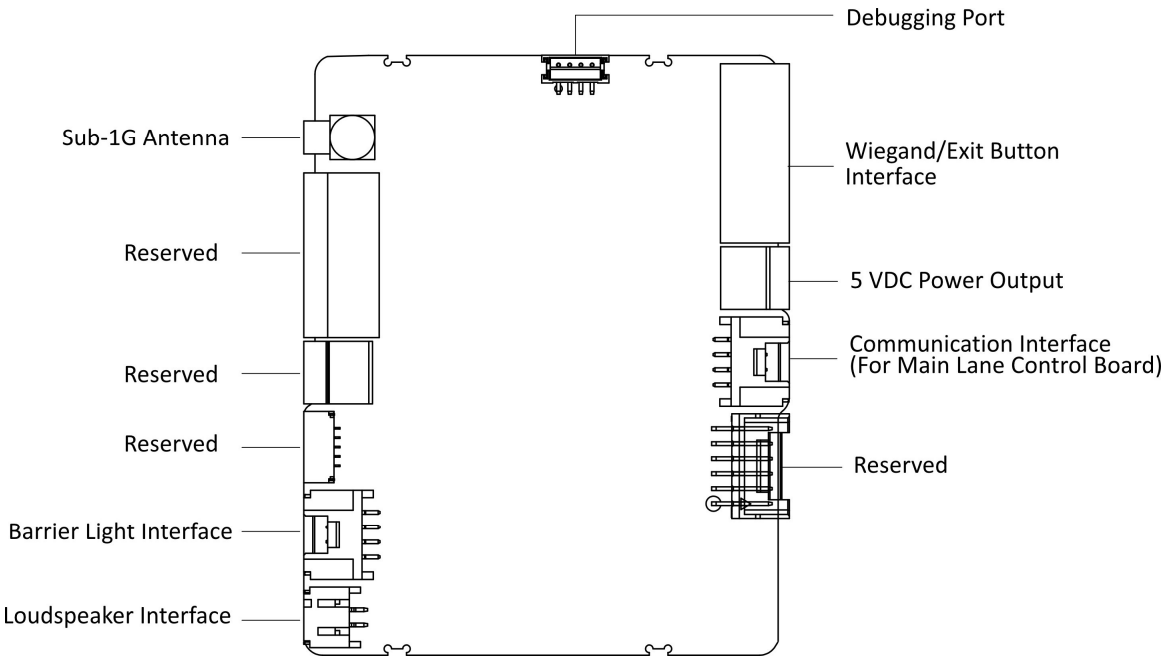


図 4-8 メイン拡張インターフェースボード端子

注

デバイスにアクセス制御ボードが取り付けられている場合、スピーカーはアクセス制御ボードに接続する必要があります。そうでない場合、スピーカーはメイン拡張インターフェースボードに接続する必要があります。

4.3.6 カードリーダーボード端末の説明

カードリーダーボードは、RS-485 インターフェースを介してアクセス制御ボードに接続できます。

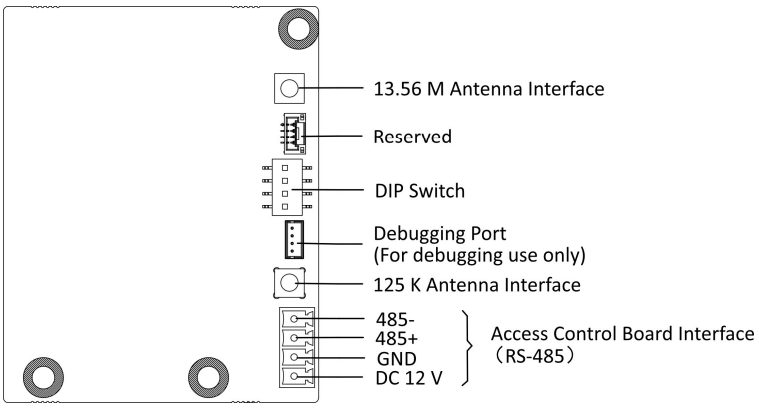
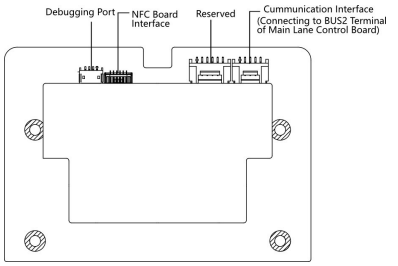
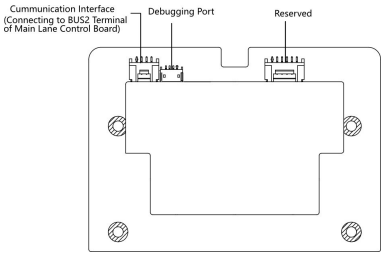
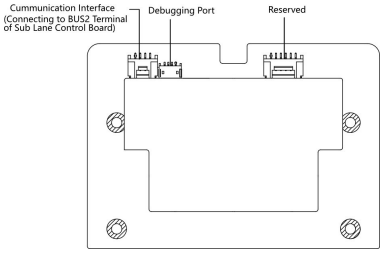
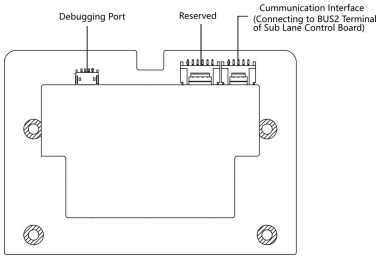
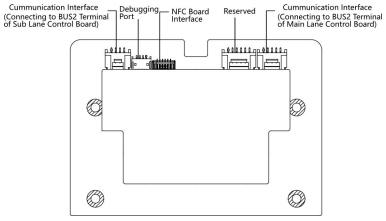
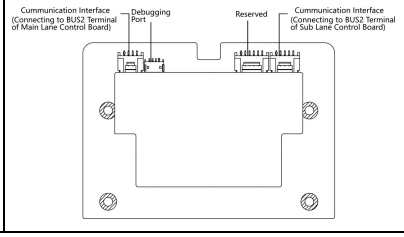


図4-9 カードリーダーボード

4.3.7 レーン状態表示ボード

レーン状態表示板の位置の詳細については、を参照してください。
異なるペデスタルに設置されたレーン状態表示ボードは、以下のとおりです。

表4-1 レーン状態表示ボード

支柱	入口	出口
右支柱		
左ペデスタル		
中央ペデスタル		

4.3.8 認証インジケータボード ターミナル説明

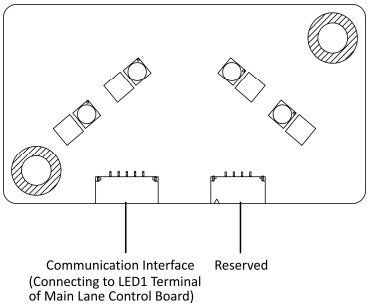


図4-10 認証表示板

認証表示板は、メインレーン制御板のLED1端子に接続されています。

4.3.9 RS-485 配線

アクセス制御ボードおよびサブ拡張インターフェースボードの RS-485 インターフェースは、顔認識モジュールまたはカードリーダーに接続することをお勧めします。ここでは、カードリーダーとの接続を例に説明します。

注

アクセス制御ボードには、入口用に 2 つの RS-485 インターフェースがあります。詳細については、「*アクセス制御ボードの端子説明（オプション）*」を参照してください。

サブ拡張インターフェースボードには、出力用の RS-485 インターフェースが 2 つあります。詳細については、を参照してください。

- RS-485をカードリーダーに接続する場合、デフォルトではカードリーダーのDIPスイッチを以下の設定に設定してください：
  - 入口の場合は、4 桁の DIP スイッチの No.1 を ON 側に設定してください。
  - 退出の場合は、4 桁の DIP スイッチの No.3 を ON 側に設定してください。
- 他のRS-485デバイスが接続されている場合、RS-485のIDが衝突しないようにしてください。
- 顔認証端末用の 12 V 電源インターフェースは、他の 12 V 機器と接続することはできません。

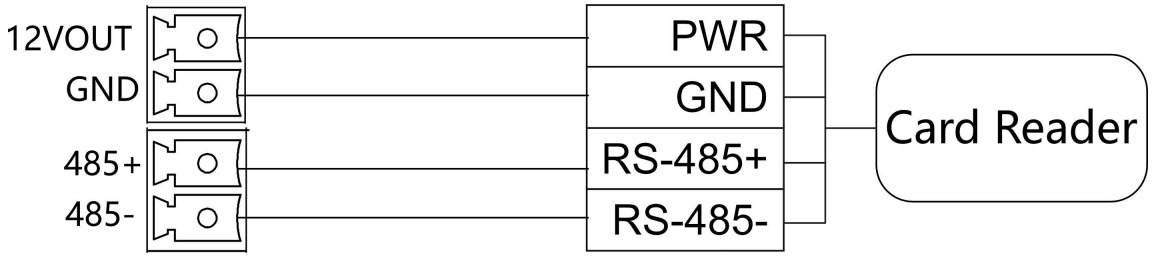


図4-11 RS-485の配線

4.3.10 RS-232 配線

注

- アクセス制御ボードの拡張インターフェースには、1 つの RS-232 インターフェースがあります。***アクセス制御ボードの端子説明(オプション)***を参照してください。RS-232A は、Web 上の UART 1 に対応しています。
- サブ拡張インターフェースボードには 1 つの RS-232 インターフェースがあります。RS-232B は、ウェブ上の UART 2 に対応しています。

  RS-232C インターフェースは予約されています。

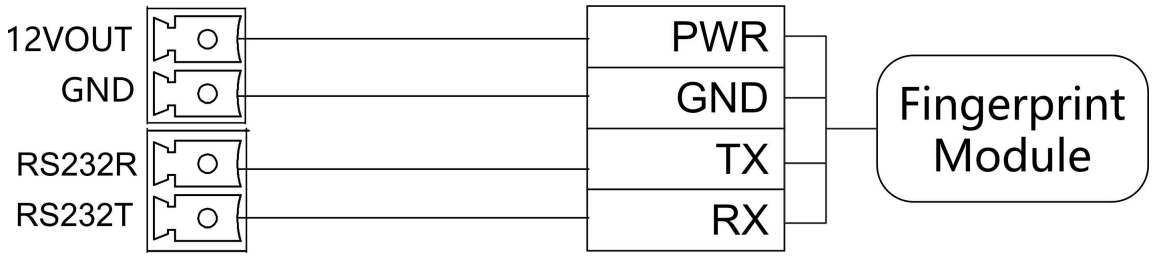


図4-12 RS-232 配線

4.3.11 アラーム入力の配線

メインレーン制御ボードでは、火災アラーム入力インターフェースを配線することができます。

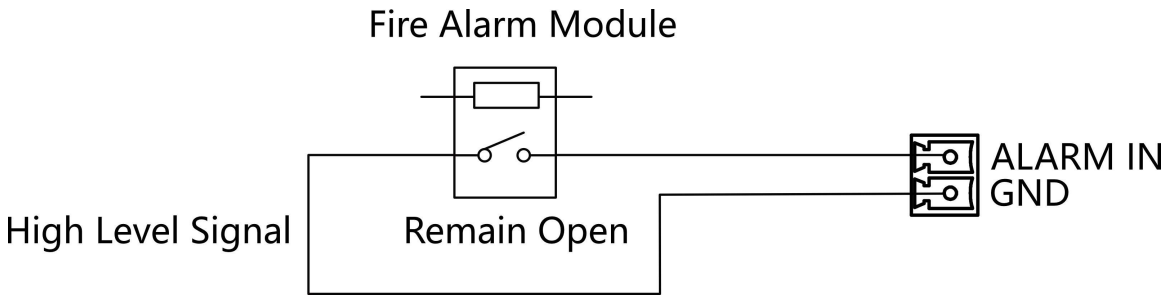


図4-13 残りの接続

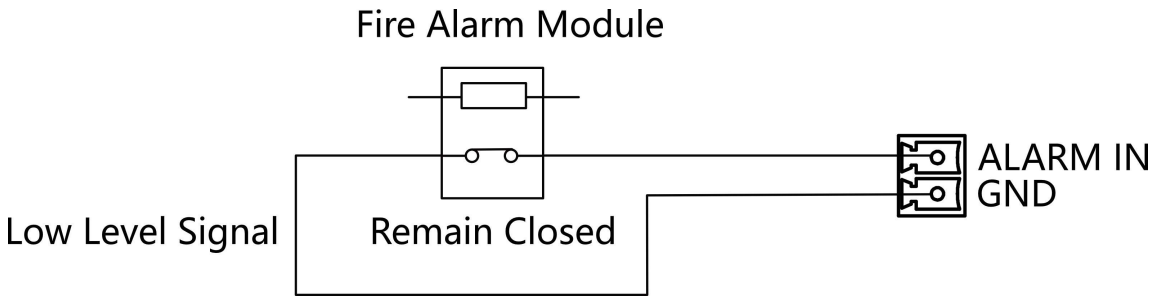


図4-14 残りの閉回路

4.3.12 出口ボタン配線

メインレーン制御盤とサブレーン制御盤には、それぞれ 1 つのボタンインターフェースがあり、出口ボタンまたは顔認識装置に接続することができます。

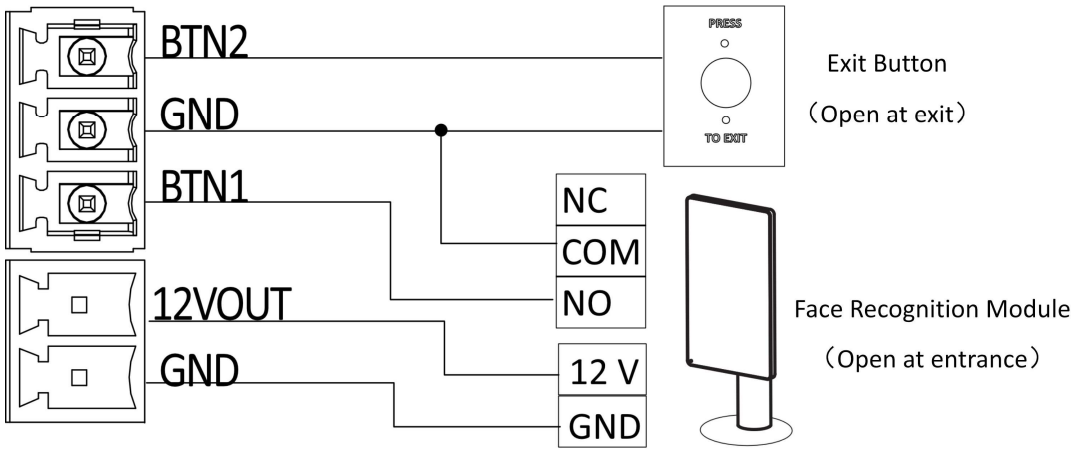


図4-15 出口ボタン配線

注

- 顔認識装置は、メインおよびサブレーン制御ボードの 12 VDC 電源出力インターフェースから電源を供給されます。
- 入口のバリアが開いています：BTN1とGNDに接続してください。
- 出口のバリアが開いた場合：BTN2とGNDに接続してください。

4.4 デバイス設定（ボタン経由）

メインレーン制御ボードのボタンまたはアクセス制御ボードのDIPスイッチを使用して、デバイスを設定できます。

機能	メインレーン制御ボードおよびスピーカー（メイン拡張インターフェースボードに接続	メインレーン制御基板 & アクセス制御基板 & スピーカー（アクセス制御基板に接続）
動作モード		
通常/学習モード	ボタンで設定（参照：*ボタンで学習モードを設定*）	DIP スイッチで設定（*DIPによる学習モードの設定 スイッチ（オプション）*を参照）
キーフォブペアリング	ボタンを使用して設定（参照：*キーフォブをボタンでペアリングする*）を参照）	DIP スイッチで設定します（*DIP スイッチによるキーフォブのペアリング（オプション）*を参照してください）。
通過モード	ボタンで設定	ボタン/ウェブ経由で設定

機能	メインレーンコントロールボードおよびスピーカー（メイン拡張インターフェースボードに接続）	メインレーン制御ボード & アクセス制御ボード & ラウドスピーカー（アクセス制御ボードに接続）
メモリモード	ボタン経由で設定	ボタン/ウェブ経由で設定
制御モード	ボタンで設定	ボタン/ウェブ経由で設定
アプリケーションモード	ボタンで設定	ボタンを使用して設定
パラメーター設定		
バリアの開閉速度	ボタンで設定	ボタン/ウェブ経由で設定
バリアの閉速度	ボタンで設定	ボタン/ウェブ経由で設定
アラームエリアでのカード読み取り	ボタンで設定	ボタン/ウェブ経由で設定
期間を入力	ボタン経由で設定	ボタン/ウェブ経由で設定
終了期間	ボタンで設定	ボタン/ウェブ経由で設定
赤外線センサーの検知時間	ボタンで設定	ボタン/ウェブ経由で設定
侵入検知時間	ボタンで設定	ボタン/ウェブ経由で設定
滞在超過時間	ボタン経由で設定	ボタン/ウェブ経由で設定
バリア閉門遅延時間	ボタンで設定	ボタン/ウェブ経由で設定
バリア回復時間	ボタンで設定	ボタンで設定
音量調整	ボタンで設定	ボタンで設定
バリア材質	ボタンで設定	ボタン/ウェブ経由で設定
バリアの長さ	ボタンで設定	ボタン/ウェブ経由で設定
バリアの高さ	ボタンで設定	ボタン/ウェブ経由で設定
ブレーキ	ボタンで設定	ボタンで設定
ブレーキ角度	ボタンで設定	ボタンで設定
赤外線センサー	ボタンで設定	ボタン/ウェブ経由で設定
ファン	ボタンで設定	ボタンで設定
ライトの明るさ	ボタンで設定	ボタン/ウェブ経由で設定
デフォルトに戻す	ボタンで設定	ボタン/ウェブ経由で設定
音声プロンプト		

機能	メインレーンコントロールボード＆スピーカー（メイン拡張インターフェースボードに接続	メインレーン制御ボード & アクセス制御ボード & 拡声器（アクセス制御ボードに接続）
バリア越え	ボタンで有効/無効を切り替える	ボタンで有効/無効を切り替え
逆方向通過	ボタンで有効/無効を切り替え	ボタンで有効/無効を切り替える
通過時間超過	ボタンで有効/無効を切り替える	ボタンで有効/無効を切り替える
侵入検知アラーム	ボタンで有効/無効を切り替える	ボタンで有効/無効を切り替える
テイルゲートアラーム	ボタンで有効/無効を切り替える	ボタンで有効/無効を切り替える
オーバーステイアラーム	ボタンで有効/無効を切り替える	ボタンで有効/無効を切り替え
モーター点検	ボタンで設定	ボタンで設定
自己診断音声ガイド	ボタンで有効/無効を切り替える	ボタンで有効/無効を切り替える
学習モードの音声ガイド	ボタンで有効/無効を切り替える	ボタンで有効/無効を切り替える

注意

- 詳細については、「*ボタン設定の説明*」を参照してください。
- デバイスにアクセス制御ボードが搭載されていない場合、スピーカーはメイン拡張インターフェースボードに接続する必要があります。
- デバイスにアクセス制御ボードが搭載されている場合、スピーカーはアクセス制御ボードに接続する必要があります。カスタム放送コンテキストはウェブ経由で設定可能です。詳細については*「プロンプトスケジュール」を*参照してください。

4.4.1 ボタンによる設定

ボタン説明

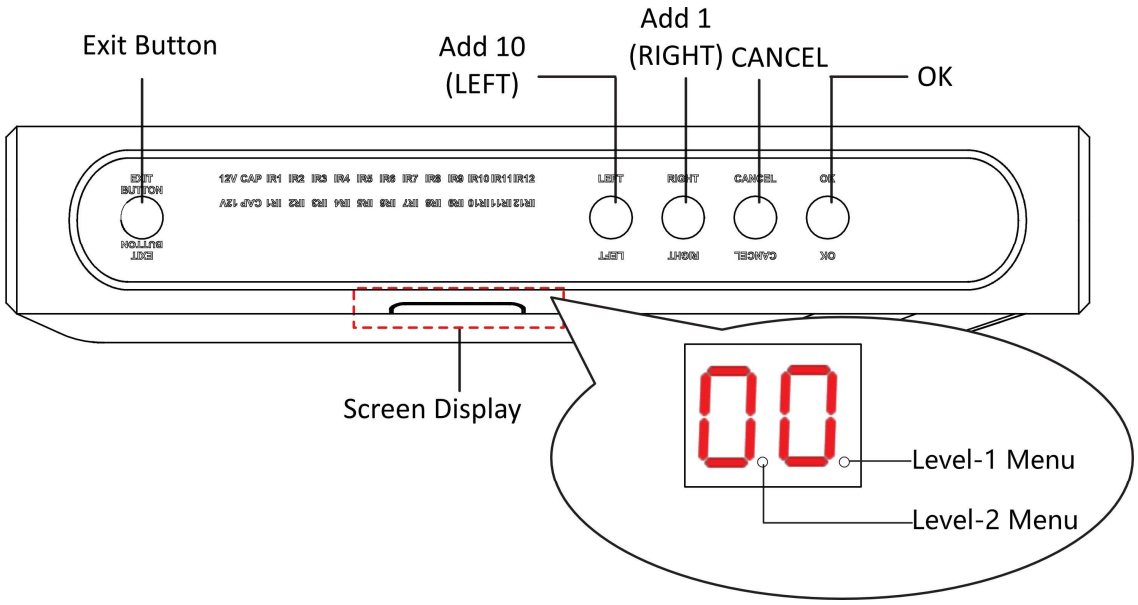


図4-16 ボタン

退出ボタン

- 押すと、入口位置からバリアを開きます。
- 2回押すと、出口位置からバリアを開きます。

パラメーター設定ボタン

- 左：設定データに10を加えるために押します。
- 右：1つの設定データを追加するには、ここを押してください。
- キャンセル：レベル 1 メニューに戻ります。または、レベル 1 メニューを終了します。
- OK：設定を確認、または設定モードに入る、またはレベル 2 メニューに入る。

注

- 設定 No. は 2 桁のデジタルチューブで表示されます。
- レベル 1 メニュー：右側の小数点が点灯している場合は、レベル 1 メニューを示しています。数字は設定番号を表しています。
- レベル 2 メニュー：中央の小数点が点灯している場合は、レベル 2 メニューです。数字は設定番号を表します。

ボタン設定手順

ここでは、侵入検知の持続時間を 12 秒に設定する場合を例に説明します。

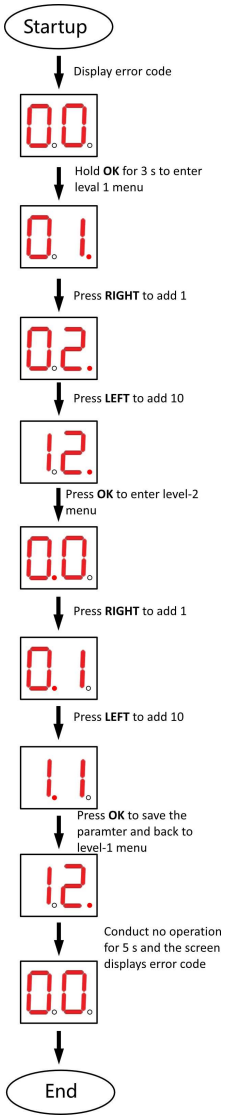


図4-17 手順

手順:

1. **OK** ボタンを 3 秒間押し続けて、ビープ音が 1 回鳴るまで待ちます。デバイスが設定モードに入ります。レベル 1 メニューが点灯します。ディスプレイ画面に設定番号 **1** が表示されます。
2. レベル 1 メニューで、**左**（+10）**を** 1 回、**右**（+1）を 2 回押して、設定番号を 12 に設定します。**OK** を押して設定を保存し、レベル 2 メニューに入ります。または、**CANCEL** を押して現在のメニューを終了するか、5 秒間操作を行わないと、設定がキャンセルされ、現在のメニューが終了します。
3. レベル 2 メニューに入った後、**左**（+10）を 1 回、**右**（+1）を 2 回押して、設定番号を 12 に設定します。**OK** を押して設定を保存します。または、**CANCEL** を押して現在のメニューを終了するか、5 秒間操作を行わないと、設定がキャンセルされ、現在のメニューが終了します。

注意

- 設定番号が順番に表示されます。
- 各設定 No. は、機能に対応しています。設定 No. とその機能の詳細については、*「ボタン設定の説明」*を参照してください。

4.4.2 学習モード設定

デバイスのバリアの閉位置を設定します。

ボタンを使用して学習モードを設定する

ボタン設定を通じてスタディモードに入り、デバイスのバリアの閉位置を設定します。

手順

注意

- デバイスにアクセス制御ボードが搭載されている場合、アクセス制御ボード上のDIPスイッチのみを使用して学習モードを設定できます。
- ボタンの操作に関する詳細については、*「ボタンによる設定」*を参照してください。
- 設定番号とその機能については、*「ボタン設定の説明」*を参照してください。

1. 学習モードに入ります。

1) 設定モードに入ります。

2) レベル 1 の設定 No. を **1** に設定します。デバイスは学習モードに入ります。

3) レベル 2 メニューの設定 No. を **2** に設定します。デバイスは学習モードに入ります。

2. デバイスの電源をオフにし、バリアを台座に対して垂直になるまでスイングします。

3. 装置の電源をオンにします。
デバイスは現在の位置を自動的に記憶します。

4. **「研究完了」**の音声が聞こえたら、デバイスを**再起動してください。**

DIP スイッチで学習モードを設定する（オプション

DIPスイッチを切り替えて学習モードに入り、デバイスのバリアの閉位置を設定します。

手順

1. 以下の図を参照して、アクセス制御ボードの 2 桁の DIP スイッチの No.1 を ON に設定し、学習モードに入ります。

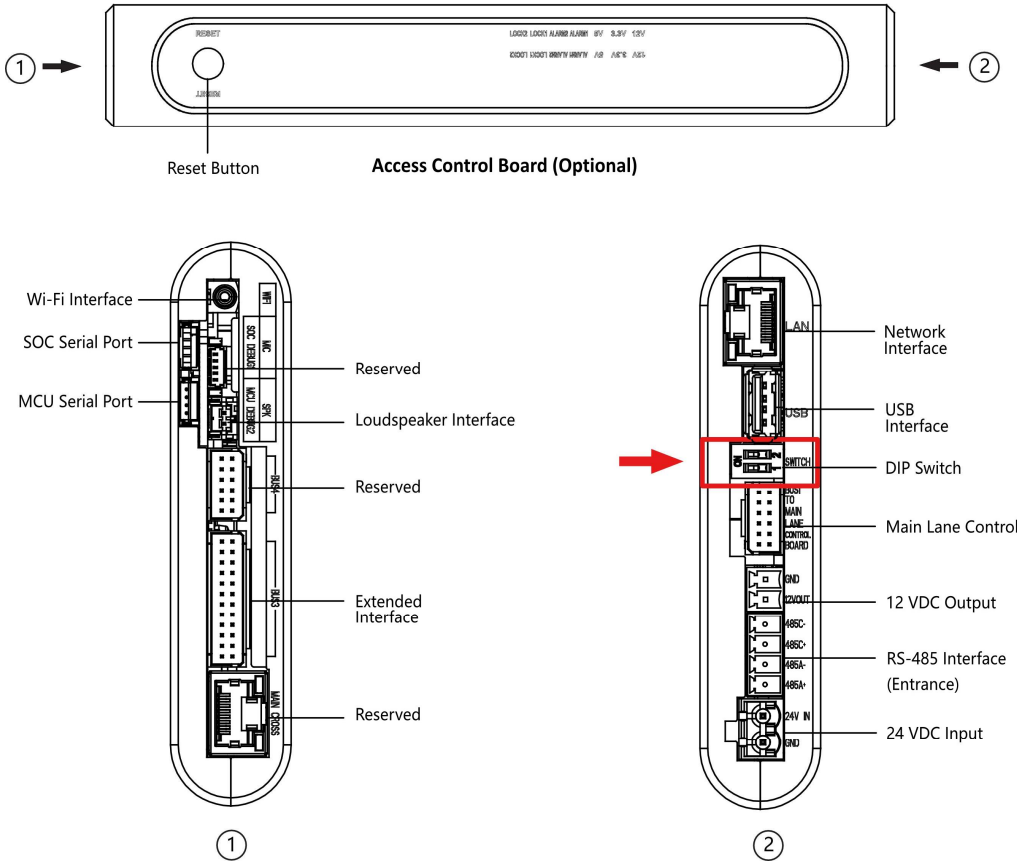


図4-18 DIPスイッチの位置

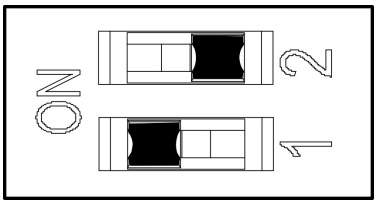


図4-19 学習モード

2. バリアの閉位置を調整します。

3. 装置の電源をオンにします。

デバイスは現在の位置（閉位置）を自動的に記憶します。

4. デバイスの電源を切ります。

5. メインユーザ拡張インターフェースボードの 2 桁の DIP スイッチの No.1 スイッチを、次の図を参照して設定します。

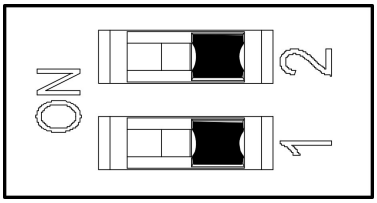


図4-20 通常モード

6. 装置の電源を再度投入します。

注意

DIP スイッチの値と意味の詳細については、「*DIP スイッチの説明」を*参照してください。

バリアが自動的に開き、閉じた位置に戻ります。この状態では、デバイスは正常モードに入ります。

4.4.3 キーフォブペアリング

キーフォブをボタンまたはDIPスイッチでペアリングします。

キーフォブをボタンでペアリングします。

キーフォブをデバイスにボタン操作でペアリングし、バリアをリモートで開閉します。

開始前に

技術サポートまたは営業部門にお問い合わせいただき、キーフォブをご購入ください。

手順

注意

- デバイスにアクセス制御ボードが搭載されている場合、キーフォブはアクセス制御ボードのDIPスイッチのみを使用してペアリングできます。
- ボタンの操作詳細については、***「ボタンによる設定」***を参照してください。
- 設定番号とその機能の詳細については、「***ボタン設定の説明」***を参照してください。
- キーフォブの操作手順の詳細については、キーフォブのユーザーマニュアルをご確認ください。

1. キーフォブのペアリングモードに入ります。

1) 設定モードに入ります。

2) レベル 1 の設定番号を **2** に設定します。デバイスはキーフォブペアリングモードに入ります。

3) レベル 2 メニューの設定 No. を **2** に設定します。デバイスはキーフォブペアリングモードになります。

2. Closeボタンを10秒以上長押しします。

ペアリングが完了すると、キーフォブのインジケーターが点滅します。

3. キーフォブペアリングモードを終了します。
1) 設定モードに入ります。
2) レベル 1 の設定番号を **2** に設定します。デバイスはキーフォブペアリングモードに入ります。
3) レベル 2 メニューの設定番号を **1** に設定します。デバイスはキーフォブペアリングモードを終了します。

4. デバイスを再起動して設定を有効化します。

DIP スイッチによるキーフォブのペアリング（オプション

DIPスイッチを使用してリモートコントロールをデバイスとペアリングし、バリアをリモートで開閉できるようにします。

開始前に

技術サポートまたは営業部門にお問い合わせいただき、キーフォブをご購入ください。

手順

1. ターンスタイルの電源を切ってください。

2. アクセス制御ボードのDIPスイッチのNo.2スイッチをON側に設定します。

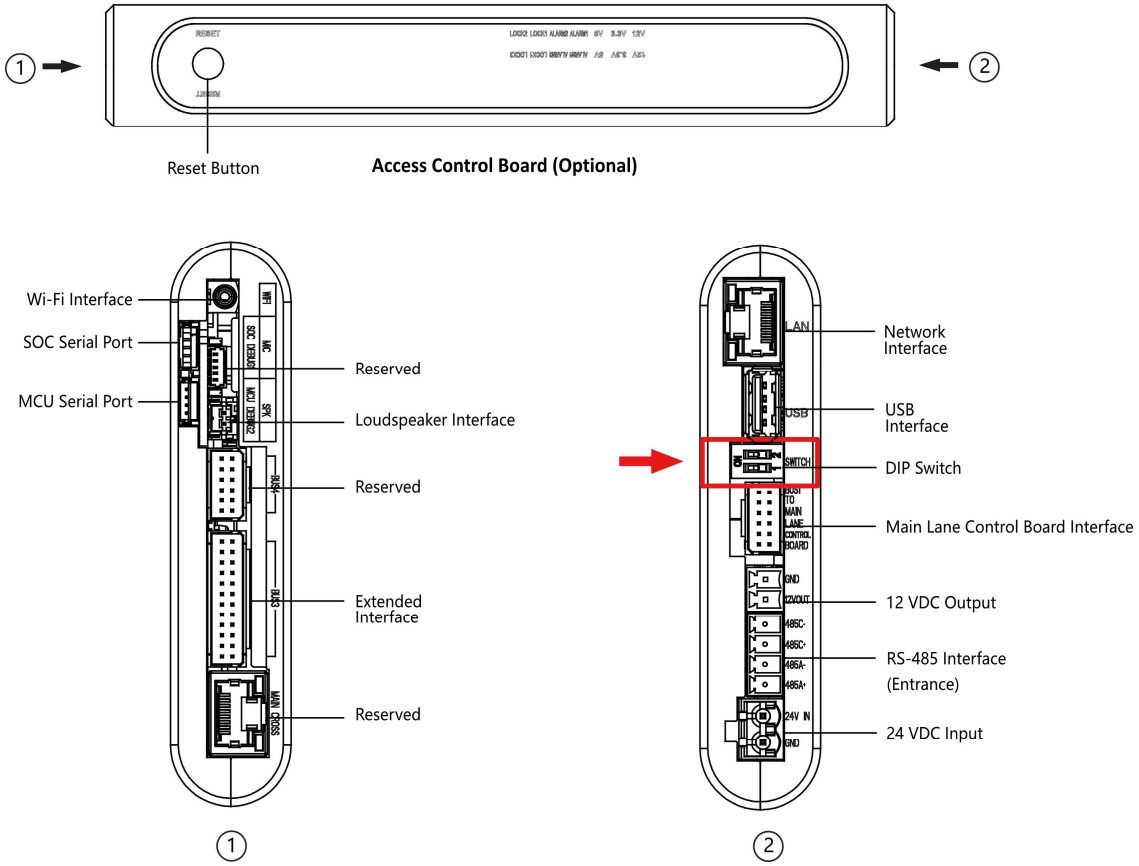


図4-21 DIPスイッチの位置

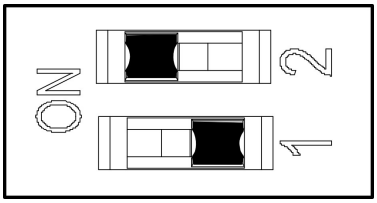


図4-22 キーフォブペアリングモードの有効化

3. ターンスタイルの電源を入れ、キーフォブペアリングモードに入ります。
4. **クローズ**ボタンを10秒以上長押しします。

   ペアリングが完了すると、キーフォブのインジケーターが2回点滅します。
5. No.2スイッチをOFF側に設定し、ターンスタイルを再起動して有効にしてください。

注意

- キーフォブは1つのターンスタイルのみとペアリング可能です。複数のターンスタイルがペアリングモードの場合、キーフォブはそれらの中から1つを選択してペアリングします。
- DIP スイッチの値と意味の詳細については、「***DIP スイッチの説明」を***参照してください。

6. **オプション：**クライアントソフトウェアのリモコンページで、**[System→ User→ Keyfob User]** に移動し、キーフォブを削除します。

4.4.4 デバイスの初期化

手順

1. アクセス制御ボードの初期化ボタンを5秒間押し続けてください。

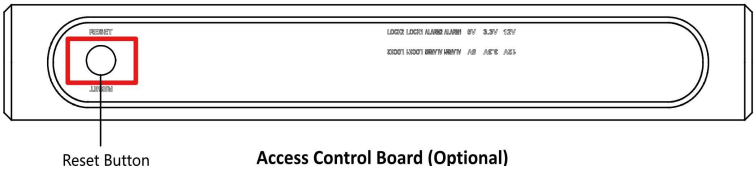


図4-23 初期化ボタン的位置

2. デバイスは工場出荷時設定への復元を開始します。
3. プロセスが完了すると、デバイスが3秒間ビープ音を鳴らします。

注意

デバイスの初期化を行うと、すべてのパラメータがデフォルト設定に戻り、デバイスのイベントはすべて削除されます。

注意

デバイスの電源を入れる際は、レーンに人がいないことを確認してください。

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。デバイスの電源をオンにすると、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、SADP ツール、および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次のとおりです。

- デフォルトのIPアドレス：192.0.0.64
- デフォルトのポート番号：80
- デフォルトのユーザー名：admin

5.1 ウェブブラウザーによるアクティベーション

ウェブブラウザーからデバイスをアクティベートすることができます。

手順

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

   Enterキーを押します。

   デバイスのIPアドレスとコンピュータのIPアドレスが同じIPセグメント内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

   強力なパスワードを推奨 - 製品のセキュリティを強化するため、お客様独自の強力なパスワード（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、セキュリティの高いシステムでは、パスワードを定期的にリセットすることをお勧めします。パスワードを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。

3. アクティベートをクリックしてください。
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で編集できます。

5.2 モバイルウェブ経由でアクティベート

モバイルウェブ経由でデバイスをアクティベートできます。

手順

1. モバイルフォンでデバイスのホットスポットに接続し、ホットスポットのパスワードを入力します。

注意

- 非アクティブなデバイスでは、ホットスポットはデフォルトで有効になっています。
- デフォルトのホットスポットパスワードは、デバイスのシリアル番号です。

ログインページがポップアップ表示されます。

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

強力なパスワードをお勧めします - 製品のセキュリティを強化するため、お客様ご自身で強力なパスワード（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、セキュリティの高いシステムでは、パスワードを定期的にリセットすることをお勧めします。パスワードを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。

「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。

注意

3. アクティベートをクリックしてください。

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で編集できます。

5.3 SADP経由でアクティベート

SADPは、LAN経由でデバイスの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

- 付属のディスクまたは公式ウェブサイト ***http://www.hikvision.com/en/*** からSADPソフトウェアを取得し、表示される指示に従ってSADPをインストールしてください。
- SADPツールを実行するデバイスとPCは、同じサブネット内に配置されている必要があります。

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ます。バッチ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一覧から対象のデバイスを検索し、選択します。

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ます。

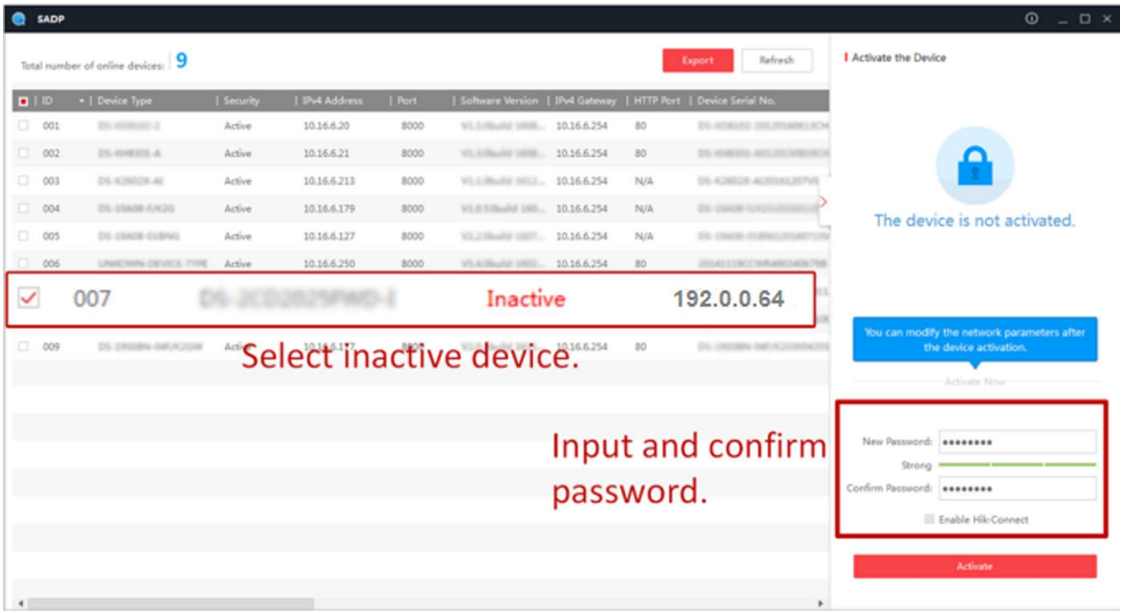
注意

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、お客様独自の強力なパスワード（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、特にセキュリティの高いシステムでは、パスワードを定期的にリセットすることをお勧めします。パスワードを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」を含む文字列は、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。



アクティベーションが成功すると、デバイスの状態が「**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) デバイスを選択してください。
   2) 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設定するため、IPアドレスを手動で変更するか、**DHCPを有効にする**チェックボックスをオンにします。
   3) 管理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化します。

5.4 iVMS-4200 クライアントソフトウェアを使用してデバイスをアクティブ化

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、パスワードを作成してデバイスをアクティベートする必要があります。

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. デバイス管理ページを開きます。
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てください。

注意
デバイスのパスワードの強度については、自動的に確認することができます。製品のセキュリティを強化するため、お客様ご自身でパスワードを変更することを強くお勧めします（8 文字以上で、大文字、小文字、数字、特殊文字の 3 種類以上を含む）。また、セキュリティ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。特に、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設定は、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」を含む文字列は、アクティベーションパスワードとして設定できません。

7. **OK**をクリックしてデバイスをアクティベートします。

第 6 章 ウェブブラウザーによる操作

6.1 ログイン

ウェブブラウザー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。

注意

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。アクティベーションの詳細については、*「アクティベーション」を*参照してください。

ウェブブラウザーからログイン

ウェブブラウザー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を表示します。デバイスのユーザー名とパスワードを入力し、**[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からログインする

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。

6.2 概要

デバイスのコンポーネントの状態、リアルタイムイベント、人物情報、ネットワークの状態、基本情報、デバイスの容量を確認できます。また、バリアをリモートで制御することもできます。

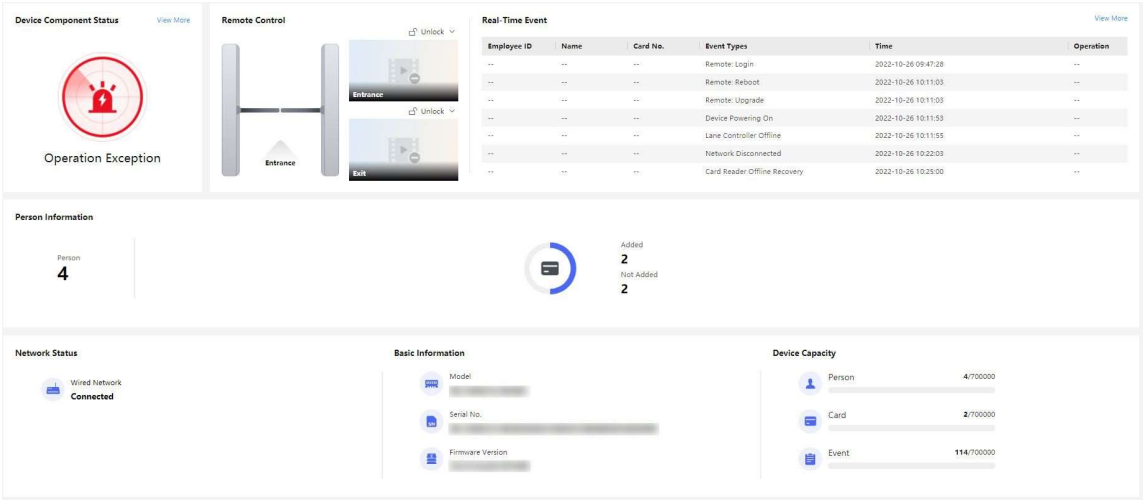


図6-1 概要

機能の説明

デバイスコンポーネントの状態

デバイスが正常に動作しているかどうかを確認できます。詳細なコンポーネントの状態を確認するには、**「詳細を表示」**をクリックしてください。

リモートコントロール

/ /

ドアが開いています/閉まっています/開いたままです/閉まったままです。

リアルタイムイベント

イベント従業員 ID、名前、カード番号、イベントの種類、時間、操作を確認できます。また、**「詳細」**をクリックして、イベントの種類、従業員 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」**をクリックすることもできます。結果は右側のパネルに表示されます。

人物情報

人物とカードに関する追加済みと未追加の情報を確認できます。

ネットワークステータス

ネットワーク接続の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。

デバイスの容量

人物、カード、イベントの容量を確認できます。

6.3 人物管理

「追加」をクリックして、基本情報、証明書、認証、設定を含む人物の情報を追加できます。

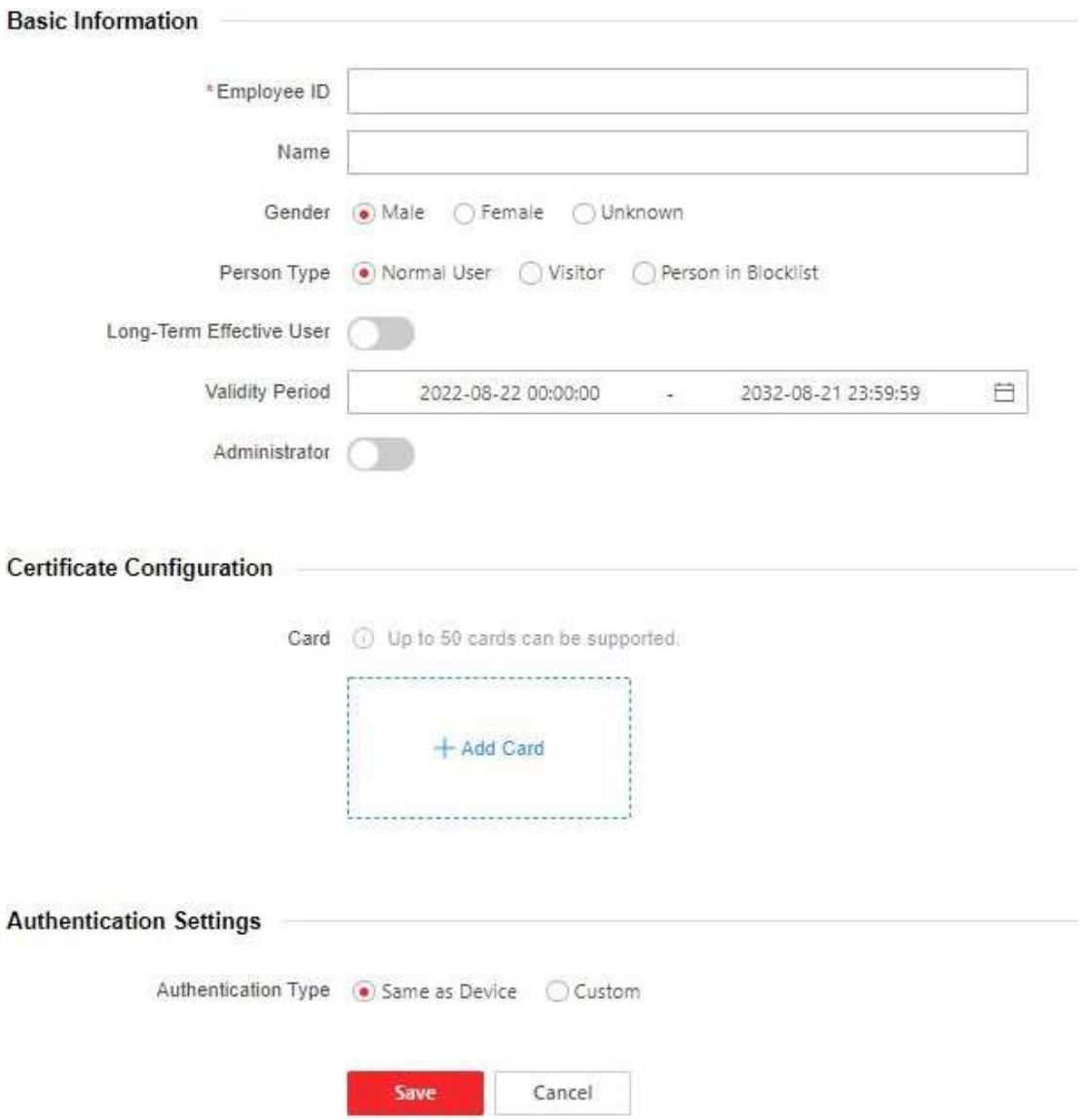


図6-2 ユーザーを追加

基本情報の追加

「人物管理」をクリックし、**「→」の「追加」**をクリックして「人物を追加」ページに移動します。
従業員ID、従業員の名前、従業員の種類を含む、従業員の基本情報を入力します。
「訪問者」を人物タイプとして選択した場合、訪問時間を設定できます。設定を
保存するには**「保存」**をクリックしてください。

アクセス権限時間を設定

「Person Management」をクリックし、**「→」をクリックして**「Add Person」ページに移動します。

「長期有効ユーザーを有効にする」を選択するか、**有効期間**を設定すると、ユーザーは設定した期間内のみ権限を取得できます。
設定を保存するには**「保存」**をクリックしてください。

カードを追加

「ユーザー管理」をクリックし、**「→」を選択し**、「追加」**をクリックして**「ユーザー追加」ページに移動します。
カードを追加] をクリックし、**カード番号を入力**して**プロパティ**を選択し、**[OK]** をクリックしてカードを追加します。

注意

最大 50 枚のカードを追加できます。**保**

存をクリックして設定を保存します。

認証設定

「Person Management」をクリックし、**「→」をクリックし、**「Add」をクリックして「Add Person」ページに移動します。**認証タイプを「Same as Device」**または**「Custom」**に設定します。
設定を保存するには**「保存」**をクリックしてください。**ユーザーデータのインポート/エクスポートユーザーデータのエクスポート**

追加した人物データをバックアップや他のデバイスへのインポートのためにエクスポートすることができます。
「ユーザーデータをエクスポート」をクリックし、暗号化パスワードを設定して確認します。**OK**をクリックします。

注意

- 個人データがPCにダウンロードされます。
- 設定したパスワードは、データファイルのインポート時に必要になります。

個人データのインポート

「個人データのインポート」をクリックし、ファイルを選択します。**「インポート」**をクリックします。
個人データをデバイスにインポートして同期するには、暗号化パスワードを入力してください。

6.4 イベントを検索

イベント検索をクリックして、検索ページに入ります。

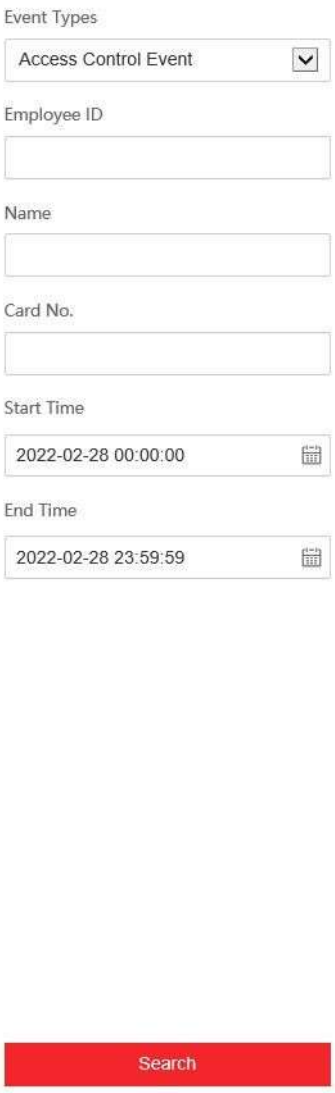


図 6-3 イベント検索

イベントタイプ、社員 ID、名前、カード番号、開始時刻、終了時刻などの検索条件を入力し、[**検索**] をクリックします。

イベントの種類には、アクセス制御イベントと ID カードイベントがあります。ID カードイベントを検索する場合は、社員 ID、名前、カード番号を入力する必要はありません。

結果は右側のパネルに表示されます。

6.5 設定

6.5.1 デバイス情報の表示

設定をクリックし、**→システム、→システム設定、→基本情報を**順に選択して設定ページに移動します。
デバイス名、言語、モデル、シリアル番号、バージョン、IO 入力、IO 出力、ローカル RS-485 番号を確認できます。
デバイス名を変更し、**保存**をクリックできます。
人、カード、イベントなど、デバイスの容量を確認できます。

6.5.2 時間を設定

デバイスの時間を設定します。

設定をクリックし、**→システム、→システム設定、→時間設定を選択します**。

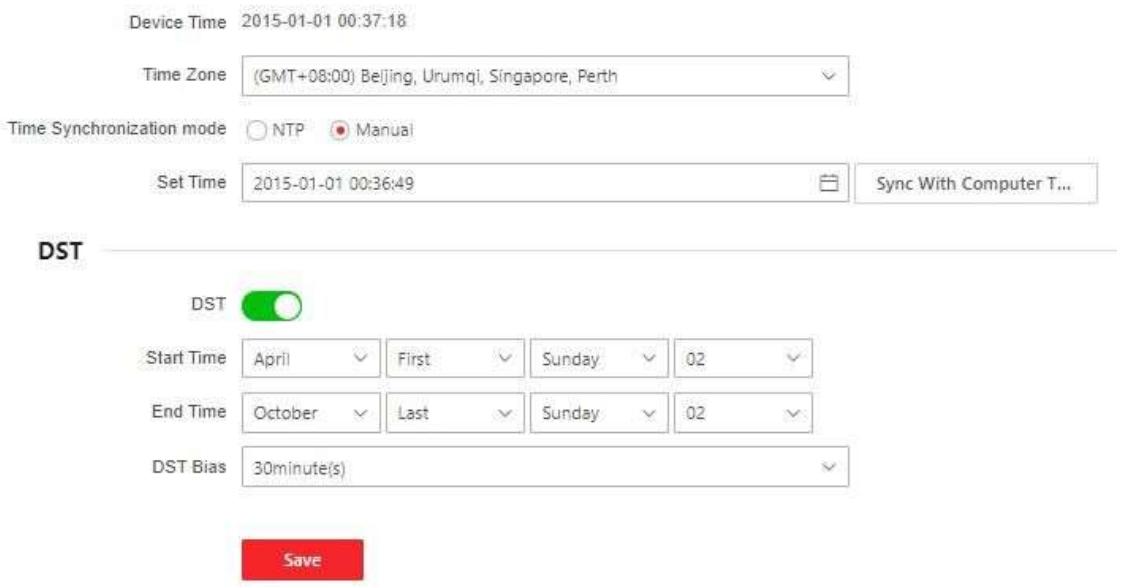


図6-4 時間設定

設定を保存するには、設定後に「**保存**」をクリックします。

タイムゾーン

ドロップダウンリストからデバイスの所在するタイムゾーンを選択します。

タイムシンク。

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されます。デバイスの時刻を手動で設定するか、または**「コンピュータの時刻と同期」**を選択**して**、デバイスの時刻をコンピュータの時刻と同期させることができます。

サーバー アドレス タイプ/サーバー アドレス/NTP ポート/間隔

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

6.5.3 DSTの設定

手順

1. **「設定」**をクリックし、**「→ 」→「システム」→「→ 」→「システム設定」→「→ 」→「Time Settings」**を選択します。
2. **DST**を有効にします。
3. DSTの開始時間、終了時間、およびバイアス時間を設定します。
4. 設定を保存するには**「保存」**をクリックしてください。

6.5.4 管理者のパスワードを変更する

手順

1. **「設定」**をクリックし、**→ユーザー管理を選択します**。
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. **[OK]** をクリックします。

注意

デバイスのパスワードの強度は自動的にチェックすることができます。製品のセキュリティを強化するため、お客様ご自身でパスワードを変更することを強くお勧めします（8 文字以上、大文字、小文字、数字、特殊文字の 3 種類以上を含む）。また、セキュリティ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。パスワードを毎月または毎週変更することで、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設定は、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。

6.5.5 オンラインユーザー

デバイスにログインしたユーザーの情報を表示します。

[Configuration] (設定) **[→] (システム) [→] (ユーザー管理) [→] (オンラインユーザー)** に移動して、オンラインユーザーのリストを表示します。

6.5.6 デバイス武装/解除情報の表示

デバイスの武装タイプと武装IPアドレスを表示します。

[Configuration] (設定) [→] (ユーザー) [→] (ユーザー管理) [Arming/Disarming Information] (武装/武装解除情報) に移動します。デバイスの武装/解除情報を表示できます。ページを更新するには**「リフレッシュ」**をクリックしてください。

6.5.7 ネットワーク設定

TCP/IP、ホットスポット、およびHTTP(S)パラメーターを設定します。

基本ネットワークパラメータの設定

設定」をクリックし、**「→」**をクリックします**。ネットワーク」をクリックし、「→」をクリックします。ネットワーク設定」をクリックし、「→」をクリックします。TCP/IP**」をクリックします。

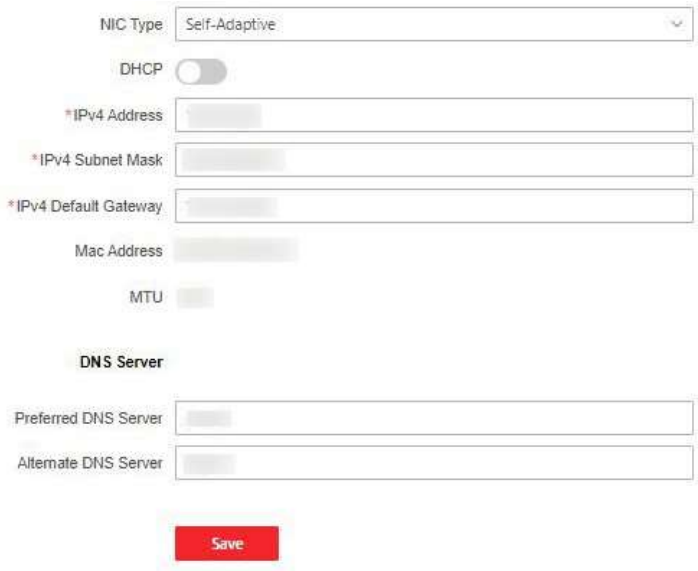


図6-5 TCP/IP 設定ページ

パラメーターを設定し、**[保存]** をクリックして設定を保存します。

NIC タイプ

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

DHCP

この機能をオフにすると、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。

この機能を有効にすると、システムが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

お好みのDNSサーバーと代替DNSサーバーを、実際の必要に応じて設定してください。

デバイス ホットスポット

デバイスのホットスポットを設定します。

[設定]、**[→]**、**[ネットワーク]**、**[→]**、**[ネットワーク設定]**、**[→]**、[**デバイスホットスポット**] の順にクリックします。**デバイスホットスポットを有効にするには**、クリックします。ホットスポットの**名前**と**パスワード**を設定します。

保存をクリックします。

ポートパラメーターを設定します。

HTTP、HTTPS、およびHTTPリスニングパラメーターを設定します。

[Configuration]、**[→]**、**[Network]**、**[→]**、**[Network Service]**、**[→]**、**[HTTP(S)]** の順にクリックします。

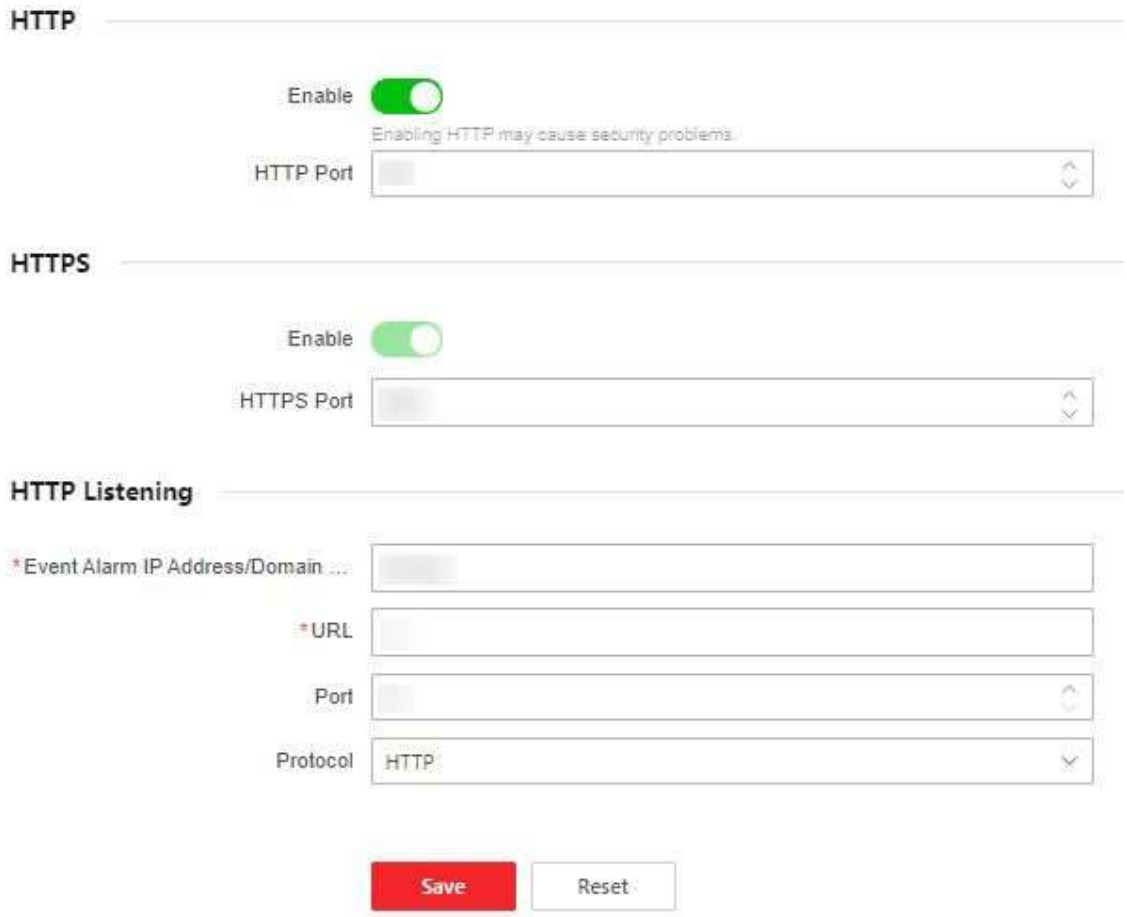


図 6-6 ネットワークサービス

HTTP

これは、ブラウザがデバイスにアクセス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、ログインするにはブラウザに ***http://192.0.0.65:81*** と入力する必要があります。

HTTPS

ブラウザへのアクセスにHTTPSを設定します。アクセス時には証明書が必要です。

HTTP リスニング

デバイスは、HTTP プロトコル/HTTPS プロトコルを介して、イベントアラームの IP アドレスまたはドメイン名にアラーム情報を送信できます。イベントアラームの IP アドレスまたはドメイン名、URL、ポート、およびプロトコルを編集します。

注意

イベントアラームの IP アドレスまたはドメイン名は、アラーム情報を受信するために *HTTP プロトコル/HTTPS プロトコル*に対応している必要があります。

.

6.5.8 オーディオパラメータの設定

画像の品質、解像度、およびデバイスの音量を設定します。

オーディオパラメータの設定

[Configuration] (構成) をクリックし、**[→] (ビデオ/オーディオ)** をクリックし、**[→] (オーディオ)** をクリックします

図 6-7 オーディオパラメータの設定

ブロックをドラッグして出力音量を調整します。
設定後、**保存**をクリックして設定を保存します。**音声プロンプトを**
有効にすることもできます。

注
機能はモデルによって異なります。詳細は実際のデバイスをご確認ください。

6.5.9 イベントのリンク方法

イベントに連動する動作を設定します。

手順

1. **[Configuration]、[→]、[Event]、[→]、[Event Detection]、[→]、[Linkage Settings]** の順にクリックして、ページを表示します。

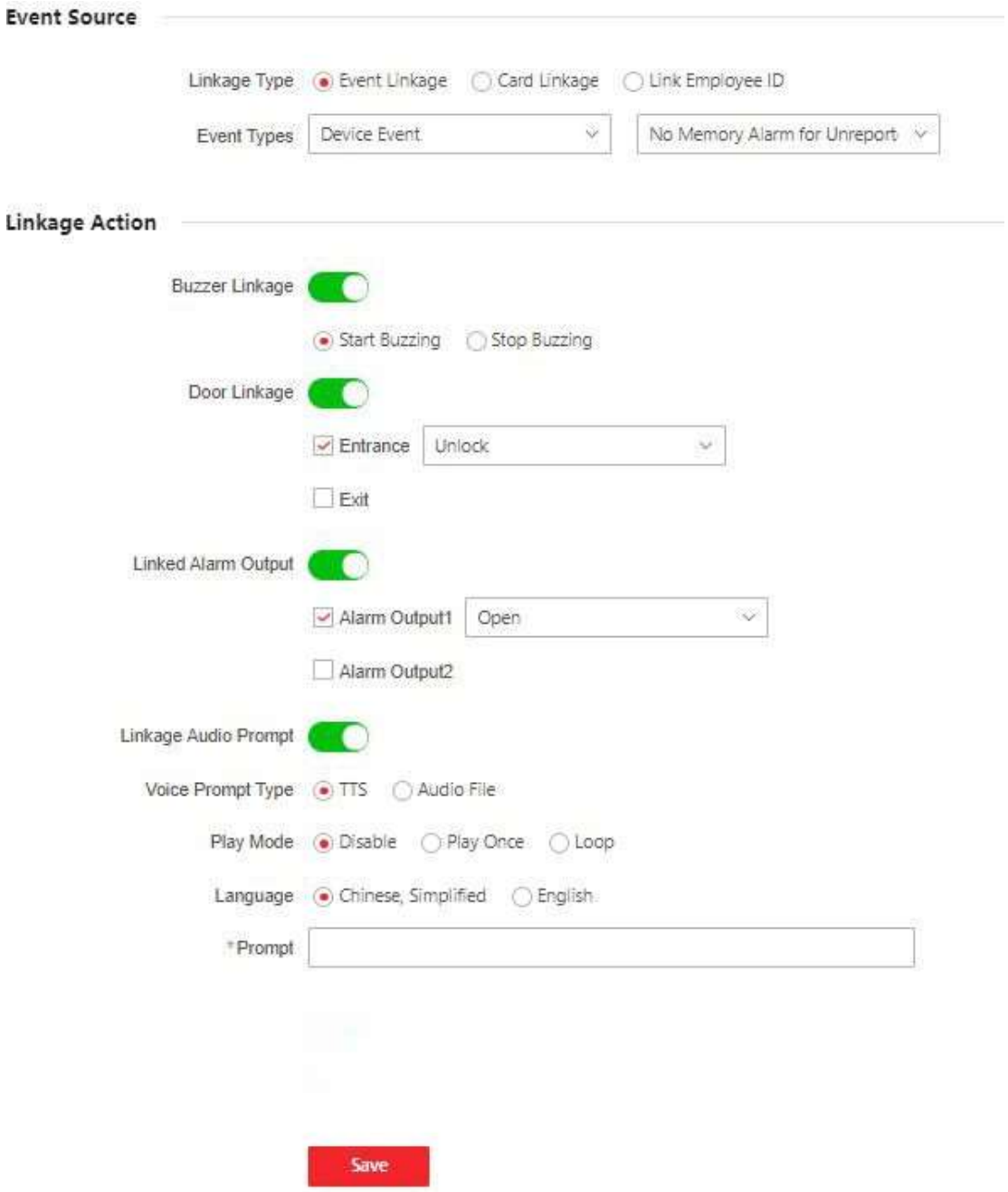


図 6-8 イベントリンク

2. イベントソースを設定します。

- **リンク方法を「イベントリンク」**に選択した場合は、イベントタイプをドロップダウンリストから選択する必要があります。

  ドロップダウンリストから選択する必要があります。
- **リンクタイプを「カードリンク」**に選択した場合は、カード番号を入力し、カードリーダーを選択する必要があります。

- **リンク方法を**「**従業員 ID リンク**」に選択した場合は、従業員 ID を入力し、カードリーダーを選択する必要があります。

3. 関連アクションを設

定します。

リンクされたブザー

リンクされたブザーを有効にし、ターゲットイベントに対して**「ブザーを鳴らす」**または「**ブザーを停止する」**を選択します。

リンクドア

リンクドアを有効にし、**[入室]** または **[退室]** をチェックし、対象イベントのドアの状態を設定します。

リンクアラーム出力

リンクアラーム出力を有効にし、**アラーム出力 1** または**アラーム出力 2** をチェックし、対象イベントのアラーム出力ステータスを設定します。

リンクされたオーディオプロンプト

リンクされたオーディオプロンプトを有効にし、再生モードを選択します。

- **TTS** を選択した場合は、言語を設定し、プロンプトの内容を入力する必要があります。
- **オーディオファイル**を選択した場合は、ドロップダウンリストから利用可能なオーディオファイルを選択するか、**[全般リンク設定]** をクリックして新しいオーディオファイルを追加する必要があります。

6.5.10 アクセス制御設定

認証パラメーターの設定

「設定」をクリックし、**「→」→「アクセス制御」→「→認証設定」を選択します**。

注意

機能はモデルによって異なります。詳細については、実際のデバイスを参照してください。

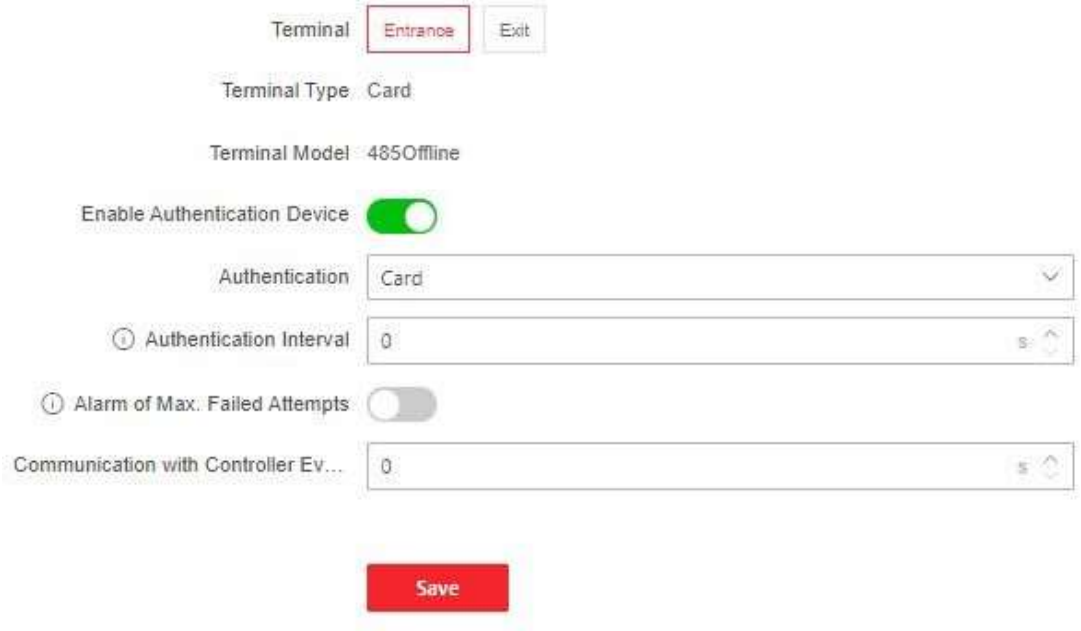


図6-9 認証パラメーターの設定

設定を保存するには、設定完了後に**「保存」**をクリックしてください。

ターミナル

設定のために**「入口」**または**「出口」**を選択してください。

ターミナルタイプ/ターミナルモデル

ターミナル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

実際の要件に応じて、ドロップダウンリストから認証モードを選択します。

認証間隔

同じユーザーが認証を行う際の認証間隔を設定できます。設定された間隔内では、同じユーザーは1回のみ認証可能です。2回目の認証は失敗します。

最大失敗回数アラーム

カード読み取り回数が設定値に達したときにアラームを報告できるようにします。

最大認証失敗回数

カード読み取り試行回数が設定値に達した場合にアラームを報告します。

コントローラーとの通信間隔

アクセス制御装置がカードリーダーと設定された時間を超えて接続できない場合、カードリーダーは自動的にオフラインになります。

注意
認証間隔の値は2秒から255秒の範囲です。

ドアパラメーターの設定

設定をクリックし、**→アクセス制御→ドアパラメーターを選択します。**

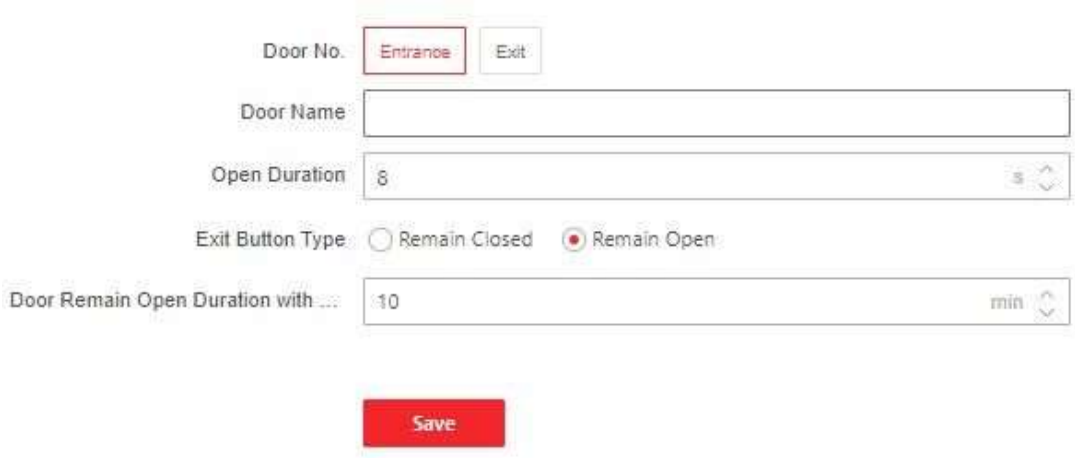


図6-10 ドアパラメーター設定ページ

設定を保存するには、設定完了後に**「保存」**をクリックしてください。

ドア番号

設定対象を「**入口**」または「**出口**」から選択します。

ドア名

ドアの名前を指定できます。

開錠時間

ドアの解錠時間を設定します。設定した時間内にドアが開かれない場合、ドアはロックされます。

注意
時間は5秒から60秒まで設定可能です。

退出ボタンタイプ

出口ボタンを、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。デフォルトでは「**開いたまま**」に設定されています。

最初の人が入った際のドアの開いたままの持続時間

最初の人がドア内にいる間のドアの開いた状態の持続時間を設定します。最初の人が認証されると、複数の人がドアにアクセスしたり、他の認証アクションを実行したりできるようになります。

注意
時間は1秒から1440秒まで設定可能です。

シリアルポート設定

シリアルポートのパラメーターを設定します。

手順

1. **「設定」**をクリックし、**「→」→「アクセス制御」→「→」→「シリアルポート設定」を選択します。**

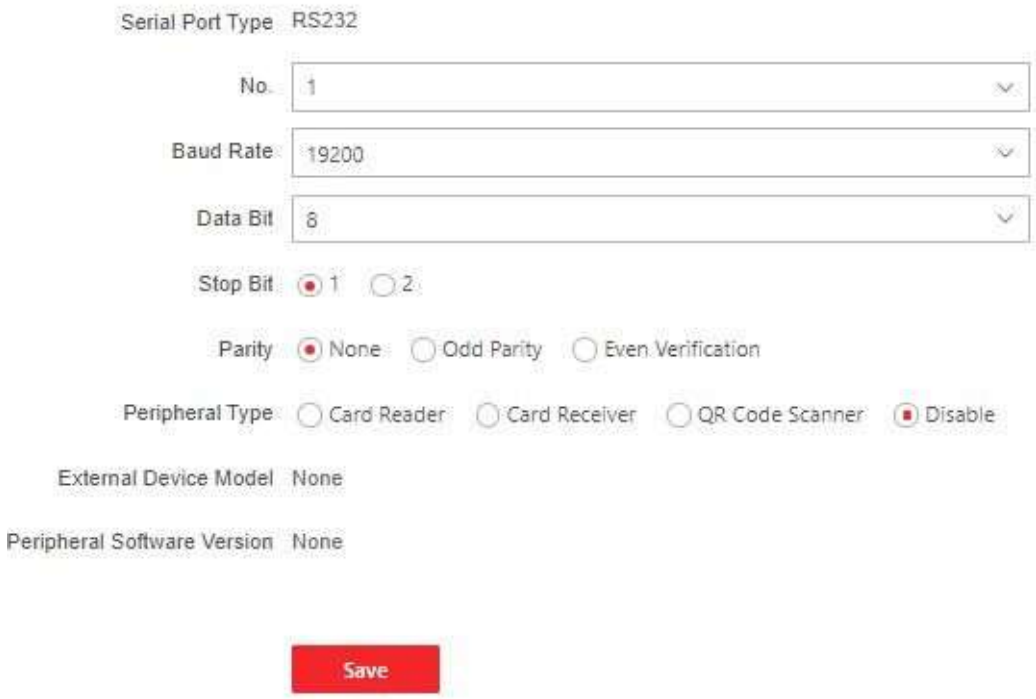


図6-11 シリアルポート設定

2. **No.**、**ボーレート**、**データビット**、**ストップビット**、**パリティ**を設定します。

3. **周辺機器の種類**を**カードリーダー**、**QRコードスキャナー**、または**無効に設定**します。

4. シリアルポートの種類、接続されたデバイスのモデル、および周辺機器ソフトウェアのバージョンを確認できます。

5. **保存**をクリックします。

ワイガンドパラメーターを設定します。

Wiegand伝送方向を設定できます。

手順

注意
一部のデバイスモデルではこの機能に対応していません。設定時は実際の製品をご確認ください。

1. **設定**をクリックし、**→アクセス制御、→Wiegand設定を選択します**。
2. **入口**または**出口**を選択します。
3. **Wiegand**機能を有効にします。
4. Wiegandの送信方向はデフォルトで**入力**に設定されています。

   注意
   入力：このデバイスはWiegandカードリーダーを接続できます。
5. 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ーを保存した後、デバイスは自動的に再起動します。

ホストパラメーター

ドア接点の設定と RS-485 プロトコルを設定します。

手順

1. **「設定」**をクリックし、**「→」→「アクセス制御」→「→ホストパラメーター」**を選択してページに移動します。
2. ドアコンタクトを設定します。

   注
   ドアコンタクトは、実際のニーズに応じて**「ドア開状態」**または**「ドア閉状態」**に設定できます。デフォルトでは**「ドア開状態」**です。
3. RS-485 プロトコルを設定します。
4. **保存**をクリックします。

ターミナルパラメーターを設定します。

動作モードとリモート検証を設定します。

手順

1. **「設定」→「→」→「アクセス制御」→「→」→「Terminal Parameters」**をクリックしてページに移動します。

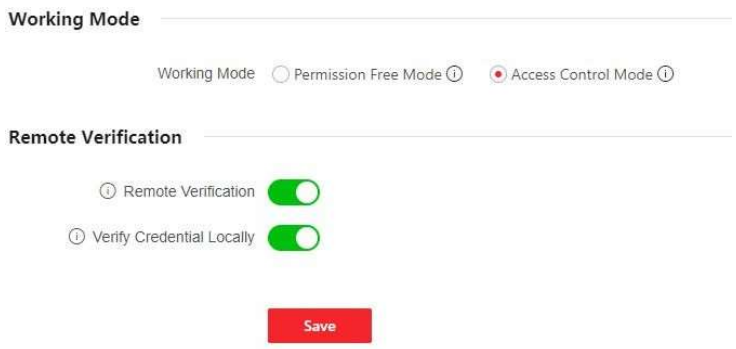


図6-12 ターミナルパラメーター

2. デバイスの動作モードを設定します。

許可フリーモード

デバイスはユーザーの許可を確認しません。ただし、ユーザーの有効期間のみを確認します。ユーザーが有効期間内にある場合、バリアが開きます。

「ローカルで資格情報を検証」機能を有効にできます。この機能を有効にすると、デバイスはスケジュールテンプレートなどなしで、ユーザーの権限のみを検証します。

アクセス制御モード

デバイスは通常通り動作し、バリアを開くためのユーザーの権限を確認します。

3. リモート検証を設定します。

1) **リモート検証を**有効にします。

注意

デバイスは、ユーザー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、バリアを開くかどうかを判断します。

2) **オプション：ローカルでの認証情報の確認を**有効にします。

注意

機能有効化後、デバイスはスケジュールテンプレートなどなしで、ユーザーの権限のみを確認します。

4. **「保存」**をクリックして、端末のパラメーター設定を完了してください。

6.5.11 ターンスタイル

基本パラメーター

ターンスタイルの基本パラメーターを設定します。

手順

1. **「設定」**をクリックし、**「→ターンスタイル」→「→基本設定」**を選択してページに移動します。

2. **デバイスタイプ**、**デバイスモデル**、および**動作状態**を確認します。

3. **バリアの材質**、**レーン幅**、**バリアの高さ**、**バリアの開閉速度**を設定します。

4. 通過モードを設定します。

- **「一般通行」**を選択すると、入口と出口のバリアの状態をドロップダウンリストから選択できます。

注意

ーモードを設定した場合、バリアは開いたままになり、認証に失敗した際に閉まります。

- **「週間スケジュール」**を選択した場合、入口と出口のバリアの週間スケジュールを設定できます。

5. **保存**をクリックしてください。

キーフォブ

キーフォブのパラメーターを設定します。

手順

1. **設定**をクリックします**。→ターンスタイル→キーフォブ**をクリックしてページに移動します。

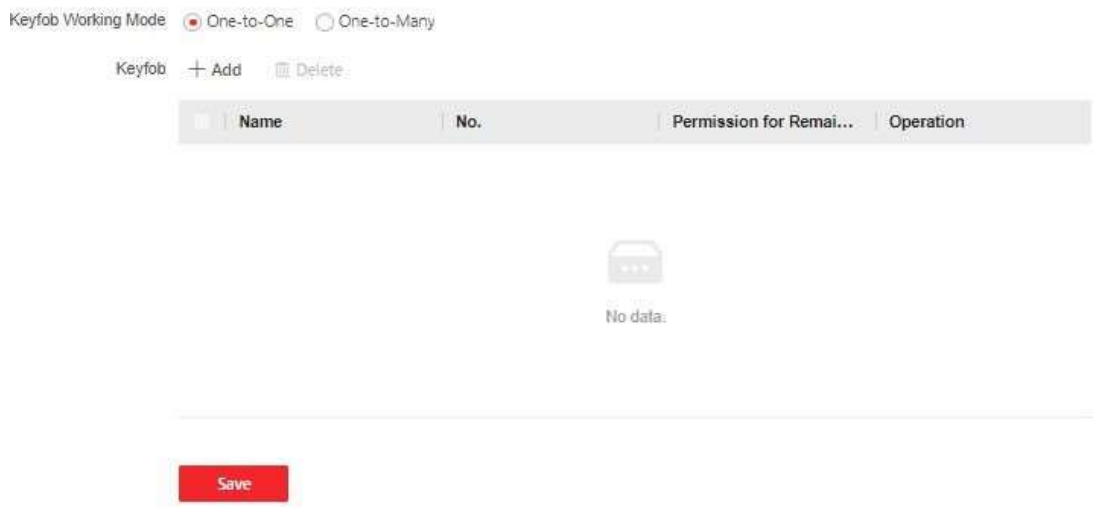


図6-13 キーフォブ

2. **作業モードを「1対1」**または**「1対多」**に設定します。

3. キーフォブを追加します。

1) **「追加」**をクリックすると、キーフォブ追加ウィンドウがポップアップ表示されます。

2) **名前**と**シリアル番号**を入力します。

3) 実際の必要に応じて**「常時開錠許可」を**有効にします。

4) **「OK」**をクリックしてキーフォブを追加します。

4. オプション：キーフォブを選択し、**[削除]** をクリックしてキーフォブを削除します。

5.「保存」をクリックします。

赤外線検出器

赤外線検出器を設定します。

手順

1.「設定」をクリックし、「→」→「**Turnstile**」→「→」→「**IR Detector**」をクリックしてページに移動します。

図6-14 IR検出器

2. 入口と出口の誘導モードを「**単一トリガー**」または「**同時トリガー**」に設定してください。

3. カスタム赤外線検出モードを設定します。

赤外線緊急モードを有効にします。

一部の赤外線ビームが正常に動作しない場合、それらの赤外線ビームを遮断してレーンを復旧できます。ただし、この操作は人に当たって怪我を引き起こす可能性があります。

ドア閉塞時のカスタムアンチピンチ機能を有効にします。

ドア閉め時のアンチピンチとは、デバイスがレーン内に人を検出した場合、バリアが閉まらない機能です。人がレーンから出た後にのみ、バリアが閉まります。この機能を有効にすると、バリアを閉める際に赤外線ビームの一部を事前に遮断できます。ただし、この操作により人が接触し、けがをする可能性があります。

4. 保存をクリックしてください。

人検知

人数のカウントを設定します。

手順

1.「設定」をクリックし、**→ターンスタイル→人数カウント**を選択してページに移動します。

図6-15 人数カウント

2. **人数のカウントを**有効にするには、チェックボックスをオンにします。

3. 実際の必要に応じて、**デバイスオフライン時の人数カウントを**有効にします。

4. **人数のカウントタイプを**「**無効**」「**通過検出**」「**認証番号**」から選択します。

5. **オプション：クリア**をクリックして、人数のカウント情報をすべてクリアします。

インジケータの色を設定

インジケーターの色を設定します。

手順

1. 「**設定**」をクリックし、「**→ ターンスタイル**」**→**「**→ ライト設定**」を選択してページに移動します。

2. レーンステータスインジケーターのライトの色を設定します。

1) **ライトの明るさを**「**自動**」または「**固定**」に設定します。「**固定**」を選択した場合は、ブロックをドラッグするか、値を入力してライトの明るさを手動で調整できます。

2) 誘導、禁止、認証通過のライトの色を設定します。

3. バリアライトの色を設定します。

1) 実際の使用状況に応じて、**スタンバイ時にライトを点灯**させるかどうかを選択します。

2) バリアライトの色を設定します。

4. **保存**をクリックします。

その他の設定

その他のパラメーターを設定します。

手順

1. **設定**をクリックします。**→ Turnstile→ Other Settings** をクリックしてページに移動します。

2. **アラーム出力の持続時間を**設定します。

注

アラーム出力の持続時間は 0 秒から 3599 秒の範囲で設定できます。

3. **温度単位**を設定してください。
4. **車線が空いていない場合にバリアを開けないようにする**設定を有効にします。
5. ブロックをドラッグするか、値を入力して照明パネルの明るさを調整します。
6. アラームブザーの鳴動時間、ドアの閉遅延時間、侵入検知時間、滞留時間、IR 障害時間を設定します。
7. 実際の必要に応じて「**メモリモード**」を有効にします。

注意

メモリモードを有効にすると、複数人の通過に複数のカードを使用することができます。通過者の数がカード提示数を超えた場合、またはドアの開時間内に通過者がいないまま最後の通過者が通過した後、ドアは自動的に閉まります。

8. 制御モードを選択してください。

ソフトモード

尾行や強制アクセスなどがある場合、人がバリアを通過した後、バリアが閉まります。

ガードモード

テールゲート、強制アクセスなどが発生した場合、バリアは即座に閉じます。

9. 火災入力タイプを設定してください。
10. クリックして**モーターのセルフテストを**有効にし、モーターのセルフテストを開始するメインレーンまたはサブレーンを選択します。
11. **保存**をクリックしてください。

6.5.12 カード設定

カードのセキュリティを設定する

設定をクリックし、→ **カード設定、→ カードタイプ**を選択して設定画面を開きます。パラメーターを設定し、**保存**をクリックします。

NFC カードを有効にする

携帯電話がアクセス制御のデータを取得できないように、NFC カードを無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 カード有効化

M1カードを有効にすると、M1カードを提示して認証が可能になります。

M1 カード暗号化セクター

M1 カードの暗号化により、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。

機能を有効にし、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が暗号化されています。セクター13の暗号化を推奨します。

EMカード機能を有効にします

EMカードを有効化し、EMカードを提示して認証を行う機能が利用可能になります。

注意

周辺機器のカードリーダーがEMカードの提示に対応している場合、EMカード機能の有効/無効設定機能も利用可能です。

CPUカード有効化

CPU カードの有効化と、CPU カードを提示しての認証機能が利用可能です。

CPUカードの内容を読み取る

CPUカードの内容読み取り機能を有効にすると、デバイスはCPUカードの内容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。

カード認証パラメーターの設定

デバイスでカード経由で認証を行う際に、カード読み取り内容を設定します。

設定へ移動→ **カード設定→ カードNO.認証設定**

カード認証モードを選択し、必要に応じて「カード番号の逆順」を有効にします。**「保存」**をクリックします。

6.5.13 プライバシーパラメーターを設定

イベントストレージのタイプを設定します。

[設定]、[→]、[セキュリティ]、[→]、[プライバシー設定] の順に移動します。

イベント保存タイプは、デフォルトでは上書きです。保存されたイベントが容量の 95% を超えた場合、最も古い 5% のイベントが削除されます。

6.5.14 プロンプトスケジュール

認証が成功および失敗したとき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. 設定→ 設定→ プロンプトスケジュール をクリックします。

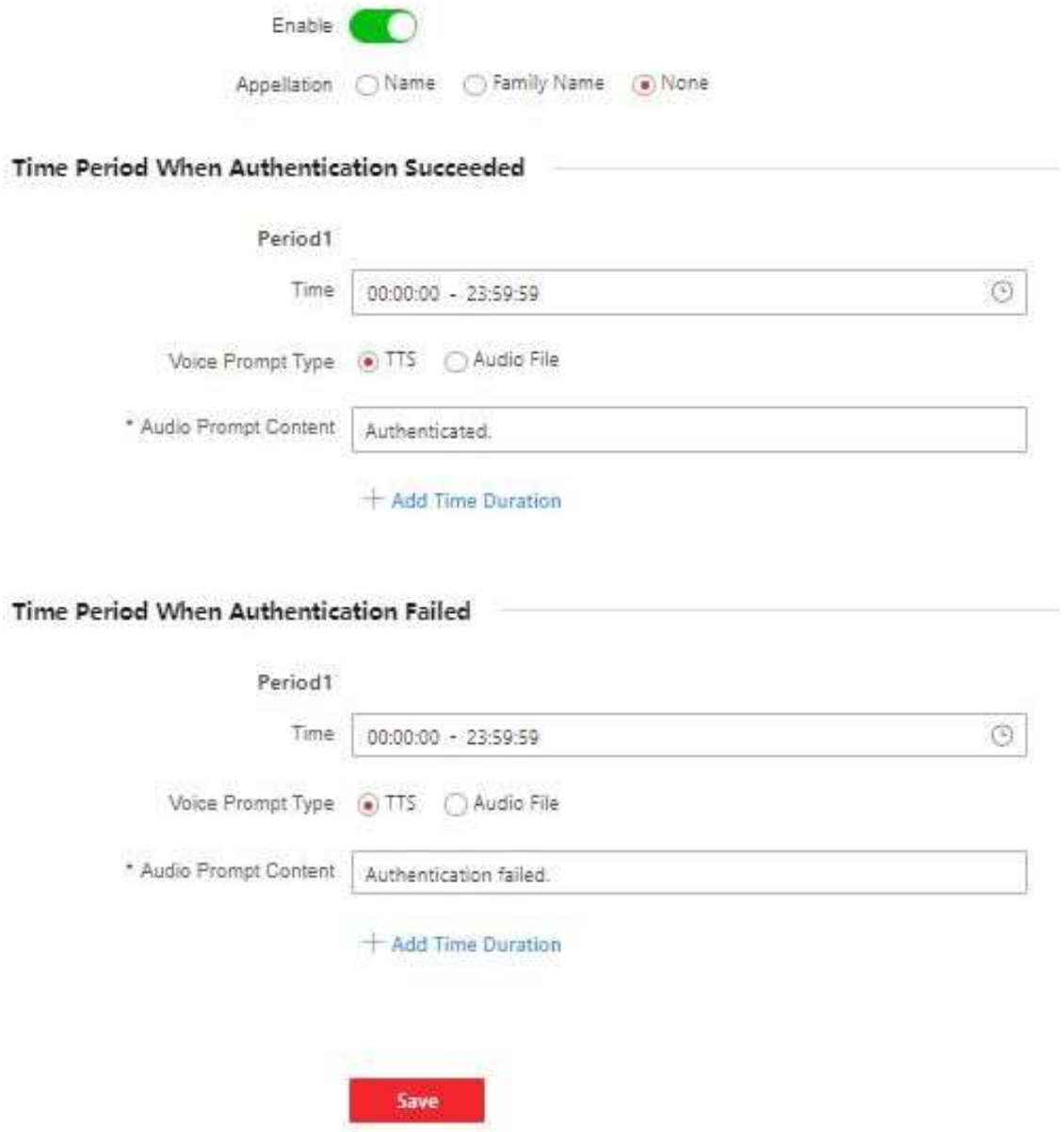


図 6-16 オーディオコンテンツのカスタマイズ

2. 時間スケジュールを選択してください。

3. 機能を有効にします。

4. 名称を設定します。

5. 認証が成功した時間帯を設定します。

1) **「時間期間を追加」**をクリックします。

2) 時間間隔を設定します。

注意

設定した時間範囲内で認証が成功した場合、デバイスは設定されたコンテンツをブロードキャストします。

3) オーディオコンテンツを設定します。

TTS

TTS を選択した場合は、言語を設定し、認証成功時のプロンプト内容を入力する必要があります。

オーディオファイル

オーディオファイルを選択した場合は、ドロップダウンリストから利用可能なオーディオファイルを選択するか、**[オーディオファイルの管理]** をクリックして新しいファイルを追加する必要があります。

注意

オーディオファイルの形式は wav、サイズは 200 KB 以内にしてください。

4) **オプション：** サブステップ 1 から 3 を繰り返します。

5) **オプション：** をクリックして、設定した時間制限を削除します。

6. 認証に失敗した際の時間設定を設定します。

1) **「Add」** をクリックします。

2) 時間設定を設定します。

注意

認証が設定された時間内に失敗した場合、デバイスは設定されたコンテンツをブロードキャストします。

3) オーディオコンテンツを設定します。

TTS

TTS を選択した場合は、言語を設定し、認証失敗時のプロンプト内容を入力する必要があります。

オーディオファイル

オーディオファイルを選択した場合は、ドロップダウンリストから利用可能なオーディオファイルを選択するか、**[オーディオファイル管理]** をクリックして新しいファイルを追加する必要があります。

注意

オーディオファイルの形式は wav で、サイズは 200 KB 以内にしてください。

4) **オプション：** サブステップ 1 から 3 を繰り返します。

5) **オプション：** [ ] をクリックして、設定した時間制限を削除します。

7. **「保存」** をクリックして設定を保存します。

6.5.15 アップグレードとメンテナンス

デバイスを再起動し、デバイスのパラメーターを復元し、デバイスのバージョンをアップグレードします。

デバイスの再起動

[メンテナンスとセキュリティ]、[→]、[→]、[Restart] の順にクリックします。
[Restart] をクリックして、デバイスを再起動します。

アップグレード

[メンテナンスとセキュリティ]、[→]、[→]、[Upgrade] の順にクリックします。
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。

注意
アップグレード中は電源を切らないでください。

パラメーターの復元

[メンテナンスとセキュリティ]、[→ のメンテナンス]、[→ のバックアップとリセット] の順にクリックします。

すべてを復元

すべての設定が工場出荷時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。

復元

ネットワークパラメータとユーザー情報を除き、デバイスはデフォルト設定に復元されます。

パラメーターのインポートとエクスポート

[メンテナンスとセキュリティ]、[→]、[メンテナンス]、[→]、[バックアップとリセット] の順にクリックします。

エクスポート

「エクスポート」をクリックして、デバイスのパラメーターをエクスポートします。

注意
エクスポートしたデバイス パラメーターを別のデバイスにインポートできます。

インポート

「」をクリックし、インポートするファイルを選択します。インポートを開始するには「**Import**」をクリックします。

6.5.16 デバイス デバッグ

デバイス デバッグ パラメーターを設定できます。

手順

1. **[メンテナンスとセキュリティ]、[→]、[→]、[Device Debugging]** の順にクリックします。
2. 以下のパラメーターを設定できます。

SSHを有効にする

ネットワークのセキュリティを強化するには、SSH サービスを無効にしてください。この設定は、専門家によるデバイスのデバッグにのみ使用されます。

ログの印刷

「**エクスポート**」をクリックしてログをエクスポートできます。

6.5.17 コンポーネントの状態

メインレーンとサブレーンの状態を確認できます。

メインレーンの状態

デバイスコンポーネント

アクセス制御ボード、レーン制御ボード、ユーザー拡張インターフェースボード、および通過モード表示ボードの状態を確認できます。

周辺

RS-485カードリーダーと不正操作入力のステータスを確認できます。

温度

ペデスタルの温度を確認できます。

動作

モーターエンコーダの動作状態を確認できます。

サブレーン状態

デバイスコンポーネント

レーン制御ボード、通過モード表示ボード、および上部赤外線アダプターの状態を確認できます。

周辺機器

RS-485カードリーダー、RS-232カード受信機、および不正操作入力の状態を確認できます。

動作

モーターエンコーダの動作状態を確認できます。

その他

通過モード

入口と出口のモードを確認できます。

赤外線検出器の状態

各赤外線ビームセンサーのペアの状態を確認できます。

入力と出力の状態

イベント入出力、アラーム入出力、火災報知器のステータスを確認できます。

その他の状態

バリアとキーフォブ受信モジュールの状態を確認できます。

6.5.18 ログ検索

デバイスのログを検索して表示できます。

[メンテナンスとセキュリティ]、[→]、[→]、[Log] の順に選択します。

ログタイプの主要タイプと副次タイプを設定します。検索の開始時間と終了時間を設定し、**検索**をクリックします。

結果には、No.、時間、メジャータイプ、マイナータイプ、チャンネル番号、ローカル/リモートユーザー情報、リモートホストIPなどが表示されます。

6.5.19 証明書管理

サーバー/クライアント証明書および CA 証明書を管理するのに役立ちます。

注意

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。

自己署名証明書を作成してインストールする

手順

1. **[メンテナンスとセキュリティ]、[→ セキュリティ]、[→ 証明書管理]** の順に選択します。
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して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指定したファイルに保存してください。
7. 要求ファイルを認証局に送信して署名を取得します。
8. 署名された証明書をインポートします。
   1) 「**パスワードのインポート**」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、[**インストール**] をクリックします。
   2) 「**通信証明書をインポート**」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、[**インストール**] をクリックします。

その他の承認済み証明書をインストール

既に承認済み証明書（デバイスで作成されていないもの）がある場合は、直接デバイスにインポートできます。

手順

1. **[メンテナンスとセキュリティ]**、**[→ セキュリティ]**、**[→ 証明書管理]** の順に移動します。
2. **「パスワードのインポート」**と**「通信証明書のインポート」**領域で、証明書タイプを選択し、証明書をアップロードします。
3. **インストールを**クリックします。

CA証明書をインストール

開始前に

事前にCA証明書を準備してください。

手順

1. **[メンテナンスとセキュリティ]**、**[→ セキュリティ]**、**[→ 証明書管理]** の順に移動します。
2. **「CA 証明書をインポート」**領域で ID を作成します。

   注意

   入力する証明書 ID は既存のものと同一にしてはいけません。
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. **インストールを**クリックします。

第7章 モバイルブラウザ経由でデバイスを設定する

7.1 ログイン

モバイルブラウザからログインできます。

注意
デバイスがアクティブ化されていることを確認してください。

以下の方法でごログインいただけます：

- デバイスのホットスポットが無効になっている場合は、携帯電話とデバイスが同じ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。携帯電話を NFC エリアに置くと、ログインページがポップアップ表示されます。デバイスのホットスポットが有効になっている場合は、携帯電話を NFC エリアに置くと、名前とパスワードが
- デバイスのホットスポットが有効になっている場合は、デバイスのホットスポットに接続すると、ログインページがポップアップ表示されます。

  デバイスのユーザー名とパスワードを入力し、**ログイン**をクリックしてください。
- デバイスのホットスポットが有効になっている場合、スマートフォンをNFCエリアに近づけると、デバイスのホットスポットの名前とパスワードが自動的に取得されます。

注意
NFC機能に対応したAndroidシステムが推奨されます。iOSシステムは対応していません。

7.2 概要

デバイスの状態を確認したり、リモート操作を行ったりできます。

デバイスの状態を確認できます。例外が発生した場合、タップしてコンポーネントの詳細を確認できます。アイコンをタップしてバリアをリモート制御できます。

図 7-1 ショートカット入力とネットワークステータス

タップすると、基本設定ページ、ユーザーページ、キーフォブページ、ライトページ、ネットワークページにすばやく移動できます。

7.3 設定

7.3.1 ターンスタイルの基本パラメーター

ターンスタイルの基本パラメーターを設定できます。

概要ページにあるショートカットエントリの「**基本設定**」をタップします。

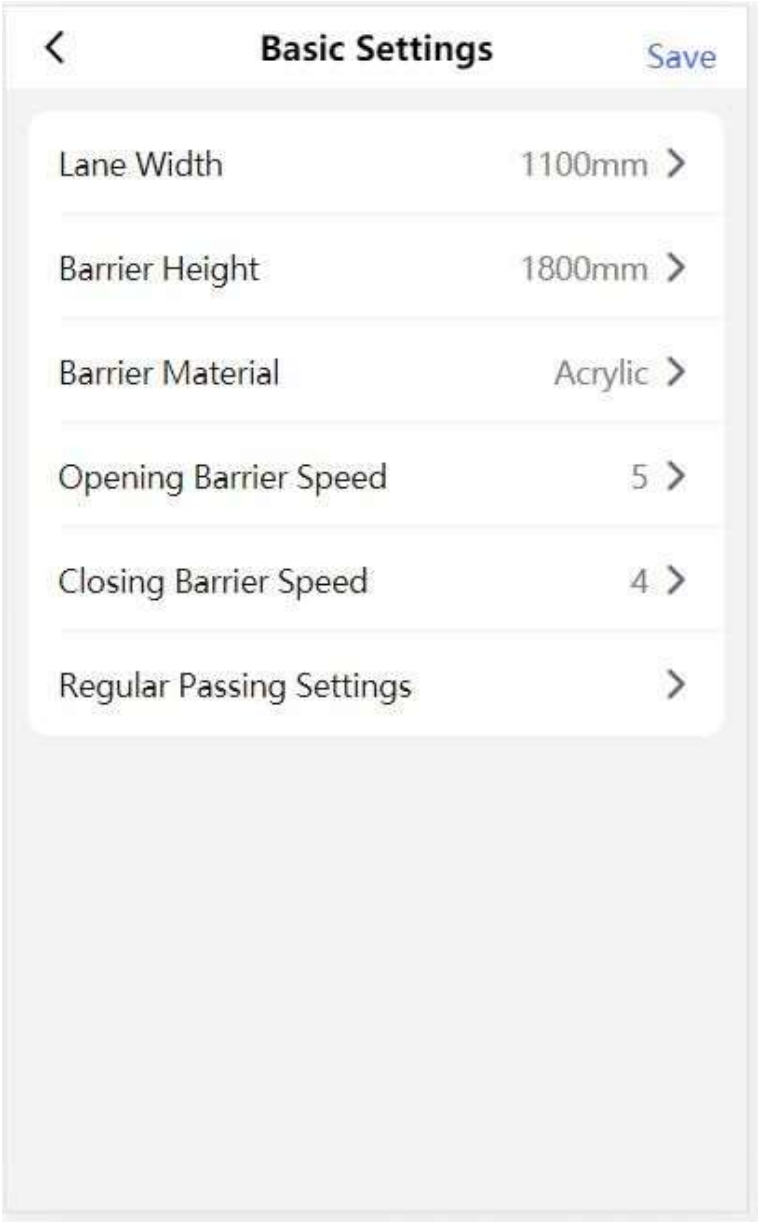


図7-2 ターンスタイルの基本パラメーター

レーン幅、**バリア高さ**、**バリア高さ**、**バリア開閉速度**を設定します。入口と出口の通常の通過モードを設定します。

保存をタップします。

7.3.2 ユーザー管理

モバイルウェブブラウザーから、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. **ユーザー**をタップして設定画面に入ります。

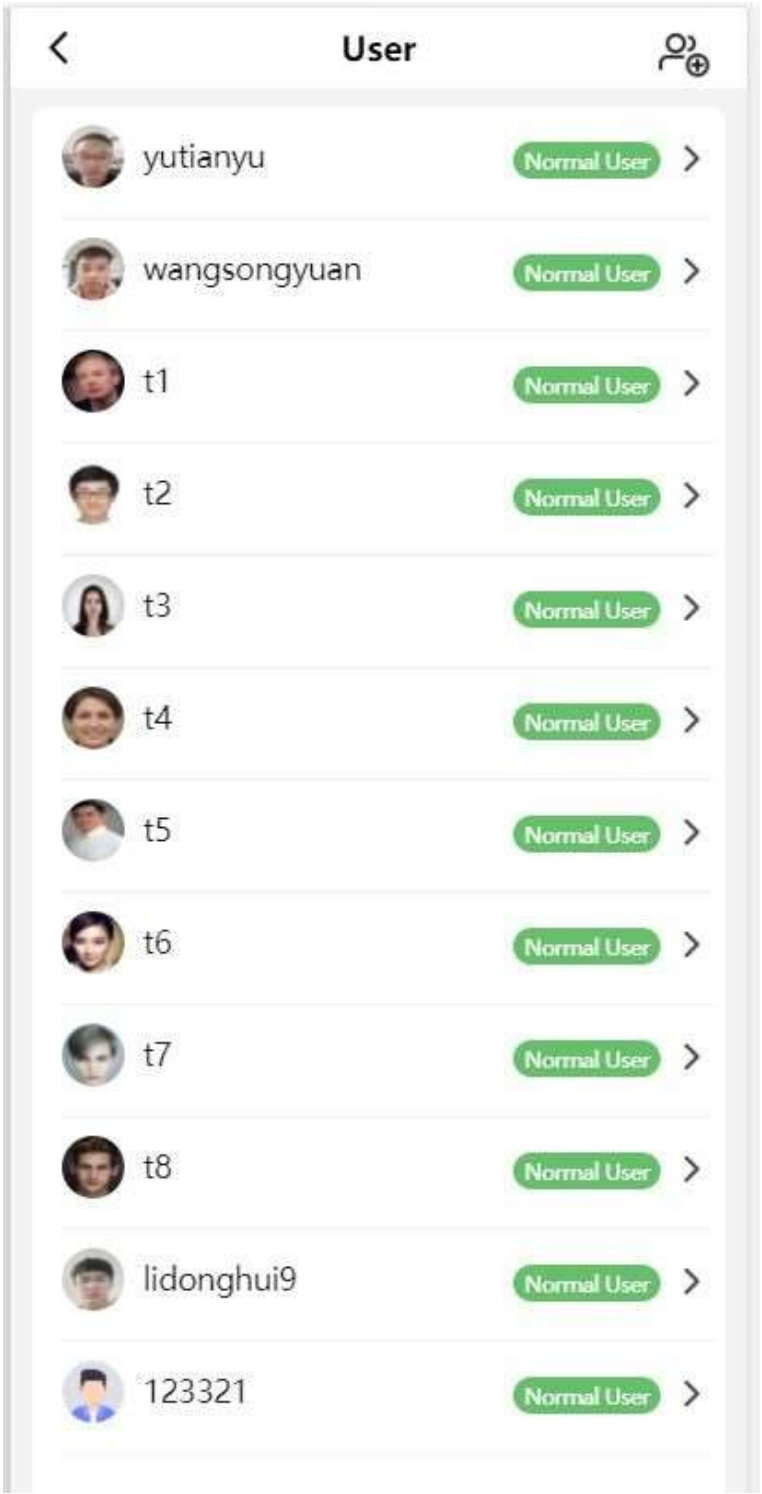


図7-3 ユーザーを追加

2. ユーザーを
追加します。
1) 「」をタップします。
2) 以下のパラメーターを設定します。

従業員ID

従業員IDを入力してください。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、小文字のアルファベットと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、大文字と小文字の英字、および文字が含まれます。名前は32文字以内を推奨します。

ユーザーロール

ユーザー役割を選択してください。

カード

カードを追加します。**カード→ カードを追加** をタップし、カード番号を入力して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. ユーザーリストから編集が必要なユーザーをタップして情報を編集します。

7.3.3 キーフォブ設定

概要画面のショートカットエントリにある**キーフォブ**をタップします。

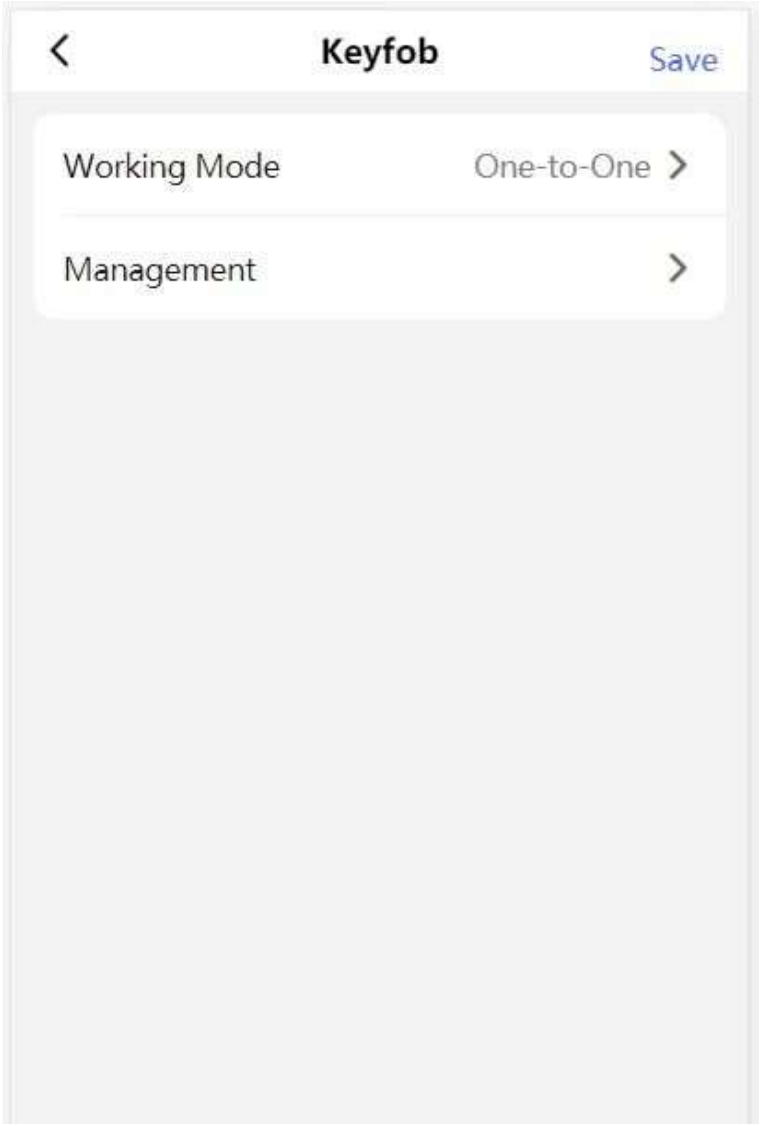


図7-4 キーフォブ設定

動作モードを「1対1」または**「1対多」**に設定します。

「管理」をタップして、ページに入ります。**「+」**をタップして、キーフォブを追加します。キーフォブ名、シリアル番号、および開いたままにする許可を設定します。

7.3.4 ライト設定

概要画面のショートカット項目にある**「ライト」**をタップします。

レーン状態インジケーター

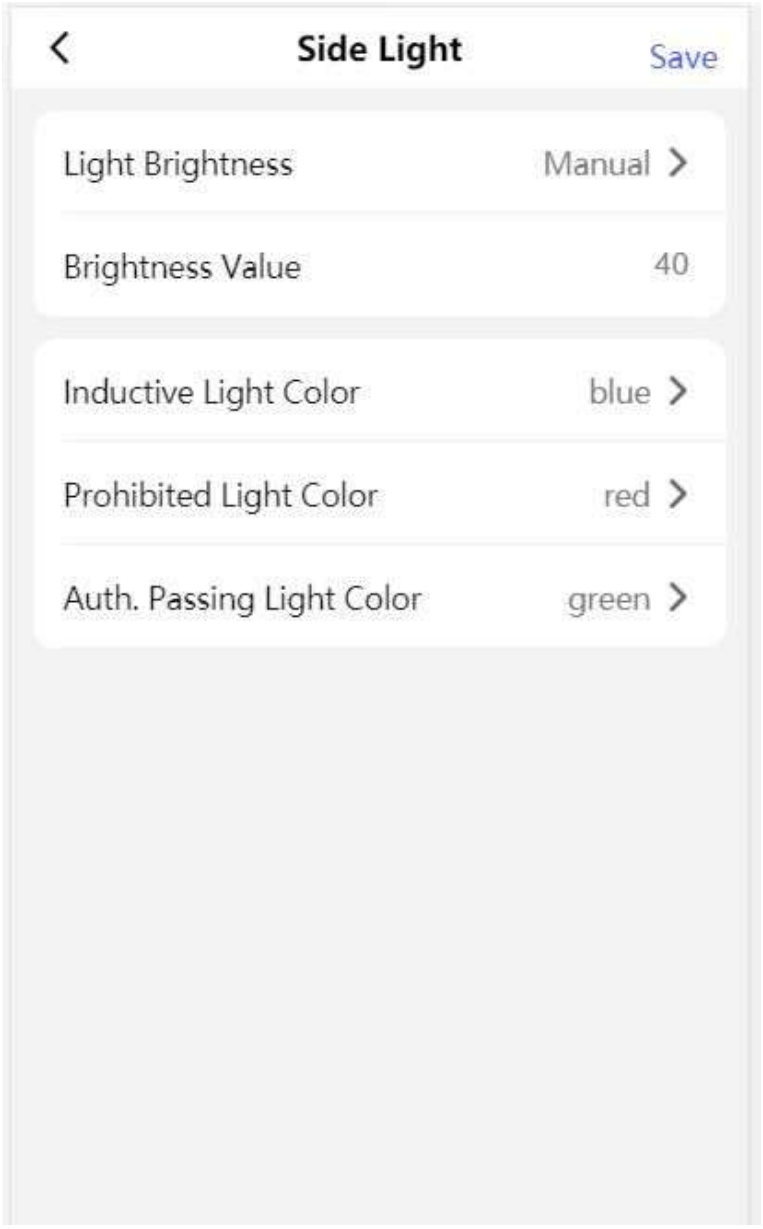


図7-5 レーン状態インジケーター設定

ライトの明るさは、デフォルトでは**手動**に設定されています。ライトの明るさを手動で調整するには、値を入力してください。誘導/開状態、閉状態、制御/バリアフリーモードごとにライトの色を設定します。

バリアライト

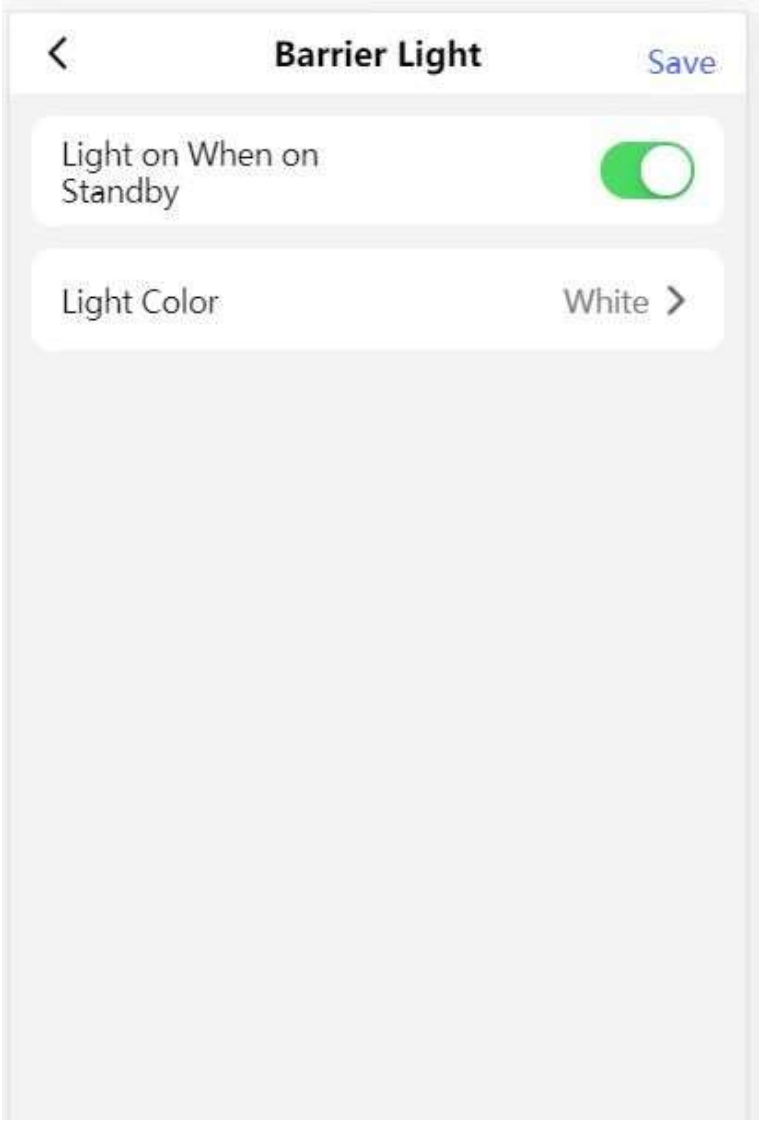


図7-6 バリアライト設定

必要に応じて、**[待機時にライトをオンにする]** をタップして有効にし、バリアライトの色を設定します。

7.3.5 ネットワーク設定

有線ネットワーク、デバイスのホットスポット、および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。

設定、→通信設定、→有線ネットワークの順にタップして、設定ページに入ります。

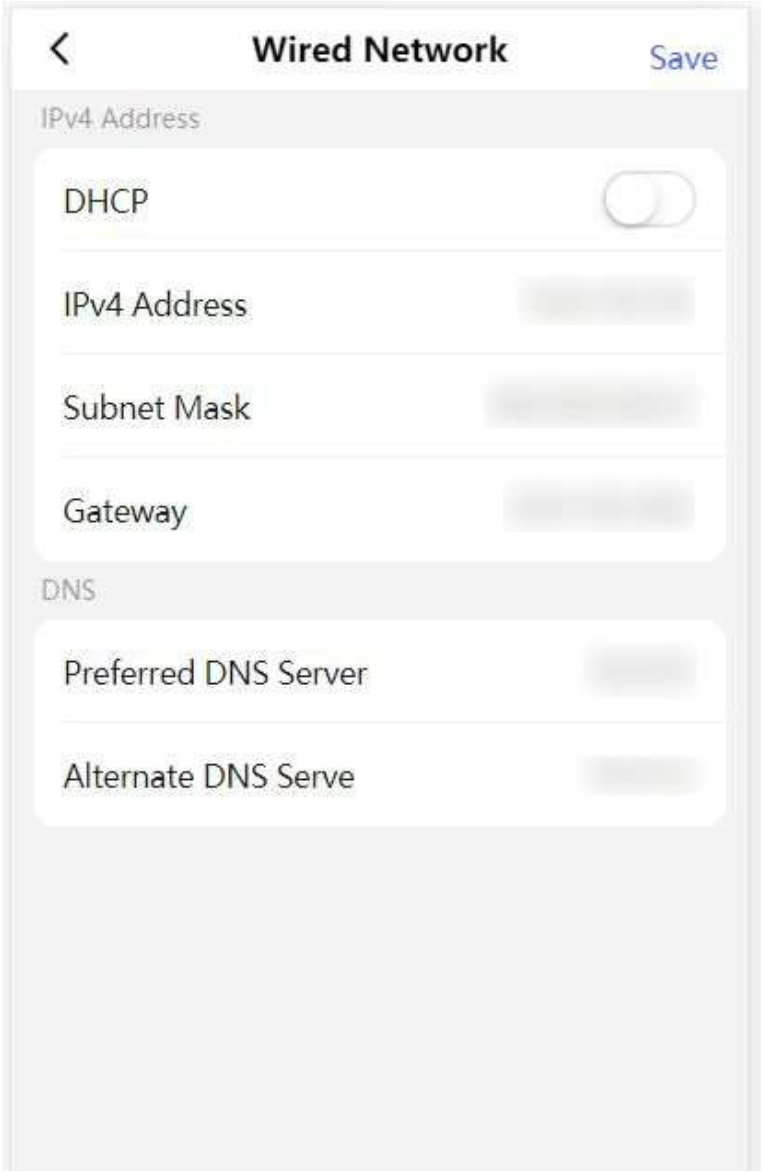


図 7-7 有線ネットワーク

DHCP

この機能を無効にした場合、IPv4アドレス、IPv4サブネットマスク、およびIPv4デフォルトゲートウェイを設定する必要があります。

この機能を有効にした場合、システムが自動的にIPv4アドレス、IPv4サブネットマスク、およびIPv4デフォルトゲートウェイを割り当てます。

DNSサーバー

実際の必要に応じて、優先DNSサーバーと代替DNSサーバーを設定してください。

デバイス ホットスポット

デバイス ホットスポットを設定します。

設定をタップし、**→通信設定→デバイス ホットスポット**を選択して設定画面に移動します。

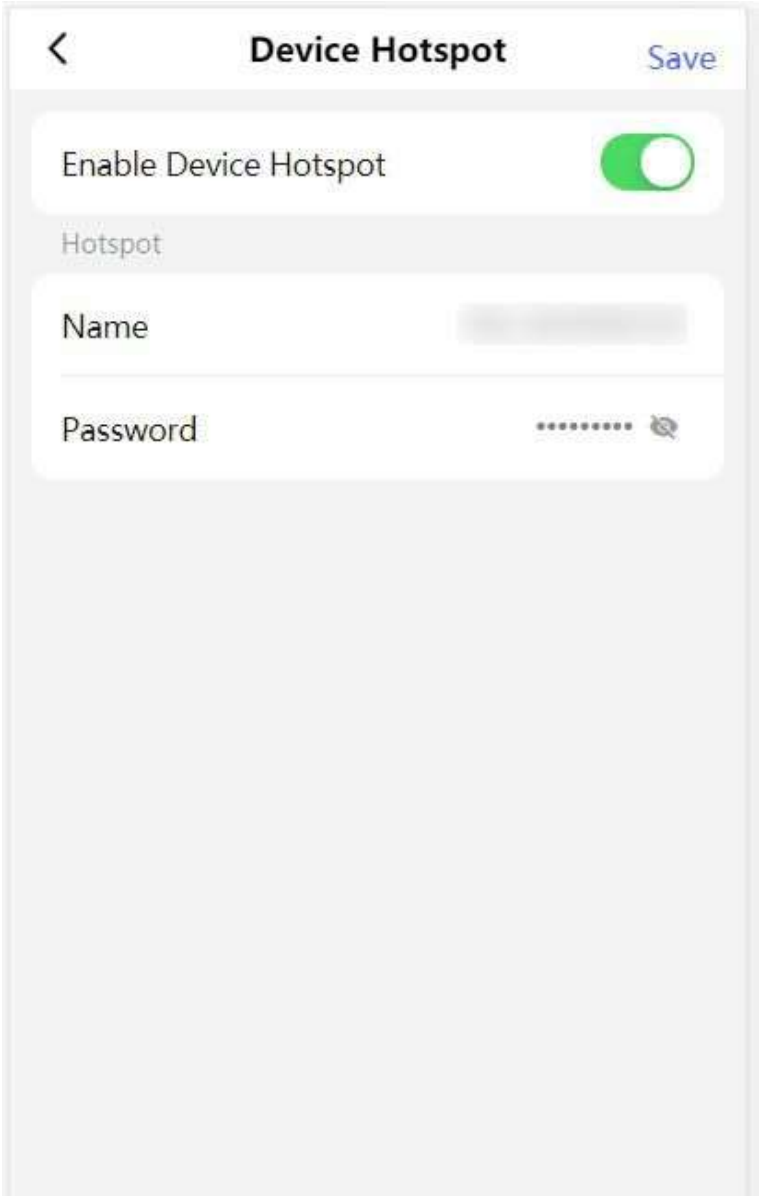


図7-8 デバイス ホットスポット

デバイス ホットスポットを有効にするには、タップしてください。ホットスポットの**名前**と**パスワード**を設定します。**保存**をクリックします。

シリアルポートの設定

シリアルポートを設定します。

設定をタップし、→**通信設定**、→**シリアルポート設定**を選択して設定画面に移動します。

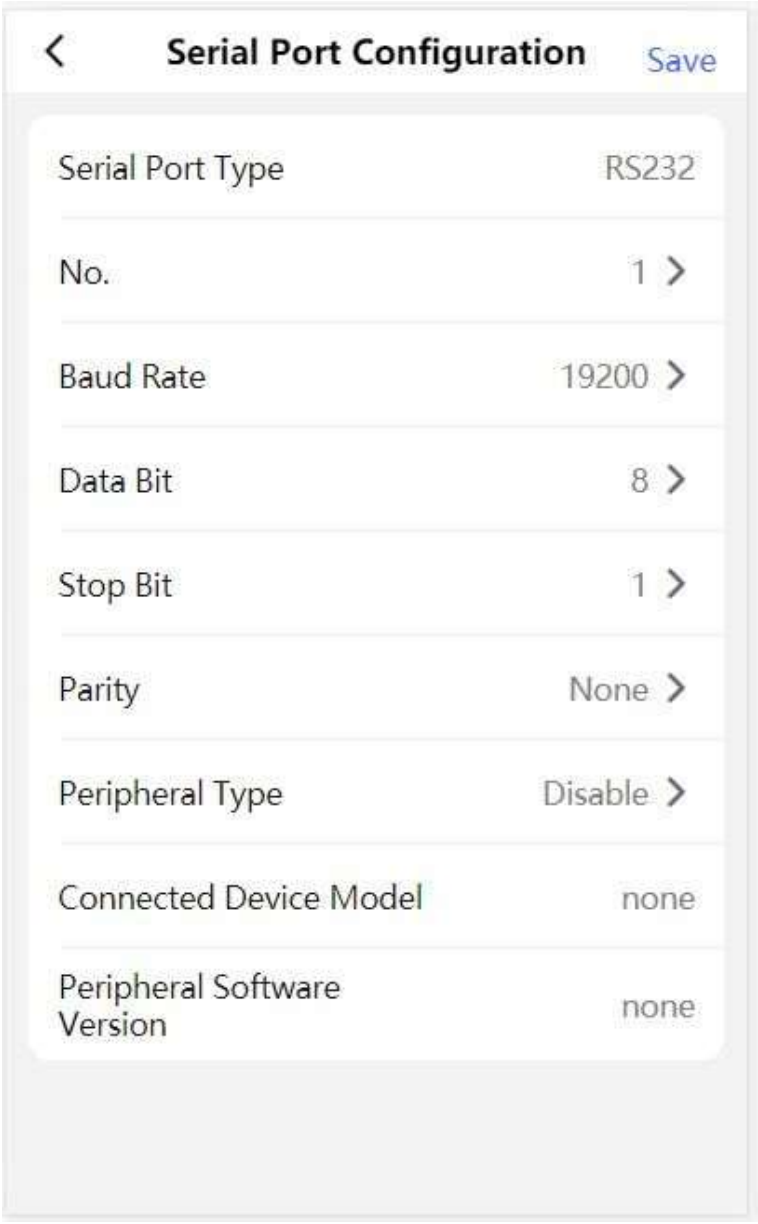


図7-9 シリアルポート設定

ポート**番号**を選択し、**ボーレート**、**データビット**、**ストップビット**、**パリティ**を設定します。
周辺機器の種類を**カードリーダー**、**カード受信機**、**QRコードスキャナー**、または**無効に設定**します。**保存**をタップします。

7.3.6 デバイス基本設定

オーディオ、時間、スリープ時間、プライバシーを設定します。

設定をタップし、→**の基本設定**を選択して設定画面に入ります。

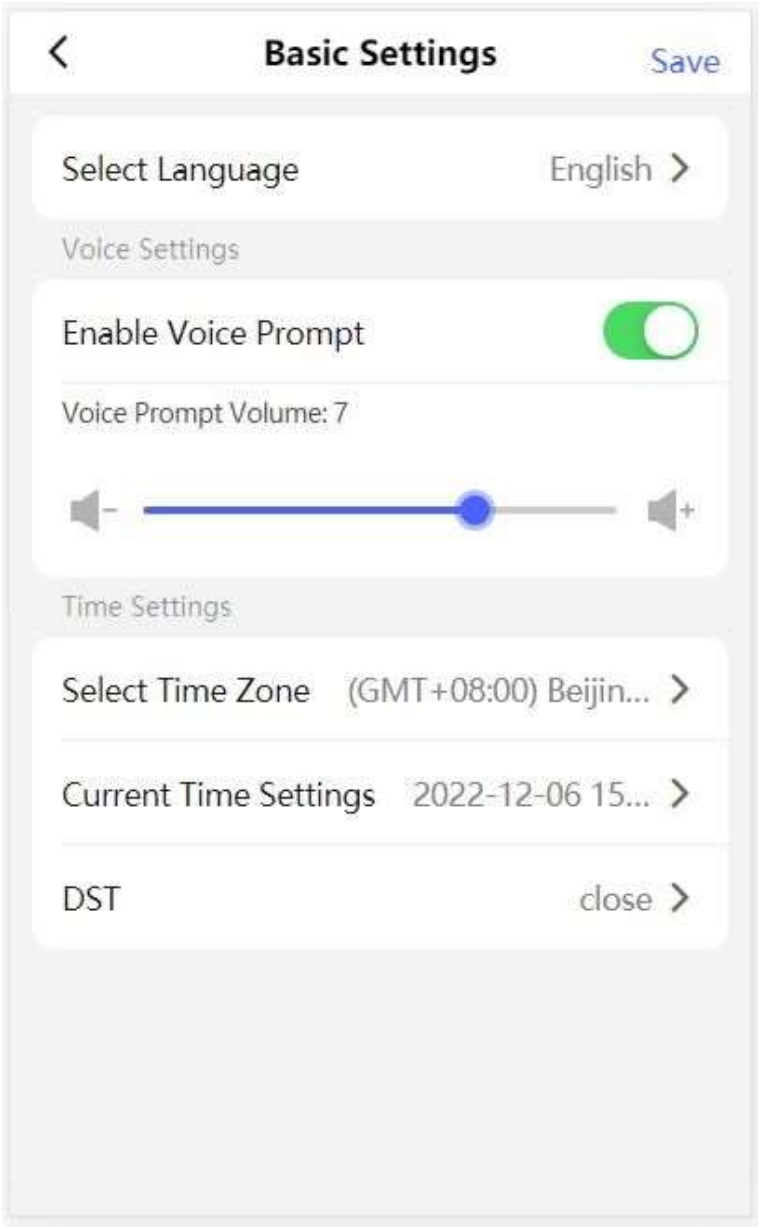


図7-10 基本設定

言語

言語は、デフォルトで英語に設定されています。

音声設定

音声プロンプトを有効にするにはタップし、音声プロンプトを設定する入口または出口を選択し、ドラッグして音量を設定します。

時間設定

タップしてタイムゾーンとデバイスの時間を設定します。

DST をタップして、DST 設定画面に移動します。DST を有効にし、DST の開始時間、終了時間、およびバイアス時間を設定します

7.3.7 アクセス制御設定

ドアパラメーターを設定します

設定をタップし、**→アクセス制御→ドアパラメーターを選択します**。

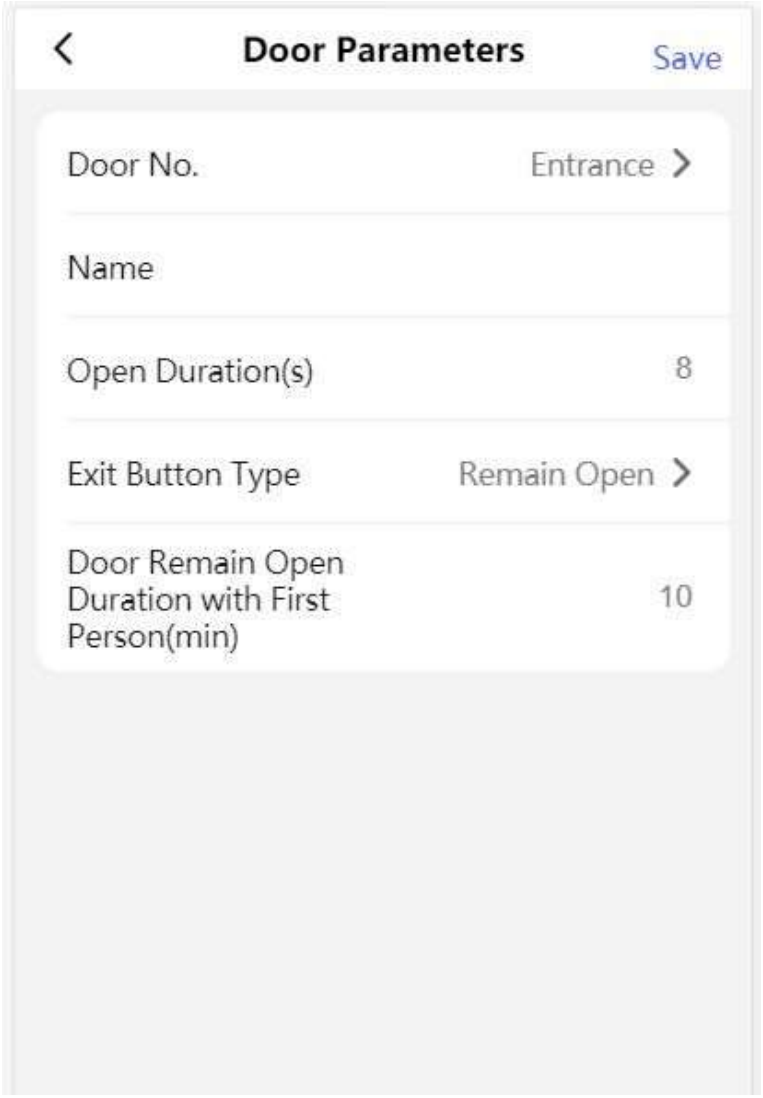


図7-11 ドアパラメーター設定画面

設定を保存するには、設定後**「保存」**をクリックします。

ドア番号

対応するドア番号のデバイスを選択します。

名前

ドアの名前を指定できます。

開錠時間

ドアの解錠時間を設定します。設定した時間内にドアが開かれない場合、ドアがロックされます。

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。デフォルトでは**「開いたまま」**です。

最初の人が入った際のドアの開いたままの持続時間

最初の人が入室した際のドアの開錠時間を設定します。最初の人が認証されると、複数の人物がドアにアクセスしたり、他の認証アクションを実行したりできるようになります。

認証パラメーターを設定します

認証パラメーターを設定します。

手順

1. **設定**をタップ**→ アクセス制御→ 認証設定** .

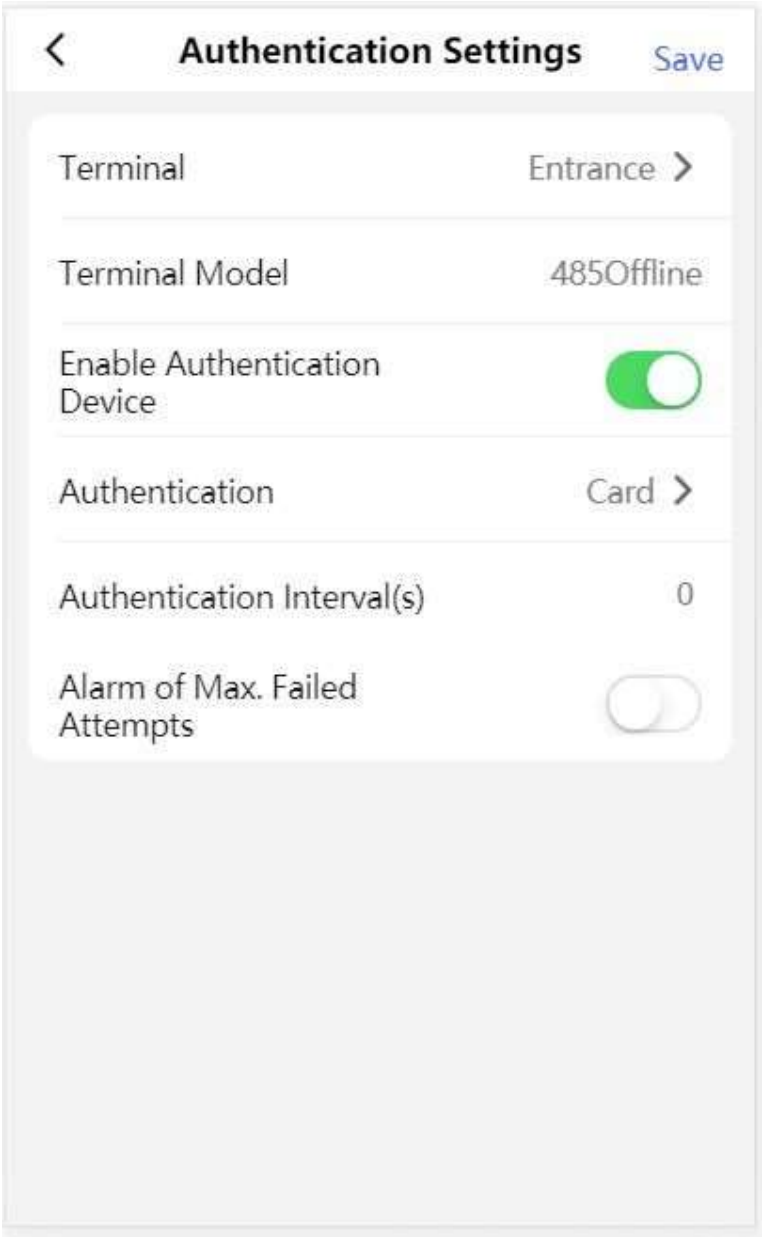


図7-12 認証設定

2. タップして **保存**。**ターミナル**

設定対象として「**入口**」または「**出口**」を選択します。

ターミナルモデル

ターミナルモデル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

デフォルトでカードによる認証を使用します。

認証間隔

同じユーザーが認証を行う際の認証間隔を設定できます。同じユーザーは設定された間隔内に1回のみ認証可能です。2回目の認証は失敗します。

最大失敗回数アラーム

カード読み取りの試行回数が設定値に達した場合にアラームを通知します。

カードのセキュリティ設定

[設定**]**、**[→]**、**[アクセス制御]**、**[→]**、**[カードセキュリティ]** の順にタップして、設定ページを表示します。

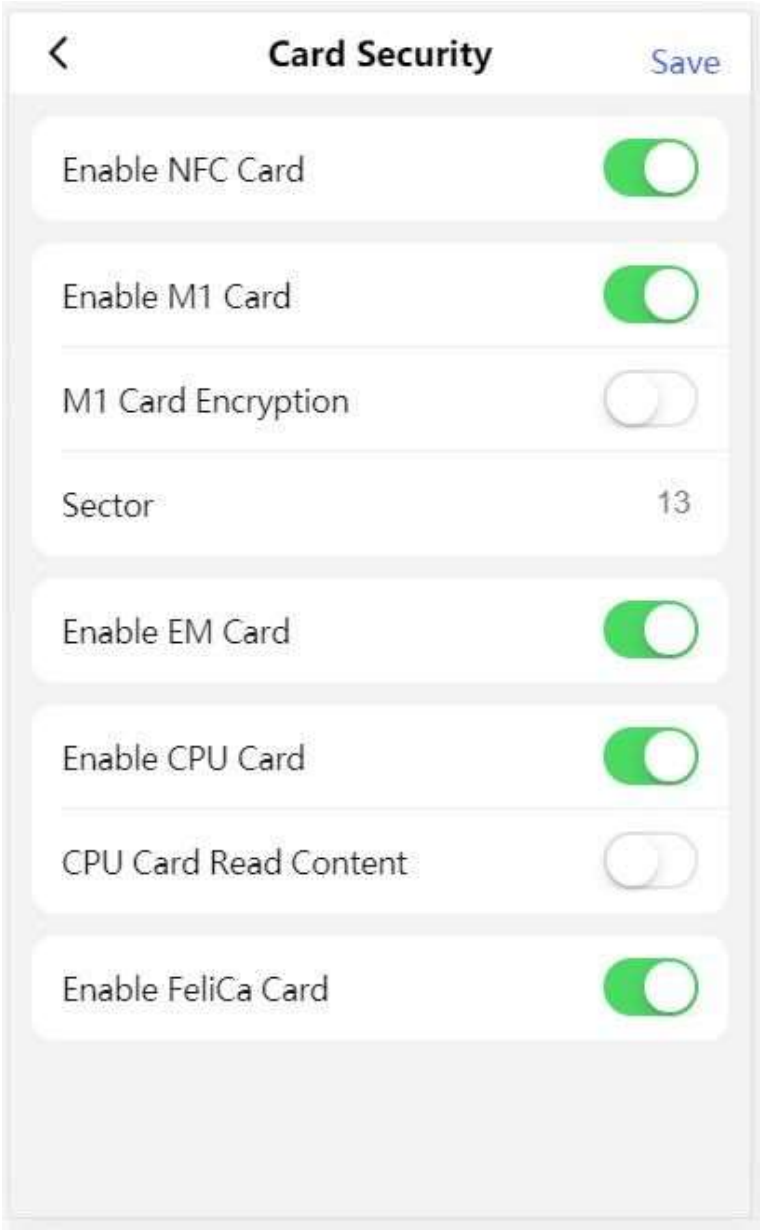


図 7-13 カードセキュリティ

パラメーターを設定し、**[保存]** をクリックします。

NFC カード有効化

携帯電話がアクセス制御のデータを取得できないように、NFC カードを無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 カード有効化

M1 カードを有効にすると、M1 カードを提示して認証が可能になります。

M1カード暗号化

M1 カードの暗号化により、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

機能を有効にし、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が暗号化されています。セクター13の暗号化を推奨します。

EMカード機能を有効にします

EMカードを有効化し、EMカードを提示して認証を行う機能が利用可能になります。

注意

周辺機器のカードリーダーがEMカードの提示に対応している場合、EMカード機能の有効/無効設定機能も利用可能です。

CPUカード機能を有効にする

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

CPUカードの内容を読み取り

CPUカードの内容読み取り機能を有効にすると、デバイスはCPUカードの内容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。

ターミナル設定

動作モードを設定します。

設定をタップし、**→、アクセス制御、→、Terminal** Parametersの順に選択して設定画面に入ります。

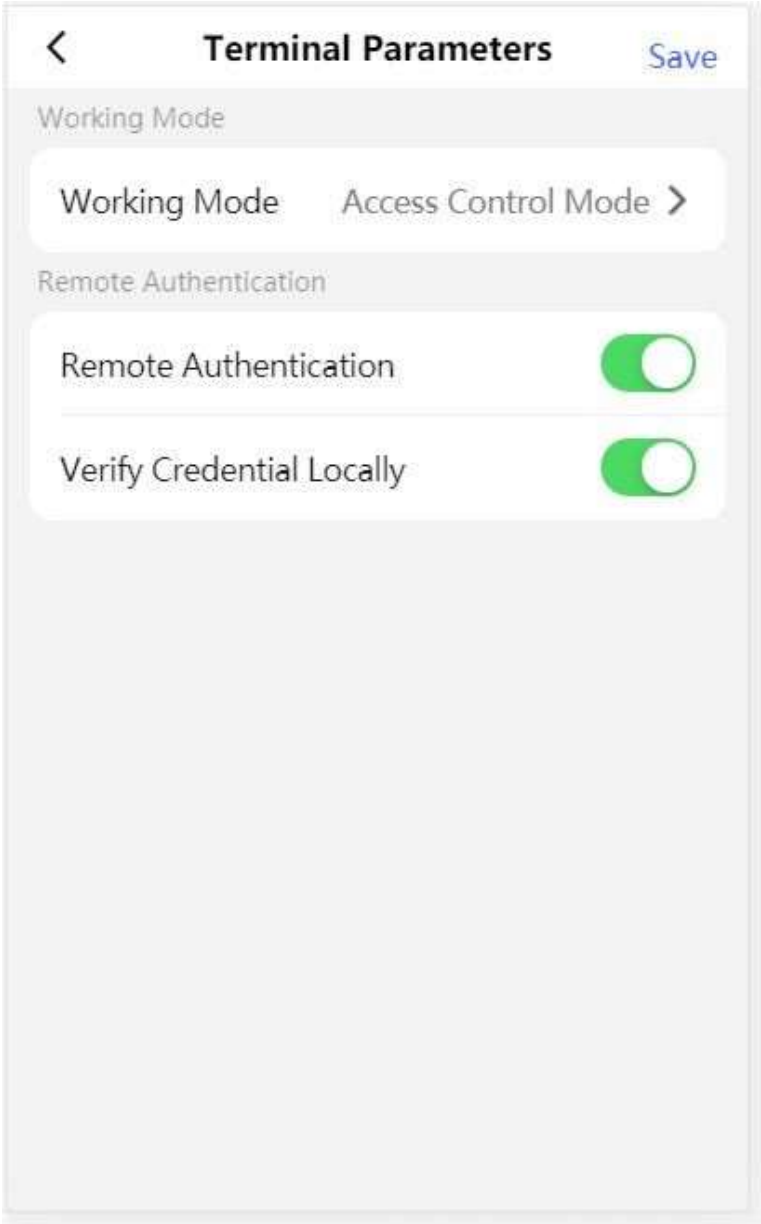


図7-14 端末パラメーター

許可フリーモード

デバイスはユーザーの許可を確認せず、ユーザーの有効期間のみを確認します。ユーザーが有効期間内にある場合、バリアが開きます。

「ローカルで資格情報を確認する」を有効にできます。この機能を有効にすると、デバイスはスケジュールテンプレートなどなしで、ユーザーの権限のみを確認します。

アクセス制御モード

デバイスは通常通り動作し、バリアを開くためのユーザーの権限を確認します。

リモート認証

デバイスは、ユーザーの認証情報をプラットフォームに送信します。プラットフォームがバリアを開くかどうかを判断します。

ローカルでの認証情報の確認

デバイスは、スケジュールテンプレートなどなしで、人物のアクセス権限のみを検証します。

7.3.8 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、バージョンなどを表示します。

設定→システム情報を選択して設定画面を開きます。

言語、モデル、シリアル番号、バージョン、IO 入力および出力番号、ローカル RS-485 番号、MAC アドレス、オープンソースライセンスを確認できます。

デバイス名を変更できます。**保存**をタップします。

7.3.9 デバイス容量

設定→ デバイスの容量をタップして、ページに入ります。ユーザー、カード、イベントの数量を確認できます。

7.3.10 ログエクスポート

設定→ ログエクスポートをタップしてページに移動します。ログの種類を選択し、**エクスポートを**タップします。

7.3.11 復元と再起動

デバイスを再起動し、デバイスのパラメーターを復元します。

復元

設定をタップし、**→復元** を選択します。

すべての設定が工場出荷時設定に復元されます。

デバイスを再起動します

設定をタップし、**→デバイスを再起動を選択します**。**再起動**をタップしてデバイスを再起動します。

第 8 章 クライアントソフトウェアの設定

ホットラインに電話して、iVMS-4200 クライアントソフトウェアのインストールパッケージを入手してください。

8.1 クライアントソフトウェアの設定フロー

以下のフロー図に従って、クライアントソフトウェアの設定を行ってください。

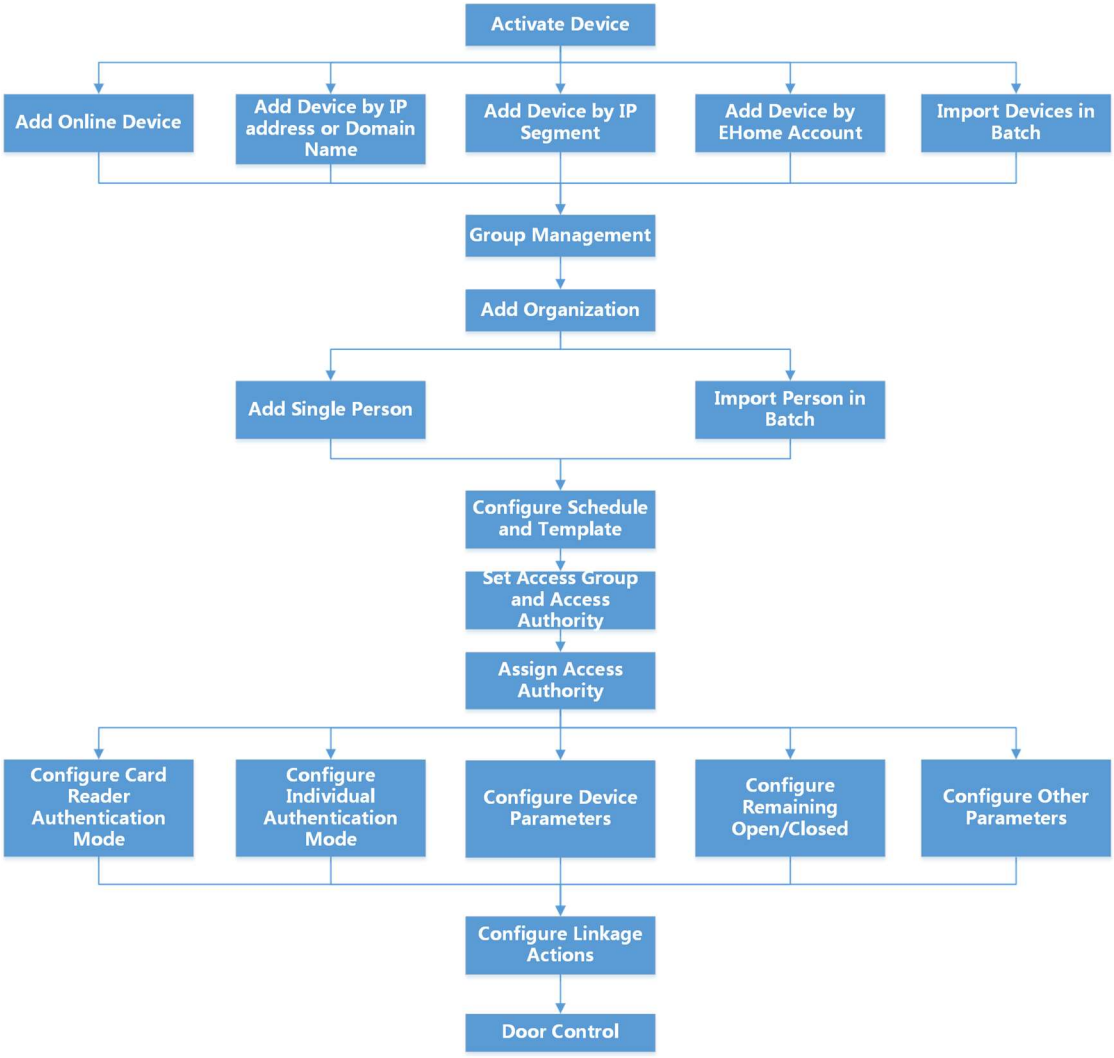


図 8-1 クライアントソフトウェアの設定フロー図

8.2 デバイス管理

クライアントは、アクセス制御デバイスおよびビデオインターコムデバイスの管理をサポートしています。

例
クライアントにアクセス制御デバイスを追加すると、入退室を制御し、出席を管理することができます。また、屋内ステーションやドアステーションとビデオインターホンを行うことができます。

8.2.1 デバイスを追加

クライアントには、IP/ドメイン、IP セグメント、ISUP プロトコルによる 3 つのデバイス追加モードがあります。
また、追加するデバイスが大量にある場合は、複数のデバイスをバッチでインポートすることもできます。

IPアドレスまたはドメイン名によるデバイスの追加

追加するデバイスの IP アドレスまたはドメイン名がわかっている場合は、IP アドレス（またはドメイン名）、ユーザー名、パスワードなどを指定して、クライアントにデバイスを追加することができます。

手順

1. デバイス管理モジュールを開きます。

2. 右パネルの上部にある**「デバイス」**タブをクリックします。

追加されたデバイスは右側のパネルに表示されます。

3. **「追加」**をクリックして「追加」ウィンドウを開き、追加モードとして**「IP/ドメイン」**を選択します。

4. 必要な情報を入力します。

名前

デバイスにわかりやすい名前を付けます。たとえば、デバイスの位置や機能を示すニックネームを使用することができます。

アドレス

デバイスのIPアドレスまたはドメイン名。

ポート

追加するデバイスは同じポート番号を共有します。デフォルト値は***8000***です。

注意
一部のデバイスタイプでは、ポート番号として ***80*** を入力することができます。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。

ユーザー名

デバイスのユーザー名を入力します。デフォルトのユーザー名は***admin です***。

パスワード

デバイスのパスワードを入力してください。

注意

デバイスのパスワードの強度については、自動的に確認することができます。製品のセキュリティを強化するため、お客様ご自身でパスワードを変更することを強くお勧めします（8 文字以上で、大文字、小文字、数字、特殊文字の 3 種類以上を含む）。また、セキュリティ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。パスワードを毎月または毎週変更することで、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設定は、設置者および/またはエンドユーザーの責任となります。

5. **オプション：** セキュリティのために、TLS（Transport Layer Security）プロトコルを使用した送信の暗号化を有効にするには、**[送信の暗号化 (TLS)]** をチェックします。

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。
- 証明書検証を有効にしている場合は、**[証明書ディレクトリを開く]** をクリックしてデフォルトのフォルダを開き、デバイスからエクスポートした証明書ファイルをこのデフォルトのディレクトリにコピーして、セキュリティを強化してください。証明書検証の有効化の詳細については、を参照してください。
- ウェブブラウザーでデバイスにログインして、証明書ファイルを取得することができます。

6. デバイスをクライアントに追加した後、**[時刻の同期]** をチェックして、デバイスの時刻をクライアントを実行している PC の時刻と同期させます。
7. **オプション：[グループにインポート]** をチェックすると、デバイス名によるグループが作成され、そのデバイスに属するすべてのチャンネルがグループにインポートされます。

例

アクセス制御デバイスでは、そのアクセスポイント、アラーム入力/出力、およびエンコーディングチャンネル（存在する場合）がこのグループにインポートされます。

8. デバイスの追加を完了します。
   - **「追加」** をクリックしてデバイスを追加し、デバイス一覧ページに戻ります。
   - **「追加」と「新規」** をクリックして設定を保存し、他のデバイスを追加し続けます。

デバイスをバッチでインポート

あらかじめ定義した CSV ファイルにデバイスのパラメータを入力することで、クライアントに複数のデバイスをまとめて追加することができます。

手順

1. デバイス管理モジュールを開きます。
2. 右パネルの上部にある **「デバイス」** タブをクリックします。
3. **「追加」** をクリックして「追加」ウィンドウを開き、追加モードとして **「一括インポート」** を選択します。
4. **「テンプレートをエクスポート」** をクリックし、事前に定義されたテンプレート（CSVファイル）をPCに保存します。

5. エクスポートしたテンプレートファイルを開き、追加するデバイスの必要な情報を対応する列に入力します。

注意
フィールドの詳細については、テンプレートの説明を参照してください。

追加モード

0、***1***、または***2***を入力してください。

アドレス

デバイスの住所を編集してください。

ポート

デバイスのポート番号を入力してください。デフォルトのポート番号は***8000***です。

ユーザー名

デバイスユーザー名を入力してください。デフォルトのユーザー名は ***「admin」*** です。

パスワード

デバイスのパスワードを入力してください。

注意
デバイスのパスワードの強度については、自動的に確認することができます。製品のセキュリティを強化するため、お客様ご自身でパスワードを変更することを強くお勧めします（8 文字以上で、大文字、小文字、数字、特殊文字の 3 種類以上を含む）。また、セキュリティ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。パスワードを毎月または毎週変更することで、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設定は、設置者および/またはエンドユーザーの責任となります。

グループへのインポート

1を入力して、デバイス名でグループを作成します。デバイスのすべてのチャンネルは、デフォルトで対応するグループにインポートされます。***0***を入力してこの機能を無効にします。

6. 「…」をクリックし、テンプレートファイルを選択します。

7. **「追加」**をクリックしてデバイスをインポートします。

8.2.2 デバイスパスワードのリセット

検出されたオンラインデバイスのパスワードを忘れた場合は、クライアントからデバイスのパスワードをリセットすることができます。

手順

1. デバイス管理ページに移動します。

2. **「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。

同じサブネットを共有するすべてのオンラインデバイスがリストに表示されます。

3. リストからデバイスを選択し、操作列の「」をクリックします。

4. デバイスのパスワードをリセットします。

- 「**生成**」をクリックして QR コードウィンドウをポップアップ表示し、「**ダウンロード**」をクリックして QR コードを PC に保存します。QR コードの写真を撮影して携帯電話に保存することもできます。その写真を当社のテクニカルサポートまでお送りください。

注意

パスワードのリセットに関する以下の操作については、当社の技術サポートまでご連絡ください。

注意

デバイスのパスワードの強度は自動的にチェックすることができます。製品のセキュリティを強化するため、お客様ご自身でパスワードを変更することを強くお勧めします（8 文字以上、大文字、小文字、数字、特殊文字の 3 種類以上を含む）。また、セキュリティ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。パスワードを毎月または毎週変更することで、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設定は、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。

8.2.3 追加されたデバイスの管理

デバイスをデバイス一覧に追加した後、追加したデバイスを管理できます。これには、デバイスのパラメーター編集、リモート設定、デバイス状態の確認などが含まれます。

表8-1 追加したデバイスの管理

デバイス編集	「」をクリックして、デバイス名、アドレス、ユーザー名、パスワードなど、デバイスの情報を編集します。
デバイスを削除	1つまたは複数のデバイスを選択し、**[削除]** をクリックして選択したデバイスを削除します。
リモート設定	をクリックして、対応するデバイスのリモート設定を設定します。詳細については、デバイスのユーザーマニュアルを参照してください。
デバイス状態の表示	をクリックすると、ドア番号、ドアの状態など、デバイスのステータスを表示できます。 **注意** 異なるデバイスでは、デバイスの状態に関する異なる情報が表示されます。

オンラインユーザーを表示	「 」をクリックすると、デバイスにアクセスしているオンラインユーザーの詳細（ユーザー名、ユーザータイプ、IPアドレス、ログイン時間など）を確認できます。
デバイス情報の更新	をクリックして、最新のデバイス情報を更新します。

8.3 グループ管理

クライアントは、追加したリソースをさまざまなグループで管理するためのグループ機能を提供しています。リソースの場所に応じて、リソースをさまざまなグループにグループ化することができます。

例
たとえば、1階には16個のドア、64個のアラーム入力、16個のアラーム出力が設置されています。これらのリソースを1つのグループ（1階）にまとめて管理すると、管理が便利になります。リソースをグループで管理した後、ドアの状態の制御や、デバイスのその他の操作を行うことができます。

8.3.1 グループを追加

追加したデバイスを整理して管理しやすくするために、グループを追加できます。

手順

1. デバイス管理モジュールに入ります。

2. **「デバイス管理」→「→」→「グループ」**をクリックして、グループ管理ページに移動します。

3. グループを作成します。

- **「グループを追加」**をクリックし、任意のグループ名を入力してください。
- **「デバイス名でグループを作成」**をクリックし、追加したデバイスを選択して、選択したデバイスの名前で新しいグループを作成します。

注意
このデバイスのリソース（アラーム入力/出力、アクセスポイントなど）は、デフォルトでグループにインポートされます。

8.3.2 グループにリソースをインポート

デバイスリソース（アラーム入力/出力、アクセスポイントなど）を、追加したグループに一括でインポートすることができます。

開始前に
デバイスを管理するためのグループを追加します。***グループを追加する***を参照してください。

手順

1. デバイス管理モジュールを開きます。

2. **「デバイス管理」→「→グループ」**をクリックして、グループ管理ページに移動します。
3. グループリストからグループを選択し、リソースタイプを「**アクセスポイント**」、**「アラーム入力**」、「**アラーム出力**」などから選択します。
4. **「インポート」**をクリックします。
5. サムネイル/リスト表示でリソースのサムネイル/名前を選択します。

注意

クリックできます または をクリックして、リソースの表示モードをサムネイル表示またはリスト表示に切り替えることができます。

6. **「インポート」**をクリックして、選択したリソースをグループにインポートします。

8.4 人員管理

アクセス制御、ビデオインターホン、勤怠管理などのさらなる操作のために、システムに人物情報を追加することができます。追加した人物に対して、カードの発行、人物情報の一括インポートおよびエクスポートなどの管理を行うことができます。

8.4.1 組織の追加

組織を追加し、その組織に人物情報をインポートすることで、人物の効率的な管理が可能です。追加した組織に上位組織を追加することもできます。

手順

1. **「人物」**モジュールを開きます。
2. 左側の列から親組織を選択し、左上隅の**「追加」**をクリックして組織を追加します。
3. 追加した組織の名前を入力してください。

注

最大 10 レベルの組織を追加できます。

4. **オプション：**以下の操作を実行します。

組織の編集	追加した組織にマウスを合わせ、[ ] をクリックして名前を編集します。
組織の削除	た組織にマウスを合わせ、 をクリックして削除します。 **注意** • 組織を削除すると、その下位の組織も削除されます。 • 組織の下に人が追加されていないことを確認してください。追加されている場合、組織は削除できません。
サブ組織内のユーザーを表示	**「サブ組織内のユーザーを表示**」にチェックを入れ、サブ組織内のユーザーを表示する組織を選択してください。

8.4.2 人物の識別情報のインポートとエクスポート

複数の人の情報や写真をクライアントソフトウェアに一括でインポートすることができます。また、人の情報や写真をエクスポートして、PC に保存することもできます。

人物情報のインポート

あらかじめ用意されたテンプレート（CSV/Excel ファイル）に複数の人の情報を入力して、その情報をクライアントに一括でインポートすることができます。

手順

1. 「個人」モジュールを開きます。
2. リストから追加した組織を選択するか、左上隅の**「追加」**をクリックして組織を追加し、その後選択します。
3. **「インポート」**をクリックしてインポートパネルを開きます。
4. インポートモードとして**「個人情報」**を選択します。
5. **「個人情報のインポート用テンプレートをダウンロード」**をクリックしてテンプレートをダウンロードします。
6. ダウンロードしたテンプレートに個人情報を入力します。

注意

- 人物が複数のカードを持っている場合は、カード番号をセミコロンで区切ってください。
- アスタリスクが付いた項目は必須です。
- デフォルトでは、採用日は現在の日付です。

7. クリック をクリックして、ローカルPCから個人情報が含まれたCSV/Excelファイルを選択してください。
8. **「インポート」**をクリックしてインポートを開始します。

注意

- クライアントのデータベースにすでにその人物のNo.が存在する場合、インポートする前に既存の情報を削除してください。
- 2,000人分の情報をインポートできます。

人物写真のインポート

クライアントに追加した人物の顔写真をインポートすると、追加した顔認識端末で写真の人物を識別できるようになります。人物の写真は、1人ずつインポートすることも、必要に応じて複数人分を一度にインポートすることもできます。

開始前に

事前にクライアントに人物情報をインポートしておいてください。

手順

1. 「人物」モジュールを開きます。

2. リストから追加した組織を選択するか、左上隅の**「追加」**をクリックして組織を追加し、その後選択します。
3. **「インポート」**をクリックしてインポートパネルを開き、**「顔」**にチェックを入れます。
4. **オプション：**クライアントで管理されている顔認識デバイスが写真内の顔を認識できるかどうかを確認するには、**[デバイスで確認]** を有効にします。
5. 「 ... 」をクリックして顔写真ファイルを選択します。

注意

- 顔写真のフォルダーは ZIP 形式で保存されている必要があります。
- 各画像ファイルは JPG 形式で、200 KB 以内にしてください。
- 各画像ファイルは「Person ID_Name」という名前で保存してください。Person IDは、インポートした人物情報と一致する必要があります。

6. **「インポート」**をクリックしてインポートを開始します。
インポートの進行状況と結果が表示されます。

人物情報のエクスポート

追加した人物の情報をCSV/Excelファイルとしてローカル**PC**にエクスポートできます。

開始前に

- 組織に人物を追加していることを確認してください。
- 「**個人情報のエクスポート**機能」が有効になっていることを確認してください。これにより、**エクスポート**ボタンが表示されることを確認してください。詳細については、以下を参照してください。

手順

1. 「個人」モジュールを開きます。
2. **オプション：**リストから組織を選択します。

注意

組織を選択しない場合、すべての人の情報がエクスポートされます。

3. **エクスポート**をクリックします。
4. 検証用にスーパーユーザー名とパスワードを入力してください。エクスポートパネルが表示されます。
5. エクスポートする内容として**「個人情報をチェック」**を選択してください。
6. エクスポートする項目を選択してください。
7. **「エクスポート」**をクリックして、エクスポートしたファイルを**PC**にCSV/Excelファイルとして保存します。

人物写真のエクスポート

追加した人物の顔写真ファイルをエクスポートし、**PC**に保存できます。

開始前に

- 組織に人物と顔写真を追加していることを確認してください。
- 「**人物情報のエクスポート**」機能を有効にしていることを確認してください。これにより、「**エクスポート**」ボタンが表示されていることを確認してください。詳細については、以下を参照してください。

手順

1. 「人物」モジュールを開きます。
2. **オプション：** リストから組織を選択します。

注意

組織を選択しない場合、すべての人の顔写真がエクスポートされます。

3. 上部メニューバーの「**エクスポート**」をクリックしてください。
4. 認証のため、スーパーユーザー名とパスワードを入力してください。
   エクスポートパネルが表示されます。
5. エクスポートするコンテンツとして「**顔**」を選択します。
6. 「**エクスポート**」をクリックし、エクスポートするファイルを暗号化するための暗号化キーを設定します。

注意

- エクスポートされたファイルはZIP形式です。
- エクスポートされた顔画像は「Person ID_Name_0」（「0」は正面向きの顔の場合）という名前で保存されます。

8.4.3 アクセス制御デバイスから個人情報を取得する

アクセス制御デバイスに個人情報（人物の詳細、指紋、発行カード情報など）が設定されている場合、追加したデバイスからその個人情報を取得し、クライアントにインポートしてさらに操作を行うことができます。

手順

注意

- デバイスに保存されている人物名が空の場合、クライアントにインポートすると、人物名は発行カード番号で入力されます。
- 人物はデフォルトで「**男性**」となります。
- デバイスに保存されているカード番号または人物ID（社員ID）がクライアントのデータベースにすでに存在する場合、このカード番号または人物IDを持つ人物はクライアントにインポートされません。

1. **人物**モジュールを開きます。
2. インポートする人物を含む組織を選択してください。
3. 「**デバイスから取得**」をクリックします。
4. ドロップダウンリストから追加したアクセス制御デバイスまたは登録ステーションを選択します。

注意

登録ステーションを選択した場合は、**[ログイン]** をクリックし、デバイスの IP アドレス、ポート番号、ユーザー名、およびパスワードを入力してください。

5. **取得モード**を選択します。

注意

取得モードは、デバイスによって異なります。アクセス制御デバイスは、従業員 ID による人物情報の取得に対応しています。1 回に指定できる従業員 ID は、最大 5 つまでです。

6. **インポート**をクリックして、クライアントへの人物情報のインポートを開始します。

注意

最大 2,000 人、5,000 枚のカードをインポートできます。

人物情報（人物の詳細情報、人物の指紋情報（設定されている場合）、および関連付けられたカード（設定されている場合））が、選択した組織にインポートされます。

8.4.4 一括で人物にカード発行

クライアントでは、複数の個人にカードをまとめて発行する便利な機能があります。

手順

1. **「人物」**モジュールを開きます。
2. **「一括カード発行」**をクリックします。

   カードが発行されていない追加された人物は、右側のパネルにすべて表示されます。
3. **オプション：**入力ボックスにキーワード（名前または人物 ID）を入力して、カードを発行する必要がある人物をフィルタリングします。
4. **オプション：[設定]** をクリックして、カード発行のパラメータを設定します。詳細については、を参照してください。
5. **初期化**をクリックして、カード登録ステーションまたはカードリーダーを初期化し、カード発行の準備を整えます。
6. **カード番号]** 列をクリックして、カード番号を入力します。
   - カードをカード登録ステーションに置きます。
   - カードリーダーにカードをスワイプしてください。
   - カード番号を手動で入力し、**Enter** キーを押してください。リストに

   表示された人物にカードが発行されます。

8.4.5 カード紛失の報告

カードを失くした場合は、カード紛失を報告することで、該当するカードのアクセス権限が無効化されます。

手順

1. **「人物」**モジュールを開きます。
2. カード紛失を報告する対象者を選択し、**編集**をクリックして「編集」ウィンドウを開きます。
3. 「**Credential→ Card**」パネルで、追加したカードを選択し、そのカードに「 」をクリックして、このカードを紛失したカードとして設定します。

   カード紛失を報告すると、このカードのアクセス権限は無効になり、使用不能になります。この紛失したカードを取得した他のユーザーは、このカードでドアにアクセスできなくなります。
4. **オプション：**紛失したカードが見つかった場合は、[ ]をクリックして紛失をキャンセルすることができます。

   紛失をキャンセルすると、該当者のアクセス権限は有効かつアクティブになります。
5. 紛失したカードが 1 つのアクセスグループに追加されており、そのアクセスグループがすでにデバイスに適用されている場合、カードの紛失を報告または紛失をキャンセルすると、デバイスに変更を適用するよう通知するウィンドウがポップアップ表示されます。デバイスに適用すると、これらの変更はデバイスに有効になります。

8.4.6 カード発行パラメーターの設定

クライアントには、カードの番号を読み取るための 2 つのモードがあります。カード登録ステーションを使用する方法と、アクセス制御デバイスのカードリーダーを使用する方法です。カード登録ステーションが利用可能な場合は、USB インターフェースまたは COM を使用して、クライアントを実行している PC に接続し、カード登録ステーションにカードをかざしてカード番号を読み取ります。利用できない場合は、追加したアクセス制御デバイスのカードリーダーでカードをスワイプしてカード番号を取得することもできます。その結果、1 人にカードを発行する前に、発行モードや関連パラメータなどのカード発行パラメータを設定する必要があります。

1人にカードを追加する際は、**設定をクリックして**「カード発行設定」ウィンドウを開きます。

ローカルモード：カード発行ステーションでカードごとに発行

カード登録ステーションを、クライアントを実行している PC に接続します。カード登録ステーションにカードを置くと、カード番号を取得できます。

カード登録ステーション

接続されたカード登録ステーションのモデルを選択します

注意

現在、対応しているカード登録ステーションのモデルは、DS-K1F100-D8、DS-K1F100-M、DS-K1F100-D8E、およびDS-K1F180-D8Eです。

カードの種類

このフィールドは、モデルが DS-K1F100-D8E または DS-K1F180-D8E の場合にのみ使用可能です。実際のカードの種類に応じて、カードの種類を EM カードまたは IC カードから選択してください。

シリアルポート

DS-K1F100-M の場合のみ使用可能です。カード登録ステーションが接続する COM を選択してください。

ブザー

カード番号が正常に読み取られた際にブザーをオンまたはオフにします。

カード番号タイプ

実際の要件に応じて、カード番号のタイプを選択してください。

M1カード暗号化

このフィールドは、モデルが DS-K1F100-D8、DS-K1F100-D8E、または DS-K1F180-D8E の場合にのみ使用できます。

カードがM1カードの場合、M1カード暗号化機能を有効にする必要がある場合は、この機能を有効にし、暗号化対象のカードのセクターを選択してください。

リモートモード：カードリーダーでカード発行

クライアントに追加したアクセス制御デバイスを選択し、そのカードリーダーでカードをスワイプしてカード番号を読み取ります。

8.5 スケジュールとテンプレートを設定する

テンプレートには休日や週のスケジュールを設定できます。テンプレートを設定した後、アクセスグループを設定する際、設定したテンプレートを適用することで、アクセスグループがテンプレートの時間範囲内で有効になります。

注意

アクセスグループの設定については、*「アクセスグループを設定してユーザーにアクセス権限を付与する」*を参照してください。

8.5.1 休日を追加

休日を作成し、休日の開始日、終了日、および休日の日数を設定できます。

手順

注

ソフトウェアシステムには、最大 64 件の休日を追加することができます。

1. **「アクセス制御」→「→」→「Schedule」→「→」→「Holiday」**をクリックして、休日設定画面に移動します。
2. 左側のパネルの「**追加**」をクリックします。
3. 休日の名前を入力します。
4. **オプション：**この休日の説明や通知を「備考」ボックスに入力します。
5. 休日リストに休日期間を追加し、休日の期間を設定します。

注意

1 つの休日に最大 16 個の休日期間を追加できます。

1)「休暇リスト」フィールドで**「追加」**をクリックします。

2) カーソルをドラッグして時間範囲を指定します。この時間範囲中は、設定されたアクセスグループが有効になります。

注

1 つの休日期間に設定できる時間枠は最大 8 つです。

3) **オプション：**時間枠を編集するには、次の操作を行います。
   - カーソルを時間範囲に合わせ、カーソルが「」に変わったら、タイムラインバー上の時間範囲をドラッグして希望の位置に移動します。
   - 時間範囲をクリックし、表示されたダイアログで開始/終了時間を直接編集します。
   - 時間範囲の開始または終了位置にカーソルを移動し、カーソルが「」に変わったらドラッグして時間範囲を延長または短縮します。
4) **オプション：**削除する時間範囲を選択し、[操作] 列の [] をクリックして、選択した時間範囲を削除します。
5) オプション：　をクリックして、タイムバー内のすべての時間範囲をクリアします。
6) オプション：　操作列をクリックして、この追加した休日期間を休日リストから削除します。

6. **保存**をクリックします。

8.5.2 テンプレートを追加

テンプレートには週のスケジュールと休日が含まれます。週のスケジュールを設定し、異なるユーザーまたはグループに対してアクセス権限の時間範囲を割り当てることができます。また、テンプレートに追加した休日を選択することもできます。

手順

注意

ソフトウェアシステムには、最大 255 個のテンプレートを追加できます。

1. **「アクセス制御」→「→ スケジュール」→「→ テンプレート」**をクリックしてテンプレートページに移動します。

注

デフォルトのテンプレートは「All-Day Authorized」と「All-Day Denied」の2つで、編集や削除はできません。

All-Day Authorized

アクセス許可は、週の各日に有効であり、休日はありません。

終日拒否

アクセス権限は、各曜日に無効となり、休日はありません。

2. 左側のパネルの**「追加」**をクリックして新しいテンプレートを作成します。

3. テンプレートの名前を入力してください。

4. このテンプレートの説明や通知事項を「備考」ボックスに入力します。

5. 週のスケジュールを編集してテンプレートに適用します。

1) 下部のパネルで「**週間スケジュール**」タブをクリックします。
2) 週の曜日を選択し、タイムラインバーに時間範囲をドラッグして設定します。

注

ウィークスケジュールでは、1 日につき最大 8 つの時間枠を設定できます。

3) **オプション：**時間枠を編集するには、次の操作を行います。

- カーソルを時間枠に移動し、カーソルが に変わったら、タイムラインバー上で時間枠をドラッグして希望の位置に移動します。
- 時間範囲をクリックし、表示されたダイアログで開始/終了時間を直接編集します。
- 時間範囲の開始または終了位置にカーソルを移動し、カーソルが に変わったらドラッグして時間範囲を延長または短縮します。

4) 上記の2つの手順を繰り返し、週の他の日に追加の時間範囲を描画します。

6. 休日を追加してテンプレートに適用します。

注意

1 つのテンプレートには、最大 4 つの休日を追加できます。

1) 「**休日**」タブをクリックします。
2) 左のリストから休日を選択すると、右のパネルの選択リストに追加されます。
3) **オプション：[追加]** をクリックして、新しい休日を追加します。

注意

休日の追加方法の詳細については、「*休日の追加*」を参照してください。

4) **オプション：**右側のリストで選択した休日を選択し、 をクリックして選択した休日を削除するか、**クリア**をクリックして右側のリストから選択したすべての休日をクリアします。

7. 設定を保存してテンプレートの追加を完了するには、**[保存]** をクリックします。

8.6 アクセスグループを設定して、ユーザーへのアクセス権限を割り当てます。

ユーザーを追加し、そのユーザーの認証情報を設定した後、どのユーザーがどのドアにアクセスできるかを定義するアクセスグループを作成し、そのアクセスグループをアクセス制御デバイスに適用して有効化できます。

開始前に

- クライアントに人を追加します。
- クライアントにアクセス制御デバイスを追加し、アクセスポイントをグループ化します。詳細については、*「グループ管理」*を参照してください。
- テンプレートを追加します。

手順

アクセスグループ設定を変更した場合、変更を反映させるために、デバイスにアクセスグループを再適用する必要があります。アクセスグループの変更には、テンプレートの変更、アクセスグループ設定の変更、ユーザーのアクセスグループ設定の変更、および関連するユーザーの詳細（カード番号、指紋、顔など）が含まれます。

画像、カード番号と指紋のリンク、カード番号と指紋のリンク、カードパスワード、カードの有効期間など）。

1. **[アクセス制御]、[→]、[Authorization]、[→]、[Access Group]** の順にクリックして、アクセスグループインターフェースに入ります。
2. **「追加」**をクリックして「追加」ウィンドウを開きます。
3. **名前**テキストフィールドに、アクセスグループの名前の任意の名前を入力します。
4. アクセスグループ用のテンプレートを選択します。

注意

アクセスグループの設定を行う前に、テンプレートを設定する必要があります。詳細については、***「スケジュール設定」とテンプレートの***を参照してください。

5. 「Select Person」フィールドの左側のリストから、アクセス権限を付与するユーザーを選択します。
6. 「アクセスポイントを選択」フィールドの左側のリストから、選択したユーザーがアクセスできるドア、ドアステーション、またはフロアを選択します。
7. **「保存」**をクリックします。
   インターフェースの右側に、選択した人物と選択したアクセスポイントが表示されます。

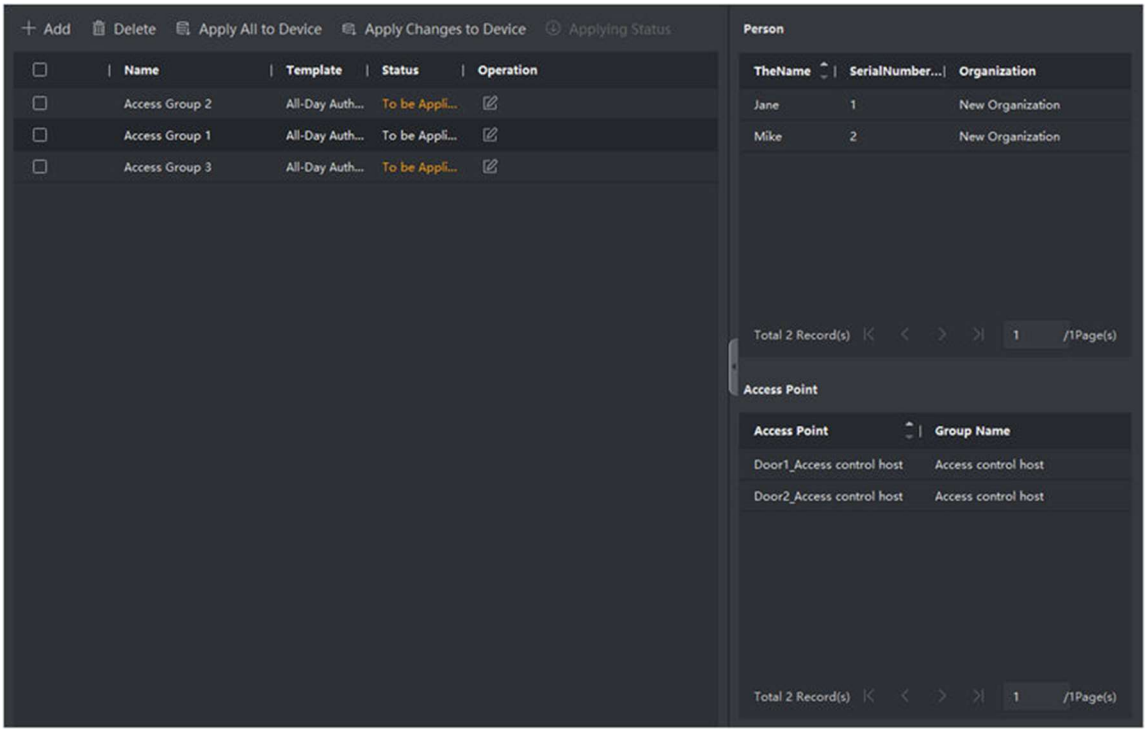


図8-2 選択したユーザーとアクセスポイントの表示

8. アクセスグループを追加した後、アクセス制御デバイスに適用する必要があります。
   1) アクセス制御デバイスに適用するアクセスグループを選択します。
   2) **「すべてのデバイスに適用」**をクリックすると、選択したすべてのアクセスグループがアクセス制御デバイスまたはドアステーションに適用されます。

3) **「すべてのデバイスに適用」**または「**変更をデバイスに適用**」をクリックします。**すべてのデバイスに適用**

この操作は、選択したデバイスの既存のすべてのアクセスグループを削除し、新しいアクセスグループをデバイスに適用します。

デバイスに変更を適用

この操作は、選択したデバイスの既存のアクセスグループを削除せず、選択したアクセスグループの変更部分のみをデバイスに適用します。

4) 適用状態はステータス列で確認するか、**適用状態**をクリックして適用されたすべてのアクセスグループを表示できます。

注意

「表示失敗のみ」にチェックを付けると、適用結果をフィルタリングできます。

適用されたアクセスグループに選択されたユーザーは、リンクされたカードまたは指紋を使用して、選択されたドア/ドアステーションへの入退室が許可されます。

9. オプション：必要に応じて、[ ]をクリックしてアクセスグループを編集します。

注

その人物のアクセス情報などを変更すると、クライアントの右下に**「適用するアクセスグループ」**というプロンプトが表示されます。
このメッセージをクリックすると、変更したデータをデバイスに適用できます。適用方法として「**今すぐ適用**」または「**後で適用**」を選択できます。

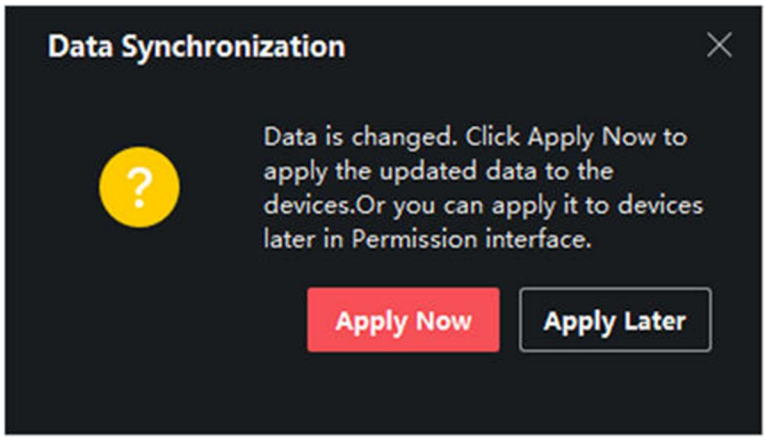


図8-3 データ同期

8.7 高度な機能の設定

アクセス制御の高度な機能を設定し、異なるシーンにおける特別な要件に対応できます。例えば、多要素認証、パスバック防止などです。

注意

- カード関連機能（アクセス制御カードのタイプ/多要素認証）については、アクセスグループが適用されたカードのみがカード追加時に一覧に表示されます。
- 高度な機能はデバイスでサポートされている必要があります。
- カーソルを高度な機能の上に移動し、[⚙] をクリックして、表示する高度な機能をカスタマイズします。

8.7.1 デバイスパラメーターの設定

アクセス制御デバイスを追加したら、アクセス制御デバイス（アクセスコントローラ）、アクセス制御ポイント（ドアまたはフロア）、アラーム入力、アラーム出力、カードリーダー、レーンコントローラのパラメータを設定できます。

アクセス制御デバイスのパラメーターを設定する

アクセス制御デバイスを追加した後、そのパラメーターを設定できます。具体的には、画像にユーザー情報を重ねて表示する、画像の撮影後に画像をアップロードする、撮影した画像を保存する、などです。

開始前に

クライアントにアクセス制御デバイスを追加します。

手順

1. **アクセス制御**をクリックします。→ クリックします。**Advanced Function をクリックします。→ をクリックします。**

   Parameter をクリックします。

   注意

   「高度な機能」リストに「デバイス パラメーター」が見つからない場合は、カーソルを「高度な機能」に合わせ、次にクリックします。 ⚙ をクリックして、表示するデバイス パラメーターを選択します。

2. 右側のページに表示するアクセスデバイスを選択します。
3. スイッチをONに切り替えて、対応する機能を有効にします。

   注

   - 表示されるパラメーターは、アクセス制御デバイスによって異なる場合があります。
   - 以下のパラメーターのいくつかは基本情報ページに表示されていません。パラメーターを編集するには**「詳細」**をクリックしてください。

   RS-485 通信冗長化

   RS-485カードリーダーをアクセス制御デバイスに冗長接続する場合、この機能を有効にしてください。

   認証時に検出された顔を表示

   認証時に顔写真を表示します。

   カード番号を表示

認証時にカード情報を表示します。

人物情報を表示

認証時に人物情報を表示します。

画像に人物情報を重ねて表示する。

キャプチャした画像に人物情報を表示します。

音声ガイド

この機能を有効にすると、デバイスで音声ガイドが有効になります。デバイスを操作する際、音声ガイドが再生されます。

リンクしたカメラで撮影した画像をアップロード

リンクされたカメラで撮影した画像を自動的にシステムにアップロードします。

リンクキャプチャ後に画像を保存

この機能を有効にすると、リンクカメラで撮影した画像をデバイスに保存することができます。

カード番号を入力するにはキーを押してください

この機能を有効にすると、キーを押してカード番号を入力することができます。

Wi-Fi プローブ

この機能を有効にすると、デバイスは周囲の通信デバイスの MAC アドレスをプローブし、その MAC アドレスをシステムにアップロードします。MAC アドレスが指定の MAC アドレスと一致する場合、システムはリンク動作をトリガーします。

3G/4G

この機能を有効にすると、デバイスは 3G/4G ネットワークで通信することができます。

NFC 複製防止

この機能を有効にすると、複製されたカードは認証に使用できなくなり、セキュリティがさらに強化されます。

4. **OK**をクリックしてください。
5. **オプション：[コピー先]** をクリックし、ページ内のパラメータをコピーするアクセス制御デバイスを選択します。

ドア/エレベーターのパラメーターを設定

アクセス制御デバイスを追加した後、そのアクセスポイント（ドアまたはフロア）のパラメーターを設定できます。

開始前に

クライアントにアクセス制御デバイスを追加します。

手順

1. **アクセス制御**をクリックします。**→ をクリックします。Advanced Functionをクリックします。→ をクリックします。Device Parameterをクリック**します。
2. 左側のパネルでアクセス制御デバイスを選択し、[▸] をクリックして、選択したデバイスのドアまたはフロアを表示します。

3. 右側のページに表示するドアまたは床を選択してください。

4. ドアまたは床のパラメーターを編集します。

注意

- 表示されるパラメーターは、アクセス制御デバイスによって異なる場合があります。
- 以下のパラメーターのいくつかは基本情報ページに表示されていません。編集するには**「詳細」**をクリックしてください。

名前

カードリーダーの名前を任意で編集してください。

ドアコンタクト

ドアセンサーを「常に閉」または「常に開」に設定できます。通常は「常に閉」です。

出口ボタンタイプ

出口ボタンを「常に閉じた状態」または「常に開いた状態」に設定できます。通常は「常に開いた状態」に設定されています。

ドアロック時間

通常のカードでスワイプし、リレー動作が完了すると、ドアのロックタイマーが動作を開始します。

延長開錠時間

延長アクセス権限を持つユーザーがカードをかざす必要があり、適切な遅延後にドアコンタクトを有効にできます。

ドア開時間切れアラーム

設定された時間内にドアが閉まらなかった場合、アラームが作動します。0 に設定すると、アラームは作動しません。

ドアが閉まったらロックする

ドアが閉まると、**ドアロック時間設定が**到達していなくてもロックされます。

緊急コード

緊急事態が発生した場合、緊急コードを入力するとドアを開けることができます。同時に、クライアントは緊急事態を報告することができます。

スーパーパスワード

特定の人がスーパーパスワードを入力すると、ドアを開けることができます。

解除コード

カードリーダーのブザーを停止するための解除コードを作成します（キーパッドに解除コードを入力することで使用可能です）。

注

- 緊急コード、スーパーコード、および終了コードは異なる必要があります。
- 緊急コード、スーパーパスワード、および解除コードは、認証パスワードと異なる必要があります。
- 緊急コード、スーパーパスワード、および解除コードの長さはデバイスによって異なります。通常、4から8桁の数字で構成されます。

5. **OK**をクリックしてください。
6. オプション：**コピー先**をクリックし、ページ内のパラメータをコピーするドア/フロアを選択します。

注意：床の状態の持続時間設定は、選択したドア/床にもコピーされます。

カードリーダーのパラメーターを設定する

アクセス制御デバイスを追加した後、そのカードリーダーのパラメーターを設定できます。

開始前に

クライアントにアクセス制御デバイスを追加します。

手順

1. **アクセス制御**をクリック→**をクリックしますAdvanced Functionをクリックします→ をクリックしますDevice Parameter**をクリックします。
2. 左側のデバイス一覧で「 」をクリックしてドアを展開し、カードリーダーを選択すると、右側でカードリーダーのパラメーターを編集できます。
3. 基本情報ページでカードリーダーの基本パラメーターを編集します。

注意

- 表示されるパラメーターは、アクセス制御デバイスによって異なる場合があります。以下のリストに一部のみが記載されています。詳細については、デバイスのユーザーマニュアルをご参照ください。
- 以下のパラメーターのいくつかは基本情報ページに表示されていません。編集するには**「詳細」**をクリックしてください。

名前

カードリーダーの名前を任意で編集してください。

OK LED極性/エラーLED極性/ブザー極性

カードリーダーのパラメータに応じて、メインボードの OK LED の極性、エラー LED の極性、およびブザー LED の極性を設定します。通常、デフォルト設定を採用します。

最小カードスワイプ間隔

同じカードのスワイプ間隔が設定値未満の場合、スワイプは無効となります。設定値は0から255まで設定可能です。

PWD 入力時の最大間隔

カードリーダーでパスワードを入力する際、2つの数字を入力する間の間隔が設定値を超えると、以前に入力した数字が自動的に消去されます。

最大失敗回数アラーム

カード読み取りの試行回数が設定値に達した場合にアラームを鳴らすかどうかを設定します。

カード読み取りの最大失敗回数

カード読み取りの最大失敗回数を設定します。

不正操作検出

カードリーダーの改ざん検出機能を有効にします。

コントローラーと通信する

アクセス制御装置がカードリーダーと設定された時間を超えて接続できない場合、カードリーダーは自動的にオフラインになります。

ブザー鳴動時間

カードリーダーのブザー音を鳴らす時間を設定します。設定可能な時間は0から5,999秒です。0は連続したブザー音を意味します。

カードリーダーのタイプ/カードリーダーの説明

カードリーダーのタイプと説明を取得します。これらは読み取り専用です。

指紋認証レベル

ドロップダウンリストから指紋認識のレベルを選択します。

デフォルトのカードリーダー認証モード

デフォルトのカードリーダー認証モードを表示します。

指紋容量

利用可能な指紋の最大数を表示します。

既存の指紋の数

デバイスに保存されている指紋の数を表示します。

スコア

デバイスは、ヨー角、ピッチ角、瞳孔距離に応じて、キャプチャした画像にスコアを付けます。スコアが設定値より低い場合、顔認識は失敗します。

顔認識タイムアウト値

認識時間が設定された時間を超過した場合、デバイスが通知します。

顔認識間隔

認証時に連続する2つの顔認識の間隔。デフォルトでは2秒です。

顔1対1一致閾値

1:1マッチングモードで認証を行う際の一致閾値を設定します。値が大きいほど、認証時の誤認率が低く、誤拒否率が大きくなります。

1:N セキュリティレベル

1:N 照合モードで認証を行う場合の一致セキュリティレベルを設定します。値が大きいほど、認証時の誤認識率は低くなり、誤拒否率は高くなります。

ライブ顔検出

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

ライブ顔検出セキュリティレベル

ライブ顔検出機能を有効にした後、ライブ顔認証を行う際の一致セキュリティレベルを設定できます。

顔認証の最大失敗回数

ライブ顔検出の失敗回数の最大値を設定します。設定した回数を超える失敗が発生した場合、システムはユーザーの顔を5分間ロックします。同じユーザーは5分間、偽の顔での認証はできません。5分間以内に、ユーザーは本物の顔で連続して2回認証を行うことでロックを解除できます。

認証失敗時の顔ロック

ライブ顔検出機能を有効にした後、設定された回数を超えてライブ顔検出に失敗した場合、システムはユーザーの顔を5分間ロックします。同じユーザーは5分以内に偽の顔で認証できません。5分以内に、ユーザーは本物の顔で連続して2回認証することでロックを解除できます。

アプリケーションモード

実際の環境に応じて、屋内またはその他のアプリケーションモードを選択できます。

4. **OK**をクリックしてください。
5. **オプション：[コピー先]** をクリックし、ページ内のパラメータをコピーするカードリーダーを選択します。

アラーム出力のパラメータを設定する

アクセス制御デバイスを追加した後、デバイスがアラーム出力にリンクしている場合は、パラメータを設定できます。

開始前に

クライアントにアクセス制御デバイスを追加し、そのデバイスがアラーム出力をサポートしていることを確認してください。

手順

1. **アクセス制御**をクリックし、**→**、**Advanced Function**、**→ Device Parameter** の順にクリックして、アクセス制御パラメーター設定ページに移動します。
2. 左側のデバイスリストで「 」をクリックしてドアを展開し、アラーム入力を選択すると、右側でアラーム入力のパラメータを編集できます。
3. アラーム出力パラメータを設定します。

名前

カードリーダーの名前を任意で編集します。

アラーム出力アクティブ時間

アラーム出力のトリガー後、アラーム出力が持続する時間。

4. **OK**をクリックします。
5. **オプション：**アラーム出力をトリガーするには、右上隅のスイッチを **ON** に設定します。

レーンコントローラーのパラメーターを設定する

レーンコントローラをクライアントに追加したら、レーンを通過するためのそのパラメータを設定できます。

開始前に

クライアントにアクセス制御デバイスを追加します。

手順

1. **[アクセス制御] > [→] >[Advanced Function] > [→] >** [**Device Parameter**] をクリックして、パラメーター設定ページを開きます。
2. 左側のデバイス一覧からレーンコントローラーを選択し、右側でレーンコントローラーのパラメーターを編集できます。
3. パラメーターを編集します。

通過モード

デバイスのバリア状態を制御するコントローラーを選択してください。

- **「レーンコントローラーのDIP設定に従う」**を選択した場合、デバイスはレーンコントローラーのDIP設定に従ってバリアを制御します。ソフトウェアの設定は無効になります。
- **「メインコントローラーの設定に従う」**を選択した場合、デバイスはソフトウェアの設定に従ってバリアを制御します。レーンコントローラーのDIP設定は無効になります。

フリーパス認証

この機能を有効にすると、入口と出口の両方のバリアモードが「開いたまま」の場合、歩行者はレーンを通過するたびに認証を行う必要があります。または、アラームが作動します。

バリアの開閉速度

バリアの開閉速度を設定します。1から10まで選択可能です。数値が大きいほど速度が速くなります。

注意

です。

音声アラームの持続時間

アラームが作動したときに鳴るオーディオの再生時間を設定します。

注

0 は、アラームが終了するまでアラーム音が鳴り続けることを意味します。

温度単位

デバイス状態に表示される温度単位を選択します。

4. **OK**をクリックしてください。

8.7.2 その他のパラメーターを設定する

アクセス制御デバイスを追加した後、ネットワークパラメータ、キャプチャパラメータ、RS-485 パラメータ、Wiegand パラメータなどのパラメータを設定できます。

顔認識端末のパラメーター設定

顔認識端末では、顔画像データベース、QRコード認証など、そのパラメーターを設定できます。

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. アクセス制御モジュールを開きます。

2. 左側のナビゲーションバーで、**[Advanced Function]**、**[→]**、**[More Parameters]** の順に選択します。

3. デバイス一覧からアクセス制御デバイスを選択し、**顔認識端末**をクリックします。

4. パラメーターを設定します。

注意
表示されるパラメーターは、デバイスモデルによって異なります。

COM

設定する COM ポートを選択します。COM1 は RS-485 インターフェース、COM2 は RS-232 インターフェースを指します。

顔画像データベース

顔画像データベースとして「Deep Learning」を選択してください。

QRコードによる認証

有効にすると、デバイスのカメラで QR コードをスキャンして認証を行うことができます。デフォルトでは、この機能は無効になっています。

ブロックリスト認証

有効に設定されている場合、デバイスはアクセスを要求した人物とブロックリストに登録されている人物を比較します。

一致した場合（その人物がブロックリストに登録されている場合）、アクセスは拒否され、デバイスはクライアントにアラームを送信します。

一致しない場合（ブロックリストに該当する人物がいない場合）、アクセスが許可されます。

認証時の顔写真を保存

有効にすると、認証時にキャプチャした顔写真がデバイスに保存されます。

MCUバージョン

デバイスのMCUバージョンを確認します。

5. **保存**をクリックします。

RS-485 パラメーターの設定

ボーレート、データビット、ストップビット、パリティタイプ、フロー制御タイプ、通信モード、作業モード、接続モードなど、アクセス制御装置の RS-485 パラメータを設定できます。

開始前に

クライアントにアクセス制御デバイスを追加し、そのデバイスが RS-485 インターフェースに対応していることを確認してください。

手順

1. アクセス制御モジュールを開きます。

2. 左側のナビゲーションバーで、**[Advanced Function]**、**[→]**、**[More Parameters]** の順に選択します。

3. デバイス一覧からアクセス制御デバイスを選択し、**RS-485をクリック**してRS-485設定ページに移動します。

4. RS-485パラメーターを設定するには、ドロップダウンリストからシリアルポート番号を選択してください。

5. ドロップダウンリストからボーレート、データビット、ストップビット、パリティタイプ、通信モード、動作モード、接続モードを設定します。

注意

接続モードが「**アクセス制御デバイスに接続**」の場合、出力タイプとして**「カード番号」**または「人ID」を選択できます。

ユーザーIDを出力タイプとして選択できます。

6. **保存**をクリックします。

- 設定したパラメーターはデバイスに自動的に適用されます。
- 動作モードまたは接続モードを変更すると、デバイスは自動的に再起動します。

Wiegand パラメーターの設定

アクセス制御デバイスのWiegandチャネルと通信モードを設定できます。Wiegandパラメーターを設定後、デバイスはWiegand通信経由でWiegandカードリーダーと接続できます。

開始前に

クライアントにアクセス制御デバイスを追加し、デバイスが Wiegand をサポートしていることを確認してください。

手順

1. アクセス制御モジュールを開きます。

2. 左側のナビゲーションバーで、**[Advanced Function]**、**[→]**、**[More Parameters]** の順に選択します。

3. デバイス一覧からアクセス制御デバイスを選択し、**[Wiegand]** をクリックして Wiegand 設定ページに移動します。
4. デバイスのWiegand機能を有効にするため、スイッチをオンに設定します。
5. ドロップダウンリストから Wiegand チャンネル番号と通信モードを選択します。

注意

通信方向を「**送信**」に設定した場合、**Wiegand モード**を
ワイガンド 26 または **ワイガンド 34**。

6. **保存**をクリックします。
   - 設定したパラメーターは自動的にデバイスに適用されます。
   - 通信方向を変更すると、デバイスは自動的に再起動します。

M1カード暗号化を有効にする

M1 カード暗号化を有効にすると、認証のセキュリティレベルが向上します。

手順

注意
この機能は、アクセス制御デバイスとカードリーダーの両方でサポートされている必要があります。

1. アクセス制御モジュールを開きます。
2. 左側のナビゲーションバーで、**[Advanced Function]**、**[→]**、**[More Parameters]** の順に選択します。
3. デバイス一覧からアクセス制御デバイスを選択し、**[M1カード暗号化]**をクリックしてM1カード暗号化ページに移動します。
4. スイッチをオンに設定して、M1カード暗号化機能を有効にします。
5. セクターIDを設定します。

   セクターIDは1から100までの範囲です。
6. 設定を保存するには「**保存**」をクリックします。

8.8 ドア/エレベーター制御

モニタリングモジュールでは、追加したアクセス制御デバイスによって管理されているドアやエレベーターのリアルタイムの状態を確認できます。また、クライアントからリモートでドアの開閉、ドアの開けたまま/閉めたままの状態の維持など、ドアやエレベーターを制御することもできます。リアルタイムのアクセスイベントは、このモジュールに表示されます。アクセス詳細および人物の詳細を確認できます。

注意
ドア/エレベーターの制御権限を持つユーザーは、モニタリングモジュールにアクセスし、ドア/エレベーターを制御できます。または、制御用のアイコンが表示されません。ユーザー権限の設定については、を参照してください。

8.8.1 ドアの状態制御

ドアのステータスを制御できます。具体的には、ドアの解錠、ドアの施錠、ドアを解錠したままにする、ドアを施錠したままにする、すべてのドアを解錠したままにするなどです。

開始前に

- ユーザーを追加し、指定したユーザーにアクセス権限を付与します。これにより、ユーザーはアクセスポイント（ドア）へのアクセス権限を取得します。詳細については、*「ユーザー管理」*および「*ユーザーにアクセス権限を付与するためのアクセスグループの設定*」を参照してください。
- 操作ユーザーがアクセスポイント（ドア）の権限を持っていることを確認してください。詳細については、を参照してください。

手順

1. **「モニタリング」**をクリックしてステータス監視ページに移動します。
2. 画面右上にあるアクセスポイントグループを選択します。

注意

アクセスポイントグループの管理については、*グループ管理*を参照してください。選択

したアクセス制御グループ内のドアが表示されます。

3. ドアアイコンをクリックしてドアを選択するか、**Ctrl キー**を押しながら複数のドアを選択します。

注意

「**すべてのドアを解錠したまま**」および「**すべてのドアを施錠したまま**」を選択した場合、この手順を無視してください。

4. 以下のボタンをクリックしてドアを制御します。

解錠

ドアがロックされている場合、ロックを解除すると、一度だけ開きます。開いている間は、ドアは自動的に閉まり、再びロックされます。

ロック

ドアが解錠されている場合、施錠するとドアが閉まります。アクセス権限を持つユーザーは、認証情報を使用してドアにアクセスできます。

施錠解除状態を維持

ドアはロック解除されます（閉まっているか開いているかは関係ありません）。すべての人が認証情報なしでドアにアクセスできます。

常に施錠状態

ドアは閉まり、ロックされます。スーパーユーザーを除き、認証情報を持つユーザーもドアにアクセスすることはできません。

すべて解錠状態を維持

グループ内のすべてのドアのロックが解除されます（閉まっているか開いているかは関係ありません）。すべての人が認証情報なしでドアにアクセスできます。

すべてのドアをロックしたままにする

グループ内のすべてのドアが閉まり、ロックされます。スーパーユーザーを除き、認証情報を持っている人でもドアにアクセスすることはできません。

キャプチャ

手動で写真を撮影します。

メモ

キャプチャボタンは、デバイスがキャプチャ機能をサポートしている場合に表示されます。写真は、クライアントを実行している PC に保存されます。保存先の設定については、を参照してください。

結果

操作が成功した場合、ドアのアイコンは操作に応じてリアルタイムで変更されます。

8.8.2 リアルタイムアクセス記録の確認

カードスワイプ記録、顔認識記録、皮膚表面温度情報など、リアルタイムのアクセス記録をクライアントに表示することができます。また、人物情報やアクセス時に撮影された画像も確認することができます。

開始前に

クライアントに人物とアクセス制御デバイスを追加していること。詳細については、*「人物の管理」*および「*デバイスの追加*」を参照してください。

手順

1. **「モニタリング」**をクリックしてモニタリングモジュールに入ります。

   リアルタイムアクセス記録は、ページの下部に表示されます。カード番号、人物名、イベント時間、ドアの位置、温度、認証タイプなどの記録の詳細を確認できます。

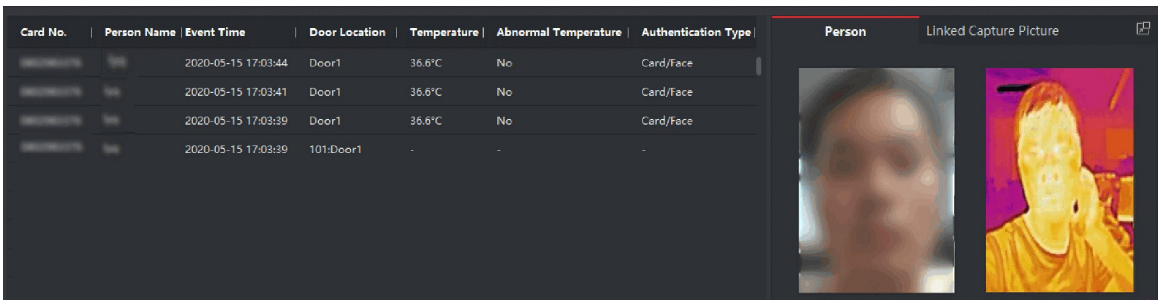


図8-4 リアルタイムアクセス記録

注

アクセスイベントテーブルの列名を右クリックすると、実際の必要に応じて列の表示/非表示を切り替えることができます。

2. **オプション：**右上隅のドロップダウンリストからアクセスポイントグループを選択すると、選択したグループのリアルタイムアクセス記録を表示できます。
3. **オプション：**イベントタイプとイベントステータスを確認します。

   チェックしたタイプおよびステータスの検出イベントが、以下のリストに表示されます。
4. **オプション：**最新のアクセス記録を表示するには、**「最新の**イベントを表示**」**にチェックを入れます。記録リストは、新しい順に表示されます。
5. **オプション：「異常温度の警告を表示」**にチェック**を入れると、**皮膚表面の異常温度の警告を表示することができます。

   アラートを有効にします。

注意

有効にすると、異常温度情報がある場合、モニタリングモジュールに入ると「異常温度」ウィンドウがポップアップし、人物の写真、皮膚表面温度、カード番号、人物名などが表示されます。

6. **オプション：**イベントをクリックすると、人物の写真（撮影された写真とプロフィールを含む）を表示できます。

注

リンクされたキャプチャ画像フィールドで、キャプチャした画像をダブルクリックすると、拡大表示された画像を表示できます。

7. オプション： をクリックして、監視の詳細（人物の詳細情報とキャプチャされた画像を含む）を表示できます。

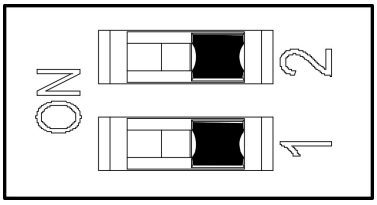
注意

ポップアップウィンドウで、 をクリックして、監視の詳細をフルスクリーン

付録A. DIPスイッチ

A.1 DIP スイッチ 説明

DIPスイッチはアクセスコントロールボード上にあります。No.1とNo.2は、下位ビットから上位ビットです。



図A-1 DIPスイッチ

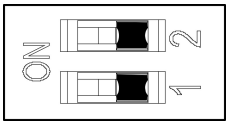
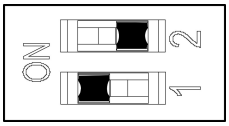
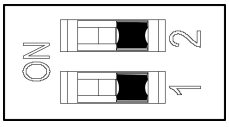
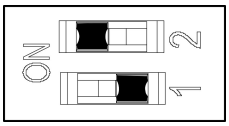
スイッチがONの方向にある場合、スイッチが有効であることを示し、そうでない場合はスイッチがオフです。

A.2 DIPスイッチに対応する機能

注意

DIPスイッチを設定した後、デバイスを再起動する必要があります。そうでないと、機能は有効になりません。

2ビットのDIPスイッチとアクセス制御ボードの対応する機能は以下の通りです:

ビット	デバイスモード	機能	10進値	DIPスイッチアドレス図
1	動作モード	通常モード	0	
		学習モード	1	
2	キーフォブペアリングモード	キーフォブペアリングモードを無効にする	0	
		キーフォブペアリングモードを有効にする	1	

付録 B. ボタン設定説明

メインレーン制御ボードのボタンを使用したデバイス設定については、以下の表を参照してください。

レベル 1 構成 No.	説明	レベル 1 構成 No. と機能	備考
1	学習モード	1-学習モード終了/通常モード 2-学習モード **メモ** デフォルトでは、ディスプレイ画面に「1」が表示されます。	デバイスにアクセス制御ボードが搭載されている場合、設定はDIPスイッチ経由でのみ可能です。
2	キーフォブペアリングモード	1-通常モード 2-ペアリングモード **注** デフォルトでは、ディスプレイ画面に「1」が表示されます。	デバイスにアクセス制御ボードが搭載されている場合、DIPスイッチでのみ設定可能です。
3	通過モード	1-両側制御中 **注意** デフォルトでは、ディスプレイ画面に「1」が表示されます。 2-入口は制御中；出口は禁止 3-入口は制御中；出口は誘導モード 4-両側誘導モード	

レベル-1 構成 No.	説明	レベル-1 構成 No. および機能	備考
		5-誘導モードでの進入；制御下での退出 6-誘導モードで進入；制御下で退出 7-両側禁止 8-入口禁止；出口は制御下で許可 9-入口禁止；出口は誘導モードで 10-入口は制御下で、出口は開いたままです 11-入口は制御下にあります；出口は自由モードです 12-入口は誘導方式で制御中；出口は常に開いています 13-入口は誘導方式；出口は自由モード 14-入口禁止；出口は開いたまま 15-入口禁止；出口は自由モード 16-入口は開いたまま；出口は制御下にあります 17-入口は開いたまま；出口は誘導モード	

レベル-1 構成 No.	説明	レベル-1 構成 No. および機能	備考
		18-入口は開いたまま；出口は開いたまま 19-入口は開いたまま；出口は自由モード 20-入口は開いたまま；出口は禁止 21-入口は自由モード；出口は制御下 22-入口は自由モード；出口は誘導モード 23-入口は自由モード；出口は開いたまま 24-入口は自由モード；出口は自由モード 25-入口は自由通行；出口は禁止	
4	メモリモード	1-無効 2-有効 **注意** デフォルトでは、ディスプレイ画面に2が表示されます。	
5	キーフォブ リモコン	1-1対1 2-1対複数 **注** デフォルトでは、ディスプレイ画面に1が表示されます。	

レベル 1 設定 No.	説明	レベル 1 設定 No. と機能	備考
6	バリアの開閉速度	1-1、2-2、...10-10  注 デフォルトでは、ディスプレイ画面に5が表示されます。	
7	バリアの閉速度	1-1、2-2、...10-10  注 デフォルトでは、ディスプレイ画面に5が表示されます。	
8	アラームエリアでのカード読み取り	1-開けない 2-開ける  注意 デフォルトでは、ディスプレイ画面に2が表示されます。	
9	期間を入力	5-5秒、6-6秒、7-7秒、...、60-60秒  注 デフォルトでは、ディスプレイ画面に5が表示されます。	
10	退出時間	5-5秒、6-6秒、7-7秒、...、60-60秒  注 デフォルトでは、ディスプレイ画面に5が表示されます。	
11	赤外線センサーの検知時間	0-0秒、1-1秒、2-2秒、...、25-25s	

レベル 1 構成 No.	説明	レベル 1 構成 No. および機能	備考
		注 デフォルトでは、ディスプレイ画面に0が表示されます。	
12	侵入検知時間	0-0秒、1-1秒、2-2秒、...、20-20秒 注 デフォルトでは、ディスプレイ画面に0が表示されます。	
13	超過時間	0-0秒、1-1秒、2-2秒、...、20-20秒 注 デフォルトでは、表示画面に0が表示されます。	
14	バリア閉塞遅延時間	0-0秒、1-1秒、2-2秒、3-3秒、4-4秒、5-5秒 注 デフォルトでは、ディスプレイ画面に0が表示されます。	
15	制御モード	1-ボタン設定 2-アクセス制御ボードのDIPスイッチ 注 デフォルトでは、ディスプレイ画面に「1」が表示されます。	
18	レーン番号	1-2車線	変更不可

レベル-1 構成 No.	説明	レベル-1 構成 No. および機能	備考
		2-シングルレーン 注 デフォルトでは、ディスプレイ画面に1が表示されます。	
19	モーターの回転	1-時計回り 2-反時計回り 注 デフォルトでは、ディスプレイ画面に「1」が表示されます。	変更できません
21	音量	1-0，2-1，3-2，4-3， 5-4 注 デフォルトでは、ディスプレイ画面に「2」が表示されます。	「1」に設定すると、デバイスがミュートされます。
22	認証通過	1-無効 2-有効 注 デフォルトでは、ディスプレイ画面に「1」が表示されます。	ボタンで変更できません
23	無効なカード番号	1-2を無効にする - 有効にする 注意 デフォルトでは、ディスプレイ画面に1が表示されます。	ボタンで変更できません

レベル-1 設定 No.	説明	レベル-1 設定 No. と機能	備考
2	指紋不一致	1-無効 2-有効 注 デフォルトでは、ディスプレイ画面に1が表示されます。	ボタンで変更できません
25	障害物を乗り越える	1-無効 2-有効 注 デフォルトでは、ディスプレイ画面に1が表示されます。	
26	逆方向通過	1-無効 2-有効 注 デフォルトでは、ディスプレイ画面に1が表示されます。	
27	通過時間超過	1-無効 2-有効 注 デフォルトでは、ディスプレイ画面に1が表示されます。	
28	侵入検知アラーム	1-無効 2-有効 注 デフォルトでは、ディスプレイ画面に1が表示されます。	

レベル-1 設定 No.	説明	レベル-1 構成番号と機能	備考
29	強制通過	1-無効 2-有効 注 デフォルトでは、ディスプレイ画面に1が表示されます。	ボタンで変更できません
3	テールゲートアラーム	1-無効 2-有効 注 デフォルトでは、ディスプレイ画面に1が表示されます。	
31	無許可の追い越し	1-無効 2-有効 注 デフォルトでは、ディスプレイ画面に1が表示されます。	ボタンで変更できません
32	認証有効期限超過	1-無効 2-有効 注 デフォルトでは、ディスプレイ画面に1が表示されます。	ボタンで変更できません
33	認証に失敗しました	1-無効 2-有効 注 デフォルトでは、ディスプレイ画面に1が表示されます。	ボタンで変更できません

レベル-1 設定 No.	説明	レベル-1 設定 No. と機能	備考
3	有効期限切れの資格情報	1-無効 2-有効 注 デフォルトでは、ディスプレイ画面に1が表示されます。	ボタンで変更できません
35	オーバーステイアラーム	1-無効 2-有効 注 デフォルトでは、ディスプレイ画面に1が表示されます。	
36	バリア材質	1-アクリル 2-ステンレス鋼3層ガラス	
3	バリア長	1-550 2-600 3-650 4-700 5-750 6-800 7-850 8-900 9-950 10-1000 11-1100 12-1200 13-1300 14-1400	

レベル-1 構成 No.	説明	レベル-1 構成番号と機能	備考
		注 デフォルトでは、ディスプレイ画面に8が表示されます。	
3	モーター点検	1- 無効 2- メインレーンで有効 3- サブレーンで有効にする 注 デフォルトでは、ディスプレイ画面に1が表示されます。	
3	ライトの明るさ	0-0，1-1，2-2, … , 10-10 注 デフォルトでは、ディスプレイ画面に3が表示されます。	値が高いほど、光が明るくなります。
4	自己診断音声ガイド	1- 無効 2-有効 注 デフォルトでは、ディスプレイ画面に「2」が表示されます。	
41	学習モード音声プロンプト	1- 無効 2-有効 注 デフォルトでは、ディスプレイ画面に2が表示されます。	

レベル-1 設定 No.	説明	レベル-1 設定 No. と機能	注
4	c	4-4，6-6，8-8, 注 デフォルトでは、ディスプレイ画面に4が表示されます。	ボタンで変更できません
43	アプリケーションモード	1-防風2室内用 デフォルトでは、ディスプレイ画面に1が表示されます。	
44	バリア回復時間	1-通常速度 2-高速回復 デフォルトでは、ディスプレイ画面に1が表示されます。	
45	ブレーキ	1-無効 2-バリア位置異常 3-侵入検知 デフォルトでは、ディスプレイ画面に2が表示されます。	
4	ブレーキ角度	1-5° 2-10° 3-15° デフォルトでは、ディスプレイ画面に1が表示されます。	
47	赤外線センサー	1-単発トリガー 2-同時トリガー	

レベル-1 設定 No.	説明	レベル-1 構成 No. および機能	注
		デフォルトでは、ディスプレイ画面に1が表示されます。	
4	ファン	1-無効 2-有効 デフォルトでは、ディスプレイ画面に2が表示されます。	
49	バリアの高さ	1-700 2-1200 3-1400 4-1600 5-1800 デフォルトでは、ディスプレイ画面に5が表示されます。	
99	デフォルトに戻す	1- デフォルト 2- 開始 注 デフォルトでは、ディスプレイ画面に1が表示されます。	

付録 C. イベントおよびアラームの種類

イベント	アラームタイプ
車間距離不足	視覚的および聴覚的
後方通過	視覚的および聴覚的
強制アクセス	なし
障害物を乗り越える	視覚的および聴覚的
滞在時間超過	視覚的および聴覚的
通過タイムアウト	なし
侵入検知	視覚的および聴覚的
認証失敗時の通過許可	視覚的および聴覚的
バリアが遮断されています	なし

付録 D. オーディオインデックス関連コンテンツの表

注

- デバイスにアクセス制御ボードが搭載されていない場合、スピーカーはメイン拡張インターフェースボードに接続する必要があります。
- デバイスにアクセス制御ボードが搭載されている場合、スピーカーはアクセス制御ボードに接続する必要があります。ウェブ経由でカスタム放送設定を行うことができます。

内容
バリアを乗り越える。
逆方向通行。
通過時間切れ。
侵入検知
車間距離の過近接近。
滞在時間超過。

付録 E. エラーコードの説明

エラーが発生すると、スイングバリアは 7 セグメントディスプレイにエラーコードを表示します。各番号の説明については、以下の表をご覧ください。

エラー原因	コード	エラー原因	コード
最初の赤外線ビームがトリガーされました	0	13番目の赤外線ビームがトリガーされました	13
2番目の赤外線ビームがトリガーされました	02	14番目の赤外線ビームがトリガーされました	14
第3の赤外線ビームがトリガーされました	03	認証表示板（入口）オフライン	49
第4の赤外線ビームがトリガーされました	04	認証表示板（出口）オフライン	50
第5の赤外線ビームがトリガーされました	05	赤外線アダプターボード オフライン	5
6番目の赤外線ビームがトリガーされました	06	インターコネクト例外	53
7番目の赤外線ビームがトリガーされました	07	学習中ではない	54
第8の赤外線ビームがトリガーされました	08	障害物	55
第9の赤外線ビームがトリガーされました	09	測定範囲外	56
第10の赤外線ビームがトリガーされました	10	エンコーダー異常	57
11番目の赤外線ビームがトリガーされました	11	モーターの例外	58
12番目の赤外線ビームがトリガーされました	12	拡張インターフェースボードオフライン（ボードがインストールされていない場合、エラーコード「49」が表示されますが、デバイスは正常に機能します）	59

付録 F. 通信マトリックスおよびデバイスコマンド

通信マトリックス

以下のQRコードをスキャンして、デバイスの通信マトリックスを取得してください。
このマトリックスには、Hikvision アクセス制御およびビデオインターコムデバイスのすべての通信ポートが含まれています。

図 F-1 通信マトリックスの QR コード

デバイスコマンド

以下のQRコードをスキャンして、デバイスの共通シリアルポートコマンドを取得してください。
コマンドリストには、すべての Hikvision アクセス制御およびビデオインターコムデバイスで一般的に使用されるシリアルポートコマンドがすべて含まれていることにご注意ください。

図 F-2 デバイスコマンド


See Far, Go Further