DS-K6B530TXシリーズ スイングバリア モジュール

ユーザーマニュアル

安全に関する注意事項

本取扱説明書は、ユーザーが製品を正しく使用し、危険や財産の損失を避けることを目的としています。

注意事項は「危険」と「注意」に分類されます：

危険：警告を無視すると、重傷または死亡事故を引き起こす可能性があります。

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

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

⚠ 危険：

- 本製品の使用にあたっては、お住まいの国および地域の電気安全規制を厳守してください。
- 本装置は接地された電源コンセントに接続してください。
- 感電の危険！保守作業前には全ての電源を切断してください。
- 回路ブレーカーをオフにした後、インレットのむき出しの金属接点に触れないでください。電気は依然として存在しています。
- ϟ は危険な通電状態を示し、端子に接続される外部配線は訓練を受けた者による設置が必要です。
- この機器は、子供がいる可能性のある場所での使用には適していません。
- 聴覚障害を防ぐため、長時間大音量で聴かないでください。
- すべての電子機器の操作は、お住まいの地域の電気安全規制、防火規制、およびその他の関連規制を厳守してください。
- 付属の電源アダプターをご使用ください。消費電力は規定値以上である必要があります。
- 複数の機器を1つの電源アダプターに接続しないでください。アダプターの過負荷により過熱や火災の危険が生じる可能性があります。
- 配線、設置、または分解を行う前に、必ず電源が切断されていることを確認してください。
  メンテナンスのため上蓋を開け、装置の電源を入れる場合は、必ず次のことを確認してください：
  1. 操作者が誤って負傷するのを防ぐため、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. メンテナンス後は、スイッチの配線順序が正しいことを確認してください。
- 配線、設置、または分解を行う前に、必ず電源が切断されていることを確認してください。
- 壁や天井に設置する場合、本装置は確実に固定してください。

- 煙、異臭、異音が装置から発生した場合は、直ちに電源を切り、電源ケーブルを抜いてください。その後、サービスセンターまでご連絡ください。
- 電池を飲み込まないでください。化学火傷の危険があります。
  本製品にはボタン電池が含まれています。ボタン電池を飲み込むと、わずか2時間で重度の内部やけどを引き起こし、死に至る可能性があります。
  新品および使用済みの電池は、子供の手の届かない場所に保管してください。電池ケースが確実に閉まらない場合は、製品の使用を中止し、子供から遠ざけてください。電池を飲み込んだ可能性や体内に挿入した可能性がある場合は、直ちに医師の診察を受けてください。
- 製品が正常に動作しない場合は、販売店または最寄りのサービスセンターにお問い合わせください。絶対に自分で分解しないでください。（無許可の修理やメンテナンスによる問題については、一切の責任を負いかねます。）

⚠注意事項:

- 本機器は水滴や飛沫にさらさないでください。また、花瓶などの液体入りの容器を機器の上に置かないでください。
- AC電源接続用の端子配線が正しいことを確認してください。
- 本装置は、必要に応じてIT配電システムへの接続用に設計・改造されています。
- + は、直流を使用する、または直流を生成する機器のプラス端子を示します。
  + は、直流を使用する、または直流を生成する機器のマイナス端子を示します。
- 点灯したろうそくなどの裸火を機器の上に置かないでください。
- 換気口を新聞紙、テーブルクロス、カーテンなどの物品で覆い、換気を妨げてはいけません。機器をベッド、ソファ、敷物、その他の同様の表面に置くことで、換気口を絶対に塞いではなりません。
- 本装置のシリアルポートはデバッグ専用です。
- ステンレス鋼は状況によっては腐食する可能性があります。ステンレス用クリーナーを使用して装置の清掃と手入れを行ってください。月1回の清掃が推奨されます。
- 装置を落下させたり物理的衝撃を与えたりせず、高電磁波放射環境に曝さないでください。振動面や衝撃を受ける場所への設置は避けてください（不注意による装置損傷の原因となります）。
- 極端な高温（詳細な動作温度は装置の仕様を参照）、低温、粉塵、湿気の多い場所に装置を置かないでください。また、強い電磁放射にさらさないでください。
- 屋内用カバーは雨や湿気を避けて保管してください。
- 機器を直射日光、換気の悪い場所、またはヒーターやラジエーターなどの熱源にさらすことは禁止されています（無知による火災の危険性があります）。
- 本装置を太陽や極端に明るい場所に向けてはいけません。そうすると、ブローム現象やスミアが発生する可能性があります（ただし、これは故障ではありません）。同時に、センサーの耐久性にも影響を与えます。
- 装置カバーを開ける際は付属の手袋を使用し、装置カバーへの直接接触を避けてください。指の酸性汗が装置カバーの表面コーティングを侵食する恐れがあります。

- 装置カバーの内外表面を清掃する際は、柔らかく乾いた布を使用し、アルカリ性洗剤は使用しないでください。
- 開封後は、将来の使用に備えすべての包装材を保管してください。故障が発生した場合、元の包装材と共に製品を工場へ返送する必要があります。元の包装材なしで輸送すると、製品が損傷し追加費用が発生する可能性があります。
- 電池の不適切な使用または交換は爆発の危険を招く恐れがあります。同種または同等品のみと交換してください。使用済み電池は電池メーカーの指示に従って廃棄してください。
- 生体認証製品は、100%の偽装防止環境を保証するものではありません。より高いセキュリティレベルが必要な場合は、複数の認証モードをご利用ください。
- デバイスが再起動中はレーン内に立ち入らないでください。
- 誤った種類の電池に交換すると爆発の危険があります。使用済み電池は指示に従って廃棄してください。
- コンクリートまたはその他の不燃性表面への取り付けにのみ適しています。
- 本機器の保護接地導体は、設置物の保護接地導体に接続すること。
- 切断装置のない恒久的に接続された装置の場合、接続された建物の電気設備には、容易にアクセス可能な切断装置（推奨定格電圧：400 VAC、極数：2極、定格電流：6 A）を組み込むこと。
- ポート67：デバイス内の統合DHCPサーバーのリスニングポートであり、無線端末がデバイスのホットスポットに接続する際にIPアドレスを割り当てるために使用されます。このポートは、デバイスのホットスポット機能が有効化されると有効になり、ホットスポット機能が無効化されると無効になります。
- ポート53: デバイス内の統合DNSサーバーのリスニングポートは、無線端末がデバイスにアクセスした際にドメイン名をデバイスのモバイルWebアドレスへリダイレクトするために使用されます。このポートは、デバイスのホットスポット機能が有効化されると有効になり、ホットスポット機能が無効化されると無効になります。
- ポート37020：デバイスのSADPサービスポートは、デバイスネットワーク検出およびネットワーク情報設定に使用されます。このポートは、デバイスのホットスポット機能が有効な場合に有効になり、無効な場合に無効になります。
- ポート443：本デバイスのHTTPSサーバーポートは、上位層プラットフォームがデバイスにアクセスするためのより安全な方法を提供し、デバイスパラメータの取得と設定を可能にします。このポートは、デバイスのホットスポット機能が有効化されている場合に有効となり、ホットスポット機能が無効化されると無効となります。

目次

第1章 システム配線

設置前の準備と一般的な配線。

手順

1. 左または右の台座の設置面に中心線を引きます。

2. 他の台座を設置するための平行線を引きます。

注記

最も近い2本の線間の距離はL+277 mmです。Lは車線幅を表します。

3. 取り付け面のスロット加工を行い、穴位置図に従って取り付け穴を掘削してください。

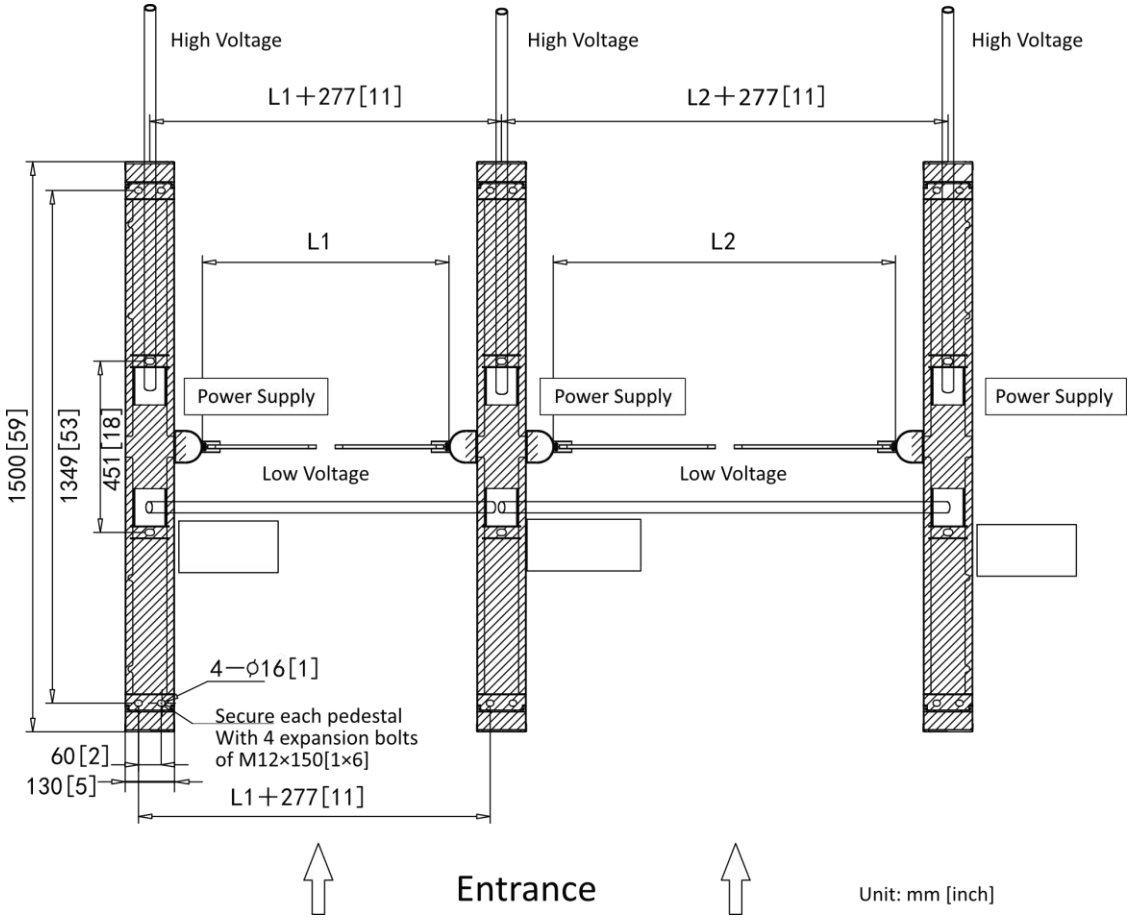


図1-1 穴位置図

4. ケーブルを埋設します。

注記

- 高電圧：200～240 VAC、50～60 Hz AC 電源入力。サイズ：3 × 1.0mm2、地面からの予備長：2.3 m。
- 低電圧：1 本のネットワーク通信ケーブル（3 m）。
- 低電圧用導管および高電圧（AC電源コード）用導管の内径は30mm以上とする。左側ペデスタルに高電力認証装置を設置する場合は、その導管の直径をさらに大きくすること。
- AC電源コードと低電圧ケーブルの両方を埋設する場合、干渉を避けるため、2本のケーブルは別々の導管に入れるべきである。
- 接続する周辺機器が増える場合は、導管の直径を大きくするか、外部ケーブル用に別の導管を埋設してください。
- 外部AC電源コードは二重絶縁であること。
- ネットワークケーブルはCAT5eまたはそれ以上の性能を持つケーブルを使用すること。
- 穴を掘る前に、設置面の厚さを評価し、貫通を避けること。

第2章 ペデスタルの設置

作業開始前に
設置工具の準備、装置と付属品の確認、設置基盤の清掃を行ってください。

手順

注意
- 装置は平坦な面に設置してください。設置基盤は硬質で、厚さはアンカーボルトの長さを超える必要があります。
- 設置作業およびその他の操作中は、装置の電源がオフになっていることを確認してください。
- 設置工具は台座のパッケージ内に収納されています。
- 設置時の汚れによるステンレスの錆を防ぐため、設置後は保護フィルムを剥がすことをお勧めします。
- フィルムの切断位置に接着剤の残留がある場合があります。フィルムを剥がした後、WD-40保護液で接着剤を拭き取ることをお勧めします。
- 屋内専用です。台座を水に浸さないでください。
- 設置場所が壁に近い場合、台座と壁の間の距離は20mm以上確保してください。そうしないと、装置の損傷や台座の上部パネルが開かなくなる恐れがあります。

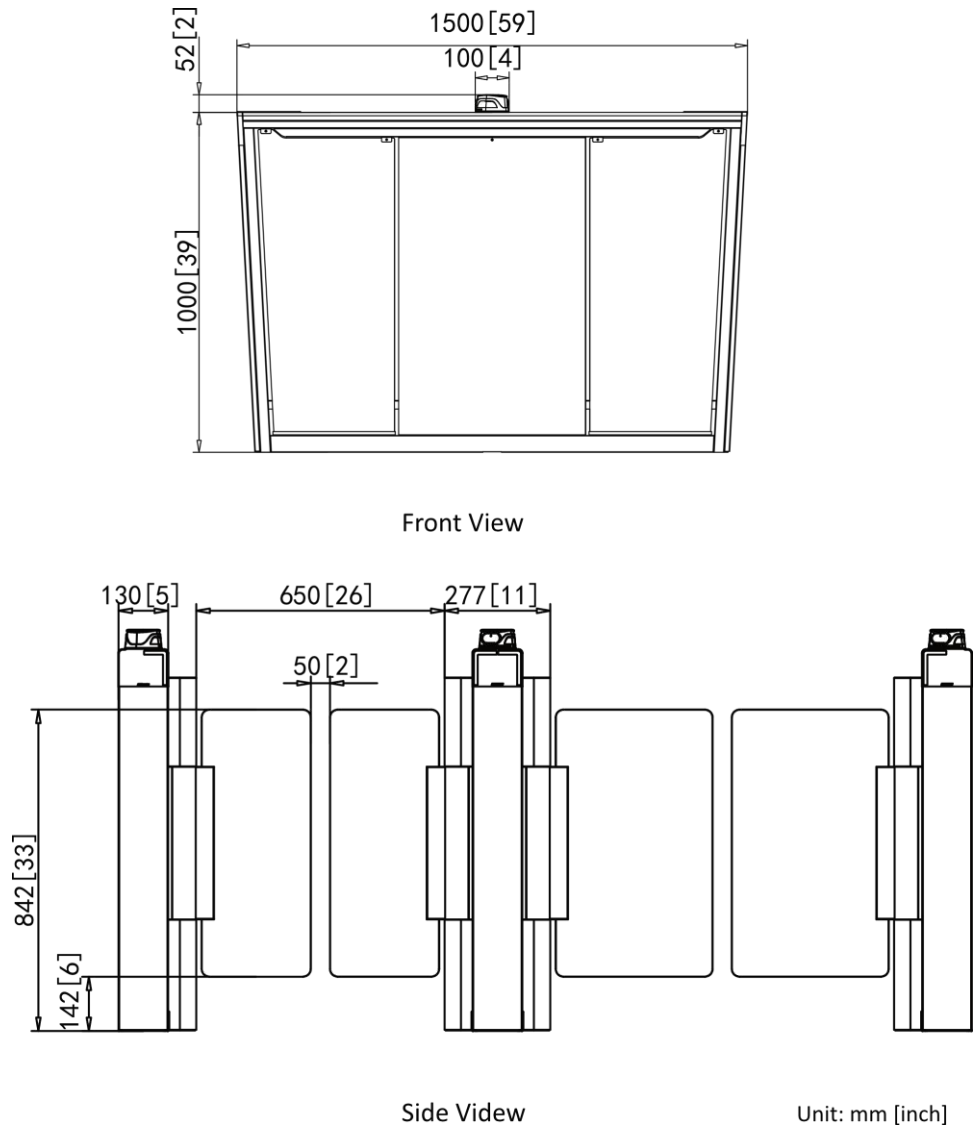


図2-1 寸法

1. 設置工具を準備し、部品を確認し、設置ベースを清掃してください。

2. 台座を事前に埋め込まれた拡張ボルトに合わせて位置合わせし、側面のメンテナンスドアを取り外します。

3. 各台座をアンカーボルトで固定し、メンテナンスドアを元の位置に固定します。

第3章 カードリーダーモジュールの取り付け（オプション）

デバイスにカードリーダーモジュールがインストールされていない場合、認証通過のためにターンスタイルにカードリーダーモジュールをインストールすることを選択できます。

手順

1. カバーを開けます。

2. 3本のネジ（M3-6）を使用して、カードリーダーをブラケットに固定します。

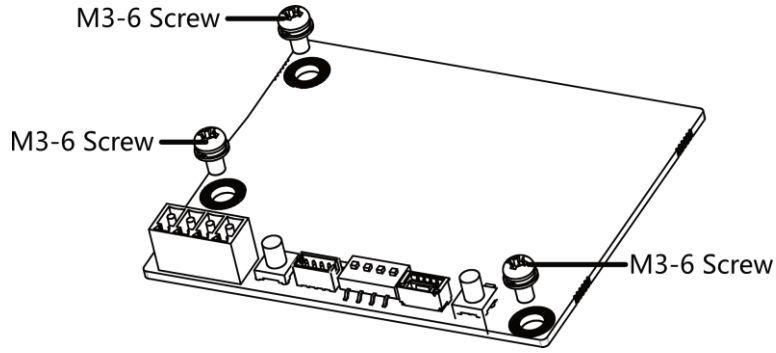


図 3-1 カードリーダーをブラケットに固定

3. 4本のネジでカードリーダーモジュールを所定の位置に取り付けます。

4. カバーにコイルを取り付ける。

5. カバーを元に戻します。

注記

画像はイメージです。実際の製品をご参照ください。

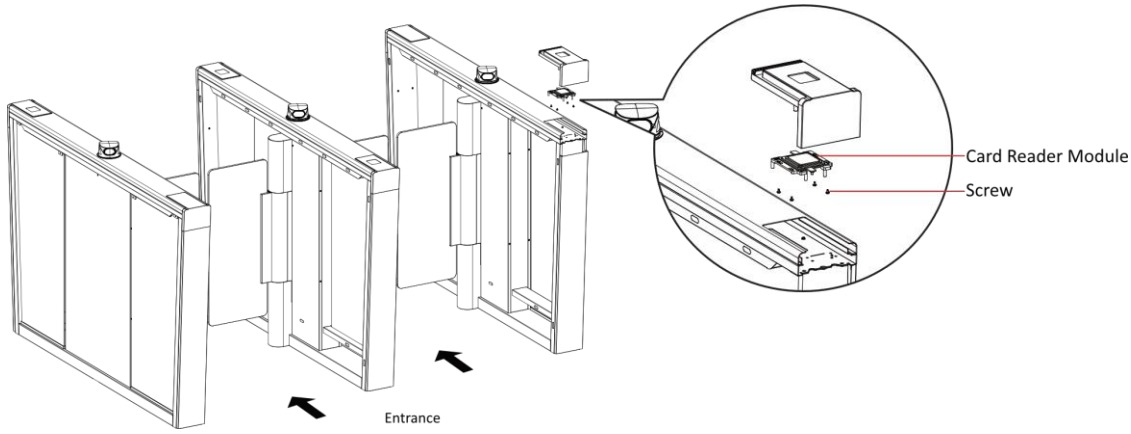


図3-2 カードリーダーモジュールの取り付け

第4章 サブ1Gモジュールの取り付け（オプション）

デバイスにサブ 1G モジュールがインストールされていない場合、NFC 認証用にターンスタイルにモジュールをインストールすることを選択できます。

手順

1. カバーを開けます。
2. サブ 1G モジュールを 4 本のネジで所定の位置に取り付けます。
3. カバーを元に戻します。

注記

画像はイメージです。実際の製品をご参照ください。

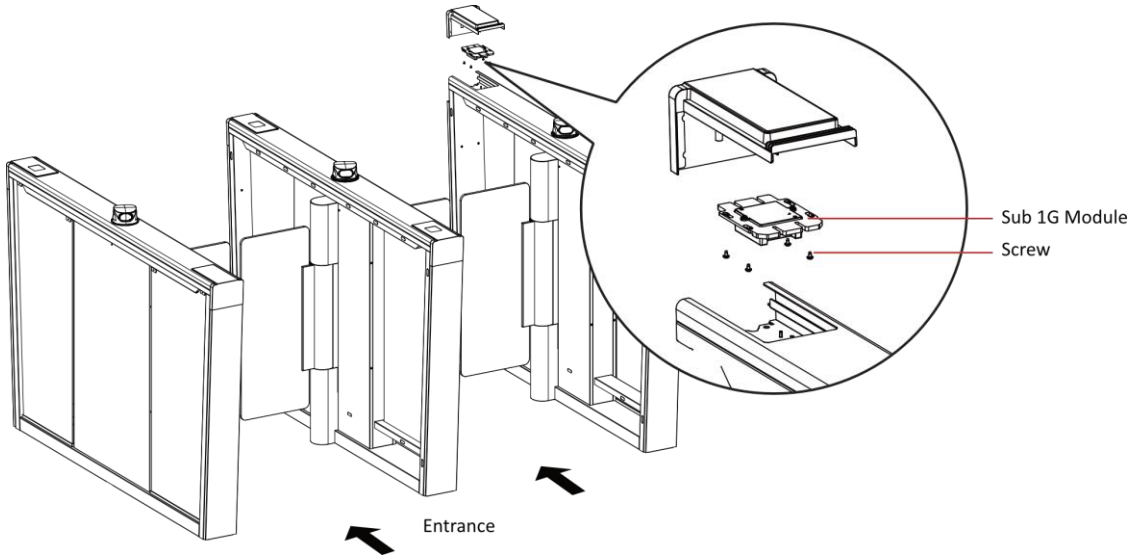


図4-1 サブ1Gモジュールのインストール

第5章 QRコードモジュールの取り付け（オプション）

QRコード認証用のモジュールがターンスタイルにインストールされていない場合、QRコード認証用のモジュールをインストールすることを選択できます。

手順

1. カバーを開けます。
2. QRコードモジュールを4本のネジで所定の位置に取り付けます。
3. カバーを元に戻します。

注意

画像はイメージです。実際の製品をご参照ください。

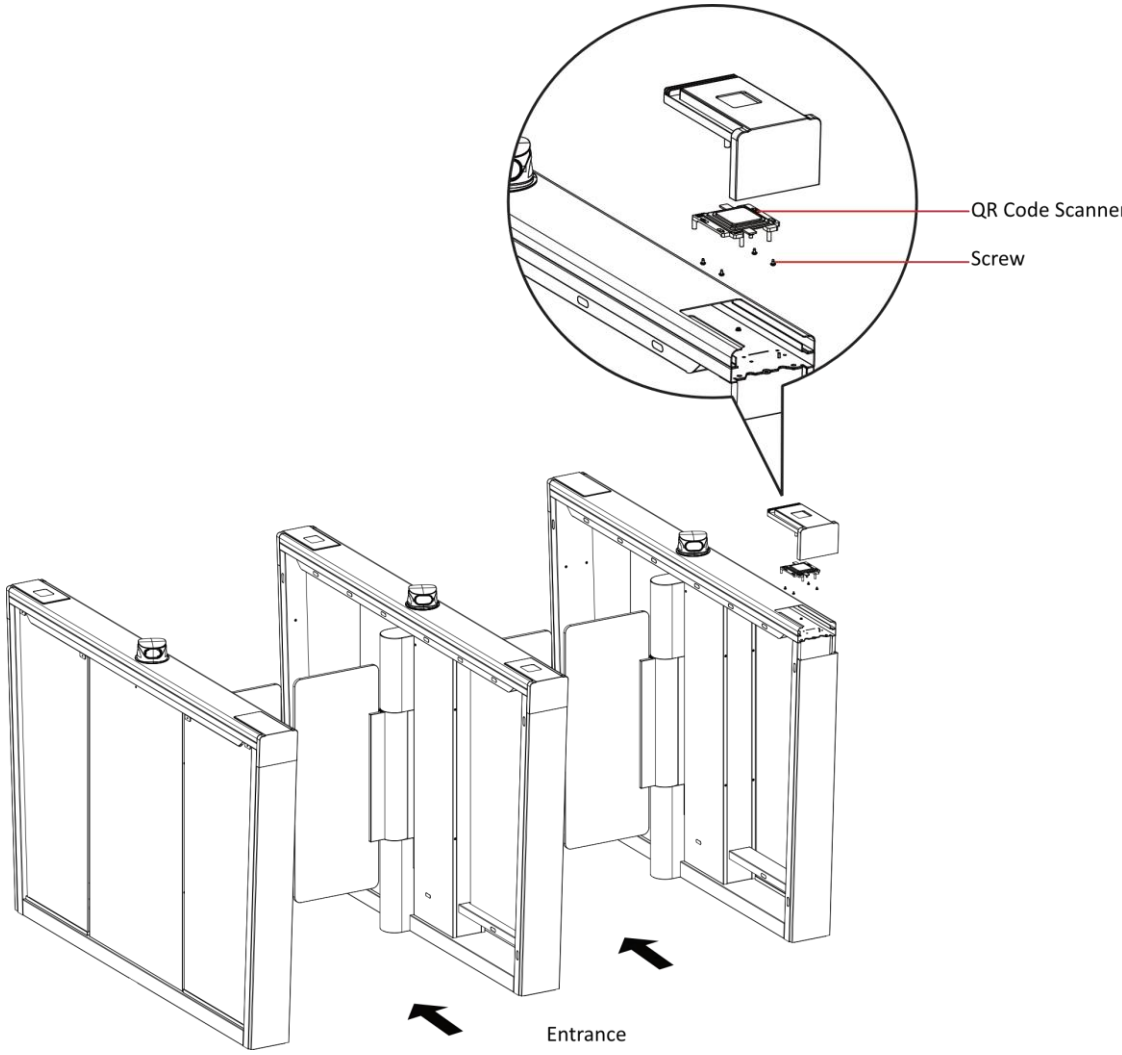


図5-1 QRコードモジュールのインストール

第6章 一般的な配線

注記

- 高電圧モジュールの保守または分解を行う際は、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保守作業を行ってください。保守作業前に周辺機器に接続されているケーブルを必ず抜いて、機器の損傷を防いでください。
- 高電圧モジュールを分解する際は、感電事故を防ぐため電源を切断してください。
- メンテナンスを伴わない配線作業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済みです。AC電源とスイッチ間を接続する14AWGケーブルは別途購入が必要です。

QRコードをスキャンして配線ガイド動画をご覧ください。

6.1 コンポーネント紹介

デフォルトでは、ターンスタイルの基本コンポーネントは適切に接続されています。ペデスタルは相互接続ケーブルを配線することで通信可能です。また、ターンスタイルはシステム全体の電源供給のためのAC電源配線をサポートしています。

注意

電源電圧の変動範囲は100VAC～220VAC、周波数50Hz～60Hzです。

下図は、ターンスタイル上の各コンポーネントの位置を示しています。

注記

この図は参考用です。

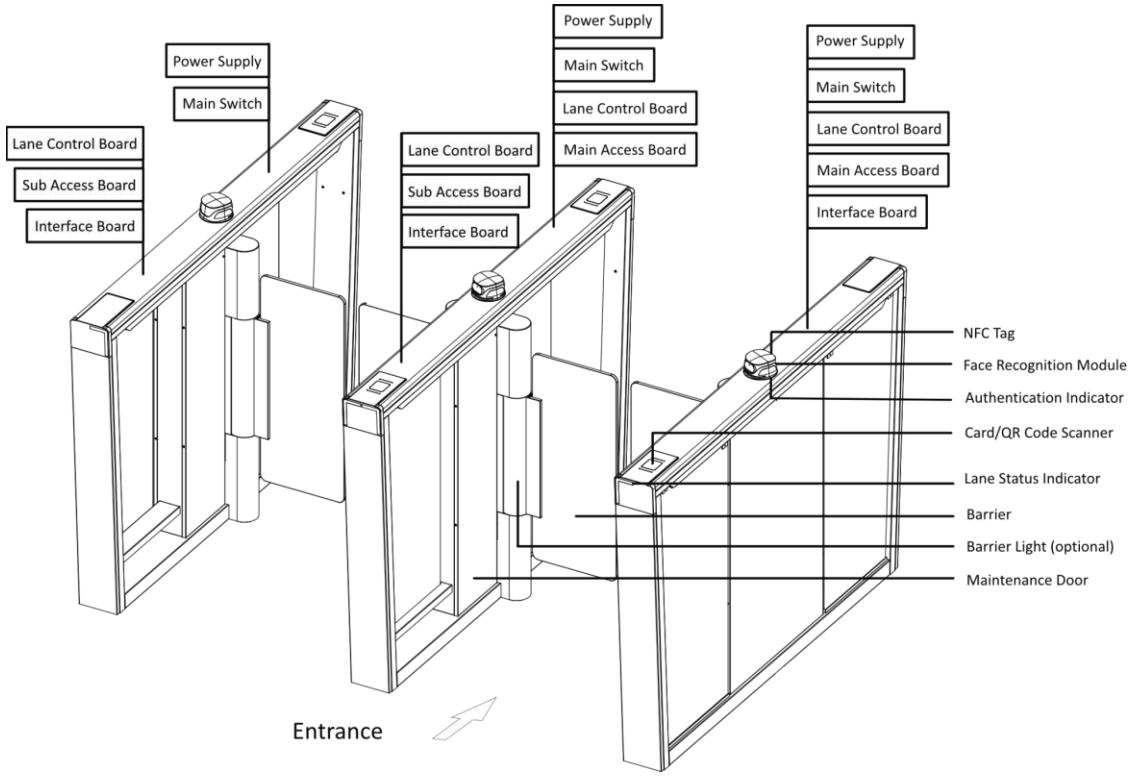
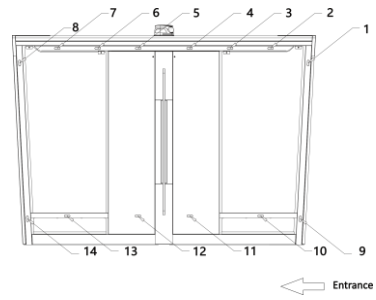
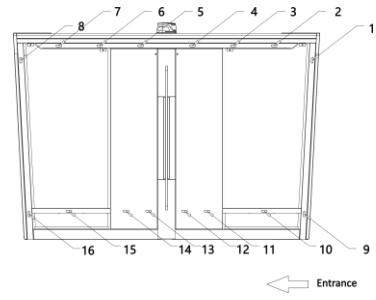


図 6-1 部品図

以下の図は、IRモジュールと台座上の対応する番号を示しています。





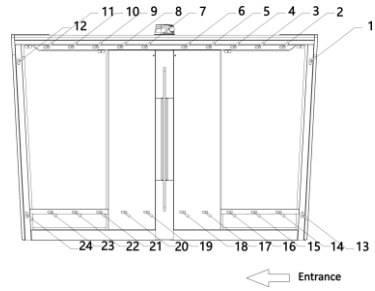


図6-2 IRモジュール

6.2 配線 電源供給

ペデスタル内のスイッチに電源を配線します。端子Lと端子Nはスイッチに接続され、端子PEは接地線（黄緑色線）に接続する必要があります。

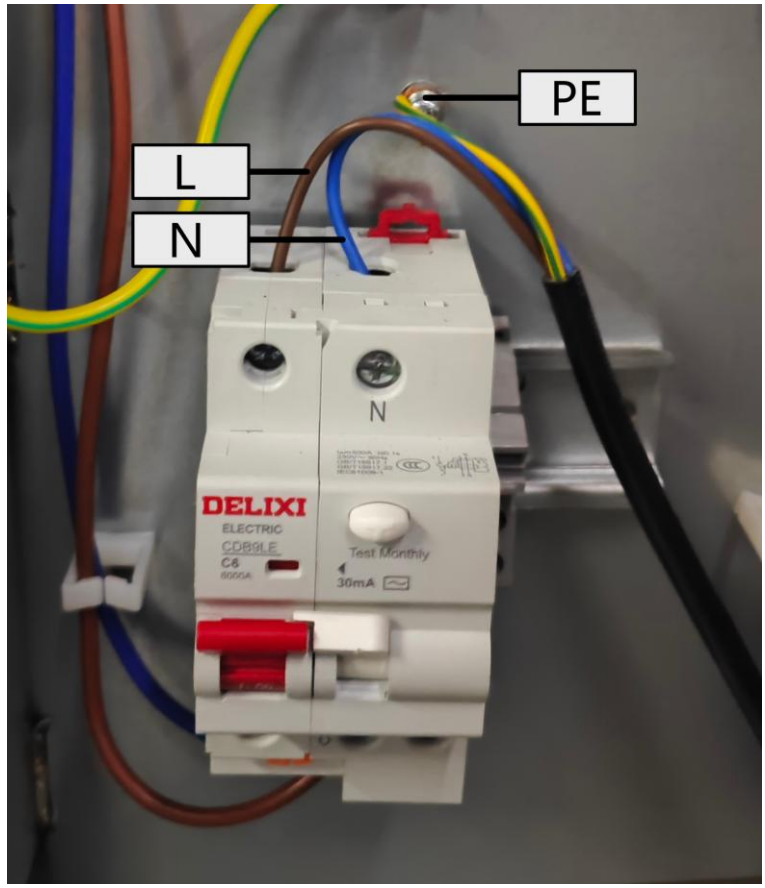


図6-3 電源配線

注意

人身事故や機器損傷を防ぐため、PE端子は必ず接地してください。

注

- ケーブルの露出部分は8mmを超えてはいけません。可能であれば、露出ケーブルの先端に絶縁キャップを装着してください。配線後は露出銅線やケーブルがないことを確認してください。
- 端子Lと端子Nは逆接続できません。入力端子と出力端子を逆接続しないでください。
- 人身事故や機器損傷を防ぐため、試験時には等電位点の接地抵抗が2Ωを超えてはいけません。
- 本装置はUPSと併用してください。
- 接地ケーブルが引き剥がされた際の負傷を防ぐため、接地配線用ケーブルは高電圧ケーブルよりも長くする必要があります。

6.3 UART説明

カードリーダー、QRコードスキャナー、顔認識モジュールなどをデバイスに搭載しない場合、予備のUARTを使用して配線できます。

次の図は、UART の位置を示しています。

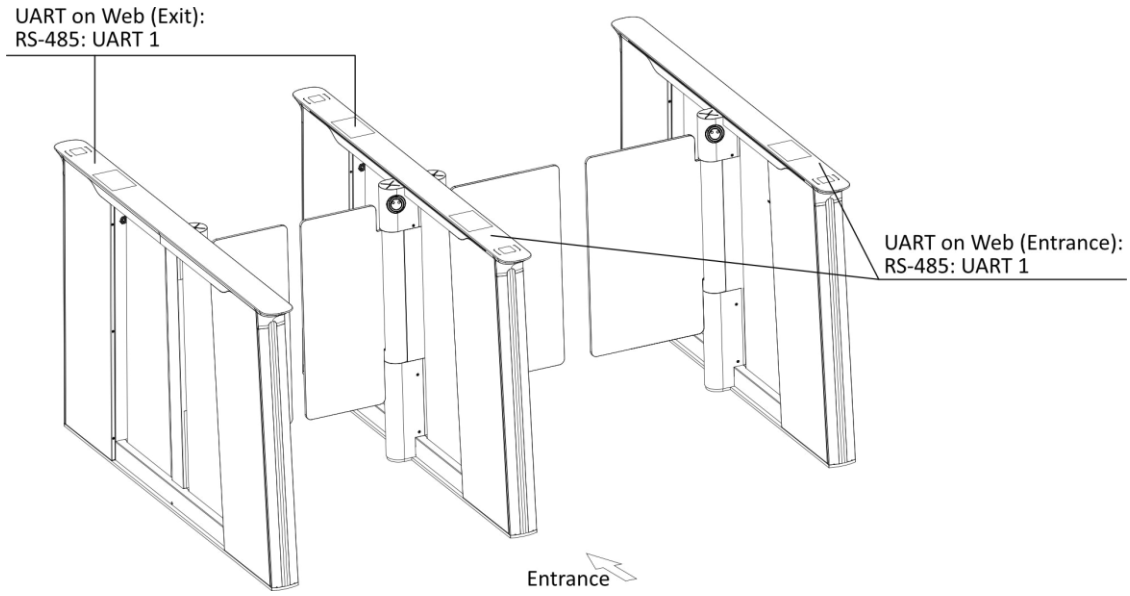


図 6-4 UART の説明

第 7 章 端子の説明

7.1 一般的な配線

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

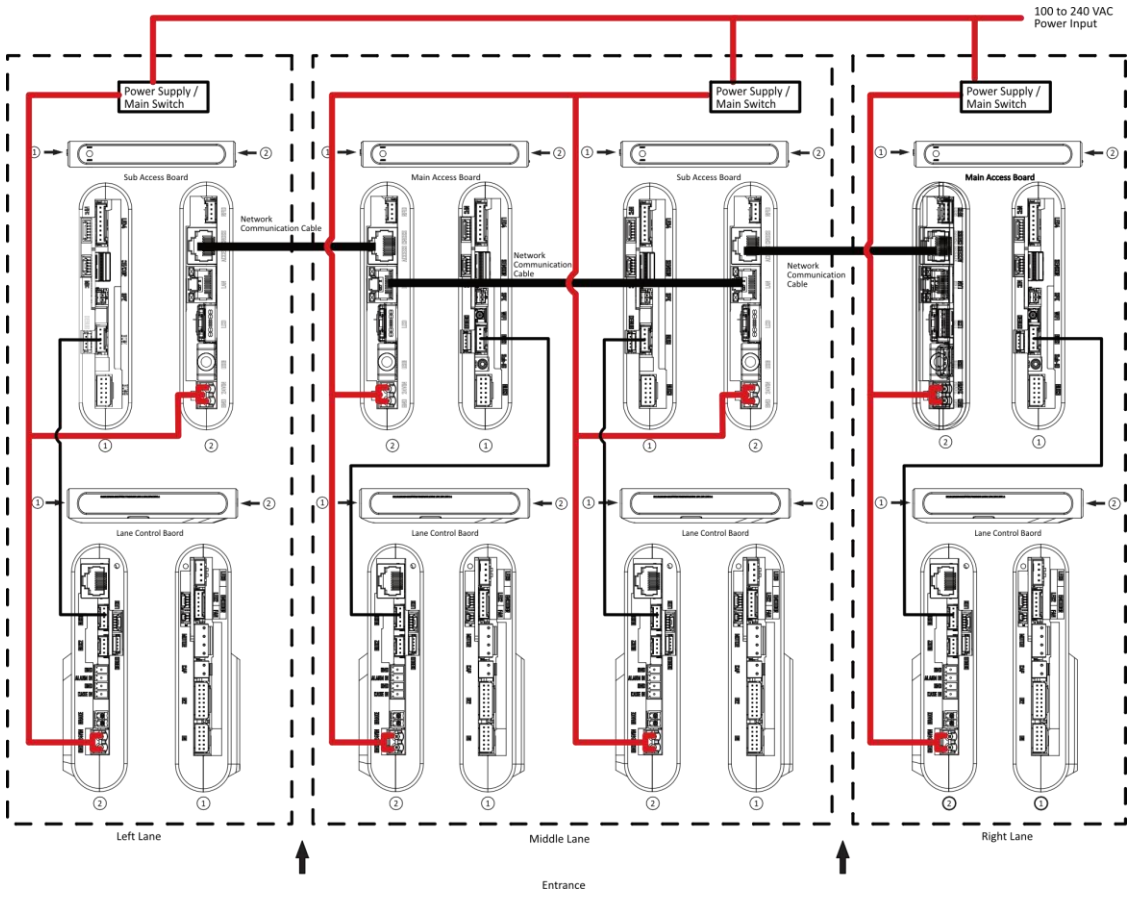


図7-1 一般的な配線

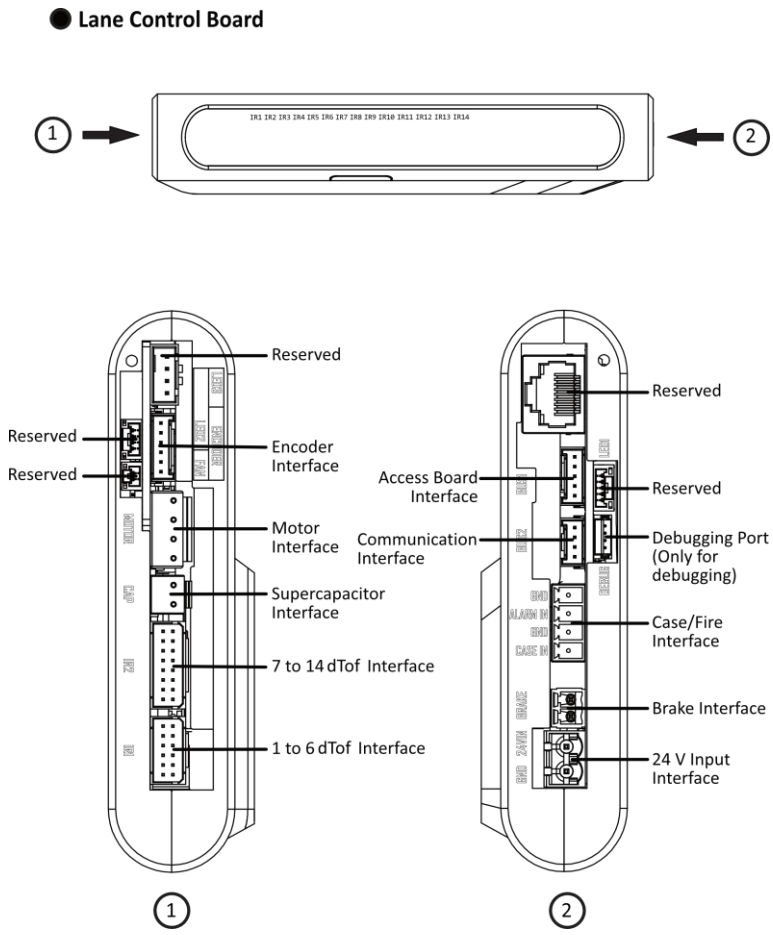
注記

- 電源からメインレーン制御基板への電源ケーブルは接続済みです。AC電源入力から電源装置へ接続するための14AWG電源ケーブルを準備する必要があります。
- 入口/出口でバリアが開く場合：BTN1/BTN2とGNDに接続してください。

7.2 メイン制御基板端子説明

下図はメイン制御基板の配線図です。

● Lane Control Board



注記

- 通信インターフェースは IR アダプタに接続できます。15 から 24 IR を IR アダプタに接続できます。
- 赤外線アダプターは、16および24個の赤外線センサーで構成されたスイングバリア向けに提供されます。
- ケース/火災インターフェースによりドアの開放が可能。

7.3 アクセスボード

アクセスボードは、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。

注記

デスタルのメインアクセスボードのみにSUB-1Gアンテナインターフェースが搭載されています。中央アクセスボードにはSUB-1Gアンテナインターフェースはありません。

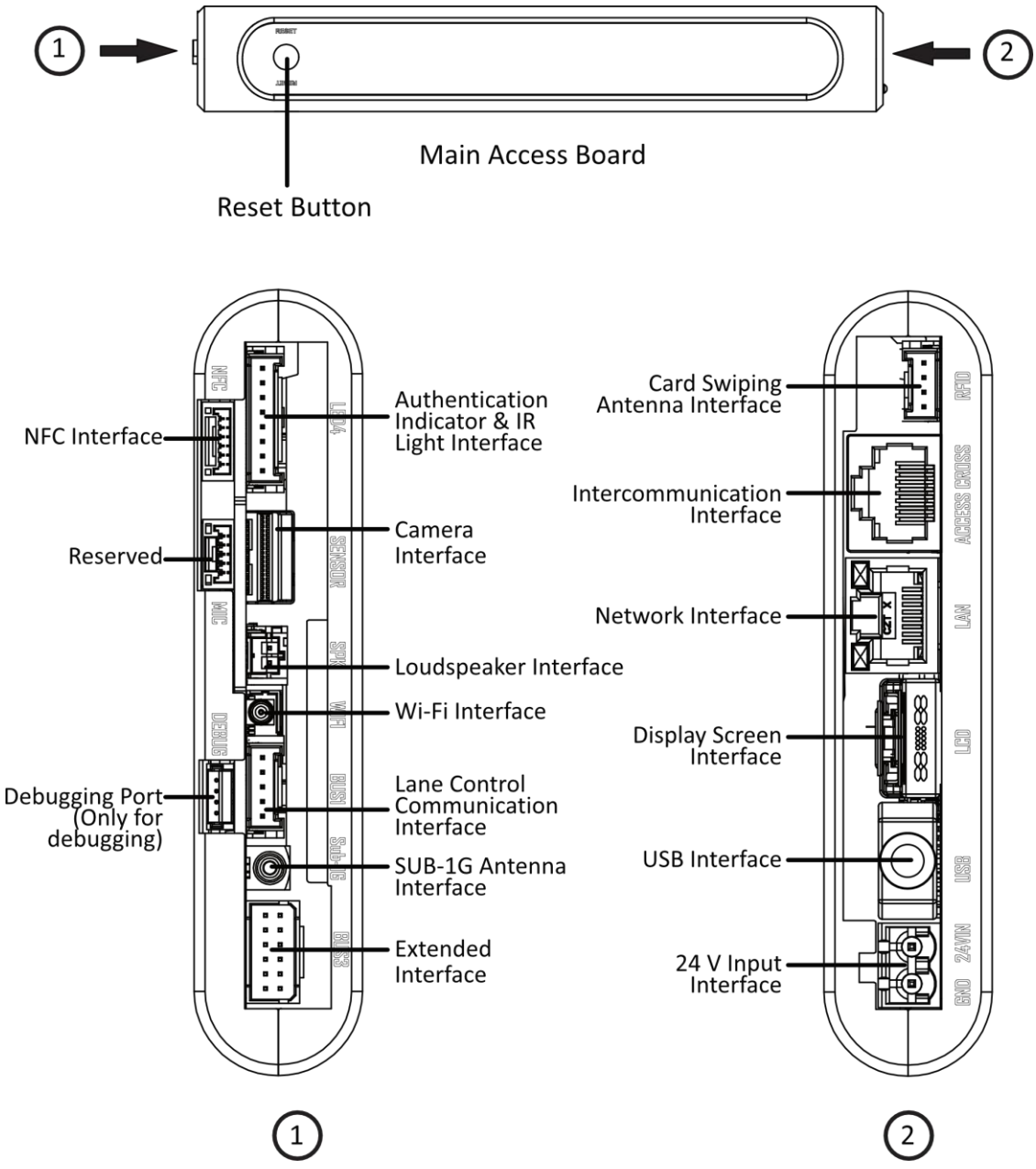


図7-2 メインアクセスボード

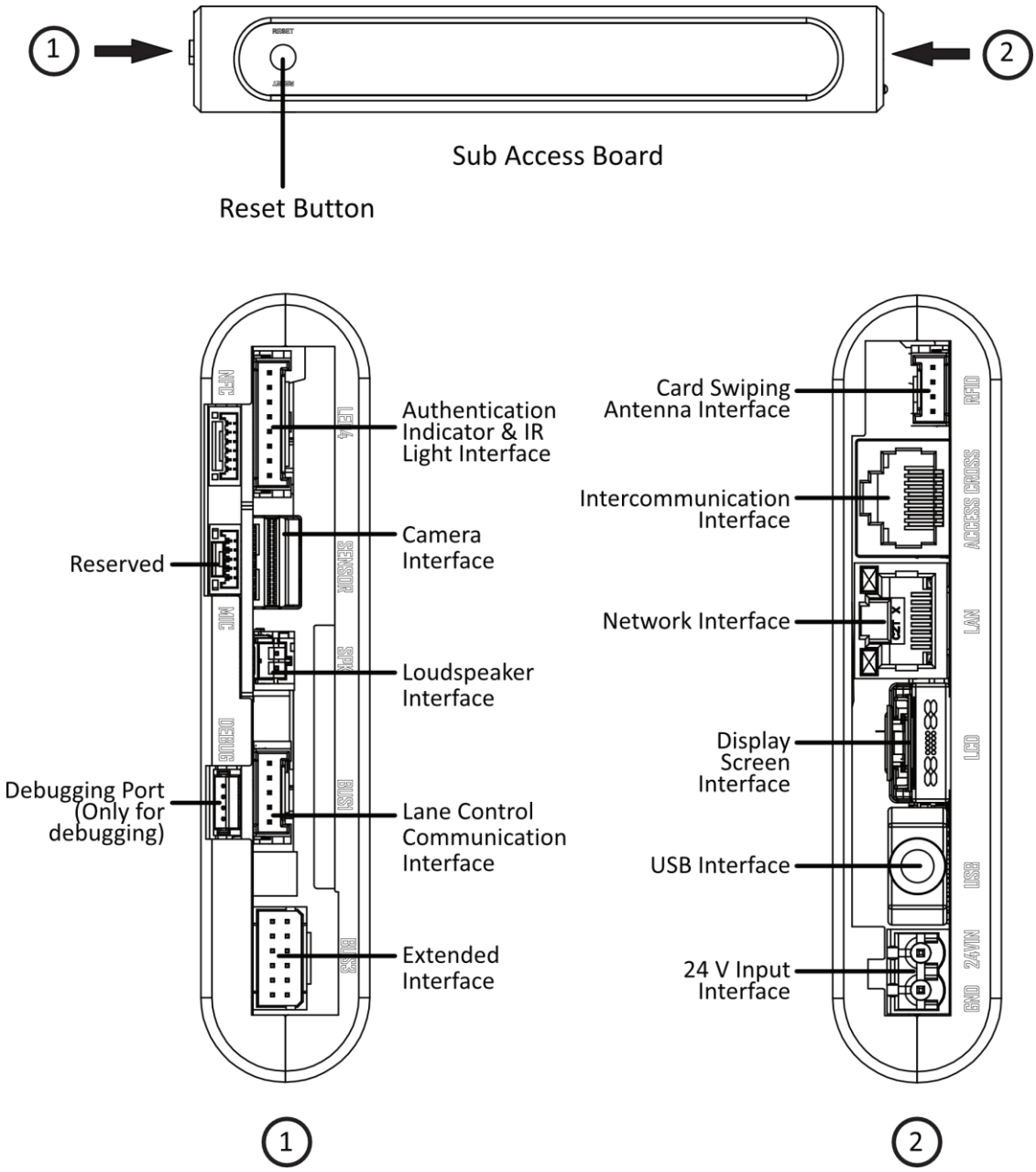


図7-3 サブアクセスボード

アクセスボードの拡張インターフェースの配線図を以下に示す。

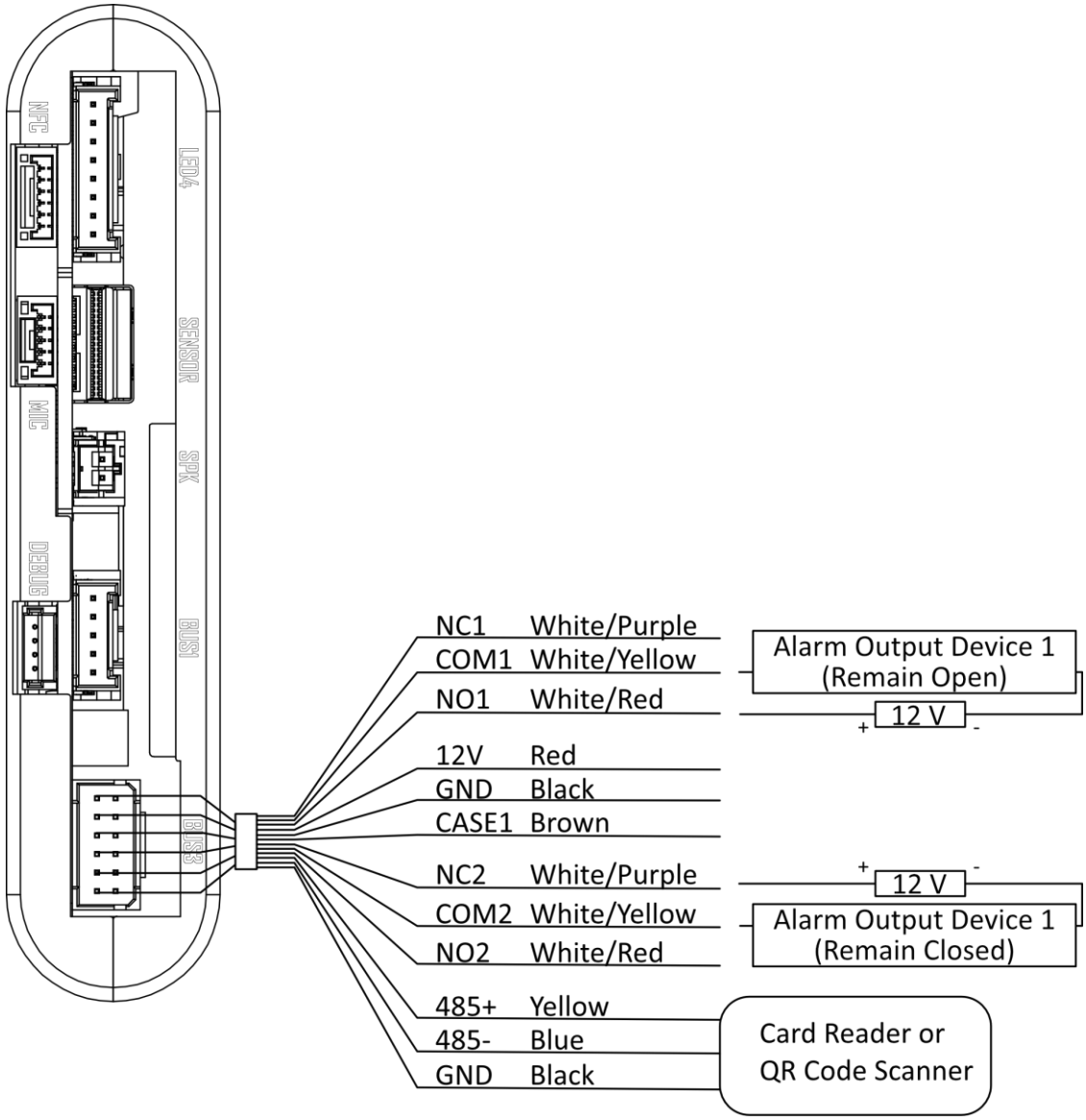


図7-4 BUS3インターフェースの配線図

7.4 インターフェースボードの説明

本インターフェースボードは、カード受信機、カードリーダー、QRコードスキャナー、人流計測モジュールなどを接続可能です。

インターフェースボードは下記の通りです：

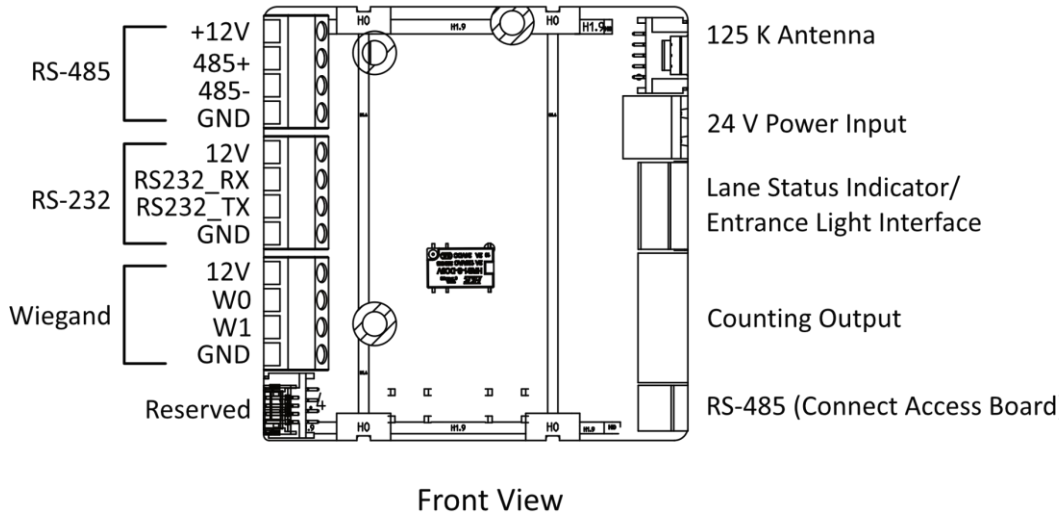


図7-5 インターフェースボード（前面）

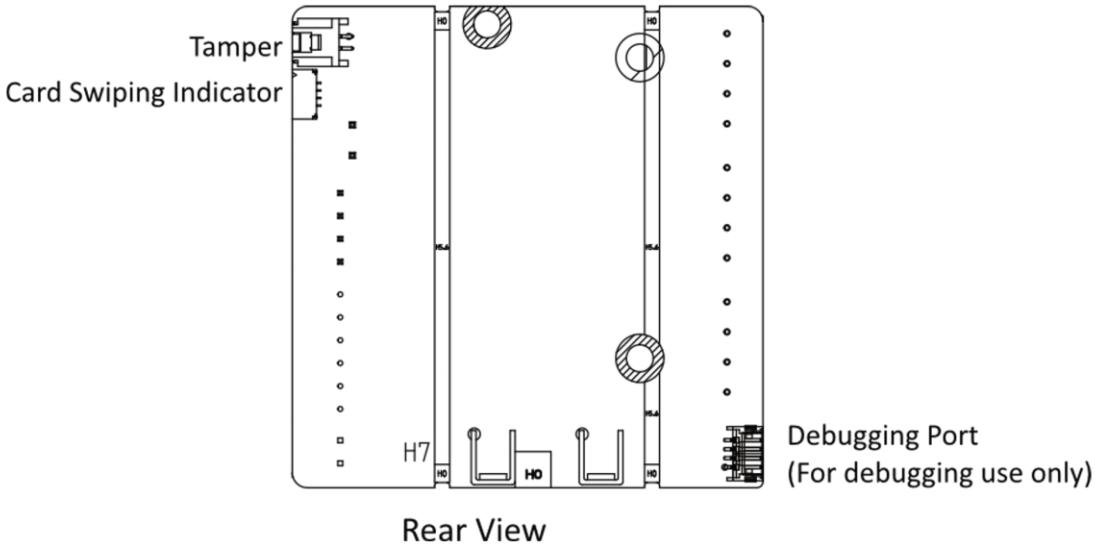


図7-6 インターフェースボード（背面）

7.5 カードリーダーモジュール配線（オプション）

カードリーダーモジュールは、RS-485インターフェースを介してアクセス制御ボードまたはインターフェースボードに接続できます。

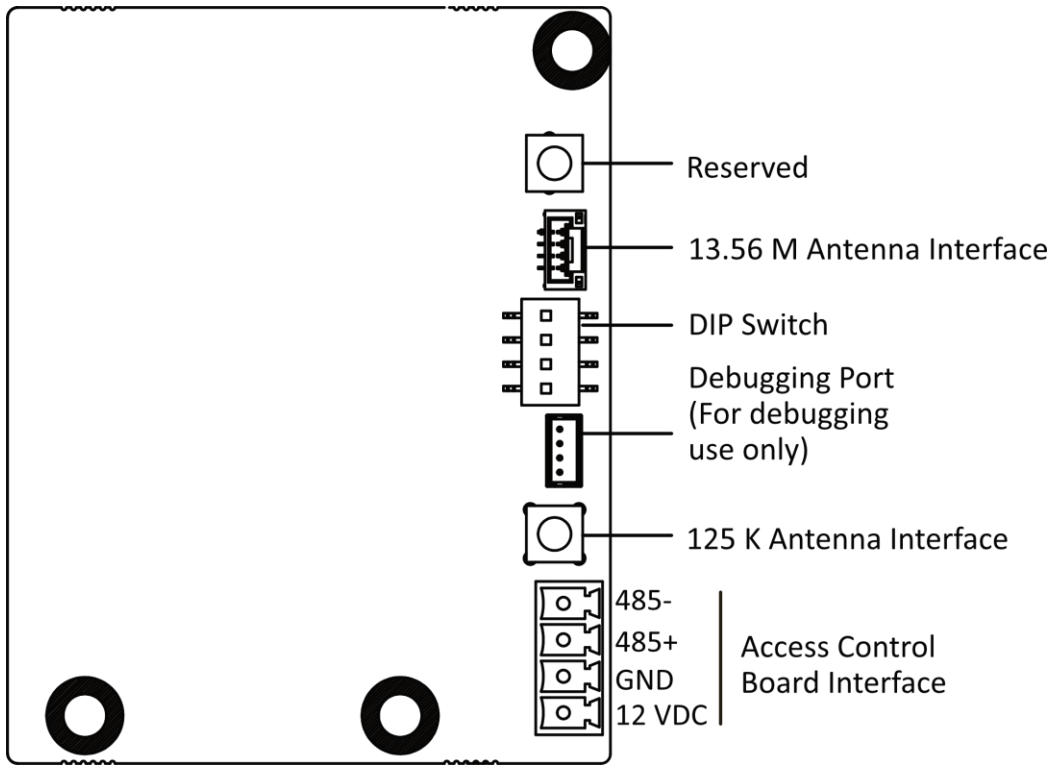


図7-7 カードリーダーモジュール

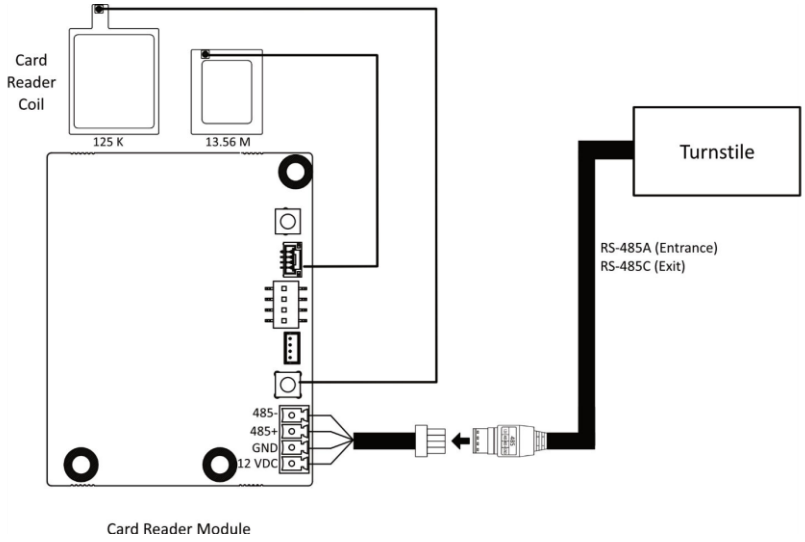


図7-8 配線図（RS-485付き）

注記

- この配線は参考用です。異なるターンスタイルでは、接続インターフェースが異なります。
- RS-485パラメータは設定できません。デフォルトでは、通信ビットレートは19200、データビットは8、ストップビットは1、奇数偶数チェックはなしです。

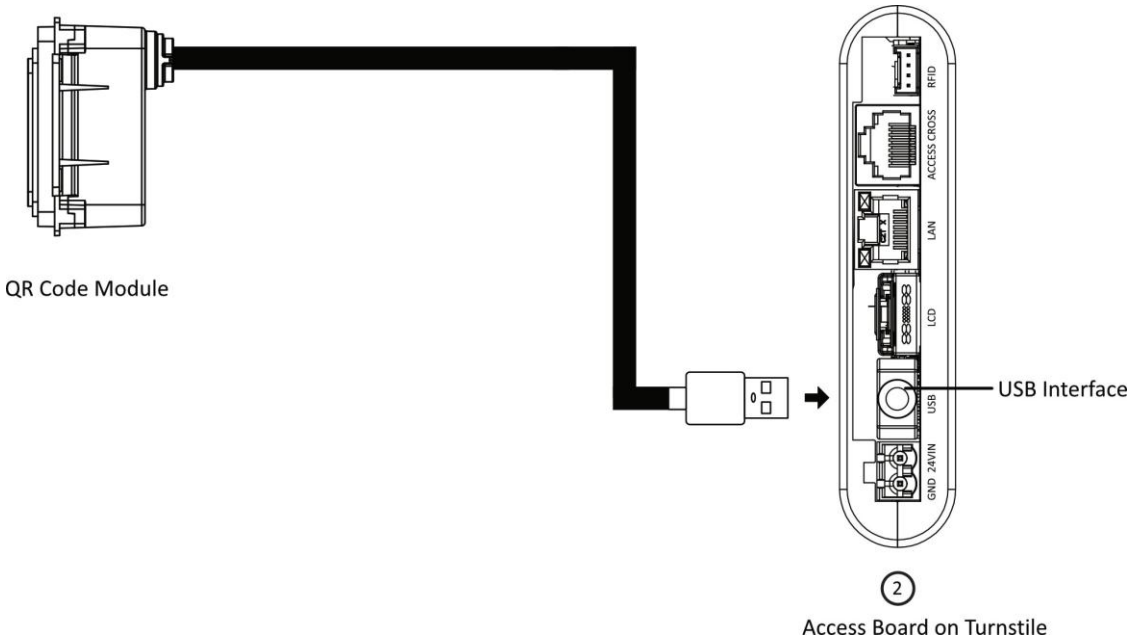


図 7-9 配線図（RS-485 付き）

注意

こちらの配線は参考用です。異なるターンスタイルでは接続インターフェースが異なります。

7.6 サブ1Gモジュール配線（オプション）

サブ1Gモジュールはレーン制御ボードに接続可能です。

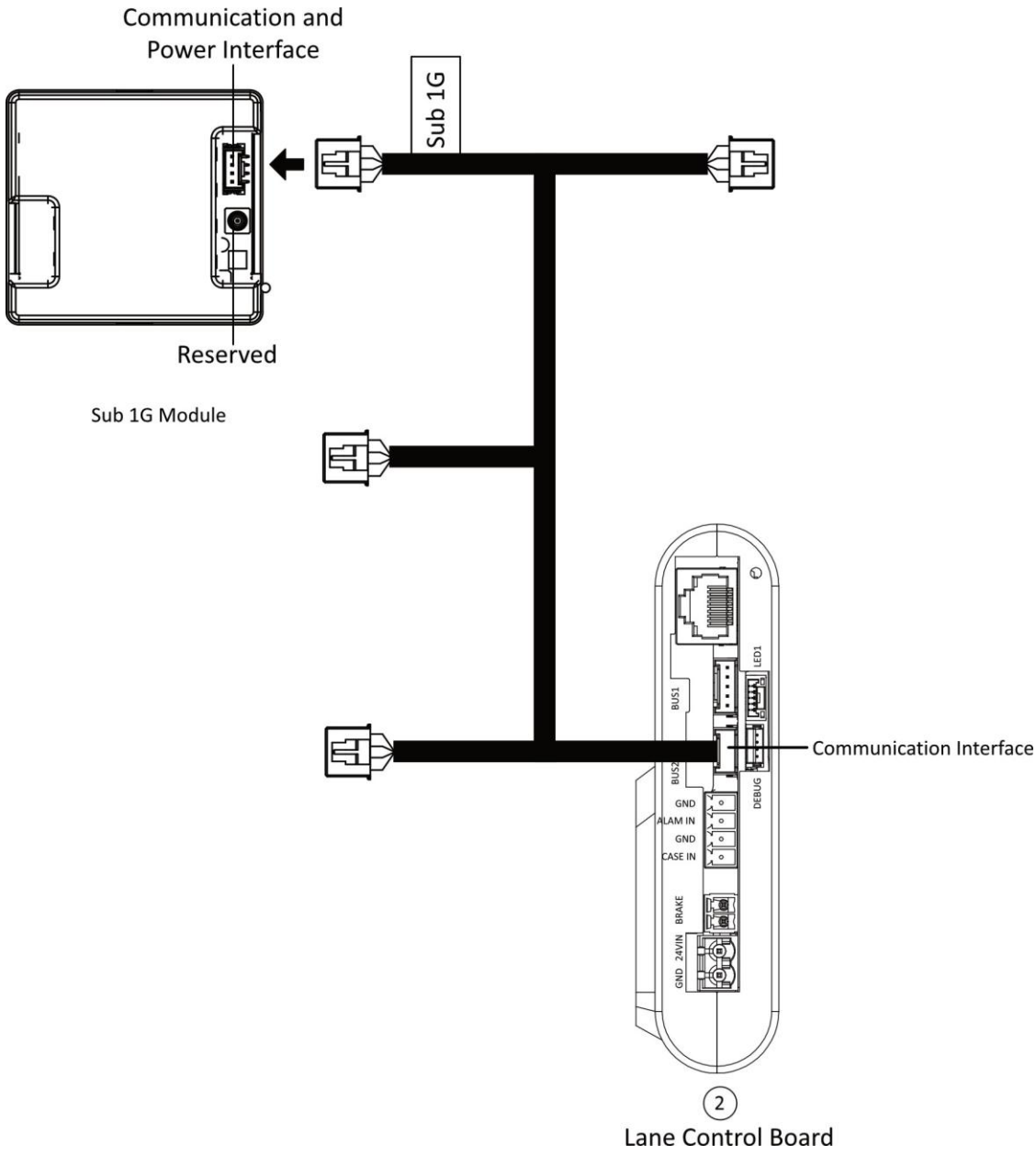


図 7-10 サブ 1G モジュール配線

7.7 QRコードモジュール配線

QRコードモジュールは、RS-485インターフェースを介してアクセス制御ボードまたはインターフェースボードに接続できます。

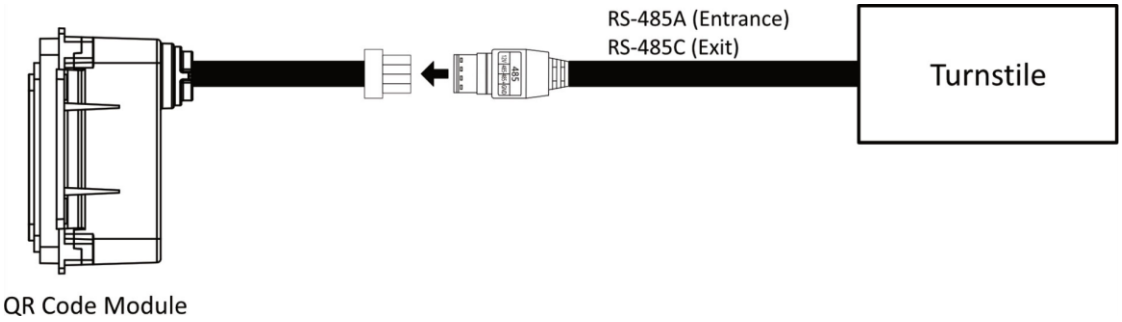


図 7-11 QR コードモジュールの配線（RS-485 付き）

注記

- こちらの配線は参考用です。異なるターンスタイルでは接続インターフェースが異なります。
- RS-485パラメータは設定不可です。デフォルトでは、通信ビットレートは19200、データビットは8、ストップビットは1、奇数偶数チェックなしです。

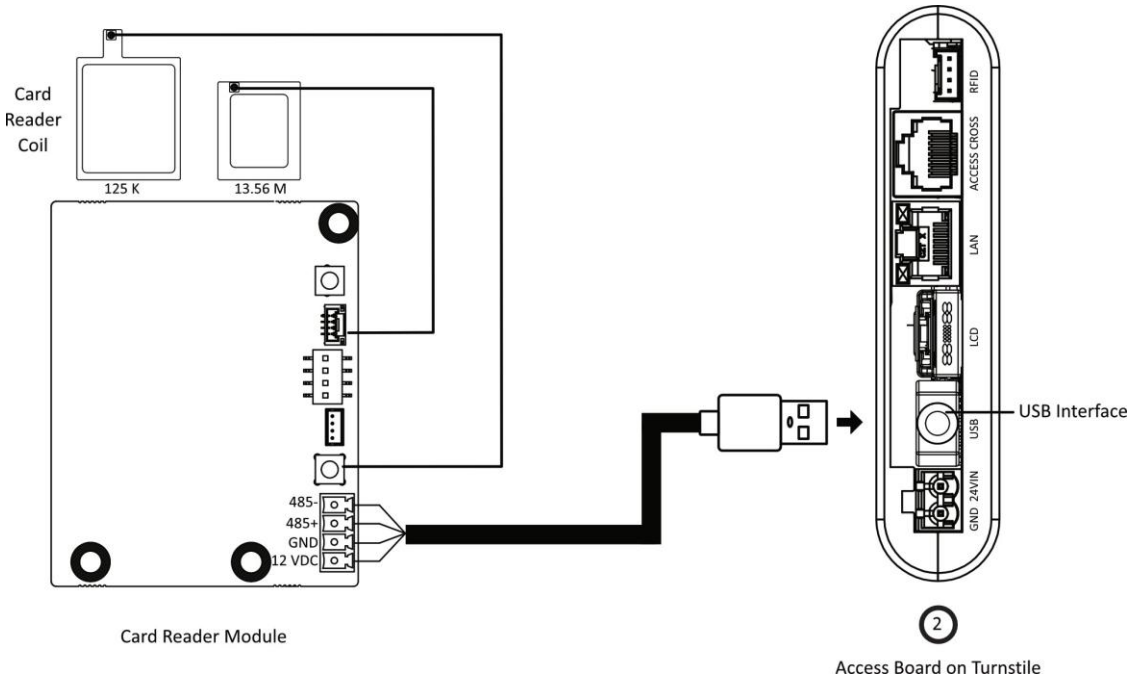


図7-12 QRコードモジュール配線（USB付き）

注意

ここでの配線は参考用です。異なるターンスタイルでは接続インターフェースが異なります。

7.8 インジケータボード

インジケータボードを確認してください。

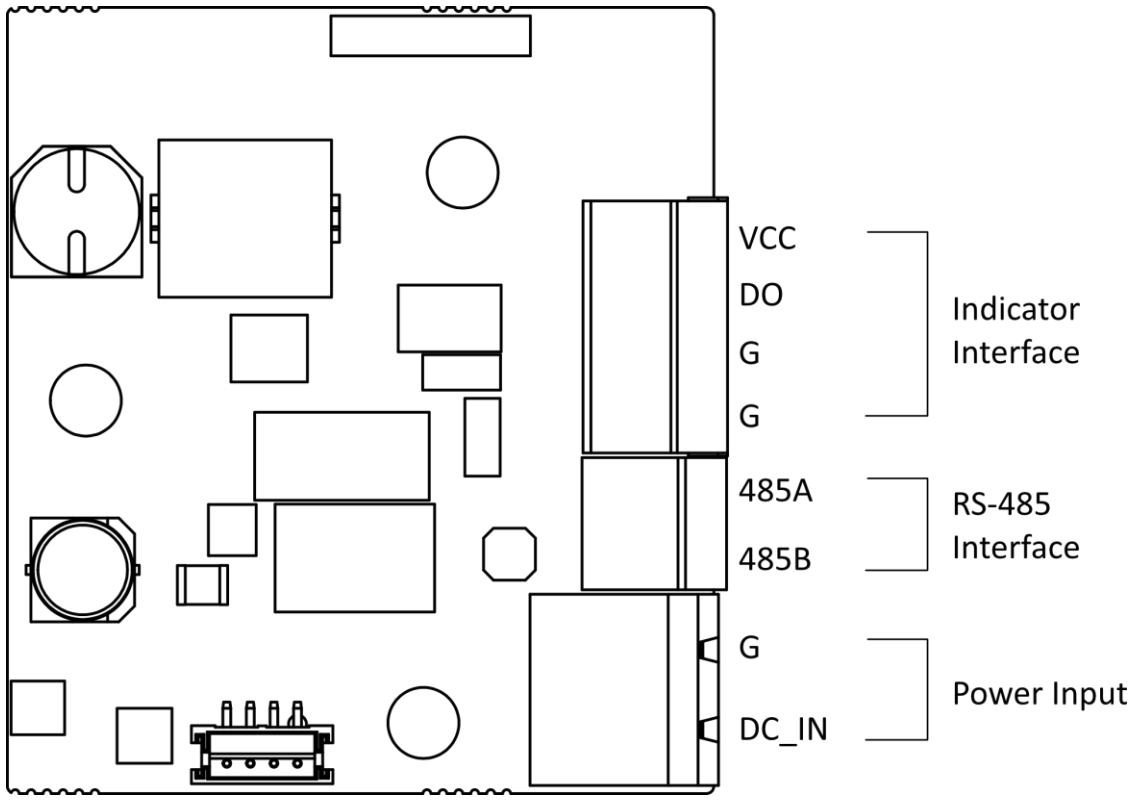


図 7-13 表示ボード

7.9 カメラボード

カメラボードを見る。

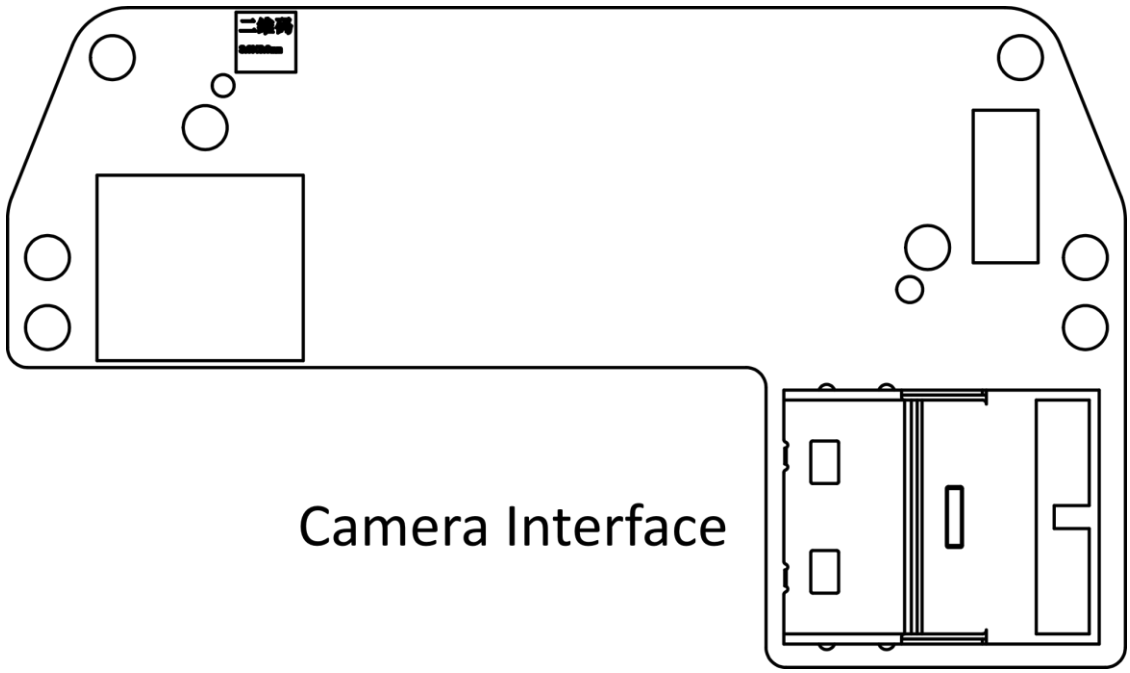


図 7-14 カメラボード

7.10 警報入力配線

レーン制御基板上で、火災警報入力インターフェースを配線できます。

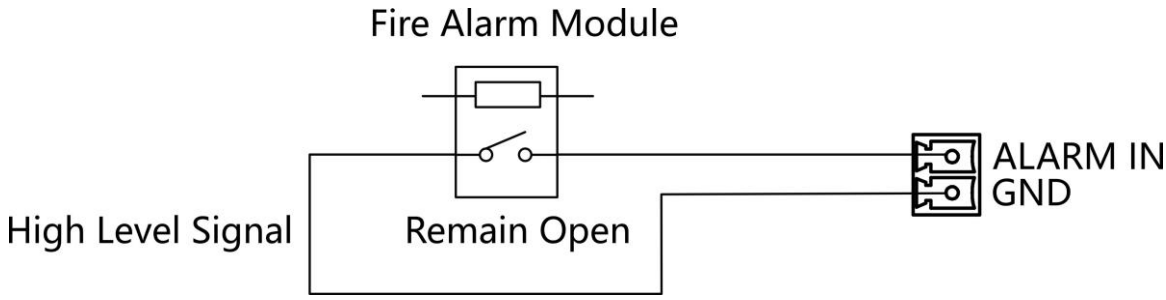


図7-15 残りの開放

7.11 退出ボタン配線

退出ボタンの配線図を表示できます。

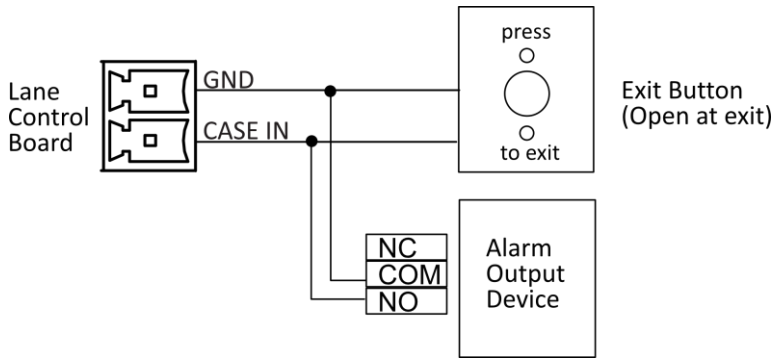


図 7-16 退出ボタン配線

第8章 リセット装置

手順

1. リセットボタンを押したままにします。

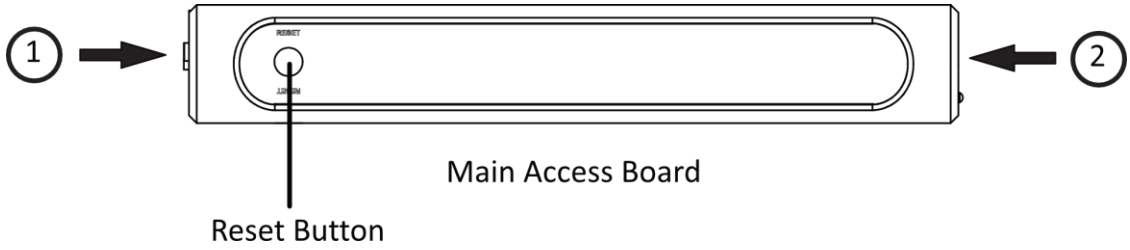


図 8-1 初期化リセット位置

2. リセットボタンを 5 秒間押し続けると、デバイスが 2 回ビープ音を鳴らし（メインアクセスボードのみ）、工場出荷時の設定への復元を開始します。

注意
デバイスの初期化により、すべてのパラメータがデフォルト設定に復元され、すべてのデバイスイベントが削除されます。

注意
デバイスの電源投入時には、レーン内に人がいないことを確認してください。リセッ

トが完了しました。

第 9 章 ライトの説明

レーン状態インジケータ

サイドライトは、誘導、通行禁止、認証済み通行など、レーンのさまざまなステータスを示します。

注意スが1.5m以内に人を検知すると、サイドライトが点滅します。

- 右側のライトのみが車線状態を示します。
- 青色のまま：通行可能
- ライトが緑のまま：認証済み通行
- 赤点灯：通行禁止

バリアライト

バリアライトはデフォルトで白色です。バリアライトの色は必要に応じて設定できます。バリアライトは車線状態や認証結果に応じて色が変わることはありません。

認証インジケーター

カードライトは、デバイスが人の接近を検知してからその人が通過するまで白色で点灯します。

第10章 作動

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

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

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

10.1 Webブラウザ経由でのアクティベーション

Webブラウザ経由でデバイスをアクティベートできます。

手順

1. ウェブブラウザのアドレスバーにデバイスのデフォルトIPアドレス（192.0.0.64）を入力し、Enterキーを押してください。

Enterキーを押します。

注

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

2. 新しいパスワード（管理者パスワード）を作成し、パスワードを確認します。

注意

- デバイスのパスワード強度を自動的に確認できます。製品のセキュリティ強化のため、ご自身で選択したパスワード（8文字以上で、大文字、小文字、数字、特殊文字の少なくとも3種類を含む）への変更を強く推奨します。また、特に高セキュリティシステムでは、パスワードを定期的に変更することを推奨します。月次または週次での変更により、製品をより効果的に保護できます。
- すべてのパスワードおよびその他のセキュリティ設定の適切な構成は、サービスプロバイダーおよび / またはエンドユーザーの責任です。
- パスワードには以下の文字を含めないでください：ユーザー名、123、admin（大文字小文字を区別しない）、4つ以上の連続した昇順または降順の数字、4つ以上の連続した繰り返し文字。
- パスワードには、hik、hkws、hikvision などの単語を含めることはできません（大文字と小文字は区別されません）。

3. **「有効化」**をクリックします。

4. デバイスのIPアドレスを編集します。IPアドレスはSADPツール、デバイス本体、クライアントソフトウェアから編集できます。

10.2 モバイルWeb経由でアクティベート

モバイルWeb経由でデバイスをアクティベートできます。

手順

1. デバイスのホットスポットが無効の場合：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、デバイスのIPアドレスが表示されます。アドレスをタップしてログインページに移動します。
2. デバイスのホットスポットが有効な場合：
   - Androidシステムの場合：スマートフォンをNFCエリアに置くと、デバイスのホットスポット名とパスワードが自動的に取得されます。接続を確認すると、ログインページに移動します。
   - iOSシステム：スマートフォンのWi-Fi機能を有効にし、現在のデバイスのホットスポットに接続してください。ホットスポット接続後、ログインページが表示されます。

注意

- ホットスポット名：AP_シリアル番号
- ホットスポットパスワード：デバイスのシリアル番号

ご注意

強力なパスワードの使用を推奨 - 製品のセキュリティを強化するため、お客様自身で選択した強力なパスワード（大文字、小文字、数字、特殊文字を含む8文字以上）を作成することを強く推奨します。また、特に高セキュリティシステムでは、パスワードを定期的にリセットすることを推奨します。毎月または毎週パスワードをリセットすることで、製品をより効果的に保護できます。

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。

3. 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

強力なパスワードの使用を推奨 - 製品のセキュリティを強化するため、ご自身で選択した強力なパスワード（大文字、小文字、数字、特殊文字を含む 8 文字以上）を作成することを強くお勧めします。また、特にセキュリティレベルの高いシステムでは、パスワードを定期的にリセットすることをお勧めします。毎月または毎週パスワードを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。

4. **アクティベート**をクリックしてください。
5. ターンスタイルの基本パラメータ、キーフォブ設定、照明設定、ネットワーク設定、アクセス制御設定などを設定できます。

10.3 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、変更するためのツールです。

開始前に

- 付属ディスクまたは公式ウェブサイト *http://www.hikvision.com/en/* から SADP ソフトウェアを入手し、指示に従って SADP をインストールしてください。
- SADP ツールを実行する PC とデバイスは、同じサブネット内に存在し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。一括アクティベーションおよびIPアドレス変更の詳細については、*SADPユーザーマニュアル*を参照してください。

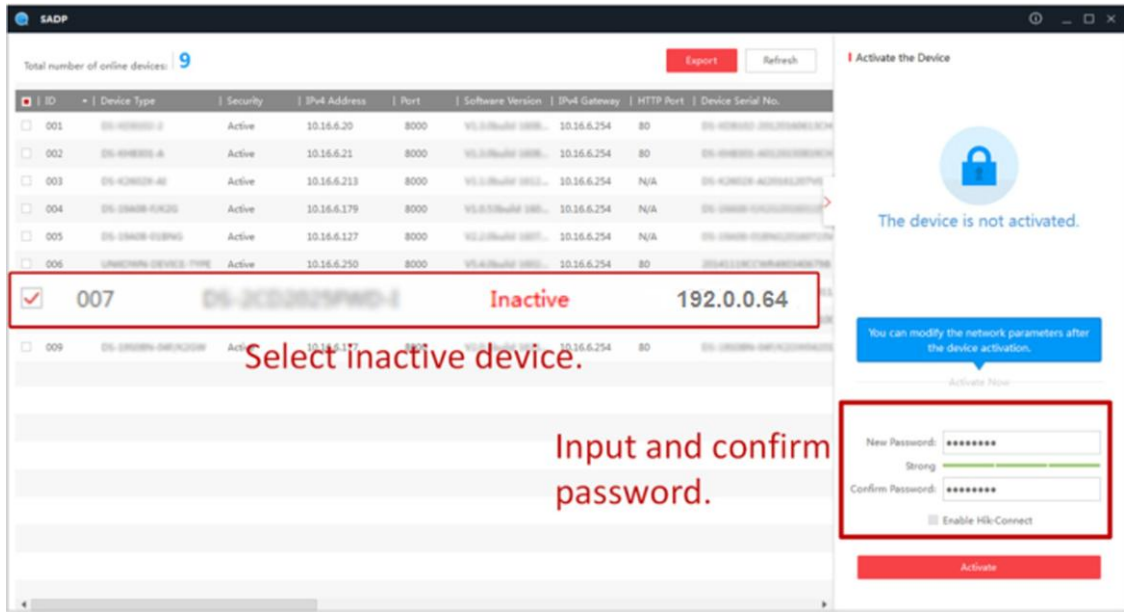
手順

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デバイスを選択します。
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します-製品のセキュリティ強化のため、ご自身で選択した強力なパスワード（大文字、小文字、数字、特殊文字を含む8文字以上）の設定を強く推奨します。また、特に高セキュリティシステムでは、パスワードを定期的に（月次または週次で）リセットすることで製品をより効果的に保護できます。

4. **アクティベート**をクリックして有効化を開始してください。



アクティベーションが成功すると、デバイスのステータスが「**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) デバイスを選択します。
2) IPアドレスを手動で変更するか、**[DHCPを有効にする]**をチェックして、デバイスのIPアドレスをコンピュータと同じサブネットに変更します。
3) 管理者パスワードを入力し、「**変更**」をクリックしてIPアドレス変更を有効化してください。

10.4 iVMS-4200クライアントソフトウェア経由でのデバイス有効化

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、有効化用のパスワードを作成する必要があります。

手順

注記
この機能はデバイスがサポートしている必要があります。

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

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

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

7. **[OK]**をクリックしてデバイスをアクティブ化します。

第11章 モバイルWeb経由でのデバイス設定

11.1 ログイン

モバイルブラウザからログインできます。

注
デバイスがアクティベートされていることを確認してください。

デバイスのホットスポットが無効の場合：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、デバイスのIPアドレスが表示されます。アドレスをタップするとログインページに移動します。

デバイスのホットスポットが有効な場合：

Androidシステム：スマートフォンをNFCエリアに置くと、デバイスホットスポットの名称とパスワードが自動的に取得されます。接続を確認すると、ログインページに移動します。

iOSシステム: スマートフォンのWi-Fi機能を有効にし、現在のデバイスのホットスポットに接続してください。ホットスポット接続後、ログインページが表示されます。

ホットスポット名: AP_シリアル番号ホットス

ポットパスワード: デバイスのシリアル番号

11.2 概要

デバイスのステータス確認やリモート操作などが行えます。

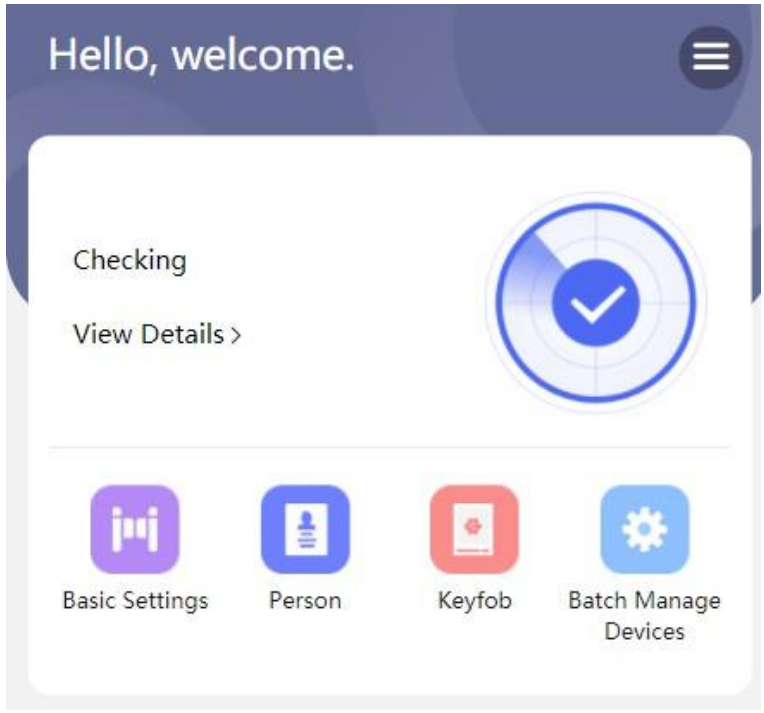


図 11-1 ステータスとクイック設定

デバイスの状態を確認できます。異常がある場合は、タップしてコンポーネントの詳細を表示できます。

基本設定ページ、ユーザーページ、キーフォブページ、ネットワークページ、バッチデバイス管理ページをタップして素早く入力できます。

図11-2 リモートコントロール

アイコンをタップすると、バリアをリモート制御できます。

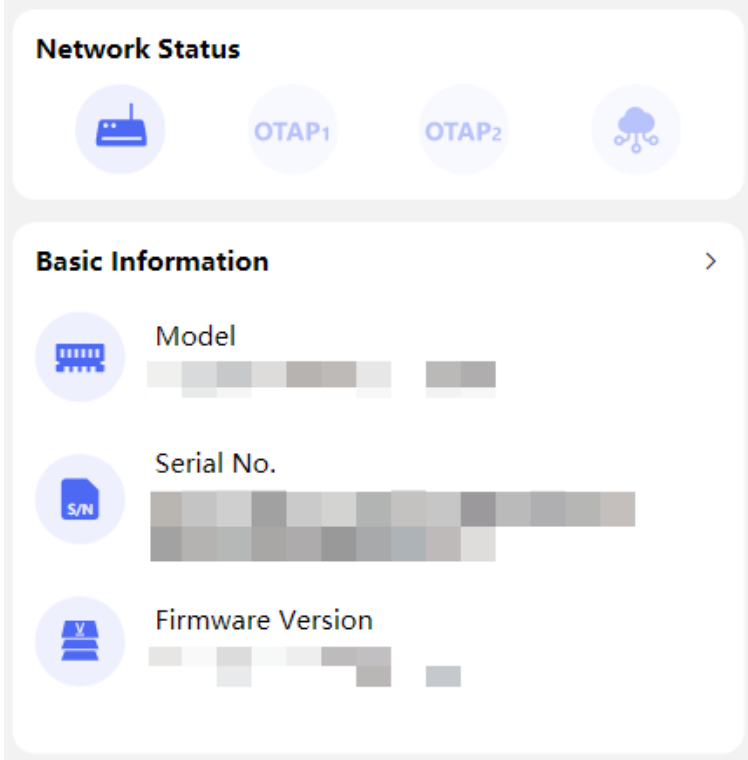


図 11-3 ネットワークステータスと基本情報

ネットワークステータス、モデル、シリアル番号、ファームウェアバージョンを表示でき、タップすると基本情報ページに素早く移動できます。

11.3 設定

11.3.1 初期化ウィザード ゲート開閉

学習

開始前に

→ **初期化ウィザード** をタップします。

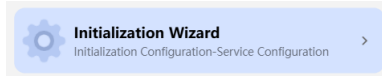
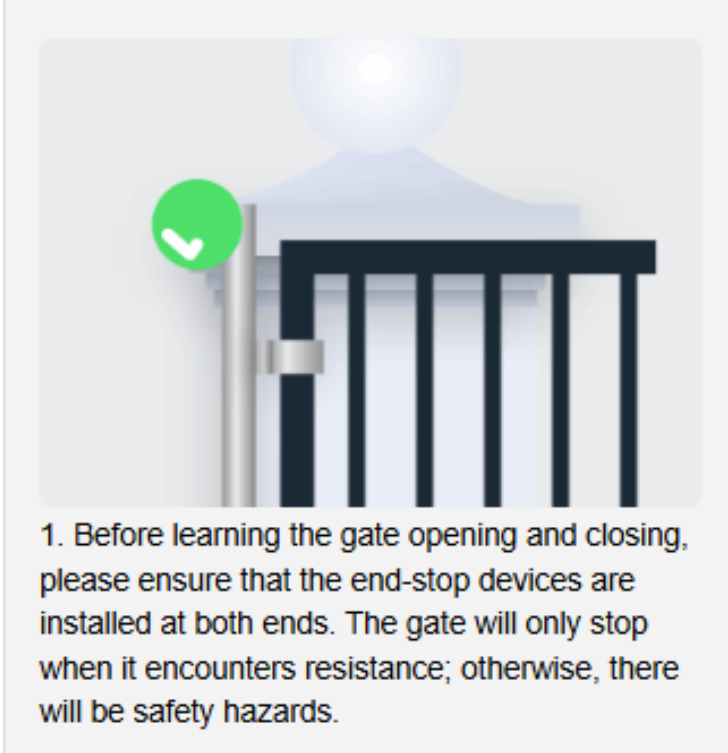


図11-4 インストールウィザード

手順

1. 両端にエンドストップデバイスが設置されていることを確認してください。学習期間中は、連動検知器などの安全設定は利用できません。



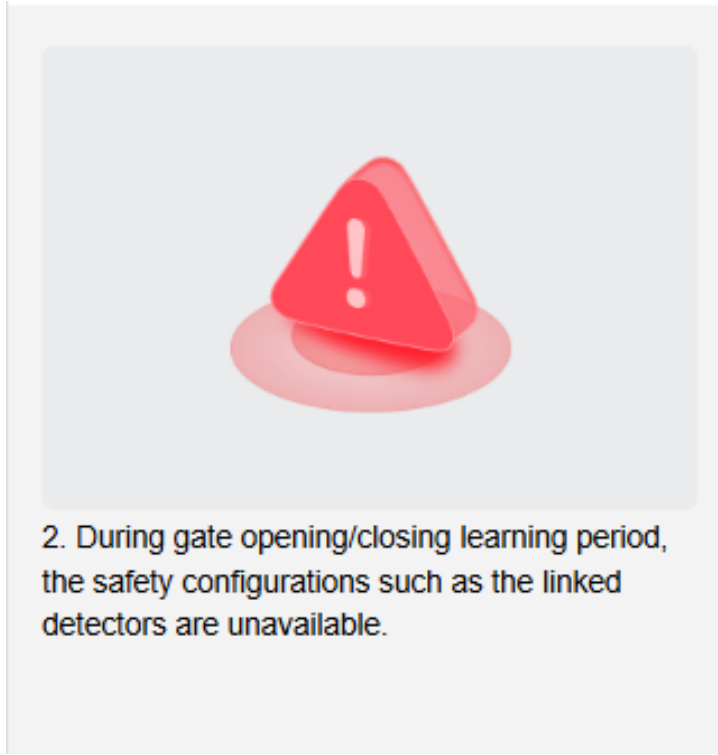


図 11-5 安全確認

2. **「開始」**をタップして最初の終端位置を特定します。ゲートが終端位置に到達したら**「到達」**をタップするか、最初の終端位置を再設定するには**「未到達」**をタップします。

図 11-6 最初の終端位置の特定

3. 別の終点を設定します。ゲートが終点に到達したら「**到着**」をタップするか、終点を再設定するには「**未到達**」をタップします。
をタップして終端点を再設定します。

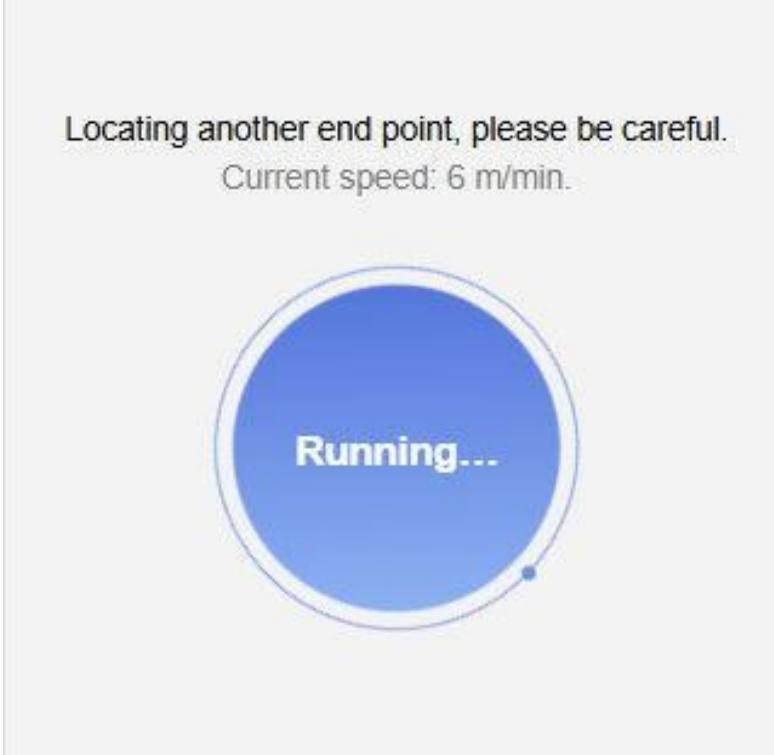


図11-7 別の終端点を特定する

4. 試行実行。

]

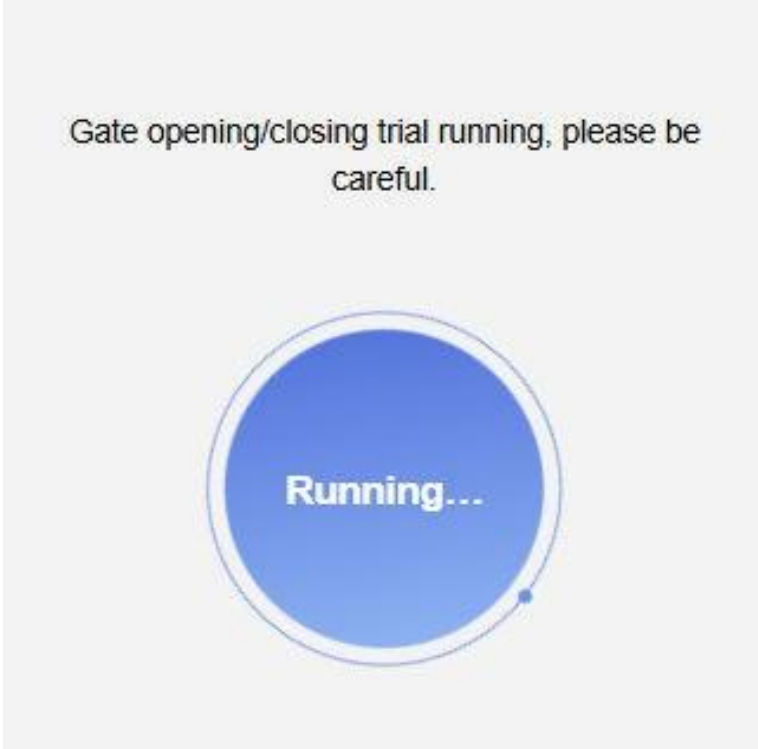


図11-8 トライアル実行

5. ゲート状態、走行速度、デバイス時間などの実行設定を設定します。

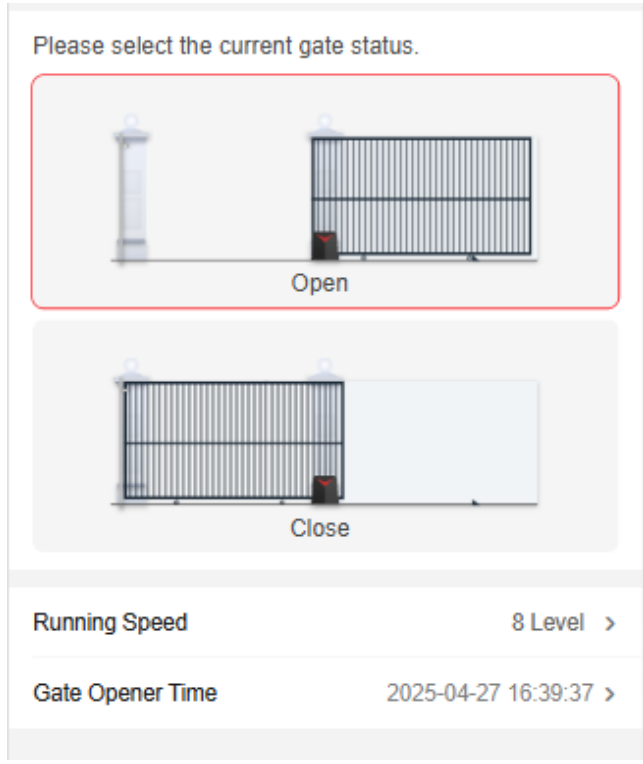


図 11-9 実行設定

6. 検出器の設定を行います。

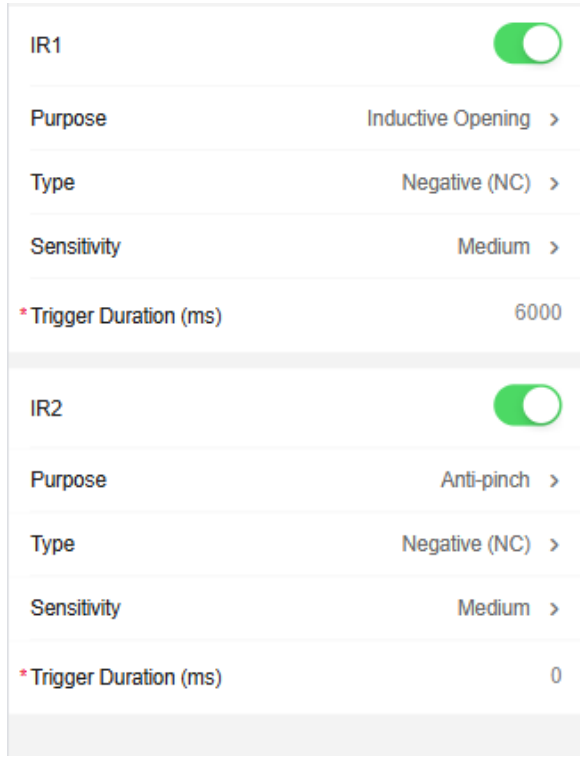


図 11-10 検出器設定

7. 設定を保存して次のパラメータに進むには、**[次へ]** をタップします。設定をスキップするには、**[スキップ]** をタップします。

11.3.2 ターンスタイルの基本設定

ターンスタイルの基本パラメータを設定できます。

概要ページでショートカットエントリの**「基本設定」**をタップするか、「 」→**「基本設定」**をタップします。

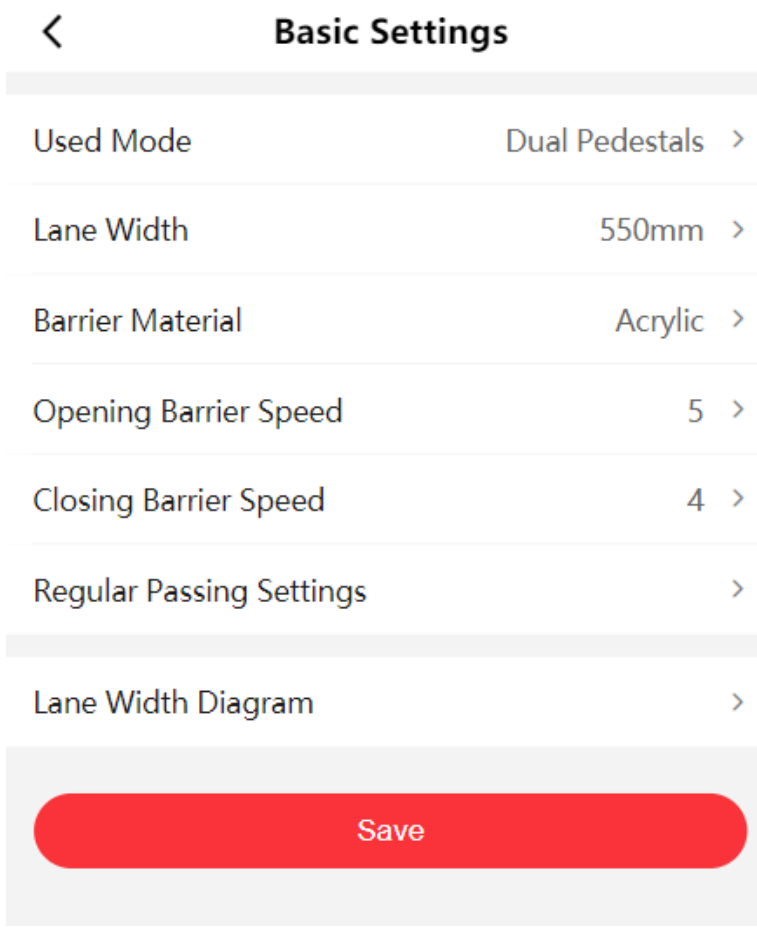


図11-11 ターンスタイル基本パラメータ

使用モード、レーン幅、バリア材質、バリア開放速度、バリア閉鎖速度を設定します。**使用モード**

実際のニーズに応じて、**シングルペデスタル**または**デュアルペデスタル**を選択します。

シングルペデスタル

1基の支柱のみを使用する場合は、このオプションを選択してください。

デュアルペデスタル

デュアルペデスタルのみを使用する場合、このオプションを選択してください。

遮蔽材

実際の状況に応じてバリア材を選択してください。

レーン幅

実際の状況に応じてレーン幅を選択してください。

バリア開閉速度

バリアの開閉速度を設定します。

「通常通行設定」をタップして、出入口の通行モードを設定します。「**レーン幅図**」をタップして、装置図を表示します。

保存をタップします。

デバイスの基本情報を表示

デバイス名、言語、モデル、シリアル番号、バージョン、Mac アドレスなどを表示できます。「 」→**「システム設定」→「基本情報」**をタップします。

デバイスの名前を変更できます。

デバイスの言語、モデル、シリアル番号、バージョン、ローカルRS-485番号、アラーム入力数、アラーム出力数、MACアドレス、工場情報などを確認できます。

デバイス容量をタップすると、人物、顔、カード、イベントの数量と容量を確認できます。**保存**をタップします。

時間設定

現在の時刻を表示し、タイムゾーンを設定します。

→ **System Settings** → **Time Settings** をタップします。

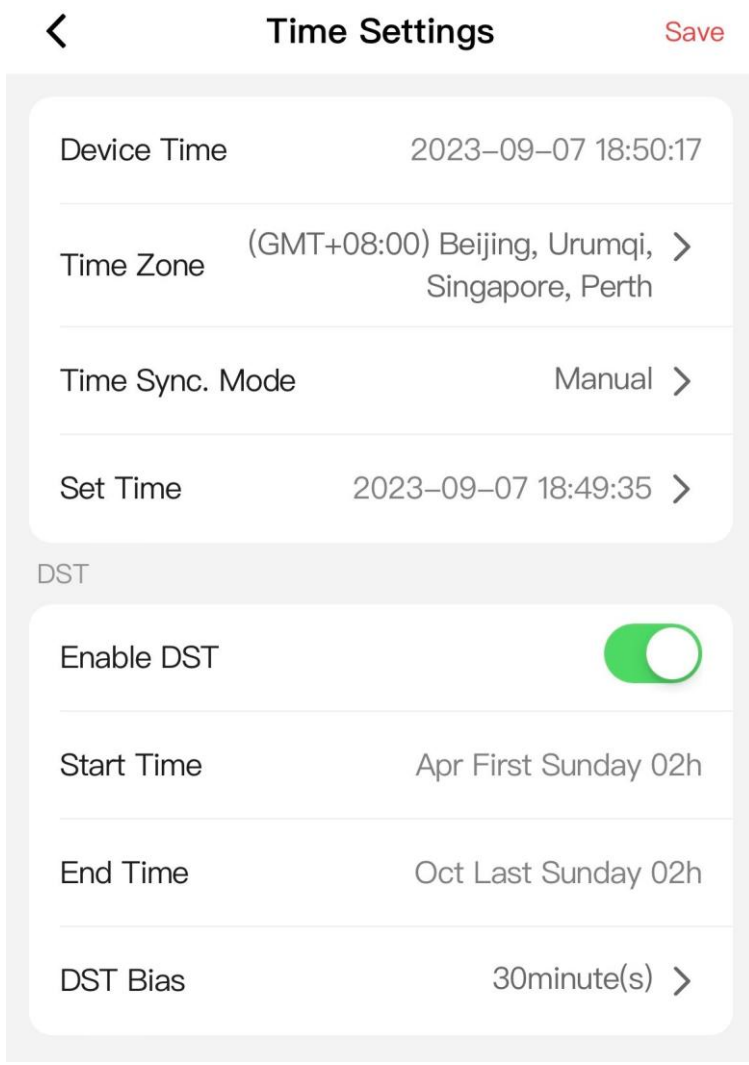


図 11-12 時間設定

デバイスの時刻

現在の時刻を表示できます。

タイムゾーン

ドロップダウンリストから、デバイスが置かれているタイムゾーンを選択します。

時刻同期モード手動

デフォルトでは、デバイスの時刻は手動で同期する必要があります。デバイスの時刻は手動で設定できます。

NTP

NTPサーバーのIPアドレス、ポート番号、間隔を設定します。

夏時間

スライドして夏時間を有効にし、開始時刻、終了時刻、および夏時間補正を設定します。

保存をタップします。

11.3.3 ユーザー管理

ユーザーパスワードを変更できます。

ホームページで、[ ] → **[User Management]** をタップします。
ユーザーをタップし、古いパスワードを入力して新しいパスワードを作成し、パスワードを確認します。**保存**をタップします。

11.3.4 ネットワーク

有線ネットワーク

有線ネットワークを設定します。

→ **Network Settings → TCP/IP** をタップして設定ページに入ります。

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。

DHCP

この機能を無効にする場合は、IPv4 アドレス、IPv4 サブネットマスク、IPv4 デフォルトゲートウェイ、IPv6 モード、IPv6 アドレス、IPv6 サブネットプレフィックス長、IPv6 デフォルトゲートウェイを設定する必要があります。

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

MACアドレスとMTU

デフォルトの MAC アドレスと MTU を表示できます。

IPv6モード

ルートアドバタイズメント

IPv6 アドレスは、ルートアドバタイズメントとデバイスの MAC アドレスを組み合わせて生成されます。

注記 バタイズメントモードは、デバイスが接続されているルーターのサポートが必要です。

手動

IPv6アドレス、IPv6サブネットマスク、およびIPv6デフォルトゲートウェイを入力してください。必要な情報についてはネットワーク管理者に確認してください。

DHCP

IPv6 アドレスは、サーバー、ルーター、またはゲートウェイによって割り当てられます。

DNS サーバー

注

DHCPが有効な場合にのみ、DNSサーバーを設定できます。

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

Wi-Fiの設定

Wi-Fiを有効にした後、Wi-Fiに接続できます。

ホーム画面で、（設定）→ **Network Settings（ネットワーク設定）→ Wi-Fi** をタップします。

デバイスのホットスポットを設定

デバイスのホットスポットを有効にした後、携帯電話を使用してホットスポットに接続し設定できます。ホーム画面で、[ ] → **[Network Settings] → [Device Hotspot]** をタップします。

デバイスホットスポットを有効にするためにスライドし、ホットスポット**の名前**を設定し、パスワードを入力して確認します。「**保存**」**を**タップします。

ポートパラメータの設定

ネットワーク経由でデバイスにアクセスする際、実際のニーズに応じてHTTP、HTTPSを設定できます。 →

Network Service → HTTP(S) をタップして設定ページに入ります。

HTTP

これは、ブラウザがデバイスにアクセスする際に使用するポートを指します。例えば、HTTPポートが81に変更された場合、ログインにはブラウザに***http://192.0.0.65:81***と入力する必要があります。

HTTPS

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

WebSocketの設定

ネットワーク経由でデバイスにアクセスする際、実際の必要に応じてWebSocketを設定できます。

→ **Network Service → WebSocket(s)** をタップして設定ページに入ります。

WebSocket

ブラウザアクセス用のWebSocketを表示します。

WebSockets

ブラウザアクセス用のWebSocketsを表示します。

プラットフォームアクセス

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

手順

1. （設定）→ **Device Access（デバイスアクセス）→ Hik-Connect** をタップして設定ページに入ります。

   注記

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

2. 機能を有効にするにはスライドしてください。
3. **カスタムを**有効にしてサーバーアドレスを入力できます。

   注意

   - 6～12文字（a～z、A～Z）または数字（0～9）、大文字小文字を区別します。8文字以上の英数字の組み合わせを使用することを推奨します。

4. **登録状況**と**紐付け状況**を確認できます。
5. **「アカウントを紐付ける」→「QRコードを表示」**をタップし、QRコードをスキャンしてアカウントを紐付けできます。
6. 設定を有効にするには「**保存」を**タップしてください。

OTAPプロトコルを設定する

OTAPプロトコルによりデバイスをメンテナンスプラットフォームに接続し、デバイス情報の検索·取得、デバイス稼働状況および例外のアップロード、再起動およびアップグレードを実現できます。

手順

1. → **Device Access → OTAP** をタップします。

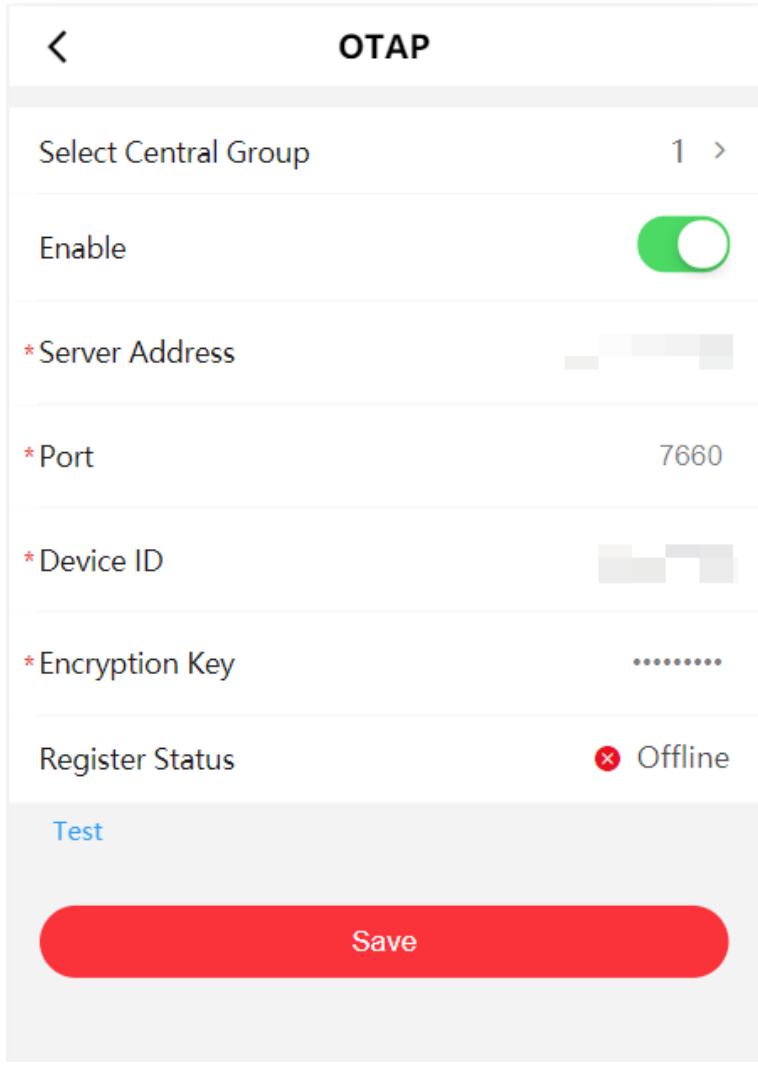


図 11-13 OTAP

2. **中央グループ選択**から 1 または 2 を選択します。
3. **有効化を**スライドします。
4. サーバーアドレス、ポート、デバイスID、暗号化キーを設定します。
5. **[テスト] を**タップし、デバイスがサーバーに接続でき、登録が完了したことを確認します。
6. **保存**をタッ

プします。**結**

果

ウェブページを更新するか、デバイスを再起動して、OTAPの**登録ステータスが**オンラインに切り替わることを確認してください。

ネットワーク侵入サービスの設定

デバイスがLANに展開されている場合、リモートデバイス管理を実現するために侵入サービスを有効化できます。

手順

1. → **Device Access** → **Network Penetration Settings** をタップして設定ページに入ります。
2. **「侵入サービスを有効にする」**を有効にします。
3. **サーバーIPアドレス**と**サーバーポート**を入力します。
4. ログイン**ユーザー名**と**パスワード**を入力します。
5. **ハートビートタイムアウト**を設定します。範囲は1から6000です。
6. **オンライン状態**を確認できます。最新状態を表示するには「**更新**」をクリックしてください。
7. **保存**をタップします。

11.3.5 アラーム出力パラメータの設定

実際のニーズに応じて、アラーム名、アラーム継続時間、カスタムを設定できます。 → **Alarm Setting** → **Alarm Output** をタップして設定ページに入ります。

アラーム持続時間

アラーム持続時間を「**連続アラーム**」または「**カスタムアラーム持続時間**」に設定します。

カスタム

カスタムアラーム持続時間を設定します。持続時間を0に設定すると、残りの出力が有効になります。

11.3.6 シリアルポート設定

シリアルポートのパラメータを設定します。

手順

1. → **Access Configuration** → **Serial Port Configuration** をタップして設定ページに入ります。

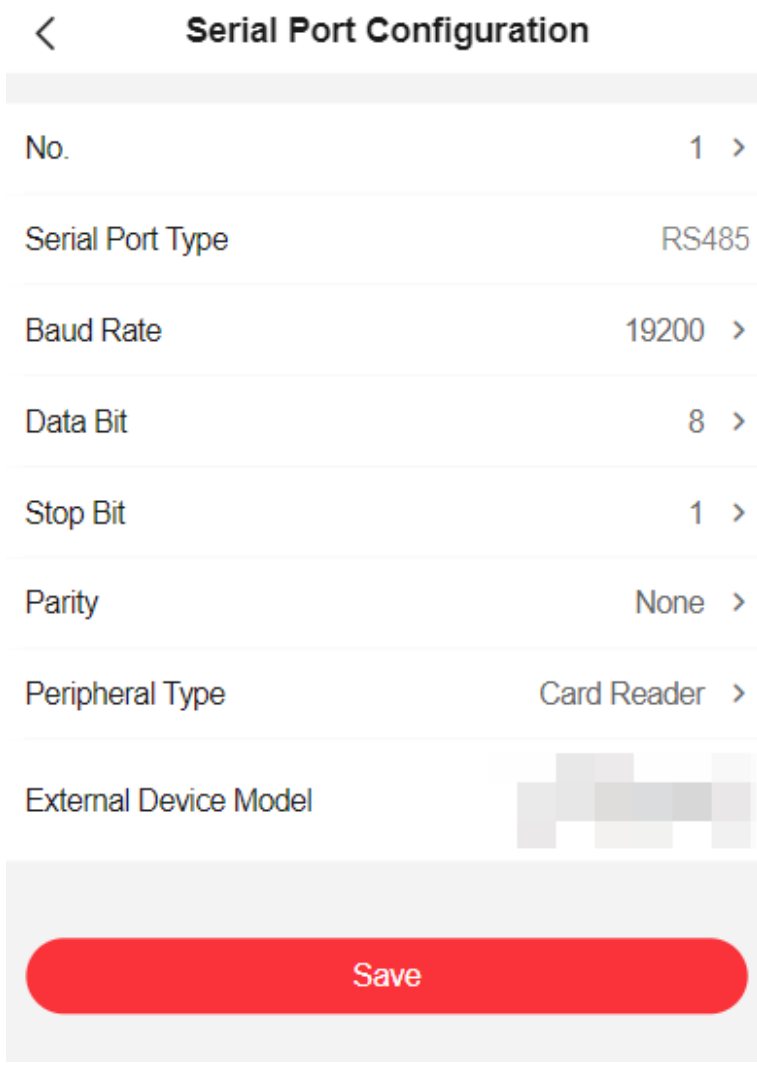


図 11-14 シリアルポート設定

2. シリアルポートの位置を「**入力**」または「**出力**」に設定します。
3. シリアルポート番号を選択すると、対応するシリアルポートタイプが自動的に表示されます。
4. シリアルポートのパラメータを設定します。

ボーレート

データ転送速度を設定します。

データビット

データを送信するビット数を設定します。

ストップビット

1フレーム分のデータの終点を選択してください。

パリティ

シリアル通信のエラー検出方式を選択します。データビットとチェックビットの1の数が奇数か偶数かを検出するか、チェックビットがないかを検出するかを選択できます。

5. 接続ポートの**周辺機器タイプ**を設定します。
6. 外部デバイスのモデルを確認できます。
7. **保存**をタップします。

11.3.7 人物管理

「**Person**」をタップするか、「☰」→「**Person Management**」をタップしてページに入ります。

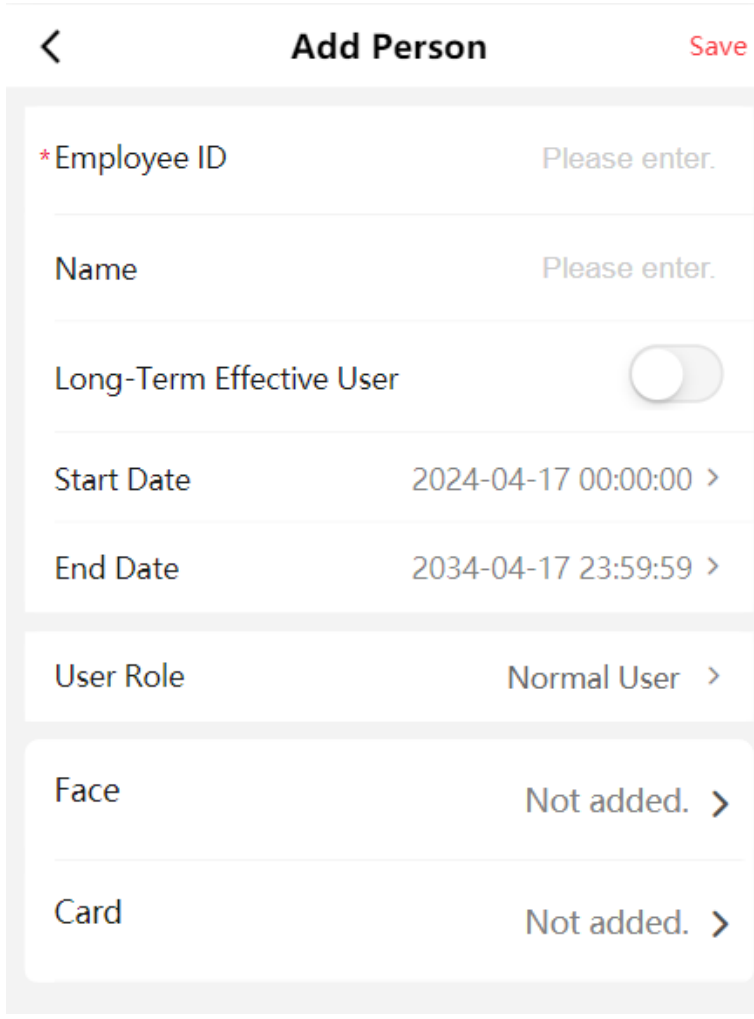


図 11-15 人物管理

基本情報の追加

人物管理ページで、**[+]** をタップします。
従業員IDと名前を作成し、ユーザーロールを選択します。**保存**をタップします。

顔写真を追加

人物管理ページで、**+ → 顔写真を**タップします。**+ を**タップ
し、写真を撮るか写真を選択します。
保存をタップします。

カードを追加

人物管理ページで、**+ → カード** をタップします。
+ をタップし、カード番号を入力してカードのプロパティ（種類）を選択
します。**保存**をタップします。

人物の権限設定

人物管理ページで、**+ を**タップします。
長期有効ユーザーを有効にし、対象者の開始時間と終了時間を設定します。**保存**をタップします。

人物管理

管理ページで人物情報を編集します。人物をタップし、情報を編集し
ます。
保存をタップします。

11.3.8 アクセス制御設定

ドアパラメータの設定

ドア名、開放時間、退出ボタンパラメータを設定できます。 **→ Access Control →**

Door Parameters をタップします。

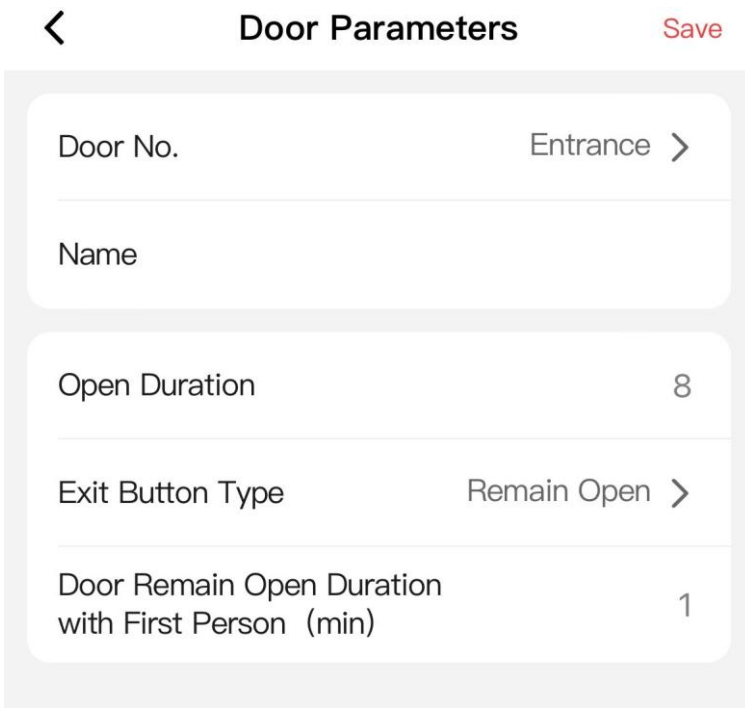


図 11-16 ドアパラメータ

設定対象として入口または出口を選択し、名称と**開放時間を**設定し、**退出ボタンタイプ**を選択します。

ファーストパーソンによるドア開放時間設定。このモードは、観光地への入場者など、複数人の通過に適しています。設定人数が通過した後、ドアは設定時間だけ開放され、他の者は認証なしで通過できます。

設定後、「**保存**」をクリックして設定を保存します。

IR検出器設定

赤外線検知器のパラメータを設定します。

手順

1. → **IR検出器設定**をタップして設定ページに入ります。
2. **誘導モード（入口）**と**誘導モード（出口）**を設定します。
3. IR検出器をカスタマイズできます。

例外的なIR自動遮蔽

赤外線検出器が損傷した場合、一時的にレーンを復旧させるために遮蔽できますが、バリアの開閉時に通行人に怪我を負わせる可能性があります。

注意

例外的なIR自動遮蔽機能は一時的な遮蔽です。1時間以内に例外が発生しない場合、復旧します。

IR緊急モード

一部の赤外線ビームが正常に作動しない場合、それらのビームを遮蔽することで通路を復旧できます。ただし、この操作により人に接触し負傷させる可能性があります。

ドア閉時のカスタム挟み込み防止機能を有効にする

ドア閉め時の挟み込み防止機能は、バリアが閉じる際に通路内に人が残っていると装置が検知した場合に使用されます。この場合、バリアは閉じません。人が通路から完全に退出してから初めてバリアは閉じます。この機能を有効にすると、一部の赤外線センサーを遮断できるため、人が通過した後にバリアを事前に閉じることが可能ですが、バリアの開閉時に通行人を傷つける可能性があります。

本機能の有効化を推奨します。

4. **保存**をタップしてください。

11.3.9 イベント検索

→ **Event Search** をタップします。

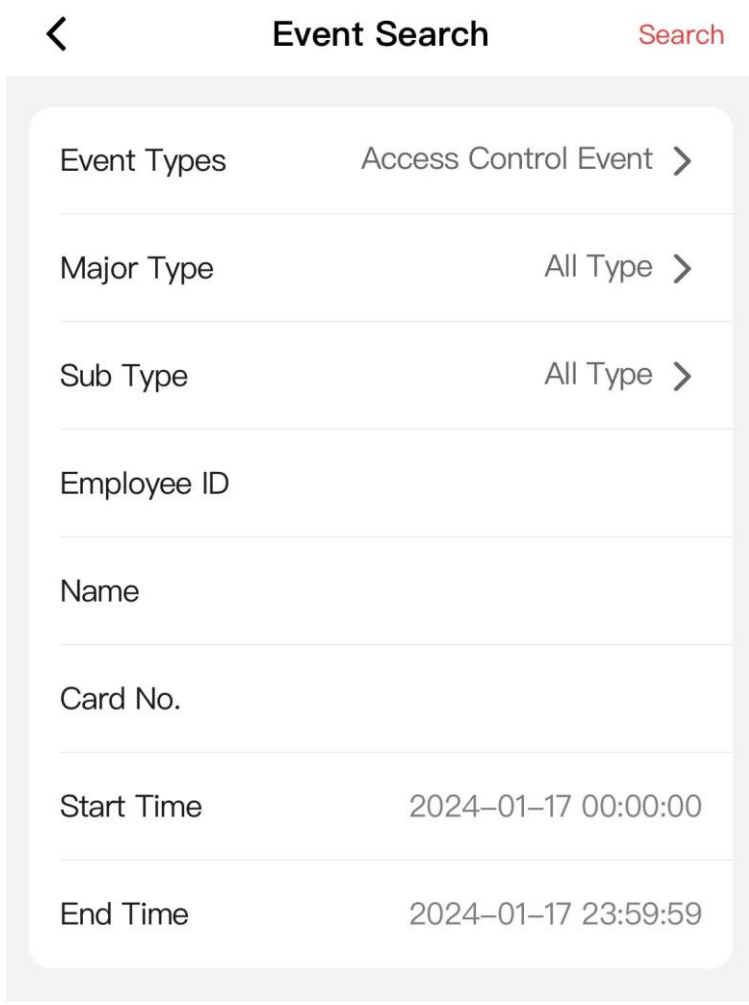


図 11-17 イベント検索

イベントタイプ、主要タイプ、サブタイプを選択します。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ます。**検索**をタップします。

注
128 桁以内の名前検索に対応しています。

検索結果はリストに表示されます。

11.3.10 アップグレードとメンテナンス

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

デバイスの再起動

（再起動）→ **Restart（再起動）**をタップします。
再起動をタップしてデバイスを再起動します。

アップグレード

（アップグレード）→ Upgrade（アップグレード）をタップします。
アップグレードをタップしてデバイスをアップグレードします。

注
アップグレード中は電源を切らないでください。

パラメータの復元

（デフォルト設定）→ **Default**（デフォルト）をタップします。
デフォルト設定に復元
デバイスはデフォルト設定に復元されます。ただし、デバイスのIPアドレスとユーザー情報は除きます。
工場出荷時設定への復元
すべてのパラメータが工場出荷時の設定に復元されます。使用前にデバイスをアクティベートする必要があります。

ログのエクスポート

→ **Log Export** をタップします。
ログの種類を選択し、「**エクスポート」を**タップしてメンテナンスログをダウンロードします。

11.3.11 デバイスのデバッグ

学習と自己診断を完了し、デバッグを管理できます。 → **Device Debugging を**
タップします。
レーン学習/モーター自己診断
レーン学習
レーン学習をタップすると、装置は学習モードに入ります。バリアの閉位置を学習します。
モーター自己診断
モーター自己診断をタップすると、デバイスのモーターが自己診断を開始します。
エンコーダ自己診断
1. レーンを選択し、エンコーダテストを開始します。
2. バリアが閉位置にあることを確認してください。**OK**をタップします。

3. バリアを開位置に回転させます。**テスト停止**をタップします。

4. 結果を待ちます。

IR セルフテスト

チャンネル（レーン）を選択し、**IRセルフテスト**をタップすると、装置は全ての赤外線検出器をテストします。IRセルフテスト機能を有効にした後、装置は開閉前にチャンネル（レーン）を退出する音を発します。バリアは入口/出口で最高速度で開くように強制され、この時IR挟み込み防止機能は無効になります。赤外線がトリガーされたり遮断されたりすると、装置は検知失敗を音で知らせます。

注意

レーン内に人がいないことを確認してください。

デバッグコマンド管理

コマンドタイプを選択し、コマンドを選択するか手動でタップします。**「送信」**をタップすると、コマンドがデバイスに送信されます。

コマンドが完了すると、結果がページに表示されます。「**デバッグ終了**」をタップしてデバッグを終了します。

注意

「デバッグ終了」をタップしない場合、デバイスは7×24時間以内に自動的にデバッグモードを終了します。

IR例外情報

「エクスポート」をタップすると、例外的な赤外線検出器レポートをエクスポートできます。

デモモード

有効化後、デバイスは顔認識後に自動的に追加および認証を行います。有効期間を設定できます。

無効にした場合、デモモードで追加されたすべての個人情報は無効化後に消去されます。

11.3.12 ユーザー文書を表示

ユーザードキュメントを表示します。

注意

IPアドレスでモバイルWebにアクセスした場合のみ、ユーザードキュメントを閲覧できます。ホットスポット経由のログインではこの機能はサポートされていません。

をタップしてページにアクセスしてください。

「オンラインドキュメントを表示」をタップしてユーザーマニュアルを表示します。

11.3.13 ログアウト

設定ページからログアウトします。

→ **Logout** をタップし、**OK** をタップします。

設定ページに再度アクセスする場合は、ユーザー名とパスワードの再入力が必要です。

第12章 Webブラウザによるクイック操作

12.1 時間設定

ウェブページの右上にある「 」をクリックしてウィザードページに入ります。

デバイスの時刻

デバイスの時刻をリアルタイムで表示します。

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。

時刻同期モード NTP

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

手動

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

夏時間

夏時間（DST）を有効にしたり、夏時間の開始時刻、終了時刻、およびバイアス時間を設定 確認できます。

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

第13章 Webブラウザによる操作

13.1 ログイン

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

注
デバイスが起動していることを確認してください。

Webブラウザ経由のログイン

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

クライアントソフトウェアのリモート設定によるログイン

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

13.2 パスワードを忘れた場合

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

ログインページで「**パスワードを忘れた場合**」をクリックしてください。**認証モード**を選択してください。

セキュリティ質問による認証

セキュリティの質問に答えてください。

メール認証

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

13.3 ヘルプ

13.3.1 オープンソースソフトウェアライセンス

オープンソースソフトウェアのライセンスを確認できます。

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

13.3.2 オンラインヘルプドキュメントを表示

Web 設定のヘルプ文書を表示できます。

→ Web ページの右上にある **[オンラインドキュメント]** をクリックしてドキュメントを表示します。

13.3.3 ログアウト

アカウントからログアウトします。

admin → Logout → OK をクリックしてログアウトします。

13.4 Webブラウザによるクイック操作

13.4.1 時間設定

ウェブページの右上にある「 」をクリックしてウィザードページに入ります。

デバイスの時刻

デバイスの時刻をリアルタイムで表示します。

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。

時刻同期モード NTP

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

手動

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

夏時間

夏時間（DST）を有効にしたり、夏時間の開始時刻、終了時刻、およびバイアス時間を設定 ·確認できます。

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

13.5 人物管理

基本情報、資格情報、認証、設定を含む人物情報を追加できます。

基本情報の追加

「人物管理」→「追加」をクリックすると、「人物追加」ページが表示されます。
従業員ID、氏名、人物タイプを含む基本情報を追加します。
人物タイプで「**訪問者**」を選択した場合、訪問時間を設定できます。**「保存」**をクリックして設定を保存してください。

許可時間の設定

「人物管理」→「追加」をクリックし、「人物追加」ページに入ります。
「**長期有効ユーザー**」を有効にするか、**開始時間**と**終了時間を**設定し、実際のニーズに応じて設定された期間内にのみ権限を付与することができます。
設定を保存するには、**[保存]**をクリックします。

顔写真を追加

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

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

設定を保存するには「**保存**」をクリックします。

カード追加

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

デバイス番号設定

「人員管理」→「追加」をクリックして「人員追加」ページに入ります。
人物が改札機を通過した後にエレベーター呼び出し機能を実現するため、人物に部屋番号を紐付けることができます。
「Add」をクリックし、**Room No.** と **Floor No.** を入力します。 をクリックして部屋番号を削除することもできます。**「Save」**をクリックして設定を保存します。

認証設定

「人物管理」→「追加」をクリックして「人物追加」ページに入ります。**認証タイプ**を「**デバイスと同じ**」または「**カスタム**」に設定します。
設定を保存するには、**[保存]**をクリックします。

人物データのインポート/エクスポート

「Person Management」をクリックして「Person」ページに入ります。

個人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用にエクスポートできます。
「人物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てください。
「OK」をクリックします。

注意

- 個人データは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となります。

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。
暗号化パスワードを入力して、人物データをインポートし、デバイスに同期します。

13.6 デバイス管理

13.6.1 サブアクセス制御ボード管理

このページでサブアクセス制御ボードを管理できます。

手順

1. デバイス管理 → デバイス管理 → サブアクセス制御ボードをクリックしてページに入ります。

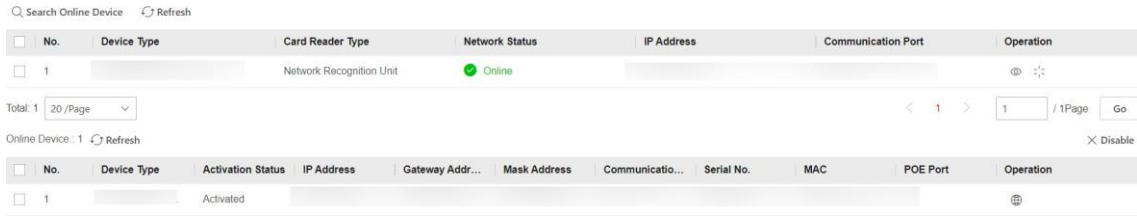


図13-1 デバイス管理

2. デバイスパラメータを設定します。

機能	説明
	デバイス名を設定し、**デバイスモデル**、**シリアル番号**、**バージョン**、**アラーム入力**、**アラーム出力**を表示します。
	デバイスの再起動。
更新	デバイスリストを更新します。
	サブアクセス制御ボードのネットワークパラメータ（**IPアドレス**など）を編集し、**ゲートウェイアドレス**、**IPv4サブネットマスク**、**通信ポート**を確認します。管理者パスワードを入力してください。

注意

サブアクセスボードとメインアクセスボードのIPアドレスは同一IPセグメント内にあることを確認してください。さもなければサブアクセスボードがオフラインになる可能性があります。

3. **保存**をクリックします。

13.6.2 デバイス一括管理

現在のデバイスと同じネットワークセグメントにあるすべてのメインアクセス制御ボードの情報を表示できます。バリアの位置確認、ネットワークパラメータの設定、サブアクセス制御ボードとのパラメータ同期、単一メインアクセス制御ボードのデバイス名編集が可能です。また、バッチデバイスを選択してネットワークパラメータの設定、パラメータの同期、アクティベートを行うこともできます。

手順

1. **[デバイス管理]→[デバイス管理]→[デバイスの一括管理]** をクリックしてページに入ります。

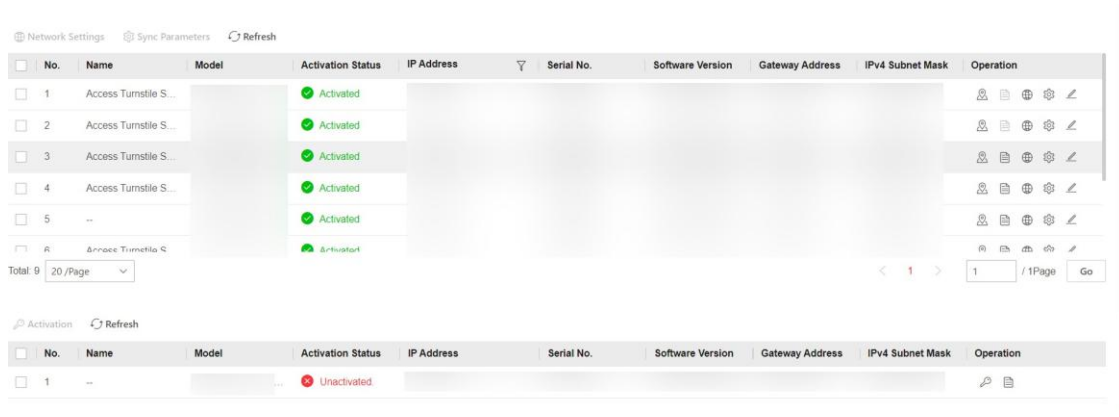


図13-2 バッチ管理デバイスページ

サブアクセス制御ボードと同じネットワーク下にあるすべてのデバイス（メインアクセス制御ボード）がページに表示されます。

注記

ページの上部領域はアクティブ化されたデバイス、下部領域は非アクティブ化されたデバイスです。

2. アクティブ化されたデバイスに対して、以下の操作を実行できます。

アイコンをクリックすると、バリアの状態を確認できます。

アイコンをクリックしてサブアクセス制御ボードの情報を表示し、ネットワークパラメータを設定します。管理者パスワードを入力し、「**保存**」をクリックしてください。

注意

- DHCP機能を無効にした場合は、IPv4アドレス、IPv4サブネットマスク、ゲートウェイアドレスを設定する必要があります。
- DHCP 機能をチェックすると、システムは IPv4 アドレス、IPv4 サブネットマスク、およびゲートウェイアドレスを自動的に割り当てます。

アイコンをクリックして、メインおよびサブアクセス制御ボードのネットワークパラメータを設定し、管理者パスワードを入力して「**保存**」をクリックします。

DHCP

この機能をオフにした場合、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。

この機能のチェックを外す場合は、IPv4アドレス、IPv4サブネットマスク、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。

IPv6モード手

動

IPv6 アドレス、IPv6 サブネットプレフィックス長、および IPv6 デフォルトゲートウェイを手動で設定します。

DHCP

システムは、IPv6 アドレス、IPv6 サブネットプレフィックス長、および IPv6 デフォルトゲートウェイを自動的に割り当てます。

ルートアドバタイズメント

IPv6プロトコルスタックにおける自動アドレス設定メカニズム。環境内にルーティング通知メッセージを提供できるルータが存在する場合、デバイスはIPv6アドレス設定を完了できる。

「**ルートアドバタイズメントを表示**」をクリックすると、IPv6アドレス一覧を表示できます。

アイコンをクリックして対応するパラメータを現在のデバイスと同期し、管理者パスワードを入力して「**保存**」をクリックします。

アイコンをクリックしてデバイスの名前を編集し、管理者パスワードを入力して「**保存**」をクリックします。

3. 非アクティブ状態のデバイスに対して以下の操作を実行できます。

アイコンをクリックしてメインおよびサブアクセス制御ボードのネットワークパラメータを設定し、管理者パスワードを入力して「**保存**」をクリックします。

4. バッチデバイスは以下のように管理できます：

デバイスを選択し、アイコンをクリックしてメインアクセス制御ボードのネットワークパラメータを設定します。管理者パスワードを入力し、「**保存**」をクリックしてください。

注意

システムは選択されたデバイスに順番にIPアドレスを割り当てます。サブアクセスボードのIPはメインアクセスボードのIP+1となります。

デバイスを選択し、アイコンをクリックして現在のデバイスと対応するパラメータを同期させ、管理者パスワードを入力して「**保存**」をクリックします。

デバイスを選択し、アイコンをクリックしてアクティブ化します。管理者パスワードを入力し、**保存をクリックします**。

13.7 ターンスタイル

13.7.1 概要

デバイスのコンポーネントステータス、リアルタイムイベント、人物情報、ネットワークステータス、基本情報、デバイス容量を表示できます。また、バリアをリモートで制御することもできます。

機能説明：

デバイスコンポーネントの状態

装置が正常に動作しているか確認できます。「**詳細を表示**」をクリックすると、詳細なコンポーネント状態を確認できます。

リモコン

/ / /

ドアが開いた/閉まった/開いたまま/閉まったまま。

リアルタイムイベント

イベントの従業員ID、名前、カード番号、イベントタイプ、時間、操作を確認できます。また、「**詳細を表示**」をクリックして、イベントタイプ、従業員ID、名前、カード番号、開始時間、終了時間などの検索条件を入力し、「**検索**」をクリックできます。結果は右パネルに表示されます。

人物情報

人物、顔、カードの追加済み/未追加情報を確認できます。

ネットワーク状態

ネットワーク接続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、顔、カード、イベントの容量を確認できます。

13.7.2 イベント検索

ターンスタイル → イベント検索をクリックしてページに入ります。

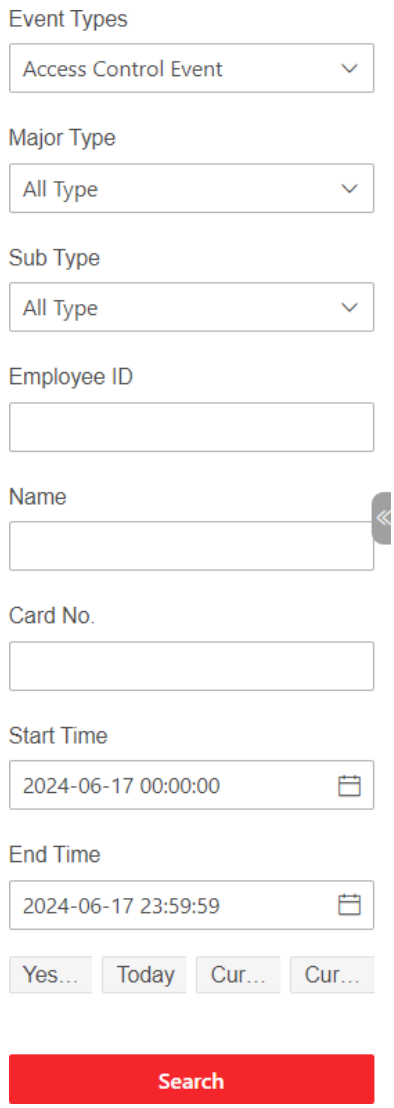


図 13-3 イベント検索

イベントタイプ、主要タイプとサブタイプ、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」**をクリックします。

検索結果は右パネルに表示されます。

13.7.3 パラメータ設定

ドアパラメータの設定

ターンスタイル → パラメータ設定 → ドアパラメータ をクリックします。

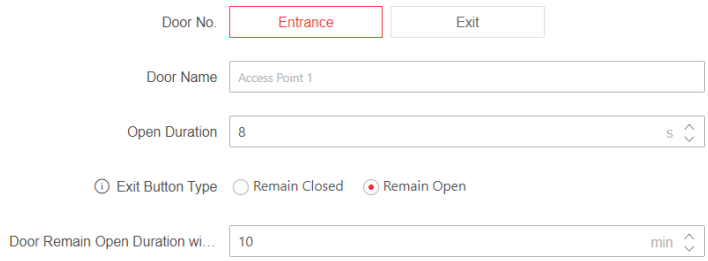


図13-4 ドアパラメータ設定

パラメータを設定し、設定後に「**保存**」をクリックして設定を保存します。

ドア番号

設定には「**入口**」または「**出口**」を選択します。

ドア名

ドアに名前を付けることができます。

開錠時間

ドアのロック解除時間を設定します。設定時間内にドアが開かれない場合、ドアはロックされます。

注意
開は5秒から60秒の範囲です。

終了ボタンのタイプ

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

ドア開放持続時間（最初の人物対応）

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

プライバシーパラメータの設定

イベント保存タイプ、画像アップロード·保存パラメータ、画像消去パラメータを設定します。

ターンスタイルをクリック → **パラメータ設定 → プライバシー設定**。

イベント保存設定

イベントを削除する方法を選択します。デバイスは**上書き**をサポートしています。**上書き**

保存容量が95%を超えた場合、最も古い5%のイベントが削除されます。

画像アップロードと保存

認証時に画像を保存

認証時に画像を自動的に保存します。

認証時に画像をアップロード

プラットフォームへの認証時に画像を自動的にアップロードします。

登録済み画像を保存

この機能を有効にすると、登録された顔写真がシステムに保存されます。

リンク撮影後の画像保存

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

リンク撮影後の画像アップロード

リンクカメラで撮影した画像を自動的にプラットフォームにアップロードします。

デバイス内の全画像を消去

注意

削除した写真は復元できません。

登録済み顔写真を消去

デバイスに登録されているすべての写真が削除されます。

撮影した写真を消去

デバイス内のすべての撮影済み画像が削除されます。

13.7.4 ターンスタイル設定

基本パラメータ

ターンスタイルの基本パラメータを設定します。

手順

1. **ターンスタイル → ターンスタイル設定 → 基本パラメータ**をクリックしてページに入ります。

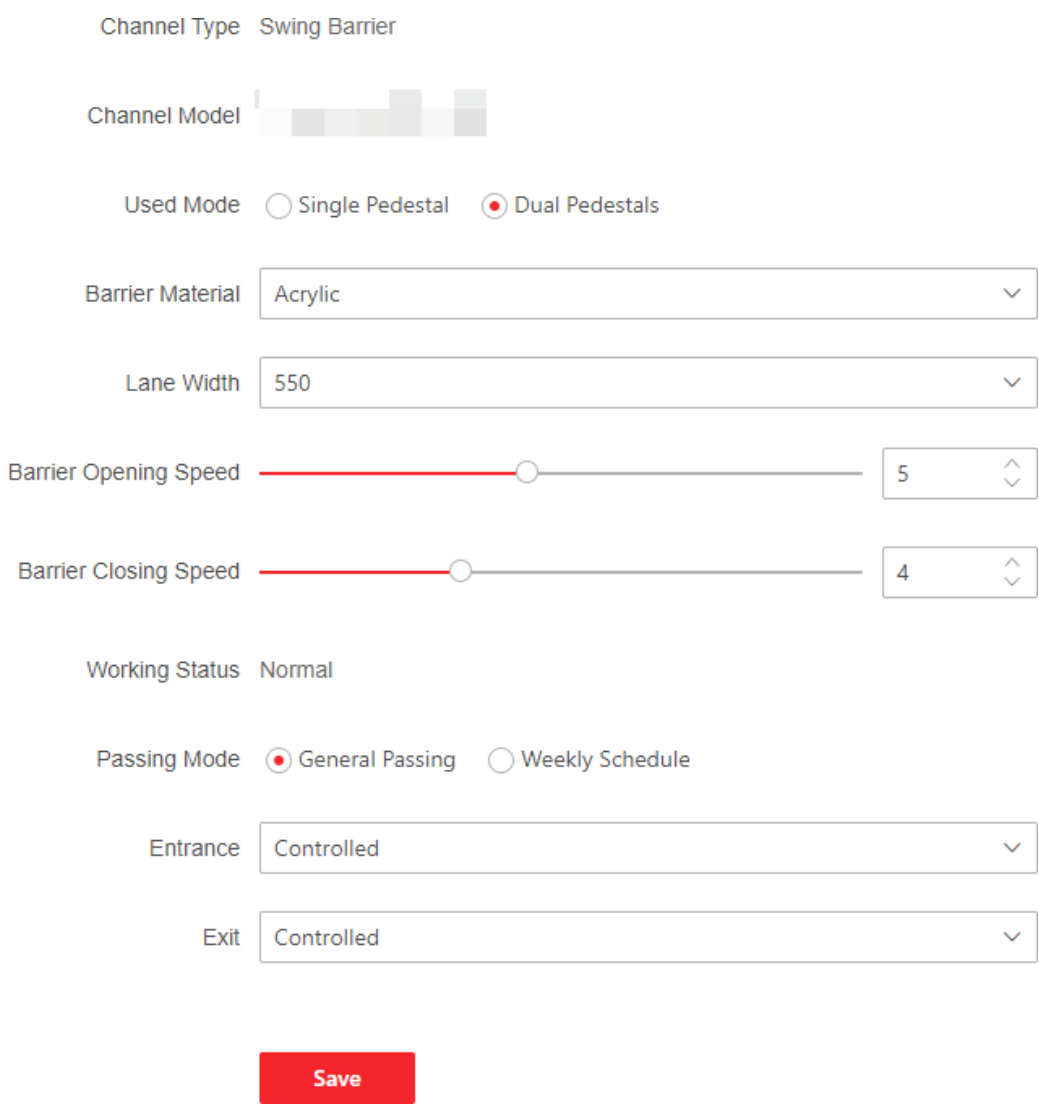


図13-5 基本パラメータ

2. **チャネルタイプ**、**チャネルモデル**、**動作状態**を表示します。
3. **使用モード**、**バリア材質**、**レーン幅**、**バリア開放速度**、**バリア閉鎖速度**を設定します。

使用モード

実際のニーズに応じて、**シングルペデスタル**または**デュアルペデスタル**を選択してください。

シングルペデスタル

ペデスタルを1台のみ使用する場合は、このオプションを選択してください。

デュアルペデスタル

デュアルペデスタルのみを使用する場合、このオプションを選択してください。

注記
製品が本機能をサポートしているかどうかは、具体的なモデルに基づいて確認してください。

バリア材

実際の状況に応じてバリア素材を選択してください。

レーン幅

実際の状況に応じてレーン幅を選択してください。

バリア開閉速度

バリアの開閉速度を設定します。

4. 通行モードを設定します。
- **一般通行**を選択した場合、入口と出口のバリア状態をドロップダウンリストから選択できます。
- **「週間スケジュール」**を選択した場合、入退場バリアの週間スケジュールを設定できます。

5. **入口**と**出口**の状態を設定します。

6. **保存**をクリックします。

13.8 システムとメンテナンス

システム情報と容量を確認できます。また、デバイスのアップグレード、工場出荷時設定への復元、デフォルト設定への復元、デバイスの再起動も実行できます。

13.8.1 デバイス情報の表示

デバイス名、言語、モデル、シリアル番号、バージョン、チャンネル数、入出力、警報入力、警報出力、デバイス容量などを表示します。

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

言語、モデル、シリアル番号、バージョン、IO入力、IO出力、アラーム入力、アラーム出力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。**「アップグレード」**をクリックしてファームウェアバージョンをアップグレードします。

デバイス容量（人物、顔、カード、イベント、掌紋）を確認できます。

13.8.2 時刻設定

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

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

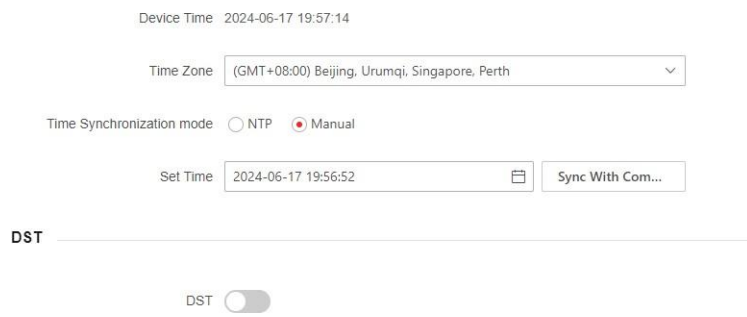


図 13-6 [時間設定]

設定後、**保存**をクリックして設定を保存します。

タイムゾーン

ドロップダウンリストから、デバイスが所在するタイムゾーンを選択します。

時刻同期

NTP

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

手動

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

夏時間

夏時間の開始時刻、終了時刻、およびバイアス時間を設定できます。

13.8.3 管理者のパスワードを変更

手順

1. パスワード変更ページに入ります。

- **システムとメンテナンス → システム構成 → システム → ユーザー管理 → ユーザー管理** をクリックし、 をクリックします。
- ページの右上隅にある「**admin**」→「**パスワードの変更**」をクリックします。

2. 古いパスワードを入力し、新しいパスワードを作成してください。

3. 新しいパスワードを確認してください。

4. **保存**をクリックしてください。

ご注意

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

13.8.4 オンラインユーザー

デバイスにログインしているユーザーの情報が表示されます。

オンラインユーザーの一覧を表示するには、**[システムとメンテナンス] → [システム設定] → [システム] → [ユーザー管理] → [オンラインユーザー]** に移動します。

13.8.5 PC Web 経由でデバイスの武装/武装解除情報を表示

デバイスの武装タイプと武装 IP アドレスを表示します。

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

13.8.6 ネットワーク設定

基本ネットワークパラメータの設定

システムとメンテナンス → システム構成 → システム → ネットワーク → ネットワーク設定 → TCP/IP をクリックします。
MAC アドレスと MTU を表示できます。
パラメータを設定し、「**保存**」をクリックして設定を保存します。

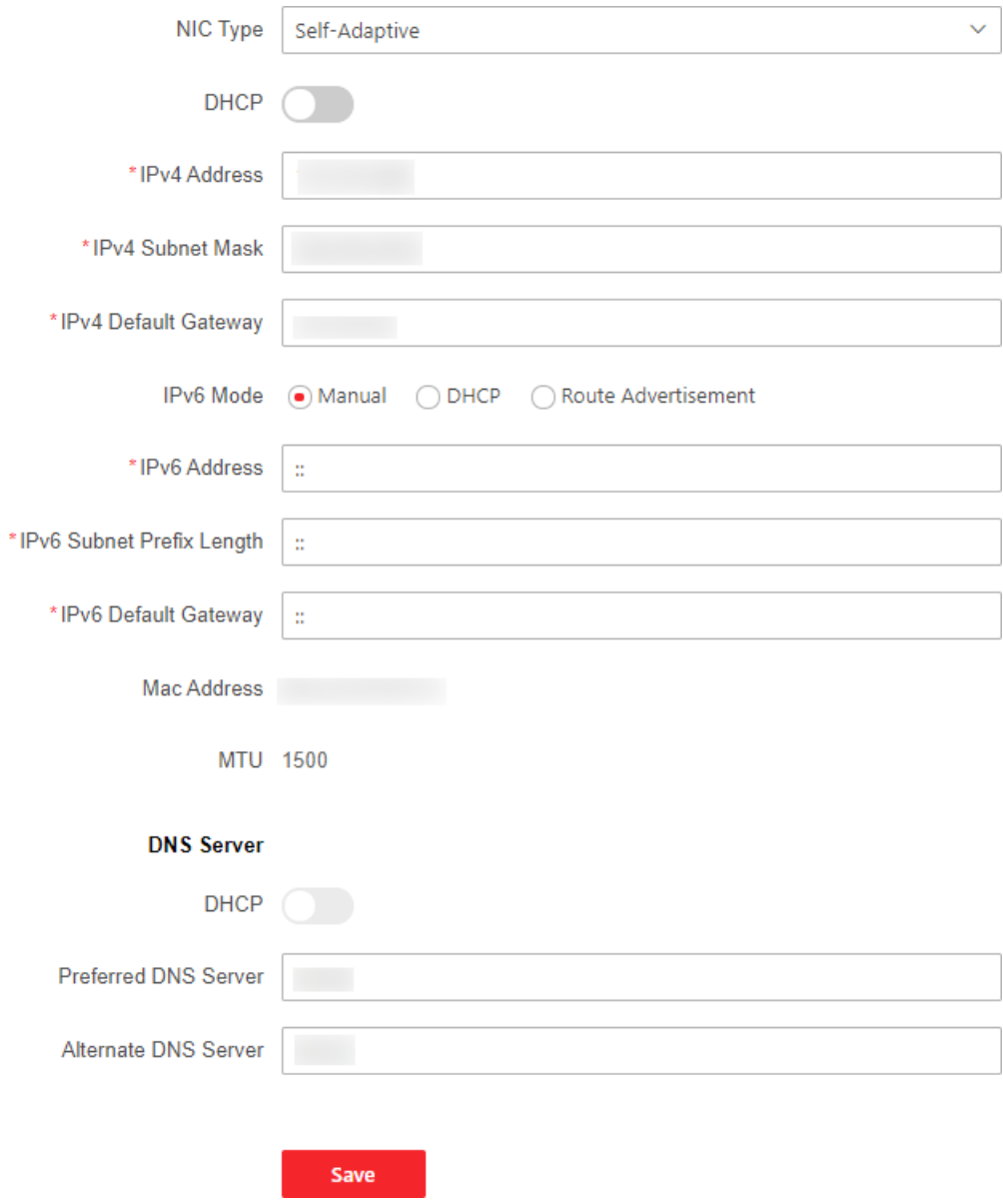


図 13-7 TCP/IP の設定

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

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

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

IPv6モード

手動

IPv6 アドレス、IPv6 サブネットプレフィックス長、IPv6 デフォルトゲートウェイを手動で設定します。

DHCP

システムは、IPv6 アドレス、IPv6 サブネットプレフィックス長、および IPv6 デフォルトゲートウェイを自動的に割り当てます。

ルートアドバタイズメント

IPv6プロトコルスタックにおける自動アドレス設定メカニズム。環境内にルーティング通知メッセージを提供できるルータが存在する場合、デバイスはIPv6アドレス設定を完了できる。

「ルートアドバタイズメントを表示」をクリックすると、IPv6アドレス一覧を表示できます。

DNSサーバー

注記

DHCPが有効な場合のみ、DNSサーバーを設定できます。

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

デバイスのホットスポット

デバイスのホットスポットを設定します。

システムとメンテナンス → システム構成 → ネットワーク → ネットワーク設定 → デバイスホットスポット をクリックします。

デバイスホットスポットを有効にするにはクリックしてください。ホットスポット**名**と**パスワード**を設定します。

保存をクリック。携帯電話でホットスポットに接続し、モバイルウェブでパラメータを設定できます。

PCウェブ経由でポートを設定

システムとメンテナンス → システム構成 → ネットワーク → ネットワークサービス をクリックします。

HTTP

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

HTTPS

ブラウザアクセス用にHTTPSを設定してください。アクセス時には証明書が必要です。

HTTPリスニング

本装置は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へ警報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、プロトコルを編集してください。

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プロトコルをサポートしている必要があります。

システムとメンテナンス → システム設定 → ネットワーク → ネットワークサービス → RTSP をクリックします。

RTSP

リアルタイムストリーミングプロトコルのポートを指します。

PC Web経由でOTAPを設定

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

手順

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

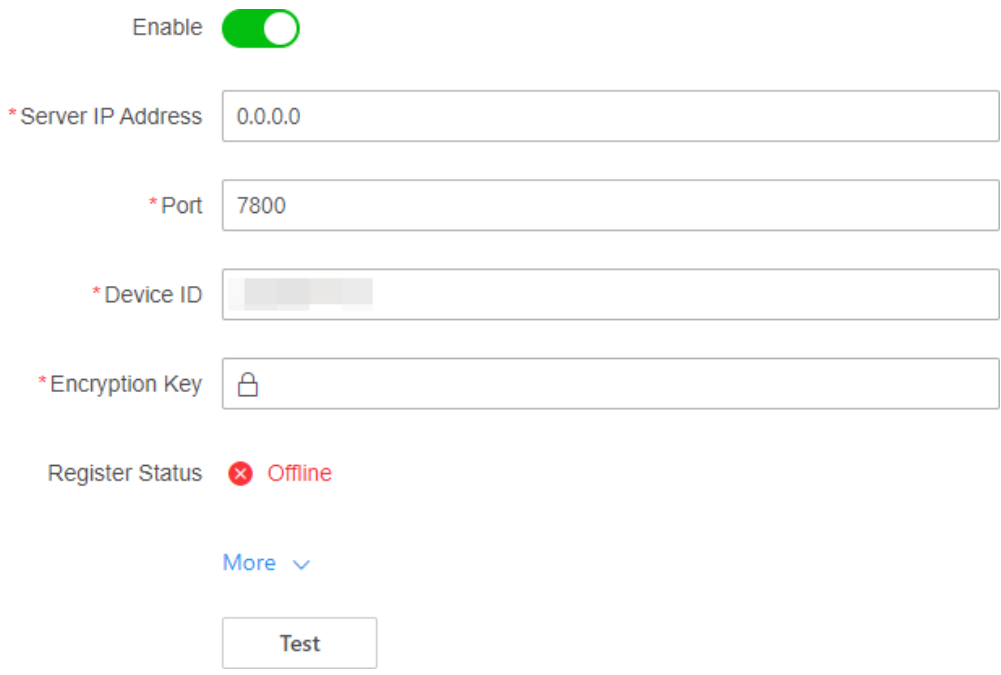


図13-8 OTAPの設定

2. 中央グループを選択します。
3. OTAP を**有効にする**をクリックします。
4. **サーバーIPアドレス、ポート、デバイスID、暗号化キー**を設定します。
5. **[詳細]** をクリックして、ネットワークタイプとアクセスポリシーを表示します。操作アイコンを上下にドラッグして、ネットワークの優先度を調整します。

6. **「テスト」**をクリックし、デバイスがサーバーに接続して正常に登録できることを確認してください。ページを更新するかデバイスを再起動して、**登録ステータスを**確認してください。
7. **保存**をクリックしてください。

PC Web経由のプラットフォームアクセス

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

手順

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

注

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

2. 有効にするには**「有効」**をチェックしてください。
3. **オプション：**「**カスタム**」のチェックボックスをオンにすると、サーバーアドレスを自分で設定できます。
4. 確認コードを入力してください。
5. **オプション：「有効にする」**をチェックしてビデオ暗号化を有効にし、暗号化パスワードを設定して確認します。
6. **「詳細」**をクリックしてネットワークタイプとアクセス優先度を確認します。操作アイコンを上下にドラッグしてネットワーク優先度を調整します。
7. **「表示」**をクリックしてデバイスのQRコードを表示します。QRコードをスキャンしてアカウントを紐付けます。

注意

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

8. 設定を有効にするには「**保存**」をクリックしてください。

13.8.7 シリアルポート設定

シリアルポートのパラメータを設定します。

手順

1. **システムとメンテナンス → システム構成 → アクセス構成 → シリアルポート構成** をクリックします。

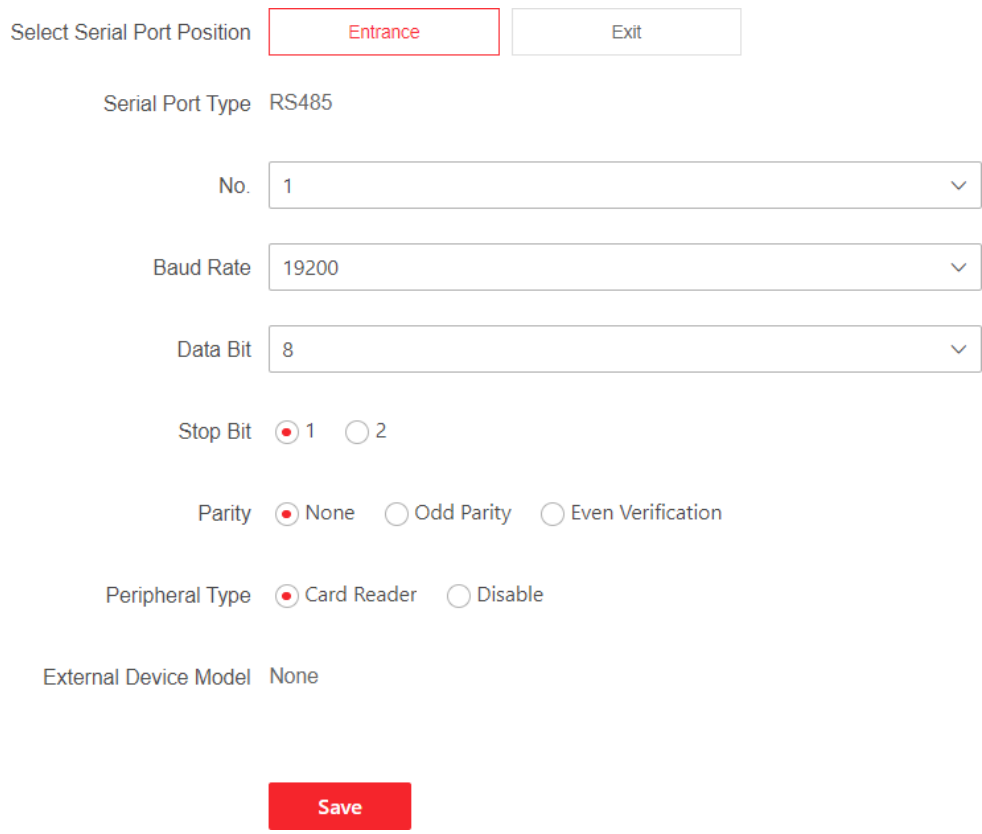


図 13-9 シリアルポート設定

2. シリアルポートの位置を「**入力**」または「**出力**」に設定します。
3. シリアルポート番号を選択すると、対応するシリアルポートタイプが自動的に表示されます。
4. シリアルポートのパラメータを設定します。

ボーレート

データ転送速度を設定します。

データビット

データを送信するビット数を設定します。

ストップビット

1フレームのデータの終了点を選択します。

パリティ

シリアル通信のエラー検出方式を選択します。データビットとチェックビットの1の数が奇数か偶数かを検出するか、チェックビットを使用しないかを選択できます。

5. 接続ポートの**周辺機器タイプ**を設定します。
6. 外部デバイスのモデルを確認できます。
7. **保存**をクリックしてください。

13.8.8 アラーム設定

デバイスのアラーム出力パラメータを設定します。

設定 → イベント → アラーム設定 をクリックします。
有線アラーム出力デバイスの名前を作成し、出力遅延時間を設定します。**保存**をクリックします。

注記
出力遅延は 0 から 5999 の範囲である必要があります。

13.8.9 イベントの連動

イベントに連動するアクションを設定します。

手順

1. ターンスタイル → パラメータ設定 → 連動設定をクリックして設定ページに入ります。

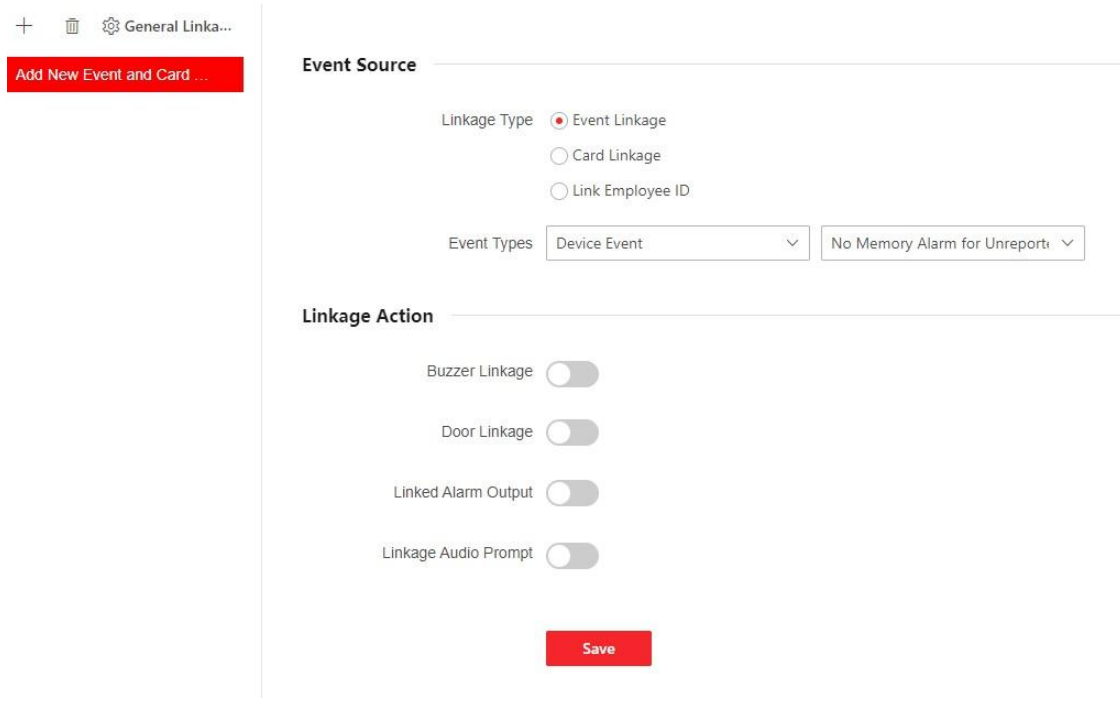


図 13-10 イベント連動

2. 「+」をクリックしてイベントソースを設定します。
- **リンクタイプを**「**イベントリンク**」に設定する場合、ドロップダウンリストからイベントタイプを選択する必要があります。
- **連携タイプ**を**カード連携に**選択した場合、カード番号を入力しカードリーダーを選択する必要があります。

- **連携タイプ**を「**従業員ID連携**」に選択した場合、従業員IDを入力し、カードリーダーを選択する必要があります。

3. 連携アクションを設定します。

ドア連動

ドア連動を有効にし、対象イベントのドア状態を「入室」および「**退室**」に設定します。

連動警報出力

連動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** をチェックして、対象イベントのアラーム出力ステータスを設定します。

連動音声プロンプト

リンクされた音声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**、言語を設定し、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を選択した場合**、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、**一般リンク設定**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。

リンクキャプチャ

リンクキャプチャを有効にし、ターゲットイベントのキャプチャ対象として「入室」または「退室」を選択します。

13.8.10 アップグレードとメンテナンス

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

デバイスの再起動

システムとメンテナンス → メンテナンス → 再起動をクリックします。**再起動**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

システムとメンテナンス → メンテナンス → アップグレード をクリックします。

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てください。［ ］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てください。［**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。

パラメータの復元

システムとメンテナンス → メンテナンス → バックアップとリセット をクリックします。

すべて復元

すべてのパラメータが工場出荷時の設定に復元されます。使用前にデバイスをアクティベートしてください。

復元

ネットワークパラメータとユーザー情報を除き、デフォルト設定に復元されます。

インポートとエクスポートのパラメータ

システムとメンテナンス → メンテナンス → バックアップとリセット をクリックします。

エクスポート

デバイスパラメータをエクスポートするには、**[エクスポート]**をクリックします。

注記

エクスポートしたデバイスパラメータ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。**Import**をクリックして設定ファイルのインポートを開始します。

13.8.11 デバイスのデバッグ

デバイスのデバッグパラメータを設定できます。

手順

1. **システムとメンテナンス → メンテナンス → デバイスデバッグ** をクリックします。
2. 以下のパラメータを設定できます。

レーン学習/モーター自己診断 SSHを有効化

ネットワークセキュリティを強化するため、SSHサービスを無効化してください。この設定は専門家によるデバイスのデバッグ専用です。

モーター学習＆自己診断レーン学習

[開始]をクリックすると、デバイスは学習モードに入ります。バリアの閉位置を学習します。

モーター自己診断

スタートをクリックすると、モーターが自動的に動作状態をテストします。

エンコーダ自己診断

チャンネル（レーン）を選択し、**「スタート」**をクリックすると、選択したレーンのエンコーダが自動的に動作状態をテストします。

IR セルフテスト

赤外線自己診断機能を有効にした後、開閉前に装置が音でチャネル（レーン）退出を通知します。バリアは最高速度で入退場時に強制開放されます。

速度で強制的に開きます。この時、IR挟み込み防止機能は無効となります。IRが作動または遮断された場合、装置は検知失敗を音で通知します。

レーンを選択し、**IRセルフテスト**をタップすると、装置はすべてのIR検出器をテストします。

注意

レーン内に人がいないことを確認してください。

ログを印刷

エクスポートをクリックするとログをエクスポートできます。

ネットワークパケットのキャプチャ

パケットキャプチャの継続時間と**サイズ**を設定し、「**キャプチャ開始**」をクリックしてキャプチャを実行**できます**。

デバッグコマンド管理

クイックコマンドのコマンドタイプを選択するか、**カスタムコマンドの内容**を入力します。

ドロップダウンリストからボードタイプを選択し、「**送信**」をクリックしてデバッグコマンドを送信します。「**実行結果**」でデバイスが受信したコマンド情報を確認できます。

デバッグ終了をクリックすると、デバイスは通常の動作状態に戻ります。

注記

- デバイスの性能を確保するため、デバッグコマンドを終了するには「**デバッグ終了**」をクリックしてください
- **デバッグ終了**をタップしない場合、デバイスは7×24時間以内に自動的にデバッグモードを終了します。

IR例外情報

例外的な赤外線検出器レポートをエクスポートするには、「**エクスポート**」をクリックしてください。

デモモード

有効化後、デバイスは顔認識後に自動的に追加および認証を行います。有効期間を設定できます。

無効にした場合、デモモードで追加されたすべての個人情報は無効化後に消去されます。

PC Web経由でネットワークパケットをキャプチャ

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

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

PC Web経由でのプロトコルテスト

プロトコルアドレスを選択し、テストするプロトコルを入力します。応答ヘッダーと返り値に基づいてデバイスのデバッグが可能です。

システムとメンテナンス → メンテナンス → デバイスデバッグ → プロトコルテスト に移動します。

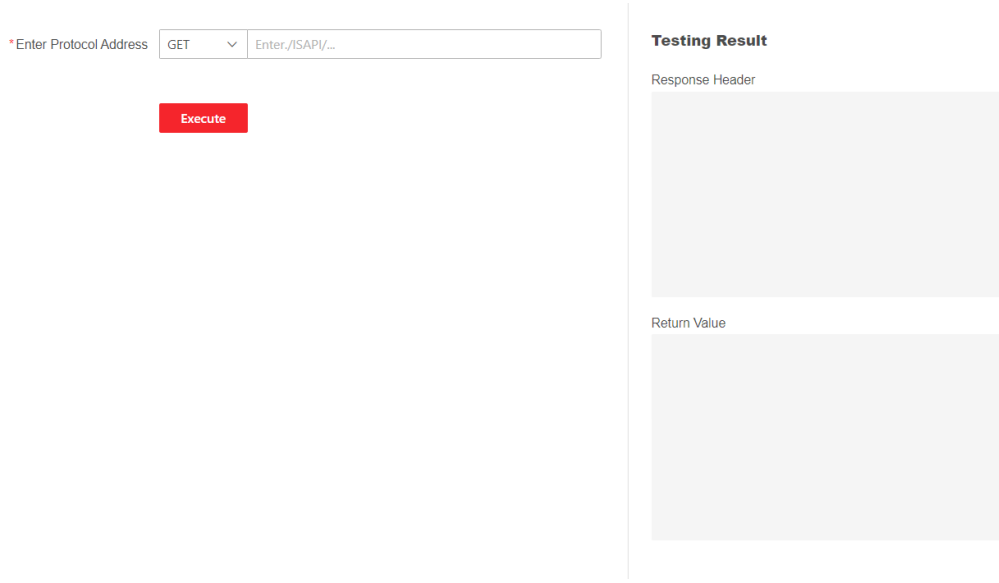


図13-11 プロトコルテスト

プロトコルアドレスを選択し、プロトコルを入力します。**実行**をクリックします。

応答ヘッダーと返り値に基づいてデバイスをデバッグします。

PC Web経由でネットワーク侵入サービスを設定

デバイスがLANに展開されている場合、侵入サービスを活用してデバイス遠隔管理を実現できます。

手順

1. **システムとメンテナンス → メンテナンス → デバイスデバッグ → ネットワーク侵入サービス** に移動します。
2. **「侵入サービス有効化」**をスライドします。
3. **サーバーIP**アドレスと**サーバーポート**を設定します。**ユーザー**名と**パスワード**を作成します。
4. **オプション：ハートビートタイムアウト**を設定できます。設定範囲は1～6000です。
5. **オプション：**侵入サービスのステータスを確認できます。ステータスを更新するには**「更新」**をクリックします。
6. **保存**をクリックします。

注意

ペネトレーションサービスは48時間後に自動無効化されます。

13.8.12 コンポーネントの状態

各種コンポーネントの状態を確認できます。

メインレーン状態

デバイスコンポーネント

アクセス制御ボード、レーン制御ボードなどのステータスを確認できます。

周辺機器

RS-485 カードリーダーの状態を確認できます。

温度

台座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。

その他

通過モード

入退場モードを確認できます。

入力および出力ステータス

イベント入力、警報出力、火災警報の状態を確認できます。

その他の状態

バリアおよびキーフォブ受信モジュールの状態を確認できます。

13.8.13 PC Web経由でのログ閲覧

デバイスのログを検索・閲覧できます。

システムとメンテナンス → メンテナンス → ログ に移動します。

ログタイプのメジャータイプとマイナータイプを設定します。検索の開始時間と終了時間を設定し、**検索**をクリックします。

結果は以下に表示されます。これには、番号、時刻、主要タイプ、副次タイプ、チャネル番号、ローカル/リモートユーザー情報、リモートホストIPなどが含まれます。

13.8.14 証明書管理

サーバー/クライアント証明書および CA 証明書の管理に役立ちます。

注記
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。

HTTPS証明書の作成とインポート

手順

1. **システムとメンテナンス → 安全 → 証明書管理** に移動します。
2. **HTTPS 証明書**エリアで、**[証明書要求の作成]** をクリックします。
3. 証明書情報を入力し、「**保存**」をクリックします。
   - 「**表示**」をクリックすると、作成された証明書が表示されます。
   - 証明書は自動的に保存されます。
4. 証明書をダウンロードし、ローカルコンピュータの要求ファイルに保存します。
5. 要求ファイルを認証機関に送信し、署名を受け取ります。
6. 署名済み証明書をインポートします。
   1) **[キーのインポート]** 領域で、ローカルから証明書を選択し、**[インポート]** をクリックします。
   2) **インポート通信**証明書領域で、ローカルから証明書を選択し、
      インポートをクリックします。

SYSLOG証明書の作成とインポート

手順

1. **システムとメンテナンス → 安全 → 証明書管理** に移動します。
2. **SYSLOG 証明書**エリアで、**[証明書要求の作成]** をクリックします。
3. 証明書情報を入力し、「**保存**」をクリックします。
   - 「**表示**」をクリックすると、作成された証明書が表示されます。
   - 証明書は自動的に保存されます。
4. 証明書をダウンロードし、ローカルコンピュータの要求ファイルに保存します。
5. 要求ファイルを認証機関に送信し、署名を受け取ります。
6. 署名済み証明書をインポートします。
   1) **[キーのインポート]** 領域で、ローカルから証明書を選択し、**[インポート]** をクリックします。
   2) **通信証明書のインポート**領域で、ローカルから証明書を選択し、[インポート] をクリックします。
      インポートをクリックします。

CA証明書のインポート

開始前に

CA 証明書を事前に準備してください。

手順

1. **システムとメンテナンス → セキュリティ → 証明書管理** に移動します。
2. **CA**証明書ID領域でIDを作成します。

   注記

   入力する証明書 ID は、既存のものと同じにすることはできません。

3. ローカルから証明書ファイルをアップロードします。
4. **インポート**をクリックします。

第14章 その他の設定プラットフォーム

iVMS-4200 クライアントソフトウェアまたは HikCentral アクセス制御を介してデバイスを設定することもできます。詳細については、各プラットフォームのユーザーマニュアルを参照してください。

iVMS-4200 クライアントソフトウェア

クライアントソフトウェアのユーザーマニュアルを表示するには、リンクをクリック/タップしてください。

http://enpinfodata.hikvision.com/analysisQR/showQR/ca930247

付録A. 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
テールゲティング	視覚的および聴覚的
逆方向通過	視覚的および聴覚的
強制アクセス	なし
障壁越え	視覚的および聴覚的
滞在超過	視覚的および聴覚的
タイムアウト経過	なし
侵入	視覚および聴覚
バリア遮断	なし

付録B. 法的情報

本ドキュメントについて

- 本ドキュメントには、製品の使用および管理に関する指示が含まれています。以下に示す写真、図表、画像、およびその他すべての情報は、説明および解説のみを目的としています。
- 本ドキュメントに記載されている情報は、ファームウェアの更新その他の理由により、予告なく変更される場合があります。最新バージョンのドキュメントは、Hikvision ウェブサイト (***https://www.hikvision.com***) でご確認ください。別段の合意がない限り、杭州 Hikvision デジタルテクノロジー株式会社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。
- 本製品をサポートする訓練を受けた専門家の指導と支援のもとで、この文書をご利用ください。

本製品について

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

知的財産権に関する承認

- Hikvision は、本書に記載された製品に組み込まれた技術に関連する著作権および/または特許を所有しており、これには第三者から取得したライセンスが含まれる場合があります。
- 本ドキュメントのテキスト、画像、グラフィック等を含む一切の部分は、Hikvisionに帰属します。書面による許可なく、本ドキュメントの一部または全部を、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Hikvisionの商標およびロゴは、各管轄区域においてHikvisionの所有物です。
- 記載されているその他の商標およびロゴは、それぞれの所有者に帰属します。

免責事項

- 適用される法律で許容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（そのハードウェア、ソフトウェア、ファームウェアを含む）は、「現状有姿のまま」かつ「すべての欠陥およびエラーを含むまま」提供されます。Hikvision は、明示または黙示を問わず、いかなる保証も行いません。

明示的、黙示的を問わず、商品性、満足のいく品質、特定目的への適合性を含むがこれらに限定されない一切の保証を否認します。 本製品のご利用はお客様ご自身の責任において行ってください。いかなる場合においても、HIKVISIONは、特別損害、結果的損害、付随的損害、間接損害（事業利益の損失、事業中断、データ損失、 システムの破損、または文書の損失を含むがこれらに限定されない損害について、契約違反、不法行為（過失を含む）、製造物責任その他のいかなる法的根拠に基づくものであっても、本製品の使用に関連して生じた場合、HIKVISIONがそのような損害または損失の可能性について事前に通知されていた場合であっても、一切の責任を負いません。

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

データ保護

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