DS-K3BC430LXシリーズ スイングゲート

UD32855B

製品仕様

本ドキュメントについて

- 本ドキュメントには、製品の使用および管理に関する説明が含まれています。以下に掲載されている写真、図表、画像、およびその他すべての情報は、説明および解説のみを目的としています。
- 本ドキュメントに含まれる情報は、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***）でご覧ください。別段の合意がない限り、杭州海康威視数字技術有限公司またはその関連会社（以下「Hikvision」）は、明示または黙示を問わず、いかなる保証も行いません。
- 本ドキュメントは、本製品のサポートに関する訓練を受けた専門家の指導および支援のもとでご使用ください。

本製品について

- 本製品は、購入された国または地域でのみアフターサービスサポートを受けることができます。
- お選びいただいた商品が動画商品の場合、下記のQRコードをスキャンして「動画商品の利用に関する取り組み」を取得し、必ずお読みください。

知的財産権に関する承認

- Hikvision は、本書に記載された製品に組み込まれた技術に関連する著作権および/または特許を所有しており、これには第三者から取得したライセンスが含まれる場合があります。
- 本文書のテキスト、写真、グラフィックなど、その一部はすべて Hikvision に帰属します。書面による許可なく、本文書のいかなる部分も、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 Hikvision の商標およびロゴは、さまざまな法域における Hikvision の所有物です。
- 記載されているその他の商標およびロゴは、それぞれの所有者に帰属します。

法的免責事項

- 適用される法律で許容される最大限の範囲において、本書および記載された製品（ハードウェア、ソフトウェア、ファームウェアを含む）は「現状有姿のまま」かつ「あらゆる欠陥およびエラーを含む状態で」提供されます。 HIKVISIONは、商品性、満足のいく品質、特定目的への適合性を含むがこれらに限定されない、明示的または黙示的な保証を行いません。 本製品の使用は、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、たとえ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。
- 本文書と適用される法律との間に矛盾が生じた場合は、後者が優先する。

データ保護

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

管理措置の実施、セキュリティ管理の有効性に関する定期的な見直しと評価の実施など。

規制情報

FCC 情報

コンプライアンスの責任者が明示的に承認していない変更または改造は、ユーザーによる機器の操作権限を無効にする可能性があることにご留意ください。

FCC準拠：本機器は、FCC規則第15部に準拠し、クラスBデジタル機器の制限値に適合することが試験により確認されています。これらの制限値は、住宅環境における有害な干渉から合理的な保護を提供するために設計されています。本機器は無線周波エネルギーを発生・使用し、放射する可能性があります。取扱説明書に従って設置・使用されない場合、無線通信に有害な干渉を引き起こす恐れがあります。 ただし、特定の設置環境において干渉が発生しない保証はありません。本機器がラジオやテレビの受信に有害な干渉を引き起こしている場合（機器の電源をオフにしてからオンにすることで確認可能）、ユーザーは以下の対策のいずれかまたは複数を試み、干渉の解消を図ることを推奨します：

–受信アンテナの方向や設置場所を変更する。

–本機器と受信機の間隔を広げる。

–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本機器を接続する。

–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

本機器は、放射器と身体の間に最低20cmの距離を保って設置・操作してください。

FCC条件

本装置はFCC規則第15部に準拠しています。以下の2条件に従って動作します：

1. 本装置は有害な干渉を引き起こしてはなりません。

2. 本装置は、受信したあらゆる妨害（意図しない動作を引き起こす可能性のある妨害を含む）を受け入れる必要があります。

EU適合宣言

本製品および付属品（該当する場合）には「CE」マークが付けられております、EMC指令2014/30/EU、RE指令2014/53/EU、RoHS指令2011/65/EU

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

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

安全上の注意

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

注意事項は「危険」と「注意」に分類されます：

危険：警告を無視すると、重傷または死亡事故を引き起こす可能性があります。

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

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

⚠危険：

- すべての電子機器の操作は、お住まいの地域の電気安全規制、防火規制およびその他の関連規制を厳守してください。
- 通常の会社から提供されている電源アダプターをご使用ください。消費電力は要求値を下回ってはいけません。
- 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恐れがあります。
- 配線、設置、または分解を行う前に、電源が切断されていることを必ず確認してください。
- 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。
- 本機から煙、異臭、異音が発生した場合は、直ちに電源を切り、電源プラグを抜いてください。その後、サービスセンターまでご連絡ください。
- 電池を飲み込まないでください。化学火傷の危険があります。本製品にはコイン型電池が含まれています。コイン型電池を飲み込むと、わずか2時間で重度の内部やけどを引き起こし、死に至る可能性があります。新品・使用済み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・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：

- 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製品の清掃と手入れを行ってください。毎月1回の清掃をお勧めします。
- 本装置を落下させたり物理的な衝撃を与えたりせず、高電磁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可能性のある場所への設置は避けてください（不注意による装置損傷の原因となります）。
- 極端な高温（詳細な動作温度は装置仕様を参照）、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。
- 屋内用機器カバーは雨や湿気を避けてください。
- 機器を直射日光、換気の悪い場所、ヒーターやラジエーターなどの熱源にさらさないでください（火災の危険があります）。
- 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。
- バッテリー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。使用済みバッテリーはメーカーの指示に従って廃棄してください。
- 生体認証製品は、完全ななりすまし防止環境を保証するものではありません。より高いセキュリティレベルが必要な場合は、複数の認証モードを併用してください。
- デバイスが再起動中はレーンに留まらないでください。
- 誤ったタイプのバッテリーに交換すると爆発の危険性があります。使用済みバッテリー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。
- 本取扱説明書では、機器保護接地導体を設備保護接地導体に接続することを要求します。

利用可能なモデル

製品名	モデル
スイングゲート	DS-K3BC430LX

内容

1 概要

1.1 はじめに

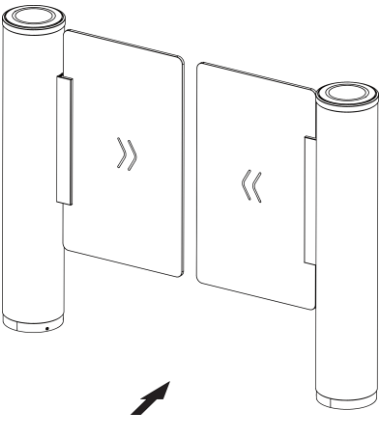


図 1-1 外観

1.2 主な特徴

- 入口・出口双方向で制御モード、常開モード、常閉モードをサポート。
- 自己検出、自己診断、自動警報
- 火災警報通過
  火災警報が作動すると、緊急避難のためバリアは自動的に開きます。
- 有効通行時間の設定
  有効通過時間内にレーンを通過しなかった場合、システムは通過許可をキャンセルします。
- 双方向（入退場）レーン
  バリアの開閉速度は、訪問者の流れに応じて設定できます。
- TCP/IP ネットワーク通信
  通信データは特別に暗号化されており、プライバシー漏洩の懸念を軽減します。
- キーフォブによる遠隔バリア開閉、スピーカーによる放送（アクセス制御ボードと併用時はカスタム放送内容に対応）。

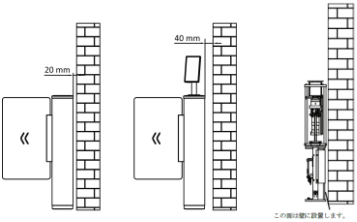
2 システム配線

設置前の準備と一般的な配線。

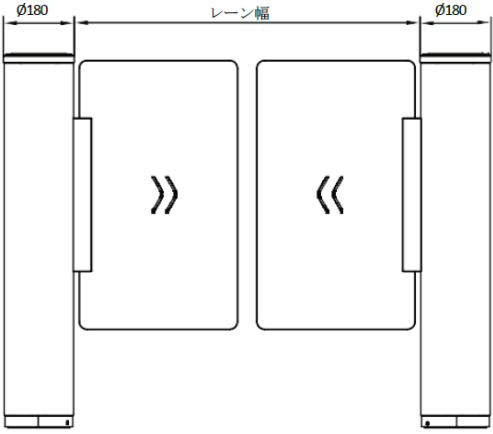
手順

注記

- 本装置はコンクリート面またはその他の平坦な不燃性表面に設置してください。
- 設置場所が壁に近すぎる場合は、台座と壁の間の距離が 20 mm 以上（顔認識端末付きの場合は 40 mm 以上）であることを確認してください。そうしないと、台座の上部パネルを開けられない、またはデバイスが損傷するおそれがあります。



- 寸法は以下の通りです。



単位：mm

図 2-1 寸法

1. 左または右の台座の設置面に中心線を描きます。

2. 他の台座を設置するために、他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 + 180 mmです。Lは車線幅を表します。

3. 設置面には溝を設け、設置穴を掘削する。各支柱にはM12*150の拡張ボルトを3本取り付ける。

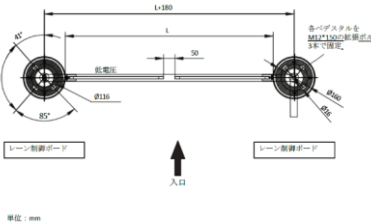


図2-2 穴位置とシステム配線

4. ケーブルを埋設します。

注記

- 相互接続ケーブル（2基以上の台座で使用可能）：推奨長さはL+1.5 mです。
  ネットワーク通信ケーブル：CAT5e またはそれ以上の性能のネットワークケーブルの使用を推奨します。
- 推奨される低電圧導管の外径は30mmです。
- 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する必要があります。
- 穴を掘る前に、設置面の厚さを評価し、貫通を避けるようにしてください。
- 設置面に溝を切る際は、バリアの位置ずれを防ぐため、溝の位置と幅に注意してください。
- 1台の配電キャビネットは1基のペデスタルに供給します。
  電源ケーブルの最大許容直径は12AWG（UL1015）で、伝送距離は100mです。
  1つの配電キャビネットは2つのペデスタルに供給します。
  電源ケーブルの最大許容直径は16AWG（UL1015）で、伝送距離は25mです。

3 ペデスタルの設置

始める前に
設置工具を準備し、装置と付属品を確認し、設置場所を片付けてください。

手順

注意

- 設置図はイメージです。詳細は「***配線***に関するビデオガイド」を参照してください。
- 装置はコンクリート面またはその他の平坦な不燃性表面に設置してください。
- 設置およびその他の操作中は、必ず装置の電源を切ってください。
- 設置工具は台座のパッケージ内に同梱されています。

- 施工中の汚れによるステンレス鋼の錆発生を防ぐため、設置完了後に保護フィルムを剥がすことを推奨します。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。フィルム剥離後はWD-40保護液で拭き取ることを推奨します。
- スリーブの取り付けには、少なくとも2名での共同作業をお勧めします。作業中は手袋を着用し、慎重に取り扱い、挟み込みや圧迫による負傷に十分注意してください。

---

1. 取り付け工具を準備し、部品を確認し、設置基盤を整えてください。

2. 台座底部は防水材で密封し、水溜りを防止してください。

3. 装置上部の保護パネルを取り外し、デフォルトのバリア開放方向マークに従ってバリアの方向と台座の設置位置を決定してください。

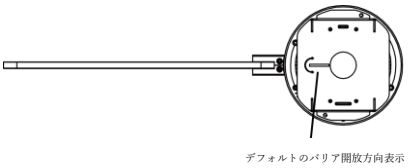


図3-1 既定のバリア開方向マーク

注記

台座を水に浸さないでください。特別な状況下では、浸漬高さは150mmを超えてはいけません。底面回路基板は浸漬できません。

---

4. 十字ドライバーを使用して、装飾リングとケーブル保護パネルのネジを取り外し、配線を完了してください。

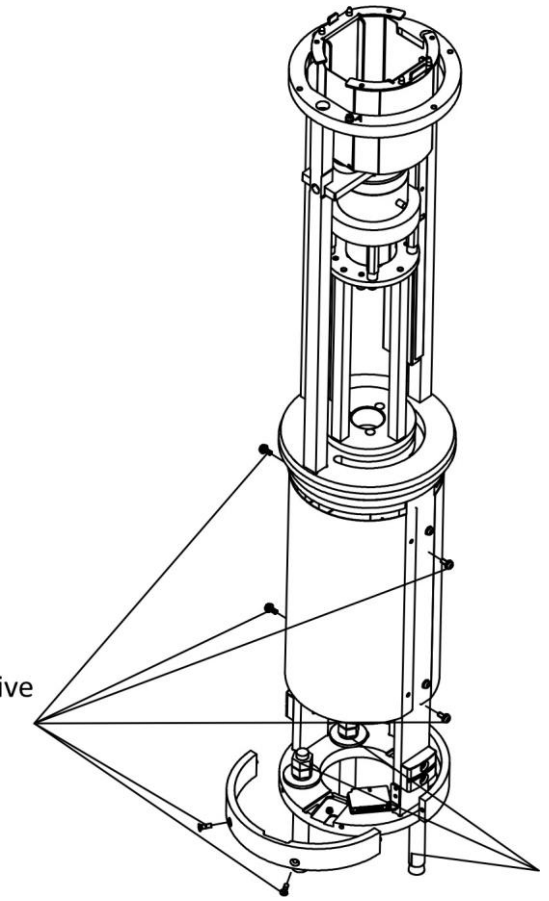


図 3-2 装飾リングとケーブル保護パネルの取り外し

5. 十字ドライバーを使用して上部プラスチック部品を固定し、六角レンチを使用して回転チューブを固定します。

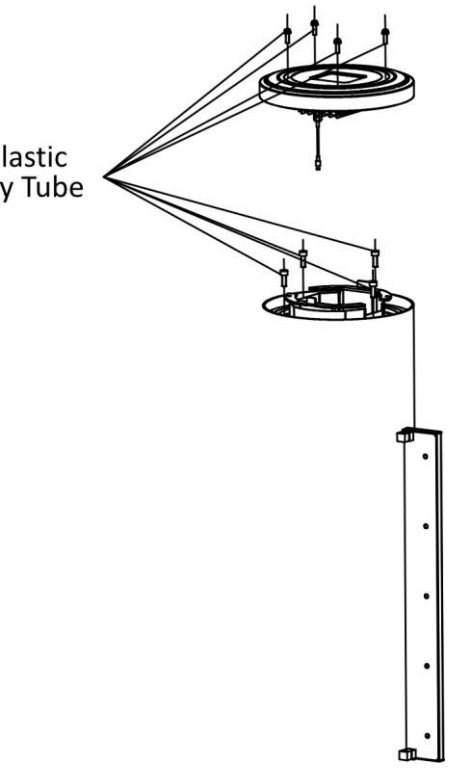


図3-3 上部プラスチック部品と回転チューブの固定

6. バリアと装飾部品を固定する。

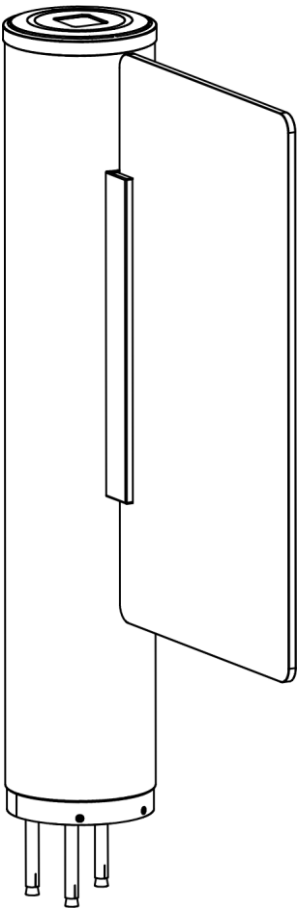


図3-4 バリアの固定

4 一般的な配線

注記

- 付属の相互接続ケーブルは、現場で接続する必要があります：CAT5e 通信ケーブル。ケーブルの長さは 3 m で、パッケージ内に収められています。

4.1 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。

注記

電源：24 V DC

電源電圧変動範囲：±5%

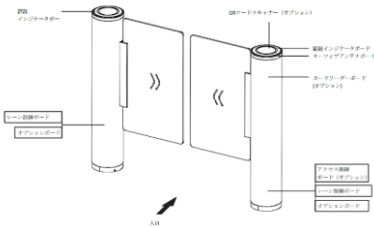


図4-1 構成部品紹介

4.2 配線

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。

4.3 端子説明

4.3.1 一般配線

レーン制御ボード、アクセス制御ボード、オプションボードの一般的な配線。

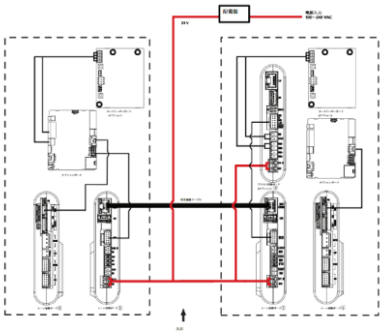


図 4-2 一般的な配線

注記

- AC 電源を 24 V に変換するには、Hikvision 対応の分配キャビネット（別売）の使用を推奨します。
- ①と②は同一基板の両面を指します。
- 入口/出口でバリアが開く場合：BTN1/BTN2 および GND に接続してください。

4.3.2 レーン制御ボード端子説明

レーン制御ボードには、表示板インターフェース、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、12VDC出力インターフェース、24VDC入力インターフェース、通信インターフェース、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、ブレーキインターフェース、および改ざん検知インターフェースが含まれます。

下図はレーン制御基板の配線図を示す。

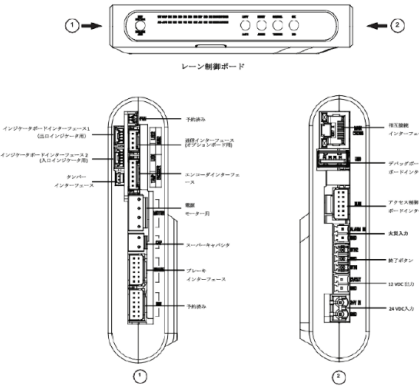
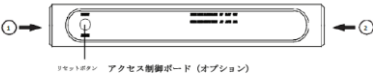


図4-3 レーン制御ボード

4.3.3 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、上位プラットフォームおよびレーンコントローラとの通信に使用されます。



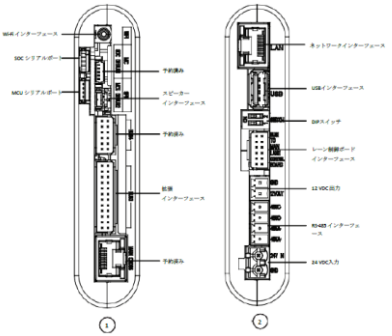


図4-4 アクセス制御ボード

注記

- RS-485A は Web 上の UART 5 に対応し、デフォルトでは入口の QR コードスキャナ接続用です。RS-485C は Web 上の UART 7 に対応し、デフォルトでは入口のカードリーダー接続用です。
- SOC および MCU のシリアルポートは、メンテナンスおよびデバッグ専用です。
- リセットボタンを 5 秒間押し続けると、デバイスは工場出荷時の設定に復元されます。
- DIP スイッチは学習モード設定とキーフォブペアリング用です。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拡張インターフェースの配線図は下記の通りです。

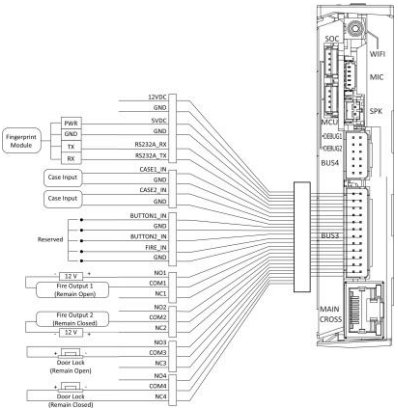


図4-5 BUS3インターフェースの配線図

注記

RS-232A は Web 上の UART 1 に対応します。

4.3.4 オプションボード端子説明

オプションボードには、サブ 1G アンテナインターフェース、485/232 インターフェース、12 V 出力インターフェース、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、BUS インターフェース、5 VDC 出力、および通信インターフェースが含まれています。

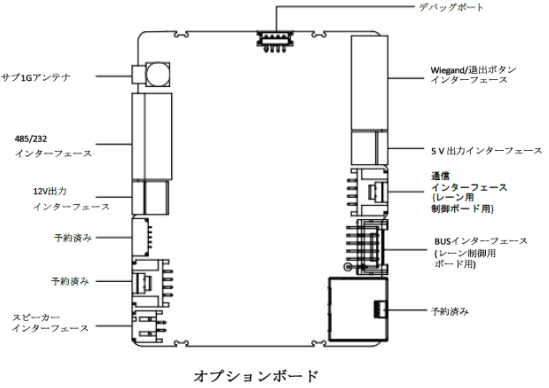


図 4-6 オプションボード端子

4.3.5 カードリーダーボード端子説明

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。

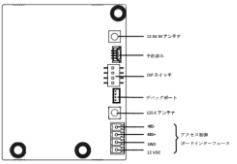


図 4-7 カードリーダーボード

4.3.6 RS-485 配線

アクセス制御ボードおよびオプションボードの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との接続が推奨されます。ここではカードリーダーとの接続を例に説明します。

注意

- アクセス制御ボードには入館用として2つのRS-485インターフェースがあります。詳細は「***アクセス制御ボード端子説明（オプション）***」を参照してください。オプションボードには出口用RS-485インターフェースが2つあります。詳細は該当資料を参照してください。
- 他のRS-485デバイスを接続する場合、RS-485のIDが競合しないようにしてください。
- 顔認証端末の接続済み12V電源インターフェースは、他の12V機器と接続できません。

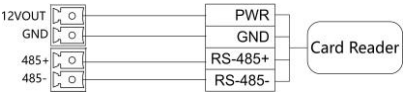


図 4-8 RS-485 配線

4.3.7 RS-232 配線

注記

- 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。
- オプションボードには 1 つの RS-232 インターフェースがあります。RS-232B は、Web 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済みです。

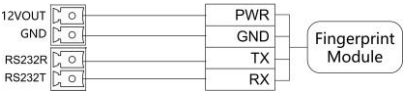


図 4-9 RS-232 配線

4.3.8 アラーム入力配線

メインレーン制御盤では、火災警報入力インターフェースを配線できます。

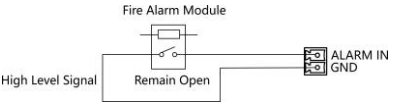


図4-10開放状態を維持

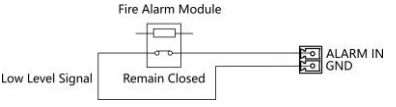


図4-11 閉鎖状態を維持

4.3.9 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、退出ボタンまたは顔認証装置に接続できます。

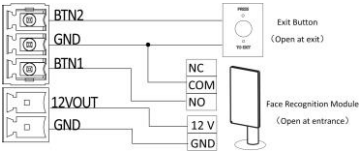


図 4-12 退出ボタン配線

注記

- 顔認識装置は、メインレー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給電されます。
- 入口のバリアが開いている場合：BTN1とGNDに接続。
- 出口のバリアが開いている場合：BTN2とGNDに接続。

4.4 ボタンによるデバイス設定

レーン制御ボード上のボタンでデバイスを設定できます。

注記

- 詳 細 については、***ボタン設定の説明***を参照してください。
- オプショ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「59」が表示されますが、デバイスは正常に機能します。
- メインレーンでは、デフォルトで画面に「99」が表示されます。サブレーンでは、デフォルトで画面に「00」が表示されます。

4.4.1 ボタンによる設定

ボタン説明

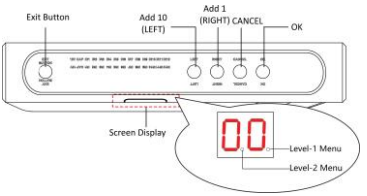


図 4-13 ボタン

出口ボタン

- 押すと、バリアが入口位置から開きます。
- ダブルプレスで出口位置からバリアを開きます。

パラメータ設定ボタン

- LEFT：設定データに 10 を加算します。
- RIGHT：設定データを 1 加算します。
- CANCEL：レベル1メニューに戻る、またはレベル1メニューを終了します。
- OK：設定を確認、設定モードに入る、レベル 2 メニューに入る。

注記

- 設定番号は2つ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、レベル1メニューを示します。数字は設定番号を表します。
- レベル2メニュー：中央の小数点が点灯している場合、レベル2メニューを示します。数字は設定番号を表します。

ボタン設定手順

ここでは侵入検知持続時間を12秒に設定する例を示します：

図4-14 手順

手順：

1. OKボタンを3秒間押し続け、ビープ音が1回鳴るまで保持します。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。表示画面に設定番号**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、**キャンセル**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を終了します。

3. レベル2メニュー進入後、**左**（＋10）を1回、**右**（＋1）を2回押して設定番号を12に設定。**OK**を押して設定を保存。**またはCANCEL**を押して現在のメニューを終了、もしくは5秒間操作なしの場合設定をキャンセルし現在のメニューを終了。

注意

- 設定番号は循環表示されます。
- 各設定番号は機能に対応しています。設定番号と関連機能の詳細については、「***ボタン設定説明***」を参照してください。

4.4.2 ボタンでスタディモードを設定

ボタン設定により学習モードに入り、装置バリアの閉位置を設定します。

手順

注意

- ボタンの操作の詳細については、「***ボタンによる設定」を***参照してください。
- 設定番号とその関連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。

1. 研究モードに入ります。

1) 設定モードに入ります。

2) レベル1の設定番号を**1**に設定してください。装置は研究モードに入ります。

3) レベル2メニューの設定番号を**2**に設定してください。装置は研究モードに入ります。

2. 装置の電源を切り、バリアを台座に対して垂直になるまでスイングさせます。

3. 装置の電源を入れます。
装置は現在の位置を自動的に記憶します。

4. **「学習完了。再起動してください」**という音声が流れたら、デバイスを再起動してください**。**

4.4.3 ボタンによるキーフォブのペアリング

キーフォブをボタン操作でデバイスとペアリングし、バリアを遠隔で開閉します。

開始前に

技術サポートまたは営業部門にお問い合わせの上、キーフォブをご購入ください。

手順

注意

- ボタン操作の詳細については、「***ボタンによる設定」***を参照してください。
- 設定番号とその関連機能の詳細については、「***ボタン設定説明」***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、キーフォブの取扱説明書を参照してください。

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メニューの設定番号を**2に**設定してください。デバイスはキーフォブペアリングモードに入ります。

2. **クローズ**ボタンを10秒以上押し続けてください。
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. 設定を有効にするにはデバイスを再起動してください。

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4-15 初期化ボタンの位置

2. デバイスの初期化ボタンを5秒間押し続けてください。

3. プロセスが完了すると、デバイスは 3 秒間ビープ音を鳴らします。

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

デバイスの電源を入れる際には、レーン内に人がいないことを確認してください。

5 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
- デフォルトポート番号：80
- デフォルトユーザー名：admin

5.1 SADPによるアクティベーション

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。
- デバイスとSADPツールを実行するPCは同一サブネット内に配置してください。

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

手順

1. SADP ソフトウェアを実行し、オンラインデバイスを検索します。

2. オンラインデバイスリストから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。

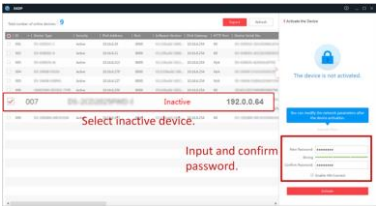
注意

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。

注意

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

4. **アクティベート**をクリックしてアクティベーションを開始します。



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は「**Active**」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てください。

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。

5.2 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、お客様自身で選択したパスワード（大文字、小文字、数字、特殊文字の 3 種類以上を含む 8 文字以上）に変更することを強くお勧めします。また、特にセキュリティレベルの高いシステムでは、パスワードを定期的に変更することをお勧めします。毎月または毎週パスワードを変更することで、製品をより確実に保護することができます。

すべてのパスワードおよびその他のセキュリティ設定の適切な構成は、設置者および／またはエンドユーザーの責任です。

注記

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

7. **[OK]** をクリックしてデバイスをアクティベートします。

5.3 Web ブラウザによるアクティベーション

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

注

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。

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**をクリックします。

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

6 Webブラウザによるクイック操作

6.1 時刻設定

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

タイムゾーン

ドロップダウンリストからデバイスの所在するタイムゾーンを選択します。

時刻同期

NTP

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

手動

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

夏時間

夏時間を有効にします。夏時間の開始時刻、終了時刻、および偏移時間を設定します

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。

6.2 管理者設定

手順

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

注

少なくとも1つの認証情報を選択する必要があります。

1) **「カードを追加」**をクリックしてカード番号を入力し、カードの特性を選択します。

注

最大50枚のカードをサポートします。

4. 設定を完了するには**「完了」**をクリックしてください。

7 Webブラウザによる操作

7.1 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。

注記

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。

Webブラウザ経由でのログイン

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アクセスします。

デバイスのユーザー名とパスワードを入力してください。**ログイン**をクリックしてください。

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。デバイスを追加後、[ ]をクリックして設定ページに入ります。

7.2 概要

デバイスのコンポーネント状態、リアルタイムイベント、人物情報、ネットワーク状態、基本情報、デバイス容量を確認できます。また、バリアを遠隔操作することも可能です。

図7-1 概要

機能説明:

デバイスコンポーネントの状態

デバイスの正常動作を確認できます。**「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。

リモート制御

/ / /

ドアが開く／閉まる／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ID、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」**をクリックすることもできます。結果は右パネルに表示されます。

人物情報

人物とカードの追加済み・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、ファームウェアの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。

7.3 人物管理

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

図7-2 人物追加

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、人物タイプなどの基本情報を追加します。

人物タイプとして「**訪問者**」を選択した場合、訪問時間を設定できます。

設定を保存するには「**保存**」をクリックします。

許可時間の設定

「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。

長期有効ユーザーを有効にするか、**有効期間**を設定し、実際のニーズに応じて設定された期間内のみ権限を付与できます。

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

「人物管理」→「追加」をクリックし、「人物追加」ページに入ります。

カード追加をクリックし、**カード番号**を入力して**物件**を選択し、**OK**をクリックしてカードを追加します。

注記

最大50枚のカードを追加できます。

設定を保存するには「**保存**」をクリック

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

人物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。

「人物データのエクスポート」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となります。

人物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および同期するには、暗号化パスワードを入力してください。

注記

- インポートするファイルの名前が「UserDataFile」であることを確認してください。

7.4 イベント検索

イベント検索をクリックして、検索ページに入ります。

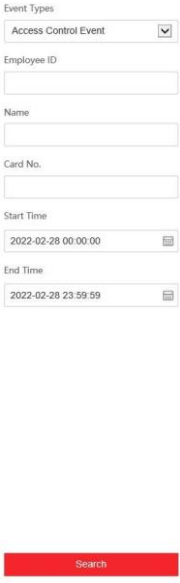


図 7-3 イベント検索

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**」をクリックします。

イベントタイプにはアクセス制御イベントとIDカードイベントが含まれます。IDカードイベントを検索する場合、従業員ID、氏名、カード番号の入力は不要です。

検索結果は右パネルに表示されます。

7.5 設定

7.5.1 デバイス情報の表示

設定 → システム → システム設定 → 基本情報 をクリックして設定ページに入ります。

デバイス名、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 番号を表示できます。

デバイス名を変更し、「保存」をクリックできます。

デバイス容量（人員、カード、イベントを含む）を確認できます。

7.5.2 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。

設定 → システム → システム設定 → 時刻設定 をクリックします。

図 7-4 時刻設定

設定後、[**保存**] をクリックして設定を保存します。

タイムゾーン

ドロップダウンリストから、デバイスが所在するタイムゾーンを選択します。

時刻同期

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」に**チェックを入れて、デバイスの時刻をコンピューターの時刻と同期させることができます。

サーバーIPアドレス/NTPポート/間隔

サーバーのIPアドレス、NTPポート、および間隔を設定できます。

7.5.3 DSTを設定

手順

1. **設定 → システム → システム設定 → 時刻設定** をクリックします。
2. **夏時間（DST）** を有効にします。
3. DST の開始時刻、終了時刻、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**をクリックします。

7.5.4 管理者のパスワードを変更する

手順

1. **設定 → ユーザー管理** をクリックします。
2. をクリックします。
3. 古いパスワードを入力し、新しいパスワードを作成します。
4. 新しいパスワードを確認します。
5. **OK**をクリックしてください。

注意

デバイスのパスワード強度を自動的に確認できます。製品のセキュリティを強化するため、お客様ご自身で選択したパスワード（大文字、小文字、数字、特殊文字の少なくとも3種類を含む、8文字以上）に変更することを強くお勧めします。また、特に高セキュリティシステムでは、パスワードを定期的に変更することをお勧めします。毎月または毎週パスワードを変更することで、製品をより効果的に保護できます。

すべてのパスワードおよびその他のセキュリティ設定の適切な構成は、設置業者および/またはエンドユーザーの責任となります。

7.5.5 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。

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、オンラインユーザーのリストを表示します。

7.5.6 デバイスの武装/解除情報を表示

デバイスの武装タイプと武装IPアドレスを表示します。

設定 → ユーザー管理 → 警備/解除情報 に移動します。

デバイスの武装/解除情報を表示できます。

更新をクリックするとページが更新されます。

7.5.7 ネットワーク設定

TCP/IP および HTTP(S) を設定します。

基本ネットワークパラメータの設定

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

図 7-5 TCP/IP 設定ページ

パラメータを設定し、**[保存]**をクリックして設定を保存します。

NIC タイプ

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

DHCP

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

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

DNS サーバー

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

ポートパラメータの設定

HTTP、HTTPS、HTTPリスニングパラメータを設定します。

設定 → ネットワーク → ネットワークサービス → HTTP(S) をクリックします。

図 7-6 ネットワークサービス

HTTP

ブラウザがデバイスにアクセスする際に使用するポートを指します。例えば、HTTPポートを 81 に変更した場合、ログインにはブラウザで ***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の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ます。

注記

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。

7.5.8 イベント連動

イベントに連動するアクションを設定します。

手順

1. **設定 → イベント → 基本イベント → イベント連動**をクリックしてページに入ります。

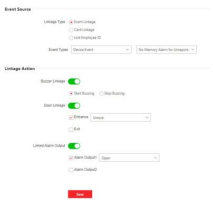


図 7-7 イベント連動

2. イベントソースを設定します。
   - **連携タイプ**を「**イベント連携**」に選択した場合、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。

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

3. リンク動作を設定します。

プザー連動

プザー連動を有効にし、対象イベントに対して「**プザーを鳴らす**」または「**プザーを止める**」を選択します。

ドア連動

ドア連動を有効にし、**入室**または**退室**をチェックし、対象イベントのドア状態を設定します。

連動アラーム出力

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、対象イベントのアラーム出力ステータスを設定します。

7.5.9 アクセス制御設定

認証パラメータの設定

設定 → アクセス制御 → 認証設定 をクリックします。

注記

機能は機種によって異なります。詳細は実際の機器を参照してください。

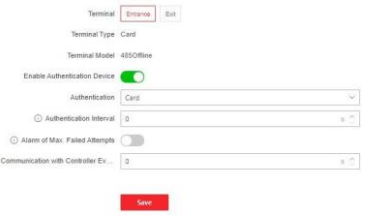


図 7-8 認証パラメータの設定

設定後、**保存**をクリックして設定を保存します。

端末

設定には「**入口**」または「**出口**」を選択します。

端末タイプ/端末モデル

端末の説明を取得します。これらは読み取り専用です。

認証デバイスの有効化

認証機能を有効にします。

認証

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

認証間隔

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

最大失敗試行回数アラーム

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

最大認証失敗回数

設定値に達したときに警報を通知する機能を有効にします。

コントローラとの通信間隔

アクセス制御デバイスが設定時間以上カードリーダーと接続できない場合、カードリーダーは自動的にオフラインになります。

注記

認証間隔の値は 2 秒から 255 秒の範囲で設定できます。

ドアパラメータの設定

設定 → アクセス制御 → ドアパラメータ をクリックします。

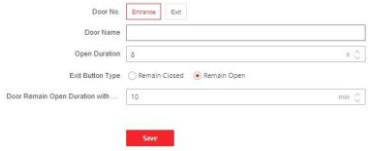


図7-9 ドアパラメータ設定ページ

設定後、**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

開錠時間は5秒から60秒の範囲で設定できます。

退出ボタンタイプ

出口ボタンは、実際の必要に応じて「**開いたままにする**」または「**閉じたままにする**」に設定できます。
実際のニーズに応じて設定できます。デフォルトは「**開いたまま**」です。

ドア開状態持続時間（最初の人物対応）

最初の認証者が入室した際のドア開放時間を設定します。最初の認証者が許可された後、複数人の入室やその他の認証操作を許可します。

注意

時間は1秒から1440秒の範囲で設定できます。

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. **[設定] → [アクセス制御] → [シリアルポート設定]** をクリックします。

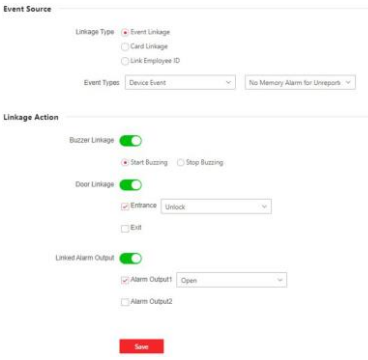


図 7-10 シリアルポート設定

2. **番号**、**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. **周辺機器タイプ**を**カードリーダー**、**カードレシーバー**、**QRコードスキャナー**、または**無効**に設定します。
4. **周辺機器の位置を入口**または**出口**に設定します。
5. シリアルポートタイプ、外部デバイスモデル、周辺機器ソフトウェアバージョンを確認できます。
6. **保存**をクリックします。

Wiegand パラメータを設定

Wiegand 伝送方向を設定できます。

手順

注

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

1. **設定 → アクセス制御 → ウィーガンド設定** をクリックします。
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 伝送方向は、デフォルトで**入力に**設定されています。

注意

入力：デバイスはウィーガンドカードリーダーに接続できます。

5. **Wiegandモード**を選択します。
6. 設定を保存するには、[**保存**] をクリックします。

注記

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

ターミナルパラメータの設定

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 → 端末パラメータ**をクリック
   ページに入力します。

図7-11 端末パラメータ

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

デバイスは人物の許可を検証せず、有効期間のみを確認します。人物が有効期間内であれば、バリアが開きます。

ローカル認証を有効にすることができます。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を使用せずに、人物の許可のみを検証します。

アクセス制御モード

デバイスは通常通り動作し、バリアを開くために人物の許可を検証します。

3. リモート検証を設定します。

1) **リモート認証を**有効にします。

注記

デバイスは対象者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否かを判断します。

2) **オプション：ローカルでの認証情報検証を**有効にする。

注記

機能を有効にした後、デバイスはスケジュールテンプレートなどなしで、人物の許可のみを検証します。

4. 保存をクリックして端末パラメータ設定を完了します。

7.5.10 ターンスタイル

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. 設定 → ターンスタイル → 基本設定をクリックしてページに入ります。

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

3. バリア材質、**レーン幅**、**バリア高さ**、バリア**開閉速度**を設定します。

4. 通信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。

注記

バリアフリーモードを設定すると、バリアは開いたままとなり、認証が失敗した場合に閉じます。

- **週単位スケジュール**を選択すると、入退場バリアの週単位スケジュールを設定できます。

5. 保存をクリックします。

キーフォブ

キーフォブのパラメータを設定します。

手順

1. **設定→ターンスタイル→キーフォブ**をクリックしてページに入ります。

図7-12 キーフォブ

2. **動作モードを**「**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) 実際のニーズに応じて「**開いたままにする許可**」**を**有効にするためにチェックを入れます。
   4) キーフォブを追加するには「**OK**」をクリックします。
4. **オプション：**キーフォブを選択し、**削除**をクリックするとキーフォブが削除されます。
5. **保存**をクリックします。

人数のカウント

人数のカウントを設定します。

手順

1. **設定→ターンスタイル→人数カウント**をクリックしてページに入ります。

図7-13 人数カウント

2. **人流計測を**有効にします。
3. 実際のニーズに応じて、**デバイスオフラインでの人数のカウントを有効にしてください**。
4. **「人物統計タイプ」を「無効」**または「**認証番号**」として選択します。
5. **オプション：「クリア」**をクリックすると、すべての人のカウント情報が消去されます。

その他の設定

その他のパラメータを設定します。

手順

1. **設定→ターンスタイル→その他の設定**をクリックしてページに入ります。

2. **アラーム出力時間を**設定します。

注

アラーム出力時間は0秒から3599秒の範囲です。

3. **温度単位**を設定してください。

4. ブロックをドラッグするか、値を入力してライトボードの明るさを調整します。

5. アラームブザーの鳴動時間、ドア閉遅延時間を設定します。

6. 制御モードを選択してください。

ソフトモード

人がバリアを通過した後、バリアが閉じます。

ガードモード

バリアは直ちに閉じます。

7. 火災入力タイプを設定します。

8. **モーター自己診断を**有効にするにはクリックし、メインレーンまたはサブレーンを選択してモーター自己診断を開始します。

9. **保存**をクリックしてください。

10. **「詳細」**をクリックして**バリア開放角度を**調整します。

7.5.11 カード設定

カードセキュリティの設定

設定→カード設定→カードタイプをクリックして設定ページに入ります。

パラメータを設定し、「**保存**」をクリックします。

NFC カードを有効にする

予約済み。

M1カードの有効化

M1 カードを有効にすると、M1 カードを提示して認証を行うことができます。

M1 カードの暗号化

セクター

M1カードの暗号化は、認証のセキュリティレベルを向上させます。

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

EMカード有効化

EMカードを有効にすると、EMカードの提示による認証が可能になります。

注意

周辺機器のカードリーダーがEMカードの提示をサポートしている場合、EMカード機能の有効化/無効化機能もサポートされます。

DESFireカード有効化

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

DESFire カードの内容を読み取る

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

デバイス上でカードによる認証を行う際のカード読み取り内容を設定します。

設定 → カード設定 → カード番号認証設定 に移動します。

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

7.5.12 プライバシーパラメータの設定

イベント保存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 に移動

イベント保存タイプはデフォルトで上書き保存です。保存済みイベントが総容量の95%を超えた場合、最も古い5%のイベントが削除されます。

7.5.13 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

[メンテナンスとセキュリティ] → [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

[メンテナンスとセキュリティ] → [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

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

[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] 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。

パラメータ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] をクリックします。

エクスポート

エクスポートをクリックして、デバイスパラメータをエクスポートします。

注

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。

7.5.14 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. **[メンテナンスとセキュリティ] → [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。

SSHを有効にする

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。

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。

ネットワークパケットのキャプチャ

キャプチャパケットの持続時間と**キャプチャパケットサイズ**を設定し、**「開始」**をクリックしてキャプチャを開始できます。

7.5.15 概要

メインレーンとサブレーンのステータスを表示できます。

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の状態を確認できます。

周辺機器

RS-485 カードリーダーおよび RS-232 カードレシーバーのステータスを確認できます。

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。

サブレーン状態

デバイスコンポーネント

レーン制御盤の状態を確認できます。

周辺機器

RS-485 カードリーダーおよび RS-232 カードレシーバーのステータスを確認できます。

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・出力状態

イベント入力/出力、警報入力/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。

7.5.16 ログクエリ

デバイスのログを検索および表示できます。

[メンテナンスとセキュリティ] → **[メンテナンス]** → **[ログ]**に移動します。

ログタイプの大分類と小分類を設定します。検索の開始時刻と終了時刻を設定し、「**検索**」をクリックします。

検索結果が以下に表示されます。これには、番号、時刻、メジャータイプ、マイナータイプ、チャネル番号、ローカル/リモートユーザー情報、リモートホストIPなどが含まれます。

7.5.17 証明書管理

サーバー/クライアント証明書および CA 証明書の管理に役立ちます。

注

この機能は特定のデバイスモデルでのみサポートされています。

自己署名証明書の作成とインポート

手順

1. **[メンテナンスとセキュリティ]** → **[セキュリティ]** → **[証明書管理]** に移動します。
2. **[証明書ファイル]** 領域で、ドロップダウンリストから **[証明書の種類]** を選択します。
3. **作成**をクリックします。
4. 証明書情報を入力します。
5. **[OK]** をクリックして証明書を保存およびインストールします。

   作成された証明書は、**[証明書の詳細]** 領域に表示されます。

   証明書は自動的に保存されます。

6. 証明書をダウンロードし、ローカルコンピュータの要求ファイルに保存します。

7. 要求ファイルを認証機関に送信し、署名を受け取ります。

8. 署名済み証明書をインポートします。

1) **[キーのインポート]** 領域で証明書の種類を選択し、ローカルから証明書を選択して **[インポート]** をクリックします。

2) **通信証明書**インポート領域で証明書の種類を選択し、ローカルから証明書を選択して「**インポート**」をクリックします。

その他の認証済み証明書のインポート

認証済み証明書（デバイスで作成されていないもの）を既に所有している場合は、それをデバイスに直接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 に移動します。

2. 「**キーのインポート**」および「**通信証明書のインポート**」で、証明書の種類を選択し、証明書をアップロードします。

3. インポートをクリックします。

CA証明書のインポート

開始前に

CA証明書を事前に準備してください。

手順

1. 「**メンテナンスとセキュリティ**」→「**セキュリティ**」→「**証明書管理**」に移動します。

2. 「**CA証明書のインポート**」領域でIDを作成します。

注

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てください。

4. インポートをクリックします。

8 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することができます。

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上で設定を行ってください。

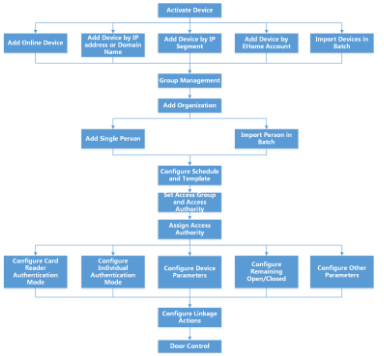


図 8-1 クライアントソフトウェアの設定フロー図

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ホン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機器を追加すると、入退室管理や勤怠管理が可能になります。室内機やドアステーションとのビデオインターホンも利用できます。

8.2.1 デバイス追加

クライアントは、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を提供します。また、大量のデバイスを追加する場合、複数のデバイスを一括でインポートすることもサポートしています。

IPアドレスまたはドメイン名によるデバイス追加

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、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できます。

手順

1. デバイス管理モジュールに入ります。
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。
   を追加モードとして選択します。
4. 必要な情報を入力します。
   名前
   デバイスの説明的な名前を作成します。例えば、デバイスの場所や特徴を示すニックネームを使用できます。
   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***80***00です。

注記

一部のデバイスタイプでは、ポート番号として***80***を入力できます。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、お客様ご自身で選択したパスワード（大文字、小文字、数字、特殊文字の少なくとも 3 種類を含む 8 文字以上）に変更することを強くお勧めします。また、特にセキュリティレベルの高いシステムでは、パスワードを定期的に変更することをお勧めします。毎月または毎週パスワードを変更することで、製品をより確実に保護することができます。

すべてのパスワードおよびその他のセキュリティ設定の適切な構成は、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。

5. **オプション:** セキュリティ目的でTLS（Transport Layer Security）プロトコルを使用した送信暗号化を有効にするには、**「送信暗号化（TLS）」**にチェックを入れます。

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。
- 証明書検証を有効にした場合は、**[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。
- Web ブラウザを使用してデバイスにログインし、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後、**[時刻を同期する]**をチェックすると、クライアントを実行しているPCとデバイスの時刻を同期できます。

7. **オプション:** **「グループにインポート」**にチェックを入れると、デバイス名でグループを作成し、そのデバイスの全チャンネルをこのグループにインポートします。

例

アクセス制御デバイスの場合、そのアクセスポイント、警報入力/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、他のデバイスの追加を続行します。

デバイスを一括インポート

クライアントに複数のデバイスをまとめて追加するには、事前定義されたCSVファイルにデバイスパラメータを入力します。

手順

1. デバイス管理モジュールに入ります。
2. 右パネル上部にある「**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。

注記

必須項目の詳細な説明については、テンプレートの導入部分を参照してください。

追加モード

0、***1***、***2***のいずれかを入力してください。

アドレス

デバイスのアドレスを編集します。

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

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強度を自動的に確認できます。製品のセキュリティ強化のため、ご自身で選択したパスワード（8文字以上で、大文字、小文字、数字、特殊文字の少なくとも3種類を含む）への変更を強く推奨します。また、特に高セキュリティシステムでは、パスワードを定期的に変更することを推奨します。月次または週次での変更により、製品をより効果的に保護できます。

すべてのパスワードおよびその他のセキュリティ設定の適切な構成は、設置業者および／またはエンドユーザーの責任となります。

グループへのインポート

1を入力すると、デバイス名でグループを作成します。デフォルトでは、デバイスの全チャンネルが対応するグループにインポートされます。***0***を入力すると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 デバイスのパスワードをリセット

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、クライアント経由でデバイスのパスワードをリセットできます。

手順

1. デバイス管理ページに入ります。
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コードを撮影してスマートフォンに保存することも可能です。撮影した画像をテクニカルサポートまでお送りください。

注意

パスワードをリセットする以下の操作については、当社のテクニカルサポートまでお問い合わせください。

注意

本製品のパスワード強度を自動で確認できます。製品のセキュリティ強化のため、お客様ご自身で選択したパスワード（8文字以上で、大文字、小文字、数字、特殊文字の少なくとも3種類を含む）に変更されることを強く推奨します。また、特に高セキュリティシステムでは、パスワードを定期的に変更することを推奨します。月次または週次での変更により、製品をより効果的に保護できます。

すべてのパスワードおよびその他のセキュリティ設定の適切な構成は、設置業者および/またはエンドユーザーの責任となります。

8.2.3 追加デバイスの管理

デバイスをデバイスリストに追加した後、追加したデバイスの管理（デバイスパラメータの編集、リモート設定、デバイスステータスの表示など）が可能です。

表 8-1 追加デバイスの管理

デバイスの編集	をクリックすると、デバイス名、アドレス、ユーザー名、パスワードなどのデバイス情報を編集できます。
デバイスの削除	1つ以上のデバイスをチェックし、[**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行います。詳細については、デバイスのユーザーマニュアルを参照してください。
デバイスの状態を表示	をクリックすると、ドア番号、ドアの状態などのデバイスステータスを表示できます。 **注記** 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	をクリックすると、最新のデバイス情報を取得できます。

8.3 グループ管理

クライアントは、追加されたリソースを異なるグループで管理するためのグループ機能を提供します。リソースの場所に応じて、リソースを異なるグループに分類できます。

例

例えば、1階には16個のドア、64個の警報入力、16個の警報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（名前：1階）にまとめて管理しやすくできます。リソースをグループ単位で管理した後、ドアの状態を制御したり、デバイスのその他の操作を行ったりできます。

8.3.1 グループを追加

追加したデバイスを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入ります。
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ます。
   - **「デバイス名でグループを作成」**をクリックし、追加されたデバイスを選択すると、選択したデバイスの名前で新しいグループが作成されます。

注

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 リソースをグループにインポート

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できます。

開始前に

デバイス管理用のグループを追加します。「***グループの追加***」を参照してください。

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、グループ管理ページに入ります。
3. グループ一覧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/リストビューでリソースのサムネイル/名前を選択します。

注記

] または] をクリックすると、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 人物管理

システムに人物情報を追加し、アクセス制御、ビデオインターホン、勤怠管理などの操作を実行できます。追加した人物に対して、一括でのカード発行、人物情報の一括インポート/エクスポートなどの管理が可能です。

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、人物の効果的な管理が可能です。追加した組織に対して上位組織を追加することもできます。

手順

1. **「人物」**モジュールに入ります。
2. 左カラムで親組織を選択し、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作成してください。

注記

最大10階層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	追加した組織にマウスを合わせ、[ ]をクリックして削除します。
	注 • 組織を削除すると、下位組織も削除されます。 • 組織の下に追加された人物がいないことを確認してください。いない場合のみ、組織を削除できます。
下位組織の人員を表示	**サブ組織の人員を表示するに**チェックを入れ、そのサブ組織の人員を表示する組織を選択します。

8.4.2 人物識別情報のインポートとエクスポート

複数人の情報と写真を一括でクライアントソフトウェアにインポートできます。同時に、人物情報と写真をエクスポートしてPCに保存することも可能です。

人物情報のインポート

あらかじめ定義されたテンプレート（CSV/Excelファイル）に複数人の情報を入力し、クライアントに一括で情報をインポートできます。

手順

1. 「人物」モジュールに入ります。
2. リストから追加済みの組織を選択するか、左上の**［追加］**をクリックして組織を追加し、その後選択してください。
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「**個人情報の**インポート」を選択します。
5. 個人情報をインポートするためのテンプレートをダウンロードするには、**[**テンプレートをダウンロード**]**をクリックします。
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

- 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ている項目は必須です。
- デフォルトでは、採用日は現在の日付です。

7. をクリックし、ローカルPCから個人情報のCSV/Excelファイルを選択します。
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既に個人番号が存在する場合、インポート前に既存の情報を削除してください。
- 最大2,000人分の情報をインポートできます。

個人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たことを確認してください。
- **「人物情報をエクスポート」**機能を有効にしていることを確認してください。**機能が**有効になっていることを確認してください。

手順

1. 「人物」モジュールに入ります。
2. **オプション：**リストから組織を選択します。

注

組織を選択しない場合、全人物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. 確認のため、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. エクスポートする内容として「**個人」に**チェックを入れます。
6. エクスポートしたい項目にチェックを入れてください。
7. **エクスポート**をクリックすると、エクスポートしたファイルがP C にCSV/Excelファイルとして保存されます。

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人物情報が設定されている場合、追加されたデバイスから人物情報を取得し、クライアントにインポートしてさらに操作することができます。

手順

注

- デバイスに保存されている人物名が空の場合、クライアントへのインポート後、人物名は発行済みカード番号で埋まります。
- デバイスに保存されているカード番号または人物ID（従業員ID）がクライアントデータベースに既に存在する場合、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**モジュールに入ります。
2. 個人をインポートする組織を選択します。
3. **デバイスから取得**をクリックします。
4. 追加されたアクセス制御デバイスまたは登録ステーションをドロップダウンリストから選択します。

   注記

   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、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

   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をサポートします。一度に最大5つの従業員IDを指定できます。

6. **「インポート」**をクリックすると、クライアントへの人物情報の取り込みが開始されます。

   注意

   最大2,000名の人物と5,000枚のカードをインポートできます。

   登録された個人情報は、選択された組織にインポートされます。

8.4.4 個人へのカード一括発行

クライアントは、複数の個人に一括でカードを発行する便利な方法を提供します。

手順

1. **「人物」**モジュールに入ります。
2. **オプション：**人物グループを選択し、カードが発行されていない人物を選択します。
   - 選択した人物グループ内でカードが発行されていない人物が右パネルに表示されます。
   - 人物グループでカード未発行の人物を選択しない場合、追加されたカード未発行の人物がすべて右パネルに表示されます。
3. **「カードを一括発行」**をクリックします。
4. **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。

5. **オプション：設定**をクリックしてカード発行パラメータを設定します。詳細は*ローカルモードによるカード発行*を参照してください。

6. **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。

7. **カード番号**欄をクリックし、カード番号を入力してください。
   - カードをカード登録ステーションに置きます。
   - カードリーダーでカードをスワイプします。
   - カード番号を手動で入力し、**Enter**キーを押します。

   リストに表示されている人物にカードが発行されます。

8.4.5 カードの紛失を報告する

カード紛失の場合、カード紛失を報告すると、そのカードに関連するアクセス権限が無効になります。

手順

1. **「担当者」**モジュールに入ります。

2. カード紛失を報告したい人物を選択し、「**編集**」をクリックして
   「編集」をクリックして「人物編集」ウィンドウを開きます。

3. **Credential** → **Card**パネルで、追加されたカード上の「」をクリックし、このカードを紛失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化され、使用できなくなります。紛失カードを所持している他の人が、このカードをスワイプしても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、[]をクリックして紛失をキャンセルできます。

   紛失登録を解除すると、当該カード の利用権限は有効かつアクティブ状態に戻ります。

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既にデバイスに適用されている場合、カード紛失の報告または紛失カードキャンセル後、変更をデバイスに適用するよう通知するウィンドウが表示されます。デバイスへの適用後、これらの変更はデバイス上で有効になります。

8.4.6 カード発行パラメータの設定

クライアントは、カード番号を読み取るために**2**つのモードを提供します：カード登録ステーション経由、またはアクセス制御デバイスのカードリーダー経由です。カード登録ステーションが利用可能な場合、USBインターフェースまたはCOMポートでクライアントを実行しているPCに接続し、カードをカード登録ステーションに置いてカード番号を読み取ります。利用できない場合は、追加済みの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。結果として、**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を含む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場合、「**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：カード登録ステーションによるカード発行

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。カードをカード登録ステーションに置くことでカード番号を取得できます。

カード登録ステーション

接続したカード登録ステーションのモデルを選択してください

注記

現在、サポートされ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。

カードタイプ

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

実際のカードタイプに応じて、カードタイプを 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

この機能は、モデルがDS-K1F100-Mの場合にのみ利用可能です。カード登録ステーションが接続するCOMポートを選択してください。

ブザー音

カード番号の読み取りに成功した際のブザー音の有効／無効を設定します。

カード番号タイプ

実際のニーズ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て、暗号化するカードのセクターを選択してください。

リモートモード：カードリーダーによるカード発行

クライアントに追加され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の設定

休日や週単位のスケジュールを含むテンプレートを設定できます。テンプレート設定後、アクセスグループ設定時にこの設定済み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有効期間内に機能するようになります。

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人物にアクセス権限を割り当てる***」を参照してください。

8.5.1 休日の追加

休日を作成し、開始日、終了日、1 日の休暇期間など、休日の日数を設定することができます。

手順

注

ソフトウェアシステムでは最大64件の休日を追加できます。

1. **アクセス制御 → スケジュール → 休日**をクリックして休日ページに入ります。
2. 左パネルの「**追加**」をクリックします。
3. 休日の名前を作成します。

4. オプション：備考欄にこの休日の説明や通知事項を入力します。

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。

注記

1 つの休日には、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の「**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描画します。これは、設定されたアクセスグループがその時間範囲内で有効化されることを意味します。

注記

1 つの休日期間に最大 8 つの時間枠を設定できます。

3) **オプション：**以下の操作で時間範囲を編集できます。

●カーソルを時間範囲に移動し、カーソルが に変わったタイミングで、タイムラインバー上の時間範囲を目的の位置までドラッグします。

●時間枠をクリックし、表示されるダイアログで開始/終了時間を直接編集します。

●カーソルを時間範囲の開始点または終了点に移動し、カーソルが に変わった状態でドラッグすると、時間範囲を延長または短縮できます。

4) **オプション：**削除が必要な時間範囲を選択し、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：**操作列の「 」をクリックすると、タイムバー上のすべての時間範囲をクリアできます。

6) **オプション：**操作列の「 」をクリックすると、休日リストから追加した休日期間を削除できます。

6. 保存をクリックします。

8.5.2 テンプレートの追加

テンプレートには週スケジュールと休日が含まれます。週スケジュールを設定し、異なる個人またはグループに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

注記

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入ります。

注記

デフォルトで「終日許可」と「終日拒否」の 2 つのテンプレートが用意されていますが、これらは編集も削除もできません。

終日許可

アクセス許可は週の毎日有効であり、休日設定はありません。

終日拒否

アクセス許可は週のすべての日に無効であり、休日設定はありません。

2. 左パネルの「**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作成します。

4. 備考欄にこのテンプレートの説明や通知事項を入力してください。

5. 週スケジュールを編集してテンプレートに適用します。

1) 下部パネルの「**週間スケジュール**」タブをクリックします。

2) 曜日を選択し、タイムラインバー上に時間枠を描画します。

注記

週スケジュールでは、各曜日に最大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以下の操作を行います。

●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の時間枠を希望の位置までドラッグします。

●時間枠をクリックし、表示されるダイアログで開始/終了時間を直接編集します。

●カーソルを時間区間の開始点または終了点に移動し、カーソルが に変わった状態でドラッグすると、時間区間を延長または短縮できます。

4) 上記の2つの手順を繰り返して、他の曜日の時間枠を追加で描画します。

6. 休日を追加してテンプレートに適用します。

注記

1 つのテンプレートに最大 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) 左側のリストから休日を選択すると、右側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。

注記

休日の追加に関する詳細は、***「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]**をクリックして右リストの選択済み休日をすべてクリアします。

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、人物にアクセス権限を割り当てる

担当者を追加し、その認証情報を設定した後、アクセスグループを作成して、どの担当者がどのドアにアクセスできるかを定義し、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にすることができます。

開始前に

- クライアントに人物を追加する。
- クライアントとグループアクセスポイントにアクセス制御デバイスを追加します。詳細は「***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、変更を有効にするにはデバイスにアクセスグループを再度適用する必要があります。アクセスグループ変更には、テンプレートの変更、アクセスグループ設定の変更、個人のアクセスグループ設定の変更、および関連する個人詳細の変更が含まれます。

1. **[アクセス制御]** → **[認証]** → **[アクセスグループ]** をクリックしてアクセスグループ画面に入ります。

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、アクセスグループに任意の名前を入力してください。

4. アクセスグループのテンプレートを選択します。

注記

アクセスグループ設定の前にテンプレートを設定する必要があります。詳細は ***「スケジュールとテンプレートの設定」*** を参照してください。

5. 「人物の選択」フィールドの左リストで、アクセス権限を割り当てる人物を選択します。

6. [アクセスポイントの選択]フィールドの左リストから、選択した人物がアクセスするドア、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で、選択した人物とアクセスポイントを確認できます。

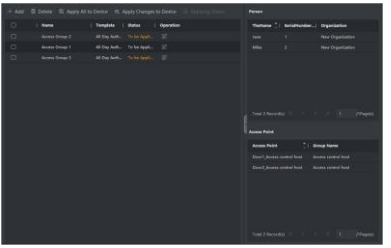


図8-2 選択された人物とアクセスポイントの表示

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して有効に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) **[デバイスにすべて適用]** をクリックして、選択したすべてのアクセスグループをアクセス制御デバイスまたはドアステーションに適用し始めます。

3) **[デバイスにすべて適用]** または **[デバイスに変更を適用]** をクリックします。**デバイスにすべて適用**

この操作により、選択したデバイスの既存のアクセスグループがすべてクリアされ、新しいアクセスグループがデバイスに適用されます。

デバイスへの変更の適用

この操作では、選択したデバイスの既存のアクセスグループはクリアされず、選択したアクセスグループのうち変更された部分のみがデバイスに適用されます。

4) 適用ステータスは「ステータス」列で確認するか、
適用状況をクリックすると、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

適用結果をフィルタリングするには、**[失敗のみ表示]** をチェックします。

適用されたアクセスグループで選択された人物は、関連付けられたカードを使用して、選択されたドア／ドアステーションへの入退室権限を有します。

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。

注記

アクセスグループに属する人物のアクセス情報またはその他の関連情報を変更すると、クライアントの右隅に**「適用されるアクセスグループ」** というプロンプトが表示されます。

このプロンプトをクリックすると、変更したデータをデバイスに適用できます。**Apply Now（今すぐ適用）またはApply Later（後で適用）** のいずれかを選択できます。

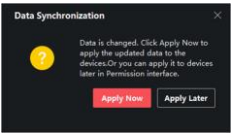


図 8-3 データ同期

8.7 詳細設定

さまざまなシーンにおける特別な要件を満たすために、アクセス制御の高度な機能を設定できます。

注記

- カード関連機能（アクセス制御カードの種類）については、カード追加時にアクセスグループが適用されたカードのみが表示されます。
- 高度な機能は、デバイスがサポートしている必要があります。
- カーソルを「詳細機能」に合わせ、「 」をクリックすると、表示する詳細機能をカスタマイズできます。

8.7.1 デバイスパラメータの設定

アクセス制御デバイスを追加した後、アクセス制御デバイスおよびアクセス制御ポイント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設定

アクセス制御デバイスを追加した後、そのパラメータを設定できます。これには、写真へのユーザー情報の重ね合わせ、撮影後の写真のアップロード、撮影済み写真の保存などが含まれます。

開始前に

クライアントにアクセス制御デバイスを追加する。

手順

1. **アクセス制御 → 高度な機能 → デバイスパラメータ** をクリックします。

注記

詳細機能リストに「デバイスパラメータ」が見つからない場合は、詳細機能にカーソルを合わせ、
をクリックして表示するデバイスパラメータを選択してください。

2. アクセスデバイスを選択すると、右ページにそのパラメータが表示されます。

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。

注記

- 表示されるパラメータは、アクセス制御デバイスによって異なる場合があります。
- 以下のパラメータの一部は基本情報ページに表示されません。編集するには「**詳細**」をクリックしてください。

NFCを有効にする

この機能を有効にすると、デバイスは NFC カードを認識できるようになります。デバイスに NFC カードを提示することができます。

M1カード有効化

この機能を有効にすると、デバイスはM1カードを認識できます。デバイスにM1カードを提示できます。

EMカード有効化

この機能を有効にすると、デバイスはEMカードを認識できます。デバイスにEMカードを提示できます。

CPUカード有効化

予約済み。この機能を有効にすると、デバイスはCPUカードを認識できます。デバイスにCPUカードを提示できます。

IDカード有効化

予約済み。この機能を有効にすると、デバイスはIDカードを認識できます。デバイスにIDカードを提示できます。

4. **[OK]**をクリックします。

5. **オプション：「コピー先」**をクリックし、選択したアクセス制御デバイス にページ内のパラメータをコピーします。

ドア/エレベーターのパラメータ設定

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する。

手順

1. **アクセス制御 → 高度な機能 → デバイスパラメータ** をクリックします。

2. 左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. ドアまたはフロアを選択すると、右ページにそのパラメータが表示されます。

4. ドアまたはフロアのパラメータを編集します。

注記

- 表示されるパラメータは、アクセス制御デバイスによって異なる場合があります。
- 以下のパラメータの一部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に編集してください。

終了ボタンのタイプ

退出ボタンを「閉じたまま」または「開いたまま」に設定できます。通常は「開いたまま」です。

開放時間

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

5. **OK**をクリックします。

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。

注記

ドアまたはフロアの状態持続時間設定は、選択したドア/フロアにもコピーされます

カードリーダーのパラメータ設定

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する。

手順

1. **左側のデバイス一覧で「xml-ph-0000@deepl.internal」**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を編集**できます。

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を編集します。

注記

- 表示されるパラメータは、アクセス制御デバイスによって異なる場合があります。以下に一部パラメータを記載します。詳細はデバイスのユーザーマニュアルを参照してください。
- 以下のパラメータの一部は基本情報ページに表示されません。「**詳細**」をクリックして編集してください。

名前

カードリーダー名を任意に編集します。

カード認証間隔

認証時に連続する2回のカード認識の間隔を設定します。

繰り返し認証間隔

指定された間隔内で、同一カード番号（異なるデバイスからアップロードされたもの）の繰り返し認証は無効となり、1回の認証のみが実行されます。

認証の失敗回数制限を有 効 にする

カード読み取り試行回数が設定値に達したときにアラームを通知する機能を有効にします。

カードリーダータイプ/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。

4. **[OK]** をクリックします。

5. **オプション：「コピー先」**をクリックし、選択したカードリーダーにページ内のパラメータをコピーします。

アラーム出力のパラメータ設定

アクセス制御デバイスを追加後、デバイスが警報出力にリンクしている場合、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、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 → 高度な機能 → デバイスパラメータ**をクリックし、アクセス制御パラメータ設定ペ ー ジ に入ります。

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. 警報出力パラメータを設定します。

名前

カードリーダー名を任意に編集してください。

アラーム出力アクティブ時間

アラーム出力は、トリガー後どのくらい持続しますか。

4. **OK**をクリックしてください。

5. **オプション：**右上隅のスイッチを **ON** に設定すると、アラーム出力がトリガーされます。

レーンコントローラのパラメータ設定

レーンコントローラをクライアントに追加した後、レーン通過のため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する。

手順

1. **アクセス制御 → 高度な機能 → デバイスパラメータ**をクリックし、パラメータ設定ページに入ります。

2. 左側のデバイス一覧でレーンコントローラを選択すると、右側でそのパラメータを編集できます。

3. パラメータを編集します。

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を選択します。

バリア開閉速度

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

推奨値は6です。

警報音声プロンプト時間

アラームが作動した際に再生される音声の継続時間を設定します。

注記

0は、アラームが終了するまでアラーム音が再生されることを示します。

温度単位

デバイスのステータスに表示される温度の単位を選択します。

ライトボードの明るさ

デバイスのライトの明るさを調整します。

バリア材質

バリアゲートの材質を選択します。ドロップダウンリストからバリア材質を選択できます。

注記

バリアの材質はデバイスの動作に影響を与える可能性があります。正しいバリア材質を選択してください。誤った材質を選択するとバリアが開かない場合があります。

レーン長

レーンの幅。レーンの幅を設定できます。

注記

レーン幅はデバイスの動作に影響を与える可能性があります。正しいレーン幅を設定してください。さもないとバリアが開かない場合があります。

4. **OK**をクリックしてください。

8.7.2 デバイスパラメータの設定

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などのパラメータを設定できます。

RS-485 パラメータの設定

アクセス制御デバイスの RS-485 パラメータ（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、動作モード、接続モードなど）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、デバイスがRS-485インターフェース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に入ります。
2. 左側のナビゲーションバーで、**[詳細機能] → [その他のパラメータ]** に移動します。
3. デバイスリストからアクセス制御デバイスを選択し、
   RS-485をクリックし、RS-485設定ページに入ります。
4. 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、RS-485パラメータを設定します。

5. 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、接続モードをドロップダウンリストで設定します。

6. **保存**をクリックします。

- 設定したパラメータは自動的にデバイスに適用されます。
- 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。

ウィーガンドパラメータの設定

アクセス制御デバイスのウィーガンドチャネルと通信モードを設定できます。ウィーガンドパラメータ設定後、デバイスはウィーガンド通信経由でウィーガンドカードリーダーに接続できます。

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、デバイスがウィーガンド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に入ります。
2. 左側のナビゲーションバーで、**[詳細機能]** → **[その他のパラメータ]** に移動します。
3. デバイスリスト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設定ページに入ります。
4. スイッチをオンに設定して、デバイスのウィーガンド機能を有効にします。
5. ドロップダウンリストからウィーガンドチャネル番号と通信モードを選択します。

注記

通信方向を送信に設定する場合、ウィーガンドモードは**ウィーガンド26**または**ウィーガンド34**に設定する必要があります。

6. **保存**をクリックします。

- 設定したパラメータは自動的にデバイスに適用されます。
- 通信方向を変更した後、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カード暗号化は、認証のセキュリティレベルを向上させます。

手順

注記

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に入ります。
2. 左側のナビゲーションバーで、**[詳細機能]** → **[その他のパラメータ]** を選択します。
3. デバイスリスト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入ります。
4. スイッチをオンに設定して、M1カードの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**]をクリックしてください。

8.8 ドア/エレベーター制御

監視モジュールでは、追加されたアクセス制御デバイスが管理するドアやエレベーターのリアルタイム状態を確認できます。クライアント経由でドアの開閉操作やドアの開放/閉鎖状態の維持など、ドアやエレベーターを遠隔操作することも可能です。リアルタイムのアクセスイベントがこのモジュールに表示されます。アクセス詳細と人物詳細を確認できます。

注記

ドア/エレベーター制御権限を持つユーザーは、監視モジュールにアクセスしてドア/エレベーターを制御できます。権限がないユーザーには制御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

ドアの状態を制御できます。これには、ドアのロック解除、ドアのロック、ドアのロック解除状態の維持、ドアのロック状態の維持、すべてのドアのロック解除状態の維持などが含まれます。

開始前に

- 人物を追加し、指定した人物にアクセス権限を割り当てると、その人物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。詳細は「***人物管理***」および「***人物へのアクセス権限割り当てのためのアクセスグループ設定***」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。

手順

1. **「監視」**をクリックして状態監視ページに入ります。

2. 右上隅でアクセスポイントグループを選択します。

注記

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。

注記

「すべてロック解除のまま」および「**すべてロックのまま」**の場合は、この手順をスキップしてください。

4. ドアを制御するには、以下のボタンをクリックします。

ドアのロック解除

ドアがロックされている場合、アンロックすると一度だけ開きます。開いている時間が経過すると、ドアは自動的に閉まり、再びロックされます。

ドアをロック

ドアがロックされていない場合は、ロックすると閉まります。アクセス権限を持つ者は認証情報でドアにアクセスできます。

開錠状態を維持

ドアは解錠状態（閉まっているか開いているかを問わず）になります。認証情報なしで全ての人が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、認証情報を持つ者であってもアクセスできません。

すべて開錠状態を維持

グループ内の全てのドアは施錠解除状態となります（閉まっているか開いているかを問わず）。認証情報なしで全ての人がドアにアクセスできます。

すべて施錠状態を維持

グループ内のすべてのドアは閉められ、施錠されます。スーパーユーザーを除き、認証資格を持つ者であってもドアにアクセスすることはできません。

キャプチャ

手動で画像をキャプチャします。

注記

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利用可能です。画像はクライアントを実行している**PC**に保存されます。

ドアステーションのリモートアンロック

グループにドアステーションが含まれている場合、**Lock1**

または**Lock2**を**選択し**、「**ドアのロック解除**」をクリックするとドアステーションのロックを解除できます。

注記

デフォルトでは、ドアステーションには **Lock1** がチェックされています。

ステータスの更新

ドアの最新状態を取得するには「**状態を更新**」をクリックしてください。

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化します。

8.8.2 リアルタイムアクセス記録の確認

リアルタイムアクセス記録はクライアントに表示できます。また、人物情報も閲覧できます。

ご利用の前に

クライアントに人物とアクセス制御デバイスを追加済みであること。詳細は「***人物管理***」および「***デバイスの追加***」を参照してください。

手順

1. **「監視」**をクリックして監視モジュールに入ります。

   リアルタイムのアクセス記録はページ下部に表示されます。記録の詳細を確認できます

   注記

   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/非表示を切り替えられます。

2. **オプション：**右上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が表示されます。

3. **オプション：**イベントタイプとイベントステータスをチェックします。

チェックしたタイプとステータスの検出イベントが下のリストに表示されます。

4. **オプション：「最新のイベントを表示」**をチェックすると、最新のアクセス記録を表示できます。

   記録リストは新しい順に表示されます。

5. **オプション：**「」をクリックして詳細を表示します。

注記

ポップアップウィンドウで、[]をクリックすると、詳細を全画面表示で確認できます。

A. DIPスイッチ

A.1 DIPスイッチの説明

DIPスイッチはアクセス制御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。

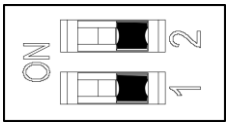


図 A-1 DIP スイッチ

スイッチが ON 側にある場合、スイッチは有効であることを意味し、それ以外の場合、スイッチはオフです。

B. ボタン設定説明

レーン制御ボード上のボタンによる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 設定番号	説明	レベル2 構成番号と機能	注記
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  注記 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	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。	
3	通過モード	1- 両側制御下  注記 デフォルトでは、表示画面に「1」が表示されます。 2- 入口は通行可、出口は通行禁止 7-両方向通行禁止 8-進入禁止；退出管理中 10-入口は制御下；出口は開放中 14-入口閉鎖中；出口は開放中 16-入口開放中；出口制御中	

レベル 1 構成番号	説明	レベル 2 構成番号および機能	注記
		18-入口開放中、出口開放中 20-入口開放状態；出口禁止	
4	メモリモード	1- 無効化 2- 有効化  注記 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	キーフォブリモートコントロール	1- 1対1 2- 1対多  注記 デフォルトでは、ディスプレイ画面に1が表示されます。	
6	バリア開閉速度	1-1、2-2、...10-10  注記 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	バリア閉速度	1-1、2-2、...10-10  注記 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	警報エリアでのカード読み取り	1- 開けないでください 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	

レベル 1 構成番号	説明	レベル2 構成番号と機能	注記
		 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  デフォルトでは、表示画面に 5 が表示されます。	
21	音量	1-0, 2-1, 3-2, 4-3, 5-4  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、デバイスの音はミュートになります。
36	バリア材質	1-アクリル 2-ガラス  デフォルトでは、ディスプレイ画面に1が表示されます。	
37	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  デフォルトでは、8 が	

レベル1 構成番号	説明	レベル 2 構成番号と機能	注記
		表示されます。	
38	モーター点検	1- 無効 2- メインレーンで有効化 3- サブレーンで有効化  **注記** デフォルトでは、表示画面に 1 が表示されます。	
39	ライトの明るさ	0-0, 1-1, 2-2, …、10-10  **注記** デフォルトでは、表示画面に3が表示されます。	数値が高いほど、光は明るくなります。
40	自己診断音声プロンプト	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。	
41	学習モード音声プロンプト	1- 無効 2-有効  **注記** デフォルトでは、ディスプレイ画面に 2 が表示されます。	
43	アプリケーションモード	1- 防風 2-屋内  **注記** 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	

レベル1 構成番号	説明	レベル2 構成番号と機能	注記
		 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- バリア位置例外 3- 侵入  デフォルトでは、ディスプレイ画面に 2 が表示されます。	
46	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。	
48	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。	
50	メインレーンまたはサブレーン	1- メインレーン 2- サブレーン	

レベル1 構成番号	説明	レベル2 構成番号と機能	注記
		 デフォルトでは、ディスプレイ画面に 1 が表示されます。	
51	組み合わせモード	1- メインレーンとサブレーン 2- シングルメインレーン  デフォルトでは、ディスプレイ画面に1が表示されます。	
52	バリア開放モード	1- 通常 2-逆バリア開放  デフォルトでは、ディスプレイ画面に 1 が表示されます。	
53	機械式挟み込み防止回復時間	1-1秒 2-2秒 3-3秒 4-4秒 5-5秒  デフォルトでは、ディスプレイ画面に 3 が表示されます。	
99	デフォルトに復元	1-デフォルト 2-開始 デフォルトでは、ディスプレイ画面に 1 が表示されます。	

注

- 設定番号50および51を調整した場合は、デバイスを手動で再起動する必要があります。

C. イベントとアラームの種類

イベント	アラームタイプ
通過タイムアウト	なし
バリア遮断	なし

D. オーディオインデックス関連コンテンツ一覧

インデックス	コンテンツ
1	認証済み。
2	カード番号が存在しません。
3	タイムアウトを許可します。
4	権限がありません。
5	認証タイムアウト。
6	認証に失敗しました。
7	カードの有効期限が切れています。

E. エラーコード説明

スイングゲートは、エラーが発生した場合、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。各数字の説明については、以下の表を参照してください。

エラーの原因	コード	エラー原因	コード
相互接続例外	53	勉強していない	54
妨害	55	学習範囲の超過	56
エンコーダ例外	57	モーター例外	58
オプションボードオフライン（ボードがインストールされていない場合、エラーコード「59」が表示されますが、デバイスは正常に機能します）	59		