DS-K1T502 シリーズ アクセス制御端末

ユーザーマニュアル

法的情報

このドキュメントについて

- この文書には、製品の使用および管理に関する手順が記載されています。本文中に含まれる図、表、画像およびその他の情報は、説明および参考目的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またはその他の理由により、予告なしに変更される場合があります。最新のバージョンは、Hikvisionのウェブサイト（***https://www.hikvision.com***）でご確認ください。別途合意がない限り、杭州 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」といいます）は、明示的または黙示的ないかなる保証もいたしません。
- 本ドキュメントは、製品をサポートする専門家の指導と支援を受けてご使用ください。

本製品について

- この製品は、購入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。
- 選択された製品が動画製品の場合、以下のQRコードをスキャンして「動画製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

- 本ドキュメントに記載される製品に組み込まれた技術に関する著作権および/または特許権は、Hikvisionが所有しています。これには第三者から取得したライセンスを含む場合があります。
- 本文書の一部（テキスト、画像、グラフィックなど）はすべてHikvisionに帰属します。本文書のいかなる部分も、書面による許可なしに、引用、複製、翻訳、または改変を行うことはできません。
- **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の財産です。
- その他の商標およびロゴは、それぞれ該当する所有者の財産です。

法的免責事項

- 適用される法律で許される最大限の範囲において、本文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」かつ「一切の瑕疵およびエラーを含む」状態で提供されます。ヒクビジョンは、明示的または黙示的ないかなる保証もいたしません。

明示的または黙示的な一切の保証（商品性、満足のいく品質、または特定の目的への適合性を含むがこれらに限定されない）は、一切提供されません。製品の使用は、お客様の責任において行われます。いかなる場合においても、HIKVISIONは、特別損害、付随的損害、間接損害、または派生損害（事業利益の損失、事業の中断、データの損失を含むがこれらに限定されない）について、契約違反、不法行為（過失を含む）、製品責任、またはその他のいかなる理由に基づくものであっても、一切の責任を負いません。システムの破損、または文書の損失を含む損害について、契約違反、不法行為（過失を含む）、製品責任、またはその他の理由に基づくものであっても、製品の使用に関連して生じた場合、HIKVISIONは一切の責任を負いません。これは、HIKVISIONがそのような損害または損失の可能性について事前に通知を受けていた場合でも同様です。

- あなたは、インターネットの性質上、内在するセキュリティリスクが存在することを承認し、HIKVISIONは、サイバー攻撃、ハッカー攻撃、ウイルス感染、またはその他のインターネットセキュリティリスクに起因する異常な動作、プライバシー漏洩、またはその他の損害について一切の責任を負いません。ただし、必要に応じて適切な技術サポートを提供します。
- あなたは、この製品を適用されるすべての法律に準拠して使用することに同意し、あなたの使用が適用される法律に準拠していることを確保する責任は、あなたのみに帰属します。特に、あなたは、第三者の権利（publicity rights、知的財産権、データ保護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）を侵害しない方法で本製品を使用する責任を負います。お客様は、大量破壊兵器の開発または製造、化学兵器または生物兵器の開発または製造、核爆発または安全でない核燃料サイクルに関連するいかなる活動、または人権侵害を支援する目的での使用を含みます。
- 本文書と適用される法律との間に矛盾が生じた場合、後者が優先されます。

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の場合、生体認証データは暗号化方式で製品内に保存されます。指紋認証製品の場合、指紋テンプレートのみが保存され、指紋画像の復元は不可能です。
- データ管理者/処理者として、個人データの収集、保管、利用、処理、開示、削除などを行う場合があります。個人データの保護に関する適用される法律および規制（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）に留意し、遵守するようご注意ください。具体的には、個人データを保護するための合理的な管理上および物理的なセキュリティ対策を実施し、セキュリティ対策の有効性を定期的にレビューおよび評価を行うことが含まれます。

©杭州海康威視デジタルテクノロジー株式会社。著作権所有。

記号の規約

本文書において使用される記号は、以下のとおり定義されます。

記号	説明
 危険	危険な状況を示し、回避しない場合、死亡または重大なけがを引き起こす可能性があります。
 注意	回避しない場合、機器の損傷、データ損失、性能の低下、または予期しない結果を引き起こす可能性がある危険な状況を示します。
 注意	本文の重要な点を強調または補足するための追加情報を提供します。

規制情報

FCC情報

注意：本機器の製造者または販売者によって明示的に承認されていない変更または改造は、本機器の操作権限を無効にする可能性があります。

FCC準拠：この機器は、FCC規則第15条に準拠し、クラスBデジタル機器の制限値に適合することが確認されています。これらの制限値は、住宅環境での使用において有害な干渉から合理的な保護を提供するよう設計されています。この機器は、無線周波数エネルギーを発生、使用し、放射する可能性があります。指示に従って設置および使用されない場合、無線通信に有害な干渉を引き起こす可能性があります。ただし、特定の設置環境において干渉が発生しないことを保証するものではありません。この機器がラジオまたはテレビの受信に有害な干渉を引き起こす場合（機器の電源をオン/オフすることで確認できます）、ユーザーは次の措置の1つまたは複数を試すよう推奨されます：

—受信アンテナの向きや位置を変更する。

—機器と受信機との距離を離す。

—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機器を接続してください。

—販売店または経験豊富なラジオ/テレビ技術者に相談してください。

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

FCC 条件

この装置はFCC規則の第15部に準拠しています。動作は次の2つの条件に準拠しています：

1. この装置は有害な干渉を引き起こしてはなりません。
2. この装置は、受信するすべての干渉を許容しなければなりません。これには、正常な動作を妨げる可能性のある干渉も含まれます。

EU適合宣言

この製品および適用される場合、付属品も「CE」マークが付与されており、EMC指令 2014/30/EU、RoHS指令 2011/65/EUに定める調和欧州規格に準拠しています。

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

2006/66/EC（電池指令）：この製品には、欧州連合において一般廃棄物として処分できない電池が含まれています。電池に関する詳細は製品ドキュメントをご確認ください。電池にはこのマークが記載されており、カドミウム（Cd）、鉛（Pb）、または水銀（Hg）を示す文字が含まれる場合があります。適切なリサイクルのため、電池は販売店または指定の回収場所に返却してください。詳細については、www.recyclethis.info をご覧ください。

カナダ産業省 ICES-003 準拠

この機器は、CAN ICES-3 (B)/NMB-3(B) 規格の要件を満たしています。
この装置は、カナダ産業省の免許不要RSS規格に準拠しています。動作は、以下の2つの条件に準拠する必要があります:

1. この装置は干渉を引き起こしてはなりません、および
2. この装置は、装置の正常な動作を妨げる可能性のある干渉を含む、いかなる干渉も受け入れる必要があります。

この装置は、カナダ産業省のライセンス免除無線機器に関するCNRに準拠しています。使用は、以下の2つの条件を満たす場合に限り許可されます:

1. この装置は干渉を引き起こしてはなりません、および
2. この装置のユーザーは、受けたすべての無線干渉を受け入れる必要があります。この干渉が装置の動作を妨げる可能性があっても同様です。

産業省の規制に従い、この無線送信機は、産業省が当該送信機に対して承認した種類および最大（またはそれ以下の）利得を有するアンテナを使用する場合にのみ動作可能です。他のユーザーへの無線干渉を最小限に抑えるため、アンテナの種類およびその利得は、等価全方向放射電力（e.i.r.p.）が通信の成功に必要な値を超えないように選択する必要があります。
産業省の規制に従い、本無線送信機は、産業省により当該送信機用に承認された種類および最大（またはそれ以下の）利得を有するアンテナを使用してのみ動作可能です。他のユーザーへの無線干渉を最小限に抑えるため、アンテナの種類およびその利得は、等方放射電力（e.i.r.p.）が通信の成功に必要な強度を超えないように選択する必要があります。

放射等価電力（p.i.r.e.）が、満足のいく通信を確立するために必要な強度を超えないようにする必要があります。
この機器は、ラジエーターと身体の間に最低20cmの距離を保って設置し、使用してください。
この機器は、ラジエーターと身体の間に20cm以上の距離を保って設置し、使用してください。

安全注意事項

これらの指示は、ユーザーが製品を正しく使用し、危険や財産の損失を防止するために用意されています。

安全対策は「危険」と「注意」に分類されています:

危険: 警告を無視すると、重大な怪我や死亡事故を引き起こす可能性があります。

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

⚠	⚠
危険: 重大な怪我や死亡を防止するため、これらの安全対策を必ず遵守してください。	**注意:** これらの注意点を遵守し、怪我や材料の損傷を防止してください。

⚠危険

- すべての電子機器の操作は、地域で適用される電気安全基準、防火基準、その他の関連法規に厳格に従ってください。
- 電源アダプターは、当社が提供する正規品を使用してください。消費電力は、必要な値を下回らないようにしてください。
- 複数の機器を1つの電源アダプターに接続しないでください。アダプターの過負荷により、過熱や火災の危険があります。
- 装置の配線、取り付け、または分解を行う前に、必ず電源を切断してください。
- 製品を壁や天井に設置する際は、装置をしっかりと固定してください。
- 装置から煙、臭い、または異音が発生した場合は、直ちに電源を切り、電源ケーブルを抜いてから、サービスセンターまでご連絡ください。
- 電池を誤飲しないでください。化学やけどの危険があります。
  この製品にはコイン型/ボタン型電池が含まれています。コイン型/ボタン型電池を誤飲すると、2時間以内に重度の内部やけどを引き起こし、死亡する可能性があります。
  新しい電池と使用済みの電池は、子供の手の届かない場所に保管してください。電池 compartment がしっかり閉まらない場合は、製品の使用を中止し、子供の手の届かない場所に保管してください。電池が誤って飲み込まれたり、体の内部に挿入された可能性がある場合は、直ちに医療機関を受診してください。
- 製品が正常に動作しない場合は、販売店または最寄りのサービスセンターまでご連絡ください。絶対に自分で分解しないでください。（不正な修理やメンテナンスによる問題については、当社は一切の責任を負いません。）

⚠注意

- 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。
- 装置を落としたり、物理的な衝撃を与えたり、高電磁波放射にさらさないでください。振動する表面や衝撃を受ける可能性のある場所に装置を設置しないでください。（無視すると装置が損傷する可能性があります）

- 装置を極端に高温（装置の仕様書で詳細な動作温度を確認してください）、低温、塵埃の多い、または湿気の多い場所に置かないでください。また、高レベルの電磁波にさらさないでください。
- 室内用装置のカバーは、雨や湿気から保護してください。
- 装置を直射日光、換気不良の場所、またはヒーターやラジエーターなどの熱源にさらさないでください（無視すると火災の危険があります）。
- 装置を太陽や極端に明るい方向に向けないでください。そうすると、画像の白化やにじみが発生する可能性があります（これは故障ではありませんが）、同時にセンサーの耐久性に影響を与える可能性があります。
- デバイスカバーを開ける際は、必ず付属の手袋を使用してください。デバイスカバーに直接触れないようにご注意ください。指の酸性汗がデバイスカバーの表面コーティングを腐食する可能性があります。
- デバイスカバーの内外表面を清掃する際は、柔らかく乾いた布を使用し、アルカリ性洗剤は使用しないでください。
- 梱包材は開封後、今後の使用のために保管してください。万一故障が発生した場合は、元の梱包材と共に工場へ返送してください。元の梱包材なしで輸送した場合、デバイスに損傷が生じ、追加費用が発生する可能性があります。
- バッテリーの不適切な使用または交換は、爆発の危険を引き起こす可能性があります。バッテリーは、同じまたは同等のタイプのものと交換してください。使用済みのバッテリーは、バッテリー製造元の指示に従って処分してください。
- デバイスのライセンスは、以下のウェブサイトから確認できます：*http://opensource.hikvision.com/Home/List? id=46*.

対応モデル

アクセス制御端末には、以下のモデルが含まれます：

製品名	モデル	ワイヤレス
アクセス制御端末	DS-K1T502DBWX-C	13.56 MHz カード読み取り周波数、Wi-Fi、2.4GHz、Bluetooth
	DS-K1T502DBFWX-C	13.56 MHz カード読み取り周波数、Wi-Fi、2.4GHz、Bluetooth
	DS-K1T502DBFWX	13.56 MHz カード読み取り周波数、Wi-Fi、2.4GHz、Bluetooth
	DS-K1T502DBWX	13.56 MHz カード読み取り周波数、Wi-Fi、2.4GHz、Bluetooth

表1-1 利用可能なモバイルウェブブラウザ

オペレーティングシステム	ブラウザ	バージョン	利用可能
Android	Xiaomi 12、デフォルトのブラウザ	16.6.6	はい
	Huawei P30、デフォルトのブラウザ	12.1.1.321	はい
	Xiaomi 5s plus、デフォルトのブラウザ	14.2.22	はい
	Huawei P30 Pro、デフォルトのブラウザ	12.1.2.301	はい
	Redmi K40、デフォルトのブラウザ	16.5.12	はい
iOS	Safari	15.4	はい

目次

第1章 概要

1.1 概要

アクセス制御端末は、認証機能を備えたアクセス制御端末の一種です。双方向音声通信、リモートライブビュー、画像キャプチャ、NVR経由の動画記録などに対応しています。

1.2 機能

- 1台のデバイスでアクセス制御、ビデオインターコム、ビデオセキュリティを管理
- IP65およびIK09保護規格に準拠し、亜鉛合金素材を採用することで高い安定性を実現
- 指紋認証、カード認証など、複数の認証方法に対応

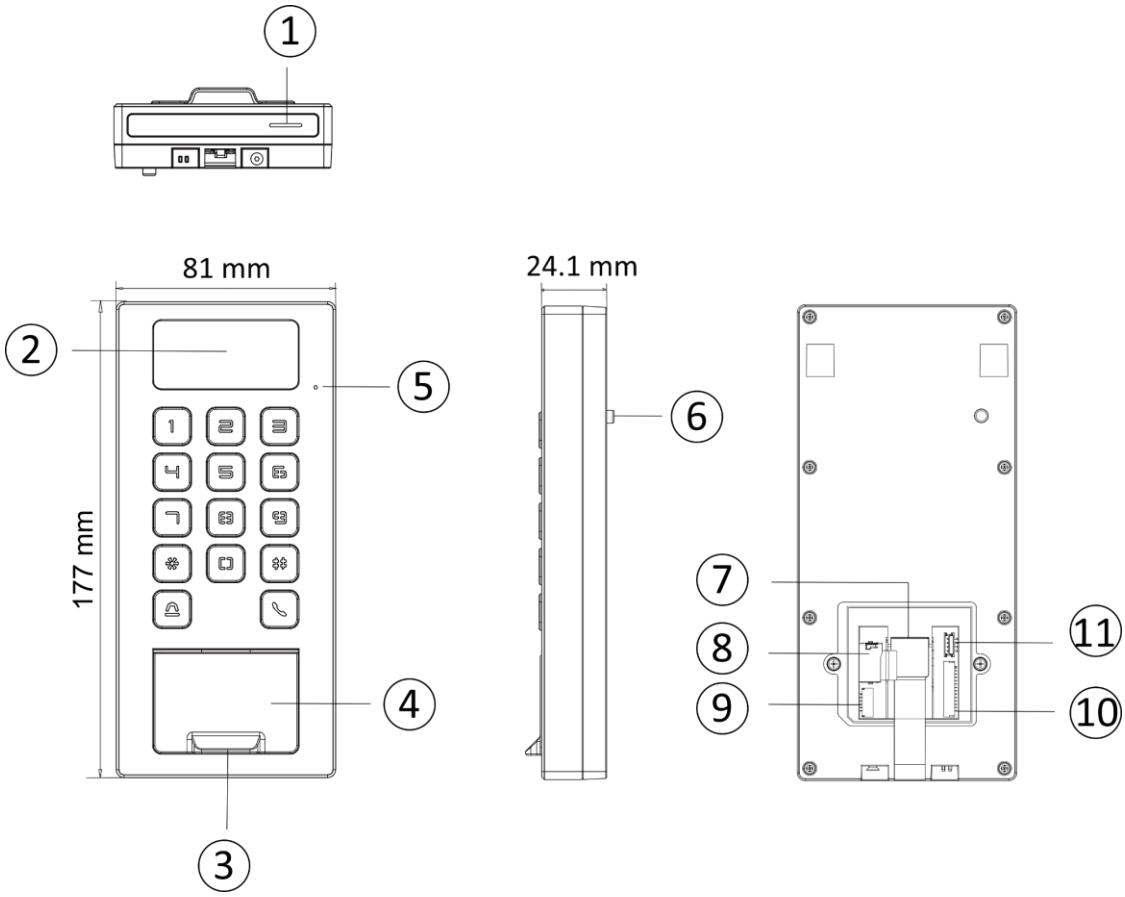
注意

指紋認証機能は、デバイスモジュールの特定の部品でサポートされています。

- Hik-Connectモバイルアプリ経由のリモートコントロール
- Wiegandプロトコル経由で外部アクセスコントローラーと接続
- SIP 2.0プロトコル経由の双方向音声通信
- RS-485通信で外部カードリーダーと接続可能
- AP経由のネットワーク接続に対応
- H.265動画エンコード形式に対応

1.3 外観説明

デバイスの外観説明を確認してください。



注意

ここに掲載されている画像は参考用です。

表1-1 外観説明

番号	説明
1	スピーカー
2	カメラ（一部のデバイスモデルで対応）
3	指紋認証モジュール（一部のデバイスモデルで対応）
4	カード挿入部
5	マイク
6	改ざん
7	ネットワークインターフェース
8	SDカードスロット
9	アラーム入出力用配線端子

番号	説明
10	配線端子
11	デバッグポート（デバッグ専用）

第2章 インストール

2.1 インストール環境

- デバイスを、光源から少なくとも2メートル以上、窓やドアから少なくとも3メートル以上離して設置してください。
- 環境の照度が100ルクス以上であることを確認してください。

注意

設置環境の詳細については、*「設置環境のヒント」*を参照してください。

2.2 ギャングボックスなしでインストール

手順

注意

追加の力は、機器の重量の3倍に等しいものでなければなりません。機器とその関連する取り付け手段は、取り付け中に確実に固定されている必要があります。取り付け後、機器（関連する取り付けプレートを含む）は損傷を受けてはなりません。

1. 取り付けプレートを壁に4本の付属ネジ（SC-KA4X25-SUS）で固定してください。

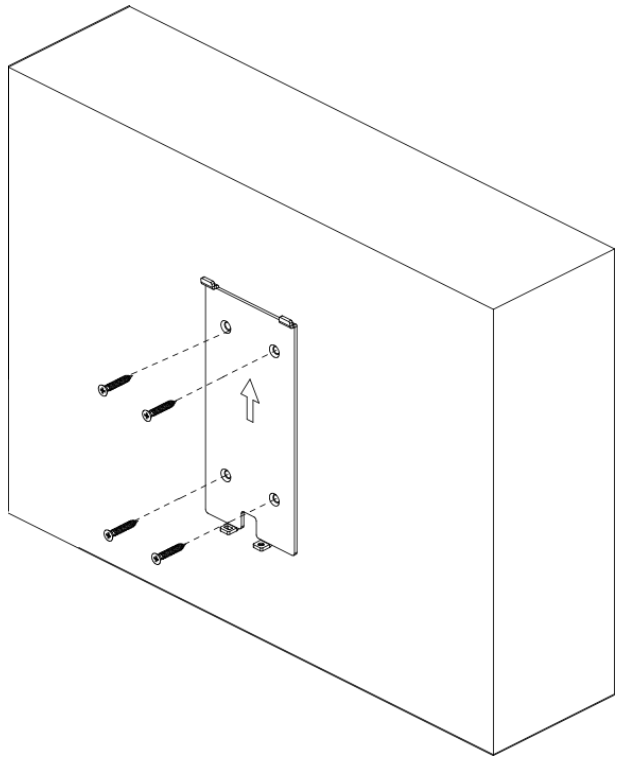


図2-1 固定取り付け板の固定

2. ケーブルを固定プレート のケーブル穴に通し、対応する外部機器のケーブルに接続してください。

3. デバイス後部パネルと壁の接合部（下側を除く）にシリコーンシーラントを塗布し、雨滴の侵入を防いでください。

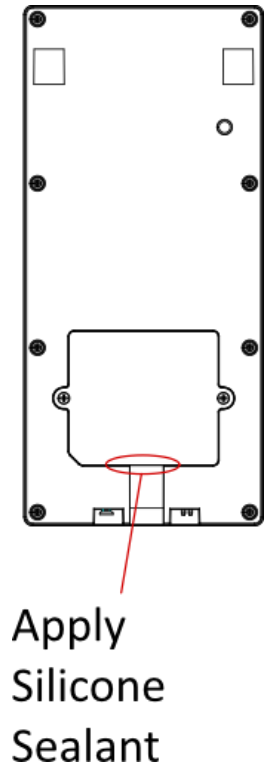


図2-2 側面へのシリコーンシーラントの塗布

4. デバイスをマウントプレートに合わせ、付属のネジ（SC-KM3X6-T10-SUS）1本でデバイスをマウントプレートに固定します。

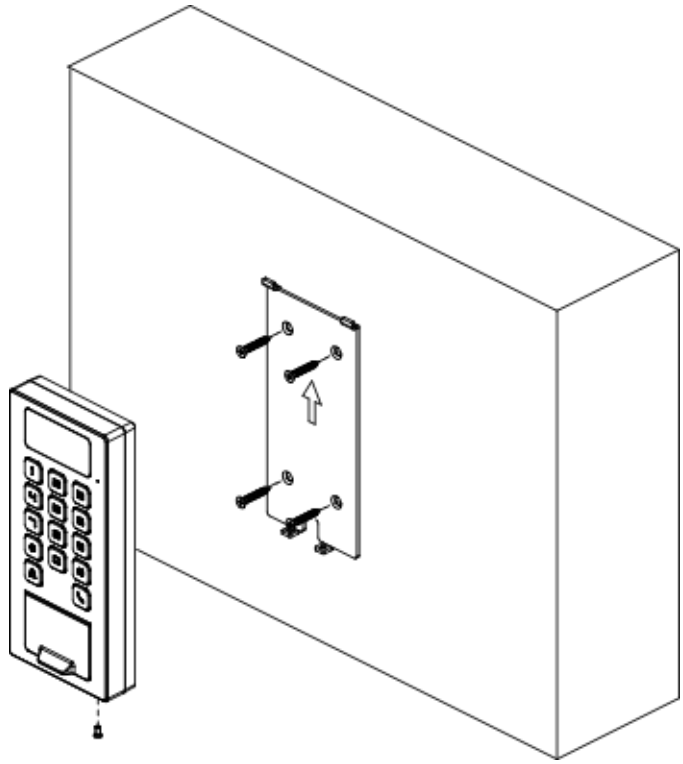


図2-3 デバイスを固定する

第3章 デバイスの配線

3.1 端子説明

端子には、電源入力、アラーム入力、アラーム出力、RS-485、Wiegand出力、およびドアロックが含まれます。

ターミナルの図は次のとおりです:

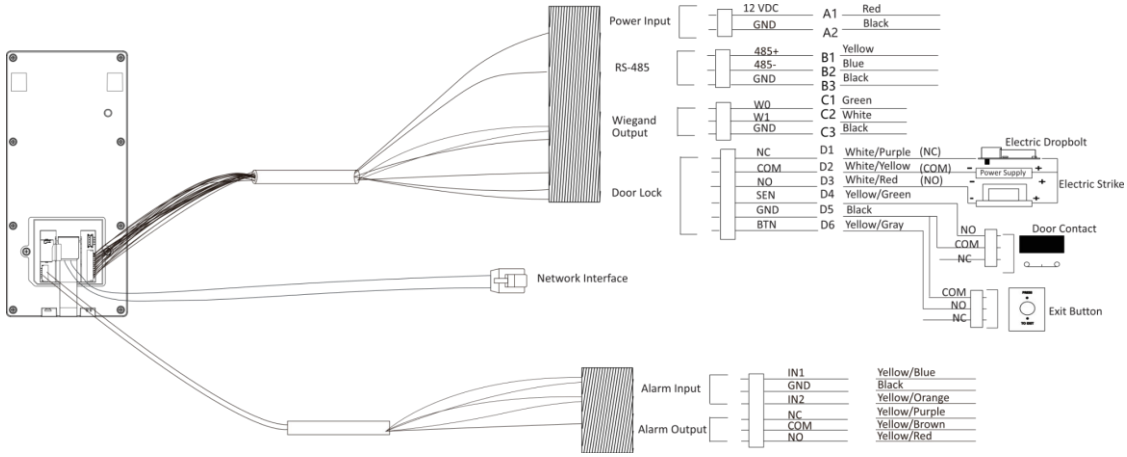


図3-1 ターミナル図

各端子の説明は次のとおりです:

表3-1 ターミナルの説明

グループ	番号	機能	色	名前	説明
グループA	A1	入力電力	赤	+12 V	12 VDC電源供給
	A2		黒	GND	接地
グループB	B1	RS-485	黄色	485+	RS-485 配線
	B2		青	485-	
	B3		黒	GND	接地
グループC	C1	ワイガンド	グリーン	W0	ワイガンド配線 0
	C2		ホワイト	W1	Wiegand 配線 1
	C3		黒	GND	接地

グループ	番号	機能	色	名前	説明
グループ D	D1	ドアロック	白/紫	NC	ロック配線（NC）
	D2		白/黄	COM	共通
	D3		白/赤	NO	ロック配線（NO）
	D4		黄色/緑	センサー	ドアコンタクト
	D5		黒	GND	接地
	D6		黄色/灰色	BTN	出口ドア配線

3.2 外部デバイス配線

外部デバイスを配線してください。

配線図は次のとおりです。

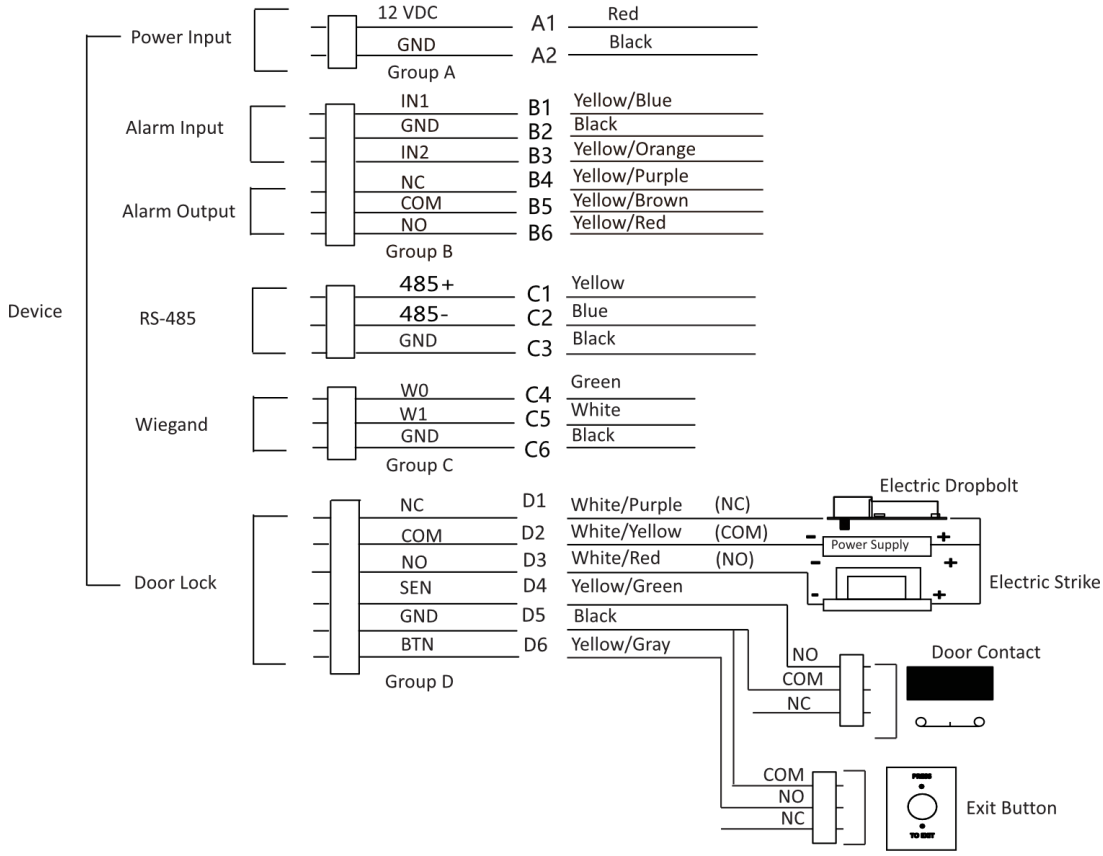


図3-2 外部デバイス配線

3.3 セキュアドア制御ユニットの配線

セキュアドア制御ユニットと端子をつなげます。配線図は次のとおりです。

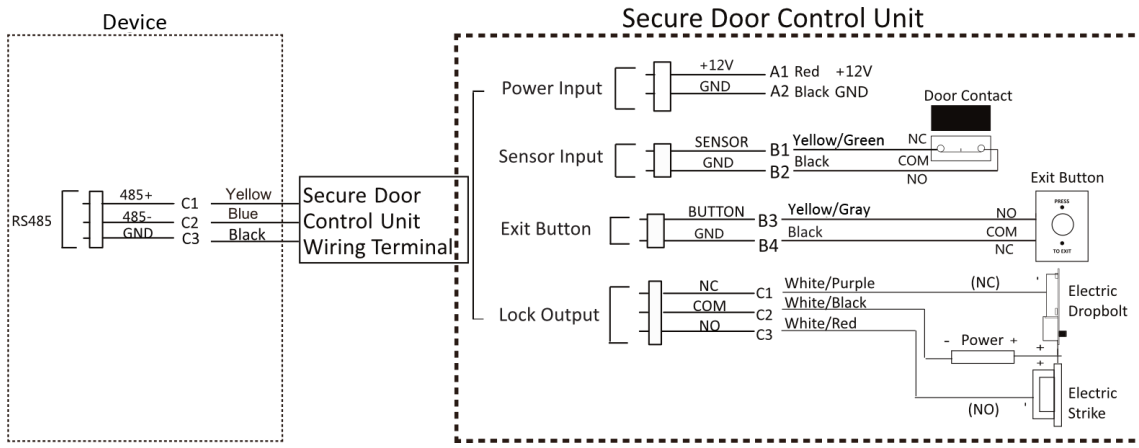


図3-3 セキュアドア制御ユニットの配線

注意

- セキュアドア制御ユニットは、外部電源に別途接続する必要があります。推奨される外部電源は12V、0.5Aです。
- 安全性が特に高いシナリオでは、まずセキュアドアコントロールユニットの配線を使用してください。
- セキュアドアコントロールユニットの別途購入については、技術サポートにお問い合わせください。
- ここにある図は配線の一部です。詳細については、セキュアドアコントロールユニットのユーザーマニュアルをご確認ください。
- このデバイスは、バインディング機能を備えたセキュアドアコントロールユニットとの接続をサポートしています。他のデバイスとバインディングされているセキュアドアコントロールユニットは、新しいデバイスとバインディングする前にバインディングを解除する必要があります。

第4章 アクティベーション

デバイスを初めてログインする前に、デバイスをアクティベートする必要があります。デバイスを電源投入後、システムはデバイスアクティベーション画面に切り替わります。

デバイスのアクティベーションは、デバイス本体、SADPツール、およびクライアントソフトウェアのいずれかを使用して行うことができます。デバイスのデフォルト設定は以下の通りです：

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

4.1 モバイルウェブ経由でのアクティベーション

モバイルウェブ経由でデバイスをアクティベーションできます。

手順

注意
デバイスを初めて電源を入れた後、ホットスポット機能がデフォルトで有効になっています。

1. スマートフォンのWi-Fi機能を有効にします。デバイスホットスポットを検索し、追加します（ホットスポット名：AP_シリアル番号）。

   注意
   - ホットスポット名/パスワード：AP_シリアル番号
   - デバイスのキーパッドでキー5を5秒間長押しして、ホットスポット機能を有効/無効にします。
   - デバイスを起動後30分経過すると、ホットスポット機能が自動的に無効になります。
   - デバイスをアクティベートした後、ホットスポットのパスワードはデバイスアクティベートパスワードに変更されます。

2. スマートフォンはウェブブラウザのページに切り替わります。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
   「admin」と「nimda」を含む文字は、アクティベーションパスワードとして設定できません。

   注意
   強固なパスワードの設定を推奨します-製品のセキュリティを強化するため、ご自身で選択した強固なパスワード（大文字、小文字、数字、特殊文字をそれぞれ1つ以上含む8文字以上）を設定することを強く推奨します。また、特に高セキュリティシステムでは、パスワードを定期的に変更することを推奨します。月次または週次でのパスワード変更は、製品の保護をさらに強化します。

3. **「アクティベート」**をクリックしてください。
4. デバイスのIPアドレスを編集します。IPアドレスは、SADPツール、PCのウェブブラウザ、またはクライアントソフトウェアから編集できます。

4.2 ウェブブラウザ経由でアクティベート

ウェブブラウザ経由でデバイスをアクティベートできます。

手順

1. ウェブブラウザのアドレスバーにデバイスのデフォルトIPアドレス（192.0.0.64）を入力し、

   Enter キーを押します。

   注意

   デバイスのIPアドレスとコンピュータのIPアドレスが同じ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

   強固なパスワードの使用を推奨します-製品のセキュリティを強化するため、ご自身で選択した強固なパスワード（大文字、小文字、数字、特殊文字をそれぞれ1つ以上含む8文字以上）を設定することを強く推奨します。また、特に高セキュリティシステムでは、パスワードを定期的に変更することを推奨します。月次または週次でのパスワード変更は、製品の保護をさらに強化します。

   「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. **注意ート**をクリックしてください。
4. デバイスのIPアドレスを編集します。IPアドレスは、SADPツール、デバイス、またはクライアントソフトウェアから編集できます。

4.3 SADP経由でアクティベートします。

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

開始前に

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

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

手順

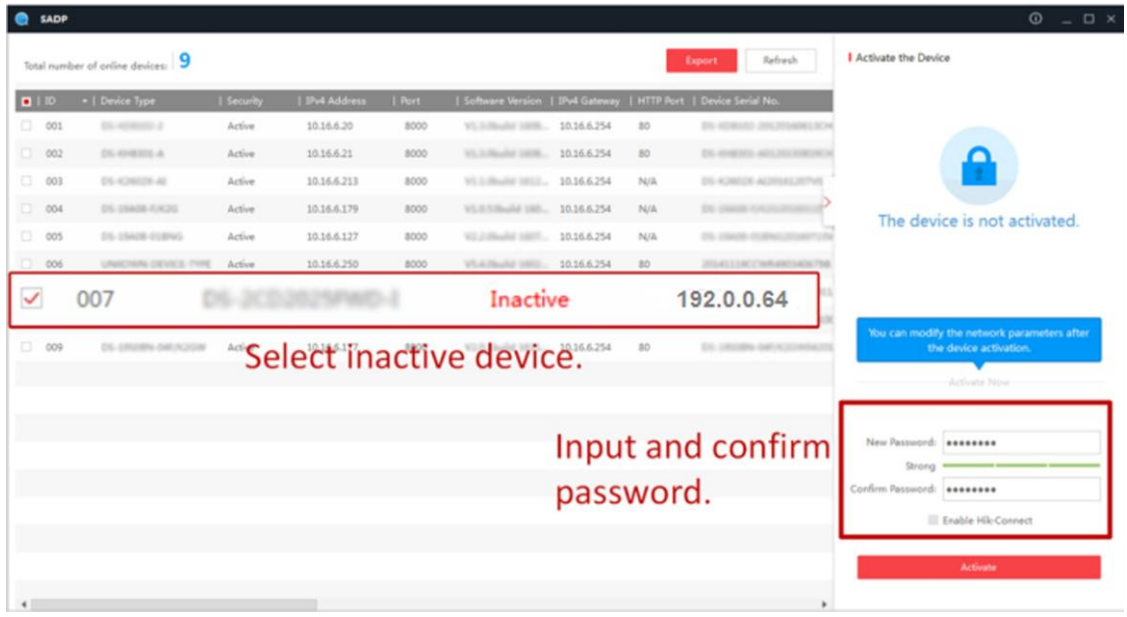
1. SADP ソフトウェアを実行し、オンラインデバイスを検索します。

2. オンラインデバイス一覧から対象のデバイスを検索し、選択します。
3. 新しいパスワード（管理者パスワード）を入力し、パスワードを確認します。

注意

強固なパスワードの使用を推奨します-製品のセキュリティを強化するため、ご自身で選択した強固なパスワード（大文字、小文字、数字、特殊文字をそれぞれ1つ以上含む8文字以上）を設定することを強く推奨します。また、特に高セキュリティシステムでは、パスワードを定期的に変更することを推奨します。月次または週次でのパスワード変更は、製品の保護をさらに強化します。

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



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

4.4 iVMS-4200 クライアント ソフトウェア経由でデバイスを有効化

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、パスワードを作成して有効化する必要があります。

手順

注意
この機能はデバイスでサポートされている必要があります。

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

注意

デバイスのパスワードの強度は自動的に確認できます。製品のセキュリティを強化するため、ご自身で選択したパスワード（8文字以上で、大文字、小文字、数字、特殊文字の少なくとも3種類を含む）に変更することを強くおすすめします。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すすめします。月次または週次での変更は、製品の保護をさらに強化します。
すべてのパスワードおよびその他のセキュリティ設定の適切な設定は、インストール担当者および/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有効化します。

第5章 身分認証

ネットワーク設定、システムパラメーター設定、およびユーザー設定が完了したら、身分認証の初期画面に戻ることができます。システムは、設定された認証モードに従ってユーザーを認証します。

5.1 単一認証情報による認証

認証前にユーザー認証タイプを設定します。詳細については、を参照してください。指紋、カード、PIN、またはQRコードで認証します。

指紋

登録済みの指紋を指紋モジュールに置き、指紋による認証を開始します。

カード

カードをカード提示エリアに提示し、カード経由で認証を開始してください。

注意

カードは通常のICカードまたは暗号化カードです。

QRコード

デバイスのカメラにQRコードを向けて、QRコード経由で認証を行います。

注意

- 動的QRコードは有効期間内に認証する必要があります。QRコードが更新されると、古いQRコードは認証されなくなります。
- QRコードによる認証は、デバイスでサポートされている必要があります。

PIN

PINを入力してPINで認証してください。

認証が完了すると、「認証完了」というメッセージが表示されます。

5.2 複数の認証情報を使用して認証する

開始前に

認証前にユーザー認証の種類を設定してください。詳細については、を参照してください。

手順

1. ライブビューページに表示される指示に従って、任意の認証情報を認証します。

注意

- カードは通常のICカードまたは暗号化カードのいずれかです。
- QRコードスキャン機能が有効になっている場合、デバイスのカメラにQRコードを向けることで、QRコードによる認証を行うことができます。

2. 前の認証情報が認証された後、他の認証情報を認証し続けてください。

注意

指紋スキャンに関する詳細情報は、*「指紋スキャンのヒント」*を参照してください。認証が成功した場合、「認証完了」というメッセージが表示されます。

第6章 コールとビデオインターコム

SIPサーバーのIPを設定すると、デバイス間の通話とビデオインターコムが利用可能になります。

デバイスAをSIPサーバーとして設定し、デバイスAのIPアドレスをSIPサーバーのIPアドレスに設定します。詳細については、を参照してください。相互に通信する必要がある他のすべてのデバイスは、サーバーに登録する必要があります。

デバイスルーム番号を設定します。詳細については、「***Web経由でデバイス番号を設定する」***を参照してください。

デバイスのメイン画面で、通話先のデバイス番号を入力します。相手デバイスが応答すると、ビデオインターコムが実行できます。

第7章 ウェブブラウザ経由の操作

7.1 ログイン

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

注意
デバイスがアクティベートされていることを確認してください。アクティベーションに関する詳細情報は、*アクティベーション*をご覧ください。

ウェブ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移動します。
デバイスのユーザー名とパスワードを入力し、**[ログイン]** をクリックします。

クライアントソフトウェアのリモート設定経由でログイン

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画面に移動します。

7.2 パスワードを忘れた場合

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

ログイン画面で「**パスワードを忘れた**」をクリックします。**検証モード**を選択します。

セキュリティ質問による確認

セキュリティ質問に回答してください。

メール認証

1. QRコードをエクスポートし、***pw_recovery@hikvision.com*** 宛てに添付ファイルとして送信してください。
2. 5分以内に、ご登録のメールアドレスに検証コードが送信されます。
3. 確認コードを「確認コード」欄に入力し、ご本人確認を行ってください。**次に「次へ」**をクリックし、新しいパスワードを作成し、確認してください。

7.3 Webプラグインのダウンロード

プラグイン非対応のライブビューと、プラグインをダウンロード後のライブビューの両方が利用可能です。より良いライブビューをご利用いただくためには、ライブビュー用のプラグインのダウンロードを推奨します。

「 」をクリックしてください。→「**Download Web Pug-In**」をクリックして、プラグインをローカルにダウンロードしてください。

7.4 ヘルプ

7.4.1 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。

画面右上にある「 」をクリックし、→ **Open Source Software Statement** を選択してライセンスを確認してください。

7.4.2 オンラインヘルプドキュメントを表示

Web 設定のヘルプドキュメントを表示できます。

Webページの右上にある「 」をクリックし、次に「→ **Online Document**」をクリックしてドキュメントを表示します。

7.5 ログアウト

アカウントからログアウトします。

「**admin**」をクリックし、→ の「**Logout**」をクリックし、→ の「**OK**」をクリックしてログアウトします。

7.6 Webブラウザからのクイック操作

7.6.1 セキュリティ質問を設定する

デバイスアクティベーションパスワードを忘れた場合、セキュリティ質問とメールを使用してパスワードを変更できます。設定前にセキュリティ質問を設定してください。

ウェブページの右上にある「 」をクリックして、**パスワード変更**ページに移動します。

セキュリティ質問の確認

セキュリティ質問に回答してください。

メール確認

1. QRコードをエクスポートし、***pw_recovery@hikvision.com* に**添付ファイルとして送信してください。
2. ご登録のメールアドレスに5分以内に確認コードが送信されます。
3. 検証コードを検証コード欄に入力し、ご本人確認を行ってください。**次に進む**をクリックしてください。または、**スキップ**をクリックしてこのステップをスキップできます。

7.6.2 言語を選択

デバイスのシステム言語を選択できます。

ウェブページの右上にある「 」をクリックして、**デバイス**言語設定ページに移動します。ドロップダウンリストからデバイスシステムの言語を選択できます。

デフォルトでは、システム言語は英語です。

注意

システム言語を変更すると、デバイスが自動的に再起動します。

7.6.3 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移動します。

デバイス時間

デバイスの時間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。

時間同期モード 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、デバイスの時間は手動で同期されます。デバイスの時間を手動で設定するか、または**「コンピュータの時間と同期」にチェック**を付けて、デバイスの時間をコンピュータの時間と同期させることができます。

夏時間

夏時間（DST）を有効にできます。夏時間の開始時間、終了時間、および偏移時間を設定し、確認できます。

「次へ」をクリックして設定を保存し、次のパラメーターに移動します。または**「スキップ」**をクリックして時間設定をスキップします。

7.6.4 プライバシー設定

画像のアップロードと保存に関するパラメーターを設定します。

ウェブページの右上にある「 」をクリックしてウィザードページに移動します。デバイス言語、時間、環境を設定後、**「次へ」**をクリックしてプライバシー設定ページに移動できます。

画像のアップロードと保存

リンクしたカメラで撮影した写真をアップロード

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

リンクしたカメラで撮影した写真を保存

この機能を有効にすると、リンクされたカメラで撮影した画像をデバイスに保存できます。設定を保存して次のパラメーターに進むには**「次へ」**をクリックしてください。または、プライバシー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。

7.6.5 番号とシステムネットワーク

手順

1. ウェブページの右上にある「 」をクリックしてウィザードページに移動します。以前の設定後、**次へをクリック**して「**No. and Network System Network**」設定ページに移動します。
2. デバイスタイプを設定します。

注意

- デバイスタイプを「**ドアステーション**」に設定すると、**フロア番号**、**ドアステーション番号**、**コミュニティ番号**、**建物番号**、**ユニット番号**、**フロア番号**、および**ドアステーション番号**を設定できます。
- デバイスタイプを「**外ドアステーション**」に設定した場合、**外ドアステーション番号**を設定できます。

コミュニティ番号

デバイスタイプ

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

コミュニティ番号

デバイスのコミュニティ番号を設定します。

建物番号

装置の番号を設定してください

ユニット番号

デバイスユニット番号を設定してください。

階番号

デバイスが設置されている階番号を設定してください。

ドアステーション番号

デバイスが設置されているドアステーション番号を設定します。

注

メインドアステーション番号は0で、サブドアステーション番号は1から16までです。

外ドアステーション番号

デバイスにインストールされた外ドアステーションの番号を設定してください。

注

番号は1から99までです。

3. ビデオインターコムのネットワークパラメーターを設定します。

登録パスワード

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

メインステーションのIPアドレス

通信に使用するメインステーションのIPアドレスを入力してください。

プライベートサーバーIP

SIPサーバーのIPアドレスを指します。通信に使用するメインステーションのIPアドレスを入力してください。この時点では、メインステーションがSIPサーバーとして機能します。他のインターコムデバイスはこのサーバーアドレスに登録する必要があります。

プロトコル 1.0 を有効にする

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

4. 設定を完了するには**「完了」**をクリックしてください。

7.7 ユーザー管理

「追加」をクリックして、基本情報、証明書、認証、設定を含むユーザーの情報を追加します。

基本情報の追加

「ユーザー管理」をクリックします。**「→」をクリックします。**「追加」**をクリックして**「ユーザー追加ページ」に移動します。
従業員ID、氏名、性別、従業員タイプなどの基本情報を入力します。
人物の種類に「**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。

権限時間を設定する

「Person Management」をクリックし、**→をクリックして**「Add Person」ページに移動します。
「長期有効ユーザーを有効にする」を選択するか、または**「長期有効ユーザー」**を設定すると、そのユーザーは設定した期間内のみ権限が有効になります。
ドアの権限を設定します。
「保存」をクリックして設定を保存します。

カードを追加

「Person Management」をクリックし、**「→」をクリックして**「Add Person」ページに移動します。
「カードを追加」をクリックし、**カード番号**を入力し、**プロパティ**を選択し、**OKをクリック**してカードを追加します。
「保存」をクリックして設定を保存します。

指紋を追加

注意
指紋機能に対応したデバイスのみ、指紋を追加できます。

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

「指紋を追加」をクリックし、デバイスの指紋認証モジュールに指を置いて指紋を追加します。

「保存」をクリックして設定を保存します。

PINの追加

パスワードを設定する前に、パスワードがデバイス設定の個人用PINかプラットフォーム適用型個人用PINかを明確にする必要があります。デバイス設定の個人用PINの場合、デバイスまたはウェブ上で作成または編集でき、他のプラットフォームでは設定できません；プラットフォーム適用型個人用PINの場合、プラットフォーム上で作成または編集でき、デバイスに発行されるまで使用できません。デバイスまたはウェブ上で設定できません。

→設定をクリックし、**→ セキュリティ → パスワードモード**を選択し、**PIN**モードとして**「デバイス設定の個人用PIN」**を選択します。**個人管理**をクリックし、**追加**をクリックして「個人を追加」ページに移動します。

PINを設定します。

保存をクリックして設定を保存します。

認証設定

「Person Management」をクリックし、**「→」を選択し、**「Add」をクリックして「Add Person」ページに移動します。認証タイプを設定します。

保存をクリックして設定を保存します。

ユーザーを削除

ユーザー管理ページで、削除するユーザーを選択し、**削除**をクリックします。**すべて削除**をクリックすると、すべてのユーザーが削除されます。

ユーザー編集

人物管理ページで、編集が必要な人物を選択します。人物情報を編集するには、[ ] をクリックします。

フィルタ

人物管理ページで、**従業員ID/名前/カード番号**を入力します。**資格ステータス**を選択し、**フィルター**をクリックして人物をフィルターします。**リセット**をクリックしてすべての条件をクリアします。

7.8 アクセス制御管理

7.8.1 概要

デバイスのライブ動画、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、およびデバイス容量を確認できます。

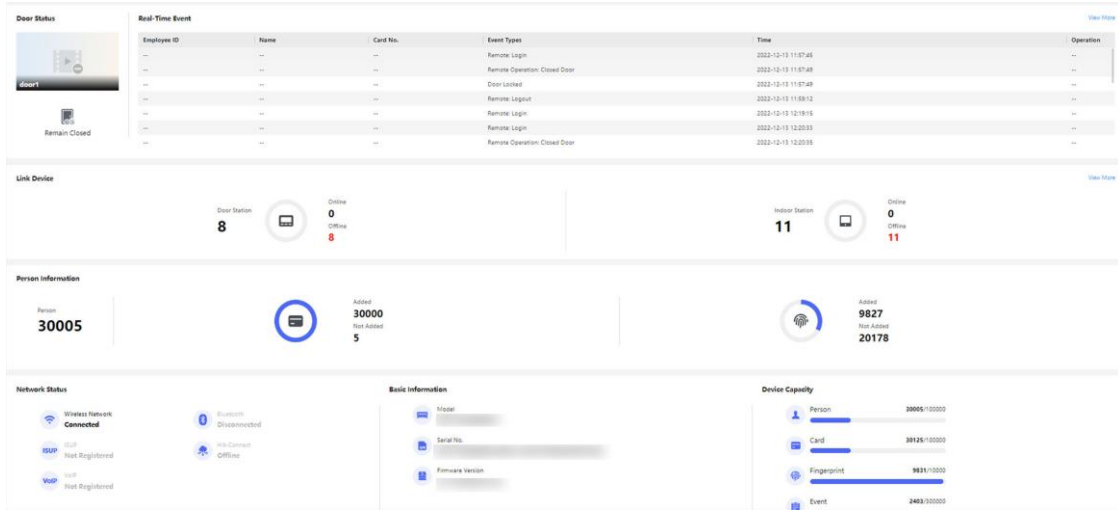


図7-1 概要ページ

機能説明:

ドアの状態

「 」をクリックして、デバイスのライブビューを表示します。

ライブビューを開始する際に音量を設定してください。

注意

双方向オーディオを開始時に音量を調整すると、繰り返し音が聞こえる場合があります。ライブビューを開始時に

画像を撮影できます。

ライブビューを開始する際にストリーミングタイプを選択してください。メインストリームとサブストリームから選択できます。

フルスクリーン表示。

/ / /

ドアの状態は、開いている/閉まっている/開いたまま/閉まったままです。

制御状態

実際のニーズに応じて、開いている/閉まっている/開いたまま/閉まったままの状態を選択できます。

リアルタイムイベント

イベントの従業員ID、名前、カード番号、イベントタイプ、時間、および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。検索結果は右側のパネルに表示されます。

個人情報

人、カード、指紋の追加済みと未追加の情報を確認できます。

ネットワーク状態

有線ネットワーク、無線ネットワーク、Bluetooth、ISUP、VoIP、およびクラウドサービスの接続状態と登録状態を確認できます。

基本情報

モデル、シリアル番号、およびファームウェアバージョンを確認できます。

デバイス容量

人物、カード、イベント、および指紋の容量を確認できます。

注

指紋機能に対応したデバイスのみ、指紋の容量を表示できます。

詳細を表示

「詳細を表示」をクリックすると、イベントの詳細を確認できます。

7.8.2 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移動します。

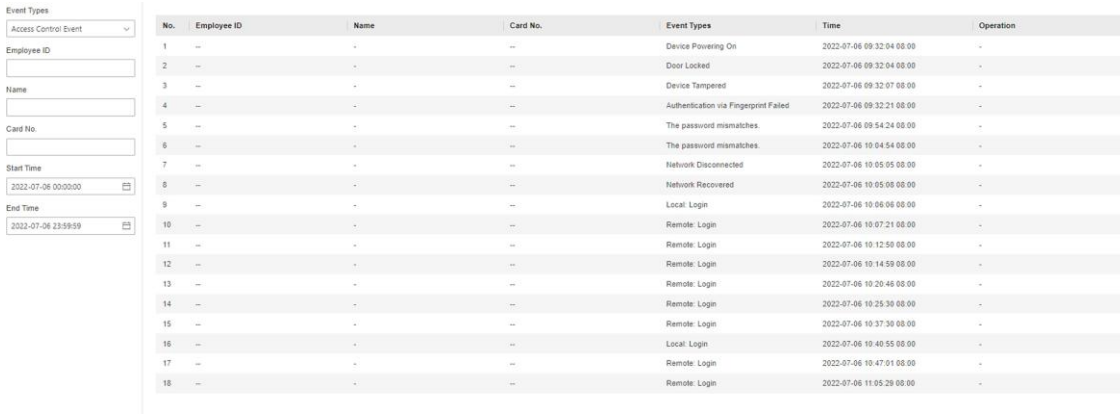


図7-2 イベント検索

イベントの種類、従業員ID、名前、カード番号、開始時間、終了時間などの検索条件を入力し、**検索**をクリックします。結果は右側のパネルに表示されます。

7.8.3 ドアパラメーター設定

ドアの解錠パラメーターを設定します。

ドア名の設定

ドアの名前を作成します。

「アクセス制御」→「→ パラメーター設定」→「→ ドアパラメーター」をクリックして設定画面を開きます。**ドア名**を入力し、**「保存」**をクリックします。

PC Web経由でドアの開錠時間を設定

カードをかざした後にドアロックが開く時間を設定できます。

アクセス制御をクリックし、**→ パラメーター設定、→ ドアパラメーター**を選択して設定画面に移動します。
開錠後の動作時間（ドアが開錠された後の動作時間）を設定します。設定した時間内にドアが開かれない場合、ドアは自動的にロックされます。設定可能な時間：1秒から255秒。
「保存」をクリックします。

PC Web 経由でドア開時間切れアラームを設定

ロック動作時間が経過してもドアが閉まらない場合、アクセス制御ポイントがアラームを鳴らします。

アクセス制御をクリックし、**→ パラメーター設定、→ ドアパラメーター**を選択して設定画面を開きます。
ドアの開錠タイムアウトアラームを設定します。ドアがロック動作時間内に閉まらない場合、アクセス制御ポイントでアラームが鳴ります。0に設定すると、アラームは有効になりません。
保存をクリックします。

PC ウェブ経由でドア磁気センサータイプを設定

配線方法に応じてドアコンタクトタイプを選択できます。

アクセス制御 → パラメーター設定 → ドアパラメーターをクリックして設定画面に入ります。磁気センサータイプを「閉じたまま」または「開いたまま」を選択します。デフォルトは「**閉じたまま**」です。
（特別支援を要する者を除く）。
「保存」をクリックしてください。

PCウェブ経由で退出ボタンを設定

実際の配線方法に応じて、退出ボタンを「常に開く」または「常に閉じる」に設定します。

アクセス制御をクリックします。**→ パラメーター設定をクリックします。→ ドアパラメーター**をクリックして設定画面に入ります。**退出ボタンタイプ**を設定します。デフォルトでは「開いたまま」（特別な要件を除く）です。

保存をクリックします。

PC Web経由で拡張開錠時間を設定

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

アクセス制御をクリックし、**→ パラメーター設定、→ ドアパラメーター**を選択して設定画面を開きます。

拡張開錠時間を設定します。拡張アクセス権限を持つユーザーがカードをかざした後、適切な遅延後にドアの接触センサーを有効にできます。

保存をクリックします。

PC ウェブ経由で最初のユーザーによるドアの開いたまま保持時間を設定します。

最初の人が認証されると、複数の人物がドアへのアクセスまたは他の認証アクションを実行できるようになります。

「アクセス制御」をクリックし、**「→ パラメーター設定」→「→ ドアパラメーター」**を選択して設定画面を開きます。最初の人がドア内にいる際のドアの開状態持続時間を設定し、**「保存」**をクリックします。

PCウェブ経由で緊急コードを設定

緊急コードを設定後、緊急事態が発生した際にコードを入力してドアを開錠します。同時に、アクセス制御システムは緊急事態を報告します。

「アクセス制御」→「→ パラメーター設定」→「→ ドアパラメーター」をクリックして設定画面を開きます。緊急コードを設定し、「**保存**」をクリックします。

注意

緊急コードとスーパーパスワードは重複できません。通常、4から8桁の数字で構成されます。

PCウェブ経由でスーパーパスワードを設定

管理者または指定されたユーザーがスーパーパスワードを入力してドアを開錠できます。

アクセス制御 → パラメーター設定 → ドアパラメーターをクリックして設定画面を開きます。**スーパーパスワード**を設定すると、指定されたユーザーがスーパーパスワードを入力してドアを開けることができます。

保存をクリックします。

注意
緊急コードとスーパーパスワードは重複できません。通常、4から8桁の数字で構成されます。

PCウェブ経由で解除コードを設定

管理者または指定されたユーザーは、アラームを解除するために解除コードを入力できます。**アクセス制御 → パラメーター設定 → ドアパラメーター**をクリックします。

アラームを**解除するためのコード**を作成します。アラームが鳴った際に、この解除コードを入力することでアラームを解除できます。
アラームを解除できます。

保存をクリックします。

7.8.4 認証設定

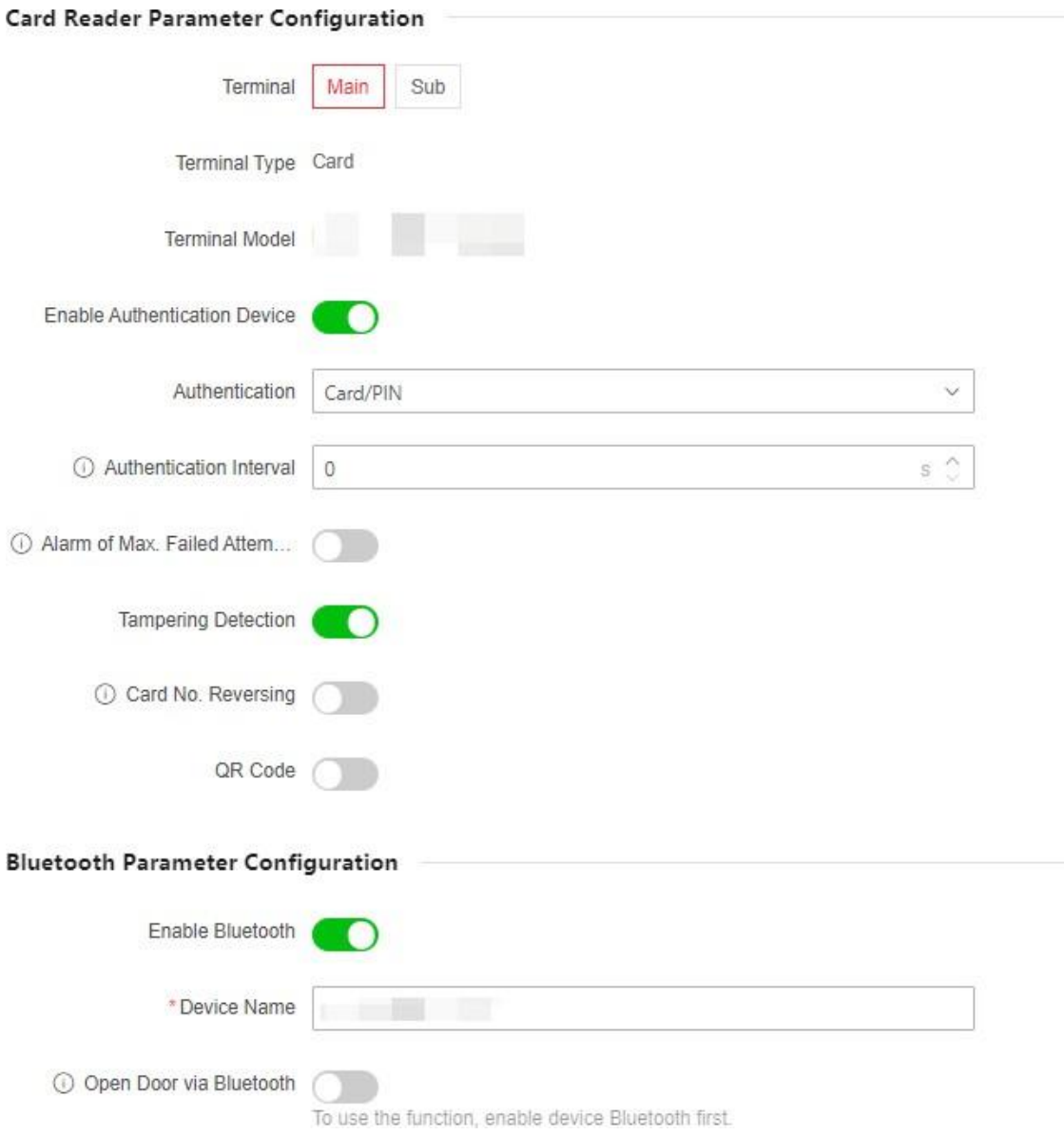


図7-3 認証設定

PC Web経由でメインまたはサブのカードリーダーを選択

ユーザー認証用の端末を設定します。

アクセス制御をクリックします。→ **パラメーター設定**→ **認証設定**をクリックして設定画面に移動します。端末をメインまたはサブカードリーダーとして選択します。

その他のパラメーターを設定し、**保存**をクリックします。

PC Web経由でターミナルのタイプとモデルを確認します。

ターミナルの種類とモデルを確認できます。

アクセス制御をクリックし、→ **パラメーター設定**、→ **認証設定**を選択して設定画面に移動します。**ターミナルタイプ**と**ターミナルモデル**を確認します。

PCウェブ経由で認証デバイスを有効化

有効化後、認証端末でカード読み取りが可能になります。

手順

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

PC ウェブ経由で認証を設定

認証の設定。

アクセス制御をクリックし、→ **パラメーター設定**、→ **認証設定**を選択して設定画面に移動します。

メインのカードリーダーをターミナルとして選択した場合、ドロップダウンリストから「認証」を選択できます。認証方法が複数ある場合は、**シングルクレデンシャル認証タイムアウト**と**初期認証タイプの制御を設定**する必要があります。

シングルクレデンシャル認証タイムアウト

各認証の有効期間を設定できます。

注意

パスワード認証タイムアウトはデフォルトで20秒であり、上記の設定によって制限されません。

初期認証タイプの制御

有効にすると、選択したすべてのタイプが初回認証に使用可能です。

ターミナルとしてサブカードリーダーを選択した場合、ドロップダウンリストから「認証」を選択できます。

保存をクリックします。

PC Web経由で認証間隔を設定する

同じ人物の認証間隔を設定できます。設定された間隔内では、同じ人物は1回のみ認証可能です。2回目の認証は失敗します。設定された間隔内に他の人が認証した場合、その人物は再度認証可能です。

「アクセス制御」→「→ パラメーター設定」→「→ 認証設定」をクリックして設定画面に移動します。ターミナルをメインカードリーダーとして選択し、**認証間隔**を設定して「**保存**」をクリックします。

PCウェブ経由で最大失敗試行回数のアラームを有効にする

カード読み取り試行回数が設定値に達した際にアラームを通知するように設定します。

アクセス制御をクリックし、**→ パラメーター設定、→ 認証設定**を選択して設定画面に入ります。

メインまたはサブカードリーダーとして端末を選択し、**最大失敗試行回数のアラームを**有効にするためにスライダーを移動し、**最大認証失敗試行回数を**設定します。

「**保存**」をクリックします。

PC Web経由での改ざん検出の有効/無効設定

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

「アクセス制御」→「→ パラメーター設定」→「→ 認証設定」をクリックして設定画面に移動します。

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

「**保存**」をクリックします。

PC Web経由でのカード番号反転の有効/無効設定

カード番号の反転機能を有効または無効にできます。

「アクセス制御」→「→ パラメーター設定」→「→ 認証設定」をクリックして設定画面に移動します。**「カード番号反転」**を有効にすると、読み取ったカード番号が逆順で表示されます。

「**保存**」をクリックします。

Webクライアント経由でのQRコード認識の有効/無効設定

QRコード認識機能を有効/無効にできます。

アクセス制御→ パラメーター設定→ 認証設定をクリックして設定画面に入ります。

デバイスがQRコードの読み取りに対応している場合、**QRコードを**有効にすると、デバイスはカード番号から変換されたQRコードを読み取ることができます。

保存をクリックしてください。

コントローラーとの通信をPCウェブ経由で設定

サブカードリーダーごとのコントローラーとの通信を設定できます。カードリーダーが設定された時間内にアクセスコントローラーと接続できない場合、カードリーダーはオフライン状態になります。

「アクセス制御」→「→ パラメーター設定」→「→ 認証設定」をクリックして設定画面に移動します。

ターミナルをサブカードリーダーとして選択し、**[コントローラーとの通信間隔] を [毎回]** に設定し、**[保存]** をクリックします。

Webクライアント経由でのパスワード入力のタイムアウト期間を設定します

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

「アクセス制御」→「→ パラメーター設定」→「→ 認証設定」をクリックして設定画面に移動します。

サブカードリーダーをターミナルとして選択した場合、**パスワード入力時の最大間隔**を設定し、**[保存]をクリックします**。

PC Web経由でOK LEDの極性とエラー LEDの極性を設定します。

OKとERRインターフェースのダイオードの極性を実際の配線に合わせて設定します。デフォルトは正極性です。

「アクセス制御」→「→ パラメーター設定」→「→ 認証設定」をクリックして設定画面に入ります。

ターミナルをサブカードリーダーとして選択した場合、**OK LEDの**極性と**エラーLEDの極性を**設定し、**[保存]**をクリックします。

PC Web経由でBluetoothの有効/無効を切り替える

Bluetoothを有効にして、Bluetooth対応のサウンドデバイスを接続できます。

手順

1. **アクセスコントロール**をクリックし、**→ パラメーター設定、→ 認証設定**を選択して設定画面に入ります。
2. Bluetoothパラメーター設定セクションで、**Bluetoothを有効にします**。
3. **デバイス名に**外部サウンドを入力します。Bluetoothが接続された後、**保存**をクリックします。
4. **Bluetooth経由で**ドアの**開閉**をリモート操作可能にします。

注意

操作前に、デバイスをモバイルアプリに追加する必要があります。

7.8.5 カード設定

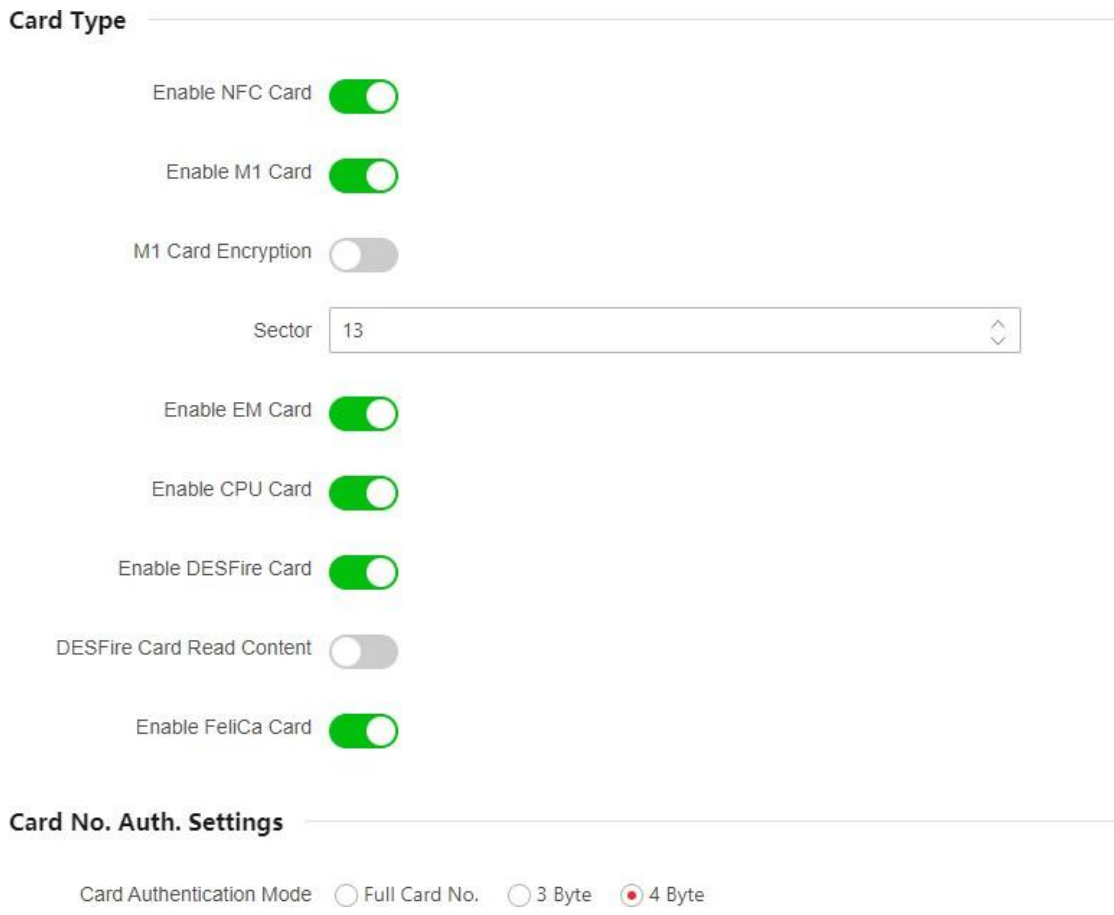


図7-4 カード設定

PC ウェブ経由で NFC 保護の有効/無効を切り替える

有効化後、デバイスはNFCカードを読み取ることができます。

「アクセス制御」→「→ パラメーター設定」→「→ カード設定」をクリックして設定画面に移動します。

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

Webクライアント経由でM1カード有効/無効化

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

M1 カードを有効にするをクリックします。

M1カード暗号化

M1カード暗号化を有効にすると、入口カードのセキュリティレベルが向上します。これにより、入口カードがコピーされにくくなります。

セクター

M1カード暗号化を有効にした後、暗号化セクターを設定する必要があります。

注意

セクター13を暗号化することをおすすめします。

保存をクリックします。

Webクライアント経由でEMカードの有効/無効を切り替える

有効化後、デバイスはEMカードを認識し、ユーザーはデバイス経由でEMカードをスワイプできます。**アクセス制御 → パラメーター設定 → カード設定**をクリックして設定画面に移動します。

EMカード有効化をクリックし、**保存**をクリックします。

注意

EMカードを読み取れる周辺カードリーダーが接続されている場合、この機能を有効にすると、このカードリーダー経由でEMカードをスワイプすることも可能です。

Webクライアント経由でCPUカードの設定を有効/無効にする

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

CPU カードを有効にするをクリックします。

「CPUカードの内容を読み取る」をクリックして**有効化します**。有効化後、デバイスはCPUカードの内容を読み取ることができます。

「保存」をクリックします。

有効化後、デバイスはDESFireカードを読み取ることができます。

アクセス制御 →→ パラメーター設定 →→ カード設定をクリックして設定画面に入ります。**DESFire カードを読み取り可能にするを選択します**。

「DESFireカードの内容を読み取る」を有効にし、**保存**をクリックします。有効化後、デバイスはDESFireカードを読み取ることができます。

有効化後、デバイスはFeliCaカードを読み取ることができます。

アクセス制御 →→ パラメーター設定 →→ カード設定をクリックして設定画面に入ります。**FeliCa カードを読み取るを有効にします**。

「保存」をクリックします。有効化後、デバイスはFeliCaカードを読み取ることができます。

ウェブブラウザ経由でカード認証モードを設定する

カード番号で認証を行う際にデバイスが読み取るカード番号の内容を設定できます。**パラメーター設定 → カード設定**をクリックして設定画面に移動します。

カード認証モードを選択し、**保存**をクリックします。

全カード番号

すべてのカード番号が読み込まれます。

3 バイト

デバイスは3バイトのみ読み取ります。

4 バイト

デバイスは4バイトのみを読み取りました。

7.8.6 リンク設定

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

手順

1. アクセス制御をクリックし、**→ パラメーター設定、→ リンク設定**を選択して設定画面に移動します。

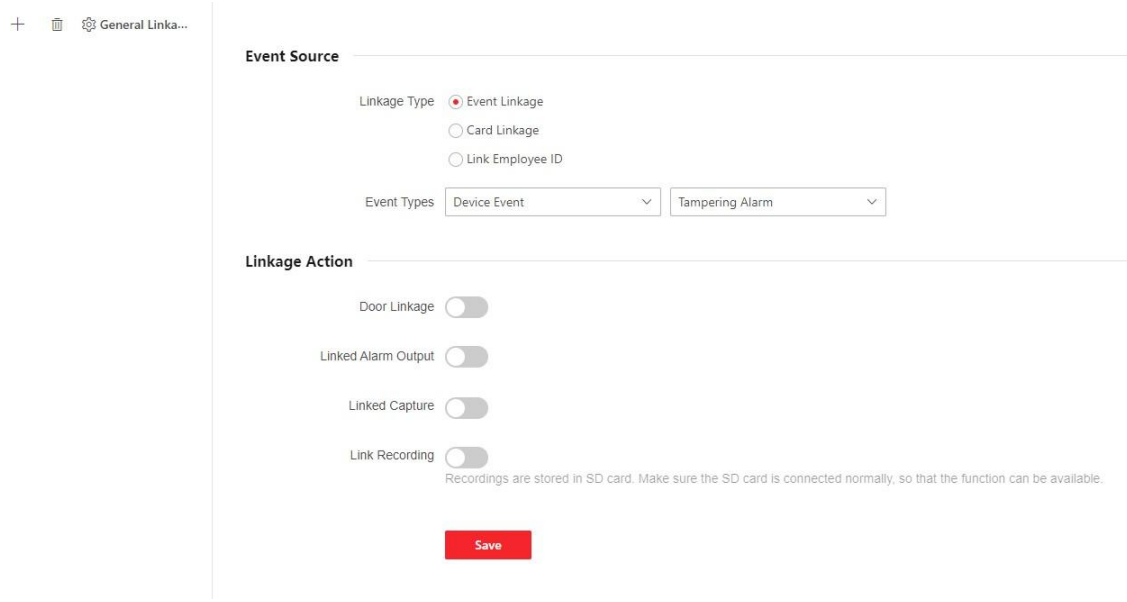


図7-5 リンク設定

2. **+**「 」をクリックします。

3. イベントソースを設定します。リンクタイプを「**イベントリンク**」「**カードリンク**」または「**従業員IDリンク**」から選択します。

- **リンクタイプを**「**イベントリンク**」に選択すると、実際のニーズに応じてイベントタイプを選択できます。
- **リンクタイプを**「**Card Linkage**」に選択した場合、**カード番号**を入力し、**カードリーダー**を選択します。
- **リンクタイプを**「**従業員IDリンク**」に選択し、**従業員ID**を入力し、**カードリーダー**を選択します。

4. リンク動作を設定します。

1) **ドアリンクを**有効にし、ドアアクションを選択します。
2) **リンクアラーム出力を**有効にし、アラーム出力アクションを選択します。
3) **リンクキャプチャを**有効にします。
4) **リンク記録を**有効にし、**一般リンク設定**をクリックして事前記録時間と記録遅延を設定し、動画記録時に音声記録を有効にします。**保存**をクリックします。

注意

録画機能を使用するには、SDカードを用意する必要があります。録画後、クリックできます。

イベント検索で録画を確認できます。詳細については、***イベント検索***をご覧ください。

5. **「保存」をクリックして**設定を有効にします。

7.8.7 PC ウェブ経由で作業モードを設定

デバイスの端末パラメーターを設定できます。

注意

この機能は一部のモデルのみ対応しています。詳細な情報は、該当するデバイスをご確認ください。

アクセス制御をクリックし、**→ パラメーター設定、→ 端末パラメーター**を選択して設定画面に移動します。

動作モード

動作モードをアクセス制御モードまたは許可フリーモードに設定できます。

アクセス制御モード

アクセス制御モードはデバイスの通常モードです。アクセスするには、資格情報を認証する必要があります。

7.8.8 リモート認証の設定

デバイスは、ユーザーの認証情報をプラットフォームに送信します。プラットフォームは、ドアを開けるかどうかを判断します。

アクセス制御に移動**→ パラメーター設定→ ターミナルパラメーター**。パラメーターを設定後、**保存をクリックします**。

リモート検証

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

7.8.9 プライバシー設定

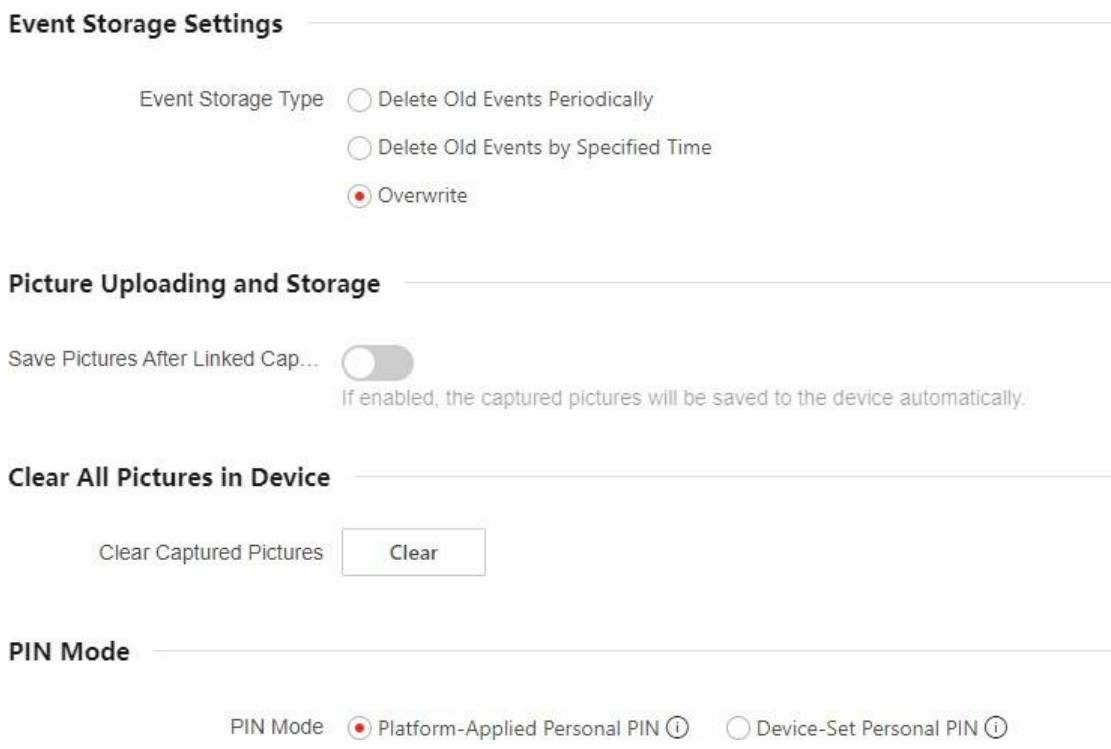


図7-6 プライバシー設定

PCのウェブブラウザからイベントの保存タイプを設定する

イベントの保存タイプを設定できます。

アクセス制御をクリックし、→**パラメーター設定**、→**プライバシー設定**を選択して設定画面に移動します。

イベントの保存タイプとして「**古いイベントを定期的に削除**」「**指定した時間に古いイベントを削除**」または「**上書き**」を選択できます。

古いイベントを定期的に削除

ブロックをドラッグするか、数値を入力してイベント削除の期間を設定します。設定された時間経過後にすべてのイベントが削除されます。

指定した時間で古いイベントを削除

指定した時間にすべてのイベントが削除されます。

上書き

システムが保存されたイベントが総容量の95%を超えたことを検出すると、最も古い5%のイベントが削除されます。

保存をクリックしてください。

画像のアップロードと保存パラメーターを設定

画像のアップロードと保存パラメーターを設定します。

アクセス制御をクリック→**パラメーター設定→プライバシー設定**。機能を有効にします。

リンクキャプチャ後に画像を保存

この機能を有効にすると、キャプチャされた画像は自動的にデバイスに保存されます。

保存をクリックしてください。

PCのウェブブラウザからデバイス内のすべての画像を削除する

デバイス内のすべての撮影した画像を削除できます。

アクセス制御をクリックします**。→パラメーター設定をクリックします**。**→プライバシー設定をクリック**します。**クリア**をクリックします。すべての保存された画像が削除されます。

PC ウェブ経由で PIN モードを設定する

設定前に、PINがプラットフォーム適用型個人PINかデバイス設定型個人PINかを確認してください。デバイス設定型個人PINの場合、デバイスまたはPCウェブでPINを編集できますが、プラットフォームで設定できません。プラットフォーム適用型個人PINの場合、プラットフォームでPINを設定し、デバイスまたはPCウェブでは設定できません。

アクセス制御→ パラメーター設定→プライバシー設定に移動します。

PINモード モジュールでは、以下のパラメーターを設定できます。パラメーター設定後、**[保存]** をクリックしてください。

プラットフォーム適用個人PIN

プラットフォーム上で個人用PINを作成できます。PINはデバイスに適用する必要があります。デバイスまたはPC Web上でPINを作成または編集することはできません。

デバイス設定の個人用PIN

デバイスまたはPC WebでPINを作成または編集できます。プラットフォームでPINを設定することはできません。

保存をクリックしてください。

7.9 ビデオインターコム設定

7.9.1 デバイス管理

デバイス番号、タイプ、IPアドレス、シリアル番号、モデル、バージョン、階数、部屋番号、番号、武装状態、ユーザー名、ネットワーク状態、および操作を確認できます。デバイス管理ページでは、室内ステーションとサブドアステーションを追加し、デバイスを管理、アップグレード、または削除することもできます。

手順

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

デバイスを削除　削除するデバイスを選択し、**削除**をクリックします。

デバイスをインポート　**「インポート」**をクリックし、テンプレートをダウンロードします。情報を入力後、「」をクリックしてデバイスをインポートします。

デバイスをエクスポート　**「エクスポート」**をクリックし、デバイス情報ファイルをローカルPCにエクスポートします。

7.9.2 Web経由でデバイス番号を設定

このデバイスはドアステーションまたは外ドアステーションとして使用できます。使用前にデバイス番号を設定する必要があります。

「アクセス制御」→「→」→「Call Settings」→「→」→「Device No.」をクリックします。

図7-7 デバイス番号設定

デバイスタイプを「**ドアステーション**」に設定した場合、**フロア番号**、**ドアステーション番号**、**コミュニティ番号**、**建物番号**、および**ユニット番号**を設定できます。

デバイスタイプ

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

注意
デバイスタイプを変更した場合、デバイスを再起動する必要があります。

階番号

デバイスが設置されている階番号を設定してください。

ドアステーション番号

デバイスが設置されている階番号を設定してください。

注意

- 番号を変更した場合は、デバイスを再起動する必要があります。
- メインドアステーションの番号は0で、サブドアステーションの番号は1から16までです。

コミュニティ番号

デバイスのコミュニティ番号を設定してください。

建物番号

デバイスのビル番号を設定してください。

ユニット番号

デバイスのユニット番号を設定します。

注
番号を変更した場合、デバイスを再起動する必要があります。設定を保

存するには、設定後**「保存」**をクリックしてください。

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

外ドアステーション番号

外ドアステーションをデバイスタイプとして選択した場合、1から

99の数字を入力する必要があります。

注意
番号を変更した場合、デバイスを再起動する必要があります。

コミュニティ番号

デバイスのコミュニティ番号を設定します。

7.9.3 ウェブブラウザ経由でビデオインターコムのネットワークパラメーターを設定します。

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

「**Call Settings**」をクリックし、→ **Video Intercom** Networkを選択して設定画面に入ります。

登録パスワード

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

メインステーションIP

通信に使用するメインステーションのIPアドレスを入力してください。

プライベートサーバーIP

SIPサーバーのIPアドレスを指します。通信に使用するメインステーションのIPアドレスを入力してください。この時点では、メインステーションがSIPサーバーとして使用されます。他のインターコムデバイスはこのサーバーアドレスに登録する必要があります。

プロトコル 1.0 を有効にする

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

図7-8 ビデオインターコムネットワーク

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

保存をクリックします。

7.9.4 コール設定

最大通信時間を設定します。

アクセス制御に移動し、→ **コール設定**、→ **コール設定を選択します**。

図7-9 コール設定

最大通信時間

メインステーションと他のデバイスが通話中の際の最大通信時間です。通信時間が設定された時間を超えると、通信が停止します。最大通信時間の範囲は90秒から120秒です。

7.9.5 PC ウェブ経由で呼び出すためのボタンを設定

通話用のボタンリンクデバイスを設定します。

手順

1. **アクセス制御**をクリック→**通話設定**→**ボタンを押して通話を選択します**。

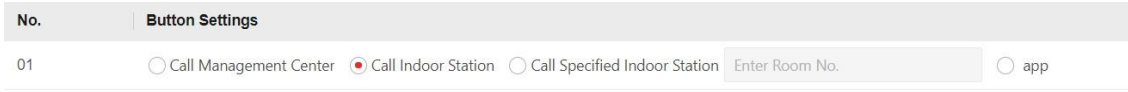


図7-10 ボタンを押して呼び出し

2. ボタンを「**コール管理センター**」「**室内呼び出し端末**」「**指定の室内呼び出し端末**」または「アプリ」に設定してください。

注意

- 「指定室内ステーションへの通話」を選択した場合、リンクされた部屋の番号を設定する必要があります。
- アプリを選択した場合、HCまたはHCCに呼び出すことができます。

3. **保存**をクリックします。

7.9.6 PCウェブ経由での番号設定

部屋のSIP番号を設定します。部屋はSIP番号経由で相互に通信できます。

手順

1. **アクセス制御**に移動し、→**コール設定**→**番号設定を選択します**。

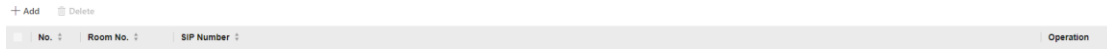


図7-11 番号設定

2.「**追加**」をクリックし、**部屋番号**と**SIP1**電話番号を入力します。

3. オプション：SIP番号を追加するには「**追加**」をクリック、または番号を削除するには「🗑」をクリックします。

4. 保存をクリックします。

5. オプション：削除をクリックして、部屋番号とそのSIP番号を削除できます。

7.10 システム設定

7.10.1 ローカルパラメーターを設定します。

ライブビューのパラメーターを設定し、記録ファイルの保存パスと撮影した写真の保存パスを設定します。

ライブビューパラメーターの設定

システムとメンテナンスをクリックし、→ Localを選択してローカルページに移動します。ストリームタイプ、再生パフォーマンス、ライブビューの自動開始、画像形式を設定し、**保存**をクリックします。

記録ファイルの保存パスを設定する

「**設定**」をクリックし、→ **Local** を選択してローカルページに移動します。記録ファイルのサイズを選択し、ローカルコンピュータから保存パスを選択し、**保存**をクリックします。

詳細を確認するには、**[開く]** をクリックしてファイルフォルダーを開くこともできます。

キャプチャした写真の保存先を設定する

「**設定**」をクリックし、→ **の「ローカル」**を選択してローカルページに移動します。ローカルコンピュータから保存先を選択し、「**保存**」をクリックします。

「**開く**」をクリックすると、ファイルフォルダーを開いて詳細を確認できます。

7.10.2 PC ウェブ経由でデバイス情報を表示

デバイス名、デバイス番号、言語、モデル、シリアル番号、バージョン、チャンネル数、IO入力、IO出力、ロック、アラーム入力、アラーム出力、デバイス容量など、デバイスの詳細情報を表示します。

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→ 基本情報を選択して設定ページに移動します。

デバイス名、デバイス番号、言語、モデル、シリアル番号、バージョン、チャンネル数、IO入力、IO出力、ロック、アラーム入力、アラーム出力、デバイス容量など、各種情報を確認できます。

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

7.10.3 時間設定

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、および間隔を設定できます。

「システムとメンテナンス」をクリックし、**「→」→「System Configuration」→「→」→「System」→「→」→「System Settings」→「→」→「Time Settings」**を選択します。

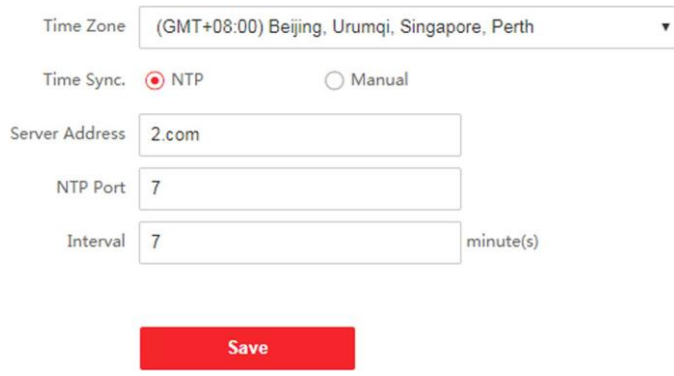


図7-12 時刻設定

設定を保存するには、設定完了後に**「保存」**をクリックしてください。

タイムゾーン

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てください。

タイムシンクロナイズ

NTP

NTPサーバーのIPアドレス、ポート番号、および間隔を設定してください。

手動

デフォルトでは、デバイスの時間は手動で同期されます。デバイスの時間を手動で設定するか、または**「コンピュータの時間と同期」にチェック**を付けて、デバイスの時間をコンピュータの時間と同期させることができます。

サーバー アドレス タイプ/サーバー アドレス/NTP ポート/間隔

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

7.10.4 DSTの設定

手順

1. **システムとメンテナンス**をクリックします。**→システム構成をクリックします。→システムをクリックします。→システム設定をクリックします。→時間設定をクリックします。**
2. **夏時間（DST）**を有効にする。
3. DSTの開始時間、終了時間、およびバイアス時間を設定します。
4. **保存**をクリックして設定を保存します。

7.10.5 管理者のパスワードを変更する

手順

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

注意

デバイスのパスワードの強度は自動的に確認できます。製品のセキュリティを強化するため、ご自身で選択したパスワード（8文字以上で、大文字、小文字、数字、特殊文字の少なくとも3種類を含む）に変更することを強くおすすめします。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すすめします。月次または週次での変更は、製品の保護をさらに強化します。
すべてのパスワードおよびその他のセキュリティ設定の適切な設定は、インストール担当者および/またはエンドユーザーの責任です。

7.10.6 PCウェブ経由のアカウントセキュリティ設定

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

手順

1. **システムとメンテナンス**をクリックし、**→ システム構成→ システム→ ユーザー管理 → ユーザー管理 → アカウントセキュリティ設定を選択します**。
2. 実際の必要に応じて、セキュリティ質問またはメールアドレスを変更します。
3. デバイスパスワードを入力し、**OK**をクリックして変更を確認します。

7.10.7 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を表示します。

システムとメンテナンスに移動し、**→ システム構成→ システム→ ユーザー管理 → オンラインユーザー**を選択して、オンラインユーザーのリストを表示します。

7.10.8 PC ウェブ経由でデバイス武装/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に移動し、**→システム構成→システム→ユーザー管理→武装/解除情報を選択します。**
デバイスの武装/解除情報を表示できます。ページを更新するには**「リフレッシュ」**をクリックしてください。

7.10.9 ネットワーク設定

基本ネットワークパラメーターを設定します。

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

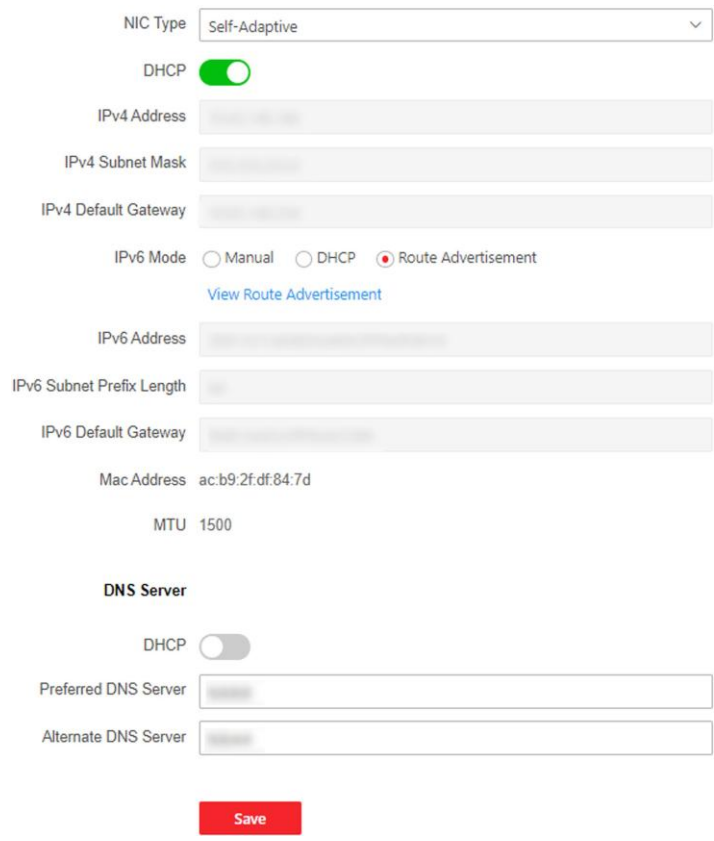


図7-13 TCP/IP 設定ページ

パラメーターを設定し、**[保存]** をクリックして設定を保存します。

NIC タイプ

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

DHCP

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

機能を確認すると、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、IPv6モード、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。

DNSサーバー

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

Wi-Fi パラメーターを設定

デバイスの無線接続用のWi-Fiパラメーターを設定します。

手順

注意

この機能はデバイスでサポートされている必要があります。

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

図7-14 Wi-Fi 設定ページ

2. **Wi-Fi** を確認します。
3. Wi-Fi を選択
   - リストからWi-Fiを選択し、Wi-Fiの🔗をクリックし、Wi-Fiのパスワードを入力します。
   - **「追加」**をクリックし、Wi-Fi の名前、パスワード、および暗号化タイプを入力します。**「接続」**をクリックします。Wi-Fi が接続されたら、**「OK」**をクリックします。

4. オプション: WLAN パラメーターを設定します。

1) IPアドレス、サブネットマスク、およびデフォルトゲートウェイを設定します。または**DHCPを**有効にすると、システムがIPアドレス、サブネットマスク、およびデフォルトゲートウェイを自動的に割り当てます。

5. 保存をクリックします。

デバイス ホットスポット

デバイスのホットスポットを設定します。

システムとメンテナンスをクリックし、**→ →システム構成→→ →Network→ →Network Settings → Device Hotspot** を選択します。

「デバイス ホットスポットを有効にする」をクリックして機能を有効にし、デバイス ホットスポットの名前を表示します。

注意

デフォルトでは、ホットスポット名は「AP_デバイス シリアル番号」です。

「保存」をクリックします。

PCのウェブブラウザでポートを設定します。

システムとメンテナンスをクリックします。**→ システム構成をクリックします。→ ネットワークをクリックします。→ 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ためのポートを指します。例えば、HTTP ポートを 81 に変更した場合、ログインするにはブラウザに ***http://192.0.0.65:81*** と入力する必要があります。

HTTPS

ブラウザからのアクセスにHTTPSを設定します。アクセス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プロトコル経由でイベントアラームIPアドレスまたはドメイン名にアラーム情報を送信できます。イベントアラーム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。

注意

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

システムとメンテナンスをクリックし、**→ システム構成をクリックし、→ ネットワークをクリックし、→ ネットワークサービスをクリックし、→ RTSP** を選択します。

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ISUPパラメーターを設定

ISUPプロトコルを使用してデバイスにアクセスするためのISUPパラメーターを設定します。

手順

注意
この機能はデバイスでサポートされている必要があります。

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

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

PC Web経由でのプラットフォームアクセス

プラットフォームへのアクセスにより、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利用可能です。

手順

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

   注意
   Hik-Connectはモバイルデバイス用のアプリケーションです。このアプリを使用すると、デバイスのライブ映像を確認したり、アラーム通知を受け取ったりできます。
2. **「有効」**にチェックを入れて機能を有効にします。
3. **オプション:「カスタム」**のチェックボックスをオンにすると、サーバーアドレスを自分で設定できます。
4. 検証コードを入力してください。
5. **「表示」**をクリックしてデバイスのQRコードを表示します。QRコードをスキャンしてアカウントを連携します。

   注意
   8文字から32文字（aからz、AからZ）または数字（0から9）、大文字小文字を区別します。8文字以上の文字または数字の組み合わせを使用することをおすすめします。
6. **「保存」**をクリックして設定を有効にします。

Bluetooth設定

Bluetooth機能を有効にできます。

設定をクリックし、**→ ネットワーク、→ ネットワーク設定、→ Bluetoothを選択します**。

開

「Bluetooth」を有効にするには、「有効」**をタップします**。

デバイス名

Bluetoothに接続されているデバイスの名前を編集できます。

接続状態

接続状態を確認できます。

Bluetooth経由でドアを開ける

この機能を有効にすると、HikCentral ConnectまたはHikCentral Access Control経由でドアを開けることができます。

注意

Bluetooth経由でドアを開ける前に、デバイスをHCCまたはHCACに追加する必要があります。HCAC経由では、自動ドア開閉機能も実現できます。詳細については、HCACのユーザーマニュアルをご確認ください。

VoIP アカウント設定

ネットワーク経由で音声通話を実現できます。

手順

1. **システムとメンテナンス**に移動し、**→ システム構成→ ネットワーク→ デバイスアクセス→ VoIP**。
2. **VoIP ゲートウェイを**有効にします。
3. **ユーザー名、登録パスワード、サーバーIPアドレス、サーバーポート、有効期限、登録状態、番号、表示ユーザー名を設定**します。

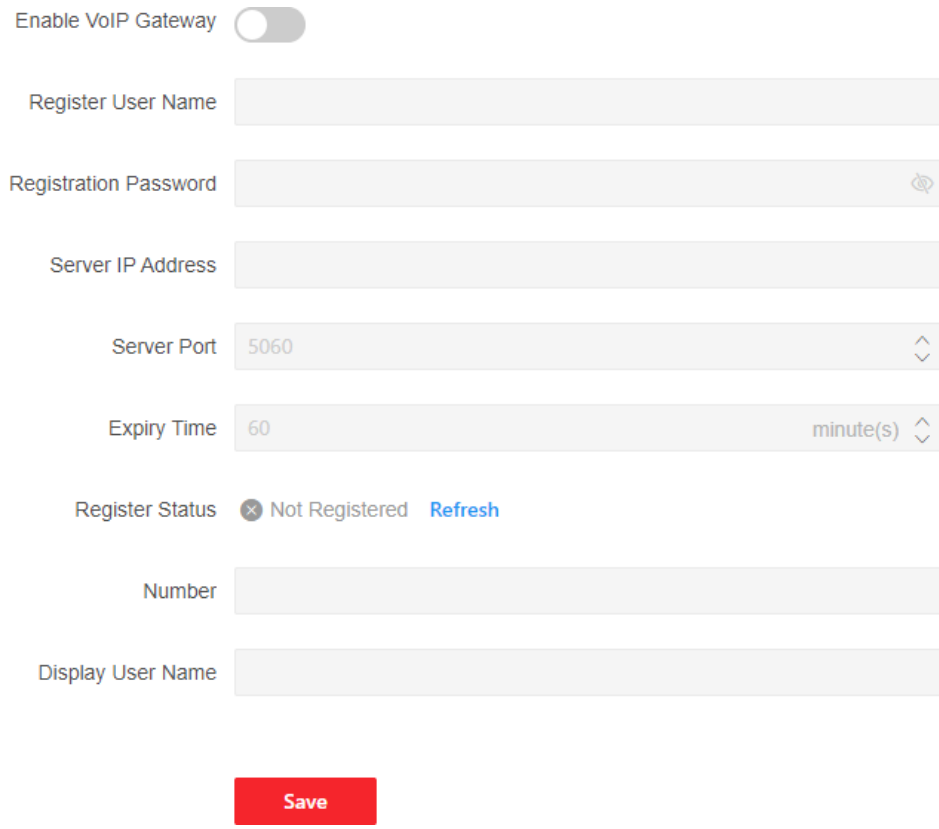


図7-15 VoIP アカウント設定

登録パスワード

SIPサーバー経由の通信用の登録パスワードを入力します。SIPサーバーの登録パスワードは、通常、メインステーションのSIP設定で設定されます。

サーバーIPアドレス

VoIP通信に使用するメインステーションのIPアドレスを入力します。この時点では、メインステーションがSIPサーバーとして機能します。他のインターコムデバイスはこのサーバーアドレスに登録する必要があります。

番号 / ユーザー名表示

デバイスは、通話番号とユーザー名を表示しました。

4. **保存**をクリックします。

7.10.10 PCウェブ経由でビデオとオーディオのパラメーターを設定

ウェブブラウザ経由でビデオパラメーターを設定

デバイスのカメラの画質、解像度、その他のパラメーターを設定できます。

システムとメンテナンスをクリックします。→ **システム構成をクリックします。→ ビデオ/オーディオ→ ビデオ**をクリックして設定画面に移動します。

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

「**保存**」をクリックします。

PCウェブ経由でオーディオ設定を構成

デバイスの音量を設定できます。

システムとメンテナンス→ システム構成→ ビデオ/オーディオ→ オーディオ。

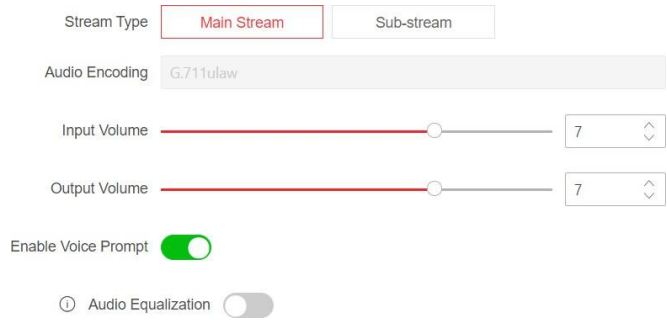


図7-16 オーディオ

実際のニーズに応じてストリームタイプとオーディオエンコードを設定します。スライダーを動かして入力と出力の音量を設定します。

スライダーを動かして**音声ガイドを**有効にします。

オーディオイコライゼーションを有効にすると、デバイスはオーディオアルゴリズムにより周波数を自動調整し、オーディオ品質を向上させ、オーディオ効果を均一化します。

保存をクリックします。

7.10.11 画像パラメーター設定

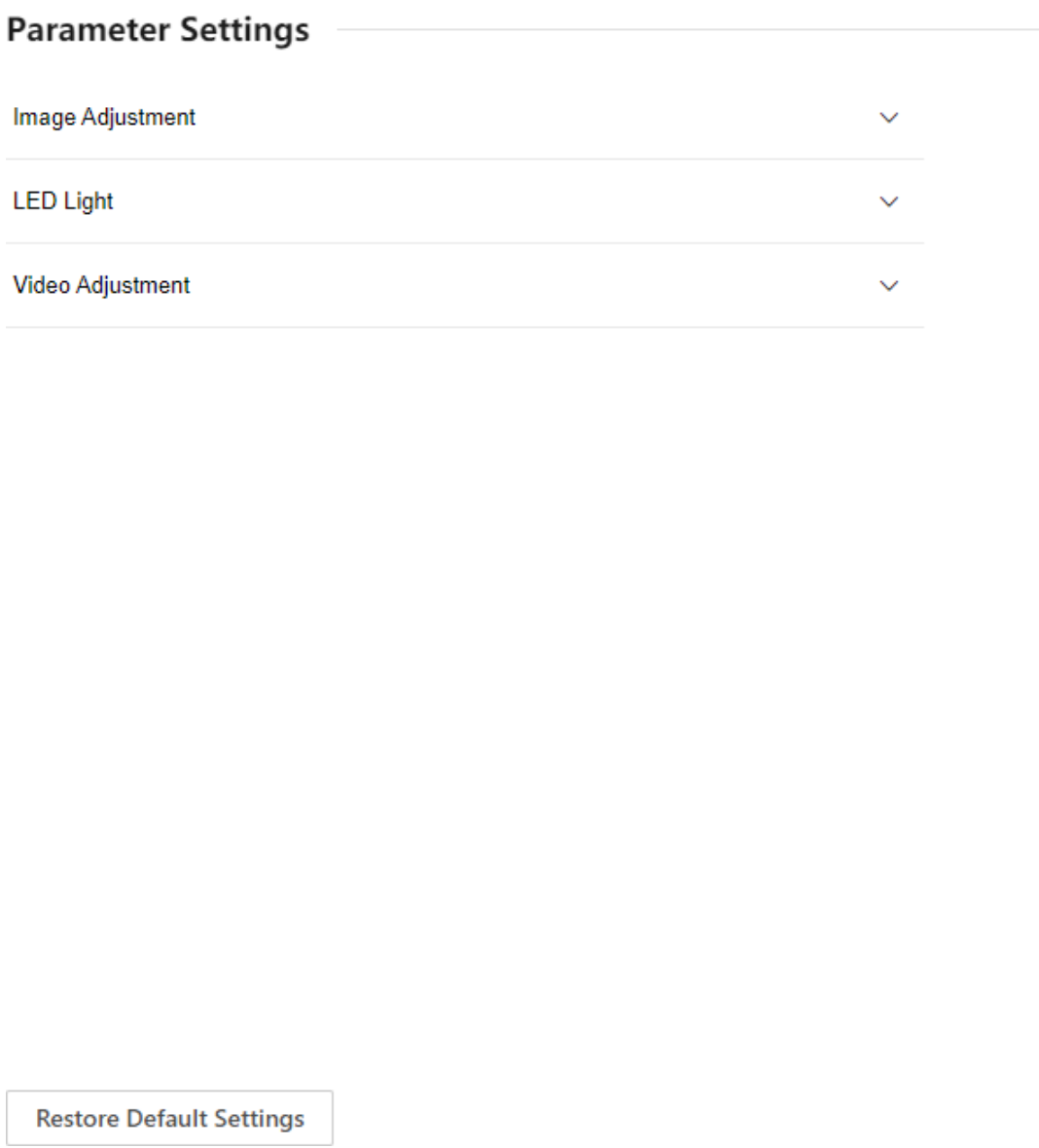


図7-17 ディスプレイ設定

PC ウェブ経由で明るさ/コントラスト/彩度/シャープネスを設定

ライブビュー画面の明るさ、コントラスト、彩度、シャープネスなどの画像設定を変更できます。

システムとメンテナンスをクリックし、**→**、**システム構成**、**→**、**Image**、**→**、**Display Settings**の順にクリックして設定画面に移動します。

画像調整

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

PC Web経由でLEDライトを設定

補助ライトの明るさを調整できます。

手順

1. **システムとメンテナンス**をクリックします**。→ システム構成をクリックします。→ イメージをクリックします。→ ディスプレイ設定**をクリックして設定画面に入ります。
2. 補助照明のタイプ、モード、明るさを設定します。
3. **オプション：デフォルト設定に戻す**をクリックして、デフォルト設定に戻します。

PC ウェブ経由でビデオ標準を設定

ライブビューページのビデオ標準を設定できます。

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

ビデオ調整

リモートプレビュー中に動画のフレームレートを設定します。新しい設定を有効にするには、デバイスを再起動する必要があります。

PAL

25フレーム/秒。中国本土、香港（中国）、中東諸国、ヨーロッパ諸国などに対応しています。

NTSC

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

「**デフォルト設定に戻す**」をクリックして、デフォルト設定に戻します。

7.10.12 PCウェブ経由でイベント検出を設定します。

モーション検出イベントを設定した後、移動物体がトリガーされた場合、デバイスはプラットフォームに報告します。

システムとメンテナンスをクリックし、**→、システム構成、→、イベント、→、Event Detectionを選択します。**
モーションを有効にします。

ページのライブビュー部分でモーション検出領域を設定します。

「  」をクリックし、ライブビューページに領域を描画します。領域内に移動物体が進入すると、アラームがトリガーされます。

 をクリックして領域を削除します。

 をクリックして画面をキャプチャします。

 をクリックして録画を開始します。もう一度クリックすると停止します。録画はローカルPCに保存されます。

 をクリックして、ライブビューをフルスクリーンモードで表示します。

感度

ルールをトリガーする感度を設定します。感度が高いほど、ルールがトリガーされやすくなります。

アラームスケジュール

時間スケジュールを終了します。

「編集」をクリックし、**「武装」**をクリックします。時間スケジュールで武装期間を指定できます。**保存**をクリックします。武装期間中にルールがトリガーされた場合、プラットフォームに報告されます。

監視センターに通知

機能有効化後、ルールがトリガーされた場合、デバイスはプラットフォームに報告します。

HTTP

機能を有効にした後、ルールがトリガーされた場合、デバイスはHTTP経由でプラットフォームに報告します。**保存**をクリックしてください。

7.10.13 PC Web経由でのアラーム設定

アラーム出力パラメーターを設定します。

手順

1. **システムとメンテナンス**をクリックし、→、**システム構成**、→、**イベント**、→、**アラーム設定**、→、**アラーム出力を選択します**。
2. **アラーム名**と**アラーム持続時間**を設定します。

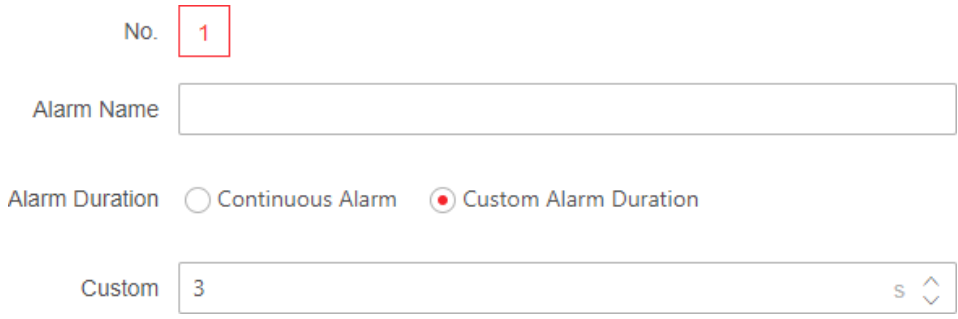


図7-18 アラーム設定

連続アラーム

アラームがトリガーされると、アラームが継続的に鳴動します。

カスタムアラーム持続時間

アラームがトリガーされた際に、デバイスの**アラーム持続時間**を設定できます。

7.10.14 アクセス設定

PCウェブ経由でRS-485パラメーターを設定

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

システムとメンテナンスをクリックし、→**システム設定**→**アクセス設定**→**RS-485を選択します**。ドロップダウンリストからRS-485のプロトコルを選択します。

「RS-485を有効にする」にチェックを入れ、パラメーターを設定します。

設定を保存するには、設定完了後に**「保存」**をクリックしてください。

No.

RS-485番号を設定してください。

周辺機器の種類

実際の状況に応じてドロップダウンリストから周辺機器を選択してください。選択可能なオプションは**カードリーダー**、**拡張モジュール**、**アクセスコントローラー**、または**無効**。

注意

周辺機器を変更して保存すると、デバイスが自動的に再起動します。

RS-485 アドレス

実際の要件に応じてRS-485アドレスを設定してください。

注意

アクセスコントローラーを選択した場合：RS-485インターフェース経由でデバイスをターミナルに接続する場合、RS-485アドレスを2に設定してください。デバイスをコントローラーに接続する場合、ドア番号に応じてRS-485アドレスを設定してください。

ボーレート

RS-485プロトコルでデバイスが通信する際のボーレートです。

PC Web経由でWiegandパラメーターを設定

Wiegandの送信方向を設定できます。

手順

注意

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

1. **システムとメンテナンス**をクリックします。→**システム構成をクリックします。→アクセス構成をクリックします。→Wiegand 設定をクリックします**。

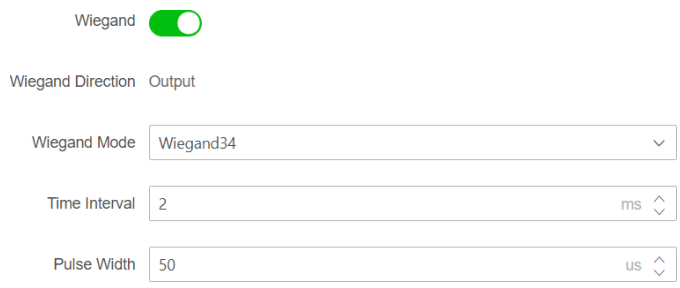


図7-19 Wiegand ページ

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

出力

外部アクセスコントローラーを接続できます。2つのデバイスは、Wiegand 26または34経由でカード番号を送信します。

4. 設定を保存するには**「保存」**をクリックします。

注意
周辺機器を変更し、デバイスパラメーターを保存した後、デバイスは自動的に再起動します。

PCウェブ経由のエレベーター制御

手順

1. **システムとメンテナンス**をクリックします。**→システム構成をクリックします。→アクセス構成をクリックします。→エレベーター制御パラメーターをクリック**します。

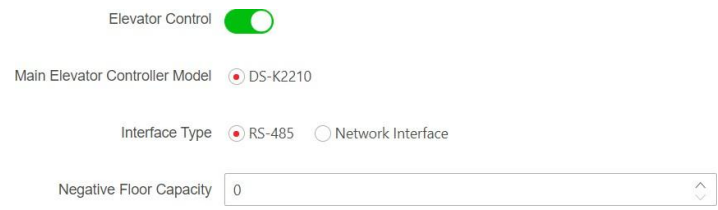


図7-20 エレベーター制御

2. **エレベーター制御を**有効にします。

3. エレベーターのパラメーターを設定します。

メインエレベーターコントローラーモデル

エレベーターモデルを表示します。

インターフェースタイプ

エレベーター通信用の通信タイプをドロップダウンリストから選択してください。

RS-485を選択した場合、デバイスを**RS-485**ケーブルでエレベーターコントローラーに接続していることを確認してください。

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

負の階数容量

負の階数を設定します。

注

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

7.11 システムとメンテナンス

7.11.1 再起動

デバイスを再起動できます。

システムとメンテナンスをクリックします。→ **Maintenanceをクリックします。→ をクリックし**、再起動して設定画面に移動します。**再起動**をクリックしてデバイスを再起動します。

7.11.2 アップグレード

PC ウェブ経由でローカルにアップグレード

デバイスをローカルでアップグレードできます。

システムとメンテナンスをクリックし、→ **Maintenance→ Upgrade** を選択して設定画面に移動します。
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。

PCウェブ経由でのオンラインアップグレード

デバイスをオンラインでアップグレードできます。

システムとメンテナンスをクリックし、→ **Maintenance→ Upgrade** をクリックして設定画面に移動します。更新を確認**をクリックして**、更新されたバージョンがあるかどうかを確認します。
デバイスがネットワークに接続されており、Hik-Connect アプリに追加されている場合、Hik-Connect アプリに更新バージョンがある場合に、デバイス上で「**デバイス アップグレード**」→「→ **オンライン アップグレード**」をタップしてアップグレードできます。

7.11.3 復元

ウェブブラウザ経由で工場設定に復元

デバイスを工場出荷時設定に復元できます。

システムとメンテナンス→ Maintenance→ Backup and Reset をクリックして設定画面に入ります。
「**すべてを復元**」をクリックすると、すべての設定が工場出荷時の設定に戻ります。使用前にデバイスをアクティベートしてください。

PC ウェブ経由でデフォルト設定に復元

デバイスをデフォルト設定に復元できます。

「システムとメンテナンス」をクリックし、**「→ メンテナンス」を選択し、「→ バックアップとリセット」**をクリックして設定画面に移動します。

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

7.11.4 PCウェブ経由でデバイスパラメーターをエクスポート

デバイスのパラメーターをエクスポートします。

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

バックアップ

「エクスポート」をクリックしてデバイス設定をエクスポートします。

注意

デバイスのパラメーターをエクスポートし、他のデバイスにインポートします。

7.11.5 PC Web経由でデバイスパラメーターをインポート

構成パラメーターをインポートします。

システムとメンテナンスに移動し、**→ メンテナンス、→ バックアップとリセットを選択します**。

設定ファイルのインポート

「 」をクリックし、ローカルPCからファイルを選択します。**「インポート」**をクリックします。

7.11.6 デバイス デバッグ

デバイスのデバッグ設定を指定できます。

Web ブラウザ経由で SSH を有効/無効にします

SSHを有効にしてリモートデバッグを実行できます。

システムとメンテナンスをクリックし、**→ Maintenance、→ Device Debugging、→ Log for Debugging** の順に選択し、**SSH を有効にします**。

SSHはリモートデバッグに使用されます。このサービスを使用しない場合は、セキュリティを向上させるため、SSHを無効にすることをおすすめします。

PCのウェブブラウザでプロトコルをテスト

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。応答ヘッダーと返された値に基づいてデバイスをデバッグできます。

システムとメンテナンスに移動し、**→メンテナンス、→デバイス デバッグ、→プロトコル テストを選択します**。

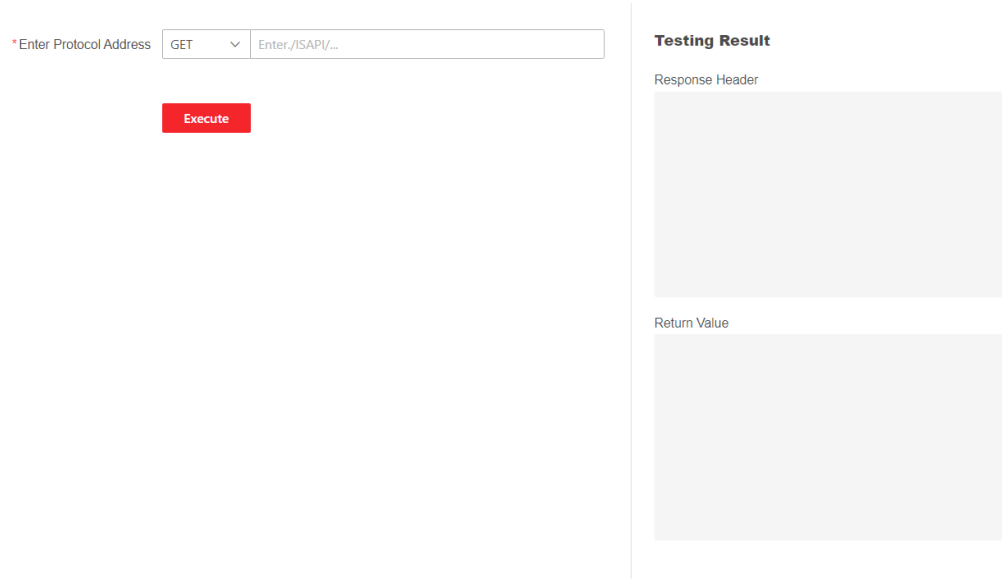


図7-21プロトコルテスト

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。
応答ヘッダーと返された値に基づいてデバイスをデバッグします。

7.11.7 PC ウェブ経由でログを表示

デバイスログを検索して表示できます。

システムとメンテナンスに移動し、**→メンテナンス、→ログを選択します**。
ログタイプの主要タイプと副次タイプを設定します。検索の開始時間と終了時間を設定し、**[検索]**をクリックします。
結果は以下に表示され、番号、時間、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。

7.11.8 セキュリティモード設定

クライアントソフトウェアのログ記録用のセキュリティモードを設定します。

「管理対象デバイス」ページで、**「メンテナンスとセキュリティ」→「→セキュリティ」→「→セキュリティサービス」**をクリックします。

セキュリティモードを選択し、[**保存**] をクリックします。

セキュリティモード

クライアントソフトウェアにログインする際のユーザー情報検証に高いセキュリティレベルを適用します。

互換モード

ログイン時にユーザー情報の検証が古いクライアントソフトウェアバージョンと互換性があります。

7.11.9 証明書管理

サーバー/クライアント証明書およびCA証明書を管理するのに役立ちます。

注意

この機能は、特定のデバイスモデルでのみサポートされています。

自己署名証明書を作成してインポートする

手順

1. **システムとメンテナンス**に移動し、**→ を選択し、→ を選択し、証明書管理を選択します**。
2. **証明書**ファイル領域で、ドロップダウンリストから**証明書タイプ**を選択します。
3. **「作成」**をクリックします。
4. 証明書情報を入力します。
5. **OK**をクリックして証明書を保存し、インストールします。
   作成した証明書が**証明書詳細**領域に表示されます。証明書は自動的に保存されます。
6. 証明書をダウンロードし、ローカルコンピュータの指定したファイルに保存します。
7. 要求ファイルを認証局に送信して署名を取得します。
8. 署名付き証明書をインポートします。
   1) 「**キーのインポート**」領域で証明書タイプを選択し、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) 「**通信証明書をインポート**」領域で証明書タイプを選択し、ローカルから証明書を選択し、[**インポート**] をクリックします。

その他の承認済み証明書をインポート

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

手順

1. **システムとメンテナンス**に移動し、**→、Safe、→、Certificate Management** の順に選択します。
2. **「インポートキー」**と**「インポート通信証明書」**の領域で、証明書タイプを選択し、証明書をアップロードします。

3. **インポート**をクリックします。

CA証明書をインポート

開始前に

事前にCA証明書を準備してください。

手順

1. **システムとメンテナンス**に移動します**。→安全→証明書管理**。

2. 「**CA証明書をインポート**」領域でIDを作成します。

注意

入力する証明書 ID は既存のものと同一にしてはいけません。

3. ローカルから証明書ファイルをアップロードします。

4. **インポート**をクリックします。

第8章 モバイルブラウザを使用してデバイスを設定する

TCP/IP を使用してネットワークを設定

デバイスが有線ネットワークに接続されている場合、Webブラウザを使用してデバイスのIPアドレスを設定し、デバイスのホットスポットを有効にします。詳細については、PCのWebブラウザの設定を参照してください。

スマートフォンのWi-Fi機能を有効にし、デバイスのホットスポットを検索します。
スマートフォンのブラウザを開き、デバイスのIPアドレスを入力してモバイルブラウザの設定画面にアクセスします。

Wi-Fi経由でネットワークを設定する

デバイスがWi-Fiに接続されている場合、デバイスのIPアドレスを設定し、Webブラウザ経由でデバイスのホットスポットを有効にします。詳細については、PCのWebブラウザの設定をご確認ください。

スマートフォンのWi-Fi機能を有効にし、デバイスのホットスポットを検索してください。

注意

デバイスとスマートフォンは同じWi-Fi環境に接続されている必要があります。そうでない場合、スマートフォンのブラウザからデバイスにアクセスできません。

スマートフォンのブラウザを開き、デバイスのIPアドレスを入力してモバイルブラウザの設定ページにアクセスします。

8.1 ログイン

モバイルブラウザからログインできます。

注

- モデルの特定の部品はWi-Fi設定に対応しています。
- デバイスが起動していることを確認してください。
- デバイスとスマートフォンが同じWi-Fi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。

モバイルブラウザのアドレスバーにデバイスのIPアドレスを入力し、**Enterキー**を押してログイン画面を表示します。
デバイスのユーザー名とパスワードを入力し、**ログイン**をタップしてください。

8.2 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、セキュリティ質問を使用してパスワードを変更できます。

手順

1. ログイン画面で「**パスワードを忘れた場合**」をタップします。
2. 「認証モード」を選択します。

   セキュリティ質問の確認

   デバイスまたはモバイルウェブでセキュリティ質問を設定している場合、その回答を入力してパスワードをリセットできます。**「セキュリティ質問の確認」を**タップし、**「次へ」を**タップします。
3. セキュリティ質問の回答を入力し、**「次へ」を**タップします。
4. 新しいパスワードを入力し、確認します。
5. **「次へ」**をタップします。

8.3 アカウントのセキュリティ設定

予約済みの電話番号を変更し、パスワードを忘れた場合は、その電話番号を使用してログインパスワードを変更できます。

手順

注意

デバイスと電話が同じLAN内にあり、設定画面が表示される必要があります。

1. 「 」をタップします。**「→ 」**をタップします**。「User Management」をタップします。「 → 」 をタップします。「 … 」をタップします。「→」**をタップします。
2. 予約済みの電話番号を変更します。ログインパスワードを忘れた場合、電話番号を入力してパスワードを変更できます。
3. **保存**をタップします。

8.4 ホーム

ドアの状態を確認できます。ショートカット入力で設定ページにアクセスできます。ネットワークの状態を確認できます。基本情報を表示できます。

ドアの状態

ドアの状態を確認できます。また、ドアの状態を制御できます。

ショートカット入力

設定機能名を選択し、ページに移動します。

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

デバイスモデル、シリアル番号、バージョンを確認したり、基本情報ページに入力できます。

8.5 設定

8.5.1 デバイス情報を表示

デバイス名、言語、モデル、シリアル番号、バージョン、IO入力番号、ローカルRS-485番号、アラーム出力数、レジスタ番号、MACアドレス、デバイス容量など、各種情報を表示します。

「 」をタップし、→、**System Settings**、→、**Basic** Informationの順にタップして設定画面に入ります。

デバイス名、言語、モデル、シリアル番号、バージョン、IO入力番号、ローカルRS-485番号、アラーム出力数、レジスタ番号、MACアドレス、およびデバイス容量などを表示できます。

8.5.2 時間設定

タイムゾーン、時間同期モード、表示時間を設定します。

「 」をタップし、→**システム設定**→**時間設定**を選択して設定画面に入ります。

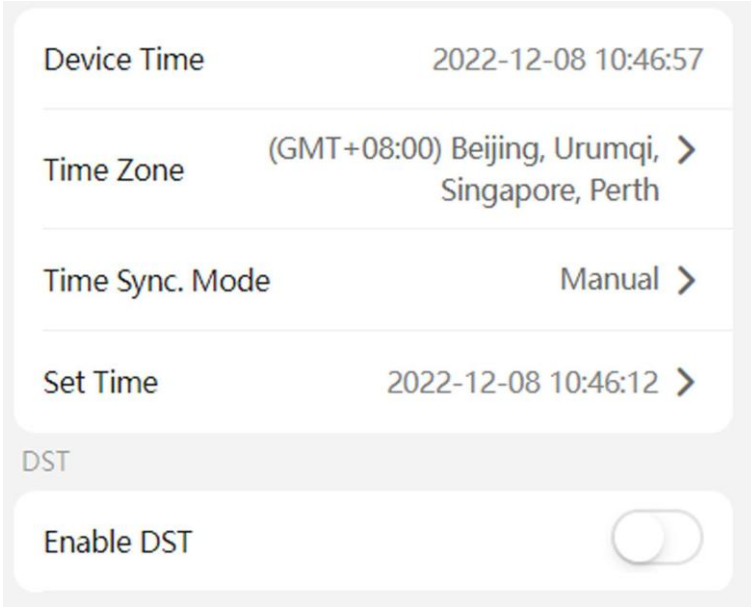


図8-1 タイム設定

「保存」をタップして設定を保存します。

タイムゾーン

デバイスの所在地に対応するタイムゾーンをドロップダウンリストから選択します。

時間同期モード手動

デフォルトでは、デバイスの時間は手動で同期されます。デバイスの時間を手動で設定できます。

NTP

NTPサーバーのIPアドレス、ポート番号、および間隔を設定します。

8.5.3 夏時間設定

手順

1. 「 」をタップします。「→」→「**System Settings**」→「→」→「**Time Settings**」をタップして、設定画面に移動します。

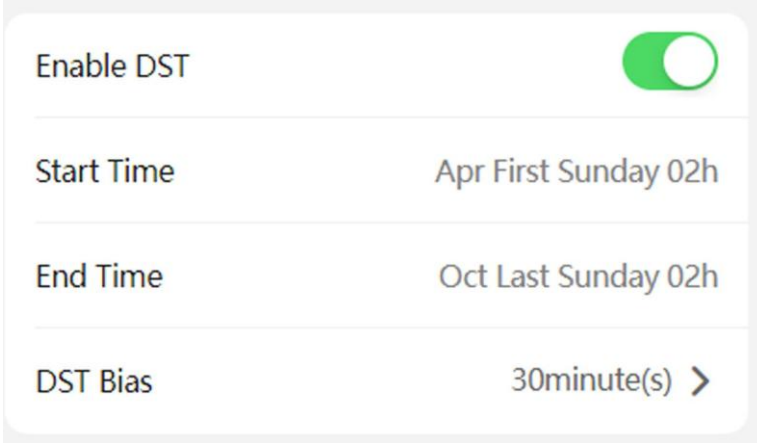


図8-2 DST

2. 「**DSTを有効にする**」をタップします。

3. 開始時間、終了時間、およびDSTのオフセットを設定します。

4. 「**保存**」をタップします。

8.5.4 ユーザー管理

手順

1. 「 」をタップします。→ **User Management**→ **User Management**→ **admin** にアクセスして設定画面を開きます。

2. 古いパスワードを入力し、新しいパスワードを作成します。

3. 新しいパスワードを確認します。

4. 「**保存**」をタップします。

注意

デバイスのパスワードの強度は自動的にチェックされます。製品のセキュリティを強化するため、ご自身で選択したパスワード（8～16文字で、大文字、小文字、数字、特殊文字の少なくとも2種類を含む）に変更することを強くおすすめします。また、パスワードの変更を定期的に行うことをおすすめします。

定期的に、特に高セキュリティシステムでは、パスワードを毎月または毎週変更することで、製品をより安全に保護できます。

8.5.5 ネットワーク

ネットワーク設定パラメーター、Wi-Fi パラメーター、およびアクセスポイントパラメーターを設定可能です。

有線ネットワーク

有線ネットワークを設定します。

「 」をタップします。→ **通信設定→ Wired Network** をタップして設定画面に移動します。

DHCP

この機能を無効にした場合、IPv4アドレス、IPv4サブネットマスク、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、MACアドレス、およびMTUを設定する必要があります。

この機能を有効にすると、システムは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、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。

DNSサーバー

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

Wi-Fi設定

デバイスのWi-Fiパラメーターを設定します。

開始前に

デバイスがアプリに追加された後、デバイスのWi-Fi機能を有効にできます。その後、モバイルウェブでWi-Fiパラメーターを設定できます。

手順

1. ホーム画面で、[ ]をタップします。→ **通信設定→ Wi-Fi**。
2. **Wi-Fi** を有効にします。
3. リストからWi-Fiを選択し、パスワードを入力して接続します。
4. **オプション:** Wi-Fi を追加します。
   1) ページを最後までスクロールし、「**ネットワークを追加**」をタップします。
   2) **Wi-Fi 名**を入力し、Wi-Fi の**暗号化タイプ**を選択します。
   3) 「**OK**」をタップします。
5. **オプション：** WLANを設定します。
   1) 接続しているWi-Fiの名前を設定し、ネットワークの詳細を確認します。
   2) 「**WLAN設定**」をタップします。
   3) WLANのパラメーターを設定します。

DHCPを有効にします。

DHCPを有効にし、**DNSを自動設定**に設定すると、デバイスがIPアドレスとDNSを自動的に割り当てます。

DHCPを無効にします

IPアドレスとDNSサーバーを手動で設定します。

4) **保存**をタッ

プします。**結果**

Wi-FiとWLANの設定後、モバイルブラウザにWLANのIPアドレスを入力してデバイスにログインできます。

デバイス ホットスポットを設定

デバイスのホットスポットを設定し、スマートフォンをデバイスに接続してモバイルブラウザにアクセスできます。

手順

1. 「 」をタップします。「**→ Communication Settings**」をタップします。「**→ Device Hotspot**」をタップします。

2. デバイスのホットスポットを有効にし、ホットスポットの名前を確認できます。

注意

デフォルトでは、ホットスポット名は「AP_Device シリアル番号」です。

3. 「**保存**」をタップします。

ポートパラメーターの設定

ネットワーク経由でデバイスにアクセスする際、実際の要件に応じてHTTPとHTTPSを設定できます。「 」→「**Network Service**」→「**HTTP(S)**」をタップして、設定画面に移動します。

HTTP

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

HTTPS

ブラウザへのアクセスに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。

プラットフォームアクセス

プラットフォームアクセスは、プラットフォーム経由でデバイスを管理するオプションを提供します。

手順

1. 「 」をタップします。**「→ デバイスアクセス」をタップします。「→ Hik-Connect**」をタップして設定画面に移動します。

注意

Hik-Connectはモバイルデバイス用のアプリケーションです。このアプリを使用すると、デバイスのライブ画像を表示したり、アラーム通知を受け取ったりできます。

2. **「有効」**をタップして機能を有効にします。
3. **「カスタム」**を有効にすると、サーバーアドレスを入力できます。

注意

- 6文字から12文字（aからz、AからZ）または数字（0から9）、大文字と小文字を区別します。8文字以上の文字または数字の組み合わせを使用することをおすすめします。
- 検証コードは「***123456 /*** または「***abcdef***」（大文字小文字を区別しない）に設定できません。

4. **登録状態**と**バインド状態**を確認できます。
5. **「アカウントをバインド」**をタップし、**→ の「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バインドできます。
6. **「保存」**をタップして設定を有効にします。

ISUPパラメーターを設定してください。

ISUPプロトコルを使用してデバイスにアクセスするためのISUPパラメーターを設定します。

手順

注

この機能はデバイスでサポートされている必要があります。

1. 「 」をタップします。**「→ 」→「Device Access」→「→ 」→「ISUP」**を選択して設定画面に移動します。
2. **ISUPを**有効にします。
3. ISUPバージョン、サーバーアドレス、ポート、デバイスID、および暗号化キーを設定します。

注意

バージョンに5.0を選択した場合、暗号化キーも設定する必要があります。

4. 設定を保存するには**「保存」**をタップしてください。

VoIP 設定

「 」をタップします。**「→デバイス アクセス」をタップし、→VoIP** をタップして設定画面に移動します。**「VoIP ゲートウェイ」**をタップして**有効にします**。

VoIP パラメーターを設定し、**保存**をタップしてパラメーターを保存します。

8.5.6 ユーザー管理

モバイルウェブブラウザ経由でユーザーを追加、編集、削除、検索できます。

手順

1. → **Person Management** をタップして設定画面に入ります。

2. ユーザーを追加します。

1) **+** をタップします。

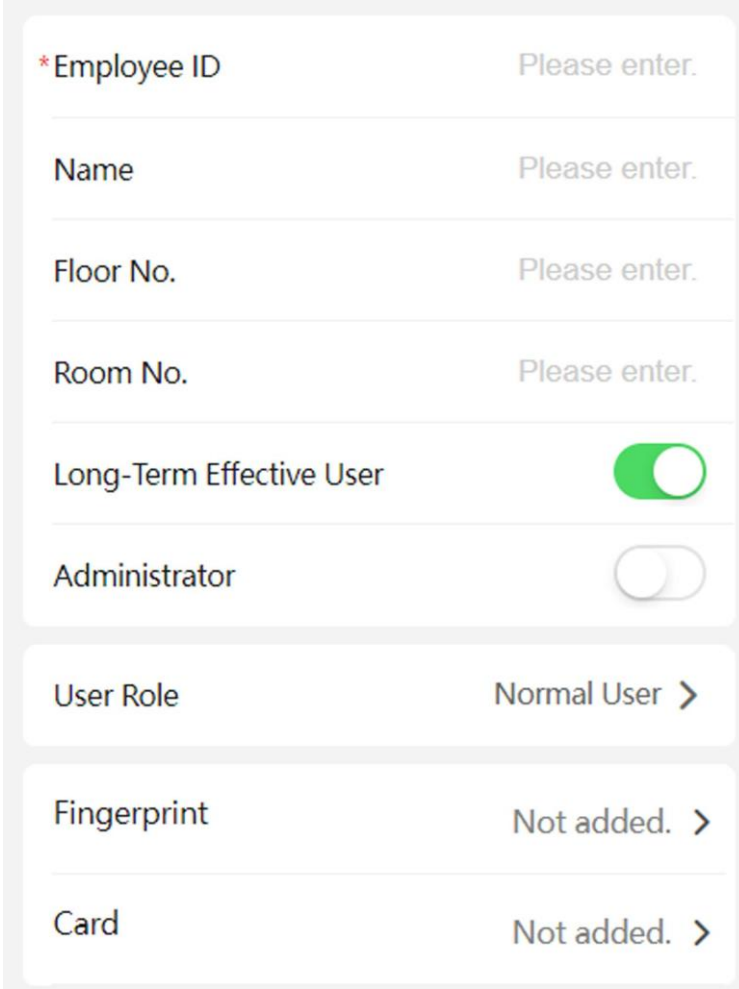


図8-3 ユーザーを追加

2) 以下のパラメーターを設定します。

従業員ID

従業員IDを入力してください。従業員IDは0または32文字を超えることはできません。大文字、小文字のアルファベットと数字の組み合わせで構成できます。

名前

名前を入力してください。名前には数字、大文字と小文字の英字、および文字が含まれます。名前は32文字以内が推奨されます。

階数/部屋番号

フロア番号/部屋番号を入力してください。

長期有効

ユーザー権限を長期有効に設定してください。

開始日/終了日

ユーザー権限の**開始**日と**終了日を**設定してください。

管理者

ユーザーを管理者として設定する必要がある場合、**管理者権限を**有効にできます。

ユーザーロール

ユーザー役割を選択してください。

指紋

指紋を追加します。**「指紋」**をタップし、次に「**+**」をタップし、指紋モジュール経由で指紋を追加します。

カード

カードを追加します。**カードを追加**をタップします。**カード番号**を入力するか、デバイスにカードを提示して**読み取りをタップし**、**プロパティ**を選択します。**保存**をタップしてカードを追加します。

パスワード

- パスワードを設定する前に、パスワードがデバイスで設定された個人用PINか、プラットフォームで適用された個人用PINかを確認する必要があります。デバイスで設定された個人用PINの場合、Web上で作成および編集が可能ですが、プラットフォーム上では作成および編集できません。プラットフォームで適用された個人用PINの場合、プラットフォーム上で設定する必要があり、Web上では編集できません。
- **パスワードモードが「デバイスパスワード」**に設定されていることを確認してください。

「Person Management」をタップし、**「→」をタップして**「Add」をタップし、追加ページに移動します。パスワードを入力します。

3)**「保存」**をタップします。

3. ユーザーリストで編集が必要なユーザーをタップして情報を編集します。

4. ユーザーリストから削除したいユーザーをタップし、[ ] をタップしてユーザーを削除します。

5. 検索バーに従業員IDまたは名前を入力してユーザーを検索できます。

8.5.7 イベント検索

「 」をタップし、**次に「→」をタップします。**

検索条件（従業員ID、名前、カード番号、開始時間、終了時間）を入力し、[**検索**] をタップします。

注意

内の名前検索に対応しています。

結果はリストに表示されます。

8.5.8 オーディオ設定

オーディオを有効にしたり、設定を調整したり

できます。 → **Audio** をタップします。

必要に応じて「**音声ガイドを有効にする」をオン**にします。デバイスが音声ガイドを再生します。

オーディオの音量も調整できます。

オーディオイコライゼーションを有効にすると、デバイスはオーディオアルゴリズムにより周波数を自動調整し、オーディオ品質を向上させ、オーディオ効果を均一化します。

「保存」をタップします。

8.5.9 アクセス制御設定 認証パラメー

ターを設定

認証パラメーターを設定します。

手順

1. 「 」をタップします。→ **アクセス制御**→ **認証設定**。

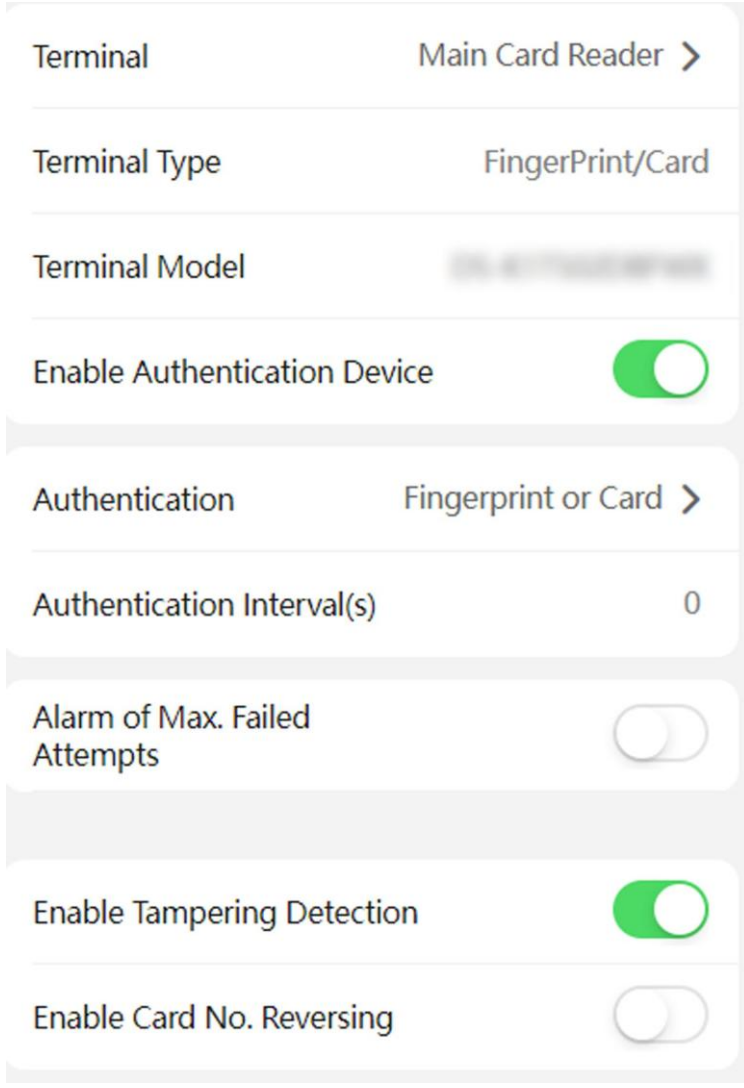


図8-4 認証設定

2. **保存**をタップ。**ターミナル**

メインカードリーダー

デバイスのカードリーダーのパラメーターを設定できます。メインカードリーダーを選択した場合、以下のパラメーターを設定する必要があります：**ターミナルタイプ**、**ターミナルモデル**、**カードリーダーを有効にする**、**認証**、**認識間隔（秒）**、**最小カードスワイプ間隔（秒）**、**最大認証失敗試行回数アラーム/最大失敗試行回数アラーム**、**改ざん検出を有効にする**、**カード番号反転を有効にする**。

カードリーダータイプ

カードリーダーのタイプを取得します。

カードリーダーの説明

カードリーダーの説明を取得します。読み取り専用です。

カードリーダーを有効にする

カードリーダーの機能を有効にします。

認証

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

認証間隔

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

最大認証失敗回数アラーム/最大失敗回数アラーム

設定値に達した際にアラームを通知するように有効にします。

改ざん検出を有効にする

カードリーダーの改ざん検出を有効にします。

カード番号の逆転を有効にする

機能有効化後、カード番号は逆順で表示されます。

QRコード

機能を有効にすると、ユーザーはQRコードを使用してドアを開けることができます。

注意

- QRコード機能を有効にする場合は、赤外線ライトを無効にしてください。詳細については、を参照してください。赤外線ライトを無効にすると、低照度環境での画像が影響を受ける可能性があります。
- QRコード機能をHCCまたはHCECで設定する際は、1.0または2.0に対応したバージョンを選択してください。2.0が推奨されます。

ドアパラメーターを設定してください。

ドアのパラメーターを設定します。これには、ドア名、開門時間、出口ボタンタイプ、最初の人がドアを開けた後の開門保持時間、開門タイムアウトアラーム、ドアコンタクト、延長開門時間、緊急コード、スーパーパスワード、およびキャンセルコードが含まれます。

「 」をタップします。「**→**」→「**Access Control**」→「**→**」→「**Door Parameters**」をタップします。設定後、「**Save**」をタップします。

名前

ドアの名前を入力します。

開錠時間

カードをかざしてからドアが解錠されるまでの時間を設定します。

退出ボタンタイプ

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

最初の人が開けた後のドアの開いたままの持続時間

最初の人が入室した際のドアの開錠時間を設定します。最初の人が認証されると、複数の人物がドアへのアクセスまたはその他の認証アクションを実行できるようになります。

ドア開錠タイムアウトアラーム閾値

ドアがロック動作時間内に閉まらない場合、アクセス制御ポイントでアラームが鳴動します。0に設定すると、アラームは有効になりません。

ドアコンタクト

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

延長開錠時間

ドアの接触センサーは、拡張アクセス権限を持つユーザーがカードをかざした後、適切な遅延後に有効化されます。

緊急コード

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

スーパーパスワード

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

解除コード

解除コードを作成します。アラームがトリガーされた場合、解除コードを入力してアラームを解除できます。

注意 とスーパーパスワードは複製できません。通常、4から8桁の数字で構成されています。

アクセス制御とエレベーター制御

手順

1. をタップ→ **Access Control**→ **Elevator Control Parameters**。
2. **エレベーター制御を**有効にし、**ネガティブフロア容量**、**メインエレベーターコントローラーモデル**、および**インターフェースタイプを設定します**。

   注意

   - メインドアステーションのみがエレベーター制御をサポートします。
   - インターフェースタイプとして「**ネットワークインターフェース**」を選択した場合、サーバーアドレス、ポート、ユーザー、パスワードを設定する必要があります。

3. **保存**をタップします。

ターミナルパラメーター

ターミナルへのアクセス設定を行うことができます。

「 」をタップします。「→」→「Access Control」→「→」→「Terminal Parameters」を選択します。

アクセス制御モードとして**作業モード**を設定できます。アクセス制御モードはデバイスの通常モードです。アクセスするには、資格情報を認証する必要があります。

設定を保存するには、設定後「**保存**」をタップします。

RS-485 パラメーターの設定

RS-485 パラメーター（周辺機器、アドレス、ボーレートなど）を設定できます。 → **Access Control** → **RS-485** をタップします。

設定後、**保存**をタップして設定を保存します。

周辺機器タイプ

実際の状況に応じて、ドロップダウンリストから周辺機器を選択してください。選択可能な周辺機器は**カードリーダー**、**拡張モジュール**、または**アクセスコントローラーから選択できます**。

注意

周辺機器を変更して保存すると、デバイスが自動的に再起動します。

RS-485 プロトコルプライベート

このデバイスはRS-485経由で第三者デバイスと接続可能です。

OSDP

標準のRS-485プロトコル。

RS-485 アドレス

実際の要件に応じてRS-485アドレスを設定してください。

注意

アクセスコントローラーを選択した場合：RS-485インターフェース経由でデバイスをターミナルに接続する場合、RS-485アドレスを2に設定してください。デバイスをコントローラーに接続する場合、ドア番号に応じてRS-485アドレスを設定してください。

ボーレート

RS-485プロトコルでデバイスが通信する際のボーレートです。

データビット

RS-485プロトコルでデバイスが通信する際のデータビット数。

ストップビット

RS-485プロトコルでデバイスが通信する際のストップビット。

パリティ/フロー制御/通信モード

デフォルトで有効です。

出力タイプ

出力タイプを実際のニーズに合わせて設定してください。

カードセキュリティを設定してください。

デバイス用のカードを構成します。

「 」をタップします。「→」→「**Access Control**」→「→」→「**Card Security**」を選択します。

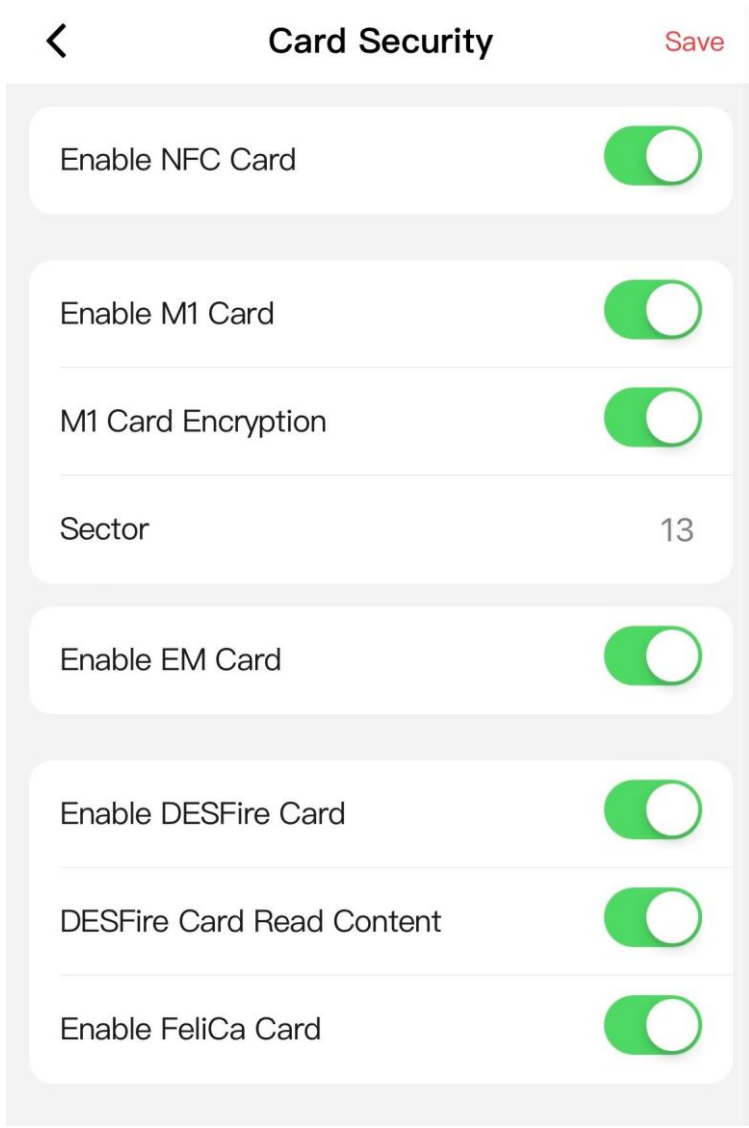


図8-5 カードセキュリティ

カードパラメーターを設定し、[**保存**] をクリックします。

NFC カードを有効にする

モバイルフォンがアクセス制御のデータを取得しないようにするため、NFC カードを無効にすることでデータのセキュリティレベルを向上させることができます。

M1 カードを有効にする

M1 カードを有効にすると、M1 カードを提示して認証が可能になります。

M1カード暗号化

M1カード暗号化は、認証のセキュリティレベルを向上させます。

セクター

機能を有効にし、暗号化セクターを設定します。

注意
セクター13の暗号化を推奨します。

EMカード有効化

EMカードを有効化し、EMカードを提示して認証を行う機能が利用可能です。

注意
周辺機器のカードリーダーがEMカードの提示に対応している場合、EMカード機能の有効/無効を切り替える機能も利用可能です。

DESFire カード有効化

デバイスは、DESFireカード機能有効時に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

デバイスは、FeliCaカード機能有効時にFeliCaカードからデータを読み取ることができます。

8.5.10 設定呼び出し

モバイルウェブ経由でデバイス番号を設定します。

このデバイスは、アクセス制御装置、ドアステーション、または外ドアステーションとして使用できます。ビデオインターコム用のデバイス番号を設定できます。

「☰」をタップします。「**→ Intercom**」をタップします。
「**→ Device ID Settings**」をタップします。「**Save**」をタップします。
デバイスタイプを**ドアステーション**または**アクセス制御デバイス**に選択した場合、デバイス番号、建物番号、ユニット番号、階数、およびドアステーション番号を設定できます。

デバイスタイプ

このデバイスはドアステーションとして使用できます。ドロップダウンリストから他のデバイスタイプを選択できます。

コミュニティ番号

デバイスのコミュニティ番号（期間番号）を入力します。

建物番号

装置の建物番号を入力してください。

番号

デバイス番号をカスタマイズしてください。

注意

- デバイスタイプが**ドアステーション**または**アクセス制御デバイスの**場合、番号は0から99の間で指定してください。
- デバイスタイプまたは番号を変更した後は、変更を反映させるためにデバイスを再起動する必要があります。

ユニット番号

デバイスのユニット番号を入力してください。

フロア番号

デバイスの階番号を入力してください。

デバイスタイプを「**外ドアステーション**」を選択した場合、デバイス番号と外ドアステーション番号を設定できます。

デバイスタイプ

このデバイスは外ドアステーションとして使用できます。ドロップダウンリストから他のデバイスタイプを選択できます。

コミュニティ番号

デバイスのコミュニティ番号（周期番号）を入力してください。

番号

デバイス番号をカスタマイズしてください。

注

- デバイスタイプが「**外ドアステーション**」の場合、番号は1から99の間で指定してください。
- デバイスタイプまたは番号を変更した後は、変更を反映させるためにデバイスを再起動する必要があります。

注意

デバイスタイプまたは番号を変更した後は、変更を反映させるためにデバイスを再起動する必要があります。

セッション設定

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

「 」をタップします。**「→」をタップします。「→」をタップします。「Session Settings」**をタップします。

「Registration Password」

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

メイン駅 IP

通信に使用するメインステーションのIPアドレスを入力してください。

プライベートサーバーIP

SIPサーバーのIPアドレスを指します。通信に使用するメインステーションのIPアドレスを入力してください。この時点では、メインステーションがSIPサーバーとして機能します。他のインターコムデバイスはこのサーバーアドレスに登録する必要があります。

プロトコル 1.0 を有効にする

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

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

保存をクリックします。

コール設定

メインステーションと他のデバイス間の最大通信時間を設定できます。 → **Intercom** → **コール設定**をタップします。

最大通信時間

メインステーションと他のデバイスが通話中における最大通信時間です。通信時間が設定された時間を超えると、通信が停止します。最大通信時間の範囲は90秒から120秒です。

番号設定

部屋のSIP番号を設定します。部屋はSIP番号を介して相互に通信できます。

手順

1. 「 」をタップします。**「→」をタップします。「→」をタップします。「Number Settings」を**タップします。
2. **ルーム番号**と**SIP番号1**を入力します。
3. **「保存」**をタップします。
4. **オプション:** 設定済みの部屋番号をタップし、編集するか、**+Add**をタップして別のSIP番号を追加します。
5. **オプション：削除**をタップして部屋番号を削除します。

ボタンを押してモバイルウェブ経由で通話します

ボタンを押して通話できます。

手順

1. 「 」をタップします**。→ インターコム→「ボタンを押して通話」を タップ**します。
2. **1**をタップしてページに移動します。

注意

- 「指定の室内ステーションに電話をかける」にチェックを付けた場合、リンクされた部屋の番号を設定する必要があります。
- デフォルトでは、ボタンを押すと室内呼び出し装置に呼び出し、ボタンを長押しするとコールセンターに呼び出しが可能です。

3. ボタンがリンクされている項目を選択します。「**指定した室内ステーションを呼び出す**」を選択した場合、部屋の番号を設定する必要があります。
4. **「保存」**をタップします。

8.5.11 モバイルウェブ経由でプライバシー設定を設定する

画像のアップロードと保存パラメーターを設定します。「 」

→「プライバシー設定」をタップします。

画像のアップロードと保存

「リンク後に画像を保存」または**「リンク後に画像をアップロード」**を有効にできます。キャプチャされた画像はプラットフォームにアップロードまたは保存されます。

「保存」をタップしてください。

8.5.12 パスワードモード

パスワードを設定する前に、パスワードがデバイスで設定された個人用PINか、プラットフォームで適用された個人用PINかを明確にする必要があります。デバイスで設定された個人用PINの場合、デバイスまたはウェブ上で作成または編集でき、他のプラットフォームでは設定できません；プラットフォームで適用された個人用PINの場合、プラットフォーム上で作成または編集でき、使用前にデバイスに発行する必要があります。デバイスまたはウェブ上で設定できません。

手順

1. 「 」をタップ**「→」**をタップ**「Configuration」をタップ「→」を**タップ**「Security」をタップ「→」**をタップ**「Password Mode」を**タップ**「Device-Set Personal PIN」を**

   デバイスまたはウェブ上で作成または編集でき、他のプラットフォームでは設定できません。

   プラットフォーム適用型個人用PIN

   プラットフォーム上で作成または編集でき、使用可能になる前にデバイスに発行する必要があります。デバイス上やウェブ上で設定することはできません。

2. **「保存」**をタップします。

8.5.13 アップグレードとメンテナンス

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

デバイスを再起動します

「 」をタップします。→ **Restart Device」をタップ**します。

「再起動」をタップしてデバイスを再起動します。

アップグレード

「 」をタップし、→**「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。

注意

アップグレード中は電源を切らないでください。

パラメーターを復元

「 」をタップし、→**をデフォルトに設定します**。

デフォルト設定に戻す

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。

工場出荷時設定に戻す

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

8.5.14 ユーザーマニュアルを表示

ユーザーマニュアルを表示します。

注意

IPアドレスでモバイルウェブにアクセスした場合のみ、ユーザーマニュアルを表示できます。ホットスポット経由でのログインではこの機能は利用できません。

「 」をタップしてページに移動してください。

「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。

8.5.15 オープンソースソフトウェアのライセンス

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。

「 」をタップしてページに移動してください。

「オープンソースソフトウェアライセンス」をタップしてください。

8.5.16 モバイルウェブからログアウト

モバイルウェブの構成ページからログアウトします。

ホーム画面で「 」をタップし、→ **Log Out** をタップし、**OK** をタップしてウェブからログアウトします。
設定ページに移動する必要がある場合は、ユーザー名とパスワードを再度入力してください。

第9章 その他の設定対象プラットフォーム

デバイスは、iVMS-4200 クライアント ソフトウェアまたは HikCentral アクセス コントロール 経由でも設定可能です。詳細については、各プラットフォームのユーザー マニュアルをご参照ください。

iVMS-4200 クライアントソフトウェア

リンクをクリックまたはタップして、クライアント ソフトウェアのユーザー マニュアルを表示してください。

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

HikCentral Access Control (HCAC)

リンクをクリックまたはタップして、HCACのユーザーマニュアルを表示します。

http://enpinfodata.hikvision.com/analysisQR/showQR/f2f6cf42

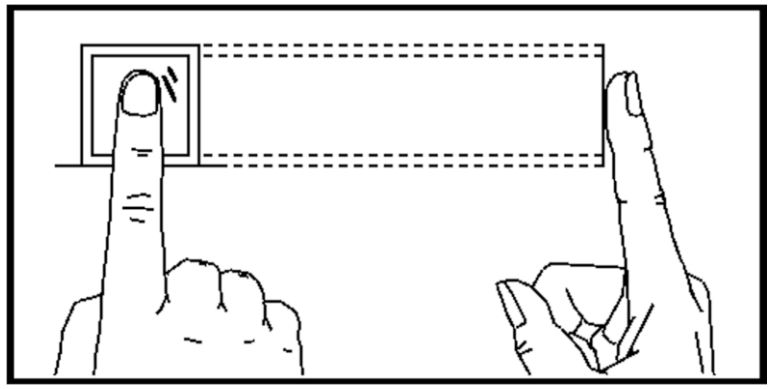
付録A. 指紋スキャン時のヒント

推奨される指

人差し指、中指、または薬指。

正しいスキャン方法

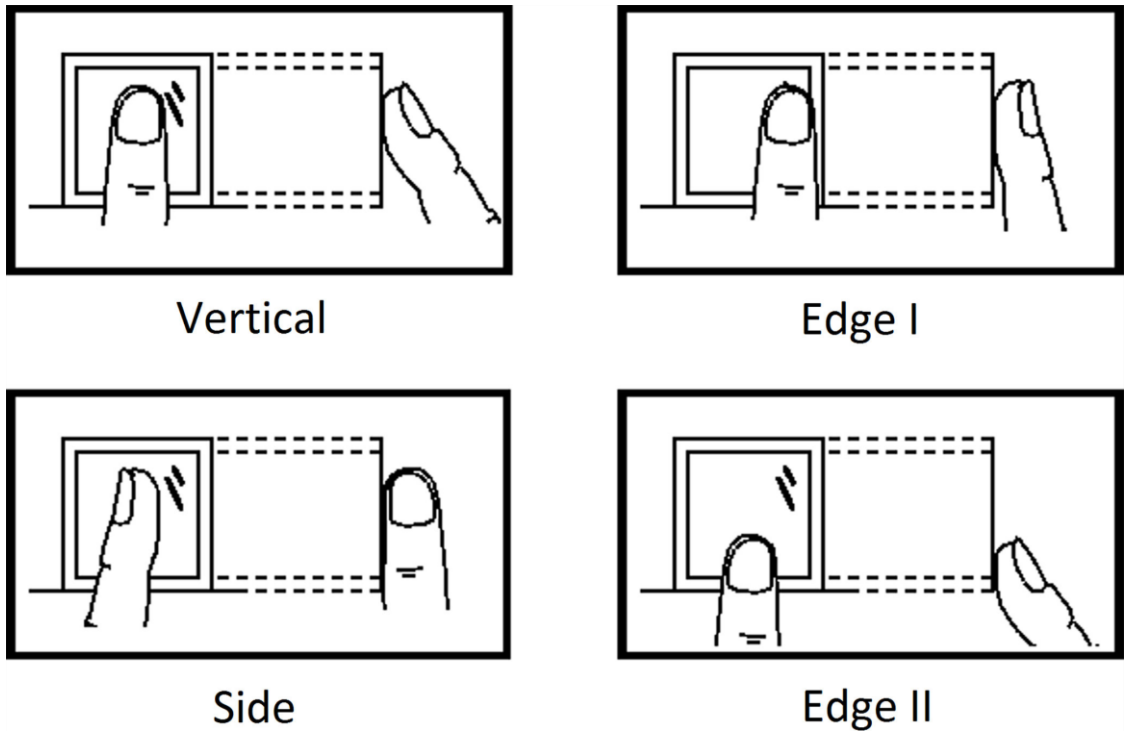
以下の図は、指をスキャンする正しい方法です:



指をスキャナーに水平に押し当ててください。スキャンされた指の中心がスキャナーの中心と一致するようにしてください。

不正なスキャン

以下の図は指紋スキャンの誤った例です:



環境

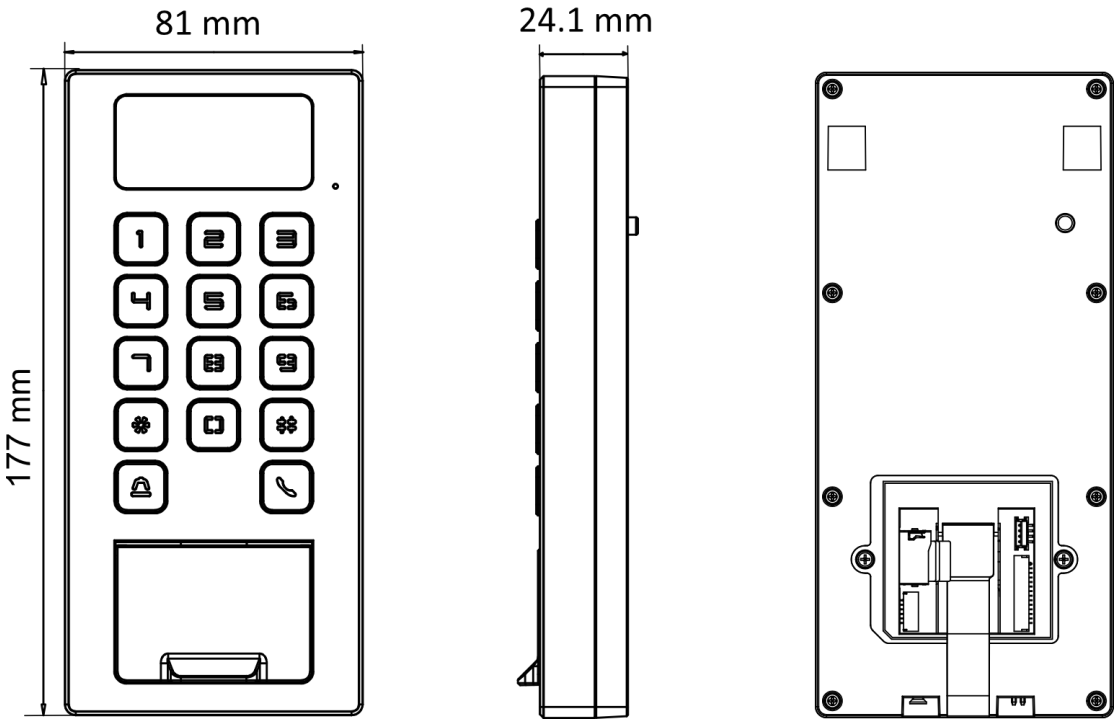
スキャナーは直射日光、高温、湿気、雨を避けてください。乾燥している場合、スキャナーが指紋を正しく認識できない可能性があります。指に息を吹きかけてから再度スキャンしてください。

その他

指紋が浅い場合、または指紋の読み取りが難しい場合は、他の認証方法をご利用いただくことをおすすめします。
スキャンする指に傷がある場合、スキャナーが認識しない可能性があります。別の指に変更して再度お試しください。

付録B. 寸法

デバイスの寸法




See Far, Go Further