



DS-K1T341A シリーズ顔認識端末

ユーザーマニュアル

法規関連情報

©2020 Hangzhou Hikvision Digital Technology Co., Ltd. All Rights Reserved.

本マニュアルについて

本マニュアルには製品の使用および管理についての指示が含まれています。ここに記載されている写真、グラフ、画像などの情報はすべて、説明のみを目的としています。本マニュアルに含まれる情報は、ファームウェア更新その他理由で事前の通知なく変更されることがあります。本マニュアルの最新バージョンは Hikvision の Web サイトを参照してください (<https://www.hikvision.com/>)。

この製品に関するサポート訓練を受けている専門家の指導や援助を受けた上で本マニュアルを使用してください。

商標

HIKVISION およびその他 Hikvision の商標およびロゴは、あらゆる裁判管轄地域において Hikvision の所有物です。

本マニュアルに示されたその他の商標およびロゴは、各権利保有者の所有物です。

免責事項

適用法により許容される範囲内で、本マニュアル、記載の製品とそのハードウェア、ソフトウェアおよびファームウェアは、あらゆる不具合や瑕疵を含め、現状有姿で提供されるものとし、Hikvision は明示の有無によらず一切の保証（性能、品質、特定の目的に対する適合性を含むが、これらに限定しない）を行いません。この製品は、ユーザーの責任で使用してください。Hikvision は、この製品の利用に関連する事業利益の損失や事業妨害、データの損失、システムの破損、文書の損失に関する損害を含む特別、必然的、偶発的または間接的な損害に対して、契約の違反、不法行為（過失を含む）、製造物責任、その他を問わず、たとえ Hikvision がそれらについて通知を受けていたとしても、一切の責任を負いません。

ユーザーは、インターネットの性質上、セキュリティリスクが内在していることを承知するものとし、Hikvision は、異常操作、プライバシー漏えいまたはサイバー攻撃、ハッキング、ウィルス検査やその他のセキュリティリスクから生じるその他の損害に対して一切の責任を負わないものとし、ただし、必要に応じて Hikvision は適宜技術サポートを提供します。

ユーザーは、この製品をすべての適用法に従って使用することに同意するものとし、使用方法が適用法に準拠するようにすることについては、ユーザー自身が一切の責任を負うものとし、特に、ユーザーは、第三者の権利（パブリシティ権、知的財産権、データ保護、および他のプライバシー権を含むが、これらに限定しない）を侵害しない方法でこの製品を使用することに責任を負います。ユーザーはこの製品を、大量破壊兵器の開発または製造、生物化学兵器の開発または製造、いかなる核爆発物または安全でない核燃料サイクルに関連する状況または人権侵害の支援での一切の活動を含む、いかなる禁止された最終用途にも使用しないものとし、

本マニュアルと適用法との間に矛盾が存在する場合は、後者が優先されます。




データ保護

デバイスの使用中には、個人情報の収集、保存、処理が行われます。データを保護するため、Hikvision におけるデバイスの開発には、設計原理としてプライバシー保護が組み込まれています。たとえば、顔認識機能を搭載するデバイスでは、バイオメトリクスデータはお使いのデバイスに暗号化して保存されます。また、指紋用デバイスの場合は、指紋画像の復元が不可能な状態で指紋テンプレートのみが保存されます。

データ管理者には、適用されるデータ保護法令に準拠してデータを収集、保存、処理、転送すること（これには合理的な管理上および物理的なセキュリティ管理などの個人データ保護を行うこと、その他が含まれます）に加えて、実施中のセキュリティ管理の実効性を定期的に見直し、評価することが推奨されます。

記号の定義

本マニュアルで使用する記号は以下のように定義されています。

記号	説明
 危険	防止できなかった場合に死亡や重傷を招くおそれのある危険な状況を示します。
 注意	潜在的に危険となりうる状況を示しており、防止できなかった場合、機器の破損、データの消失、性能劣化など、予測不能な結果が生じる可能性があります。
 メモ	本文内の重要事項を強調または補足する追加情報を提供します。

規制情報

FCC 情報

規制順守担当当局によって明示的に承認されていない変更や改造を行うと、本デバイスを操作するユーザーの権利が無効になる場合があります。

FCC への準拠: 本デバイスはテスト済みであり、FCC 規則第 15 条に規定されるクラス B デジタルデバイスの制限に適合することが確認されています。これらの制限事項は、住居内に設置した場合の有害な干渉に対して妥当なレベルの防護を提供するためのものです。本デバイスは無線周波数エネルギーを発生および使用し、また、これを放射する可能性があります。取扱説明書に従った設置および使用を行わなかった場合、無線通信に有害な干渉を引き起こすことがあります。しかし、特定の設置状況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。本デバイスがラジオやテレビの受信状態に有害な干渉を引き起こす場合（これは本デバイスの電源をオン、オフにすることで確認できます）、ユーザーは以下の手段の 1 つまたはそれ以上を実行して調整することが推奨されます。

- 受信アンテナの方向や位置を変える。
 - 本デバイスと受信機の距離を大きくする。
 - 本デバイスを受信機が接続されているものとは異なる回路のコンセントに接続する。
 - 支援が必要な場合は、販売店または経験豊富なラジオ/TV の技術者に相談してください
- 本デバイスは、放射部と身体との間の距離が 20cm 以上になるように設置し、操作してください。

FCC による条件

本デバイスは、FCC 規則第 15 条に準拠しています。本デバイスの使用にあたっては以下の 2 つの条件に従うものとします。

- 1.本デバイスが有害な干渉を引き起こすおそれがないこと。
- 2.本デバイスは、望ましくない操作を引き起こす可能性のある干渉を含むあらゆる干渉受信を受容しなければならないこと。

EU 適合宣言



本製品および同梱の周辺機器（適用可能な場合）には「CE」マークが付いており、EMC 指令（2014/30/EU）、RE 指令（2014/53/EU）、RoHS 指令（2011/65/EU）に掲げる適用可能な欧州統一基準に準拠しています。



2012/19/EU（WEEE 指令）：この記号が付いている製品は、欧州連合（EU）内の地方自治体の未分別廃棄物として処分することはできません。適切にリサイクルするために、本製品は同等の新しい装置を購入する際に、お近くの販売業者に返却いただくか、指定された収集場所で処分してください。詳細については以下をご覧ください。www.recyclethis.info



2006/66/EC（バッテリー指令）：本製品には、欧州連合（EU）内の地方自治体の未分別廃棄物として処分できないバッテリーが含まれています。特殊バッテリー情報に関する製品資料をご覧ください。このタイプのバッテリーにはこの記号が付いており、カドミウム（Cd）、鉛（Pb）、水銀（Hg）を示す文字も記載されています。適切にリサイクルするために、販売業者か、指定された収集場所にご返却ください。詳細については以下をご覧ください。www.recyclethis.info



安全上の指示

これらの指示は、ユーザーが製品を正しく使用し、危険や財産損失を回避できるようにすることを目的としています。

使用上の注意の基準は、以下のように「危険」と「注意」に分かれています。

危険: これらの警告を無視した場合、重傷事故または死亡事故が発生するおそれがあります。

注意: これらの注意を無視した場合、負傷事故または機器の破損が発生するおそれがあります。

	
危険: 重傷事故や死亡事故を防ぐために、これらの安全対策に従ってください。	注意: 負傷や物損の可能性を防ぐために、これらの注意に従ってください。

危険:

- 電氣的な操作はすべて、お住いの地域の電気保安規制、防火規制、その他の関連規制に厳格に従う必要があります。
- 電源アダプタは一般の企業が提供しているものを利用してください。この消費電力は必要値を下回ってはなりません。
- 1 つの電源アダプタに複数のデバイスを接続しないでください。過負荷によりオーバーヒートや火災の危険があります。
- 本デバイスの接続、取り付け、取り外しを行う前には必ず、電源が切断されていることを確認してください。
- 本デバイスを壁または天井に取り付ける場合、デバイスをしっかりと固定する必要があります。
- 本デバイスから煙や異臭、異音が発生した場合、すぐに電源を切り、電源ケーブルを抜いて、サービスセンターにご連絡ください。
- バッテリーを飲み込まないでください。化学熱傷を負う危険性があります。
本デバイスにはコイン／ボタン型の電池が含まれています。コイン／ボタン型電池を飲み込むと、わずか 2 時間のうちに体内に深刻な熱傷が生じ、死亡に至るおそれがあります。
新品および中古のバッテリーは子どもの手の届かない所で保管してください。バッテリーの収納場所を安全に閉じることができない場合は本デバイスの使用を中止し、子どもの手の届かない所で保管してください。バッテリーを飲み込んだかまたはバッテリーが体内のどこかにあるおそれがある場合、即座に医療従事者の指示に従ってください。
- 本デバイスが正しく動作しない場合、販売店または最寄りのサービスセンターに連絡してください。本デバイスを決してご自身で分解しようとししないでください。（承認されていない修理や保守行為による問題について、当社はいかなる責任も負いません）。

▲注意:


- 本デバイスを落下させたり、物理的な衝撃を与えたりしないでください。また、強度の電磁放射にさらさないようにしてください。本デバイスを振動面や衝撃が加わりやすい場所に取り付けることは避けてください（この指示を守らないと、デバイスが破損することがあります）。
- 本デバイスを高温（動作温度の詳細についてはデバイスの仕様を参照してください）の場所、低温の場所、ほこりの多い場所、あるいは湿度の高い場所に設置しないでください。また、強度の電磁放射にさらさないようにしてください。
- 屋内用のデバイスカバーは雨や湿気にさらさないようにしてください。
- 本デバイスを直射日光にさらしたり、換気の悪い場所に置いたり、ヒーターやラジエーターなどの熱源にさらすことは禁止されています（この指示を守らないと、火災の危険があります）。
- 太陽や極めて明るい場所に本デバイスを向けないでください。焦点ボケや不鮮明化が起こる可能性があります（動作不良ではありません）。また、センサーの寿命に影響が及ぶ可能性があります。
- デバイスカバーを開ける時は、同梱の手袋を着用して、デバイスカバーに直接触れることは避けてください。指の汗は酸性であるため、デバイスカバーの表面のコーティングが侵食されるおそれがあります。
- デバイスカバーの内側と外側の表面の清掃には、柔らかく乾いた布を用いてください。アルカリ洗剤は使わないでください。
- 梱包材は開梱後も保存しておき、将来利用できるようにしておいてください。何か不具合があった場合、本デバイスを工場に返送する際には納品時の梱包材を使う必要があります。納品時の梱包材以外を使った場合、デバイスが破損し、追加費用が発生する可能性があります。
- バッテリーの使用や交換を不適切に行うと、爆発の危険があります。バッテリーは、同一または同等のタイプのもののみと交換してください。使用済みバッテリーは、バッテリーのメーカーの指示に従って処分してください。
- バイオメトリクス認証製品は、アンチスプーフィング環境に完全に適応しているわけではありません。より高いセキュリティレベルが必要な場合は、複数の認証モードを使用してください。
- 入力電圧は、IEC60950-1 標準に従い、SELV（安全超低電圧）および 100～240 VAC または 12 VDC の有限電源を満たす必要があります。詳細情報に関しては技術仕様を参照してください。

販売中のモデル

製品名	モデル
顔認識端末	DS-K1T341AM
	DS-K1T341AMF

ユーザーマニュアルで指定されている、以下の電源のみをご使用ください。

モデル	メーカー	標準
ADS-26FSG-12 12024EPG	Shenzhen Honor Electronic Co.,Ltd	PG
MSA-C2000IC12.0-24P-DE	MOSO Technology Co.,Ltd	PDE
ADS-26FSG-12 12024EPB	Shenzhen Honor Electronic Co.,Ltd	PB
ADS-26FSG-12 12024EPCU/EPC	Shenzhen Honor Electronic Co.,Ltd	PCU
ADS-26FSG-12 12024EPI-01	Shenzhen Honor Electronic Co.,Ltd	PI
ADS-26FSG-12 12024EPBR	Shenzhen Honor Electronic Co.,Ltd	PBR

 **メモ:** 電源が屋内で使用され、動作温度が 0~40℃ であることを確認してください。

目次

第 1 章 概要	1
1.1 概要	1
1.2 機能	1
第 2 章 外観	3
第 3 章 取り付け	5
3.1 設置環境	5
3.2 ギャングボックスを用いた取り付け	5
3.3 ギャングボックスを使用しない場合の取り付け	8
第 4 章 配線	12
4.1 端末の説明	12
4.2 通常のデバイスの配線	13
4.3 セキュリティドア制御ユニットの配線	14
4.4 消火モジュールの配線	14
4.4.1 電源オフ時にドアが開放される配線図	14
4.4.2 電源オフ時にドアがロックされる配線図	16
第 5 章 アクティブ化	18
5.1 デバイス経由のアクティベート	18
5.2 Web ブラウザでのアクティベート	19
5.3 SADP 経由のアクティベート	20
5.4 クライアントソフトウェア経由でのデバイスのアクティベート	21
第 6 章 基本操作	23
6.1 アプリケーションモードの設定	23
6.2 管理者の設定	24
6.3 ログイン	27
6.3.1 管理者によるログイン	27
6.3.2 アクティブ化パスワードによるログイン	28

6.4	通信設定	30
6.4.1	有線ネットワークパラメータの設定	30
6.4.2	RS-485 パラメータの設定	30
6.4.3	Wiegand パラメータの設定	31
6.5	ユーザー管理	32
6.5.1	顔画像の追加	32
6.5.2	指紋の追加	34
6.5.3	カードの追加	35
6.5.4	パスワードの追加	36
6.5.5	認証モードの設定	37
6.5.6	ユーザーの検索と編集	38
6.6	データ管理	38
6.6.1	データの削除	38
6.6.2	データのインポート	38
6.6.3	データのエクスポート	39
6.7	ID 認証	40
6.7.1	単一の認証情報による認証	40
6.7.2	複数の認証情報による認証	40
6.8	基本設定	41
6.9	生体認証パラメータの設定	43
6.10	入退室管理パラメータの設定	45
6.11	時間および出勤状態の設定	46
6.11.1	デバイスによる出勤モードの無効化	46
6.11.2	デバイスによる出勤モードの手動設定	47
6.11.3	デバイスによる出勤モードの自動設定	47
6.11.4	デバイスによる出勤モードの手動および自動設定	49
6.12	システムメンテナンス	50
6.13	ビデオインターコム	51
6.13.1	デバイスからクライアントソフトウェアの呼び出し	51

6.13.2	デバイスからセンターの呼び出し	52
6.13.3	クライアントソフトウェアからデバイスの呼び出し	53
6.13.4	デバイスから部屋の呼び出し	53
第 7 章	Web ブラウザによる操作	55
7.1	ログイン	55
7.2	ライブビュー	55
7.3	人物管理	57
7.4	イベントの検索	57
7.5	設定	58
7.5.1	デバイス情報の表示	58
7.5.2	時間の設定	58
7.5.3	RS-485 パラメータの設定	59
7.5.4	Wiegand パラメータの設定	60
7.5.5	DST の設定	61
7.5.6	アップグレードとメンテナンス	61
7.5.7	管理者パスワードの変更	62
7.5.8	ネットワークパラメータの基本設定	63
7.5.9	EHome パラメータの設定	64
7.5.10	ビデオとオーディオのパラメータの設定	64
7.5.11	オーディオコンテンツのカスタマイズ	65
7.5.12	ビデオインターコムパラメータの設定	66
7.5.13	入退室管理および認証パラメータの設定	67
7.5.14	画像パラメータの設定	69
7.5.15	補助光輝度の設定	70
7.5.16	顔パラメータの設定	70
7.5.17	通知書の設定	73
第 8 章	クライアントソフトウェアの設定	74
8.1	クライアントソフトウェアの設定フロー	74
8.2	デバイス管理	74

8.2.1	デバイスの追加	75
8.2.2	デバイスのパスワードリセット	84
8.3	グループ管理	85
8.3.1	グループの追加	85
8.3.2	グループへのリソースのインポート	85
8.3.3	リソースパラメータの編集	86
8.3.4	グループからのリソースの削除	86
8.4	人物管理	86
8.4.1	組織の追加	87
8.4.2	基本情報の設定	87
8.4.3	ローカルモードでのカード発行	88
8.4.4	ローカル PC からの顔写真のアップロード	90
8.4.5	クライアント経由の写真撮影	91
8.4.6	入退室管理デバイスでの顔画像の取り込み	91
8.4.7	クライアントでの指紋の取り込み	92
8.4.8	入退室管理デバイスでの指紋の取り込み	93
8.4.9	入退室管理情報の設定	94
8.4.10	関係者情報のカスタマイズ	95
8.4.11	居住者情報の設定	96
8.4.12	追加情報の設定	97
8.4.13	人物の ID 情報のインポートとエクスポート	97
8.4.14	関係者情報のインポート	97
8.4.15	人物画像のインポート	98
8.4.16	関係者情報のエクスポート	99
8.4.17	人物画像のエクスポート	99
8.4.18	入退室管理デバイスからの関係者情報の取得	100
8.4.19	別組織への人物の移動	101
8.4.20	複数の人物へのカードの一括発行	101
8.4.21	カード紛失の報告	101

8.4.22 カードの発行パラメータ設定	102
8.5 スケジュールとテンプレートの設定	103
8.5.1 休日の追加	103
8.5.2 テンプレートの追加	105
8.6 アクセスグループの設定によるアクセス認証の人物への割り当て	106
8.7 詳細機能の設定	107
8.7.1 デバイスパラメータの設定	108
8.7.2 開放状態／閉鎖状態の設定	113
8.7.3 多要素認証の設定	115
8.7.4 Wiegand ルールのカスタム設定	117
8.7.5 人物の認証モードの設定	119
8.7.6 カードリーダーの認証モードおよびスケジュールの設定	120
8.7.7 最初の人物の入室設定	121
8.7.8 アンチパスバックの設定	122
8.7.9 デバイスパラメータの設定	124
8.8 入退室管理のリンク操作設定	130
8.8.1 アクセスイベントに対するクライアント操作の設定	131
8.8.2 アクセスイベントに対するデバイス操作の設定	132
8.8.3 カードのスワイプ動作に対するデバイス操作の設定	133
8.8.4 人物 ID に対するデバイス操作の設定	134
8.9 ドアの状態の制御	135
8.10 イベントセンター	136
8.10.1 デバイスからのイベント受信の有効化	136
8.10.2 リアルタイムイベントの表示	137
8.10.3 過去イベントの検索	140
8.11 時間および出勤	143
8.11.1 出勤パラメータの設定	143
8.11.2 タイムテーブルの追加	149
8.11.3 シフトの追加	150

8.11.4 シフトスケジュールの管理.....	151
8.11.5 チェックイン／チェックアウト記録の手動補正.....	155
8.11.6 休暇と出張の追加.....	156
8.11.7 出勤データの計算.....	158
8.11.8 出勤統計.....	159
A. 指紋スキヤンのヒント.....	163
B. 顔画像を取り込む／比較する場合のヒント.....	165
C. 設置環境のヒント.....	167
D. 寸法.....	168
E. 通信マトリックスとデバイスコマンド.....	170

第 1 章 概要

1.1 概要

顔認識端末には、入退室管理デバイスとして顔認識を実行する機能が備わっており、主に物流センターや空港、大学キャンパス、アラームセンター、住居などでセキュリティ用途の入退室管理システムとして使用されています。

1.2 機能

- 4.3 インチタッチスクリーン 2 MP ワイドアングルデュアルレンズ
- 顔アンチスプーフィング
- 顔認識の距離: 0.3 m~1.5 m
- ディープラーニングアルゴリズム
- 顔画像 1,500 件、カード 1,500 枚、指紋 1,500 件（デバイスモデルでサポートが必要）、イベント 150,000 件まで保存可能
- 顔認識に要する時間 < 0.2s/ユーザー、顔認識精度 ≥ 99%
- キャプチャリンクとキャプチャ画像のストレージ
- TCP/IP プロトコルを介して、カードとユーザーのデータをクライアントソフトウェアと送受信し、クライアントソフトウェア上にデータを保存
- USB フラッシュドライブから本デバイスへ画像をインポート。または本デバイスから USB フラッシュドライブへ画像とイベントをエクスポート
- スタンドアロン動作仕様
- 本デバイスにローカルでログイン後、デバイスのデータを管理、検索、設定
- RS-485 プロトコル経由で 1 つの外部カードリーダーに接続
- 端末の破壊時にドアが解錠する事態を避けるため、RS-485 プロトコルを介してセキュリティドア制御ユニットに接続
- Wiegand プロトコルを介して外部のアクセスコントローラまたは Wiegand カードリーダーに接続
- 屋内ステーションとマスターステーションを備えた 2 ウェイオーディオ
- チェックイン、チェックアウト、休憩開始、休憩終了、残業開始、残業終了の 6 つの出勤状態をサポート
- Web クライアントを介した設定
- リモートでドアを開放し、モバイルクライアントからライブビューを開始
- ISAPI および EHome 5.0 プロトコルをサポート

 メモ

バイオメトリクス認証製品は、アンチスプーフィング環境に完全に適応しているわけではありません。より高いセキュリティレベルが必要な場合は、複数の認証モードを使用してください。

第 2 章 外観

本顔認識端末の詳細については、以下をご覧ください。

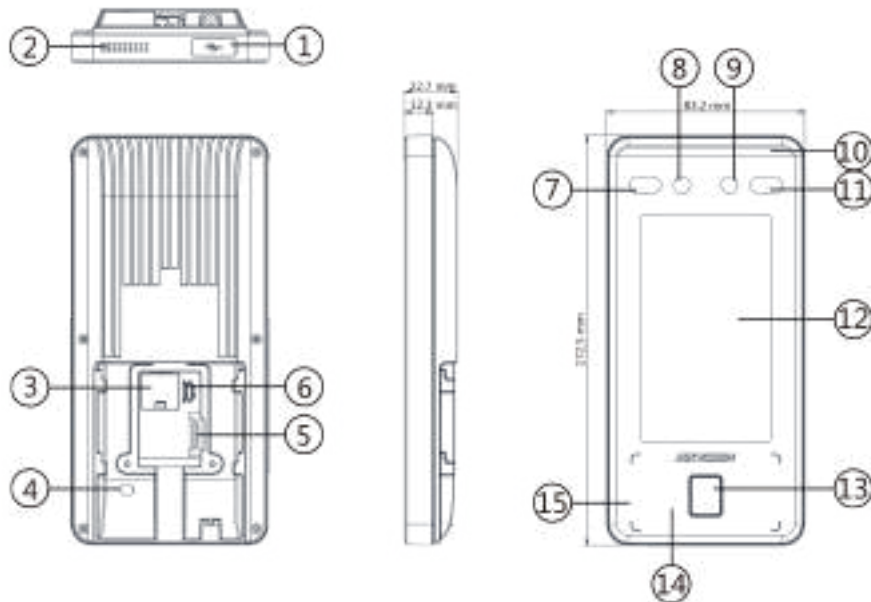




図 2-1 顔認識端末の図

表 2-1 顔認識端末各部の説明

番号	説明
1	microUSB インターフェース <hr/>  メモ パッケージには USB - microUSB ケーブルが含まれています。
2	スピーカー
3	ネットワークインターフェイス
4	タンパー
5	配線端末
6	デバッグポート
7	赤外線光
8	カメラ

番号	説明
9	カメラ
10	白色ライト
11	赤外線光
12	ディスプレイ画面
13	指紋モジュール <hr/>  メモ デバイスモジュールの一部でサポートされています。 <hr/>
14	カード提示エリア
15	マイク

第 3 章 取り付け

3.1 設置環境

- バックライト、直射日光、間接太陽光を避けてください。
- 認識の精度を上げるため、設置環境内またはその近くに光源を用意してください。

メモ

設置環境の詳細については、[設置環境のヒント](#)をご覧ください。

3.2 ギャングボックスを用いた取り付け

手順

メモ

追加の力は、装置の重量の 3 倍に相当します。装置とそれに関連する取り付け方法は、設置中も安全な状態を維持する必要があります。設置後は、関連する取り付けプレートを含め、装置を破損しないようにしてください。

1. ギャングボックスが壁に取り付けられていることを確認します。

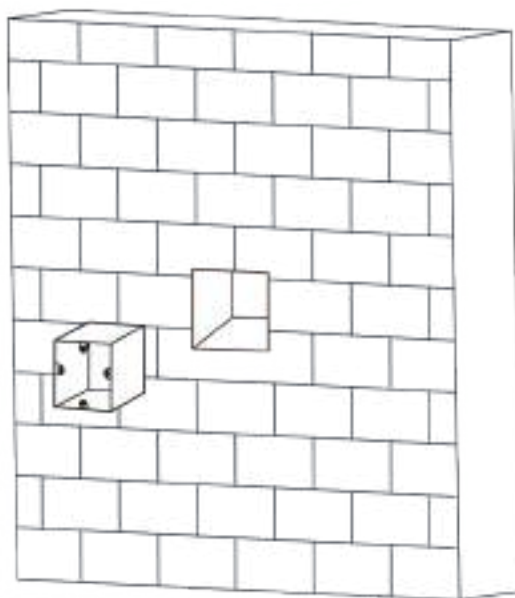


図 3-1 ギャングボックスの取り付け

2. 付属の 2 本のネジ (SC-K1M4×6-SUS) を使用して、ギャングボックス上にベースプレートを固定します。

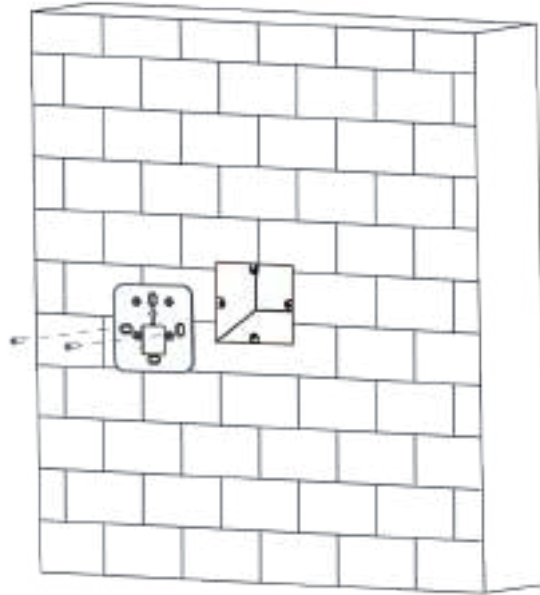


図 3-2 ベースプレートの固定

3. 付属の 4 本のネジ (KA4×22-SUS) を使用して、ベースプレート上に取り付けプレートを固定します。

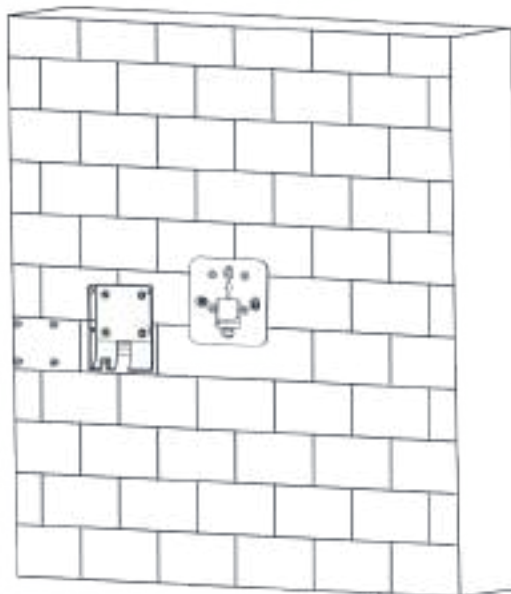


図 3-3 取り付けプレートの設置

4. 取り付けプレートの穴にケーブルを通し、対応する外部デバイスのケーブルに接続します。
5. 本デバイスを取り付けプレート上の正しい位置に置きます。

 **メモ**

デバイスを屋外に設置する場合は、保護シールドを取り付ける必要があります。詳細については、当社の技術サポートにお問い合わせください。

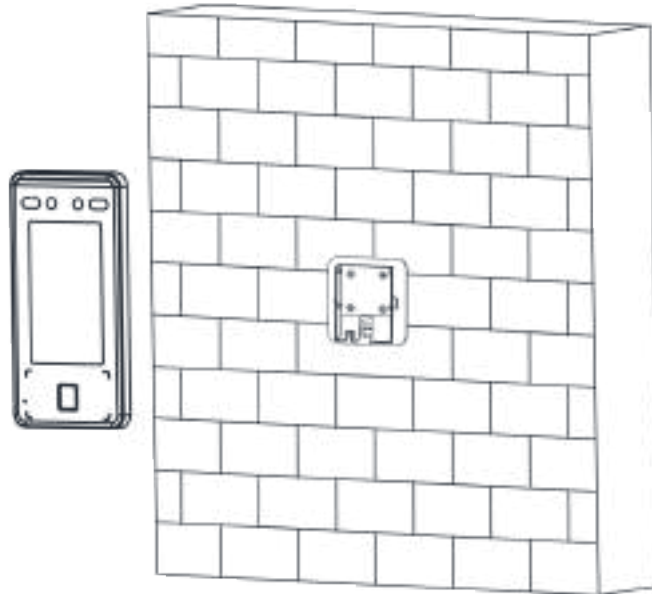


図 3-4 デバイスの取り付け

- 6.1 本の付属ネジ（SC-KM3X6-H2-SU）を使用して、デバイスと取り付けプレートを固定します。

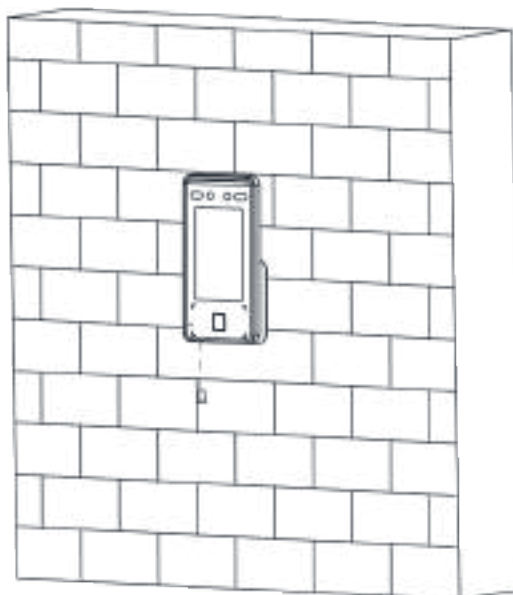


図 3-5 デバイスの固定

7. デバイスの背面パネルと壁（下部を除く）の間の接合部にシリコン製密封材を塗布して、雨滴が入らないようにします。

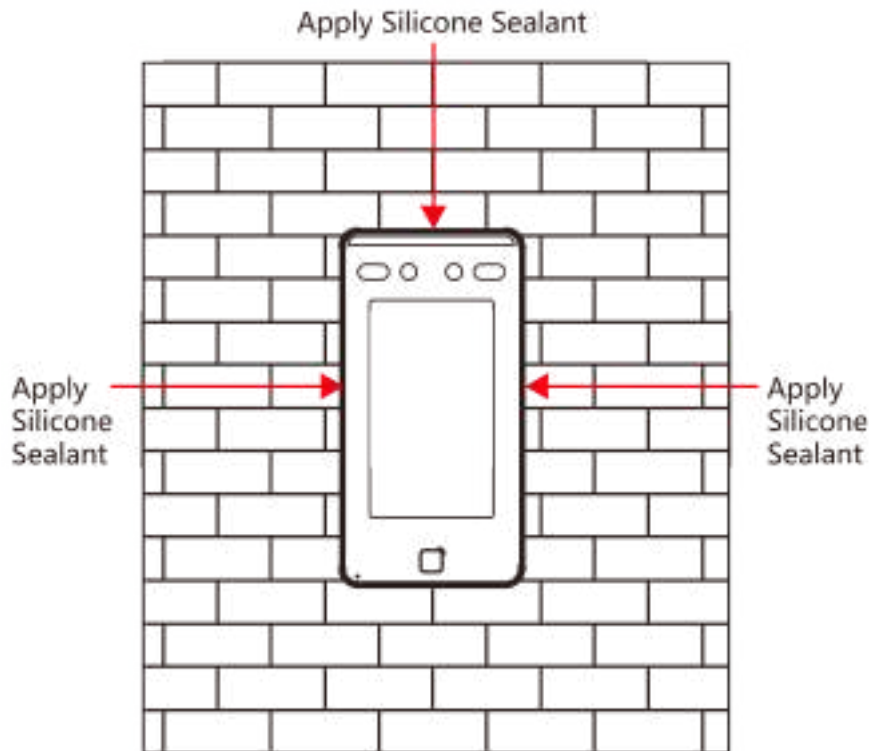


図 3-6 シリコン製密封材を側面に塗布

3.3 ギャングボックスを使用しない場合の取り付け

手順

メモ

追加の力は、デバイスの重量の 3 倍に相当します。デバイスとそれに関連する取り付け方法は、設置中も安全な状態を維持する必要があります。設置後は、関連する取り付けプレートを含め、デバイスを破損しないようにしてください。

1. 取り付けテンプレート上の基準線が地上 1.4m の高さになるように、取り付けテンプレートを壁などの面に設置します。

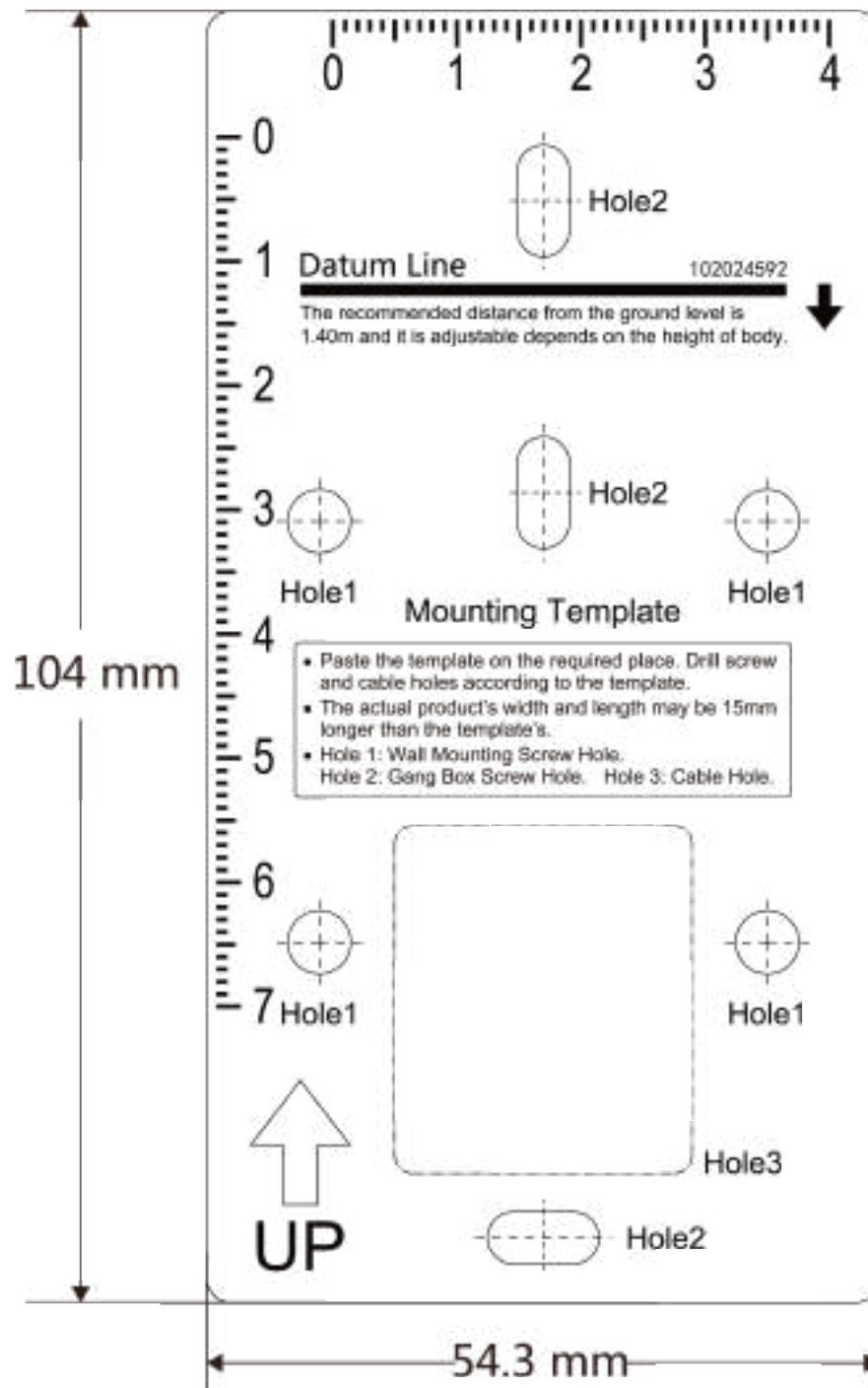


図 3-7 取り付けテンプレート

2. 取り付けテンプレートの指示に従って壁などの面に穴を開けます。
3. 取り付けプレートの穴にケーブルを通し、対応する外部デバイスのケーブルに接続します。
4. 取り付けプレートに穴を合わせ、付属の 4 本のネジで壁に取り付けプレートを固定します。

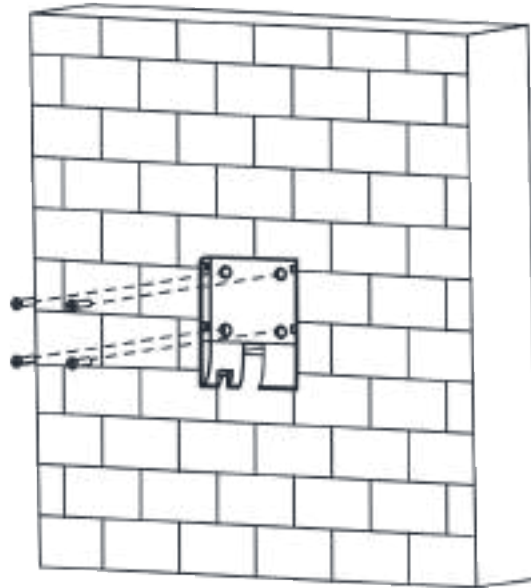


図 3-8 取り付けプレートの設置

5. 本デバイスを取り付けプレート上の正しい位置に置きます。

 **メモ**

デバイスを屋外に設置する場合は、保護シールドを取り付ける必要があります。詳細については、当社の技術サポートにお問い合わせください。

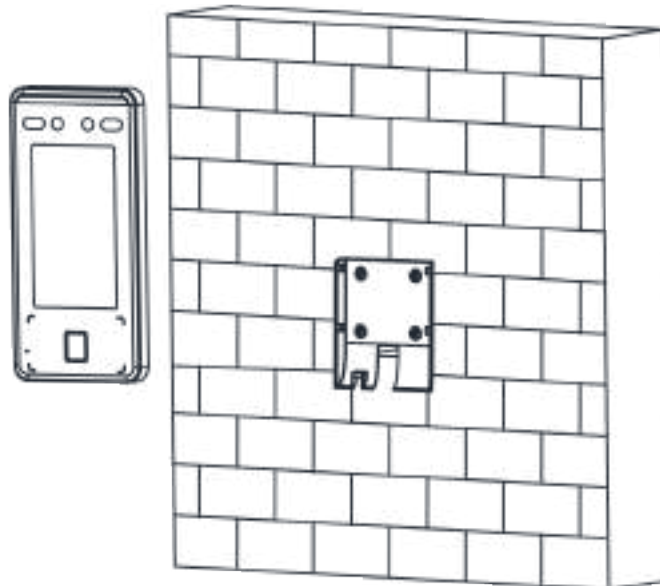


図 3-9 デバイスの取り付け

6. 付属のネジ 1 本を使用して、デバイスと取り付けプレートを固定します。

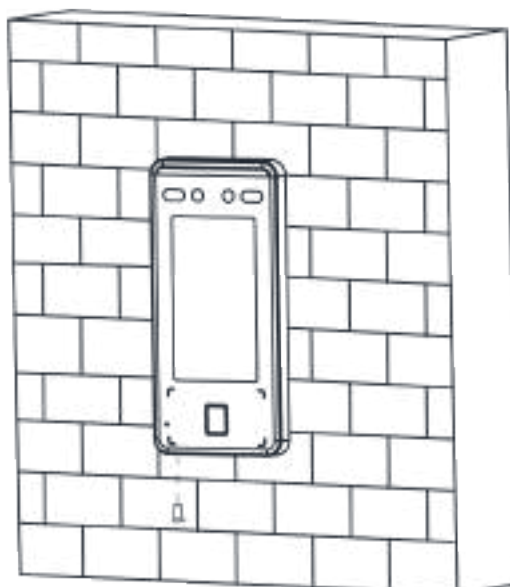


図 3-10 デバイスの固定

7. デバイスの背面パネルと壁（下部を除く）の間の接合部にシリコン製密封材を塗布して、雨滴が入らないようにします。

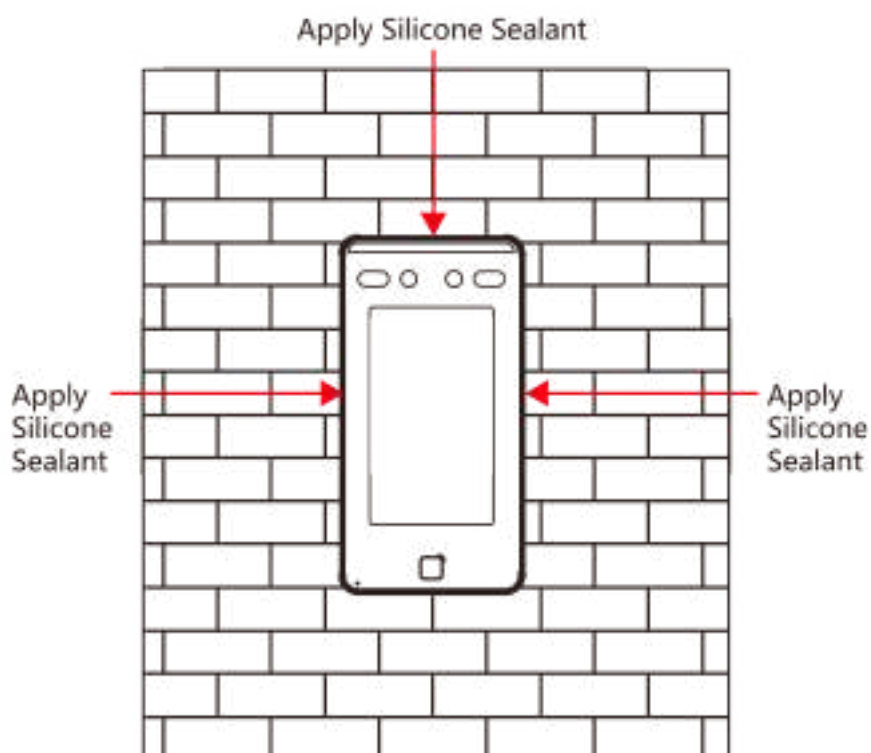


図 3-11 シリコン製密封材を側面に塗布

第 4 章 配線

以下の機器同士を接続できます。具体的には、RS-485 端末と RS-485 カードリーダー、NC/COM 端末とドアロック、センサー端末とドアの接触装置、BTN/GND 端末と出口ボタン、そして Wiegand 端末と Wiegand 規格のカードリーダーまたはアクセスコントローラです。

Wiegand 端末をアクセスコントローラに接続すると、顔認識端末が認証情報をアクセスコントローラに送信し、アクセスコントローラがドアの開閉を判断します。

メモ

ケーブルサイズが 18 AWG の場合、単一のデバイスを配線するときは、電源装置とデバイス間の距離が 60 m を超えないようにしてください。ドアロックとその他の周辺機器は、12 VDC 外部電源に接続する必要があります。12 VDC ドアロックに接続する場合、電源装置とデバイスの距離は 30 m でなければなりません。

4.1 端末の説明

本端末には電源入力、RS-485、Wiegand 出力、ドアロックが含まれています。端末の説明は以下のとおりです。

表 4-1 端末の説明

グループ	番号	機能	カラー	名前	説明
グループ A	A1	電源入力	赤	+ 12V	12 VDC 電源
	A2		黒	GND	アース
グループ B	B1	RS-485	黄	485 +	RS-485 の配線
	B2		青	485 -	
	B3		赤/黒	GND	アース
グループ C	C1	Wiegand	緑	W0	Wiegand の配線 0
	C2		白	W1	Wiegand の配線 1
	C3		白/黒	GND	アース
グループ D	D1	ドアロック	白/紫	NC	ロックの配線 (NC)
	D2		白/黄	COM	共通
	D3		白/赤	NO	ロックの配線

グループ	番号	機能	カラー	名前	説明
					(NO)
	D4		黄／緑	センサー	ドアの接触装置
	D5		黒	GND	アース
	D6		黄／グレー	ボタン	出口ドアの配線
	D7		黄／黒	GND	アース

4.2 通常のデバイスの配線

この端末を通常の周辺機器に接続できます。

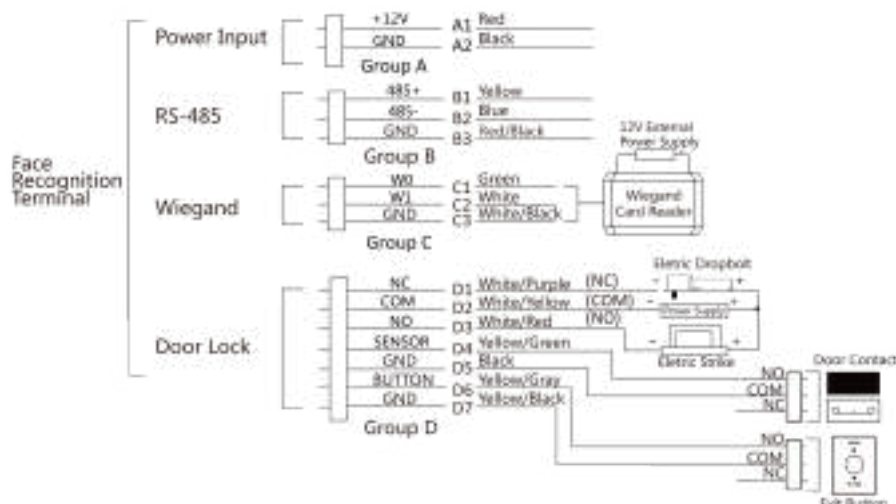


図 4-1 デバイスの配線

メモ

- Wiegand カードリーダーに接続する場合、顔認識端末の Wiegand 方向を「入力」に設定してください。アクセスコントローラに接続する場合、Wiegand 方向を「出力」に設定し、認証情報をアクセスコントローラへ送信してください。
- Wiegand 方向設定の詳細については、「Wiegand パラメータの設定」をご覧ください。

4.3 セキュリティドア制御ユニットの配線

この端末をセキュリティドア制御ユニットに接続できます。
配線図は以下のとおりです。

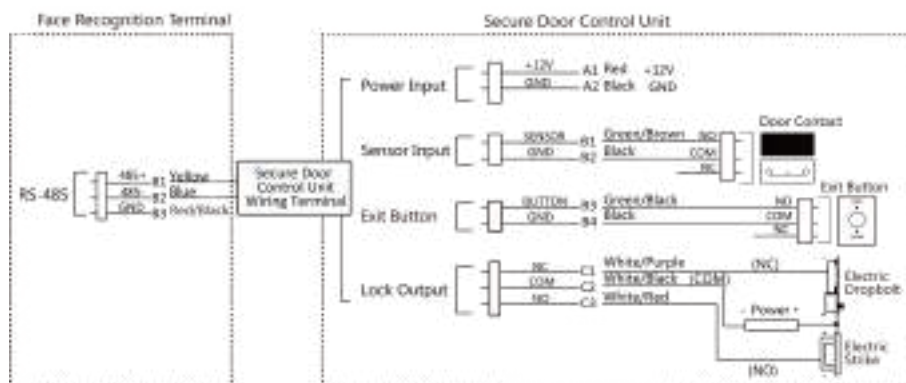


図 4-2 セキュリティドア制御ユニットの配線

メモ

セキュリティドア制御ユニットは、別途、外部電源に接続する必要があります。12V、0.5A の外部電源を推奨します。

4.4 消火モジュールの配線

4.4.1 電源オフ時にドアが開放される配線図

ロックタイプ: 陽極ロック、磁気ロック、および電気ボルト (NO)

セキュリティタイプ: 電源オフ時にドアが開いている

シナリオ: ファイアエンジンアクセスにインストールされている

タイプ 1

メモ

消火システムは、入退室管理システムの電源を制御します。

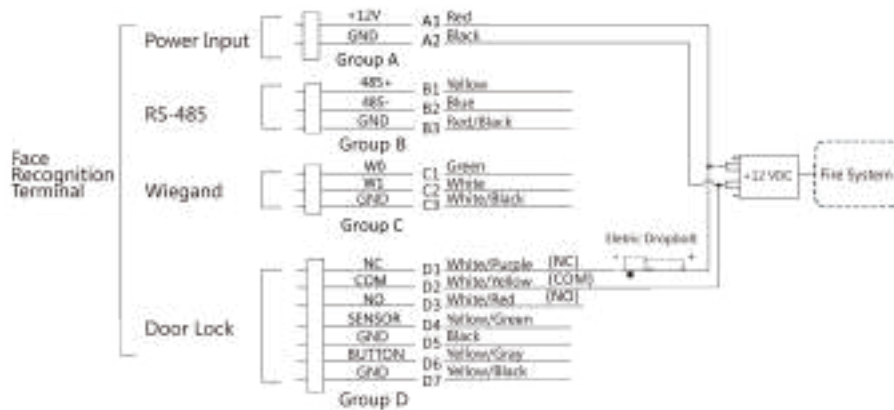


図 4-3 デバイスの配線

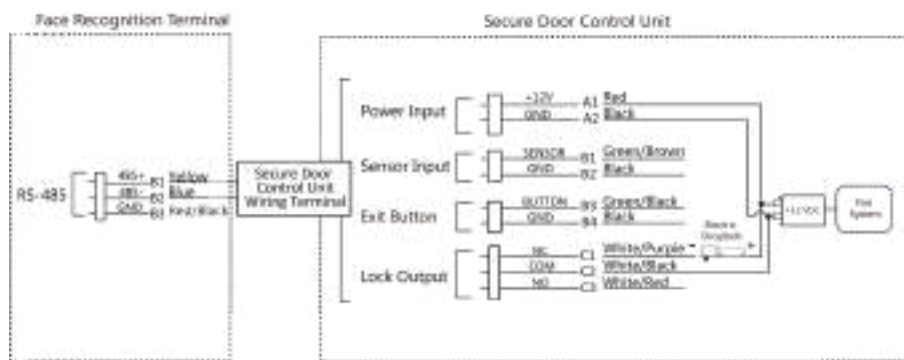


図 4-4 セキュリティドア制御ユニットの配線

タイプ 2

メモ

消火システム（NO および COM、通常は電源オフ時に開いている）は、ロックと電源装置に直列接続されています。火災警報が作動すると、ドアは開いたままになります。通常の場合、NO と COM は閉じています。

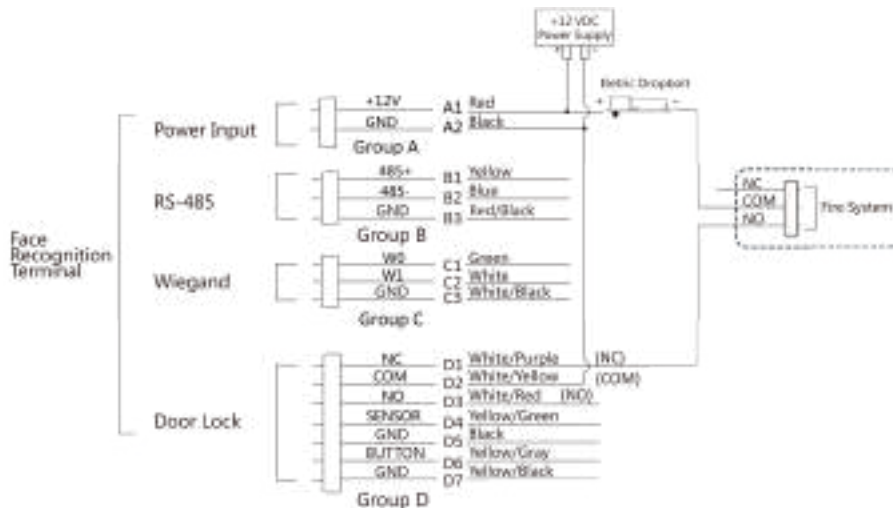


図 4-5 デバイスの配線

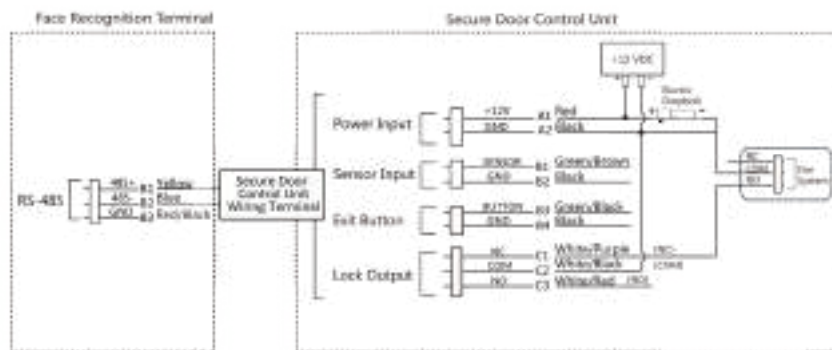


図 4-6 セキュリティドア制御ユニットの配線

4.4.2 電源オフ時にドアがロックされる配線図

ロックタイプ: 陰極ロック、電気ロック、および電気ボルト (NC)

セキュリティタイプ: 電源オフ時にドアがロックされる

シナリオ: 消火リンクで入口/出口に取り付け

メモ

- 無停電電源装置 (UPS) が必要です。
- 消火システム (NC および COM、通常は電源オフ時に閉じている) は、ロックと電源装置に直列に接続されています。火災警報が作動すると、ドアは開いたままになります。通常時は、NC と COM が開いています。

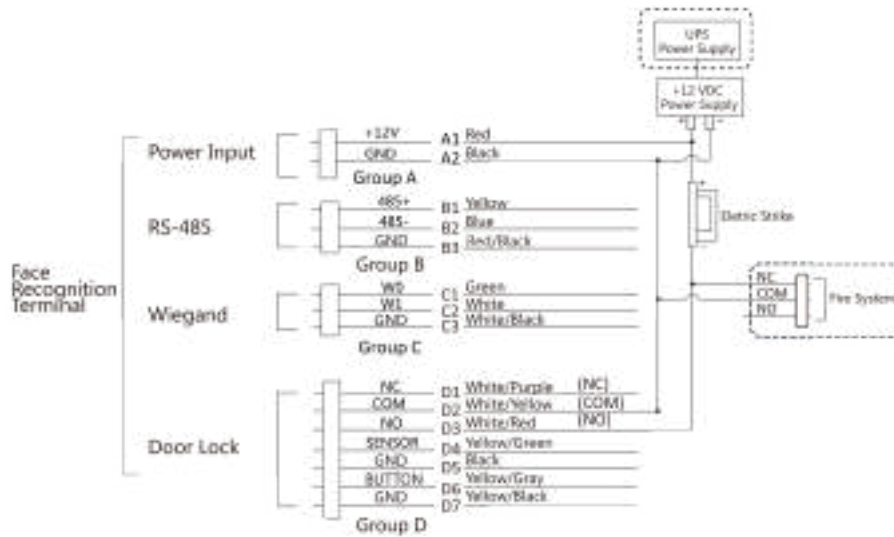


図 4-7 デバイスの配線

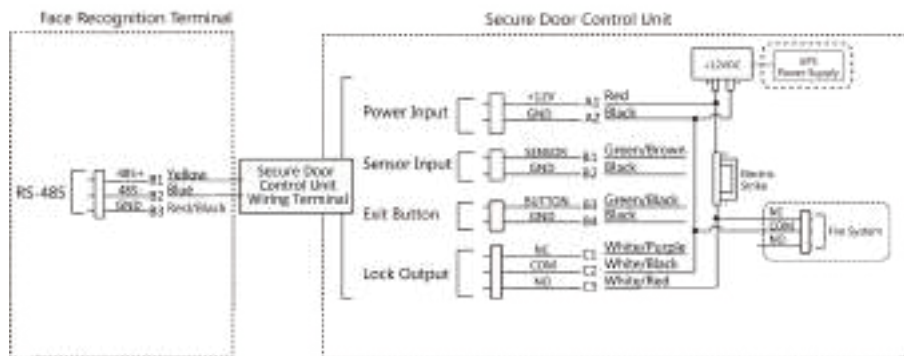


図 4-8 配線図

第 5 章 アクティブ化

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。電源の入力後、[デバイスのアクティブ化] ページが表示されます。

アクティブ化は、デバイス、SADP ツール、クライアントソフトウェア経由で行うことができます。

本デバイスのデフォルト値は以下のとおりです。

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

5.1 デバイス経由のアクティベート

本デバイスをアクティベートしていない場合、電源の入力後にアクティベートできます。[デバイスをアクティベート] ページでパスワードを作成し、確認してください。[アクティベート] をタップすると、デバイスがアクティベートされます。



図 5-1 [アクティブ化] ページ

 **注意**

デバイスのパスワードの強度は、自動的に確認することができます。デバイスのセキュリティを高めるため、ご自身で作成した強力なパスワード（大文字、小文字、数字、特殊記号のうち、少なくとも 3 つのカテゴリで構成される文字を含む 8 文字以上のパスワード）を設定することを強く推奨します。また、定期的にパスワードを変更することを推奨します。特にセキュリティ要件の高いシステムでは、毎月または毎週パスワードを変更すると、より安全にデバイスを保護できます。パスワードなどのセキュリティ設定はすべて、設置者／エンドユーザーの責任で適切に行ってください。

- アクティブ化後、アプリケーションモードを選択する必要があります。詳細については、「**アプリケーションモードの設定**」を参照してください
- アクティブ化後、クライアントソフトウェアまたはその他のプラットフォームにデバイスを追加する必要がある場合は、デバイスの IP アドレスを編集する必要があります。詳細については、「**通信設定**」をご覧ください。

5.2 Web ブラウザでのアクティベート

Web ブラウザを通じて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。

 **メモ**

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 セグメントで設定されてい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、確認します。

 **注意**

強力なパスワードの推奨 - 製品のセキュリティ向上のため、ご自身で選択した強力なパスワード（最低 8 文字を使用し、大文字、小文字、数字、特殊記号のすべてを含む）を作成することを強く推奨します。また、定期的にパスワードを再設定することを推奨します。特にセキュリティ要件の高いシステムでは、毎月または毎週パスワードを再設定すると、より安全にデバイスを保護できます。

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。この IP アドレスは、SADP ツール、デバイス、クライアントソフトウェアを使用して編集できます。

5.3 SADP 経由のアクティベート

SADP は、LAN 内にあるデバイスの IP アドレスの検知、アクティベート、変更を行うためのツールです。

始める前に

- 付属ディスク、または公式 Web サイト <http://www.hikvision.com/en/> から SADP ソフトウェアをダウンロードし、プロンプトに従ってインストールしてください。
- 本デバイスと SADP ツールを実行する PC は、同じサブネット内に配置してください。

本デバイスをアクティベートして IP アドレスを変更する手順は以下のとおりです。アクティベートと IP アドレス変更を一括して行う方法については、「SADP のユーザーマニュアル」をご覧ください。

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のリストから該当のデバイスを探し、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、確認します。

注意

強力なパスワードの推奨 - 製品のセキュリティ向上のため、ご自身で選択した強力なパスワード（最低 8 文字を使用し、大文字、小文字、数字、特殊記号のすべてを含む）を作成することを強く推奨します。また、定期的にパスワードを再設定することを推奨します。特にセキュリティ要件の高いシステムでは、毎月または毎週パスワードを再設定すると、より安全にデバイスを保護できます。

4. [アクティベート] をクリックしてアクティブ化を開始します。



アクティブ化に成功すると、デバイスの状態は [アクティブ] になります。

5. デバイスの IP アドレスを変更します。

1) デバイスを選択します。

2) IP アドレスを手動で変更するか、[DHCP を有効化] にチェックを入れて、デバイスの IP アドレスをお使いのコンピュータと同じサブネットに設定してください。

3) 管理者パスワードを入力して [変更] をクリックし、IP アドレスの変更をアクティベートします。


5.4 クライアントソフトウェア経由でのデバイスのアクティベート

デバイスによっては、ソフトウェアに追加して適切に動作させるために、デバイスをアクティベートするためのパスワードを作成する必要があります。

手順

メモ

使用するデバイスがこの機能に対応し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] の右側で  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、オンラインデバイスエリアを表示します。
検索したオンラインデバイスがリスト内に表示されます。
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ます。
5. [アクティベート] をクリックして [アクティブ化] ダイアログを開きます。
6. パスワードフィールドに新たな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、自動的に確認することができます。デバイスのセキュリティを高めるため、ご自身で作成した強力なパスワード（大文字、小文字、数字、特殊記号のうち、少なくとも 3 つのカテゴリで構成される文字を含む 8 文字以上のパスワード）を設定することを強く推奨します。また、定期的にパスワードを変更することを推奨します。特にセキュリティ要件の高いシステムでは、毎月または毎週パスワードを変更すると、より安全にデバイスを保護できます。パスワードなどのセキュリティ設定はすべて、設置者／エンドユーザーの責任で適切に行ってください。

7. **[OK]** をクリックしてデバイスをアクティベートします。

第 6 章 基本操作

6.1 アプリケーションモードの設定

デバイスをアクティベートした後、デバイスの用途に合わせてアプリケーションモードを選択する必要があります。

手順

1. [ようこそ] ページでドロップダウンリストの中から[屋内] または [その他] を選択します。

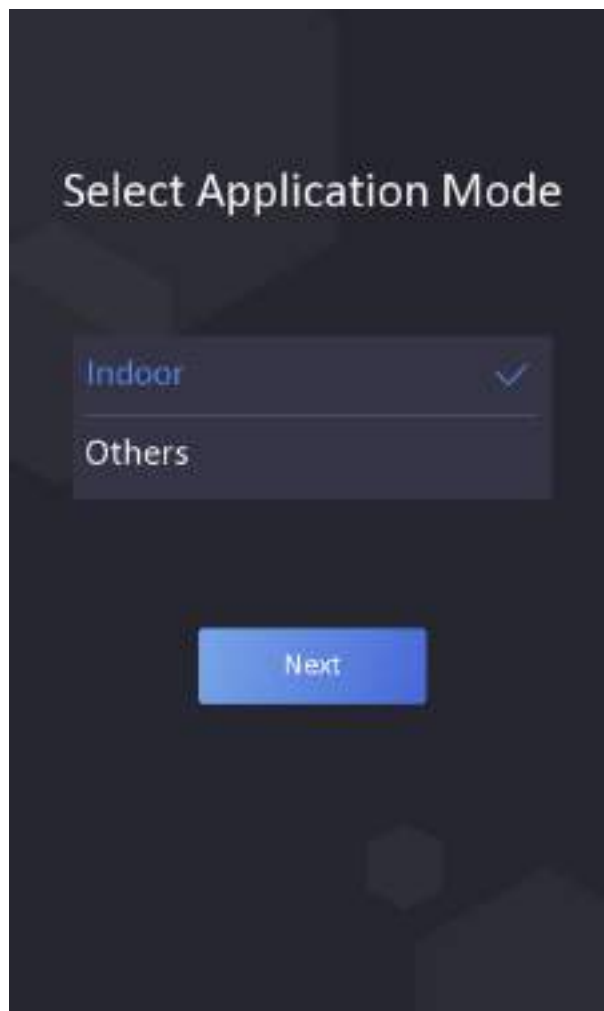


図 6-1 [ようこそ] ページ

2. [OK] をタップして保存します。

 **メモ**

- この設定は [システム設定] でも変更できます。
 - 屋内でも窓の近くにデバイスを取り付ける場合、または顔認識機能が正常に動作していない場合は、[その他] を選択してください。
 - アプリケーションモードを設定せずに [次へ] をタップした場合、[屋内] がデフォルトで選択されます。
 - 他のツールを使用してリモートでデバイスをアクティベートすると、アプリケーションモードには [屋内] がデフォルトで選択されます。
-

6.2 管理者の設定

デバイスをアクティブ化した後、管理者を追加してバックエンドを管理できます。

始める前に

デバイスをアクティベートして、アプリケーションモードを選択します。

手順

 **メモ**

[スキップ] をタップして管理者の追加をスキップします。

1. 管理者の名前を入力し（オプション）、[次へ] をタップします。

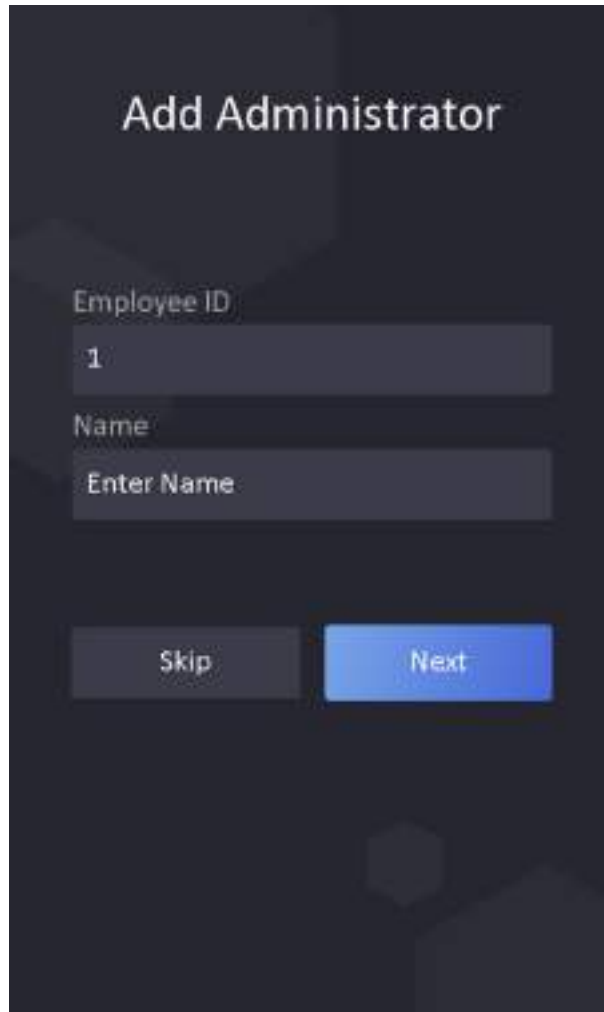








図 6-2 [管理者を追加] ページ

2. 追加する認証情報を選択します。

 **メモ**

認証情報を 1 つ追加する必要があります。

- : 顔をカメラに向けます。顔認識エリアに顔が来るようにしてください。  をクリックしてキャプチャし、  をクリックして確認します。
 - : デバイス画面の指示に従って指を押します。  をクリックして確認します。
 - : カード番号を入力するか、カードの提示エリアにカードを近づけます。 **[OK]** をクリックします。
3. **[OK]** をクリックします。
認証ページが表示されます。

状態アイコンの説明



左から、デバイスが警戒状態／非警戒状態です。



左から、デバイスの有線ネットワークが接続されている状態／接続されていない状態／接続に失敗した状態です。



左から、デバイスの Wi-Fi が有効で接続済みの状態／未接続状態／有効だが未接続の状態です。

ショートカットキーの説明



画面に表示されるショートカットキーを設定できます。詳細については、「**基本設定**」をご覧ください。




QR コードをスキャンして認証します。



QR コードは、ビジター端末から入手できます。



- デバイスの部屋番号を入力し、[OK] をタップして電話をかけます。
 -  をタップしてセンターに電話します。
-



デバイスを中央に追加する必要があります。そうしないと、呼び出し操作が失敗します。



パスワードを入力して認証します。

6.3 ログイン

デバイスのバックエンドにログインして、デバイスの基本パラメータを設定します。

6.3.1 管理者によるログイン

デバイスに管理者を追加した後は、デバイスの操作をするためにログインできるのは管理者のみになります。

手順

1. 最初のページを 3 秒間長押しし、ジェスチャーにしたがって左右にスライドして管理者ログインページを表示します。



図 6-3 管理者ログイン



2. 管理者の顔、指紋、またはカードを認証し、ホームページを開きます。



図 6-4 [ホーム] ページ

メモ

指紋またはカードの認証に 5 回失敗すると、デバイスは 30 分間ロックされます。

3. オプション:  をタップしてデバイスのアクティブ化パスワードを入力すると、ログインできます。
4. オプション:  をタップすると、管理者ログインページが閉じます。

6.3.2 アクティブ化パスワードによるログイン

デバイスに他の操作を行う前に、システムへログインする必要があります。管理者を設定しない場合は、以下の手順に従ってログインしてください。

手順

1. 最初のページを 3 秒間長押しし、ジェスチャーにしたがって左右にスライドしてパスワード入力ページを開きます。

2. [パスワード] フィールドをタップしてデバイスのアクティブ化パスワードを入力します。
 3. [OK] をタップしてホームページを開きます。
-

 **メモ**

パスワードの入力に 5 回失敗すると、デバイスは 30 分間ロックされます。



図 6-5 [ホーム] ページ

6.4 通信設定

通信設定ページでは、ネットワークパラメータ、RS-485 パラメータ、Wiegand パラメータを設定できます。

6.4.1 有線ネットワークパラメータの設定

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

手順

1. [ホーム] ページで **[通信]** (通信設定) をタップして、[通信設定] ページを開きます。
2. [通信設定] ページで、**[有線ネットワーク]** をタップします。



図 6-6 有線ネットワークの設定

3. DHCP、IP アドレス、サブネットマスク、またはゲートウェイを設定します。

メモ

デバイスの IP アドレスとコンピュータの IP アドレスを同じ IP セグメントで設定してください。

6.4.2 RS-485 パラメータの設定

顔認識端末は、RS-485 端末を経由して外部のアクセスコントローラやセキュリティドア制御ユニット、またはカードリーダーに接続できます。

手順

1. [ホーム] ページで **[通信]** (通信設定) をタップして、[通信設定] ページを開きます。
2. [通信設定] ページで **[RS-485]** をタップして [RS-485] タブを開きます。

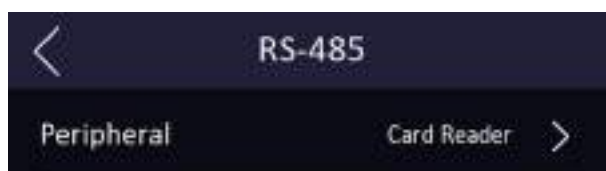


図 6-7 RS-485 パラメータの設定

3. 実際の使用状況に応じて周辺機器のタイプを選択します。

メモ

アクセスコントローラを選択した場合: RS-485 インタフェースを介してデバイスを端末に接続する場合は、RS-485 アドレスを 2 に設定します。デバイスをコントローラに接続する場合は、ドア番号に従って RS-485 アドレスを設定します。

4. 左上の [戻る] アイコンをタップします。パラメータを変更する場合は、デバイスを再起動する必要があります。

6.4.3 Wiegand パラメータの設定

Wiegand の通信方向を設定できます。

手順

1. [ホーム] ページで [通信] (通信設定) をタップして、[通信設定] ページを開きます。
2. [通信設定] ページで [Wiegand] をタップして [Wiegand] タブを開きます。

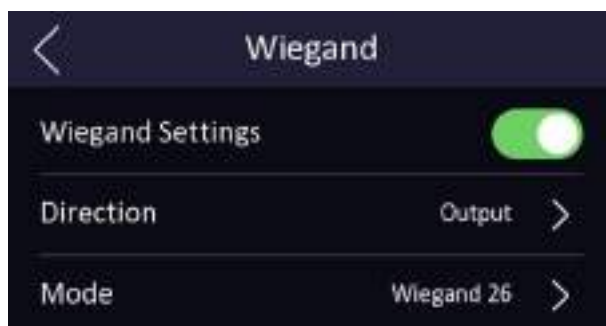


図 6-8 Wiegand の設定

3. Wiegand 機能を有効にします。
4. 通信方向を選択します。
 - 出力: 顔認識端末は、外部のアクセスコントローラに接続できます。また、この 2 つのデバイスは、Wiegand 26 または Wiegand 34 を経由してカード番号を通信します。
 - 入力: 顔認識端末は Wiegand 規格のカードリーダーに接続できます。
5. をタップしてネットワークのパラメータを保存します。

 **メモ**

外部デバイスを変更してデバイスのパラメータを保存すると、そのデバイスは自動的に再起動します。

6.5 ユーザー管理

[ユーザー管理] インターフェースでは、ユーザーを追加、編集、削除、検索できます。

6.5.1 顔画像の追加

ユーザーの顔画像を本デバイスに追加すると、その顔画像を使用して認証できるようになります。

手順

 **メモ**

顔画像を最大 1,500 枚追加できます。

1. 最初のページを 3 秒間長押しし、ジェスチャーにしたがって左右にスライドしてバックエンドにログインします。
 2. [ユーザー] → [+] の順にタップして [ユーザーを追加] ページを開きます。
 3. 従業員 ID を編集します。
-

 **メモ**

- 従業員 ID は 32 文字未満に設定してください。小文字、大文字、数字を組み合わせることができます。
 - 従業員 ID は重複させないでください。
-

4. [名前] フィールドをタップして、ソフトキーボードでユーザー名を入力します。
-

 **メモ**

- ユーザー名には、数字、大文字、小文字、特殊記号を使用できます。
 - ユーザー名の推奨文字数は 32 文字以内です。
-

5. [顔画像] フィールドをタップして顔画像の追加ページを開きます。
-

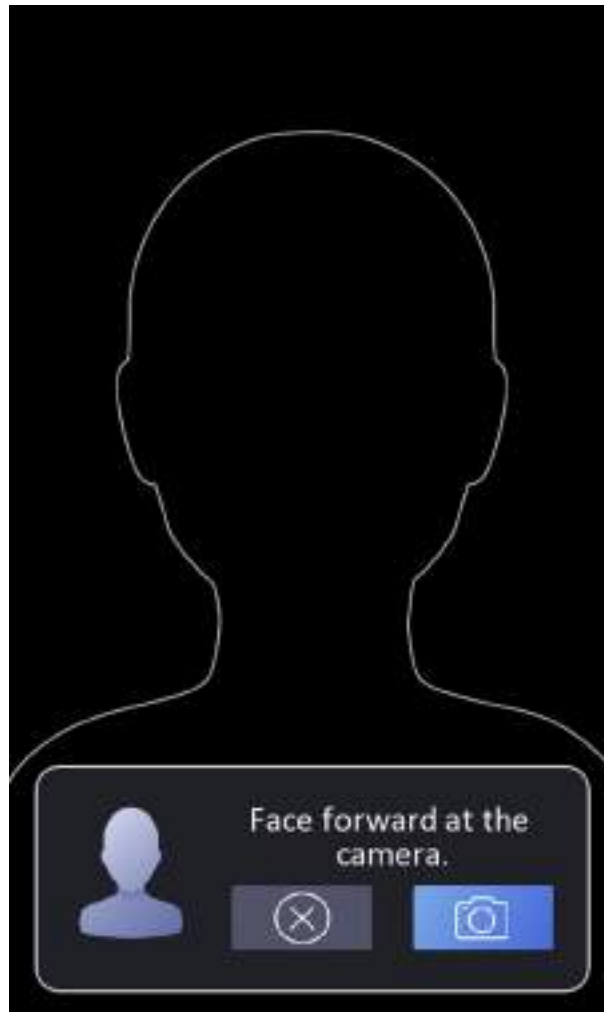


図 6-9 顔画像の追加

6. カメラを見てください。

 **メモ**

- 顔画像の追加時には、顔画像の輪郭に顔が収まっていることを確認してください。
- 撮影した顔画像が良好かつ正確であることを確認してください。
- 顔画像の追加方法の詳細については、「顔画像を取り込む／比較する場合のヒント」をご覧ください。

顔画像の追加が完了すると、取り込んだ顔画像がページの右上に表示されます。

7. **[保存]** をタップして顔画像を保存します。
8. オプション: **[再試行]** をタップすると、顔の位置を調整して顔画像の追加を再度実行することができます。
9. ユーザーロールを設定します。

管理者

ユーザーを管理者として登録します。管理者は、標準の出勤機能のほか、権限の承認後に [ホーム] ページを開いて操作を行うことができます。

一般ユーザー

ユーザーを一般ユーザーとして登録します。このユーザーは、最初のページで認証または出勤確認のみを実行できます。

10. をタップして設定を保存します。

6.5.2 指紋の追加

ユーザーの指紋を追加すると、登録した指紋でユーザーを認証できます。

手順

メモ

- 使用するデバイスがこの機能に対応している必要があります。
 - 最大 1,500 件の指紋を追加できます。
-

1. 最初のページを 3 秒間長押しし、ジェスチャーにしたがって左右にスライドして、デバイスのバックエンドを入力します。
 2. [ユーザー] → [+] の順にタップして [ユーザーを追加] ページを開きます。
 3. [従業員 ID] フィールドをタップして従業員 ID を編集します。
-

メモ

- 従業員 ID は 32 文字未満に設定してください。小文字、大文字、数字を組み合わせることができます。
 - 従業員 ID を 0 から開始することはできず、重複も認められません。
-

4. [名前] フィールドをタップして、ソフトキーボードでユーザー名を入力します。
-

メモ

- ユーザー名には、数字、大文字、小文字、特殊記号を使用できます。
 - ユーザー名の推奨文字数は 32 文字以内です。
-

5. [指紋] フィールドをタップして [指紋登録] ページを開きます。
 6. 指示に従って指紋を追加します。
-

 **メモ**

- 同じ指紋は繰り返し追加できません。
 - ユーザー 1 人に対して最大 10 件の指紋を追加できます。
 - クライアントソフトウェアや指紋レコーダーで指紋を登録することもできます。指紋のスキャン方法の詳細については、「指紋スキャンのヒント」をご覧ください。
-


7. ユーザーロールを設定します。

管理者

ユーザーを管理者として登録します。管理者は、標準の出勤機能のほか、権限の承認後に [ホーム] ページを開いて操作を行うことができます。

一般ユーザー

ユーザーを一般ユーザーとして登録します。このユーザーは、最初のページで認証または出勤確認のみを実行できます。

8.  をタップして設定を保存します。

6.5.3 カードの追加

ユーザーのカードを追加すると、登録したカードでユーザーを認証できます。

手順

 **メモ**

最大 1,500 件のカードを追加できます。

1. 最初のページを 3 秒間長押しし、ジェスチャーにしたがって左右にスライドしてバックエンドにログインします。
 2. [ユーザー] → [+] の順にタップして [ユーザーを追加] ページを開きます。
 3. 配線図に従って、外部のカードリーダーを接続します。
 4. [従業員 ID] フィールドをタップして従業員 ID を編集します。
-

 **メモ**

- 従業員 ID は 32 文字未満に設定してください。小文字、大文字、数字を組み合わせることができます。
 - 従業員 ID は重複させないでください。
-

5. [名前] フィールドをタップして、ソフトキーボードでユーザー名を入力します。

 **メモ**

- ユーザー名には、数字、大文字、小文字、特殊記号を使用できます。
 - ユーザー名の推奨文字数は 32 文字以内です。
-

6. [カード] フィールドをタップし、[+] をタップします。

7. カード番号の設定

手動でカード番号を入力します。カード提示エリアにカードを近づけてカード番号を入力します。

 **メモ**

- カード番号は空白にできません。
 - カード番号には最大 20 文字まで使用できます。
 - カード番号は重複できません。
-

8. カードタイプを設定してください。


9. ユーザーロールを設定します。

管理者

ユーザーを管理者として登録します。管理者は、標準の出勤機能のほか、権限の承認後に [ホーム] ページを開いて操作を行うことができます。

一般ユーザー

ユーザーを一般ユーザーとして登録します。このユーザーは、最初のページで認証または出勤確認のみを実行できます。

10.  をタップして設定を保存します。

6.5.4 パスワードの追加

ユーザーのパスワードを追加すると、登録したパスワードでユーザーを認証できます。

手順

1. 最初のページを 3 秒間長押しし、ジェスチャーにしたがって左右にスライドしてバックエンドにログインします。
 2. [ユーザー] → [+] の順にタップして [ユーザーを追加] ページを開きます。
 3. [従業員 ID] フィールドをタップして従業員 ID を編集します。
-

 **メモ**

- 従業員 ID は 32 文字未満に設定してください。小文字、大文字、数字を組み合わせることができます。
 - 従業員 ID は重複させないでください。
-

4. [名前] フィールドをタップして、ソフトキーボードでユーザー名を入力します。

 **メモ**

- ユーザー名には、数字、大文字、小文字、特殊記号を使用できます。
 - ユーザー名の推奨文字数は 32 文字以内です。
-

5. [パスワード] フィールドをタップしてパスワードを作成し、確認します。

 **メモ**

- このパスワードには数字のみを使用できます。
 - このパスワードには 4~8 桁のみ使用できます。
-


6. ユーザーロールを設定します。

管理者

ユーザーを管理者として登録します。管理者は、標準の出勤機能のほか、権限の承認後に [ホーム] ページを開いて操作を行うことができます。

一般ユーザー

ユーザーを一般ユーザーとして登録します。このユーザーは、最初のページで認証または出勤確認のみを実行できます。

7.  をタップして設定を保存します。

6.5.5 認証モードの設定

ユーザーの顔画像、指紋、パスワードなどの認証情報を追加後に、認証モードの設定が必要です。設定を完了すると、設定済みの認証モードでユーザーを認証できます。

手順


1. 最初のページを 3 秒間長押しし、ジェスチャーにしたがって左右にスライドしてバックエンドにログインします。
2. [ユーザー] → [ユーザーを追加/ユーザーを編集] → [認証モード] をタップします。
3. 認証モードとして [デバイス] または [カスタム] を選択します。

デバイス

デバイスモードを選択する場合、最初に [入退室管理設定] ページで端末の認証モードを設定してください。詳細については、「入退室管理パラメータの設定」をご覧ください。

カスタム



実際の使用状況に応じて、複数の認証モードを組み合わせることができます。

4.  をタップして設定を保存します。
-


6.5.6 ユーザーの検索と編集

ユーザーを追加すると、そのユーザーの検索と編集を行うことができます。

ユーザーの検索

[ユーザー管理] ページで  をタップして [ユーザー検索] ページを開きます。ページ左側の [カード] をタップし、ドロップダウンリストから検索タイプを選択します。検索する従業員 ID、カード番号、またはユーザー名を入力します。 をタップして検索を実行します。

ユーザーの編集

[ユーザー管理] ページでユーザーリストからユーザーを選択し、[ユーザーを編集] ページを開きます。ユーザーのパラメータを編集するには、「ユーザー管理」に記載の手順に従ってください。 をタップして設定を保存します。

メモ

従業員 ID は編集できません。

6.6 データ管理

データの削除、インポート、およびエクスポートを行うことができます。

6.6.1 データの削除

ユーザーデータを削除します。

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

6.6.2 データのインポート

手順

1. デバイスに USB フラッシュドライブを差し込みます。
2. [ホーム] ページで、[データ] → [データのインポート] をタップします。
3. [ユーザーデータ] または [顔データ] をタップすると、選択したデータがデバイスにインポートされます。

 **メモ**

- すべてのユーザー情報のあるデバイス（デバイス A）から別のデバイス（デバイス B）へ転送する場合、まずデバイス A から USB フラッシュドライブへエクスポートし、次に USB フラッシュドライブからデバイス B へインポートします。この場合、プロフィール画像のインポート前にユーザーデータをインポートしておく必要があります。
- 使用できる USB フラッシュドライブの形式は FAT32 です。
- インポートした画像はルートディレクトリ（enroll_pic）に保存し、画像ファイルの名前を以下のルールに従って設定してください。
カード番号_名前_部門_従業員 ID_性別.jpg
- enroll_pic ファイルにインポートしたすべての画像を保存できない場合、ルートディレクトリ内に enroll_pic1、enroll_pic2、enroll_pic3、enroll_pic4 などの名前で別ファイルを作成できます。
- 従業員 ID は 32 文字未満に設定してください。小文字、大文字、数字を組み合わせることができます。重複はできず、0 から始めることもできません。
- 顔画像は以下のルールに従うものとします。カメラをまっすぐに見て、正面から撮影します。顔画像の撮影時には、帽子など頭を覆うものを着用しないでください。ファイル形式は JPEG または JPG です。解像度は 640 × 480 ピクセル以上に設定してください。画像サイズは 60KB～200KB に設定してください。

6.6.3 データのエクスポート

手順

1. [ホーム] ページで、[データ] → [データのエクスポート] をタップします。
2. [イベントデータ]、[ユーザーデータ]、または [顔データ] をタップします。
3. オプション: エクスポート用のパスワードを作成します。これらのデータを別のデバイスにインポートする場合は、パスワードを入力する必要があります。

 **メモ**

- 対応している USB フラッシュドライブの形式は DB です。
- 保存容量が 1G から 32G までの USB フラッシュドライブを使用できます。USB フラッシュドライブの空き領域が 512M 以上あるか確認してください。
- DB 形式のユーザーデータをエクスポートしますが、このデータは編集できません。

6.7 ID 認証

ネットワーク設定、システムパラメータの設定、ユーザー設定を済ませると、最初のページに戻り、ID 認証を実行できます。設定した認証モードに基づいて個人を認証します。1:1 マッチまたは 1:N マッチで ID を認証できます。

1:N マッチ

キャプチャされた顔画像を、デバイス内に保存したすべての顔画像と比較します。

1:1 マッチ

キャプチャされた顔画像を、デバイス内に保存したすべての顔画像と比較します。

6.7.1 単一の認証情報による認証

認証の前にユーザー認証タイプを設定します。詳細については、[認証モードの設定] を参照してください。

顔、指紋、カード、QR コードを認証します。

顔

顔をカメラに向け、顔認証で認証を開始します。

指紋

登録した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

カードを提示エリアに近づけて、認証を開始します。

メモ

通常の IC カードまたは暗号化カードを使用できます。

QR コード

QR コードをデバイスカメラの前に置き、認証を行います。

メモ

使用するデバイスが、QR コードによる認証に対応している必要があります。

認証が完了すると、[認証済] プロンプトがポップアップ表示されます。

6.7.2 複数の認証情報による認証

始める前に

認証の前にユーザー認証タイプを設定します。詳細については、「認証モードの設定」を参照してください。

手順

1. 認証モードが、カードと顔、パスワードと顔、カードとパスワード、カードと顔と指紋の場合は、ライブビューページの指示に従って認証情報を認証します。
-

メモ

- 通常の IC カードまたは暗号化カードを使用できます。
 - QR コードスキャン機能が有効な場合、デバイスカメラの前に QR コードをかざすことで認証が可能です。
-

2. 以前の認証情報が認証されたら、他の認証情報の認証を続行します。
-

メモ

- 指紋スキャンの詳細については、「指紋スキャンのヒント」をご覧ください。
 - 顔認証の詳細については、「顔画像を取り込む／比較する場合のヒント」をご覧ください。
-

認証に成功すると、[認証済] プロンプトがポップアップ表示されます。

6.8 基本設定

ショートカットキー、音声、時間、コミュニティ番号、建物番号、ユニット番号を設定できます。

最初のページを 3 秒間長押しし、ジェスチャーにしたがって左右にスライドして、デバイスのホームページにログインします。[基本] をタップします。

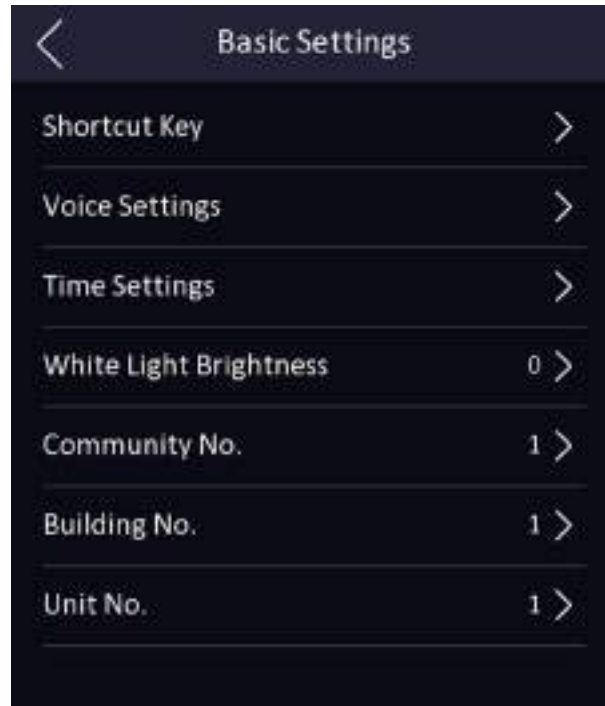


図 6-10 基本設定ページ

ショートカットキー、音声、時間、コミュニティ番号、建物番号、ユニット番号

ショートカットキー

QR コード機能、コール機能、パスワード入力機能など、認証ページに表示されるショートカットキーを選択します。

音声設定

音声プロンプト機能を有効／無効にしたり、音量を調整したりできます。

メモ

音量は 0 から 10 の間で設定できます。

時間設定

タイムゾーン、デバイス時間、DST を設定します。

コミュニティ番号

デバイスを取り付けたコミュニティの番号を設定します。

建物番号

デバイスを取り付けた建物の番号を設定します。

ユニット番号

デバイスを取り付けたユニットの番号を設定します。

6.9 生体認証パラメータの設定

顔のパラメータをカスタマイズして、顔認識のパフォーマンスを向上させることができます。設定可能なパラメータには、アプリケーションモード、顔の活性レベル、顔認識距離、顔認識間隔、ワイドダイナミック、顔 1:N セキュリティレベル、顔 1:1 セキュリティレベル、ECO 設定が含まれます。

最初のページを 3 秒間長押しし、ジェスチャーにしたがって左右にスライドして、ホームページにログインします。[生体認証] をタップします。

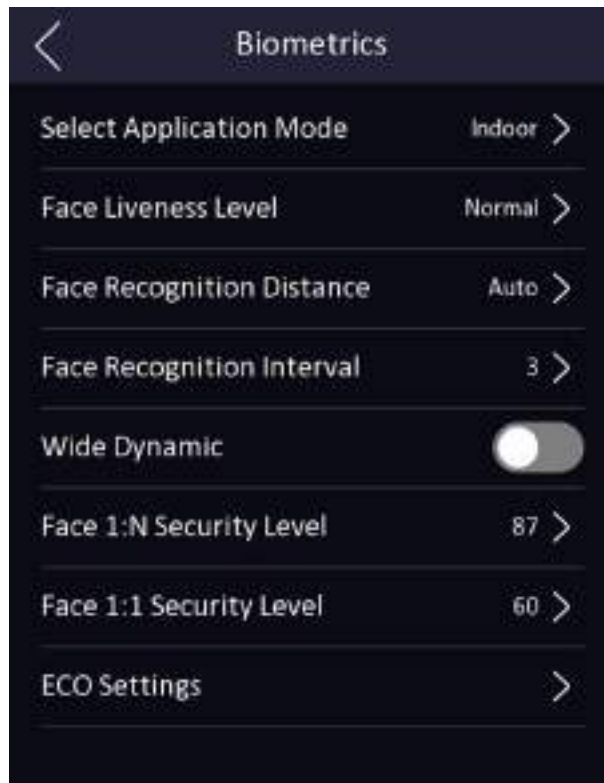




図 6-11 生体認証パラメータページ

表 6-1 顔画像パラメータ

パラメータ	説明
アプリケーションモードを選択	実際の使用状況に応じて [その他] または [屋内] を選択します。
顔の活性レベル	生体顔認証を実行する際に、顔のスプーフィング防止マッチングセキュリティレベルを設定できます。

パラメータ	説明
	 メモ バイオメトリクス認証製品は、アンチスプーフィング環境に完全に適応しているわけではありません。より高いセキュリティレベルが必要な場合は、複数の認証モードを使用してください。
顔認識距離	認証時にユーザーとカメラ間の有効な距離を設定します。
顔認識間隔	認証時における 2 つの連続する顔認識の実行間隔を示します。  メモ 1 から 10 までの数字を入力できます。
ワイドダイナミック	視野内に非常に明るい領域と非常に暗い領域が同時に存在する場合、ワイドダイナミック機能は画像全体の明るさレベルのバランスを取り、細部まで明瞭な画像を提供します。
顔 1:N セキュリティレベル	1:N マッチモードで認証する場合に、認証のしきい値を設定します。値が大きいくほど他人受入率は低下し、本人拒否率は上昇します。
顔 1:1 セキュリティレベル	1:1 マッチモードで認証する場合に、認証のしきい値を設定します。値が大きいくほど他人受入率は低下し、本人拒否率は上昇します。
ECO モード	ECO モードを有効にすると、光が弱かったり暗かったりする状態でも、IR カメラで顔認証を実行できます。また、ECO モードのしきい値、ECO モード (1:N)、ECO モード (1:1) を設定できます。
ECO しきい値	ECO モードを有効にすると、ECO モードのしきい値を設定できます。値が大きいくほど、ECO モードを起動しやすくなります。
ECO モード (1:N)	ECO モードの 1:N マッチモードで認証する場合に、マッチのしきい値を設定します。値が大きいくほど他人受入率は低下し、本人拒否率は上昇します。
ECO モード (1:1)	ECO モードの 1:1 マッチモードで認証する場合にマッチのしきい値を設定します。値が大きいくほど他人受入率は低下し、本人拒否率は上昇します。

6.10 入退室管理パラメータの設定

認証モードの機能、NFC カードの有効化、ドアの接触装置、ドアのオープン時間など、入退室管理の権限を設定できます。

ホームページで [ACS]（入退室管理設定）をタップして [入退室管理設定] ページを開きます。このページで入退室管理パラメータを編集します。



図 6-12 入退室管理パラメータ

利用可能なパラメータの説明は以下のとおりです。

表 6-2 入退室管理パラメータの説明

パラメータ	説明
端末認証モード	<p>顔認識端末の認証モードを選択します。この認証モードはカスタマイズできます。</p> <hr/> <p>メモ</p> <ul style="list-style-type: none"> 指紋関連の機能を使用できるのは、指紋モジュールを搭載するデバイスのみです。 バイオメトリクス認証製品は、アンチスプーフィング環境に完全に適応しているわけではありません。より高いセキュリティレベルが必要な場合は、複数の認証モードを使用してください。 複数の認証モードを採用する場合は、顔認証を行う前に他の認証方法を使用する必要があります。

パラメータ	説明
リーダー認証モード（カードリーダー認証モード）	カードリーダーの認証モードを選択します。
NFC カードの有効化	この機能を有効にすると、NFC カードで認証できるようになります。
ドアの接触装置	実際の使用状況に応じて、[開放（開放状態）] または [閉鎖（閉鎖状態）] を選択できます。デフォルトでは [閉鎖（閉鎖状態）] に設定されています。
開放継続時間	ドアロック解除の継続時間を設定します。設定した時間内にドアが開かれなかった場合、ドアはロックされます。設定可能な施錠時間: 1~255 秒。

6.11 時間および出勤状態の設定

時間および出勤状態を設定します。実際の状況に応じて、出勤モードをチェックイン、チェックアウト、休憩開始、休憩終了、残業開始、残業終了に設定できます。

メモ

この機能を使用するには、クライアントソフトウェアの時間および出勤機能との連携が必要です。

6.11.1 デバイスによる出勤モードの無効化

出勤モードを無効にすると、最初のページに出勤状態が表示されなくなります。**[T&A 状態]** をタップして **[T&A 状態]** ページを開きます。

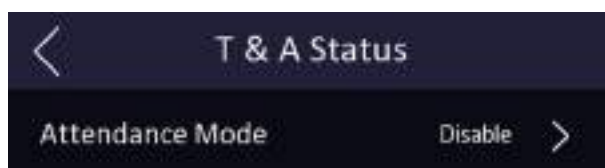


図 6-13 出勤モードの無効化

[出勤モード] を **[無効]** に設定します。

最初のページに出勤状態は表示されず、設定もできなくなります。システムは、このプラットフォームで設定した出勤ルールに従って動作します。

6.11.2 デバイスによる出勤モードの手動設定

出勤モードを手動設定にすると、出勤の記録時に手動で状態を選択できます。

始める前に

少なくともユーザーを 1 名追加し、そのユーザーの認証モードを設定してください。詳細については、「ユーザー管理」をご覧ください。

手順

- 1.[T&A 状態] をタップして [T&A 状態] ページを開きます。
- 2.[出勤モード] を [手動] に設定します。

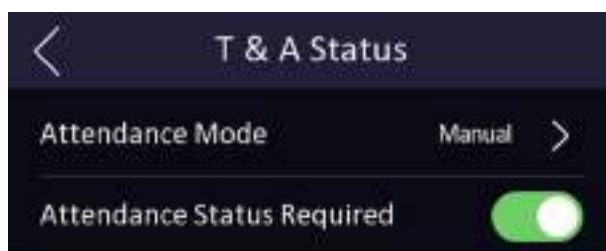


図 6-14 出勤モードの手動設定

- 3.[出勤状態] 機能を有効にします。

結果

認証後に出勤状態を手動で選択することになります。

メモ

状態を選択しなかった場合は認証に失敗し、有効な出勤として記録されません。

6.11.3 デバイスによる出勤モードの自動設定

出勤モードを [自動] に設定すると、出勤状態および利用可能なスケジュールを設定できます。設定したパラメータに基づいて、出勤状態が自動的に変更されます。

始める前に

少なくともユーザーを 1 名追加し、そのユーザーの認証モードを設定してください。詳細については、「ユーザー管理」をご覧ください。

手順

- 1.[T&A 状態] をタップして [T&A 状態] ページを開きます。
- 2.[出勤モード] を [自動] に設定します。

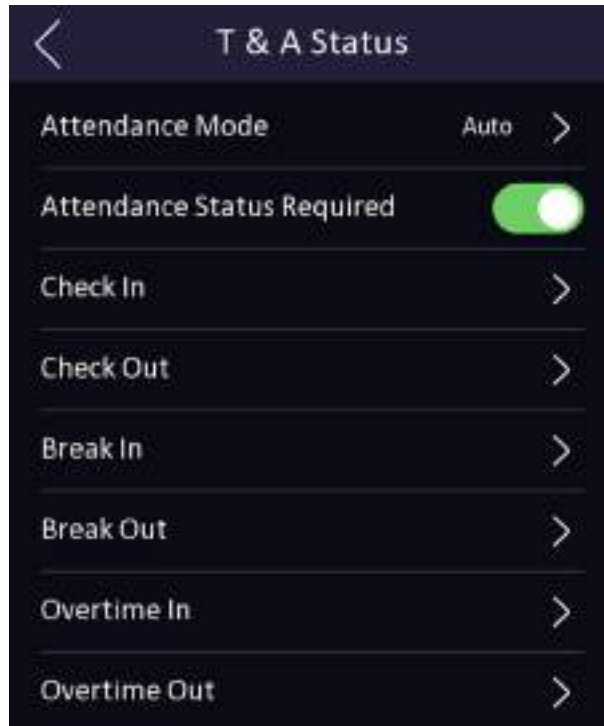


図 6-15 出勤モードの自動設定

3. 出勤状態とそのスケジュールを選択します。

- 1) 出勤状態として、[チェックイン]、[チェックアウト]、[休憩開始]、[休憩終了]、[残業開始]、または [残業終了] を選択します。
- 2) [スケジュール] をタップします。
- 3) [月曜日]、[火曜日]、[水曜日]、[木曜日]、[金曜日]、[土曜日]、[日曜日] のいずれかを選択します。
- 4) 選択した日付をタップして、選択した出勤状態の開始時間を設定します。
- 5) [確認] をタップします。
- 6) 実際の必要性に従ってステップ 1 から 5 を繰り返します。

メモ

出勤状態は設定したスケジュールの範囲内で有効になります。

結果

最初のページで認証を行うと、その認証は設定したスケジュールに従って、設定済みの出勤状態として記録されます。

例

[Break Out Schedule (休憩開始スケジュール)] を月曜日 11:00、[Break In Schedule (休憩終了スケジュール)] を月曜日 12:00 に設定すると、ユーザー認証に成功した場合に月曜日の 11:00~12:00 は休憩時間として記録されます。

6.11.4 デバイスによる出勤モードの手動および自動設定

出勤モードを [手動および自動] に設定すると、設定したパラメータに従って出勤状態が自動的に変更されます。また、認証後に出勤状態を手動で変更することもできます。

始める前に

少なくともユーザーを 1 名追加し、そのユーザーの認証モードを設定してください。詳細については、「ユーザー管理」をご覧ください。

手順

1. [T&A 状態] をタップして [T&A 状態] ページを開きます。
2. [出勤モード] を [手動および自動] に設定します。

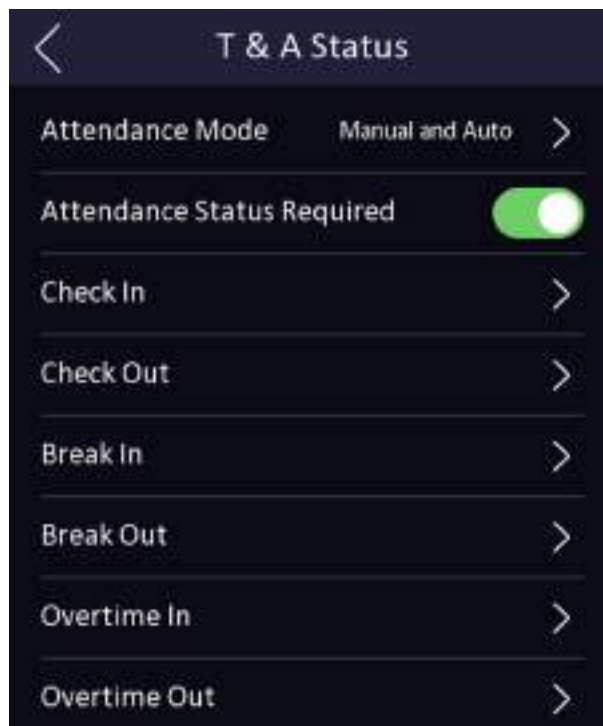


図 6-16 手動および自動モード

3. 出勤状態とそのスケジュールを選択します。
 - 1) 出勤状態として、[チェックイン]、[チェックアウト]、[休憩開始]、[休憩終了]、[残業開始]、または [残業終了] を選択します。
 - 2) [スケジュール] をタップします。
 - 3) [月曜日]、[火曜日]、[水曜日]、[木曜日]、[金曜日]、[土曜日]、[日曜日] のいずれかを選択します。
 - 4) 選択した日付をタップして、選択した出勤状態の開始時間を設定します。
 - 5) [確認] をタップします。
 - 6) 実際の必要性に従ってステップ 1 から 5 を繰り返します。

 **メモ**

出勤状態は設定したスケジュールの範囲内で有効になります。

結果

最初のページで認証を行います。状態を選択しなかった場合、その認証はスケジュールに従って、設定済みの出勤状態として記録されます。[Select Status (状態を選択)] をタップして出勤を記録すると、その認証は選択済みの出勤状態として記録されます。

例

[Break Out Schedule (休憩開始スケジュール)] を月曜日 11:00、[Break In Schedule (休憩終了スケジュール)] を月曜日 12:00 に設定すると、ユーザー認証に成功した場合に月曜日の 11:00~12:00 は休憩時間として記録されます。

6.12 システムメンテナンス

システム情報と容量を表示できます。また、デバイスのアップグレード、工場出荷時設定への復元、およびデフォルト設定への復元を行うこともできます。最初のページを 3 秒間長押しし、ジェスチャーにしたがって左右にスライドして、ホームページにログインします。[メンテナンス] をタップします。



図 6-17 メンテナンスページ

システム情報

デバイスモデル、シリアル番号、バージョン、アドレス、プロダクションデータ、QRコード、およびオープンソースコードライセンスを表示できます。

メモ

デバイスのモデルによって表示されるページは異なります。詳細については実際のページを参照してください。

容量

ユーザー、顔画像、カード、イベント、指紋の数を表示できます。

メモ

デバイスモデルの一部では、指紋番号の表示がサポートされています。詳細については実際のページを参照してください。

デバイスアップグレード

デバイスの USB インターフェイスに USB フラッシュドライブを差し込みます。[アップグレード] をタップすると、デバイスは USB フラッシュドライブの `digicap.dav` ファイルを読み取り、アップグレードを開始します。

デフォルト設定への復元

通信設定以外のすべてのパラメータは、リモートでインポートされたユーザー情報を除き、デフォルト設定に復元されます。システムが再起動して有効になります。

工場出荷時設定への復元

すべてのパラメータが工場出荷時の設定に復元されます。システムが再起動して有効になります。

6.13 ビデオインターコム

デバイスをクライアントソフトウェアに追加した後は、クライアントソフトウェアからのデバイスへの呼び出し、デバイスからマスターステーションへの呼び出し、デバイスからクライアントソフトウェアへの呼び出し、デバイスから屋内ステーションへの呼び出しが可能になります。

6.13.1 デバイスからクライアントソフトウェアの呼び出し

手順

1. 付属ディスクから、または公式 Web サイトからクライアントソフトウェアを入手し、プロンプトに従ってソフトウェアをインストールします。
2. クライアントソフトウェアを実行すると、ソフトウェアのコントロールパネルがポップアップ表示されます。
3. [デバイス管理] をクリックして [デバイス管理] インターフェイスを開きます。
4. クライアントソフトウェアにデバイスを追加します。

 **メモ**

デバイスの追加方法の詳細については、「**デバイスの追加**」をご覧ください。

5. クライアントソフトウェアを呼び出します。
 - 1) デバイスの最初のページで **[コール]** をタップします。
 - 2) ポップアップウィンドウで **「0」** を入力します。
 - 3) **[コール]** をタップしてクライアントソフトウェアを呼び出します。
 6. クライアントソフトウェアのポップアップページで **[Answer (応答)]** をタップすると、デバイスとクライアントソフトウェア間で 2 ウェイオーディオを開始できます。
-

 **メモ**

デバイスを複数のクライアントソフトウェアに追加した状態でデバイスからクライアントソフトウェアを呼び出すと、デバイスに最初に追加したクライアントソフトウェアのみに着信ウィンドウがポップアップされます。

6.13.2 デバイスからセンターの呼び出し

手順

1. 付属ディスクから、または公式 Web サイトからクライアントソフトウェアを入手し、プロンプトに従ってソフトウェアをインストールします。
 2. クライアントソフトウェアを実行すると、ソフトウェアのコントロールパネルがポップアップ表示されます。
 3. **[デバイス管理]** をクリックして **[デバイス管理]** インターフェースを開きます。
 4. クライアントソフトウェアにマスターステーションとデバイスを追加します。
-


 **メモ**

デバイスの追加方法の詳細については、「**デバイスの追加**」をご覧ください。

5. リモート設定ページでマスターステーションの IP アドレスと SIP アドレスを設定します。
-

 **メモ**

操作の詳細については、マスターステーションのユーザーマニュアルをご覧ください。

6. センターを呼び出します。
 - **[基本設定]** でセンターを呼び出すよう設定した場合は、 をタップしてセンターを呼び出すことができます。
-

- [基本設定] でセンターを呼び出すよう設定していない場合は、 →  をタップしてセンターを呼び出す必要があります。

7. マスターステーションで呼び出しに応答し、2 ウェイオーディオを開始します。

メモ

デバイスはマスターステーションを優先的に呼び出します。

6.13.3 クライアントソフトウェアからデバイスの呼び出し

手順

1. 付属ディスクから、または公式 Web サイトからクライアントソフトウェアを入手し、プロンプトに従ってソフトウェアをインストールします。
 2. クライアントソフトウェアを実行すると、ソフトウェアのコントロールパネルがポップアップ表示されます。
 3. [デバイス管理] をクリックして [デバイス管理] ページを開きます。
 4. クライアントソフトウェアにデバイスを追加します。
-

メモ

デバイスの追加方法の詳細については、「[デバイスの追加](#)」をご覧ください。

5. [ライブビュー] ページを開き、追加したデバイスをダブルクリックしてライブビューを開始します。
-

メモ

[ライブビュー] ページの操作の詳細については、クライアントソフトウェアのユーザーマニュアルに記載の「[ライブビュー](#)」をご覧ください。

6. ライブビュー画像を右クリックして右クリックメニューを開きます。
 7. [2 ウェイオーディオを開始] をクリックして、デバイスとクライアントソフトウェア間で 2 ウェイオーディオを開始します。
-

6.13.4 デバイスから部屋の呼び出し




手順

1. 付属ディスクから、または公式 Web サイトからクライアントソフトウェアを入手し、プロンプトに従ってインストールします。
 2. クライアントソフトウェアを実行すると、ソフトウェアのコントロールパネルがポップアップ表示されます。
 3. [デバイス管理] をクリックして [デバイス管理] インターフェースを開きます。
-

4. クライアントソフトウェアに屋内ステーションとデバイスを追加します。
-

 **メモ**

デバイスの追加方法の詳細については、「**デバイスの追加**」をご覧ください。

5. ユーザーを屋内ステーションに関連付けて、屋内ステーションの部屋番号を設定します。
6. 部屋を呼び出します。
- **[基本設定]** で部屋番号を指定している場合は、 をタップしてその部屋を呼び出すことができます。
- [基本設定]** で部屋番号を指定していない場合は、デバイスの認証ページの  をタップする必要があります。ダイヤルページで部屋番号を入力し、 をタップして部屋を呼び出します。
7. 屋内ステーションが呼び出しに応答した後、屋内ステーションと 2 ウェイオーディオを開始できます。

第 7 章 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を介してログインできます。




デバイスがアクティベートされていることを確認します。アクティブ化の詳細については、「アクティブ化」を参照してください。

Web ブラウザによるログイン

Web 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を開きます。

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] をクリックします。

クライアントソフトウェアのリモート設定によるログイン

クライアントソフトウェアをダウンロードして開きます。デバイスを追加したら、 をクリックして [ライブビュー] ページを開きます。

7.2 ライブビュー

デバイスのライブビデオを表示できます。

ログインすると、[ライブビュー] ページが表示されます。ライブビュー、キャプチャ、ビデオ録画、およびその他の操作を実行できます。



図 7-1 ライブビューページ

機能説明:



ライブビューの開始時に画像サイズを選択します。



ライブビューの開始時に音量を設定します。

メモ

2 ウェイオーディオの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。



ライブビューの開始時に画像をキャプチャできます。



予約された機能。ライブビュー画像を拡大できます。



リンクされたドアをロック解除します。



ライブビューを開始または停止します。



ビデオ録画を開始または停止します。



ライブビュー開始時にストリームタイプを選択します。メインストリームとサブストリームから選択できます。



ウィンドウ分割タイプを選択し、ライブビューを開始します。



全画面表示になります。

7.3 人物管理

人物の情報（基本情報、カード、認証モードなど）をクリックして追加し、**[OK]** をクリックして設定を保存します。

基本情報の追加

[ユーザー] → **[追加]** の順にクリックして **[関係者を追加]** ページを開きます。従業員 ID、名前、性別、ユーザーロールなどの人物の基本情報を追加します。**[保存]** をクリックして設定を保存します。

カードの追加

[ユーザー] → **[追加]** の順にクリックして **[関係者を追加]** ページを開きます。**[カードを追加]** をクリックして、カード番号を入力します。**[保存]** をクリックして設定を保存します。

顔画像の追加

[ユーザー] → **[追加]** の順にクリックして **[関係者を追加]** ページを開きます。右側の **[+]** をクリックして、ローカル PC から顔画像をアップロードします。



メモ

画像形式は JPEG で、サイズは 200K 未満である必要があります。

[保存] をクリックして設定を保存します。

認証モードの追加

[ユーザー] → **[追加]** の順にクリックして **[関係者を追加]** ページを開きます。認証モードを設定します。**[保存]** をクリックして設定を保存します。

7.4 イベントの検索

[検索] をクリックして検索ページを開きます。



The image shows a search form with the following fields:

- Employee ID:
- Name:
- Card No.:
- Start Time:
- End Time:

At the bottom of the form is a red button labeled "Search".

図 7-2 検索ページ

従業員 ID、名前、カード番号、開始時間、終了時間などの検索条件を入力し、**[検索]** をクリックします。
検索結果が右側の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

デバイス番号、モデル、シリアル番号、バージョン、デバイス容量などを表示します。
[設定] → **[システム]** → **[システム設定]** → **[基本情報]** をクリックして、設定ページを開きます。
デバイス番号、モデル、シリアル番号、バージョン、デバイス容量などを表示できます。

7.5.2 時間の設定

デバイスのタイムゾーン、同期モード、およびデバイス時間を設定します。
[設定] → **[システム]** → **[システム設定]** → **[時間設定]** をクリックします。



図 7-3 時間設定

設定後は **[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、デバイスが位置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、デバイス時間は手動で同期する必要があります。デバイス時間を手動で設定するか、**[コンピュータの時間と同期]** をオンにして、デバイス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。

7.5.3 RS-485 パラメータの設定

周辺機器、アドレス、ボーレート、出力タイプなどの RS-485 パラメータを設定できます。**[設定]** → **[システム]** → **[システム設定]** → **[RS-485 設定]** をクリックします。



図 7-4 RS-485 ページ

設定後は **[保存]** をクリック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ます。**[カードリーダー]**、**[拡張モジュール]**、**[アクセスコントローラ]**、**[無効化]** から選択できます。

メモ

周辺機器を変更して保存すると、デバイスは自動的に再起動します。

RS-485 アドレス

実際の状況に合わせて RS-485 アドレスを設定します。

メモ

アクセスコントローラを選択した場合: RS-485 インタフェースを介してデバイスを端末に接続する場合は、RS-485 アドレスを 2 に設定します。デバイスをコントローラに接続する場合は、ドア番号に従って RS-485 アドレスを設定します。

ボーレート

デバイスが RS-485 プロトコルを介して通信しているときのボーレート。

出力タイプ

周辺機器タイプとして [アクセスコントローラ] を選択した場合は、パラメータを設定する必要があります。デバイスは、カード番号または従業員 ID をアクセスコントローラに出力します。

7.5.4 Wiegand パラメータの設定

Wiegand の通信方向を設定できます。

手順

1. [設定] → [システム] → [システム設定] → [Wiegand Settings (Wiegand 設定)] をクリックします。

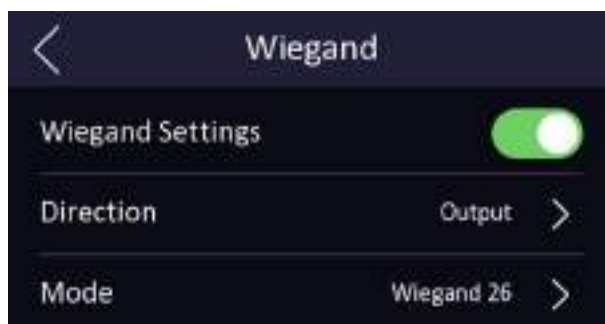


図 7-5 Wiegand ページ

2. [Wiegand] にチェックを入れて Wiegand 機能を有効化します。
3. 通信方向を設定します。

入力

デバイスは Wiegand カードリーダーに接続できます。

出力

デバイスを外部のアクセスコントローラに接続できます。また、この 2 つのデバイスは、Wiegand 26 または Wiegand 34 を経由してカード番号を通信します。

4. [保存] をクリックして設定を保存します。

 **メモ**

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

7.5.5 DST の設定

手順

1. [設定] → [システム] → [システム設定] → [DST] をクリックします。



図 7-6 DST ページ

2. [DST を有効化] にチェックを入れます。
3. DST 開始時間、終了時間、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。

7.5.6 アップグレードとメンテナンス

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

デバイスの再起動

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



図 7-7 アップグレードとメンテナンスページ

[再起動] をクリックしてデバイスの再起動を開始します。

パラメータの復元

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

工場

すべてのパラメータが工場出荷時の設定に復元されます。使用前にデバイスをアクティベートする必要があります。

デフォルト

デバイスの IP アドレスとユーザー情報を除き、デバイスはデフォルト設定に戻ります。

パラメータのインポートとエクスポート

[設定] → [システム] → [メンテナンス] → [アップグレードとメンテナンス] 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、ログまたはデバイスパラメータをエクスポートします。

メモ


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

 をクリックして、インポートするファイルを選択してください。[インポート] 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。

アップグレード

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

ドロップダウンリストから、アップグレードのタイプを選択します。 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、アップグレードを開始します。


メモ

アップグレード中は電源を切らないでください。

7.5.7 管理者パスワードの変更

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. 旧パスワードを入力したら、新しいパスワードを作成します。
4. 新しいパスワードを確認します。
5. **[OK]** をクリックします。

注意

デバイスのパスワードの強度は、自動的に確認することができます。デバイスのセキュリティを高めるため、ご自身で作成した強力なパスワード（大文字、小文字、数字、特殊記号のうち、少なくとも 3 つのカテゴリで構成される文字を含む 8 文字以上のパスワード）を設定することを強く推奨します。また、定期的にパスワードを変更することを推奨します。特にセキュリティ要件の高いシステムでは、毎月または毎週パスワードを変更すると、より安全にデバイスを保護できます。パスワードなどのセキュリティ設定はすべて、設置者／エンドユーザーの責任で適切に行ってください。

7.5.8 ネットワークパラメータの基本設定

TCP/IP パラメータを設定

[設定] → **[ネットワーク]** → **[基本設定]** → **[TCP/IP]** をクリックします。



図 7-8 TCP/IP 設定ページ

[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、MTU、およびデバイスポートを設定する必要があります。この機能をチェックすると、IPv4 アドレス、IPv4 サブネットマスク、および IPv4 デフォルトゲートウェイが自動的に割り当てられます。

DNS サーバー

実際の必要性に応じて、メイン DNS サーバーとサブ DNS サーバーを設定します。

7.5.9 EHome パラメータの設定

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

手順

メモ

使用するデバイスがこの機能に対応している必要があります。

1. [設定] → [ネットワーク] → [詳細設定] → [プラットフォーム] をクリックします。
2. プラットフォームアクセスモードドロップダウンリストから [EHome] を選択します。
3. [有効] にチェックを入れます。
4. EHome バージョン、サーバーアドレス、デバイス ID、および EHome の状態を設定します。

メモ

バージョンとして 4.0 を選択した場合は、EHome キーも設定する必要があります。

5. [保存] をクリックします。

7.5.10 ビデオとオーディオのパラメータの設定

画質、解像度、およびデバイス音量を設定します。

ビデオパラメータの設定

[設定] → [ビデオ/オーディオ] → [ビデオ] の順にクリックします。



図 7-9 ビデオ設定ページ

ストリームタイプ、ビデオタイプ、ビットレートタイプ、フレームレート、最大ビットレートを設定します。

設定後は **[保存]** をクリックして設定を保存します。

オーディオパラメータの設定

[設定] → **[ビデオ/オーディオ]** → **[オーディオ]** の順にクリックします。

ブロックをドラッグして、デバイスの出力ボリュームを調整します。

設定後は **[保存]** をクリックして設定を保存します。

7.5.11 オーディオコンテンツのカスタマイズ

認証に成功した場合と失敗した場合それぞれの出力オーディオコンテンツをカスタマイズします。

手順

1. **[設定]** → **[ビデオ/オーディオ]** → **[オーディオプロンプト]** の順にクリックします。

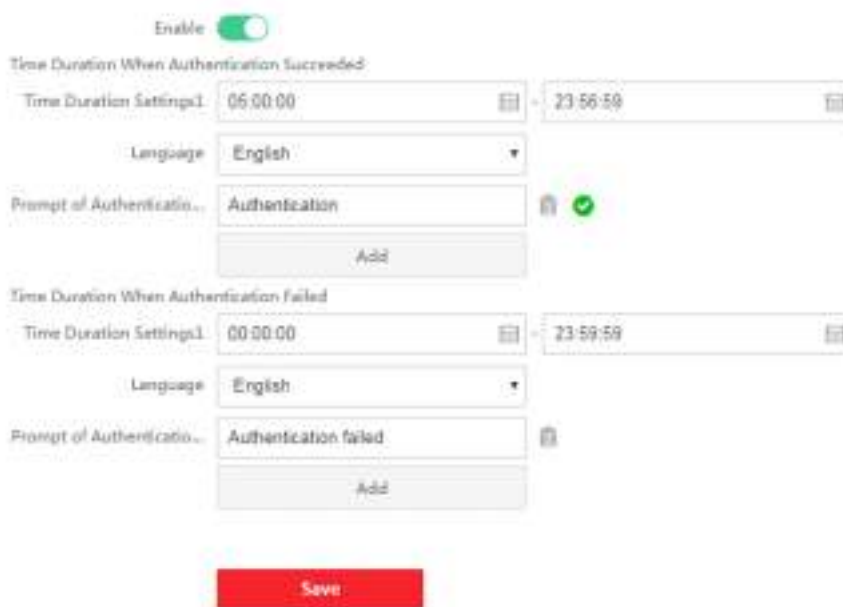



図 7-10 オーディオコンテンツのカスタマイズ

2. 機能を有効にします。
3. 認証が成功した場合の継続時間を設定します。
 - 1) **[追加]** をクリックします。
 - 2) 継続時間と言語を設定します。


 **メモ**

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

- 3) オーディオコンテンツを入力します。
 - 4) オプション: サブステップ 1~3 を繰り返します。
 - 5) オプション:  をクリックして、設定された継続時間を削除します。
4. 認証に失敗した場合の継続時間を設定します。
- 1) **[追加]** をクリックします。
 - 2) 継続時間と言語を設定します。

 **メモ**

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

- 3) オーディオコンテンツを入力します。
 - 4) オプション: サブステップ 1~3 を繰り返します。
 - 5) オプション:  をクリックして、設定された継続時間を削除します。
5. **[保存]** をクリックして設定を保存します。

7.5.12 ビデオインターコムパラメータの設定

デバイスは、ドアステーションまたは外側ドアステーションとして使用できます。使用する前に、デバイス番号を設定する必要があります。

デバイス番号の設定

[設定] → **[ビデオインターコム]** → **[デバイス番号]** をクリックします。



Device Type	Door Station
Community No.	1
Building No.	1
Unit No.	1
Floor No.	1

Save

図 7-11 デバイス番号の設定

設定後は **[保存]** をクリックして設定を保存します。

デバイスタイプ

デバイスは、ドアステーションまたは外側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ます。

コミュニティ番号

デバイスを取り付けたコミュニティの番号を設定します。

建物番号

デバイスを取り付けた建物の番号を設定します。

ユニット番号

デバイスを取り付けたユニットの番号を設定します。

フロア番号

デバイスを取り付けたフロアの番号を設定します。

番号

デバイスタイプとして [外側ドアステーション] を選択した場合は、1~99 の数値を入力する必要があります。

メモ

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。

リンクされたネットワーク設定の設定

[設定] → [ビデオインターコム] → [リンクされたネットワーク設定] の順にクリックします。

デバイスタイプ、SIP サーバーの IP アドレス、およびマスターステーションの IP アドレスを設定できます。

これらのパラメータを設定すると、入退室管理デバイス、ドアステーション、屋内ステーション、マスターステーション、プラットフォームの間で通信できるようになります。

設定後は [保存] をクリックして設定を保存します。

7.5.13 入退室管理および認証パラメータの設定

入退室管理パラメータと認証パラメータを設定します。

ドアパラメータの設定

[設定] → [入退室管理] → [ドアパラメータ] の順にクリックします。



図 7-12 ドアパラメータ設定ページ

設定後は [保存] をクリックして設定を保存します。

ドアの接触装置

実際の状況に応じて、[開放状態] または [閉鎖状態] を選択できます。デフォルトでは [閉鎖状態] に設定されています。

開放継続時間

ドアロック解除の継続時間を設定します。設定した時間内にドアが開かれなかった場合、ドアはロックされます。

ドア開放時間超過アラーム

設定した時間内にドアが閉鎖しない場合、アラームが作動します。

認証パラメータの設定

[設定] → [入退室管理] → [認証設定] の順にクリックします。



図 7-13 認証パラメータの設定

設定後は [保存] をクリックして設定を保存します。

認証

実際の使用状況に応じて、ドロップダウンリストから認証モードを選択します。

以下で結果を表示

[顔画像]、[名前]、または [従業員 ID] にチェックを入れます。認証が完了すると、選択したコンテンツが結果に表示されます。

最小認識間隔

同じカードをかざす間隔が設定値より短い場合、カードをかざした行為は無効になります。

7.5.14 画像パラメータの設定

ビデオ標準、WDR、輝度、コントラスト、彩度、および鮮明度を設定します。

手順

1. [設定] → [画像] をクリックします。

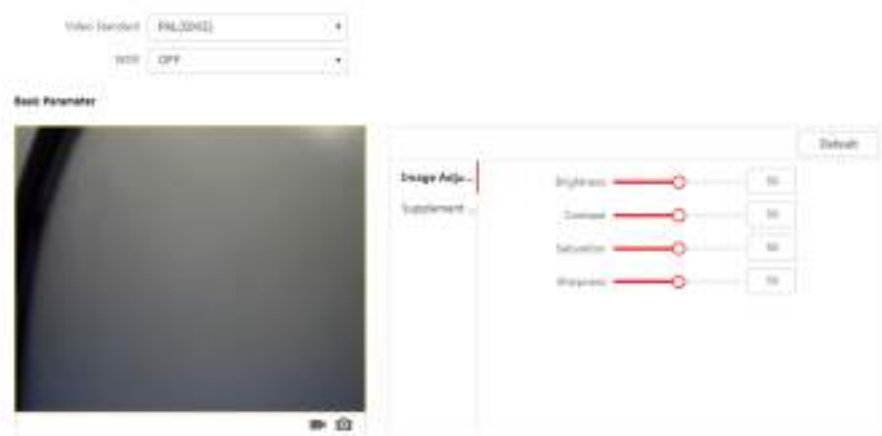


図 7-14 画像設定ページ

2. パラメータを設定して画像を調整します。

ビデオ標準

ライブビューをリモートで実行する場合は、ビデオフレームレートを設定します。標準を変更したら、デバイスを再起動して有効に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適しています。

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。

WDR

WDR 機能を有効化または無効化できます。

視野内に非常に明るい領域と非常に暗い領域が同時に存在する場合、WDR 機能は画像全体の明るさレベルのバランスを取り、細部まで明瞭な画像を提供します。

輝度/コントラスト/彩度/鮮明度

ブロックをドラッグするか値を入力して、ライブビデオの明るさ、コントラスト、彩度、鮮明度を調整します。



ビデオの録画を開始または終了します。



画像をキャプチャします。

7.5.15 補助光輝度の設定

デバイスの補助光輝度を設定します。

手順

1. [設定] → [画像] をクリックします。



図 7-15 補助光設定ページ

2. 基本パラメータパネルで [補助光輝度] をクリックします。
3. ドロップダウンリストから補助光のタイプとモードを選択します。モードを [オン] にした場合は、輝度を設定する必要があります。
4. オプション: [デフォルト] をクリックして、パラメータをデフォルト設定に戻します。

7.5.16 顔パラメータの設定

基本パラメータの設定

- [設定] → [スマート] → [スマート] をクリックします。



図 7-16 スマート設定ページ

設定後は [保存] をクリックして設定を保存します。

顔アンチスプーフィング

生体顔検知機能を有効または無効にします。この機能を有効にすると、認証対象が人間であるかどうかを識別できます。

メモ

バイオメトリクス認証製品は、アンチスプーフィング環境に完全に適応しているわけではありません。より高いセキュリティレベルが必要な場合は、複数の認証モードを使用してください。

生体顔検知セキュリティレベル

[顔アンチスプーフィング] 機能を有効にすると、生体顔認証の実行時に作動する認証セキュリティのレベルを設定できます。

顔認識距離

認証ユーザーとデバイスカメラ間の距離を選択します。

アプリケーションモード

実際の使用状況に応じて [その他] または [屋内] を選択します。

連続する顔認識間隔

認証時における 2 つの連続する顔認識の実行間隔を設定します。

ピッチアングル

顔認証の開始時の最大ピッチアングルを示します。

ヨーアングル

顔認証の開始時の最大ヨーアングルを示します。

顔 1:1 マッチしきい値

1:1 マッチモードで認証する場合に、認証のしきい値を設定します。値が大きいほど他人受入率は低下し、本人拒否率は上昇します。

顔 1:N マッチしきい値

1:N マッチモードで認証する場合に、認証のしきい値を設定します。値が大きいほど他人受入率は低下し、本人拒否率は上昇します。

ECO モード

ECO モードを有効にすると、光が弱かったり暗かったりする状態でも、IR カメラで顔認証を実行できます。また、ECO モードのしきい値、ECO モード (1:N)、ECO モード (1:1) を設定できます。

ECO モード (1:1)

ECO モードの 1:1 マッチモードで認証する場合にマッチのしきい値を設定します。値が大きいほど他人受入率は低下し、本人拒否率は上昇します。

ECO モード (1:N)

ECO モードの 1:N マッチモードで認証する場合に、マッチのしきい値を設定します。値が大きいほど他人受入率は低下し、本人拒否率は上昇します。

指紋セキュリティレベル

指紋のセキュリティレベルを選択します。

セキュリティレベルが高いほど、他人受入率 (FAR) は低下します。



セキュリティレベルが高いほど、本人拒否率 (FRR) は上昇します。

認識エリアを設定

[設定] → [スマート] → [エリア設定] をクリックします。

ライブビデオの黄色のフレームをドラッグして、認識エリアを調整します。エリア内の顔のみがシステムによって認識されます。

[保存] をクリックして設定を保存します。

 または  をクリックして、ビデオの録画または画像のキャプチャを行います。

7.5.17 通知書の設定

デバイスのスクリーンセーバーとスリープ時間を設定できます。
[設定] → [Notice Publication (通知書)] をクリックします。



図 7-17 通知ページ

スリープ

[スリープ] を有効にすると、設定されたスリープ時間で何も操作が行われない場合、デバイスはスリープモードに入ります。

スクリーンセーバーのカスタマイズ

この機能を有効にすると、ローカル PC からスクリーンセーバーの画像をアップロードできます。スクリーンセーバーのスライドショー間隔を設定することもできます。

第 8 章 クライアントソフトウェアの設定

8.1 クライアントソフトウェアの設定フロー

クライアントソフトウェアで設定を行うには、次のフロー図に従ってください。

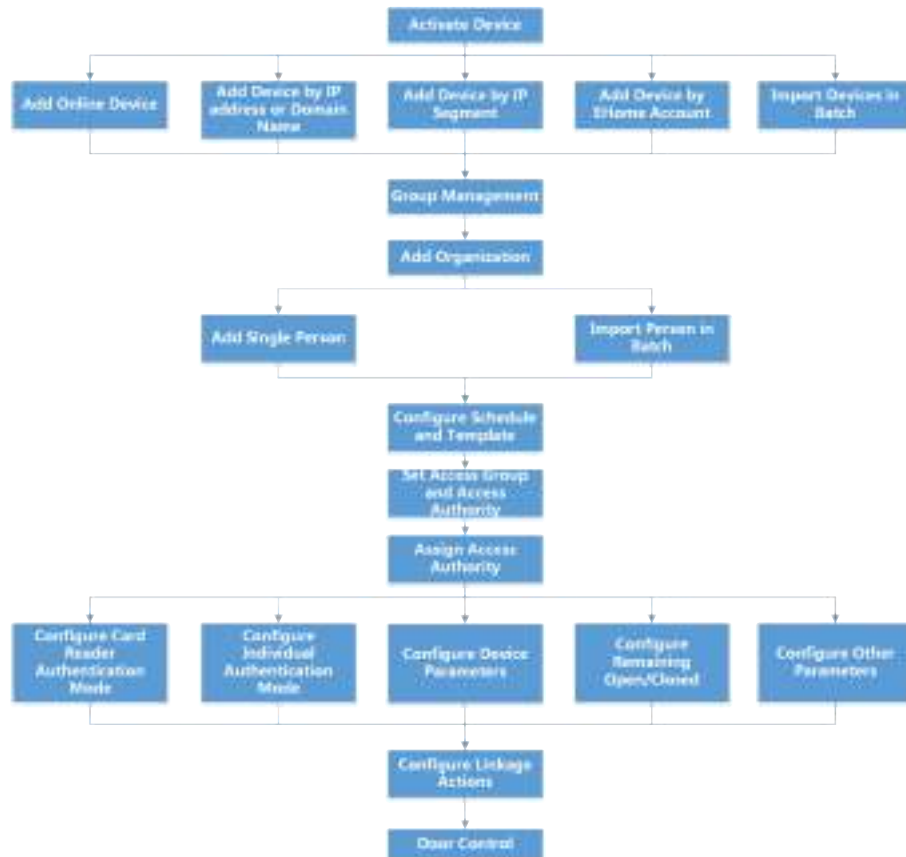


図 8-1 クライアント・ソフトウェアの設定のフロー図

8.2 デバイス管理

クライアント上で、デバイスの追加、編集、削除などの管理を実行できます。また、デバイスの状態の確認なども実行できます。

8.2.1 デバイスの追加

クライアントを実行後、入退室管理デバイスやビデオインターコムデバイスなどをクライアントに追加して、ドアの状態管理、出勤管理、イベント設定などのリモート設定と管理を実行する必要があります。

オンラインデバイスの追加

クライアントソフトウェアと同じローカルサブネットに属するアクティブなオンラインデバイスは、[オンラインデバイス] エリアに表示されます。


メモ

- [60 秒ごとに更新] ボタンをクリックすると、オンラインデバイスの情報を更新できます。
- [オンラインデバイス] を右クリックすると、SADP ログ機能を有効または無効にできます。

1 台のオンラインデバイスの追加

クライアントソフトウェアに 1 台のオンラインデバイスを追加できます。

手順

1. [デバイス管理] モジュールを開きます。
2. オプション: [デバイス管理] の右側で  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、オンラインデバイスエリアを表示します。
検索したオンラインデバイスがリスト内に表示されます。
4. [オンラインデバイス] エリアからオンラインデバイスを選択します。

メモ

非アクティブなデバイスを使用する場合、デバイスの追加にはパスワードの作成が必要になります。詳細な手順については、「アクティブ化」をご覧ください。

5. [追加] をクリックしてデバイスの追加ウィンドウを開きます。
6. 必要な情報を入力します。

名前

デバイスの内容を示す名前を入力します。

アドレス

この追加モードでは、デバイスの IP アドレスが自動的に取得されます。

ポート

ポート番号は自動的に取得されます。

ユーザー名

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ます。

注意

デバイスのパスワードの強度は、自動的に確認することができます。デバイスのセキュリティを高めるため、ご自身で作成した強力なパスワード（大文字、小文字、数字、特殊記号のうち、少なくとも 3 つのカテゴリで構成される文字を含む 8 文字以上のパスワード）を設定することを強く推奨します。また、定期的にパスワードを変更することを推奨します。特にセキュリティ要件の高いシステムでは、毎月または毎週パスワードを変更すると、より安全にデバイスを保護できます。パスワードなどのセキュリティ設定はすべて、設置者／エンドユーザーの責任で適切に行ってください。

- オプション: デバイスをクライアントに追加した後、**[時間を同期]** にチェックを入れると、クライアントを実行中の PC とデバイスの時間を同期できます。
 - オプション: デバイス名でグループを作成するには、**[グループにインポート]** にチェックを入れます。
-

メモ


デフォルト設定では、デバイスの全チャンネルを該当するグループにインポートできます。

- [OK]** をクリックし、デバイスを追加します。

複数のオンラインデバイスの追加

クライアントソフトウェアに複数のオンラインデバイスを追加できます。

手順

- [デバイス管理] モジュールを開きます。
 - [デバイス管理] の右側で  をクリックし、[デバイス] を選択します。
 - [オンラインデバイス] をクリックし、オンラインデバイスエリアを表示します。
検索したオンラインデバイスがリスト内に表示されます。
 - 複数のデバイスを選択します。
-

メモ

非アクティブなデバイスを使用する場合、デバイスの追加にはパスワードの作成が必要になります。詳細な手順については、「**アクティブ化**」をご覧ください。

- [追加]** をクリックしてデバイスの追加ウィンドウを開きます。
-

6. 必要な情報を入力します。

ユーザー名

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ます。



注意

デバイスのパスワードの強度は、自動的に確認することができます。デバイスのセキュリティを高めるため、ご自身で作成した強力なパスワード（大文字、小文字、数字、特殊記号のうち、少なくとも 3 つのカテゴリで構成される文字を含む 8 文字以上のパスワード）を設定することを強く推奨します。また、定期的にパスワードを変更することを推奨します。特にセキュリティ要件の高いシステムでは、毎月または毎週パスワードを変更すると、より安全にデバイスを保護できます。

パスワードなどのセキュリティ設定はすべて、設置者／エンドユーザーの責任で適切に行ってください。

-
7. オプション: 複数のデバイスをクライアントに追加後、[時間を同期] にチェックを入れると、クライアントを実行中の PC とデバイスの時間を同期できます。
8. オプション: デバイス名でグループを作成するには、[グループにインポート] にチェックを入れます。



メモ

デフォルト設定では、デバイスの全チャンネルを該当するグループにインポートできます。

9. [OK] をクリックし、デバイスを追加します。

IP アドレスまたはドメイン名によるデバイスの追加

追加するデバイスの IP アドレスや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することで、デバイスをクライアントに追加できます。

手順

1. [デバイス管理] モジュールを開きます。
2. 右側のパネルの上にある [デバイス] タブをクリックします。
追加したデバイスは右側のパネルに表示されています。
3. [追加] をクリックして [追加] ウィンドウを開き、追加モードで [IP/ドメイン] を選択します。

4. 必要な情報を入力します。

名前

デバイスの内容を示す名前を作成します。例えば、デバイスの場所や特徴を示すニックネームも使用できます。

アドレス

デバイスの IP アドレスまたはドメイン名です。

ポート

追加するデバイスのポート番号はすべて同じです。デフォルト値は **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** です。

パスワード

デバイスのパスワードを入力します。

 **注意**

デバイスのパスワードの強度は、自動的に確認することができます。デバイスのセキュリティを高めるため、ご自身で作成した強力なパスワード（大文字、小文字、数字、特殊記号のうち、少なくとも 3 つのカテゴリで構成される文字を含む 8 文字以上のパスワード）を設定することを強く推奨します。また、定期的にパスワードを変更することを推奨します。特にセキュリティ要件の高いシステムでは、毎月または毎週パスワードを変更すると、より安全にデバイスを保護できます。パスワードなどのセキュリティ設定はすべて、設置者／エンドユーザーの責任で適切に行ってください。

5. オプション: セキュリティを確保するために TLS（トランスポートレイヤーセキュリティ）プロトコルを使用して伝送暗号化を有効化するには、**[伝送暗号化 (TLS)]** にチェックを入れます。
-


 **メモ**

- 使用するデバイスがこの機能に対応している必要があります。
 - デバイスにログインすると、Web ブラウザで証明書ファイルを入手できます。
-

6. デバイスをクライアントに追加した後、**[時間を同期]** にチェックを入れると、クライアントを実行中の PC とデバイスの時間を同期できます。
7. オプション: デバイス名でグループを作成するには、**[グループにインポート]** にチェックを入れます。
8. デバイスの追加を終了します。
- **[追加]** をクリックすると、そのデバイスが追加され、デバイスリストのページに戻ります。
-


- [Add and New (追加および新規)] をクリックすると、その設定が保存され、続けて他のデバイスを追加できます。


9. オプション: 以下の操作を実行します。


リモート設定 [操作] 列で  をクリックし、対応するデバイスのリモート設定を行います。


メモ

リモート設定の詳細な操作手順については、デバイスのユーザーマニュアルをご覧ください。

デバイスの状態 [操作] 列で  をクリックすると、カメラ、録画状態、信号状態、ハードウェア状態など、デバイスの各種状態を確認できます。

デバイス情報の編集 [操作] 列で  をクリックすると、IP アドレス、ユーザー名、パスワードなどの各種デバイス情報を編集できます。

オンラインユーザーの確認 [操作] 列で  をクリックすると、ユーザー名、ユーザータイプ、ユーザーの IP アドレス、ログイン時間など、デバイスにアクセスするオンラインユーザーを確認できます。

更新 [操作] 列で  をクリックすると、最新のデバイス情報を取得できます。

デバイスの削除 1 つ以上のデバイスを選択して [削除] をクリックすると、選択したデバイスをクライアントから削除できます。

IP セグメントによるデバイスの追加

デバイス間で同じポート番号、ユーザー名、パスワードを共有し、IP アドレスも同じ IP セグメントを共有している場合、クライアントに追加するデバイスの開始 IP アドレスと終了 IP アドレス、ポート番号、ユーザー名、パスワードなどを指定できます。

手順

1. [デバイス管理] モジュールを開きます。
2. 右側のパネルの上にある [デバイス] タブをクリックします。
追加したデバイスは右側のパネルに表示されています。
3. [追加] をクリックし、[追加] ウィンドウを開きます。
4. [IP セグメント] を追加モードとして選択します。

5. 必要な情報を入力します。

開始 IP

開始 IP アドレスを入力します。

終了 IP

開始 IP と同じネットワークセグメント内に存在する終了 IP アドレスを入力します。

ポート

デバイスのポート番号を入力します。デフォルト値は **8000** です。

ユーザー名

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ます。

 **注意**

デバイスのパスワードの強度は、自動的に確認することができます。デバイスのセキュリティを高めるため、ご自身で作成した強力なパスワード（大文字、小文字、数字、特殊記号のうち、少なくとも 3 つのカテゴリで構成される文字を含む 8 文字以上のパスワード）を設定することを強く推奨します。また、定期的にパスワードを変更することを推奨します。特にセキュリティ要件の高いシステムでは、毎月または毎週パスワードを変更すると、より安全にデバイスを保護できます。パスワードなどのセキュリティ設定はすべて、設置者／エンドユーザーの責任で適切に行ってください。

6. オプション: セキュリティを確保するために TLS（トランスポートレイヤーセキュリティ）プロトコルを使用して伝送暗号化を有効化するには、**[伝送暗号化（TLS）]** にチェックを入れます。
-


 **メモ**

- 使用するデバイスがこの機能に対応している必要があります。
 - デバイスにログインすると、Web ブラウザで証明書ファイルを入手できます。
-

7. デバイスをクライアントに追加した後、**[時間を同期]** にチェックを入れると、クライアントを実行中の PC とデバイスの時間を同期できます。
8. オプション: デバイス名でグループを作成するには、**[グループにインポート]** にチェックを入れます。
9. デバイスの追加を終了します。
- **[追加]** をクリックすると、そのデバイスが追加され、デバイスリストのページに戻ります。
-


- [Add and New (追加および新規)] をクリックすると、その設定が保存され、続けて他のデバイスを追加できます。


10. オプション: 以下の操作を実行します。


リモート設定 [操作] 列で  をクリックし、対応するデバイスのリモート設定を行います。


メモ

リモート設定の詳細な操作手順については、デバイスのユーザーマニュアルをご覧ください。

デバイスの状態 [操作] 列で  をクリックすると、カメラ、録画状態、信号状態、ハードウェア状態など、デバイスの各種状態を確認できます。

デバイス情報の編集 [操作] 列で  をクリックすると、IP アドレス、ユーザー名、パスワードなどの各種デバイス情報を編集できます。

オンラインユーザーの確認 [操作] 列で  をクリックすると、ユーザー名、ユーザータイプ、ユーザーの IP アドレス、ログイン時間など、デバイスにアクセスするオンラインユーザーを確認できます。

更新 [操作] 列で  をクリックすると、最新のデバイス情報を取得できます。

デバイスの削除 1 つ以上のデバイスを選択して [削除] をクリックすると、選択したデバイスをクライアントから削除できます。

EHome アカウントによるデバイスの追加

入退室管理デバイスが EHome 5.0 プロトコルをサポートしている場合、サーバーアドレス、ポート番号、およびデバイス ID を設定していれば、デバイス ID とキーを入力した後で EHome プロトコルを使用してクライアントに追加できます。

始める前に

デバイスがネットワークに正しく接続されていることを確認します。

手順

1. [デバイス管理] モジュールを開きます。
追加したデバイスは右側のパネルに表示されています。
2. [追加] をクリックし、[追加] ウィンドウを開きます。

3. [EHome] 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。

デバイスアカウント

EHome プロトコルに登録済みのアカウント名を入力します。

EHome キー

EHome 5.0 デバイスの場合、ネットワークセンターのパラメータを設定したときに、そのデバイス用に EHome キーを設定していた場合はそれを入力します。

メモ





使用するデバイスがこの機能に対応している必要があります。

5. オプション: デバイスをクライアントに追加した後、[時間を同期] にチェックを入れると、クライアントを実行中の PC とデバイスの時間を同期できます。
6. オプション: [グループにインポート] にチェックを入れ、デバイス名でグループを作成し、デバイスのすべてのチャンネルをグループにインポートします。
7. デバイスの追加を終了します。
 - [追加] をクリックすると、そのデバイスが追加され、デバイスリストに戻ります。
 - [Add and New (追加および新規)] をクリックすると、その設定が保存され、続けて他のデバイスを追加できます。

メモ

顔画像は、EHome アカウントで追加されたデバイスには適用できません。

8. オプション: 以下の操作を実行します。

デバイスの状態	[操作] 列で  をクリックすると、デバイスの状態を確認できます。
デバイス情報の編集	[操作] 列で  をクリックすると、デバイス名、デバイスアカウント、EHome キーなどの各種デバイス情報を編集できます。
オンラインユーザーの確認	[操作] 列で  をクリックすると、ユーザー名、ユーザータイプ、ユーザーの IP アドレス、ログイン時間など、デバイスにアクセスするオンラインユーザーを確認できます。
更新	[操作] 列で  をクリックすると、最新のデバイス情報を取得できます。
デバイスの削除	1 つ以上のデバイスを選択して [削除] をクリックすると、選択したデバイスをクライアントから削除できます。

デバイスの一括インポート

定義済みの CSV ファイルにデバイス情報を入力することで、ソフトウェアにデバイスを一括登録できます。

手順

1. [デバイス管理] ページを開きます。
2. [追加] をクリックし、デバイスの追加ウィンドウを開きます。
3. [一括インポート] を追加モードとして選択します。
4. [エクスポートテンプレート] をクリックし、定義済みのテンプレート（CSV ファイル）をお使いの 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情報を対応する列に入力します。

モードの追加

異なる追加モードを示す **0** または **1** を入力できます。**0** は IP アドレスまたはドメイン名で、**1** は EHome 経由でデバイスを追加したことを示します。

アドレス

デバイスのアドレスを編集します。追加モードに **0** を設定する場合、デバイスの IP アドレスまたはドメイン名を入力する必要があります。**1** を設定する場合、このフィールドの入力は不要です。

ポート

デバイスのポート番号を入力します。デフォルト値は 8000 です。

デバイス情報

追加モードに **0** を設定する場合、このフィールドは不要です。追加モードに **1** を設定する場合、EHome アカウントを入力してください。

ユーザー名

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

パスワード


追加モードに **0** を設定する場合、パスワードを入力してください。追加モードに **1** を設定する場合、EHome キーを入力してください。

 **注意**

デバイスのパスワードの強度は、自動的に確認することができます。デバイスのセキュリティを高めるため、ご自身で作成した強力なパスワード（大文字、小文字、数字、特殊記号のうち、少なくとも 3 つのカテゴリで構成される文字を含む 8 文字以上のパスワード）を設定することを強く推奨します。また、定期的にパスワードを変更することを推奨します。特にセキュリティ要件の高いシステムでは、毎月または毎週パスワードを変更すると、より安全にデバイスを保護できます。パスワードなどのセキュリティ設定はすべて、設置者／エンドユーザーの責任で適切に行ってください。

グループにインポート


1 を入力すると、デバイス名でグループを作成できます。デバイスのチャンネルはすべて、対応するグループにデフォルトでインポートされます。0 はこの機能の無効化を意味しています。

6.  をクリックして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、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リセット

検知し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その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] ページを開きます。
2. [オンラインデバイス] をクリックし、オンラインデバイスエリアを表示します。
同じサブネット内のオンラインデバイスがすべてリストに表示されます。
3. リストからデバイスを選択して、[操作] 列で  をクリックします。
4. [エクスポート] をクリックしてお使いの PC にデバイスのファイルを保存し、そのファイルを当社のテクニカルサポートへ送信してください。

 **メモ**

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**

デバイスのパスワードの強度は、自動的に確認することができます。デバイスのセキュリティを高めるため、ご自身で作成した強力なパスワード（大文字、小文字、数字、特殊記号のうち、少なくとも 3 つのカテゴリで構成される文字を含む 8 文字以上のパスワード）を設定することを強く推奨します。また、定期的にパスワードを変更することを推奨します。特にセキュリティ要件の高いシステムでは、毎月または毎週パスワードを変更すると、より安全にデバイスを保護できます。パスワードなどのセキュリティ設定はすべて、設置者／エンドユーザーの責任で適切に行ってください。

8.3 グループ管理

追加されたリソースは、アクセスポイントなどの管理を容易にするために、グループに編成する必要があります。グループを介して、デバイスのいくつかの操作を実行できます。

8.3.1 グループの追加

グループの追加により、追加されたデバイスを整理し、管理しやすくすることができます。

手順

1. [デバイス管理] モジュールを開きます。
2. [デバイス管理] → [グループ] の順にクリックしてグループ管理ページを開きます。
3. グループを作成します。
 - [グループを追加] をクリックし、必要に応じてグループ名を入力します。
 - [デバイス名別にグループを作成] をクリックし、追加したデバイスを選択して、選択したデバイスの名前で新しいグループを作成します。

8.3.2 グループへのリソースのインポート

追加したグループにデバイスリソースを一括でインポートできます。

始める前に

デバイスを管理するためのグループを追加します。「グループの追加」を参照してください。

手順

1. [デバイス管理] モジュールを開きます。
2. [デバイス管理] → [グループ] の順にクリックしてグループ管理ページを開きます。

3. グループリストからグループを選択し、[入退室管理ポイント] などのリソースタイプを選択します。
4. [インポート] をクリックします。
5. [To Be Imported (インポートする)] エリアからチャンネルを選択します。
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。

8.3.3 リソースパラメータの編集

リソースをグループにインポートしたら、リソースパラメータを編集できます。アクセスポイントでは、リソース名を編集できます。

始める前に

リソースをグループにインポートします。「リソースのグループへのインポート」を参照してください。

手順

1. [デバイス管理] モジュールを開きます。
2. [デバイス管理] → [グループ] の順にクリックしてグループ管理ページを開きます。追加したグループはすべて左側に表示されます。
3. グループリストでグループを選択し、リソースタイプをクリックします。グループにインポートされたリソースチャンネルが表示されます。
4. [操作] 列の をクリックして、[カメラを編集] ウィンドウを開きます。
5. 必要な情報を編集します。
6. [OK] をクリックし、新しい設定を保存します。

8.3.4 グループからのリソースの削除

追加したリソースをグループから削除できます。

手順

1. [デバイス管理] モジュールを開きます。
2. [デバイス管理] → [グループ] の順にクリックしてグループ管理ページを開きます。追加したグループはすべて左側に表示されます。
3. グループをクリックすると、このグループに追加されたリソースが表示されます。
4. リソースを選択し、[削除] をクリックして、グループからリソースを削除します。

8.4 人物管理

関係者情報をシステムに追加することで、入退室管理、ビデオインターコム、時間および出勤などの追加操作を実行できます。カードの一括発行や関係者情報の一括インポート／エクスポートなど、追加した人物に対する管理が可能になります。

8.4.1 組織の追加

組織を追加し、その組織に関係者情報をインポートすることで、人物に対する管理が容易になります。また、その組織に下部組織も追加できます。


手順


1. [人物] モジュールを開きます。
2. 左列の親組織を選択して左上隅の [追加] をクリックし、組織を追加します。
3. 追加する組織の名前を作成します。

メモ

最大 10 階層まで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。

組織を編集 追加した組織にカーソルを合わせ、 をクリックすると名前を編集できます。

組織の削除 追加した組織にカーソルを合わせ、 をクリックすると名前を削除できます。

メモ

- 組織を削除すると、その下部組織も削除されます。
 - 組織の下に誰も追加されていないことを確認してください。追加されている場合は、その組織を削除できません。
-

下部組織の人物の表示 [Show Persons in Sub Organization (下部組織の人物を表示)] にチェックを入れて組織を選択し、下部組織に属する人物を表示します。

8.4.2 基本情報の設定

人物をクライアントソフトウェアに 1 人ずつ追加して、名前、性別、電話番号などの基本情報を設定できます。

手順

1. [人物] モジュールを開きます。
 2. 組織リスト内の組織を選択して人物を追加します。
 3. [追加] をクリックして人物の追加ウィンドウを開きます。
人物 ID が自動生成されます。
 4. 人物名、性別、電話番号、電子メールアドレスなどの基本情報を入力します。
-

5. オプション: その人物に対する有効期間を設定します。有効期間を過ぎると、その人物の認証情報と入退室管理設定は無効になり、ドア／フロアの入室許可が下りなくなります。

例

例えば、その人物が訪問者の場合、有効期間は短く、一時的なものになります。

6. 内容を確認して人物を追加します。
- **[追加]** をクリックすると、その人物が追加され **[関係者を追加]** ウィンドウが閉じます。
 - **[Add and New (追加および新規)]** をクリックすると、その人物が追加され、続けて他の人物を追加できます。

8.4.3 ローカルモードでのカード発行

カード登録ステーションが利用可能な場合は、ローカルモードでカードを発行できます。カード番号を読み取るには、クライアントを実行中の PC に USB インターフェースまたは COM で接続し、カード登録ステーションにカードを置きます。

手順

1. **[人物]** モジュールを開きます。
2. 組織リスト内の組織を選択して人物を追加し、**[追加]** をクリックして **[関係者を追加]** パネルを開きます。

メモ

最初に、その人物の基本情報を入力します。人物の基本情報の設定の詳細については、「**基本情報の設定**」をご覧ください。

3. **[認証情報]** → **[カード]** エリアで、**[+]** をクリックします。
4. **[設定]** をクリックし、**[設定]** ページを開きます。
5. カード発行モードとして **[ローカル]** を選択します。

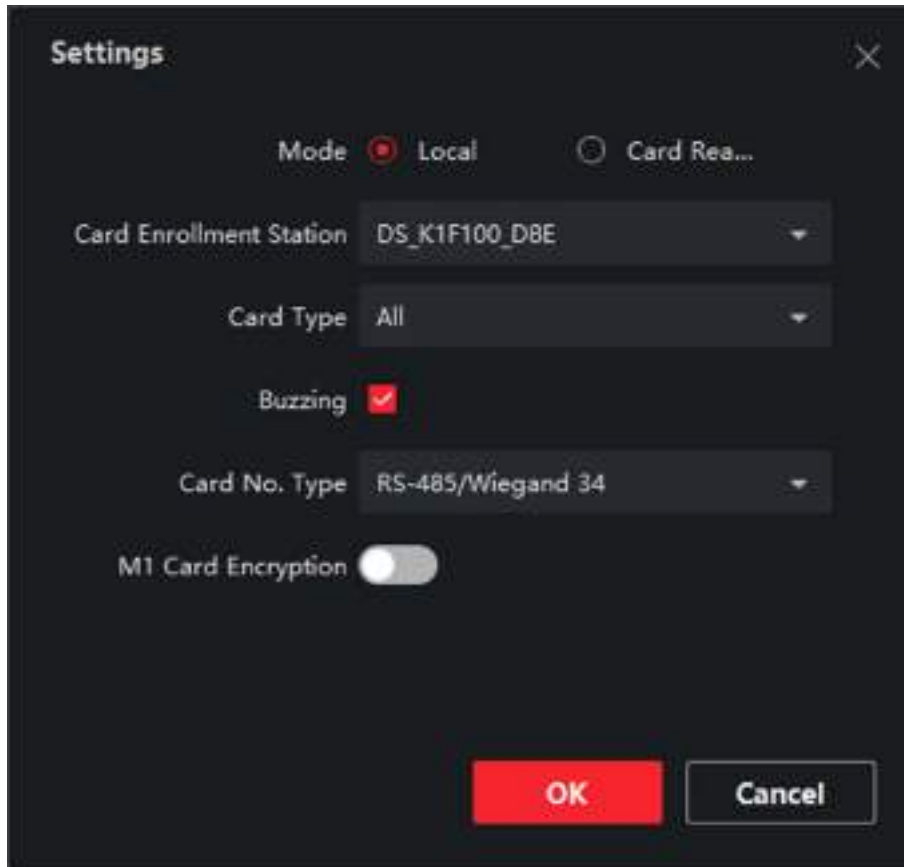


図 8-2 ローカルモードでのカード発行

6. その他の関連パラメータを設定します。

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ます。

メモ

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

カードタイプ

使用モデルが DS-K1F100-D8E または DS-K1F180-D8E の場合に限り、このフィールドを使用できます。実際のカードタイプに応じて、EM カードまたは Mifare カードを選択します。

ブザー

カード番号の読み取りに成功した時に、ブザーを鳴らすかどうかを選択します。

カード番号タイプ

実際の使用状況に応じて、カード番号のタイプを選択します。

M1 カード暗号化

使用モデルが DS-K1F100-D8、DS-K1F100-D8E または DS-K1F180-D8E の場合に限り、このフィールドを使用できます。使用するカードが M1 カードの場合、その暗号化機能を有効化し、カード内の暗号化するセクターを選択する必要があります。

7. [OK] をクリックし、操作を確認します。
8. カード登録ステーションにカードを置き、[Read (読み取り)] をクリックしてカード番号を読み取ります。
カード番号は [カード番号] フィールドに自動的に表示されます。
9. [追加] をクリックします。
その人物にカードが発行されます。

8.4.4 ローカル PC からの顔写真のアップロード

人物を追加する際に、ローカル PC に保存した顔写真を人物プロフィールとしてクライアントへアップロードできます。

手順

1. [人物] モジュールを開きます。
2. 組織リスト内の組織を選択して人物を追加し、[追加] をクリックします。

メモ

最初に、その人物の基本情報を入力します。人物の基本情報の設定の詳細については、「**基本情報の設定**」をご覧ください。

3. [基本情報] パネルで [顔の追加] をクリックします。
4. [アップロード] を選択します。
5. クライアントを実行中の PC から画像を選択します。

メモ

画像は JPG または JPEG 形式で、サイズは 200KB 未満にしてください。

6. オプション: [デバイスによる認証] を有効化すると、クライアントの顔認識デバイスが写真内の顔を認識できるかどうかを確認できます。
7. 内容を確認して人物を追加します。
 - [追加] をクリックすると、その人物が追加され [関係者を追加] ウィンドウが閉じます。
 - [Add and New (追加および新規)] をクリックすると、その人物が追加され、続けて他の人物を追加できます。

8.4.5 クライアント経由の写真撮影

人物を追加する際に、クライアントを実行中の PC に搭載したウェブカムでその人物の写真を撮影し、その写真を人物プロフィールとして設定できます。

始める前に



入退室管理デバイスを 1 つ以上追加し、クライアント側で管理する顔認識デバイスで写真内の顔を認識できるか確認してください。

手順

1. [人物] モジュールを開きます。
2. 組織リスト内の組織を選択して人物を追加し、[追加] をクリックします。

メモ

最初に、その人物の基本情報を入力します。人物の基本情報の設定の詳細については、「**基本情報の設定**」をご覧ください。

3. [基本情報] パネルで [顔の追加] をクリックします。
4. [写真撮影] を選択します。
5. クライアントを実行中の PC に、顔スキャナを接続します。
6. オプション: [デバイスによる認証] を有効化すると、クライアントの顔認識デバイスが写真内の顔を認識できるかどうかを確認できます。
7. 写真を撮影します。
 - 1) PC のウェブカムを真正面から見て、自身の顔がキャプチャウィンドウの中央に位置していることを確認します。
 - 2)  をクリックして顔写真を撮影します。
 - 3) オプション:  をクリックすると、再度撮影できます。
 - 4) [OK] をクリックして撮影した写真を保存します。
8. 内容を確認して人物を追加します。
 - [追加] をクリックすると、その人物が追加され [関係者を追加] ウィンドウが閉じます。
 - [Add and New (追加および新規)] をクリックすると、その人物が追加され、続けて他の人物を追加できます。

8.4.6 入退室管理デバイスでの顔画像の取り込み

人物を追加する際に、クライアントに追加した入退室管理デバイスを使用して顔画像を取り込むことができます。その場合、クライアントが顔認識機能に対応している必要があります。


手順

1. [人物] モジュールを開きます。

2. 組織リスト内の組織を選択して人物を追加し、**[追加]** をクリックします。

メモ

最初に、その人物の基本情報を入力します。人物の基本情報の設定の詳細については、「**基本情報の設定**」をご覧ください。

3. **[基本情報]** パネルで **[顔の追加]** をクリックします。
4. **[Remote Collection (リモート取り込み)]** を選択します。
5. ドロップダウンリストの中から、顔認識機能に対応する入退室管理デバイスを選択します。
6. 顔画像を取り込みます。
 - 1) 選択した入退室管理デバイスのカメラを真正面から見て、自身の顔がキャプチャウィンドウの中央に位置していることを確認します。
 - 2)  をクリックして顔写真を撮影します。
 - 3) **[OK]** をクリックして撮影した写真を保存します。
7. 内容を確認して人物を追加します。
 - **[追加]** をクリックすると、その人物が追加され **[関係者を追加]** ウィンドウが閉じます。
 - **[Add and New (追加および新規)]** をクリックすると、その人物が追加され、続けて他の人物を追加できます。

8.4.7 クライアントでの指紋の取り込み

クライアントを実行中の PC に直接接続した指紋レコーダーを使用することで、指紋をローカルで取り込むことができます。取り込んだ指紋は、ドアへのアクセスを許可するための個人認証用の認証情報として使用できます。

始める前に

クライアントを実行中の PC に指紋レコーダーを接続します。

手順

1. **[人物]** モジュールを開きます。
2. 組織リスト内の組織を選択して人物を追加し、**[追加]** をクリックします。

メモ

最初に、その人物の基本情報を入力します。人物の基本情報の設定の詳細については、「**基本情報の設定**」をご覧ください。

3. **[認証情報]** → **[指紋]** パネルの順に進み、**[+]** をクリックします。
4. ポップアップウィンドウで、取り込みモードに **[ローカル]** を選択します。
5. 接続した指紋レコーダーのモデルを選択します。

 **メモ**

指紋レコーダーが DS-K1F800-F の場合、**[設定]** をクリックして、指紋レコーダーを接続中の COM を選択できます。

6. 指紋を取り込みます。
 - 1) **[開始]** をクリックします。
 - 2) 指紋レコーダー上に指を置き、指紋を取り込ませます。
 - 3) **[追加]** をクリックし、取り込んだ指紋を保存します。
 7. 内容を確認して人物を追加します。
 - **[追加]** をクリックすると、その人物が追加され **[関係者を追加]** ウィンドウが閉じます。
 - **[Add and New (追加および新規)]** をクリックすると、その人物が追加され、続けて他の人物を追加できます。
-

 **メモ**

指紋が追加されると、指紋タイプは変更できません。

8.4.8 入退室管理デバイスでの指紋の取り込み

人物を追加する際に、入退室管理デバイスの指紋モジュールを使用して指紋情報を取り込むことができます。取り込んだ指紋は、ドアへのアクセスを許可するための個人認証用の認証情報として使用できます。

始める前に

お使いの入退室管理デバイスが指紋取り込み機能に対応していることを確認してください。

手順

1. **[人物]** モジュールを開きます。
 2. 組織リスト内の組織を選択して人物を追加し、**[追加]** をクリックします。
-

 **メモ**

最初に、その人物の基本情報を入力します。人物の基本情報の設定の詳細については、「**基本情報の設定**」をご覧ください。

3. **[認証情報]** → **[指紋]** パネルの順に進み、**[+]** をクリックします。
 4. ポップアップウィンドウで、取り込みモードに **[リモート]** を選択します。
 5. ドロップダウンリストの中から、指紋認識機能が使用できる入退室管理デバイスを選択します。
 6. 指紋を取り込みます。
-

- 1) **[開始]** をクリックします。
 - 2) 選択した入退室管理デバイスの指紋スキャナの上に指を置き、指紋を取り込ませます。
 - 3) **[追加]** をクリックし、取り込んだ指紋を保存します。
7. 内容を確認して人物を追加します。
- **[追加]** をクリックすると、その人物が追加され **[関係者を追加]** ウィンドウが閉じます。
 - **[Add and New (追加および新規)]** をクリックすると、その人物が追加され、続けて他の人物を追加できます。
-

メモ

指紋が追加されると、指紋タイプは変更できません。

8.4.9 入退室管理情報の設定

人物を追加する際に、訪問者、ブラックリスト内の人物、特別の権限を有するスーパーユーザーなど、その人物の入退室管理プロパティを設定できます。

手順

1. **[人物]** モジュールを開きます。
2. 組織リスト内の組織を選択して人物を追加し、**[追加]** をクリックします。
3. **[入退室管理]** エリア内でその人物の入退室管理プロパティを設定します。

アクセスグループ

1 つまたは複数のアクセスグループを選択して、選択したアクセスポイントへの許可を付与できます。詳細については、「**アクセスグループの設定によるアクセス認証の人物への割り当て**」をご覧ください。

パスワード

アクセス時には、カードまたは指紋をスワイプした後に、パスワードを入力する必要があります。単独で使用することはできません。また、4~8桁の数字を含める必要があります。

スーパーユーザー

スーパーユーザーとして設定された人物は、すべてのドア/フロアにアクセスできるだけでなく、閉鎖状態にかかわる制約、すべてのアンチパスバックルール、最初の人物としての認証の適用からも除外されます。

ドア開放時間の延長

ドアにアクセスする時に、ドアの開放継続時間を延長してドアを通過できるようにします。スムーズに移動することが難しい人物には、この機能を使用してください。ドア開放継続時間の設定の詳細については、「**ドア／エレベータのパラメータ設定**」をご覧ください。

ブラックリストに追加

ブラックリストに追加された人物がドア／フロアへのアクセスを試みるとイベントがトリガーされ、クライアントにその情報が送信されてセキュリティ担当者に通知が届きます。

訪問者としてマーク

訪問者を認証する場合、カードと指紋によるアクセスなどの最大認証回数を設定することで、その訪問者のアクセス回数を制限します。

メモ

最大認証回数は 1～100 回の範囲で設定できます。

デバイスオペレータ

デバイスオペレータの役割を担う人物には、入退室管理デバイスの操作権限が付与されています。

メモ

[スーパーユーザー]、[ドア開放時間の延長]、[ブラックリストに追加]、[訪問者としてマーク] 機能は同時には有効化できません。例えば、ある人物をスーパーユーザーに設定した場合、その人物に対してドア開放時間の延長機能やブラックリスト機能、訪問者機能は設定できません。

4. 内容を確認して人物を追加します。

- [追加] をクリックすると、その人物が追加され [関係者を追加] ウィンドウが閉じます。
- [Add and New (追加および新規)] をクリックすると、その人物が追加され、続けて他の人物を追加できます。

8.4.10 関係者情報のカスタマイズ

実際の使用状況に応じて、クライアントに事前定義されていない人物プロパティをカスタマイズできます (例: 出生地)。カスタマイズ後に人物を追加すると、そのカスタム情報を入力することで関係者情報の登録が完成します。

手順

1. [人物] モジュールを開きます。

2. カスタム情報のフィールドを設定します。
 - 1) [カスタムプロパティ] をクリックします。
 - 2) [追加] をクリックして新規プロパティを追加します。
 - 3) プロパティ名を入力します。
 - 4) [OK] をクリックします。
 3. 人物を追加する際に、カスタム情報を設定します。
 - 1) 組織リスト内の組織を選択して人物を追加し、[追加] をクリックします。
-

メモ

最初に、その人物の基本情報を入力します。人物の基本情報の設定の詳細については、「基本情報の設定」をご覧ください。

- 2) [カスタム情報] パネル内で関係者情報を入力します。
- 3) [追加] をクリックすると、その人物を追加して [関係者を追加] ウィンドウが閉じます。または [Add and New (追加および新規)] をクリックすると、その人物を追加した後で、引き続き別の人物を追加できます。

8.4.11 居住者情報の設定

登録する人物が居住者の場合、ビデオインターコムを使用するには、その人物の部屋番号を設定して屋内ステーションに関連付ける必要があります。関連付けを行った後は、屋内ステーションでこの人物を呼び出し、ビデオインターコムで話すことができます。

手順

1. [人物] モジュールを開きます。
 2. 組織リスト内の組織を選択して人物を追加し、[追加] をクリックします。
-

メモ

最初に、その人物の基本情報を入力します。人物の基本情報の設定の詳細については、「基本情報の設定」をご覧ください。

3. [居住者情報] パネル内で屋内ステーションを選択し、その人物と関連付けます。
-

メモ

[アナログ屋内ステーション] を選択した場合には [ドアステーション] フィールドが表示され、アナログの屋内ステーションで通信するドアステーションの選択が必要になります。

4. その人物のフロア番号と部屋番号を入力します。
 5. 内容を確認して人物を追加します。
-

- [追加] をクリックすると、その人物が追加され [関係者を追加] ウィンドウが閉じます。
- [Add and New (追加および新規)] をクリックすると、その人物が追加され、続けて他の人物を追加できます。

8.4.12 追加情報の設定

人物を追加する際に、実際の使用状況に応じて、その人物の ID タイプ、ID 番号、国籍などの追加情報を設定できます。

手順

1. [人物] モジュールを開きます。
2. 組織リスト内の組織を選択して人物を追加し、[追加] をクリックします。

メモ

最初に、その人物の基本情報を入力します。人物の基本情報の設定の詳細については、「基本情報の設定」をご覧ください。

3. [追加情報] パネル内で、実際の使用状況に応じて、その人物の ID タイプ、ID 番号、役職などの追加情報を入力します。
4. 内容を確認して人物を追加します。
 - [追加] をクリックすると、その人物が追加され [関係者を追加] ウィンドウが閉じます。
 - [Add and New (追加および新規)] をクリックすると、その人物が追加され、続けて他の人物を追加できます。

8.4.13 人物の ID 情報のインポートとエクスポート

複数の人物の情報と画像をクライアントソフトウェアに一括でインポートできます。また、人物の情報と画像をお使いの PC にエクスポートして保存することもできます。

8.4.14 関係者情報のインポート

事前定義したテンプレート (CSV ファイル) に複数の人物の情報を入力して、クライアントに一括でインポートできます。


手順

1. [人物] モジュールを開きます。
2. リストに追加した組織を選択するか、左上隅の [追加] をクリックして組織を追加した後、その組織を選択します。
3. [インポート] をクリックして [インポート] パネルを開きます。
4. インポートモードで [関係者情報] を選択します。

5. [人物インポート用テンプレートをダウンロードする] をクリックし、テンプレートをダウンロードします。
 6. ダウンロードしたテンプレートに関係者情報を入力します。
-

メモ

- その人物が複数のカードを所有している場合、セミコロンを使用して各カード番号を入力します。
 - アスタリスク付きの項目の入力は必須です。
 - デフォルトでは、[採用日] は現在の日付になります。
-

7.  をクリックして関係者情報を記載した CSV 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。
-

メモ

- その人物の番号がクライアントのデータベース内にすでに存在する場合、インポート前に既存の情報を削除してください。
 - 最大で 10,000 名分の情報をインポートできます。
-

8.4.15 人物画像のインポート


追加した人物の顔画像をクライアントにインポートした後は、追加した顔認識端末でその人物の画像を識別できます。必要に応じて、人物の画像を 1 枚ずつ、または同時に複数枚をインポートできます。

始める前に

事前に関係者情報をクライアントにインポート済みであることを確認してください。

手順

1. [人物] モジュールを開きます。
2. リストに追加した組織を選択するか、左上隅の [追加] をクリックして組織を追加した後にその組織を選択します。
3. [インポート] をクリックして [インポート] パネルを開き、[顔] にチェックを入れます。
4. オプション: [デバイスによる認証] を有効化して、クライアントが管理する顔認識デバイスが、写真内の顔を認識できるか確認します。

5.  をクリックして顔画像ファイルを選択します。

メモ

- 顔画像（のフォルダ）は ZIP 形式で格納してください。
 - 各画像ファイルは JPG 形式で、サイズは 200KB 以下にしてください。
 - 各画像ファイルの名前は「人物 ID_名前」で設定してください。インポートした関係者情報と同じ 人物 ID を使用してください。
-

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

8.4.16 関係者情報のエクスポート

追加した関係者情報を CSV ファイル形式でローカル PC にエクスポートできます。

始める前に

その人物を組織に追加済みであることを確認してください。

手順

1. [人物] モジュールを開きます。
 2. オプション: リスト内の組織を選択します。
-

メモ

組織を選択しない場合、すべての人物の情報がエクスポートされます。

3. [エクスポート] をクリックして [エクスポート] パネルを開き、エクスポートするコンテンツで [関係者情報] にチェックを入れます。
4. エクスポートする項目にチェックを入れます。
5. [エクスポート] をクリックし、エクスポートした CSV ファイルをお使いの PC に保存します。

8.4.17 人物画像のエクスポート

追加した人物の顔画像ファイルをエクスポートして、お使いの PC に保存できます。

始める前に

その人物とその顔画像を組織に追加済みであることを確認してください。

手順

1. [人物] モジュールを開きます。
 2. オプション: リスト内の組織を選択します。
-

 **メモ**

組織を選択しない場合、すべての人物の顔画像がエクスポートされます。

3. **[エクスポート]** をクリックして **[エクスポート]** パネルを開き、エクスポートするコンテンツで **[顔]** にチェックを入れます。
 4. **[エクスポート]** ボタンをクリックしてエクスポートを開始します。
-

 **メモ**

- ファイルは ZIP 形式でエクスポートされます。
 - エクスポートする顔画像の名前は「人物 ID_名前_0」です（「0」は真正面からの顔画像を示します）。
-

8.4.18 入退室管理デバイスからの関係者情報の取得

入退室管理デバイスに、関係者情報（人物の詳細、指紋、発行済みカード情報など）を設定済みの場合、そのデバイスから関係者情報を取得した後に、クライアントへインポートして操作できます。

手順

 **メモ**

- デバイスに保存した人物名が空白の場合、クライアントにインポートすると、人物名には発行済みのカード番号が表示されます。
 - 人物の性別はデフォルトでは **[男性]** になります。
 - デバイスに保存したカード番号または人物 ID（従業員 ID）がクライアントのデータベースに保存済みの場合、このカード番号または人物 ID に該当する人物は、クライアントへインポートされません。
-

1. **[人物]** モジュールを開きます。
 2. その人物の情報をインポートする組織を選択します。
 3. **[デバイスから入手]** をクリックします。
 4. ドロップダウンリストから入退室管理デバイスを選択します。
 5. **[入手]** をクリックし、クライアントへの関係者情報のインポートを開始します。
関係者詳細、指紋情報（設定済みの場合）、リンク済みカード場合（設定済みの場合）などの関係者情報が選択した組織にインポートされます。
-

8.4.19 別組織への人物の移動

必要に応じて、追加した人物を別組織に移動できます。

始める前に

- 少なくとも 2 つの組織を追加済みであることを確認してください。
- 関係者情報をインポート済みであることを確認してください。

手順

1. [人物] モジュールを開きます。
2. 左側のパネルで組織を選択します。
その組織に属する人物が右側のパネルに表示されます。
3. 移動させる人物を選択します。
4. [Change Organization (組織を変更)] をクリックします。
5. その人物の移動先となる組織を選択します。
6. [OK] をクリックします。

8.4.20 複数の人物へのカードの一括発行

クライアントには、複数の人物にカードを一括で発行する便利な機能が備わっています。

手順



1. [人物] モジュールを開きます。
2. [カードの一括発行] をクリックします。
追加されていて、まだカードを発行されていない人物がすべて表示されます。
3. カードの発行パラメータを設定します。詳細については、「カードの発行パラメータ設定」をご覧ください。
4. [初期化] をクリックしてカードの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します。
5. カード番号の列をクリックし、カード番号を入力します。
 - カード登録ステーションにカードを置きます。
 - カードリーダー上でカードをスワイプします。
 - 手動でカード番号を入力し、キーボードの **Enter** キーを押します。カード番号が自動的に読み取られ、リスト内の人物にカードが発行されます。
6. 上記の手順を繰り返し、リスト内の人物へ続けてカードを発行します。

8.4.21 カード紛失の報告

カードを紛失した場合、それを報告することで、カード関連の認証を無効化できます。

手順

1. [人物] モジュールを開きます。

2. カードの紛失を報告する人物を選択して **[編集]** をクリックし[関係者を編集] ウィンドウを開きます。
3. **[認証情報]** → **[カード]** パネルの順に進み、該当する追加カードで  をクリックして紛失カードとして設定します。
カードの紛失を報告した後は、そのカードのアクセス認証は無効かつ非アクティブになります。別の人物がこのカードを入手してスワイプしてもドアは開放されません。
4. オプション: 紛失したカードが見つかった場合、 をクリックすると紛失設定をキャンセルできます。
カードの紛失設定をキャンセルした後は、その人物のアクセス認証は有効かつアクティブになります。
5. 紛失したカードが単一のアクセスグループに追加されていて、そのアクセスグループをデバイスに適用済みの場合、カードの紛失または紛失のキャンセルを報告すると、変更事項をこのデバイスに適用することを通知するウィンドウがポップアップ表示されます。デバイスに適用した後、そのデバイスで、これらの変更事項が有効になります。

8.4.22 カードの発行パラメータ設定

クライアント側では、カード登録ステーションまたは入退室管理デバイスのカードリーダーの 2 種類のモードでカード番号を読み取ることができます。カード登録ステーションが利用可能な場合、クライアントを実行中の PC に USB インターフェースまたは COM で接続し、カード登録ステーションにカードを置いてカード番号を読み取ります。カード登録ステーションが利用できない場合でも、追加した入退室管理デバイスのカードリーダーにカードをスワイプすると、カード番号を取得できます。そのため、人物にカードを発行する前に、発行モードやカード関連パラメータなどの発行パラメータを設定しておく必要があります。

カードを 1 人の人物に発行する場合、**[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でのカード発行

クライアントを実行中の PC にカード登録ステーションを接続します。カード登録ステーションにカードを置き、カード番号を入手します。

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ます。

メモ

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

カードタイプ

使用モデルが DS-K1F100-D8E または DS-K1F180-D8E の場合に限り、このフィールドを使用できます。

実際のカードタイプに応じて、EM カードまたは IC カードを選択します。

シリアルポート

使用モデルが DS-K1F100-M の場合に限り、このフィールドを使用できます。

カード登録ステーションの接続先となる COM を選択します。

ブザー

カード番号の読み取りに成功した時に、ブザーを鳴らすかどうかを選択します。

カード番号タイプ

実際の使用状況に応じて、カード番号のタイプを選択します。

M1 カード暗号化

使用モデルが DS-K1F100-D8、DS-K1F100-D8E または DS-K1F180-D8E の場合に限り、このフィールドを使用できます。

使用するカードが M1 カードで、その暗号化機能を有効化する必要がある場合、この機能を有効化し、カード内の暗号化するセクターを選択する必要があります。

リモートモード: カードリーダーでのカード発行

クライアントに追加した入退室管理デバイスを選択し、カードリーダー上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

休日と週のスケジュールを含むテンプレートを設定できます。このテンプレートを設定した後は、アクセスグループの設定時に設定済みのテンプレートをアクセスグループに適用し、テンプレートの期間内でアクセスグループを有効化できるようになります。

メモ

アクセスグループ設定の詳細については、「アクセスグループの設定によるアクセス認証の人物への割り当て」をご覧ください。

8.5.1 休日の追加

休日を作成して、開始日、終了日、1 日以内での休時間帯などを設定できます。

手順

 メモ

このソフトウェアシステムには休日を最大 64 日追加できます。

1. [入退室管理] → [スケジュール] → [休日] の順にクリックし、[休日] ページを開きます。
2. 左側のパネルにある [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: [注釈] ボックスに、休日の説明または通知事項を入力できます。
5. 休日期間を休日リストに追加し、休日の期間を設定します。






 メモ

休日 1 日に対して最大 16 の休時間帯を追加できます。

- 1) [休日リスト] フィールドで [追加] をクリックします。
- 2) カーソルで時間帯をドラッグ操作して、設定したアクセスグループがその時間中はアクティブの状態になるようにします。

 メモ

休日 1 期間に対して最大 8 つの休時間帯を設定できます。

- 3) オプション: 以下の操作を実行すると、時間帯を編集できます。
 - カーソルを時間帯に移動し、カーソルが  に切り替わると、タイムラインバーの時間帯をドラッグして目的の位置へ移動します。
 - 時間帯をクリックし、ダイアログが表示されたら開始時間／終了時間を直接編集します。
 - カーソルを時間帯の開始時間または終了時間に移動し、カーソルが  に変わると、ドラッグ操作で時間帯を延長または短縮できます。
 - 4) オプション: 削除する時間帯を選択し、[操作] 列で  をクリックすると選択した時間帯を削除できます。
 - 5) オプション: [操作] 列で  をクリックすると、タイムバー内の時間帯をすべて削除できます。
 - 6) オプション: [操作] 列で  をクリックすると、追加した休日を休日リストから削除できます。
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、週のスケジュールと休日が含まれています。週のスケジュールを設定して、異なる人物またはグループにアクセス認証期間を割り当てることができます。追加した休日もテンプレートで選択できます。

手順

メモ

このソフトウェアシステムには最大 255 件のテンプレートを追加できます。

1. [入退室管理] → [スケジュール] → [テンプレート] の順にクリックし、[テンプレート] ページを開きます。

メモ

デフォルトのテンプレートは 2 つあります。デフォルトのテンプレートには、全日認証と全日拒否の 2 種類があり、それらの編集や削除は実行できません。

全日認証

このアクセス認証は該当する週の各日で有効であり、休日はありません。



全日拒否

このアクセス認証は該当する週の各日で無効であり、休日はありません。

2. 左側のパネルで [追加] をクリックし、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. このテンプレートの説明または通知事項を [注釈] ボックスに入力します。
5. 週のスケジュールを編集し、テンプレートに適用します。
 - 1) 下部のパネルで [Week Schedule (週スケジュール)] タブをクリックします。
 - 2) 該当する週の日付を選択し、タイムラインバーで期間を示します。

メモ

週のスケジュールでは、各日あたり最大 8 つの時間帯を設定できます。

- 3) オプション: 以下の操作を実行すると、時間帯を編集できます。
 - カーソルを時間帯に移動し、カーソルが  に切り替わると、タイムラインバーの時間帯をドラッグして目的の位置へ移動します。
 - 時間帯をクリックし、ダイアログが表示されたら開始時間／終了時間を直接編集します。
 - カーソルを時間帯の開始時間または終了時間に移動し、カーソルが  に変わると、ドラッグ操作で時間帯を延長または短縮できます。
 - 4) 上記の手順を繰り返し、該当する週の別の日付にも時間帯を追加します。
-

6. 休日を追加してテンプレートに適用します。


 **メモ**

1 つのテンプレートには最大 4 件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済みリストに追加されます。
- 3) オプション: **[追加]** をクリックすると、新しい休日を追加できます。

 **メモ**

休日の追加方法の詳細については、「**休日の追加**」をご覧ください。

- 4) オプション: 右側のリストから選択済みの休日を選択し、 をクリックすると、選択した休日を削除できます。また、**[消去]** をクリックすると、右側のリストにある選択済みの休日をすべて消去できます。
7. **[保存]** をクリックして設定を保存し、テンプレートの追加を終了します。

8.6 アクセスグループの設定によるアクセス認証の人物への割り当て

人物を追加してその人物の認証情報を設定した後は、アクセスグループを作成して、どの人物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入退室管理デバイスに適用することで設定を有効化できるようになります。

手順

- 1 名に対して、1 台のデバイスの入退室管理ポイント 1 カ所につき、最大で 4 つのアクセスグループを追加できます。
 - 合計 128 のアクセスグループを追加できます。
 - アクセスグループの設定を変更した場合、そのアクセスグループをデバイスに適用して有効化する必要があります。アクセスグループの変更事項には、テンプレート、アクセスグループ設定、人物のアクセスグループ設定、アクセスグループに関連する人物の詳細（例: カード番号、指紋、顔画像、カード番号と指紋の関連付け、またはカード番号と指紋、カードのパスワード、カードの有効期限との関連付け）が含まれます。
1. **[入退室管理]** → **[アクセスグループ]** の順をクリックし、**[アクセスグループ]** インターフェースを開きます。
 2. **[追加]** をクリックし、**[追加]** ウィンドウを開きます。
 3. **[名前]** テキストフィールドで希望のアクセスグループ名を作成します。
 4. アクセスグループのテンプレートを選択します。

 **メモ**

アクセスグループの設定前にテンプレートを設定しておく必要があります。詳細については、「スケジュールとテンプレートの設定」をご覧ください。


5. [関係者を選択] フィールドの左側のリストで人物を選択すると、その人物が選択したリストに追加されます。
6. [Select Door (ドアを選択)] フィールドの左側のリストで、選択した人物がアクセスするドアまたはドアステーションを選択すると、選択したドアまたはドアステーションが選択したリストに追加されます。
7. [OK] をクリックします。
8. アクセスグループの追加後に、そのグループを入退室管理デバイスに適用して有効化する必要があります。
 - 1) 入退室管理デバイスに適用するアクセスグループを選択します。

複数のアクセスグループを選択するには、[Ctrl] または [Shift] キーを押しながらアクセスグループを選択します。
 - 2) [Apply All to Devices (デバイスにすべて適用)] をクリックし、入退室管理デバイスまたはドアステーションに対して選択したすべてのアクセスグループの適用を開始します。

 **注意**

- [Apply All to Devices (デバイスにすべて適用)] をクリックすると、選択したデバイス内のすべてのアクセスグループが消去され、新しいアクセスグループが適用されるため、デバイスをリスクにさらす可能性があります。クリック時には注意してください。
 - [Apply Changes to Devices (デバイスに変更を適用)] をクリックして、選択したアクセスグループ内の変更事項のみをデバイスに適用することもできます。
-


- 3) [状態] 列で状態の適用を表示させるか、[Applying Status (状態を適用)] をクリックして適用したすべてのアクセスグループを表示させます。

適用したアクセスグループ内で選択した人物は、リンク済みのカードまたは指紋を使用して、選択したドア／ドアステーションから入室／退室する権限を持ちます。
9. オプション: 必要に応じて  をクリックし、アクセスグループを編集します。

8.7 詳細機能の設定

入退室管理の詳細機能を設定することで、さまざまなシーンにおける特別な要件に対応できます。

 **メモ**

- カード関連機能（入退室管理カードのタイプ）の場合、カードの追加時には、アクセスグループを適用したカードのみがリストに表示されます。
 - デバイスが該当の詳細機能に対応している必要があります。
 - [詳細機能] にカーソルを移動して  をクリックし、表示する詳細機能をカスタマイズします。
-

8.7.1 デバイスパラメータの設定

入退室管理デバイスの追加後に、入退室管理のパラメータと入退室管理ポイントを設定できるようになります。


入退室管理デバイスのパラメータ設定

入退室管理デバイスを追加した後、ユーザー情報の画像へのオーバーレイ、キャプチャ後の画像のアップロード、キャプチャ画像の保存などのパラメータを設定できます。

手順

1. [入退室管理] → [詳細機能] → [デバイスパラメータ] の順にクリックします。
-

 **メモ**

[詳細機能] リスト内に [デバイスパラメータ] がある場合、カーソルを [詳細機能] に移動して  をクリックし、[デバイスパラメータ] を選択して表示させます。

2. 右側のページでアクセスデバイスを選択し、そのパラメータを表示させます。
 3. スイッチを [ON] にして対応する機能を有効にします。
-

 **メモ**

- 入退室管理デバイスごとに表示するパラメータが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] ページにリスト表示されないため、パラメータを編集するには [詳細] をクリックしてください。
-

音声プロンプト

この機能を有効にすると、デバイスで音声プロンプトを使用できます。デバイスの動作中、音声プロンプトを聞くことができます。

画像のアップロード（リンクキャプチャ後）

リンク済みカメラでキャプチャした画像を、システムへ自動的にアップロードします。

画像の保存（リンクキャプチャ後）

この機能を有効にすると、リンク済みカメラでキャプチャした画像をデバイスに保存できます。

顔認識モード

通常モード

カメラを使用する標準的な顔認識機能です。

Deep Mode（ディープモード）

通常モードよりもはるかに広範囲な人物認証が可能です。より複雑な環境に適しています。

NFC カードの有効化

この機能を有効にすると、デバイスが NFC カードを認識できるようになります。NFC カードはデバイスに装着可能です。

M1 カードの有効化

この機能を有効にすると、デバイスは M1 カードを認識できるようになります。M1 カードはデバイスに装着可能です。

EM カードの有効化

この機能を有効にすると、デバイスが EM カードを認識できるようになります。EM カードはデバイスに装着可能です。

CPU カードの有効化

予約済み。この機能を有効にすると、デバイスが CPU カードを認識できるようになります。CPU カードはデバイスに装着可能です。

ID カードの有効化

予約済み。この機能を有効にすると、デバイスが ID カードを認識できるようになります。ID カードはデバイスに装着可能です。

4. [OK] をクリックします。

5. オプション: [コピー先] をクリックして入退室管理デバイスを選択すると、ページ内のパラメータを選択したデバイスにコピーできます。

ドア／エレベータのパラメータ設定

入退室管理デバイスの追加後に、そのアクセスポイント（ドア）のパラメータを設定できるようになります。

手順

1. [入退室管理] → [詳細機能] → [デバイスパラメータ] の順にクリックします。

2. 左側のパネルで入退室管理デバイスを選択し、■ 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させます。
 3. 右側のページでドアまたはフロアを選択し、そのパラメータを表示させます。
 4. ドアまたはフロアのパラメータを編集します。
-

メモ

- 入退室管理デバイスごとに表示するパラメータが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] ページにリスト表示されないため、パラメータを編集するには [詳細] をクリックしてください。
-

名前

カードリーダー名を編集して希望する名前にします。

ドアの接触装置

ドアセンサーは、閉鎖状態または開放状態に設定できます。通常は閉鎖状態に設定されています。

出口ボタンのタイプ

出口ボタンは、閉鎖状態または開放状態に設定できます。通常は開放状態に設定されています。

ドアロック時間

通常カードをスワイプして中継操作を実行すると、ドアをロックするタイマーが作動します。

延長開放継続時間

アクセス時間の延長が必要な人物が自身のカードをスワイプすると、ドアの接触装置が作動して開放時間を適切に延長します。

ドア開放タイムアウトアラーム

設定した時間内にドアが閉鎖しない場合、アラームをトリガーさせることができます。0 に設定するとアラームはトリガーされません。

強要コード

緊急時には、強要コードを入力するとドアが開きます。同時に、クライアントが強要イベントを報告することができます。

スーパーパスワード

指定された人物がスーパーパスワードを入力すると、ドアを開くことができます。

メモ

- 強要コードとスーパーコードは別の値に設定してください。
 - 強要コードとスーパーパスワードは、認証パスワードとは別の値に設定してください。
 - 強要コードとスーパーパスワードの長さは、デバイスにより異なります。通常は 4～8 桁で設定します。
-

5. [OK] をクリックします。
 6. オプション: [コピー先] をクリックしてドアを選択すると、ページ内のパラメータを選択したドアにコピーできます。
-


メモ

選択したドアには、ドアの状態継続時間の設定もコピーされます。

カードリーダーのパラメータ設定

入退室管理デバイスの追加後に、そのカードリーダーのパラメータを設定できるようになります。

手順

1. [入退室管理] → [詳細機能] → [デバイスパラメータ] の順にクリックします。
 2. 左側のデバイスリスト内で  をクリックしてドアの項目を展開し、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。
-

メモ

- 入退室管理デバイスごとに表示するパラメータが異なる場合があります。以下のようなパラメータがリスト表示されます。詳細については、デバイスのユーザーマニュアルをご覧ください。
 - 以下のパラメータの一部は [基本情報] ページにリスト表示されないため、パラメータを編集するには [詳細] をクリックしてください。
-

基本情報

名前

カードリーダー名を編集して希望する名前にします。

カードスワイプ最小間隔

同じカードのスワイプ間隔が設定値より短い場合、そのカードのスワイプが無効になります。0~255 の範囲で設定できます。

最大試行失敗回数アラーム

カードの読み取り試行回数が設定値に達した場合、アラーム通知が作動します。

カードリーダーのタイプ/カードリーダーの説明

カードリーダーのタイプと説明を示します。読み取りのみに対応しています。

指紋の容量

保存できる指紋の最大数を表示します。

Existing Fingerprint Number (既存の指紋数)

デバイスに保存されている既存の指紋の数を表示します。

詳細

カードリーダーの有効化

機能を有効にすれば、e デバイスをカードリーダーとして使用できます。

OK LED 極性/エラー LED 極性/ブザー極性

カードリーダーのパラメータに従って、メインボードの OK LED 極性/エラー LED 極性/ブザー極性を設定します。一般にはデフォルト設定を適用します。

パスワード入力時の最長間隔

カードリーダーにパスワードを入力する時に入力する数字と数字の間隔が設定値より長い場合、直前に入力した数字が自動的に消去されます。

タンパー検知

カードリーダーの干渉検知を有効にします。

カード試行失敗最大許容回数

カード読み取りで許容する最大の試行回数を設定します。

指紋認識レベル

ドロップダウンリストから指紋の認証レベルを選択します。

顔 1:N マッチしきい値

1:N マッチモードで認証する場合に、一致セキュリティレベルを設定します。この値が大きいほど認証時の他人受入率は低下し、本人拒否率は上昇します。

顔認識間隔

認証時における 2 つの連続する顔認識の実行間隔を示します。デフォルト値は 2 秒です。

顔アンチスプーフィング

顔アンチスプーフィング機能を有効化または無効化します。この機能を有効にすると、認証対象が人間であるかどうかを識別できます。

顔 1:1 マッチしきい値

1:1 マッチモードで認証する場合に、認証のしきい値を設定します。この値が大きいほど認証時の他人受入率は低下し、本人拒否率は上昇します。

アプリケーションモード

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

顔のロック認証に失敗

ライブ顔検知機能を有効化した場合、設定した試行回数を超えてライブ顔検知に失敗するとそのユーザーの顔の使用が 5 分間ロックされます。その間には、本物であると認証されなかったその顔で、同じユーザーが試行しても認証されません。5 分以内に、本物の顔を使用して 2 回連続で認証に成功するとロックが解除されます。

生体検知セキュリティレベル

[生体顔認証] 機能を有効にすると、生体顔認証の実行時に作動する一致セキュリティのレベルを設定できます。

4. [OK] をクリックします。
5. オプション: [コピー先] をクリックしてカードリーダーを選択すると、ページ内のパラメータを選択したカードリーダーにコピーできます。

8.7.2 開放状態／閉鎖状態の設定

ドアの開放／閉鎖状態を設定できます。例えば、休日を閉鎖状態、仕事日の特定期間を開放状態に設定できます。

始める前に



システムに入退室管理デバイスを追加しておいてください。

手順

1. [入退室管理] → [詳細機能] → [開放状態／閉鎖状態] の順にクリックし、[開放状態／閉鎖状態] のページを開きます。
2. 左側のパネルで設定が必要なドアを選択します。
3. 仕事日の間にドアの状態を設定するには、[Week Schedule (週スケジュール)] をクリックして以下の操作を実行します。
 - 1) [開放状態] または [閉鎖状態] をクリックします。
 - 2) カーソルで時間帯をドラッグ操作して、設定したアクセスグループがその時間中はアクティブの状態になるようにします。

 **メモ**

週のスケジュールでは、各日あたり最大 8 つの時間帯を設定できます。

- 3) オプション: 以下の操作を実行すると、時間帯を編集できます。
- カーソルを時間帯に移動し、カーソルが  に切り替わると、タイムラインバーの時間帯をドラッグして目的の位置へ移動します。
 - 時間帯をクリックし、ダイアログが表示されたら開始時間／終了時間を直接編集します。
 - カーソルを時間帯の開始時間または終了時間に移動し、カーソルが  に変わると、ドラッグ操作で時間帯を延長または短縮できます。
- 4) **[保存]** をクリックします。



関連操作




- | | |
|----------------|--|
| 週全体にコピー | タイムバー上で 1 つの時間帯を選択して [週全体をコピー] をクリックすると、このタイムバー上のすべての時間帯設定を別の仕事日にコピーできます。 |
| 選択対象を削除 | タイムバー上で 1 つの時間帯を選択し、 [選択対象を削除] をクリックすると、その時間帯を削除できます。 |
| 消去 | [消去] をクリックすると、週のスケジュール内のすべての時間帯設定を消去できます。 |

4. 休日のドアの状態を設定するには、**[休日]** をクリックして以下の操作を実行します。
- 1) **[開放状態]** または **[閉鎖状態]** をクリックします。
 - 2) **[追加]** をクリックします。
 - 3) 開始日と終了日を入力します。
 - 4) カーソルで時間帯をドラッグ操作して、設定したアクセスグループがその時間中はアクティブの状態になるようにします。
-

 **メモ**

休日 1 期間に対して最大 8 つの休時間帯を設定できます。

- 5) 時間帯を編集するには、以下の操作を実行します。
- カーソルを時間帯に移動し、カーソルが  に切り替わると、タイムラインバーの時間帯をドラッグして目的の位置へ移動します。
 - 時間帯をクリックし、ダイアログが表示されたら開始時間／終了時間を直接編集します。
 - カーソルを時間帯の開始時間または終了時間に移動し、カーソルが  に変わると、ドラッグ操作で時間帯を延長または短縮できます。
-

- 6) オプション: 削除する時間帯を選択し、[操作] 列で  をクリックすると選択した時間帯を削除できます。
 - 7) オプション: [操作] 列で  をクリックすると、タイムバー内の時間帯をすべて削除できます。
 - 8) オプション: [操作] 列で  をクリックすると、追加した休日を休日リストから削除できます。
 - 9) [保存] をクリックします。
5. オプション: [コピー先] をクリックすると、このドアの状態設定を別のドアにコピーできます。

8.7.3 多要素認証の設定

グループ別に人物を管理して、1 つの入退室管理ポイント（ドア）に対する複数名の認証を設定できます。

始める前に

アクセスグループを設定し、そのアクセスグループを入退室管理デバイスに適用します。詳細については、「アクセスグループの設定によるアクセス認証の人物への割り当て」をご覧ください。

単一の入退室管理ポイント（ドア）に対して複数のカードの認証を設定する場合、このタスクを実行してください。

手順

1. [入退室管理] → [詳細機能] → [Multi-Factor Auth（多要素認証）] の順にクリックします。
2. 左側のパネルで、デバイスリストの中から入退室管理デバイスを選択します。
3. この入退室管理デバイスに人物／カードのグループを追加します。
 - 1) 右側のパネルにある [追加] をクリックします。
 - 2) 希望するグループ名を作成します。
 - 3) その人物／カードのグループに適用する有効期間の開始時間と終了時間を指定します。
- 4) [利用可能] リスト内でメンバーおよびカードを選択して [選択済み] リストに追加します。

メモ

その人物にカードを発行済みであることを確認してください。
アクセスグループを設定し、そのアクセスグループを入退室管理デバイスへ適用済みであることを確認してください。

- 5) [保存] をクリックします。

- 6) オプション: 人物／カードのグループを選択し、[削除] をクリックすると、その項目を削除できます。
- 7) オプション: 人物／カードのグループを選択して [適用] をクリックすると、適用に失敗したアクセスグループを入退室管理デバイスへ再適用できます。
4. 左側のパネルで、選択したデバイスの入退室管理ポイント（ドア）を選択します。
5. パスワード入力時の最大間隔を入力します。
6. 選択した入退室管理ポイントに使用する認証グループを追加します。
 - 1) [認証グループ] パネルで [追加] をクリックします。
 - 2) ドロップダウンリストの中から設定したテンプレートを選択し、認証テンプレートに設定します。

メモ

テンプレート設定の詳細については、「スケジュールとテンプレートの設定」をご覧ください。

- 3) ドロップダウンリストの中から、認証タイプとして[ローカル認証]、[ローカル認証とリモートでドアを開放]、または [ローカル認証とスーパーパスワード] を選択します。

ローカル認証

入退室管理デバイスごとの認証設定を示します。

ローカル認証およびリモートでドアを開放

入退室管理デバイス別およびクライアント別の認証設定を示します。デバイスにカードをスワイプすると、ウィンドウがポップアップ表示されます。クライアント経由でドアを解錠できます。

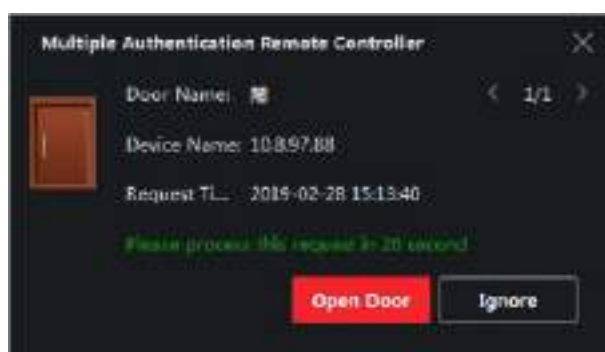


図 8-3 リモートでドアを開放

メモ

入退室管理デバイスがクライアントに接続されていない場合、[オフライン認証] にチェックを入れるとスーパーパスワード認証を有効化できます。

ローカル認証およびスーパーパスワード

入退室管理デバイス別、およびスーパーパスワード別の認証設定を示します。

- 4) 左側のリストで追加した人物／カードのグループを選択すると、認証グループとして右側の [選択済み] リストに追加されます。
- 5) 右側のリスト内で追加した認証グループをクリックし、[Auth Times (認証回数)] 列で認証回数を設定します。

メモ

- 認証回数は、0 より大きく、人物グループに追加した人数より小さく設定してください。
- 認証回数は最大 16 回です。

-
- 6) [保存] をクリックします。

メモ

- 各入退室管理ポイント（ドア）に対して、認証グループを最大 4 つ追加できます。
- 認証タイプが [ローカル認証] の認証グループには、人物／カードのグループを最大 8 件追加できます。
- 認証タイプが [ローカル認証とスーパーパスワード] または [ローカル認証とリモートでドアを開放] の認証グループには、人物／カードのグループを最大 7 件追加できます。

-
7. [保存] をクリックします。

8.7.4 Wiegand ルールのカスタム設定

サードパーティ製 Wiegand 規格のアップロードルールを理解すると、デバイスとサードパーティ製カードリーダー間の通信に利用する Wiegand 規格のルールを複数カスタマイズできます。

始める前に

デバイスにサードパーティ製カードリーダーを配線します。

手順

メモ

- デフォルトでは Wiegand のカスタム機能は無効化されています。Wiegand のカスタム機能を有効にすると、カスタマイズした Wiegand プロトコルをデバイス内のすべての Wiegand インターフェースで使用できます。
 - 最大 5 つのカスタム Wiegand を設定できます。
 - Wiegand のカスタマイズ設定の詳細については、「Wiegand ルールのカスタマイズ設定」セクションの説明をご覧ください。
-

1. [入退室管理] → [詳細機能] → [Custom Wiegand (カスタム Wiegand)] の順にクリックし、[Custom Wiegand (カスタム Wiegand)] のページを開きます。
2. 左側で [Custom Wiegand (カスタム Wiegand)] を選択します。
3. Wiegand の名前を作成します。

メモ

カスタム Wiegand 名には最大 32 文字まで使用できます。

4. [デバイスを選択] をクリックして、カスタム Wiegand を設定する入退室管理デバイスを選択します。
5. サードパーティ製カードリーダーのプロパティに応じて、パリティモードを設定します。

メモ

- 合計長は最大 80 ビットです。
 - 奇数パリティのスタートビット、奇数パリティの長さ、偶数パリティのスタートビット、偶数パリティの長さは、1 から 80 ビットまでで設定します。
 - カード ID、メーカーコード、サイトコード、OEM のスタートビットは、1 から 80 ビットまでの間で設定します。
-

6. 出力の変換ルールを設定します。
 - 1) [ルール設定] をクリックし、[出力変換ルール] を開きます。

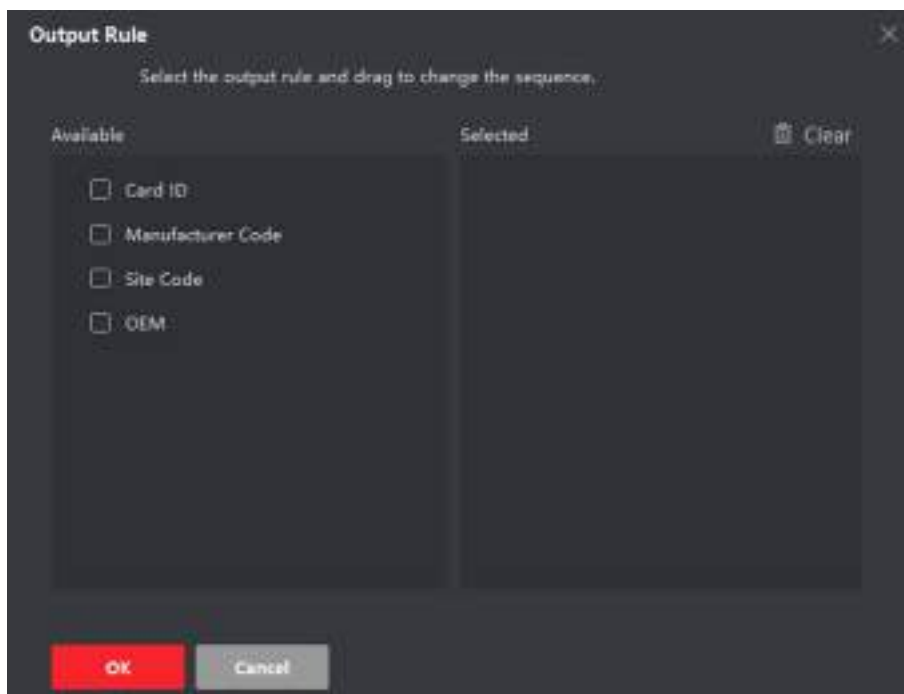


図 8-4 出力変換ルールを設定

- 2) 左側のリストからルールを選択します。
選択したルールは右側のリストに追加されます。
 - 3) オプション: ルールをドラッグすると、ルールの順番を変更できます。
 - 4) [OK] をクリックします。
 - 5) [Custom Wiegand (カスタム Wiegand)] タブで、ルールのスタートビット、長さ、および 10 進数字を設定します。
7. [保存] をクリックします。

8.7.5 人物の認証モードの設定

実際の使用状況に応じて、入退室管理デバイスで使用するカードリーダーの通過ルールを設定できます。

始める前に

入退室管理デバイスが人物の認証機能をサポートしていることを確認します。

手順

1. [入退室管理] → [詳細機能] → [認証] の順にクリックします。
2. 左側のパネルで入退室管理デバイス（人物の認証機能をサポート）を選択し、[人物認証モード] ページを表示します。
3. [追加] をクリックし、[追加] ウィンドウを開きます。
4. 左側のパネルで設定が必要な人物を選択します。
選択した人物は右側のパネルに追加されます。
5. [認証モード] のドロップダウンリストで認証モードを選択します。
6. [OK] をクリックします。

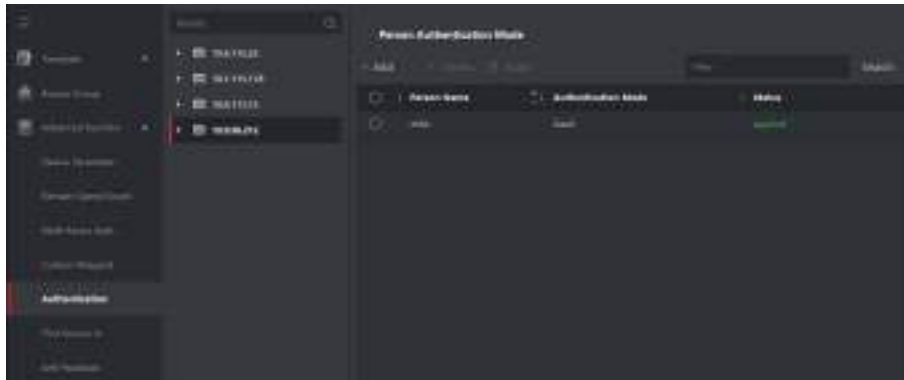


図 8-5 人物の認証モード設定

7. オプション: [人物の認証モード] ページで [人物] を選択し、[適用] をクリックして人物の認証モードをデバイスに適用します。

 **メモ**

人物の認証は、他の認証モードよりも優先されます。入退室管理デバイスが人物の認証モードに設定されている場合、人物は、人物の認証モードを使用してこのデバイスで認証を受ける必要があります。

8.7.6 カードリーダーの認証モードおよびスケジュールの設定

実際の使用状況に応じて、入退室管理デバイスで使用するカードリーダーの通過ルールを設定できます。

手順

1. [入退室管理] → [詳細機能] → [認証] の順にクリックし、認証モード設定ページを開きます。
2. 左側でカードリーダーを選択して設定します。
3. カードリーダーの認証モードを設定します。
 - 1) [設定] をクリックします。

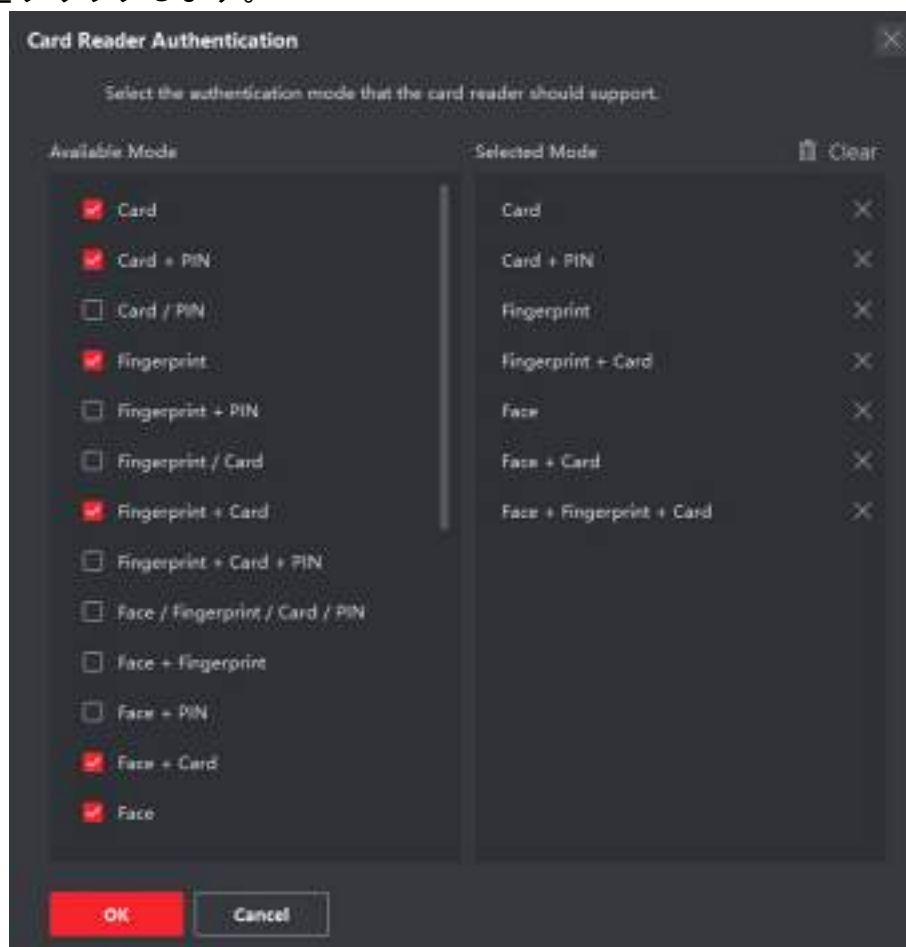


図 8-6 カードリーダー認証モードの選択

 **メモ**

PIN は、ドアを開くための PIN コードを意味しています。詳細については、「**入退室管理情報の設定**」をご覧ください。

- 2) [Available Mode (利用可能モード)] のリスト内のモードにチェックを入れると、そのモードが選択したモードリストに追加されます。
- 3) [OK] をクリックします。
モードを選択すると、そのモードが別の色でアイコンとして表示されます。
4. アイコンをクリックしてカードリーダーの認証モードを選択した後に、カーソルをドラッグしてスケジュール上にカラーバーを引いて期間を指定すると、その期間はカードリーダーの認証が有効になります。
5. 他の期間を設定する場合、上記の手順を繰り返してください。

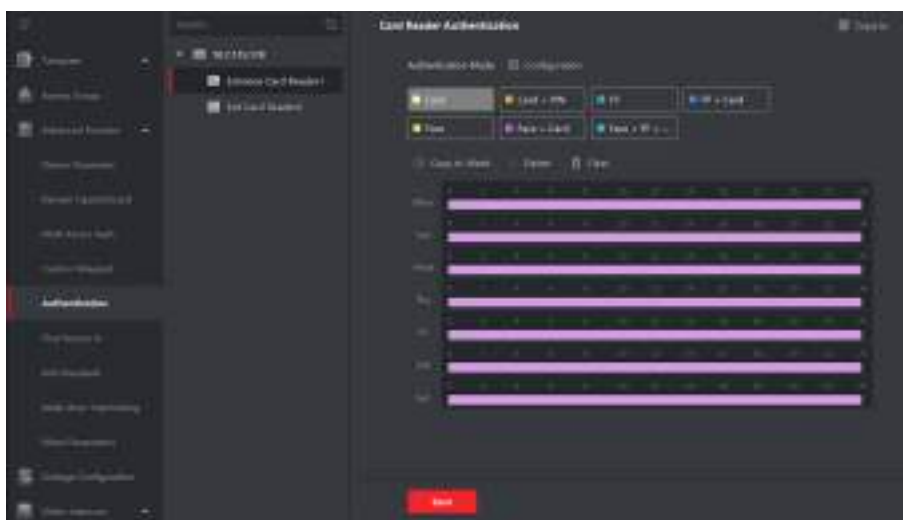


図 8-7 カードリーダーの認証モード設定

6. オプション: 設定済みの日付を選択して [週全体にコピー] をクリックすると、同じ設定を週全体にコピーできます。
7. オプション: [コピー先] をクリックすると、その設定を他のカードリーダーにコピーできます。
8. [保存] をクリックします。

8.7.7 最初の人物の入室設定

1 つの入退室管理ポイントに対して、最初にアクセスする人物を複数設定できます。最初の人物が認証された後に、複数名のアクセスなどの認証動作が許可されます。

始める前に

アクセスグループを設定して、そのアクセスグループを入退室管理デバイスに適用します。詳細については、「**アクセスグループの設定によるアクセス認証の人物への割り当て**」をご覧ください。

最初の人物によるドア開放を設定する時に、このタスクを実行してください。

手順

1. **[入退室管理]** → **[詳細機能]** → **[First Person In (最初の人物の入室)]** の順にクリックし、**[First Person In (最初の人物の入室)]** ページを開きます。
2. 左側のパネルで、リストの中から入退室管理デバイスを選択します。
3. 選択したデバイスの各入退室管理ポイントに対して、現在のモードとしてドロップダウンリストの中から **[Enable Remaining Open after First Person (最初の人物の後、開放状態を有効にする)]** または **[Disable Remaining Open after First Person (最初の人物の後、開放状態を無効にする)]** を選択します。

Enable Remaining Open after First Person (最初の人物の後、開放状態を有効にする)

最初の人物の認証後、開放状態の継続時間が終了するまでドアの開放が保持されます。このモードを選択した場合、開放継続時間を設定してください。

メモ

開放状態の継続時間は、0 から 1440 分までです。デフォルトでは、開放状態の継続時間は 10 分に設定されています。

Disable Remaining Open after First Person (最初の人物の後、開放状態を無効にする)

最初の人物の入室に関する設定を無効化して、通常の認証に切り替えます。

メモ

最初の人物モードを無効化するために、最初の人物で再認証することもできます。

4. **[First Person List (最初の人物リスト)]** パネルで **[追加]** をクリックします。
5. 左側のリスト内で人物を選択すると、ドアの最初の人物としてその人物が選択済み人物に追加されます。
追加した最初の人物は、**[First Person List (最初の人物リスト)]** に表示されます。
6. オプション: リストから最初の人物を選択して **[削除]** をクリックすると、最初の人物リストからその人物を削除できます。
7. **[保存]** をクリックします。

8.7.8 アンチパスバックの設定

指定パスのみで入退室管理ポイントを通過できて、カードのスイープで 1 名のみが入退室管理ポイントを通過できるように設定できます。

始める前に

入退室管理デバイスのアンチパスバック機能を有効にします。

入退室管理デバイスにアンチパスバック機能を設定する場合、このタスクを実行してください。

手順

メモ

1 台の入退室管理デバイスに対して、アンチパスバック機能または複数ドアのインターロック機能を同時に設定できます。複数ドアのインターロック設定については、ユーザーマニュアルの該当するセクションをご覧ください。

1. [入退室管理] → [詳細機能] → [アンチパスバック] の順にクリックし、[アンチパスバック設定] ページを開きます。
 2. リストで入退室管理デバイスを選択します。
 3. [First Card Reader (最初のカードリーダー)] フィールド内でパスの最初に記載するカードリーダーを選択します。
 4. [後続カードリーダー] 列で、選択済みカードリーダーのテキストフィールドをクリックして [カードリーダーの選択] ダイアログを開きます。
 5. 最初のカードリーダーの後続となるカードリーダーを選択します。
-

メモ

1 台のカードリーダーに対して、後続のカードリーダーを最大 4 台まで追加できます。

6. ダイアログ内で [OK] をクリックし、選択情報を保存します。
 7. [アンチパスバック] ページの右上にある [保存] をクリックして設定を保存し、その設定を有効化します。
-

メモ

スーパーカード、スーパーパスワード、スーパーフィンガープリントなどのスーパークレデンシャルには、アンチパスバックルールに準拠しない権限があります。

例

カードスワイプのパスを設定します。最初のパスとして「Reader In_01」を、関連付けカードリーダーとして「Reader In_02」と「Reader Out_04」を選択すると仮定します。この場合、「Reader In_01」、「Reader In_02」、「Reader Out_04」の順にカードをスワイプした場合に限り、入退室管理ポイントを通過できます。

8.7.9 デバイスパラメータの設定

入退室管理デバイスの追加後に、ネットワークパラメータなどの各種パラメータを設定できるようになります。

複数の NIC パラメータの設定

デバイスが複数のネットワークインターフェースに対応している場合、クライアント側で IP アドレス、MAC アドレス、ポート番号などの NIC ネットワークのパラメータを設定できます。

手順

メモ

使用するデバイスがこの機能に対応している必要があります。

1. [入退室管理] 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] → [詳細パラメータ] の順に入ります。
3. デバイスリスト内で入退室管理デバイスを選択して [NIC] をクリックし、[Multiple NIC Settings (複数の NIC パラメータ)] ページを開きます。
4. ドロップダウンリストから、設定する NIC を選択します。
5. 該当する IP アドレス、デフォルトゲートウェイ、サブネットマスクなどのネットワークパラメータを設定します。

MAC アドレス

メディア入退室管理アドレス (MAC アドレス) は、物理的なネットワークセグメント上での通信のために、ネットワークインターフェースに割り当てられる一意の識別子です。

MTU

ネットワークインターフェースの最大転送単位 (MTU) を示します。

6. [保存] をクリックします。

ネットワークパラメータの設定

入退室管理デバイスの追加後は、デバイスログのアップロードモードを設定して、有線ネットワーク経由で EHome アカウントを作成できるようになります。

ログのアップロードモード設定

デバイスが EHome プロトコル経由でログをアップロードするモードを設定できます。

手順

メモ

EHome によってデバイスが追加されていないことを確認してください。

1. [入退室管理] 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] → [詳細パラメータ] の順に入ります。
 3. デバイスリスト内で入退室管理デバイスを選択し、[ネットワーク] → [アップロードモード] の順に移動します。
 4. ドロップダウンリストからセンターグループを選択します。
 5. [有効] にチェックを入れてアップロードモードの設定を有効化します。
 6. ドロップダウンリストからアップロードモードを選択します。
 - メインチャンネルまたはバックアップチャンネル用に [N1] または [G1] を有効化します。
- [閉じる] を選択してメインチャンネルまたはバックアップチャンネルを無効化します。
-

メモ

- メインチャンネルとバックアップチャンネルで同時に N1 または G1 を有効化することはできません。
 - N1 は有線ネットワーク、G1 は GPRS を指します。
-

7. [保存] をクリックします。

有線通信モードでの EHome アカウントの作成

有線通信モードでは、EHome プロトコル用のアカウントを設定できます。その後に EHome プロトコルでデバイスを追加します。

手順

メモ

- 使用するデバイスがこの機能に対応している必要があります。
 - EHome によってデバイスが追加されていないことを確認してください。
-

1. [入退室管理] 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] → [詳細パラメータ] の順に入ります。
 3. デバイスリスト内で入退室管理デバイスを選択し、[ネットワーク] → [ネットワークセンター] の順に入ります。
 4. ドロップダウンリストからセンターグループを選択します。
 5. [アドレスタイプ] で [IP アドレス] または [ドメイン名] を選択します。
 6. アドレスタイプに応じて、IP アドレスまたはドメイン名を入力します。
 7. プロトコルのポート番号を入力します。
-

 **メモ**

無線および有線ネットワークのポート番号は、EHome のポート番号と一致させてください。

8. [プロトコルタイプ] で [EHome] を選択し、EHome バージョンを選択します。
-

 **メモ**

EHome バージョンを 5.0 に設定する場合は、EHome アカウントの EHome キーを作成する必要があります。

9. ネットワークセンターのアカウント名を設定します。
10. [保存] をクリックします。

デバイスのキャプチャパラメータの設定

手動キャプチャやイベントトリガーのキャプチャなど、入退室管理デバイスのキャプチャパラメータを設定できます。

 **メモ**

- 使用するデバイスがこのキャプチャ機能に対応している必要があります。
 - キャプチャパラメータの設定前に、画像ストレージを設定し、イベントトリガー画像の保存場所を定義しておく必要があります。詳細については、クライアントソフトウェアのユーザーマニュアルに記載の「画像ストレージの設定」をご覧ください。
-

トリガーされたキャプチャパラメータの設定

イベントが発生すると、入退室管理デバイスに搭載のカメラがトリガーされて画像をキャプチャし、イベント発生時の出来事を記録します。[イベントセンター] のイベント詳細を確認すると、キャプチャ画像を閲覧できます。その前に、一度にキャプチャする画像枚数などのキャプチャパラメータを設定しておく必要があります。

始める前に

キャプチャパラメータの設定前に、画像ストレージを設定し、キャプチャ画像の保存場所を定義しておく必要があります。詳細については、クライアントソフトウェアのユーザーマニュアルに記載の「画像ストレージの設定」をご覧ください。

手順

 **メモ**

使用するデバイスがこの機能に対応している必要があります。

1. [入退室管理] 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] → [詳細パラメータ] → [キャプチャ] の順に開きます。
3. デバイスリスト内で入退室管理デバイスを選択し、[リンクキャプチャ] を選択します。
4. 画像サイズと画質を設定します。
5. トリガー後のキャプチャ回数を設定し、一度にキャプチャする枚数を定義します。
6. キャプチャ回数が 1 より大きい場合、キャプチャの間隔を設定してください。
7. [保存] をクリックします。

手動キャプチャのパラメータ設定

[状態モニター] モジュールでは、入退室管理デバイスに搭載のカメラのボタンをクリックして画像を手動でキャプチャすることができます。その前に、画質などのキャプチャパラメータを設定しておく必要があります。

始める前に

キャプチャパラメータの設定前に、保存先パスを設定し、キャプチャ画像の保存場所を定義しておく必要があります。詳細については、クライアントソフトウェアのユーザーマニュアルに記載の「**画像ストレージの設定**」をご覧ください。

手順



使用するデバイスがこの機能に対応している必要があります。

1. [入退室管理] 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] → [詳細パラメータ] → [キャプチャ] の順に開きます。
3. デバイスリスト内で入退室管理デバイスを選択し、[手動キャプチャ] を選択します。
4. ドロップダウンリストから、キャプチャ画像の解像度を選択します。
5. 画質として [高]、[中]、または [低] を選択します。画質が高いほど、画像サイズは大きくなります。
6. [保存] をクリックします。

顔認識端末のパラメータの設定

顔認識端末のパラメータを設定できます。

手順



使用するデバイスがこの機能に対応している必要があります。

1. [入退室管理] 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] → [詳細パラメータ] の順に移動します。
 3. デバイスリスト内で入退室管理デバイスを選択し、[顔認識端末] をクリックします。
 4. パラメータを設定します。
-

メモ

デバイスのモデルによって表示されるパラメータは異なります。

アルゴリズム

顔画像データベースで [ディープラーニング] を選択します。

認証中の顔画像を保存

有効化すると、認証中のキャプチャされた顔画像がデバイスに保存されます。

ECO モード

ECO モードを有効にすると、光が弱かったり暗かったりする状態でも顔認証を実行できます。また、ECO モードのしきい値、ECO モード (1:N)、ECO モード (1:1) を設定できます。

メモ

ECO モードのパラメータ設定は、通常モードのデバイスでのみ行うことができます。

動作モード

デバイスの動作モードを [入退室管理モード] に設定します。デバイスの標準は、入退室管理モードです。アクセスするには認証情報の認証が必要です。

5. [保存] をクリックします。

RS-485 パラメータの設定

入退室管理デバイスの RS-485 パラメータを設定します。例えば、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、接続モードなどが該当します。

手順

メモ

使用するデバイスが RS-485 の設定に対応している必要があります。

1. [入退室管理] 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]** → **[詳細パラメータ]** の順に移動します。
3. デバイスリスト内で入退室管理デバイスを選択して **[RS-485]** をクリックし、**[RS-485 設定]** ページを開きます。
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 のパラメータを設定します。
5. ドロップダウンリストで、ボーレート、データビット、ストップビット、パリティタイプ、通信モード、動作モード、接続モードを設定します。
6. **[保存]** をクリックします。
 - 設定したパラメータはデバイスへ自動適用されます。
 - 動作モードまたは接続モードの変更後、デバイスは自動的に再起動します。

Wiegand パラメータの設定

入退室管理デバイスの Wiegand チャンネルと通信モードを設定できます。Wiegand パラメータの設定後は、Wiegand 通信で Wiegand 規格のカードリーダーにデバイスを接続できるようになります。

手順

メモ

使用するデバイスがこの機能に対応している必要があります。

1. **[入退室管理]** 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]** → **[詳細パラメータ]** の順に移動します。
3. デバイスリスト内で入退室管理デバイスを選択して **[Wiegand]** をクリックし、**[Wiegand Settings (Wiegand 設定)]** ページを開きます。
4. スイッチを **[ON]** にしてデバイスの Wiegand 機能を有効にします。
5. ドロップダウンリストから Wiegand のチャンネル番号と通信モードを選択します。

メモ

[Communication Direction (通信方向)] を **[Sending (送信)]** に設定する場合、**[Wiegand モード]** を **[Wiegand 26]** または **[Wiegand 34]** に設定する必要があります。

6. **[Enable Wiegand (Wiegand を有効化)]** にチェックを入れて Wiegand 機能を有効化します。
7. **[保存]** をクリックします。
 - 設定したパラメータはデバイスへ自動適用されます。
 - 通信方向の変更後、デバイスは自動的に再起動します。

M1 カードの暗号化を有効にする

M1 カードを暗号化すると、認証のセキュリティレベルが向上します。

手順

メモ

入退室管理デバイスとカードリーダーがこの機能に対応している必要があります。

1. [入退室管理] 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] → [詳細パラメータ] の順に移動します。
 3. デバイスリスト内で入退室管理デバイスを選択して [M1 カード暗号化] をクリックし、[M1 カード暗号化] ページを開きます。
 4. スイッチを [ON] にして 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。
-

メモ

- セクター ID は、1~100 の範囲で設定します。
 - デフォルトでは、セクター 13 は暗号化されています。セクター 13 を暗号化することをお勧めします。
-

6. [保存] をクリックして設定を保存します。

8.8 入退室管理のリンク操作設定

入退室管理デバイスが検知したイベントに対して、異なるリンク操作を設定できます。設定後、イベント発生時にリンク操作がトリガーされます。この仕組みは、セキュリティ担当者にイベントを通知したり、リアルタイムで自動入退室管理をトリガーするために使用します。

サポートされているリンク操作は以下の 2 種類です。

- **クライアント操作:** イベントが検知されると、クライアントによる音声警告など、クライアント側の動作を実行します。
- **デバイス操作:** イベントが検知されると、カードリーダーのブザーやドアの開放/閉鎖など、特定デバイスの動作を実行します。

8.8.1 アクセスイベントに対するクライアント操作の設定

アクセスポイントから遠く離れている場合にも、クライアント側でアクセスイベントのリンク操作を設定することで、何が起きているか、そしてそのイベントの緊急度を把握できます。イベントに即応できるように、イベント発生時にクライアント側で通知を受け取ります。アクセスポイントのクライアント操作を一度に一括で設定することもできます。

手順

メモ

ここで説明するリンク操作とは、音声による警告や電子メールリンクなど、クライアントソフトウェア独自の動作に対するリンクを指しています。

1. **[イベント管理]** → **[入退室管理イベント]** の順にクリックします。
追加した入退室管理デバイスがデバイスリストに表示されます。
2. デバイスリストからリソース（例: デバイス、アラーム入力、ドア/エレベータ、カードリーダー）を選択します。
選択したリソースが対応するイベントの種類が表示されます。
3. イベントを選択して **[優先度の編集]** をクリックし、そのイベントの優先度を定義します。この設定は、**[イベントセンター]** でイベントをフィルタする時に使用します。
4. 選択したイベントのリンク操作を設定します。
 - 1) イベントを選択して **[リンクを編集]** をクリックし、イベント発生時のクライアント側の動作を設定します。

音声による警告

アラームが作動すると、クライアントソフトウェアが音声による警告を実施します。警告に使用するアラーム音を選択できます。

メモ

アラーム音の設定については、クライアントソフトウェアのユーザーマニュアルに記載の「**アラーム音の設定**」をご覧ください。

電子メールの送信

アラーム情報を電子メールで 1 名以上のユーザーに送信します。

電子メールパラメータの設定の詳細については、クライアントソフトウェアのユーザーマニュアルに記載の「**電子メールのパラメータ設定**」をご覧ください。

- 2) **[OK]** をクリックします。
5. イベントを有効化すると、イベントの検知時にイベントがクライアントに送信され、リンク操作がトリガーされます。
6. オプション: **[コピー先...]** をクリックすると、イベントの設定を他の入退室管理デバイス、アラーム入力、ドア、またはカードリーダーにコピーできます。

8.8.2 アクセスイベントに対するデバイス操作の設定

入退室管理デバイスのトリガーイベントに対して、入退室管理デバイスのリンク操作を設定できます。イベントがトリガーされると、同じデバイスでアラーム出力、ホストブザーなどの動作が実行されます。

手順

メモ

使用するデバイスがこの機能に対応している必要があります。

1. [入退室管理] → [リンク設定] の順にクリックします。
2. 左側のリストで入退室管理デバイスを選択します。
3. [追加] ボタンをクリックして新しいリンクを追加します。
4. イベントソースで [イベントリンク] を選択します。
5. イベントタイプと詳細を選択してリンクを設定します。
6. [対象リンク] エリアでプロパティ対象を設定し、この操作を有効化します。

コントローラのブザー

入退室管理デバイスの音声による警告がトリガーされます。

キャプチャ

リアルタイムキャプチャがトリガーされます。

アクセスポイント

ドアの状態（開放、閉鎖、開放状態、閉鎖状態）がトリガーされます。

メモ

対象のドアとソースドアは同じにできません。

7. [保存] をクリックします。
8. オプション: デバイスのリンク設定を追加した後に、以下の操作を 1 つまたは複数実行できるようになります。

リンク設定の編集 デバイスリスト内で設定済みのリンクを選択すると、そのイベントソースのパラメータ（イベントソースや対象リンクなど）を編集できます。

リンク設定の削除 デバイスリスト内で設定済みのリンクを選択して [削除] をクリックすると、その設定を削除できます。

8.8.3 カードのスイープ動作に対するデバイス操作の設定

特定のカードのスイープ動作に対して、入退室管理デバイスのリンク操作を設定できます。特定のカードでスイープすると、同じデバイスでホストブザーなどの動作がトリガーされます。

手順

メモ

使用するデバイスがこの機能に対応している必要があります。

1. [入退室管理] → [リンク設定] の順にクリックします。
2. 左側のリストで入退室管理デバイスを選択します。
3. [追加] ボタンをクリックして新しいリンクを追加します。
4. イベントソースで [Card Linkage (カードリンク)] を選択します。
5. カード番号を入力するか、ドロップダウンリストから該当するカードを選択します。
6. カードをスイープしてリンク操作をトリガーさせるカードリーダーを選択します。
7. [対象リンク] エリアでプロパティ対象を設定し、この操作を有効化します。

コントローラのブザー

入退室管理デバイスの音声による警告がトリガーされます。

キャプチャ

リアルタイムキャプチャがトリガーされます。

アクセスポイント

ドアの状態（開放、閉鎖、開放状態、または閉鎖状態）が作動します。

8. [保存] をクリックします。
（手順 5 で設定した）カードを（手順 6 で設定した）カードリーダーにスイープすると、（手順 7 で設定した）リンク操作がトリガーされます。
9. オプション: デバイスのリンク設定を追加した後に、以下の操作を 1 つまたは複数実行できるようになります。

リンク設定の削除 デバイスリスト内で設定済みのリンクを選択して [削除] をクリックすると、その設定を削除できます。

リンク設定の編集 デバイスリスト内で設定済みのリンクを選択すると、そのイベントソースのパラメータ（イベントソースや対象リンクなど）を編集できます。

8.8.4 人物 ID に対するデバイス操作の設定

特定の人物 ID に対して、入退室管理デバイスのリンク操作を設定できます。入退室管理デバイスは、指定された人物 ID を検知すると、カードリーダーのブザーやその他の操作をトリガーすることができます。

手順

メモ

使用するデバイスがこの機能に対応している必要があります。

1. [入退室管理] → [リンク設定] の順にクリックします。
2. 左側のリストで入退室管理デバイスを選択します。
3. [追加] をクリックして新しいリンクを追加します。
4. イベントソースで [Person Linkage (人物リンク)] を選択します。
5. 従業員番号を入力するか、ドロップダウンリストから該当する従業員を選択します。
6. カードをスワイプするカードリーダーを選択します。
7. [対象リンク] エリアでプロパティ対象を設定し、この操作を有効化します。

コントローラのブザー

入退室管理デバイスの音声による警告がトリガーされます。

リーダーのブザー

カードリーダーの音声による警告がトリガーされます。

キャプチャ

選択されたイベントが発生すると、イベントに関連する画像をキャプチャします。

録画

選択されたイベントが発生すると、イベントに関連する画像をキャプチャします。

メモ

使用するデバイスが録画機能に対応している必要があります。

アクセスポイント

ドアの状態（開放、閉鎖、開放状態、または閉鎖状態）が作動します。

8. [保存] をクリックします。

9. オプション: デバイスのリンク設定を追加した後に、以下の操作を 1 つまたは複数実行できるようになります。

リンク設定の削除 デバイスリスト内で設定済みのリンクを選択して [削除] をクリックすると、その設定を削除できます。

リンク設定の編集 デバイスリスト内で設定済みのリンクを選択すると、そのイベントソースのパラメータ（イベントソースや対象リンクなど）を編集できます。

8.9 ドアの状態の制御

開放、閉鎖、開放状態、閉鎖状態など、1 つのドアの状態を制御できます。

手順

1. [監視中] をクリックし、[status monitoring（状態の監視中）] ページを開きます。
2. 右上隅でアクセスポイントのグループを選択します。

メモ

アクセスポイントのグループ管理については、クライアントソフトウェアのユーザーマニュアルに記載の「グループ管理」をご覧ください。

選択した入退室管理グループ内のドアが表示されます。

3. ドアのアイコンをクリックしてドアを 1 つ選択するか、[Ctrl] を押しながら複数のドアを選択します。
4. 以下のボタンをクリックしてドアを制御します。

ドアを開放

ドアがロックされている場合、ロック解除して一度開きます。開放継続時間の経過後、自動的にドアが閉じて施錠されます。

ドアを閉鎖

ドアのロックが解除されている場合、ドアをロックするとドアが閉じます。アクセス認証の権限を有する人物は、認証情報を使用してドアにアクセスできます。

開放状態

（閉鎖または開放の場合を問わず）ドアはロック解除されます。認証情報は不要で、すべての人物がドアにアクセスできます。

閉鎖状態

ドアが閉じ、ロックされます。スーパーユーザーを除き、認証権限を有するユーザーでもドアにはアクセスできません。

キャプチャ

画像を手動でキャプチャします。

メモ

使用するデバイスがキャプチャ機能に対応している場合にのみ、この[キャプチャ]ボタンを使用できます。キャプチャした画像は、クライアントを実行中の PC に保存されます。保存先パスの設定については、クライアントソフトウェアのユーザーマニュアルに記載の「ファイルの保存先パスの設定」をご覧ください。

結果

正常に操作が行われると、操作の内容に応じてドアのアイコンがリアルタイムで変更されます。

8.10 イベントセンター

イベントセンターでは、リアルタイムイベントの表示、履歴イベントの検索、ポップアップアラーム情報の表示を行うことができます。


クライアントがデバイスからイベント情報を受信するには、デバイスを有効化する必要があります。詳細については、「デバイスからのイベント受信の有効化」を参照してください。

ポップアップアラーム情報を表示するには、イベントセンターでアラームトリガーポップアップ画像を有効にする必要があります。詳細については以下を参照してください。

8.10.1 デバイスからのイベント受信の有効化

クライアントがデバイスからイベント情報を受信するには、デバイスを有効化する必要があります。

手順

1.  → [ツール] → [デバイス警戒制御] の順にクリックし、[デバイス警戒制御] ページを開きます。
このページには追加したすべてのデバイスが表示されます。
2. [操作] 列で自動警戒有効化をオンにするか、[すべて警戒] をクリックしてすべてのデバイスに対する警戒を有効化します。

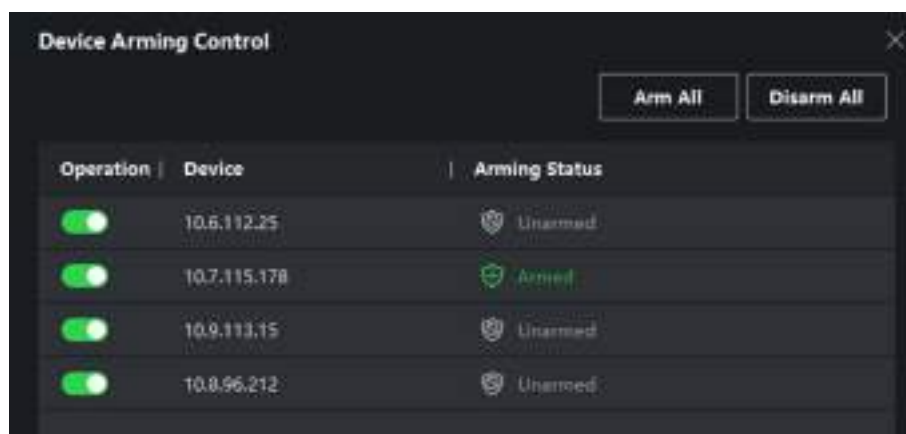


図 8-8 デバイス警戒制御

3. [警戒状態] 列で各デバイスの警戒状態を表示します。

結果

イベントがトリガーされると、警戒を有効化したイベントがクライアントに自動的にアップロードされます。

8.10.2 リアルタイムイベントの表示

イベントセンターページの [リアルタイムイベント] モジュール内では、イベントソース、イベント時間、優先、イベントのキーワードなど、イベントの各種情報をリアルタイムで表示できます。

始める前に

クライアントがデバイスからイベント情報を受信するには、そのデバイスのイベント受信を有効化する必要があります。詳細については、「デバイスからのイベント受信の有効化」をご覧ください。

手順

1. [イベントセンター] → [リアルタイムイベント] の順にクリックして [リアルタイムイベント] ページを開くと、クライアントが受信したリアルタイムイベントを確認できます。

イベント時間

ビデオデバイスのイベント時間は、クライアントがイベントを受信したクライアント時間を意味しています。ビデオ以外のデバイスのイベント時間は、イベントがトリガーされた時間を意味しています。

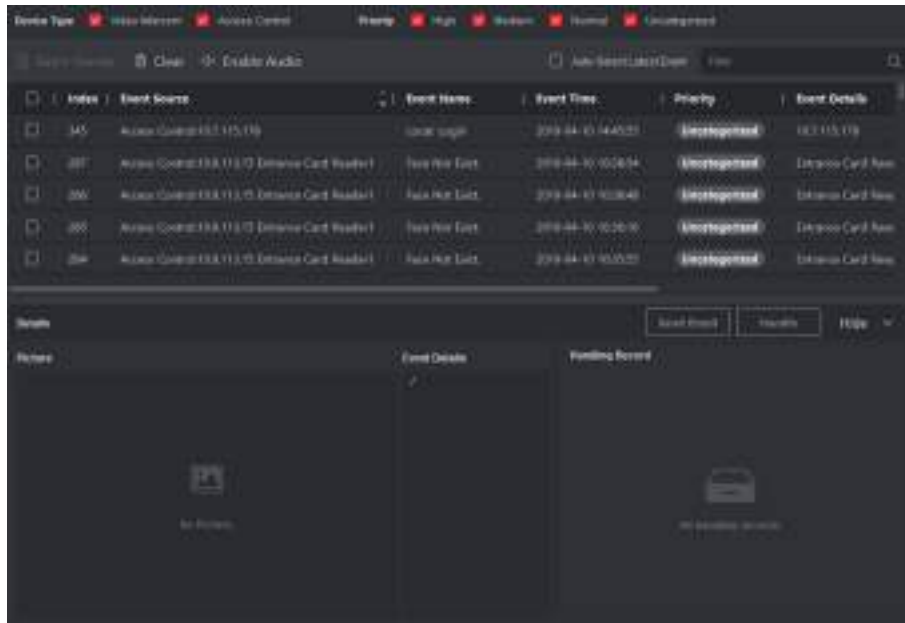


図 8-9 リアルタイムイベントの表示

2. フィルタ条件を設定するか、[フィルタ] テキストフィールドでイベントのキーワードを入力し、目的のイベントのみを表示させます。

デバイスタイプ

イベントが発生したデバイスのタイプを示します。

優先

イベントの緊急度を反映した優先度を示します。

3. オプション: イベントリスト表のヘッダ一部分を右クリックすると、イベント関連の項目をカスタマイズし、イベントリストに表示させることができます。

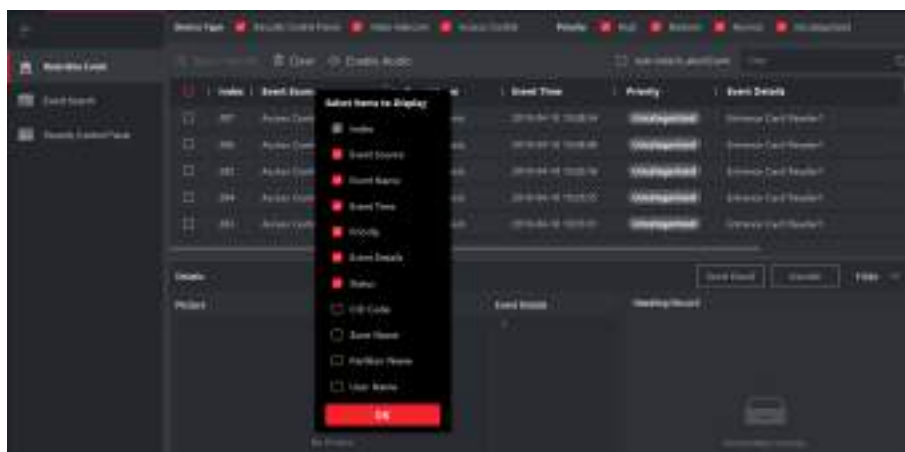


図 8-10 イベント関連の項目をカスタマイズして表示

4. イベントの詳細情報を表示します。
 - 1) イベントリストからイベントを選択します。
 - 2) ページ右下隅の **[展開]** をクリックします。

- 3) イベントに関連する画像、詳細説明、処理記録を表示します。
- 4) オプション: 関連する画像にカーソルを合わせ、右上隅のダウンロードアイコンをクリックすると、ローカル PC へダウンロードできます。保存先パスは手動で設定できます。
5. オプション: 必要に応じて以下の操作を実行してください。

単一イベントの処理 **[処理]** をクリックして処理の提案ページを開き、**[Commit (コミット)]** をクリックします。

 **メモ**

イベントの処理後、**[処理]** ボタンが **[Add Remark (注釈の追加)]** に切り替わります。その後、**[Add Remark (注釈の追加)]** をクリックし、処理済みイベントの詳細情報を追加します。

イベントの一括処理 処理が必要な複数のイベントを選択し、**[Handle in Batch (一括処理)]** をクリックします。処理の提案ページに入り、**[Commit (コミット)]** をクリックします。

アラームオーディオの有効化／無効化 **[オーディオを有効化]／[オーディオを無効化]** をクリックしてイベントのオーディオを有効化／無効化します。

最新のイベントを自動選択 **[最新のイベントを自動選択]** にチェックを入れると、最新のイベントが自動的に選択され、イベントの詳細情報が表示されます。

イベントの消去 **[消去]** をクリックすると、イベントリスト内のすべてのイベントを消去できます。

電子メールの送信 イベントを選択して**[電子メールを送信]** をクリックすると、そのイベントの詳細情報が電子メールで送信されます。

 **メモ**

最初に電子メールのパラメータを設定する必要があります。詳細については、クライアントソフトウェアのユーザーマニュアルに記載の「**電子メールのパラメータ設定**」をご覧ください。

8.10.3 過去イベントの検索

イベントセンターページの [イベント検索] モジュールでは、特定のデバイスタイプに合わせて、時刻やデバイスタイプなどの条件で過去のイベントを検索し、イベントを処理できます。

始める前に

クライアントがデバイスからイベント情報を受信するには、そのデバイスのイベント受信を有効化する必要があります。詳細については、「デバイスからのイベント受信の有効化」をご覧ください。

手順

1. [イベントセンター] → [イベント検索] の順にクリックし、イベント検索のページを開きます。

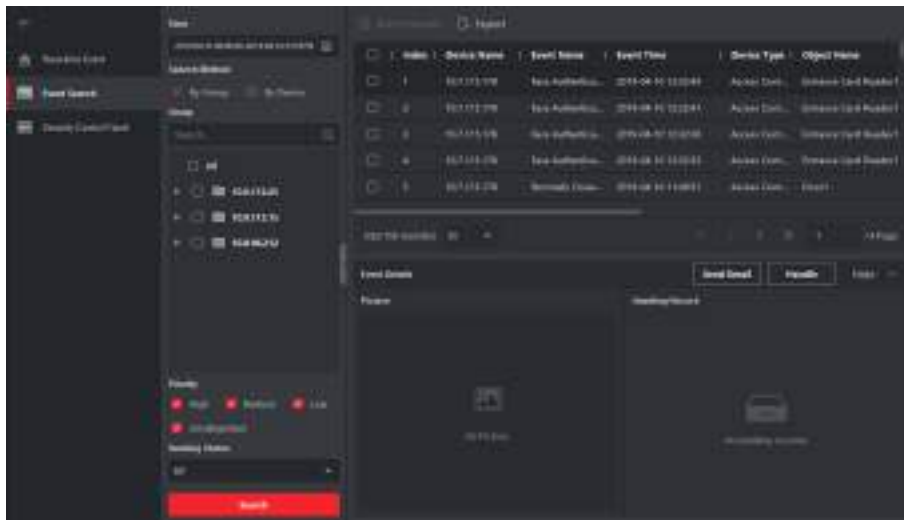


図 8-11 過去イベントの検索

2. フィルタ条件を設定して目的のイベントのみを表示させます。

時間

イベント開始時のクライアント側の時間を示します。

検索条件

グループ: 選択したグループ内のリソースで発生したイベントを検索します。

デバイス: 選択したデバイスで発生したイベントを検索します。

デバイスタイプ

イベントが発生したデバイスのタイプを示します。

すべて

すべてのデバイスタイプを対象とします。グループ、優先、状態をフィルタ条件として設定できます。

ビデオインターコム

ビデオインターコムのイベントでは、[All Record (すべての録画)] または [Only Unlocking (ロック解除のみ)] で検索範囲を選択する必要があります。

- All Records (すべての録画)
- : すべてのビデオインターコムのイベントをフィルタできます。なお、デバイス、優先、状態でフィルタ条件を設定する必要があります。
- Only Unlocking (ロック解除のみ)
- : すべてのビデオインターコムのロック解除イベントをフィルタできます。なお、デバイスとロック解除タイプでフィルタ条件を設定する必要があります。

入退室管理

入退室管理のイベントでは、以下のフィルタ条件を設定できます: デバイス、優先、状態、イベントタイプ、カードリーダーのタイプ、人物名、カード番号、組織。

メモ

[詳細を表示] をクリックすると、イベントのタイプ、カードリーダーのタイプ、人物名、カード番号、組織を設定できます。

グループ

イベントが発生したデバイスのグループを示します。[デバイスタイプ] で [すべて] を選択した場合は、フィルタ条件でグループを選択する必要があります。

デバイス

イベントが発生したデバイスを示します。

優先

低、中、高、カテゴリなしで、アラームの緊急度を示します。

状態

イベントの処理状態を示します。

3. [検索] をクリックし、設定した条件と一致するイベントを検索します。
4. オプション: イベントリスト表のヘッダ一部分を右クリックすると、イベント関連の項目をカスタマイズし、イベントリストに表示させることができます。

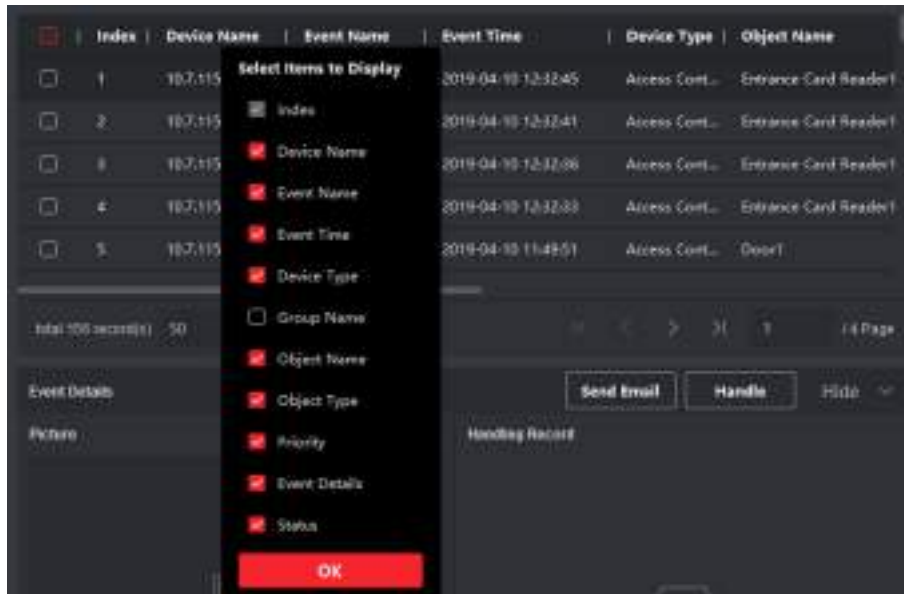


図 8-12 イベント関連の項目をカスタマイズして表示

5. オプション: イベントの処理。

- 単一イベントの処理: 処理に必要な単一のイベントを選択し、イベントの詳細情報ページで**[処理]** をクリックして処理の提案ページを開きます。
- イベントの一括処理: 処理に必要なイベントを複数選択して **[Handle in a Batch (一括処理)]** をクリックし、処理の提案ページを開きます。

 メモ

イベントの処理後、**[処理]** ボタンが **[Add Remark (注釈の追加)]** に切り替わります。その後、**[Add Remark (注釈の追加)]** をクリックし、処理済みイベントの詳細情報を追加します。

6. オプション: イベントを選択して**[電子メールを送信]** をクリックすると、そのイベントの詳細情報が電子メールで送信されます。

 メモ

最初に電子メールのパラメータを設定する必要があります。詳細については、クライアントソフトウェアのユーザーマニュアルに記載の「**電子メールのパラメータ設定**」をご覧ください。

7. オプション: **[エクスポート]** をクリックすると、イベントログまたはイベント画像を CSV 形式でローカル PC にエクスポートできます。保存先パスは手動で設定できます。
8. 関連する画像にカーソルを合わせ、右上隅のダウンロードアイコンをクリックすると、ローカル PC へダウンロードできます。保存先パスは手動で設定できます。

8.11 時間および出勤

[Time and Attendance (時間および出勤)] モジュールには、従業員の始業時刻と終業時刻を追跡および監視する機能に加えて、遅刻、早退、休憩時間、長期欠勤などの労働時間を完全に管理する機能も備わっています。

メモ

このセクションでは、出勤レポートの作成前に設定しておく必要のある各種設定について説明します。これらの設定を行った後に記録されたアクセス記録については、そのデータ内での計算が行われます。

8.11.1 出勤パラメータの設定

一般ルール、残業パラメータ、出勤チェックポイント、休日、休暇タイプなどの出勤パラメータを設定できます。

一般ルールの設定

週の開始日、月の開始日、週末、欠勤などの出勤計算に使用する一般ルールを設定できます。

手順

メモ

このパラメータは、新規に追加した時間帯でデフォルト設定になります。これは、既存の時間帯には影響を及ぼしません。

1. [Time & Attendance (時間および出勤)] モジュールを開きます。
2. [出勤設定] → [一般ルール] の順にクリックします。
3. 週の開始日と月の開始日を設定します。
4. 週末に該当する日を選択します (複数選択可)。
5. 欠勤パラメータを設定します。
6. [保存] をクリックします。

残業パラメータの設定

残業レベル、時給、残業の出勤状態など、勤務日と非番日の残業パラメータを設定できます。

手順

1. [Time & Attendance (時間および出勤)] モジュールを開きます。

2. [出勤設定] → [残業] の順にクリックします。
3. 必要な情報を設定します。

平日の残業レベル

平日の終業時刻以降に勤務する場合、複数の残業レベルが適用されます（残業レベル 1、残業レベル 2、残業レベル 3）。3 つの残業レベル別に異なる時給を設定できます。

時給

3 つの残業レベルごとに時給を設定すると、その設定が通常の合計勤務時間の計算に使用されます。

非番日の残業ルール

非番日の残業ルールを有効化して計算モードを設定できます。

4. [保存] をクリックします。

出勤チェックポイントの設定

アクセスポイントのカードリーダーを出勤チェックポイントとして設定することで、カードリーダーの認証機能を使用して出勤状況を記録できます。

始める前に

出勤チェックポイントの設定前に、入退室管理デバイスを追加しておく必要があります。詳細については、「[デバイスの追加](#)」をご覧ください。

手順

メモ

デフォルトでは、追加した入退室管理デバイスの全カードリーダーが出勤チェックポイントとして設定されています。

1. [Time & Attendance（時間および出勤）] モジュールを開きます。
2. [出勤設定] → [出勤チェックポイント] の順にクリックし、[Attendance Check Point Settings（出勤チェックポイント設定）] ページを開きます。
3. オプション: [すべてのカードリーダーをチェックポイントとして設定] のスイッチをオフにします。
リスト内のカードリーダーのみが出勤チェックポイントとして設定されます。
4. デバイスリスト内で、目的のカードリーダーを出勤チェックポイントに設定します。
5. チェックポイント機能を [始業/終業]、[始業]、または [終業] に設定します。
6. [チェックポイントとして設定] をクリックします。
右側のリストに、設定した出勤チェックポイントが表示されます。

休日の設定

休日を指定して、その期間中はチェックインまたはチェックアウトを記録しないように設定できます。

定期休日の追加

1 年の内で元日、独立記念日、クリスマスなど、有効期間中に定期休日となる休日を設定できます。

手順

1. [Time & Attendance (時間および出勤)] モジュールを開きます。
2. [出勤設定] → [休日] の順にクリックし、[休日設定] ページを開きます。
3. 休日タイプで [定期休日] にチェックを入れます。
4. 休日の名前をカスタマイズします。
5. 休日の開始日を設定します。
6. 休日の日数を入力します。
7. 従業員が休日に勤務する場合、出勤状態を設定します。
8. オプション: [毎年繰り返す] にチェックを入れると、その休日の設定を毎年繰り返し適用できます。
9. [OK] をクリックします。
追加した休日は、休日リストとカレンダーに表示されます。
その日付が異なる祝日として選択された場合、最初に追加した休日として記録されます。
10. オプション: 休日の追加後に、以下の操作のうち 1 つを実行します。

休日の編集 をクリックし、休日情報を編集します。

休日の削除 1 つ以上の休日を選択して [削除] をクリックし、休日リストからその休日を削除します。

不定期休日の追加

毎年の法定休日など、有効期間中に不定期で定休日になる休日を設定できます。

手順

1. [Time & Attendance (時間および出勤)] モジュールを開きます。
2. [出勤設定] → [休日] の順にクリックし、[休日設定] ページを開きます。
3. [追加] をクリックして [休日を追加] ページを開きます。
4. 休日タイプで [不定期休日] にチェックを入れます。
5. 休日の名前をカスタマイズします。
6. 休日の開始日を設定します。

例

2019 年 11 月第 4 木曜日を感謝祭として祝日に設定する場合、ドロップダウンリストから 2019 年 11 月の第 4 木曜日を選択します。

7. 休日の日数を入力します。
8. 従業員が休日に勤務する場合、出勤状態を設定します。
9. オプション: [毎年繰り返し] にチェックを入れると、その休日の設定を毎年繰り返し適用できます。
10. [OK] をクリックします。
追加した休日は、休日リストとカレンダーに表示されます。
その日付が異なる祝日として選択された場合、最初に追加した休日として記録されます。
11. オプション: 休日の追加後に、以下の操作のうち 1 つを実行します。

休日の編集 をクリックし、休日情報を編集します。

休日の削除 1 つ以上の休日を選択して [削除] をクリックし、休日リストからその休日を削除します。

休暇タイプの設定

実際の使用状況に応じて、休暇タイプ（主タイプと副タイプ）をカスタマイズできます。休暇タイプは編集または削除できます。

手順

1. [Time & Attendance（時間および出勤）] モジュールを開きます。
2. [出勤設定] → [休暇タイプ] の順にクリックし、[休暇タイプ設定] ページを開きます。
3. 左側の [追加] をクリックし、主タイプの休暇を追加します。
4. オプション: 主タイプの休暇に対して、以下の操作のうち 1 つを実行します。

編集 主タイプの休暇の上にカーソルを合わせて、 をクリックし、主タイプの休暇を編集します。

削除 主タイプの休暇を 1 つ選択し、左側の [削除] をクリックして主タイプの休暇を削除します。

5. 右側の [追加] をクリックし、副タイプの休暇を追加します。
6. オプション: 副タイプの休暇に対して、以下の操作のうち 1 つを実行します。

編集 副タイプの休暇の上にカーソルを合わせて、 をクリックし、副タイプの休暇を編集します。

削除 副タイプの休暇を 1 つ以上選択して右側の [削除] をクリックし、選択した副タイプの休暇を削除します。

認証記録のサードパーティ製データベースとの同期

クライアントソフトウェア内の出勤データ記録を使用して、計算などの処理を他のシステムに実行させることができます。同期機能を有効化して、クライアントソフトウェアからの認証記録をサードパーティ製データベースに自動適用できます。

手順

1. [Time & Attendance (時間および出勤)] モジュールを開きます。
2. [出勤設定] → [サードパーティデータベース] の順にクリックします。
3. [データベースに適用] のスイッチをオンにして同期機能を有効化します。
4. データベースのタイプ、サーバーの IP アドレス、データベース名、ユーザー名、パスワードなど、サードパーティ製データベースに必要なパラメータ情報を設定します。
5. 実際の設定状況に応じて、データベースのテーブルパラメータを設定します。
 - 1) サードパーティ製データベースのテーブル名を入力します。
 - 2) クライアントソフトウェアとサードパーティ製データベース間でマッピング済みのテーブルフィールドを設定します。
6. [接続テスト] をクリックし、データベースに接続できるかテストします。
7. [保存] をクリックし、データベースに接続して正常に設定を保存できるかテストします。
 - 出勤データがサードパーティ製データベースに書き込まれます。
 - 同期中に、クライアントがサードパーティ製データベースと接続を切断すると、クライアントは 30 分ごとに再接続を試行します。再接続後、クライアントは接続が切断された期間に記録されたデータをサードパーティ製データベースと同期します。

休憩時間の設定

休憩時間を追加して、開始時間、終了時間、継続時間、計算モードなどの休憩パラメータを設定できます。追加した休憩時間は編集したり削除したりできます。

手順

1. [Time & Attendance (時間および出勤)] → [タイムテーブル] の順にクリックします。追加したタイムテーブルがリストに表示されます。
2. 追加したタイムテーブルを選択するか、[追加] をクリックしてタイムテーブルの設定ページを開きます。
3. 休憩時間エリアで [設定] をクリックし、休憩時間の管理ページを開きます。
4. 休憩時間を追加します。
 - 1) [追加] をクリックします。
 - 2) 休憩時間の名前を入力します。
 - 3) 休憩時間の関連パラメータを設定します。

開始時間／終了時間

休憩の開始時間と終了時間を設定します。

以降／以前

休憩開始の最も早いスワイプ対応時間と休憩終了の最も遅いスワイプ対応時間を設定します。

休憩継続時間

休憩の開始時間から終了時間までの時間を示します。

計算

Auto Deduct（自動控除）

指定した休憩時間を勤務時間から控除します。

Must Check（確認必須）

休憩時間を計算して、実際のチェックインとチェックアウト時刻に応じて勤務時間から休憩時間を控除します。

メモ

計算方法として [Must Check（確認必須）] を選択した場合、休憩から遅く戻る時、または早く戻る時の出勤状態を設定しておく必要があります。

5. [保存] をクリックして設定を保存します。
6. オプション: [追加] をクリックし、休憩時間の追加を継続します。

レポート表示の設定

会社名、ロゴ、日付の形式、時刻の形式、マークなど、出勤レポートに表示するコンテンツを設定できます。

手順

1. [Time & Attendance（時間および出勤）] モジュールを開きます。
2. [Attendance Statistics（出勤統計）] → [Report Display（レポート表示）] の順にクリックします。
3. 出勤レポートの表示を設定します。

会社名

レポートに記載する会社名を入力します。

日付の形式／時刻の形式

実際の使用状況に応じて、日付の形式と時刻の形式を設定します。

レポート内の出勤状態のマーク

マークを入力し、色を選択します。選択したマークと色で、レポート内の出勤状態に関連するフィールドが表示されます。

レポート内の週末のマーク

マークを入力し、色を選択します。選択したマークと色で、レポート内の週末フィールドが表示されます。

4. [保存] をクリックします。

8.11.2 タイムテーブルの追加

シフトスケジュールにタイムテーブルを追加できます。

手順

1. [Time & Attendance (時間および出勤)] → [タイムテーブル] の順にクリックし、タイムテーブルの設定ウィンドウを開きます。
2. [追加] をクリックし、タイムテーブルの追加ページを開きます。
3. タイムテーブルの名前を作成します。
4. 計算方法を選択します。

最初のチェックインと最終チェックアウト

最初のチェックイン時間が始業時間として、最後のチェックアウト時間が終業時間として記録されます。

各チェックイン／アウト

各チェックイン時間とチェックアウト時間が有効である場合、隣接するチェックイン時間からチェックアウト時間までの合計が有効な勤務時間として記録されます。

この計算方法の有効な認証と間隔を設定する必要があります。例えば、同じカードのスイープ間隔が設定値より短い場合、カードのスイープが無効になります。

5. オプション: [T&A 状態の有効化] スイッチをオンにし、デバイスの出勤状態に応じて計算します。
6. 関連する出勤時間を設定します。

始業／終業時間

始業時間と終業時間を設定します。

有効なチェックイン／アウト時間

チェックインまたはチェックアウトが有効な時間帯を設定します。

計算対象

実際の勤務時間として計算する継続時間を設定します。

遅刻／早退許容

遅刻／早退が許容範囲内となる時間帯を設定します。

7. オプション: 休憩時間を勤務時間から控除するように選択できます。

メモ

[設定] をクリックすると休憩時間を管理できます。休憩時間の設定の詳細については、「休憩時間の設定」をご覧ください。

8. [保存] をクリックし、タイムテーブルを追加します。
9. オプション: タイムテーブルの追加後、以下の 1 つまたは複数の操作を実行します。

タイムテーブルの編集 リストからタイムテーブルを選択し、関連情報を編集します。

タイムテーブルの削除 リストからタイムテーブルを選択し、[削除] をクリックして削除します。

8.11.3 シフトの追加

シフトスケジュールにシフトを追加できます。

始める前に

最初にタイムテーブルを追加します。詳細については、「タイムテーブルの追加」をご覧ください。

手順

1. [Time and Attendance (時間および出勤)] → [シフト] の順にクリックし、シフトの設定ページを開きます。
2. [追加] をクリックし、[シフトの追加] ページを開きます。
3. シフトの名前を入力します。
4. ドロップダウンリストからシフト期間を選択します。
5. 追加したタイムテーブルを選択し、タイムバーをクリックしてタイムテーブルに適用します。

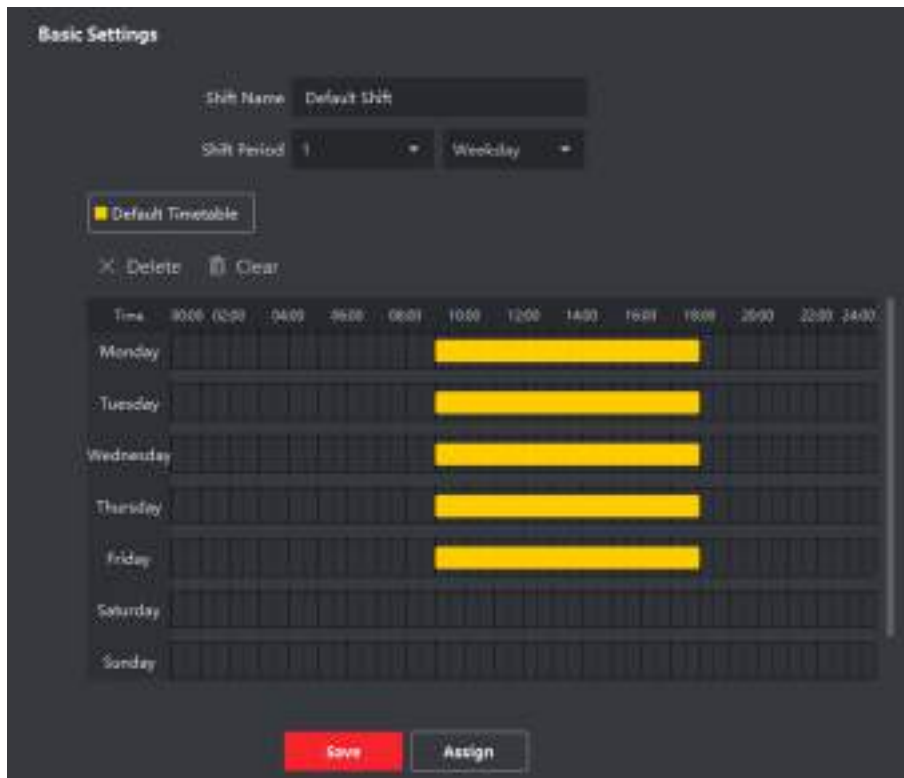


図 8-13 シフトの追加

6. **[保存]** をクリックします。
追加したシフトがページ左側のパネルに一覧表示されます。最大 64 件のシフトを追加できます。
7. オプション: シフトを組織または人物に割り当てて、クイックシフトスケジュールを作成します。
 - 1) **[割り当て]** をクリックします。
 - 2) **[組織]** または **[人物]** タブを選択し、目的の組織または人物のボックスにチェックを入れます（複数選択可）。
選択した組織または人物がページの右側に表示されます。
 - 3) シフトスケジュールの有効期間を設定します。
 - 4) このシフトスケジュールに対して、Check-in Not Required（チェックイン不要）、Check-out Not Required（チェックアウト不要）、Effective for Holiday（休日に有効）、Effective for Overtime（残業に有効）など、その他のパラメータも設定します。
 - 5) **[保存]** をクリックし、クイックシフトスケジュールを保存します。

8.11.4 シフトスケジュールの管理

交代勤務とは、1 週間の各日で 24 時間を有効に活用するための勤務制度です。一般的にこの勤務制度では 1 日を複数のシフトに分割し、各シフトに割り当てる時間を設定します。

部門のスケジュール、従業員のスケジュール、臨時スケジュールを設定できます。

部門スケジュールの設定

部門のシフトスケジュールを設定することで、その部門の全従業員にそのシフトスケジュールが割り当てられます。

始める前に

[Time & Attendance (時間および出勤)] モジュールでは、部門リストは組織と同じになります。最初に [人物] モジュールで組織と人物を追加する必要があります。詳細については、「人物管理」をご覧ください。

手順

1. [Time and Attendance (時間および出勤)] → [シフトスケジュール] の順にクリックし、[シフトスケジュール管理] ページを開きます。
2. [部門スケジュール] をクリックし、[部門スケジュール] ページを開きます。
3. 左側の組織リストから部門を選択します。

メモ

組織を選択する時に [下部組織を含む] にチェックが入っている場合、下部組織も同時に選択されます。

4. ドロップダウンリストからシフトを選択します。
5. チェックボックスにチェックを入れて [Multiple Shift Schedules (複数のシフトスケジュール)] を有効化します。

メモ

[Multiple Shift Schedules (複数のシフトスケジュール)] にチェックを入れると、選択した部門の人物に対して、追加した時間帯の中から有効な時間帯を選択できます。

Multiple Shift Schedules (複数のシフトスケジュール)

ここには複数の時間帯が含まれています。選択した人物は、この時間帯の任意の時点でチェックイン/チェックアウトでき、出勤も記録されます。

複数のシフトスケジュールに 3 つの期間が含まれている場合：00:00~07:00、08:00~15:00 および 16:00~23:00。この複数のシフトスケジュールが適用される人物は、3 つの時間帯のどの時点で出勤しても記録されます。その人物が 07:50 にチェックインする場合、直近の時間帯である 08:00~15:00 に出勤が記録されます。

6. 開始日と終了日を設定します。
7. このスケジュールに対して、Check-in Not Required (チェックイン不要)、Check-out Not Required (チェックアウト不要)、Effective for Holiday (休日に有効)、Effective for Overtime (残業に有効) など、その他のパラメータも設定します。
8. [保存] をクリックします。

人物スケジュールの設定

1 名または複数名にシフトスケジュールを割り当てることができます。その人物のスケジュール詳細も確認できます。

始める前に

[人物] モジュールに部門と人物を追加します。詳細については、「人物管理」をご覧ください。

手順

メモ

人物のスケジュールは、部門のスケジュールよりも優先されます。

1. [Time and Attendance (時間および出勤)] → [シフトスケジュール] の順にクリックし、[シフトスケジュール管理] ページを開きます。
 2. [Person Schedule (人物スケジュール)] をクリックし、[Person Schedule (人物スケジュール)] ページを開きます。
 3. 組織と人物を選択します。
 4. ドロップダウンリストからシフトを選択します。
 5. チェックボックスにチェックを入れて [Multiple Shift Schedules (複数のシフトスケジュール)] を有効化します。
-

メモ

[Multiple Shift Schedules (複数のシフトスケジュール)] にチェックを入れた後に、追加したタイムテーブルの中からその人物に適用するタイムテーブルを選択してください。

Multiple Shift Schedules (複数のシフトスケジュール)

ここには複数のタイムテーブルが含まれています。その人物は、タイムテーブル内の任意の時点でチェックイン/チェックアウトでき、出勤も記録されます。

複数のシフトスケジュールに 3 つのタイムテーブルが含まれている場合: 00:00~07:00、08:00~15:00 および 16:00~23:00。この複数のシフトスケジュールが適用される人物は、3 つのタイムテーブルのどの時点で出勤しても記録されます。その人物が 07:50 にチェックインする場合、直近のタイムテーブルである 08:00~15:00 に出勤が記録されます。

6. 開始日と終了日を設定します。
 7. このスケジュールに対して、Check-in Not Required (チェックイン不要)、Check-out Not Required (チェックアウト不要)、Effective for Holiday (休日に有効)、Effective for Overtime (残業に有効) など、その他のパラメータも設定します。
 8. [保存] をクリックします。
-

臨時スケジュールの設定

従業員に臨時スケジュールを追加し、臨時のシフトスケジュールを割り当てることができます。その臨時スケジュールの詳細を確認することもできます。

始める前に

[人物] モジュールに部門と人物を追加します。詳細については、「人物管理」をご覧ください。

手順

メモ

臨時スケジュールは、部門スケジュールや人物スケジュールよりも優先されます。

1. [Time and Attendance (時間および出勤)] → [シフトスケジュール] の順にクリックし、[シフトスケジュール管理] ページを開きます。
2. [Temporary Schedule (臨時スケジュール)] をクリックし、[Temporary Schedule (臨時スケジュール)] ページを開きます。
3. 組織と人物を選択します。
4. 臨時スケジュール用に、1 つの日付をクリックするか、ドラッグして複数の日付を選択します。
5. ドロップダウンリストから[勤務日] または [非番日] を選択します。

[非番日] を選択した場合、以下のパラメータを設定する必要があります。

計算対象

臨時スケジュールに通常レベルと残業レベルのどちらで出勤状態を記録するかを選択します。

タイムテーブル

ドロップダウンリストからタイムテーブルを選択します。

複数のシフトスケジュール

ここには複数のタイムテーブルが含まれています。その人物は、タイムテーブル内の任意の時点でチェックイン/チェックアウトでき、出勤も記録されます。

複数のシフトスケジュールに 3 つのタイムテーブルが含まれている場合: 00:00~07:00、08:00~15:00 および 16:00~23:00。この複数のシフトスケジュールが適用される人物は、3 つのタイムテーブルのどの時点で出勤しても記録されます。その人物が 07:50 にチェックインする場合、直近のタイムテーブルである 08:00~15:00 に出勤が記録されます。

ルール



[Check-in Not Required (チェックイン不要)]、[Check-out Not Required (チェックアウト不要)] など、スケジュールに適用するルールを設定します。

6. [保存] をクリックします。

シフトスケジュールの確認

カレンダーモードまたはリストモードでシフトスケジュールを確認できます。シフトスケジュールを編集または削除することもできます。

手順

1. [Time and Attendance (時間および出勤)] → [シフトスケジュール] の順にクリックし、[シフトスケジュール管理] ページを開きます。
2. 組織と該当する人物を選択します。
3.  または  をクリックして、カレンダーモードまたはリストモードでシフトスケジュールを表示します。

カレンダー

カレンダーモードでは、1 カ月内の各日のシフトスケジュールを確認できます。臨時スケジュール内の特定の日付をクリックして、編集または削除することもできます。

リスト

リストモードでは、シフト名、タイプ、有効期間など、特定の人物または組織についてシフトスケジュールの詳細を確認できます。シフトスケジュールにチェックを入れて [削除] をクリックすると、選択したシフトスケジュールを削除できます（複数選択可）。

8.11.5 チェックイン／チェックアウト記録の手動補正

出勤状態が正しくない場合、チェックイン／チェックアウト記録を手動補正できます。チェックイン／チェックアウト記録を編集、削除、検索、エクスポートすることもできます。

始める前に


- [人物] モジュールで組織と人物を追加する必要があります。詳細については、「人物管理」をご覧ください。
- その人物の出勤状態が正しくないことが前提となります。

手順

1. [Time and Attendance (時間および出勤)] → [出勤処理] の順にクリックし、出勤処理のページを開きます。
2. [Correct Check-In/Out (チェックイン／アウトを修正)] をクリックし、チェックイン／アウトの修正ページを開きます。
3. 左側のリストから修正する人物を選択します。
4. 修正する日付を選択します。
5. チェックイン／アウトのパラメータを設定します。



[チェックイン] を選択して正しい始業時間に設定します。[チェックアウト] を選択して正しい終業時間に設定します。

メモ

 をクリックすると、複数のチェックイン／アウト項目を追加できます。最大 8 件のチェックイン／アウト項目に対応しています。

- オプション: 注釈を記入したい場合は入力します。
- [保存] をクリックします。
- オプション: チェックイン／アウトの修正後に、以下の操作のうち 1 つを実行します。

表示

 または  をクリックして、カレンダーモードまたはリストモードに追加済みの処理情報を表示します。

メモ

カレンダーモードで 1 カ月内の出勤状態を取得するには、[計算] をクリックする必要があります。

編集

- カレンダーモードで、日付の関連ラベルをクリックして詳細を編集します。
- リストモードで [日付]、[処理タイプ]、[時間]、または [注釈] 列内の関連フィールドをダブルクリックし、その情報を編集します。

削除

選択した項目を削除します。

エクスポート

出勤処理の詳細をローカル PC にエクスポートします。

メモ

詳細情報は CSV 形式で保存されます。

8.11.6 休暇と出張の追加

従業員が休暇または出張を申し出た場合、休暇と出張を追加できます。

始める前に

[人物] モジュールで組織と人物を追加する必要があります。詳細については、「人物管理」をご覧ください。

手順



1. [Time and Attendance (時間および出勤)] → [出勤処理] の順にクリックし、出勤処理のページを開きます。
 2. [休暇／出張の適用] をクリックし、休暇／出張の追加ページを開きます。
 3. 左側のリストから人物を選択します。
 4. 休暇または出張の日付を設定します。
 5. ドロップダウンリストから主タイプの休暇と副タイプの休暇を選択します。
-

メモ

[出勤設定] で休暇のタイプを設定できます。詳細については、「**休暇タイプの設定**」をご覧ください。

6. 休暇の期間を設定します。
7. オプション: 注釈を記入したい場合は入力します。
8. [保存] をクリックします。
9. オプション: 休暇または出張の追加後に、以下の操作のうち 1 つを実行します。

表示

 または  をクリックして、カレンダーモードまたはリストモードに追加済みの処理情報を表示します。

メモ

カレンダーモードで 1 ヶ月内の出勤状態を取得するには、[計算] をクリックする必要があります。

編集

- カレンダーモードで、日付の関連ラベルをクリックして詳細を編集します。
- リストモードで [日付]、[処理タイプ]、[時間]、または [注釈] 列内のフィールドをダブルクリックし、関連情報を編集します。

削除

選択した項目を削除します。

エクスポート

出勤処理の詳細をローカル PC にエクスポートします。

メモ

詳細情報は CSV 形式で保存されます。

8.11.7 出勤データの計算

出勤データ、従業の詳細な出勤データ、従業員の異常な出勤データ、従業員の残業データ、およびカードのスイプログの概要を検索および閲覧する前に、出勤データを計算する必要があります。

出勤データの自動計算

クライアントが設定した時間に出勤データを毎日自動で計算するように、スケジュールを設定できます。

手順

メモ

計算されるのは前日までの出勤データです。

1. [Time & Attendance (時間および出勤)] モジュールを開きます。
2. [出勤設定] → [一般ルール] の順にクリックします。
3. [Auto-Calculate Attendance (出勤データの自動計算)] エリア内で、クライアントにデータを毎日計算させる時間を設定します。
4. [保存] をクリックします。

出勤データの手動計算

データ範囲を設定することで、出勤データを手動で計算できます。

手順

1. [Time & Attendance (時間および出勤)] モジュールを開きます。
2. [Attendance Statistics (出勤統計)] → [出勤の計算] の順にクリックします。
3. 開始時間と終了時間を設定し、出勤データの範囲を定義します。
4. 部門、人物名、従業員番号、出勤状態などの条件を設定します。
5. [計算] をクリックします。

メモ

過去 3 ヶ月以内の出勤データのみを計算できます。

6. 以下の操作のうち 1 つを実行します。

チェックイン／アウトを修正	[チェックイン／アウトを修正] をクリックし、チェックイン／アウトの修正を追加します。
レポート	[レポート] をクリックし、出勤レポートを生成します。
エクスポート	[エクスポート] をクリックし、出勤データをローカル PC にエクスポートします。



詳細情報は CSV 形式で保存されます。

8.11.8 出勤統計

出勤データの計算結果に基づいて、元の出勤記録を確認したり、出勤レポートを生成およびエクスポートしたりできます。

元の出勤記録の入手

期間内の従業員の出勤時間、出勤状態、チェックポイントなどを検索して、各従業員に対する元の記録を取得できます。

始める前に

- [人物] モジュールで組織と人物を追加したうえで、その人物がカードをスワイプ済みである必要があります。詳細については、「人物管理」をご覧ください。
- 出勤データを計算します。



- クライアントは、翌日 1:00 am に前日の出勤データを自動計算します。
 - 1:00 am にはクライアントを起動状態にしておいてください。起動していない場合、前日の出勤データを自動計算できません。自動的に計算されなかった場合も手動で出勤データを計算できます。詳細については、「出勤データの手動計算」をご覧ください。
-

手順

1. [Time & Attendance (時間および出勤)] モジュールを開きます。
2. [Attendance Statistics (出勤統計)] → [元の記録] の順にクリックします。
3. 検索する出勤の開始時間と終了時間を設定します。
4. 部門、人物名、従業員番号などその他の検索条件を設定します。

5. オプション: [デバイスから入手] をクリックして、デバイスから出勤データを入力します。
6. オプション: [リセット] をクリックすると、すべての検索条件をリセットし、検索条件を再度編集することができます。
7. [検索] をクリックします。
検索結果がページ上に表示されます。その従業員の必要な出勤状態とチェックポイントを確認できます。
8. オプション: 検索後に、以下の操作のうち 1 つを実行します。
 - レポートの生成 [レポート] をクリックし、出勤レポートを生成します。
 - レポートのエクスポート [エクスポート] をクリックし、結果をローカル PC にエクスポートします。

インスタントレポートの生成

一連の出勤レポートを手動で生成し、従業員の出勤結果を確認することができます。

始める前に

出勤データを計算します。

メモ

出勤データを手動で計算するだけでなく、スケジュールを設定してクライアント側で毎日自動的に計算することもできます。詳細については、「出勤データの計算」をご覧ください。

手順

1. [Time & Attendance (時間および出勤)] モジュールを開きます。
2. [Attendance Statistics (出勤統計)] → [レポート] の順にクリックします。
3. レポートタイプを選択します。
4. 部門または人物を選択し、出勤レポートを表示します。
5. 出勤データをレポート内に記載する際の開始時間と終了時間を設定します。
6. [レポート] をクリックして統計レポートを生成し、開きます。

出勤レポートのカスタマイズ

クライアントは複数のレポートタイプに対応しています。レポート内容を事前に定義すると、設定した電子メールアドレスにレポートが自動送信されます。

手順

 メモ

電子メールの自動送信機能を有効化する前に、電子メールのパラメータを設定してください。詳細については、クライアントソフトウェアのユーザーマニュアルに記載の「電子メールのパラメータ設定」をご覧ください。

1. [Time & Attendance（時間および出勤）] モジュールを開きます。
2. [Attendance Statistics（出勤統計）] → [カスタムレポート] の順にクリックします。
3. [追加] をクリックし、レポートの内容を事前定義します。
4. レポートの内容を設定します。

レポート名

レポート名を入力します。

レポートタイプ

レポートタイプを 1 つ選択すると、指定したタイプでレポートが生成されます。

レポート時間

レポートタイプごとに異なる時間を選択できます。

人物

レポートに出勤記録を記載する人物を選択します。

5. オプション: スケジュールを設定して、電子メールアドレスにレポートを自動送信することができます。
 - 1) [Auto-Sending Email（電子メールの自動送信）] にチェックを入れ、この機能を有効化します。
 - 2) 選択した送信日付にクライアントがレポートを送信する機能に対して、その有効期間を設定します。
 - 3) クライアントがレポートを送信する日付を選択します（複数選択可）。
 - 4) クライアントがレポートを送信する時間を設定します。

例

有効期間を 2018/3/10～2018/4/10、送信の曜日を金曜日、送信時間を 20:00:00 に設定した場合、クライアント側は 2018/3/10 から 2018/4/10 の間、金曜日の 8 p.m.にレポートを送信します。

 メモ

送信時間の前に出勤記録を計算済みであることを確認してください。出勤データを手動で計算するだけでなく、スケジュールを設定してクライアント側で毎日自動的に計算することもできます。詳細については、「出勤データの計算」をご覧ください。

5) 電子メールの宛先を入力します（複数入力可）。

 **メモ**

[+] をクリックすると、新しい電子メールアドレスを追加できます。電子メールアドレスは最大 5 件追加できます。

6) オプション: [プレビュー] をクリックすると、電子メールの詳細を表示できます。

6. [OK] をクリックします。

7. オプション: カスタムレポートの追加後、以下の操作を 1 つまたは複数実行できます。

レポートの編集 追加したレポートを 1 つ選択し、[編集] をクリックして設定を編集します。

レポートの削除 追加したレポートを 1 つ選択し、[削除] をクリックして削除します。

レポートの生成 追加したレポートを 1 つ選択し、[レポート] をクリックしてレポートを即座に生成し、レポートの詳細を表示できます。

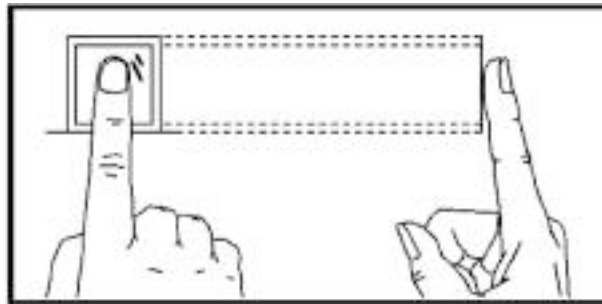
A. 指紋スキヤンのヒント

推奨する指紋の採取部位

人差し指、中指、または薬指。

正しいスキヤン方法

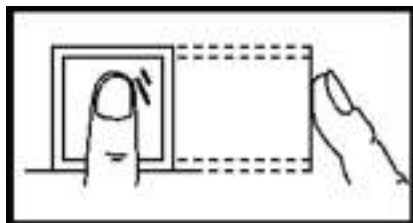
下図は正しい指紋のスキヤン方法を示しています。



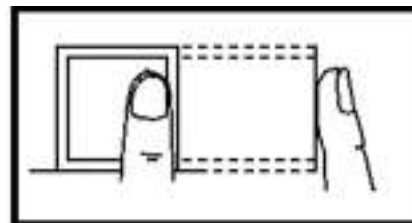
指を立ててスキヤナの面を押します。スキヤンする指の中央部分とスキヤナ面の中央が一致するようにします。

正しくないスキヤン方法

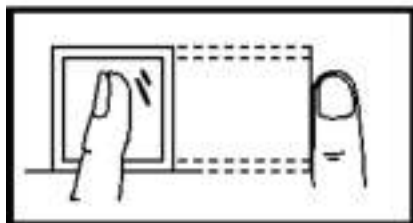
下図は正しくないスキヤン方法を示しています。



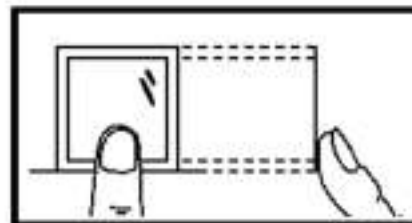
Vertical



Edge I



Side



Edge II

環境

スキャン時は、直射日光、高温、高湿度、雨中の状況を避けてください。

指が乾燥していると、スキャナが指紋を正常に認識できない場合があります。指に息を吹きかけて、再度スキャンしてください。

その他

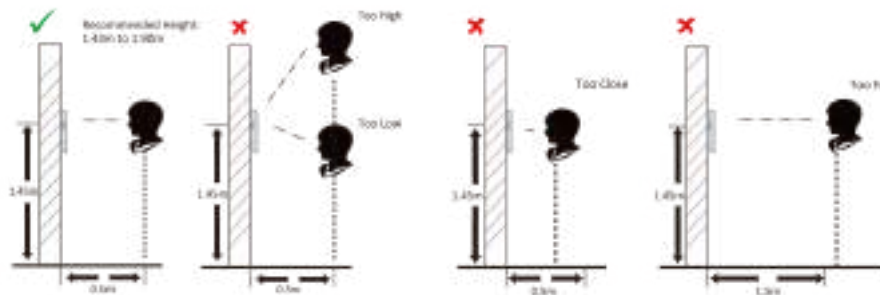
指紋が薄い、またはスキャンが困難な場合は、指紋以外の方法で認証することをお勧めします。

スキャンする指紋に傷がある場合、認識できない可能性があります。別の指で試すか、再度スキャンしてください。

B. 顔画像を取り込む／比較する場合のヒント

顔画像を取り込む場合または比較する場合は、下図のように立ってください。

位置（推奨距離: 0.5m）



表情

- 顔画像を取り込む／比較する時は、下図のように自然な表情を保ってください。



- 帽子やサングラスなど、顔認識機能に悪影響を及ぼす可能性のあるアクセサリは着用しないでください。
- 髪が目や耳を覆わないようにしてください。また、濃い化粧も避けてください。

姿勢

撮影品質が高く正確な顔画像を撮影するため、顔画像を取り込む／比較する時にはカメラの方をまっすぐ向くようにしてください。



サイズ

ウィンドウの中央に顔が来るようにします。



C. 設置環境のヒント

1. 光源照度の参照値



ろうソク: 10Lux



電球: 100~850Lux



太陽光: 1200Lux 以上

2. 本デバイスは、照明から 2m 以上、窓やドアから 3m 以上離して取り付けてください。



3. 逆光、直射日光、間接太陽光を避けてください。



Backlight



Direct Sunlight



Direct Sunlight
through Window



Indirect Light
through Window



Close to Light

D. 寸法

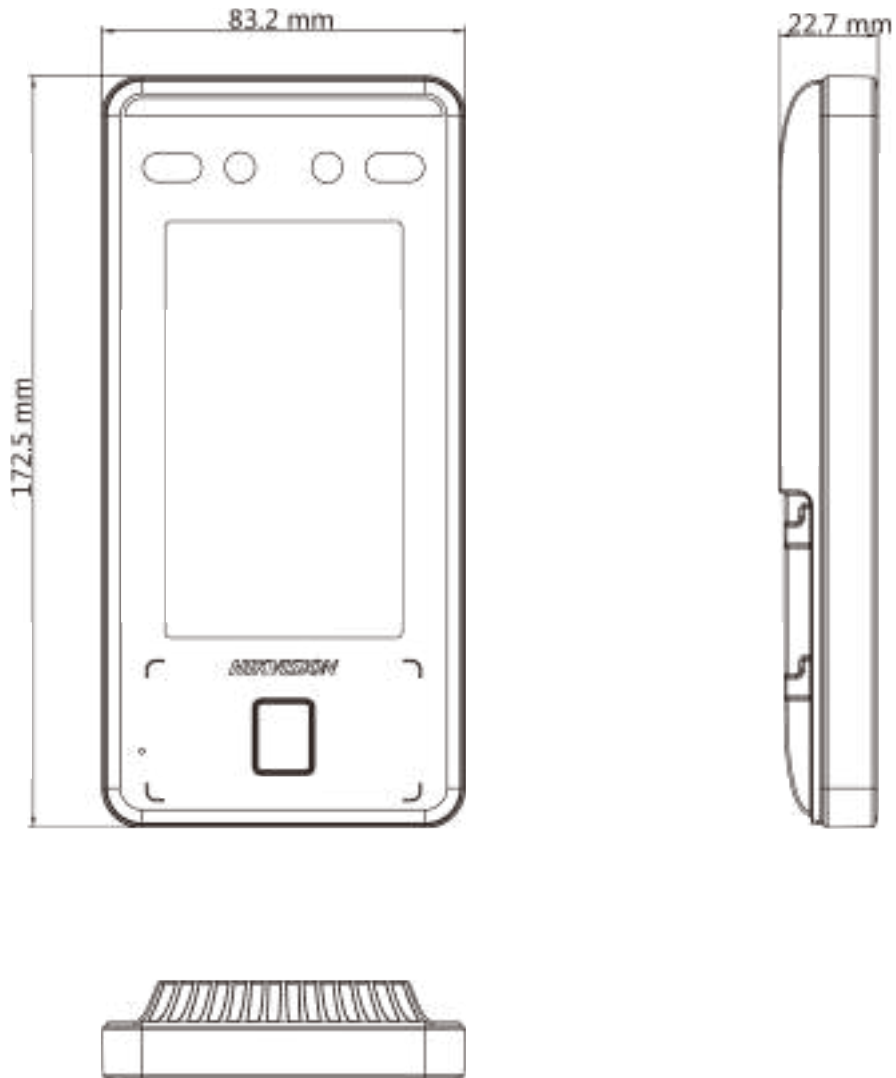


図 D-1 指紋あり

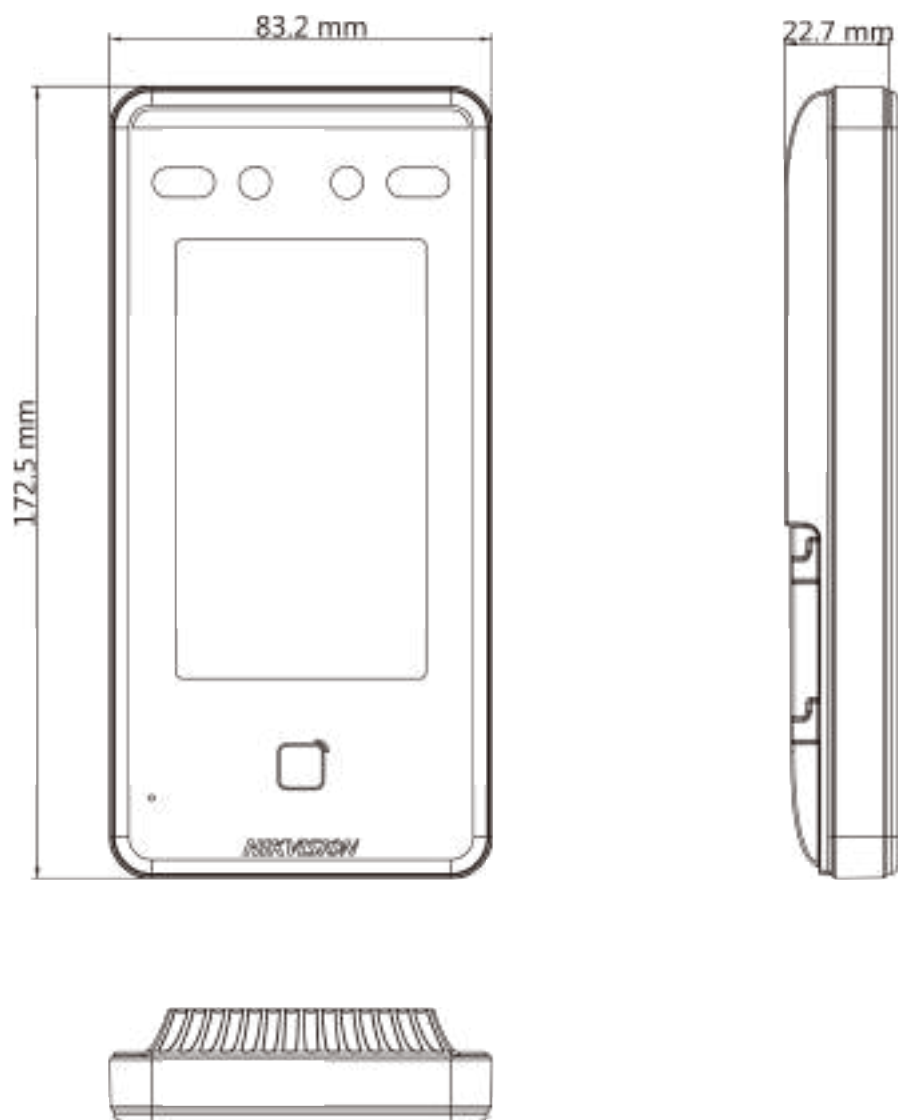


図 D-2 指紋なし

E. 通信マトリックスとデバイスコマンド

通信マトリックス

次の QR コードをスキャンして、デバイスの通信マトリックスを入手してください。マトリックスには、Hikvision 入退室管理およびビデオインターコムデバイスのすべての通信ポートが含まれていることに注意してください。



図 E-1 通信マトリックスの QR コード

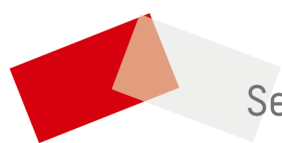
デバイスコマンド

デバイスの共通シリアルポートコマンドを取得するには、次の QR コードをスキャンします。

コマンドリストには、すべての Hikvision 入退室管理およびビデオインターコムデバイスで一般的に使用されるすべてのシリアルポートコマンドが含まれていることに注意してください。



図 E-2 デバイスコマンド



See Far, Go Further