

Gate Keeper ユーザーズマニュアル Version 2.1

Edge AI Box Tablet



はじめに

このたびは、弊社製品をお買い上げいただきまして誠にありがとうございます。

本製品の性能を十分活かしてご使用いただくためにも、本書をよくお読みいただき、正しく、安全にお使いくださるようお願いいたします。

本製品は、厳密な検査を行って出荷しておりますが、ご使用になる前に動作チェックを行なってください。

万一破損している場合や、仕様どおりに動作しない場合は、弊社までご連絡ください。

■ 本書について

- 本書に記載された製品および仕様は、製品の改良などのために予告なしに変更することがあります。
- 本書の一部または全部を無断で転載または改変することは禁止されています。
- 本書の作成には万全を期しておりますが、万一、不明な点や、誤り、その他お気づきの点がありましたら、弊社までご連絡ください。
- 運用の結果につきましては、上記項目に関わらず責任を負いかねますのでご了承ください。

■ 商標

- 「Wi-Fi」および「Wi-Fi」ロゴは、Wi-Fi Alliance®の登録商標です。
- EDGEMATRIX は EDGEMATRIX 株式会社の登録商標です。

お問い合わせ先

EDGEMATRIX 株式会社

〒150-0021

東京都渋谷区恵比寿西 2-3-16 CAT ビル 9 階

電話 : 03-6416-5861

FAX : 03-6416-5862

E-mail : device_support@edgematrix.com

HP : <https://edgematrix.com/>

改版履歴

発行年月	版数
2020 年 7 月	初版
2020 年 8 月	1.1
2021 年 1 月	1.2
2021 年 6 月	2.0
2021 年 9 月	2.1

安全上のご注意

ご使用前にこの「安全上のご注意」をよくお読みの上、本製品を正しくお使いください。




また、お読みになった後は大切に保管してください。

ここに示した注意事項は、お使いになる人や他の人への危害、財産への損害を未然に防ぐための内容を記載していますので、必ずお守りください。

本書では、本製品を安全にご使用いただくために、注意事項を以下のような表示で記載しています。







■ 区分

誤った使い方をしたときに生じる危害や損害の程度は、以下の表示で区分しています。







 危険	取り扱いを誤った場合、「死亡または重傷を負う危険が生じるおそれ大きい」注意事項を示しています。
 警告	取り扱いを誤った場合、「死亡または重傷を負う危険が生じるおそれがある」注意事項を示しています。
 注意	取り扱いを誤った場合、「軽傷を負う可能性が想定される場合および物的損害が想定される」注意事項を示しています。

■ 記号





注意事項の内容は、以下の記号で示しています。

 注意	一般的な注意事項を示しています。
 感電注意	感電の可能性が想定されることを示しています。
 禁止	一般的な禁止事項を示しています。
 分解禁止	分解してはいけないことを示しています。
 濡れ手禁止	濡れた手で扱ってはいけないことを示しています。
 指示	必ず実行していただくことを示しています。

⚠ 危険







 禁止	高温になる場所や熱のこもりやすい場所（火のそば、暖房器具のそば、直射日光の当たる場所など）で使用、保管、放置しないでください。 火災、けが、感電の原因となります。
 禁止	飲料水、汗、海水、ペットの尿などの液体で本製品を濡らさないでください。 火災、やけど、けが、感電の原因となります。
 禁止	コネクターに飲料水、汗、海水、ペットの尿などの液体を入れないでください。 火災、やけど、けが、感電の原因となります。
 禁止	砂や土、泥をかけたり、直に置いたりしないでください。また、砂などが付着した手で本製品に触れないでください。 火災、やけど、けが、感電の原因となります。
 分解禁止	分解、改造をしないでください。 火災、やけど、けが、感電の原因となります。
 感電注意	雷が発生している際は、本製品やケーブルに触れないでください。 感電の原因となります。

⚠ 警告

 注意	煙や異臭、異常な音、手で触れられないほど熱いときは、すぐに本製品の電源を切ってください。 火災、やけど、感電の原因となります。
 禁止	落下させる、踏みつける、投げつけるなど強い力や衝撃、振動を与えないでください。 火災、やけど、けが、感電の原因となります。
 濡れ手禁止	手がぬれた状態で本製品やケーブルに触れないでください。 感電の原因となります。
 禁止	本製品の内部に以下のような異物を入れないでください。 ショートによる火災の原因となります。 <ul style="list-style-type: none"> ・ 金属物 ・ 水などの液体 ・ 燃えやすい物質 ・ 薬品

 禁止	<p>付属の AC アダプター以外で使用しないでください。 火災、感電、発煙の原因となります。</p>
 禁止	<p>付属の AC アダプターのコードを傷つけないでください。 火災や感電の原因となります。</p>
 指示	<p>AC アダプターを取り扱う際は、以下の点をお守りください。 火災、感電、発火、発煙の原因となります。</p> <ul style="list-style-type: none"> ・ 折れ曲がった状態や束ねた状態で使用しない。 ・ つけ根の部分を無理に曲げない。 ・ 重いものを載せない。 ・ 布などでくるまない。
 禁止	<p>不安定な場所に置かないでください。 転倒、落下などにより、けがの原因となります。</p>
 指示	<p>設置・移動するときは電源プラグを抜いてください。 感電の原因となります。</p>
 指示	<p>接続・取り付け作業は電源を切った状態で行ってください。 感電の原因となります。</p>
 指示	<p>ビニール袋などの梱包材料は、お子さま（特に乳幼児）の手の届かない場所に保管してください。 口に入れたり、頭からかぶったりすることで、窒息事故の原因となります。</p>
 指示	<p>医用電気機器などを装着している場合は、医用電気機器メーカーまたは販売業者に、電波による影響についてご確認のうえご使用ください。 電波により医用電気機器などに悪影響を及ぼす場合があります。</p>
 指示	<p>高精度な制御や微弱な信号を取り扱う電子機器の近くでは、本製品を使用しないでください。 電波により電子機器（補聴器、心臓ペースメーカーなど）が誤動作するなどの悪影響を及ぼす場合があります。</p>

⚠ 注意

 禁止	<p>本製品を以下のような場所で使用しないでください。 感電の原因となります。</p> <ul style="list-style-type: none"> • 風呂場など、湿気の多い場所 • 料理台や加湿器のそばなど、水、湿気、湯気、油煙などの多い場所
 禁止	<p>通電中や電源を切った直後は、本製品に直接触れないでください。 火傷の原因となります。</p>
 禁止	<p>アンテナに強い力を加えないでください。 破損の原因となります。</p>
 禁止	<p>電源プラグにほこりがたまったままの状態では本製品を使用しないでください。 火災の原因となります。</p>
 指示	<p>お手入れの際は、必ず本製品の電源を切り、ACアダプターを抜いてください。 感電の原因となります。</p>
 指示	<p>本製品を長期間使用しないときは、ACアダプターを抜いてください。 絶縁劣化による漏電火災の原因となります。</p>

取り扱い上のお願ひ

■ 使用環境

- 振動や衝撃の多い場所では使用しないでください。また、本製品を落下させないでください。内部の精密部品に影響を及ぼし、性能低下や故障の原因となります。
- 直射日光の当たる場所や高温になる場所、極端に低温になる場所、湿気やほこりの多い場所で使用、保管しないでください。故障の原因となります。
- 仕様で定められた温度、湿度の範囲内でご使用ください。
- データの書き込み中や通信中に、振動や衝撃を与えたり、電源を切ったりしないでください。データの消失・故障の原因となります。

■ 設置

- 腐食性の薬品のそばや腐食性ガスの発生する場所に設置しないでください。
- 低温で溶ける物質や発火する物質に触れる場所に設置しないでください。
- カメラやケーブルなどを着脱する際は、必ず本製品の電源を切ってください。電源を入れた状態でカメラやケーブルなどを着脱すると、破損の原因となります。
- ケーブルを引っ張ったり、曲げたりしてコネクタに負荷をかけないでください。コネクタが破損する原因となります。

■ その他

- お手入れは、本製品の電源を切ってから行ってください。
- お手入れは乾いた柔らかい布で拭いてください。アルコール、シンナー、ベンジン、洗剤、ガラスクリーナーなどで拭くと、故障の原因となります。
- 本製品の譲渡および廃棄時は、登録したデータをすべて消去してください。データが残っている場合、悪意のある第三者が不正に読み出し、漏えいする危険性があります。
- 万一、本製品に異常を感じた場合は、すぐに使用を中止し、電源を切ったうえで弊社までご連絡ください。

目次

はじめに.....	2
お問い合わせ先.....	3
改版履歴.....	3
安全上のご注意.....	4
目次.....	9
1 クイックスタート	17
1.1 設置要件	17
1.2 基本設定フロー	18
1.3 アクティベーションコード取得	18
1.3.1 管理プラットフォームにログイン.....	18
1.3.2 デバイスのアクティベーションコードの取得.....	21
1.4 デバイスのアクティベーション	23
1.4.1 デバイスの電源オン	23
1.4.2 デバイスの表示言語選択	23
1.4.3 日付と時刻の設定	24
1.4.4 稼働モードの選択	25
1.4.5 ネットワークの設定	25
1.4.5.1 WLAN	26
1.4.5.2 LAN	26
1.4.6 アクティベーションコードの入力.....	27
1.4.7 利用許諾契約とプライバシー条項の確認.....	29
1.4.8 デバイス管理者の作成と登録.....	30
1.4.8.1 デバイス管理者の作成.....	30
1.4.8.2 デバイス管理者の登録.....	31
1.4.9 ワークモードの選択	32
1.4.9.1 デバイスへのログイン.....	32
1.4.9.2 ワークモードの選択.....	33
1.4.10 アラーム通知の登録	34
1.4.11 デバイスの登録者容量	35
1.4.12 利用者の登録	35
1.4.12.1 写真の規格	36
1.4.12.1.1 撮影要件	36
1.4.12.1.2 デジタル写真ファイルの規格.....	36
1.4.12.1.3 要件の例	36
1.4.12.1.3.1 光、露出、人物の位置.....	36

	1.4.12.1.3.2 背景.....	37
	1.4.12.1.3.3 姿勢.....	37
	1.4.12.1.3.4 表情.....	37
	1.4.12.1.3.5 顔にかぶさる物.....	38
	1.4.12.1.3.6 規格・その他.....	38
	1.4.12.2 個別登録.....	39
	1.4.12.3 バッチ登録.....	40
1.4.13	通行規則の作成と適用.....	45
	1.4.13.1 通行規則の作成.....	45
	1.4.13.2 通行規則の適用.....	47
2	デバイス.....	50
2.1	システム概要.....	50
	2.1.1 システム構成.....	50
	2.1.2 一般的な使用の流れ.....	50
2.2	ハードウェア.....	52
	2.2.1 本体のサイズ(単位:mm).....	52
	2.2.2 温度測定モジュールのサイズ(単位:mm).....	52
	2.2.3 指紋モジュールのサイズ(単位:mm).....	53
	2.2.4 ポート説明.....	54
	2.2.5 仕様.....	54
	2.2.6 設置について.....	55
	2.2.7 設置高さについて.....	56
2.3	デバイス操作ガイド.....	56
	2.3.1 前提条件.....	56
	2.3.2 操作概要.....	56
	2.3.3 デバイスの電源オン/オフ.....	57
	2.3.3.1 電源をオンにする.....	58
	2.3.3.2 シャットダウン/再起動.....	58
	2.3.3.3 デバイスログの保存.....	58
	2.3.4 デバイスのアクティベート.....	58
	2.3.4.1 デバイスのアクティベート (クラウドサービスモード).....	58
	2.3.4.1.1 前提条件.....	59
	2.3.4.1.2 デバイス基本情報の設定.....	59
	2.3.4.1.3 ネットワーク接続の設定.....	59
	2.3.4.1.4 アクティベーションコードの入力.....	60
	2.3.4.1.5 使用開始.....	61
	2.3.4.2 デバイス管理者の追加 (クラウドサービスモード).....	61
	2.3.5 デバイスの設定.....	61
	2.3.5.1 デバイスへのログインと管理.....	61
	2.3.5.2 ホームボタンの設定.....	62
	2.3.5.3 基本設定.....	63
	2.3.5.3.1 情報.....	63

2.3.5.3.2	容量	64
2.3.5.3.3	記録統計	64
2.3.5.3.4	一般設定	65
2.3.5.3.5	ワークモード.....	66
2.3.5.3.6	検証順	67
2.3.5.3.7	顔識別設定	67
2.3.5.3.7.1	採集精度.....	69
2.3.5.3.7.2	マスク検知.....	70
2.3.5.3.7.3	識別モード.....	71
2.3.5.3.7.4	使用シーン.....	72
2.3.5.3.7.5	認証対象.....	75
2.3.5.3.7.6	繰り返し識別間隔.....	75
2.3.5.3.7.7	背景画像の特定.....	76
2.3.5.3.7.8	検証結果の表示時間.....	76
2.3.5.3.7.9	顔検出フレーム.....	77
2.3.5.3.7.10	顔追跡.....	77
2.3.5.3.8	温度測定設定.....	77
2.3.5.3.9	IC カード照合設定.....	79
2.3.5.3.10	識別ルール	80
2.3.5.3.11	デバイスルール.....	80
2.3.5.3.12	登録管理	81
2.3.5.3.13	ネットワーク.....	82
2.3.5.3.14	Bluetooth	83
2.3.5.3.15	日付と時刻	83
2.3.5.3.16	再起動	83
2.3.5.3.17	工場出荷時の状態に戻す.....	83
2.3.5.3.18	デフォルト設定に戻す.....	83
2.3.5.3.19	ドアオープン.....	83
2.3.5.3.20	ドアオープン保持.....	83
2.3.5.3.21	システム更新.....	83
2.3.5.3.22	管理者	85
2.3.5.3.23	Bluetooth ロック	86
2.3.5.3.24	指紋登録	86
2.3.5.4	拡張設定	86
2.3.5.4.1	カメラ設定	86
2.3.5.4.2	識別記録	88
2.3.5.4.3	案内設定	90
2.3.5.4.4	アクセスコントロール.....	92
2.3.5.4.5	コンテンツ再生.....	95
2.3.5.4.6	ODSL 拡張設定.....	98
2.3.5.4.7	ライセンス	98
2.3.5.4.8	取り外しアラーム.....	98

2.3.5.4.9	登録写真の最小サイズ.....	98
2.3.5.4.10	ローカルに登録写真を不保持.....	99
2.3.5.4.11	拡張アプリ	100
2.3.5.4.12	照合登録者ライブラリと小 N ライブラリの閾値	100
2.3.5.4.13	ウェブ管理機能.....	100
2.3.5.4.14	距離センサー設定.....	101
2.3.6	デバイスのメンテナンス	102
2.3.6.1	警告メッセージ	102
2.3.6.2	ステータスの確認.....	103
2.3.6.3	デバイス情報の確認.....	103
2.3.6.4	使用容量の確認	103
2.3.6.5	再起動	104
2.3.6.6	工場出荷状態に戻す.....	104
2.3.6.7	オープン/ドアオープン保持	105
2.3.6.8	デバイスのウェブ管理機能ツール.....	105
3	クラウド管理プラットフォーム	106
3.1	概要説明	106
3.1.1	概要	106
3.1.2	デバイス設定	106
3.1.3	登録者設定	107
3.1.4	アクセス設定	108
3.1.5	アプリ設定	108
3.1.6	システムメンテナンス	108
3.2	操作説明 (ユーザーセンター)	109
3.2.1	ログイン	109
3.2.2	パスワード取得	110
3.2.3	個人情報変更	110
3.3	操作について (クラウド管理プラットフォーム)	110
3.3.1	概要説明	110
3.3.2	ダッシュボード	111
3.3.2.1	トップページ	111
3.3.2.1.1	概要情報の確認.....	112
3.3.2.1.2	ユーザー情報の変更.....	112
3.3.2.2	アラームセンター.....	113
3.3.2.2.1	デバイスアラームの確認.....	113
3.3.2.3	操作ログ	114
3.3.2.3.1	操作ログの確認.....	115
3.3.3	登録管理	115
3.3.3.1	登録管理	115
3.3.3.1.1	登録者の検索.....	116
3.3.3.1.2	登録者詳細情報の照合.....	116
3.3.3.1.3	登録者の個別追加.....	117

3.3.3.1.4	登録者の一括追加.....	118
3.3.3.1.5	登録者の編集.....	119
3.3.3.1.6	登録者の削除.....	119
3.3.3.1.7	登録者の一括削除.....	119
3.3.3.1.8	登録者データの一括エクスポート.....	120
3.3.3.1.9	表示項目設定.....	120
3.3.3.2	組織管理.....	120
3.3.3.2.1	組織の確認.....	121
3.3.3.2.2	組織の追加.....	121
3.3.3.2.3	組織の編集.....	122
3.3.3.2.4	組織の削除.....	122
3.3.4	デバイス管理.....	122
3.3.4.1	デバイス管理.....	122
3.3.4.1.1	デバイスの確認.....	123
3.3.4.1.2	デバイス設定のクローン配信.....	124
3.3.4.1.3	プロンプトメッセージのインポートと送信.....	124
3.3.4.1.4	アクティベーションコード.....	125
3.3.4.1.5	デバイスの再起動.....	125
3.3.4.1.6	デバイスの設定.....	125
3.3.4.1.6.1	本体について.....	125
3.3.4.1.6.2	ワークモード.....	126
3.3.4.1.6.3	検証順.....	126
3.3.4.1.6.4	一般設定.....	126
3.3.4.1.6.5	顔識別設定.....	127
3.3.4.1.6.6	温度測定設定.....	129
3.3.4.1.6.7	アクセス制御信号設定.....	129
3.3.4.1.6.8	カメラ設定.....	130
3.3.4.1.6.9	ICカード照合設定.....	131
3.3.4.1.6.10	案内設定.....	132
3.3.4.1.6.11	コンテンツ再生.....	133
3.3.4.1.6.12	システム更新.....	134
3.3.4.1.6.13	日付と時刻.....	134
3.3.4.1.6.14	取り外しアラーム.....	134
3.3.4.1.6.15	登録写真の最小サイズ.....	134
3.3.4.1.6.16	識別記録.....	135
3.3.4.1.6.17	距離センサー設定.....	135
3.3.4.1.6.18	デバイスのウェブ管理機能.....	136
3.3.4.1.7	遠隔解錠.....	136
3.3.4.2	デバイスグループ.....	137
3.3.4.2.1	デバイスグループの確認.....	137
3.3.4.2.2	デバイスグループの追加.....	138
3.3.4.2.3	デバイスグループの編集.....	138

3.3.4.2.4	デバイスグループの削除.....	138
3.3.4.3	管理者	139
3.3.4.3.1	管理者の確認.....	139
3.3.4.3.2	管理者の追加.....	140
3.3.4.3.3	管理者の編集.....	140
3.3.4.3.4	管理者の削除.....	140
3.3.4.3.5	関連付けられているデバイス.....	141
3.3.4.4	設定管理	141
3.3.4.4.1	デバイスの設定管理.....	142
3.3.4.4.2	認証閾値ライブラリの追加.....	145
3.3.4.4.3	認識パラメータライブラリの編集.....	145
3.3.4.4.4	認証閾値ライブラリの削除.....	145
3.3.4.4.5	認証閾値ライブラリのパラメータ設定.....	146
3.3.4.4.6	デバイス設定の同期.....	146
3.3.4.5	コマンド配信記録.....	146
3.3.4.5.1	送信記録の確認.....	147
3.3.5	権限	148
3.3.5.1	ロール管理	148
3.3.5.1.1	ロールの確認.....	148
3.3.5.1.2	ロールの追加.....	148
3.3.5.1.3	ロールの編集.....	149
3.3.5.1.4	ロールの削除.....	149
3.3.5.2	権限付与	150
3.3.5.2.1	アカウントの検索.....	150
3.3.5.2.2	アカウントの追加.....	151
3.3.5.2.3	アカウントの編集.....	151
3.3.5.2.4	アカウントの削除.....	152
3.3.6	データ管理	152
3.3.6.1	認識記録	152
3.3.6.1.1	認識記録の確認.....	153
3.3.6.1.2	認識記録のエクスポート.....	154
3.3.6.1.3	認識記録の削除.....	154
3.3.6.1.4	認識記録の一括削除.....	155
3.3.6.1.5	記録のエクスポート履歴の確認.....	155
3.3.7	業務管理	155
3.3.7.1	通行規則	155
3.3.7.1.1	通行規則の確認.....	156
3.3.7.1.2	通行規則の追加.....	156
3.3.7.1.3	時間規則の追加.....	157
3.3.7.1.4	適用単位	157
3.3.7.1.5	通行規則の編集.....	158
3.3.7.1.6	通行規則の削除.....	158

3.3.7.1.7	通行規則の一括削除.....	158
3.3.7.2	ルール配信	159
3.3.7.2.1	通行規則の送信.....	159
3.3.8	アプリ	159
3.3.8.1	アプリ管理	160
3.3.8.1.1	アプリの確認.....	160
3.3.8.1.2	アプリの作成.....	160
3.3.8.1.3	イベントの説明.....	161
3.3.8.1.4	アプリの編集.....	162
3.3.8.1.5	アプリの無効化.....	163
3.3.8.1.6	アプリの削除.....	163
3.3.8.1.7	トークンの削除.....	163
3.3.9	システムの管理	163
3.3.9.1	システムアーカイブ.....	163
3.3.9.1.1	認識記録のアーカイブ	164
3.3.9.2	アカウント	164
3.3.9.2.1	自動登録招待のオン/オフ	165
3.3.9.3	メインアカウント.....	165
3.3.9.3.1	メイン管理者の変更.....	166
3.3.9.4	アラーム通知	166
3.3.9.4.1	アラーム通知の登録.....	166
3.3.9.4.2	アラーム通知の編集.....	167
3.3.9.4.3	アラーム通知の削除.....	167
4	インタラクティブ	167
4.1	認証	167
4.1.1	スタンバイ状態	167
4.1.2	認証プロセス	168
4.1.3	認証結果	169
4.2	温度測定	170
4.2.1	温度測定プロセス	170
4.2.2	認証結果	171
4.2.2.1	温度測定モード	171
4.2.2.2	温度測定+顔認証モード.....	172
4.3	メンテナンス情報	175
4.3.1	警告メッセージ	175
4.3.2	ステータスの確認	175
4.3.3	デバイス情報の確認	176
4.3.4	使用容量の確認	176
5	拡張方法	177
5.1	概要説明	177
5.2	WebAPI(RESTful).....	177
6	付録	179

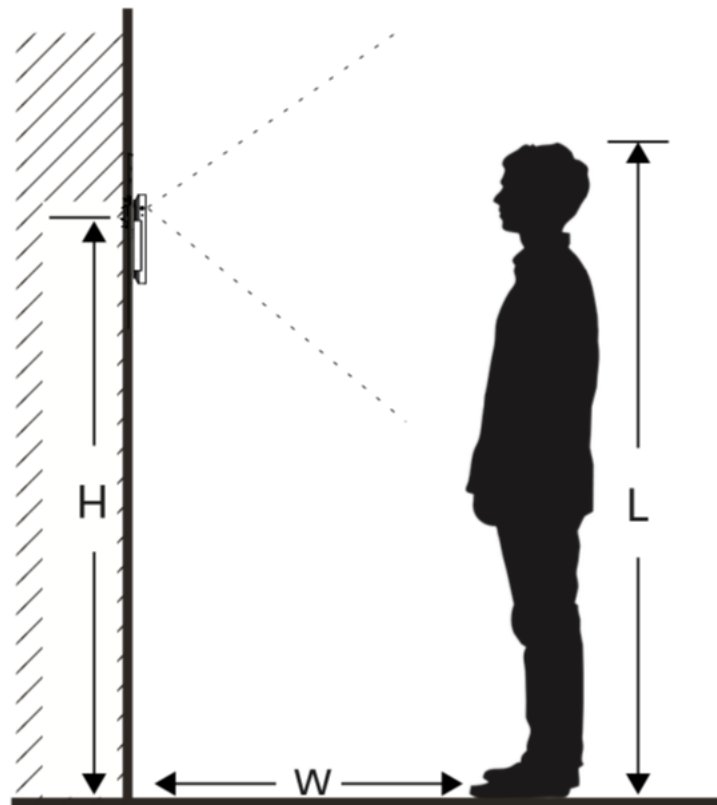
6.1	デバイスの登録者容量ライセンス.....	179
6.2	認証方法の説明	179
7	FAQ.....	183
7.1	デバイスが管理プラットフォームへ接続できません。	183
7.2	一つのクラウドアカウントへ複数同時にログインができません。	183
7.3	アクティベーションコードを更新した場合、旧コードを使用できますか。	183

1 クイックスタート

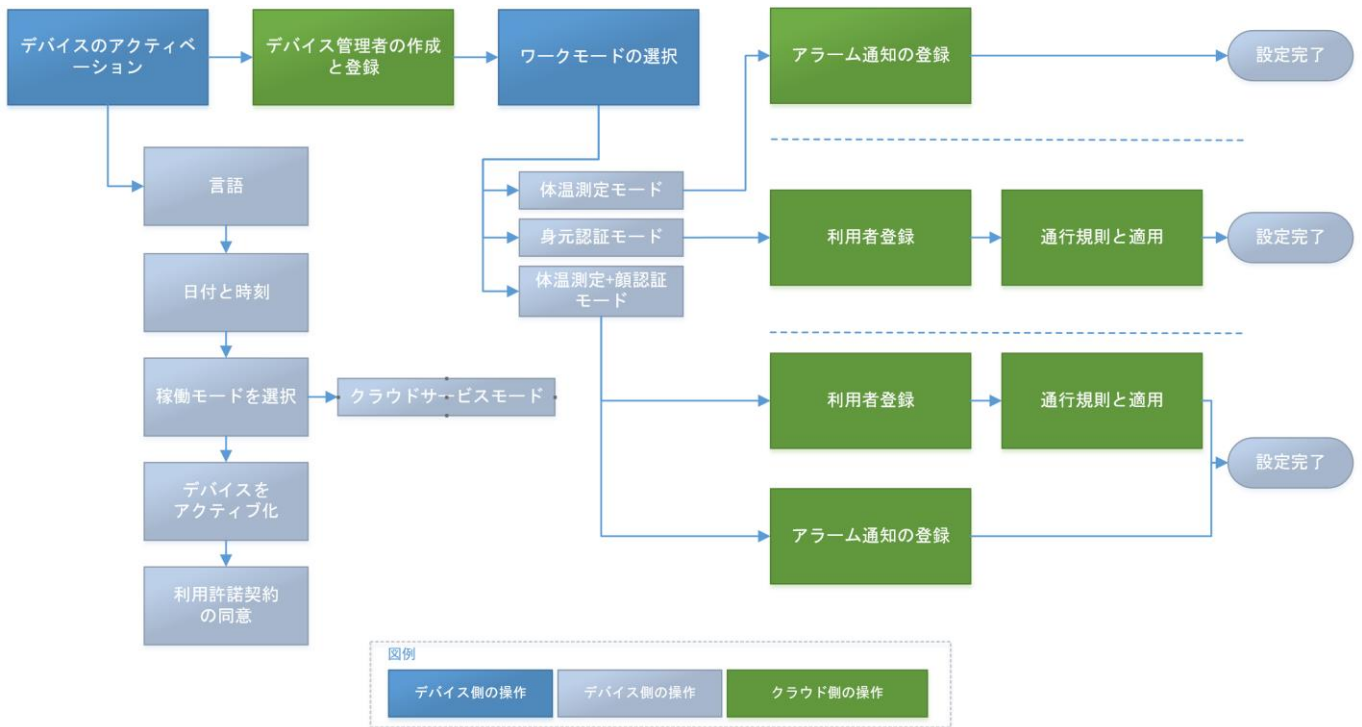
1.1 設置要件

注意事項：

- 1、デバイスの設置高さ（認証カメラの地面からの高さ）：1.5m、認証可能距離：50～130cm、認証可能身長範囲：110～220cm。
- 2、デバイスは光源から少なくとも2メートル離して設置してください。
- 3、温度測定の場合、**認証距離 50～130cm、身長 120～190cm**
- 4、温度測定の場合、室内環境での使用を前提とするもので、温度測定の結果に影響しないよう、**撮影範囲内には高温熱源を置かないでください。**
- 5、温度測定の場合、温度測定カメラの電源をオンにしてから20分間のウォームアップで、測定精度がより高まります。



1.2 基本設定フロー



1.3 アクティベーションコード取得

1.3.1 管理プラットフォームにログイン

ステップ1 <https://gk.edgемatrix.com/> を開きます。



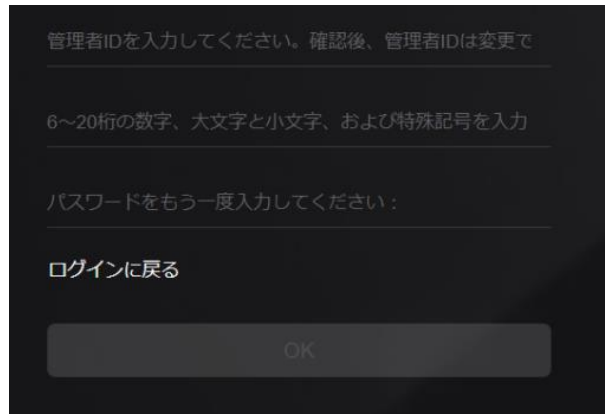
- ◇ 管理プラットフォームへログイン用のアカウントとパスワードをお分かりにならない場合は、EDGEMATRIX 株式会社にお問い合わせください。

ステップ2 アカウント(メールアドレス)とパスワードを入力して、「認証コードを取得」をクリックします。
 ログイン ID が作成されていない場合には、ステップ3に進みます。
 ログイン ID が作成されている場合には、ステップ4へと続きます。



- ◇ アカウントのメールアドレスとは、利用者様がクラウドサービスを申請する時に提出したメールアドレスです。
- ◇ メールアドレスはログイン後に変更することが可能です。

ステップ3 ログイン ID が作成されていない場合、ログイン ID 作成画面が表示されます



- 1、新規ログイン ID を入力する
- 2、新しいパスワードを入力する
- 3、「OK」をクリックする

ログイン ID が正常に設定されると再度ログイン画面に戻ります。

再度メールアドレス/ログイン ID、パスワード入力後にステップ4の認証コード受信へと進みます。

- ◇ ログイン ID は一度作成したら、後から変更することが出来ません。なお、パスワードは後から変更できます。
- ◇ ログイン ID が既に作成されている場合には、この画面は表示されません。
- ◇ ログイン ID はすべて半角文字にて、最初の文字は必ずアルファベット指定で、あとはアルファベットと数字と三つの特殊文字(. _ -)の組み合わせで入力してください。ログイン ID の文字数は、6~100文字(半角)です。
- ◇ ログイン ID が作成されている場合には、ログイン画面ではログイン ID とメールアドレスのどちらでもログインできます。

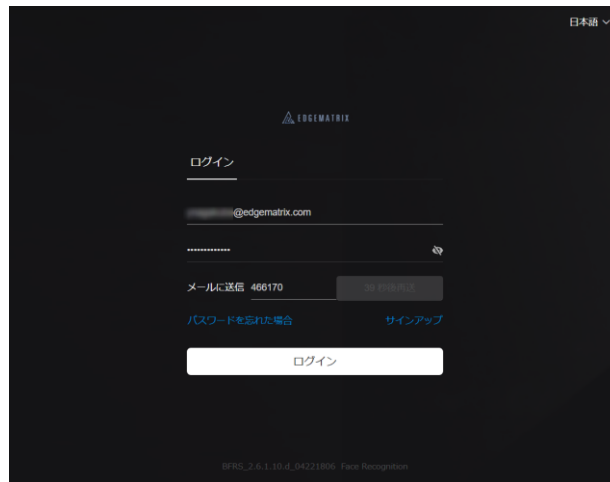
ステップ4 6桁の数字コードを受信します。

EdgeMatrix Account Register

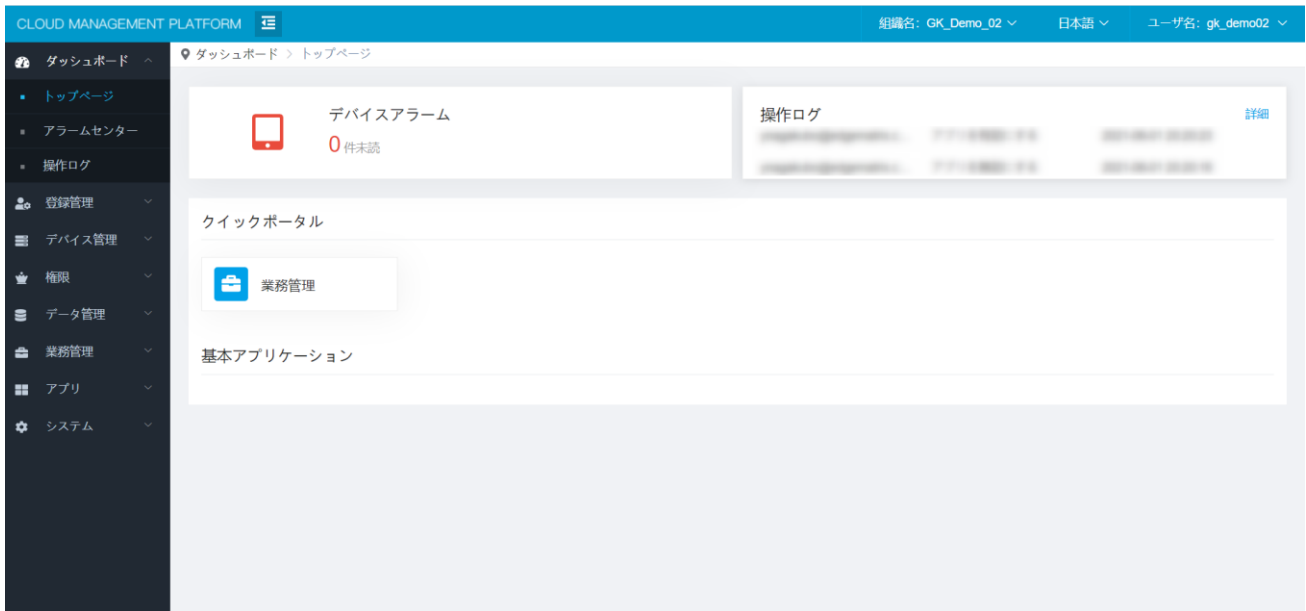
Dear Customer, The current verification code for login is [466170], which is valid for 5 minutes, please check

Edgematrix Support Team

6桁の数字コードを入力し、「ログイン」をクリックします。



ダッシュボードのトップページが開きます。



1.3.2 デバイスのアクティベーションコードの取得

ステップ1 デバイス管理が開きます。

アクセス手順：左側メニュー → デバイス管理 → デバイス管理

CLOUD MANAGEMENT PLATFORM 組織名: GK_Demo_02 | 日本語 | ユーザー名: gk_demo02

📍 デバイス管理 > デバイス管理

デバイス名: シリアル番号: タイプ:
 デバイスグループ: 管理者: 状態:

<input type="checkbox"/>	デバイス名	シリアル番号	タイプ	デバイスグル...	ROMバージ...	管理者	状態	操作時間	操作
<input type="checkbox"/>	オフライン	...	設定 ドアオープン
<input type="checkbox"/>	オフライン	...	設定 ドアオープン
<input type="checkbox"/>	オフライン	...	設定 ドアオープン
<input type="checkbox"/>	オフライン	...	設定 ドアオープン
<input type="checkbox"/>	オンライン	...	設定 ドアオープン
<input type="checkbox"/>	オンライン	...	設定 ドアオープン

合計 6 件 < 1 > Go to 1 ページ目へ

ステップ2 アクティベーションコードをクリックします。
 アクティベーションコードを表示します。



ドメインとコードを記録してください。
 または QR コードをプリントアウトするか、チャプチャー等で残して下さい。

- ◇ デバイスをアクティブ化する際、QR コードをスキャンさせることで、ドメインとコードを手入力する作業が省けます。
- ◇ アクティベーションコードは、「リフレッシュ」ボタンをクリックするたびに更新されます。更新されると旧アクティベーションコードは即時無効となります。

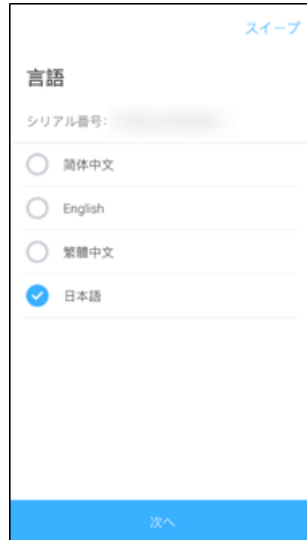
1.4 デバイスのアクティベーション

1.4.1 デバイスの電源オン

デバイスがシャットダウンしている状態で電源ボタンを長押し、デバイスの電源をオンにします。
 デバイスが初めて電源オンになる場合にはアクティベーション画面に進みます。

1.4.2 デバイスの表示言語選択

「言語」画面で、デバイスのシステム言語を設定します。



「次へ」をタップして、「日付と時刻」画面を開きます。



◇ デバイスのシステム言語は後から変更できます。

1.4.3 日付と時刻の設定

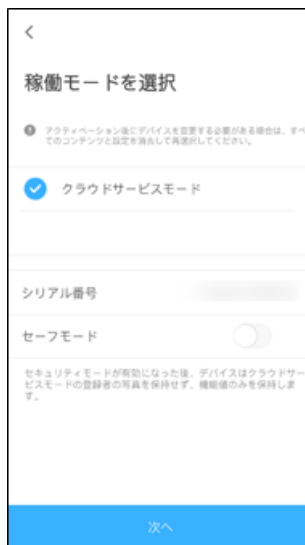
「日付と時刻」画面で、自動設定をオンにします（既定値）。
デバイスのタイムゾーンを設定します。




「次へ」をタップして、「稼働モードを選択」画面を開きます。

1.4.4 稼働モードの選択

「稼働モードの選択」画面で、「クラウドサービスモード」を選択します。



- ◇ ローカルに登録写真を不保持/セーフモードをオンにすると、デバイスには登録者の写真をクラウド側からダウンロードせずに特徴値のみを保持となります。
- 
 ◇ ローカルに登録写真を不保持は一度選択すると変更できません。変更する場合、出荷時状態にまで戻す必要があります。

「次へ」をタップして、「ネットワーク」画面を開きます。

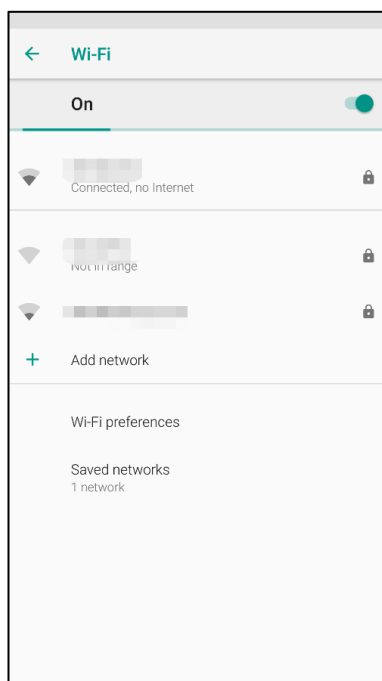
1.4.5 ネットワークの設定

「ネットワーク」画面で、デバイスのネットワーク接続を設定します。デバイスは「WLAN」と「LAN」の2種類のネットワーク接続方式をサポートしています。実際の運用に応じて選択してください。



1.4.5.1 WLAN

「WLAN」を選択して「WLAN」画面を開き、無線ネットワークを設定します。



1.4.5.2 LAN

「LAN」を選択して「LAN」画面を開き、有線ネットワークを設定します。

デバイスは IP アドレスの自動取得または手動取得の 2 種類の設定方法がサポートされています。



1.4.6 アクティベーションコードの入力



入力項目の説明

NO.	項目	説明
1	サーバーアドレス	必須、変更不可
2	コード	必須、変更不可

3	デバイス名	オプション、変更可
4	デバイスグループコード	オプション、変更可

入力方法 1 : QR コードをスキャンして、サーバーアドレス、アクティベーションコード、デバイスのグループ名などの情報が含まれる QR コードを読み取らせ、情報を自動的に入力させます。

入力方法 2 : ソフトキーボードで手入力する。

「ターミナルをアクティブにする」をタップして、「ようこそ」の画面を開きます。

1.4.7 利用許諾契約とプライバシー条項の確認

「ようこそ」の画面で、「使用開始」をタップしてください。



アクティベーションが完了して、機能動作画面が開きます。



- ✧ デバイス管理者を登録しない場合、デバイスの管理画面にアクセスはできません。
- ✧ クラウドでデフォルトデバイス管理者が設定された場合、デバイスアクティベート時にデバイスに適用されます。

1.4.8 デバイス管理者の作成と登録

1.4.8.1 デバイス管理者の作成

アクセス手順：左側メニュー → デバイス管理 → 管理者



「新規追加」をクリックして、「デバイス管理者の新規追加」画面を開きます。

新規追加 ×

* 名前

* パスワード

携帯電話

* 写真

+

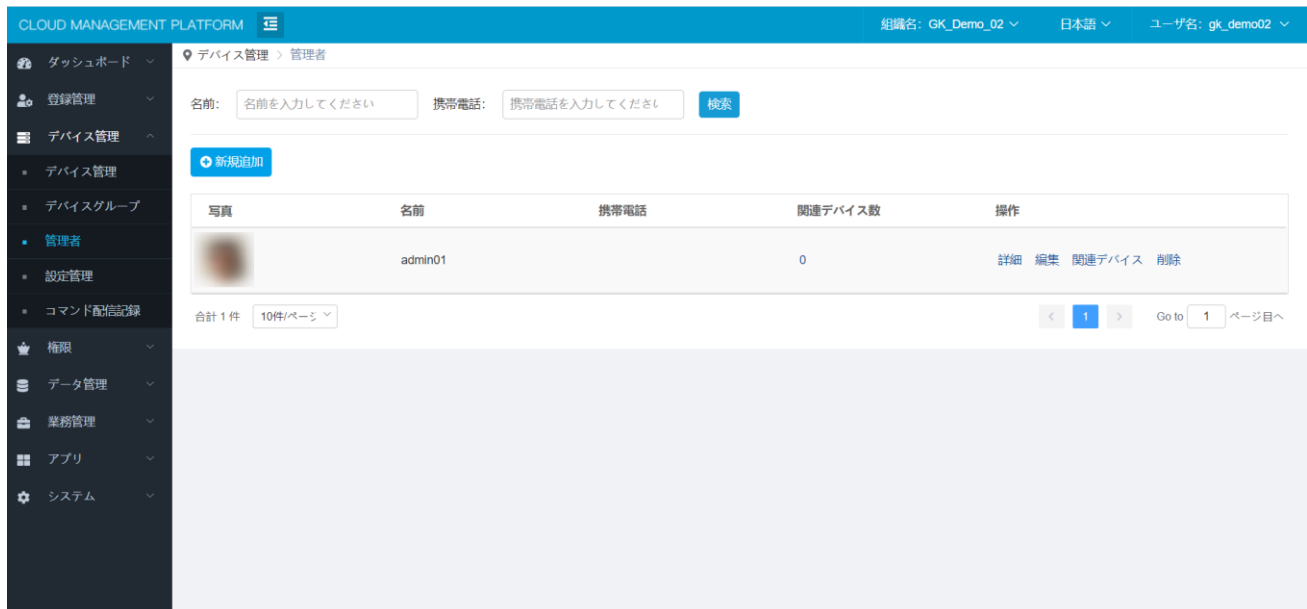
顔を正面に向けたまま、目を閉じていなく、無帽、無マスク、画像ソフト等での加工なしの写真を利用してください。

デフォルト管 (チェックした場合、この管理者がデフォルトの管理者として設定され
理者

入力項目の説明

NO.	項目	説明
1	名前	必須
2	パスワード（4桁の数字）	必須
3	携帯電話	オプション
4	写真	必須
5	デフォルト管理者	オプション チェックした場合、該当クラウドアカウントよりアクティブ化したデバイスへ自動的に設定されます。

入力が完了したら「OK」をクリックして、デバイス管理者を作成します。



1.4.8.2 デバイス管理者の登録

登録するデバイス管理者の「関連デバイス」をクリックして、「関連デバイス」画面が開きます。

登録するデバイスを選択して、「関連デバイス」をクリックします。



「関連デバイス数」が増えたことを確認してください。



デバイス管理者の登録を完了します。

- ◇ デバイス管理者とは、デバイスをタッチ画面から操作する場合とデバイスのウェブ管理機能からアクセスする場合の管理者です。
- ◇ クラウドサービスの管理者とは別アカウントとなります。
- ◇ 1台のデバイスに最大10人のデバイス管理者を設定できます。

1.4.9 ワークモードの選択

1.4.9.1 デバイスへのログイン

デバイスの認証画面で、下の上矢印をタップするかスライドすると、操作アイコンが表示されます。



赤枠に囲まれるアイコンをタッチして、管理者登録画面を開きます。

登録済みのデバイス管理者は「顔スキャン」と「パスワード」の2種類の方法でデバイスにログインできます。

ログインに成功した場合、デバイスの設定画面が開きます。

1.4.9.2 ワークモードの選択

アクセス手順：設定画面 → ワークモード



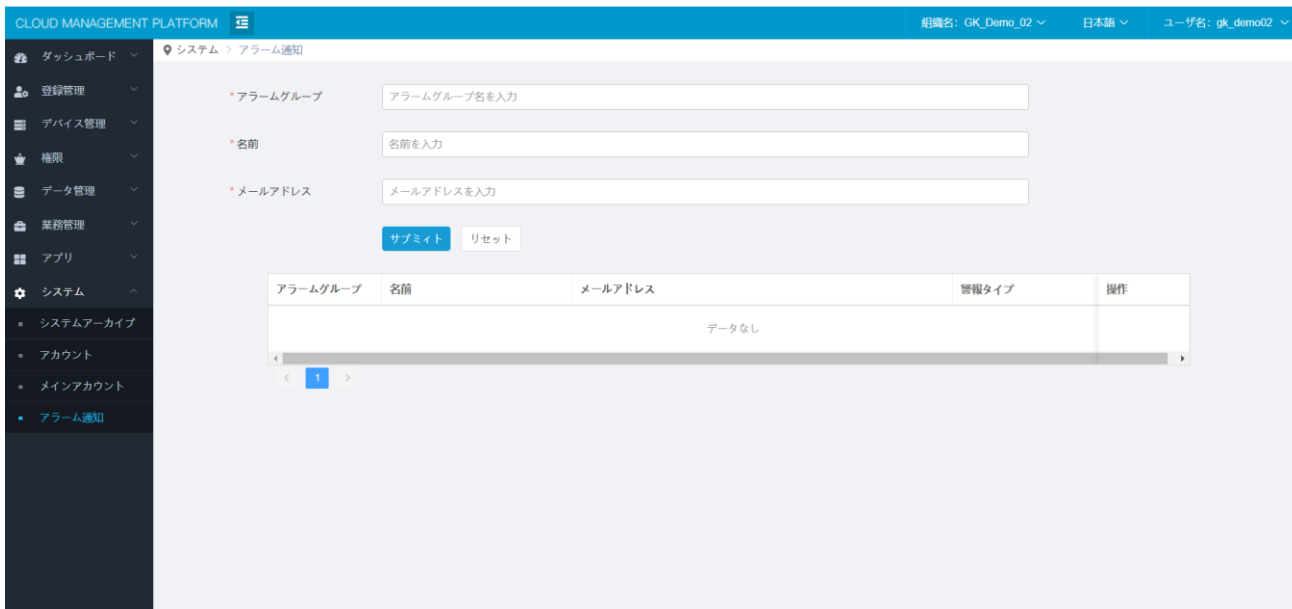
ワークモードの説明

NO.	項目	説明
1	温度測定モード	温度測定のみの場合 登録者は不要です
2	顔認証モード	顔認証のみの場合、既定値 登録者と通行規則の登録が必要 です
3	温度測定と顔認証モード	温度測定と顔認証を同時に行う 場合 登録者と通行規則の登録が必要 です

実際の運用に応じて、ワークモードを選択してください。

1.4.10 アラーム通知の登録

アクセス手順：左側メニュー → システム → アラーム通知



クラウド管理プラットフォームの「アラーム通知」登録画面のスクリーンショット。画面には入力フォームと一覧表が確認できる。

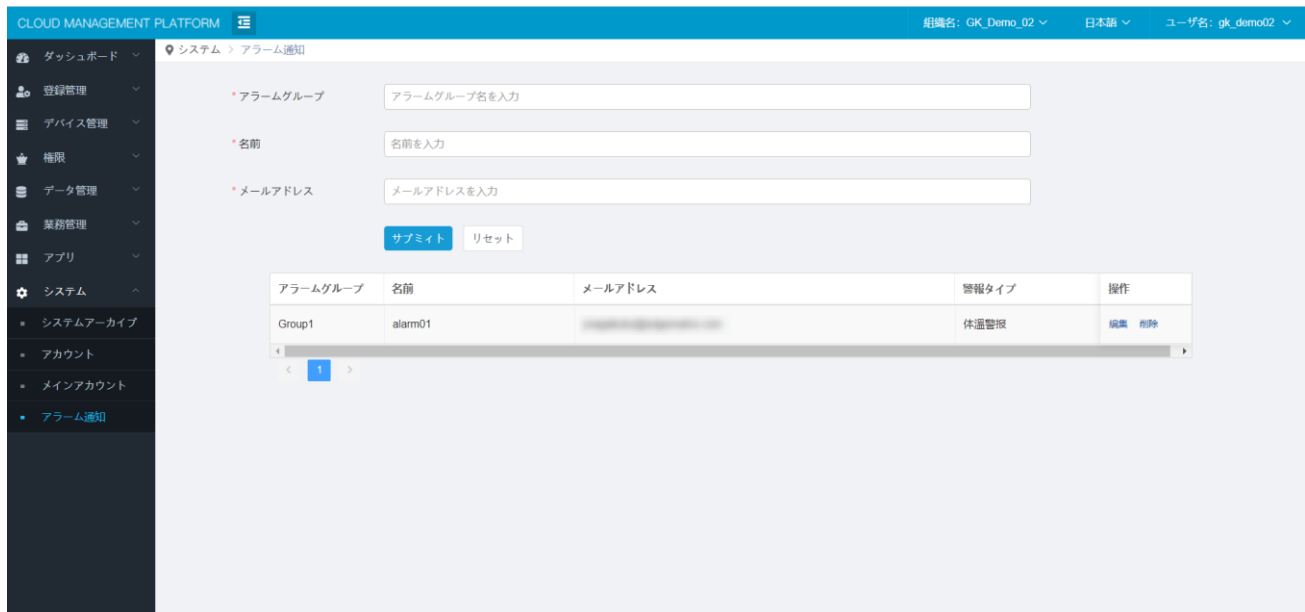
アラームグループ	名前	メールアドレス	警報タイプ	操作
データなし				

ステップ1 アラーム通知を登録します。

入力項目の説明

NO.	項目	説明
1	アラームグループ	必須
2	名前	必須
3	メールアドレス	必須

ステップ2 登録したアドレスが一覧表に表示されることを確認します。



◇ 現在、高体温のアラーム通知のみに対応します。

1.4.11 デバイスの登録者容量

デバイスのデフォルト登録数は 50,000 名です。

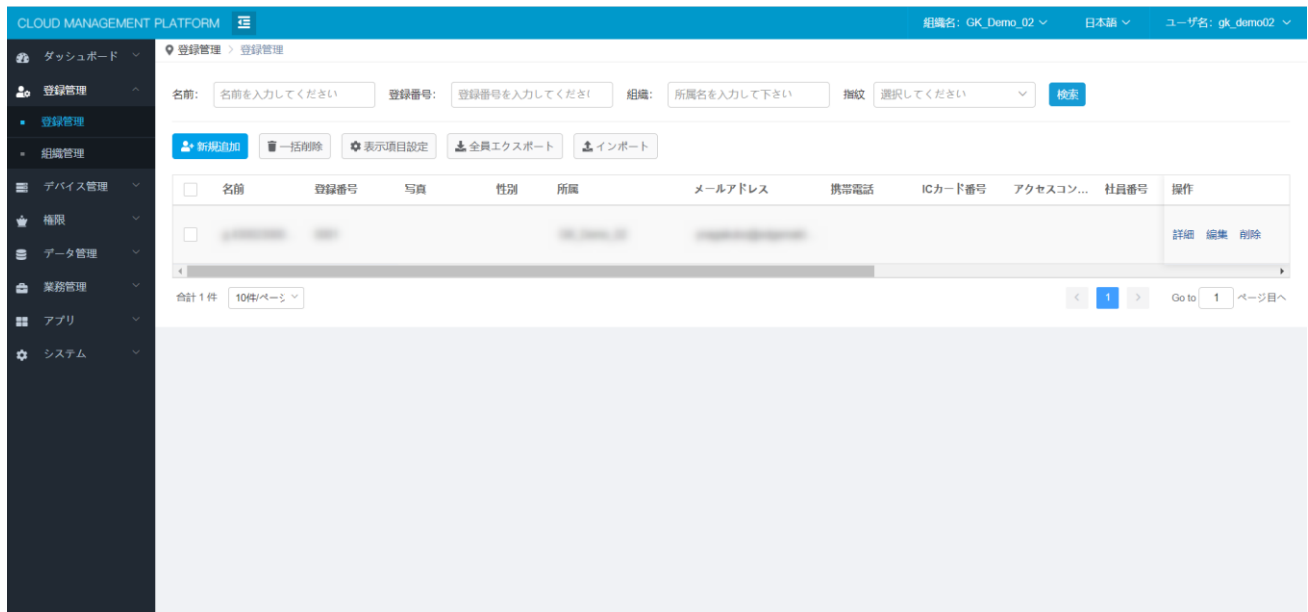
別料金で 100,000 人まで拡張できます。EDGEMATRIX 株式会社にお問い合わせください

- ◇ クラウド側の登録人数には、登録人数ライセンスは不要です。
- ◇ クラウドサービスモードをご利用の場合、デバイスの初回のクラウド接続時に登録人数ライセンスが自動的に適用されます。

詳細については、『6.1 デバイスの登録者容量ライセンス』をご参照ください。

1.4.12 利用者の登録

アクセス手順：左側メニュー → 登録管理 → 登録管理



利用者登録には、個別登録とバッチ登録の2種類の方法があります。

1.4.12.1 写真の規格

1.4.12.1.1 撮影要件

登録者は肩を水平に保ち、レンズをまっすぐ見る。

登録者は自然な姿勢で目を自然に開き、髪の毛が目にかぶさらないようにする。厚化粧を避ける。

登録者はメガネを外す。

照明を均一にし、顔が影や光ができないようにする。

背景色を均一にし、グラデーションや影、他の人物や物が映らないようにする。

1.4.12.1.2 デジタル写真ファイルの規格

ファイルの画像形式は、JPEG、JPG、PNG にする。

画像ファイルのサイズは 20KB～1MB にする。

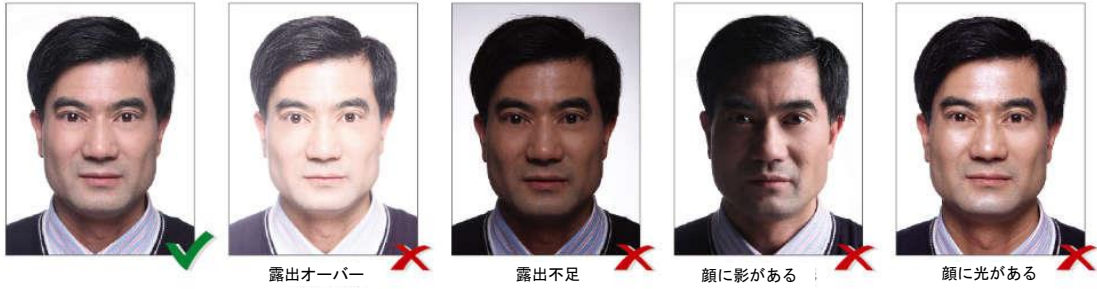
画像の解像度は 1024*1024 以下にする。

1.4.12.1.3 要件の例

1.4.12.1.3.1 光、露出、人物の位置

撮影環境の光を均一にし、人が中央にくるようにする。

適切な露出で、影や光ができないようにする。



1.4.12.1.3.2 背景

背景色を均一にし、グラデーション、他の人物や物が映らないようにする。
背景色を白または薄い青色で統一する。



1.4.12.1.3.3 姿勢

姿勢を整える
肩は自然に水平にする
レンズをまっすぐ見る



1.4.12.1.3.4 表情

自然な表情
目は自然に開く
口は自然に閉じる



1.4.12.1.3.5 顔にかぶさる物

髪の毛が目にかぶさらないようにする

登録者はかぶりものをしたり、一時的な装飾品で顔が覆われたりしてはいけません。顔と服は背景色と対照的でなければなりません。

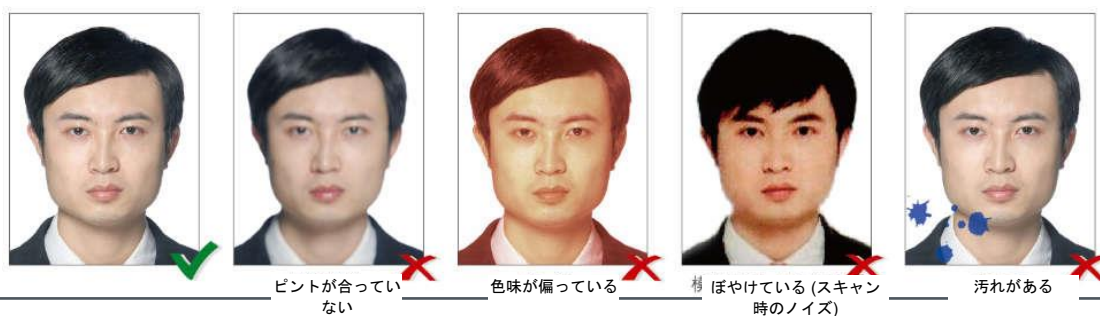


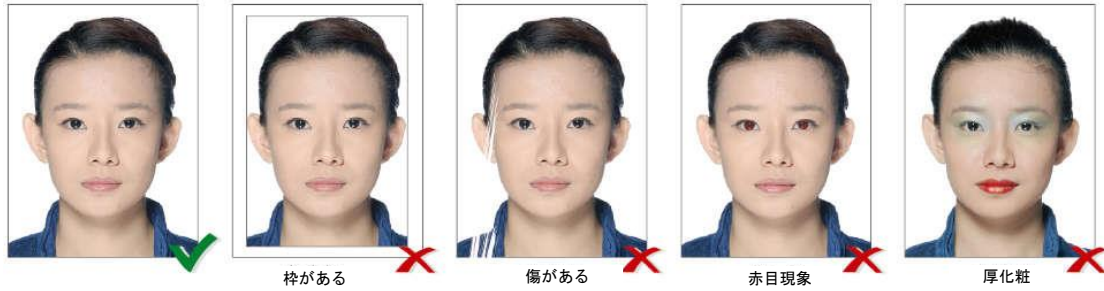
1.4.12.1.3.6 規格・その他

ピントを正確に合わせる、赤目現象がない、顔の歪みがない。

紙の写真の場合：人がはっきりと写っている。ぼやけ(スキャン時のノイズ)、汚れ、しわ、粹、傷があってはならない。

厚化粧を避ける





前後に遮る物があるてはならない(手、おもちゃなど)



1.4.12.2 個別登録

ステップ1 「新規追加」をクリックして、「新規追加」画面を開きます。

新規追加

<p>* 名前 <input type="text" value="名前を入力してください"/></p> <p>写真 <div style="border: 1px dashed gray; width: 60px; height: 60px; display: flex; align-items: center; justify-content: center; margin: 5px auto;">+</div> 顔を正面に向けたまま、目を閉じていなく、無帽、無マスク、画像ソフト等での加工なしの写真を利用してください。</p> <p>ICカード番号 <input type="text" value="ICカード番号を入力してください"/></p>	<p>* 登録番号 <input type="text" value="登録番号を入力してください"/></p> <p>性別 <input type="text" value="性別"/></p> <p>* 所属 <input type="text" value="GK_Demo_02"/></p> <p>メールアドレス <input type="text" value="メールアドレスを入力してください"/></p> <p>携帯電話 <input type="text" value="携帯電話を入力してください"/></p> <p>社員番号 <input type="text" value="社員番号を入力してください"/></p> <p>4桁パスワード <input type="text" value="4桁の数字パスワードを入力してください"/></p>
---	---

キャンセル

ステップ2 登録者の情報を入力します。


入力項目の説明

NO.	項目	説明
1	名前	必須

2	登録番号	必須
3	所属	必須
4	写真	オプション

ステップ3 入力を完了した後、「OK」をクリックして該当利用者を登録します。

ステップ4 登録者一覧から、登録した利用者を確認します。



1.4.12.3 バッチ登録

ステップ1 「インポート」をクリックして、「インポート」画面を開きます。



ステップ2 「テンプレート・ダウンロード」のリンクをクリックして、
テンプレートをダウンロードします。

ステップ3 テンプレートに必要な事項を記入します。

	A	B	C	D	E	F	G	H
	Name of the person (Required, length [1-64]) 人員姓名 (必須, 長さ【1-64】)	Person No. (Required, only, length [1-20]) 人員番号 (必須, 唯一, 長さ【1-20】)	Name of picture (File name, extension) (Only support image to be uploaded in .jpg, .png and .bmp format, and the image size is not less than 320 * 320 px with the maximum of 10MB) 照片名称 (文件名, 后缀名) (仅支持照片上传, .jpg、.png、.bmp格式, 照片尺寸不小于320*320px, 照片最大为10MB)	Wechat Login password (Length [6-20]) 微信端登录密码 (长度【6-20】)	Gender (Male/Female/Null) 性別 (Male/Female/空)	Affiliated organization (Required, organization already exists in the platform) 所属组织 (必須, 平台内已存在组织)	Email box (The length is limited to [4-64]) 电子邮箱 (长度限制为【4-64】)	Phone number (The length is limited to [4-11]) 手机号码 (长度限制为【4-11】)
1								
2	AAA	1001	AAA.jpg			FaceSecTest10X		
3	BBB	1002	BBB.jpg			技術1部		
4	CCC	1003	CCC.jpg			技術1部		
5	DDD	1004	DDD.jpg			営業1部		
6	EEE	1005	EEE.jpg			営業1部		
7								
8								
9								
10								
11								
12								
13								
14								
15								

- ◇ 赤い色の項目は必須項目です。
- ◇ 登録者番号は一旦登録されたら修正できません。
- ◇ 登録写真欄に該当登録者の写真ファイル名を記入します。組織は、実際に存在する組織名を記入します。上部組織、下部組織も指定可能です。

ステップ4 登録者写真をフォルダに用意し、ZIP ファイルに圧縮します。

AAA.jpg	2019/11/25 18:18
BBB.jpg	2019/10/15 16:12
CCC.jpg	2020/4/24 15:08
DDD.jpg	2020/6/28 11:59
EEE.jpeg	2019/10/22 17:04

ステップ5 テンプレートファイルと写真の ZIP ファイルを追加して、「次のステップ」をクリックして、データをアップロードします。



CLOUD MANAGEMENT PLATFORM

組織名: GK_Demo_02 | 日本語 | ユーザー名: gk_demo02

ダッシュボード > 登録管理 > 登録管理 > インポート

データインポート データレビュー 完成

メッセージ:

ステップ1: データインポート用のExcelテンプレートをダウンロード; テンプレート・ダウンロード

ステップ2: テンプレート通りにインポートデータを記入します (赤色は必須項目、写真の形式はPNG/JPG/BMP、写真のサイズ320 x 320ピクセル);

ステップ3: インポートしたファイルの合計サイズは2GBを超えることはできません。写真が5,000枚以上の場合は、ZIPファイルを使用してインポートすることを推奨します。

*登録情報

Excelファイル

ル 追加 importPersons_20...

登録写真

ZIPファイル 追加 avatars_20210607...

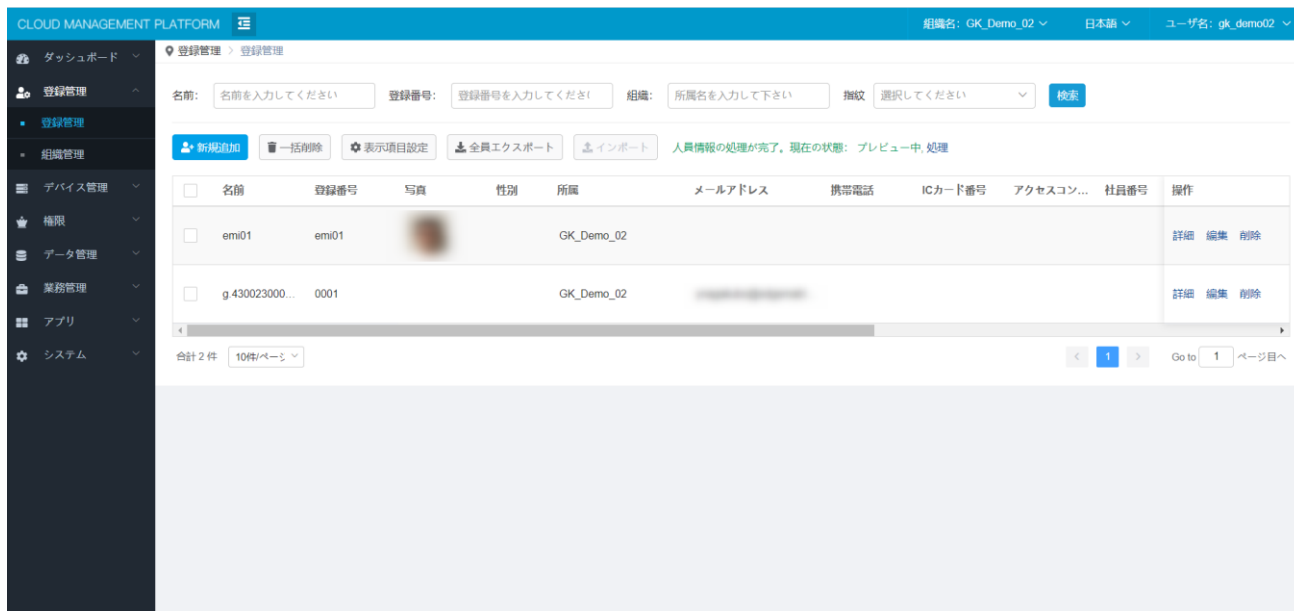
フォルダ 追加

次のステップ

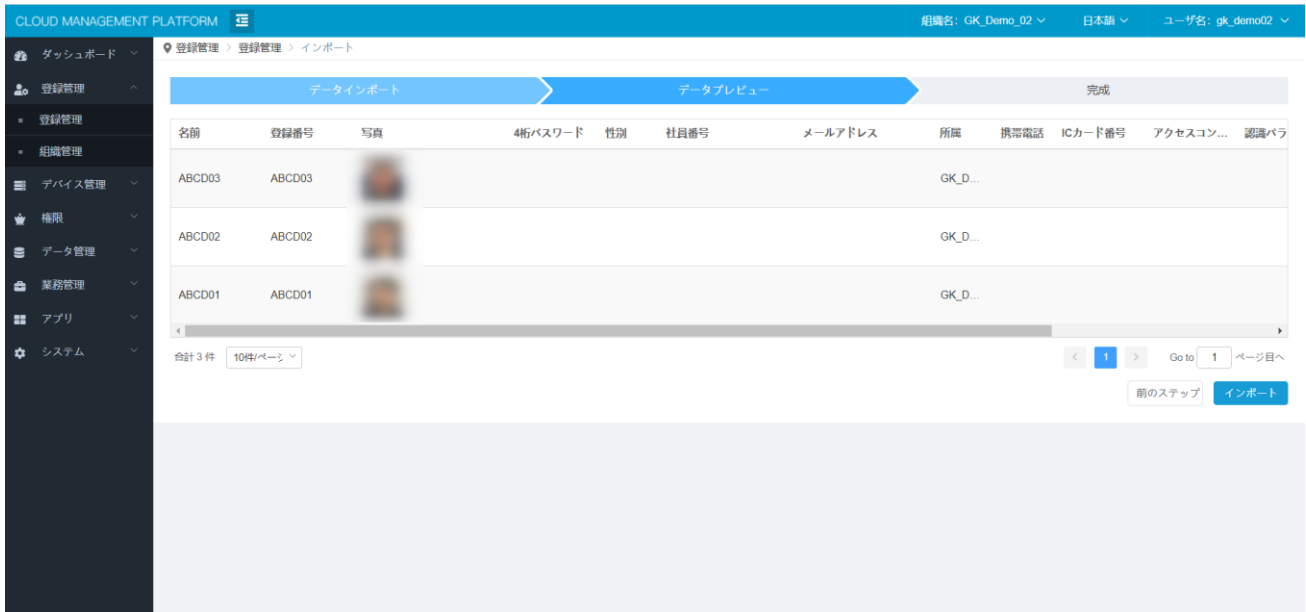
ステップ6 データの整合性と写真の品質を解析します。「OK」ボタンをクリックすると解析結果が表示されます。



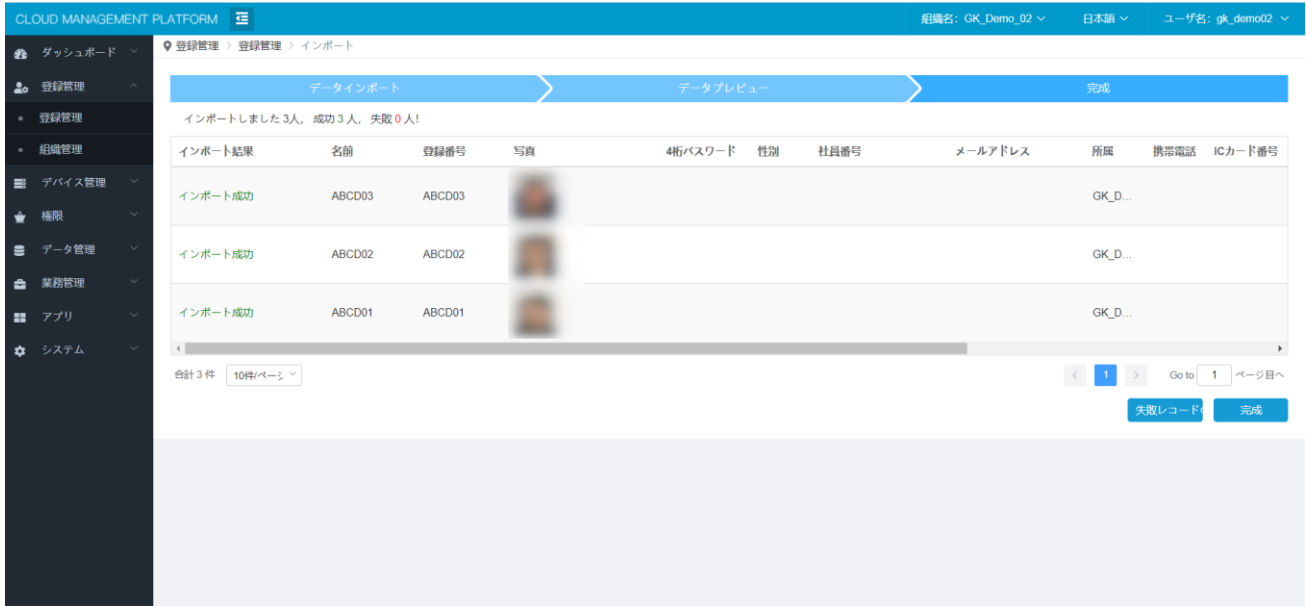
ステップ7 データ解析が正常な場合、「OK」をクリックして、「処理」をクリックします。
問題があった場合、データを修正して再アップロードします。



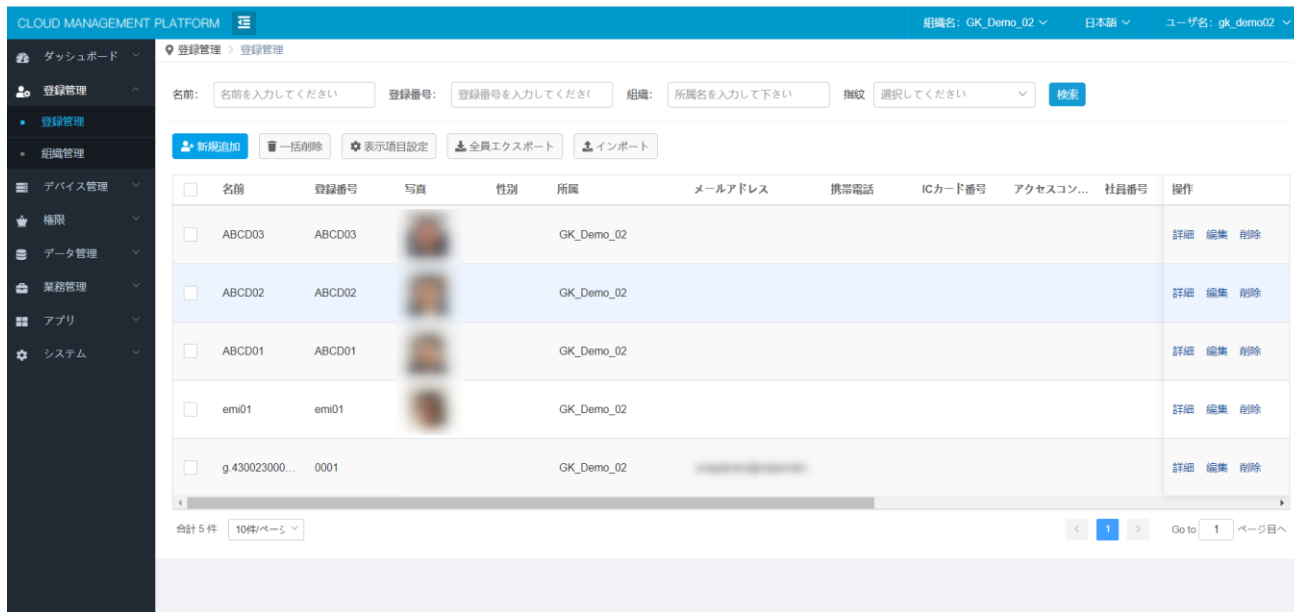
ステップ8 インポート前の最終確認です。
問題がない場合、「インポート」をクリックしてインポートを実行します。



- ステップ9 インポート結果の照合画面です。
 インポートに失敗があった場合に確認ができます。
 最後に「完成」ボタンを押すとインポート作業が完了して、一覧画面に戻ります。



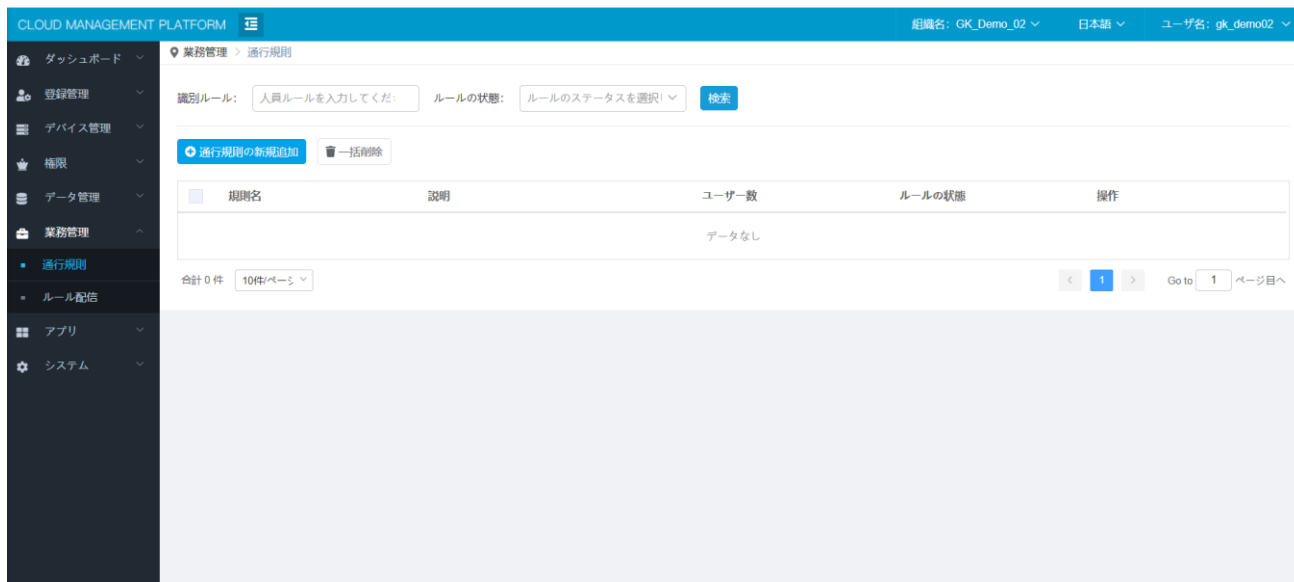
- ステップ10 インポート結果を確認します。



1.4.13 通行規則の作成と適用

1.4.13.1 通行規則の作成

アクセス手順：左側メニュー → 業務管理 → 通行規則



ステップ1 「通行規則の新規追加」をクリックして、「通行規則の新規追加」画面を開きます。

×

通行規則の新規追加

* 規則名

説明

* 通行方式 顔 ①

* 時間規則 + 時間規則

名称	日付	曜日	時間	通行可否	操作
データなし					

* 適用単位

入力項目の説明

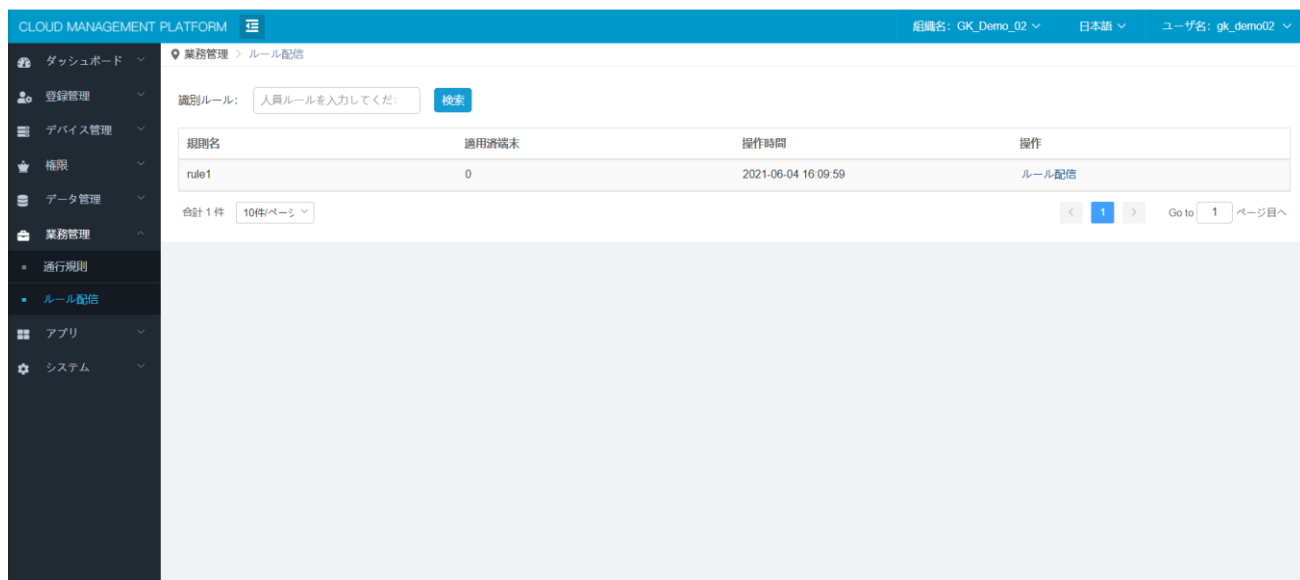
NO.	項目	説明
1	規則名	必須
2	説明	オプション
3	通行方式	必須 認証方式を設定します。 複数の認証方式を同時に設定できます。
4	時間規則	必須 時間帯の通行可/通行不可を設定します。
5	適用単位	必須 利用者を登録します。 利用者単位と組織単位の2種類の設定方法があります。

ステップ2 規則を入力して、「OK」をクリックし規則を作成します。



1.4.13.2 通行規則の適用

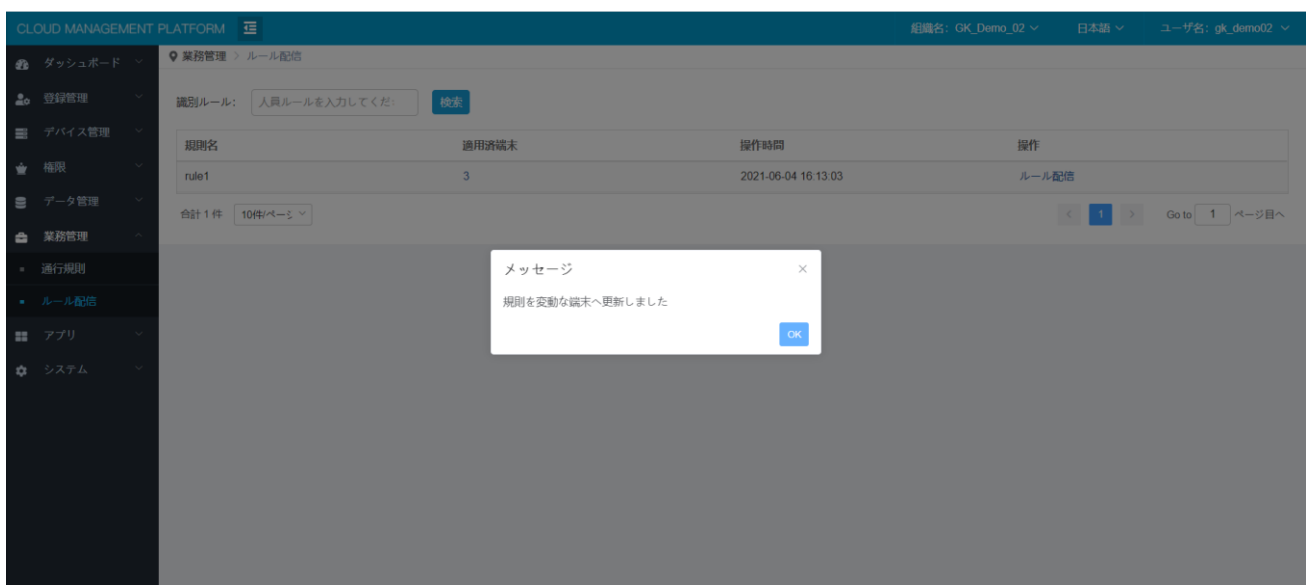
アクセス手順: 左側メニュー → 業務管理 → ルール配信



ステップ1 「ルール配信」をクリックして、「ルール配信」画面を開きます。



ステップ2 適用するデバイスを選択し、「OK」をクリックして通行規則をデバイスに適用させます。



CLOUD MANAGEMENT PLATFORM 組織名: GK_Demo_02 | 日本語 | ユーザー名: gk_demo02

業務管理 > ルール配信

識別ルール:

規則名	適用済端末	操作時間	操作
rule1	3	2021-06-04 16:13:03	ルール配信

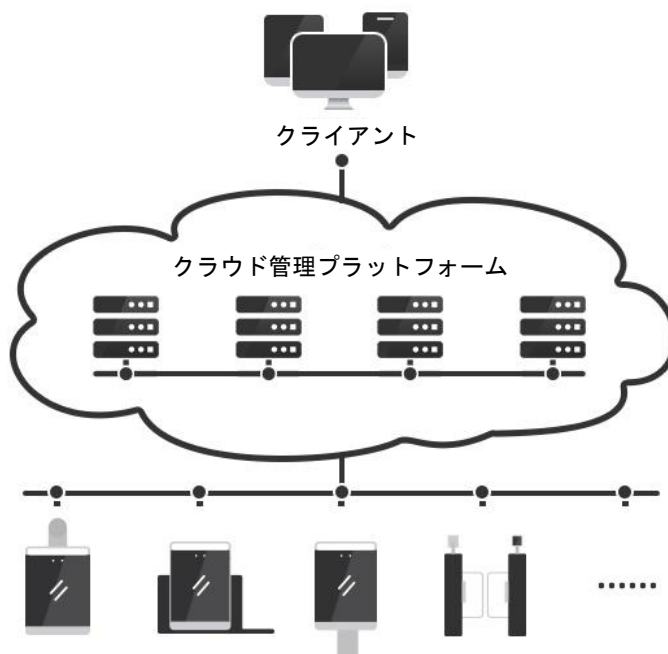
合計 1 件 < 1 > Go to 1 ページ目へ

2 デバイス

2.1 システム概要

2.1.1 システム構成

デバイスはクラウド管理プラットフォームと併用する必要があります。クラウドサービスモデルのネットワーク・トポロジーは下図のとおりです。



2.1.2 一般的な使用の流れ

ネットワークを経由し、デバイスをクラウドプラットフォームに接続します。

認証の流れ：

A-1：デバイスがクラウド管理プラットフォームから登録者および対応する認証ルールをダウンロードします。

A-2：デバイスのカメラが登録者のスナップ写真を収集してデバイスの登録者ライブラリと比較し、アクセス権限を判断します。

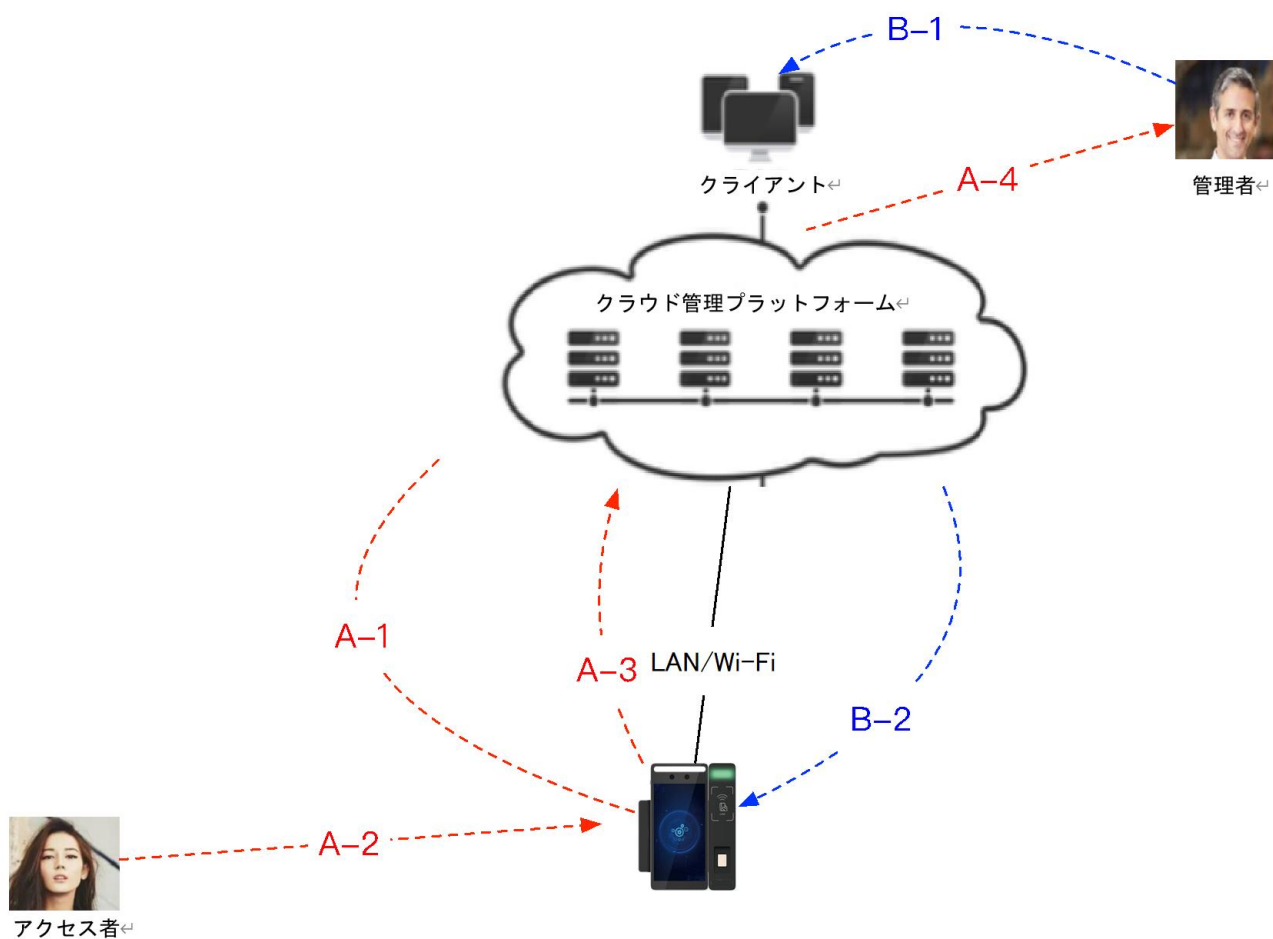
A-3：デバイスにより認証結果がクラウド管理プラットフォームにアップロードされ、保存・分析されます。

A-4：クラウド管理プラットフォームは、異常情報やイベントを管理者に通知します。

管理の流れ：

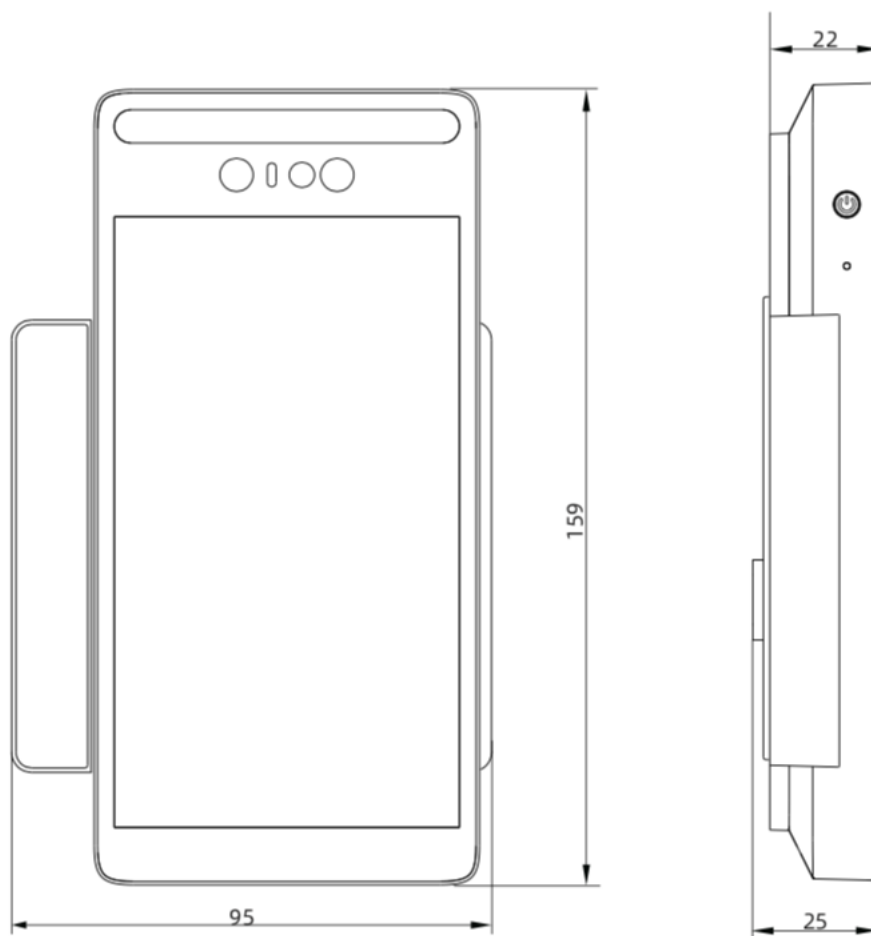
B-1：管理者はWeb ブラウザで登録者の管理、デバイスの管理、権限の管理などを設定します。

B-2：クラウド管理プラットフォームは、設定した情報を指定のデバイスに配信します。

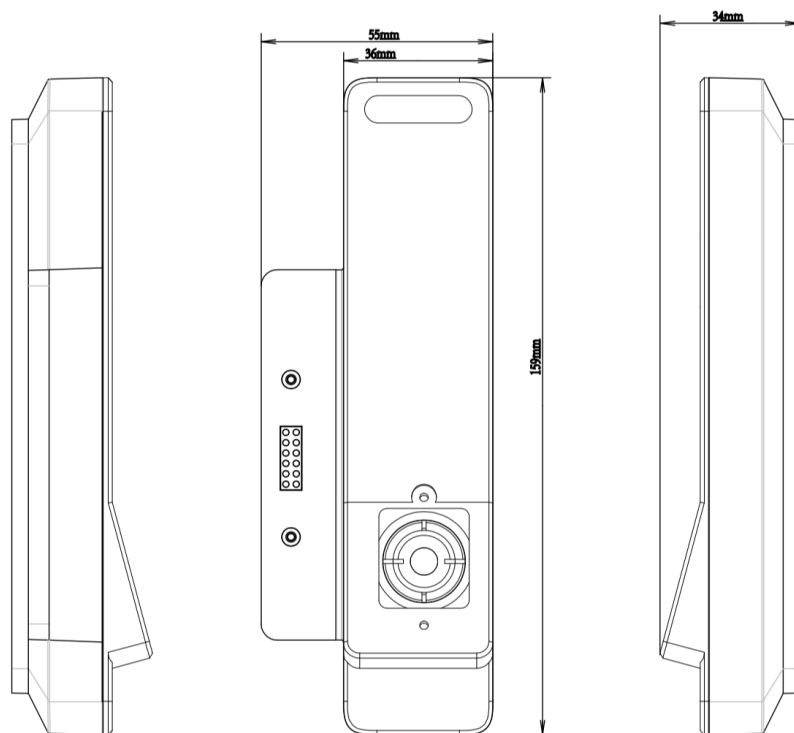


2.2 ハードウェア

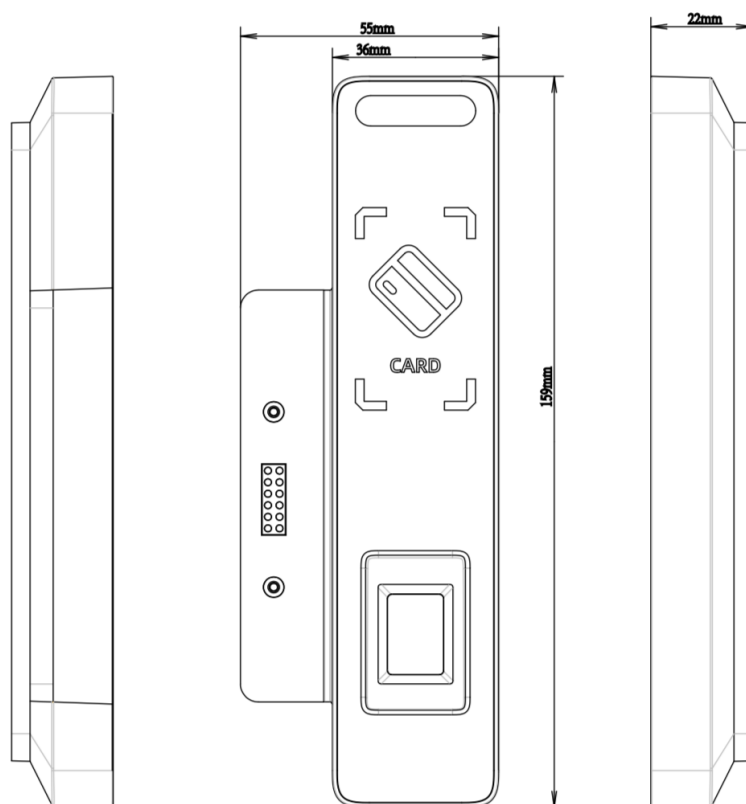
2.2.1 本体のサイズ(単位:mm)



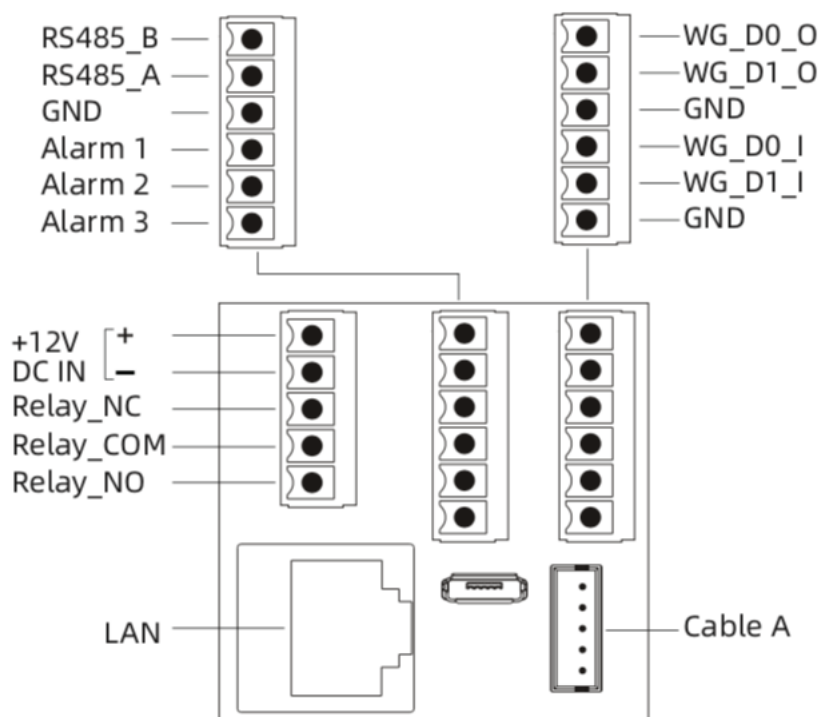
2.2.2 温度測定モジュールのサイズ(単位:mm)



2.2.3 指紋モジュールのサイズ(単位:mm)



2.2.4 ポート説明



2.2.5 仕様

生体認証偽造防止	サポート	
認証距離	50~130cm	
ワークモード	温度測定モード、顔認証モード、温度測定+顔認証モード	
検証方法	1:1、1:N、1:1/1:N(Mixモード)	
顔識別速度	識別時間(1:Nの場合) ≤ 0.3秒	
登録者容量	最大 100,000人 ※初期顔認証の登録人数は5万人(別料金で10万人まで拡張可能)	
オペレーティングシステム	Android 8.1	
カメラ	デュアル広角カメラ (RGB+NIR)	
ディスプレイ	5.5インチ LCD タッチスクリーン	
マルチタッチ	サポート	
取り外しアラーム	サポート	
動作温度	-10° C~55° C	
相対湿度	5%~95%(結露しない環境下)	
サイズ	95*159*25mm	
電源	DC 12V 3A	
通信方法	Wi-Fi	2.4GHz/5GHz、IEEE 802.11a/g/b/n; IEEE 802.11ac をサポート
	Ethernet	サポート
物理インターフェース	RS485*1、ウィーグランド出力*1、ウィーグランド入力*1、ドライ接点*1、RJ45*1、アラーム I/F*3	

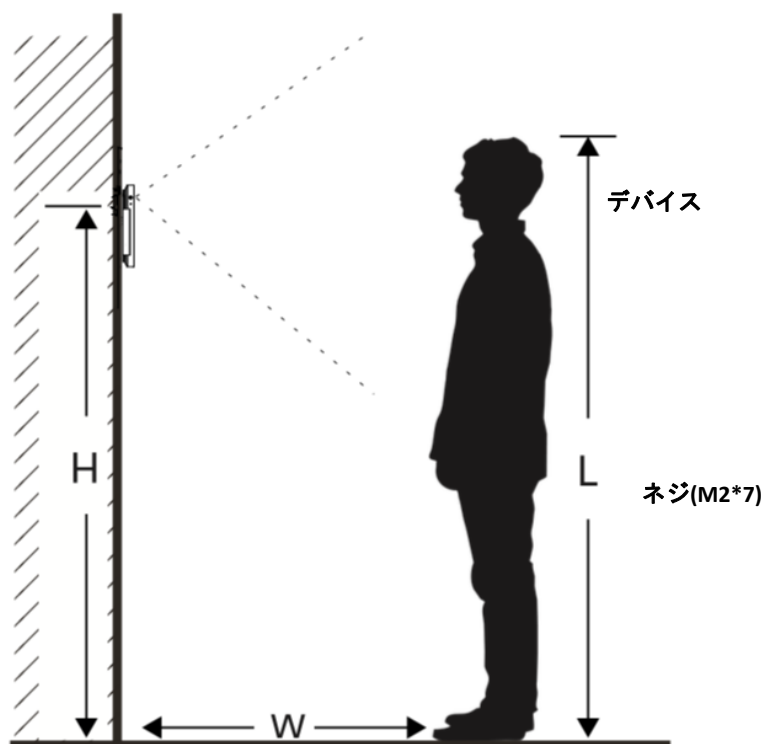
電源ボタン	サポート
-------	------

サーマルカメラ 仕様	解像度	160 x 120 pix
	計測範囲	30~42°C
	計測精度	±0.3°C

2.2.6 設置について

壁への取り付け、セキュリティゲート、フラッパーゲートやスタンドへの設置工事につきましては EDGEMATRIX 株式会社にお問い合わせください。

2.2.7 設置高さについて



人物とカメラの距離 W (cm)	カメラと地面の距離 H (cm)	認証可能な身長 L (cm)
60	130	80~200
	140	90~210
	150	100~220

注：温度測定の場合、認証距離 50~130cm、身長 120~190cm

2.3 デバイス操作ガイド

2.3.1 前提条件

デバイスのアクティベーションが完了し、電源が入っていること。

2.3.2 操作概要

デバイスの基本的な操作方法は、図 1 のとおりです。

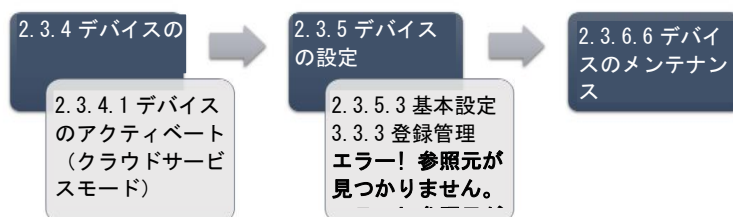


図 1 デバイス操作の流れ

ステップ	サブステップ	説明
デバイスの初期化	デバイスが初期化されていない場合、電源をオンにして初期化した後で、機能の設定を行い、使用します。 <ul style="list-style-type: none"> ◇ 一度初期化すれば、電源をオンにするたびに初期化する必要はありません。 ◇ 新しい機器を初めてオンにする時、工場出荷状態に戻した場合は、デバイスを初期化します。 	
	デバイスのアクティベート	初めてデバイスの電源をオンにする場合、システムの基本情報を設定してください。
	デバイス管理者の追加	デバイス管理者は、デバイスの設定や管理について最高の権限を持ちます。工場出荷時、デフォルトの管理者は設定されていません。デバイスのアクティベーション後に設定してください。
デバイスの設定	実際のデバイスの使用状況に応じて、機能の設定と登録管理を行います。認証後に問題がなければ、日常的に使用できます。	
	機能の設定	実際のデバイスの使用状況に応じて、デバイスの機能を設定します。
	登録者の管理	実際のデバイスの使用状況に応じて、登録者情報とデータを管理します。
	機能の検証	機能の設定と登録者の管理が完了したら、デバイスの機能を検証し、画面に表示される情報とロジックが正しいか確認します。
日常メンテナンス	日常的なデバイスの使用において異常が発生した場合は、日常メンテナンスを実施してください。	
システムの更新	デバイスのフォームウェアをアップグレードします。	

2.3.3 デバイスの電源オン/オフ

2.3.3.1 電源をオンにする

デバイスがシャットダウンしている状態で電源オンボタンを長押しし、デバイスの電源をオンにします。デバイスを初めてオンにすると、アクティベーションページに進みます。

2.3.3.2 シャットダウン/再起動

ステップ1 デバイスの電源がオンの状態で電源オンボタンを長押しすると、ダイアログが開きます。

ステップ2 ダイアログで、「Power off」をクリックすると、「Enter Password」ダイアログが開きます。

ステップ3 「Enter Password」ダイアログに管理者パスワードを入力し、「確認」をクリックします。

2.3.3.3 デバイスログの保存

ステップ1 デバイスの電源がオンの状態で電源オンボタンを長押しすると、ダイアログが開きます。

ステップ2 ダイアログで、「Save logs」をクリックすると、「ログの保存」ダイアログが開きます。デバイスは「USB メモリに保存」と「ローカルに保存」の 2 種類をサポートしています。

◇ USB メモリは FAT32 のファイルシステムにフォーマットされている必要があります。

ステップ3 「ログのエクスポート」ダイアログで、エクスポート方法を選択し、「エクスポート」をクリックします。

2.3.4 デバイスのアクティベート

デバイスがアクティベートされていない場合、電源をオンにしてアクティベートした後で、機能の設定や使用ができます。

◇ 一度アクティベートすれば、電源をオンにするたびにアクティベートする必要はありません。

◇ 新しい機器を初めてオンにする時や、工場出荷状態に戻した場合などには、アクティベートが必要となります。

2.3.4.1 デバイスのアクティベート（クラウドサービスモード）

2.3.4.1.1 前提条件

事前に申請したアカウントを用いてクラウド管理プラットフォームにログインし、アクティベーションQRコード、アクティベーション情報、デバイスのグループコードを取得します。

- ◇ クラウド管理プラットフォームのアカウントと初期パスワードは、クラウド管理プラットフォームのご購入時に発行されます。

2.3.4.1.2 デバイス基本情報の設定

ステップ1 「言語」画面で、デバイスのシステム言語を設定します。

- ◇ Edge AI Tablet は多言語をサポートしており、アクティベート時、または設定画面で選択できます。

「次へ」をクリックすると、「日付と時刻」画面が開きます。

ステップ2 「日付と時刻」画面で、デバイスのタイムゾーン、日付、時間を設定します。

- ◇ クラウドサービスモードの場合、「自動設定」をオンにし、クラウド管理プラットフォームを介して自動的に時間設定を同期させてください。

「次へ」をタップすると、「稼働モードの選択」画面が開きます。

ステップ3 「稼働モードの選択」画面で、「クラウドサービスモード」を選択します。

「次へ」をタップすると、「ネットワーク」画面が開きます。

2.3.4.1.3 ネットワーク接続の設定

ステップ1 「ネットワーク」画面で、デバイスのネットワーク接続を設定します。

デバイスは「WLAN」と「LAN」の2種類のネットワーク接続方式をサポートしています。

ステップ2 「WLAN」を選択すると、「WLAN」画面が開き、無線ネットワークを設定できます。

「LAN」を選択すると、「LAN」画面が開き、有線ネットワークを設定できます。

デバイスはIPアドレスの自動取得または手動取得の2種類の有線ネットワーク設定方法をサポートしています。

ステップ3 「スキップ」をタップするかネットワーク設定の完了後、「次へ」をタップすると、「デバイスのアクティベート」画面が開きます。



図 2 ネットワーク

2.3.4.1.4 アクティベーションコードの入力

ステップ1 デバイスの「デバイスのアクティベート」画面で、アクティベーション情報を入力します。

方法 1: 「スキャン」をタップし、デバイスでサーバーアドレス、アクティベーションコード、デバイスのグループ名などの情報が含まれる QR コードを読み取ると、情報が自動的に入力されます。

方法 2: 「サーバーアドレス」、「アクティベーションコード」、「デバイス名」、「デバイスのグループコード」を入力します。

オプション	説明
サーバーアドレス	クラウド管理プラットフォームのサーバーアドレスを設定できます。
アクティベーションコード	クラウド管理プラットフォームにログインし、アクティベーションコードを取得します。
デバイス名	オプション。 デバイス名を設定できます。最大 64 文字まで入力できます。
デバイスのグループコード	オプション。最大 20 文字まで入力できます。

オプション	説明
	デバイスのグループコードを設定できます。

「次へ」をタップすると、「ようこそ」の画面が開きます。

2.3.4.1.5 使用開始

ステップ1 ようこそ画面で、「使用開始」を選択することによりアクティベートが完了し、「認証画面」画面が開きます。

2.3.4.2 デバイスマネージャーの追加（クラウドサービスモード）

デバイスのアクティベーション後、クラウド管理プラットフォームからデフォルトの管理者を自動的に取得します。デフォルトの管理者が設定されていない場合、「管理者の設定」画面下に「管理者を関連付けてください」と表示されます。

クラウド管理プラットフォームにログインして管理者を追加する方法の詳細については、『3.3.4.3 管理者』をご参照ください。

各デバイスに最大 10 人のデバイスマネージャーを設定できます。

2.3.5 デバイスの設定

実際のデバイスの使用状況に応じて、機能の設定と登録者の管理を行います。設定した内容を動作確認した後、使用が始まります。

2.3.5.1 デバイスへのログインと管理

登録済みの管理者は「顔認証ログイン」と「パスワード認証ログイン」の 2 種類の方法でデバイスの設定画面にログインできます。

ステップ1 認証画面で、下の上矢印をタップするかスライドすると、操作アイコンが表示されます。



図 3 操作アイコン

- ◇ 操作アイコンをカスタマイズできます。操作方法については、『2.3.5.2 ホームボタンの設定』をご参照ください。

左から右の操作アイコンは以下のとおりです。

操作アイコン	説明
	コントロールするドアを開きます。
	「設定」画面を開きます。
	「登録者管理」画面を開きます。
	デバイス「運行情報」画面を開きます。

ステップ2 操作アイコンをタップすると、「管理者ログイン」画面が開きます。

デバイスは「顔認証ログイン」と「パスワード認証ログイン」の2種類の認証方法に対応しています。デフォルトは「顔認証」です。

ステップ3 「管理者ログイン」画面で、右上の「パスワード認証」をタップすると、認証方法が切り替わります。

- ◇ デバイスは選択されている認証方法をデフォルトの認証方法として記憶します。

ステップ4 認証が成功したら、指定の操作を実行します。

2.3.5.2 ホームボタンの設定

ステップ1 認証画面で、画面右の拡張ボタンをタップするか左にスライドすると、右欄のボタン領域の操作アイコンとホームボタンの設定アイコンが表示されます。

ステップ2 ホームボタンの設定アイコンをタップすると、「ホームボタンの設定」画面が開きます。

ステップ3 「ホームボタンの設定」画面で、認証画面の下部領域のボタンとサイドバーのボタン領域を含む操作アイコンの表示位置を調整します。

- 1) 「未選択のボタン」領域でアイコンを選択し、「下部領域に追加」または「サイドバー領域に追加」をタップすると、指定したアイコンが指定した領域に追加されます。
- 2) 「下部領域に追加」または「サイドバー領域に追加」で、アイコン上部の「×」記

号をタップすると、指定したアイコンを領域から移動させることができます。

2.3.5.3 基本設定

デバイスの設定画面は以下の図面の通りになります。



2.3.5.3.1 情報

「情報」では、デバイスの基本情報を照合できます。

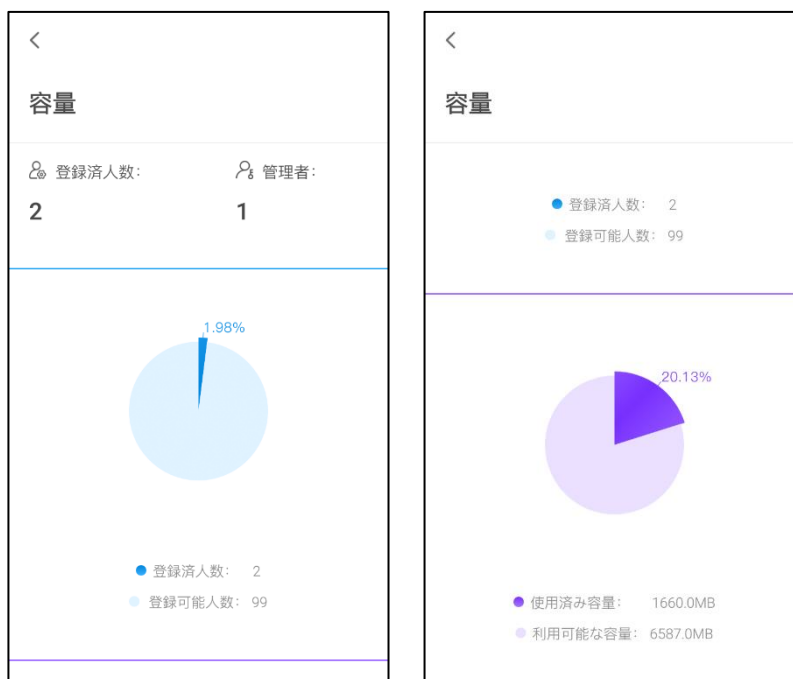
アクセス手順：認証画面から「設定」→「情報」



2.3.5.3.2 容量

「容量」では、デバイスの「登録者数」、「管理者数」、「ストレージ容量」を確認できます。

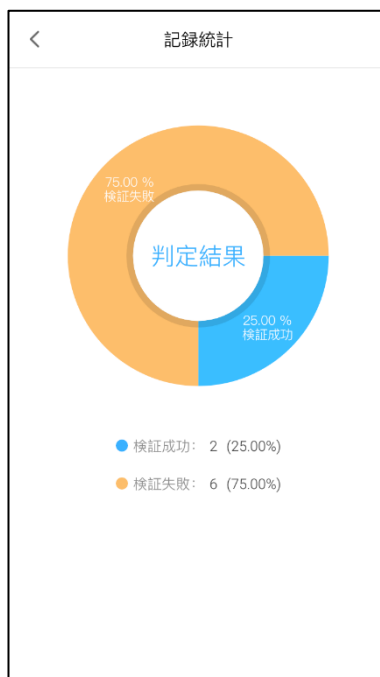
アクセス手順：認証画面から「設定」→「容量」



2.3.5.3.3 記録統計

「記録統計」では、デバイスの識別記録の判定結果の統計を確認できます。

アクセス手順：認証画面から「設定」→「記録統計」



2.3.5.3.4 一般設定

一般設定では、「システム言語」、「音量」、「画面の明るさ」を設定できます。

アクセス手順：認証画面から「設定」→「一般」

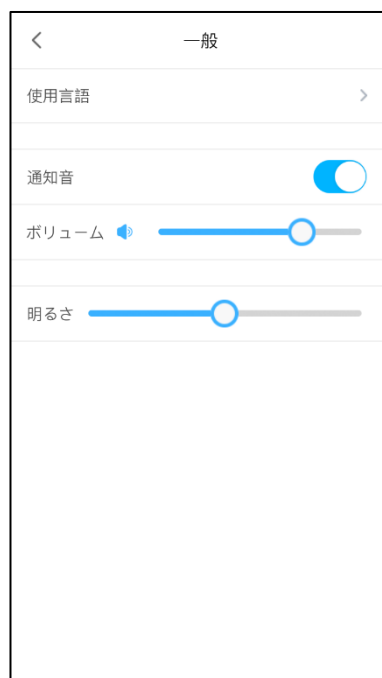


図 4 「一般設定」画面

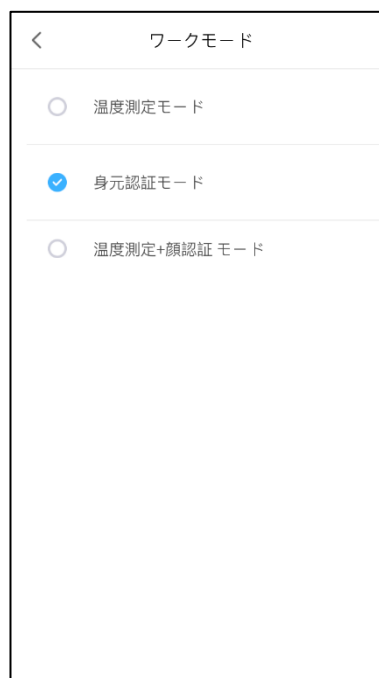
オプション	説明
使用言語	デバイスのシステム言語を設定できます。
通知音	デバイスのサウンドをオン/オフにできます。既定値：オン
ボリューム	「通知音」がオンの場合、音量を設定できます。
明るさ	デバイスの画面の明るさを設定できます。

2.3.5.3.5 ワークモード

ワークモードの設定では、デバイスのワークモードを設定できます。

「温度測定モード」、「身元認証モード」、「温度測定+顔認証モード」の3種類を選択できます。

アクセス手順：認証画面から「設定」 → 「ワークモード」 → 「ワークモード」画面



オプション	説明
温度測定モード	温度測定のシーンのみで使用します。このシーンでは、検温者の認証を行いません。
身元認証モード	顔認証のみのシーンで使用します。既定値
温度測定+顔認証モード	顔認証と同時に温度測定するシーンで使用します。

2.3.5.3.6 検証順

「検証順」では、デバイスの認証開始トリガーのモードを設定します。

アクセス手順：認証画面から「設定」 → 「検証順」 → 「検証順」画面



図 5 「検証順」画面

オプション	説明
サードパーティトリガー	認証開始のトリガーがスクリーンタッチに設定されます。待機画面の「ようこそ」をタッチすることになり認証が開始されます。
自動トリガー	既定値。認証対象を検知すると認証が自動的に開始されます。

2.3.5.3.7 顔識別設定

「顔識別設定」では、採集精度、マスク検知、使用シーン、繰り返し識別間隔などの設定ができます。

アクセス手順：認証画面から「設定」 → 「顔識別設定」 → 「顔識別設定」画面



図 6 「顔識別設定」画面

オプション	説明
採取精度	認証時のスナップショットに、撮影角度、あいまいさ(ぼやけ)、オクルージョン(かぶり)の3項目の品質判定設定できます。より厳密な認証が求められる場合に使用します。既定値：オフ
マスク検知	マスク着用を検知します。マスクを着用していない場合は注意喚起メッセージを画面表示し、検温または認証を行いません。既定値：オフ
識別モード	1:N、1:1、1:N/1:1 同時使用モードを設定します。既定値：1:N/1:1 同時使用モード
使用シーン	快速シーン(生体検出オフ)、安全シーン(生体検出オン)、カスタムシート(各閾値をカスタマイズ)を設定します。
識別対象	顔、顔+QRコード、QRコードを設定できます。既定値：顔 ※EDGEMATRIX Gatekeeper サービスではQRコード認証機能を提供しておりません。顔認証のみご利用いただけます。
繰り返し識別間隔	同一利用者の次の認証を行うまでの動作間隔を設定します。既定値：0秒
背景画像の特定	認証画面で、背景エリア(顔認証の枠以外)を異なる色の表示を設定します。既定値：オン
検証成功表示時間	検証成功のメッセージを表示する時間を設定します。既定値：1秒
検証失敗表示時間	検証失敗のメッセージを表示する時間を設定します。既定値：1秒

オプション	説明
顔検出フレーム	認証画面で、顔の周りに検出フレームの表示を設定します。既定値：オフ
顔追跡	認証が成功した場合、登録写真を表示します。該当機能を利用するには、コンテンツ再生をサインージモードに設定する必要があります。既定値：オフ

2.3.5.3.7.1 採集精度

アクセス手順：認証画面から「設定」→「顔識別設定」→「採集精度」

ステップ1 「高精度」をオンにすると、角度、ぼやけ、の3方面からスナップ写真の品質判定を設定します。



図7 「採集精度」画面

オプション	説明
高精度オン/オフ	「高精度」をオン/オフにします。既定値：オフ
撮影角度制限	キャプチャした顔の角度を制限できます。既定値：オン
あいまいさの識別の閾値	キャプチャした顔のぼやけを制限できます。既定値：100% 数字を低くすればするほど、鮮明な画像が要求されます。高くするとぼやけの許容値が大きくなります。

オプション	説明
オクルージョン識別の 閾値	<p>キャプチャした顔のオクルージョン(かぶり)を制限できます。既定値：100%</p> <p>数字を低くすればするほど、かぶりの面積が小さな画像が要求されます。高くするとかぶりの許容値が大きくなります。</p> <p>◇ かぶりとは人物が帽子をかぶっていたり、マスクをつけたりして顔を遮蔽している状態のことです。</p>

- ◇ この機能はより厳密な認証が求められる場合にのみ設定する機能となります。設定をオンにした場合、識別速度とユーザー体験に影響を与える可能性があるため、実際のシナリオに合わせて最適値を調整いただく必要があります。

2.3.5.3.7.2 マスク検知

マスク検知の設定では、規格の判断、使用シーン、検証方法、認証の繰り返し間隔の設定ができます。

アクセス手順：認証画面から「設定」 → 「顔識別設定」 → 「マスク検知」



オプション	説明
マスク検知	マスク検知機能をオン/オフを設定します。既定値：オフ
マスク検知閾値	<p>マスク検知閾値を設定します。既定値：50</p> <p>※マスクは単色かつ薄色のものが推奨されます。濃い色や模様、柄等がついたマスクは検知されにくい可能性があります。</p>

- ◇ マスク検知をオンにした場合、マスクを着用していない人に対して検温または認証を行いません。実際のシナリオに合わせて最適な設定を行ってください。

マスク検知を有効にしたうえで顔認証と生体認証を同時に有効にする場合、認識精度と速度の兼ね合いを考慮し、以下のパラメータ設定を推奨します。

アクセス手順：認証画面から「設定」 → 「顔識別設定」
→ 「使用シーン」 → カスタマイズ → 拡張設定

設定グループ	パラメータ	説明
生体認証偽装防止パラメータ	生体検出の可視光閾値	推奨値：1% 既定値：50% ※1%で生体検出が有効になり、最低限の写真等を使った認証突破を防止可能です。
	生体検出の近赤外線閾値	推奨値：1% 既定値：50% ※1%で生体検出が有効になり、最低限の写真等を使った認証突破を防止可能です。
1:N モードパラメータ	可視光閾値	推奨値：70% 既定値：80% ※マスクの装着部分を調整して顔の露出部分を多くするほど顔認証のスコアが高くなります。

2.3.5.3.7.3 識別モード

アクセス手順：認証画面から「設定」 → 「顔識別設定」 → 「識別モード」

デバイスは、「1:1 モード」、「1:N モード」、「混合モード」の3種類の識別モードをサポートしています。デフォルトは「混合モード」です。



図 8 「識別モード」画面

オプション	説明
1:Nモード	実際に撮影した顔をデバイスに登録済みのすべての人物と比較します。
1:1モード	実際に撮影した顔を対応する証明書の写真と比較します。
Mixモード	「1:1モード」と「1:Nモード」を同時に使用できます。既定値

2.3.5.3.7.4使用シーン

アクセス手順：認証画面から「設定」→「顔識別設定」→「使用シーン」



図9 「使用シーン」画面

オプション	説明
快速シーン	生体検出はオフで、認証速度が要求されるシーンに適しています。通行速度を効果的に向上することができます。既定値
安全シーン	生体認証はオンで、比較的厳しい通行審査のシーンに適しています。安全性を効果的に向上できます。
カスタムシーン	「生体認証偽造防止パラメータ」、「1:N 認証パラメータ」、「1:1 認証パラメータ」を手動で設定します。 ☆ この機能は識別速度とユーザー体験に影響を与える可能性があるため、実際のシナリオに合わせて最適値を調整いただく必要があります。

カスタムシーンを利用する場合

アクセス手順：「使用シーン」→「カスタマイズ」→「拡張設定」



図 10 「カスタムシーン」画面

設定グループ	パラメータ	説明
生体認証偽造防止パラメータ	生体検出の可視光閾値	可視光の条件下で生体認証を行います。識別点数が指定した閾値を超えると、認証成功です。値が大きいほど、認証が厳しくなります。 既定値：50%
	生体検出の近赤外線閾値	赤外線の条件下で生体認証を行います。識別点数が指定した閾値を超えると、認証成功です。値が大きいほど、認証が厳しくなります。 既定値：50%
1:N モードパラメータ	認証閾値ライブラリ設定	顔認証に使用する閾値ライブラリを設定できます。 ◇ 認証閾値ライブラリはクラウド管理プラットフォームで設定され、デバイスに配信されます。 ◇ 登録者毎に、個別な設定が可能です。
	可視光閾値	可視光の条件下で顔認証を行います。識別点数が指定した閾値を超えると、認証成功です。 既定値：80%
	近赤外線閾値	近赤外線の条件下で顔認証を行います。識別点数が指定した閾値を超えると、認証成功です。 既定値：0%

設定グループ	パラメータ	説明
1:1 モードパラメータ	可視光閾値	可視光の条件下で顔認証を行います。識別点数が指定した閾値を超えると、認証成功です。 既定値：70%

2.3.5.3.7.5 認証対象

デバイスの作動モードは、クラウドサービスモードを設定した場合の機能です。

デバイスは顔または QR コードで認証できます。

※EDGEMATRIX Gatekeeper サービスでは QR コード認証機能を提供していません。

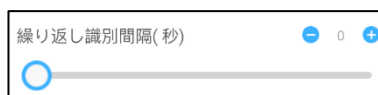
デバイス側の設定手順

アクセス手順：認証画面から「設定」→「顔識別設定」→「識別対象」

以下の項目を設定します。

オプション	説明
顔	設定するとデバイスは顔のみを認証します。既定値
顔と QR コード	設定するとデバイスは顔と QR コードを同時に認証します。
QR コード	デバイスは QR コードのみを認証します。

2.3.5.3.7.6 繰り返し識別間隔



同一利用者の前の識別と次の識別の動作間隔を設定します。設定した動作間隔の間に、同一利用者の認証が成功した場合、二度認証を行わない機能です。値の設定範囲は 0～300 秒です。既定値：0 秒。

- ◇ ユーザー体験を向上させるため、実際のシナリオに合わせて最適値を調整いただく必要があります。

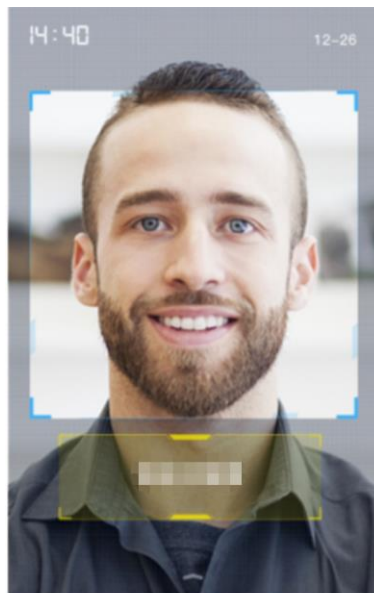
設定例：

「認証の繰り返し間隔」を 3 秒に設定すると、A 者の顔認証が成功した後、以下の判断が行われます。

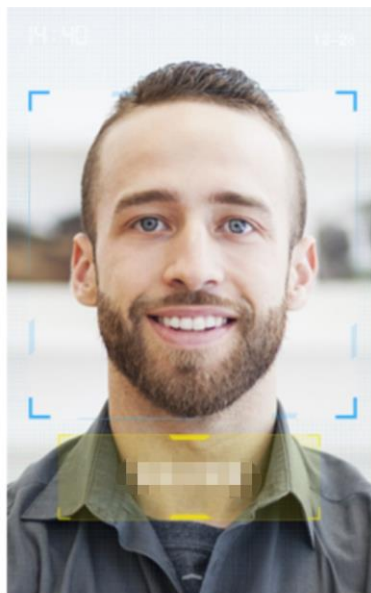
- 1) 過去3秒以内にA者の顔認証の成功記録がない場合、「A,こんにちは」(認証成功)と表示されます。
- 2) 過去3秒以内にAの顔認証の成功記録がある場合、「認証を繰り返さないでください」と表示されます。

2.3.5.3.7.7背景画像の特定

認証画面で、背景エリア(顔認証の枠以外)を異なる色での表示を設定します。既定値：オン



設定：オン



設定：オフ

2.3.5.3.7.8検証結果の表示時間

検証成功のメッセージを表示する時間を設定します。

値の設定範囲は1~10秒です。既定値：1秒



検証失敗のメッセージを表示する時間を設定します。既定値：1秒

値の設定範囲は1~10秒です。既定値：1秒



2.3.5.3.7.9 顔検出フレーム

認証画面で、顔の周りに検出フレームの表示を設定します。既定値：オフ

2.3.5.3.7.10 顔追跡

認証が成功した場合、登録写真を表示します。既定値：オフ

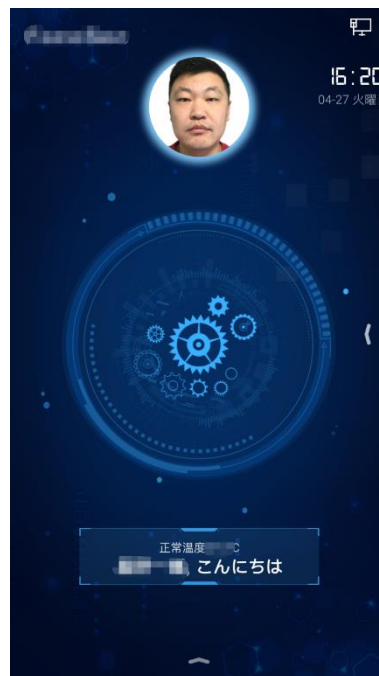
該当機能を利用するには、コンテンツ再生をサインージモードに設定する必要があります。

サインージモードの設定手順

アクセス手順：認証画面から「設定」→「拡張設定」→「コンテンツ再生」→「表示モード」



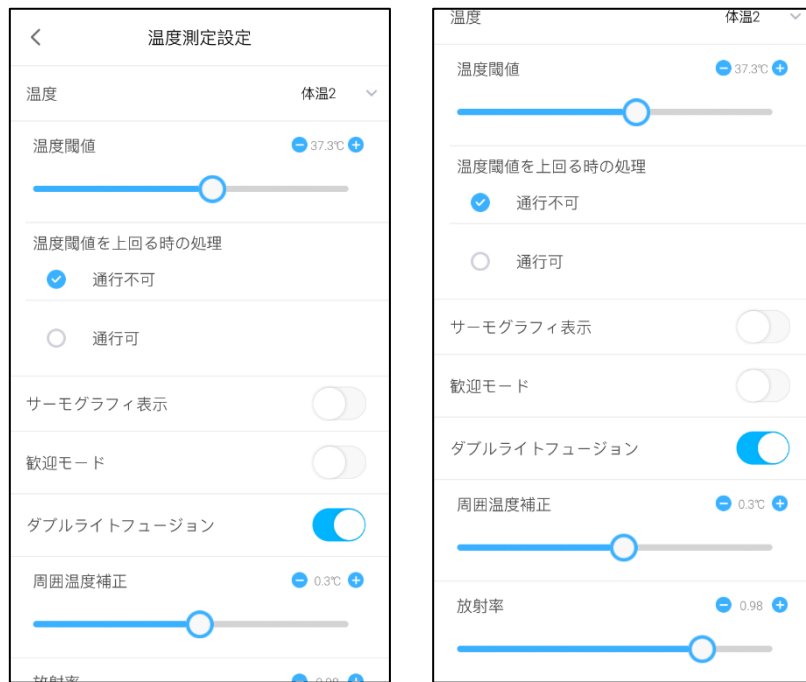
識別中



認証成功

2.3.5.3.8 温度測定設定

温度測定のシーンで使用する場合、「温度測定の閾値」と「温度超過閾値の処理」を設定できます。



グループ化	パラメータ	説明
検温	温度	体温、体温2、皮膚温度の三つのモードを設定できます。 ・体温モードは、従来の皮膚温度からコア温度を換算するアルゴリズムです。(デフォルト) ・体温2モードは、新しくリリースされた皮膚温度からコア温度の換算アルゴリズムで、従来のアルゴリズムより体温が高めに評価されます。 ・皮膚温度は、サーマルカメラが測定したオリジナルの皮膚温度であり、検温システムを校正するための機能です。一般シーンで検温として利用するモードではありません。
	温度閾値	検温結果が温度閾値を超えると、温度閾値を上回る時の処理で設定された処理が行われます。
温度閾値を上回る時の処理	通行不可	温度が閾値を超えると、高体温と表示され、電気錠、ゲートと連動する場合は通行できません。既定値
	通行可	温度が閾値を超えると、高体温と表示され、電気錠、ゲートと連動する場合でも通行することができます。

グループ化	パラメータ	説明
拡張設定	サーモグラフィ表示	検温システムを設置する際、サーモカメラの視界内に他の熱源があるかどうか確認出来ます。既定値：オフ
	ウェルカムモード	ワークモードが温度測定+顔認証に設定されている場合、同一デバイスでゲストと登録者の同時利用を可能にする機能です。登録者の場合は、検温結果と認証結果を表示し、ゲスト(未登録者)は検温結果のみを表示します。既定値：オフ
	ダブルライトフュージョン	可視光カメラとサーモカメラをマッピングし、顔の輪郭内のみを検温し、他の熱源との誤検温を防ぐためのスマート機能です。但し、実環境の複雑な要因により、ほかの熱源の誤検温を完全には防止できないため、設置要件に従って視界内から熱源を外すよう運用してください。 一時的にオフにすることにより、黒体を用いた検温システム校正にも適用いただけます。 既定値：オン
	周囲環境補正	周囲環境温の変化より、サーモカメラを正常に動作するための補正值です。
	放射率	検温システムを校正するための機能です。一般のユーザー向けの機能ではありません。既定値のままご利用してください。既定値：0.98

- ◇ クラウドプラットフォームでアラーム通知を登録した場合、温度閾値を上回ると高体温アラームを登録した宛先へメール送信します。
- ◇ 設置要件に従ってデバイスを設置してください。
- ◇ 本製品は医療機器ではありません。体温測定や診断目的での温度検知には、医療機器を使用してください。

2.3.5.3.9 IC カード照合設定

顔データと指紋データを保存する IC カードを使用して 1:1 認証を利用する機能です。

※EDGEMATRIX Gatekeeper サービスではデバイスでの IC カード/指紋の読み取り機能を提供していません。

2.3.5.3.10 識別ルール

デバイスで、クラウドプラットフォームから配信されている識別ルールの詳細を確認できます。

アクセス手順：認証画面から「設定」→「識別ルール」



◇ 識別ルールの作成・更新・削除はクラウドプラットフォームで行われ、デバイスでは確認のみを行うことができます。

2.3.5.3.11 デバイスルール

デバイスルールで、デバイスが通過を許可する時間と禁止する時間を設定できます。1つのデバイスルールに複数の時間を設定できます。

ステップ1 認証画面で、「設定」>「デバイスルール」を選択すると、「デバイスルール」画面が開き、設定済みのルールリストを確認できます。

ステップ2 「デバイスルール」画面で、「デフォルトの時間ルール」を選択すると、「デフォルトの時間ルール」画面が開きます。「新規追加」を選択すると、「時間ルールの追加」画面が開きます。



図 11 「デバイスルール」画面

オプション	説明
名称	期間名を設定できます。
有効の曜日	ルールを有効にする曜日を設定できます。
有効な時間帯	ルールが有効になる時間帯を設定できます。
通行可否	通行可、通行不可を選択できます。

ステップ3 「デフォルト/時間ルールの追加」画面で、「削除」をタップすると、現在のルールを削除できます。「保存」をタップすると、現在のルールが保存されます。

2.3.5.3.12 登録管理

「登録管理」では、デバイスに配信される識別ルールに含まれる登録者一覧と登録者詳細を確認できます。

アクセス手順：認証画面から「設定」→「登録管理」



- ◇ デバイスへの登録者の配信、削除はクラウドプラットフォームで行われ、デバイスでは確認のみを行うことができます。
- ◇ アクティベート時に「ローカルに登録写真を不保持」と設定している場合、顔写真は表示されません。

2.3.5.3.13 ネットワーク

ネットワーク設定で、デバイスのネットワーク接続方法を設定できます。「WLAN」と「有線ネットワーク」の2種類の方法を選択できます。

アクセス手順：認証画面から「設定」→「ネットワーク」

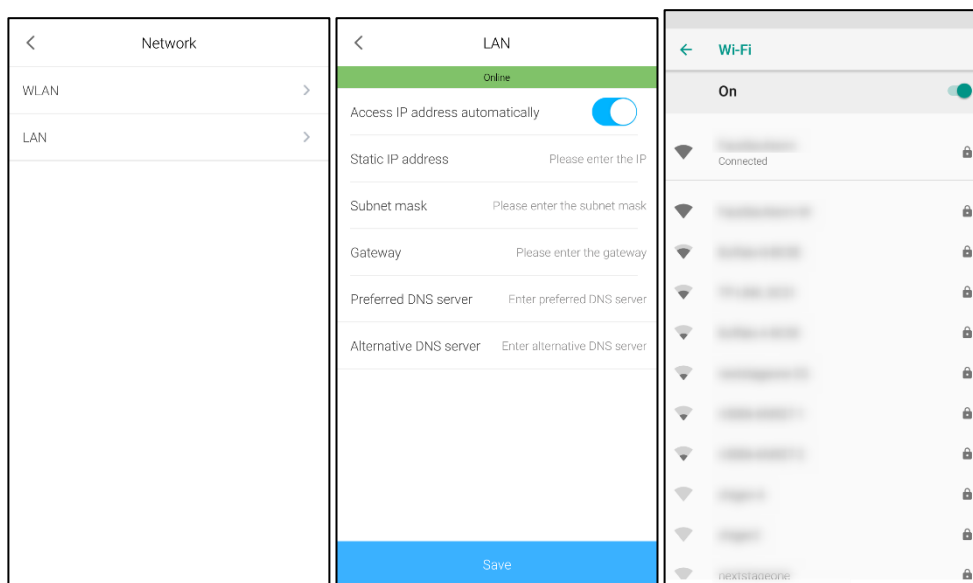


図 12 「ネットワーク」画面

2.3.5.3.14 Bluetooth

Bluetooth の設定で、外部デバイスと接続する Bluetooth の設定ができます。例：Bluetooth ロック。

※EDGEMATRIX Gatekeeper サービスでは Bluetooth 連携機能を提供していません。

2.3.5.3.15 日付と時刻

デバイスの日付フォーマット、タイムゾーンを設定します。

時間の校正は、NTP サーバと同期するため、設定を変更できません。

2.3.5.3.16 再起動

デバイスを再起動します。

2.3.5.3.17 工場出荷時の状態に戻す

デバイスを工場出荷状態に初期化します。



- ◇ デバイスのすべての設定とデータを消すため、この操作を行う前に十分に確認してから行ってください。
- ◇ この操作を行った後は、デバイスをもう一度アクティベートする必要があります。
- ◇ この操作は、クラウドプラットフォーム側の関連データには影響しません。

2.3.5.3.18 デフォルト設定に戻す

デバイスの設定内容を既定値に戻ります。

2.3.5.3.19 ドアオープン

対象デバイスと連動する電気錠、フリッパーゲートを一回アンロックします。

2.3.5.3.20 ドアオープン保持

対象デバイスと連動する電気錠、フリッパーゲートをアンロックの状態を維持します。

- ◇ 連動する電気錠、フリッパーゲートをロック状態に戻す場合は、該当設定をオフにしてください。

2.3.5.3.21 システム更新

デバイスのフォームウェアの更新方法を設定します。

以下の四つの更新方法を提供します。ユーザー側の状況に合わせて、最適な更新方法を選択してください。

更新方法 1：オンライン自動更新。更新がある場合、自動的に更新が行われます。オンライン自動更新を有効にするには、「自動更新」をオンにしてください。

更新方法 2：オンライン手動更新。更新がある場合、更新通知を表示します。ユーザーは確認してから、「更新」を押すと、更新が始まります。既定値

更新方法 3：事前に PC とデバイスを同一ネットワーク環境に置き、最新版のフォームウェアを取得して PC に保存します。PC ブラウザからデバイスのウェブ管理機能にログインし、ローカル更新する方法です。こちらの更新をご希望の場合は EDGEMATRIX 株式会社にお問い合わせください。





- ◇ オンライン更新を行うには、デバイスをクラウドプラットフォームに接続しておく必要があります。
- ◇ システム更新後、自動で再起動します。
- ◇ システム更新後、フォームウェアのバージョンを「情報」画面とクラウドプラットフォームで確認できます。

2.3.5.3.22 管理者

デバイス管理者を確認できます。



- ◇ デバイス管理者の登録とメンテナンスを、クラウドプラットフォームで行います。

- ◇ 1台のデバイスには、最大 10 名の管理者を登録できます。

2.3.5.3.23 Bluetooth ロック

デバイスが Bluetooth ロックとの連動を希望する場合、Bluetooth ロックと接続する機能です。

※EDGEMATRIX Gatekeeper サービスでは Bluetooth 連携機能を提供していません。

2.3.5.3.24 指紋登録

指紋認証を利用する場合、指紋を登録する機能です。

※EDGEMATRIX Gatekeeper サービスではデバイスでの指紋読み取り連携機能を提供していません。

2.3.5.4 拡張設定

デバイスの拡張設定画面は以下の図面の通りになります。

- ◇ 拡張設定は既定値を変更する前に、機能と手順を十分に理解したで行ってください。

アクセス手順：認証画面から「設定」→「拡張設定」



2.3.5.4.1 カメラ設定

カメラ設定では、デバイスのカメラの照明効果、補助光の調節、認証距離、露出の調整を設定できます。

アクセス手順：「拡張設定」→「カメラ設定」


図 13 「カメラ設定」画面

グループ	パラメータ	説明
照明設定	待機中の明るさ	デバイスは待機状態の補助光の明るさを設定できます。値が大きいほど、補助光が明るくなります。既定値：3%
	識別中の明るさ	デバイスは認証中の補助光の明るさを設定できます。値が大きいほど、補助光が明るくなります。既定値：100%
	識別中の照明時間	顔認証のシーンの補助光の照明時間を設定できます。値が大きいほど、補助光の照明時間が長くなります。既定値：3秒
	識別中の照明感度	近づいてくる人物への補助光の照明感度を調整できます。値が小さいほど、感度が高くなります。既定値：0%
近赤外線補助光の強さ	近赤外線補助光の強さ	近赤外線のシーンの近赤外線補助光の明るさを設定できます。値が大きいほど、近赤外線補助光が明るくなります。既定値：100%
認証距離	最大識別距離	顔認証のシーンの顔とデバイスの距離を設定できます。設定範囲：30～150cm 既定値：150cm

グループ	パラメータ	説明
可視光カメラの露出設定	露出モード	可視光認証のシーンのカメラの露出モードを設定できます。「手動モード」と「自動モード」をサポートしています。 既定値：「自動モード」
	手動露出	可視光認証のシーンのカメラの露出補正を設定できます。 値の範囲：-24～24 既定値：0 値が大きいほど露出が高くなり、画面が明るくなります。
近赤外線カメラの露出調整	露出モード	近赤外線認証のシーンのカメラの露出モードを設定できます。「手動モード」、「自動モード」、「スマートモード」をサポートしています。既定値：「自動モード」
	手動露出	近赤外線認証のシーンのカメラの露出補正を設定できます。 値の範囲：-24～24 既定値：0 値が大きいほど露出が高くなり、画面が明るくなります。

2.3.5.4.2 識別記録

識別記録では、識別記録の保存と送信を設定できます。テスターが必要なテストデータを取得するなどの PUSH 運用に役立ちます。

アクセス手順：「拡張設定」→「識別記録」



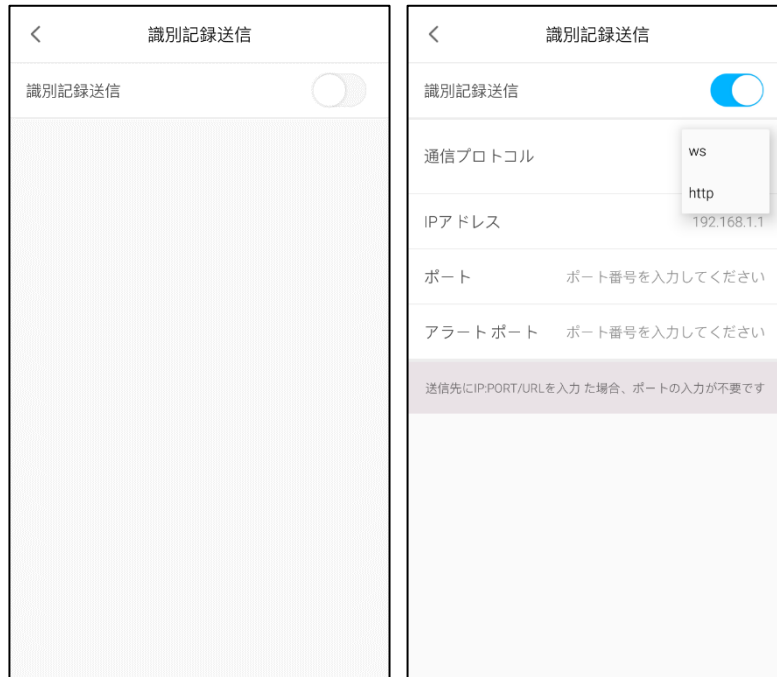
図 14 「識別記録」画面

オプション	説明
テストモード	テストモードのオンオフの設定ができます。既定値：オフ オンにすると、テスターはテストファイルをエクスポートできます。
近赤外線写真	近赤外線写真のオンオフの設定ができます。既定値：オン オンにすると、認識記録に近赤外線スナップ写真が含まれます。
記録写真の解像度	スナップ写真のサイズを設定できます。 値の範囲：軽量、標準、HD(高画質) 既定値：軽量 <ul style="list-style-type: none"> ◇ 変更した設定を有効にするためには、デバイスを再起動してください。 ◇ スナップ写真のサイズにより、デバイスのストレージの消費に影響を及ぼすため、実際のシナリオに合わせて最適な設定をおこなってください。
識別記録送信	識別記録をサードパーティのインターフェースに送信する際の設定ができます。 既定値：オフ
特徴量アップロード	1:1 顔認証を利用する場合、写真と特徴量のクラウド同期を設定できます。オンに設定した場合、特徴量のみを同期します。 既定値：オフ

識別記録送信機能は、他システムと連携する方式の一つであり、識別記録を発生する場合はデバイスから送信先のサーバへ識別記録を PUSH 送信します。送信先のサーバが識別記録を受信できるよう準備していただく必要があります。

- ◇ リアルタイム性が高い連携運用に適しています。

アクセス手順：「拡張設定」→「識別記録」→「識別記録送信」



オプション	説明
識別記録送信	「識別記録の送信」のオンオフの設定ができます。既定値：オフ
通信プロトコル	「識別記録の送信」がオンの場合、識別記録の送信に使用する通信プロトコルを ws(WebSocket)と http から選択できます。既定値：ws ◇ http の場合、http と https を選択できます。
IP アドレス	「識別記録の送信」がオンの場合、送信先の IP アドレスもしくは URL を設定できます。
ポート番号	「識別記録の送信」がオンの場合、送信先のポート番号を設定できます。
アラートポート	

2.3.5.4.3 案内設定

案内設定では、認証結果の表示項目、音声をカスタマイズする機能です。

アクセス手順：「拡張設定」→「案内設定」

案内設定では、「スマート案内」と「MP3 プロンプト」の2種類の方法を選択できます。

既定値：「MP3 プロンプト」

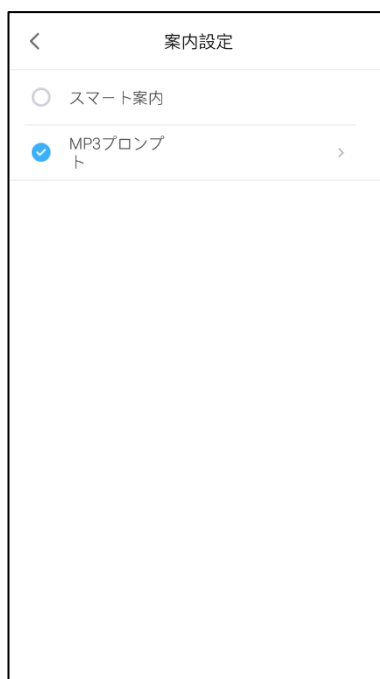


図 15 「案内設定」画面

オプション	説明
スマート案内	プロンプトを設定すると、デバイスにプロンプトを表示することができます。 また、TTS で音声に変換されます。 <ul style="list-style-type: none"> ◇ ODSL 機能を使用する場合は、「スマートプロンプト」を選択する必要があります。 ◇ 該当機能の詳細手順については、EDGEMATRIX 株式会社にお問い合わせください
MP3 プロンプト	プロンプト音声を設定します。デフォルトの音声を使用するか、異なる言語ごとにカスタム音声をアップロードできます。各言語で「認証成功のプロンプトメッセージ」、「認証失敗のプロンプトメッセージ」、「証明書をセンサーに置いてくださいのプロンプトメッセージ」を含む 3 つの音声をアップロードできます。



- ✧ 温度をオフにした場合、検温結果の表示に温度数値は表示されません。

2.3.5.4.4 アクセスコントロール

アクセスコントロール信号は、ウィーガンドプロトコルに準拠した通信信号です。ウィーガンド接続により、デバイスとサードパーティのアクセスコントローラーを連動させ、通路のデバイスやドアのアクセス機能をコントロールできます。

- ✧ デバイスで「顔+アクセスカード」の認証方法を使用する場合、アクセス制御信号を設定する必要があります。

アクセス手順 : 「拡張設定」 → 「アクセスコントロール」



図 16 「アクセスコントロール」画面

オプション	サブオプション	説明
ウィーガンドタイプ	ウィーガンドタイプ	ウィーガンドタイプを設定できます。標準「ウィーガンドモード」と「カスタムウィーガンドモード」の2種類の方法をサポートしています。
	標準ウィーガンド	次の四種類ウィーガンドを選択できます。 値の範囲：26bit、34bit、36bit、64bit
	カスタムウィーガンド	ウィーガンドをカスタマイズ(パリティ検査、総ビット、データビット、先頭の偶数パリティ、最後の奇数パリティなど)できます。設定方法の詳細については、 ステップ1 をご参照ください。
パルス間隔	ウィーガンド信号のパルス間隔を設定できます。 値の範囲：100～2000us。既定値：1000us	
パルス幅	ウィーガンド信号のパルス持続時間を設定できます。 値の範囲：20～400us。既定値：100 us	
カード情報ビット	アクセスコントロールシステムの物理カード番号のビット数を設定できます。 標準一般タイプのウィーガンドの値の範囲：16～（「データビット」-2） カスタムタイプのウィーガンドの値の範囲： 1) パリティ検査オン：16～（「データビット」-2） 2) パリティ検査オフ：16～「データビット」	

オプション	サブオプション	説明
デフォルトのウィーガンド出力設定	デバイスで特定の認証結果を得た場合に出力されるウィーガンド信号のエンコードをカスタマイズできます。開発用機能となります。	
	1:1 カード番号がライブラリに存在しない	カード番号がライブラリに存在しない場合に出力されるウィーガンド信号のエンコードを設定できます。 検証モードが「1:1 モード」または「混合モード」のシーンのみ。
	1:1 認証失敗	カード番号はライブラリに存在するものの、認証に失敗した場合に出力されるウィーガンド信号のエンコードを設定できます。 検証モードが「1:1 モード」または「混合モード」のシーンのみ。
	1:1 認証成功	顔認証が成功した場合に出力されるウィーガンド信号のエンコードを設定できます。 検証モードが「1:1 モード」または「混合モード」のシーンのみ。
	ドライ接点信号の時間	ドライ接点信号の出力時間を設定できます。 値の範囲：200～3000ms。デフォルト：750ms
アラームインターフェース (カラーシリーズ：5.5インチ)	ソフトウェアインターフェースを介してハードウェアのアラームインターフェースの切り替えができます。 アラームインターフェースには「電磁ロックの状態確認」と「アラーム入力」があり、デフォルトは「電磁ロックの状態確認」です。	

ステップ1 「アクセス制御信号の設定」画面で、「カスタムタイプのウィーガンド」を選択すると、「アクセス制御信号のカスタマイズ」画面が開きます。

オプション	説明
パリティ	ウィーガンド信号のエンコードにパリティを使用するか設定できます。
総ビット	ウィーガンド信号の総ビットを設定できます。 値の範囲：26～64。デフォルト：26。
データビット	ウィーガンド信号のデータビットを設定できます。 「パリティ検査」がオフの場合：データビット = 総ビット 「パリティ検査」がオンの場合：データビット = 総ビット - 2

オプション	説明
先頭の偶数パリティ	偶数パリティのデータビットを設定できます。
最後の奇数パリティ	奇数パリティのデータビットを設定できます。

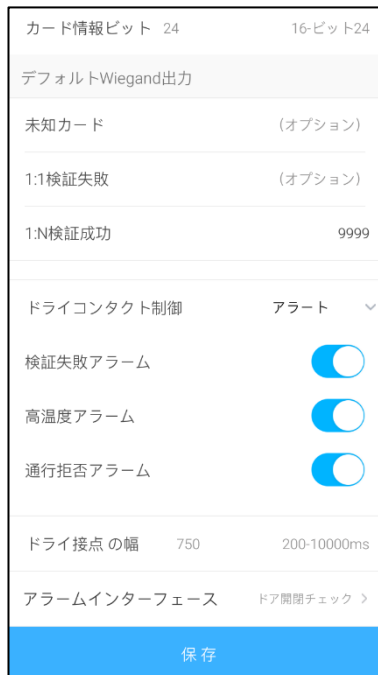
ステップ2 「保存」をタップし、設定を保存します。

- ✧ 「アラームインターフェース」を変更する場合、再起動確認ダイアログを開き、「再起動」をタップします。デバイスの再起動後、設定が有効になります。

表示灯連動設定

デバイスのドライ接点を表示灯と連動するための機能です。デバイスのドライ接点を表示灯に接続します。

表示灯を表示する条件を選択します。



- ✧ PATLITE 社の表示灯との連動を動作確認済です。
- ✧ 表示灯メーカーの製品マニュアルに従い、表示灯の設定を適意にしてください必要があります。

2.3.5.4.5 コンテンツ再生

デバイスのスタンバイ中にブランドメッセージを含む広告動画やその他の画像を再生する場合、スタンバイ画面で設定できます。

アクセス手順：「拡張設定」→「コンテンツ再生」


図 17 「コンテンツ再生」画面

グループ化	オプション	説明
表示モード	表示モード	デバイスが再生するコンテンツのディスプレイモードを設定できます。「フェイスモード」または「サイネージモード」の2種類のモードがあり、デフォルトは「フェイスモード」です。
待機文のカスタマイズ	1行目の待機文	デバイスの待機中の1行目の表示メッセージを設定します。最大で半角20文字、全角10文字まで表示できます。既定値：「ようこそ」
	2行目の待機文	デバイスの待機中の1行目の表示メッセージを設定します。最大で半角20文字、全角10文字まで表示できます。既定値：空白
	待機文表示	待機中で、待機文を表示するか設定できます。 フェイスモード：既定値：オン サイネージモード：既定値：オフ
その他	待機時計表示	サイネージモードの場合、待機画面で日付と時刻を表示するか設定できます。既定値：オフ
	待受壁紙	待機中に表示する壁紙を設定できます。

グループ化	オプション	説明
		<ul style="list-style-type: none"> ◇ 画像ファイル 1 枚のサイズは 10Mb 以下をおすすめします。 ◇ 画像のファイル形式は、jpg、jpeg、png、bmp にしてください。
	待受動画	待機中に表示する動画を設定できます。
サインページモード専用	識別丸区域の透明度	既定値：100(不透明) 待受け表示内容を最適な表現するために、透明度を適切に変更してください。

アクセス手順：「拡張設定」→「コンテンツ再生」→「待受壁紙」



図 18 「待受壁紙」画面

オプション	説明
リピート再生	待機中に壁紙をリピート再生するか設定できます。
再生時間	「リピート再生」がオンになっている場合、壁紙の再生時間の間隔を設定できます。単位：秒

アクセス手順：「拡張設定」→「コンテンツ再生」→「待受動画」



オプション	説明
リピート再生	待機中の動画をリピート再生するか設定できます。

2.3.5.4.6 ODSL 拡張設定

システム拡張向けの開発者機能となります。EDGEMATRIX 株式会社にお問い合わせください。

2.3.5.4.7 ライセンス

デバイスのライセンスを照合します。

2.3.5.4.8 取り外しアラーム

デバイスが取り外された場合にアラームを発報します。既定値：オン

2.3.5.4.9 登録写真の最小サイズ

登録写真の最小サイズでは、写真の規格を確保するため、デバイスが画像をインストールする際に許可する最小ピクセルを設定できます。

「32×32」、「128×128」、「320×320」の3種類の規格があり、デフォルトは「320×320」です。

アクセス手順：「拡張設定」→「登録写真の最小サイズ」

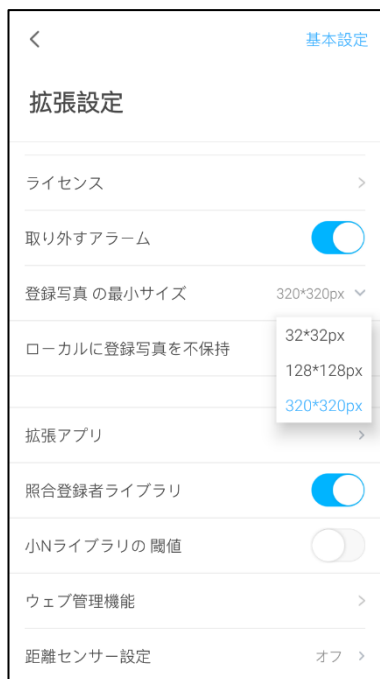


図 19 「登録写真の最小サイズ」画面

2.3.5.4.10 ローカルに登録写真を不保持

「ローカルに登録写真に不保持」では、クラウドサービスモードで、クラウド管理プラットフォームが登録者写真を配信した後、デバイスが画像の特徴値を抽出し、写真を削除するか設定できます。

アクセス手順：「拡張設定」→「ローカルに登録写真に不保持」

状態	説明
オン	クラウド管理プラットフォームが登録者写真を配信した後、デバイスが写真の特徴値を抽出し、写真を削除します。
オフ	クラウド管理プラットフォームが登録者写真を配信した後、デバイスが写真の特徴値を抽出し、写真を削除しません。

- ◇ デバイスアクティベート時にのみ選択できます。
- ◇ 設定を変更する場合、デバイスを工場出荷時の状態に戻す必要があります。

2.3.5.4.11 拡張アプリ

デバイスにインストールされる拡張アプリを照合します。システム拡張向けの開発機能です。詳細は EDGEMATRIX 株式会社にお問い合わせください。

2.3.5.4.12 照合登録者ライブラリと小 N ライブラリの閾値

登録者ライブラリの比較では、クラウドサービスモードで、デバイスが人物を比較する時に、プラットフォームが送信した人物ライブラリを使用するか、サードパーティが指定した登録者ライブラリを使用するか設定できます。システム拡張向けの開発者機能です。

状態	説明
オン	デバイスが登録者を識別する時に、プラットフォームが配信した登録者ライブラリを使用するように設定できます。
オフ	デバイスが登録者を識別する時に、サードパーティが追加した登録者ライブラリを使用するように設定できます

2.3.5.4.13 ウェブ管理機能

デバイスのウェブ管理機能では、パソコンまたはタブレットのブラウザからデバイスの管理を許可するか設定できます。

アクセス手順：「拡張設定」→「ウェブ管理機能」

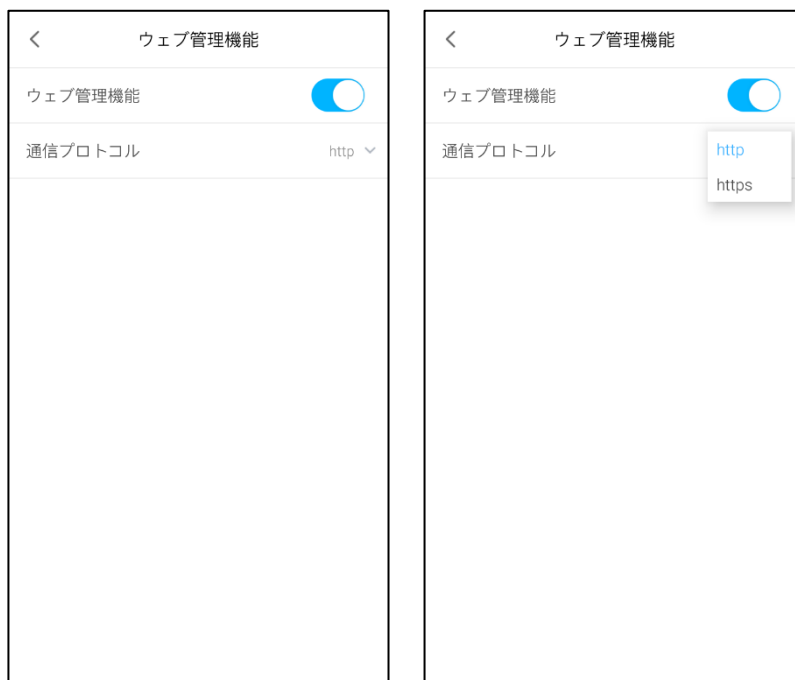


図 20 デバイスのウェブ管理機能

オプション	説明
ウェブ管理機能	ウェブ管理機能をオンにすると、パソコンまたはタブレットのブラウザからデバイスの管理画面へアクセスすることを許可します。既定値：オン
通信プロトコル	パソコンまたはタブレットのブラウザからデバイスの管理画面へアクセスする際に使用する通信プロトコルを「http」もしくは「https」に設定できます。 既定値：http

- ◇ 上記の設定変更を有効するには、デバイスを再起動する必要があります。

2.3.5.4.14 距離センサー設定

距離センサー(P-Sensor)の設定では、デバイスで P-Sensor をオンにするかと有効時間を設定できます。

P-Sensor をオンにした場合は、認証を行わない際にデバイスのディスプレイ表示がオフになります。

グループ化	オプション	説明
なし	P-Sensor オン/オフ	P-Sensor をオンにするか設定できます。
	有効時間	P-Sensor の有効時間を設定できます。「全期間」と「カスタム期間」があります。デフォルトは「全期間」です。

グループ化	オプション	説明
カスタム期間		「有効時間」で「カスタム期間」が設定されている場合、「期間の追加」をクリックし、以下のオプションを設定します。
	名称	カスタム期間の名前を設定できます。
	曜日選択	カスタム期間の繰り返し周期を「曜日」単位で設定できません。
	時間帯設定	カスタム期間の開始/終了時間を設定できます。
	有効/無効	カスタム期間の有効期間または無効期間を設定できます。

2.3.6 デバイスのメンテナンス

日常的なデバイスの使用において異常が発生した場合は、メンテナンスを実施してください。

2.3.6.1 警告メッセージ

デバイスのエラー警告メッセージは以下のとおりです。

警告メッセージ	警告の説明
ストレージエラー	デバイスのストレージの空き容量が 15%未満になると、デバイスの画面右上にアイコンが表示され、認識記録が自動的にスクロールし、クリアされます。
カメラが壊れている	カメラが故障している場合、スタンバイ画面左上に「カメラが見つかりません。デバイスを確認してください。」のメッセージが表示されます。
取り外しアラーム	取り付け式のデバイスが取り外されると警告音が鳴ります。 認証画面で、「設定」>「詳細設定」を選択し、「取り外しアラーム」をオフにすると、警告がオフになります。 ◇ 取り付け式のデバイスのみ適用されます。
ネットワーク障害	ネットワーク障害によりデバイスとクラウド管理プラットフォームが接続できない場合、スタンバイ画面右上にオフラインアイコンが表示されます。
登録者の配信	クラウド管理プラットフォームからデータをインポートしている時、スタンバイ画面左上にダウンロード進行状況のパーセンテージが表示されます。

2.3.6.2 ステータスの確認

認証画面で、「ステータス」を選択すると、「運行情報」ダイアログが表示されます。

「運行情報」ダイアログで、デバイスの「CPU 使用率」、「メモリ使用量」、「CPU 温度」、「ライトの明るさ」、パソコンデバイスでウェブ管理機能へログインする URL、モバイルデバイスでウェブ管理機能へログインする QR コードを確認できます。



図 21 「ステータス」画面

2.3.6.3 デバイス情報の確認

ステップ1 アクセス手順：認証画面から「設定」→「情報」

ステップ2 「本体について」画面で、デバイス情報を確認できます。

2.3.6.4 使用容量の確認

ステップ1 アクセス手順：認証画面から「設定」→「容量」

ステップ2 「使用容量」画面で、「登録済人数/管理者」、「登録済人数/登録可能人数」、「使用済容量/使用可能容量」を確認できます。

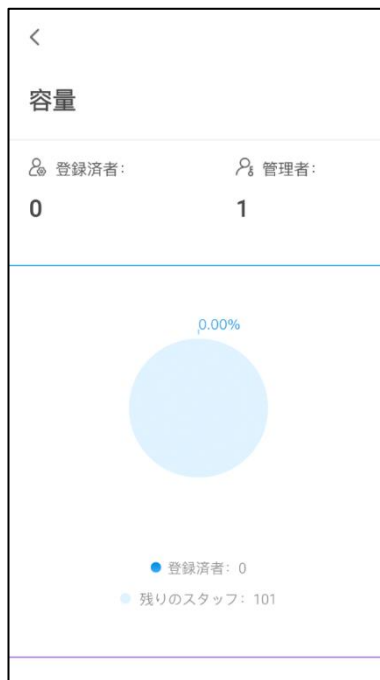


図 22 「容量」画面

2.3.6.5 再起動

ステップ1 アクセス手順：認証画面から「設定」→「再起動」

ステップ2 確認ダイアログで、「OK」をタップすると、デバイスが再起動します。



図 23 再起動

2.3.6.6 工場出荷状態に戻す

ステップ1 認証画面で、「設定」>「工場出荷の状態に戻す」を選択すると、確認ダイアログが表示されます。

ステップ2 確認ダイアログで、「OK」をタップすると、デバイスのデータが削除され、工場出荷状態に戻ります。



- ◇ 実行後、削除された情報やデータは復元できません。慎重に操作してください。
- ◇ デバイスの再起動後に初期化する必要があります。

2.3.6.7 オープンドアオープン保持

ステップ1 認証画面で、「設定」>「オープン」を選択すると、ドアロック解除画面が5秒間表示されます。

ステップ2 「設定」画面で、「ドアオープン保持」をオンにすると、ドアロックは常に解除されます。



図 24 オープン

2.3.6.8 デバイスのウェブ管理機能ツール

パソコンまたはモバイルデバイスからウェブ管理機能画面を使用してデバイスの管理を設定します。

- ✧ デバイスのウェブ管理機能オン。
- ✧ パソコン・モバイルとデバイスは同じネットワークセグメント上に存在する。

ステップ1 認証画面で、「ステータス」を選択すると、「運行情報」画面が開きます。

ステップ2 「運行情報」画面で、ウェブ管理へログイン URL と QR コードを確認できます。

ステップ3 ブラウザにログイン URL を入力するか、QR コードをスキャンすることで、デバイスのウェブ管理画面にアクセスできます。

3 クラウド管理プラットフォーム

3.1 概要説明

3.1.1 概要

クラウド管理プラットフォームの作業プロセスは以下のステップに分けられます。図 25 のとおりです。



図 25 クラウド管理プラットフォームの作業プロセス

ステップ	説明
デバイス設定	デバイスのアクティベーションコード/情報、グループ管理、基本設定、管理者割り当てなどをデバイスにリモート設定します。
登録設定	登録者、組織の管理が、アクセス・アプリの設定の基礎となります。クラウド管理プラットフォームの操作権限を設定します。
アクセス設定	システムデータに基づき、デバイスの認証方法、アクセスルールを設定します。
アプリ設定	システムデータに基づき、作業機能を設定します。
システムメンテナンス	システムの状態を日常的に点検・管理します。

3.1.2 デバイス設定

クラウドサービスモードでは、クラウド管理プラットフォームと組み合わせてデバイスを設定する必要があります。

タスク	シーンの説明	操作
アクティベート/ デバイスの追加	クラウドサービスモードでデバイスをアクティベートするステップは以下のとおりです。 1) クラウド管理プラットフォームで、アクティベート QR コードとアクティベート情報を作成します。 2) デバイスで QR コードをスキャンするか情報を入力します。 3) デバイスをアクティベートすると、デバイスの情報が自動的にクラウド管理プラットフォーム	3.3.4.1.4 アクティベーションコード

タスク	シーンの説明	操作
	に追加されます。	
デバイスグループの設定	クラウド管理プラットフォームに追加されたアクティブされているデバイスをグループ化します。	3.3.4.2 デバイスグループ
デバイス情報の同期	設定済のデバイス（送信元デバイス）のパラメータを他のデバイス（送信先デバイス）と同期します。複数のデバイスを一括設定するシーンに適しています。	3.3.4.1.2 デバイス設定のクローン配信
デバイス管理者の追加	クラウドサービスモードでは、クラウド管理プラットフォームでデバイス管理者を追加する必要があります。ステップは以下のとおりです。 1) デバイス管理者を追加する。 2) デバイスデバイスを関連付ける。 デバイス管理者はデバイスにログインし、権限の範囲内でデバイスを設定できます。	3.3.4.3 管理者
デバイス基本機能の設定	クラウドサービスモードでは、デバイス管理者はクラウド管理プラットフォームでデバイスの基本機能をリモート設定できます。	3.3.4.1.6 デバイスの設定
認証閾値ライブラリの設定	クラウドサービスモードでは、クラウド管理プラットフォームで認証閾値ライブラリを設定し、デバイスに送信できます。	3.3.4.4 設定管理

3.1.3 登録者設定

クラウドサービスモードでは、クラウド管理プラットフォームで、登録情報、デバイスなどのデータの管理を行えます。

タスク	シーンの説明	操作
登録者/組織の設定	前提条件：認証閾値ライブラリが設定されている。 クラウドサービスモードでは、クラウド管理プラットフォームで、人物の追加、人物のグループ化ができます。	3.3.3 登録管理
ブラックリストの設定	アクセスを禁止する人物を設定すると、自動的にデバイスに送信されます。ブラックリストの人物が、フロント受付、訪問予約、デバイスを通過すると、システムが警告を發します。	

タスク	シーンの説明	操作
ロール/アカウントの設定	クラウド管理プラットフォームとその他のアプリ操作の権限を設定します。ステップは以下のとおりです。 <ol style="list-style-type: none"> 1) ロールを追加し、人物データ、デバイスデータ、アプリデータのアクセス権限、プラットフォームの操作権限、アプリ管理を設定します。 2) ロールとその権限をもつクラウド管理プラットフォームの管理者アカウントを追加します。 	3.3.5 権限

3.1.4 アクセス設定

クラウドサービスモード下では、クラウド管理プラットフォームで、登録者データに基づき、デバイスへのアクセス方法を設定できます。

タスク	シーンの説明	操作
ルールの設定	指定時間内に人物がデバイスにアクセスした際の認証方法を設定します。	3.3.7 業務管理

3.1.5 アプリ設定

クラウドサービスモードでは、WebAPI(RESTful)を利用したデータ連携をアプリの設定ができます。

詳細は EDGEMATRIX 株式会社にお問い合わせください。

3.1.6 システムメンテナンス

正常な使用下において、システムの状態を日常的に点検・管理します。

タスク	シーンの説明	操作
システム情報の確認	概要情報、アラーム情報、操作ログを含むシステムのステータスを確認します。	3.3.2.1 トップページ 3.3.2.2 アラームセンター 3.3.2.3 操作ログ
確認/エクスポート/認識記録のアーカイブ	登録者のデバイスでのアクセス記録を確認します。	3.3.6.1 認識記録 3.3.9.1.1 認識記録のアーカイブ

タスク	シーンの説明	操作
自動登録招待オン	人物のユーザーセンターからの登録を許可します。	3.3.9.2.1 自動登録招待のオン/オフ
デバイス/登録者/アクセス/応用設定の変更	設定済の設定の最適化/変更。	3.3.4.1.6 デバイスの設定 3.3.3 登録管理 3.3.7 業務管理

3.2 操作説明（ユーザーセンター）

3.2.1 ログイン

ステップ1 ログイン画面で、登録済のアカウント情報を入力します。

オプション	説明
メールアドレス	登録したアカウントのメールアドレスを入力します。
パスワード	登録したアカウントのパスワードを入力します。
認証コード	6桁の認証コードをメールアドレスから取得し、入力します。
認証コード	画像認証を入力します。 <ul style="list-style-type: none"> ◇ 3回連続で間違った「パスワード」を入力すると、「認証コード」オプションが表示されます。 ◇ 画像をタップして、認証コードを更新します。

ステップ2 「ログイン」をタップします。

ログインが完了すると、マイアカウント画面が開きます。

- ◇ ユーザーごとに権限が異なるため、クラウド管理プラットフォームはユーザーがもつ権限範囲に応じた操作画面を表示します。
- ◇ 24時間以内に間違った「パスワード」を10回入力すると、アカウントが10分間ロックされ、10分後引き続きログインを試すことができます。
- ◇ パスワードが間違っていてログインできない場合、「パスワードを忘れた場合」をタップし、アカウントのパスワードを取得してください。

3.2.2 パスワード取得

ステップ1 ログイン画面で、「パスワードを忘れた場合」をタップすると、パスワード設定画面が開きます。

ステップ2 登録されているメールアドレスを入力し、「認証コードを取得」をクリックし、送信された認証コードを入力します。

ステップ3 設定されるパスワードとパスワードの再確認を入力し「OK」をクリックして設定を保存します。

ステップ4 ログイン画面に戻りますので、ステップ3で設定されたパスワードでログインします。

3.2.3 個人情報変更

ステップ1 クラウド管理プラットフォームの操作画面右上の、ユーザー名 > 「プロフィール」をタップすると、「プロフィール」が開きます。

ステップ2 「個人情報」画面。

- 1) ニックネームの後ろにある「変更」をタップし、ニックネームを変更します。
- 2) パスワードの後ろにある「パスワードの変更」をタップし、パスワードを変更します。
- 3) アカウント情報の後ろにある「変更」をタップし、登録メールアドレスを変更します。
- 4) 認証コードの取得と入力。

ステップ3 「保存」をタップすると、変更が完了します。

3.3 操作について（クラウド管理プラットフォーム）

3.3.1 概要説明

クラウド管理プラットフォームには、ダッシュボード、登録管理、デバイス管理、権限、データ管理、業務管理、アプリ、システムの8つの機能モジュールが含まれます。

名前	説明
ダッシュボード	デバイスアラーム、操作ログなど日常のモニタリング情報を確認できます。ルール、訪問者アプリ、メッセージ送信アプリ、自己登録、連動、勤怠管理、ブラックリスト、ビデオドアホンアプリへのショートカットが提供されています。
登録管理	登録者とその情報を管理し、登録者をグループ化など登録者に関わる管理操作をできます。

名前	説明
デバイス管理	デバイスの管理と操作、デバイスのグループ化、デバイスの管理者、デバイスの基本パラメータの設定、認証閾値ライブラリの設定、設定をデバイスへの配信の照合などデバイスに関わる操作を行えます。
権限	ロールに基づき、クラウド管理プラットフォームの権限を管理できます。
データ管理	デバイスがアップロードした認識記録を確認/管理できます。
業務管理	認証ルールを管理し、人物情報と関連付けられた認証ルールをデバイスに送信できます。
アプリ	アプリ管理を管理できます。
システム	認識記録のアーカイブ、アカウントの管理、メイン管理者の変更、アラーム通知など、システムの維持管理ができます。

3.3.2 ダッシュボード

クラウド管理プラットフォームでは、デバイスアラーム、操作ログなど日常のモニタリング情報を確認できます。また、ルールのショートカットが提供されています。

3.3.2.1 トップページ

トップページでは、デバイスアラームの統計、最新の操作ログなどの概要情報を確認できます。また、クイックポータルにはショートカットを掲示します。

※EDGEMATRIX Gatekeeper サービスでは基本アプリケーションの追加機能を提供していません。

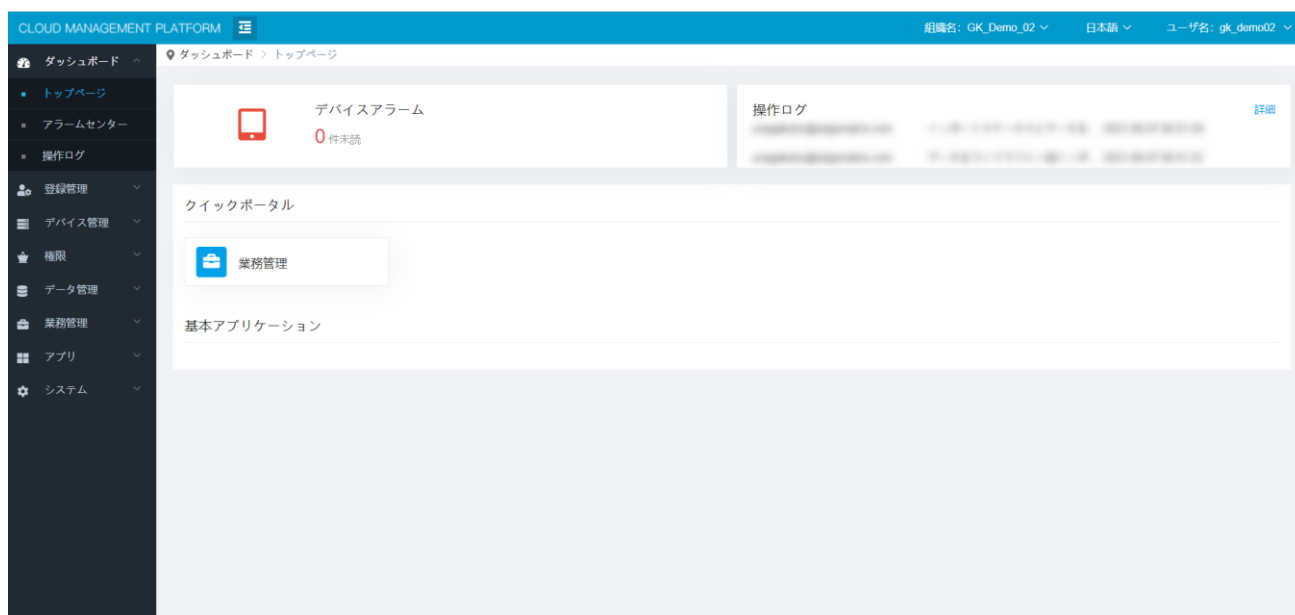


図 26 トップページ

3.3.2.1.1 概要情報の確認

ステップ1 **アクセス手順**：左側メニュー→ダッシュボード→トップページ

「トップページ」画面が開き、概要情報とショートカットを確認できます。

概要情報：デバイスアラーム統計情報、最新の操作ログ。

ショートカット：業務管理へのリンク。

ステップ2 「トップページ」画面：

- 1) ユーザー名をクリックすると、「プロフィール」画面が開き、ユーザー情報を照合できます。

ユーザー情報：ニックネーム、パスワード、管理者 ID、メールアドレス。詳細：『3.3.2.1.2 ユーザー情報の変更』

- 2) 「デバイスアラーム」をクリックすると、「アラームセンター」画面が開きます。詳細：『3.3.2.2.13.3.2.2.1 デバイスアラームの確認』

- 3) 「操作ログ」>「詳細」をクリックすると、「操作ログ」画面が開きます。詳細：『3.3.2.3.1 操作ログの確認』

- 4) 「業務管理」をクリックすると、「通行規則」画面が開きます。詳細：『3.3.7.1 通行規則』

- 5) 基本アプリ領域のアプリをクリックすると、指定したアプリへジャンプする画面が開きます。

3.3.2.1.2 ユーザー情報の変更

ステップ1 **アクセス手順**：左側メニュー→ダッシュボード→トップページ

ステップ2 ログインユーザー名をクリックすると、「プロフィール」画面が開きます。



プロフィール

アバター 

ニックネーム ユーザー名: gk_demo02 [変更](#)

パスワード 6~20桁のパスワード (数字、大文字、小文字、特殊記号) [変更](#)

現在のアカウント

管理者ID 

メールアドレス  [変更](#)

ステップ3 「変更」をクリックすると、ログインユーザーのニックネーム、パスワード、メールアドレスを変更できます。

3.3.2.2 アラームセンター

アラームセンターでは、デバイスのアラート情報を確認できます。アラームタイプには以下が含まれます。

タイプ	説明
温度が高すぎる	デバイスの温度が 90℃ を超えている。
カメラが壊れている	デバイスのカメラが壊れている。
ストレージの事前警告	デバイスのストレージの空き容量が 15% 未満。
デバイスがオフライン	デバイスがクラウド管理プラットフォームに接続されていない。
デバイスが取り外された	「デバイスの取り外しアラーム」がオンになっているデバイスが取り外された。
セキュリティゲート警告	デバイスが重なっている人物、逆行している人物を検出した。
人の出入り警告	ブラックリストの人の通行。
体温アラーム	検温結果が温度閾値を超えている。

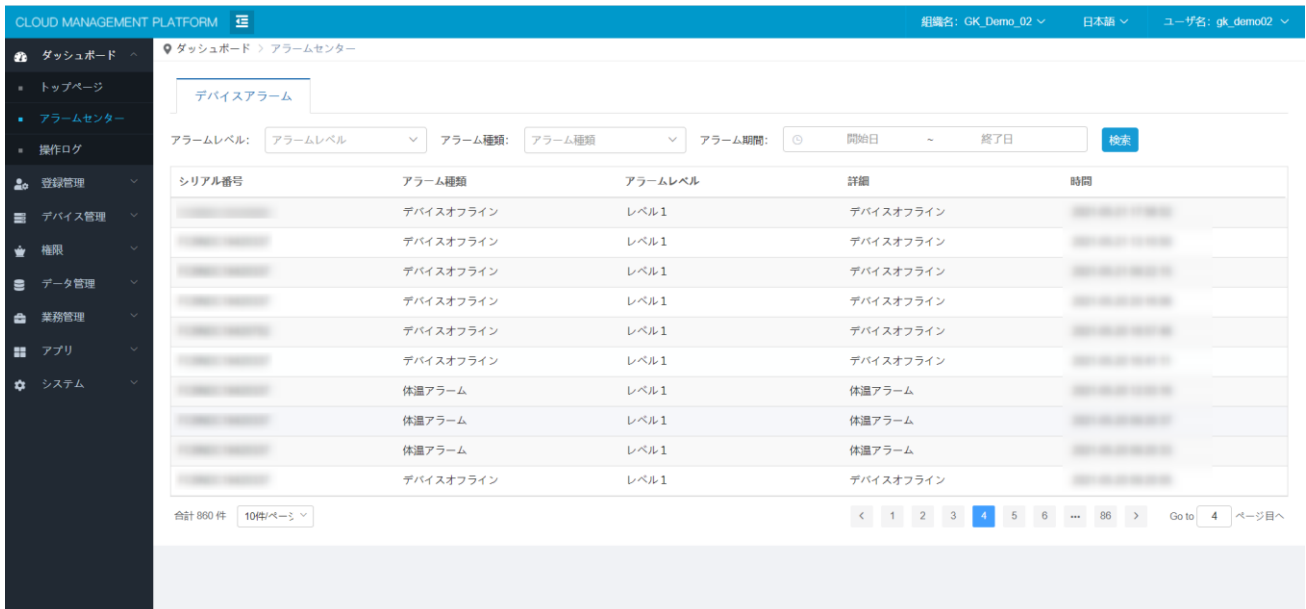


図 27 アラームセンター

3.3.2.2.1 デバイスアラームの確認

ステップ1 **アクセス手順：左側メニュー→ダッシュボード→アラームセンター**

「アラームセンター」画面が開き、デバイスアラームを照合できます。

デバイスアラーム情報：シリアル番号、アラーム種類、アラームレベル、詳細、時間。

ステップ2 「アラームセンター」画面：

- 1) 「アラームレベル」を選択し、「検索」をクリックすると、指定したアラームレベルのアラーム情報を照合できます。
- 2) 「アラーム種類」を選択し、「検索」をクリックすると、指定したアラーム種類のアラーム情報を照合できます。

アラーム種類には以下が含まれます。

アラーム種類	説明
高温	デバイスの温度が 90℃ を超えている。
カメラの損傷	デバイスのカメラが壊れている。
ストレージの警告	デバイスのストレージの空き容量が 15%未滿。
デバイスオフライン	デバイスがクラウド管理プラットフォームに接続されていない。
デバイスが取り外されました	「デバイスの取り外し事前警告」がオンになっている取り付け式のデバイスが取り外された。
スピードゲート警報	デバイスは重なっている人物、逆行している人物を識別します。
人員の出入りアラーム	ブラックリストの人物の通行。
体温アラーム	検温結果が温度閾値を超えている。
ソフトウェアのダウンロード失敗	ダウンロードしたデバイスファームのファイルチェックサムに失敗。

- 3) 「アラーム期間」の「開始日」と「終了日」を入力し、「検索」をクリックすると、指定した期間のアラーム情報を照合できます。

3.3.2.3 操作ログ

操作ログ画面では、管理者によるクラウド管理プラットフォームの操作ログ情報を照合できます。

CLOUD MANAGEMENT PLATFORM

組織名: GK_Demo_02 日本語 ユーザー名: gk_demo02

ダッシュボード > 操作ログ

管理者: 操作時間: ~

管理者	主要機能	操作詳細	操作時間
...	デバイス管理	シリアル番号によって設定を更新	...
...	登録管理	インポートステータスとデータをクリア	...
...	登録管理	データをライブラリに一括インポート	...
...	登録管理	人員プロフィールを一括でインポート	...
...	登録管理	インポートステータスとデータをクリア	...
...	登録管理	データをライブラリに一括インポート	...
...	登録管理	人員プロフィールを一括でインポート	...
...	登録管理	人員を一括削除	...
...	ルール配信	ルールをデバイスへ配信	...
...	設定管理	端末構成を追加	...

合計 384 件 ... ページ目へ

図 28 操作ログ

3.3.2.3.1 操作ログの確認

ステップ1 アクセス手順：左側メニュー→ダッシュボード→操作ログ

「操作ログ」画面が開き、各クラウド管理者のクラウド管理プラットフォームの操作ログを照合できます。

操作ログ：管理者、主要機能、操作詳細、操作時間。

ステップ2 「操作ログ」画面：

- 1) 「管理者」を入力し、「検索」をクリックすると、指定した管理者の操作ログを検索できます。
- 2) 「操作時間」の「開始日」と「終了日」を入力すると、指定期間の操作ログを確認できます。

3.3.3 登録管理

登録管理では、登録者とその情報を管理し、登録者をグループ化できます。

3.3.3.1 登録管理

登録管理では、登録者とその情報を管理できます。

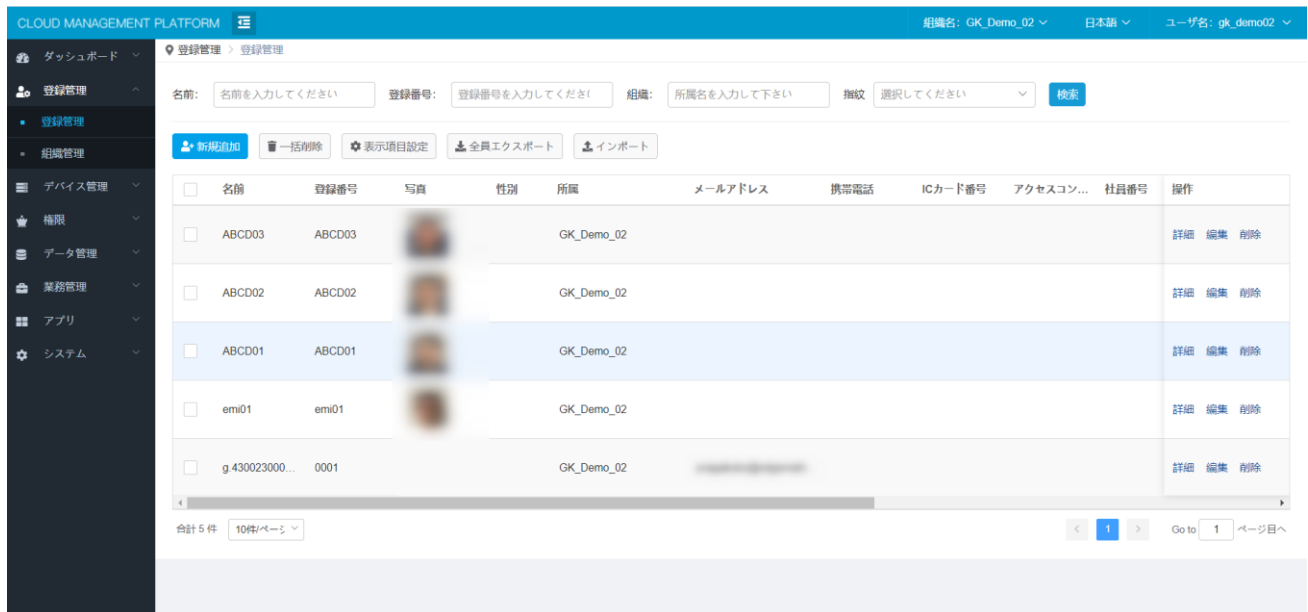


図 29 登録管理

3.3.3.1.1 登録者の検索

ステップ1 **アクセス手順**：左側メニュー→登録管理→登録管理

登録者一覧を照合できます。

ステップ2 「登録管理」画面：

- 1) 「名前」を入力し、「検索」をクリックすると、指定した名前の登録者を照合できます。
- 2) 「登録番号」を入力し、「検索」をクリックすると、指定した登録番号の登録者を照合できます。
- 3) 「組織」を入力し、「検索」をクリックすると、指定した組織の登録者を照合できます。
- 4) 「指紋」を選択し、「検索」をクリックすると、指紋あり/なしの登録者を照合できます。

※EDGEMATRIX Gatekeeper サービスでは指紋関連機能を提供していません。

3.3.3.1.2 登録者詳細情報の照合

ステップ1 **アクセス手順**：左側メニュー→登録管理→登録管理

ステップ2 「登録管理」画面で、登録者を検索します。

ステップ3 登録者リストで、「操作」列の「詳細」をクリックすると、「登録者詳細」画面が開き、指定した登録者の詳細情報を照合できます。

- ☆ 登録者詳細情報のフィールドには、12 の必須フィールド(デフォルト)と 10 のカスタムフィールドがあります。フィールド設定操作の詳細について『3.3.3.1.9 表示項目設定』を参考してください。


3.3.3.1.3 登録者の個別追加


ステップ1 アクセス手順：左側メニュー→登録管理→登録管理

「登録管理」画面が開きます。

ステップ2 「登録管理」画面で、「新規追加」をクリックすると、「登録者の新規追加」画面が開きます。

ステップ3 登録者情報を入力します。

オプション (*必須)	説明
名前*	登録者の名前を指定できます。 値の範囲：64 桁以内 以下の特殊文字は入力できません：「'」、「%」、「\」、「/」、「 」、「_」、「&」、「#」、「:」。
登録番号*	登録者の登録番号を指定でき、登録者を一意に識別します。 データタイプ：数字、アルファベット、アンダーライン、ハイフン 値の範囲：32 桁以内  ◇ 人物番号は一度設定すると変更できません。慎重に操作してください。
写真	登録者の写真を登録できます。
性別	登録者の性別を設定できます。
組織*	登録者の所属組織を設定できます。 設定について：「所属組織」は事前に設定した組織です。
メールアドレス	登録者のメールアドレスを設定できます。 ◇ 登録者のメールアドレスは一意でなければなりません。 ◇ 登録者の追加後、メールアドレスは登録者のみが編集・変更できます。管理者はこの操作を実行できません。
携帯電話	人物の携帯電話番号を設定できます。 ◇ 登録者の携帯電話は一意でなければなりません。 ◇ 登録者の追加後、携帯電話番号は人物のみが編集・変更できます。管理者はこの操作を実行できません。
IC カード番号	ウィーガンドタイプではない IC カード番号を設定できます。 データタイプ：英語、数字 値の範囲：32 桁以内 ※EDGEMATRIX Gatekeeper サービスでは IC カード関連機能を提供

オプション (*必須)	説明
	していません。
社員番号	登録者の社員番号を設定できます。
認証パスワード	数字 4 桁のアクセス認証パスワードを設定できます。
アクセスコントロール番号	登録者と関連付けられたウィーガンドタイプの IC カード番号を設定できます。 データタイプ：数字 値の範囲：20 桁以内
認識パラメータライブラリ	登録者が所属する認証パラメータライブラリを設定できます。個別の識別閾値を利用する場合に役立ちます。 設定について：「認識パラメータライブラリ」は事前に設定する必要があります。 操作の詳細について：『3.3.4.4 設定管理』
指紋 1	デバイスでキャプチャした人物の指紋を同期できます。
指紋 2	デバイスでキャプチャした人物の指紋を同期できます。
<カスタムフィールド>	<p>カスタム情報フィールドを設定できます。</p> <ul style="list-style-type: none"> ◇ 人物情報には 10 個のカスタムフィールドを含めることができます。フィールド設定操作の詳細について：『3.3.3.1.9 表示項目設定』  ◇ カスタムフィールドでデータの競合が発生しやすくなるため、使用をおすすめしません。

ステップ4 「OK」をクリックし、設定を保存します。

3.3.3.1.4 登録者の一括追加

ステップ1 **アクセス手順：左側メニュー→登録管理→登録管理**

ステップ2 「登録管理」画面で、「インポート」をクリックすると、「インポート」画面が開きます。

ステップ3 「インポート」画面：

- 1) 「テンプレートのダウンロード」をクリックして登録者リストのテンプレートをダウンロードし、「プロンプト」に従って登録者データを準備します。
- 2) 「登録者情報」>「Excel」>「追加」をクリックし、登録者リストをアップロードします。

- 3) (オプション)「人物の写真」>「zip ファイル/フォルダ」>「追加」をクリックし、写真が保存されている zip ファイル/フォルダを指定します。
- 4) 「次へ」をクリックします。

登録者データのアップロードが完了すると、「データプレビュー」画面が開きます。

◇ 一括追加の場合、一度に追加するのは2万人以下をおすすめします。

ステップ4 「データプレビュー」画面：

- 1) 登録者データに間違いがないか確認します。
- 2) 「インポート」をクリックします。

インポートが完了すると、「完了」画面が開きます。

ステップ5 「完了」画面で、インポート結果を確認します。

インポートが失敗した場合、「失敗記録のエクスポート」をクリックします。成功した場合は、「完了」をクリックします。

3.3.3.1.5 登録者の編集

ステップ1 アクセス手順：左側メニュー→登録管理→登録管理

ステップ2 「登録管理」画面で、登録者を検索し、指定します。

ステップ3 「編集」をクリックすると、「登録者の編集」画面が開きます。

ステップ4 登録者情報を変更します。

ステップ5 「OK」をクリックし、変更を保存します。

3.3.3.1.6 登録者の削除



- ◇ 登録者を削除すると復元できません。慎重に操作してください。
- ◇ メイン管理者は削除できません。

ステップ1 アクセス手順：左側メニュー→登録管理→登録管理

ステップ2 「登録管理」画面で、登録者を検索し、指定します。

ステップ3 「操作」列の「削除」をクリックし、登録者を削除します。

3.3.3.1.7 登録者の一括削除



- ◇ 登録者を削除すると復元できません。慎重に操作してください。
- ◇ メイン管理者は削除できません。

- ステップ1 アクセス手順：左側メニュー→登録管理→登録管理
- ステップ2 「登録管理」画面で、登録者を検索し、指定します。
- ステップ3 登録者リストで、1人または複数の「名前」の左側にあるチェックボックスを選択します。
- ステップ4 「一括削除」をクリックすると、指定した登録者が削除されます。

3.3.3.1.8 登録者データの一括エクスポート

- ステップ1 アクセス手順：左側メニュー→登録管理→登録管理
- ステップ2 「登録管理」画面で、エクスポートする登録者を検索します。
- ◇ 検索条件が設定されていない場合、デフォルトですべての登録者データがエクスポートされます。
 - ◇ 1度にエクスポートできる人数は5000人以下です。

- ステップ3 「一括エクスポート」をクリックすると、指定した検索条件と一致する登録者データがエクスポートされます。

エクスポートされるデータ：登録者情報のExcelリスト、登録者の写真zipファイル。

3.3.3.1.9 表示項目設定

- ステップ1 アクセス手順：左側メニュー→登録管理→登録管理
- ステップ2 「登録管理」画面で、「表示項目設定」をクリックすると、「表示項目設定」画面が開きます。
- ステップ3 「表示項目設定」画面：
- 1) 「オプション項目」区域で、カスタム項目を設定/変更/選択します。
- ステップ4 「OK」をクリックし、設定を保存します。
- ◇ フィールドの追加は、登録済の登録者にも適用されます。
 - ◇ フィールドを隠しても、登録済の登録者フィールドの情報は削除されません。

3.3.3.2 組織管理

組織管理では、登録者をグループ化できます。管理や承認に役立ちます。

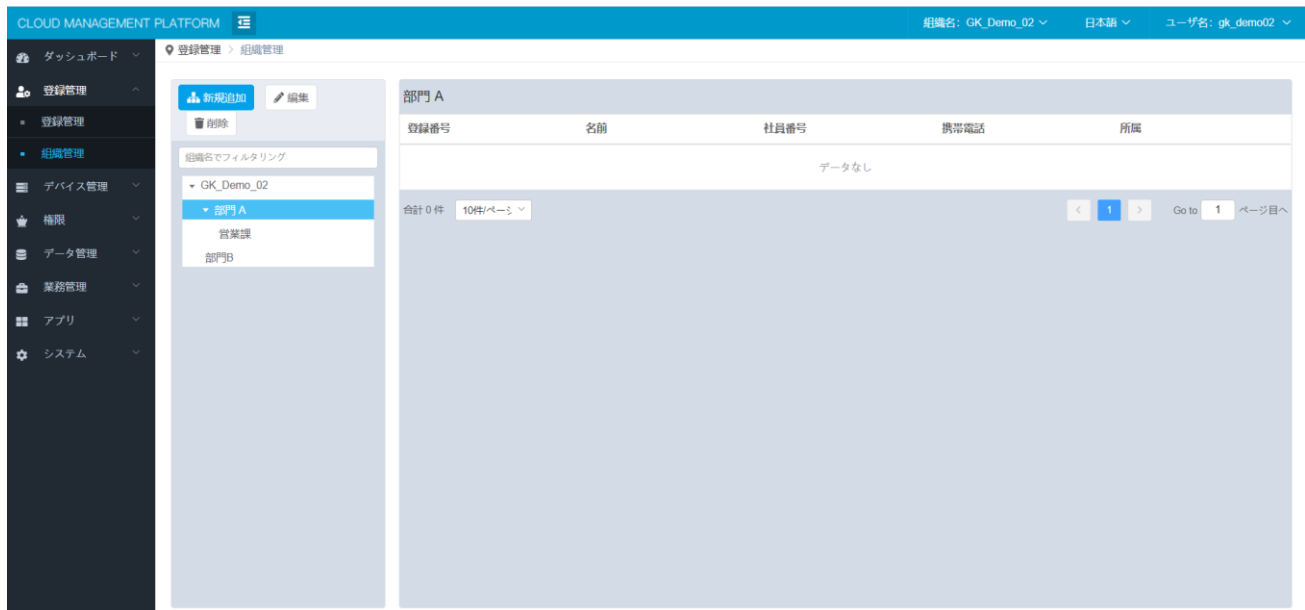


図 30 組織管理

3.3.3.2.1 組織の確認

- ステップ1 **アクセス手順**：左側メニュー→登録管理→組織管理
- ステップ2 「組織管理」画面の左側リストに、登録済の組織、組織のツリー構造が表示されます。
- ステップ3 左側リストのテキストボックスにキーワードを入力すると、組織名であいまい検索し、検索条件と一致する組織をフィルタリングできます。
- ステップ4 左側リストで組織名をクリックすると、指定した組織に含まれる登録者リストが右側に表示されます。

3.3.3.2.2 組織の追加

- ステップ1 **アクセス手順**：左側メニュー→登録管理→組織管理
- ステップ2 「組織」画面で、組織を検索すると、追加する組織の親組織を指定できます。



◇ 追加組織の「親組織」は一度設定すると変更できません。慎重に操作してください。

- ステップ3 「新規追加」をクリックすると、「組織の追加」ダイアログが開きます。
- ステップ4 「組織の追加」ダイアログ：
- 1) 「上級組織」のデフォルトはアカウント設定時に設定した最上位組織です。
 - 2) 「名称」を入力し、追加する組織の名前を設定します。
- ステップ5 「OK」をクリックし、設定を保存します。

3.3.3.2.3 組織の編集

- ステップ1 **アクセス手順**：左側メニュー→登録管理→組織管理
- ステップ2 「組織」画面で、組織を検索し指定します。
- ステップ3 「編集」をクリックすると、「組織の編集」ダイアログが開きます。
- ステップ4 「組織の編集」ダイアログで、「名前」を入力し、「OK」をクリックすると設定が保存されます。

3.3.3.2.4 組織の削除

- ステップ1 **アクセス手順**：左側メニュー→登録管理→組織管理
- ステップ2 「組織」画面で、組織を検索し指定します。
- ステップ3 指定した組織に登録者が含まれていない場合、「削除」をクリックすると、削除確認ダイアログが開きます。「OK」をクリックすると、指定した登録者組織が削除されます。
- ステップ4 指定した組織に登録者が含まれている場合、「削除」をクリックすると、「組織の削除」ダイアログが開き、「この組織には登録者情報が含まれています。登録者の処理方法を選択してください」と表示されます。
- 1) 組織とその組織のすべての登録者を削除する
 - 2) 組織とその組織のすべての登録者が削除されます。登録者の組織を指定する必要があります。
- 「OK」をクリックします。



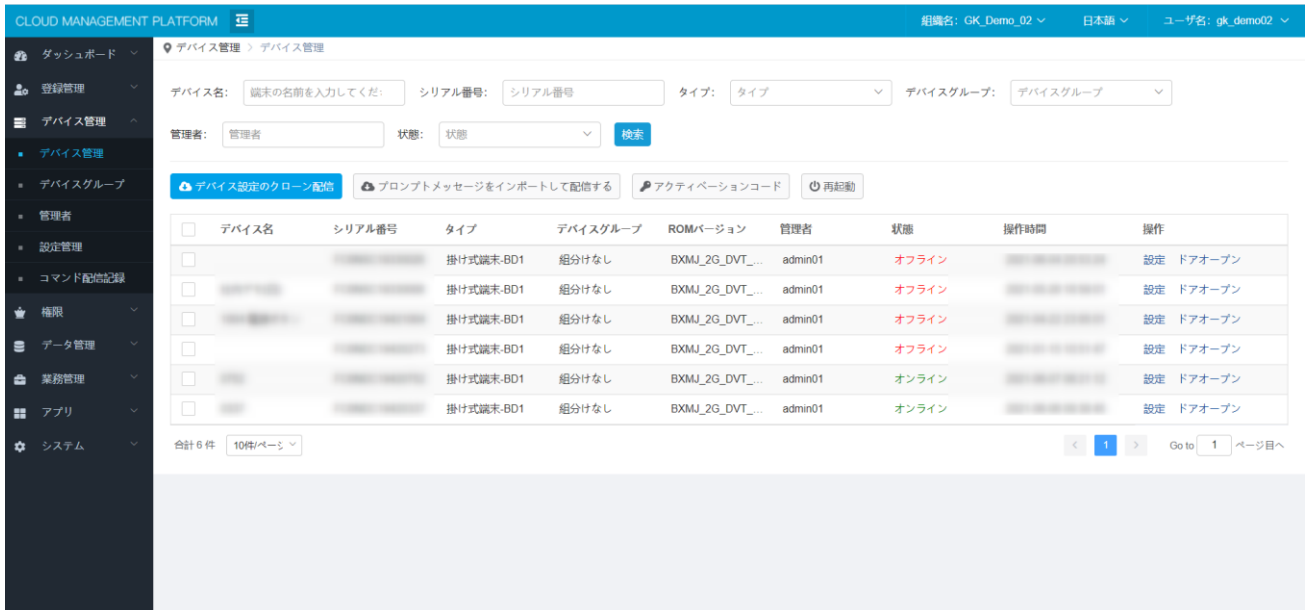
- ◇ 組織とその登録者は一度削除すると、変更できません。慎重に操作してください。

3.3.4 デバイス管理

デバイスの管理では、デバイスとその情報の管理、デバイスのグループ化、管理者、デバイスの関連付け、デバイスの基本パラメータの設定、認証閾値ライブラリの設定、設定の送信ができます。

3.3.4.1 デバイス管理

デバイスの管理画面では、デバイスとその情報の管理、デバイスのリモート管理/コントロール、プロンプトメッセージのインポートと送信、デバイスのアクティベーションコードと情報の取得ができます。



クラウド管理プラットフォームの「デバイス管理」画面のスクリーンショット。検索フィルターとデバイスリストが表示されています。

デバイス名	シリアル番号	タイプ	デバイスグループ	ROMバージョン	管理者	状態	操作時間	操作
		掛け式端末-BD1	組分けなし	BXMJ_2G_DVT_...	admin01	オフライン		設定 ドアオープン
		掛け式端末-BD1	組分けなし	BXMJ_2G_DVT_...	admin01	オフライン		設定 ドアオープン
		掛け式端末-BD1	組分けなし	BXMJ_2G_DVT_...	admin01	オフライン		設定 ドアオープン
		掛け式端末-BD1	組分けなし	BXMJ_2G_DVT_...	admin01	オフライン		設定 ドアオープン
		掛け式端末-BD1	組分けなし	BXMJ_2G_DVT_...	admin01	オンライン		設定 ドアオープン
		掛け式端末-BD1	組分けなし	BXMJ_2G_DVT_...	admin01	オンライン		設定 ドアオープン

図 31 デバイスの管理

3.3.4.1.1 デバイスの確認

ステップ1 アクセス手順：左側メニュー→デバイス管理→デバイス管理

「デバイス管理」画面を開き、登録済のデバイスリストを確認します。

デバイス情報：デバイス名、シリアル番号、タイプ、デバイスグループ、バージョン番号、管理者、状態、操作時間。

ステップ2 「デバイス管理」画面：

- 1) 「デバイス名」を入力し、「検索」をクリックすると、指定した名前のデバイスを確認できます。
- 2) 「シリアル番号」を入力し、「検索」をクリックすると、指定したシリアル番号のデバイスを確認できます。
- 3) 「タイプ」を入力し、「検索」をクリックすると、指定したタイプのデバイスを確認できます。
- 4) 「デバイスグループ」を入力し、「検索」をクリックすると、指定したデバイスグループに属するデバイスを確認できます。

「デバイスグループ」は事前に設定したデバイスグループです。操作の詳細については：『3.3.4.2 デバイスグループ』

- 5) 「管理者」を入力し、「検索」をクリックすると、指定した管理者が管理するデバイスを確認できます。
- 6) 「状態」を入力し、「検索」をクリックすると、指定した状態のデバイスを確認できます。

デバイスの状態には「オフライン」と「オンライン」の2種類の状態があります。

3.3.4.1.2 デバイス設定のクローン配信

デバイス設定のクローン配信では、設定済のデバイスの設定パラメータを取得し、他のデバイス（送信先デバイス）にクローンできます。複数のデバイスを同様に設定するシーンに適しています。

ステップ1 アクセス手順：左側メニュー→デバイス管理→デバイス管理

ステップ2 「デバイス管理」画面で、指定する送信元デバイスを検索して表示させ、「デバイス名」の左側にあるチェックボックスをチェックします。

- ◇ オンラインのデバイスをしか選択できません。
- ◇ 一台のデバイスをしか選択できません。
- ◇ 設定先のデバイスと同じのデバイスタイプのデバイスを選択してください。

ステップ3 「デバイス設定のクローン配信」をクリックし、「プロンプト」ダイアログが開けば、クラウド管理プラットフォームは指定したデバイスからの設定パラメータの取得を完了しています。

ステップ4 「プロンプト」ダイアログで、「設定を一括デリバリー」をクリックすると、「設定を一括デリバリー」ダイアログが開きます。

ステップ5 「設定を一括デリバリー」ダイアログで、指定する1つまたは複数の配信先デバイスを検索して表示させ、「デバイス名」の左側にあるチェックボックスをチェックします。

ステップ6 「ダウンデリバリーを確定」をクリックすると、指定したデバイスに設定が同期されます。

3.3.4.1.3 プロンプトメッセージのインポートと送信

ステップ1 アクセス手順：左側メニュー→デバイス管理→デバイス管理

ステップ2 「デバイス管理」画面で、指定するデバイスを検索して表示させます。

ステップ3 デバイスリストで、「デバイス名」の前にあるチェックボックスを1つ選択します。

ステップ4 「プロンプトメッセージをインポートして送信する」をクリックすると、「プロンプトメッセージをインポートして送信する」ダイアログが開きます。

ステップ5 「プロンプトメッセージのインポートと送信」ダイアログに、関連情報を入力します。

オプション	説明
言語の選択	プロンプトメッセージの言語を設定できます。
プロンプトメッセージ	JSON形式のプロンプトメッセージファイルをアップロードできます。

ステップ6 「歩調を合わせる」をクリックすると、指定したプロンプトメッセージがインポートされ、デバイスに送信されます。

※JSON 形式のプロンプトメッセージファイルの作成については EDGEMATRIX 株式会社にお問い合わせください。

3.3.4.1.4 アクティベーションコード

- ステップ1 **アクセス手順：左側メニュー→デバイス管理→デバイス管理**
- ステップ2 「デバイス管理」画面で、「アクティベーションコード」をクリックすると、「デバイスのアクティベーションコード」ダイアログが開きます。「プラットフォームのドメイン」、「アクティベーションコード」、「デバイスグループコード」、デバイスのアクティベーション情報を含んだ QR コード。
- ステップ3 「リフレッシュ」をクリックし、「アクティベーションコード」と QR コードをリフレッシュします。
- アクティベーション情報とアクティベーションコードは、デバイスのアクティベートに使用します。

3.3.4.1.5 デバイスの再起動

- ステップ1 **アクセス手順：左側メニュー→デバイス管理→デバイス管理**
- ステップ2 「デバイス管理」画面で、指定するデバイスを検索して表示させます。
- ステップ3 デバイスリストで、「デバイス名」の前にあるチェックボックスを 1 つまたは複数選択します。
- ステップ4 「再起動」をクリックすると、指定したデバイスが再起動します。

3.3.4.1.6 デバイスの設定

- ステップ1 クラウド管理プラットフォームの左側のリストにある、「デバイス」>「デバイス管理」をクリックすると、「デバイス管理」画面が開きます。
- ステップ2 「デバイス管理」画面で、指定するデバイスを検索して表示させます。
- ◇ デバイスの状態が「オフライン」の場合、デバイスは設定できません。
- ステップ3 デバイスリストで、「操作」列の「設定」をクリックすると、「デバイスの設定」ダイアログが開きます。

3.3.4.1.6.1 本体について

- ステップ1 「情報」タブでは、デバイスの情報を確認できます：デバイス名、デバイスタイプ、シリアル番号、ソフトウェアバージョン、アルゴリズムバージョン、ハードウェアの

バージョン、無線 MAC アドレス、有線 MAC アドレス、登録者ライブラリの容量。
ステップ2 「名称」を入力し、「OK」をクリックすると、デバイス名を変更できます。

3.3.4.1.6.2 ワークモード

「ワークモード」では、以下を含むデバイスのワークモードを設定できます。

オプション	説明
温度測定モード	温度測定のシーンのみで使用します。このシーンでは、登録者の認証を行いません。
身元認証モード	顔認証のみのシーンで使用します。
温度測定+顔認証モード	顔認証と同時に温度測定するシーンで使用します。

3.3.4.1.6.3 検証順

「検証順」では、デバイスが認証を開始するトリガーを設定でき、以下が含まれます。

オプション	説明
ドキュメント/カードトリガー	「検証モード」で「1:1 モード」を設定すると、証明書またはカード（アクセスカード、IC カードを含む）がデバイスの認証開始トリガーに設定されます。 ※EDGEMATRIX Gatekeeperサービスでは顔認証以外の認証機能を提供していません。
サードパーティトリガー	デバイスの認証開始トリガーが端末画面の二回タップに設定されます。
自動トリガー	認証の自動起動を設定します。

3.3.4.1.6.4 一般設定

「一般」では、システム言語、音量、画面の明るさを設定できます。

オプション	説明
使用言語	デバイス操作画面の言語環境を設定できます。

オプション	説明
通知音	デバイスの通知音をオン/オフにできます。デフォルトはオンです。
ボリューム	通知音がオンの場合、音量を設定できます。
明るさ	デバイスの画面の明るさを設定できます。

3.3.4.1.6.5 顔識別設定

顔識別の設定では、規格の判断、使用シーン、検証方法、認証の繰り返し間隔の設定ができます。

グループ化	オプション	説明
高精度		デバイスがキャプチャーした写真の角度、ぼやけ、遮蔽の3項目を判断項目にするかを設定できます。
	高精度 オン/オフ	「高精度」をオン/オフにできます。デフォルトはオフです。オンの場合、角度、ぼやけ、かぶりの3方面から写真の規格を判断します。
	撮影角度制限	キャプチャした顔の角度を制限できます。デフォルトはオンです。
	あいまいさの識別の閾値	キャプチャした顔のぼやけを制限できます。デフォルトは 100% です。 数字を低くすればするほど、鮮明な画像が要求されます。高くするとぼやけの許容値が大きくなります。
	オクルージョン識別の閾値	キャプチャした顔の遮蔽を制限できます。デフォルトは 100% です。 <ul style="list-style-type: none"> ◇ ここでの遮蔽とは登録者が帽子をかぶっていたり、マスクをつけたりしている状態のことです。 ◇ 数字を低くすればするほど、遮蔽面積が小さな画像が要求されます。高くすると遮蔽の許容値が大きくなります。
識別モード		デバイスの識別モードを設定できます。「1:1 モード」、「1:N モード」、「モード」の3種類のモードがあります。デフォルトは「Mix モード」です。
	1:N モード	実際に撮影した顔を登録済みのすべての登録者と比較します。
	1:1 モード	実際に撮影した顔を対応する証明書の写真と比較します。
	Mix モード	「1:1 モード」と「1:N モード」の2種類の検証モードを同時にサポートします。

グループ化	オプション	説明
使用シーンの 選択		デバイスのプリセットまたはカスタムシーンを選択できます。「快速シーン」、「安全シーン」、「カスタムシーン」3種類のシーンがあります。 ◇ デフォルトで「快速シーン」が選択されています。
	快速シーン	生体認証はオフで、人の流れが比較的多いシーンに適しています。識別速度を効果的に向上できます。
	安全シーン	生体認証はオンで、比較的厳しい通行審査のシーンに適しています。安全性を効果的に向上できます。
	カスタマイズ シーン	「生体認証偽造防止パラメータ」、「1:N 認証比較パラメータ」、「1:1 認証比較パラメータ」を手動で設定します。

「シーンの選択」で「カスタマイズシーン」を選択した場合、引き続き以下のオプションを設定します。

グループ化	オプション	説明
生体検出 パラ メータ	生体検出用の 可視光閾値	可視光の条件下で生体認証を行います。生体認証のスコアが指定した閾値を超えると、認証成功です。 値が大きいほど、認証が厳しくなります。デフォルトは 50%です。
	生体検出用の 近赤外線閾値	近赤外線の条件下で生体認証を行います。生体認証のスコアが指定した閾値を超えると、認証成功です。 値が大きいほど、認証が厳しくなります。デフォルトは 50%です。
1:N モードパ ラメータ	認証閾値ライ ブラリの設定	登録者認証に使用する閾値ライブラリを設定できます。 ◇ 認証閾値ライブラリは事前に設定する必要があります。
	可視光閾値	可視光の条件下で顔識別を行います。写真比較の数値が指定した閾値を超えると、認証成功です。デフォルトは 80%です。
	近赤外線閾値	近赤外線の条件下で顔識別を行います。写真比較の数値が指定した閾値を超えると、認証成功です。デフォルトは 0%です。
1:1 モードパラ メータ	可視光閾値	「1:N モードパラメータ」の「可視光閾値」と同じ。デフォルトは 70%です。

認証の繰り返し間隔を設定すると、登録者が短時間に何度も認証されるのを防ぐことができます。値の範囲は 0~300 秒で、デフォルトは 0 です。

応用例：

例えば、「認証の繰り返し間隔」を3秒に設定すると、Aの顔スキャンが成功した後、以下の判断が行われます。

- 1) 過去3秒以内にAの顔スキャンの成功記録がない場合、「認証成功」と表示されます。
- 2) 過去3秒以内にAの顔スキャンの成功記録がある場合、「認証を繰り返さないでください」と表示されます。

3.3.4.1.6.6 温度測定設定

温度測定パラメータの設定では、温度測定を使用するシーンに関するパラメータを設定できます。

グループ化	パラメータ	説明
温度閾値	温度閾値	温度測定閾値で、測定温度が閾値を超えると、温度超過閾値の処理が起動します。
温度閾値を上回る時の処理	通行不可	温度が閾値を超えると、認証失敗、温度異常と表示され、通行が禁止されます。
	通行可	温度が閾値を超えると、イベントのみが記録され、通行は禁止されません。

3.3.4.1.6.7 アクセス制御信号設定

アクセス制御信号では、ウィーガンドプロトコルに準拠した通信信号です。ウィーガンド接続により、デバイスとサードパーティのアクセス制御を連動させ、通路のデバイスやドアのアクセス機能をコントロールできます。

- ◇ デバイスを他のウィーガンドプロトコル準拠機器と連携するための機能となります。
- ◇ デバイスマネージャがウィーガンドプロトコルの基本を理解した上で設定頂く必要があります。

オプション	説明
ウィーガンドタイプ	ウィーガンドタイプを設定できます：ウィーガンド26、ウィーガンド34、ウィーガンド36、ウィーガンド64、カスタムタイプ。 ウィーガンドタイプを「カスタムタイプ」に設定している場合、以下のオプションを設定する必要があります。
パリティ	ウィーガンド信号のエンコードにパリティを使用するか設定できます。

オプション	説明
総ビット	ウィーガンド信号の総ビットを設定できます。デフォルトの値は 26 です。
データビット	ウィーガンド信号のデータビットを設定できます。 「パリティ検査」がオフの場合：データビット = 総ビット 「パリティ検査」がオンの場合：データビット = 総ビット - 2
先頭の偶数パリティ	偶数パリティのデータビットを設定できます。
最後の奇数パリティ	奇数パリティのデータビットを設定できます。
パルス間隔	ウィーガンド信号のパルス間隔を設定できます。デフォルトの値は 1000us です。
パルス持続時間	ウィーガンド信号のパルス持続時間を設定できます。デフォルトの値は 100 us です。
認証カード番号のビット数	アクセス制御システムの物理カード番号のビット数を設定できます。 一般タイプのウィーガンドの値の範囲：16 ~ (「データビット」 - 2) カスタムタイプのウィーガンドの値の範囲： パリティ検査オン：16 ~ (「データビット」 - 2) パリティ検査オフ：16 ~ 「データビット」
1:1 カード番号がライブラリに存在しない	カード番号がライブラリに存在しない場合に出力されるウィーガンド信号のエンコードを設定できます。引き続き妥当性のある二次開発が行えます。 検証モードが「1:1 モード」または「混合モード」のシーンのみ。
1:1 認証失敗	カード番号はライブラリに存在するものの、認証に失敗した場合に出力されるウィーガンド信号のエンコードを設定できます。引き続き妥当性のある二次開発が行えます。 検証モードが「1:1 モード」または「混合モード」のシーンのみ。
1:1 認証成功	顔識別に成功した際に出力されるウィーガンド信号のエンコードを設定できます。引き続き妥当性のある二次開発が行えます。 検証モードが「1:1 モード」または「混合モード」のシーンのみ。
ドライ接点信号の時間	ドライ接点信号の出力時間を設定できます。 値の範囲：200~1000ms。デフォルト：300ms

3.3.4.1.6.8 カメラ設定

カメラ設定では、デバイスのカメラの照明効果、補助光の調節、認証距離、露出の調整を設定できます。

グループ化	パラメータ	説明
なし	待機中の明るさ	一般照明のシーンの補助光の明るさを設定できます。値が大きいほど、補助光が明るくなります。デフォルトは 3%です。
	識別中の明るさ	顔認証のシーンの補助光の明るさを設定できます。値が大きいほど、補助光が明るくなります。デフォルトは 100%です。
	識別中の照明時間	顔認証のシーンの補助光の照明時間を設定できます。値が大きいほど、補助光の照明時間が長くなります。デフォルトは 3 秒です。
	識別中の照明感度	近づいてくる登録者への補助光の照明感度を調整できます。値が小さいほど、感度が高くなります。デフォルトは 0%です。
	近赤外線補助光調整	近赤外線のシーンの近赤外線補助光の明るさを設定できます。値が大きいほど、近赤外線補助光が明るくなります。デフォルトは 100%です。
	識別距離	顔認証のシーンの顔とデバイスの距離を設定できます。デフォルトは 180cm です。
可視光カメラの露出設定	露出モード	可視光認証のシーンのカメラの露出モードを設定できます。「手動モード」と「自動モード」をサポートしています。デフォルトは「自動モード」です。
	マニュアル露出	可視光認証のシーンのカメラの露出補正を設定できます。値の範囲：-3、-2、-1、0、1、2、3 値が大きいほど露出が高くなり、画面が明るくなります。デフォルトは 0 です。
近赤外線カメラの露出調整	露出モード	近赤外線認証のシーンのカメラの露出モードを設定できます。「手動モード」、「自動モード」、「スマートモード」をサポートしています。デフォルトは「自動モード」です。
	手動露出	近赤外線認証のシーンのカメラの露出補正を設定できます。値の範囲：-3、-2、-1、0、1、2、3 値が大きいほど露出が高くなり、画面が明るくなります。デフォルトは 0 です。

3.3.4.1.6.9IC カード照合設定

※EDGEMATRIX Gatekeeper サービスでは IC カード/指紋関連機能を提供していません。

オプション	説明
許可リスト	身分証明書の比較をオン/オフにできます。
指紋	指紋の比較をオン/オフにできます。
指紋検証	「指紋」がオンの場合、指紋の検証方法を設定できます。「顔または指紋」と「顔と指紋」の2種類の方法があります。
IC カード指紋照合閾値	指紋認証がオンの場合、指紋の比較値が指定した閾値を超えると、認証成功になります。デフォルトは 600 です。

3.3.4.1.6.10 案内設定

案内設定では、認証成功、認証失敗、証明書を置くなど、デバイスのヒントの言語を設定できます。

オプション	説明
案内設定	<p>以下を含むプロンプトメッセージのタイプを設定できます。</p> <ol style="list-style-type: none"> 1) スマートプロンプト : プロンプトを設定すると、デバイスにプロンプトを表示し、また、TTS で音声に変換できます。 2) テキストと音声のプロンプト : プロンプトテキストと音声を設定します。 <ul style="list-style-type: none"> ◇ 開発機能の ODSL 機能を使用する場合は、「スマート案内」を選択する必要があります。 ◇ 「MP3 プロンプト」を設定する場合、デフォルトの音声を使用するか、カスタム音声をアップロードできます。 ◇ カスタム音声は、ウェブ管理機能ツールまたはデバイスでインポートできます。
テキストプロンプトスイッチ	<p>名前 : 認証結果に登録者の名前を表示するか設定できます。デフォルトは ON です。</p> <p>温度 : 認証結果に検温結果の温度を表示するか設定できます。デフォルトは ON です。</p>
音声プロンプトスイッチ	<p>検証成功の音声アナウンス : 認証成功時に音声を再生するか設定できます。デフォルトは ON です。</p> <p>検証失敗音声アナウンス : 認証失敗時に音声を再生するか設定できます。</p>
音声プロンプトオーディオ	<p>検証結果に再生する音声を設定できます。「デフォルト」と「カスタム」をサポートしています。「カスタム」の場合、音声をデバイスのウェブ管理機能ツールまたはデバイスでインポートできます。</p>

3.3.4.1.6.11 コンテンツ再生

コンテンツの再生では、スタンバイ画面の壁紙または動画を設定できます。

グループ化	オプション	説明
なし	表示モード	ディスプレイモードを「フェイスモード」または「再ネジモード」に設定できます。 デフォルトは「フェイスモード」です。
サイネージモードの設定	表示モードを「サイネージモード」に設定している場合、この項目のオプションを設定します。	
	案内情報表示	プロンプトメッセージを表示するか設定できます。デフォルトはオンです。
	識別丸区域の透明度	プロンプトメッセージの透明度を設定できます。デフォルトは 100 です。
	ウィンドウサイズ	識別ウィンドウのサイズを「小」、「中」、「大」と設定できます。
	待機文表示	スタンバイ中にメッセージを表示するか設定できます。デフォルトはオンです。
	待機時計表示	時間メッセージを表示するか設定できます。デフォルトはオンです。
フェイスモードの設定	表示イモードを「フェイスモード」に設定している場合、この項目のオプションを設定します。	
	待機文表示	スタンバイ中にメッセージを表示するか設定できます。デフォルトはオンです。
	待機時計表示	時間メッセージを表示するか設定できます。デフォルトはオンです。
スタンバイ中の表示メッセージ	1行目の待機文	デバイスのスタンバイ中に表示する「ようこそ」のメッセージを設定できます。最大で 20 文字、漢字は 10 文字まで表示できます。
	2行目の待機文	デバイスのスタンバイ中に表示するメッセージの 2 行目を設定できます。最大で半角 20 文字、全角 10 文字まで表示できます。デフォルトは空白で表示されません。
	待機文表示	スタンバイ中にメッセージを表示するか設定できます。デフォルトはオンです。

グループ化	オプション	説明
	待機時計表示	時間メッセージを表示するか設定できます。デフォルトはオンです。
待受壁紙	リピート再生	スタンバイ中に壁紙をリピート再生するか設定できます。デフォルトはオンです。
	再生時間	リピート再生がオンの時の再生時間を設定します。単位：秒。デフォルトは20です。
待受動画	リピート再生	スタンバイ中に壁紙をリピート再生するか設定できます。デフォルトはオンです。

3.3.4.1.6.12 システム更新

ソフトウェアのアップデートでは、デバイスが自動的にクラウド管理プラットフォームへ接続し、ソフトウェアバージョンをアップデートするか設定できます。デフォルトはオフです。

3.3.4.1.6.13 日付と時刻

日付と時刻では、デバイスで表示する時間の形式、タイムサーバーとの同期をオンにするか設定できます。

オプション	説明
日付の形式	デバイスで表示する時間の形式を設定できます。「MM-DD」、「MM月DD日」、「DD-MM」などの形式があり、デフォルトは「MM-DD」です。
タイムサーバーと同期	デバイスのタイムサーバーとの同期をオンにするか設定できます。デフォルトはオンです。

3.3.4.1.6.14 取り外しアラーム

取り外しアラームでは、デバイスの取り外しアラームをオンにするか設定できます。取り付け式デバイスが取り外された場合、警告音が鳴ります。

3.3.4.1.6.15 登録写真の最小サイズ

登録写真の最小サイズでは、デバイスが写真を受信する際に許可する最小ピクセルの基準を設定できます。登録写真の最小サイズには、「32×32」、「128×128」、「320×320」の3種類があります。デフォルトは「320×320」です。

3.3.4.1.6.16 識別記録

識別記録では、識別記録の保存と送信を設定でき、テスターが必要なテストデータを取得するのに役立ちます。

グループ化	オプション	説明
なし	テストモード	テストモードをオンにするか設定できます。オンにすると、テスターはテストファイルをエクスポートできます。
	赤外線写真	近赤外線写真をオンにするか設定できます。オンにすると、識別記録に近赤外線写真が含まれます。
	記録写真の解像度	保存する認証画像のサイズを設定します。デフォルトは「軽量」です。
識別記録送信	識別記録をサードパーティのインターフェースに送信する際の設定ができます。	
	識別記録送信	識別記録の送信をオンにするか設定できます。デフォルトはオフです。
	通信プロトコル	「識別記録の送信」がオンの場合、識別記録の送信に使用する通信プロトコルを表示できます。「WS」と「HTTP」をサポートしています。デフォルトはWSです。
	IP アドレス	「識別記録の送信」がオンの場合、送信先の IP アドレスを設定できます。
	ポート	「識別記録の送信」がオンの場合、送信先のポート番号を設定できます。
	アラートポート	「識別記録の送信」がオンの場合、アラートの送信先のポート番号を設定できます。

3.3.4.1.6.17 距離センサー設定

距離センサー設定では、デバイスで P-Sensor をオンにするかと有効時間を設定できます。

グループ化	オプション	説明
なし	P-Sensor オン/オフ	P-Sensor をオンにするか設定できます。

グループ化	オプション	説明
	有効時間	P-Sensor の有効時間を設定できます。「全期間」と「カスタム期間」があります。デフォルトは「全期間」です。
カスタム期間	「有効時間」で「カスタム期間」が設定されている場合、「期間の追加」をクリックし、以下のオプションを設定します。	
	名前	カスタム期間の名前を設定できます。
	週	カスタム期間の繰り返し周期を「週」単位で設定できます。
	時間	カスタム期間の開始/終了時間を設定できます。
	有効/無効	カスタム期間の有効期間または無効期間を設定できます。

3.3.4.1.6.18 デバイスのウェブ管理機能

デバイスのウェブ管理機能では、デバイスがパソコンまたはスマートフォンから管理画面へアクセスし、管理を行えるかどうか設定できます。

オプション	説明
ウェブ管理機能	ウェブ管理機能をオンにし、パソコンまたはスマートフォンから管理画面へアクセスしデバイスを管理できるようにするか設定できます。
通信プロトコル	パソコンまたはスマートフォンから管理画面へアクセスする際に使用する通信プロトコルを設定できます。「http」と「https」があり、デフォルトは「http」です。

3.3.4.1.7 遠隔解錠

クラウド管理プラットフォームからセキュリティゲートと連携されているデバイスに対して開錠信号を送送することができます。

ステップ1 **アクセス手順**：左側メニュー→デバイス管理→デバイス管理

ステップ2 「デバイス管理」画面で、指定するデバイスを検索して表示させます。

✧ オンラインのデバイスをしか操作できません。

ステップ3 デバイスリストで、「操作」列の「ドアオープン」をクリックし、遠隔解錠を実施します。

3.3.4.2 デバイスグループ

デバイスのグループ化では、アクティベートされているデバイスをグループ化でき、管理やメンテナンスに役立ちます。

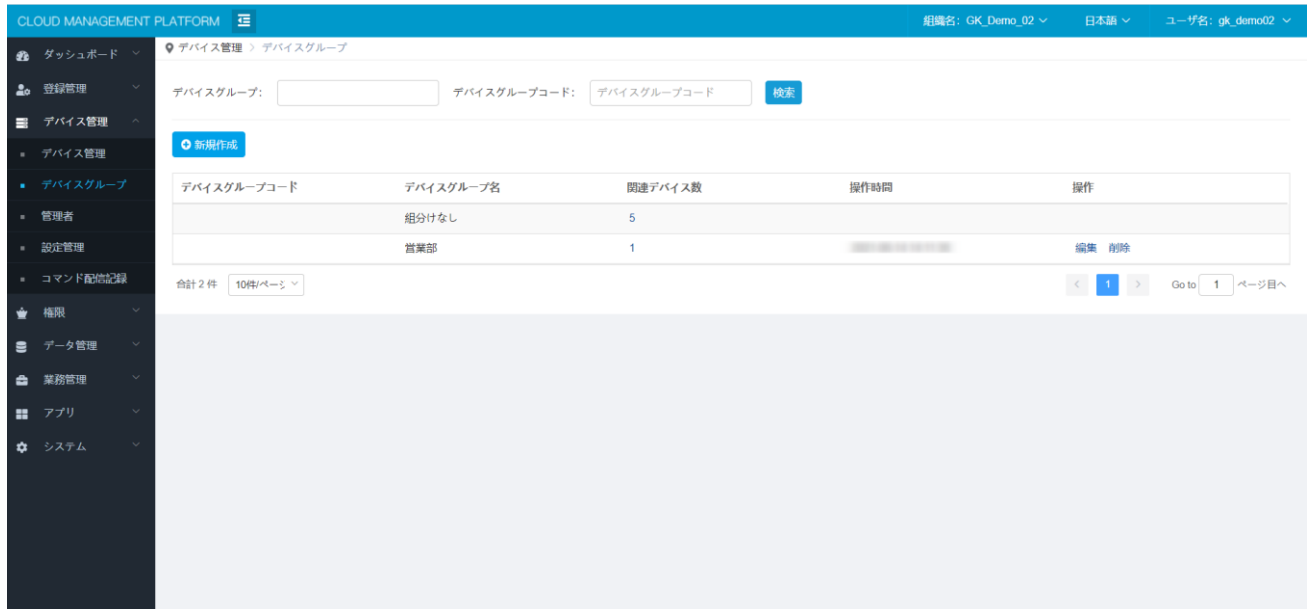


図 32 デバイスグループ

3.3.4.2.1 デバイスグループの確認

ステップ1 アクセス手順：左側メニュー→デバイス管理→デバイスグループ

「デバイスグループ」画面を開き、登録済のデバイスグループリストを確認します。

デバイスグループの情報：デバイスグループコード、デバイスグループ名、関連デバイス数、操作時間。

ステップ2 「デバイスグループ」画面：

- 1) 「デバイスグループ」のキーワードを入力し、「検索」をクリックすると、指定した名称のデバイスグループを検索できます。
- 2) 「デバイスグループコード」を入力し、「検索」をクリックすると、指定したコードのデバイスグループを確認できます。

ステップ3 デバイスグループリストで、「関連付けられているデバイス数」列の数字をクリックすると、「デバイスグループのデバイスを確認する」ダイアログが表示され、指定したデバイスグループに関連付けられているデバイス情報を確認できます。

デバイス情報：デバイス名、シリアル番号、タイプ、状態、バージョン番号、管理者。

3.3.4.2.2 デバイスグループの追加

ステップ1 アクセス手順：左側メニュー→デバイス管理→デバイスグループ

ステップ2 「デバイスグループ」画面で、「デバイスグループの追加」をクリックすると、「デバイスグループの追加」ダイアログが開きます。

ステップ3 「デバイスグループの追加」ダイアログで、デバイスグループ情報を入力します。

オプション	説明
デバイスグループ	デバイスグループの名前を設定できます。最大 64 文字まで入力できます。
デバイスのグループコード	デバイスグループのコードを設定できます。最大 20 文字まで入力できます。
関連付けられているデバイス	<p>デバイスとデバイスグループ間の関連付けを設定できます。</p> <p>設定について：</p> <ol style="list-style-type: none"> 1) 左側の「グループ化されていないデバイス」リストでデバイスを検索して 1 つまたは複数のデバイスを選択し、「>」矢印をクリックすると、右側の「追加済のデバイス」リストに移動し、指定したデバイスとデバイスグループが関連付けられます。 2) 右側の「追加済のデバイス」リストでデバイスを検索して 1 つまたは複数のデバイスを選択し、「<」矢印をクリックすると、左側の「グループ化されていないデバイス」リストに移動し、指定したデバイスとデバイスグループの関連付けが解除されます。 <ul style="list-style-type: none"> ☆ 1つのデバイスに1つのデバイスグループのみを関連付けることができます。

ステップ4 「OK」をクリックし、設定を保存します。

3.3.4.2.3 デバイスグループの編集

ステップ1 アクセス手順：左側メニュー→デバイス管理→デバイスグループ

ステップ2 「デバイスグループ」画面で、デバイスグループを検索し指定します。

ステップ3 デバイスグループリストで、「操作」列の「編集」をクリックすると、「デバイスグループの編集」ダイアログが開きます。

ステップ4 「デバイスグループの編集」ダイアログで、デバイスグループの情報を入力します。

3.3.4.2.4 デバイスグループの削除

ステップ1 アクセス手順：左側メニュー→デバイス管理→デバイスグループ

ステップ2 「デバイスグループ」画面で、デバイスグループを検索し指定します。

ステップ3 デバイスグループリストで、「操作」列の「削除」をクリックすると、指定したデバイスグループが削除されます。

- ◇ デバイスグループの削除では、デバイスグループのみが削除され、デバイスグループと関連付けられたデバイスは削除されません。
- ◇ デバイスグループを削除すると、デバイスグループに関連付けられていたデバイスが、グループ化されていないデバイスに復元されます。

3.3.4.3 管理者

管理者画面では、デバイスの管理者、デバイスの関連付けを設定し、デバイスへ送信できます。

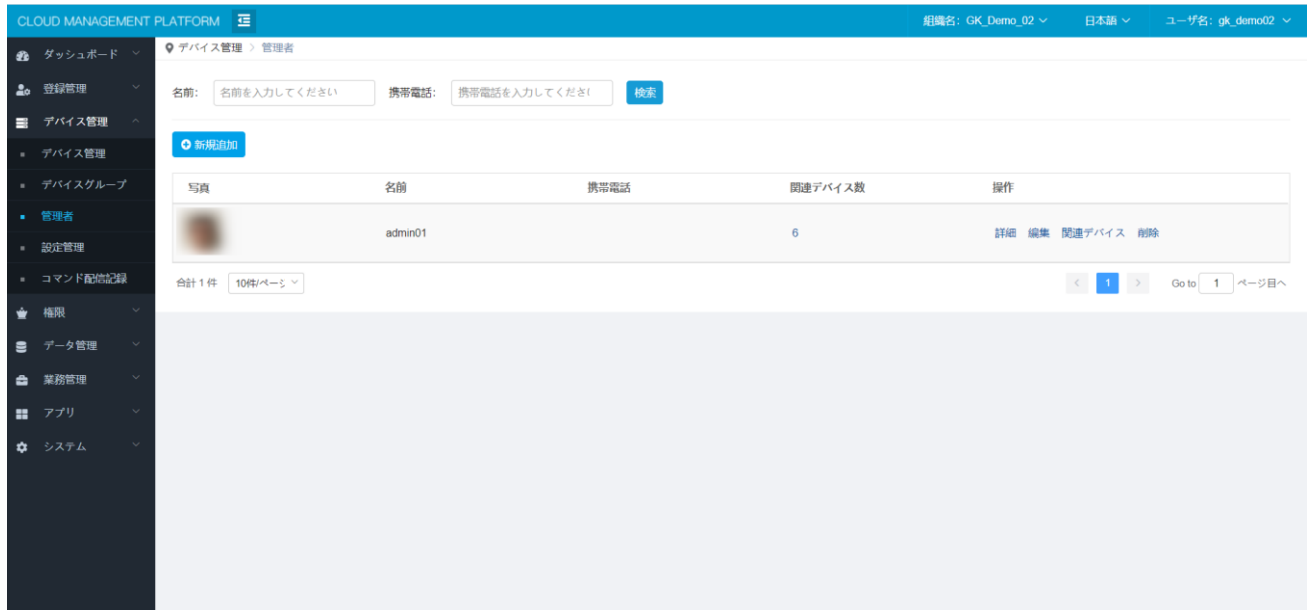


図 33 管理者

3.3.4.3.1 管理者の確認

ステップ1 アクセス手順：左側メニュー→デバイス管理→管理者

「管理者」画面が開き、登録済の管理者リストを確認できます。

管理者の情報：写真、管理者名、携帯電話番号、関連付けられているデバイス数。

ステップ2 「管理者」画面：

- 1) 「管理者名」のキーワードを入力し、「検索」をクリックすると、指定した名前の管理者をあいまい検索できます。
- 2) 「携帯電話番号」を入力し、「検索」をクリックすると、指定した携帯電話番号の管理者を確認できます。

ステップ3 管理者リストで、「関連付けられているデバイス数」列の数字をクリックすると、「管理者のデバイス確認」ダイアログが表示され、指定した管理者に関連付けられているデバイス情報を確認できます。

デバイス情報：デバイス名、シリアル番号、タイプ、状態、デバイスグループ、パー

ジョン番号。

ステップ4 「管理者」画面で、「操作」列の「詳細」をクリックすると、「管理者の確認」ダイアログが表示され、管理者の情報を確認できます。

管理者の情報：管理者名、パスワード、携帯電話番号、写真。

3.3.4.3.2 管理者の追加

ステップ1 アクセス手順：左側メニュー→デバイス管理→管理者

ステップ2 「管理者」画面で、「管理者の追加」をクリックすると、「管理者の追加」ダイアログが開きます。

ステップ3 「管理者の追加」ダイアログで、管理者の情報を入力します。

オプション	説明
管理者名	管理者名を設定できます。
パスワード	管理者がデバイスにログインする数字4桁のパスワードを設定できます。
携帯電話番号	管理者の携帯電話番号を設定できます。
写真	管理者の証明写真を設定できます。
デフォルト管理者	管理者をデフォルト管理者にするか設定できます。 ☆ クラウドサービスモードのデバイスをアクティベートすると、クラウド管理プラットフォームが、デフォルト管理者をデバイスの管理者として自動的に送信します。 ☆ クラウド管理プラットフォームでは、最大10名のデフォルト管理者を設定できます。

ステップ4 「OK」をクリックし、設定を保存します。

3.3.4.3.3 管理者の編集

ステップ1 アクセス手順：左側メニュー→デバイス管理→管理者

ステップ2 「管理者」画面で、指定する管理者を検索して表示させます。

ステップ3 管理者リストで、「操作」列の「編集」をクリックすると、「管理者の編集」ダイアログが開きます。

ステップ4 「管理者の編集」ダイアログで、管理者の情報を入力します。

ステップ5 「OK」をクリックし、設定を保存します。

3.3.4.3.4 管理者の削除



☆ 管理者を削除すると復元できません。慎重に操作してください。

ステップ1 アクセス手順：左側メニュー→デバイス管理→管理者

ステップ2 「管理者」画面で、指定する管理者を検索して表示させます。

ステップ3 管理者リストで、「操作」列の「削除」をクリックすると、削除確認ダイアログが開きます。

ステップ4 削除確認ダイアログで、「OK」をクリックすると、指定した管理者が削除されます。

3.3.4.3.5 関連付けられているデバイス

ステップ1 アクセス手順：左側メニュー→デバイス管理→管理者

ステップ2 「管理者」画面で、指定する管理者を検索して表示させます。

ステップ3 管理者リストで、「操作」列の「関連付けられているデバイス」をクリックすると、「関連付けられているデバイス」ダイアログが開きます。

ステップ4 「関連付けられているデバイス」ダイアログで、指定するデバイスを検索して表示させます。

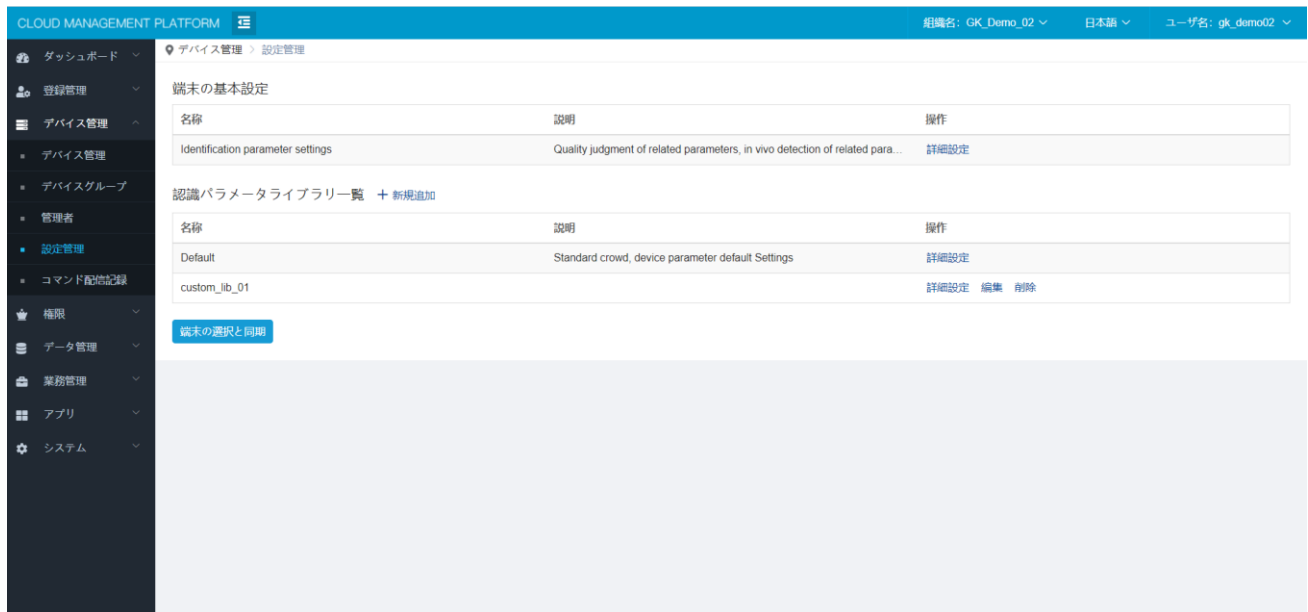
ステップ5 デバイスリスト：

- 1) 「デバイス名」の前にあるチェックボックスをオンにすると、デバイスが関連付けられます。
- 2) 「デバイス名」の前にあるチェックボックスをオフにすると、デバイスの関連付けが解除されます。

ステップ6 「関連付けられているデバイス」をクリックすると、設定が保存されます。

3.3.4.4 設定管理

管理設定画面では、デバイスの基本パラメータ、認証閾値ライブラリとそのパラメータを設定し、デバイスと同期できます。



認証閾値ライブラリでは、デバイスで登録者の顔認証を行う時に使用する登録者ライブラリを指定できます。例：

A、B、C、3つの認証閾値ライブラリがあり、それぞれの閾値が90、80、70に設定され、デバイスが30人を追加。その内、Aに属する者が10人、Bに属する者が10人、Cに属する者が10人である。

例：太郎さんがデバイスの前で1:N認証を行う場合のプロセスは以下のとおりです。

- 1) 太郎さんとAライブラリの10人を比較してスコアを付け、最高スコアがa、89点。
- 2) 太郎さんとBライブラリの10人を比較してスコアを付け、最高スコアがb、88点。
- 3) 太郎さんとCライブラリの10人を比較してスコアを付け、最高スコアがc、87点。
- 4) スコアの高い順は、 $a > b > c$ であるため、比較順序はa、b、cに決定されます。
- 5) $a < 90$ 、比較失敗。
- 6) $b > 80$ 、比較成功。そのため、太郎さんはbであると判定されます。

3.3.4.4.1 デバイスの設定管理

ステップ1 アクセス手順：左側メニュー→デバイス管理→設定管理

ステップ2 「管理設定」画面の「端末の基本設定」領域にあるリストで、「操作」列の「詳細設定」をクリックすると、「認識パラメータの設定」ダイアログが開きます。

ステップ3 「認識パラメータの設定」ダイアログで、パラメータの値を設定します。

グループ化	オプション	説明
高精度		デバイスがキャプチャーした写真の角度、ぼやけ、遮蔽の3項目を判断項目にするかを設定できます。

グループ化	オプション	説明
	高精度 オン/オフ	「高精度」をオン/オフにできます。デフォルトはオフです。 オンの場合、角度、ぼやけ、かぶりの3方面から写真の規格を判断します。
	撮影角度制限	キャプチャした顔の角度を制限できます。デフォルトはオンです。
	あいまいさの識別の閾値	キャプチャした顔のぼやけを制限できます。デフォルトは 100% です。 数字を低くすればするほど、鮮明な画像が要求されます。高くするとぼやけの許容値が大きくなります。
	オクルージョン識別の閾値	キャプチャした顔の遮蔽を制限できます。デフォルトは 100% です。 <ul style="list-style-type: none"> ◇ ここでの遮蔽とは登録者が帽子をかぶっていたり、マスクをつけたりしている状態のことです。 ◇ 数字を低くすればするほど、遮蔽面積が小さな画像が要求されます。高くすると遮蔽の許容値が大きくなります。
識別モード	デバイスの識別モードを設定できます。「1:1 モード」、「1:N モード」、「モード」の3種類のモードがあります。デフォルトは「Mix モード」です。	
	1:N モード	実際に撮影した顔を登録済みのすべての登録者と比較します。
	1:1 モード	実際に撮影した顔を対応する証明書の写真と比較します。
	Mix モード	「1:1 モード」と「1:N モード」の2種類の検証モードを同時にサポートします。
使用シーンの選択	デバイスのプリセットまたはカスタムシーンを選択できます。「快速シーン」、「安全シーン」、「カスタムシーン」3種類のシーンがあります。 <ul style="list-style-type: none"> ◇ デフォルトで「快速シーン」が選択されています。 	
	快速シーン	生体認証はオフで、人の流れが比較的多いシーンに適しています。識別速度を効果的に向上できます。
	安全シーン	生体認証はオンで、比較的厳しい通行審査のシーンに適しています。安全性を効果的に向上できます。
	カスタマイズシーン	「生体認証偽造防止パラメータ」、「1:N 認証比較パラメータ」、「1:1 認証比較パラメータ」を手動で設定します。

グループ化	オプション	説明
高精度		デバイスがキャプチャーした写真の角度、ぼやけ、遮蔽の3項目を判断項目にするかを設定できます。
	高精度 オン/オフ	「高精度」をオン/オフにできます。デフォルトはオフです。オンの場合、角度、ぼやけ、かぶりの3方面から写真の規格を判断します。
	撮影角度制限	キャプチャした顔の角度を制限できます。デフォルトはオンです。
	あいまいさの識別の閾値	キャプチャした顔のぼやけを制限できます。デフォルトは100%です。 数字を低くすればするほど、鮮明な画像が要求されます。高くするとぼやけの許容値が大きくなります。
	オクルージョン識別の閾値	キャプチャした顔の遮蔽を制限できます。デフォルトは100%です。 <ul style="list-style-type: none"> ◇ ここでの遮蔽とは登録者が帽子をかぶっていたり、マスクをつけたりしている状態のことです。 ◇ 数字を低くすればするほど、遮蔽面積が小さな画像が要求されます。高くすると遮蔽の許容値が大きくなります。
識別モード		デバイスの識別モードを設定できます。「1:1 モード」、「1:N モード」、「モード」の3種類のモードがあります。デフォルトは「Mix モード」です。
	1:N モード	実際に撮影した顔を登録済みのすべての登録者と比較します。
	1:1 モード	実際に撮影した顔を対応する証明書の写真と比較します。
	Mix モード	「1:1 モード」と「1:N モード」の2種類の検証モードを同時にサポートします。
使用シーンの選択		デバイスのプリセットまたはカスタムシーンを選択できます。「快速シーン」、「安全シーン」、「カスタムシーン」3種類のシーンがあります。 <ul style="list-style-type: none"> ◇ デフォルトで「快速シーン」が選択されています。
	快速シーン	生体認証はオフで、人の流れが比較的多いシーンに適しています。識別速度を効果的に向上できます。
	安全シーン	生体認証はオンで、比較的厳しい通行審査のシーンに適しています。安全性を効果的に向上できます。
	カスタマイズ	「生体認証偽造防止パラメータ」、「1:N 認証比較パラメータ」、

グループ化	オプション	説明
	シーン	「1:1 認証比較パラメータ」を手動で設定します。

ステップ4 「OK」をクリックし、設定を保存します。

3.3.4.4.2 認証閾値ライブラリの追加

ステップ1 **アクセス手順**：左側メニュー→デバイス管理→設定管理

ステップ2 「管理設定」画面の「認識パラメータライブラリー一覧」領域で、「新規追加」をクリックすると、「認識パラメータライブラリの新規追加」ダイアログが開きます。

ステップ3 「認識パラメータライブラリの新規追加」ダイアログで、閾値ライブラリの情報を入力します。

オプション	説明
ライブラリ名	閾値ライブラリ名を設定できます。
説明	閾値ライブラリの説明情報を追加できます。

ステップ4 「OK」をクリックし、設定を保存します。

3.3.4.4.3 認識パラメータライブラリの編集

ステップ1 クラウド管理プラットフォームの左側のリストで、「デバイス」>「管理設定」をクリックすると、「管理設定」画面が開きます。

ステップ2 「管理設定」画面の「認証閾値ライブラリリスト」領域にあるリストで、「操作」列の「編集」をクリックすると、指定した認証閾値ライブラリの「認証閾値ライブラリの編集」ダイアログが表示されます。

ステップ3 「認証閾値ライブラリの編集」ダイアログで、認証閾値ライブラリの情報を入力します。

ステップ4 「OK」をクリックし、設定を保存します。

3.3.4.4.4 認証閾値ライブラリの削除

ステップ1 **アクセス手順**：左側メニュー→デバイス管理→設定管理

ステップ2 「管理設定」画面の「認証閾値ライブラリリスト」領域にあるリストで、「操作」列の「削除」をクリックすると、削除確認ダイアログが開きます。

ステップ3 削除確認ダイアログで、「OK」をクリックすると、指定した認証閾値ライブラリが削除されます。

- ◇ 認証閾値ライブラリは削除すると復元できません。慎重に操作してください。

3.3.4.4.5 認証閾値ライブラリのパラメータ設定

ステップ1 アクセス手順：左側メニュー→デバイス管理→設定管理

ステップ2 「管理設定」画面の「認識パラメータライブラリー一覧」領域にあるリストで、「操作」列の「詳細設定」をクリックすると、指定した認証閾値ライブラリの「パラメータライブラリの設定」ダイアログが表示されます。

ステップ3 「パラメータライブラリの設定」ダイアログで、設定情報を入力します。

オプション	説明
可視光閾値	可視光の条件下で顔認証を行います。写真比較の数値が指定した閾値を超えると、認証成功です。デフォルトは80%です。
近赤外線閾値	近赤外線の条件下で顔認証を行います。写真比較の数値が指定した閾値を超えると、認証成功です。デフォルトは0%です。

ステップ4 「OK」をクリックし、設定を保存します。

3.3.4.4.6 デバイス設定の同期

ステップ1 アクセス手順：左側メニュー→デバイス管理→設定管理

ステップ2 「管理設定」画面で、「端末の選択と同期」をクリックすると、「端末の選択と同期」ダイアログが開きます。

ステップ3 「端末の選択と同期」ダイアログで、指定するデバイスを検索して表示させます。

ステップ4 デバイスリストで、「デバイス名」の前にあるチェックボックスをオンにします。

ステップ5 「同期を確定」をクリックすると、クラウド管理プラットフォームの「認識パラメータライブラリー一覧」が指定されたデバイスに同期されます。

3.3.4.5 コマンド配信記録

記録の送信画面では、データ、設定、ルール、アプリを含む、クラウド管理プラットフォームがデバイスに送信した設定情報の履歴を確認できます。

CLOUD MANAGEMENT PLATFORM

組織名: GK_Demo_02 日本語 ユーザー名: gk_demo02

デバイス管理 > コマンド配信記録

シリアル番号: コマンド: 状態: 時間: -

シリアル番号	コマンド	コマンドID	状態	配信時刻	アプリID	オペレーター	操作
	ドアオープン	1623647203000000003	実行成功		bbox-service		詳細
	ドアオープン	1623647203000000002	実行成功		bbox-service		詳細
	ドアオープン	1623647203000000001	実行成功		bbox-service		詳細
	設定アップロード	1623646303000000001	実行成功		bbox-service		詳細
	設定アップロード	1623646303000000002	実行成功		bbox-service		詳細
	設定アップロード	1623646303000000001	実行成功		bbox-service		詳細
	設定アップロード	1623639103000000001	実行成功		bbox-service		詳細
	設定アップロード	1623638203000000001	実行成功		bbox-service		詳細
	設定アップロード	1623394303000000001	実行成功		bbox-service		詳細
	設定アップロード	1623394303000000003	実行成功		bbox-service		詳細

合計 1008 件 ... ページ目へ

図 34 コマンド配信記録

3.3.4.5.1 送信記録の確認

ステップ1 **アクセス手順**：左側メニュー→デバイス管理→コマンド配信記録

「コマンド配信記録」画面が開き、送信記録リストを確認できます。

送信記録の情報：シリアル番号、コマンド、コマンド ID、状態、配信時間、アプリ ID、操作者。

ステップ2 「コマンド配信記録」画面：

- 1) 「シリアル番号」を入力し、「検索」をクリックすると、指定したデバイスの送信記録を確認できます。
- 2) 「コマンド」を入力し、「検索」をクリックすると、指定した送信コマンドの送信記録を確認できます。
- 3) 「開始日」と「終了日」を入力すると、指定した期間の送信記録を確認できます。

ステップ3 指定する送信記録を検索して表示させ、送信記録リスト「操作」列にある「詳細」をクリックすると、「送信記録の詳細」ダイアログが開き、指定した送信記録の詳細情報を確認できます。

詳細情報：指定された名前、コマンド ID、シリアル番号、アプリ ID、データダウンロードアドレス、フィードバック処理アドレス、状態、操作者、送信時間、待ち行列時間、発信時間、到着時間、コマンド実行開始時間、コマンド完了時間。

3.3.5 権限

権限の管理では、ロールの設定に基づき、クラウド管理プラットフォームの使用権限を管理できます。

3.3.5.1 ロール管理

ロールの管理画面では、メイン管理者のアカウントでクラウド管理プラットフォームにログインし、実際のシーンに基づき、プラットフォームの管理者アカウントのロールを管理できます。

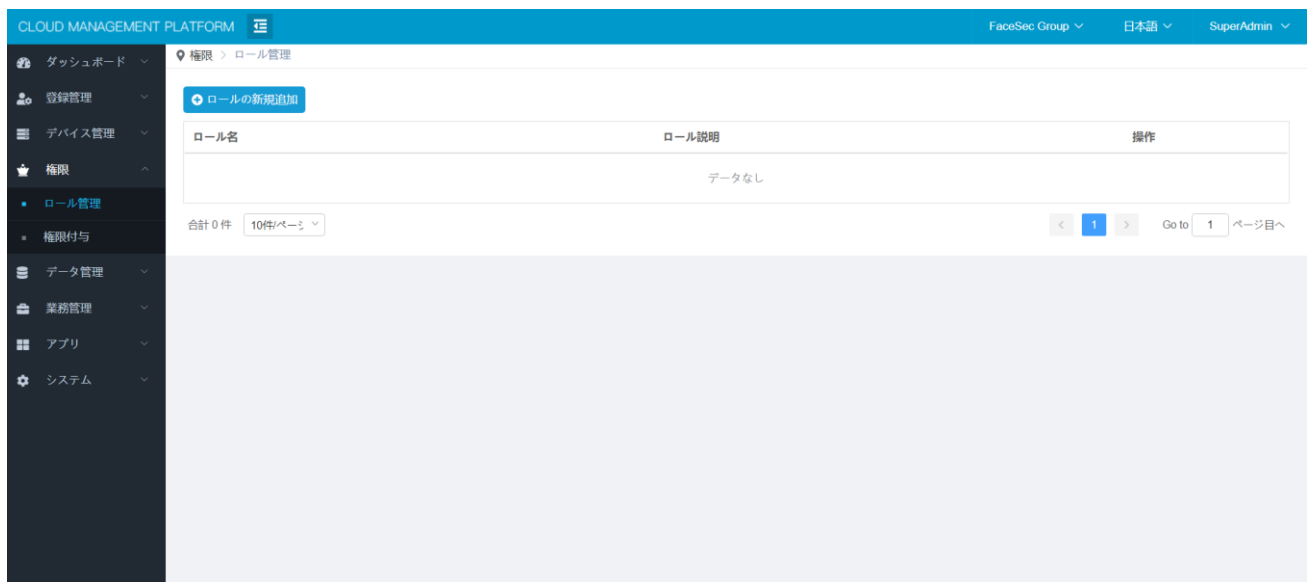


図 35 ロール管理

3.3.5.1.1 ロールの確認

ステップ1 **アクセス手順**：左側メニュー→権限→ロール管理

「ロール管理」画面が開き、ロールリストを確認できます。

ロール情報：ロール名、ロールの説明。

ステップ2 「ロールの管理」画面で、ロールリストの「操作」列にある「詳細」をクリックすると、指定したロールの「ロールの詳細」ダイアログが開きます。

ロールの詳細：ロール名、ロールの説明、プラットフォームの権限、データの権限（登録者データ、デバイスデータ、アプリデータ）。

3.3.5.1.2 ロールの追加

ステップ1 **アクセス手順**：左側メニュー→権限→ロール管理

ステップ2 「ロールの管理」画面で、「ロールの追加」をクリックすると、「ロールの追加」ダイアログが開きます。

ステップ3 「ロールの追加」ダイアログで、ロールの情報を入力します。

オプション	説明
ロール名	ロール名を設定できます。
ロールの説明	ロールの説明情報を追加できます。
データの権限	<p>ロールの登録者データ、デバイスデータ、アプリデータに関するアクセス権限を設定できます。</p> <p>登録者データのアクセス権限は設定済の組織に基づいて設定します。</p> <p>デバイスデータのアクセス権限は設定済のデバイスグループに基づいて設定します。</p> <p>◇ 新しいロールでは設定済のデータ権限項目を選択できます。現在の操作者がもつデータの権限より強くなることはありません。プラットフォーム/アプリ権限も同様です。</p>
プラットフォームの権限	<p>ロールのクラウド管理プラットフォームに関するアクセス権限を設定できます。</p> <p>◇ 「デバイス」の下にある「オンライン承認」権限は、「デバイス承認アシスタント」を介してのみデバイスのオンライン承認ができます。</p>
アプリ管理	ロールのアプリの管理権限を設定できます。

ステップ4 「OK」をクリックし、設定を保存します。

3.3.5.1.3 ロールの編集

◇ 操作者は自分のロールを変更できません。

ステップ1 **アクセス手順**：左側メニュー→権限→ロール管理

ステップ2 「ロールの管理」画面で、ロールリストにある「操作」列の「編集」をクリックすると、指定したロールの「ロールの編集」ダイアログが開きます。

ステップ3 「ロールの編集」ダイアログで、ロールの情報を変更します。

ステップ4 「OK」をクリックし、設定を保存します。

3.3.5.1.4 ロールの削除



◇ 操作者は自分のロールを削除できません。
 ◇ ロールを一度削除すると復元できません。慎重に操作してください。

ステップ1 **アクセス手順**：左側メニュー→権限→ロール管理

ステップ2 「ロールの管理」画面で、ロールリストにある「操作」列の「削除」をクリックすると、削除確認ダイアログが開きます。

ステップ3 「OK」をクリックすると、指定したロールが削除されます。

- ◇ ロールに関連付けられた登録者がいる場合、ロールを削除すると、登録者のアカウントは保持されますが、ロールに関連付けられた権限は削除されません。
- ◇ ロールが関連付けられていない登録者のアカウントでログインすると、ログイン失敗と表示されます。

3.3.5.2 権限付与

アカウントの管理画面では、登録済のプラットフォーム管理者アカウントでクラウド管理プラットフォームにログインし、実際のシーンに基づき、プラットフォームの管理者アカウントを管理できます。その権限は関連付けられたロールにより決定されます。



図 36 権限付与

3.3.5.2.1 アカウントの検索

ステップ1 アクセス手順：左側メニュー→権限→権限付与

「権限付与」画面が開き、クラウド管理プラットフォームの管理者アカウントリストを確認できます。

表示情報：名前、携帯電話、メールアドレス、ロール、操作。

- ◇ メイン管理者のロールはリストに表示されません。

ステップ2 「権限付与」画面：

- 1) 「名前」を入力し、「検索」をクリックすると、指定した名前の登録者のアカウント

トを確認できます。

- 2) 「携帯電話番号」を選択し、「検索」をクリックすると、指定した登録済携帯電話番号と一致するアカウントを確認できます。
- 3) 「メールアドレス」を選択し、「検索」をクリックすると、指定した登録済メールアドレスと一致するアカウントを確認できます。

ステップ3 アカウントリスト「操作」列の「詳細」をクリックすると、指定したアカウントの「アカウントの詳細」ダイアログが開きます。

アカウントの詳細：アカウント、ユーザー、ロール、作成者、状態、責任者、メールアドレス、携帯電話番号。

3.3.5.2.2 アカウントの追加

前提条件：操作者には登録者の管理権限、デバイスの管理権限、データ、プラットフォーム、アプリの管理権限が必要です。

- ✧ スマートフォンで登録した管理者は、携帯電話番号をもつ登録者のアカウントのみ追加できます。
- ✧ メールアドレスで登録した管理者は、メールアドレスをもつ登録者のアカウントのみ追加できます。
- ✧ 登録者のアカウントは繰り返し追加できません。
- ✧ メイン管理者のアカウントは追加できません。

ステップ1 **アクセス手順：左側メニュー→権限→権限付与**

ステップ2 「アカウントの管理」画面で、「アカウントの追加」をクリックすると、「アカウントの追加」ダイアログが開きます。

ステップ3 「アカウントの追加」ダイアログで、アカウント情報を入力します。

オプション	説明
登録者	ユーザーはクラウドプラットフォーム管理者のアカウントを設定します。名前を入力して組織内の登録者を検索し選択します。
ロール	アカウントが属するロールを設定できます。ロールは事前に設定する必要があります。

ステップ4 「OK」をクリックし、設定を保存します。

3.3.5.2.3 アカウントの編集

- ◇ 操作者は自分のアカウントを編集できません。

- ステップ1 **アクセス手順：左側メニュー→権限→権限付与**
- ステップ2 「アカウントの管理」画面で、アカウントリストにある「操作」列の「編集」をクリックすると、指定したアカウントの「アカウントの編集」ダイアログが表示されます。
- ステップ3 「アカウントの編集」ダイアログで、アカウント情報を変更します。
- ステップ4 「OK」をクリックし、設定を保存します。

- ◇ メイン管理者のアカウントは編集できません。

3.3.5.2.4 アカウントの削除



- ◇ 操作者は自分のロールを削除できません。
- ◇ アカウントは一度削除すると復元できません。慎重に操作してください。
- ◇ メイン管理者のアカウントは削除できません。

- ステップ1 **アクセス手順：左側メニュー→権限→権限付与**
- ステップ2 「アカウントの管理」画面で、ロールリストにある「操作」列の「削除」をクリックすると、削除確認ダイアログが開きます。
- ステップ3 「今すぐ削除」をクリックすると、指定したアカウントが削除されます。

3.3.6 データ管理

記録の管理では、デバイスがアップロードした認識記録を確認・管理できます。

3.3.6.1 認識記録

認識記録画面では、デバイスがクラウド管理プラットフォームにアップロードした認識記録を確認・管理できます。

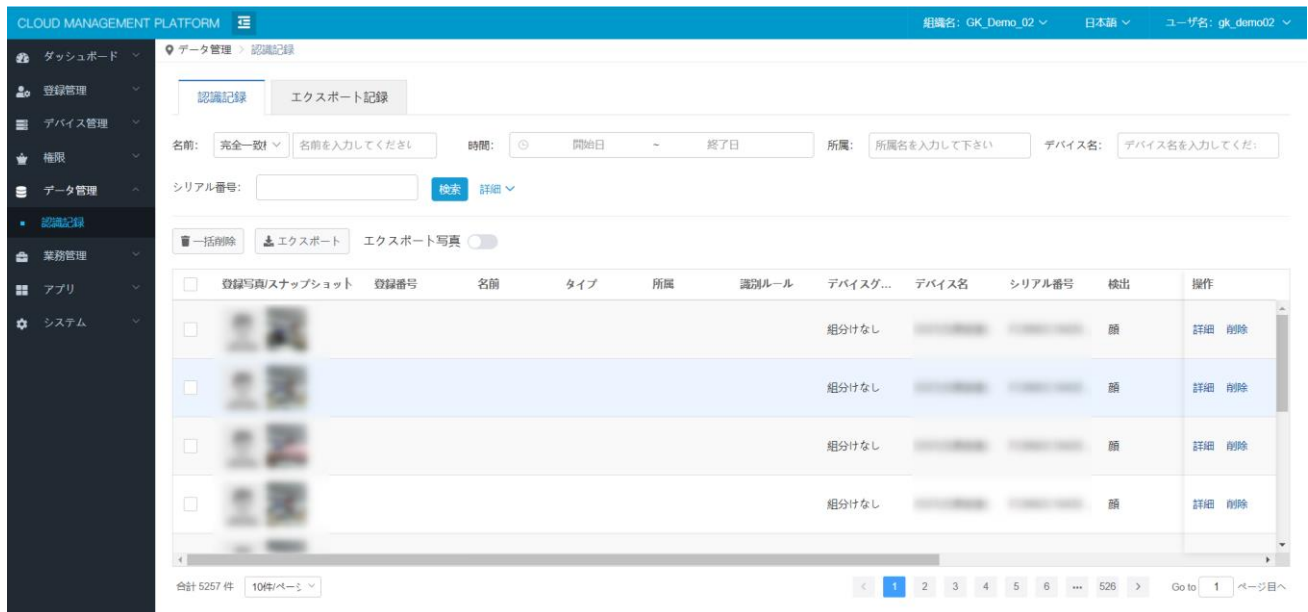


図 37 認識記録

3.3.6.1.1 認識記録の確認

ステップ1 **アクセス手順：左側メニュー→データ管理→認識記録**

デフォルトで「認識記録」画面が開き、デバイスがアップロードした認識記録リストを確認できます。

認識記録情報：登録写真、スナップ写真、登録者番号、名前、登録者タイプ、所属組織、識別ルール、デバイスグループ、デバイス名、シリアル番号、認証方法、認証結果、比較スコア、時間。

ステップ2 「認識記録」画面：

- 1) 「詳細」をクリックすると、すべてのフィルタリング項目が表示されます。「折りたたむ」をクリックすると、よく使用するフィルタリング項目が表示されます。
- 2) 「名前」を入力し、「完全一致」または「あいまい検索」を設定して、「検索」をクリックすると、指定した名前の登録者の認識記録を完全一致/あいまい検索できます。
- 3) 「開始日」と「終了日」を入力し、「検索」をクリックすると、指定した期間の認識記録を確認できます。
- 4) 「所属組織」を入力し、「検索」をクリックすると、指定した組織に属する登録者の認識記録を確認できます。
- 5) 「デバイス名」を入力し、「検索」をクリックすると、指定した名前のデバイスがアップロードした認識記録をあいまい検索できます。
- 6) 「シリアル番号」を入力し、「検索」をクリックすると、指定したシリアル番号の

デバイスがアップロードした認識記録を確認できます。

- 7) 「登録者番号」を入力し、「検索」をクリックすると、指定した登録者番号の登録者の認識記録を確認できます。
- 8) 「認証ルール」を入力し、「検索」をクリックすると、指定した認証ルールの認識記録を確認できます。
- 9) 「認証結果」を選択し、「検索」をクリックすると、指定した結果の認識記録を確認できます。
- 10) 「デバイスグループ」を選択し、「検索」をクリックすると、指定したデバイスグループがアップロードした認識記録を確認できます。デバイスグループは事前に設定する必要があります。
- 11) 「登録者タイプ」を選択し、「検索」をクリックすると、指定した結果の認識記録を確認できます。

ステップ3 指定する認識記録を検索して表示させ、認識記録リストにある「操作」列の「詳細」をクリックすると、指定した認識記録の「認識記録の詳細」ダイアログが開きます。

3.3.6.1.2 認識記録のエクスポート

ステップ1 **アクセス手順：左側メニュー→データ管理→識別記録**

ステップ2 「認識記録」画面で、指定する認識記録を検索して表示させます。

- ◇ フィルタリング条件が設定されていない場合、デフォルトですべての認識記録がエクスポートされます。

ステップ3 「エクスポート」をクリックすると、認識記録がエクスポートされます。

- ◇ 一度に最大2万件の認識記録をエクスポートできます。

3.3.6.1.3 認識記録の削除

ステップ1 **アクセス手順：左側メニュー→データ管理→識別記録**

ステップ2 「認識記録」画面で、指定する認識記録を検索して表示させます。

ステップ3 認識記録リストで、「操作」列にある「削除」をクリックすると、削除確認ダイアログが開きます。

ステップ4 「OK」をクリックすると、指定した認識記録が削除されます。

- ◇ 認識記録は削除すると復元できません。慎重に操作してください。

3.3.6.1.4 認識記録の一括削除



◇ 認識記録は削除すると復元できません。慎重に操作してください。

- ステップ1 **アクセス手順**：左側メニュー→データ管理→識別記録
- ステップ2 「認識記録」画面で、指定する認識記録を検索して表示させます。
- ステップ3 認識記録リストで、認識記録の前にあるチェックボックスを1つまたは複数選択します。
- ステップ4 「一括削除」をクリックすると、削除確認ダイアログが開きます。
- ステップ5 「OK」をクリックすると、指定した認識記録が削除されます。

3.3.6.1.5 記録のエクスポート履歴の確認

- ステップ1 **アクセス手順**：左側メニュー→データ管理→識別記録→エクスポート記録
- 「記録のエクスポート」画面が開き、認識記録のエクスポートリストを確認できます。
 記録のエクスポート情報：エクスポートファイル名、エクスポートアカウント。
- ステップ2 「記録のエクスポート」画面：
- 1) リストにある「操作」列の「ダウンロード」をクリックすると、指定した認識記録のエクスポートファイルがダウンロードされます。
 - 2) リストにある「操作」列の「削除」をクリックすると、削除確認ダイアログが開き、「OK」をクリックすると、指定した認識記録のエクスポートファイルが削除されます。

3.3.7 業務管理

ルールの管理では、認証ルールを設定・管理し、登録者情報と関連付けられた認証ルールをデバイスに送信できます。

3.3.7.1 通行規則

通行規則(認証ルール)画面では、認証ルールを設定・管理でき、指定された登録者は指定時間内に指定の方法でデバイスを通過します。

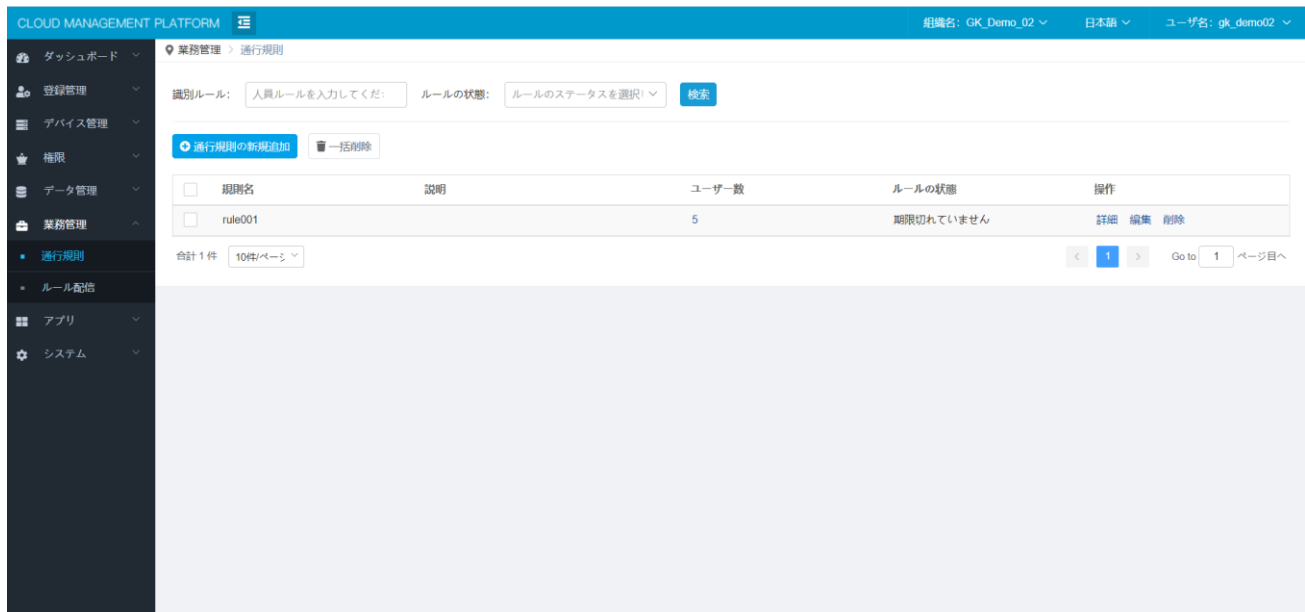


図 38 通行規則

3.3.7.1.1 通行規則の確認

ステップ1 **アクセス手順**：左側メニュー→業務管理→通行規則

「通行規則」画面が開き、通行規則リストを確認できます。

通行規則情報：規則名、説明、ユーザー数、ルールの状態。

ステップ2 「通行規則」画面：

- 1) 「識別ルール」を入力し、「検索」をクリックすると、指定した名前の通行規則を確認できます。
- 2) 「ルールの状態」を選択し、「検索」をクリックすると、指定した状態の認証ルールを確認できます。

ステップ3 指定する通行規則を検索して表示させ、通行規則リストにある「操作」列の「詳細」をクリックすると、指定した通行規則の「通行規則の詳細」ダイアログが開きます。

通行規則の詳細：規則名、説明、通行方式、時間規則、適用単位。

3.3.7.1.2 通行規則の追加

ステップ1 **アクセス手順**：左側メニュー→業務管理→通行規則

ステップ2 「通行規則」画面で、「通行規則の新規追加」をクリックすると、「通行規則の新規追加」ダイアログが開きます。

ステップ3 「通行規則の新規追加」ダイアログに通行規則情報を入力します。

オプション	説明
規則名	規則の名前を設定できます。
説明	規則の説明情報を追加できます。
通行方式	<p>認証方法を指定できます。顔、顔+ID カード、顔+パスポート、顔+アクセスカード、顔+IC カード、QR コード、顔+パスワード、IC カード、指紋があります。</p> <p>※EDGEMATRIX Gatekeeper サービスでは「顔」以外の認証機能を提供していません</p> <ul style="list-style-type: none"> ◇ デフォルトでは「顔」のチェックボックスがオンになっています。 ◇ 「顔」のチェックボックスがオンになっている場合、補助認証方法で「QR コード」と「顔+パスワード」は選択できません。 ◇ 「パスワード」は数字 4 桁のアクセス認証パスワードです。
時間規則	規則の有効期間を設定できます。
適用単位	規則が適用される単位を設定できます。

ステップ4 「OK」をクリックし、設定を保存します。

3.3.7.1.3 時間規則の追加

前提条件：3.3.7.1.2 通行規則の追加

ステップ1 「通行規則の追加」ダイアログで、「+時間規則」をクリックすると、「時間規則の新規追加」画面が開きます。

ステップ2 「時間規則の新規追加」画面に時間規則の情報を入力します。

オプション	説明
名前	時間規則の名前を設定できます。
日付	時間規則の有効期間を設定できます。
曜日	時間規則を有効にする曜日を設定できます。
時間	時間規則を有効にする時間を設定できます。
通行方法	時間規則何にアクセスを許可するか設定できます。

ステップ3 「OK」をクリックし、設定を保存します。

3.3.7.1.4 適用単位

前提条件：3.3.7.1.2 通行規則の追加

ステップ1 「通行子息」ダイアログ：

1) 「適用単位」を「人員単位で配信」に設定すると、登録者のチェックボックスが表示されます。

登録者は事前に設定する必要があります。

2) 「適用単位」を「組織単位で配信」に設定すると、組織のチェックボックスが表示されます。

組織は事前に設定する必要があります。

ステップ2 「すべての登録者/組織」リストで、指定する登録者/組織を検索して表示させます。

ステップ3 登録者/組織名の前にあるチェックボックスをオンにし、矢印をクリックすると、指定した登録者/組織が「選択中の登録者/組織」リストに移動します。

ステップ4 「OK」をクリックし、設定を保存します。

◇ 組織ごとの通行規則を送信した後で組織に登録者を追加した場合、追加された登録者は組織の通行規則に従います。

3.3.7.1.5 通行規則の編集

ステップ1 **アクセス手順：左側メニュー→業務管理→通行規則**

ステップ2 「通行規則」画面で、指定する通行規則を検索して表示させます。

ステップ3 通行規則リストで、「操作」列にある「編集」をクリックすると、指定した通行規則の「通行規則の編集」ダイアログが開きます。

ステップ4 「通行規則の編集」ダイアログで、通行規則情報を変更します。

ステップ5 「OK」をクリックし、設定を保存します。

3.3.7.1.6 通行規則の削除

ステップ1 **アクセス手順：左側メニュー→業務管理→通行規則**

ステップ2 「通行規則」画面で、指定する通行規則を検索して表示させます。

ステップ3 通行規則リストで、「操作」列にある「削除」をクリックすると、削除確認ダイアログが開きます。

ステップ4 「削除」をクリックすると、指定した通行規則が削除されます。

3.3.7.1.7 通行規則の一括削除

ステップ1 **アクセス手順：左側メニュー→業務管理→通行規則**

ステップ2 「通行規則」画面で、指定する通行規則を検索して表示させます。

ステップ3 通行規則リストで、通行規則の前にあるチェックボックスを1つまたは複数選択します。

ステップ4 「一括削除」をクリックすると、削除確認ダイアログが開きます。

ステップ5 「削除」をクリックすると、指定した1つまたは複数の通行規則が削除されます。

3.3.7.2 ルール配信

ルール配信画面では、設定した通行規則を指定のデバイスに適用できます。

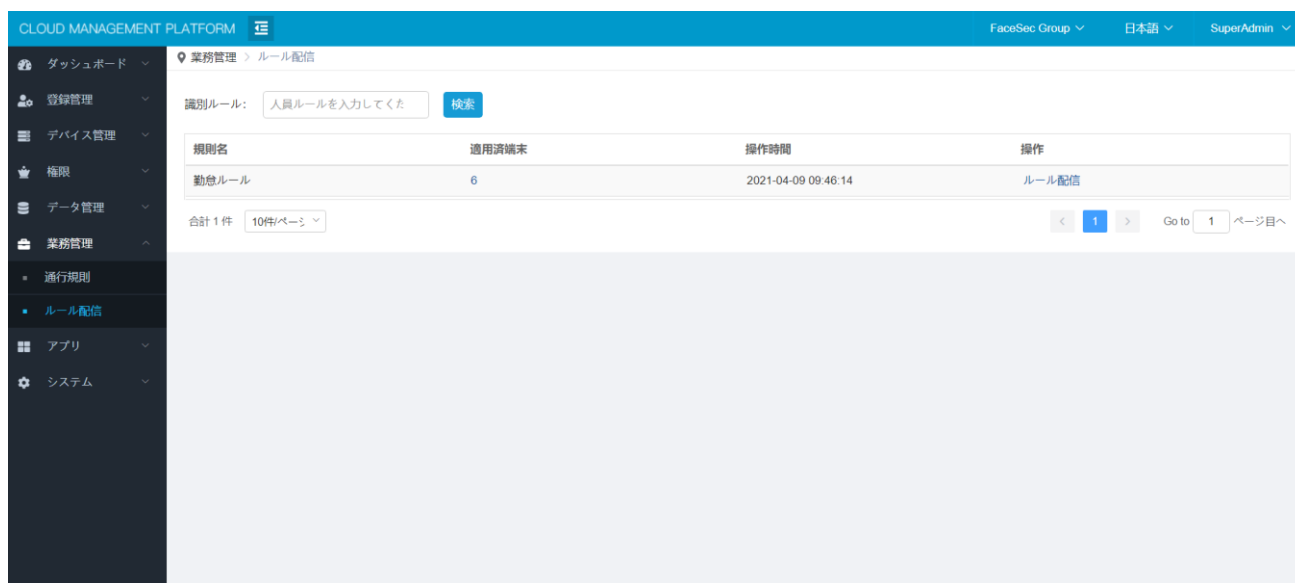


図 39 ルール配信

3.3.7.2.1 通行規則の送信

- ステップ1 **アクセス手順**：左側メニュー→業務管理→ルール配信
- ステップ2 「ルール配信」画面で、指定する通行規則を検索して表示させます。
- ステップ3 通行規則リストで、「操作」リストの「ルール配信」をクリックすると、「ルール配信」ダイアログが開きます。
- ステップ4 「ルール配信」ダイアログの「すべてのデバイス」リストから、指定するデバイスを検索して表示させ、チェックボックスを1つまたは複数選択します。
- ステップ5 矢印をクリックすると、指定した1つまたは複数のデバイスが、「選択中のデバイス」リストに追加されます。
- ステップ6 「OK」をクリックすると、通行規則および関連付けられた登録者が指定のデバイスに送信されます。
通行規則は事前に設定する必要があります。

3.3.8 アプリ

アプリの管理では、サードパーティアプリとの連携の承認を管理できます。

アプリの管理では、アクセス者の管理、メッセージ送信、自己登録アプリを設定できます。

3.3.8.1 アプリ管理

アプリ管理画面では、サードパーティアプリ開発者のプラットフォームに基づいたアプリの作成、プラットフォームとのデータの連携の設定ができます。

図 40 アプリ管理

3.3.8.1.1 アプリの確認

ステップ1 アクセス手順：左側メニュー→アプリ→アプリ管理

「アプリ管理」画面が開き、アプリのリストを確認できます。

アプリの情報：アプリ名、アプリ ID、Secure_Key、Push_key、作成時間、状態。

ステップ2 「アプリ管理」画面：

- 1) 「アプリ名」を入力し、「検索」をクリックすると、指定した名前のアプリをあいまい検索できます。
- 2) 「アプリ ID」を入力し、「検索」をクリックすると、指定した ID のアプリを確認できます。

ステップ3 検索条件を指定し、指定するアプリを検索して表示させます。

ステップ4 アプリリストで、「操作」列の「詳細」をクリックすると、指定したアプリの「詳細」画面が開きます。

3.3.8.1.2 アプリの作成

ステップ1 アクセス手順：左側メニュー→アプリ→アプリ管理

ステップ2 「アプリ管理」画面で、「アプリ ID を作成」をクリックすると、「アプリ ID を作成」画面が開きます。

ステップ3 「アプリ ID を作成」画面で、アプリ情報を入力します。

オプション	説明
アプリ ID	アプリの ID を設定し、アプリを一意に識別できます。 このオプションは、以下 2 種類の方法で設定できます： <ol style="list-style-type: none"> 1) 「作成」をクリックすると、アプリ ID が自動的に作成されます。 2) 文字列を入力し、アプリ ID をカスタマイズします。
アプリ名	アプリの名前を設定できます。
ダッシュボードに追加	ダッシュボードに追加かどうか設定できます。 ※EDGEMATRIX Gatekeeper サービスではアプリのダッシュボード登録機能を提供していません。「いいえ」をお選びください。
ジャンプ先	アプリのアクセスアドレスを設定できます。

オプション	説明
	<p>「ダッシュボードに追加」が「はい」に設定されている場合、「ジャンプ先」を指定する必要があります。</p> <p>※EDGEMATRIX Gatekeeper サービスではアプリのダッシュボード登録機能を提供しておりません。「いいえ」をお選びください。</p>
Secure_key	<p>Secure_key を設定できます。サードパーティのアプリがクラウド管理プラットフォームインターフェースを呼び出す時、appid と Secure_key を介してトークンを取得します。</p> <p>このオプションでは、自動作成とカスタムの2種類の設定方法を使用できます。</p>
Push_key	<p>プッシュ通知サービスのKeyを設定できます。サードパーティのアプリは、appid と Push_key を介し、クラウド管理プラットフォームからプッシュ通知される情報を受信します。</p> <p>このオプションでは、自動作成とカスタムの2種類の設定方法を使用できます。</p>
アドレスのプッシュ通知	<p>プッシュ通知アドレスを設定し、指定した「イベントタイプのプッシュ通知」の情報をそのアドレスにプッシュ通知できます。</p> <p>「Push_key」を設定している場合、「アドレスのプッシュ通知」を設定する必要があります。</p>
イベントタイプのプッシュ通知	<p>プッシュ通知するイベントのタイプを設定できます。</p>

ステップ4 「テスト」をクリックし、「ジャンプ先」または「アドレスのプッシュ通知」が使用可能かテストします。

ステップ5 「OK」をクリックし、設定を保存します。

3.3.8.1.3 イベントの説明

グループ化	イベント	説明
認識記録イベント	認識記録を追加	デバイスを介して登録者のアクセス認証が行われ、認識記録が追加されると作成されます。
登録者イベント	新規追加	デバイスまたはクラウド管理プラットフォームを介して、アクセス者が追加されると作成されます。
	人員を更新	デバイスまたはクラウド管理プラットフォームを介して、アクセス者がアップデートされると作成されます。
	人員プロフィール	デバイスまたはクラウド管理プラットフォームを介し

グループ化	イベント	説明
	を削除	て、アクセス者が削除されると作成されます。
通行規則イベント	規則を新規追加	デバイスまたはクラウド管理プラットフォームを介して、アクセスルールが追加されると作成されます。
	規則更新	デバイスまたはクラウド管理プラットフォームを介して、アクセスルールがアップデートされると作成されます。
	規則削除	デバイスまたはクラウド管理プラットフォームを介して、アクセスルールが削除されると作成されます。
デバイスイベント	デバイス情報更新	デバイスのアクティベートが完了すると作成されます。
	デバイスネットワークキング	デバイスがネットワークに接続されると作成されます。
	デバイスが切断されました	デバイスがネットワークから切断されると作成されます。
	出荷時状態にリセット	デバイスまたはクラウド管理プラットフォームを介して、デバイスが工場出荷状態に戻されると作成されます。
権限イベント	組織を新規追加	クラウド管理プラットフォームを介して、組織が追加された時に作成されます。
	組織を更新	クラウド管理プラットフォームを介して、組織が変更された時に作成されます。
	組織を削除	クラウド管理プラットフォームを介して、組織が削除された時に作成されます。

3.3.8.1.4 アプリの編集

ステップ1 **アクセス手順**：左側メニュー→アプリ→アプリ管理

ステップ2 「アプリ管理」画面で、指定するアプリを検索して表示させます。

ステップ3 アプリリストで、「操作」列の「編集」をクリックすると、指定したアプリの「アプリの編集」ダイアログが開きます。

ステップ4 「アプリの編集」ダイアログで、アプリの情報を変更します。

ステップ5 「OK」をクリックし、設定を保存します。

3.3.8.1.5 アプリの無効化

ステップ1 アクセス手順：左側メニュー→アプリ→アプリ管理

ステップ2 「アプリ管理」画面で、指定するアプリを検索して表示させます。

ステップ3 アプリリストで、「操作」列の「無効/有効」をクリックすると、指定したアプリを無効/有効にできます。

◇ 無効状態のアプリにはアクセスできません。

3.3.8.1.6 アプリの削除



◇ アプリを削除すると復元できません。慎重に操作してください。

ステップ1 アクセス手順：左側メニュー→アプリ→アプリ管理

ステップ2 「アプリ管理」画面で、指定するアプリを検索して表示させます。

ステップ3 アプリリストで、「操作」列の「削除」をクリックすると、削除確認ダイアログが開きます。

ステップ4 削除確認ダイアログで、「削除」をクリックすると、指定したアプリが削除されます。

3.3.8.1.7 トークンの削除

ステップ1 アクセス手順：左側メニュー→アプリ→アプリ管理

ステップ2 「アプリ管理」画面で、指定するアプリを検索して表示させます。

ステップ3 アプリリストで、「操作」列の「トークン」をクリックすると、「トークンを作成」ダイアログが開き、自動的に作成されたトークンとその有効期限が表示されます。

◇ トークンの有効期限は 30 分です。期限切れ後は手動で更新できます。

ステップ4 「トークンの作成」ダイアログ：

- 1) 「リフレッシュ」をクリックして、トークンを更新します。
- 2) 「コピー」をクリックして、トークンをコピーします。

3.3.9 システムの管理

設定画面では、認識記録のアーカイブ、登録者のアカウントの管理、メイン管理者の変更など、本システムの維持管理ができます。

3.3.9.1 システムアーカイブ

システムのアーカイブ画面では、システムログをダウンロードできます。



図 41 システムアーカイブ

3.3.9.1.1 認識記録のアーカイブ

ステップ1 アクセス手順：左側メニュー→システム→システムアーカイブ

ステップ2 「新しいアーカイブ」ダイアログで、アーカイブの「開始時間」と「終了時間」を設定します。

「アーカイブデータ」、「アーカイブデータの推定容量」、「推定ディスク容量」に、指定したアーカイブ時間内の関連データ量が表示されます。

◇ 1回の操作で最大2万件のデータをアーカイブできます。

ステップ3 「OK」をクリックすると、指定したアーカイブ時間内の認識記録がアーカイブされます。

ステップ4 「システムアーカイブ」画面に戻ると、アーカイブリストでアーカイブタスクを確認できます。

1) 「操作」列の「ダウンロード」をクリックすると、アーカイブファイルをダウンロードできます。

2) 「操作」列の「削除」をクリックすると、アーカイブファイルを削除できます。



◇ アーカイブされた認識記録は7日後に自動的に削除されます。

3.3.9.2 アカウント

登録者のアカウント画面では、現在のアカウントの登録タイプを確認できます。携帯電話番号登録とメールアドレス登録に分かれています。登録招待を自動的に送信するか設定できます。



図 42 アカウント

3.3.9.2.1 自動登録招待のオン/オフ

ステップ1 アクセス手順：左側メニュー→システム→アカウント

ステップ2 「登録者のアカウント」画面で、「登録招待を自動的に送信」のスイッチをクリックすると、送信をオンまたはオフにできます。

3.3.9.3 メインアカウント

メインアカウント画面では、メイン管理者の登録情報を変更できます。

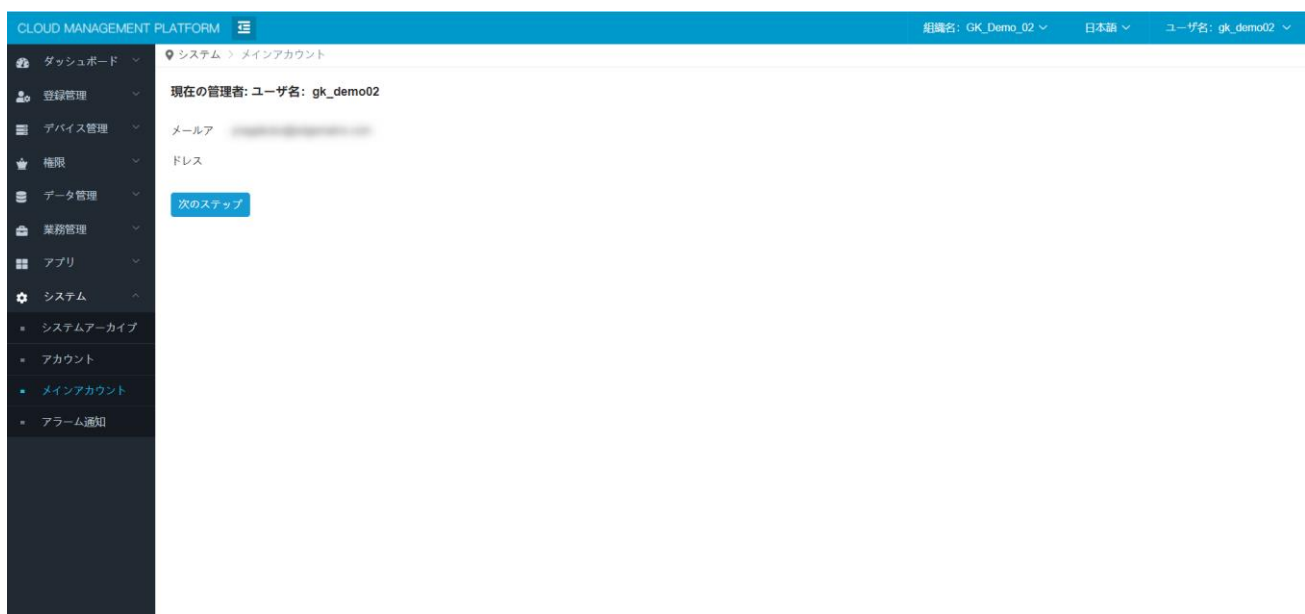


図 43 メインアカウント

3.3.9.3.1 メイン管理者の変更

ステップ1 アクセス手順：左側メニュー→システム→メインアカウント

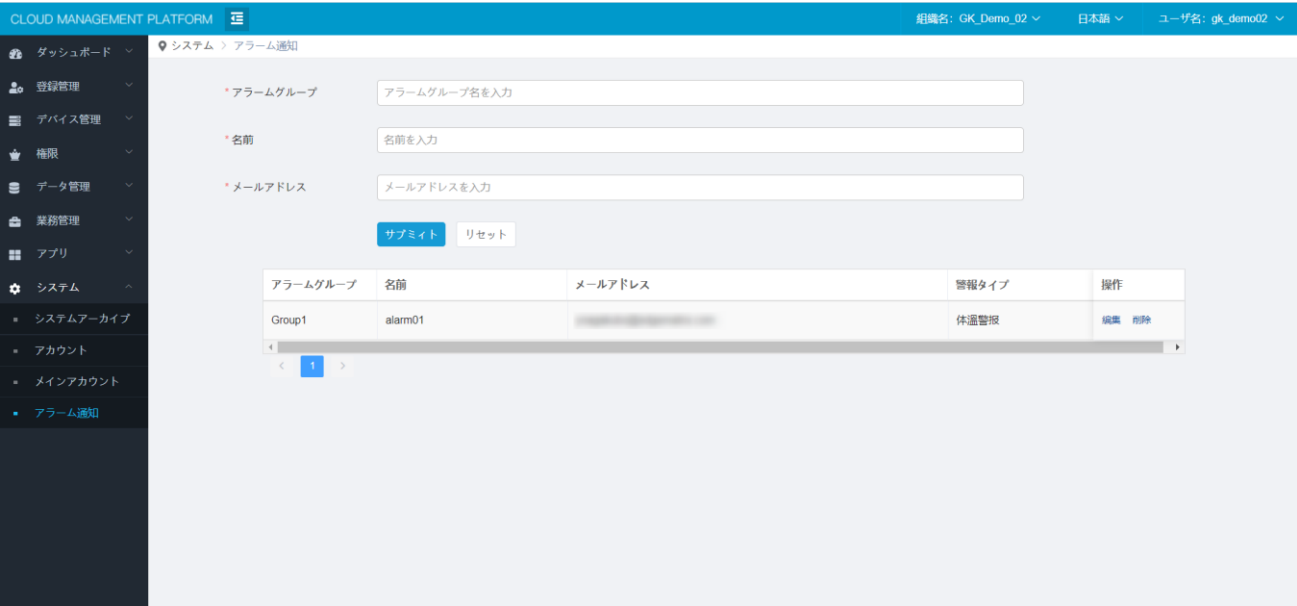
ステップ2 変更画面：

- 1) 「認証コードの取得」をクリックし、メイン管理者のアカウントを認証します。認証完了後、「次へ」をクリックすると、メイン管理者の設定画面に進みます。
- 2) 名前を入力し、組織に所属する登録者を検索して選択します。
- 3) 「認証コードの取得」をクリックし、認証コードを取得します。
- 4) 受信した認証コードを入力し、新規アカウントを認証します。

「確定変更」をクリックすると、メイン管理者の変更が完了します。

3.3.9.4 アラーム通知

アラーム通知画面では、アラームが発生した時に、事前に登録した送信先にアラームを送信します。



The screenshot shows the 'Alarm Notification' page in the Cloud Management Platform. The page has a blue header with 'CLOUD MANAGEMENT PLATFORM' and user information. A left sidebar contains a navigation menu with 'Alarm Notification' selected. The main content area contains a form with three input fields: 'Alarm Group Name', 'Name', and 'Email Address'. Below the form are 'Submit' and 'Reset' buttons. A table below the form lists existing alarm groups.

アラームグループ	名前	メールアドレス	警報タイプ	操作
Group1	alarm01		体温警報	編集 削除

☆ 現在では、測温アラームのみを対応します。

3.3.9.4.1 アラーム通知の登録

ステップ1 アクセス手順：左側メニュー→システム→アラーム通知

ステップ2 アラームグループ、名前、メールアドレスを入力します。

ステップ3 サブミットをクリックし、アラーム通知先を登録します。

3.3.9.4.2 アラーム通知の編集

ステップ1 **アクセス手順**：左側メニュー→システム→アラーム通知

ステップ2 アラーム通知先のリストから、編集する通知先の右側の「編集」をクリックします。

ステップ3 編集画面で、登録情報を編集します。

ステップ4 サブミットをクリックし、編集した情報を反映します。

3.3.9.4.3 アラーム通知の削除

ステップ1 **アクセス手順**：左側メニュー→システム→アラーム通知

ステップ2 アラーム通知先のリストから、削除する通知先の右側の「削除」をクリックします。

ステップ3 該当アラーム通知先を削除します。

4 インタラクティブ

4.1 認証

デバイスが認証対象を捉え、顔またはその他検証方法で認証を行った結果の確認方法を記載します。

4.1.1 スタンバイ状態

- 1) スタンバイ画面未設定：システムのデフォルトスタンバイ画面が表示されます。
- 2) スタンバイ画面設定済：設定に従い情報が画面に表示されます。スタンバイ画像または動画が再生されます。



4.1.2 認証プロセス

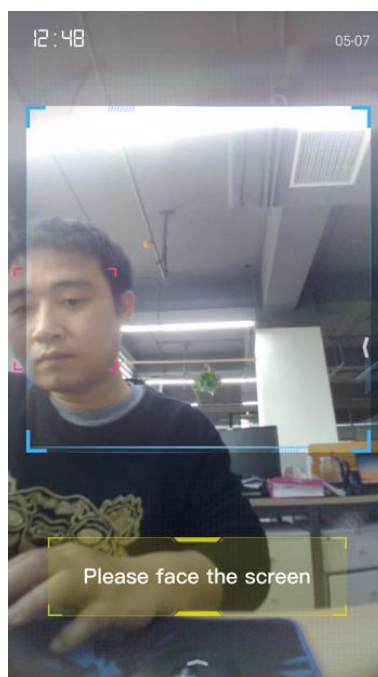
1) 識別中、少々お待ちください：

テスターの顔が正面を向いているか、タップタッチスクリーンを3回タップした場合、認証画面が開き、以下のプロンプトメッセージが表示されます：認証中、しばらくお待ちください…。



2) スクリーンに向かってください：

顔が正面を向いていない、顔認証の質がよくない、非生体の顔を認証した場合、認証画面に以下のプロンプトメッセージが表示されます：スクリーンに向かってください



4.1.3 認証結果

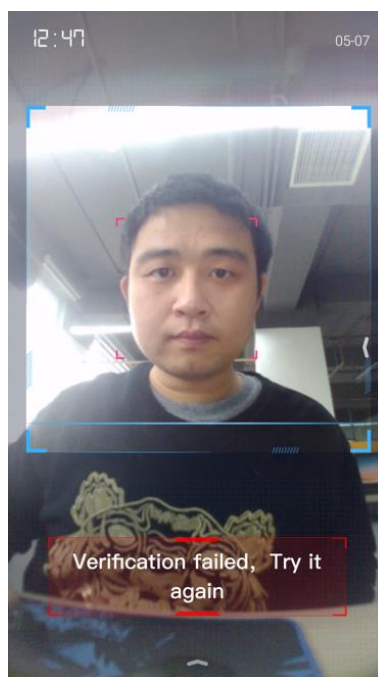
1) 認証成功 :

指定された検証方法で、認証に合格した場合、認証画面に以下のプロンプトメッセージが表示されます : XXX、こんにちは。



2) 認証失敗 :

指定された検証方法で、テスターが認証に合格しなかった場合、認証画面に以下のプロンプトメッセージが表示されます : 認証失敗。もう一度やりなおしてください。



4.2 温度測定

「温度測定」、「温度測定+顔認証」モードがオンの状態で、テスターがデバイスを通過すると、顔スキャン方式で測定/確認され、認証結果が表示されます。

4.2.1 温度測定プロセス

1) 温度測定機能オフ：

デバイスが温度測定カメラに接続されていないまたは温度測定に関する機能の権限がない場合、以下のプロンプトメッセージが表示されます：*IT カメラが見つかりません。*



2) 顔が温度測定エリア内がない場合：

テスターの顔が温度測定エリア内がない場合、認証画面に以下のプロンプトメッセージが表示されます：**正面を向いて温度測定をやり直してください。**



4.2.2 認証結果

4.2.2.1 温度測定モード

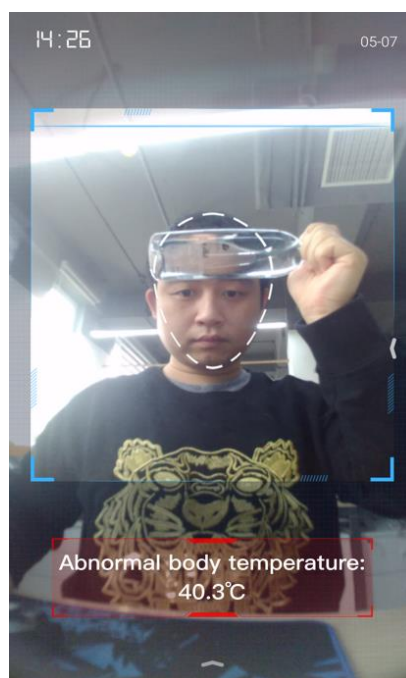
1) 正常温度：

テストターの温度が正常な場合、認証画面に以下のプロンプトメッセージが表示されます：温度



2) 異常温度：

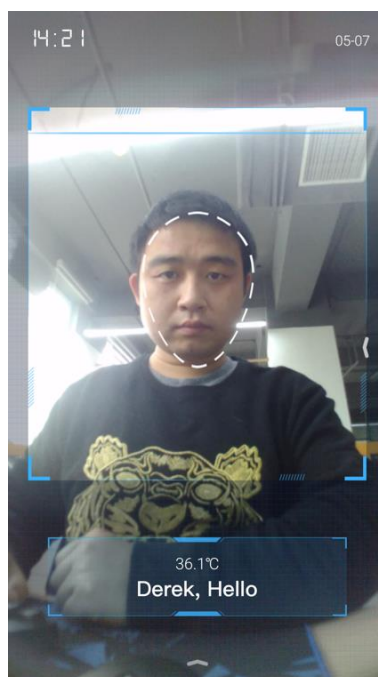
テストターの温度は異常な場合、認証画面に以下のプロンプトメッセージが表示されます：異常温度 温度



4.2.2.2 温度測定+顔認証モード

1) 正常温度、認証成功

テストターの温度が正常で顔認証に合格した場合、認証画面に以下のプロンプトメッセージが表示されます：温度 XXX、こんにちは



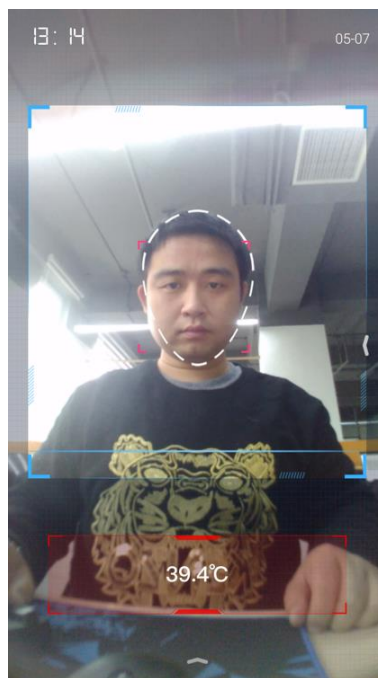
2) 異常温度、認証成功

温度が異常で顔認証に合格した場合、認証画面に以下のプロンプトメッセージが表示されます：温度



3) 異常温度、認証失敗

テストターの温度が異常で顔認証に合格しなかった場合、認証画面に以下のプロンプトメッセージが表示されます：温度



4) 正常温度、認証失敗

テストの温度が正常で顔認証に合格しなかった場合、認証画面に以下のプロンプトメッセージが表示されます：温度



4.3 メンテナンス情報

4.3.1 警告メッセージ

デバイスのエラー警告メッセージは以下のとおりです。

警告メッセージ	警告の説明
ストレージエラー	デバイスのストレージの空き容量が 15%未満になると、デバイスの画面右上にアイコンが表示され、認識記録が自動的にスクロールし、クリアされます。
カメラが壊れている	カメラが故障している場合、スタンバイ画面左上に「カメラが見つかりません。デバイスを確認してください。」のメッセージが表示されます。
取り外しアラーム	<p>取り付け式のデバイスが取り外されると警告音が鳴ります。</p> <p>認証画面で、「設定」>「詳細設定」を選択し、「取り外しアラーム」をオフにすると、警告がオフになります。</p> <p>◇ 取り付け式のデバイスのみ適用されます。</p>

4.3.2 ステータスの確認

認証画面で、「ステータス」を選択すると、「ステータス」ダイアログが表示されます。

「ステータス」ダイアログで、デバイスの「CPU 使用率」、「メモリ使用量」、「CPU 温度」、「ライトの明るさ」、パソコンでウェブ管理機能へログインする URL、モバイルデバイスでウェブ管理機能へログインする QR コードを確認できます。



図 44 「ステータス」画面

4.3.3 デバイス情報の確認

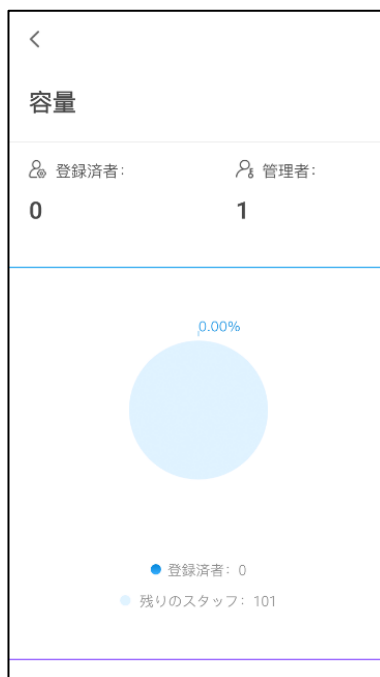
ステップ1 認証画面で、「設定」>「情報」を選択すると、「情報」画面が開きます。

ステップ2 「情報」画面で、デバイス情報を確認できます。

4.3.4 使用容量の確認

ステップ1 認証画面で、「設定」>「容量」を選択すると、「容量」画面が開きます。

ステップ2 「容量」画面で、「登録済人数/管理者」、「使用済登人数/登録可能人数」数、「使用済み容量/使用可能な容量」を確認できます。



5 拡張方法

5.1 概要説明

分類	拡張方法	説明
デバイスカスタマイズ	識別距離	実の運用シナリオと最適なユーザー体験に合わせて、最適な識別距離を設定できます。
	提示文字と提示音	ユーザーの独自案内文と音声をカスタマイズできます。
デジタルサイネージ	ローカル管理	デバイスに画像・動画をインポートし、待受け画面で再生できます。
	クラウド管理	クラウドの拡張 APP で、画像・動画をアップロードし、マルチ再生スケジュールとマルチデバイスで再生内容タスクを一元化管理できます。
機能拡張	デバイス ODSL	Android JavaSDK を用い、独自の Android APP を開発できます。それに、ODSL で独自の AndroidAPP を既存のワークフローに組み込むことができます。 例 1：本人認証後に、有効なチケット/会議参加者/当日出勤シフトなどの二次認証を行うスマート運用。 例 2：実際の業務フローの中にデバイスでの本人認証ポイントとして組み込む。
	デバイス WebAPI	WebAPI を用い、デバイスをダイレクトに制御し、サードパーティ/ユーザーの業務システムにシームレスに整合できます。例：ERP、OA、MES など
	クラウド管理プラットフォーム WebAPI	WebAPI を用い、クラウドのユーザーが所有するデバイスとデータを制御し、サードパーティ/ユーザーの業務システムにシームレスに整合できます。例：ERP、OA、MES など
	デバイス PUSH	デバイスから、識別記録を指定した独自のサーバへ、リアルタイム PUSH できます。リアルタイムの連動運用シーンに最適です。例：CRM システム。
	クラウド PUSH	クラウドから、識別記録を指定した独自のサーバへ、リアルタイム PUSH できます。リアルタイムの連動運用シーンに最適です。例：CRM システム。
	ハードウェア I/F	他社のセキュリティシステム、消防システム、カードリーダー、電気錠、アクセスコントローラー、フリッパーゲート、表示灯、他の設備と連動できます。

5.2 WebAPI(RESTful)

クラウド管理プラットフォームにより、サードパーティの開発者/ISV は、独自のビジネス開発を迅速に完了させることができます。クラウド管理プラットフォームを呼び出すオープン API により、サードパーティプラットフォームのアプリは、メンバーの変更、ルールのカスタマイズ、データの送信など、クラウド管理プラットフォームのコア層となる機能を柔軟かつ簡単に使用でき、デバイスと顧客のアプリケーションシステムをより深く統合できます。

API 接続により、以下の機能が可能になります。テナント情報の取得、登録者の追加・削除・変更・確認（および顔デバイスとの同期）、登録者の所属組織の追加・削除・変更・確認、デバイス情報の取得、ルールの管理、認識記録の取得、写真のトリミング、顔 1:1 などの機能。

インターフェースの詳細については、EDGEMATRIX 株式会社にお問い合わせください。

6 付録

6.1 デバイスの登録者容量ライセンス

当社のデバイス製品をご利用の際は、デバイスの登録人数ライセンスが必要です。初期設定は5万人ライセンスとなっております。最大で10万人まで拡張登録できます。詳細はEDGEMATRIX株式会社にお問い合わせください。

クラウドサービスモードをご利用の場合、デバイスの初回のクラウド接続時に登録人数ライセンスが自動的に適用されます。手動でのアクティベーション操作は不要です。

6.2 認証方法の説明

認証方法はさまざまな組み合わせで設定できます。詳細は以下のとおりです。

※EDGEMATRIX Gatekeeper サービスでは顔以外の認証機能を提供していません。

オプション	説明
顔	操作：「顔」のチェックボックスをオンにします。 入力：顔。 認証：顔と登録者ライブラリ情報で1:N認証を行います。 説明：このシーンでは、「検証モード」は「1:Nモード」または「混合モード」に設定する必要があります。
指紋 (カラーシリーズ)	操作：「指紋」のラジオボタンをオンにします。 入力：指紋。 認証：指紋と登録者ライブラリ情報で認証を行います。
ICカード (カラーシリーズ)	操作：「ICカード」のラジオボタンをオンにします。 入力：ICカード。 認証：ICカードと登録者ライブラリ情報で1:1認証を行います。 説明：このシーンでは、「検証モード」は「1:1モード」または「混合モード」に設定する必要があります。

オプション	説明
QR コード (クラウド サービスモ ード)	<p>操作：認証ルールがクラウド管理プラットフォームで設定され、デバイスに送信されると有効になります。</p> <p>入力：QR コード。</p> <p>認証：QR コードと。</p> <p>説明：このシーンでは、「認証対象」は「顔と QR コード」または「QR コード」に設定する必要があります。</p>
顔+身分証明書	<p>操作：「顔+身分証明書」のラジオボタンをオンにします。</p> <p>入力：顔+身分証明書。</p> <p>認証：顔と身分証明書情報で 1:1 認証を行います。</p> <p>説明：</p> <ol style="list-style-type: none"> 1) 身分証明書を使用して認証するシーンでは、顔と身分証明書の写真を比較するほか、さらに安全性を向上させるために、「承認リスト」と「身分証明書の指紋データ比較」の 2 種類の比較方法がサポートされています。 2) このシーンでは、「検証モード」は「1:1 モード」または「混合モード」に設定する必要があります。
顔+パスポート	<p>操作：「顔+パスポート」のラジオボタンをオンにします。</p> <p>入力：顔+パスポート。</p> <p>認証：顔とパスポート情報で 1:1 認証を行います。</p> <p>説明：このシーンでは、「検証モード」は「1:1 モード」または「混合モード」に設定する必要があります。</p>
顔+アクセスカード	<p>操作：「顔+アクセスカード」のラジオボタンをオンにします。</p> <p>入力：顔+アクセスカード。</p> <p>認証：顔とアクセスカードに対応する登録者情報で 1:1 認証を行います。</p> <p>説明：このシーンでは、「検証モード」は「1:1 モード」または「混合モード」に設定する必要があります。</p>
顔+IC カード	<p>操作：「顔+IC カード」のラジオボタンをオンにします。</p> <p>入力：顔+IC カード。</p> <p>認証：顔と IC カードに対応する登録者情報で 1:1 認証を行います。</p> <p>説明：このシーンでは、「検証モード」は「1:1 モード」または「混合モード」に設定する必要があります。</p>
顔+パスワード	<p>操作：「顔+パスワード」のラジオボタンをオンにします。</p> <p>入力：顔+パスワード。</p> <p>認証：</p> <ol style="list-style-type: none"> 1) 顔と登録者ライブラリ情報で 1:N 認証を行います。 2) 顔認証の完了後、パスワードと登録者ライブラリで事前に設定したパスワードの認証を行います。 <p>説明：このシーンでは、「検証モード」は「1:N モード」または「混合モード」に設定す</p>

オプション	説明
	する必要があります。
顔：顔+身分証明書	操作：「顔」のチェックボックスと「顔+身分証明書」のラジオボタンを両方オンにします。 入力：顔（+身分証明書）。 認証： 1) 顔+身分証明書のシーン：顔と身分証明書情報で 1:1 認証を行います。 2) 顔のみのシーン：顔と登録者ライブラリ情報で 1:N 認証を行います。 説明： 1) 身分証明書を使用して認証するシーンでは、顔と身分証明書の写真を比較するほか、さらに安全性を向上させるために、「承認リスト」と「身分証明書の指紋データ比較」の 2 種類の比較方法がサポートされています。 2) このシーンでは、「検証モード」を「混合モード」に設定する必要があります。
顔：顔+パスポート	操作：「顔」のチェックボックスと「顔+パスポート」のラジオボタンを両方オンにします。 入力：顔（+パスポート）。 認証： 1) 顔+身分証明書のシーン：顔とパスポート情報で 1:1 認証を行います。 2) 顔のみのシーン：登録者ライブラリ情報と 1:N 認証を行います。 説明：このシーンでは、「検証モード」を「混合モード」に設定する必要があります
顔：顔+アクセスカード	操作：「顔」のチェックボックスと「顔+アクセスカード」のラジオボタンを両方オンにします。 入力：顔（+アクセスカード）。 認証： 1) 顔+アクセスカードのシーン：顔とアクセスカード情報で 1:1 認証を行います。 2) 顔のみのシーン：顔と登録者ライブラリ情報で 1:N 認証を行います。 説明：このシーンでは、「検証モード」を「混合モード」に設定する必要があります。
顔：顔+ICカード	操作：「顔」のチェックボックスと「顔+IC カード」のラジオボタンを両方オンにします。 入力：顔（+IC カード）。 認証： 1) 顔+IC カードのシーン：顔と IC カード情報で 1:1 認証を行います。 2) 顔のみのシーン：顔と登録者ライブラリ情報で 1:N 認証を行います。 説明：このシーンでは、「検証モード」を「混合モード」に設定する必要があります。
顔：IC カード （カラーシリーズ）	操作：「顔」のチェックボックスと「IC カード」のラジオボタンを両方オンにします。 入力：顔または IC カード。 認証： 1) 顔のシーン：顔と登録者ライブラリ情報で 1:N 認証を行います。

オプション	説明
	2) ICカードのシーン：ICカードと登録者ライブラリ情報で 1:1 認証を行います。 説明：このシーンでは、「検証モード」を「混合モード」に設定する必要があります。
顔：指紋 （カラーシリーズ）	操作：「顔」のチェックボックスと「指紋」のラジオボタンを両方オンにします。 入力：顔または指紋。 認証： 1) 顔のシーン：顔と登録者ライブラリ情報で 1:N 認証を行います。 2) 指紋のシーン：指紋と登録者ライブラリ情報で認証を行います。 説明：このシーンでは、「検証モード」は「1:Nモード」または「混合モード」に設定する必要があります。

7 FAQ

7.1 デバイスが管理プラットフォームへ接続できません。

1. ネットワーク環境を確認します。
2. ファイアウォールで 80、443、123、6666 ポートが許可されているかを確認します。

7.2 一つのクラウドアカウントへ複数同時にログインができません。

安全性確保のため一つのアカウントには同時に一人しかログインできない仕様となっております。

7.3 アクティベーションコードを更新した場合、旧コードを使用できますか。

アクティベーションコードを更新した場合、旧コードは即時に無効となります。
なお、既にアクティブ化されたデバイスには影響がありません。