# 顔認証コネクトデバイス
# ユーザーズマニュアル
# 製品型番：LTC-FPT50/IPV2

**第 1 版**




| | |
|---|---|
| 作　成　者 | ロジテック INA ソリューションズ株式会社 |
| 作　成　日 | 2026 年 7 月 5 日 |
| 最終更新日 | 2026 年 7 月 5 日 |

Logitec

# 目次

1. はじめに ..... 5
2. 製品に関する注意事項 ..... 5
2.1. 使用前の注意事項 ..... 5
2.2. 使用時の注意事項 ..... 6
2.3. 保管時の注意事項 ..... 6
3. 製品の概要 ..... 7
3.1. 製品について ..... 7
3.2. 認証方式について ..... 9
3.3. 製品タイプ ..... 10
3.4. 製品構成 ..... 10
3.5. 各部の名称 ..... 11
4. 顔認証デバイスの導入（初期設定） ..... 13
4.1. 壁面取り付け方法 ..... 13
4.2. 電源接続方法の選択 ..... 16
4.3. ネットワーク接続方法の選択 ..... 16
4.4. クラウドサーバの設定 ..... 21
5. 管理ソフトの導入（初期設定） ..... 22
5.1. 管理ソフトの動作環境要件 ..... 22
5.2. 管理ソフトのダウンロード ..... 23
5.3. 管理ソフトのインストール ..... 25
5.4. 管理者アカウントの設定 ..... 30
5.5. ライセンス認証 ..... 32
5.6. ライセンス認証の解除 ..... 34
5.7. 自己署名証明書のインストール ..... 36
5.8. 管理ソフトの基本操作 ..... 38
5.9. 管理ソフトの再インストール ..... 42
5.10. 管理ソフトが稼働する PC/サーバーの入れ替え ..... 45
6. ユーザー登録（勤怠/入退 共通） ..... 48
6.1. 自動バックアップ ..... 49
6.2. エリア設定 ..... 50
6.3. 部署を設定する ※本手順は省略することができます ..... 53
6.4. ユーザー情報の一括登録 ..... 56
6.5. 顔認証を利用する場合 ..... 58
7. 勤怠連携（導入編） ..... 62
7.1. 顔認証デバイス設定（勤怠 Push） ..... 63
7.2. デバイス登録 ..... 64
7.3. エリア別ユーザー登録 ..... 66
7.4. 打刻方法の設定 ..... 70
7.5. 勤怠打刻と勤怠履歴 ..... 79
7.6. 顔認証または他の認証を利用する場合 ..... 82
7.7. 外部勤怠管理システムと連携 ..... 87

7.8. 打刻データ連携ツールの実行方法 ..... 88
8. 入退室管理（導入編） ..... 92
8.1. 顔認証デバイス設定（入退 Push） ..... 93
8.2. タイムゾーン（アクセス可能時間） ..... 94
8.3. デバイス管理 ..... 95
8.4. ドア ..... 98
8.5. グループ登録 ..... 99
8.6. アクセス設定 ..... 102
8.7. リアルタイムモニタリング ..... 104
8.8. アラームモニタリング ..... 104
8.9. 全トランザクション ..... 106
8.10. 顔認証または他の認証を利用する場合 ..... 107
9. 管理ソフトの機能説明 ..... 112
9.1. システム管理 ..... 112
9.2. 権限管理 ..... 129
9.3. 通信管理 ..... 135
9.4. サードパーティの統合 ..... 136
9.5. 外部連携 ..... 136
9.6. ユーザー管理 ..... 146
9.7. カード管理 ..... 167
9.8. 勤怠連携 ..... 170
9.9. デバイス管理 ..... 171
9.10. 勤怠レポート ..... 191
9.11. 出席日報 ..... 194
9.12. 出席月次レポート ..... 194
9.13. 出席統計レポート ..... 194
9.14. 出欠カスタムレポート ..... 194
9.15. 入退室管理 ..... 195
9.16. アクセスデバイス ..... 196
9.17. アクセスルール ..... 220
9.18. アクセス制御レポート ..... 243
10. 顔認証デバイスの機能説明 ..... 247
10.1. ユーザー管理 ..... 250
10.2. ユーザー権限（カスタム権限） ..... 257
10.3. 通信設定 ..... 258
10.4. システム設定 ..... 267
10.5. パーソナリティ設定 ..... 285
10.6. データ管理 ..... 293
10.7. アクセスコントロール ..... 297
10.8. 勤怠検索 ..... 306
10.9. 自動テスト ..... 308
10.10. システム情報 ..... 309

11. サービスコントローラ（データ復元など）.....311
11.1. サービスコントローラの起動.....311
11.2. サーバーポートの設定変更.....312
11.3. データベースの設定変更.....313
11.4. データベースのバックアップ先変更.....313
11.5. データベースの復元.....314
11.6. 管理ソフトのサービスの停止／再開.....316
11.7. SSL 証明書のインポート.....317
11.8. 言語パックのインポート.....317
11.9. モジュールの追加.....318
11.10. データベース接続パスワード変更.....318
11.11. Redis 接続パスワード変更.....318
11.12. Toggle HTTP.....318
11.13. ログの表示.....318
12. お取り扱い上の注意.....319
12.1. 廃棄・譲渡時のデータに関する注意.....322
12.2. 電波に関する注意事項.....322
12.3. 免責事項.....323
12.4. 保証規定.....324
12.5. 修理規定.....324
12.6. サポート・修理窓口のご案内.....325
13. 付録 A 製品仕様.....327
14. 付録 B 製品サイズ.....328
15. 付録 C 顔登録ガイドライン（外部リンク）.....332
16. 付録 D データ消去サービスについて.....333

# 1. はじめに

この取扱説明書は、ロジテック INA ソリューションズ株式会社（以下「当社」という）製の顔認証コネクトデバイス LTC-FPT50/IPV2（以下「顔認証デバイス」という）と ZKBio CV Security（以下「管理ソフト」という）のセットアップおよび使用方法についての取扱説明書です。本書の構成は、「顔認証デバイスの導入」、「管理ソフトの導入」、「ユーザー登録（勤怠／入退共通）」、「勤怠連携（導入編）」、「入退室管理（導入編）」、「管理ソフトの機能説明」および「顔認証デバイスの機能説明」に分類して説明します。

本取扱説明書は常に最新のユーザーズマニュアルを当社ホームページに公開しています。製品のバージョン変更によって、取扱説明書内の挿絵及び端末画面の写真が実際の製品と異なる場合があります。また、この取扱説明書にて提供する情報は、事前の告知なく変更される場合があります。製品に関するアップデート情報は、ロジテック INA ソリューションズ株式会社までお問い合わせください。

## 会社情報

社名：　ロジテック INA ソリューションズ株式会社
本社所在地：　長野県伊那市美篶 8268 番地 1000
Web サイト：　https://www.logitec.co.jp/

## 著作権

この取扱説明書に含まれる全てのコンテンツ及び挿絵、端末画面写真の著作権及び知的財産権はロジテック INA ソリューションズ株式会社に帰属します。ロジテック INA ソリューションズ株式会社による事前の書面による承認が無くこの取扱説明書を無断で使用、複製、流通及び配布する行為は知的財産権の侵害となり厳格に禁じます。

## 個人情報の保護について

本製品および本製品を使用したシステムで撮影・記録された本人が判別できる情報は、「個人情報の保護に関する法律」で定められた「個人情報」に該当します。法律に従って、情報を適切にお取り扱いください。

# 2. 製品に関する注意事項

本製品を安全にご使用いただくために、以下の注意事項及び「12 お取り扱い上の注意」を必ずお読みになり、指示に従って製品をご利用ください。

## 2.1. 使用前の注意事項

- 本製品は生体認証技術を使って個人を特定する製品です。生体認証の特性上、認証率 100%を保証するものではありません。より高い認証率を維持するためにも、ユーザー登録方法のガイドラインに従って顔または掌の登録をお願いします。
- 本製品は屋外（IP66*）・室内のいずれかで使用できます。
  *IP66：IEC（国際電気標準会議）および JIS（日本工業規格）で定められた電気機器の内部への異物侵入に対する保護等級の 1 つです。IP の後に続く第一特性数字が外来固形物に対する保護等級である「防塵」、第 2 特性数字が水の侵入に対する保護等級である「防滴」の性能を示します。本製品は IP66 のため、粉塵が内部に入らない耐塵性能があり、あらゆる方向からの暴噴流に対して保護されている耐水性能があります。
- 夏場など設置環境が高温になる場合、製品仕様の動作保証で規定する温度・湿度内でご使用ください。
- 本製品を壁掛けで使用する場合、平面かつネジが固定できる素材に設置し、付属の固定用ブラケットおよびアンカーを使用してしっかりと固定し、落下防止の対策をしてください。必要な場合、有償の設置・設定サービスをご利用ください。

- 本製品をフロアスタンド（別売オプション品）で使用する場合、製品が倒れないよう安全な場所に設置し、付属のアンカーなどで転倒防止の対策をしてください。
- 製品を使用する際は、製品を安全な場所に設置できたことを確認してから、指定の箇所に電源ケーブルを接続してください。
- 本製品は生体検知機能で近赤外線を利用します。認証精度に影響を及ぼすような次の設置場所を避けてください。
  - 端末本体の画面に直射日光や、照明などの照射が直接あたる場所。
  - 端末本体の画面に雨や雪、凍結や結露が発生する場所。
- 過度な湿気を避け、製品内部に水などの液体や異物が入らないように注意してください。
- 本製品は日本国内向けに製造されています。

## 2.2. 使用時の注意事項

- 製品を分解、修理、改造したり、衝撃を与えたりしないでください。製品を分解、修理、改造された場合は、製品保証の対象外となります。
- 接続したケーブルに無理な力を加えないでください。ケーブル接続部が緩くなる、または、断線や破損する可能性があります。
- ボタンまたは画面に無理に力を加える、または、先の尖った道具などで力を加えないでください。ボタンまたは画面の破損の原因になります。
- 製品や画面の汚れを取る場合は、アルコールなどの化学物質や洗剤を使用せず、柔らかい布でやさしく拭き取ってください。硬い布で拭いたり、強く擦ったりしますと、製品の外観やパネル表面のフィルムに傷が付きますのでご注意ください。
  ガラス用クリーナーやスプレー式のクリーナーは、製品の外観やパネル表面が変質、または、内部に侵入し、故障の原因になる恐れがあるので、使用しないでください。
  化学雑巾やアルコール、ベンジン、シンナー、酸性/ アルカリ性/ 研磨剤入り洗浄剤などは、その成分により、製品の外観やパネル表面が変質、または、変色する恐れがありますのでご使用にならないでください。
- 製品から異臭や煙が発生、あるいは製品の異常な動作（動画・音声の再生など）が生じた際には、すぐにコンセントからACアダプタを抜いてください。感電、火災の原因になります。
- 製品に同梱されたACアダプタ以外は使用しないでください。同梱されたACアダプタ以外を使用した場合、故障、感電、火災の原因になります。
- 端末内のソフトウェアやファイルを削除しないでください。端末が正常に動作しなくなる場合があります。
- 製品の故障が疑われる場合は購入先の販売店へお問合せください。
- 本製品や管理ソフトウェアに記録されたデータ(登録済みのユーザー情報や、アクセス履歴等)は、当社では保証せず、当該データの消失、破損、変更等につきましては、当社は一切責任を負いません。データの消失、破損等に備え、外部記憶装置などに定期的にバックアップをとられることをお勧めいたします。バックアップの方法は、「9.1.2 データ管理」の「3.自動バックアップ」を参照してください。
- 本製品を他の機器と接続して使用する場合、事前に概要機器と本製品との適合性についてご確認ください。

## 2.3. 保管時の注意事項

- 未使用時、または、長期間使用しない場合は、PoE給電のLANケーブルやACアダプタを機器から抜いた状態で保管してください。
- 日光や照明などの光が直接当たらず、常温、乾燥した場所に保管してください。
- 薬品の近くやガスが発生する場所など、火災の危険がある場所を避けて保管してください。

# 3. 製品の概要

## 3.1. 製品について

顔認証デバイス「LTC-FPT」シリーズは、生体認証などにより個人を特定して認証する装置です。また、入退室管理用途では「入退 Push モード」、勤怠管理用途では「勤怠 Push モード」とそれぞれ端末運用モードを切り替えて利用する製品です。

顔認証デバイスおよびユーザー情報や各種記録の設定・管理の主体は統合管理ソフト「ZKBio CVSecurity（以下、「管理ソフト」という）」を使用します。下表の通り、本管理ソフトは管理するデバイスの台数に応じて年間ライセンス費用*1 がかかります。用途に応じて必要なメニュー*を、必要なライセンス分ご購入していただきます。なお、ユーザー管理とシステム管理は管理ソフトの共通メニューのため、入退室管理や勤怠連携など、いずれか 1 つを導入いただいた際に付属します。

・ユーザー管理
・入退室管理
・勤怠連携
・システム管理　など
*利用できるメニューは随時追加予定となります。

| | |
|---|---|
|  |  |
| 顔認証デバイスを利用するユーザーを登録、管理するメニューです。<br>・ユーザーの登録、編集、削除<br>・ユーザー写真の登録、削除など<br>※最大ユーザー登録数は 30,000 人 | 入退室管理を行うためのメニューです。<br>・デバイスの登録<br>・アクセス権限設定<br>・監視、制御など |
|  |  |
| 顔認証デバイスをタイムレコーダーとして使用し、外部システムに打刻データを連携するためのメニューです。<br>・デバイスの登録<br>・打刻方法の設定<br>・エリア毎のユーザー管理など | 管理ソフトを使用するにあたり、各メニュー共通の設定と表示を行います。<br>・エリア設定<br>・ユーザーの権限管理設定<br>・データベースの管理<br>・システムパラメータの設定など |

### 勤怠連携用ライセンス（初年度）

管理ソフトの勤怠管理メニューを利用するため、導入初年度に必要なライセンスです。

| 製品型番 | 内容 |
|---|---|
| LTC-ATTSW10/1Y | 1 年間の端末管理 10 台以下のライセンス（勤怠モード 10 台を含む） |
| LTC-ATTSW20/1Y | 1 年間の端末管理 20 台以下のライセンス（勤怠モード 20 台を含む） |
| LTC-ATTSW30/1Y | 1 年間の端末管理 30 台以下のライセンス（勤怠モード 30 台を含む） |
| LTC-ATTSW40/1Y | 1 年間の端末管理 40 台以下のライセンス（勤怠モード 40 台を含む） |
| LTC-ATTSW50/1Y | 1 年間の端末管理 50 台以下のライセンス（勤怠モード 50 台を含む） |

※1 年間の端末管理 60 台～200 台以下のライセンスは表示を省略

### 勤怠連携用ライセンス（1 年更新用）

管理ソフトの勤怠管理メニューを 2 年目以降、1 年間ずつ利用するための更新ライセンスです。

| 製品型番 | 内容 |
|---|---|
| UPD-ATTSW10/1Y | 1 年間の端末管理 10 台以下のライセンス（勤怠モード 10 台を含む）1 年更新 |
| UPD-ATTSW20/1Y | 1 年間の端末管理 20 台以下のライセンス（勤怠モード 20 台を含む）1 年更新 |
| UPD-ATTSW30/1Y | 1 年間の端末管理 30 台以下のライセンス（勤怠モード 30 台を含む）1 年更新 |
| UPD-ATTSW40/1Y | 1 年間の端末管理 40 台以下のライセンス（勤怠モード 40 台を含む）1 年更新 |
| UPD-ATTSW50/1Y | 1 年間の端末管理 50 台以下のライセンス（勤怠モード 50 台を含む）1 年更新 |

※1 年間の端末管理 60 台～200 台以下のライセンスは表示を省略

### 入退室管理用ライセンス（初年度）

管理ソフトの入退室管理メニューを利用するため、導入初年度に必要なライセンスです。

| 製品型番 | 内容 |
|---|---|
| LTC-CHKSW10/1Y | 1 年間の端末管理 10 台以下のライセンス（入退モード 10 台） |
| LTC-CHKSW20/1Y | 1 年間の端末管理 20 台以下のライセンス（入退モード 20 台） |
| LTC-CHKSW30/1Y | 1 年間の端末管理 30 台以下のライセンス（入退モード 30 台） |
| LTC-CHKSW40/1Y | 1 年間の端末管理 40 台以下のライセンス（入退モード 40 台） |
| LTC-CHKSW50/1Y | 1 年間の端末管理 50 台以下のライセンス（入退モード 50 台） |

※1 年間の端末管理 60 台～200 台以下のライセンスは表示を省略

### 入退室管理用ライセンス（1 年更新用）

管理ソフトの入退室管理メニューを 2 年目以降、1 年間ずつ利用するための更新ライセンスです。

| 製品型番 | 内容 |
|---|---|
| UPD-CHKSW10/1Y | 1 年間の端末管理 10 台以下のライセンス（入退モード 10 台を含む）1 年更新 |
| UPD-CHKSW20/1Y | 1 年間の端末管理 20 台以下のライセンス（入退モード 20 台を含む）1 年更新 |
| UPD-CHKSW30/1Y | 1 年間の端末管理 30 台以下のライセンス（入退モード 30 台を含む）1 年更新 |
| UPD-CHKSW40/1Y | 1 年間の端末管理 40 台以下のライセンス（入退モード 40 台を含む）1 年更新 |
| UPD-CHKSW50/1Y | 1 年間の端末管理 50 台以下のライセンス（入退モード 50 台を含む）1 年更新 |

※1 年間の端末管理 60 台～200 台以下のライセンスは表示を省略

### 勤怠管理及び入退室管理の 2 つのライセンス（初年度）

管理ソフトで勤怠管理と入退室管理の 2 つのメニューを利用するため、導入初年度に必要なライセンスです。

| 製品型番 | 内容 |
|---|---|
| LTC-FPSW10/1Y | 1 年間の端末管理 10 台以下のライセンス（入退モード 10 台／勤怠モード 10 台を含む） |
| LTC-FPSW20/1Y | 1 年間の端末管理 20 台以下のライセンス（入退モード 20 台／勤怠モード 20 台を含む） |
| LTC-FPSW30/1Y | 1 年間の端末管理 30 台以下のライセンス（入退モード 30 台／勤怠モード 30 台を含む） |
| LTC-FPSW40/1Y | 1 年間の端末管理 40 台以下のライセンス（入退モード 40 台／勤怠モード 40 台を含む） |
| LTC-FPSW50/1Y | 1 年間の端末管理 50 台以下のライセンス（入退モード 50 台／勤怠モード 50 台を含む） |

※1 年間の端末管理 60 台以上のライセンスはありません

**勤怠連携及び入退室管理の 2 つのライセンス（1 年更新用）**

管理ソフトで勤怠管理と入退室管理の 2 つのメニューを 2 年目以降、1 年間ずつ利用するための更新ライセンスです。

| 製品型番 | 内容 |
|---|---|
| UPD-FPSW10/1Y | 1 年間の端末管理 10 台以下のライセンス（入退モード 10 台／勤怠モード 10 台を含む）1 年更新 |
| UPD-FPSW20/1Y | 1 年間の端末管理 20 台以下のライセンス（入退モード 20 台／勤怠モード 20 台を含む）1 年更新 |
| UPD-FPSW30/1Y | 1 年間の端末管理 30 台以下のライセンス（入退モード 30 台／勤怠モード 30 台を含む）1 年更新 |
| UPD-FPSW40/1Y | 1 年間の端末管理 40 台以下のライセンス（入退モード 40 台／勤怠モード 40 台を含む）1 年更新 |
| UPD-FPSW50/1Y | 1 年間の端末管理 50 台以下のライセンス（入退モード 50 台／勤怠モード 50 台を含む）1 年更新 |

※1 年間の端末管理 60 台以上のライセンスはありません

**顔認証コネクトデバイス「統合管理ソフトウェア 1 年ライセンス」利用規約**

統合管理ソフトウェアの利用規約は下記 URL よりダウンロードできます。本規約はライセンスのご注文を以って同意したものとします。また、本規約は予告なく更新される場合があります。常に最新の規約を参照してください。

https://dl.logitec.co.jp/downloadfile/DLfile/LST-M/ltcfpt_swlicense_kiyaku.pdf

**注意事項**

***1 ライセンス費用は、契約日を基点に毎年更新が必要になります。契約更新日の 2 か月前に更新のご案内とお見積もりをご提示いたします。契約を更新される場合、契約満了日までに該当する製品型番のご注文をお願いします。また、契約期間中に顔認証デバイスの台数を変更する場合、既にお支払いいただいているライセンス費用の日割りなどによるご返金は対応できかねます。新規に該当する製品型番のご注文をお願いします。なお、契約日は新規に契約が成立した日を基点とします。**

## 3.2. 認証方式について

生体情報による認証方式は顔認証・掌認証、所持情報による認証方式は IC カード認証（FeliCa/Mifare）、知識情報による認証方式はパスワード認証に対応します。異なる認証方式を組み合わせた多要素認証、異なる生体認証方式を組み合わせたマルチモーダル認証に対応します（表 1）。

（表 1）

| 知識情報による認証 | 所持情報による認証 | 生体情報による認証 |
|---|---|---|
| 本人だけが知っている情報を利用<br>例）パスワード、暗証番号など | 本人だけが所持しているものを利用<br>例）IC カード、QR など | 本人だけに備わっている特徴を利用<br>例）指紋、顔、静脈、虹彩など |
| **本製品で利用できる認証方式** | | |
| 下記の認証に対応します<br>● パスワード（登録数 50,000 件） | 下記の IC カード・QR 認証に対応します*2（登録数 50,000 件）<br>● FeliCa：ISO/IEC 18092「NFC Type F」に対応<br>● Mifare：ISO/IEC 14443「Type A」に対応 | 下記の生体認証に対応します<br>● 顔（登録数 10,000 件）<br>● 掌（登録数 5,000 件） |

**注意事項**

***2 カード ID 情報の取得（読み取り）のみをサポートします。動作確認済みのカードは以下の通りです。**
**・「FeliCa」の「IDm」情報**
**・「Mifare Plus」の「UID」情報**
**・「Mifare Ultralight EV1」の「UID」情報**
**・「Mifare Classic 1K」の「UID」情報**

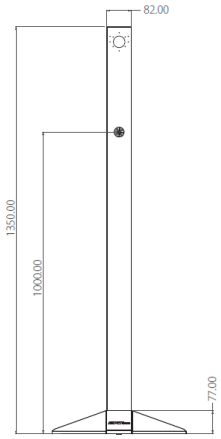
## 3.3. 製品タイプ

本製品は壁掛けタイプの製品です。本体に付属する固定用ブラケットを使用して壁面へ取り付けを行います。フロアスタンドをご利用する場合、別途本製品専用のフロアスタンド（LTC-FPFLOOR/OP）をお買い求めください。

LTC-FPT50/IPV2（壁掛け）



LTC-FPFLOOR/OP（別売：オプション品）




## 3.4. 製品構成



顔認証デバイス本体



AC アダプタ



ユーザーズマニュアルのご案内



固定位置合わせ用ステッカー



固定用ブラケット
※タンパーアラーム用マグネット付き



壁掛け用バックカバー
※固定用ブラケットは不要です



※取り付けネジ付属
プラスドライバーが必要です



レインカバー
※屋外利用時に取り付けます

レインカバー用ビスキット
M3×6 ネジ（銀）：2 本



ビスキット
M3.5×40（銀）：4 本
M3×6 ネジ（黒）：1 本
アンカー（白）：4 本



トルクスドライバー（T10）



ダイオード（FR107）



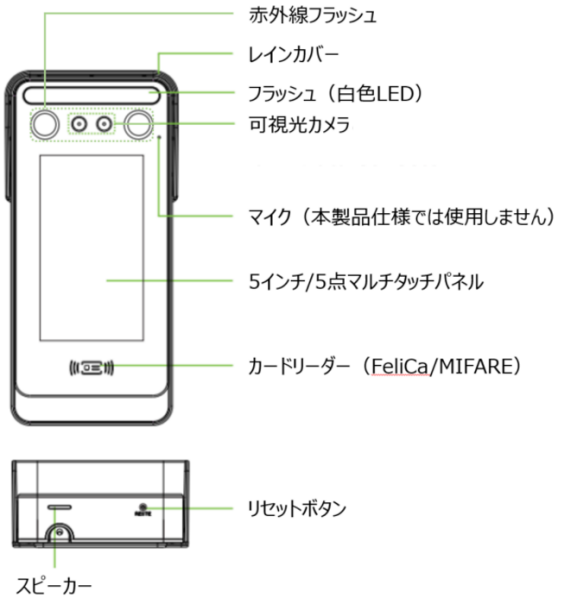
ケーブルキット（3 本）

※製品構成は、製品の性能や品質向上のために予告なく変更となる場合があります。

## 3.5. 各部の名称

顔認証デバイスの各部の名称と説明をします。

### 3.5.1. 顔認証デバイス本体正面



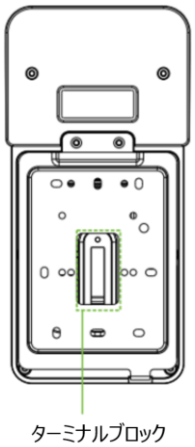

| 名称 | 説明 |
|---|---|
| 近赤外線 | 画像・動画などの偽造防止*1 に使用します。 |
| レインカバー | 屋外設置時、雨や日光からレンズを保護します。 |
| フラッシュ | 認証時の被写体を鮮明に映します。 |
| 可視光カメラ | 顔認識・掌認識用のカメラです。 |
| マイク | 本製品仕様では使用しません。 |
| 5 インチタッチパネル | ソフトウェアの各種操作や結果を表示します。 |
| カードリーダー | IC カードの読み取り専用リーダーです。 |
| スピーカー | 音声案内と警告音が鳴ります。 |
| リセットボタン | ピンホール内のリセットボタンを約 1 秒押すと電源リセットを行い端末が再起動します。 |

**注意事項**

***1 赤外線偽造防止について（重要）**

**太陽光が直接被写体にあたっている場合、もしくは、太陽光が鏡面やガラス面に反射して被写体に当たっている場合、赤外線偽造防止の判定で NG（未登録）と判定されます。本機から照射する IR LED(波長 700～1500nm 程度までの近赤外線)の光を被写体にあて、その反射光から被写体の濃淡を判別することにより検知しています。このため、太陽光は、この近赤外線の波長も含むため、直接被写体にあたると、その反射光は IR LED による反射光より多くなり、被写体の濃淡を判別することができなくなり、生体検知機能が正常に動作しません。対応策として、被写体に直接太陽光が当たらない位置に設置するか、ブラインドなどで太陽光を遮断して使用する、または、赤外線偽造防止機能を OFF にしてソフトウェア・アルゴリズムによる偽造防止機能を使用します。**

### 3.5.2. 顔認証デバイス本体背面

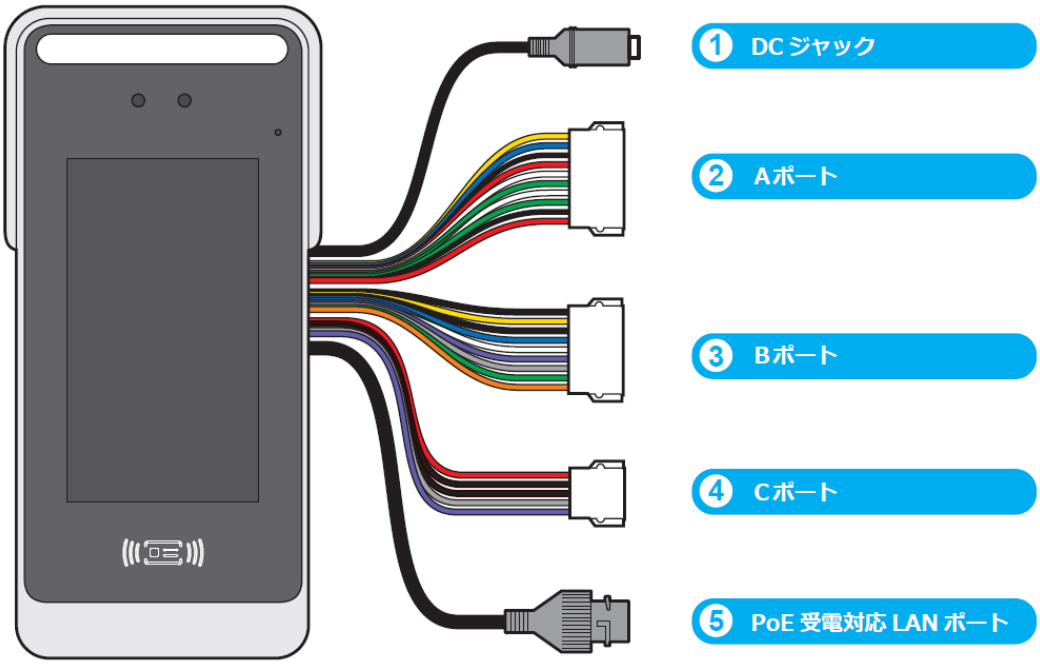



| 名称 | 説明 |
|---|---|
| ターミナルブロック | 付属の専用 AC アダプタや有線 LAN 接続などの各種コネクタ・配線ケーブルです。 |

※左図は固定用ブラケットを装着したイラストになります。

## 3.5.3. ターミナルブロック接続図

### 1. ポート名




### 2. ポート詳細とサポート対象範囲

**② Aポート**

| 名称および用途 | 色 | 信号名 |
|---|---|---|
| RS485 ※ | ● | 485B |
| | ● | 485A |
| Power Out | ● | GND |
| | ● | 12V-OUT |
| アンチパスバック専用 出力ポート | ○ | WD1-OUT |
| | ● | WD0-OUT |
| アンチパスバック専用 入力ポート | ○ | IWD1 |
| | ● | IWD0 |
| Power Out | ● | GND |
| | ● | 12V-OUT |

※将来の機能拡張用であり、現状は未サポートです。

**③ Bポート**

| 名称および用途 | 色 | 信号名 |
|---|---|---|
| Auxiliary Input ※ | ● | AUX |
| Sensor Input ※ | ● | SEN |
| Exit Button | ● | GND |
| | ● | BUT |
| Lock | ○ | NO |
| | ● | COM |
| | ● | NC |
| Alarm | ● | AL- |
| | ● | AL+ |

※将来の機能拡張用であり、現状は未サポートです。

**④ Cポート**

| 名称および用途 | 色 | 信号名 |
|---|---|---|
| Power Out | ● | 12V-OUT |
| | ● | GND |
| RS232 ※ | ● | GND |
| | ● | RS232-RXD |
| | ● | RS232-TXD |

※将来の機能拡張用であり、現状は未サポートです。

Power Out（12V-OUT）は全ポート合計で最大 300mA です。

**注意事項**

**※印は、将来の機能拡張用であり、現状はサポート対象外です。**

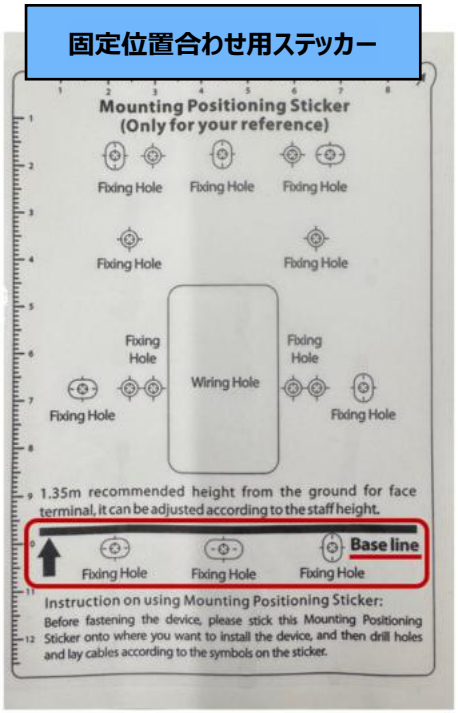
# 4. 顔認証デバイスの導入（初期設定）

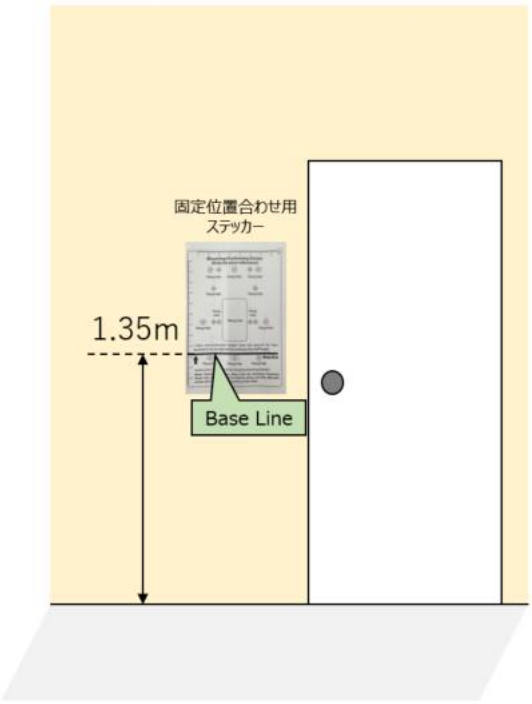
顔認証デバイスの初期設定について説明します。

## 4.1. 壁面取り付け方法

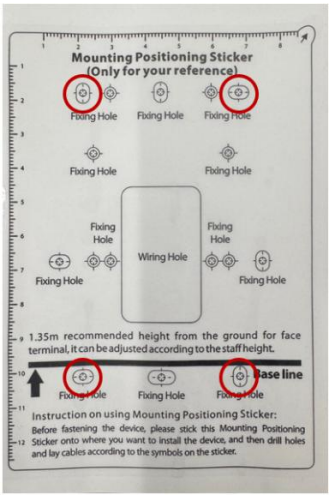
製品本体に付属の「固定位置合わせ用ステッカー」を使用して壁に取り付けを行います。
※配線や取り付けに工事を伴いますのでお客様で業者を手配いただくか、当社専用サービス（有償）をご利用ください。

### 1. 固定位置合わせ用ステッカーの貼付




### 2. 固定用ブラケット（専用フロアスタンド･壁内配線用）の取り付け



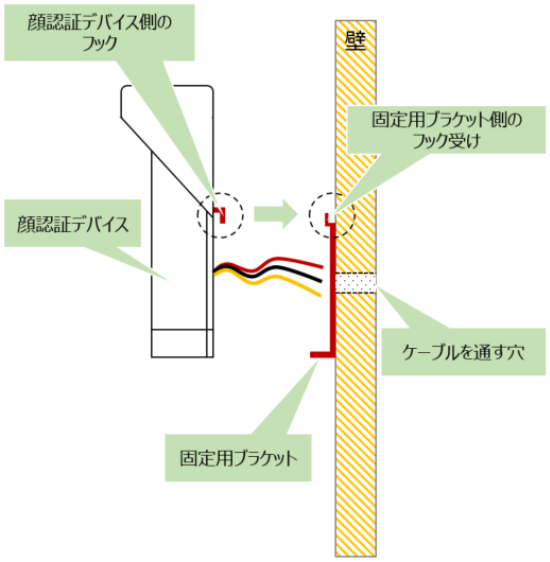
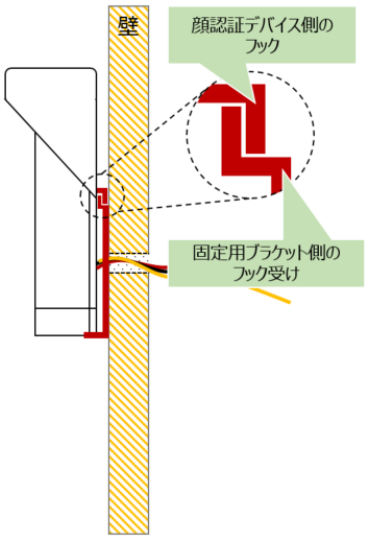

※本ステッカーは下穴をあけるためのものです。
赤丸は下穴の位置を示しています。



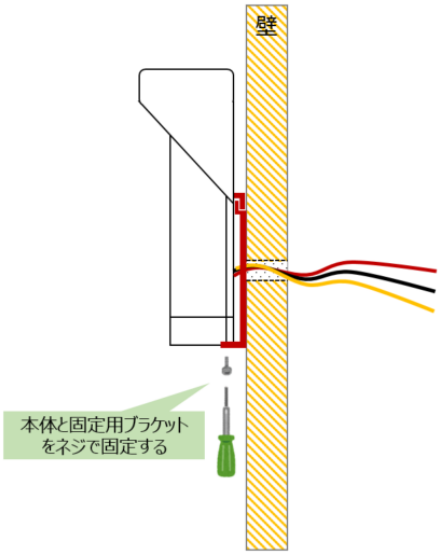

※タンパーアラーム用のマグネットがあることを確認します

① 固定用ブラケットを付属の「M3.5×40（銀）：４本」で取り付けます。直接壁にネジを打つとしっかりと固定できない場合、下穴をあけた上で付属の「アンカー（白）：４本（プラスチック製のアンカー）」を取り付けます。
※取り付けする壁素材（コンクリートなど）により、業者へ相談して適切なアンカーを選定してください。

② 固定用ブラケットへ顔認証端末を取り付けます。

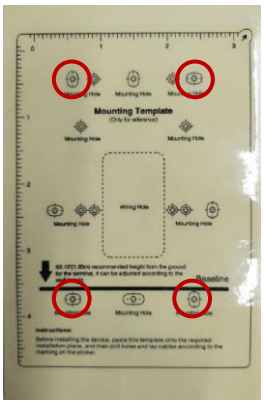
| ☑ 顔認証デバイス側のフックを固定用ブラケット側のフック受けに引っ掛けます。 | ☑ しっかりと固定していることを確認します。 |
|---|---|
|  |  |

③ 本体と固定用ブラケットを付属の「トルクスドライバー（T10）」と「M3×6 ネジ（黒）：1 本」を使用して固定します。



### 3. バックカバー（壁外配線用）の取り付け ※レインカバーは取り外す必要があります

バックカバーは必要なケーブルだけを下の穴のフタを外して、必要なケーブル（電源、LAN など）を通して壁外で接続することができます。通したケーブルは必要に応じてモール処理をしてください。

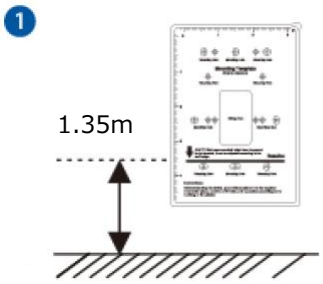



※本ステッカーは下穴をあけるためのものです。
赤丸は下穴の位置を示しています。



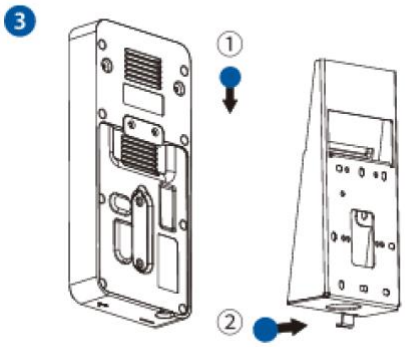

※タンパーアラーム用のマグネットを固定用ブラケットから外して取り付けます。

① 床から 1.35m の位置と固定位置合わせ用ステッカーの Baseline を合わせます。
② 固定用ブラケットを付属の「M3.5×40（銀）：4 本」で取り付けます。直接壁にネジを打つとしっかりと固定できない場合、下穴をあけた上で付属の「アンカー（白）：４本（プラスチック製のアンカー）」を取り付けます。
※取り付けする壁素材（コンクリートなど）により、業者へ相談して適切なアンカーを選定してください。
③ 顔認証デバイス側のフックをバックカバー側のフック受けに引っ掛けます。
④ 本体とバックカバーを付属の「トルクスドライバー（T10）」と「M3×6 ネジ（黒）：1 本」を使用して固定します。









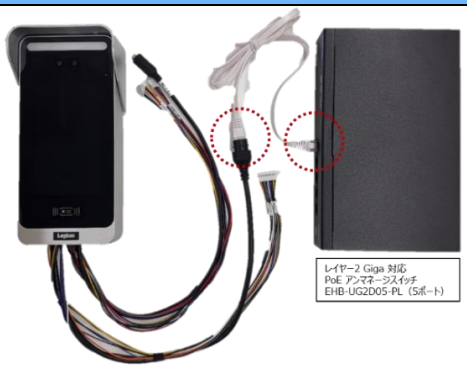




以上で壁面取り付け方法の説明を終わります。

## 4.2. 電源接続方法の選択

顔認証デバイスは本製品に付属の専用 AC アダプタを使用する、または、有線 LAN 接続による PoE 受電を使用します。
※初めて顔認証デバイスの電源を入れる場合、プライバシーポリシーへの同意が必要になります。

| 付属の専用 AC アダプタ | PoE 受電 |
|---|---|
| 本体側の「12V-IN」へ AC アダプタを接続します<br><br>Input：12V 2A | <br>10baseT/100baseTX<br>PoE+ 25W（IEEE 802.3at） |
| AC アダプタ型番：LA-24W12S-01 | 本製品には給電機能付きのネットワーク機器および LAN ケーブルは付属しません。お客様にて別途ご購入をお願いします。 |

AC アダプタを使用する場合、必ず付属の専用 AC アダプタを使用してください。PoE 受電を使用する場合、給電側のネットワーク機器が PoE 給電の機能をサポートしており、給電する最大電力を超えていないことを確認して使用してください。PoE 給電機能が搭載されたスイッチング HUB やインジェクターなどのネットワーク機器は、エレコム製品のご使用をお勧めします。

## 4.3. ネットワーク接続方法の選択

顔認証デバイスをネットワークに接続します。ネットワーク接続方法は「有線 LAN 接続」と「Wi-Fi」接続が利用できます。各接続方法に関する対応規格は（表 1）を参照して顔認証デバイスを導入する環境に適合するか確認してください。なお、顔認証デバイスは、固定 IP アドレスで運用してください。

（表 1）

| 有線 LAN の対応規格 | | Wi-Fi の対応規格 | |
|---|---|---|---|
| 通信方式 | 10baseT/100baseTX | 通信方式 | IEEE 802.11 a/b/g/n（2.4/5GHz） |
| 規格バージョン | IEEE802.3 | 認証方式 | OPEN/WEP/WPA-PSK/WPA2-PSK |
| MDI-X | 非対応 | 暗号方式 | CCMP（AES）/TKIP |
| PoE | PoE+ 25W（IEEE 802.3at） | 通信速度 | 最大 54Mbps |

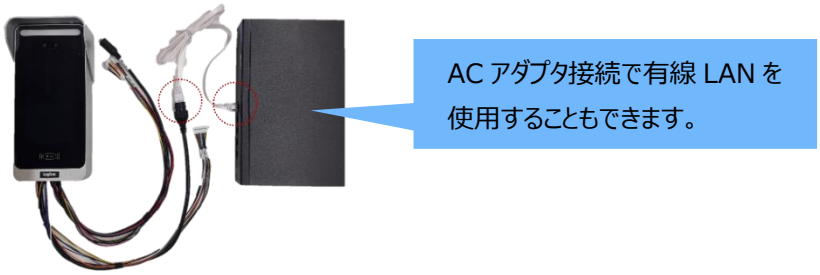
※Wi-Fi 接続の場合、管理ソフトと顔認証デバイスが相互通信するため、ネットワーク機器の設定が必要になる場合があります。
例）プライバシーセパレータ機能（Wi-Fi 接続端末同士の相互通信を遮断する機能）など
※付属の AC アダプタ―を利用の際、ネットワーク接続方法は Wi-Fi または有線 LAN のいずれも利用することができます。

**注意事項**

**＊1 顔認証デバイス及び管理ソフトが稼働するオンプレミスの PC/サーバーは、固定 IP アドレスで運用してください。固定 IP アドレスやゲートウェイの情報はネットワーク管理者へお問合せをお願いします。また、利用するネットワーク情報は、顔認証デバイスと管理ソフトが相互通信できるよう、予めアクセス制限などの環境設定を実施してから顔認証デバイスや管理ソフトの設定をお願いします。**

## 1. 有線 LAN 接続を設定する

① 顔認証デバイス側の LAN ポートへ LAN ケーブルを接続し、ネットワーク機器（ルーターやスイッチング HUB など）側にも LAN ケーブルを接続し顔認証デバイスとネットワーク機器を有線 LAN 接続します。




※写真は PoE 給電対応のスイッチング HUB と接続した例です

② 画面右下の「メインメニューアイコン※」→「セキュリティ警告」→「通信設定」→「イーサネット」をタップします。

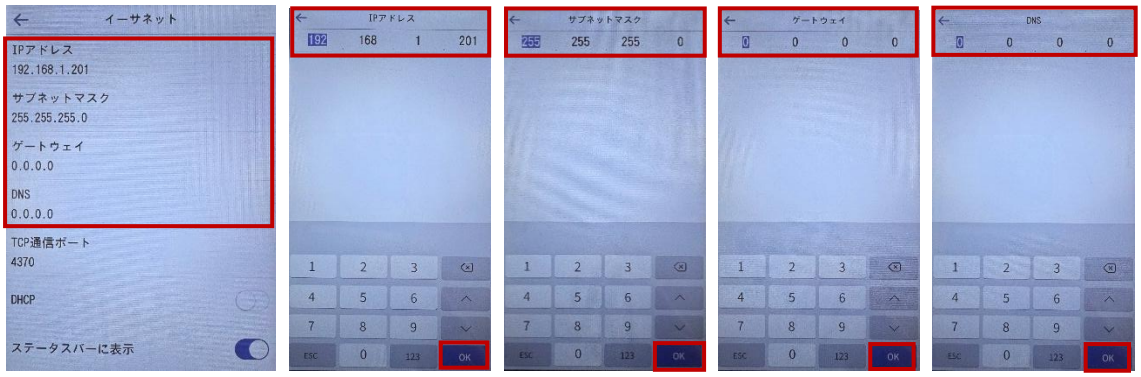



※スクリーンセーバーが表示されている場合は画面をタップします。

③ IP アドレスの取得方法*1 を選択します（初期値：固定 IP アドレス）。

④ 固定 IP アドレスで設定します。

(ア) 入力する各項目をタップして編集し、入力情報を保存するために「OK」ボタンをタップします。



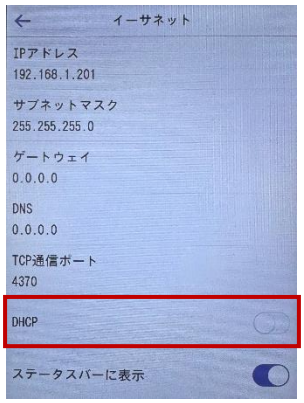

(イ) 画面左上の「戻る」ボタンをタップして、認証待機画面に戻ります。

※TCP 通信ポートは「初期値：4370」のままご使用ください。

⑤ DHCP による IP アドレスの自動取得をする場合（固定 IP アドレスを推奨します）

(ア) DHCP を「ON（有効）」にします。

(イ) DHCP を ON にするとネットワーク上のゲートウェイの情報および IP アドレスの情報を自動取得します。
自動取得した情報が設定したい内容と異なる場合は、④の（ア）固定 IP アドレスの設定で対応してください。




(ウ) 以上で設定は終わりです。画面左上の「戻る」ボタンをタップして、認証待機画面に戻ります。
※TCP 通信ポートは「初期値：4370」のままご使用ください。

## 2. Wi-Fi 接続を設定する（AC アダプタ接続の場合、有線 LAN の接続方法も選択できます）

① 顔認証デバイスの本体に付属の専用 AC アダプタを接続します。



② 画面右下の「メインメニューアイコン」→「セキュリティ警告」→「通信設定」→「Wi-Fi 設定」をタップします。



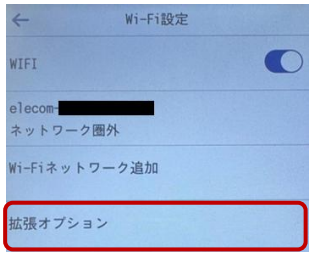

③ IP アドレスの取得方法*1 を選択します（初期値：固定 IP アドレス）。

**注意事項**

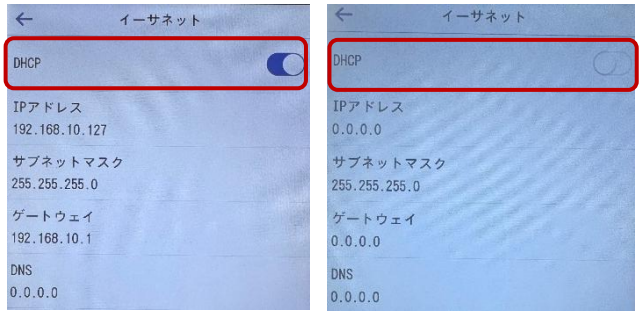
***1 顔認証デバイス及び管理ソフトが稼働するオンプレミスの PC/サーバーは、固定 IP アドレスで運用してください。固定 IP アドレスやゲートウェイの情報はネットワーク管理者へお問合せをお願いします。また、利用するネットワーク情報は、顔認証デバイスと管理ソフトが相互通信できるよう、予めアクセス制限などの環境設定を実施してから顔認証デバイスや管理ソフトの設定をお願いします。**

④ 固定 IP アドレスで設定します。

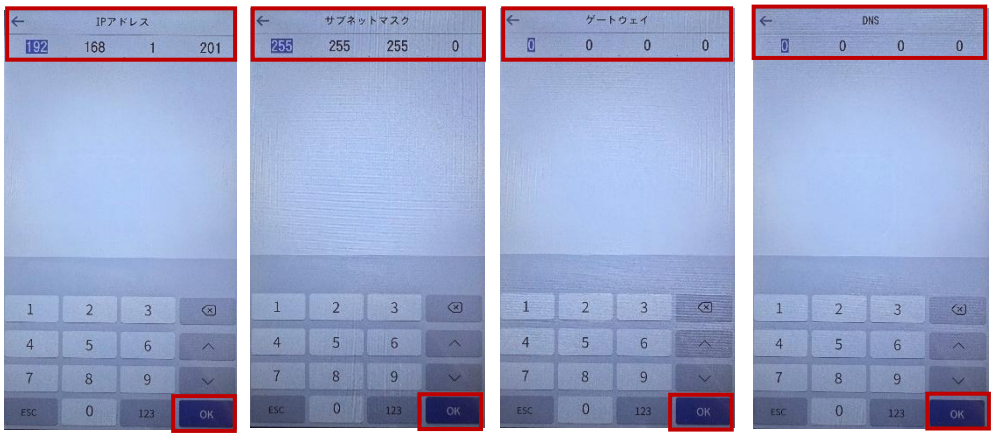
(ア) 画面右上のスクロールアイコン「 」で移動し末尾の「拡張オプション」のメニューで設定します。



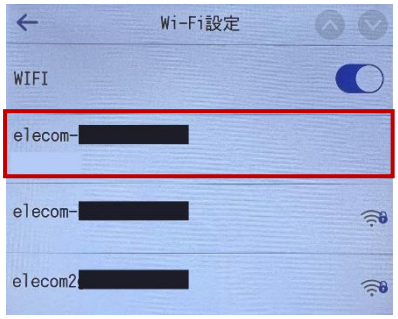

(イ) 「拡張オプション」をタップし、DHCP を「OFF（無効）」にします。



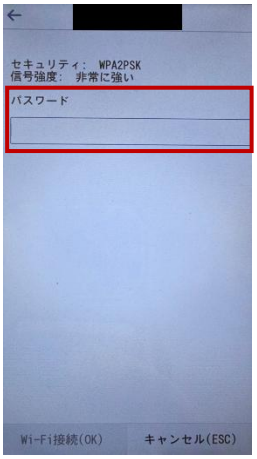

(ウ) 入力する各項目をタップして編集し、入力情報を保存するために「OK」ボタンをタップします。

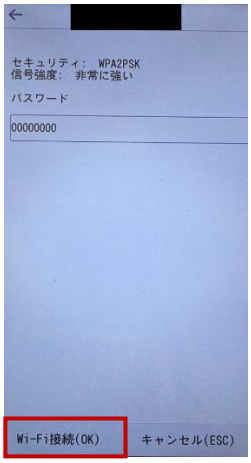



(エ) 画面左上の「戻る」ボタンをタップして SSID 一覧を表示する画面へ戻り、接続する SSID をタップします。



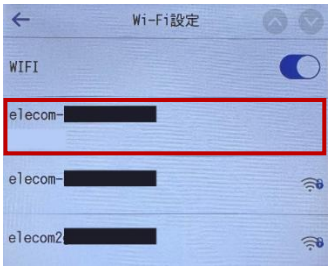
(オ) SSID に接続するためのパスワードを入力し、最後に「Wi-Fi 接続（OK）」をタップします。
接続状態が「接続中…」から「接続済み」になっていることを確認してください。



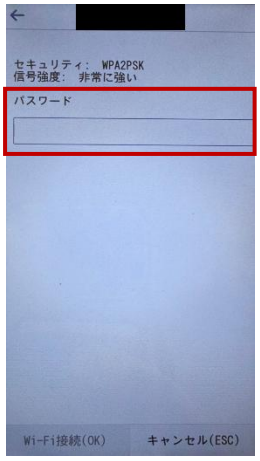



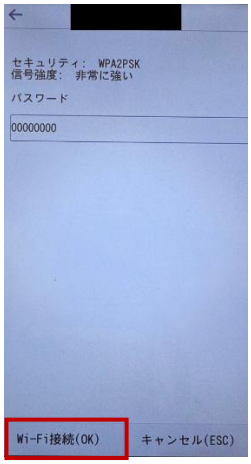

(カ) 以上で設定は終わりです。画面左上の「戻る」ボタンをタップして、認証待機画面に戻ります。

⑤ DHCP による IP アドレスの自動取得をする場合（固定 IP アドレスを推奨します）
(ア) SSID 一覧を表示し、接続する SSID をタップします。




(イ) SSID に接続するためのパスワードを入力し、最後に「Wi-Fi 接続（OK）」をタップします。
接続状態が「接続中…」から「接続済み」になっていることを確認してください。




以上で設定は終わりです。画面左上の「戻る」ボタンをタップして、認証待機画面に戻ります。

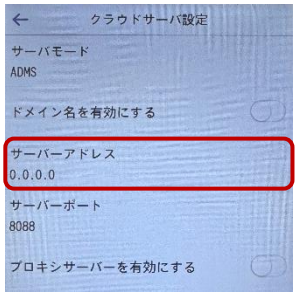
## 4.4. クラウドサーバの設定

顔認証デバイスと管理ソフトの通信設定を説明します。「クラウドサーバ」とは、管理ソフトをインストールするオンプレミスの PC/サーバーを指します。管理ソフトをインストールするオンプレミスの PC/サーバーは固定 IP アドレスで運用してください。

1. 画面右下の「メインメニューアイコン」→「通信設定」→「クラウドサーバ設定」をタップします。
   ※メインメニューの表示は無操作状態が 60 秒（初期値）続くとタイムアウトします。




2. サーバーアドレス*1 を設定します（管理ソフトが稼働するオンプレミスの PC/サーバーを指定します）。

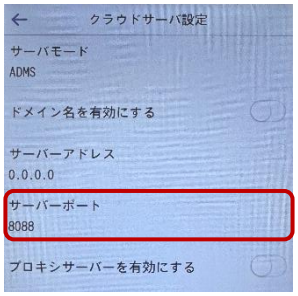



**注意事項**

***1 顔認証デバイス及び管理ソフトが稼働するオンプレミスの PC/サーバーは、固定 IP アドレスで運用してください。固定 IP アドレスやゲートウェイの情報はネットワーク管理者へお問合せをお願いします。また、利用するネットワーク情報は、顔認証デバイスと管理ソフトが相互通信できるよう、予めアクセス制限などの環境設定を実施してから顔認証デバイスや管理ソフトの設定をお願いします。**

3. サーバーポートを「8088」へ設定します（初期値：8088）

   ※ADMS ポート番号「8088」が利用できない場合は「11.2 サーバーポートの設定変更」を参照して変更してください。




**<ご参考>**

- ✓ デバイスの TCP/IP 通信が成功すると、待受画面の右上に アイコンが表示されます。
- ✓ サーバーとの通信に成功すると、待受画面の右上に アイコンが表示されます。

# 5. 管理ソフトの導入（初期設定）

管理ソフトをインストール*1 する PC またはサーバー機器は、顔認証デバイスと同一ネットワークまたは顔認証デバイスと相互通信できるネットワーク環境下に接続をします。また、管理ソフトをインストールする PC またはサーバー機器は、必ず固定 IP アドレスで運用をお願いします。

**注意事項**

***1 当社は管理ソフトの「セットアップウィザード」に従って初期値でインストールする方法のみをサポートします。データベースの変更やポート番号の変更など、初期値以外の設定でセットアップする場合はサポート対象外となります。お客様の責任の下、インストールをお願いします。**

## 5.1. 管理ソフトの動作環境要件

管理ソフトが動作するための最小構成要件を説明しています。

| 環境項目 | 最小構成要件 | |
|---|---|---|
| **管理ソフトに接続する顔認証デバイス数** | **1～50 台まで** | **51～200 台まで** |
| CPU | Intel® Core™ i5 Quad-core （4 コア） 2.8GHz 以上 | Intel® Core™ i5 Hexa-core （6 コア） 3.0GHz 以上 |
| システムメモリ | 8GB 以上 | 16GB 以上 |
| ディスクドライブ | HDD または SSD（推奨） | SSD |
| | データ領域 100GB 以上の空き領域<br>（システム領域の空き容量は 15GB 以上） | データ領域 200GB 以上の空き領域<br>（システム領域の空き容量は 30GB 以上） |
| サポート OS | Microsoft® Windows® 11<br>Microsoft® Windows Server® 2019<br>Microsoft® Windows Server® 2022<br>Microsoft® Windows Server® 2025 | |
| ネットワークカード | 推奨されるネットワーク速度は 1Gbps 以上 | |
| 液晶モニタ | 21.5 インチ以上で、解像度「1920×1080」、拡大縮小とレイアウト「100%」の設定を推奨します。その他の倍率で使用すると管理ソフトの画面表示が隠れてしまうなど、表示が異常になる場合があります。（ブラウザの拡大・縮小でも調整できます） | |
| インターネットブラウザ | Microsoft® Edge 89＋、Google Chrome® 84＋ | |
| データベース | PostgreSQL<br>※管理ソフトのインストール時に自動でインストール及びデータベースが構築されます。<br>※当社では PostgreSQL 以外のデータベースはサポートの対象外となります。 | |

## 5.2. 管理ソフトのダウンロード

1. 製品本体底面にあるシリアル番号（S/N）の番号を確認します。




2. 以下の Web ページへアクセスし、「１」のシリアル番号をフォームへ入力して「認証」をクリックします。
https://dl.logitec.co.jp/download.php?pn=LST-D-957



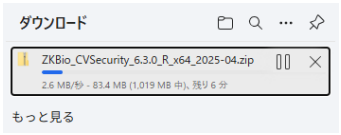

3. 認証後に表示されるページの「ダウンロード」の「ファイル名」をクリックし、ソフトウェア使用許諾契約書を表示します。
（ソフトウェアバージョンは一例です）



4. 「ソフトウェア使用許諾契約書」を必ずご一読いただき、「ソフトウェア使用許諾契約書に同意します。」へチェックを入れ「ダウンロードする」をクリックします。



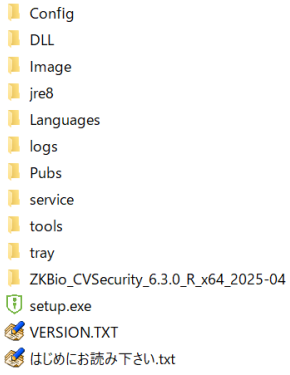

5. ダウンロードフォルダにダウンロードが開始されます。（画面例は Windows の場合です）




6. ZIP 圧縮ファイルを解凍します。（ソフトウェアバージョンは一例です）




7. 解凍すると「はじめにお読みください」のテキストファイルの他、インストールに必要なファイルが表示されます。
※フォルダ内の各種ファイルは、ダウンロードしたバージョンによって異なる場合があります。



## 5.3. 管理ソフトのインストール

**注意事項**

- ✓ **インストールする前に、システムにインストールされているウィルス対策ソフトを終了することをお勧めします。**
- ✓ **ウィルス対策ソフトが異常を検出する場合、プログラム及びフォルダの除外設定をお願いします。**

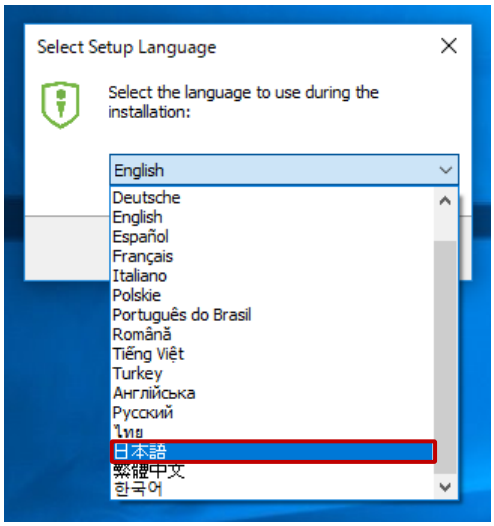
1. ダウンロードしたファイルを解凍し、フォルダ内の実行ファイル（setup.exe）をダブルクリックします。なお、ユーザーアカウント制御で「このアプリがデバイスに変更を加えることを許可しますか？」と表示される場合は「はい」をクリックします。

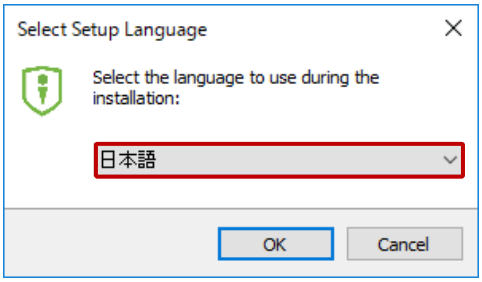



※管理ソフトのバージョンはダウンロードするタイミングで異なる場合があります。




2. セットアップおよび管理ソフトの使用言語（日本語）を選択し、「OK」をクリックします。日本語以外はサポート対象外です。



3. 管理ソフトをインストールするハードウェア環境が管理ソフトの動作に適した環境であるのかテストをします。Windows ファイヤーウォールなど、ウィルス対策ソフトがインストールされている場合は「警告」が表示されます。「無視」をクリックしてインストールを進めます。何らかの「エラー」が表示された場合は、判定結果（エントリ）をクリックして案内に従ってください。

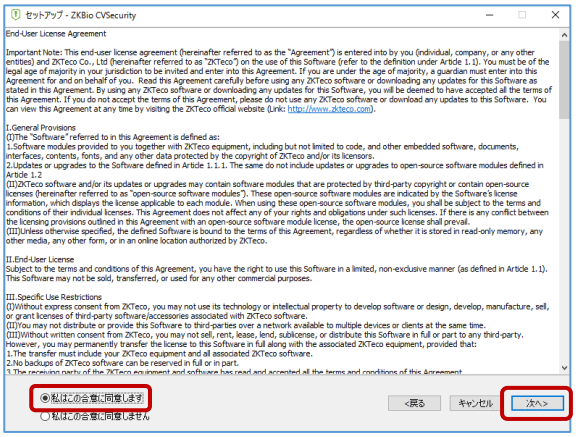



| テスト項目（略称） | 説明 |
|---|---|
| 管理ユーザー | インストールの実行アカウントが管理者権限であることを確認します。 |
| 環境変数 | 管理ソフトから設定する環境変数を確認します。 |
| ソフトウェアの競合 | 管理ソフトと競合するソフトウェアが存在しないのか確認します。 |
| サービスポート | 管理ソフトが使用する特定のポート番号が利用できるのか確認します。 |
| ウィルス対策ソフトウェア | ウィルス対策ソフトの有効・無効を確認します。通信許可など、管理ソフトの動作に必要な設定をします。 |
| 互換性 | 管理ソフトと互換性があるシステム（Windows 系 OS）であるのかを確認します。 |
| 利用可能なシステムメモリ | 管理ソフトが動作するために必要なシステムメモリ容量であるのかを確認します。インストール先の PC/サーバーに共存する別システムの使用分を除き、使用可能なメモリ容量を判定します。 |

4. セットアップウィザードを開始します。インストールを進める場合は「次へ」をクリックします。




5. ソフトウェア利用規約に同意いただきます。「私はこの合意に同意します」を選択して「次へ」をクリックします。



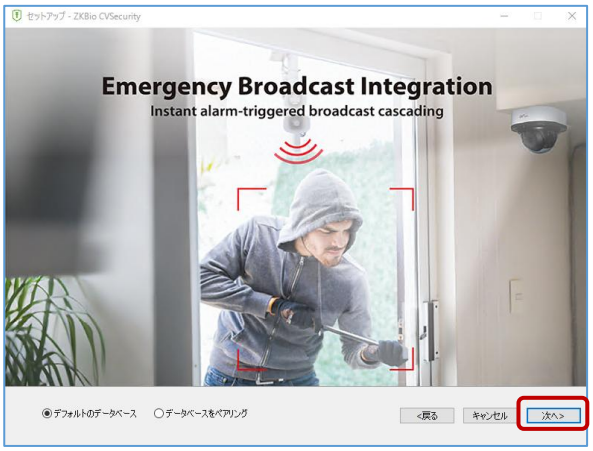
6. ネットワーク通信に関するポートの設定をします。初期値の状態で「次へ」をクリックします。
※【初期値】Web ポート：8098、Adms ポート：8088、ファイヤーウォールに例外を追加する：チェック、https を使用：チェック



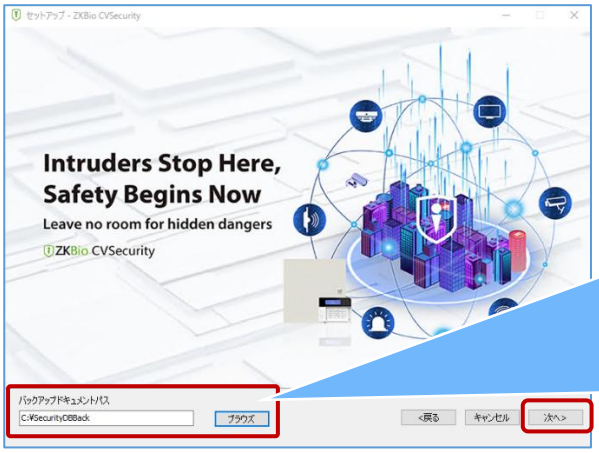

7. 管理ソフトのインストール先を指定します。インストール先の変更が必要な場合は「ブラウズ」をクリックし変更をしてください。変更しない場合は「次へ」をクリックします。（初期値：C:¥Program Files¥ZKBioCVSecurity）




8. 利用するデータベースを選択します。初期値の状態で「次へ」をクリックします。



9. バックアップ先のフォルダを指定します。バックアップ先*の変更が必要な場合は「ブラウズ」をクリックし変更をしてください。
変更しない場合は「次へ」をクリックします。（初期値：C:¥SecurityDBBack）

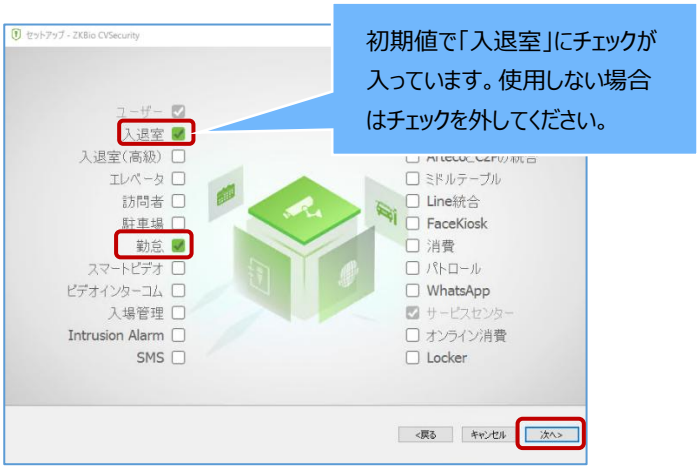



**＊バックアップドキュメントパスについて【重要】**

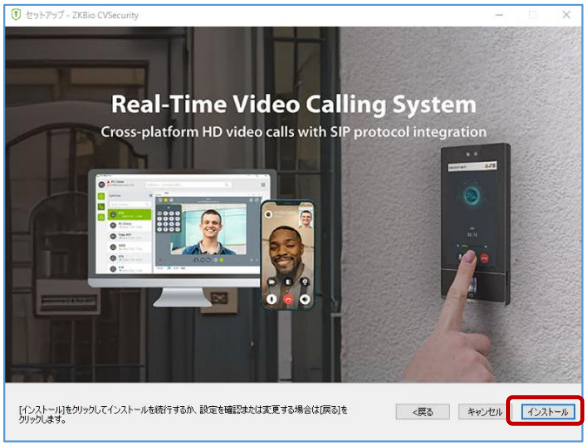
バックアップ（複製）とは、PC/サーバー機器の内部ストレージとは別の外部ストレージにバックアップを行ない、複製データを作成することをいいます。万が一、PC/サーバー機器が故障した場合、外部ストレージにある複製データから復元できます。

バックアップドキュメントパスは、管理ソフトのインストール後に「11.4 データベースのバックアップ先変更」の手順で変更することができますが、必ず外部ストレージを用意・接続してバックアップの設定をしてください。

10. サービスメニュー*の選択をします。「入退室」または「勤怠」、もしくは両方にチェックを入れて「次へ」をクリックします。
※管理ソフトの購入ライセンスの種類に従って選択します。ソフトウェアのバージョンにより、表示内容が異なる場合があります。




11. これまでの各種設定で問題がなければ「インストール」をクリックします。修正が必要な場合は「戻る」をクリックして該当箇所の修正をしてください（前項の手順に従ってやり直しをしてください）。



12. インストールが開始されます。完了するまで PC またはサーバー機器の操作は行わないようにしてください。




13. 下記の画面が表示されましたら「完了」をクリックして画面を閉じ、PC/サーバーを再起動してください。




以上で管理ソフトのインストールは終わりです。

## 5.4. 管理者アカウントの設定

1. 管理ソフトのインストールでデスクトップに作成された「ZKBio CVSecurity」のショートカットをダブルクリックします。管理ソフトのアドレスは初期値【https://localhost:8098/】です。localhost で管理画面が表示されない場合は管理ソフトをインストールしている PC/サーバーの IP アドレス【https://xxx.xxx.xxx.xxx:8098/】*を入力してアクセスします。

   ※インストール直後に管理ソフトを実行した後、管理画面にアクセスできるまで数分かかります。
   ※Web ポート番号「8098」が利用できない場合は「11.2 サーバーポートの設定変更」を参照して変更してください。

2. ブラウザ上で「接続がプライベートではありません」という警告が表示されます。

   ※ご使用のインターネットブラウザの種類により一部の表示内容が異なる場合があります。
   ※インターネットブラウザの画面及び記載されている IP アドレスは例です。localhost で管理画面が表示された場合は IP アドレスではなく localhost と表示されます。

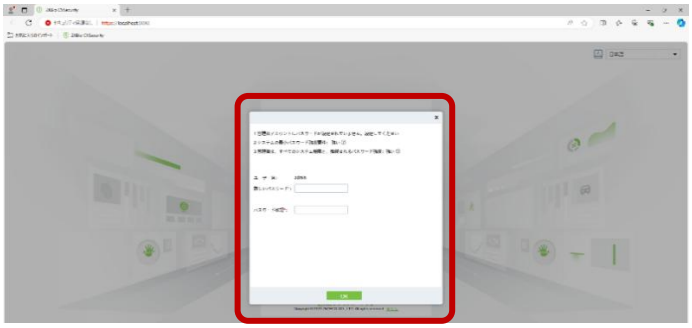
   ① 警告表示されたら「詳細設定」をクリックします。

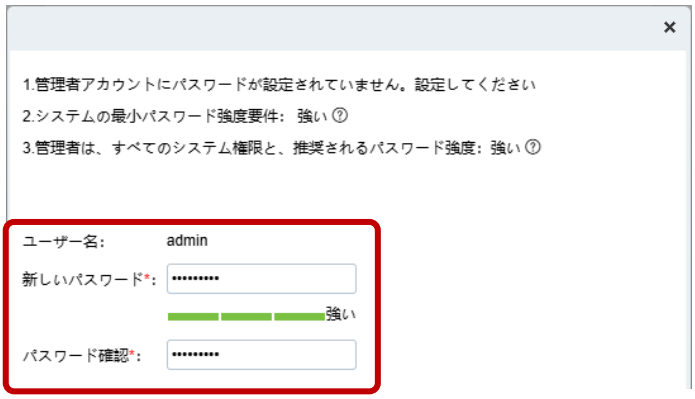



   ② 「192.168.2.155 に進む（安全ではありません）」をクリックします。
   ※IP アドレスは「localhost」と表示される場合もあります。



3. 管理画面が開きます。管理者アカウントのパスワードは、<パスワード要件>を参考に設定します。

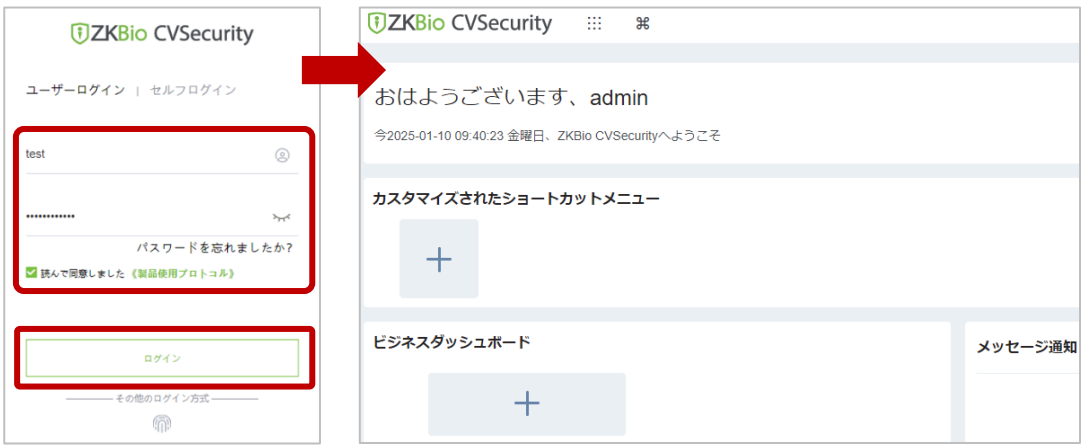





**<パスワード要件>**

| パスワード強度レベル | 設定条件 |
|---|---|
| 無し | パスワードを設定しません（推奨しません。必ずパスワードの設定をお願いします。） |
| 弱い | 8 文字以上で、数字、小文字、大文字、特殊文字から 2 種類以上を使用します。 |
| 中 | 8 文字以上で、数字、小文字、大文字、特殊文字から 2 種類以上を使用します。但し、数字と小文字だけの組み合わせは不可、数字と大文字を含める必要があります。 |
| 強い | 8 文字以上で、数字、小文字、大文字、特殊文字から 3 種類以上を使用します。 |

4. ユーザー名には「admin（初期値）」を入力、前項で設定した管理者パスワードを入力、同意事項にチェックを入れて、「ログイン」をクリックします。設定した管理者パスワードでログインできることを確認します。*




※セルフログインに関する説明は「7.5 勤怠打刻と勤怠履歴」を参照してください。

## 5.5. ライセンス認証

当社から案内されたライセンスキーを管理ソフトへ登録します。

1. ログイン後の画面で、右上「admin」メニュー内の「さらに」をクリックします。




2. オンライン認証をクリックします。

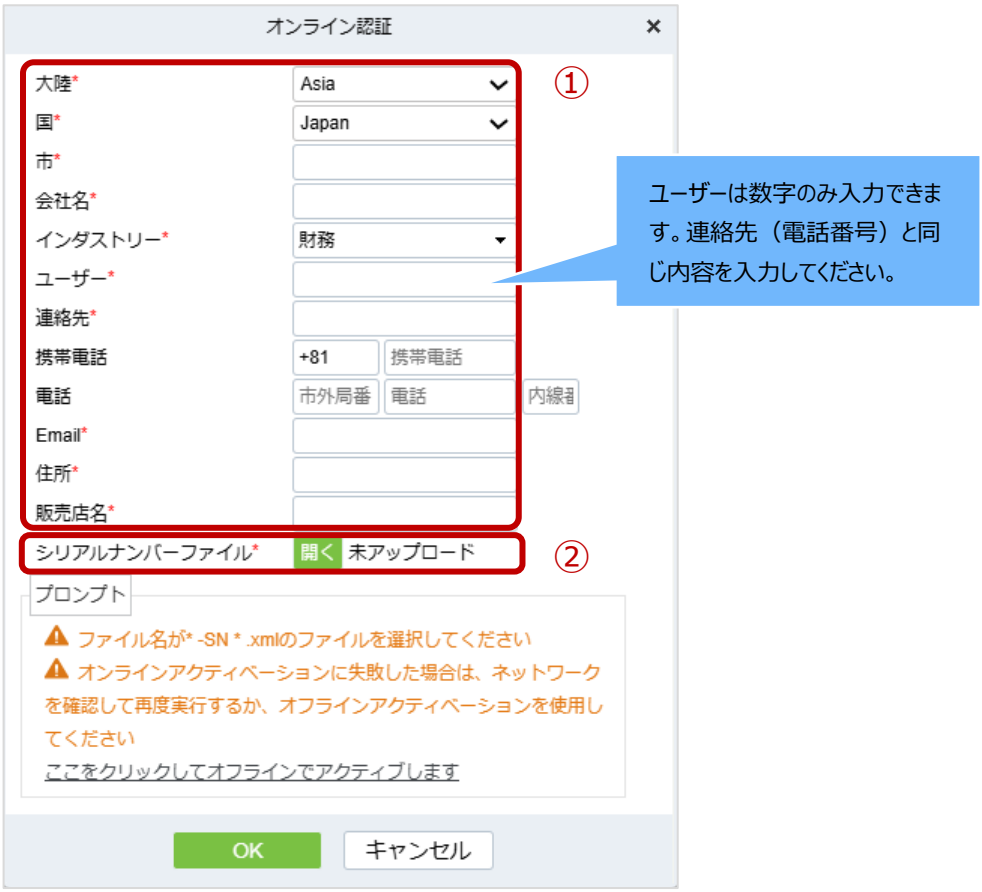



**注意事項**

**各管理メニュー（ライセンス情報詳細の各アイテム）のライセンス有効期限は、当社ではサポート対象外となります（ライセンス有効期限の表示に対応していません）。当社が規定するライセンス契約に従って、販売元のエレコム株式会社が管理します。**

3. 下記の情報やファイルを順番に設定します。

① ライセンスキーを所有するお客様の情報を入力します。
② 「開く」をクリックして、ご購入いただいたライセンスキー（XML ファイル）を選択します。




4. 最後に「OK」をクリックします。

**注意事項**

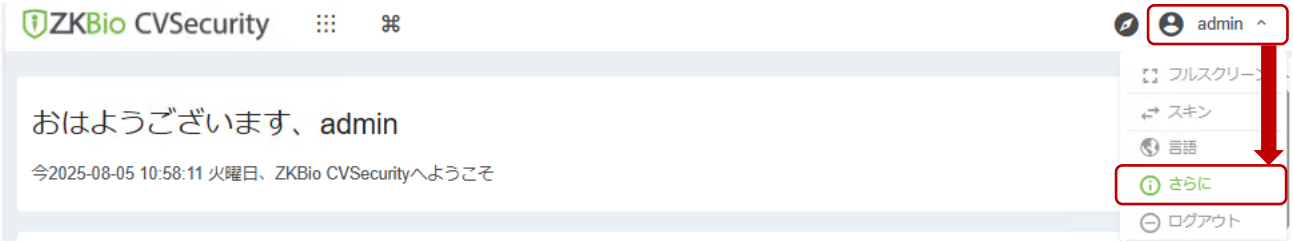
**オンライン認証で入力されたお客様情報及びライセンスキーは管理ソフトを有効化するために使用されます。特に、お客様情報は第三者へ情報が送信または開示されることはありませんのでご安心ください。**

## 5.6. ライセンス認証の解除

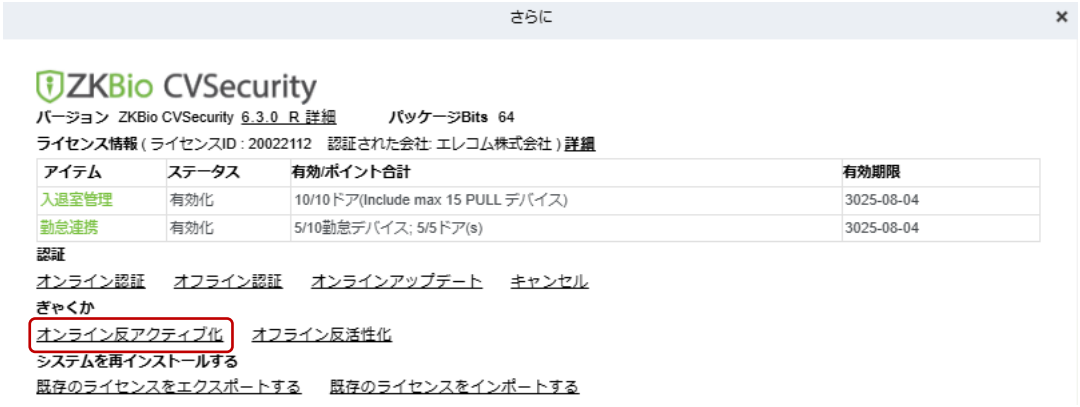
管理ソフトの年間利用契約について、契約更新を行わない場合にライセンス認証を解除する方法を説明します。当社の契約管理窓口から契約更新の 2 か月前に契約更新意思の確認をさせていただきます。契約を更新しない場合、下記手順に従ってライセンスの解除をお願いします。契約終了後も本手続きを行わなかった場合、ライセンス違反となりますのでご注意ください。

※契約満了月の翌月中にライセンス認証の解除が行われなかった場合、年額利用料をご請求させていただきます。
※当社で管理されている契約者以外の方へライセンスを譲渡することはできません。

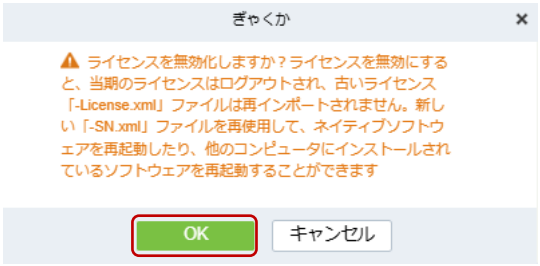
1. 管理ソフトへログインします。管理ソフトの画面右上の管理者アカウントをクリックして「さらに」をクリックします。



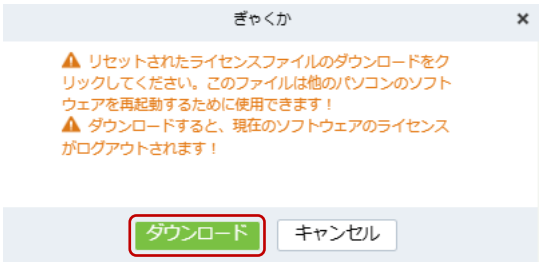

2. 「オンライン反アクティブ化」をクリックします。



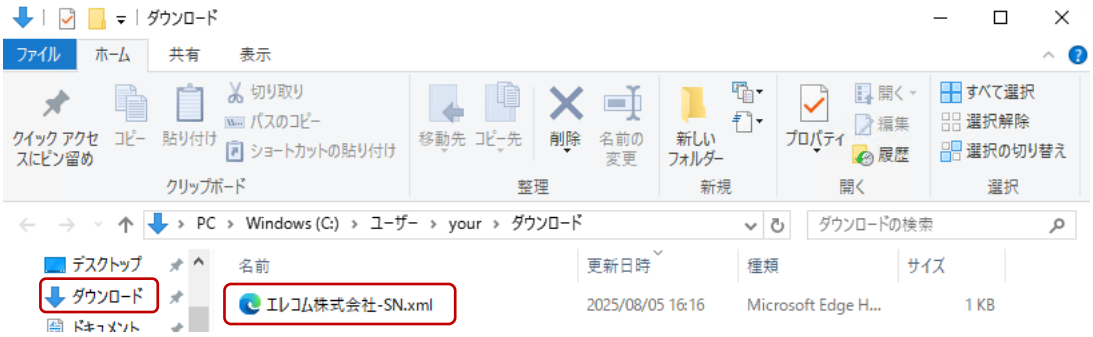

3. 「ライセンス無効化」の注意事項が表示されますので「OK」をクリックします。
※本手順により、一度ライセンスが無効になりステータスは「試用版」となります。



4. 認証済みのライセンスファイルを取得するために「ダウンロード」をクリックします。
※エクスポート先は、初期値で Windows の「ダウンロード」フォルダです。




例）ダウンロードしたライセンスファイル「xxx-SN.xml」




5. 手順 4 で取得したライセンスファイルを契約時に発行された「ライセンス証書」と一緒に下記窓口まで提出をお願いします。

**＜契約解除に提出が必要なもの＞**

✓ ライセンスファイル　例）xxx-SN.xml（xxx はライセンス認証時に入力した会社名になります）
✓ ライセンス証書　　管理ソフトの年間利用契約を締結した際に発行される証書

**＜提出先の窓口＞**

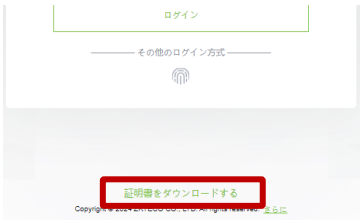
メールの件名は「年間利用契約の解除申請」を指定してください。

biometrics-support@elecom.co.jp

## 5.7. 自己署名証明書のインストール

セキュリティ強化のため、自己署名証明書（以下「証明書」という）*1 を PC またはサーバー機器及び PC またはサーバー機器と通信を行うクライアント機器にインストールすることで、管理ソフト（PC またはサーバー機器）との間で行われる通信を HTTPS 通信*2 で暗号化します。証明書のインストールは以下の通りです。

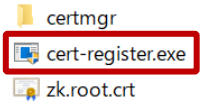
1. 管理ソフトが動作する PC またはサーバー機器へ証明書インストールソフトをダウンロードします。管理ソフトのログイン画面の下部にある「証明書をダウンロードする」をクリックします。

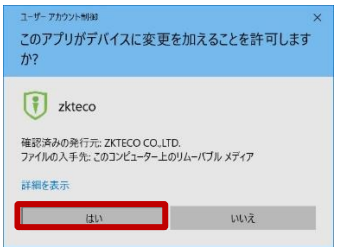



2. ダウンロードした ZIP（圧縮）ファイルを右クリックし、「すべて展開」から解凍します（圧縮・解凍ソフトが必要です）。
※Windows11 でも同様の操作をします（“すべて展開”をおこないとエラーでインストールできません）

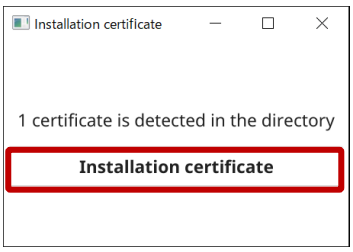



3. 解凍されたフォルダ内の「cert-register.exe」をダブルクリックします。なお、ユーザーアカウント制御で「このアプリがデバイスに変更を加えることを許可しますか？」と表示される場合は「はい」をクリックします。

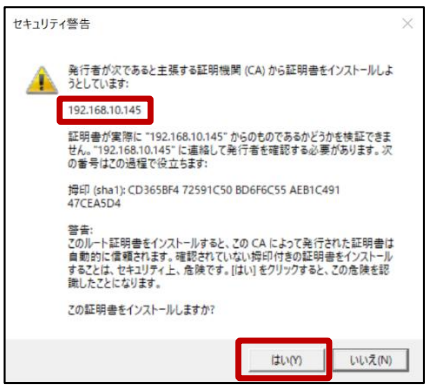


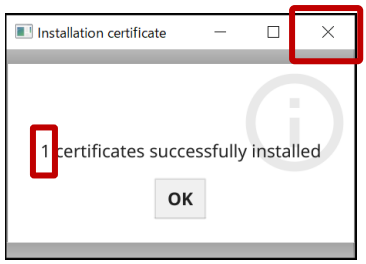

4. 「Installation certificate」をクリックします。*3



5. 「この証明書をインストールしますか？」というセキュリティ警告が表示されます。インストールを進める場合は「はい」をクリックします。（ご参考：証明書の発行元は PC またはサーバー機器の IP アドレスが表示されます）




6. 「1 certificates successfully installed」と表示されたらインストールは完了です。「×」をクリックして証明書インストールソフトを終了します。インターネットブラウザを一度閉じて、再起動してから管理画面へアクセスします。セキュリティ警告の表示が消えていることを確認します。




**注意事項**

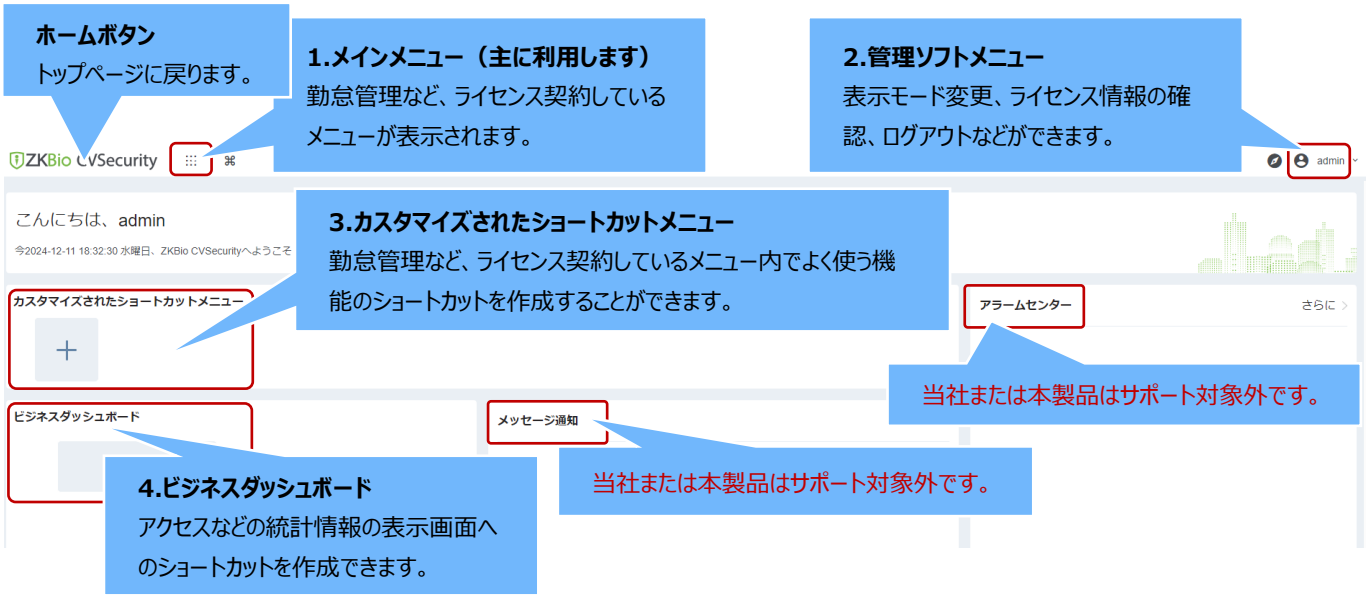
***1 デジタル署名の発行形態の一つです。本来の証明書は TLS／SSL 証明書は中間認証局（CA）が署名を行いますが、認証局を通さず、ウェブサイトの管理責任者が自身で発行した秘密鍵を用いて署名を行う仕組みです。本機能は、ローカルエリアネットワーク（LAN）内での使用を目的とした仕組みです。なお、自己署名証明書はアクセス元であるクライアント PC 毎にインストールする必要があります。**

***2 Web ブラウザと Web サイト間でデータを送受信するために使用されるプロトコルである HTTP を暗号化通信により、通信内容を暗号化したプロトコルです。これにより、HTTPS を利用して通信を行うことで通信内容を改竄／盗聴から守ることができます。**

***3 自己署名証明書をインストールした後、再度「cert-register.exe」を実行するとアンインストールすることができます。**

## 5.8. 管理ソフトの基本操作

管理ソフトの基本操作について説明します。初期設定で登録した管理ソフトの管理者ユーザー名とパスワードでログインします。
ログインに成功すると下図トップページに遷移します。（クッキーが有効の場合、ログアウト直前に操作していた画面が開きます）




### 1. メインメニュー

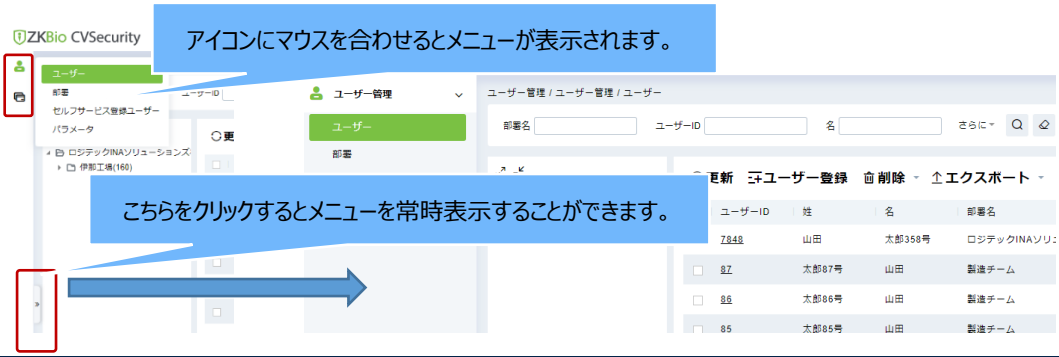
「⁞⁞」にマウスカーソルを合わせると、ライセンス契約しているメニューが表示されます。




| ライセンスメニュー | 内容 |
|---|---|
| ユーザー管理 | 顔認証デバイスを利用するユーザーを管理するメニュー（登録、編集など）です。 |
| 入退室管理（年間利用料が必要です） | 顔認証デバイスで入退室管理をするメニュー（デバイス管理、アクセス権など）です。<br>※アクセスコントロールモジュールセットアップウィザードが表示されたら閉じてください。 |
| 勤怠連携（年間利用料が必要です） | 顔認証デバイスで勤怠管理をするメニュー（デバイス管理、レポートなど）です。 |
| システム管理 | 管理ソフトの共通設定メニュー（運用設定など）です。 |

#### ① ユーザー管理

ユーザー管理に必要な共通設定（パラメータ）や部署設定などができます。



② **入退室管理（年間ライセンスが必要です）**

入退室管理に必要な共通設定（パラメータ）や詳細なアクセス権限などを管理できます。




③ **勤怠連携（年間ライセンスが必要です）**

勤怠管理に必要な共通設定（パラメータ）やデバイス管理ができます。




④ **システム管理**

管理ソフト（システム）の共通設定（パラメータ）やバックアップ、導入前の基本設定ができます。




## 2. 管理ソフトメニュー



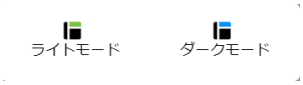

| 項目 | 内容 |
|---|---|
| フルスクリーン | ディスプレイに合わせて管理ソフトを全画面表示することができます。 |
| スキン | ライトモード（初期値）とダークモードを選択できます。 |
| 言語 | 管理ソフトで表示する言語を選択できます。 |
| さらに | 管理ソフトのライセンス情報を確認できます。 |
| ログアウト | 管理ソフトからログアウトします。 |

① **フルスクリーン**

ディスプレイに合わせて管理ソフトを全画面表示することができます。全画面表示を終了するにはキーボードの「ESC（エスケープ）」を押すか、マウスを全画面表示している画面の上部へ移動すると表示する「×」をクリックします。

② **スキン**

管理ソフトの基調色について、ライトモード（初期値）とダークモードを選択できます。モードを切り替える場合、いずれかをクリックします。




**<ライトモード>**




**<ダークモード>**




③ **言語**

管理ソフトの表示言語を選択できます。（当社または本製品は日本語のみをサポートします）




④ **さらに**

管理ソフトのライセンス認証やライセンス情報を表示します。

**注意事項**

***ライセンス期限は表示内容と提供期限が異なります。お客様の契約期間はエレコム株式会社で管理します。契約期間等のお問合せは、最寄りのエレコム営業窓口へお問合せください。**



⑤ **ログアウト**

管理ソフトからログアウトをします。管理画面の無操作状態が 30 分継続すると強制ログアウトになります。但し、アクセスのリアルタイムモニタリング、マップの画面を表示している場合、管理画面の無操作状態が 30 分継続しても強制ログアウトされません。

### 3. カスタマイズされたショートカットメニュー

各ライセンスメニューの中のよく使う項目をショートカットとしてトップページに表示することができます。これにより迅速に必要な機能の操作が行えるようになります。追加したいメニューを選択して「OK」をクリックします。




※ショートカットを削除する場合は、ショートカットを削除するには、ショートカットへマウスカーソルを合わせ、右上「×」をクリックします。




※ショートカットを作成できる数は最大 10 個です。

### 4. ビジネスダッシュボード

当社または本製品はサポート対象外です。

### 5. メッセージ通知

当社または本製品はサポート対象外です。

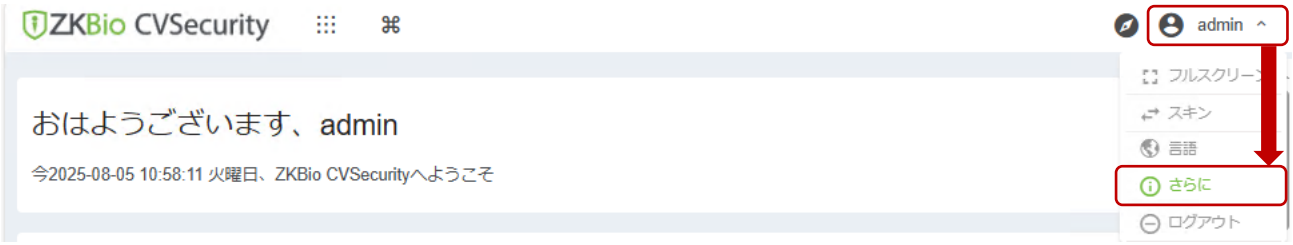
### 6. アラームセンター

当社または本製品はサポート対象外です。

## 5.9. 管理ソフトの再インストール

同じ PC/サーバーへ管理ソフトを再ストールする手順を説明します。なお、再インストール前に、必ず手動バックアップを実行します。バックアップ方法は「9.1.2 データ管理」の「すぐにバックアップ（手動）」を参照してください。

1. 管理ソフトへログインします。管理ソフトの画面右上の管理者アカウントをクリックして「さらに」をクリックします。

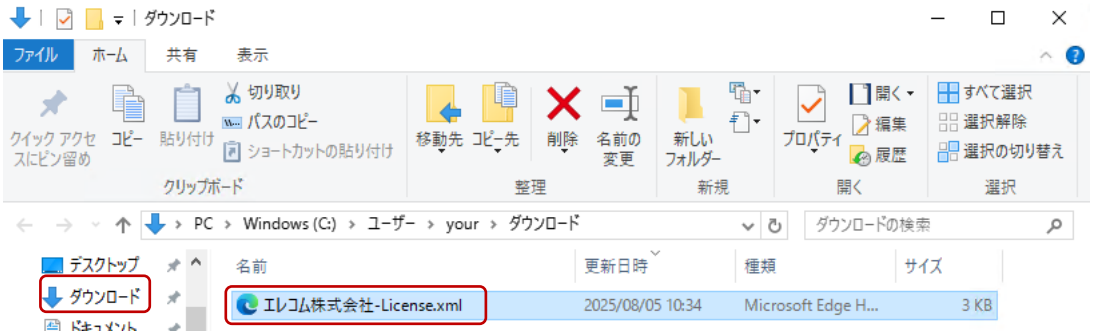



2. 「システムを再インストールする」から「既存のライセンスをエクスポートする」をクリックして、認証済みのライセンスをエクスポートします。

※エクスポート先は、初期値で Windows の「ダウンロード」フォルダです。

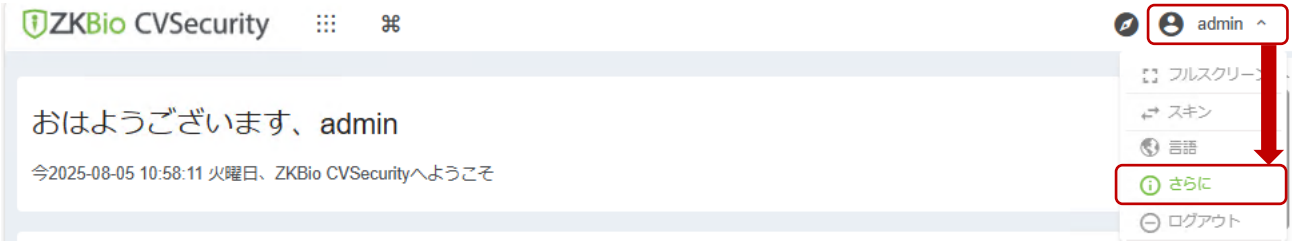



例）ダウンロードしたライセンスファイル「xxx-License.xml」



3. 管理ソフトを再インストールします。インストール手順は「5.3 管理ソフトのインストール」を参照してください。

4. 管理ソフトの再インストールが完了したら、管理ソフトへログインします。管理ソフトの画面右上の管理者アカウントをクリックして「さらに」をクリックします。



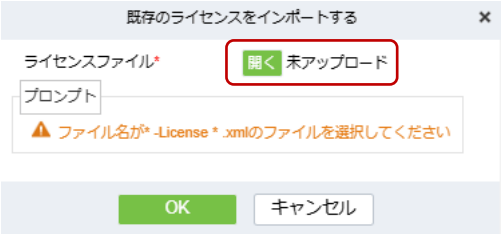

5. 「システムを再インストールする」の「既存のライセンスをインポートする」をクリックします。

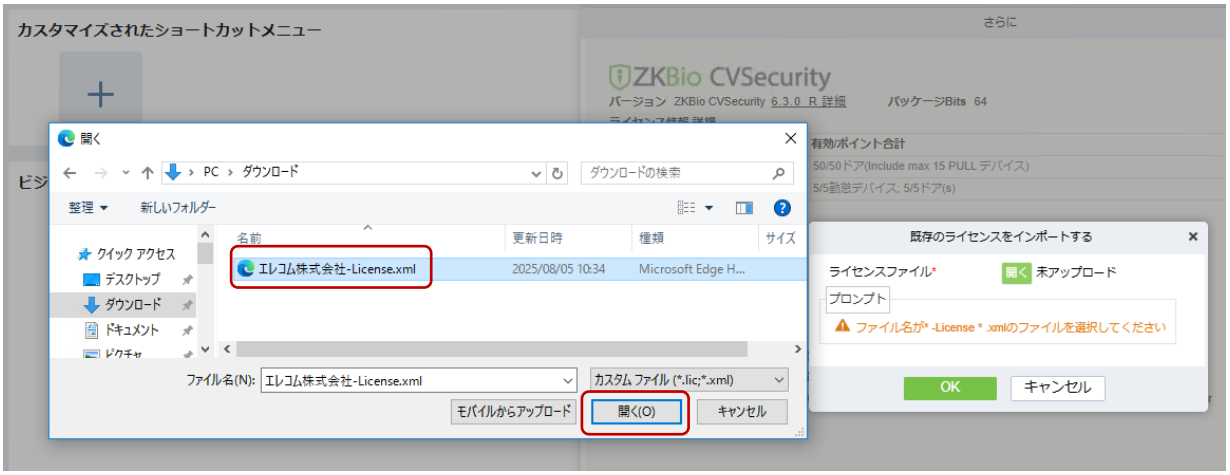
※ライセンス認証前はステータスが「試用版」と表示されます




6. 「既存のライセンスをインポートする」ための画面が表示されます。「開く」をクリックして、エクスポートしたライセンスファイルを選択して「開く」をクリックします。

※ライセンスファイル名は「xxx-License.xml」となります。xxx はライセンス認証時に登録した会社名です。

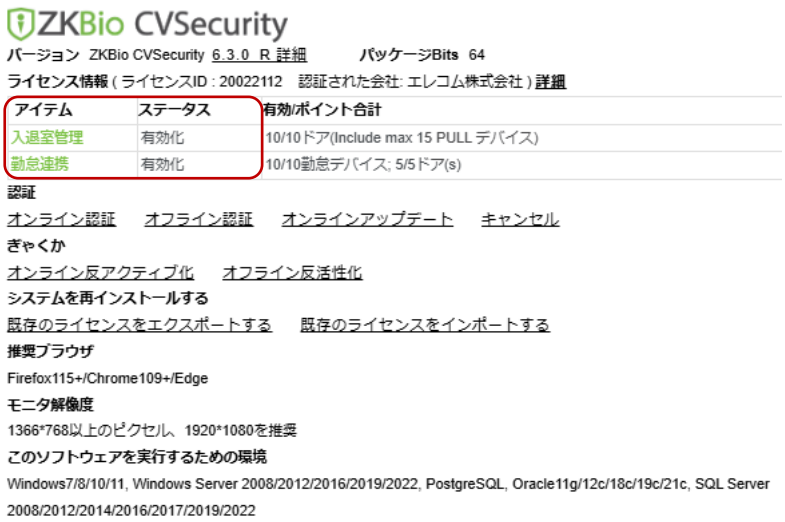





7. 選択したライセンスファイルを確認し、問題が無ければ「OK」をクリックします。




8. インポートが完了するとライセンス情報を表示する画面に戻ります。「ステータス」を確認して「試用版」から「有効化」になっていることを確認してください。



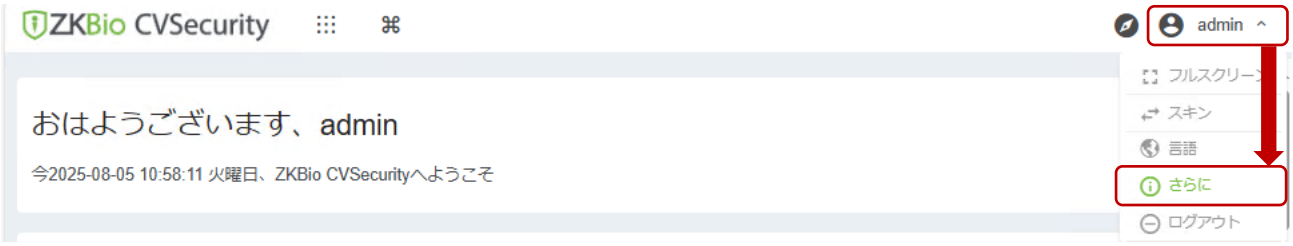

※必要な場合、バックアップから復元を行います。復元手順は「11.5 データベースの復元」を参照してください。

## 5.10. 管理ソフトが稼働する PC/サーバーの入れ替え

PC/サーバーのパーフォーマンスが低下した場合など、元の PC/サーバーから新しい PC/サーバーへライセンスを移行する手順を説明します。なお、入れ替え作業の前に、必ず手動バックアップを実行します。バックアップ方法は「9.1.2 データ管理」の「すぐにバックアップ（手動）」を参照してください。

※当社で管理されている契約者以外の方へライセンスを譲渡することはできません。ライセンス違反となりますのでご注意ください。

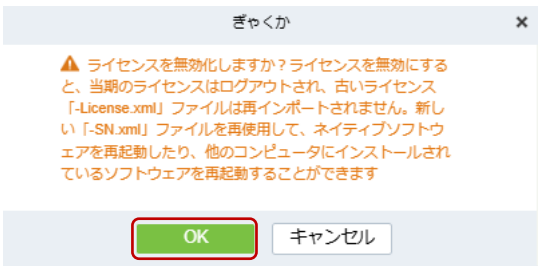
1. 管理ソフトへログインします。管理ソフトの画面右上の管理者アカウントをクリックして「さらに」をクリックします。



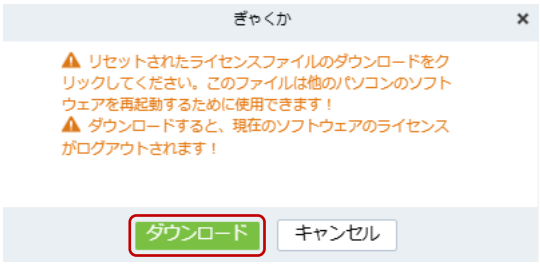

2. 「オンライン反アクティブ化」をクリックします。



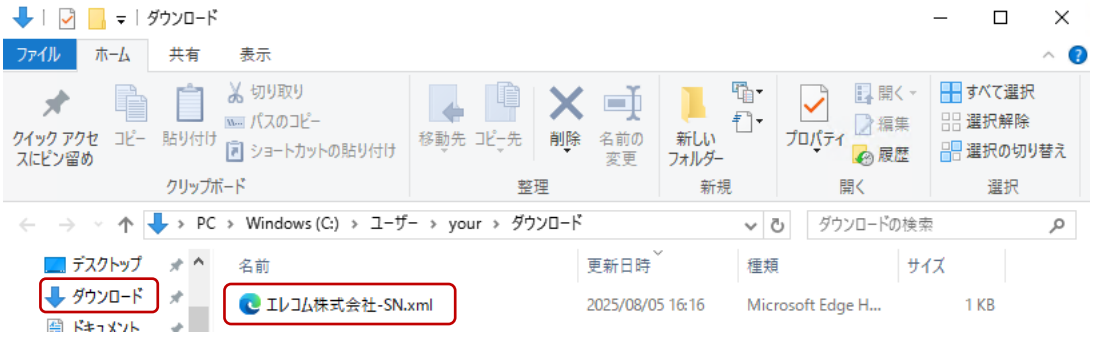

3. 「ライセンス無効化」の注意事項が表示されますので「OK」をクリックします。
※本手順により、一度ライセンスが無効になりステータスは「試用版」となります。



4. 認証済みのライセンスファイルを取得するために「ダウンロード」をクリックし、ダウンロードしたファイルは新しい PC/サーバーへ移行してください。 ※エクスポート先は、初期値で Windows の「ダウンロード」フォルダです。

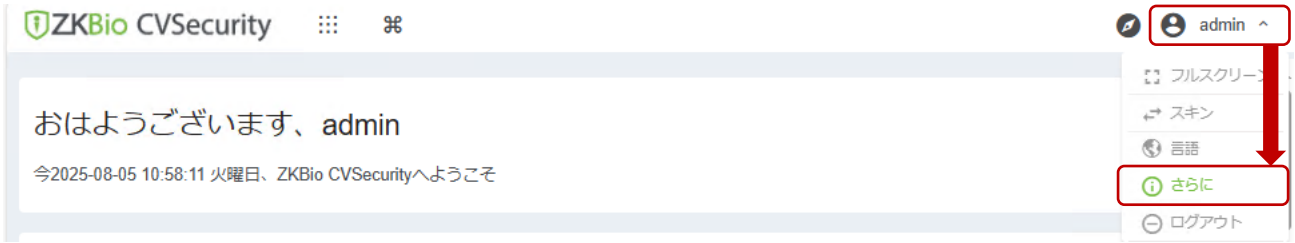



例）ダウンロードしたライセンスファイル「xxx-SN.xml」




5. 新しい PC/サーバーへ管理ソフトをインストールします。インストール手順は「5.3 管理ソフトのインストール」を参照してください。

6. 管理ソフトへログインします。管理ソフトの画面右上の管理者アカウントをクリックして「さらに」をクリックします。




7. 「オンライン認証」をクリックします。



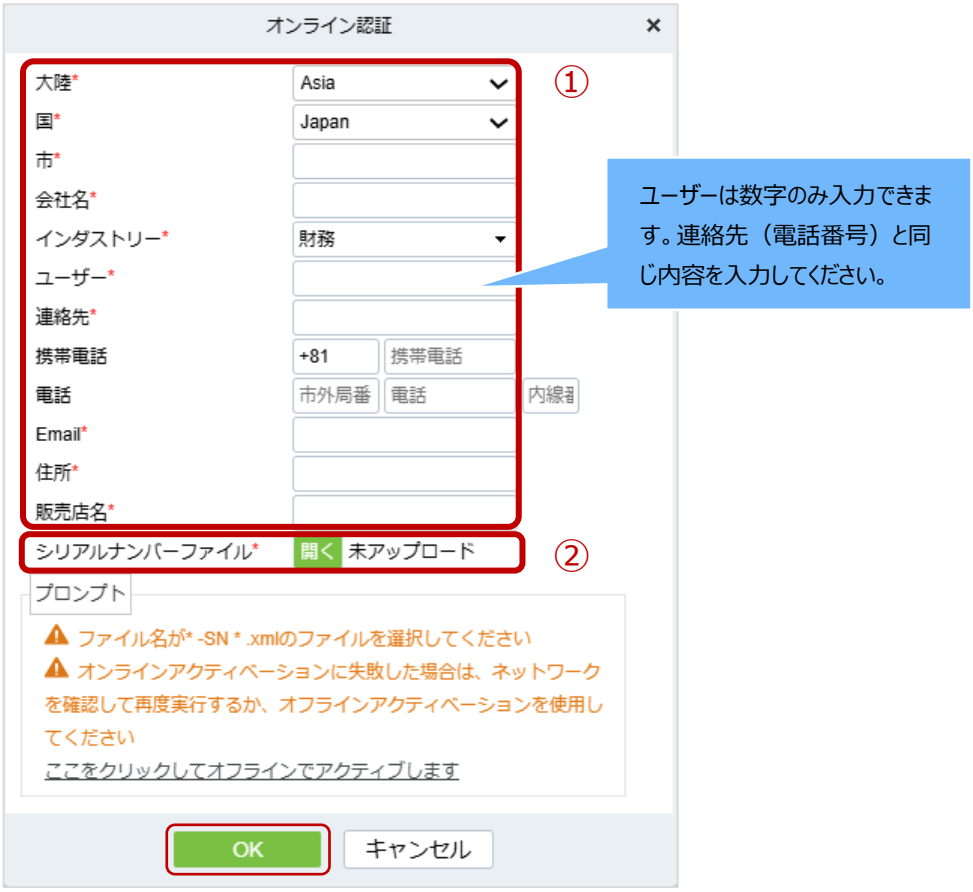
8. 下記の情報やファイルを順番に設定します。

① ライセンスキーを所有するお客様の情報を入力します。

② 「開く」をクリックして、手順 4 でダウンロードしたライセンスファイルを選択します。

※ライセンスファイル名は「xxx-SN.xml」となります。xxx はライセンス認証時に登録した会社名です。

③ 全ての情報を入力したら「OK」をクリックします。




9. ライセンス認証が完了するとライセンス情報を表示する画面に戻ります。「ステータス」を確認して「試用版」から「有効化」になっていることを確認してください。




※必要な場合、バックアップから復元を行います。復元手順は「11.5 データベースの復元」を参照してください。

# 6. ユーザー登録（勤怠/入退 共通）

ユーザー情報を登録*するための設定を説明します。「STEP 番号」をクリックすると各項目の説明へジャンプします。

**注意事項**

***ユーザー登録する情報で、ユーザー番号、顔情報、掌情報、カード No（IC カード）、Email は重複して登録することができません。**
***最大ユーザー登録数は 30,000 人です。なお、顔認証デバイス（LTC-FPT50/IPV2）側の認証方式の登録数の上限（顔：10,000／掌：5,000／IC カード：50,000）とは異なりますので注意が必要です。**

**STEP1**

- 使用メニュー：システム管理 > システム管理 > データ管理
- 内容：**自動バックアップを設定する**

**STEP2**

- 使用メニュー：システム管理 > システム管理 > エリア設定
- 内容：**顔認証デバイスで勤怠管理または入退室管理するエリアを設定する**

**STEP3**

- 使用メニュー：ユーザー管理 > ユーザー管理 > 部署（**設定省略可**）
- 内容：**お客様の組織に合わせて部署を設定する**

**STEP4**

- 使用メニュー：ユーザー管理 > ユーザー管理 > ユーザー > ユーザーインポート
- 内容：**ユーザー情報の一括登録（テキスト情報のみ）**

**STEP5**

- 使用メニュー：ユーザー管理 > ユーザー管理 > ユーザー > ユーザー写真インポート
- 内容：**ユーザーの顔登録をする（顔認証の場合）**

## 6.1. 自動バックアップ

ユーザー登録 STEP 一覧に戻る

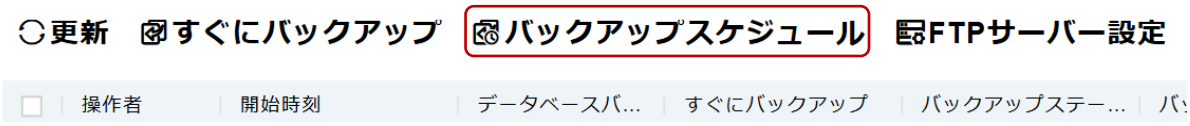
**【管理ソフト：システム管理 ＞ データ管理 ＞ バックアップスケジュール】**

各種設定を行う前に管理ソフト上に保存されたデータベースのバックアップの設定をします。万が一のデータ消失に備えて、必ず定期的な手動バックアップまたは自動バックアップの設定をしてください（詳細は「9.1.2 データ管理」を参照してください）。




指定した日時と間隔でデータベースのバックアップを自動で作成します。バックアップの作成先は、管理ソフトのインストール時に設定したバックアップ先（初期値：C:¥SecurityDBBack）です。インストール時に変更されている場合は、変更したバックアップ先が初期値になりますので、変更先のフォルダをご確認ください。

① 「バックアップスケジュール」をクリックします。

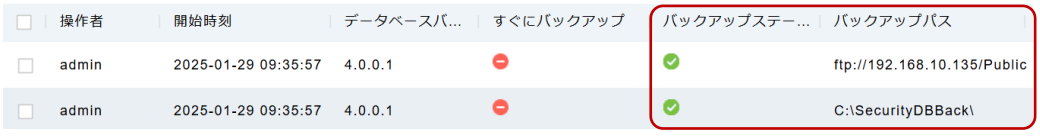



② バックアップスケジュール設定画面が開きます。From で「開始日時」を指定し、バックアップの作成間隔を「日数」で指定します。「同時に FTP サーバーにバックアップ」にチェックを入れると、「C:¥SecurityDBBack」と「FTP サーバー設定※」で指定した FTP サーバーへバックアップを作成します。最後に「OK」をクリックします。

※予め FTP サーバー設定がされていない場合、チェック時にエラーとなります。



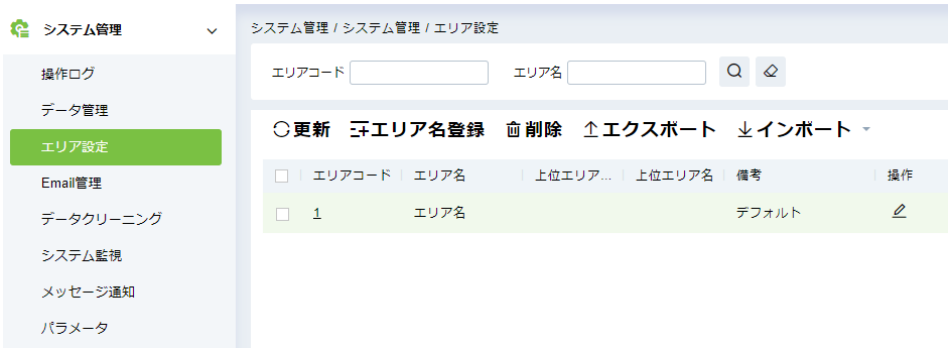

③ スケジュール通りバックアップが実行された場合、バックアップの実行日時などの情報が記録されます。「バックアップステータス」に緑チェックが表示されていれば、バックアップは正常に完了しています。



## 6.2. エリア設定

ユーザー登録 STEP 一覧に戻る

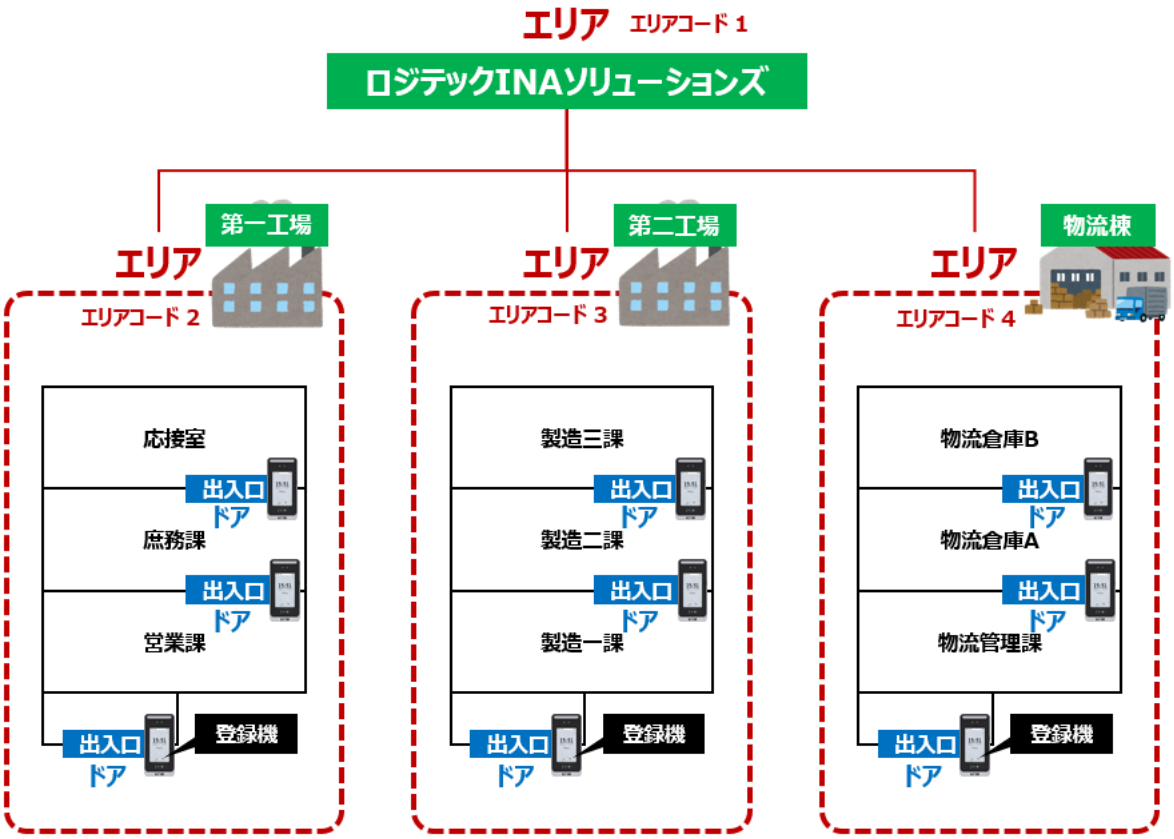
**【管理ソフト：システム管理 ＞ システム管理 ＞ エリア設定】**




「エリア」とは、顔認証デバイスを導入して管理する「拠点」を示します。初期値で「エリア名」というエリアが設定されています。エリア名は、顔認証デバイスを設置した拠点名を登録します。複数の拠点がない場合、初期値の「エリア名」というエリアをお客様の社名に変更して使用します。拠点が複数ある場合は拠点毎にエリア名を設定します*。

**注意事項**

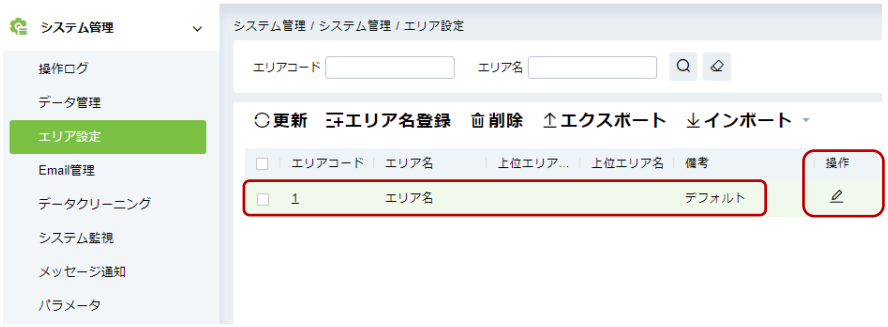
***外部の勤怠管理または入退室管理システムの一部では、このエリア設定で設定されたエリアコードで勤務場所を特定します。お客様の運用に応じてエリア名とエリアコードの設定をお願いします。**



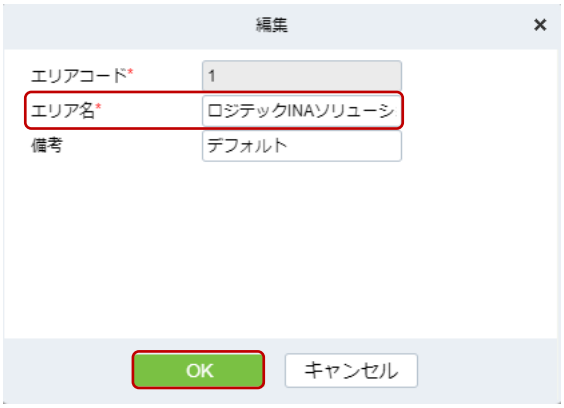
## 1. 初期値（エリア名）の変更

顔認証デバイスで勤怠または入退室管理を行う拠点が１つの場合、管理ソフトに初期値で登録されている「エリア名」というエリアを編集します。

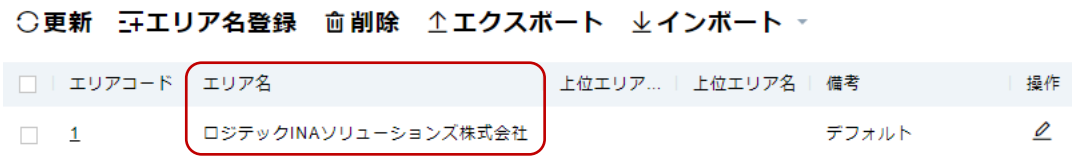
① 初期値で登録されている「エリアコード１ ：エリア名」を、お客様の会社名などに変更します。
変更するには「操作」の「編集」をクリックします。




② 編集画面が開いたら、エリア名を変更します。例は「ロジテック INA ソリューションズ株式会社」です。
設定を保存するには「OK」をクリックします。
※初期値で登録されているエリアコード「１」は編集することはできません。




③ 設定が反映されていることを確認します。



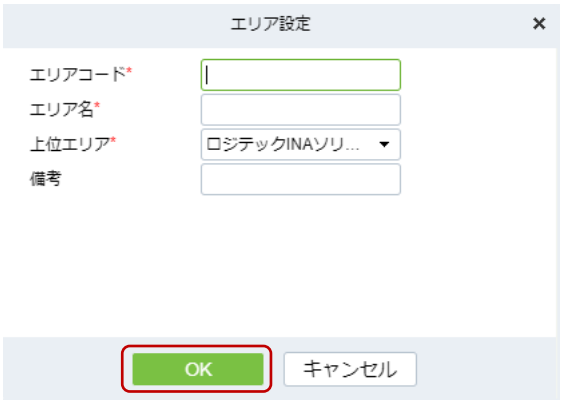
## 2. エリア名登録

顔認証デバイスで勤怠管理または入退室管理を行う拠点が複数の場合、前項「**1.初期値（エリア名）の変更**」の手順に加え、拠点数分のエリアを登録します。




※最上位エリアは複数登録することはできません。

① 「エリア名登録」をクリックし、「エリアコード」「エリア名」を入力します。上位エリアを変更する場合は「上位エリア」から選択してください。




| 設定項目 | 内容 |
|---|---|
| エリアコード* | 1～30 字の半角英数字を指定します。 |
| エリア名* | 1～30 文字を入力します。 |
| 上位エリア* | 登録するエリアの上位エリアを指定します。 |
| 備考 | 1～50 文字の自由入力欄です。 |

*印は必須です

エリアコード「１」を編集する場合は、「上位エリア」は表示されません。

**登録例）**

| エリアコード | エリア名 | 上位エリア... | 上位エリア名 | 備考 | 操作 |
|---|---|---|---|---|---|
| 1 | ロジテックINAソリューションズ株式会社 | | | デフォルト | |
| 2 | 第一工場 | 1 | ロジテックINA | | |
| 3 | 第二工場 | 1 | ロジテックINA | | |
| 4 | 物流棟 | 1 | ロジテックINA | | |

② 「OK」をクリックします。

エリア名登録は、以上で終わりです。

## 6.3. 部署を設定する ※本手順は省略することができます

ユーザー登録 STEP 一覧に戻る

**【管理ソフト：ユーザー管理 ＞ ユーザー管理 ＞ 部署】**

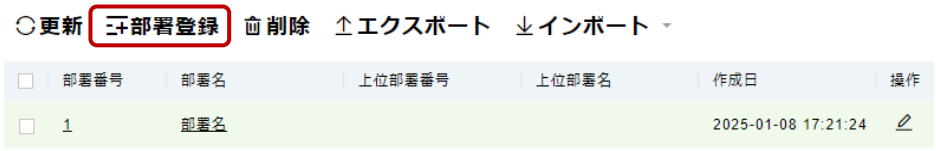
管理ソフト上でお客様の会社組織に合わせて部署を設定することができます。通常は「初期値：部署名」のまま利用するため本設定は省略することができます。管理ソフト上の部署設定となるため、外部勤怠管理または入退室管理システムとの連携に必要な設定ではありません。なお、管理ソフト上もお客様の会社組織に合わせて設定する場合は以下の通りです。



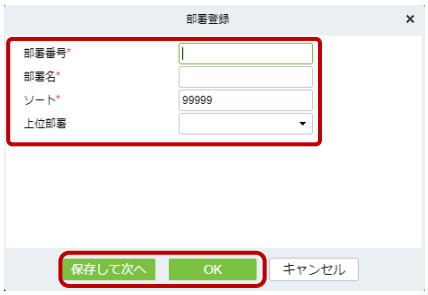

### 1. 部署登録

新規に部署を登録する場合は「部署登録」をクリックします。

※初期値の「部署名」の名称変更する場合は「操作」の「編集」をクリックしてください。新規に追加する部署との関連性が分かり易くなります。




部署番号（重複なし）、部署名、ソート順、必要な場合は上位部署を選択し「OK」をクリックします。続けて部署を登録する場合は「保存して次へ」をクリックします。




| 設定項目 | 内容 |
|---|---|
| 部署番号* | 半角英数字 1～30 文字 |
| 部署名* | 全角かな 1～200 文字、半角英数字 1～100 文字 |
| ソート* | 半角数字 1～999999 の間で指定します |
| 上位部署 | 表示される部署のリストから選択します |

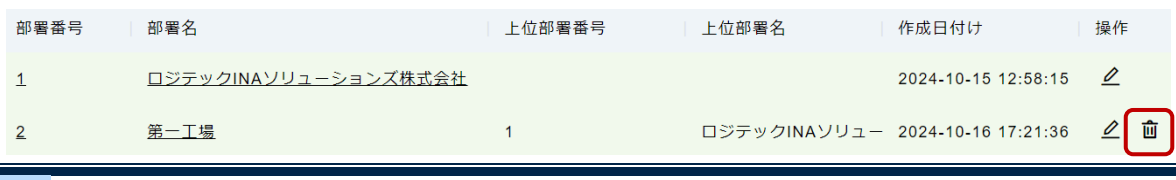
*は必須項目です。

部署登録の説明は、以上で終わりです。

### 2. 削除

該当部署の「ゴミ箱」アイコンをクリックします。

※初期値で登録されている「部署名」は削除することはできません。



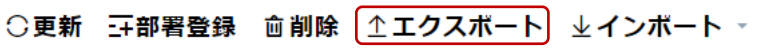
確認画面が表示されるので削除をする場合は「OK」をクリックします。削除しない場合は「キャンセル」をクリックします。

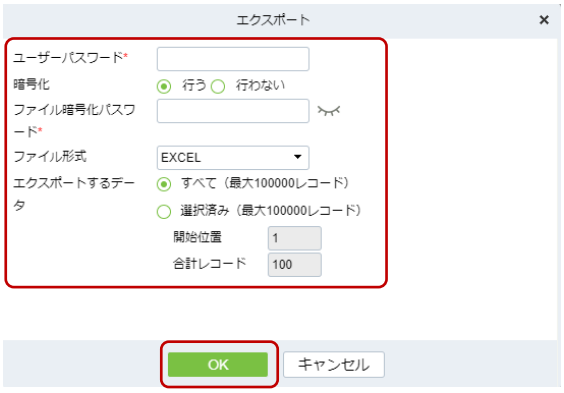



削除の説明は、以上で終わりです。

### 3. エクスポート

登録した部署の一覧を EXCEL・PDF・CSV・TXT のいずれかの形式でエクスポートすることができます。各条件を指定して最後に「OK」をクリックします。エクスポートしたファイルはブラウザで指定したダウンロードファイルの保存先へ保存されます。なお、暗号化した場合、Windows 標準の解凍ツールは使用できません。



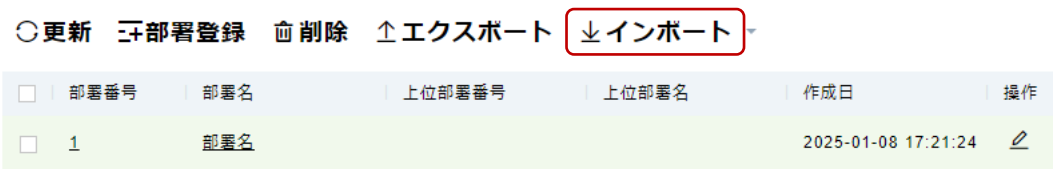

| 設定項目 | 内容 |
|---|---|
| ユーザーパスワード* | 管理者ユーザーのパスワードを入力します。 |
| ファイル暗号化 | データの暗号化を指定します。 |
| ファイル暗号化パスワード* | ファイル暗号化を指定した場合、復号化するパスワードを指定します。 |
| ファイル形式 | EXCEL・PDF・CSV・TXT から選択します。 |
| エクスポートするデータ | すべて：最大 10 万件を上限にの全データをダウンロードします。 |
| | 選択済み：開始レコードと上限（終了レコード）を指定してダウンロードします。 |

*印は必須です

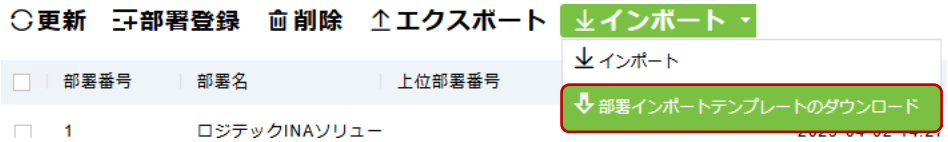
エクスポートの説明は、以上で終わりです。

### 4. インポート

インポート用のフォーマットを使用して一括登録することができます。既に登録されている情報がある場合は上書き保存されます。




インポートテンプレートをダウンロードします。



インポートテンプレート：　部署テンプレート_20241017132655.xls

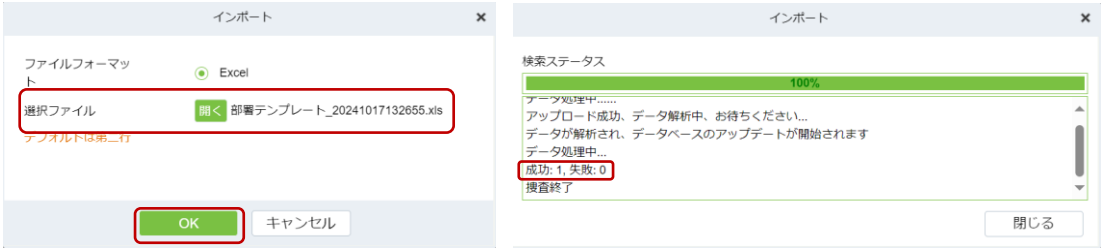
ダウンロードしたインポートテンプレートに情報を入力して「上書き保存」します。

| | A | B | C | D |
|---|---|---|---|---|
| 1 | 部署テンプレート | | | |
| 2 | 部署番号 | 部署名 | 上位部署番号 | 上位部署名 |
| 3 | | | | |
| 4 | | | | |

「インポート」をクリックします。




「開く」をクリックし、インポートするインポートテンプレートを選択します。最後に「OK」をクリックします。
インポートの進捗が表示され、最後にインポート結果が表示されます。




インポート後、正常に部署が登録されているかを確認してください。

| 部署番号 | 部署名 | 上位部署番号 | 上位部署名 | 作成日付け | 操作 |
|---|---|---|---|---|---|
| 1 | ロジテックINAソリューー | | | 2024-10-15 12:58:15 | |
| 2 | 商品開発部 | 1 | ロジテックINAソリューー | 2024-10-17 13:31:29 | |

インポートの説明は、以上で終わりです。

## 6.4. ユーザー情報の一括登録

ユーザー登録 STEP 一覧に戻る

**【管理ソフト：ユーザー管理 ＞ ユーザー管理 ＞ ユーザー ＞ インポート】**

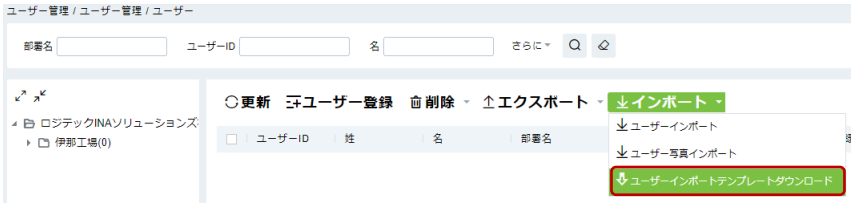
テンプレートを使用したユーザー情報の一括登録手順について説明します。

※ユーザー登録前に、ユーザーID の入力ルール（英数字または数字）を決める必要があります。「ユーザー管理 ＞ パラメータ」にある「ユーザーID 設定」を参照して運用開始前に設定をします。なお、運用中に入力ルールは変更できません。

**注意事項**

**ユーザー登録方法は、重複及び既存情報の上書きを避けるため、次のいずれかの方法で統一してください。**
**管理ソフトで個別登録：個別登録及び一括登録で登録されたユーザー情報内で重複をチェックしません**
**管理ソフトで一括登録：個別登録及び一括登録で登録されたユーザー情報内で重複をチェックしません**
**セルフサービス登録　：セルフサービス登録で登録されたユーザー情報内で重複をチェックしません**
**端末で登録　：管理ソフトからデバイスに同期されたユーザー情報内で重複をチェックします**

1. 「ユーザーインポートテンプレートダウンロード」をクリックします。




2. 選択操作ができない項目はテンプレートに出力されます。その他の入力項目（電話番号、カード No、Email）は、必要に応じて選択し「OK」をクリックします。




3. ユーザーインポートテンプレートのフォーマットに従ってユーザー情報を入力します。

※ユーザーID、姓、名、部署 No、所属部署は必須です。ユーザーID、カード No、Email は重複して登録することはできません。ユーザーID は、先頭 8 または 9 から始まる ID は別システムメニューの予約番号です。入退または勤怠メニューでは影響なく使用することができます。

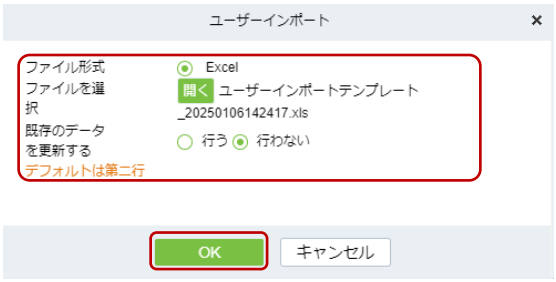
※「6.3 部署を設定する　※本手順は省略することができます」で部署設定を行なっていない場合、部署 No は「1」を指定します。



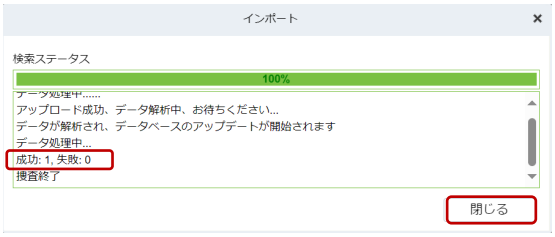
4. ユーザーインポート
「ユーザーインポートテンプレート」を使ってユーザー情報を入力したファイルをインポートします。「ユーザーインポート」をクリックします。




5. インポートするユーザーインポートテンプレートを選択します。既存のデータを上書き更新する場合は「行う」、上書き更新しない場合は「行わない（初期値）」を選択し、最後に「OK」をクリックします。




6. インポートの結果が表示されます。問題がなければ「閉じる」をクリックします。エラーメッセージが表示された場合は対象行に対して修正して再登録を行います。



## 6.5. 顔認証を利用する場合

ユーザー登録 STEP 一覧に戻る

顔認証を利用する場合は、続けて顔写真の登録を行います。「15 付録 C 顔登録ガイドライン」に従って顔写真の撮影をすることで、登録方法による認証精度に違いはありません。

### 1. ユーザー写真インポート（顔認証を利用する場合）

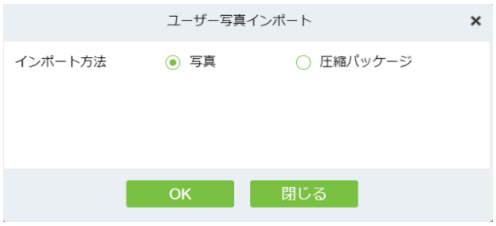
**注意事項**

**＊写真データ名は、ユーザーID を指定します。**
**＊データ形式は JPG／PNG でフル HD（1920×1080）以上、データ容量 5MB 未満を推奨します。**
**＊写真データ名には特殊文字が使用されていないことを確認してください。**
**＊一度に選択できる写真データは、499 枚です。500 枚以上の写真データを選択しないようにしてください。**

① 「ユーザー写真インポート」をクリックします。




② ユーザー写真インポートの画面が表示されます。




| 設定項目 | 内容 |
|---|---|
| 写真 | 非圧縮の写真データをそのまま複数選択してインポートします。 |
| 圧縮パッケージ | 写真データを 1 つの ZIP 形式の圧縮ファイル（500MB 以下）でインポートします。 |

**【インポート方法が「写真」の場合】**

(ア) 「写真を選択してください」をクリックして写真を選択します。キーボードの「shift」キーを押して複数選択できます。



(イ) 選択した写真に問題がなければ「アップロードを開始」をクリックします。

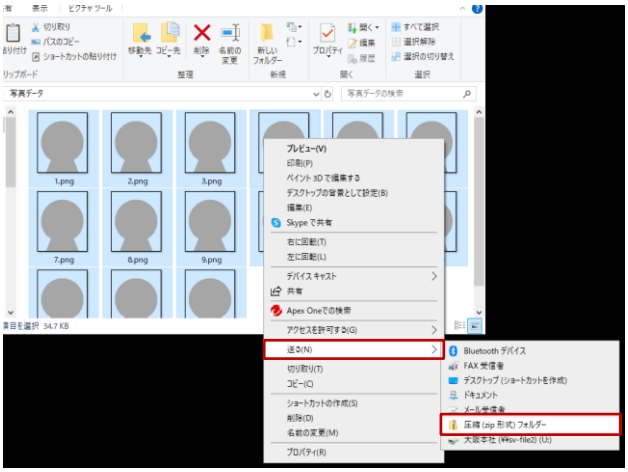



(ウ) アップロードが完了しましたら、アップロード結果を確認して「×」をクリックします。写真アップロード結果で「エラープロンプト」が表示されている場合、エラー情報を確認して登録写真を変更してください。




**【インポート方法が「圧縮パッケージ」の場合】**

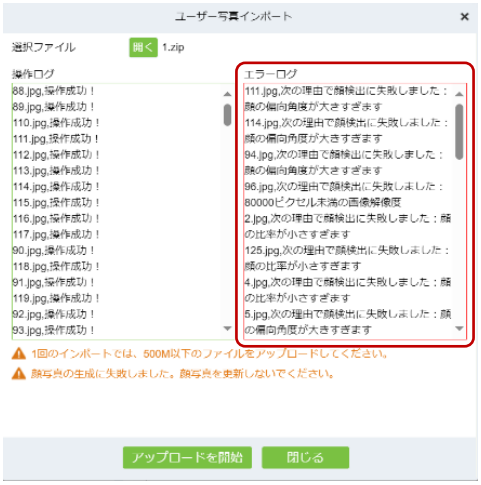
(ア) 写真データを ZIP 形式の圧縮ファイルにします。圧縮ファイルの中身は「フォルダ」構造をサポートしていません。圧縮する写真データを全て選択し、右クリックから ZIP 形式の圧縮ファイルを作成します（Windows の場合）



(イ) ユーザー写真インポート画面が表示されたら「開く」をクリックし、上記の（ア）で作成した ZIP 形式の圧縮ファイルを選択します。最後に「アップロードを開始」をクリックします。




(ウ) エラーログで「エラープロンプト」が表示されている場合、エラー情報を確認して登録写真を変更してください。



**＜エラープロンプト一覧表＞　※「顔登録ガイドライン」を参照して写真の撮り直しをお願いします。**

| No | エラー内容 | 対応方法 |
|---|---|---|
| 1 | 80000 ピクセル未満の画像解像度 | 1920×1080 ピクセル/5MB 未満の写真を使用します。 |
| 2 | 顔が検出されませんでした | 何らかの理由で顔を検出できません。 |
| 3 | 複数の顔が検出されました | 背景等にモノや人物が写り込んでいます。 |
| 4 | 顔の比率が小さすぎます（顔の縮尺が小さすぎる） | 顔が小さく、顔の特徴量を抽出できません。 |
| 5 | 画像は非カラー画像です | カラー写真を使用してください。 |
| 6 | 画像がぼやけている | 顔登録ガイドラインに従って再撮影します。 |
| 7 | 画像がかなり露出している | 露出が高い状態、白飛びして顔の特徴量が抽出できません。 |
| 8 | 画像が暗すぎる | 顔の特徴量が抽出できません。 |
| 9 | ノイズの多い写真 | 鮮明でないため、顔の特徴量が抽出できません。 |
| 10 | 伸ばした顔（顔写真が伸びすぎている） | 広角などの特殊撮影は顔の特徴量が抽出できません。 |
| 11 | 顔が覆われています | 帽子やサングラスなど、顔を覆っているものを外します。 |
| 12 | 過剰な笑顔 | 平常時の表情で、顔登録ガイドラインに従って再撮影します。 |
| 13 | 顔の偏向角度が大きすぎます | 正面を向き、肩を水平にして再撮影します。 |
| 14 | 画像の明るさが重要（画像が明るすぎる） | 蛍光灯や太陽光等の光源が写真に写っています。 |
| 15 | 面切り不良タイプ | 顔の一部が検出できません。 |
| 16 | 写真の形式が正しくありません。JPG/ PNG 形式のファイルをアップロードしてください | JPG/ PNG 形式のファイルを再アップロードしてください。 |

※ユーザー登録が無い ID に対して登録を行うと、以下のエラーが表示します。

例）ユーザーID：1 の場合
1.png,ユーザーID1 は存在しません。データ処理できません！

**参考**　**顔認証デバイスを使って顔登録する場合は「7.6 顔認証または他の認証を利用する場合」を参照してください。**

# 7. 勤怠連携（導入編）

勤怠管理おいて必要最低限の初期設定について説明します。「STEP 番号」をクリックすると各項目の説明へジャンプします。
管理ソフトの詳細設定は、管理ソフトの各機能の詳細を説明する「9 管理ソフトの機能説明」を参照してください。

**STEP1**
- 使用メニュー：顔認証デバイス ＞ メインメニュー ＞ システム設定
- 内容：**デバイスタイプを設定する**

**STEP2**
- 使用メニュー：管理ソフト ＞ 勤怠連携 ＞ デバイス管理 ＞ デバイス登録
- 内容：**エリア毎に顔認証デバイスを登録する**

**STEP3**
- 使用メニュー：管理ソフト ＞ 勤怠連携 ＞ デバイス管理 ＞ エリア別ユーザー登録
- 内容：**登録済みユーザーをエリアに振り分ける**

**STEP4**
- 使用メニュー：管理ソフト ＞ 勤怠連携 ＞ デバイス管理 ＞ デバイス登録
- 内容：**打刻方法の設定**

**STEP5**
- 使用メニュー：管理ソフト ＞ 勤怠連携 ＞ 勤怠レポート ＞ トランザクション
- 内容：**勤怠打刻と勤怠履歴を確認する（運用開始）**

**STEP6**
- 使用メニュー：顔認証デバイス ＞ メインメニュー ＞ ユーザー管理
- 内容：**掌・ICカードなどの登録**

## 7.1. 顔認証デバイス設定（勤怠 Push）

勤怠連携（導入編）STEP 一覧に戻る

顔認証デバイスは「入退室管理」または「勤怠管理」の利用シーンに応じて、予め運用モード「入退 Push または勤怠 Push（初期値：入退 Push）」を設定する必要があります。

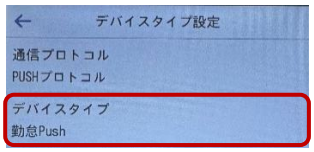
### 1. デバイスタイプの設定

勤怠管理において顔認証デバイスを利用するために運用モードを「勤怠 Push」へ設定します。

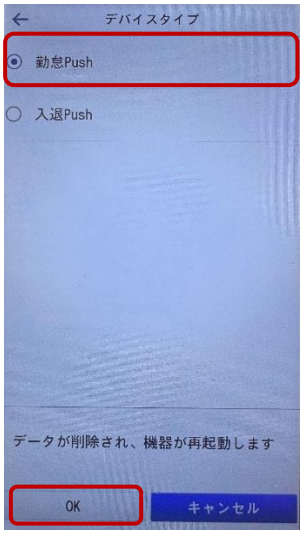
① 顔認証デバイスの画面右下「メインメニューアイコン」→「システム設定」→「デバイスタイプ設定」をタップします。




② 「デバイスタイプ」をタップします。（初期値：入退 Push）




③ 「勤怠 Push」をタップし、「OK」をタップします。顔認証デバイスが再起動します。
※顔認証デバイス内のユーザー情報や認証履歴のデータが削除されます。



## 7.2. デバイス登録

勤怠連携（導入編）STEP 一覧に戻る

**【管理ソフト：勤怠連携 ＞ デバイス管理 ＞ デバイス登録】**

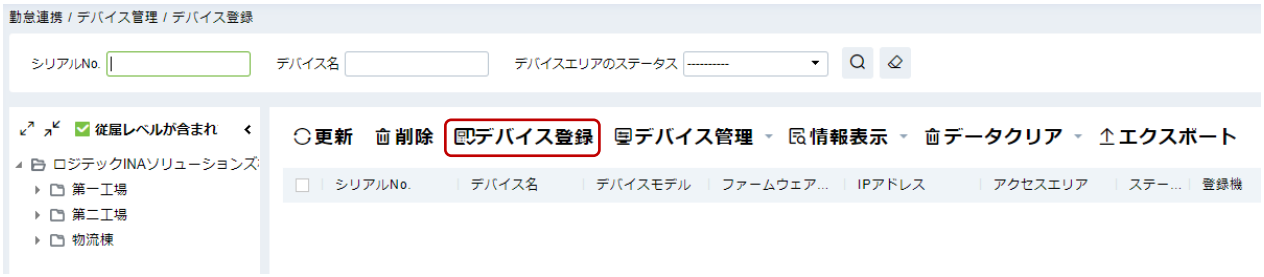
エリアごとに設置する顔認証デバイスを登録します。エリア内に登録された顔認証デバイスは「登録機」として設定することで、顔認証デバイスからユーザー情報や掌・IC カードなどを登録することができます。




### 1. デバイス登録

勤怠打刻で利用する顔認証デバイスについて、台数分を管理ソフトに登録します。

① 「デバイス登録」をクリックします。




② 同一ネットワークへ接続している顔認証デバイスが表示されます。操作列の「追加」をクリックします。

※管理ソフトが動作する PC/サーバーと顔認証デバイスが相互通信できる必要があります。

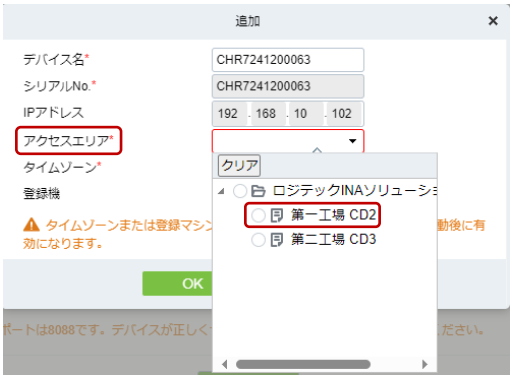
※顔認証デバイスが一覧に表示されない場合、以下の点を確認してください。

- ✓ 顔認証デバイスの電源が入っていて、ネットワークに接続して IP アドレスを取得していること
- ✓ 「デバイスタイプの設定」が「勤怠 Push」になっていること（入退 Push から勤怠 Push に変更している場合、管理ソフト上の入退室管理で登録されている顔認証デバイスも登録を削除する必要があります。）
- ✓ 「4.4 クラウドサーバの設定」で設定したクラウドサーバの IP アドレスに誤りがないこと、通信ポートが「8088」に設定されていること
- ✓ ここまで確認して検索されない場合、顔認証デバイスを「リセット」して「通信設定」をやり直してください。



③ 顔認証デバイスを利用するエリア（例：第一工場）を「アクセスエリア」のプルダウンリスト内から選択します。




④ 選択したデバイスを「登録機」として設定する場合はチェックを入れます。「登録機*」として設定すると顔認証デバイスでユーザーの個別登録や掌・IC カードなどの認証情報を設定することができます。最後に、設定を保存する場合は「OK」をクリックします。




**注意事項**

**＊顔認証デバイスを使って顔登録を行う場合、同一エリア内の登録機の設定は 1 台のみで運用をお願いします。同一エリア内で複数の登録機から同時にユーザー登録を行うとユーザー情報が正常に登録できません。**
**例）同一エリア内で 2 台の顔認証デバイスが稼働している場合**
**顔認証デバイス 2 台中 1 台を登録機に設定します。他の顔認証デバイスでも顔登録を行う場合、予め登録機として設定していた顔認証デバイスを解除してから新たに他の顔認証デバイスを登録機として設定します。**

⑤ 顔認証デバイスの登録が正常におこなわれ、デバイスを設定したエリア（例：第一工場）に表示されていることを確認します。表示されない場合は、10 秒程度時間をおいてから「更新」ボタンをクリックしてください。




デバイス登録は、以上で終わりです。

※手順①～⑤は、導入する顔認証デバイスの台数分の設定を繰り返します。

## 7.3. エリア別ユーザー登録

勤怠連携（導入編）STEP 一覧に戻る

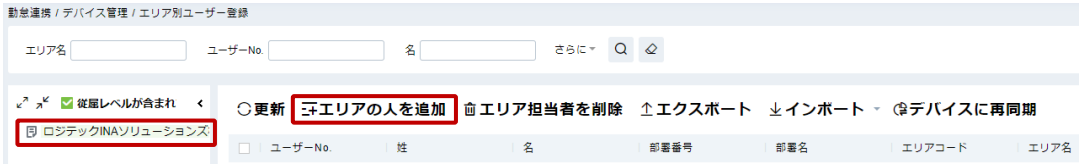
**【管理ソフト：勤怠連携 ＞ デバイス管理 ＞ エリア別ユーザー登録】**

「6.3 部署を設定する　※本手順は省略することができます」で部署を設定していない場合（初期値：部署名）と、部署を設定した場合の説明をします。

### 1. 部署を設定していない場合

管理拠点の「エリア（例：ロジテック INA ソリューションズ株式会社）」にある「部署」に所属するユーザーを選択します。

① ユーザーを追加したい「エリア名（例：ロジテック INA ソリューションズ株式会社）」をクリックし、「エリアの人を追加」をクリックします。「システム管理」でエリアを複数設定していない場合でも、初期値の「エリア名（例：ロジテック INA ソリューションズ株式会社）」に所属するユーザーを追加する必要があります。




② 「部署名（初期値）」をクリックします。「部署名」に所属するユーザーが一覧表示されます。

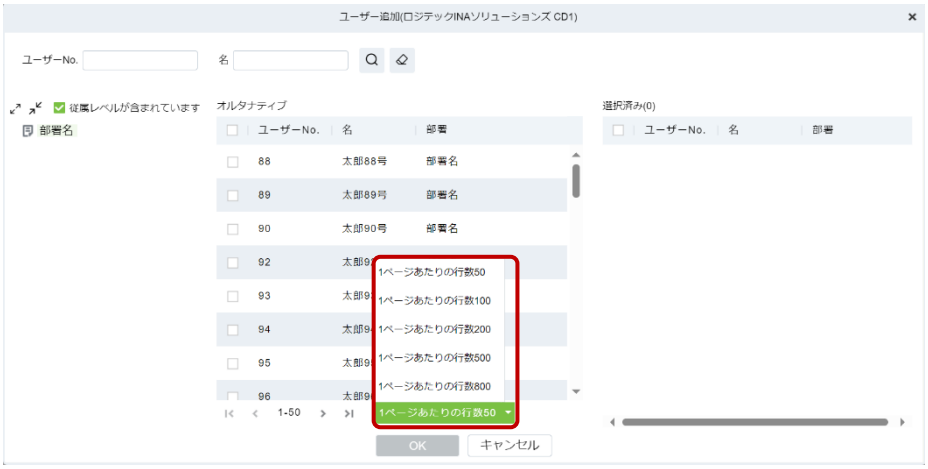



③ 初期値の「エリア名（例：ロジテック INA ソリューションズ株式会社）」に追加したいユーザーを選択します。エリアに追加したいユーザーが全て選択できましたら最後に「OK」をクリックします。




※全てのユーザーを追加する場合「1 ページあたりの行数」からユーザー表示数を変更します。（上限 800 名）

上限 800 名を超える場合、全てのユーザーを追加できるまで手順③の操作を繰り返します。



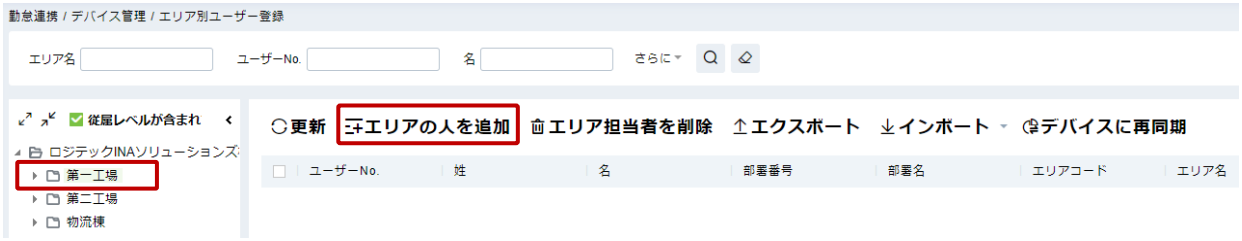

④　初期値の「エリア名（例：ロジテック INA ソリューションズ）」に追加したユーザーが表示されていることを確認します。



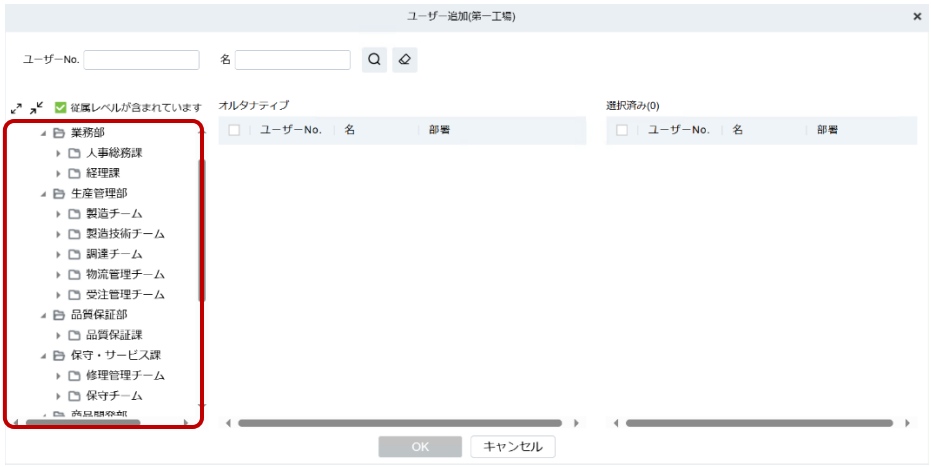

## 2.　部署を設定した場合

管理拠点となる「エリア（例：第一工場）」に属する「部署」に所属するユーザーを選択します。

①　ユーザーを追加したい「エリア名」をクリックし、「エリアの人を追加」をクリックします。



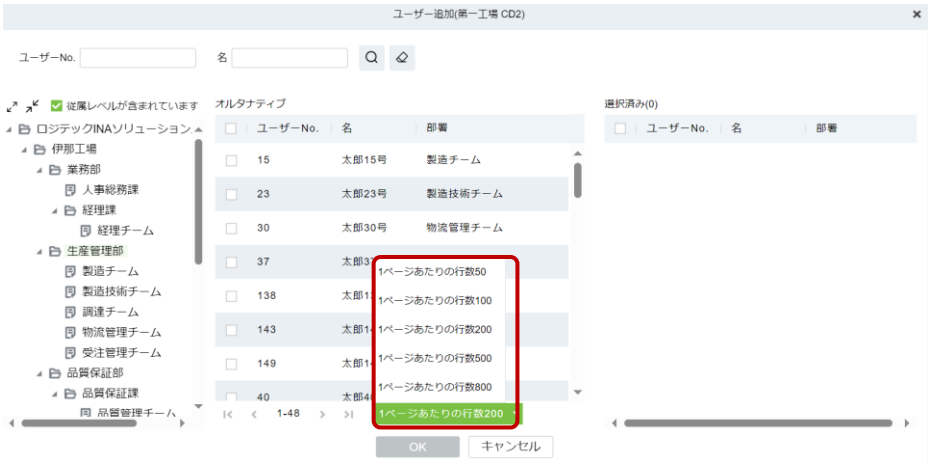
② 「エリア」に属する「部署」をクリックします。「部署」に所属するユーザーが一覧表示されます。




③ 下記例は「商品開発部」に属する各チームに所属するユーザーを選択します。エリアに追加したいユーザーが全て選択できましたら最後に「OK」をクリックします。




※全てのユーザーを追加する場合「1 ページあたりの行数」からユーザー表示数を変更します。（上限 800 名）
上限 800 名を超える場合、全てのユーザーを追加できるまで手順③の操作を繰り返します。



④ 「エリア名（例：第一工場）」に追加したユーザーが表示されていることを確認します。




エリア別ユーザー登録の説明は、以上で終わりです。

## 7.4. 打刻方法の設定

勤怠連携（導入編）STEP 一覧に戻る

管理ソフトで打刻方法を設定します。運用方法はタッチ運用とタッチレス運用があります。タッチ運用とは、認証後に表示される打刻ボタンをタップした日時を勤怠データとして記録する運用です。タッチレス運用とは、予め設定した時間に勤怠種別を自動で切り替え、認証した日時をそのまま打刻データとして記録する運用です。

### 7.4.1. 共通設定

運用に応じて打刻ボタンの名称（タッチ運用）、勤怠状態の名称（タッチレス運用）を変更することができます。変更する場合は、管理ソフトの【勤怠連携 ＞ 勤怠設定 ＞ 基本ルール】より設定します。

初期値*1 で使用する場合、設定内容の変更は不要です。次の「7.4.2 タッチ運用（マニュアルモード）」または「7.4.3 タッチレス運用（自動モード）」の手順へ進みます。

*1：**打刻ボタン名称の初期値**

| 打刻ボタン名称の初期値 | システム上管理されるコードと勤怠種別 *2 |
|---|---|
| 出勤 | F1（“出勤” として管理されています） |
| 退勤 | F2（“退勤”として管理されています） |
| 外出開始 | F3（“外出” として管理されています） |
| 外出終了 | F4（“外出戻り”として管理されています） |
| 残業開始 | F5（“残業開始” として管理されています） |
| 残業終了 | F6（“外出終了” として管理されています） |

*2：F1～F6 に対応する勤怠種別は変更できません。名称のみ変更ができます。

① 「基本ルール」の「勤怠状態の設定」で、「設定内容」を編集して打刻ボタンの名称を設定します。

※8 文字以内／特殊文字（記号や機種依存文字）使用不可



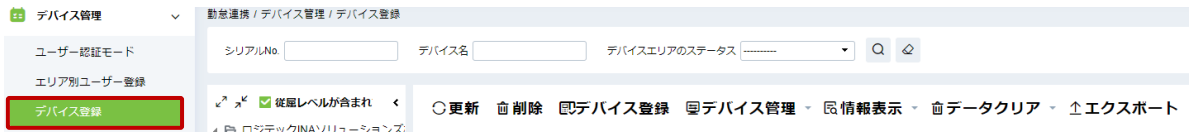

② 打刻ボタンの名称を保存するには「OK」をクリックします。

③ 次に運用方法に応じた設定を行います。タッチ運用の場合は「7.4.2 タッチ運用（マニュアルモード）」へ、タッチレス運用の場合は「7.4.3 タッチレス運用（自動モード）」の手順へ進みます。

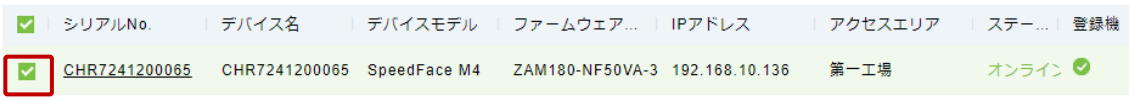
## 7.4.2. タッチ運用（マニュアルモード）

タッチ運用とは、認証後に表示される打刻ボタンをタップした日時を勤怠データとして記録する運用です。初期値は打刻ボタンをタッチするタッチ運用（手動モード）となり、認証後は「出勤」と「退勤」のみが表示されます。その他の打刻ボタンを追加する場合は、管理ソフトの【勤怠連携 ＞ デバイス管理 ＞ デバイス登録】を開きます。

### 1. 打刻ボタンの設定方法



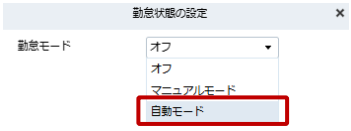

① 打刻ボタンの名称変更を行う顔認証デバイスを選択（チェック）します。 ※最大 10 台まとめて設定可




② 「デバイス管理」メニューの「勤怠状態の設定」をクリックします。




③ 勤怠モードから「自動モード」を選択します。

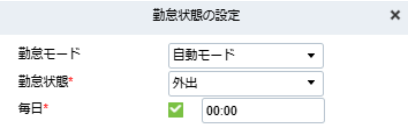
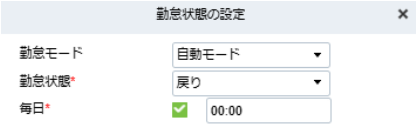



④ 顔認証デバイスへ「出勤」「退勤」以外に追加したいボタンの設定を行います。「保存して次へ」を選択すると、続けて設定が行えます。なお、各勤怠状態の切り替え時間は「毎日／0:00（設定しない）」とします。

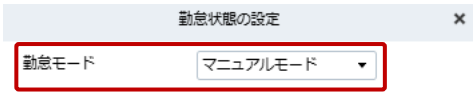
**打刻ボタン名称変更例：**

| 管理コード | 初期値 | 変更例 |
|---|---|---|
| F1 | 出勤 | 出勤テスト |
| F2 | 退勤 | 退勤テスト |
| F3 | 外出開始 | 外出テスト |
| F4 | 外出終了 | 戻りテスト |
| F5 | 残業開始 | 開始テスト |
| F6 | 残業終了 | 終了テスト |



| システム管理コード | 設定値（赤字）と打刻ボタン名称例 | 設定時の画面例 |
|---|---|---|
| F1：出勤 | 勤怠モード／自動モード<br>勤怠状態／出勤テスト（例）<br>毎日／0:00 |  |
| F2：退勤 | 勤怠モード／自動モード<br>勤怠状態／退勤テスト（例）<br>毎日／0:00 |  |
| F3：外出 | 勤怠モード／自動モード<br>勤怠状態／外出テスト（例）<br>毎日／0:00 |  |
| F4：外出戻り | 勤怠モード／自動モード<br>勤怠状態／戻りテスト（例）<br>毎日／0:00 |  |
| F5：残業開始 | 勤怠モード／自動モード<br>勤怠状態／開始テスト（例）<br>毎日／0:00 |  |
| F6：残業終了 | 勤怠モード／自動モード<br>勤怠状態／終了テスト（例）<br>毎日／0:00 |  |

⑤　最後に、勤怠モードから「マニュアルモード」を選択し「OK」をクリックします（設定値を顔認証デバイスへ反映します）。



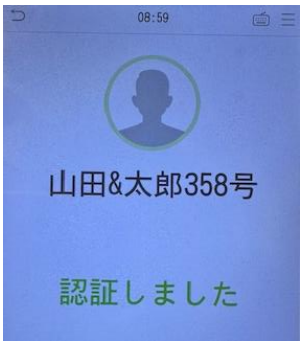




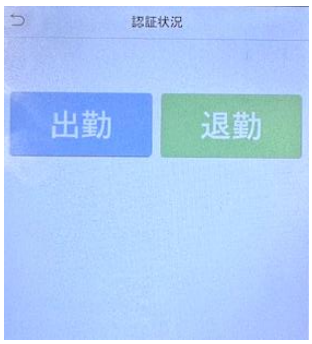
※勤怠モードをマニュアルモードに選択する前に「勤怠状態の設定」画面を閉じてしまった場合、もう一度顔認証デバイスを選択（チェック）して「勤怠状態の設定」を開き、⑤の本手順のみ実施してください。

**■認証から打刻の流れ**

STEP１．認証完了




STEP２．打刻ボタンをタップ

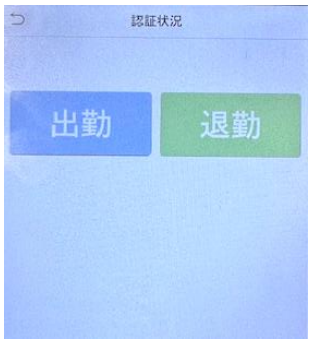
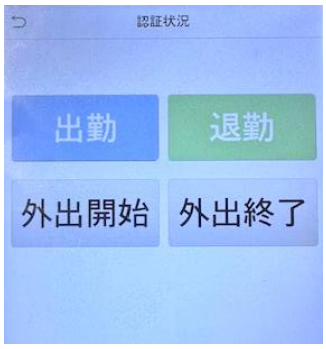
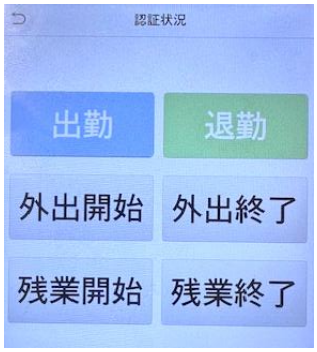



STEP３．打刻の受付完了




**■打刻ボタン表示例**

認証後に設定した打刻ボタンが表示されます。

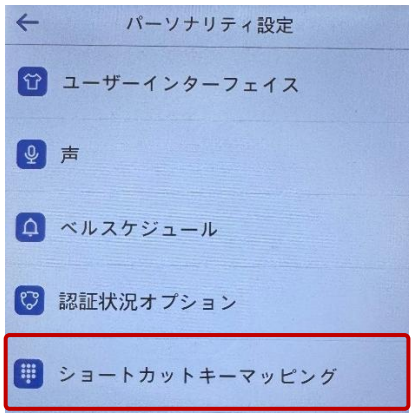
| 出勤・退勤（初期値） | 出勤・退勤・外出開始・外出終了 | 出勤・退勤・外出開始・外出終了<br>残業開始・残業終了 |
|---|---|---|
|  |  |  |

## 2．　追加した打刻ボタンの表示を削除する方法

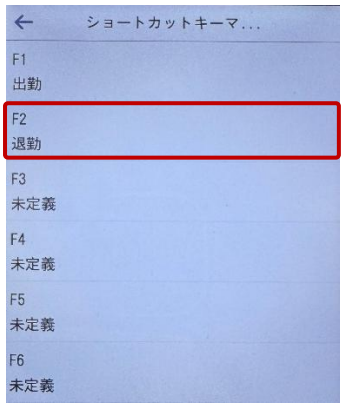
顔認証デバイスのメインメニューから打刻ボタンの表示を削除します（管理ソフトからは表示を削除できません）。

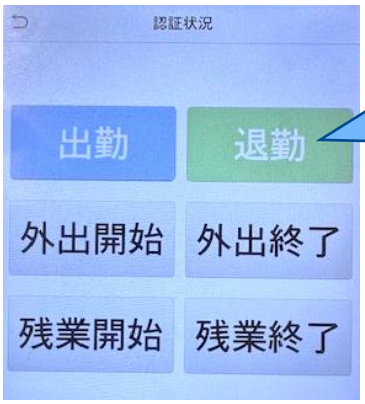
①　顔認証デバイスのメインメニュー「パーソナリティ設定」の「ショートカットキーマッピング」をタップします。



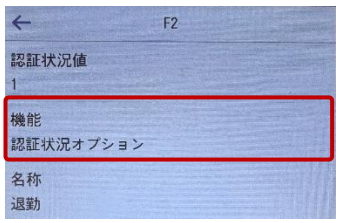
② 管理ソフトから設定された打刻ボタンが割り当てられています。表示を削除する打刻ボタンをタップします。
例は「F2：退勤」の表示を削除します。



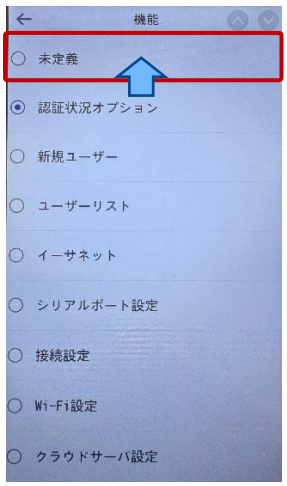




顔認証デバイス（ショートカットキーマッピング）に割り当てられている打刻ボタンの表示例です。

③ 機能の「認証状況オプション」をタップします。



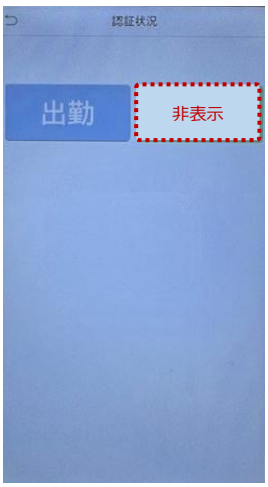

④ 認証状況オプションから「未定義」をタップして選択して「戻る」をタップします。ショートカットキーマッピングが「未定義」になっていることを確認します。









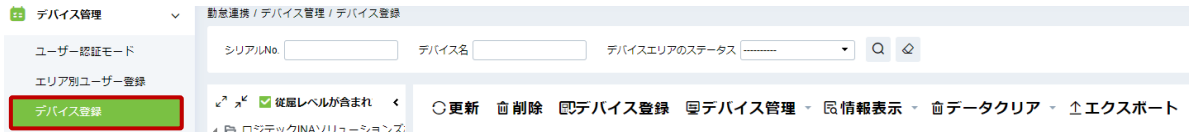

他の打刻ボタンの表示を削除する場合は、本手順の②～④を繰り返します。最後に、認証待機画面に戻り、認証した結果、打刻ボタンが表示されないことを確認します。

※ショートカットキーマッピングの「未定義」へ改めて打刻ボタンを表示する場合は、管理ソフトから設定します。詳細は「7.4.2 タッチ運用（マニュアルモード）」を参照してください。

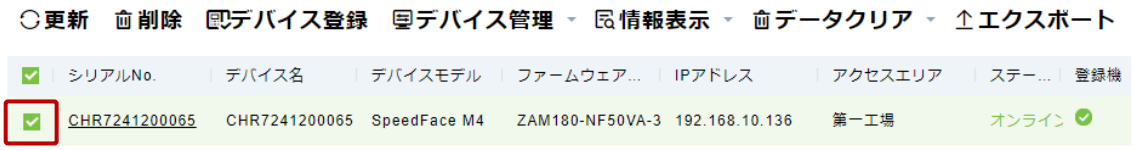
## 7.4.3. タッチレス運用（自動モード）

タッチレス運用とは、予め設定した時間に勤怠種別を自動で切り替え、認証した日時をそのまま打刻データとして記録する運用です。通常、タッチレス運用で使用する勤怠種別は「出勤」と「退勤」です。必要な場合は「残業開始」と「残業終了」を設定します。なお、「外出」「戻り」の勤怠種別は、時間の指定ができる種別ではありませんので対応できません。

顔認証デバイスへ勤怠種別の名称やボタン非表示の設定を反映するには、管理ソフトの【勤怠連携 ＞ デバイス管理 ＞ デバイス登録】を開きます。




① タッチレス運用を行う顔認証デバイスを選択（チェック）します。




② 「デバイス管理」メニューの「勤怠状態の設定」をクリックします。



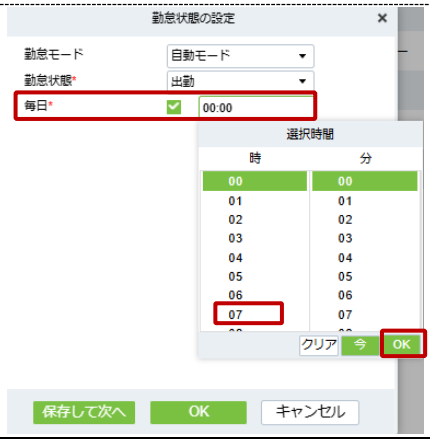

③ 勤怠モードから「自動モード」を選択します。



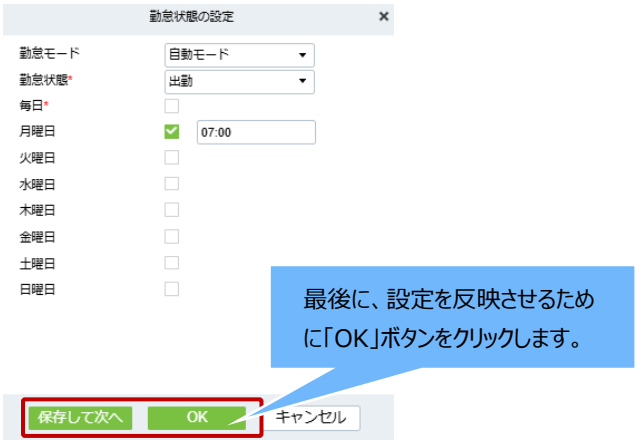
④ 「勤怠状態」を選択（例は「出勤」です）します。



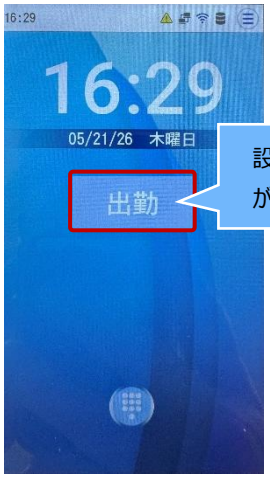

⑤ タッチレス運用（自動モード）を適用する「曜日」を選択し、勤怠状態を切り替える「時間」を入力します。

| 毎日適用する場合 | 曜日ごとに適用する場合 |
|---|---|
|  |  |
| 下記例は、毎日 AM7:00 に「出勤」へ切り替わります | 下記例は、月～金は AM7:00、<br>土日は AM9:00 に「出勤」へ切り替わります |
|  |  |

⑥ 「保存して次へ」を選択し、「退勤」についても手順③から⑥で設定します。最後に、設定を反映するために「OK」をクリックします（設定値を顔認証デバイスへ反映します）。




**■認証待機画面例**

| スクリーンセーバー表示中 | 認証待機画面表示中 |
|---|---|
|  |  |



※認証時に設定した勤怠種別を変更することはできません。

**■打刻の流れ**

認証されると STEP1→STEP2 で表示されます。

STEP１． 認証完了




STEP２． 打刻の受付完了




※自動モードで設定した勤怠種別で打刻されます。

**ご参考：顔認証デバイスを「出勤専用」または「退勤専用」に設定する方法**

1. 「出勤専用」に設定する
   ① [勤怠連携]-[デバイス管理]-[デバイス登録]-[デバイス管理]画面を表示します
   ② デバイス一覧上で設定変更するデバイスを選択（チェック）します
   ③ [デバイス管理]-[勤怠状況の設定]を選択します
   ④ 以下の設定を行います。
   勤怠モード　：自動モード
   勤怠状態　：出勤
   毎日　：チェック
   時刻　：00:00

2. 「退勤専用」に設定する
   ① [勤怠連携]-[デバイス管理]-[デバイス登録]-[デバイス管理]画面を表示します
   ② デバイス一覧上で設定変更するデバイスを選択（チェック）します
   ③ [デバイス管理]-[勤怠状況の設定]を選択します
   ④ 以下の設定を行います。
   勤怠モード　：自動モード
   勤怠状態　：退勤
   毎日　：チェック
   時刻　：00:01*

   *出勤は初期値が「00:00」ですが、退勤は初期値「00:00」以外の時間を設定する必要があります。

## 7.5. 勤怠打刻と勤怠履歴

勤怠連携（導入編）STEP 一覧に戻る

「7.4 打刻方法の設定」までの設定を完了すると、顔認証デバイスで勤怠打刻を行うことができます。実際に勤怠打刻を行い、打刻した記録を管理ソフトで確認できます。

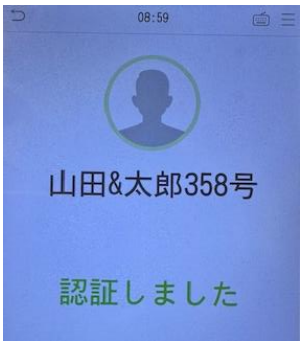
### 1. 勤怠打刻

① 顔認証デバイスの認証待機画面を表示します。顔認証（掌認証・IC カード認証などを含む）を行います。

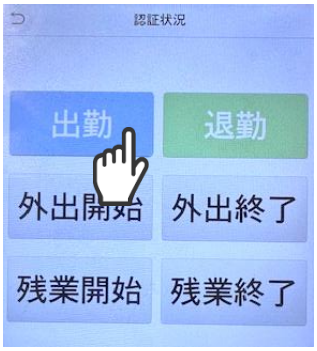



② 表示された打刻ボタンから該当する勤怠種別をタップします。

1．認証完了




2．打刻ボタンをタップ




3．打刻の受付完了

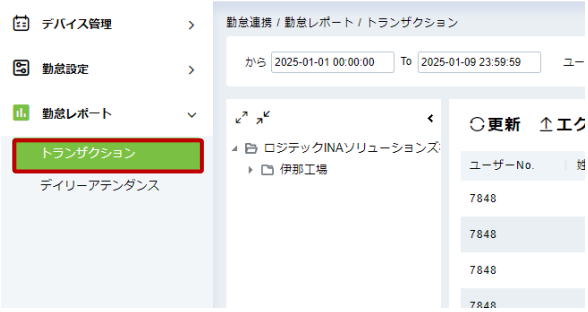



※初期値では最初の打刻から「1 分間」は再打刻できません。再打刻までの時間を変更は、顔認証デバイスの「システム設定」「勤怠」の「重複認証期間（m）（初期値：1／設定範囲：なし、1～999999）」を参照してください。

勤怠打刻の説明は、以上で終わりです。

### 2. 勤怠履歴

① 管理ソフトの「勤怠連携 ＞ 勤怠レポート ＞ トランザクション」をクリックします。



② 期間（日付）、ユーザーNo、姓名を指定して検索することができます。



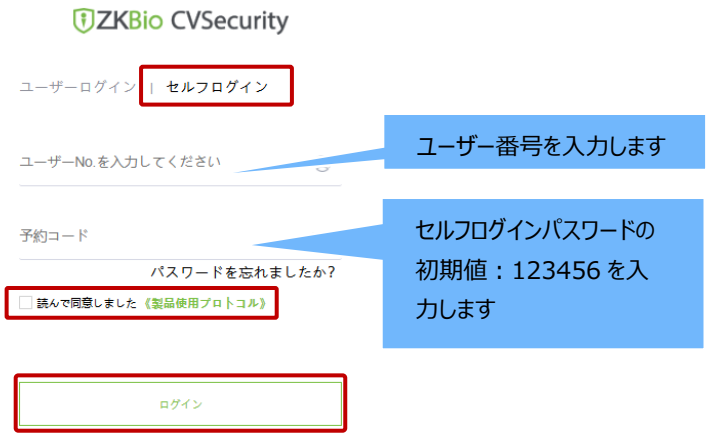

③ 検索した結果から、該当する打刻データを確認します。




## 3. セルフログインによる勤怠履歴（トランザクション）確認

管理ソフトへ「ユーザー番号」と「セルフログインパスワード」を使用して、ユーザー自身で該当する勤怠履歴を確認することができます。セルフログインパスワードは「初期値：123456」です。セルフログイン後に変更することができます。

① 管理ソフトのログイン画面で「セルフログイン」をクリックしてログイン画面を切り替えます。ユーザー番号と、予約コードにはセルフログインパスワード「初期値：123456」を入力します。「読んで同意しました」へチェックを入れ「ログイン」をクリックします。



② ログインに成功すると、該当ユーザーの勤怠履歴（トランザクション）が表示されます。勤怠履歴以外の管理ソフトの操作はできません。



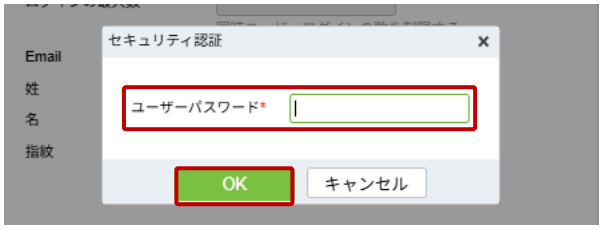

**【補足】 セルフログインパスワードを変更する場合**

① 画面右上のユーザーアイコン「 」をクリックします。

② 「パスワードリセット」へチェックを入れ、新しいパスワードを「パスワード」へ、入力間違えが無いようにもう一度「パスワード確認」へ入力をして「OK」をクリックします。




③ 「セキュリティ認証」画面が表示されるので、「ユーザーパスワード*（変更前のセルフログインパスワード）」を入力して「OK」をクリックします。




※「フロータスク」は当社または本製品のサポート対象外です。

## 7.6. 顔認証または他の認証を利用する場合

勤怠連携（導入編）STEP 一覧に戻る

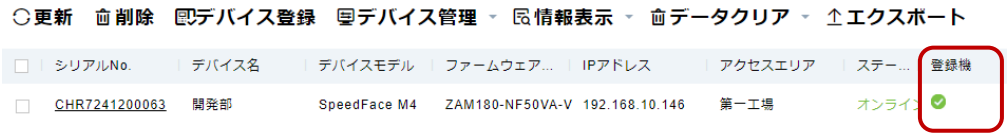
顔認証デバイスを使用して顔登録、掌情報、IC カード情報を登録します。また、IC カード情報は間違いがないように手入力ではなく、顔認証デバイスのカードリーダーを使用して登録します。

**注意事項**

**＊顔認証デバイスを使って顔登録を行う場合、同一エリア内の登録機の設定は 1 台のみで運用をお願いします。**
**同一エリア内で複数の登録機から同時にユーザー登録を行うとユーザー情報が正常に登録できません。**
**例）同一エリア内で 2 台の顔認証デバイスが稼働している場合**
**顔認証デバイス 2 台中 1 台を登録機に設定します。他の顔認証デバイスでも顔登録を行う場合、予め登録機として設定していた顔認証デバイスを解除してから新たに他の顔認証デバイスを登録機として設定します。**

### 1. 管理ソフト：勤怠連携 ＞ デバイス管理 ＞ デバイス登録）

① ユーザー情報を登録する顔認証デバイスを「登録機＊」であることを確認します。
※登録機の設定は、該当端末の「シリアル No」をクリックし、「登録機」へチェックを入れ「OK」をクリックします。




### 2. 顔認証デバイスの設定

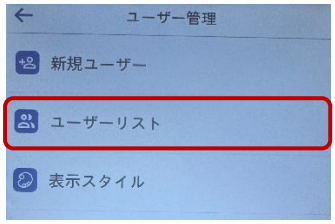
① 登録機のメインメニューを表示し「ユーザー管理」をタップします。







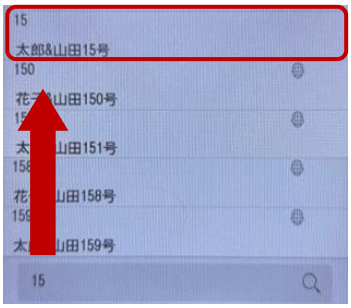
② 「ユーザーリスト」をタップします。



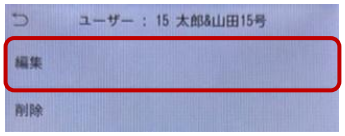
③　画面最下部にある検索フォームをタップし、ユーザー番号（ID）を入力して絞り込み検索をします。
※名前では検索できません



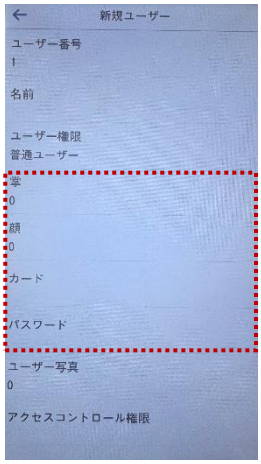

④　登録情報を更新（生体情報などの追加）するユーザーを選択（タップ）します。




⑤　「編集」をタップします。



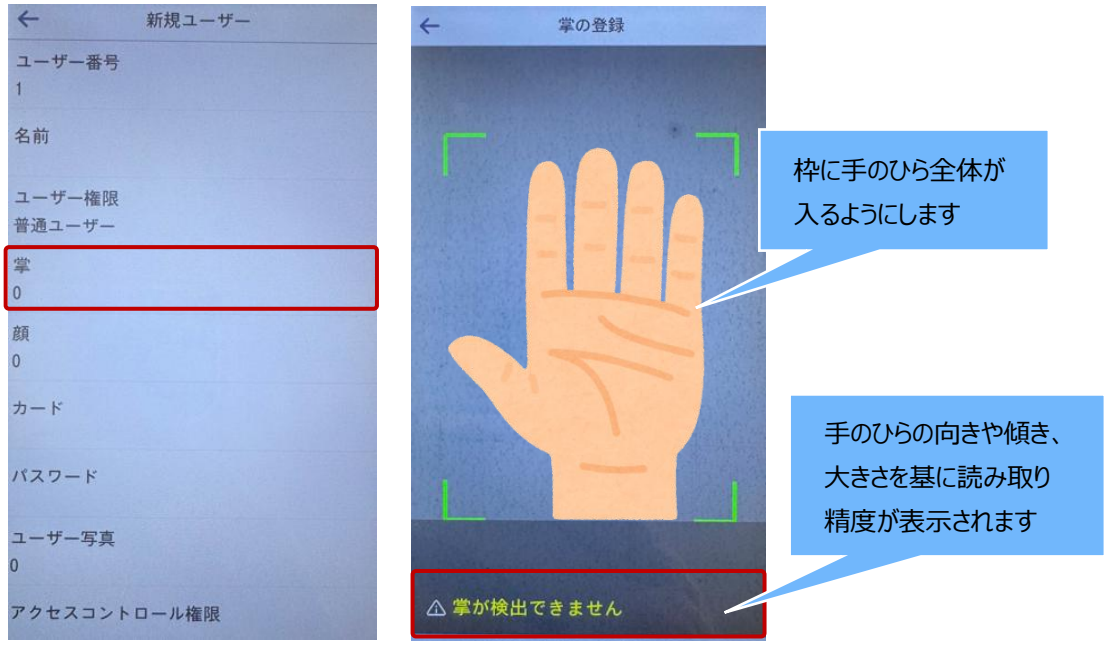

⑥　掌・顔・カードなど、認証に利用する項目をタップします。



・ **掌情報を登録する場合**

「掌」をタップし、掌 1、掌 2 のいずれかをタップします。カメラが起動したら、15～30 センチの距離で手全体を枠の中に入れて登録します。最後に画面左上の「戻る」をタップして保存します。

※登録中は画面下に読み取り精度が表示されます。精度が悪い場合は再登録となります。

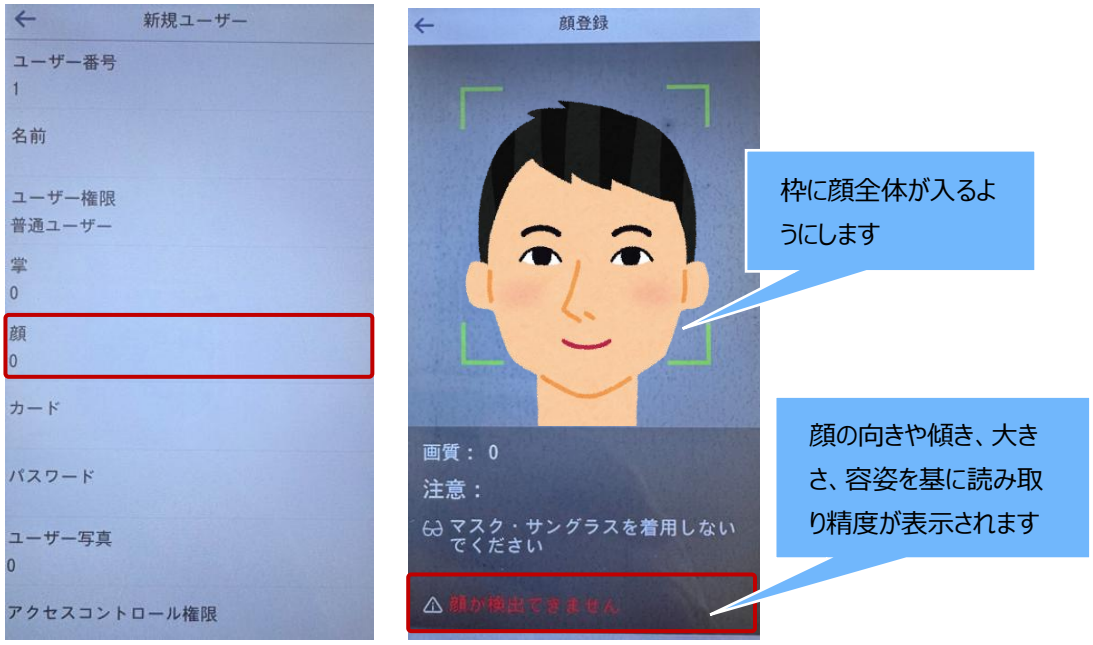



・ **顔情報を登録する場合**

「顔」をタップしてカメラを起動します。カメラが起動したら顔をかざして登録します。最後に画面左上の「戻る」をタップして保存します。

※登録中は画面下に読み取り精度が表示されます。精度が悪い場合は再登録となります。

「顔登録ガイドライン」を参照して写真の撮り直しをお願いします。



・ **IC カード情報*を登録する場合　※１枚のカード情報を複数のユーザーに登録することはできません。**

(ア) 「カード」をタップします。

(イ) IC カードアイコンをタップします。

(ウ) 本体前面の IC カードリーダーに IC カード*をかざします。

(エ) IC カードの読み取り結果を確認し、最後に画面左上の「戻る」をタップして保存します。



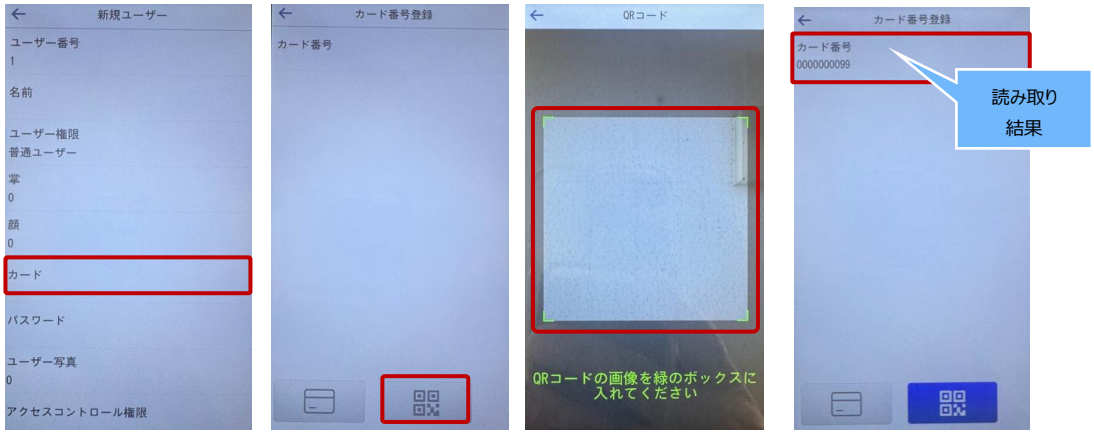

・ **QR 情報*を登録する場合（静的 QR）　※半角数字／最大 20 桁、同じ番号を複数のユーザーに登録することはできません。**

(ア) 「カード」をタップします。

(イ) QR アイコンをタップします。

(ウ) カメラが起動したら、枠内に QR をかざします。

(エ) QR 読み取り結果を確認し、最後に画面左上の「戻る」をタップして保存します。




**注意事項**

***IC カード情報は、FeliCa：ISO/IEC 18092「NFC Type F」、MIFARE：ISO/IEC 14443「Type A」に対応**

***IC カードの ID 取得（読み取り）のみをサポートします。動作確認済みのカードは以下の通りです。**

**・「FeliCa」の「IDm」情報**

**・「Mifare Plus」の「UID」情報**

**・「Mifare Ultralight EV1」の「UID」情報**

**・「Mifare Classic 1K」の「UID」情報**

***IC カード情報および QR 情報について**

**・IC カード情報と QR 情報は、入退 Push モードの場合、カード登録数（50,000）の範囲で複数登録できます。勤怠 Push モードの場合、IC カードまたは QR のいずれかの登録（排他）ができます。**

**・IC カード情報または QR 情報を削除する場合は、「ユーザーリスト」の「削除」から「カード番号のみ削除」を行ってください。**

・ **パスワード情報を登録する場合（6 桁以上、最大 8 桁の数字）**

(ア) 「パスワード」をタップします。

(イ) パスワードを入力します。

(ウ) 「パスワードを再入力してください」と表示されます。もう一度設定するパスワードを入力します。

(エ) 最後に画面左上の「戻る」をタップして保存します。



## 7.7. 外部勤怠管理システムと連携

当社では別途「設置・設定及び勤怠連携設定サービス」を有償サービスとしてご提供しています。専門スタッフが訪問し、製品の組み立てから初期設定までを行います。外部システムとの連携に必要なソフトウェア「打刻データ連携ツール」は、設定サービスを実施する際にご提供します。




**【設置・設定及び勤怠連携設定サービスが適応可能なお客様】**

・端末と勤怠連携システムを同時に導入する

・勤怠管理システム導入後に端末を導入する

**【勤怠連携設定サービスが適応可能なお客様】**

・端末を導入後に勤怠連携システムを導入する

また、製品組み立てから初期設定を行う「設置・設定及び勤怠連携設定サービス」をご利用いただくと、スムーズな製品導入が可能です。

※ご希望の訪問日の 3 週間前までに各種手続きが必要となります。

※お申し込み後のキャンセルや対応内容の変更は別途費用を申し受けます。

※該当製品新品購入時の未使用品のみ対応可能で、購入より 60 日以内に申し込むことを条件とします。

※設置・設定サービスは製品納品後、設置設定日の日程調整をさせていただきます。

## 7.8. 打刻データ連携ツールの実行方法

打刻データ連携ツールとは、管理ソフトと外部システムとの間で認証データから勤怠データを自動生成するソフトウェアです。本ソフトウェアは有償の「設置・設定及び勤怠連携設定サービス」の実施日に提供・インストールします。本項ではインストール後の実行方法について説明します。

### 1. 打刻データ連携ツール（ELECOM フォルダ）の構成

[ELECOM]フォルダ

L [curl]フォルダ　　：URL を使ったデータ送受信（API 通信・ファイル操作）を行うプログラム本体

L callImportIserMaster.bat　：外部システムからユーザーマスターをインポートするバッチファイル

L callKintai2.bat　　：勤怠データ出力のため、curl 経由で管理ソフトの API を呼び出すバッチファイル

L callNyutai2.bat　　：入退データ出力のため、curl 経由で管理ソフトの API を呼び出すバッチファイル

基本、手動実行のソフトウェアです。自動実行する場合、Windows タスクスケジューラを使用します。

### 2. インストール場所

お客様から指定がない限り、管理ソフトが動作する PC/サーバーの C ドライブの直下に ELECOM フォルダ内にインストールされます。

### 3. 手動実行方法

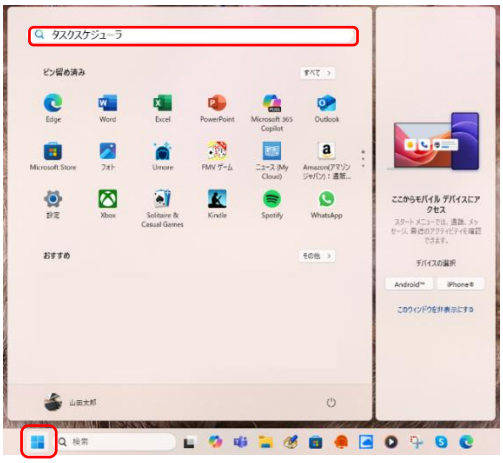
勤怠データを出力する場合は「callKintai2.bat」、入退データを出力する場合は「callNyutai2.bat」をダブルクリックします。お客様の任意のタイミングで外部システム用のデータを出力する場合に利用します。

### 4. 自動実行方法（Windows タスクスケジューラ）

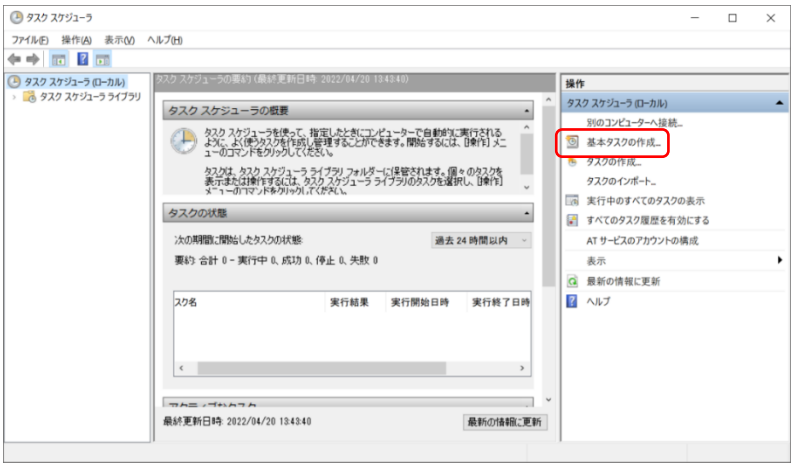
打刻データ連携ツールを指定間隔や時間で自動実行する場合、事前に外部システムの担当者の方と実行タイミングについてご相談をお願いします。ご相談無しに自動実行を設定すると、外部システムへ正常にデータが送信できない場合があります。

※Windows タスクスケジューラの設定には Administorator のアカウントとパスワード情報が必要です。

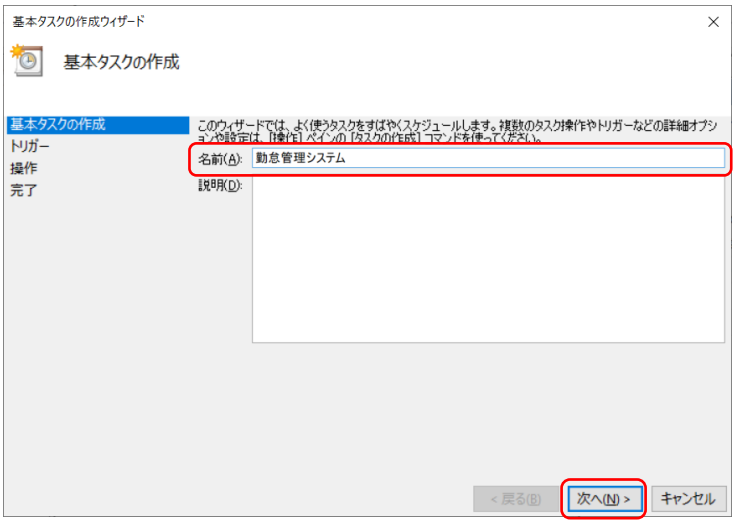
① 画面下の（スタート）をクリックし、検索フォームで「タスクスケジューラ」を検索します。タスクスケジューラ表示さますのでクリックして起動します。



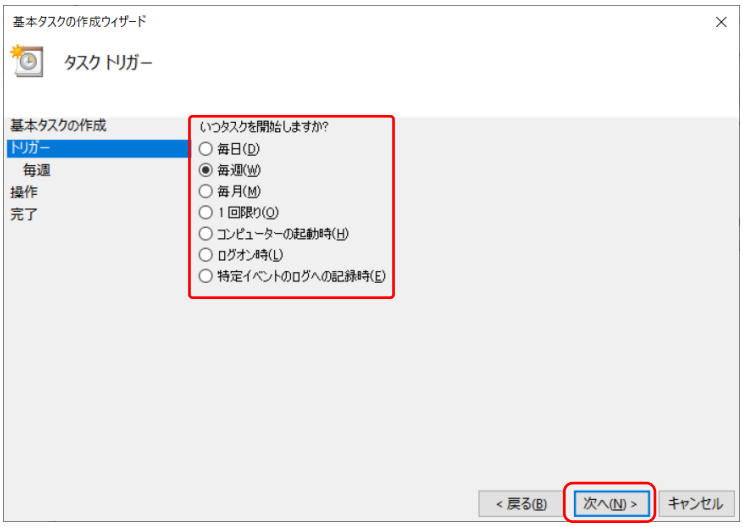
② 「基本タスクの作成」をクリックします。基本タスクの作成ウィザードが表示されます。




③ 「名前」でタスクの名前を入力し、「次へ」をクリックします。

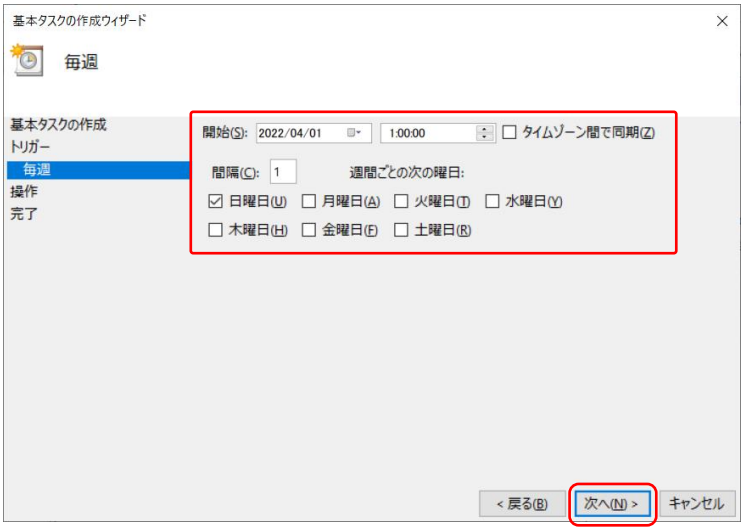



④ タスクを開始する条件をクリックして選択し。「次へ」をクリックします。

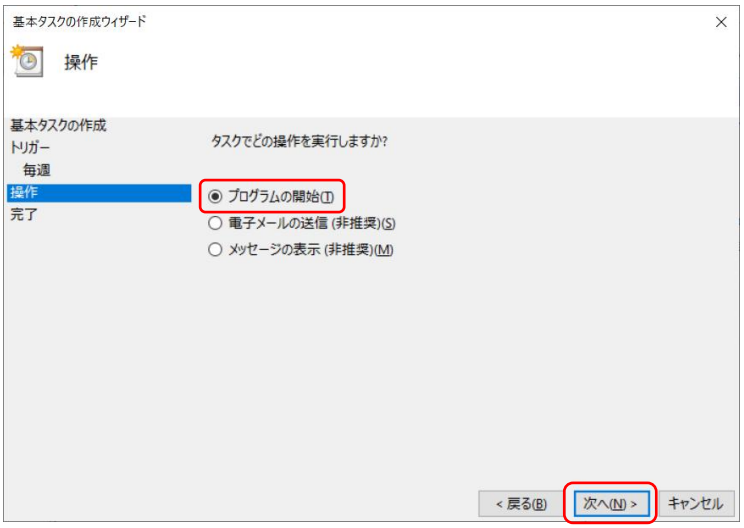


⑤ タスクの開始日時、実行間隔と曜日を設定し、「次へ」をクリックします。

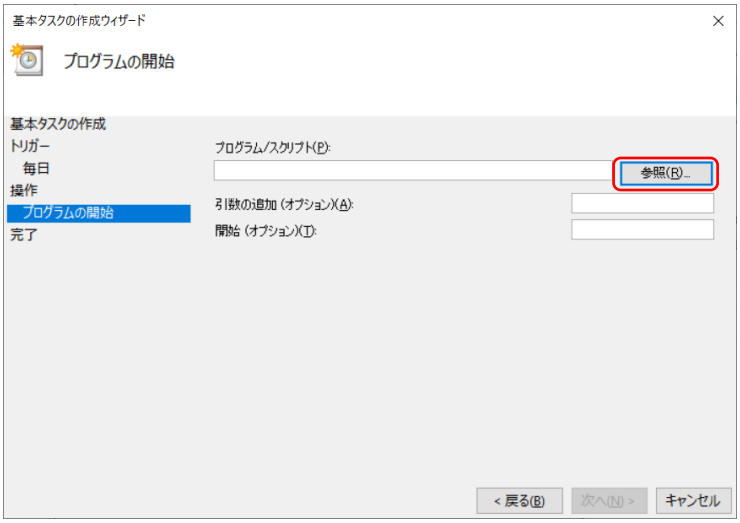
※開始時間は、15～30 分程度、未来の時間を設定します。



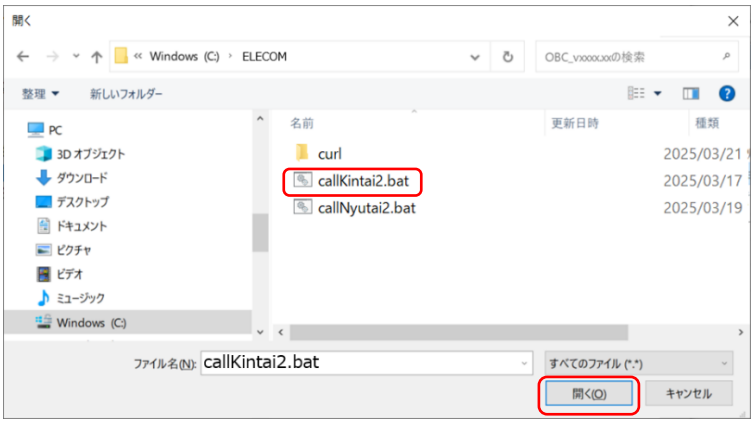

⑥ 「プログラム開始」を選択し、「次へ」をクリックします。



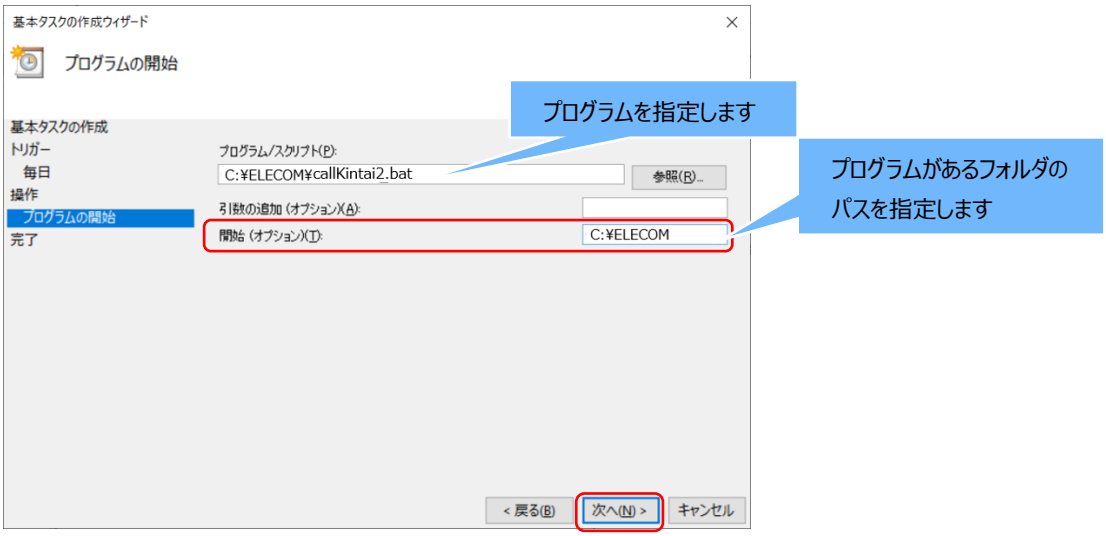

⑦ 「プログラム/スクリプト」で「参照」をクリックします。「開く」ダイアログボックスが表示されます。



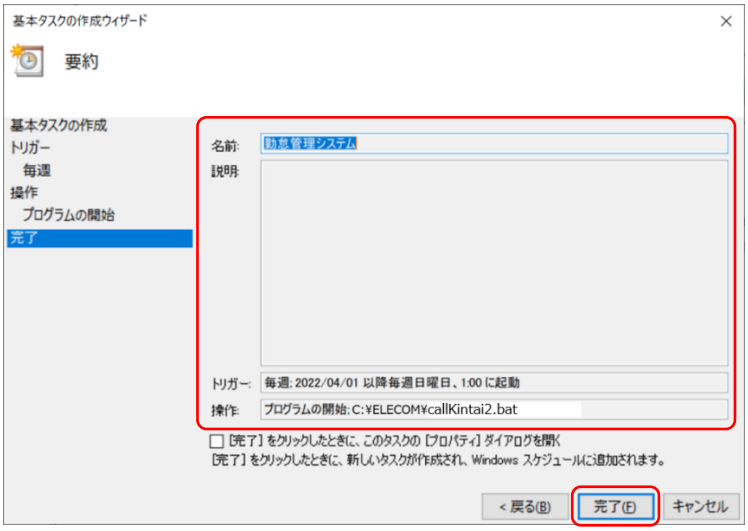
⑧ 実行するプログラム（例：callKintai2.bat）を指定し、「開く」をクリックします。基本タスクの作成ウィザードに戻ります。




⑨ 「開始（オプション）」でプログラムのフォルダパスを入力し、「次へ」をクリックします。




⑩ 設定内容を確認し、「完了」をクリックします。基本タスクの作成ウィザードが終了し、タスクスケジューラに戻ります。Administorator（管理者）のアカウントとパスワードの入力を求められた場合は、適切な Windows の管理者情報を入力してください。



# 8. 入退室管理（導入編）

入退室管理おいて必要最低限の初期設定について説明します。「STEP 番号」をクリックすると各項目の説明へジャンプします。
管理ソフトの詳細設定は「9 管理ソフトの機能説明」を参照し、運用に応じて設定・変更をお願いします。

**STEP1**
- 使用メニュー：顔認証デバイス > メインメニュー > システム設定
- 内容：**デバイスタイプを設定する**

**STEP2**
- 使用メニュー： 管理ソフト > 入退室管理 > アクセスルール > タイムゾーン
- 内容：**タイムゾーン（アクセス可能時間）を設定する**

**STEP3**
- 使用メニュー：管理ソフト > 入退室管理 > アクセスデバイス > デバイス管理及びドア
- 内容：**管理するエリアに顔認証デバイスを登録し、ドア名を設定する**

**STEP4**
- 使用メニュー：管理ソフト > 入退室管理 > アクセスルール > グループ登録
- 内容：**タイムゾーン（アクセス可能時間）を顔認証デバイス（ドア）へ割り当てる**

**STEP5**
- 使用メニュー：管理ソフト > 入退室管理 > アクセスルール > アクセス設定
- 内容：**タイムゾーン（アクセス可能時間）を登録ユーザーへ割り当てる**

**STEP6**
- 使用メニュー：管理ソフト > 入退室管理 > アクセスデバイス > リアルタイムモニタリング
- 内容：**顔認証デバイス単位でアクセスを監視する**

**STEP7**
- 使用メニュー：顔認証デバイス > メインメニュー > ユーザー管理
- 内容：**掌・ICカードなどの登録**

## 8.1. 顔認証デバイス設定（入退 Push）

入退室管理（導入編）STEP 一覧に戻る

顔認証デバイスは「入退室管理」または「勤怠管理」の利用シーンに応じて、予め運用モード「入退 Push または勤怠 Push（初期値：入退 Push）」を設定する必要があります。

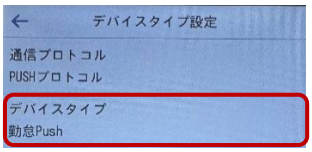
### 1. デバイスタイプの設定

入退室管理において顔認証デバイスを利用するために運用モードを「入退 Push」へ設定します。（初期値：入退 Push）

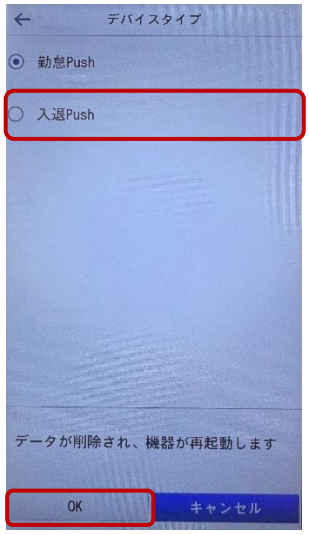
① 顔認証デバイスの画面右下「メインメニューアイコン」→「システム設定」→「デバイスタイプ設定」をタップします。




② 使用する顔認証デバイスが「勤怠 Push」に設定されている場合は「デバイスタイプ」をタップします。




③ 「入退 Push」をタップし、「OK」をタップします。顔認証デバイスが再起動します。
※顔認証デバイス内の認証履歴やユーザー情報のデータが削除されます。

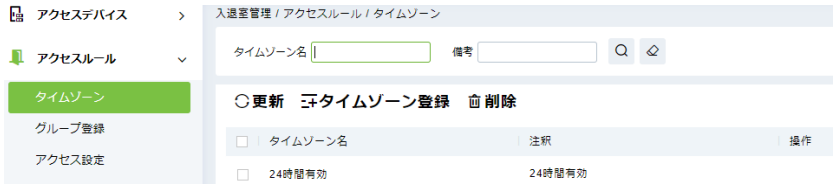


## 8.2. タイムゾーン（アクセス可能時間）

入退室管理（導入編）STEP 一覧に戻る

**【管理ソフト：入退室管理 ＞ アクセスルール ＞ タイムゾーン】**

顔認証デバイスに対してアクセス（認証可能）な時間帯を割り当てることができます。初期値では「24 時間有効」が選択できます。「24 時間有効」はどの時間帯でも認証可能となり、外部機器を制御することができます。




### 1. タイムゾーン登録 ※設定を省略することができます

タイムゾーン（アクセス可能時間）を任意の時間帯で設定して顔認証デバイスに対して割り当てることができます。
例は、「月曜日～日曜日」まで「７時 00 分～23 時 59 分」を認証可能な時間帯として追加する方法です。

① 「タイムゾーン登録」をクリックします。



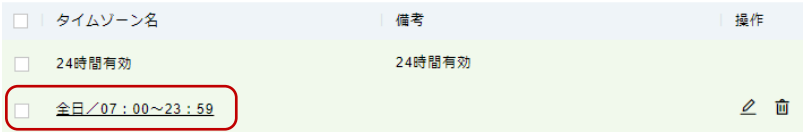

② タイムゾーン名（重複 NG）を入力します。デバイスに割り当てる時に選択肢として表示される名称のため、アクセス可能な時間帯が分かり易い名称にすると管理がし易くなります。例では「全日／07：00～23：59」としています。




③ アクセス可能な時間帯を入力します。例では「月曜日～日曜日」まで「７時 00 分～23 時 59 分」をアクセス可能な時間帯として設定しています。毎日同じ時間帯を設定したい場合、月曜日の開始・終了時間を入力後に「月曜日の設定を、他の平日にコピー」にチェックを入れると、火曜日から金曜日まで同じ内容で自動コピーされます。設定を保存する場合は「OK」をクリックします。

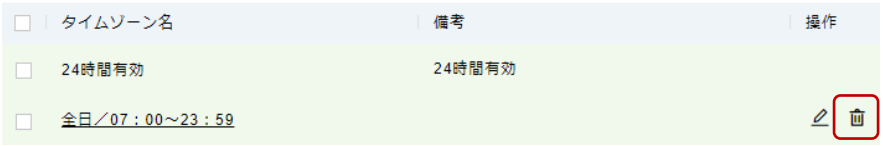


④ 追加をしたタイムゾーンが一覧に表示されていることを確認します。




**2. 削除**

タイムゾーンの操作項目「削除」アイコンをクリックします。




## 8.3. デバイス管理

入退室管理（導入編）STEP 一覧に戻る

**【管理ソフト：入退室管理 ＞ アクセスデバイス ＞ デバイス管理】**

入退室管理で設置する顔認証デバイスを登録します。エリア内を割り当てられた顔認証デバイスは「登録機」として設定することで、顔認証デバイスからユーザー情報や掌・IC カードなどを登録することができます。

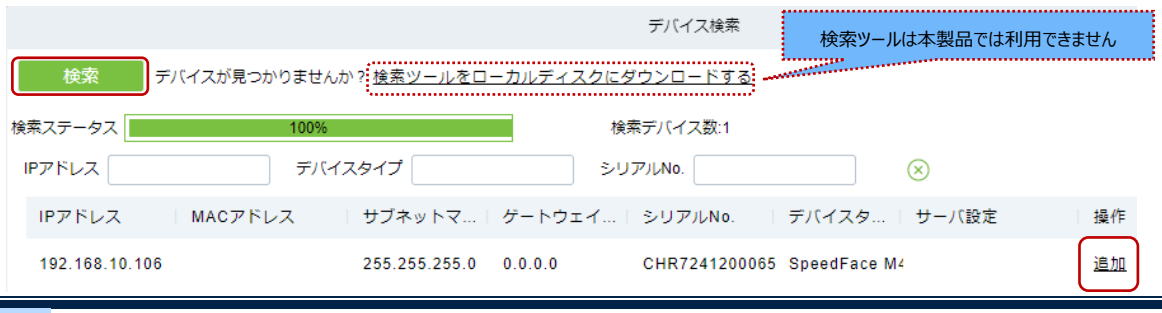



**1. デバイス登録**

① 「デバイス検索」をクリックします。



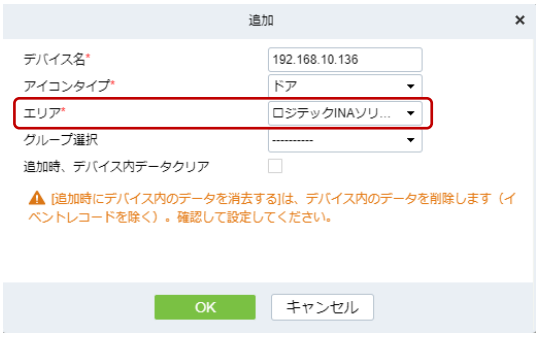

「検索」ボタンをクリックして、同一ネットワーク内にある顔認証デバイスを検索します。次に、検索された顔認証デバイスの操作欄の「追加」をクリックして登録をします。

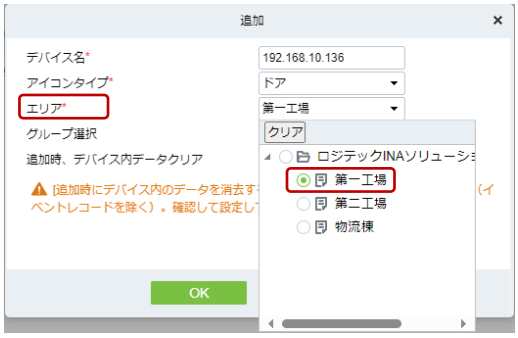


※「検索ツール」は、本製品はサポート対象外です。
※顔認証デバイスが一覧に表示されない場合、以下の点を確認してください。

- ✓ 顔認証デバイスの電源が入っていて、ネットワークに接続して IP アドレスを取得していること
- ✓ 「デバイスタイプの設定」が「入退 Push」になっていること（勤怠 Push から入退 Push に変更している場合、管理ソフト上の勤怠連携で登録されている顔認証デバイスも登録を削除する必要があります。）
- ✓ 「4.4 クラウドサーバの設定」で設定したクラウドサーバの IP アドレスに誤りがないこと、通信ポートが「8088」に設定されていること
- ✓ ここまで確認して検索されない場合、顔認証デバイスを「リセット」して「通信設定」をやり直してください。

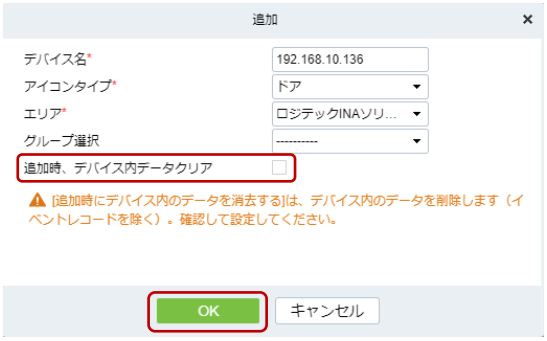
② エリアは登録する顔認証デバイスを設置するエリアを選択します。その他の項目は、初期値で構いません。




※選択する「エリア」は、デバイス、ドア、アクセスレベル（権限）、レベル（権限）設定の各設定で重要な項目です。適切なエリアを選択していない場合、管理ソフトと顔認証デバイス間の同期や設定を反映することができません。

③ 追加時に、顔認証デバイス内のイベントレコード以外のデータを削除する場合、「追加時、デバイス内データクリア」にチェックを入れ、最後に「OK」をクリックします。正常に登録されると「承認成功」が表示されますので「OK」をクリックします。







④ 顔認証デバイスの登録が正常におこなわれ、デバイス一覧に表示されていることを確認します。
表示されない場合、10 秒程度時間をおいてから「更新」をクリックします。




※手順①～④は、導入する顔認証デバイスの台数分の設定を繰り返します。

⑤ 各エリアで顔認証デバイスを「登録機」として設定する場合、登録機として指定する端末のチェックボックスを入れ、「セットアップ」→「登録機として設定」をクリックします。「登録機」として設定すると顔認証デバイスでユーザーの個別登録や掌・IC カードなどの認証情報を設定することができます。



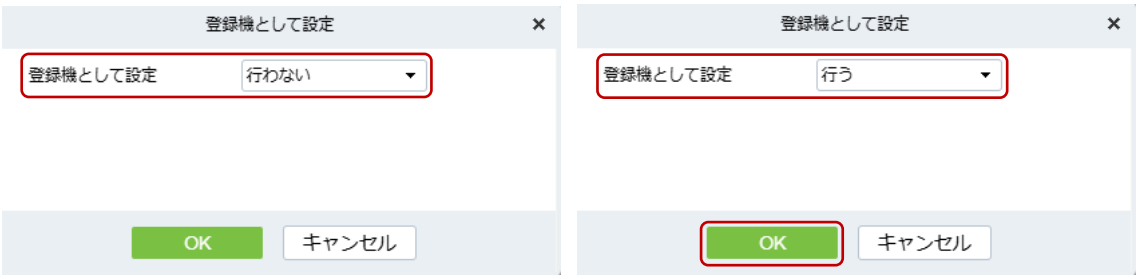

**注意事項**

***顔認証デバイスを使って顔登録を行う場合、同一エリア内の登録機の設定は 1 台のみで運用をお願いします。同一エリア内で複数の登録機から同時にユーザー登録を行うとユーザー情報が正常に登録できません。**

**例）同一エリア内で 2 台の顔認証デバイスが稼働している場合**

**顔認証デバイス 2 台中 1 台を登録機に設定します。他の顔認証デバイスでも顔登録を行う場合、予め登録機として設定していた顔認証デバイスを解除してから新たに他の顔認証デバイスを登録機として設定します。**

⑥ 登録機として設定を「行わない」から「行う」へ変更して「OK」をクリックします。




⑦ 登録機として設定が反映されると「デバイス登録」の項目に「●」が表示されます。



## 8.4. ドア

入退室管理（導入編）STEP 一覧に戻る

**【管理ソフト：入退室管理 ＞ アクセスデバイス ＞ ドア】**

### 1. ドア設定

前項の「デバイス登録」で追加されたデバイスについて、ドア名などを設定します。

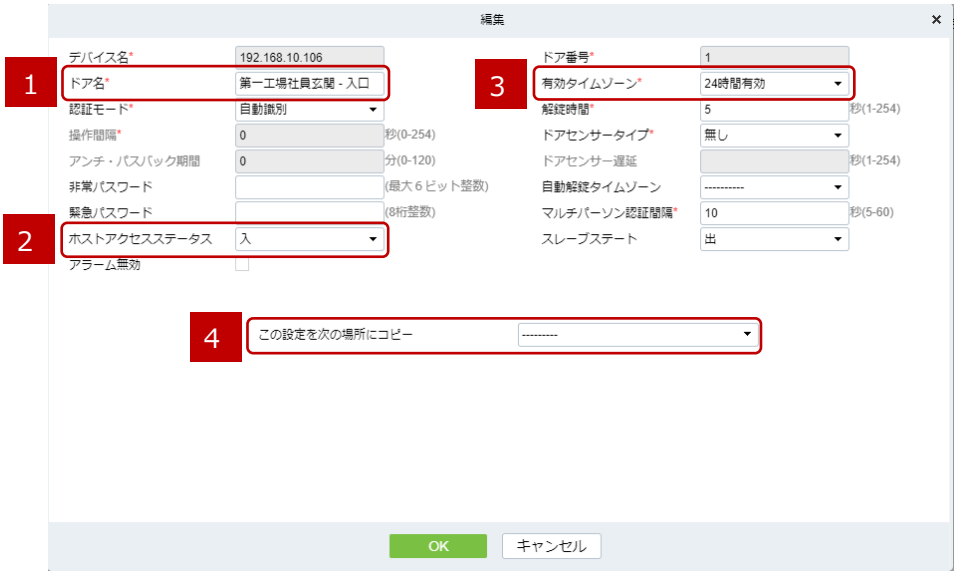
① 登録したデバイスの「ドア名」または操作項目の「編集」アイコンをクリックします。




② 編集画面が開きます。設定を保存する場合は「OK」をクリックします。

【1】ドア名を入力します。「設置場所」と「入口または出口」を明示すると管理がし易くなります。
【2】ホストアクセスステータスを設定します。設置された場所が入口側か出口側かを設定します。
【3】有効タイムゾーンは、原則、設定変更せずに運用します。
※有効タイムゾーン（アクセス可能な時間）は、次のグループ登録でユーザー毎に割り当てます。
【4】複数の顔認証デバイスがある場合、同一設定内容をコピーできます。

※その他の設定項目について、導入時は初期値で利用し、必要に応じて変更をお願いします。



## 8.5. グループ登録

入退室管理（導入編）STEP 一覧に戻る

**【管理ソフト：入退室管理 ＞ アクセスルール ＞ グループ登録】**

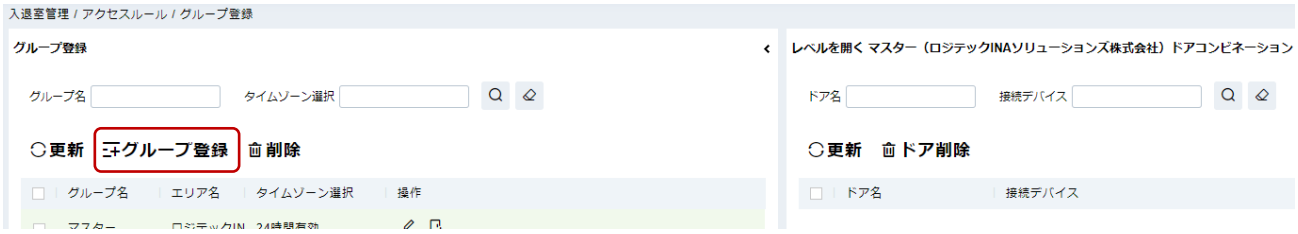
エリア（拠点）、タイムゾーン（アクセス可能な時間）、ドア（顔認証デバイス）で 1 つグループ（アクセス権限グループ）を作成します。エリア毎にアクセス可能な時間帯が異なる場合、エリア毎にタイムゾーンを設定してグループを作成して管理する必要があります。

**注意事項**

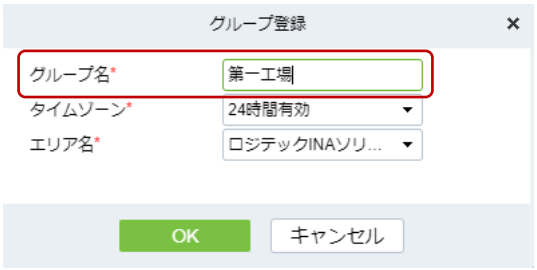
**タイムゾーン及びエリアが 1 つ（初期値）の場合、グループ登録をする「1.グループ登録：①～⑤」の手順は必要ありません。「1.グループ登録⑥以降」の手順から設定をします。**

### 1. グループ登録

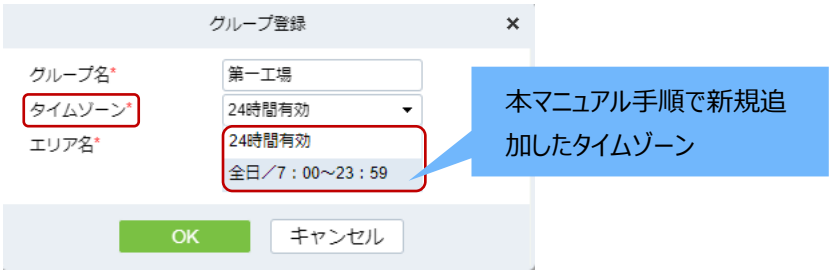
① 「グループ登録」をクリックします。



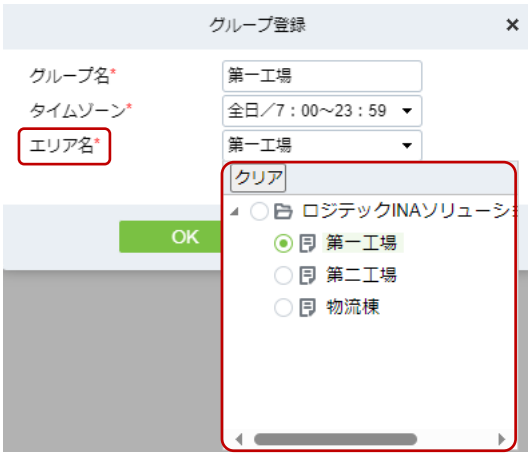

② グループ名を入力します。例はエリアと同じ「第一工場」としています。これにより、エリア毎に複数のタイムゾーンを設定している場合、エリアに対応するタイムゾーンの管理がし易くなります。



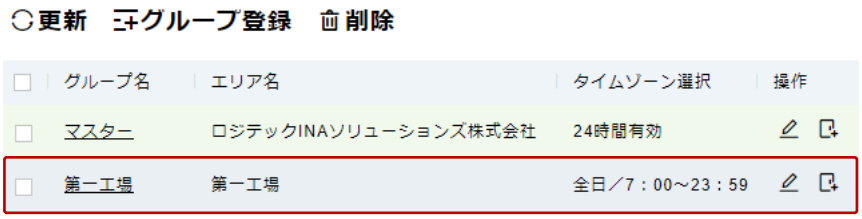

③ タイムゾーンを選択します。前項の「タイムゾーン」で新規に追加したタイムゾーンも選択できるようになります。



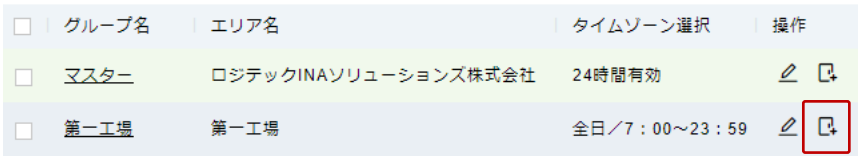
④ 前項③で選択したタイムゾーンを適用するエリア（拠点）を選択します。例ではレベル名に入力した「第一工場」を選択しています。設定を保存する場合は「OK」をクリックします。




⑤ グループ名に新規に追加されていることを確認します。




⑥ 次に、グループ登録（管理拠点：エリア、認証可能な時間：タイムゾーン）を顔認証デバイス（ドア）に割り当てます。グループ名一覧の操作項目の「」をクリックします。




⑦ 予めデバイス登録とドア設定がされた顔認証デバイスが表示されます。割り当てたいドア名のチェックボックスにチェックを入れて「＞」で選択します。

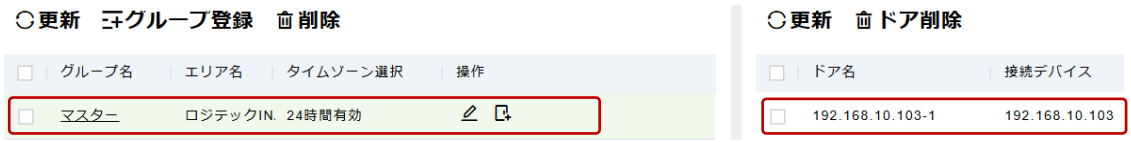
※ドア名の一覧に顔認証デバイスが表示されない場合、「デバイス管理」からデバイスの「エリア名」の設定を再確認してください。④で「第一工場」をエリアとして選択しているため、デバイスに割り当てられているエリアも「第一工場」である必要があります。



⑧ 設定する顔認証デバイスが選択できたら最後に「OK」をクリックします。エリアに紐づくデバイスが複数設置される場合は全てのデバイスを選択してください。




⑨ グループ名をクリックすると、割り当てられた顔認証デバイスが表示されることを確認します。表示されない場合は、時間を置いて「更新」をクリックします。



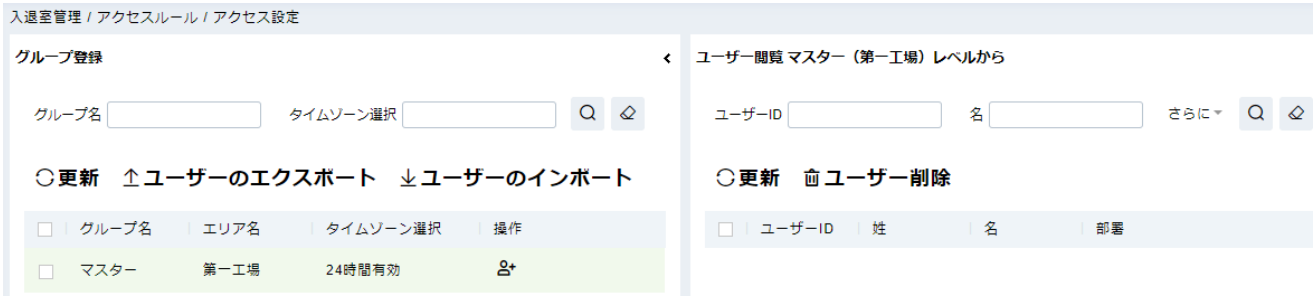

グループ登録は、以上で終わりです。

## 8.6. アクセス設定

入退室管理（導入編）STEP 一覧に戻る

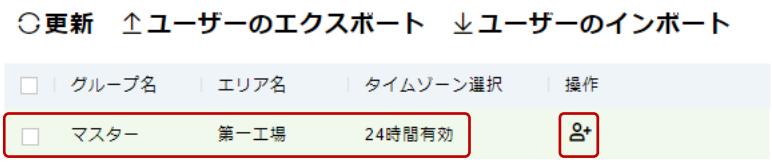
**【管理ソフト：入退室管理 ＞ アクセスルール ＞ アクセス設定】**

前項「グループ登録」で作成した「グループ」へ「ユーザー」を割り当てます。これにより、ユーザーは、グループ（関連付けられたタイムゾーン、エリア、ドア）にアクセス権が設定され、アクセス（認証）可能になります。




### 1. グループ（エリア及びタイムゾーン）をユーザーに割り当てる

① ユーザーを割り当てるグループを選択して「 」をクリックします。例では「グループ名：マスター／エリア名：第一工場」にユーザーを割り当てます。




② ユーザーを選択して「＞」をクリックします。

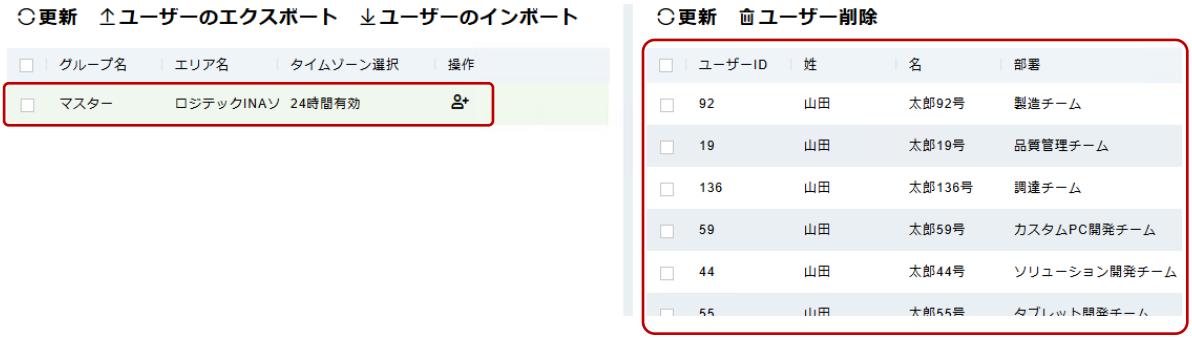
※1 ページあたりの表示件数にご注意ください。一括選択は表示されているユーザーしか選択されません。



③　設定を保存する場合は「OK」をクリックします。




④　グループに対してユーザーが割り当てられたことを確認します。




※グループが複数存在する場合は必要に応じて本項の設定を繰り返します。

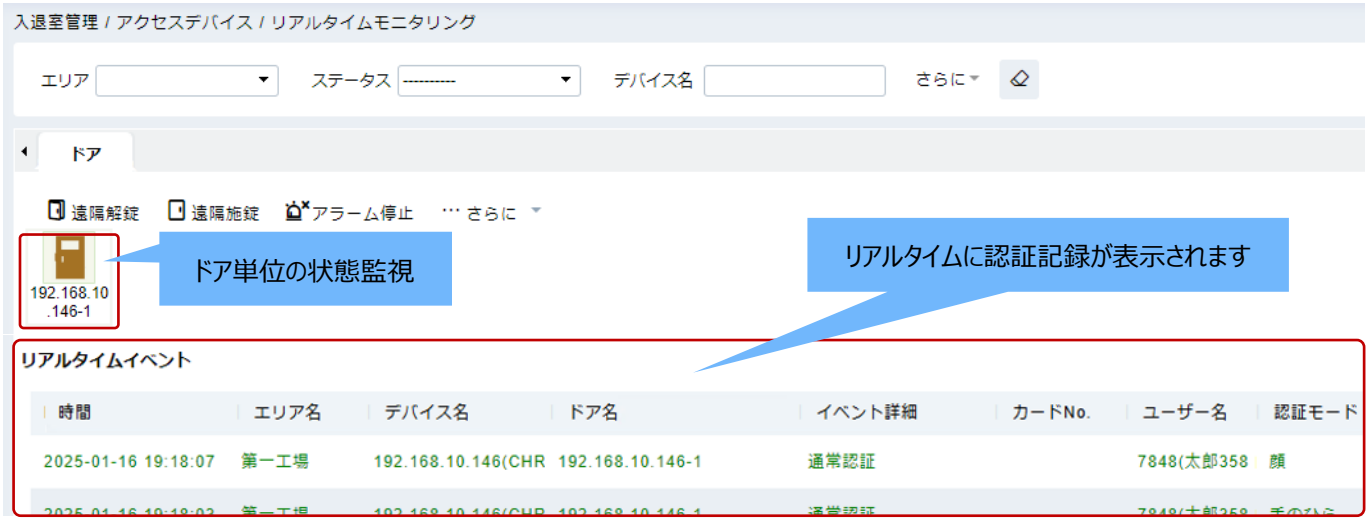
アクセス設定は、以上で終わりです。

## 8.7. リアルタイムモニタリング

入退室管理（導入編）STEP 一覧に戻る

**【管理ソフト：入退室管理 ＞ アクセスデバイス ＞ リアルタイムモニタリング】**

リアルタイムモニタリングは、認証履歴をリアルタイムでモニタリングすることができます。また、ドア単位で遠隔解錠・施錠、ドアアラームをなどのインシデントをモニタリングすることができます。なお、全ての認証履歴は「全トランザクション」を参照してください。



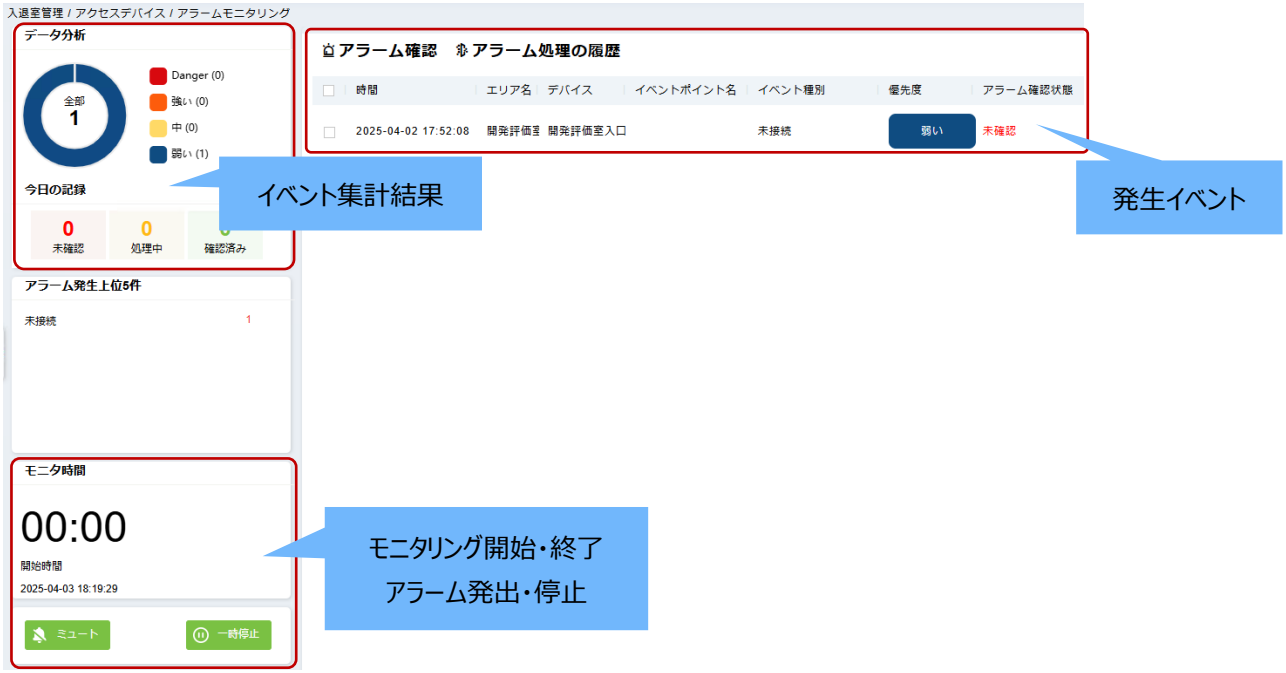

※アラームの種類は「9.16.9 リアルタイムモニタリング」を参照してください。

## 8.8. アラームモニタリング

入退室管理（導入編）STEP 一覧に戻る

**【管理ソフト：入退室管理 ＞ アクセスデバイス ＞ アラームモニタリング】**

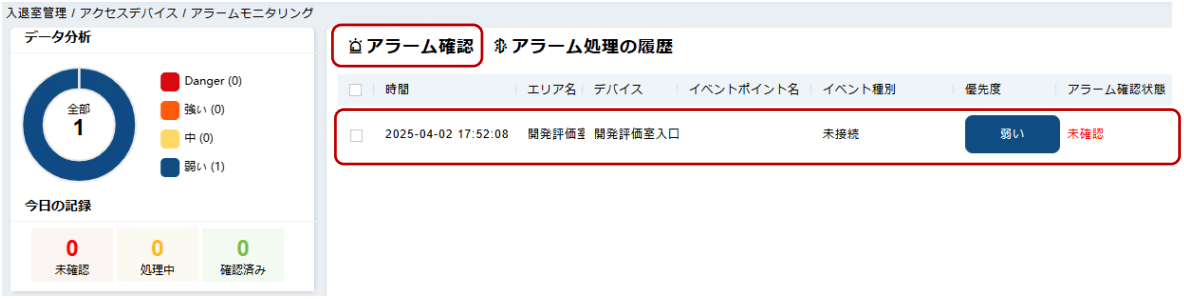
設置している顔認証デバイスで発生したイベントを一元管理できます。通信不良などのイベントが発生すると集計され、イベント毎に対応記録を保存して管理することができます。



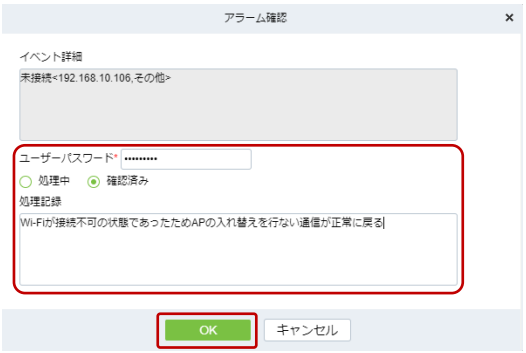
## 1. アラーム確認

発生したイベントをリアルタイムに表示し、対応履歴などを記録することができます。

① イベントを選択（チェック）して「アラーム確認」をクリックします。アラーム確認を行わない場合、ステータスは「未確認」の表示のままとなります。アラームの確認を行う場合のユーザーパスワードは管理ソフトへログインするためのパスワードを使用します。




② イベント毎に対応履歴を残すことができます。管理ソフトへログインするパスワードを入力し、対応区分「処理中」または「確認済み」を選択し、必要な場合処理記録を残します。内容を保存する場合は「OK」をクリックします。




## 2. モニタ時間

本機能でアラームモニタリングを実施することでイベント発生時にアラームを鳴らすことができます。

① モニタリングを開始するには、イベント発生時にアラームを鳴らす場合は「ミュート」を解除し、「一時停止」をクリックしてモニタリングを開始します（モニタ時間をカウントアップします）。




② アラームを停止します。アラームを停止するには、「アラーム確認」を実施する必要があります。アラーム音だけを一時的に停止したい場合は「ミュート」をクリックします。完全に停止する場合は「アラーム確認」の実施が必要です。

## 8.9. 全トランザクション

入退室管理（導入編）STEP 一覧に戻る

**【管理ソフト：入退室管理 ＞ アクセス制御レポート ＞ 全トランザクション】**

入退室管理における全ての履歴を確認できます。




全トランザクションは、期間指定、ユーザーID、デバイス名で絞り込み検索することができます。詳細検索を行う場合は「さらに▼」をクリックして検索条件（下図）を指定することができます。

（図）



## 8.10. 顔認証または他の認証を利用する場合

入退室管理（導入編）STEP 一覧に戻る

顔認証デバイスを使用して顔登録、掌情報、IC カード情報を登録します。また、IC カード情報は間違いがないように手入力ではなく、顔認証デバイスのカードリーダーを使用して登録します。

**注意事項**

**＊顔認証デバイスを使って顔登録を行う場合、同一エリア内の登録機の設定は 1 台のみで運用をお願いします。**
**同一エリア内で複数の登録機から同時にユーザー登録を行うとユーザー情報が正常に登録できません。**
**例）同一エリア内で 2 台の顔認証デバイスが稼働している場合**
**顔認証デバイス 2 台中 1 台を登録機に設定します。他の顔認証デバイスでも顔登録を行う場合、予め登録機として設定していた顔認証デバイスを解除してから新たに他の顔認証デバイスを登録機として設定します。**

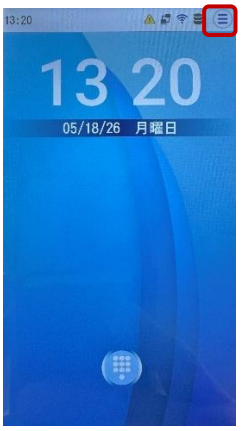
### 1. 管理ソフト：入退室管理 ＞ アクセスデバイス ＞ デバイス管理

① ユーザー情報を登録する顔認証デバイスを「登録機＊」であることを確認します。
※登録機の設定は、該当端末を選択（チェック）して、「セットアップ」→「登録機として設定」をクリックします。




### 2. 顔認証デバイスの設定

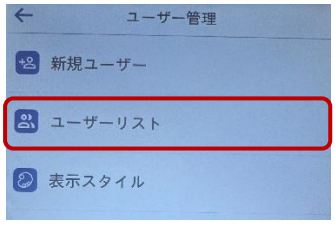
① 登録機のメインメニューを表示し「ユーザー管理」をタップします。







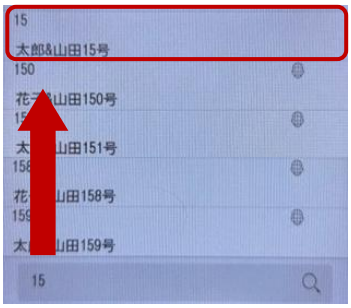
⑦ 「ユーザーリスト」をタップします。



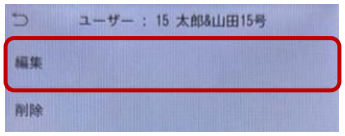
⑧　画面最下部にある検索フォームをタップし、ユーザー番号（ID）を入力して絞り込み検索をします。
※名前では検索できません



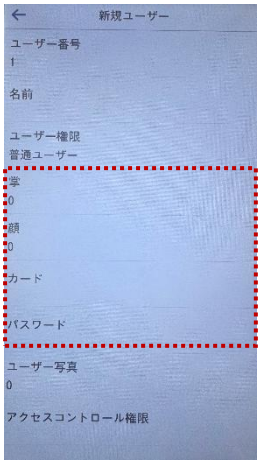

⑨　登録情報を更新（生体情報などの追加）するユーザーを選択（タップ）します。




⑩　「編集」をタップします。



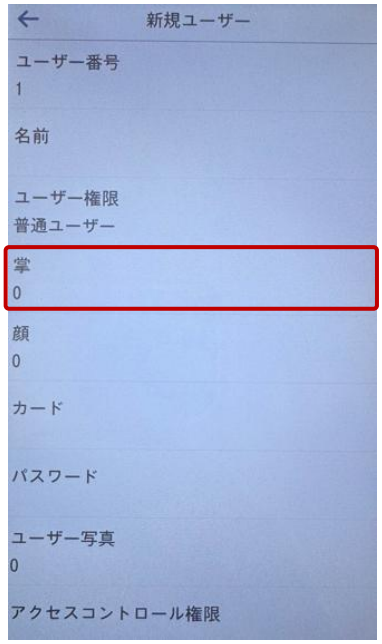

⑪　掌・顔・カードなど、認証に利用する項目をタップします。

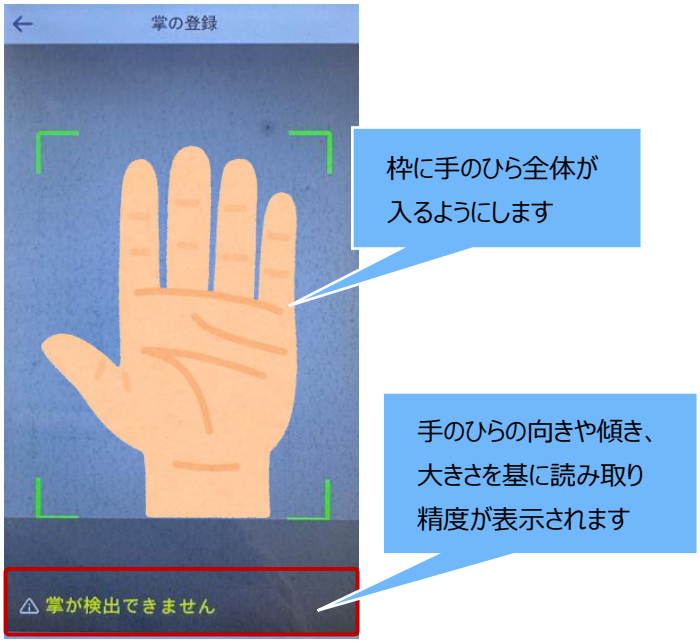


・ **掌情報を登録する場合**

「掌」をタップし、掌 1、掌 2 のいずれかをタップします。カメラが起動したら、15～30 センチの距離で手全体を枠の中に入れて登録します。最後に画面左上の「戻る」をタップして保存します。

※登録中は画面下に読み取り精度が表示されます。精度が悪い場合は再登録となります。



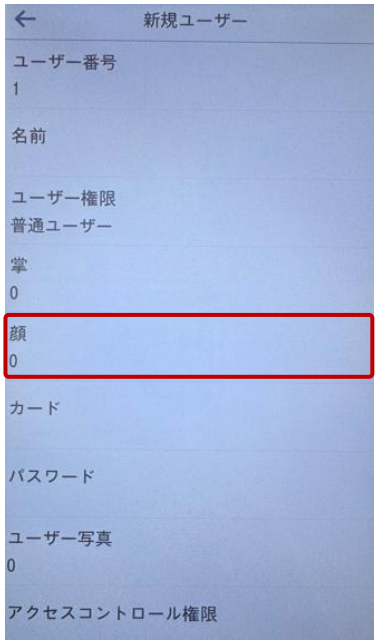



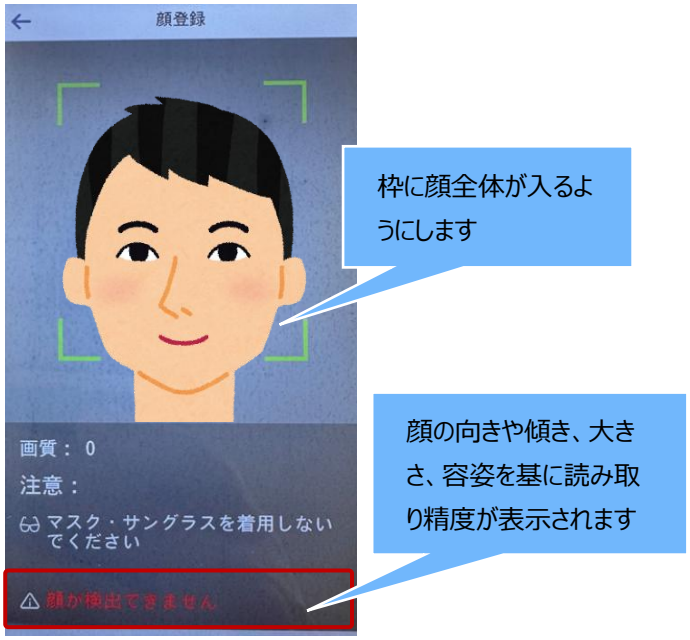

・ **顔情報を登録する場合**

「顔」をタップしてカメラを起動します。カメラが起動したら顔をかざして登録します。最後に画面左上の「戻る」をタップして保存します。

※登録中は画面下に読み取り精度が表示されます。精度が悪い場合は再登録となります。

「顔登録ガイドライン」を参照して写真の撮り直しをお願いします。



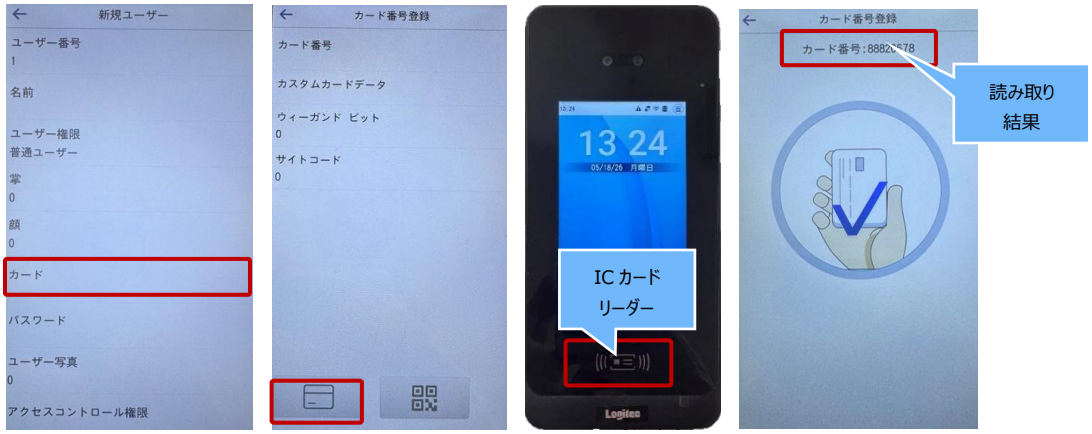
・ **IC カード情報*を登録する場合 ※１枚のカード情報を複数のユーザーに登録することはできません。**

(ア) 「カード」をタップします。 ※入退 Push の場合「カードを追加」をタップしてから(イ)の手順へ

(イ) IC カードアイコンをタップします。

(ウ) 本体前面の IC カードリーダーに IC カード*をかざします。

(エ) IC カードの読み取り結果を確認し、最後に画面左上の「戻る」をタップして保存します。



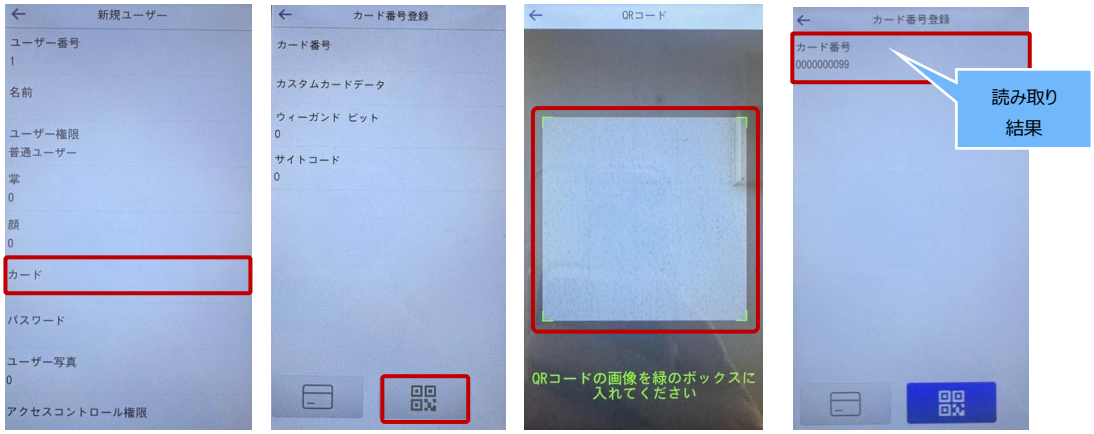

・ **QR 情報*を登録する場合（静的 QR） ※半角数字／最大 20 桁、同じ番号ををを複数のユーザーに登録することはできません。**

(ア) 「カード」をタップします。 ※入退 Push の場合「カードを追加」をタップしてから(イ)の手順へ

(イ) QR アイコンをタップします。

(ウ) カメラが起動したら、枠内に QR をかざします。

(エ) QR 読み取り結果を確認し、最後に画面左上の「戻る」をタップして保存します。




**注意事項**

***IC カード情報は、FeliCa：ISO/IEC 18092「NFC Type F」、MIFARE：ISO/IEC 14443「Type A」に対応**

***IC カードの ID 取得（読み取り）のみをサポートします。動作確認済みのカードは以下の通りです。**

**・「FeliCa」の「IDm」情報**

**・「Mifare Plus」の「UID」情報**

**・「Mifare Ultralight EV1」の「UID」情報**

**・「Mifare Classic 1K」の「UID」情報**

***IC カード情報および QR 情報について**

**・IC カード情報と QR 情報は、入退 Push モードの場合、カード登録数（50,000）の範囲で複数登録できます。勤怠 Push モードの場合、IC カードまたは QR のいずれかの登録（排他）ができます。**

**・IC カード情報または QR 情報を削除する場合は、「ユーザーリスト」の「削除」から「カード番号のみ削除」を行ってください。**

・ **パスワード情報を登録する場合（6 桁以上、最大 8 桁の数字）**

(ア) 「パスワード」をタップします。

(イ) パスワードを入力します。

(ウ) 「パスワードを再入力してください」と表示されます。もう一度設定するパスワードを入力します。

(エ) 最後に画面左上の「戻る」をタップして保存します。



# 9. 管理ソフトの機能説明

管理ソフトのユーザーインターフェイスは、標準 UI と詳細 UI の 2 種類あります。当社でサポートするのは「標準 UI」です。詳細 UI についてのお問合せには対応できかねます。お客様の責任の下、ご使用ください。なお、ユーザーインターフェイスの切り替えは「9.1.13 パラメータ」の「ソフトウェア選択」を参照してください。

## 9.1. システム管理




「システム管理」メニューは、入退室管理および勤怠管理における管理ソフトの導入時の基本設定（共通）を行います。当社がサポートする標準 UI は（表 1）を参照してください。

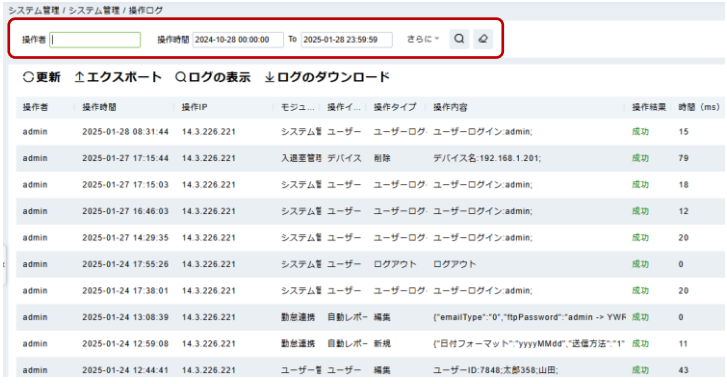
（表 1）当社がサポートする「システム管理（標準 UI）」メニューの一覧

| 大分類 | 中分類 | 標準 UI | 詳細 UI | 説明 |
|---|---|---|---|---|
| システム管理 | 操作ログ | ○ | ○ | 管理ユーザーを特定し、管理ソフトで行った操作と結果を記録・管理します。 |
| | データ管理 | ○ | ○ | 管理ソフトのデータベースについてバックアップの設定をします。 |
| | エリア設定 | ○ | ○ | 端末を設置する管理拠点（エリア）を設定します。 |
| | Email 管理 | ○ | ○ | システムから通知を受けるためのメールサーバーを設定します。「パスワードリマインダー」や「メッセージ通知」機能を利用する場合に設定が必要です。 |
| | 辞書管理 | × | ○ | 当社または本製品ではサポート対象外です。 |
| | データクリーニング | ○ | ○ | 管理ソフト上に記録されるデータの保持期間などを設定します。 |
| | リソースファイル | × | ○ | 当社または本製品ではサポート対象外です。 |
| | クラウド設定 | × | ○ | 当社または本製品ではサポート対象外です。 |
| | ID タイプ | × | ○ | 当社または本製品ではサポート対象外です。 |
| | プリントテンプレート | × | ○ | 当社または本製品ではサポート対象外です。 |
| | システム監視 | ○ | ○ | 管理ソフトが稼働する PC またはサーバー機器のシステムリソースを管理します。 |
| | メッセージ通知 | ○ | ○ | システムから送信するイベント通知の種類を設定します。 |
| | パラメータ | ○* | ○ | 日付表示形式などを設定します。初期値で運用します。 |

*サポート対応メニューの中でも当社または製品でサポートしない機能を明示しています。

### 9.1.1. 操作ログ

管理ソフト上で操作した内容を記録し確認することができます。管理ソフトにログインしたユーザー名や操作期間を指定して絞り込み検索することができます。



## 9.1.2. データ管理

「データ管理」は、管理ソフト上に保存されたデータベースのバックアップについての設定をします。万が一のデータ消失に備えて、必ず定期的な手動バックアップまたは自動バックアップの設定をしてください。なお、インストール時に指定したバックアップ先を変更するには「11.4 データベースのバックアップ先変更」を参照してください。

### 1. FTP サーバー設定

管理ソフトのインストール時に設定したバックアップ先（初期値：C:¥SecurityDBBack）とは別に、FTP サーバーが利用できる場合、本機能を設定することで手動または自動バックアップと同時に FTP サーバーへバックアップを作成します。

① 「FTP サーバー設定」をクリックします。




② FTP サーバー設定画面が開きます。FTP サーバーへ接続に必要な情報を入力します。（情報はお客様の情報システム部門へお問い合わせください）

※下図は入力例です




| 設定項目 | 内容 |
|---|---|
| FTP サーバーアドレス* | FTP サーバーの IP アドレスを指定します。 |
| ポート* | FTP で使用するポート番号を指定します。 |
| フォルダの場所 | バックアップ先のフォルダを指定します。大文字小文字を識別します。 |
| ユーザー名* | FTP に接続可能なアカウントのユーザー名を指定します。 |
| パスワード* | FTP に接続可能なアカウントのパスワードを指定します。 |
| テスト接続 | 上記で設定した内容で FTP サーバーに接続できるかどうかのテストを実行します。 |

*は必須項目です。

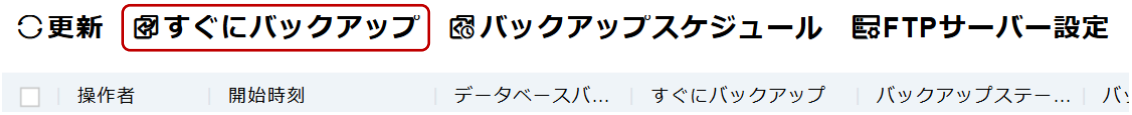
③ 「テスト接続」をクリックして、入力した情報で FTP サーバーへ接続できるか確認します。接続に成功すると「接続に成功しました！」と表示されます。設定を完了するために「OK」をクリックします。



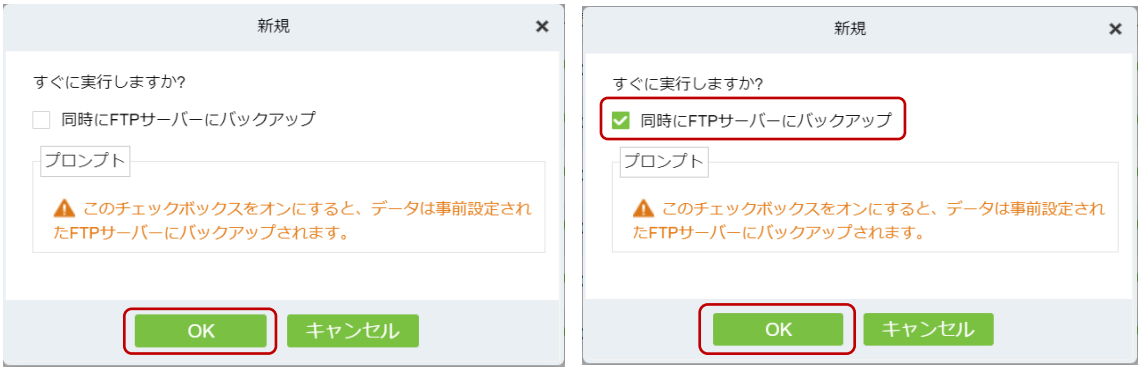
## 2. すぐにバックアップ（手動）

任意のタイミングでデータベースのバックアップを作成します。バックアップの作成先は、管理ソフトのインストール時に設定したバックアップ先（初期値：C:¥SecurityDBBack）です。インストール時に変更されている場合は、変更したバックアップ先が初期値になりますので、変更先のフォルダをご確認ください。

① 「すぐにバックアップ」をクリックします。

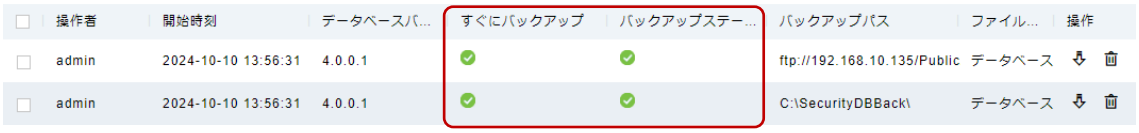



② すぐにバックアップの実行画面が開きます。「同時に FTP サーバーにバックアップ」にチェックを入れると、「C:¥SecurityDBBack」と前項「FTP サーバー設定※」で指定した FTP サーバーへバックアップを作成します。
※予め FTP サーバー設定がされていない場合、チェック時にエラーとなります。




③ 最後に「OK」をクリックします。

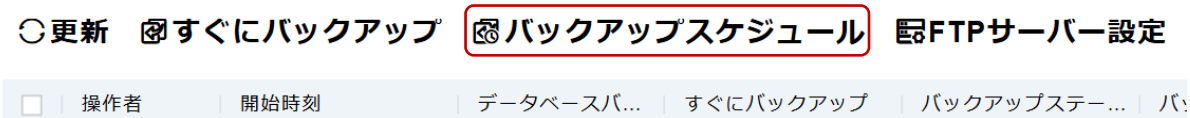
④ すぐにバックアップ（手動）の直後に、バックアップ実行日時などの情報が記録されます。
「すぐにバックアップ」と「バックアップステータス」に緑チェックが表示されていれば、バックアップは正常に完了しています。




## 3. 自動バックアップ

指定した日時と間隔でデータベースのバックアップを自動で作成します。バックアップの作成先は、管理ソフトのインストール時に設定したバックアップ先（初期値：C:¥SecurityDBBack）です。バックアップ先を変更している場合は、変更先のフォルダをご確認ください。

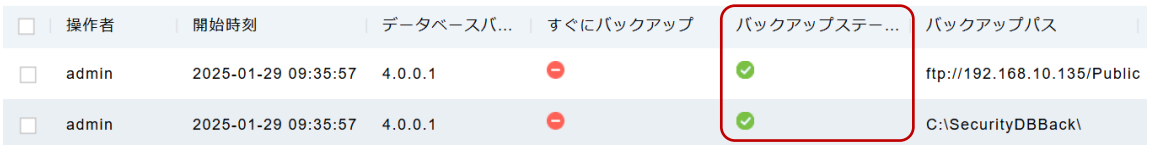
① 「バックアップスケジュール」をクリックします。



② バックアップスケジュール設定画面が開きます。From で「開始日時」を指定し、バックアップの作成間隔を「日数」で指定します。「同時に FTP サーバーにバックアップ」にチェックを入れると、「C:¥SecurityDBBack」と前項「FTP サーバー設定※」で指定した FTP サーバーへバックアップを作成します。最後に「OK」をクリックします。
※予め FTP サーバー設定がされていない場合、チェック時にエラーとなります。



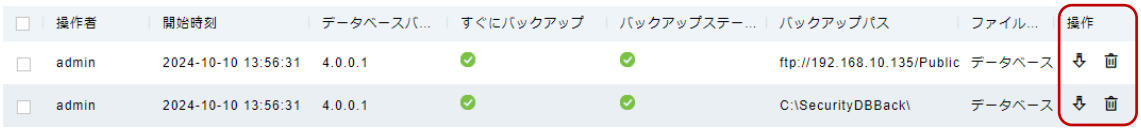

③ スケジュール通りバックアップが実行された場合、バックアップの実行日時などの情報が記録されます。「バックアップステータス」に緑チェックが表示されていれば、バックアップは正常に完了しています。



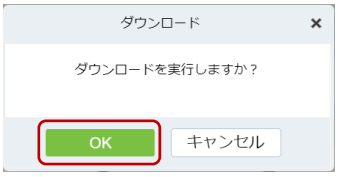

## 4. バックアップファイルのダウンロードおよび削除

過去に作成されたバックアップファイルをダウンロードまたは削除することができます。バックアップファイルは、運用期間が長くなるほどデータ容量が肥大化して PC またはサーバー機器のディスク容量を消費します。定期的にメンテナンスして削除することをお勧めします。なお、「9.1.6 データクリーニング」ではバックアップファイルを自動で削除する方法も説明しています。

① バックアップ記録の「操作」を参照します。



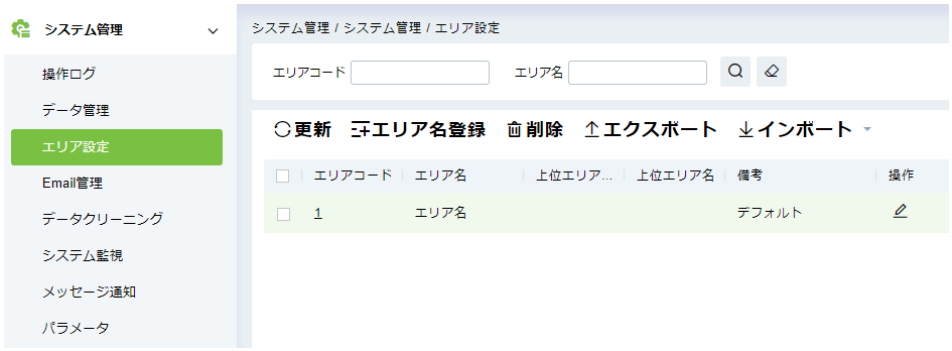

② バックアップファイルをダウンロードする場合、「矢印」アイコンをクリックします。ダウンロードするには「OK」をクリックします。




③ バックアップファイルを削除する場合は、「ゴミ箱」アイコンをクリックします。削除するには「OK」をクリックします。



## 9.1.3. エリア設定



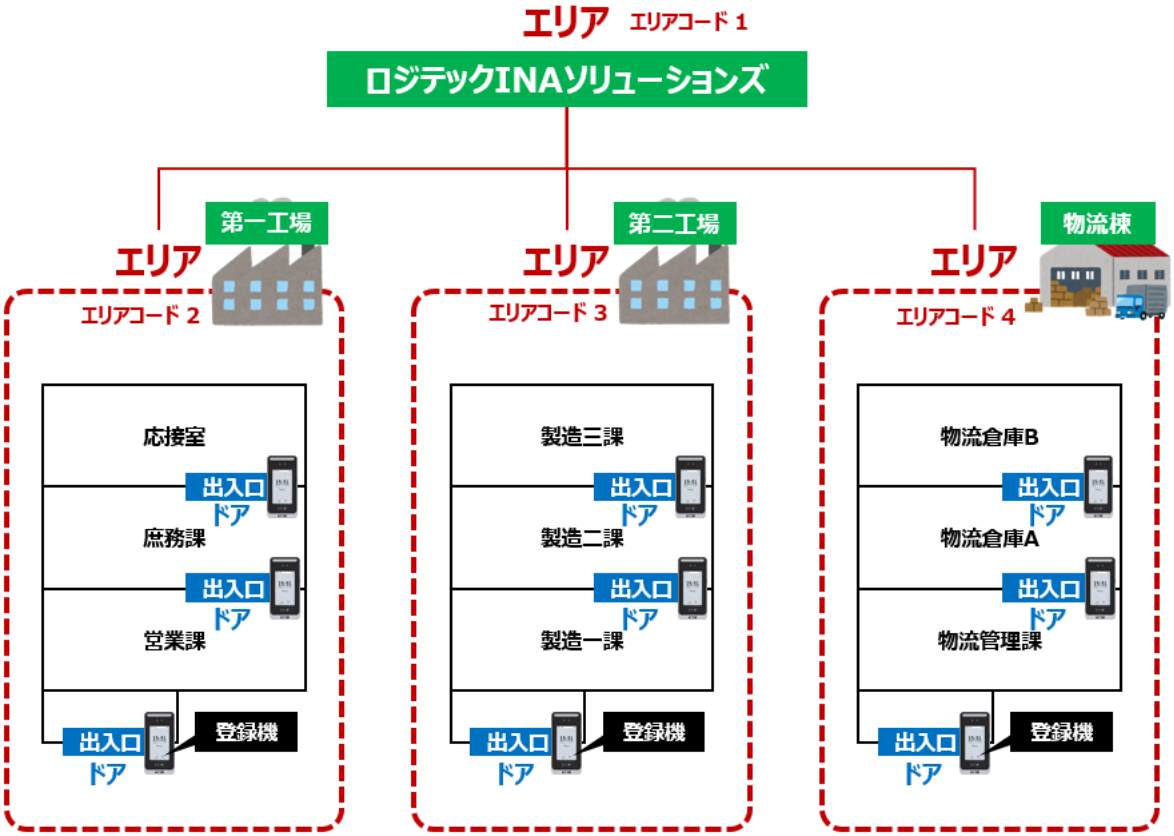

「エリア」とは、顔認証デバイスを導入して管理する「拠点」を示します。初期値で「エリア名」というエリア名が設定されています。この「エリア名」というエリア名は、お客様の社名に変更して使用します。また、顔認証デバイスを導入して管理する拠点が複数ある場合、拠点毎にエリアを設定します*。複数の拠点がない場合、１つのエリア（お客様の社名）のみで運用することができます。

**注意事項**

***外部勤怠管理システムの一部ではこのエリア設定で設定されたエリアコードで勤務場所を特定します。お客様の運用に応じてエリア名とエリアコードの設定をお願いします。**

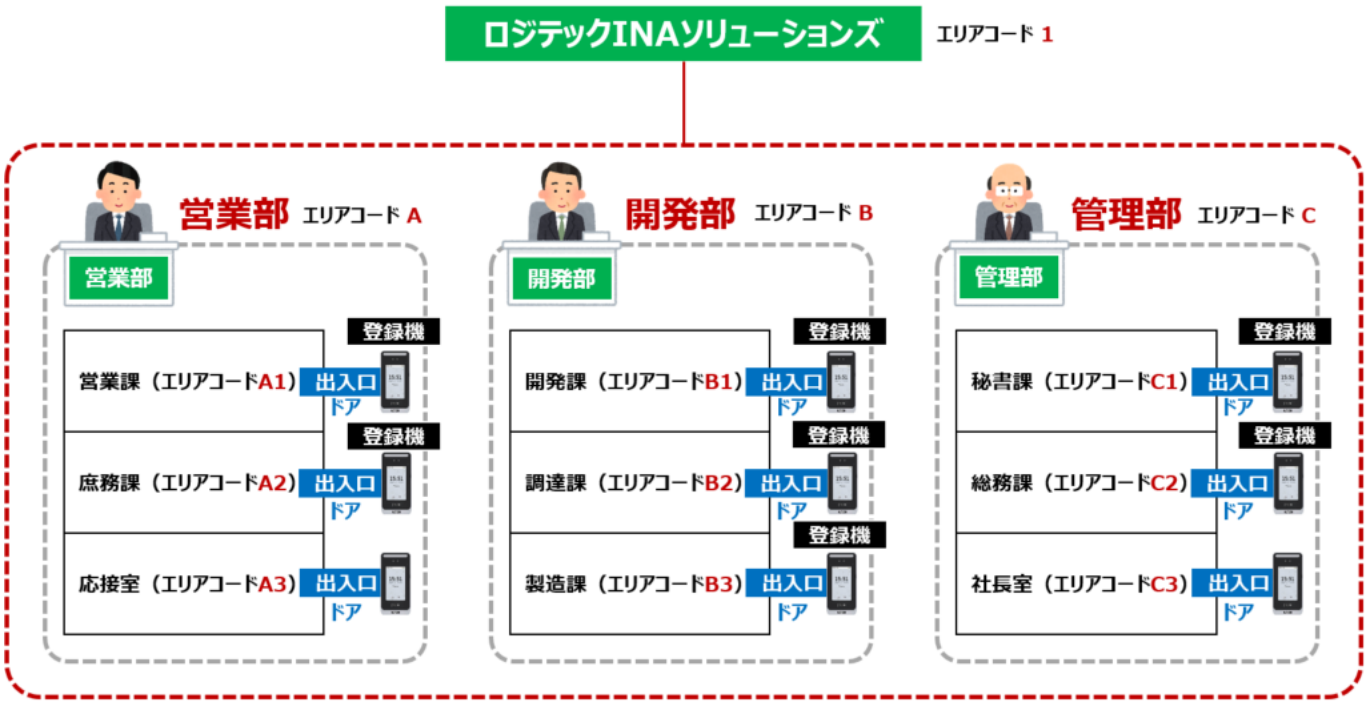
**【複数拠点の例】**

複数の拠点があり、拠点毎にエリアを作成して管理する場合は以下の通りです。顔認証デバイスは登録機として、エリア毎に１台だけ設定することができます。



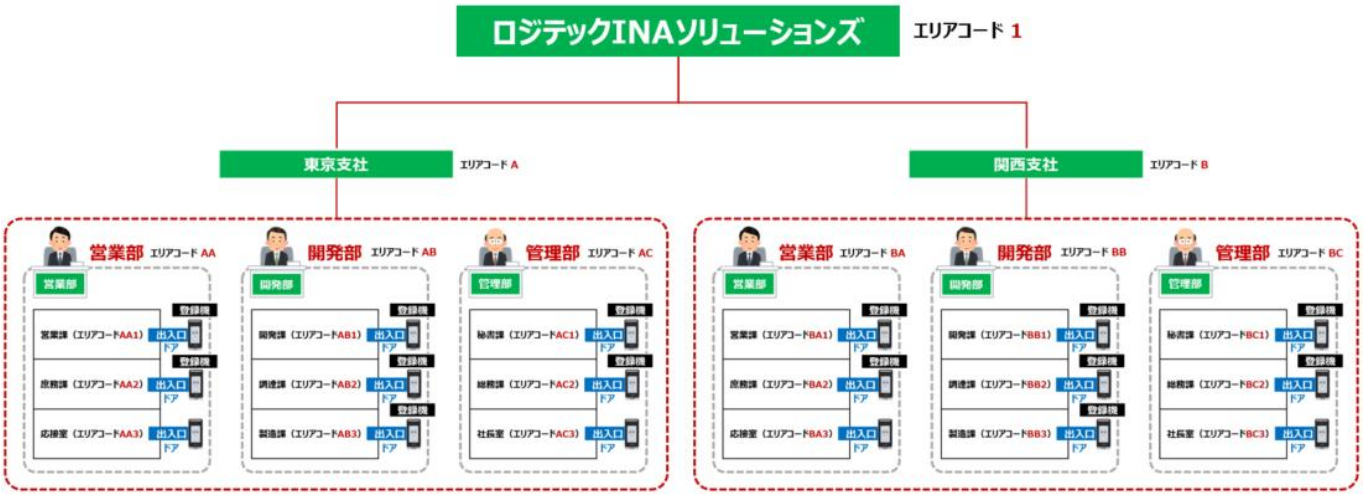
**【単一拠点の例】**

１つの拠点で、部門及び部署単位でエリアを作成して管理する場合は以下の通りです。顔認証デバイスは登録機として、エリア毎に１台だけ設定することができます。




**【拠点毎のエリアを細分化する例】**

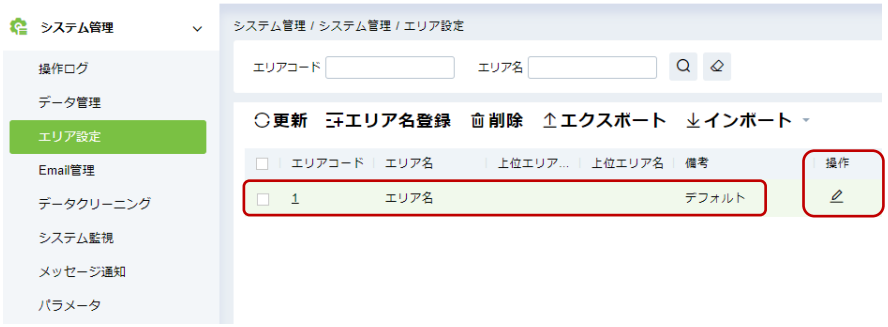
複数の拠点があり、部門及び部署単位でエリアを作成して管理する場合は以下の通りです。顔認証デバイスは登録機として、エリア毎に１台だけ設定することができます。



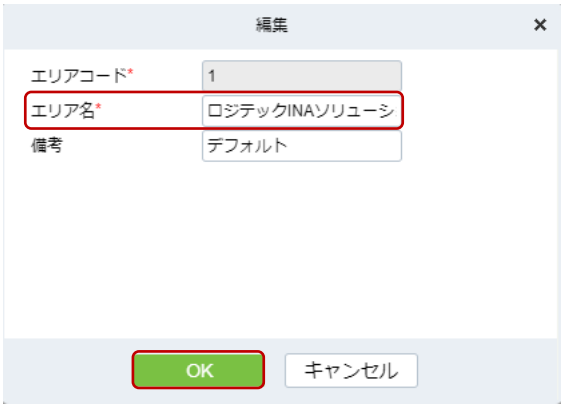
## 1. エリア名の変更

顔認証デバイスで勤怠管理または入退室管理を行う拠点が１つの場合、管理ソフトに初期値で登録されている「エリア名」というエリアを編集します。

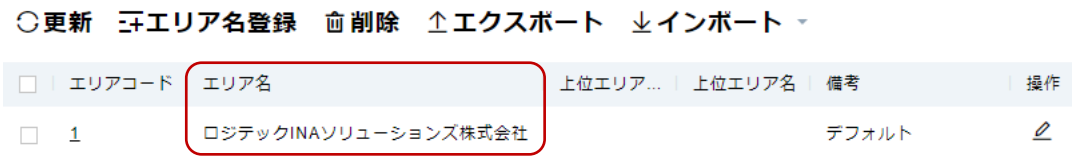
① 初期値で登録されている「エリアコード１ ：エリア名」を、お客様の会社名などに変更します。
変更するには「操作」の「編集」をクリックします。




② 編集画面が開いたら、エリア名を変更します。例は「ロジテック INA ソリューションズ株式会社」です。
設定を保存するには「OK」をクリックします。
※初期値で登録されているエリアコード「１」は編集することはできません。




③ 設定が反映されていることを確認します。

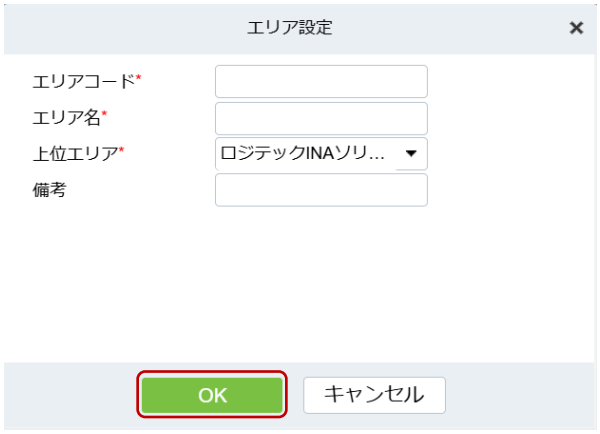


## 2. エリア名登録

顔認証デバイスで勤怠管理または入退室管理を行う拠点が複数の場合、前項「**1.初期値（エリア名）の変更**」の手順に加え、拠点数分のエリアを登録します。




① 「エリア名登録」をクリックし、「エリアコード」「エリア名」を入力します。上位エリアを変更する場合は「上位エリア」から選択してください。




| 設定項目 | 内容 |
|---|---|
| エリアコード* | 1～30 字の半角英数字を指定します。 |
| エリア名* | 1～30 文字を入力します。 |
| 上位エリア* | 登録するエリアの上位エリアを指定します。 |
| 備考 | 1～50 文字の自由入力欄です。 |

*は必須項目です。

② 最後に設定を保存する場合は「OK」をクリックします。

**登録例）**

| エリアコード | エリア名 | 上位エリア... | 上位エリア名 | 備考 | 操作 |
|---|---|---|---|---|---|
| 1 | ロジテックINAソリューションズ株式会社 | | | デフォルト | |
| 2 | 第一工場 | 1 | ロジテックINA | | |
| 3 | 第二工場 | 1 | ロジテックINA | | |
| 4 | 物流棟 | 1 | ロジテックINA | | |

エリア名登録は、以上で終わりです。

## 3. エリアの削除

登録したエリアを個別削除または一括削除することができます。

① 個別削除

登録情報の「操作」にある「ゴミ箱」アイコンをクリックします。



| | エリアコード | エリア名 | 上位エリア... | 上位エリア名 | 備考 | 操作 |
|---|---|---|---|---|---|---|
| | 1 | ロジテックINAソリューションズ株式会社 | | | | |
| | 2 | 第一工場 | 1 | ロジテックINAソリューションズ株式会社 | | |
| | 3 | 第二工場 | 1 | ロジテックINAソリューションズ株式会社 | | |
| | 4 | 第一物流倉庫 | 1 | ロジテックINAソリューションズ株式会社 | | |
| | 5 | 第二物流倉庫 | 1 | ロジテックINAソリューションズ株式会社 | | |
| | 6 | ドミトリー | 1 | ロジテックINAソリューションズ株式会社 | | |

② 一括削除

エリアコード左のチェックボックスをクリック[1]すると全てのエリアが選択されます。初期値で設定されているエリアコード「1」は削除不可（編集可）のためチェックを外し[2]、「削除」をクリック[3]します。

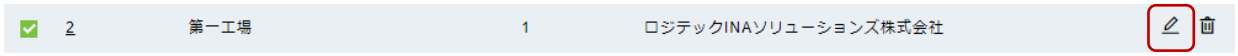
※削除するエリアに下位エリアが含まれている場合は、下位エリアを削除しないと上位エリアは削除できません。

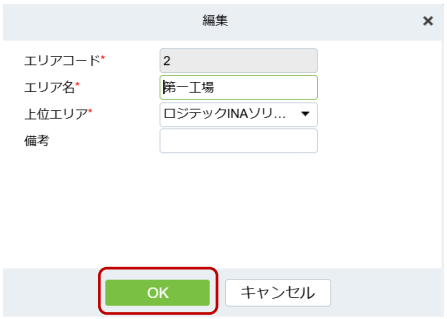



エリアの削除の説明は、以上で終わりです。

### 4. 編集

登録エリアの「編集」アイコンをクリックします。登録情報の修正をして最後に「OK」をクリックします。

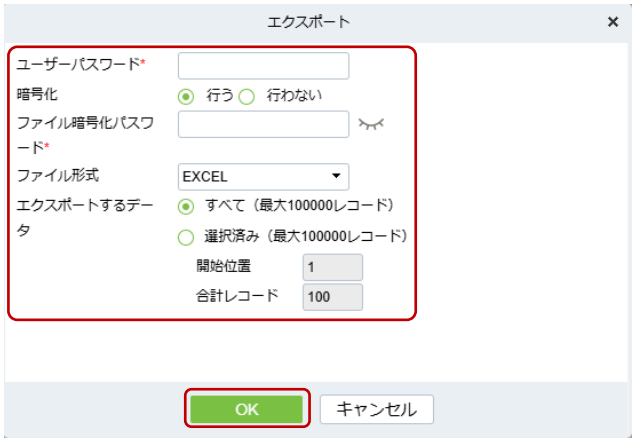



### 5. エクスポート

登録したエリアの一覧を EXCEL・PDF・CSV・TXT のいずれかの形式でエクスポートすることができます。各条件を指定して最後に「OK」をクリックします。なお、暗号化した場合、Windows 標準の解凍ツールは使用できません。



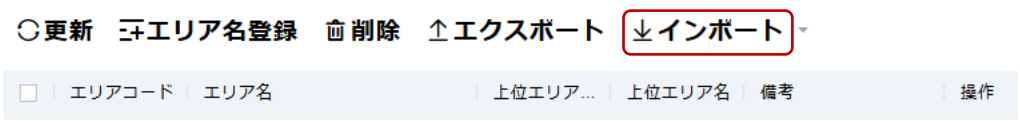

| 設定項目 | 内容 |
|---|---|
| ユーザーパスワード* | 管理者ユーザーのパスワードを入力します。 |
| ファイル暗号化 | データの暗号化を指定します。 |
| ファイル暗号化パスワード* | ファイル暗号化を指定した場合、復号化するパスワードを指定します。 |
| ファイル形式 | EXCEL・PDF・CSV・TXT から選択します。 |
| エクスポートするデータ | すべて：最大 10 万件を上限にの全データをダウンロードします。 |
| | 選択済み：開始レコードと上限（終了レコード）を指定してダウンロードします。 |

*印は必須です。

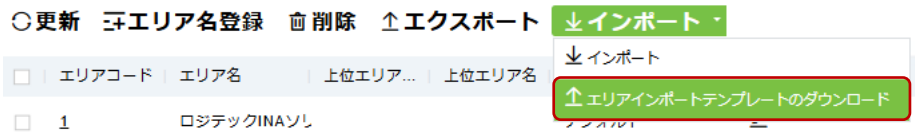
エクスポートの説明は、以上で終わりです。

### 6. インポート

インポート用のフォーマットを使用して一括登録することができます。



① インポートテンプレートをダウンロードします。

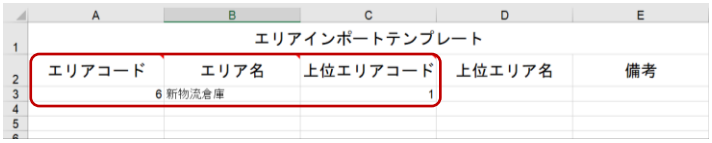



インポートテンプレート：　エリアインポートテンプレート_20241010190401.xls

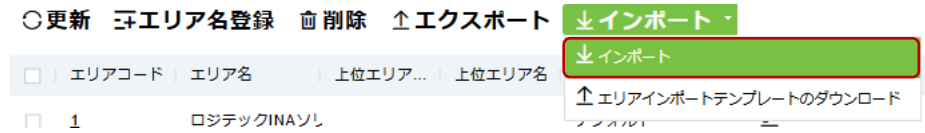
※Windows®の場合、初期値で「ダウンロード」フォルダに保存されます。

② ダウンロードしたインポートテンプレートに情報を入力して「上書き保存」します。

必須項目：エリアコード、エリア名、上位エリアコード

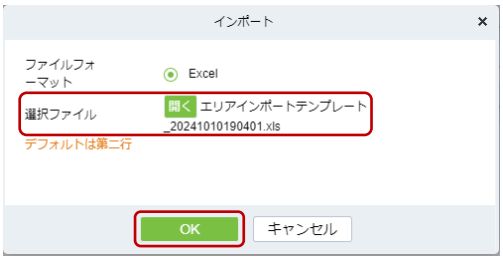


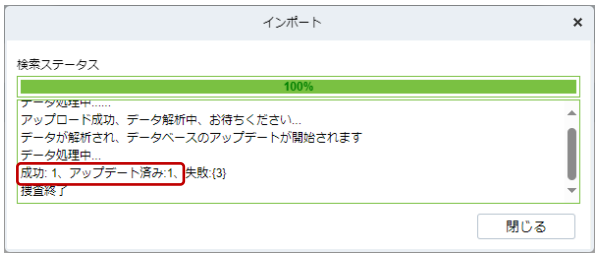

③ 「インポート」をクリックします。



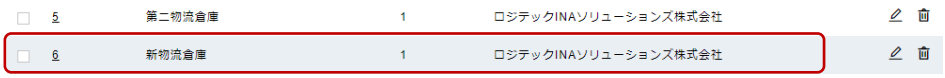

④ 「開く」をクリックし、インポートするインポートテンプレートを選択します。最後に「OK」をクリックします。

インポートの進捗が表示され、最後にインポート結果が表示されます。




⑤ インポート後、正常にエリアが登録されているかを確認してください。




## 9.1.4. Email 管理

「Email 管理」は、管理ソフトから配信されるメールの送信メールサーバーの設定や各種メール配信の履歴を管理します。管理ソフトのログインに使用するパスワードのリマインダーや、予め設定された入退や勤怠のトランザクションの結果通知に使用されます。事前に送信メールサーバーの設定をお勧めします。

## 1. 送信メールサーバー設定

送信メールサーバーの設定をすることで、管理ソフトからの各種通知を受信することができます。

① 「送信メールサーバー設定」をクリックします。




② 送信メールサーバー設定画面が開きます。




| 設定項目 | 内容 |
|---|---|
| Email 送信サーバー* | 送信サーバードレスを指定します。 |
| 通信ポート* | 通信に使用するポート番号を指定します。 |
| 認証方式 | 選択すると自動で通信ポートが設定されます。通信ポートは手動設定可。 |
| Email アカウント* | 送信サーバーに接続可能な Email アカウントを入力します。 |
| パスワード | 送信サーバーに接続可能なパスワードを入力します。 |
| 送信者名 | 送信者名を任意に設定できます。 |
| テスト接続 | 送信サーバーへの接続テストをします。 |

*は必須項目です。

③ 「テスト接続」をクリックして、入力した情報で送信メールサーバーへ接続できるか確認します。
送信メールサーバーへ接続ができると「成功」と表示されます。







## 2. メール送信履歴

① Email 管理は、管理ソフトから送信されたメール送信履歴を確認することができます。件名に応じて発生したイベントを特定することができます。下記例の「件名：パスワードを忘れた」は、管理ソフトにログインするためにパスワードリマインダーを誰から誰に実行したことがわかります。



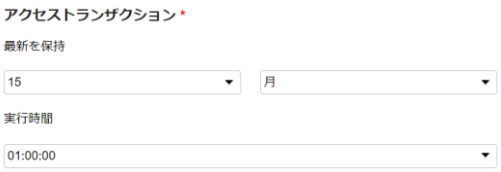
### 9.1.5. 辞書管理

当社または本製品はサポート対象外です。

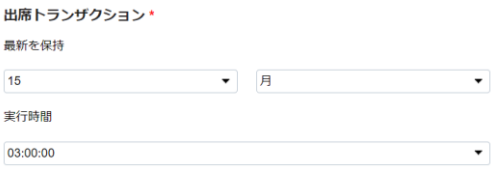
### 9.1.6. データクリーニング

データクリーニングは管理ソフト上に保存された各種データを指定した内容で自動削除します。毎日 1 回の頻度で実行され、設定された日付の前の月数を削除します。最後に各設定を反映するには [OK]をクリックします。

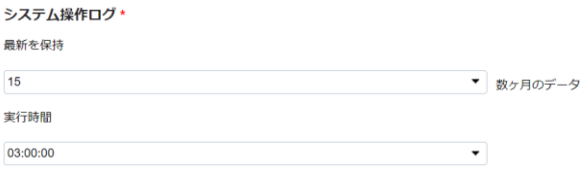
1. **履歴 – アクセストランザクション**
   データ保持期間（最新を保持）：1～36 か月を選択（初期値：15 か月）
   クリーンアップ実行時間（実行時間）：00：00：00～23：00：00 を選択（初期値：01：00：00）



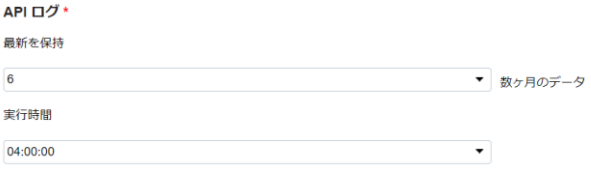

2. **履歴 – 勤怠トランザクション**
   データ保持期間（最新を保持）：1～36 か月を選択（初期値：15 か月）
   クリーンアップ実行時間（実行時間）：00：00：00～23：00：00 を選択（初期値：03：00：00）



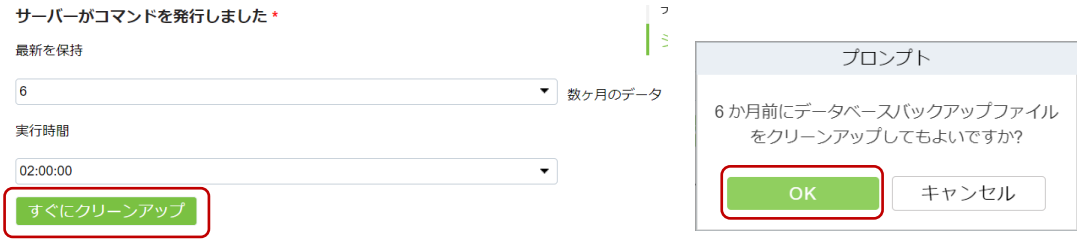

3. **システム – システム操作ログ**
   データ保持期間（最新を保持）：1～36 か月を選択（初期値：15 か月）
   クリーンアップ実行時間（実行時間）：00：00：00～23：00：00 を選択（初期値：03：00：00）



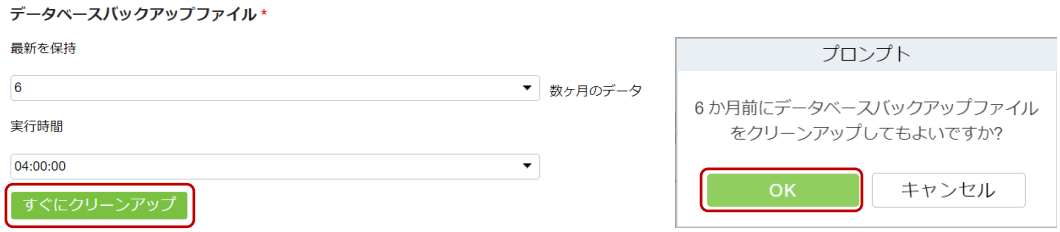

4. **システム – API ログ** ※当社ではサポートしません
   データ保持期間（最新を保持）：1～36 か月を選択（初期値：6 か月）
   クリーンアップ実行時間（実行時間）：00：00：00～23：00：00 を選択（初期値：04：00：00）



5. **システム – サーバーコマンド** ※手動でクリーンアップを実行する場合は「すぐにクリーンアップ」をクリックします。
   データ保持期間（最新を保持）：1～36 か月を選択（初期値：6 か月）
   クリーンアップ実行時間（実行時間）：00：00：00～23：00：00 を選択（初期値：02：00：00）




6. **システム – データベースバックアップファイル** ※手動でクリーンアップを実行する場合は「すぐにクリーンアップ」をクリックします。
   データ保持期間（最新を保持）：1～36 か月を選択（初期値：6 か月）
   クリーンアップ実行時間（実行時間）：00：00：00～23：00：00 を選択（初期値：04：00：00）




データクリーニングの設定は、以上で終わりです。

### 9.1.7. リソースファイル

当社または本製品はサポート対象外です。

### 9.1.8. クラウド設定

当社または本製品はサポート対象外です。

### 9.1.9. ID タイプ

当社または本製品はサポート対象外です。

### 9.1.10. プリントテンプレート

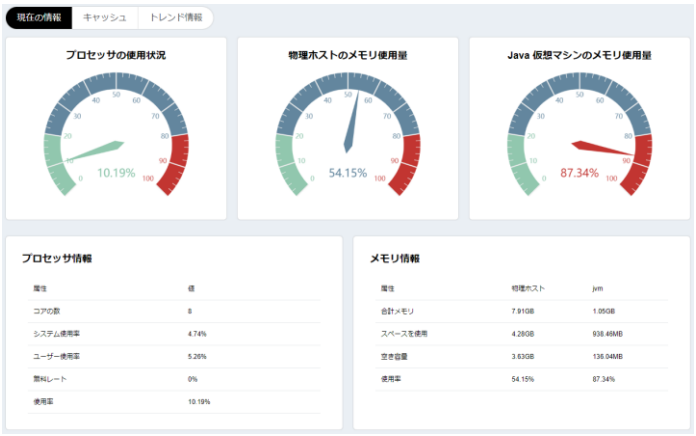
当社または本製品はサポート対象外です。

## 9.1.11. システム監視（参考情報）

管理ソフトがインストールされている PC またはサーバー機器の各種リソースをモニタリングできます。

**【現在の情報】**

CPU の情報・使用率、ホストのメモリ情報・使用率、Java 仮想マシンの情報・使用率などの状態について確認できます。




プロセッサ情報

| 属性 | 値 |
|---|---|
| コアの数 | PC/サーバーに実装されている CPU のコア数 |
| システム使用率* | システムが CPU を占有する割合 |
| ユーザー使用率 | アプリケーションが CPU を占有する割合 |
| 無料レート | アイドル（処理が無い）時間の割合<br>※通常は何等かの処理で動作しています |
| 使用率 | システム使用率＋ユーザー使用率 |

*データベースの読み込みやメール送信を行う際、アプリケーションは OS のインターフェースやハードウェアを介してデータベースやメールサーバーと通信します。このとき、OS がファイルの読み書きやネットワーク通信のために CPU を使用する部分をシステム使用率としています。

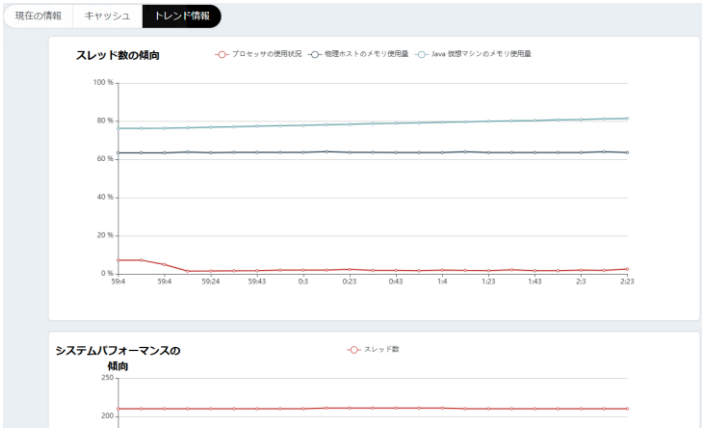
**【キャッシュ】**

クライアント情報、Redis サーバー情報、メモリ情報、および現在のデータベースの状態について確認できます。



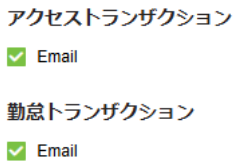

**【トレンド情報】**

CPU 使用率、メモリ使用率などをグラフィカルに表示します。



## 9.1.12. メッセージ通知

初期値（チェック）のままで使用します。チェックを外すと各種トランザクションのメール送信ができなくなります。



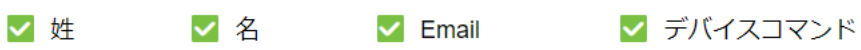

## 9.1.13. パラメータ

システム上で共通で使用されるパラメータを設定します。最後に各設定を保存するには「OK」をクリックします。

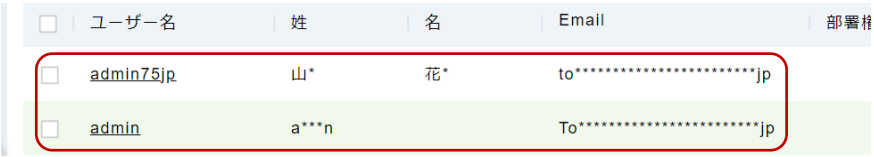
1. **QR コード設定**
   当社または本製品ではサポート対象外です。

2. **日付フォーマット設定（初期値：日付 2022-01-01／時間 00:00:00）**
   勤怠管理おける外部システム連携に影響しますので、初期値で使用してください。

3. **個人情報の保護**
   管理ソフト上の管理者ユーザーアカウント情報について、画面上で情報の表示・非表示を設定します。表示したい項目のチェックボックスを「OFF（外す）」にします。「管理ソフト：システム管理→権限管理→ユーザー」で確認することができます。
   初期値：姓／非表示、名／非表示、Email／非表示、デバイスコマンド／非表示

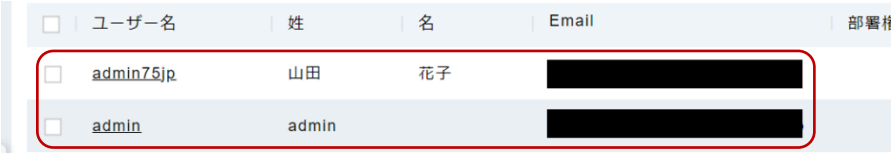



（例 1）初期値では、管理ユーザーの情報は下記のように表示されます。




（例 2）チェックボックスを外すと下記のように表示されます



### 4. ソフトウェア選択（初期値：標準 UI）

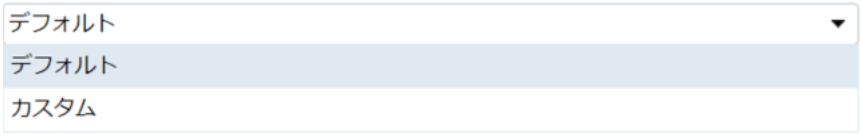
管理ソフトのユーザーインターフェイスは、標準 UI と詳細 UI の 2 種類あります。当社でサポートするのは「標準 UI」です。詳細 UI についてのお問合せには対応できかねます。お客様の責任の下、ご使用ください。なお、ユーザーインターフェイスの切り替えは UI を選択して「OK」をクリックします。




### 5. プライバシーポリシー

セルフユーザー登録時に表示するプライバシーポリシーです。テキストファイルをインポートして、独自のプライバシーポリシーを表示することができます。プライバシーポリシーをカスタマイズする方法は以下の通りです。

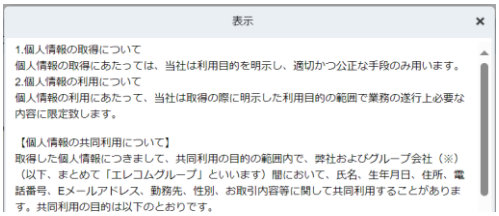
① 「デフォルト」から「カスタム」を選択します。




② 「インポート」をクリックして、プライバシーポリシーを記載したテキストファイルを選択します。
※テキストファイル保存時の「**文字コード**」は「UTF-8」を指定してください。




③ インポート完了後、「表示」をクリックします。インポートした内容が文字化けしていないことを確認します。
※文字化けする場合、前項のテキストファイル保存時の「文字コード」を確認してください。




プライバシーポリシーの説明は、以上で終わりです。

## 9.2. 権限管理

**【管理ソフト：システム管理 ＞ 権限管理】**

管理ソフト上の権限管理を設定します。当社がサポートする標準 UI は（表 1）を参照してください。

（表 1）当社がサポートする「権限管理（標準 UI）」メニューの一覧

| 大分類 | 中分類 | 標準 UI | 詳細 UI | 説明 |
|---|---|---|---|---|
| 権限管理 | ユーザー | ○ | ○ | 管理ソフトの管理者ユーザーの作成や管理ソフトの操作権限を設定します。 |
| | ロール | × | ○ | 当社または本製品ではサポート対象外です。 |
| | API 認証 | × | ○ | 当社または本製品ではサポート対象外です。 |
| | クライアント登録 | × | ○ | 当社または本製品ではサポート対象外です。 |
| | セキュリティ設定 | ○ | ○ | 管理ソフトを利用するためのログイン方法に関するセキュリティ条件を設定します。 |

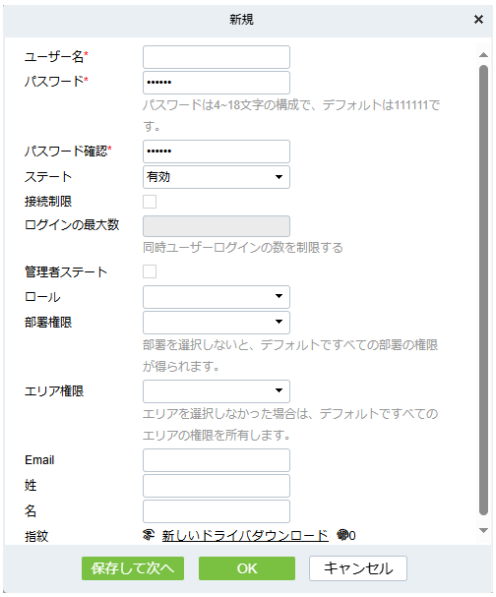
### 9.2.1. ユーザー

本項のユーザーとは、管理ソフトにログインして操作できる管理ユーザーを指します。ユーザーを複数設定する場合は以下の手順で設定します。初期値で「admin」というユーザーが作成されています。これは、管理ソフトのインストール直後に設定したログインパスワードが割り当てられているユーザーです。（admin は削除することができません）

**1．新規**

① 「admin」以外の管理ユーザーを新規に作成します。「新規」をクリックし、各項目を入力・選択します。




| 設定項目 | 内容 |
|---|---|
| ユーザー名* | 半角英数字（30 文字以内）で設定します。 |
| パスワード* | 半角英数字記号（4～18 文字）で設定します。 |
| パスワード確認* | 同上 |
| ステート | 管理ユーザーがログインしてシステムを操作の有効/無効を設定します（一時的に無効にできます）。 |
| 接続制限 | 同時ログイン数の有効/無効を設定します。 |
| ログインの最大数 | 接続制限が有効の場合、同時ログイン数を指定します。（範囲：1～100） |
| 管理者ステート | スーパー管理者のフラグを設定します。チェックをすると全ての権限を持つことができます。 |
| ロール | 管理ユーザーの役割を選択します。**（表 2 参照）** |
| 部署権限 | 特定の部署に対する管理者権限が設定できます。 |
| エリア権限 | 特定のエリアに対する管理者権限が設定できます。 |
| Email | 管理ユーザーのメールアドレスを指定します。 |
| 姓 | 管理者ユーザーの姓を入力します。 |
| 名 | 管理者ユーザーの名を入力します。 |
| 指紋 | 当社または本製品はサポート対象外です。 |

*は必須項目です。

**注意事項**

**＊管理者パスワードは「9.2.5 セキュリティ設定」の「パスワードポリシーを初期化」で「初期値：ログイン時に変更する」に設定されている場合、初回ログイン時に変更する必要があります。**

② ユーザー名、パスワード（パスワード確認）を内容に従って設定します。

| 設定項目 | 内容 |
|---|---|
| ユーザー名* | 半角英数字（30 文字以内）で設定します。 |
| パスワード* | 半角英数字記号（4～18 文字）で設定します。 |

③ ステート

作成した管理ユーザーを使用する場合、「有効（初期値）」を選択します。一時的に無効にする場合、ステートを「無効」にします。



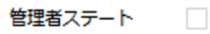

④ 接続制限

同時ログイン数の制限を行う場合は「接続制限」にチェックを入れ、「ログインの最大数」に運用に応じて数を指定します。指定した数で同時にログインできるユーザー数を制限します。



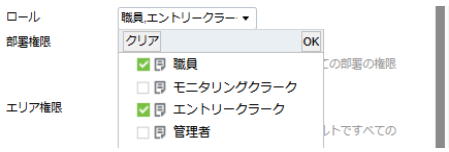

⑤ 管理ステート

作成する管理ユーザーに対して admin と同じ権限を与える場合はチェックを入れます。通常、部署およびエリア毎に管理ユーザーを割り当てて、対象部署や対象エリアの範囲で操作を制限する場合、チェックは不要です。




⑥ ロール

作成する管理ユーザーに対して管理ソフトの「操作権限範囲」を設定します。設定する場合はロールにチェックをいれ「OK」をクリックします。各ロールに応じた操作内容は下記（表 2）ロールの種類を参照してください。

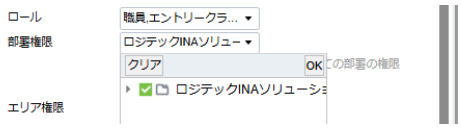



（表 2）ロールの種類

| ロール名 | 内容 |
|---|---|
| 職員 | 「勤怠連携」メニューのトランザクションとデイリーアテンダンスのみ操作権限が付与されます。 |
| モニタリングクラーク | 「入退室管理」メニューのリアルタイムモニタリングとマップのみ操作権限が付与されます。 |
| エントリークラーク | 「ユーザー管理」メニューのみ操作権限が付与されます。 |
| 管理者 | 管理ユーザーの操作権限以外の権限が付与されます。 |

⑦ 部署権限*

作成する管理ユーザーの管理対象となる部署を選択します。会社組織に合わせて部署を設定している場合、管理したい部署毎に設定して運用することができます。




⑧ エリア権限*

作成する管理ユーザーの管理対象となるエリアを選択します。拠点毎にエリアを設定している場合、作成する管理ユーザーを拠点（エリア）毎に作成して運用することができます。

**注意事項**

***アドミニストレータ（admin）権限を持つ管理ユーザーが登録した情報で本項で作成する管理ユーザーの管理対象外の場合、参照・編集等の操作をすることはできません。例えば、管理ユーザー（admin）で部署 A・エリア A に対して新規ユーザー登録した場合、本項で作成した管理ユーザーの管理対象が部署 B やエリア B の場合、新規登録ユーザーは参照・編集等の操作をすることはできません。**

⑨ Email

パスワードリマインダーを利用する場合、作成する管理ユーザーのメールアドレスを登録します。

⑩ 姓・名

管理ソフト上に姓名を表示させる場合、姓と名の欄へ入力をします。

⑪ 指紋

当社または本製品はサポート対象外です。

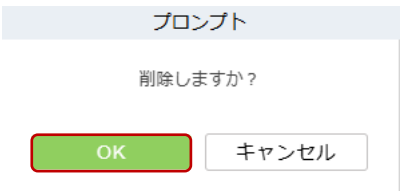
⑫ 更に管理ユーザーを作成する場合は「保存して次へ」を、管理ユーザー作成を終了するには「OK」をクリックします。

## 2．削除

① 削除するユーザーを選択して「削除」をクリックします。




② 「削除しますか？」が表示されたら「OK」をクリックします。



### 3．更新

登録された管理者ユーザーの一覧表示を最新の状態に更新します。更新する場合は「更新」をクリックします。




## 9.2.2. ロール

当社または本製品はサポート対象外です。

## 9.2.3. API 認証

当社または本製品はサポート対象外です。

## 9.2.4. クライアント登録

当社または本製品はサポート対象外です。

## 9.2.5. セキュリティ設定

管理ソフトのログイン方法に関するセキュリティ条件を設定します。最後に各設定を保存するには「OK」をクリックします。

### 1 ログイン認証設定

管理ソフトへのログイン方法を設定します。（初期値：認証コード／入力エラー後にオン）

※2FA 検証（2 ファクタ認証）は、当社または本製品はサポート対象外です。



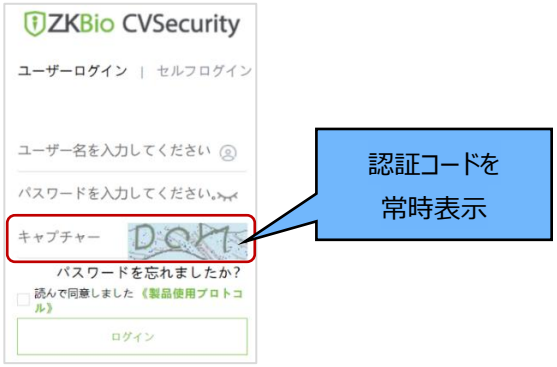

#### 1.1 認証コードを使用したログイン方法

① キャプチャーオフ

検証コードを表示しません。予め設定された管理者のユーザー名とパスワードでログインします。

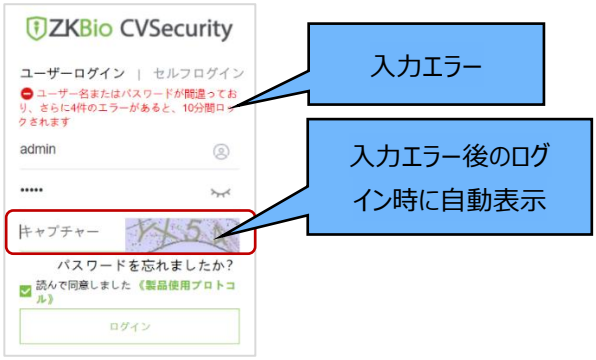
② キャプチャーオン

常時検証コードを表示します。予め設定された管理者のユーザー名とパスワードに加え、自動生成される認証コードの三要素を入力してログインします。



③　入力エラー後にオン

管理者のユーザー名とパスワードでログインに失敗した場合、認証コードを自動表示します。




## 2　パスワード強度（初期値：強い）

管理者のパスワードの強度要件を設定します。下記表にしたがって設定をします。




（表）

| パスワード強度レベル | 設定条件 |
|---|---|
| 無し | パスワードを設定しません（推奨しません。必ずパスワードの設定をお願いします。） |
| 弱い | 8 文字以上で、数字、小文字、大文字、特殊文字から 2 種類以上を使用します。 |
| 中 | 8 文字以上で、数字、小文字、大文字、特殊文字から 2 種類以上を使用します。但し、数字と小文字だけの組み合わせは不可、数字と大文字を含める必要があります。 |
| 強い | 8 文字以上で、数字、小文字、大文字、特殊文字から 3 種類以上を使用します。 |

## 3　ログインパスワード失敗許容回数（初期値：5 回）

管理ソフトのログインで何回まで失敗（入力エラー）を許可するのか上限回数を設定します。上限回数に超えると次項のロック時間に従って一定時間ログインができなくなります。




選択肢：回数無制限/1 回/2 回/3 回/4 回/5 回

## 4　ロック（初期値：10 分）

前項でログインに失敗する上限回数を超えると、設定した時間に応じてログインできなくなります。




選択肢：10 分/20 分/30 分/40 分/50 分/60 分

**5　パスワード有効期間（日）（初期値：90 日）**

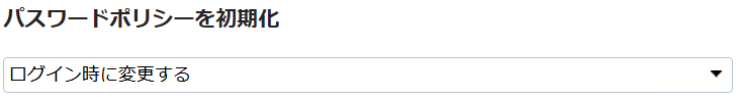
管理者のパスワードの有効期限を設定します。カスタムを選択した場合、1～365 日の数字を入力します。




選択肢：30 日/60 日/90 日/180 日/カスタム/期限切れしない（カスタム：1～365 日を指定します）

**6　パスワードポリシーを初期化（初期値：ログイン時に変更する）**

初回ログイン時にパスワードの再設定が必要になるのかを設定します。




選択肢：変更しない/ログイン時に変更する

**7　安全なパスワード認証間隔（初期値：チェック（オン）/無し）**

管理ソフトからログアウトした後、一定時間再びログインができないように設定します。




ログアウト後の次のログインまでの間隔（分）　選択肢：無し/15 分/30 分/60 分

## 9.3. 通信管理

**【管理ソフト：システム管理 ＞ 通信管理】**

通信ポートやインターネット接続状態を確認できます。当社がサポートする標準 UI は（表 1）を参照してください。最後に各設定を保存するには「OK」をクリックします。

（表 1）当社がサポートする「通信管理（標準 UI）」メニューの一覧

| 大分類 | 中分類 | 標準 UI | 詳細 UI | 説明 |
|---|---|---|---|---|
| 通信管理 | デバイスコマンド | × | ○ | 当社または本製品ではサポート対象外です。 |
| | 通信デバイス | × | ○ | 当社または本製品ではサポート対象外です。 |
| | 製品 | × | ○ | 当社または本製品ではサポート対象外です。 |
| | 許可されたデバイス | × | ○ | 当社または本製品ではサポート対象外です。 |
| | 通信監視 | ○ | ○ | 管理ソフト顔認証デバイス間の通信条件などを確認できます。 |

### 9.3.1. デバイスコマンド

当社または本製品ではサポート対象外です。

### 9.3.2. 通信デバイス

当社または本製品ではサポート対象外です。

### 9.3.3. 製品

当社または本製品ではサポート対象外です。

### 9.3.4. 許可されたデバイス

当社または本製品ではサポート対象外です。

### 9.3.5. 通信監視

管理ソフトと顔認証デバイス間の通信条件や管理ソフトが動作する PC またはサーバー機器がインターネット接続を許可されている環境であるかを確認できます。

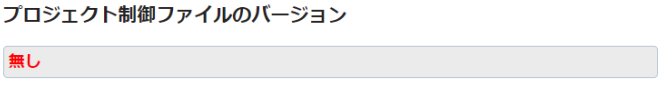
**1. Adms サービス設定 – Adms サービスポート（初期値：8088）**

管理ソフトインストール時に設定した管理ソフトと顔認証デバイスの相互通信ポートを表示します。

※初期値：8088 は管理ソフトインストール時に変更されている場合はこの限りではありません。




**2. Adms サービス設定 – プロジェクト制御ファイルのバージョン**



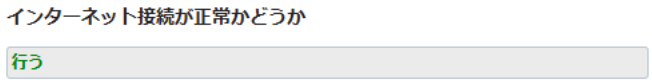
**3. Adms サービス設定 – 暗号化された送信をオンにする（初期値：行う）**

管理ソフトと顔認証デバイスの相互通信を暗号化します。




**4. サーバーネットワークの状況 – インターネット接続が正常かどうか**

管理ソフトが動作する PC またはサーバー機器がインターネット接続の状態を表示します。




行う：　インターネット接続正常

行なわない：インターネット接続異常

※管理ソフト（PC/サーバー）は、ライセンス認証やアップデート以外にインターネット接続は必須ではありません。

## 9.4. サードパーティの統合

当社または本製品ではサポート対象外です。

## 9.5. 外部連携

**【管理ソフト：システム管理 ＞ 外部連携】**

管理ソフトで顔認証デバイスから収集した記録を外部システムに連携するための設定メニューです。

（表 1）当社がサポートする「外部連携（標準 UI）」メニューの一覧

| 大分類 | 中分類 | 標準 UI | 詳細 UI | 説明 |
|---|---|---|---|---|
| 外部連携 | アマノ就業 | ○ | ○ | 本設定は当社または販売店の専門スタッフで対応します。 |
| | アマノ入退 | ○ | ○ | 本設定は当社または販売店の専門スタッフで対応します。 |
| | クロノス | ○ | ○ | 本設定は当社または販売店の専門スタッフで対応します。 |
| | 勤次郎 | ○ | ○ | 本設定は当社または販売店の専門スタッフで対応します。 |
| | OBC | ○ | ○ | 本設定は当社または販売店の専門スタッフで対応します。 |
| | NEC 勤革時 | ○ | ○ | 本設定は当社または販売店の専門スタッフで対応します。 |
| | KING OF TIME | ○ | ○ | 本設定は当社または販売店の専門スタッフで対応します。 |
| | マスターデータ連携 | ○ | ○ | 規定フォーマットのユーザー情報（CSV データ）を管理ソフトへ連携します。 |

勤怠管理システムとの連携やマスターデータ連携には「打刻データ連携ツール」が必要です。打刻データ連携ツールのダウンロードは下記からお願いします。

https://dl.logitec.co.jp/software.php?pn=LST-D-560

## 9.5.1. マスターデータ連携

**【管理ソフト ＞ システム管理 ＞ 外部連携先 ＞ マスターデータ連携】**

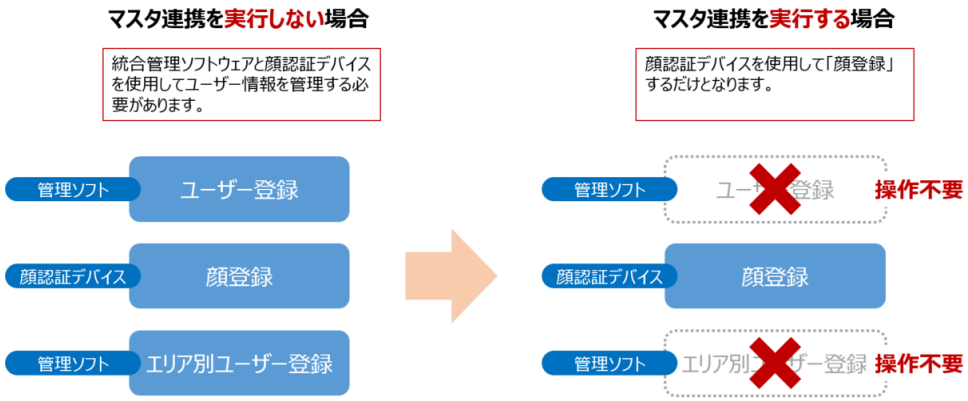
外部システムから出力された CSV データをインポートし、管理ソフトに登録されているユーザー情報を自動で追加・更新・削除する機能です。 この機能では、外部システムから提供されるユーザー情報を基準として扱い、管理ソフト側の情報を調整します。CSV データの内容を正とした統一的な情報管理が可能になります。

**注意事項**

**「マスターデータ連携」機能を使用する場合**

- 製品を導入済みのお客様は必ず「9.5.2 マスターデータ連携の運用へ切り替え方法」を参照してください。
- インポートする CSV データを「正」として取り扱います。管理ソフトからの設定は反映されません。
  ① マスターデータ連携後は、外部システムのマスターをメンテナンスして最新情報を管理ソフトにインポートします。
  ② 原則、管理ソフト上でユーザー情報の操作は行わないように注意してください。
  （例）ユーザーの新規登録、更新・編集、削除など
  ③「エリア別ユーザー登録」機能は、マスターデータ連携でインポートされたユーザーを既存のエリア全てに割り当てを行い管理します。原則、管理ソフト上でエリア別ユーザー登録の操作は行わないように注意してください。
  （例）エリア別ユーザーの新規登録、更新・編集、削除など
- 原則、1 つの CSV データ内に異なるカラム数の情報があるデータはインポートできません。万が一、インポートしてしまった場合、ユーザー情報が削除される場合がありますので注意してください。

下記はマスターデータ連携の実行有無により、省力化される内容を示しています。




### 1. CSV データ仕様

① **キー情報**

CSV インポート時のキーは個人コード（ユーザーID）とします。個人コードが一致する場合、姓名が異なっていても同一人物として扱います。

② **連携可能なマスター件数**

1 回の実行で連携できるマスター件数は上限 3,000 件です。これを超える連携はエラーになりませんが、管理ソフトの動作に予期せぬトラブルが発生する可能性があります。

③ **文字コード**

Shift_JIS（シフト JIS）、UTF-8（BOM なし／BOM あり）、UTF-16（LE/BE）

※Shift__JIS で文字化け（旧字体・異字体）が発生する場合、UTF-8 でご利用ください。

④ **囲み記号**

CSV ファイルの囲み記号として、ダブルクォーテーション（"）に対応します。

⑤ **見出し行**

1 行目に見出しがある CSV 運用を考慮し、インポート開始行を設定できます。

⑥ **EOF**

EOF の有無にかかわらず、CSV をインポートします。

⑥ **1 カラムに姓名がある場合**

姓と名の間に半角または全角スペースがある場合、管理ソフト側の姓と名へ分割して登録します。

※カラム形式はいずれかに統一して CSV を作成する必要があります。同一ファイル内で混在した形式・様式で連携すると、意図しないエラーが発生する可能性があります。

⑧ **カラム形式**

2 カラム形式： ユーザーID／姓名
3 カラム形式： ユーザーID／姓／名
4 カラム形式： ユーザーID／姓名／部署番号／部署名
5 カラム形式： ユーザーID／姓／名／部署番号／部署名

※形式以外の CSV は連携できません。

⑧ **項目仕様**

**【 2 または 4 カラム 】**

| CSV 項目 | 2 カラム | 4 カラム | 必須 | 内容 |
|---|---|---|---|---|
| ユーザーID | 項目 1 | 項目 1 | 必須 | 半角英数。外部システムで管理されている一意の番号 |
| 姓名 | 項目 2 | 項目 2 | 必須 | ユーザーの姓名（1 カラム内） |
| 部署番号 | — | 項目 3 | 任意 | 半角数字。指定無しは「部署番号:1」へ割り当てます |
| 部署名 | — | 項目 4 | 任意 | 部署の名称 |

**【 3 または 5 カラム 】**

| CSV 項目 | 3 カラム | 5 カラム | 必須 | 内容 |
|---|---|---|---|---|
| ユーザーID | 項目 1 | 項目 1 | 必須 | 半角英数。外部システムで管理されている一意の番号 |
| 姓 | 項目 2 | 項目 2 | 必須 | ユーザーの姓 |
| 名 | 項目 3 | 項目 3 | 必須 | ユーザーの名 |
| 部署番号 | — | 項目 4 | 任意 | 半角数字。指定無しは「部署番号:1」へ割り当てます |
| 部署名 | — | 項目 5 | 任意 | 部署の名称 |

※指定項目以外の電話番号や Email などの情報はデータ処理の対象外です
※CSV データの内容は、2、3、4、5 のカラム数はいずれかに統一して連携・運用する必要があります

## 2. 動作仕様（インポート時の処理）

管理ソフトは、ユーザー自動削除の有効・無効の設定に応じ、ユーザーID を基準に処理をします。本機能を使用する場合、管理ソフト上で操作・設定をしてもマスター連携により情報は CSV データで上書きされます。本機能を使用するか、管理ソフト上でユーザー登録をするか、運用方法を事前に決める必要があります。

## 3. 管理ソフトの設定（事前準備）

### ① 「マスターデータファイルパス」の設定

「マスターデータファイルパス」へ登録する CSV データの保存先を指定します。

※ユーザーID は、管理ソフトで設定している桁数とインポートする CSV の桁数が合致していることを確認してください。
管理ソフトの設定情報の確認は「9.6.8 パラメータ」を参照してください。

※管理ソフトがインストールされている PC/サーバーのローカルフォルダであることが必要です。




入力例 C:\Example

※管理ソフトは「¥（円マーク）」が、「バックスラッシュ」で表示されます

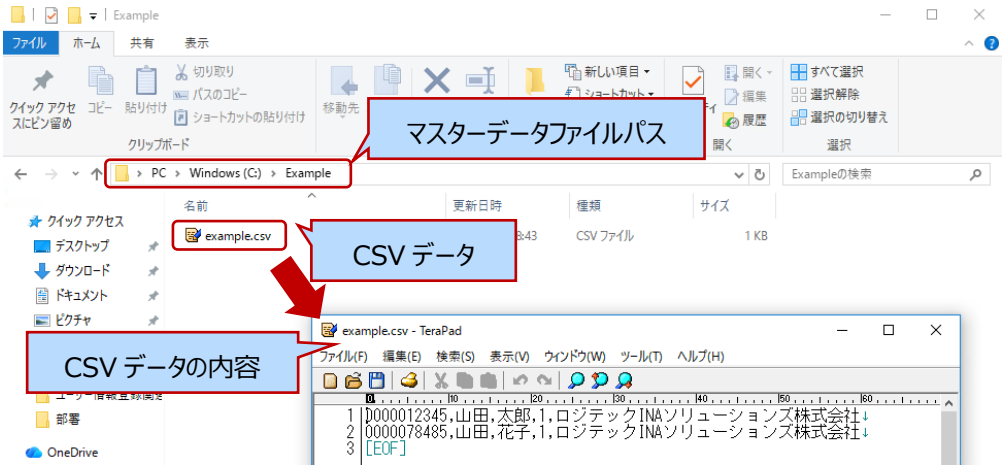
### ② 「マスターデータファイル名」の設定

「マスターデータファイル名」へ登録する CSV データのファイル名を指定します。




入力例 example.csv

**<参考>**




### ③ 「CSV データの読み取り開始行」の設定（初期値：1）

インポートする CSV のデータ開始行をしています。




例：2（CSV データの 2 行目からインポートします）

④ **「入退・勤怠共通」の設定（初期値：ユーザー自動削除無効）**

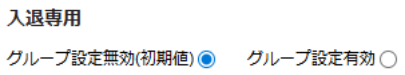
CSV をインポートした時のユーザーデータの自動削除について動作を指定します。




※詳細はマスターデータ連携の動作仕様（インポート処理時）を参照してください

⑤ **「入退専用」の設定（初期値：グループ設定無効）**

CSV インポートした時のデフォルトのアクセス権限の付与について指定します。




※詳細はマスターデータ連携の動作仕様（インポート処理時）を参照してください

## 4. マスターデータ連携の動作仕様（インポート処理時）

管理ソフトは、ユーザー自動削除の有効・無効の設定に応じ、ユーザーID を基準に処理をします。本機能を使用する場合、管理ソフト上で操作・設定をしてもマスター連携により情報は CSV データで上書きされます。本機能を使用するか、管理ソフト上でユーザー登録をするか、運用方法を事前に決める必要があります。

① **入退・勤怠共通 － ユーザー自動削除無効（初期値：無効）**

CSV に存在しないユーザーを削除しません。ユーザーID を基準に追加・更新のみを行います。

| CSV の状態 | 管理ソフトの処理 |
|---|---|
| ユーザーID が CSV に存在せず、管理ソフトに存在する | 処理をしません |
| CSV の姓名が変更されている（更新） | ユーザーID を基に姓名を更新します |
| CSV の部署情報が変更されている（更新） | ユーザーID を基に部署情報を更新します |
| ユーザーID が CSV に存在し、管理ソフトに存在しない | 新規登録され、全エリアへ割り当てます |

※部署に所属するユーザーがゼロになっても、部署情報自体は削除されません。
※管理ソフトでエリアを変更した場合でもマスターデータ連携時に全エリアへ割り当てされます。
※デバイス操作権限は、管理ソフトで設定されている情報が保持されます。

② **入退・勤怠共通 － ユーザー自動削除有効**

CSV に存在しないユーザーID の自動削除をします。削除されたユーザーのユーザーID、姓、名、部署番号などの CSV 連携対象項目は CSV に登録することで再登録できますが、顔写真やその他項目（デバイス操作権限など）は管理ソフト、または端末にて再度設定を行ってください。ユーザーが削除された場合、管理ソフトには勤怠履歴等の認証記録は残りますが、管理ソフトに登録されていない顔認証デバイスにある記録は管理ソフトに同期できません。

| CSV の状態 | 管理ソフトの処理 |
|---|---|
| ユーザーID が CSV に存在せず、管理ソフトに存在する | CSV に存在しないユーザーを削除します |
| CSV の姓名が変更されている（更新） | ユーザーID を基に姓名を更新します |
| CSV の部署情報が変更されている（更新） | ユーザーID を基に部署情報を更新します |
| ユーザーID が CSV に存在し、管理ソフトに存在しない | 新規登録され、全エリアへ割り当てます |

③ **入退専用 – グループ設定無効（初期値：無効）**

CSV のインポートによる処理はしません。

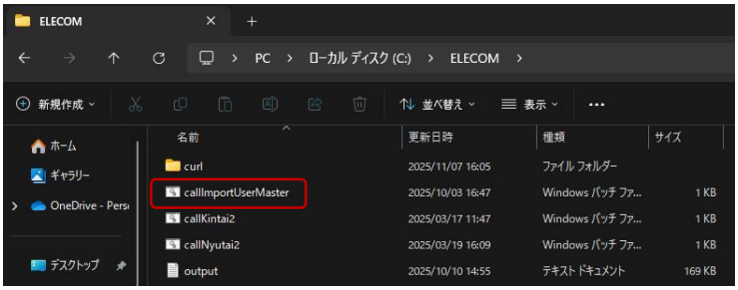
④ **入退専用 – グループ設定有効**

CSV のインポートにより、ユーザーID を基準に初期値のグループ名（マスター）へユーザーを割り当てます。

## 5. マスターデータ連携の実行

打刻データ連携ツール「ELECOM」フォルダに同梱されている「callImportUserMaster.bat」をダブルクリックします。

※実行頻度はサーバーの負荷を考慮して、多くても 1 日 1 回、利用頻度が少ない時間帯でお願いします




## 6. ログ情報と確認方法

取り込み処理の内容や結果は、以下のフォルダに自動で記録されます。ログを確認することで、取り込みが 正常に行われたか、問題が発生していないかを把握できます。

**C:¥Program Files¥ZKBioCVSecurity¥service¥zkbiosecurity¥MasterIntegrationLog**

※該当フォルダへのショートカットを作成しておくと便利です

※管理ソフトのインストール先によりドライブレター（C:）が異なる場合があります

## 7. ログに記録される内容

ログには、処理中に発生した事象が順序を追って記録されます。主な内容は次の通りです。

① **CSV 内のカラム数不一致によるエラー**

重大: Error reading person file: java.lang.ArrayIndexOutOfBoundsException: X

※X＝エラーとなったカラム数

CSV ファイル内に異なるカラム数が混在している場合に記録されます。カラム数が多いデータ形式がインポートされ、カラム数が少ないデータはインポートされません。「ユーザー自動削除"有効"」の場合、インポートされなかったユーザーID と同じユーザーが管理ソフトに存在する場合は削除されます。

情報: Start read person file ～
情報: params.length is: 5 ～
情報: params.length is: 3 ～
重大: Error reading person file: java.lang.ArrayIndexOutOfBoundsException: 3 ～
情報: Finish read person file ～
情報: del pins:9000000004,9000000003

② **パスまたはファイルが見つからない場合のエラー**

情報: The file does not exist in the specified path,file name is: example.csv

管理ソフトで設定されているパスまたはファイル名が存在しない場合に記録されます。設定されている情報「C:¥Example（＝パス）¥example.csv（＝ファイル名）」のいずれかを確認してください。

**関連ログとエラー内容：**

- File path cannot be empty!：ファイルのパスが空になっています
- current file encoding is:xxx：ファイルのエンコーディングを解析しました XXX
  ～
  Failed to detect encoding：文字エンコード検出エラー

③ **新規登録** 【情報: Added persons:】

取り込みによって新しく追加されたユーザーの情報が記録されます。例：ユーザーID、氏名など、追加されたユーザー数を把握できます。

**ユーザー追加された場合の例：**

PIN:9000000001,Name:佐藤　太郎 30

PIN:9000000002,Name:鈴木　美咲 30

④ **更新** 【情報: Modified persons:】

**名や部署（部署番号）の更新された場合の例：**

Before: PIN:9000000001,Name:佐藤　花子,DeptCode:13

--->Now: PIN:9000000001,Name:村岡　花子,DeptCode:30

⑤ **削除（管理ソフトの設定がユーザー自動削除"有効"の場合）** 【情報:del pins:】

CSV ファイルにユーザーID が存在せず、管理ソフトだけ存在するユーザーID があった場合、管理ソフトのユーザー情報を削除し、削除されたユーザーID が 記録されます。

**ユーザーが削除された場合の例：**

情報: del pins:9000000002,9000000001,9000000004,9000000003,9000000006

⑥ **Error personPin is empty**

user ID（PIN）を解析できない、または user ID（PIN）が空です

⑦ **Error processing : person with PIN:xxx, error:xxx**

user ID（PIN）が xxx のデータの処理に失敗しました。エラー内容は xxxx です。

⑧ **部署データに関するログ：**

Start department：部署データの処理を開始

deptCode:xxx deptName:xxx：部署データの分析結果

Finish department：部門データの処理が完了

error: +例外情報：エラーメッセージが表示された場合に記録されます

## 8. 勤怠連携における注意事項（多拠点運用時）

多拠点で運用する場合、マスターデータ連携によりユーザー情報がすべてのエリア（拠点）へ自動的に反映されます。そのため、以下の点を十分にご理解いただいたうえで運用いただくことが必要です。

### ① 運用開始のタイミングについて

マスターデータ連携は、管理ソフトおよびすべての顔認証デバイスの導入作業が完了し、運用が開始された 後に使用することを前提としています。導入途中で連携を行うと、設定途中の情報が全てのエリア（拠点）へ反映され、意図しない動作が発生する可能性があります。

### ② デバイス操作権限を付与する場合の注意（詳細は「P144」を参照してください）

「デバイス操作権限」を持つユーザーを設定すると、マスターデータ連携する毎に権限を持つユーザー情報が全てのエリア（拠点）に反映されます。その結果、新しく導入するエリア（拠点）でデバイスを操作するために「権限を持つユーザーの認証が必要」となり、顔登録などデバイス操作ができない状況が発生します。

このような状況を避けるため、運用開始後に設定するか、デバイス操作権限を付与するユーザーには、事前に「初期パスワード」を設定しておくことを推奨します。追加した拠点では、その初期パスワードを利用してログインし、顔登録を問題なく続けることができます。すべての拠点への導入が完了した後は、セキュリティを確保するために初期パスワードを変更または削除してください。

## 9. マスターデータ連携の処理フロー

管理ソフトへファイルパス・ファイル名の各種設定
↓
外部システム → CSV データ出力
↓
連携ツール「callImportUserMaster.bat」を実行
↓
CSV の内容に基づいてユーザー情報を更新
（新規／更新／削除）
↓
ログに結果が記録

**注意事項**

**ユーザーマスタ連携に使用する CSV データに特殊文字は利用できません。万が一、特殊文字を含む CSV が連携された場合、管理ソフトの動作に影響が出る場合があります。**
**【特殊文字の例】**
**<、>、`、~、!、@、#、$、%、^、*、?、/、|、¥、:、;、=、"、'、,、--、+、，、。、、、；、‘、’、【、】、！、¥、…、&、（、）、?**
**CSV に特殊文字が含まれている場合、下記のログが「zkbiocvsecurity.log」に記録されます。**
**～ Rcw null:Lastname and Firstname can not contain special symbols! The personnel id is:7015（ユーザ ID：7015 の姓名に特殊文字を含むことができません）**

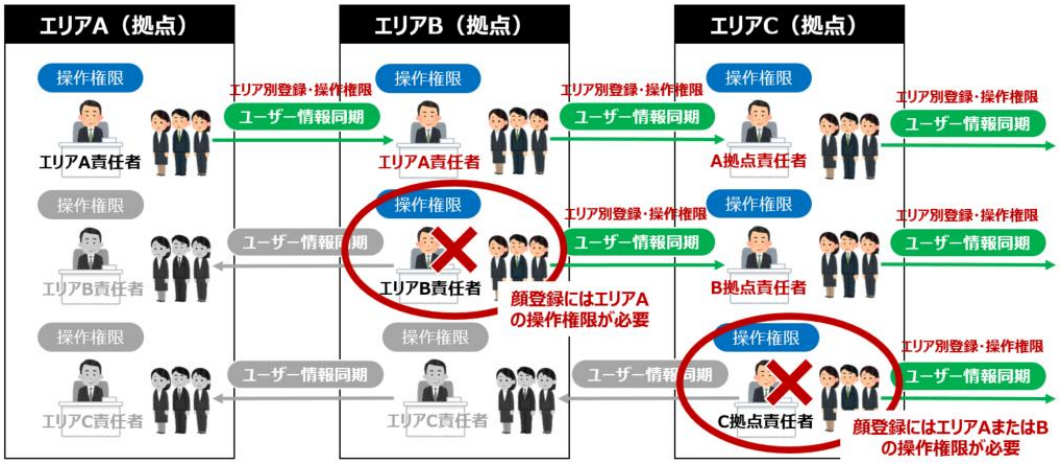
注意事項

**複数拠点で、管理者（デバイス操作権限を持つ人）が複数いる場合**

マスターデータ連携は、統合管理ソフトウェアと顔認証デバイスの導入がすべて完了し、運用を開始した後に使うことを前提としています。そのため、複数拠点で導入作業を進めながら同時に運用も始める（導入と運用を並行する）場合は、設定の順番によって不具合が起きることがあるため注意してください。

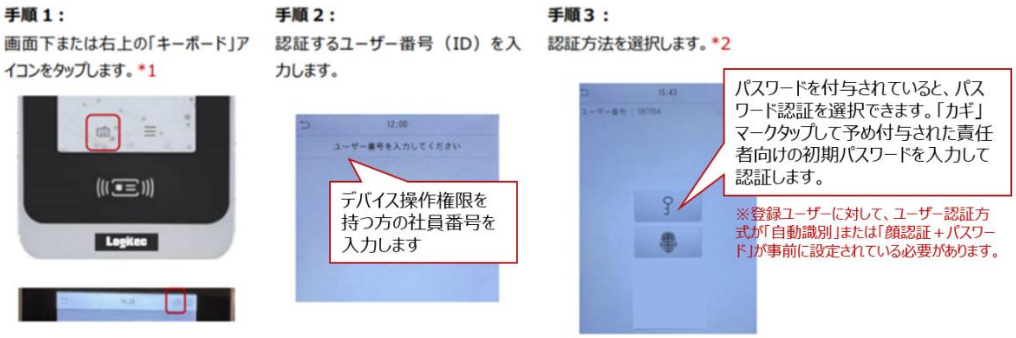
**注意が必要な運用：顔認証デバイス側で「デバイス操作権限」を付与する場合**

通常は、導入完了後に「ユーザー登録」を行い、運用開始前にデバイス操作権限を設定して、誰でも設定変更できないように保護します。しかし、導入途中の段階で、先に設置した顔認証デバイスでデバイス操作権限を付与すると、あとでマスターデータ連携を行った際に、ユーザーが拠点（エリア）ごとに自動登録される処理が動きます。この結果、先に導入した拠点の「権限を持つユーザー情報」が、他の拠点のデバイスにも登録されてしまいます。その状態になると、次に導入する拠点では、先に導入した拠点責任者（権限を持つ人）の認証ができないと操作できないため、新しい顔認証デバイスで顔登録ができなくなります。




**"顔登録ができなくなる"状態の回避方法**

ユーザー管理で責任者の方に"デバイス操作権限"を付与する際、合わせて責任者向けの"初期パスワード"を設定します。これにより、追加導入したエリア（拠点）でも"初期パスワード"を使用して顔登録が進められます。パスワードを登録した際、デバイス操作方法は以下の通りです。




*1 カメラが起動している状態では、画面右上に「キーボード」アイコンが表示されます。
*2 ユーザー毎に登録されている認証情報に基づいて各認証アイコンが表示されます。登録されていない認証方法は、アイコンとして表示されません。

※セキュリティを考慮しまして、全てのデバイスの導入が終わりましたら、パスワードは、管理ソフトまたは顔認証デバイスで"削除"または"変更"することをお勧めします。

※導入完了後にユーザー登録およびデバイス操作権限の設定を行う場合、本「回避方法」は必要ありません。

### 9.5.2. マスターデータ連携の運用へ切り替え方法

既に顔認証デバイスを導入済みのお客様で、ユーザー情報（マスター）についての管理方法を”管理ソフト主体の運用”から”マスターデータ連携”へ変更する場合の手順を説明します。

**１．データベースのバックアップ（手動実行）**

本書の「9.1.2 データ管理」にある「すぐにバックアップ（手動実行）」を参照して、バックアップを作成してください。意図しないユーザー情報の連携結果が発生した場合、バックアップから復元できるように準備します。

**２．マスターデータ連携の設定**

本書の「9.5.1 マスターデータ連携」の「管理ソフトの設定（事前準備）」を参照して、マスターデータの保存場所とデータ名などの各種設定をします。

**３．マスターデータ連携の実行**

本書の「9.5.1 マスターデータ連携」を参照して、打刻データ連携ツール「ELECOM」フォルダに同梱されている「callImportUserMaster.bat」をダブルクリックします。

※実行頻度はサーバーの負荷を考慮して、多くても 1 日 1 回、利用頻度が少ない時間帯でお願いします

## 9.6. ユーザー管理




「ユーザー管理」メニューは、入退室管理および勤怠管理において顔認証デバイスを利用するユーザー情報に関する設定をします。当社がサポートする標準 UI は（表 1）を参照してください。
※ユーザー登録またはデバイス交換を実施した場合、入退室管理であれば「全データをデバイスに同期」、勤怠連携であれば「ソフトウェアデータをデバイスに同期」を実行します。端末上のユーザー情報を最新に更新します。

**注意事項**

**ユーザー登録方法は、重複及び既存情報の上書きを避けるため、次のいずれかの方法で統一してください。**
**管理ソフトで個別登録：個別登録及び一括登録で登録されたユーザー情報内で重複をチェックしません**
**管理ソフトで一括登録：個別登録及び一括登録で登録されたユーザー情報内で重複をチェックしません**
**セルフサービス登録　：セルフサービス登録で登録されたユーザー情報内で重複をチェックしません**
**端末で登録　　：管理ソフトからデバイスに同期されたユーザー情報内で重複をチェックします**

**注意事項**

**ユーザー登録する情報で、ユーザー番号、顔情報、掌情報、カード No（IC カード）、Email は重複して登録することができません。**
**最大ユーザー登録数は 30,000 人です。なお、顔認証デバイス（LTC-FPT50/IPV2）側の認証方式の登録数の上限（顔：10,000／掌：5,000／IC カード：50,000）とは異なりますので注意が必要です。**

（表 1）当社がサポートする「ユーザー管理（標準 UI）」メニューの一覧

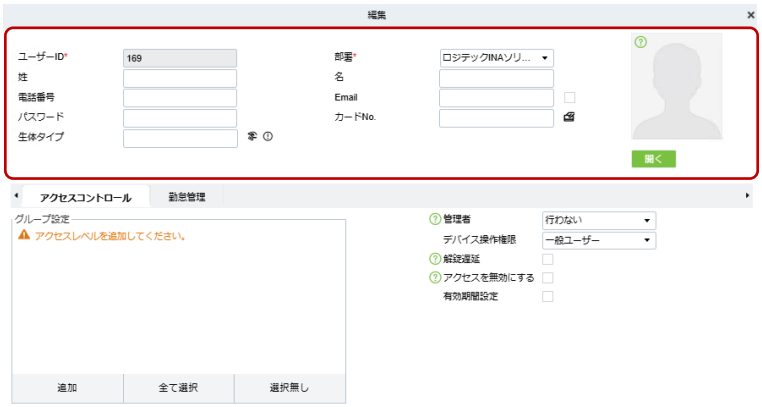
| 大分類 | 中分類 | 標準 UI | 詳細 UI | 説明 |
|---|---|---|---|---|
| ユーザー管理 | ユーザー | ○ | ○ | 入退室管理、勤怠管理におけるユーザー情報を管理します。 |
| | 部署 | ○ | ○ | ユーザーが所属する部署を設定します。 |
| | ポジション | × | ○ | 当社または本製品ではサポート対象外です。 |
| | 離職ユーザー | × | ○ | 当社または本製品ではサポート対象外です。 |
| | セルフサービス登録ユーザー | ○ | ○ | セルフサービス登録による登録申請者を管理します。 |
| | カスタム属性 | × | ○ | 当社または本製品ではサポート対象外です。 |
| | リストライブラリ | × | ○ | 当社または本製品ではサポート対象外です。 |
| | パラメータ | ○ | ○ | ユーザー管理における各種パラメータの設定をします。 |
| カード管理 | カード | ○ | ○ | 「ユーザー」で登録された IC カードを一元管理します。 |
| | Wiegand フォーマット | ○ | ○ | 当社または本製品ではサポート対象外です。 |
| | カード登録履歴 | ○ | ○ | 「ユーザー」で登録された IC カードの履歴を管理します。 |

### 9.6.1. ユーザー

#### 1. ユーザー登録（個別登録）

1 件ずつ個別登録します。登録するには「ユーザー登録」をクリックします。






| 設定項目 | 内容 |
|---|---|
| ユーザーID* 重複不可 | 9 桁（初期値）から最大 14 桁の半角英数字、先頭に 0 をつけることはできません。先頭に 0 を付ける場合は、英数字の利用設定をします（9.6.8 パラメータ）。また、顔認証デバイスは初期値で英数字の利用が ON になっています。<br>※先頭 8 または 9 から始まる ID は別メニューの予約番号です。入退/勤怠メニューでは影響なく使用できます。 |
| 部署* | ユーザーが所属する部署を選択します。 |
| 姓・名 | 姓名を入力します。 |
| 電話番号 | 半角数字で、電話番号を入力します。 |
| Email 重複不可 | 半角英数字で、Email を入力します。管理者の指定をする場合、各種イベント通知をすることができます。 |
| パスワード | 8 桁の半角数字で、パスワードを使用した認証を行う場合、パスワードを入力します。 |
| カード No 重複不可 | IC カード番号を入力します。入力間違えがないように登録機のカードリーダーで登録することをお勧めします。<br>※IC カードの登録方法は「7.6 顔認証または他の認証を利用する場合」を参照してください。 |
| 生体タイプ | 登録されている生体情報を表示します。生体情報の登録は、写真または顔認証デバイスの登録機から行います。<br>※「 （登録）」からの生体タイプの登録について、当社または本製品はサポート対象外です。 |
| 開く（顔登録） | 顔認証で利用する顔写真を選択して登録します。認証時のプロフィール写真としても利用することができます。 |

*は必須項目です。

### ① ユーザー情報に関連する入退室管理メニューおよび勤怠連携メニューの設定

ユーザー情報に紐づくアクセス権限やデバイス操作権限などの細かい設定をします。基本は初期値で設定し、特別な権限を付与するユーザーにのみ設定をします。

| 設定項目 | | 内容 |
|---|---|---|
| アクセスコントロール（入退室管理） | グループ設定 | ユーザーに与えるアクセス権のグループを選択します。 |
| | 管理者 | 当社または本製品はサポート対象外です。 |
| | デバイス操作権限 | デバイス側の操作権限を選択します。<br>一般ユーザー：デバイスのメインメニューを表示することはできません。<br>管理者：デバイスの全てのメインメニューが利用できます。<br>登録者：デバイスのユーザー管理／勤怠履歴／システム情報が利用できます。 |
| | 解錠遅延 | 電子錠と連携する場合、認証から解錠までの時間を遅延する設定です。 |
| | アクセスを無効にする | 当社または本製品はサポート対象外です。 |
| | 有効期間設定 | アクセスの有効期間を設定します。 |
| 勤怠管理（勤怠連携） | アクセスエリア | アクセスエリアを指定します。 |
| | 勤怠モード | 通常の勤怠（初期値）のまま使用します。 |
| | デバイス操作権限 | デバイス操作の操作権限を選択します。<br>ユーザー：デバイス側のメインメニューを表示することはできません。<br>登録者：ユーザー管理/通信設定/システム設定/アクセスコントロールが利用できます。<br>管理者：当社または本製品はサポート対象外です。<br>スーパー管理者：デバイス側のメインメニューが利用できます。 |
| | 認証モード | 認証方式を選択します。（初期値：自動識別） |

② **アクセスコントロール**

入退室管理を行う場合に設定します。入退室管理をしない場合は、初期値の設定で使用してください。誤った設定を行うと管理ソフトや顔認証デバイスが動作しなくなります。




(ア) グループ設定

ユーザーに与えるアクセス権のグループを設定します。管理ソフト導入直後は、初期値：マスター（24 時間有効）*を選択します。また、「入退室管理メニュー：アクセスルール ＞ タイムゾーン（アクセス可能な時間）」の設定で任意のタイムゾーンを作成することができます。ここではユーザー個人にグループを割り当てる手順を説明します。

*マスターとは、エリアとタイムゾーンをグループ化したグループ名です。初期値では、「エリア：エリア名」と「タイムゾーン：24 時間」をグループ化したグループ名が「マスター」として作成されています。

① 「追加」をクリックします。




② 予め設定された「タイムゾーン（アクセス可能時間）」を選択（チェックボックス ON）します。
例は、平日の日勤ユーザー専用のタイムゾーンです。



③ 「＞」をクリックし、「タイムゾーン（アクセス可能時間）」を移動します。
（参考）「＞＞」は全てのタイムゾーンを移動します。




④ タイムゾーン（アクセス可能時間）の追加が完了しましたら、最後に「OK」をクリックします。適切なレベル（アクセス）設定がされているか確認してください。




(イ) 管理者

当社または本製品はサポート対象外です。「初期値：行わない」で使用してください。

(ウ) デバイス操作権限

顔認証デバイス側のメインメニュー操作権限を設定します。適切な権限設定を行うことで、遠隔地にある顔認証デバイスが設置された現場側でユーザー登録や設定変更ができます。メインメニュー表示にはユーザー認証が必要です。

| ユーザー権限 | 権限内容 |
|---|---|
| 一般ユーザー | デバイス側のメインメニューを表示することはできません。 |
| 管理者 | 全てのメインメニューを表示し設定することができます。<br>表示メニュー：全て |
| 登録者 | デバイス側のメインメニュー表示を「ユーザー登録」以外の詳細設定を制限します。<br>表示メニュー：ユーザー管理/通信設定/システム設定/アクセスコントロール |

(エ) 解錠遅延

電子錠と連携する場合、認証してからの解錠時間を遅延する設定です。

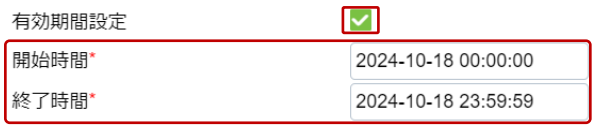
(オ) アクセスを無効にする

一時的にアクセスを無効にしたい場合「チェックボックス」を「ON」にします。

(カ) 有効期間設定

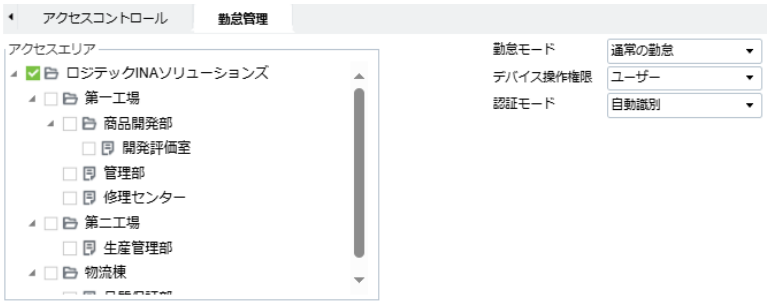
アクセス可能な期間を日時で設定する場合「チェックボックス」を「ON」にし、指定する期間を入力します。

※本製品は「年月日」までの指定となります。時間は無効となります。




### ③ 勤怠管理

勤怠管理を行う場合に設定します。勤怠管理をしない場合は、初期値の設定で使用してください。誤った設定を行うと管理ソフトや顔認証デバイスが動作しなくなります。




(ア) アクセスエリア

ユーザーがアクセス可能なエリアを設定します。設定する場合は「チェックボックス」を「ON」にします。

(イ) 勤怠モード

「初期値：通常の勤怠」で使用します。

(ウ) デバイス操作権限

顔認証デバイス側のメインメニュー操作権限を設定します。適切な権限設定を行うことで、遠隔地にある顔認証デバイスが設置された現場側でユーザー登録や設定変更ができます。メインメニュー表示にはユーザー認証が必要です。

| ユーザー権限 | 権限内容 |
|---|---|
| ユーザー | デバイス側のメインメニューを表示することはできません。 |
| 登録者 | デバイス側のメインメニュー表示を「ユーザー登録」以外の詳細設定を制限します。<br>表示メニュー：ユーザー管理/通信設定/システム設定/アクセスコントロール |
| 管理者 | 当社または本製品はサポート対象外です。 |
| スーパー管理者 | 全てのメインメニューを表示し設定することができます。<br>表示メニュー：全て |

(エ) 認証モード ※下記は当社または本製品はサポートする認証モードです。
認証モードを選択します。認証モードの組み合わせは下表を参照してください。

| 認証モード | 内容 |
|---|---|
| 自動識別 | 認証方式を自動判別して認証します。 |
| ユーザーID | ユーザー番号とパスワードで認証します。 |
| パスワードのみ | ユーザー番号とパスワードで認証します。 |
| カードのみ | IC カードで認証します。 |
| カード/パスワード | IC カードまたはパスワーで認証します。 |
| 顔 | 顔で認証します。 |
| 顔＋パスワード | 顔とパスワードの二要素で認証します。 |
| 顔＋カード | 顔と IC カードの二要素で認証します。 |
| 掌 | 掌で認証します。 |
| 掌＋カード | 掌と IC カードの二要素で認証します。 |
| 掌と顔 | 掌と顔のマルチモーダルで認証します。 |

入力および設定が完了しましたら、最後に「OK」をクリックします。連続してユーザー登録を行う場合は「保存して次へ」をクリックします。



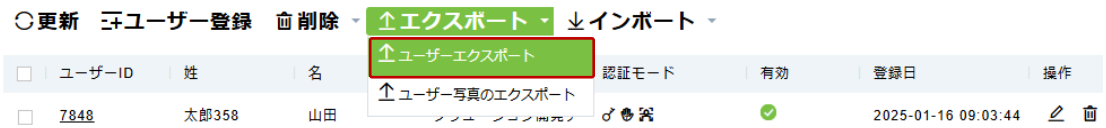

**注意事項** **デバイスのモデルにより認証方式が様々で、管理ソフト側はこれらの認証方式をマージする形で設計されているため表記が異なります。**

## 2. エクスポート*

ユーザーに紐づく各種情報をエクスポートします。エクスポートには管理ソフトの管理者パスワードが必要です。

### ① ユーザーエクスポート

ユーザー情報を EXCEL・PDF・CSV のいずれかの形式でエクスポートすることができます。各条件を指定して最後に「OK」をクリックします。なお、暗号化した場合、Windows 標準の解凍ツールは使用できません。






| 設定項目 | 内容 |
|---|---|
| 基本情報 | 出力したい項目を選択します。 |
| ユーザーパスワード* | 管理者ユーザーのパスワードを入力します。 |
| ファイル暗号化 | データの暗号化を指定します。 |
| ファイル暗号化パスワード* | ファイル暗号化を指定した場合、復号化するパスワードを指定します。 |
| ファイル形式 | EXCEL・PDF・CSV から選択します。 |
| エクスポートするデータ | すべて：最大 10 万件を上限にデータをダウンロードします。 |
| | 選択済み：開始レコードと上限（終了レコード）を指定してダウンロードします。 |

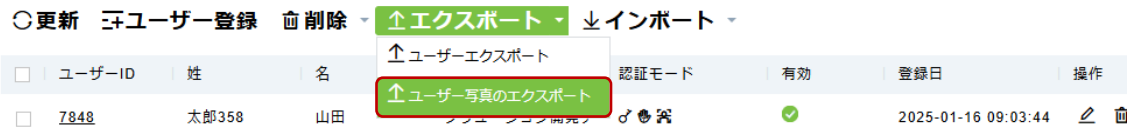
*印は必須項目です。

### ② 生体テンプレートエクスポート

当社または本製品ではサポート対象外です。

### ③ ユーザー写真のエクスポート

ユーザー写真を ZIP 圧縮形式でエクスポートすることができます。各条件を指定して最後に「OK」をクリックします。なお、暗号化した場合、Windows 標準の解凍ツールは使用できません。







| 設定項目 | 内容 |
|---|---|
| ユーザーパスワード* | 管理者ユーザーのパスワードを入力します。 |
| ファイル暗号化 | データの暗号化を指定します。 |
| ファイル暗号化パスワード* | ファイル暗号化を指定した場合、復号化するパスワードを指定します。 |
| ファイル形式 | ZIP 圧縮ファイルのみ選択できます。 |

*印は必須項目です。

ユーザーエクスポートの説明は、以上で終わりです。

**注意事項**

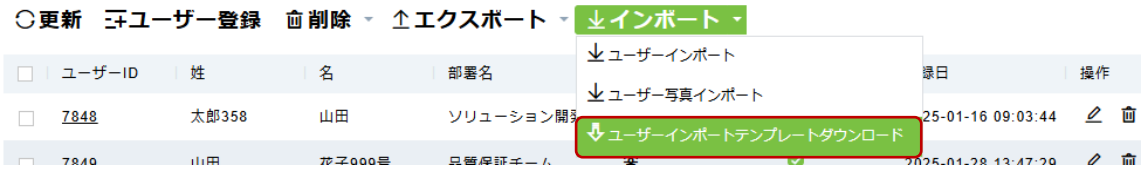
**＊ユーザー情報には個人情報が含まれます。管理ソフト及び顔認証デバイスをご使用いただくお客様の責任のもと、セキュリティ対策および個人情報のお取り扱いをお願いします。本管理ソフトおよび顔認証デバイスを使用することで、お客様及び第三者に生じた損害について、当社は一切の責任を負いかねます。**

## 3. インポート（一括登録）

ユーザー情報と、写真データの一括登録を説明します。ユーザー情報と写真データはそれぞれ登録する必要があります。

### ① ユーザーインポートテンプレートダウンロード

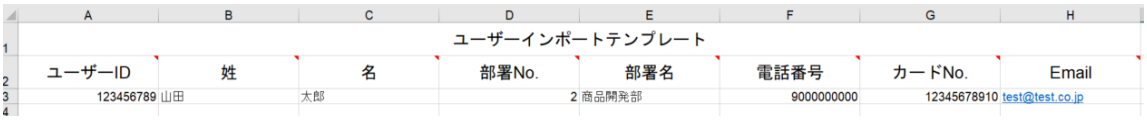
「ユーザーインポートテンプレートダウンロード」をクリックします。




テンプレートの入力項目を選択し「OK」をクリックします。




テンプレートに情報を入力します。



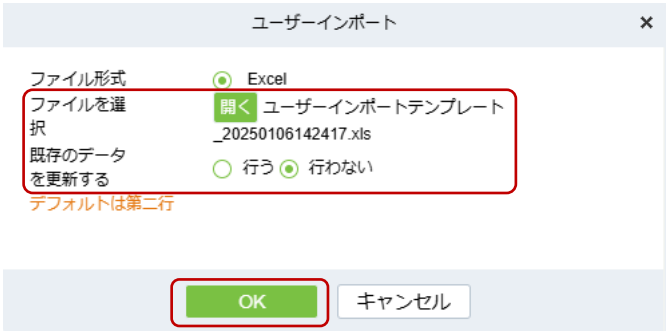

※ユーザーID、姓、名、部署 No、所属部署は必須です。ユーザーID、カード No、Email は重複して登録することはできません。ユーザーID は、先頭 8 または 9 から始まる ID は別システムメニューの予約番号です。入退または勤怠メニューでは影響なく使用することができます。

### ② ユーザーインポート

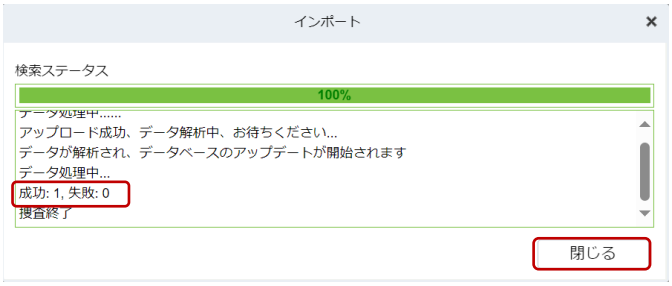
「ユーザーインポートテンプレート」を使ってユーザー情報をインポートします。「ユーザーインポート」をクリックします。




「開く」をクリックしてインポートするユーザーインポートテンプレートを選択します。既存のデータを上書き更新する場合は「行う」、上書き更新しない場合は「行わない（初期値）」を選択し、最後に「OK」をクリックします。




インポートの結果が表示されます。問題がなければ「閉じる」をクリックします。

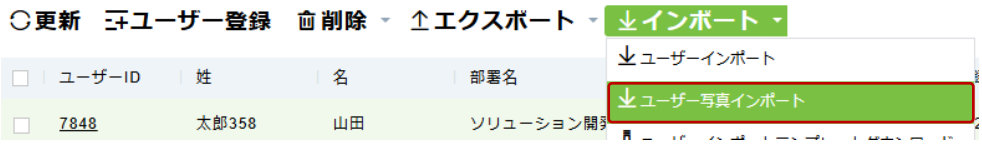



### ③ ユーザー写真インポート

「ユーザー写真のインポート」をクリックします。

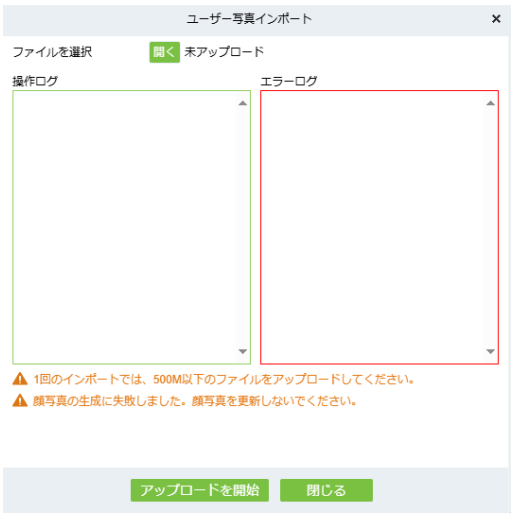
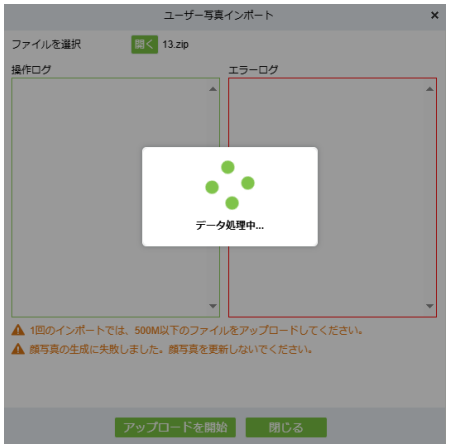
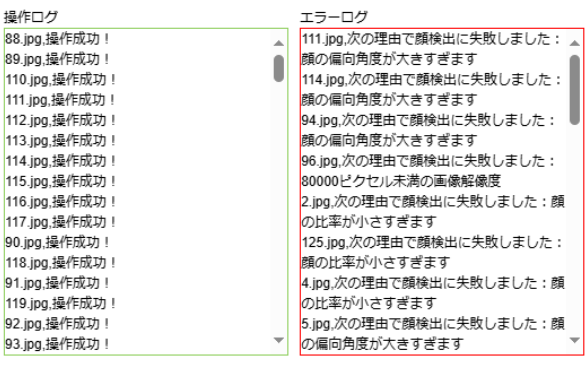
**注意事項**

**＊写真データ名は、ユーザーID を指定します（特殊文字は使用不可）。**
**＊データ形式は JPG または PNG で、フル HD（1920×1080）以上、データ容量 5MB 未満を推奨します。**
**＊一度に選択できる写真データは、499 枚です。500 枚以上の写真データを選択しないようにしてください。**




「写真」または「圧縮パッケージ」を選択し「OK」をクリックします。



| **インポート方法：写真**<br>写真を直接インポートします | **インポート方法：圧縮パッケージ**<br>写真を ZIP ファイルに圧縮したデータをインポートします |
|---|---|
| 「写真を選択してください」をクリックして写真を選択します。キーボードの「shift」キーを押しながら複数の写真を選択することができます。 | 「開く」をクリックして ZIP ファイルを選択します。 |
|  |  |
| 「アップロードを開始」をクリックします。 | 「アップロードを開始」をクリックします。 |
|  |  |
| アプロード結果で「エラープロンプト」が表示されている場合、エラー情報を確認して登録する写真を変更してください。 | アプロード結果で「エラーログ」が表示されている場合、エラー情報を確認して登録する写真を変更してください。 |
|  |  |

**＜エラープロンプト一覧表＞　※「顔登録ガイドライン」を参照して写真の撮り直しをお願いします。**

| No | エラー内容 | 対応方法 |
|---|---|---|
| 1 | 80000 ピクセル未満の画像解像度 | 1920×1080 ピクセル以上/5MB 未満の写真を使用します。 |
| 2 | 顔が検出されませんでした | 何らかの理由で顔を検出できません。 |
| 3 | 複数の顔が検出されました | 背景等にモノや人物が写り込んでいます。 |
| 4 | 顔の比率が小さすぎます（顔の縮尺が小さすぎる） | 顔が小さく、顔の特徴量を抽出できません。 |
| 5 | 画像は非カラー画像です | カラー写真を使用してください。 |
| 6 | 画像がぼやけている | 顔登録ガイドラインに従って再撮影します。 |
| 7 | 画像がかなり露出している | 露出が高い状態、白飛びして顔の特徴量が抽出できません。 |
| 8 | 画像が暗すぎる | 顔の特徴量が抽出できません。 |
| 9 | ノイズの多い写真 | 鮮明でないため、顔の特徴量が抽出できません。 |
| 10 | 伸ばした顔（顔写真が伸びすぎている） | 広角などの特殊撮影は顔の特徴量が抽出できません。 |
| 11 | 顔が覆われています | 帽子やサングラスなど、顔を覆っているものを外します。 |
| 12 | 過剰な笑顔 | 平常時の表情で、顔登録ガイドラインに従って再撮影します。 |
| 13 | 顔の偏向角度が大きすぎます | 正面を向き、肩を水平にして再撮影します。 |
| 14 | 画像の明るさが重要（画像が明るすぎる） | 蛍光灯や太陽光等の光源が写真に写っています。 |
| 15 | 面切り不良タイプ | 顔の一部が検出できません。 |
| 16 | 写真の形式が正しくありません。JPG/ PNG 形式のファイルをアップロードしてください | JPG/ PNG 形式のファイルを再アップロードしてください。 |

**注意事項**

**＊写真データ名は、ユーザーID を指定します（特殊文字は使用不可）。**
**＊データ形式は JPG または PNG で、フル HD（1920×1080）以上、データ容量 5MB 未満を推奨します。**
**＊一度に選択できる写真データは、499 枚です。500 枚以上の写真データを選択しないようにしてください。**

### ④　生体テンプレートインポート

当社または本製品ではサポート対象外です。

### ⑤　ディスミッションのインポート

当社または本製品ではサポート対象外です。

### ⑥　排出インポートテンプレートをダウンロードします

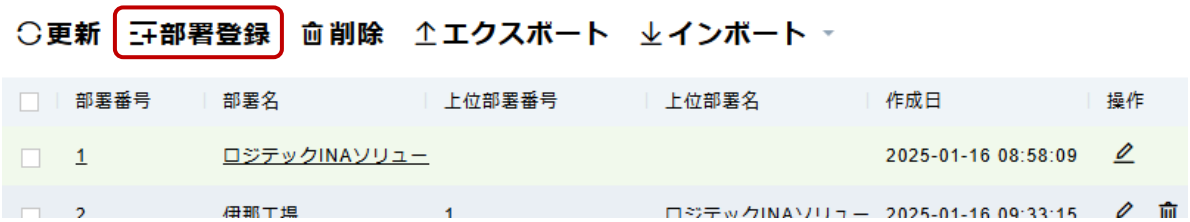
当社または本製品ではサポート対象外です。

## 9.6.2. 部署

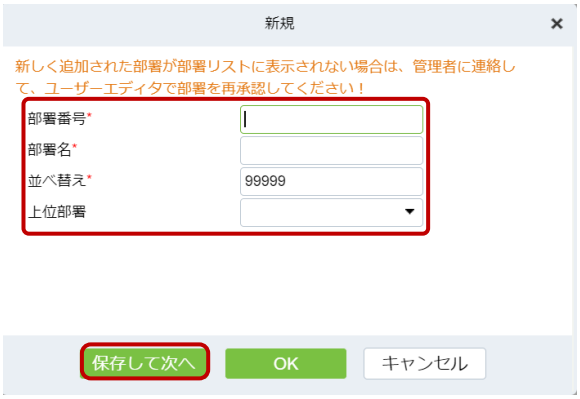
ユーザーが所属する部署の設定を説明します。（初期値：部署）

### 1. 部署登録

① 新規に部署を登録する場合は「部署登録」をクリックします。初期値で登録されている「部署名」は削除することはできません。お客様の会社名に変更すると、新規に追加する部署との関連性が分かり易くなります。

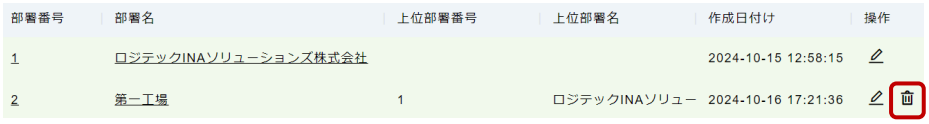



② 部署番号（重複なし）、部署名、ソート順、必要な場合は上位部署を選択し「OK」をクリックします。続けて部署を登録する場合は「保存して次へ」をクリックします。




### 2. 削除

① 該当部署の「ゴミ箱」アイコンをクリックします。

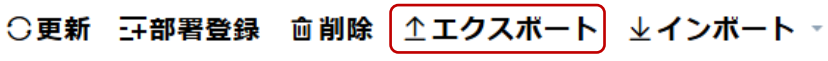


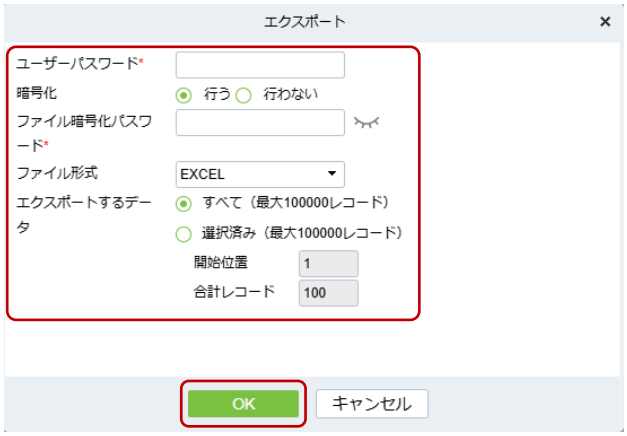

② 確認画面が表示されるので削除をする場合は「OK」をクリックします。削除しない場合は「キャンセル」をクリックします。



### 3. エクスポート

登録した部署の一覧を EXCEL・PDF・CSV・TXT のいずれかの形式でエクスポートすることができます。各条件を指定して最後に「OK」をクリックします。なお、暗号化した場合、Windows 標準の解凍ツールは使用できません。



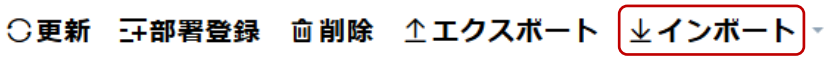

| 設定項目 | 内容 |
|---|---|
| ユーザーパスワード* | 管理者ユーザーのパスワードを入力します。 |
| ファイル暗号化 | データの暗号化を指定します。 |
| ファイル暗号化パスワード* | ファイル暗号化を指定した場合、復号化するパスワードを指定します。 |
| ファイル形式 | EXCEL・PDF・CSV・TXT から選択します。 |
| エクスポートするデータ | すべて：最大 10 万件を上限にの全データをダウンロードします。 |
| | 選択済み：開始レコードと上限（終了レコード）を指定してダウンロードします。 |

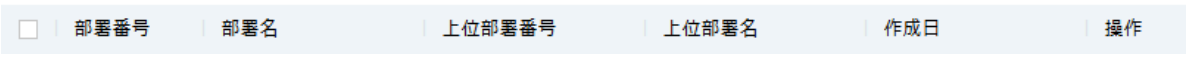
*印は必須です。

エクスポートの説明は、以上で終わりです。

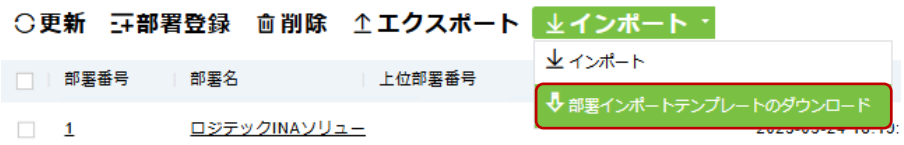
### 4. インポート

インポート用のフォーマットを使用して一括登録することができます。



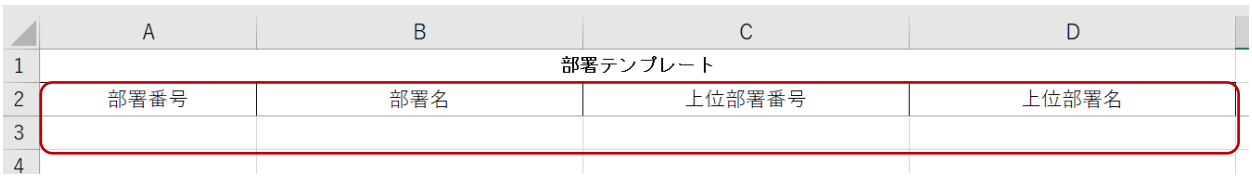




① 部署テンプレートをダウンロード（エクスポート）します。




インポートテンプレート：　部署テンプレート_20241017132655.xls

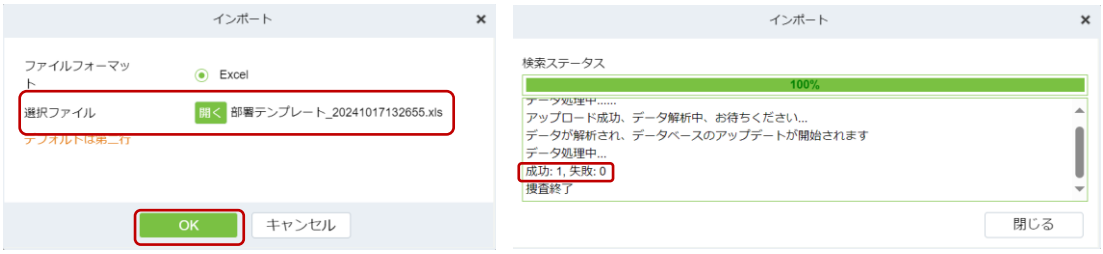
② ダウンロードしたインポートテンプレートに情報を入力して「上書き保存」します。



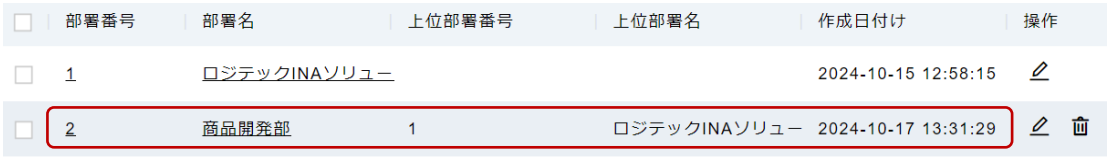
③ 「インポート」をクリックします。




④ 「開く」をクリックし、インポートするインポートテンプレートを選択します。最後に「OK」をクリックします。インポートの進捗が表示され、最後にインポート結果が表示されます。




⑤ インポート後、正常に部署が登録されているかを確認してください。




インポートの説明は、以上で終わりです。

### 9.6.3. ポジション

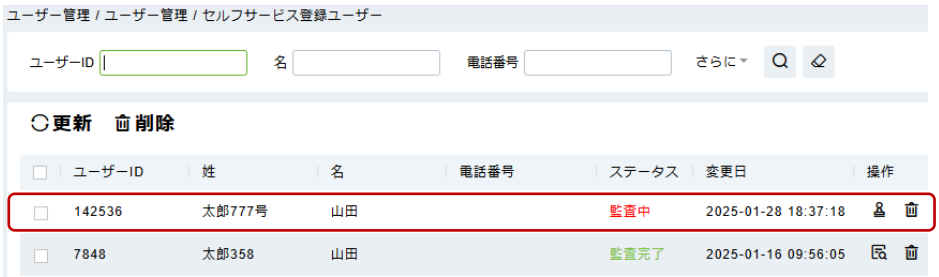
当社または本製品ではサポート対象外です。

### 9.6.4. 離職ユーザー

当社または本製品ではサポート対象外です。

### 9.6.5. セルフサービス登録ユーザー

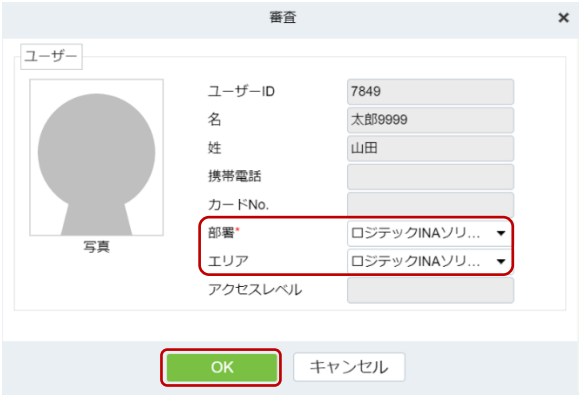
セルフサービス登録を行なったユーザーの一覧が表示されます。「セルフサービス登録ユーザーの自動監査」の設定によってステータスが「監査中」と「監査完了」で表示されます。「監査中」のユーザーの監査方法は以下の手順で行います。なお、セルフサービス登録の詳細は「9.6.9 セルフサービス登録」を参照してください。



① ユーザーを本登録する場合は操作の「」をクリックします。




② 適切な部署やエリアを設定し、監査を完了する場合は「OK」をクリックします。
※部署やエリアの選択項目が表示されない場合、既に同じユーザーID で登録されています。この状態で監査を完了すると、既存のユーザー情報が新しい情報で上書きされますので注意してください。




**注意事項**

**ユーザー登録方法は、重複及び既存情報の上書きを避けるため、次のいずれかの方法で統一してください。**
**管理ソフトで個別登録：個別登録及び一括登録で登録されたユーザー情報内で重複をチェックしません**
**管理ソフトで一括登録：個別登録及び一括登録で登録されたユーザー情報内で重複をチェックしません**
**セルフサービス登録　：セルフサービス登録で登録されたユーザー情報内で重複をチェックしません**
**端末で登録　　：管理ソフトからデバイスに同期されたユーザー情報内で重複をチェックします**

### 9.6.6. カスタム属性

当社または本製品ではサポート対象外です。

### 9.6.7. リストライブラリ

当社または本製品ではサポート対象外です。

## 9.6.8. パラメータ

「パラメータ」メニューは、ユーザー管理における共通設定です。当社がサポートする標準 UI（表 1）を参照してください。

（表 1）当社がサポートする「パラメータ」メニューの一覧

| 大分類 | 中分類 | 標準 UI | 詳細 UI | 説明 |
|---|---|---|---|---|
| パラメータ | ユーザーID 設定 | ○ | ○ | ユーザーID に関する設定をします。 |
| | カード設定 | ○ | ○ | IC カードに関する設定をします。 |
| | セルフサービス登録ユーザー設定 | ○ | ○ | ユーザー登録に管理者の許可を必要とするかどうかを指定します。 |
| | セルフサービス登録 | ○ | ○ | QR コードで登録専用アドレスを使い、ユーザー自身に顔登録をしてもらう機能です。 |
| | 顔テンプレート抽出サーバー | × | ○ | 当社または本製品ではサポート対象外です。 |
| | 個人の機密情報の保護 | ○ | ○ | 管理ソフト上でユーザー情報の表示・非表示を設定します。 |

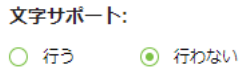
### 1. ユーザーID 設定

顔認証デバイスで取り扱うユーザーID に関する設定をします。

① ユーザーID の最大長を設定します。当社の本製品（LTC-FPT50/IPV2）の最大長は 14 です。
（初期値：9）




② ID 内に英数字を使用する場合は「行う」、数字のみの場合は「行わない」を選択します。（初期値：行わない）
※有効にするには③「ユーザーID 自動追加」を「行わない」にします。運用途中で変更することはできません。ユーザー登録を行う前に設定を変更してください。



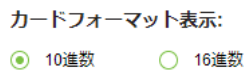

③ 個別登録時にユーザーID を数字の 1～自動採番する場合は「行う」、手動入力は「行わない」を選択します。（初期値：行う）




### 2. カード設定

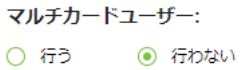
顔認証デバイスで利用するために登録する IC カード情報に関する設定をします。

① カードフォーマット表示
IC カード情報のフォーマットを指定します。（初期値：10 進数）



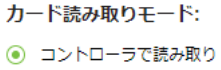
② マルチカードユーザー ※本製品ではサポート対象外です

ユーザーが所有する IC カードについて、複数登録する場合は「行う」、1 つの場合は「行わない」を選択します。（初期値：行わない）




③ カード読み取りモード

カードの読み取り方法を指定します。本製品では初期値のままお使いください。



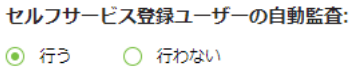

### 3. セルフサービス登録ユーザー設定／セルフサービス登録

セルフサービス登録とは、ユーザーに対して登録用 QR を発行し、スマートフォンやタブレット端末を使ってユーザー自身で登録をする機能*です。本機能で登録できる認証方式は「顔認証」のみです。必要な場合、顔認証デバイス（登録機）を使用して認証方式を追加します。

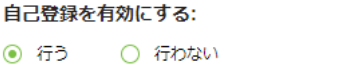
**注意事項**

***ローカルエリアネットワーク（LAN）で利用する機能です。QR を読み取る端末（スマートフォン、タブレットなど）は、PC またはサーバー機器と相互通信できる同一ネットワークに接続する必要があります。**

① セルフサービス登録の管理者による監査を行なった上で本登録する場合は「行わない」を選択します。管理者による監査を行わない場合は登録まで完了します。（初期値：行う）




② セルフサービス登録を有効にする場合は、「行う」をクリックします。（初期値：行う）



③ QR に表示する登録用サーバードレスを指定します。http（または https）://IP アドレス:8098 まで入力すると、「tokenAdreg」のパラメータは自動で入力されます。以下は、PC またはサーバー機器の IP アドレスが「192.168.10.145」の場合の入力例です。




④ 「QR コード画像をダウンロード」をクリックしてダウンロードします。メールなどで登録予定のユーザーに公開*します。
※QR を使用した登録方法は「9.6.9 セルフサービス登録」を参照してください。

## 4. 顔テンプレート抽出サーバー

当社または本製品ではサポート対象外です。

## 5. 個人の機密情報の保護（初期値：OFF）

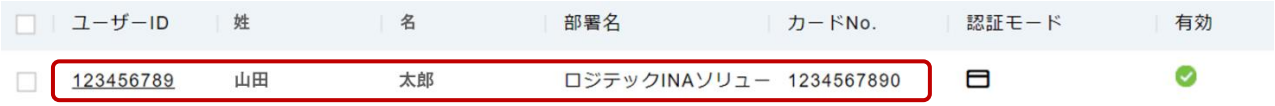
ユーザー情報一覧を表示した際、表示を保護する情報を選択します。保護したい情報のチェックを入れます。




＜チェックが入っている場合のユーザー情報＞




＜チェックが入っていない場合のユーザー情報＞



## 9.6.9. セルフサービス登録

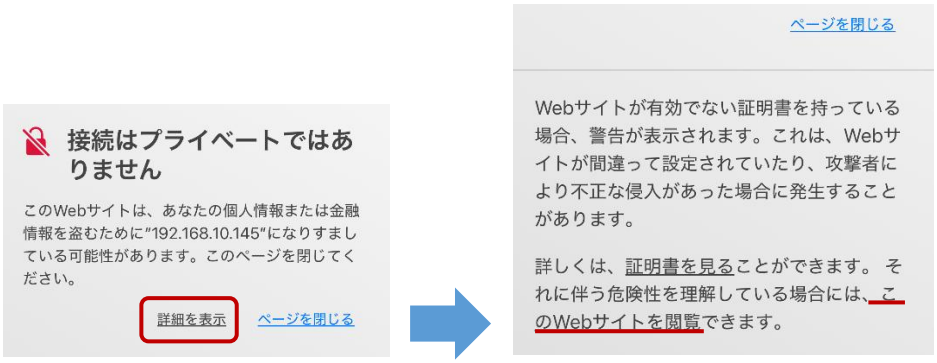
セルフサービス登録の機能*1 を使用してユーザー自身で登録する方法を説明します。本機能を使用する場合、予め「セルフサービス登録」で機能の設定をしてください。（本説明はユーザーが所持する iPhone®の Safari をデフォルトのブラウザアプリに設定した場合の例です*2）

**注意事項**

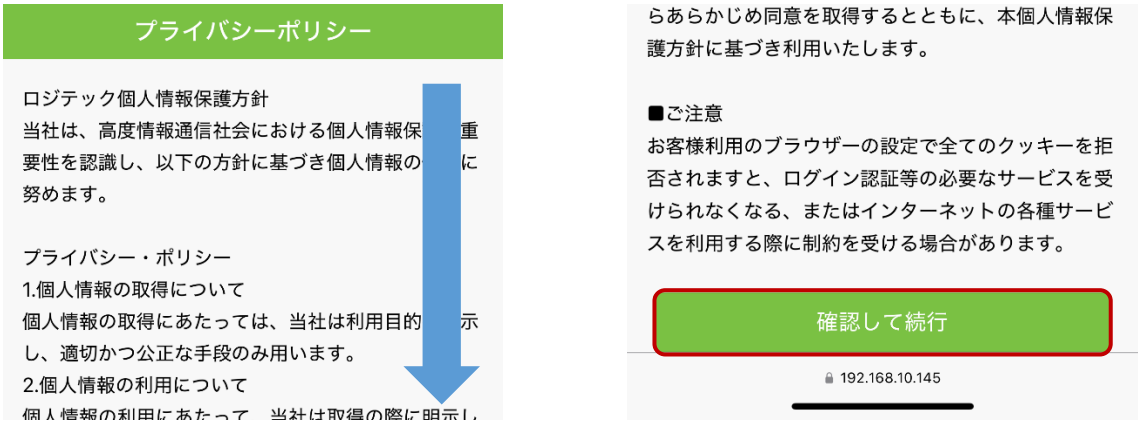
***1：エリアや部署が複数登録されている場合、初期値の自動監査ではなく管理者による監査を行い、監査時に適切なエリアと部署を選択して監査を完了してください。自動監査の場合、最上位エリアと最上位部署に自動的に登録されます。**

***2：iPhone®で登録画面が表示されない場合、iPhone®の「設定」→「アプリ」→「Safari」を開き、「プライバシーとセキュリティ」の項目の「接続が安全ではないときに警告」を「OFF」にしてから、再度 QR を読み込んでセルフサービス登録の画面を表示してみてください。**

1. セルフサービス登録用の QR をカメラまたはアプリで読み込み、URL をタップします。証明書がインストールされていないクライアント機器でアクセスすると警告が表示されます。この場合「詳細を表示」をクリックし、表示された詳細の「この Web サイトを閲覧」をタップします。




2. プライバシーポリシーが表示されます。スクロールして「確認して続行」をタップします。
（初期値：英語）※プライバシーポリシーをカスタム設定している場合はこの限りでありません。



3. 顔登録するために「カメラ」マークをタップします。予め保存されている顔写真を使用する場合は「写真ライブラリ」または「ファイルを選択」をタップして使用する顔写真を選択します。新規に顔写真を撮影する場合は「写真またはビデオを撮る」をタップして前面カメラに切り替えてから撮影をします。




4. 撮影した写真で問題がなければ「写真を使用」をタップします。再撮影する場合は「再撮影」をタップします。

5. ユーザーID、姓・名を入力し、最後に「完了」をタップします。

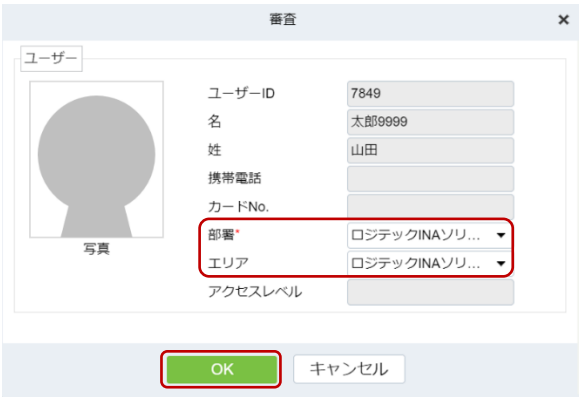



6. ユーザー登録に管理者の承認が必要な場合（自動監査でない場合）
管理者は「ユーザー管理」メニューの「セルフサービス登録ユーザー」で承認をします。

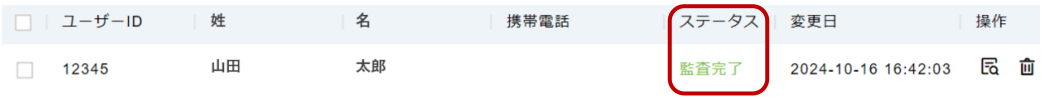
① ステータスが「監査中」となりこの時点では顔認証はできません。「」アイコンをクリックします。



② 適切な部署やエリアを設定し、監査を完了する場合は「OK」をクリックします。登録情報を修正する場合は、操作の「ゴミ箱」アイコンで申請内容を削除し、ユーザーに再申請をしてもらいます。
※部署やエリアの選択項目が表示されない場合、既に同じユーザーID で登録されています。この状態で監査を完了すると、既存のユーザー情報が新しい情報で上書きされますので注意してください。




② ステータスが「監査完了」になっていることを確認します。




7. ユーザー登録に管理者の承認が不要の場合（自動監査の場合）
自動でステータスが「監査完了」となります。登録したユーザー情報で顔認証ができるか確認してください。




セルフサービス登録を使用したユーザー登録方法の説明は、以上で終わりです。

**注意事項**

***ステータスが「監査完了」になったユーザーは、「ユーザー管理メニュー」の「ユーザー」に追加されます。「ユーザー」に追加されたユーザーを削除しても「セルフサービス登録ユーザー」内に追加された申請情報は削除されません。削除したユーザーを改めてセルフサービス登録で追加する場合、セルフサービス登録ユーザー内の対象ユーザーも削除する必要があります。**

***ユーザー登録方法は、重複及び既存情報の上書きを避けるため、次のいずれかの方法で統一してください。**
**管理ソフトで個別登録：個別登録及び一括登録で登録されたユーザー情報内で重複をチェックしません**
**管理ソフトで一括登録：個別登録及び一括登録で登録されたユーザー情報内で重複をチェックしません**
**セルフサービス登録　：セルフサービス登録で登録されたユーザー情報内で重複をチェックしません**
**端末で登録　　：管理ソフトからデバイスに同期されたユーザー情報内で重複をチェックします**

## 9.7. カード管理

IC カード情報および QR の管理をします。*

**注意事項**

***IC カード情報は、FeliCa：ISO/IEC 18092「NFC Type F」、MIFARE：ISO/IEC 14443「Type A」に対応**
***IC カードの ID 取得（読み取り）のみをサポートします。動作確認済みのカードは以下の通りです。**
**・「FeliCa」の「IDm」情報**
**・「Mifare Plus」の「UID」情報**
**・「Mifare Ultralight EV1」の「UID」情報**
**・「Mifare Classic 1K」の「UID」情報**
***IC カード情報および QR 情報について**
**・IC カード情報と QR 情報は、入退 Push モードの場合、カード登録数（50,000）の範囲で複数登録できます。**
**勤怠 Push モードの場合、IC カードまたは QR のいずれかの登録（排他）ができます。**
**・IC カード情報または QR 情報を削除する場合は、「ユーザーリスト」の「削除」から「カード番号のみ削除」を行ってください。**

### 9.7.1. カード

ユーザー情報に紐づく IC カード情報および QR を管理します。一括登録、紛失したカードを無効・有効にすることができます。




**1. カード一括登録**

当社または本製品ではサポート対象外です。

**2. ACMS カード**

当社または本製品ではサポート対象外です。

**3. 紛失カードの無効化**

紛失した IC カードおよび QR について認証を無効にします。

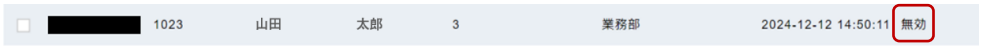
① 紛失したカードを選択して「紛失カード数」をクリックします。



② 無効化する確認画面が表示されますので「OK」をクリックします。




③ 選択したカード No の「カード状況」が「無効」になっていることを確認します。



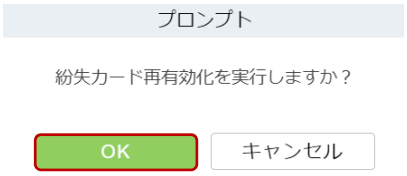

## 4. 紛失カード再有効化

紛失したカードが発見された場合、認証を有効にします。

① 有効化するカードを選択して「紛失カード再有効化」をクリックします。




② 有効化する確認画面が表示されますので「OK」をクリックします。




③ 選択したカード No の「カード状況」が「有効」になっていることを確認します。



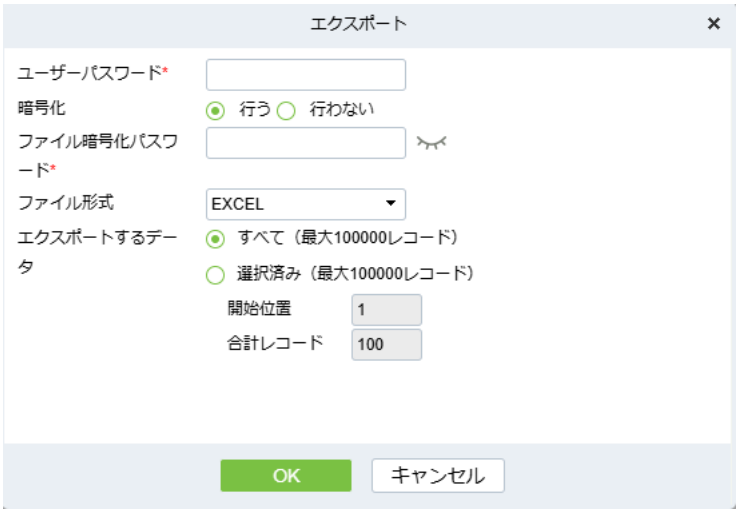

## 5. エクスポート

選択したカード情報をエクスポートします。有効・無効に関わらずカード情報はエクスポートされます。なお、暗号化した場合、Windows 標準の解凍ツールは使用できません。

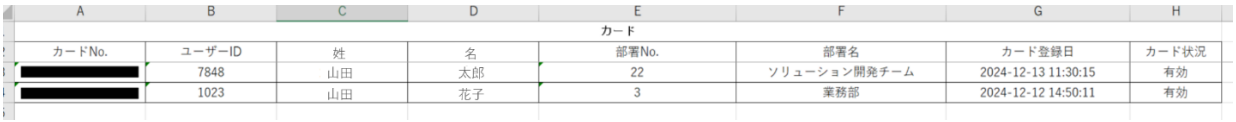
① エクスポートしたい IC カードを選択して「エクスポート」をクリックします。



② エクスポート条件を入力して「OK」をクリックします。




③ エクスポートしたデータを確認します。



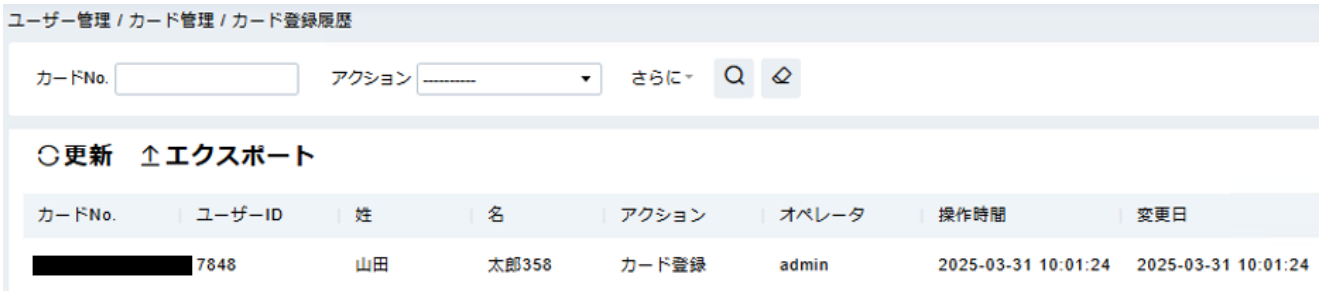
| A | B | C | D | E | F | G | H |
|---|---|---|---|---|---|---|---|
| | | | | カード | | | |
| カードNo. | ユーザーID | 姓 | 名 | 部署No. | 部署名 | カード登録日 | カード状況 |
| [redacted] | 7848 | 山田 | 太郎 | 22 | ソリューション開発チーム | 2024-12-13 11:30:15 | 有効 |
| [redacted] | 1023 | 山田 | 花子 | 3 | 業務部 | 2024-12-12 14:50:11 | 有効 |

## 9.7.2. Wiegand フォーマット

当社または本製品ではサポート対象外です。

## 9.7.3. カード登録履歴

ユーザー毎に IC カードの登録履歴を確認することができます。IC カード No や IC カードに対する処理区分（アクション）によって絞込検索をすることができます。



## 9.8. 勤怠連携




管理ソフトの「勤怠管理」メニューについて説明します。原則、勤怠管理の詳細機能（詳細 UI）は、外部連携先の勤怠管理システムで行います。当社または本製品では、顔認証デバイスをタイムレコーダーとして利用する機能に限定して提供されます。当社がサポートする標準 UI は（表 1）を参照してください。

（表 1）当社がサポートする「勤怠連携（標準 UI）」メニューの一覧

| 大分類 | 中分類 | 標準 UI | 詳細 UI | 説明 |
|---|---|---|---|---|
| デバイス管理 | ユーザー認証モード | ○ | ○ | 勤怠打刻におけるユーザーの認証方式を設定します。 |
| | エリア別ユーザー登録 | ○ | ○ | エリアに所属するユーザーを割り当てます。 |
| | デバイス登録 | ○ | ○ | 勤怠打刻に使用する顔認証デバイスを登録・管理します。 |
| | 打刻場所登録 | ○ | ○ | 将来の機能拡張用であり、現状はサポート対象外です。 |
| | サーバーコマンド | △ | ○ | 参考機能（サーバーから発行されたコマンドを記録します） |
| | デバイス操作ログ | ○ | ○ | 顔認証デバイスで操作された内容を記録します。 |
| 勤怠設定 | 基本ルール | ○ | ○ | 打刻ボタンの名称、認証時スクリーンショットを設定きます。 |
| | 休日 | × | ○ | 当社または本製品ではサポート対象外です。 |
| | 休暇タイプ | × | ○ | 当社または本製品ではサポート対象外です。 |
| | 自動レポート | ○ | ○ | 勤怠打刻を指定した日時でメール送信または FTP サーバーへ保存します。 |
| | フロー設定 | × | ○ | 当社または本製品ではサポート対象外です。 |
| シフト管理 | タイムゾーン | × | ○ | 当社または本製品ではサポート対象外です。 |
| | シフト | × | ○ | 当社または本製品ではサポート対象外です。 |
| | ユーザーシフト | × | ○ | 当社または本製品ではサポート対象外です。 |
| | グループシフト | × | ○ | 当社または本製品ではサポート対象外です。 |
| | スケジュールの詳細 | × | ○ | 当社または本製品ではサポート対象外です。 |
| 出席例外管理 | サインイン追加 | × | ○ | 当社または本製品ではサポート対象外です。 |
| | 休暇 | × | ○ | 当社または本製品ではサポート対象外です。 |
| | 残業 | × | ○ | 当社または本製品ではサポート対象外です。 |
| | 休息調整 | × | ○ | 当社または本製品ではサポート対象外です。 |
| | シフト調整 | × | ○ | 当社または本製品ではサポート対象外です。 |
| 勤怠レポート | 手動計算 | × | ○ | 当社または本製品ではサポート対象外です。 |
| | トランザクション | ○ | ○ | 勤怠履歴を確認できます。 |
| | デイリーアテンダンス | ○ | ○ | 当日の勤怠履歴を確認できます。 |
| 出席日報 | デイリーレポート | × | ○ | 当社または本製品ではサポート対象外です。 |
| | 作業時間レポート | × | ○ | 当社または本製品ではサポート対象外です。 |
| | 残業レポート | × | ○ | 当社または本製品ではサポート対象外です。 |
| | 詳細フォームを残す | × | ○ | 当社または本製品ではサポート対象外です。 |
| | 異常な出席テーブル | × | ○ | 当社または本製品ではサポート対象外です。 |
| | 後期レポート | × | ○ | 当社または本製品ではサポート対象外です。 |
| | 早期レポートを残す | × | ○ | 当社または本製品ではサポート対象外です。 |
| | 欠席レポート | × | ○ | 当社または本製品ではサポート対象外です。 |
| 出席月次レポート | マンスリーレポート | × | ○ | 当社または本製品ではサポート対象外です。 |
| | 月間作業時間レポート | × | ○ | 当社または本製品ではサポート対象外です。 |
| | 毎月のカードレポート | × | ○ | 当社または本製品ではサポート対象外です。 |
| | 毎月の残業レポート | × | ○ | 当社または本製品ではサポート対象外です。 |

| | | | | |
|---|---|---|---|---|
| 出席統計レポート | 月次統計レポート | × | ○ | 当社または本製品ではサポート対象外です。 |
| | スタッフの残業概要レポート | × | ○ | 当社または本製品ではサポート対象外です。 |
| | 休暇サマリ | × | ○ | 当社または本製品ではサポート対象外です。 |
| | 部署別レポート | × | ○ | 当社または本製品ではサポート対象外です。 |
| | 部門残業概要レポート | × | ○ | 当社または本製品ではサポート対象外です。 |
| | 部門休暇概要レポート | × | ○ | 当社または本製品ではサポート対象外です。 |
| | 年次休暇バランスシート | × | ○ | 当社または本製品ではサポート対象外です。 |
| 出欠カスタムレポート | 出欠カスタムレポート | × | ○ | 当社または本製品ではサポート対象外です。 |

## 9.9. デバイス管理

顔認証デバイスに関する設定を説明します。

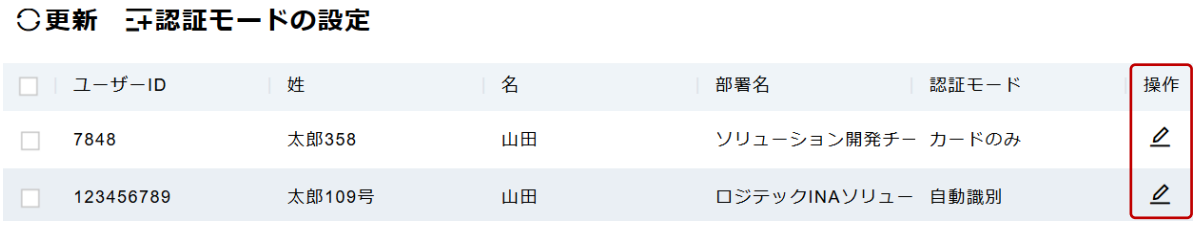
### 9.9.1. ユーザー認証モード

予め登録されているユーザーに対して認証モードを個別または一括で設定することができます。認証モードを指定する場合に本機能で設定を行います。また、ユーザー登録時、認証モードの初期値は「自動識別」で推奨設定となります。なお、該当ユーザーはユーザーID、名前、部署名で絞り込み検索ができます。



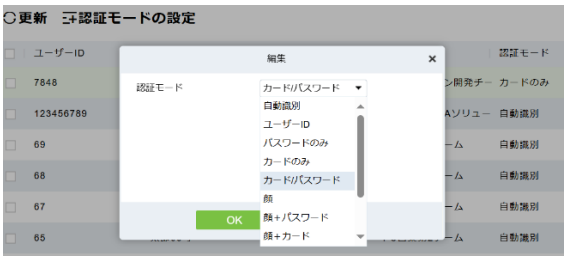

**1. 個別設定**

① 個別設定する場合、ユーザーリストの「操作」の「編集」アイコンをクリックします。

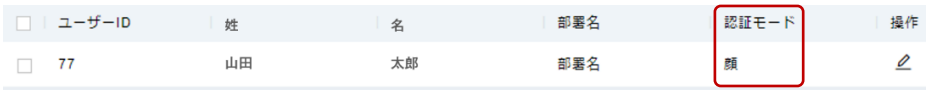



② 認証モードを選択して最後に「OK」をクリックします。

※本製品で対応している認証モードは以下の＜認証モード一覧＞を参照してください。



③ 該当ユーザーの認証方式が設定されていることを確認します。



| | ユーザーID | 姓 | 名 | 部署名 | 認証モード | 操作 |
|---|---|---|---|---|---|---|
| | 77 | 山田 | 太郎 | 部署名 | 顔 | |

## 2. 一括設定

① 該当ユーザーのチェックボックスにチェックをします。全てのユーザーを選択する場合は、1 ページあたりの行数を増やして「ユーザーID」項目名の左にあるチェックボックスにチェックを入れます。次に「認証モードの設定」をクリックします。

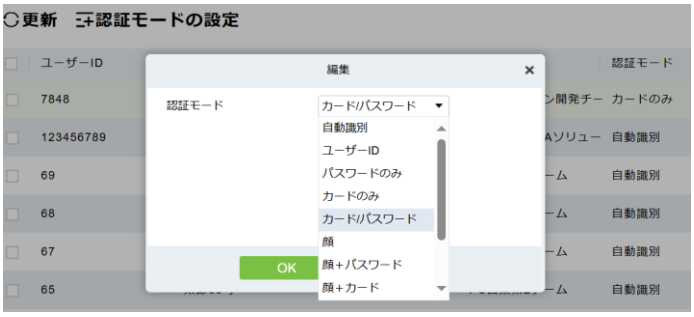


更新　認証モードの設定

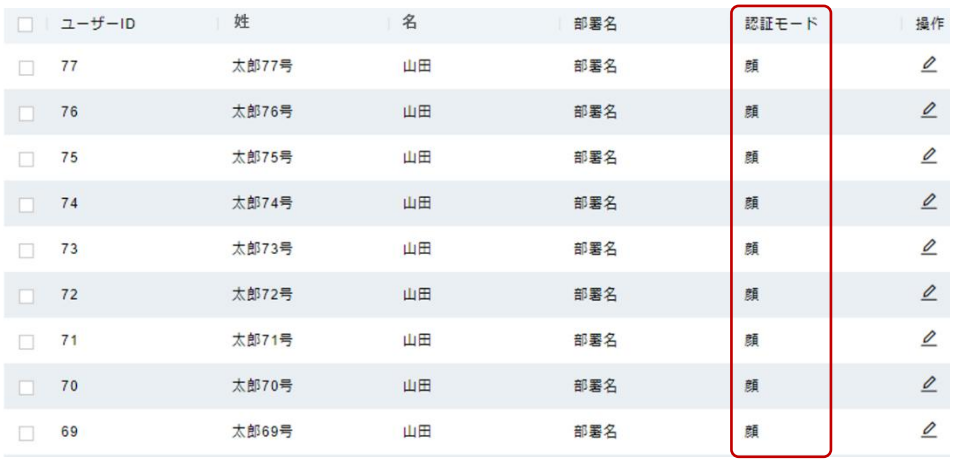
| | ユーザーID | 姓 | 名 | 部署名 | 認証モード | 操作 |
|---|---|---|---|---|---|---|
| ☑ | 7848 | 太郎358 | 山田 | ソリューション開発チー | カードのみ | |
| ☑ | 123456789 | 太郎109号 | 山田 | ロジテックINAソリュー | 自動識別 | |
| ☑ | 69 | 太郎69号 | 山田 | PC営業第2チーム | 自動識別 | |
| ☑ | 68 | 太郎68号 | 山田 | PC営業第2チーム | 自動識別 | |
| ☑ | 67 | 太郎67号 | 山田 | PC営業第2チーム | 自動識別 | |
| ☑ | 65 | 太郎65号 | 山田 | PC営業第2チーム | 自動識別 | |

② 認証モードを選択して最後に「OK」をクリックします。

※本製品で対応している認証モードは以下の＜認証モード一覧＞を参照してください。




③ 該当ユーザーの認証モードが設定されていることを確認します。



| | ユーザーID | 姓 | 名 | 部署名 | 認証モード | 操作 |
|---|---|---|---|---|---|---|
| | 77 | 太郎77号 | 山田 | 部署名 | 顔 | |
| | 76 | 太郎76号 | 山田 | 部署名 | 顔 | |
| | 75 | 太郎75号 | 山田 | 部署名 | 顔 | |
| | 74 | 太郎74号 | 山田 | 部署名 | 顔 | |
| | 73 | 太郎73号 | 山田 | 部署名 | 顔 | |
| | 72 | 太郎72号 | 山田 | 部署名 | 顔 | |
| | 71 | 太郎71号 | 山田 | 部署名 | 顔 | |
| | 70 | 太郎70号 | 山田 | 部署名 | 顔 | |
| | 69 | 太郎69号 | 山田 | 部署名 | 顔 | |

**＜認証モード一覧＞** ※下記は当社または本製品はサポートする認証モードです。

| 認証モード | 内容 |
|---|---|
| 自動識別 | 認証方式を自動判別して認証します。 |
| ユーザーID | ユーザー番号で認証します。 |
| パスワードのみ | ユーザー番号とパスワードで認証します。 |
| カードのみ | IC カードで認証します。 |
| カード/パスワード | IC カードまたはパスワードで認証します。 |
| 顔 | 顔で認証します。 |
| 顔＋パスワード | 顔とパスワードの二要素で認証します。 |
| 顔＋カード | 顔と IC カードの二要素で認証します。 |
| 掌 | 掌で認証します。 |
| 掌＋カード | 掌と IC カードの二要素で認証します。 |
| 掌と顔 | 掌と顔のマルチモーダルで認証します。 |

## 9.9.2. エリア別ユーザー登録

「6.3 部署を設定する ※本手順は省略することができます」で部署を設定していない場合（初期値：部署名）と、部署を設定した場合の説明をします。

### 1. 部署を設定していない場合

管理拠点の「エリア（例：ロジテック INA ソリューションズ株式会社）」にある「部署」に所属するユーザーを選択します。

① ユーザーを追加したい「エリア名（例：ロジテック INA ソリューションズ株式会社）」をクリックし、「エリアの人を追加」をクリックします。「システム管理」でエリアを複数設定していない場合でも、初期値の「エリア名（例：ロジテック INA ソリューションズ株式会社）」に所属するユーザーを追加する必要があります。



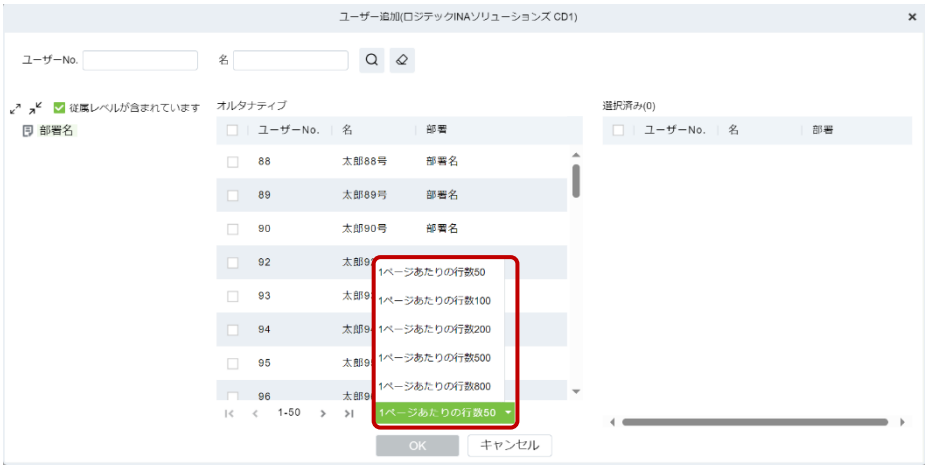

② 「部署名（初期値）」をクリックします。「部署名」に所属するユーザーが一覧表示されます。



③　初期値の「エリア名（例：ロジテック INA ソリューションズ株式会社）」に追加したいユーザーを選択しします。
エリアに追加したいユーザーが全て選択できましたら最後に「OK」をクリックします。




※全てのユーザーを追加する場合「1 ページあたりの行数」からユーザー表示数を変更します。（上限 800 名）
上限 800 名を超える場合、全てのユーザーを追加できるまで手順③の操作を繰り返します。



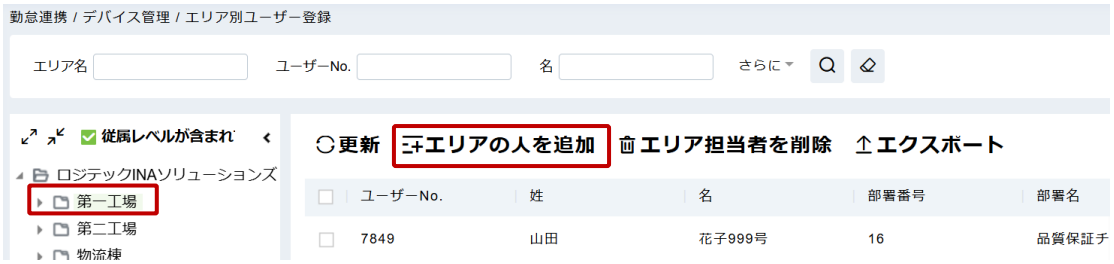

④　初期値の「エリア名（例：ロジテック INA ソリューションズ株式会社）」に追加したユーザーが表示されていることを確認します。



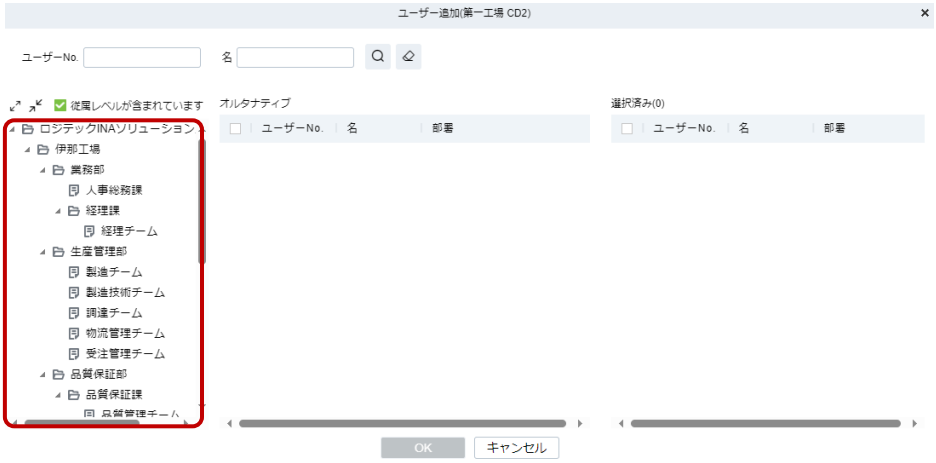
## 2. 部署を設定している場合

管理拠点となる「エリア（例：第一工場または第二工場）」に属する「部署」に所属するユーザーを選択します。

① ユーザーを追加したい「エリア名」をクリックし、「エリアの人を追加」をクリックします。



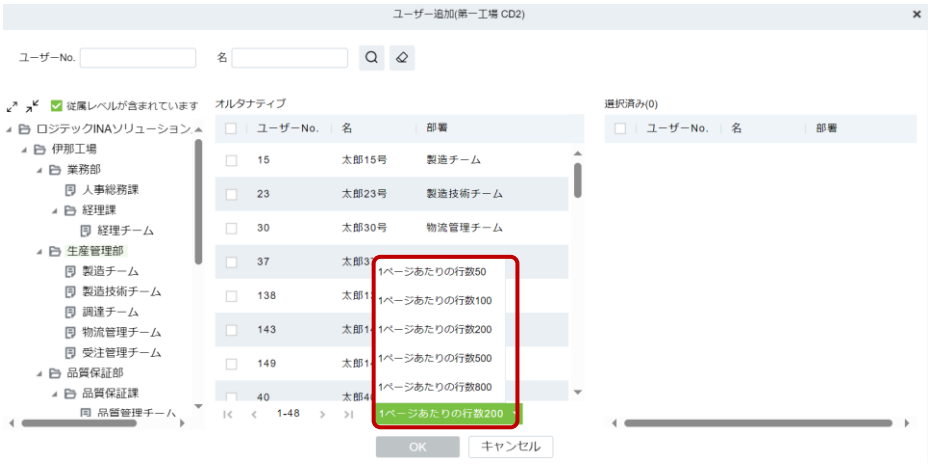

② 「エリア」に属する「部署」をクリックします。「部署」に所属するユーザーが一覧表示されます。




③ 下記例は「商品開発部」に属する各チームに所属するユーザーを選択します。エリアに追加したいユーザーが全て選択できましたら最後に「OK」をクリックします。



※全てのユーザーを追加する場合「1 ページあたりの行数」からユーザー表示数を変更します。（上限 800 名）
上限 800 名を超える場合、全てのユーザーを追加できるまで手順③の操作を繰り返します。




④ 「エリア名（例：第一工場）」に追加したユーザーが表示されていることを確認します。

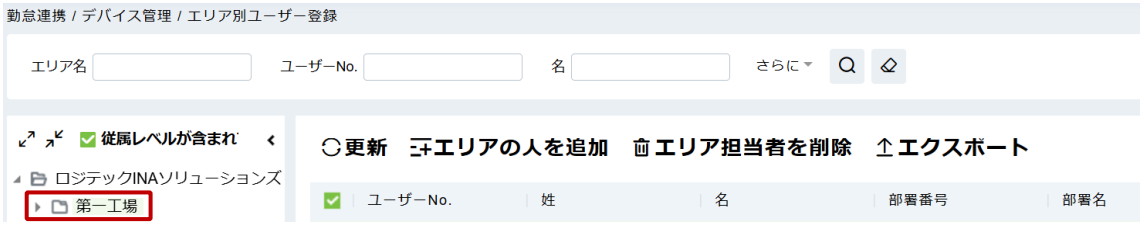



エリア別ユーザー登録の説明は、以上で終わりです。

## 3. エリア担当者を削除

エリアに割り当てられたユーザーを削除します。

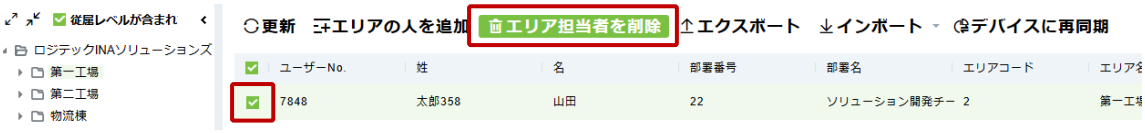
① 対象エリアをクリックします。




② ユーザーを「ユーザーNo」または「姓名」で絞り込み検索します。



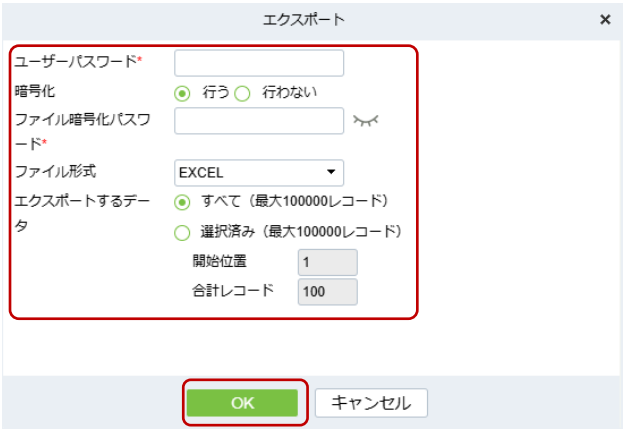
③ 削除対象のユーザーにチェックを入れ「エリア担当者を削除」をクリックします。




## 4. エクスポート

登録したエリアの一覧を EXCEL・PDF・CSV・TXT のいずれかの形式でエクスポートすることができます。各条件を指定して最後に「OK」をクリックします。エクスポートしたデータはインポートすることもできます。なお、暗号化した場合、Windows 標準の解凍ツールは使用できません。



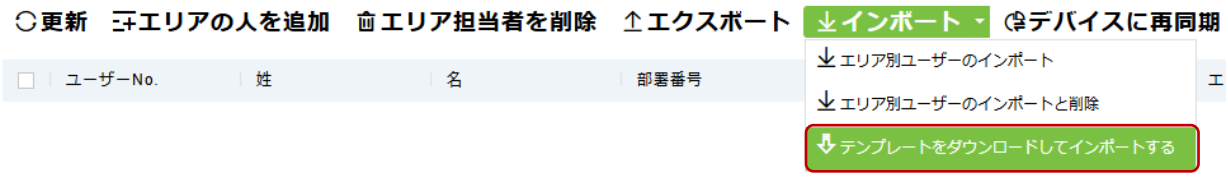




| 設定項目 | 内容 |
|---|---|
| ユーザーパスワード* | 管理者ユーザーのパスワードを入力します。 |
| ファイル暗号化 | データの暗号化を指定します。 |
| ファイル暗号化パスワード* | ファイル暗号化を指定した場合、復号化するパスワードを指定します。 |
| ファイル形式 | EXCEL・PDF・CSV・TXT から選択します。 |
| エクスポートするデータ | すべて：最大 10 万件を上限にの全データをダウンロードします。 |
| | 選択済み：開始レコードと上限（終了レコード）を指定してダウンロードします。 |

## 5. インポート

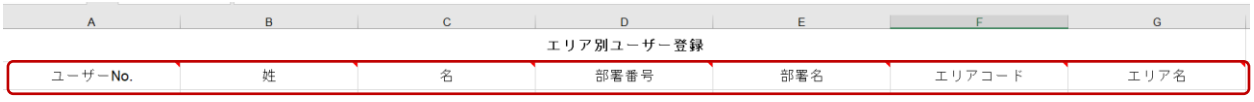
インポート用のフォーマットを使用して一括登録することができます。

① テンプレートをダウンロードします。




インポートテンプレート： エリア別ユーザー登録_20250129182727.xls

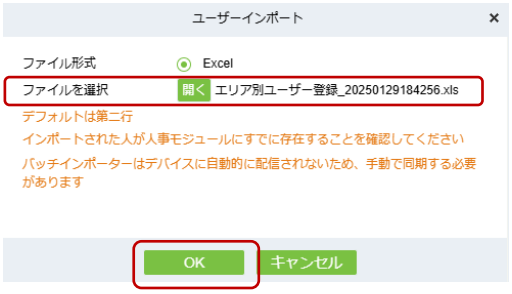
② ダウンロードしたインポートテンプレートに情報を入力して「上書き保存」します。

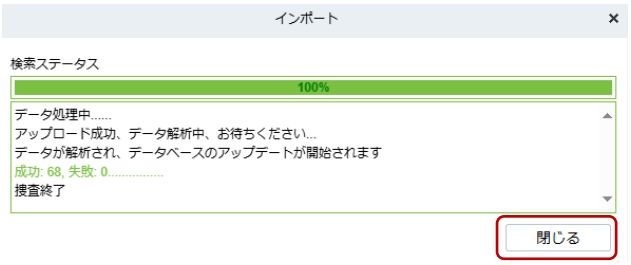


③ 「インポート」をクリックします。




④ 「開く」をクリックし、インポートするインポートテンプレートを選択します。最後に「OK」をクリックします。インポートの進捗が表示され、最後にインポート結果が表示されます。




⑤ インポート後、正常にエリアが登録されているかを確認してください。



| ユーザーNo. | 姓 | 名 | 部署番号 | 部署名 | エリアコード | エリア名 |
|---|---|---|---|---|---|---|
| 44 | 太郎44号 | 山田 | 22 | ソリューション開発チー | 2 | 第一工場 |
| 53 | 太郎53号 | 山田 | 26 | タブレット開発チーム | 2 | 第一工場 |
| 54 | 太郎54号 | 山田 | 26 | タブレット開発チーム | 2 | 第一工場 |

## 6. デバイスに再同期

顔認証デバイスへインポートした情報を同期します。なお、顔認証デバイスへ上手く同期されない場合にも使用できます。

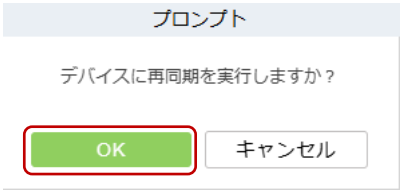
① 顔認証デバイスへ同期するユーザーを選択（チェック）して「デバイスに再同期」をクリックします。



更新 エリアの人を追加 エリア担当者を削除 エクスポート インポート デバイスに再同期

| ユーザーNo. | 姓 | 名 | 部署番号 | 部署名 | エリアコード | エリア名 |
|---|---|---|---|---|---|---|
| 44 | 太郎44号 | 山田 | 22 | ソリューション開発チー | 2 | 第一工場 |
| 53 | 太郎53号 | 山田 | 26 | タブレット開発チーム | 2 | 第一工場 |
| 54 | 太郎54号 | 山田 | 26 | タブレット開発チーム | 2 | 第一工場 |
| 55 | 太郎55号 | 山田 | 26 | タブレット開発チーム | 2 | 第一工場 |

② 確認画面が表示されますので「OK」をクリックします。



## 9.9.3. デバイス登録

エリアごとに設置する顔認証デバイスを登録します。エリア内に登録された顔認証デバイスは「登録機」として設定することで、顔認証デバイスからユーザー情報や掌・IC カードなどを登録することができます。




### 1. デバイス登録

① 「デバイス登録」をクリックします。




② 設定したエリアで利用する端末を選択して操作列の「追加」をクリックします。

※顔認証デバイスが一覧に表示されない場合、以下の点を確認してください。

- ✓ 顔認証デバイスの電源が入っていて、ネットワークに接続して IP アドレスを取得していること
- ✓ 「デバイスタイプの設定」が「入退 Push」になっていること（勤怠 Push から入退 Push に変更している場合、管理ソフト上の勤怠連携で登録されている顔認証デバイスも登録を削除する必要があります。）
- ✓ 「4.4 クラウドサーバの設定」で設定したクラウドサーバの IP アドレスに誤りがないこと、通信ポートが「8088」に設定されていること
- ✓ ここまで確認して検索されない場合、顔認証デバイスを「リセット」して「通信設定」をやり直してください。



③ 「アクセスエリア」から選択した顔認証デバイスを利用するエリア（例：第一工場）を選択します。




④ 選択したデバイスを「登録機」として設定する場合はチェックを入れます。「登録機」として設定すると顔認証デバイスでユーザーの個別登録や掌・IC カードなどの認証情報を設定することができます。最後に、設定を保存する場合は「OK」をクリックします。




**注意事項**

**＊デバイス登録後、運用中に登録機の設定を ON（チェック）/OFF（チェックを外す）と、設定を有効にするために顔認証デバイスが自動で再起動します。**

⑤ 顔認証デバイスの登録が正常におこなわれ、デバイスを設定したエリア（例：第一工場）に表示されていることを確認します。表示されない場合は、10 秒程度時間をおいてから「更新」をクリックしてください。



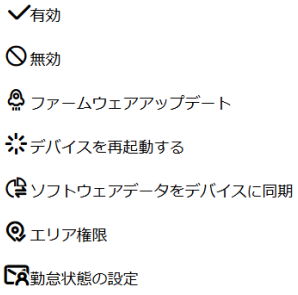

※手順①～⑤は、導入する顔認証デバイスの台数の設定を繰り返します。

**注意事項**

**＊顔認証デバイスを使って顔登録を行う場合、同一エリア内の登録機の設定は 1 台のみで運用をお願いします。**
**同一エリア内で複数の登録機から同時にユーザー登録を行うとユーザー情報が正常に登録できません。**
**例）同一エリア内で 2 台の顔認証デバイスが稼働している場合**
**顔認証デバイス 2 台中 1 台を登録機に設定します。他の顔認証デバイスでも顔登録を行う場合、予め登録機として設定していた顔認証デバイスを解除してから新たに他の顔認証デバイスを登録機として設定します。**

## 2. デバイス管理

許可されたデバイスとして登録されている顔認証デバイスを管理します。




| 設定項目 | 内容 |
|---|---|
| 有効 | オフラインに設定した顔認証デバイスをオンラインにします。 |
| 無効 | 選択した顔認証デバイスをオフラインにします。 |
| ファームウェアアップデート | 選択した顔認証デバイスのファームウェアを更新します。 |
| デバイスを再起動する | 選択した顔認証デバイスを再起動します。 |
| ソフトウェアデータをデバイスに同期 | 管理ソフトの設定情報をデバイスへ反映します。 |
| エリア権限 | 選択したデバイスのエリアを変更します。 |
| 勤怠状態の設定 | 打刻ボタン名称の設定、認証時キャプチャーを設定します。 |

### ① 有効

デバイス交換またはオフラインに設定した顔認証デバイスをオンラインに設定します。




### ② 無効

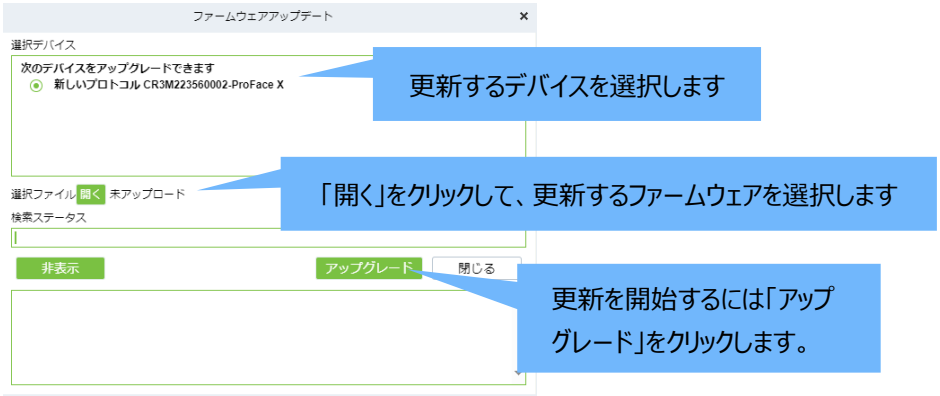
選択した顔認証デバイスをオフラインに設定します。




### ③ ファームウェアアップデート ※ロジテックのサポート情報の指示に従って実施してください

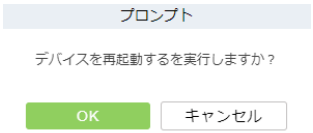
選択した顔認証デバイス（選択は 10 台以下を推奨）のファームウェアを更新します。同じモデルの場合は複数選択することができます。更新する場合、ファームウェアを選択し「アップグレード」をクリックします。ファームウェアの更新が正常に完了すると再起動します。

※ファームウェア更新中は、電源を切ったり、更新中に画面を閉じたりしないでください。端末が使用できなくなります。



**④ デバイスを再起動する**

選択した顔認証デバイスを再起動します。再起動する場合は「OK」をクリックします。

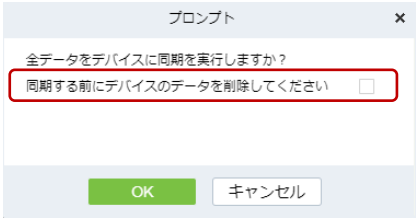



**⑤ パブリックメッセージ**

当社または本製品はサポート対象外です。

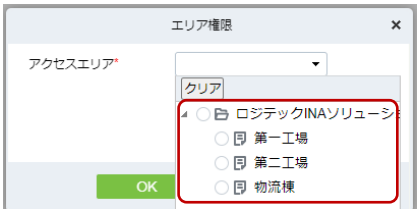
**⑥ ソフトウェアデータをデバイスに同期**

選択した顔認証デバイスへ管理ソフトで設定したユーザー情報や設定情報を送信（同期）します。顔認証デバイス内のデータを消去してから同期する場合は「同期する前にデバイスのデータを削除してください」へチェックを入れて「OK」をクリックします。




**⑦ エリア権限**

選択した顔認証デバイスのエリアを変更します。変更先のエリアを選択して「OK」をクリックします。

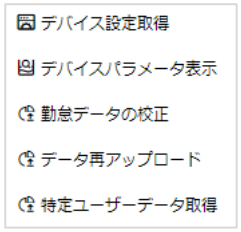



**⑧ 勤怠状態の設定**

「9.9.7 勤怠設定」を参照してください。

## 3. 情報表示

選択した顔認証デバイスの各種情報の取得を行います。




| 設定項目 | 内容 |
|---|---|
| デバイス設定取得 | 選択した顔認証デバイスのパラメータを取得します。 |
| デバイスパラメータ表示 | 選択したデバイスの各種パラメータを表示します。 |
| 勤怠データの校正 | 管理ソフトに同期されていない勤怠データを再取得します。 |
| データ再アップロード | 認証データ（履歴・認証時キャプチャー）を再取得します。 |
| 特定ユーザーデータ取得 | ユーザーを指定して勤怠データを取得します。 |

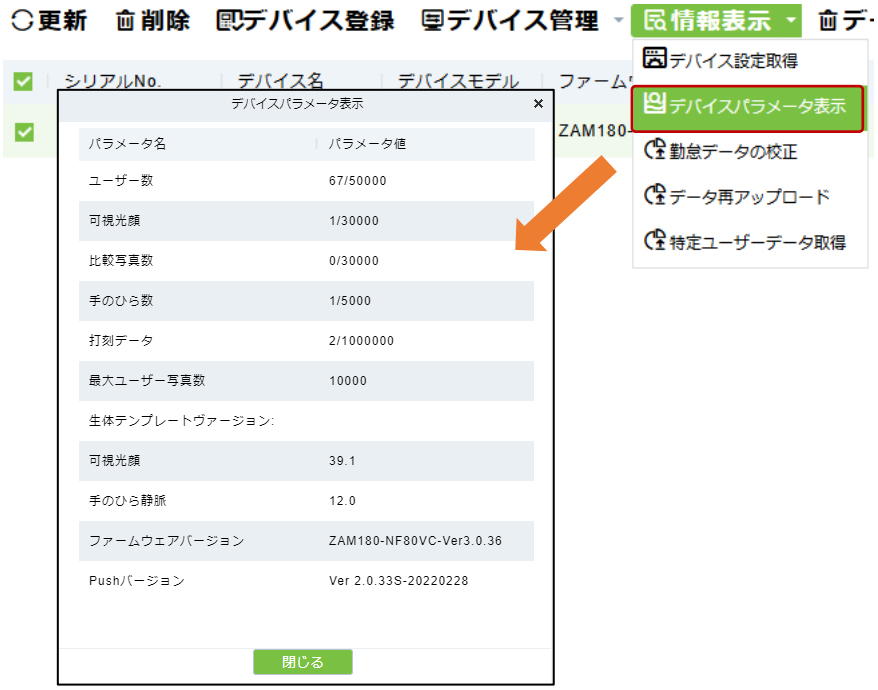
### ① デバイス設定取得

デバイスパラメータを取得します。取得したパラメータを確認するには次項「デバイスパラメータ表示」を参照してください。
「情報表示」の「デバイス設定取得」をクリックします。




### ② デバイスパラメータ表示

「デバイス設定取得」で取得した各種パラメータを表示します。表示するにはデバイスを選択して「デバイスパラメータ表示」をクリックします。



### ③ 勤怠データの校正

管理ソフトに同期されていない勤怠データについて、日時を指定して手動で再取得します。




再取得したい期間（日時）を指定して「OK」をクリックします。

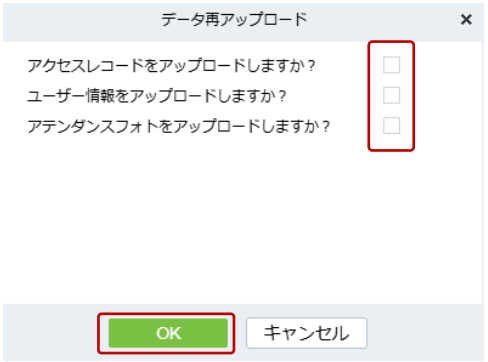



### ④ データ再アップロード

選択した顔認証デバイスから管理ソフトへ、アクセス履歴やアテンダンスフォト（認証時キャプチャ写真）の情報を取得します。




取得したい情報を選択して「OK」をクリックします。

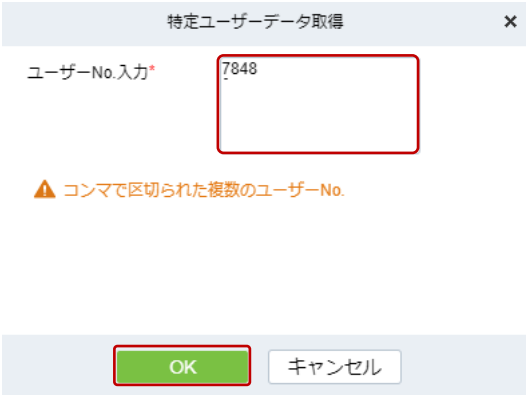


**特定ユーザーデータ取得**

「登録機」から管理ソフトへ、ユーザー番号を指定したユーザーの勤怠履歴を取得します。選択した顔認証デバイスが登録機でない場合はエラーが表示されます。

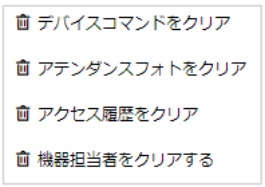



特定ユーザーの勤怠履歴を取得するには、ユーザー番号（カンマで区切ると複数指定可）を入力して「OK」をクリックします。




## 4. データクリア

選択した顔認証デバイスに記録された各種情報を削除します。




| 設定項目 | 内容 |
|---|---|
| デバイスコマンドをクリア | 選択したデバイスの操作コマンドを消去します。 |
| アテンダンスフォトをクリア | 選択したデバイスの認証時キャプチャーを消去します。 |
| アクセス履歴をクリア | 選択したデバイスの勤怠履歴を消去します。 |
| デバイスの登録ユーザーをクリアする | 選択したデバイスに登録されたユーザーを消去します。 |

### ① デバイスコマンドをクリア

選択された顔認証デバイスのコマンド履歴（再起動など）を削除します。削除する場合は「OK」をクリックします。本操作を行わない場合でも保存上限に達すると古い履歴から自動的に削除されます。



② **アテンダンスフォトをクリア**

選択された顔認証デバイス側のカメラモードを使って勤怠打刻時に撮影した写真データを削除します。削除する場合は「OK」をクリックします。本操作を行わない場合でも保存上限に達すると古い履歴から自動的に削除されます。



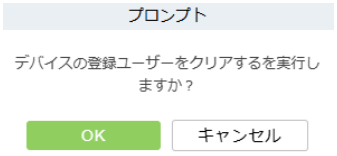

③ **アクセス履歴をクリア**

選択された顔認証デバイスの勤怠履歴を削除します。削除する場合は「OK」をクリックします。本操作を行わない場合でも保存上限に達すると古い履歴から自動的に削除されます。




④ **デバイスの登録ユーザーをクリアする**

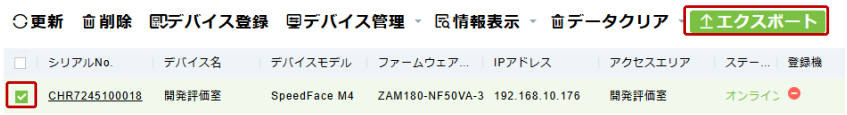
選択された顔認証デバイスに登録されたユーザーを削除します。



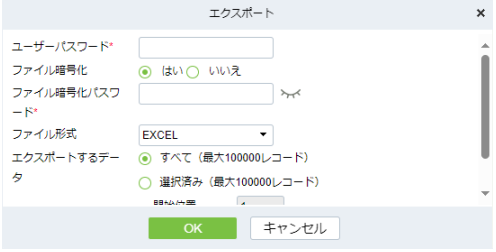

## 5. エクスポート

登録した顔認証デバイスの一覧をエクスポートすることができます。なお、暗号化した場合、Windows 標準の解凍ツールは使用できません。

① エクスポートしたい顔認証デバイスを選択し「エクスポート」をクリックします。




② エクスポート条件を入力して「OK」をクリックします。



## 9.9.4. 打刻場所登録

将来の機能拡張用であり、現状はサポート対象外です。

## 9.9.5. サーバーコマンド（参考）

管理ソフトから顔認証デバイスに対して発行されたコマンドを確認することができます。管理ソフトからコマンドを発行した結果、デバイスとの相互通信が「成功・失敗・応答なし（戻らなかった）」の項目で閲覧することができます。




## 9.9.6. デバイス操作ログ（参考）

勤怠管理用で登録された顔認証デバイス側の操作ログを確認することができます。



## 9.9.7. 勤怠設定

勤怠連携に関する各種共通の運用設定をすることができます。設定した条件を保存する場合は「OK」をクリックします。

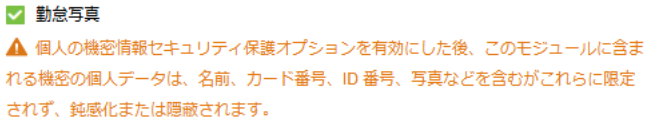
### 1. 基本ルール

#### ① 勤怠状態の設定

勤怠打刻ボタンの名称設定を行います。詳細は「7.4 打刻方法の設定」を参照してください。

#### ② 個人の機密情報の保護（初期値：ON）

顔認証デバイスから取得した認証時のキャプチャ（勤怠写真）をトランザクション上で表示する設定を行います。非表示するには ON（チェック）、表示するには OFF（チェックを外す）に設定します。




### 2. 休日

当社または本製品はサポート対象外です。

### 3. 休暇タイプ

当社または本製品はサポート対象外です。

### 4. 自動レポート

勤怠履歴を指定した日時でメール送信または FTP サーバーへ保存します。

※レポートには打刻種別の情報は出力されません




① 自動レポートを作成するには「新規」をクリックします。



② 各情報を入力・選択します。

**<メール送信の場合>**




**<FTP サーバへ保存する場合>**



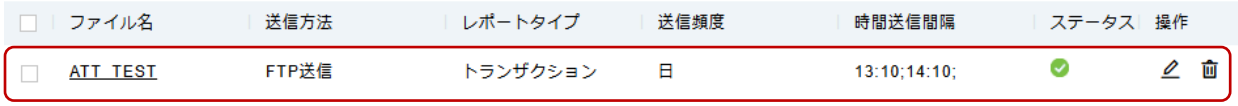
| カテゴリ | 設定項目 | 内容 |
|---|---|---|
| レポート設定 | レポートタイプ* | トランザクション（全て）、デイリーアテンダンス（当日）、デイリーレポート（当日）から選択します。 |
| | ファイル名* | 送信するファイル名を任意で決めます。 |
| | 日付フォーマット | 「YYYYMMDD／YYYY-MM-DD」から選択します。 |
| | ファイルタイプ* | 「EXCEL／TXT」から選択します。 |
| 送信頻度 | 送信頻度 | 「毎日／毎月」を選択します。 |
| | 毎日：時・分 | 毎日：送信時間を指定します。（最大 6 回） |
| | 毎月：月末・月初・特定の日付 | 毎月：毎月指定日を設定します。 |
| 送信方法設定 | 送信方法* | 「メール送信／FTP 送信」を選択します。 |
| メール設定 | 受信者設定 | 「ユーザー／部署／エリア」から選択します。 |
| | メールアドレス* | 受信者をユーザーにした場合、送信先アドレスを指定します。 |
| | 件名 | 送信レポートの件名を指定します。（50 文字まで） |
| | 本文 | 送信レポートの本文を指定します。（200 文字まで） |
| FTP 設定 | FTP サーバーIP* | FTP サーバーのアドレスを指定します。 |
| | FTP サーバーポート* | FTP サーバーのポート番号を指定します。 |
| | FTP ユーザー名* | FTP サーバーに接続及び書き込みできるユーザーを指定します。 |
| | FTP パスワード* | ユーザーのパスワードを指定します。 |
| | テスト接続 | FTP サーバーへの接続テストを行います。 |

*は必須項目です。

③ 設定を保存する場合は「OK」をクリックします。続けてレポートを作成する場合は「保存して次へ」をクリックします。




④ 作成されたレポートが表示されているか確認します。




**＜自動レポートを有効／無効にする方法＞**

作成した自動レポート送信を一時的に無効にしたり、有効に戻すことができます。無効にする場合は、レポートを選択して「無効」をクリックします。有効に戻す場合は、レポートを選択して「有効」をクリックします。ステータスで有効／無効を確認します。



**＜自動レポートを削除する方法＞**

削除するレポートを選択して「削除」をクリックします。




**5. フロー設定**

当社または本製品はサポート対象外です。

### 9.9.8. シフト管理

当社または本製品はサポート対象外です。

### 9.9.9. 出席例外管理

当社または本製品はサポート対象外です。

## 9.10. 勤怠レポート

### 9.10.1. 手動計算

当社または本製品はサポート対象外です。

### 9.10.2. トランザクション

打刻データの一覧を確認することができます。認証が成功し、打刻情報が生成された記録のみを表示します。認証に成功しても打刻ボタンをタップしないなど、打刻情報が生成されない場合は記録が残りません。




※トランザクションの「勤怠写真」を有効にする場合は、顔認証デバイス側の設定をする必要があります。詳しくは、顔認証デバイスの「10.4 システム設定」の「勤怠 ＞ カメラモード」を参照してください。
※トランザクションの「勤怠写真」を表示する場合は「9.9.7 勤怠設定」の「個人の機密情報の保護」を参照してください。

## 1. 更新

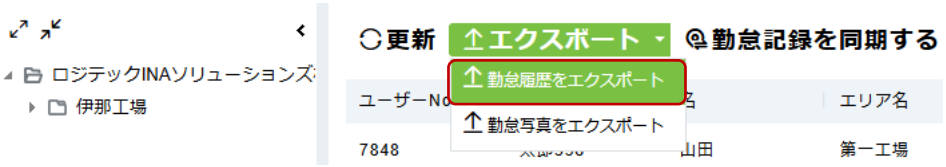
顔認証デバイスから取得した勤怠履歴を最新の状態に更新して表示します。更新する場合は「更新」をクリックします。

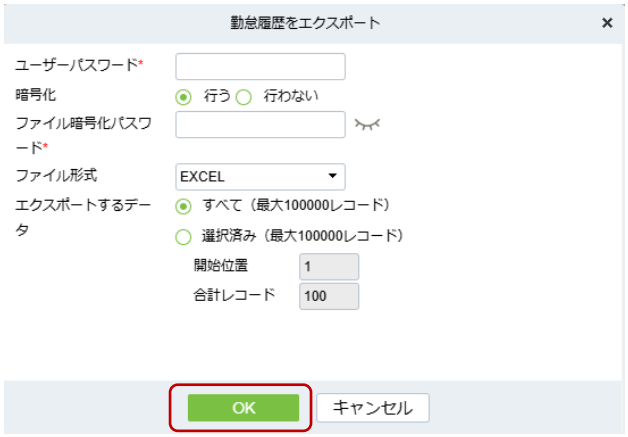



## 2. エクスポート

トランザクション（勤怠履歴／勤怠写真）をエクスポートすることができます。なお、暗号化した場合、Windows 標準の解凍ツールは使用できません。

① 「勤怠履歴をエクスポート」をクリックし、必要事項を入力して最後に「OK」をクリックします。

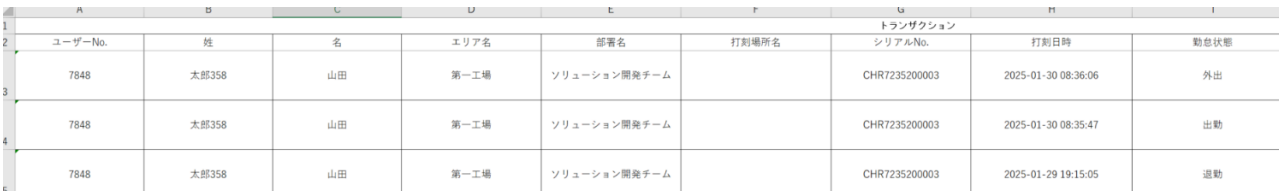



| 設定項目 | 内容 |
|---|---|
| ユーザーパスワード* | 管理者ユーザーのパスワードを入力します。 |
| 暗号化 | データの暗号化を指定します。 |
| ファイル暗号化パスワード* | ファイル暗号化を指定した場合、復号化するパスワードを指定します。 |
| ファイル形式 | EXCEL・PDF・CSV・TXT から選択します。 |
| エクスポートするデータ | すべて：最大 10 万件を上限にデータをダウンロードします。 |
| | 選択済み：開始レコードと上限（終了レコード）を指定してダウンロードします。 |

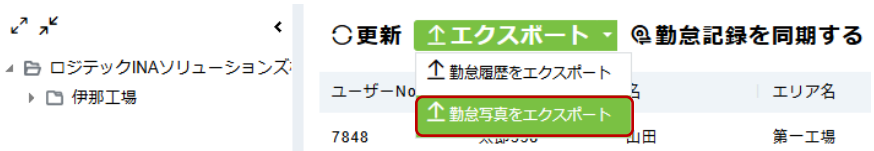
*印は必須項目です。

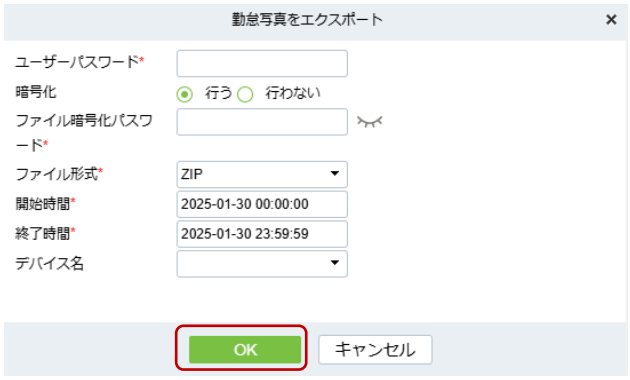
**<トランサクション（勤怠履歴）のエクスポート例>**



| ユーザーNo. | 姓 | 名 | エリア名 | 部署名 | 打刻場所名 | シリアルNo. | 打刻日時 | 勤怠状態 |
|---|---|---|---|---|---|---|---|---|
| 7848 | 太郎358 | 山田 | 第一工場 | ソリューション開発チーム | | CHR7235200003 | 2025-01-30 08:36:06 | 外出 |
| 7848 | 太郎358 | 山田 | 第一工場 | ソリューション開発チーム | | CHR7235200003 | 2025-01-30 08:35:47 | 出勤 |
| 7848 | 太郎358 | 山田 | 第一工場 | ソリューション開発チーム | | CHR7235200003 | 2025-01-29 19:15:05 | 退勤 |

② 「勤怠写真をエクスポート」をクリックし、必要事項を入力して最後に「OK」をクリックします。






| 設定項目 | 内容 |
|---|---|
| ユーザーパスワード* | 管理者ユーザーのパスワードを入力します。 |
| 暗号化 | データの暗号化を指定します。 |
| ファイル暗号化パスワード* | ファイル暗号化を指定した場合、復号化するパスワードを指定します。 |
| ファイル形式 | ZIP から選択します。 |
| 開始時間* | エクスポートする開始日時を指定します。 |
| 終了時間* | エクスポートする終了日時を指定します。 |
| デバイス名 | エクスポートする顔認証デバイスを指定します。 |

*印は必須項目です。

※トランザクションの「勤怠写真」を有効にする場合は、顔認証デバイス側の設定をする必要があります。詳しくは、顔認証デバイスの「10.4 システム設定」の「アクセスログ設定 ＞ カメラモード」を参照してください。
※トランザクションの「勤怠写真」を表示する場合は「9.9.7 勤怠設定」の「個人の機密情報の保護」を参照してください。

### 3. 勤怠記録を同期する

当社または本製品はサポート対象外です。

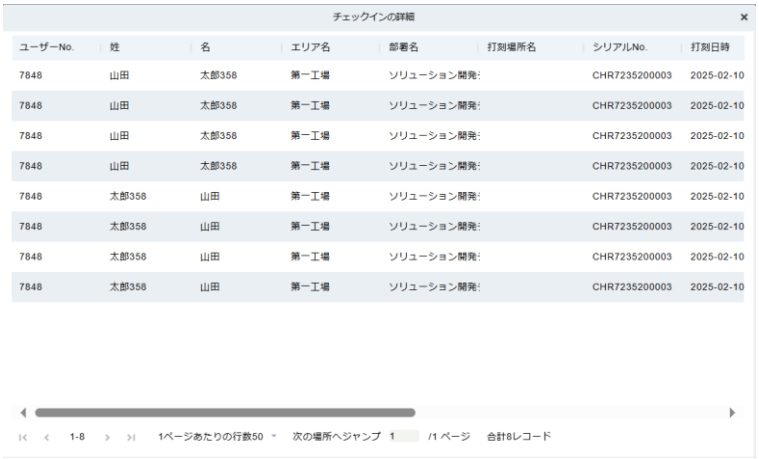
## 9.10.3. デイリーアテンダンス

ユーザー単位で当日の打刻の最初の打刻と最後の打刻、打刻回数などを表示します。「操作」アイコンをクリックすると、ユーザー毎の詳細レポートを表示することができます。

※集計までに時間がかかる場合があります。




**＜詳細レポート例＞**



## 9.11. 出席日報

当社または本製品はサポート対象外です。

## 9.12. 出席月次レポート

当社または本製品はサポート対象外です。

## 9.13. 出席統計レポート

当社または本製品はサポート対象外です。

## 9.14. 出欠カスタムレポート

当社または本製品はサポート対象外です。

## 9.15. 入退室管理




「入退室管理」メニューについて説明します。当社がサポートする標準 UI は（表 1）を参照してください。

（表 1）当社がサポートする「入退室管理（標準 UI）」メニューの一覧

| 大分類 | 中分類 | 標準 UI | 詳細 UI | 説明 |
|---|---|---|---|---|
| アクセスデバイス | デバイス管理 | ○ | ○ | デバイス登録など、デバイスの各種設定をします。 |
| | I/O 拡張ボード | × | ○ | 当社または本製品ではサポート対象外です。 |
| | ドア | ○ | ○ | デバイスに対してドア名、タイムゾーンを割り当てます。 |
| | リーダ | × | ○ | 当社または本製品ではサポート対象外です。 |
| | 補助入力 | × | ○ | 当社または本製品ではサポート対象外です。 |
| | 補助出力 | × | ○ | 当社または本製品ではサポート対象外です。 |
| | イベントタイプ | × | ○ | 当社または本製品ではサポート対象外です。 |
| | サマータイム | × | ○ | 当社または本製品ではサポート対象外です。 |
| | リアルタイムモニタリング | ○ | ○ | ドアの状態監視、認証などのログをリアルタイムに表示します。 |
| | アラームモニタリング | ○ | ○ | デバイスで発生したアラームを一元管理します。 |
| | マップ | ○ | ○ | 任意のレイアウト図を使いデバイスを配置してモニタリングします。 |
| アクセスルール | タイムゾーン | ○ | ○ | アクセス（認証）可能な時間帯のパターン作成し管理します。 |
| | 休日 | × | ○ | 当社または本製品ではサポート対象外です。 |
| | グループ登録 | ○ | ○ | タイムゾーン・エリアを 1 つのグループとして設定します。 |
| | アクセス設定 | ○ | ○ | グループに対してユーザーを割り当てます。 |
| | ユーザー設定 | × | ○ | 当社または本製品ではサポート対象外です。 |
| | 部署設定 | ○ | ○ | 部署に対してタイムゾーンを割り当てて管理します。 |
| | インターロック | × | ○ | 当社または本製品ではサポート対象外です。 |
| | リンケージ | ○ | ○ | デバイスで発生したイベントに応じて接点制御やメールを送信します。 |
| | アンチ・パスバック | ○ | ○ | 共連れ防止のための設定を行います。 |
| | ファーストユーザー解錠 | × | ○ | 当社または本製品ではサポート対象外です。 |
| | マルチパーソングループ | × | ○ | 当社または本製品ではサポート対象外です。 |
| | マルチパーソン | × | ○ | 当社または本製品ではサポート対象外です。 |
| | 認証モード | × | ○ | 当社または本製品ではサポート対象外です。 |
| | 認証モードグループ | × | ○ | 当社または本製品ではサポート対象外です。 |
| | パラメータ | ○ | ○ | 管理ソフトにおける入退室管理の共有設定をします。 |
| アクセス制御レポート | 全トランザクション | ○ | ○ | 各デバイスで発生したイベントや認証履歴を一覧表示します。 |
| | 今日のイベント | × | ○ | 当社または本製品ではサポート対象外です。 |
| | 全例外イベント | × | ○ | 当社または本製品ではサポート対象外です。 |
| | アラームログ | ○ | ○ | 発生したアラームを管理します。（アラームモニタリングと同様） |
| | アラーム処理の履歴 | × | ○ | 当社または本製品ではサポート対象外です。 |
| | ドアアクセス権限 | × | ○ | 当社または本製品ではサポート対象外です。 |
| | ユーザーアクセス権限 | × | ○ | 当社または本製品ではサポート対象外です。 |
| | 最初入り先と最後出し先 | × | ○ | 当社または本製品ではサポート対象外です。 |

# 9.16. アクセスデバイス

入退室管理における顔認証デバイスの各種設定や管理を行います。

## 9.16.1. デバイス管理

顔認証デバイスを新規登録・削除・交換、遠隔で各種操作や管理をします。




**1. 更新**

登録済みの顔認証デバイス一覧を再取得します。再取得する場合は「更新」をクリックします。

**2. デバイス登録**

当社または本製品はサポート対象外です。本項の「**5.デバイス検索**」で新規デバイスの登録をします。

**3. 削除**

登録された顔認証デバイスを個別削除、選択削除または一括削除します。個別削除する場合は、操作項目の「ゴミ箱」アイコンをクリックします。選択削除をする場合は、削除したい顔認証デバイスにチェックを入れ「削除」をクリックします。一括削除うをする場合は、一番上のチェックボックスを選択して全ての顔認証デバイスを選択して「削除」をクリックします。

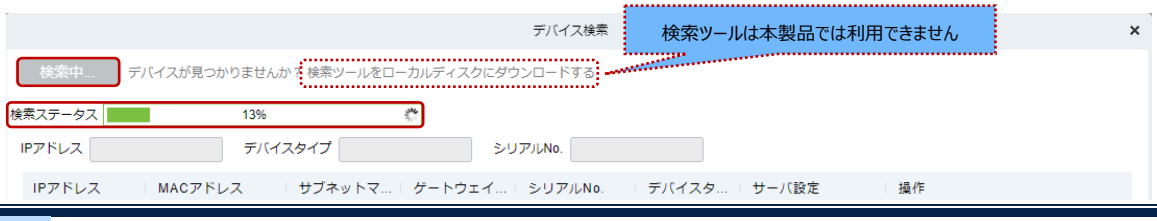



**4. デバイス検索**

同一ネットワーク内に設置された顔認証デバイスを自動で検索して登録することができます。ネットワーク上の顔認証デバイスを検索する場合は「デバイス検索」をクリックします。




① 検索画面が表示されたら「検索」をクリックします。



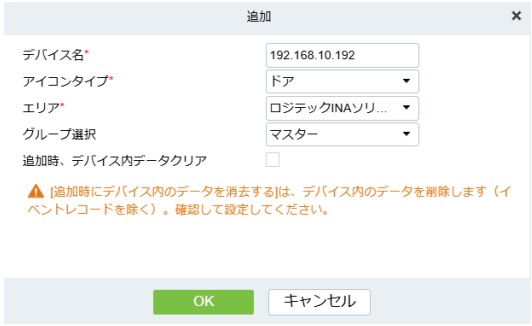
② 顔認証デバイスが検索されたら操作項目の「追加」をクリックします。




※顔認証デバイスが一覧に表示されない場合、以下の点を確認してください。

- ✓ 顔認証デバイスの電源が入っていて、ネットワークに接続して IP アドレスを取得していること
- ✓ 「デバイスタイプの設定」が「入退 Push」になっていること（勤怠 Push から入退 Push に変更している場合、管理ソフト上の勤怠連携で登録されている顔認証デバイスも登録を削除する必要があります。）
- ✓ 「4.4 クラウドサーバの設定」で設定したクラウドサーバの IP アドレスに誤りがないこと、通信ポートが「8088」に設定されていること
- ✓ ここまで確認して検索されない場合、顔認証デバイスを「リセット」して「通信設定」をやり直してください。

※下図は入力例です




| 設定項目 | 内容 |
|---|---|
| デバイス名* | 任意のデバイス名を入力します。 |
| アイコンタイプ* | 初期値で利用します。 |
| エリア* | デバイスを設置するエリアを選択します。 |
| グループ選択* | デバイスに割り当てるアクセス権限を選択します。 |
| 追加時、デバイス内データクリア | 新規登録時にデバイス内のデータを削除します |

③ 入力・選択内容を保存する場合は「OK」をクリックします。登録に成功すると「承認完了」が表示されますので「OK」を押して画面を閉じます。



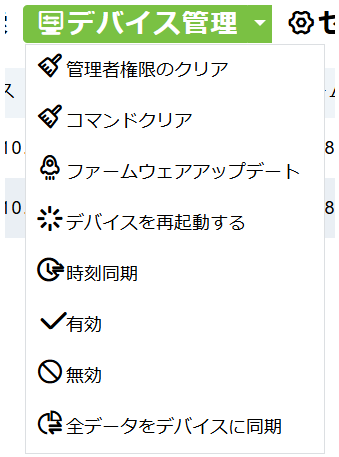

④ 顔認証デバイスの登録が正常におこなわれ、デバイス一覧に表示されていることを確認します。
表示されない場合、10 秒程度時間をおいてから「更新」をクリックします。




※手順①～④は、導入する顔認証デバイスの台数分の設定を繰り返します。

## 5. デバイス管理

顔認証デバイスに対する各種遠隔操作ができます。




| 設定項目 | 内容 |
|---|---|
| 管理者権限のクリア | ユーザーに付与された管理者権限をクリアします。 |
| コマンドクリア | 過去の発行コマンドをクリアします。管理ソフト側は消えません。 |
| ファームウェアアップデート | 当社から提供されるアップデータを指定してファームウェアをアップデートすることができます。 |
| デバイスを再起動する | 遠隔で顔認証デバイスを再起動します。 |
| 時刻同期 | 遠隔で顔認証デバイスを時刻同期（修正）します。 |
| 有効 | 一時的に無効である顔認証デバイスを有効に戻します。 |
| 無効 | 一時的に顔認証デバイスを無効（使用不可）にします。 |
| 全データをデバイスに同期 | アクセス権限などの設定情報をデバイスへ手動で同期します。 |

### ① 管理者権限のクリア

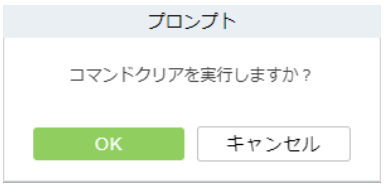
顔認証デバイスに登録されているユーザーの管理者権限を削除します。削除する場合は対象端末を選択し「管理者権限をクリア」をクリックします。実行する場合は「OK」をクリックします。




※ユーザー登録情報に設定されている管理者権限はクリアされません。一時的に管理者権限を無効にして顔認証デバイスを操作する時に利用します。ユーザー登録情報に設定されている管理者権限を変更する場合は、「9.6.1 ユーザー」を参照してください。

### ② コマンドクリア

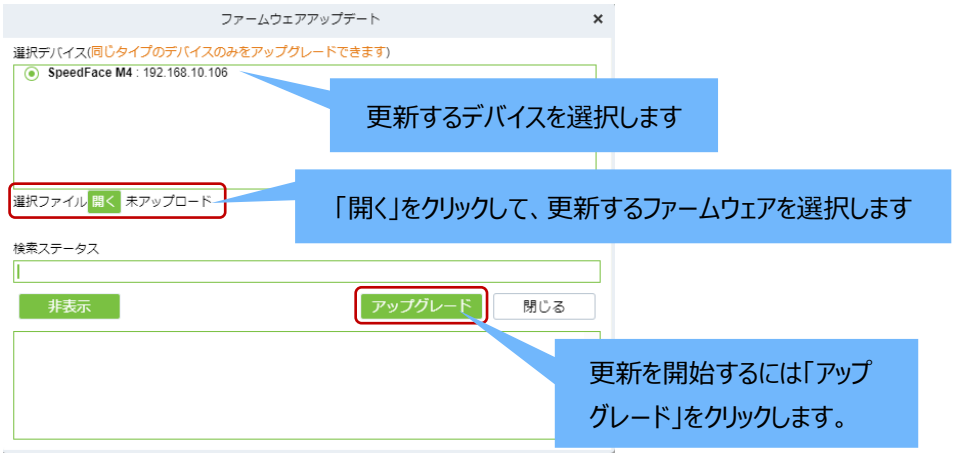
管理ソフトと顔認証デバイスの相互通信で記録された情報を顔認証デバイスから削除します。削除する場合は対象端末を選択し「コマンドクリア」をクリックします。実行する場合は「OK」をクリックします。



③ **ファームウェアアップデート** **※ロジテックのサポート情報の指示に従って実施してください**

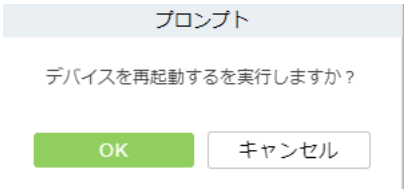
選択した顔認証デバイス（選択は 10 台以下を推奨）のファームウェアを更新します。同じモデルの場合は複数選択することができます。更新する場合、ファームウェアを選択し「アップグレード」をクリックします。ファームウェアの更新が正常に完了すると再起動します。

※ファームウェア更新中は、電源を切ったり、更新中に画面を閉じたりしないでください。端末が使用できなくなります。



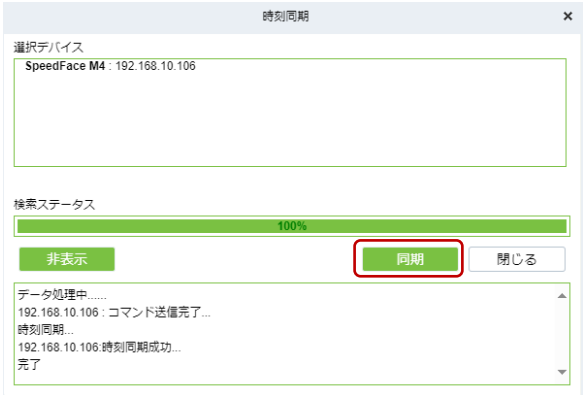

③ **デバイスを再起動する**

顔認証デバイスを遠隔で再起動することができます。動作が不安定になるなどの症状が発生した場合、先ずは顔認証デバイスの再起動を試して症状が改善されるか確認をします。実行する場合は「OK」をクリックします。



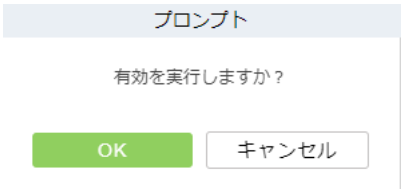

④ **時刻同期**

顔認証デバイスの時刻を遠隔から同期（修正）します。顔認証デバイスがオンラインである必要があります。同期する場合は「同期」をクリックします。



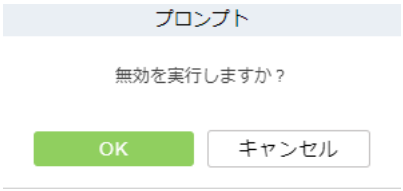
⑤ **有効**

次の⑦で一時的に顔認証デバイスの利用を「無効」に設定またはデバイス交換を行った場合、「有効」にします。




⑥ **無効**

利用中の顔認証デバイスを一時的に「無効」に設定して使用不可にます。利用再開は⑥を参照してください。




⑦ **全データをデバイスに同期**

顔認証デバイスの交換後など、管理ソフト側からグループ登録などの設定情報を同期します。同期する場合は「全データをデバイスに同期」をクリックし、同期する情報を選択して「同期」をクリックします。必要な場合、「同期する前にデバイスのデータを削除してください」にチェックを入れ、最後に「OK」をクリックします。

※ユーザー登録またはデバイス交換を実施した場合、「全データをデバイスに同期」を実行してください。




**＜同期する設定内容は以下の通りです＞** ※（ ）は当社または本製品はサポート対象外です。

| | | |
|---|---|---|
| アクセス権、ユーザー情報 | タイムゾーン（休日） | ドアパラメータ |
| アンチ・パスバック | （ファーストユーザー解錠） | （マルチパーソン） |
| リンケージ | （バックグラウンド認証オプション） | （補助入力設定） |
| 認証モードルール | | |

## 6. セットアップ

顔認証デバイスの一部の機能を遠隔から設定できます。



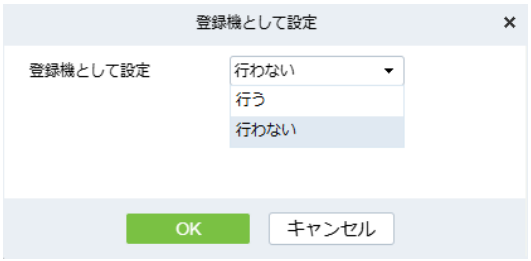

| 設定項目 | 内容 |
|---|---|
| デバイスタイムゾーン設定 | 当社または本製品ではサポート対象外です。 |
| 登録機として設定 | 顔認証デバイスからユーザー登録ができるように設定します。 |
| 指紋閾値変更 | 当社または本製品ではサポート対象外です。 |
| 拡張パラメーター設定 | 顔・アクセスの各種パラメーターを設定します。 |
| NTP サーバー設定 | 当社または本製品ではサポート対象外です。 |
| デバイスの交換 | 登録デバイスを他のデバイスと交換します。 |
| リソースファイルのアップロード | 当社または本製品ではサポート対象外です。 |

### ① デバイスタイムゾーン設定

当社または本製品ではサポート対象外です。

### ② 登録機として設定

顔認証デバイス側でユーザー登録するためには、「登録機」として設定する必要があります。登録機として設定する場合は「登録機として設定」をクリックします。「行う」または「行わない」を選択し、設定情報を保存する場合は「OK」をクリックします。




登録機として設定された顔認証デバイスは、登録機の項目で「 」と表示されます。




### ③ 指紋閾値変更

当社または本製品ではサポート対象外です。

### ④ 拡張パラメーター設定

顔パラメーターと、アクセスパラメーター（本製品ではサポート対象外）を「行う／行わない」で設定します。




| 設定項目 | 内容 |
|---|---|
| 体温検知パラメーター | 本製品ではサポート対象外です。 |
| マスク検知パラメーター | マスク検知を有効にします。 |
| 未登録ユーザー通過 | 未登録ユーザーの通過を許可します。 |
| 外部トリガーアラーム | 外部トリガーアラームを有効にします。 |

※詳細設定は、顔認証デバイスの「メインメニュー」→「システム設定」→「保護管理」で設定します。設定については「10.4 システム設定」を参照してください。

### ⑤ NTP サーバー設定

当社または本製品ではサポート対象外です。（顔認証デバイス側で設定をします）

### ⑥ デバイスの交換

登録されている顔認証デバイスを他の顔認証デバイスと交換します。交換するデバイスは同一のモデルである必要があります。交換前に「4 顔認証デバイスの導入（初期設定）」で顔認証デバイスの初期設定をしてください。

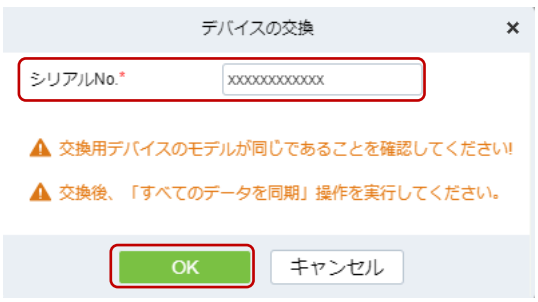
- 交換するデバイスを選択し、「セットアップ ＞ デバイスの交換」をクリックします。




- 新たに設置する顔認証デバイス管理用のシリアル No（本体背面に表示されている SN：を参照）を入力し「OK」をクリックします。

**＜顔認証デバイス管理用のシリアル No の位置＞**





- プロンプトが表示されますので「OK」をクリックします。




- 交換後の新しい顔認証デバイスを選択して「デバイス管理 ＞ 有効」をクリックします。



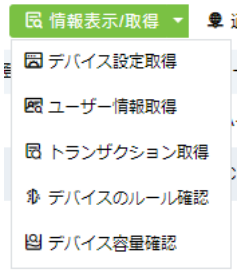

※ユーザー登録またはデバイス交換を実施した場合、「全データをデバイスに同期」を実行してください。
※交換前のデバイスは電気・機械的な故障が無ければ、顔認証デバイスをリセット（初期化）して再利用できます。

### ⑦ リソースファイルのアップロード

当社または本製品ではサポート対象外です。

## 7. 情報表示/取得

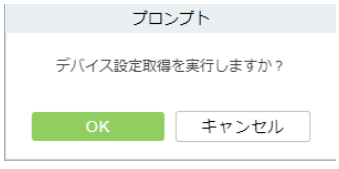
顔認証デバイスの各種データを取得することができます。




| 設定項目 | 内容 |
|---|---|
| デバイス設定取得 | 顔認証デバイスから設定情報を取得します。 |
| ユーザー情報取得 | 顔認証デバイスに登録されているユーザー情報を取得します。 |
| トランザクション取得 | 顔認証デバイスの各種記録を取得します。 |
| デバイスのルール確認 | リンケージなど、設定されたルールを遠隔で確認できます。 |
| デバイス容量確認 | 顔認証デバイスのデバイス容量を確認できます。 |

### ① デバイス設定取得

顔認証デバイスの設定情報を取得します。実行する場合は「OK」をクリックします。



### ② ユーザー情報取得

顔認証デバイス側に登録されているユーザー情報を取得します。取得する情報を選択し「開始」をクリックします。




### ③ トランザクション取得

顔認証デバイスの認証記録を取得します。取得する場合は、トランザクションの種類や有効期間を選択して「開始」をクリックします。



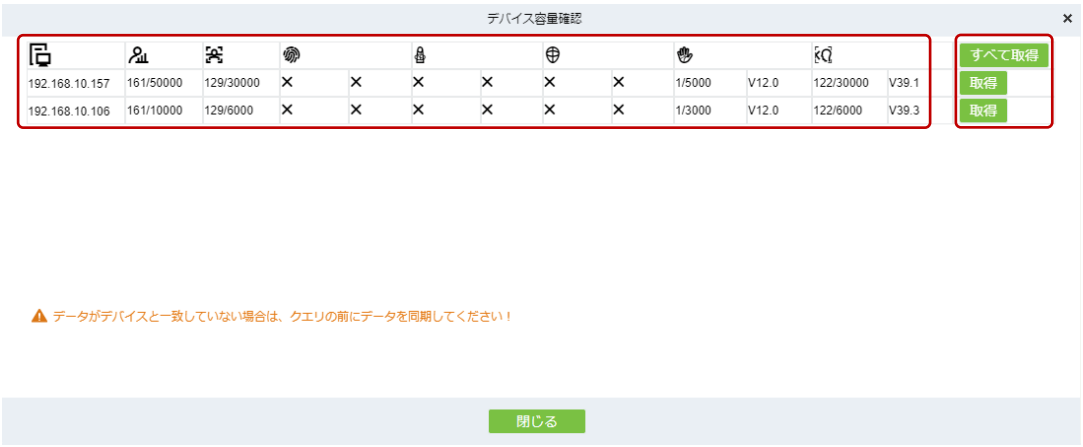

### ④ デバイスのルール確認

デバイスに設定されているアクセスレベルなどのルールを確認することができます。確認する場合は「設定済」のルールタイプをクリックすると「ルール詳細」に設定内容が表示されます。



### ⑤ デバイス容量確認

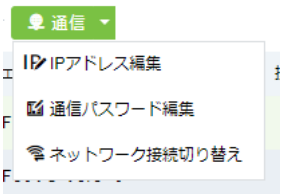
顔認証デバイスに保存された履歴や設定情報など、登録件数を遠隔から確認することができます。確認する場合は対象のデバイスを選択（複数選択可）し、「デバイス容量確認」をクリックします。次に「すべて取得」または各端末を個別に「取得」をクリックします。




※取得したデータがデバイスと一致していない場合は、①の「デバイス設定取得」で取得をしてください。

## 8. 通信 ※本機能は「詳細 UI」に切り替えてから利用してください。

顔認証デバイスの通信関連の設定を遠隔で行います。

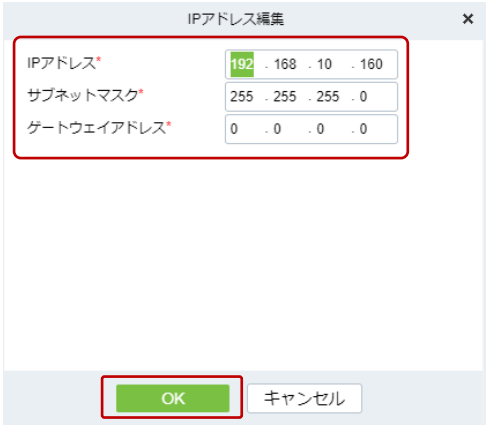



| 設定項目 | 内容 |
|---|---|
| IP アドレスの編集 | 管理ソフトから遠隔で IP アドレスを変更します。 |
| 通信パスワード編集 | 当社または本製品はサポート対象外です。 |
| ネットワーク接続切り替え | 当社または本製品はサポート対象外です。 |

### ① IP アドレス編集

「有線 LAN 接続」かつ「固定 IP アドレス」で運用している場合、管理ソフトから遠隔で IP アドレスの変更ができます。なお、IP アドレスの設定変更を実行するとデバイスは自動で再起動します。

固定 IP アドレスを変更する場合は「IP アドレス編集」をクリックし、新しい「固定 IP アドレス」、「サブネットマスク」、「ゲートウェイアドレス」を入力して「OK」をクリックします。デバイスが再起動します。



② **通信パスワード編集**

当社または本製品はサポート対象外です。

③ **ネットワーク接続切り替え**

当社または本製品はサポート対象外です。

## 9.16.2. I/O 拡張ボード

当社または本製品ではサポート対象外です。

## 9.16.3. ドア

顔認証デバイスと設置するドアを関連付けます。デバイス管理で登録されたデバイスが表示されます。ドアの制御には管理者パスワード（ユーザーパスワード）が必要になる場合があります。

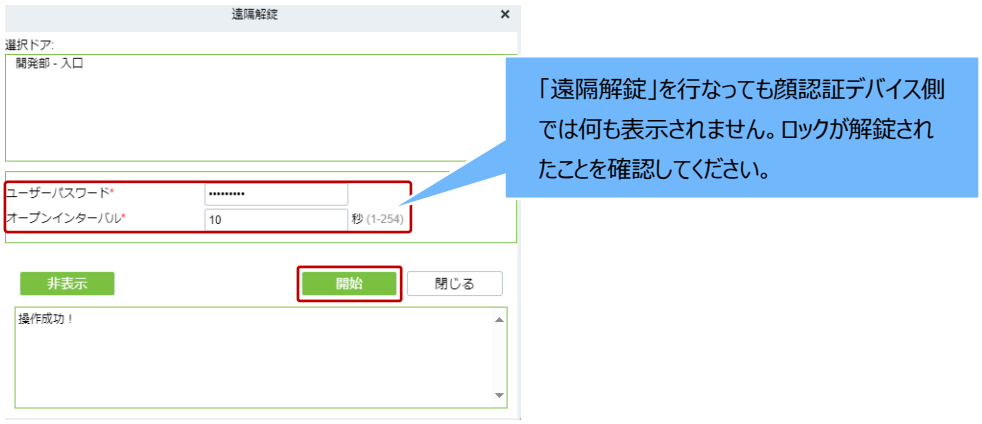



1. **更新**

登録済みの顔認証デバイス一覧を再取得します。再取得する場合は「更新」をクリックします。

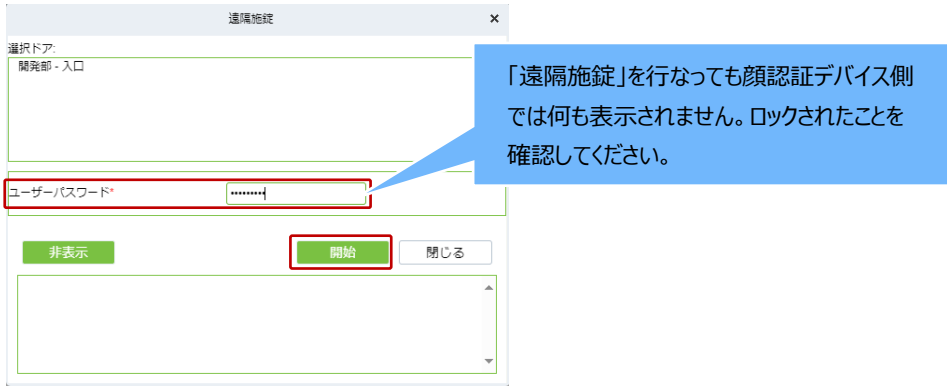
2. **遠隔解錠**

顔認証デバイスが電子錠などに接続している場合、管理ソフトから指定のドアの解錠を行います。遠隔解錠を行う場合は該当のドア名を選択し「遠隔解錠」をクリックします。管理ソフトの管理者パスワード（ユーザーパスワード）と解錠時間（オープンインターバル／初期値：５秒）を入力して「開始」をクリックします。



**3. 遠隔施錠**

顔認証デバイスが電子錠などに接続している場合、管理ソフトから指定のドアの施錠を行います。遠隔施錠を行う場合は該当のドア名を選択し「遠隔施錠」をクリックします。管理ソフトの管理者パスワード（ユーザーパスワード）を入力して「開始」をクリックします。




**4. 有効**

次の「5」で一時的にドアの動作・設定ををを「無効」にした場合、利用再開のため「有効」にします。

**5. 無効**

ドアの動作・設定を一時的に「無効」に設定して利用不可にします。利用再開は「4」を参照してください。

**6. アラームキャンセル**

ネットワーク未接続や顔認証デバイスの故障など、イベント発生で通知される各種アラームをキャンセルします。

**7. 遠隔解錠∞**

指定したドアを常時解錠に設定します。設定を無効にする場合は、次項 11 の「自動解錠タイムゾーン無効」を実行してください。

**8. ロックダウン有効**

指定した顔認証デバイスの認証を無効にします。認証することができなくなります。

※顔認証デバイス側では認証すると「失敗しました」と表示されます。

**9. ロックダウン無効**

「8」で設定した「ロックダウン有効」を「無効」にします。認証ができるようになります。

**10. 自動解錠タイムゾーン有効**

予めタイムゾーンで設定した時間帯で自動解錠タイムゾーンを有効にします。

**11. 自動解錠タイムゾーン無効**

自動解錠タイムゾーンを無効にします。

## 12. 操作

「ドア名」または「操作」アイコンをクリックします。ドアに関する設定が行えます。







| 設定項目 | 内容 |
|---|---|
| デバイス名* | デバイス管理で登録した名前を表示します。 |
| ドア名* | デバイス名に割り当てるドア名を設定します。 |
| 認証モード* | 認証モードを選択します。 |
| 操作間隔* | 本製品ではサポート対象外です。 |
| アンチ・パスバック期間 | 本製品ではサポート対象外です。 |
| 非常パスワード | 顔認証デバイス側の防犯パスワードです。 |
| 緊急パスワード | 緊急で解錠する必要がある時に使用するパスワードです。 |
| ホストアクセスステータス | 入退室管理のデータを外部連携する場合、ホストステータスで設定された値を外部出力します。 |
| アラーム無効 | ドアのアラーム表示を無効します。 |
| ドア番号* | 設定値を表示します。 |
| 有効タイムゾーン* | 原則、変更しないようにしてください。アクセス可能な時間はグループに所属するユーザー単位または部署単位で設定します。 |
| 解錠時間* | 認証成功時の解錠時間を設定します。 |
| ドアセンサータイプ* | 電子錠など外部機器の接続方法を選択します。 |
| ドアセンサー遅延 | ドアセンサータイプを選択した場合に設定します。ドアが開いた後の開放時間を設定します。ドアが「ノーマルオープン」でない時、ドアが解錠時点から、本設定時間を経過するとアラームが始まり、ドアが閉まるとアラームが停止します。 |
| 自動解錠タイムゾーン | ドアが常時開いている時間帯を選択します。 |
| マルチパーソン認証間隔* | 当社または本製品ではサポート対象外です。 |
| スレーブステート | 当社または本製品ではサポート対象外です。 |
| この設定を次の場所にコピー | 他のドアへ同一設定内容を保存します。 |

*印は必須項目です。

1. **デバイス名**
   デバイス管理で登録した顔認証デバイスに設定されているデバイス名を表示します。

2. **ドア名（初期値：デバイス登録時の IP アドレス＋枝番）**
   顔認証デバイスを設置する出入口のドア名を割り当てます。

3. **認証モード（初期値：自動識別）**
   デバイス（ドア）で実施する認証方式を選択します。2 つ以上の生体情報で認証するマルチモーダル認証や登録情報の組み合わせで認証する多要素認証を選択することができます。

4. **操作間隔**
   本製品はサポート対象外です

5. **アンチ・パスバック期間**
   本製品はサポート対象外です

6. **非常パスワード**
   意図しない解錠を管理者へ知らせるためのパスワードです。非常パスワードが使用された場合、リアルタイムモニタリングなどでアラームを確認することができます。

   顔認証デバイス側の設定では「アクセスコントロール」→「防犯オプション」→「防犯パスワード」に該当します。顔認証デバイス側で設定していても管理ソフト上で設定した場合、管理ソフト側で設定した情報が優先（デバイスに同期）されます。

7. **緊急パスワード**
   緊急でドアの解錠が必要な場合、管理者が使用します。リアルタイムモニタリングには表示されますが、アラームモニタリングには表示されません。

8. **ホストアクセスステータス**
   入退室管理の外部連携において、顔認証デバイスの入・出を出力するためには設定が必要です。

9. **アラーム無効**
   ドアでアラームが発生した場合、リアルタイムモニタリングにアラーム音を「出す／出さない」を設定します。

10. **ドア番号**
    自動採番されるドアの管理番号です。

11. **有効タイムゾーン**
    アクセス（認証）可能な時間帯をドア単位で設定します。原則、変更しないようにしてください。アクセス可能な時間はグループに所属するユーザー単位または部署単位で設定します。

**12. 解錠時間（初期値：5 秒）**

電子錠など、外部機器の解錠時間を設定します。例えば、値を「5」秒に設定した場合、認証後 5 秒間ドアが解錠された状態になります。

**13. ドアセンサータイプ**

電子錠など、外部機器の接続タイプを設定します。通常はノーマルクローズを選択し、認証時に接点を出力します。

**14. ドアセンサー遅延**

「⑬」を選択した場合、ドアが開いた後の開放時間を設定できます。解錠時点から、設定した時間を経過するとアラームが発生し、施錠されるとアラームが停止します。

**15. 自動解錠タイムゾーン**

自動解錠をする時間帯を選択します。選択できる時間帯は「アクセスルール」→「タイムゾーン」で設定した内容です。

**16. マルチパーソン認証間隔**

当社または本製品はサポート対象外です。

**17. スレーブステート**

当社または本製品はサポート対象外です。

**18. この設定を次の場所にコピー**

同一内容の設定を他のドアに反映します。

### 9.16.4. リーダ

当社または本製品ではサポート対象外です。

### 9.16.5. 補助入力

当社または本製品ではサポート対象外です。

### 9.16.6. 補助出力

当社または本製品ではサポート対象外です。

### 9.16.7. イベントタイプ

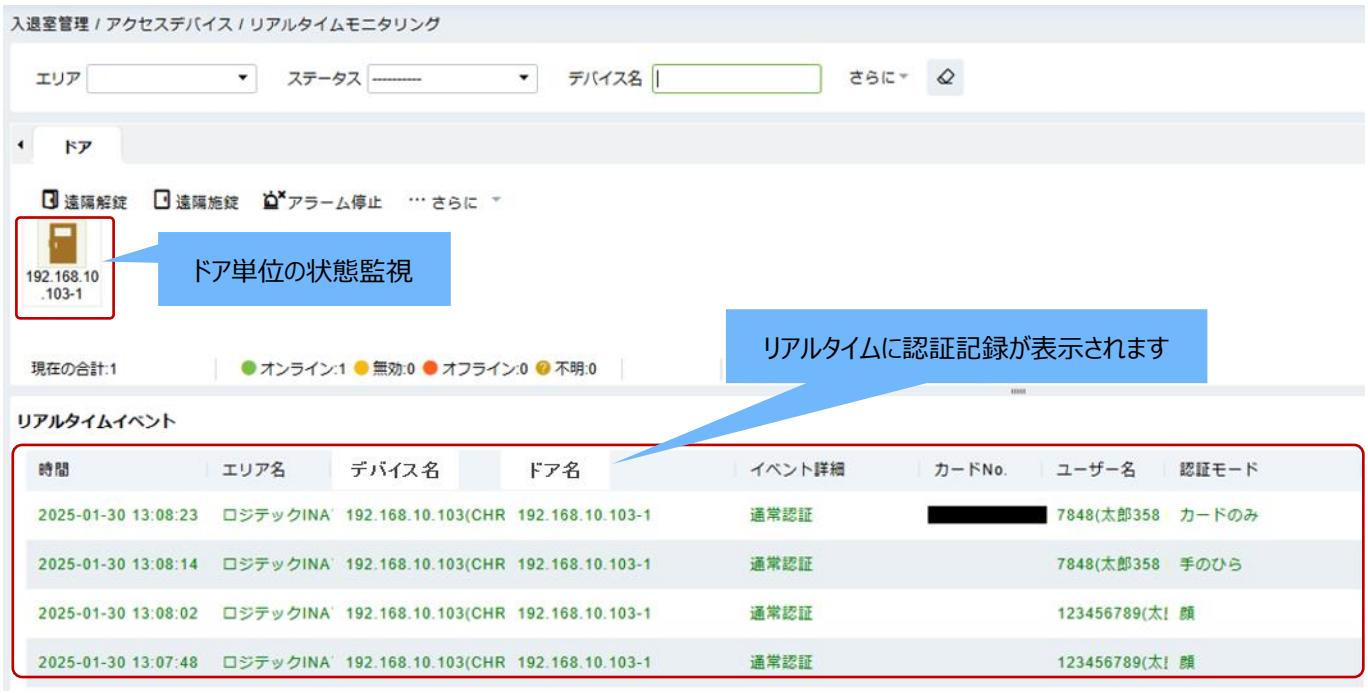
当社または本製品ではサポート対象外です。

### 9.16.8. サマータイム

当社または本製品ではサポート対象外です。

## 9.16.9. リアルタイムモニタリング

設置された顔認証デバイスをドア単位で認証状況やデバイスの稼働状況を常時監視することができます。IC カード認証のみ未登録ユーザーが表示され、顔認証や掌認証およびパスワード認証による未登録ユーザー判定の表示はされません。リアルタイムモニタリングのページを離れるとリアルタイムイベントはクリアされます。本画面の表示中は 30 分無操作による強制ログアウトはされません。※アラームモニタリングとは連動していません。




**例）タンパーアラーム（イベント）発生**

マウスのカーソルをドアのアイコンに移動するとポップアップメニューが表示され、上記の操作を迅速に行うことができます。「ドア」アイコンをマウスオーバーするとステータスを確認できます。「アラーム」の原因を確認し、アラームを一時停止する場合は「アラームキャンセル」をクリックして管理用パスワード（ユーザーパスワード）を入力します。但し、完全にアラームを停止する場合は次項のアラームモニタリングで「アラーム確認」をします。

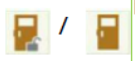
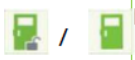
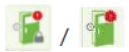
※タンパーアラームとは、顔認証デバイスが固定用ブラケット（フロアスタンド使用時にも使用する共通ブラケット）から取り外された時に通知されます。



**＜ドア操作メニュー＞**

| メニュー | 説明 |
|---|---|
| 遠隔解錠／遠隔施錠 | ドアを制御するには、対象ドアにマウスカーソルを合わせ、ポップアップダイアログボックスで「遠隔解錠」、「遠隔施錠」をクリックします。「遠隔解錠」では、ドアの開放時間を設定できます(デフォルトは 5 秒です)。 |
| ロックダウン有効 | 指定した顔認証デバイスの認証を無効にします。認証することができなくなります。<br>※顔認証デバイス側では認証すると「失敗しました」と表示されます。 |
| ロックダウン無効 | 「ロックダウン有効」を「無効」にします。認証ができるようになります。 |
| アラームキャンセル | 一時的にアラームをキャンセルする場合は「アラームキャンセル」をクリックします。恒久的にアラームを止めるには「アラームモニタリング」で「アラーム確認」の処理をします。 |
| 遠隔解錠（常時） | デバイスを遠隔で常時開くように設定します。 |
| 自動解錠タイムゾーン有効 | 予めタイムゾーンで設定した時間帯で自動解錠タイムゾーンを有効にします。ドアを閉じるには、最初に「自動解錠タイムゾーン無効」してから、「遠隔施錠」 を選択します。 |
| 自動解錠タイムゾーン無効 | 自動解錠タイムゾーンを無効にします。 |
| ドアイベントクエリ | ドアで発生したイベント一覧を表示します。 |

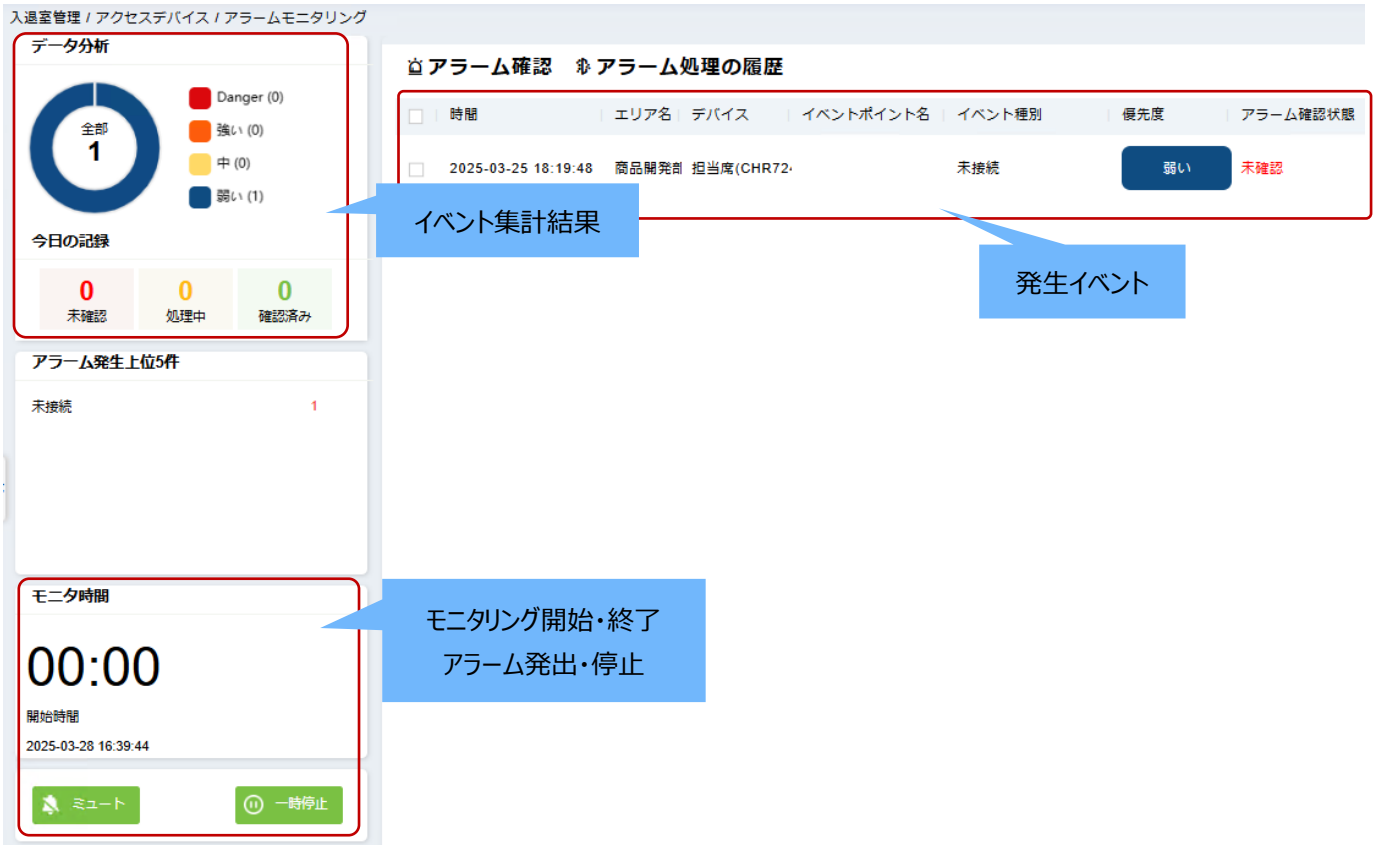
**＜アイコン表示の種類と状態の説明＞**

| アイコン | 状態 | アイコン | 状態 |
|---|---|---|---|
|  | デバイスが無効になっています |  | デバイスがオフライン状態です |
|  | ドアの開閉センサーなし<br>リレーが閉じている／リレーなし |  | ドアの開閉センサーなし<br>リレーが開いている／リレーなし |
|  | ドアが閉まっている<br>リレーが閉じている／リレーなし |  | ドアが閉まっている<br>リレーが開いている／リレーなし |
|  | ドア開いている<br>リレー閉じている／リレーなし |  | ドア開いている<br>リレー開いている／リレーなし |
|  | ドア開いてる＋アラーム有<br>リレー閉じている |  | ドアが開いている＋アラーム有<br>リレー開いている |
|  | ドア開放時間超過＋アラーム有<br>リレー閉じている／リレーなし、電磁ロック：オープン |  | ドア開放時間超過＋アラーム有<br>リレー開いている／リレーなし、電磁ロック：オープン |
|  | ドア開放時間超過＋アラーム有<br>リレー閉じている＋電磁ロック：クローズ |  | ドア開放時間超過＋アラーム有<br>リレー開いている＋電磁ロック：オープン |
|  | ドア閉じている＋アラーム有<br>リレー閉じている／リレーなし |  | ドア閉じている＋アラーム有<br>リレー開いている／リレーなし |
|  | ドアセンサーなし＋アラーム有<br>リレー閉じている |  | ドアセンサーなし＋アラーム有<br>リレー開いている |
|  | ドア開放時間超過＋アラーム有<br>リレーなし＋電磁ロック閉じている |  | ドアは施錠されている |
|  | ドア（電磁ロック）とデバイス間の通信異常 | | |

**注：**リレーがない場合は、「リレーステータスの確認」機能をサポートしていません。

## 9.16.10. アラームモニタリング

設置している顔認証デバイスで発生したイベントを一元管理できます。通信不良などのイベントが発生すると集計され、イベント毎に対応記録を保存して管理することができます。




### 1. アラーム確認

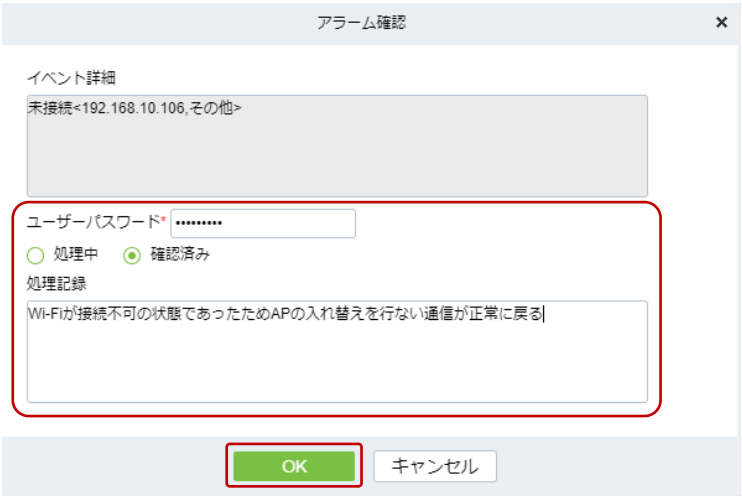
発生したイベントをリアルタイムに表示し、対応履歴などを記録することでアラームを止めることができます。

① イベントを選択（チェック）して「アラーム確認」をクリックします。アラーム確認を行わない場合、「アラーム確認状態」は「未確認」の表示のままとなります。

※イベントを複数選択することはできません



② イベント毎に対応履歴を残すことができます。管理パスワード（ユーザーパスワード）を入力し、対応区分「処理中」または「確認済み」を選択し、必要に応じて処理記録を残します。内容を保存する場合は「OK」をクリックします。




## 2. モニタ時間

本機能でアラームモニタリングを実施することでアラーム発生時に警報音を鳴らすことができます。

① モニタリングを開始するには、イベント発生時にアラームを鳴らす場合は「ミュート」を解除し、「一時停止」をクリックしてモニタリングを開始します（モニタ時間をカウントアップします）。




② アラームを停止します。アラームを停止するには、「アラーム確認」を実施する必要があります。アラーム音だけを一時的に停止したい場合は「ミュート」をクリックします。完全に停止する場合は「アラーム確認」の実施が必要です。

## 9.16.11. マップ

各フロアのレイアウト上に設置した顔認証デバイス（ドア）をグラフィカルにモニタリングすることができます。IC カード認証のみ未登録ユーザーが表示され、顔認証や掌認証およびパスワード認証による未登録ユーザー判定の記録は表示されません。ビル一棟の各フロアに設置された顔認証デバイスを管理したり、エリア内に所属するフロア上の顔認証デバイスを管理したりすることで、視覚的に顔認証デバイスをモニタリングすることができます。

※アラームモニタリングとは連動していません。




| 設定項目 | 内容 |
|---|---|
| 更新 | 表示されているページを最新の状態に更新します。 |
| 新規 | マップを新規に登録します。 |
| 編集 | 登録済みのマップを編集します。 |
| 削除 | 登録済みのマップを削除します。 |
| ポジション保存 | 配置したドア（アイコン）を保存します。 |
| 全ドア | ドアを選択して図面上に配置します。 |
| ズームイン | マップの表示を拡大します。 |
| ズームアウト | マップの表示を縮小します。 |
| フルスクリーン | マップをフルスクリーン表示します。 |

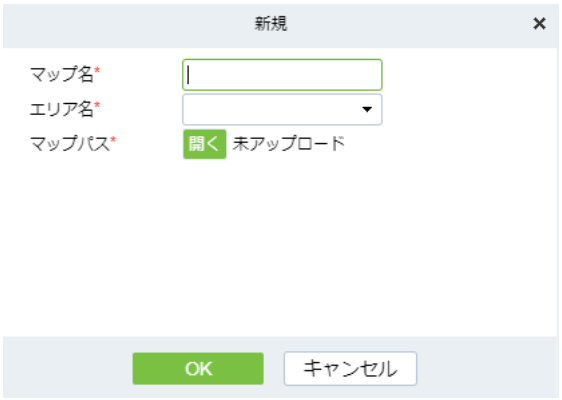
### 1. 更新

ページを最新の状態に更新します。

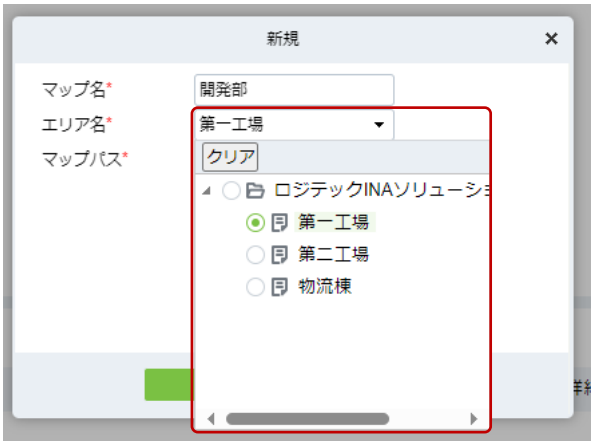
### 2. 新規

マップを新規に作成します。

① マップを新規に作成する場合、「新規」をクリックします。



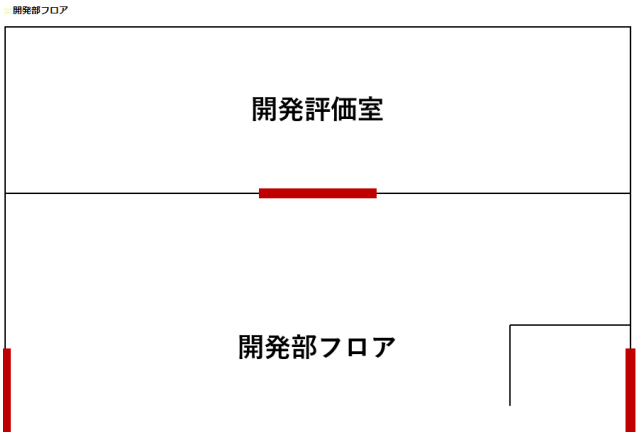

② マップ名（階数や部署名などお客様が管理し易い名称）を入入力します。次に、マップが存在するエリアをリストから選択します。最後に、マップ画像（PNG または JPEG／JPG）を選択します。




③ 入力・選択内容に問題が無いようでしたら最後に「OK」をクリックして保存ます。



マップ（例：開発フロア）が表示れていることを確認します。




### 3. 全ドア

マップ上にドアを配置します。

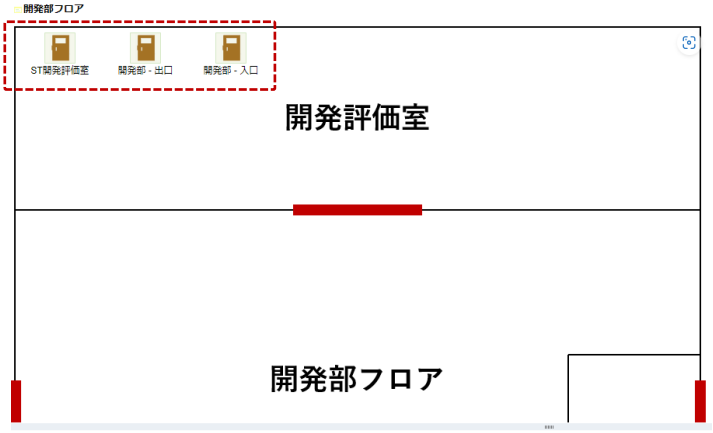
① 「全ドア」をクリックて、マップ上に配置するドアを選択します。



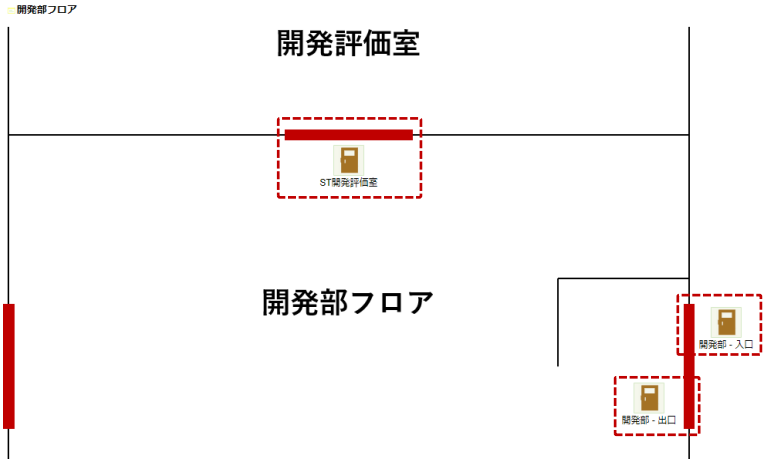

② 選択したドアを保存するには「OK」をクリックします。



③ 前項で選択したドア（アイコン）がマップ上に表示されます。ドア（アイコン）をドラッグ＆ドロップで動かして設置場所へ配置します。



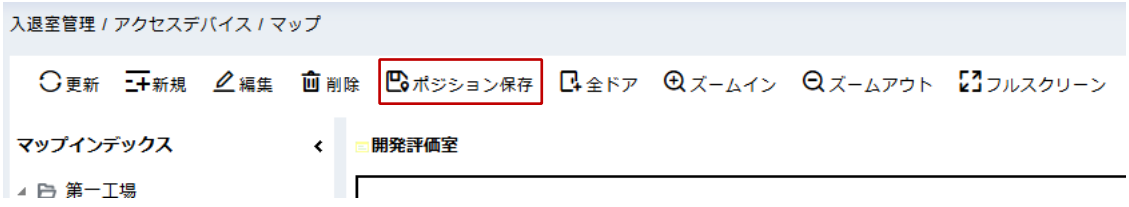

**<ドア（アイコン）配置後>**




※ドア（アイコン）上を右クリックすると「削除」することができます。




④ 配置に問題がなければ、「ポジション保存」をクリックして保存します。



**4. ポジション保存**

マップ上に配置した顔認証デバイスを保存します。

**5. 編集**

登録済みのマップ情報（名称・エリア・マップ画像）を編集します。

**6. 削除**

登録済みのマップ情報を削除します。

**7. ズームイン**

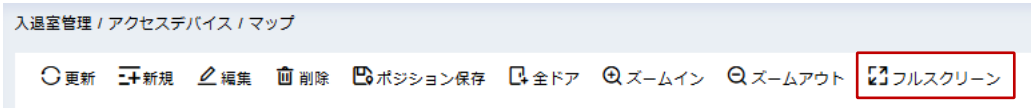
マップを拡大します。

**8. ズームアウト**

拡大（ズームイン）したマップを元に戻します。

**9. フルスクリーン**

マップを管理ソフト上でフルスクリーン表示します。フルスクリーンを停止する場合は「フルスクリーン終了」をクリックします。



# 9.17. アクセスルール

入退室管理において、各種ルールの設定をします。

## 9.17.1. タイムゾーン

顔認証デバイスに対してアクセス（認証可能）な時間帯を割り当てることができます。初期値では「24 時間有効」が選択できます。




### 1. タイムゾーン登録 ※設定を省略することができます

タイムゾーン（アクセス可能時間）を任意の時間帯で設定して顔認証デバイスに対して割り当てることができます。
例は、「月曜日～金曜日」まで「７時 00 分～23 時 59 分」を認証可能な時間帯として追加する方法です。

① 「タイムゾーン登録」をクリックします。




② タイムゾーン名（重複 NG）を入力します。デバイスに割り当てる時に選択肢として表示される名称のため、アクセス可能な時間帯が分かり易い名称にすると管理がし易くなります。例では「平日／07：00～23：59」としています。



③ アクセス可能な時間帯を入力します。例では「月曜日～金曜日」まで「７時 00 分～23 時 59 分」をアクセス可能な時間帯として設定しています。毎日同じ時間帯を設定したい場合、「月曜日の設定を、他の平日にコピー」へチェックを入れると自動コピーされます。設定を保存する場合は「OK」をクリックします。




※夜勤など「日またぎ」の設定が必要な場合、翌日の開始時間へ 0:00 以降の時間を設定します。

（例）




④ 追加をしたタイムゾーンが一覧に表示されていることを確認します。



### 2. 削除

タイムゾーンの操作項目「削除」アイコンをクリックします。



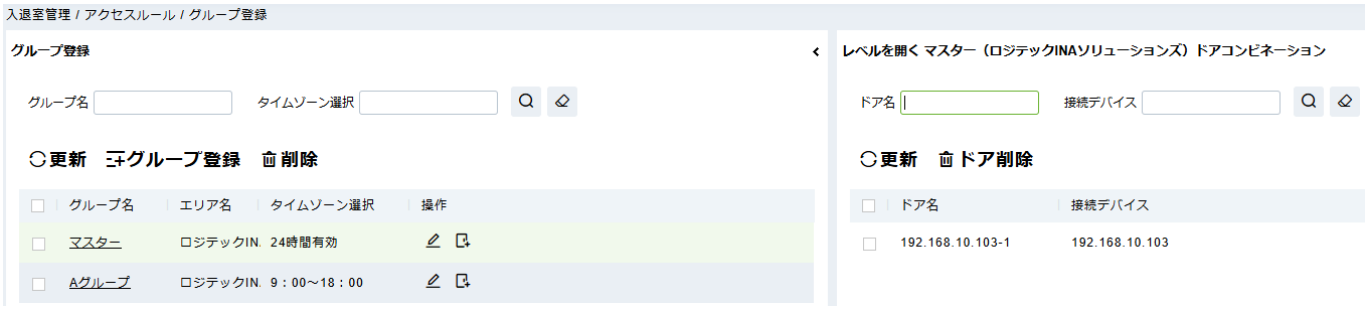

## 9.17.2. 休日

当社または本製品ではサポート対象外です。

## 9.17.3. グループ登録

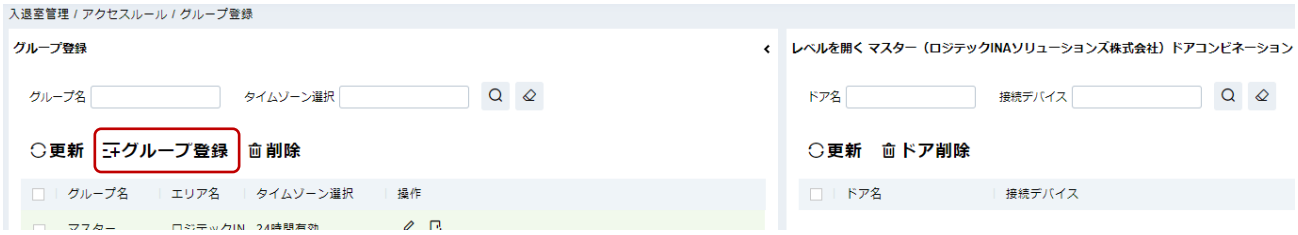
エリア（管理する拠点または部屋など）、タイムゾーン（アクセス可能な時間）、ドア（顔認証デバイス）で 1 つグループ（アクセス権限グループ）を作成します。エリア毎にアクセス可能な時間帯が異なる場合、予めタイムゾーンを作成して、エリア毎にタイムゾーンを割り当てて作成します。最後に作成したグループをユーザーまたは部署に割り当てます（9.17.4 アクセス設定）。



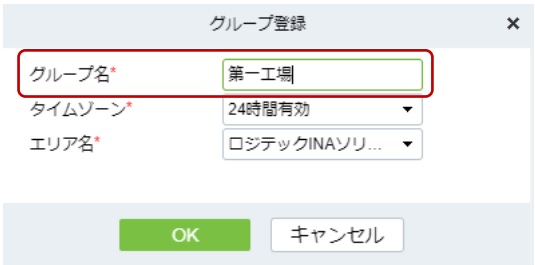




### 1. グループ登録

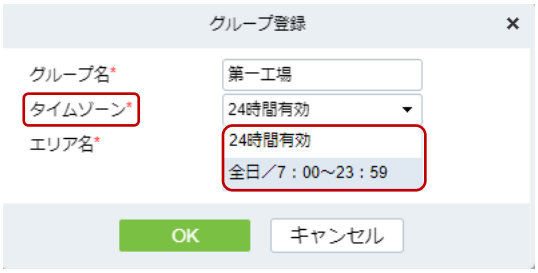
① 「グループ登録」をクリックします。



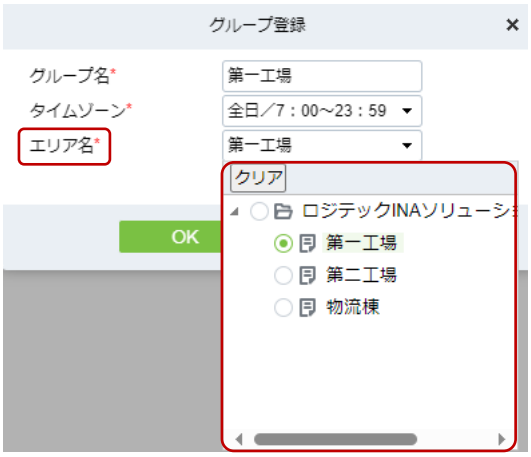

② グループ名を入力します。例はエリアと同じ「第一工場」としています。これにより、エリア毎に複数のタイムゾーンを設定している場合、エリアに対応するタイムゾーンの管理がし易くなります。



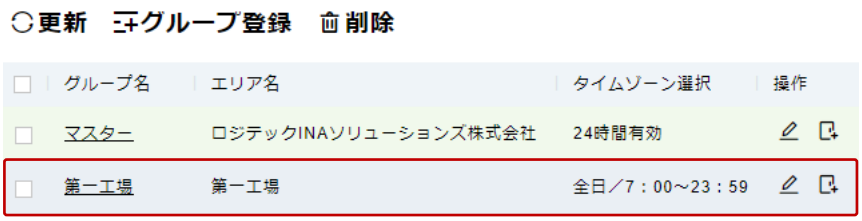
③ タイムゾーンを選択します。前項の「タイムゾーン」で新規に追加したタイムゾーンも選択できるようになります。



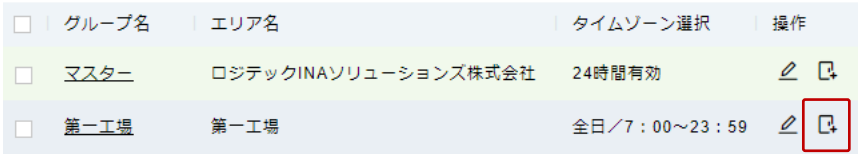

④ 前項③で選択したタイムゾーンを適用するエリア（拠点）を選択します。例ではレベル名に入力した「第一工場」を選択しています。設定を保存する場合は「OK」をクリックします。




⑤ グループ名に新規に追加されていることを確認します。




⑥ 次に、グループ登録（管理拠点：エリア、認証可能な時間：タイムゾーン）を顔認証デバイス（ドア）に割り当てます。グループ名一覧の操作項目の「」をクリックします。



⑦ 予めデバイス登録とドア設定がされた顔認証デバイスが表示されます。割り当てたいドア名を「＞」で選択します。

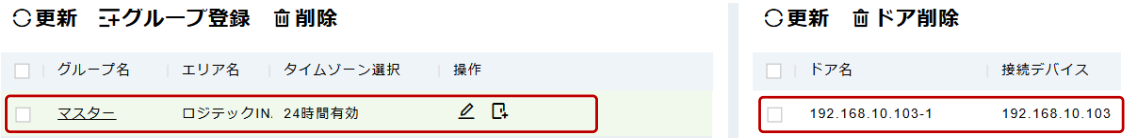
※ドア名の一覧に顔認証デバイスが表示されない場合、「デバイス管理」からデバイスの「エリア名」の設定を再確認してください。④で「第一工場」をエリアとして選択しているため、デバイスに割り当てられているエリアも「第一工場」である必要があります。




⑧ 設定する顔認証デバイスが選択できたら最後に「OK」をクリックします。エリアに紐づくデバイスが複数設置される場合は全てのデバイスを選択してください。




⑨ グループ名をクリックすると、割り当てられた顔認証デバイスが表示されることを確認します。



## 2. 削除

グループまたはグループに割り当てられたドアの削除をします。

① グループの削除

削除する「グループ名」を選択して「削除」をクリックします。削除しますか？と表示が出たら「OK」をクリックします。





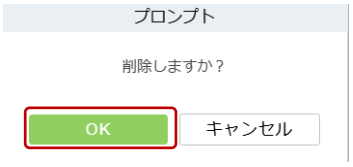


※グループを削除すると、グループに割り当てられたドアも同時に削除されます。

② ドアの削除

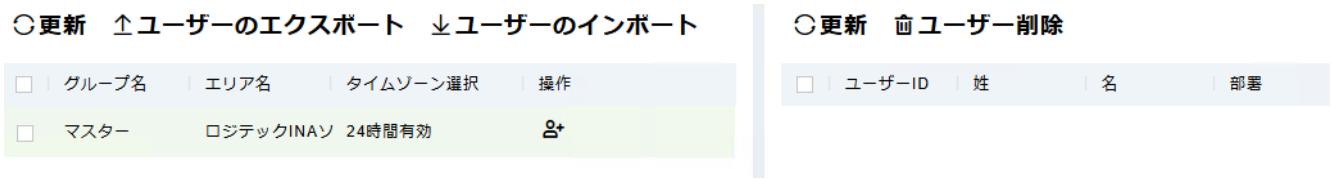
削除する「ドア名」を選択して「ドア削除」をクリックします。削除しますか？と表示が出たら「OK」をクリックします。



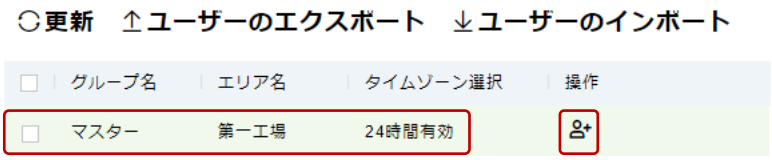
## 9.17.4. アクセス設定

タイムゾーンとエリアを登録ユーザーに割り当てます。これにより、管理する拠点（エリア）に設置された顔認証デバイス（ドア）で、割り当てたタイムゾーンで登録済みのユーザーがアクセス可能になります。




### 1. グループ（エリア及びタイムゾーン）をユーザーに割り当てる

① ユーザーを割り当てるグループを選択して「 」をクリックします。例では「グループ名：マスター／エリア名：第一工場」にユーザーを割り当てます。

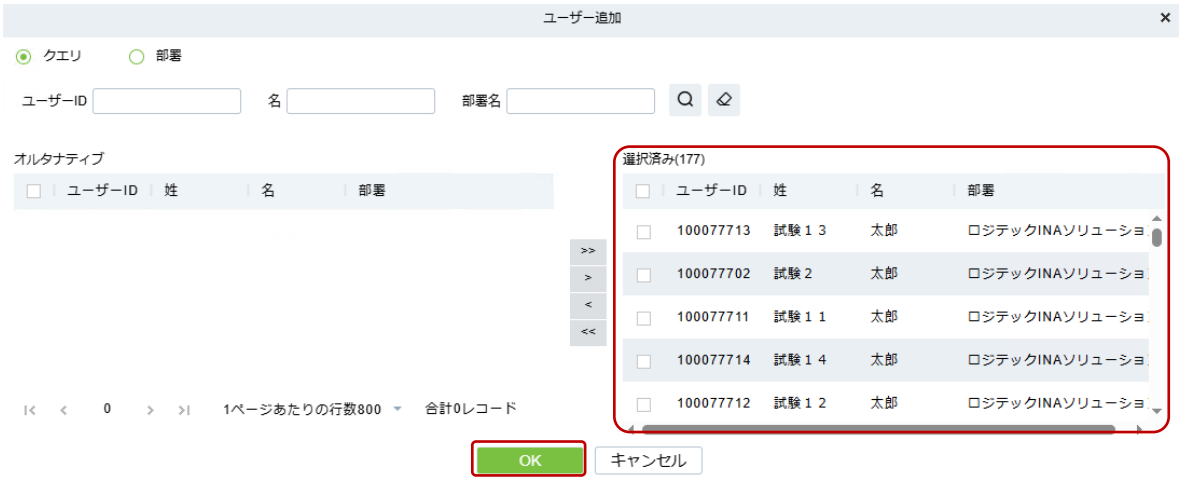



② ユーザーを選択して「＞」をクリックします。

※1 ページあたりの表示件数にご注意ください。一括選択は表示されているユーザーしか選択されません。



③　設定を保存する場合は「OK」をクリックします。




④　グループに対してユーザーが割り当てられたことを確認します。




※グループが複数存在する場合は必要に応じて本項の設定を繰り返します。

## 2.　削除

グループに割り当てたユーザーを削除します。削除しますか？と表示されたら「OK」をクリックします。



## 9.17.5. ユーザー設定

当社または本製品ではサポート対象外です。

## 9.17.6. 部署設定

部署単位でグループを割り当てることができます。部署に所属するユーザーへ各種権限が自動的に割り当てられます。

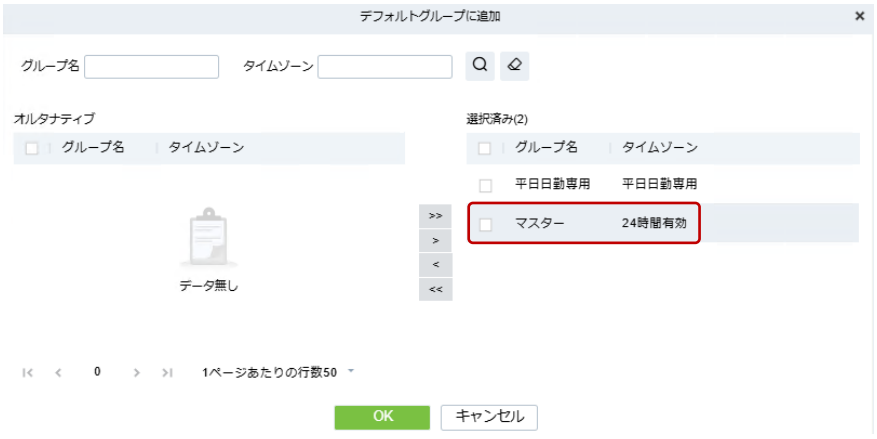



**1. 操作**

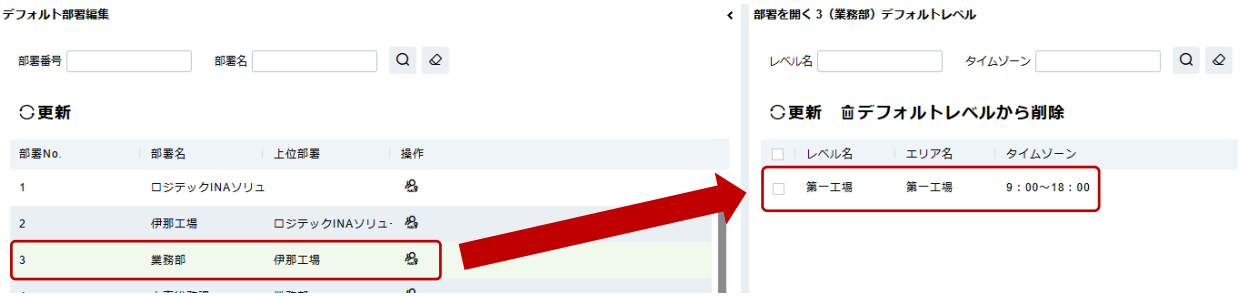
① 部署（例：業務部）をデフォルトレベルに追加します。予め登録されたレベル・タイムゾーンを選択します。




② 部署（例：業務部）に対して、レベル名「マスター」のアクセス可能時間「24 時間有効」を選択します。最後に「OK」をクリックします。



③ 部署（例：業務部）に対して、デフォルトのレベルが割り当てられていることを確認します。




## 9.17.7. インターロック

当社または本製品ではサポート対象外です。

## 9.17.8. リンケージ

動作条件に応じてメール通知や電子錠などとの連携を制御*することができます。1 つのドア（デバイス）に複数のリンケージ（動作条件）を設定することができます。本設定を有効にするためには、外部の電子錠などの連携機器や送信メールサーバーの設定がされている必要があります。

| 注意事項 | ***リンケージの設定により、顔認証デバイスは動作条件により通常設定とは異なる動作・設定に変更されます。これにより、設定を誤ってしまうと意図しない動作により入退室管理の運用ができなくなります。設定する際は十分注意をしてください。万が一、意図しない動作になってしまった場合は、リンケージの削除及び顔認証デバイスのリセットをし、最初から設定をやり直してください。** |
|---|---|




**<リンケージトリガー条件一覧>**

| 条件 | 内容 |
|---|---|
| 通常認証 | 通常の各種認証時を条件に通知または接点動作を制御します。 |
| 自動解錠中認証 | 自動解錠中に認証されたことを条件に通知または接点動作を制御します。 |
| ファーストユーザー解錠 | ファーストユーザーに指定された方が認証したことを条件に通知または接点動作を制御します。 |
| マルチパーソン認証 | 当社または本製品はサポート対象外です。 |
| 非常パスワード認証 | ドアに設定された緊急パスワードが入力されたことを条件に通知または接点動作を制御します。 |
| 自動解錠タイムゾーン | 自動解錠のアクセス時間になったことを条件に通知または接点動作を制御します。 |
| アラームキャンセル | 何らかの理由でアラームがキャンセルされたことを条件に通知または接点動作を制御します。 |
| 操作間隔が短い | デバイスの操作間隔が短くエラーが発生したことを条件に通知または接点動作を制御します。 |
| 無効タイムゾーン認証 | 無効なアクセス時間に認証されたことを条件に通知または接点動作を制御します。 |

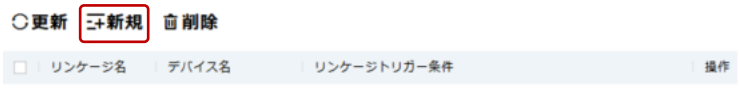
| | |
|---|---|
| 不正タイムゾーン | 設定されたタイムゾーン以外のアクセスがあった場合に制御します。 |
| アクセス拒否 | 当社または本製品はサポート対象外です。（ビジター管理機能） |
| アンチ・パスバック | 入る時に認証せずに出る時に認証した場合を条件に通知または接点動作を制御します。 |
| 未登録ユーザー | IC カード認証を条件に通知または接点動作を制御します。 |
| 開扉タイムアウト | 指定時間以上扉が開いていたことを条件に通知または接点動作を制御します。 |
| 有効期限切れユーザー | 特定のユーザーで認証有効期限切れを条件に通知または接点動作を制御します。 |
| 無効タイムゾーン（解錠スイッチ） | 退室ボタンが押され、ドアのタイムゾーンが無効になった場合を条件に通知または接点動作を制御します。（無効＝退室ボタンを使用する設定されているタイムゾーンに関わらず解錠します） |
| 自動解錠中施錠失敗 | 本人認証後自動解錠中にユーザーが通行しているため施錠ができない場合を条件に通知または接点動作を制御します。 |
| アクセスが無効になっています | アクセス権限が無効になっていることを条件に通知または接点動作を制御します。 |
| 認証モードエラー | 認証方式でエラーが発生したことを条件に通知または接点動作を制御します。 |
| Wiegand フォーマットエラー | 当社または本製品はサポート対象外です。 |
| マルチパーソン認証失敗 | 当社または本製品はサポート対象外です。 |
| ドア施錠 | ドアの施錠を条件に通知または接点動作を制御します。 |
| 不正タイムゾーン中解錠スイッチ | アクセス可能時間外の解錠を条件に通知または接点動作を制御します。 |
| ハイボディ – アクセスが拒否されました | 当社または本製品はサポート対象外です。温度測定結果で高温によるアクセス拒否が発生した場合を条件に通知または接点動作を制御します。 |
| マスクなし – アクセス拒否 | マスク未着用を条件に通知または接点動作を制御します。 |
| 無効な QR コード | 当社または本製品はサポート対象外です。 |
| QR コードの有効期限が切れました | 当社または本製品はサポート対象外です。 |
| 非常解錠アラーム | 非常パスワードを使用して解錠され、解錠アラームが発生した場合を条件に通知または接点動作を制御します。 |
| 強制解錠 | 強制解錠（管理ソフトと顔認証デバイスが正常動作し、それぞれから解錠操作がおこなわれていないにも関わらず解錠を検知した場合）を条件に通知または接点動作を制御します。 |
| ドア正常開扉 | アクセスルール通りの開扉を条件に通知または接点動作を制御します。 |
| ドア正常閉扉 | アクセスルール通りの閉扉を条件に通知または接点動作を制御します。 |
| 解錠スイッチ解錠 | 退室ボタンによる解錠を条件に通知または接点動作を制御します。 |
| 自動解錠タイムゾーン終了 | 自動解錠タイムゾーンの終了を条件に通知または接点動作を制御します。 |
| 管理者解錠 | 管理者による解錠を条件に通知または接点動作を制御します。 |
| 解錠スイッチトリガー（施錠無し） | 退室ボタンは動作し接点出力されても解錠しない（ロック解錠なし）場合を条件に通知または接点動作を制御します。 |
| ベル鳴動 | ベルが設定の時間になることを条件に通知または接点動作を制御します。 |
| デバイス呼び出し | 当社または本製品はサポート対象外です。 |
| 通話が終了しました | 当社または本製品はサポート対象外です。 |
| 補助入力イベント | 当社または本製品はサポート対象外です。 |
| 不正タイムゾーン中補助入力 | 当社または本製品はサポート対象外です。 |
| 補助入力切断 | 当社または本製品はサポート対象外です。 |
| 補助入力短絡 | 当社または本製品はサポート対象外です。 |
| デバイスイベント | 当社または本製品はサポート対象外です。 |
| タンパーアラーム | 顔認証デバイスが壁掛けアタッチメントから取りはずされたことを条件に通知または接点動作を制御します。 |

## 1. 更新

登録されたリンケージのリストを最新の状態に更新します。登録直後にリスト表示されない場合にクリックします。

## 2. 新規

① 条件に応じた通知やアクションを登録する場合は「新規」をクリックします。




② リンケージ名を入力します。




③ デバイスを選択します。




④ リンケージを設定したいドア（デバイス）を選択します。（例：開発部 – 入口）

※デバイス名は設置場所を設定しておくと管理がし易いです



⑤ 選択したドア（デバイス）で問題がなければ「OK」をクリックします。

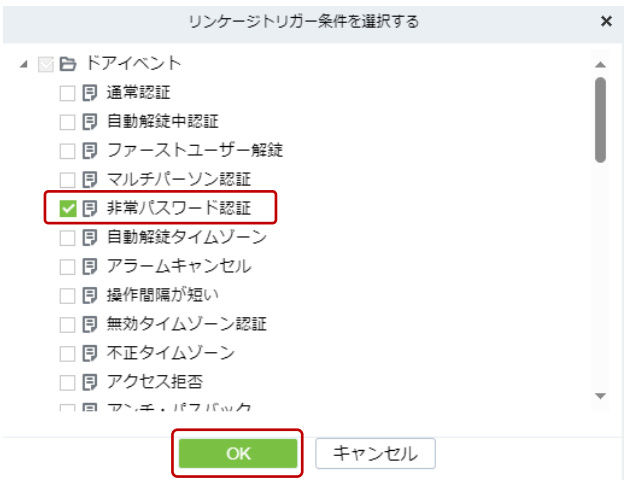



⑥ リンケージトリガー条件を追加します。「追加」をクリックします。

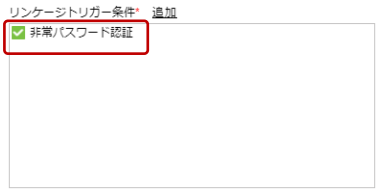



⑦ 「リンケージトリガー条件一覧」を参照し、トリガー条件（例：非常パスワード認証）を選択します。設定した条件を保存する場合は「OK」をクリックします。

※ドアイベント内、補助入力イベント内（サポート対象外）、デバイスイベント内で複数選択可



⑧ リンケージトリガー条件が追加されていることを確認します。




⑨ 「入力ポイント」を選択（例：開発部 － 入口）します。




⑩ アクションを選択します。接点制御の場合は「出力」タブ、メール通知の場合は「Email」タブをクリックします。

A：出力



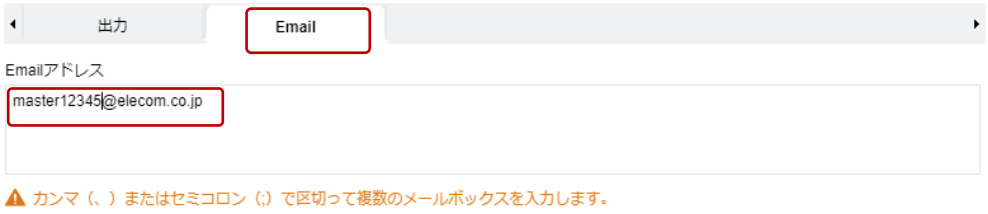

**＜ドア＞**

| アクションタイプ | 内容 |
|---|---|
| 閉じる | トリガー条件で、ドアを施錠します。 |
| 開く | トリガー条件で、ドアを解錠します。 |
| ノーマルオープン | トリガー条件で、常時解錠の状態に設定します。 |
| 施錠 | トリガー条件で、ロックダウン有効に設定されます。 |
| 解錠 | トリガー条件で、ロックダウン無効に設定されます。 |

**＜補助出力＞**

| アクションタイプ | 内容 |
|---|---|
| 閉じる | トリガー条件で、ドアを施錠します。 |
| 開く | トリガー条件で、ドアを解錠します。 |
| ノーマルオープン | トリガー条件で、常時解錠の状態に設定します。 |

B：Email

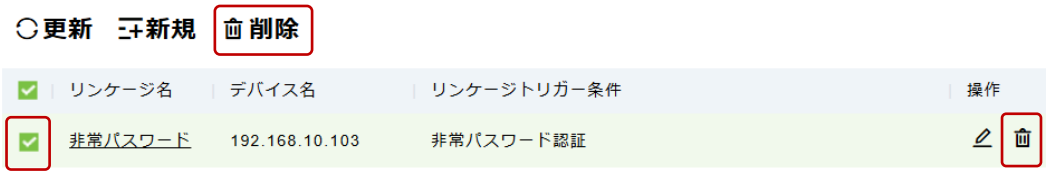


⑪ 設定を保存する場合は「OK」をクリックします。リンケージの一覧に表示されていることを確認します。

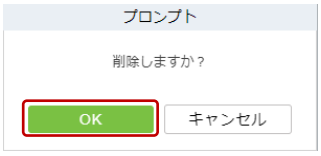



### 3. 削除

リスト内の該当リンケージ名をチェックして選択して「削除」をクリックするか、操作項目の「削除（ごみ箱アイコン）」をクリックします。




確認画面が表示されますので削除する場合は「OK」をクリックします。




**注意事項**

**＊リンケージで接点制御した場合、顔認証デバイスに選択した制御内容が反映されます。リアルタイムモニタリングなどで状態を確認して制御解除を行なってください。**

## 9.17.9. アンチ・パスバック

共連れ防止として、入室記録の無いユーザーは退室時の認証が行えないよう、より厳格な入退室管理を行う場合の機能です。
事前に 2 台の顔認証デバイスが Wiegand 接続されたデバイスが管理ソフトに登録された状態で本設定を行います。

1. 顔認証デバイス 2 台をアンチ・パスバック専用ポート同士で接続します。配線図は以下の通りです。
※鍵を保護するために部屋の内側へマスターデバイスと電磁ロックを設置するのが一般的です。

【配線図】



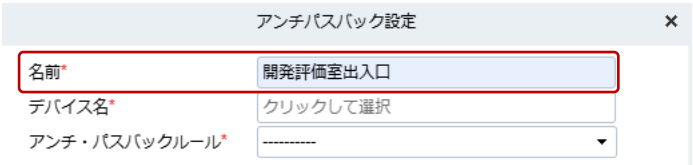

2. 管理ソフトの設定をします。



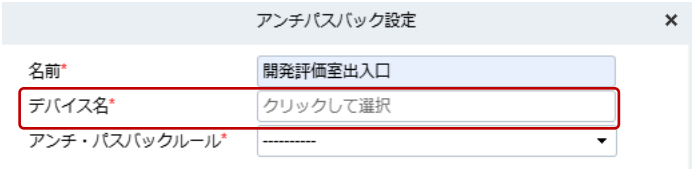

② アンチ・パスバックを設定するには、「アンチ・パスバック設定」をクリックします。



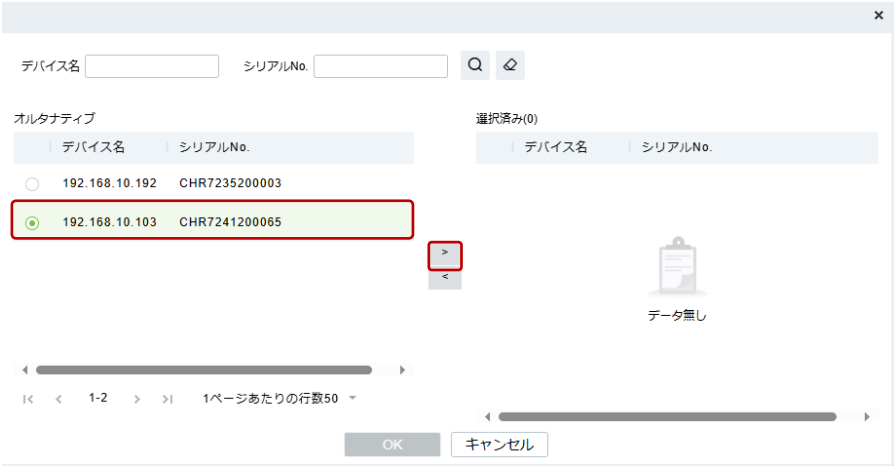

③ 「名前」にアンチ・パスバックの設定名を入力します。



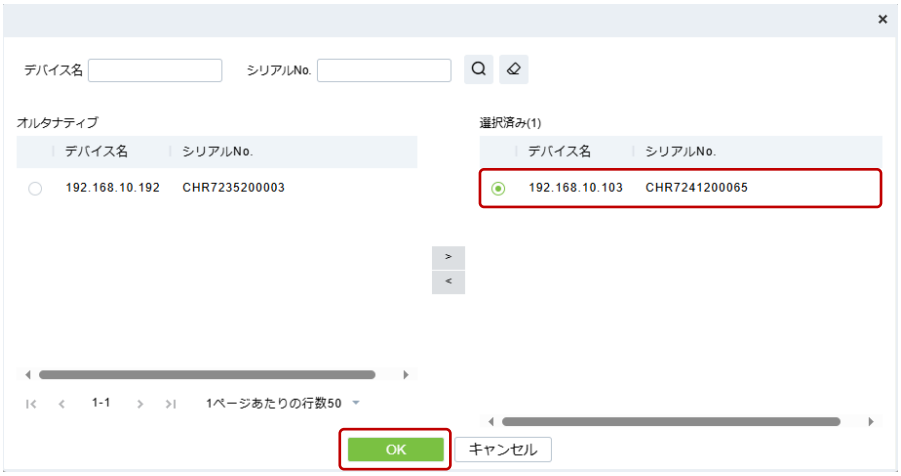
④ 「デバイス名」を選択します。フォームをクリックすると設定対象となる顔認証デバイスがリスト表示されます。



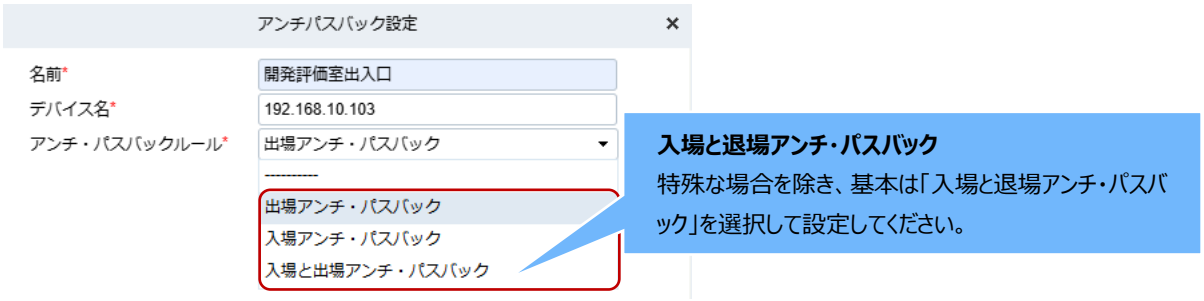

⑤ 顔認証デバイスを選択して「＞」をクリックして「選択済み」リストへ移動します。
※選択したデバイスがマスターデバイスとなります。アンチ・パスバックの設定で追加された顔認証デバイスは、デバイスリストには表示されません。アンチ・パスバック設定を削除すると、デバイスリストに再び表示されます。




⑥ 選択済みの顔認証デバイスで設定するには「OK」をクリックします。



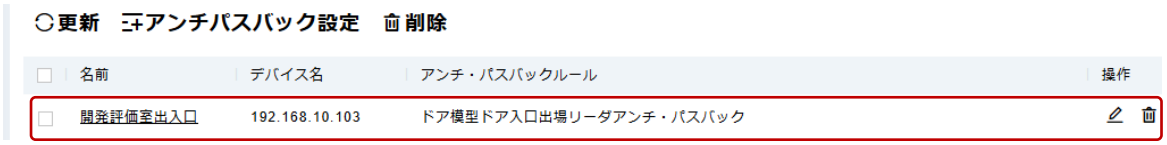
⑦ 「アンチ・パスバックルール」を選択します。




| アンチ・パスバックルール | 共連れ防止 | 警告 | 内容 |
|---|---|---|---|
| 出場アンチ・パスバック | 退室時<br>（出口） | 入口側 | 退室の本人認証が無く、入室の本人認証がある場合に「入退室ルール違反」の警告と共にロックは解除されません。 |
| 入場アンチ・パスバック | 入室時<br>（入口） | 出口側 | 入室の本人認証が無く、退室の本人認証がある場合に「入退室ルール違反」の警告と共にロックは解除されません。 |
| 入場と出場アンチ・パスバック<br>※基本は本設定で利用します | 入退室時<br>（出入口） | 両方 | 入室と退室の両方で本人認証が一対一で行われていない場合に「入退室ルール違反」の警告と共にロックは解除されません。 |

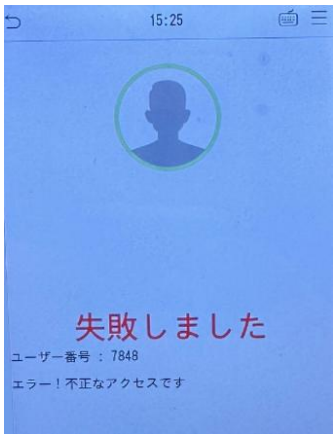
⑧ 最後に設定を保存するには「OK」をクリックします。続けてアンチ・パスバック設定をする場合は「保存して次へ」をクリックします。

⑨ 設定したデバイスが一覧リストに追加されていることを確認してください。




**【参考】**

アンチ・パスバックで「入退室ルール違反」と判定された場合、「入退室ルール違反」と音声案内と同時に下記のエラー画面が表示されます。




アンチ・パスバックは、設定したルールで認証に不整合（出入のトランザクションが一対一で記録されていない）が発生した場合に入退室ルール違反として該当ユーザーを入室または退室できないようにする目的があります。
万が一、意図しない状況で入室または退室ができない場合、下記対応でドアを解錠します。トランザクションを消去しない限り、認証に失敗した方はドアの解錠ができません。

- 管理者へ連絡し、該当ドアを遠隔解錠
- 周囲にいる方に連絡し、他の方の認証でドアを解錠

### 9.17.10. ファーストユーザー解錠

当社または本製品ではサポート対象外です。

### 9.17.11. マルチパーソングループ

当社または本製品ではサポート対象外です。

### 9.17.12. マルチパーソン

当社または本製品ではサポート対象外です。

### 9.17.13. 認証モード

当社または本製品ではサポート対象外です。

### 9.17.14. 認証モードグループ

当社または本製品ではサポート対象外です。

### 9.17.15. パラメータ

入退室管理に関する各種共通の運用設定をすることができます。設定した条件を保存する場合は「OK」をクリックします。

1. **トランザクションタイプ（初期値：新しいトランザクションを取得する時間を設定する／0:00）**
   顔認証デバイスで発生した記録（トランザクション）を取得するタイミングを設定します。間隔を指定して定期的にトランザクションを管理ソフトで収集するか、時間を指定して管理ソフトで収集するのかを選択できます。

   ① **定期的（選択範囲：1～8 時間（間隔））**
   「定期的」を選択した場合は時間を選択し取得する間隔を指定します。



② **新しいトランザクションを取得する時間を設定する**

「新しいトランザクションを取得する時間を設定する」を選択した場合はトランザクションを取得する「時間」を選択します。

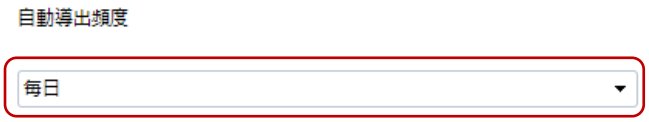



**2. イベント履歴自動導出（初期値：無し／選択範囲：毎日、毎月、無し）**

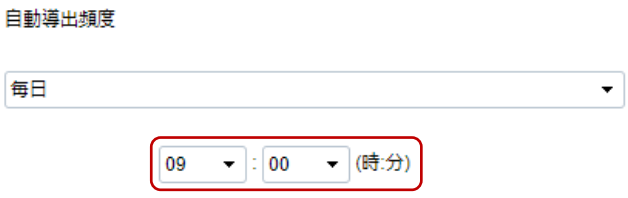
イベント履歴を予め設定されたメールアドレス宛に送信します。




① 自動導出頻度を選択します。（選択範囲：毎日、毎月、無し）




② 時間を選択します。



③ 導出モード（範囲）を選択します。日にち単位のイベントを送信対象にするか、毎回全イベント（最大 30,000 件）を対象にするか選択します。

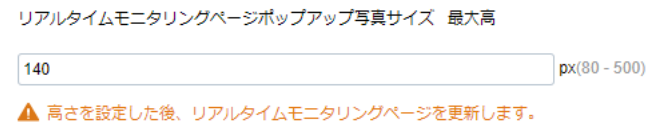



④ 送信先のメールアドレスを指定します。



### 3. リアルタイムモニタリング（初期値：140px）

リアルタイムモニタリングで表示するユーザー写真の高さ（80～500px）を指定します。




**<初期値の場合：高さ 140px>**

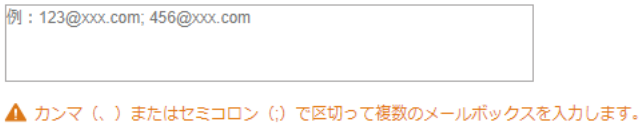



**<最大値の場合：高さ 500px>**



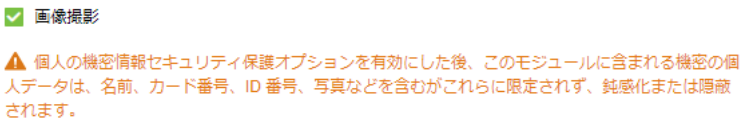
**4. アラームモニタリング受信者メールボックス（初期値：なし）**

アラームモニタリングの画面上以外に、メールアドレスを指定すると送信することができます。




**5. 個人の機密情報の保護（初期値：ON）**

当社または本製品はサポート対象外です。なお、本機能を利用する場合は、詳細 UI の「今日のイベント」でユーザー写真を表示するか否かを設定します。初期値は「ON」のため、「今日のイベント」でユーザー写真は表示されません。表示する場合はチェックボックスを外して「OFF」にします。




## 9.18. アクセス制御レポート

入退室管理の各種記録を確認することができます。

### 9.18.1. 全トランザクション

入退室管理における全ての記録を確認することができます。IC カード認証のみ未登録ユーザーが記録され、顔認証や掌認証およびパスワード認証による未登録ユーザー判定の記録は残りません。

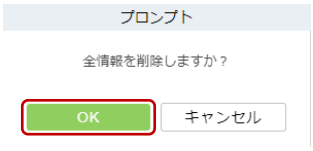



**1. 更新**

最新の状態に更新します。登録直後にリスト表示されない場合にクリックします。

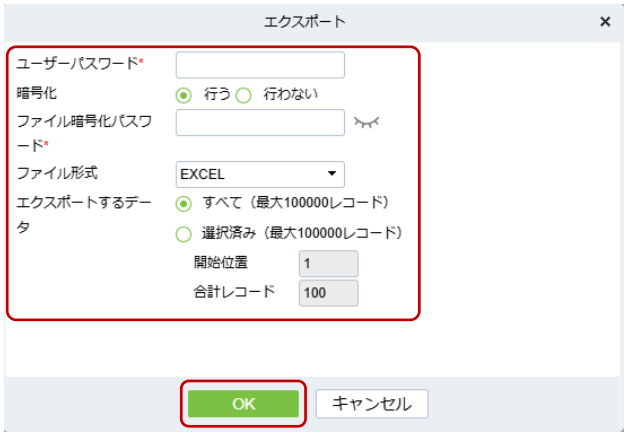
**2. 全データクリア**

記録されたデータを全てリセットします。リセットした記録は「アクセスデバイス」→「デバイス」→「情報表示／取得」→「トランザクションの取得」から、顔認証デバイス単位で再取得が可能です。但し、顔認証デバイスに残っている記録が対象となります。保存件数を超えた過去の記録は取得できません。全情報を削除する場合は「OK」をクリックします。



### 3. エクスポート

記録を指定の形式（EXCEL/PDF/CSV/TXT）でデータ出力します。なお、暗号化した場合、Windows 標準の解凍ツールは使用できません。




| 設定項目 | 内容 |
|---|---|
| ユーザーパスワード* | 管理者ユーザーのパスワードを入力します。 |
| ファイル暗号化 | データの暗号化を指定します。 |
| ファイル暗号化パスワード* | ファイル暗号化を指定した場合、復号化するパスワードを指定します。 |
| ファイル形式 | EXCEL・PDF・CSV・TXT から選択します。 |
| エクスポートするデータ | すべて：最大 10 万件を上限にの全データをダウンロードします。 |
| | 選択済み：開始レコードと上限（終了レコード）を指定してダウンロードします。 |

*印は必須です。

### 4. 写真をエクスポートする

当社または本製品はサポート対象外です。なお、本機能を利用する場合「詳細 UI」で写真データのみをダウンロードすることができます。なお、暗号化した場合、Windows 標準の解凍ツールは使用できません。

## 9.18.2. 今日のイベント

当社または本製品はサポート対象外です。

## 9.18.3. 全例外イベント

当社または本製品はサポート対象外です。

## 9.18.4. アラームログ

アラームを一覧表示することができます。期間指定、アラームの優先度やデバイス名でアラームを絞り込み検索することができます。また本画面でも「アラーム確認」することができます。アラーム確認については「9.16.10 アラームモニタリング」を参照してください。



## 1. アラーム確認

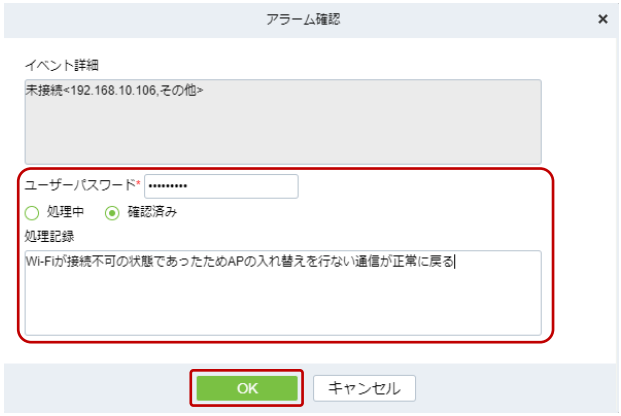
発生したイベントをリアルタイムに表示し、対応履歴などを記録することでアラームを止めることができます。

① イベントを選択（チェック）して「アラーム確認」をクリックします。アラーム確認を行わない場合、「アラーム確認状態」は「未確認」の表示のままとなります。

※イベントを複数選択することはできません

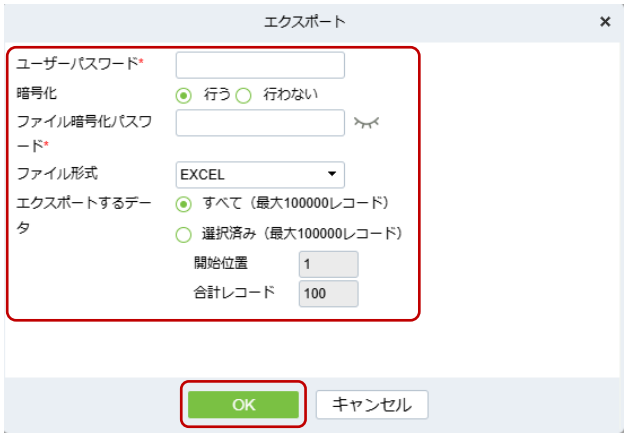



② イベント毎に対応履歴を残すことができます。管理パスワード（ユーザーパスワード）を入力し、対応区分「処理中」または「確認済み」を選択し、必要に応じて処理記録を残します。内容を保存する場合は「OK」をクリックします。




## 2. エクスポート

記録を指定の形式（EXCEL/PDF/CSV/TXT）でデータ出力します。なお、暗号化した場合、Windows 標準の解凍ツールは使用できません。




| 設定項目 | 内容 |
|---|---|
| ユーザーパスワード* | 管理者ユーザーのパスワードを入力します。 |
| ファイル暗号化 | データの暗号化を指定します。 |
| ファイル暗号化パスワード* | ファイル暗号化を指定した場合、復号化するパスワードを指定します。 |
| ファイル形式 | EXCEL・PDF・CSV・TXT から選択します。 |
| エクスポートするデータ | すべて：最大 10 万件を上限にの全データをダウンロードします。 |
| | 選択済み：開始レコードと上限（終了レコード）を指定してダウンロードします。 |

*印は必須です。

### 9.18.5. アラーム処理の履歴

当社または本製品はサポート対象外です。

### 9.18.6. ドアアクセス権限

当社または本製品はサポート対象外です。

### 9.18.7. ユーザーアクセス権限

当社または本製品はサポート対象外です。

### 9.18.8. 最初入り先と最後出し先

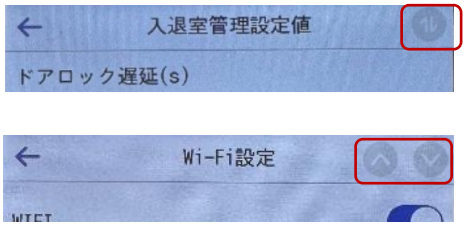
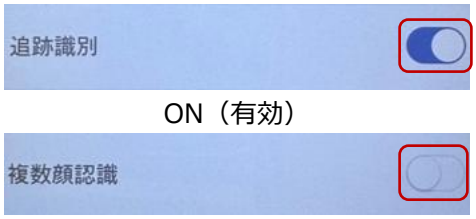
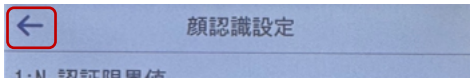
当社または本製品はサポート対象外です。

# 10. 顔認証デバイスの機能説明

顔認証デバイス本体の機能説明をします。入退 Push または勤怠 Push のモードにより表示されるメニューが異なります。基本的な設定以外は全て管理ソフトを使って顔認証デバイスへ反映します。

## 1. タッチパネルの操作方法

タッチパネルの基本的な操作方法を説明します。

| No | 操作名 | 操作方法 | 画面イメージ |
|---|---|---|---|
| ① | 選択 | アイコンや項目名をタップする |  |
| ② | 画面スクロール | 画面右上の「スクロール」アイコンをタップする |  |
| ③ | 機能 ON／OFF | 項目名をタップして ON（有効）／OFF（無効）する | <br>ON（有効）<br><br>OFF（無効） |
| ④ | 戻る | 画面左上の「戻る」アイコンをタップする |  |
| | 再起動 | 顔認証デバイス下部側面にあるピンホールのスイッチを押す（約１秒） |  |

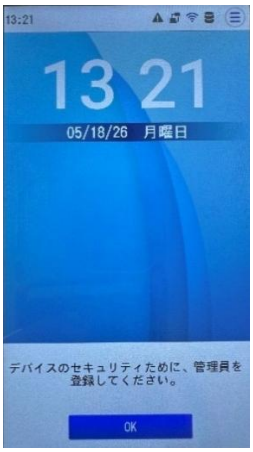
## 2. メインメニューを表示する

顔認証デバイスの「メインメニュー」アイコンをタップします。メインメニュー表示権限が設定されている場合、管理者に指定された方の認証が必要になります。画面遷移は、顔認証端末に管理者権限が付与されていない場合「手順 1→手順 2→手順 3→手順 4」、管理者権限が付与されている場合「手順 1→手順 3→手順 4」となります。

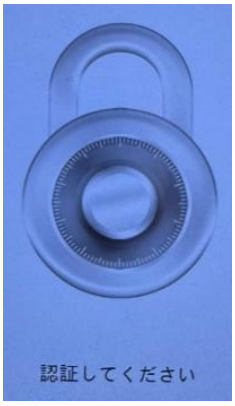
**手順 1：**
「メインメニュー」アイコンをタップ



**手順 2：**
セキュリティ警告




**手順 3：**
デバイス管理者の認証が必要です。




**手順 4：**
メインメニューの表示




※メインメニューの表示は無操作状態が 60 秒（初期値）続くとタイムアウトします。
※製品を初めて使用する際は、管理者権限を設定してから操作する必要があります。「ユーザー管理」をタップして管理者を追加、スーパー管理者としてユーザー権限を編集することができます。製品に管理者設定がない場合、メインメニューに入るたびに『デバイスのセキュリティために、管理員を登録してください。』が表示されます。

## 3. メインメニュー

をタップして、以下に示すように、初期インターフェースでメインメニューに入ります。



| メニュー名 | 説明 |
|---|---|
| **ユーザー管理** | ユーザー情報を追加、編集、表示、および削除します。 |
| **ユーザー権限** | カスタムのシステムを操作する権限範囲を設定します。 |
| **通信設定** | ネットワーク、シリアル通信、PC 接続、ウィーガンド、およびネットワーク診断の関連パラメータを設定します。 |
| **システム設定** | 日付と時間、顔と掌のパラメータ、工場出荷時の設定へのリセットなど、システムに関連するパラメータを設定します。 |
| **パーソナリティ設定** | ユーザーインターフェース、音声、ベルスケジュールを設定します。 |
| **データ管理** | デバイス内のすべての関連データを削除します。 |
| **アクセスコントロール** | 関連するアクセス制御デバイスのパラメーターを設定します。タイムスケジュール、休日設定、アクセスグループ、認証モード、アンチパスバック設定、などのメニューがあります。 |
| **勤怠検索** | アクセス履歴、写真を確認します。 |
| **自動テスト** | LCD 画面、オーディオ、カメラ、リアルタイムクロックなど、各モジュールが正しく機能するかどうかを自動的にテストします。 |
| **システム情報** | デバイス情報とファームウェアの情報、データ容量、およびデバイスのプライバシーポリシーを表示します。 |

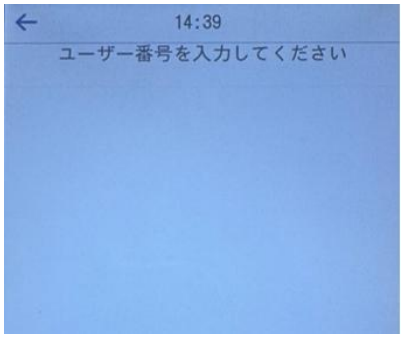
## 4. 認証方法を選択する

登録している認証情報を任意に選択してから認証することができます。設置環境（屋外などの太陽光の影響がある場所）に応じて選択することでスムーズな認証ができます。ユーザー毎に登録された認証情報により、選択できる認証方法のアイコン表示が異なります。

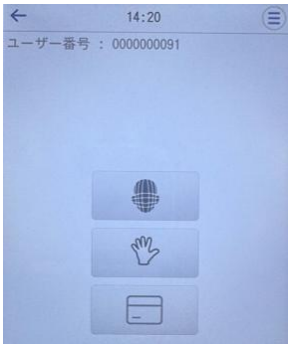
**手順 1：**
画面下または右上の「キーボード」アイコンをタップします。*1




**手順 2：**
認証するユーザー番号（ID）を入力します。




**手順 3：**
認証方法を選択します。*2




*1 カメラが起動している状態では、画面右上に「キーボード」アイコンが表示されます。
*2 ユーザー毎に登録されている認証情報に基づいて各認証アイコンが表示されます。登録されていない認証方法は、アイコンとして表示されません。

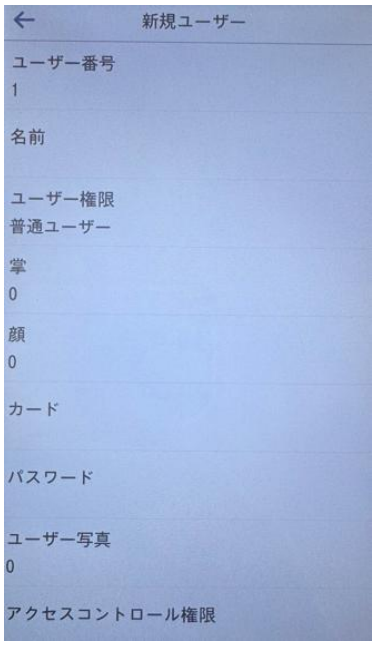
## 10.1. ユーザー管理

ユーザー情報に関する設定メニューです。

| 画面イメージ | 項目 | 説明 |
|---|---|---|
|  | 新規ユーザー | 顔認証デバイスで新規ユーザー登録をします。 |
| | ユーザーリスト | 顔認証デバイスに許可されたユーザーを一覧表示します。<br>選択して編集します。 |
| | 表示スタイル | ユーザーリストの表示方法を変更します。 |

### 1. 新規ユーザー

顔認証デバイスから新規にユーザー登録ができます。登録情報を管理ソフトに集約するためには、顔認証デバイスを予め「登録機」として設定しておく必要があります。ユーザー登録途中や登録後にも顔認証デバイスを登録機として設定できます。




| 項目 | 説明 |
|---|---|
| ユーザー番号（必須） | 重複しないユーザー番号（半角英数字）<br>※重複している場合、音声とエラーを表示 |
| 名前 | 顔認証デバイスからは英数字のみの入力可<br>※管理ソフトからは日本語入力可 |
| ユーザー権限 | 顔認証デバイスに対するアクセス権限設定<br>普通ユーザー/スーパー管理者 |
| 掌 | 掌情報を登録（両手の 2 件可） |
| 顔 | 顔情報を登録（1 件のみ） |
| カード | IC カードまたは QR（半角数字/20 桁）情報を登録 |
| パスワード | パスワード登録（最大数字 8 桁） |
| ユーザー写真 | 認証時に表示するプロフィール写真<br>※システム設定→アクセスログ設定→ユーザー写真を表示が有効（ON）の場合 |
| アクセスコントロール権限 | 認証モードの選択など<br>※初期値で利用し管理ソフトで管理します |

① **ユーザー番号（必須）** 【初期値：半角数字／半角数字または半角英数字、1～10 桁】
ユーザー番号（ID）を 1～10 桁の半角英数字で入力します。重複して登録することはできません。



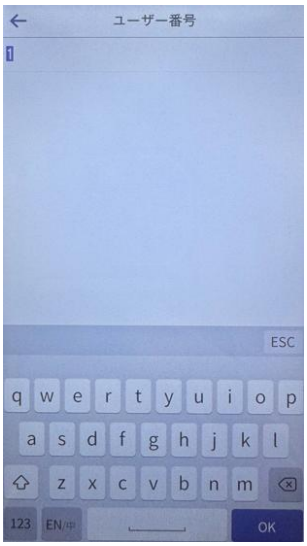

半角英数字を使用する場合は顔認証デバイスと管理ソフトの設定が必要です。

顔認証デバイスの設定は「10.4 システム設定」の「英字ユーザーID」を参照します。
管理ソフトの設定は「9.6.8 パラメータ」の「ユーザーID 設定」を参照します。

② **名前**

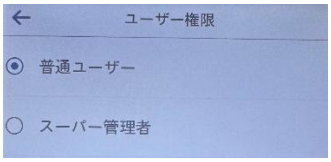
登録するユーザーの名前を入力します。顔認証デバイスからの入力は半角英数字のみです。

※管理ソフトから日本語入力できます。顔認証デバイスでの日本語表示は管理ソフトから反映します。



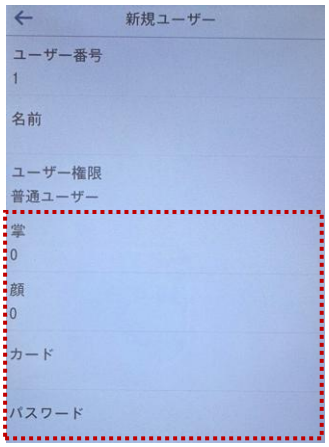

③ **ユーザー権限（初期値：普通ユーザー）**

顔認証デバイスを操作する権限設定をします。登録ユーザーのうち 1 名以上をスーパー管理者に設定した場合、次回のメインメニューの表示にはスーパー管理者による認証（基本は顔認証、その他登録してある認証方式を選択可）が必要になります。




④ **各認証情報の登録**

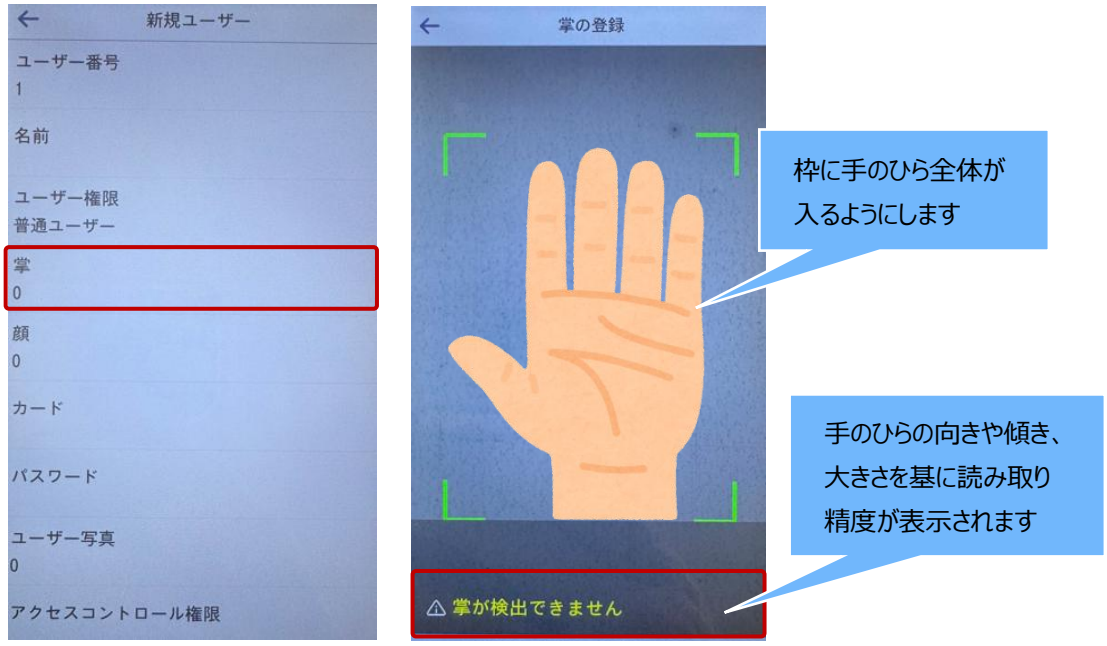
掌・顔・カードなど、認証に利用する項目をタップします。



・ **掌情報を登録する場合**

「掌」をタップし、掌 1、掌 2 のいずれかをタップします。カメラが起動したら、15～30 センチの距離で手全体を枠の中に入れて登録します。最後に画面左上の「戻る」をタップして保存します。

※登録中は画面下に読み取り精度が表示されます。精度が悪い場合は再登録となります。

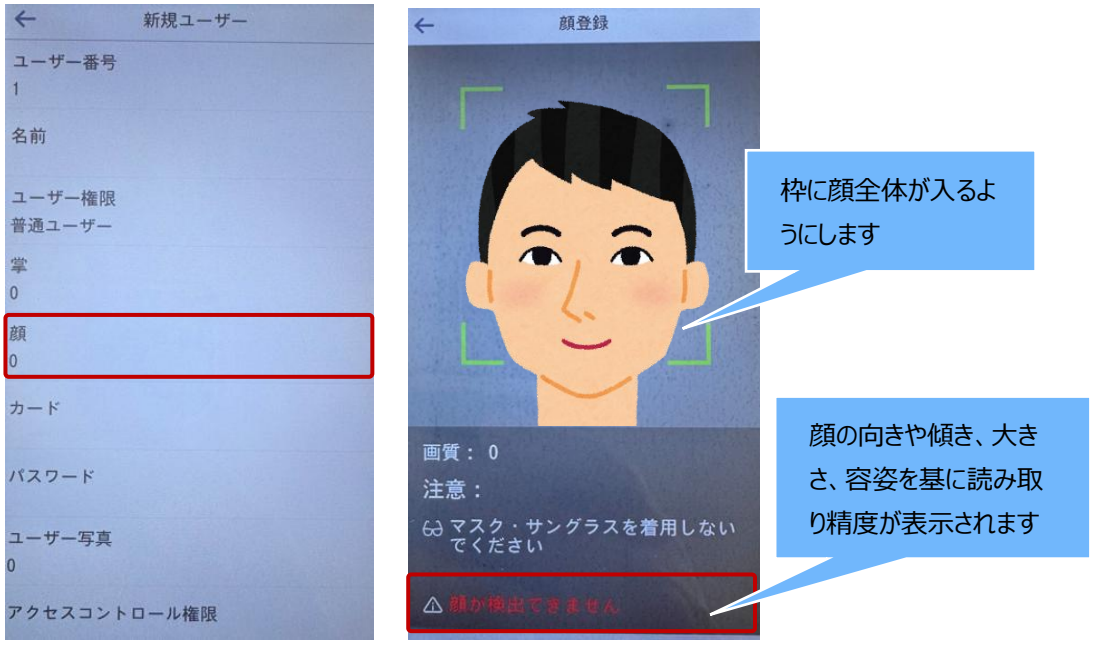



・ **顔情報を登録する場合**

「顔」をタップしてカメラを起動します。カメラが起動したら顔をかざして登録します。最後に画面左上の「戻る」をタップして保存します。

※登録中は画面下に読み取り精度が表示されます。精度が悪い場合は再登録となります。

「顔登録ガイドライン」を参照して写真の撮り直しをお願いします。



・ **IC カード情報*を登録する場合　※１枚のカード情報を複数のユーザーに登録することはできません。**

(ア)「カード」をタップします。　※入退 Push の場合「カードを追加」をタップしてから(イ)の手順へ

(イ) IC カードアイコンをタップします。

(ウ) 本体前面の IC カードリーダーに IC カード*をかざします。

(エ) IC カードの読み取り結果を確認し、最後に画面左上の「戻る」をタップして保存します。



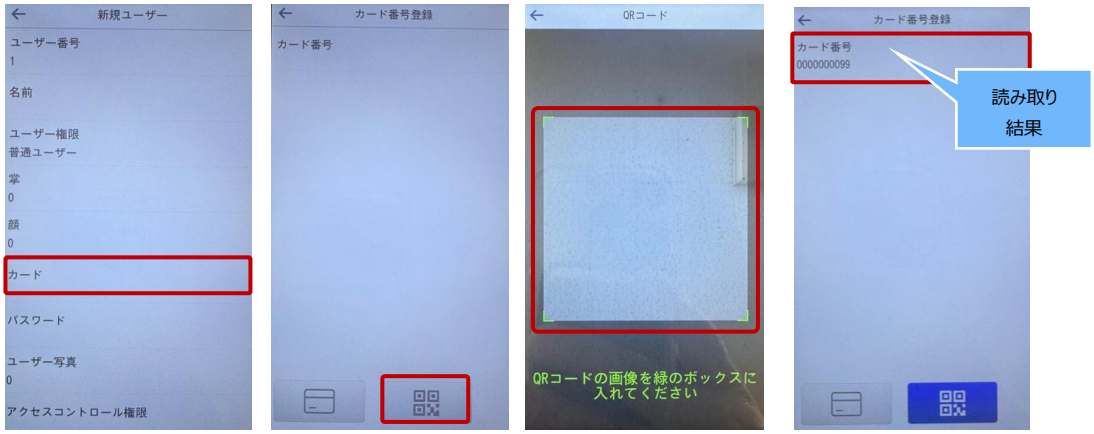

・ **QR 情報*を登録する場合（静的 QR）　※半角数字／最大 20 桁、同じ番号ををを複数のユーザーに登録することはできません。**

(ア)「カード」をタップします。　※入退 Push の場合「カードを追加」をタップしてから(イ)の手順へ

(イ) QR アイコンをタップします。

(ウ) カメラが起動したら、枠内に QR をかざします。

(エ) QR 読み取り結果を確認し、最後に画面左上の「戻る」をタップして保存します。




**注意事項**

***IC カード情報は、FeliCa：ISO/IEC 18092「NFC Type F」、MIFARE：ISO/IEC 14443「Type A」に対応**

***IC カードの ID 取得（読み取り）のみをサポートします。動作確認済みのカードは以下の通りです。**

**・「FeliCa」の「IDm」情報**

**・「Mifare Plus」の「UID」情報**

**・「Mifare Ultralight EV1」の「UID」情報**

**・「Mifare Classic 1K」の「UID」情報**

***IC カード情報および QR 情報について**

**・IC カード情報と QR 情報は、入退 Push モードの場合、カード登録数（50,000）の範囲で複数登録できます。**
**勤怠 Push モードの場合、IC カードまたは QR のいずれかの登録（排他）ができます。**

**・IC カード情報または QR 情報を削除する場合は、「ユーザーリスト」の「削除」から「カード番号のみ削除」を行ってください。**

・ **パスワード情報を登録する場合（6 桁以上、最大 8 桁の数字）**

(ア) 「パスワード」をタップします。

(イ) パスワードを入力します。

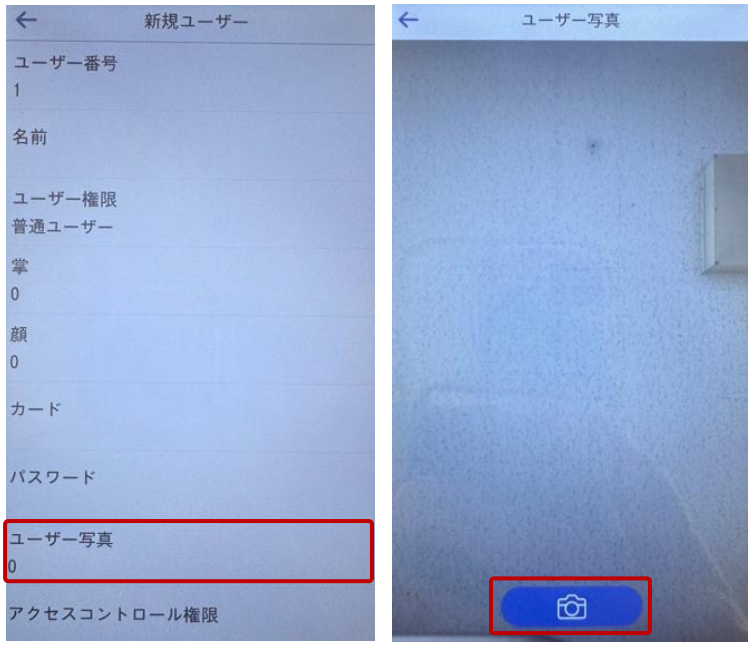
(ウ) 「パスワードを再入力してください」と表示されます。もう一度設定するパスワードを入力します。

(エ) 最後に画面左上の「戻る」をタップして保存します。




### ⑤ ユーザー写真

認証したユーザーの写真を表示します。表示する写真を登録するには、顔認証デバイスの「ユーザー写真」をタップします。カメラが起動したら「カメラ」アイコンをタップして撮影します。管理ソフトの「個別登録」や「一括登録」でも登録できます。




### ⑥ アクセスコントロール権限

本設定は管理ソフトから反映されるため初期値で利用します。

## 2. ユーザーリスト

登録されているユーザーを一覧表示、選択したユーザー情報の編集ができます。ユーザー番号（ID）による絞込検索も可能です。管理ソフトでユーザー情報のみを登録し、登録機として設定された顔認証デバイスから、ユーザー番号（ID）を検索して該当ユーザーの認証情報（顔/掌/IC カード/QR/パスワード）を登録することができます。

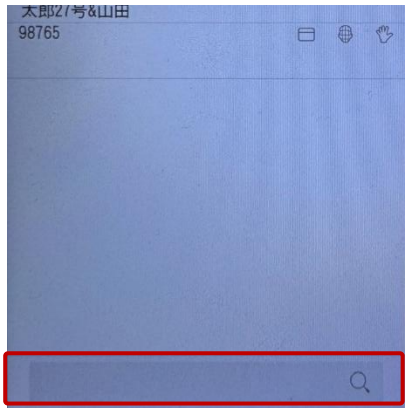



### ① ユーザー番号（ID）の検索

画面下部にある検索フォームをタップし、ユーザー番号（ID）を入力して絞り込み検索をします。

※前方一致検索

※デバイスに表示されているユーザーリストは、エリア（管理する拠点）に割り当てられた顔認証デバイスとユーザーに基づき一覧表示しています。表示されない場合、「7 勤怠連携（導入編）」または「8 入退室管理（導入編）」を参照してください。

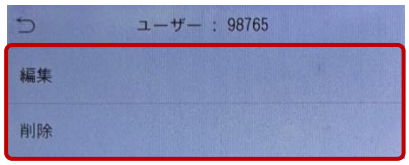


② **ユーザー情報の編集・削除**

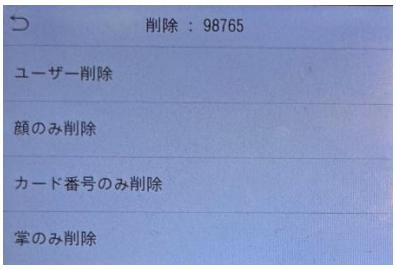
・ ユーザーリストから編集・削除するユーザーをタップします。




・ 編集または削除をタップします。編集の場合は「10.1 ユーザー管理」にある「新規ユーザー」の各種設定を参照してください。

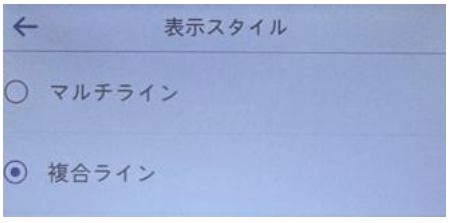



・ 削除の場合はユーザーを削除するのか、ユーザー情報内の認証情報のみを削除するのか選択してタップします。



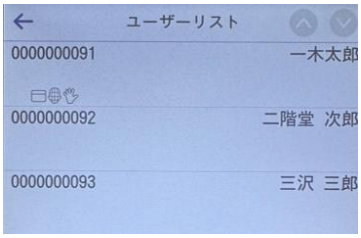

**3. 表示スタイル（初期値：複合ライン）**

ユーザーリストの表示方法を変更できます。



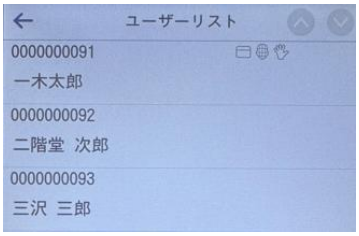

① **マルチライン**

ユーザーリストを 2 行で表示します。（名前が上段、認証情報の登録種別が下段に表示）



② **複合ライン（初期値）**

ユーザーリストを 2 行で表示します。（名前が下段、認証情報の登録種別が上段に表示）




## 10.2. ユーザー権限（カスタム権限）

顔認証デバイス側で設定する操作権限についてはサポート対象外です。

顔認証デバイスの操作権限を設定する場合、管理ソフトの「9.6.1 ユーザー」の「デバイス操作権限」を参照して設定します。

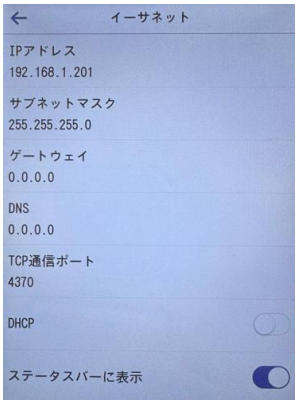
## 10.3. 通信設定

顔認証デバイスの通信に関する設定について説明します。




| 項目名 | 説明 |
|---|---|
| イーサネット | 有線 LAN 接続に関する設定です。 |
| シリアルポート設定 | サポート対象外です。初期値でご利用ください。 |
| 接続設定 | サポート対象外です。初期値でご利用ください。 |
| Wi-Fi 設定 | 無線 LAN 接続に関する設定です。 |
| クラウドサーバ設定 | 管理ソフトとの通信に関する設定です。 |
| ウィーガンド設定 | サポート対象外です。初期値でご利用ください。 |
| ネットワークテスト | 指定アドレスに Ping 通信テストを行います。 |

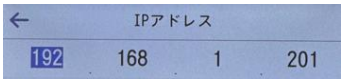
### 1. イーサネット




| 項目名 | 説明 |
|---|---|
| IP アドレス | IP アドレスを設定します。 |
| サブネットマスク | サブネットマスクを設定します。 |
| ゲートウェイ | デフォルトゲートウェイの IP アドレスを設定します。 |
| DNS | DNS サーバーの IP アドレスを設定します。 |
| TCP 通信サポート | サポート対象外です。初期値でご利用ください。 |
| DHCP | DHCP で IP アドレスを自動取得する設定をします。 |
| ステータスバーに表示 | ネットワーク接続状態を画面右上に表示します。 |

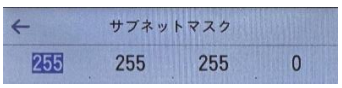
① IP アドレス（初期値：192.168.1.201）

固定 IP アドレスを使用する場合、IP アドレスの項目名をタップして、予めネットワーク管理者から指定された固定 IP アドレスを入力し「OK」をタップして保存します。DHCP で IP アドレスを自動取得する場合は⑥を参照します。



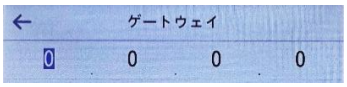

② サブネットマスク（初期値：255.255.255.0）

サブネットマスクを設定します。サブネットマスクの項目名をタップして、予めネットワーク管理者から指定されたサブネットマスクを入力し「OK」をタップして保存します。



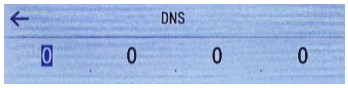
③ ゲートウェイ（初期値：0.0.0.0）

デフォルトゲートウェイを設定します。ゲートウェイの項目名をタップして、予めネットワーク管理者から指定されたサブネットマスクを入力し「OK」をタップして保存します。



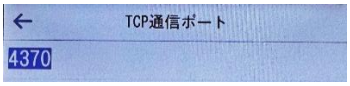

④ DNS（初期値：0.0.0.0）

DNS を設定します。DNS の項目名をタップして、予めネットワーク管理者から指定された DNS サーバーのアドレスを入力し「OK」をタップして保存します。




⑤ TCP 通信ポート（初期値：4370）

TCP 通信ポートを指定します。こちらは初期値で利用します。



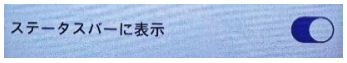

⑥ DHCP（初期値：OFF）

DHCP で IP アドレスを自動取得する場合は「ON」にします。予め無線 LAN または有線 LAN で接続している場合、ネットワーク上からデフォルトゲートウェイを検索してデフォルトゲートウェイの IP アドレスが自動で設定されます。自動で設定されない場合、またはネットワーク管理者から指定されたデフォルトゲートウェイの IP アドレスではない場合はこの限りではありません。




⑦ ステータスバーに表示（初期値：ON）

有線 LAN 接続の状態をステータスバー（認証待機画面右上）に表示する設定をします。通信状態を視覚的に確認することができます。



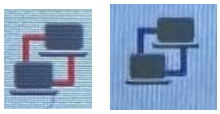

ON：




OFF：



＜ステータスバーの表示内容＞

| アイコンの種類 | 内容 |
|---|---|
|  | 【各種エラー】<br>● 固定用ブラケットから取り外された状態（タンパーアラーム）<br>● その他エラー（接点に外部装置が接続されていない等）<br>※ドアセンサータイプ（初期値：なし／選択範囲：下表参照）を参照してください |
|  | 【有線 LAN 接続状態】<br>● 線が赤：未接続<br>● 線が青：接続 |
|  | 【Wi-Fi 接続状態】<br>● 電波アイコンに×表示：未接続<br>● 電波アイコンが青（×非表示）：接続 |
|  | 【管理ソフト通信状態】<br>● サーバーに赤い地球マークが表示／非表示：通信不可／通信可<br>● 管理ソフトと通信中：上下の矢印マーク表示 |

## 2. シリアルポート設定

当社または本製品ではサポート対象外です。

## 3. 接続設定

当社または本製品ではサポート対象外です。

## 4. Wi-Fi 設定

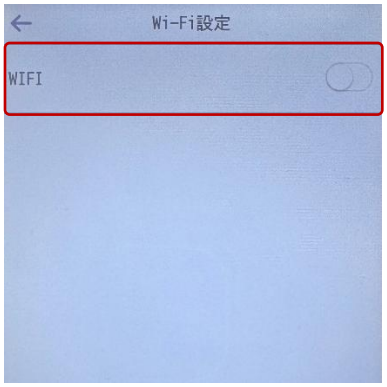


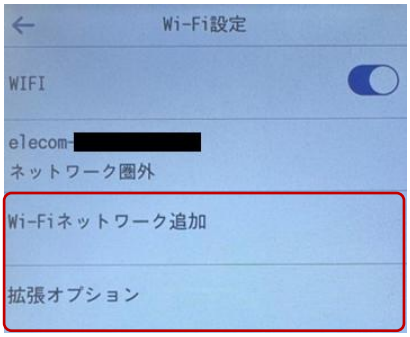

| 項目名 | 説明 |
|---|---|
| Wi-Fi | Wi-Fi 機能の ON/OFF が選択できます。 |
| Wi-Fi ネットワーク追加 | 手動入力で SSID を指定して接続します。 |
| 拡張オプション | 固定 IP アドレスで設定できます。 |

### ① Wi-Fi（初期値：ON）

検索可能な SSID リストを一覧表示します。表示されているリストから追加を行なってください。手動で SSID を設定する場合や拡張オプションで固定 IP アドレスを指定する場合は、画面右上のスクロールアイコン「」で移動し末尾の「Wi-Fi ネットワーク追加」または「拡張オプション」のメニューで設定します。

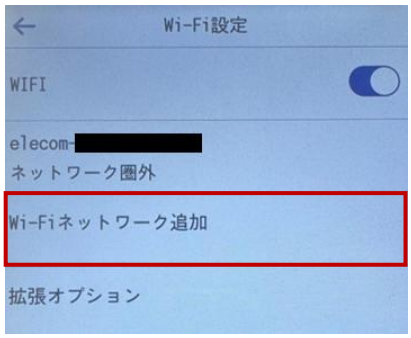


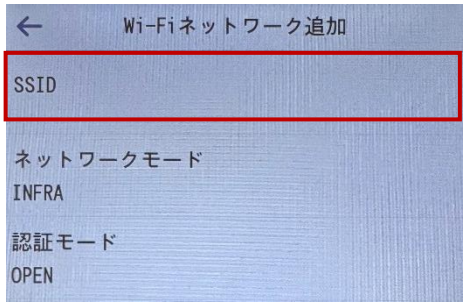




### ② Wi-Fi ネットワーク追加

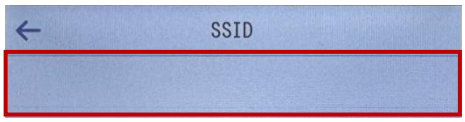
手動で SSID を設定するには、「Wi-Fi ネットワーク追加」をタップします。



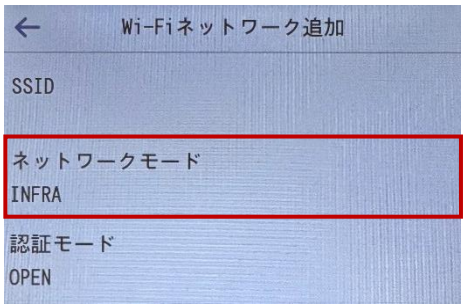
「SSID」をタップします。




ネットワーク管理者から指定された SSID を入力して最後に「OK」をタップします。




「ネットワークモード」を選択します（初期値：INFRA）
ADHOC が選択できますが、サポートしません。INFRA で利用してください。



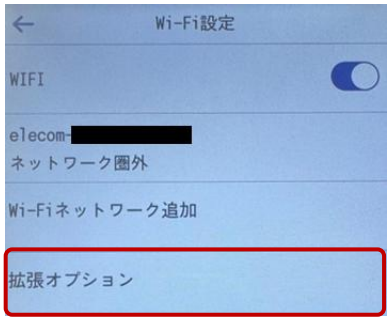

| モード | 説明 |
|---|---|
| INFRA | アクセスポイントを介して通信をします。 |
| ADHOC | 無線 LAN クライアント同士で直接通信をします。 |

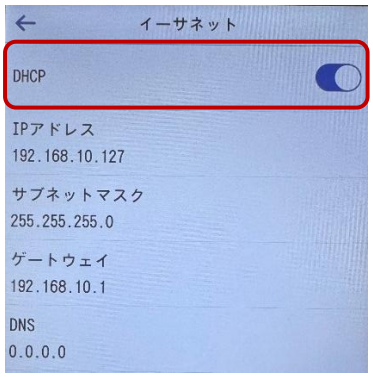
「認証モード」から認証モード及び暗号化モードを選択します。項目名をタップすると暗号化方式を切り替えて表示することができます。ネットワーク管理者から指定された認証モード及び暗号化モードを選択します。

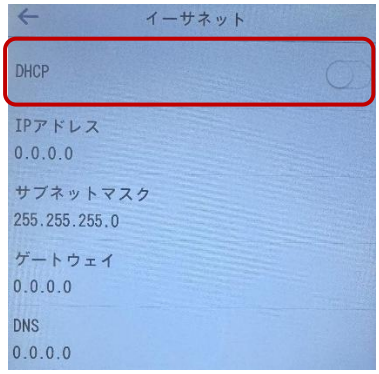
| 認証モード | 暗号化モード |
|---|---|
| OPEN | なし |
| SHARED | WEP/NONE |
| WEPAUTO | WEP/NONE |
| WPA-PSK（WPA-Personal） | TKIP/AES |
| | TKIP |
| | AES |
| WPA2-PSK（WPA2-Personal） | TKIP/AES |
| | TKIP |
| | AES |
| WPA1-PSK/WPA2-PSK（WPA-Personal/ WPA2-Personal） | TKIP/AES |
| | TKIP |
| | AES |

③ **拡張オプション**

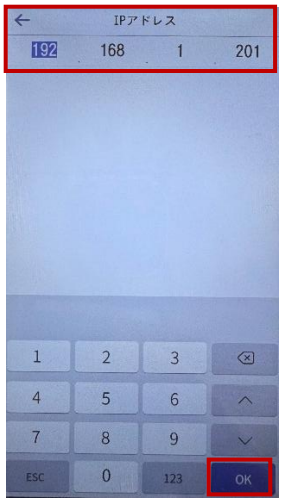
固定 IP アドレスを指定する場合、「拡張オプション」をタップし、DHCP を「OFF（無効）」にします。

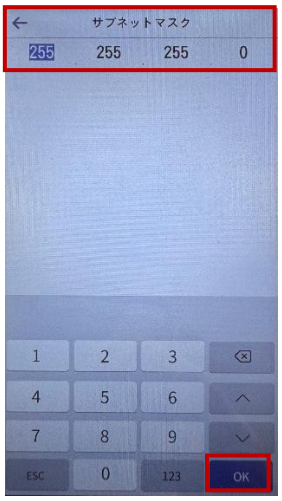


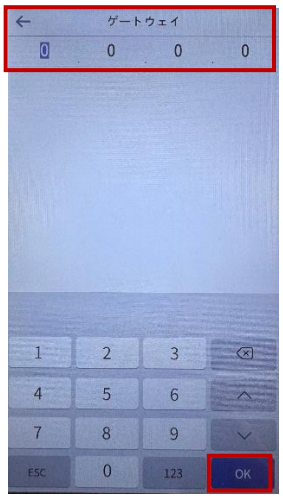



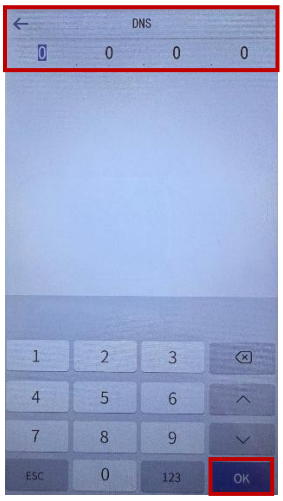




入力する各項目をタップして編集し、入力情報を保存するために「OK」ボタンをタップします。



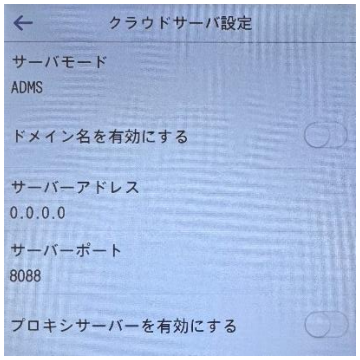




**注意事項**

**＊1 固定 IP アドレスやゲートウェイの情報はネットワーク管理者へお問合せをお願いします。また、利用するネットワーク情報は、顔認証デバイスと管理ソフトが相互通信できるよう、予めアクセス制限などの環境設定を実施してから顔認証デバイスや管理ソフトの設定をお願いします。**

## 5. クラウドサーバー設定




| 項目名 | 説明 |
|---|---|
| サーバーモード | 管理ソフトとの通信モードが指定されています。 |
| ドメイン名を有効にする | 管理ソフトが稼働する公開サーバーのドメイン（FQDN）を指定します。 |
| サーバーアドレス | 管理ソフトが稼働する PC/サーバーの IP アドレスを指定します。 |
| サーバーポート | 管理ソフトと通信するためのポートを指定します。 |
| プロキシサーバーを有効にする | プロキシサーバー経由で管理ソフトが稼働する PC/サーバーへ接続する場合の設定をします。 |

**① サーバーモード（初期値：ADMS）**

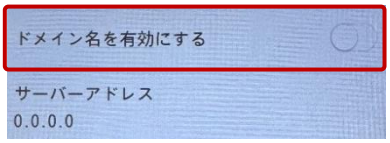
管理ソフトと相互通信するためのモード選択です。変更することはできません。

**② ドメイン名を有効にする（初期値：OFF）**

インターネット上の公開サーバーとインターネットに接続可能な顔認証デバイスの間で通信する場合に本機能を利用します。公開サーバーと通信する場合、セキュリティ設計には十分配慮して運用してください。当社はセキュリティ設計についてサポート対象外となります。お客様の情報システム部門または専門業者へご確認・ご相談をお願いします。

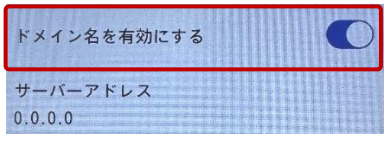
**③ サーバーアドレス（初期値：0.0.0.0）**

「ドメイン名を有効にする」が「OFF」の場合、管理ソフトが稼働する PC/サーバーのローカル IP アドレスを指定します。PC/サーバー側は固定 IP アドレスで運用します。




入力例：　　192.168.10.145

「ドメイン名を有効にする」が「ON」の場合、管理ソフトが稼働する公開サーバーのドメイン名または固定グローバル IP アドレスを指定します。IP アドレスを指定する場合、固定グローバル IP アドレスまたは動的グローバル IP アドレスは DDNS（Dynamic Domain Name System*）などの仕組みで運用します。なお、ドメイン名または IP アドレスの後に後述する「④のサーバーポート」を指定します（**:8088**／コロン ハチ ゼロ ハチ ハチ）。




入力例：　　example.com**:8088**　または　123.456.789.123**:8088**

*インターネット接続のたびに変動するグローバル IP アドレス（固定グローバル IP アドレスではない）を、固定のドメイン名（ホスト名）と自動で紐付けし続ける仕組み

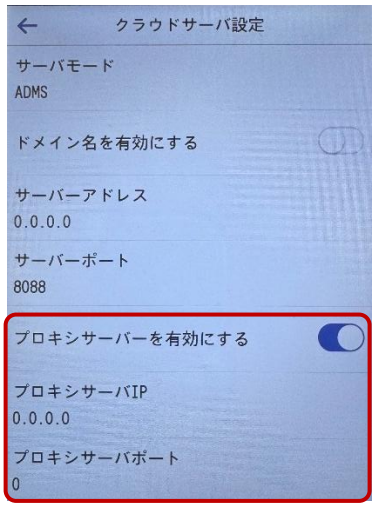
④ **サーバーポート（初期値：8088）**

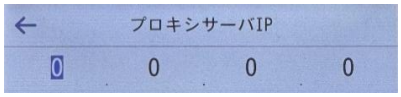
管理ソフトが稼働する（インストールされた）PC/サーバーと通信するために使用するポート番号を指定します。管理ソフトのインストール時に設定されるサーバーポートは「8088」になります。

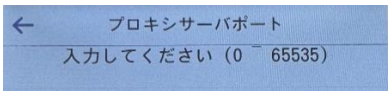
※Web ポート番号「8088」が利用できない場合は「11.2 サーバーポートの設定変更」を参照して変更してください。

⑤ **プロキシサーバーを有効にする（初期値：OFF）**

ネットワーク管理者の指定が無い限り「初期値：OFF」で利用してください。なお、管理ソフトが稼働する PC/サーバーにプロキシサーバー経由でアクセスする場合、「プロキシサーバーを有効にする」を「ON」にします。また、ネットワーク管理者から指定された IP アドレスを「プロキシサーバ IP」、使用するサーバーポート「プロキシサーバポート」へ入力します。



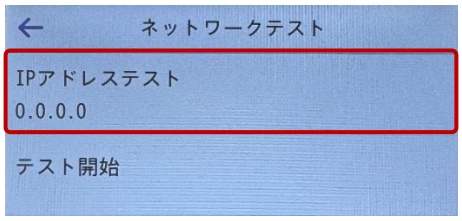
### 6. ウィーガンド設定

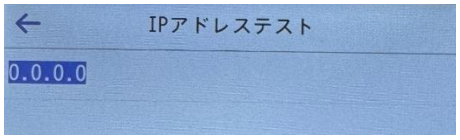
当社または本製品ではサポート対象外です。

### 7. ネットワークテスト（初期値：0.0.0.0）

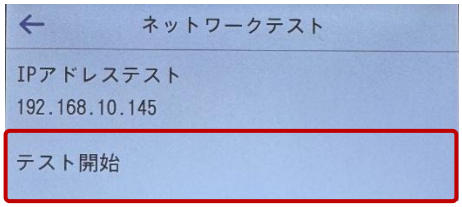
サーバーアドレスで指定した IP アドレスまたはドメイン名に対して通信テスト（Ping テスト）を実行することができます。管理ソフトとの相互通信が必要になるため、管理ソフトが稼働する PC/サーバーとの通信テストを実施する場合に有効です。なお、IP アドレスの初期値「0.0.0.0」で実行した場合、セルフテストとなります（Localhost）。

「IP アドレステスト」をタップして、管理ソフトが稼働する PC/サーバーの IP アドレスまたはドメイン名を入力します。




「テスト開始」をタップして通信テストを実行します。結果表示後に内容を確認して「OK」をタップします。







テスト結果：ネットワーク正常（合格）



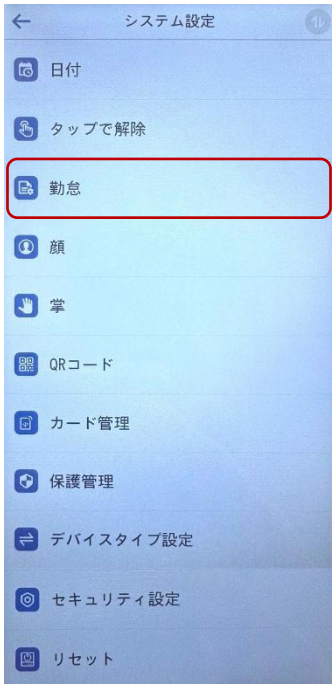

テスト結果：ネットワーク設置を検査してください（不合格）*

*「通信設定」→「クラウドサーバ設定」を確認し、サーバーアドレスの再確認をしてください。

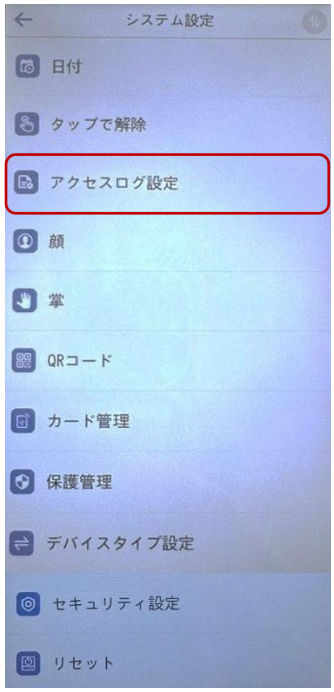
## 10.4. システム設定

顔認証デバイスのシステム設定について説明します。

勤怠 Push




入退 Push



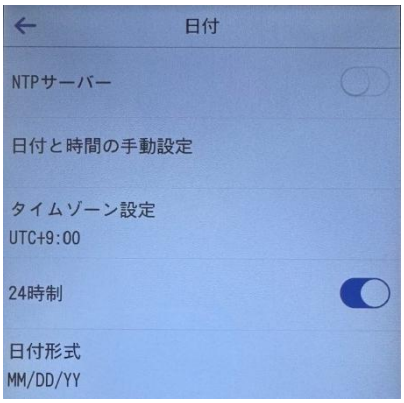

| 項目名 | 説明 |
|---|---|
| 日付 | NTP サーバーとの同期設定をします。 |
| タップで解除 | 画面をタップしてカメラ（認証モード）を起動します。 |
| 勤怠* | 勤怠履歴に関する設定をします。 |
| アクセスログ設定* | 入退履歴に関する設定をします。 |
| 顔 | 顔認証に関する設定をします。 |
| 掌 | 掌認証のパラメータ設定をします。 |
| QR コード | QR に関する設定をします。 |
| カード管理 | IC カードに関する設定をします。 |
| 保護管理 | マスク検知の設定をします。 |
| デバイスタイプ設定* | デバイスタイプ（勤怠 Push/入退 Push）を設定します。 |
| セキュリティ設定 | 初期値で利用します。 |
| リセット | 顔認証デバイスの設定値をリセットします。 |

*「勤怠」または「アクセスログ設定」は、「デバイスタイプ設定」で選択したモードにより表示されるメニューが異なります。

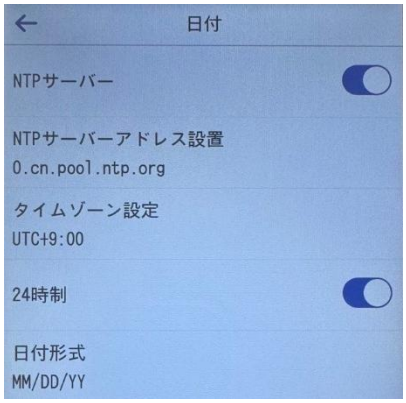
| デバイスタイプ | 表示されるメニュー |
|---|---|
| 勤怠 Push | 勤怠 |
| 入退 Push | アクセスログ設定 |

## 1. 日付

**NTP サーバー：OFF**




**NTP サーバー：ON**



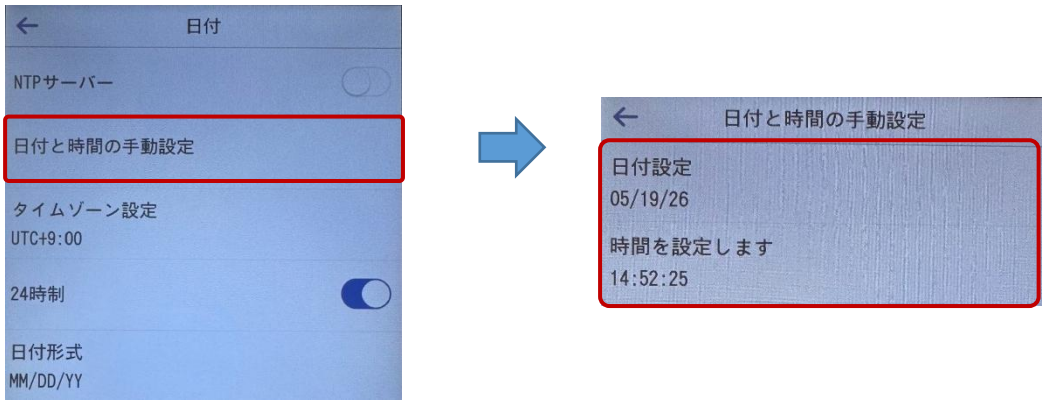

| 項目名 | 説明 |
|---|---|
| NTP サーバー | NTP サーバーと時刻同期する設定です。 |
| 日付と時間の手動設定 | 手動で日時を修正します。 |
| NTP サーバーアドレス設置 | NTP サーバーのアドレスを指定します。 |
| タイムゾーン設定 | 初期値で利用します。 |
| 24 時制 | 時計の表示方法を設定します。 |
| 日付形式 | YYYY-MM-DD など表示形式を設定します。 |

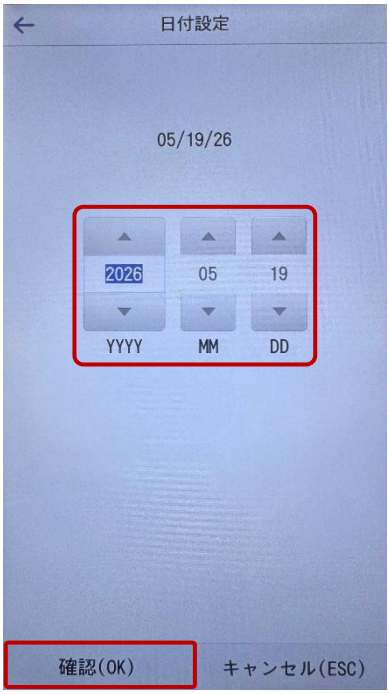
### ① NTP サーバー（初期値：OFF）

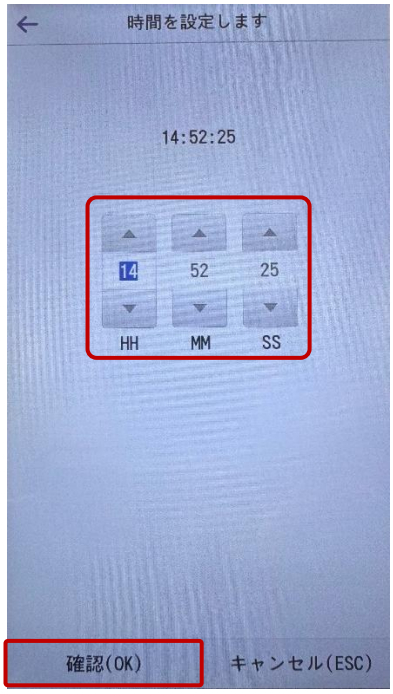
NTP サーバーと時刻同期する設定する場合は「ON」にします。ON の場合、1 時間に 1 回の間隔で NTP サーバーと同期を行います。勤怠管理や入退室管理において、正確な日時情報を記録するためには ON にします。

### ② 日付と時間の手動設定

NTP サーバーが OFF の場合、手動で日時の修正をすることができます。修正する場合は「日付と時間の手動設定」をタップし、「日付設定」または「時間を設定します」をタップして修正します。

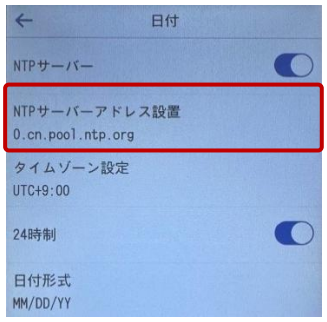





③ **NTP サーバーアドレス設置（初期値：0.cn.pool.ntp.org）**

NTP サーバーが ON の場合、NTP サーバーのドメイン名または IP アドレスを指定します。インターネット上の NTP サーバーと同期する場合はドメイン（URL）を指定し、社内 LAN の NTP サーバーを指定する場合は IP アドレスを指定します。




※インターネット上の NTP サーバーを指定する場合、ネットワーク設定にある DNS の設定は必須となります。

④ **タイムゾーン設定（初期値：UTC＋9：00）**

顔認証デバイスは日本国内の利用に限定されています。初期値で利用してください。

⑤ **24 時制（初期値：ON）**

時間の表示形式を設定します。基本は初期値で利用します。なお、外部システムと連携を行う場合は表示形式に注意してください。

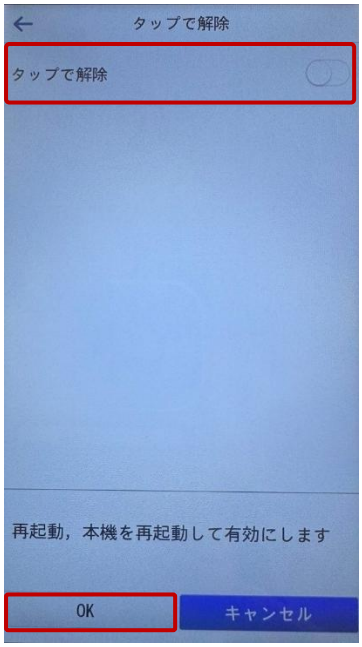
⑥ **日付形式（初期値：MM/DD/YY）**

日付の表示形式を設定します。基本は初期値で利用します。なお、外部システムと連携を行う場合は表示形式に注意してください。

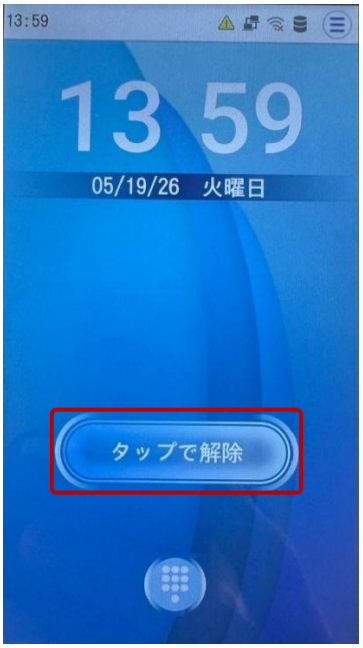
### 2. タップで解除（初期値：OFF）

初期値では顔認証デバイスの前に立つと自動でカメラが起動して認証します。本機能を ON にすると、画面をタップするまでカメラは起動しません。顔認証デバイスを人通りの多い場所に設置し、カメラが反応してしまう場合、本機能を ON にすることで意図しない認証を防止することができます。なお、設定変更（ON⇔OFF）には再起動が必要です。

ON（有効）にする場合は「OK」をクリックします

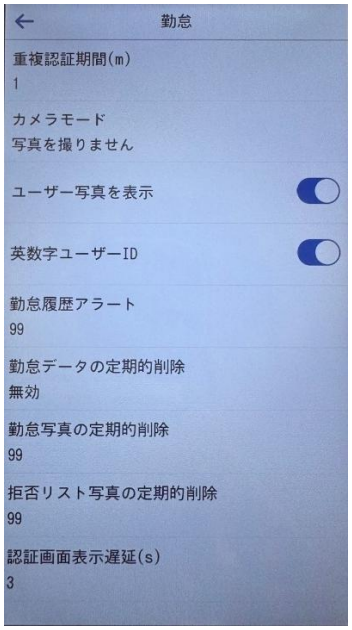



「タップで解除」をタップするとカメラが起動し認証できます



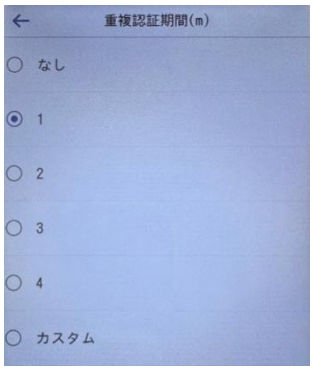

### 3. 勤怠（勤怠 Push 専用メニュー）

※本メニューは「デバイスタイプ設定」が「勤怠 Push」に設定されている場合に表示されます。




| 項目名 | 説明 |
|---|---|
| 重複認証期間（m） | 管理ソフトへデータ送信する間隔を設定します。 |
| カメラモード | 認証時のスクリーンショットを保存する設定です。 |
| ユーザー写真を表示 | 認証時ユーザー写真を表示する設定です。 |
| 英数字ユーザーID | ユーザーID の入力ルールを設定します。 |
| 勤怠履歴アラート | 履歴件数に閾値を設定して警告を画面に表示します。 |
| 勤怠データの定期的削除 | 設定した件数に到達すると古いデータから削除します。 |
| 勤怠写真の定期的削除 | 設定した件数に到達すると古いデータから削除します。 |
| 拒否リスト写真の定期的削除 | サポート対象外です。初期値でご利用ください。 |
| 認証画面表示遅延(s) | 画面下に表示される認証結果表示時間を設定します。 |

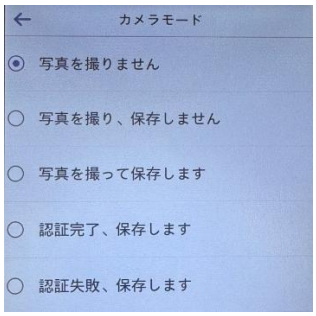
**① 重複認証期間（m）（初期値：1／設定範囲：なし、1～999999）**




ユーザーが出勤・退勤などの勤怠種別を設定して認証すると、打刻データが顔認証デバイスの勤怠履歴に保存され、管理ソフトへデータ送信が行われます。この管理ソフトへのデータ送信される間隔（分）を設定することができます。

例えば、5（m）に設定した場合、同一ユーザーが 5 分間に何回も打刻してもデータ保存や送信は、最初の 1 件だけが対象となり、他の重複打刻は破棄されます。次に保存されるデータは 5 分経過後の打刻データとなります。

**② カメラモード（初期値：写真を撮りません）**




認証時に被写体の顔写真を撮影して保存する機能です。ユーザー写真表示後に撮影時の写真を表示します。設定値による動作は以下の通りです。

| 項目名 | 説明 |
|---|---|
| 写真を撮りません | 撮影も保存もしない。 |
| 写真を撮り、保存しません | 撮影するが保存しない。 |
| 写真を撮って保存します | 認証完了前の被写体を撮影し保存する。 |
| 認証完了、保存します | IC カードまたは QR 認証完了（成功）後に写真を保存する。 |
| 認証失敗、保存します | 一部の認証失敗時に写真を保存する。* |

* IC カードまたは QR 認証失敗、入退室管理では無効タイムゾーン（アクセス不可時間）で認証失敗やアクセス権限が無効で認証失敗、勤怠連携ではエリア別ユーザー登録が無く認証失敗した時に写真を保存します。

**③ ユーザー写真を表示（初期値：ON）**

認証時、管理ソフトに予め登録されているユーザー写真*を表示する機能です。ユーザー写真が登録されていない場合は、テンプレート用のアイコンが表示されます。

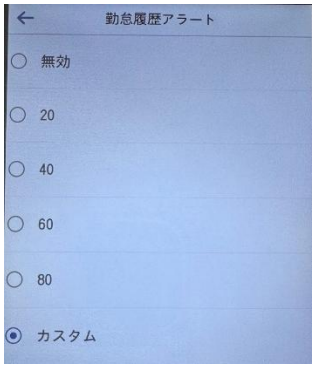
*ユーザー写真：
ユーザー写真は認証時に表示するアイコン用写真で認証用の写真ではありません。そのため登録は必須ではありません。顔認証には「ユーザー写真テンプレート」という特徴点をデータベース化した情報で認証します。仮にユーザー写真を削除しても、ユーザー写真テンプレートが削除されない限り顔認証ができます。

**④ 英数字ユーザーID（初期値：ON）**

顔認証デバイス側でユーザー番号（ID）の入力できる文字の種類を設定できます。既に数字（OFF 設定）で登録済みのユーザーが存在している状態で、英数字（ON 設定）に変更しても既存ユーザー（OFF 設定）のユーザーに影響はありません。
※「英数字ユーザーID」を「ON」にする場合、事前に管理ソフト側の利用設定も「ON」にしてください。管理ソフト側の設定については「9.6.8 パラメータ」の「ユーザーID 設定」を参照してください。

| 設定値 | 説明 |
|---|---|
| OFF | 数字の入力ができます |
| ON | 英数字の入力ができます |

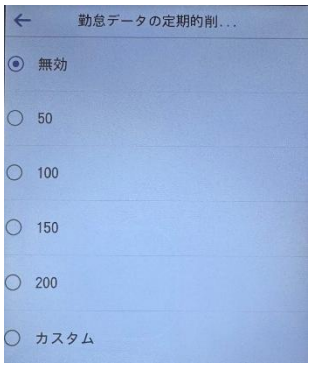
### ⑤ 勤怠履歴アラート（初期値：99／設定範囲：無効、1～9999）




勤怠履歴の残りの保存数を設定することで顔認証デバイスの画面上に警告を表示します。100 万件の履歴が保存できますが、設定した値（残りの保存可能な勤怠履歴数）で画面上に警告を表示します。

### ⑥ 勤怠データの定期的削除（初期値：無効／設定範囲：1～999）

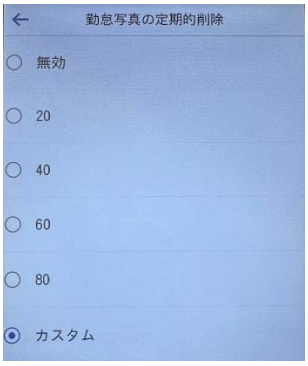
**※本設定は「無効」から設定範囲内で必ず設定をお願いします。**




勤怠履歴のデータを定期的に削除する設定です。認証時の勤怠履歴が上限に達した時に設定した値（レコード数）で古い履歴から一括削除して、デバイスの空き容量を確保します。なお、無効にした場合、最大保存件数（100 万件）まで保存されますが、新しいデータの記録ができなくなりますのでご注意ください。

### ⑦ 勤怠写真の定期的削除（初期値：99／設定範囲：無効、1～99）

**※本設定は「無効」せず、設定範囲内で必ず設定をお願いします。**

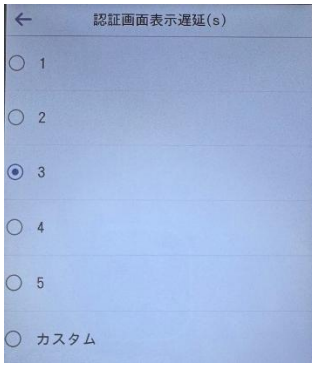



認証時の写真を定期的に削除する設定です。認証時の勤怠写真が上限に達した時に設定した値（レコード数）で古い写真から一括削除して、デバイスの空き容量を確保します。なお、無効にした場合、最大保存件数（7,500 件）まで保存されますが、新しいデータの記録ができなくなりますのでご注意ください。

### ⑧ 拒否リスト写真の定期的削除（初期値：99／設定範囲：無効、1～99）

当社または本製品ではサポート対象外です。

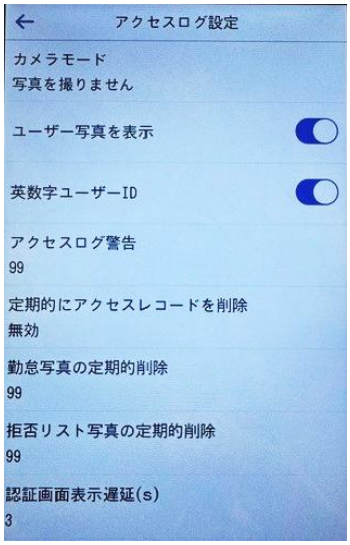
### ⑨ 認証画面表示遅延(s)（初期値：3／設定範囲：無効、1～9）




画面下に表示される認証結果の表示時間を設定できます。

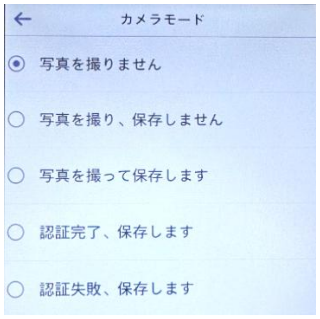
## 4. アクセスログ設定（入退 Push 専用メニュー）

※本メニューは「デバイスタイプ設定」が「入退 Push」に設定されている場合に表示されます。




| 項目名 | 説明 |
|---|---|
| カメラモード | 認証時のスクリーンショットを保存する設定です。 |
| ユーザー写真を表示 | 認証時ユーザー写真を表示する設定です。 |
| 英数字ユーザーID | ユーザーID の入力ルールを設定します。 |
| アクセスログ警告 | 履歴件数に閾値を設定して警告を画面に表示します。 |
| 定期的にアクセスレコードを削除 | 設定した件数に到達すると古いデータから削除します。 |
| 勤怠写真の定期的削除 | 設定した件数に到達すると古いデータから削除します。 |
| 拒否リスト写真の定期的削除 | サポート対象外です。初期値でご利用ください。 |
| 認証画面表示遅延(s) | 画面下に表示される認証結果表示時間を設定します。 |

### ① カメラモード（初期値：写真を撮りません）




認証時に被写体の顔写真を撮影して保存する機能です。ユーザー写真表示後に撮影時の写真を表示します。設定値による動作は以下の通りです。

| 項目名 | 説明 |
|---|---|
| 写真を撮りません | 撮影も保存もしない。 |
| 写真を撮り、保存しません | 撮影するが保存しない。 |
| 写真を撮って保存します | 認証完了前の被写体を撮影し保存する。 |
| 認証完了、保存します | IC カードまたは QR 認証完了（成功）後に写真を保存する。 |
| 認証失敗、保存します | 一部の認証失敗時に写真を保存する。* |

* IC カードまたは QR 認証失敗、入退室管理では無効タイムゾーン（アクセス不可時間）で認証失敗やアクセス権限が無効で認証失敗、勤怠連携ではエリア別ユーザー登録が無く認証失敗した時に写真を保存します。

② **ユーザー写真を表示（初期値：ON）**

認証時、管理ソフトに予め登録されているユーザー写真*を表示する機能です。ユーザー写真が登録されていない場合は、テンプレート用のアイコンが表示されます。

*ユーザー写真：

ユーザー写真は認証時に表示するアイコン用写真で認証用の写真ではありません。そのため登録は必須ではありません。顔認証には「ユーザー写真テンプレート」という特徴点をデータベース化した情報で認証します。仮にユーザー写真を削除しても、ユーザー写真テンプレートが削除されない限り顔認証ができます。

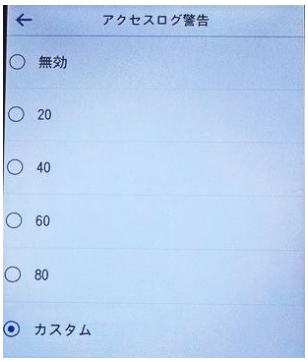
③ **英数字ユーザーID（初期値：ON）**

顔認証デバイス側でユーザー番号（ID）の入力できる文字の種類を設定できます。既に数字（OFF 設定）で登録済みのユーザーが存在している状態で、英数字（ON 設定）に変更しても既存ユーザー（OFF 設定）のユーザーに影響はありません。

※「英数字ユーザーID」を「ON」にする場合、事前に管理ソフト側の利用設定も「ON」にしてください。管理ソフト側の設定については「9.6.8 パラメータ」の「ユーザーID 設定」を参照してください。

| 設定値 | 説明 |
|---|---|
| OFF | 数字の入力ができます |
| ON | 英数字の入力ができます |

④ **アクセスログ警告（初期値：99／設定範囲：無効、1～9999）**




アクセス履歴の残りの保存数を設定することで顔認証デバイスの画面上に警告を表示します。100 万件の履歴が保存できますが、設定した値（残りの保存可能なアクセス履歴数）で画面上に警告を表示します。

⑤ **定期的にアクセスレコードを削除（初期値：無効／設定範囲：1～999）**

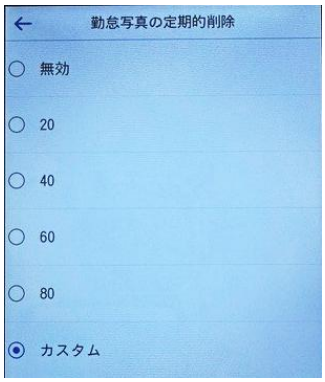
**※本設定は「無効」から設定範囲内で必ず設定をお願いします。**




アクセス履歴のデータを定期的に削除する設定です。認証時のアクセス履歴が上限に達した時に設定した値（レコード数）で古い履歴から一括削除して、デバイスの空き容量を確保します。なお、無効にした場合、最大保存件数（100 万件）まで保存されますが、新しいデータの記録ができなくなりますのでご注意ください。

⑥ **勤怠写真の定期的削除（初期値：99／設定範囲：無効、1～99）**

**※本設定は「無効」にせず、設定範囲内で必ず設定をお願いします。**

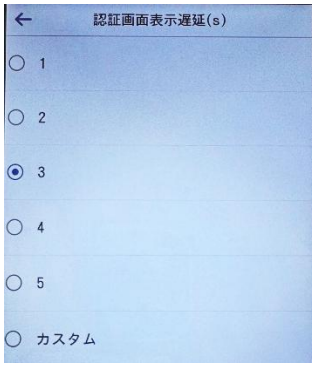



認証時の写真を定期的に削除する設定です。認証時の写真が上限に達した時に設定した値（レコード数）で古い写真から一括削除して、デバイスの空き容量を確保します。なお、無効にした場合、最大保存件数（7,500 件）まで保存されますが、新しいデータの記録ができなくなりますのでご注意ください。

⑦ **拒否リスト写真の定期的削除（初期値：99／設定範囲：無効、1～99）**

当社または本製品ではサポート対象外です。

⑧ **認証画面表示遅延(s)（初期値：3／設定範囲：無効、1～9）**

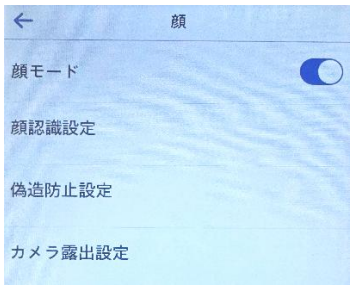



画面下に表示される認証結果の表示時間を設定できます。

## 5. 顔

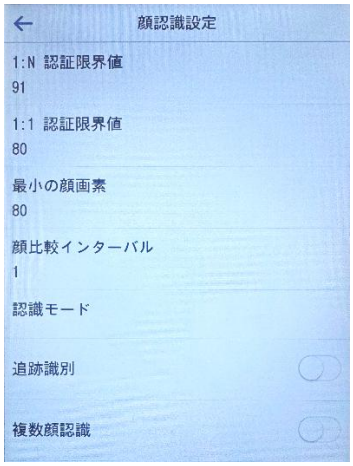
顔認証に関する閾値などの設定です。初期値は、顔認証アルゴリズムの観点から最良の数値を設定しています。

※認証関連の閾値は、原則、設定の変更は行わないようにお願いします。




| 項目名 | 説明 |
|---|---|
| 顔モード | 顔認証の ON/OFF を設定します。 |
| 顔認識設定 | 顔認証に関する詳細設定をします。 |
| 偽造防止設定 | 生体検知に関する設定をします。 |
| カメラ露出設定 | カメラの機能に関する設定をします。 |

### 5-1. 顔認識設定




| 項目名 | 説明 |
|---|---|
| 1:N 認証限界値 | 1:N 認証の閾値が設定できます。 |
| 1:1 認証限界値 | 1:1 認証の閾値が設定できます。 |
| 最小の顔画素数 | 登録と認証に必要な最小顔サイズを設定します。 |
| 顔比較インターバル | 顔認証間隔を設定します。 |
| 顔認証モード | — |
| 追跡識別 | 1 回の認証プロセスで 1 度だけ認証できます。 |
| 複数顔認識 | 一度に複数の顔を認識できます（最大 4 名）<br>※入退 Push および勤怠 Push の自動モードで利用できます。 |

#### ① 1:N 認証限界値（初期値：91／設定範囲：0～100）

1:N 認証における閾値です。数値を下げることで認証基準が緩くなります。数値を上げることで厳しくなります。

| 設定 | 認証時の動作内容 |
|---|---|
| 閾値を下げる | 他人として誤認証されやすくなります。（他人受入率が高くなります） |
| 閾値を上げる | 本人として認証され難くなります。（誤判定が低くなります／拒否率が高くなる） |

#### ② 1:1 認証限界値（初期値：80／設定範囲：0～100）

登録時、認証時ともに「デバイスに近づき、正面を向く」など、制約条件の厳しさを設定します。数値を下げることで認証基準が緩くなります。数値を上げることで厳しくなります。

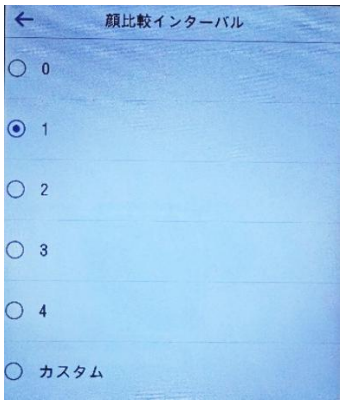
| 設定 | 認証時の動作内容 |
|---|---|
| 閾値を下げる | 他人として誤認証されやすくなります。（他人受入率が高くなります） |
| 閾値を上げる | 本人として認証され難くなります。（誤判定が低くなります／拒否率が高くなる） |

### ③ 最小の顔画素（初期値：80／設定範囲：0～180）

カメラに映った顔を認識するために必要な大きさの基準です。この値を調整することで顔認証距離を調整できます。

| 設定 | 認識される顔 | 認証距離 | 精度 | 使いやすさ |
|---|---|---|---|---|
| 閾値を下げる | 小さい | 遠い | 誤判定高い | 認証し易い |
| 閾値を上げる | 大きい | 近い | 誤判定低い | 認証し難い |

### ④ 顔比較インターバル*（初期値：1／設定範囲：0～9）




1 回目の顔認証から次の顔認証までの間隔（秒）を設定できます。

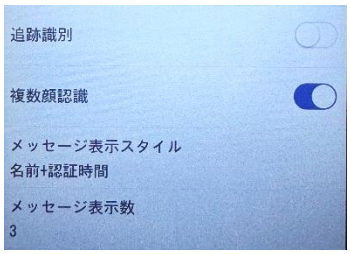
※一度の認証で 2 回続けて認証されてしまう場合、間隔（時間）を大きい数字に設定することで解決します。
※追跡識別が OFF の時に設定できます。

### ⑤ 追跡識別*（初期値：OFF）




連続認証を防止する機能です。設定を ON にすると、認証時にカメラに映った同じ顔は一度しか認識できません。再度認識させる場合は、一度顔認識エリアを離れてから再び顔認識エリアに入る必要があります。

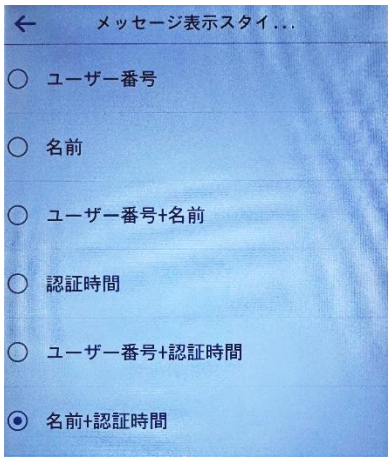
### ⑥ 複数顔認識（初期値：OFF） ※最大 4 人まで認証可能



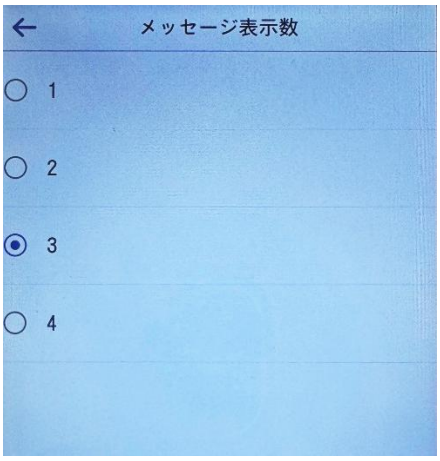

設定を ON にすると、カメラに映った複数の顔を一度に認識することができます。次項の「メッセージ表示スタイル」と「メッセージ表示件数」は、本機能を ON にした場合のみ設定できます。

※入退 Push および勤怠 Push の自動モードで利用できます。勤怠 Push のマニュアルモードは一人ひとり打刻ボタンをタップする運用のため利用できません。

**メッセージ表示スタイル（初期値：名前+認証時間）**
顔認証成功後、顔認証デバイスの画面内に映るユーザーの下に表示される情報を選択できます。




**メッセージ表示件数（初期値：3）**
顔認証デバイスの画面内の顔認証結果の表示数を選択できます。

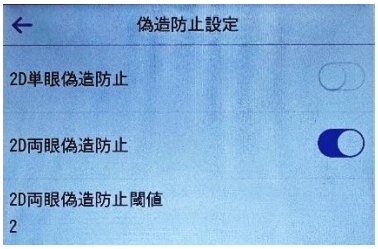



※「メッセージ表示スタイル」と「メッセージ表示件数」は、複数顔認識を ON にした場合のみ設定できます。

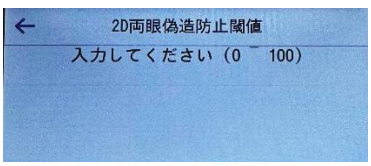
## 5-2. 偽造防止設定

① **2D 単眼偽造防止（初期値：OFF）**
可視光と認証アルゴリズムによる生体検知機能です。

② **2D 両眼偽造防止（初期値：ON）**
可視光と近赤外線を使用したなりすまし防止機能です。近赤外線ライトを使い、被写体の明暗（凹凸）を分析して生体検出をおこないます。太陽光など、近赤外線と同じ波長が顔認証デバイスに照射されている場合、本機能は利用できません。①の単眼偽造防止（生体検出機能）でなりすまし防止の対策をお願いします。




③ **2D 両眼偽造防止閾値（初期値：2／設定範囲：0～100）**
近赤外線による生体検知機能が ON の場合に設定できる閾値です。



### 5-3. カメラ露出設定

**① 顔認識エリア（初期値：OFF）**

オートエクスポージャー（露出補正）機能です。露出の高低に応じて自動補正をし、認証精度を高める機能です。

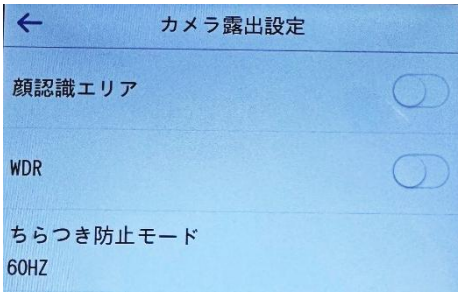
**② WDR（初期値：OFF）**

ワイドダイナミックレンジ（光補正）機能です。明るい場所、暗い場所で認証する時に認証精度を高める機能です。

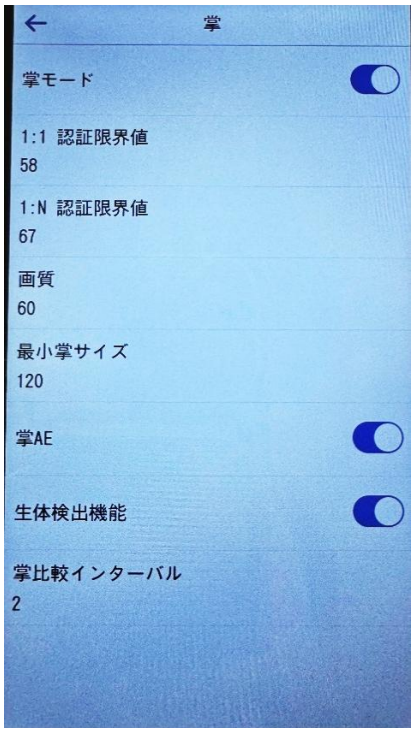
※設定変更を有効にするためには顔認証デバイスの再起動が必要です。

**③ ちらつき防止モード（初期値：50Hz／選択範囲：無効･50Hz･60Hz）**

本機能は②の WDR が OFF の時、50Hz･60Hz の外部光に対して顔認証時のスクリーンのちらつきを防止する機能です。




## 6. 掌




| 項目名 | 説明 |
|---|---|
| 掌モード | 掌認証の ON/OFF を設定します。 |
| 1:1 認証限界値 | 掌の 1:1 認証の閾値を設定します。 |
| 1:N 認証限界値 | 掌の 1:N 認証の閾値を設定します。 |
| 画質 | 掌の登録と認証を行うための画像品質です。 |
| 最小掌サイズ | 認証距離を調整します。 |
| 掌 AE | 掌の認識性能を向上します。 |
| 生体検出機能 | 近赤外線を使用した生体検知機能です。 |
| 掌比較インターバル | 掌の認証間隔を設定します。 |

① **1:1 掌限界値（初期値：58／設定範囲：0～1000）**

登録時、認証時ともに「デバイスに近づき、手のひらを正面に向ける」など、制約条件の厳しさを設定します。数値を下げることで認証基準が緩くなります。数値を上げることで厳しくなります。

② **1:N 掌限界値（初期値：67／設定範囲：0～1000）**

1:N 認証における閾値です。数値を下げることで認証基準が緩くなります。数値を上げることで厳しくなります。

| 設定 | 認証時の動作内容 |
|---|---|
| 閾値を下げる | 他人として誤認証されやすくなります。（他人受入率が高くなります） |
| 閾値を上げる | 本人として認証され難くなります。（誤判定が低くなります／拒否率が高くなる） |

③ **画質（初期値：60／設定範囲：0～100）**

掌の登録と認証を行うための画像品質を設定します。値が大きいほど、掌の画像の鮮明さが必要になります。

④ **最小掌サイズ（初期値：120／設定範囲：100～360）**

カメラに映った掌を認識するために必要な大きさの基準です。この値を調整することで掌認証距離を調整できます。

| 設定 | 認識される掌 | 認証距離 | 精度 | 使いやすさ |
|---|---|---|---|---|
| 閾値を下げる | 小さい | 遠い | 誤判定高い | 認証し易い |
| 閾値を上げる | 大きい | 近い | 誤判定低い | 認証し難い |

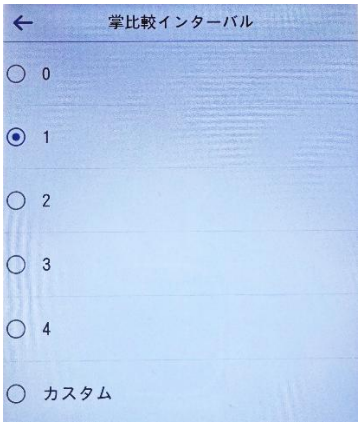
⑤ **掌 AE（初期値：ON）**

掌 AE モードで掌がカメラにかざすと、掌部分の明るさが増し、背景なのどの他の部分が暗くなります。これにより掌の認識精度が向上します。

⑥ **生体検出機能（初期値：ON）**

可視光と近赤外線を使用したなりすまし防止機能です。近赤外線ライトを使い、被写体の明暗（凹凸）を分析して生体検出をおこないます。太陽光など、近赤外線と同じ波長が顔認証デバイスに照射されている場合、本機能は利用できません。

⑦ **掌比較インターバル（初期値：1／設定範囲：0～9）**

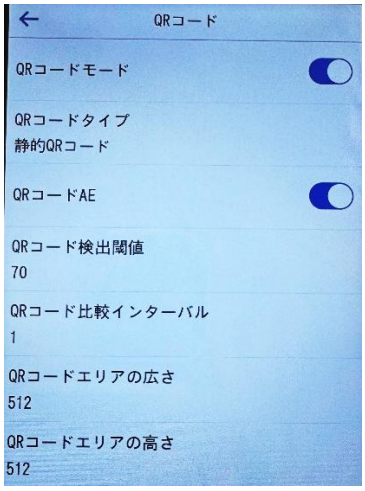



1 回目の掌認証から次の掌認証までの間隔（秒）を設定できます。

※一度の認証で 2 回続けて認証されてしまう場合、間隔（時間）を大きい数字に設定することで解決します。

## 7. QR コード（初期値：ON）

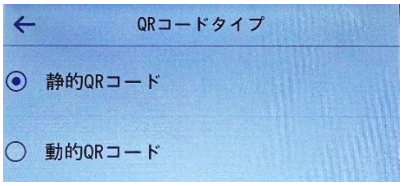
QR 認証に関する設定です。本製品は静的 QR のみ対応します。




| 項目名 | 説明 |
|---|---|
| QR コードモード | 機能の ON／OFF の設定をします。 |
| QR コードタイプ | 静的または動的の QR が選択できます。<br>※本製品は静的 QR のみ対応します。 |
| QR コード AE | QR の認識性能を向上します。 |
| QR コード検出閾値 | 近赤外線による偽造防止機能を調整します。 |
| QR コード比較インターバル | QR の認証間隔を設定します。 |
| QR コードエリアの広さ | QR を認識する幅を調整します。 |
| QR コードエリアの高さ | QR を認識する高さを調整します。 |

### ① QR コードタイプ（初期値：静的 QR コード／選択範囲：静的 QR コード･動的 QR コード）

QR 認証において読み取り可能な QR の種類を選択できます。ユーザー情報に紐づく QR を登録する場合、静的 QR で登録する必要があります。



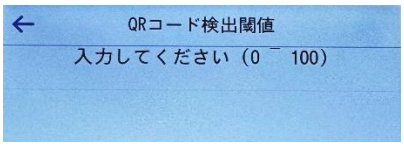

※本製品は静的 QR のみ対応します。

### ② QR コード AE（初期値：ON）

QR コードがカメラにかざすと、QR 部分の明るさが増し、背景などの他の部分は暗くなります。これにより QR の認識精度が向上します。

### ③ QR コード検出閾値（初期値：70／設定範囲：0～100）

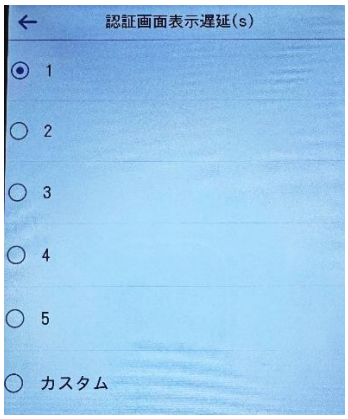
近赤外線スペクトル画像*が偽の写真や動画であるかどうかを判断するのに便利です。




| 設定 | 精度 |
|---|---|
| 閾値を下げる | 性能低下（緩い） |
| 閾値を上げる | 性能向上（厳しい） |

*目に見えない「近赤外線」の反射･吸収の違いを画像化したものです。

**④ QR コード比較インターバル（初期値：1／設定範囲：1～9）**




1 回目の顔認証から次の顔認証までの間隔（秒）を設定できます。

※一度の認証で 2 回続けて認証されてしまう場合、間隔（時間）を大きい数字に設定することで解決します。

**⑤ QR コードエリアの広さ（初期値：512／設定範囲：50～720）**

読み込み可能な QR コードの幅を調整します。初期値でご利用ください。

**⑥ QR コードエリアの高さ（初期値：512／設定範囲：50～1280）**

読み込み可能な QR コードの高さを調整します。初期値でご利用ください。

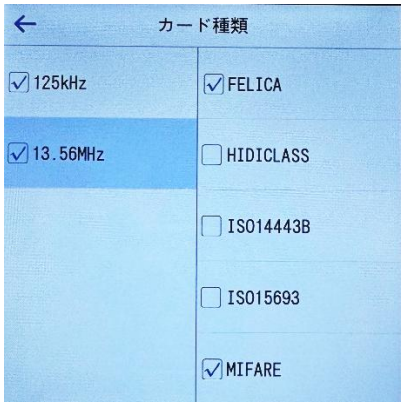
## 8. カード管理

使用する IC カードの種類を選択できます。使用しないカードを無効にすることでセキュリティを確保できます。

125kHz（低周波数帯）




13.56MHz（高周波数帯）




| 項目名 | 説明 |
|---|---|
| カード種類 | 読み取り可能なカードの種類を選択します。 |
| 125kHz | EM4102 |
| 13.56MHz | FELICA： |
| | HIDICLASS |
| | ISO14443B |
| | ISO15693 |
| | MIFARE |

**① 125kHz（初期値：ON）**

EM4102 の読み取り可否を設定します。

**② 13.56MHz（初期値：FELICA･MIFARE／選択範囲は＜ご参考＞を参照）**

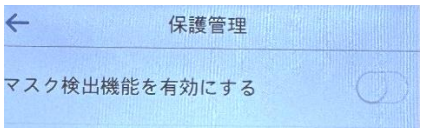
FeliCa などの読み取り可否を設定します。

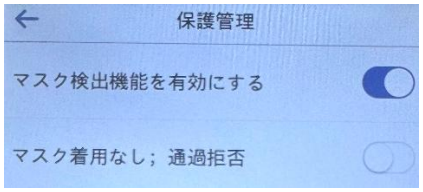
**<ご参考>**

| 種類 | 周波数 | 主な分類 | 特徴 | セキュリティ |
|---|---|---|---|---|
| **EM4102** | 125kHz | LF RFID | 固定 ID を読み取るシンプルなカード。読み取り専用が基本 | 低い |
| **MIFARE** | 13.56MHz | HF／ISO14443A 系 | 入退室、社員証、会員証などで広く利用。種類によりデータ書き込み可能 | 種類により中～高 |
| **FeliCa** | 13.56MHz | HF／独自方式 | 交通系 IC、電子マネー、社員証などで利用。高速通信が特徴 | 高め |
| **HID iCLASS** | 13.56MHz | HF／HID 系カード | HID 社の入退室管理向けカード。企業のセキュリティカードで多い | 種類により中～高 |
| **ISO14443B** | 13.56MHz | HF／近接型カード | ISO14443 規格の Type B。身分証、認証カード、IC カードで利用されることがある | 実装方式により異なる |
| **ISO15693** | 13.56MHz | HF／近傍型カード | ISO14443 より読み取り距離が長め。物流、図書館、物品管理、資産管理などで利用 | 実装方式により異なる |

## 9. 保護管理

マスク検出に関する設定です。機能を ON にすると詳細設定メニューが表示されます。




| 項目名 | 説明 |
|---|---|
| マスク検出機能を有効にする | 機能の ON／OFF を設定します。 |
| マスク着用なし：通過拒否 | マスク着用なしの場合、通過を拒否します。 |

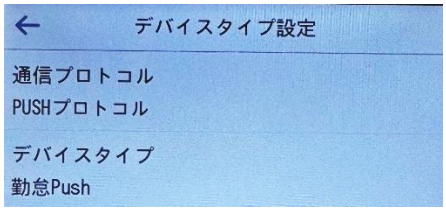
① **マスク検出機能を有効にする（初期値：OFF）**

マスク検出機能の ON/OFF を設定できます。ON にするとマスク着用で認証した場合、認証結果画面に「マスクを着用しています」と判定結果を表示します。マスク未着用で認証した場合、認証結果画面に「マスクがありません」の警告を表示します。

② **マスク着用なし：通過拒否（初期値：OFF）**

マスクを着用していない場合、通過を拒否する機能です。外部アラームと連動します。

## 10. デバイスタイプ設定




| 項目名 | 説明 |
|---|---|
| 通信プロトコル | PUSH プロトコル（固定値） |
| デバイスタイプ | 勤怠管理または入退室管理で利用する際のモードを選択できます。 |

### ① 通信プロトコル

顔認証デバイスと管理ソフト間で通信するためのプロトコルを表示しています。変更はできません。

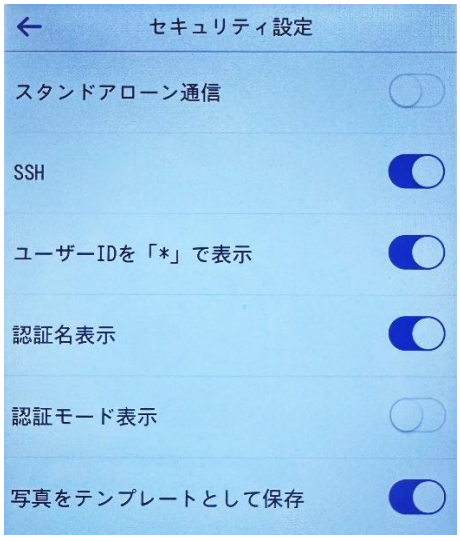
### ② デバイスタイプ（初期値：入退 Push）【重要】

顔認証デバイスを利用する際、用途に応じてモードを切り替えます。運用途中でモードを切り替えると、顔認証デバイスに保存されたデータ（ユーザー情報や履歴など）が削除されますので注意が必要です。但し、顔認証デバイスの設定情報は残ります。

| 用途 | 選択するモード |
|---|---|
| 入退室管理 | 入退 Push |
| 勤怠管理 | 勤怠 Push |

## 11. セキュリティ設定

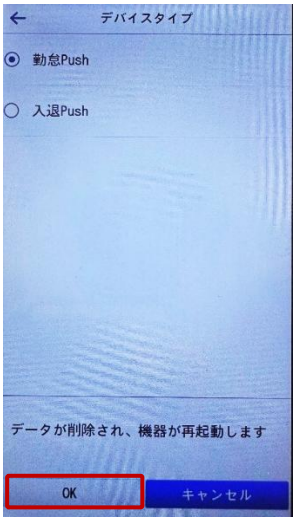
本設定は初期値で使用します。




| 項目名 | 説明 |
|---|---|
| スタンドアローン通信<br>（初期値：OFF） | 当社または本製品はサポート対象外です。 |
| SSH<br>（初期値：ON） | 当社または本製品はサポート対象外です。 |
| ユーザーID を「*」で表示<br>（初期値：ON） | 当社または本製品はサポート対象外です。 |
| 認証名表示<br>（初期値：ON） | 認証名を表示します。 |
| 認証モード表示<br>（初期値：OFF） | 端末画面に認証モードを表示します。 |
| 写真をテンプレートとして保存<br>（初期値：ON） | 顔認証アルゴリズム更新時に更新前の生体情報を継承します。OFF にすると顔情報の再登録が必要です。 |

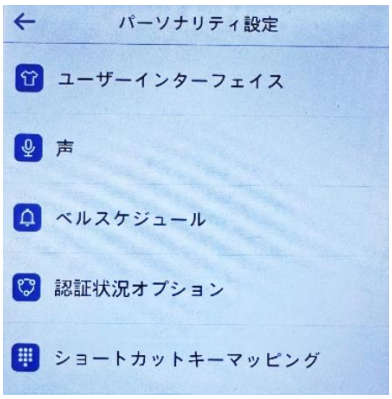
### 12. リセット

顔認証デバイスの設定情報を削除します。ユーザー情報など、記録された情報はリセットされません。ユーザー情報などの記録された情報を削除する場合は「10.6 データ管理」を参照してください。なお、顔認証デバイスの設定情報を削除するには「リセット」をタップし、「リセット？再起動」の表示が出たら「OK」をタップします。




## 10.5. パーソナリティ設定

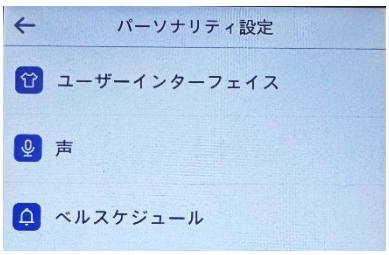
**勤怠 Push の表示**



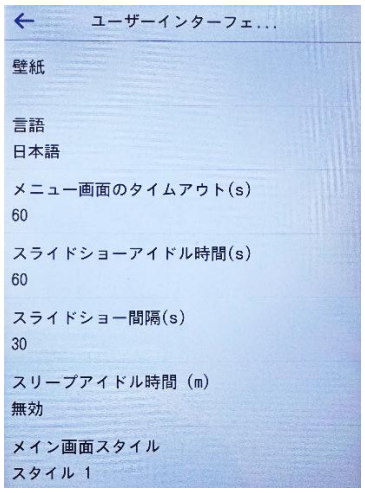

| 項目名 | 説明 |
|---|---|
| ユーザーインターフェイス | 画面表示やタイムアウトの設定をします。 |
| 声 | 音声やタッチ音、音量などを設定します。 |
| ベルスケジュール | スケジュール設定した時間に音を鳴らします。 |
| 認証状況オプション* | 勤怠種別の自動選択またはマニュアル選択を設定します。 |
| ショートカットキーマッピング* | マニュアル選択の内容をカスタマイズできます。<br>※基本は変更しないようにしてください |

*入退 Push のモードを選択している時は表示されません

**入退 Push の表示**



## 1. ユーザーインターフェイス




| 項目名 | 説明 |
|---|---|
| 壁紙 | 壁紙 2 種類（スタイル 1/2）を選択できます。 |
| 言語 | 日本語か英語か表示言語を選択できます。 |
| メニュー画面のタイムアウト(s) | メインメニューの表示時間を設定できます。 |
| スライドショーアイドル時間(s) | スクリーンセーバー起動までの時間を設定できます。 |
| スライドショー間隔(s) | スクリーンセーバーのスライドショーの変更間隔を設定できます。 |
| スリープアイドル時間(m) | スリープモードに入るまでの時間を設定できます。 |
| メイン画面スタイル | 待機画面を時計または打刻ボタンにするか選択できます。 |

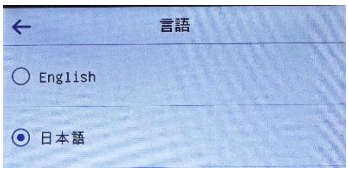
### ① 壁紙

顔認証デバイスの待機画面で表示する壁紙を選択できます。設定するには、使用したい壁紙をタップします。



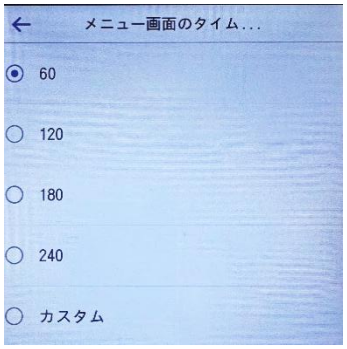

### ② 言語（初期値：日本語／選択範囲：日本語、英語（English））

日本語か英語か表示言語を選択できます。



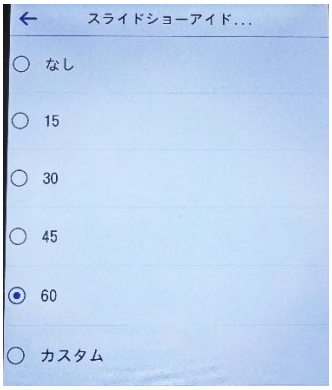
**③ メニュー画面のタイムアウト（s）（初期値：60s／設定範囲：無効、60～99999）**

メインメニューについて、無操作の状態が継続した時にタイムアウトする時間を設定できます。



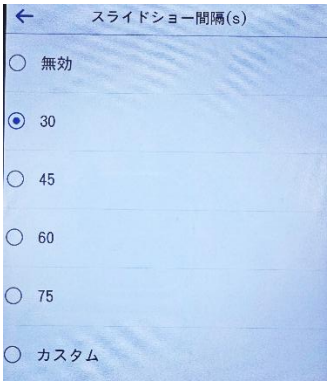

**④ スライドショーアイドル時間（s）（初期値：60s／設定範囲：なし、3～999）**

認証待機画面からスクリーンセーバー（スライドショー実行）画面に切り替えるまでの時間を設定できます。



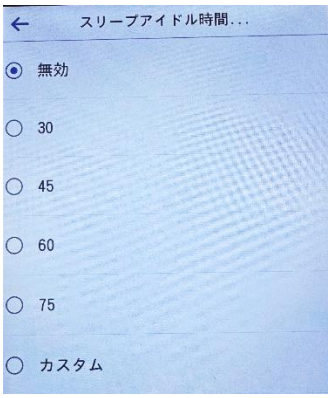

**⑤ スライドショー間隔（s）（初期値：30s／設定範囲：無効、3～999）**

スクリーンセーバー（スライドショー実行）において、画像を切り替えるまでの時間を設定できます。



⑥ **スリープアイドル時間（m）（初期値：無効／設定範囲：無効、1～999）**

カメラで人物を検知しない状態が継続した場合にスリープモードにすることができます。スリープモードに入るまでの時間を設定できます。




⑦ **メイン画面スタイル（初期値：スタイル 1 時計表示／選択範囲：スタイル 1 時計表示、スタイル 2 打刻ボタン表示）**

認証待機画面の表示スタイルを設定することができます。設定する場合は「＞＞」をタップして表示種類を切り替えます。最後に画面したにある「設定」をタップします。設定をしない場合は「戻る」をタップします。

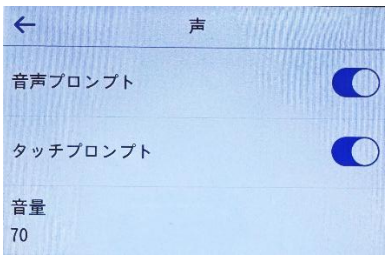
※勤怠管理、入退室管理において「スタイル 1 時計表示」で運用をお願いします。なお「スタイル 2 打刻ボタン表示」は、当社または本製品はサポート対象外です。







## 2. 声




| 項目名 | 説明 |
|---|---|
| 音声プロンプト | 音声案内を ON／OFF できます。 |
| タッチプロンプト | タッチ操作音を ON／OFF できます。 |
| 音量 | 音量を調整できます。 |

① **音声プロンプト（初期値：ON）**

音声による案内を ON／OFF する場合、「音声プロンプト」項目名や「ボタン」をタップします。

② **タッチプロンプト（初期値：ON）**

タッチ操作音を ON／OFF する場合、「タッチプロンプト」項目名や「ボタン」をタップします。

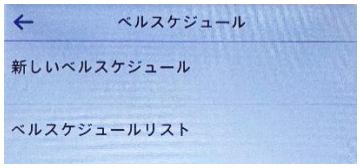
③ **音量（初期値：70）**

音声またはタッチ操作音のボリュームを調整することができます。ボリュームを変更する場合、音量調整ボタン（UP／DOWN）をタップして調整します。設定を反映するには「確認」をタップします。

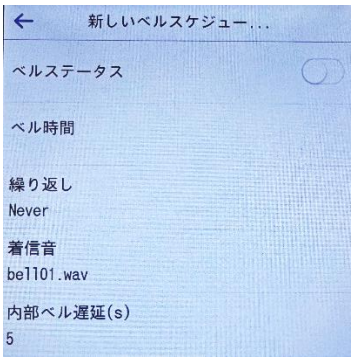



## 3. ベルスケジュール ※本機能は端末側のみで設定可能です

所定の時間でアラームを鳴らすことができます。また複数のスケジュールを作成して、1 日の中で複数回鳴らすこともできます。




| 項目名 | 説明 |
|---|---|
| 新しいベルスケジュール | 新しいベルスケジュールを作成します。 |
| ベルスケジュールリスト | 作成されたベルスケジュールを一覧表します。 |




| 項目名 | 説明 |
|---|---|
| ベルステータス | 設定したベルスケジュールを ON／OFF します。 |
| ベル時間 | ベルを鳴らす時間を設定します。 |
| 繰り返し | ベルを鳴らす曜日を選択します。 |
| 着信音 | 音の種類を選択します。 |
| 内部ベル遅延（s） | 設定時間後何秒でベルを鳴らすか設定します。 |

① **新しいベルスケジュール**

新規にベルを鳴らすスケジュールを作成します。作成する場合、「新しいベルスケジュール」項目名をタップします。

**(ア) ベルステータス（初期値：OFF）**

有効にする場合は「ON」にします。ベルスケジュールを一時的に OFF にする場合も本設定で操作します。

**(イ) ベル時間**

ベルを鳴らす時間を UP／DOWN をタップして設定します。設定を反映するには「確認」をタップします。



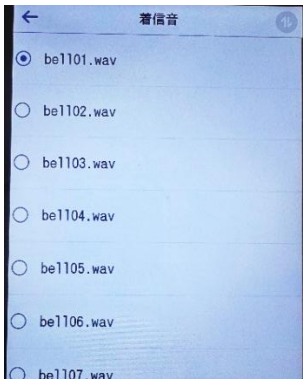

**(ウ) 繰り返し（初期値：Naver／選択範囲：月曜日～日曜日）**

ベルを鳴らす曜日を選択できます。ベルを鳴らしたい曜日にチェックボックスを入れ、最後に「戻る」をタップします。



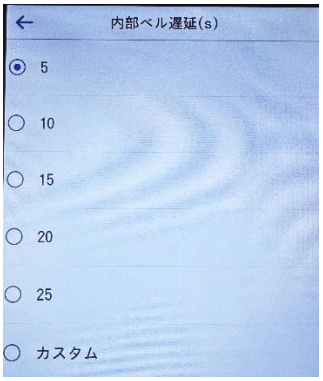

**(エ) 着信音（初期値：be1101.wav／選択範囲：10 種類）**

ベルの種類を選択できます。項目名をタップすると選択と同時にベルの音を確認できます。



**（オ）内部ベル遅延（s）（初期値：5／設定範囲：1～999）**

指定時間からベルを鳴らすタイミングを設定できます。

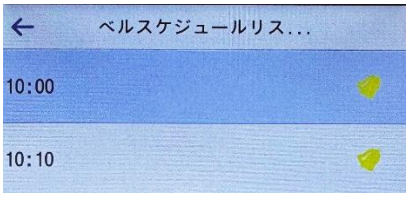


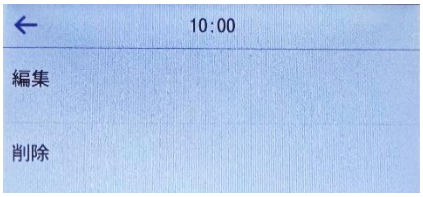

※作成したスケジュールは「ベルスケジュールリスト」で確認できます。

**② ベルスケジュールリスト**

作成されたベルスケジュールを一覧表示します。一覧の中からベルスケジュールを選択して、編集または削除ができます。

「編集」する場合、編集したいベルスケジュールをタップし、①の「ア」からの手順を行なってください。

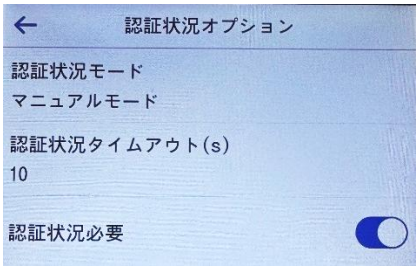



※設定期間が経過したスケジュールリストは「ベル」アイコンがグレーアウトします。

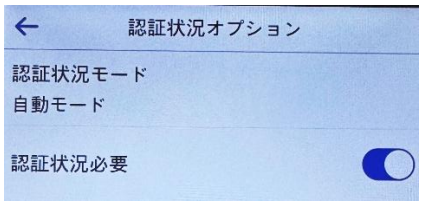
※ベルスケジュールが設定されている場合、認証待機画面の右上に「」が表示されます。

## 4. 認証状況オプション ※入退 Push のモードに設定されたデバイスには表示されません




| 項目名 | 説明 |
|---|---|
| 認証状況モード | 認証モード（打刻方法）を切り替えます |
| 認証状況タイムアウト（s）＊ | 勤怠種別の選択可能な時間を設定します。 |
| 認証状況必要 | 打刻ボタンの表示／非表示を設定します。 |

＊自動モードを選択している時は表示されません

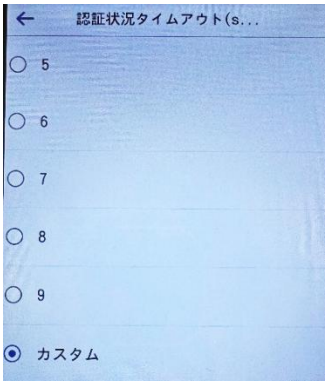


① 認証状況モード（初期値：マニュアルモード（勤怠 Push）、オフ（入退 Push）／設定範囲：オフ、マニュアルモード、自動モード）

勤怠種別の入力方法を選択します。

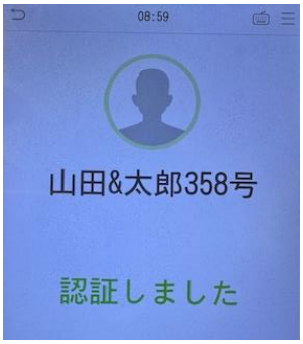
| モードの種類 | 打刻方法 |
|---|---|
| オフ | 認証状況モードを ON/OFF に設定します。 |
| マニュアルモード（推奨／初期値） | 勤怠種別をタップし、タップした日時で打刻します。 |
| 自動モード | 顔認証日時で打刻します。 |

② 認証状況タイムアウト（s）（初期値：10s／設定範囲：5～999）
勤怠種別を選択できる時間（表示時間）を設定できます。

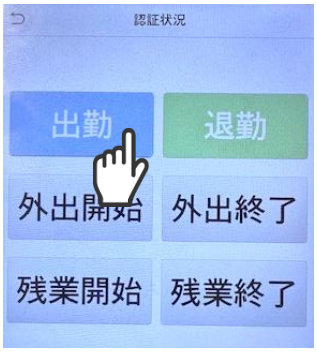



③ 認証状況必要（初期値：ON）
顔認証で PASS した時に勤怠種別のボタンを表示します。

1．認証完了




2．打刻ボタンをタップ




3．打刻の受付完了

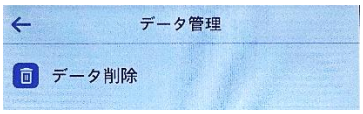



**5. ショートカットキーマッピング** ※入退 Push のモードに設定されたデバイスには表示されません
管理ソフトで設定した値が反映されます。設定は管理ソフトの「7.4 打刻方法の設定」を参照してください。なお、管理ソフトでの設定以外はサポート対象外です。

## 10.6. データ管理

顔認証デバイス内に保存された各種データ（履歴、写真、ユーザー情報など）を削除するメニューです。削除したデータは端末に復元することはできません。過去の各種データは管理ソフトから確認します。

データ管理



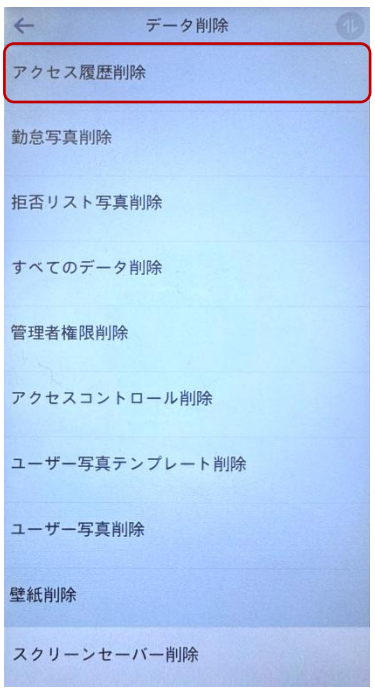

| 項目名 | 説明 |
|---|---|
| データ削除 | — |

勤怠 Push




| 項目名 | 説明 |
|---|---|
| 勤怠データ削除* | 勤怠履歴を一括または期間指定で削除します。 |
| アクセス履歴削除* | アクセス履歴を一括または期間指定で削除します。 |
| 勤怠写真削除 | 勤怠写真を一括または期間指定で削除します。 |
| 拒否リスト写真削除 | 拒否リスト写真を一括または期間指定で削除します。 |
| すべてのデータ削除 | スクリーンセーバー・壁紙以外の全てのユーザー関連含めた情報を削除します。 |
| 管理者権限削除 | 全ユーザーの管理者権限を削除します。 |
| アクセスコントロール削除 | アクセスコントロールの設定情報を削除します。 |
| ユーザー写真テンプレート削除 | ユーザー写真テンプレートを削除します。（削除は推奨しません） |
| ユーザー写真削除 | 認証時表示用の顔写真を削除します。 |
| 壁紙削除 | 壁紙を選択して削除します。（削除したら復元はできません） |
| スクリーンセーバー削除 | スクリーンセーバーを選択して削除します。（削除したら復元はできません） |

入退 Push



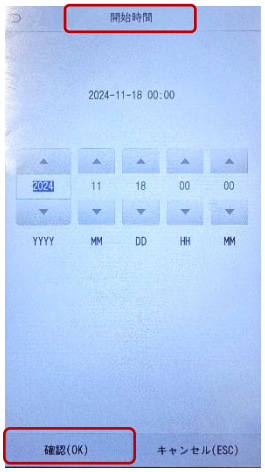

*「勤怠データ削除」または「アクセス履歴削除」は、「デバイスタイプ設定」で選択したモードにより表示されるメニューが異なります。

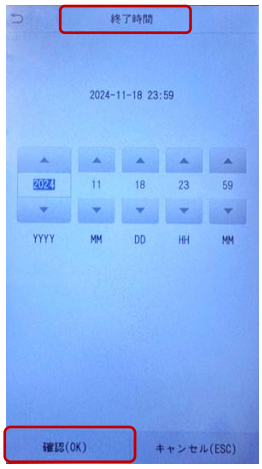
| デバイスタイプ | 表示されるメニュー |
|---|---|
| 勤怠 Push | 勤怠データ削除 |
| 入退 Push | アクセス履歴削除 |

## 1. 勤怠データ削除 ※勤怠 Push 専用メニュー

勤怠データを削除することができます。記録の一括削除または期間指定で削除できます。期間指定をする場合、最初に開始期間→「確認（OK）」、次に終了期間→「確認（OK）」をタップします。最後に「勤怠データ削除？」の表示がされますので「OK」をタップします。



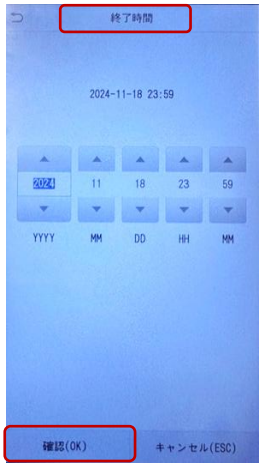

## 2. アクセス履歴削除 ※入退 Push 専用メニュー

アクセス履歴を削除することができます。記録の一括削除または期間指定で削除できます。期間指定をする場合、最初に開始期間→「確認（OK）」、次に終了期間→「確認（OK）」をタップします。最後に「アクセス履歴削除？」の表示がされますので「OK」をタップします。









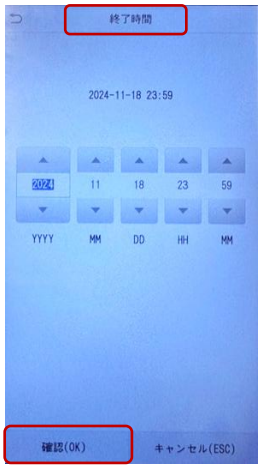
### 3. 勤怠写真削除

認証時の写真を削除します。記録の一括削除または期間指定で削除できます。期間指定をする場合、最初に開始期間→「確認（OK）」、次に終了期間→「確認（OK）」をタップします。最後に「勤怠写真削除？」の表示がされますので「OK」をタップします。









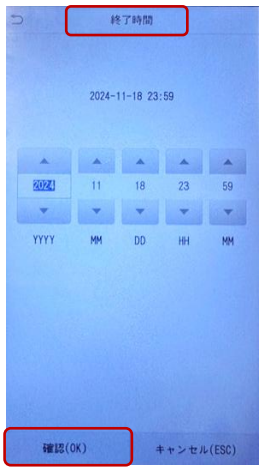

### 4. 拒否リスト写真削除

拒否リストで撮影された写真を削除します。記録の一括削除または期間指定で削除できます。期間指定をする場合、最初に開始期間→「確認（OK）」、次に終了期間→「確認（OK）」をタップします。最後に「拒否リスト写真削除？」の表示がされますので「OK」をタップします。










### 5. すべてのデータ削除

スクリーンセーバー、壁紙以外の全てのユーザー関連の情報を削除します。削除をする場合は「すべてのデータ削除」をタップします。「すべてのデータ削除？」の表示がされますので「OK」をタップします。削除されたデータは復元するこはできません。

### 6. 管理者権限削除

全てのユーザーの管理者権限を削除します。スーパー管理者およびカスタム権限も削除され、全てのユーザーは初期値の「普通ユーザー」の権限が付与されます。削除をする場合は「管理者権限削除」をタップします。「管理者権限削除？」の表示がされますので「OK」をタップします。

**7. アクセスコントロール削除**

アクセスコントロールで設定した情報を削除します。削除をする場合は「アクセスコントロール削除」をタップします。「アクセスコントロール削除？」の表示がされますので「OK」をタップします。

**8. ユーザー写真テンプレート削除**

データベース化された認証用データ（特徴点など）を削除します。削除をする場合は「ユーザー写真テンプレート削除」をタップします。警告メッセージが表示されますので、確認の上「OK」をタップします。削除されたデータは復元することはできません。

※削除は推奨しません。万が一、削除してしまった場合は、再度顔登録をしてください。

**9. ユーザー写真削除**

認証時に表示する顔写真を削除します。削除をする場合は「ユーザー写真削除」をタップします。「ユーザー写真削除？」の表示がされますので「OK」をタップします。削除されたデータは復元することはできません。

**10. 壁紙削除**

待機画面で表示する壁紙を削除します。削除をする場合は「壁紙削除」をタップします。削除したい壁紙を選択して「選択した画像削除」または「すべての画像削除」を選択します。最後に確認メッセージが表示されますので「OK」をタップします。削除されたデータは復元することはできません。

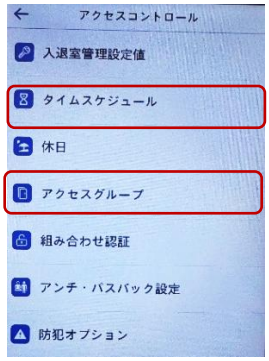
**11. スクリーンセーバー削除**

スクリーンセーバーで表示する画像を削除します。削除をする場合は「スクリーンセーバー削除」をタップします。削除したいスクリーンセーバーを選択して「選択した画像削除」または「すべての画像削除」を選択します。最後に確認メッセージが表示されますので「OK」をタップします。削除されたデータは復元することはできません。

## 10.7. アクセスコントロール

入退室管理における顔認証デバイス側の設定を行うことができます。

勤怠 Push




入退 Push



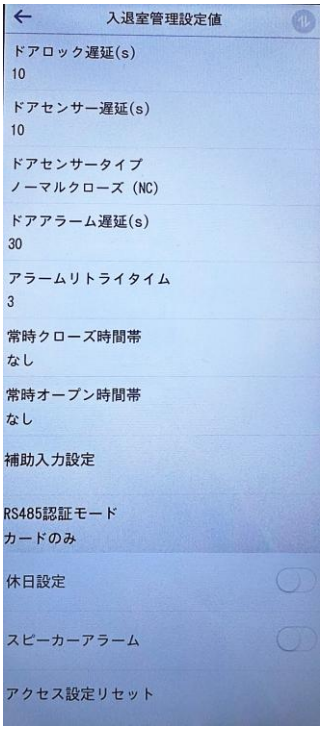

| 項目名 | 説明 |
|---|---|
| 入退室管理設定値 | 入退室管理における値を設定します。 |
| タイムスケジュール* | 管理ソフトで設定します。初期値でご利用ください。 |
| 時間ルール設定* | 管理ソフトで設定します。初期値でご利用ください。 |
| 休日 | 当社または本製品はサポート対象外です。 |
| アクセスグループ* | 当社または本製品はサポート対象外です。 |
| 組み合わせ認証 | 当社または本製品はサポート対象外です。 |
| アンチ・パスバック設定 | 管理ソフトで設定します。初期値でご利用ください。 |
| 防犯オプション | 防犯用の機能を設定します。 |

*「タイムスケジュール」「時間ルール設定」「アクセスグループ」は、「デバイスタイプ設定」で選択したモードにより表示されるメニューが異なります。

| デバイスタイプ | 表示されるメニュー |
|---|---|
| 勤怠 Push | タイムスケジュール、アクセスグループ |
| 入退 Push | 時間ルール設定 |

### 1. 入退室管理設定値

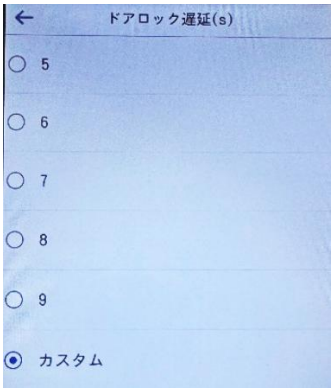
#### 1－1. 勤怠 Push




| 項目名 | 説明 |
|---|---|
| ドアロック遅延（s） | 電気錠制御におけるロック解除時間を設定します。 |
| ドアセンサー遅延（s） | ドアセンサーを制御している場合、開放アラーム送信までの時間を設定します。 |
| ドアセンサータイプ | 外部接続機器の接続方式を選択します。 |
| ドアアラーム遅延（s） | ドアセンサー遅延によって送信されたアラームの継続時間を設定します。 |
| アラームリトライタイム | ドアセンサー遅延によって送信されたアラームを何回繰り返すのかを設定します。 |
| 常時クローズ時間帯 | ドア施錠時間を入退室管理のタイムゾーンで設定します。 |
| 常時オープン時間帯 | ドア解錠時間を入退室管理のタイムゾーンで設定します。 |
| 補助入力設定 | AUX ポートを用いて外部装置から解錠・アラーム指示を受ける設定をします。 |
| RS485 認証モード | 当社または本製品はサポート対象外です。 |
| 休日設定 | 休日設定でアクセス時間外の認証を制御します。 |
| スピーカーアラーム | 認証が無いのにドアが開閉した時にアラームを発出します。（認証せずにドアを開けた時など） |
| アクセス設定リセット | 入退室管理設定値を初期値に戻します。 |

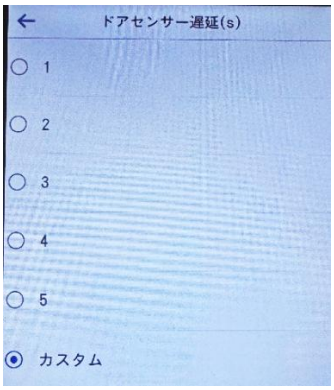
**① ドアロック遅延（s）（初期値：10s／設定範囲：1～10）**

顔認証デバイスが電子錠を制御している場合、ロックを解除しておく時間を設定します。




**② ドアセンサー遅延（s）（初期値：10s／設定範囲：1～255）**

顔認証デバイスが電子錠を制御している場合、ドアの開閉を検知するドアセンサーとの連動で使用します。ドアがロックされておらず一定時間開いた状態になっている時にアラームが送信されるまでの時間を設定します。

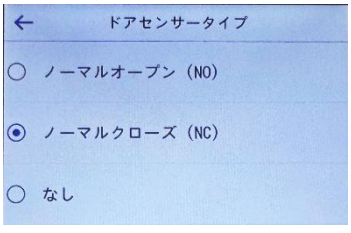



**③ ドアセンサータイプ（初期値：なし／選択範囲：下表参照）**

顔認証デバイスに外部接続機器（電子錠など）を接続している場合、通常時の動作モードを選択します。

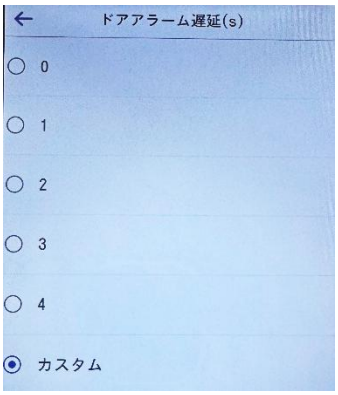
※外部接続機器が接続されていない場合は「なし」を選択します。

| モードの種類 | ロックの状態 |
|---|---|
| ノーマルオープン（NO） | 通常時オープンされている外部機器を接続する場合に選択 |
| ノーマルクローズ（NC） | 通常時ロックされている外部機器を接続する場合に選択 |
| なし | — |



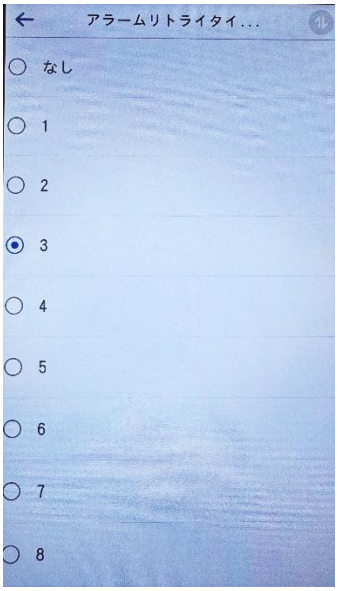
**④ ドアアラーム遅延（s）（初期値：30s／設定範囲：0～999）**

本機能は②の「ドアセンサー遅延」によって送信されたアラームの継続時間を設定できます。



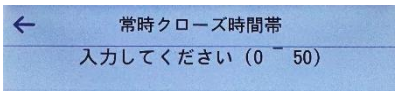

**⑤ アラームリトライタイム（初期値：3）／選択範囲：なし～9）**

本機能は②の「ドアセンサー遅延」によって送信された④の「ドアアラーム遅延」の繰り返す回数を設定できます。例えば、ドアアラーム遅延「30s」、アラームリトライタイムを「3 回」とした場合、30s×3 回＝90s の間アラームが継続します。本例は、ドアアラーム遅延を「90s」、アラームリトライタイムを「なし」に設定した時間と同じになります。



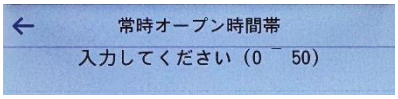

**⑥ 常時クローズ時間帯（初期値：なし／設定範囲：0～50）**

ドア解錠時間を入退室管理のタイムゾーンで設定します。設定した時間で常時ドアを施錠します。



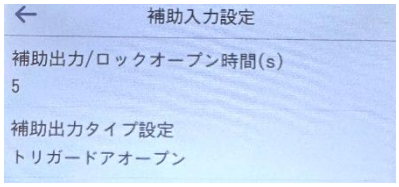
**⑦ 常時オープン時間帯（初期値：なし／設定範囲：0～50）**

ドア解錠時間を入退室管理のタイムゾーンで設定します。設定した時間で常時ドアを解錠します。




**⑧ 補助入力設定**

AUX ポートに接続している外部装置から解錠・アラームの指示（信号）を受ける時の各種設定ができます。




| 項目名 | 説明 |
|---|---|
| 補助出力/ロックオープン時間（s） | 外部措置から指示（信号）を継続する時間を設定します。 |
| 補助出力タイプ設定 | 顔認証デバイスへ接続する外部装置の種類を選択します。 |

**補助出力/ロックオープン（初期値：5s／設定範囲：1～255）**

AUX ポートに接続している外部装置から解錠・アラームの指示（信号）を継続する時間を設定します

**補助出力タイプ設定（初期値：トリガードアオープン／選択範囲：下表参照）**

顔認証デバイスへ接続する外部装置の種類を選択します。

| No | 補助出力タイプ | AUX ポートに接続している外部装置の例 |
|---|---|---|
| 1 | トリガードアオープン | ドアの開放を知らせる外部装置（例：ドア開閉センサーなど） |
| 2 | トリガーアラーム | アラームを送信する外部装置（例：火災報知器など） |
| 3 | トリガードアオープンおよびアラーム | No1 と No2 の両方 |

**⑨ RS485 認証モード（初期値：カードのみ／選択範囲：カードのみ・カード＋パスワード）**

当社または本製品はサポート対象外です。

**⑩ 休日設定（初期値：OFF）**

当社または本製品はサポート対象外です。

**⑪ スピーカーアラーム（初期値：OFF）**

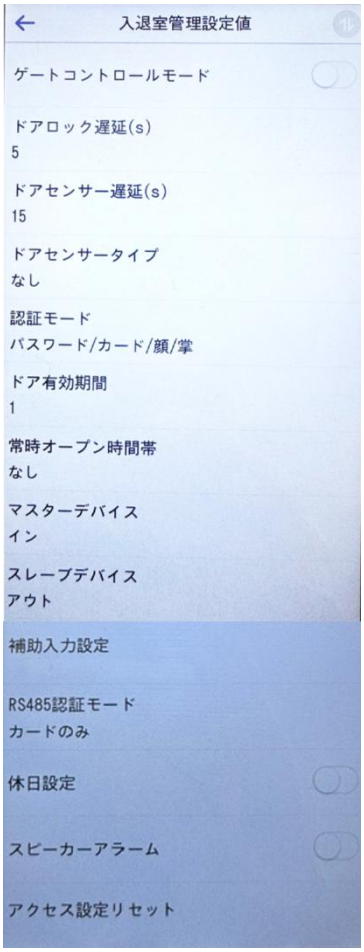
認証がされていない状態でドアが開閉した時にアラームを送信します。

**⑫ アクセス設定リセット**

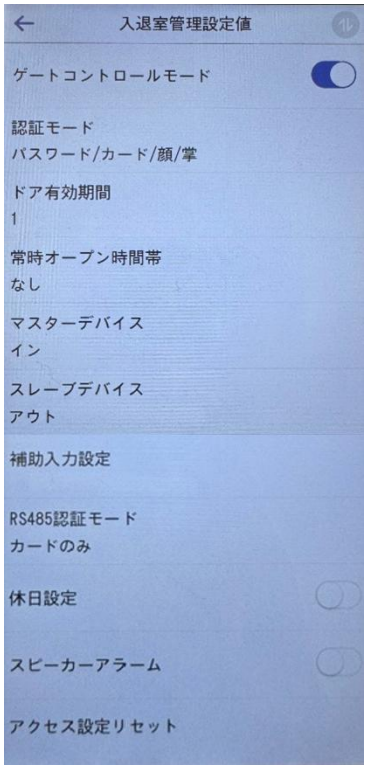
「入退室管理設定値」で設定変更されている値を初期値に戻します。リセットする場合は「アクセス設定リセット」をタップします。「再起動して有効にしますか？」の表示がされるので「OK」をタップします。顔認証デバイスが再起動し、リセットが完了します。

## 1－2. 入退 Push

ゲートコントロールモード：OFF




ゲートコントロールモード：ON

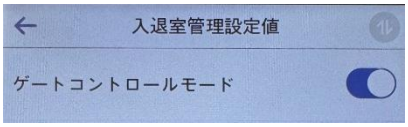



| 項目名 | 説明 |
|---|---|
| ゲートコントロールモード | フラッパーゲートを接続する際に選択します。 |
| ドアロック遅延（s）* | 電気錠制御におけるロック解除時間を設定します。 |
| ドアセンサー遅延（s）* | ドアセンサーを制御している場合、開放アラーム送信までの時間を設定します。 |
| ドアセンサータイプ* | 外部接続機器の接続方式を選択します。 |
| 認証モード | 管理ソフトで設定します。初期値でご利用ください。 |
| ドア有効期間 | 管理ソフトで設定します。初期値でご利用ください。 |
| 常時オープン時間帯 | 管理ソフトで設定します。初期値でご利用ください。 |
| マスターデバイス | 管理ソフトで設定します。初期値でご利用ください。 |
| スレーブデバイス | 管理ソフトで設定します。初期値でご利用ください。 |
| 補助入力設定 | AUX ポートを用いて外部装置から解錠・アラーム指示を受ける設定をします。 |
| RS485 認証モード | 当社または本製品はサポート対象外です。 |
| スピーカーアラーム | 認証が無いのにドアが開閉した時にアラームを発出します。（認証せずにドアを開けた時など） |
| アクセス設定リセット | 入退室管理設定値およびアクセス設定を初期値に戻します。 |

*ゲートコントロールモードを ON にすると表示が消えます。

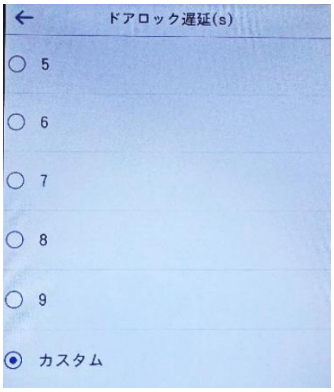
**① ゲートコントロールモード（初期値：OFF）**

顔認証デバイスをフラッパーゲートと接続する時に選択します。ゲートコントロールモードを ON にすると「ドアロック遅延／ドアセンサー遅延／ドアセンサータイプ」の表示が消えます。また、「アクセス設定リセット」を行なっても初期値には戻りません。



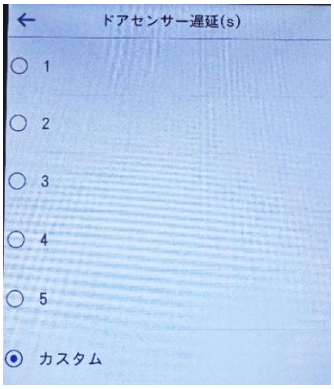

**② ドアロック遅延（s）（初期値：5s／設定範囲：1～99）**

顔認証デバイスが電子錠を制御している場合、ロックを解除しておく時間を設定します。




**③ ドアセンサー遅延（s）（初期値：10s／設定範囲：1～255）**

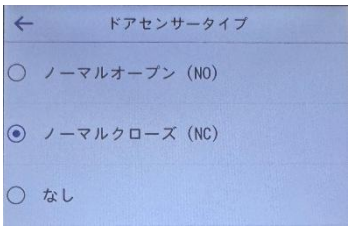
顔認証デバイスが電子錠を制御している場合、ドアの開閉を検知するドアセンサーとの連動で使用します。ドアがロックされておらず一定時間開いた状態になっている時にアラームが送信されるまでの時間を設定します。



④ **ドアセンサータイプ（初期値：なし／選択範囲：下表参照）**

顔認証デバイスにドアセンサーを接続している場合、通常時のドア開閉の状態に応じて動作モードを選択します。

| モードの種類 | ロックの状態 |
|---|---|
| ノーマルオープン（NO） | 通常時オープンされている電子錠を接続する場合に選択 |
| ノーマルクローズ（NC） | 通常時ロックされている電子錠を接続する場合に選択 |




⑤ **認証モード（初期値：パスワード･カード･顔･掌／選択範囲：12 種類）**

管理ソフトの「入退室管理 / アクセスデバイス / ドア」で設定した認証モードを端末へ反映します。初期値でご利用ください。

⑥ **ドア有効期間（初期値：1）**

管理ソフトの「入退室管理 / アクセスデバイス / ドア」で設定した有効タイムゾーンを端末へ反映します。初期値でご利用ください。時間帯でアクセス制限をする場合は「9.17.3 グループ登録」で設定してください。

⑦ **常時オープン時間帯（初期値：なし）**

管理ソフトの「入退室管理 / アクセスデバイス / ドア」で設定した「自動解錠タイムゾーン」を端末へ反映します。

⑧ **マスターデバイス（初期値：イン）**

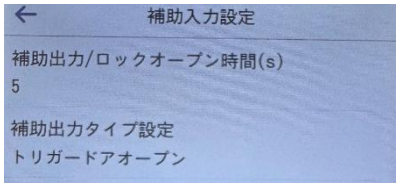
管理ソフトの「入退室管理 / アクセスデバイス / ドア」で設定した「ホストアクセスステータス」を端末へ反映します。

⑨ **スレーブデバイス（初期値：アウト）**

管理ソフトの「入退室管理 / アクセスデバイス / ドア」で設定した「スレーブステート」を端末へ反映します。

⑩ **補助入力設定**

AUX ポートに接続している外部装置から解錠･アラームの指示（信号）を受ける時の各種設定ができます。




| 項目名 | 説明 |
|---|---|
| 補助出力/ロックオープン時間（s） | 外部措置から指示（信号）を継続する時間を設定します。 |
| 補助出力タイプ設定 | 顔認証デバイスへ接続する外部装置の種類を選択します。 |

**補助出力/ロックオープン（初期値：5s／設定範囲：1～255）**

AUX ポートに接続している外部装置から解錠･アラームの指示（信号）を継続する時間を設定します

**補助出力タイプ設定（初期値：トリガードアオープン／選択範囲：下表参照）**
顔認証デバイスへ接続する外部装置の種類を選択します。

| No | 補助出力タイプ | AUX ポートに接続している外部装置の例 |
|---|---|---|
| 1 | トリガードアオープン | ドアの開放を知らせる外部装置（例：ドア開閉センサーなど） |
| 2 | トリガーアラーム | アラームを送信する外部装置（例：火災報知器など） |
| 3 | トリガードアオープンおよびアラーム | No1 と No2 の両方 |

⑪ **RS485 認証モード（初期値：カードのみ）**
当社または本製品はサポート対象外です。

⑫ **スピーカーアラーム（初期値：OFF）**
認証がされていない状態でドアが開閉した時にアラームを送信します。

⑬ **アクセス設定リセット**
「入退室管理設定値」で設定変更されている値および端末への「アクセス設定」を初期値に戻します。リセットする場合は「アクセス設定リセット」をタップします。「再起動して有効にしますか？」の表示がされるので「OK」をタップします。顔認証デバイスが再起動し、リセットが完了します。
※管理ソフトで設定した「アクセス設定」も初期化されるため認証できなくなります。再度、管理ソフトの「入退室管理 ＞ アクセスデバイス ＞ デバイス管理」の「デバイス管理 ＞ 全データをデバイスに同期（"同期する前にデバイスのデータを削除してください"をチェックする）」を行なってアクセス権限情報の同期を行なってください。

**2. タイムスケジュール** ※勤怠 Push 専用メニュー
管理ソフトの「入退室管理 / アクセスルール / タイムゾーン」で設定した「タイムゾーン」を端末へ反映します。初期値でご利用ください。

**3. 時間ルール設定** ※入退 Push 専用メニュー
管理ソフトの「入退室管理 / アクセスルール / タイムゾーン」で設定した「タイムゾーン」及び「入退室管理 / アクセスデバイス / ドア」で設定した「ドア」を端末へ反映します。初期値でご利用ください。

**4. 休日**
当社または本製品はサポート対象外です。

**5. アクセスグループ** ※勤怠 Push 専用メニュー
当社または本製品はサポート対象外です。

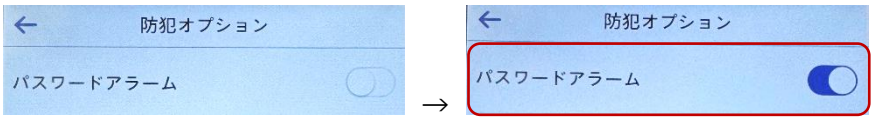
**6. 組み合わせ認証**
当社または本製品ではサポート対象外です。

**7. アンチ・パスバック設定**
管理ソフトの「入退室管理 / アクセスルール / アンチ・パスバック」で設定した「アンチ・パスバック」を端末へ反映します。初期値でご利用ください。

## 8. 防犯オプション

### ① パスワードアラーム（初期値：OFF）

パスワードアラームを有効にすると、パスワード認証の際に「非常解錠アラーム」が生成され管理ソフト（アラームモニタリングなど）へ記録されます。有効にする場合は「パスワードアラーム」を「ON」にします。



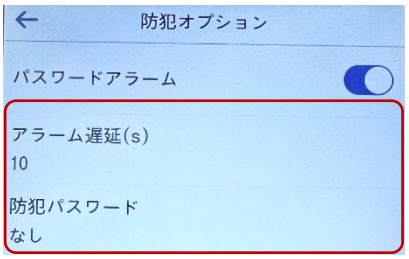

### ② アラーム遅延（初期値：10s／設定範囲：1～999）

アラーム遅延時間が経過するまで「非常解錠アラーム」は送信されません。

### ③ 防犯パスワード（初期値：なし／設定範囲：数字 6 桁） ※入退 Push 専用メニュー

本機能で設定した防犯パスワード（管理ソフトでは「非常パスワード」という）を、ユーザー認証の時に入力すると「非常解錠アラーム」が生成され管理ソフト（アラームモニタリングなど）へ記録されます。

例えば、何らかの理由で登録ユーザー以外の未登録ユーザーによって入室を強要されている場合、防犯パスワードを入力することで管理ソフト（管理者）へ通知を行うことができます。なお、ユーザー個別に設定したパスワードによる認証ではアラームは送信されません。




※防犯パスワードは「パスワードアラーム」が「OFF」でも動作します。

※防犯パスワードが顔認証デバイスで入力されると、管理ソフトの「アラームモニタリング」に通知されます。「8.8 アラームモニタリング」の手順に従って確認をします。

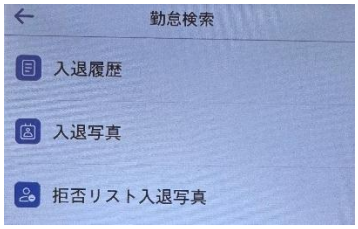
**通知例）**



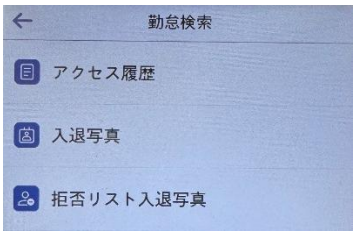
## 10.8. 勤怠検索

顔認証デバイス上でユーザー番号や期間を指定して履歴を確認することができます。

**勤怠 Push**




**入退 Push**




| 項目名 | 説明 |
|---|---|
| 入退履歴* | 入退履歴を検索します。 |
| アクセス履歴* | アクセス履歴を検索します。 |
| 入退写真 | 入退の認証時顔写真を検索します。 |
| 拒否リスト入退写真 | サポート対象外です。初期値でご利用ください。 |

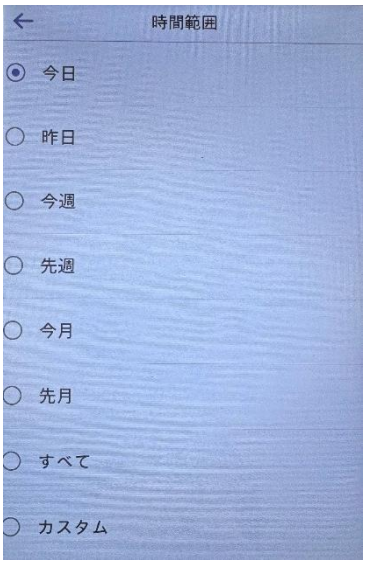
*「入退履歴」「アクセス履歴」は、「デバイスタイプ設定」で選択したモードにより表示されるメニューが異なります。

| デバイスタイプ | 表示されるメニュー |
|---|---|
| 勤怠 Push | 入退履歴 |
| 入退 Push | アクセス履歴 |

### 1. 入退履歴／アクセス履歴

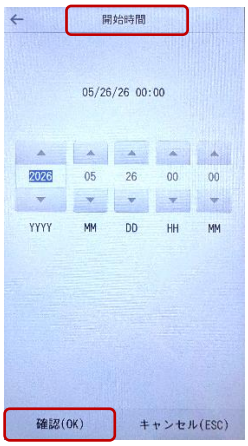
入退履歴／アクセス履歴について、検索範囲を指定して検索することができます。また、ユーザー番号を入力せずに「OK」をタップすると、全ユーザーに対して検索範囲を指定して検索することができます。

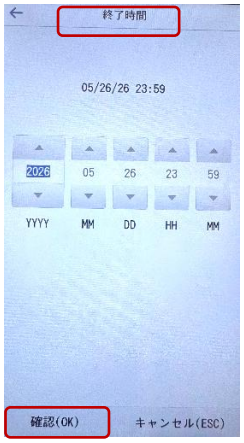
＜日にちの範囲を指定した検索方法＞




※検索したい時間範囲をタップします。

＜日時指定のカスタム検索方法＞



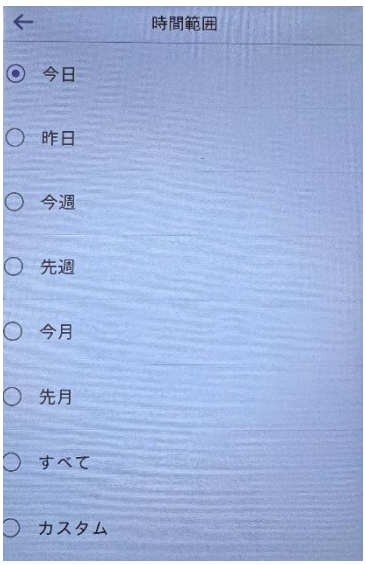




※ユーザーID を指定せずに検索すると全データを表示します。入退 Push の場合、履歴に表示されるユーザーID：0 は、未登録ユーザー（認証失敗）のアクセス履歴です。

## 2. 入退写真

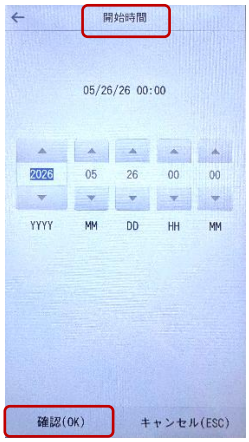
入退履歴について、ユーザー番号の入力後、検索範囲を指定して検索することができます。ユーザー番号を入力せずに「OK」をタップすると、全ユーザーに対して検索範囲を指定して検索することができます。

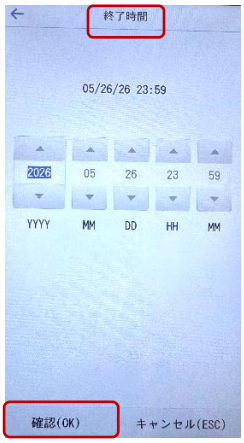
＜日にちの範囲を指定した検索方法＞




※検索したい時間範囲をタップします。

＜日時指定のカスタム検索方法＞




※本履歴を確認するには「システム設定→アクセスログ設定または勤怠→カメラモード」で「写真を撮影し保存する」へ設定する必要があります。

**3. 拒否リスト入退写真**

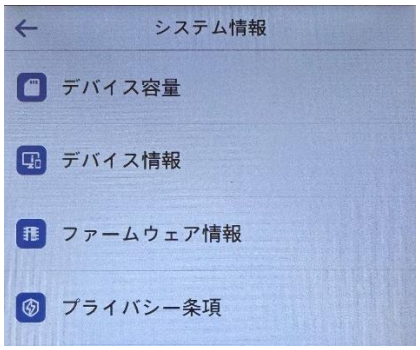
当社または本製品ではサポート対象外です。

## 10.9. 自動テスト

当社または本製品ではサポート対象外です。サポートからの指示があった場合に実施してください。

## 10.10. システム情報

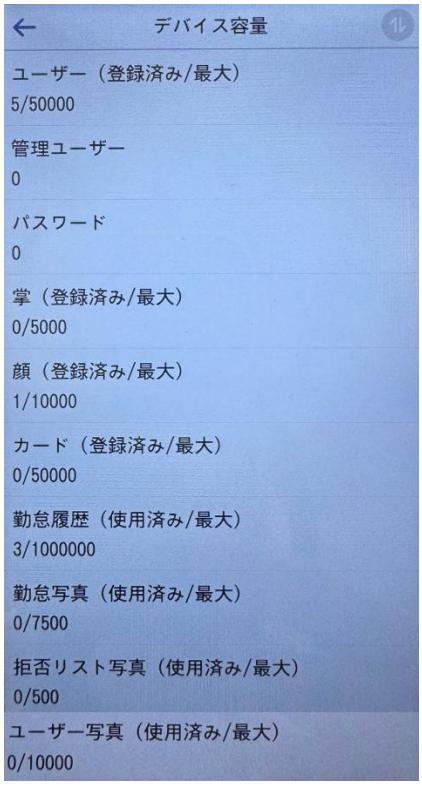
顔認証デバイス上のユーザー登録数や生体情報登録数など、各情報を一覧で表示・確認することができます。




| 項目名 | 説明 |
|---|---|
| デバイス容量 | 登録済みのユーザー数や履歴数を確認できます。 |
| デバイス情報 | デバイス名やシリアル番号が確認できます。 |
| ファームウェア情報 | デバイスの各ファームウェアの情報を確認できます。 |
| プライバシー条項 | 管理ソフトと顔認証デバイス間で取り扱うデータに関するプライバシーポリシーです（英文）。 |

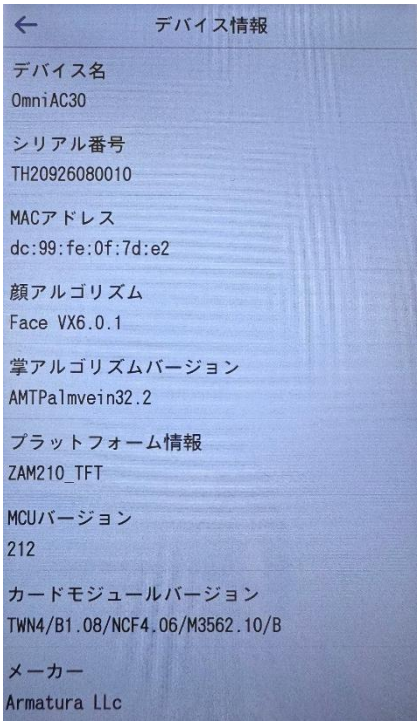
### 1. デバイス容量

ユーザー登録数や、ユーザー情報に紐づく生体情報などの登録数を一覧表示します。現在の状態を確認して上限数に近い場合は既に使用されていないユーザー情報などを整理して空き容量を増やします。

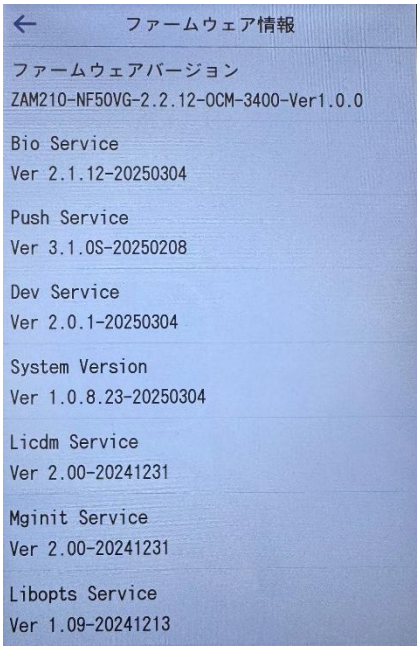



| 項目名 | 説明 |
|---|---|
| ユーザー（登録済み/最大） | 登録数/上限数 |
| 管理ユーザー | 管理ユーザーとして指定した人数 |
| パスワード | パスワード登録数 |
| 掌（登録済み/最大） | 登録数/上限数 |
| 顔（登録済み/最大） | 登録数/上限数 |
| カード（登録済み/最大） | 登録数/上限数 |
| 勤怠履歴／履歴数（使用済み/最大） | 記録数/上限数 |
| 勤怠写真（使用済み/最大） | 記録数/上限数 |
| 拒否リスト写真（使用済み/最大） | サポート対象外です。 |
| ユーザー写真（使用済み/最大） | 記録数/上限数 |

**2. デバイス情報（参考）** ※顔認証デバイスの固有の情報を表示します




**3. ファームウェア情報（参考）** ※顔認証デバイスに実装されている各種ファームウェアのバージョンを表示します




**4. プライバシー条項**

管理ソフトと顔認証デバイス間で取り扱うデータに関するプライバシーポリシーです（英文）。

# 11. サービスコントローラ（データ復元など）

管理ソフト付属のサービスコントローラの操作方法を説明します。当社がサポートする標準 UI は（表 1）を参照してください。

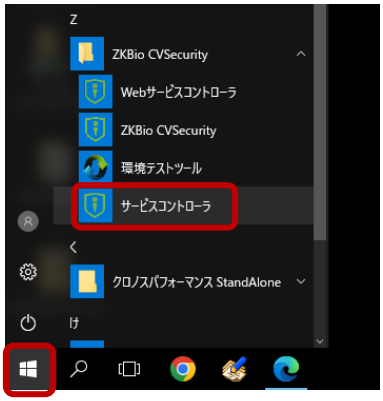
（表 1）当社がサポートするメニューの一覧

| メニュー | サポート対象 | 内容 |
|---|---|---|
| Configure the Server Port | ○ | サーバーポートの設定を変更する |
| Configuration Database | × | 当社または本製品はサポート対象外です。 |
| Configuration Database Local Backup Path | ○ | データベースのバックアップ先を変更する |
| Restore Database | ○ | データベースを復元する |
| Service is running,click here to stop | ○ | 管理ソフトの Web サービスを停止／再開する |
| Import SSL Certificate | × | 当社または本製品はサポート対象外です。 |
| Import Language Pack | × | 当社または本製品はサポート対象外です。 |
| Add Module | × | 当社または本製品はサポート対象外です。 |
| Modify The Database Password | × | 当社または本製品はサポート対象外です。 |
| Modify The Redis Password | × | 当社または本製品はサポート対象外です。 |
| Toggle HTTP | × | 当社または本製品はサポート対象外です。 |
| Log Folder | ○ | 管理ソフト（サーバー）のログを表示する |

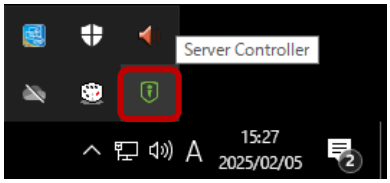
## 11.1. サービスコントローラの起動

管理ソフトに付属する「サービスコントローラ」の起動方法を説明します。

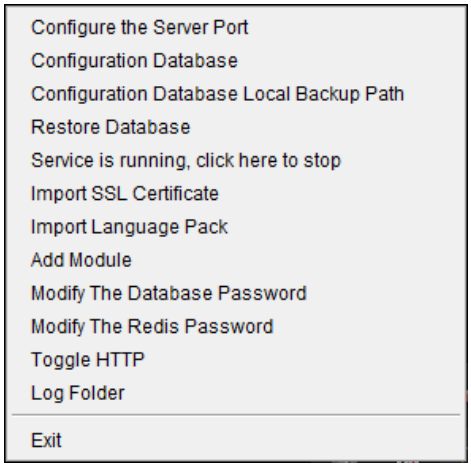
① Windows®のプログラムメニューの中から「ZKBio CVSecurty」を開き、「サービスコントローラ」をクリックします。
※「Web サービスコントローラ」は、当社または本製品はサポート対象外です。




② Windows®のタスクトレイにある「サービスコントローラ」をクリックします。



③ サービスコントローラで設定できるメニューが一覧表示されます。必要な場合、当社または本製品はサポートするメニューをクリックします。



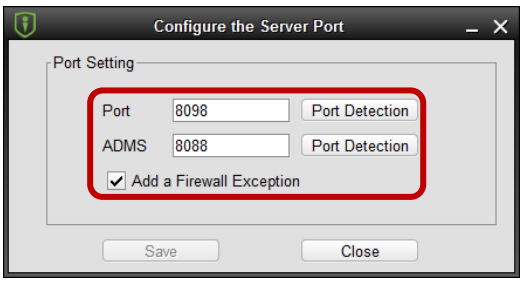

## 11.2. サーバーポートの設定変更

「Configure the Server Port」：サーバーポートの設定を変更する方法を説明します。本操作は、お客様の環境において初期値のサーバーポートで運用が難しい場合にのみ設定変更をします。

① 「Configure the Server Port」をクリックします。



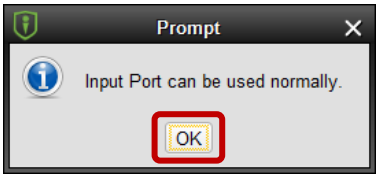

② 「Port Setting」の画面が開きますので、ポート番号を変更して「Port Detection」をクリックします。
※設定するポート番号が利用できることを確認してください。
※「Add a Firewall Exception：ファイヤーウォールに例外として登録」のオプションは必ずチェックを入れます。



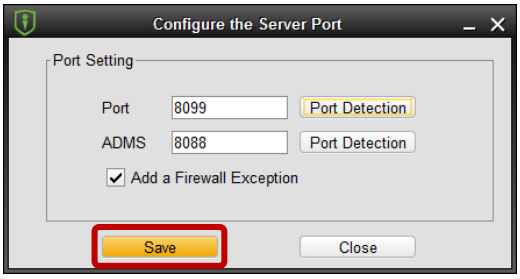

**注意事項**

- ✓ **「Port」を変更した場合は「5.4 管理者アカウントの設定」の URL の末尾は変更後のポート番号になります。**
- ✓ **「ADMS」を変更した場合は「4.4 クラウドサーバの設定」の「サーバーポート」を変更後のポート番号になります。**

③ 「Input Port can be used normally」と表示されますので「OK」をクリックします。




④ 設定したポート番号を保存する場合は「Save」をクリックします。



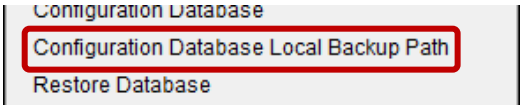

## 11.3. データベースの設定変更

「Configuration Database」：当社または本製品はサポート対象外です。

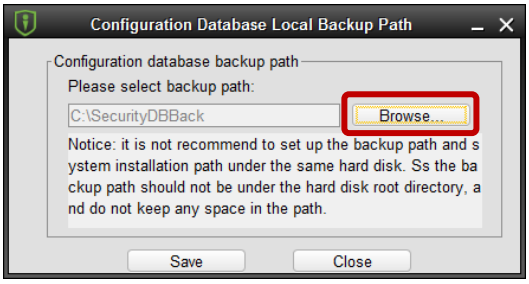
## 11.4. データベースのバックアップ先変更

「Configuration Database Local Backup Path」：データベースのバックアップ先を変更する方法を説明します。バックアップ先は、Windows®と同一パーティションや別パーティションではなく、別のストレージ製品（HDD/SSD など）を指定します。

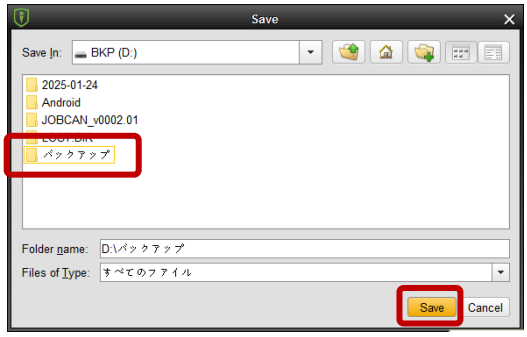
① 「Configuration Database Local Backup Path」をクリックします。



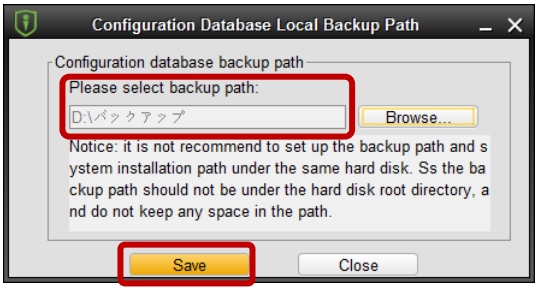

② 「Browse」をクリックします。



③ バックアップ先を指定して、指定したパスを保存するには「Save」をクリックします。



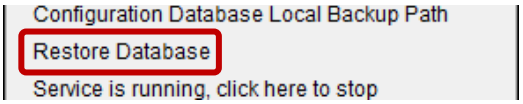

④ バックアップ先の変更を保存するには「Save」をクリックします。



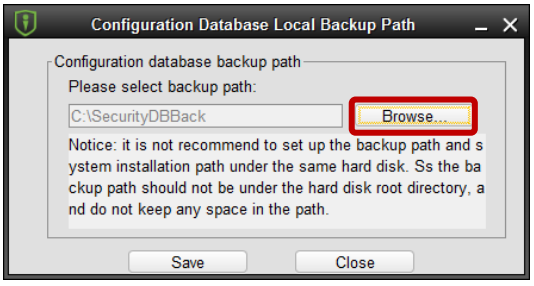

## 11.5. データベースの復元

「Restore Database」：データベースのバックアップから復元する方法について説明します。復元する際は、管理ソフトからログアウトして終了してください。

① 「Restore Database」をクリックします。

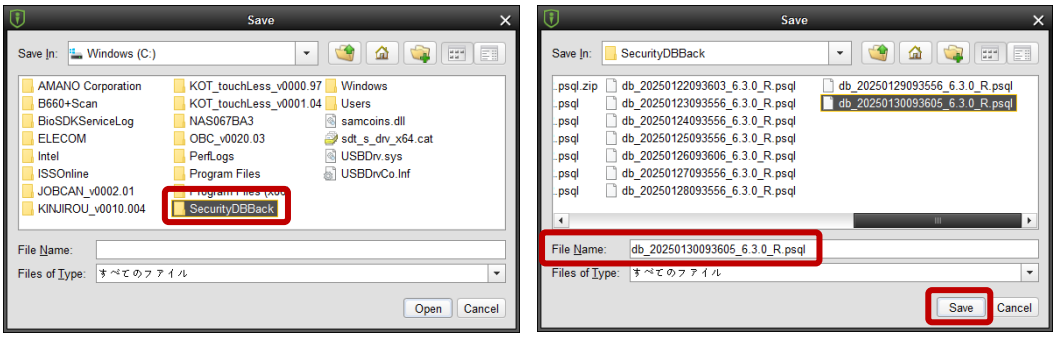



② 「Browse」をクリックします。

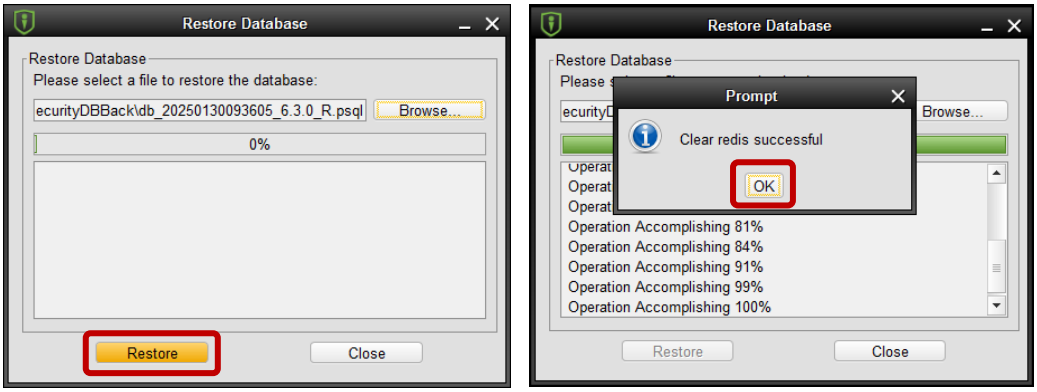


③ バックアップファイルを選択して「Save」をクリックします。（初期値：C:¥SecurtyDBBack*）

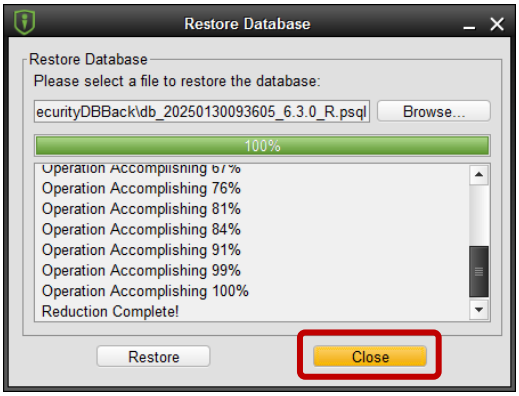
※バックアップ先を変更している場合は、変更先のフォルダを参照してください。




④ 復元を開始するには「Restore」をクリックします。「Clear Redis successful」と表示されたら「OK」をクリックします。




⑤ 最後に「Close」をクリックします。



## 11.6. 管理ソフトのサービスの停止／再開

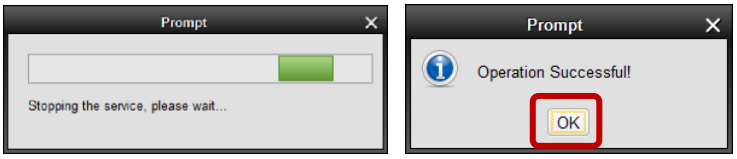
「Service is running,click here to stop」：管理ソフトのサービスを停止／再開について説明します。

### 1. サービスの停止方法

① 「Service is running,click here to stop」をクリックします。



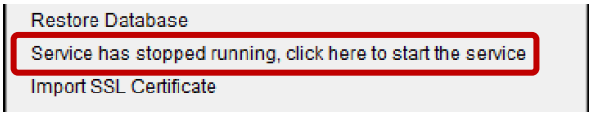

② サービス停止中の画面が表示され、停止結果が表示されますので「OK」をクリックします。



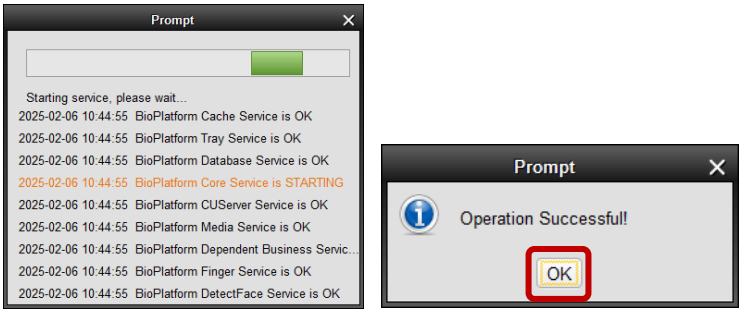

③ サービスコントローラの表示が「**Service is running,click here to stop**」から「**Service has stopped running**, …」へ表示が変わっていることを確認してください。管理ソフトにアクセスできなくなります。

### 2. サービスの再開方法

① 「Service has stopped running, click here to start the service」をクリックします。




② サービス開始中の画面が表示され、停止結果が表示されますので「OK」をクリックします。サービスコントローラの表示が「**Service has stopped running**, …」から「**Service is running**,…」へ表示が変わっていることを確認してください。管理ソフトにアクセスできるようになります。



**3. サービスの起動確認（Windows タスクマネージャーで確認）**

管理ソフトにアクセスできないなどの事象が発生した場合、Windows 上で各種サービスが起動していることを確認してください。下記、重要なサービスが起動していないと管理ソフトを正常に利用できません。

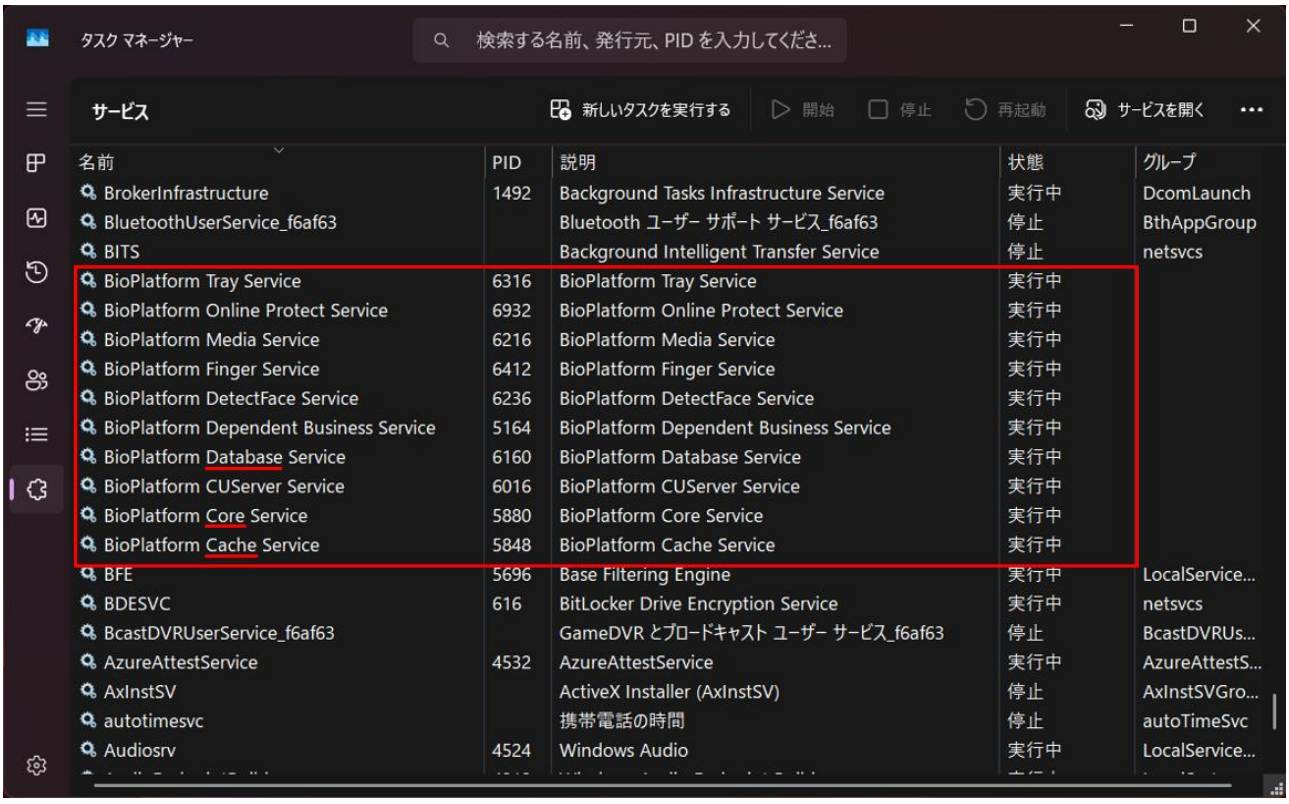
通常、Service（サービス）は Windows 側で自動的に管理されるため、プログラムやサービスの起動に手動で操作・介入する必要はありません。例えば、DetectFace Service を手動で強制終了すると、Web で顔画像のアップロード機能に影響が出る可能性があります。ご利用状況に応じて判断していただく必要がある場合もあります。

**＜重要なサービスの一覧＞**

サービスの確認手順：Windows タスクマネージャー起動 → 「サービス」をクリック → 「名前」でソート

① BioPlatform Cache Service：Web ページやその関連データを一時的に保存し、サーバーレスポンスを向上させる仕組み
② BioPlatform Core Service：Web サーバー
③ BioPlatform Database Service：DB サーバー（PostgresQL）

（ご参考）「BioPlatform～」のサービスも管理ソフトに付随するサービスとなります。




| 名前 | PID | 説明 | 状態 | グループ |
|---|---|---|---|---|
| BrokerInfrastructure | 1492 | Background Tasks Infrastructure Service | 実行中 | DcomLaunch |
| BluetoothUserService_f6af63 | | Bluetooth ユーザー サポート サービス_f6af63 | 停止 | BthAppGroup |
| BITS | | Background Intelligent Transfer Service | 停止 | netsvcs |
| BioPlatform Tray Service | 6316 | BioPlatform Tray Service | 実行中 | |
| BioPlatform Online Protect Service | 6932 | BioPlatform Online Protect Service | 実行中 | |
| BioPlatform Media Service | 6216 | BioPlatform Media Service | 実行中 | |
| BioPlatform Finger Service | 6412 | BioPlatform Finger Service | 実行中 | |
| BioPlatform DetectFace Service | 6236 | BioPlatform DetectFace Service | 実行中 | |
| BioPlatform Dependent Business Service | 5164 | BioPlatform Dependent Business Service | 実行中 | |
| BioPlatform Database Service | 6160 | BioPlatform Database Service | 実行中 | |
| BioPlatform CUServer Service | 6016 | BioPlatform CUServer Service | 実行中 | |
| BioPlatform Core Service | 5880 | BioPlatform Core Service | 実行中 | |
| BioPlatform Cache Service | 5848 | BioPlatform Cache Service | 実行中 | |
| BFE | 5696 | Base Filtering Engine | 実行中 | LocalService... |
| BDESVC | 616 | BitLocker Drive Encryption Service | 実行中 | netsvcs |
| BcastDVRUserService_f6af63 | | GameDVR とブロードキャスト ユーザー サービス_f6af63 | 停止 | BcastDVRUs... |
| AzureAttestService | 4532 | AzureAttestService | 実行中 | AzureAttestS... |
| AxInstSV | | ActiveX Installer (AxInstSV) | 停止 | AxInstSVGro... |
| autotimesvc | | 携帯電話の時間 | 停止 | autoTimeSvc |
| Audiosrv | 4524 | Windows Audio | 実行中 | LocalService... |

## 11.7. SSL 証明書のインポート

「Import SSL Certificate」：当社または本製品はサポート対象外です。

## 11.8. 言語パックのインポート

「Import Language Pack」：当社または本製品はサポート対象外です。

## 11.9. モジュールの追加

「Add Module」：当社または本製品はサポート対象外です。

## 11.10. データベース接続パスワード変更

「Modify The Database Password」：当社または本製品はサポート対象外です。

## 11.11. Redis 接続パスワード変更

「Modify The Redis Password」：当社または本製品はサポート対象外です。

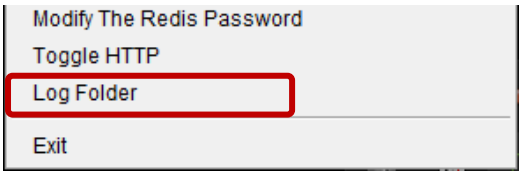
## 11.12. Toggle HTTP

「Toggle HTTP」：当社または本製品はサポート対象外です。

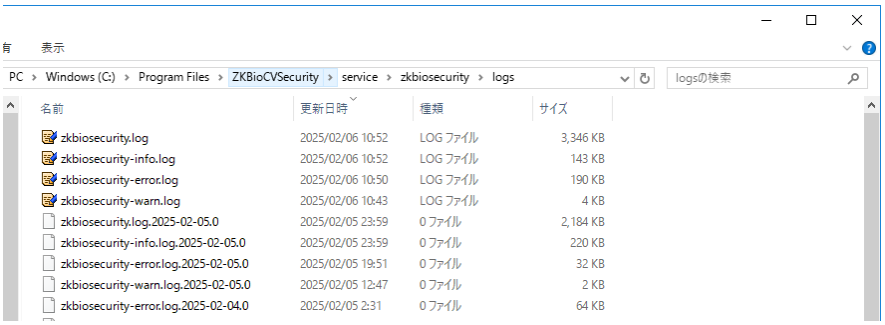
## 11.13. ログの表示

「Log Folder」：管理ソフト（サーバー）のログを表示する方法を説明します。トラブルシュートのため、オペレーターから指定されたログをご提供をしていただく場合があります。

① 「Log Folder」をクリックします。




② ログが保存されているフォルダが開きます。作業が終了しましたらフォルダを閉じてください。



# 12. お取り扱い上の注意

■ 本製品を正しく安全に利用するために

- 本書では製品を正しく安全に使用するための重要な注意事項を説明しています。必ずご使用前にこの注意事項を読み、記載事項にしたがって正しくご使用ください。
- 本書は読み終わった後も、必ずいつでも見られる場所に保管してください。

■ 表示について

この「取り扱い上のご注意」では以下のような表示（マーク）を使用して注意事項を説明しています。内容を理解してから、本文をお読みください。




この表示を無視して取扱いを誤った場合、使用者が死亡または重傷を負う危険性がある項目です。




この表示を無視して取扱いを誤った場合、使用者が障害を負う危険性、もしくは物的損害を負う危険性がある項目です。



三角のマークは何かに注意しなければならないことを意味します。三角の中には注意する項目が絵などで表示されます。例えば左図のマークは感電に注意しなければならないことを意味します。



丸に斜線のマークは何かを禁止することを意味します。丸の中には禁止する項目が絵などで表示されます。例えば左図のマークは分解を禁止することを意味します。



塗りつぶしの丸のマークは何かの行為を行わなければならないことを意味します。丸の中には行わなければならない行為が絵などで表示されます。例えば、左図のマークは必ず実行していただく（強制）内容のことを意味します。

**警告**



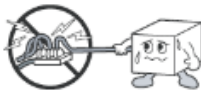
万一、異常が発生したとき。
本体から異臭や煙が出た時は、ただちに LAN ケーブル、AC アダプタを抜いて当社指定のサポート窓口にご相談ください。



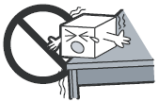
異物を入れないでください。
通気孔などから、金属類や燃えやすいものを入れないでください。そのまま使用すると感電や火災の原因になります。万一、異物が入った場合は、ただちに電源を切り、当社指定のサポート窓口にご相談ください。



分解しないでください。
本書の指示に従う作業を除いては、自分で修理や改造・分解をしないでください。感電や火災、やけどの原因になります。特に電源内部は高電圧が多数あり、万一、触れると危険です。



AC アダプタはなるべくコンセントに直接接続してください。
タコ足配線や何本も延長したテーブルタップの使用は火災の原因となります。



不安定な場所に置かないでください。
ぐらついた台の上や傾いた所、振動、衝撃のある所に置くと、落下や転落等からケガの原因になります。



付属の AC アダプタ以外使用しないでください。
感電や火災、故障の原因になります。



濡れた手で触らないでください。
本製品を濡れた手で触ると、感電や火災、故障の原因となります。



電源プラグの接触不良やトラッキング。
ケーブル類は次のようにしないと、トラッキングの発生や接触不良で過熱し、火災の原因になります。・ケーブル

類は根元までしっかり差し込んでください。・ケーブル類はほこりや水滴が付着していないことを確認し、差し込んでください。付着している場合は乾いた布などで拭き取り、差し込んでください。



ケーブル類を大切に。

AC アダプタは必ず本製品付属のものを使用し、以下の点に注意してください。取り扱いを誤ると、感電や火災の原因となります。「ものを載せない」「引っ張らない」「押し付けない」「折り曲げない」「加工しない」「束ねない」「熱器具のそばで使用しない」



雷が鳴るなど、電圧の状態が不安定なときには使用しないでください。データが消失したり、故障の原因となります。



装置の上に物を置かないでください。本製品の上に重いものや、水の入った容器類、または虫ピン、クリップなどの小さな金属類を置かないでください。故障や感電、火災の原因になります。



本製品を小さなお子様の手の届く場所へ放置しないでください。機器を損傷する可能性があるだけでなく、お子様がケガをする危険があります。




指定された電源で使用してください。AC アダプタは必ず AC100V のコンセントに接続してください。



揮発性液体の近くでの使用は避けてください。

マニュキュア、ペディキュアや除光液などの揮発性液体は、装置の近くで使わないでください。装置の中に入って発火すると火災の原因になります。



ケーブル類の抜き差しには注意してください。

□ケーブル類を差し込むとき、または抜くときは必ずコネクタを持って行ってください。無理にケーブルを引っ張るとケーブル類の一部が断線してその部分が過熱し、火災の原因になります。

□長期間ご使用にならないときは、ケーブルを抜いてください。使用していないときにも通電しているため、万一、部品破損時には火災の原因になります。

□ケーブル類を抜き差しするときは、乾いた手で行ってください。濡れた手で行うと感電の原因になります。



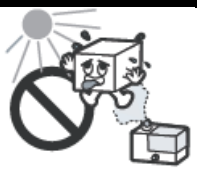
LCD パネルが破損した場合は割れたガラスでけがをしないように十分注意をしてください。また、LCD パネルが破損すると、内部の液体（液晶）がもれることがあります。このような場合には、液体を口にしたり、吸い込んだり、皮膚につけないように十分ご注意ください。万一、眼や口に入った場合は、速やかに水ですすぎ、医師の診断を受けてください。また、皮膚や衣服についた場合は、アルコールなどでふき取り、石鹸で水洗いしてください。そのまま放置すると皮膚や衣服を傷める可能性があります。



日本国以外では使用しないでください。

この装置は日本国内専用です。電圧の違いや環境の違いにより、国外で使用すると火災や感電の原因になります。また他国には独自の安全規格が定められており、この装置は適合していません。

**注意**



高温・多湿の場所、長時間直射日光のあたる場所での使用・保管は避けてください。屋外での使用は禁止します。また、周辺の温度変化が激しいと内部結露によって誤動作する場合があります。



本体は精密な電子機器のため、衝撃や振動の加わる場所、または加わりやすい場所での使用や保管は避けてください。



浴室・洗面台・台所の流し台・洗濯機など水を使用する場所の近傍、湿気の多い地下室、水泳プールの近傍や埃の多い場所では使用しないでください。電気絶縁の低下によって火災や感電の原因になります。



装置の梱包用ポリ袋はお子様の手の届くところに置かないでください。かぶったりすると窒息の恐れがあります。



コネクタ等の接続端子に手や金属で触れたり、針金等の異物を挿入したりしないでください。また、金属片のある場所に置かないでください。発煙や接触不良などにより故障の原因になります。



ケーブルは足などをひっかけないように配線してください。足を引っかけるとケガや接続機器の故障の原因になります。また、大切なデータが失われるおそれがあります。ケーブルの上に重量物を載せないでください。また、熱器具のそばに配線しないでください。ケーブル被覆が破れ、接続機器などの故障の原因になります。



本製品の稼働中に接続ケーブルなどを抜かないでください。データの損失や機器の故障の原因になります。



AC アダプタについて本製品に添付されている AC コードは本製品専用です。他の機器に利用しないようにしてください。



LCD パネルに圧力を加えないでください。表示異常の原因となったり、LCD パネルの破損につながります。
LCD パネルの表面に硬いものをあてたり、こすったりしないでください。LCD パネルの傷や破損につながります。



本製品が汚れた場合
本製品が汚れた場合は必ず本体の電源を切ってから、柔らかい布で軽くふいてください。揮発性の薬品（ベンジン・シンナーなど）を用いますと、変形・変色の原因になる事があります。
同じ画面を長時間表示させると、残像が残ることがあります。使用しない場合は電源を切ってください。



液晶モニタは膨大な数の薄膜トランジスタ（TFT）で構成されています。画面上で少数のドットに欠落、変色、発光が見られることがありますが、これは TFT 液晶技術に起因するもので、製品自体の欠陥によるものではありません。



地震対策について
地震などによる振動で装置の移動、転倒あるいは窓からの飛び出しが発生し、重大な事故へと発展する恐れがあります。これを防ぐため、地震・振動対策を専門業者にご相談いただき、実施してください。



布やじゅうたん、スポンジ、発砲スチロール、ダンボールなど、保温性や保湿性が高いものの近くで使用しないで下さい。火災の原因になります。



本製品の設置や角度調整時、ネジや工具を使用して固定が必要な時など、指などをはさまないように気を付けてください。



本製品に記録された情報内容と、本製品とともに使用する記憶媒体に記録された情報内容は、「個人情報」に該当する場合がございます。本製品が廃棄、譲渡、修理などで第三者に渡る場合には、その取り扱いに十分ご注意ください。



本製品を廃棄する場合は、お住まいの地方自治体で定められた方法で廃棄してください。

## 12.1. 廃棄・譲渡時のデータに関する注意

ご利用の製品を廃棄等される場合には、以下の事項にご注意ください。端末本体を廃棄あるいは譲渡する際、記録されたお客様のデータが再利用され、データが流出してしまうことがあります。端末本体に記録されたデータは、「削除」や「フォーマット」をおこなっただけではデータは消えたように見えるだけで、特殊なソフトウェアを使うことにより、消失したはずのデータが再生されることがあります。顔認証端末の「リセット（初期化）」及び、顔認証デバイスの「メインメニュー」の「データ管理」から各情報の「データ削除」を実行して下さい。
デバイス本体内部のデータが第三者に流出することがないよう、全データ消去の対策をお願いいたします。また、デバイス本体上のソフトウェアを消去することなく譲渡しますと、ソフトウェアライセンス使用許諾に抵触する場合がありますのでご注意ください。お客様のデータが漏洩することによる、いかなるトラブルも当社はその責任を負いかねます。
ご参考：データ消去専門サービスのご用命は「16 付録 D データ消去サービスについて」を参照してください。

## 12.2. 電波に関する注意事項

**無線 LAN 接続時のセキュリティに関するご注意**
**お客様の権利（プライバシー保護）に関する重要な事項です**

本製品は有線接続でつなぐ代わりに無線電波を利用して直接情報のやり取りを行うため、電波の届く範囲であれば自由に接続が可能であるという利点があります。その反面、電波はある範囲内であれば障害物（壁等）を超えてすべての場所に届くため、セキュリティに関する設定を行っていない場合、以下のような問題が発生する可能性があります。

**●通信内容を盗み見る**
悪意ある第三者が、電波を故意に傍受し、ID やパスワード等、本製品間で通信しているデータ内容を盗み見る行為を行われてしまう可能性があります。

**●不正に侵入される**
悪意がある第三者が無断で本製品へアクセスし、個人情報を取り出す（情報漏洩）等の行為を行われてしまう可能性があります。本製品はこれらの問題に対応するためのセキュリティの仕組みを持っていますが、設定や運用方法によって上記に示した様な問題が発生する可能性があります。
従って、お客様がセキュリティ問題発生の可能性を少なくするためには、本製品をご使用の前に、必ずセキュリティに関する全ての設定をマニュアルに従って行ってください。
なお、本製品の仕様上、特殊な方法によりセキュリティ設定が破られる事もありますので、ご理解の上ご使用ください。セキュリティ設定などについては、お客様ご自身で対処できない場合は、ロジテックテクニカルサポートセンターまでお問い合わせください。
当社ではお客様がセキュリティに関する設定を行わないで使用した場合の問題を充分に理解した上で、お客様自身の判断と責任においてセキュリティに関する設定を行い、製品を使用することをお勧めします。
※セキュリティの設定を行わず、または本製品の仕様上やむを得ない事情によりセキュリティ問題が発生してしまった場合、当社では、これによって生じた一切の責任を負いかねます。

**■電波に関する注意事項**

この機器の仕様周波数帯では、電子レンジ等の産業・科学・医療用機器のほか工場の製造ライン等で使用されている移動体識別用の構内無線局（免許を要する無線局）及び特定小電力無線局（免許を要しない無線局）並びにアマチュア無線局（免許を要する無線局）が運用されています。

1. この機器を使用する前に、近くで移動体識別用の構内無線局及び特定小電力無線局並びにアマチュア無線局が運用されていないことを確認してください。
2. 万一、この機器から移動体識別用の構内無線局に対して有害な電波干渉の事例が発生した場合には、速やかに使用周波数を変更するか又は電波の発射を停止した上、当社 テクニカルサポートまでご連絡いただき、混信回避のための処置等（例えば、パーティションの設置など）についてご相談してください。
3. その他、この機器から移動体識別用の特定小電力無線局あるいはアマチュア無線局に対して有害な電波干渉の事例が発生した場合など何かお困りのことが起きたときは当社テクニカルサポートまでお問い合わせください。

使用周波数帯域　　：2.4GHz
変調方式　　：DS-SS 方式、OFDM 方式
周波数変更の可否　：全体域を使用し、移動体識別装置の帯域を回避可能

## 12.3. 免責事項

1. 本書の一部または全部を当社に無断で転載することは禁止されております。
2. 本製品および本書を運用した結果による損失、利益の逸失の請求などにつきましては、当社でいかなる責任も負いかねますので、あらかじめご了承ください。
3. 本製品の仕様、デザインおよびマニュアルの内容については、製品改良のため予告なく変更する場合があります。
4. お客様にて接続された機器やインストールしたアプリケーションと本製品の動作を保証するものではありません。これにより誤動作・故障・障害などから生じた損害に関して、当社は一切責任を負いかねます。
5. 電源ボタンの操作方法以外の方法で OS・システムが破損した場合は保証対象外となります。
6. 本製品は壁や棚など設置するための付属品や取り付け金具を用意しています。取り付ける場所の安全の確保はお客様の責任において実施いただくとともに、本製品及び付属品、関連製品の設置から生じた損害に関して、当社は一切責任を負いかねます。
7. 本製品は、人命に関わる設備や機器、および高い信頼性や安全性を必要とする設備や機器（医療関係、航空宇宙関係、輸送関係、原子力関係等）への組み込みなどは考慮されていません。これらの設備や機器で本製品を使用したことにより人身事故や財産損害などが発生しても、当社ではいかなる責任も負いかねます。
8. 本製品は日本国内仕様ですので、本製品を日本国外で使用された場合、当社でいかなる責任も負いかねます。また、当社は海外での（海外に対する対応を含む）サービスおよび技術サポートを行っておりません。

## 12.4. 保証規定

当社が定める保証期間（本製品ご購入日から起算されます。）内に適切な使用環境で発生した本製品の故障に限り、無償で本製品を修理または同等品への交換を致します。

**■無償保証範囲**

以下の場合には、保証対象外となります。

1. 本製品購入の際の証明書（レシート、納品書等/以下「購入証明」と表記）と、本製品をご提出頂けない場合。
2. 購入証明など販売店・購入年月日の記載あるものをご提示いただけない場合。
3. 購入証明に、偽造・改変などが認められた場合。
4. 当社及び当社が指定する機関以外の第三者ならびにお客様による本製品の改造、分解、修理が行われている場合。
5. 当社が定める機器以外に接続、または組み込んで使用し、故障または破損した場合。
6. マニュアル、文書、説明ファイルに記載の使用方法、及びご注意に反するお取扱いによって生じた故障、破損の場合。
7. 通常で想定される使用環境の範囲を超える温度、湿度、振動等により故障した場合。
8. 本製品を購入頂いた後の輸送中に発生した衝撃、落下等により故障した場合。
9. 地震、火災、落雷、風水害、その他の天変地異、公害、異常電圧などの外的要因により故障した場合。
10. その他、無償修理または交換が認められない合理的事由が認められた場合。

## 12.5. 修理規定

1. 修理のご依頼は、購入証明を本製品に添えてお買い上げの販売店にお持ち頂くか、当社修理センターに送付してください。
2. 当社修理センターへご送付頂く場合の送料はお客様ご負担となります。また、ご送付頂く際、適切な梱包の上、紛失防止のため譲渡の確認できる手段(宅配や簡易書留など)をご利用下さい。尚、当社では運送中の製品の破損及び紛失については一切の責任を負いかねます。
3. 当社修理センターへご送付頂く場合、必ず「お客様のご連絡先(ご住所/電話番号)」「故障の状態」を書面にして本製品に添付して下さい。
4. 保証期間経過後の修理については、お見積もりの必要の有無、及び修理限度額を明示の上、本製品に添付して下さい。
5. ご送付頂く際の送付状控えは大切に保管下さい。
6. 修理、もしくは同機種での交換ができない場合は、保証対象製品と同等またはそれ以上の性能を有する他の製品と交換させて頂く場合がございます。
7. 有償・無償に関わらず、修理等により交換された本製品またはその部品等は返却致しかねます。
8. 記録メディア・ストレージ製品において、当社修理センターにてドライブ交換、製品交換を実施した際にはデータの保全を行わず全て初期化致します。記録メディア・ストレージ製品を修理に出す前には、お客様ご自身でデータのバックアップを取って頂きますようお願い致します。
9. 本規定における「故障」とは、本製品が本製品の仕様の定めるとおりに機能しないことをいいます。外観損傷（本製品の傷や破損）については、保証対象外となりますので、外観損傷に対する修理・修繕は行いません。

## 12.6. サポート･修理窓口のご案内

注意事項

### 個人情報の取り扱いについて

**修理依頼、製品に関するお問い合わせなどでご提供いただいたお客様の個人情報は、修理品やアフターサポートに関するお問い合わせ、製品およびサービスの品質向上、アンケート調査等、これらの目的のために関連会社または業務提携先に提供する場合を除き、お客様の同意なく第三者への開示は行いません。お客様の個人情報は細心の注意を払って管理しますのでご安心ください。**

### サポート窓口のご案内

製品に対する技術的な質問や、取扱説明書に対する疑問点は、専用サポート窓口までお問い合わせください。

**TEL. 0570-070-040 FAX. 0570-033-034**
**受付時間： 09:00 ～ 12:00 / 13:00 ～ 18:00**
**月曜日～金曜日（祝祭日、夏期、年末年始特定休業日を除く）**

### 修理センター窓口のご案内

郵送、宅配便にて修理を依頼される場合、以下の点をご確認の上、当社修理受付窓口まで製品を送付ください。

**修理受付窓口（修理品送付先）**
**〒396-0111 長野県伊那市美すず 8268 番地 1000**
**エレコムグループ修理センター（3 番窓口）**
**TEL. 0265-74-1423 FAX. 0265-74-1403**
**受付時間： 9:00 ～ 12:00 / 13:00 ～ 17:00**
**月曜日～金曜日（祝祭日、夏期、年末年始特定休業日を除く）**

1. 必ず、修理依頼書に「お客様のご連絡先（ご住所/電話番号）」「故障の状態」を書面に記述し製品と共に添付してください。修理依頼書は、Web サイトよりダウンロード可能です。また修理に関するご説明やお願いを掲載しています。修理依頼書がダウンロード出来ない場合には書面に記載の上添付してください。
2. 送料および、梱包費用は保証期間の有無を問わずお客様のご負担です。
3. 修理を依頼される場合は、保証書及び納品日が判別できる物（納品書のコピーなど）を製品に添付してください。
4. 保証期間経過後の修理については、お見積りの必要の有無、または修理限度額および連絡先を明示の上、製品に添付してください。
5. ご送付の際は、製品が梱包されていた箱、梱包材を使用しお送りください。お送りいただいた修理依頼書と運送会社のお問い合わせ番号等は必ずお手元にお控えください。

注意事項

### データの取り扱いについて

**万一、盗難等により端末本体内にあるお客様の個人情報および各種データが流出した場合、当社は一切の責任を負いかねます。大切なデータを管理するため、盗難防止など、必要な措置を講じておくようお願いいたします。**
**端末本体および内部記憶装置は消耗品です。不適切な使用や電気的ノイズ、静電気による障害、強い衝撃、落雷などの天変地異により故障する場合があります。重要なデータは万一に備えて必ず他のメディアにバックアップを取っておくようお願いいたします。不適切な使用や故障の結果生じたデータの直接的または間接的な損害については、当社では一切の保証をいたしません。本製品を使用した際のデータの消失については、いかなる運用形態にかかわらず、当社では一切その責任を負いません。**

- 本書の著作権は、ロジテック INA ソリューションズ株式会社が所有しています。
- 本書の内容の一部または全部を無断で複製/転載する事を禁止させていただきます。
- 本書の内容に関しては万全を期しておりますが、万一ご不審な点がございましたら、ロジテックテクニカルサポートセンターまでご連絡願います。
- 本製品の仕様および外観は、製品の改良のため予告なしに変更する場合があります。
- 実行した結果の影響につきましては、上記の理由にかかわらず責任を負いかねますので、ご了承ください。
- 本製品のうち、戦略物質または役務に該当するものの輸出にあたっては、外為法に基づく輸出または役務取引許可が必要です。
- Microsoft®、Windows®は、米国 Microsoft 社の登録商標です。
- Mac、Mac OS、Macintosh は、Apple Inc.の登録商標です。
- 「Android」、「Android ロゴ」は、Google LLC の登録商標です。
- 「QR コード」は株式会社デンソーウェーブの登録商標です。
- その他、本書または関連文書に記載されている商品名、社名などは、一般に商標ならびに登録商標です。

# 13. 付録 A 製品仕様

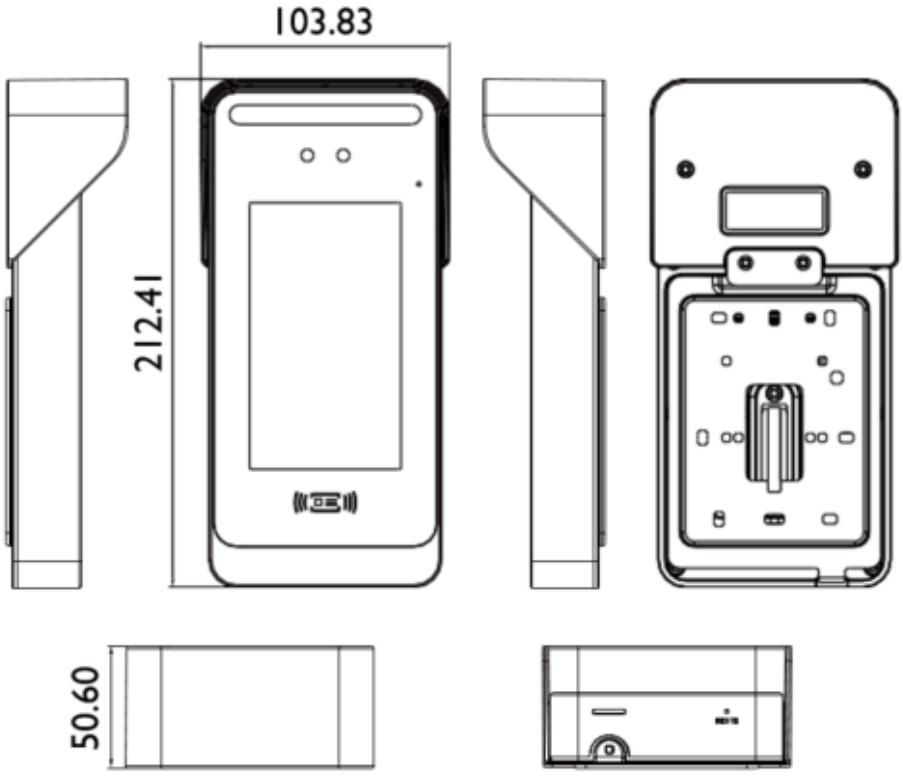
| | | |
|---|---|---|
| 顔認証 | 認証時間 0.10 秒（実測） | |
| | 認証距離 0.4m～2m<br>※2D 単眼偽造防止を選択すると最大の顔認識距離が 2m<br>※2D 両眼偽造防止を選択すると最大の顔認識距離が 1.2～1.4m<br>※顔の画素数（認識できる顔の大きさで調整可） | |
| | 登録ユーザー数 最大 10,000 人 | |
| 掌認証 | 認証時間 0.14 秒（実測） | |
| | 認証距離 0.2m～0.4m | |
| | 登録ユーザー数 最大 5,000 人 | |
| IC カード認証<br>（カードリーダー機能） | FeliCa（ISO/IEC 18092（NFC Type F）に対応）<br>MIFARE（ISO/IEC 14443（Type A）に対応）<br>※カード ID 取得のみ（以下、動作確認済み）<br>・「FeliCa」の「IDm」情報<br>・「Mifare Plus」の「UID」情報<br>・「Mifare Ultralight EV1」の「UID」情報<br>・「Mifare Classic 1K」の「UID」情報 | |
| | 登録ユーザー数 最大 50,000 人（QR 認証と共用キャパシティ） | |
| QR 認証 | 登録ユーザー数 最大 50,000 人（IC カード認証と共用キャパシティ） | |
| パスコード認証 | 登録ユーザー数 最大 50,000 人 | |
| OS | 非公開 | |
| CPU | 非公開 | |
| メモリ | 2GB | |
| ストレージ | 16GB | |
| ディスプレイ | 720x1280 5 インチ タッチパネル | |
| カメラ | RGB カメラ（2MP） | |
| | IR カメラ（2MP） | |
| 無線 LAN | IEEE802.11 a/b/g/n（2.4GHz/5GHz） | |
| 有線 LAN | 10BASE-T/100BASE-TX（MDI-X 対応） | |
| | RJ45×1（PoE+ 25W 対応） | |
| インターフェース | Relay | |
| | 接点仕様： | 無電圧 c 接点 |
| | NO 端子： | ノーマルオープン |
| | NC 端子： | ノーマルクローズ |
| | ピンアサイン： | コネクタピンアサイン参照 |
| | 許容電力： | 最大 30W（DC）／最大 37.5VA（AC）※抵抗負荷時 |
| | 許容電圧： | 最大 30V（DC）／最大 125V（AC）※抵抗負荷時 |
| | 許容電流： | 最大 1A（DC）／最大 0.3A（AC）※抵抗負荷時 |
| 動作時環境条件 | 温度：0℃～40℃ | |
| | 湿度：10%～90%（ただし、結露無きこと） | |

| | |
|---|---|
| 保管時環境条件 | 温度：-20℃～60℃ |
| | 湿度：10%～90%（ただし、結露無きこと） |
| 入力電圧 | AC100V/1.5A（AC アダプタ使用時） |
| 消費電力 | 25W |
| 対応言語 | 日本語、英語（サポート窓口では日本語のみ対応） |
| 外形寸法(W×D×H) | 103x50x212 ㎜（レインカバーを取り付けた状態） |
| 質量 | 約 0.85 kg |
| 冷却ファン | 無し |
| 本体カラー | ブラック |
| 個装寸法(W×D×H) | 270×200×120 ㎜ |
| 梱包質量 | 約 1.6 kg |
| 保証期間 | 1 年間（別途有償保守サービス有り） |
| 法規対応 | RoHS 準拠、PSE 取得、技適取得 |
| 防塵・防水性能 | IP66 |

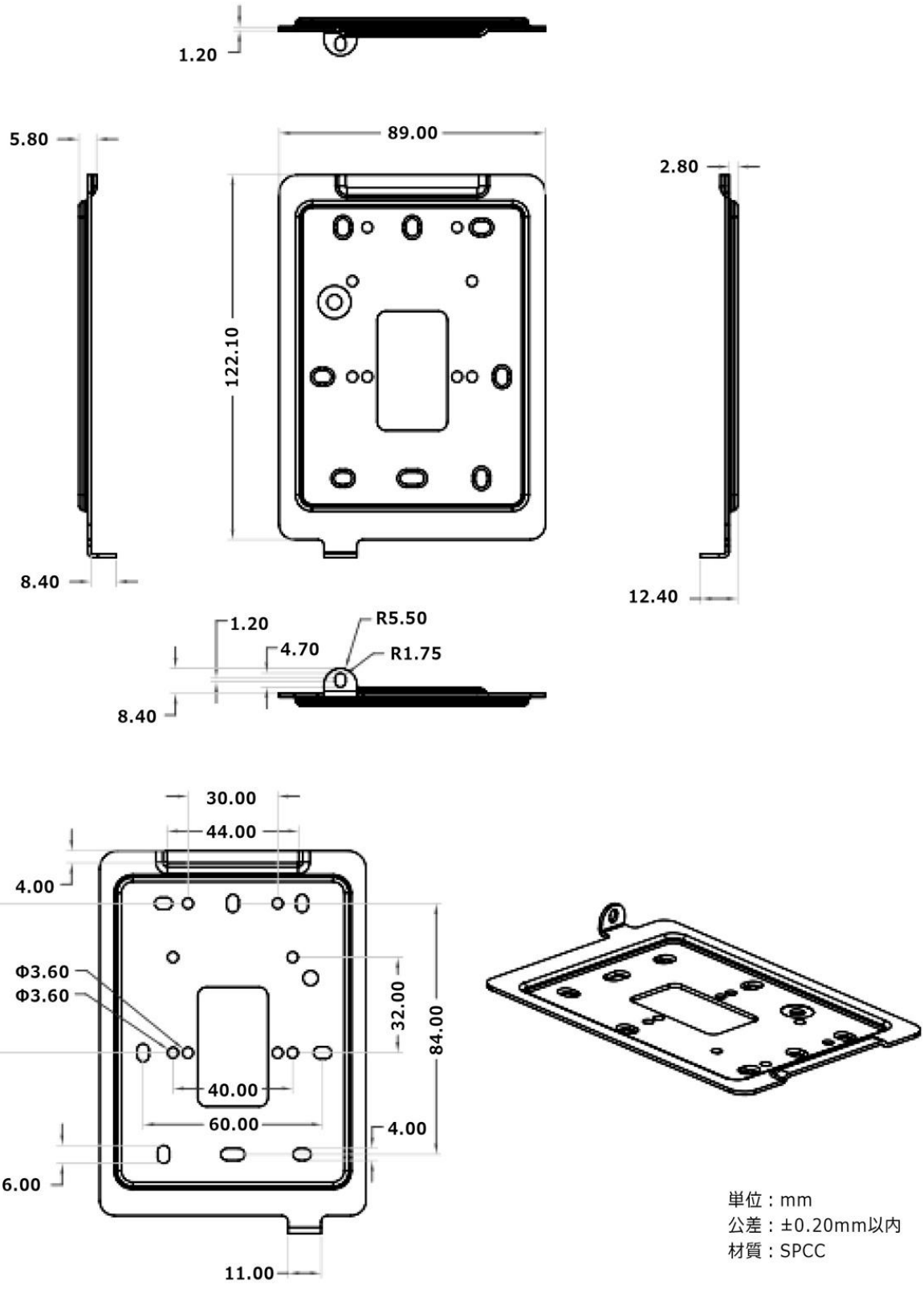
# 14. 付録 B 製品サイズ

| | 質量（約） | 外形寸法(W×D×H) |
|---|---|---|
| 顔認証デバイス本体 | 0.85 kg | 103 x 50 x 212 mm<br>※レインカバーを取り付けた状態 |
| フロアスタンド（別売品） | 7.0 kg | 440 x 265 x 1350 mm |

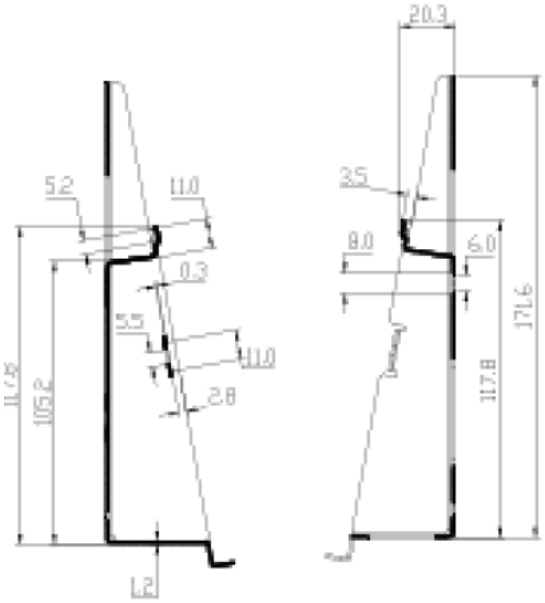
**顔認証デバイス本体**



**顔認証デバイス本体付属：固定用ブラケット**

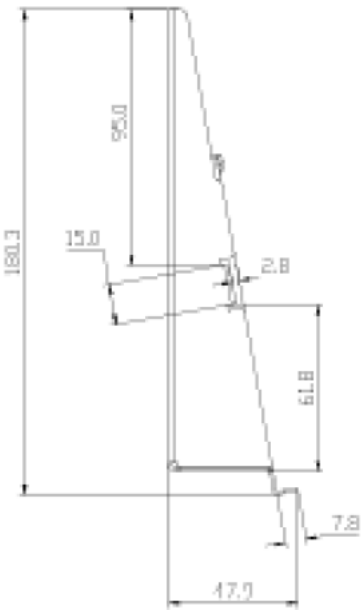


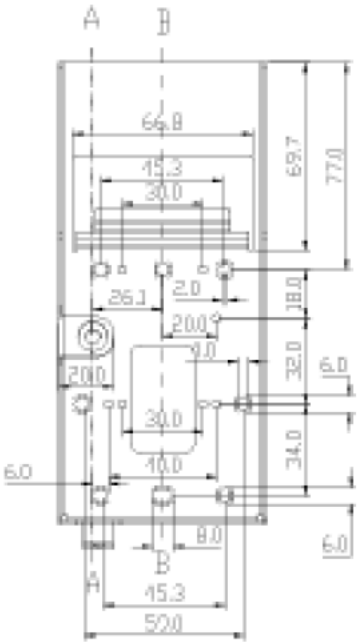
**顔認証デバイス本体付属：壁掛け用バックカバー**

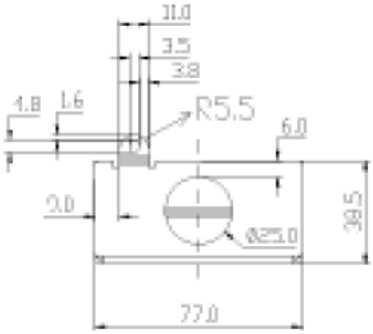


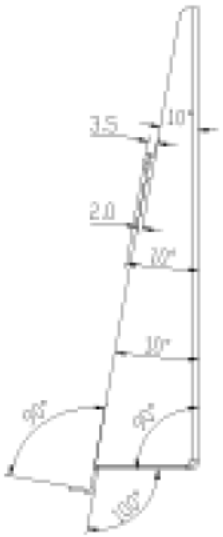

截面 A-A　　截面 B-B

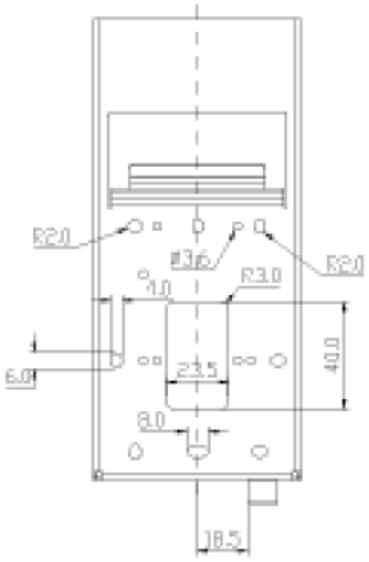


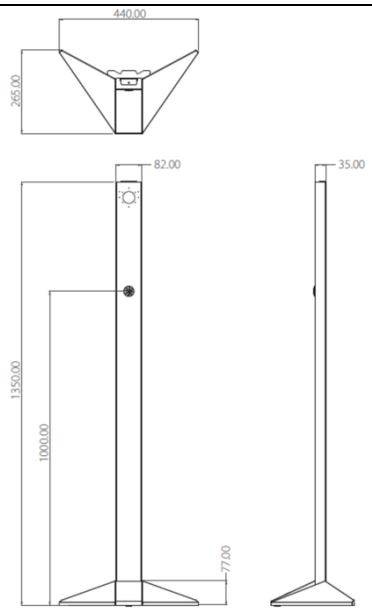




3.5
10°
2.0
10°
10°
90°
90°
105°


R2.0
ø3.6
R3.0
R2.0
1.0
40.0
6.0
23.5
8.0
18.5

**フロアスタンド（別売品）**


440.00
265.00
82.00
35.00
1350.00
1000.00
77.00

# 15. 付録 C 顔登録ガイドライン（外部リンク）

## 顔登録ガイドライン

**顔認証による本人認証で使用する写真は、国際規格に従うパスポート用写真の撮影と同じガイドラインです。**

顔認証は登録する写真から本人の特徴点（パーツの大きさ、位置など）を抽出してデータベース化を行います。写真の精度により、特徴点の抽出ができません。また、抽出できる特徴点が極端に少ない場合、他人と判定される確率が高くなります。認証率が低い・誤認証される場合、ガイドラインと比較して修正ポイントを確認してから顔写真の撮影をやり直してください。

### 適当な写真の例

1. 顔認証は目の周辺の変化が影響します。髪の毛、眼鏡、つけまつげ、まつげエクステ等の一部やその影が写りこまないようにします。



2. 輪郭が露出しているもの
3. 背景が無いもの（影や写り込みがないもの）
4. 人物と背景の境界線がはっきりとしているもの
5. 目線・体の向きが正面を向いて撮影されたもの
4. 顔登録から6か月以内に撮影されたもの
5. 無帽で過度な装飾品は身に着けていないもの
   ※業務上、打刻する時の容姿を再現するために身に着ける場合、認証率で判断してください
6. 写真サイズは、1920×1080ピクセル 以上



### 不適当な写真の例

#### 顔の向き、表情等



自然な表情で口をとじる。



口をとじ、大袈裟な表情をつくらない。



肩を水平にし、左右に偏らず顔が中央にくるようにする。



目線はカメラに向ける。



下を向かず、正面（カメラ）を見る。



目を閉じない。

#### 服装・装飾品等



タートルネック、マフラー、パーカーのフードなど、衣類などで顔の一部が隠れないようにする。



マスクなどは撮影時には完全に取り外して撮影する。



無帽で撮影する。

#### 背景※



背景に他の人が写りこまないようにする。



背景に物などが写りこまないようにする。人物（髪の色や服装など）と背景の境界線をはっきりさせる。



背景に撮影対象となる人物の影などがうつらないようにする。人物に当たる光を均一にする。

#### 画像品質



ノイズ（画像の乱れ）、ジャギー（階段状のギザギザ模様）、ピンボケした写真は使用しない。



目を大きくしたり、顔のパーツを加工したもの、変形やマスキングなどの画像処理したものは使用しない。



モノクロ写真や画像が粗い写真は使用せず、鮮明なカラー写真を使用する。

#### 影・光・目の周り



フラッシュや光等で、人物の顔やその一部が白飛びしないようにする。



光を均一に当て、顔や背景に影ができないようにする。



全体的に暗い写真の場合、光を均一に当て、全体の露出を高くする。



瞳の位置は眼鏡のフレームの中心にくるようにする。眼鏡に光が反射しないようにする。



眉や目に髪の毛が被らないようにする。目の周りの変化は特に認証率に影響があります。



カラーコンタクトは外し、フラッシュやライトの形状の写りこみ、瞳が赤く映らないようにする。

※背景は無地（単色）とし、背景と顔（髪）との境界線をはっきりさせること。また、顔や背景に影が写っていないこと。
※撮影するカメラアプリ等によって写真の左右反転する場合がありますが、不適当です。

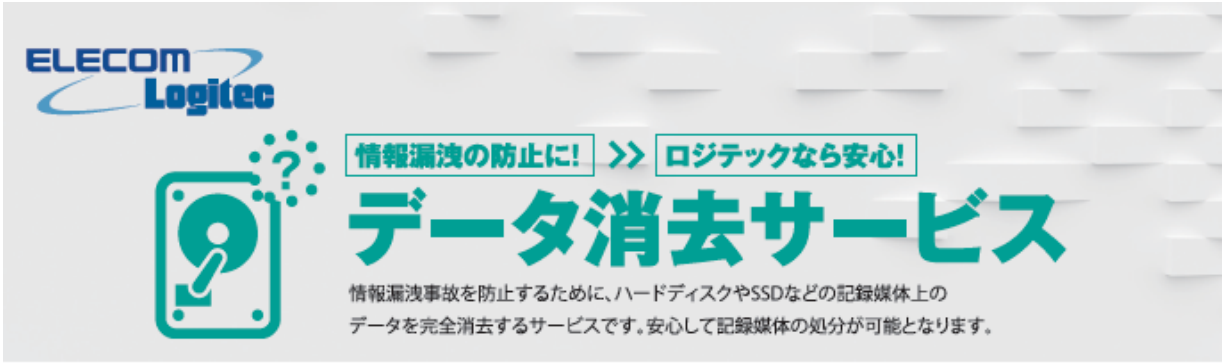
66003052 顔認証精度について 2024年6月 LTC-T80/LT80 Series V02

ロジテックINAソリューションズ株式会社 ©2024 Logitec INA Solutions Co.,Ltd, All rights reserved.

# 16. 付録 D データ消去サービスについて

端末内のデータ消去には専門サービスをご利用することをお勧めします。

データ消去サービス ｜ Logitec データ復旧技術センター




## データ消去の必要性

記録メディアに記録されたデータは、フォーマットしたりOSのリカバリを行っても完全に消去は行えません。企業や公共性の高い仕事で使用したパソコンや記録媒体等は、破壊する前に、情報が外部への流出を避けるため、専門の業者に依頼することが重要です。ロジテックでは、専門の技術者が、専用装置や専用ソフトを用いてデータを確実に消去いたします。また、情報の取り扱いについて厳しく管理しております。

**総務省"地方公共団体セキュリティポリシーガイドライン"に沿った**
**データ消去サービスなので安心です**

### 消去方法

**強磁気破壊方式**
HDD、テープ、FD、ZIPに対応
強磁界を印加し、物理破壊を伴わずに磁気データを破壊します。

**加圧変形破壊方式**
HDD、SSD、メモリカード、USBメモリ、光学メディアに対応
専用装置を使用してデータ記憶領域（プラッタ、メモリチップ）に物理的に加圧変形を加えて破壊します。

**ソフトウェア消去方式**
データ適正消去実行証明協議会
HDD、SSDに対応（搭載PC含む）
「OS等からアクセス可能なドライブの全領域」「OS等からアクセス可能な領域」に上書き消去・暗号化消去を行います。
※第三者機関による消去証明証の発行もできます。（有償）

| 対応メディア | HDD | SSD | FD | テープ | USBメモリ | メモリカード | 光学メディア |
|---|---|---|---|---|---|---|---|
| | 3.5型、2.5型 | | 3.5型FD、5型FD、ZIPディスク | CMT、DLT、DAT、LTO、DDS、3480テープ | | | |

## サービスご利用の流れ

お客様 WEB受付（WEBにてお申し込み） ▶ ロジテック 請求書を発行 ▶ お客様 発送とご入金（ロジテックへの配送費は、お客様負担） ▶ ロジテック データ消去作業 ▶ ロジテック 証明書発行

Webサイトからお申し込みいただけます。 http://www.logitec.co.jp/data_recovery/data_delete/

■個人情報保護について　当センターではセキュリティに関する国際規格(ISMS)を認証・取得して管理運営をしています。■FD、テープ、光学メディア以外のメディアは消去後に有価物として引き取ることが可能です。■本サービスはセンドバック消去サービスです。お客様から記録媒体をご送付いただき、弊社内でデータ消去を行います。

※弊社センターまでの送付料金はお客様ご負担とさせていただきます。　※対象機器から取り外しを行う場合「破棄」する可能性がございますので予めご了承のほどお願い致します。

**消去証明書の発行**
サービス完了時に、完全に消去した事を証明する「データ消去作業完了証明書」を発行いたします。

### お問い合わせ先

ロジテックはエレコムグループの会社です
**ロジテックINAソリューションズ株式会社**
〒396-0111 長野県伊那市美すず8268番地1000 ⑦番窓口

データ復旧技術センター　データ消去係
フリーコール 0800-888-6409
FAX.0265-74-1402