ASC-7213M

顔認証ミニアクセスコントローラ

取使説明書

V1.0.0

参照

一般

本書では、顔認証アクセスコントローラ(以下、アクセスコントローラと呼びます)の設置と基本操作について説明します。

安全上の注意

マニュアルには、意味が定義されている以下のカテゴリ別の注意喚起語が記載されている場合があります。

シグナルワード	意味
 危険	回避しないと、致命的または重傷につながる可能性のある高危険性を示します。
 警告	回避しない場合、軽度または中度の傷害を招く可能性がある中程度または低レベルの潜在的な危険性を示します。
 注意	回避しない場合、物的損害、データ損失、パフォーマンスの低下、または予期せぬ結果を招く可能性がある潜在的なリスクを示します。
 ヒント	問題の解決または時間の節約に役立つ方法を提供します。
 注	テキストの強調と補足として追加情報を提供します。

改訂履歴

バージョン	改訂内容	リリース日
V1.0.0	最初のリリース。	2020年12月

マニュアルについて

- 本書は参考用です。マニュアルと実際の製品の間に矛盾がある場合は、実際の製品が優先されます。
- 取扱説明書に準拠していない操作に起因する損失については、当社は一切責任を負いません。
- マニュアルは、関連地域の最新の法規制に従って更新されます。詳細については、紙の取扱説明書、CD-ROM、QRコード、または当社の公式ウェブサイトを参照してください。紙の取扱説明書と電子版に矛盾がある場合は、電子版が優先されます。
- すべての設計およびソフトウェアは、事前の文書による通知なしに変更されることがあります。製品のアップデートによって、実際の製品とマニュアルに一部違いが生じる場合があります。最新のプログラムと補足マニュアルについては、カスタマーサービスにお問い合わせください。

- それでも、技術データ、機能および操作の説明に逸脱がある場合や、印刷上のエラーがある場合があります。疑問や問題がある場合は、弊社の最終説明を参照してください。
- 取扱説明書(PDF形式)が開けない場合は、リーダーソフトウェアをアップグレードするか、他の主流のリーダーソフトウェアをお試しください。
- 取扱説明書に記載されている商標、登録商標、会社名は、それぞれの所有者の所有物です。
- 製品の使用時に問題が発生した場合は、当社のWebサイトにアクセスし、サプライヤまたはカスタマーサービスにお問い合わせください。
- 不確実性や問題がある場合は、弊社の最終説明を参照してください。

重要な安全対策と警告

本章では、アクセスコントローラの適切な取り扱い、危険防止、物的損害の防止について説明します。これらの内容をよく読んでから、アクセスコントローラを使用し、使用時に準拠し、後で参照できるように十分に保管しておいてください。

動作要件

- アクセスコントローラは、日光のあたる場所や熱源の近くに置いたり、設置したりしないでください。
- アクセスコントローラーを汚れ、粉じん、ばいじんから離れないようにしてください。
- 落下防止のため、アクセスコントローラは安定した場所に水平に設置しておいてください。
- アクセスコントローラに液を落としたりスプラッシュしたりしないでください。また、アクセスコントローラに液が流れ込むのを防ぐために、アクセスコントローラに液で満たされた物体がないことを確認してください。
- アクセスコントローラを通気の良い場所に設置し、アクセスコントローラの通気を遮断しないでください。
- アクセスコントローラは、電源入出力の定格範囲内でご使用ください。
- アクセスコントローラをランダムに分解しないでください。
- アクセスコントローラの輸送、使用、保管は、湿度と温度が許容される条件下で行ってください。

電気的安全性

- バッテリを不適切に使用すると、火災、爆発、または火災の原因となる場合があります。
- 電池交換の際は、同じ機種をご使用ください。
- 地域の推奨電源ケーブルを使用し、定格電力仕様に準拠してください。
- アクセスコントローラに付属の電源アダプタを使用しないと、けがやデバイスの損傷を招く可能性があります。
- 電源は、Safety Extra Low Voltage(SELV)規格の要件に準拠し、IEC60950-1に従ったLimited power source requirementに準拠した定格電圧の電源を供給する必要があります。電源の要件は、デバイスラベルに従うことに注意してください。
- デバイス(I型構造)を保護接地付き電源ソケットに接続してください。

目次

フォアワード I
重要な安全対策と警告 III
1 概要 1
1.1 序文 1
1.2 機能 1
1.3 アプリケーション 1
1.4 寸法と構成部品 2
2 接続とインストール 3
2.1 ケーブル接続 3
2.2 設置に関する注意事項 4
2.3 設置 5
2.3.1 モデルGの設置 5
3 システム操作 7
3.1 基本的な設定手順 7
3.2 共通アイコン 8
3.3 初期化 9
3.4 スタンバイインタフェース 9
3.5 メインメニュー 11
3.6 ロック解除方法 12
3.6.1 カード 12
3.6.2 顔 12
3.6.3 ユーザーパスワード 12
3.6.4 管理者パスワード 13
3.7 ユーザ 13
3.7.1 新規ユーザー 13
3.7.2 基本情報の確認 16
3.8 アクセス 16
3.8.1 期間管理 16
3.8.2 アンロックモード 17
3.8.3 アラーム 21
3.8.4 ドアステータス 22
3.8.5 ロック保持時間 22
3.9 出勤 22
3.10 接続 23
3.10.1 IP設定 24
3.10.2 アクティブ登録 24
3.10.3 シリアルポート 25
3.11 システム 33
3.11.1 時間 26

3.11.2 顔パラメータ 26
3.11.3 画像モード設定 27
3.11.4 音量 28
3.11.5 言語 28
3.11.6 赤外線ライト設定 28
3.11.7 スクリーン設定 28
3.11.8 出荷時設定の復元 28
3.11.9 リブート(再起動) 28
3.12 USB 29
3.12.1 USBエクスポート 29
3.12.2 USBインポート 30
3.12.3 USB更新 31
3.13 特徴 31
3.13.1 プライバシー設定 33
3.13.2 結果フィードバック 33
3.14 録画 34
3.15 装置情報 35
4 Web操作 36
4.1 初期化 36
4.2 ログイン 38
4.3 パスワードのリセット 39
4.4 アラーム連動 40
4.4.1 アラームリンクの設定 40
4.4.2 アラームログ 41
4.5 データ容量 42
4.6 ビデオ設定 42
4.6.1 データレート 43
4.6.2 画像 43
4.6.3 露光 45
4.6.4 動体検出 47
4.6.5 画像モード 49
4.7 顔検知 50
4.8 ネットワーク設定 51
4.8.1 TCP/IP 51
4.8.2 ポート 52
4.8.3 登録 53
4.9 安全管理 54
4.9.1 IP権限 54
4.9.2 システム 55
4.10 ユーザ管理 56
4.10.1 ユーザの追加 56
4.10.2 ユーザー情報の変更 56
4.10.3 ONVIFユーザ 56

4.11 メンテナンス 57
4.12 設定管理 57
4.12.1 設定ファイルのエクスポート 57
4.12.2 設定ファイルのインポート 58
4.13 更新 58
4.14 バージョン情報 59
4.15 オンラインユーザー 59
4.16 システムログ 60
4.16.1 ログ 60
4.16.2 バックアップログ 61
4.16.3 管理ログ 61
4.17 終了 61
5 SmartPSS AC設定 62
5.1 ログイン 62
5.2 デバイスの追加 62
5.2.1 自動検索 62
5.2.2 手動追加 63
5.3 ユーザ管理 64
5.3.1 カードタイプ設定 64
5.3.2 ユーザーの追加 65
5.3.3 カードー括発行 71
5.3.4 ユーザー情報のエクスポート 72
5.4 許可設定 72
5.4.1 許可グループの追加 72
5.4.2 許可の設定 74
5.5 アクセス管理 75
5.5.1 ドアをリモートで開く/閉じます 75
5.5.2 ノーマルオープンとノーマルクローズの設定 76
5.5.3 ドアステータスのリセット 76
5.6 出勤管理 77
5.6.1 レポート検索 77
5.6.2 その他の構成 78
6 FAQ 79
付録1顔記録/比較の注意事項 80
付録2サイバーセキュリティに関する推奨事項 83

1 概要

1.1 序文

アクセスコントローラは、顔、パスワード、カードによるロック解除をサポートし、それらの組み合わせによるロック解除をサポートするアクセスコントロールパネルです。

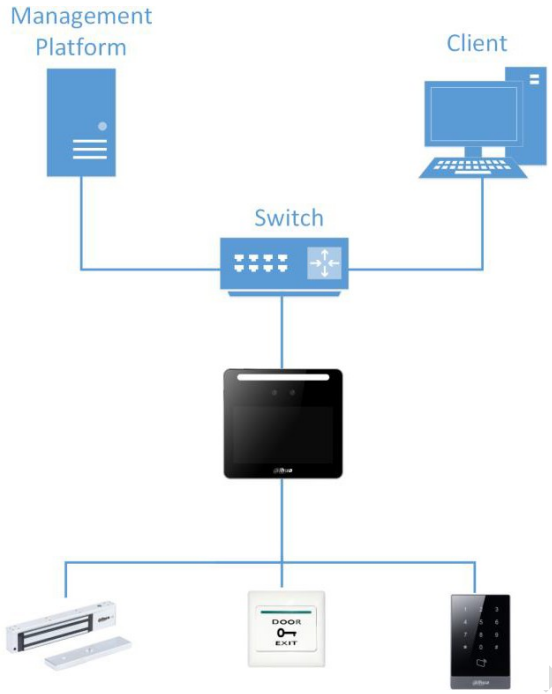
1.2 機能

- LCDディスプレイ、4.3インチアクセスコントローラの解像度は480×272です。
- 顔ロック解除、ICカードロック解除、指紋ロック解除、パスワードロック解除をサポート、期間ごとにロック解除
- 顔検出ボックスを使用すると、同時に表示される顔のうち最大の顔が最初に認識されます。最大の顔サイズはWebで設定できます。
- 2MP広角WDRレンズ;オート/マニュアルイルミネータ付き
- 顔認識距離は0.3m-1.5m
- 顔認識アルゴリズムにより、アクセスコントローラは人間の顔上で360以上の位置を認識できます
- 顔認証精度>99.5%、誤認識率低
- プロファイル認識をサポートします。プロファイルの角度は0°～90°です。
- ライブネス検出をサポートします
- デュレスアラーム、タンパアラーム、侵入アラーム、ドアコンタクトタイムアウトアラーム、不正カード超過しきい値アラーム、不正パスワード超過しきい値アラーム、外部アラームをサポート
- 一般ユーザー、パトロールユーザー、ブラックリストユーザー、VIPユーザー、ゲストユーザー、特殊ユーザー、カスタムユーザーをサポート
- 各種ロック解除状態表示モードにより、ユーザープライバシーを保護

1.3 アプリケーション

アクセスコントローラは、パーク、オフィスビル、学校、工場、住宅地などに適用されます。

図1-1ネットワーク



1.4 寸法と構成部品

図1-2　寸法と構成部品(mm[inch])

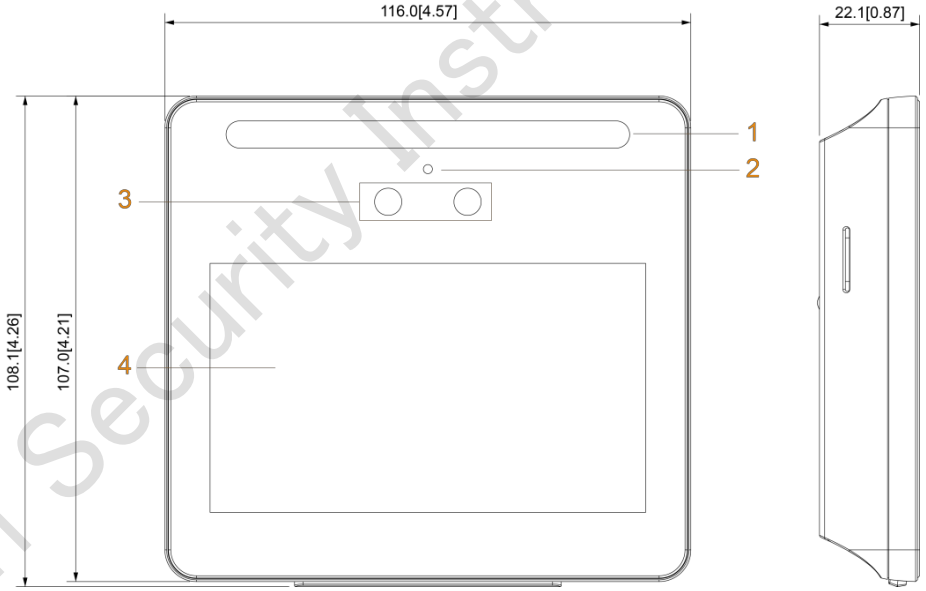


表1-1構成部品の説明

番号	名前	番号	名前
1	白色LEDイルミネータ	3	デュアルカメラ
2	マイク	4	表示

2 接続とインストール

2.1 ケーブル接続

- アクセスコントロールセキュリティモジュールが機能>セキュリティモジュールで有効になっているかどうかを確認します。有効になっている場合は、アクセス・コントロール・セキュリティ・モジュールを別途購入する必要があります。セキュリティモジュールには別途電源が必要です。
- セキュリティモジュールを有効にすると、終了ボタン、ターンスタイルコントロール、ファイアウォーティングリンケージは無効になります。

ケーブル接続

図2-1　ケーブル接続

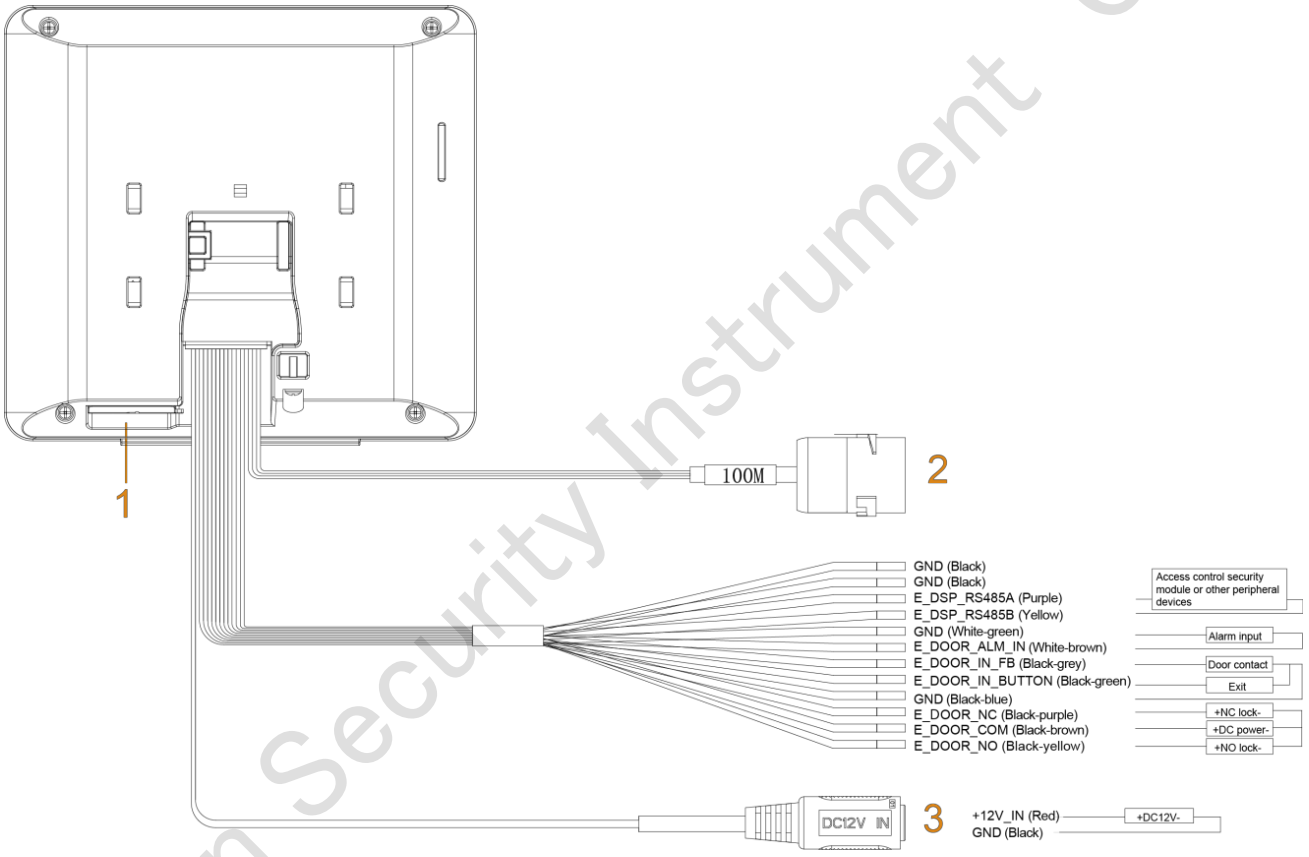


図2-2 ポート

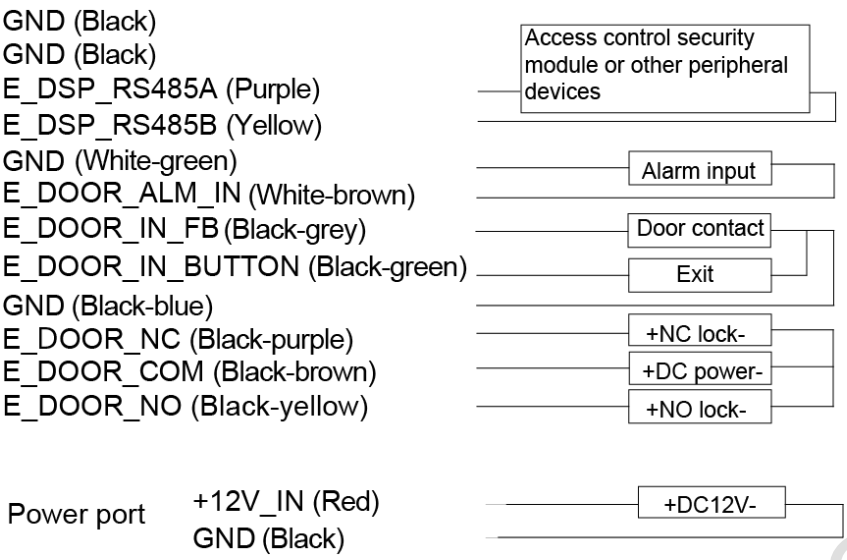


表2-1コンポーネントの説明(1)

番号	名前
1	USBポート
2	100Mネットワークポート
3	電源ポート

2.2 設置に関する注意事項

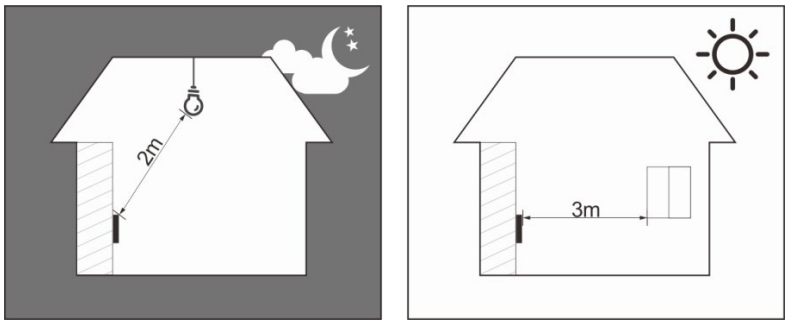
- アクセスコントローラから0.5メートル離れた場所にライトソースがある場合、最小照明は100Lux以上にする必要があります。
- アクセスコントローラは、窓やドアから3メートル以上離れた場所に屋内に設置し、ライトから2メートル離れた場所に設置することをお勧めします。
- バックライトと直射日光を避けます。

周囲照度要件

図2-5周囲照度要件

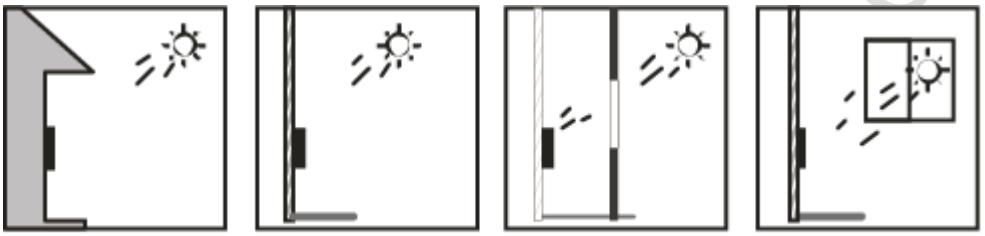
推奨場所

図2-6推奨される場所



推奨されない場所

図2-7推奨されない場所



2.3 設置

2.3.1 設置

デスクトップ設置

デスクトップブラケットのバックルをアクセスコントローラの背面スロットに挿入し、最後までスライドさせます。

図2-8デスクトップの取り付け(1)

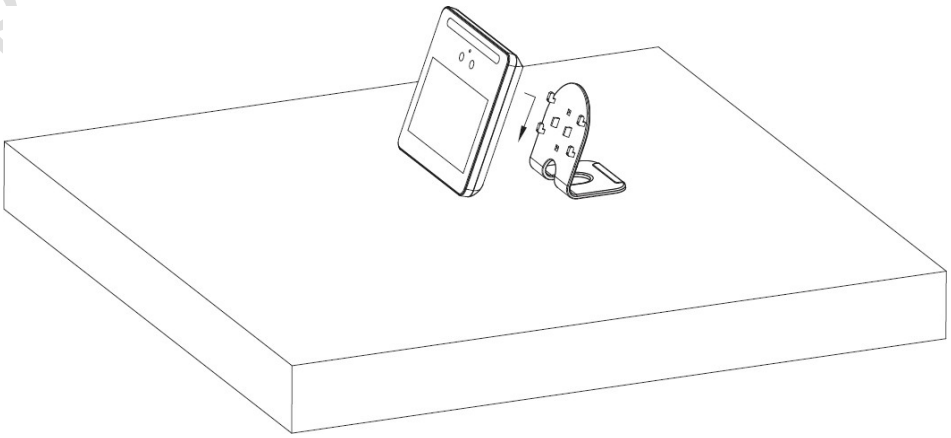
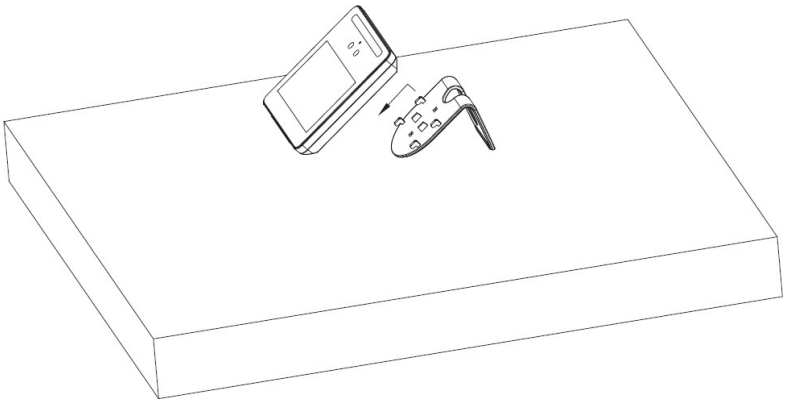


図2-9デスクトップの取り付け(2)



壁面設置

レンズとグラウンドの間の推奨距離は1.4～1.6メートルです。

図2-10設置高さ

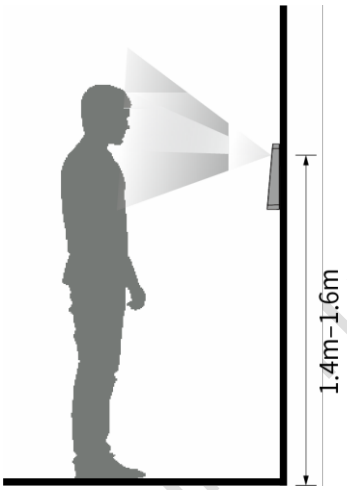
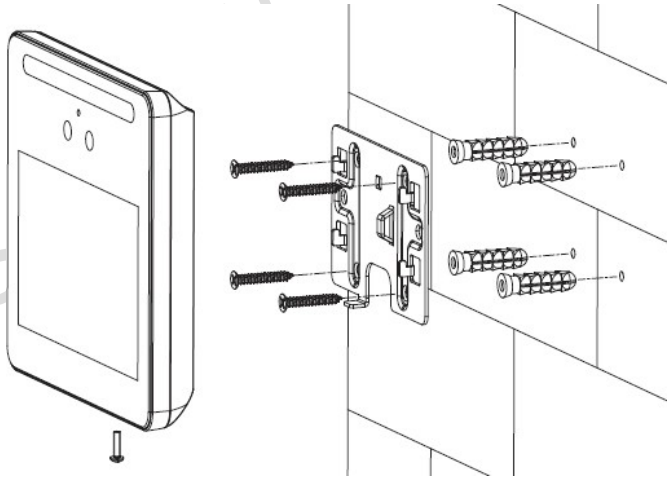


図2-11壁面設置



ステップ1ブラケットの穴に従って、壁に4つの穴を開けます。

ステップ2拡張ネジを4つのブラケット取り付け穴に取り付けて、ブラケットを壁面に固定します。

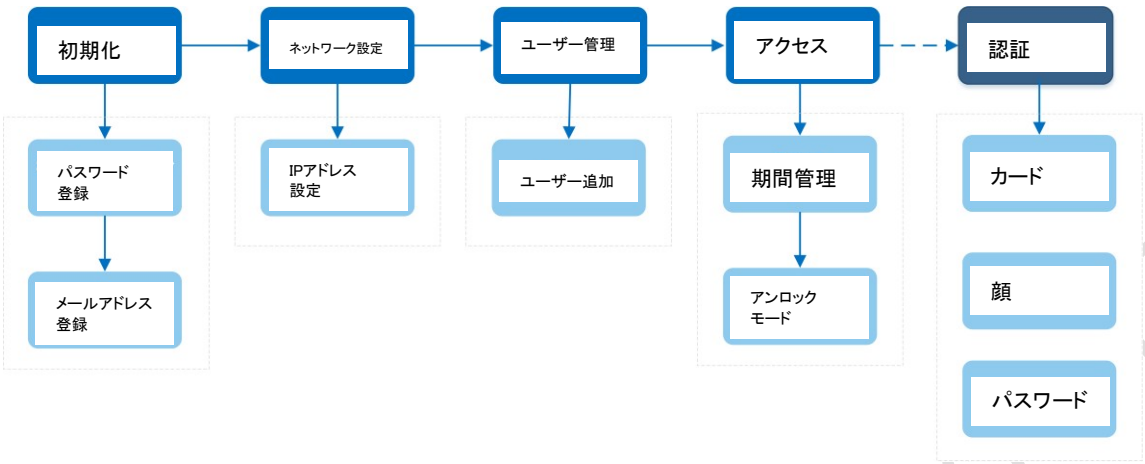
ステップ3アクセスコントローラ用のケーブルを接続します。「2.1ケーブルの接続」を参照してください。

ステップ4アクセスコントローラをブラケットフックに掛けます。

ステップ5アクセスコントローラの底部にあるネジを締めます。

3.1 基本的な設定手順

図3-1基本的な設定手順



3.2 共通アイコン

表3-1アイコンの説明

アイコン	説明
	確認アイコン。
	リストの最初のページに回します。
	リストの最後のページに回します。
	リストの前のページに移動します。
	リストの次のページに回します。
	前のメニューに戻ります。
	有効。
	無効。
	前のページに切り替えます。
	次のページに回します。

3.3 初期化

管理者パスワードと電子メールは、アクセスコントローラの初回電源投入時またはリセット後に設定する必要があります。設定しないと、アクセスコントローラを使用できません。

図3-2初期化

- このインターフェースで設定された管理者とパスワードは、Web管理プラットフォームへのログインに使用されます。
- 管理者パスワードは、管理者がパスワードを忘れた場合に、入力した電子メールアドレスを介してリセットできます。
- パスワードは、8～32文字の空白以外の文字で構成し、大文字、小文字、数字、特殊文字(''";:&を除きます)のうち、少なくとも2種類の文字を含む必要があります。

3.4 スタンバイインタフェース

顔、パスワード、カードを使ってドアのロックを解除できます。

- 30秒以内に何も操作しないと、アクセスコントローラはスタンバイモードに移行します。
- スタンバイインタフェースはバージョンによって異なる可能性があり、実際のインタフェースが優先されます。

図3-4スタンバイインタフェース

番号	説明
1	ロック解除方法:カード、顔、指紋、パスワード。 カード、顔、指紋、パスワードがすべてロック解除モードに設定されている場合、パスワードアイコンはアクセスコントローラの左上隅に表示されません。
2	日付と時刻。現在の日時を表示します。
3	ネットワークの状態とUSBの状態を表示します。
4	顔認識領域。
5	パスワードロック解除アイコン。
6	管理者パスワードロック解除アイコン。
7	カードスワイプ領域。

3.5 メインメニュー

管理者は、メインメニューで、さまざまなレベルのユーザの追加、アクセス関連パラメータの設定、ネットワーク設定、アクセスレコードとシステム情報の表示などを行うことができます。

ステップ1スタンバイインターフェースで、スクリーンを長押しして管理者ログインインターフェースに移動します。
ステップ2メインメニューの入力方法を選択します。

モードによって、異なるロック解除方法がサポートされ、実際のインタフェースが優先されます。

図3-5 管理者ログイン

メインメニューインタフェースが表示されます。

図3-6 メインメニュー

3.6 ロック解除方法

顔、パスワード、指紋、カードを介してドアのロックを解除できます。

3.6.1 カード

カードをカードスワイプエリアに置き、ドアのロックを解除します。

3.6.2 顔

顔が顔認識フレームの中央にあることを確認してから、ドアのロックを解除できます。

3.6.3 ユーザーパスワード

ユーザーパスワードを入力すると、ドアのロックを解除できます。

ステップ1　タップ＞ホームページ「パスワードロック解除」をタップします。

ステップ2　ユーザーIDとパスワードを入力し、をタップします。

ステップ3　ドアがロック解除されます。

3.6.4 管理者パスワード

管理者パスワードを入力すると、ドアのロックを解除できます。1つのアクセスコントローラには1つの管理者パスワードしかありません。管理者パスワードは、ユーザーレベル、ロック解除モード、期間、休日プラン、パスバック防止の影響を受けずにドアをロック解除できます。

「3.8.1.5NC周期」でNCを選択した場合、管理者パスワードは使用できません。

ステップ1　  タップ＞ホームページに。「管理パスワード」をタップします。

ステップ2　管理者パスワードを入力し、☑をタップします。

ステップ3　ドアがロック解除されます。

3.7 ユーザ

ユーザーインターフェースで、新しいユーザーの追加、ユーザーリストの表示、管理者リストの表示、管理者パスワードの変更を行うことができます。

3.7.1 新規ユーザー

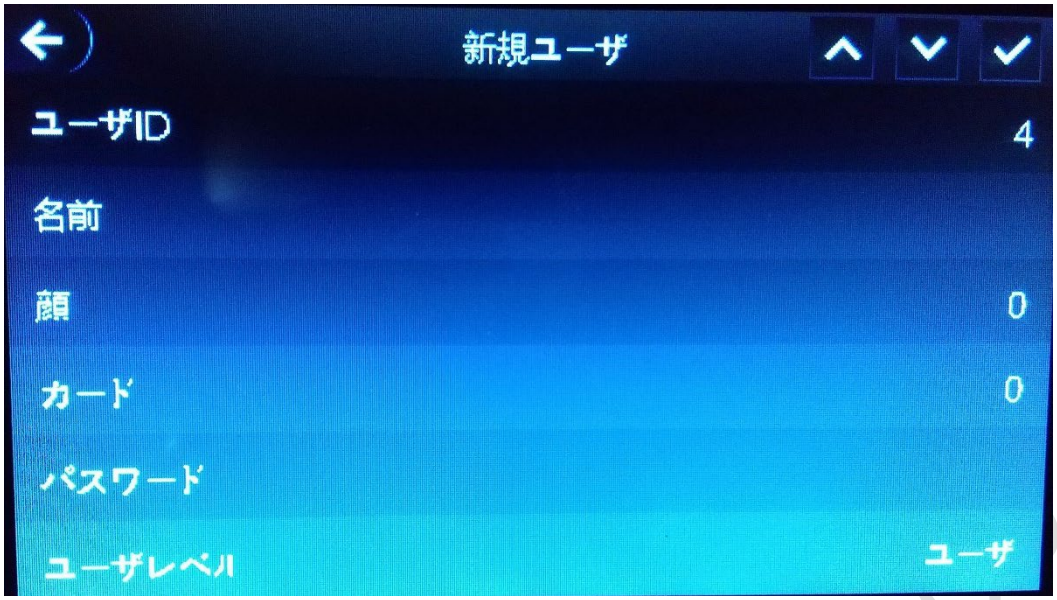
ユーザーID、名前、顔画像、カード、パスワード、ユーザーレベルの選択などを入力して、新しいユーザーを追加できます。

以下の図は参照専用であり、実際のインターフェースが優先されます。

ステップ1　メインメニューインタフェースにログインします。

ステップ2　ユーザー/新規ユーザーを選択します。

図3-7新規ユーザー情報



ステップ3　インターフェースでパラメータを設定します。

表3-3新規ユーザー・パラメーターの説明

パラメータ	説明
ユーザーID	ユーザーIDを入力します。 IDには数字、文字、およびその組み合わせを使用でき、IDの最大長は32文字です。各IDは一意です。
名前	名前は最大32文字(数字、記号、文字を含みます)まで入力できます。
指紋	1人のユーザーの指紋を最大3つまで記録でき、1つの指紋を3回検証する必要があります。 各指紋の下で脅迫FP機能を有効にすることができ、3つの指紋のうち1つのみを耐久性のある指紋にすることができます。耐久性のあるフィンガープリントを使用してドアのロックを解除すると、アラームがトリガーされます。 📖 ● 耐久性のある指紋として最初の指紋を選択することはお勧めしません。 ● 指紋ロック解除は、指紋センサー付きのアクセスコントローラでのみサポートされます。
顔	顔が画像取り込みフレームの中央にあることを確認します。アクセスコントローラが新しいユーザーの顔の画像を自動的に取得します。

カード	ユーザーごとに最大5枚のカードを登録できます。カード登録インターフェースで、カード番号を入力するか、カードをスワイプすると、カード情報がアクセスコントローラによって読み取られます。 カード登録インターフェースで脅迫カード機能を有効にすることができます。耐久性カードを使用してドアのロックを解除すると、アラームがトリガーされます。 📖 カードロック解除は、特定の機種でのみサポートされます。
パスワード	ドアロック解除パスワード。パスワードの最大長は8桁です。 📖 アクセスコントローラがタッチスクリーンなしの場合は、アクセスコントローラを周辺機器カードリーダーに接続する必要があります。カードリーダーにはボタンがあります。
ユーザーレベル	新しいユーザーのユーザーレベルを選択できます。2つのオプションがあります: ● ユーザー:ユーザーにはドアロック解除権限のみがあります。 ● 管理者:管理者はドアのロックを解除でき、パラメータ設定権限も持つことができます。 📖 アクセスコントローラに管理者がいるかどうかにかかわらず、管理者ID認証が必要です。
期間	ユーザーがドアのロックを解除できる期間を設定できます。
休日プラン	ユーザーがドアのロックを解除できる休日プランを設定できます。
有効日付	ユーザーのロック解除情報が有効な期間を設定できます。
ユーザーレベル	6つのレベルがある: ● 一般:一般ユーザーは、ドアを通常どおりにロック解除できます。 ● ブラックリスト:ブラックリストのユーザーがドアのロックを解除すると、サービス担当者にプロンプトが表示されます。 ● ゲスト:ゲストは、ドアを特定の時間ロック解除できます。最大時間を超えると、ドアを再びロック解除することはできません。 ● パトロール:パトロールユーザーは出席状況を追跡できますが、ロック解除権限はありません。 ● VIP:VIPがドアのロックを解除すると、サービス担当者にプロンプトが表示されます。 ● 特殊:特別な人がドアのロックを解除すると、ドアが閉じるまでに5秒の遅延が発生します。 ● Custom User1:カスタマイズ用に予約済み。ユーザーはドアのロックを通常どおり解除できます。 ● Custom User2:カスタマイズ用に予約済み。 ユーザーはドアのロックを通常どおり解除できます。
使用時間	ユーザーレベルが「ゲスト」の場合、ユーザーがドアのロックを解除できる最大回数を設定できます。

ステップ4 ホーム画面 ✔ 設定を保存します。

3.7.2 基本情報の確認

ユーザーインターフェースを使用して、ユーザーリスト、管理者リスト、および管理者パスワードを表示できます。

3.8 アクセス

アクセス管理は、期間、ロック解除モード、アラーム、ドアステータス、ロック保持時間で行うことができます。アクセス管理インターフェースに移動するには、「アクセス」をタップします。

3.8.1 期間管理

期間、休日期間、休日プラン期間、ドアノーマルオン期間、ドアノーマルクローズ期間、およびリモート検証期間を設定できます。

3.8.1.1 期間の設定

ローカルで期間を設定することができます。

数値の範囲が0～127の128期間(週)を設定できます。期間(週)の各日に4つの期間を設定できます。ユーザーは、設定した期間でのみドアのロックを解除できます。

3.8.1.2 休日ホリデーグループ

休日グループをローカルで設定できます。

グループ休日を設定し、休日グループのプランを設定できます。0～127の範囲で128のグループを設定できます。1つのグループに16の祝日を追加できます。祝日グループの開始時刻と終了時刻を設定すると、ユーザーは設定した期間でのみドアのロックを解除できます。

名前は32文字(数字、記号、文字を含みます)で入力できます。タップ＞祝日グループ名を登録します。

3.8.1.3 休日プランの設定

休日プランをローカルで設定できます。

休日プランに休日グループを追加できます。休日プランを使用して、異なる休日グループのユーザーアクセス権限を管理することができます。ユーザーは、設定した期間内にのみドアのロックを解除できます。

3.8.1.4 NO期間

NO期間に期間が追加された場合、ドアは通常その期間内に開いています。NO/NC期間の許可は、他の期間の許可よりも高くなります。

3.8.1.5 NC期間

NC期間にピリオドが追加された場合、ドアは通常その期間内に閉じられます。ユーザーはこの期間内にドアのロックを解除することはできません。

3.8.1.6 リモート認証期間

リモート検証期間を設定した場合、設定した期間中にドアのロックを解除すると、リモート検証が必要になります。この期間でドアのロックを解除するには、管理プラットフォームから送信されたドアのロック解除指示が必要になります。

リモート検証期間を有効にする必要があります。

-  有効を意味します。
-  無効を意味します。

3.8.2 アンロックモード

アンロックモードには、アンロックモード、ピリオドによるアンロック、およびグループの組み合わせの3つがあります。ロック解除モードはコントローラアクセスモデルによって異なり、実際のコントローラアクセスが優先されます。

3.8.2.1 アンロックモード

ロック解除モードがオンの場合、ユーザーはカード、顔、パスワード、またはすべてのロック解除方法のいずれかを使用してロックを解除できます。

ステップ1　メインメニューインタフェースにログインします。

ステップ2　アクセス/ロック解除モード/ロック解除モードを選択します。

図3-8要素(複数選択)

ステップ3 ロック解除モードを選択。

選択したロック解除モードをもう一度タップすると、ロック解除モードが削除さ

ステップ4 れます。コンビネーションモードを選択します。

- + および は「選択したエレメントすべて」を意味します。たとえば、カード+パスワードを選択した場合は、ドアのロックを解除するには、まずカードをスワイプしてからパスワードを入力する必要があります。

ステップ5

- / または は「選択したエレメントのうちひとつ」を意味します。たとえば、カード/パスワードを選択した場合は、ドアのロックを解除するために、カードをスワイプするか、パスワードを入力することができます。

ステップ6 タップして設定を保存します。
その後、「ロック解除モード」インターフェースが表示さ
れます。ロック解除モードを有効にします。

- 有効を意味します。
- 無効を意味します。

3.8.2.2 時間帯によるアンロック

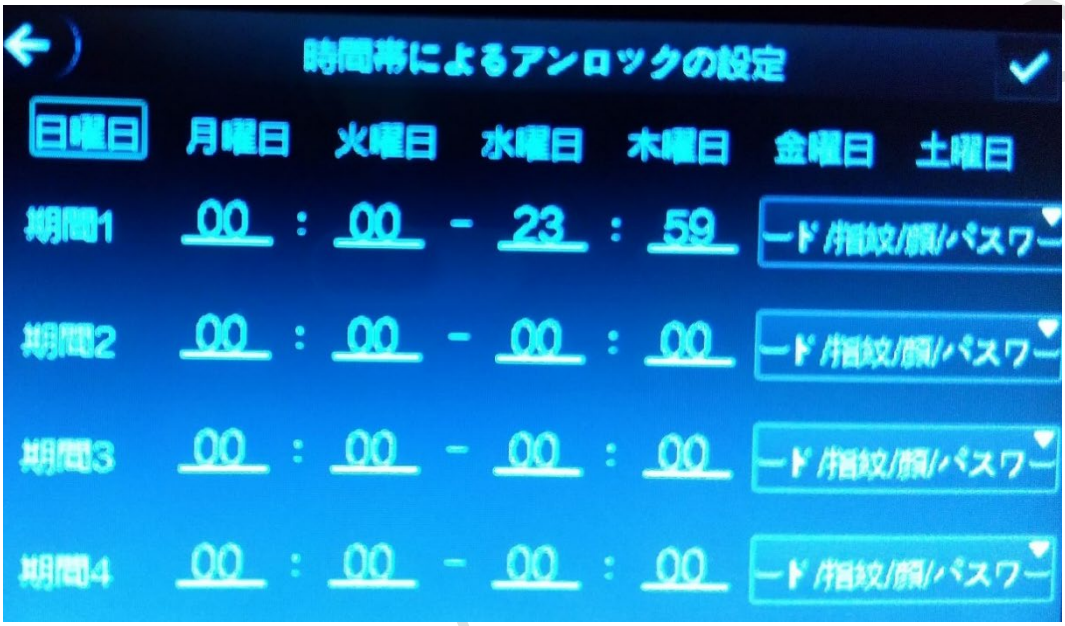
ローカルで期間ごとにアンロックを設定できます。

ドアは、さまざまなロック解除モードを通じて、さまざまな期間でロック解除することができます。たとえば、期間1では、ドアはカードからしかロック解除できず、期間2では、ドアは面からしかロックできません。

ステップ1　メインメニューインタフェースにログインします。

ステップ2　アクセス>ロック解除モード>期間ごとのロック解除を選択します。

図3-9周期によるロック解除



ステップ3　期間の開始時刻と終了時刻を設定し、ロック解除モードを選択します。タップして設定を保存します。

ステップ4　ロック解除モードのインタフェースが表示されます。Unlock by Period機能を有効にします。

ステップ5　■  有効を意味します。

■  無効を意味します。

3.8.2.3 グループの組み合わせ

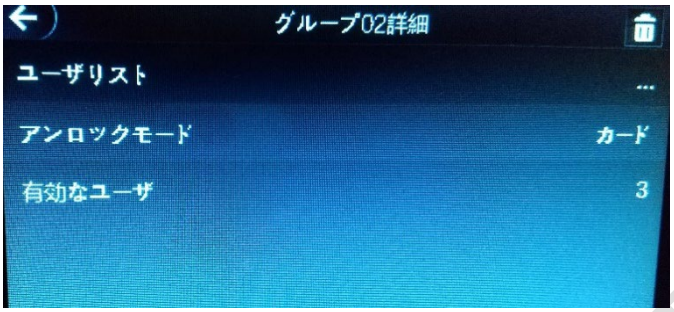
グループコンビネーションを局所的に構成することができます。

ドアは、グループの組み合わせが有効になっている場合、複数のユーザーで構成されるグループによってのみロック解除できます。

ステップ1　メインメニューインタフェースにログインします。

ステップ2　アクセス/ロック解除モード/グループの組み合わせを選択します。

図3-10グループの組み合わせ



ステップ3　タップしてグループを作成します。

図3-11グループの追加

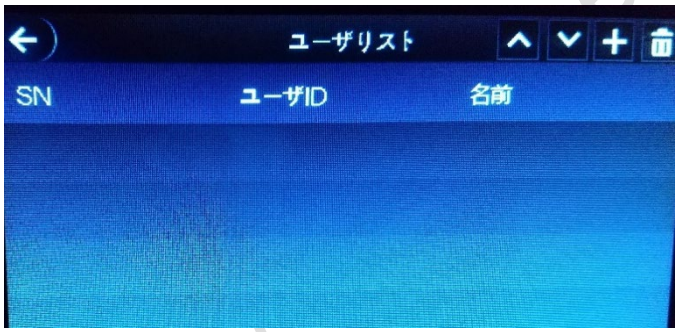


表3-4Groupパラメータ

パラメータ	説明
ユーザーリスト	新しく作成したグループにユーザーを追加します。 1. 「ユーザリスト」をタップします。 User Listインターフェースが表示されます。 2. タップし、ユーザーIDを入力します。 3. タップして設定を保存します。
ロック解除モード	カード、パスワード、顔の3つのオプションがあります。

有効なユーザー	有効なユーザーは、ロック解除権限を持つユーザーです。ドアのロックを解除できるのは、ドアのロックを解除するユーザー数が有効なユーザー数と等しい場合のみです。 ● 有効なユーザーは、グループ内のユーザーの合計数を超えることはできません。 ● 有効なユーザーがグループ内の合計ユーザー数と等しい場合、ドアはグループ内のすべてのユーザーのみがロック解除できます。 ● 有効なユーザーがグループ内の合計ユーザー数より少ない場合、ドアは有効なユーザー数と等しい数のユーザーによってロック解除できます。

ステップ4　前のインターフェースに戻るには をタップします。

ステップ5　タップして設定を保存します。グループの組み合わせを有効にします。

ステップ6　■ 有効を意味します。

■ 無効を意味します。

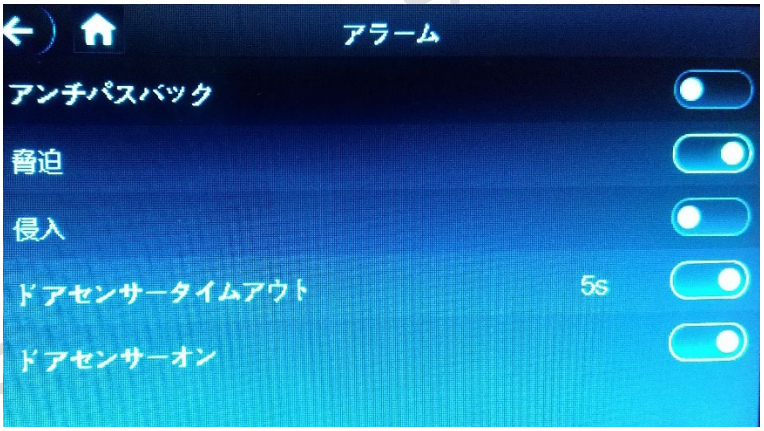
3.8.3 アラーム

管理者は、アラーム設定によってビジターのロック解除権限を管理できます。

ステップ1　メインメニューインタフェースにログインします。

ステップ2　アクセス>アラームを選択します。アラームインターフェースが表示されます。

図3-12アラーム



■ 有効を意味します。

■ 無効を意味します。

表3-5アラーム・インターフェースのパラメータ

パラメータ	説明
アンチパスバック	アンチパスバックが有効になった後、ユーザは入口と出口の両方でIDを検証する必要があります。そうしないと、アラームがトリガーされます。 ● IDをチェックした状態で入室し、IDをチェックせずに終了すると、その人が再び入室しようとしたときにアラームがトリガーされ、その人にはドアのロックを解除する権限がなくなります。 ● 本人確認を行わずに入室した場合、本人確認を行ったまま退出しようとしたときにアラームが発生し、その人にはドアをアンロックする権限がなくなります。.
脅迫	耐久性カードまたは耐久性パスワードを使用してドアのロックを解除すると、アラームがトリガーされます。
不正なカード時間超過	不正なカードを使用してドアのロックを50秒間に5回以上解除すると、アラームがトリガーされます。
侵入	ドアの接点が解除されずにドアがロック解除されると、侵入アラームがトリガーされます。
ドアセンサータイムアウト	ドアのロック解除にかかる時間がドアセンサーのタイムアウト時間を超えると、タイムアウトアラームがトリガーされます。 ドアセンサータイムアウト時間の範囲は1～9999秒です。
ドアセンサー	ドアセンサーオンが有効になっている場合のみ、侵入アラームとドアセンサータイムアウトアラームをトリガーできます。

3.8.4 ドアステータス

NO、NC、正常の3つのオプションがあります。

- NO:NOを選択すると、ドアステータスは通常開になり、ドアは閉じられません。
- NC:NCを選択した場合、ドアのステータスは通常閉じられます。つまり、ドアはロック解除されません。
- 正常:設定に応じてドアのロックが解除され、ロックされます。

3.8.5 ロック保持時間

ロック保持時間は、ロックが解除される期間です。ロックが継続時間を超える期間ロック解除されている場合は自動的にロックされます。

3.9 出勤

出勤を有効にし、出勤モードを設定できます。自動/手動、オート、手動、固定の4つのモードがあります。

出勤状況には、チェックイン、退勤、再出勤、チェックアウト、残業開始、残業終了の6つがあります。

ステップ1　メインメニューインタフェースにログインします。

ステップ2　出勤をタップし、 をタップして出勤を有効にします。

図3-13出席

ステップ3　「モード設定」をタップして、応答モードとさまざまな状況の期間を設定します。

- 「自動/手動モード」:スタンバイインターフェースでパンチインまたはパンチアウトしたときに、出勤時間に応じて自動的に出勤状況が表示されます。また、スタンバイインターフェースでパンチイン/アウトしたときに、手動でアテンダント状況を選択することもできます。
- 自動モード:スタンバイインターフェースでパンチイン/アウトしたときに、出勤時刻に応じて自動的に出勤状況を表示します。
- マニュアルモード:スタンバイインターフェースでパンチインまたはパンチアウトすると、手動で出勤状況を選択する必要があります。
- 固定モード:スタンバイインターフェースでパンチインまたはパンチアウトするときに、アテンダントステータスが固定されます。

3.10 接続

アクセスコントローラを正常に動作させるには、ネットワーク、シリアルポート、およびWiegandポートのパラメータを設定する必要があります。

3.10.1 IPアドレス

アクセスコントローラのIPアドレスを設定して、ネットワークに接続できるようにします。

ステップ1　メインメニューインタフェースにログインします。

ステップ2　接続>ネットワーク>IPアドレスを選択し、IPアドレスパラメータを設定します。

図3-14IPアドレスの設定

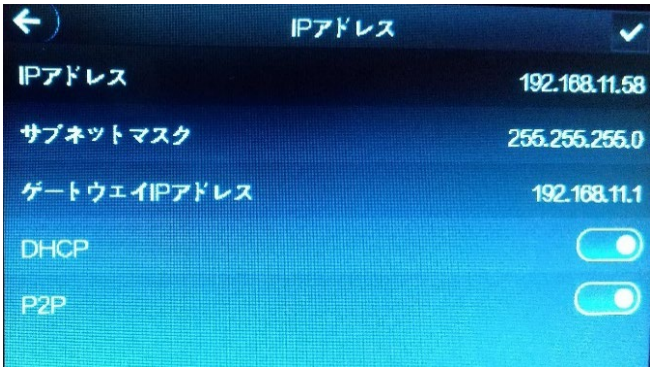


表3-6IP設定パラメータ

パラメータ	説明
IPアドレス/サブネットマスク/ゲートウェイIPアドレス	IPアドレス、サブネットマスク、およびゲートウェイIPアドレスは、同じネットワークセグメント上にある必要があります。設定後、をタップして設定を保存します。
DHCP	DHCP(Dynamic Host Configuration Protocol). DHCPを有効にすると、IPアドレスの自動取得が可能になり、IPアドレス、サブネットマスク、ゲートウェイIPアドレスを手動で設定できなくなります。
P2P	P2Pはプライベートネットワークトラバーサルテクノロジーで、DDNS、ポートマ ッピング、トランジットサーバーを必要とせずにデバイスを管理できます。

Webへのログインに使用するコンピュータがデバイスと同じLANにあることを確認してください。

3.10.2 アクティブ登録

アクティブな登録により、アクセスコントローラを管理プラットフォームに接続し、管理プラットフォームを介してアクセスコントローラを管理できます。

お客様が行った設定は、管理プラットフォーム上でクリアすることができ、アクセスコントローラを初期化することができます。不正な操作によってデータが失われた場合に備えて、プラットフォーム管理権限を保護する必要があります。

ステップ1　メインメニューインタフェースにログインします。

ステップ2　接続>ネットワーク設定>アクティブ登録を選択すると、アクティブ登録画面が表示されます。

ステップ3　タップしてアクティブ登録を有効にし、パラメータを設定します。

表3-7アクティブレジスタ

名前	パラメータ
サーバIPアドレス	管理プラットフォームのIPアドレス。
ポート	管理プラットフォームのポート番号。
デバイスID	管理プラットフォームの下位デバイス番号。

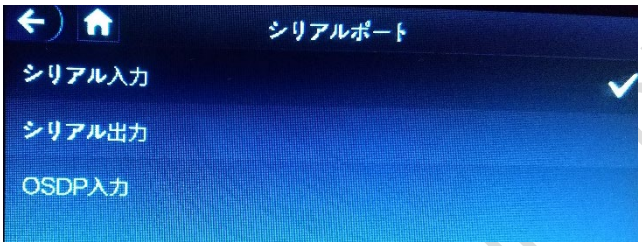
3.10.3 シリアルポート

外部機器の用途に応じて、シリアル入力またはシリアル出力を選択します。

ステップ1　メインメニューインタフェースにログインします。

ステップ2　接続>シリアルポートを選択すると、シリアルポートインターフェースが表示されます。

図3-16シリアルポート



- カードの読み書き機能を持つ外部機器がアクセスコントローラに接続されている場合は、「シリアル入力」を選択します。Serial Input(シリアル入力)は、アクセスカード情報をアクセスコントローラおよび管理プラットフォームに送信できるようにするために選択されます。
- 顔認識機能を持つアクセスコントローラの場合、カードの読み取りおよび書き込み機能を選択すると、アクセスコントローラはアクセスコントローラにロック/アンロック情報を送信します。ロック/アンロック情報には、次の2種類があります:
  - ■ ユーザーID
  - ■ カード番号
- OSDPプロトコルのカードリーダーがアクセスコントローラに接続されている場合は、OSDP入力を選択します。アクセスコントローラは、カード情報を管理プラットフォームに送信できます。

3.11 システム

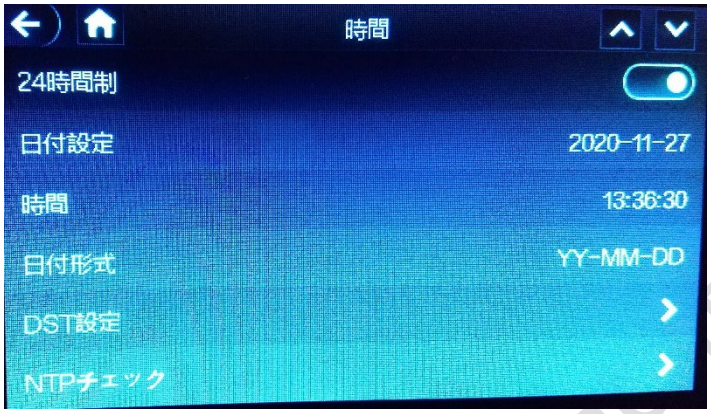
3.11.1 時間

日付形式の設定、日付の設定、時刻の設定、サマータイムの設定、NTPチェック、タイムゾーンの設定ができます。

ステップ1　メインメニューインタフェースにログインします。

ステップ2　システム>時間を選択し、時間パラメータを設定します。

図3-18時刻



NTP(Network Time Protocol)を選択する場合は、まずNTPチェック機能を有効にする必要があります。「サーバIPアドレス」:タイムサーバのIPアドレスを入力します。アクセスコントローラの時刻がタイムサーバと同期されます。

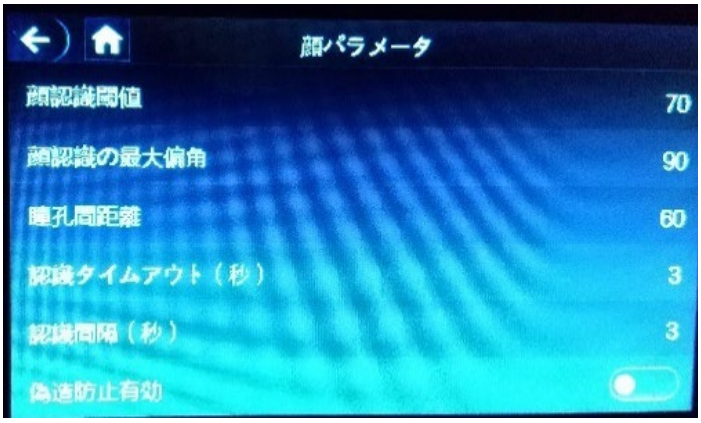
- ポート:タイムサーバのポート番号を入力します。
- Interval(min):NPTチェック間隔。保存する保存アイコンをタップします。

3.11.2 顔パラメータ

ステップ1　メインメニューインタフェースにログインします。

ステップ2　「システム」>「顔パラメータ」と選択すると、「顔パラメータ」インターフェースが表示されます。

図3-19顔パラメータ



ステップ3パラメータをタップして設定を行い、 をタップします。

表3-9顔パラメータ

パラメータ	説明
顔のしきい値	顔認識の精度を調整できます。 値が大きいほど、精度は高くなります。
最大面の角度	プロファイルのコントロールパネル撮影角度を設定します。 値が大きいほど、プロファイルの範囲が広く認識されます。
瞳孔距離	刺しゅう距離とは、各目の視点の中心間にある画像のピクセル値のことです。アクセスコントローラが必要に応じて顔を認識できるように、適切な値を設定する必要があります。顔の大きさや、顔とレンズの距離によって値が変わります。面がレンズに近づくほど、値は大きくなります。 成人がレンズから1.5メートル離れている場合、刺しゅう距離の値は50～70の範囲内になります。
認識タイムアウト	有効な顔認識中のプロンプトの間隔。
プロンプト間隔	無効な顔認識中のプロンプトの間隔。
偽造防止閾値	人物の顔画像や顔モデルによるロック解除を防止します。 値が大きいほど、顔画像が難しくなりドアのロックを解除できます。推奨値の範囲は80を超えています。

3.11.3 画像モード設定

3つのオプションがあります:

- 屋内:アクセスコントローラが屋内に設置されている場合、屋内を選択します;
- 屋外:アクセスコントローラが屋外に設置されている場合は屋外を選択;
- その他:アクセスコントローラがバックライトのある場所に設置されている場合は、「その他」を選択します。

3.11.4 音量


をタップして、音量を調整します。

3.11.5 言語

言語は、英語、日本語です。

3.11.6 赤外線ライト設定


をタップして、赤外線ライトの明るさを調整します。値が大きいほど、赤外光が明るくなります。

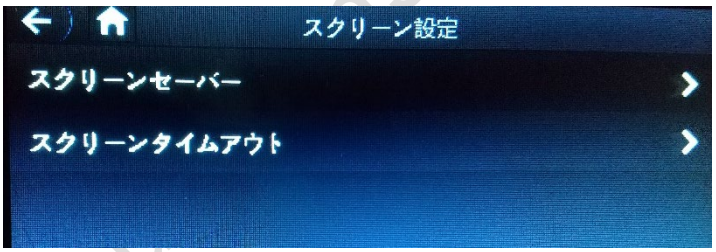
3.11.7 スクリーン設定

スクリーンセーバー時間とスクリーンオフ時間を設定できます。

ステップ1　メインメニューインタフェースにログインします。

ステップ2　システム>スクリーン設定を選択すると、スクリーン設定インタフェースが表示されます。

図3-20画面設定



3.11.8 出荷時設定の復元

- アクセスコントローラを工場出荷時の設定に復元すると、データは失われます。
- アクセスコントローラを工場出荷時の設定に復元した後は、IPアドレスは変更されません。

ユーザー情報やログを保持するかどうかを選択できます。

- すべてのユーザー情報とデバイス情報を削除した状態で、アクセスコントローラを工場出荷時の設定に復元するかどうかを選択できます。
- ユーザー情報とデバイス情報を保持した状態で、アクセスコントローラを工場出荷時の設定に復元することを選択できます。

3.11.9 リブート(再起動)

ステップ1　メインメニューインタフェースにログインします。
ステップ2　システム>再起動を選択すると、アクセスコントローラが再起動されます。

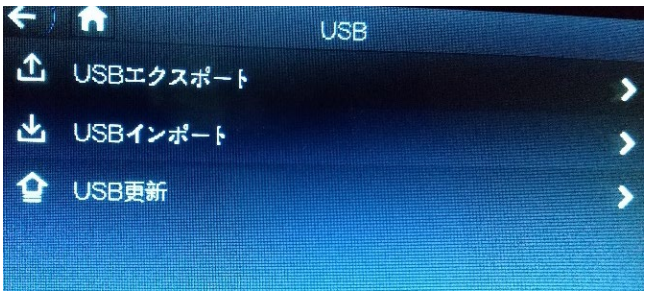
3.12 USB

- ユーザー情報をエクスポートして更新する前に、USBが挿入されていることを確認してください。エクスポート中やアップデート中は、USBを抜いたり、その他の操作を行わないでください。そうしないと、エクスポートやアップデートに失敗します。
- USBを使用して別のアクセスコントローラに情報をインポートする前に、1つのアクセスコントローラからUSBに情報をインポートする必要があります。
- USBを使用してプログラムをアップデートすることもできます。

3.12.1 USBエクスポート

USBを挿入した後、アクセスコントローラからUSBにデータをエクスポートできます。エクスポートされたデータは暗号化され、編集できません。
ステップ1　メインメニューインタフェースにログインします。USB>USBエクスポートを選択します。
ステップ2　USBエクスポートインタフェースが表示されます。

図3-21USBエクスポート



ステップ3　エクスポートするデータ型を選択します。エクスポートの確認プロンプトが表示されます。OKをタップします。

ステップ4　エクスポートされたデータはUSBに保存されます。

3.12.2 USBインポート

アクセスコントローラからエクスポートされたUSB内のデータのみを別のアクセスコントローラにインポートできます。

ステップ1　メインメニューインタフェースにログインします。USB>USB インポートを選択します。

ステップ2　USBインポートインタフェースが表示されます。

ステップ3　インポートするデータ型を選択します。インポートを確認するプロンプトが表示されます。OKをタップします。

ステップ4　USBメモリー内のデータがアクセスコントローラーに取り込まれます。

3.12.3 USB更新

USBフラッシュドライブを使用して、システムを更新することができます。

ステップ1　アップデートファイル名を「update.bin」に変更し、「update.bin」ファイルをUSBフラッシュドライブのルートディレクトリに保存します。

Webへのログインに使用するコンピュータが、デバイスと同じLANにあることを確認してください。

ステップ2　メインメニューインタフェースにログインします。USB>USBアップデートを選択します。

ステップ3　アップデートの確認プロンプトが表示されます。
OKをタップします。

ステップ4　アップデートが開始され、アップデートの終了後にアクセスコントローラが再起動します。

3.13 特徴

プライバシー、カード番号反転、セキュリティモジュール、ドアセンサータイプ、結果フィードバックに関する設定を行うことができます。

ステップ1　メインメニューインタフェースにログインします。

ステップ2　「機能」をタップすると、「機能」のインターフェースが表示されます。

図3-23機能

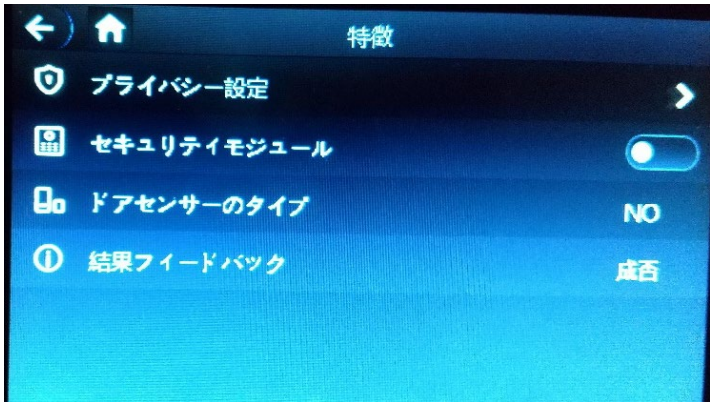


表3-10機能の説明

パラメータ	説明
プライバシー設定	詳細は「3.13.1プライバシー設定」を参照してください。
セキュリティモジュール	● セキュリティモジュールが有効になっている場合は、アクセスコントロールセキュリティモジュールを別途購入する必要があります。セキュリティモジュールは、電力を供給するために別々の電源装置を必要とします。 ● セキュリティモジュールが有効になると、終了ボタン、ロック制御、ファイアウォーティング連携は無効になります。
ドアセンサー	NOとNCの2つのオプションがあります。
結果フィードバック	ロック解除中の結果フィードバックモードを選択します。 結果フィードバックモードには、「成功/失敗」、「名前のみ」、「写真と名前」、「写真と名前」の4つがあります。

3.13.1 プライバシー設定

図3-24プライバシー設定

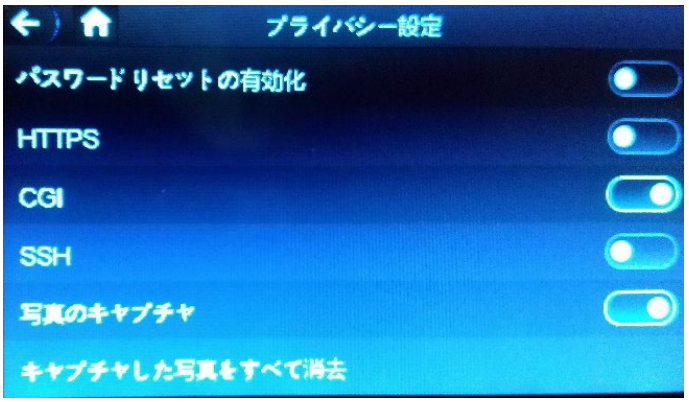


表3-11プライバシー設定

パラメータ	説明
パスワードリセット 有効	有効にすると、パスワードをリセットできます。 パスワードリセット機能は、デフォルトで有効になっています。
HTTPS	HTTPS(Hypertext Transfer Protocol Secure)は、コンピュータネットワークを介したセキュアな通信のためのプロトコルです。 HTTPSを有効にすると、CGIコマンドへのアクセスにHTTPSが使用されます。 それ以外の場合はHTTPが使用されます。 HTTPSが有効になると、アクセスコントローラは自動的に再起動します。
CGI	Common Gateway Interface(CGI)は、Webページを動的に生成するサーバー上で実行されるコンソールアプリケーションのように実行するプログラムをWebサーバーが実行するための標準プロトコルを提供します。 CGIが有効な場合、CGIコマンドを使用できます。 CGIはデフォルトで有効になっています。
SSH	セキュアシェル(SSH)は、セキュアでないネットワーク上でネットワークサービスを安全に運用するための暗号化ネットワークプロトコルです。 SSHが有効な場合、SSHはデータ送信のための暗号化サービスを提供します。
写真のキャプチャ	「ON」を選択すると、ユーザーがドアのロックを解除すると、ユーザーの写真が自動的に撮影されます。この機能はデフォルトでオンになっています。
すべてクリア 撮影した 写真	アイコンをタップすると、撮影したすべての写真を削除できます。

3.13.2 結果フィードバック

結果フィードバックモードには、「成功/失敗」、「名前のみ」、「写真と名前」、「写真と名前」の4つがあります。必要に応じて結果フィードバックモードを選択できます。

写真&ネームモード

ロック解除中は、撮影した顔画像、顔データベースに保存されている画像、ユーザーID、ユーザー名、時刻がすべて表示されます。

写真&名前モード

ロック解除中は、顔データベースに保存されている画像、ユーザーID、ユーザー名、時刻がすべて表示されます。

ネームモードのみ

ロック解除中は、ユーザーID、ユーザー名、時刻のみ表示されます。

成功/失敗モード

ロック解除中に成功または失敗のみを表示します。

3.14 録画

すべてのロック解除レコードを照会できます。

図3-29パンチレコードの検索

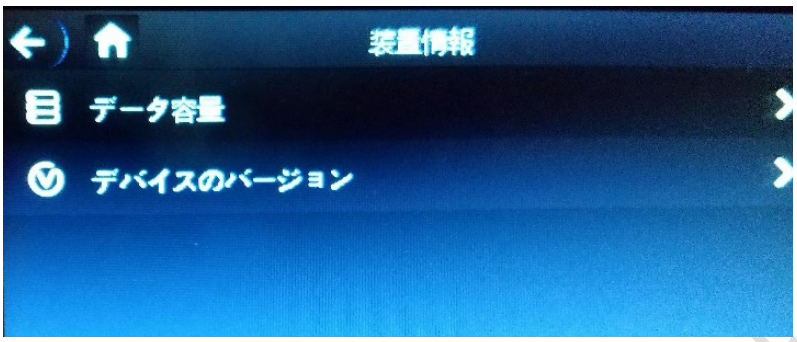
3.15 装置情報

装置情報インタフェースで、アクセスコントローラのデータ容量、デバイスバージョン、およびファームウェア情報を表示できます。

ステップ1　メインメニューインタフェースにログインします。

ステップ2　「システム情報」をタップすると、「システム情報」インターフェースが表示されます。

図3-30システム情報



4　Web操作

アクセスコントローラは、Web上で設定および操作することができます。Webを介して、ネットワークパラメータ、ビデオパラメータ、およびアクセスコントローラパラメータを設定したり、システムを保守および更新したりすることもできます。

4.1 初期化

Webに初めてログインする前に、パスワードと電子メールアドレスを設定する必要があります。

ステップ1　IE Webブラウザを開き、アドレスバーにアクセスコントローラのIPアドレス(デフォルトアドレスは192.168.1.108)を入力し、Enterキーを押します。

- IE8よりも新しいブラウザを使用します。そうしないと、Webにログインできない場合があります。
- Webへのログインに使用するコンピュータが、デバイスと同じLANにあることを確認します。

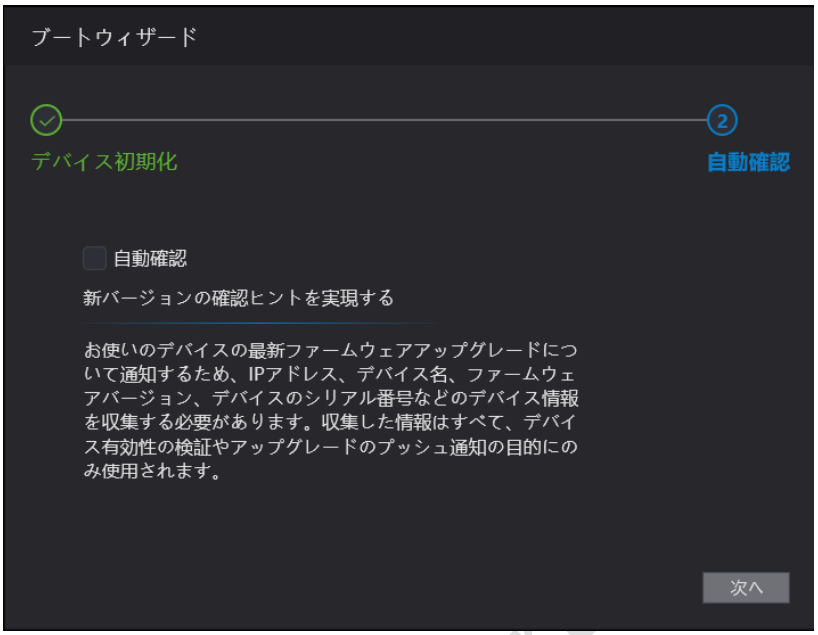
ステップ2　新しいパスワードを入力し、パスワードを確認して、電子メールアドレスを入力し、決定をクリックします。

- パスワードは、8～32文字の空白以外の文字で構成し、大文字、小文字、数字、特殊文字('";:&を除きます)のうち、少なくとも2種類の文字を含む必要があります。パスワード・ストレングス・プロンプトに従って、高セキュリティー・レベルのパスワードを設定します。
- セキュリティのため、初期化後はパスワードを適切に保持し、定期的にパスワードを変更してください。
- QRコードを読み取って管理者パスワードをリセットする必要がある場合は、セキュリティコードを受信するためにメールアドレスが必要です。

ステップ3　自動チェックを選択するかどうかを決定できます。

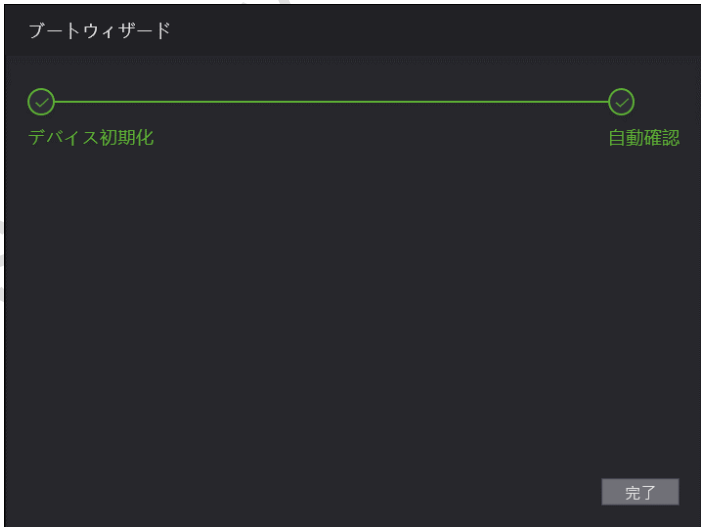
最新のプログラムを実行するには、Auto Check(自動チェック)を選択することをお勧めします。次へをクリックします。

図4-2自動チェック



ステップ4

図4-3設定の終了



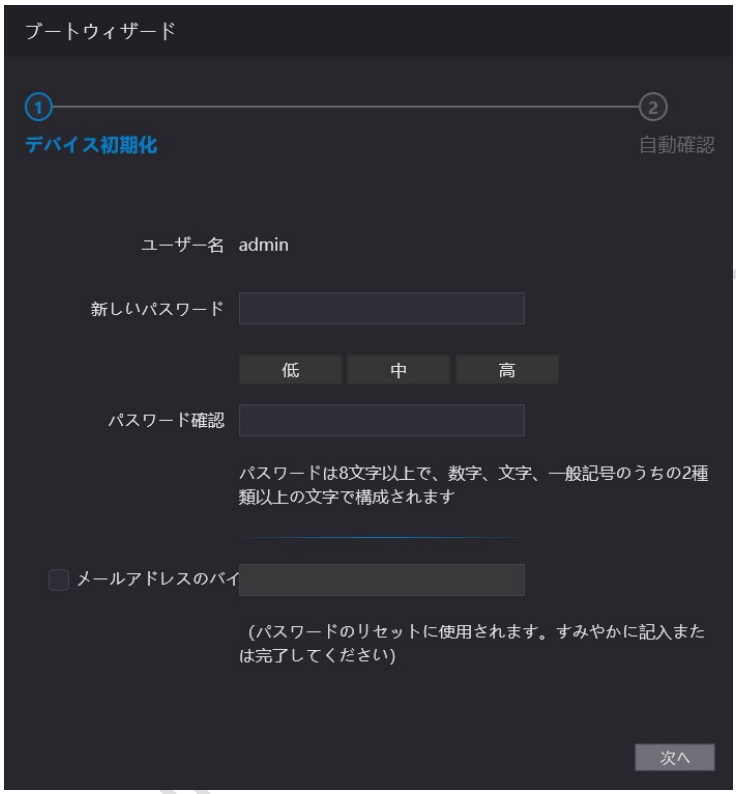
ステップ6　完了をクリックすると、初期化が完了します。

4.2 ログイン

ステップ1　IE Webブラウザを開き、アドレスバーにアクセスコントローラのIPアドレスを入力し、Enterキーを押します。

- IE8よりも新しいブラウザを使用します。そうしないと、Webにログインできない場合があります。
- Webへのログインに使用するコンピュータが、デバイスと同じLANにあることを確認します。
- デフォルトのIPアドレスは192.168.1.108です。

図4-4ログイン



ステップ2　ユーザー名とパスワードを入力します。

- デフォルトの管理者名はadmin、パスワードはアクセスコントローラの初期化後のログインパスワードです。管理者を定期的に変更し、セキュリティのために適切に保管しておいてください。

  管理者のログインパスワードを忘れた場合は、パスワードを忘れた場合？をクリックしてリセットします。「4.3パスワードのリセット」を参照してください。

  ログインをクリックします。

ステップ3　Webインターフェースがログインされています。

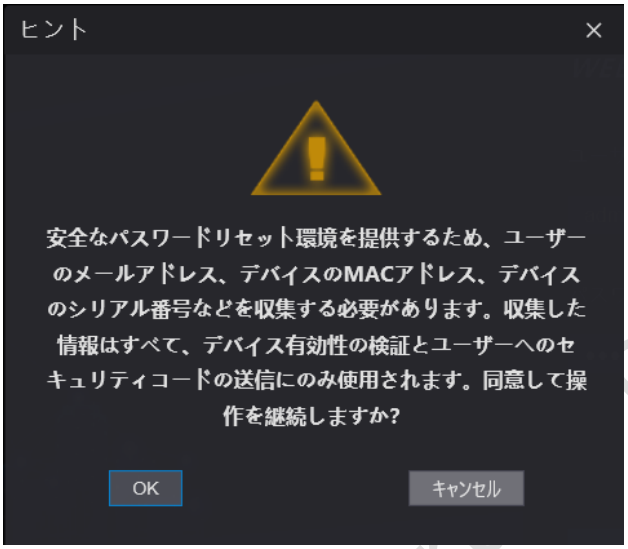
4.3 パスワードのリセット

管理者アカウントのパスワードをリセットする場合は、電子メールアドレスが必要になります。

ステップ1「パスワードを忘れた場合？」をクリックします。

ログインインターフェースで。Tipsインタフェースが表示されます。

図4-5ヒント



ステップ2　注意事項を確認し、[OK]をクリックします。

ステップ3　パスワードのリセットインタフェースが表示されます。

ステップ4　インターフェース上のQRコードをスキャンすると、暗証番号が取得されます。

- 同じQRコードを読み取ると、最大2つの暗証番号が生成されます。暗証番号が無効になった場合は、さらに暗証番号を取得するには、QRコードを更新してください。
- QRコードを読み取った後に取得した内容を指定したメールアドレスに送信し、暗証番号を取得する必要があります。端末暗証番号は、受信後24時間以内にご利用ください。それ以外の場合は無効になります。
- 暗証番号を5回続けて間違えると、管理者は5分間凍結されます。

ステップ5　受信した暗証番号を入力します。

ステップ6　次へをクリックします。

ステップ7　パスワードのリセットインタフェースが表示されます。新しいパスワードをリセットして確認します。

パスワードは、8～32文字の空白以外の文字で構成し、大文字、小文字、数字、特殊文字('";:&を除きます)のうち、少なくとも2種類の文字を含むようにしてください。

ステップ8　OKをクリックすると、リセットが完了します。

4.4 アラーム連動

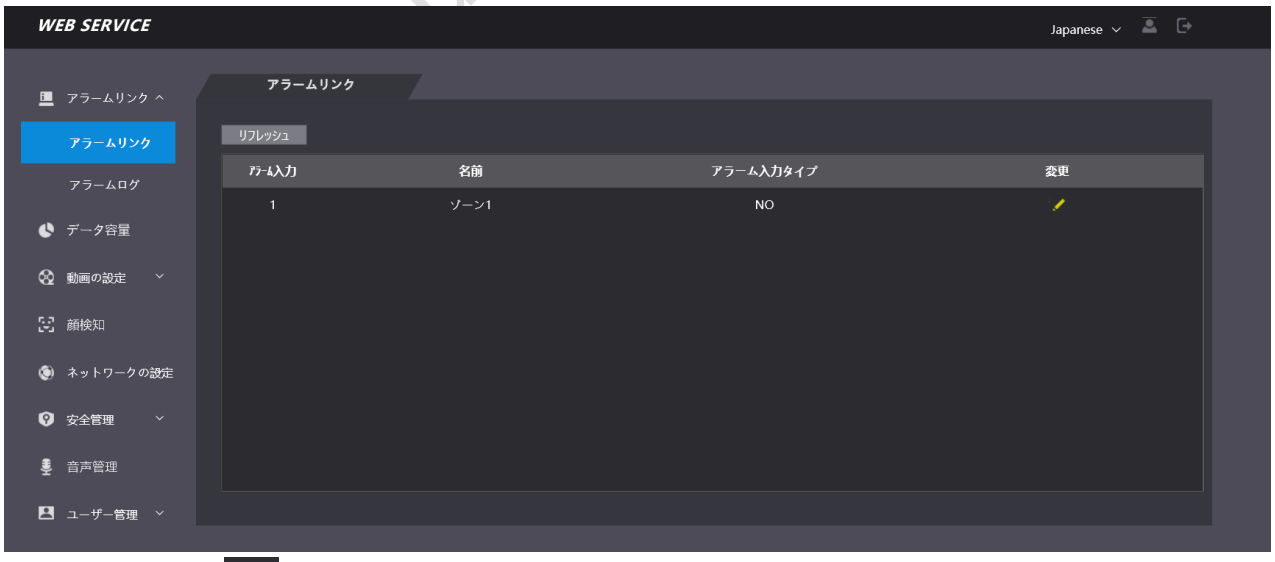
4.4.1 アラームリンクの設定

アラーム入力デバイスをアクセスコントローラに接続し、必要に応じてアラーム連動パラメータを変更することができます。

ステップ1　Webインターフェースにログインします。

ステップ2　ナビゲーションバーの「アラームリンク」を選択します。アラームリンクインターフェースが表示されます。

図4-7アラーム連動



ステップ3　をクリックしアラームリンクのパラメータを変更できます。

図4-8アラームリンクパラメータの変更

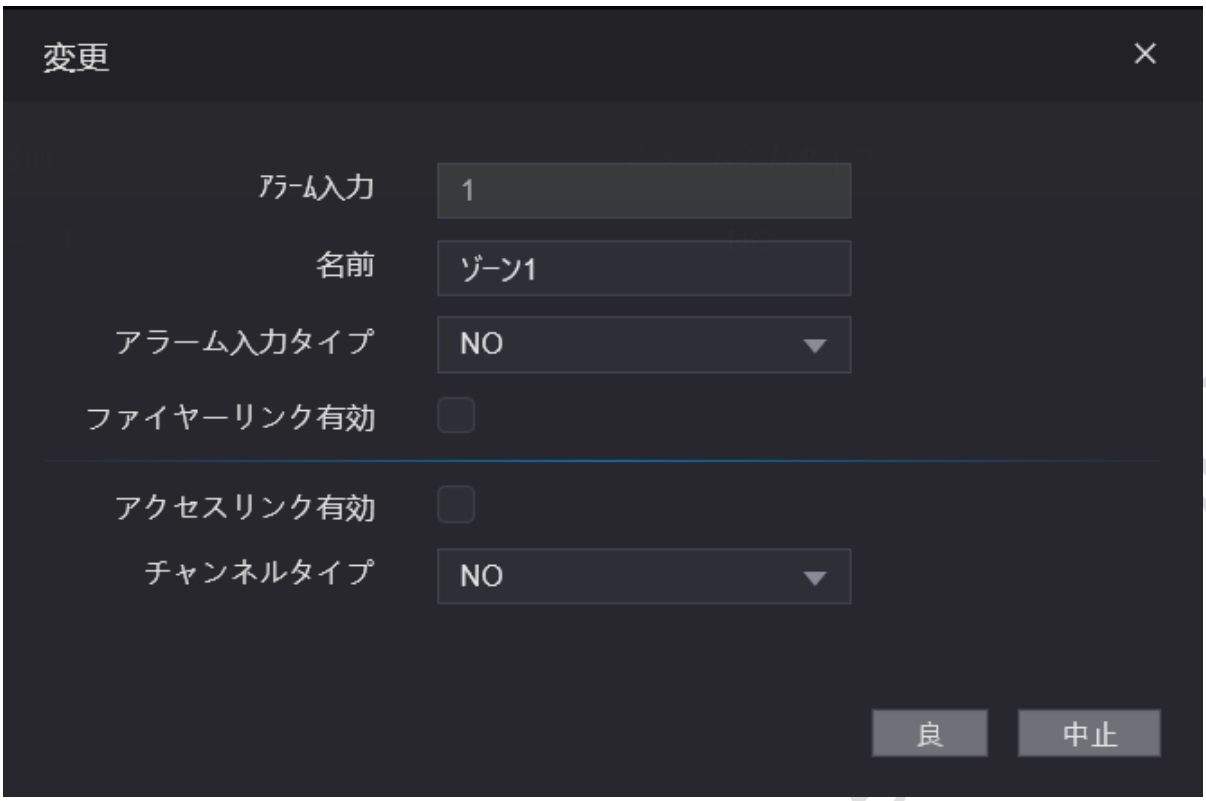


表4-1アラームリンクパラメータの説明

パラメータ	説明
アラーム入力	値は変更できません。デフォルトのままにします。
名前	ゾーン名を入力します。
アラーム入力タイプ	NOとNCの2つのオプションがあります。 購入したアラームデバイスのアラーム入力タイプが「NO」の場合は「NO」を選択し、それ以外の場合は「NC」を選択します。
ファイヤーリンク有効	火災リンクが有効になっている場合、火災アラームがトリガーされると、アクセスコントローラはアラームを出力します。アラームの詳細がアラームログに表示されます。 火災リンクが有効な場合、アラーム出力とアクセスリンクはデフォルトでNOです。
アクセスリンク有効	アクセスリンクを有効にすると、入力アラーム信号がある場合、アクセスコントローラは正常にオンになるか、正常に閉じられます。
チャンネルタイプ	NOとNCの2つのオプションがあります。

ステップ4OKをクリックし、設定が完了します。

アクセスコントローラがクライアントに追加されている場合、Web上の設定はクライアント内の設定と同期されます。

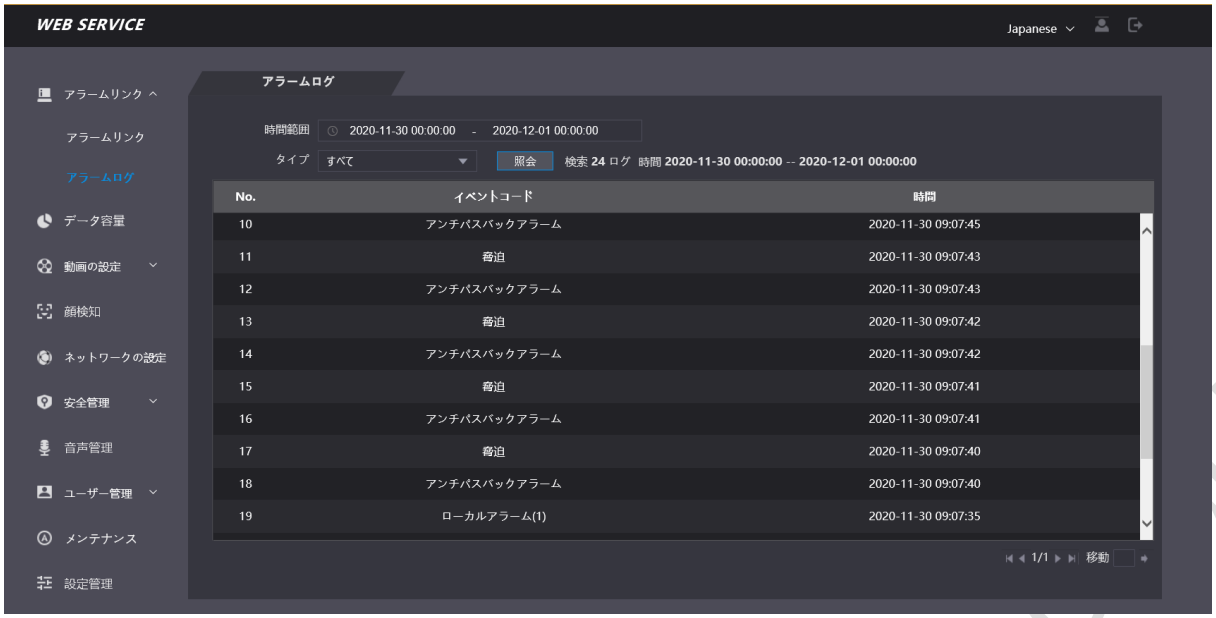
4.4.2 アラームログ

アラームの種類と時間範囲は、アラームログインターフェイスで確認できます。

ステップ1　Webインターフェースにログインします。

ステップ2　アラームリンク>アラームログを選択します。

図4-9アラームログ



ステップ3　時間範囲とアラームタイプを選択し、照会をクリックします。照会結果が表示されます。

4.5 データ容量

アクセスコントローラが保持できるユーザ、カード、指紋、顔画像の数は、データ容量インターフェイスで確認できます。

ステップ1　Webインターフェースにログインします。

ステップ2　ナビゲーションバーでデータ容量を選択します。

データ容量インタフェースが表示されます。

4.6 ビデオ設定

ビデオ設定インターフェイスでは、データレート、画像パラメータ(明るさ、コントラスト、色相、彩度など)、露出などのパラメータを設定できます。

4.6.1 データレート

チャネル1のストリームパラメータを設定できます。

ステップ1　Webインターフェースにログインします。

ステップ2　動画設定>動画の設定>レートを選択します。

図4-11レート

表4-2ストリーム・パラメータの説明

パラメータ		説明
ビデオ規格		NTSCとPALの2つのオプションがあります。 お住まいの地域のビデオ規格に合わせて規格を選択してください。
チャンネルID		1と2.1は白色ライトカメラ、2はIRライトカメラの2つの選択肢があります。
一次レート	動画リスト	D1、VGA、720p、1080pの4つのオプションがあります。欲しい映像品質に応じてオプションを選んでください。
	フレームレート	連続したフレームがディスプレイに表示されるレート。 フレームレートの範囲は1～30fpsです。
	ビットレート	時間単位ごとに伝達または処理されるビット数。 2Mbps、4Mbps、6Mbps、8Mbps、10Mbpsの5つのオプションがあります。
追加フォーマット	動画リスト	DV1、VGA、QVGAの3つのオプションがあります。
	フレームレート	連続したフレームがディスプレイに表示されるレート。 フレームレートの範囲は1～30fpsです。
	ビットレート	時間単位ごとに伝達または処理されるビット数。オプションは512Kbps、640Kbps、768Kbps、896Kbps、1024Kbps、1.25Mbps、1.5Mbps、1.75Mbps、2Mbpsです。

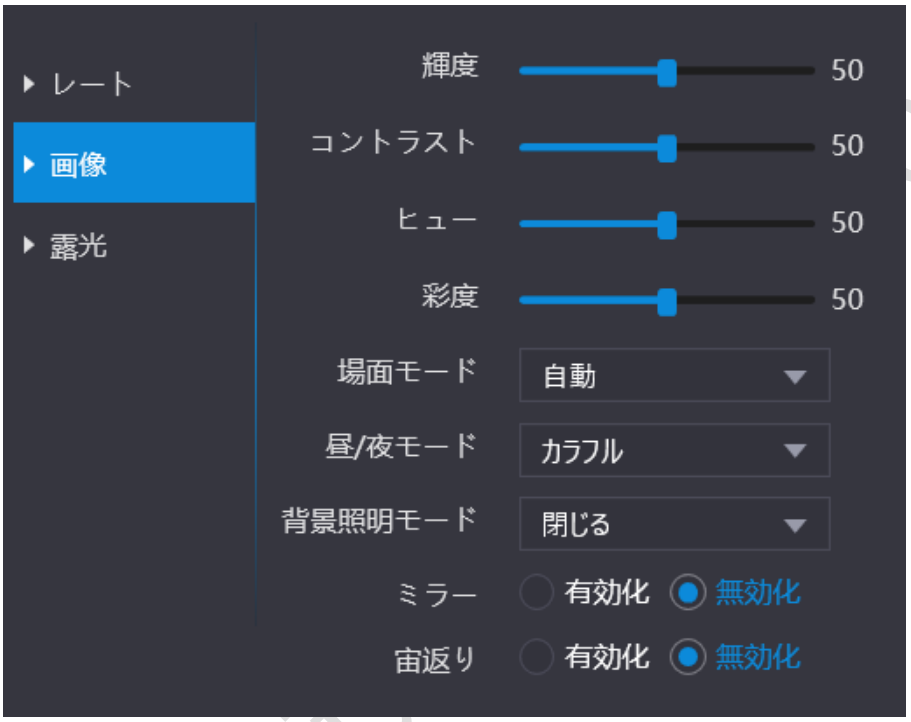
4.6.2 画像

チャンネルは2つあり、チャンネルごとにパラメーターを設定する必要があります。

ステップ1　Webインターフェースにログインします。

ステップ2　動画の設定>動画の設定>画像を選択します。

図4-12画像



ステップ3　背景照明モードでワイドダイナミックを選択します。

表4-3画像パラメータの説明

パラメータ	説明
輝度	値が大きいほど、画像は明るくなります。
コントラスト	コントラストとは、オブジェクトを識別可能にする輝度または色の差です。コントラストの値が大きいほど、明るさと色のコントラストが大きくなります。
色相	値が大きいほど、色は深くなります。
彩度	値が大きいほど、色が明るくなります。 値は画像の明るさを変えません。
場面モード	● 閉じる:モードなし。 ● 自動:システムはシーンモードを自動的に調整します。 ● 晴天:このモードでは、画像の色合いが低下します。 ● 夜間:このモードでは、画像の色合いが大きくなります。 **Sunnyはデフォルトで選択されています。**
昼/夜モード	昼/夜モードは、フィルライトの作動状況を決定します。 ● 自動:システムは自動的に日中/夜間モードを調整します。 ● カラフル:このモードでは、画像は色付きです。 ● 白黒:このモードでは、画像は白黒で表示されます。
背景照明モード	● 閉じる:バックライト補正なし。 ● 逆光:極端に高いまたは低いレベルの光で領域を補正し、焦点が合っている対象物に対して正常で使用可能なレベルの光を維持します。 ● ワイドダイナミック:システムは明るい領域を暗くし、暗い領域を補正して、明るい領域と暗い領域のオブジェクトの定義を保証します。 人間の顔がバックライトにあるときは、WDRを有効にする必要があります。 ● 抑制:ハイライト補正は、スポットライト、ヘッドライト、ポーチライトなどのハイライトまたは強い光源の露出過多を補正して、使用可能で明るい光に追い越されないイメージを作成するために必要です。
ミラー	機能を有効にすると、左右を反転して画像が表示されます。
反転	この機能を有効にすると、画像を裏返すことができます。

4.6.3 露光

露光パラメータを設定できます。

ステップ1　Webインターフェースにログインします。

ステップ2　ビデオ設定>ビデオ設定>露光を選択します。

図4-13露出

表4-4露光パラメータの説明

パラメータ	説明
明滅防止	● 50Hz:交流の商用周波数が50Hzの場合、画像に縞模様がないことを確認するために露光が自動的に調整されます。 ● 60Hz:交流の商用周波数が60Hzの場合、画像に縞模様がないことを確認するために露光が自動的に調整されます。 ● 屋外:屋外を選択すると、露出モードを切り替えることができます。
露出モード	🕮 ● 「アンチフリッカー」ドロップダウンリストで「屋外」を選択すると、露出モードとして「シャッター優先」を選択できます。 ● 異なる装置の露出モードは異なる可能性があり、実際の製品が優先されるものとします。 選択可能: ● 自動:アクセスコントローラが自動的に画像の明るさを調整します。 ● シャッター優先順位:アクセスコントローラーは、シャッター露光値の範囲に応じて画像の明るさを調整します。画像の明るさが十分でなく、シャッター値が上限または下限に達している場合、アクセスコントローラはゲイン値を自動的に調整して理想的な明るさを得ます。 ● 手動:ゲインとシャッター値を手動で設定して、画像の明るさを調整できます。
シャッター	シャッター値が大きく、露出時間が短いほど暗くなります。「シャッター優先順位」を選択すると、カスタマイズできます。
シャッター (値範囲)	「シャッター優先順位」を選択すると、シャッター値の範囲をカスタマイズできます。
ゲイン値の範囲	ゲイン値の範囲を設定すると、映像品質が向上します。「手動(露光モード)」を選択すると、値の範囲をカスタマイズできます。
露出補正	露光補正値を調整すると、ビデオの明るさを上げることができます。
3D NR	3Dノイズリダクション(RD)を有効にすると、ビデオノイズを低減でき、高精細度ビデオが生成されます。
グレード	3D NRが有効な場合、3D NRの値を調整できます。 値が大きいほどノイズが少なくなります。

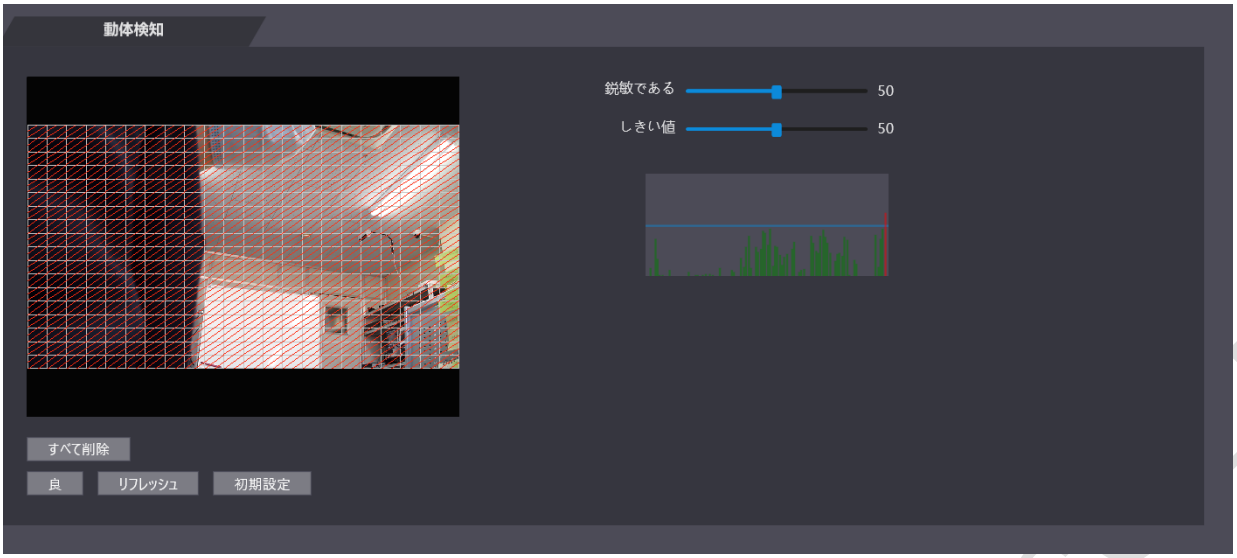
4.6.4 動体検出

動く物体を検知できる範囲を設定します。

ステップ1　Webインターフェースにログインします。

ステップ2　ビデオ設定>動体検出を選択します。動体検知インタフェースが表示されます。

図4-14モーション検出



ステップ3　左マウスボタンを押したまま、赤い領域でマウスをドラッグします。

ステップ4　**動体検知エリアが表示されます。**

- 赤い長方形は動体検出エリアです。デフォルトのモーション検出範囲は、すべての矩形です。
- 動体検出エリアを描画するには、まず「すべて削除」をクリックする必要があります。
- 描画する動体検出エリアは、デフォルトのモーション検出エリアで描画すると、非動体検出エリアになります。

- 感度は、各グリッドが動きを感知する能力を表します。値が大きいほど感度が高くなります。
- しきい値は、モーション検出の条件です。グリッド番号がしきい値に達すると、モーション検出がトリガーされます。値が小さいほど、モーション検出がトリガーされる可能性が高くなります。
- グリッド番号がしきい値より小さい場合は緑色の線が表示され、しきい値より大きい場合は赤色の線が表示されます。図4-14を参照してください。

ステップ5　「OK」をクリックして設定を終了します。

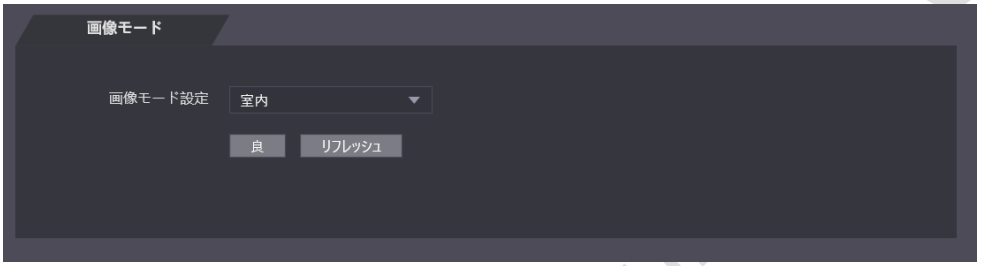
4.6.5 画像モード

屋内、屋外、その他の3つのオプションがあります。アクセスコントローラが屋内に設置されている場合は「屋内」を、アクセスコントローラが屋外に設置されている場合は「屋外」を選択し、コリドーやホールウェイなどのバックライトが設置されている場所にアクセスコントローラが設置されている場合は「その他」を選択します。

ステップ1　　Webインターフェースにログインします。

ステップ2　　ビデオ設定>画像モードを選択します。

図4-17イメージモード



4.7 顔検知

顔認識の精度を高めるために、このインターフェースで人の顔に関連するパラメータを設定できます。

ステップ1　Webインターフェースにログインします。

ステップ2　顔検知を選択します。

図4-18顔検知

ステップ3　パラメータを設定します。

表4-5顔検知パラメータの説明

パラメータ	説明
顔認識閾値	値が大きいほど、精度は高くなります。
顔認識の最大角度	角度が大きいほど、プロファイルの範囲が広く認識されます。
偽造防止閾値	人物の顔画像や顔モデルによるロック解除を防止します。 「有効化」と「閉じる」の2つのオプションがあります。
赤外線	スクロールバーをドラッグして、IRブライトネスを調整します。
認識タイムアウト	有効な顔認識中のプロンプトの間隔。
認識間隔	無効な顔認識中のプロンプトの間隔。
瞳孔間距離	瞳孔間距離とは、各目の視点の中心間にある画像のピクセル値のことです。アクセスコントローラが必要に応じて顔を認識できるように、適切な値を設定する必要があります。顔の大きさや、顔とレンズの距離によって値が変わります。顔がレンズに近づくほど、値は大きくなります。 成人がレンズから1.5メートル離れている場合、瞳孔間距離の値は50～70の範囲内になります。

チャネルID	1と2.1は白色ライトカメラ、2はIRライトカメラの2つの選択肢があります。
顔露光を有効にする	顔露出を有効にすると、アクセスコントローラを屋外に設置したときに人の顔が鮮明になります。
顔ターゲットの輝度	デフォルト値は50です。必要に応じて明るさを調整します。
顔露光間隔検出時間（秒）	顔が検出されると、アクセスコントローラは顔を照らすためのライトを発し、設定した間隔が経過するまでアクセスコントローラはライトを再び発しません。
露出(QRコード)	現在、この機能はサポートされていません。
目標を描く	最小限の顔検出フレームを描画できます。 「すべて削除」をクリックすると、描画したすべてのフレームを削除できます。
検知領域	マウスを動かして、顔検出リージョンを調整します。「すべて削除」をクリックすると、すべての検出領域を削除できます。

ステップ4　OKをクリックして設定を終了します。

4.8 ネットワーク設定

4.8.1 TCP/IP

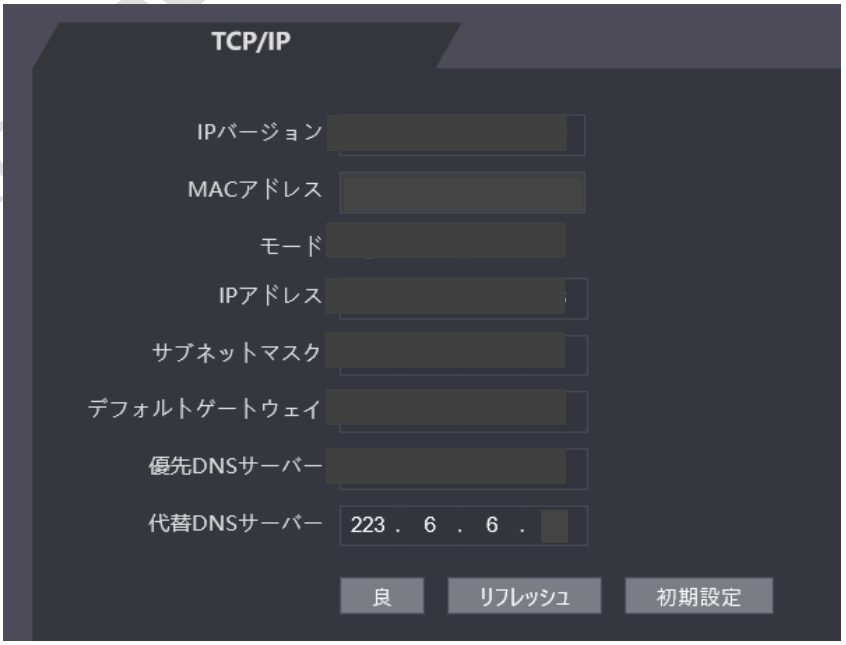
アクセスコントローラが他のデバイスと通信できるように、IPアドレスとDNSサーバを構成する必要があります。

アクセスコントローラがネットワークに正しく接続されていることを確認してください。

ステップ1　Webインターフェースにログインします。

ステップ2　ネットワーク設定>TCP/IPを選択します。

図4-19TCP/IP



ステップ3　パラメータを設定します。

表4-6TCP/IP

パラメータ	説明
IPバージョン	IPv4という1つのオプションがあります。
MACアドレス	アクセスコントローラのMACアドレスが表示されます。
モード	● 静的 IPアドレス、サブネットマスク、ゲートウェイアドレスを手動で設定します。 ● DHCP ■ DHCPを有効にすると、IPアドレス、サブネットマスク、およびゲートウェイアドレスを設定できなくなります。 ■ DHCPが有効な場合、IPアドレス、サブネットマスク、ゲートウェイアドレスが自動的に表示されます。DHCPが有効でない場合、IPアドレス、サブネットマスク、ゲートウェイアドレスはすべてゼロになります。 ■ DHCPが有効なときにデフォルトIPを表示する場合は、DHCPを無効にする必要があります。
リンクローカルアドレス	リンクローカルアドレスは、IPバージョンでIPv6が選択されている場合にのみ使用できます。 通信を可能にするために、各ローカルエリアネットワークのネットワークインタフェースコントローラに固有のリンクローカルアドレスが割り当てられます。リンクローカルアドレスは変更できません。
IPアドレス	IPアドレスを入力し、サブネットマスクとゲートウェイアドレスを設定します。 IPアドレスとゲートウェイアドレスは、同じネットワークセグメント内にある必要があります。
サブネットマスク	
デフォルトゲートウェイ	
優先DNSサーバー	優先DNSサーバのIPアドレスを設定します。
代替DNSサーバー	代替DNSサーバのIPアドレスを設定します。

ステップ4　OKをクリックして設定を完了します。

4.8.2 ポート

アクセスコントローラが接続できる最大接続クライアント数とポート番号を設定します。

ステップ1　Webインターフェースにログインします。

ステップ2　ネットワーク設定>ポートを選択します。ポートインタフェースが表示されます。

ステップ3　ポート番号を設定します。次の表を参照してください。

最大接続数を除き、値を変更した後に設定を有効にするには、アクセスコントローラを再起動する必要があります。

表4-7ポートの説明

パラメータ	説明
最大接続数	アクセスコントローラが接続できるクライアントの最大接続数を設定できます。 📖 SmartPSS ACなどのプラットフォームクライアントはカウントされません。
TCPポート	デフォルト値は37777です。
HTTPポート	デフォルト値は80です。 他の値がポート番号として使用される場合は、ブラウザ経由でログインするときに、この値をアドレスの後ろに追加する必要があります。
HTTPSポート	デフォルト値は443です。
RTSPポート	デフォルト値は554です。

ステップ4　OKをクリックして設定を完了します。

4.8.3 登録

外部ネットワークに接続すると、アクセスコントローラは、クライアントがアクセスコントローラにアクセスできるように、ユーザが指定したサーバにそのアドレスを報告します。

ステップ1　Webインターフェースにログインします。

ステップ2　ネットワーク設定>登録を選択します。登録インタフェースが表示されます。

ステップ3　有効化を選択し、ホストIP、ポート、およびサブデバイスIDを入力します。

表4-8自動レジスタの説明

パラメータ	説明
ホストIP	サーバのIPアドレスまたはサーバのドメイン名。
ポート	自動登録に使用されるサーバポート。
サブデバイスID	サーバによって割り当てられたアクセスコントローラID。

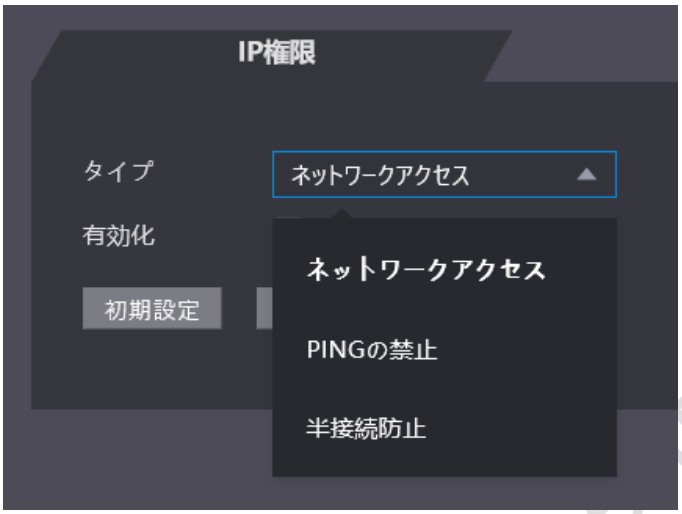
ステップ4　OKをクリックして設定を完了します。

4.9 安全管理

4.9.1 IP権限

必要に応じてサイバーセキュリティモードを選択します。

図4-21IP権限



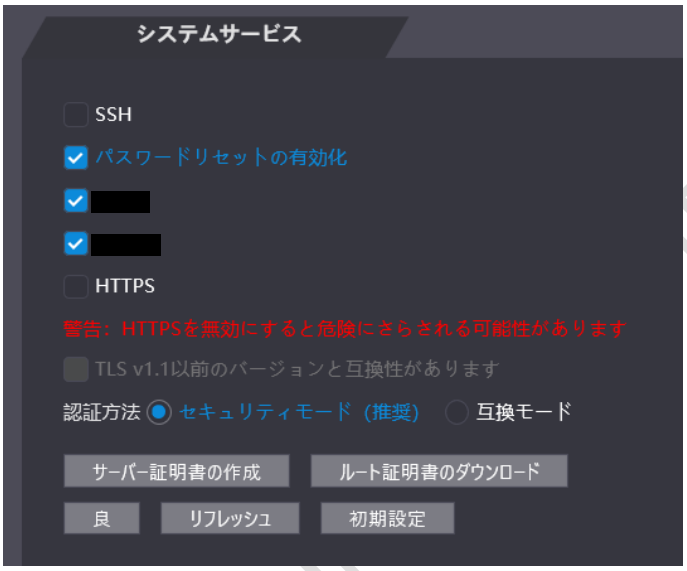
4.9.2 システム

4.9.2.1 システムサービス

SSH、パスワードリセットの有効化、CGI、ONVIF、HTTPSの5つのオプションがあります。1つ以上を選択するには、「3.13機能」を参照してください。

ウェブページで行うシステムサービス構成と、アクセスコントローラーのフィーチャーズインターフェースでの構成が同期されます。

図4-22システムサービス



サーバ証明書の作成

「サーバー証明書の作成」をクリックし、必要な情報を入力し、「保存」をクリックしてから、アクセスコントローラを再起動します。

4.9.2.2 ルート証明書のダウンロード

ステップ1　ルート証明書のダウンロードをクリックします。
ファイルの保存ダイアログボックスで証明書を保存するパスを選択します。

ステップ2　ダウンロードしたルート証明書をダブルクリックして、証明書をインストールします。画面の指示に従って証明書をインストールします。

4.10 ユーザ管理

ユーザーの追加と削除、ユーザーのパスワードの変更、パスワードを忘れたときにパスワードをリセットするための電子メールアドレスの入力を行うことができます。

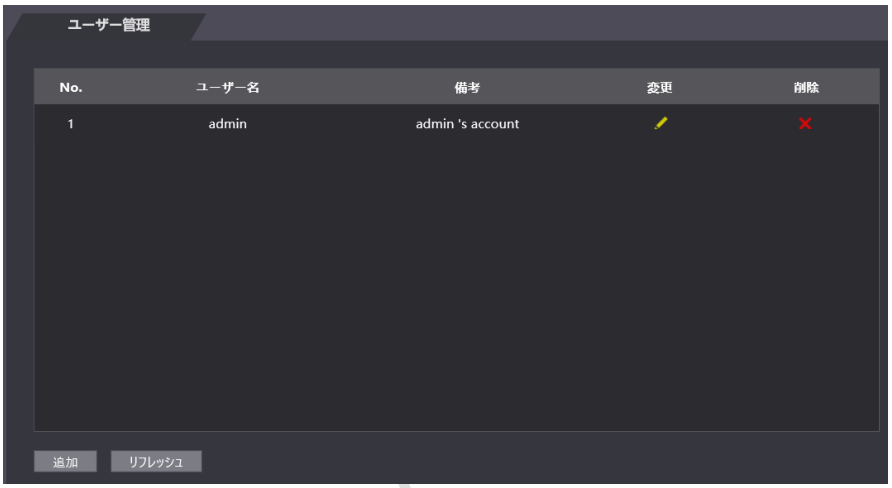
4.10.1 ユーザの追加

User MgmtでAddをクリックします。ユーザーを追加するためのインターフェース。ユーザー名、パスワード、確認済みパスワード、および注釈を入力します。「OK」をクリックして、ユーザーの追加を完了します。

4.10.2 ユーザー情報の変更

ユーザー管理の アイコンをクリックすると、ユーザー情報を変更することができます。

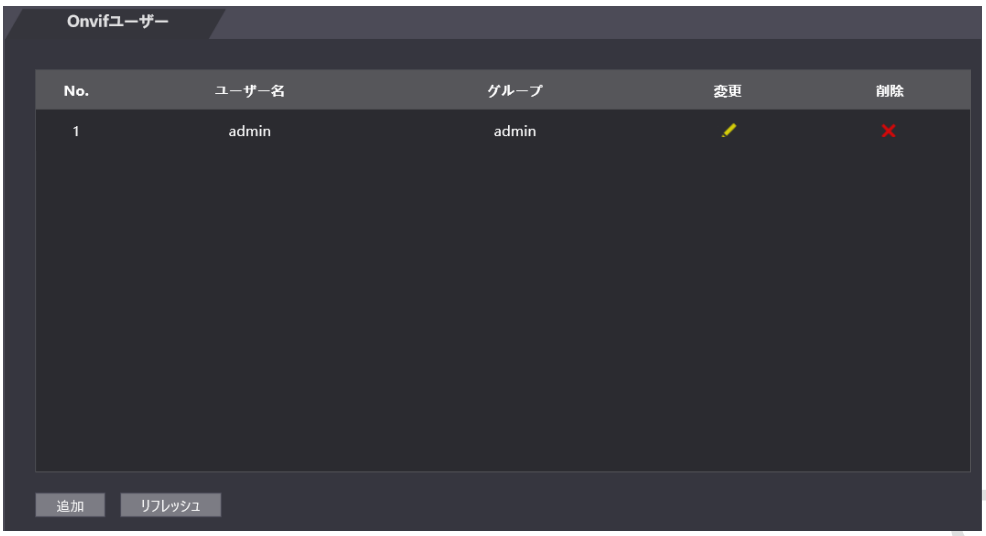
図4-23ユーザー管理



4.10.3 ONVIFユーザ

Open Network Video Interface Forum(ONVIF)は、物理的なIPベースのセキュリティ製品のインターフェースのためのグローバルオープンスタンダードの開発と使用を促進することを目的とした、グローバルでオープンな業界フォーラムです。ONVIFを使用する場合、管理者、オペレータ、ユーザはONVIFサーバの権限が異なります。必要に応じてONVIFユーザを作成します。

図4-24Onvifユーザー



4.11 メンテナンス

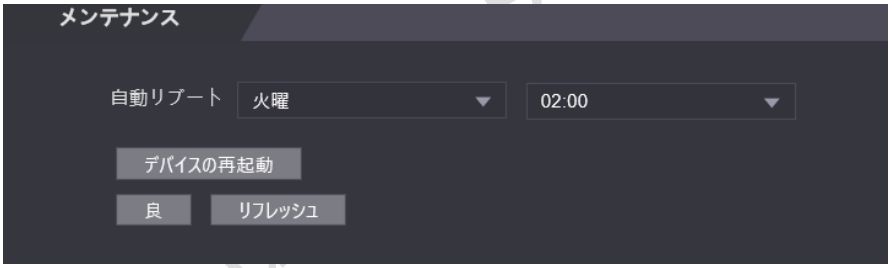
アクセスコントローラの実行速度を向上させるために、アイドル時間でアクセスコントローラをリブートさせることができます。自動リブートの日時を設定する必要があります。

ステップ1　Webインターフェースにログインします。

ステップ2　ナビゲーションバーで「メンテナンス」を選択します。

ステップ3　自動リブート(再起動)時間を設定し、「OK」をクリックします。

図4-25メンテナンス



たとえば、アクセスコントローラは毎週火曜日の午前2時に再起動します。

自動リブートをクリックすると、アクセスコントローラがただちに再起動します。

4.12 設定管理

複数のアクセスコントローラが同じ設定を必要とする場合は、設定ファイルをインポートまたはエクスポートしてパラメータを設定できます。

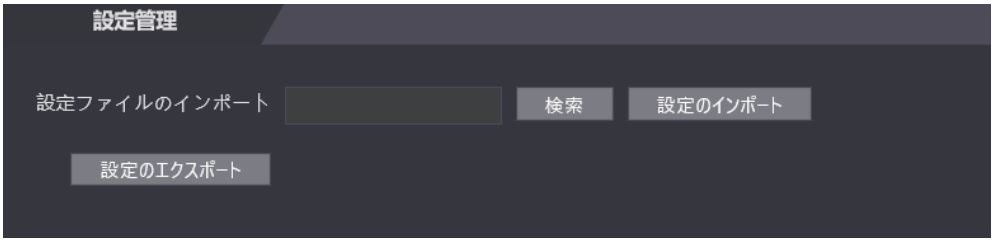
4.12.1 設定ファイルのエクスポート

バックアップ用にアクセスコントローラの設定ファイルをエクスポートできます。

ステップ1　Webインターフェースにログインします。

ステップ2　ナビゲーションバーで「設定管理」を選択します。

図4-26構成管理



ステップ3　設定ファイルをローカルに保存するには、「設定のエクスポート」をクリックします。

アクセスコントローラのIP情報はエクスポートされません。

4.12.2 設定ファイルのインポート

アクセスコントローラから同じモデルの別のアクセスコントローラにエクスポートされた設定ファイルをインポートできます。

ステップ1　Webインターフェースにログインします。

ステップ2　ナビゲーションバーで「設定管理」を選択します。

ステップ3　設定管理インタフェースで、「検索」をクリックしてインポートする設定ファイルを選択し、「設定のインポート」をクリックします。

設定ファイルをインポートすると、アクセスコントローラが再起動します。

4.13 更新

- アップグレード前にバックアップ用の設定ファイルをエクスポートし、アップグレードの完了後にインポートします。
- アップグレードファイルが取得されていることを確認してください。テクニカルサポートから入手できます。
- アップグレード中は、電源やネットワークを切断したり、デバイスを再起動またはシャットダウンしたりしないでください。

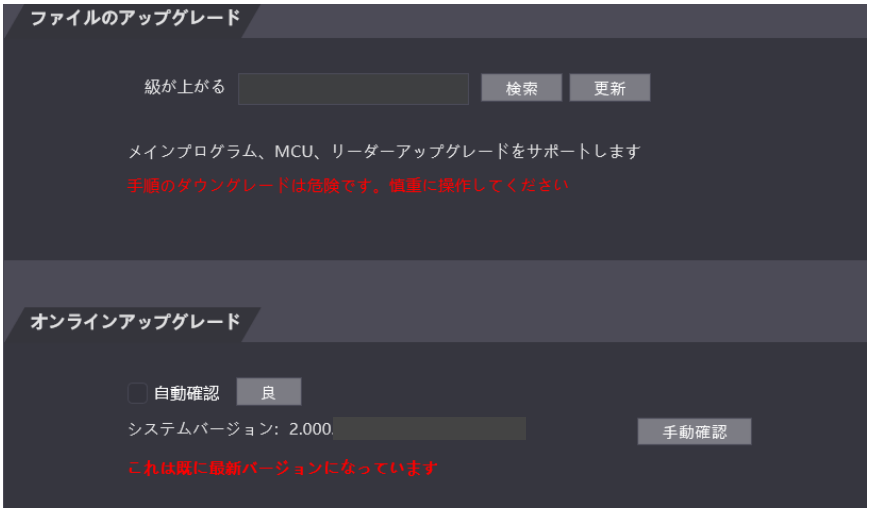
ステップ1　Webインターフェースにログインします。

ステップ2　ナビゲーションバーで「更新」を選択します。

ステップ3　更新インタフェースで、「参照」をクリックしてアップグレードファイルを選択し「更新」をクリックします。

アップグレード。

図4-27更新



アップグレードが成功すると、アップグレードが完了したことを示すメッセージがポップアップ表示されます。アップグレードに失敗すると、対応するプロンプトが表示されます。

- 自動チェックを選択すると、システムを自動的にアップグレードできます。手動チェックを選択すると、システムを手動でアップグレードすることもできます。
- アップグレード後、アクセスコントローラが再起動します。
- 左側のナビゲーションメニューの「バージョン情報」をクリックして、アップグレード後のバージョンを確認します。

4.14 バージョン情報

MAC住所、シリアル番号、MCU版、Web版、セキュリティベースライン版、システム版、ファームウェア版などの情報を閲覧できます。

ステップ1　Webインターフェースにログインします。

ステップ2　ナビゲーションバーの「バージョン情報」を選択します。バージョン情報インターフェースが表示されます。

4.15 オンラインユーザー

ユーザー名、IPアドレス、およびユーザーログイン時間は、オンラインユーザーインターフェイスで確認できます。

ステップ1　Webインターフェースにログインします。

ステップ2　ナビゲーションバーで「オンラインユーザ」を選択します。

図4-28オンラインユーザー

4.16 システムログ

システムログは、システムログインタフェースで照会およびバックアップできます。

4.16.1 ログ

システムログを照会できます。

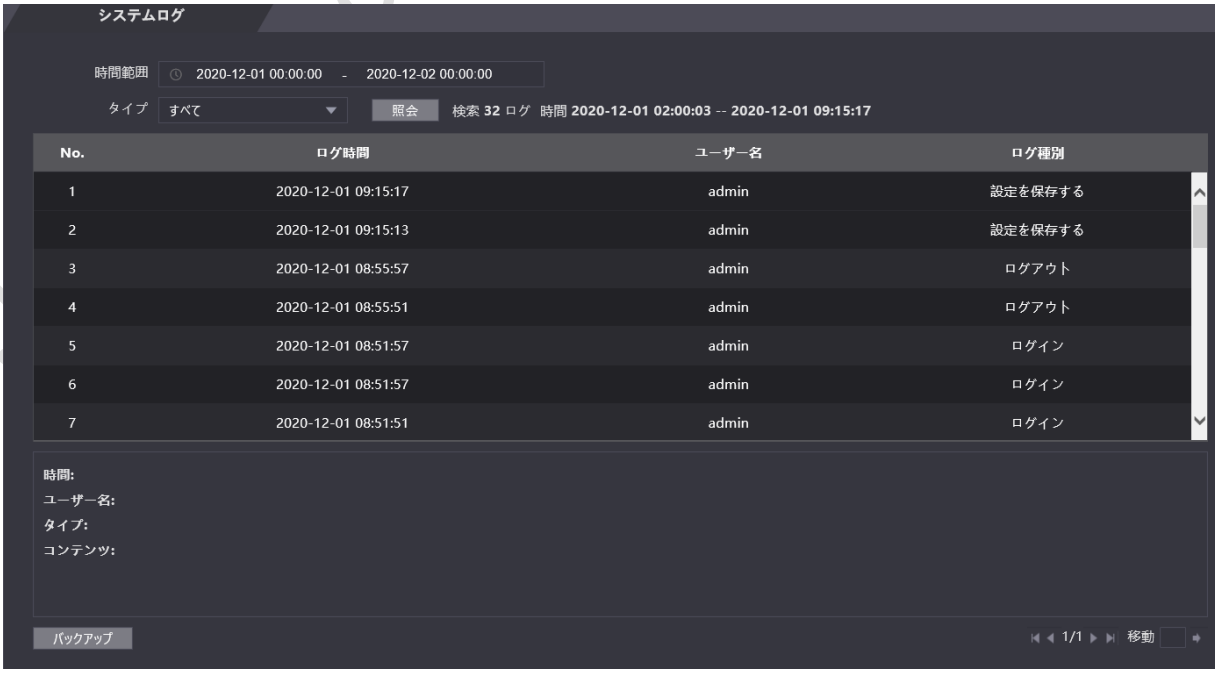
ステップ1 Webインターフェースにログインします。

ステップ2 ナビゲーションバーで「システムログ」を選択します。

ステップ3 時間範囲とそのタイプを選択して、「照会」をクリックします。

条件を満たすログが表示されます。

図4-29システムログ



4.16.2 バックアップログ

クエリされたログをバックアップできます。

ステップ 1　Webインターフェースにログインします。

ステップ 2　ナビゲーションバーで「システムログ」を選択します。

ステップ 3　時間範囲とそのタイプを選択して、「照会」をクリックします。

ステップ4　「バックアップ」をクリックして、表示されたログをバックアップします。

4.16.3 管理ログ

管理者 IDで管理ログを検索できます。

ステップ1　Webインターフェースにログインします。

ステップ2　「システムログ>管理ログ」を選択します。

ステップ3　管理ログインタフェースで、管理 IDを入力し、照会をクリックします。管理者の操作レコードが表示されます。

図4-30管理者ログ

4.17 終了

画面右上の  をクリック　OKをクリックし、Webインタフェースをログアウトします。

5 SmartPSS_AC 設定

アクセス・コントローラは、SmartPSS ACクライアントを介して管理できます。詳細な設定については、SmartPSS ACのユーザマニュアルを参照してください。

SmartPSS ACインターフェイスはバージョンによって異なる場合があり、実際のインターフェイスが優先されます。

5.1 ログイン

ステップ1　SmartPSS ACをインストールします。

ステップ2　ダブルクリックしてから、手順に従って初期化を終了し、ログインします。

5.2 デバイスの追加

SmartPSS ACにアクセス・コントローラを追加する必要があります。自動検索をクリックして追加し、追加をクリックしてデバイスを手動で追加できます。

5.2.1 自動検索

同じネットワーク・セグメントのアクセス・コントローラを検索し、SmartPSS ACに追加できます。

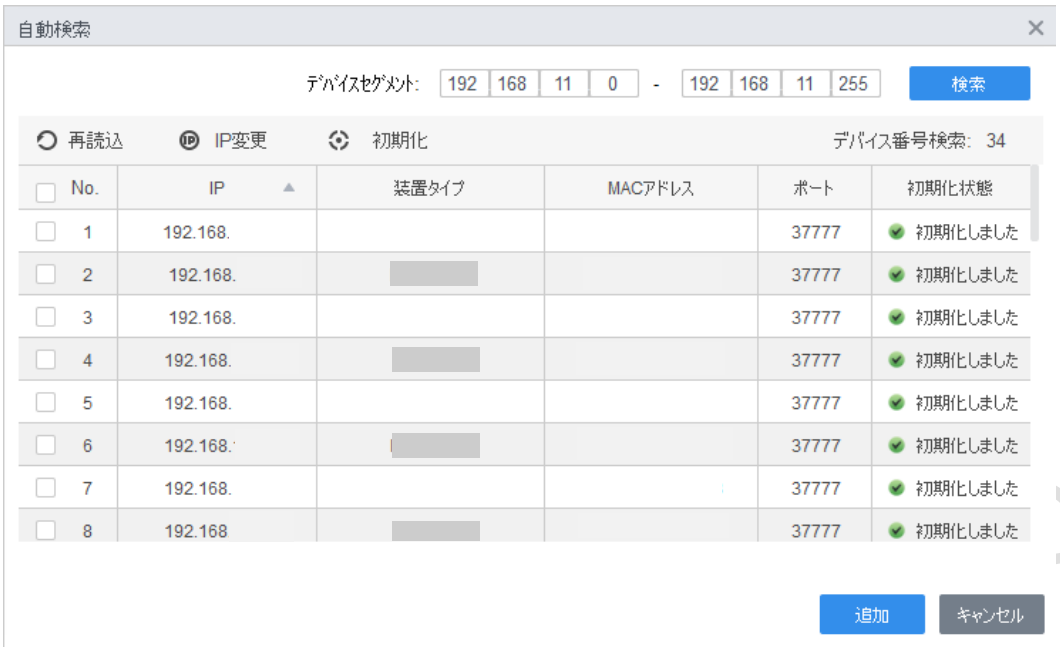
ステップ1　SmartPSS ACにログインします。

ステップ2　左下の「デバイス」をクリックすると、「デバイス」インターフェースが表示されます。

図5-1デバイス

ステップ3自動検索をクリックすると、自動検索インターフェースが表示されます。

図5-2自動検索



ステップ4　ネットワークセグメントを入力し、検索をクリックします。検索結果一覧が表示されます。

ステップ5　SmartPSS ACに追加するアクセスコントローラを選択し、「追加」をクリックします。ログイン情報ダイアログボックスが表示されます。

ステップ6　ログインするユーザー名とログインパスワードを入力します。

追加されたアクセスコントローラは、デバイスインターフェイスで確認できます。

アクセスコントローラを選択し、IPの変更をクリックして、アクセスコントローラのIPアドレスを変更できます。IPアドレスの変更については、SmartPSS ACのユーザーマニュアルを参照してください。

5.2.2 手動追加

アクセスコントローラは手動で追加できます。追加するアクセスコントローラのIPアドレスとドメイン名を知っておく必要があります。

ステップ1　SmartPSS ACにログインします。

ステップ2　左下の「デバイスマネージャ」をクリックすると、「デバイス」インターフェースが表示されます。

ステップ3　「デバイス」インターフェースで「追加」を選択すると、「手動追加」インターフェースが表示されます。

図5-3手動追加

ステップ4　デバイス名を入力し、追加する方法を選択し、IP、ポート番号(デフォルトでは37777)、ユーザー名、パスワードを入力します。

ステップ5　「追加」をクリックすると、追加したアクセスコントローラがデバイスインタフェースに表示されます。

5.3 ユーザ管理

5.3.1 カードタイプ設定

カードを発行する前に、カードの種類を設定してください。たとえば、発行されたカードがIDカードの場合、IDカードとしてタイプを選択します。

カードの種類は、カード発行者の種類と同じである必要があります。同じでないと、カード番号を読み取ることができません。

ステップ1　SmartPSS ACにログインします。

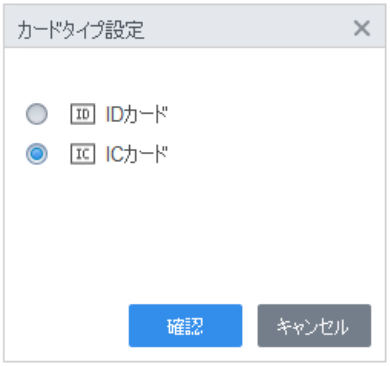
ステップ2　「従業員の管理者」をクリックすると、従業員の管理者インターフェースが表示されます。

図5-4従業員の管理者

ステップ3　従業員の管理者インタフェースで「ユーザー＞カードの発行タイプ」をクリックします。

ステップ4　「カードタイプの設定」インタフェースで、カードタイプを選択します。

図5-5カードタイプの設定



ステップ6　[確認]をクリックします。

5.3.2 ユーザーの追加

ユーザーを追加する方法のいずれかを選択します。

- 手動でユーザーを1つずつ追加します。
- バッチでユーザーを追加します。
- 他のデバイスからユーザー情報を抽出します。
- ローカルからユーザー情報をインポートします。

5.3.2.1 手動追加

手動でユーザーを1つずつ追加できます。

ステップ1　SmartPSS ACにログインします。

ステップ2　従業員の管理者>ユーザー >追加の順にクリックします。ユーザーの基本情報を追加します。

ステップ3　1)　「ユーザの追加」インターフェースの「基本情報」タブを選択し、ユーザの基本情報を追加します。

2)　画像をクリックし、「画像をアップロード」をクリックして顔画像を追加します。アップロードした顔画像がキャプチャフレームに表示されます。

画像の画素数が500×500以上、画像サイズが120Kバイト未満であることを確認してください。

図5-6基本情報の追加

ステップ4 「証明」タブをクリックして、ユーザの証明書情報を追加します。

- パスワードの設定。
  パスワードを設定します。第2世代アクセスコントローラの場合は、担当者パスワードを設定し、その他のデバイスの場合は、カードパスワードを設定します。新しいパスワードは6桁で構成する必要があります。
- カードの設定。

カード番号は、自動的に読み取ることも、手動で入力することもできます。自動的に読み取るには、カードリーダーを選択し、カードリーダーにカードを置きます。その後、カード番号が自動的に読み取られます。

1) をクリックして、カードリーダーとしてデバイスまたはカード発行者を選択します。
2) カードを追加します。第2世代以外のアクセスコントローラを使用する場合は、カード番号を付加する必要があります。
3) 増設後は、カードをメインカードまたは脅迫カードとして選択するか、新しいカードに交換するか、カードを削除することができます。

- 指紋情報を設定します。

1) をクリックして、指紋採集および機器を指紋スキャナーを選択します。
2) 指紋を追加します。指紋の追加をクリックし、スキャナーの指を3回連続して押します。

図5-7認証の設定

ステップ5　ユーザの権限を設定します。
詳細は「5.4許可設定」を参照してください。

図5-8許可設定

ステップ6完了をクリックします。

5.3.2.2 一括追加

ユーザーをバッチで追加できます。カードとユーザーIDの一括登録ができます。

ステップ1 SmartPSS ACにログインします。

ステップ2 従業員の管理者>ユーザー>バッチ追加をクリックします。

ステップ3 カードリーダーとユーザーの部門を選択します。カードの開始番号、カード数量、有効時間、有効期限を設定します。

ステップ4 発行をクリックしてカードの発行を開始します。

ステップ5 カード番号が自動的に読み込まれます。カード発行後に停止をクリックし、OKをクリックします。

図5-9バッチでのユーザーの追加

ステップ6　ユーザのリストで、✎をクリックして情報を変更するか、ユーザの詳細を追加します。

5.3.2.3 デバイスからのユーザーの抽出

デバイスからユーザー情報を抽出できます。

ステップ1　SmartPSS ACにログインします。

ステップ2　担当者マネージャ>ユーザー>引き出すをクリックします。

ステップ3　ターゲットデバイスを検索して選択し、「OK」をクリックします。

図5-10ユーザー情報を持つデバイス

ステップ4　必要に応じてユーザーを選択し、「OK」をクリックします。

ステップ5　ユーザーのリストで、をクリックして情報を変更するか、ユーザーの詳細を追加します。

5.3.2.4 ユーザーのインポート

ユーザーをローカルにインポートできます。

ステップ1　SmartPSS ACにログインします。

ステップ2　担当者マネージャ>ユーザー>インポートをクリックします。

ステップ3　指示に従ってユーザー情報をインポートします。

5.3.3 カードー括発行

カードが追加されていてもカードがないユーザーにカードを発行できます。

ステップ1　SmartPSS ACにログインします。

ステップ2　人事管理>ユーザーを選択します。

ステップ3　必要に応じてユーザーを選択し、「一括カード発行」をクリックします。

ステップ4　カードをバッチで発行します。カード番号は、カードリーダーで自動読み込みすることも、手動で入力することもできます。

- 自動読み取り

1) カード読み取り装置を選択し、発行をクリックします。
2) カードリストに従って、対応するユーザーのカードを順番にカードリーダーに配置すると、システムはカード番号を自動的に読み取ります。
3) カード検証の開始時刻や終了時刻などのユーザー情報を変更します。

- 手動で入力

1) カードー覧でユーザーを選択し、対応するカード番号を入力します。
2) カード検証の開始時刻や終了時刻などのユーザー情報を変更します。

図5-11カードのバッチ発行

ステップ5　OKをクリックします。

5.3.4 ユーザー情報のエクスポート

ユーザー情報をエクスポートできます。

ステップ1　SmartPSS ACにログインします。

ステップ2　人事管理>ユーザーを選択します。

ステップ3　エクスポートする必要があるユーザー情報を選択し、「エクスポート」をクリックしてすべてのユーザー情報をローカルにエクスポートします。

5.4 許可設定

5.4.1 許可グループの追加

ステップ1SmartPSS ACにログインします。

ステップ2従業員の管理者 >(左側一覧)許可設定をクリックします。

図5-12許可グループ一覧

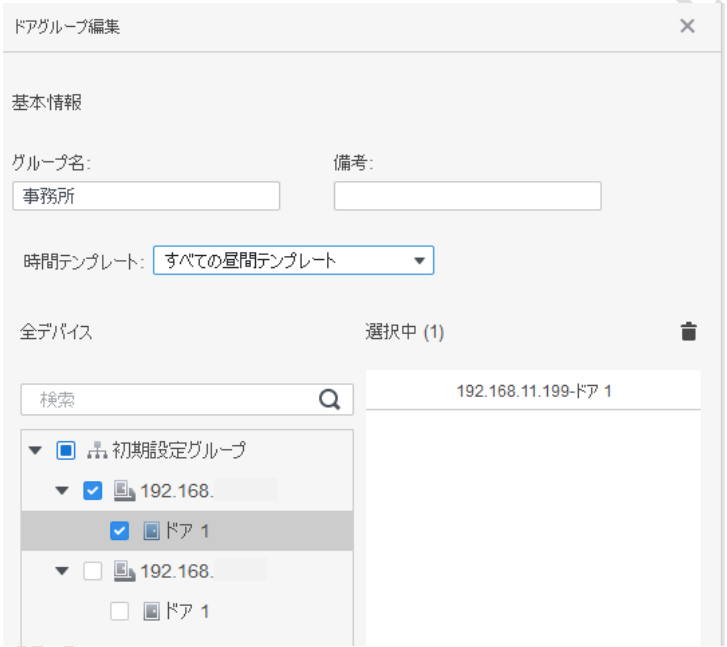
ステップ3 ➕をクリックして権限グループを追加します。権限パラメータを設定します。

ステップ4
1) グループ名と備考を入力します。
2) 必要な時間テンプレートを選択します。

時間テンプレート設定の詳細については、SmartPSS ACユーザマニュアルを参照してください。

3) ドア1など、対応するデバイスを選択します。

図5-13権限グループの追加



ステップ5 OKをクリックします。

許可グループリストインターフェースで、次の操作を実行できます:

- クリック　グループを削除します。
- クリック　グループ情報の変更
- 権限グループ名をダブルクリックして、グループ情報を表示します。

5.4.2 許可の設定

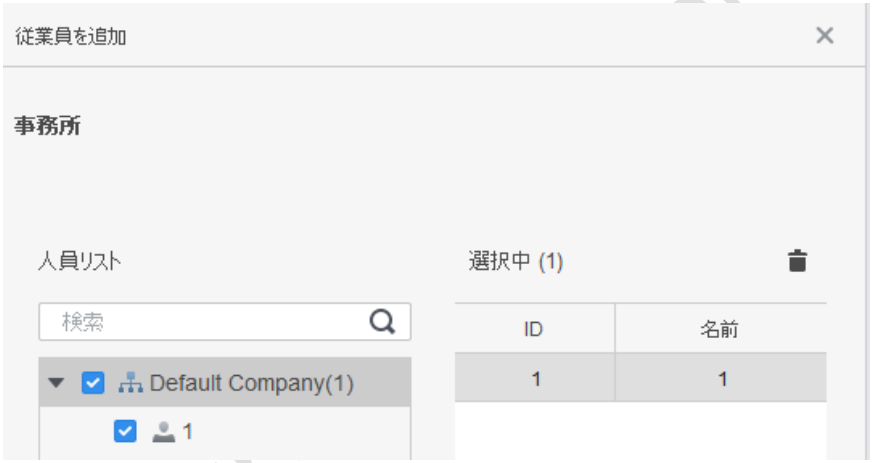
部門とユーザーの権限を設定する方法は似ています。ここでは、ユーザーを例に説明します。

ステップ1　SmartPSS ACにログインします。

ステップ2　従業員の管理者>(左側一覧)許可設定をクリックします。

ステップ3　任意の許可グループを選択し、をクリックします。

図5-14「設定」権限



ステップ4　権限を設定する必要があるユーザを選択します。

ステップ5　[OK]をクリックします。

5.5 アクセス管理

5.5.1 ドアをリモートで開く/閉じます

アクセス設定後、SmartPSS ACを介してドアをリモート制御できます。

ステップ1　ホームページのアクセスマネージャーをクリックします。(または、アクセスガイドをクリックします。).

ステップ2　ドアをリモート制御します。2つの方法があります。

- 方法1:ドアを選択し、右クリックして閉じるを選択します。

- または をクリックしてドアを開閉します。

図5-16リモート制御(方法2)

ステップ3　「イベント情報」リストでドアの状態を表示します。

- イベントフィルタリング:「イベント情報」でイベントタイプを選択すると、選択したタイプのイベントがイベントリストに表示されます。たとえば、「アラーム」を選択すると、イベントリストにアラームイベントのみが表示されます。
- イベント・リフレッシュ・ロック:ロックまたはロック解除するには、イベント情報の右側の をクリック

  イベントリスト、リアルタイムイベントは表示できません。
- イベントの削除:イベント情報の右側の をクリックすると、

  イベント内のすべてのイベントを消去します。

5.5.2 ノーマルオープンとノーマルクローズの設定

常時開または常時閉に設定すると、ドアは常時開または閉になり、手動で制御することはできません。ドアを再度手動で制御する場合は、「ノーマル」をクリックしてドアの状態をリセットします。

ステップ1　ホームページのアクセスマネージャーをクリックします。(または、アクセスガイドをクリックします。).

ステップ2　必要なドアを選択し、「ノーマルクローズ」または「ノーマルオープン」をクリックします。

図5-17常時開/常時閉の設定

5.5.3 ドアステータスのリセット

ノーマルオープンまたはノーマルクローズをクリックしたときにドアを手動で再制御する場合は、「ノーマル」をクリックしてドアのステータスをリセットします。

ステップ1　ホームページのアクセスマネージャーをクリックします。(または、アクセスガイドをクリックします。).

ステップ2　必要なドアを選択し、「ノーマル」をクリックします。画面の指示に従って操作してください。

図5-18ドアステータスのリセット

5.6 出勤管理

出席時間の設定、出席シフトの追加、人事スケジューリング、プロセス出席、出席統計の管理、レポートの検索、休日の追加、出席の設定を行うことができます。

5.6.1 レポート検索

ここでは、通常の出席、出席異常、残業出席、スタッフ情報を確認できます。また、統計はレポートとしてエクスポートできます。

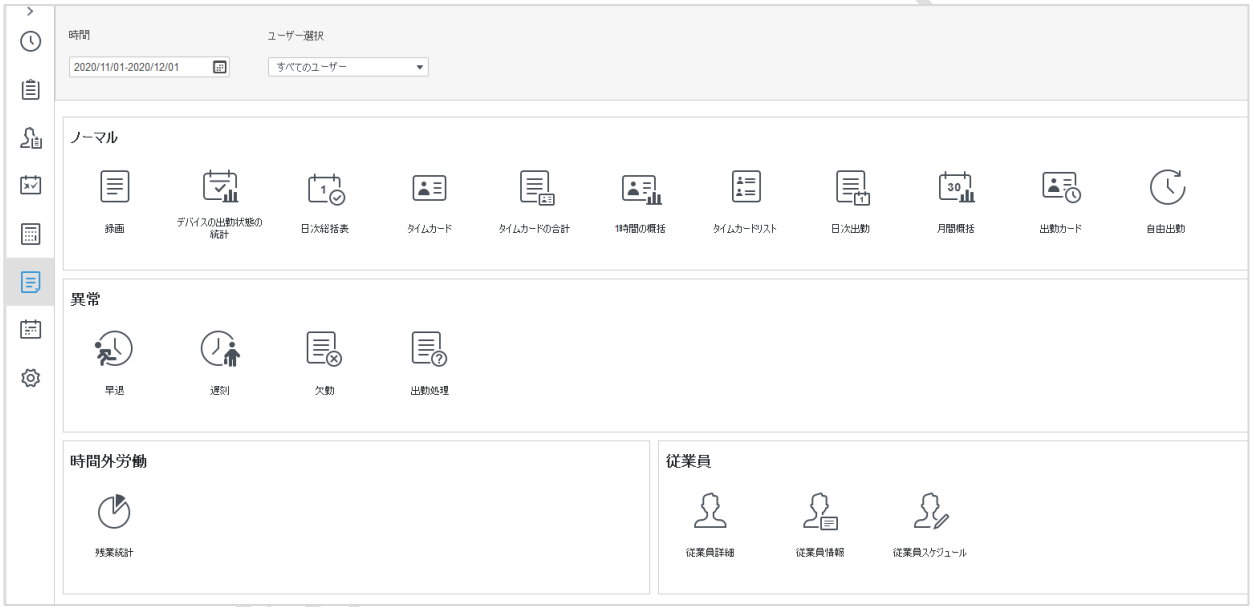
ステップ1　SmartPSS ACにログインします。

ステップ2　「出勤ソリューション＞出勤」をクリックすると、出勤インタフェースが表示されます。

ステップ3　左側のメニューバーで、をクリックします。

ステップ4　時間、部門、統計タイプを選択して、対応するレポートを表示します。

図5-19レポート検索



デバイスが追加され、SmartPSS ACプラットフォームで認証されると、対応する出席ステータスがプラットフォームに報告され、プラットフォームは対応する出席ステータスレポートを生成します。保存形式はPDF、SVC,XLSから選択できます。

図5-20デバイスの出席ステータスレポート

Default Company

1時間の概括報告

から 2020/11/01 ～へ 2020/12/01

部門		部門がありません							
社員番号	氏名	標準時間	残業時間	休み	欠勤	実質時間	遅刻	早退	休暇と出張
1	1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
合計時間		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

5.6.2 その他の構成

出勤期間、出勤シフト、人員スケジューリング、出勤処理と出勤統計、祝日と出勤構成の追加などのその他の構成については、SmartPSS ACのユーザーズマニュアルを参照してください。

ステップ　SmartPSS ACにログインします。

ステップ2　左側のメニューバーの をクリックすると、出勤ソリューションのホームページが表示されます。

ステップ3 右下隅にある「出勤ガイド」をクリックします。

ステップ4 「ユーザーマニュアル」をクリックします。

図5-21SmartPSS ACユーザーズマニュアルの表示

6 FAQ

1　電源を入れた後、アクセスコントローラの起動に失敗します。

12V電源は正しく接続されているかご確認ください。また、本体の端子接続部分は非常に抜けやすくなっておりますので、奥までしっかり差し込まれているかご確認ください。

2　アクセスコントローラの電源を入れても顔を認識できません。

ロック解除モードで「顔」が選択されていることを確認してください。「3.8.2ロック解除」を参照してください。「アクセス>アンロックモード(文字をタップ)>認識方法選択画面」で「顔」がロック解除モードとして選択されていることを確認してください。「3.8.2.3グループの組み合わせ」を参照してください。

3　アクセスコントローラと外部コントローラがWiegandポートに接続したところ、出力信号がありません。

アクセスコントローラのGNDケーブルと外部コントローラは接続されているか確認して下さい。

4　管理者のパスワードを忘れてしまいました。

管理者とパスワードを忘れた後は設定できません。プラットフォームを介して管理者を削除するか、テクニカルサポートに連絡してアクセスコントローラのロックをリモートで解除します。

5　ユーザー情報、顔画像をアクセスコントローラに取り込むことができません。

システムがファイルをタイトルで識別するため、XMLファイルの名前とテーブルのタイトルが変更されていないかどうかを確認してください。

6　ユーザーの顔が認識されていますが、他のユーザーの情報が表示されました。

人の顔を読み込むときは、周囲に他の人がいないことを確認してください。元の顔を削除し、マスクやメガネなどの装飾品をはずした写真を用意し、もう一度読み込んでください。

付録1顔の注意事項

記録/比較

登録前

- ガラス、帽子、およびマスクが顔認識性能に影響を及ぼす可能性があります。
- ハットを着用するときは、目を覆わないでください。
- デバイスを使用する場合は、顔のスタイルを大きく変更しないでください。そうしないと、顔の認識に失敗する可能性があります。
- 装置は、光源から2メートル以上離し、窓やドアから3メートル以上離してください。バックライトや直射日光が装置の顔認識性能に影響を与える可能性があります。

登録中

アクセスコントローラまたはプラットフォームを介して顔を登録できます。プラットフォーム経由の登録については、プラットフォームのユーザーマニュアルを参照してください。

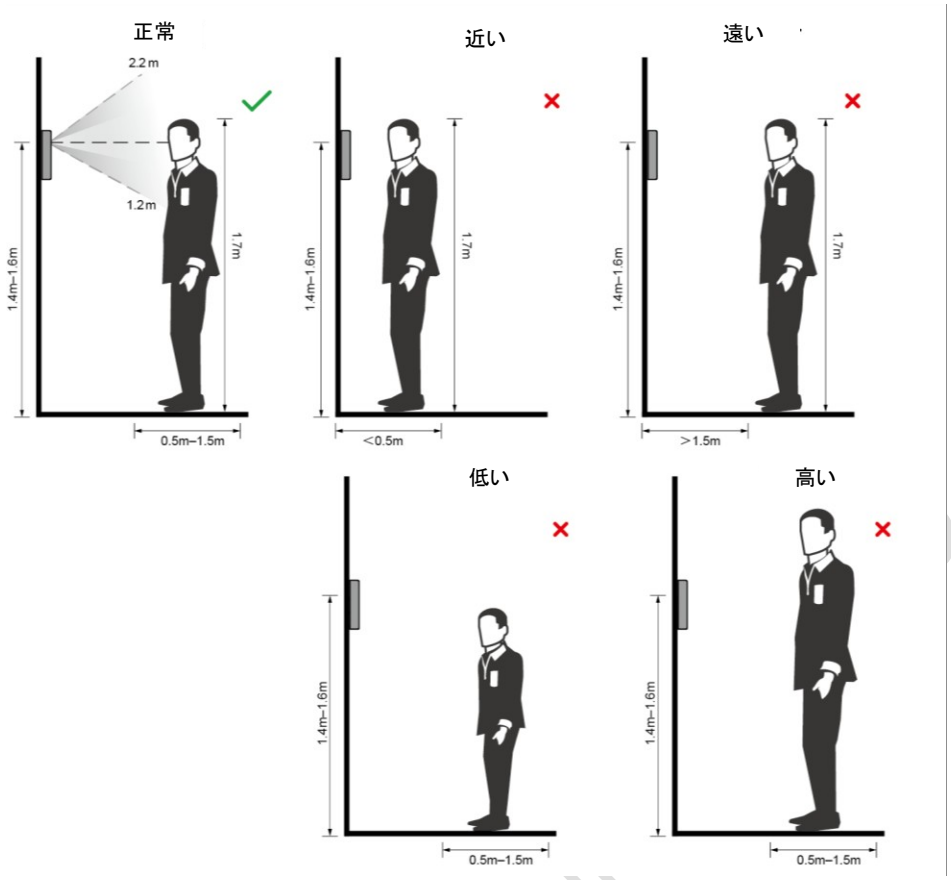
ヘッドをフォトキャプチャフレームの中央に配置します。顔の画像が自動的にキャプチャされます。

- 頭や体を振らないでください。登録に失敗することがあります。
- 2つの面が同時にキャプチャフレームに表示されないようにします。

顔の位置

顔が適切な位置にないと、顔認識効果に影響する場合があります。

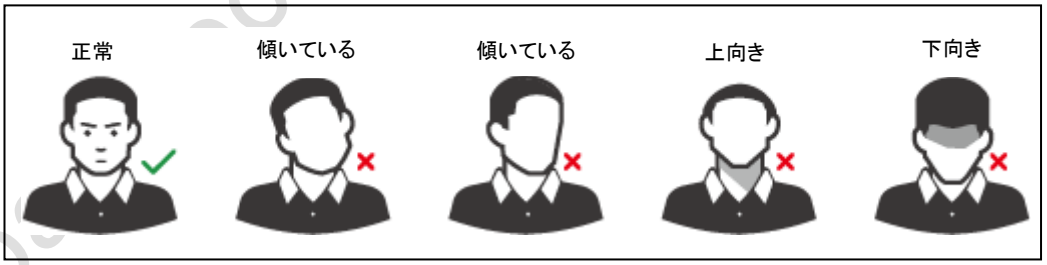
付図1-2適切な面位置



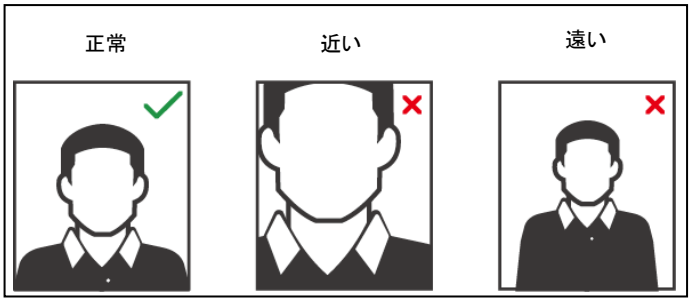
顔の要件

- 顔が隠れておらず、前頭部が髪で隠れていないこと。
- 顔画像の記録に影響するメガネ、帽子、マスクなどの顔装飾品は着用しないでください。
- 目が開いた状態で、顔の表情がない状態で、カメラの中央に顔を向けるようにしてください。
- 顔を記録するときや顔認識中は、顔をカメラに近づけすぎたり、カメラから離しすぎたりしないでください。

付図1-3ヘッド位置



付図1-4面間隔



- 管理プラットフォームから顔画像をインポートする場合は、画像解像度が150×300×600×1200、画像ピクセルが500×500、画像サイズが75KB未満、画像名と人物IDが同じであることを確認してください。
- 顔が画像領域全体の2/3を占めず、アスペクト比が1:2を超えないようにしてください。

付録2サイバーセキュリティに関する推奨事項

サイバーセキュリティは単なるバズワードではなく、インターネットに接続されているすべてのデバイスに関連するものです。IPビデオ監視はサイバーリスクに影響されませんが、ネットワークとネットワーク化されたアプライアンスを保護し、強化するための基本的なステップを踏むことで、攻撃の影響を受けにくくなります。以下に、セキュリティシステムをより安全に作成する方法に関するヒントと推奨事項をいくつか示します。

基本的な機器ネットワークセキュリティのために取るべき必須の措置:

1. **強力なパスワードの使用**

   パスワードを設定するには、次の提案を参照してください

   - 長さは8文字未満にすることはできません。
   - 文字の種類には、大文字と小文字、数字、記号を含め、少なくとも2種類の文字を含めます。
   - アカウント名またはアカウント名を逆の順序で含めないでください。
   - 123、abcなどの連続した文字は使用しないでください。
   - 111、aaaなど、重複する文字は使用しないでください。

2. **ファームウェアとクライアントソフトウェアを時間単位で更新します**

   - テクニカル業界の標準手順に従って、お使いの機器(NVR、DVR、IPカメラなど)のファームウェアを最新の状態に保ち、システムに最新のセキュリティパッチと修正が確実に適用されるようにすることをお勧めします。機器がパブリックネットワークに接続されている場合は、「アップデートの自動チェック」機能を有効にして、製造元がリリースしたファームウェアアップデートのタイムリーな情報を取得することをお勧めします。
   - 最新バージョンのクライアントソフトウェアをダウンロードして使用することをお勧めします。

機器のネットワークセキュリティを向上させるには、「Nice to have」の推奨事項が必要です:

1. **物理的保護**

   装置、特にストレージデバイスに対して物理的な保護を実行することをお勧めします。例えば、装置を特別なコンピュータルームやキャビネットに設置し、十分に完了したアクセス制御許可や鍵管理を実施して、ハードウェアの破損、リムーバブル装置(USBフラッシュディスク、シリアルポートなど)の不正な接続などの物理的な接触を許可されていない人員が行うことを防止します。

2. **パスワードを定期的に変更します**

   パスワードを定期的に変更して、推測または解読されるリスクを減らすことをお勧めします。

3. **パスワードの設定と更新による情報のタイムリーなリセット**

   本器はパスワードリセット機能に対応しています。エンドユーザーのメールボックスやパスワード保護の質問など、パスワードリセットの関連情報を時間単位で設定してください。情報が変更された場合は、時間内に変更してください。パスワード保護に関する質問を設定する場合は、簡単に推測できるものを使用しないことをお勧めします。

4. **アカウントロックを有効にします**

   アカウントロック機能はデフォルトで有効になっており、アカウントセキュリティを保証するためにオンにしておくことをお勧めします。攻撃者が間違ったパスワードで何度かログインしようとすると、対応するアカウントと送信元IPアドレスがロックされます。

5. **デフォルトのHTTPおよびその他のサービスポートの変更**

   デフォルトのHTTPおよびその他のサービスポートを1024～65535の任意の数字のセットに変更することをお勧めします。これにより、外部者が使用しているポートを推測できるリスクが軽減されます。

6. **HTTPSの有効化**

   安全な通信チャネルを介してWebサービスにアクセスできるように、HTTPSを有効にすることをお勧めします。

7. **ホワイトリストの有効化**

   ホワイトリスト機能を有効にして、指定したIPアドレスを除くすべてのユーザーがシステムにアクセスできないようにすることをお勧めします。そのため、必ずコンピュータのIPアドレスと付随する機器のIPアドレスをホワイトリストに追加してください。

8. **MACアドレスバインディング**

   ゲートウェイのIPおよびMACアドレスを機器につなぎ、ARPスプーフィングのリスクを軽減することをお勧めします。

9. **適切なアカウントと権限の割り当て**

   ビジネスおよび管理の要件に従って、合理的にユーザーを追加し、それらに最小限の権限セットを割り当てます。

10. **不要なサービスの無効化と安全モードの選択**

    不要な場合は、SNMP、SMTP、UPnPなどの一部のサービスをオフにしてリスクを軽減することをお勧めします。

    必要に応じて、次のサービスを含むセーフモードを使用することを強くお勧めします(ただし、これらに限定されません):

    - SNMP:SNMP v3を選択し、強力な暗号化パスワードと認証パスワードを設定します。
    - SMTP:メールボックスサーバにアクセスするには、TLSを選択します。
    - FTP:SFTPを選択し、強力なパスワードを設定します。
    - APホットスポット:WPA2-PSK暗号化モードを選択し、強力なパスワードを設定します。

11. **音声・映像暗号化伝送**

    オーディオとビデオのデータコンテンツが非常に重要または機密である場合は、伝送中にオーディオとビデオのデータが盗まれるリスクを減らすために、暗号化された伝送機能を使用することをお勧めします。

    注意:暗号化された送信は、送信効率に多少の損失をもたらします。

12. **セキュア監査**

    - オンラインユーザーをチェックする:デバイスが認証なしでログインしているかどうかを確認するために、オンラインユーザーを定y期的にチェックすることをお勧めします。
    - 機器ログを確認する:ログを表示することで、デバイスへのログインに使用されたIPアドレスとそのキー操作を知ることができます。

13. **ネットワークログ**

    装置の記憶容量が限られているため、保存されるログには制限があります。ログを長時間保存する必要がある場合は、ネットワークログ機能を有効にして、重要なログがトレースのためにネットワークログサーバに確実に同期されるようにすることをお勧めします。

14. **安全なネットワーク環境の構築**

    機器の安全性を確保し、潜在的なサイバーリスクを軽減するために、以下をお勧めします:

    - ルータのポートマッピング機能を無効にして、外部ネットワークからイントラネットデバイスに直接アクセスしないようにします。
    - ネットワークは、実際のネットワークのニーズに応じて分割し、隔離する必要があります。

2つのサブネットワーク間に通信要件がない場合は、ネットワーク分離効果を実現するために、VLAN、ネットワークGAP、およびその他のテクノロジを使用してネットワークを分割することをお勧めします。

- プライベートネットワークへの不正アクセスのリスクを軽減するため、802.1xのアクセス認証システムを確立します。
- デバイスのファイアウォールまたはブラックリストおよびホワイトリスト機能を有効にして、デバイスが攻撃されるリスクを軽減することをお勧めします。