

顔認証アクセスコントローラー

WEST E40

ユーザーズマニュアル



前書き

一般

本書は、顔認証式アクセスコントローラー（以下、アクセスコントローラー）の詳しい操作方法を紹介しています。



本マニュアルでは、モデルJのアクセスコントロール装置の図を例にして説明しています。

安全上の注意

マニュアルには、以下のように意味が定義されたシグナルワードが登場することがあります。

シグナルワード	意味
 危険	この表示を無視して、誤った取扱いをすると、人が死亡または重症を負う可能性が想定される内容を示しています。
 警告	避けなければ、軽度または中程度の傷害を負う可能性がある、中程度または低い潜在的危険性を示します。
 注意	避けられない場合、物的損害、データ損失、性能低下、または予期しない結果を引き起こす可能性がある潜在的なリスクを示します。
 ヒント	問題解決や時間短縮のための方法を提供します。
 注釈	テキストの強調・補足として追加情報を提供します。

改定履歴

バージョン	修正内容	発売日
V1.0.0	初版	2021年8月

マニュアルについて

- マニュアルに従わない操作によって生じた損害については、当社は一切責任を負いません。
- このマニュアルは、関連する地域の最新の法律や規制に基づいて更新されます。詳細な情報は、紙のマニュアル、CD-ROM、QRコード、または当社の公式ウェブサイトをご覧ください。紙のマニュアルと電子版の間に相違がある場合は、電子版が優先されます。
- すべての製品仕様とソフトウェアは、事前の書面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り、実際の製品と取扱説明書が異なる場合があります。最新のプログラムや補足説明書については、カスタマーサービスまでお問い合わせください。
- 本マニュアルと実際の製品との間に相違がある場合は、実際の製品が優先されます。
- 技術データや機能・操作説明に相違がある場合や、印刷に誤りがある場合があります。疑問がある場合は、最新版のマニュアルを参照してください。
- マニュアル(PDF)が開けない場合は、リーダーソフトをアップグレードするか、他のリーダーソフトをお試しください。
- 本マニュアルに記載されているすべての商標、登録商標および会社名は、それぞれの所有者に帰属します。
- ご使用中に何か問題が発生した場合は、当社のウェブサイトをご覧ください。販売代理店または当社担当窓口にご連絡ください。

安全に関する重要な項目

この章では、アクセスコントローラの正しい取り扱い方、危険防止、および物的損害の防止に関する内容を説明しています。ご使用になる前にこの内容をよくお読みになり、ご使用の際にはこれを遵守し、大切に保管してください。

動作条件

- 日光の当たる場所や熱源の近くにアクセスコントローラーを置いたり、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湿気やほこり、すすなどから遠ざけてください。
- アクセスコントローラーが落下しないように、安定した場所に設置してください。
- アクセスコントローラーに液体をこぼしたり、かけたりしないでください。また、アクセスコントローラーに液体が流れ込まないように、アクセスコントローラーの上に液体がないようにしてください。
- アクセスコントローラーは風通しの良い場所に設置し、アクセスコントローラーの換気を妨げないようにしてください。
- アクセスコントローラーは、定格の電力入力および出力の範囲内で動作させてください。
- アクセスコントローラーを分解しないでください。
- アクセスコントローラーの輸送、使用、保管は、許容される湿度と温度の条件で行ってください。
- 高温になる屋外で使用する場合は、画面や金属製のバックシェル、指紋センサーなどのアクセスコントローラーの表面に直接触れないようにしてください。

電気安全

- 地域で推奨されている電源ケーブルを使用し、定格電力の仕様に準拠してください。
守らない場合は人身事故やアクセスコントローラーの破損の原因となります。
- 電源は必ず付属の電源アダプタを使用してください。
- 配線の際は接触不良を起こさないよう、正しい結線を行い、必ず絶縁をしてください。
圧着の場合は、正しい圧着端子と圧着工具の組み合わせにより施工してください。
- 器具のカプラーは断線防止のための器具です。カプラーを使用する際は、操作しやすい角度を保ってください。

目次

前書き.....	I
一般.....	I
安全上の注意.....	I
改定履歴.....	I
マニュアルについて.....	II
安全に関する重要な項目.....	III
動作条件.....	III
電気安全.....	III
1 概要.....	1
1.1 はじめに.....	1
1.2 特徴.....	1
1.3 アプリケーション.....	2
2 システム運用.....	3
2.1 基本的な設定方法.....	3
2.2 共通アイコン.....	3
2.3 初期化.....	4
2.4 スタンバイ・インターフェース.....	4
2.5 メインメニュー.....	6
2.6 ロック解除方法.....	7
2.6.1 カード.....	7
2.6.2 顔.....	7
2.6.3 指紋.....	7
2.6.4 ユーザーパスワード.....	8
2.6.5 スーパーパスワード.....	8
2.7 ユーザー管理.....	8
2.7.1 新規ユーザーの追加.....	8
2.7.2 ユーザー情報の閲覧.....	11
2.8 アクセス管理.....	11
2.8.1 期間管理.....	12
2.8.1.1 期間設定.....	12
2.8.1.2 ホリデーグループ.....	12
2.8.1.3 ホリデープラン.....	12
2.8.1.4 NO 期間.....	12
2.8.1.5 NC 期間.....	12

2.8.1.6	リモート検証期間.....	12
2.8.2	ロック解除.....	13
2.8.2.1	アンロックモード.....	13
2.8.2.2	温度監視モード.....	14
2.8.3	アラーム設定.....	14
2.8.4	ドアの状態.....	15
2.8.5	ロック保持時間.....	15
2.9	出勤.....	16
2.10	ネットワーク通信.....	18
2.10.1	IP コンフィギュレーション.....	18
2.10.2	アクティブレジスタ.....	19
2.10.3	Wi-Fi.....	19
2.10.4	シリアルポートの設定.....	20
2.10.5	ウィーガンド (Wiegand) 構成.....	20
2.11	システム.....	22
2.11.1	時間.....	22
2.11.2	顔パラメータ.....	23
2.11.3	画像モード.....	27
2.11.4	音量.....	27
2.11.5	言語.....	27
2.11.6	赤外線ライト設定.....	27
2.11.7	スクリーン設定.....	27
2.11.8	工場出荷時設定への復元.....	28
2.11.9	リブート (再起動)	28
2.12	USB.....	28
2.12.1	USB エクスポート.....	28
2.12.2	USB インポート.....	29
2.12.3	USB 更新 (アップデート)	30
2.13	特徴.....	31
2.13.1	プライバシー設定.....	32
2.13.2	結果フィードバック.....	34
2.14	録画.....	37
2.15	システム情報.....	37
3	ウェブ運用.....	38
3.1	初期化.....	38
3.2	ログイン.....	40
3.3	パスワードの再設定.....	41
3.4	ドアパラメータ.....	43
3.5	アラーム連動.....	45

3.5.1	アラーム連動の設定.....	45
3.5.2	アラームログ.....	47
3.6	トークバック設定.....	48
3.6.1	SIP サーバー.....	48
3.6.1.1	SIP サーバーとしてのアクセスコントローラー.....	48
3.6.1.2	SIP サーバーとしての他のデバイス.....	49
3.6.2	ローカル構成.....	50
3.6.2.1	SIP サーバーとしてのアクセスコントローラー.....	50
3.6.2.2	SIP サーバーとしての他のデバイス.....	51
3.6.3	VTO 番号管理.....	52
3.6.4	VTH 番号管理.....	54
3.6.4.1	VTH を一つずつ追加.....	54
3.6.4.2	VTH を一括して追加.....	55
3.6.5	VTS マネジメント.....	56
3.6.6	オンラインステータス.....	57
3.6.7	通話ログ.....	57
3.7	タイムセクション.....	58
3.7.1	時間を設定するセクション.....	58
3.7.2	ホリデーグループの設定.....	59
3.7.3	ホリデーグループの設定.....	60
3.8	データ容量.....	61
3.9	ビデオ設定.....	61
3.9.1	データレート.....	61
3.9.2	イメージ.....	62
3.9.3	露光.....	64
3.9.4	動体検知.....	65
3.9.5	ボリューム設定.....	66
3.9.6	イメージモード.....	67
3.9.7	ローカルコーディング.....	67
3.10	顔検出.....	68
3.11	ネットワーク設定.....	71
3.11.1	TCP/IP.....	71
3.11.2	ポート.....	73
3.11.3	登録.....	73
3.11.4	P2P.....	74
3.12	安全管理.....	75
3.12.1	IP 権限.....	75
3.12.2	システム.....	75
3.12.2.1	システムサービス.....	75

3.12.2.2	サーバー証明書の作成.....	77
3.12.2.3	ルート証明書のダウンロード.....	77
3.13	ユーザーの管理.....	77
3.13.1	ユーザーの追加.....	77
3.13.2	ユーザー情報の変更.....	77
3.13.3	ONVIF ユーザー.....	78
3.14	メンテナンス.....	78
3.15	設定管理.....	79
3.15.1	設定ファイルのエクスポート.....	79
3.15.2	設定ファイルの読み込み.....	79
3.15.3	初期設定.....	79
3.16	アップグレード.....	80
3.17	バージョン情報.....	81
3.18	オンラインユーザー.....	81
3.19	システムログ.....	81
3.19.1	システムログ.....	81
3.19.2	管理者ログ.....	82
3.19.3	アンロック記録.....	82
3.20	フュージョン・キャリブレーション.....	83
3.21	アドバンスド.....	84
3.22	ログアウト.....	84
4	SmartPSS AC の設定	85
4.1	ログイン.....	85
4.2	デバイスの追加.....	85
4.2.1	オートサーチ.....	85
4.2.2	マニュアル追加.....	86
4.3	ユーザー管理.....	88
4.3.1	カードタイプの選択.....	88
4.3.2	ユーザーの追加.....	89
4.3.2.1	マニュアル追加.....	89
4.3.2.2	バッチの追加.....	93
4.3.2.3	デバイスからユーザーを抽出.....	94
4.3.2.4	ユーザーのインポート.....	94
4.3.3	カードを一括して発行する.....	94
4.3.4	ユーザー情報のエクスポート.....	96
4.4	許可設定.....	96
4.4.1	許可グループの追加.....	96
4.4.2	許可設定.....	98
4.5	アクセスマネージャー.....	98

4.5.1 遠隔でドアを開閉する.....	98
4.5.2 常時開・常時閉の設定.....	99
4.5.3 ドアの状態をリセットする.....	100
4.6 アテンダンス・マネージメント.....	100
4.6.1 レポート検索.....	101
4.6.2 その他の構成.....	101
5 よくある質問.....	103
Appendix 1 顔登録の注意点/比較.....	104
Appendix 2 サイバーセキュリティに関する提言.....	107
問い合わせ先.....	110

1 概要

1.1 はじめに

アクセスコントローラーは、顔、パスワード、カードによる解錠、およびそれらの組み合わせによる解錠をサポートするアクセスコントロールパネルです。

1.2 特徴

- 液晶ディスプレイは、4.3 インチ（解像度は 480×272）です。
- フェイスロック、IC カードロック、パスワードロックに対応し、期間によるロック解除も可能です。
- 顔検出ボックスでは、同時に現れた顔の中で最も大きな顔が最初に認識されますが、最大の顔サイズは Web インターフェースで設定できます。
- 2MP 広角 WDR レンズ、オート/マニュアル照明付き。
- 顔認証の距離は 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ーは顔の 360 以上の位置を認識することができます。
- 顔認証精度 99.5%以上、低誤認識率。
- プロファイル認識に対応し、プロファイルの角度は 0° ～90° です。
- ライブネス検出に対応。
- 強迫警報、タンパー警報、侵入警報、ドア接点タイムアウト警報、不正カード超過警報、不正パスワード超過警報、外部警報をサポートします。
- 一般ユーザー、パトロールユーザー、ブロックリストユーザー、VIP ユーザー、ゲストユーザー、その他のユーザー、およびカスタムユーザーをサポートします。
- ユーザーのプライバシーを守るための様々なロック解除状態の表示モード。
- 体温モニターに対応。



当機種には指紋認証機能はありませんが、メニュー上で指紋機能に関する表示が出る場合は、機能しませんので無視してください。

1.3 アプリケーション

オフィス、学校、工場、住宅などに適用できるアクセスコントローラーです。顔認証により本人確認を行い、接触のない通行を実現します。

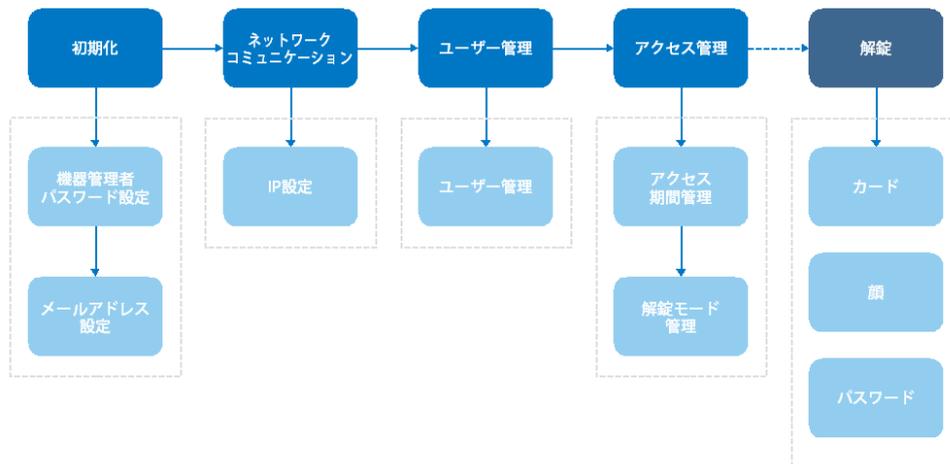
Figure 1-1 ネットワーク図



2 システム運用

2.1 基本的な設定方法

Figure 2-1 基本的な設定方法



2.2 共通アイコン

Table 2-1 アイコンの説明

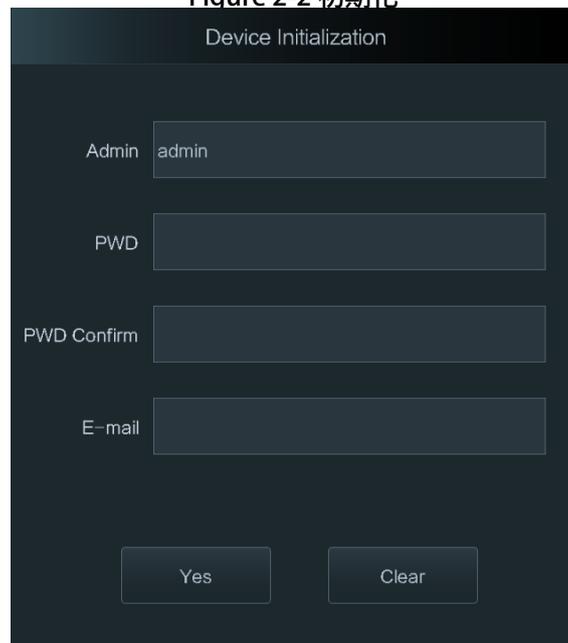
アイコン	説明
	アイコンを確認します。
	リストの最初のページに移動します。
	リストの最後のページに移動します。
	リストの前のページに移動します。
	リストの次のページに移動します。
	前のメニューに戻ります。
	有効にします。
	無効にします。
	前のページに移動します。
	次のページに移動します。

2.3 初期化

機器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最初の電源投入時または設定初期化後に必ず設定する必要があり、設定しないとアクセスコントローラを使用できません。

1つのアクセスコントローラーには機器管理者パスワードは1つしかありません。

Figure 2-2 初期化



- この画面で設定された管理者パスワードは、ウェブ管理プラットフォームにログインするために使用されます（IDは“Admin”固定です）。
- 機器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、入力したメールアドレスから再設定することができます。
- パスワードは、8～32個の空白以外の文字で構成され、大文字、小文字、数字、特殊文字（「」 ; : &を除く）のうち、少なくとも2種類の文字を含む必要があります。

2.4 スタンバイ・インターフェース

顔、指紋、パスワード、カードでロックを解除できます。



- ロック解除の方法は、機種によって異なる場合があります。
- 30秒以内に操作がない場合、アクセスコントローラーは待機状態になります。
- 本項で示した待受画面は参考例であり、実際のものとは異なる場合があります。

Figure 2-3 スタンバイ・インターフェース

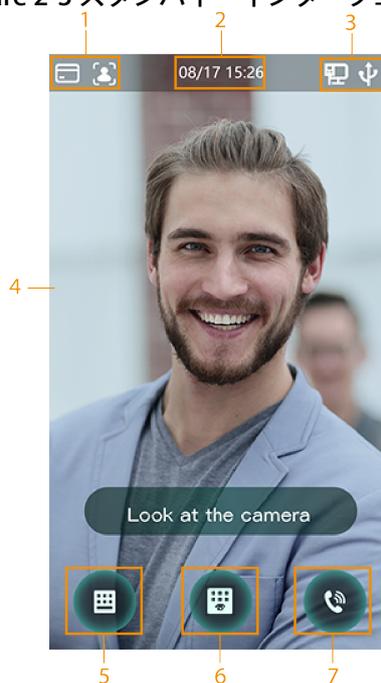


Table 2-2 ホーム画面の説明

No.	説明
1	<p>ロック解除方法。カード、顔認証、パスワード</p> <p></p> <p>カード、顔、パスワードのすべてをロック解除モードに設定すると、アクセスコントローラーの左上にパスワードのアイコンが表示されなくなります。</p>
2	日付と時刻。現在の日付と時刻を表示します

No.	説明
3	ネットワークと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	管理者パスワードのロック解除アイコン
7	タップすると、他のデバイスに電話をかけることができます（要設定）
-	カード読取りエリア（画面下の四角枠）

2.5 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ーを追加したり、アクセス関連のパラメータを設定したり、ネットワークの設定を行ったり、アクセス記録やシステム情報を確認したりすることができます。

Step 1 待機中の画面を3秒を長押しすると、管理者ログインのインターフェースになります。

Step 2 管理者ログインの方法を選択します。



モードによって対応するロック解除方法が異なりますので、実際のインターフェースを優先してください。

Figure 2-5 管理者ログイン

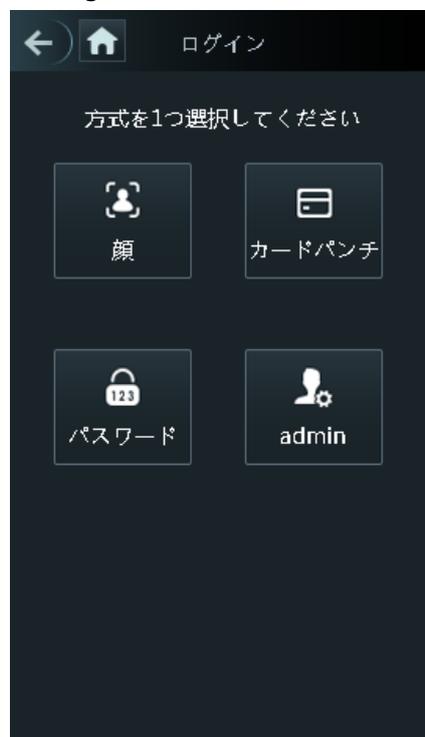


Figure 2-6 メインメニュー



2.6 ロック解除方法

顔、パスワード、カードでロックを解除できます。

2.6.1 カード

カードをカード読取りエリアに置き、認証されると、ドアのロックが解除されます。

2.6.2 顔

顔認証枠の中央に顔を映し、認証されると、ドアのロックが解除されます。

2.6.3 指紋

指紋センサーに指紋を当て、認証されると、ドアのロックが解除されます。



当機種には指紋認証機能はございません、メニュー上に存在しますが機能しません。

2.6.4 ユーザーパスワード

ユーザーパスワードを入力すると、ドアのロックが解除された状態になります。

Step 1 ホーム画面のをタップします。

Step 2 パスワードアンロック画面が表示されます。

Step 3 ユーザー ID とパスワードを入力し、をタップします。ドアのロックが解除されます。

2.6.5 スーパーパスワード

スーパーパスワードを入力すると、解錠することができます。スーパーパスワードは、1つのアクセスコントローラーに対して1つだけです。スーパーパスワードは、ユーザーレベル、ロック解除モード、期間、ホリデープラン、アンチパスバックの影響を受けずにドアをロック解除することができます。



ユーザのスーパーパスワードを"有効"し、スーパーパスワードを設定しないと利用できません。

"2.8.1.5NC 期間"でNCを選択した場合、スーパーパスワードは使用できません。

Step 1 ホームページのをタップします。

Step 2 スーパーパスワード画面が表示されます。

Step 3 スーパーパスワードを入力して、をタップします。ドアのロックが解除されています。

2.7 ユーザー管理

ユーザー管理では、新規ユーザーの追加、ユーザーリスト、管理者リストの表示、スーパーパスワードの変更が可能です。

2.7.1 新規ユーザーの追加

ユーザー ID、名前、顔画像、カード、パスワードの入力、ユーザーレベルの選択などにより、新たなユーザーを追加することができます。

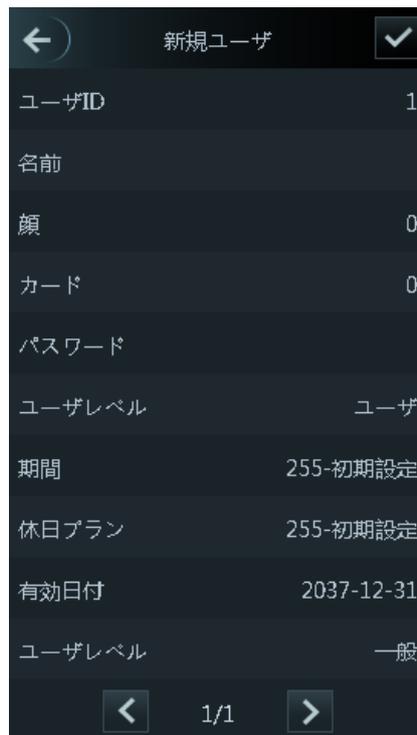


以下の図は参照用であり、実際の画面が優先されます。

Step 1 メインメニューにログインします。

Step 2 ユーザー->新規ユーザーを選択します。

Figure 2-7 新規ユーザー登録



Step 3 新規ユーザーのパラメータを設定します。

Table 2-3 新規ユーザーパラメータの説明

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が使用でき、最大 32 文字でユーザー ID は重複できません。
名前	文字数 32 文字以内（数字、記号、文字を含む）です。
顔	自分の顔が写真撮影枠の中央にあることを確認すると、アクセスコントローラーは自動的に新しいユーザーの顔を撮影します。
カード	ユーザーごとに最大で 5 枚のカードを登録できます。カード登録のインターフェイスで、カード番号を入力するか、カードを読み取ると、カード情報がアクセスコントローラーに読み込まれます。 カード登録インターフェイスで強迫カード機能を有効にすることができます。強迫カードがドアの解錠に使用されると、アラームが作動します。  カードロック解除に対応しているのは一部の機種のみです。

パラメータ	説明
パスワード	<p>ドアロック解除のパスワードです。パスワードの最大長は数字8桁です。</p> <p> アクセスコントローラーにタッチパネルがない場合は、アクセスコントローラーと周辺機器のカードリーダーを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。</p>
ユーザーレベル	<p>新規に使用するユーザーレベルを選択することができます。2つのオプションがあります。</p> <ul style="list-style-type: none"> ● ユーザー：ユーザーはドアロック解除の権限のみを持っています。 ● 管理者：管理者はドアのロックを解除することができ、設定の権限も持っています。 <p> 初期化時に設定した機器管理者ユーザー以外にも、必要に応じて管理者権限のあるユーザーを登録できます。</p>
期間	<p>ユーザーが解錠できる期間を設定することができます。</p> <p>詳細は“3.7 タイムセクション”を参照してください。</p>
ホリデープラン	<p>ユーザーが解錠できる休日プランを設定することができます。</p> <p>詳細は“3.7 タイムセクション”を参照してください。</p>
有効期限	<p>ユーザーのロック解除情報を有効にする期間を設定できます。</p>

パラメータ	説明
ユーザーレベル	<p>レベルは6段階あります。</p> <ul style="list-style-type: none"> ● 一般ユーザー：一般ユーザーは通常通りドアを解錠できます。 ● ブロックリスト：ブロックリストに登録されているユーザーはロック解除の権限がありません。このユーザーがドアのロックを解除しようとする、アクセスコントローラは「このユーザーはブロックリストのユーザーである」というプロンプトを表示します。 ● ゲスト：ゲストは一定の時間、ドアを開けることができます。一度上限回数を超えてしまうと、再度解錠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、勤怠を追跡することができますが、ロック解除の許可はありません。 ● VIP：VIPがドアを開けると、サービスマンにプロンプトが表示されます。 ● その他：特別な人がロックを解除すると、ドアが閉まるまでに5秒間の遅延が発生します。 ● Custom User 1：カスタマイズ用に予約されています。ユーザーは通常のロック解除が可能です。 ● Custom User 2：カスタマイズ用に予約されています。ユーザーは通常のロック解除が可能です。
使用時間	ユーザーレベルが「ゲスト」の場合、解錠できる最大回数を設定することができます。

Step 4 をタップして設定を保存します。

2.7.2 ユーザー情報の閲覧

ユーザーインターフェースでは、ユーザーリスト、管理者リスト、管理者パスワードの有効化を行うことができます。

2.8 アクセス管理

期間、ロック解除モード、アラーム、ドアの状態、ロック保持時間などのアクセス管理が可能です。アクセスをタップすると、アクセス管理のインターフェースになります。

2.8.1 期間管理

期間、休日期間、休日計画期間、ドア通常オン期間、ドア通常クローズ期間、遠隔確認期間を設定することができます。

2.8.1.1 期間設定

 ウェブインターフェイスで期間を設定することができます。

設定できる期間（週）は、0～127までの128種類です。1つの期間（週）の各日に4つの期間を設定できます。ユーザーは、設定した期間にしか解錠できません。

2.8.1.2 ホリデーグループ

 ウェブインターフェイスでホリデーグループを設定することができます。

グループの休日を設定し、休日グループのプランを設定することができます。設定できるグループは、0～127までの128グループです。1つのグループに16の休日を追加できます。ホリデーグループの開始時間と終了時間を設定し、設定した時間帯のみユーザーが解錠できるようにします。

 入力できる文字数は32文字（数字、記号、文字を含む）です。 をタップすると、ホリデーグループ名が保存されます。

2.8.1.3 ホリデープラン

 ウェブインターフェイスでホリデープランを設定することができます。

休日プランに休日グループを追加することができます。休日プランを使って、異なる休日グループのユーザーのアクセス許可を管理することができます。ユーザーは、設定した期間にしかドアを解錠できません。

2.8.1.4 NO 期間

NO 期間に期間を加えると、その期間はドアが正常に開いている状態になります。

 NO/NC 期間の権限は、他の期間設定の権限よりも高くなります。

2.8.1.5 NC 期間

NC 期間に期間が追加された場合、その期間はドアが通常閉まっている状態になります。この期間はユーザーでは解錠できません。

2.8.1.6 リモート検証期間

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を解錠するには、リモート検証が必要となります。この期間にドアをロック解除するには、管理プラットフォームから送信されるドアロック解除命令が必要です。

 リモート検証期間を有効にする必要があります。

-  は、有効であることを意味します。
-  は、無効を意味します。

2.8.2 ロック解除

ロック解除モードには、ロック解除モードと温度監視モードの2種類があります。本項で説明するロック解除モードは参考値であり、モデルによって異なる場合があります。

2.8.2.1 アンロックモード

ロック解除モードをオンにすると、カード、顔、指紋、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って、ロック解除することができます。

Step 1 メインメニューにログインします。

Step 2 アクセス→アンロックモード→アンロックモードを選択します。

Figure 2-8 認証方法（複数選択可）



Step 3 ロック解除方法を1つまたは複数選択します。

- 上の図に表示されているロック解除方法はあくまでも参考であり、モデルによって異なる場合があります。※指紋認証はありませんので、選択しないでください。
- 選択したロック解除方法をもう一度タップすると、その選択が解除されます。

Step 4 組み合わせモードを選択します。

- + および (And) : 例えば、「card + PWD」を選択した場合、まずカードで認証し、次にパスワードで認証後に解除されます。
- / または (Or) : 例えば、「card/PWD」を選択した場合、カードで認証するか、パスワードで認証すると解除されます。

Step 5 をタップをすると設定が保存されます。

Step 6 アンロックモードを有効にする。

- は、有効であることを意味します。
- は、無効を意味します。

2.8.2.2 温度監視モード

温度が正常になると、アクセスコントローラーがドアのロックを解除します。

Step 1 メインメニューにログインします。

Step 2 アクセス→アンロックモードを選択し、**測温モードのみ**を有効にします。

2.8.3 アラーム設定

管理者はアラームの設定により、訪問者のロック解除権限を管理することができます。

Step 1 メインメニュー画面にログインします。

Step 2 アクセス→アラームを選択します。

Figure 2-9 アラーム



- は、有効であることを意味します。
- は、無効を意味します。

Table 2-4 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	アンチパスバックを有効にした後は、入退室時に ID を確認する必要があります。そうしないとアラームが作動します。 <ul style="list-style-type: none"> ● ID を確認して入室し、ID を確認せずに退室した場合、その人が再び入室しようとするときアラームが作動し、その人はそれ以上ドアのロックを解除することができなくなります。 ● ID を確認せずに入室した場合、ID を確認して退室しようとするときアラームが作動し、それ以上の解錠許可が得られなくなります。
強迫	強迫カードや強迫パスワードで解錠されると、アラームが作動します。 ※何者かに脅され、解錠を迫られた際に使用する機能です。
侵入	ドアコンタクトが解除されていない状態でドアが解錠されると、侵入アラームが作動します。
ドアセンサータイムアウト	ユーザーがドアのロックを解除するのにかかった時間が、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作動します。 ドアセンサーのタイムアウト時間の範囲は 1~9999 秒です。
ドアセンサーオン	ドアセンサーオンが有効な場合のみ、侵入アラームとドアセンサーのタイムアウトアラームが作動します。

2.8.4 ドアの状態

3つのオプションがあります。NO、NC、Normalの3種類です。

- NO：NOを選択した場合、ドアの状態はノーマルオープンとなり、ドアが閉じられることはありません。
- NC：NCを選択した場合、ドアの状態はノーマルクローズとなり、ドアのロックが解除されないこととなります。
- Normal：Normalを選択すると、設定に応じてドアの解錠・施錠が行われます。

2.8.5 ロック保持時間

ロック保持時間は、ロックが解除されている期間です。ロックが解除されている期間がこの期間を超えると、自動的にロックされます。

2.9 出勤

必要に応じて出勤（勤怠）を有効にしたり、出勤モードを設定することができます。



この機能は、プラットフォームとの連携が必要です。詳しくは、対応するユーザーズマニュアルをご覧ください。

Step 1 メインメニューにログインします。

Step 2 出勤をタップし、出席可能をタップし  有効にします。

Figure 2.10 アテンダンス



Step 3 モード設定をタップすると、出席モードと、出席状況に応じた時間を設定できます。

- **自動/手動モード**：チェックイン（出勤）またはチェックアウト（退勤）した時間に応じて出席状況を表示します。チェックインまたはチェックアウトの時間が定義されていない場合は、出席イベントをタップして、必要に応じて出席状況を選択することができます。
- **オートモード**：チェックイン・アウトした時間に応じて、出席状況を表示します。
- **手動モード**：チェックインやチェックアウトの際に、手動で出席状況を選択する必要があります。
- **固定モード**：待機中のインターフェースでパンチイン/アウトすると、出席状況が固定されます。

Figure 2-11 出席状況



自動/手動モード	
チェックイン	06:00-09:59
退勤	10:00-12:59
再出勤	13:00-15:59
チェックアウト	16:00-20:59
残業開始	00:00-00:00
残業終了	00:00-00:00



6つのステータスについては、仕事始めの **Check In** や、昼休みの **Break Out** など、必要に応じて定義することができます。

2.10 ネットワーク通信

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

2.10.1 IP コンフィギュレーション

アクセスコントローラーがネットワークに接続されるようにIPアドレスを設定します。※有線LAN

Step 1 メインメニューにログインします。

Step 2 接続→ネットワーク設定→IPアドレスを選択し、IPアドレスのパラメータを設定します。

Figure 2-12 IPアドレスの設定

Table 2-5 IP 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、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、 <input checked="" type="checkbox"/> をタップして設定内容を保存します。
DH CP	DH CP (Dynamic Host Configuration Protocol)。 DH CP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アドレスの手動設定ができなくなります。
P2P	P2Pは、DDNSやポートマッピング、トランジットサーバーを必要とせず、ユーザーがデバイスを管理できるプライベートネットワークトラバーサル技術です。



Web インターフェースにログインするコンピューターが、アクセスコントローラーと同じLAN内にあることを確認してください。

2.10.2 アクティブレジスタ

アクティブ登録することで、アクセスコントローラーと管理プラットフォームを接続し、管理プラットフォームでアクセスコントローラーを管理することができます。

 管理台で行った設定をクリアし、アクセスコントローラーを初期化することができますが、不適切な操作によるデータ損失に備えて、管理台の権限を保護する必要があります。

Step 1 メインメニューにログインします。

Step 2 接続→ネットワーク→アクティブ登録を選択します。

Step 3  をタップしてアクティブレジスターを有効にし、パラメータを設定します。

Table 2-6 アクティブレジスタ

名前	パラメータ
サーバー IP アドレス	管理するプラットフォームの IP アドレス。
ポート	管理する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上の下位デバイスの番号。

2.10.3 Wi-Fi

アクセスコントローラーに Wi-Fi 機能が搭載されている場合は、Wi-Fi でアクセスコントローラーをネットワークに接続することができます。

Step 1 メインメニュー画面にログインします。

Step 2 接続→ネットワーク→Wi-Fiを選択します。

Step 3  をタップして Wi-Fi を有効にします。

Step 4  をタップし、ネットワークを選択して、パスワードを入力します。

以下のインターフェイスでネットワークの情報を見ることができます。

Figure 2-13 Wi-Fi



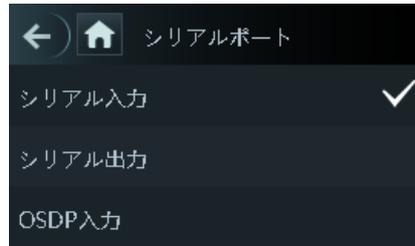
2.10.4 シリアルポートの設定

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。

Step 1 メインメニュー画面にログインします。

Step 2 接続→シリアルポートを選択します。

Figure 2-14 シリアルポート



- カードの読み書き機能を持つ外部機器をアクセスコントローラに接続する場合は、**シリアル入力**を選択します。シリアル入力を選択すると、アクセスカードの情報をアクセスコントローラや管理プラットフォームに送信することができます。
- 顔認証やカードの読み書き機能を持つアクセスコントローラの場合、**シリアル出力**を選択すると、アクセスコントローラが他の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2種類あります。ユーザー ID とカード番号です。
- 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、**OSDP Input**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することができます。

2.10.5 ウィーガンド (Wiegand) 構成

Wiegand 入力または **Wiegand 出力**を適宜選択してください。

Step 1 メインメニュー画面にログインします。

Step 2 接続→**Wiegand**を選択します。

Figure 2-15 ウィーガンド



- 外部のカードスワイプ機構をアクセスコントローラに接続する場合は、**Wiegand 入力**を選択します。

- アクセスコントローラが他のコントローラに接続可能なリーダーとして動作する場合は、**Wiegand 出力**を選択します。Table 2-7 を参照してください。

Table 2-7 ウィーガンド出力

パラメータ	説明
ウィーガンド出力タイプ	<p>Wiegand 出力種別は、カード番号またはアクセスコントローラが認識できる番号の桁を決定します。</p> <ul style="list-style-type: none"> ● Wiegand26、3バイト、6桁。 ● Wiegand34、4バイト、8桁。 ● Wiegand66、8バイト、16桁。
パルス幅	<ul style="list-style-type: none"> ● 必要に応じてパラメータを設定する。
パルスインターバル	
出力データタイプ	<ul style="list-style-type: none"> ● ユーザー ID：ユーザー ID が出力されます。 ● カード番号：カード番号が出力されます。

2.11 システム

2.11.1 時間

日付フォーマット設定、日付設定、時刻設定、サマータイム設定、NTP チェック、タイムゾーン設定などができます。

Step 1 メインメニュー画面にログインします。

Step 2 システム→時間を選択し、時間のパラメータを設定します。

Figure 2-16 時間



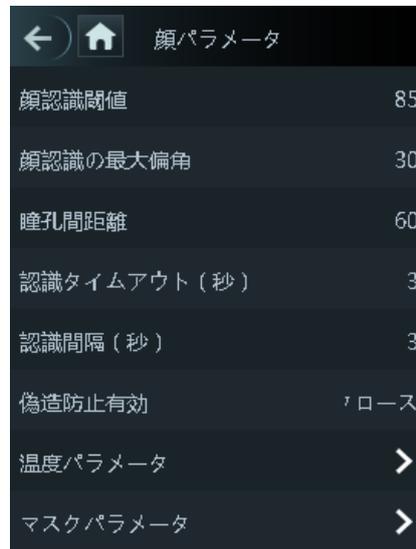
- NTP(Network Time Protocol)を選択した場合は、まず NTP チェック機能を有効にする必要があります。サーバー IP アドレス：タイムサーバーの IP アドレスを入力すると、アクセスコントローラーの時刻がタイムサーバーに同期されます。
- ポート：NTP サーバーのポート番号を入力します。
- インターバル（分）：NTP サーバーへのチェックの間隔。保存する場合は、保存アイコンをタップします。

2.11.2 顔パラメータ

Step 1 メインメニューにログインします。

Step 2 システム→顔パラメータを選択します。

Figure 2-17 フェイスパラメータ



Step 3 パラメータをタップして設定を行い、をタップします。

Table 2-8 顔のパラメータ

パラメータ	説明
顔認識閾値	顔認識の精度を調整することができます。この値が大きいほど、精度が高くなります。
顔認識の最大偏角	プロファイルのコントロールパネルの撮影角度を設定します。値が大きくなるほど、プロファイルの認識範囲が広がります。
瞳孔間距離	瞳孔間距離とは、両眼の瞳孔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ーが必要に応じて顔を認識するためには、適切な値を設定する必要があります。この値は、顔の大きさや、顔とレンズの距離によって変化します。顔とレンズの距離が近いほど、値を大きくする必要があります。大人がレンズから 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。
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	顔にアクセス許可がない場合、コントローラーはその顔が無効であることをプロンプト表示します。プロンプトの間隔は、無効な顔のプロンプト間隔です。
偽造防止有効	顔画像やモデルを使ったロック解除を防ぐ機能です。

パラメータ	説明
温度パラメータ	<ul style="list-style-type: none"> ● 温度測定：この機能を有効または無効にします。 ● 測温エリア枠：温度監視ボックスを表示するかどうかを設定します。 ● 測温距離 (cm)：デフォルトでは 50。定義した距離でアクセスコントローラーから離れて立って温度をモニターする必要があります。 ● 温度設定値：温度のしきい値を設定します。モニターの体温が設定値以上の場合、高温と判断されます。 ● 高温：測定温度範囲の最高温度を設定します。 ● 低温：測定温度範囲の最低温度を設定します。 ● 温度校正值：このパラメータはテスト用です。温度モニター環境の違いにより、モニター温度と実際の温度に誤差が生じる場合があります。テスト用に複数のモニターサンプルを選択し、モニター温度と実際の温度の比較に応じて、このパラメータで温度偏差を補正することができます。例えば、モニター温度が実際の温度よりも 0.5°C 低い場合、補正值は 0.5°C に設定され、モニター温度が実際の温度よりも 0.5°C 高い場合、補正值は -0.5°C に設定されます。 ● 温度監視モード： <ul style="list-style-type: none"> ◆ オートモード：顔のヒートマップを使って顔認識を行います。ヒートマップが見つからない場合は、自動的にキャリブレーションモードに切り替わります。 ◆ サーマルモード：顔認識と温度監視にヒートマップのみを使用。 ◆ 標定モード：顔の白色光画像を使用して顔認識を行い、顔のヒートマップ上の座標を抽出して適用し、温度モニタリングを行う。 ● 温度単位：°C または °F を選択します。 ● 補償値：モニター環境の温度に加算される値です。 ● 測温戦略：

パラメータ	説明
	<ul style="list-style-type: none"> ◆ 最大：最も高い温度を結果とします。 ◆ 平均：平均温度を結果とします。
マスクのパラメータ	<ul style="list-style-type: none"> ● マスクモデル：マスク検出のパラメータを設定します。 <ul style="list-style-type: none"> ◆ テストなし：顔認識時にマスクを検出しない。 ◆ マスク注意：顔認識時にマスクが検出されます。マスクを着用していない人物が検出された場合、システムはマスクリマインダーを促し、通行が許可されます。 ◆ マスク阻止：顔認識時にマスクを検出します。マスクを着用していない人物が検出された場合、システムはマスクリマインダーを促し、通過は許可されません。 ● マスク認識閾値：マスクが検出されると、この値が顔認識に適用されます。この値が大きいほど、要求される精度が高くなり、マスクをしている人を認識するのが難しくなります。

2.11.3 画像モード

3つの選択肢があります。

- 屋内：アクセスコントローラーが屋内に設置されている場合は、**屋内**を選択します。
- 屋外：アクセスコントローラーが屋外に設置されている場合は、**屋外**を選択します。
- その他：通路や廊下など、バックライトがある場所にアクセスコントローラーを設置する場合は、**その他**を選択してください。

2.11.4 音量

ビープ音、マイク音量それぞれ調整できます。

■ または ■ をタップして音量を調整します。

2.11.5 言語

以下の言語に対応しています。英語、イタリア語、スペイン語、日本語、ロシア語、トルコ語、ポーランド語、韓国語、アラビア語、スペイン語（ラテンアメリカ）、タイ語。

2.11.6 赤外線ライト設定

■ または ■ をタップして、赤外線の色を調整します。

この値が大きいほど、赤外線は明るくなります。

2.11.7 スクリーン設定

スクリーンセーバーの時間とスクリーンタイムアウトの時間を設定できます。

Step 1 メインメニューにログインします。

Step 2 システム→スクリーン設定を選択します。



スクリーンセーバーの時間とスクリーンタイムアウトの時間は常に次の関係を保つような設定が必要です。スクリーンセーバー<スクリーンタイムアウト

Figure 2-18 画面設定



2.11.8 工場出荷時設定への復元



- アクセスコントローラーを工場出荷時の状態に戻すと、データは失われます。
- アクセスコントローラーを工場出荷時の状態に戻しても、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て、アクセスコントローラーを工場出荷時の状態に戻すことが選択できます。
- ユーザー情報やデバイス情報を保持したまま、アクセスコントローラーを工場出荷時の状態に戻すことが選択できます。

Step 1 メインメニューにログインします。

Step 2 システム→出荷時設定の復元を選択し、出荷時設定の復元か、出荷時設定の復元（ユーザとログの保存）を選択すると、アクセスコントローラーが再起動します。

2.11.9 リブート（再起動）

Step 1 メインメニューにログインします。

Step 2 システム→リブートを選択すると、アクセスコントローラーが再起動します。

2.12 USB



- ユーザー情報のエクスポートやアップデートを行う前に、アクセスコントローラーにUSBメモリが挿入されていることを確認してください。
- 書き出しやアップデート中は、USBメモリを抜いたり、アクセスコントローラーを操作したりしないでください。
- あるアクセスコントローラーの情報をUSBにエクスポートして、別のアクセスコントローラーにインポートすることができますが、顔や指紋など、機種によって対応する情報の種類が異なります。
- USBメモリはプログラムのアップデートにも利用できます。

2.12.1 USBエクスポート

USBメモリを挿入した後、アクセスコントローラーからUSBメモリにデータをエクスポートすることができます。エクスポートされたデータは暗号化され、編集することはできません。

Step 1 メインメニューにログインします。

Step 2 USB→USBエクスポートを選択します。

Figure 2-19 USB エクスポート



Step 3 エクスポートしたいデータタイプを選択します。

 指紋認証に対応しているのは一部のモデルのみです。

Step 4 OKをタップします。

データはUSBメモリに保存されます。

2.12.2 USB インポート

あるアクセスコントローラーからエクスポートされたUSBメモリ内のデータのみが、別のアクセスコントローラーにインポートできます。

Step 1 メインメニューにログインします。

Step 2 USB→USBインポートを選択します。

Figure 2-20 USB インポート



Step 3 インポートしたいデータタイプを選択します。

 指紋認証に対応しているのは一部のモデルのみです。

Step 4 OK をタップします。

USB メモリ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。

2.12.3 USB 更新 (アップデート)

USB メモリでのアップデートが可能です。

Step 1 アップデート用のファイル名を "update.bin" に変更し、USB メモリーのルートディレクトリに "update.bin" ファイルを保存してください。

Step 2 メインメニューにログインします。

Step 3 **USB→USB 更新** を選択します。

Step 4 **OK** をタップします。

アップデートが開始され、アップデート終了後にアクセスコントローラーが再起動します。

2.13 特徴

プライバシー設定、カード番号逆順、セキュリティモジュール、サーマルディスプレイ、外部検温モジュール、ドアセンサータイプ、結果フィードバックなどの設定が可能です。

Step 1 メインメニューにログインします。

Step 2 特徴をタップします。

Figure 2-21 特徴



Table 2-9 特徴

パラメータ	説明
プライバシー設定	詳しくは2.13.1 プライバシー設定をご覧ください。
カード番号逆順	サードパーティ製カードリーダーをwiegand出力ポート経由でアクセスコントローラに接続する必要がある場合は、カード番号リバース機能を有効にする必要があります。そうしないと、アクセスコントローラとサードパーティ製カードリーダー間の通信がプロトコルの不一致により失敗する可能性があります。
セキュリティモジュール	<ul style="list-style-type: none"> ● セキュリティモジュールを有効にする場合は、別途、アクセスコントロール用セキュリティモジュールを購入する必要があります。また、セキュリティモジュールには別途電源が必要となります。 ● セキュリティモジュールを有効にすると、出口ボタン、ロックコントロール、消火器の連動は無効になります。
サーモグラム表示	左上にヒートマップを表示します。

外付けリーダーの 温度監視	有効にすると、カードリーダーが人の体温も監視します。
ドアセンサー	NO はノーマルオープン、 NC はノーマルクローズです。
結果フィードバック	ロック解除時の結果フィードバックモードを選択します。2.13.2 結果フィードバックをご参照ください。

2.13.1 プライバシー設定

Figure 2-22 プライバシー設定



Table 2-10 プライバシー設定

パラメータ	説明
パスワードリセットのイネーブル	<p>パスワードリセットイネーブル機能が有効な場合、パスワードをリセットすることができます。</p> <p>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。</p>
HTTPS	<p>HTTPS (Hypertext Transfer Protocol Secure) は、コンピュータネットワーク上で安全な通信を行うためのプロトコルです。</p> <p>HTTPS が有効な場合は、CGI コマンドへのアクセスに HTTPS が使用され、そうでない場合は HTTP が使用されます。</p> <p></p> <p>HTTPS を有効にすると、アクセスコントローラーは自動的に再起動します。</p>
CGI	<p>CGI (Common Gateway Interface) は、Web ページを動的に生成するサーバー上で動作するコンソールアプリケーションと同様に、Web サーバープログラムを実行するための標準プロトコルを提供します。</p> <p>CGI を有効にすると、CGI コマンドが使用できるようになります。初期設定では CGI が有効になっています。</p>
SSH	<p>Secure Shell (SSH) は、安全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操作するための暗号化ネットワークプロトコルです。</p> <p>SSH を有効にすると、データ送信時に SSH による暗号化サービスが行われます。</p>
写真を撮る	<p>ON を選択すると、ユーザーがドアをロック解除したときに、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は ON になっています。</p>
デバッグモード	<p>このモードを有効にすると、スタンバイ・インターフェースに黒体の温度が表示されます。それに応じて、黒体の温度を修正することができます。</p> <p></p> <ul style="list-style-type: none"> ● この機能に対応しているのは一部の機種のみです。 ● このモードを有効にすると、どのような方法でもドアを開けることができなくなります。
温度表示	<p>有効にすると、ロック解除の結果に温度が表示されます。</p>
キャプチャした写真をクリアにする	<p>撮影した写真をすべて削除します。</p>
顔プライバシー	<p>有効にすると、待機中のインターフェースがモザイクで覆われます。</p>

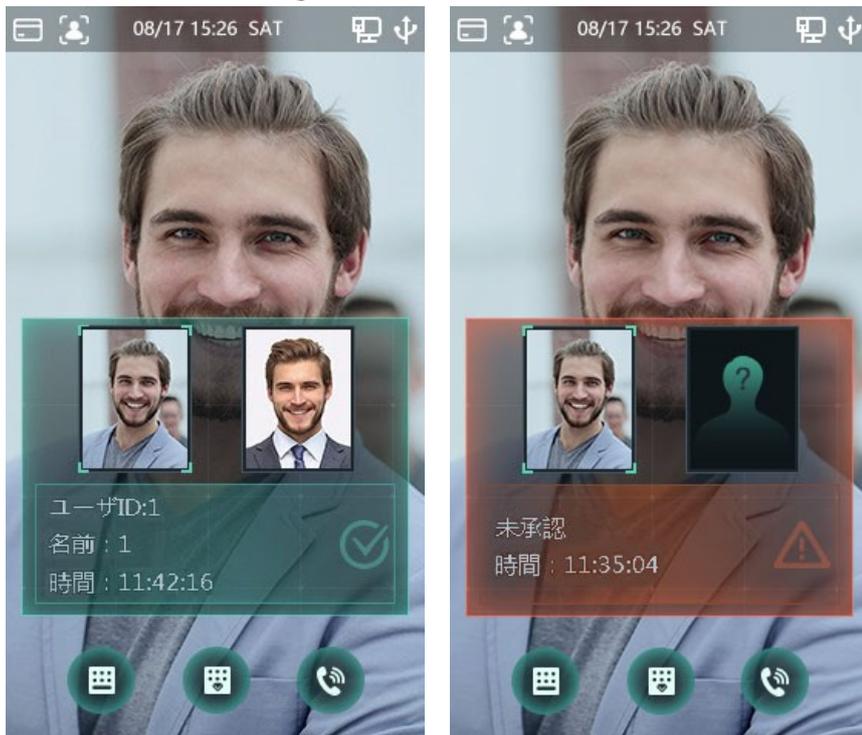
2.13.2 結果フィードバック

4つの結果フィードバックモードがあります。成否、名前のみ、ユーザーの写真と、写真比較と名前。

必要に応じて、結果のフィードバックモードを選択することができます。

- 写真比較と名前モード
- ロック解除時には、撮影された顔画像、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、時刻などが表示されます。

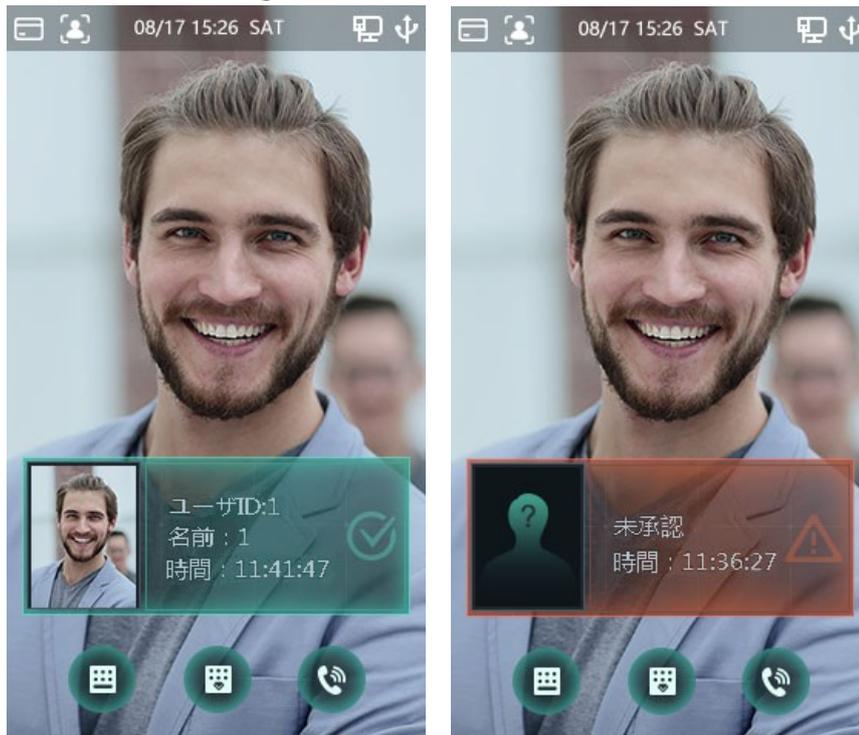
Figure 2-23 写真比較と名前モード



- ユーザーの写真を表示モード

ロック解除時には、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、時刻が表示されます。

Figure 2-24 ユーザーの写真を表示モード



- 名前のみモード

ロック解除時に表示されるのは、ユーザー ID、ユーザー名、時間のみです。

Figure 2-25 オンリーネームモード



- 成否モード

ロック解除時に成功か失敗かだけを表示します。

Figure 2-26 成否モード



2.14 録画

すべてのロック解除記録を照会できます。

Figure 2-27 パンチの記録を検索



ユーザID	時間	結果	認識方式
1	07-22 11:42	OK	顔
1	07-22 11:42	OK	顔
1	07-22 11:41	OK	顔
1	07-22 11:41	OK	顔
1	07-22 11:41	OK	顔
1	07-22 11:41	OK	顔
1	07-22 11:41	OK	顔
1	07-22 11:40	OK	顔
1	07-22 11:39	OK	顔
	07-22 11:38	NG	顔

2.15 システム情報

アクセスコントローラーのデータ容量、デバイスバージョン、ファームウェア情報は、「システム情報」インターフェースで確認できます。

Step 1 メインメニューにログインします。

Step 2 装置情報をタップします。

Figure 2-28 システム情報



3 ウェブ運用

アクセスコントローラーの設定・操作は Web 上で行うことができます。Web 上では、ネットワークパラメーター、ビデオパラメーター、アクセスコントローラーのパラメーターを設定し、システムのメンテナンスやアップデートを行うことができます。

3.1 初期化

初めてウェブにログインする前に、パスワードとメールアドレスを設定する必要があります。

Step 1 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ーの IP アドレス（デフォルトは 192.168.1.108）を入力し、Enter キーを押します。



- 推奨ブラウザは Google Chrome 及び、Internet Explorer 8 以降です。
- Web にログインするパソコンが、アクセスコントローラーと同じ LAN 内にあることを確認してください。
- WiFi 接続で DHCP 利用場合は IP アドレスが自動取得されますので WiFi 設定画面で IP アドレスを確認してください。
- 本体初期化時に管理者 ID とパスワードが設定済みであれば、この項目は出ません。
Step4 のオートチェックより進めてください。

Figure 3-1 初期化

Boot Wizard

① Device Initialization ② Auto Check

Username admin

New Password

Low Medium High

Confirm Password

Password shall be at least 8 digits, and shall at least include two types, including number, letter and common character

Bind Email

(It will be used to reset password. Please fill in or complete it timely)

Next

Step 2 新しいパスワードの入力、パスワードの確認、Eメールアドレスの入力を行い、「次へ」をクリックします。



- パスワードは、8～32 個の空白でない文字で構成され、大文字、小文字、数字、特殊文字（";:&を除く）のうち少なくとも2種類の文字を含む必要があります。セキュリティレベルの高いパスワードを設定するには、「パスワードの強度」のプロンプトに従ってください。
- セキュリティのため、初期化後もパスワードを適切に管理し、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再設定する場合は、セキュリティコードを受け取るためのメールアドレスが必要です。

Step 3 「次へ」をクリックします。

Figure 3-2 オートチェック



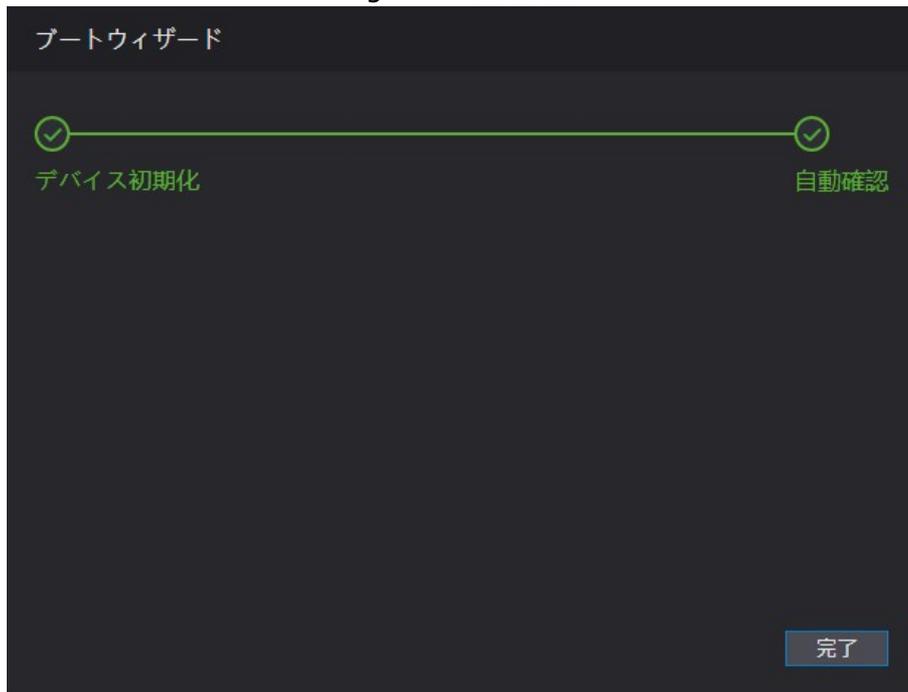
Step 4 **自動確認（オートチェック）**を選択するかどうかを決めることができます。



最新のプログラムを入手するには、**自動確認**を選択することをお勧めします。

Step 3 「次へ」をクリックします。

Figure 3-3 設定完了



Step 5 完了をクリックすると、初期化が完了します。

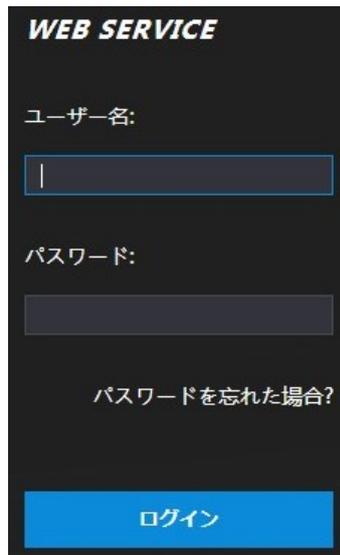
3.2 ログイン

Step 1 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ーの IP アドレスを入力し、**Enter** キーを押します。



- 推奨ブラウザは Google Chrome 及び、Internet Explorer 8 以降です。古いバージョンの場合はログインできない場合があります。
- Web にログインするパソコンが、アクセスコントローラーと同じ LAN 内にあることを確認してください。
- デフォルトの IP アドレスは 192.168.1.108 です。
WiFi 接続で DHCP 使用の場合は IP アドレスを自動取得しますので、アクセスコントローラーの WiFi 画面にて確認してください。

Figure 3-4 ログイン



Step 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ーの初期化後のログインパスワードです。管理者パスワードは定期的に変更し、適切に管理してください。
- 管理者ログインのパスワードを忘れてしまった場合は、「パスワードを忘れましたか?」"3.3 パスワードの再設定"をご覧ください。

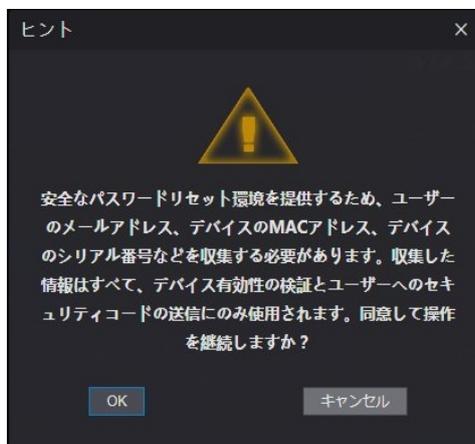
Step 3 ログインをクリックします。

3.3 パスワードの再設定

管理者アカウントのパスワードをリセットする際には、お客様のメールアドレスが必要となります。

Step 1 ログイン画面で「パスワードを忘れました」をクリックします。

Figure 3-5 ヒント



Step 2 ヒントを読む。

Step 3 **OK** をクリックします。

Figure 3-6 パスワードの再設定



Step 4 インターフェイス上の QR コードをスキャンすると、セキュリティコードが表示されます。



- 同じ QR コードを読み取ると、最大で 2 つのセキュリティコードが生成されます。セキュリティコードが無効になった場合は、QR コードを更新することで、より多くのセキュリティコードを得ることができます。
- QR コードを読み取って得られたコンテンツを指定のメールアドレスに送信すると、セキュリティコードが表示されます。
- セキュリティコードは、受け取ってから 24 時間以内にご使用ください。そうしないと、セキュリティコードが無効になります。
- 誤ったセキュリティコードが連続して 5 回入力されると、管理者が 5 分間フリーズします。

Step 5 受け取ったセキュリティコードを入力して下さい。

Step 6 「次へ」をクリックします。

Step 7 リセットして、新しいパスワードを確認します。



パスワードは、8~32 個の空白でない文字で構成され、大文字、小文字、数字、特殊文字（'";:&を除く）のうち、少なくとも 2 種類の文字を含む必要があります。

Step 8 **OK** をクリックすると、リセットが完了します。

3.4 ドアパラメータ

アクセスコントロールパラメータの設定

Step 1 Web インターフェースにログインします。

Step 2 ドアパラメータを選択します。

Figure 3-7 ドアパラメータ

ドアパラメータ

名前 Door1

状態 正常

開扉方法 アンロックモード

組み合わせ または

エレメント (複数選択) カード 指紋 パスワード 顔認識

保持時間 (秒) 3.0 (0.2-600)

常時開時間 無効化

常時閉時間 無効化

タイムアウト (秒) 60 (1-9999)

脅迫アラーム

ドアセンサー

侵入アラーム

時間切れアラーム

アンチバックアラーム

良 リフレッシュ 初期設定

Step 3 開扉方法の設定

- 時間セクション：開扉方法—時間セクションを選択

1)  をクリックして下さい。

Figure 3-8 タイムセクションパラメータ

変更

	日曜	月曜	火曜	水曜	木曜	金曜	土曜
<input checked="" type="checkbox"/> 有効化	時間セクシ...		00:00:00	-	23:59:59	開扉方法	カード/指紋/顔認識/パスワ
<input type="checkbox"/> 有効化	時間セクシ...		00:00:00	-	00:00:00	開扉方法	カード/指紋/顔認識/パスワ
<input type="checkbox"/> 有効化	時間セクシ...		00:00:00	-	00:00:00	開扉方法	カード/指紋/顔認識/パスワ
<input type="checkbox"/> 有効化	時間セクシ...		00:00:00	-	00:00:00	開扉方法	カード/指紋/顔認識/パスワ
<input type="checkbox"/> 週全体に適用							

良 中止

2) 時間帯別に時刻と開店方法を設定します。1日に最大4つの時間帯を設定することができます。

3) オプション) 他の日に設定をコピーするには、「週全体に適用」を選択します。

4) 良をクリックします。

- マルチカード：開扉方法—マルチカードを選択

1)  をクリックし、次に「追加」をクリックします。

Figure 3-9 複数人のパラメータ

- 2) 開封方法を選択し、有効なユーザーの番号を入力します。
- 3) ユーザーリストセクションでは、必要に応じてユーザーのIDを入力します。
ユーザーIDについては、「2.7 ユーザー管理」を参照してください。



- VIP、パトロール、ブロックリストのユーザーは追加できません。
 - ドアのロックを解除するには、異なるグループのすべてのユーザーがグループ内で自分のIDを確認する必要があります。
- アンロックモード
 - 1) エレメントのロック解除方法を選択してください（複数選択可）。

Figure 3-10 アンロックモードパラメータ

- 2) "または" または "および" を選択します。"または" は、定義されたすべての方法でドアを開ける必要があることを意味し、"および" は、定義されたどの方法でもドアを開けることができることを意味します。

Step 4 その他のパラメータを設定します。

Table 3-1 パラメータの説明

パラメータ	説明
名前	このアクセスコントローラーが制御するドアの名前を入力します。
状態	ノーマルクローズの場合は NC を選択し、ノーマルオープンの場合は NO を選択します。どちらかを選択した場合、定義された開扉方法は有効になりません。
開扉方法	上記の Step 3 を参照してください。
保持時間(秒)	ロック解除の期間。期限切れになると、ドアがロックされます。
常時開時間	ドアは常に開いているか閉じている状態になります。
常時閉時間	
タイムアウト (秒)	この値を超えてドアがロックされていない状態が続くと、タイムアウトアラームが発生します。
強迫アラーム	Table 2-4 参照
ドアセンサー	
侵入アラーム	
時間切れアラーム	
アンチパスバック・アラーム	

Step 5 良をクリックします。

3.5 アラーム連動

3.5.1 アラーム連動の設定

アラーム入力機器をアクセスコントローラーに接続し、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。

Step 1 Web インターフェースにログインします。

Step 2 アラームリンク > アラームリンク を選択します。

Figure 3-11 アラーム連動

アラーム入力	名前	アラーム入力タイプ	変更
1	Zone1	NO	

Step 3 をクリックすると、アラーム連動のパラメータを変更できます。

Figure 3-12 アラーム連動パラメータの変更

Table 3-2 Alarm Linkage パラメータの説明

パラメータ	説明
アラーム入力	値を変更することはできません。デフォルトのままです。
名前	ゾーン名を入力します。
アラーム入力タイプ	購入した警報機器の警報入力タイプが NO の場合は NO を、それ以外の場合は NC を選択してください。
ファイアーリンク有効	<p>ファイアーリンクが有効になっている場合、アクセスコントローラーは火災警報が発生するとアラームを出力します。アラームの詳細はアラームログに表示されます。</p> <p></p> <p>ファイアー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。</p>

パラメータ	説明
アクセスリンク有効	有効にすると、アクセスコントローラは、入力されたアラーム信号があるときに、通常オンまたは通常クローズになります。
チャンネルタイプ	2つの選択肢があります。NO と NC です。

Step 4 良をクリックすると設定が完了します。



アクセスコントローラをクライアントに追加すると、Web 上の設定がクライアントの設定と同期します。

3.5.2 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ースで確認できます。

Step 1 Web インターフェースにログインします。

Step 2 「アラームリンク」 → 「アラームログ」を選択します。

Figure 3-13 アラームログ



Step 3 時間範囲とアラームの種類（タイプ）を選択して、「照会」をクリックします。
照会結果が表示されます。

Figure 3-14 検索結果

No.	イベントコード	時間
1	脅迫	2021-07-20 11:27:36
2	脅迫	2021-07-20 11:27:31

3.6 トークバック設定

アクセスコントローラーは、ドアステーション（VTO）として動作し、他の機器を呼び出すことができます。

3.6.1 SIP サーバー

Web 上では、ドアステーションとインドアステーションを SIP サーバーに追加して、相互に会話できるようにします。SIP サーバーは、アクセスコントローラーや他のドアステーションでも構いません。



アクセスコントローラーが SIP サーバーとして機能する場合は、他のアクセスコントローラーと屋内モニター（VTH）を合わせて最大 50 台まで接続することができます。

3.6.1.1 SIP サーバーとしてのアクセスコントローラー

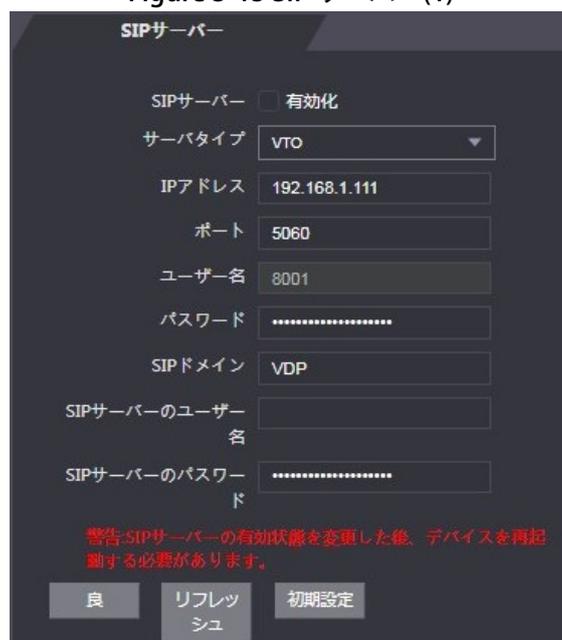
Step 1 Web インターフェースにログインします。

Step 2 「トークバック設定」→「SIP サーバー」を選択します。

Step 3 「SIP サーバー」の有効化にチェックを入れ、「良」をクリックします。

アクセスコントローラーが再起動します。

Figure 3-15 SIP サーバー(1)



SIPサーバー

SIPサーバー 有効化

サーバタイプ VTO

IPアドレス 192.168.1.111

ポート 5060

ユーザー名 8001

パスワード

SIPドメイン VDP

SIPサーバーのユーザー名

SIPサーバーのパスワード

警告:SIPサーバーの有効状態を変更した後、デバイスを再起動する必要があります。

良 リフレッシュ 初期設定

3.6.1.2 SIP サーバーとしての他のデバイス

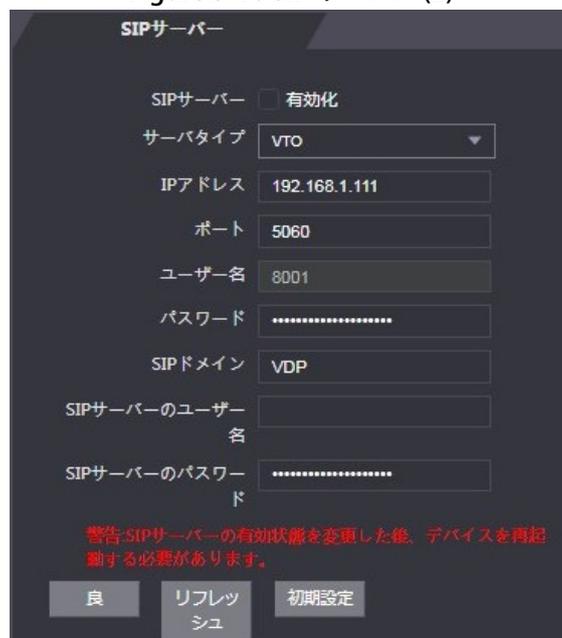
Step 1 Web インターフェースにログインします。

Step 2 「トークバック設定」→「SIP サーバー」を選択します。

Step 3 SIP サーバーを無効（チェックを外す）にして、サーバタイプを VTO に設定します。

Step 4 パラメータの設定をします。

Figure 3-16 SIP サーバー(2)



SIPサーバー

SIPサーバー 有効化

サーバタイプ VTO

IPアドレス 192.168.1.111

ポート 5060

ユーザー名 8001

パスワード

SIPドメイン VDP

SIPサーバーのユーザー名

SIPサーバーのパスワード

警告:SIPサーバーの有効状態を変更した後、デバイスを再起動する必要があります。

良 リフレッシュ 初期設定

Table 3-3 SIP サーバーのパラメータ説明(1)

パラメータ	説明
IP アドレス	SIP サーバーとして動作する VTO の IP アドレス。
ポート	デフォルトでは 5060 です。
ユーザー名	初期値のままです。
パスワード	
SIP ドメイン	VDP であること。
SIP サーバー のユーザー名	SIP サーバーのログインユーザー名とパスワード。
SIP サーバー のパスワード	

Step 5 「良」をクリックします。

3.6.2 ローカル構成

デバイスの種類と番号を設定します。

3.6.2.1 SIP サーバーとしてのアクセスコントローラー

Step 1 Web インターフェースにログインします。

Step 2 トークバック設定 > ローカルを選択します。

Step 3 パラメータを設定します。

Figure 3-17 ローカル(1)

Table 3-4 SIP パラメータの説明

パラメータ	説明
デバイスタイプ	アクセスコントローラーはユニット VTO としてのみ動作します。
グループ通話番号	管理センターの番号を入力します。最大 9 桁の数字を入力できます。

パラメータ	説明
VTO 番号	アクセスコントローラーが SIP サーバーとして動作している場合は設定できません。
グループコール	有効にすると、アクセスコントローラーがメイン VTH を呼び出しているときに、すべてのサブ VTH も呼び出しを受けます。  この機能は、アクセスコントローラーが SIP サーバーとして動作している場合のみ使用できます。
送信モード	<ul style="list-style-type: none"> ● モード 1 リアルタイムでの通話が可能ですが、ネットワーク環境が悪いと映像や音声が遅延することがあります。 ● モード 2 リアルタイム通話ではありませんが、スムーズな映像と音声を確保します。

Step 4 確認をクリックします。

3.6.2.2 SIP サーバーとしての他のデバイス

Step 1 Web インターフェイスにログインします。

Step 2 トークバック設定 > ローカルを選択します。

Step 3 パラメータを設定します。

Figure 3-18 ローカル(2)



Table 3-5 パラメータの説明

パラメータ	説明
デバイスタイプ	アクセスコントローラーは、ユニットドアステーションやフェンスステーションとして機能します。
グループ通話番号	管理センターの番号を入力してください。最大 9 桁の数字を入力できます。
VTO 番号	数字を設定します。  ● 4 桁の数字でなければなりません。最初の 2 つは 80 で、最後の 2 つは 8001 のように 01 で始まります。

パラメータ	説明
	<ul style="list-style-type: none"> ● 複数のVTOが存在する場合、それらのVTO番号を同じにすることはできません。
伝送モード	<ul style="list-style-type: none"> ● モード1 リアルタイムで通話ができますが、ネットワーク環境が悪いと映像や音声が遅れます。 ● モード2 リアルタイム通話ではありませんが、スムーズな映像と音声を確保します。

3.6.3 VTO 番号管理

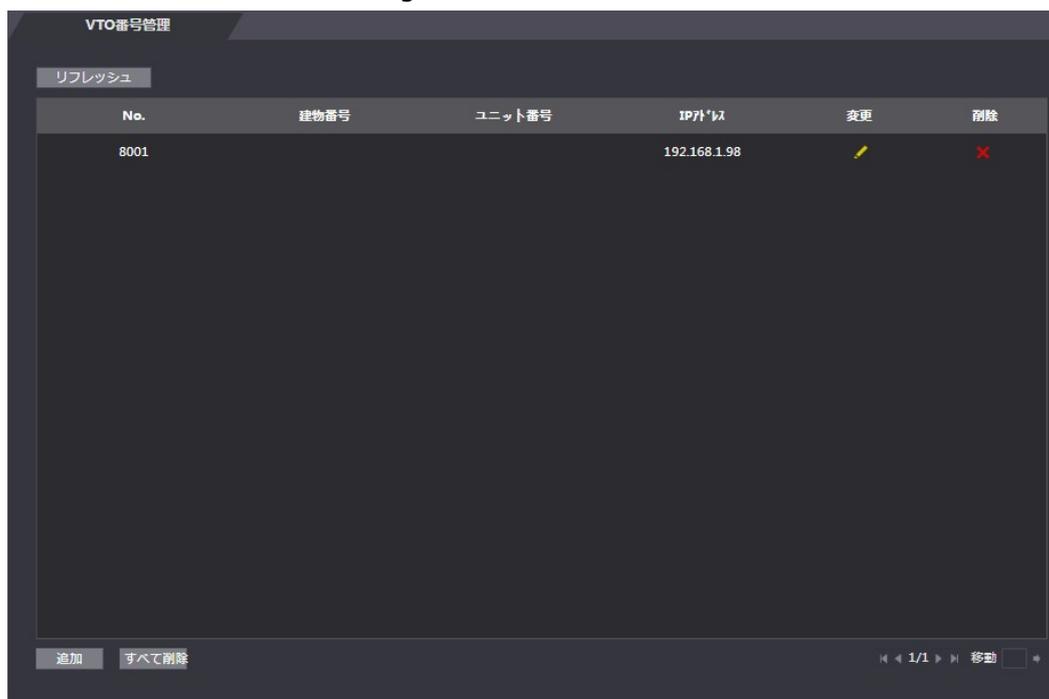
アクセスコントローラーが SIP サーバーとして動作する場合は、他の VTO を追加して呼び出します。

Step 1 Web インターフェースにログインします。

Step 2 トークバック設定 > VTO 番号管理を選択します。

Step 3 「追加」をクリックします。

Figure 3-19 VTO 番号管理



Step 4 パラメータを設定します。

Figure 3-20 ドアステーションの追加

Table 3-6 パラメータの説明

パラメータ	説明
登録番号	追加したいVTOの番号を入力します。
登録パスワード	デフォルトのままでいい。
建物番号	設定できません。
ユニット番号	
IPアドレス	追加したいVTOのIPアドレス。
ユーザー名	追加するVTOのWebインターフェースのログインユーザー名とパスワード。
パスワード	

Step 5 良をクリックします。

3.6.4 VTH 番号管理

アクセスコントローラーが SIP サーバーとして動作する場合は、VTH を追加して呼び出します。



メイン VTH とサブ VTH がある場合は、グループコール機能を有効にしてから追加する必要があります。3.6.2.1 SIP サーバーとしてのアクセスコントローラー」を参照してください。

3.6.4.1 VTH を一つずつ追加

Step 1 Web インターフェースにログインします。

Step 2 トークバック設定 > ルーム番号管理を選択します。

Step 3 「追加」をクリックします。

Figure 3-21 部屋番号管理



Step 4 情報を入力してください。

Figure 3-22 VTH を 1 つ追加

Table 3-7 パラメータの説明

パラメータ	説明
名前	他の VTH と区別するための設定。
姓名	
ニックネーム	
ルーム番号	VTH の部屋番号  <ul style="list-style-type: none"> ● 5桁までの数字で、室内モニターで設定したものと同じである必要があります。 ● メイン VTH とサブ VTH がある場合、メイン VTH の部屋番号の末尾は「-0」、サブ VTH の部屋番号の末尾は「-1」、「-2」、「-3」... とします。
登録タイプ	デフォルトのままです。
登録パスワード	

Step 5 良をクリックします。



エクスポートをクリックすると、部屋番号をエクスポートして、他のデバイスにインポートすることができます。

3.6.4.2 VTHを一括して追加

VTH は最大 1024 個まで追加できます。

Step 1 Web インターフェースにログインします。

Step 2 トークバック設定 > ルーム番号管理を選択します。

Step 3 建物の全階数、一層の部屋数、1 階の番号、2 階の番号を設定します。

Step 4 「追加」をクリックします。

Figure 3-23 屋内モニターを一括で追加



3.6.5 VTS マネジメント

アクセスコントローラーが SIP サーバーとして動作する場合は、マスターステーション (VTS) を追加して呼び出します。

Step 1 Web インターフェースにログインします。

Step 2 トークバック設定 > VTS 番号管理を選択します。

Step 3 「追加」をクリックします。

Figure 3-24 管理デバイスの追加

Step 4 情報を入力してください。

- **VTS 番号**：最大 9 桁の数字を入力できます。
- **登録パスワード**：デフォルトのままでもいいです。
- **IP アドレス**：VTS の IP アドレス。

Step 5 良をクリックします。

関連操作

-  : VTS の情報を変更する。
-  : VTS の削除。

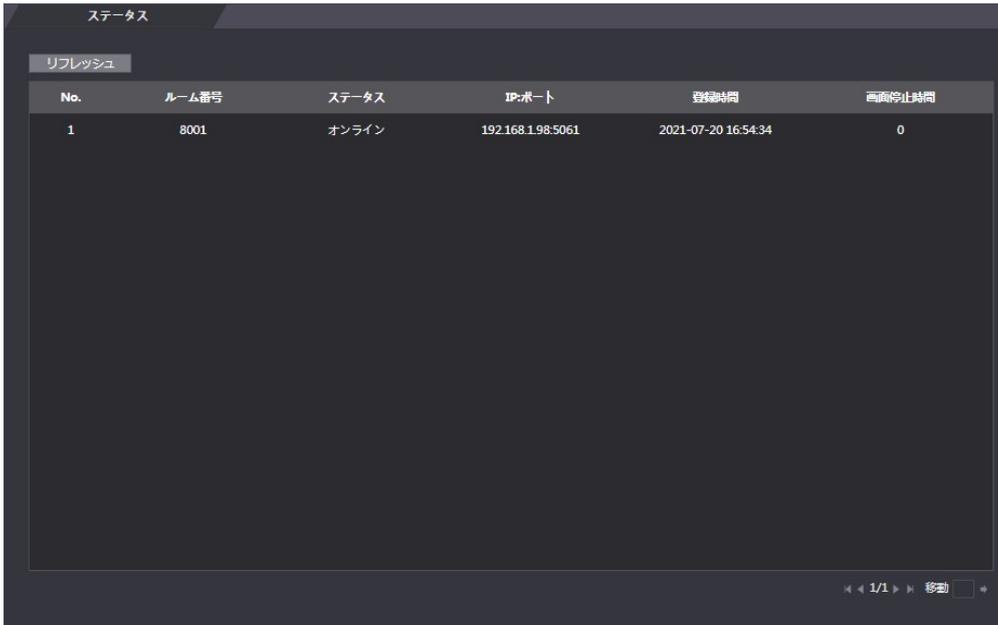
3.6.6 オンラインステータス

アクセスコントローラーが SIP サーバーとして動作している場合、管理者は Web インターフェースにログインしてオンライン機器の情報を確認することができます。

Step 1 ウェブにログインします。

Step 2 トークバック設定>ステータスを選択します。

Figure 3-25 ステータス



No.	ルーム番号	ステータス	IP:ポート	登録時間	画面停止時間
1	8001	オンライン	192.168.198:5061	2021-07-20 16:54:34	0

3.6.7 通話ログ

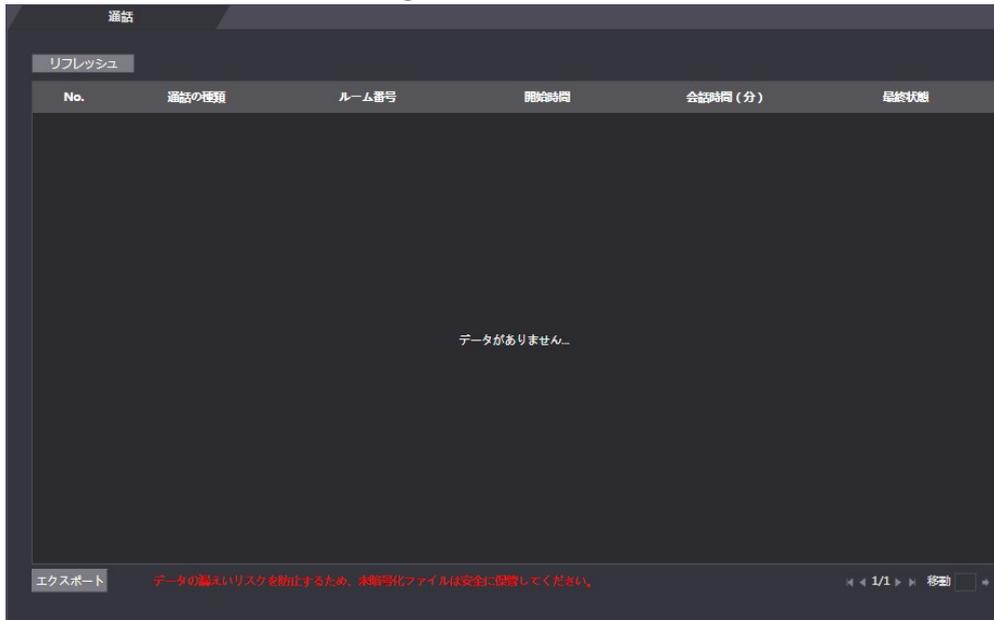
通話履歴は最大 1024 件まで確認できます。

Step 1 Web インターフェースにログインします。

Step 2 トークバック設定>通話を選択します。

Step 3 (オプション) 「データのエクスポート」をクリックすると、すべてのログがエクスポートされます。

Figure 3-26 通話ログ



3.7 タイムセクション

時間帯や休日の計画を設定し、ユーザーがいつドアを開ける権限を持つかを定義することができます。

3.7.1 時間を設定するセクション

ユーザーが一日にいつドアを開けることができるかを設定します。

Step 1 Web インターフェースにログインします。

Step 2 **時間セクション**>**時間セクション**を選択します。

Figure 3-27 時間セクション

Step 3 タイムセクションの番号と名前を入力します。

Step 4 日ごとに期間を設定します。最大で4つの期間を設定できます。

Step 5 (オプション) 「週全体に適用」をクリックすると、設定が他の日にもコピーされます。

Step 6 OKをクリックします。

3.7.2 ホリデーグループの設定

ホリデープランを設定する前に、ホリデーグループを設定する必要があります。

Step 1 Web インターフェースにログインします。

Step 2 時間セクション>休日ホリデーグループを選択します。

Step 3 「良」をクリックします。

Figure 3-28 ホリデーグループの追加

No.	休日名	開始時刻	終了時刻	変更	削除
データがありません...					

Step 4 ホリデーグループの番号と名前を入力します。

Step 5 「良」をクリックします。

Figure 3-29 ホリデーグループの追加

休日名	
時間セクション	2021-07-21 - 2021-07-22

Step 6 休日の名前を入力し、開始日と終了日を選択して、「OK」をクリックします。



1つの休日グループに複数の祝日を追加することができます。

Step 7 良をクリックします。

3.7.3 ホリデーグループの設定

ホリデープランを設定します。アクセスコントローラーにユーザーを追加する際に、ホリデープランを選択すると、ユーザーはホリデープランで定義された日の中でのみドアを開けることができます。

Step 1 Web インターフェイスにログインします。

Step 2 時間セクション> 休日プランの設定を選択します。

Step 3 「追加」をクリックします。

Figure 3-30 ホリデーグループの追加

Step 4 ホリデープランの番号と名前を入力します。

Step 5 設定したホリデーグループの番号を選択します。



ホリデーグループを選択しない場合は、255 を選択します。

Step 6 選択したホリデーグループのすべての日に期間を設定します。最大で4つの期間を設定できます。

Step 7 良をクリックします。

3.8 データ容量

アクセスコントローラーが保存できるユーザー、カード、指紋、顔画像の数は、「データ容量」インターフェースで確認できます。

Step 1 Web インターフェースにログインします。

Step 2 ナビゲーションバーの「データ容量」を選択します。

3.9 ビデオ設定

データレート、画像パラメータ（輝度、コントラスト、色相、彩度など）、露出などのパラメータは、**動画の設定**インターフェースで設定できます。

3.9.1 データレート

チャンネル1のストリームパラメータを設定することができます。

Step 1 Web インターフェースにログインします。

Step 2 「動画の設定」→「動画の設定」→「レート」を選択します。

Figure 3-31 データレート



Table 3-8 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	お住まいの地域の映像規格に合わせて、NTSCまたはPALを選択してください。
チャンネルID	選択肢は2つあります。1は白色光カメラ、2はIR光カメラです。

パラメータ		説明
音声収集		有効にすると、他の機器がアクセスコントローラーからビデオストリームを引き出す際に、オーディオストリームも受け取るようになります。
メインフォーマット	動画リスト	ご希望の画質に合わせて、D1、VGA、720p、1080p を選択してください。
	フレームレート	ディスプレイ上に連続したフレームが表示される速度のこと。フレームレートの範囲は1~30fps です。
	ビットレート	単位時間あたりに搬送または処理されるビット数のこと。5つの選択肢があります。2Mbps、4Mbps、6Mbps、8Mbps、10Mbpsの5種類。
エクストラフォーマット	ビデオフォーマット	3つの選択肢があります。D1」「VGA」「QVGA」の3種類です。

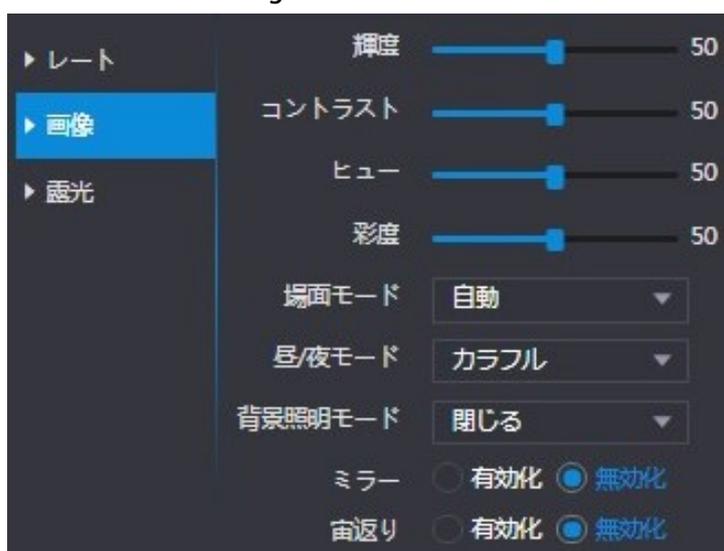
3.9.2 イメージ

2つのチャンネルがあり、それぞれのチャンネルにパラメータを設定する必要があります。

Step 1 Web インターフェースにログインします。

Step 2 「動画の設定」 → 「動画の設定」 → 「画像」を選択します。

Figure 3-32 イメージ



Step 3 背景照明モードで「ワイドダイナミック」を選択。

Table 3-9 画像パラメータの説明

パラメータ	説明
輝度	この値が大きいほど、画像は明るくなります。
コントラスト	コントラストとは、物体を識別するための輝度や色の差のことです。コントラストの値が大きければ大きいほど、輝度や色のコントラストが強くなります。
ヒュー（色相）	色合いが変化します。：値小（緑）←→値大（赤）
彩度	色の濃さが変化します。
場面モード	<ul style="list-style-type: none"> ● 閉じる：モードなし ● オート：システムがシーンモードを自動調整します。 ● 晴天：このモードでは、画像の色合いが減少します。 ● 夜間：このモードでは、画像の色合いが強調されます。 <p> 初期設定では自動が選択されています。</p>
昼/夜モード	<p>フィルライトの動作状態を決定します。</p> <ul style="list-style-type: none"> ● 自動：昼間/夜間のモードを自動的に調整してくれます。 ● カラフル：このモードでは、画像に色がつきます。 ● 白黒：このモードでは、画像が白黒になります。
背景照明モード	<ul style="list-style-type: none"> ● 閉じる：バックライト補正なし ● 逆光：逆光補正とは、光量が極端に多い領域や少ない領域を補正して、ピントを合わせたときに正常な光量になるようにすることです。 ● ワイドダイナミック：ワイドダイナミックレンジモードでは、明るい部分を暗くし、暗い部分を補正することで、明るい部分と暗い部分の被写体の鮮明さを確保します。 <p> 人の顔が逆光になるときは、WDRを有効にする必要があります。</p> <ul style="list-style-type: none"> ● 抑制：ハイライト補正は、ハイライト部分の露出オーバーや、スポットライト、ヘッドライト、ポーチライトなどの強い光源を補正して、明るい光に負けない使い勝手の良い画像を作るために必要です。
ミラー	この機能を有効にすると、画像は左右が反転して表示されます。
宙返り	この機能を有効にすると、画像を裏返して表示することができます。

3.9.3 露光

露光のパラメータを設定することができます。

Step 1 Web インターフェースにログインします。

Step 2 「動画の設定」 → 「動画の設定」 → 「露光」を選択します。

Figure 3-33 露出



Table 3-10 露光パラメータの説明

パラメータ	説明
明滅防止 (アンチフリッカー)	<ul style="list-style-type: none"> ● 50Hz：商用周波数が 50Hz の場合。 ● 60Hz：商用周波数が 60Hz の場合。 ● 屋外：露光モードを切り替えることができます。
露光モード	<ul style="list-style-type: none"> ● 自動：アクセスコントローラーが画像の明るさを自動的に調整します。 ● シャッター優先：アクセスコントローラーは、シャッター露出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た場合、アクセスコントローラーは理想的な明るさを得るためにゲイン値を自動的に調整します。 ● 手動：ゲインとシャッター値を手動で設定し、画像の明るさを調整することができます。 <p></p> <ul style="list-style-type: none"> ● 明滅防止の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」を選択することができます。 ● 下記の露出モードは参考値であり、機種によって異なる場合があります。

パラメータ	説明
シャッター	カスタムレンジを選択すると、シャッターの速度範囲をカスタマイズすることができます。 シャッタースピードを遅くすると、露光時間が短くなり、画像が暗くなります。
ゲイン	ゲイン値の範囲を設定すると、映像品質が向上します。
露出補正	露出補正值を調整することで、動画の輝度を上げることができます。
3D NR	3D ノイズリダクションを有効にすると、映像のノイズが低減され、高精細な映像が得られます。
等級	3D NR が有効になっているときに、3D NR の値を調整できる。 この値が大きいほど、ノイズが少なくなります。

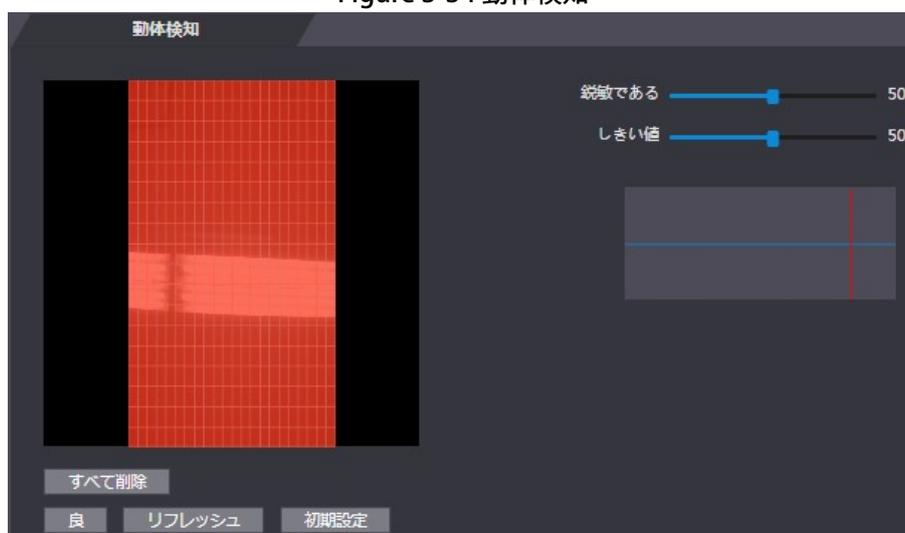
3.9.4 動体検知

動体を検出できる範囲を設定します。

Step 1 Web インターフェースにログインします。

Step 2 「動画の設定」→「動体検知」を選択します。

Figure 3-34 動体検知

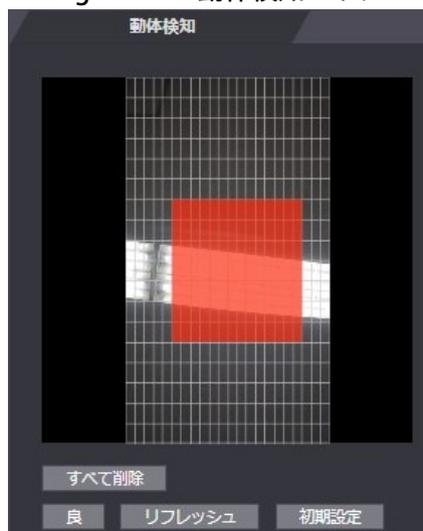


Step 3 マウスの左ボタンを押したまま、赤い部分でマウスをドラッグします。



- 赤色が動体検出エリアです。デフォルトの動き検出範囲は、すべての部分です。
- 動体検出エリアを描くには、まず「すべて削除」をクリックする必要があります。
- デフォルトの動体検出エリアに描いた場合、描いたエリアは非動体検出エリアになります。

Figure 3-35 動体検知エリア



Step 4 感度と閾値を設定します。



- 感度とは、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いことになります。
- しきい値とは、動体検出の条件です。グリッド番号がしきい値に達すると、動き検出がトリガーされます。値が小さいほど、動き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のラインが表示され、グリッド番号がしきい値より大きい場合は赤のラインが表示されます。Figure 3-34 を参照してください。

Step 5 良をクリックして設定を終了します。

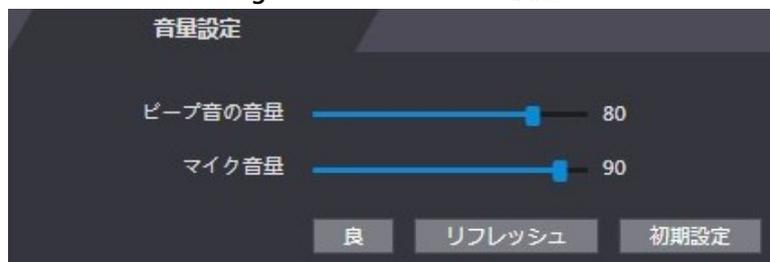
3.9.5 ボリューム設定

スピーカーやビープ音の音量を調整してください。

Step 1 Web インターフェースにログインします。

Step 2 「動画の設定」 → 「音量設定」を選択します。

Figure 3-36 ボリューム設定



3.9.6 イメージモード

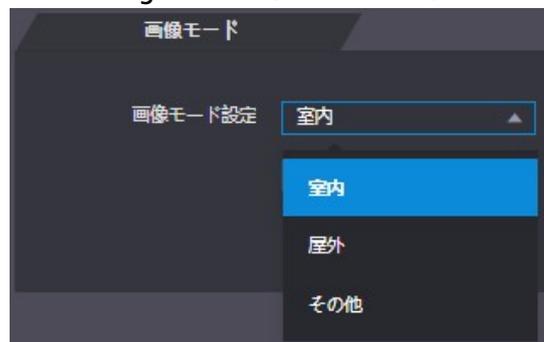
アクセスコントローラーが設置されている場所に合わせて、インドア、アウトドア、その他を選択します。

Step 1 Web インターフェイスにログインします。

Step 2 「動画の設定」→「画像モード」を選択します。

- 屋内：アクセスコントローラーが屋内に設置されていること。
- 屋外：アクセスコントローラーが屋外に設置されている。
- その他：廊下などの照明がある場所にアクセスコントローラーを設置。

Figure 3-37 イメージモード



3.9.7 ローカルコーディング

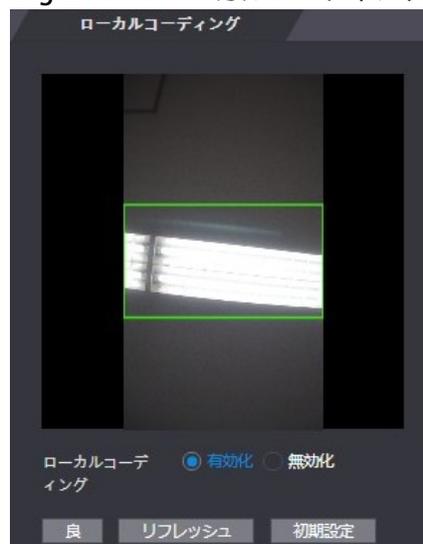
室内モニターに表示するエリアを設定します。

Step 1 Web インターフェイスにログインします。

Step 2 「動画の設定 > ローカルコーディング」を選択します。

Step 3 機能を有効にします。

Figure 3-38 ローカルコーディング



Step 4 OK クリックします。

3.10 顔検出

このインターフェースでは、顔認識の精度を高めるために、人の顔に関するパラメータを設定することができます。

Step 1 Web インターフェースにログインします。

Step 2 「顔検出」を選択します。

Figure 3-39 顔検出



Step 3 パラメータの設定を行います。

Table 3-11 顔検出パラメータの説明

パラメータ	説明
顔認識閾値	この値が大きいくほど、精度が高くなります。
顔認識の最大角度	角度が大きいくほど、より広い範囲のプロファイルを認識することができます。
偽造防止有効	顔画像やモデルを使ったロック解除を防ぐ機能です。
赤外線	スクロールバーをドラッグして、IRの明るさを調整します。
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	無効な顔認識時のプロンプトの間隔。
瞳孔間距離	瞳孔距離とは、両眼の瞳孔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ーが必要に応じて顔を認識するためには、適切な値を設定する必要があります。この値は、顔の大きさや、顔とレンズの距離によって変化します。顔とレンズの距離が近いほど、値を大きくする必要があります。大人がレンズから1.5メートル離れている場合、瞳孔距離の値は50~70以内に収まります。
チャンネルID	選択肢は2つあります。1は白色光カメラ、2はIR光カメラです。
顔露光を有効にする	有効にすると、アクセスコントローラーが屋外に設置されている場合、人間の顔が鮮明になります。
顔ターゲットの輝度	初期値は50です。必要に応じて明るさを調整してください。
顔露光間隔検出時間	顔を検出した後、アクセスコントローラーは顔を照らすために発光し、設定した間隔が経過するまで再び発光することはありません。
温度測定	温度モニター機能の有効・無効を選択します。
温度単位	「℃」または「F」を選択してください。
測温エリア枠	待機中のインターフェースに温度モニターボックスを表示するかどうかを設定します。
温度補正時間(ms)	温度を監視する場合、アクセスコントローラーはこのパラメータで定義された時間後に温度値を取得します。  このパラメータは、一部のモデルでのみサポートされています。
測温距離 (cm)	初期設定では50です。設定した距離に応じて、必要に応じてモニター温度を補正することができます。  このパラメータは、一部のモデルでのみサポートされています。

パラメータ	説明
温度設定値	温度の閾値を設定します。モニター体温が設定値以上の場合、高温と判断します。
高温 低温	必要な温度範囲を設定します。モニター温度が下限値より低い場合は、温度が低すぎることを促し、上限値より高い場合は、機能を妨げる熱源があることを促します。
温度校正值	このパラメータはテスト用です。温度モニター環境の違いにより、モニター温度と実際の温度に誤差が生じる場合があります。テスト用に複数のモニターサンプルを選択し、モニター温度と実際の温度の比較に応じて、このパラメータで温度偏差を補正することができます。例えば、モニター温度が実際の温度よりも0.5℃低い場合、補正值は0.5℃に設定され、モニター温度が実際の温度よりも0.5℃高い場合、補正值は-0.5℃に設定されます。
温度監視モード	<ul style="list-style-type: none"> ● オート：顔のヒートマップを使って顔認識を行います。ヒートマップが見つからない場合は、自動的にキャリブレーションモードに切り替わります。 ● サーマル：顔認識と温度監視にヒートマップのみを使用。 ● 標定：顔の白色光画像を使用して顔認識を行い、顔のヒートマップ上の座標を抽出して適用し、温度モニタリングを行う。 <p> このパラメータは、一部のモデルでのみサポートされています。</p>
サーモディスプレイ	<p>左上にヒートマップを表示します。</p> <p> このパラメータは、一部のモデルでのみサポートされています。</p>
マスクモデル	<ul style="list-style-type: none"> ● テストなし：顔認識時にマスクを検出しません。 ● マスク注意：顔認識時にマスクを検出します。 マスクを着用していない人物が検出された場合、システムはマスク着用を促し、通行が許可されます。 ● マスク阻止：顔認識時にマスクを検出します。 マスクを着用していない人物が検出された場合、システムはマスク着用を促し、通過は許可されません。

パラメータ	説明
ターゲットフィルター	「目標を描く」をクリックすると、最小の顔検出フレームが描画されます。 「すべて削除」をクリックすると、描いたフレームをすべて削除することができます。
検知領域	「検知領域」をクリックしてマウスを動かすと、顔検出領域を調整することができます。 「すべて削除」をクリックすると、すべての検出領域が削除されます。

Step 5 良をクリックして設定を終了します。

3.11 ネットワーク設定

3.11.1 TCP/IP

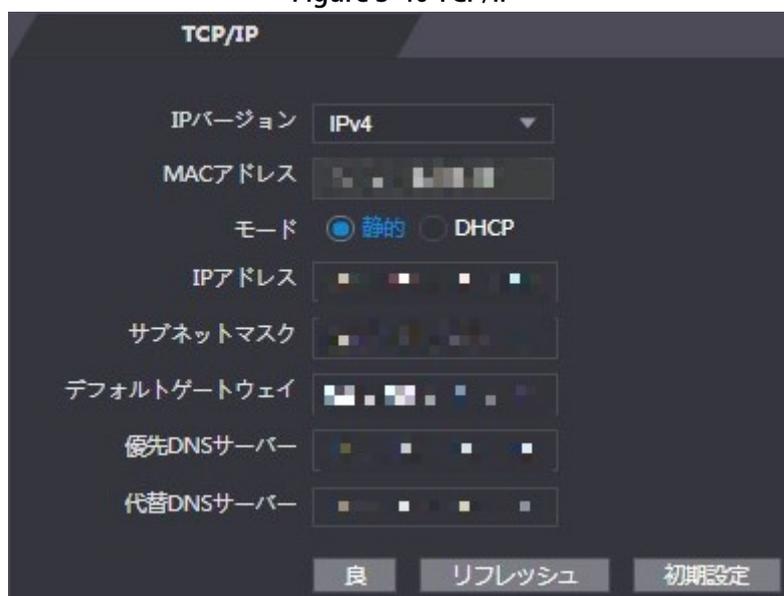
アクセスコントローラーが他の機器と通信できるように、IPアドレスとDNSサーバーを設定する必要があります。

アクセスコントローラーがネットワークに正しく接続されているか確認してください。

Step 1 Web インターフェイスにログインします。

Step 2 ネットワークの設定>TCP/IP を選択します。

Figure 3-40 TCP/IP



Step 3 パラメータの設定をします。

Table 3-12 TCP/IP

パラメータ	説明
IPバージョン	選択肢はIPv4のみです。
MACアドレス	アクセスコントローラーのMACアドレス（有線LAN）です。
モード	<ul style="list-style-type: none"> ● 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：自動設定 <ul style="list-style-type: none"> ・ DHCPを有効にすると、IPアドレス、サブネットマスク、ゲートウェイアドレスの設定ができなくなります。 ・ DHCPが有効な場合は、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、DHCPが有効でない場合は、IPアドレス、サブネットマスク、ゲートウェイアドレスがすべて0になります。 ・ DHCPが有効なときにデフォルトIPを確認したい場合は、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	IPバージョンでIPv6を選択した場合のみ有効です。各ローカルエリアネットワークのネットワークインターフェースコントローラーに固有のリンクローカルアドレスが割り当てられ、通信が可能になります。リンクローカルアドレスの変更はできません。
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/代替DNSサーバー	優先/代替するDNSサーバーのIPアドレスを設定します。

Step 4 良をクリックすると設定が完了します。

3.11.2 ポート

アクセスコントローラーが接続できる最大の接続クライアントとポート番号を設定します。

Step 1 Web インターフェースにログインします。

Step 2 「ネットワークの設定」→「ポート」を選択します。

Step 3 ポート番号の設定を行います。次の表を参照してください。



最大接続を除き、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ーを再起動する必要があります。

Table 3-13 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ー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	初期値は 37777 です。
HTTP ポート	デフォルト値は 80 です。他のポート番号を使用している場合は、ブラウザ機能でログインする際に、アドレスの後ろにこの値を追加する必要があります。
HTTPS ポート	既定値は 443 です。
RTSP ポート	初期値は 554 です。

Step 4 良をクリックすると設定が完了します。

3.11.3 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ーはユーザーが指定したサーバーにアドレスを報告し、クライアントがアクセスコントローラーにアクセスできるようになります。

Step 1 Web インターフェースにログインします。

Step 2 「ネットワークの設定」→「登録」を選択します。

Step 3 「有効化」にチェックを入れ、ホスト IP、ポート、サブデバイス ID を入力します。

Table 3-14 オートレジスタの説明

パラメータ	説明
ホスト IP	サーバーの IP アドレスまたはサーバーのドメイン名。
ポート	自動登録に使用するサーバーポート。
サブデバイス ID	サーバーから割り当てられたアクセスコントローラー ID。

Step 4 良をクリックすると設定が完了します。

3.11.4 P2P

ピア・ツー・ピア・コンピューティングやネットワーキングは、タスクやワークロードを複数のピアに分割する分散型アプリケーション・アーキテクチャです。ユーザーはQRコードを読み取ってモバイルアプリケーションをダウンロードし、アカウントを登録することで、複数のアクセスコントローラーをモバイルアプリケーション上で管理することができます。ダイナミックドメイン名の適用やポートマッピング、トランジットサーバーは必要ありません。

 P2Pを使用する場合は、アクセスコントローラーを外部ネットワークに接続する必要があります。

Figure 3-41 P2P



Step 1 Web インターフェースにログインします。

Step 2 「ネットワークの設定」→「P2P」を選択します。

Step 3 P2P 機能を有効にするには**有効化**を選択します。

Step 4 **良**をクリックします。

 Web インターフェースでQRコードを読み取ると、アクセスコントローラーのシリアルナンバーが表示されます。

3.12 安全管理

3.12.1 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。

Figure 3-42 オーソリティ



3.12.2 システム

3.12.2.1 システムサービス

必要に応じて、システムサービスを有効または無効にしてください。



Web インターフェイス上のシステムサービスの設定は、アクセスコントローラーの特徴一プライバシー設定画面に同期されます。

Figure 3-43 システムサービス

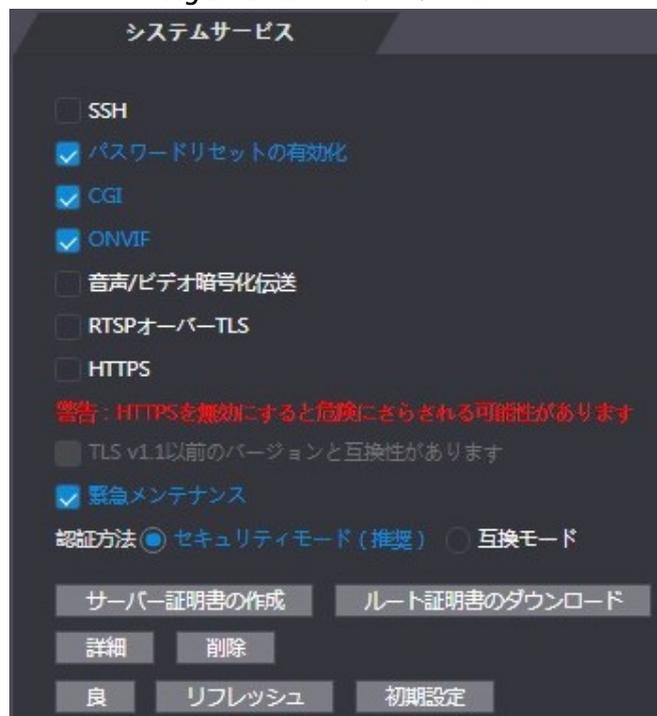


Table 3-15 システムサービスの説明

パラメータ	説明
SSH	Secure Shell (SSH) は、安全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操作するための暗号化ネットワークプロトコルです。 SSHを有効にすると、データ送信時にSSHによる暗号化サービスが行われます。
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することができます。この機能はデフォルトで有効になっています。
CGI	CGI (Common Gateway Interface) は、Web ページを動的に生成するサーバー上で動作するコンソールアプリケーションと同様に、Web サーバプログラムを実行するための標準プロトコルを提供します。 CGIを有効にすると、CGI コマンドが使用できるようになります。初期設定では CGI が有効になっています。
ONVIF	ONVIF プロトコルにより、他の機器が VTO のビデオストリームを引き出せるようにする。
音声・映像伝送の暗号化	音声通話やビデオ通話中のすべてのデータを暗号化することができます。
RTSP over TLS	暗号化されたビットストリームを RTSP で出力。
HTTPS	HTTPS (Hypertext Transfer Protocol Secure) は、コンピュータネットワーク上で安全な通信を行うためのプロトコルです。 HTTPS が有効な場合は、CGI コマンドへのアクセスに HTTPS が使用され、そうでない場合は HTTP が使用されます。  HTTPS を有効にすると、アクセスコントローラーは自動的に再起動します。
TLSv1.1 以前のバージョンに対応	お使いのブラウザが TLS V1.1 以前のバージョンを使用している場合は、この機能を有効にしてください。 ※設定不可
緊急メンテナンス	故障解析や修理に有効です。 この関数は、8088 と 8087 のポートを占有します。

パラメータ	説明
認証方法	<ul style="list-style-type: none"> ● セキュリティモード（推奨）。Digest 認証でのログインに対応。 ● 互換モードです。旧来のログイン方法を使用します。

3.12.2.2 サーバー証明書の作成

「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て「良」をクリックすると、アクセスコントローラーが再起動します。

3.12.2.3 ルート証明書のダウンロード

Step 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。

Step 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する。

画面上の指示に従って、証明書をインストールします。

3.13 ユーザーの管理

3.13.1 ユーザーの追加

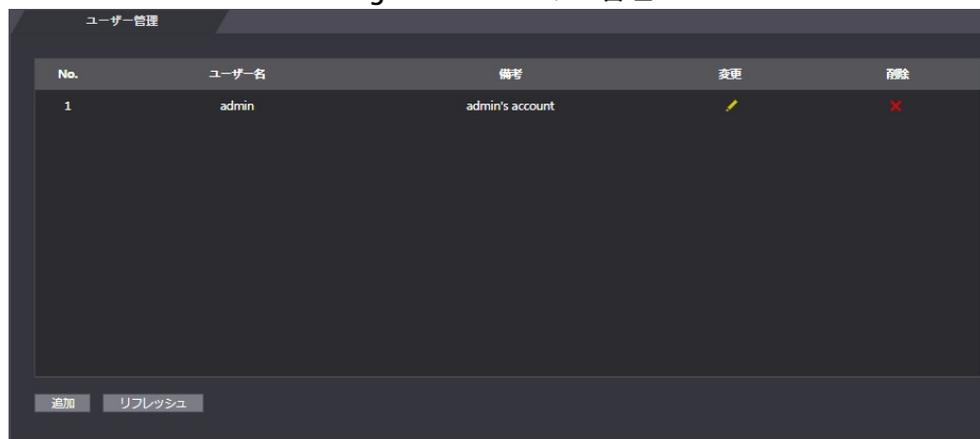
ユーザー追加するには、ユーザー管理インターフェースの追加をクリックし、ユーザー名、パスワード、パスワード確認、および備考を入力します。「良」をクリックすると、ユーザーの追加が完了します。

3.13.2 ユーザー情報の変更

ユーザー管理インターフェースの変更  をクリックすると、ユーザー情報を修正することができます。

 アクセスコントローラー初期設定時に設定した管理者の修正は No.1 のユーザーで行えます。
(メールアドレス、パスワード変更)

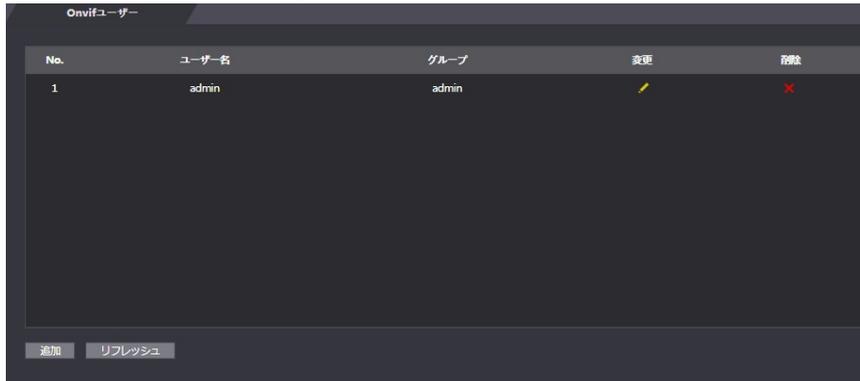
Figure 3-44 ユーザー管理



3.13.3 ONVIF ユーザー

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な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 が使用されている場合、管理者、オペレーター、ユーザーは ONVIF サーバーの異なる権限を持っています。必要に応じて、ONVIF のユーザーを作成してください。

Figure 3-45 ONVIF ユーザー



3.14 メンテナンス

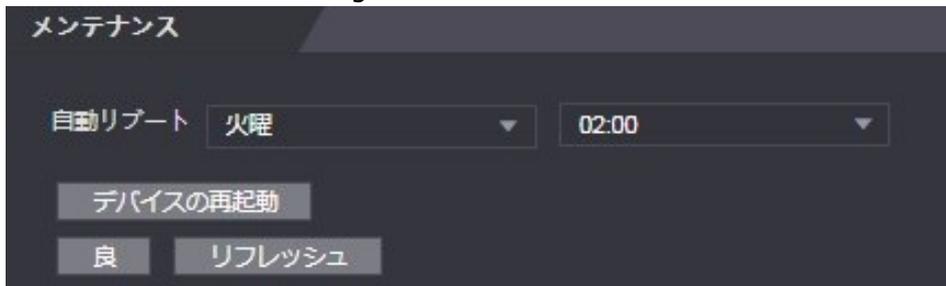
アクセスコントローラの動作速度を向上させるために、アイドル時にアクセスコントローラを自動再起動させることができます。自動再起動の日時を設定する必要があります。

Step 1 Web インターフェースにログインします。

Step 2 「メンテナンス」を選択します。

Step 3 自動再起動の時間を設定して、「良」をクリックします。

Figure 3-46 メンテナンス



例えば、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。

「デバイスの再起動」をクリックすると、アクセスコントローラがすぐに再起動します。

3.15 設定管理

複数のアクセスコントローラーが同じ設定を必要とする場合、設定ファイルをインポートまたはエクスポートすることで、それらのコントローラーに同じパラメータを設定することができます。

3.15.1 設定ファイルのエクスポート

アクセスコントローラーの設定ファイルをエクスポートしてバックアップすることができます。

Step 1 Web インターフェースにログインします。

Step 2 ナビゲーションバーの**設定管理**を選択します。

Figure 3-47 コンフィギュレーション管理



Step 3 設定ファイルをローカルに保存する場合は、「**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ーの IP 情報はエクスポートされません。

3.15.2 設定ファイルの読み込み

アクセスコントローラーからエクスポートした設定ファイルを、同一機種別のアクセスコントローラーにインポートすることができます。

Step 1 Web インターフェースにログインします。

Step 2 ナビゲーションバーの**設定管理**を選択します。

Step 3 設定管理インターフェースで、「**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。

設定ファイルのインポート後、アクセスコントローラーが再起動します。

3.15.3 初期設定

- **出荷時設定の復元（工場出荷時の状態に戻す）**：アクセスコントローラーのすべてのデータと設定をリセットします。
- **出荷時設定の復元（ユーザー & ログの保存）**：ユーザー情報とログを除く、すべてのデータと設定をリセットします。

3.16 アップグレード



- アップグレード前に設定ファイルをエクスポートしてバックアップし、アップグレード完了後にインポートしてください。
- 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。アップグレードファイルは、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の切断、アクセスコントローラーの再起動やシャットダウンは行わないでください。

Step 1 Web インターフェースにログインします。

Step 2 ナビゲーションバーの「更新」を選択します。

Step 3 「ファイルアップグレード」インターフェースで、「検索」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。

Figure 3-48 アップグレード



アップグレードが成功した場合は、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。アップグレードが失敗した場合は、対応するプロンプトが表示されます。



- 「自動確認」を選択すると、自動的にアップグレードが行われます。また、「手動確認」を選択すると、手動でシステムをアップグレードすることができます。
- アップグレード後、アクセスコントローラーは再起動します。
- アップグレード後のバージョンを確認するには、ナビゲーションメニューにある「バージョン情報」をクリックします。

3.17 バージョン情報

MACアドレス、シリアルナンバー、MCUバージョン、Webバージョン、セキュリティベースラインバージョン、システムバージョン、ファームウェアバージョンなどの情報を確認できます。

Step 1 Web インターフェースにログインします。

Step 2 ナビゲーションバーの「バージョン情報」を選択します。

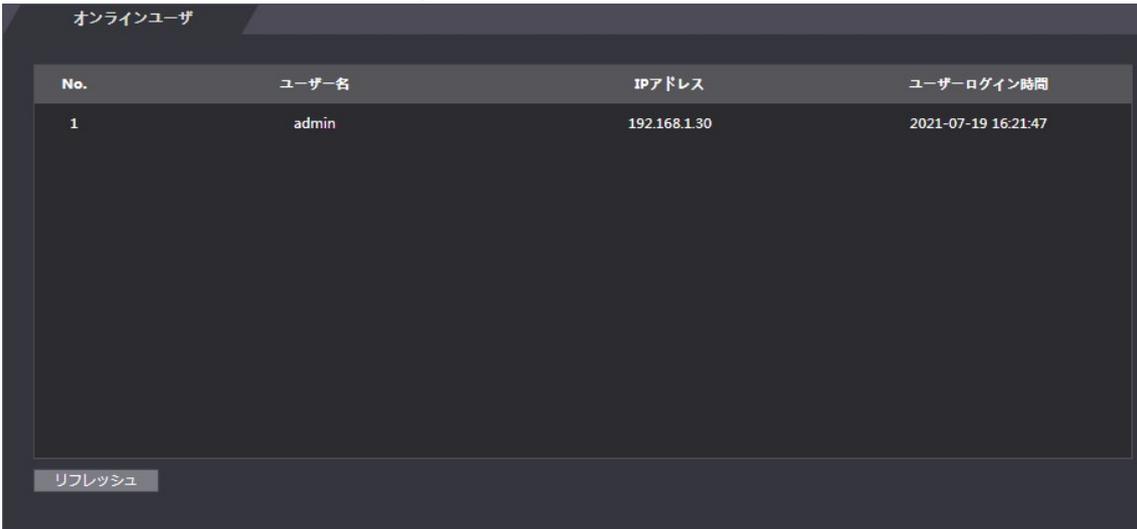
3.18 オンラインユーザー

ユーザー名、IPアドレス、ユーザーのログイン時間は、オンラインユーザーインターフェースで確認できます。

Step 1 Web インターフェースにログインします。

Step 2 ナビゲーションバーの「オンラインユーザ」を選択します。

Figure 3-49 オンラインユーザ



No.	ユーザー名	IPアドレス	ユーザーログイン時間
1	admin	192.168.1.30	2021-07-19 16:21:47

リフレッシュ

3.19 システムログ

システムログ、管理者ログ、ロック解除の記録を閲覧、バックアップすることができます。

3.19.1 システムログ

システムログの閲覧・検索

Step 1 Web インターフェースにログインします。

Step 2 「システムログ」 → 「システムログ」を選択します。

Step 3 時間範囲とタイプを選択して、「照会」をクリックします。

 「バックアップ」をクリックすると、結果をダウンロードできます。

Figure 3-50 ログを照会する



3.19.2 管理者ログ

管理者 ID で管理者ログを検索します。

Step 1 Web インターフェースにログインします。

Step 2 「システムログ」 > 「管理ログ」 を選択します。

Step 3 管理者 ID を入力して、「照会」をクリックします。

Figure 3-51 管理者ログ



3.19.3 アンロック記録

ロック解除の記録を検索し、エクスポートすることができます。

Step 1 Web インターフェースにログインします。

Step 2 「システムログ」 → 「パンチ記録の検索」 を選択します。

Step 3 時間範囲とタイプを選択して、「照会」をクリックします。

Step 4 「エクスポート」をクリックすると、結果をダウンロードできます。

3.20 フュージョン・キャリブレーション

白色光の顔画像と顔面ヒートマップの座標関係を設定します。キャリブレーションモードを有効にすると、アクセスコントローラーはこの座標関係を利用してフェイスヒートマップ上の温度を測定します。

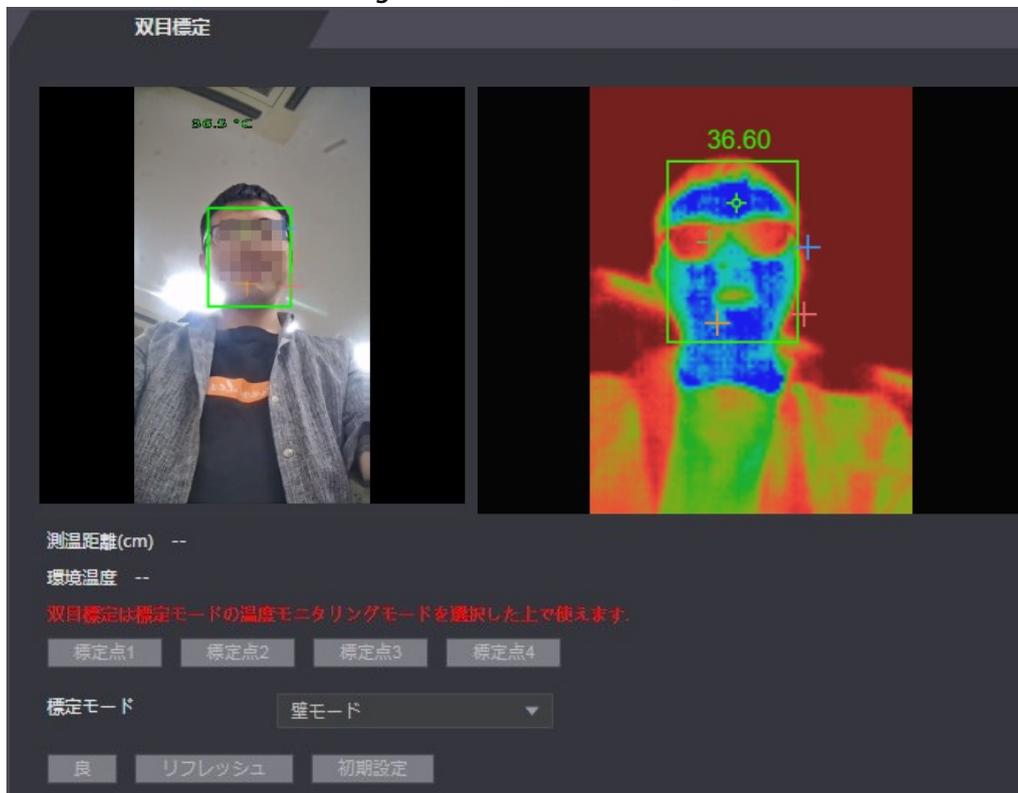


- この機能に対応しているのは一部の機種のみです。
- 「温度監視モード」を「標定モード」に変更します。詳しくは「3.10 顔検出」をご覧ください。

Step 1 「**双目標定**」を選択します。

Step 2 アクセスコントローラーの種類に応じて、**Calibration Mode** から機種を選択します。

Figure 3-52 座標関係の設定



Step 3 「**標定点 1**」をクリックします。

Step 4 左の画像をクリックしてから右の画像をクリックすると、2つの場所の関係が設定されます。

Step 5 「**標定確定**」をクリックします。

Step 6 ステップ 2-4 を標定点 2-4 に対して繰り返します。

Step 7 「**良**」をクリックします。

Step 8 (オプション) **初期設定**をクリックすると、すべての構成をデフォルト設定に戻します。

3.21 アドバンスド

環境温度、ターゲットのコア温度や体表面温度を見ることができます。



この機能に対応しているのは一部の機種のみです。

3.22 ログアウト

右上の  ボタンをクリックし、「OK」をクリックすると、Web インターフェースからログアウトします。

4 SmartPSS AC の設定

アクセスコントローラーの管理は、SmartPSS AC クライアントで行います。詳しい設定については、SmartPSS AC のユーザーマニュアルをご覧ください。



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

4.1 ログイン

Step 1 SmartPSS AC をインストールします。

Step 2  をダブルクリックし、指示に従って初期化を終了してログインします。

4.2 デバイスの追加

SmartPSS AC にアクセスコントロールの機器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たり、「追加」をクリックして手動でデバイスを追加することができます。

4.2.1 オートサーチ

同じネットワークセグメントにある入退室管理者を検索し、SmartPSS AC に追加することができます。

Step 1 SmartPSS AC にログインします。

Step 2 左下の「デバイス」をクリックします。

Figure 4-1 デバイス



No.	名前	IP	装置タイプ	デバイスモデル	ポート	チャンネル番号	オンラインステータス	S/N	操作
1	192.168.1.110	192.168.1.110	N/A	N/A	37777	0/0/0/0	● オフライン	N/A	 
2	192.168.1.120	192.168.1.120	アクセスコントロール	ASi6213J-FT1	37777	2/0/1/0	● オンライン	7F01B37GAJE06D2	 

Step 3 「自動検索」をクリックします。

Figure 4-2 自動検索

<input type="checkbox"/> No.	IP	装置タイプ	MACアドレス	ポート	初期化状態
<input type="checkbox"/> 1	192.168.1.98	ASI6213J-FT1	6c:1c:71:bd:0c:1c	37777	初期化しました

Step 4 デバイス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。

Step 5 SmartPSS AC に追加したいアクセスコントローラーを選択し、「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。

Step 6 ユーザー名とログインパスワードを入力してログインします。

追加されたアクセスコントローラーは、「デバイス」のインターフェイスに表示されます。

 アクセスコントローラーを選択し、「修正」をクリックすると、アクセスコントローラーの IP アドレスを修正することができます。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ご参照ください。

4.2.2 マニュアル追加

アクセスコントロールを手動で追加することができます。追加したいアクセスコントロールの IP アドレスとドメイン名を知っておく必要があります。

Step 1 SmartPSS AC にログインします。

Step 2 左下の「デバイス」をクリックします。

Step 3 「デバイス」インターフェイスの「追加」をクリックすると、「追加」インターフェイスが表示されます。

Figure 4-3 マニュアル追加



追加

チャンネル名: *

登録モード: IP

IP: *

ポート: * 37777

ユーザー名: *

パスワード: *

追加と続行 追加 キャンセル

Step 4 デバイス名の入力、登録モードの選択、IP、ポート番号（デフォルトでは37777）、ユーザー名、パスワードの入力を行います。

Step 5 「追加」をクリックすると、「デバイス」インターフェースに追加されたアクセスコントローラが表示されます。

4.3 ユーザー管理

4.3.1 カードタイプの選択

カードを発行する前に、まずカードの種類を設定します。例えば、発行するカードがIDカードの場合、タイプをIDカードにします。

 カードの種類は、カード発行者の種類と同じでなければなりません。そうでなければ、カード番号を読み取ることはできません。

Step 1 SmartPSS AC にログインします。

Step 2 「従業員の管理者」をクリックします。

Figure 4-4 従業員の管理者



Step 3 従業員の管理者のインターフェースで、 をクリックし、次に  をクリックします。

Step 4 「カードタイプの設定」画面で、カードタイプを選択します。

Step 5  をクリックすると、カード番号の表示方法を10進数か16進数で選択できます。

Figure 4-5 カードタイプの設定



Step 6 「確認」をクリックします。

4.3.2 ユーザーの追加

ユーザーを追加する方法を選択してください。

- ユーザーを1人ずつ追加。
- ユーザーを一括追加。
- 他のデバイスからユーザー情報を抽出。
- ユーザー情報をローカルから取り込む。

4.3.2.1 マニュアル追加

ユーザーを1人ずつ手動で追加することもできます。

Step 1 SmartPSS AC にログインします。

Step 2 「**従業員の管理者**」 → 「**ユーザー**」 → 「**追加**」をクリックします。

Step 3 ユーザーの基本情報を追加します。

- 1) 「**ユーザーの追加**」インターフェースの「**基本情報**」タブをクリックして、ユーザーの基本情報を追加します。
- 2) 画像をクリックし、「**画像のアップロード**」をクリックして顔画像を追加します。
アップロードされた顔画像は、キャプチャーフレームに表示されます。



画像のピクセル数が 500×500 以上、画像サイズが 120KB 以下であることを確認してください。

Figure 4-6 ユーザーの追加（基本情報）

ユーザーの追加

基本情報 証明 許可設定

ユーザーID: * 2

名前: * test

部門: Default Company

ユーザー種別: 一般

有効時間: 2021/7/21 0:00:00 2031/7/21 23:59:59 3653 日

使用数: 制限なし

画像アップロード

イメージのサイズ: 0-120kb

詳細情報

性別: 男性 女性

証明書タイプ: ID

タイトル: Mr

身分証明書のナン...

出生年月日: 1985/03/15

会社:

電話:

持ち場:

メール:

入職時間: 2021/7/20 14:47:59

通信アドレス:

辞任時間: 2031/7/21 14:47:59

管理者:

備考:

増加を続けます 終了 キャンセル

Step 4 証明タブをクリックして、ユーザーの認証情報を追加します。

- パスワードの設定

パスワードを設定します。第2世代のアクセスコントロールシステムでは、人員のパスワードを設定し、その他の機器では、カードのパスワードを設定します。新しいパスワードは6桁の数字でなければなりません。

- カードの設定



カード番号は、自動的に読み取ることも、手動で記入することもできます。自動で読み取る場合は、カードリーダーを選択し、カードをカードリーダーにセットします。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「**機器**」または「**カード発行機**」をクリックして選択します。
- 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ーを使用する場合は、カード番号の追加が必要です。
- 3) 追加した後は、そのカードをメインカードやドレスカードとして選択したり、新しいカードと交換したり、カードを削除したりすることができます。

- 指紋の設定

- 1)  をクリックして、指紋スキャナーとして**機器**または**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**」をクリックして、スキャナーに指を3回連続して押しします。

Figure 4-7 ユーザーの追加（認証の設定）

ユーザー編集
✕

基本情報
証明
許可設定

パスワード 第二世代アクセスコントローラーの場合、従業員パスワードとなります。それ以外では、カードパスワードとなります。

カード 追加 第二世代アクセスコントローラーを使用していない場合、カード番号は必ず追加するものとします。

1

カード発行...	2021-05-10
カード置換...	2021-05-10

指紋

+ 追加
 削除

<input type="checkbox"/>	指紋名	操作
<input type="checkbox"/>	指紋1	
<input type="checkbox"/>	指紋2	
<input type="checkbox"/>	指紋3	

終了
キャンセル

Step 5 ユーザーの権限を設定する。

詳細は「4.4 許可設定」をご覧ください。

Figure 4-8 許可設定

基本情報
証明
許可設定

許可グループは、出勤確認やアクセス制御を含む様々なデバイスを組み合わせたものです。許可グループを選択すると、従業員情報は対応デバイスに送信され、アクセス制御や出勤確認に関する機能に活用されます。

グループを追加

<input type="checkbox"/>	許可グループ	ノート
<input type="checkbox"/>	許可グループ1	

Step 6 「終了」をクリックします。

4.3.2.2 バッチの追加

ユーザーを一括して追加することができます。

Step 1 SmartPSS AC にログインします。

Step 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。

Step 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、カード枚数、有効時間、有効期限を設定します。

Step 4 「発行」 をクリックすると、カードの発行が開始されます。

カード番号は自動的に読み取られます。

Step 5 カード発行後に「停止」 をクリックして、「OK」 をクリックします。

Figure 4-9 バッチ追加

ID	カードナンバー
----	---------

Step 6 ユーザーのリストで  をクリックすると、情報の修正や使用法の詳細を追加できます。

4.3.2.3 デバイスからユーザーを抽出

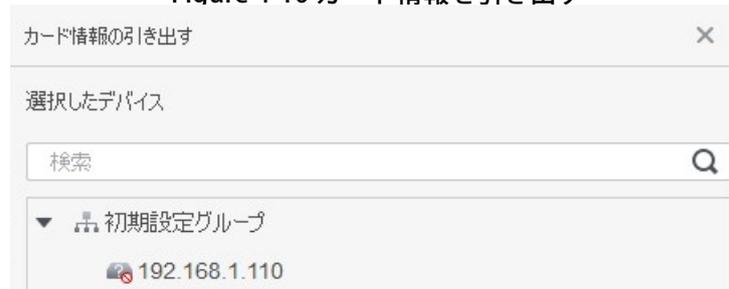
デバイスからユーザー情報を抽出することができます。

Step 1 SmartPSS ACにログインします。

Step 2 「**従業員の管理者**」→「**ユーザー**」→「**引き出す**」をクリックします。

Step 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。

Figure 4-10 カード情報を引き出す



Step 4 必要に応じてユーザーを選択し、「**引き出す**」をクリックします。

Step 5 ユーザーのリストで、ユーザーの情報を修正したり、詳細を追加したりするには、 をクリックします。

4.3.2.4 ユーザーのインポート

ユーザーをローカルに取り込むことができます。

Step 1 SmartPSS ACにログインします。

Step 2 「**従業員の管理者**」→「**ユーザー**」→「**インポート**」をクリックします。

Step 3 指示に従ってユーザー情報をインポートします。

4.3.3 カードを一括して発行する

追加されたのにカードを持っていないユーザーにカードを発行することができます。

Step 1 SmartPSS ACにログインします。

Step 2 「**従業員の管理者**」→「**ユーザー**」を選択します。

Step 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。

Step 4 カードを一括して発行することができます。カード No.はカードリーダーで自動読み取り、または手入力が可能です。

- 自動読み取り

- 1) カード読取装置を選択して、「発行」をクリックします。

- 2) カードリストに基づいて、対応するユーザーのカードをカードリーダーに順番に置くと、システムがカード番号を自動で読み取ります。

- 3) カード検証の開始時間や終了時間などのユーザー情報を変更する。

- 手動で入力

- 1) カードリスト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間や終了時間などのユーザー情報を変更する。

Figure 4-11 一括カード発行

一括カード発行

機器:

ID: 名前:

カードナンバー: 部門:

開始時間: 終了時間:

カードリスト

ユーザーID	名前	カードナンバー	操作
yamguchi001	yamaguchi		

Step 5 「OK」をクリックします。

4.3.4 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することができます。

Step 1 SmartPSS AC にログインします。

Step 2 「従業員の管理者」 → 「ユーザー」を選択します。

Step 3 エクスポートする必要があるユーザー情報を選択し、「バックアップ」をクリックすると、すべてのユーザー情報がローカルにエクスポートされます。

4.4 許可設定

4.4.1 許可グループの追加

Step 1 SmartPSS AC にログインします。

Step 2 「従業員の管理者」 → 「許可設定」をクリックします。

Figure 4-12 許可グループリスト



<input type="checkbox"/>	許可グループ	操作
<input type="checkbox"/>	許可グループ1	  

Step 3  をクリックして許可グループを追加します。

Step 4 許可パラメータの設定

- 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 のユーザーマニュアルをご参照ください。

- 3) 「ドア 1」など、対応するデバイスを選択します。

Figure 4-13 権限グループの追加

Step 5 「OK」をクリックします。



許可グループリストのインターフェースでは、以下のことができます。

-  をクリックするとグループを削除します。
-  をクリックすると、グループ情報が変更されます。
- 許可グループ名をダブルクリックすると、グループ情報が表示されます。

4.4.2 許可設定

部署の権限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。

Step 1 SmartPSS AC にログインします。

Step 2 「従業員の管理者」 → 「許可設定」をクリックします。

Step 3 対象となる許可グループを選択して、 をクリックします。

Figure 4-14 許可設定



Step 4 ユーザーが必要とする権限を選択します。

Step 5 「OK」をクリックします。

4.5 アクセスマネージャー

4.5.1 遠隔でドアを開閉する

アクセス設定後、SmartPSS AC を使ってドアを遠隔操作することができます。

Step 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」 → 「アクセスマネージャー」をクリックします。

Step 2 ドアを遠隔操作する。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「開く」を選択します。

Figure 4-15 遠隔操作（方法1）



- 方法2: または をクリックしてドアを開閉します。

Figure 4-16 遠隔操作（方法2）



Step 3 イベント情報リストでドアの状態を確認



- イベントのフィルタリング。イベント情報でイベントの種類を選択すると、イベントリストには選択した種類のイベントが表示されます。例えば、「アラーム」を選択すると、イベントリストにはアラームイベントのみが表示されます。
- イベントの更新ロック。イベント情報の右側 をクリックして、イベントリストをロックまたはロック解除すると、リアルタイムのイベントが表示されなくなります。
- イベントの削除イベント情報の右側 をクリックすると、イベントリストのすべてのイベントが消去されます。

4.5.2 常時開・常時閉の設定

「常時開」または「常時閉」を設定すると、ドアは常に開状態または閉状態となり、手動でコントロールすることはできません。再び手動でドアを制御したい場合は、「通常」をクリックしてドアの状態をリセットしてください。

Step 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」→「アクセスマネージャー」をクリックします。

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

Figure 4-17 常に開いているか、常に閉じているか

4.5.3 ドアの状態をリセットする



「ノーマルオープン」または「ノーマルクローズ」をクリックした後、再び手動でドアを制御したい場合は、「ノーマル」をクリックしてドアの状態をリセットします。

Step 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」→「アクセスマネージャー」をクリックします。

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

Figure 4-18 ドアの状態をリセット



4.6

アテンダンス・マネージメント

出勤時間の設定、出勤シフトの追加、人事スケジューリング、出勤処理、出勤統計の管理、レポートの検索、休日の追加、出勤の設定などができます。

4.6.1 レポート検索

ここでは、通常出勤、出勤異常、残業出勤、スタッフ情報などを見ることができます。また、統計データはレポートとして出力することができます。

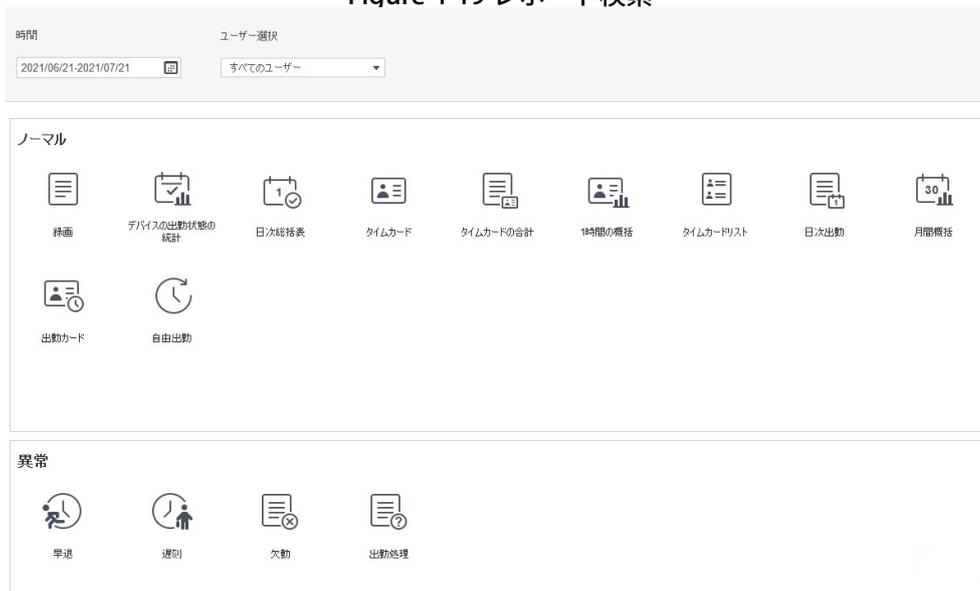
Step 1 SmartPSS AC にログインします。

Step 2 左のメニューの  をクリックします。

Step 3 右下の「出勤ガイド」をクリックし、「出勤クイックガイド」 の  をクリックします。

Step 4 時間、部門、統計の種類を選択すると、対応するレポートが表示されます。

Figure 4-19 レポート検索



SmartPSS AC プラットフォーム上でデバイスが追加され、認証された後、対応する出席状況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状況レポートを生成します。

Figure 4-20 デバイスの出席状況レポート

Default Company
Device Attendance State Summary Report From 2020/05/16 to 2020/06/16

Department		No Department								
Employee No.	Date	Away Time	Return Time	Total (Minute)	Card No.		Total (Minute)	Overtime work sign in	Overtime work sign out	Total (Minute)
2	2020/06/16					17:14:55				

4.6.2 その他の構成

その他の設定（出勤期間、出勤シフト、人員スケジューリング、出勤処理、出勤統計、休日の追加、出勤設定など）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。

Step 1 SmartPSS AC にログインします。

Step 2 左のメニュー  をクリックします。

Step 3 右下の「出勤ガイド」をクリックします。

Figure 4-21 SmartPSS AC のユーザーズマニュアルを見る



5 よくある質問

- 1. アクセスコントローラーの電源投入後の起動に失敗しました。**
12V 電源が正しく接続されているかを確認してください。
- 2. アクセスコントローラーの電源を入れた後は、顔の認識ができません。**
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。「2.8.2 ロック解除」をご覧ください。
- 3. Wiegand ポートにアクセスコントローラーと外部コントローラーが接続されている場合、出力信号はありません。**
アクセスコントローラと外部コントローラの GND ケーブルが接続されているか確認してください。
- 4. 管理者 ID とパスワードを忘れてしまい、設定ができなくなりました。**
プラットフォームを通じて管理者を削除するか、テクニカルサポートに連絡してリモートでアクセスコントローラーを解除してください。
- 5. ユーザー情報や顔写真をアクセスコントローラーに取り込むことができません。**
XML ファイルの名前やテーブルのタイトルが変更されていないか確認してください。
- 6. ユーザーの顔を認識しても、他の利用者の情報が表示されてしまう。**
人の顔を取り込む際には、周囲に他の人がいないことを確認してください。元の顔を削除して、再度インポートします。

Appendix 1

顔登録の注意点/比較

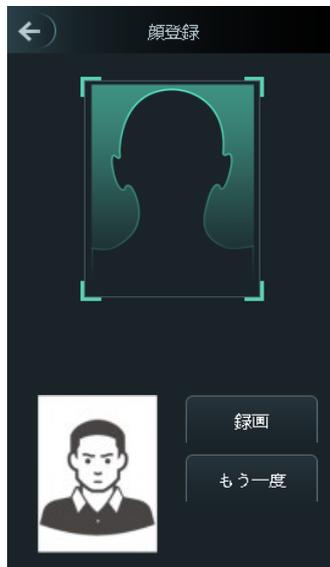
登録前

- 眼鏡や帽子、ひげなどが顔認識性能に影響を与える可能性があります。
- 帽子をかぶるときは、眉毛を隠さないようにしましょう。
- 顔認証に失敗する可能性がありますので、使用する際にはヒゲのスタイルを大きく変えないでください。
- 顔を清潔に保つ。
- 逆光や直射日光が当たると、本機の顔認識性能に影響を与える可能性があります。

登録時

顔の登録は、アクセスコントローラーからでも、プラットフォームからでも可能です。プラットフォームからの登録については、プラットフォームのユーザーマニュアルをご覧ください。写真撮影フレームに頭を中心に合わせてください。顔の写真が自動的に撮影されます。

Appendix Figure 1-1 登録

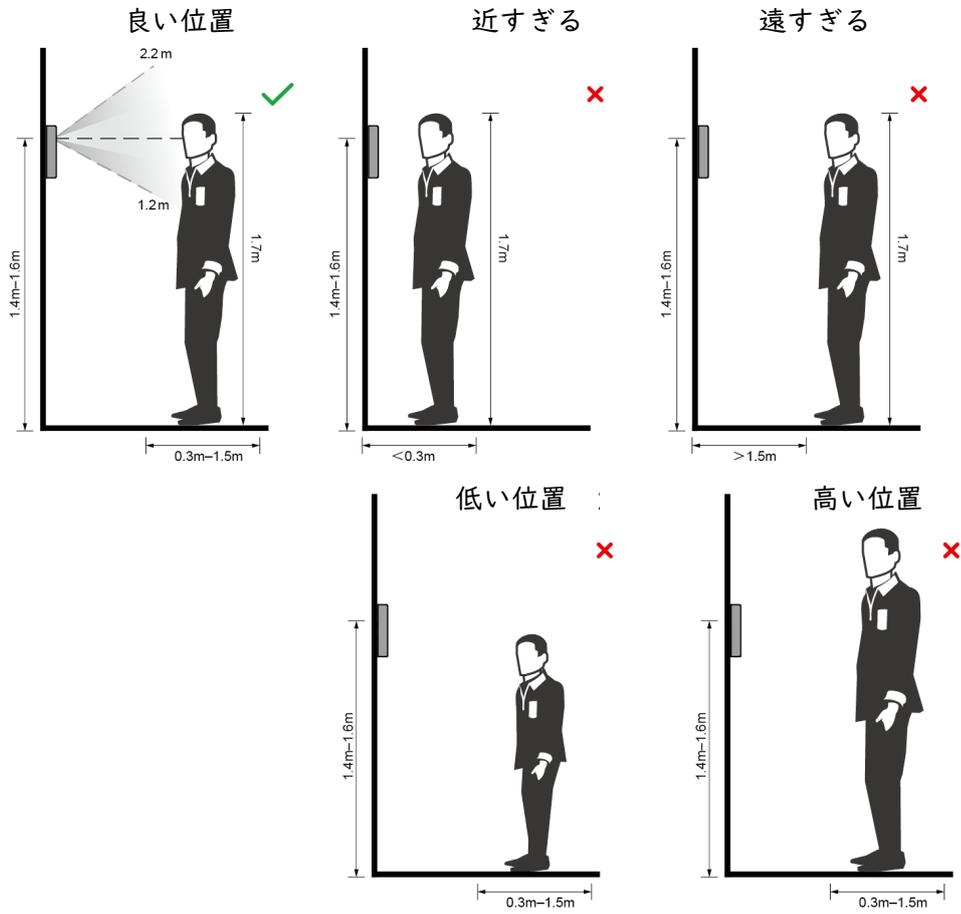


- 頭や体を揺らさないようにすると、登録に失敗することがあります。
- 2つの顔が同時に写らないようにします。

顔の位置

顔の位置が適切でないと、顔認識性能に影響が出る可能性があります。

Appendix Figure 1-2 適切なフェイスポジション



顔の条件

- 顔が清潔であること、額が髪で覆われていないことを確認してください。
- 眼鏡や帽子、濃いひげなど、顔画像の記録に影響を与える顔の装飾品をつけないでください。
- 目を開けて、無表情で、顔をカメラの中心に向けて撮影してください。
- 顔の撮影や顔認識の際には、顔をカメラに近づけすぎたり、遠ざけすぎたりしないようにしてください。

Appendix Figure 1-3 適切な顔の向き



Appendix Figure 1-4 顔の距離



- 管理画面から顔画像を取り込む際には、画像の解像度が $150 \times 300 \sim 600 \times 1200$ 以内、画像の画素数が 500×500 以上、画像サイズが 75KB 以下、画像名と人物 ID が同じであることを確認してください。
- 顔の占める割合が全体の $1/3$ 以上 $2/3$ 以下で、アスペクト比が $1:2$ を超えないようにしてください。

Appendix 2

サイバーセキュリティに関する提言

サイバーセキュリティは、単なる流行語ではなく、インターネットに接続されているすべての機器に関するものです。IPビデオ監視システムは、サイバーリスクと無縁ではありませんが、ネットワークやネットワーク機器を保護・強化するための基本的なステップを踏むことで、攻撃を受けにくくなります。以下では、より安全なセキュリティシステムを構築するためのヒントや推奨事項をご紹介します。

基本的なデバイスのネットワークセキュリティのための必須アクション。

1. 強力なパスワードの使用

以下の提案を参考にして、パスワードを設定してください。

- 長さは8文字以下にしてください。
- 大文字、小文字、数字、記号など、少なくとも2種類の文字が含まれていること。
- アカウント名やアカウント名の逆順を含まないでください。
- 123、abcなどの連続した文字は使用しないでください。
- 111、aaaなどの重複した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適時にアップデート

- Tech-industryの標準的な手順によると、システムに最新のセキュリティパッチや修正プログラムを適用するために、お使いのデバイス（NVR、DVR、IPカメラなど）のファームウェアを最新に保つことを推奨しています。デバイスがパブリックネットワークに接続されている場合は、メーカーがリリースするファームウェアアップデートの情報をタイムリーに入手するために、「アップデートの自動チェック」機能を有効にすることをお勧めします。
- 最新のクライアントソフトウェアをダウンロードしてお使いになることをお勧めします。

デバイスのネットワークセキュリティを向上させるための「必要な」推奨事項：

1. 物理的保護

デバイス（特にストレージデバイス）に対して物理的な保護を行うことをお勧めします。例えば、特別なコンピュータールームやキャビネットにデバイスを設置し、権限のない人がハードウェアの破損やリムーバブルデバイス(USBフラッシュディスクや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行うことがないように、適切なアクセス制御許可や鍵の管理を実施してください。

2. パスワードの定期的な変更

推測されたり、クラックされたりするリスクを減らすために、パスワードを定期的に変更することをお勧めします。

3. パスワードの設定と更新情報のリセットは適宜に

本機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ための質問など、パスワードリセットのための関連情報を時間をおいて設定してください。情報が変更された場合は、適宜修正してください。パスワード保護用の質問を設定する際には、容易に推測できるものは使用しないことをお勧めします。

4. アカウントロックの有効化

アカウントロック機能は、デフォルトで有効になっていますが、アカウントのセキュリティを保証するために、この機能をオンにしておくことをお勧めします。攻撃者が誤ったパスワードで何度もログインしようとする、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. HTTP およびその他のサービスのデフォルトポートの変更

デフォルトの HTTP およびその他のサービスポートを 1024~65535 の間の任意の数字に変更することをお勧めします。これにより、部外者が使用しているポートを推測できるリスクを軽減できます。

6. HTTPS を有効にする

お客様が安全な通信経路でウェブサービスを利用できるように、HTTPS を有効にすることをお勧めします。

7. MAC アドレスバインディング

ゲートウェイの IP アドレスと MAC アドレスを本機にバインドすることで、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。

8. アカウントと権限の合理的な割り当て

ビジネスやマネジメントの要求に応じて、合理的にユーザーを追加し、最低限の権限を割り当てます。

9. 不要なサービスの停止と安全なモードの選択

必要のない場合は、リスクを軽減するために、SNMP、SMTP、UPnP などの一部のサービスをオフにすることをお勧めします。

必要に応じて、以下のサービスを含む安全なモードを使用することを強くお勧めしますが、これに限定されるものではありません。

- 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ーへのアクセスに 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 ホットスポットです。WPA2-PSK の暗号化モードを選択し、強力なパスワードを設定してください。

10. 音声・映像の暗号化伝送

音声・映像データの内容が非常に重要な場合は、伝送中に音声・映像データが盗まれるリスクを減らすために、暗号化伝送機能を使用することをお勧めします。

注意：暗号化された伝送は、伝送効率が多少低下します。

11. セキュア・オーディティング

- オンラインユーザーの確認：定期的にオンラインユーザーを確認し、デバイスが不正にログインされていないかを確認することをお勧めします。
- デバイスのログを確認します。ログを見ることで、機器へのログインに使用された IP アドレスや、その主要な操作を知ることができます。

12. ネットワークログ

デバイスの記憶容量には限りがあるため、保存されるログには制限があります。ログを長期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、重要なログがネットワークログサーバーに同期してトレースされるようにすることをお勧めします。

13. 安全なネットワーク環境の構築

デバイスの安全性をより確実にし、潜在的なサイバーリスクを低減するために、私たちは以下のことを推奨します。

- ルーター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の機器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必要性に応じて、分割・分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、VLAN やネットワーク GAP などの技術を使ってネットワークを分割し、ネットワークの分離効果を得ることが推奨されます。
- 802.1x アクセス認証システムを構築し、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低減する。
- IP/MAC アドレスフィルタリング機能を有効にして、デバイスへのアクセスを許可するホストの範囲を制限します。

問い合わせ先

株式会社ウエスト

TEL 072-826-0323

※9:00～17:00のみ

(土日祝日、夏季休業、年末年始等は除く)

<https://west-lock.co.jp/>

