DHI-ASI7213X-T1マニュアル

20200621

序文

初めに

本書では、顔認証アクセスコントローラー（以下「アクセスコントローラー」といいます）の設置と基本操作についてご紹介します。

マニュアルについて

・マニュアルは参照用です。マニュアルと実際の製品との間に矛盾がある場合は、
　実際の製品が優先されます。
・マニュアルに記載されていない操作により生じたいかなる損害についても責任を負いません。
・マニュアルは、関連する地域の最新の法律および規制に従って更新されます。
　紙のマニュアルと電子版の間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、事前の書面による通知なしに変更される場合があります。
　製品のアップデートにより、実際の製品とマニュアルが異なる場合があります。
　最新のプログラムと補足ドキュメントについては、カスタマーサービスにお問い合わせください。
・技術データ、機能と操作の説明、または印刷のエラーに偏差がある可能性があります。
　その場合は販売代理店へご連絡ください。
・マニュアルを開けない場合は、リーダソフトウェアをバージョンアップするか、
　他のソフトウェアで試してみてください。
・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、
　それぞれの所有者の財産です。
・デバイスの使用中に問題が発生した場合は、弊社のWebサイトにアクセスし、
　カスタマーサービスにお問い合わせください。
・疑問点などある場合は、販売店までご連絡をお願い致します。

注意

本製品は体温をはかるものではございません。
表面温度を表示するようになっております。
正確な体温を測定するには接触型の体温計を使用ください。

重要な保護手段と警告

この章では、アクセスコントローラの適切な取り扱い、危険防止、および物的損害の防止に関する内容について説明します。
アクセスコントローラーを使用する前にこれらの内容を注意深く読み、使用するときはこれを遵守し、将来の参照のために保管してください。

動作要件

・日光が当たる場所や熱源の近くにアクセスコントローラを設置または設置しないでください。

・アクセスコントローラを湿気、ほこり、またはすすに近づけないでください。

・アクセスコントローラーが水平になるように安定した場所に設置し、落下しないようにしてください。

・アクセスコントローラーに液体を落としたり、かけたりしないでください。
また、液体がアクセスコントローラーに流れ込むのを防ぐために、液体で満たされた物体がアクセスコントローラー上にないことを確認してください。

・アクセスコントローラーは換気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は、入出力定格範囲内の電源で操作してください。

・アクセスコントローラーをランダムに分解しないでください。

・許可された湿度と温度の条件下でアクセスコントローラの輸送、使用、および保管します。

・温度監視ユニットを備えたアクセスコントローラーの場合：
★温度監視ユニットは、風のない屋内環境に設置し、屋内の周囲温度を15°C～32°Cに維持してください。

★温度監視ユニットが熱平衡に到達できるように、電源投入後20分以上温度監視ユニットをウォームアップします。

電気安全

・バッテリーを不適切に使用すると、火災、爆発、または炎症を引き起こす可能性があります。

・電池交換の際は、必ず同一機種をご使用ください。

・地域で推奨されている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ーに付属の電源アダプターを使用してください。
付属以外の電源を使用するとデバイスの損傷につながる可能性があります。

・電源は、安全特別低電圧（SELV）規格の要件に準拠し、IEC60950-1に基づく制限電源の要件に準拠する定格電圧で電力を供給します。電源要件はデバイスラベルの対象になることに注意してください。

・デバイス（Iタイプの構造）を保護接地付きの電源ソケットに接続します。

・電気器具のカプラーは切断装置です。
カプラーを使用するときは、操作しやすい角度にしてください。

目次

1 概要

1.1 前書き

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。

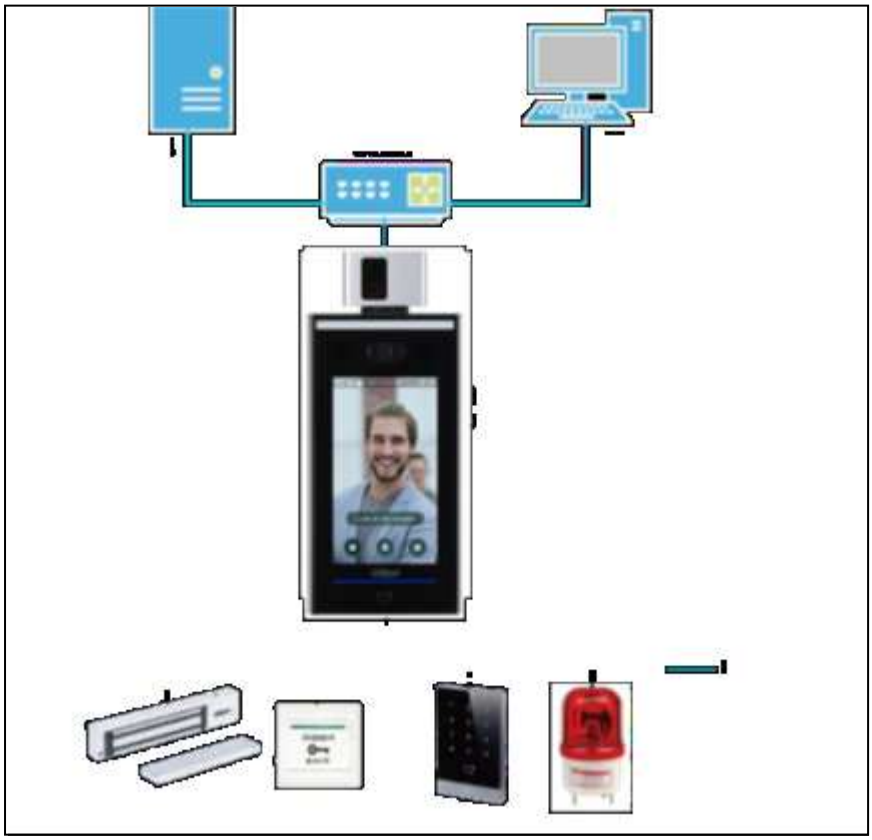
1.2 特長

- 7インチLCDディスプレイのアクセスコントローラーで解像度は1024×600です。
- 顔認証、ICカード認証、パスワード認証をサポート。期間ごとにロック解除可能。
- 顔検出ボックス付き：範囲内に表示された顔の中で最大の顔が最初に認識されます。
- 2MP広角WDRレンズ：自動/手動照明付き
- 顔認識アルゴリズムにより、アクセスコントローラーは人間の顔の360を超える位置を認識できます。
- 顔認証精度> 99.5％;
- ０℃~90℃の横顔認識サポート。
- 生体検知サポート。
- 強迫警報、改ざん警報、侵入警報、ドア接触タイムアウト警報、および違法カード超過しきい値警報をサポート。
- 一般ユーザー、巡回ユーザー、ブラックリストユーザー、VIPユーザー、ゲストユーザー、特別ユーザーをサポート。
- さまざまなロック解除ステータス表示モードでユーザーのプライバシーを保護。
- 周辺温度監視ユニットによる体温監視をサポート

1.3 運用

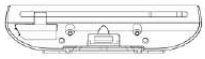
アクセスコントローラーは、オフィスビル、学校、工場、住宅地などの場所に最適です。
顔認証で本人確認を行い、ストレスのない通過を実現します。

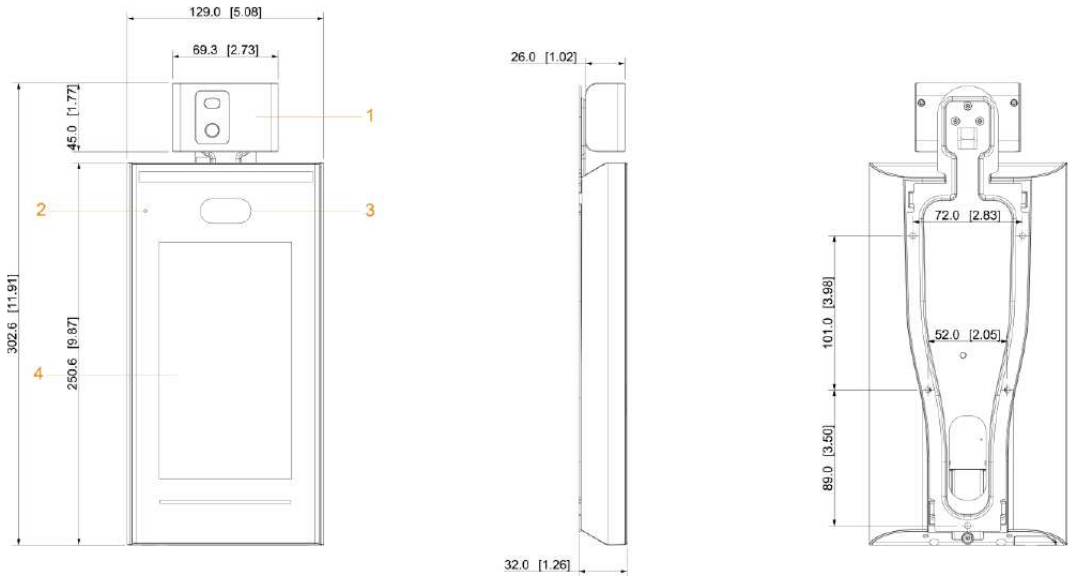
図1-1　ネットワーク



1.4 寸法とコンポーネント

図1-2　寸法とコンポーネント





テーブル1-1　コンポーネント詳細

No.	名称	No.	名称
1	温度監視ユニット	3	デュアルカメラ
2	マイク	4	ディスプレイ

2 接続と設置

2.1 ケーブル接続

アクセスコントローラーは、サイレン、リーダー、ドアの接点などのデバイスに接続する必要があります。
ケーブル接続については、テーブル2-1を参照してください。

テーブル2-1　ケーブル接続

ポート	ケーブル色	ケーブル名	詳細
CON1	Black	RD－	外部カードリーダーのマイナス電極
	Red	RD+	外部カードリーダーの正極
	Blue	CASE	外部カードリーダーの改ざんアラーム入力
	White	D1	ウィーガンドD1入力（外部カードリーダーに接続）/出力（コントローラーに接続）
	Green	D0	ウィーガンドD0入力（外部カードリーダーに接続）/出力（コントローラーに接続）
	Brown	LED	外部リーダーインジケーターに接続
	Yellow	B	RS-485負極入力（外部カードリーダーに接続）/出力（コントローラーに接続、またはドア制御セキュリティモジュールに接続） セキュリティモジュールが有効になっている場合は、アクセス制御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個の電源を必要とします。 セキュリティモジュールが有効になると、終了ボタン、ロックコントロール、および消防リンケージは無効になります。
	Purple	A	RS-485正極入力（外部カードリーダーに接続）/出力（コントローラーに接続、またはドアコントロールセキュリティモジュールに接続） セキュリティモジュールが有効になっている場合は、アクセス制御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個の電源を必要とします。 セキュリティモジュールが有効になると、終了ボタン、ロックコントロール、および消防リンケージは無効になります。
CON2	White and red	ALARM1_NO	アラーム1出力ポート：NO(ノーマルオープン)
	White and orange	ALARM1_COM	アラーム1出力ポート：コモン
	White and blue	ALARM2_NO	アラーム2出力ポート：NO(ノーマルオープン)
	White and gray	ALARM2_COM	アラーム2出力ポート：コモン
	white and green	GND	共通GND
	White and Brown	ALARM1	アラーム1入力ポート
	White and yellow	GND	共通GND
	White and purple	ALARM2	アラーム2入力ポート
CON3	Black and red	RX	RS-232受信ポート
	Black and orange	TX	RS-232送信ポート
	Black and blue	GND	共通GND
	Black and gray	SR1	ドア接触検知に使用　Used for door contact detection.
	Black and green	PUSH1	ドアNo.1のドアオープンボタン　Door open button of door No.1
	Black and Brown	DOOR1_COM	ロック制御共通ポート
	Black and yellow	DOOR1_NO	ロック制御ポート：NO（ノーマルオープン）
	Black and purple	DOOR1_NC	ロック制御ポート：NC（ノーマルクローズ）

2.2 設置環境

- **アクセスコントローラーから0.5メートル離れた場所に光源がある場合、最低照度は100ルクス以上である必要があります。**

- **アクセスコントローラーは、窓とドアから少なくとも3メートル、照明から2メートル離れた屋内に設置することをお勧めします。**

- **逆光や直射日光を避けてください。**

周囲照明の要件

図2-1　ネットワーク

蝋燭：約10Lux　**電球：約100～850Lux**　**日光：≧1200Lux**

温度検知の要件

・ 温度監視ユニットは、屋内の無風環境（屋外から比較的離れた場所）に設置し、
周囲温度を15°C～32°Cに維持することをお勧めします。

・ 温度監視ユニット平衡化するため、電源投入後20分以上経過してからご使用ください。

・ 屋外には設置しないでください。

・ 日光、風、冷気、冷房と温風の空調などの要素は、人体の表面温度とアクセスコントローラーの動作状態に簡単に影響を及ぼし、監視された温度と実際の温度との間に温度偏差を引き起こします。ご注意ください。

・ 温度監視の影響因子
・風：風は額から熱を奪います。これは、温度監視の精度に影響します。

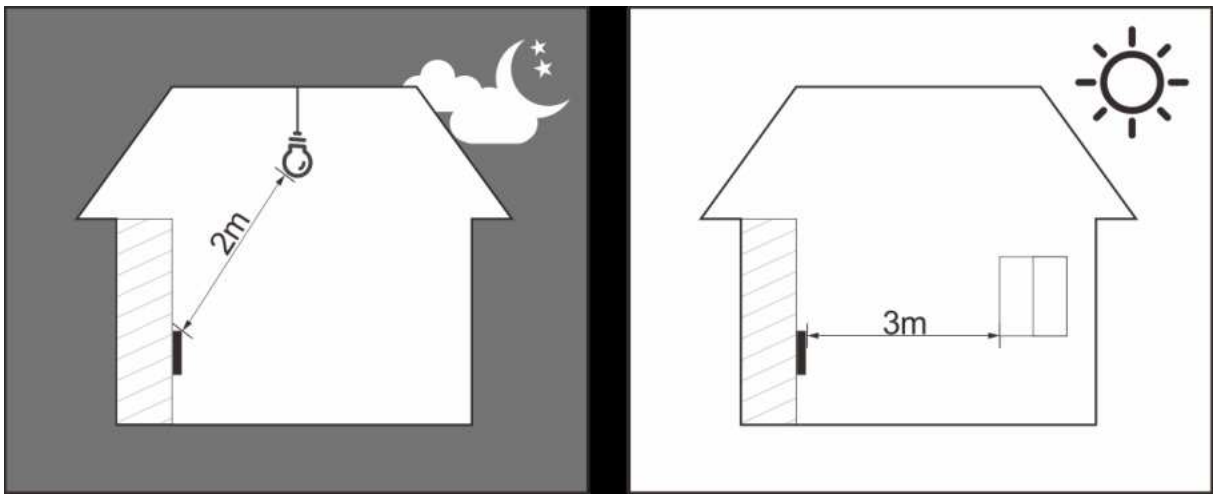
・発汗：発汗は、体が自動的に冷えて熱を放散します。汗をかくと、体温も下がります。

・室温：室温が低いと人体の表面温度が下がります。室内温度が高すぎると、
人体が発汗し始め、温度監視の精度に影響を与えます。

・温度監視ユニットは、波長10um～15umの光波に敏感です。
太陽、蛍光灯の光源、エアコンの吹き出し口、暖房、冷気の吹き出し口、ガラスの表面での使用は避けてください。

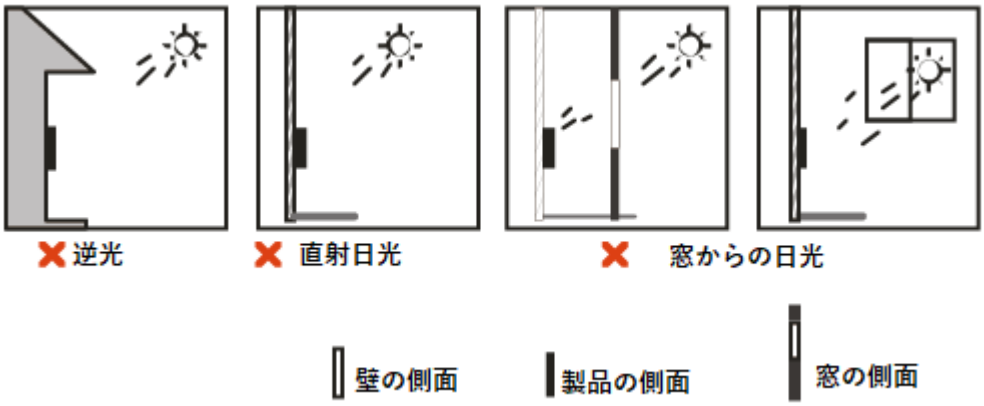
推奨設置場所

図2-2



推奨しない設置位置

図2-3



2.3 設置取付

カメラと地面の間の距離が1.4メートルであることを確認します。

図2-4

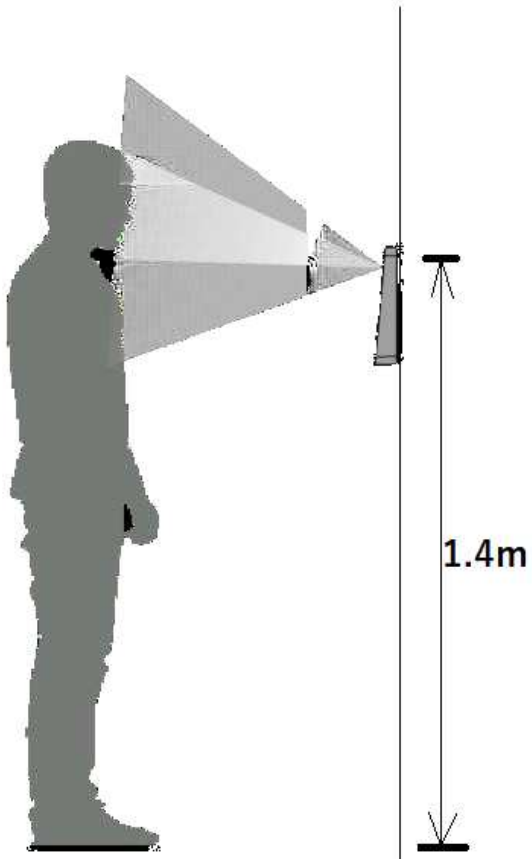
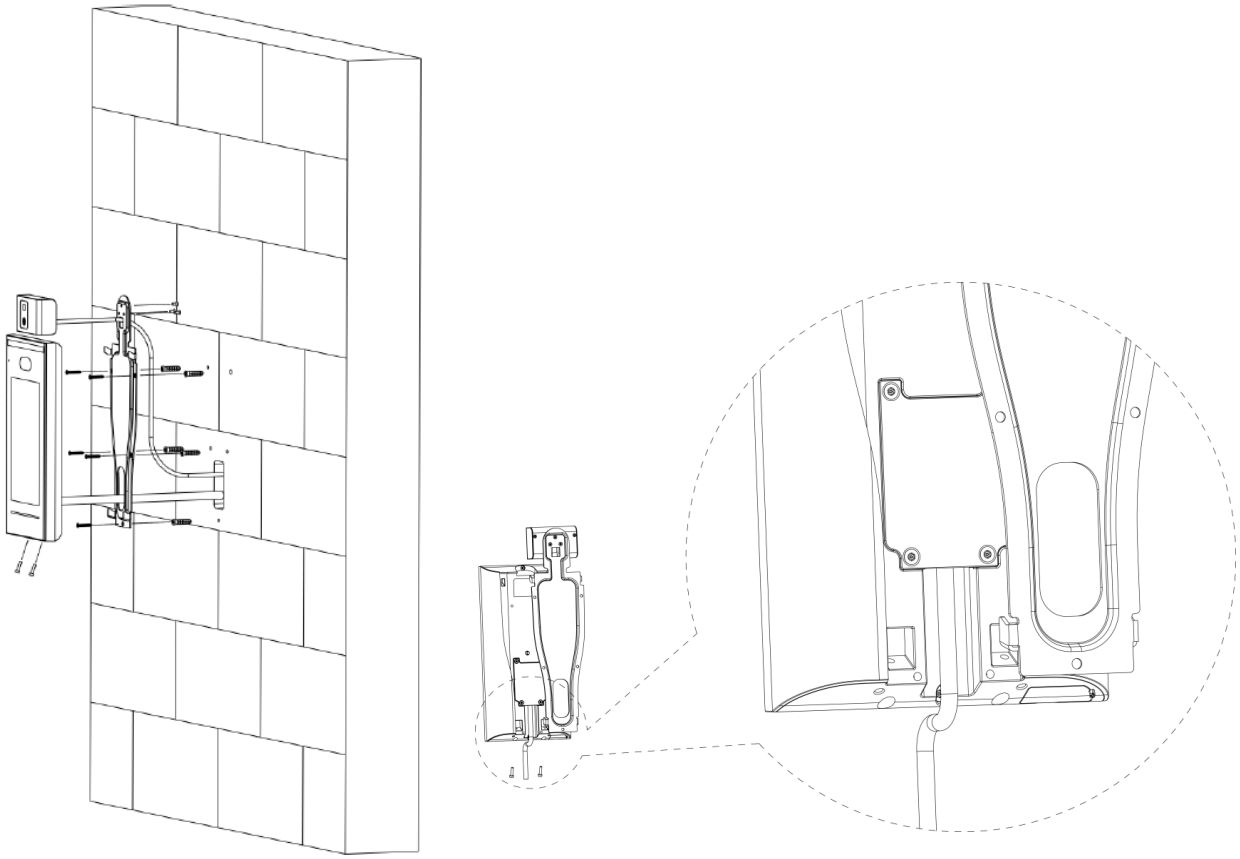


図2-5



設置手順

Step 1　3本のネジで温度監視ユニットをブラケットに固定します。

Step 2　ブラケットの穴に従って、壁に6つの穴（5つのブラケット取り付け穴と1つのケーブル入口）を開けます。

Step 3　6つのブラケット取り付け穴に拡張ネジを取り付けて、ブラケットを壁に固定します。

Step 4　本体のケーブルを接続します。「2.1ケーブル接続」を参照してください。

Step 5　本体をブラケットのフックに掛けます。

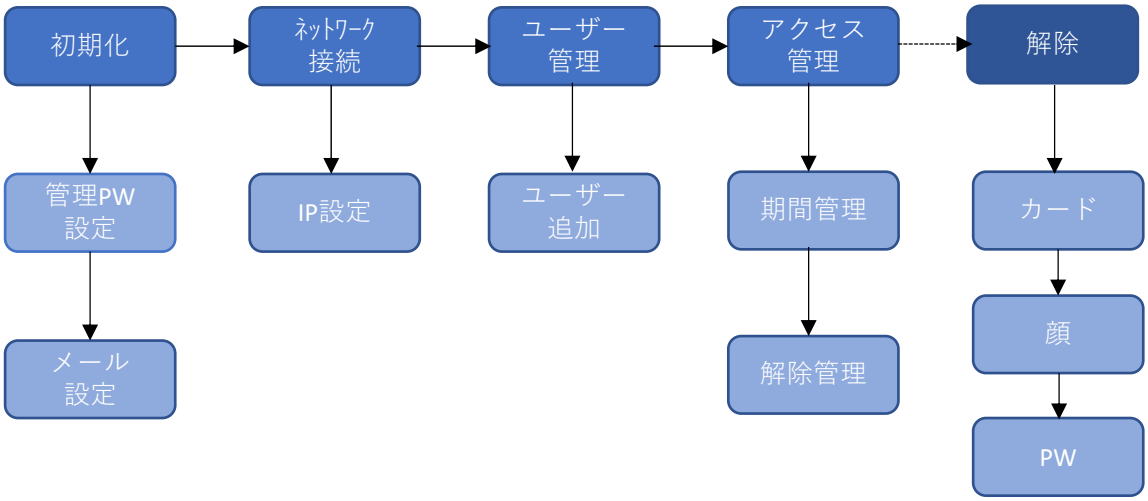
Step 6　本体の下部にあるネジを締めます。

Step 7　本体のケーブルコンセントにシリコンシーラントを塗布します。

3. システム操作

3. 1 基本的設定手順

図3-1　基本設定



3. 2 共通アイコン

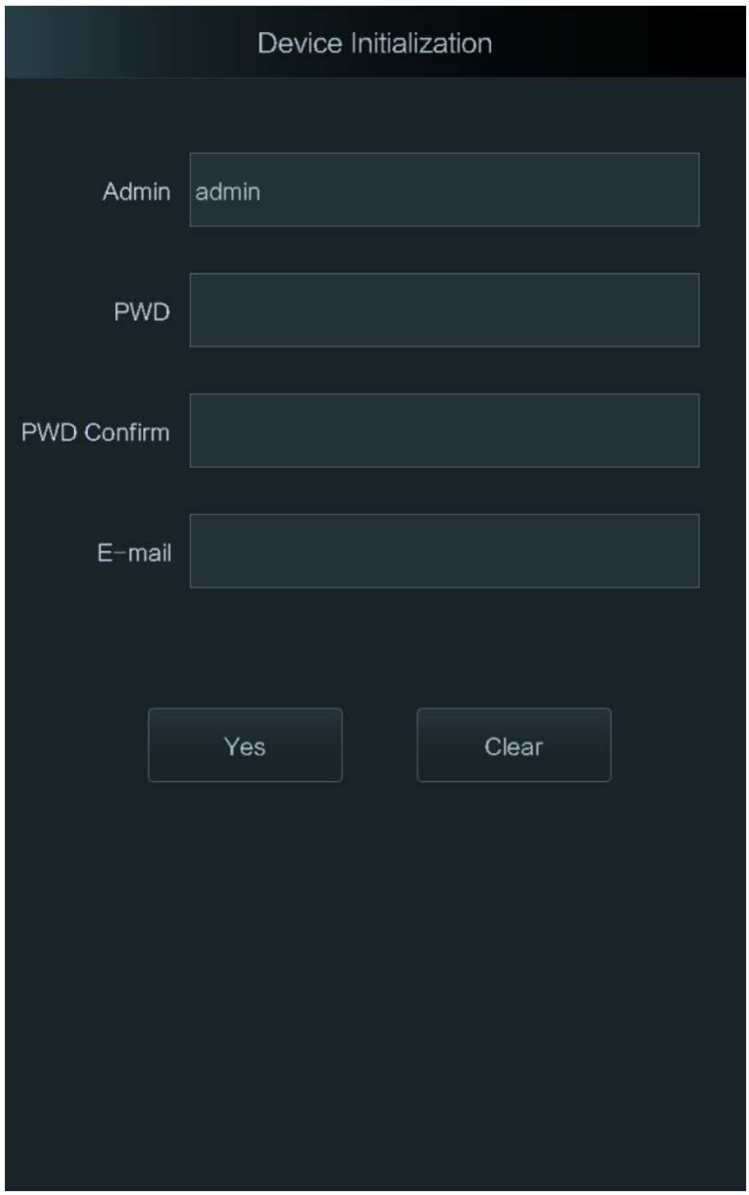
テーブル3-1　アイコン

アイコン	詳細
	メインメニューアイコン
	確定・確認アイコン
	リストの最初ページへ移動
	リストの最後ページへ移動
	1つ前のページへ移動
	1つ後のページへ移動
	1つ前のメニューへ移動
	有効
	無効

3. 3　初期化

本製品をを初めてオンにしたとき、管理者パスワードと電子メールはまたはリセット後に設定する必要があります。

図3-2



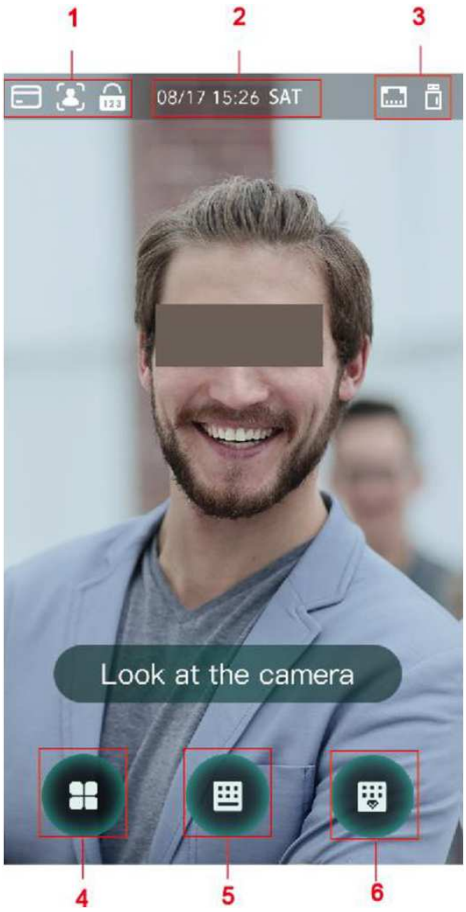
このインターフェイスで設定された管理者とパスワードは、Web管理プラットフォームへのログインに使用されます。
管理者のパスワードは、管理者がパスワードを忘れた場合に、入力した電子メールアドレスを使用してリセットできます。
パスワードは、8～32文字の空白以外の文字で構成され、大文字、小文字、数字、特殊文字（'";：＆を除く）の少なくとも2種類の文字を含む必要があります。

3. 4　スタンバイ

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。
図3-2を参照してください。

30秒間操作がない場合、アクセスコントローラはスタンバイモードになります。
スタンバイ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。

図3-3



テーブル3-2

No	詳細
1	ロック解除方法：カード、顔、パスワード カード、顔、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ーの左上隅に表示されません。
2	日付時刻。現在の日付と時刻を表示します
3	ネットワークの状態とUSBの状態を表示します
4	メインメニューアイコン(管理者権限を持つユーザーのみがメインメニューに入ることができます。)
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。

3.5　メインメニュー

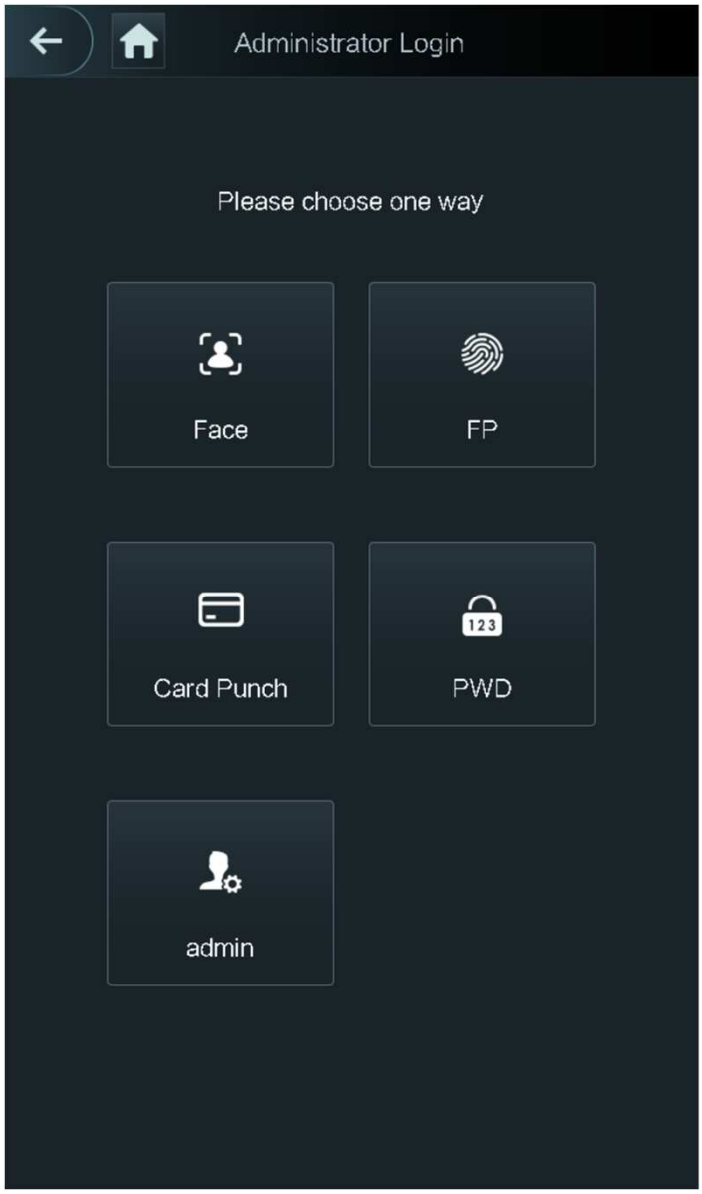
管理者は、メインメニューで、さまざまなレベルのユーザーの追加、アクセス関連のパラメーターの設定、ネットワーク構成の実行、アクセスレコードとシステム情報の表示などを行うことができます。

Step 1　スタンバイ画面の  ボタンをタップします。

Step 2　メインメニューの入力方法を選択します。

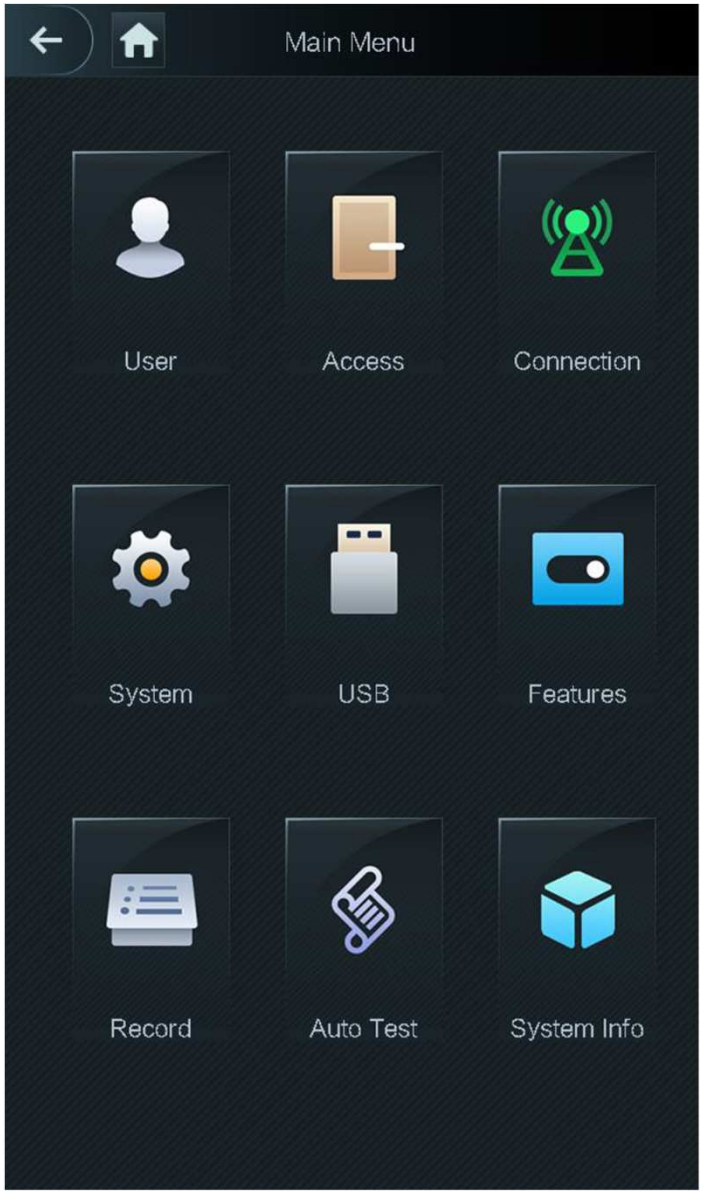
異なるモードは異なるロック解除方法をサポートし、実際のインターフェースが優先されます。

図3-4



メインメニューインターフェイスが表示されます。

図3-5



3. 6　ロック解除方法

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。

3.6.1　カード

カードスワイプエリアにカードを置き、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　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。

Step 1　スタンバイ画面の  ボタンをタップします。

Step 2　ユーザーIDを入力し、【はい】ボタンをタップします。

Step 3　ユーザーのパスワードを入力してから、【はい】ボタンをタップします。
IDとパスワードが正しければ解除されます。

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ーに対して管理者パスワードは1つしかありません。
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、休日の計画、アンチパスバックの対象となることなく、ドアのロックを解除できます。

「3.8.1.5 NC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。

Step 1　スタンバイ画面の  ボタンをタップします。

Step 2　【スーパーパスワードを入力してください】をタップします。

Step 3　管理者パスワードを入力してから、  ボタンをタップします。

パスワードが正しければ解除します。

3.7　ユーザー管理

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

3.7.1　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、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。

以下の図は参照用であり、実際のインターフェースが優先されます。

図3-6

テーブル3-3

項目	詳細
ユーザー ID	ユーザーIDを入力します。IDには、数字、文字、およびそれらの組み合わせを使用できます。IDの最大長は32文字です。
名前	名前は最大32文字（数字、記号、文字を含む）で入力してください。
顔	顔が写真キャプチャフレームの中央にあることを確認してください。アクセスコントローラが新しいユーザーの顔の写真を自動的に撮影します。
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イスで、カード番号を入力するか、カードをスワイプすると、 アクセスコントローラーによってカード情報が読み取られます。カード登録インターフェースで強迫カード機能を有効にすることができます。 ドアのロックを解除するために強迫カードが使用された場合、アラームがトリガーされます。
パスワード	ロック解除パスワード。最大8文字まで登録可能です。
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。 ・User：ユーザーはロック解除権限のみを持っています。 ・Admin：管理者はロックを解除することができ、各設定の権限も持っています。
期間	ユーザーが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を有効にする期間を設定できます。
ユーザーレベル	6つのレベルがあります。 ・General：General ユーザーは通常どおりロックを解除できます。 ・Blacklist：ブラックリストのユーザーが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。 ・Guest：ゲストは特定の時間にドアのロックを解除できます。設定した時間を超えると、ロックを解除することはできません。 ・Patrol：ユーザーは認識状況を追跡できますが、ロック解除の権限はありません。 ・VIP：ロックを解除すると、サービス担当者がプロンプトを表示します。 ・Special：ロックを解除すると、ドアが閉まるまでに5秒の遅延があります。
利用時間	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。

Step 1【ユーザー】→【新規ユーザー】を選択します。

Step 2　設定画面が表示されます。

Step 3　各項目を選択して入力し、  ボタンで設定を保存します。

3.7.2　ユーザー情報の表示

項目の【ユーザーリスト】を選択して、登録されたユーザー情報を確認することができます。

3.8　アクセス管理

メインメニューの【アクセス】より期間、ロック解除モード、アラーム、ドアのステータス、ロック保持時間に関する設定をを行うことができます。
【アクセス】をタップして、アクセス管理インターフェイスに移動します。

3.8.1　期間管理

期間、休日期間、休日計画期間、ドア通常オン期間、ドア通常閉期間、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

番号の範囲が0～127の128の期間（週）を構成できます。
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

グループの休日を設定してから、休日グループの計画を設定できます。番号の範囲が0～127の128個のグループを構成できます。グループに16の休日を追加できます。休日グループの開始時刻と終了時刻を構成すると、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。
※名前は32文字（数字、記号、文字を含む）で入力できます。

 **ボタンをタップして休日グループ名を保存します。**

3.8.1.3　休日プランの設定

休日グループを休日計画に追加できます。休日プランを使用して、さまざまな休日グループのユーザーアクセス許可を管理できます。ユーザーは、設定した期間のみドアのロックを解除できます。

3.8.1.4　NO期間

期間がNO期間に追加される場合、ドアは通常その期間に開いています。
NO / NC期間の権限は、他の期間の権限よりも高くなっています。

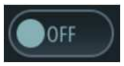
3.8.1.5　NC期間

NC期間に期間が追加された場合、ドアは通常その期間に閉じられます。
この期間、ユーザーはドアのロックを解除できません

3.8.1.6　リモート認証期間

リモート検証期間を構成した場合、構成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。この期間に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の指示が必要です。

：有効



：無効

3.8.2　アンロック

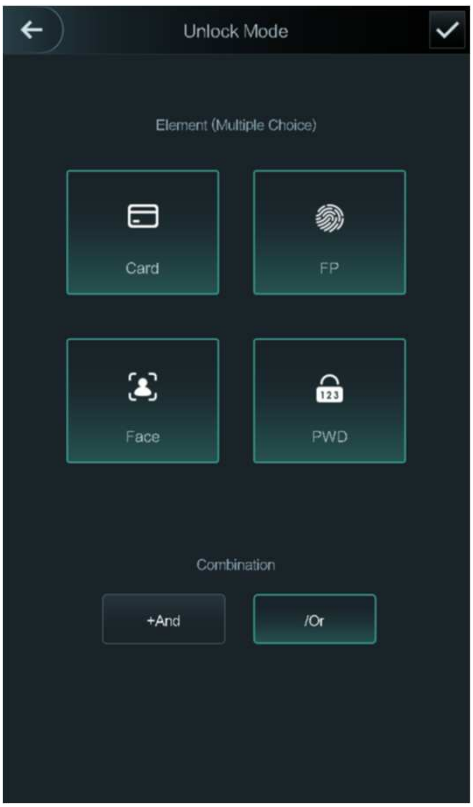
ロック解除モードには、時間帯による解除、グループの組み合わせ、測温モードのみの3つがあります。ロック解除モードはコントローラーアクセスモデルによって異なり、実際のコントローラーアクセスが優先されます。

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。

Step 1　メインメニューの【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。

図3-7



Step 2　組み合わせを選択します。

「および」は　and（プラス）を意味します。たとえば、「カード」と「パスワード」を選択した場合、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。

「または」は、orを意味します。たとえば、「カード」と「パスワード」を選択した場合、ドアのロックを解除するには、カードをスワイプするか、パスワードを入力します。

Step 3　ボタンをタップして設定を保存します。そして、ロック解除モードのインターフェースが表示されます。

ON：有効

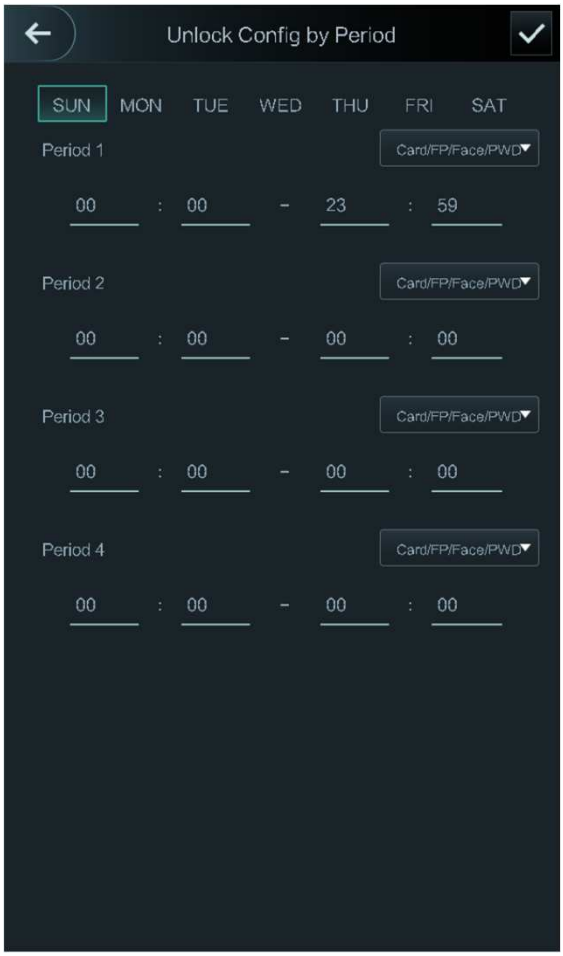
OFF：無効

3.8.2.2　時間帯によるアンロック

異なる期間に異なるロック解除モードでロック解除できます。
たとえば、期間1では、カードを介してのみロック解除できます。期間2では、顔を通してのみロックできます。

Step 1　メインメニューの【アクセス】→【アンロックモード】→【時間帯によるアンロック】を選択します。

図3-8



Step 2　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。

Step 3　ボタンをタップして設定を保存します。
ロック解除モードのインターフェースが表示されます。

：有効

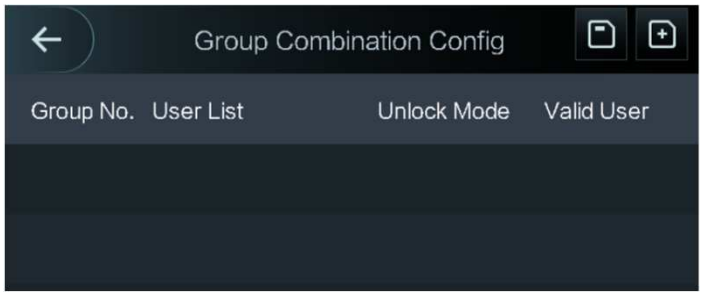
：無効

3.8.2.3　グループの組み合わせ

グループの組み合わせが有効になっている場合、ドアは3人以上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

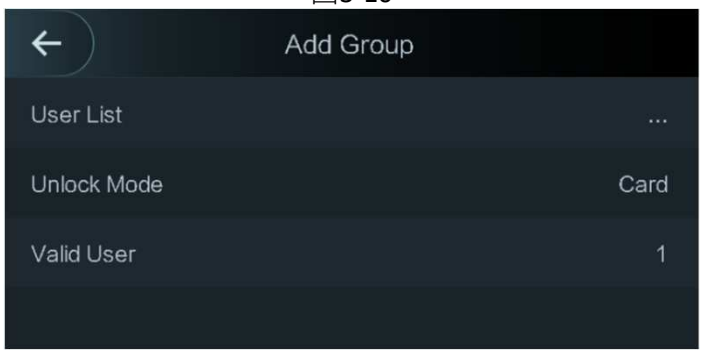
Step 1　メインメニューの【アクセス】→【アンロックモード】→【ぐるーうの組み合わせ】を選択します。

図3-9



Step 2　ボタンをタップしてグループを作成します。

図3-10



テーブル3-4

項目	詳細
ユーザリスト	新しく作成したグループにユーザーを追加します。 1.　ユーザーリストをタップします。 　　ユーザーリストインターフェイスが表示されます。 2.　ボタンをタップして、ユーザーIDを入力します。 3.　ボタンをタップして設定を保存します。
アンロックモード	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	有効なユーザーは、ロック解除権限を持つユーザーです。 ドアをロック解除できるのは、ドアをロック解除するユーザーの数が有効なユーザー数と等しい場合のみです。

Step 3　ボタンをタップして前のインターフェースに戻ります

Step 4　ボタンをタップして設定を保存します。

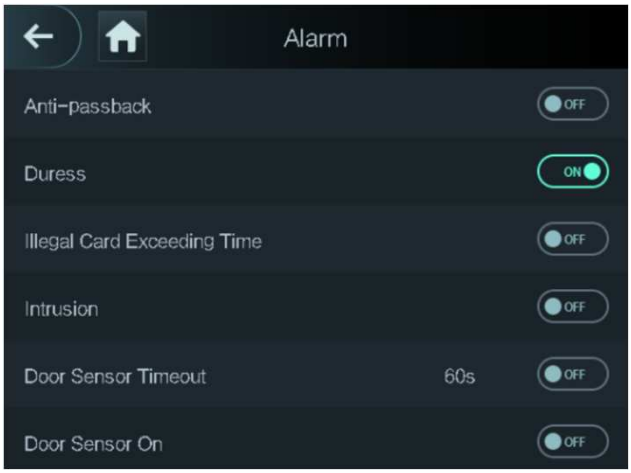
ON：有効

OFF：無効

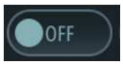
3.8.3　アラーム

管理者は、アラーム設定を通じて訪問者のロック解除権限を管理できます。
メインメニューの【アクセス】→【アラーム】を選択します。

図3-11



：有効



：無効

テーブル3-5

項目	詳細
アンチパスバック	アンチパスバックを有効にした後、ユーザーは入口と出口の両方でIDを確認する必要があります。 そうでない場合、アラームがトリガーされます。 ・IDを確認した状態で入室し、IDを確認せずに退室した場合、その人物が再び入ろうとするとアラームが トリガーされ、ドアのロックを解除する権限がなくなります。 ・IDを確認せずに人が入ると、IDを確認した状態で退出しようとするとアラームがトリガーされ、 ドアのロックを解除する権限がなくなります。
脅迫	脅迫カードまたは脅迫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。
時間を経過している不正カード	許可されていないカードを使用して50秒間に5回以上ロック解除を試みると、アラームがトリガーされます。
侵入	ドアの接点が解放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	ユーザーがドアのロックを解除するの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Iの3つのオプションがあります。

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時間です。
ロックが期間を超えてロック解除された場合、ロックは自動的にロックされます。

3.9　接続

アクセスコントローラー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
ウィーガンドポートのパラメーターを構成する必要があります。

3.9.1　ネットワーク設定

3.9.1.1　IPアドレス

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アドレスを構成します。
図3-12およびテーブル3-6を参照してください。

図3-12

テーブル3-6

項目	詳細
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が有効になっている場合、IPアドレスは自動的に取得され、
P2P	IPアドレス、サブネットマスク、ゲートウェイIPアドレスは手動で構成できません。 P2Pは、ユーザーがDDNS、ポートマッピング、または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るようにする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す。

・Webへのログインに使用するコンピューターがデバイスと同じLANにあることを確認します。
・本製品にはデュアルNICが搭載されています。 のデフォルトの管理アドレス
1000Mネットワークポートは192.168.1.108、100Mネットワークポートは192.168.2.108です。
（デフォルト）

3.9.1.2　アクティブ登録

アクティブに登録することで、アクセスコントローラー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ーを管理できます。

設定構成は管理プラットフォームでクリアでき、アクセスコントローラーを初期化できます。
不適切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。

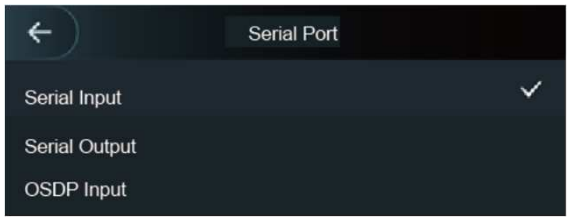
テーブル3-7

項目	詳細
サーバー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上の従属デバイス番号。

3.9.2 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てください。メインメニューの【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イスが表示されます。

図3-13

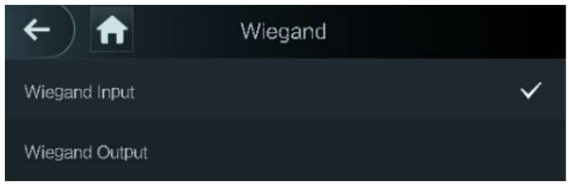


・カードの読み取りおよび書き込み機能を備えた外部デバイスがアクセスコントローラーに接続されている場合は、[シリアル入力]を選択します。シリアル入力を選択して、アクセスカード情報をアクセスコントローラーと管理プラットフォームに送信できるようにします。
・顔認識、カード読み取りおよび書き込み機能を備えたアクセスコントローラーの場合、[シリアル出力]を選択すると、アクセスコントローラーはロック/ロック解除情報をアクセスコントローラーに送信します。
ロック/ロック解除情報には次の2つのタイプがあります。
【ユーザーID】【カード番号】
・OSDPプロトコルのカードリーダーがアクセスコントローラーに接続されている場合は、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。

3.9.3 Wiegand

ウィーガンド入力またはウィーガンド出力を選択します。
メインメニューの【接続】→【Wiegand】を選択すると、ウィーガンドインターフェイスが表示されます。

図3-14



外部カードスワイプメカニズムがアクセスコントローラーに接続されている場合は、[ウィーガンド入力]を選択します。
アクセスコントローラーがコントローラーに接続できるリーダーとして機能する場合は、[ウィーガンド出力]を選択します。テーブル3-8を参照してください。

テーブル3-8

項目	詳細
Wiegand出力種別	アクセスコントローラーが認識できるカード番号または番号の桁を決定します。 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	パルス幅とパルス間隔を設定できます
パルス間隔	
	出力データの種類を選択できます。
出力データのタイプ	・ユーザーID：ユーザーIDを選択した場合、ユーザーIDが出力されます。 ・カード番号：カード番号を選択すると、カード番号が出力されます。

3.10　システム

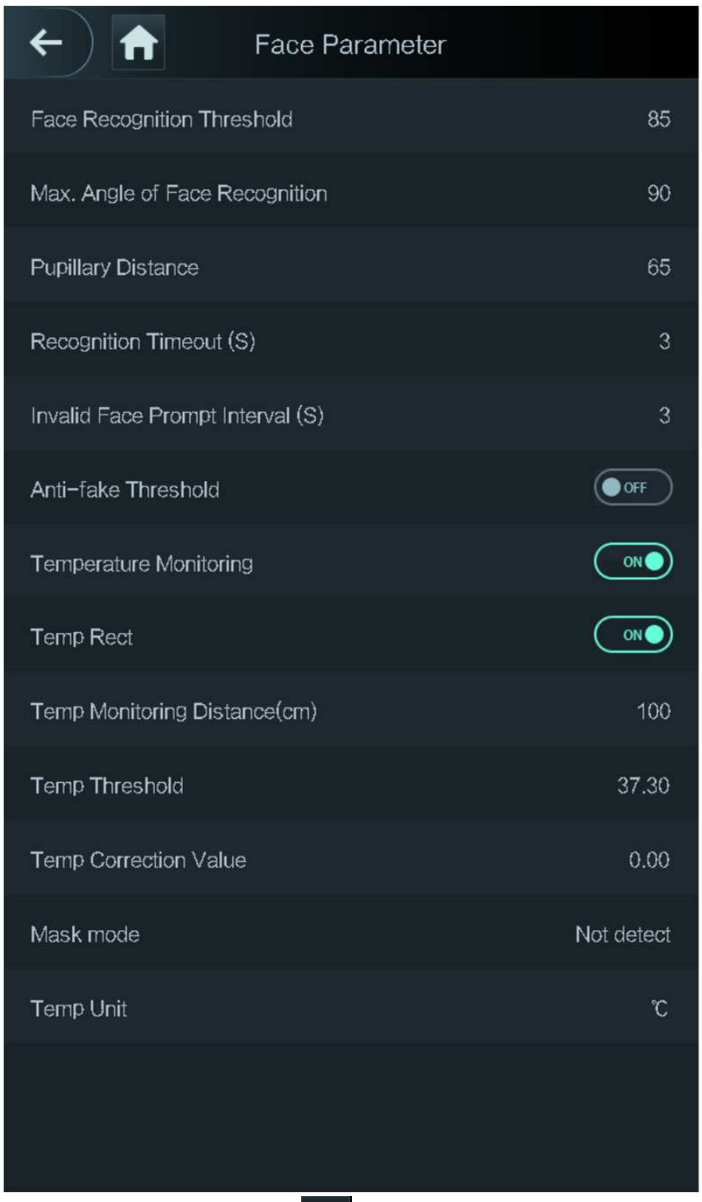
3.10.1　時間

日付形式設定、日付設定、時刻設定、DST設定、NTPチェック、タイムゾーン設定を行うことができます。

・ネットワークタイムプロトコル（NTP）を選択する場合は、最初に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アドレスを入力します。アクセスコントローラーの時間がタイムサーバーと同期されます。
・ポート：タイムサーバーのポート番号を入力します。
・間隔（分）：NPTチェック間隔。保存アイコンをタップして保存します。

3.10.2　顔パラメーター

図3-15



パラメータをタップして設定を行い、 ボタンで設定を保存します。

テーブル3-9

項目	詳細
顔認識閾値	顔認識の精度を調整できます。値が大きいほど精度が高くなります。
顔認証の最大偏角	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。 値が大きいほど、認識されるプロファイルの範囲が広くなります。
瞳孔間距離	瞳孔間距離は、各目の瞳孔の中心間の画像のピクセル値です。 アクセスコントローラー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。 顔のサイズや顔とレンズの距離によって値が変わります。顔がレンズに近いほど、値は大きくなります。 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の範囲になります。
認識アイムアウト(秒)	アクセス権を持たない人がアクセスコントローラの前に立って顔を認識させると、コントローラは顔認識に 失敗したことを通知します。プロンプト間隔は、認識タイムアウトと呼ばれます。
認識間隔（秒）	アクセス許可を持っている人がアクセスコントローラーの前に立って顔を認識させると、コントローラーは 顔認識が成功したことを通知します。プロンプト間隔は、認識間隔です。
偽造防止有効	この機能は、人間の顔画像または顔モデルによってロック解除されるのを防ぎます。 値が大きいほど、ロック解除できる顔の画像が難しくなります。推奨値は80以上で、この機能を有効にすると 顔認識の時間がかかります。
温度測定	体温測定を有効にするかどうかを設定します
測温エリア枠	測温エリア枠をディスプレイ上に表示するかどうかを設定します。有効の場合は赤枠で表示されます。
測温距離（cm）	デフォルトの値は0です。他の値を設定して、定義された距離内の温度監視を有効にします。推奨は80cm。
温度設定値（°C）	温度しきい値を設定します。測定された体温が、設定値以上であれば高温と判断します。
温度校正値（°C）	このパラメーターは補正の為です。温度監視環境の違いにより、監視温度と実際の温度に温度差が生じる場合があります。 複数の監視対象サンプルを選択し、監視対象の温度と実際の温度との比較に従って、このパラメーターによって温度偏差を修正できます。 たとえば、監視された温度が実際の温度より0.5° C低い場合、補正値は0.5° Cに設定されます。 モニターされた温度が実際の温度より0.5° C高い場合、補正値は-0.5° Cに設定されます。
マスクモデル	・テストなし：顔認識中にマスクは検出されません。 ・マスク注意：マスクは顔認識中に検出されます。マスクを着用せずに人が検出された場合、システムはマスク着用の注意を促し、ロック解除が許可されます。 ・マスク阻止：マスクは顔認識中に検出されます。マスク着用せずに人が検出された場合、システムはマスクの着用を促し、ロック解除されません。
温度単位	温度の単位を選択します。

3.10.3 画像モード設定

3つのオプションがあります。
・室内：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、「室内」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：廊下や廊下などの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」を選択します。

3.10.4 照明モード設定を記入する

必要に応じてフィルライトモードを選択できます。3つのモードがあります。
・自動：フォトセンサーが周囲環境が暗くないことを検出すると、通常、補助光はオフになります。それ以外の場合、補助ライトはオンになります。
・NO：補助ライトは通常オンです。
・NC：補助ライトは通常オフです。

3.10.5 照度設定を記入する

必要に応じて、補助光の明るさを選択できます。

3.10.6 音量

「+」または「-」ボタンをタップして音量を調整します。

3.10.7 赤外線ライト設定

暗視状態で値が大きいほど、画像が鮮明になります。

3.10.8　出荷時設定の復元

・アクセスコントローラーを工場出荷時の設定に復元すると、データが失われます。
・ただし、IPアドレスは変更されません。

ユーザー情報と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設定に復元することを選択できます。
・ユーザー情報とデバイス情報を保持したまま、アクセスコントローラーを工場出荷時の設定に復元することを選択できます。

3.10.9　リブート

リブート]をタップすると、アクセスコントローラーが再起動されます。

3.11　USB

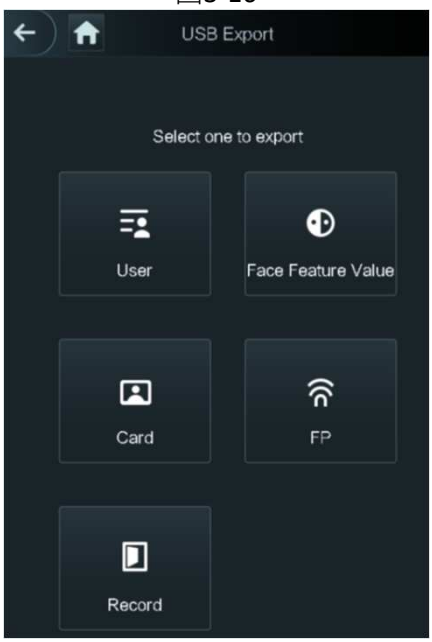
・ユーザー情報をエクスポートして更新する前に、USBが挿入されていることを確認してください。エクスポートまたは更新中は、USBを引き出したり、その他の操作を行ったりしないでください。そうしないと、エクスポートまたは更新が失敗します。
・USBを使用して別のアクセスコントローラーに情報をインポートする前に、1つのアクセスコントローラーからUSBに情報をインポートする必要があります。
・USBを使用してプログラムを更新することもできます。

3.11.1　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ており、編集できません。

Step 1　「USBエクスポート」を選択します。USBエクスポートインターフェイスが表示されます。

図3-16



Step 2　エクスポートするデータタイプを選択します。エクスポートの確認のプロンプトが表示されます。

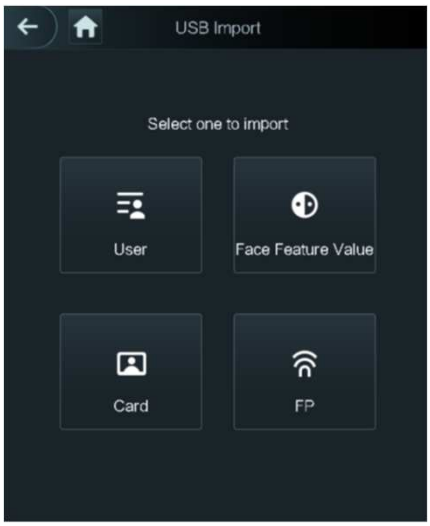
Step 3　OKをタップします。エクスポートされたデータはUSBに保存されます。

3.11.2 USBインポート

別のアクセスコントローラーにインポートできるのは、1つのアクセスコントローラーからエクスポートされたUSB内のデータのみです。

Step 1 「USBインポート」を選択します。USBインポートインターフェイスが表示されます。

図3-17



Step 2 インポートするデータタイプを選択します。インポートの確認のプロンプトが表示されます。

Step 3 OKをタップします。USBフラッシュドライブのデータがアクセスコントローラーにインポートされます。

3.11.3 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できます。

Step 1 更新ファイルの名前を「update.bin」に変更し、「update.bin」ファイルをUSB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ーがデバイスと同じLANにあることを確認します。
7インチモデルXアクセスコントローラには、デュアルNICが搭載されています。
1000Mネットワークポートのデフォルトの管理アドレスは192.168.1.108で、100Mネットワークポートのデフォルトの管理アドレスは192.168.2.108です。

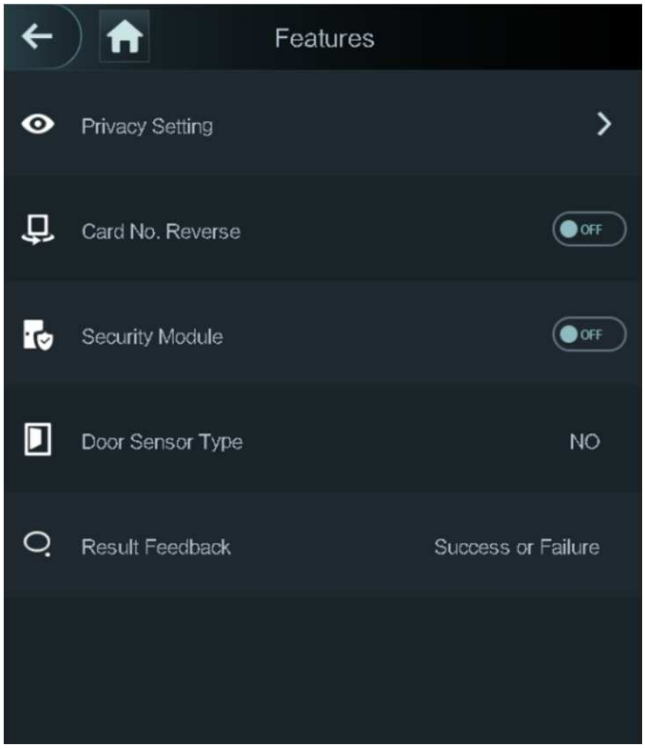
Step 2 「USB更新」を選択します。更新の確認のプロンプトが表示されます

Step 3 OKをタップします。更新が開始され、更新が完了するとアクセスコントローラーが再起動します。

3.12　特徴

プライバシー、カード番号の反転、セキュリティモジュール、ドアセンサーの種類、および結果のフィードバックに関する設定を行うことができます。
上記の関数の詳細については、図3-18およびテーブル3-10を参照してください。

図3-18

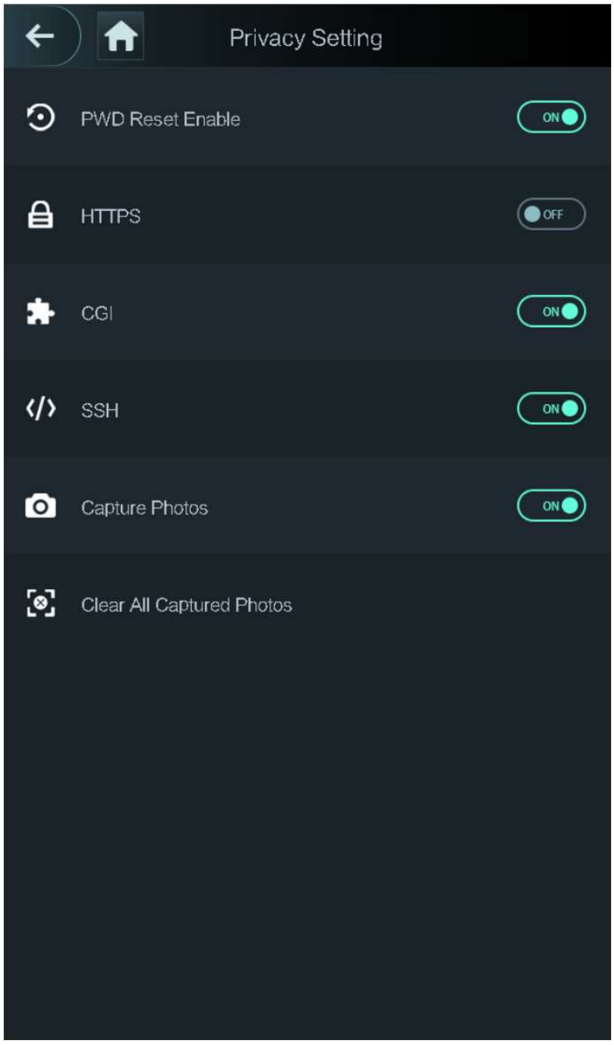


テーブル3-10

項目	詳細
プライバシー設定	詳細は「3.12.1プライバシー設定」を参照してください。
カード番号逆順	サードパーティのカードリーダーをウィーガンド出力ポートを介してアクセスコントローラーに 接続する必要がある場合は、カード番号逆機能を有効にする必要があります。そうしないと、プロトコルの不一致が原因で、 アクセスコントローラとサードパーティのカードリーダー間の通信が失敗する可能性があります。
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、アクセス制御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個の電源を必要とします。 ・セキュリティモジュールが有効になると、終了ボタン、ロックコントロール、および消防リンケージは無効になります。
ドアセンサーのタイプ	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	ロック解除が成功したか失敗したかを表示します。

3.12.1　プライバシー設定

図3-19



テーブル3-11

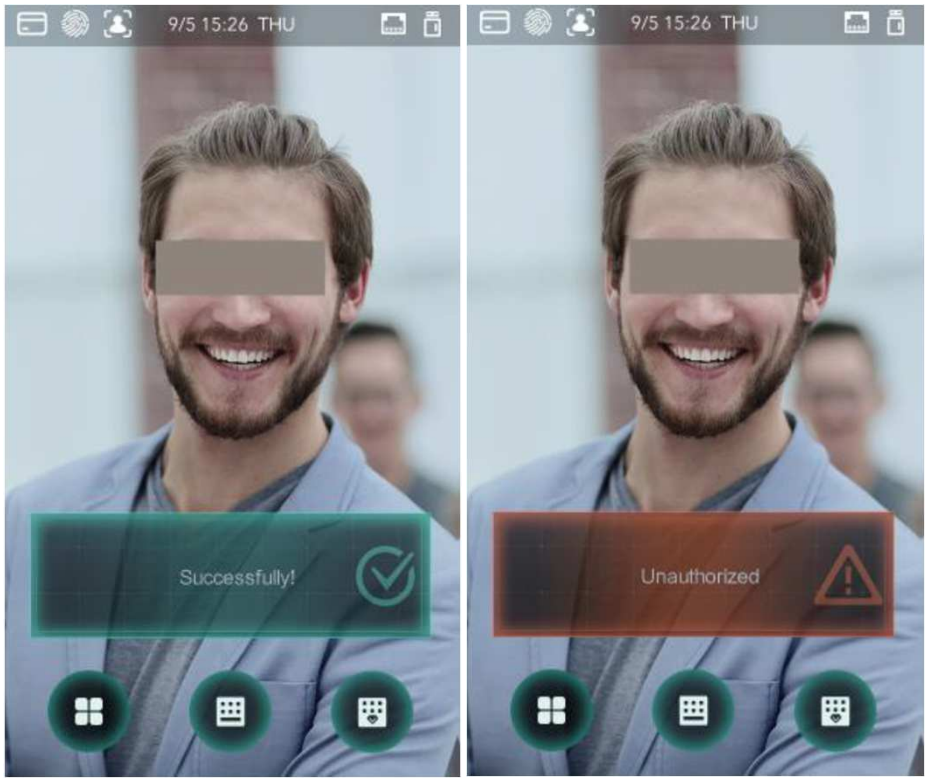
項目	詳細
パスワードリセットの有効化	パスワードリセットイネーブル機能が有効になっている場合、パスワードをリセットできます。 この機能はデフォルトで有効になっています。
HTTPS	ハイパーテキスト転送プロトコルセキュア（HTTPS）は、コンピューターネットワークを介した安全な通信のためのプロトコルです。 HTTPSが有効な場合、HTTPSを使用してCGIコマンドにアクセスします。それ以外の場合は、HTTPが使用されます。 **HTTPSが有効に設定変更した場合、アクセスコントローラーは自動的に再起動します。**
CGI	Common Gateway Interface（CGI）は、WebサーバーがWebページを動的に生成するサーバー上で実行されてい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実行するためのWebサーバー用の標準プロトコルを提供します。 CGIが有効になっている場合、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、セキュリティで保護されてい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が有効になっている場合、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	[オン]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。
キャプチャした写真をすべて消去	アイコンをタップすると、撮影した写真をすべて削除できます。

3.12.2　結果フィードバック

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。

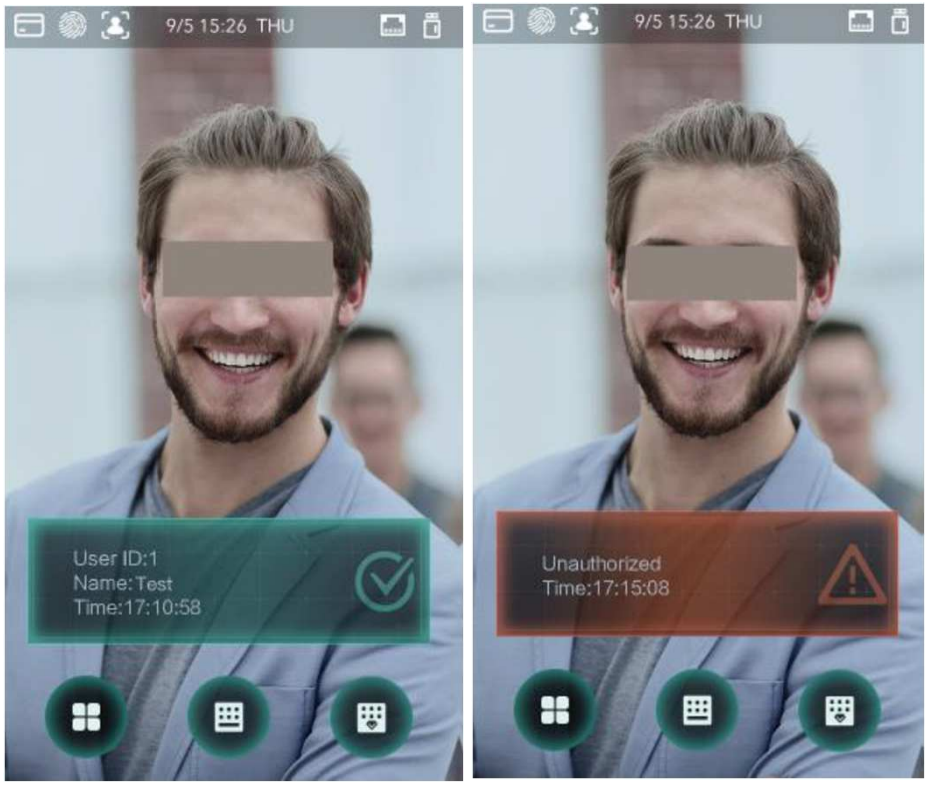
成否

図3-20



名前のみ

図3-21

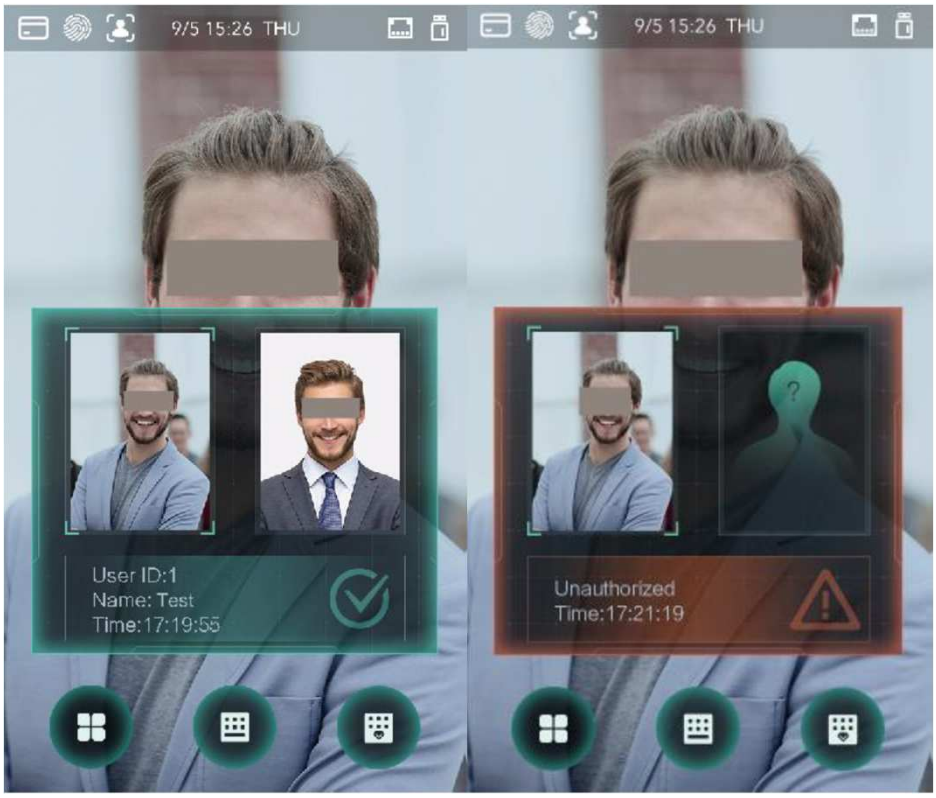


ユーザーの写真と名前

図3-22

写真比較と名前

図3-23



3.13 録画

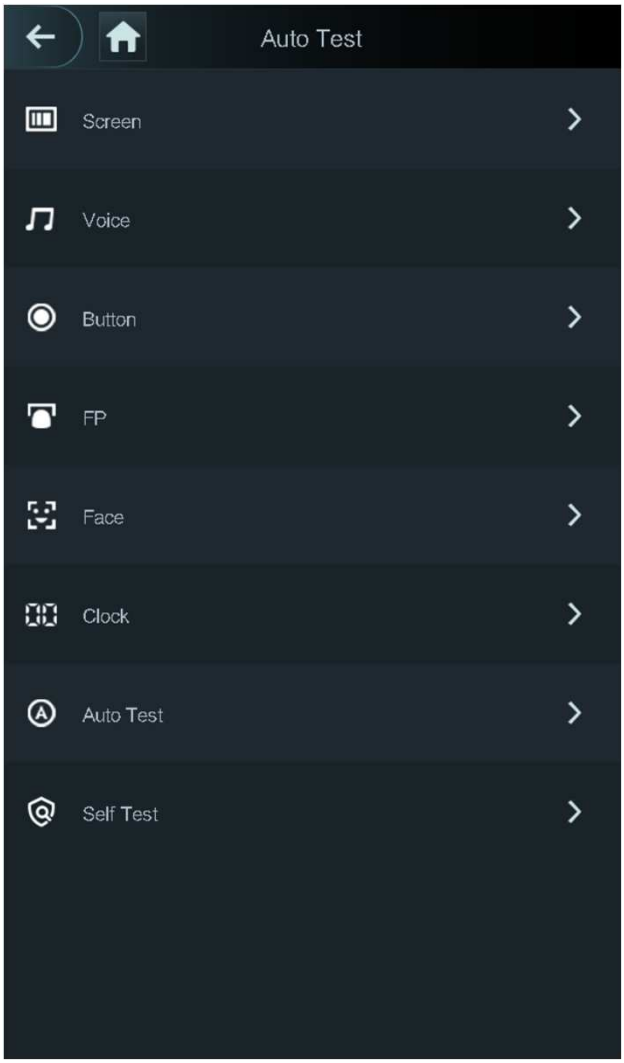
すべてのロック解除レコードを照会できます。

図3-24

3.14　自動テスト

アクセスコントローラーを初めて使用するとき、またはアクセスコントローラーが故障したときに、自動テスト機能を使用して、アクセスコントローラーが正常に動作するかどうかを確認できます。プロンプトに従ってアクションを実行します。

図3-25



自動テストを選択すると、アクセスコントローラーがすべての自動テストを実行するように案内します。

3.15　装置情報

システム情報インターフェイスで、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、およびファームウェア情報を表示できます。

4 Web 操作

アクセスコントローラは、Web上で設定または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ー、ビデオパラメーター、
およびアクセスコントローラーパラメーターを設定できます。
また、システムを保守および更新することもできます。

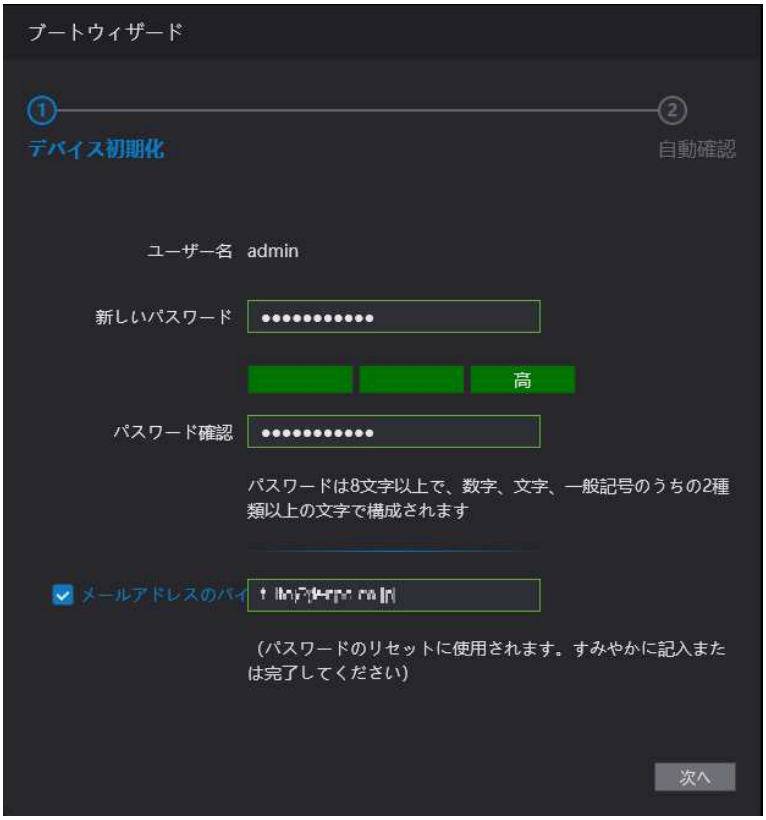
4.1 ブートウィザード（初期化後）

初めてWebにログインする前に、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。
Step 1 IE Webブラウザーを開き、アドレスバーにアクセスコントローラーのIPアドレス
（デフォルトのアドレスは192.168.1.108）を入力して、Enterキーを押します。

注意

- IE 8以上で使用してください。IE8未満だとログインできない可能性があります。
- Webへのログインに使用するコンピューターがデバイスと同じLANにあることを確認します。
- 本製品はデュアルNICがあります。
  1000Mネットワークポートのデフォルトアドレスは192.168.1.108、
  100Mネットワークポートのデフォルトアドレスは192.168.2.108です。

図4-1ブートウィザード



Step 2 新しいパスワードを入力し、パスワードを確認し、電子メールアドレスを入力して、
【次へ】をクリックします。

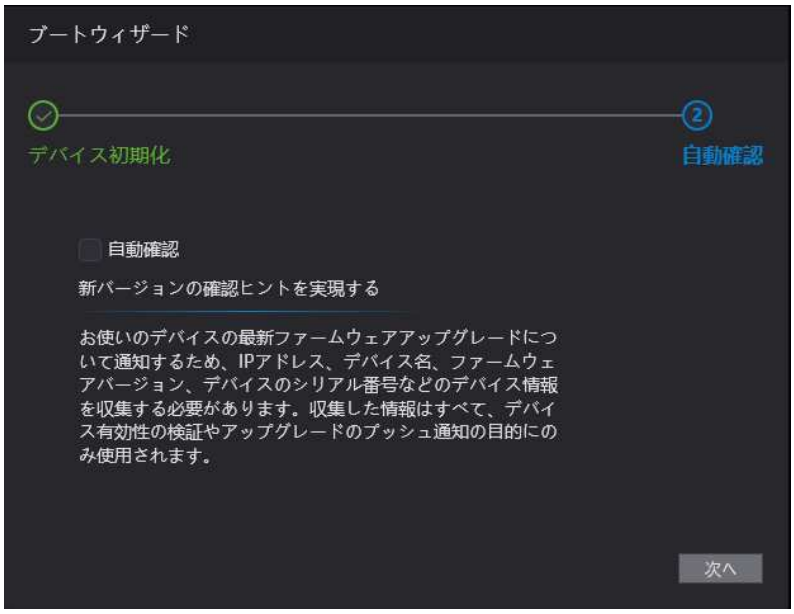
注意

- パスワードは、8～32文字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。
  パスワード強度のプロンプトに従って、セキュリティレベルの高いパスワードを設定します。

・定期的にパスワードを変更することをお勧めします。
・QRコードをスキャンして管理者パスワードをリセットする必要がある場合、
セキュリティコードを受信す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。

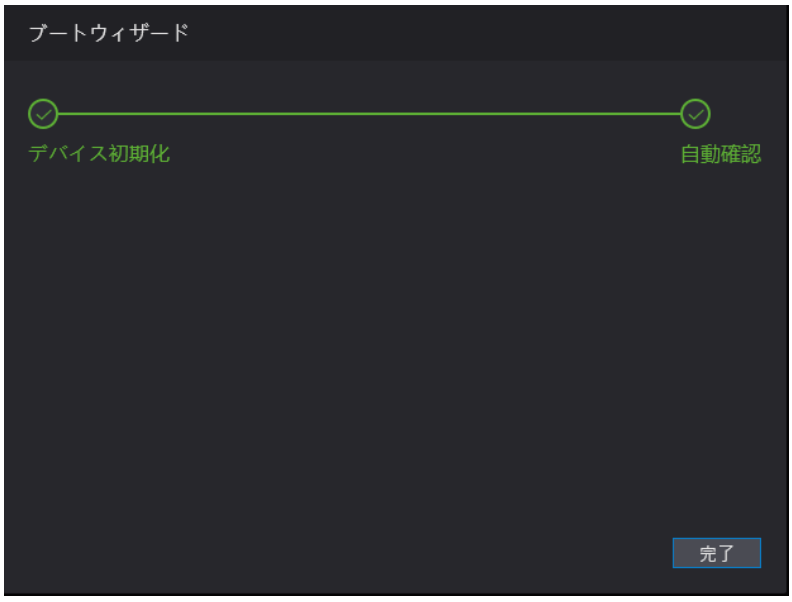
図4-2自動確認



Step 4 自動確認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取得するには、自動確認を選択することをお勧めします。

Step 5 【次へ】をクリックします。

図4-3設定完了



Step 6 「完了」をクリックすると、初期化が完了します。
Webログイン画面が表示されます。

4.2 ログイン

Step 1　IE ブラウザーを開き、アドレスバーにアクセスコントローラーのIPアドレスを入力して、Enterキーを押します。

※IE 8以上で使用してください。IE8未満だとログインできない可能性があります。
Webへのログインに使用するコンピューターがデバイスと同じLANにあることを確認します。
本製品はデュアルNICがあります。
1000Mネットワークポートのデフォルトipアドレスは192.168.1.108、
100Mネットワークポートのデフォルトアドレスは192.168.2.108です。

図4-4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で、パスワードは初期化後のログインパスワードです。
管理者のログインパスワードを忘れた場合は、[パスワードをお忘れですか？]を選択し、
リセットしまします。詳しくは【4.3パスワードのリセット】を参照してください。

Step 3　【ログイン】をクリックし、Webインターフェースに入ります。

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、メールアドレスが必要になります。

Step 1　ログイン画面の「パスワードを忘れた場合？」をクリックします。

ヒントウインドウが表示されます。

図4-5 ヒント

Step 2　ヒントを読み、【OK】ボタンをクリックします。

パスワードのリセットインターフェイスが表示されます。

図4-6 パスワードのリセット

Step 3　QRコードをスキャンすると、セキュリティコードを取得できます。

同じQRコードをスキャンすると、最大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、さらにセキュリティコードを取得するには、QRコードを更新してください。

QRコードをスキャンした後に取得したコンテンツを指定のメールアドレスに送信する必要があります。その後、セキュリティコードを取得します。
暗証番号はお受け取りから24時間以内にご利用ください。
24時間以上経過した場合は無効になります。
間違ったセキュリティコードを5回続けて入力すると、
管理者は5分間、凍結します。ご注意ください。

Step 4　受け取ったセキュリティコードを入力します。

Step 5　【次へ】ボタンをクリックします。
パスワードのリセット画面が表示されます。

Step 6　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文字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）の少なくとも2種類の文字を含む必要があります。

Step 7　【保存】ボタンをクリックしてリセット完了です。

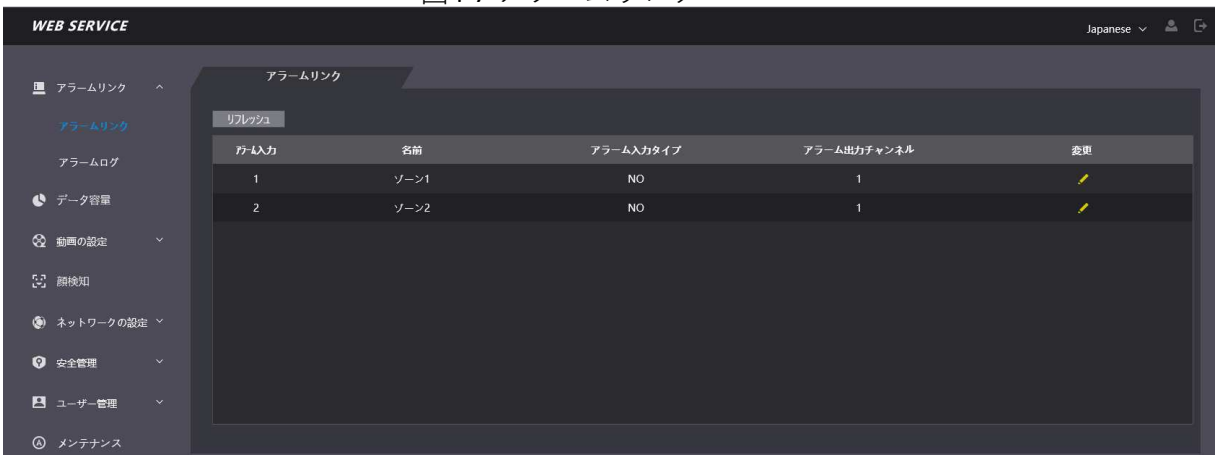
4.4 アラームリンク

4.4.1 アラームリンク設定

アラーム入力デバイスはアクセスコントローラーに接続でき、必要に応じてアラームリンクパラメーターを変更できます。

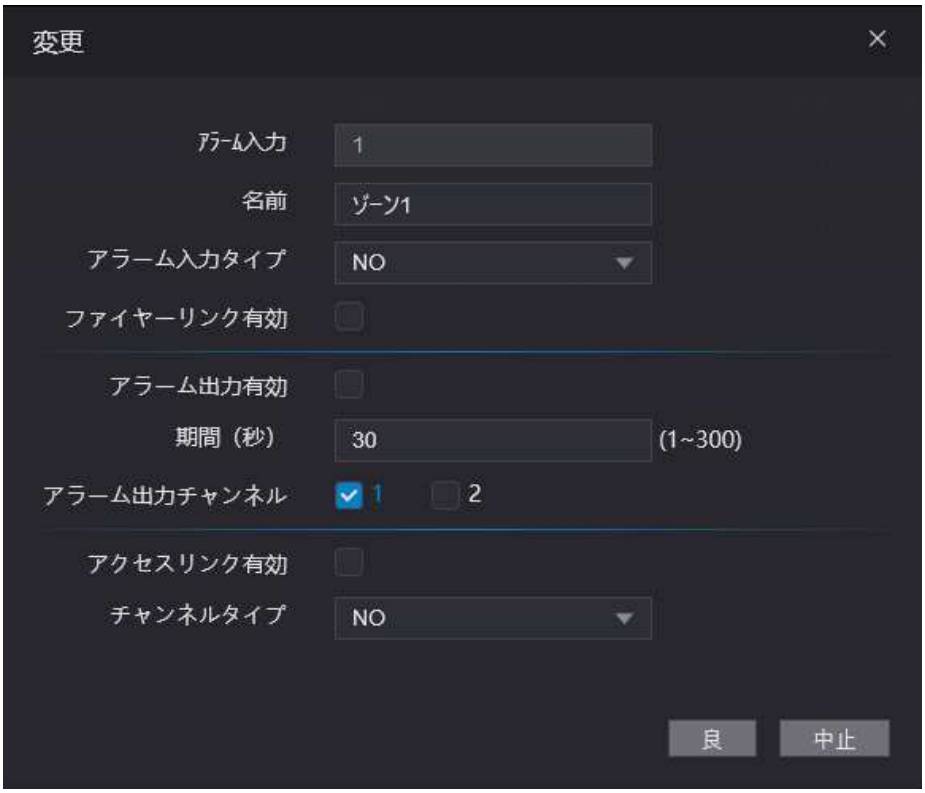
Step 1　画面左側のメニュ画面から【アラームリンク】を選択します。

図4-7 アラームリンク



Step 2　  　をクリックするとアラームリンクの内容を変更できます。

図4-8　アラーム連動項目



テーブル4-1　アラーム連動項目詳細

項目	詳細
アラーム入力	値を変更することはできません
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つから選択します アラーム機器のタイプがNO(ノーマルオープン)の場合はNOを選択 それ以外の場合は、NC(ノーマルクローズ)を選択
ファイヤーリンク有効	チェック時、火災警報がトリガーされたときに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 **※アラーム出力とアクセスリンクはNO(デフォルト)です**
アラーム出力有効	アラーム出力が有効な場合、リレーはアラーム情報を出力できます （管理プラットフォームに送信されます）
期間（秒）	アラームの持続時間(1～300秒)
アラーム出力チャンネル	設置した警報器に合わせて警報出力チャンネルを選択 各警報装置はチャネルと見なすことができます
アクセスリンク有効	入力アラーム信号がある場合、アクセスコントローラーは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	NOとNCの2つから選択します

Step 3　【良】ボタンをクリックすると設定が保存されます。

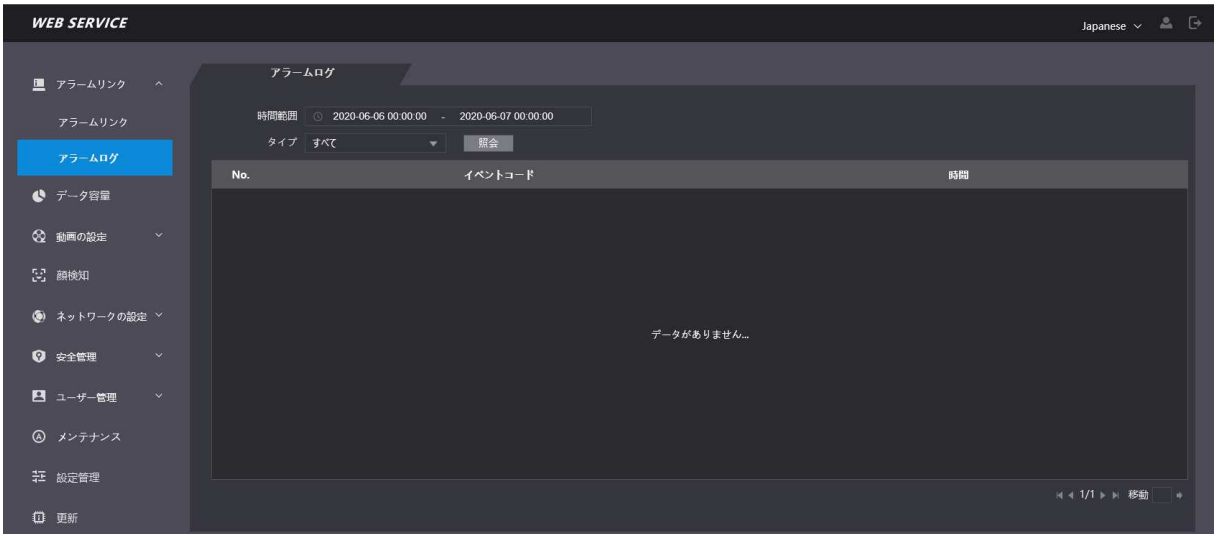
※アクセスコントローラーがクライアントに追加されている場合、
Web上の構成はクライアントの構成と同期されます。

4.4.2 アラームログ

アラームログ画面でアラームタイプと時間範囲を表示できます。

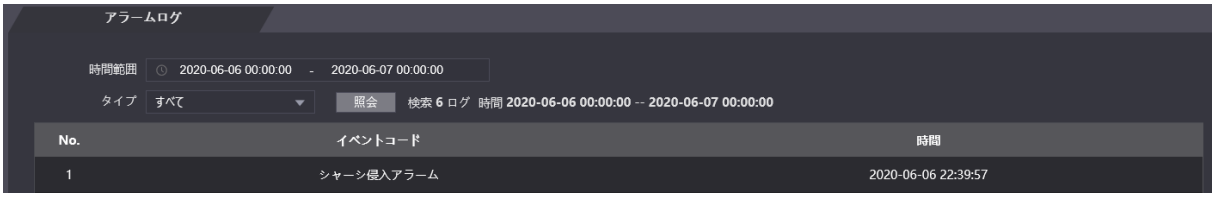
Step 1　アラームリンク⇒アラームログから画面が表示されます。

図4-9　アラームログ



Step 2　時間範囲とアラームタイプを選択し、【照会】ボタンをクリックします。
結果が表示されます。

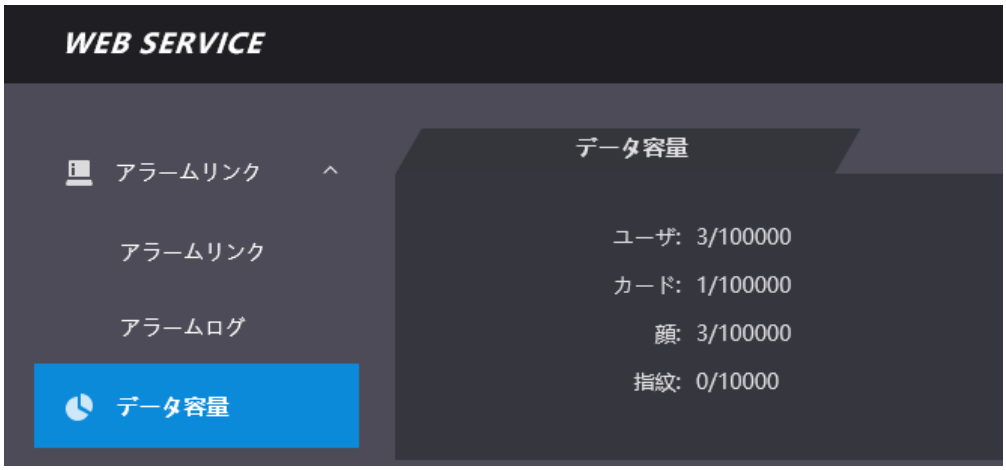
図4-10　アラーム検索結果



4.5 データ容量

本製品が保持できるユーザー、カード、顔の画像数のデータ容量を確認できます。

図4-11　データ容量



4.6 動画の設定

ビデオ設定インターフェイスで、データレート、画像パラメーター（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ーを設定できます。

4.6.1 レート

図4-12　レート

テーブル4-2　レートパラメーター詳細

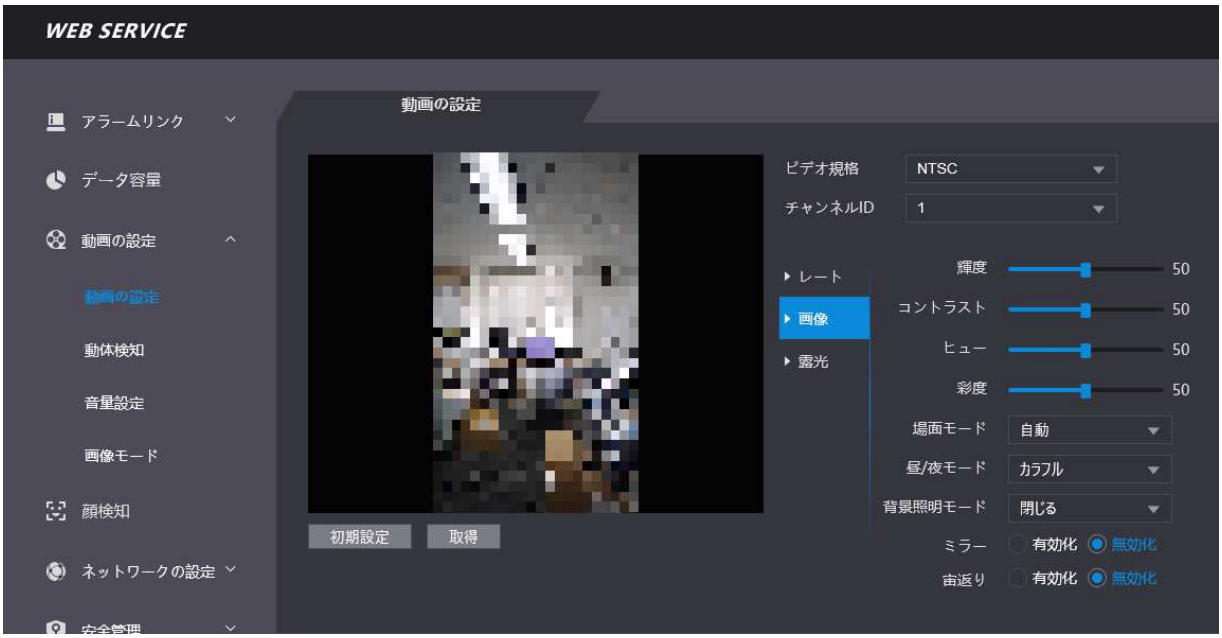
項目		詳細
ビデオ規格		NTSCとPALの2つから選択。お住まいの地域のビデオ規格に従った標準を選択。
チャンネルID		1と2の選択。1：白色光カメラ／2：IR光カメラ
一次レート	動画リスト	D1、VGA、720p、1080pの4つから選択
	フレームレート	1秒間に表示するフレーム数（30で動画）1~30で選択
	ビットレート	2Mbps、4Mbps、6Mbps、8Mbps、10Mbpsの5つから選択
レート	動画リスト	D1、VGA、QVGAの3つから選択
	フレームレート	1秒間に表示するフレーム数（30で動画）1~30で選択
	ビットレート	512Kbps,640Kbps,768Kbps,896Kbps,1024Kbps,1.25Mbps,1.5Mbps,1.75Mbps,2Mbpsから選択

4.6.2 画像

2つのチャネルがあり、各チャネルのパラメーターを構成する必要があります。

Step 1　動画の設定⇒動画の設定⇒画像から画面が表示されます。

図4-13　画像



Step 2　背景照明モードで【ワイドダイナミック】を選択します。

テーブル4-3　画像

項目	詳細
輝度	値が大きくなるほど明るくなります。
コントラスト	値が大きくなるほど画像の明暗差が大きく出ます。
ヒュー	値が大きくなるほど色が濃くなります。
彩度	値が大きくなるほど明るくなります。 **※画像の輝度は変更しません。**
場面モード	閉じる：モード無し 自動：場面を自動的に調整します。 晴天：このモードでは、画像の色相が減少します。 夜間：このモードでは、画像の色合いが増加されます。
昼/夜モード	カラー・白黒表示モード 自動：自動的にカラーと白黒表示に切り替えます。 カラフル：カラー表示固定となります。 白黒：白黒表示固定になります。
背景照明モード	閉じる：逆光補正無し 逆光：バックライト補正は、非常に高いまたは低いレベルの光で領域を補正し、 焦点の合ったオブジェクトに対して通常の使用可能なレベルの光を維持します。 ﾜｲﾄﾞﾀﾞｲﾅﾐｯｸ：明暗差のある領域を補正します。 抑制：強力な光源がある場合、光源を抑えるようにします。
ミラー	有効にすると、左右画像が反転します。
宙返り	有効にすると、上下画像が反転します。

4.6.3 露光

テーブル4-4　露光

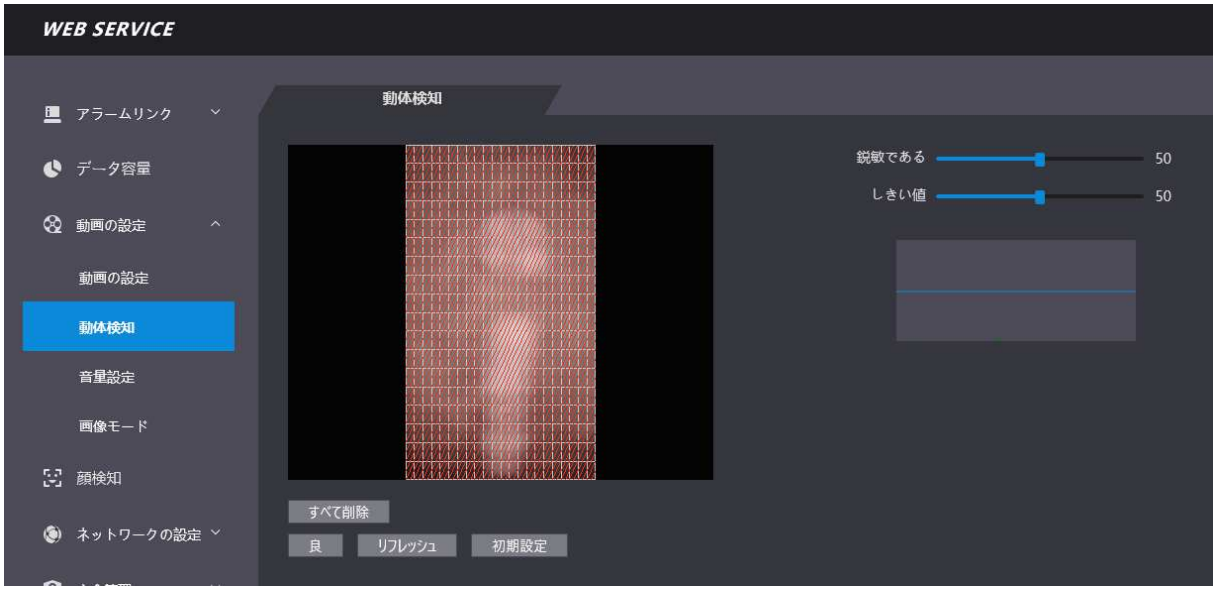
項目	詳細
明滅防止	50Hz：画面にフリッカーが出る場合選択します。 60Hz：周波数が60Hzの場合選択します。 屋外：屋外設置の場合選択します。
露光モード	自動：輝度を自動的に調整します。 手動：ゲインとシャッター値を手動で設定して、画像の明るさを調整できます。
シャッター	シャッター値が大きいほど、画像は暗くなります。**※露光モードで手動選択時**
ゲイン	ゲイン値の範囲を設定すると、ビデオ品質が向上します。**※露光モードで手動選択時**
露出補正	露出補正値を調整することにより、ビデオの輝度を上げることができます。
3D NR	3Dノイズリダクション（RD）を有効にすると、ビデオノイズを低減でき、高解像度ビデオが生成されます。
等級	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 動体検知

動体を検知できる範囲を設定します。

Step 1　【動画の設定】⇒【動体検知】を選択します。動体検知インターフェースが表示されます。

図4-14　動体検知



Step 2　マウスの左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。
動体検知エリアが表示されます。

赤い長方形はモーション検知エリアです。デフォルトのモーション検知範囲はすべての長方形です。
モーション検知領域を描画するには、最初に【すべて削除】をクリックする必要があります。
デフォルトのモーション検出領域に描画すると、描画するモーション検出領域は非モーション検出領域になります。

Step 3　感度としきい値を設定します。

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知の条件です。
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も小さい場合、緑色の線が表示されます。 グリッド番号がしきい値を超えると、赤い線が表示されます。

Step 4　【良】ボタンで設定します。

4.6.5 音量設定

スピーカーの音量調整ができます。

図4-15　音量設定

4.6.6 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ーが屋内に設置されている場合は、【室内】を選択します。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。通路や廊下などのバックライトがある場所にアクセスコントローラーが設置されている場合は、【その他】を選択します。

図4-16　画像モード

4.7 顔検知

顔に関連するパラメータを設定して、顔認識の精度を高めることができます。

Step 1　【顔検知】を選択します。顔検知が表示されます。

図4-17　顔検知

Step 2　設定を変更する場合は、【良】をクリックします。

テーブル4-5　顔検知

項目	詳細
顔認識閾値	値が大きいほど精度が高くなります。
顔認識の最大角度	角度が大きいほど、より広い範囲が認識されます。
偽造防止有効	この機能は、写真の顔画像または顔模型によってロック解除されるのを防ぎます。 有効化にすると認証スピードが遅くなります。
照度設定を記入する	白光ライトの明るさを設定できます。
照明モード設定を記入する	3つの白光ライトモードがあります。 NO：常時白光ライトが点灯します。 NC：常時白光ライトは消灯します。 自動：モーション検出イベントがトリガーされると、白光ライトが自動的にオンになります。 ※自動を選択すると、赤外線ライトの値が19を超えていても、白光ライトはオンになりません。
赤外線	スクロールバーをドラッグして赤外線の明るさを調整します。
認識タイムアウト	顔と認識するまでの最大時間（1~6秒）
認識間隔	アクセス権があるかどうかを認識するまでの最大時間（1~6秒）
瞳孔間距離	瞳孔間距離は、各目の瞳孔の中心間の画像のピクセル値です。アクセスコントローラー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。顔のサイズや顔とレンズの距離によって値が変わります。 顔がレンズに近いほど、値は大きくなります。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の範囲になります。
チャンネルID	1と2から選択。1は白色光カメラ、2はIRライトです。
顔露光を有効にする	顔の露出を有効にすると、人間の顔がより鮮明になります。屋外設置の場合は有効化してください。
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を描画できます。【すべて削除】をクリックするとフレームを削除します。
検知領域	【検知領域】をクリックすると顔検出領域を調整できます。【すべて削除】をクリックすると領域を削除します。
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てください。
顔露光間隔検出時間	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光を発します。 設定した間隔が経過するまで、アクセスコントローラは再び光を発しません。
体温検知	**体温測量：**体温検知を有効にするかどうかを設定します。 **温度単位：**温度単位を選択します。 **測温エリア枠：**温度測定範囲のボックスを表示するかどうかを設定します。 **測温距離(cm)：**デフォルトの値は0です。他の値を設定して、定義された距離内の温度監視を有効にします。推奨80cm **温度設定値（℃）：**警告する閾値を設定します。検知された体温は、設定値以上であれば高温と判断します。 **温度校正値（℃）：**温度監視環境の違いにより、監視温度と実際の温度に温度差が生じる場合があります。 監視温度と実際の温度の比較に応じて、このパラメーターで温度偏差を補正できます。
マスクモデル	**テストなし：**顔認識中にマスクは検出されません。 **マスク注意：**マスク着用の有り無しが判別され、マスクを着用せずに人が検出された場合、システムはマスクの着用を促し、許可されます。 **マスク阻止：**マスク着用の有り無しが判別され、マスクを着用せずに人が検出された場合、システムはマスクの着用を促し、許可されません。

4.8 ネットワークの設定

4.8.1 TCP/IP

アクセスコントローラーが他のデバイスと通信できるようにするには、IPアドレスとDNSサーバー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。

Step 1　【ネットワークの設定】⇒【TCP/IP】を選択します。

図4-18　TCP/IP

テーブル4-6　TCP/IP

項目	詳細
NIC	1000Mと100Mから選択します。
IPバージョン	IPv4のみサポートしています。
MACアドレス	本製品の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：**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を構成できなくなります。 DHCPが有効な場合、IPアドレス、サブネットマスク、および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、およびゲートウェイアドレスはすべてゼロになります。
IPアドレス	IPアドレスを入力してから、サブネットマスクとゲートウェイアドレスを構成します。 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サーバーのIPアドレスを設定します。
代替DNSサーバー	代替DNSサーバーのIPアドレスを設定します。

Step 2　設定を変更する場合は【良】をクリックして保存してください。

4.8.2 ポート

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とポート番号を設定します。

Step 1　【ネットワークの設定】⇒【ポート】を選択します。
ポートの画面が表示されます。

Step 2　各ポート番号を設定します。

値を変更した後で構成を有効にするには、アクセスコントローラーを再起動する必要があります。

テーブル4-7　ポート

項目	詳細
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。 Smart PSS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。他の値をポート番号として使用する場合は、 ブラウザから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。

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します。

Step 1　【ネットワークの設定】⇒【登録】を選択します。
登録の画面が表示されます。

Step 2　【有効化】にチェックし、ホストIP、ポート、サブデバイスIDを入力します。

項目	詳細
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	自動登録に使用されるサーバーポート。
サブデバイスID	サーバーによって割り当てられたアクセスコントローラーID。

4.8.4 P2P

ピアツーピアコンピューティングまたはネットワーキングは、ピア間でタスクまたはワークロードを分割する分散アプリケーションアーキテクチャです。
ユーザーはQRコードをスキャンしてモバイルアプリケーションをダウンロードし、アカウントを登録して、モバイルアプリで複数のアクセスコントローラーを管理できます。
動的ドメイン名を適用したり、ポートマッピングを行ったり、トランジットサーバーを必要としたりする必要はありません。

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。そうでない場合、アクセスコントローラーは使用できません。

図4-19　P2P

Step 1　【ネットワークの設定】⇒【P2P】を選択します。
登録の画面が表示されます。

Step 2　【有効化】にチェックを入れます。

Step 3　【良】をクリックします。

QRコードをスキャンして、アクセスコントローラーのシリアル番号を取得します。

4.10 安全管理

4.10.1 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てください。

図4-21　IP権限

4.10.2.1 システムサービス

SSH、PWDリセット有効、CGI、HTTPSの4つのオプションがあります。
「3.12機能」を参照して、1つまたは複数を選択してください。
Webページで行われたシステムサービス構成とアクセスコントローラーの機能インターフェイスの構成が同期されます。

図4-22　システムサービス

4.10.2.2 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[保存]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。

4.10.2.3 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。

4.11 ユーザー管理

ユーザーを追加および削除したり、ユーザーのパスワードを変更したり、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メールアドレスを入力したりできます。

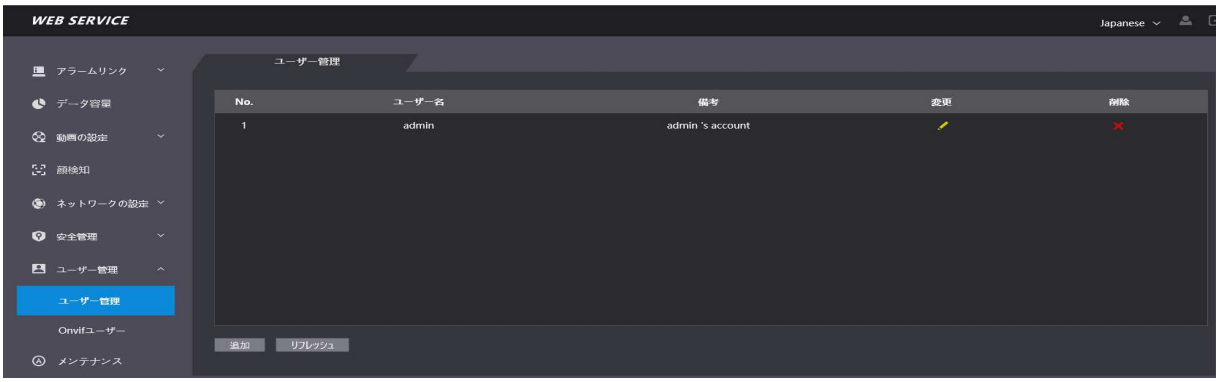
4.11.1 ユーザー追加

ユーザー管理で【追加】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イス、およびユーザー名、パスワード、確認済みパスワード、およびコメントを入力します。
【良】をクリックして、ユーザーの追加を完了します。

4.11.2 ユーザー情報変更

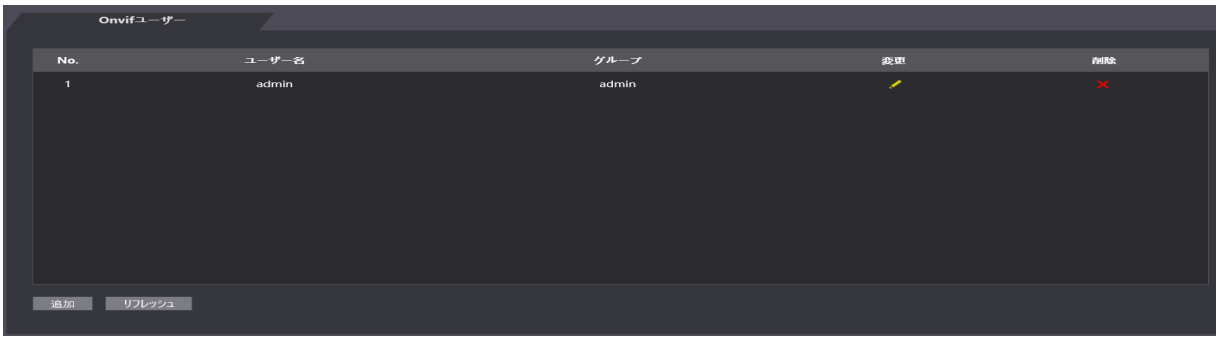
変更  をクリックするとユーザー情報を変更できます。

図4-23　ユーザー管理



4.11.3 Onvifユーザー情報変更

オープンネットワークビデオインターフェースフォーラム（ONVIF）。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。ONVIFを使用する場合、管理者、オペレーター、およびユーザーはONVIFサーバーの異なる権限を持ちます。必要に応じてonvifユーザーを作成します。



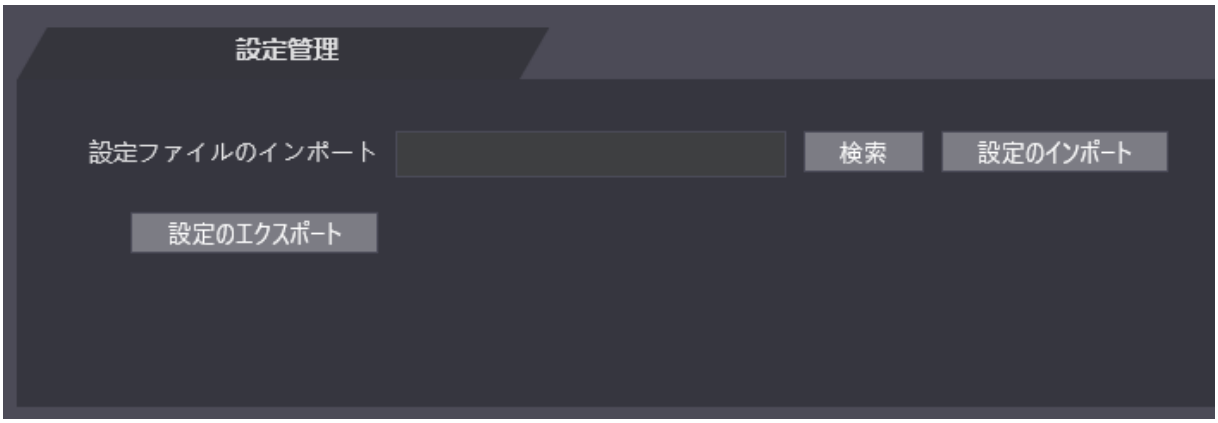
4.12 メンテナンス

アクセスコントローラーをアイドル時間に再起動して、アクセスコントローラーの実行速度を向上させることができます。自動再起動の日付と時刻を設定する必要があります。デフォルトの再起動時間は火曜日の午前2時です。【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ーがすぐに再起動します。【良】をクリックすると、アクセスコントローラーが毎週火曜日の午前2時に再起動します。

4.13 設定管理

複数のアクセスコントローラーが同じ構成を必要とする場合、構成ファイルをインポートまたはエクスポートすることにより、それらのパラメーターを構成できます。

図4-24　設定管理



4.14 更新

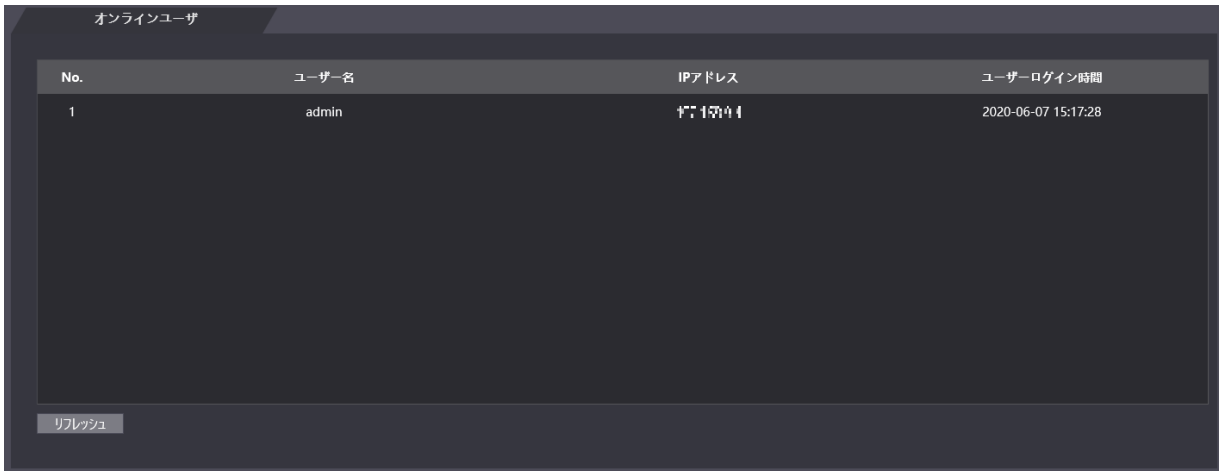
FWを手動でアップグレードできます。
また、オンライン状態であれば、自動でアップグレードすることも可能です。

4.15 バージョン情報

MACアドレス、シリアル番号、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などの情報を表示できます

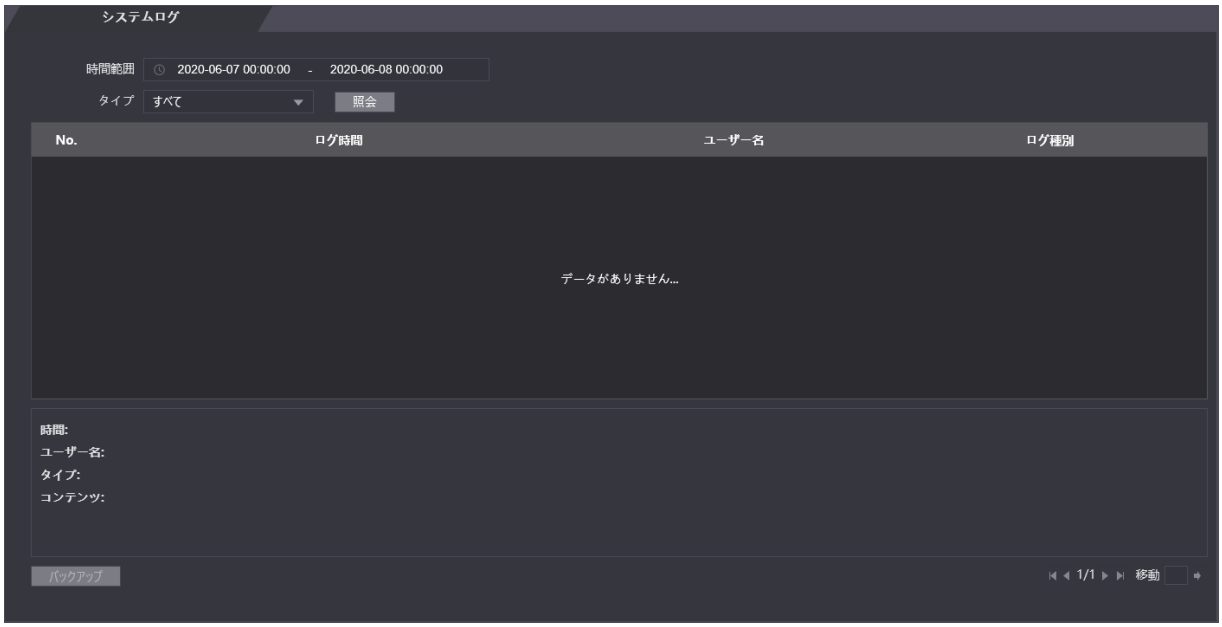
4.16 オンラインユーザー

ユーザー名、IPアドレス、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。



4.17 システムログ

システムログインターフェイスでシステムログを表示およびバックアップできます。



4.17.1 照会ログ

時間範囲とそのタイプを選択し、【照会】をクリックすると、条件を満たすログが表示されます。

4.17.2 バックアップ

表示されたログをバックアップするには、【バックアップ】をクリックします。

4.17.3 管理ログ

管理者ログインターフェイスで管理者IDを入力し、【照会】をクリックすると、管理者の操作記録が表示されます。


にマウスカーソルを合わせると、現在のユーザーの詳細情報が表示されます。

4.18 ログアウト


このアイコンをクリックするとログアウトします。。

5 FAQ

1　電源投入後、アクセスコントローラーが起動しません。

⇒12V電源が正しく接続されているか、電源ボタンが押されているかを確認します。

2　アクセスコントローラーの電源を入れた後、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ます。
「3.8.2ロック解除」を参照してください。
アクセス>ロック解除モード>グループの組み合わせで、ロック解除モードとして顔が選択されていることを確認します。
「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ーと外部コントローラーがWiegandポートに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ーのGNDケーブルと外部コントローラーが接続されているか確認してください。

4　管理者のパスワードを忘れてしまい設定に入ることができない。

⇒プラットフォームから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ーをリモートでロック解除してください。

5　ユーザー情報と顔画像をアクセスコントローラーにインポートできません。

⇒システムはタイトルでファイルを識別するため、XMLファイルの名前とテーブルのタイトルが変更されたかどうかを確認します。

6　ユーザーの顔は認識されているが、他のユーザーの情報が表示されてしまう。

⇒人間の顔をインポートするときは、周囲に人がいないことを確認してください。
登録された顔データを削除して、もう一度登録し直してください。
システム→顔パラメータ→顔認識閾値の数値を大きくしてみてください。

付録1　温度監視の注意事項

・電源投入後20分以上にわたって温度監視ユニットを
ウォームアップして、温度監視ユニットが熱平衡に達するようにします。

・温度監視ユニットを室内の無風環境に設置し、室内の周囲温度を
15°C～32°Cに維持してください。

・温度監視ユニットに直射日光が当たらないようにしてください。

・温度監視ユニットを光源のあるガラスに向けて設置しないでください。

・温度監視ユニットを熱源から離して設置してください。

・日光、風、冷気、冷房と温風の空調などの要素は、人体の表面温度に
影響を及ぼし、監視されている温度と実際の温度との間に温度偏差が
発生します。

・発汗は、体が自動的に冷えて熱を放散する方法でもあります。これにより、
監視されている温度と実際の温度との間に温度偏差が生じます。

・定期的に（2週間ごとに）温度監視ユニットを保守してください。
温度センサーと距離センサーの表面にあるほこりを柔らかくほこりの出ない
布でやさしく拭いて、清潔に保ちます。

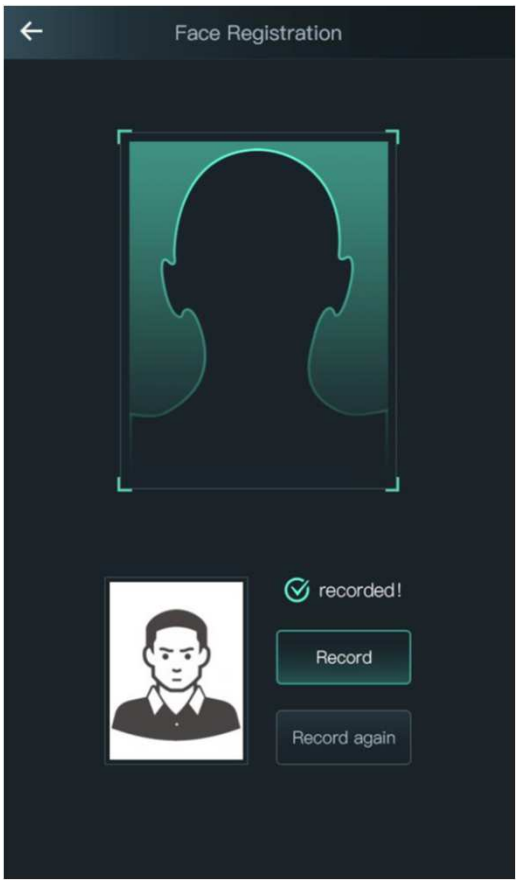
付録2　顔のメモ
記録/比較

登録前

・メガネ、帽子、ひげは、顔認識のパフォーマンス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覆わないでください。
・デバイスを使用する場合は、ひげのスタイルを大幅に変更しないでください。
顔認識がうまくできない可能性があります。
・顔を清潔に保ちます。
・デバイスを光源から少なくとも2メートル、窓またはドアから少なくとも
3メートル離れた位置に設置してください。逆光や直射日光の影響で顔認識
パフォーマンスに影響を与える可能性があります。

登録中

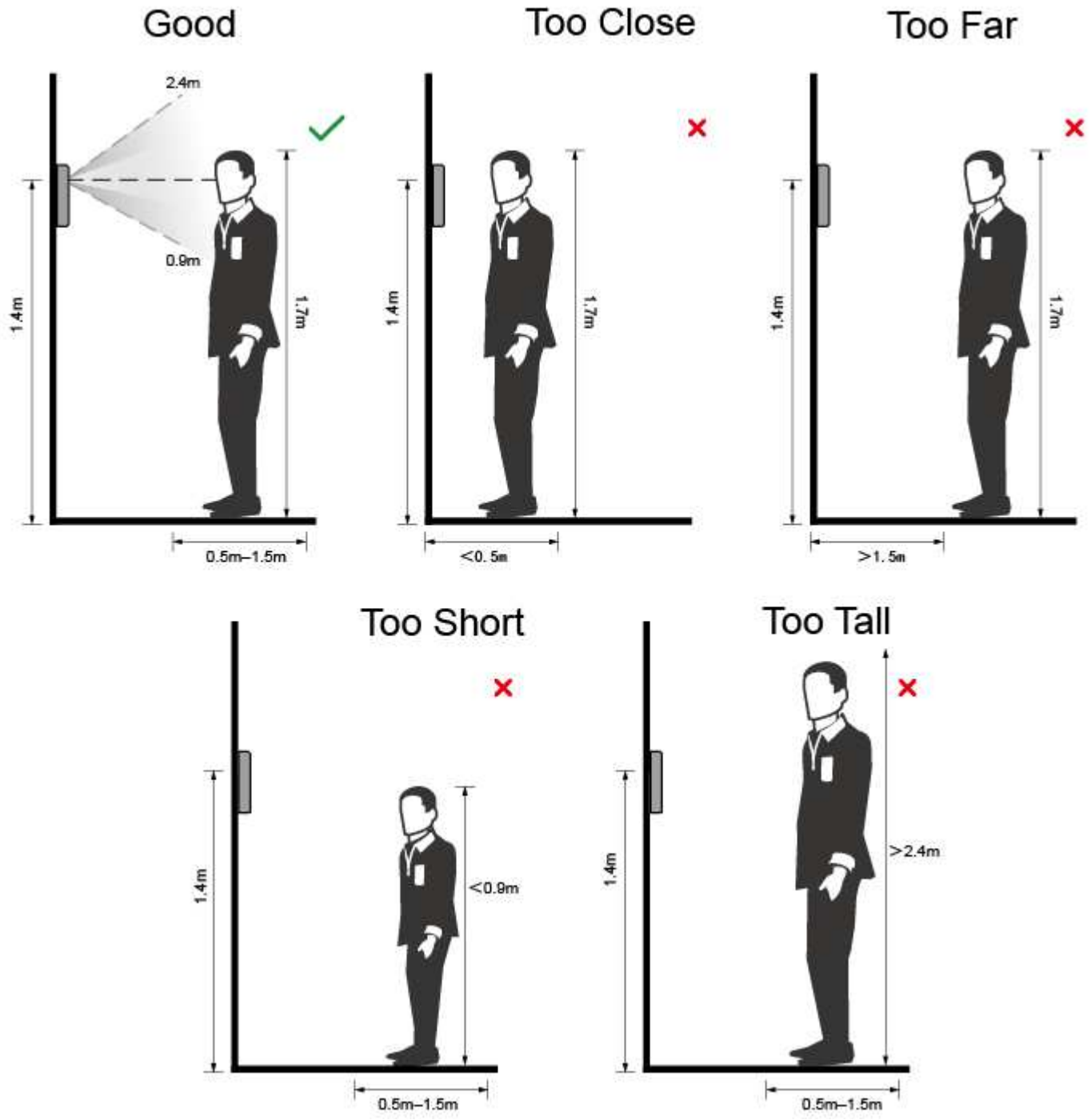
アクセスコントローラまたはプラットフォームを介して顔を登録できます。
プラットフォームを介した登録については、プラットフォームのユーザーマニュアルを参照してください。フォトキャプチャフレームの頭の中心を作成します。
あなたの顔の写真が自動的にキャプチャされます。



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つの顔が同時にキャプチャフレームに表示されないようにしてください。

顔の位置

顔が適切な位置にない場合、顔認識に影響を与える可能性があります。



顔の登録・認識条件

・顔全体が覆われていなく、額が髪で覆われていないことを確認してください。
・顔画像の記録に影響を与えるメガネ、帽子、ひげ、その他の顔の装飾品を着用しないでください。
・目を開けて、顔の表情なしで、顔をカメラの中心に向けます。
・顔を記録するとき、または顔を認識しているときは、顔をカメラに近づけたり遠ざけたりしないでください。

・管理プラットフォームを介して顔画像をインポートする場合は、
画像の解像度が150×300～600×1200の範囲内であることを確認してください。
（画像のピクセルが500×500以上、画像サイズは75 KB未満で、画像名と個人IDは同じ）

・顔が画像領域全体の2/3を占めておらず、アスペクト比が1：2を超えていないことを確認してください。

付録3　サイバーセキュリティの推奨事項

サイバーセキュリティは単なる流行語ではありません。
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係します。
IPビデオ監視はサイバーリスクの影響を受けにくいですが、
ネットワークやネットワーク化されたアプライアンスを保護および強化するための
基本的な手順を実行することで、攻撃の影響をさらに受けにくくなります。
以下は、より安全なセキュリティシステムを作成するためのヒントと推奨事項です。

基本的な機器のネットワークセキュリティのために実行する必要があるアクション：

1.強力なパスワードを使用する

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文字以上でなければなりません。
・少なくとも2種類の文字を含みます。文字タイプは、大文字と小文字、数字、記号が含まれます。
・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などの重複文字を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更新する

・標準手順に従って、システム（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プログラムが確実にインストール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、「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。
・クライアントソフトウェアの最新バージョン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ための推奨事項：

1.物理的保護
機器、特にストレージデバイスを物理的に保護することをお勧めします。たとえば、特別なコンピュータルームとキャビネットに機器を配置し、よく行われたアクセス制御許可とキー管理を実装し、ハードウェアの損傷、リムーバブル機器（USBフラッシュディスクなど）の不正な接続など、許可されていない人物が物理的な接触を実行するのを防ぎます。
2.パスワードを定期的に変更する
推測またはクラックされ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、タイムリーな情報のリセット
機器はパスワードリセット機能をサポートしています。エンドユーザーのメールボックスやパスワード保護に関する質問など、パスワードをリセットするための関連情報をすぐに設定してください。情報が変更された場合は、時間内に変更してください。パスワード保護の質問を設定するときは、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する
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。アカウントのセキュリティを確保するために、この機能をオンにしておくことをお勧めします。攻撃者が間違ったパスワードで数回ログインしようとすると、対応するアカウントとソース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を変更する
デフォルトのHTTPおよびその他のサービスポートを1024から65535の間の任意の数のセット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
安全な通信チャネルを通じて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.ホワイトリストを有効にする
ホワイトリスト機能を有効にして、指定されたIPアドレスを持つ人を除く全員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。したがって、必ずコンピュータのIPアドレスと付属機器の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アドレスを機器にバインドして、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.アカウントと権限を適切に割り当てる
ビジネス要件および管理要件に従って、合理的にユーザーを追加し、最小限の権限セットをユーザーに割り当てます。
10.不要なサービスを無効にし、セキュアモードを選択する
不要な場合は、リスクを減らすために、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、セーフモードを使用することを強くお勧めします。これには、次のサービスが含まれますが、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ー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.オーディオおよびビデオ暗号化送信
オーディオおよびビデオデータの内容が非常に重要または機密である場合は、暗号化された送信機能を使用して、送信中にオーディオおよびビデオデータが盗まれるリスクを軽減することをお勧めします。
注意：暗号化された伝送は、伝送効率のいくらかの損失を引き起越す可能性があります。
12.安全な監査
・オンラインユーザーを確認する：オンラインユーザーを定期的に確認して、デバイスが不正にログインしていないか確認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アドレスとその主要な操作を確認できます。
13.ネットワークログ
機器の保存容量には限りがあるため、保存されるログは限られています。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と同期してトレースでき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を構築する
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、次のことをお勧めします。
・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ニーズに応じて分割および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、ネットワークGAP、およびその他のテクノロジーを使用してネットワークを分割し、ネットワーク分離効果を実現することをお勧めします。
・802.1xアクセス認証システムを確立して、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します。
・デバイスが攻撃されるリスクを軽減するために、デバイスのファイアウォールまたはブラックリストとホワイトリストの機能を有効にすることをお勧めします。