顔認識アクセスコントローラー

取扱説明書

V1.0.1

はじめに

全般

このマニュアルでは、顔認識アクセスコントローラー（以下、「アクセスコントローラー」と呼びます）のインストールと基本操作について説明します。）

安全指示

定義された意味を持つ以下の分類された注意喚起語がマニュアルに表示される場合があります。

注意喚起	意味
注意	テキストの強調と補足として追加情報を提供します。

改訂履歴

ヴァージョン	改訂内容	発売日
V1.0.0	初版	2020年4月

マニュアルについて

■このマニュアルは参照専用です。マニュアルと実際の製品との間に矛盾がある場合、実際の製品が優先されます。

■マニュアルに準拠していない操作によって生じた損失については責任を負いません。

■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。詳細については、紙のマニュアル、CD−ROM、QRコード、または当社の公式Webサイトを参照してください。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。

■すべてのデザインとソフトウェアは、事前の書面による通知なしに変更される場合があります。製品の更新により、実際の製品とマニュアルの間に違いが生じる場合があります。最新のプログラムと補足資料については、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、機能と操作の説明にずれがある、または印刷に誤りがある可能性があります。疑問や不明点がある場合は、最終説明をご参照ください。

■マニュアル（PDF形式）を開けない場合は、リーダーソフトウェアをアップグレードするか、

■他の主流のリーダーソフトウェアを試してください。

■マニュアル内のすべての商標、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、当社のWebサイトにアクセスし、サプライヤーまたはカスタマーサービスにお問い合わせください。

重要な安全対策と警告

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ご一読いただき、今後の参照のために保管してください。

操作要件

■太陽光が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、ほこり、すすから離してください。

■落下防止のために、アクセスコントローラーを安定した場所に水平に設置してください。

■アクセスコントローラーに液体を溢したり、かけたりしないでください。
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、アクセスコントローラーの周囲に液体がないことをご確認ください。

■換気の良い場所にアクセスコントローラーを設置し、換気を妨げないでください。

■電源入力と出力の定格範囲内でアクセスコントローラーを操作してください。

■アクセスコントローラーを分解しないでください。

■許可された湿度と温度条件下でアクセスコントローラーを使用、保管してください。

電気の安全

■バッテリーの不適切な使用は、火災、爆発、または炎症を引き起こす可能性があります。

■バッテリーを交換するときは、同じモデルが使用されていることをご確認ください。

■地域で推奨され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。
怪我やデバイスの損傷につながる可能性があるため、アクセスコントローラーに付属の電源アダプターをご使用ください。

■電源は、Safety Extra Low Voltage（SELV）規格の要件に適合し、IEC60950-1に基づく制限電源要件に適合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であることにご注意ください。

■デバイス（I型構造）を保護接地付きの電源ソケットに接続します。

■アプライアンスカプラーは切断装置です。
カプラーを使用するときは、簡単に操作できるように角度を保ちます。

目次

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、指紋、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のがアクセスコントロールパネルです。

1.2 機能

■顔、ICカード、指紋、パスワードのロック解除をサポート。 期間ごとにロックを解除します。

■顔検出ボックス付き。 同時に現れる顔の中で最大の顔が最初に認識されます。
Webで最大顔サイズを設定できます。

■2MP広角WDRレンズ。 自動/手動補助光。

■顔とカメラの距離：0.3 m～2.0 m。 人間の身長：0.9 m-2.4 m

■顔認識アルゴリズムにより、端末は人間の顔の360を超える位置を認識できます。

■顔認証精度> 99.5%; 低い誤認識率。

■プロファイル認識をサポートします。 プロファイル角度は0°～90°です。

■活性検出をサポート

■強要アラームと改ざんアラームをサポート

■一般ユーザー、強要ユーザー、パトロールユーザー、ブラックリストユーザー、
VIPユーザー、ゲストユーザー、および障害のあるユーザーをサポートする。

■4つのロック解除ステータス表示モードとさまざまな音声プロンプトモード

1.3 寸法とコンポーネント

アクセスコントローラには7インチと10インチのアクセスコントローラの2つのタイプがあります。
図 1-1 ～ 図 1-4をご参照ください。

7インチアクセスコントローラー

図1-1 寸法とコンポーネント（1）（mm [inch]）

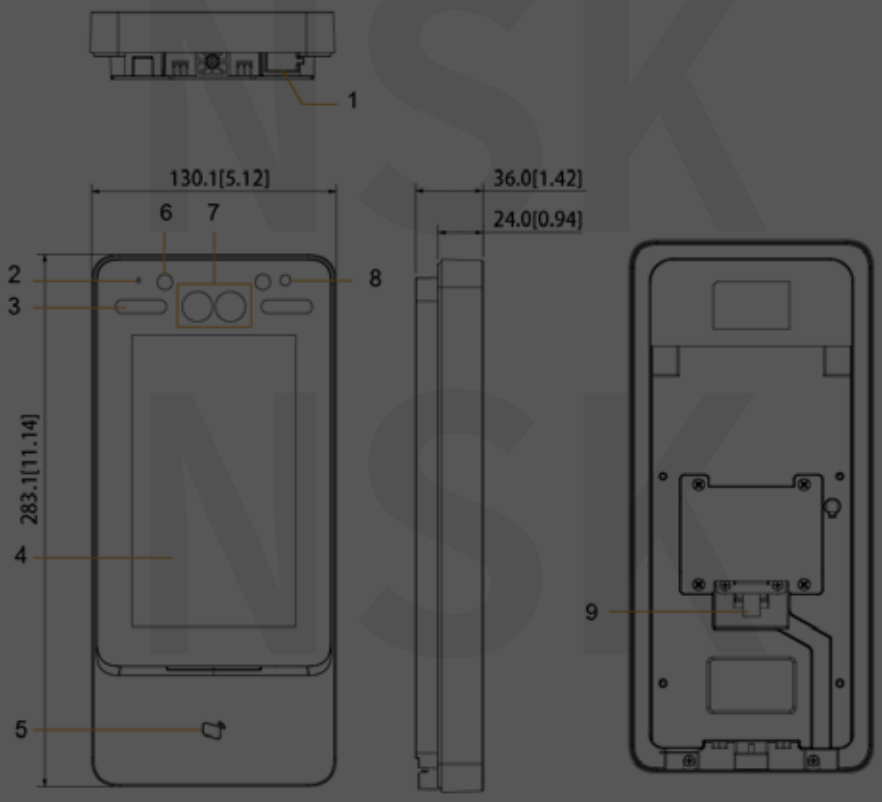


表1-1コンポーネントの説明（1）

No.	名前	No.	名前
1	USBポート	6	IR ライト
2	MIC	7	デュアルカメラ
3	ホワイトフィルライト	8	フォトトランジスタ
4	表示	9	ケーブルの入り口
5	カードスワイプエリア	–	–

図 1-2寸法とコンポーネント（2）（mm [inch]）

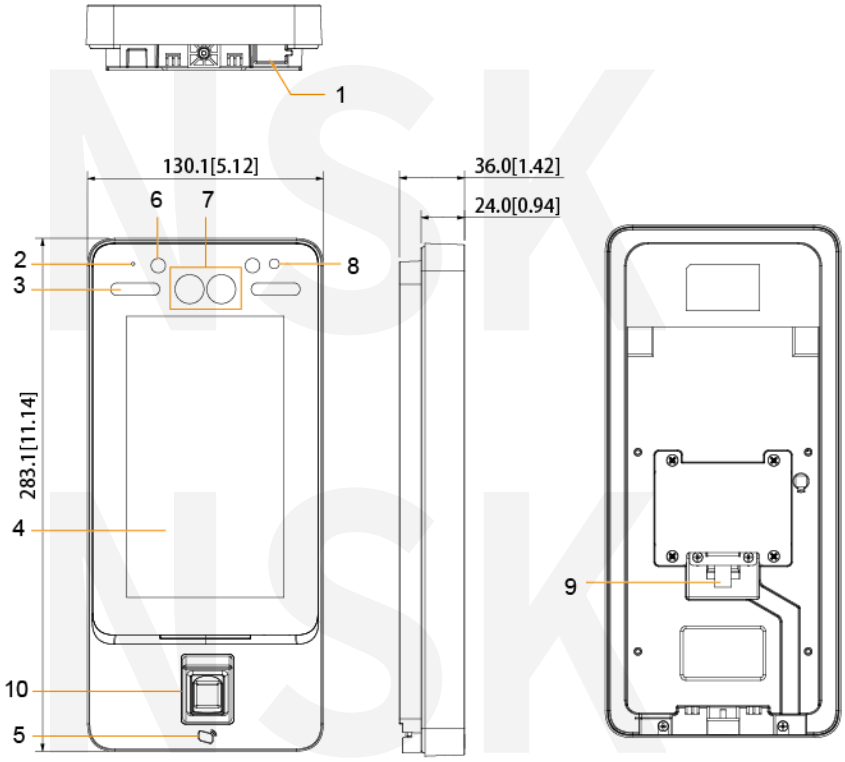


表 1-2コンポーネントの説明（2）

No.	名前	No.	名前
1	USBポート	6	IRライト
2	MIC	7	デュアルカメラ
3	ホワイトフィルライト	8	フォトトランジスタ
4	表示	9	ケーブルの入り口
5	カードスワイプエリア	10	指紋センサー

10インチアクセスコントローラー

図 1-3寸法とコンポーネント（3）（mm [inch]）

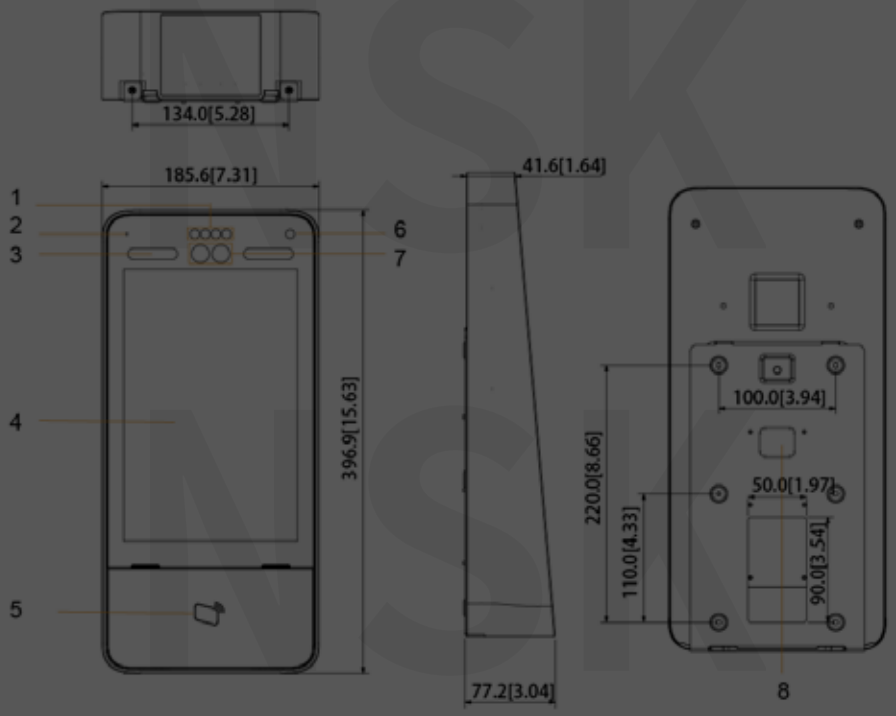


表 1-3コンポーネントの説明（3）

No.	名前	No.	名前
1	USBポート	6	フォトトランジスタ
2	MIC	7	デュアルカメラ
3	ホワイトフィルライト	8	ケーブルの入り口
4	表示	9	–
5	カードスワイプエリア	10	–

図 1-4寸法とコンポーネント（4）（mm [inch]）

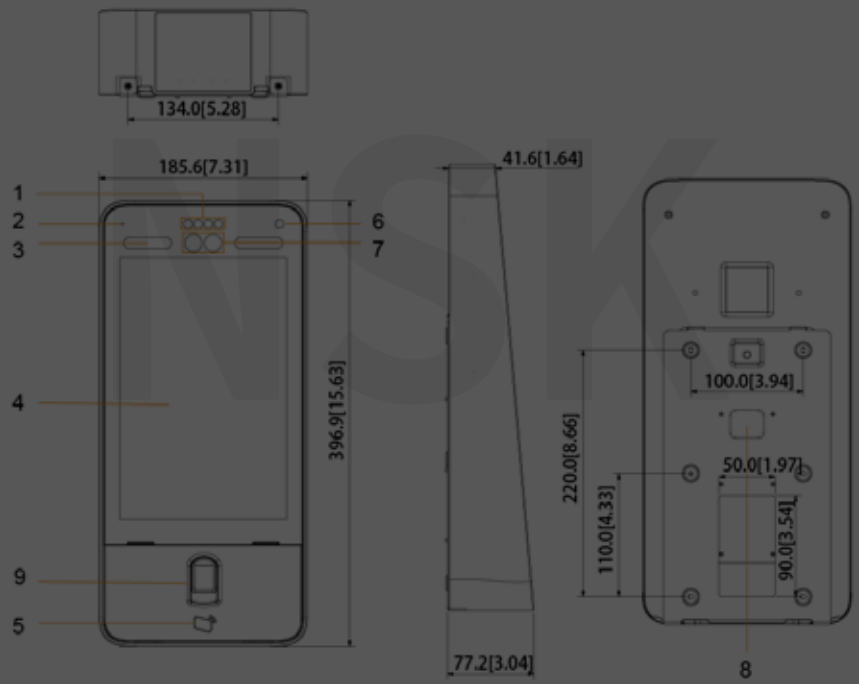


表1-4コンポーネントの説明（4）

No.	名前	No.	名前
1	IRライト	6	フォトトランジスタ
2	MIC	7	デュアルカメラ
3	ホワイトフィルライト	8	ケーブルの入り口
4	表示	9	指紋センサー
5	カードスワイプエリア	10	–

2 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、ドアコンタクト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、表2-1をご参照ください。

表 2-1ポートの説明

ポート	ケーブルの色	ケーブル名	説明
CON1	黒	RD-	外部カードリーダー電源の負電極。
	赤	RD+	外部カードリーダー電源の正極。
	青	CASE	外部カードリーダーのアラーム入力を改ざんします。
	白	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）
	緑	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）
	茶	LED	外部リーダーインジケータに接続
	黄	B	RS-485負電極入力（外部カードリーダーに設続）/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、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には、電力を供給するための個別の電源が必要です。 ■セキュリティモジュールを有効にすると、終了ボタン、ロック制御、および消防連携が無効になります。
	紫	A	RS-485正電極入力（外部カードリーダーに設続）/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、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。セキュリティジュールには、電力を供給するための個別の電源が必要です。 ■セキュリティモジュールを有効にすると、終了ボタン、ロック制御、および消防連携が無効になります。

ポート	ケーブルの色	ケーブル名	説明
CON2	白と赤	ALARM1_NO	アラーム1は通常、出力ポートを開きます。
	白とオレンジ	ALARM1_COM	アラーム1の共通出力ポート。
	白と青	ALARM2_NO	アラーム2は通常、出力ポートを開きます。
	白とグレー	ALARM2_COM	アラーム2の共通出力ポート。
	白と緑	GND	共通のGNDポートに接続されています。
	ホワイトブラウン	ALARM1	アラーム1入力ポート。
	白と黄	GND	共通のGNDポートに接続されています。
	白と紫	ALARM2	アラーム2入力ポート。
CON3	黒と赤	RX	RS-232受信ポート。
	黒とオレンジ	TX	RS-232送信ポート。
	黒と青	GND	共通のGNDポートに接続されています。
	黒とグレー	SR1	ドアの接触検出に使用されます。
	黒と緑	PUSH1	1番ドアのドアオープンボタン
	黒と茶	DOOR1_COM	ロック制御共通ポート。
	黒と黄	DOOR1_NO	ロック制御は通常ポートを開きます。
	黒と紫	DOOR1_NC	ロック制御は通常ポートを閉じます。

2.2 インストール

すべてのコントローラーのインストール方法は同じです。 レンズと地面の間の距離が1.4メートルであることを確認してください。 図 2-1をご参照ください。

図 2-1設置高さ

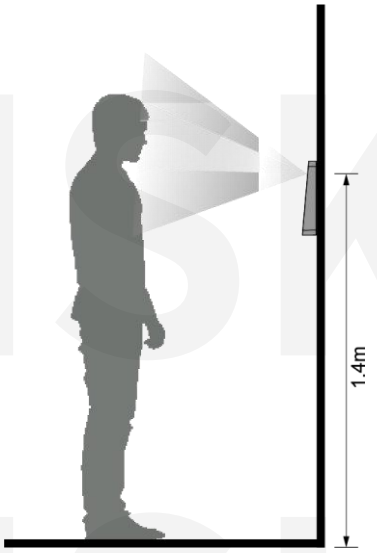
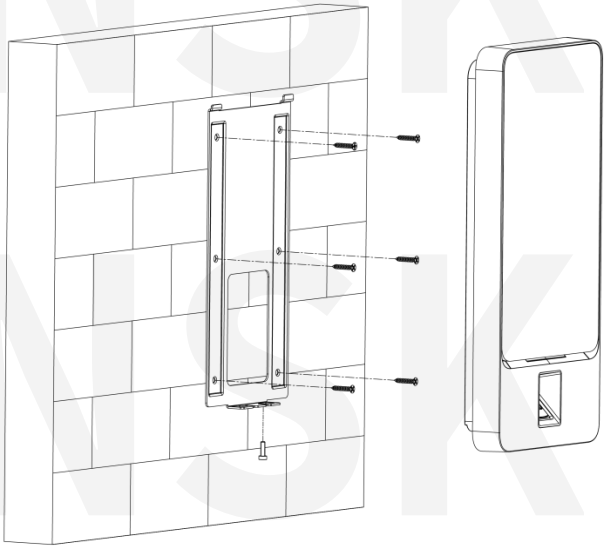


図 2-2設置図



インストール手順

Step 1　ブラケットの穴に応じて、壁に7つの穴（6つのブラケット取り付け穴と1つのケーブル挿入口）を開けます

Step 2　6本のブラケットに拡張ネジを取り付けて、壁にブラケットを固定します。

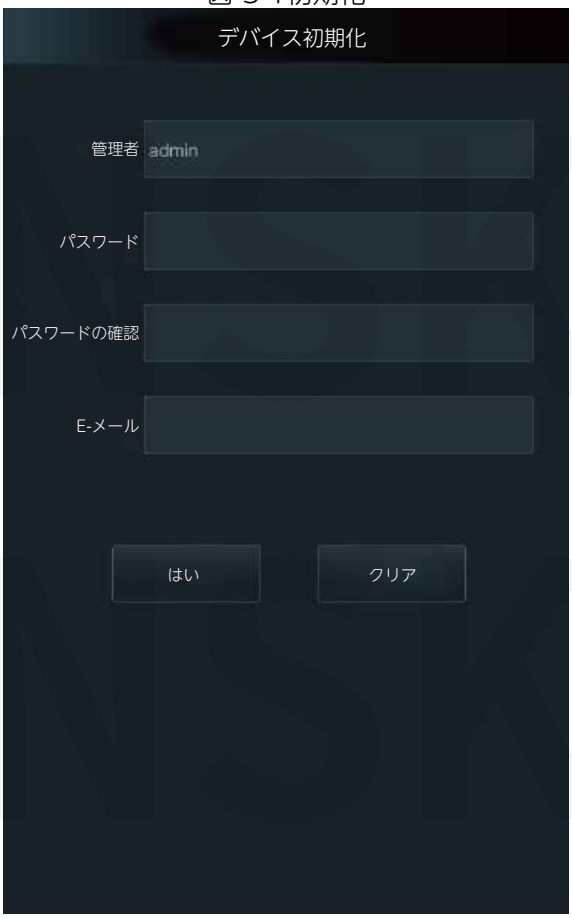
Step 3　アクセスコントローラーのケーブルを接続します。「2.1ケーブル接続」を参照してください。
Step 4　アクセスコントローラーをブラケットフックに掛けます。
Step 5　アクセスコントローラーの底部のネジを締めます。
Step 6　インストールが完了しました。

3 システム運用

3.1 初期化

管理者パスワードと電子メールは、アクセスコントローラーを初めてオンにするときに設定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ーを使用できません。

図 3-1初期化



■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。

■管理者が管理者パスワードを忘れた場合、管理者パスワードは入力したメールアドレスでリセットできます。

■パスワードは8～32文字の非空白文字で構成され、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。

3.2 スタンバイインターフェイス

顔、パスワード、カード、指紋を通じてドアのロックを解除できます。 表3-1を参照してください。

30秒以内に操作がない場合、アクセスコントローラーはスタンバイモードになります。

図 3-2ホームページ

表 3-1ホームページの説明

No.	説明
1	ロック解除方法：カード、顔、指紋、およびパスワード。 カード、顔、指紋、および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には表示されません。
2	日付と時刻：現在の日付と時刻がここに表示されます。
3	ネットワークステータスとUSBステータスがここに表示されます。
4	メインメニューアイコン。 管理者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。

3.3 ロック解除方法

顔、パスワード、指紋、およびカードを使用してドアをロック解除できます。顔、パスワード、指紋、およびカードを使用してドアをロック解除できます。

3.3.1カード

カードをカードスワイプエリアに置いて、ドアのロックを解除します。

3.3.2 顔

顔が顔認識フレームの中心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。

3.3.3 指紋

指紋センサーに指紋を置き、ドアのロックを解除します。

3.3.4 ユーザーパスワード

ユーザーパスワードを入力すると、ドアのロックを解除できます。

Step 1  ナンバーアイコンをタップします。

Step 2 ユーザーIDを入力してから をタップします

Step 3 ユーザー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。

3.3.5 管理者パスワード

管理者パスワードを入力すると、ドアのロックを解除できます。 1つのアクセスコントローラに対して1つの管理者パスワードがあります。 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、休暇計画、およびアンチパスバックの影響を受けずにドアをロック解除できます。

Step 1  管理者アイコンをタップします。

Step 2 **管理者PWD**をタップします。

Step 3 管理者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。

3.4 メインメニュー

管理者は、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メインメニューで行うことができます。

Step 1 スタンバイインターフェイス  をタップします。
管理者ログインインターフェイスが表示されます。

異なるモードが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 3-3管理者ログイン

Step 2　メインメニューの入力方法を選択します。メインメニューインターフェイスが表示されます。

図 3-4メインメニュー

3.5 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、ユーザーリストの表示、管理者リストの作成、管理者パスワードの変更を行うことができます。

3.5.1 新しいユーザーの追加

ユーザーID、名前の入力、指紋のインポート、顔の画像、カード、パスワード、ユーザーレベルの選択などにより、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。

Step 1 [ユーザー]> [新しいユーザー]を選択します。

新規ユーザー情報インターフェースが表示されます。 図 3-5をご参照ください。

図 3-5新規ユーザー情報

Step 2 インターフェイスのパラメーターを構成します。 表 3-2をご参照ください。

表 3-2新しい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を入力できます。 IDには数字、文字、およびそれらの組み合わせを使用でき、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）で入力できます。
FP	1人のユーザーの最大3つの指紋を記録でき、1つの指紋を3回検証する必要があります。各指紋の下でDuress FP機能を有効にでき、3つの指紋のうち1つだけが強迫指紋になります。ドアのロックを解除するために強迫指紋が使用されると、アラームがトリガーされます。 最初の指紋を強迫指紋として選択することはお勧めしません。
顔	顔が画像キャプチャフレームの中心にあることを確認してください。アクセスコントローラーが新しいユーザーの顔の写真を自動的に撮影します。詳細については、クイックスタートガイドを参照してください。

パラメータ	説明
カード	ユーザーごとに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、カード情報がアクセスコントローラーによって読み取られます。 カード登録インターフェースで強要カード機能を有効にできます。 強要カードを使用してドアのロックを解除すると、アラーム出力されます。 🕮 特定のモデルのみがカードのロック解除をサポートしています。
PWD	ドアのロック解除パスワード。ID桁の最大長は8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。 ユーザー：ドアのロック解除権限のみがあります。 管理者　：管理者はドアのロックを解除できるだけでなく、パラメータ設定権限も持つことができます。 🕮 アクセスコントローラーに管理者がいるかどうかに関係なく、管理者ID認証が必要です。
期間	ユーザーがドアのロックを解除できる期間を設定できます。
休日プラン	ユーザーがドアのロックを解除できる休日計画を設定できます。
有効日付	ユーザーのロック解除情報が有効な期間を設定できます。
ユーザータイプ	6つのレベルがあります。 ■一般：一般ユーザーは通常どおりドアのロックを解除できます。 ■ブラックリスト：ブラックリストのユーザーがドアのロックを解除すると、サービス担当者にプロンプトが表示されます。 ■ゲスト：ゲストは特定の時間にドアのロックを解除できます。最大時間を超えると、再びドアのロックを解除することはできません。 ■パトロール：パトロールユーザーは出席を追跡できますが、ロック解除権限はありません。 ■VIP：VIPがドアのロックを解除すると、サービス担当者がプロンプトを表示します。 ■無効化：無効化されたドアのロックを解除すると、ドアが閉じるまで5秒の遅延が生じます。
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が設定できます。

Step 3　すべてのパラメーターを構成したら、✓をタップし、設定を保存します。

3.5.2 ユーザー情報の表示

ユーザーインターフェイスを使用し、ユーザーリスト、管理者リストを表示し、管理者パスワードを有効にできます。

3.6 アクセス管理

ロック解除モード、アラーム、ドアの状態、およびロック保持時間にアクセス管理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。

3.6.1 期間管理

期間、休日期間、休日計画期間、通常はオンの期間、通常はドアを閉じた期間、およびリモート検証期間を設定できます。

3.6.1.1 期間の設定

0～127の番号範囲を持つ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、設定した期間内にのみドアのロックを解除できます。

3.6.1.2 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。番号範囲が0～127の128個のグループを構成でき、16の休日をグループに追加できます。休日グループの開始時間と終了時間を設定すると、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。 をタップします。

休日グループ名を保存します。

3.6.1.3 休日プランの設定

休日グループを休日プランに追加できます。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権限を管理できます。ユーザーは、設定した期間内にのみドアのロックを解除できます。

3.6.1.4 NO期間

NO期間に期間が追加された場合、ドアは通常その期間に開きます。

NO / NC期間の許可は、他の期間の許可よりも高くなっています。

3.6.1.5 NC期間

NC期間に期間が追加されると、通常はその期間にドアが閉じられます。この期間中、ユーザーはドアのロックを解除できません。

3.6.1.6 リモート認証期間

リモート認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、リモート認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指示が必要です。

リモート認証期間を有効にする必要があります。

-  有効
-  無効

3.6.2 ロック解除

ロック解除モードには、ロック解除モード、期間ごとのロック解除、3つのグループの組み合わせがあります。実際のアクセスコントローラーのほうが優先されます。

3.6.2.1 アンロックモード

アンロックモードがオンの場合、ユーザーはカード、指紋、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解除できます。

Step 1 [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。
要素（複数選択）インターフェイスが表示されます。 図 3-6をご参照ください。

図 3-6要素（複数選択）

Step ロック解除モードを選択します。選択したロック解除モードをもう一度タップすると、ロック解除モードがOFFになります。

Step 3 組み合わせモードを選択します。

■+および。たとえばカード+ FP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指紋をスキャンする必要があります。

■/または。 たとえば、カード/ FP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、指紋をスキャンできます。

Step 4 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。

Step 4 ロック解除モードを有効にします。

- 有効
- 無効

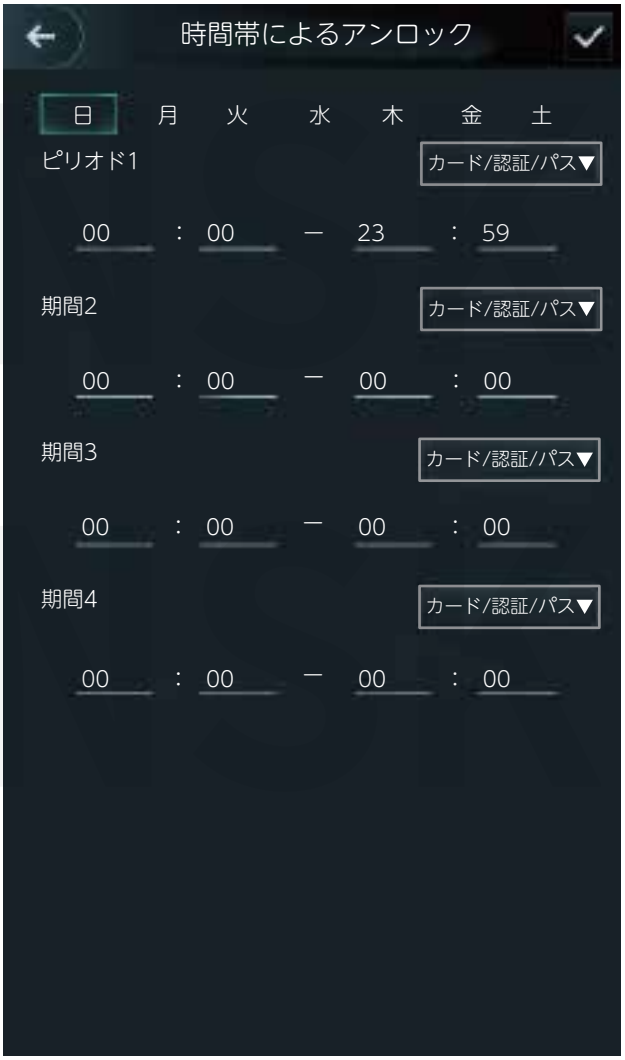
3.6.2.2 時間帯によるアンロック

ドアは、異なる期間に異なるロック解除モードで解除できます。 たとえば、期間1では、ドアはカードを介してのみロック解除できます。 期間2では、ドアは指紋でしかロックできません。

Step 1 [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。

期間ごとの構成のロック解除インターフェースが表示されます。図 3-7をご参照ください。

図 3-7期間ごとのロック解除



Step 2 期間の開始時間と終了時間を設定し、ロック解除モードを選択します。

Step 3 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。

Step 4 期間ごとのロック解除機能を有効にします。

- 有効
- 無効

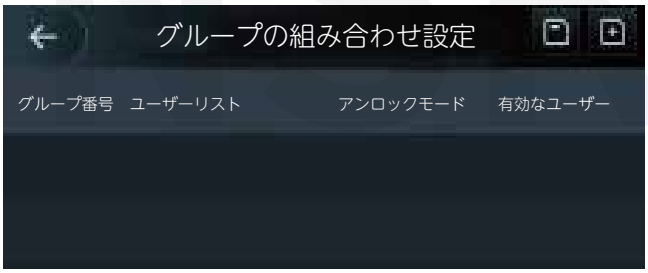
3.6.2.3 グループの組み合わせ

グループの組み合わせが有効になっている場合、3人以上のユーザーで構成されるグループでのみロック解除できます。

Step 1 [アクセス]> [アンロックモード]> [グループの組み合わせ]を選択します。

グループの組み合わせ構成はインターフェースが表示されます。 図 3-8をご参照ください。

図 3-8グループの組み合わせ



Step 2 グループを作成します。

グループの追加インターフェイスが表示されます。 図 3-9をご参照ください。

図 3-9グループの追加

表 3-3グループパラメーター

パラメータ	説明
ユーザーリスト	新しく作成したグループにユーザーを追加します。 1.ユーザ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. 次にユーザーIDを入力します。 3. をタップして設定を保存します。
ロック解除モード	カード、FP、PWD、および顔の4つのオプションがあります。
有効なユーザー	有効なユーザーとは、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ユーザーの数が有効なユーザー数と等しい場合にのみ、ドアをロック解除できます。 ■有効なユーザーはグループ内のユーザーの総数を超えることはできまん。 ■有効なユーザーがグループ内の合計ユーザー数と等しい場合、グループ内のすべてのユーザーのみがドアをロック解除できます。 ■有効なユーザーがグループ内のユーザーの総数よりも少ない場合、有効なユーザー番号と等しい番号を持つユーザーがドアのロックを解除できます。

Step 3 前のインターフェイスに戻ります。

Step 4 をタップして設定を保存します。

Step 5 グループの組み合わせを有効にします。

- 有効
- 無効

3.6.3 アラーム設定

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。
[アクセス]> [アラーム]を選択します。 アラームインターフェイスが表示されます。
図 3-10をご参照ください。

図 3-10アラーム

-  有効
-  無効

表 3-4アラームインターフェイスのパラメーター

パラメータ	説明
アンチパスバック	• アクセスコントローラーがIDを確認してドアをロック解除しても アクセスコントローラーがIDを確認せずに外に出ると、アラームが起動し、ロック解除する権限がなくなります。 • カードを画面をスワイプ（指で左右に滑らす）せずに建物や部屋へ入室し、またカードをスワイプして外に出た場合、その人はドアのロックを解除する権限を失います。
強迫	強迫カード、強迫パスワード、または強迫指紋を使用してドアのロックを解除すると、アラームが起動します。
不正カード	不正なカードを使用してドアを50秒以内に5回以上ロック解除すると、アラームが起動します。
侵入	ドアの接触を解除せずにロックを解除すると、侵入アラームが起動します。
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起動します。 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になっている場合のみ、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起動します。

3.6.4 ドアのステータス

NO、NC、正常の3つのオプションについて

■NO：ドアの状態は通常開いていますのでドアが閉じられることはありません。
■NC：ドアステータスは通常閉じられていますのでドアはロック解除されません。
■正常：設定に応じてドアがロック解除およびロックされます。

3.6.5 ロック保持時間

ロック保持時間はロックが解除される期間です。 ロックが期間を超えてロック解除された場合、自動的にロックされます。

3.7 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、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。

3.7.1 IPアドレス

3.7.1.1 IP設定

ネットワークに接続されるように、アクセスコントローラーのIPアドレスを構成します。 図 3-11 および、表 3-5をご参照ください。

図 3-11 IPアドレスの構成

表 3-5 IP構成パラメーター

パラメータ	説明
IPアドレス サブネットマスク ゲートウェイIPアドレス	IPアドレス、サブネットマスク、およびゲートウェイIPアドレスがオンになっている必要があります。 同じネットワークセグメント。 設定後　　をタップして設定を保存します。
DHCP	DHCP（動的ホスト構成プロトコル） DHCPを有効にすると、IPアドレスを自動的に取得でき、IPアドレス、サブネットマスク、およびゲートウェイIPアドレスを手動で構成することはできません。
P2P	P2PとはユーザーがDDNS、ポートマッピング、または中継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。

3.7.1.2 アクティブ登録

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

行った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。誤操作によるデータ損失の場合に、プラットフォーム管理機関を保護する必要があります。
アクティブなレジスタパラメータについては、表 3-6をご参照ください。

表 3-6 アクティブレジスタ

名前	パラメータ
サーバの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。

3.7.1.3 Wi-Fi

使用できません。

3.7.2 シリアルポート設定

入る方向と出る方向に応じて、シリアル入力またはシリアル出力を選択します。
[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 3-12をご参照ください。

図 3-12 シリアルポート

■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。 アクセスカード情報をアクセスコントローラと管理プラットフォームに送信できるようにするには、シリアル入力を選択します。

■顔認識、指紋認識、カードの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2つのタイプがあります。

- ◇ ユーザーID
- ◇ カート番号

■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、OSDP入力を選択します。アクセスコントローラーはカード情報を管理プラットフォームに送信できます。

このアクセスコントローラーは、カードリーダーとして他のデバイスに接続できません。

3.7.3 ウィーガンド構成

進入方向と退出方向に応じて、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。
[接続]> [ウィーガンド]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 3-13をご参照ください。

図 3-13Wiegand（ウィーガンド）

◇ 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は、Wiegand 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、Wiegand 出力を選択します。 表 3-7をご参照ください。

表 3-7Wiegand出力

パラメータ	説明
Wiegand output タイプ	Wiegand出力タイプは、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数字の桁を決定します。 ■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 パルス間隔	パルス幅とパルス間隔を設定できます。
Output Data タイプ	出力データのタイプを選択できます。 ■ユーザーID：ユーザーIDを選択するとユーザー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。

このアクセスコントローラーは、カードリーダーとして他のデバイスに接続できません。

3.8 システム

3.8.1 時間

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

■Network Time Protocol（NTP）を選択する場合、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刻は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。

3.8.2 顔パラメータ

3.8.2 顔パラメータ

パラメータをタップして設定を行い、次に をタップします

表 3-8 顔パラメータ

名前	説明
顔認識しきい値	顔認識の精度を調整でき、値が大きいほど、精度が高くなります。
顔認識の最大アングル	プロファイルのコントロールパネルの撮影角度を設定できます。 値が大きいほど、より広い範囲のプロファイルが認識されます。
瞳孔間距離	瞳孔距離は、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。 値は顔のサイズと顔とレンズ間の距離に応じて変化します。 顔がレンズに近いほど値は大きくなり、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の範囲内になります。
認識タイムアウト	アクセス権限を持っていない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に失敗したことを促します。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	アクセス権限を持つ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促します。 プロンプト間隔は認識間隔です。
顔IDのしきい値	この機能は人間の顔画像または顔モデルによるロック解除を防ぎます。 値が大きいほど、画像がドアのロック解除するのが難しくなります。 80以上が推奨値の範囲です。

3.8.3 照明モード設定

必要に応じて補助光モードを選択できます。 次の3つのモードがあります。

■自動：周囲環境が暗いことをフォトセンサーが検出すると、通常、補助光はオフになります。
そうでない場合、フィルライトが点灯します。

■NO：補助光は通常点灯しています。
■NC：通常、フィルライトは閉じています。

3.8.4 照度設定

必要に応じて、補助光の明るさを選択できます。

3.8.5 音量調整

 or  いずれかををタップして音量を調整します。

3.8.6 IRライトの輝度調整

値が大きいほど画像は鮮明になります。

3.8.7 FPパラメーター

指紋精度レベルを設定します。 レベルが高いほど誤認識率は低くなります。

3.8.8 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設定に戻すとデータは失われます。
■アクセスコントローラーが工場出荷時の設定に復元された後、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た状態で、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設定に復元することを選択できます。

3.8.9 再リブート

[システム]> [再起動]を選択し、[再起動]をタップすると、アクセスコントローラーが再起動します。

3.9 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に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。
それらを行うことによって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はプログラムの更新にも使用できます。

3.9.1 USBエクスポート

USBを挿入した後、アクセスコントローラーから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> USB Export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 3-15をご参照ください。

図 3-15 USBエクスポート

Step 2　エクスポートするデータ型を選択します。
エクスポートの確認プロンプトが表示されます。

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。

3.9.2 USBインポート

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内のデータのみを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 **USB> USB Import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 3-16をご参照ください。

図 3-16 USBインポート

Step 2 インポートするデータタイプを選択します。
インポートの確認プロンプトが表示されます。
Step 3 OKをタップします。

USB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。

3.9.3 USB更新

USBを使用してシステムを更新できます。
Step 1 アップデートファイルの名前を「update.bin」に変更し「update.bin」ファイルをUSBのルートディレクトリに保存します。
Step 2 USB>USBアップデートを選択します。更新の確認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。

3.9.4 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。 上記の機能の詳細については、図 3-17及び表 3-9をご参照ください。

図 3-17機能

表 3-9特徴の説明

パラメータ	説明
プライバシー設定	詳細については、「3.9.5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、アクセス制御キュリティモジュールを別途購入する必要があります。セキュリティモジュールには、電力を供給するための個別の電源が必要です。 ■セキュリティモジュールを有効にすると、終了ボタン、ロック制御、および消防連携が無効になります。
ドアセンサータイプ	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。

3.9.5 プライバシー設定

図 3-18プライバシー設定

表 3-10機能

パラメータ	説明
PWDリセット有効	PWDリセット有効化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。 PWDリセット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を有効にすると、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、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が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で実行されるコンソールアプリケーションのように実行される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が有効な場合、CGIコマンドを使用できます。 CGIはデフォルトで有効になっています。
SSH	Secure Shell（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を有効にすると、SSHはデータ送信用の暗号化サービスを提供します。

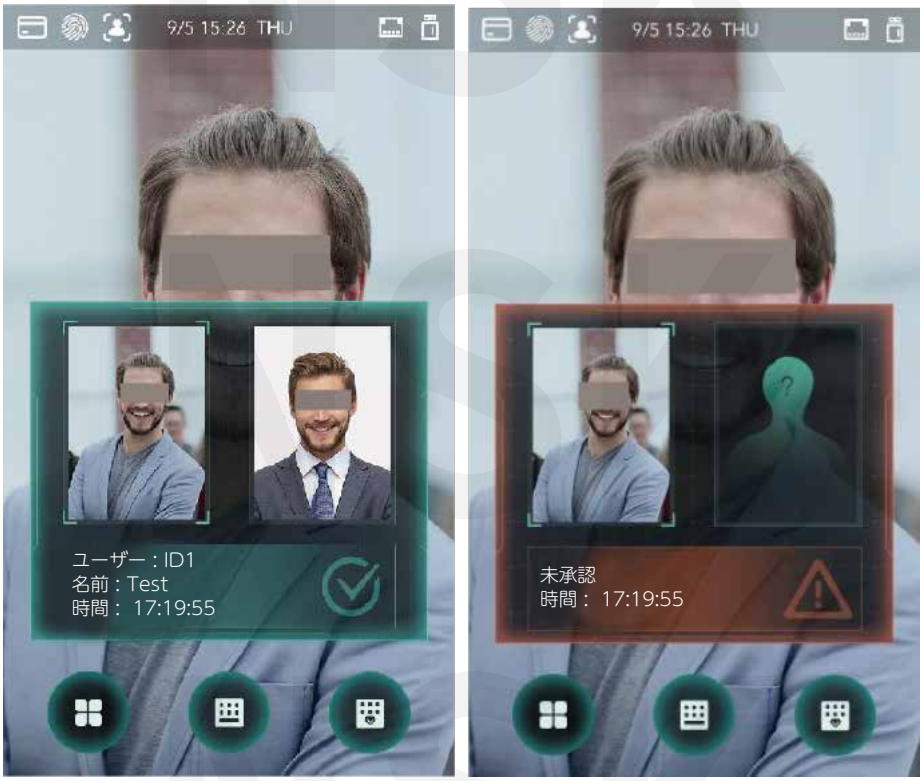
パラメータ	説明
FP	指紋（FP）で[オフ]を選択した場合、ユーザーが指紋を記録するとき、または指紋を使用してドアのロックを解除するときに、ユーザーの指紋情報は表示されません。
写真を撮る	[オン]を選択すると、ユーザーがドアのロックを解除すると、ユーザーの写真が自動的に撮影されます。 この機能はデフォルトでオンです。
キャプチャした写真を消去する	アイコンをタップすると、キャプチャしたすべての写真を削除できます。

3.9.6 結果のフィードバック

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。

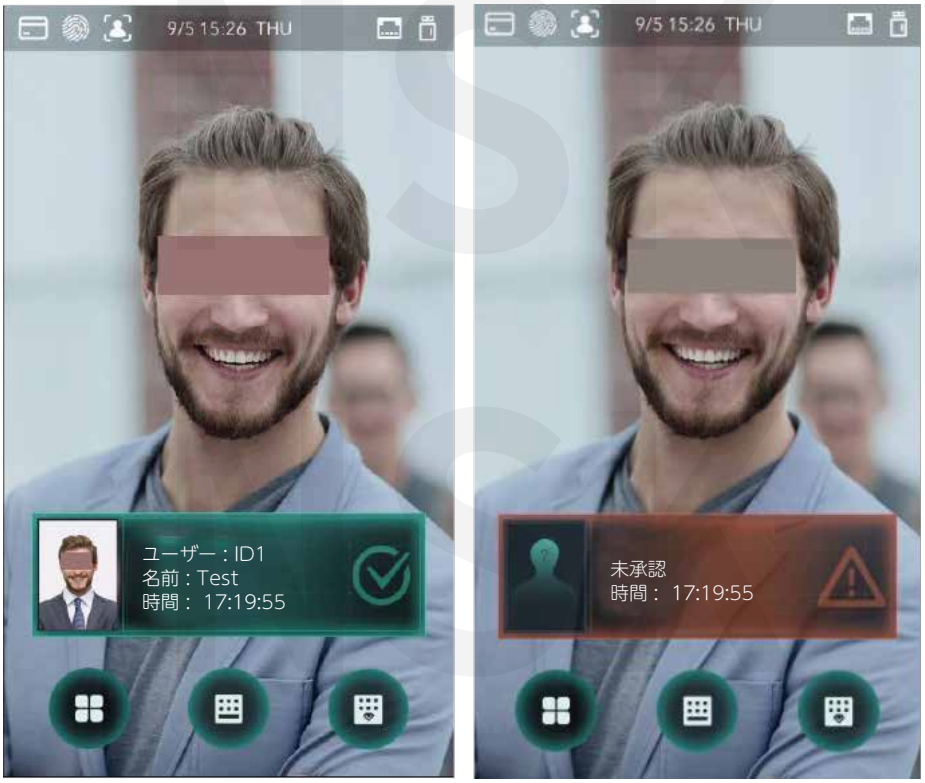
モード1

図 3-19 モード1



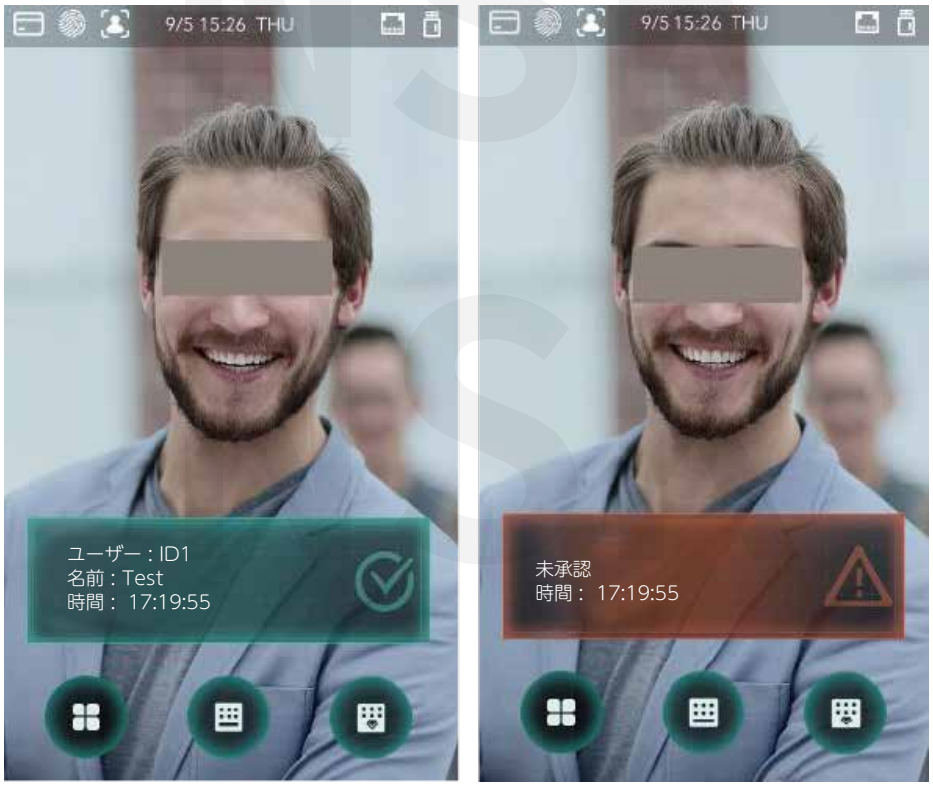
モード2

図 3-20モード2



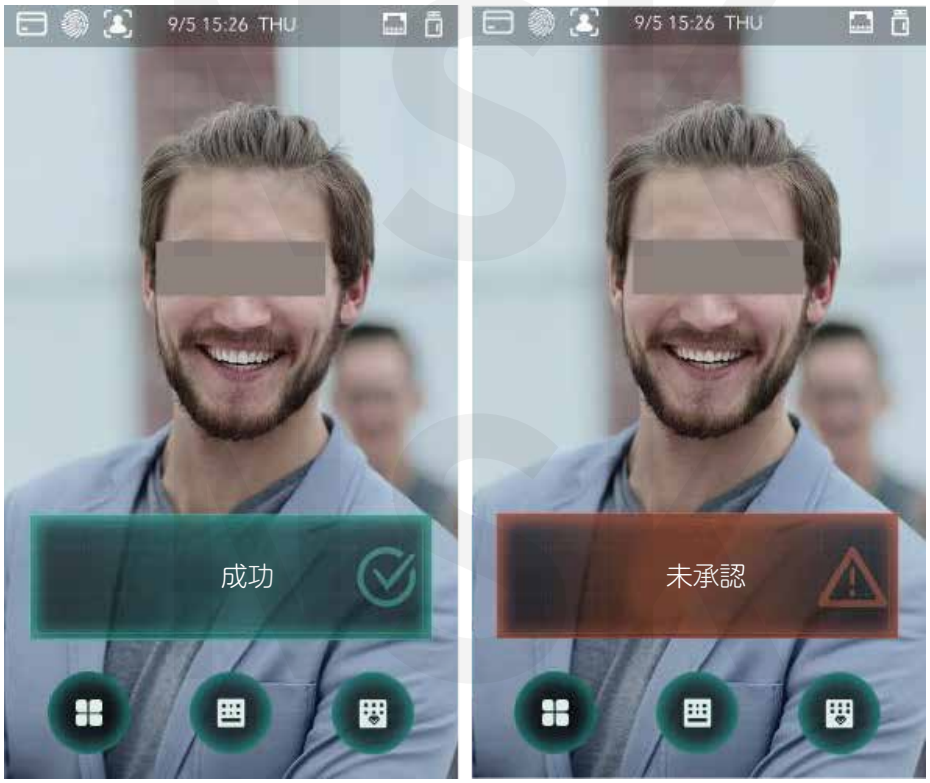
モード3

図 3-21モード3



モード4

図 3-22モード4



3.10 録画

すべてのロック解除レコードを照会できます。

図 3-23パンチ記録の検索

3.11 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誤動作したとは、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機能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 3-24自動テスト

[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の実行をガイドします。

3.12 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 ウェブ操作

アクセスコントローラーは、Web上で構成および操作できます。Webを介して、ネットワークパラメータ、ビデオパラメータ、およびアクセスコントローラパラメータを設定できます。　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 初期化

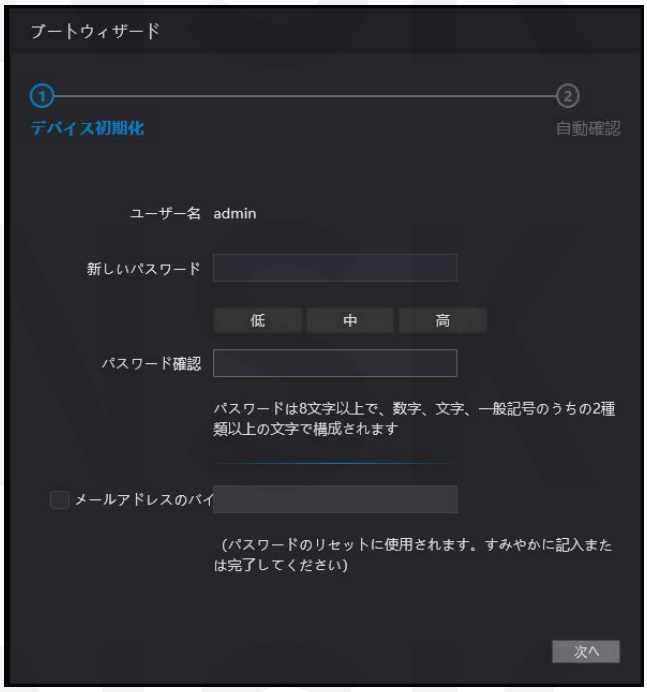
Webに初めてログインする前に、パスワードとメールアドレスを設定する必要があります。

Step 1　IEWebブラウザを開き、IPアドレスを入力します（デフォルトアドレスは192.168.1.108）

アドレスバーのアクセスコントローラの[Enter]を押します。初期化インターフェースが表示されます。 図 4-1を参照してください。

IE 8より新しいブラウザを使用してください。そうしないと、Webにログインできない場合があります。

図 4-1初期化



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]をタップします。

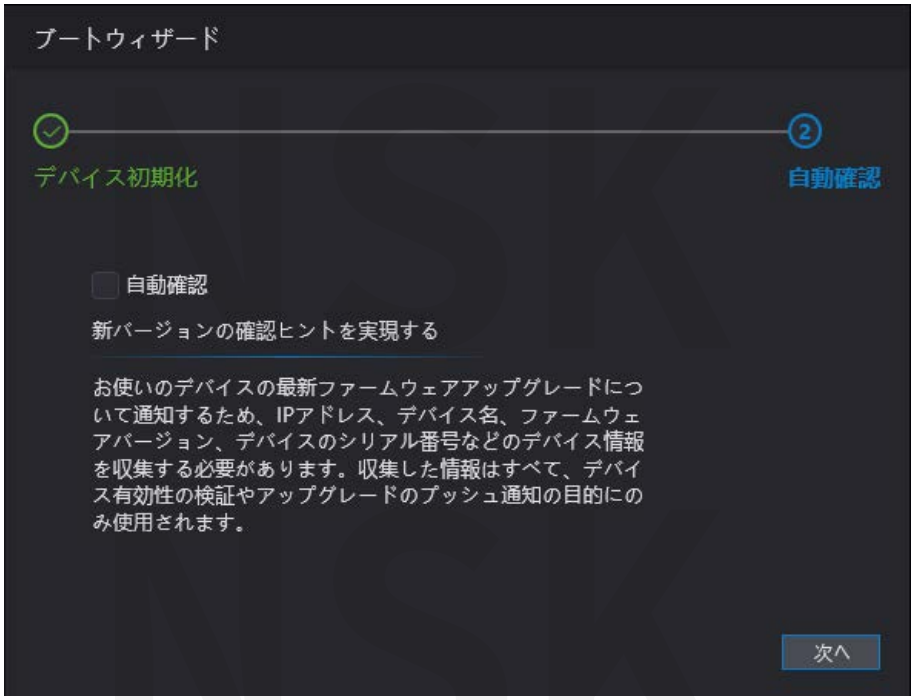
■セキュリティのため、初期化後にパスワードを適切に保持し、定期的にパスワードを変更します。
■パスワードは8～32文字の空白以外の文字で構成し、大文字、小文字、数字、特殊文字（ '";：＆を除く）の少なくとも2種類の文字を含める必要があります。

■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。

自動チェックインターフェイスが表示されます。 図 4-2をご参照ください。

図 4-2自動テスト



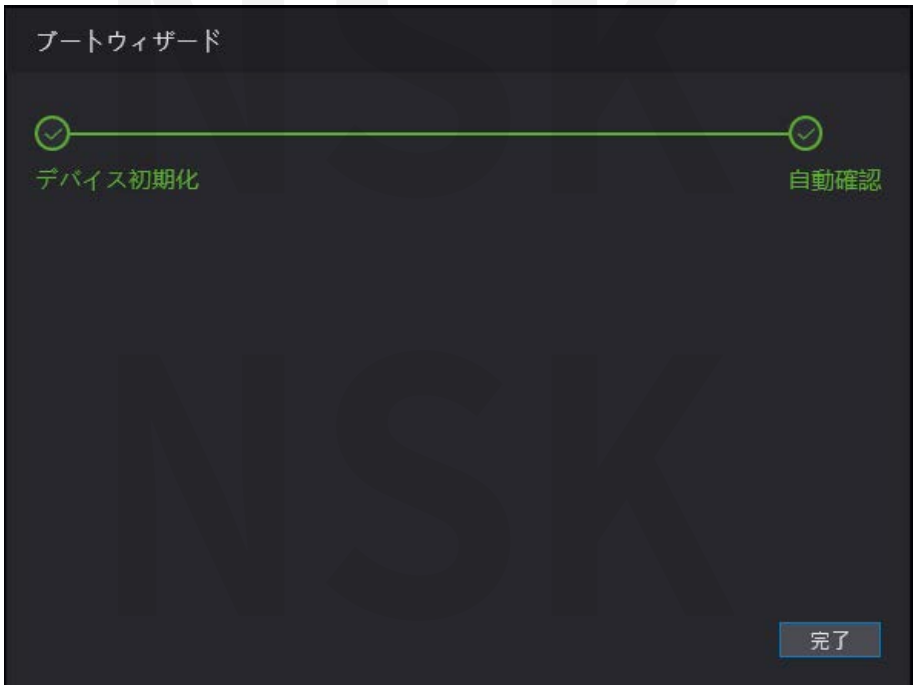
Step 4 自動チェックを選択するかどうかを決定できます。

最新のプログラムを取得するには、自動チェック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。

設定が完了しました。 図 4-3を参照してください。

図 4-3完成した構成

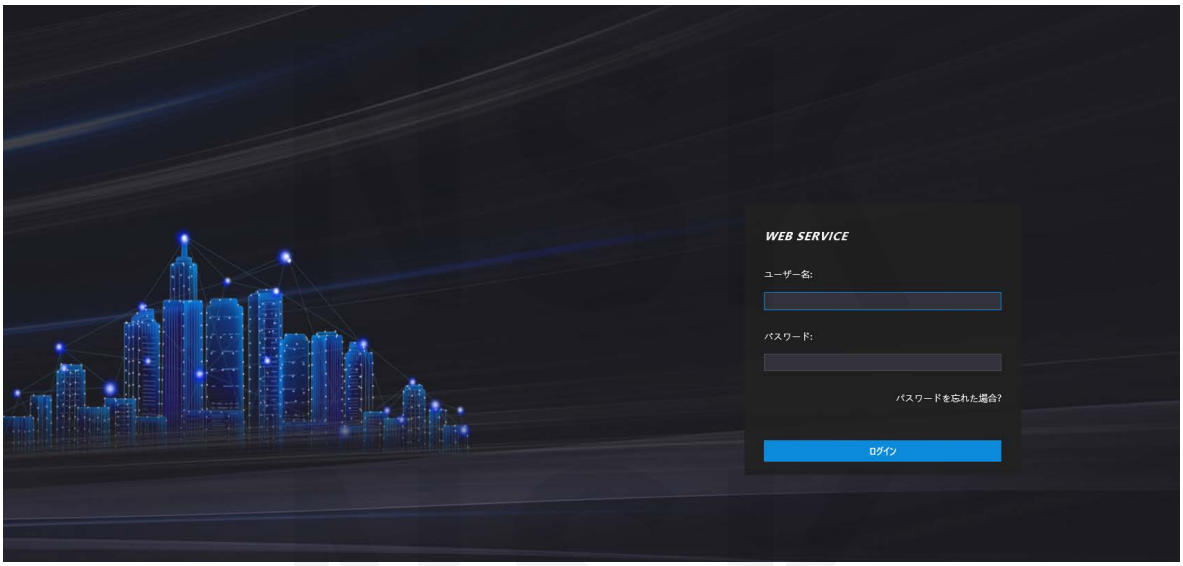


Step 6 [完了]をクリックすると、初期化が完了します。
Webログインインターフェイスが表示されます。

4.2 ログイン

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アドレスを入力しエンターを押します。

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、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。 管理者を定期的に変更しセキュリティのために適切に保管してください。

■管理者のログインパスワードを忘れた場合は、[パスワードを忘れた場合]をクリックできるのでそれをリセットします。「4.3パスワードのリセット」を参照してください。

Step 3 ログインをクリックします。
Webインターフェースがログインします。

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 ヒントインターフェイスが表示されます。
[パスワードをお忘れですか？]をクリックします。

図 4-5ヒント

Step 2 ヒントを読んでください。

Step 3 OK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 4 インターフェイスのQRコードをスキャンすると、セキュリティコードが取得されます。

■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で、新たにセキュリティコードを取得する際はQRコードを更新します。

■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。

■セキュリティコードは、受け取ってから24時間以内に使用してください。
そうしないと、無効になります。
■間違ったセキュリティコードが5回連続して入力された場合、管理者は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ます。
Step 6 次へをクリックします。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。
Step 7 新しいパスワードをリセットして確認します。

パスワードは8～32文字の空白以外の文字で構成し、大文字、小文字、数字、特殊文字（ '";：＆を除く）のうち少なくとも2種類の文字を含める必要があります。

Step 8 [OK]をクリックすると、リセットが完了します。

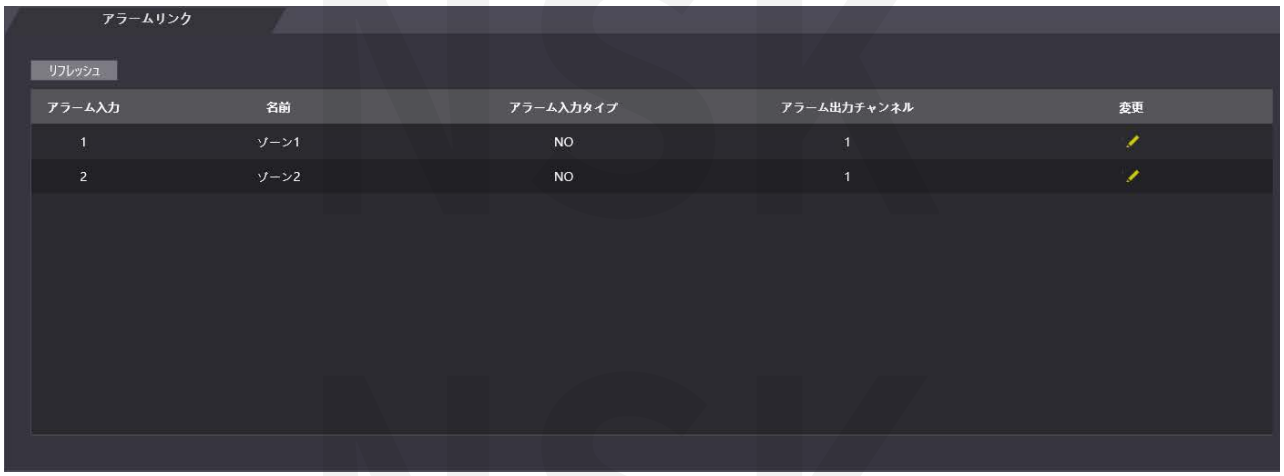
4.4 アラームリンク

4.4.1 アラームリンクの設定

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 ナビゲーションバーで[アラームリンク]を選択します。
アラームリンクインターフェイスが表示されます。 図 4-7をご参照ください。

図 4-7アラームリンク



Step 2  をクリックすると、アラームリンクパラメータを変更できます。
図 4-8をご参照ください。

図 4-8アラームリンクパラメーターの変更

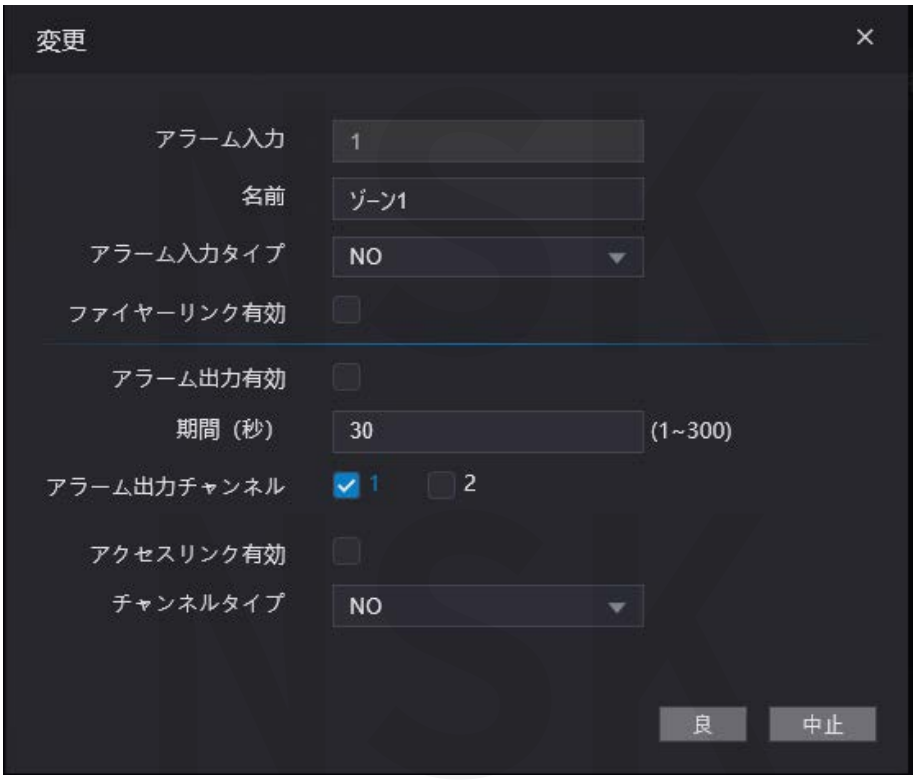


表 4-1アラーム連動パラメーターの説明

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。デフォルトのままにします。
名前	ゾーン名を入力してください。
アラーム入力タイプ	NOとNCの2つのオプションがあります。 購入したアラームデバイスのアラーム入力タイプがNOの場合、NOを選択し、それ以外の場合はNCを選択します。
ファイヤーリンク有効	ファイヤーリンクが有効になっている場合、火災警報が起動すると、アクセスコントローラーは警報を出力します。アラームの詳細は、アラームログに表示されます。 📖 ファイヤーリンクが有効の場合、アラーム出力とアクセスリンクはデフォルトでNOです。
アラーム出力有効	アラーム出力が有効になっている場合、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、および範囲は1～300秒です。
アラーム出力チャンネル	取り付けたアラームデバイスに応じて、アラーム出力チャネルを選択できます。各アラームデバイスは、チャネルと見なすことができます。
アクセスリンク有効	アクセスリンクが有効になった後、入力アラーム信号がある場合、アクセスコントローラは通常オンになるか、通常閉じられます。
チャンネルタイプ	NOとNCの2つのオプションがあります。

Step 3 [OK]をクリックすると、構成が完了します。

📖
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

アラームログインターフェイス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]を選択します。

アラームログインターフェイスが表示されます。図 4-9をご参照ください。

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]をクリックします。

照会結果が表示されます。 図 4-10をご参照ください。

図 4-10クエリ結果

4.5 データ容量

アクセスコントローラーがデータ容量インターフェースで保持できるユーザー、カード、顔画像、指紋の数を確認できます。

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（輝度、コントラスト、色相、彩度ど）、露出などのパラメーターを設定できます。

4.6.1 データレート

図 4-12データレート

表 4-2データレートパラメータの説明

パラメータ		説明
ビデオ標準		NTSCとPALの2つのオプションがありますのでお住まいの地域のビデオ規格に従って選択してください。
チャネル		以下2のオプションがあります。 1：白色光カメラ　2：IR光カメラ
メイン フォーマット	ビデオ フォーマット	D1、VGA、720p、1080pの4つのオプションがあります。 希望するビデオ品質に応じてオプションを選択します。
	フレーム レート	連続したフレームがディスプレイに表示される割合。 フレームレートの範囲は1～25fpsです。

パラメータ		説明
	ビットレート	時間単位ごとに伝達または処理されるビット数に5つのオプションがあります。 1.75Mbps、2Mbps、4Mbps、6Mbps、および8Mbps
追加フォーマット	ビデオフォーマット	D1、VGA、およびQVGAの3つのオプションがあります。
	フレームレート	連続したフレームがディスプレイに表示される割合。 フレームレートの範囲は1～25fpsです。
	ビットレート	時間単位毎に処理されるビット数のオプションがあります。 256Kbps、320Kbps、384Kbps、448Kbps、512Kbps、640Kbps、768Kbps、896Kbps、1024Kbps、1.25Mbps、1.5Mbps、1.75Mbps

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 [ビデオ設定]> [ビデオ設定]> [画像]を選択します。

図 4-13画像

Step 2 バックライトモードでワイドダイナミックを選択します。

表 4-3画像パラメーターの説明

パラメータ	説明
輝度	値が大きいほど、画像は明るくなります。
コントラスト	コントラストは、オブジェクトを区別できるようにする輝度または色の違いです。 コントラスト値が大きいほど、明るさと色のコントラストが大きくなります。
ヒュー	値が大きいほど、色は濃くなります。
彩度	値が大きいほど、色が明るくなります。 この値は画像の明るさを変更しません。

パラメータ	説明
場面	■閉じる：モードなし。 ■自動　：システムはシーンモードを自動的に調整します。 ■晴天　：このモードでは、画像の色相が減少します。 ■夜間　：このモードでは、画像の色相が増加します。 デフォルトでは、自動が選択されています。
昼/夜モード	デイ/ナイトモードは、フィルライトの動作状態を決定します。 ■自動：システムはデイ/ナイトモードを自動的に調整します。 ■カラフル：このモードでは画像は色付きです。 ■白黒：このモードの画像は白黒です。
背景照明モード	■閉じる：バックライトなし。 ■逆光：バックライト補正は、非常に高いレベルまたは低いレベルの光がある領域を補正して、焦点が合っているオブジェクトに対して通常の使用可能な光のレベルを維持します。 ■WDR：ワイドダイナミックレンジモードでは、システムは明るい領域を暗くし、暗い領域を補正して、明るい領域と暗い領域のオブジェクトを明確にします。 顔がバックライトにある場合、ワイドダイナミックを有効にします。 ■抑制：ハイライトの過剰露出またはスポットライト、ヘッドライト、ポーチライトなどの強力な光源を補正して、明るい光に追いつかない使いやすい画像を作成するには、ハイライト補正が必要です。
ミラー	この機能を有効にすると、画像が左右を反転して表示されます。
宙返り	この機能を有効にすると、ビデオを裏返すことができます。

4.6.3 露光

露光パラメータの説明については、表 4-4をご参照ください。

表 4-4露光パラメータの説明

パラメータ	説明
明滅防止	■50Hz：交流の商用周波数が50Hzの場合、画像に縞がないように露出が自動的に調整されます。 ■60Hz：交流の商用周波数が60Hzの場合、露出が画像に縞がないように自動的に調整されます。 ■屋外：屋外を選択すると、露出モードを切り替えることができます。

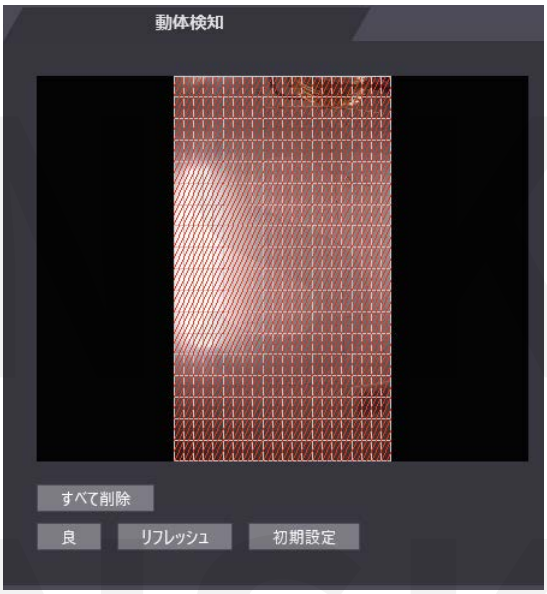
パラメータ	説明
露光モード	🕮 ■[ちらつき防止]ドロップダウンリストで[屋外]を選択すると、露出モードとして[シャッター優先度]を選択できます。 ■異なるデバイスの露出モードは異なる場合があり、実際の製品が優先されます。 以下から選択できます。 ■自動：アクセスコントローラーは画像の明るさを自動的に調整します。 ■シャッター優先：アクセスコントローラーは、シャッター露出値の範囲に応じて画像の明るさを調整します。 画像の明るさが十分でなく、シャッター値が上限または下限に達した場合、アクセスコントローラーはゲイン値を自動的に調整して理想的な明るさを取得します。 ■手動：ゲインとシャッター値を手動で設定して、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く、露光時間が短いほど、画像は暗くなります。
シャッター値の範囲	[カスタマイズ範囲]を選択するとシャッター値の範囲をカスタマイズできます。
ゲイン値の範囲	ゲイン値の範囲を設定すると、ビデオの品質が向上します。
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、高解像度のビデオが生成されます。
グレード	3D NRが有効な場合、3D NRの値を調整できます。 値が大きいほど、ノイズが少なくなります。

4.6.4 動体検知

動く物体を検出できる範囲を設定します。

Step 1 [ビデオ設定]> [ビデオ設定]> [動き検出]を選択します。動体検知インターフェイスが表示されます。図 4-14をご参照ください。

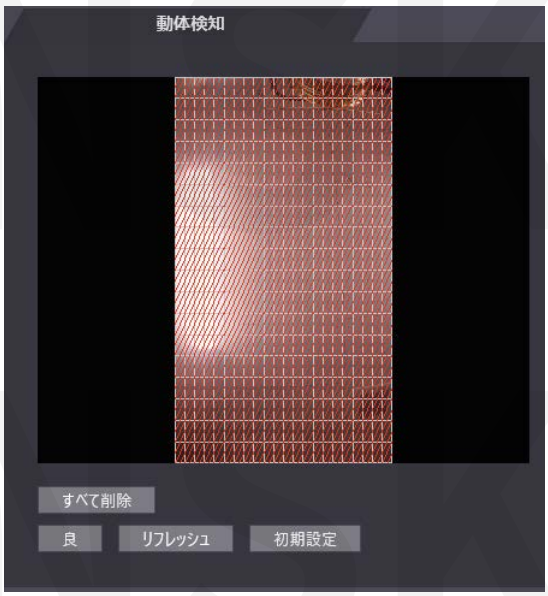
図 4-14動体検知



Step 2　マウスの左ボタンを押したまま、マウスを赤い領域にドラッグします。動体検知エリアが表示されます。 図 4-15をご参照ください。

■赤い長方形はモーション検出エリアです。 デフォルトのモーション検出範囲はすべての長方形です。
■モーション検知エリアを描画するには、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。

図4-15動体検知エリア



Step 3　[OK]をクリックして設定を終了します。

4.6.5 画像モード

屋内、屋外、その他の3つのオプションがあります。アクセスコントローラーが屋内に設置されている場合は屋内を選択します。アクセスコントローラーを屋外に設置する場合は屋外を選択します。
アクセスコントローラーが廊下や廊下などのバックライトのある場所に設置されている場合は[その他]を選択します。

図 4-17画像モード

4.7 顔検知

このインターフェイスで人間の顔に関連するパラメーターを構成して、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。

顔検出インターフェイスが表示されます。 図 4-18をご参照ください。

図 4-18顔検出

Step 2 パラメーターを構成します。 表 4-5をご参照ください。

表 4-5顔検出パラメーターの説明

パラメータ	説明
顔認識しきい値	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、より広い範囲のプロファイルが認識されます。
偽造防止有効	有効と閉じるの2つのオプションがあります。
明るさの設定	補助光の明るさを設定できます。
フィルライト モード設定	3つの補助光モードがあります。 ■NO→通常、フィルライトはオンです。 ■NC→通常、フィルライトは閉じています。 ■自動→モーション検知イベントが起動するとフィルライトは自動的にオンになります。 [自動]が選択されている場合、赤外線ライトの値が19を超えていてもフィルライトはオンになりません。
赤外線ライト	スクロールバーをドラッグして、明るさを調整します。
認識タイムアウト	アクセス権限を持っていない人がアクセスコントローラーに顔を認識させると、コントローラーは顔認識に失敗したことを促します。プロンプト間隔は、認識タイムアウトと呼ばれます。
無効な顔のプロンプト間隔	顔にアクセス権限がない場合、アクセスコントローラの前に立つと、コントローラは無効であることを促します。 プロンプト間隔は無効なフェイスプロンプトです。
瞳孔間距離	瞳孔距離は、各目の瞳孔の中心間の画像のピクセル値です。そのため、適切な値を設定する必要があります。

パラメータ	説明
	アクセスコントローラーは必要に応じて顔を認識できます。値は顔のサイズと顔とレンズ間の距離に応じて変化します。顔がレンズに近いほど、値は大きくなり、大人がレンズから1.5メートル離れている場合、瞳孔距離の範囲内は50～70の値になります。
顔の露出を有効にする	顔の露出を有効にし、アクセスコントローラーを屋外に設置すると、より鮮明に映ります。
チャンネルID	以下の2つのオプションがあります。 1：白色光カメラ　2：IR光カメラ
ターゲットを描く	[ターゲットの描画]をクリックすると最小の顔検出フレームを描画します。 [すべて削除]をクリックすると、描いたすべてのフレームを削除できます。
領域を検出	[領域の検出]をクリックしてマウスを動かす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、すべての検出領域を削除できます。

Step 3 [OK]をクリックして設定を終了します。

4.8 ネットワーク設定

4.8.1 TCP / IP

IPアドレスとDNSサーバーを構成して、アクセスコントローラーが他のデバイスと通信できることを確認する必要があります。

前提条件

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ことを確認してください。
ステップ1 [ネットワーク設定]> [TCP / IP]を選択します。

図 4-19 TCP / IP

Step 2 パラメーターを構成します。

表 4-6 TCP / IP

パラメータ	説明
IPバージョン	オプション：IPv4
Macアドレス	アクセスコントローラのMACアドレスが表示されます。
モード	■静的 IPアドレス、サブネットマスク、ゲートウェイアドレスを手動で設定します。 ■DHCP DHCPを有効にすると、IPアドレス、サブネットマスク、およびゲートウェイアドレスを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。 ◇DHCPが有効なときにデフォルトIPを表示する場合はDHCPを無効にします。
リンクローカルアドレス	リンクローカルアドレスは、IPバージョンでIPv6が選択されている場合に限り使用できます。リンクローカルアドレスが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イスコントローラーに割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は変更できません。
IPアドレス	IPアドレスを入力し、サブネットマスクとゲートウェイアドレスを構成します。 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に存在する必要があります。
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 3 [OK]をクリックして設定を完了します。

4.8.2ポート

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

Step 1　[ネットワーク設定]> [ポート]を選択します。
ポートインターフェイスが表示されます。

Step 2　ポート番号を構成します。 次の表をご参照ください。

📖
最大接続を除き、アクセスコントローラーを再起動して値を変更した後に構成を有効にします。

表 4-7ポートの説明

パラメータ	説明
最大接続	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。他の値がポート番号として使用されている場合、ブラウザを介してログインする時にアドレスの後ろにこの値を追加します。
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。

Step 3 [OK]をクリックして設定を完了します。

4.8.3 登録

外部ネットワークに接続すると、アクセスコントローラーはそのアドレスをユーザーが指定したサーバーに報告し、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 [ネットワーク設定]>[自動登録]を選択します。
自動登録インターフェイスが表示されます。

Step 2 [有効]を選択し、ホストIP、ポート、およびサブデバイスIDを入力します。

表 4-8自動レジスタの説明

パラメータ	説明
ホストIP	サーバーの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。

Step 3 [OK]をクリックして設定を完了します。

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クは、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コードをスキャンすることでモバイルアプリケーションをダウンロードし、アプリで複数のアクセスコントローラーを管理できるようになりアカウントを登録できます。動的なドメイン名を適用したり、ポートマッピングを行ったり、中継サーバーを使用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。そうしないと、アクセスコントローラーを使用できません。

図 4-20 P2P

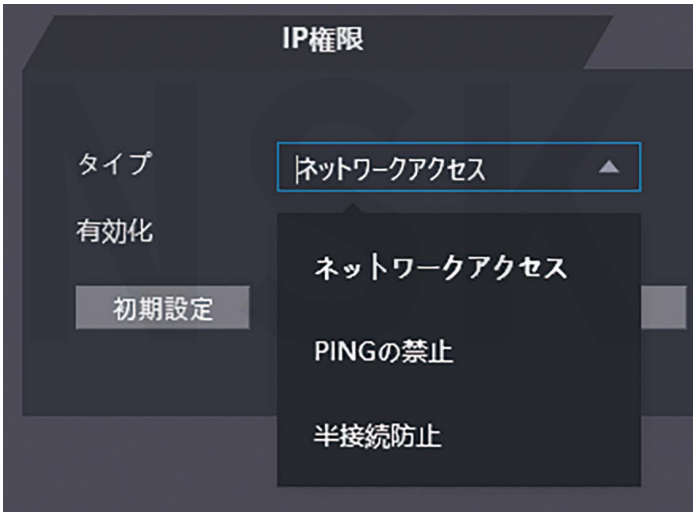
Step 1 [ネットワーク設定]> [P2P]を選択します。
P2Pインターフェイスが表示されます。
Step 2 [有効]を選択して、P2P機能を有効にします。
Step 3 [OK]をクリックして設定を完了します。

Webインターフェイスで 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。

4.9 安全管理

4.9.1 IPオーソリティ

図 4-21 IP機関



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。

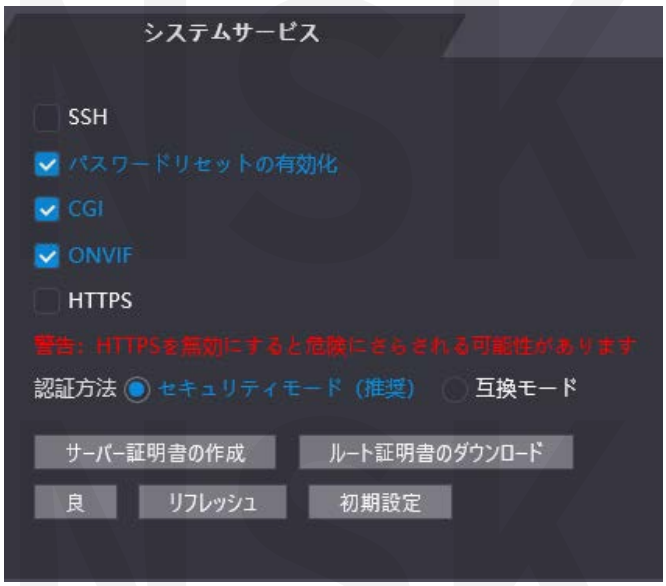
4.9.2 システム

4.9.2.1 システムサービス

SSH、PWD Reset Enable、CGI、HTTPSの4つのオプションがあります。
1つまたは複数の機能を選択するには「3.9.4機能」を参照してください。

Webページで実行されるシステムサービスの構成と、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



4.9.2.2 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。

4.9.2.3 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。

4.9.3 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。

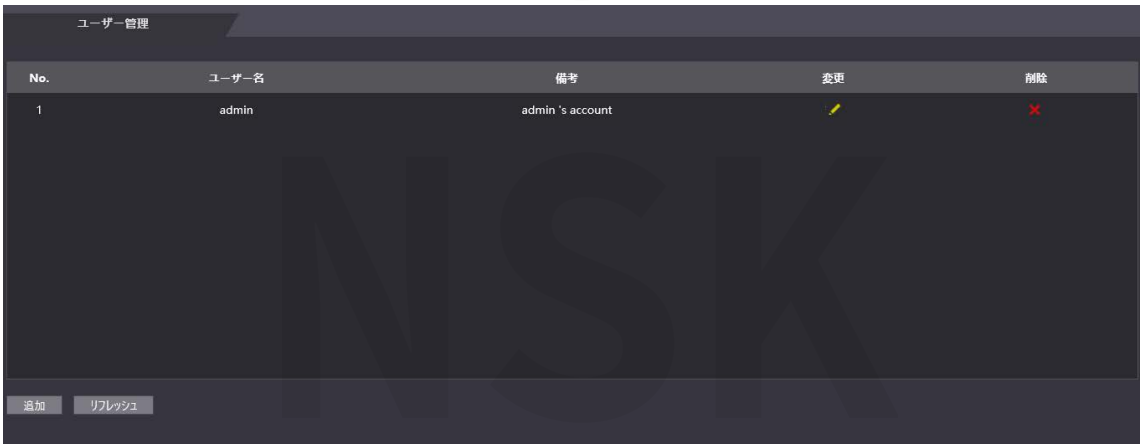
4.9.3.1 ユーザーの追加

ユーザー管理で追加をクリックします。 インターフェースを使用してユーザーを追加し、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。 [OK]をクリックして、ユーザーの追加を完了します。

4.9.3.2 ユーザー情報の変更

をクリックしてユーザー情報を変更できます。図 4-23をご参照ください。

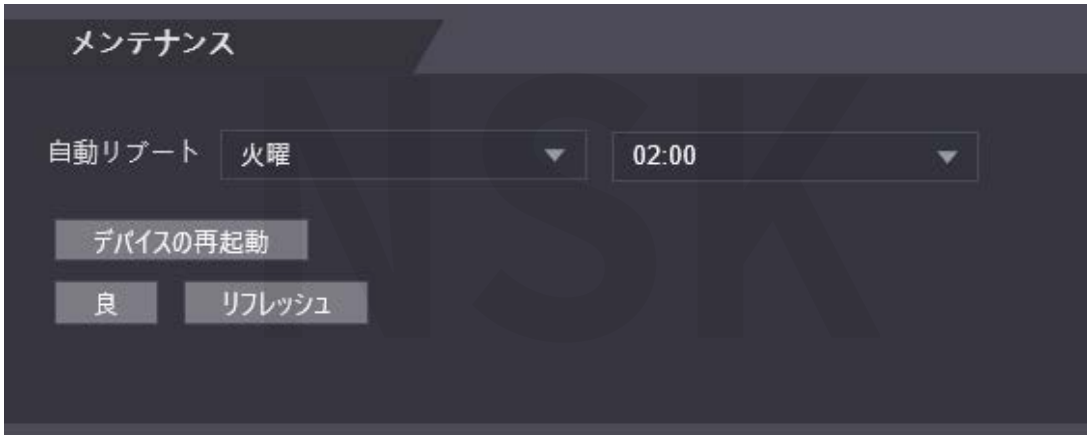
図 4-23ユーザー管理



4.9.4 メンテナンス

アクセスコントローラーの実行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ーを再起動することができます。 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。
[OK]をクリックすると、アクセスコントローラーは毎週火曜日の午前2時に再起動します。
図 4-24をご参照ください。

図 4-24メンテナンス



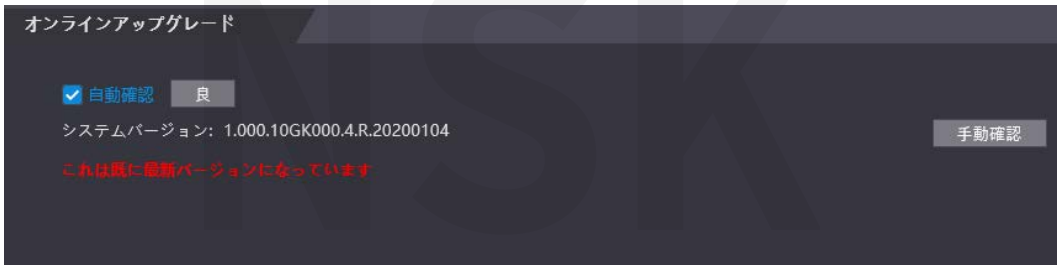
4.9.5 構成管理

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で、それらのパラメーターを構成できます。
図 4-25をご参照ください。

図 4-25構成管理

4.9.6 アップグレード

自動チェックを選択して、システムを自動的にアップグレードできます。
手動チェックを選択して、手動でもアップグレードできます。



4.9.7 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。

4.9.8 オンラインユーザー

オンラインユーザーインターフェイスでユーザー名、IPアドレス、およびユーザーログイン時間を表示できます。 図 4-26をご参照ください。

図 4-26オンラインユーザー

4.10 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。
図 4-27をご参照ください。

図 4-27システムログ

4.10.1 ログのクエリ

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

4.10.2 ログのバックアップ

[バックアップ]をクリックして、表示されたログをバックアップします。

4.11 管理ログ

管理ログインターフェースで管理者IDを入力し[クエリ]をクリックすると、管理者の操作記録が表示されます。 図 4-28をご参照ください。

図 4-28管理ログ

マウスカーソルを上に移動すると、 現在のユーザーの詳細情報が表示されます。

4.12 終了

[OK]をクリックすると、Webインターフェイスからログアウトします。

5 スマートPSS設定

Smart PSSクライアントを介して、単一のドアまたはドアグループへのアクセス許可設定を行うことができます。構成の詳細については、Smart PSSユーザーマニュアルをご参照ください。

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

5.1ログイン

Smart PSS（デフォルトのユーザー名はadmin、デフォルトのパスワードはadmin123）をインストールし、 をダブルクリックして操作します。 指示に従って初期化を完了しログインします。

5.2デバイスの追加

スマートPSSにアクセスコントローラーを追加する必要があります。
[自動検索]をクリックして追加し、[追加]をクリックしてデバイスを手動で追加します。

5.2.1自動検索

同じネットワークセグメントにあるアクセスコントローラーを検索してSmart PSSに追加できます。
図 5-1および、図 5-2を参照してください。

図 5-1デバイス

図 5-2自動検索

Step 1 [自動検索]をクリックし、ネットワークセグメントを入力して、[検索]をクリックするとリストが表示されます。

Step 2 スマートPSSに追加するアクセスコントローラーを選択し、[追加]をクリックすると[ログイン情報]ダイアログボックスが表示されます。

Step 3 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。

追加したアクセスコントローラーは、デバイスインターフェイスで確認できます。

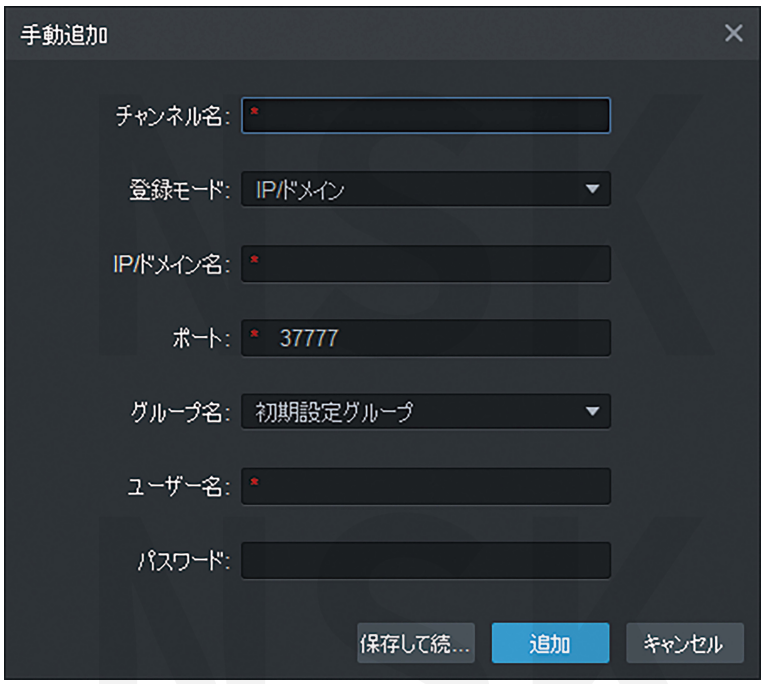
アクセスコントローラーを選択し、[IPの変更]をクリックすると、アクセスコントローラーのIPアドレスを変更できます。 IPアドレスの変更の詳細については、Smart PSSユーザーマニュアルをご参照ください。

5.2.2 手動追加

追加するアクセスコントローラのIPアドレスとドメイン名を知る必要があります。
図 5-3および、図 5-4をご参照ください。

図 5-3デバイス

図 5-4手動追加



Step 1 [デバイス]インターフェイスで[追加]をクリックすると、手動追加インターフェイスが表示されます。

Step 2 デバイス名を入力し、追加する方法を選択する。
IP/ドメイン名、ポートを入力します
番号（デフォルトでは37777）、グループ名、ユーザー名、およびパスワード。

Step 3 [追加]をクリックすると、追加されたアクセスコントローラーが[デバイス]インターフェイスに表示されます。

5.3 ユーザーの追加

ユーザーをSmart PSSに追加したら、[新規]> [アクセス]でユーザーのアクセス許可ができます。図 5-5をご参照ください。

図 5-5新規

5.3.1 カードタイプの選択

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。
そうしないと、カード番号を読み取ることができません。

アクセスインターフェイスで、 をクリックしてから、ICまたはIDカードのアイコンをクリックし、カードの種類を選択します。 IDカードとICカードの2つのオプションがあります。 図 5-6および、図 5-7をご参照ください。

図 5-6アクセス

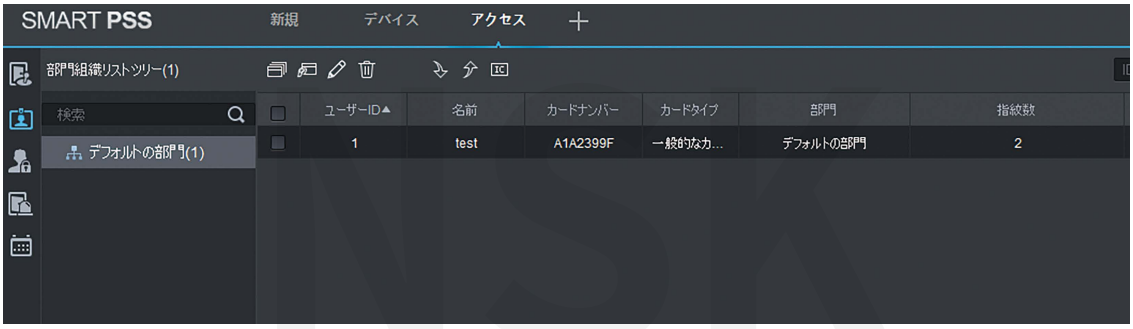
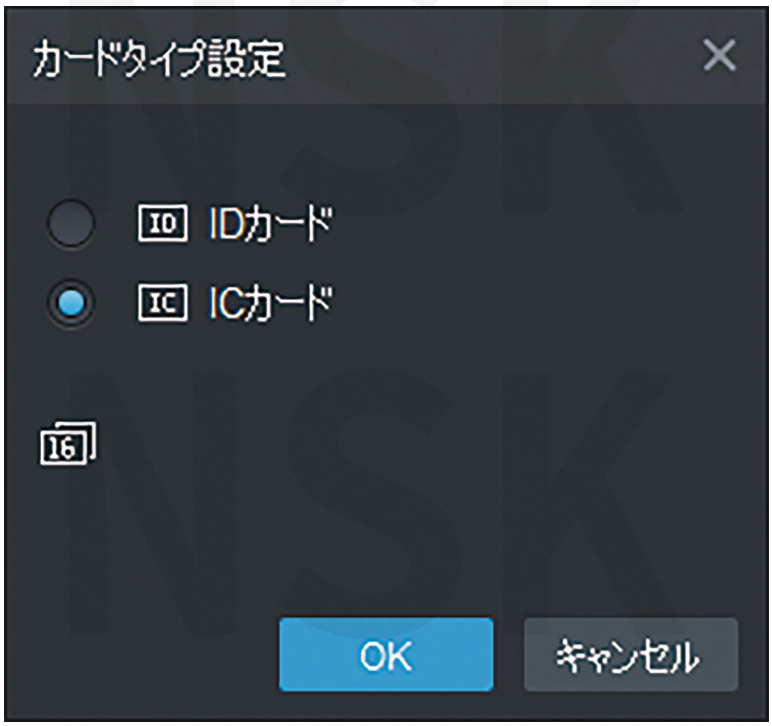


図 5-7カードタイプの設定



5.3.2 1人のユーザーの追加

ユーザーを1つずつ追加できます。

Accessインターフェースで、  をクリックしてから  をクリックしユーザーの情報を入力します。[完了]をクリックして、ユーザーの追加を完了します。 図 5-8および、図 5-9をご参照ください。

図 5-8アクセス

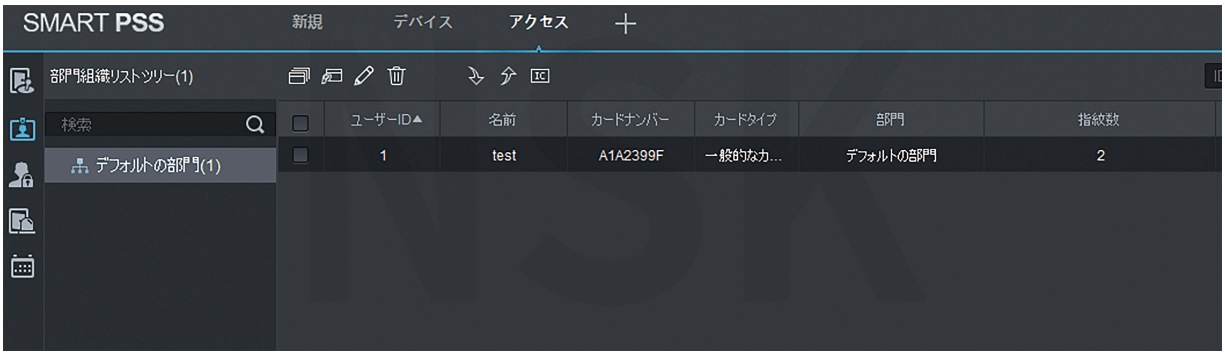


図 5-9ユーザーの追加

5.4 ドアグループの追加

ドアをグループ化して、ドアを管理できます。

アクセスインターフェイスで  をクリックし、[追加]をクリックして、ドアグループ名を入力したらタイムゾーンを選択します。 [完了]をクリックしユーザーの追加は完了です。
図 5-10および、図 5-11をご参照ください。

図 5-10アクセス

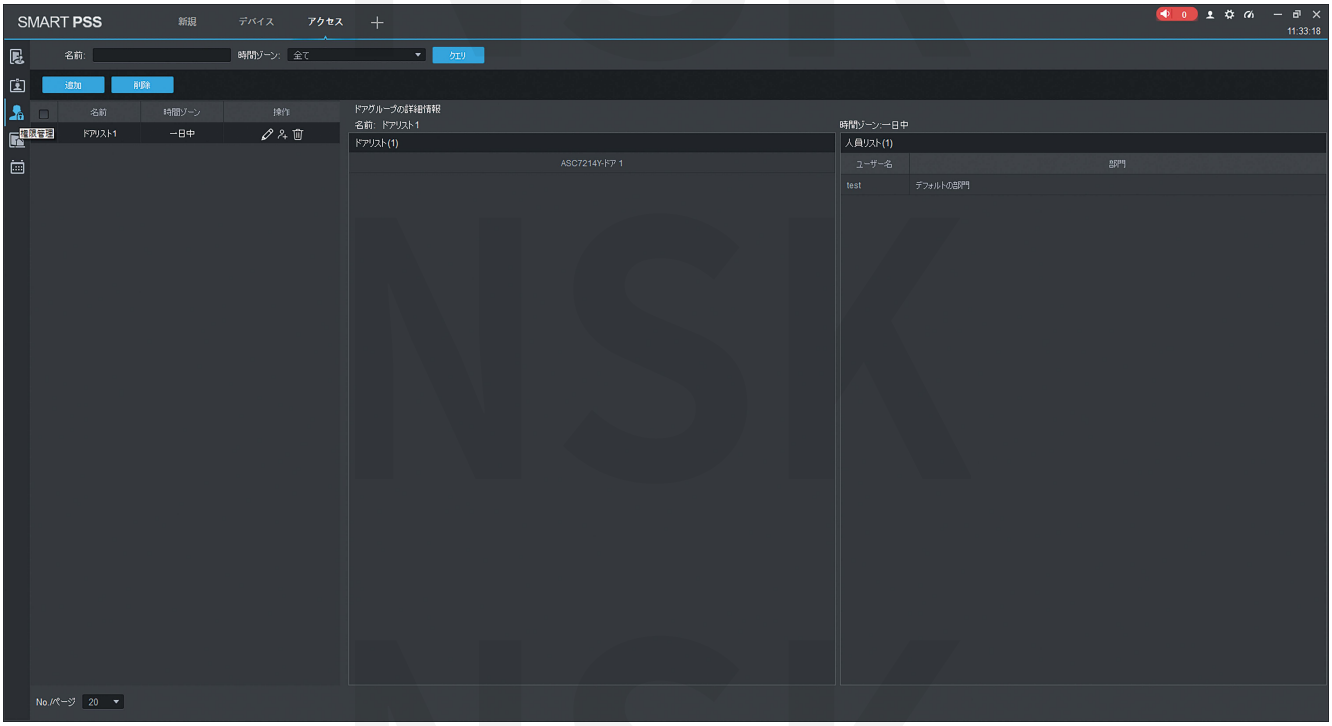
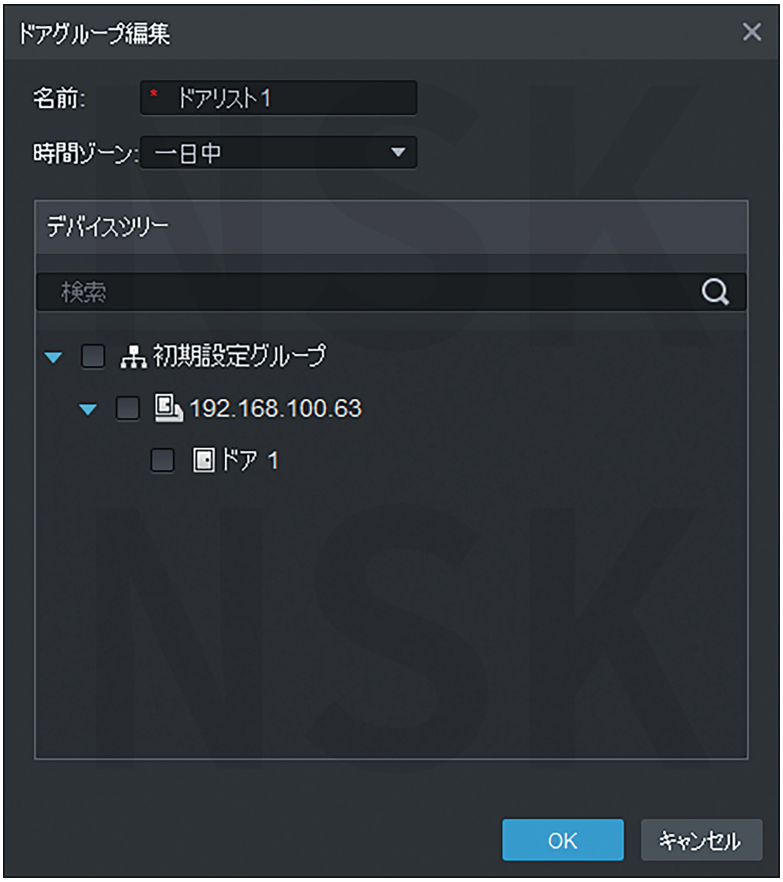


図 5-11ドアグループの追加



5.5 アクセス許可の構成

アクセス許可の構成を行うことができます。ドアグループアクセス許可とユーザーアクセス許可の2つのオプションがあります。スマートPSSとアクセスコントローラーでアクセス許可が与えられているユーザーの情報は同期されます。

5.5.1 ドアグループによる許可の付与

ドアグループを選択し、ユーザーをドアリストに追加すると、ドアリストのユーザーがドアリストのすべてのドアのアクセス許可を取得します。 図 5-12および、図 5-13をご参照ください。

図 5-12アクセス

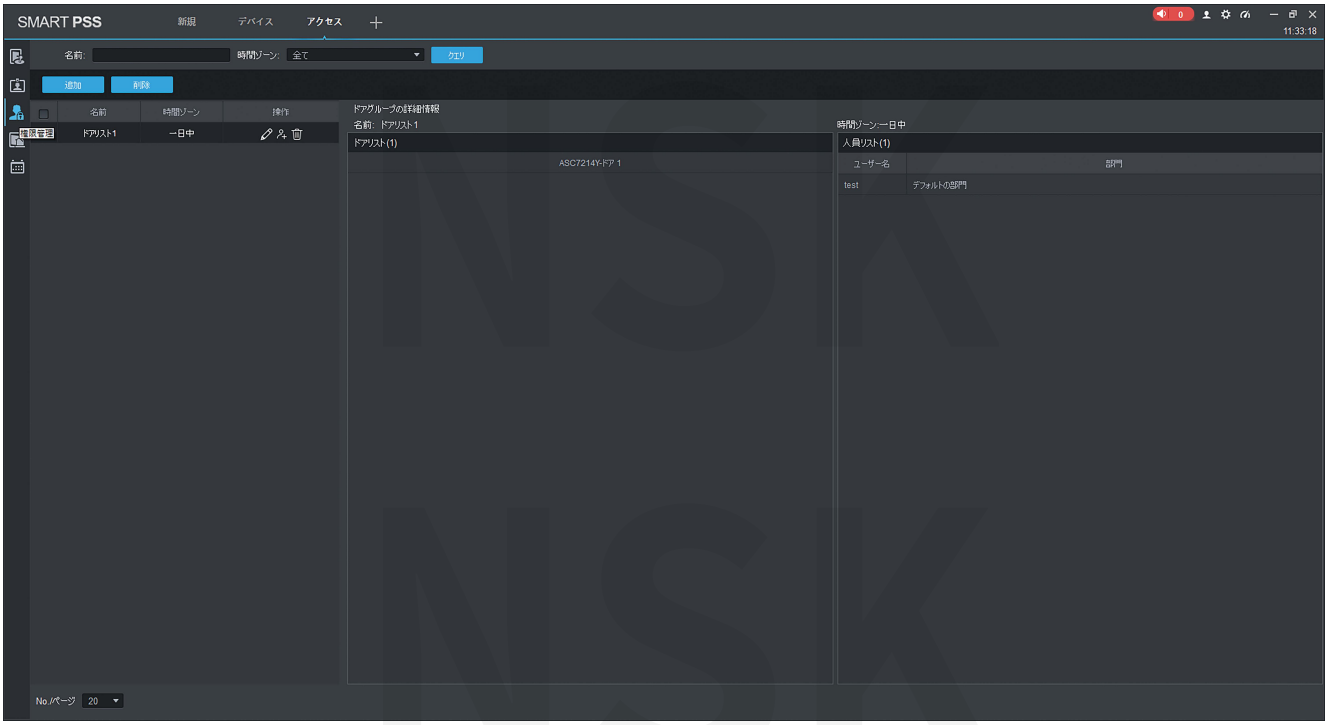


図 5-13ユーザー選択

Step 1 アクセスインターフェイスで  をクリックし[追加]をクリックして、
[ドアグループのアクセス許可]をクリックします。

Step 2  をクリックします。ドロップダウンリストでユーザー部門を選択するか、
ユーザーID /名前を入力します。

Step 3 次にユーザーを検索します。 見つけたユーザーからユーザーを選択します。
[完了]をクリックして構成を完了します。

ユーザーIDのないユーザーが見つかりません。

5.5.2 ユーザーIDによる許可の付与

ユーザーを選択してアクセス許可を付与し、そのユーザーのドアグループを選択できます。
図 5-14、図 5-15をご参照ください。

図 5-14アクセス

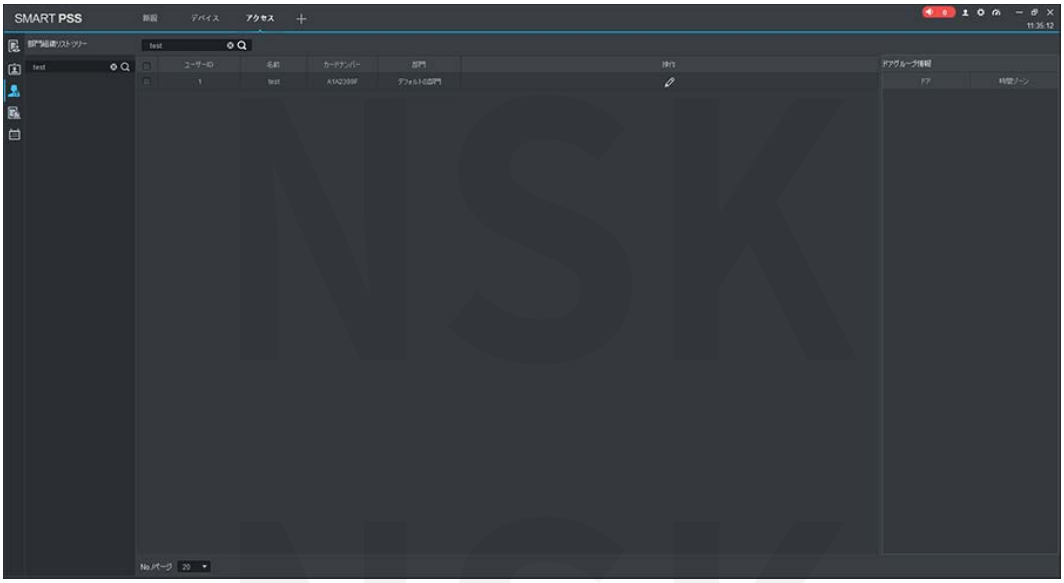


図 5-15ドアグループの選択

Step1 アクセスインターフェイスで、  をクリックします。

Step 2  をクリックします。ドアグループの選択インターフェイスが表示されます。

Step 3 ドロップダウンリストでユーザー部門を選択するか、ユーザーID/名前を入力しドアリストを選択します。

Step 4 [完了]をクリックして構成を完了します。

付録1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するものです。IPビデオ監視はサイバーリスクの影響を受けませんが、ネットワークおよび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対策を講じることで、攻撃を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取られる必須のアクション：

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。

・2種類の文字を含めた8文字以上の文字（大文字、小文字、数字、記号を含む）
・アカウント名そのものやを逆の順序にしたりしないでください。
・123、abcなどの連続文字を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。

ハイテク業界の標準手順に従って、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が確実に適用されるようにします。

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、メーカーがリリースしたアップデートのタイムリーな情報を取得してください。

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ください。

機器のネットワークセキュリティを改善するための「必要な」推奨事項

1 物理的な保護

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。例えば、機器を特別なコンピューター室とキャビネットに配置し、よく行われたアクセス制御許可とキー管理を実装して、ハードウェアの損傷、リムーバブル機器の不正接続（USBフラッシュディスク）シリアルポート等。

2 パスワードを定期的に変更する

推測やクラックの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をタイムリーにリセット

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、パスワードのリセットに関する関連情報を時間内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、簡単に推測できる質問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保証するためこの機能を保持することをお勧めします。

間違ったパスワードで数回ログインすると、アカウントと送信元IPアドレスがロックされます。

5 デフォルトのHTTPおよびその他のサービスポートの変更

デフォルトのHTTPおよび他のサービスポートを1024～65535の任意の数値セットに変更して、部外者が使用しているポートを推測できるリスクを減らすことをお勧めします。

6 HTTPSを有効にする

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

7 ホワイトリストを有効にする

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。お使いのコンピューターの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必ず追加してください。

8 MACアドレスバインディング

ゲートウェイのIPアドレスと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減らすことをお勧めします。

9 アカウントと特権を合理的に割り当てる

ビジネスおよび管理の要件に従って、ユーザーを合理的に追加し、最小限の権限セットを割当てます。

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、次のサービスを含むがこれらに限定されないセーフモードを使用してください。

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：TLSを選択してメールボックスサーバーにアクセスします。
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。

5 オーディオとビデオの暗号化された伝送

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、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減らすことをお勧めします。
注意：暗号化された送信は、送信効率の低下を引き起こします。

6 安全な監査

オンラインユーザーの確認：オンラインユーザーを定期的に確認して、デバイスが許可なくログインしているかどうかを確認することをお勧めします。
機器ログの確認：ログを表示することにより、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知ることができます。

7 ネットワークログ

機器のストレージ容量が限られているため、保存されるログは制限されています。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、重要なログがトレースのためにネットワークログサーバーと同期されるようにすることをお勧めします。

8 安全なネットワーク環境を構築する

機器の安全性をより確実に確保し、潜在的なサイバーリスクを減らすために、以下をお勧めします。
外部ネットワークからイントラネットデバイスへの直接アクセスを避けるために、ルーターのポートマッピング機能を無効にします。

■ネットワークは、実際のネットワークのニーズに応じて分割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減らします。