BioStar 2 管理者ガイド

BioStar 2.9.4 第1版

1 目次

2 はじめに

本文書は、Suprema 社の製品である BioStar 2 の設置に関する説明や搭載機能の基本的な説明を記述しています。

本文書の内容は、Suprema 社から発行されるドキュメント（英語版）を日本語に翻訳したものです。

本文書の翻訳に誤りが含まれている可能性があります。

正確な情報を確認するために、Suprema 社から発行された英語のドキュメントを参照してください。

本文書の内容は、予告なく変更される場合があります。

3 BioStar2 概要

BioStar 2 は、OS に依存せずに使用できる Web ベースのアクセスコントロールシステムです。

ライセンス

ライセンスを適用することにより、さまざまな機能が有効化されます。

ライセンスの内容は、弊社が提供する仕様書をご覧ください。

BioStar2 と端末ファームウェアの互換性

BioStar 2.9.4 と互換性のあるファームウェア

BioLite Net: 2.3.5 もしくは、それ以降

BioEntry Plus: 2.3.4 もしくは、それ以降

BioEntry W: 2.3.4 もしくは、それ以降

Xpass: 2.4.4 もしくは、それ以降

Xpass S2: 2.4.4 もしくは、それ以降

BioStation 2: 1.10.1 もしくは、それ以降

BioStation A2: 1.9.1 もしくは、それ以降

BioStation L2: 1.6.1 もしくは、それ以降

BioEntry W2: 1.7.1 もしくは、それ以降

FaceStation 2: 1.5.3 もしくは、それ以降

CoreStation: 1.6.1 もしくは、それ以降

BioEntry P2: 1.4.4 もしくは、それ以降

BioEntry R2: 1.4.1 もしくは、それ以降

BioLite N2: 1.6.0 もしくは、それ以降

XPass D2: 1.3.2 もしくは、それ以降

XPass D2 (Rev 2): 1.7.1 もしくは、それ以降

FaceLite: 1.3.4 もしくは、それ以降

XPass 2: 1.3.2 もしくは、それ以降

FaceStation F2: 2.1.4 もしくは、それ以降

X-Station 2: 1.2.2 もしくは、それ以降

OM-120: 1.2.1 もしくは、それ以降

Secure I/O 2: 1.3.1 もしくは、それ以降

DM-20: 1.2.2 もしくは、それ以降

IM-120: 1.0.0 もしくは、それ以降

BioStation 3: 1.1.1 もしくは、それ以降

4 インストレーション

BioStar 2 を使用してアクセスコントロールシステムを導入する前に、BioStar 2 サーバーを管理 PC にインストールします。

システム要件

弊社が提供する仕様書をご覧ください。

BioStar2 インストール

弊社が用意するインストール手順書をご覧ください。

メモ

- 32 ビット オペレーティング システム用のインストール ファイルは、BioStar 2.9.2 からは提供されません。
- BioStar 1 がインストールされている PC に BioStar 2 をインストールしないでください。これにより、パフォーマンスの問題が発生する可能性があります。
- BioStar 2.3.0 が BioStar 2.2.1 または 2.2.2 インストールの上にインストールされている場合、SQLite データベースに保存されているすべての情報が新しい MariaDB データベースに移行されます。

BioStar 2 アップグレード

アップグレードパスに従ってアップグレードしてください。

現在	アップグレードパス
2	2.2.1 > 2.3 > 2.4 > 2.4.1 > 2.5.0 > 2.6.4 > 最新バージョン
2.2 2.2.1 2.2.2	2.3 > 2.4 > 2.4.1 > 2.5.0 > 2.6.4 > 最新バージョン
2.3	2.4 > 2.4.1 > 2.5.0 > 2.6.4 > 最新バージョン
2.4	2.4.1 > 2.5.0 > 2.6.4 > 最新バージョン
2.5 2.6	2.6.4 > 最新バージョン
2.6.4 以上	最新バージョン

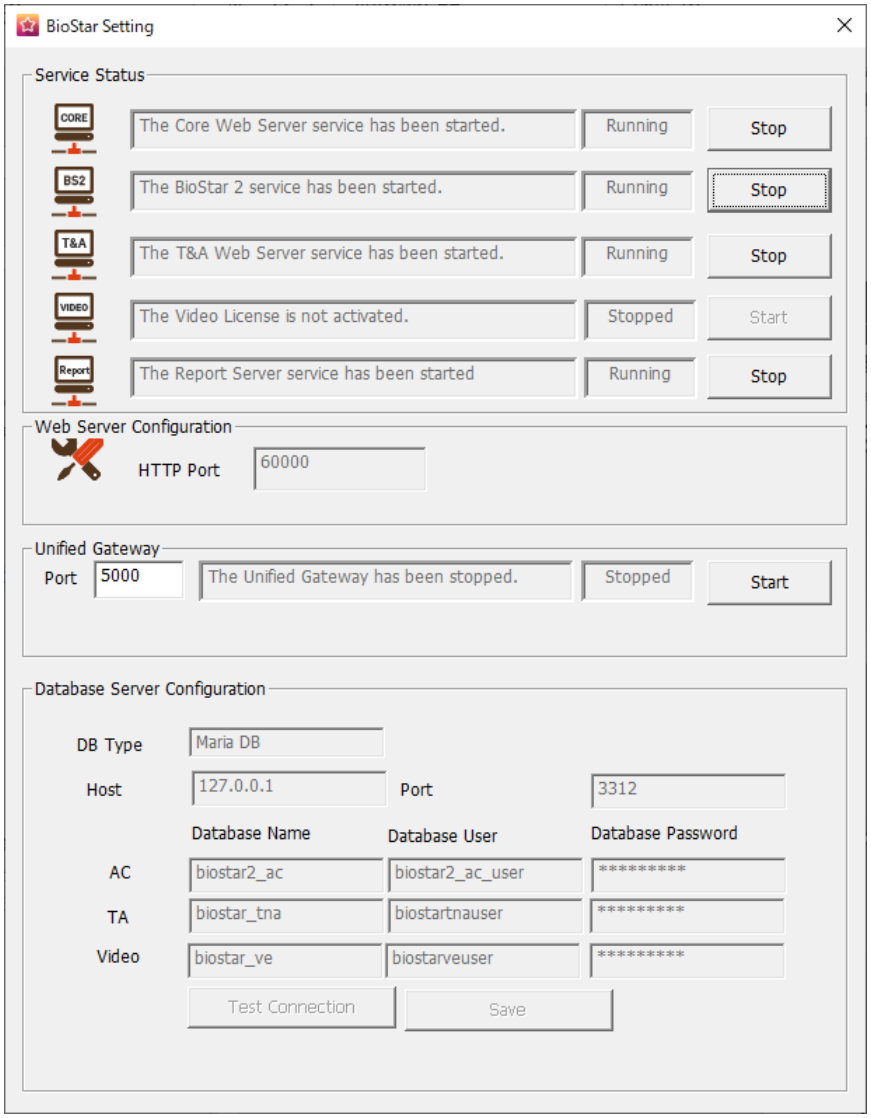
メモ

- Windows 8.1 または Windows Server 2012 R2 を使用している場合は、次の Web ページを参照して KB2919355 更新プログラムをインストールしてください。
  https://support.microsoft.com/en-us/help/2919355/windows-rt-8-1--windows-8-1--and-windows-server-2012-r2-update-april-2
- 古いバージョンの BioStar 2 からデータベースをバックアップする場合は、すべてのサービスと手順を無効にしてください。
  また、AC データベースと TA データベースを一緒にバックアップおよびリストアしない場合、TA データベースを使用できません。
- BioStar 2 のデータベースをバックアップする場合は、¥Program Files¥BioStar 2 (x64)¥util フォルダーの enckey と、¥Program Files¥BioStar 2(x64)の system.conf および setting.conf ファイルも必ずバックアップしてください。
- 弊社の用意するインストール手順通りにインストールする場合、BioStar 2 が使用するポートの初期値は以下です。別のプログラムが同じポートを使用している場合、BioStar 2 が正しく動作しない可能性があります。

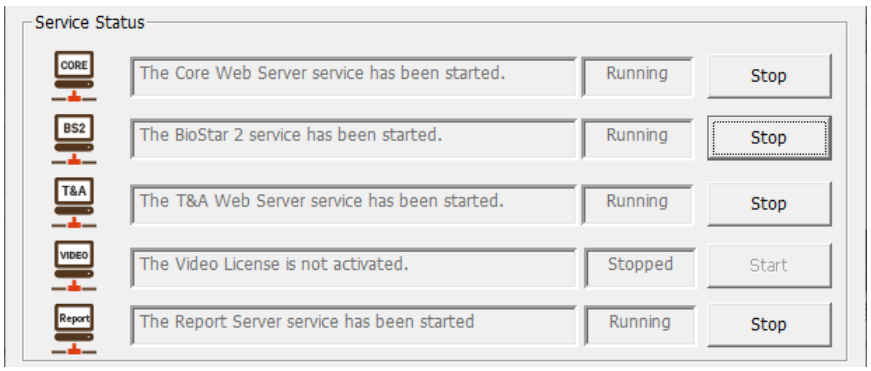
5 BioStar 2 サーバーサービスの再起動

BioStar 2 サーバーの状態を確認し、サーバーを停止または開始できます。

1 [スタート] > [すべてのプログラム] > [BioStar 2] > [BioStar Settings]をクリックします。



2 停止したいサーバーの[Stop ボタン]をクリックします。



3 [Start]ボタンをクリックして、サーバーを再起動します。

メモ

BioStar 2 サーバーの時刻設定が変更された場合は、コア Web サーバーを停止して再起動します。
行わない場合、BioStar 2 が正しく動作しない可能性があります。

6 ご使用になられる前に

BioStar 2 は、アクセスコントロールに関する WEB ベースのサービスとさまざまな機能を提供します。

BioStar 2 で設定するアクセスグループとは、入退室のアクセス権限のことです。

アクセスグループは、ユーザー、アクセスレベル、ドア(端末)の情報を組み合わせて設定します。

BioStar 2 の使い方の流れについては、以下のステップを参照してください。

1 ライセンスを適用する

BioStar 2 ライセンスを購入した後、適用することで、より多くの機能を使用できます。

➢ 関連情報

ライセンス

2 端末の追加

BioStar 2 に接続する端末を追加します。

端末種別ごとに認証モードの設定や各端末に管理者を割り当てることができます。

端末で発生するさまざまなイベント（認証失敗、強制指紋認証、アンチパスバック違反など)に応じて実行するアクションの設定を行えます。

➢ 関連情報

端末グループの追加と管理

基本的な検索と登録

指定端末検索と登録

スレーブ端末の検索と登録

端末の設定と情報の編集

3 ドアの追加と構成

端末が設置されているドアの情報を追加します。リレー、アンチパスバック、二重認証、警報などの設定を行えます。

➢ 関連情報

ドアグループの追加と管理

ドアを追加する

4 アクセスレベルの設定

ドアとスケジュールの情報を組み合わせて、アクセスレベルを作成できます。

複数のドアとスケジュールを 1 つのアクセスレベルに登録できます。

➢ 関連情報

アクセスレベルの追加と管理

5 アクセスグループの設定

アクセスレベル(ドアとスケジュール)とユーザー情報を組み合わせて、アクセスグループを作成できます。

1 つのアクセスグループに複数のアクセスレベルとユーザーを登録できます。

➢ 関連情報

アクセスグループの追加と管理

6 ユーザーの追加

ユーザー情報、顔、指紋、カードなどのアクセスコントロールに使用する情報を追加します。

ユーザー情報は、BioStar 2 を実行している PC に登録しますが、画面がある端末であれば端末で登録することも可能です。

端末内に登録されているユーザー情報を BioStar 2 にアップロードや BioStar2 内に登録されているユーザー情報を端末に転送できます。

➢ 関連情報

ユーザーグループの追加と管理

ユーザー情報の追加

ユーザー認証情報の追加

7 ゾーン設定

アンチパスバックや火災警報などのゾーンの設定を行えます。

アクセスコントロールのスタンダードライセンス以上を購入した場合のみ利用できます。

➢ 関連情報

ゾーン

ゾーン状態

8 ログの表示

イベントログ、端末状態、ドア状態、警告履歴の表示、リアルタイムのログ情報の表示を行えます。

➢ 関連情報

イベントログ

リアルタイムログ

端末の状態

ドアの状態

警告履歴

7 ダッシュボード

ダッシュボードメニューでは、主要なイベントの状況や使用状況がグラフィカルに表示されます。

お知らせ(お客様番号)や警報などの確認も行えます。

1	期間別の警告イベント状況	4	お知らせ
2	利用量	5	警告リスト
3	警報モニター		

メモ

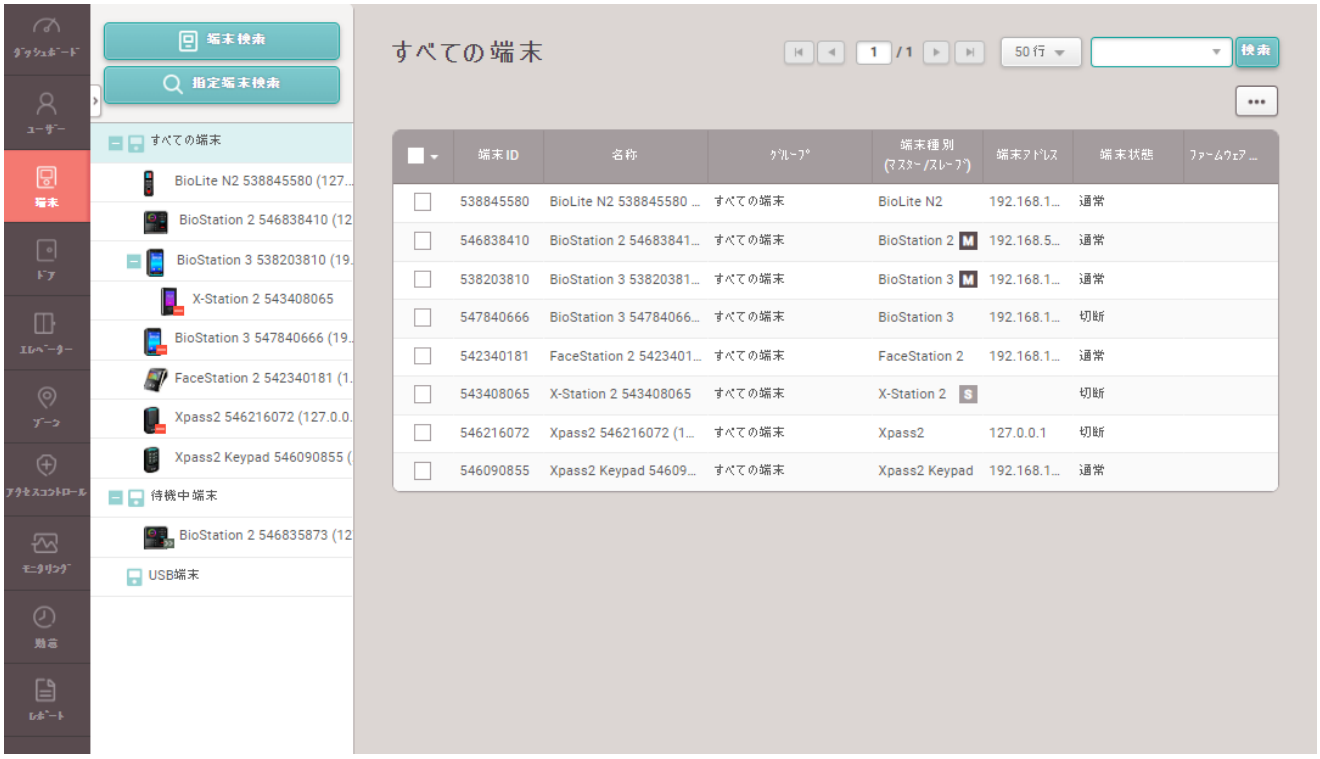
- [設定] > [警告]にて、何を表示するかを設定できます。
- 「警報モニター」には、過去 1 ヶ月間に見逃した 15 件の警報が新しい順に表示されます。
- 警告リストのアイコンをクリックすると、監視対象の警告の一覧を表示し、メモを書き込むことができます。

➢ 関連情報

警報履歴

8 端末

端末メニューでは、端末についての様々な設定を行えます。



- 端末グループの追加と管理
- 基本的な検索と登録
- 指定端末検索と登録
- Wiegand 端末の検索と登録
- スレーブ端末の検索と登録
- CoreStation での 3rd パーティ製 OSDP 端末の登録と交換
- 端末別ユーザー情報の整理
- ファームウェアのアップグレード
- 端末の設定と情報の編集

1	端末検索	5	機能ボタン （データ削除＆端末同期、印刷、カラム設定）
2	指定端末検索	6	端末一覧
3	ページナビゲーションボタンとリストの行数	7	端末と端末グループ一覧
4	登録端末検索	8	展開ボタン

メモ

登録された端末は、登録端末検索で「端末 ID、端末名称、端末 IP アドレス」を入力して検索できます。

端末一覧から端末を選択すると、以下の機能を使用できます。

端末一覧から複数の端末を選択すると、⑤「一括編集」の機能を使用できます。

項番	項目	説明
1	再接続	選択した端末を再接続します。 この機能は、端末が 1 つだけ選択されている場合に使用できます。
2	端末と同期	BioStar 2 からのユーザーおよびアクセスコントロール情報を登録済みの端末と同期します。 サーバーのデータベースの情報に基づいて同期が行われ、端末に存在するユーザーのみが削除されます。 [端末別ユーザー情報の整理]をクリックして、ユーザーを端末から BioStar サーバーにアップロード可能です。
3	データ削除&端末同期	端末の上のユーザー、アクセスグループ、スケジュールなどのユーザー関連データを削除し、サーバー上のデータを端末に転送できます。 端末一覧ページで、対象端末を選択し、機能ボタン(•••)をクリックして、[データ削除&端末と同期]を選択します。
4	一括編集	複数の端末の情報を一度に編集します。 この機能は、複数の端末が選択されている場合にのみ使用できます。
5	端末別ユーザー情報の整理	端末に登録されているユーザー情報を削除または BioStar 2 にアップロードします。
6	ファームウェアアップグレード	端末のファームウェアをアップグレードできます。
7	端末の削除	選択した端末を一覧から削除します。 ドアまたはゾーンとして設定されている端末は削除できません。

端末グループの追加と管理

複数の端末を管理するために、端末グループを登録できます。

端末グループの追加

1 [端末]をクリックします。

2 [すべての端末]を右クリックし、[端末グループを追加]をクリックします。

3 名前を入力します。

メモ

- 端末グループは、作成できる深さは最大 8 ネスト(階層)までできます。
- 端末グループ名は 48 文字まで入力できます。

端末グループの名前変更

1 [端末]をクリックします。

2 名前を変更するグループの名前を右クリックし、[端末グループの名称変更]をクリックします。

3 名前を入力します。

メモ

端末グループ名は 48 文字まで入力できます。

端末グループの削除

1 [端末]をクリックします。

2 削除するグループの名前を右クリックし、[端末グループを削除]をクリックします。

メモ

グループを削除すると、グループに含まれるすべての端末が削除されます。

基本的な検索と登録

BioStar 2 に接続されている端末を検索して登録できます。

端末を検索する前に、端末が正しく接続されているかどうかを確認してください。

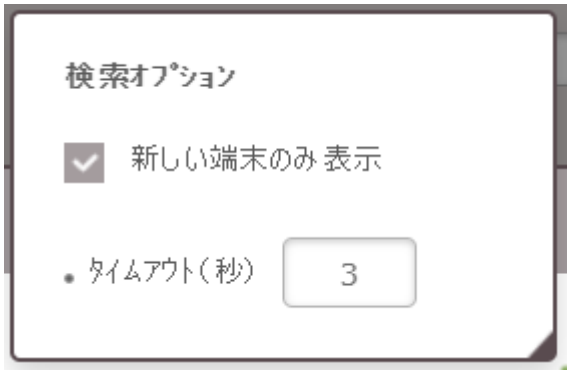
一度に複数の端末を追加する場合、各端末の位置、ID、および IP アドレスなどの情報を事前に控えておく必要があります。

1 [端末] > [端末検索]をクリックします。

2 登録可能なすべての端末が表示されます。

ユーザーID 種別が BioStar 2 と一致しない場合、端末のユーザーID 種別は BioStar 2 に従って自動的に変更されます。

3 新しく見つかった端末のみを表示するには、歯車アイコン( )をクリックしてから、[新しい端末のみ表示]をクリックします。



メモ

- デフォルトの時間内に応答しない端末を非表示にするには、歯車アイコン( )をクリックし、[タイムアウト(秒)]に時間を入力します。
- 探している端末がリストに表示されていない場合は、[検索]をクリックして端末を再度検索します。

4 見つかった端末の名前とグループを変更できます。

端末の IP アドレスを使用できない場合、または変更する必要がある場合は、[IP アドレス設定]をクリックして変更します。

5 動的 IP アドレスを使用するには、[DHCP 利用]を選択します。

IP アドレス、サブネットマスク、およびゲートウェイを手動で入力するには、[DHCP 利用]の選択を解除します。

BioStar 2 ネットワーク情報を入力するには、[端末 --> サーバー接続]を選択し、[サーバーアドレス]と[サーバーポート]を入力します。

6 IP 設定を保存するには、[適用]をクリックします。

7 設定済みの端末を登録するには、[追加]をクリックします。

8 登録済みの端末を選択し、[端末と同期]をクリックします。

メモ

- 新しい端末を追加すると、端末のキーがサーバー上のデータ暗号化キーの値に変更されます。
  キーを変更すると、端末の上のすべてのユーザーデータが削除されます。
- ユーザーを含むユーザー関連データを削除し、端末のグループとスケジュールにアクセスして、サーバー上のデータを端末に転送するには、[データ削除&端末同期]をクリックします。端末一覧ページで、対象端末を選択し、機能ボタン(•••)をクリックして、[データ削除&端末同期]を選択します。
- 端末を登録した後、[端末の設定と情報の編集]を参照して、その詳細を編集できます。
- すべての待機中端末を待機中端末グループに登録するには、グループ名を右クリックし、[待機中端末を追加]をクリックします。各端末を登録するには、端末名を右クリックして[待機中端末を追加]をクリックします。
- BioStar 2 と端末に異なるユーザーID 種別が設定されている場合は、BioStar 2 のユーザーID 設定に従って端末設定を変更します。
- BioStar 2 のユーザーID 種別が[英数字]に設定されている場合、一部の端末で使用できない場合や制限が発生する場合があります。詳細については、[サーバー]を参照してください。

指定端末検索と登録

端末の IP アドレスとポート番号を指定して端末を登録できます。

1 [端末] > [指定端末検索]をクリックします。

2 検索する端末の IP アドレスとポート番号を入力します。

3 [検索]をクリックして、見つかった端末のリストを表示します。
探している端末がリストに表示されていない場合は、[検索]をクリックして再度検索します。

4 見つかった端末を追加するグループを選択し、[追加]をクリックします。

5 登録済みの端末を選択し、[端末と同期]をクリックします。

メモ

端末を登録した後、[端末の設定と情報の編集]を参照して、その詳細を編集できます。

Wiegand 端末の検索と登録

マスター/スレーブ端末に接続された Wiegand 端末を簡単に追加できます。

1 [端末]をクリックします。

2 マスター/スレーブ端末の名前を右クリックして Wiegand 端末を検索し、[Wiegand 端末を追加]をクリックします。

3 マスター/スレーブ端末に接続されている Wiegand 端末のリストが表示されます。

4 追加する端末を選択し、[追加]をクリックします。

スレーブ端末の検索と登録

スレーブ端末を既存のマスター端末に追加することで、入退室管理システムのネットワークを簡単に拡張できます。

マスター端末とスレーブ端末を RS-485 で接続できます。

通常の端末に加えて、Secure I/O 2 などの追加の端末を接続できます。

1 [端末]をクリックします。

2 マスター端末の名前を右クリックしてスレーブ端末を検索し、[スレーブ端末を検索]をクリックします。

3 マスター端末に接続されているスレーブ端末の一覧が表示されます。

探している端末がリストに表示されていない場合は、[検索]をクリックして端末を再度検索します。

4 端末を登録するグループを選択し、[追加]をクリックします。

メモ

- 指紋認証機器がマスター端末の場合、顔認証機器をスレーブ端末として追加することはできません。
- 顔認証機器がマスター端末で、既に別のスレーブ端末が追加されている場合、顔認証機器をスレーブ端末として追加することはできません。
- 顔認証機器がマスター端末で、顔認証機器をスレーブ端末として接続する場合、スレーブ端末として追加できる顔認証機器は 1 台だけです。
- 顔認証機器をマスター端末とし、別の顔認証機器をスレーブ端末として接続する場合、Secure I/O 2 と DM-20 をそれぞれ 1 台ずつ追加接続できます。
- 接続できるスレーブ端末の最大数は、認証方法、ユーザー数、および端末の数によって異なります。
  また、スレーブ端末の数が認証速度に影響することにも注意してください。

3rd パーティ製 OSDP 端末の登録と交換

重要

本機能は弊社でサポート対象外の機能です。

3rd パーティ製 OSDP 端末の登録

3rd パーティの OSDP 端末を登録済みの CoreStation に追加します。

1 [端末]をクリックします。

2 CoreStation の名前を右クリックし、[OSDP 端末の追加]をクリックします。
マスター/スレーブ端末に接続されている Wiegand 端末のリストが表示されます。

3 ポートのリストが表示されます。
Port Status が Available のポートの中から、OSDP 端末を追加するポートを選択します。

メモ

CoreStation のポートごとに最大 2 台、合計 8 台まで接続できます。

4 情報、ネットワーク(RS-485)、認証を設定します。

項目	説明
情報	・ 名前:端末名を入力します。入力しない場合は、自動的に割り当てられます。 ・ ステータス:端末の状態を設定します。Inactive に設定すると、CoreStation は OSDP 端末と通信しません。
ネットワーク (RS-485)	・ OSDP ID:OSDP 端末のアドレスを入力します。0 ～ 126 の数値を入力します。 ・ 安全な通信:CoreStation と OSDP 端末間の通信は、SCB キーで保護できます。Secure Communication が Use に設定されている場合、CoreStation は SCB キーを OSDP 端末に送信します。OSDP 端末は、この SCB キーを使用して、安全なチャネルを介して CoreStation との間でデータを送受信できます。
認証	・ 認証モード:OSDP 端末の認証モードを設定できます。BioStar 2 は、カードと PIN の組み合わせを認証モードとして使用できます。 メモ ・ [+追加]をクリックし、利用可能なオプションをドラッグアンドドロップして認証モードを作成します。スケジュールを選択して[OK]をクリックすると、認証モードが登録されます。希望のスケジュールがない場合は、[+スケジュールを追加]をクリックして作成します。 ・ スケジュールの設定の詳細については、「スケジュール」を参照してください。 ・ フルアクセス: アクセスグループを設定せずに、OSDP 端末内に登録されているユーザーにフルアクセスを許可できます。 ・ 認証タイムアウト:認証モードで複数の認証資格の組み合わせを使用する場合、システムは 2 番目の認証資格を認証するためにこの時間待機します。最初の認証資格を認証した後、2 番目の認証資格を認証するためのタイムアウト期間を設定します。この時間内に 2 番目の認証資格が入力されない場合、認証は失敗します。

5 [OK]をクリックして、構成済みの OSDP 端末を登録します。

メモ

接続された OSDP リーダーの LED/ブザー動作を設定します。OSDP 端末 LED/ブザーの詳細な設定については、OSDP 端末 LED/ブザーを参照してください。

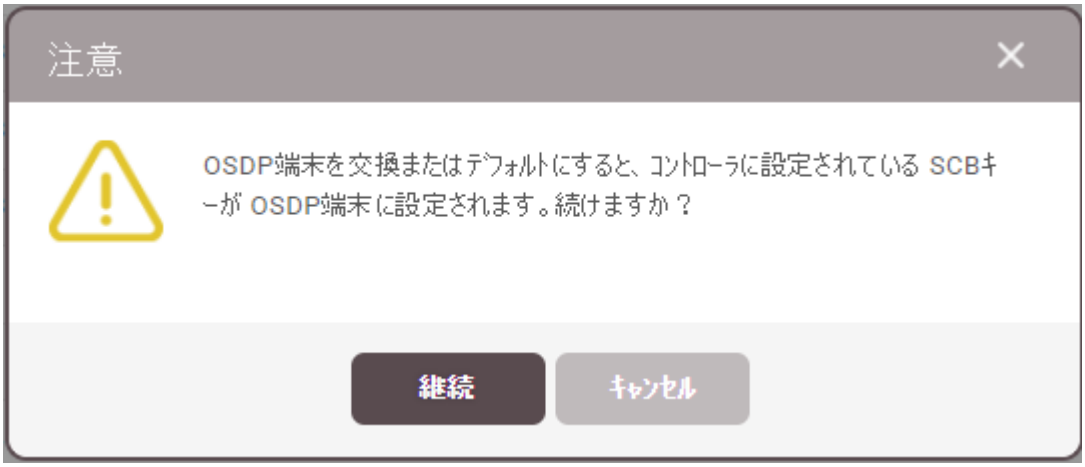
3rd パーティ製 OSDP 端末の交換

CoreStation に登録されている OSDP 端末を別のデバイスに置き換えます。

1 [端末]をクリックします。

2 CoreStation に登録されている OSDP 端末のうち、交換する OSDP 端末の名前を右クリックし、[Replace OSDP Device]をクリックします。

3 警告ポップアップ メッセージを読んだ後、[続行]をクリックします。OSDP 端末の交換プロセスが続行されます。



メモ

OSDP 端末が切断されている場合、または SCB キーが既に設定されている場合、OSDP 端末の交換は失敗する可能性があります。デバイスと SCB キーの接続状態を確認してから、再試行してください。

U&Z 無線ドアロックの登録

CoreStation に登録された無線ドアロックを追加します。

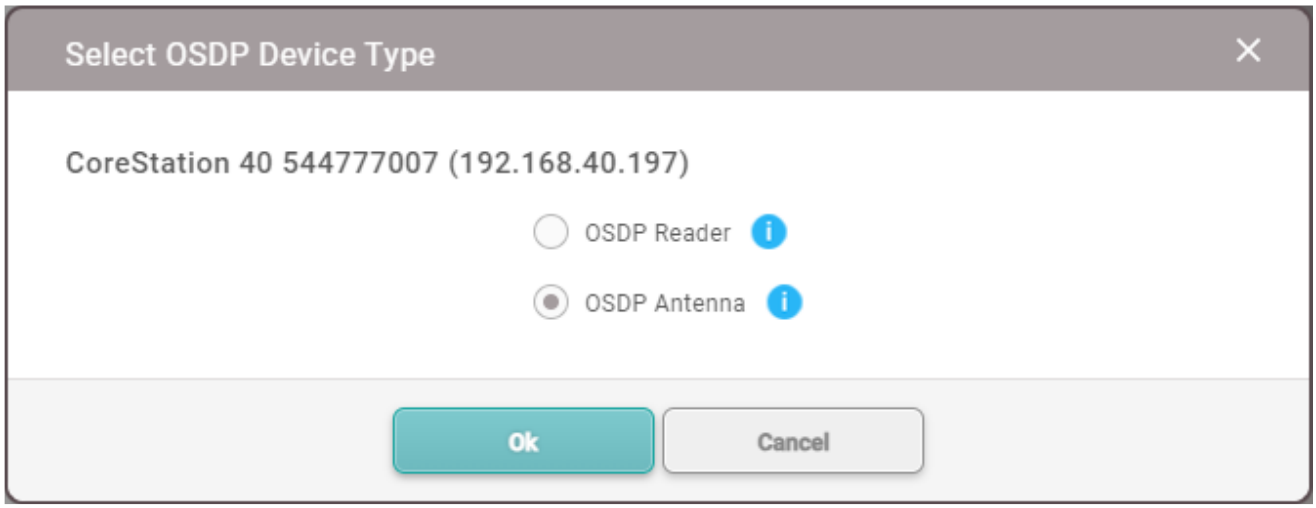
メモ

- U&Z 無線ドアロックは、CoreStation v1.7.1 以降および BioStar 2 v2.9.4 以降で使用できます。
- U&Z 無線ドアロックを接続するには、無線アンテナモジュールを CoreStation に接続する必要があります。接続できる無線アンテナモジュールは 1 つだけです。
- 1 つの CoreStation に接続できる U&Z 無線ドアロックの最大数は 8 です。
- BioStar 2 では、U&Z 無線ドアロックの交換はサポートされていません。

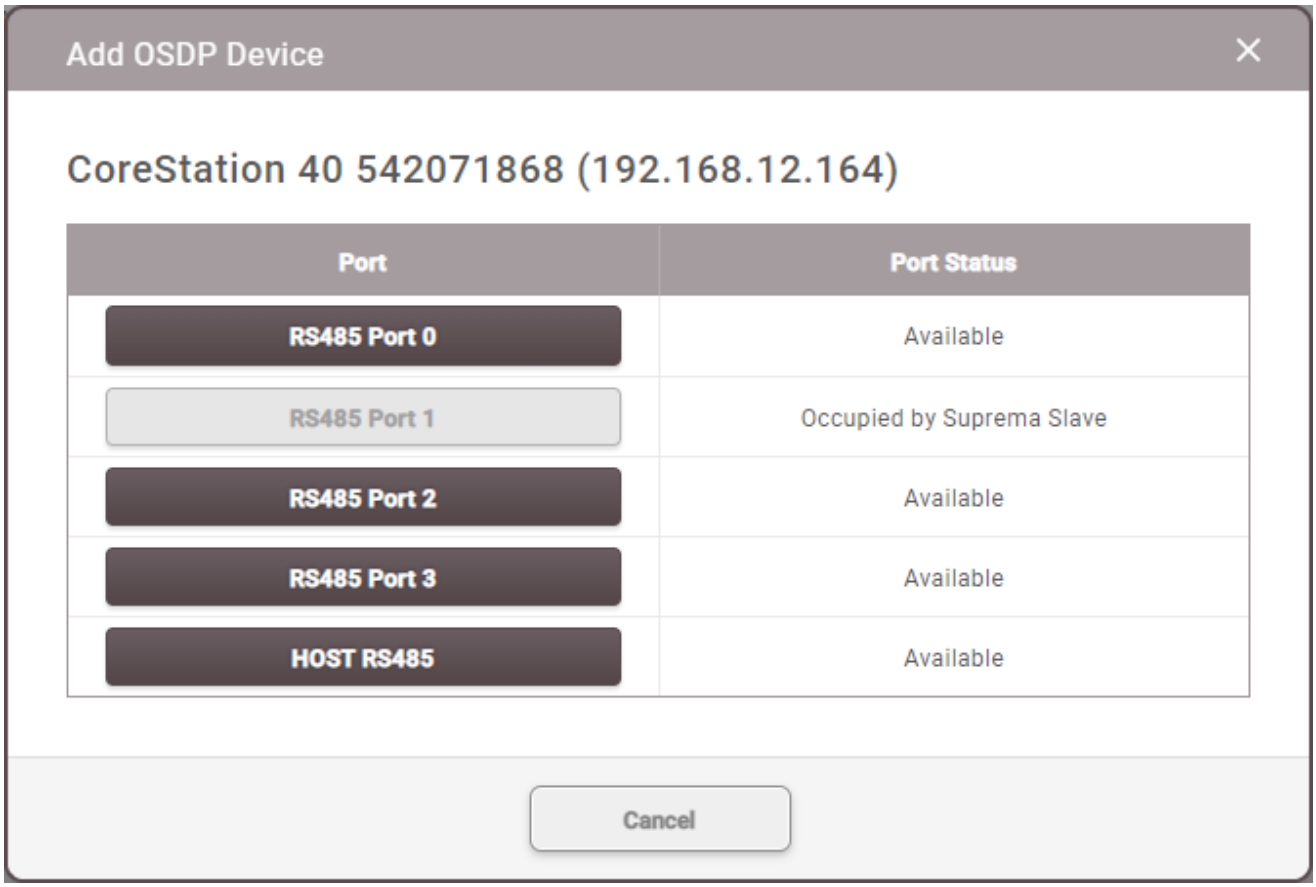
1 [端末]をクリックします。

2 CoreStation の名前を右クリックし、[OSDP 端末の追加]をクリックします。

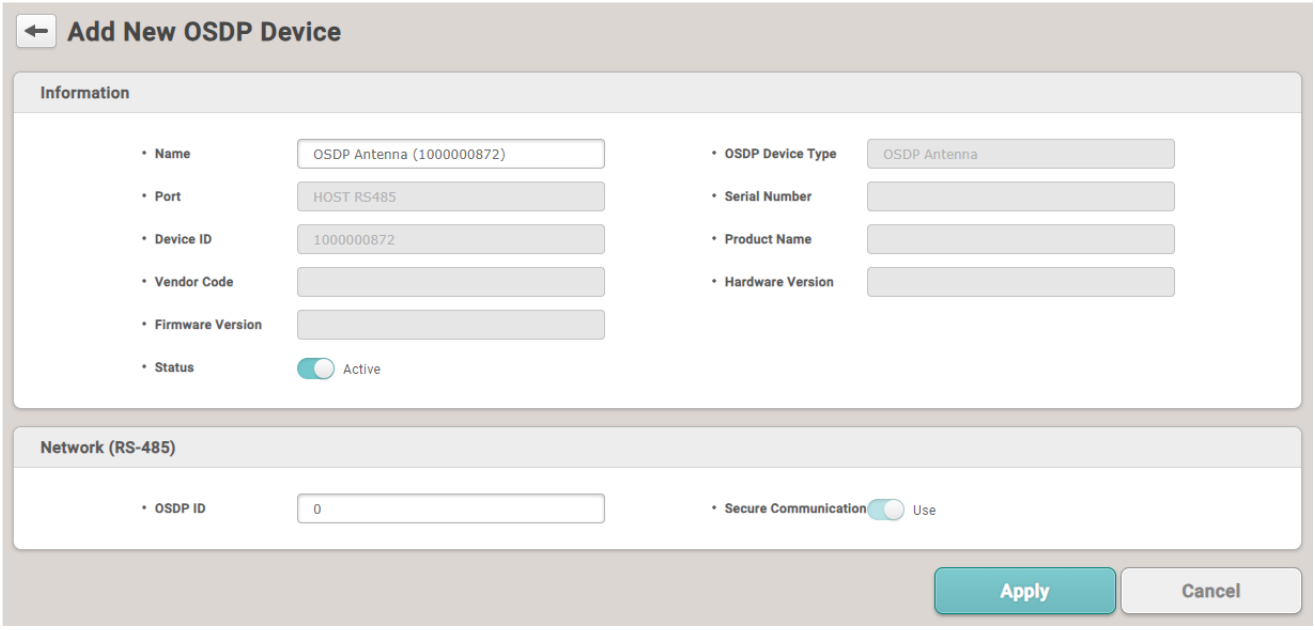
3 [OSDP 端末種別の選択]ウィンドウが表示されます。OSDP アンテナを選択します。



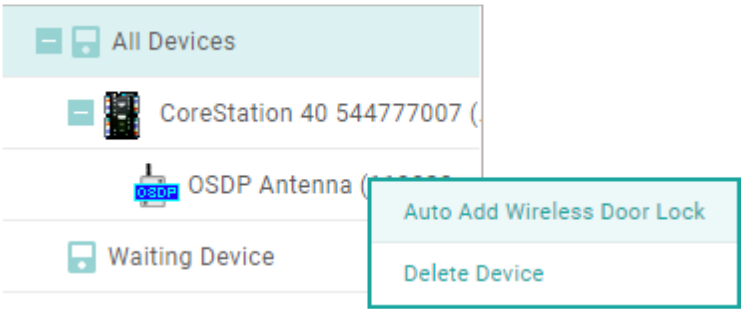
4 ポートのリストが表示されます。Port Status が「Available」になっているポートのうち、OSDP アンテナを追加するポートを選択します。



5 情報、ネットワーク(RS-485)を設定し、適用をクリックします。



6 追加した OSDP アンテナを右クリックし、[ワイヤレス ドア ロックの自動追加] をクリックします。



7 U&Z ワイヤレス ドア ロックに付属の SERVICEKEY カードをタグ付けします。

8 OSDP アンテナはワイヤレス ドア ロックに接続します。

➢ 関連情報

U&Z 無線ドアロック

端末別ユーザー情報の整理

端末に保存されているユーザー、指紋、顔、およびカードの数を確認できます。

端末に保存されているユーザー情報と、BioStar 2 に登録されているユーザー情報を比較したり、BioStar 2 に情報を転送したり、情報を削除できます。

メモ

端末内のユーザーの管理機能は、1 つの端末が選択されている場合にのみ使用できます。

1 [端末]をクリックします。

2 端末を選択し、[端末別ユーザー情報の整理]をクリックします。

端末に登録されているユーザー情報と、BioStar 2 に登録されているユーザー情報を比較して表示します。

項目	説明
同じ	ユーザーの情報は、BioStar 2 内に登録されている情報と同じです。
不一致	ユーザーの情報が、BioStar 2 に登録されている情報と異なります。
新しいユーザー	ユーザーは BioStar 2 に登録されていません。

3 ユーザー情報を選択したら、[削除]をクリックして削除するか、[アップロード]をクリックして BioStar 2 にアップロードします。

[アップロード]をクリックすると、BioStar 2 に同じ ID のユーザー情報が含まれている場合、端末内の情報で更新できます。

メモ

- 端末を登録した後、[端末の設定と情報の編集]を参照して、その詳細を編集できます。
- ユーザー情報を削除すると、端末からのみ削除され、BioStar 2 の情報はそのまま残ります。

ファームウェアのアップグレード

BioStar 2 に接続された端末のファームウェアをアップグレードできます。

ダウンロードしたファームウェアファイルを次のフォルダーにコピーします。

フォルダーが存在しない場合は、作成する必要があります。

・

・ 64 ビット オペレーティング システム: C:¥Program Files¥BioStar 2(x64)¥firmware

1 [端末]をクリックします。

2 端末を選択し、[ファームウェアアップグレード]をクリックします。同じ種別の複数の端末を一括アップグレードできます。

3 ファームウェアバージョンをクリックすることで、アップグレードを開始します。

メモ

- 同じ RS-485 モードの複数の端末を同時にアップグレードすることができます。
  たとえば、多数のマスター端末を同時にアップグレードでき、多数のスレーブ端末も同時にアップグレードできます。
- 多数のマスター端末またはマスター端末を持たないスレーブ端末を同時にアップグレードすることができます。
- 同じマスター端末に接続されている複数のスレーブ端末を同時にアップグレードすることはできません。

・ 関連情報

情報

端末の設定と情報の編集

登録した機器の詳細情報を編集できます。

端末の登録の詳細については、[端末検索と登録]または[指定端末検索と登録]を参照してください。

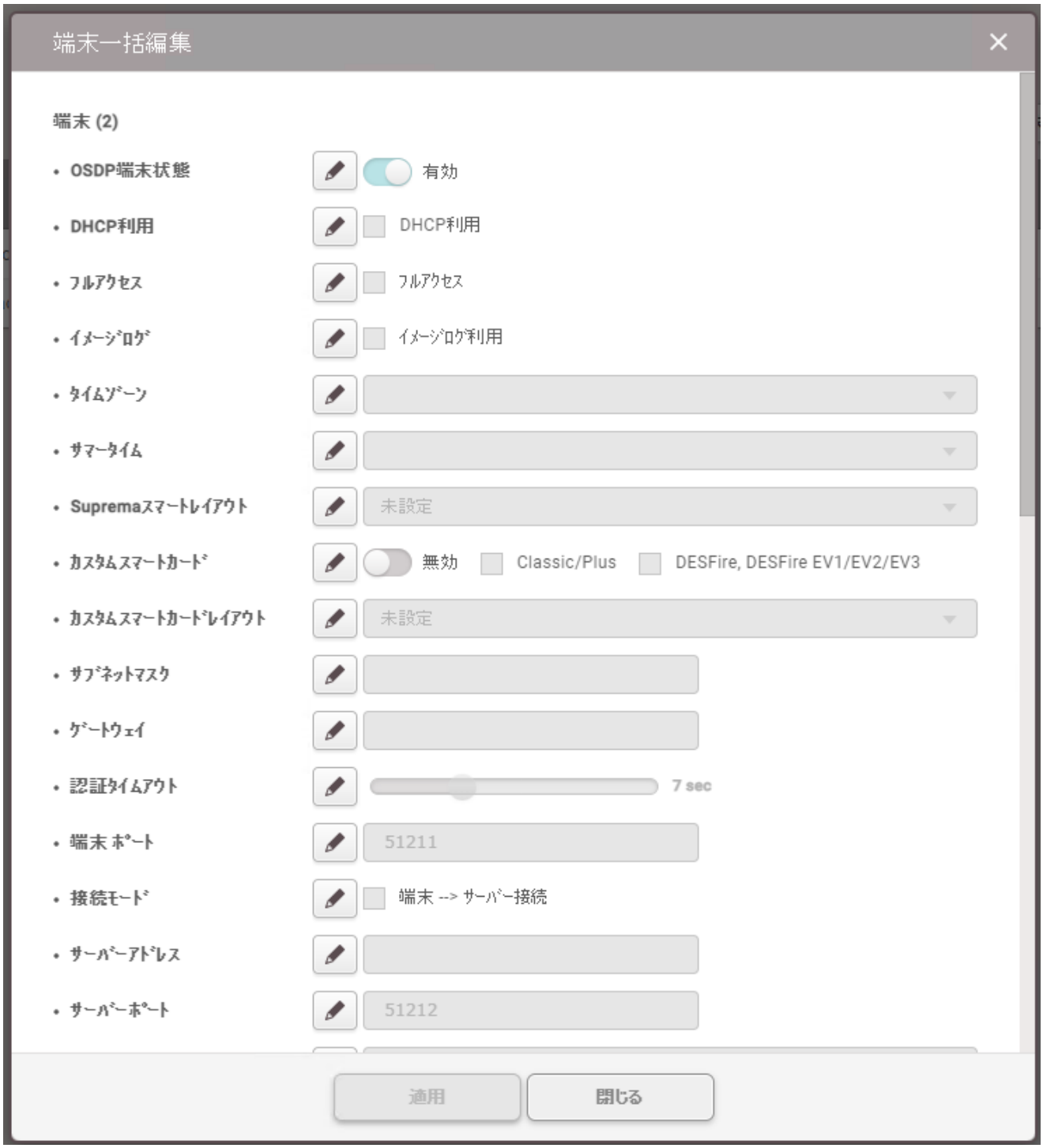
表示される詳細は、RS-485 接続種別または端末種別によって異なる場合があります。

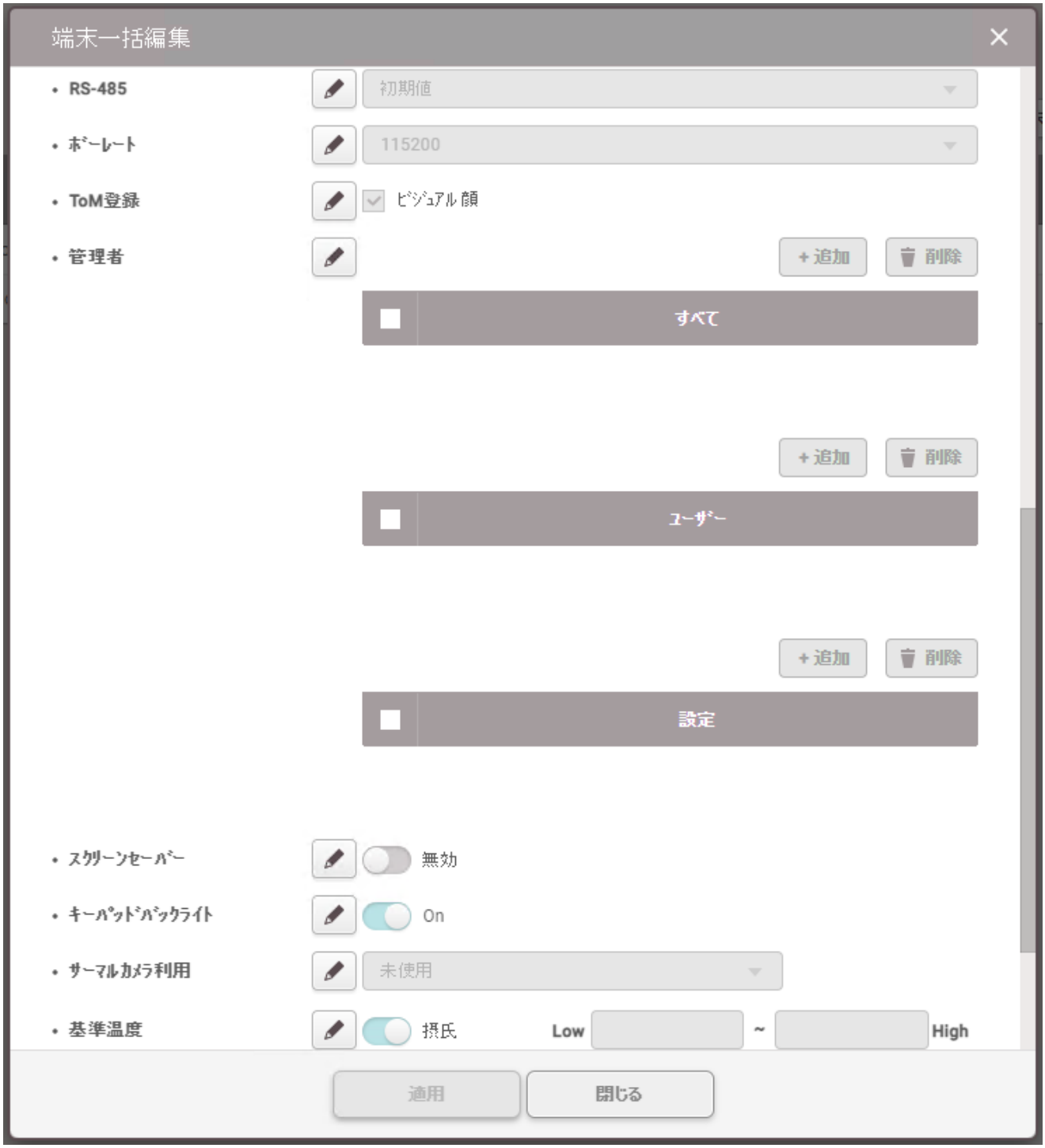
1 [端末]をクリックします。

2 端末一覧で編集する端末をクリックします。

3 [情報]、[ネットワーク]、[認証]、[詳細設定]、[サーマル&マスク]、[SIP インターホン]、[RTSP]、[DM-20]、[OM-120]、[CoreStation]、[Wiegand 端末]を参照してフィールドを編集します。

4 複数の端末の情報を編集するには、複数の端末を選択して[一括編集]をクリックします。





5 編集したいフィールドのえんぴつアイコン(✎)をクリックして、情報を編集します。

6 すべての情報を編集したら、[適用]をクリックします。

メモ

- 一括編集に表示されるフィールドは、選択した端末種別によって異なる場合があります。
- マスター端末とスレーブ端末の両方を選択して[一括編集]をクリックすると、[認証]フィールドと[表示/サウンド]フィールドの一部のみを編集できます。

情報

端末の名前とグループを入力または編集できます。

ファームウェアアップグレードもこの項目で可能です。

[情報]タブのフィールドを編集します。

項番	項目名	説明
1	名称	端末名を入力します。
2	端末 ID	端末 ID を表示します。
3	ファームウェアバージョン	[ファームウェアアップグレード]をクリックして、 新しいファームウェアバージョンをインストールします。
4	カーネルバージョン	カーネルバージョンを表示します。
5	工場出荷時設定	端末の設定をリセットします。 ・ リセット：すべての設定をリセットします。 ・ ネットワーク設定以外：ネットワーク設定を除くすべての設定をリセットします。
6	タイムゾーン	端末のタイムゾーンを設定します。
7	サマータイム	端末にサマータイムを適用します。 新しいサマータイムルールを追加するには、サマータイムを参照してください。
8	グループ	端末グループを変更します。端末グループの追加の詳細については、端末グループの追加と管理を参照してください。
9	端末種別	端末種別を表示します。
10	装置タイプ	モデル名を表示します。
11	ハードウェア バージョン	ハードウェアバージョンを表示します。
12	ロック中	ロック解除ボタンは、端末がトリガーおよび動作などによって端末利用不可(無効)になっている場合に使用できます。
13	サーバーと時刻同期	端末の時刻情報をサーバーと同期するオプションを選択します。
14	表示日時	日付と時刻を手動で設定するには、をクリックします。

		[サーバーと時刻同期]オプションが選択されている場合、日付と時刻を手動で選択することはできません。
15	端末時刻取得	ボタンをクリックすると、端末に設定されている時刻を取得します。
16	時刻設定	ボタンをクリックすると、BioStar 2 に設定された時刻を端末に適用します。

1 [適用]をクリックして設定を保存します。

メモ

イベントログとリアルタイムログに記録されるので、正しい日付と時刻を設定してください。

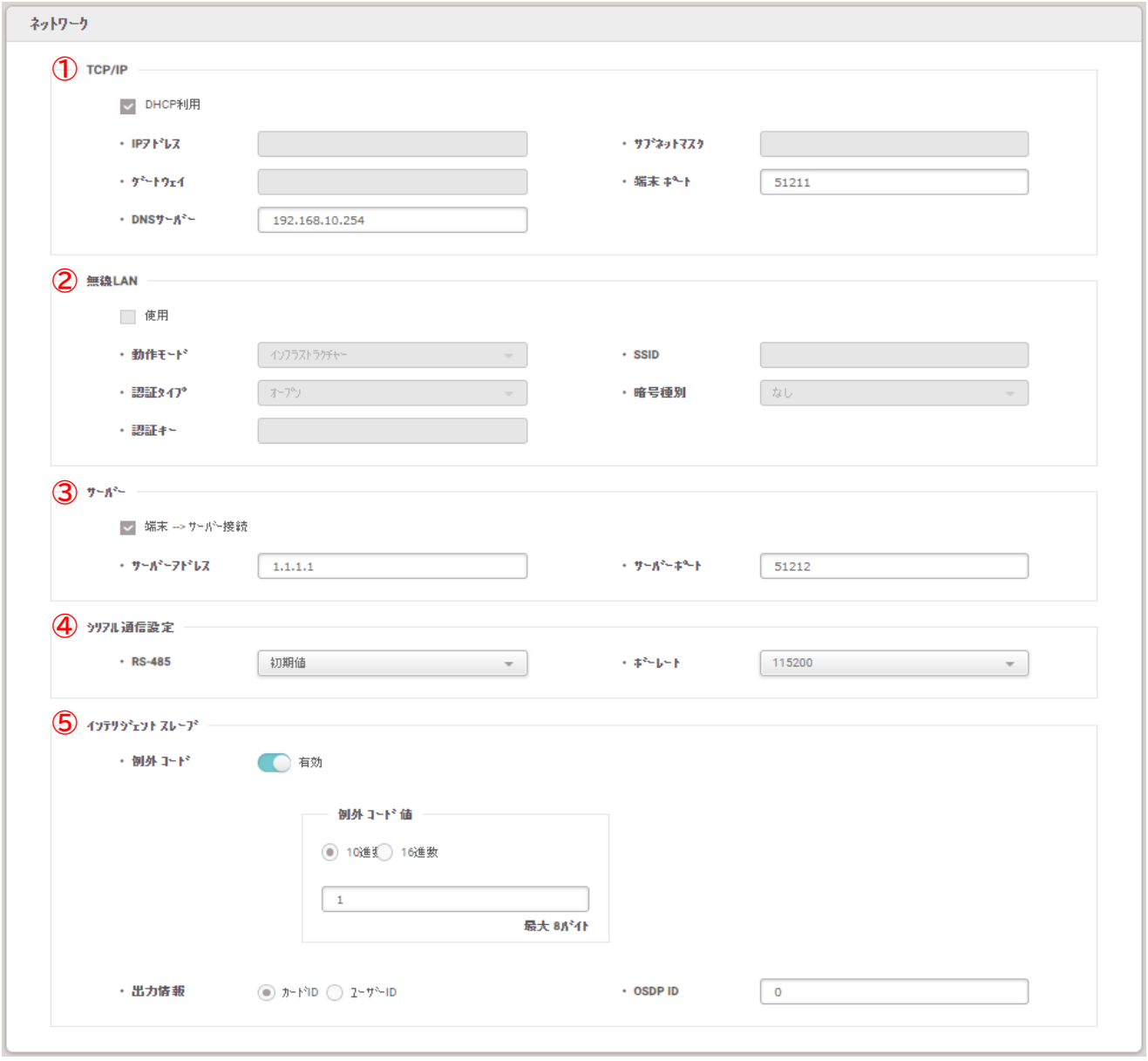
ネットワーク

TCP/IP や RS-485 など、様々な接続設定を行うことができます。

メモ

編集可能なフィールドは、端末種別によって異なります。

1 [ネットワーク]タブのすべてのフィールドを編集します。



項番	項目名	説明
1	TCP/IP	端末の TCP/IP 接続設定を設定できます。 ・ DHCP 利用：このオプションを選択して、端末が動的 IP アドレスを使用できるようにします。このオプションを選択すると、ネットワーク設定を入力できません。 ・ IP アドレス、サブネットマスク、ゲートウェイ：デバイスのネットワーク設定を入力します。

		・ 端末ポート: 端末が使用するポートを入力します。 ・ DNS サーバー: DNS サーバーのアドレスを入力します。 **メモ** DNS サーバーアドレスを入力できる機器とファームウェアのバージョンは以下です。 BioStation L2 FW 1.0.0 以降 BioStation A2 FW 1.0.0 以降 BioStation 2 FW 1.2.0 以降 BioLite Net FW 2.2.0 以降 BioEntry Plus FW 2.2.0 以降 BioEntry W FW 2.2 .0 以降 Xpass FW 2.2.0 以降 Xpass S2 FW 2.2.0 以降 FaceStation 2 FW 1.0.0 以降 BioLite N2 FW 1.0.0 以降 FaceLite FW 1.0.0 以降 XPass 2 FW 1.0.0 以降 FaceStation F2 FW 1.0.0 以降 X-Station 2 FW 1.0.0 以降 BioStation 3 FW 1.0.0 以降
2	無線 LAN	無線 LAN をオンまたはオフにします。端末メニューから無線 LAN 関連の設定を行うこともできます。詳細については、端末のユーザーガイドを参照してください。 **メモ** ・ BioStation 2、BioStation A2、FaceStation 2、および BioStation 3 のみ。
3	サーバー	サーバーモードで使用する接続設定を入力できます。 ・ [端末 --> サーバー接続]: このオプションを選択して、端末に接続するための BioStar 2 設定を設定します。このオプションを選択すると、BioStar 2 サーバーのネットワーク設定を入力できます。 ・ サーバーアドレス: BioStar 2 サーバーの IP アドレスまたはドメイン名を入力します。 ・ サーバーポート: BioStar 2 サーバーのポート番号を入力します。 **メモ** サーバーアドレスにドメインアドレスを入力できる端末とファームウェアのバージョンは以下です。 BioStation L2 FW 1.0.0 以降 BioStation A2 FW 1.0.0 以降 BioStation 2 FW 1.2.0 以降 BioEntry W2 FW 1.0.0 以降

		BioEntry P2 FW 1.0.0 以降 FaceStation 2 FW 1.0 .0 以降 BioLite N2 FW 1.0.0 以降 BioLite Net FW 2.2.0 以降 BioEntry Plus FW 2.2.0 以降 BioEntry W FW 2.2.0 以降 Xpass FW 2.2.0 以降 Xpass S2 FW 2.2.0 以降 XPass 2 FW 1.0.0 以降 X-Station 2 FW 1.0.0 以降 BioStation 3 FW 1.0.0 以降
4	シリアル通信設定	RS-485 経由で接続された端末の接続モードとボーレートを設定できます ・ RS-485: RS-485 のモードを設定します。 ・ ボーレート: RS-485 接続のボーレートを設定します。
5	インテリジェントスレーブ	ユーザーが 3rd パーティ製コントローラーに接続された Suprema 端末で指紋認証を実行すると、認証結果が OSDP カード データとして送信され、複数の 1:1 または 1:N マッチングが実行されます。 ・ 例外コード: インテリジェントスレーブを使用する場合、10 進数または 16 進数の例外コードを送信して、認証失敗などの例外的な状況で正確なログを集計できます。 10 進数は 0 ～ 18446744073709551615、 16 進数は 0 ～ FFFFFFFFFFFFFFFF または 16 進数の文字を入力できます。 ・ 出力情報: 認証成功時にカード ID またはユーザーID を出力できます。 ・ OSDP ID: 端末の OSDP アドレスを入力します。0 ～ 126 の数値を入力できます。 **メモ** ・ インテリジェントスレーブは、シリアル通信設定の RS-485 オプションが[初期値]に設定されている場合にのみ有効になります。 ・ インテリジェントスレーブをサポートする端末とファームウェアのバージョンは以下です。 BioEntry W2 FW 1.6.3 以降 BioStation L2 FW 1.6.1 以降 BioEntry P2 FW 1.4.1 以降 XPass 2 FW 1.2.3 以降 X-Station 2 FW 1.1.0 以降 BioLite N2 FW 1.4.1 以降 FaceStation F2 FW 1.1.2 以降 BioStation 3 FW 1.0.0 以降 ・ 例外コードのデータサイズは 8 バイトまで入力できます。

2 [適用]をクリックして設定を保存します。

認証

端末のユーザー認証設定を設定できます。

> **メモ**
>
> 編集可能なフィールドは、端末種別によって異なります。

1 [認証]タブのすべてのフィールドを編集します。

一般設定

項番	項目名	説明
1	認証モード	端末の認証モードを設定できます。BioStar 2 は、認証モードとして指紋、ID、カード、PIN、および顔の任意の組み合わせを使用できます。 ・ [+追加]をクリックし、利用可能なオプションをドラッグアンドドロップして認証モードを作成します。スケジュールを選択して[OK]をクリックすると、認証モードが登録されます。希望のスケジュールがない場合は、[+スケジュール追加]をクリックして作成します。 ・ スケジュールの設定の詳細については、[スケジュール]を参照してください。
2	フルアクセス	アクセスグループを設定せずに、端末に登録されているユーザーにフルアクセスの権限を付与できます。
3	サーバーマッチング	サーバーマッチングの設定が可能です。有効に設定すると、BioStar 2 がインストールされている PC に保存されているユーザー情報を使用して認証が実行され、無効に設定すると、端末に保存されているユーザー情報を使用して認証が実行されます。 サーバーマッチングを使用する場合、BioStar 2 のサーバーマッチングも有効にする必要があります。 詳細については、[サーバー]を参照してください。 **メモ** サーバーマッチングが利用できる端末とファームウェアのバージョンは以下です。

		CoreStation FW 1.0.0 以降 BioEntry P2 FW 1.0.0 以降 BioEntry W2 FW 1.0.0 以降 BioStation L2 FW 1.0.0 以降 BioStation A2 FW 1.0.0 以降 BioStation 2 FW 1.2.0 以降 BioLite Net FW 2.2.0 以降 BioEntry Plus FW 2.2.0 以降 BioEntry W FW 2.2.0 以降 Xpass FW 2.2.0 以降 Xpass S2 FW 2.2.0 以降 BioLite N2 FW 1.0.0 以降 XPass D2 FW 1.0.0 以降 XPass 2 FW 1.0.0 以降 FaceStation 2 FW 1.4.0 以降 FaceStation F2 FW 1.0.0 以降 X-Station 2 FW 1.0.0 以降 BioStation 3 FW 1.0.0 以降 ・ FaceLite は、サーバーマッチングで使用できません。 ・ ビジュアル顔のサーバーマッチングは、FaceStation F2 および BioStation 3 では使用できません。
4	認証タイムアウト	[認証モード]にて、複数の認証資格の組み合わせを使用する場合、システムは 2 番目の認証資格を認証するため認証タイムアウトに設定した時間待機します。 最初の認証資格で認証した後、2 番目の認証資格で認証するまでのタイムアウト時間を設定します。 2 番目の認証資格が設定した時間内に認証されない場合、認証は失敗します。
5	顔検出レベル	ユーザーが認証しようとしたときに、端末に組み込まれたカメラで顔を認識するためのアルゴリズムステップを設定できます。 [通常]に設定すると、およそ腕の長さ程度の距離で顔を検出できます。 [高い]に設定すると、より短い距離で顔を検出できます。 [未使用]に設定すると、顔認識機能を使用できません。 **メモ** BioStation A2 および X-Station 2 のみ。

指紋

項番	項目名	説明
1	指紋	指紋に関する詳細な設定を行えます。 **メモ** ・ 編集可能なフィールドは、端末種別によって異なります。 ・ 画像の表示は、BioStation 2、BioStation A2、BioStation L2、BioLite N2、FaceStation F2 (FSF2-ODB)、および X-Station 2 (XS2-ODPB、XS2-OAPB) でのみ使用できます。 ・ 指紋 LFD は、BioStation A2、BioStation L2、BioEntry W2、BioLite N2、FaceStation F2 (FSF2-ODB)、および X-Station 2 (XS2-ODPB、XS2-OAPB) でのみ使用できます。
A	1:N セキュリティレベル	指紋認証に使用するセキュリティレベルを設定できます。 セキュリティレベルを高く設定すると、本人拒否率(FRR)は高くなりますが、本人拒否率(FAR)は低くなります。
B	スキャンタイムアウト	指紋スキャンのタイムアウト期間を設定できます。 設定した時間内に指紋を読み取らないと、認証に失敗します。
C	センサー感度	指紋認識センサーの感度レベルを設定できます。より高いセンサー感度レベルを使用して、より詳細な指紋情報を取得したい場合は、センサー感度を高く設定します。
D	1:N 認証速度	指紋認証速度を設定できます。自動を選択すると、端末内に登録されている指紋テンプレートの合計量に従って認証速度が構成されます。
E	テンプレート	指紋テンプレートフォーマットを表示できます。
F	認証タイムアウト	認証タイムアウト時間を設定できます。設定時間内に認証が完了しない場合、認証に失敗します。
G	画像表示	認証プロセス中に画面に指紋の画像を表示します。
H	センサーモード	オプションが[自動 ON]に設定されている場合、センサーは指を検出すると自動的にオンになります。オプションが[常に ON]に設定されている場合、センサーは常にオンになります。
I	拡張登録	スキャンされた指紋の品質をチェックして、低品質の指紋テンプレート登録を回避します。

		スキャンされた指紋の品質が低い場合、ユーザーに警告が表示され、登録手順が示されます。
J	生体指紋検知	ライブ指紋検出レベルを設定できます。ライブ指紋検出レベルが高いほど、実際の人間の指紋に対する本人拒否率が高くなります。
K	重複チェック	指紋登録時に重複をチェックできます。

顔

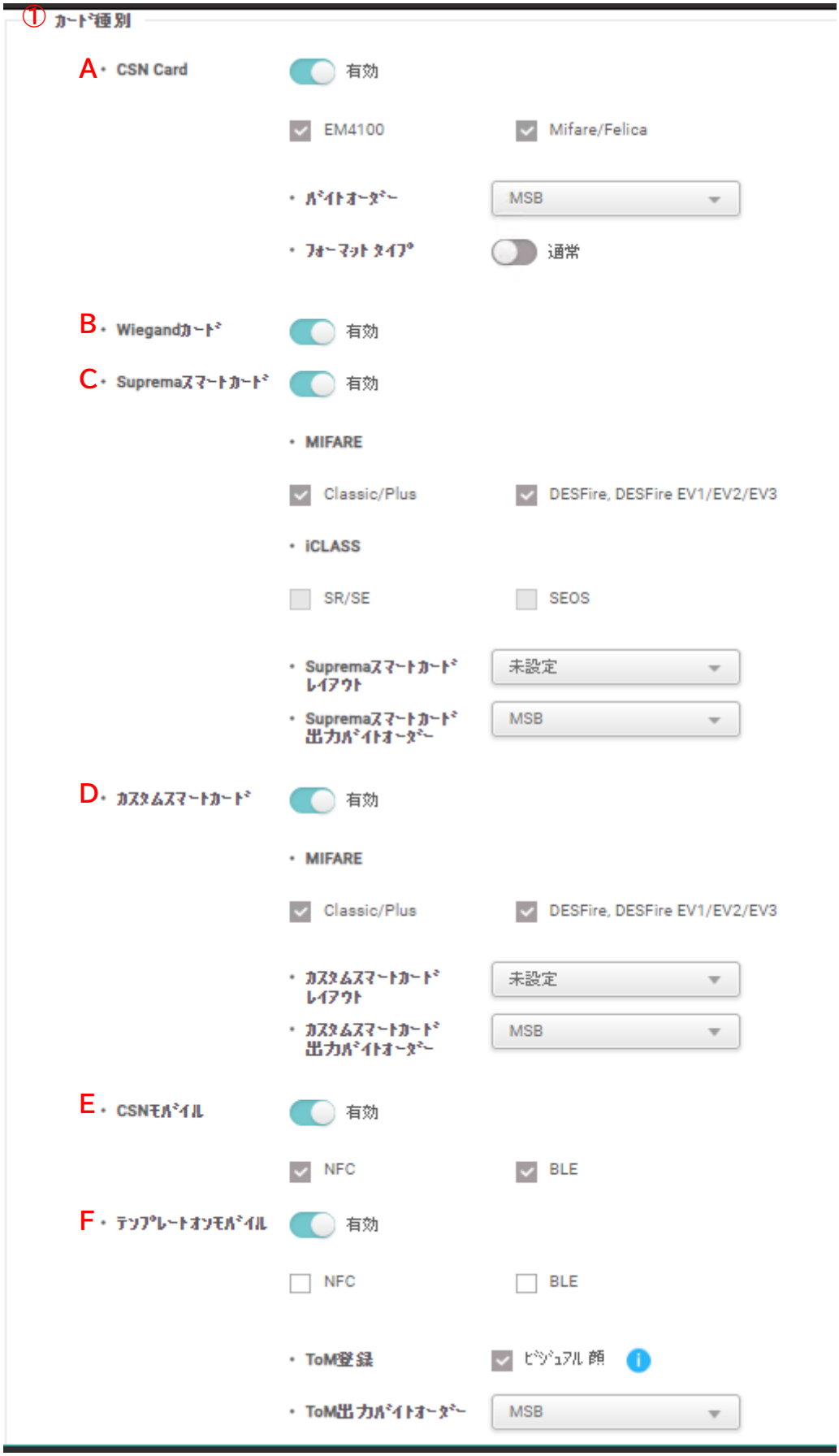
項番	項目名	説明
1	顔	顔認証に関する詳細設定ができます。 **メモ** ・ 編集可能なフィールドは、端末種別によって異なります。 ・ [周囲の照度]、[偽顔登録拒否レベル]、[簡易顔登録]は、FaceStation 2 および FaceLite のみ使用できます。 ・ [LED 照度]は、FaceStation F2 FW 1.1.0 以降でのみ使用できます。 ・ [顔検出設定]と[動作モード]は、FaceStation F2 と BioStation 3 のみ使用できます。
A	1:N セキュリティレベル	顔認証に使用するセキュリティレベルを設定できます。 セキュリティ レベルを高く設定すると、本人拒否率(FRR)は高くなりますが、他人受入率 (FAR)は低くなります。
B	登録タイムアウト	ユーザーの顔を登録する際に、設定した時間内に顔が登録されていない場合、顔の登録はキャンセルされます。 ・

C	モーションセンサー感度	端末近傍の動きを検出する感度を設定します。
D	周囲の照度 または LED 照度	・ 周囲の照度：端末の近くの明るさを感知し、IR LED の強度を調整します。 ・ LED 照度：IR LED の輝度レベルを手動で調整します。「通常」または「高」を選択してレベルを変更するか、「未使用」を選択してライトをオフにします。
E	偽顔登録拒否レベル	偽顔登録拒否するレベルを設定することができます。 偽顔登録拒否レベルが高いほど、実際の顔に対する本人拒否率が高くなります。
F	簡易顔登録	簡易顔登録を利用するかどうかを設定します。このオプションを有効に設定すると、顔の登録手順が 1 ステップに設定されます。オプションを無効に設定すると、3 つのステップに設定されます。高品質の顔テンプレートを登録するには、簡易顔登録は無効にします。
G	顔検出設定	顔認証時にユーザーの顔を認識するための環境を設定します。 ・ 頭の回転角度: 頭部回転の最大角度を設定します。 ・ 検出距離: 最小および最大検出距離を設定します。 ・ ワイドサーチ: ON に設定すると、カメラ画像全体で顔を検出します。
H	動作モード	顔認証時の端末の動作モードを設定します。 ・ フュージョンマッチング： ビジュアルカメラと赤外線カメラの両方を使用して、顔認証の精度を高めます。 ・ 高速マッチング： 照合速度が速くなります。ウォークスルーでの認証を行いたい場合に設定します。
I	偽顔検出レベル	端末は、写真などの偽の顔を使用したユーザー認証を防止します。動作モードがフュージョンマッチングに設定されている場合に使用できます。
J	重複チェック	顔登録時に重複チェックを行うか設定できます。

QR/バーコード

項番	項目名	説明
1	QR/バーコード	QR/バーコード認証に関する詳細設定ができます。 **メモ** ・ [カメラによる QR/バーコードを使用]を使用するには、別途、端末ライセンスが必要です。詳細については、[端末ライセンス]を参照してください。 ・ [カメラによる QR/バーコードを使用]、[スキャンタイムアウト]、[QR をカードとして利用]を設定可能な端末は以下です。 X-Station 2 (XS2-ODPB、XS2-OAPB、XS2-DPB、XS2-APB) FW 1.2.0 以降 BioStation 3 (BS3-DB, BS3-APWB) FW 1.1.0 以降 ・ [スキャナーによる QR/バーコードを使用]、[スキャンタイムアウト]を使用できる端末は以下です。 X-Station 2 (XS2-QDPB、XS2-QAPB)
A	カメラによる QR/バーコードの使用	端末のカメラで QR/バーコード認証を使用するかどうかを設定します。
B	スキャンタイムアウト	[カメラによる QR/バーコードを使用]が有効の場合に、カメラの QR/バーコードスキャンのタイムアウト時間を設定できます。設定した時間内に QR/バーコードを読み取らないと、認証に失敗します。
C、F	QR をカードとして利用	発行された CSN カードまたは Wiegand カードと同じデータの QR コードで認証できます。
D	スキャナーによる QR/バーコードを使用	端末のスキャナーで QR/バーコード認証を使用するかどうかを設定します。
E	スキャンタイムアウト	[スキャナーによる QR/バーコードを使用]が有効の場合に、QR/バーコードスキャンのタイムアウト時間を設定できます。設定した時間内に QR/バーコードを読み取らないと、認証に失敗します。

カード種別



項番	項目名	説明
1	カード種別	端末で使用するカードの種類を設定できます。 **メモ** 端末がサポートしているカードの種類が表示されます。
A	CSN カード	CSN カードとフォーマットタイプを選択し、バイトオーダーを設定できます。 **メモ** ・ [フォーマットタイプ]が通常に設定されている場合、端末はカードのシリアル番号(CSN)を読み取ります。オプションが Wiegand に設定されている場合、端末は、ユーザーが定義した Wiegand 形式でカードのシリアル番号を読み取ります。 ・ [フォーマットタイプ]が Wiegand に設定されている場合、端末で使用する Wiegand 形式を選択できます。新しい Wiegand 形式を設定するには、[Wiegand]を参照してください。 ・ [バイトオーダー]が MSB に設定されている場合、端末はカード ID を最上位バイトから最下位バイトへと読み取ります。たとえば、カード ID 0x12345678 の最上位バイトは 0x12 であり、端末は 0x12、0x34、0x56、0x78 を順番に読み取ります。オプションが LSB に設定されている場合、端末はカード ID を最下位バイトから最上位バイトに読み取ります。
B	Wiegand カード	Wiegand カードの種類を選択し、Wiegand 形式を設定できます。 **メモ** 端末で使用する Wiegand 形式を選択できます。新しい Wiegand 形式を設定するには、[Wiegand]を参照してください。
C	Suprema スマート カード	端末で使用する Suprema スマートカードのレイアウトを選択し、バイトオーダーを設定することができます。新しいスマートカードレイアウトを設定するには、[スマート/モバイル カード]を参照してください。 **メモ** Suprema スマート カードバイトオーダーが MSB に設定されている場合、端末はカード ID を最上位バイトから最下位バイトへと読み取ります。オプションが LSB に設定されている場合、端末はカード ID を最下位バイトから最上位バイトに読み取ります。
D	カスタムスマート カード	サードパーティが発行したカスタムスマートカードのレイアウトを選択し、バイトオーダーを設定することができます。新しいスマートカードレイアウトを設定するには、[スマート/モバイル カード]を参照してください。

		メモ ・ カスタムスマートカードを使用できる端末とファームウェアのバージョンは以下のとおりです。 XPass D2 FW 1.7.1 以降 ・ カスタムスマート カードバイトオーダーが MSB に設定されている場合、端末はカード ID を最上位バイトから最下位バイトへと読み取ります。オプションが LSB に設定されている場合、端末はカード ID を最下位バイトから最上位バイトに読み取ります。
E	CSN モバイル	モバイルカードの認識方法を選択します。
F	テンプレートオンモバイル	テンプレートオンモバイル: モバイルのテンプレートの認識方法を選択し、ユーザーが端末に直接登録する生体認証を指定し、バイトオーダーを設定します。 **メモ** ・ テンプレートオンモバイルを使用できる端末とファームウェアのバージョンは以下のとおりです。 - BioStation 3 FW 1.2.0 以降 ・ ToM Output Byte Order が MSB に設定されている場合、端末はカード ID を最上位バイトから最下位バイトまで読み取ります。このオプションが LSB に設定されている場合、端末はカード ID を最下位バイトから最上位バイトまで読み取ります。

メモ

・ テンプレートの形式を変更すると、以前に保存されたすべての指紋が使用できなくなります。ユーザーの指紋を登録する前に、必ず正しいテンプレート形式を選択してください。

・ [フルアクセス]が有効に設定されている場合、端末をアクセスレベルに追加することはできません。

2 [適用]をクリックして設定を保存します。

➢ 関連情報

サーバー

詳細設定

管理者、表示・音、トリガーおよび動作を設定できます。

1 詳細設定タブをクリックします。

2 [管理者]、[勤怠]、[表示/音声]、[トリガーおよび動作]、[イメージログ]、[Wiegand]、[セキュアタンパー]、[アナログインターフォン]、[カメラ]を参照してフィールドを編集します。

3 [適用]をクリックして設定を保存します。

メモ

編集可能なフィールドは、端末種別によって異なります。

管理者

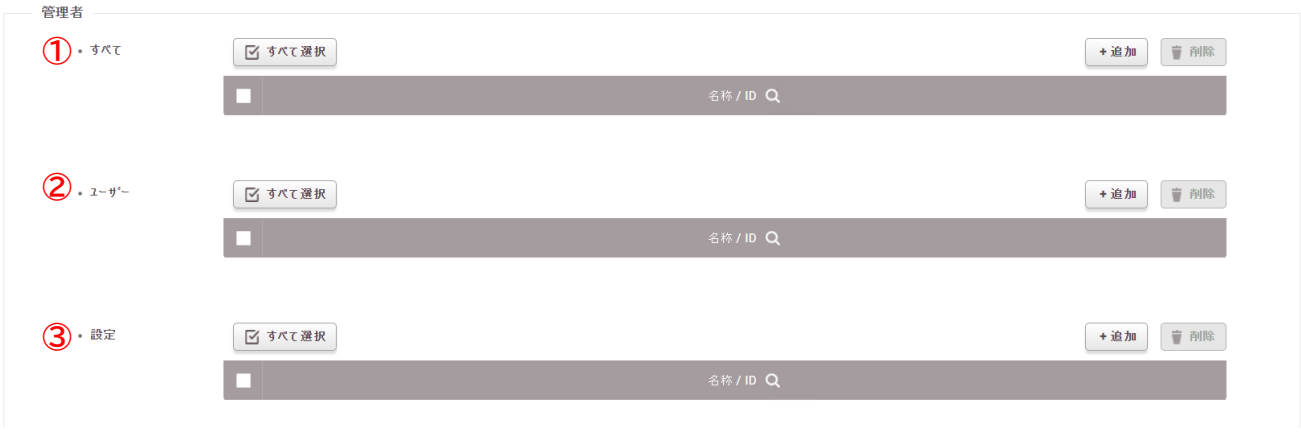
端末の管理者権限を割り当てて管理できます。

メモ

最大 1,000 人の管理者を追加して管理できます。

追加できる管理者の数は、端末のファームウェアバージョンによって異なります。

1 [+追加]をクリックして、ユーザーを選択します



項番	項目名	説明
1	すべて	割り当てられた管理者は、ユーザーの追加や編集など、すべてのメニュー機能を使用できます。
2	ユーザー	割り当てられた管理者は、ユーザー情報を管理できますが、端末の表示/音声、ネットワーク、および RS-485 設定を変更することはできません。
3	構成	割り当てられた管理者は、端末の表示/音声、ネットワーク、および RS-485 設定を変更できますが、ユーザー情報を管理することはできません。

メモ

- ゴミ箱ボタン( )をクリックすると、登録済みのユーザーが削除されます。
- 各端末に構成された管理者設定は、BioStar 2 のログイン権限には影響しません。

勤怠

端末の勤怠イベントの名前を変更し、端末の勤怠モードを設定できます。

1 必要なフィールドを編集します。

項番	項目名	説明
1	勤怠モード	勤怠イベント設定を設定できます。 ・未使用：ユーザーは 勤怠イベントを記録できません。 ・ユーザー選択：ユーザーは、認証前に 勤怠イベントを手動で選択できます。 ・スケジュール：勤怠イベントは、事前定義されたスケジュールに従って自動的に変更されます。勤怠イベントプションでスケジュールを選択できます。 ・最終選択内容：勤怠イベントを手動で変更するまで、最後のユーザーが選択した 勤怠イベントは変更されません。 ・固定：ユーザーは、固定の 勤怠イベントのみを使用できます。勤怠モードを固定に設定し、固定として使用するイベントを選択します。
2	勤怠必須入力	ユーザーは、認証プロセス中に勤怠イベントを選択する必要があります。[勤怠必須入力]オプションを使用するには、[勤怠モード]オプションを[ユーザー選択]に設定する必要があります。
3	勤怠イベント	勤怠イベントの名前を設定し、勤怠モードを[スケジュール]に設定したときに使用されるスケジュールを追加できます。 ・勤怠イベントボタン：勤怠イベントの選択に使用できるキーを一覧表示します。編集するファンクションキーの 1 つを選択します。 ・表示：勤怠イベントボタンの勤怠イベントの名前を変更できます。 ・スケジュール：スケジュールを設定できます。このオプションを有効にするには、勤怠モードを[スケジュール]に設定する必要があります。新しいスケジュールの設定の詳細については、「スケジュール」を参照してください。

メモ

- LCD 画面のない端末の場合、勤怠モードは[固定]または[スケジュール]に設定できます。固定の勤怠イベント、またはスケジュールに合わせて変化する勤怠イベントを登録できます。
- サポートされている端末は、BioEntry P2、BioEntry W2、BioEntry Plus、BioEntry W、Xpass、Xpass S2、XPass D2、および XPass 2 です。

表示/音声

端末の表示と音声の設定を編集できます。イベントごとに LED またはブザーの動作を設定できます。

メモ

編集可能なフィールドは、端末の種類によって異なる場合があります

1 必要なフィールドを編集します。

BioEntry P2、BioEntry W2、BioLite Net、BioEntry Plus、BioEntry W、Xpass、Xpass S2、XPass D2、XPass 2

メモ

言語、メニュータイムアウト、バックライト消灯、メッセージタイムアウトは、BioLite Net でのみ使用できます。

項番	項目名	説明
1	言語	端末の表示言語を設定します。

		[リソースアップデート]をクリックして、言語ファイルを端末に適用します。
2	音量	音声をオンまたはオフにします。
3	メニュータイムアウト	メニュー画面から待受画面に遷移するまでのタイムアウト時間を設定します。
4	バックライト消灯	ディスプレイのバックライトが自動的にオフになるまでのタイムアウト時間を設定します。
5	メッセージタイムアウト	さまざまなメッセージが自動的に消えるまでのタイムアウト時間を設定します。
6	LED/ブザー	イベントを選択し、そのイベントの LED またはブザー動作を設定します。
7	Keypad Backlight	キーパッドのバックライトをオンまたはオフに切替ます。 キーパッドのバックライトを有効にすると、キーパッドの背面が点灯し、暗い環境でもキーを識別しやすくなります。

BioStation 2、BioStation L2、BioLite N2、FaceLite

項番	項目名	説明
1	言語	端末の表示言語を設定します。 [リソースアップデート]をクリックして、言語ファイルを端末に適用します。
2	音量	音量を調整します。
3	メニュータイムアウト	メニュー画面のタイムアウトを設定します。
4	ホーム画面	端末のホーム画面のスタイルを変更します。
5	バックライト消灯	バックライトのタイムアウトを設定します。
6	メッセージタイムアウト	さまざまなメッセージが自動的に消えるまでのタイムアウト時間を設定します。
7	音声ガイダンス	音声ガイダンスを有効にします。
8	背景	端末のホーム画面に表示する項目を設定します。

		・ ロゴ：ユーザーがアップロードした画像をホーム画面に表示します。[追加]をクリックして、画像をアップロードできます。 ・ お知らせ：管理者が入力したメッセージを表示します。 ・ スライドショー：最大 10 枚の画像のスライド ショーを表示します。[追加]をクリックして、画像をアップロードできます。 **メモ** ・ [更新]をクリックして、設定を端末に即座に適用します。 ・ [背景]を変更すると、[更新]をクリックしても適用されません。[適用]をクリックした時に設定が適用されます。 ・ BioStation 2 は、[お知らせ]と[スライドショー]に対応します。
9	効果音	起動時、認証成功時、認証失敗時の効果音を設定します。 [検索]をクリックし、*.wav ファイル（500KB 未満）を選択します。 **メモ** [更新]をクリックすると、設定がリアルタイムで端末に適用されます。

BioStation 3、BioStation A2、FaceStation 2、FaceStation F2、X-Station 2

項番	項目名	説明
1	言語	端末の表示言語を設定します。 [リソースアップデート]をクリックして、言語ファイルを端末に転送します。
2	音量	端末のデフォルトの音量を制御します。
3	インターホンスピーカー音量	インターホン機能使用時のスピーカー音量を設定します。

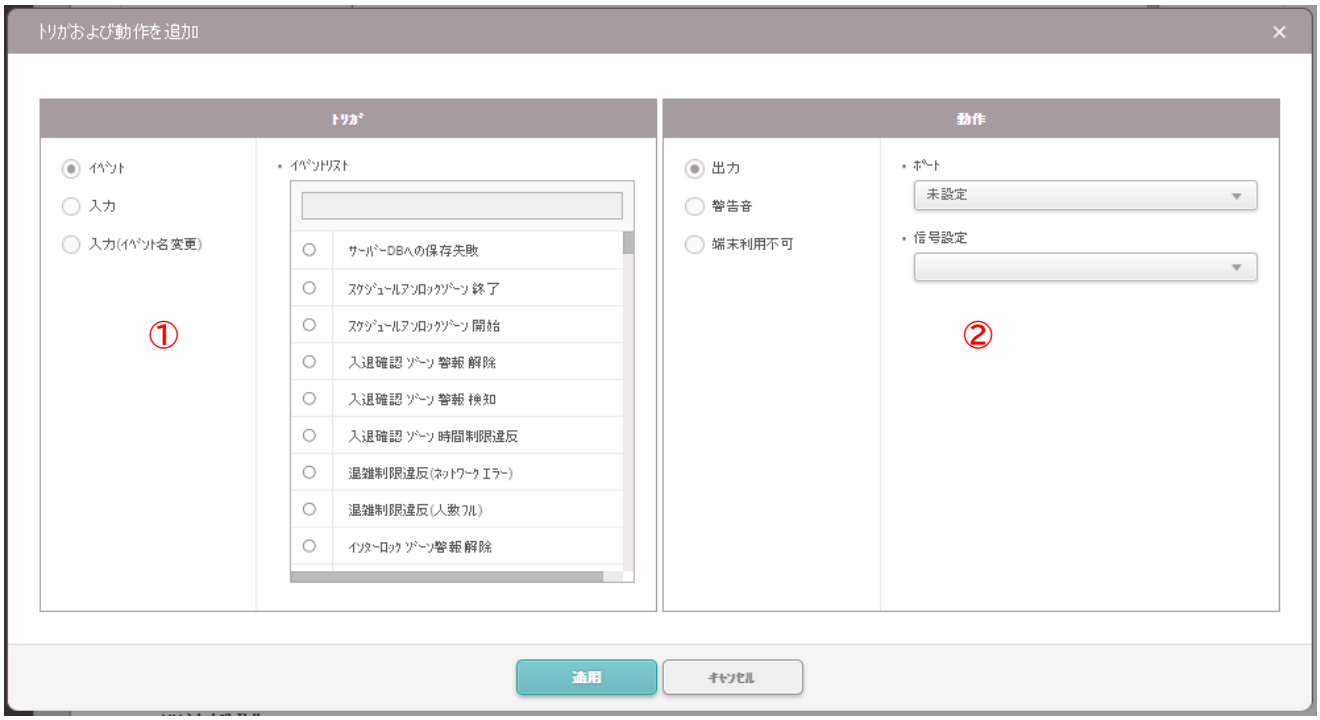
4	インターホンマイクロフォン音量	インターホン機能使用時のマイク音量を設定します。
5	メニュータイムアウト	メニュー画面のタイムアウトを設定します。
6	バックライトタイムアウト	バックライトのタイムアウトを設定します。
7	メッセージタイムアウト	各種メッセージが自動的に消えるまでのタイムアウト時間を設定します。
8	スクリーンセーバー	スクリーンセーバー機能を使用するには、このオプションを設定します。端末が使用されていない時に LCD 画面の輝度を下げることで、無駄なエネルギー消費を抑えます。 **メモ** スクリーンセーバーは、FaceStation 2、FaceStation F2、X-Station 2、BioStation 3 でサポートされています。
9	音声ガイダンス	音声ガイダンスを有効にします。
10	ホーム画面	端末のホーム画面に表示する項目を設定します。 ・通常: ホーム画面にデフォルトの画像を表示します。 ・ロゴ: ユーザーがアップロードした画像をホーム画面に表示します。[追加]をクリックして、画像をアップロードできます。 ・お知らせ: 管理者が入力したメッセージを表示します。 **メモ** ・ [更新]をクリックすると、設定を端末に即座に適用します。 ・ [背景]を変更すると、[更新]をクリックしても適用されません。[適用]をクリックして構成を保存します。 ・ ホーム画面にロゴを設定し、スライドショーを有効に設定すると、ホーム画面に最大 10 枚の画像のスライドショーを表示できます。[追加]をクリックして、画像をアップロードできます。 ・ スクリーンセーバーは、FaceStation 2、FaceStation F2、X-Station 2、および BioStation 3 でサポートされています。
11	効果音	起動時、認証成功時、および認証失敗時の効果音を設定します。 [検索]をクリックし、*.wav ファイル（500KB 未満）を選択します。 **メモ** ・ [更新]をクリックして、設定をリアルタイムで端末に適用します。

トリガーおよび動作

状況ごとにトリガーおよび動作を設定できます。たとえば、認証に失敗したときにアラームを鳴らしたり、RS-485 の接続が切断したときに端末を端末の利用を無効にしたりできます。

イベントを選択することも、目的のトリガーおよび動作を設定することもできます。

[+追加]をクリックして、設定を行ないます。



項番	項目名	説明
1	トリガ	定義済みのイベントを選択するか、ユーザー定義のトリガーを追加できます。 ・ イベント：事前定義されたイベントを選択できます。 ・ 入力：ポート、スイッチ、期間（ミリ秒）、およびスケジュールを選択して、ユーザー定義のトリガーを設定できます。 ・ 入力(イベント名変更)：ポート、スイッチ、期間（ミリ秒）、スケジュール、およびイベント名を選択して、ユーザー定義のトリガーを設定できます。 **メモ** ・ トリガーをイベントとして設定すると、イベント リストから 1 つのイベントのみを選択できます。 ・ [入力(イベント名変更)]を選択してユーザー定義条件を設定する場合、目的のスケジュールが使用できない場合は、[+スケジュールの追加]をクリックして作成します。スケジュールの設定の詳細については、「スケジュール」を参照してください。 ・ [入力(イベント名変更)]を選択してユーザー定義条件を設定する場合、目的のイベント名が使用できない場合は、[イベント名 追加]をクリックして作成します。イベントが発生すると、イベント名がイベントログとリアルタイムログに表示されます。 ・ イベント名は 64 文字まで入力できます。
2	動作	定義済みのアクションを選択するか、ユーザー定義のアクションを追加できます。 **メモ** ・ [出力]を選択してユーザー定義アクションを設定する時に、目的のシグナルが使用できない場合は、[+シグナルの追加]をクリックして作成します。

		・ トリガーを[入力(イベント名変更)]として設定すると、動作を[未設定]に設定できます。

イメージログ

端末で使用するイメージログイベントとスケジュールを設定できます。

> **メモ**
>
> BioStation A2、FaceStation 2、FaceStation F2、X-Station 2、BioStation 3 のみ対応

1 イメージログを有効に設定します。

[詳細設定] > [イメージログ]からイメージログを残すイベントやスケジュールを設定することが可能です。

詳細については、イメージログを参照してください。

2 [+追加]をクリックして、目的のイベントとスケジュールを設定します。

Wiegand

Wiegand 入力/出力を定義できます。

1 必要なフィールドを編集します。

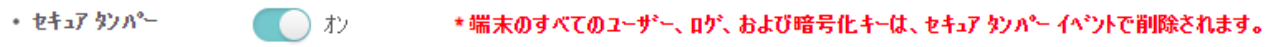
項番	項目名	説明

1	入力/出力	入出力モードを選択できます。
2	Wiegand 入力フォーマット	Wiegand のフォーマットを設定できます。Wiegand 形式の設定の詳細については、カード形式を参照してください。
3	出力モード	Wiegand 信号の出力モードを設定できます。 通常に設定されている場合、カードは設定された Wiegand 形式でスキャンされます。 バイパスに設定すると、Wiegand 認証に関係なく CSN が送信されます。 ドア制御機能のない端末を使用する場合は、バイパスを設定する必要があります。 通常に設定すると、フェールコードや、Wiegand カードの認証失敗時に送信する値の選択が可能です。
4	パルス幅	Wiegand 信号のパルス幅を設定できます。
5	パルス間隔	Wiegand 信号のパルス間隔を設定できます。
6	出力情報	ユーザー認証時に端末に出力する情報を選択できます。

セキュアタンパー

端末でタンパーイベントが発生した場合、端末に保存されているユーザー情報全体、ログ全体、およびセキュリティキーを削除するように設定できます。

1 セキュアタンパーを使用するには、[オン]に設定します。



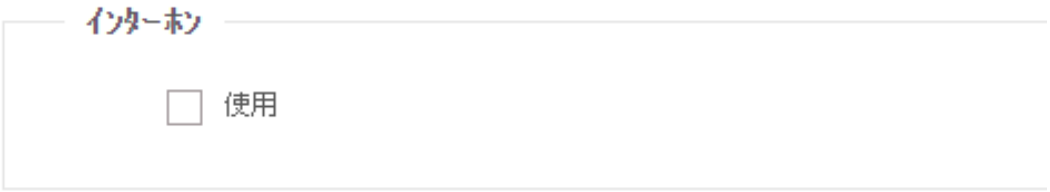
アナログインターホン

アナログインターホンを使用する場合は設定できます。

メモ

- BioStation 2 専用です。

1 [使用]をクリックして、接続されたインターホンを使用します。



カメラ

カメラの電源周波数を設定することができます。

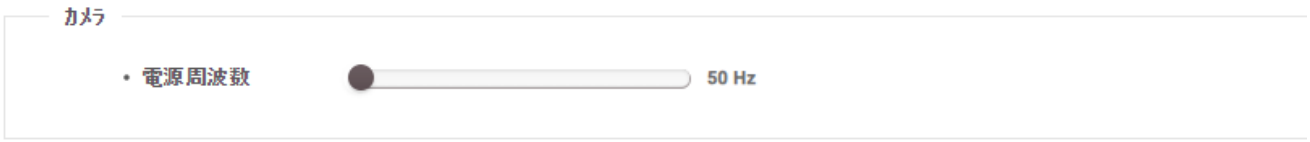
蛍光灯を使用する環境で周波数の設定を誤ると、映像にちらつきが発生する場合があります。

地理的な場所に応じて、異なるカメラの電源周波数が使用されます。

メモ

- BioStation A2 専用です。

1 周波数を選択します



サーマル&マスク

サーマルカメラやマスク検出の詳細設定ができます。

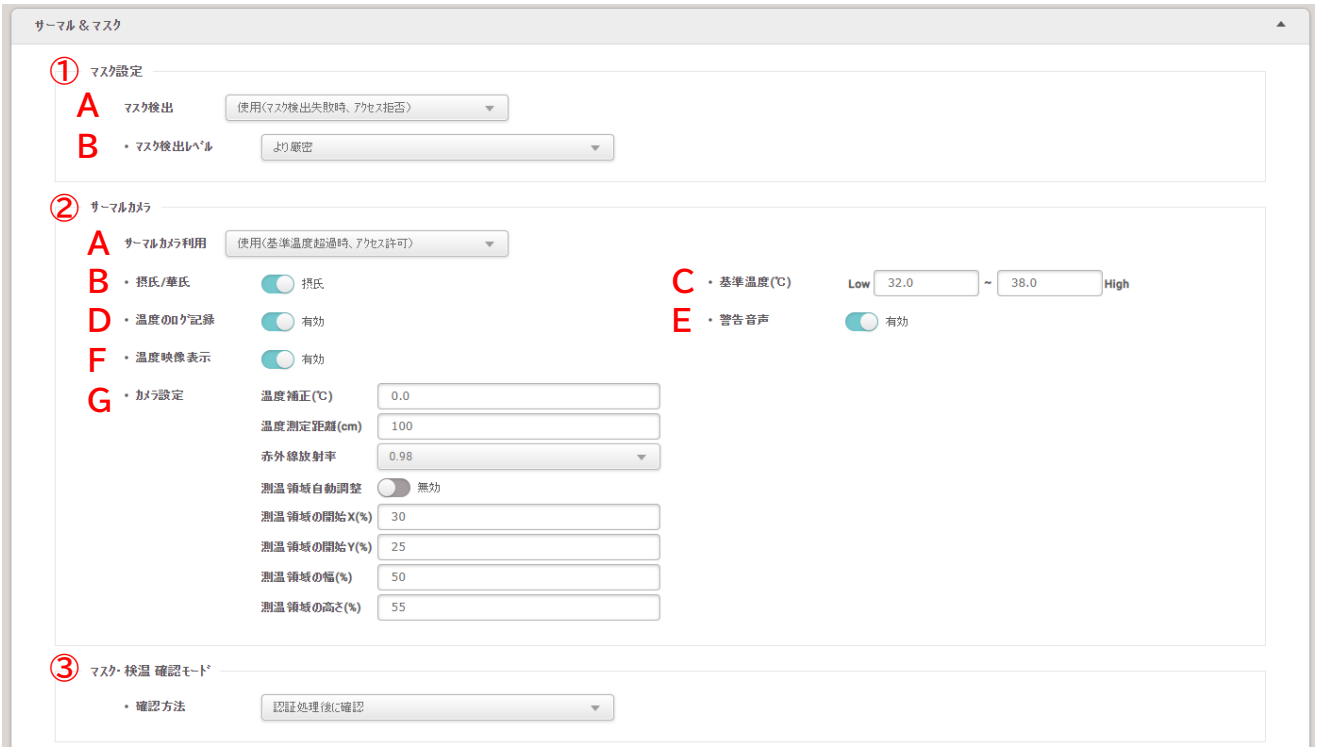
Suprema 顔認証端末に対応するサーマルカメラは、認証するユーザーの温度を測定し、事前設定された閾値よりも高い温度のユーザーのアクセスを制限します。

また、顔認証端末はマスクを検出し、マスクを着用していないユーザーへのアクセスを制限することができます。

メモ

- FaceStation 2 と FaceStation F2 のみがサーマルカメラに対応しています。
- 対応しているサーマルカメラは次のとおりです。
  TCM10-FS2
  TCM10-FSF2
- FaceStation F2 と BioStation 3 のみがマスク検出に対応します。

1 必要な項目を編集します。



項番	項目名	説明
1	マスク設定	マスク検出を使用するかどうかを設定できます。
1-A	マスク検出	マスク検出を使用するかどうかを設定できます。 [使用(マスク検出失敗時、アクセス拒否)]を選択すると、マスクを着用していないユーザーの認証を拒否し、イベントログを保存します。 [使用(マスク検出失敗時、アクセス許可)]を選択すると、マスクを着用していないユーザーは認証できますが、イベントログは保存されます。

1-B	マスク検出レベル	マスク検出の感度を設定できます。
2	サーマルカメラ	サーマルカメラを使用するかどうかのオプションを設定し、詳細設定を編集できます。
2-A	サーマルカメラ利用	サーマルカメラを使用するかどうかを設定できます。 [使用(マスク検出失敗時、アクセス拒否)]を選択すると、温度が設定された閾値を超えたユーザーの認証を拒否し、イベントログを保存します。 [使用(マスク検出失敗時、アクセス許可)]を選択すると、温度が事前設定された閾値よりも高いユーザーは認証できますが、イベントログは保存されます。
2-B	摂氏/華氏	温度の単位を変更します。
2-C	基準温度(℃)	最低温度と最高温度の値を設定して、アクセスを制限できます。皮膚の表面温度が閾値の温度より低いまたは高いユーザーのアクセスは、サーマルカメラの使用設定に応じて制限されます。1 °C ～ 45 °C の範囲で設定でき、Low 値を High 値より高く設定することはできません。
2-D	温度のログ記録	温度データを保存します。このモードが有効の場合、認証ログと温度ログの両方が保存されます。このモードが無効の場合、認証ログのみが保存されます。
2-E	警告音声	温度が事前設定されたしきい値よりも高い場合にトリガーするように警告を設定します。
2-F	温度映像表示:	端末の画面に赤外線画像を表示します。
2-G	カメラ設定	正確な測定のために、赤外線カメラの設定を設定します。 ・ 温度補正(℃): 端末の使用環境に応じて、温度を特定の値まで測定するように校正することができます。たとえば、温度値が常に 0.1℃高い環境では、温度補正値を-0.1℃に設定します。 ・ 温度測定距離(cm) : ユーザーと端末間の距離を設定します。 ・ 赤外線放射率: 放射率を設定して、ユーザーの温度を正確に測定します。 ・ 測温領域自動調整: 端末の視野にライトがある場合、そのライトではなくユーザーの体温を自動的に測定するように赤外線カメラを設定できます。 測温領域の開始X(%)、測温領域の開始Y(%)、測温領域の幅(%)、測温領域の高さ(%): [測温領域自動調整]を無効に設定すると、ROI(測温領域)を手動で設定できます。ROI のサイズと位置を調整して、温度測定領域を設定します。 **メモ** ・ 基準温度の Low 値と High 値は以下のファームウェアバージョンから設定できます。 FaceStation 2 FW 1.4.2 以降 FaceStation F2 FW 1.0.2 以降

<table>
<tr><td></td><td></td><td>最高のパフォーマンスを得るために、[カメラ設定]はデフォルト値から変更しないことを推奨します。端末ごとの各オプションのデフォルト値は次のとおりです。
<table>
<tr><td>項目</td><td>FaceStation 2</td><td>FaceStation F2</td></tr>
<tr><td>距離(cm)</td><td>100</td><td>100</td></tr>
<tr><td>放射率</td><td>0.98</td><td>0.98</td></tr>
<tr><td>ROI X(%)</td><td>47</td><td>30</td></tr>
<tr><td>ROI Y(%)</td><td>45</td><td>25</td></tr>
<tr><td>ROI の幅(%)</td><td>15</td><td>50</td></tr>
<tr><td>ROI の高さ(%)</td><td>10</td><td>55</td></tr>
</table></td></tr>
<tr><td>3</td><td>マスク&検温
確認モード</td><td>[マスク&検温確認モード]は用途に合わせて設定してください。
・認証処理後に確認：認証成功後、温度測定やマスク検出を行います。
・確認後に認証処理：マスク着用や検温の有無を確認した上で認証を行います。このモードを使用すると、ユーザーがマスクを着用していない場合、または体温がしきい値を超えていることが検出された場合、ユーザーの認証処理を行いません。
・認証なし確認：端末は、マスクが着用されているかどうかを判断するため、または体温を測定するためにのみ使用できます。このモードでは、認証に関係なく、マスクを着用しているユーザーまたは基準温度を下回っているすべてのユーザーがアクセスできます。</td></tr>
</table>

2 [適用]をクリックして設定を保存します。

SIP インターホン

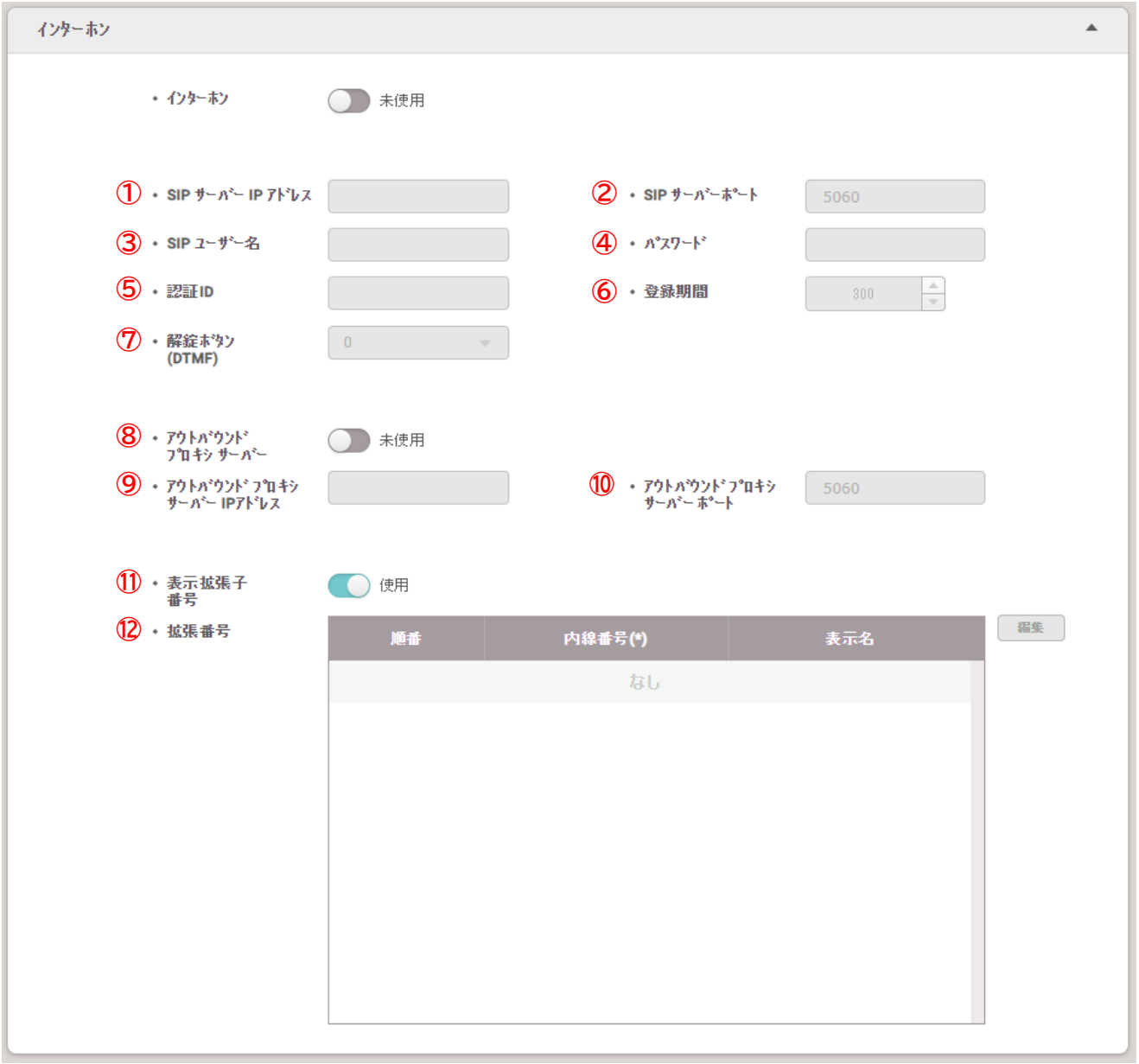
SIP インターホンの詳細設定ができます。

メモ

- SIP インターホンは、BioStation 3、FaceStation 2、BioStation A2 のみサポートされています。
- 編集可能なフィールドは、端末種別によって異なります。

1 インターホンを使用に設定します。

2 SIP 構成を入力して端末を SIP サーバーに登録します。



項番	項目名	説明
1	SIP サーバーアドレス	SIP サーバーのアドレスを入力します。

2	SIP サーバーポート	SIP サーバーのポートを入力します。
3	SIP ユーザー名	SIP アカウントのユーザー名を入力します。 **メモ** SIP ユーザー名には、英数字（大文字と小文字が区別される）および特殊文字(+, -, @, .)のみを入力できます。
4	パスワード	SIP アカウントのパスワードを入力します。
5	認証 ID	SIP アカウントの認証 ID を入力します。 **メモ** 認可 ID には、英数字（大文字と小文字が区別される）および特殊文字(+, -, @, .)のみを入力できます。
6	登録期間(秒)	登録期間を秒単位で入力します。 端末(SIP エンドポイント)は、設定された登録期間ごとに SIP サーバーへの登録を試みます。 **メモ** 登録期間は 60 ～ 600 秒の間で設定できます。
7	解錠ボタン(DTMF)	遠隔でドアを解錠するボタンを設定します。
8	送信プロキシサーバー	SIP サービスに別の（アウトバウンド）プロキシサーバーがある場合は、[使用]に設定します。
9	送信プロキシサーバードレス	送信プロキシサーバーのアドレスを入力します。
10	送信プロキシサーバーポート	送信プロキシサーバーのポートを入力します。
11	表示拡張子番号	画面に内線番号が表示されるのが気になる場合は、これを[未使用]に設定します。 **メモ** 表示名が設定されていないと、受信者を区別できません。
12	拡張番号	内線番号は 128 まで登録できます。「編集」をクリックして追加・編集してください。  ・ トップに戻る: 選択した内線番号がリストの一番上に移動します。

		・ CSV インポート: CSV ファイルから内線番号をインポートします。 ・ CSV エクスポート: 内線番号を CSV ファイルにエクスポートします。 ・ 追加: 内線番号を追加します。 ・ 削除: 内線番号を削除します。 ・ 順番変更: ドラッグアンドドロップで内線番号を並べ替えます。 **メモ** ・ FaceStation 2 および BioStation A2 の内線番号の数は最大 16 です。 ・ CSV ファイルには、サポートされている内線番号の最大数を超える数を含めることはできません。 ・ 内線番号には、英数字（大文字と小文字が区別される）および特殊文字(+, -, @, .)のみを入力できます。

3 [適用]をクリックして設定を保存します。

RTSP

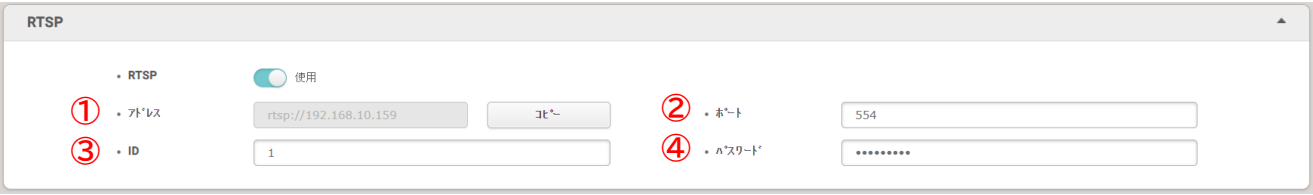
RTSP を使用するかどうかを設定できます。

メモ

- RTSP は BioStation 3 でのみサポートされています。

1 RTSP を[使用]に設定します。

2 必要なフィールドに入力します。



項番	項目名	説明
1	アドレス	RTSP アドレスは固定です。 ・ コピー: RTSP アドレスを簡単にコピーします。
2	ポート	RTSP ポートを設定します。
3	ID	RTSP クレデンシャルの ID を設定します。
4	パスワード	RTSP クレデンシャルのパスワードを設定します。

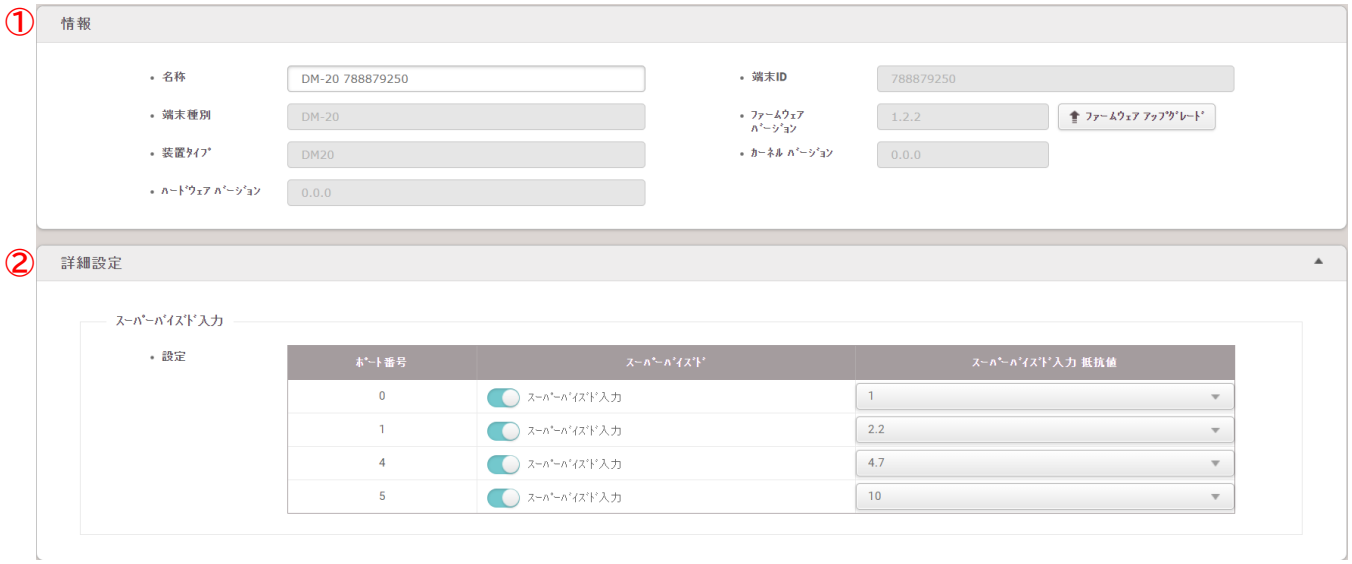
3 [適用]をクリックして設定を保存します。

DM-20

登録した DM-20 の詳細設定を編集できます。

1 [端末]をクリックします。

2 編集する端末一覧で DM-20 をクリックします。



項番	項目名	説明
1	情報	端末の設定を変更できます。 ・名称: 端末名を入力します。 ・端末 ID: 端末 ID を表示します。 ・端末種別: 端末の種類を表示します。 ・ファームウェアバージョン: [ファームウェアアップグレード]をクリックして、新しいファームウェアバージョンをインストールします。 ・装置タイプ:モデル名を表示します。
2	詳細設定	監視入力の設定を変更できます。DM-20 は監視入力ポートに接続された端末のオン、オフ、オープン、およびショート状態を監視でき、終端抵抗を 1 kΩ、2.2 kΩ、4.7 kΩ、10 kΩに設定できます。

3 [適用]をクリックして設定を保存します。

OM-120

登録した OM-120 の詳細設定を編集できます。

1 [端末]をクリックします。

2 編集する端末一覧で OM-120 をクリックします。

項目	説明
情報	端末の設定を変更できます。 ・名前:端末名を入力します。 ・端末 ID: 端末 ID を表示します。 ・端末種別: 端末の種類を表示します。 ・ファームウェアバージョン: [ファームウェア アップグレード]をクリックして、新しいファームウェアバージョンをインストールします。 ・装置タイプ:モデル名を表示します。 ・カーネルバージョン: カーネルバージョンを表示します。 ・ハードウェアバージョン: ハードウェアバージョンを表示します。

3 [適用]をクリックして設定を保存します。

IM-120

IM-120 は、検出された入力をリアルタイムで BioStar 2 に接続することにより、即時のリレー動作を提供します。

マスター端末との接続が切断された状態で、リレーを動作させたり、検出された入力のログを保存します。

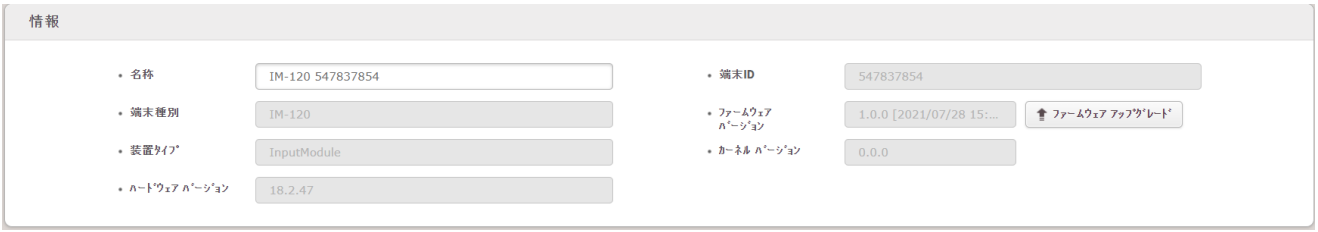
登録した OM-120 の詳細設定を編集できます。

1 [端末]をクリックします。

2 編集する端末一覧で IM-120 をクリックします。

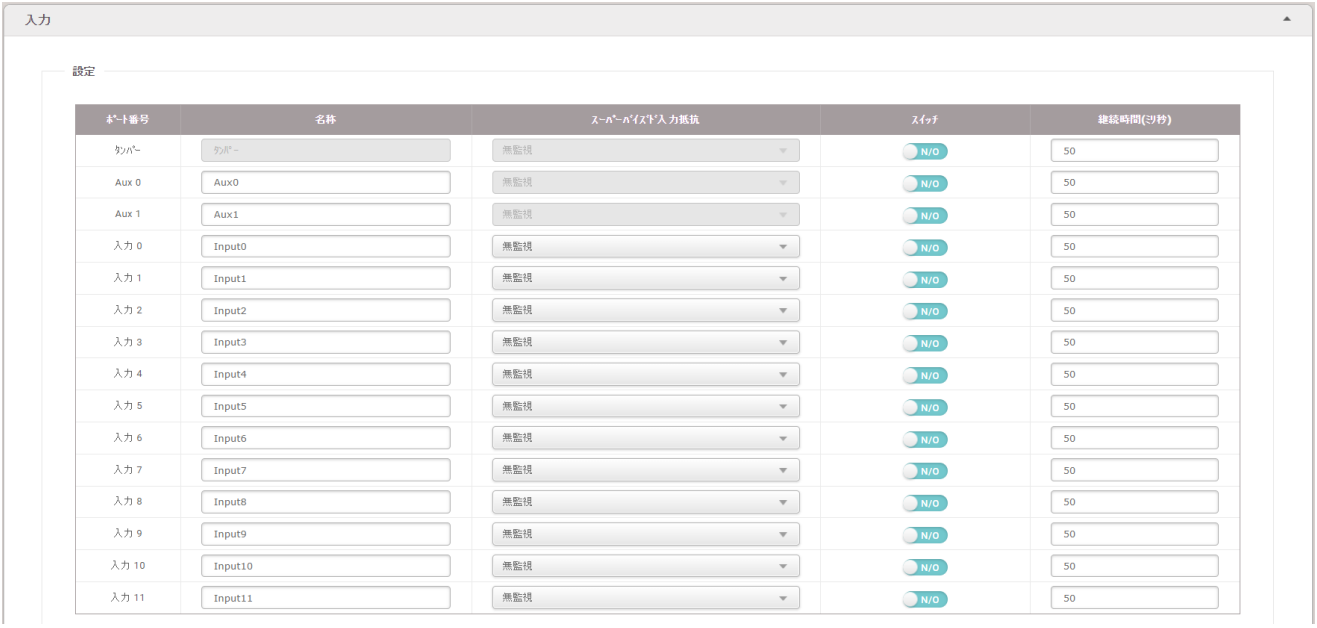
3 必要な項目を編集します。

情報



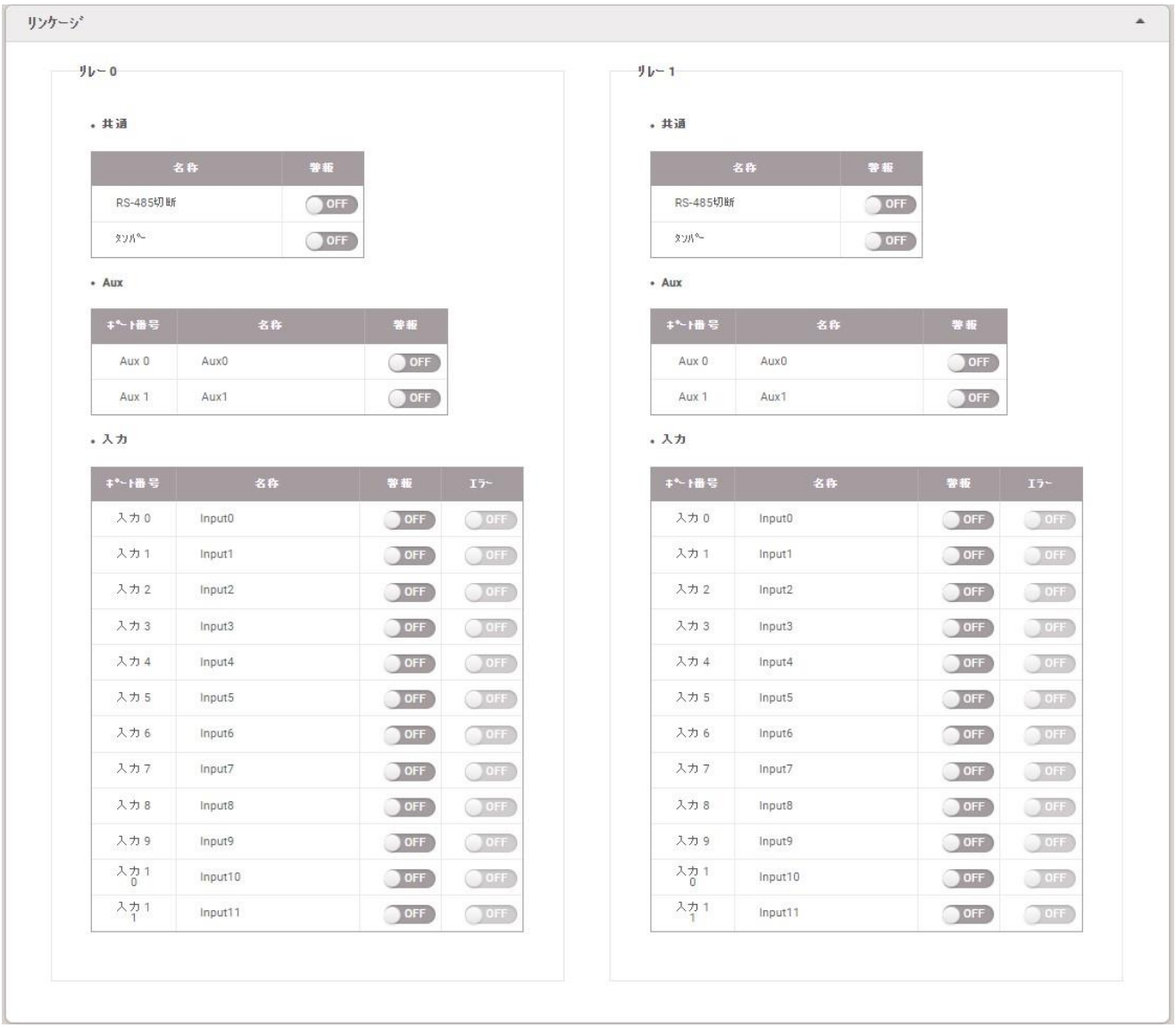
項目	説明
情報	端末の設定を変更できます。 ・名称: 端末名を入力します。 ・端末 ID: 端末 ID を表示します。 ・端末種別: デバイスの種類を表示します。 ・ファームウェアバージョン: [ファームウェア アップグレード]をクリックして、新しいファームウェアバージョンをインストールします。 ・装置タイプ: モデル名を表示します。 ・カーネルバージョン: カーネルバージョンを表示します。 ・ハードウェアバージョン: ハードウェアバージョンを表示します。

入力



項目	説明
入力	各入力ポートの名前を入力し、抵抗値、スイッチ、持続時間を設定できます。 ・ポート番号 ：IM-120 が対応している入力 12 点、AUX 入力 2 点、タンパーを検索欄に表示します。 ・名称: 各入力の名前を入力します。 ・Supervised Input ポートを使用してオン、オフ、オープン、ショートの 4 つの状態を検出できます。 ・BioStar 2 の「Trigger and Action」機能を使えば、DM-20 が開放・短絡状態を検知した時の動作をプリセットできます。 ・Supervised Input は、回路上の電圧値を検出し、4 つの状態(オープン、ショート、ON、 OFF)に基づいて入力監視します。その場合、抵抗を接続する必要があります。。スーパーバイズド入力抵抗が無監視に設定されている場合、監視入力ポートは TTL 入力として使用されます。抵抗値は 1 kΩ 、2.2 kΩ 、4.7 kΩ 、10 kΩが設定できます。 **メモ** 入力機器に接続する抵抗と同じ抵抗値に設定してください。 ・ スイッチ: スイッチは N/C または N/O に設定できます。 ・ 継続時間(ミリ秒)： 入力信号が発生したときに有効と見なされる最小時間を設定できます。継続時間は、50 から 65535 までの数字のみを入力できます。

リンケージ



項目	説明
リンケージ	入力ごとにリレーの動作を設定できます。リレー 0 とリレー 1 の動作をそれぞれ設定できます。 ・共通 RS-485 切断: マスター端末との接続が失われたときにアラームをトリガーするかどうかを設定できます。 タンパー: タンパーが発生したときに警報をトリガーするかどうかを設定できます。 ・AUX: AUX 信号が発生したときに警報をトリガーするかどうかを設定できます。AUX ポートは、電源障害検出器または別のデバイスからのドライ接点出力を接続するために使用できます。 ・入力: 入力信号が発生したときに、警報またはエラー動作を設定できます。エラー動作(カットおよびショート)は、スーパーバイズド入力抵抗で抵抗値を選択することによって監視入力が有効になっている場合にのみ有効になります。

4 [適用]をクリックして設定を保存します。

CoreStation

登録した CoreStation の詳細設定を編集できます。

1 [端末]をクリックします。

2 端末一覧で CoreStation をクリックして編集します。

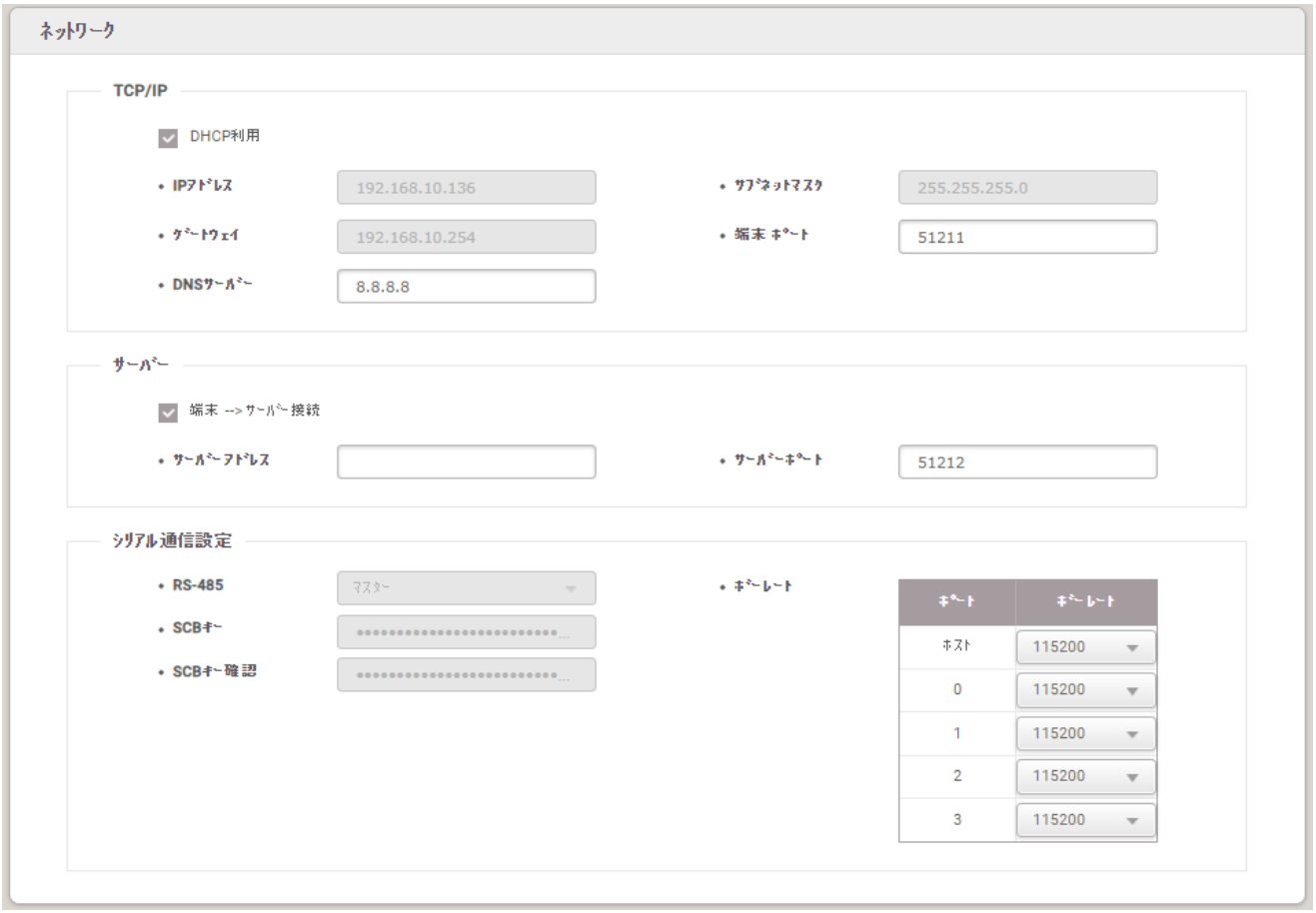
3 必要な項目を編集します。

情報

項目	説明
情報	・名称: 端末名を入力します。 ・端末 ID: 端末 ID を表示します。 ・ファームウェアバージョン: [ファームウェア アップグレード]をクリックして、新しいファームウェアバージョンをインストールします。 ・カーネルバージョン: カーネルバージョンを表示します。 ・工場出荷時設定: 端末の設定をリセットします。すべての設定をリセットするには、[すべて]をクリックします。[ネットワーク設定以外]をクリックして、ネットワーク設定を除くすべての設定をリセットします。 ・タイムゾーン: 端末のタイムゾーンを設定します。BioStar 2 サーバーのタイムゾーンとは異なる端末の標準タイムゾーンを設定できます。 ・サマータイム: サマータイムを端末に適用します。新しいサマータイムルールを追加するには、サマータイム を参照してください。 ・グループ: 端末グループを変更します。端末グループの追加の詳細については、端末グループの追加と管理を参照してください。 ・端末種別: 端末の種類を表示します。 ・装置タイプ: モデル名を表示します。 ・ハードウェアバージョン: ハードウェアバージョンを表示します。 ・ロック中: トリガーおよび動作でデバイスが無効になっている場合、ロック解除ボタンを使用できます。 ・サーバーと時刻同期: 端末時刻情報をサーバーと同期するオプションを選択します。

システム	・表示日時: 日付と時刻を手動で設定します。[サーバーとの時刻同期]オプションが選択されている場合、日付と時刻を手動で選択することはできません。 ・端末時刻取得: ボタンをクリックして、端末に設定されている時刻を取得します。 ・時刻設定: ボタンをクリックして、BioStar 2 で設定された時間を端末に適用します。

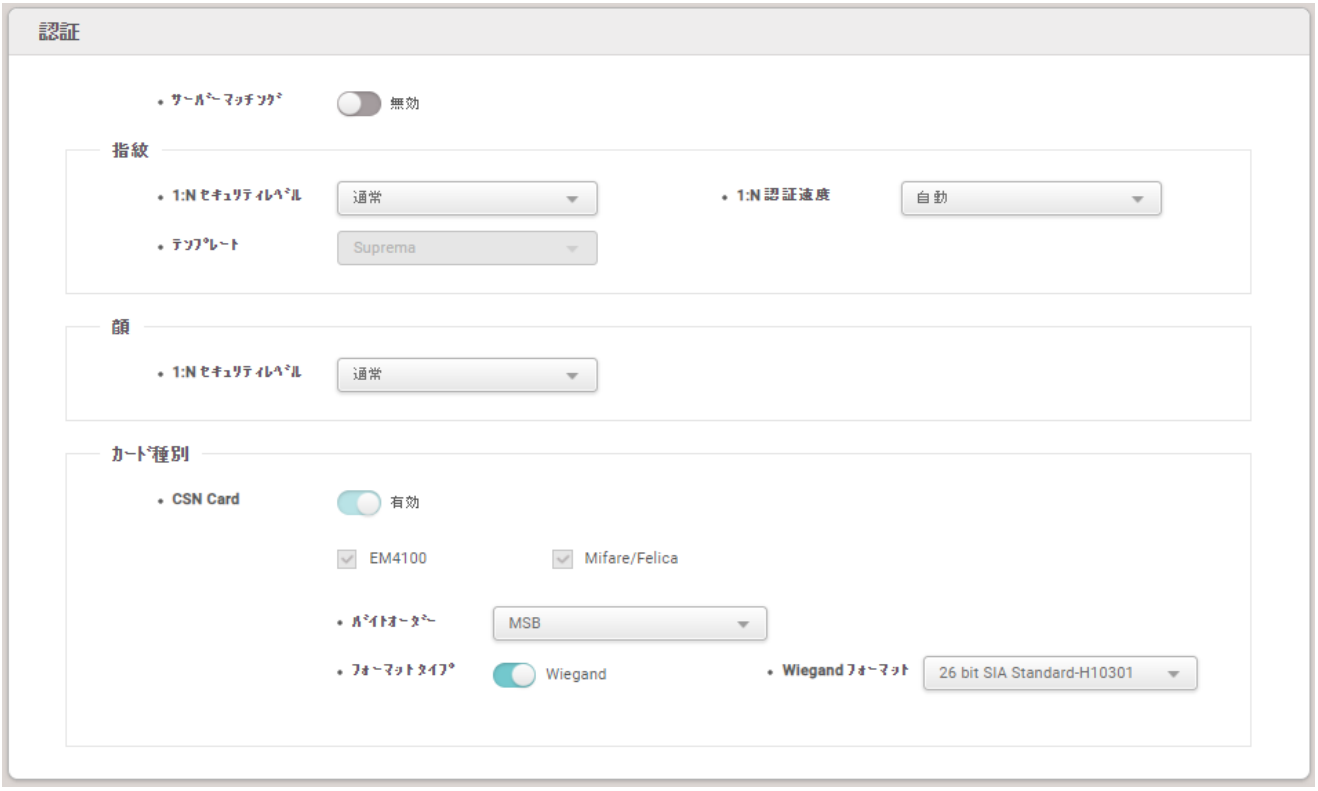
ネットワーク



項目	説明
TCP/IP	・DHCP 利用: このオプションを選択して、端末が動的 IP アドレスを使用できるようにします。このオプションを選択すると、ネットワーク設定を入力できません。 ・IP アドレス,サブネットマスク,ゲートウェイ: 端末に固定 IP を割り当てるには、各ネットワークの情報を入力します。[DHCP 利用] をオフにして、情報を入力します。 ・端末ポート: 端末が使用するポートを入力します。 このポートは、BioStar 2 と端末間の通信に使用されます。 ・DNS サーバーアドレス: DNS サーバーアドレスを入力します。
サーバー	・端末 --> サーバー接続: 端末からサーバーに接続するための BioStar 2 サーバーのネットワーク設定を入力します。 ・サーバーアドレス: BioStar 2 サーバーの IP アドレスまたはドメイン名を入力します。 ・サーバーポート: BioStar 2 サーバーのポート番号を入力します。

シリアル通信設定	・RS-485 :マスターのみ使用できます。 ・ボーレート: RS-485 接続のボーレートを設定します。 ・SCB キー: 端末の SCB キーを設定します。 この機能は、CoreStation に RS-485 端末が接続されていない場合にのみ有効になります。 ・SCB キー確認: 設定した SCB キーと一致することを確認します。この機能は、CoreStation に RS-485 端末が接続されていない場合にのみ有効になります。 **メモ** ・ SCB キーは 16 バイトまで入力できます。

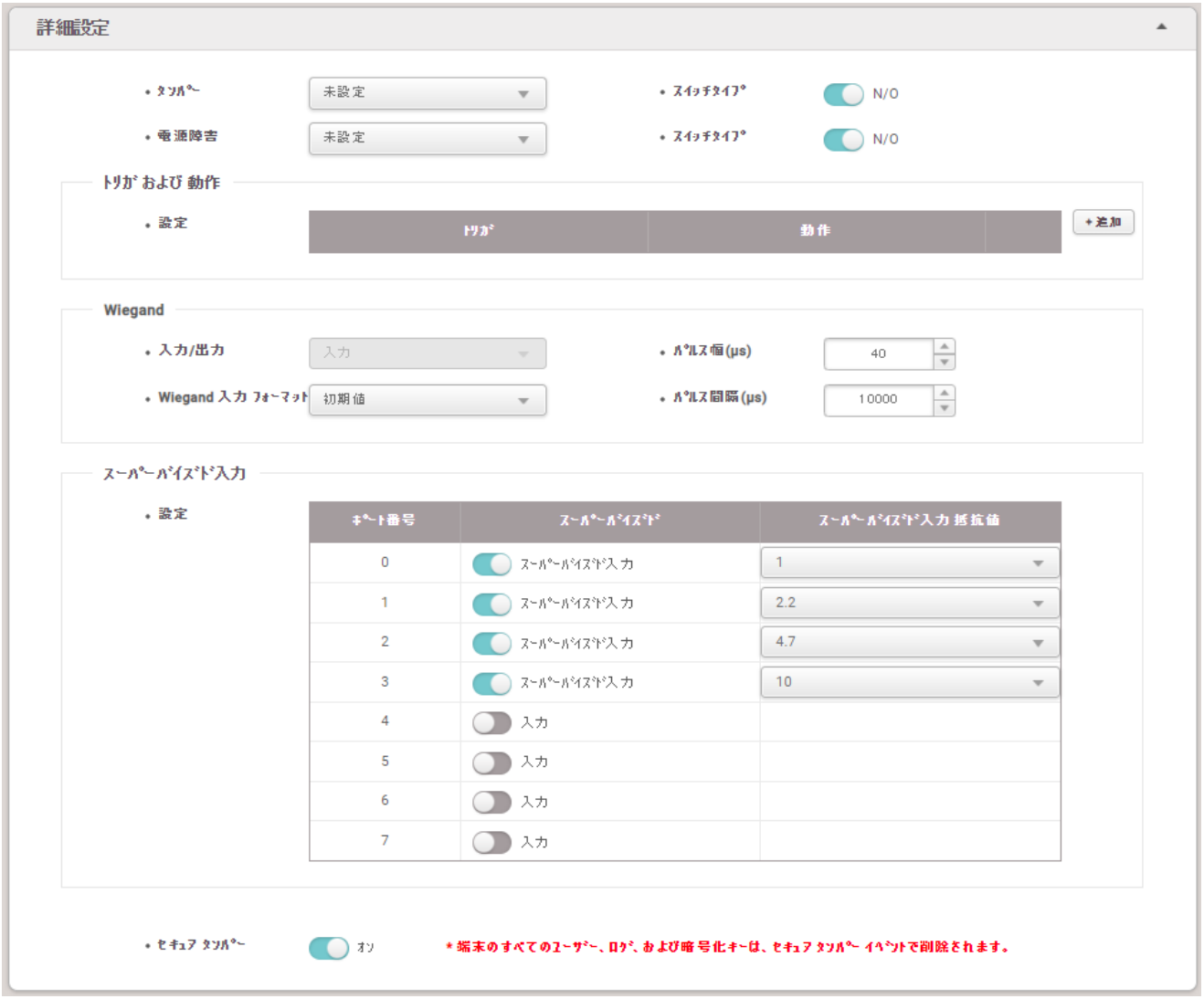
認証



項目	説明
認証	サーバーマッチング: サーバーマッチングを設定できます。有効に設定すると、BioStar 2 がインストールされている PC に保存されているユーザー情報を使用して認証が実行され、無効に設定すると、端末に保存されているユーザー情報を使用して認証が実行されます。サーバーマッチングを使用する場合、BioStar 2 のサーバーマッチングも有効にする必要があります。詳細については、サーバーを参照してください。
指紋	・1:N セキュリティレベル: 指紋認証または顔認証に使用するセキュリティレベルを設定できます。セキュリティレベルを高く設定すると、本人拒否率（FRR）は高くなりますが、本人拒否率（FAR）は低くなります。

	・1:N 認証速度: 指紋認証速度を設定できます。自動を選択すると、端末内に登録されている指紋テンプレートの合計量に従って認証速度が構成されます。 ・テンプレート: 指紋テンプレートフォーマットを表示できます。
カードの種類	端末で使用するカードの種類を設定できます。 **メモ** 端末が対応しているカードの種類が表示されます。 ・ CSN カード: CSN カードとフォーマットタイプを選択し、バイトオーダーを設定できます。 **メモ** ・ フォーマットタイプが通常に設定されている場合、端末はカードのシリアル番号（CSN）を読み取ります。Wiegand に設定されている場合、端末は、ユーザーが定義した Wiegand 形式でカードのシリアル番号を読み取ります。 ・ フォーマットタイプが Wiegand に設定されている場合、端末で使用する Wiegand 形式を選択できます。新しい Wiegand 形式を設定するには、Wiegand を参照してください。 ・ バイトオーダーが MSB に設定されている場合、端末はカード ID を最上位バイトから最下位バイトへと読み取ります。たとえば、カード ID 0x12345678 の最上位バイトは 0x12 であり、端末は 0x12、0x34、0x56、0x78 を順番に読み取ります。LSB に設定されている場合、端末はカード ID を最下位バイトから最上位バイトに読み取ります。 ・ ・モバイルカード: モバイルカードの種類を設定できます。

詳細設定



項目	説明
詳細設定	・ タンパー ： タンパーが接続されている AUX ポートを設定できます。 ・ 電源障害: 電源入力信号を監視する AUX ポートを設定できます。
トリガーおよび動作	・ 設定: 事前に定義されたアラームまたは信号入力に従って、端末の動作を設定できます。たとえば、CoreStation でタンパーオンの信号が発生した場合に、ユーザーが設定した信号を出力するか、端末を使用しないように設定できます。
Wiegand	・ 入力/出力: 入力モードのみ使用できます。 ・ Wiegand 入力フォーマット: Wiegand の形式を設定できます。Wiegand 形式の設定の詳細については、カード形式を参照してください。 ・ パルス幅: Wiegand 信号のパルス幅を設定できます。 ・ パルス間隔: Wiegand 信号のパルス間隔を設定できます。
スーパーバイズド入力	CoreStation のスーパーバイズド入力ポートを TTL 入力ポートとして使用するように設定し、監視入力に使用する抵抗値を設定できます。抵抗値は 1 kΩ、2.2 kΩ、4.7 kΩ、10 kΩが設定できます。

セキュアタンパー	端末でタンパーが発生した場合、端末に保存されているユーザー情報全体、ログ全体、およびセキュリティキーを削除するように設定できます。

OSDP 端末 LED/ブザー

項目	説明
OSDP 端末 LED/ブザー	CoreStation に接続されているすべての OSDP 端末でイベントが発生した場合、LED とブザーの動作を一括で設定できます。 **メモ** CoreStation に接続された OSDP 端末が LED とブザーに対応していない場合、設定どおりに動作しない場合があります。
LED	入力大気中、認証成功、認証失敗イベントが発生した時の LED の動作を設定します。 ・ モード: OFF、一定、点滅の中から希望の動作を設定します。 ・ 周期: モードが点滅に設定されている場合、LED の点滅回数を入力します。無限をオンにすると、設定したモードが連続して繰り返されます。 ・ 色/遅延: モードが点滅に設定されている場合、設定された繰り返し回数で点滅する 2 つの色を選択し、遅延を入力します。モードが一定に設定されている場合、表示する色を 1 つ選択し、遅延を入力します。
ブザー	入力待ちイベント、認証成功イベント、認証失敗イベント発生時のブザー動作を設定します。 ・ モード: OFF、一定、ビーピングの中から目的の動作を設定します。 ・ 周期: モードがビーピングに設定されている場合、ブザーの再生回数を入力します。無限をオンにすると、設定した Mode が連続して繰り返されます。 ・ 遅延: モードがビーピングに設定されている場合、設定された繰り返し回数ごとにブザーが再生される時間を入力します。モードが一定に設定されている場合、ブザーが再生される時間を入力します。

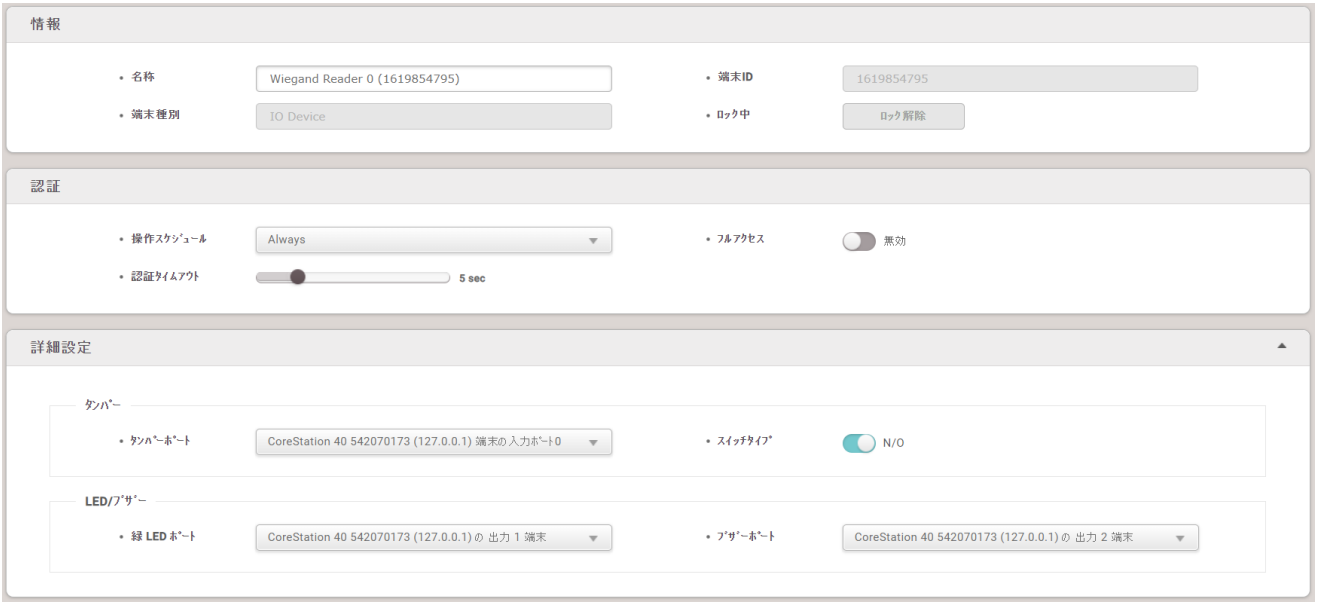
4 [適用]をクリックして設定を保存します。

Wiegand 端末

登録された Wiegand 端末の詳細情報を編集できます。

1 [端末]をクリックします。

2 編集する端末一覧で Wiegand 端末をクリックします。

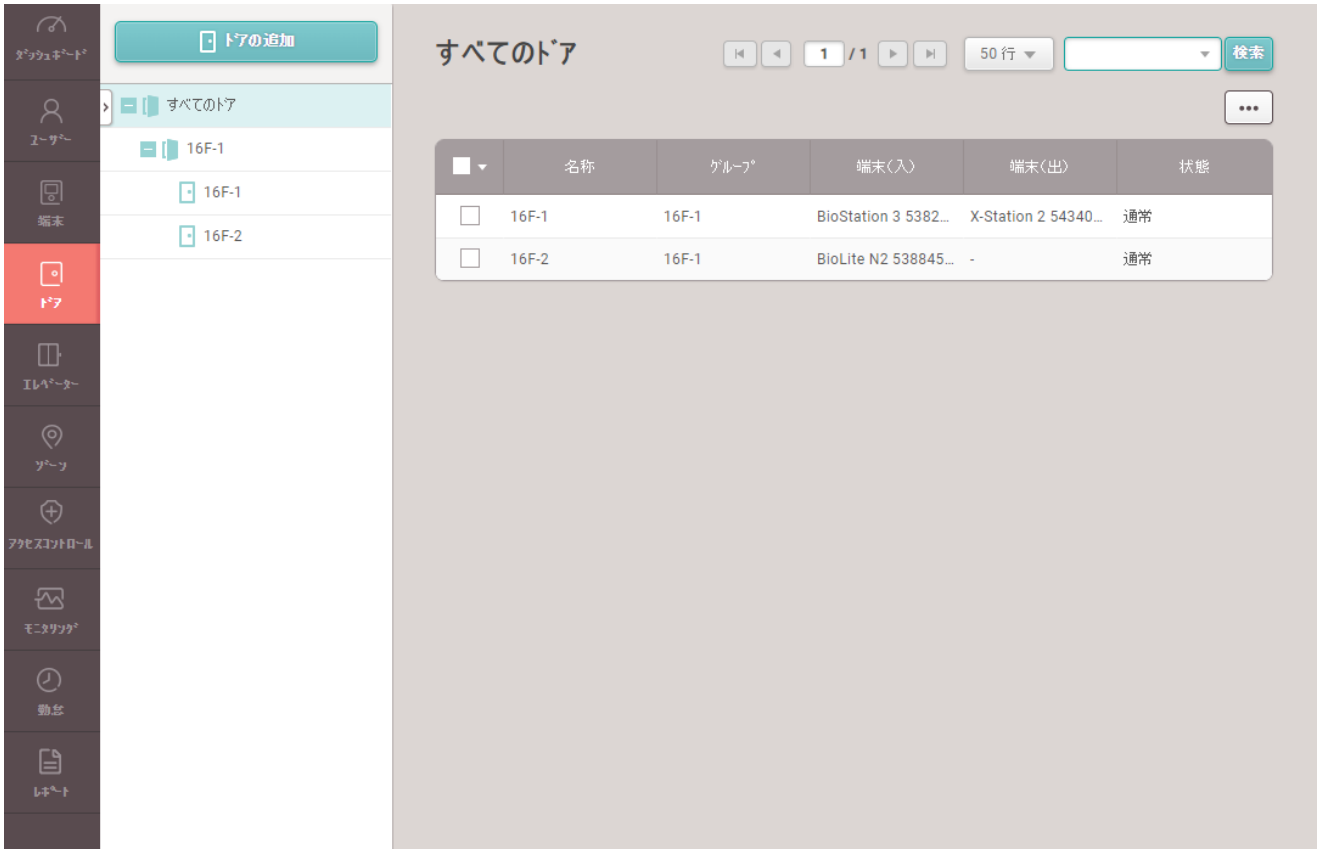


項番	項目名	説明
1	情報	Wiegand 端末の設定を変更できます。 ・ 名前: 端末名を入力します。 ・ 端末 ID: 端末 ID を表示します。 ・ 端末種別: 端末の種類を表示します。
2	認証	Wiegand 端末の認証設定を変更します。 ・ 操作スケジュール: 端末の有効な時間を設定します。 ・ フルアクセス: ユーザーがいつでも認証できるようにします。 これにより、マスター端末の上のユーザーのアクセスグループが上書きされます。 ・ 認証タイムアウト: 認証タイムアウト期間を設定できます。 設定時間内に認証が完了しない場合、認証に失敗します。
3	詳細設定	Wiegand 端末のタンパー スイッチと LED の設定を変更します。 ・ タンパーポート: Wiegand 端末のタンパースイッチが接続されている入力ポートを選択します。 ・ スイッチタイプ: タンパー操作のタンパー スイッチ タイプを選択します。 ・ 緑 LED ポート: 緑 LED の制御ポートを選択します。 ・ ブザーポート: ブザーの制御ポートを選択します。

3 [適用]をクリックして設定を保存します。

9 ドア

ドアメニューでは、端末に接続されたドアに関する情報の設定を行えます。



- ドアグループの追加と管理
- ドアを追加
- ドアの編集

1	ドアを追加	5	ドアー覧
2	ページ ナビゲーション ボタンとリストの行数	6	ドアとグループのリスト
3	登録端末検索	7	展開ボタン
4	機能ボタン(印刷、カラム設定)		

ドアを選択すると、以下を実行できます。

・ ドアの削除: 選択したドアをリストから削除します。

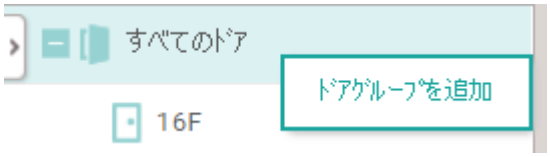
ドアグループの追加と管理

グループを追加して、複数のドアを簡単に管理できます。

ドアグループを追加する

1 [ドア]をクリックします。

2 [すべてのドアグループ]を右クリックし、[ドアグループを追加]をクリックします。



3 グループ名を入力します。

メモ

- ドアグループは最大 8 レベルで作成できます。
- ドアグループ名は 48 文字まで入力できます。

ドアグループの名前を変更する

1 [ドア]をクリックします。

2 名前を変更するグループの名前を右クリックし、[ドアグループの名前を変更]をクリックします。

3 名前を入力します。

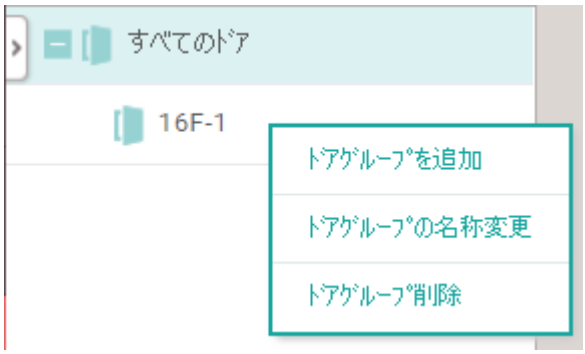
メモ

ドアグループ名は 48 文字まで入力できます。

ドアグループを削除する

1 [ドア]をクリックします。

2 削除するグループの名前を右クリックし、[ユーザーグループの削除]をクリックします。



メモ

グループを削除すると、グループ内のすべてのドアが削除されます。

ドアを追加する

アクセスコントロールで使用するドアを設定できます。

入室端末と退出端末を選択し、アンチパスバック設定を構成してセキュリティを強化し、ドアごとに警報を設定できます。

1 [ドア]をクリックし、[ドアを追加]をクリックします。

2 情報、設定、追加設定、アンチパスバック、警報を参照して設定を行います。

3 すべての情報を編集したら、[適用]をクリックします。

➢ 関連情報

基本的な検索と登録

スレーブ端末の検索と登録

アクセスレベルの追加と管理

情報

ドアの名前、グループ、および説明を入力または編集できます。

1 [情報]タブのすべてのフィールドを編集します。

項番	項目名	説明
1	名称	ドア名を入力します。
2	グループ	ドアグループを設定します。 ドアグループの追加の詳細については、ドアグループの追加と管理を参照してください。
3	説明	ドアの簡単な説明を入力します。

2 [適用]をクリックして設定を保存します。

設定

端末、退出ボタン、ドアセンサーなどのさまざまな設定を行うことができます。

1 [設定]タブのフィールドを編集します。

項番	項目名	説明
1	端末(入)	入室に使用する端末を選択します。登録されている端末のリストから端末を選択できます。 登録済みの端末が利用できない場合は、基本的な検索と登録、指定端末検索と登録、Wiegand 端末の検索と登録、またはスレーブ端末の検索と登録を参照してください。 **メモ** U & Z 無線ドアロックが端末(入)として選択されている場合は、U & Z 無線ドア ロックが端末(出)としても選択されている必要があります。
2	ドアリレー(*)	電気錠を制御するリレーを選択します。 **メモ** U & Z 無線ドアロックが端末(入)として選択されている場合は、ドアリレーは表示されません。
3	退出ボタン	退出ボタンに使用するポートを選択します。
3-A	スイッチ	N/O または N/C に設定できます。
3-B	解錠とみなす	退出ボタンが押されたときに、ドア解錠要求ログが発生するが、リレーが作動しないように設定できます。
4	ドア開閉確認	ドアの状態を確認するポートを選択します。 [ドア開閉確認]が未使用に設定されている場合、[警報]タブは編集できません。
4-A	スイッチ	N/O または N/C に設定できます。
4-B	通行確認 APB 利用時のドアセンサー利用	入室確認 APB 使用時にドアセンサーを使用するかどうかを設定できます。
5	端末(出)	退室に使用する端末を選択します。 退室端末は、スレーブ端末が接続されている場合にのみ使用できます。 スレーブ端末が登録されていない場合は、基本的な検索と登録、指定端末検索と登録、Wiegand

		端末の検索と登録、またはスレーブ端末の検索と登録を参照してください。 [端末(出)]が選択されていない場合、[アンチパスバック]タブは編集できません。

2 [適用]をクリックして設定を保存します。

メモ

CoreStation を端末(入)または端末(出)として設定することはできません。

➢ 関連情報

アンチパスバック

追加設定

追加のオプションを設定できます。

1 [追加設定]タブのフィールドを編集します。

項番	項目名	説明
1	解錠	ドア開閉に関するオプションを設定できます。
1-A	解錠時間	ユーザー認証が完了した後、ドアへの解錠信号を維持する時間を設定します。 認証が成功すると、設定した時間だけリレーが作動します。 この時間が経過すると、リレーはドアに信号を送信しなくなります。 **メモ** ・ 使用する電気錠の種類によって、解錠時間を設定します。
1-B	ドアを閉じた時に強制施錠	扉が閉まっていることをドアセンサーが検知すると施錠します。 [解錠時間の経過時に施錠]がオンに設定されている場合、このオプションは使用できません。
1-C	解錠時間の経過時に施錠	自動ドアを玄関ドアとして使用する場合、ドアセンサーの状態に関係なくリレーが作動します。 このオプションは、[ドアを閉じた時に強制施錠]がオンに設定されている場合は使用できません。
2	二重認証	2 人(一般ユーザーと管理者)の資格情報を認証する場合にのみ、ドアが開くように設定できます。
2-A	端末	二重認証を使用する端末を選択します。[未設定]が選択されている場合、二重認証モードは無効になります。 **メモ** ・ 以前に混雑制限ゾーンで端末(入)または端末(出)として設定されていた端末で二重認証機能を使用する場合は、[ゾーン] > [混雑制限]をクリックし、端末を端末(入)または端末(出)として再度設定します。詳細については、混雑制限ゾーンを参照してください。 ・ スケジュール: 二重認証を使用するスケジュールを設定します。希望のスケジュールがない場合は、[+スケジュールを追加]をクリックして作成します。スケジュール

		の設定の詳細については、「スケジュール」を参照してください。
2-B	認証順条件	管理者の認証順序を設定できます。[未使用]に設定すると、アクセスグループに関係なく、2 人のユーザーが認証を受ける必要があります。[2 回目指定]に設定すると、通常のユーザー認証の後に、設定されたアクセスグループに属するユーザーによる認証が必要になります。
2-C	2 回目 認証グループ	管理者が属するグループを設定できます。
2-D	タイムアウト	最初の資格情報が認証された後、2 番目の資格情報を認証するためのタイムアウト時間を設定します。最初の認証資格が認証された後、タイムアウト期間内に 2 番目の認証資格が認証されない場合、ドアは開きません。
3	共連れ検知	共連れを検出するようにドアを設定できます。
3-A	センサー	共連れを検出するセンサーを選択できます。
3-B	スイッチ	N/O または N/C に設定できます。

2 [適用]をクリックして設定を保存します。

アンチパスバック

この機能は、端末(入)と端末(出)の両方が設定されている場合に使用できます。
端末(出)が[未設定]の場合、この機能は使用できません。
端末(出)の設定詳細については、[設定]を参照してください。

メモ

ドアページのアンチパスバック項目を有効にするには、マスター端末とスレーブ端末を RS-485 インターフェイス経由で接続する必要があります。

1 アンチパスバックタブのフィールドを編集します。

項番	項目名	説明
1	種別	アンチパスバックタイプを選択します。 ・なし: アンチパスバック機能を無効にするには、このオプションを選択します。 ・ソフト APB: このオプションを選択すると、認証は成功します。アンチパスバックに違反したイベントが発生します。 ・ハード APB: このオプションを選択すると、認証は失敗します。アンチパスバックに違反したイベントが発生します。
2	APB 解除時間	アンチパスバック機能をリセットする期間を設定できます。 可能な最大期間は 7 日間(10, 080 分)です。 0 に設定すると、無期限となり、機能はリセットされません。

2 [適用]をクリックして設定を保存します。

警報

ドアのこじ開けが発生した時、開けっ放しになっている時、または、アンチパスバック違反が発生した時に、警報を鳴らし、端末を端末利用不可にするように設定できます。

1 [警報]タブのフィールドを編集します。動作を追加するには、[+追加]をクリックします。

項番	項目名	説明
1	ドア開放	ドアが開けっ放しになっている時に実行される警報動作を設定できます。 [+追加]をクリックして、動作を選択します。[OK]をクリックして動作を追加します。
2	ドア開放時間	ドアが開けっぱなしになっているとみなす時間を設定できます。
3	認証なしドアオープン	ドアがこじ開けられた時に実行される警報動作を設定できます。 [+追加]をクリックして、動作を選択します。[OK]をクリックして動作を追加します。
4	アンチパスバック	アンチパスバック違反が発生した時に実行される警報動作を設定できます。 [+追加]をクリックして、動作を選択します。[OK]をクリックしてアクションを追加します。 ・ アンチパスバックを設定するには、端末(出)を登録する必要があります。

2 [適用]をクリックして設定を保存します。

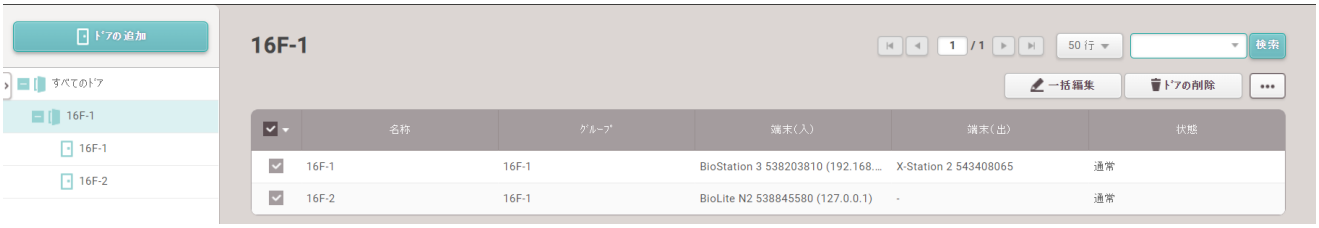
ドアの編集

既存のドアの編集や、複数のドアの一括編集を行えます。

1 [ドア]をクリックします。

2 ドア一覧で、編集するドアをクリックします。

3 ドアの追加の手順を参照して、詳細を編集します。



4 複数のドアの情報を編集するには、複数のドアを選択して[一括編集]をクリックします

5 編集したいフィールドのえんぴつマーク(✎)をクリックして、情報を編集します。

6 情報を編集した後、[OK]をクリックします。

10 エレベーター

エレベーターメニューでは、エレベーター制御に関する項目の設定を行えます。

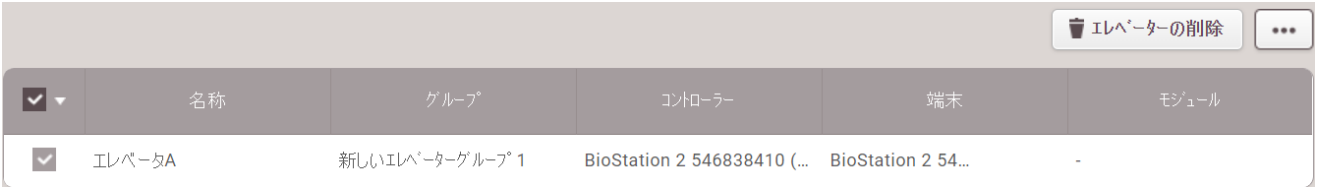
メモ

AC ライセンスのアドバンスド以上のライセンスを有効にすると表示されます。

- エレベーターグループの追加と管理
- エレベーターの追加
- エレベーターの編集

エレベーターを選択すると、次のアクションを実行できます。

1	エレベーターの追加	5	エレベーター一覧
2	ページナビゲーションボタンとリストの行数	6	エレベーターとグループ一覧
3	登録されたエレベーターの検索	7	展開ボタン
4	機能ボタン(印刷、カラム設定)		



・ エレベーターの削除：選択したエレベーターをリストから削除します。

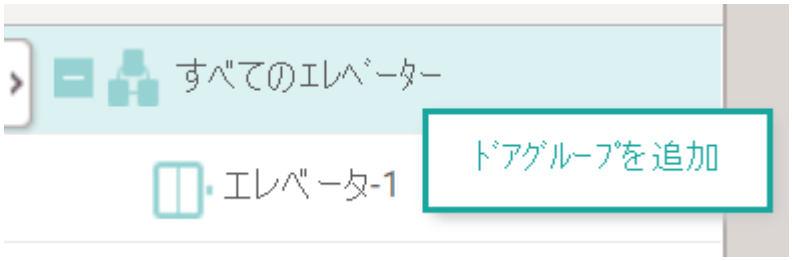
エレベーターグループの追加と管理

複数のエレベーターの管理のためにグループを追加してグルーピング管理できます。

エレベーターグループの追加

1 [エレベーター]をクリックします。

2 [すべてのエレベーター]を右クリックし、[ドアグループを追加]をクリックします。



3 グループ名を入力します。

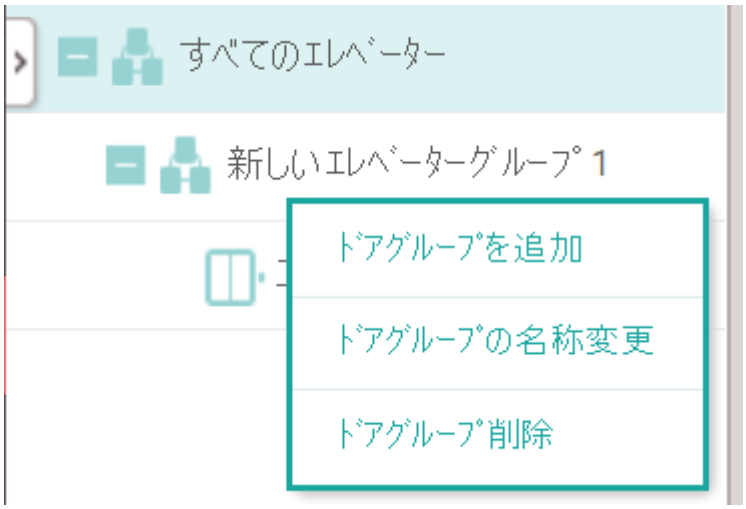
メモ

- エレベーターグループは最大 8 レベルまで作成できます。
- エレベーターグループ名は 48 文字まで入力できます。

エレベーターグループの名前変更

1 [エレベーター]をクリックします。

2 名前を変更するグループの名前を右クリックし、[ドアグループの名称変更]をクリックします。



3 名前を入力します。

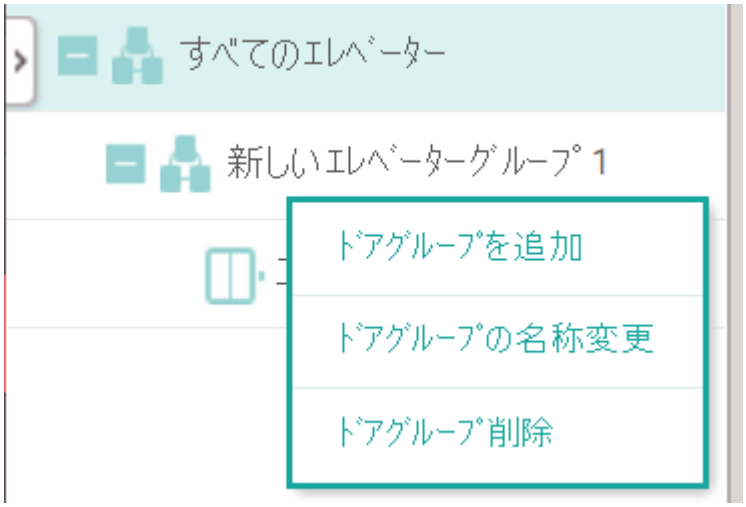
メモ

エレベーターグループ名は 48 文字まで入力できます。

エレベーターグループの削除

1 [エレベーター]をクリックします。

2 削除するグループの名前を右クリックし、[ドアグループ削除]をクリックします。



メモ

グループを削除すると、グループ内のすべてのエレベーターが削除されます。

エレベーターの追加

エレベーター制御に使用するエレベーターを設定できます。

1 [エレベーター]をクリックし、[エレベーターの追加]をクリックします。

2 情報、詳細、追加設定、警報を参照して設定します。

3 すべての情報を編集したら、[適用]をクリックします。

➢ 関連情報

基本的な検索と登録

スレーブ端末の検索と登録

アクセスレベルの追加と管理

情報

エレベーターの名前、グループ、および説明を入力または編集できます。

1 [情報]タブのすべてのフィールドを編集します。

項番	項目名	説明
1	名前	エレベーター名を入力してください。
2	グループ	エレベーターグループを設定します。ドアグループの追加の詳細については、「エレベーターグループの追加と管理」を参照してください。
3	説明	エレベーターの簡単な説明を入力します。

2 [適用]をクリックして設定を保存します。

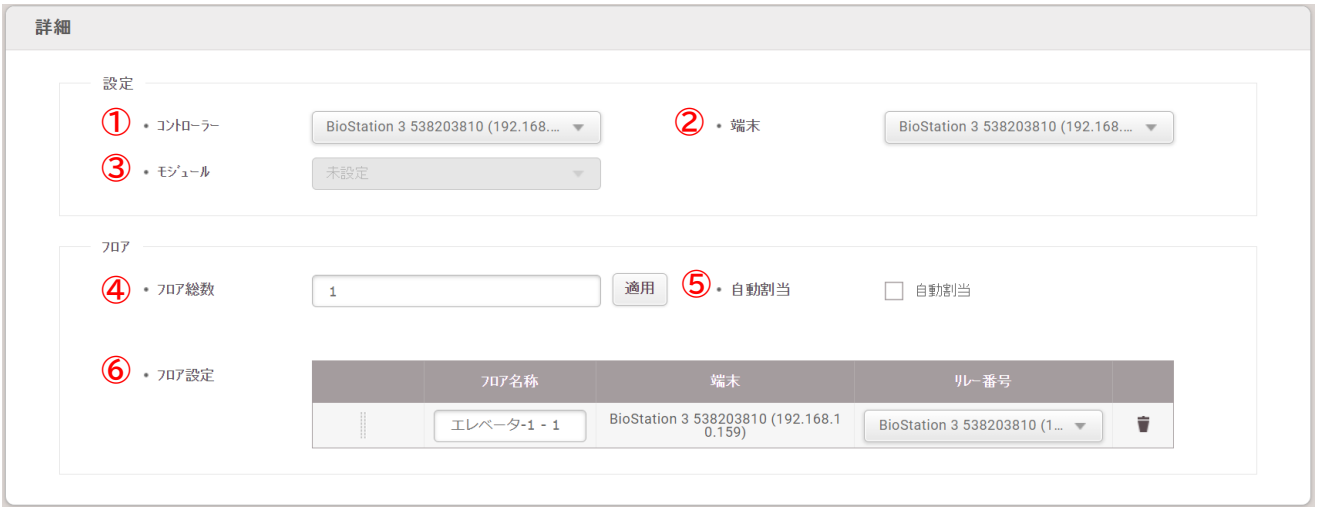
詳細

エレベーターとフロア情報に接続する端末を選択できます。

メモ

BioEntry Plus、BioEntry W、BioLite Net はコントローラーとして使用できません。

1 詳細タブのすべてのフィールドを編集します。



項番	項目名	説明
1	コントローラー	エレベーターのアクセス許可を制御する端末を選択します。 **メモ** ・ マスター端末のみを選択できます。 ・ 登録されている端末の一覧から選択できます。 登録済みの端末がない場合は、基本的な検索と登録を参照してください。
2	端末	認証に使用する端末を選択します。 **メモ** ・ マスター端末、スレーブ端末、Wiegand 端末の中から端末を選択できます。 ・ 最大 4 台のリーダーを選択できます。 ・ OM-120 をリーダーとしての設定は行えません。
3	モジュール	端末を選択して、エレベーターのフロアボタンへのリレーを制御します。 **メモ** OM-120, DM-20, IM-120, SIO2 のみ選択可能です。
4	フロア総数	エレベーターで移動できるフロアの総数を入力します。

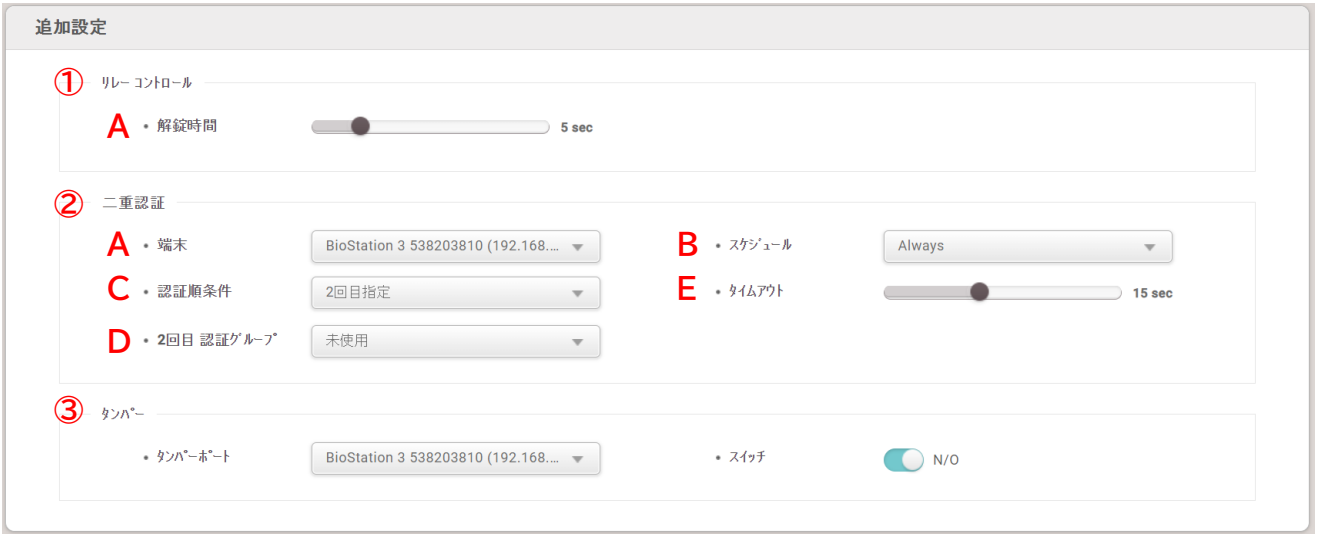
		メモ 192 フロアまで入力を行えます。
5	自動割当	自動割当を使用するかどうかを選択します。 自動割当を使用する場合、リレー番号は連続した順序で割り当てられます。
6	フロア設定	フロアを制御するフロア名とリレー番号を設定できます。

2 [適用]をクリックして設定を保存します。

追加設定

追加のオプションを設定できます。

1 [追加設定]タブのフィールドを編集します。



項番	項目名	説明
1	リレーコントロール	エレベーターのフロアボタンのリレー制御に関するオプションを設定できます。
1-A	解錠時間	ユーザー認証が完了した後、フロアボタンが有効になる時間を設定します。 認証が成功すると、設定した時間だけリレーが作動します。 この時間が経過すると、フロアボタンが有効になる信号の送信を終了します。
2	二重認証	2 人(通常のユーザーと管理者)の資格情報を認証する場合にのみ有効になるようにフロアボタンを設定できます。
2-A	端末	二重認証を使用する端末を選択します。 [未使用]が選択されている場合、二重認証モードは無効になります。 **メモ** 以前に混雑制限ゾーンで端末(入)または端末(出)として設定されていた端末で二重認証機能を使用する場合は、[ゾーン] > [混雑制限]をクリックし、端末を端末(入)または端末(出)として再度設定します。詳細については、混雑制限ゾーンを参照してください。
2-B	スケジュール	二重認証を使用するスケジュールを設定します。 希望のスケジュールがない場合は、[+スケジュールを追加]をクリックして作成します。 スケジュールの設定の詳細については、[スケジュール]を参照してください。
2-C	認証順条件	管理者の認証順序を設定できます。[未使用]に設定すると、アクセスグループに関係なく、2人のユーザーが認証を受ける必要があります。[最終選択内容]に設定すると、通常のユーザー認証の後に、設定されたアクセスグループに属するユーザーによる認証が必要になります。
2-D	2 回目認証グループ	管理者が属するグループを設定できます。

2-E	タイムアウト	最初の資格情報が認証された後、2 番目の資格情報を認証するためのタイムアウト時間を設定します。最初の認証資格が認証された後、タイムアウト時間内に 2 番目の認証資格が認証されない場合、信号は送信されません。
3	タンパー	タンパー信号を出力するポートを設定できます。
3-1	タンパーポート	入力に使用するポートを設定します。
3-2	スイッチ	N/O または N/C に設定できます。

2 [適用]をクリックして設定を保存します。

警報

タンパー入力や入力信号を検出したときの動作を設定できます。

1 [警報]タブのフィールドを編集します。動作を追加するには、[+追加]をクリックします。

項番	項目名	説明
1	トリガ	タンパー入力検出、または、入力信号検出を設定できます。
2	動作	トリガーに設定した項目の状態に応じて、動作を実行するように設定できます。 エレベーターのフロアボタンを有効化など特定の信号の出力を設定できます。

2 [適用]をクリックして設定を保存します。

エレベーターの編集

既存エレベーターの編集、複数のエレベーターの一括編集などを行えます。

1. [エレベーター]をクリックします。
2. エレベーター一覧で、編集するエレベーターをクリックします。
3. エレベーターの追加の手順を参照して、詳細を編集します。
4. 複数のエレベーターの情報を編集するには、複数のエレベーターを選択して[一括編集]をクリックします。
5. 編集したいフィールドをえんぴつマーク(✎)をクリックして、情報を編集します。
6. すべての情報を編集したら、[OK]をクリックします。

11 アクセスコントロール

アクセスコントロールメニューでは、端末で認証を行った時に照合されたユーザーID のアクセス権限の有無に関する設定を行えます。ドアとアクセススケジュールを設定してアクセスレベルを作成し、アクセスレベルとユーザーやユーザーグループの情報を構成してアクセスグループの設定を行えます。設定されたアクセスグループは、アクセスコントロール(アクセス権限の有無)の構成要素として使用されます。

メモ

AC ライセンスのアドバンスド以上のライセンスを有効にすると、[フロアレベル]タブと[フロアレベル追加]ボタンが表示されます。

- アクセスレベルの追加と管理
- アクセスグループの追加と管理
- フロア レベルの追加と管理
- アクセス権限ステータス

1	アクセスグループの追加	6	機能ボタン(カラム設定)
2	アクセスレベルの追加	7	アクセスグループ / アクセスレベル / フロアレベル一覧
3	フロアレベルの追加	8	アクセスグループ / アクセスレベル / フロアレベル グループ
4	ページナビゲーションボタンとリストの行数	9	アクセスグループ、アクセスレベル、フロアレベル、および、状態一覧ページへのタブボタン
5	検索欄	10	展開ボタン

アクセスグループ、アクセスレベル、フロアレベルを選択すると、次の動作を実行できます。

- アクセスグループの削除: 選択したアクセスグループを一覧から削除します。
- アクセスレベルの削除: 選択したアクセスレベルを一覧から削除します。
- フロアレベルの削除: 選択したフロアレベルを一覧から削除します。

アクセスレベルの追加と管理

ユーザーがドアにアクセス許可するスケジュールを設定し、アクセスレベルにとして追加を行えます。

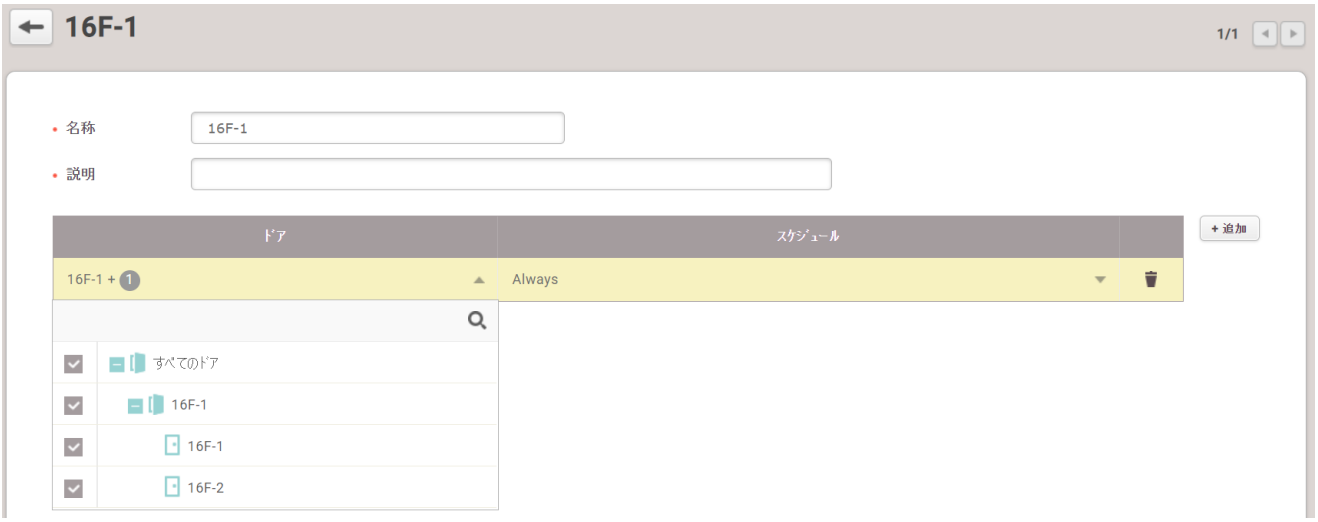
アクセスレベルの追加

1 [アクセスコントロール] > [アクセスレベルの追加]をクリックします。

2 アクセスレベルの名前と説明を入力します。

3 [+追加]をクリックします。

1 ドアのリスト展開ボタン(▼)をクリックして選択します。



メモ

- 検索ボタン(🔍)をクリックして項目を検索します。
- 目的のドアが見つからない場合は、ドアの追加を参照して追加します。
- 目的のスケジュールが見つからない場合は、[+スケジュールを追加]をクリックして作成します。スケジュールの設定の詳細については、「スケジュール」を参照してください。
- アクセスグループごとに最大 128 のアクセスレベルの追加を行えます。
- ゴミ箱ボタン(🗑)をクリックして項目を削除します。

4 [適用]をクリックして設定を保存します。

アクセスレベルの編集

1 [アクセスコントロール] > [アクセスレベル]タブをクリックします。

2 アクセスレベル一覧で、編集するアクセスレベルを選択します。

3 必要なフィールドを編集したら、[適用]をクリックします。

アクセスレベルの削除

1 [アクセスコントロール] > [アクセスレベル]タブをクリックします。
2 アクセスレベル一覧で、削除するアクセスレベルを選択します。
3 [アクセスレベルの削除]をクリックします

アクセスグループの追加と管理

アクセスレベルとユーザーやユーザーグループの情報を使用して、アクセス権限の設定を行えます。

アクセスグループの追加

2 [アクセスコントロール] > [アクセスグループの追加]をクリックします。

3 アクセスグループの名前と説明を入力します。

4 各フィールドの[+追加]をクリックします。

5 アクセスレベル、フロアレベル、ユーザーグループ、ユーザーのリスト展開ボタン(▼)をクリックして選択します。

メモ

- 必要なアクセスレベルがない場合は、[+アクセスレベルの追加]をクリックして作成します。アクセスレベルの詳細については、アクセスレベルの追加と管理を参照してください。
- 必要なフロアレベルがない場合は、[+フロアレベルの追加]をクリックして作成します。フロアレベルの詳細については、フロアレベルの追加と管理を参照してください。
- ゴミ箱ボタン(🗑)をクリックして項目を削除します。

4 [適用]をクリックして設定を保存します。

アクセスグループの編集

1 [アクセスコントロール] > [アクセスグループ]タブをクリックします。

2 アクセスグループ一覧で、編集するアクセスグループを選択します。

3 必要なフィールドを編集したら、[適用]をクリックします。

アクセスグループの削除

1 [アクセスコントロール] > [アクセスグループ]タブをクリックします。
2 アクセスグループ一覧で、削除するアクセスグループを選択します。
3 [アクセスグループの削除]をクリックします。

フロアレベルの追加と管理

エレベーターとフロア情報を使用して、フロアのアクセス権限の設定を行えます。

メモ

AC ライセンスのスタンダード以上のライセンスを適用した場合のみ、[フロアレベル]タブと[フロアレベルの追加]ボタンが表示されます。

フロアレベルの追加

1 [アクセスコントロール] > [フロアレベルの追加]をクリックします。
2 フロアレベルの名前と説明を入力します。
3 [+追加]をクリックします。
4 エレベーター、フロア名、スケジュールをリスト展開ボタン(▼)をクリックして選択します。

メモ

・検索ボタン(🔍)をクリックして項目を検索します。
・目的のエレベーターが見つからない場合は、エレベーターの追加を参照して追加してください。
・目的のスケジュールが見つからない場合は、[+スケジュールを追加]をクリックして作成します。スケジュールの設定の詳細については、「スケジュール」を参照してください。
・ゴミ箱ボタン(🗑)をクリックして項目を削除します。

5 [適用]をクリックして設定を保存します。

フロアレベルの編集

1 [アクセスコントロール] > [フロアレベル]タブをクリックします。
2 フロアレベル リストで、編集するフロアレベルを選択します。
3 目的のフィールドを編集したら、[適用]をクリックします。

フロアレベルの削除

1 [アクセスコントロール] > [フロアレベル]タブをクリックします。
2 フロアレベル リストで、削除するフロアレベルを選択します。
3 [アクセスレベルの削除]をクリックします。

アクセスグループ状態

特定のドアにアクセス権限の有るユーザーの確認を行えます。

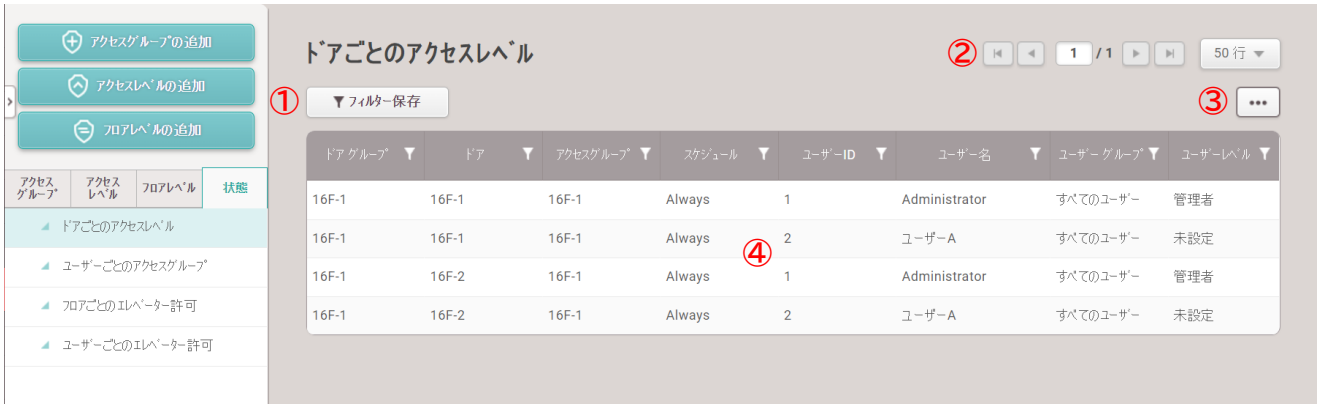
フィルターの使用、フィルターを組み合わせて結果の絞り込みを行えます。

結果は CSV ファイルとしてエクスポートを行えます。

1 [アクセスコントロール] > [状態]をクリックします。

2 ドアごとのアクセスレベル、ユーザーごとのアクセスグループ、フロアごとのエレベーターの許可、ユーザーごとのエレベーター許可を選択します。

3 フィルタリングした結果のみを表示するには、列のフィルターボタン()をクリックしてフィルターを適用します。



項番	項目名	説明
1	フィルター保存ボタン	設定したフィルターの保存を行えます。
2	ページナビゲーションボタンとリストの行数	ページの移動や 1 ページに表示する行数の設定を行えます。 最初のページに移動します。 前のページに移動します。 2 / 2 移動するページ番号を入力します。 次のページに進みます。 最後のページに移動します。 25 行 1 ページに表示する行数を設定します。
3	機能ボタン (CSV エクスポート、カラム設定)	CSV ファイルの保存やカラム設定の変更を行えます。
4	状態一覧	アクセス権限状態の閲覧を行えます。

12 ユーザー

ユーザーメニューでは、BioStar 2 や端末にユーザーの追加などユーザーに関する管理を行えます。

- ユーザーグループの追加と管理
- ユーザー情報の追加
- ユーザー認証資格の追加
- カード登録
- ユーザー情報を端末に転送する
- 端末からユーザー削除
- ユーザー情報の編集
- 長期未使用ユーザーの管理
- ビジュアル顔マイグレーション

1	ユーザーの追加	5	機能ボタン (印刷、カラム設定、CSV エクスポート、CSV インポート、ビジュアル顔のインポート、データファイルエクスポート、データファイルインポート、ビジュアル顔モバイル登録リンクを送信、ビジュアル顔マイグレーション)
2	ユーザー、長期未使用ユーザー画面へのタブ	6	ユーザー一覧
3	ページナビゲーションボタンとリストの行数	7	ユーザーグループ
4	検索欄	8	展開ボタン

メモ

・検索欄では「ユーザー名、メールアドレス」で検索できます。

・[ビジュアル顔モバイル登録リンクを送信]の詳細については、ビジュアル顔を登録を参照してください。

ユーザーを選択すると、次の操作を行えます

・一括編集: 複数のユーザーの情報を一括編集します。この機能は、複数のユーザーが選択されている場合にのみ行えます。

・端末に転送: BioStar 2 に登録されているユーザー情報を端末に転送します。

・端末から削除: 選択したユーザーを端末から削除します。

・ユーザー削除: 選択したユーザーを BioStar 2 から削除します。端末に登録されているユーザーは削除されません。

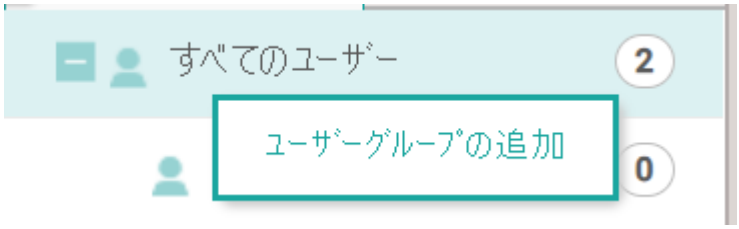
ユーザーグループの追加と管理

グループを追加して、複数のユーザーを簡単に管理できます。

ユーザーグループの追加

1 [ユーザー]をクリックします。

2 [すべてのユーザー]を右クリックし、[ユーザーグループの追加]をクリックします。



3 グループ名を入力します。

メモ

・ユーザーグループは最大 8 レベルまで作成できます。

・ユーザーグループ名は 48 文字まで入力できます。

ユーザーグループの名前変更

1 [ユーザー]をクリックします。

2 名前を変更するグループの名前を右クリックし、[ユーザーグループの名称変更]をクリックします。

3 グループ名を入力します。

メモ

ユーザーグループ名は 48 文字まで入力できます。

ユーザーグループの削除

1 [ユーザー]をクリックします。

2 削除するグループの名前を右クリックし、[ユーザーグループを削除]をクリックします。

ユーザー情報の追加

ユーザーの追加を行えます。

1 [ユーザー] > [ユーザーの追加]をクリックします。

2 [情報]タブで必要なフィールドを入力、または、選択します。

メモ

・必須アイコン(*)が付いている情報の入力は必須です。

項番	項目名	説明
1	写真	ユーザーの写真を追加します。[+画像]をクリックして、ユーザーの写真を選択します。 **メモ** ・ アップロードできるのは画像ファイルのみです。 ・ モバイルアクセスカードにユーザーの画像を表示するには、ユーザーの写真が必要です。
2	名前	ユーザーの名前を入力します。 **メモ** 最大 48 文字まで入力を行えます。 ※特殊文字は「~, !, @, #, $, %, ^, &, (,), -, _, =, +, [,], {, }, ;, ,」のみ使用可能
3	部門	ユーザーが所属する部門を入力します。

		メモ ・ 部門は、ユーザーの部門をモバイルアクセスカードに表示するために必要です。 ・ 最大 64 文字まで入力できます。 ※特殊文字はスペース( )またはアンダーバー(_)のみ使用可能
4	ID	ユーザーに割り当てる一意の ID を入力します。 メモ ・ [設定] > [サーバー]で[ユーザーID 種別]が[数字]に設定されている場合、1 ～ 4294967294 の数字の入力を行えます。 ・ [設定] > [サーバー]で[ユーザーID 種別]が[英数字]に設定されている場合、英字と数字の組み合わせの入力を行えます。 ・ ID を入力するときは、スペースは使用できません。 ・ ユーザーID 種別は、[数字]または[英数字]を設定できます。詳細については、サーバーを参照してください。
5	グループ	ユーザーグループを選択します。使用できるユーザーグループがない場合は、「ユーザーグループの追加と管理」を参照して追加します。
6	有効期限	ユーザーアカウントの有効期限を設定します。
7	BioStar 操作権限	BioStar の操作に関するアカウント権限を設定します。 ・未設定 : ユーザーには BioStar の操作権限がありません。 ・管理者: ユーザーはすべてのメニューの使用を行えます。 ・ユーザーオペレーター: ユーザーは、ユーザーおよび設定メニューのみの使用を行えます。 ・監視オペレーター: ユーザーは、モニタリングおよび設定メニューを使用でき、ダッシュボード、ユーザー、端末、ドア、ゾーン、アクセスコントロールメニューのみの表示を行えます。 ・勤怠オペレーター: ユーザーは勤怠メニューのみを使用と、ユーザーメニューのみの表示を行えます。 ・ユーザー: ユーザーは自分の情報と勤怠のみの表示を行えます。 メモ ・ 新しいユーザー権限を設定するには、カスタムアカウントレベルの追加を参照してください。 ・ BioStar 2.5.0 から BioStar 2.6.0 以降にアップグレードし、モニタリングのカスタムアカウントレベルを使用している場合は、[BioStar 操作権限]を再度設定する必要があります。
8	ログイン ID	ログイン ID を入力します。 メモ

		・ [BioStar 操作権限]を設定すると、[ログイン ID]が表示されます。
9	パスワード	ログインパスワードを入力します。セキュリティを参照して、パスワードレベルの変更を行えます。 **メモ** ・ [BioStar 操作権限]を設定すると、[パスワード]が表示されます。 ・ パスワードを入力すると、[パスワード確認]が表示されます。 確認のため、パスワードをもう一度入力します。
10	E メール	メールアドレスを入力します。 **メモ** ・ モバイルアクセスメッセージの項目が[E メール]に設定されている場合、モバイルアクセスを使用するときにユーザーの電子メールアドレスが必要です。 ・ ビジュアル顔モバイル登録、または、Secure QR(QR コード付きメールの送信)を使用する場合、ユーザーの電子メールアドレスが必要です。
11	役職	ユーザーの役職を入力します。 **メモ** ・ モバイルアクセスカードにユーザーの役職を表示するには、役職の入力が必要です。 ・ スペースまたはアンダーバー(_)のみを含めて 64 文字まで入力できます。
12	電話	電話番号を入力します。 **メモ** モバイルアクセスメッセージの項目が[テキスト メッセージ]に設定されている場合、モバイルアクセスを使用するときにユーザーの電話番号が必要です。
13	状態	ユーザーアカウントの一時的な無効化を行えます。
14	アクセスグループ	アクセスグループを設定します。 目的のアクセスグループがない場合は、アクセスグループの追加と管理を参照して追加します。
15	ユーザーIP	ユーザーIP を入力します。 ユーザーIP を登録すると、アカウントに登録した IP 情報と PC の IP 情報が一致した場合のみアクセスを許可することで、セキュリティの強化を行えます。 **メモ** ・ユーザー IP は、xxx.xxx.xxx.xxx の形式で入力できます。各オクテットには、0 ～ 255 の数字のみを入力できます。 ・ユーザーIP が登録されていないユーザーは、PC の IP 情報に関係なくログイン

		できます。 ・ クラウド(クラウド経由アクセス)を利用する場合、ユーザーは PC の IP 情報に関係なくログインできます。
16	カードを印刷	ユーザー情報をカードテンプレートとしてカードの印刷を行えます。 カードプリンターについては、カードプリンターを参照してください。

3 [資格]タブで必要なフィールドを入力または選択し、[適用]をクリックします。
資格情報の追加の詳細については、ユーザー資格情報の追加を参照してください。

メモ

・ 追加のユーザー情報用にカスタムユーザーフィールドを追加する方法については、サーバーのユーザー/端末管理を参照してください。

➢ 関連情報

ユーザー認証資格の追加
カード登録
アカウント
サーバー

CSV エクスポート/インポート

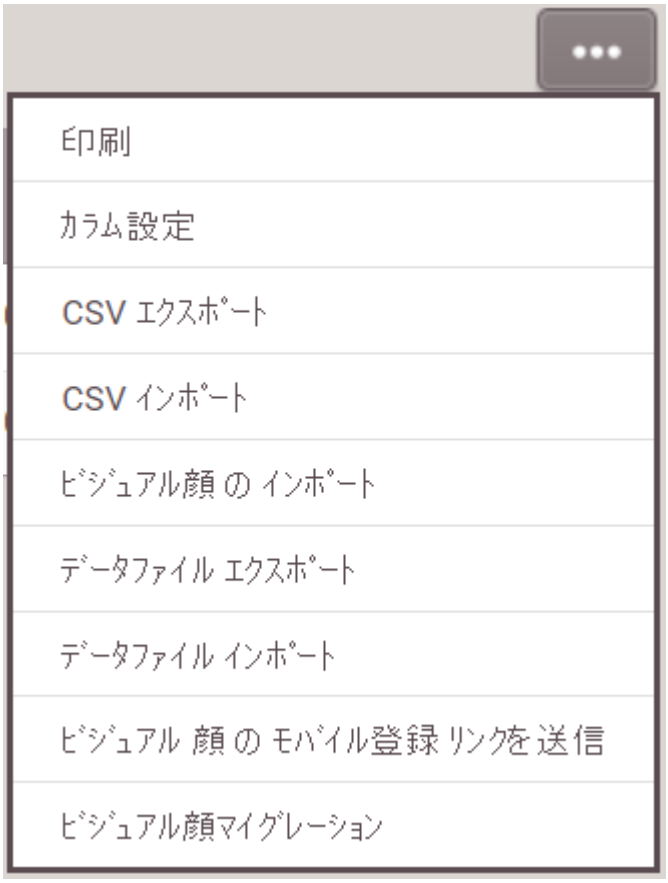
ユーザーデータの CSV エクスポートやインポートを行えます。

メモ

・インポートする CSV ファイルにカスタムユーザーフィールドのデータが含まれていて、そのフィールドがサーバー上に存在しない場合、フィールドのデータはインポートプロセス中に無視されます。
カスタムユーザーフィールドについては、サーバーを参照してください。
・ユーザー情報を英語または韓国語以外で入力する場合は、CSV ファイルを UTF-8 形式で保存してください。

CSV エクスポート

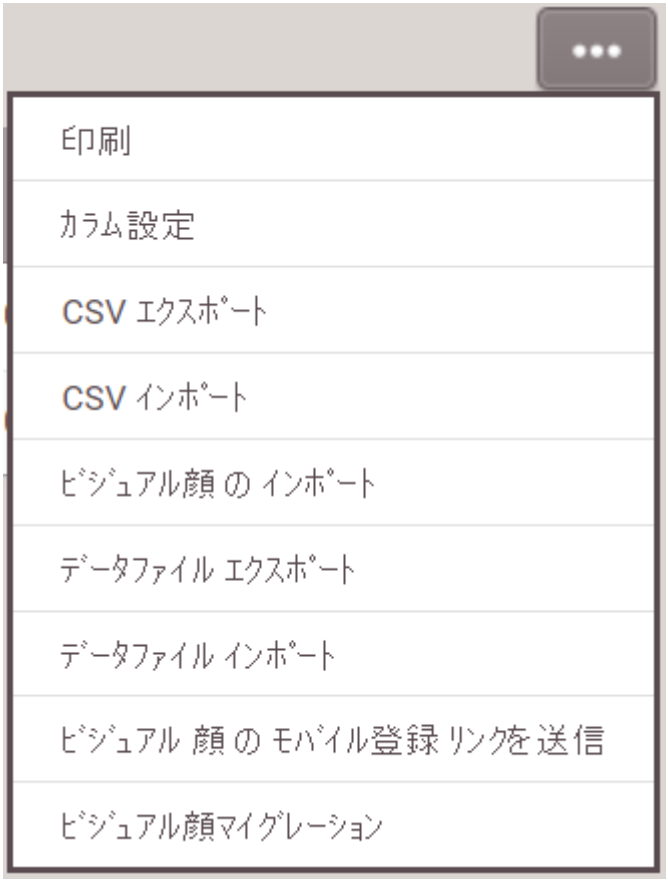
1 ユーザー一覧から CSV ファイルに保存するユーザーを選択し、機能ボタン(•••)をクリックします。
2 [CSV エクスポート]をクリックします。



3 CSV ファイルがダウンロードされます。

CSV インポート

1 機能ボタン(•••)をクリックし、[CSV インポート]をクリックします。



2 [参照]をクリックし、CSV ファイルを選択します。

3 [行のインポート開始]を設定し、[次へ]をクリックします。

4 CSV ファイルのユーザーデータフィールドと BioStar 2 のユーザーデータフィールドが自動的にマッピングされて表示

されます。

[再定義]をクリックすると、同じ名前のフィールドがリマップされます。

5 既に BioStar 2 に登録されているユーザーID のユーザーデータは更新しないか、CSV ファイルの情報で上書きするかを選択して、[次へ]をクリックします。

メモ

- CSV インポートでモバイルアクセスカードを発行できます。レギュラーサイトを使用している場合、CSV インポートが完了すると、Airfob ポータルのモバイルアクセスカードごとに 1 クレジットが差し引かれます。
  モバイルアクセスカードを発行したくない場合は、モバイルアクセスカードの列は未設定にしてください。
- 既に BioStar 2 に登録されているユーザーに発行されたモバイルアクセスカードと同じデータが CSV ファイルに存在する場合、データを更新しないか上書きすることができ、既存のモバイルアクセスカードは維持されます。
- 既に BioStar 2 に登録されているユーザーに発行されたモバイルアクセスカードと異なるデータが CSV ファイルにある場合、データが残っている場合は既存のモバイルアクセスカードを維持し、上書きされた場合は新しいモバイルアクセスカードを発行します。
- ダイナミックサイトを使用する場合、CSV インポートを使用してユーザーにモバイルアクセスカードを発行する場合、mobile_start_datetime フィールドと mobile_expiry_datetime フィールドを入力する必要があります。
- CSV インポート経由で BioStar 2 QR を発行することはできません。
- CSV インポートにて、ユーザーのビジュアル顔を登録できます。
  詳細については、ビジュアル顔を登録を参照してください。
- CSV インポートにて、ユーザーの PIN を登録できます。詳細については、PIN の追加を参照してください。

6 CSV インポートでエラーが発生した場合、エラー行のみの CSV ファイルをダウンロードおよび内容を確認し、CSV ファイルにエラーが無いように編集した後、再度アップロードを行ってください。

メモ

CSV ファイルに基本的なユーザー列以外の追加の列がある場合、BioStar 2 は CSV ファイルのインポートに失敗します。

ユーザー情報のエクスポート/インポート

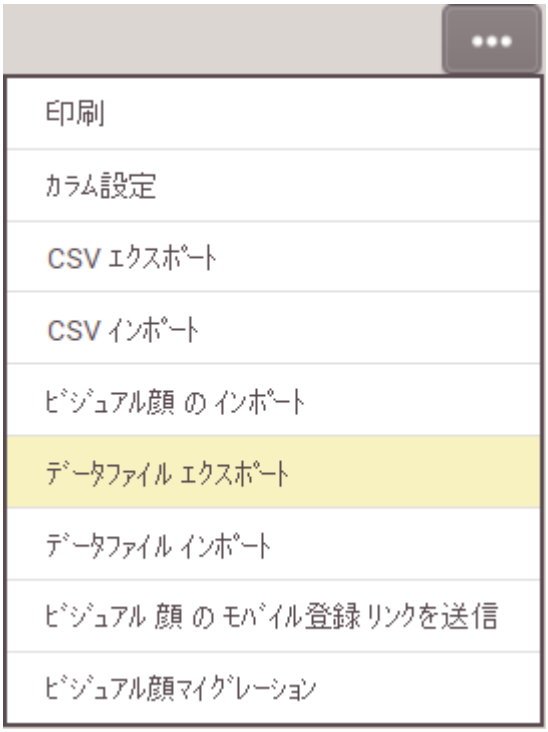
外部ストレージ(USB)にデータファイルを保存し、BioStar 2 または、端末にインポートを行えます。
最大 500,000 人のユーザーをサーバーから端末、または、端末から端末に移動できます。

メモ

- 古いファームウェアバージョンを使用している端末からエクスポートされたデータファイルは、BioStar 2 にインポートできません。常に最新バージョンのファームウェアを使用してください。
- BioStar 2.8.10 以降を使用している場合、以前のバージョンの BioStar 2 からエクスポートされたデータはインポートできません。
- BioStar 2.8.10 以降を使用している場合、古いファームウェアバージョンを使用している端末からデータを読み取ることはできません。端末のファームウェアと互換性のあるバージョンにアップグレードします。
  対応機種とファームウェアバージョンは以下の通りです。
  - BioStation 2 FW 1.9.0 以降
  - BioStation A2 FW 1.8.0 以降
  - FaceStation 2 FW 1.4.0 以降
  - FaceStation F2 FW 2.0.0 以降
  - X-Station 2 FW 1.0.0 以降
  - BioStation 3 FW1.0.0 以降
- 指紋テンプレートのフォーマットが異なる場合、データファイルのインポートを行えません。
  たとえば、Suprema 指紋テンプレートフォーマットを使用する端末からエクスポートされたデータファイルは、ISO 指紋テンプレートフォーマットを使用する端末にインポートを行えません。
- FaceStation F2 から登録されたビジュアル顔を含むユーザーデータをインポートする場合、画像のアップロードまたはモバイル端末経由で BioStar 2 にビジュアル顔データが既に登録されている場合、既存のデータは保持されます。

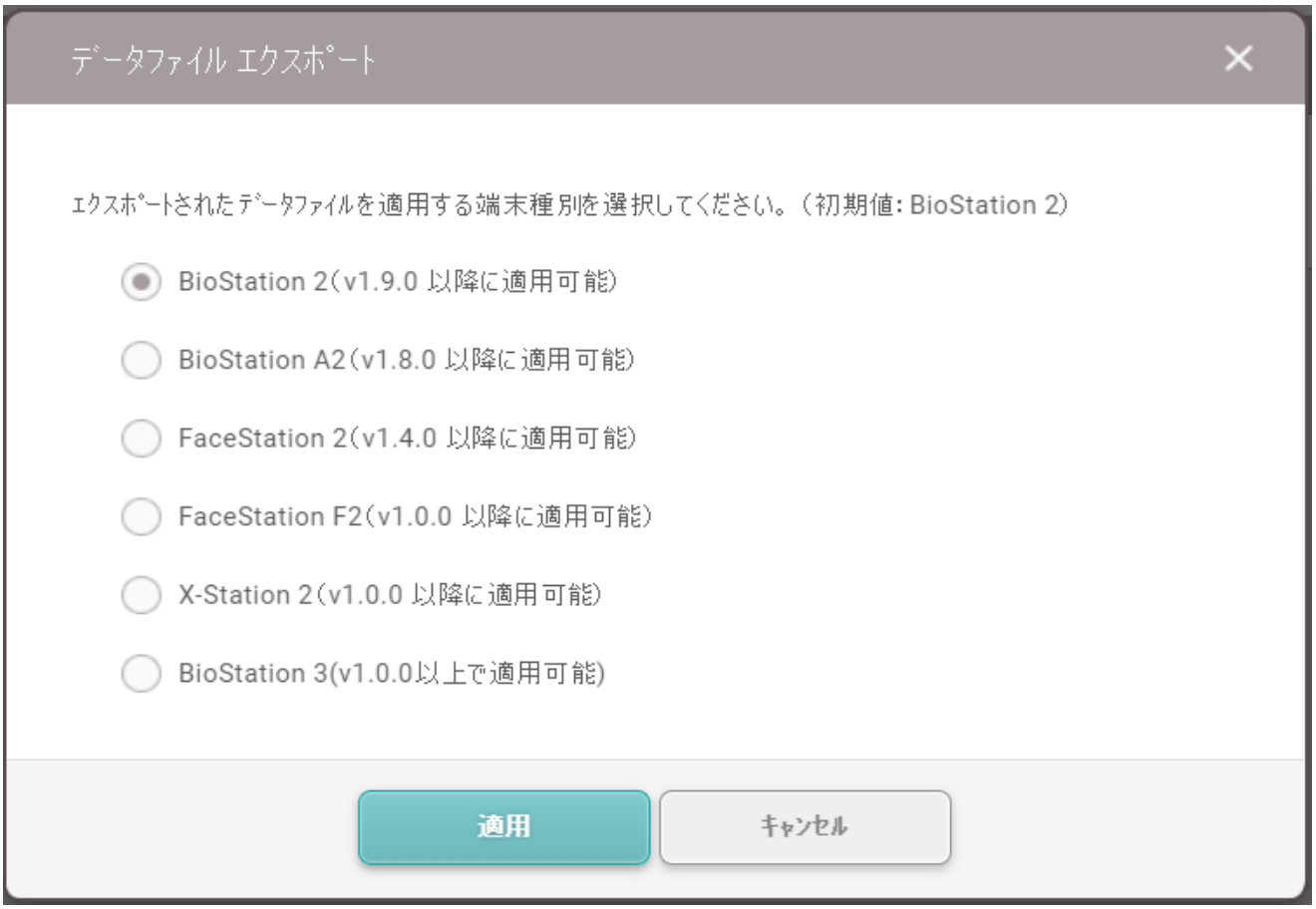
データファイルのエクスポート

1 ユーザー一覧からデータファイルにエクスポートするユーザーを選択し、機能ボタン(•••)をクリックします。
2 [データファイル エクスポート]をクリックします。



3 エクスポートされたデータファイルを適用する端末種別を選択します。

USB ポートを備えた端末のみが表示されます。



4 データファイルがダウンロードされます。

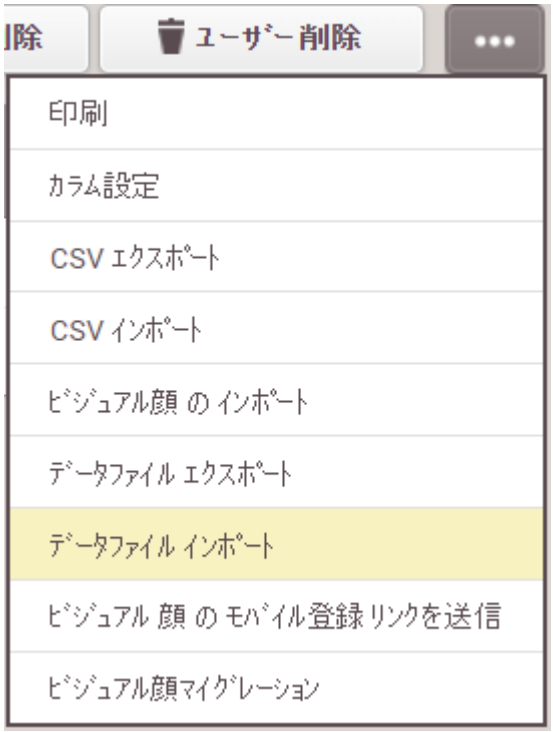
メモ

・エクスポートされたデータファイルには、写真、ユーザーID、名前、有効期限、アクセスグループ、PIN、認証モード、資格情報(顔、指紋、カード、モバイルアクセスカード、ビジュアル顔、BioStar 2 QR、QR/バーコード)、1:1 セキュリティレベルの情報が含まれます。

・端末が正しく選択されていることを確認してください。
正しく選択されていないと、端末はデータファイルを認識できません。

データファイルのインポート

1 機能ボタン(•••)をクリックし、[データファイル インポート]をクリックします。



2 目的のファイル（*.tgz）を選択し、[開く]をクリックします。

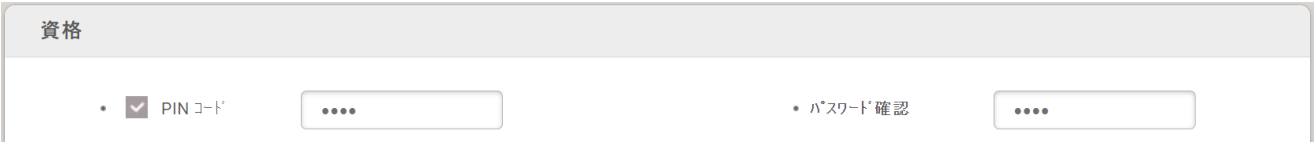
3 インポートが成功すると、成功メッセージが画面に表示されます。

ユーザー認証資格の追加

PIN、指紋、カードなど、さまざまなユーザー資格情報の追加を行えます。

PIN の追加

1 [PIN コード]を選択し、PIN を入力します。



2 確認のため、[パスワード確認]にもう一度 PIN を入力します。

3 [適用]をクリックして設定を保存します。

CSV インポートで登録

CSV ファイルをインポートして、ユーザーの PIN の登録を行えます。

1 インポートする CSV ファイルに PIN 列を追加します。

2 PIN 列にユーザーに割り当てる PIN を入力し、ファイルを保存します。

3 CSV インポートを参照して、PIN 列を追加した CSV ファイルを BioStar 2 にインポートします。

メモ

登録された PIN データの CSV エクスポートは行えません。

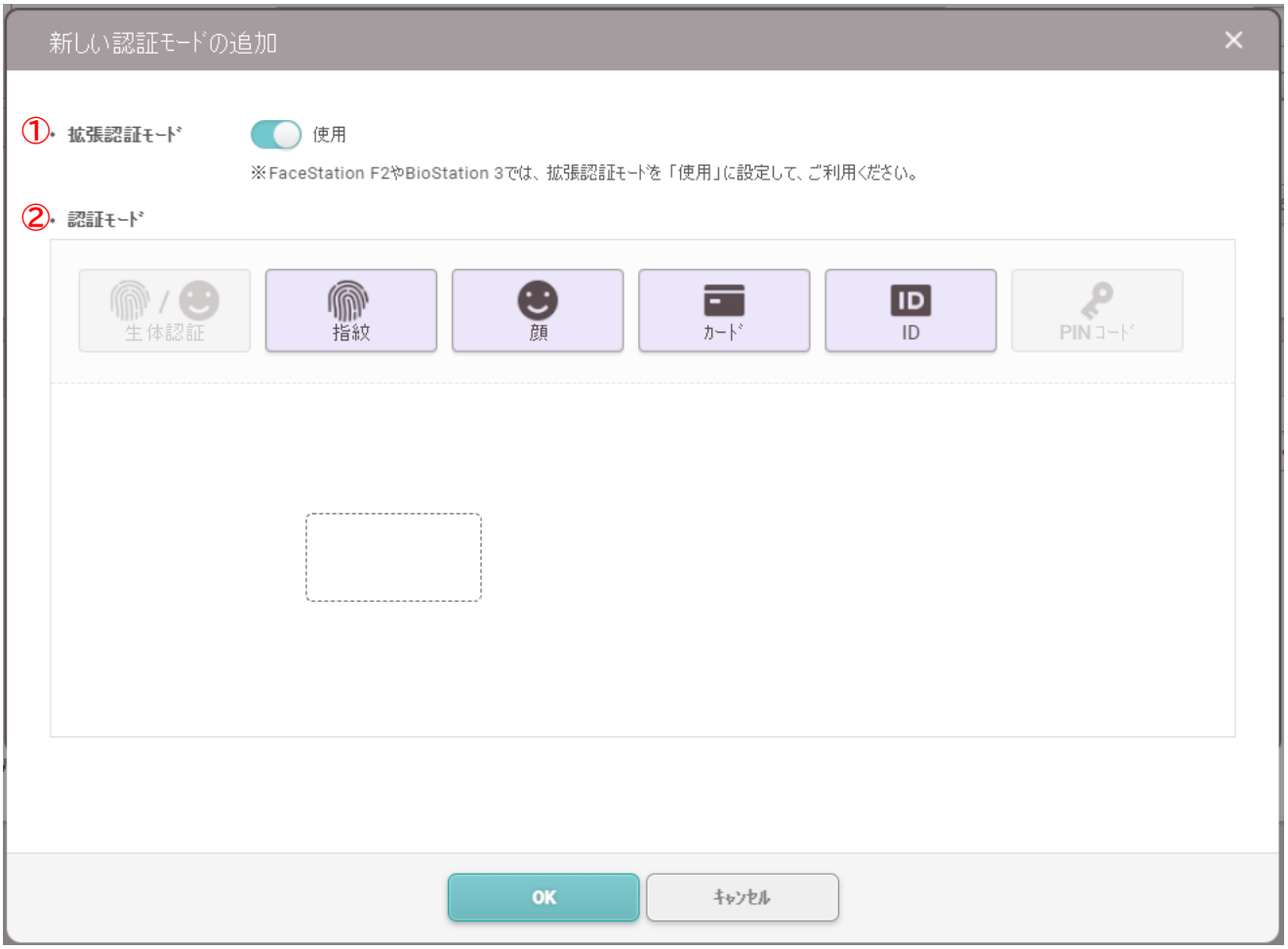
認証モード

ユーザーごとに認証モードを設定できます。

認証モードに[端末標準設定]を選択して、ユーザーが端末の[認証]で構成された認証モードを使用して認証できるようにするか、[個別設定]を選択して、各ユーザーに固有の認証モードの割り当てを行えます。

1 認証モードを[個別設定]に設定します。

2 [+追加]をクリックして、設定を設定します。



項番	項目名	説明
1	拡張認証モード	拡張認証モードを使用するかを設定します。拡張認証モードが[使用]に設定されている場合、顔と指紋の両方を含む認証モードを組み合わせることができます。 **メモ** 拡張認証モードは、FaceStation F2 および BioStation 3 でのみサポートされています。
2	認証モード	使用する認証方法をドラッグアンドドロップします。

3 [適用]をクリックして、認証モードを追加します。

メモ

- [端末の初期値の認証モードを除外]が設定されている場合、BioStar 2 で設定された個別設定の認証モードのみを使用できます。
- [端末の初期値の認証モードを含む]が設定されている場合、端末に設定されている認証モードと BioStar 2 に設定されている個別設定の認証モードの両方を使用します。

指紋登録

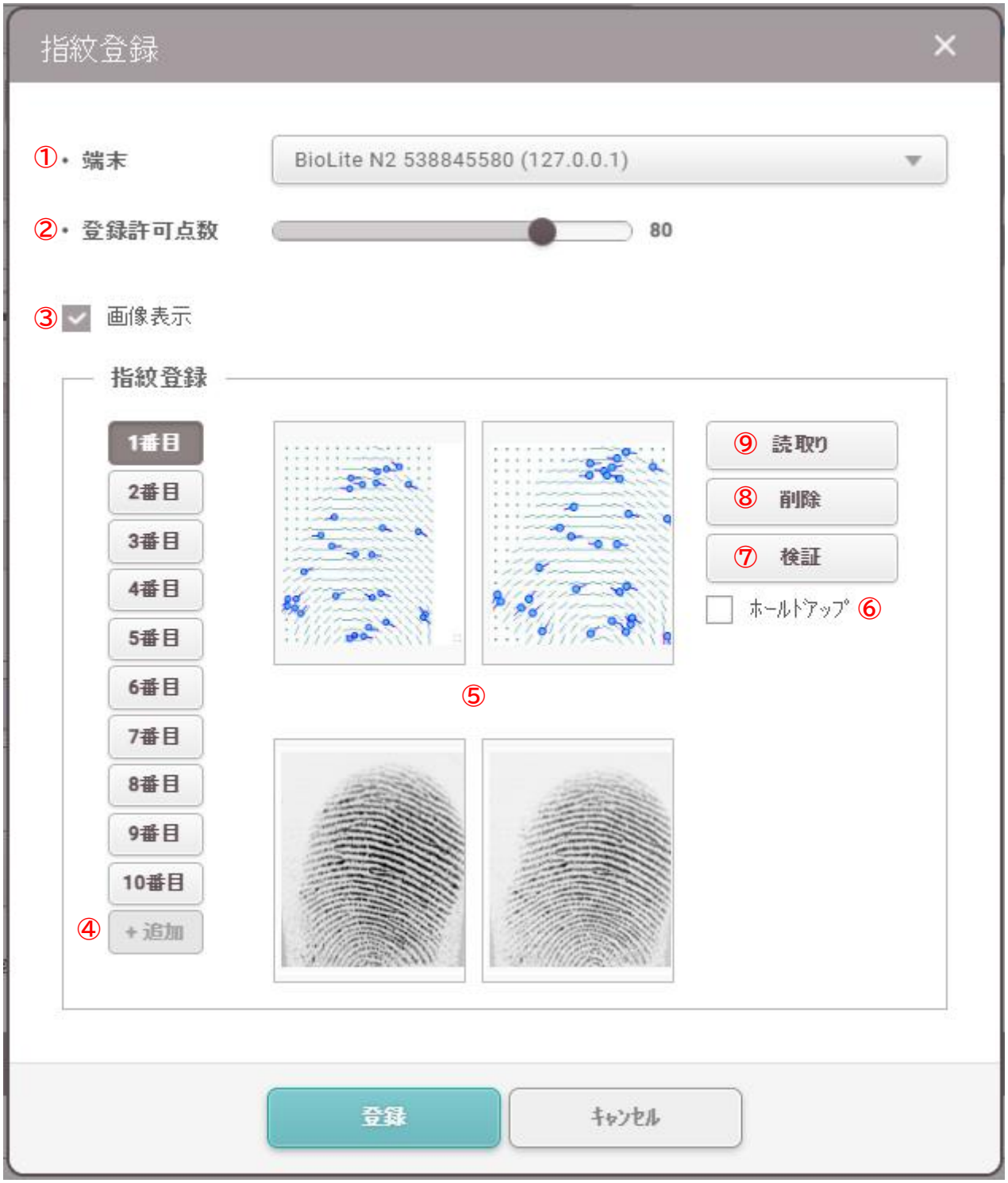
端末が指紋認証をサポートしている場合は、ユーザーの指紋情報の追加を行えます。

指紋は、USB 指紋スキャナーを使用するか、指紋認証機が設置されている場所でスキャンすることにより登録を行えます。

メモ

- 指紋登録するユーザーの指が清潔で乾燥していることを確認してください。
- 傷がある指や指紋が薄い指を追加しないでください。

1 [+指紋]をクリックして、設定を設定します。



項番	項目名	説明
1	端末	指紋を登録する端末を選択します。
2	登録許可点数	指紋登録の品質レベルを選択します。品質要件を満たさない指紋は登録されません。
3	画像表示	指紋をスキャンしたときに元の画像を表示するには、このオプションを選択します。
4	指紋登録	**[+追加]**をクリックして指紋を追加します。最大 10 個の指紋の追加を行えます。
5	指紋画像	登録された指紋がプレビューされます。

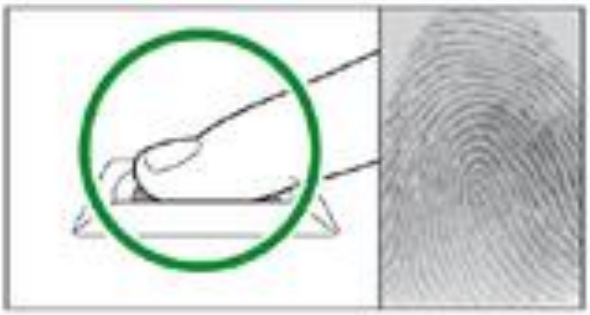
6	ホールドアップ	登録する指紋をホールドアップ指紋として追加するには、このオプションを選択します。 誰かにドアを開けるように脅された場合、ユーザーはこの指紋を使用して認証し、BioStar 2 に警報の送信を行えます。
7	検証	サーバーマッチングを使用する場合、指紋が登録済みかどうかを確認することができます。
8	削除	選択した指紋を削除します。
9	読取り	**[読取り]**をクリックし、USB 指紋スキャナーまたは指紋認証機の指紋センサーに指を置きます。

2 [登録]をクリックして指紋を登録します。

3 1:1 セキュリティ レベルを設定し、[適用]をクリックします。

メモ

- 通常の認証に使用される指紋は、ホールドアップ指紋として登録すべきではありません。
- [画像表示]を設定すると、指紋画像を表示しますが、BioStar には保存しません。
- 指紋認証率が低い場合は、既存の指紋情報を削除し、新しい指紋を追加してください。
- 適切なセキュリティレベルを使用します。1:1 セキュリティレベルが高く設定しすぎた場合、指紋認証率が低くなったり、本人拒否率(FRR)が高くなったりする可能性があります。
- 登録指紋の品質を最高に高くするには、指紋センサーの表面全体を指で覆うようにしてください。
  また、人差し指か中指を登録することを推奨します。



顔の登録

端末が顔認証をサポートしている場合は、ユーザーの顔の追加を行えます。

メモ

- 顔を登録するときは、端末と顔の距離を 40cm ～ 80cm 離してください。
- 顔の表情を変えないように注意してください。(笑顔、描き顔、ウインクなど)
- 画面の指示に従わないと、顔登録に時間を要したり、失敗する場合があります。
- 目や眉毛を覆わないように注意してください。
- 帽子、マスク、サングラス、眼鏡は着用しないでください。
- 画面に 2 つの顔が表示されないように注意してください。1 人ずつ登録してください。
- 眼鏡をかけている方は、眼鏡あり・なしの両方の顔を登録することを推奨します。

1 [+顔]をクリックします。

項番	項目名	説明
1	端末	顔を登録する端末を選択します。
2	顔の登録角度レベル	顔登録時の顔の位置、角度、距離の感度を設定します。 詳細な顔テンプレートを取得したい場合は、感度を高く設定してください。
3	顔の登録	**[+追加]**をクリックして顔を追加します。最大 5 つの顔の追加を行えます。
4	顔画像	登録する顔を表示します。
5	プロフィールイメージで使用	プロフィール画像として使用する登録済みの顔を選択します。
6	削除	選択した面を削除します。
7	読取り	**[読取り]**をクリックし、端末画面の指示に従ってスキャンします。

2 [登録]をクリックして、顔を登録します。

3 1:1 セキュリティレベルを設定し、[適用]をクリックします。

メモ

- 顔認証率が低い場合は、既存の顔情報を削除し、新しい顔を追加してください。
- 適切なセキュリティレベルを使用します。1:1 セキュリティレベルが高く設定しすぎた場合、指紋認証率が低くなったり、本人拒否率(FRR)が高くなったりする可能性があります。

ビジュアル顔を登録

ビジュアル顔は、ビジュアルカメラでユーザーの顔をキャプチャする認証資格です。

ビジュアル顔をサポートする端末でのみ登録を行えます。

ビジュアル顔は、ユーザーのモバイル端末を使用して地理的に離れた場所からでも登録を行えます。

メモ

- ビジュアル顔を利用できる端末は以下の通りです。

  FaceStation F2、BioStation 3

- ビジュアル顔を登録する際の注意事項は各端末のユーザーマニュアルを参照してください。

端末から登録

FaceStation F2、または BioStation 3 でビジュアル顔の登録を行えます。

1 [+ビジュアル顔]をクリックします。

項番	項目名	説明
1	端末	ビジュアル顔を登録する端末を選択します。
2	ビジュアル顔 登録	**[+追加]**をクリックしてビジュアル顔を追加します。 最大 2 つのビジュアル顔の追加を行えます。
3	ビジュアル顔イメージ	読み取りまたは写真アップロードされた画像を表示します。 ドラッグ＆ドロップで画像ファイルをアップロードすることもできます。
4	読取り	**[読取り]**をクリックし、デバイス画面の指示に従ってスキャンします。
5	写真アップロード	ビジュアル顔として登録する画像をアップロードします。 **メモ** ・ サポートされている画像ファイルのサイズは最大 10MB です。 ・ サポートされている画像ファイル形式は、JPG、JPEG、および PNG です。
6	削除	選択したビジュアル顔を削除します。
7	プロフィールイメージで使用	プロフィール画像として使用する登録済みの顔を選択します。

2 [登録]をクリックしてビジュアル顔を登録します。

CSV インポートで登録

CSV インポートにより、ユーザーにビジュアルの登録を行えます。

1 [ユーザー]をクリックします。
2 ユーザー一覧からビジュアル顔を登録するユーザーを選択します。
3 CSV エクスポートを参照して、対象ユーザーを選択し CSV ファイルにエクスポートします。
4 CSV ファイルのビジュアル顔列(face_image_file1, face_image_file2)に拡張子を含めたビジュアル顔の画像ファイル名を入力し、保存します。
5 CSV インポートを参照して、ビジュアル顔を追加した CSV ファイルを BioStar 2 にインポートします。
6 [参照]をクリックし、ビジュアル顔の画像が保存されているパスを選択して、[アップロード]をクリックします。

メモ

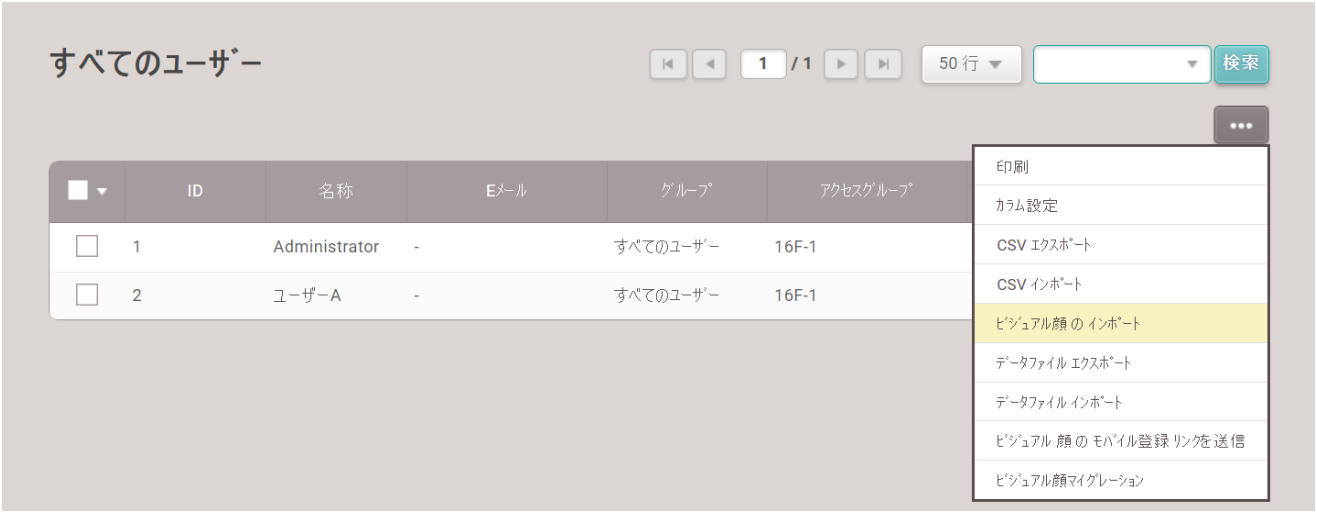
- 読み込む CSV ファイルとビジュアル顔画像ファイルは同じパスを使用することを推奨します。
- サポートされている画像ファイルのサイズは最大 10MB です。
- サポートされている画像ファイル形式は、JPG、JPEG、および PNG です。

7 [次へ]をクリックして、CSV インポートを完了します。
CSV ファイル情報のインポートでエラーが発生した場合、エラー行のみの CSV ファイルをダウンロード、および内容を確認した後、CSV ファイルを修正し再度アップロードを行います。

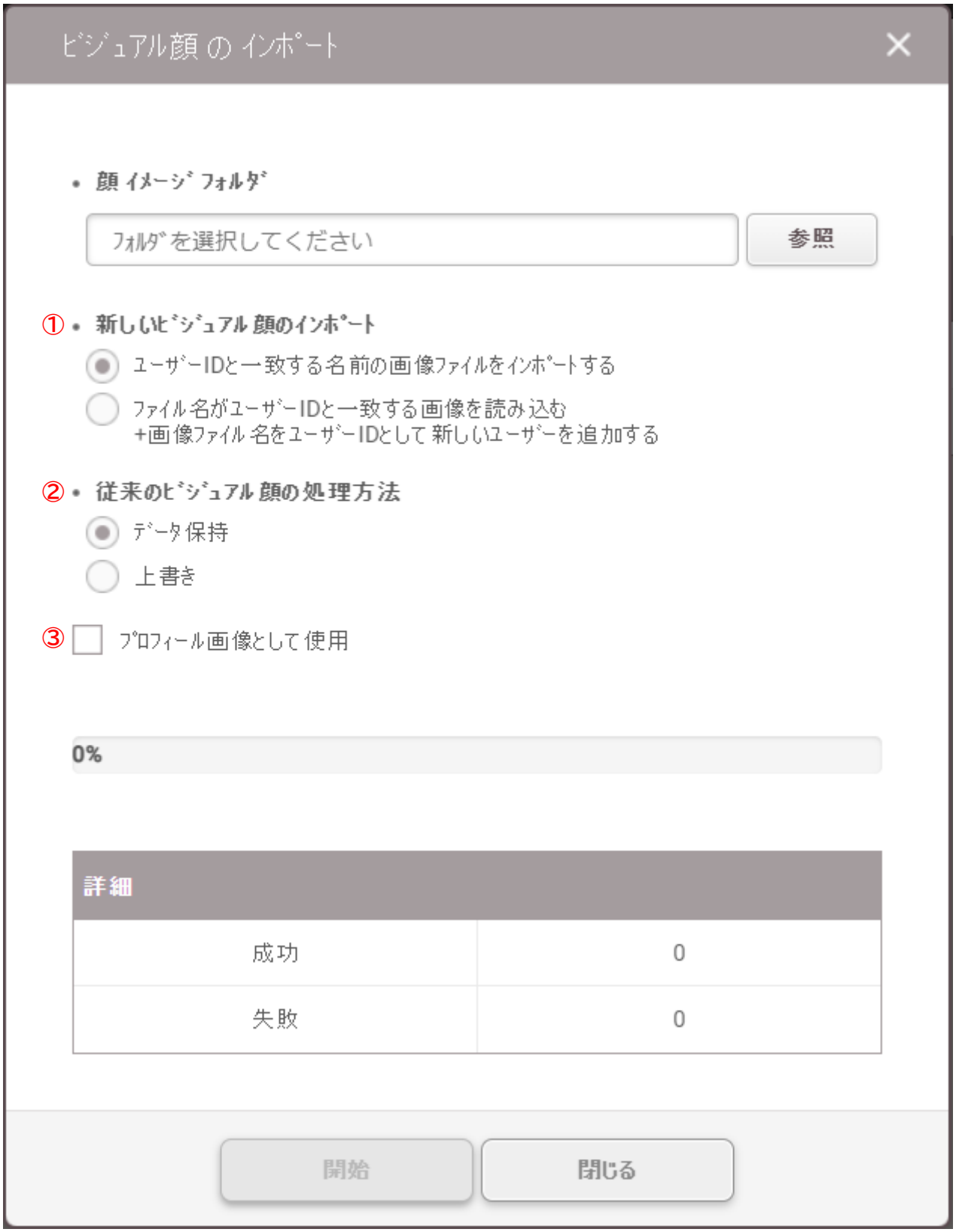
ビジュアル顔インポートで登録

ユーザーID に一致する顔画像ファイルをインポートすることで、ユーザーにビジュアル顔の登録を行えます。

1 [ビジュアル顔のインポート]をクリックします。



2 [参照]をクリックし、顔画像ファイルが保存されているフォルダを選択して、[アップロード]をクリックします。



項番	項目名	説明
1	新しいビジュアルのインポート	・ユーザー ID と一致する名前の画像ファイルをインポートする: BioStar 2 に登録されているユーザー ID とファイル名が一致する場合にのみ画像がインポートされ、一致しないファイルは無視されます。

		・ファイル名がユーザーID と一致する画像を読み込む+画像ファイル名をユーザーID として新しいユーザーを追加する: ファイル名が BioStar 2 に登録されているユーザー ID と一致する場合、画像がインポートされ、一致しないファイル名がある場合は、ファイル名をユーザー ID として使用して新しいユーザーが追加され、ビジュアル顔が登録されます。
2	従来のビジュアル顔の処理方法	・データ保持 : すでに登録されているユーザーの視覚面を維持します。 ・上書き: 新しくインポートされたビジュアル顔を既存のビジュアル顔に上書きします。
3	プロフィール画像として使用	インポートされたビジュアル顔をユーザーのプロフィール画像として使用する場合は、このオプションをオンにします。

3 [開始]をクリックして、ビジュアル顔のインポートを開始します。
画像ファイルのインポート中にエラーが発生した場合、BioStar 2 はインポートに失敗した画像ファイルのリストを返します。どの顔画像ファイルが適切でないかなどの確認を行えます。

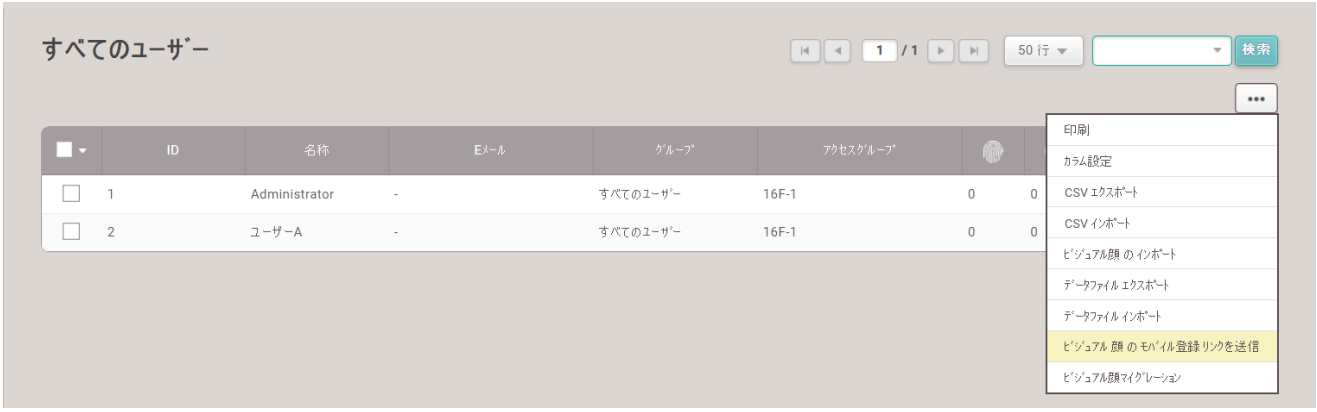
メモ

- サポートされている画像ファイルのサイズは最大 10MB です。
- サポートされている画像ファイル形式は、JPG、JPEG、および PNG です。
- ユーザー ID ごとにインポートできるビジュアル顔は 1 つのみです。

モバイル端末で登録する

ビジュアル顔登録用のモバイル登録リンクをメールでユーザーに送信を行えます。
ユーザーは自分のモバイル端末からリンクにアクセスして、ビジュアル顔を直接登録を行えます。

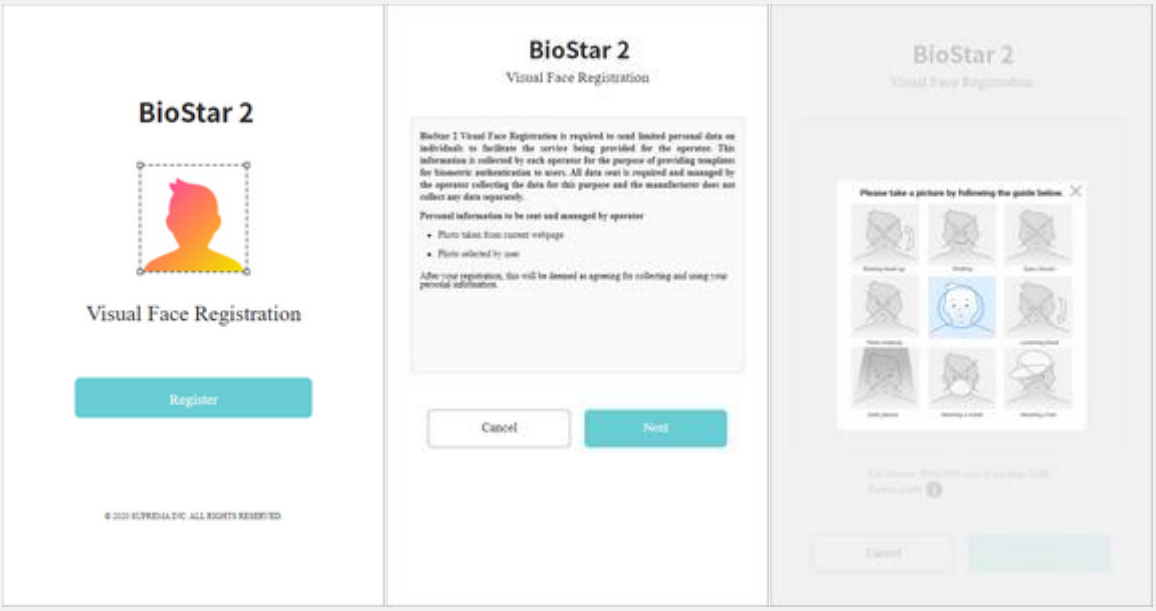
1 ユーザー一覧からビジュアル顔を登録するユーザーを選択し、機能ボタン(•••)をクリックします。

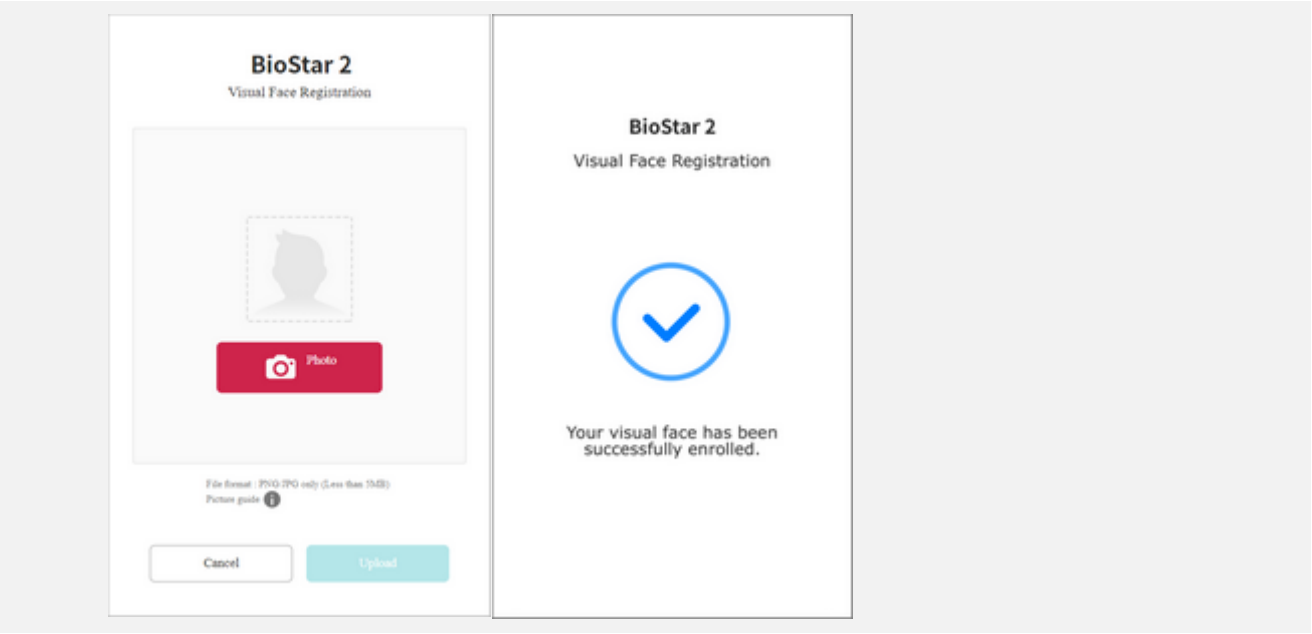


2 [ビジュアル顔モバイル登録リンクを送信]を選択し、ガイドに従って操作すると、ビジュアル顔の登録リンクが、選択したユーザーの電子メールに送信されます。ユーザーがアップロードを完了すると、ビジュアル顔がユーザー情報に登録されます。

メモ

- ビジュアル顔のモバイル登録を使用する前に、SMTP 設定を含む電子メール設定を完了する必要があります。詳細については、メール設定を参照してください。
- メールが正常に送信されたかどうかは、監査記録で確認できます。
  詳細については、監査記録を参照してください。
- ビジュアル顔モバイル登録リンクを受信したユーザーが外部の電子メールアプリケーションを使用している場合、電子メールアプリケーションの言語を自分の国の言語に設定する必要があります。
  言語が Unicode をサポートしていない場合、メールのテキストが破損して表示される可能性があります。
- サポートされている画像ファイルのサイズは最大 10MB です。
- サポートされている画像ファイル形式は、JPG、JPEG、および PNG です。
- 送信されたビジュアル顔登録リンクの有効期限は 24 時間です。
- 顔写真のアップロード後、ビジュアル顔モバイル登録のプロセスが成功すると、画面に登録成功メッセージが表示されます。登録が失敗した場合、失敗メッセージと理由が表示されます。ユーザーは別の顔写真を使用してビジュアル顔登録を再試行してください。
- ユーザーが受信したメールの ビジュアル顔モバイル登録 のリンクをクリックすると、
  ビジュアル顔登録プロセスが以下のように実行されます。画面の指示に従ってビジュアル顔を登録します。





カード登録

ユーザーにカードの割り当てや、既存のカードの管理を行えます。

端末がサポートするカードの種類については、端末の仕様書を参照してください。

- CSN カードの登録
- Wiegand カードの登録
- スマートカード・モバイルカードを登録する

USB 登録機を利用したカード登録の対応表を以下に示します。

カードの種類	CSN	Wiegand	スマートカード
EM	X	X	X
Mifare	○	X	○
DESFire	○	X	○
Felica	○	X	X
HID Prox	X	X	X
HID iCLASS	X	X	X

※○は「対応」、X は「非対応」

CSN カードの登録

CSN カードの登録を行えます。

1 [+カード]をクリックします。

2 カード種別に CSN を選択します。

3 登録方法を選択します。

カードリーダーによる登録

BioStar 2 に接続された端末に物理カードをスキャンすることで、カードを登録する方法です。

A) [登録方法]で[カードリーダーによる登録]を選択します。

B) 端末にカードをスキャンする端末を選択します。

C) [カード読出し]をクリックし、端末でカードをスキャンします。

カード割当

ユーザーに登録済みの未割当カードを割り当てる登録方法です。

A) [登録方法]で[カードの割当]を選択します。

B) 一覧から割り当てるカードをクリックするか、カードを検索します。

手動入力

カード番号を入力して登録する方法です。

A) [登録方法]で[手動入力]を選択します。

B) [ユーザーID を使用]をクリックするか、直接入力します。

4 [登録]をクリックしてカードを登録します。

➢ 関連情報

カード利用状況

カードフォーマット

Wiegand カードの登録

Wiegand カードの登録を行えます。

1 [+カード]をクリックします。

2 カード種別に[Wiegand]を選択します。

3 カードデータ形式を設定します。
目的のカードデータ形式が見当たらない場合は、Wiegand を参照して Wiegand 形式を設定してください。

4 目的の登録方法を選択します。

カードリーダーによる登録

BioStar 2 に接続された端末に物理カードをスキャンすることで、カードを登録する方法です。

A) [登録方法]で[カードリーダーによる登録]を選択します。

B) カードをスキャンする端末を選択します。使用可能な端末が端末一覧の一番上に表示されます。
使用できる端末が見つからない場合は、認証の CSN カードフォーマットを参照してください。

C) [カード読出し]をクリックし、端末でカードをスキャンします。

カード割当

ユーザーに登録済みの未割当カードを割り当てる登録方法です。

A) [登録方法]で[カードの割当]を選択します。

B) 表示された一覧から割り当てるカードを選択します。

メモ

一覧に表示されるカードはカードデータフォーマットの設定されているカードのみです。

手動入力

カード番号を入力して登録する方法です。

A) [登録方法]で[手動入力]を選択します。

B) [ファシリティコード]、[カード ID]を入力します。

5 [登録]をクリックしてカードを登録します。

➢ 関連情報

カード利用状況

カードフォーマット

スマートカード・モバイルカードを登録

アクセスオンカード、または、セキュア資格カードの登録を行えます。

メモ

- モバイルカードを設定するには、[設定] > [サーバー]の[ユーザー/端末管理]タブで[モバイルカードの登録]を有効にします。
- スマートカードまたはモバイル カードを発行するには、正しいカード種別を設定する必要があります。
  カード種別に関する詳細な内容については、スマート/モバイル カードを参照してください。

1 [+カード]をクリックします。

2 [カード種別]で[スマートカード]を選択します。

3 IC カードが使用できる端末を選択します。
スマートカードレイアウトを設定するには、「認証 > カード種別 > スマートカード」を参照してください。

4 カードレイアウトフォーマットを設定します。スマートカードからカードのレイアウトを設定することができます。

5 スマートカードの種類を選択します。

項目名	説明
アクセスオンカード	ユーザー情報(カード ID、PIN、アクセスグループ、有効期限、指紋テンプレート)をカードに保存します。
セキュア資格カード	ユーザー情報(カード ID、PIN、指紋テンプレート)をカードに保存します。 ユーザーの指紋テンプレートと PIN 情報がカードにない場合、認証には使用できません。 認証は、ユーザー情報が端末、または、BioStar 2 に保存されている場合に使用できます。 BioStar 2 でマッチングを行うには、サーバーマッチングを有効にする必要があります。
カスタムスマートカード	サードパーティが発行したスマートカードを登録できます。選択した登録オプションに基づいて登録を続行します。 **メモ** ・ カスタムスマートカード を使用できるデバイスとファームウェアのバージョンは以下のとおりです。 XPass D2 FW 1.7.1 以降 ・ 新しいスマートカード レイアウトを設定するには、スマート/モバイル カードを参照してください。

6 [モバイルカード発行]または[スマートカード書き込み]をクリックすると、カードが登録されます。

メモ

・モバイルカードが発行されている場合は、発行されたカードが BioStar 2 Mobile アプリを通じて有効化された後にのみ使用できます。
・セキュア資格カードのカード ID は直接設定を行えます。
・BioStar 2 に保存されている情報は、スマートカードに保存されるユーザー情報に使用されます。
新しいユーザー情報が保存されていない場合、誤ったユーザー情報が IC カードに保存される可能性があります。
また、変更したユーザー情報が端末と同期していない場合、機器で認証できない場合があります。

➢ 関連情報

カード利用状況

カードフォーマット

スマートカードの読み取り/フォーマット

IC カードのデータフォーマットや、カードへの情報書き込みを行えます。

1 [+ カード]をクリックします。

2 [カード種別]で[カード読出し]を選択します。

3 スマートカードを読み取ることが可能な端末を選択します。

端末の一覧は、スマートカードレイアウトが設定されている場合にのみ表示されます。

設定については、「認証 > カード種別 > スマートカードレイアウト」を参照してください。

4 スマートカードの種類を選択します。

5 [カード読出し]をクリックします。

6 カード情報を確認し、フォーマットする場合は、[フォーマットカード]をクリックします。

➢ 関連情報

カード利用状況

カードフォーマット

モバイルアクセスカードの登録

モバイルアクセスを Suprema Airfob ポータルと組み合わせて使用する場合、ユーザーにモバイルアクセスの割り当てを行えます。

モバイルアクセスカードは、各ユーザーを個別に登録することも、CSV インポートを介して一度に複数のユーザーを登録することも可能です。

Airfob ポータルで設定したモバイルアクセスカードの発行方法によっては、ユーザーのメールアドレスまたは電話番号を入力する必要があります。

メモ

Suprema Airfob ポータルとモバイルアクセスの使用の詳細については、モバイルアクセスを参照してください。

➢ 関連情報

CSN モバイルカードの登録

テンプレートオンモバイルの登録

CSN モバイルアクセスカードをユーザーに発行します。

1 [+モバイル]をクリックします。

2 希望の登録オプションを選択します。

カードの割当

ユーザーに登録済みの未割当カードを割り当てる登録方法です。

A) [登録方法]で[カードの割当]を選択します。

B) 表示される一覧から割り当てるカードをクリックするか、カードを検索します。

C) 情報欄の設定と有効期限を設定したら、登録をクリックします。

メモ

・ユーザーの写真、部門、役職をユーザー情報に設定すると、該当する情報をユーザーのモバイルアクセスカードに表示することが可能です。モバイルアクセスカードに表示する項目を有効にします。

・有効期限は、サイトタイプ[ダイナミック]を使用する場合にのみ有効です。
ユーザーのモバイルアクセスカードの有効期限の設定を行えます。

手動入力

CSN モバイルカードは、手動で入力したカード ID またはランダムなカード ID で登録を行えます。

A) [登録方法]で[手動入力]を選択します。

B) 入力種別が[ランダムカード ID を利用]に設定されている場合、カード ID は自動的に生成されます。
[ユーザーID]をクリックして、ユーザーID をカード ID として使用することも可能です。
入力種別が[手動入力]に設定されている場合、カード ID を手動で入力します。

C） 情報欄の設定と有効期限を設定した後、登録をクリックします。

メモ

・重複したカード ID の生成防止のため、[入力種別]は[ランダムカード ID を利用]に設定することを推奨します。
・ユーザーの写真、部門、役職をユーザー情報に設定すると、その情報をユーザーのモバイルアクセスカードに表示できます。モバイルアクセスカードに表示する項目を有効にします。
・有効期限は、サイトタイプ[ダイナミック]を使用する場合にのみ有効です。
ユーザーのモバイルアクセスカードの有効期限を設定できます。

3 [登録]をクリックして、モバイルアクセスカードを登録します。

メモ

・電子メールまたはテキストメッセージで送信されたアクティベーションコードを紛失または削除した場合は、[再発行]をクリックしてアクティベーションコードを再発行できます。
ただし、Airfob ポータルでアクティベートされたモバイルアクセスカードは再発行できません。

種別	ｶｰﾄﾞﾃﾞｰﾀ形式	概要	
ﾓﾊﾞｲﾙCSN	ﾓﾊﾞｲﾙ ｱｸｾｽ ｶｰﾄﾞ	ID: 169285617343549 (Period: 2023/08/25 20:16 ~ 2023/08/26 20:16)	再発行 無効化

➢ 関連情報

ユーザー情報の追加

モバイルアクセス

テンプレートオンモバイルの登録

テンプレートオンモバイルは、ユーザーの生体認証テンプレートを保存できるモバイルアクセスカードです。

生体認証情報は BioStar 2 サーバー、Airfob ポータル、端末に保存されていなくても、生体認証を使用できます。

テンプレートオンモバイルは、生体認証を資格情報として使用したいが、プライバシー上の懸念によりサーバーや端末に生体認証情報を保存できない環境で役立ちます。

メモ

- テンプレートオンモバイルをサポートする端末とファームウェアのバージョンは次のとおりです。
  - BioStation 3 FW 1.2.0 以降
- Suprema Airfob ポータルとモバイルアクセスの使用の詳細については、「モバイルアクセス」を参照してください。
- モバイルアクセスカードは、CSN モバイルカードまたはテンプレートオンモバイルのいずれかのみを使用できます。
- モバイルではユーザーごとに 1 つのテンプレートのみを発行できます。

1 [+ モバイル]をクリックします。

2 テンプレートオンモバイルのテンプレートとしてカード種別を選択します。

3 スマートカード種別を選択します。

- アクセスオンカード: ユーザー情報（カード ID、PIN、アクセス グループ、期間、プライベート認証モード）をカードに保存できます。
- セキュア資格カード: ユーザー情報（カード ID、PIN）をカードに保存できます。BioStar 2 に保存されているユーザー情報を使用するには、サーバーマッチングを有効にする必要があります。

4 情報と有効期間を設定したら、「登録」をクリックします。

メモ

- ユーザー情報にユーザーの写真、所属、役職を設定すると、モバイルアクセスカードに該当の情報を表示できます。モバイルアクセスカードに表示される項目を有効にします。
- 有効期限は、サイト種別「ダイナミック」を使用する場合にのみ有効です。ユーザーのモバイルアクセスカードの有効期限と使用期間を設定できます。

- 登録ユーザーのメールアドレスに発行メールが送信されます。利用するには、メール内のリンクから Airfob Pass アプリをインストールし、スマートフォンでテンプレートオンモバイルを発行する必要があります。

5 発行されたスマートフォンを端末にかざし、画面上の指示に従ってテンプレートオンモバイルにビジュアル顔を登録します。

メモ

- テンプレートオンモバイルの認証方法
  スマートフォンを端末にかざし、その後、指示に従って顔を認証します。

➢ 関連情報

ユーザー情報の追加

モバイルアクセス

QR/バーコードの登録

QR/バーコードを認証手段として使用することが可能です。

メモ

- QR/バーコードをスキャナーで読み取り可能な端末は以下です。
  X-Station 2 (XS2-QDPB、XS2-QAPB)
- QR/バーコードをカメラで読み取り可能な端末は以下です。
  X-Station 2 (XS2-ODPB、XS2-OAPB、XS2-DPB、XS2-APB) ファームウェア 1.2.0 以降
  BioStation 3 (BS3-DB、BS3-APWB) ファームウェア 1.1.0 以降
- [カメラによる QR/バーコードの使用]を使用するには、別途端末ライセンスが必要です。
  詳細については、端末ライセンスを参照してください。

1 [+QR/バーコード]をクリックします。
2 QR/バーコード種別を選択します。

BioStar 2 QR

BioStar 2 QR とは、BioStar 2 で暗号化された PIN を含む QR コードのことです。

BioStar2 で QR コードの発行を行えます。

ユーザー情報に登録したメールアドレスに QR コード付きのメールが送信されます。

メモ

- BioStar 2 QR を使用する前に、SMTP 設定を含む電子メール設定を完了してください。
  詳細については、メール設定を参照してください。
- BioStar 2 QR を発行するには、ユーザー情報にユーザーのメールアドレスが登録されている必要があります。

A) [QR/バーコード]で BioStar 2 QR を選択します。

B) 情報欄で発行するカードの詳細を設定します。入力種別を[ランダムカード ID を利用]に設定すると、カード ID が自動的に生成されます。
入力種別を[手動入力]に設定する場合、カード ID を手動で入力する必要があります。

メモ

- 重複したカード ID の生成防止のため、入力種別を[ランダムカード ID を利用]に設定することを推奨します。

QR/バーコード

QR/バーコードとは、3rd パーティのシステムから発行された QR/バーコードのことです。

A) [QR/バーコード]で[QR/バーコード]を選択します。

B) [登録方法]で[手動入力]を選択します。

C) カード ID を手動で入力します。

メモ

・ 英数字、または、特殊文字を含む最大 32 文字のカード ID を入力することが可能です。

3 [登録]をクリックして、QR/バーコードを登録します。

生体認証情報の同期

生体認証資格情報を端末に再送信を行えます。

メモ

[設定] > [サーバー] > [ユーザー/デバイスの管理]で[ユーザー自動同期]が[未使用]に設定されている場合、本機能は使用できません。

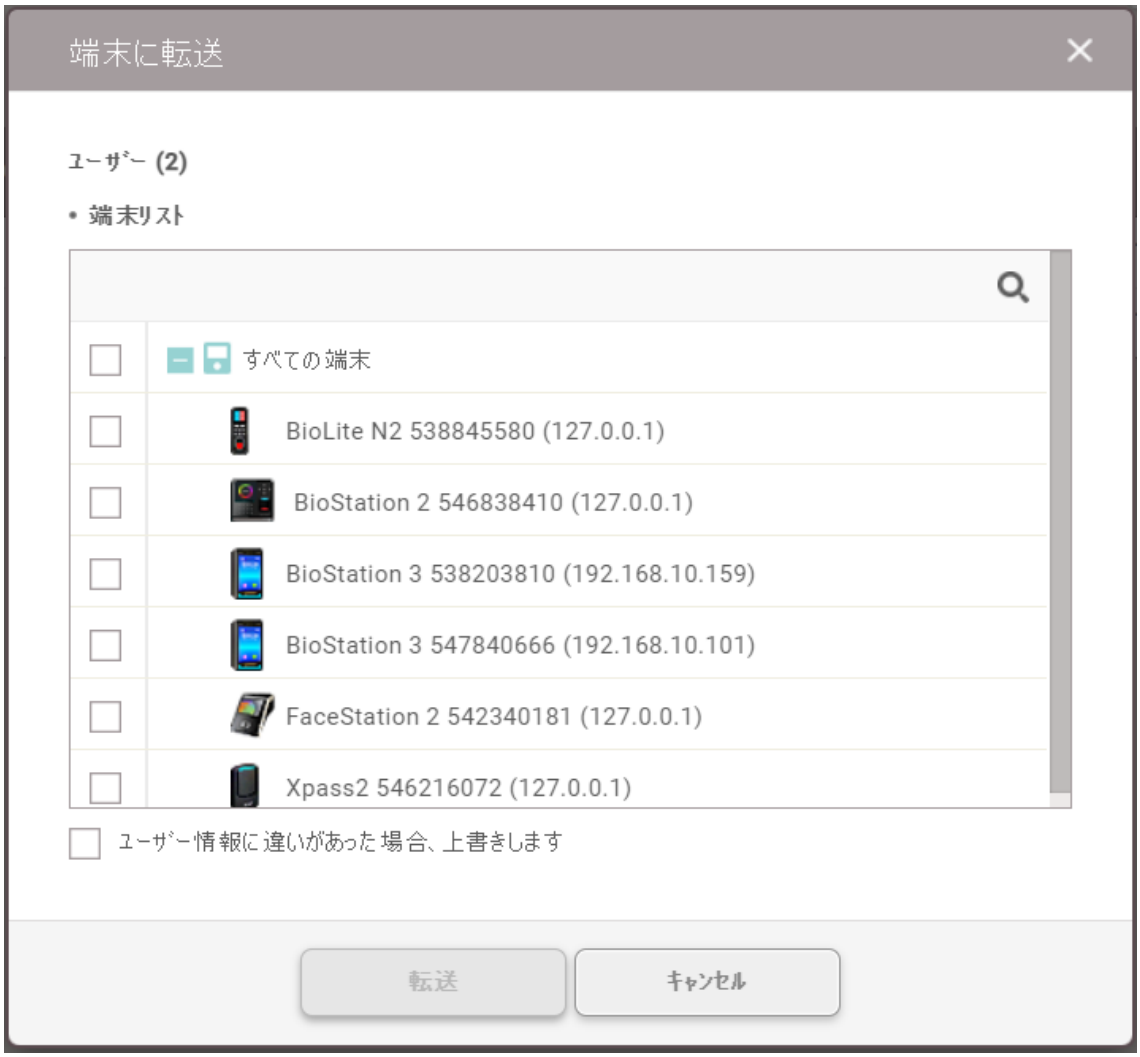
1 [同期]をクリックします。

種別	ｶｰﾄﾞﾃﾞｰﾀ形式	概要	
ﾋﾞｼﾞｭｱﾙ 顔	-	1	同期

ユーザー情報を端末に転送する

BioStar 2 に登録されているユーザー情報を端末に転送を行えます。

1 転送するユーザーを選択し、[端末に転送]をクリックします。



2 重複するユーザー情報を上書きするには、[ユーザー情報に違いがあった場合、上書きします]を選択します。

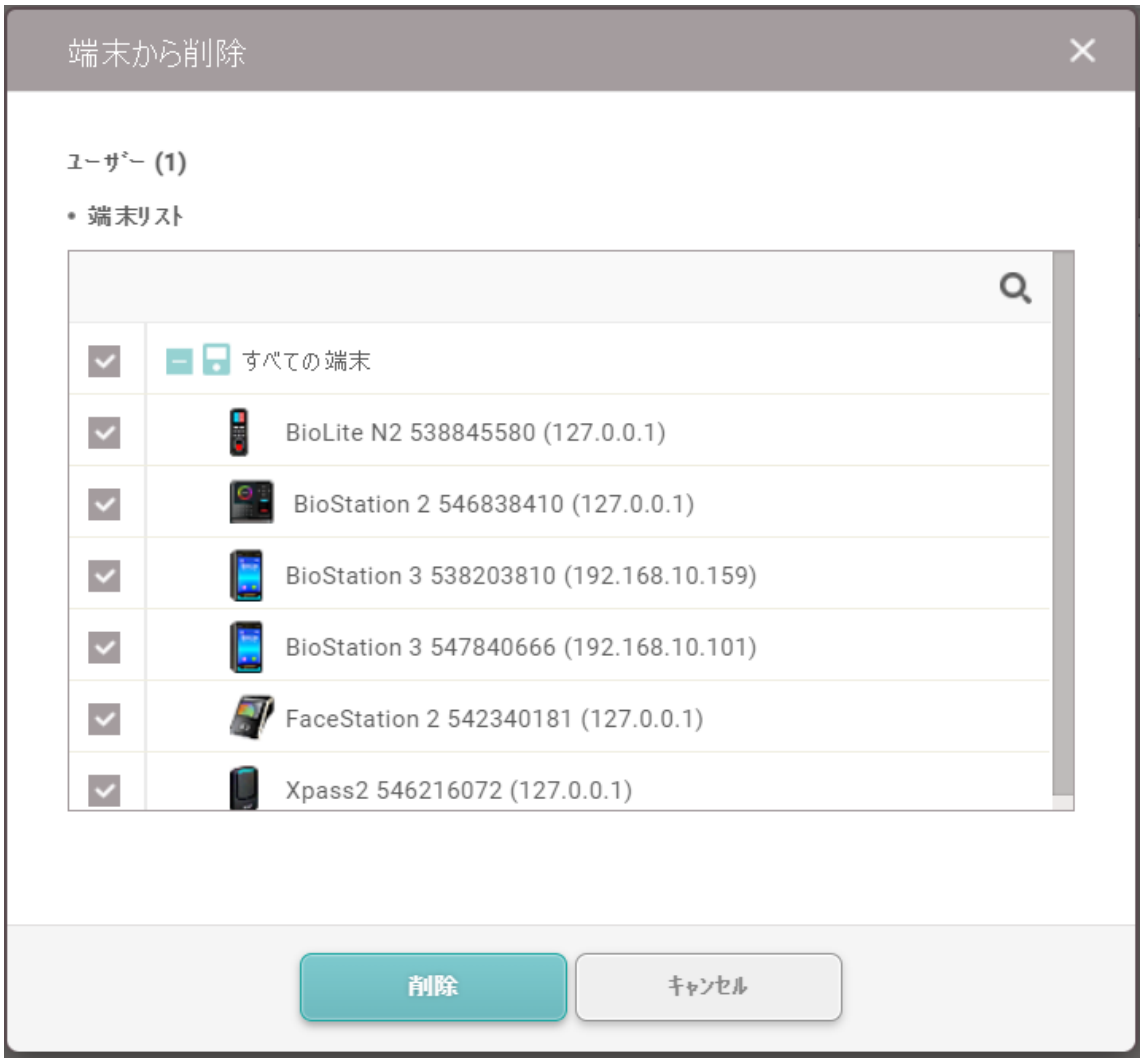
3 情報を転送する端末を選択します。検索ボタン(🔍)をクリックして端末を検索します。

4 [転送]をクリックして、ユーザー情報を端末に転送します。

端末からユーザー削除

端末からユーザーの削除を行えます。

1 端末から削除するユーザーを選択し、[端末から削除]をクリックします。



メモ

・[端末から削除]ボタンは、[自動ユーザー同期]が[未使用]に設定されている場合にのみ有効になります。
自動ユーザー同期の詳細については、ユーザー/端末管理を参照してください。

2 ユーザーを削除する端末を選択します。検索ボタン(🔍)をクリックして端末を検索します。

3 [削除]をクリックしてユーザーを削除します。

メモ

ユーザーを削除すると、端末からのみ削除され、BioStar 2 のユーザーはそのまま残ります。

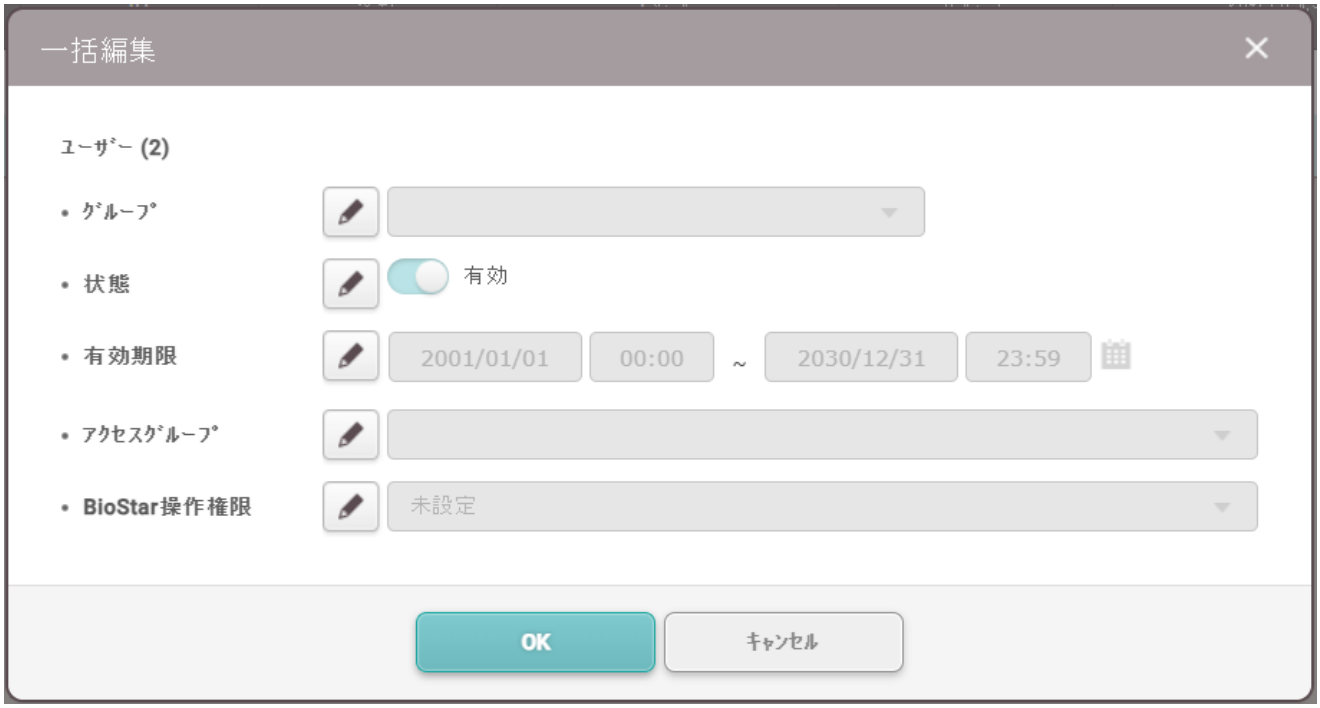
ユーザー情報の編集

既存のユーザーを編集するか、複数のユーザーを一括編集できます。

1 ユーザー一覧で、編集するユーザーをクリックします。

2 ユーザー情報の追加、ユーザー資格情報の追加、および登録カードの手順を参照して、詳細を編集します。

3 複数のユーザーの情報を一括編集するには、複数のユーザーを選択して[一括編集]をクリックします。



4 目的の設定項目のえんぴつマーク(✎)をクリックして、情報を編集します。

5 [OK]をクリックして変更を保存します。

メモ

BioStar 操作権限は「管理者」に変更できません。

長期未使用ユーザーの管理

最近のログから入退室の履歴が無いユーザーの表示、編集、削除を行えます。

1. [状態]タブをクリックします。
2. 表示する期間を設定します。1 ヶ月から 6 か月以上未使用から選択可能です。
3. 表示されたユーザー一覧のヘッダーにフィルターを設定することで、結果の絞り込みを行えます。
4. 複数のユーザーを削除する場合は、複数のユーザーを選択した後、[ユーザーの削除]をクリックします。

メモ

[ユーザーの削除]メニューを使用できるのは、管理者またはユーザーオペレーターの BioStar 操作権限を持つユーザーのみです。BioStar 操作権限の詳細については、ユーザー情報の追加を参照してください。

ビジュアル顔マイグレーション

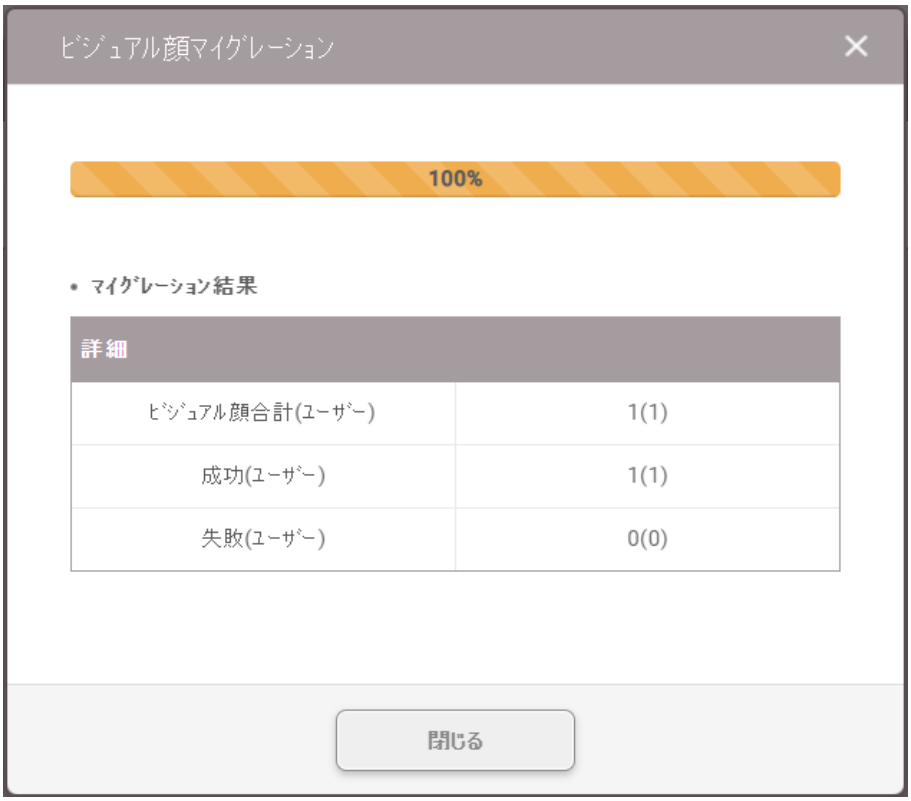
BioStar2 に登録されているすべてのビジュアル顔を、以前のバージョンから改善されたビジュアル顔アルゴリズムに適した顔データにマイグレーションします。

1 [ユーザー]をクリックします。

2 機能ボタン(•••)をクリックして、[ビジュアル顔マイグレーション]を選択します。

3 警告ポップアップメッセージを読んだ後、[続行]をクリックすると、ビジュアル顔マイグレーションプロセスが開始されます。

4 ビジュアル顔マイグレーションが完了すると、結果のポップアップが表示されます。
BioStar 2 に登録されているビジュアル顔の総数と、移行に成功したビジュアル顔と移行に失敗したビジュアル顔の数の確認を行えます。



5 マイグレーションエラーが発生した場合、マイグレーションに失敗したユーザーのリストが CSV ファイルとしてダウンロード可能です。[削除]をクリックすると、マイグレーションに失敗したビジュアル顔の一括削除を行えます。

13 ゾーン

ゾーンメニューでは、基本的な入退室の拡張機能として、以下のゾーンの設定および管理を行えます。

メモ

AC ライセンスのアドバンスド以上のライセンスを有効にすると表示されます。

- アンチパスバックゾーン
- 火災警報ゾーン
- スケジュールロックゾーン
- スケジュールアンロックゾーン
- 警備警報ゾーン
- インターロックゾーン
- 入退確認ゾーン
- 混雑制限ゾーン

1	ゾーンの追加	5	ゾーン一覧
2	ページナビゲーションボタンとリストの行数	6	ゾーン種別
3	検索	7	展開ボタン
4	機能ボタン(カラム設定)		

アンチパスバックゾーン

アンチパスバックゾーンは、ドアベースのアンチパスバック機能よりも強化された機能を提供します。

1 [ゾーン]をクリックし、[ゾーンの追加]をクリックします。

2 [アンチパスバック]をクリックし、[適用]をクリックします。

項番	項目名	説明
1	情報	アンチパスバックゾーンの情報を変更します。
1-A	名称	アンチパスバック名を入力します。
1-B	種別	ゾーンタイプを表示します。
2	設定	アンチパスバックのゾーン設定を変更します。

2-A	モード	ゾーンの適用範囲をローカルまたはグローバルに設定できます。 ローカルは、入室端末と RS-485 で接続されたスレーブ端末のみでゾーンを構成します。 グローバルは、BioStar 2 に登録されているすべての端末でゾーンを構成します。
2-B	有効/無効	アンチパスバックゾーンの有効と無効の切り替えを行えます。
2-C	APB タイプ	アンチパスバックのタイプを選択します。
2-D	APB 解除時間	パスバック違反をリセットするまでの待機時間を設定できます。 ユーザーは待機時間経過後に認証可能になります。最長 7 日間(10080 分)に設定できます。 0 に設定すると、アンチパスバックの違反状態は無期限でリセットされず、違反状態を解除するまで認証できません。
2-E	通行確認 APB	アンチパスバックを適用する範囲を設定できます。Entry Confirmed APB が ON に設定されている場合、アンチパスバックは、入退室デバイスが構成されているドアの実際の操作に従って適用されます。このオプションを OFF に設定すると、ドアの操作に関係なく、ユーザーの認証に従ってルールが適用されます。[ドアの構成に従う]に設定すると、アンチ パスバック ルールは、ドアの［入室確認 APB が有効な場合にセンサーを使用]オプションの設定に従って適用されます。
2-F	入室端末	入室に使用する端末を選択します。 登録済みの端末の一覧から入室端末を選択できます。 目的の端末が表示されない場合は、基本的な検索と登録、指定端末検索と登録、Wiegand 端末の検索と登録、またはスレーブ端末の検索と登録を参照してください。
2-G	退室端末	退室に使用する端末を選択します。 登録済みの端末の一覧から退室端末を選択できます。 目的の端末が表示されない場合は、基本的な検索と登録、指定端末検索と登録、Wiegand 端末の検索と登録、またはスレーブ端末の検索と登録を参照してください。
2-H	ネットワーク失敗アクション	BioStar 2 とアンチパスバックが設定されている端末間の通信が失われた場合の施解錠に関する操作の設定を行えます。 モードがグローバルの時に設定する項目です。 ・ [認証資格により解錠]は、ユーザー照合成功し、アクセス権限が有る場合、解錠します。 ・ [APB ログを記録し、認証資格により解錠]は、ユーザー照合成功し、アクセス権限が有る場合、解錠します。ただし、アンチパスバック違反イベントは発生します。 ・ [APB ログを記録し、ドアは施錠]は、アンチパスバック違反警報が発生し、解錠しません。
3	警報	APB 違反が発生したときにトリガーする動作を設定します。
4	APB バイパス	APB バイパスするアクセスグループを選択します。 設定したアクセスグループに属するユーザーは、アンチパスバックルールの適用対象外となります。

3 [適用]をクリックして設定を保存します。

➢ 関連情報

アンチパスバック

火災警報ゾーン

火災警報ゾーンを設定します。

1 [ゾーン]をクリックし、[ゾーンの追加]をクリックします。

2 [火災警報ゾーン]をクリックし、[適用]をクリックします。

項番	項目名	説明
1	情報	火災警報ゾーンの情報を修正します。
1-A	名前	火災警報ゾーン名を入力します。
1-B	種別	ゾーン種別を表示します。
2	設定	火災警報ゾーンのゾーン設定を変更します。 **メモ** ・モードがローカルに設定されている場合、ドアとエレベーターのいずれかを火災警報ゾーンとして設定できます。 ・モードがグローバルに設定されている場合、ドアとエレベーターの両方を同時に火災警報ゾーンとして設定できます。
2-A	モード	2 つの異なるモードで火災警報を設定できます。 ローカルモードでは、RS-485 経由で接続されているマスター端末とスレーブ端末を選択できま

		す。 グローバルモードでは、BioStar 2 に追加されたすべての端末を選択できます。
2-B	有効/無効	火災警報ゾーンの有効/無効の切り替えが行えます。
2-C	ドア	火災報知ゾーンに含めるドアを選択します。
2-D	エレベーター	火災警報ゾーンに含めるエレベーターを選択します。 複数のエレベーターを選択できます。
2-E	端末/入力	[+追加]をクリックし、デバイスを構成して火災報知信号を鳴らします。
3	警報	火災警報信号発生時の動作を選択します。

3 [適用]をクリックして設定を保存します。

スケジュールロックゾーン

スケジュールロックゾーンは、設定したスケジュールに基づいてドアを施錠します。

メモ

スケジュールロックゾーンは、ローカルモードのみをサポートします。

1 [ゾーン]をクリックし、[ゾーンの追加]をクリックします。

2 [スケジュールロックゾーン]をクリックし、[適用]をクリックします。

項番	項目名	説明
1	情報	スケジュールロックゾーンの情報を修正します。
1-A	名称	スケジュールロックゾーンの名前を入力します。
1-B	種別	ゾーン種別が表示されます。
2	設定	スケジュールされたロックのゾーン設定を変更します。 **メモ** ローカルモードで複数のドアを選択して、スケジュールロックゾーンを設定できます。

2-A	有効/無効	スケジュールロックゾーンの有効/無効の切り替えを行えます。
2-B	ドアロックタイプ	ゾーンを構成して、入室端末のみをロックするか、入室端末と退室端末の両方をロックすることができます。 ・出口ボタン無効: 入室端末のみをロックします。 ・出口ボタン有効:入室端末と退室端末の両方をロックします。
2-C	ドア	スケジュールされたロックゾーンに含めるドアを選択します。
2-D	スケジュール	スケジュールを選択します。 目的のスケジュールが見つからない場合は、[+スケジュールを追加]をクリックして作成します。
3	警報	スケジュールロック信号が発生したときにトリガーされる動作を選択します。
4	スケジュールロックバイパス	スケジュールロックをバイパスするアクセスグループを選択します。 設定したアクセスグループに属するユーザーは、スケジュールロックルールの適用対象外となります。

3 [適用]をクリックして設定を保存します。

スケジュールアンロックゾーン

スケジュールアンロックゾーンは、設定したスケジュールに基づいてドアを解錠します。

メモ

スケジュールアンロックゾーンは、ローカルモードのみをサポートします。

1 [ゾーン]をクリックし、[ゾーンの追加]をクリックします。

2 [スケジュールアンロック]をクリックし、[適用]をクリックします。

項番	項目名	説明
1	情報	スケジュールアンロックゾーンの情報を修正します。
1-A	名称	スケジュールアンロックゾーンの名前を入力します。
1-B	種別	ゾーン種別が表示されます。
2	構成	スケジュールアンロックゾーンの設定を変更します。 **メモ** ・ ローカルモードで複数のドアを選択して、スケジュールアンロックゾーンを設定できます。 ・ 既に別のスケジュールアンロックゾーンが設定されているエレベーターを選択した場合、同じフロアを設定することはできません。
2-A	有効/無効	スケジュールアンロックゾーンの有効/無効の切り替えを行えます。
2-B	ユーザー認証により開始	アクティブに設定されている場合、アクセスグループに属するユーザーは、スケジュールのロック解除を開始するために構成されたスケジュールで認証する必要があります。

2-C	ドア/エレベーター	ドアまたはエレベーターをスケジュールアンロックゾーンとして設定することが可能です。
2-D	スケジュール	スケジュールを選択します。 目的のスケジュールが見つからない場合は、[+スケジュールの追加]をクリックして作成します。
2-E	ドア または エレベーター	ドアを選択すると、ドア一覧が有効になります。 スケジュールアンロックゾーンに含めるドアを選択します。 エレベーターを選択すると、エレベーターリストがアクティブになります。 スケジュールアンロックゾーンに含めるエレベーターを選択します。 複数のエレベーターを選択できます。
	フロア	選択したエレベーターのフロア数を選択できます。
3	スケジュール解錠の認証	スケジュールアンロックを開始できるユーザーが属するアクセスグループを選択します。

3 [適用]をクリックして設定を保存します。

警備警報ゾーン

警備警報ゾーンを使用すると、許可されていないユーザーが指定されたゾーンに無断で侵入することを検出できます。

1 [ゾーン]をクリックし、[ゾーンの追加]をクリックします。

2 [警備警報ゾーン]をクリックし、[適用]をクリックします。

項番	項目名	説明
1	情報	警備警報ゾーンの情報を修正します。
1-A	名称	警備警報ゾーン名を入力します。
1-B	種別	ゾーン タイプを表示します。
2	設定	警備警報ゾーンの一般設定を変更できます。

2-A	モード	ゾーンの適用範囲を確認できます。警備警報ゾーンはローカルモードのみ対応しており、入室機器と RS-485 に接続された機器のみゾーン設定が可能です。
2-B	有効/無効	警備警報 ゾーンを無効にすることができます。アクティブを選択して有効にします。
2-C	ドア	警備警報ゾーンに含めるドアを選択します。
3	警備/警備解除設定	警備開始 と 警備解除 の認証設定を追加できます。 **メモ** 設定にて、ドアが設定されている場合にのみ有効化されます。
3-A	遅延時間	警備開始または警備解除の遅延時間を設定できます。 警備は認証から警備までの遅延時間、警備解除は警備検知から警報発生までの遅延時間です。
3-B	警備用カード	警備開始または警備解除の許可を持つカードを追加できます。 警備用カードは 128 枚まで登録できます。
3-C	アクセスグループ	警備開始または警備解除する権限を持つアクセスグループを追加できます。 最大 128 個のアクセスグループを登録できます。
3-D	警備/警備解除設定	端末または入力信号によって警備/警備解除を行えます。 [+追加]をクリックし、各項目を設定します。 ・警備設定の追加(端末) [端末]をクリックして、ドアの入退室端末の中から警備警報ゾーンに割り当てる端末を選択します。[警備タイプ]を選択します。 [入力種別]は、[カード]、[キー]、[カードまたはキー]から選択できます。 ※LCD 画面のない端末の入力タイプは[カード]のみです。 

<table>
<tr><td>4</td><td>警備検知設定</td><td>警備警報信号を設定できます。
[+追加]をクリックして下図のように設定すると、X-Station 2 の入力ポート 0 に接続された N/O センサーが 100(ms)信号を受信した時点で、端末は警備検知と認識します。
・ 入力信号による警備解除の追加
[端末]をクリックして、警備警報ゾーンを制御する端末を選択します。
ポートをクリックし、選択した端末の入力ポートを選択します。
警備タイプを選択し、スイッチと継続時間(ミリ秒)を設定します。
 

メモ
設定にて、ドアが設定されている場合にのみ有効化されます。</td></tr>
<tr><td>5</td><td>警報</td><td>警備警報ゾーンで特定のイベントが発生した場合に実行する警報の動作を設定します。
メモ
設定にて、ドアが設定されている場合にのみ有効化されます。</td></tr>
</table>

インターロックゾーン

インターロックゾーンは、ドアセンサーとリレーの状態によって 2 つ以上のドアの状態を監視し、他のドアが解錠されている場合にドアを開閉できないように制御を行えます。

ユーザーがゾーン内部に留まっている場合はアクセス拒否するなどの設定を行えます。

重要

本機能は弊社でサポート対象外の機能です。

メモ

- インターロックゾーンは、最大 4 つのドアで設定できます。
- インターロックゾーンは、CoreStation に接続された端末でのみドアの設定を行えます。
- インターロックゾーンに設定した端末を別のゾーンに設定することはできません。
- インターロックゾーンに設定したドアは、火災警報ゾーン以外に設定することはできません。

1 [ゾーン]をクリックし、[ゾーンの追加]をクリックします。

2 [インターロックゾーン]をクリックし、[適用]をクリックします。

3 必要な項目を編集します。

項番	項目名	説明
1	情報	インターロックゾーンの情報を修正します。 ・ 名前: インターロックゾーン名を入力します。 ・ 種別: ゾーン タイプを表示します。

2	設定	インターロックゾーンの一般設定を変更できます。 ・ モード: ゾーンの適用範囲を確認できます。インターロックゾーンはローカルモードのみサポートされており、ゾーンは CoreStation と RS-485 に接続された端末でのみ設定できます。 ・ 有効化/無効化: インターロックゾーンの有効/無効の状態の切り替えを行えます。 ・ ドア: インターロックゾーンに含めるドアを選択します。 ドアセンサーが接続されているドアを少なくとも 2 つ選択する必要があります。
3	追加設定	ユーザーがゾーンにとどまる場合、このオプションにより、他のユーザーがゾーンに入るのを防ぐことができます。 メモ 設定からドアが設定されている場合にのみ有効化されます。
4	警報	インターロックゾーンで特定のイベントが発生したときに実行する警報動作を設定します。 メモ 設定からドアが設定されている場合にのみ有効化されます。

4 ［適用］をクリックして設定を保存します。

入退確認ゾーン

入退確認ゾーンは、特定エリアの人数や利用者一覧のモニタリング、特定エリアに長時間滞在した場合に管理者に通知を行えます。

1 [ゾーン]をクリックし、[ゾーンの追加]をクリックします。
2 [入退確認ゾーン]をクリックし、[適用]をクリックします。
3 必要な項目を編集します。

項番	項目名	説明
1	情報	入退確認ゾーンの情報を変更します。
1-A	名称	入退確認ゾーン名を入力します。
1-B	種別	ゾーン種別が表示されます。
2	構成	入退確認ゾーンの一般設定を変更できます。
2-A	モード	ゾーンの適用範囲を確認できます。 入退確認ゾーンではグローバルモードのみがサポートされており、BioStar 2 に追加されたすべての端末でゾーンを設定できます。
2-B	有効/無効	入退確認ゾーンを無効にできます。アクティブを選択して有効にします。
2-C	入室端末	入力に使用する端末を選択します。 追加された端末の一覧から端末を選択できます。

		登録済みの端末が見つからない場合は、基本的な検索と登録、指定端末検索と登録、Wiegand 端末の検索と登録、またはスレーブ端末の検索と登録を参照してください。
2-D	退室端末	退室時に使用する端末を選択します。 追加された端末の一覧から端末を選択できます。 目的の端末が登録されていない場合は、基本的な検索と登録、指定端末検索と登録、Wiegand 端末の検索と登録、またはスレーブ端末の検索と登録を参照してください。
2-E	対象者グループ	入退確認ゾーンに滞在するユーザーが属するアクセスグループを設定します。 最大 16 のアクセスグループを設定できます。
2-F	最大入室継続時間	ユーザーがゾーンに滞在できる最大時間を設定します。 最大 4320 分まで設定可能で、指定時間を超えて入退確認ゾーンに滞在すると警報が発生します。
3	警報	入退確認ゾーンで特定のイベントが発生したときに実行する警報動作を設定します。 **メモ** 設定にて、入室端末と退室端末が設定されている場合にのみ有効化されます。

4 [適用]をクリックして設定を保存します。

混雑制限ゾーン

混雑制限ゾーンは、特定のエリア内部の人数の管理および制御を行えます。

混雑制限ゾーンの状態をモニタリングし、一定の人数に達した時に通知を受け取るなどを行えます。

メモ

- 混雑制限ゾーンは、最大 100 まで追加できます。
- 混雑制限ゾーン機能と互換性のある端末とファームウェアのバージョンは以下です。

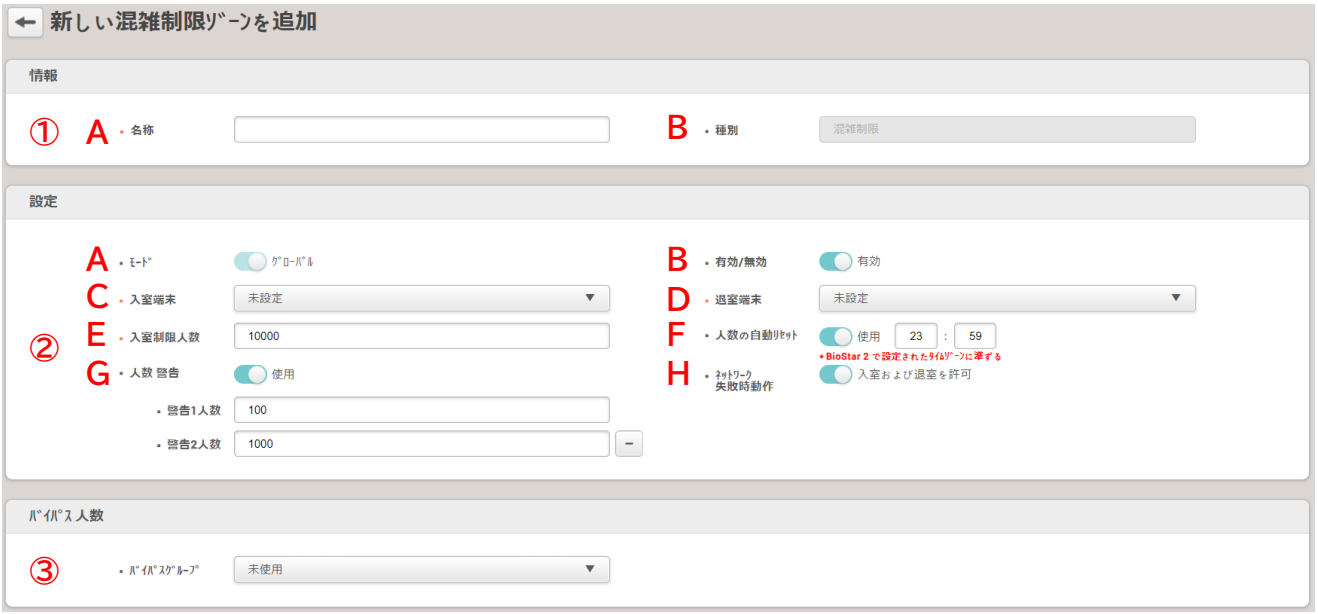
  FaceStation F2 ファームウェア バージョン 1.1.0 以降

  FaceStation 2 ファームウェア バージョン 1.5.0 以降

1 [ゾーン]をクリックし、[ゾーンの追加]をクリックします。

2 [混雑制限ゾーン]をクリックし、[適用]をクリックします。

3 必要な項目を編集します。



項番	項目名	説明
1	情報	混雑制限ゾーンの情報を修正します。
1-A	名称	混雑制限ゾーン名を入力します。 **メモ** ・ 名前は最大 48 文字で、他のゾーンと同じ名前を設定することはできません。
1-B	種別	ゾーン種別が表示されます。
2	設定	混雑制限ゾーンの設定を変更します。

		メモ ・ 端末を入室端末と退室端末に同時に割り当てることはできません。 ・ 入室端末と退室端末を合わせて最大 128 個まで設定できます。 ・ 二重認証を使用する端末は、入室または退室端末として設定できません。 ・ ゾーンは、BioStar2 で設定されたタイムゾーンに基づいて、自動リセットの時刻を設定します。たとえば、タイムゾーンが UTC+9 で 00:00 に設定されている場合、人数は UTC+10 で 01:00 の時点で自動的にリセットされます。 ・ 人数警告に 2 つの警告を設定した時、制限値より小さい数値のみを入力できます。両方の警告の値は異なる必要があります。
2-A	モード	ゾーンのモードが表示されます。 混雑制限ゾーンはグローバルモードのみをサポートします。
2-B	有効/無効	混雑制限ゾーンを有効/無効の切り替えを行えます。 ゾーンが無効にすると、ゾーン内のユーザー数を参照するカウントとカウントのバイパス設定の両方が初期化されます。
2-C	入室端末	入室に使用する端末を選択します。 追加された端末一覧から端末を選択できます。 目的の端末が見つからない場合は、基本的な検索と登録、指定端末検索と登録を参照してください。
2-D	退室端末	退室に使用する端末を選択します。 追加された端末一覧から端末を選択できます。 目的の端末が登録されていない場合は、基本的な検索と登録、指定端末検索と登録を参照してください。
2-E	入室制限人数	ゾーンへの入室を制限するユーザーの人数を入力します。 ゾーン内のユーザー数が制限に達すると、入室が制限されます。 0 から 10,000 までの数字を入力でき、0 に設定すると制限無くゾーン内に入室できます。
2-F	人数の自動リセット	カウントを自動的に初期化する時間を設定します。カウントは毎日設定した時刻に初期化されます。
2-G	人数警告	管理者に警告を設定するか、カウントが混雑制限に達する前にイベントログを保存するように設定します。 人数警告を設定すると、警告 1 の入力フィールドが表示されます。 追加ボタン(+)をクリックして警告 2 を設定します。
2-H	ネットワーク失敗アクション	ゾーンに設定された端末でネットワークエラーが発生した場合に、ユーザーの入退室を許可するかどうかを設定します。 入退室を許可するに設定すると、端末がネットワーク接続を失ったときに入室制限が停止され、ゾーン内の人数カウントが入室制限人数を超えても、ゾーンに入室することができます。
3	バイパス人数	カウントをバイパスするアクセスグループの設定を行えます。 グループ内のユーザーは人数カウントに影響を与えずに自由にゾーンを入退室ができます。

		バイパス人数列には、ゾーン一覧のバイパス人数から人数を確認できます。 **メモ** ・ サーマルカメラを搭載した端末を使用時、サーマルマスクチェックモードを[認証なし確認]に設定している場合、バイパス人数の機能を使用することはできません。 ・ 最大 16 個のバイパスグループを追加できます。

4 [適用]をクリックして設定を保存します。

登録された混雑制限ゾーンの一覧が表示され、現在のゾーンの状況が表示されます。

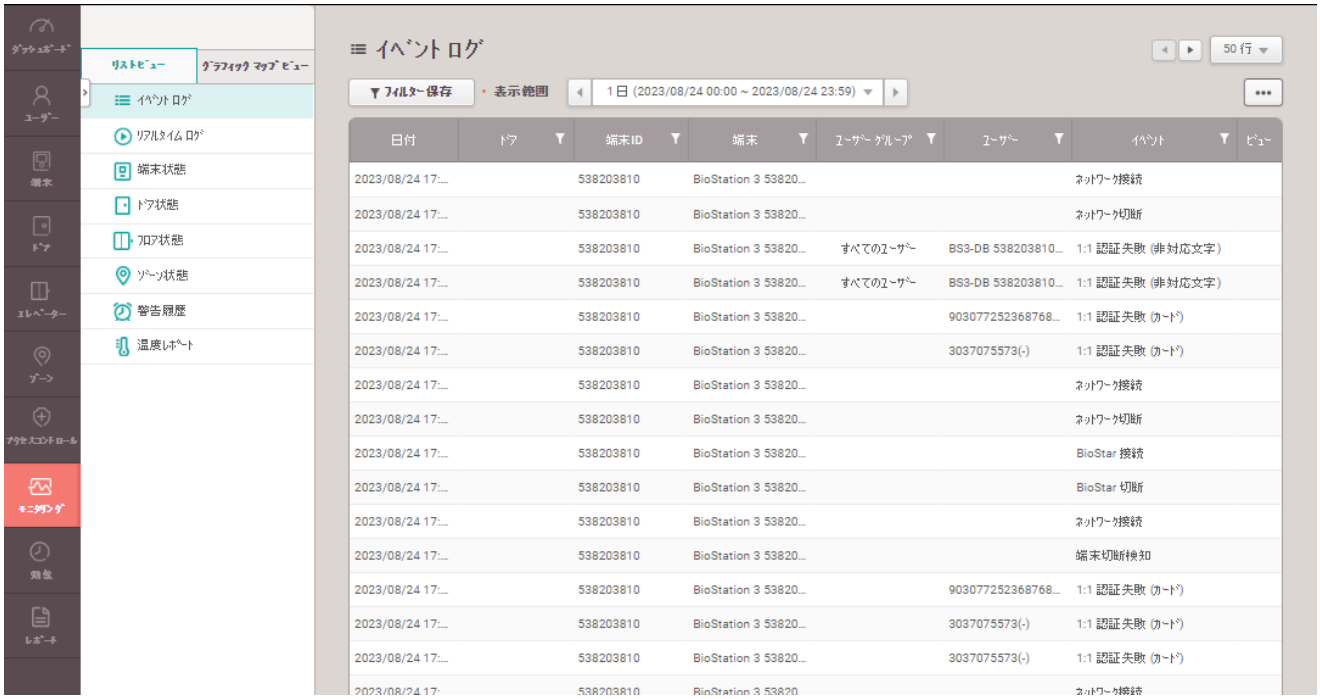
項番	項目名	説明
1	すべて選択	表示されている混雑制限ゾーンをすべて選択します。
2	人数リセット	人数カウントとバイパス人数カウントの両方の状態を初期化します。 初期化後、ユーザーの入退出ログは削除され、ネットワークの状態によってカウントが不正確になる場合があります。
3	ページナビゲーションボタンとリストの行数	ページの移動や 1 ページに表示する行数の設定を行えます。 最初のページに移動します。 前のページに移動します。 2 / 2 移動するページ番号を入力します。 次のページに進みます。 最後のページに移動します。 25 行 1 ページに表示する行数を設定します。
4	有効	無効の状態のゾーンを有効化します。
5	無効	混雑制限ゾーンを無効にします。 ゾーンを無効にすると、人数カウントとバイパス人数カウントが両方とも初期化されます。
6	検索	登録されたゾーンを検索します。
7	削除	ゾーンを削除します。
8	混雑制限ゾーン一覧	登録された混雑制限ゾーンのリストが表示され、現在のゾーンの状況が表示されます。
8-A	名前	ゾーン名を表示します。
8-B	状態	ゾーンの状態を表示します。

		・ 通常: ゾーン内のユーザー数は、事前設定された警告または入室制限人数に達していません。 ・ 人数警告: ゾーン内の人数が警告 1 または警告 2 に達しました。 ・ フル: ゾーン内のユーザー数が入室制限人数に達しました。これ以上の入室は制限されます。
8-C	人数/制限	現在ゾーンにいるユーザーの人数と混雑制限を表示します。 管理者は、[-] または [+] ボタンをクリックするか、[カウント] セクションをクリックした後に値を入力することにより、カウントを直接変更できます。
8-D	バイパス人数	ゾーン内のバイパス人数に属するユーザーの数を表示します。
8-E	端末状態	ゾーンに設定されているデバイスのネットワーク ステータスを表示します。 ・ 正常: ネットワークは正常に動作します。 ・ ネットワーク障害: 1 つまたは複数の端末でネットワーク エラーが発生しています。
8-F	フルスクリーン	フルスクリーンで混雑制限ゾーンの現在の状態を表示します。 **メモ** ・Limit を設定している場合は、50,000 まで入力できます。Limit を設定していない場合は、999,999 まで入力できます。(数字のみ) 最大入力値を超える数値は入力できません。ゾーン内の実際の人数が最大入力値を超える場合、超過した値はデータベースに保存されません。

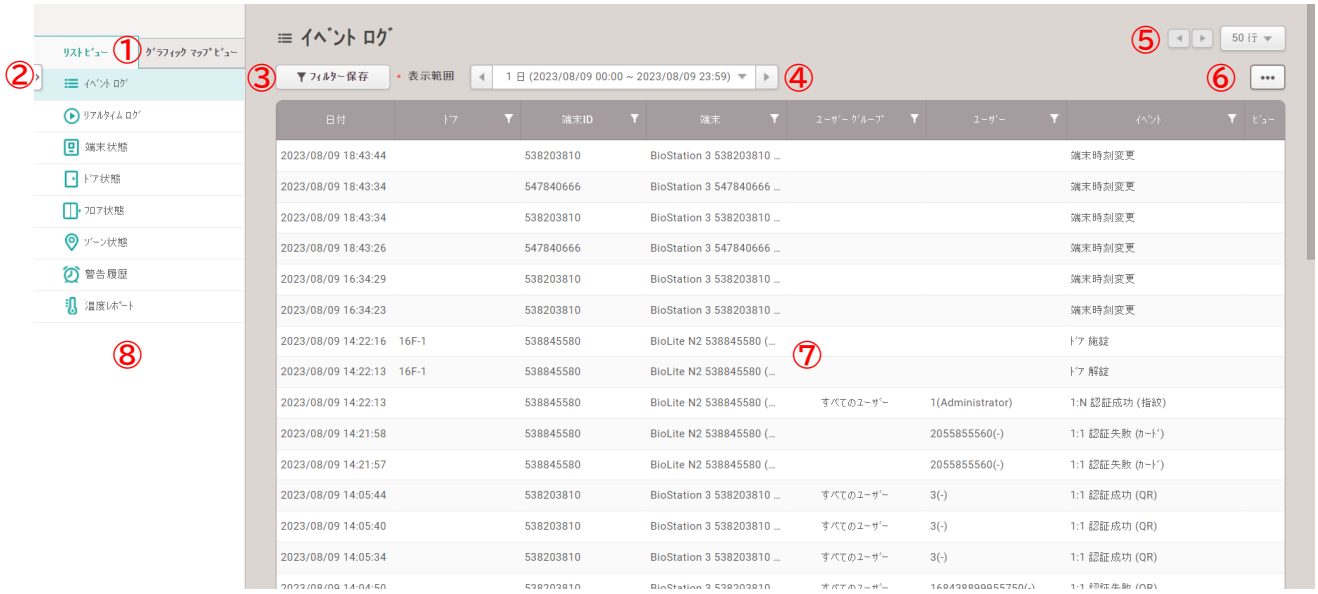
14 モニタリング

モニタリングメニューでは、アクセスコントロールのイベントログ、端末、ドア、ゾーンの状態、警告履歴の確認を行えます。

グラフィックマップを追加すると、ドアの状態をグラフィックかつリアルタイムに表示および制御を行えます。



- リストビュー
- グラフィカルマップビュー



1	リストビューとグラフィックマップビューのタブボタン	5	ページナビゲーションボタンとリストの行数
2	展開ボタン	6	機能ボタン(印刷、CSV エクスポート、データファイルインポート、カラム設定)
3	フィルター保存ボタン	7	モニタリングカテゴリで選択した項目の一覧表
4	イベントログの検索期間	8	モニタリングカテゴリ

メモ

AC ライセンスのスタンダード以上のライセンスを適用した場合のみ、フロア状態、ゾーン状態、グラフィックマップビューが表示されます。

リストビュー

アクセスコントロールのイベントログ、端末、ドア、ゾーンの状態、警告履歴の確認を行えます。

- イベントログ
- リアルタイムログ
- 端末の状態
- ドアの状態
- 無線ドアロック状態
- フロアの状態
- ゾーンの状態
- 警告履歴
- 温度レポート

メモ

AC ライセンスのスタンダード以上のライセンスを適用した場合のみ、フロア状態、ゾーン状態、グラフィックマップビューが表示されます。

イベントログ

過去のすべてのイベントログの表示を行えます。

フィルターの適用や、データのソートを行えます。

メモ

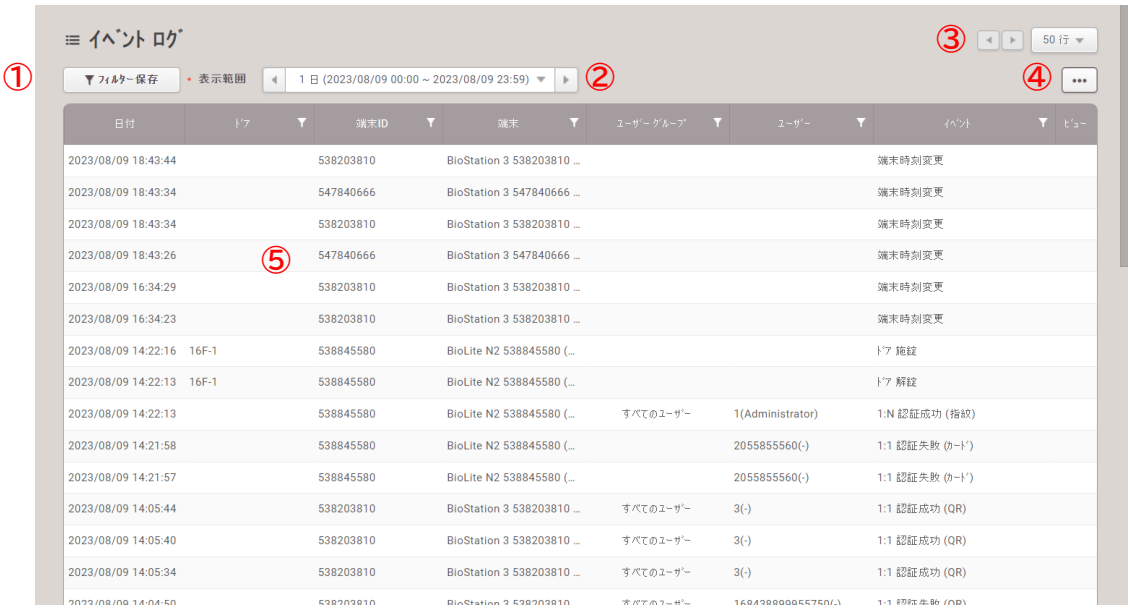
・端末時刻と日付の設定が正しいか確認してください。

端末時刻の設定の詳細については、情報を参照してください。

・イメージログを設定すると、保存した画像を原寸大で閲覧・保存できます。

1 [モニタリング] > [リストビュー] > [イベントログ]をクリックします。

2 フィルタリングした結果のみを表示するには、列のフィルターボタン()をクリックしてフィルターを適用します。



項番	項目名	説明
1	フィルター保存ボタン	設定したフィルターを保存します。
2	表示期間	任意の期間を設定し、イベントログを並べ替えることができます。
3	ページナビゲーションボタンとリストの行数	ページの移動や 1 ページに表示する行数の設定を行えます。 前のページに移動します。 次のページに進みます。 25 行 1 ページに表示する行数を設定します。
4	機能ボタン (印刷、CSV エクスポート、データファイルインポート、カラム設定)	イベントログで追加機能を使用できます。 イベントログを印刷する ・印刷：イベントログを PDF や SVG 形式で印刷 ・CSV エクスポート：CSV ファイルにエクスポート

		・データファイルインポート：データファイルのインポート ・カラム設定：列の表示設定の変更 **メモ** データファイルのインポートの詳細については、「 イベントログのインポート 」を参照してください。
5	イベントログ	イベントログを表示します。 イメージログが存在する場合は、ビューアイコン( )が表示されます。 撮影した画像を PC で原寸大で閲覧・保存することができます。

メモ

・ [ログのアップロード]が[手動]に設定されている場合、ユーザーは[ログ更新]をクリックしてログを手動でインポートできます。ログのアップロード設定を変更する方法については、サーバーを参照してください。

最新のログが設定されている場合、BioStar 2 に最後に保存されたログの日付以降に保存されたログが端末からインポートされ、すべてのログが設定されている場合、端末のすべてのログが BioStar 2 にインポートされます。ログをインポートする日付範囲の設定も行えます。

イベントログのインポート

メモ

- 古いファームウェアバージョンを使用している端末からエクスポートされたデータファイルは、BioStar 2 にインポートできません。常に最新バージョンのファームウェアを使用してください。
- FacaStation F2、FaceStation 2、FaceLite、BioStation A2、BioStation 2、X-Station 2、および BioStation 3 からエクスポートされたデータファイルのみをインポートできます。
- ドア、エレベーター、またはゾーンが BioStar 2 に設定されていない場合、イベントログの一部の情報が空白として表示されることがあります。

1 機能ボタン(…)をクリックし、[データファイルのインポート]をクリックします。
2 目的のファイル(*.tgz)を選択し、[開く]をクリックします。
3 インポートが成功すると、成功メッセージが画面に表示されます。

リアルタイムログ

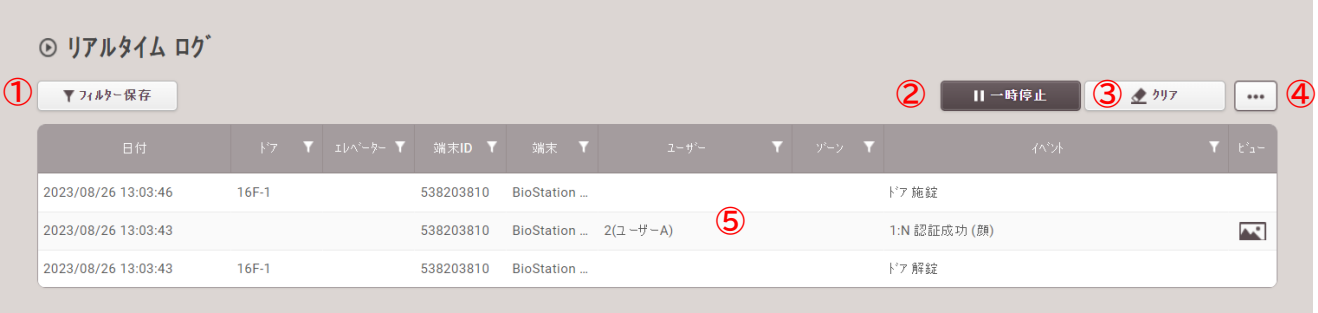
イベントログをリアルタイムに表示および閲覧を行えます。

メモ

・端末時刻と日付の設定を確認してください。端末時刻の設定の詳細については、情報を参照してください。
・リアルタイムログは、[リアルタイムログ]ページが表示されている間に発生したイベントのみ表示されます。
・サーバーで[ログのアップロード]が手動に設定されている場合、リアルタイムログは表示されません。
・イメージログを設定すると、保存した画像を原寸大で閲覧・保存できます。

1 [モニタリング] > [リストビュー] > [リアルタイムログ]をクリックします

2 フィルタリングした結果のみを表示するには、列のフィルターボタン( )をクリックしてフィルターを適用します。



項番	項目名	説明
1	フィルター保存ボタン	設定したフィルターを保存します。
2	開始/一時停止	リアルタイムログ収集を一時停止または開始します。
3	クリアボタン	表示されているログ情報をクリアします。 すべてのイベントログを表示するには、イベントログを参照してください。
4	機能ボタン (カラム設定)	ログのカラム設定を変更します。
5	イベントログ	イベントログを表示します。 イメージログが発生すると、ブラウザ画面左側に通知がポップアップ表示され、PC に保存されているキャプチャ画像はビューアイコン( )を押して確認します。

端末の状態

端末の状態、警報、最終イベントなど、端末の状態の表示および操作を行えます。

1 [モニタリング] > [リストビュー] > [端末の状態]をクリックします。

2 フィルタリングした結果のみを表示するには、列のフィルターボタン()をクリックしてフィルターを適用します。

項番	項目名	説明
1	フィルター保存ボタン	設定したフィルターを保存します。
2	機能ボタン (カラム設定)	一覧表のカラム設定を変更します。
3	端末の状態一覧	端末の状態一覧を表示します。 端末を選択し、[警報解除]をクリックすると、警報を解除できます。

ドアの状態

ドアの状態、リレーの状態、警報、最終イベントなど、ドアの状態の表示および操作を行えます。

1 [モニタリング] > [リストビュー] > [ドア ステータス]をクリックします。

2 フィルタリングした結果のみを表示するには、列のフィルターボタン(▼)をクリックしてフィルターを適用します。

項番	項目名	説明
1	フィルター保存ボタン	設定したフィルターを保存します。
2	機能ボタン (カラム設定)	ログの列設定を変更します。
3	ドア状態一覧	ドアの状態一覧を表示します。 選択したドアでは、次の操作が可能です。 ・ 連続施錠: ユーザーが認証してもドアが解錠されなくなります。(常時施錠) ・ 連続解錠: ユーザーが認証しなくてもドアが常時解錠されます。 ・ 通常状態: 管理者が操作した連続施錠または連続解錠を解除します。 ・ 一回解錠: 管理者が遠隔でドアの解錠時間だけドアが解錠されます。 ・ 警報を解除: すべてのドアの警報を解除します。ゾーンに警報が設定されている場合、ドア状態の警報を解除しても警報が解除されない場合があります。 その場合、ゾーン状態の[警報を解除]をクリックします。 ・ APB リセット: すべてのユーザーまたはユーザーを選択して、APB 違反状態をリセットします。

メモ

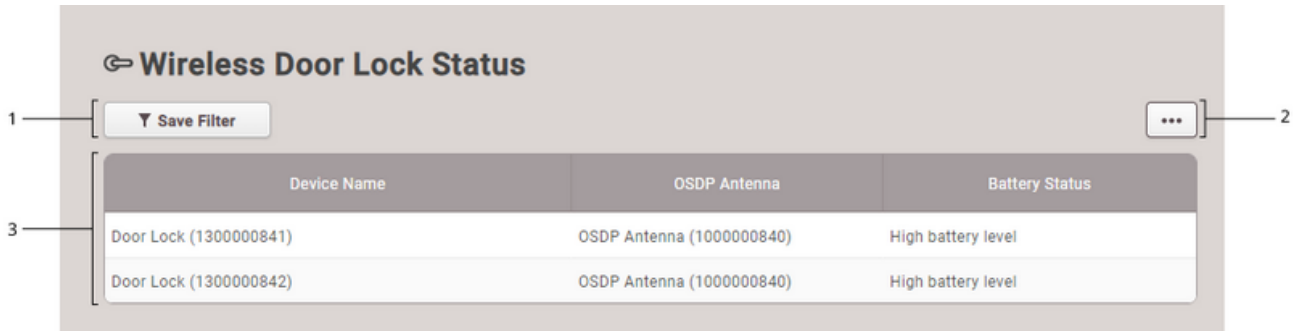
- ドアイベントの説明は以下を参照してください。
- Fire alarm unlocked:火災警報ゾーンによる警報が発生したため、火災警報ゾーンに設定されたドアが解錠された状態。
- Manual Lock: ユーザーが認証してもドアが解錠されない状態(常時施錠状態)
- Manual Unlock: ユーザーが認証しなくてもドアが常時解錠されている状態。
- Schedule Locked: スケジュールによりドアが施錠されている状態。
- Schedule Unlocked: スケジュールによりドアが解錠されている状態。
- Normal: 通常の状態。

無線ドアロック状態

使用中の無線ドアロックのバッテリー状態を確認できます。

1 [モニタリング] > [リストビュー] > [無線ドアロック状態]をクリックします。

2 フィルタリングした結果のみを表示するには、列のフィルターボタン(▼)をクリックしてフィルターを適用します。



項番	項目名	説明
1	フィルター保存ボタン	設定したフィルターを保存します。
2	機能ボタン (カラム設定)	一覧表の カラム設定を変更します。
3	ステータス一覧	使用中の無線ドアロックのバッテリーを確認してください。 ・ High バッテリーレベル: バッテリー残量は十分です。 ・ Low バッテリーレベル / Critical バッテリーレベル: バッテリー残量が低下しています。スムーズに動作させるためにバッテリーを交換することをお勧めします。 ・ バッテリーが空です: バッテリー残量がほぼ空です。交換してください。 **メモ** ・ [設定] > [警報] メニューにて、それぞれのバッテリーレベルに移行した場合に警報が発生するように設定できます。

フロア状態

フロアの状態、リレーの状態、警報、最終イベントなど、フロアの状態の表示および操作を行えます。

メモ

AC ライセンスのアドバンスドを適用にすると、フロア状態メニューが表示されます。

1 [モニタリング] > [リストビュー] > [フロア状態]をクリックします。

2 フィルタリングした結果のみを表示するには、列のフィルターボタン( )をクリックしてフィルターを適用します。

項番	項目名	説明
1	フィルター保存ボタン	設定したフィルターを保存します。
2	機能ボタン(カラム設定)	ログのカラム設定を変更します。
3	ステータス一覧	フロアの状態一覧を表示します。 選択したフロアでは、次の操作が可能です。 ・ 連続施錠: ユーザーが認証してもドアが解錠されなくなります。(常時施錠) ・ 連続解錠: ユーザーが認証しなくてもフロアが常時解錠されます。 ・ 通常状態: 管理者が操作した連続施錠または連続解錠を解除します。 ・ 一回解錠: 管理者が遠隔でフロアの解錠時間だけフロアが解錠されます。 ・ 警報を解除: すべてのドアの警報を解除します。ゾーンに警報が設定されている場合、フロア状態の警報を解除しても警報が解除されない場合があります。 その場合、ゾーン状態の[警報を解除]をクリックします。

ゾーン状態

ゾーンの有効無効、警報、最終イベントなどのゾーン状態の表示および操作を行えます。

メモ

・AC ライセンスのスタンダード以上のライセンスを適用した場合のみ、ゾーン状態メニューが表示されます。
・混雑制限ゾーンの現在の状態を確認するには、[ゾーン] > [混雑制限]をクリックします。

1 [モニタリング] > [リストビュー] > [ゾーン状態]をクリックします。

2 フィルタリングした結果のみを表示するには、列のフィルターボタン(▼)をクリックしてフィルターを適用します。

項番	項目名	説明
1	フィルター保存ボタン	設定したフィルターを保存します。
2	機能ボタン (カラム設定)	ログのカラム設定を変更します。
3	ステータス一覧	ゾーンの状態 リストを表示します。 選択したゾーンでは、次の操作を実行できます。 ・APB リセット : すべてのユーザーまたはユーザーを選択して、APB 違反状態をリセットします。この機能は、アンチパスバックゾーンを選択する場合にのみ使用できます。 ・警報を解除: アンチパスバックゾーンを選択するとアンチパスバック違反警報を解除し、火災警報ゾーンを選択すると火災警報によって解錠されているドアリレーを通常状態に戻します。 **メモ** 入退確認ゾーンが設定されている場合は、[入退状態]をクリックしてユーザーの状態を確認できます。

警告履歴

警告の履歴と状態の表示を行えます。

1 [モニタリング] > [リストビュー] > [警告履歴]をクリックします。

2 フィルタリングした結果のみを表示するには、列のフィルターボタン()をクリックしてフィルターを適用します。

項番	項目名	説明
1	フィルター保存ボタン	設定したフィルターを保存します。
2	ページインジケータとナビゲーションボタン	ページの移動や 1 ページに表示する行数の設定を行えます。 最初のページに移動します。 前のページに移動します。 2 / 2 移動するページ番号を入力します。 次のページに進みます。 最後のページに移動します。 25 行 1 ページに表示する行数を設定します。
3	機能ボタン(印刷、カラム設定)	ログの印刷や、カラムの設定を変更します。
4	警告履歴	警告一覧を表示します。 レポートマーク()をクリックして警告の詳細を表示します。

測温レポート

ユーザーの温度情報を含むイベントの表示を行えます。

1 [モニタリング] > [リストビュー] > [温度レポート]をクリックします。

2 フィルタリングした結果のみを表示するには、列のフィルターボタン( )をクリックしてフィルターを適用します。

項番	項目名	説明
1	フィルター保存ボタン	設定したフィルターを保存します。
2	表示範囲	任意の期間を設定し、温度レポートを並べ替えることができます。
3	摂氏/華氏	温度の単位を設定できます。
4	ページナビゲーションボタンとリストの行数	ページの移動や 1 ページに表示する行数の設定を行えます。 前のページに移動します。 次のページに進みます。 25 行 1 ページに表示する行数を設定します。
5	機能ボタン（印刷、CSV エクスポート、カラム設定）	温度レポートで追加機能を使用できます。 ・ 印刷：イベントログを PDF や SVG 形式で印刷 ・ CSV エクスポート：CSV ファイルのエクスポート ・ カラム設定：列の設定の変更
6	レポート	ユーザーの温度情報を含むイベントが表示されます。 **メモ** [日付]列をクリックすると、リストを昇順または降順で並べ替えることができます。

関連情報

サーマル&マスク

グラフィカルマップビュー

グラフィックマップを追加すると、ドアの状態をグラフィックかつリアルタイムに表示および制御を行えます。

- グラフィックマップ グループの追加と管理
- グラフィックマップの追加と管理

メモ

AC ライセンスのスタンダード以上のライセンスを適用した場合のみ、グラフィカルマップビューメニューが表示されます。

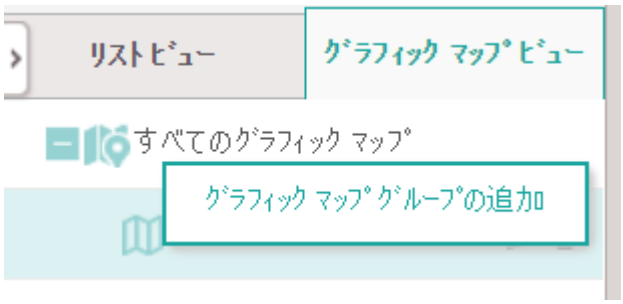
グラフィカルマップグループの追加と管理

グラフィックマップグループを作成し、複数の端末をグルーピングして管理を行えます。

グラフィックマップ グループの追加

1 [モニタリング] > [グラフィックマップビュー]をクリックします。

2 [すべてのグラフィックマップ]を右クリックし、[グラフィカルマップグループの追加]をクリックします。



3 グループ名を入力します。

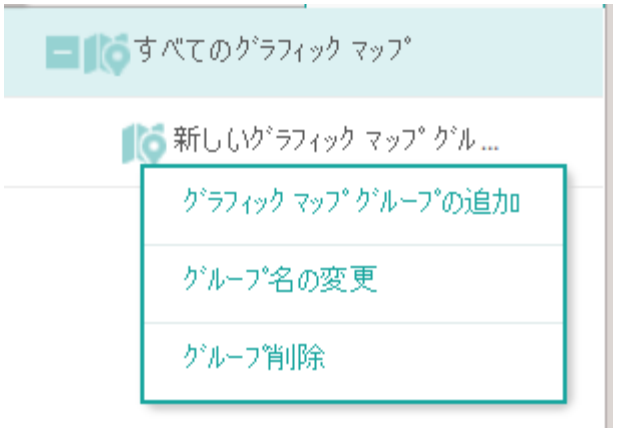
メモ

- グラフィックマップグループは、最大 8 レベルで作成できます。
- グラフィックマップグループ名は 48 文字まで入力できます。

グラフィックマップ グループの名前変更

1 [モニタリング] > [グラフィックマップビュー]をクリックします。

2 名前を変更するグループの名前を右クリックし、[グループ名のを変更]をクリックします。



3 グループ名を入力します。

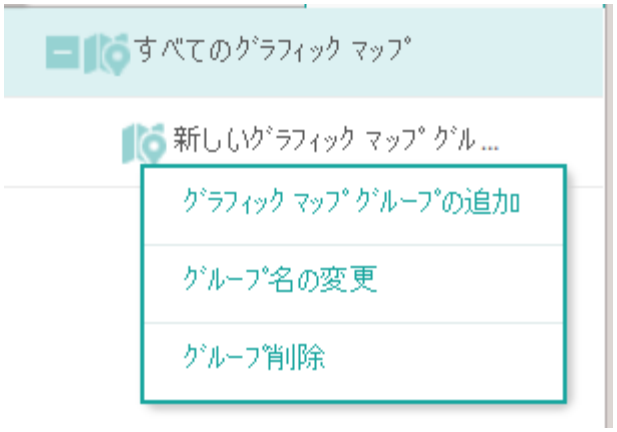
メモ

- グラフィックマップグループ名は 48 文字まで入力できます。

グラフィックマップ グループの削除

1 [モニタリング] > [グラフィックマップビュー]をクリックします。

2 削除するグループの名前を右クリックし、[グループ削除]をクリックします。



メモ

・ グループにグラフィックマップが含まれている場合、そのグループを削除することはできません。
グループを削除するには、グループに属するすべてのグラフィックマップを削除する必要があります。

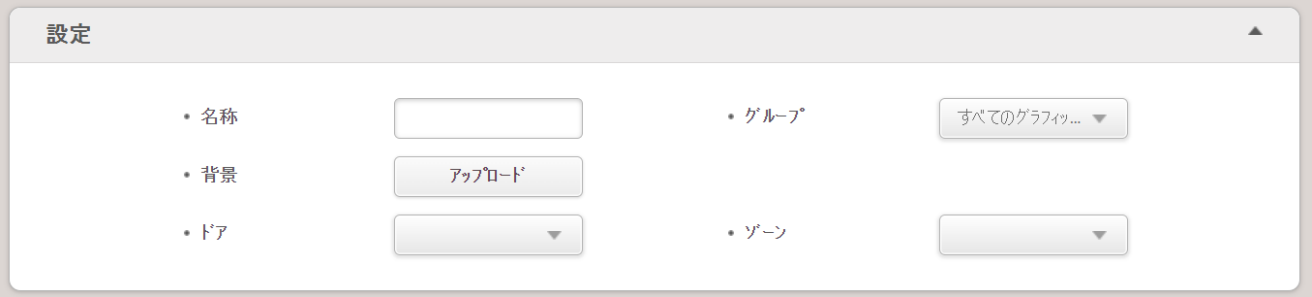
グラフィカルマップの追加と管理

グラフィックマップを追加すると、ドアの状態をグラフィックかつリアルタイムに表示および制御を行えます。

グラフィックマップの追加

1 [モニタリング] > [グラフィックマップビュー]をクリックします。

2 [グラフィックマップを追加]をクリックします。



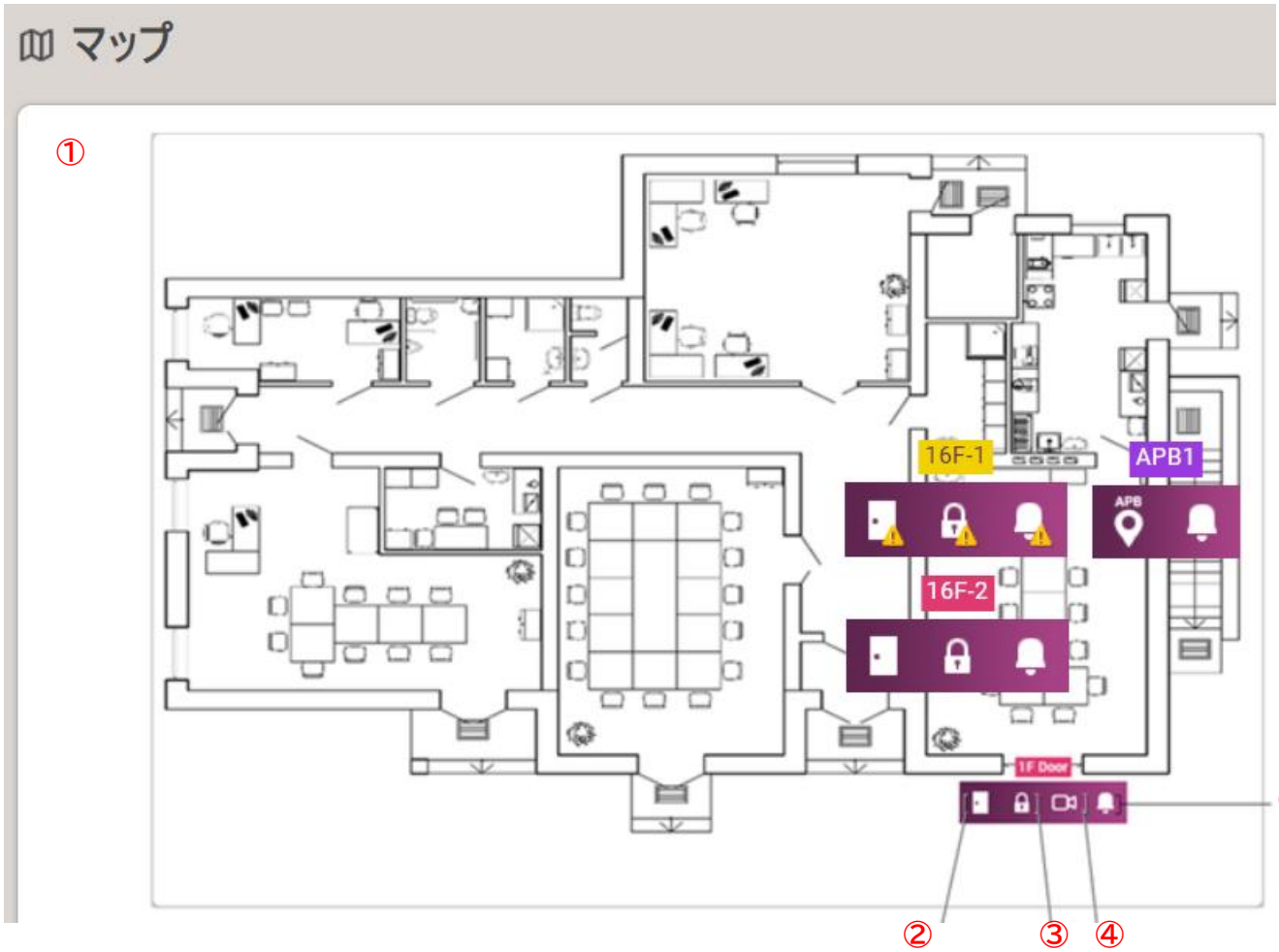
3 グラフィックマップの名前とグループを設定します。

4 [アップロード]をクリックし、グラフィックマップとして使用する背景を選択します。

メモ

- 背景として使用できる画像の最大サイズは 5MB です。
- サポートされている画像ファイル形式は、BMP、GIF、JPG、JPEG、PNG です。
- BioStar 2 データベースをバックアップすると、グラフィックマップに登録された画像ファイルが削除される場合があります。データベースのバックアップ後も、背景として登録した画像を引き続き使用したい場合は、画像ファイルをバックアップしてください。

5 グラフィックマップに表示するドアを[ドア]から選択します。ドア状態のバーが表示されます。



項番	項目名	説明
1	グラフィックマップ	アップロードした背景画像が表示されます。
2	ドアの状態	ドアの状態を確認し、ドアの遠隔解錠を行えます。
3	ドアリレー	ドアの遠隔施解錠を行えます。
4	ライブビデオビュー	**重要** 本機能は弊社でサポート対象外の機能です。 ドアに登録した IP カメラの画面をリアルタイムで見ることができます。 **メモ** ・ ライブ ビデオ ビュー ボタンは、カメラがドアで登録されている場合にのみ有効になります。
5	警報	ドアで発生した警報の表示や警報の解除を行えます。

6 グラフィックマップに表示するゾーンを[ゾーン]から選択します。ゾーンの状態バーが表示されます。

項目	説明
ゾーン	ゾーン種別を判別できます。 **メモ** ・ ゾーンは 100 まで選択できます。
警報	ゾーンで発生した警報の表示や警報の解除を行えます。

7 ドアとゾーンの状態バーをグラフィックマップ内のドアとゾーンの位置にドラッグ&ドロップします。

8 設定が終了したら、[適用]をクリックします。

グラフィックマップの編集

1 [モニタリング] > [グラフィックマップビュー]をクリックします。

2 編集するグラフィックマップのえんぴつマーク()をクリックします。

3 必要な情報を編集したら、[適用]をクリックします。

グラフィックマップの削除

1 [モニタリング] > [グラフィックマップビュー]をクリックします。

2 削除するグラフィックマップのゴミ箱ボタン()をクリックします。

3 [はい]をクリックして、選択したグラフィックマップを削除します。

15 勤怠

勤怠メニューでは、時間規則、シフト、スケジュールを構成して、タイムカードやレポートの表示および出力を行えます。

- シフト
- スケジュール
- レポート
- 設定

勤怠を使用する流れは、次の手順を参考にしてください。

1 時間規則設定

勤怠・残業・休暇の種類ごとの時間規則を作成します。

- 関連情報

  時間規則

2 シフト設定

シフト設定は、毎日(24 時間)単位で設定を行えます。

- 関連情報

  シフト

3 スケジュールテンプレートの設定

日単位や週単位のシフトでスケジュールテンプレートの設定を行えます。

- 関連情報

  スケジュールテンプレート

4 残業ルールの設定

シフトに残業管理の時間規則が設定されていない場合に使用します。

シフト設定で設定する残業時間には開始時刻と終了時刻がありますが、残業ルールでは規定のサービス時間の範囲を超えて合

計時間を計算します。残業ルールは、日、週、月の合計残業時間を管理するのに便利で、残業ルールを設定すると、シフトに追加された残業時間規則の代わりに適用されます。

➢ 関連情報

残業ルール

5 スケジュール設定

前の手順で設定したスケジュールテンプレートに適用する期間、ユーザー、残業ルール、休暇スケジュールの設定を行えます。

➢ 関連情報

スケジュール

シフト

時間規則、時間規則の時間区分、スケジュールテンプレート、残業ルールの設定を行えます。

勤怠管理の主要な構成要素は以下です。

時間規則

稼働時間の計算に使用する時間規則の設定を行えます。

勤怠管理、残業管理、休暇管理など種類ごとの時間規則を作成します。

時間規則ごとに異なる割増率を割り当て使用できます。

1 [勤怠] > [シフト] > [時間規則]をクリックします。

2 [時間規則の追加]をクリックし、各項目を設定します。

項番	項目名	説明
1	名称	時間規則名を入力します。
2	説明	時間規則の簡単な説明を入力します。
3	種別	時間規則の種類を設定します。 ・ 勤怠管理: 勤怠記録に使用する時間規則 ・ 残業管理: 残業に使用する時間規則 ・ 休暇管理: 外出、外出、出張、休暇で使用する時間規則 **メモ** ・ シフトが現在使用している時間規則の場合、種別は変更できません。 ・ 種別が休暇管理の場合、割増率は設定できません。
4	割増率	時間規則に合わせて割増率を設定します。1 はデフォルトの割増率です。 2 を設定すると、設定した時間規則適用時の時給の 2 倍で計算されます。
5	カラー	時間規則を区別する色を設定します。

1 設定を保存するには、[適用]をクリックします。

シフトを追加するには、[適用して次へ]をクリックします。

設定を保存して別の時間規則を追加するには、[適用して新規追加]をクリックします。

➢ 関連情報

シフト

シフト

24 の時間サイクルに基づいて、時間帯ごとに異なる時間規則を適用してシフトの作成を行えます。

固定勤務、流動勤務、フレックス勤務のいずれかを選択でき、開始時刻と丸めルールの設定を行えます。

1 [勤怠] > [シフト] > [シフト]をクリックします。

2 [シフトの追加]をクリックし、各項目を設定します。

項番	項目名	説明
1	名称	シフト名を入力してください。
2	説明	シフトの簡単な説明を入力します。
3	種別	シフト種別を設定します。 詳細設定はシフトタイプによって異なります。 ・固定勤務：定時に出退勤が固定の時間の勤務体系 ・フレックス勤務：出退勤時間を固定しないフレキシブル勤務体系

		・流動勤務: 出退勤時間が決まっていないフローティング勤務体系 出勤時間に応じて自動的にシフトが適用されるシフト種別です。
4	日の開始時刻	1 日の開始時刻を設定します。 [日の前後の時間を許可]を利用すると、設定した始業時刻を基準に、24 時間を超える勤務時間のシフトを設定できます。 **メモ** シフト種別を固定勤務に設定した場合にのみ、[日の前後の時間を許可]を有効化できます。
5	先頭認証を出勤 最終認証を退勤	[はい]に設定すると、最初のユーザー認証時刻が出勤時刻、最後のユーザー認証時刻が退勤時刻として記録されます。 **メモ** [先頭認証を出勤 最終認証を退勤]が[はい]に設定されている場合、打刻による休憩を設定してユーザーの休憩時間を記録する必要があります。
6	時間セグメント	シフト種別を固定勤務に選択した場合、 勤怠レコードとして設定されている給与コードを選択し、開始時刻、終了時刻を設定します。 時間猶予、丸め、食事控除、休憩時間の設定も行えます。 設定が完了したら、[追加]をクリックします。 **メモ** ・ 1 日の許容時間 前後の時間は最大 6 時間まで設定できます。 ・ 勤怠管理として設定した時間規則は、シフトに 1 つだけ追加できます。 ・ 残業管理に設定されている時間規則は、開始時刻、終了時刻、最小時刻、期間、丸めのみ設定できます。 シフト種別でフレックス勤務を選択した場合、 1 日の稼働時間を設定し、時間規則を選択します。 出勤制限時刻、退勤制限時刻、食事控除、四捨五入、休憩時間の設定も行えます。 **メモ** ・ シフト種別でフレックス勤務を選択した場合、残業用の時間規則を付加することはできません。 シフト種別で流動勤務を選択した場合、 時間規則を選択し、開始時刻、終了時刻、最小期間を設定します。 打刻許可時間帯、時間猶予、丸め、食事控除、休憩時間の設定を行えます **メモ** ・ 最大 5 つの時間セグメントでシフトを設定できます。

		・ 流動勤務を使用する場合は、休暇管理を設定するときに、[このセグメントまで休暇適用対象]を選択する必要があります。 シフトとして設定された時間区分から、[このセグメントまで休暇適用対象]を選択できます。 ・ 残業管理に設定されている時間規則は、開始時刻、終了時刻、最小期間、期間、丸めのみ設定できます。
7	丸め	時間の丸めルールを設定できます。 単位は四捨五入する時間、基準は四捨五入を適用する時間です。たとえば、単位に 10 分、基準に 7 分が設定されている場合、8:05 に発生したイベントは 8:00 に発生したとみなされ、8:08 に発生したイベントは 8:10 に発生したと見なされます。使用する項目を選択し、単位と基準を設定します。 ・出勤: 設定した開始時刻より早い/遅い出席イベントの登録時に、登録時刻を処理する四捨五入ルールを設定できます。 ・退勤: 設定した終了時刻より早い／遅い退出イベントが登録された場合に、登録時刻を処理する四捨五入ルールを設定できます。 メモ ・ 丸めは Grace に優先して適用されます。
8	食事控除 1、2	シフトから食事時間を差し引くように設定できます。 ・打刻: 食事の控除時間を固定せず、端末に登録された記録に従って控除するように設定できます。 ・自動: 控除時間と控除前の最小時間数を設定して、食事控除を設定できます。 ・固定:開始時刻と終了時刻を設定して、固定食事控除を設定できます。 メモ ・食事控除 2 を使用すると、シフトから 2 回の食事時間を差し引くことができます。 ・食事控除の種類を自動または固定として使用する場合、食事控除 1 と食事控除 2 は同じ種類にのみ設定できます。
9	休憩時間	休憩時間を設定できます。 ・打刻: 休憩時間を固定せずに、端末に登録されている記録に従って確認するように設定できます。打刻を選択すると、許可された休憩時間の最大値を設定できます。 ・固定: 開始時刻と終了時刻を設定することで、固定の休憩時間を設定できます。

3 設定を保存するには、[適用]をクリックします。スケジュールテンプレートを追加するには、[適用して次へ]をクリックします。設定を保存して別のシフトを追加するには、[適用して新規追加]をクリックします。

➢ 関連情報

スケジュールテンプレート

スケジュールテンプレート

設定されたシフトを使用して、毎週および毎日のスケジュールテンプレートの作成を行えます。

1 [勤怠] > [シフト] > [スケジュールテンプレート]をクリックします。

2 [スケジュールテンプレートの追加]をクリックし、各項目を設定します。

項番	項目名	説明
1	名前	目的のスケジュールテンプレート名を入力します。
2	説明	スケジュールテンプレートの簡単な説明を入力します。
3	種別	スケジュールテンプレートは毎週または毎日のいずれかを設定でき、毎日を選択した場合は繰り返し使用する期間を設定できます。
4	週末	週末として使用する曜日を設定できます。
5	サービスルール	設定されたサービスルールが表示されます。
6	スケジュール	設定したサービスルールにドラッグ＆ドロップを設定します。

		一度にすべて適用するには、[毎日コピー]をクリックします。 **メモ** ・ [先頭認証を出勤 最終認証を退勤]を設定したシフトを適用する場合、「前日シフト」の「始業時刻の 24 時間前」は[先頭認証を出勤 最終認証を退勤]を設定できません。

3 設定を保存するには、[適用]をクリックします。スケジュールを追加するには、[適用して次へ]をクリックします。設定を保存して別のスケジュールテンプレートを追加するには、[適用して新規追加]をクリックします。

➢ 関連情報

残業ルール

残業ルール

シフトに残業管理の時間規則が設定されていない場合に使用します。

シフト設定で設定する残業時間には開始時刻と終了時刻がありますが、残業ルールでは規定のサービス時間の範囲を超えて合計時間を計算します。残業ルールは、日、週、月の合計残業時間を管理するのに便利で、残業ルールを設定すると、シフトに追加された残業時間規則の代わりに適用されます。

1 [勤怠] > [シフト] > [ルール]をクリックします。

2 [ルールの追加]をクリックし、各項目を設定します。

項番	項目名	説明
1	名称	残業ルール名を入力します。
2	説明	残業ルールの簡単な説明を入力します。
3	残業	残業ルールを設定します。 日残業、週残業、月残業ルールでは、通常の勤務時間の後に適用される残業時間規則を設定でき、一定時間後に別の残業時間規則を適用できます。最大残業時間を設定して、従業員の残業時間を制限することもできます。 次のように設定すると、通常の勤務時間が午前 8 時から午後 5 時までの場合、午後 5 時から午後 11 時までは「残業管理」の時間規則が適用され、午後 11 時から午前 2 時までは「残業管理」の時間規則が適用されます。また、従業員の 1 日の最大残業時間は 9 時間に制限されており、日給は午前 2 時までの勤務実績のみを使用して計算されます。 **メモ** ・ 総労働時間には、休憩時間や食事時間は含まれません。 ・ 土日残業・休日残業ルールは、時間規則と始業時間を設定でき、[先頭認証を出勤 最終認証を退勤]のみ設定可能です。

3 設定を保存するには、[適用]をクリックします。スケジュールを追加するには、[適用して次へ]をクリックします。設定を保存して別のルールを追加するには、[適用して新規追加]をクリックします。

➢ 関連情報

スケジュール

スケジュール

設定したスケジュールテンプレート、残業ルール、期間、休日をユーザーに割り当ててスケジュールの作成を行えます。

作成したスケジュールに一時スケジュールや個別休暇を追加することも行えます。

メモ

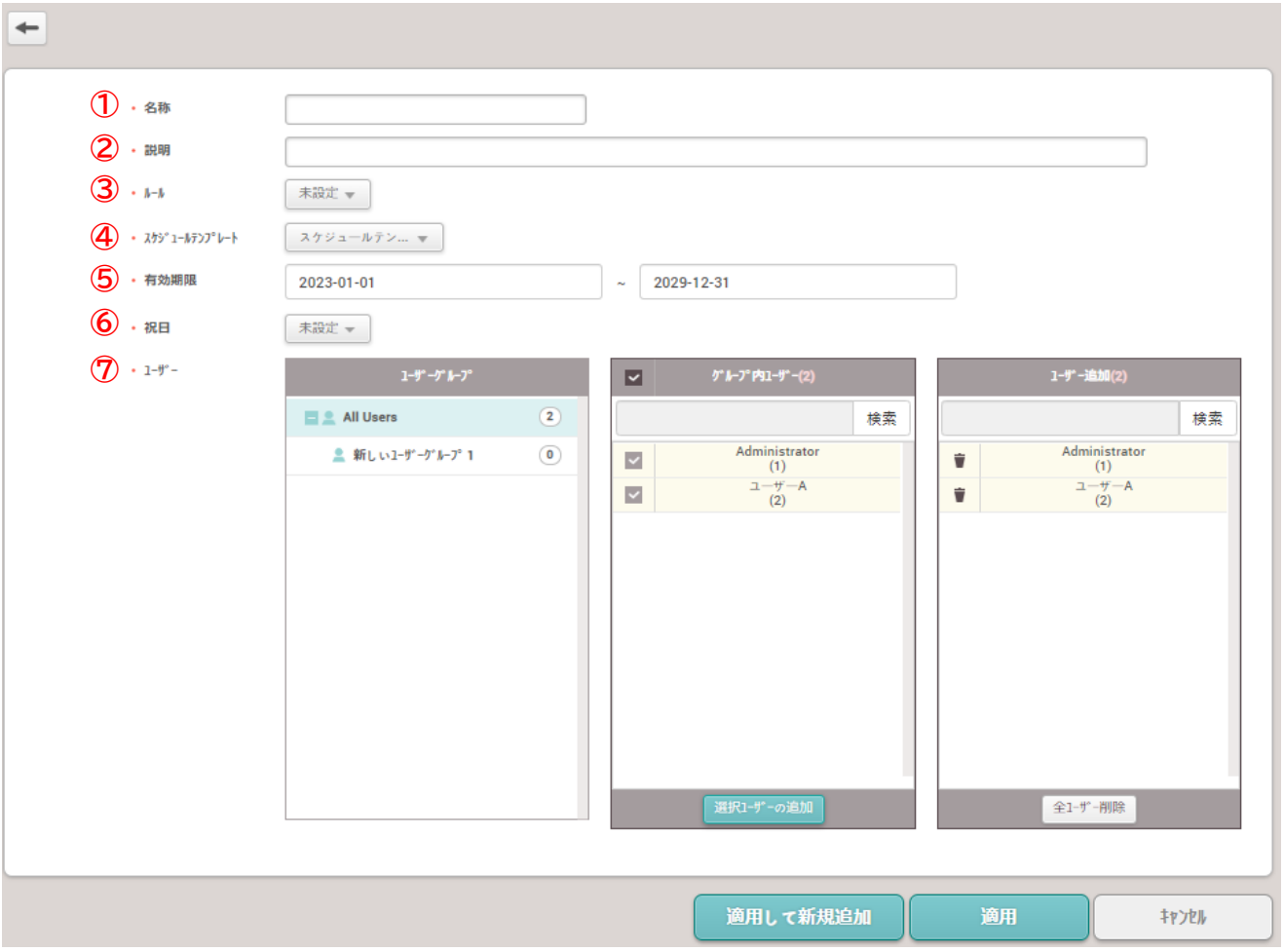
スケジュールを作成する前に、使用する時間規則、シフト、スケジュールテンプレート、休日が正しく作成されているか確認してください。

スケジュールの追加と削除

登録ユーザーのスケジュールを作成できます。

1 [勤怠] > [スケジュール]をクリックします。

2 [追加]をクリックし、各項目を設定します。



項番	項目名	説明
1	名前	目的のスケジュール名を入力します。
2	説明	スケジュールの簡単な説明を入力します。

3	ルール	設定した残業ルールを選択します。 残業ルールが設定されている場合、スケジュールテンプレートに設定されているシフトの残業設定は適用されません。使用しない場合は未使用に設定してください。 **メモ** 目的の残業ルールがない場合は、残業ルールを参考に設定してください。
4	スケジュールテンプレート	設定されたスケジュールテンプレートを選択します。 **メモ** ・ 目的のスケジュールテンプレートがない場合は、スケジュールテンプレートを参照して設定してください。 ・ スケジュールテンプレートは、一度設定すると変更できません。
5	期間	勤怠イベントを収集する期間を設定します。 **メモ** 開始日が設定されると、変更することはできません。終了日は変更可能で、設定日より前の日付に変更した場合、変更後の期間の休暇イベントは削除されます。
6	祝日	設定された休暇スケジュールを選択します。使用しない場合は未使用に設定してください。 **メモ** 目的の休暇スケジュールがない場合は、スケジュールを参照して休暇スケジュールを追加します
7	ユーザー	ルールを適用するユーザーを追加します

3 設定を保存するには、[適用]をクリックします。

4 スケジュールを削除するには、リストから削除するスケジュールを選択し、[スケジュールの削除]をクリックします。

メモ

スケジュール全体に含まれるユーザー数は、選択した勤怠ライセンスの最大ユーザー数を超えることはできません。ライセンスごとの最大ユーザー数について詳しくは、ライセンスを参照してください。

一時スケジュールの追加と削除

既にスケジュールを登録している場合、一時的に別のサービスルール(スケジュールテンプレート)をユーザーに設定できます。

1 リストからスケジュールに割り当てられたユーザーを選択し、カレンダーの日付をクリックします。

2 一時スケジュール追加を選択し、各項目を設定します。

他のユーザーも同様に適用するには、検索ボタン(🔍)をクリックしてユーザーを追加します。

3 適用をクリックすると、設定した期間のシフトが変更されます。

4 一時スケジュールを削除するには、設定した一時スケジュールのサービスルール(スケジュールテンプレート)をクリックし、[はい]をクリックします。

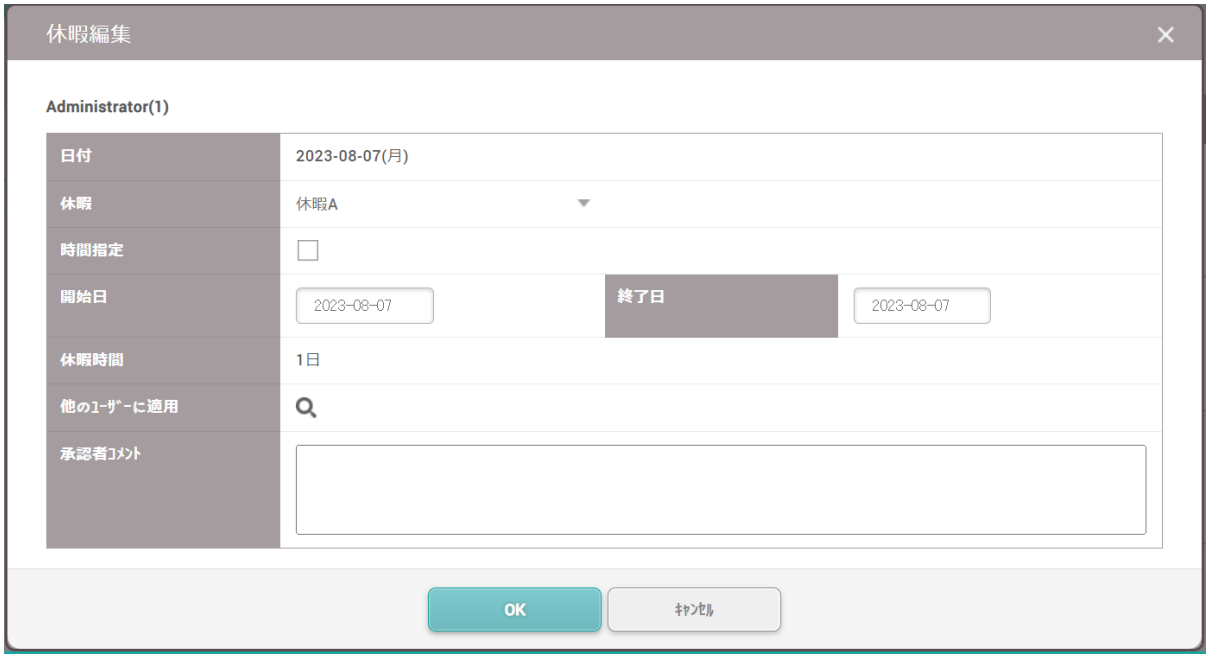
休暇の追加と削除

ユーザーの個別の休暇スケジュールの追加を行えます。

1 リストからスケジュールに割り当てられたユーザーを選択し、カレンダーの日付をクリックします。

2 休暇の追加を選択し、各項目を設定します。

他のユーザーも同様に適用するには、検索ボタン(🔍)をクリックしてユーザーを追加します。



3 OK をクリックすると、設定した期間に休暇が登録されます。

4 休暇を削除するには、登録されている休暇をクリックし、[はい]をクリックします。

メモ

目的の休暇管理時間規則が見つからない場合は、時間規則を参照して追加してください。

レポート

ユーザーの勤怠イベントログから勤怠レポートを作成し、レコードを CSV ファイルまたは PDF ファイルとして編集またはエクスポートを行えます。

7 つの事前設定されたレポートフィルターを使用することや、管理者がフィルターを手動で設定することも行えます。

多言語レポートをご利用になる前に

BioStar 2 は韓国語と英語をサポートしています。多言語レポートを使用するには、以下を確認してください。

フォント設定

1 [C:¥Program Files¥BioStar 2(x64)¥ta¥dist¥setup¥report_fonts]に移動します。

2 使用する言語名でフォルダーを作成します。言語名については、ISO 639-1 規格を参照してください。
たとえば、スペイン語を使用するには、「es」という名前のフォルダーを作成します。

3 フォントファイルをコピーして、作成したフォルダーに貼り付けます。サポートされる TrueType フォントは 1 つだけです。

PDF 表示設定

1 リンクをクリックして、PDF ビューアーを Google Chrome にインストールします。
https://chrome.google.com/webstore/detail/pdf-viewer/oemmndcbldboiebfnladdacbdfmadadm

レポートを更新する前に

BioStar 2 は、デフォルトのデータベースとして MariaDB を使用します。MS SQL データベースを使用している場合は、以下を確認してください。

BioStar 2 を MS SQL データベースとともに使用する場合、多数の登録ユーザーがいる場合、レポートを更新するたびに PC のメモリ使用量が蓄積されます。MS SQL データベースの最大サーバー メモリをリセットします。

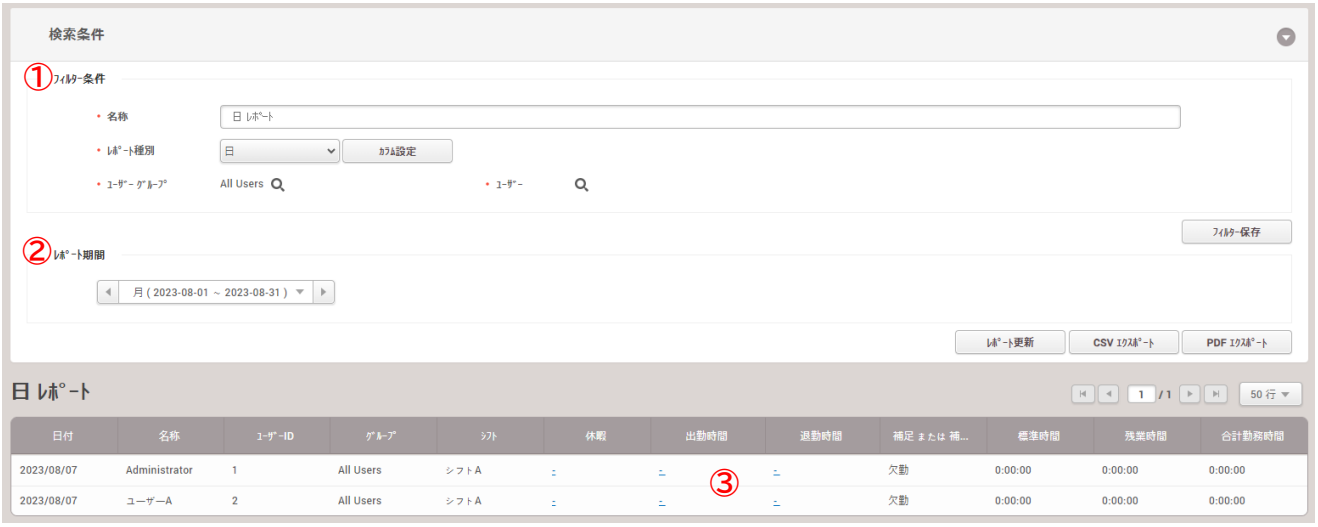
1. SQL Server Management Studio の Micros を実行します。
2. オブジェクト エクスプローラーで BioStar 2 データベースを右クリックし、[プロパティ] をクリックします。
3. 「Memory」をクリックし、「Max Server Memory」の値を減らします。

> **メモ**
>
> MariaDB および MS SQL Server の設定の詳細については、「BioStar 2 のインストール」を参照してください。

1 [勤怠] > [レポート]をクリックします。

2 事前設定されたフィルターリストを使用するには、目的のフィルタータイプを選択し、[ユーザーグループ]または[ユーザー]を設定して[レポートの更新]をクリックします。

3 新規フィルターを登録するには、[フィルターの追加]をクリックし、各項目を設定します。



項番	項目名	説明
1	フィルター条件	新しい勤怠レポートを設定します。 ・ 名称: 目的のレポート名を入力します。 ・ レポート種別: 目的のレポートの種類を選択します。「日、日の概要、個人、個人の概要、休暇、補足 または 補足数、修正済み打刻ログ記録、労働警報時間」のレポートが利用可能です。 ・ カラム設定: レポートテーブルの列の順序を変更または非表示にします。 ・ フィルター: この機能は、[レポート種別]に[休暇]または[補足 または 補足数]が設定されている場合にのみ有効であり、[休暇]または[補足 または 補足数]のレコードの詳細条件を選択できます。 ・ ユーザーグループ/ユーザー: レポートを作成するユーザーグループまたはユーザーを選択します。 ・ フィルター保存: 設定した勤怠レポートをフィルターとして保存します。
2	レポート期間	レポート期間を設定します。 ・ 期間: レポートを作成する期間を日単位、週単位、月単位、またはカスタムに設定します。 ・ 出退勤打刻: ユーザーの出勤と退勤のログのみをレポートに出力する場合に選択します。 ・ すべての打刻: ユーザーのすべてのパンチをレポートに出力する場合に選択します。 **メモ** 出退勤打刻とすべての打刻はレポート種別[個人]でのみ有効です。 ・ レポート更新: レポートテーブルを最新の情報に更新します。 ・ CSV エクスポート: 作成したレポートを CSV ファイルとして保存します。 ・ PDF エクスポート: 作成したレポートを PDF ファイルとして保存します。
3	レポート	作成したレポートを表示します。

労働警報時間 レポートの追加

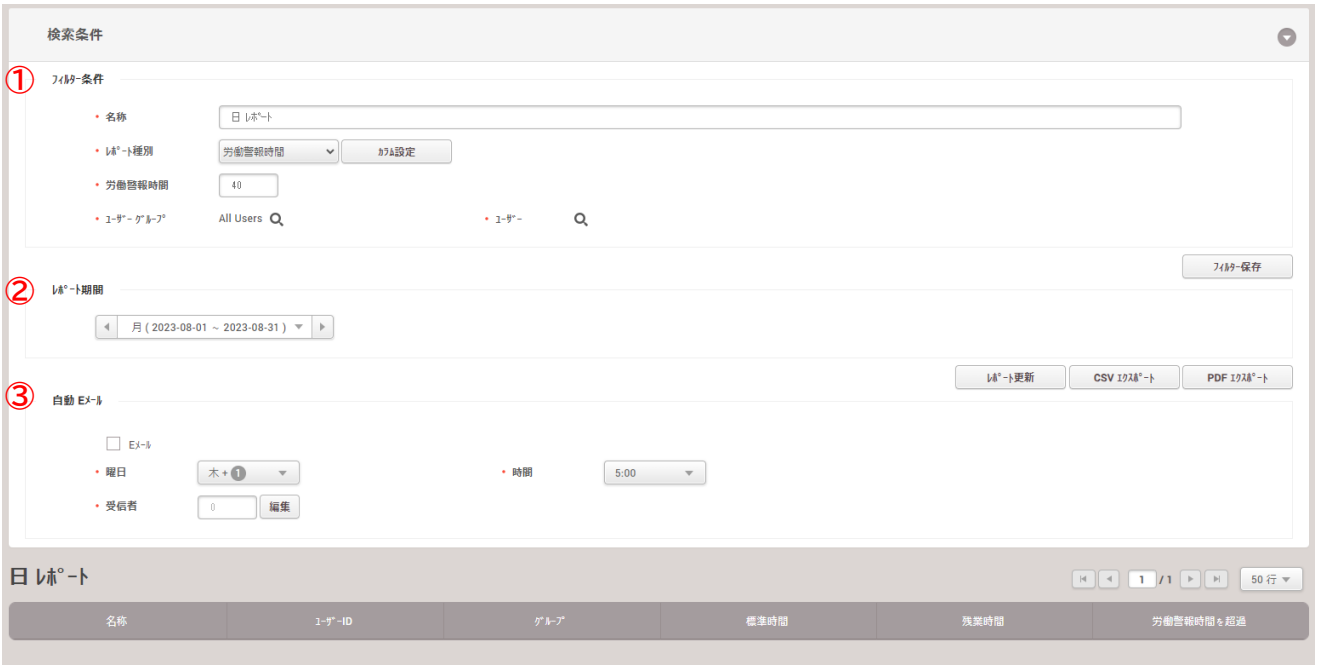
指定した勤務時間に達したユーザーのレポートを更新し、管理者に電子メールで通知できます。

労働警報時間 レポートは毎週更新できます。

1 [勤怠] > [レポート] > [労働警報時間 レポート]をクリックします。

2 [フィルター条件]と[レポート期間]の各項目を設定し、[レポートの更新]をクリックします。

3 指定した勤務時間になったユーザーを管理者にメールで通知する場合は、自動メールを設定します。



項番	項目名	説明
1	フィルター条件	新しい勤怠レポートを設定します。 ・名称: 目的のレポート名を入力します。 ・レポート種別: 目的のレポートの種類を選択します。 ・カラム設定: レポート テーブルの列の順序を変更または非表示にします。 ・労働警報時間: 労働警報時間 レポートを生成する時刻を設定します。 ・ユーザーグループ/ユーザー: レポートを作成するユーザーグループまたはユーザーを選択します。 ・フィルター保存: 設定した 勤怠レポートをフィルターとして保存します。
2	レポート期間	レポート期間を設定します。 ・レポート期間: レポートを作成する期間を設定します。 ・レポート更新: レポート テーブルを最新の情報に更新します。 ・CSV エクスポート: 作成したレポートを CSV ファイルとして保存します。 ・PDF エクスポート: 作成したレポートを PDF ファイルとして保存します。
3	自動 E メール	管理者の所定の勤務時間に達したユーザーをメールで通知できます。 ・E メール: クリックすると、管理者に電子メールが自動的に送信されます。

		・曜日: 管理者にメールを送信する曜日を設定できます。 ・時間: 管理者にメールを送信する時刻を設定できます。 ・受信者: 電子メールを受信する管理者のメールアドレスを追加できます。  メモ ・自動メールを設定するには、フィルター条件を設定してフィルターを保存する必要があります。 ・自動送信メールの差出人情報を設定できます。

勤怠レコードの編集

作成されたレポートテーブルをクリックすると、勤怠レコードの変更を行えます。

メモ

- 勤怠レコードを変更するには、最初にレポートを作成する必要があります。
  レポートの作成については、レポートを参照してください。
- 勤怠スケジュールが登録されていないユーザーの出退勤記録は修正できません。

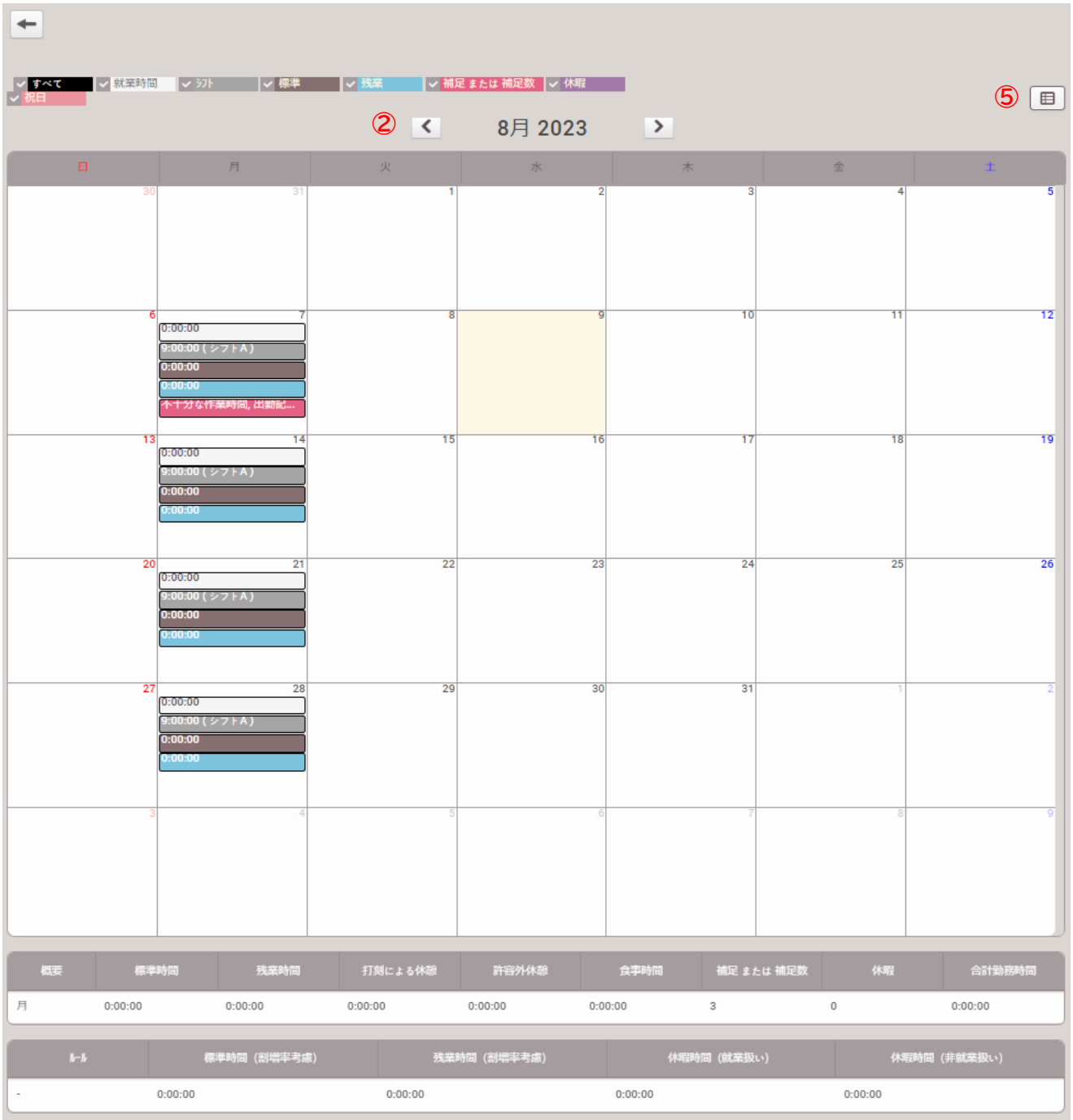
1 レコードをクリックして、作成されたレポートテーブルからレコードを変更します。

2 必要な方法に従って、勤怠レコードを変更するか、休暇を追加します。

リストでの変更

項番	項目名	説明
1	日付範囲	勤怠ログの実績を一覧表示する期間を設定できます。
2	日の勤怠記録	日の勤怠記録を表示できます。 **メモ** ・ [出退勤時間]をクリックして、勤怠レコードを追加、変更、または削除できます。出退勤時間のえんぴつマーク( )をクリックしてからをクリックすると、登録されている勤怠レコードを変更できます。[OK]をクリックすると、変更が保存されます。 ・ えんぴつマーク( )をクリックして休暇を追加できます。休暇を追加するには、休暇管理に設定されている時間規則が必要です。追加した休暇をクリックすると削除できます。
3	勤怠レコードの概要	設定した期間に応じて勤怠レコードを閲覧できます。
4	カレンダー形式で表示	勤怠レコードをカレンダーで表示できます。

カレンダーでの変更



項番	項目名	説明
1	イベントタイプ	各イベントの種類をクリックして、カレンダーに表示または非表示にすることができます。
2	月	〈 または 〉 をクリックして、前の月または次の月に移動できます 。
3	日の勤怠記録	日の勤怠記録を表示できます。 **メモ** ・ 作業時間(白)をクリックすると、勤怠レコードを追加、変更、または削除できます。え

		んぴつマーク()をクリックすると、登録済みの勤怠レコードを変更できます。[OK]をクリックすると、変更が保存されます。 ・ シフト(灰色)をクリックすると、休暇を追加できます。休暇を追加するには、休暇管理に設定されている時間規則が必要です。追加した休暇のゴミ箱マーク()をクリックすると削除できます。
4	勤怠レコードの概要	毎月の勤怠レコードを表示できます。
5	表形式で表示	勤怠レコードを一覧で表示できます。

設定

勤怠管理に使用する端末の登録が行えます。

1 [勤怠] > 設定(⚙)をクリックします。

2 各項目を設定します。

項番	項目名	説明
1	未登録端末	未登録の勤怠管理が利用可能な端末の一覧です。 目的の端末を選択し、[+登録]をクリックして、選択した端末を勤怠管理端末として登録します。
2	登録端末	現在、勤怠管理として使用されている端末の一覧です。 登録をキャンセルするには、目的の端末を選択し、「登録解除」をクリックします。 「設定」をクリックすると、登録済みの端末の勤怠設定を変更することもできます。詳細については、端末の勤怠を参照してください。 勤怠種別は、勤怠イベントキーと勤怠イベント種別(出勤、退勤、休憩開始、休憩終了、食事開始、食事終了)をマッピングする設定です。 

		メモ 端末が接続されている間のみ、端末の勤怠設定を編集することができます。
3	送信者情報	通知メールを送信する際に使用する送信者情報を設定できます。
4	エクスポート	勤怠レポートを CSV エクスポートにエクスポートするときに、ドキュメントの区切り文字を選択できます。
5	勤怠ログの保存期間	勤怠ログの保存期間を設定できます。

メモ

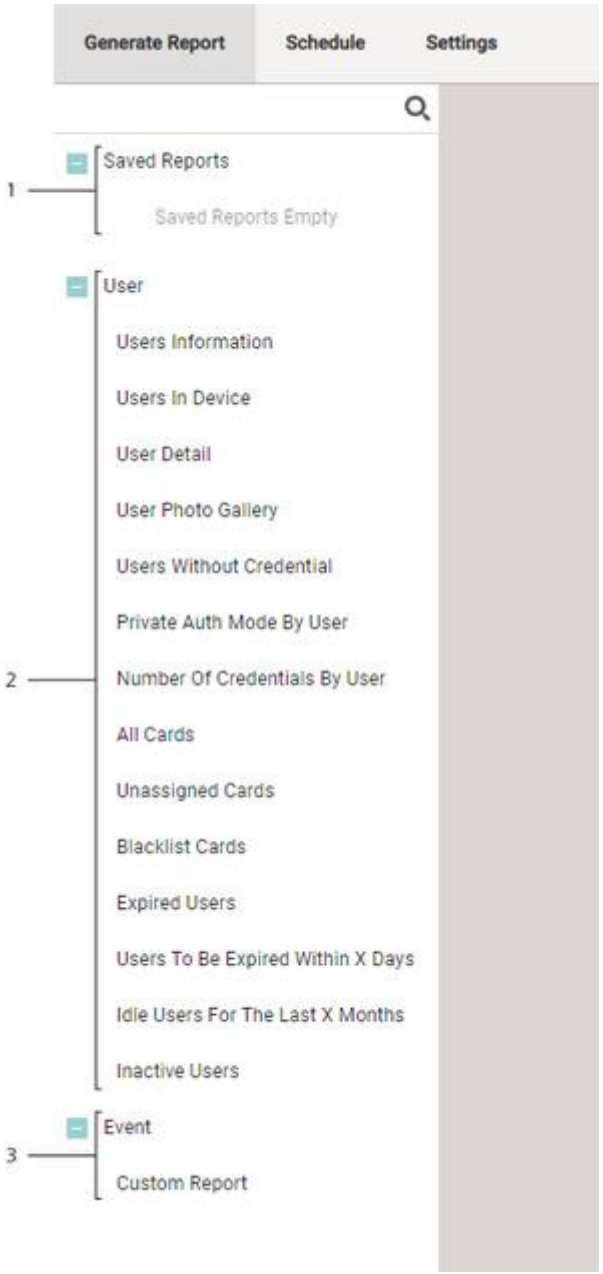
端末メニューで登録機器を削除すると、登録されている勤怠管理機器も自動的に削除されます。

16 リポート

リポートメニューでは、BioStar 2 内のユーザー情報や各種イベントを任意の形式で作成して保存します。

必要なレポートを定期的に自動生成し、生成されたレポートは CSV または PDF としてエクスポートまたは印刷できます。

レポートの生成



項番	項目名	説明
1	Saved Reports	作成したレポートで「Saved Reports」をクリックすると、その下にテンプレートとして保存されます。今後、同じ条件でレポートを作成する必要がある場合に便利です。
2	User	ユーザーに関連するテンプレートを選択してレポートを作成します。
3	Event	カスタムレポート: 必要なイベント、期間、フィルター（ユーザー、ドア、端末）を選択してレポートを作成します。

自動レポートスケジュール

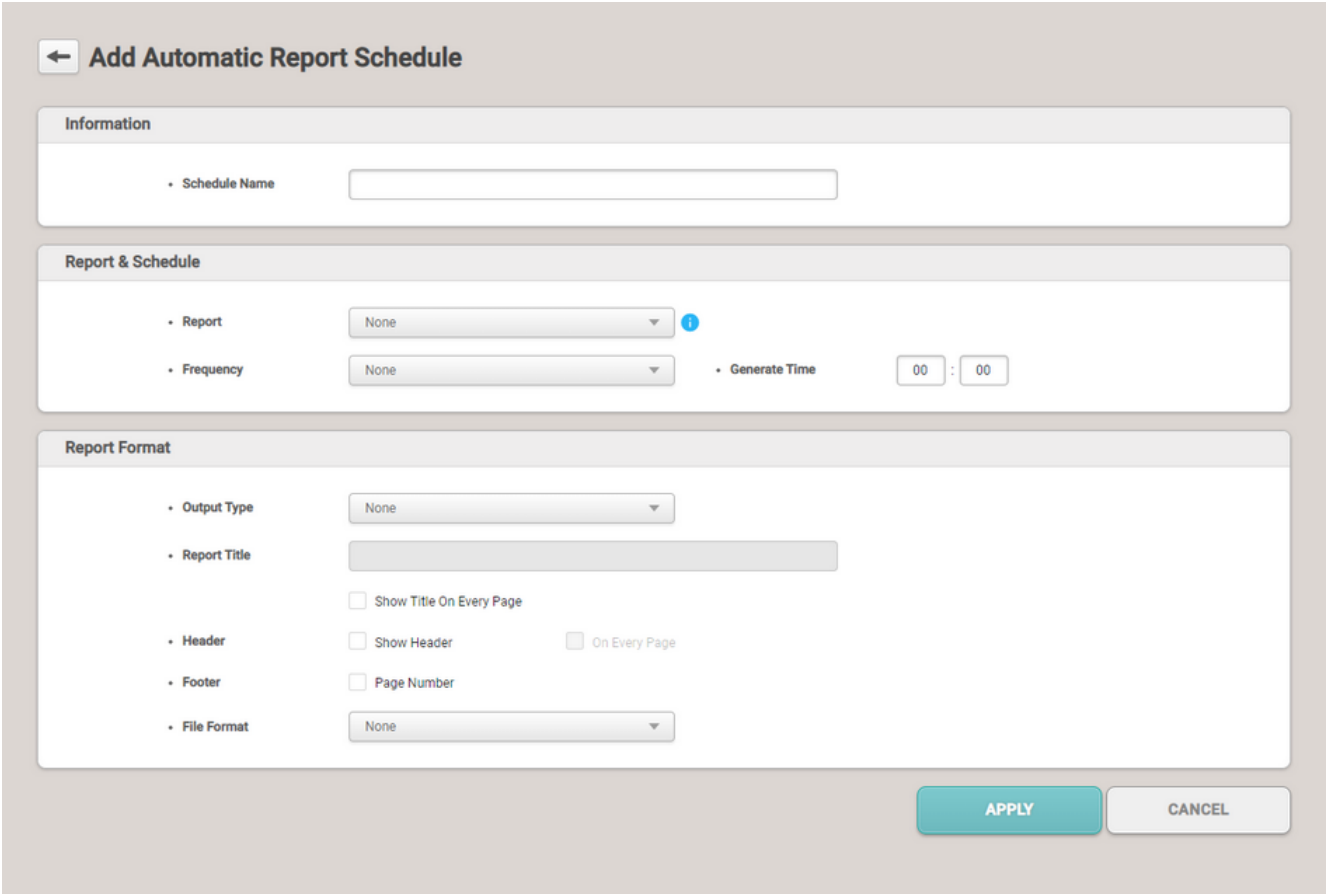
作成されたカスタムレポートを自動的に生成するスケジュールを設定します。

自動レポートスケジュールを使用するには、Biostar 2 管理者ログインが必要です。

詳細については、「Biostar 2 管理者ログイン」を参照してください。

1 [スケジュールの追加]をクリックします。

2 必要な項目を編集します。



項目	説明
Information	自動レポートスケジュールの基本情報を設定します。 ・ Schedule Name: スケジュール名を入力します。
Report & Schedule	各レポートの自動生成スケジュールを設定します。 ・ Report: 自動的に生成するカスタムレポートを選択します。ダイナミック期間に設定されたカスタムレポートのみが表示されます。 ・ Frequency: レポートを自動的に生成する頻度を設定します。 ・ Generate Time: レポートを自動生成する時間を設定します。
Report Format	各レポートの形式を設定します。 ・ Output Type: レポートの自動生成方法を設定します。 ・ Report Title:「すべてのページにタイトルを表示」を選択すると、すべてのページにレポー

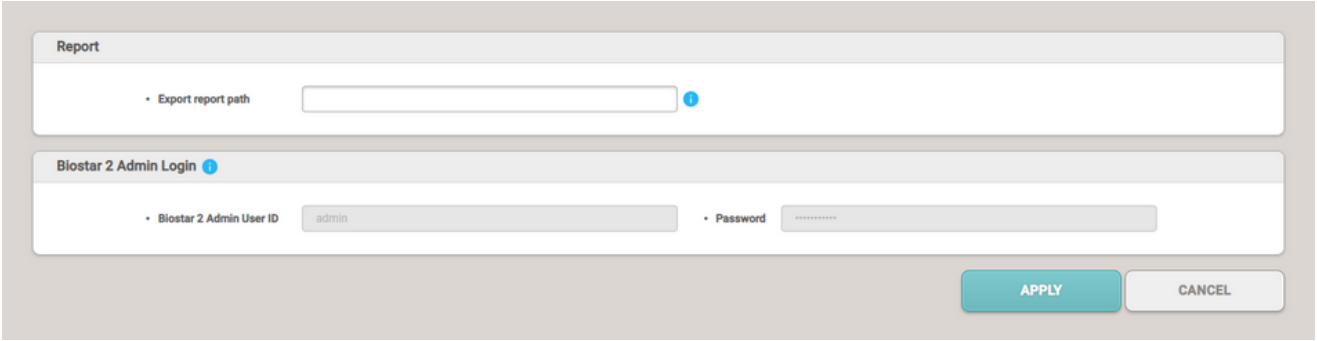
	ト名がタイトルとして表示されます。 ・Header:［ヘッダーを表示］が選択されている場合、レポートの作成時にヘッダーが表示されます。すべてのページにヘッダーを表示するには、「すべてのページ」を選択します。 **メモ** ヘッダーはレポートによって異なる場合があります。 ・ Footer: ページ番号を表示するかどうかを設定します。 ・ File Format: レポートをエクスポートするためのファイル形式を設定します。

3 「適用」をクリックして設定を保存します。

設定

1 [レポート] > [設定]をクリックします。

2 必要な項目を編集します。



項目	説明
Report	・Export report path: 保存されたパスにレポートをエクスポートします。 入力しない場合は、ユーザーの PC の「Documents¥BioStar2」に作成されます。
Biostar 2 Admin Login	管理者アカウントのログイン ID とパスワードを入力します。 自動レポートスケジュールは管理者アカウント情報を入力することで利用可能になります。 ・Biostar 2 Admin User ID: 管理者アカウントのログイン ID を入力します。 ・Password: 管理者アカウントのパスワードを入力します

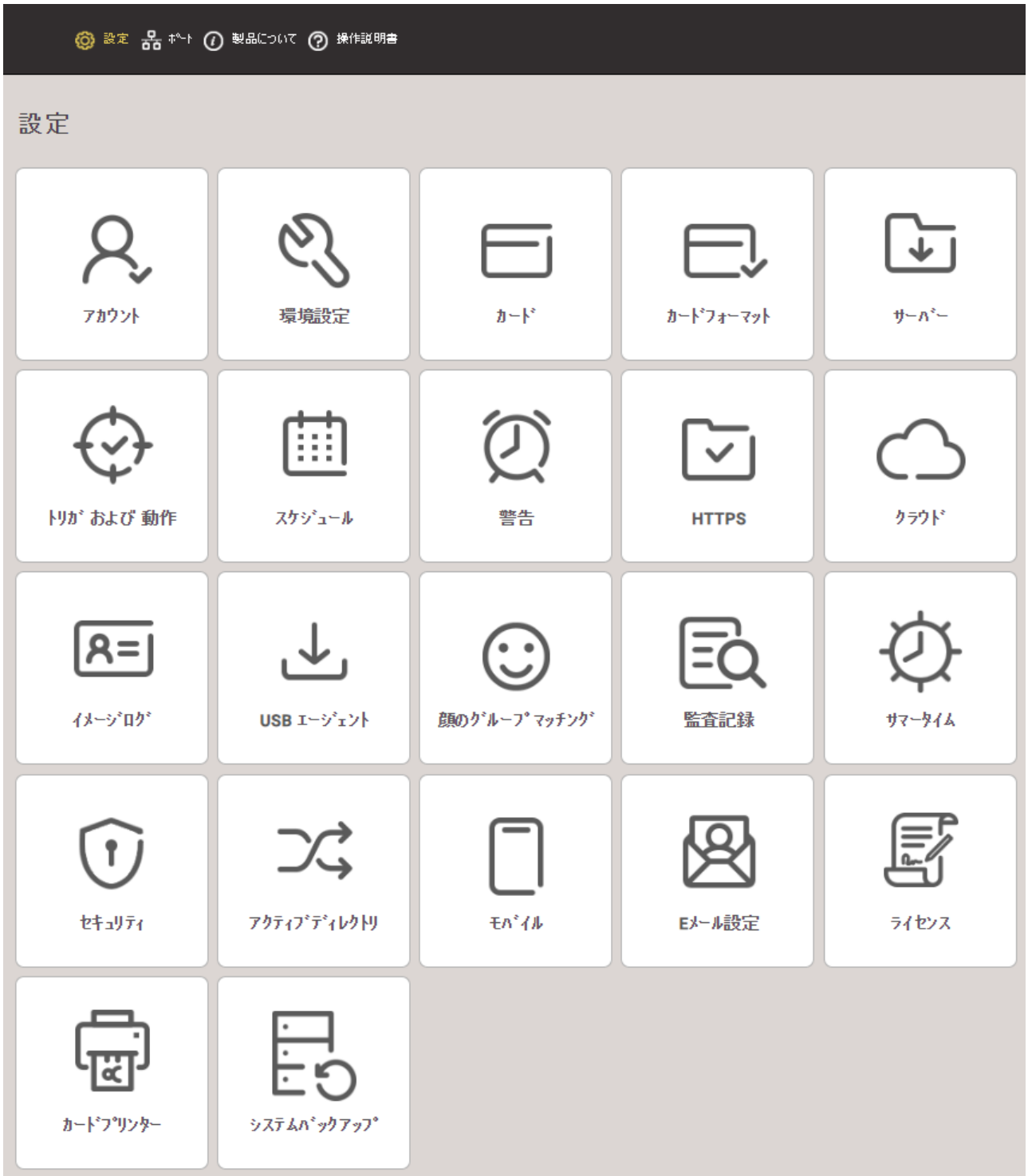
3 「適用」をクリックして設定を保存します。

17 BioStar2 の設定

設定メニューでは、ユーザーのアカウント権限、ユーザー同期モード、言語設定など、さまざまな設定を行えます。

画面の上部にある[設定]をクリックすると設定メニューが開きます。

ログインユーザーの BioStar 操作権限によって、表示される項目が異なる場合があります。



- アカウント
- 環境設定
- カード
- カードフォーマット
- サーバー
- トリガーおよび動作
- スケジュール
- 警告
- HTTPS
- クラウド
- イメージログ
- USB エージェント
- 顔グループマッチング
- 監査記録
- サマータイム
- セキュリティ
- アクティブ ディレクトリ
- モバイルアクセス
- メール設定
- ライセンス
- カードプリンター
- システムバックアップ

アカウント

ユーザーの BioStar 操作権限に割り当てるアカウントレベルの確認や、カスタムアカウントレベルを作成し、ユーザーに割り当てを行えます。

1 [設定] > [アカウント]をクリックします。

2 作成済みのアカウント種別が表示されます。

適用している AC ライセンスの種類によって、表示されるアカウント種別が異なる場合があります。

項目	説明
管理者	ユーザーはすべてのメニューを使用できます。
ユーザーオペレーター	ユーザーは、ユーザーおよび設定メニューのみを使用できます。
モニタリングオペレーター	ユーザーは、モニタリングおよび設定メニューを使用でき、ダッシュボード、ユーザー、端末、ドア、ゾーン、アクセスコントロールメニューのみを表示できます。
勤怠オペレーター	ユーザーは勤怠メニューのみを使用でき、ユーザーメニューのみ表示を行えます。
ユーザー	ユーザーは自分の情報と勤怠レコードのみ表示を行えます。

3 [+追加]をクリックしてユーザーを選択するか、検索ボタン(🔍)をクリックしてユーザーを検索します。

項番	項目	説明
1	名称	アカウントレベルの名前を表示します。
2	説明	アカウントレベルに簡単な説明を追加します。
3	管理項目設定	権限が割り当てられたグループを表示します。
4	管理者メニュー設定	割り当てられた権限を表示します。
5	ユーザー追加	権限が割り当てられているユーザーのリストを表示します。 [+追加]をクリックして、ユーザーを追加します。 ゴミ箱ボタン( )をクリックすると、登録済みのユーザーが削除されます。

4 [適用]をクリックして設定を保存します。

メモ

・ ユーザーの追加または編集中に権限が既に割り当てられている場合は、割り当てられたユーザーがリストに表示されます。

- 編集権限を持つユーザーが各メニューの詳細設定を変更した後、設定を保存しない限り、閲覧権限を持つユーザーのみが変更前の情報を参照できます。

➢ 関連情報

ユーザー情報の編集

カスタムアカウントレベルの追加

カスタムアカウントレベルの追加

カスタムアカウントレベルを作成し、ユーザーの BioStar 操作権限にカスタムアカウントレベルの割り当てを行えます。

メモ

管理者メニューの設定は、適用された AC ライセンスの種類によって異なる場合があります。

1 [設定] > [アカウント]をクリックします。

2 [カスタムレベルの追加]をクリックします。

3 必要な項目に入力または選択してください。
適用された AC ライセンスの種類によって、表示される内容が異なる場合があります。

項番	項目名	説明
1	名前	アカウントレベル名を入力します。
2	説明	アカウントレベルの簡単な説明を入力します。

3	管理項目設定	項目ごとに詳細な権限を設定します。 グループを選択して、各メニューの編集権限と読み取り権限を割り当てることができます。 管理項目設定は、ユーザーグループ、端末グループ、ドアグループ、エレベーターグループ、アクセスグループ、ゾーン種別、グラフィックマップグループに対して設定でき、既に作成されているグループ情報に基づいて設定できます。 必要なグループがない場合は、そのメニューに新しいグループを追加します。 グループの作成の詳細については、「ユーザーグループの追加と管理」、「端末グループの追加と管理」、「ドアグループの追加と管理」、「エレベーターグループの追加と管理」、「アクセスグループの追加と管理」、「グラフィックマップ グループの追加と管理」を参照してください。
4	管理者メニュー設定	メニューの編集権限と読み取り権限を設定します。 メニューごとに異なる権限の設定を行えます。 ・ 編集: メニューの項目を追加、編集、削除する権限 ・ 読込: メニューの項目を表示する権限 **メモ** 各メニューに編集権限を与えると追加ボタンが有効になります。 ただし、ダッシュボードや設定メニューには追加ボタンがないため[N/A]と表示されます。 また、アクセスコントロールメニューの追加ボタンは、管理項目設定でアクセスグループがすべてのアクセスグループに設定され、編集権限が割り当てられている場合にのみ有効になります。
5	ユーザー追加	権限を割り当てるユーザーの追加を行えます。 ユーザーを追加する場合は、[+追加]をクリックしてユーザーを追加します。 ゴミ箱ボタン( )をクリックすると、割り当て済みのユーザーが削除されます。

4 [適用]をクリックして設定を保存します。

メモ

- 管理項目設定と管理メニュー設定の構成については、次の例を参照してください。

項目名	説明
ユーザー	「ユーザーグループ 01」のユーザー情報を表示できます。 ただし、新しいユーザーの追加、既存ユーザーの編集はできません。
端末	「端末グループ 01」の端末情報を表示できます。 ただし、新しい端末の追加、既存の端末の編集はできません。
ドア	「ドアグループ 01」に含まれるドアの設定の編集や削除ができます。 「ドアグループ 01」に含まれるドアの端末を編集できます。 「ドアグループ 01」に新しいドアを追加することができます。
エレベーター	すべてのエレベーターの設定を表示できます。 ただし、新しいエレベーターの追加、既存エレベーターの編集はできません。
ゾーン	権限がありません。
アクセスコントロール	「AC グループ」に含まれるアクセスグループの設定を削除できます。 ユーザーおよびユーザーグループを「AC グループ」に追加および削除できます。
モニタリング	「端末グループ 01」に含まれる端末のイベントを確認できます。 また、端末状態、ドア状態、ゾーン状態、警告履歴を確認できます。 「すべてのグラフィカルマップ」のグラフィックマップも表示されます。 ただし、各状態を制御することはできません。

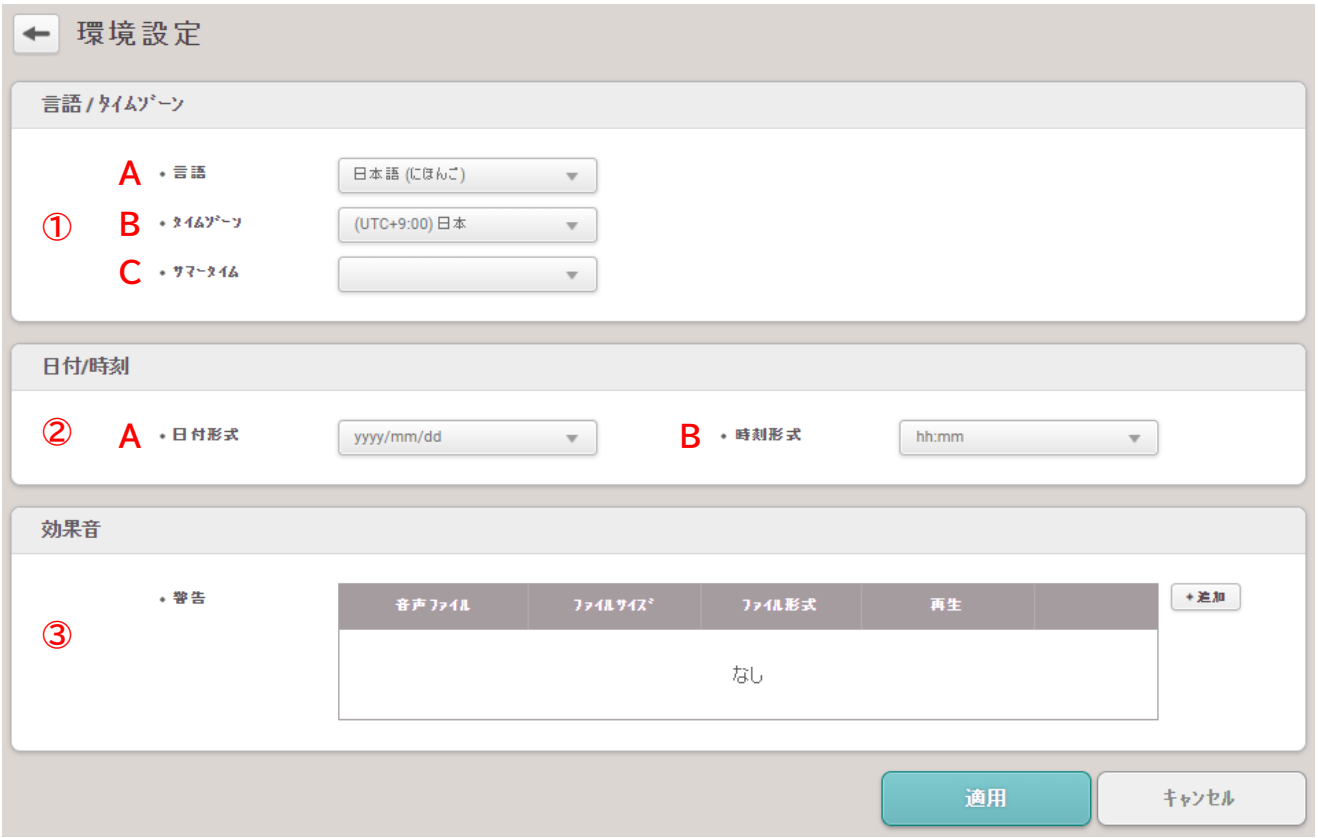
- 管理項目設定と管理メニュー設定が一致していないと、その項目に権限が付与されません。
  このカスタムアカウントレベルが割り当てられたユーザーで権限が無いメニューを選択すると、権限が無い旨のメッセージが表示されます。
- カスタムアカウントレベルの作成数に制限はありません。

設定

言語、タイムゾーン、日付/時刻の変更や、警報として使用する音声ファイルのアップロードを行えます。

1 [設定] > [環境設定]をクリックします。

2 必要なフィールドを編集します。



項番	項目名	説明
1	言語 / タイムゾーン	BioStar 2 の言語とタイムゾーンの設定を設定できます。
1-A	言語	使用する言語を選択します。
1-B	タイムゾーン	使用するタイムゾーンを選択します。
1-C	サマータイム	BioStar 2 サーバーに適用するサマータイムを選択します。 サマータイムが登録されていない場合は、サマータイムを参照してください。
2	日付/時刻	BioStar 2 で使用する日付と時刻の形式を設定できます。
2-A	日付形式	日付形式を変更します。
2-B	時刻形式	時刻形式を変更します。
3	音	BioStar 2 で使用する音声ファイルをアップロードできます。 1 [+追加]をクリックします。 2 [参照]をクリックしてファイルを選択します。 3 .wav ファイルまたは .mp3 ファイルを選択し、[開く] をクリックします。

		4 ［追加］をクリックしてアップロードします **メモ** ・ 音声ファイルは .wav または .mp3 形式である必要があります。 ・ ファイルの最大サイズは 10MB です。

3 ［適用］をクリックして設定を保存します。

➢ 関連情報

警告

カード

カードの状態、割り当てユーザー、ブラックリストなどの表示や制御を行えます。

1 [設定] > [カード]をクリックします。

登録されているカードの一覧が表示されます。

2 未割当カード、割当済みカード、ブラックリストカードを選択すると、選択したカードの一覧が表示されます。

メモ

カードが無効化された状態で割り当てていたユーザーを削除した場合のカードは、ブラックリストカード一覧に表示されます。カードのブラックリスト状態を解除するには、カードを選択して[有効化]をクリックします。

Wiegand カードのデータ形式の変更

Wiegand カードのデータフォーマットの一括変更を行えます。

メモ

ユーザーに割り当て済みのカードのデータフォーマットが変更されます。

1 [設定] > [カード]をクリックします。

2 機能ボタン(•••)をクリックし、[すべての Wiegand フォーマット]を選択します。

3 現在のリストから変更するカードデータフォーマットを選択し、変更のリストから変更するカードデータフォーマットを選択します。

4 [適用]をクリックして、カード データ形式を変更します。

カードフォーマット

カードの Wiegand 種別や、スマートカードやモバイルカードのレイアウトの設定を行えます。

1 [設定] > [カードフォーマット]をクリックします。

2 Wiegand とスマート/モバイルカードの情報を参照して設定します。

Wiegand カード

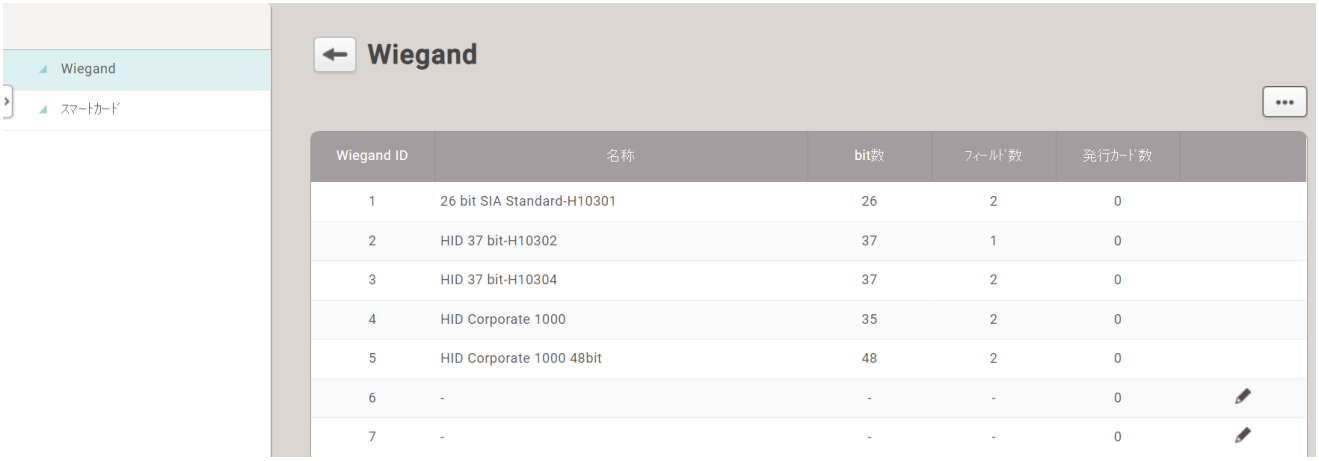
Wiegand カードデータの読み取りフォーマットを設定できます。

メモ

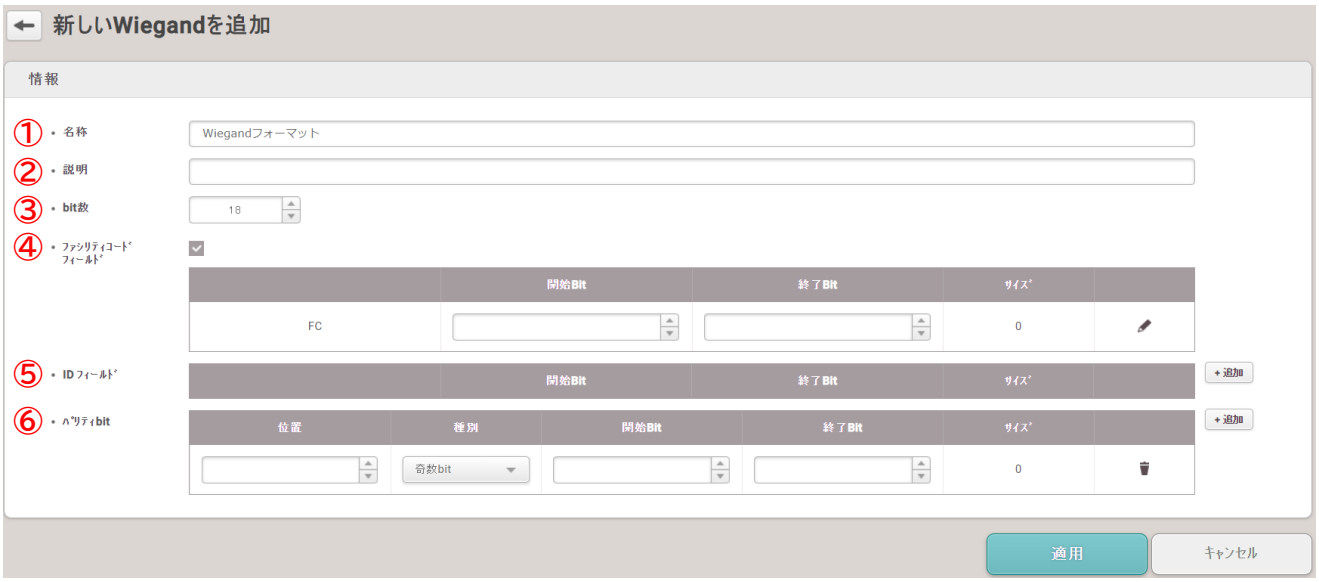
ユーザーに割り当て済みのカードのデータフォーマットが変更されます。

1 [設定] > [カードフォーマット]をクリックします。

2 Wiegand をクリックします。



3 リストからえんぴつマーク(✎)をクリックして設定します。



項番	項目名	説明
1	名称	Wiegand フォーマットの名前を入力します。
2	説明	簡単な説明を入力します。
3	ビット数	総ビット数を入力します。
4	ファシリティコードフィールド	ファシリティコードを使用するかどうかを設定できます。ファシリティコードを使用す

		る場合は、チェックボックス(☐または☑)をクリックし、スタートビットとエンドビットを入力します。
5	ID フィールド	使用する ID のスタート bit とエンド bit を入力します。 **[+追加]**をクリックして、ID フィールドを追加します。
6	パリティ bit	[+追加]をクリックして、パリティ bit を追加します。 使用するパリティ bit の位置とスタート bit とエンド bit を入力します。 **メモ** パリティビットを追加するには、ビット数を入力する必要があります。

4 [適用]をクリックして Wiegand フォーマットを追加します。

メモ

定義済みのフォーマットは、編集または削除できません。

スマート/モバイルカード

MIFARE、iCLASS、DESFire、iCLASS Seos、モバイルなどのスマートカードのレイアウトの設定を行えます。

メモ

モバイルカードを設定するには、[設定] > [サーバー]の[ユーザー/端末管理]タブで[モバイルカードの登録]を[有効]に設定します。

1 [設定] > [カードフォーマット]をクリックします。

2 [スマートカードの追加]をクリックして、設定を設定します。

項番	項目名	説明
1	スマートカード種別	カスタムスマートカードレイアウトを設定するオプションをオンにします。
2	名称	スマートカードの名前を入力します。
3	セカンダリーキー	Web サイトのセカンダリキーを使用するかの設定を行えます。 有効が設定されている場合、セカンダリキーを設定できます。 セカンダリサイトキーが設定されている場合、カードのベーシックサイトキーが一致しない場合、セカンダリサイトキーを使用して認証が行われます。
4	スマートカード設定	MIFARE、iCLASS、DESFire、iCLASS Seos、モバイルなどのスマートカードの構造を設定できます。 プライマリサイトキーとセカンダリサイトキーは、16 進数の値のみをサポートします。 画面の右側のフィールドにキーの値を入力し、「ASCII->16 進数 変換」をクリックします。 変換された値をサイトキーとして使用します。 ・ DESFire アドバンスド: サードパーティ発行の DESFire カードが使用可能です。DESFire のみ設定可能です。 **メモ** DESFire アドバンスドを使用するには、App マスターキー、App マスターキーポート番号、ファイル読出アクセスキー、ファイル読出アクセスキーポート番号、ファイル書込アクセスキー、ファイル書込アクセスキーポート番号、App ID、ファイル ID 、暗号種別の情報を正しく入力してください。. ・ プライマリーキー: スマートキーとカードリーダー間の通信の暗号化鍵です。 ・ セカンダリキー: セカンダリ Web サイトキーを設定できます。セカンダリーキーを設定すると、カードのプライマリーキーが一致しない場合にセカンダリーキーを使用して認証が行われます。セカンダリーキーは、上部にあるセカンダリーキーをアクティブにすることによってのみ入力できます。 ・ 開始ブロックインデックス: 各テンプレートが保存される開始ブロックを選択します。このブロックは、ユーザー情報が保存されるブロックのインデックスです。ユーザーが既にスマートキーを持っている場合は、保存できるブロックを設定します。MIFARE、iCLASS のみ設定可能です。 ・ App ID :アプリ ID を設定します。ファイル ID を含むディレクトリの役割を果たします。DESFire のみ設定可能です。 ・ ファイル ID :ファイル ID を設定します。DESFire のみ設定可能です。 ・ 暗号種別: 暗号種別を DES/3DES または AES に設定できます。DESFire のみ設定可能です。

		・ ADF アドレス値: デジタル認証情報が保存され、iCLASS Seos カードのみ設定可能です。 ・ スキップバイト: カード番号の読み取り開始点を設定できます。設定は、カスタム スマート カードモードの MIFARE および DESFire でのみ使用できます。 ・ データサイズ:（設定した Primary Key と Secondary Key がカードの設定値と同じ場合）読み込むカードのデータサイズを設定できます。設定は、カスタム スマート カードモードの MIFARE および DESFire でのみ使用できます。
5	レイアウト	ユーザー情報や指紋情報を記録するレイアウトを変更することが可能です。 ・ テンプレート数: レイアウトに含める指紋テンプレートの数を設定します。 ・ テンプレートサイズ: 指紋テンプレートで使用されるバイト数を設定します。 ・ 顔テンプレート利用: 顔テンプレートを使用するかどうかを選択します。 ・ 顔テンプレートサイズ: 顔テンプレートが使用するバイト数を設定します。 **メモ** 顔テンプレートは、FaceStation F2 でのみ使用できます。

3 [適用]をクリックして、スマートカード設定を登録します。

サーバー

BioStar 2 サーバー情報、ユーザー管理、端末管理、自動アップグレード設定の設定を行えます。

1 [設定] > [サーバー]をクリックします。

一般設定

項目	説明
一般設定	BioStar 2 の一般情報を設定できます。 ・BioStar IP アドレス: サーバーの IP アドレスを設定します。 特定の IP アドレスを使用するように設定を行えます。 ・BioStar ポート: サーバーポートを設定します。 ・セッションタイムアウト: セッションタイムアウトの時間を設定します。 ログイン後、設定された時間 BioStar 2 にアクティビティがない場合、セッションが切れ自動的にログアウトされます。 ・ログのアップロード: イベントログのアップロード方法を選択します。 サーバーとのリアルタイム通信が困難な場合は、この設定を[手動]にします。 ・Web サーバープロトコル: サーバーとの通信プロトコルを設定します。

ユーザー/端末管理

項番	項目名	説明
1	ユーザー/端末管理	ユーザーや端末の管理を行えます。 **メモ** ・ 自動ユーザー同期に[端末ごと(アクセス権限があるユーザーのみ)]として選択した場合、アクセスグループに属さない端末に格納されているユーザーは、サーバーで管理されません。 このオプションを使用する場合は、[端末]メニューに移動し、各端末の[データ削除&端末同期]をクリックして同期を続行します。 ・ 自動ユーザー同期に[端末ごと(アクセス権限があるユーザーのみ)]を選択しても、次のような特別な目的で設定されたアクセスグループは、端末のアクセスグループに関係なく同期されます。 ・端末とエレベーターに設定された二重認証のアクセスグループ ・アンチパスバックゾーンのバイパスグループ ・スケジュールロックゾーンのバイパスグループ ・スケジュールアンロックゾーンのスケジュール解除認証のアクセスグループ ・警備警報ゾーンのアクセスグループ ・自動ユーザー同期に[端末ごと(アクセス権限があるユーザーのみ)]として自動ユーザー同期を選択しても、BioStar 操作権限が端末管理者のユーザーは、アクセスグループに関係なく同期されます。 ・NFC カードは、以下の条件でサポートされています。 モバイル端末 OS: Android 5.0 Lollipop 以降、Android 10 以前 BioStar 2 Mobile: 2.4.1 以降 Xpass S2:XPS2M-V2 FW 2.4 以降 BioStation 2:BS2-OMPW、BS2-OIPW FW 1.4 以降、FW 1.8 以前

		BioStation A2: BSA2-OMPW、BSA2-OIPW FW 1.3 以降、FW 1.7.1 以前 BioStation L2: BSL2-OM FW 1.2 以降 BioEntry W2: BEW2-OAP、BEW2-ODP FW 1.1 以降、FW 1.5 以前 FaceStation 2：FS2-D、FS2-AWB FW 1.3.1 以前 BioLite N2：BLN2-ODB、BLN2-OAB、BLN2-PAB FW 1.2 以前 XPass D2：XPD2- MDB、XPD2-GDB、XPD2-GKDB FW 1.3 以前 FaceLite: FL-DB FW 1.1 以前 XPass 2: XP2-MDPB、XP2-GDPB、XP2-GKDPB FW 1.0 以降 BioEntry P2: BEP2-OD、BEP2-OA FW 1.0 以降 BioEntry R2: BER2-OD FW v1.1.0 以降 ・ BLE カードは以下の条件でサポートされています。 モバイル端末 OS：Android 5.0 Lollipop 以降、Android 10 以前／iOS 9.0 以降 BioStar 2 Mobile 2.4.1 以降 FaceStation 2：FS2-AWB FW 1.3.1 以前 BioLite N2：BLN2-ODB、 BLN2-OAB、BLN2-PAB FW 1.2 以前 XPass D2: XPD2-MDB、XPD2-GDB、XPD2-GKDB FW 1.3 以前 FaceLite: FL-DB FW 1.1 以前 XPass 2: XP2-MDPB、XP2- GDPB、XP2-GKDPB FW 1.0 以降 ・ モバイルカードまたはモバイルアクセスのいずれかをご利用いただけます。ファームウェアは、モバイルカードまたはモバイルアクセスを同時にサポートしていません。 ・ ユーザーID 種別を「英数字」から「数字のみ」に変更すると、BioStar 2 に登録されているすべてのユーザー情報を削除する必要があります。 ・ ユーザーID 種別を変更できる端末とファームウェアのバージョンは以下です。 CoreStation FW 1.0.0 以降 FaceStaion 2 FW 1.0.0 以降 FaceLite FW 1.0.0 以降 BioEntry W2 FW 1.1.0 以降 BioStation L2 FW 1.2.0 以降 BioStation A2 FW 1.3.0 以降 BioStation 2 FW 1.4.0 以降 BioLite N2 FW 1.0.0 以降 BioEntry P2 FW 1.0.0 以降 BioEntry R2 FW 1.0.0 以降 XPass 2 FW 1.0.0 以降 XPass D2 FW 1.0.0 以降 Xpass FW 2.4.0 以降 Xpass S2 FW 2.4.0 以降

		X-Station 2 FW 1.0.0 以降 BioStation 3 FW 1.0.0 以降 ・ カスタムユーザーフィールドの[順番]フィールドの値を変更すると、[ユーザー]メニューでのカスタムフィールドの位置が変更されます。 ・ カスタムユーザーフィールドの「数字入力ボックス」を選択した場合、0 から 4294962795 までの数値が許可され、文字は許可されません。 ・ カスタムユーザーフィールドの「テキストボックス」を選択した場合、最大 32 文字まで使用できます。 ・ カスタムユーザーフィールドの「コンボボックス」を選択した場合、以下の画像のようにコンボボックスフィールドを設定する場合は、データフィールドに「c-1;c-2;c-3;」と入力する必要があります。 
A	自動ユーザー同期	ユーザー情報の同期方法を変更します。 ・ 「利用しない」に設定すると、サーバーのユーザー情報は端末と同期されません。 ・ 「すべての端末」に設定すると、サーバーのユーザー情報は端末と同期されます。 ・ 「すべての端末(端末からのユーザー更新を含む)」に設定すると、サーバー上のユーザー情報が、サーバーに登録されているすべての端末と同期されます。ただし、端末上で変更されたユーザー情報はサーバーには同期されず、端末上で追加されたユーザー情報のみがサーバーに同期されます。 ・ 「端末ごと(アクセス権限があるユーザーのみ)」を選択すると、アクセス グループに属するデバイスのみが変更と自動的に同期されます。
B	モバイルカード登録	モバイルカードを使用するには、[有効]に設定します。
C	指紋テンプレートフォーマット	指紋テンプレートの形式を設定します。 SUPREMA、ISO、ANSI378 から選択します。 ユーザーの指紋テンプレートが端末に残っている場合、別の形式を選択することはできません。
D	ユーザーID 種別	ユーザーID に「数字のみ」または「英数字」を設定できます。 ユーザーID 種別が「英数字」に設定されている場合、BioLite Net、BioEntry Plus、BioEntry W は使用できません。 また、Xpass および Xpass S2 に保存されているすべてのユーザーが削除され、ネットワーク以外のすべての設定が初期化されます。

E	登録用端末	指紋とカードの登録に頻繁に使用する端末を登録用端末として特別に設定できます。 [+追加]をクリックして端末を選択します。
F	カスタムユーザーフィールド	追加のユーザー情報用にカスタムユーザーフィールドを追加できます。 これらのフィールドは[ユーザー]ページに表示されます。 カスタムユーザーフィールドには、「数字入力ボックス」、「テキスト入力ボックス」、「コンボボックス」の 3 種類があります。 カスタムユーザーフィールドに「コンボボックス」を選択した場合、それぞれ 32 文字の最大 20 項目を追加でき、各項目はセミコロン(;)で区切ります。
G	アクセスオンカードの発行時、個人情報と資格情報を削除	ユーザーの認証資格をスマートカードに保存するアクセスオンカードを発行する場合に設定します。設定すると、アクセスオンカードを発行する時にユーザーのデータと認証資格を自動的に削除されます。
H	アクセスコントロールイベントログ保存期間	アクセスコントロールイベントログを保存する期間を設定できます。
I	顔資格画像非表示	・顔認証情報のプレビュー画像を非表示: ユーザーのプライバシーを保護するために、顔認証情報の登録時にプレビュー画像を非表示にすることができます。このオプションを有効にすると、ユーザーの顔またはビジュアル顔を登録するときにプレビューが提供されません。

サーバーマッチング

項目	説明
サーバーマッチング	サーバーマッチングを設定できます。 サーバーマッチングを使用する場合、ユーザーの指紋は、端末ではなく BioStar 2 にて照合されます。 サーバーマッチングは、アドバンスド以上のライセンスが有効化されている場合に表示されます。 ・ サーバーマッチングを使用: サーバーマッチングを有効/無効にします。 ・ 最大同時サーバーマッチングカウント: 同時に実行できるマッチングの数を設定できます。 ・ 高速モード: 指紋照合速度を設定できます。 ・ セキュリティレベル: サーバーマッチングの指紋と顔のセキュリティレベルを設定できます。 セキュリティレベルが高く設定されるほど、本人拒否率（FRR）が発生する可能性があります。 **メモ** 最大同時サーバーマッチング数は PC の CPU 性能に依存します。

システムログレベルの設定

項目	説明
システムログレベル設定	データベースに保存するシステムログの期間とログレベルを設定できます。 システムログの保存期間は最大 120 日まで設定可能で、0 を設定するとログは削除されません。 システムログは、事前に定義されたカテゴリに従って管理され、ログレベルは、トレース、デバッグ、インフォメーション、ワーニング、エラーに分類されます。 高いレベルには、すべての低いレベルのログが含まれます。 たとえば、「トレース」に設定すると、ログレベル「デバッグ、インフォメーション、ワーニング、エラー」のログを保存します。

2 [適用]をクリックして設定を保存します。

➢ 関連情報

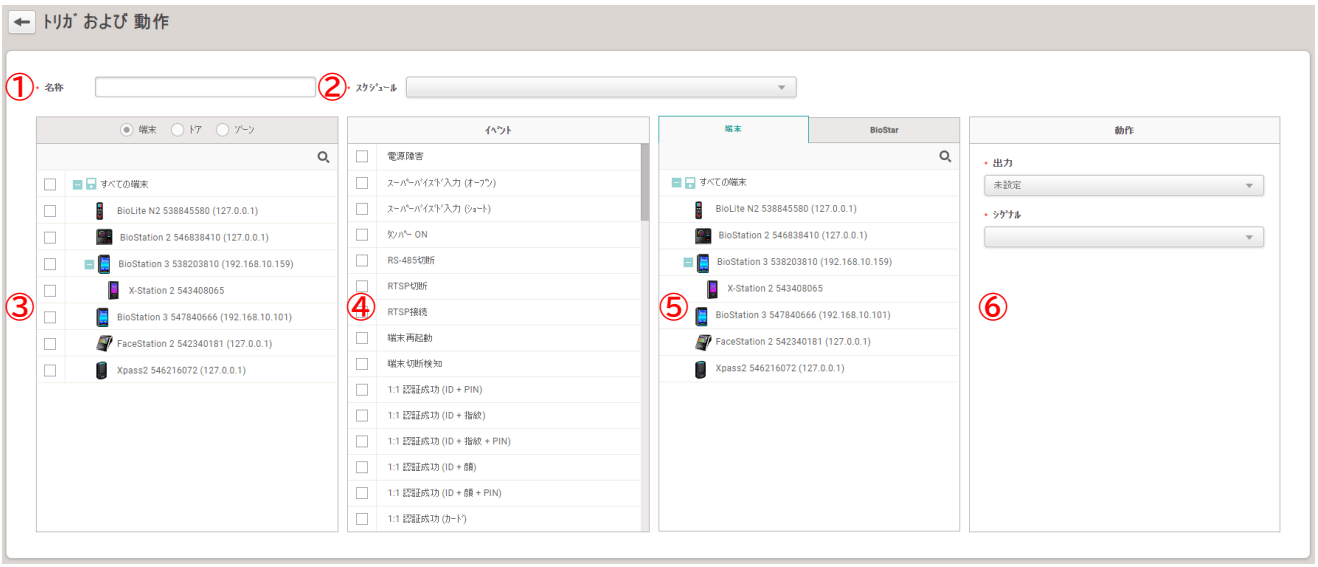
リアルタイムログ

トリガーおよび動作

端末、ドア、ゾーンで特定のイベントが発生したときに特定の動作を実行するように、端末や BioStar の設定を行えます。

1 [設定] > [トリガーおよび動作]をクリックします。

2 [トリガーおよび動作の追加]をクリックして、設定を設定します。



項番	項目名	説明
1	名称	トリガーおよび動作の名前を入力します。
2	スケジュール	スケジュールを選択します。 **メモ** ・目的のスケジュールが見つからない場合は、[スケジュールの追加]をクリックして作成します。 ・スケジュールの設定の詳細については、スケジュールを参照してください。
3	端末、ドア、ゾーン	特定のイベントをモニタリングする端末/ドア/ゾーンを選択します。 複数の端末/ドア/ゾーンを選択できます。 端末/ドア/ゾーンは、BioStar サーバーから切断されている場合でも独立して動作します。 **メモ**

		・ AC ライセンスのアドバンスドが適用されると、ゾーンが表示されます。
4	トリガーイベント	トリガーイベントを設定します。少なくとも 1 つのイベントを選択する必要があります。 **メモ** イベントリストは、端末、ドア、ゾーンで選択したオプションに応じて、異なる方法で適用する必要があります。
5	端末 BioStar	アクションを実行する端末を選択します。 端末、または、BioStar 2 の中から選択します。
6	動作	選択したトリガーイベントが発生したときに送信する信号を設定します。 BioStar 2 からログが送信される電子メールを設定することもできます。 ・BioStar を選択し、歯車アイコン( )をクリックしてメールサーバー情報を設定します。 ・メールアドレスを追加するには、[+追加]をクリックしてメールアドレスを入力します。 「OK」をクリックして受信者を追加します。

3 [適用]をクリックして設定を保存します。

メモ

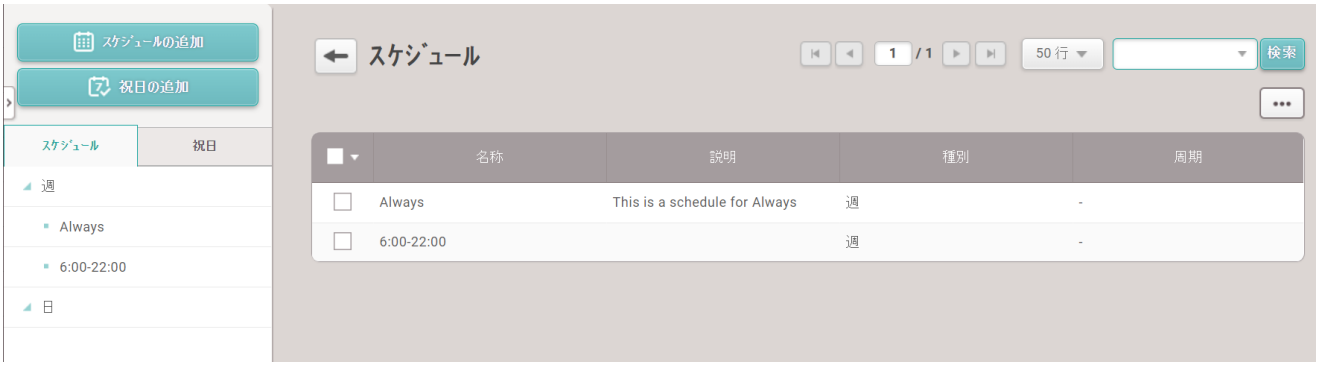
メールサーバーについては、弊社から提供するものではなくサポート対象外となります。

スケジュール

アクセススケジュールや祝日スケジュールの追加を行えます。

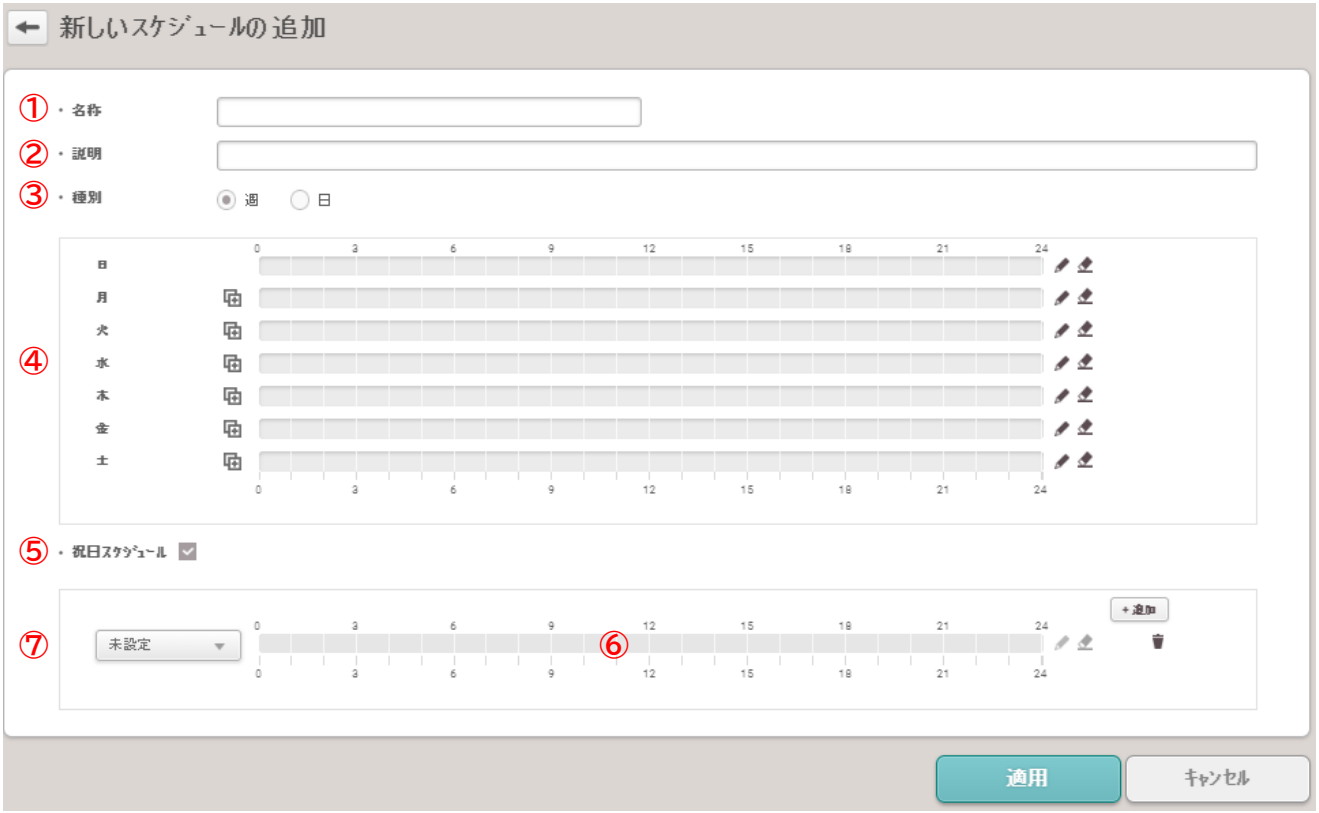
新しいスケジュールの追加

1 [設定] > [スケジュール]をクリックします。



2 [スケジュールの追加]をクリックします。

3 フィールドに必要な情報を入力し、曜日ごとにスケジュールを設定します。



項番	項目名	説明
1	名前	スケジュールの名前を入力します。
2	説明	スケジュールの簡単な説明を入力します。

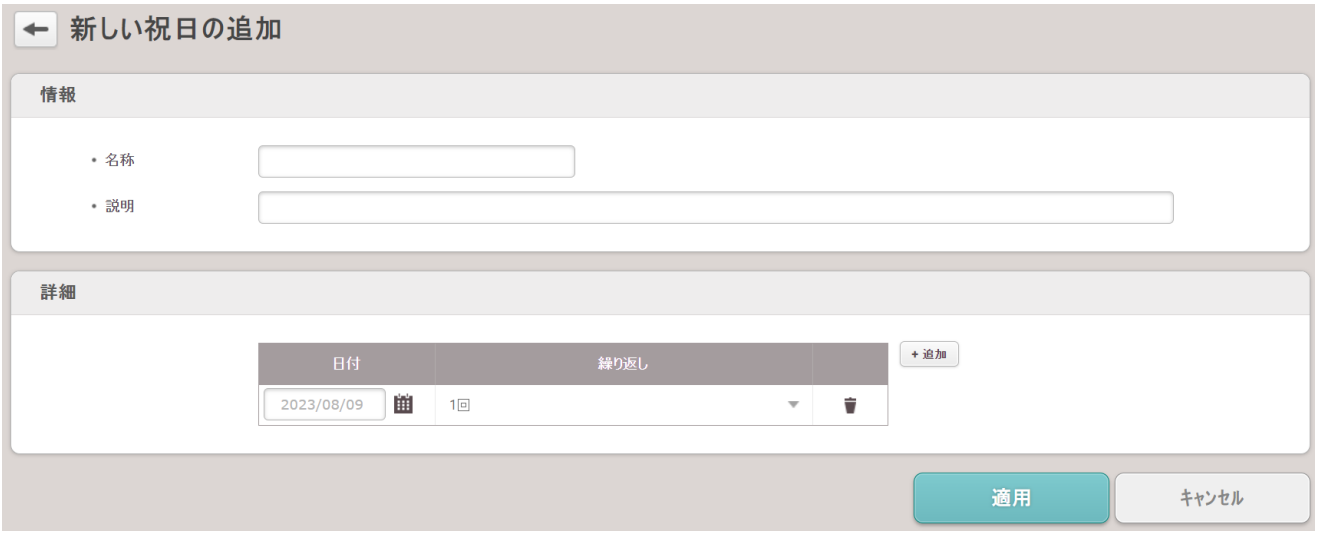
3	種別	スケジュール種別として、[週]または[日]を選択します。 [日]に設定すると、周期と開始日の選択を行えます。
4	タイムスロット	タイムスロットをクリックして目的のスケジュールを設定し、[OK]をクリックします。  ・曜日ごとまたは日ごとに最大 5 つのタイムスロットを設定できます。 ・スケジュールを設定したら、コピーボタン()をクリックして直上で設定した時間帯をコピーします。 ・タイムスロットのえんぴつマーク()をクリックして編集します。 消しゴムボタン()をクリックすると、設定した時間帯の削除を行えます。
5	祝日スケジュール	祝日スケジュールを適用するかどうかを指定します。 オプションを選択すると、詳細設定が表示されます。
6	祝日のタイムスロット	タイムスロットをクリックして、目的の祝日スケジュールを設定します。 ・タイムスロットのえんぴつマーク()をクリックして編集します。 消しゴムボタン()をクリックすると、設定した時間帯の削除を行えます。
7	祝日選択	定義済みの祝日を選択します。 ・[+追加]をクリックして、定義済みの休日を追加します。 ・祝日を削除するには、ゴミ箱ボタン()をクリックします。

4 [適用]をクリックして、スケジュールを追加します。

祝日スケジュールの追加

1 [設定] > [スケジュール]をクリックします。

2 [祝日の追加]をクリックします。



3 名前と説明を入力し、[+追加]をクリックします。

4 カレンダーマーク()をクリックして日付を選択し、繰り返し回数を設定します。

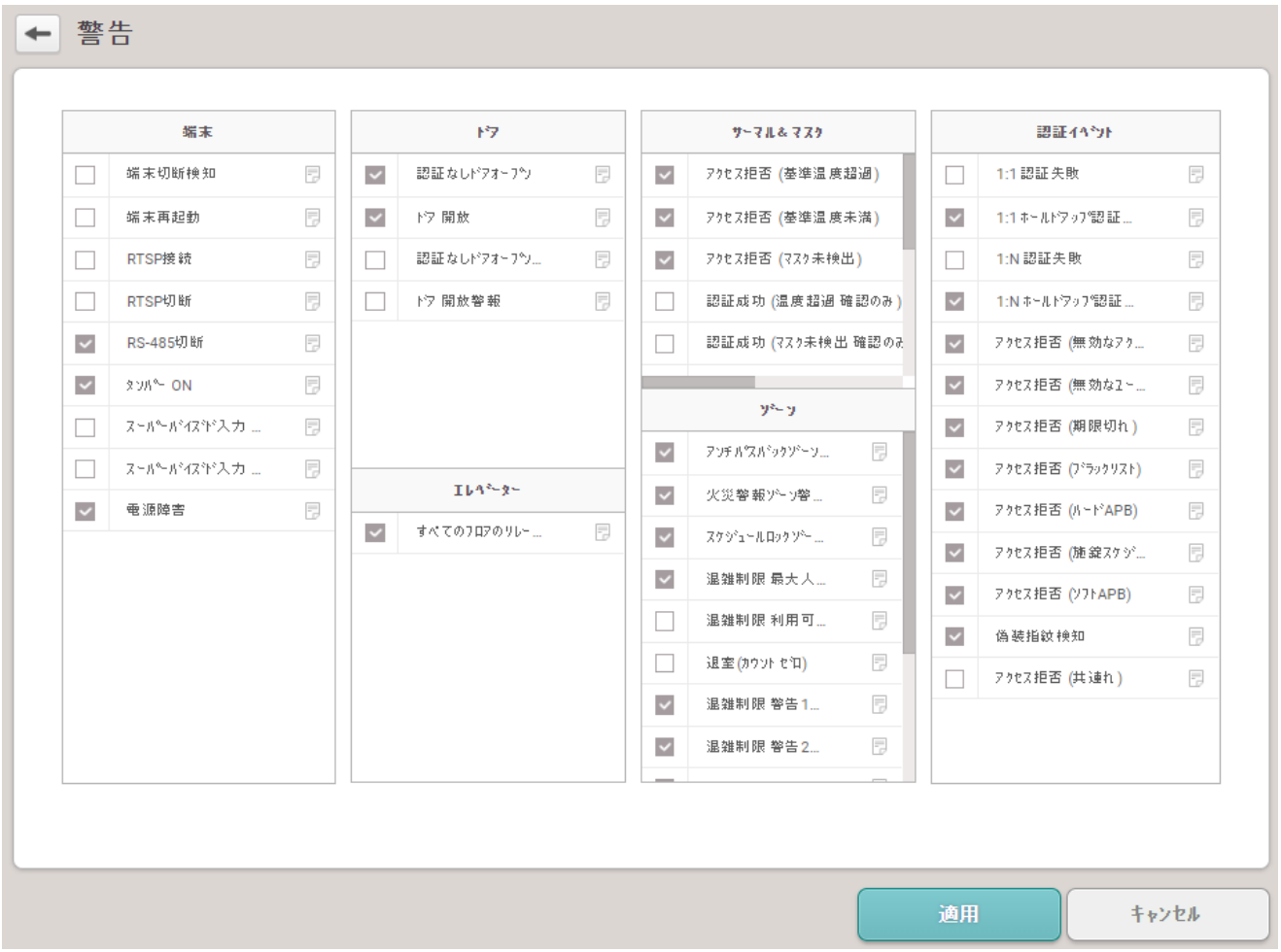
5 [適用]をクリックして、祝日スケジュールを追加します。

警告

端末、ドア、ゾーンで特定のイベントが発生したときに表示する警告タイプとメッセージを設定できます。

設定を調整して、BioStar 2 が警告の発生時にアップロードされた音声ファイルを再生するように設定できます。

1 [設定] > [警告]をクリックします。



2 画面に表示するイベントの種類を選択します。

3 メモアイコン( )をクリックして、画面に表示するメッセージを入力します。

対応するイベントの発生時に再生する音声ファイルをアップロードした場合は、[音声ファイル]のリストから選択し、[再生オプション]を設定します。

再生する音声ファイルがない場合は、設定の[音声]を参照してアップロードします。

4 [適用]をクリックして、警告メッセージを保存します。

5 [適用]をクリックして変更を保存します。

➢ 関連情報

設定

HTTPS

BioStar 2 に HTTPS 経由でアクセスするには、BioStar 2 がインストールされている IP アドレスを確認し、証明書をインストールする必要があります。

cert-register.exe（証明書登録ツール）をダウンロードが可能です。

証明書適用手順については、弊社のインストール手順書をご覧ください。

メモ

BioStar 2.5.0 は、デフォルトの通信プロトコルとして HTTPS を使用します。

クラウド(クラウド経由アクセス)

クラウド経由アクセスは、BioStar 2 サーバーにインターネットからアクセスする機能です。

メモ

- クラウド経由アクセス機能を使用するには、AC ライセンスのスタンダード以上のライセンスが必要です。
- クラウド経由アクセス機能を使用している場合、Internet Explorer または Edge 経由で BioStar 2 に接続できません。
- クラウド経由アクセスを使用して BioStar 2 にアクセスする場合、リポートメニューにアクセスできません。

1 [設定] > [クラウド]をクリックします。

2 必要なフィールドを編集します。

項番	項目名	説明
1	クラウド経由アクセス	クラウド経由アクセス機能を使用するには、使用に設定します。 **メモ** ・ クラウド経由アクセスを使用する場合、パスワードレベルは[中]または[強]に設定する必要があります。詳細については、サーバー を参照してください。
2	サブドメイン名	使用するサブドメインを入力します。 サブドメインは、ユーザーID と同じように一意の値を設定します。 会社名などの一意の文字列を使用してください。
3	管理者の E メール	管理者のメールアドレスを入力します。
4	クラウドサーバーアドレス	クラウドサーバーのアドレスが表示されます。
5	バージョン	クラウドサーバーのバージョンが表示されます。

6	クラウド利用ポート	クラウド経由アクセスを使用するポート番号です。 デフォルトは 52000 に設定されています。 クラウドが正常に動作しない場合は、BioStar 2 がインストールされている PC のファイアウォール設定から、インバウンドおよびアウトバウンドのルールを変更します。 以下は例であり、設定によって、使用ポートが異なる可能性があります。 ・インバウンドルールに追加するポート: BioStar 2 サーバーポート（デフォルト値: 80、ユーザー指定）、BioStar 2 クラウド ポート（デフォルト値: 52000、ユーザー指定） ・アウトバウンドルールに追加するポート: 4443、ngrok によって使用されるすべてのポート

3 ［適用］をクリックして変更を保存します。

メモ

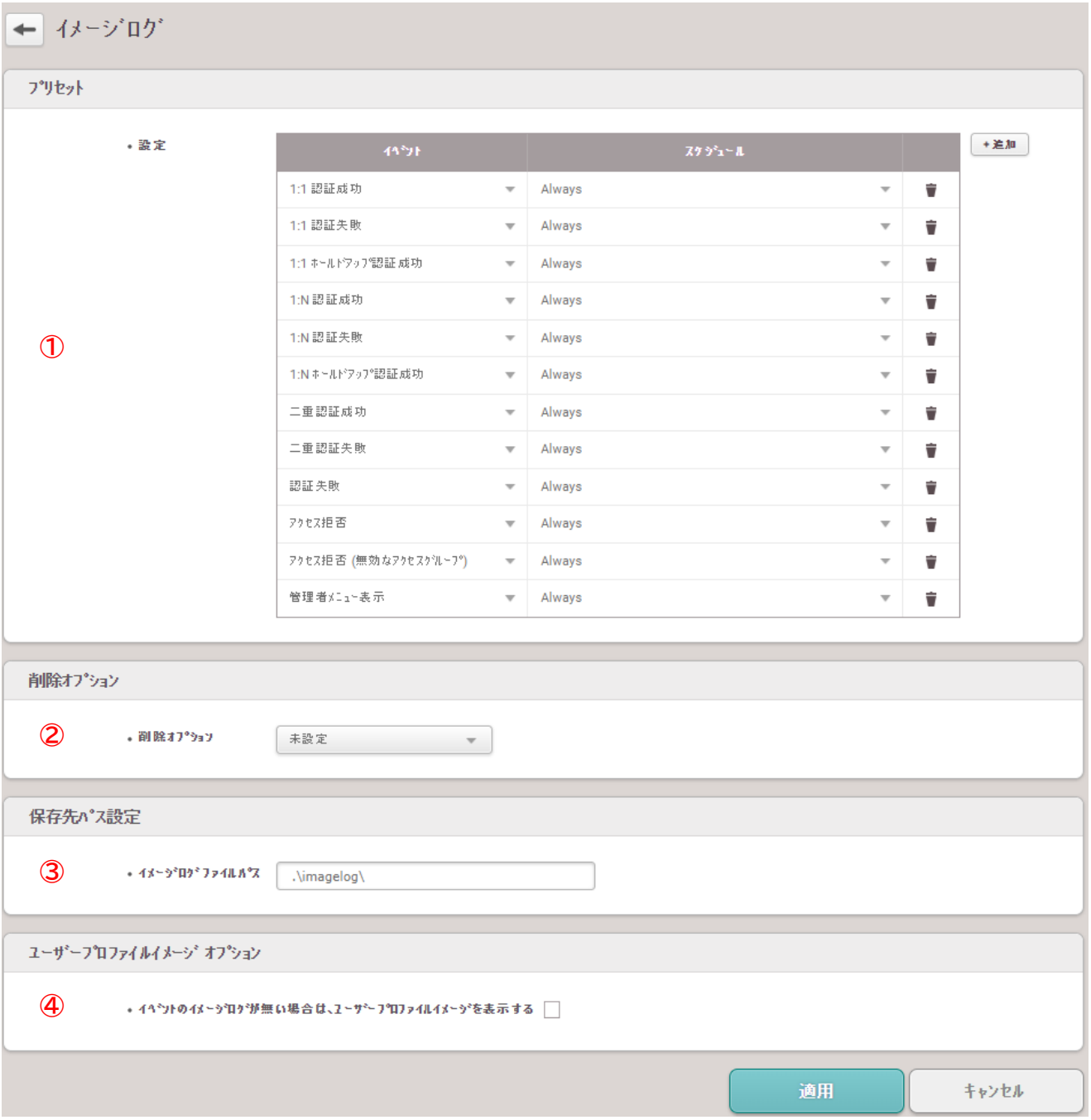
・ メール転送には最大 10 分かかる場合があります。
・ クラウドの場合、BioStar サーバーは常に起動している必要があります。
サーバーの接続が 1 週間以上失われた場合は、電子メールで再登録の手続きを行う必要があります。

イメージログ

イメージログの削除オプション、端末からのイメージログを取得するイベントなどの設定を行えます。

1 [設定] > [イメージログ]をクリックします。

2 必要なフィールドを編集します。



項番	項目名	説明
1	プリセット	イメージログを取得するイベントを設定できます。 [+追加]をクリックすると、イベントとスケジュールを追加できます。

		メモ 目的のスケジュールが見つからない場合は、[+スケジュールの追加]をクリックして希望の条件を設定します。
2	削除オプション	イメージログの削除条件を設定できます。 ・ 削除オプション: イメージログを削除する条件を設定できます。 ・ イメージログ量: 削除オプションで設定したい条件を設定できます。(MB、GB) ・ 削除サイクル: 「削除オプション」と「イメージログ量」で設定したイメージログの削除条件を実行する周期を設定できます。
3	保存先パス設定	イメージログファイルを保存するパスを設定します。 **メモ** 保存パスは、作成済みのディレクトリに設定する必要があります。
4	ユーザープロフィールイメージオプション	このオプションがオンの場合、ユーザーに関連するイベントが発生したときに、ユーザーに登録されているプロフィール画像がイベントログとリアルタイムログページに表示されます。 このオプションは、カメラが搭載されていない端末を使用している場合に特に便利です。 **メモ** ユーザープロフィール画像オプションがオンになっていても、イベントにイメージログがある場合は、端末のカメラからキャプチャされた画像が表示されます。

3 [適用]をクリックして変更を保存します。

メモ

[設定] > [イメージログ]で設定されたデフォルト設定は、端末には適用されません。端末のイメージログを追加または変更するには、イメージログを参照してください。

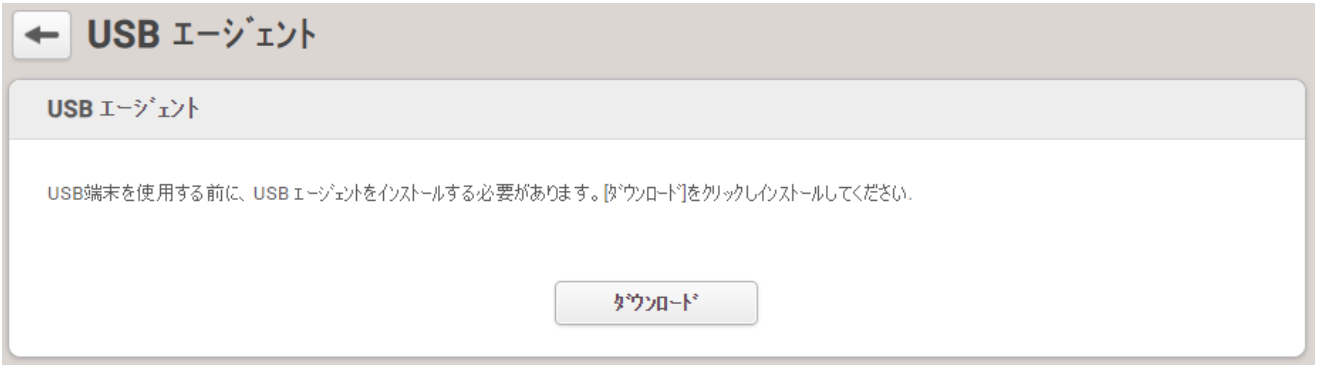
USB エージェント

クライアント PC から BioStar 2 にログインし、カード登録や指紋登録などで USB 登録機を使用する場合は、USB デバイスエージェントをインストールする必要があります。
USBデバイスエージェントのインストール手順は弊社が提供するインストール手順書をご覧ください。

メモ

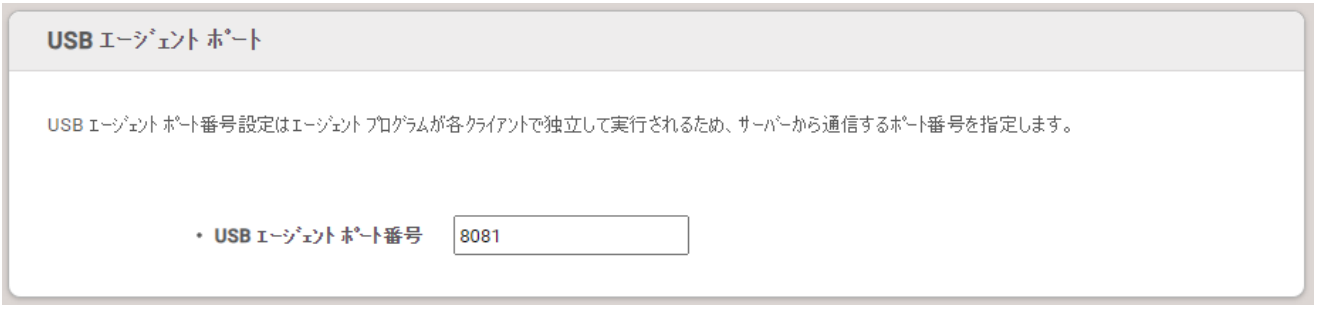
Windows でユーザーアカウント制御が有効になっている場合、USB エージェントを自動的に実行することはできません。ユーザーアカウント制御を無効にするか、管理者として実行してください。

1 [設定] > [USB エージェント]をクリックします。
2 [ダウンロード]をクリックしてファイルをダウンロードし、インストールします。



3 USB カード端末のバイトオーダーを選択します。

4 USB エージェントが使用するポートを設定します。



5 [適用]をクリックして変更を保存します。

顔のグループマッチング

顔グループマッチングとは、BioStar 2 に設定されているユーザーグループから、し、ユーザーを認証する機能です。

メモ

・最大 10 個の一致するグループを作成できます。
・各グループには、最大 3,000 個の顔テンプレートを含めることができます。
・一致するグループ内の顔テンプレートの総数が 5,000 を超えることはできません。

1 [設定] > [顔グループ マッチング]をクリックします。

2 必要なフィールドを編集します。

項番	項目名	説明
1	グループマッチング	グループマッチングを使用するかどうかを設定します。 **メモ** 運用中にグループマッチングを無効にするには、以前に設定したすべての端末とグループ設定を削除する必要があります。
2	顔のグループマッチング利用端末	グループマッチングを使用する端末を設定します。 追加できるモデルは FaceStation 2 のみです。
3	マッチンググループ設定	[+追加]をクリックし、グループ名とユーザーグループを設定します。 **メモ** ・最大 10 個のマッチンググループを作成できます。 ・1 つのマッチンググループに対して複数のユーザーグループを設定できます。 ・ユーザーグループに含まれる顔テンプレートの数が 3,000 を超える場合、マッチンググループとして設定できません。

3 [適用]をクリックして変更を保存します。

監査記録

監査記録は、BioStar2 システムで発生した操作ログを記録します。

1 [設定] > [監査記録]をクリックします。

項番	項目名	説明
1	期間	直近 1 か月または直近 3 か月から選択します。
2	フィルター	フィルター項目ごとに条件を設定できます。 **[フィルターの保存]**をクリックして、フィルターを保存します。
3	ページナビゲーションボタンと リストの行数	ページの移動や 1 ページに表示する行数の設定を行えます。 最初のページに移動します。 前のページに移動します。 2 / 2 移動するページ番号を入力します。 次のページに進みます。 最後のページに移動します。 25 行 1 ページに表示する行数を設定します。
4	機能ボタン （CSV エクスポート、カラム設定）	監査リストのリストを CSV ファイルとして保存し、列の設定を変更できます。
5	監査記録一覧	監査記録の一覧を表示します。

サマータイム

1 [設定] > [サマータイム]をクリックします。

2 [+追加]をクリックします。

3 必要な項目を編集し、[追加]をクリックします。

4 [適用]をクリックして設定を保存します。

メモ

既に使用されているサマータイムの情報の編集や削除はできません。

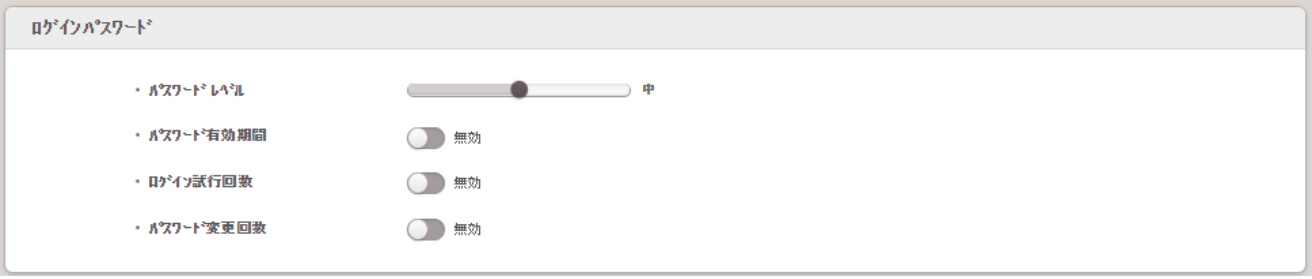
セキュリティ

ログインやパスワードに関する設定を行えます。

1 [設定] > [セキュリティ]をクリックします。

2 必要な項目を編集します。

ログインパスワード



項目	説明
パスワードレベル	BioStar 2 ログインパスワードの複雑さに関するポリシーを設定します。 ・小: 32 文字まで入力できます。 ・中: 8 ～ 32 文字の英字（大文字または小文字）と数字を組み合わせる必要があります。 ・強: 10 ～ 32 文字の英字（大文字と小文字、少なくとも 1 つの英字大文字）、数字、および記号を組み合わせる必要があります。 **メモ** クラウド経由アクセス機能を使用する場合、[中]または[強]のみを使用できます。
パスワードの有効期間	パスワードの有効期間を設定できます。 パスワードの最大有効期間を超えると、ログイン時にパスワード変更要求のメッセージが表示されます。 **メモ** パスワードの有効期間は、1 日から 180 日に設定できます。
ログイン試行回数	ログイン試行できる最大回数と再度試行可能になるまでの時間を設定できます。 設定した回数以上パスワードを間違えると、設定した時間の間はログインできません。
パスワード変更回数	パスワード変更の最大制限を設定できます。 **メモ** 最大パスワード変更制限は 10 回まで設定できます。

詳細セキュリティ設定

項目	説明
データベース上の個人データを暗号化する	[データベース上の個人データを暗号化する]が[使用]に設定されている場合、資格情報データや個人情報を含むすべての機密データは暗号化されてデータベースに保存されます。 このオプションが[未使用]に設定されている場合、暗号化されたデータは復号化され、ユーザーの個人情報は暗号化されていない状態で保存されます。 **メモ** ・ [データベース上の個人データを暗号化する]が[使用]の場合に暗号化される項目は次のとおりです。 ・プロフィール画像 ・ユーザー ID ・名前 ・電話番号 ・ユーザー IP ・送信者と受信者の電子メール情報 ・ログイン ID ・ログインパスワード ・顔テンプレート ・指紋テンプレード ・カード ID ・スマートカードレイアウト キー ・ユーザーと訪問者のカスタム情報 ・イメージログファイル ・ データベース上の個人データを暗号化している間は、サーバーを強制的に起動しないでください。BioStar 2 へのログインに失敗するなどのエラーが発生する場合があります。
個人データ暗号化キー	個人データの暗号化キーを設定できます。 [変更]をクリックして、新しい暗号化キーを設定します。

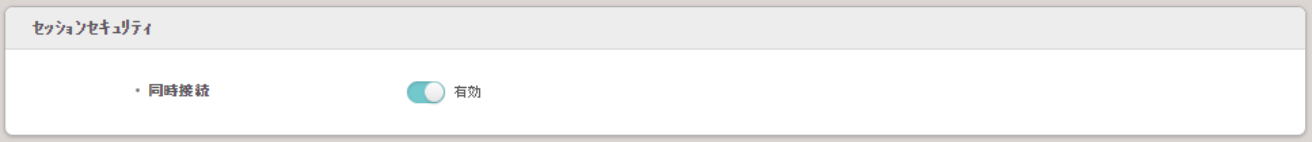
	暗号化キーを変更すると、既存のデータが再暗号化されます。 **メモ** 暗号化キーは、英数字、記号で構成された 32 文字で入力できます。
端末の暗号化通信	BioStar 2 と端末間の通信は、証明書を使用して保護できます。 [端末の暗号化通信]が使用に設定されている場合、BioStar 2 は証明書を作成して端末に送信します。 端末は、この証明書を使用して BioStar 2 とデータを交換するための安全なチャネルを使用します。外部証明書を使用するには、ルート証明書、公開鍵証明書、および秘密鍵ファイルをアップロードする必要があります。 [端末ハッシュキー]を使用に設定する場合、新しいデータ暗号化キーと管理者パスワードを設定できます。 **メモ** ・ 端末の暗号化通信を設定可能な端末とファームウェアのバージョンは以下です。 FaceStation 2 FW 1.1.0 以降 BioStation A2 FW 1.5.0 以降 BioStation 2 FW 1.6.0 以降 BioStation L2 FW 1.3.0 以降 BioLite N2 FW 1.0.0 以降 BioEntry P2 FW 1.1 .0 以降 BioEntry W2 FW 1.2.0 以降 FaceLite FW 1.0.0 以降 XPass 2 FW 1.0.0 以降 CoreStation FW 1.1.0 以降 X-Station 2 FW 1.0.0 以降 BioStation 3 FW 1.0.0 以降 ・ BioStar 2 は、端末との暗号化通信の設定状態に従って証明書を作成または削除し、以前の証明書と同じ証明書は作成されません。 例えば、[端末の暗号化通信]の設定を「使用→未使用」の順に変更すると、作成した証明書は自動的に削除されます。[使用→未使用→使用]の順に設定を変更すると、[A 証明書の作成 → A 証明書の削除 → B 証明書の作成]と操作が行われます。 ・ [端末の暗号化通信]を使用している時に、端末がネットワークから物理的に切断されている場合は、[端末の暗号化通信]を[未使用]に変更しないでください。 このような場合、BioStar 2 の証明書は削除され、端末は再度接続できなくなります。

	再度接続するには、端末に保存されている証明書を削除するか、端末を工場出荷時設定にリセットする必要があります。詳細については、端末のマニュアルを参照してください。

メモ

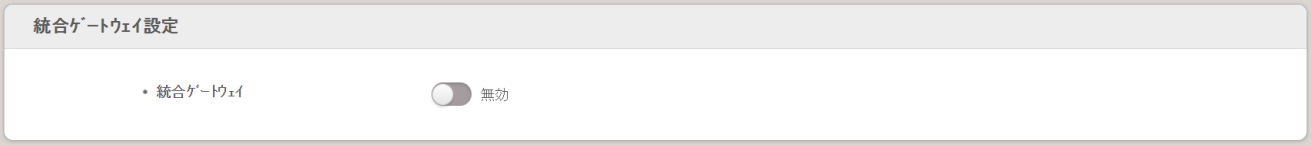
- [詳細セキュリティ設定]タブは、ユーザーが ID 番号 1 を使用している管理者としてサインインした場合にのみ編集可能になります。

セッションセキュリティ



項目	説明
同時接続	同一アカウントでの同時接続を許可するかどうかを設定できます。 [同時接続]を[無効]に設定すると、以前にログインしたユーザーが同じアカウントに同時に接続しようとすると、ログアウトされます。

統合ゲートウェイ設定



項目	説明
統合ゲートウェイ設定	BioStar 2 の実行ポートを統合ゲートウェイに変更できます。 BioStar2 サーバーへのアクセスをリバースプロキシ方式にします。 BioStar 2 サーバーへのリクエストを効率的に処理できるようになり、iframe のセキュリティの脆弱性が改善され、SSL 証明書のエラーが最小限に抑えられます。 **メモ** ・ 統合ゲートウェイを有効化すると、サーバーが再起動し、自動的にログインページに移動します。 ・ ポートが使用中の場合は、ポップアップメッセージが表示されます。別のポート番号を入力して、再度有効化します。

3 [適用]をクリックして設定を保存します。

アクティブディレクトリ

Microsoft Windows Active Directory に保存されているユーザーデータを BioStar 2 に同期できます。

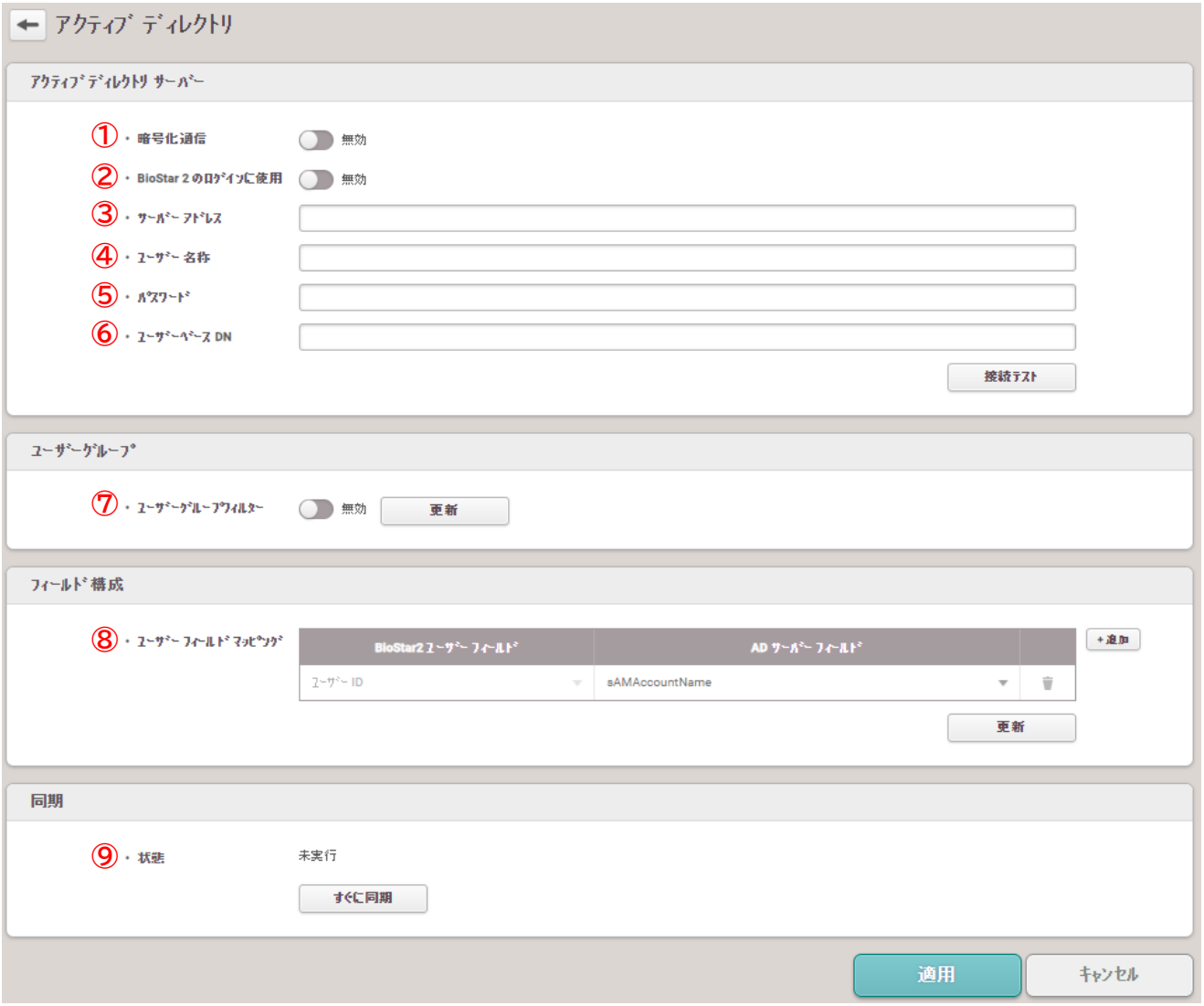
重要

本機能は弊社でサポート対象外の機能です。

メモ

- AC アドバンスドライセンスが有効化されると、Active Directory 設定が表示されます。
- Active Directory は、Windows Server 2008 R2 以降のシステム環境で使用できます。
- Active Directory を使用するには、User/Device Management を参照して、User ID Type を Alphanumeric に設定します。

1 [設定] > [アクティブ ディレクトリ]をクリックします。
2 必要な項目を編集します。



項番	項目名	説明
1	安全な転送	Windows Active Directory サーバーとの通信時に暗号化を使用できます。 Active Directory 証明書サービスをインストールし、Active Directory 暗号化を参照してキーストアのパスワードを設定します。
2	BioStar 2 ログインに使用	Windows Active Directory アカウントを使用して BioStar 2 にログインできるようにします。
3	キーストアのパスワード	Windows Active Directory サーバーの暗号鍵ストアのパスワードを入力します。これは、安全な転送を有効にする場合にのみ使用できます。
4	サーバーアドレス	Windows Active Directory のサーバーアドレスを入力します。
5	ユーザー名	Windows Active Directory で使用されるユーザー名を入力します。
6	パスワード	Windows Active Directory で使用されるパスワードを入力します。
7	ベース DN	Windows Active Directory のベース ドメイン名を入力します。 ベース ドメイン名は、次の方法で見つけることができます。

		a) Active Directory 管理センターを実行します。 b) ユーザーデータが保存されているノードを右クリックし、**[プロパティ]をクリックします。** c) プロパティウィンドウで、**[展開]をクリックし、[属性エディタ]をクリックします。** **d) distributedName** の値を表示します。
8	ユーザーグループ フィルター	ユーザーグループごとに同期を有効または無効にすることができます。
9	ユーザーグループのベース DN	Windows Active Directory のユーザーグループのベース ドメイン名を入力します。**これは、ユーザーグループ フィルター**を有効にする場合にのみ使用できます。
10	ユーザーグループ	同期するユーザーグループを選択します。**これは、ユーザーグループ フィルター**を有効にする場合にのみ使用できます。
11	ユーザー フィールド マッピング	Windows Active Directory のデータ フィールドを BioStar 2 のユーザー フィールドにマッピングできます。 マッピングするユーザー フィールドは、次のように設定できます。 a)**[+追加]をクリックして**、ユーザー フィールド スロットを追加します。 b) BioStar 2 ユーザー フィールドと AD サーバー フィールドを設定して、正しいデータを BioStar 2 のユーザー フィールドにマップします。 c)**[更新]をクリックして**、ユーザー フィールド マッピング設定を適用します。 **メモ** ・ ユーザーID フィールドは静的項目であり、削除できません。
12	同期する	**[今すぐ同期]**をクリックして、ユーザーデータを同期します。最終同期日時が表示されます。

3 [適用]をクリックして設定を保存します。

アクティブディレクトリ暗号化

Windows Active Directory サーバーとの通信時に暗号化を使用できます。
初めて暗号化を使用する場合は、次の順序で設定してください。

1 手順 1. Active Directory 証明書サービスのインストール

Windows Active Directory サーバーの暗号化通信を使用するには、Active Directory 証明書サービスをインストールする必要があります。
Active Directory 証明書サービスは、次のようにインストールできます。

A) Windows Active Directory サーバーがインストールされている PC でサーバー マネージャーを実行し、[管理] > [役割と機能の追加]をクリックします。
B) [開始する前に]で、[次へ]をクリックします。
C) [インストールの種類の選択]で、[役割ベースまたは機能ベースのインストール]を選択し、[次へ]をクリックします。
D) [対象サーバーの選択]で、[サーバー プールからサーバーを選択] を選択し、サーバーを確認して[次へ]をクリックします。
E) [サーバーの役割の選択]で、[Active Directory 証明書サービス]を選択し、[次へ]をクリックします。
F) ポップアップ ウィンドウが表示されたら、詳細を表示し、[機能の追加] > [次へ]をクリックします。
G) Active Directory 証明書サービスの詳細を表示し、[次へ]をクリックします。
H) [インストールの選択を確認する]で、[インストール]をクリックします。インストールが完了したら、[移行先サーバーで Active Directory 証明書サービスを構成する] をクリックします。
I) AD CS 構成ウィザードが表示されたら、詳細を表示して[次へ]をクリックします。
J) [役割サービス]で、[証明機関] > [次へ]をクリックします。
K) 1 [セットアップの種類]ページで、[エンタープライズ CA]を選択し、[次へ]をクリックします。
L) [CA の種類を指定する]ページで、[ルート CA]を選択し、[次へ]をクリックします。
M) [秘密キーの種類を指定する]ページで、[新しい秘密キーを作成する]を選択し、 [次へ]をクリックします。
N) CA の暗号化、CA 名、および有効期間を設定し、[次へ]をクリックします。
O) [CA データベース]ページで、証明書データベースと証明書データベース ログのフォルダーの場所を設定し、[次へ]をクリックします。
P) [確認]ページで、Active Directory 証明書サービスの詳細を表示し、[構成]をクリックします。

2 ステップ 2. LDAPS の接続（LDAP over SSL/TLS）

A) [スタート] > [ファイル名を指定して実行]をクリックします。
B) 入力フィールドに ldp と入力します。
C) [Ldp-disconnected]ウィンドウが表示されたら、[Connect]をクリックします。
D) 「サーバー」フィールドと「ポート」フィールドに入力し、「SSL」を選択します。そして、「OK」をクリックします。

3 ステップ 3. ルート証明書のコピー

A) Windows Active Directory サーバーがインストールされている PC でコマンド プロンプトを実行します。

B) certutil -ca.cert client.crt コマンドを入力して、ルート証明書をコピーします。

C) keytool -import -keystore ad.jks -file client.crt コマンドを入力して、サーバー証明書を .jks 形式に変換します。

D) .jks 形式のサーバー証明書を BioStar 2 インストール パスに保存します。

モバイルアクセス

BioStar 2 と Airfob ポータルを連携することで、BioStar 2 のユーザーにモバイルアクセスカードの発行を行えます。

メモ

- モバイルアクセスカードは、CSN モバイルカードまたはテンプレートオンモバイルのいずれかのみを使用できます。
- モバイルアクセスが利用できる端末とファームウェアのバージョンは以下の通りです。
  - XPass 2 FW 1.1.0 以降
  - XPass D2(Rev 2) FW 1.4.0 以降
  - BioLite N2 FW 1.3.0 以降
  - BioEntry W2(Rev 2) FW 1.6.0 以降
  - FaceStation 2 FW 1.4. 0 以降
  - FaceStation F2 FW 1.0.0 以降
  - BioStation 2 FW 1.9.0 以降(NFC 機能搭載モデルのみ対応)
  - BioStation A2 FW 1.8.0 以降(NFC 機能搭載モデルのみ対応)
  - FaceLite FW 1.2.0 以降
  - X-Station 2 FW 1.0.0 以降
  - BioStation 3 FW 1.0.0 以降
- テンプレートオンモバイルが利用できる端末とファームウェアのバージョンは以下の通りです。
  - BioStation 3 FW 1.2.0 以降

以下の手順で、Suprema モバイルアクセスの設定を行えます。

1 Airfob ポータルにアクセスしてサイトを開設する

Airfob ポータルでは、モバイルアクセスカードと登録端末を設定し、サイトを開設し、クレジットを登録します。

➢ 関連情報

Airfob ポータル

2 BioStar 2 でモバイルアクセスを設定する

モバイルアクセスを使用するかどうかを設定します。

➢ 関連情報

モバイルアクセスの設定

3 端末の登録

BioStar 2 に接続されている端末をモバイルアクセスで認証できるように端末を登録します。

➢ 関連情報

モバイルアクセスの設定

4 モバイルアクセスカードの発行

BioStar 2 に登録したユーザーに認証資格として、モバイルアクセスカードを発行します。

ユーザーにモバイルアクセスカードを発行するには、メッセージオプションに基づいてユーザー情報を入力する必要があります。

➢ 関連情報

ユーザー情報の追加

モバイルアクセスカードの登録

Airfob ポータル

Airfob ポータルでは、モバイルアクセスカードと端末の管理や、サイトとクレジットの管理を行えます。

重要

初回セットアップの手順が含まれますが、セットアップは販売代理店が行います。

1. Airfob ポータル(https://portal.airfob.com/ja)にアクセスします。
2. [新規登録]をクリックしてサインアップし、サイトを作成します。
3. メールアドレスを入力するフィールドに Airfob ポータル管理者のメールアドレスを入力し、[スタート]をクリックします。入力したメールアドレスに認証コードが送信されます。
4. 受け取った認証コードを認証コードフィールドに入力し、[確認]をクリックします。
5. プライバシーと利用規約を確認し、[同意する]をクリックします。
6. Airfob ポータルで使用するパスワードとニックネームを設定し、[Create Account]をクリックします。アカウントの作成が完了します。
7. [サインイン]をクリックします。
8. メールアドレスとパスワードを入力し、[サインイン]をクリックします。
9. [サイトの作成]をクリックしてサイトを開設します。

メモ

サイトとは、モバイルアクセスを使用する組織または会社を意味します。

10. サイトの名前と国を設定し、[次へ]をクリックします。
11. サイト種別を選択します。

メモ

サイト種別や状況に応じて、「ダイナミック」または「レギュラー」の 2 種類から選択します。

・ダイナミック: サイト種別ダイナミックは、モバイルアクセスカードの再発行、削除、一時利用停止、有効期限の指定を行えるサイト種別です。利用期間や端末に応じてクレジットが差し引かれる特徴があります。

・レギュラー: サイト種別レギュラーは、管理者がアクセス権限を削除するまで永久に使用できます。モバイルアクセスカードの発行枚数に応じてクレジットが差し引かれます。

12. [作成]をクリックします。サイトの作成が完了します。
13. サイト名をクリックして、サイトの Airfob ポータルにアクセスします。

メモ

Airfob ポータルの使用方法の詳細については、Airfob ポータル (https://portal.airfob.com/en) を参照してください。

モバイルアクセスの設定

モバイルアクセス、Airfob ポータルに関する設定を行えます。

モバイルアクセスカードを利用するための端末の登録も行えます。

1 [設定] > [モバイルアクセス]をクリックします。

2 必要な項目を編集します。

項目	説明
一般設定	・ モバイルアクセス設定:モバイルアクセスの使用する場合、使用に設定します。 モバイルアクセス設定を使用に設定すると、モバイルアクセスカードをユーザーに発行できます。 **メモ** BioStar 2 でモバイルアクセスを使用するには、最初に Airfob ポータルへのサインアップと初期設定を完了する必要があります。 ・ サイト種別: サイト種別の確認を行えます。 **メモ** サイト種別や状況に応じて、「ダイナミック」または「レギュラー」の 2 種類から選択します。 ・ ダイナミック: サイト種別ダイナミックは、モバイルアクセスカードの再発行、削除、一時利用停止、有効期限の指定を行えるサイト種別です。利用期間や端末に応じてクレジットが差し引かれる特徴があります。 ・ レギュラー: サイト種別レギュラーは、管理者がアクセス権限を削除するまで永久に使用できます。モバイルアクセスカードの発行枚数に応じてクレジットが差し引かれます。 ・ドメイン: Airfob ポータルのドメインアドレスが表示されます。 ・ポート: Airfob ポータルのポート番号が表示されます。 ・サイト ID: Airfob ポータルで作成したサイト ID を入力します。 サイト ID は、Airfob ポータルの[設定] > [サイト]メニューで確認できます。 ・E メール: モバイルアクセス管理者のメールアドレスを入力します。

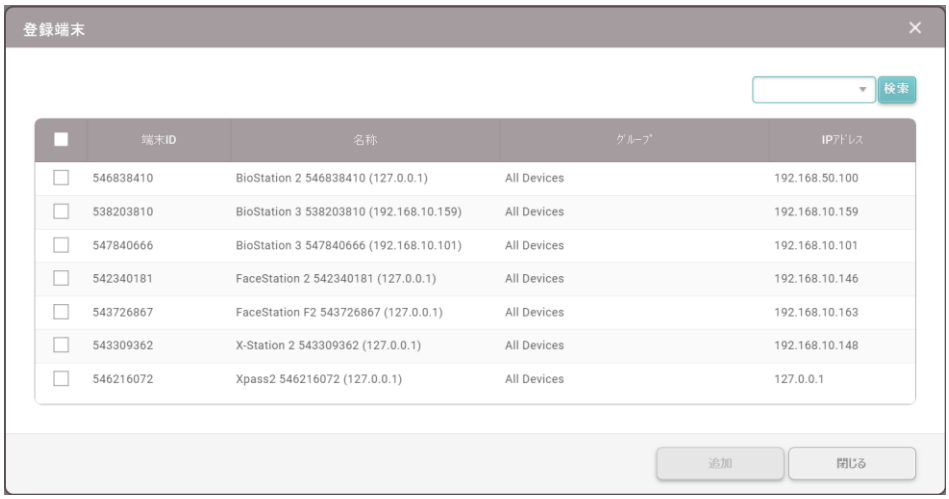
・パスワード: モバイルアクセス管理者のパスワードを入力します。

・登録端末: モバイルアクセスを使用する端末を登録できます。ドメイン、ポート、サイト ID 、電子メール、およびパスワードの入力が完了すると、以下の登録端末が表示されます。

[接続]をクリックすると、Airfob ポータルに接続されます。

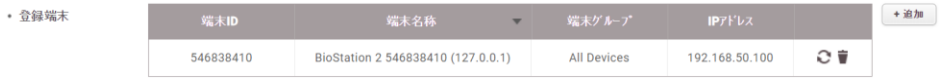
[+追加]をクリックして、モバイルアクセスを使用する端末を追加します。

BioStar 2 に登録されている端末の一覧が表示されます。



端末を選択し、[追加]をクリックします。

端末一覧に追加された端末が表示されます。



更新マーク(🔄)クリックすると、モバイルアクセス証明書の再送信を行えます。

ゴミ箱ボタン(🗑)をクリックすると、登録端末の削除を行えます。

メモ

・ モバイルアクセスが利用できる端末とファームウェアのバージョンは以下の通りです。

XPass 2 FW 1.1.0 以降

XPass D2(Rev 2) FW 1.4.0 以降

BioLite N2 FW 1.3.0 以降

BioEntry W2(Rev 2) FW 1.6.0 以降

FaceStation 2 FW 1.4. 0 以降

FaceStation F2 FW 1.0.0 以降

BioStation 2 FW 1.9.0 以降(NFC 機能搭載モデルのみ対応)

BioStation A2 FW 1.8.0 以降(NFC 機能搭載モデルのみ対応)

FaceLite FW 1.2.0 以降

	X-Station 2 FW 1.0.0 以降 BioStation 3 FW 1.0.0 以降 ・ Airfob Pass アプリを使用して端末を登録することも可能です。 ・ 登録済みの端末を削除すると、端末に送信されたモバイルアクセス証明書が削除されます。

E メール設定

メールに関する SMTP などの設定を行えます。

メモ

- E メール設定の機能をすべて利用する場合は、クラウド経由アクセスを設定してください。
  AC ライセンスのスタンダード以上のライセンスが適用されると、利用可能です。
- ビジュアル顔モバイル登録や QR コード付きのメールの送信機能を利用する場合はユーザー情報にユーザーのメールアドレスを入力する必要があります。
- ビジュアル顔を利用できる端末は以下の通りです。
  FaceStation F2、BioStation 3
- スキャナーで QR/バーコードを読み取り可能な端末は以下です。
  X-Station 2（XS2-QDPB、XS2-QAPB）
- カメラで QR/バーコードを読み取り可能な端末は以下です。
  X-Station 2（XS2-ODPB、XS2-OAPB、XS2-DPB、XS2-APB）ファームウェア 1.2.0 以降
  BioStation 3（BS3-DB、BS3-APWB）ファームウェア 1.1.0 以降
- [カメラによる QR/バーコードを使用]を使用するには、別途端末ライセンスが必要です。
  詳細については、端末ライセンスを参照してください。

1 [設定] > [メール設定]をクリックします。

2 必要な項目を編集します。

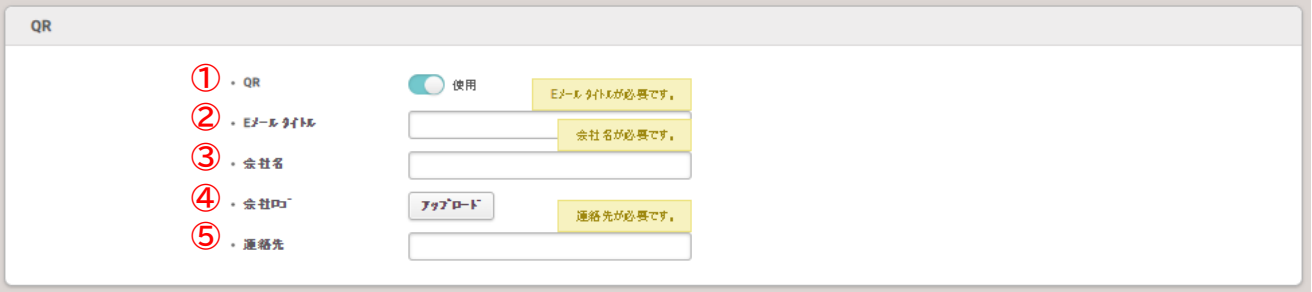
メール内容設定

項番	項目名	説明
1	SMTP 設定	メール送信用の SMTP(Simple Mail Transfer Protocol)を設定します。  ・ SMTP サーバー名:SMTP サーバー名を入力します。 ・ 説明: 説明を入力します。 ・ サーバーアドレス:SMTP サーバーアドレスを入力します。 ・ ポート(初期値:25) : SMTP サーバーのポート番号を入力します。SMTP として使用するメールの設定画面で確認できます。 ・ ユーザー名: SMTP サービスのアカウントを入力します。 ・ パスワード: SMTP サービスのパスワードを入力します。 ・ セキュリティタイプ: セキュリティの種類を選択します。 ・ 送信者:送信者のメールアドレスを入力します。
2	テスト E メール受信者アドレス	テストメールを受信するメールアドレスを入力し、[電子メールを送信]をクリックすると、設定したメールアドレスにテストメールが送信されます。

ビジュアル顔モバイル登録

項番	項目名	説明
1	ビジュアル顔モバイル登録	ビジュアル顔モバイル登録を使用するには、使用にします。 未使用にすると、ビジュアル顔モバイル登録リンクをユーザーに送信できません。
2	E メールタイトル	メールのタイトルを入力します。
3	会社名	会社名を入力します。
4	会社のロゴ	会社のロゴ画像をアップロードします。 **メモ** ・ サポートされている画像ファイル形式は、GIF、JPG、JPEG、JPE、JFIF、PNG です。 ・ 対応画像ファイルサイズは 5MB までです。
5	連絡先	担当者の連絡先を入力してください。
6	フッター	ビジュアル顔を登録しているユーザーに通知する内容を入力します。 メールの下部に表示されます。 **メモ** フッターの長さは最大 5,000 文字です。

QR



項番	項目名	説明
1	QR	QR コードを使用するには、使用にします。 未使用にするとユーザーに QR コードをメールで送信できません。
2	E メールタイトル	メールのタイトルを入力します。
3	会社名	会社名を入力します。
4	会社ロゴ	会社のロゴ画像をアップロードします。 **メモ** ・サポートされている画像ファイル形式は、GIF、JPG、JPEG、JPE、JFIF、PNG です。 ・対応画像ファイルサイズは 5MB までです。
5	連絡先	担当者の連絡先を入力してください。

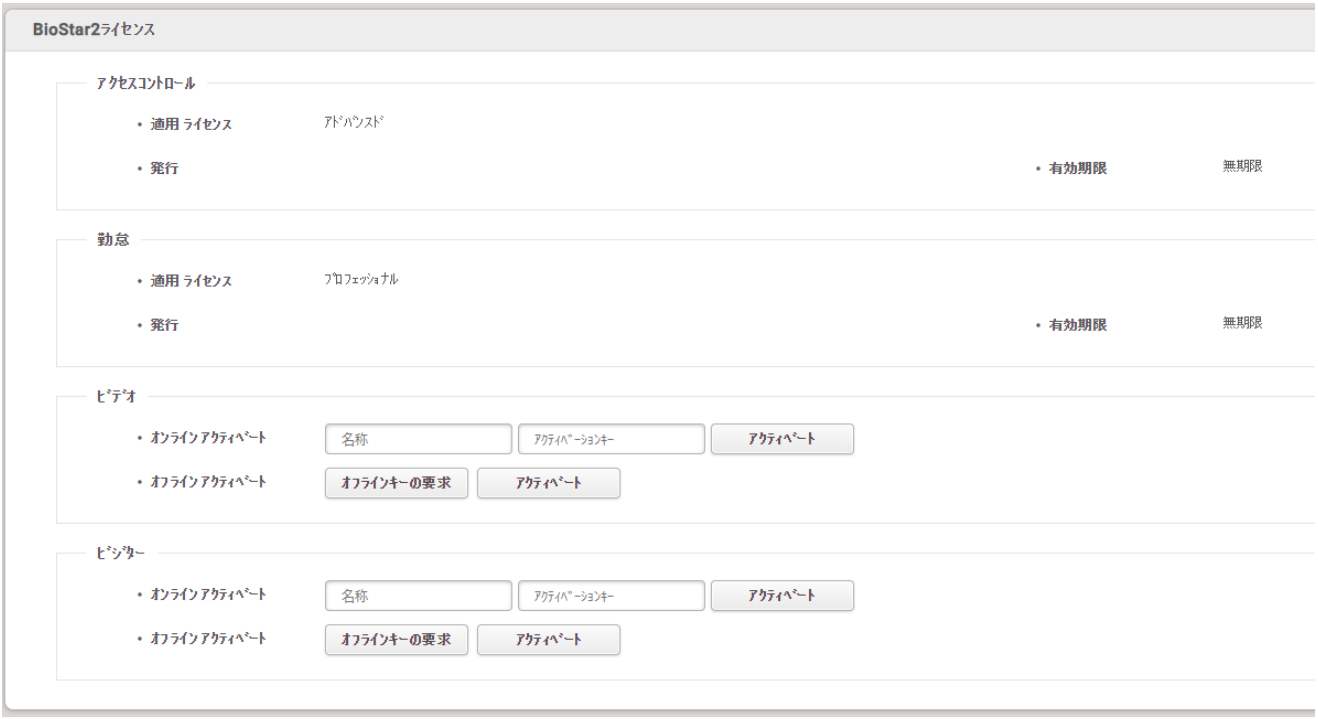
3 [適用]をクリックして設定を保存します。

ライセンス

BioStar 2 ライセンスと端末ライセンスを有効化します。

BioStar 2 ライセンス

1 [設定] > [ライセンス]をクリックします。



項目	説明
BioStar 2 ライセンス	購入した BioStar 2 ライセンスの適用を行えます。 BioStar 2 ライセンスをオンラインでアクティベートするには、登録する名称と、Suprema から受け取ったアクティベーションキーを入力した後、[アクティベート]をクリックします。BioStar 2 ライセンスをオフラインでアクティベートするには、[オフラインキーの要求]をクリックすると、[オフラインでライセンスをアクティベート]ダイアログが表示されますので、ダイアログの指示に従ってください。

端末ライセンス

Suprema が発行した端末ライセンスを適用すると、ライセンスに対応する特定の機能の使用が可能となります。
端末ライセンスの発行については、販売代理店にお問い合わせください。
端末ライセンスの適用方法は、BioStar 2 から行う方法と USB メモリを使用して端末から行う方法の 2 種類あります。

メモ

- 端末ライセンスごとに 1 つの機能をアクティベートします。
- 1 つの端末ライセンスファイルに複数の端末ライセンスを含めることができます。(100 台まで対応)
- 端末ライセンスファイルは暗号化されたファイルであり、任意に変更することはできません。
- 端末ライセンスは、端末 ID に基づいて発行されます。
  端末 ID が通常と異なる方法で変更された場合、ライセンスの保証に関するサービスは提供されません。

1 [設定] > [ライセンス]をクリックします。

項番	項目名	説明
1	ライセンスファイル	[参照]をクリックした後、PC から適用予定の端末ライセンスのファイルを選択してください。
2	ライセンスの種類	端末ライセンスファイルに含まれるライセンスの種類を確認してください。 ・Camera QR **メモ** カメラ QR を利用できる端末は以下の通りです。 X-Station 2（XS2-ODPB、XS2-OAPB、XS2-DPB、XS2-APB）ファームウェア 1.2.0 以降 BioStation 3（BS3-DB、BS3-APWB）ファームウェア 1.1.0 以降 ・U&Z 無線ドアロック **メモ** ・ 接続したい U&Z 無線ドアロックの台数と同数のデバイスを最大 8 台までデバイスライセンスを発行できます。

		・ 1 つの端末ライセンスで接続できる U&Z 無線ドアロックの最大数は 8 台です。複数の端末ライセンスを有効化した場合でも、8 台を超えることはできません。
3	端末数	端末ライセンスファイルに含まれる端末数を確認してください。
4	端末一覧	・ 端末 ID: 端末の一意の ID を表示します。 ・ 端末名: 端末名を表示します。 ・ 製品名: 端末のモデル名を表示します。 ・ 端末の状態: 端末の状態を確認します。通常状態の端末のみがライセンスをアクティベート可能です。「通常、未接続、非対応、未登録」など状態が表示されます。 ・ ライセンス状態: ライセンスが有効化されているかどうかを表示します。有効化されていない端末のみがライセンスをアクティベートできます。「有効化されていない、有効化されている、N/A」など状態が表示されます。 ・ 有効化数: U&Z 無線ドアロックの現在の接続状況を確認できます。 **メモ** 有効化数の項目は U&Z 無線ドアロックライセンスを適用した場合のみ表示されます。

2 端末一覧を確認したら、アクティベートをクリックして端末ライセンスを適用します。
ライセンスのアクティベーションに失敗した場合は、アクティベーションに失敗した旨のメッセージが表示されます。
販売代理店に問い合わせてください。

カードプリンター

カードプリンターは、BioStar 2 と cardPresso を連携させ、BioStar 2 から任意のデザインのカードの印刷を行えます。

重要

本機能は弊社でサポート対象外の機能です。

メモ

- カードプリンター機能を使用するには、cardPresso が発行したライセンスをアクティベートする必要があります。
  - ライセンスタイプ：cardPresso XXL 版
- BioStar 2 がインストールされている PC に CardPresso をインストールします。

1 [設定] > [カード プリンター]をクリックします。

2 必要な項目を編集します。

項目	説明
BioStar 2 ライセンス	購入した BioStar 2 ライセンスを有効化できます。 BioStar 2 ライセンスをオンラインで有効化するには、自分の名前と、Suprema から受け取ったアクティベーション キーを入力した後、**[有効化]をクリックします。**BioStar 2 ライセンスをオフラインでアクティベートするには、**[オフラインキーの要求]をクリックすると、[オフラインでライセンスをアクティベート]**ダイアログが表示されます。ダイアログの指示に従います。

3 「適用」をクリックして設定を保存します。

システムバックアップ

システムバックアップは、BioStar 2 のデータベースのバックアップなどを行えます。

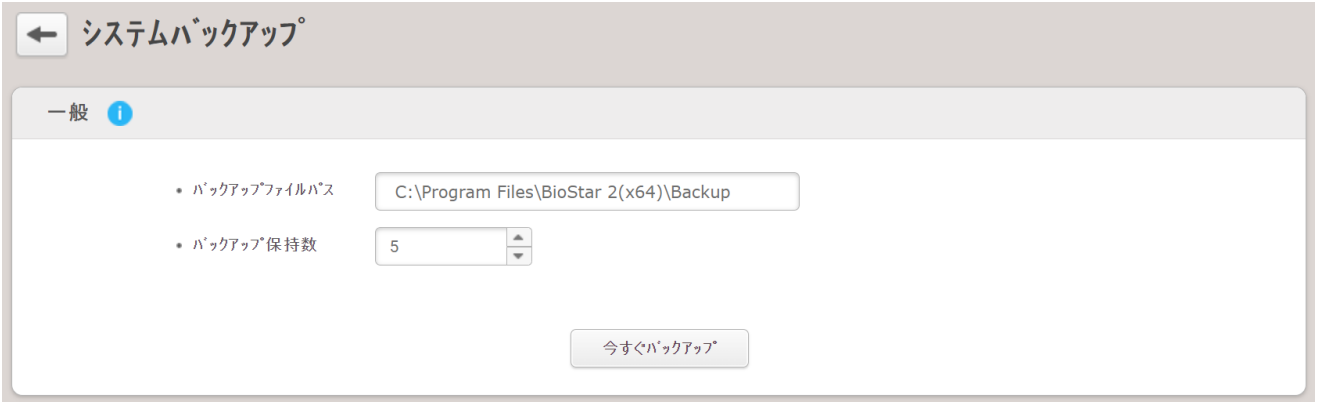
メモ

MSSQL データベースを使用している場合、または、BioStar 2 と異なる PC にデータベースがインストールされている場合、本機能とシステムバックアップの復元は利用できません。

一般的なバックアップ

システムバックアップに必要な項目を設定します。

1 [設定] > [システムバックアップ]をクリックします。
2 必要な項目を編集します。

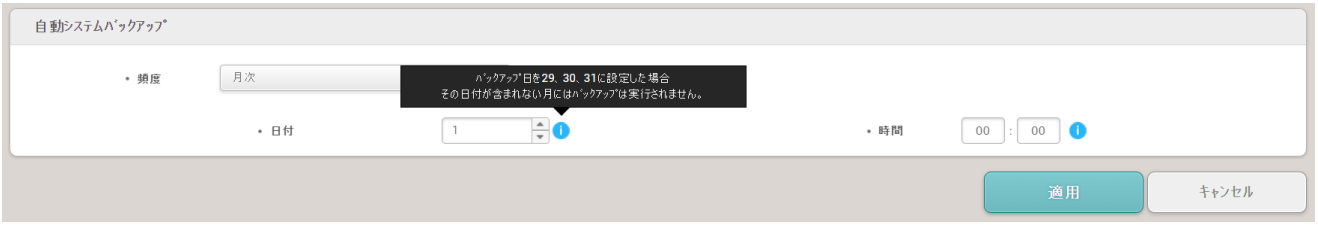


3 「適用」をクリックして設定を保存します。
4 [設定] > [ライセンス]をクリックします。

自動システムバックアップ

自動的にバックアップするように設定を行えます。

1 [設定] > [システムバックアップ]をクリックします。
2 必要な項目を編集します。



3 「適用」をクリックして設定を保存します。

関連情報

➢ システムのリストア

システムのリストア

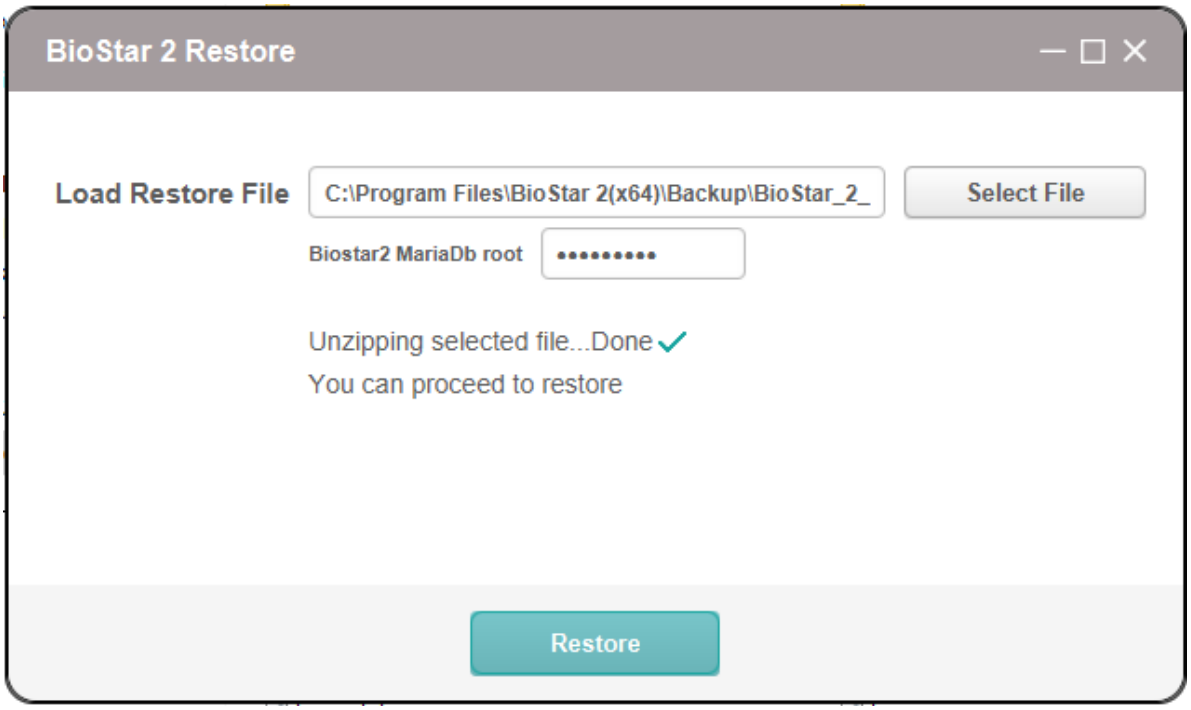
BioStar 2 が正常に動作しない場合は、BioStar 2 Restore を使用して、システムバックアップ機能で取得したバックアップファイルからリカバリポイントへの復元が可能です。

メモ

MSSQL データベースを使用している場合、または、BioStar 2 と異なる PC にデータベースがインストールされている場合、本機能とシステムバックアップの復元は利用できません。

1 [スタート] > [BioStar 2] > [BioStar 2 Restore]を実行します。
プログラムパス: C:¥Program Files¥BioStar 2(x64)¥biostar-restore.exe

2 [Select File]をクリックしてバックアップファイルを選択し、[Restore]をクリックして復元を開始します。



3 Biostar サービスを開始しています...Done メッセージが表示されたら、復元完了です。

4 BioStar 2 にアクセスしてください。

メモ

バックアップ時の BioStar 2 バージョンが現在のバージョンと異なる場合、復元できません。

18 付録

免責事項、著作権表示、オープンソースライセンス、ソフトウェアエンドユーザー使用許諾契約書(EULA)は Suprema 社から発行されるドキュメントに記載されている内容に準じます。