BioStar 2.8 マニュアル

SECURE

2.8.15

内容

はじめに

本製品をお買上げいただきまして、ありがとうございます。
以下の点につきまして、ご注意の上、正しくご利用をお願い致します。

・初期設置後、お客様ご利用のネットワーク環境の変更が必要な場合は、弊社まで ご連絡・ご相談ください。
（もし初期設定から変更されてしまった場合、お客様環境での有償での再調査が必要となる場合があります。）

・納入時に、システムの取扱説明をさせていただきます。もし、経年後お客様の操作担当者様が変更となる場合は、
操作方法や注意事項の引き継ぎをお願い致します。
（再度、取扱説明を行う場合、有償のトレーニングサービスをご利用ください。）

・計画停電等により電源が切れる場合は、事前に、認証端末の電源を OFF にし、電源の回復後に認証端末の
電源を ON にしてください。認証端末の電源操作をせずに、電源の強制的な OFF/ON があった場合、認証端末の
故障の原因となります。
また、一定時間以上 停電が継続すると、認証端末内部の一時的な充電電池が放電され、次回電源 ON 時に、
内臓の時計がリセットされます。この場合、正しく認証できなくなりますので、復電時に一定時間が経過している
場合は、再度、認証端末に対し、時刻の設定を行ってください。電源回復後、端末の日時を確認してください。
液晶画面付き端末：液晶画面の日付をご確認ください。
液晶画面無し端末：状態 LED の色をご確認ください。（青/赤の交互点滅の場合、日時がリセットされています。）

・認証端末は精密機器であるため、稀に正常に動作しない状態に陥る可能性がございます。そのような症状が
発生した場合、認証端末の電源を一旦、OFF にしていただき、数秒の後、認証端末の電源を ON にし、状態の
確認をお願い致します。

・ご不明点のお問合わせや、不具合・トラブルに関してのお問合わせの際は、まず、「お客様番号」を
確認させていただいております。お問い合わせ前に、事前に「お客様番号」のご確認をお願い致します。
お客様番号は、本画面の上部に表示されている番号となります。
また、ご契約プランにもよりますが、コールセンターのご利用は、有償となります。

・BioStar2 には、インターネットからアクセス可能とする機能があります。（初期値は利用しない設定です。）
本機能をご利用の場合は、通常のホームページと同様で、BioStar2 のサーバーに対し、外部からの不正アクセスを
される恐れがあります。弊社では、責任を負いかねますので、ご理解の上、ご利用をご検討ください。

・BioStar2 は、Google Chrome ブラウザのみの対応となります。Internet Explorer や, Edge, FireFox などのブラウザで
は、正しく動作しない機能があります。必ず、Google Chrome をご利用ください。

・解像度によっては、画面表示などの情報が正しく表示されないことがあります。

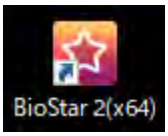
・掲載のサービス名は各社の商標、登録商標です。

通常運用編（通常の操作をされる方向け）

1　BioStar ログイン方法

入退室システムの管理を行うためには、管理ソフトウェアである、BioStar2 というソフトウェアにログインをして操作を行います。
ここでは、管理ソフトウェア BioStar2 へのログインの方法について説明します。

PC のデスクトップにある BioStar2 のアイコン（右図）をダブルクリックしてください。
以下の画面が表示されたら、ユーザーID とパスワードを入力しログインしてください。



弊社の標準でのインストールの場合、

ユーザーID：**admin**

パスワード：**Admin1234**

となります。

もし、お客様が変更された場合は、変更後の値を入力してください。

もし、右図のように、ID またはパスワードが無効との表示が出た場合は、
再度、ID とパスワードをご確認ください。

また、以下のような、アクセスできない旨の画面が出た場合は、
ご利用環境が変化した可能性が高いです。
トラブルシューティング 28 章を参考に、ご確認をお願いします。

2　ユーザーの追加（BioStar システムを利用する資格者を追加する）

ユーザーを追加するためには、BioStar2 にログイン後、左側の「ユーザー」メニューをクリックし、ユーザー編集の画面を表示します。

（※もし、「ユーザー」のメニューが表示されていない場合は、ユーザー追加の権限の無いユーザーでログインされています。
システム管理者に確認をしてください。）

ユーザーの画面に移動したら、 ユーザーの追加 ボタンをクリックしてください。

（※もし、「ユーザーの追加」のボタンが表示されていない場合は、ユーザーの追加の権限の無いユーザーでログインされています。
システム管理者に確認をしてください。）

以下のようなユーザー作成画面が、表示されます。

［情報］項目

① ユーザーの写真を追加することが可能です。必要な場合は、 ＋画像 をクリックして、写真等の画像を選択します。
また、後述する「顔」および「ビジュアル顔」の登録時に プロフィールイメージで使用 に☑を入れると、こちらの画面に反映されます。

② ユーザー名を入力してください。（区別を付けやすくするため、入力を推奨します。）最大 48 文字まで入力できます。

③ ユーザーが所属する部門名を入力してください。この項目はモバイルアクセスカードのスマートフォンアプリの「部門」に反映されます。スペース（全角および半角）および＿（半角アンダーバー）を含めて、64 文字まで入力できます。
数字は半角で入力してください。

④ 必須入力項目です。初期値は、連番の空き番の数字が自動入力されます。必要に応じて変更してください。

⑤ ユーザーの所属するグループ（部署）名を選択してください。事前に作成されているユーザーグループからの選択となります。（ユーザーグループの作成方法は、3 章をご確認ください。）

⑥ ユーザーの認証可能な有効期限（開始～終了）を設定します。
2001/1/1 0 時～2030/12/31 23 時 59 分の範囲で選択します。

⑦ WEB ブラウザから、管理ソフト BioStar2 へのログインを行うか？により設定します。
管理ソフトを操作するユーザーの場合は、操作権限を選択し、その下の ログイン ID および パスワードを設定します。
BioStar2 にはログインせず、BioStar システムの利用者（認証者）になるユーザーの場合は、「未設定」を選択してください。
この場合はログイン ID とパスワードの入力欄は表示されません。
（管理者の操作権限を作成する場合は、21.1 章を参照してください。）

⑧ E メールアドレスを入力してください。
※モバイルアクセス、またはビジュアル顔のモバイル登録をご利用の場合は必ず入力が必要となります。

⑨ 役職名を入力してください。この項目はモバイルアクセスカードのスマートフォンアプリの「役職」に反映されます。
スペース（全角および半角）および_（半角アンダーバー）を含めて、64 文字まで入力できます。
数字は半角で入力してください。

⑩ 電話番号を入力します。（必要な場合は管理用に入力してください。BioStar2 では利用しません。）

⑪ ユーザーの認証を一時的に無効にすることができます。

⑫ ユーザーを所属させるアクセスグループを選択します。事前に作成されているアクセスグループからの選択となります。
この項目でも選択可能ですが、ここで設定をするとユーザー単位でのアクセスグループ登録となるため、わかりにくくなります。
ここでは設定をせず、16 章の方法で後から設定することを推奨します。

⑬ BioStar 操作権限で、ユーザーが WEB ブラウザからアクセスすることを許可した場合に、特定の IP アドレスからしかアクセスできなくする設定です。空欄にすると、どの IP アドレスからでもログインできるようになります。

[資格]項目

その下にスクロールすると、以下の設定内容があります。

・PIN コード:ユーザーの暗証番号です。認証機に 10 キーが付いている機種の場合、PIN コードを登録しておくことで、認証方法の補助的な1つとして利用することができます。☑をすると、右側に確認入力欄が表示されます。同じ数字を入力してください。入力可能な桁数は 4 桁以上 16 桁以下の数値のみです。

・認証モード:端末標準設定 か、個別設定を選択可能です。端末標準設定を選択した場合は、端末の認証モードに従って認証します。(例えば、端末が 「カード＋指紋」の設定の場合は、このユーザーもカード＋指紋)
個別設定にした場合は、その後、個別の認証方式を設定します。(例えば、カードのみ)
そして個別設定にした場合は、端末の初期値の認証モードを含むかどうか？を選択します。
「含む」を選択した場合は、[端末の設定 ＋ ユーザーの個別の設定]の認証モードが利用可能です。
「含まない」を選択した場合は、端末の認証モード設定は関係せず、このユーザーの個別の設定モードが利用可能となります。
個別設定の認証モードを設定した場合の画面例は、以下のようになります。

・資格:指紋/顔/ビジュアル顔/カード/モバイル/QR/バーコードの登録を行う時にボタンをクリックします。BioStar では、利用される認証機により、登録する資格情報が変化しますが、複数の機種を同時に利用できるように、ユーザーに認証資格情報を登録します。

(例:
・顔認証機のみをご利用のお客様は、顔データとカードデータを登録
・指紋認証機のみをご利用のお客様は、指紋データとカードデータを登録
・カード認証機のみをご利用のお客様は、カードデータを登録
・顔認証機と指紋認証機をご利用のお客様は、顔データと指紋データとカードデータを登録
のように、必要な認証データを登録してください。)

それぞれの資格情報の登録方法は、以下の章を参照してください。

指紋情報:9 章　顔情報:10 章　ビジュアル顔情報:11 章　カード情報:8 章
モバイル情報:12 章　QR/バーコード情報:13 章

・1:1 セキュリティレベル： 1:1 認証モードの場合（指紋および顔）のセキュリティレベルを設定します。
端末標準設定の場合は、端末により自動設定されます。
その他、最低/低/通常/高/最高 まで選択可能です。セキュリティレベルを上げると、判定が厳しくなりますので、指紋のふやけや顔のむくみなどで、認証エラーになる可能性があります。しかし、逆に、セキュリティレベルを下げると、判定が緩くなるため、似ていると認証成功になる可能性が出ます。状況に応じて設定変更してください。

更に下にスクロールすると、適用ボタンがありますので、入力後、クリックしてください。

適用ボタンを押した場合に、認証機にユーザーデータが転送されるか？は、他の設定により変わりますので、その条件については、21.5 章の「サーバー項目＞自動ユーザー同期」の項目をご参照ください。

3　ユーザーグループの作成（各ユーザーの所属する部門を作成する）

ユーザーグループのイメージは、所属部署のイメージとなります。

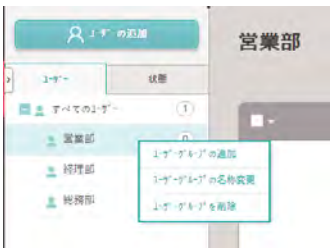
このユーザーグループは、必ず利用しないとならない機能ではありません。しかし、ユーザーグループの機能を利用することで、以下のことが、できるようになります。

・ユーザーを部署ごとに纏めて管理できるためわかり易い。（フォルダ分けのイメージ）
・アクセス権限を、ユーザーグループごとに作成できるため、ユーザーグループに所属することでアクセス権限が付与できる。
（例：総務と経理が入っている部屋のドアに対して、アクセス権限を
ユーザーグループ「総務部 と 経理部」の 2 つに設定する。
あとは、ユーザー作成の際に、ユーザーグループで、総務部 または 経理部 を選択したユーザーは、自動的に、そのドアに対してのアクセス権を得る。）
・部署単位での一括操作ができる。

ユーザーグループについては、BioStar2 は、初期値で一番上の階層に、「すべてのユーザー」という、ユーザーグループが作成されている形になります。この下の階層を編集していくことが可能です。
各階層で、右クリックすると、サブメニューが表示されますので、ユーザーグループを作成・削除・編集が可能です。

・「すべてのユーザー」階層は、名称変更/削除できないため、
ユーザーグループの追加　のみ選択可能

・その他の階層では、
・（下の階層への）ユーザーグループの追加
・ユーザーグループ名の変更
・ユーザーグループの削除
が可能です。



※ユーザーグループの名称は、48 文字まで入力可能です。（全角/半角問わず）
※ユーザーグループは、最上位（すべてのユーザー）を含まず、8 階層まで作成可能です。

事前にユーザーグループが、作成されている場合は、ユーザーの追加時に グループ の項目で選択可能となります。

また、ユーザーグループは、一度作成すると、ドラッグ＆ドロップで階層の変更が可能です。
便利な部分もありますが、予定外に変更してしまわないよう、ご注意ください。
各ユーザーグループでアクセス権限を持っている場合、親のアクセス権限に変更されてしまいます。

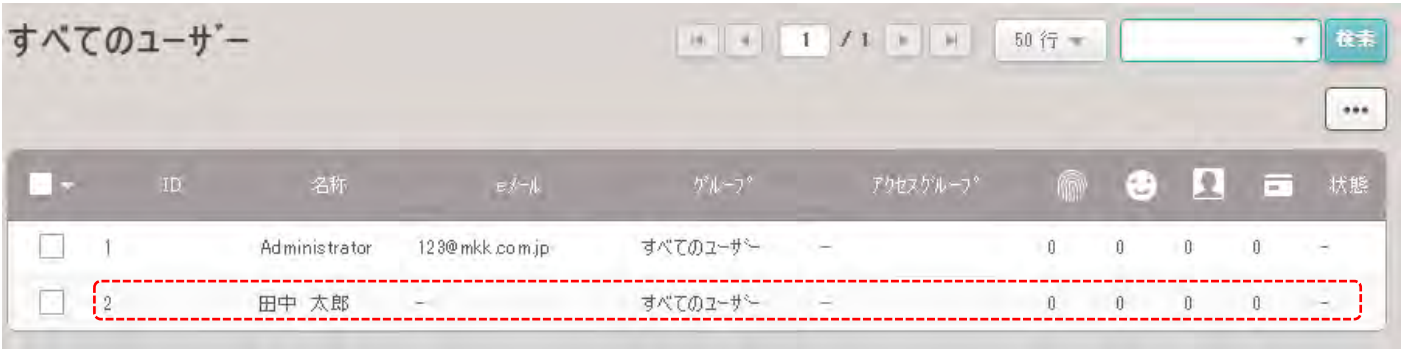
例：大阪営業所を 誤って、東京営業部の下に
ドラッグ＆ドロップしてしまった例

4　ユーザーの再編集（BioStar システムを利用する資格者の情報を編集する）

4.1　　ユーザー再編集

ユーザーの情報を変更する場合は、以下の方法で編集します。

「ユーザー」のボタンをクリックすると、下図のように、ユーザーの一覧が表示されます。



編集したいユーザーをクリックしてください。（但し、一番左のチェックボックス列を除く。上記　赤の点線範囲）

各ユーザーの編集画面になります。あとは、ユーザー作成時と同様の操作で編集し、「適用」をクリックして反映してください。

ユーザーの再編集では、以下のことが可能です。

- ユーザーの名称の変更
- ユーザーのグループの変更
- ユーザーの利用状態の変更
- ユーザーの有効期限範囲の変更
- ユーザーの BioStar 操作権限（および　パスワード）の変更
- ユーザーのアクセスグループの個人単位での変更（ユーザーグループ単位で設定されているものは変更できません。）
- ユーザーIP の変更
- PIN コードの変更
- 認証モードの変更（端末標準設定か個別指定か）
- 指紋/顔/カード等の各種　資格情報の　追加・削除・変更
- カード登録がある場合、無効化/有効化
- 1:1 セキュリティレベルの変更

4.2 一括ユーザー編集

複数のユーザーを一括で編集する場合は、以下の方法で編集します。

「ユーザー」のボタンをクリックすると、下図のように、ユーザーの一覧が表示されます。

編集したいユーザーに☑を入れると、右上に  というボタンが表示されます。そのボタンをクリックすると下図の画面が表示されます。

・グループ
・状態
・有効期限
・アクセスグループ
・BioStar 操作権限

について一括で編集することが可能です。

編集したい項目の  をクリックしてください。

一括編集を終了する場合は、「OK」をクリックしてください。

5　ユーザーの削除（BioStar システムを利用する資格者の情報を削除する）

ユーザーの削除については、21.5 章 「サーバー項目＞自動ユーザー同期」の設定により、動作が異なります。

自動ユーザー同期を行う場合は、PC（BioStar2 管理ソフトウェア）から、ユーザーを削除すると、同期され認証機からもユーザーが削除されます。

自動ユーザー同期を行わない場合は、PC（BioStar2 管理ソフトウェア）から、ユーザーを削除しても同期はされないため、認証機内のユーザー情報は、別途削除する必要があります。

また、自動ユーザー同期の設定であっても、認証機からだけユーザーを削除することが可能です。

ここでは、PC（BioStar2 管理ソフトウェア）上のユーザー削除の方法と、認証機内のユーザー削除の方法を記載します。

5.1　PC 上のユーザーを削除する方法

・自動ユーザー同期の設定が連動する設定：認証機内のユーザーも一緒に削除される。

・自動ユーザー同期の設定が連動しない設定：認証機内のユーザーは、認証機内に残る。

ユーザーの一覧の画面を表示します。

上記の赤点線枠のように、削除したいユーザーに ☑をつけます。

すると、右上に、  というボタンが表示されるので、クリックしてください。

確認画面が表示されるので、本当に削除でいい場合は、「はい」をクリックしてください。

5.2 認証機内のユーザーを削除する方法

認証機内のユーザーを削除する方法は、2 つの方法が利用可能です。

・認証機内のユーザー情報を確認しながら削除：自動ユーザー同期の設定にかかわらず利用可能。

・PC からユーザーを指定して、認証機から削除：自動ユーザー同期の設定が「利用しない」設定の場合利用可能。

認証機内のユーザー情報を確認しながら削除する方法は、以下となります。
「端末」のメニューをクリックし、該当の認証機で右クリックします。
その際に表示されるメニューの中から、
「端末別ユーザー情報の整理」というメニューを選択します。

該当端末内のユーザー情報が表示されますので、以下の画面のように、
削除したいユーザーに☑をつけて、 削除 ボタンをクリックしてください。

次に、ユーザー自動同期の設定が、利用しない設定になっている場合に利用できる方法です。
連動しない設定の場合は、ユーザーの画面で、認証機から削除したいユーザーに☑をつけると、以下の画面になります。

連動しない設定の場合は、 端末から削除 というボタンが表示されます。
そのボタンをクリックし、どの端末からユーザーを削除するかを選択して、「削除」ボタンを押してください。

このように認証機内からユーザーを削除することで、認証機で認証できなくなります。

6　ユーザーの転送（BioStar システムを利用する資格者の情報を認証機に送る）

ユーザーの転送については、21.5 章 「自動ユーザー同期」の設定により、動作が異なります。

自動ユーザー同期を行う場合は、PC（BioStar2 管理ソフトウェア）から、ユーザーを編集・適用すると、自動的に同期され認証機からにユーザーデータが転送されます。この場合は、ユーザー転送の操作を行う必要はありません。

しかし、自動ユーザー同期を利用しない設定の場合は、ユーザー情報を変更後、手動で認証機に上書きでのユーザー転送を行う必要があります。

ここでは、その場合の方法を記載します。

自動ユーザー同期が、「利用しない」設定の場合は、ユーザーの画面で、情報を変更し、認証機に転送したいユーザーに☑をつけると、以下の画面になります。

すると、右上に、 端末に転送 というボタンが表示されるので、クリックしてください。以下の画面が表示されます。

該当のユーザーを転送した端末に☑をつけ、下部の「ユーザー情報に違いがあった場合、上書きします」にも☑をつけ、「転送」ボタンをクリックしてください。

これにより、PC 上のデータが、認証機に上書きで転送され反映されます。

7　ユーザーを認証機から PC にコピー（認証機内の資格者情報を BioStar2 にコピー）

PC のユーザー情報が常に最新である場合は不要ですが、以下のような場合で必要がある場合は、認証機の中にあるユーザーデータを、PC にコピーすることが可能です。

・自動ユーザー同期は、「利用しない」設定の時、PC からユーザーを消してしまった

・PC からではなく、認証機の液晶メニューからユーザーを登録したため、認証機内にしかユーザー情報がない

・PC が故障してしまい、ユーザーデータが無くなってしまったため、認証機からユーザーデータを回復させたい

「端末」のメニューをクリックし、ユーザー情報をコピーしたい認証機で右クリックします。

その際に表示されるメニューの中から、

「端末別ユーザー情報の整理」というメニューを選択します。

該当端末内のユーザー情報が表示されますので、以下の画面のように、

PC にコピーしたいユーザーに☑をつけて、 アップロード ボタンをクリックしてください。

選択したユーザーをアップロードするか？　の確認画面が表示されます。

問題ない場合は、「はい」を選択してください。

なお、既に、アップロードするユーザーID のユーザー情報が PC 側にある場合は、上書きされてしまいますので、操作の際はご注意ください。

8　カードの管理(カードの登録・ユーザーへの割当・割当解除・無効化)

本章では、カードを管理する方法について記載します。

BioStar2 システムでは、1 ユーザーに対して、最大で 8 カードまで登録・割当可能です。
また、複数のユーザーで 1 枚のカードを共有して利用することはできません。
(CSN カード・Wiegand カード・モバイルカード・セキュア資格カード・アクセスオンカード・QR コード を含め 8 までです。)

カードは、顔認証機/指紋認証機/カード認証機のすべての認証機で利用可能です。

8.1　カードの登録 および ユーザーへのカードの割当

ユーザーに対して、カードを登録し、割当する方法は、認証機(登録機含む)で、実物のカードを読込させるか、カードの ID を手入力するか、11 章の CSV ファイルからのインポートで割当をするか、いずれかの方法となります。

ここでは、カードリーダーを利用した登録・割当方法と、カード ID の手動入力方法について説明します。

カードの登録およびユーザーへの割当は、ユーザーの画面から行います。

2 章(ユーザー追加) または 4 章(ユーザーの再編集)の操作を行い、該当ユーザーの資格情報の部分の

をクリックしてください。以下の画面が表示されます。

・カード種別:CSN/Wiegand/スマートカード および カード読出し から選択

※CSN は、Card Serial No の略であり、一般的な IC カードの ID のことを指します。
Wiegand カードは、ご利用のカードが、iCLASS/HID Prox カードの場合に利用できます。このため、弊社で取り扱いの認証機では利用できません。
スマートカードは、Mifare/DESFire カード等のカード ID の部分を利用せず、カードのユーザー書き込み領域を利用して、ID を書き込み、それを利用します。この場合は、通常のカード ID は利用できなくなり、本システムで専用に発行したカードのみが利用できるようになります。
一般的な IC カード(Mifare や、FeliCa)の場合は、 CSN を選択してください。

ここでは、CSN を選択した場合について説明します。(スマートカードの利用方法は、8.5 章を参照してください。)

・登録方法:カードリーダーによる登録/カードの割当/手動入力 から選択

カードリーダーによる登録を選択した場合は、その次に、登録に使う端末を選択します。
手動入力を選択した場合は、カード ID 枠に、ID を手入力できます。
カードの割当については、8.2 章で説明します。

・端末:登録に利用する端末を選択します。ドアの横に設置してある認証機か、USB 接続タイプの卓上型カード登録機(接続している場合)を選択することができます。

カード読出し ボタンをクリックすると、10 秒間、選択した端末がカード読出しモード（ランプが緑色の点滅）になりますので、読出しモードの間に、登録したいカードを端末にかざしてください。

読出しが完了すると、以下の画面のようにカードの ID が表示されます。

（表示される桁数は、カードの種類によっても変化します。）

読出しができたら、「登録」ボタンをクリックし、登録完了してください。

もし、登録をクリックした際に、右のような画面が表示された場合は、そのカードは既に、別のユーザーに割当たっています。
割当たっているユーザーのカードを削除するか、別のカードをご登録してください。
割当たっているユーザーの確認は、21.3 章をご確認ください。

「登録」ボタンをクリックし、そのカード ID の重複割当がない場合は、以下のように、ユーザーにカードが割当てられます。

最後に、この状態を確定させるには、ユーザー作成・編集画面の右下の「適用」ボタンをクリックする必要があります。

8.2 ユーザーへのカードの割当（登録済みカードの再割当）

本システムでは、一度、カードを読み込ませて登録すると、その情報は削除されません。
例えば、カードを登録・割当をしたユーザーから、

・カードを削除した場合
・ユーザー自体を削除した場合

は、そのカードデータは、自動的に、「未割当カード」という扱いとなります。
どのユーザーにも割当たっていないが、システムとして登録済みのカード、という扱いです。

その状態であれば、再度、カードの登録処理をし直すことなく、新たに割当てたいユーザーに対して、未割当カードの割当て処理を行うことで、カードを割当てることが可能です。

カードの割当ては、ユーザーの画面から行います。
2 章(ユーザー追加) または 4 章(ユーザーの再編集)の操作を行い、該当ユーザーの資格情報の部分の

をクリックしてください。以下の画面が表示されます。

この画面で、登録方法を、「カードの割当」としてください。

未割当カードの一覧が表示されます。その中から、割当をしたいカードを選択してください。
量が多く見つけにくい場合は、検索欄にカード ID のすべてまたは一部を入力することで、絞ることができます。
割当したいカードを選択し、「登録」をクリックすることで、未割当のカードをユーザーに再割当することが可能です。

8.3 ユーザーのカードの割当解除（ユーザーからカードの削除：カードの割当の解除）

ユーザーに割り当てたカードを解除する場合は、以下の方法があります。

・ユーザーからカードを削除する

・カードを持ったユーザー自体を削除する

ユーザー自体の削除方法は、5.1 章を参照してください。
ここでは、ユーザーからカード情報だけを削除する方法について説明します。

カードを削除したいユーザーの編集画面に進み、資格情報の部分にスクロールします。
以下のように、登録されているカードの CSN が表示されています。

ここで、削除したいカードの ゴミ箱 アイコンをクリックすることで、カード情報を削除できます。
ゴミ箱アイコンをクリックすると、「削除してよいか？」の確認が表示されますので、「はい」を選択してください。
この時点で、ユーザーから見た目上は、カードが削除されたように見えます。変更を反映するためには、この画面の一番下の「適用」ボタンをクリックしてください。
これにより、削除したカードは、未割当カードとなります。
再度、そのカードを登録する場合は、カード登録で、カードの再割当（8.2 章）の操作をするか、新規に登録（8.1 章）の操作を行ってください。

8.4 ユーザーのカードの無効化（カードのブラックリスト登録）

ユーザーに割り当てたカードを一時的に利用できなくする方法があります。
例えば、カードを紛失してしまった可能性もあるが、紛失していないかも知れない。という状態の時に、カード情報を削除してしまうと、もしも、発見された場合に、再度登録（再割当）をし直さないとなりません。
このような状態の場合に、一時的に該当カードの利用を停止することが可能です。

カードの利用を停止したいユーザーの編集画面に進み、資格情報の部分にスクロールします。
以下のように、登録されているカードの CSN が表示されています。

ここで、該当するカードの 無効化 ボタンをクリックすることで、カードがブラックリスト登録され、次回利用された際に、認証エラーとなり、ログに、ブラックリストカードが利用された旨が表示されます。
また、 無効化 ボタンをクリックすると、ボタンの表示が 有効化 と変化します。この 有効化 ボタンをクリックすることで、カードは、ブラックリストから除外され、元通りの動作になります。

一時的に該当カードでの認証を停止したい場合は、無効化してください。

尚、本説明の「無効化」および「有効化」については、クリックした時点で動作しますのでご注意ください。
画面下部の「適用」ボタン、および「キャンセル」ボタンに関係なく、「無効化」および「有効化」はクリックした時点で反映されます。

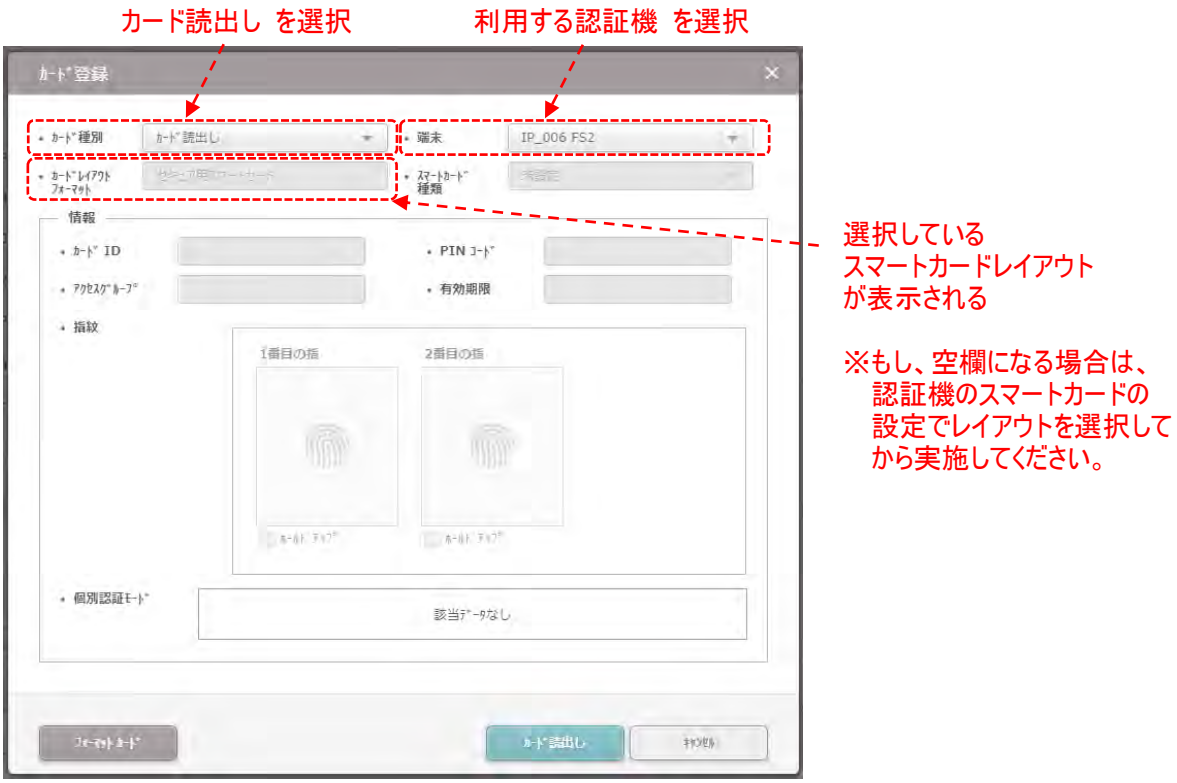
8.5 スマートカードの利用方法

スマートカードを各ユーザーが利用する場合は、初めて利用する場合に、最初に、作成したフォーマットで、
カードのユーザー領域をフォーマットする必要があります。
（認証機のスマートカードのレイアウト設定で、作成したスマートカードレイアウトが選択されている必要があります。）
その後、各ユーザーの資格情報をカードに書き込みます。

8.5.1 スマートカードのフォーマット

スマートカードを、初めて利用する場合、購入後の Mifare カード及び DES Fire カードに対して、作成した
スマートカードレイアウトでフォーマットする必要があります。

各ユーザーの画面で、 + ｶｰﾄﾞ をクリックします。開いた画面の カードの種類 を「カード読出し」にします。



ここまで確認ができたら、 フォーマット カード をクリックします。

選択した認証機が、カード読込モードになりますので、フォーマットしたいカードをかざしてください。

指定した スマートカードレイアウトで フォーマットが完了すると、上記の表示となります。

8.5.2 スマートカードの書き込み

スマートカードを書き込む際に、スマートカードの種類が、以下の 2 種類あり選択することが可能です。
用途に合わせて、選択してください。

種類 / 特徴	セキュア資格カード	アクセス オン カード
登録可能情報	・カード ID ・PIN コード ・指紋 ・ビジュアル顔	・カード ID ・PIN コード ・指紋 ・ビジュアル顔 ・アクセスグループ ・有効期限 ・個別認証モード

カードに書き込みたい情報は、事前に、BioStar2 のユーザー情報で設定しておく必要があります。

ここでは、例として、以下の状態のユーザーをスマートカードに書き込みます。

該当ユーザーの画面で、 + ｶｰﾄﾞ をクリックします。開いた画面の カードの種類 を「スマートカード」にします。

選択している
スマートカードレイアウト
が表示される

※もし、空欄になる場合は、
認証機のスマートカードの
設定でレイアウトを選択して
から実施してください。

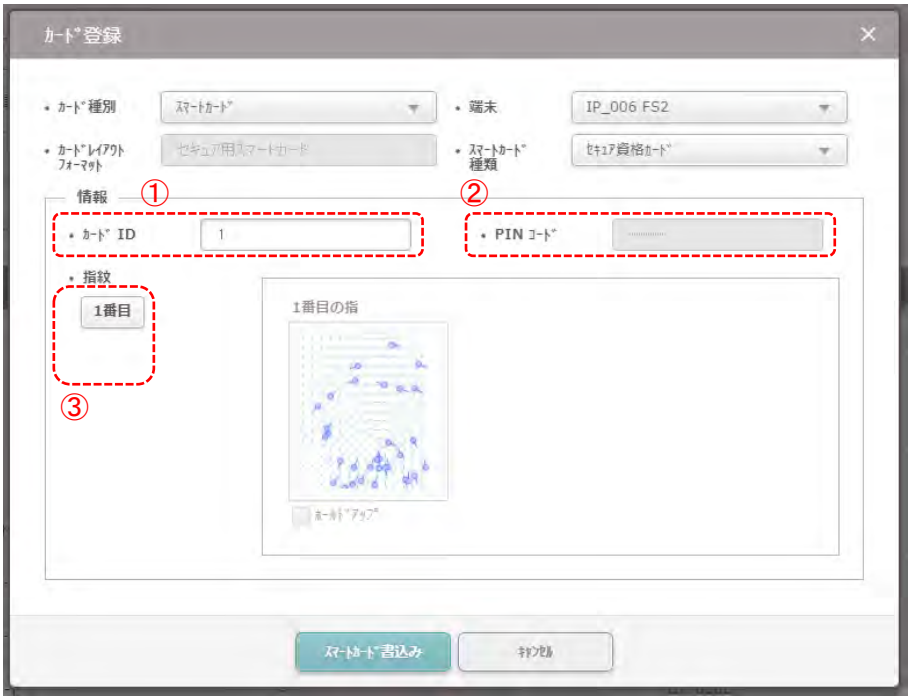
スマートカード を選択

利用する認証機 を選択

・セキュア資格カード
・アクセス オン カード
のどちらかを選択

8.5.2.1 セキュア資格カード の書き込み

スマートカードの種類で、 セキュア資格カード を選択した場合は、以下の画面となります。



① スマートカードとして利用するカード ID を登録します。
通常は、自動的に採番される番号のままで構いません。
もし、変更されたい場合は、重複しない自由な数値としてください。

② ユーザーの PIN コードのが、そのまま適用されます。

③ カードに書き込む指紋を選択します。複数登録されている場合は、複数から選択する形になります。
指紋を使わない場合は、選択しなくても構いません。

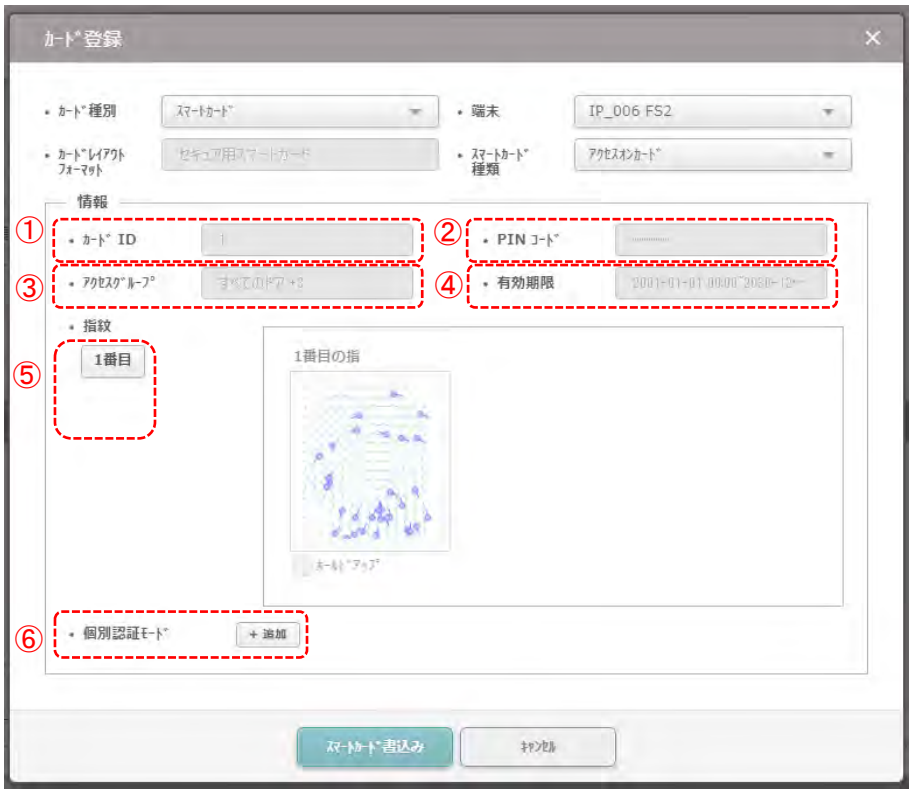
上記の設定ができたら、 ｽﾏｰﾄｶｰﾄﾞ書込み をクリックしてください。

選択した認証機が、カード読込モードになりますので、事前にフォーマット済みのカードをかざしてください。

スマートカードに書込みが完了すると、上記の表示となります。

8.5.2.2 アクセス オン カード の書き込み

スマートカードの種類で、 アクセス オン カード を選択した場合は、以下の画面となります。



① スマートカードとして利用するカード ID が登録されます。
② ユーザーの PIN コードのが、そのまま適用されます。
③ ユーザーのアクセスグループが、そのまま適用されます。
④ ユーザーの有効期限が、そのまま登録されます。
⑤ カードに書き込む指紋を選択します。複数登録されている場合は、複数から選択する形になります。
指紋を使わない場合は、選択しなくても構いません
⑥ 個別認証を行う場合は、 + 追加 をクリックします。

表示された画面で、このアクセス オン カードで行う個別の認証モードの組み合わせを行います。
組み合わせた後、 OK をクリックします。

設定が完了したら、 ｽﾏｰﾄｶｰﾄﾞ書込み をクリックしてください。

選択した認証機が、カード読込モードになりますので、事前にフォーマット済みのカードをかざしてください。

スマートカードに書込みが完了すると、上記の表示となります。

9　指紋の管理（ユーザーの指紋登録・ユーザーの指紋更新・ユーザーの指紋削除）

本章では、指紋を管理する方法について記載します。

BioStar2 システムでは、1 ユーザーに対して、最大で 10 本まで指紋登録が可能です。

指紋は、指紋認証機のすべての認証機で利用可能です。

9.1　指紋の登録

ユーザーに対して、指紋を登録する方法は、認証機（登録機含む）で、指紋を読み込ませる必要があります。

指紋の登録は、ユーザーの画面から行います。

2 章(ユーザー追加) または 4 章(ユーザーの再編集)の操作を行い、該当ユーザーの資格情報の部分の

をクリックしてください。以下の画面が表示されます。

・端末：指紋の登録時に利用する端末を選択してください。

登録されている認証機・登録機の中で、指紋登録ができる機種が表示されますので、1 台選択してください。

・登録許可点数：指紋の登録点数が、この点数以上の場合に、登録を可能とします。20～100 の範囲で選択可能です。

登録しづらい場合は、この点数を下げることで登録しやすくなりますが、点数を下げて登録した指紋が多くなると、誤認証や認証しないという状況が発生しやすくなります。極力、この点数は 80 点のまま登録することを推奨します。この点数を下げないと指紋が登録できない場合は、「カード＋指紋」での認証方式などを併用し、誤認証しないような方法をご検討ください。

・画像表示：画像表示に☑をつけると、実際の指紋画像が表示されます。

・「＋追加」ボタン：　クリックするごとに、登録用の枠が、10 本まで追加可能です。

・「〇番目」ボタン：「＋追加」をクリックするごとに、10 番目　まで、枠が増えます。指紋番号を選択します。

・「読取り」ボタン：選択している「〇番目」の指を登録します。

・「削除」ボタン：選択している「〇番目」の指紋データを削除します。

・「検証」ボタン：選択している「〇番目」の指紋データが過去に登録があるか？を確認します。

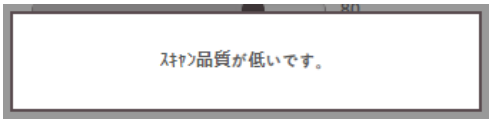
・「ホールドアップ」チェック：2 番目以降の指紋に対し、ホールドアップ指紋として設定できます。

ホールドアップ指紋とは、認証するときに、端末側は通常の動作をしますが、実際に BioStar に届くログでは、ホールドアップ指紋で認証したことがわかります。背後から無理に脅されて認証させられた場合に、本人しかわからないホールドアップ指紋で認証することで、システム管理者に通知をするための指紋です。このような理由のため、1 番目の指は、ホールドアップ指紋に登録できません。

登録手順は、以下の順番となります。

・指紋を登録する端末（認証機または登録機）を選択
・登録許可点数を指定（通常は、80 のままを推奨します）
・（初回の場合）「＋追加」ボタンをクリックし、
　「1 番目」のボタンを表示（1 番目が選択状態となっています）
・「読取り」ボタンをクリック（1 番目の指を読取る。という動作）
・指定した端末が、指紋登録モードになります。
　画面や LED の指示に従いながら、同じ指を、2 回登録します。
　何もしないまま 10 秒経過すると、タイムアウトエラーになります。
　その場合は、再度、「読取り」ボタンをクリックしてください。
・2 回とも登録許可点数以上の指紋の場合、画面に指紋の
　特徴点の画像イメージが表示されます。（右図）
・「登録」ボタンをクリックして登録します。
・最後に、ユーザーの作成・編集画面の下部の「適用」を
　クリックすることで登録完了となります。

※指紋登録の際に、2 回のうち、どちらかが登録許可点数を
　超えない場合、右図の表示がされ、指紋登録がキャンセルされます。
　再度、「読取り」ボタンのクリックから行ってください。



※指紋登録の際に、認証機ではなく、USB 接続の指紋登録機を選択された場合は、登録の際の画面が、
　上記と異なります。実際の指の画像が見える画面がポップアップされ表示されますが、基本的な考え方は、
　同じです。指紋登録許可点数を超える指の状態を 2 回スキャンして登録となります。

※登録の際に、右図の表示がされた場合は、指紋が読み取りされて
　いない場合に表示されます。特に複数の指紋を登録する場合は
　すべての登録枠をご確認ください。

9.2 指紋の更新（登録済みの指に上書きで指紋登録）

指紋の更新（指紋の上書き登録）は、新しい指紋の登録と近い操作です。ユーザーの編集画面から、資格情報の部分を確認すると、登録されている指紋の数が表示されます。

上図は、指紋が 2 本登録済みの例です。
この状態で、指紋情報を更新する場合は、 + 指紋 または、指紋情報の ✎ をクリックしてください。（どちらも同等）

再度、指紋の登録画面が表示されますので、更新したい「〇番目」のボタンをクリックし、そのまま、「読取り」ボタンを押して、再度、指紋を登録してください。自動的に古い指紋データは上書きされます。
（〇番目の指を、再度、上書きで読取る。 という操作です。）

この上書きデータも、ユーザーの画面の下部の「適用」をクリックすることで反映されますので、反映する前に、キャンセルや他の画面に遷移などをしてしまい、保存されないまま終わってしまうことが無いよう、ご注意ください。

9.3 指紋の削除

指紋の削除についてですが、ユーザーを削除した場合は、指紋も一緒に削除されます。ここでは、ユーザーは残したまま、指紋情報だけを削除する方法について記載します。

もし、複数登録があるうちの1つの指紋だけを削除する場合は、該当ユーザーで、 + 指紋 または、指紋情報の ✎ をクリックしてください。（どちらも同等）

そして、削除したい指紋を「〇番目」のボタンで選択し、「削除」ボタンをクリックしてください。

もし、該当ユーザーの指紋をすべて削除したい場合は、1 画面前の指紋情報が見えている部分（下図）で、
ゴミ箱のアイコンをクリックしてください。

「すべての指紋を削除してよろしいですか？」の確認が表示されますので、「はい」をクリックすることで、すべての指紋が削除されます。

10 顔の管理(ユーザーの顔の登録・ユーザーの顔の更新・ユーザーの顔の削除)

本章では、顔データを管理する方法について記載します。(顔情報は、FaceStation2 で利用します。)

BioStar2 システムでは、1 ユーザーに対して、最大で 5 顔まで登録が可能です。

顔は、顔認証機で利用可能です。

顔の登録には、顔認証機ごとに、「簡易顔登録」の設定が可能です。

簡易顔登録の設定が「無効」の場合は、正面→上下→左右の順番で登録処理をします。「有効」の場合は、上下のみの登録処理を行います。このため、登録が簡単です。

しかし、正確・確実な認証のためには、少し時間はかかりますが、簡易顔登録は「無効」の設定を推奨いたします。

10.1 ユーザーの顔の登録

ユーザーに対して、顔を登録する方法は、認証機で、顔を読み込ませる必要があります。

顔の登録は、ユーザーの画面から行います。

2 章(ユーザー追加) または 4 章(ユーザーの再編集)の操作を行い、該当ユーザーの資格情報の部分の  をクリックしてください。以下の画面が表示されます。

・端末:顔の登録時に利用する端末を選択してください。
登録されている顔認証機が表示されますので、1 台選択してください。

・顔の登録角度レベル:登録する顔の角度を狭めるか広範囲にするか設定します。(初期値 4)
高くすると、顔の登録する角度範囲が広範囲となります。低くすると、顔の登録する角度範囲が狭くなり、正面向きに強くなります。
比較的、狭い通路の場合は、顔の角度が変わることは少ないため、低くすることを推奨します。認証機の横方向から歩いてきて顔認証する場合は、顔の左右の角度が振れやすいので、その場合は、高くすることを推奨します。必要に応じて変更してください。

・「+追加」ボタン: クリックするごとに、登録用の枠が、5 顔まで追加可能です。
・「○番目」ボタン: 「+追加」をクリックするごとに、5 番目 まで、枠が増えます。顔番号を選択します。
・「読取り」ボタン:選択している「○番目」の顔を登録します。
・「削除」ボタン:選択している「○番目」の顔データを削除します。
・「プロフィールイメージで使用」チェック:撮影した顔写真をユーザーのプロフィール画像として登録します。
(2 章の「+画像」ボタンの説明部を参照ください。)

登録手順は、以下の順番となります。

・顔を登録する顔認証機を選択
・顔の登録角度レベルを指定（通常は、4 のままで構いません）
・（初回の場合）「＋追加」ボタンをクリックし、「1 番目」のボタンを表示（1 番目が選択状態となっています）
・「読取り」ボタンをクリック（1 番目の顔を読取る。という動作）
・指定した端末が、顔登録モードになります。（認証機側の登録が完了するまで、PC 側は待機状態になります。）
　画面の指示に従いながら、顔を登録します。
　うまく水色の円グラフが伸びない場合は登録失敗になり、タイムアウトエラーになります。
　その場合は、再度、「読取り」ボタンをクリックしてください。
・100%まで円グラフが伸びると、読取り完了です。（登録者の顔写真が表示されます。）
・「登録」ボタンをクリックして登録します。
・最後に、ユーザーの作成・編集画面の下部の「適用」をクリックすることで登録完了となります。

10.2　ユーザーの顔の更新（登録済みの顔に上書きで顔登録）

顔の更新（顔の上書き登録）は、新しい顔の登録と近い操作です。ユーザーの編集画面から、資格情報の部分を確認すると、登録されている顔の数が表示されます。

上図は、顔が 2 顔登録済みの例です。
この状態で、顔情報を更新する場合は、 ＋顔 または、顔情報の ✎ をクリックしてください。（どちらも同等）

再度、顔の登録画面が表示されますので、更新したい「〇番目」のボタンをクリックし、そのまま、「読取り」ボタンを押して、再度、顔を登録してください。自動的に古い顔データは上書きされます。
（〇番目の顔を、再度、上書きで読取る。 という操作です。）

この上書きデータも、ユーザーの画面の下部の「適用」をクリックすることで反映されますので、反映する前に、キャンセルや他の画面に遷移などをしてしまい、保存されないまま終わってしまうことが無いよう、ご注意ください。

10.3 ユーザーの顔の削除

顔の削除についてですが、ユーザーを削除した場合は、顔も一緒に削除されます。ここでは、ユーザーは残したまま、顔情報だけを削除する方法について記載します。

もし、複数登録があるうちの1つの顔だけを削除する場合は、該当ユーザーで、 または、顔情報の を クリックしてください。(どちらも同等)

そして、削除したい顔を「〇番目」のボタンで選択し、「削除」ボタンをクリックしてください。

もし、該当ユーザーの顔をすべて削除したい場合は、1 画面前の顔情報が見えている部分(下図)で、

ゴミ箱のアイコンをクリックしてください。

「すべての顔を削除してもよろしいですか？」の確認が表示されますので、「はい」をクリックすることで、すべての顔が削除されます。

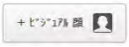
11 ビジュアル顔の管理（ユーザーの顔の登録・ユーザーの顔の更新・ユーザーの顔の削除）

本章では、ビジュアル顔データを管理する方法について記載します。（顔情報は、FaceStation F2 で利用します。）

BioStar2 システムでは、1 ユーザーに対して、最大で 2 ビジュアル顔まで登録が可能です。

11.1 ユーザーのビジュアル顔の登録

ユーザーに対して、ビジュアル顔を登録する方法は、認証機で、顔を読み込ませる方法と、画像ファイルをアップロードする方法があります。ビジュアル顔の登録は、ユーザーの画面から行います。

2 章(ユーザー追加) または 4 章(ユーザーの再編集)の操作を行い、該当ユーザーの資格情報の部分の  をクリックしてください。以下の画面が表示されます。

・① ビジュアル顔の登録時に利用する端末を選択してください。
　　登録されている FaceStation F2 が表示されますので、その中から 1 台選択してください。
・② クリックするごとに、登録用の枠が、最大 2 顔まで追加可能です。
　「〇番目」ボタンをクリックし、ビジュアル顔を登録する番号を選択します。
・③ 選択している端末で顔をスキャンし登録します。
・④ 選択している「〇番目」の顔に、アップロードする写真画像を選択する画面が表示されます。
　　形式は、jpg / png から選択可能です。
　　（小さすぎる解像度の画像は使えません。縦横 250 ピクセル以上の画像をご利用ください。
　　最大で縦横 1280 ピクセル以下です。最大ファイルは 10MB です。）
・⑤ 選択している「〇番目」の顔データを削除します。
・⑥ 「プロフィールイメージで使用」チェック：登録した顔写真をユーザーのプロフィール画像として登録する時☑をします。
　（2 章の「＋画像」ボタンの説明部を参照ください。）
・⑦ 画像ファイルをドラッグ&ドロップしてアップロードすることもできます。

「読取り」ボタンを利用した登録手順は、以下の順番となります。
・ビジュアル顔を登録する顔認証機を選択
・（初回の場合）「＋追加」ボタンをクリックし、「1 番目」のボタンを表示（1 番目が選択状態となっています）
・「読取り」ボタンをクリック（1 番目のビジュアル顔を読取る。という動作）
・指定した端末が、顔登録モードになります。（認証機側の登録が完了するまで、PC 側は待機状態になります。）
　　画面の指示に従いながら、顔を登録します。正面を向いて、顔の位置を合わせます。

・成功と表示された時、読取り完了です。(登録者の顔写真が表示されます。)
・「登録」ボタンをクリックして登録します。
・最後に、ユーザーの作成・編集画面の下部の「適用」をクリックすることで登録完了となります。

11.2 ユーザーのビジュアル顔の更新(登録済みのビジュアル顔に上書きでビジュアル顔登録)

ビジュアル顔の更新(ビジュアル顔の上書き登録)は、新しいビジュアル顔の登録と近い操作です。
ユーザーの編集画面から、資格情報の部分を確認すると、登録されているビジュアル顔の数が表示されます。

上図は、ビジュアル顔が 2 顔登録済みの例です。
この状態で、ビジュアル顔情報を更新する場合は、 + ﾋﾞｼﾞｭｱﾙ 顔 または、ビジュアル顔情報の ✎ をクリックしてください。
(どちらも同等)

再度、ビジュアル顔の登録画面が表示されますので、更新したい「〇番目」のボタンをクリックし、そのまま、
「読取り」ボタンを押して、再度、ビジュアル顔を登録してください。自動的に古いビジュアル顔データは上書きされます。
(〇番目のビジュアル顔を、再度、上書きで読取る。 という操作です。)

この上書きデータも、ユーザーの画面の下部の「適用」をクリックすることで反映されますので、反映する前に、キャンセルや他の画面に遷移などをしてしまい、保存されないまま終わってしまうことが無いよう、ご注意ください。

11.3 ユーザーのビジュアル顔の削除

ビジュアル顔の削除についてですが、ユーザーを削除した場合は、ビジュアル顔も一緒に削除されます。ここでは、ユーザーは残したまま、ビジュアル顔情報だけを削除する方法について記載します。

もし、複数登録があるうちの1つのビジュアル顔だけを削除する場合は、該当ユーザーで、 + ﾋﾞｼﾞｭｱﾙ 顔 または、ビジュアル顔情報の ✎ をクリックしてください。(どちらも同等)

そして、削除したいビジュアル顔を「〇番目」のボタンで選択し、「削除」ボタンをクリックしてください。

もし、該当ユーザーのビジュアル顔をすべて削除したい場合は、1 画面前のビジュアル顔情報が見えている部分(下図)で、ゴミ箱のアイコンをクリックしてください。

「すべての顔を削除してもよろしいですか？」の確認が表示されますので、「はい」をクリックすることで、すべてのビジュアル顔が削除されます。

12 モバイルの管理(モバイルカードの登録・無効化)

本章では、モバイルカードを管理する方法について記載します。(モバイルカードは、対応認証機で利用可能です。)
また、利用までの設定については、21.18 章を参照願います。

12.1 モバイルカードの登録 および ユーザーへのカードの割当

ユーザーに対して、モバイルカードを登録する場合は、モバイルカードの登録画面で入力するか、14 章の CSV ファイルからのインポートで割当をするか、いずれかの方法となります。

ここでは、モバイルカードの登録画面を利用した登録・割当方法について説明します。

モバイルカードの登録およびユーザーへの割当は、ユーザーの画面から行います。
2 章(ユーザー追加) または 4 章(ユーザーの再編集)の操作を行い、該当ユーザーの資格情報の部分の


をクリックしてください。以下の画面(ポータルサイトの種類により、画面が変化します。)が表示されます。

ポータルサイトが レギュラーの場合

ポータルサイトが ダイナミックの場合

・カード種別:ﾓﾊﾞｲﾙ CSN のみ

※CSN は、Card Serial No の略であり、ﾓﾊﾞｲﾙ用のカードの ID のことを指します。

・登録方法:カード割り当て / 手動入力 から選択

未登録カードの ID の中から選ぶ場合は、そのまま番号を選択してください。

手動入力を選択した場合は、ランダムで ID を決めるか、手入力が選択できます。

・情報:BioStar2 のユーザー情報に事前に入力することで、使用/未使用を変更できます。

ここで、「使用」を選択すると、スマートフォンアプリ側でその内容が表示されます。

・有効期限:ダイナミック 選択時は設定可能です。有効期限外の際は、認証してもエラーになります。

その後、「登録」をクリックし、その後、ユーザー情報自体を「適用」することで、設定されているポータルサイトと合わせ、登録されます。

登録すると、その情報は、同時にポータルサイトにも反映されるため、通信をおこないます。
以下の表示が出ることをご確認いただき、完了となります。

なお、モバイルカードを登録する場合は、利用者のスマートフォンに、ID を含めたアプリケーションのインストールリンクが送信されます。このため、ユーザー作成の時点で、必ず、E メールアドレス欄を入力しておく必要があります。
（E メールアドレス欄を入力指定ない状態だと、エラーとなります。）

また、モバイルカードの発行や、モバイルカードのシステムとしての利用期間は、ポータルサイトのタイプにより異なりますが、制限があります。クレジットが消費され、残クレジットがなくなると、発行や動作ができなくなります。
クレジット数の確認は、XXX 章をご参照ください。

12.2 モバイルカードの再発行

モバイルカードを登録したユーザーで、初回登録時のメールを再度受け取りたい場合は、再発行を行います。
登録したユーザー情報は、以下のようになっているため、再発行ボタンを押すことで、再度、ID を含めたアプリケーションのダウンロードリンクが登録メールアドレスに送信されます。

12.3 モバイルカードの無効化 および 有効化

モバイルカードを一時的に無効化する場合は、登録したユーザー情報の部分を表示し、無効化ボタンを押すことで、無効化できます。有効する場合は、同箇所の有効化ボタンをクリックしてください。

12.4 モバイルカードの削除

モバイルカードを削除する場合は、資格情報を表示し、モバイル CSN の部分で、 をクリックすることで削除できます。

クリックすると削除確認のダイアログが表示されますので、「はい」をクリックしてください。
その後、ポータルサイトから削除するために通信を行い、以下の画面が表示されます。

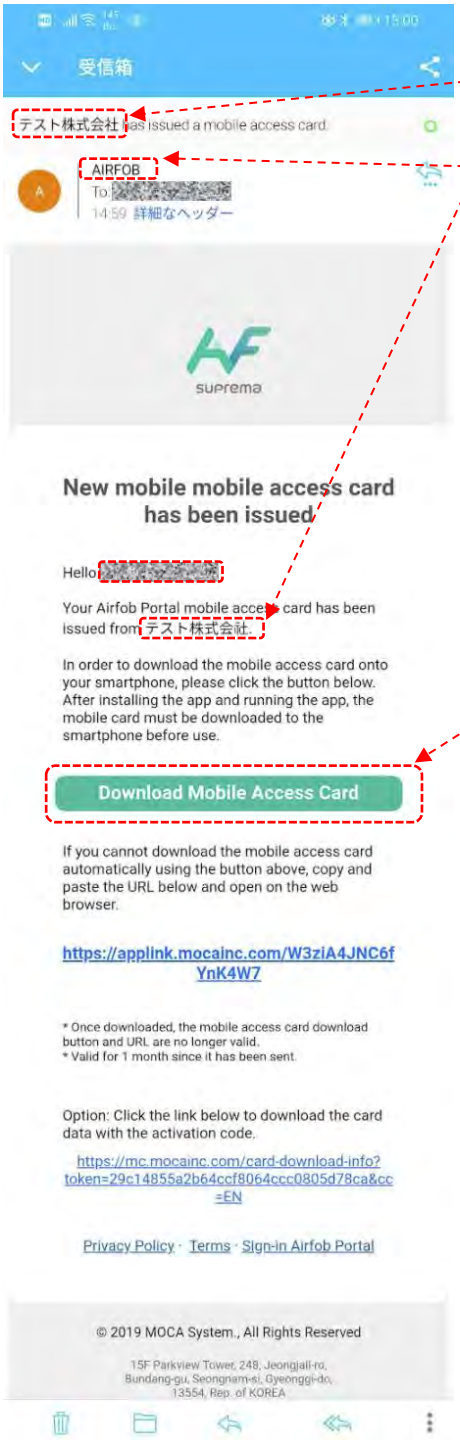
※但し、既に購入済みのモバイルクレジットを利用しているため、
削除しても、消費されたモバイルクレジットは回復しません。

12.5 モバイルカードの利用者側設定

本内容は、BioStar2 の管理者/操作者の行う操作ではありません。
管理者/操作者の方が、モバイルカードを登録すると、利用者の方にモバイルアクセス ポータルサイトよりメールが送付されます。そのメール受信及び、その先の設定について記載します。
（利用者の方に、その後の流れをご説明される場合にご利用ください。）

12.5.1 受信メール内容

BioStar2 でモバイルカードを登録すると、以下のようなメールが送付されてきます。（以下は、Android の場合です。）



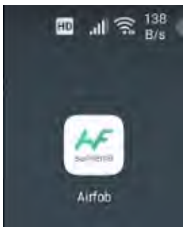
・ポータルサイト名

・送信者名：AIRFOB

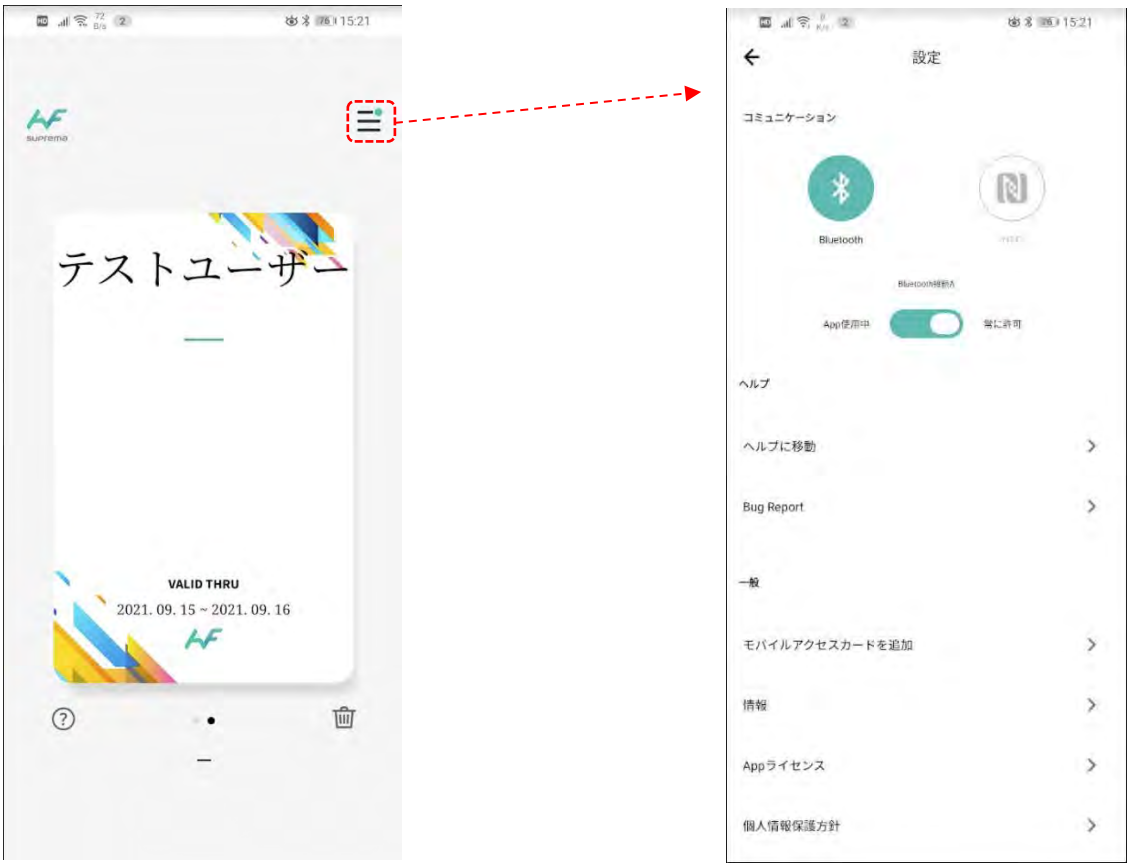
・Airfob アプリのダウンロードリンク
Android の場合は、PlayStore を開きダウンロードの確認画面に進みます。
iPhone の場合は、AppStore を開きダウンロードの確認画面に進みます。
クリックして、アプリのインストールに進んでください。

12.5.2 Airfob アプリの起動

インストールが完了すると、ホーム画面に、Airfob のアイコンが生成されます。



アプリを起動すると、Bluetooth を ON にすることや、位置情報の設定など確認されます。
指示に従い、必要な内容を設定してください。
その後、以下の画面となります。
（もし、下記の画面のようにカードの絵が表示されず、「未登録」と言う画面になる場合は、受信したメールから、再度、
Airfob アプリのダウンロードリンクの画面に進んでください。
ダウンロードの直前操作までを行うと、インストール済みのアプリが起動し、カードが登録されます。）



右上のアイコンをタップすると、設定画面が表示されます。
Android 版で、スマートフォンが、NFC に対応している場合は、NFC を選択可能です。
また、認証を Airfob アプリ起動中だけにすることも可能です。
（※常に許可 に設定しておくと、バックグラウンド動作時も認証可能です。
バックグラウンド実行も終了させた場合は、再度、Airfob アプリを起動するまで利用できません。）

12.5.3 認証動作

スマートフォンを認証機に 10cm 程度まで近づけることで、認証します。
スマートフォンのバイブレーション機能が有効な場合は、通信が始まると、バイブレーションが振動します。
1 秒程度のバイブレーションが停止した時点で、認証完了となります。
（認証成功となるか、失敗となるかは、BioStar2 のアクセスコントロールの設定により変化します。）

また、ご利用のスマートフォンケースによっては、Bluetooth 電波を通りにくくする素材のものもあります。
もし、うまく反応しない場合は、一度、スマートフォンケースをはずしてご確認ください。

そして、アプリの使い方の 1 つとして、Airfob アプリを起動し、カードの画面が出ている状態で、カードの部分を
ロングタップすると、スマートフォンの最大出力で Bluetooth 電波を飛ばします。
数 m 離れた位置から認証することも可能です。（但し、反応する認証機が近くに複数台存在しないこと）

13 QR/バーコードの管理

本章では、QR コード/バーコードを管理する方法について記載します。
（QR コード/バーコード情報は、X-Station2 で利用します。）

13.1 QR コード/バーコードの種類

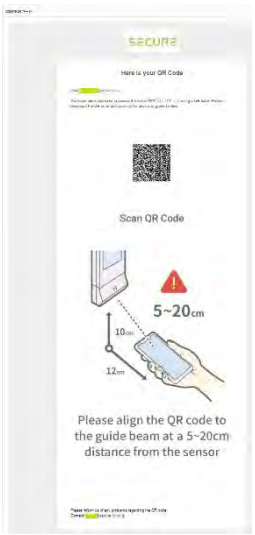
BioStar2 で扱える QR コード および バーコードは、以下の種類があります。

種類		特徴	利用条件
BioStar2 QR		BioStar2 で、QR コードを作成します。	作成される QR コードは、メールで送信されるため、以下の条件が必要となります。 ・BioStar2 サーバーPC が常時インターネットに接続されていること ・メール送信可能なメールサーバ（SMTP）があること ・QR コードを利用するユーザーには、メールアドレスを登録すること
一般 QR/バーコード	一般 QR コード	他のシステムで作成した QR コードを利用します。	暗号化されていない文字と数字のデータである必要があります
	一般バーコード	他のシステムで作成したバーコードを利用します。	暗号化されていない文字と数字のデータである必要があります

13.2 QR コード/バーコードの利用方法

13.2.1 BioStar2 QR コードの場合

BioStar2 側で作成した QR コード ID に対して、BioStar2 が QR コードを作成し、該当ユーザーの登録メールアドレスにメールを送ります。
利用者は、BioStar2 から送られてくるメールを受信してください。
そのメールをスマートフォンで確認することで、QR コード画像が表示されます。
そのまま、メールを表示した状態で、X-Station2 の下部（QR コードリーダー）にかざして認証してください。
（そのメールの QR コード部分を、印刷して、スマートフォン以外で認証することも可能です。）



受信メールイメージ

13.2.2 一般 QR コード/バーコードの場合

他のシステムで作成する QR コードやバーコードを利用する場合は、その基となる文字列、数字列がわかっている必要があります。その値と同じ値を BioStar2 に登録することで、既存の QR コードやバーコードをそのまま利用することが可能です。BioStar2 QR コードと違い、BioStar2 から各ユーザーに対してメールを送信することはありません。

BioStar2 のユーザー情報として登録が完了したら、あとは、既存の QR コード・バーコードを X-Station2 の下部（QR コードリーダー）にかざして認証してください。

但し、基となるコードがわかっている場合でも、既存の QR コードやバーコードが暗号化されていたりする特殊な場合は、利用できませんので、ご注意ください。

13.3 BioStar2 QR コードの登録方法

ユーザーに対して、BioStar2 QR コードを登録するには、ユーザーの画面から行います。

2 章(ユーザー追加) または 4 章(ユーザーの再編集)の操作を行い、該当ユーザーの資格情報の部分の

をクリックしてください。以下の画面が表示されます。

（もし、少し異なる画面が出る場合は、 QR/バーコード の項目で、BioStar2 QR を選択してください。）

・QR/バーコード：利用する QR/バーコード種別を選択します。

・カード ID：QR コードの基となる数字を選択します。

※初期値では、その下の入力種別 の項目が、ランダム ID を使用 に設定されているため、自動入力され入力できません。重複しない数字のため、そのままご利用いただくことが推奨ですが、数字を指定したい場合は、入力種別の項目を、手動入力 に切り替えると入力可能になります。

・入力種別：ランダムカード ID 利用と、手動入力 を切替可能です。

※BioStar2 QR コードを登録する場合、ユーザーのメールアドレスに対して、QR コードのメールを送付します。

このため、本登録方法を実施する前に、メールの送信設定を完了させておく必要があります。

メールの送信設定については、21.19 章 を参照ください。

14 ユーザーデータ の CSV エクスポート/インポートの形式について

BioStar 2 では、ユーザーデータの一部情報を CSV ファイルで、エクスポート/インポートすることが可能です。
アクセスグループ情報と、指紋データ および、顔データは、CSV ファイルからはインポートできません。
CSV ファイル自体は、「UTF-8 BOM 付 CRLF」で作成してください。形式が違う場合、インポートエラーや、
文字化けが発生します。CSV の形式フォーマットは、下表となります。

[ユーザーCSV フォーマット]

列数	内容	条件	標準	入出力
1	ユーザーID user_id	1～4294967295（半角数字） ※BioStar2 の設定で、アルファベットを許可している場合は、半角アルファベットも使用可能（但し、一部認証機は未対応となります。）	○ 必須	
1	ユーザー名称 name	48 文字以内（全/半角問わず）	○	
1	部門 department	64 文字以内（全/半角問わず：但し数字は半角入力のみ） ※BioStar2 では、ユーザー画面以外では利用しません。 モバイルアクセスカード利用時に、スマートフォン側のモバイルアクセスアプリに表示されます。	○	
1	役職 user_title	64 文字以内（全/半角問わず：但し数字は半角入力のみ） ※BioStar2 では、ユーザー画面以外では利用しません。 モバイルアクセスカード利用時に、スマートフォン側のモバイルアクセスアプリに表示されます。	○	
1	電話番号 phone	32 文字まで（半角数字 および -） ※BioStar2 では、ユーザー画面以外では利用しません。	○	
1	E メール email	255 文字まで（半角文字 および 半角記号） ※BioStar2 QR コードの送付や、ビジュアル顔のモバイル登録リンクを送付する場合に利用します。	○	
1	ユーザーグループ user_group	階層数 8 階層まで（最上位層 All Users は含まず） 各階層の文字数は、48 文字まで（全/半角問わず） 各階層の区切り文字は、「/」で記載 例）一番上の「すべてのユーザー」階層：All Users 二段階目の「総務部」階層：All Users/総務部	○ 必須	
1	有効期限（開始） start_datetime	有効期限の開始日時 YYYY-MM-DD HH:MM:SS 形式 初期値は、2001-01-01 00:00:00 となります。必要に応じて変更してください。 有効期限（終了）より、前の日時を設定してください。	○ 必須	
1	有効期限（終了） expiry_datetime	有効期限の終了日時 YYYY-MM-DD HH:MM:SS 形式 初期値は、2030-12-31 23:59:00 となります。必要に応じて変更してください。 有効期限（開始）より、後の日時を設定してください。	○ 必須	
複数可	カスタムフィールド	カスタムフィールド内容（列数分出力） カスタムフィールドご利用時の場合、カスタムフィールド数分の列が出力されます。	×	

1	カード ID csn	カード ID（10 進数 半角数字） カードは、1 ユーザーあたり 8 枚まで登録可能です。 (カード ID/アクセスオンカード/モバイルカード/QR コード/バーコード/Wiegand カードの合算値が 8 枚まで) 複数 ID 登録する場合は、「/」で区切って記入してください。 CSN カード利用時に、出力されます。	×	
1	セキュア資格カード secure_credential	セキュア資格カード ID（10 進数 半角数字） セキュア資格カード利用時は、エクスポートされます。 参考確認のための出力のみです。インポートすることはできません。	×	出力
1	アクセスオンカード access_on_card	アクセスオンカード ID（10 進数 半角数字） アクセスオンカード利用時は、エクスポートされます。 参考確認のための出力のみです。インポートすることはできません。	×	出力
1	モバイルカード 有効期限(開始) mobile_start_datetime	モバイルカード有効期限の開始日時 YYYY-MM-DD HH:MM:SS 形式 ※2001-01-01 00:00:00～2030-12-31 23:59:00 となります。 モバイルカード有効期限（終了）より、前の日時を設定してください。 ダイナミック サイトにより、モバイルカード利用時は、出力されます。	×	
1	モバイルカード 有効期限(終了) mobile_expiry_datetime	モバイルカード有効期限の終了日時 YYYY-MM-DD HH:MM:SS 形式 ※2001-01-01 00:00:00～2030-12-31 23:59:00 となります。 モバイルカード有効期限（開始）より、後の日時を設定してください。 ダイナミック サイトにより、モバイルカード利用時は、出力されます。	×	
1	モバイルカード ID csn_mobile	モバイルカード ID（10 進数 半角数字） カードは、1 ユーザーあたり 8 枚まで登録可能です。 (カード ID/アクセスオンカード/モバイルカード/QR コード/バーコード/Wiegand カードの合算値が 8 枚まで) 複数 ID 登録する場合は、「/」で区切って記入してください。 モバイルカード利用時は、出力されます。	×	
1	BioStar2 QR	BioStar2 QR コード ID（10 進数 半角数字） BioStar2 QR コード利用時は、エクスポートされます。 参考確認のための出力のみです。インポートすることはできません。	×	出力
1	QR/バーコード qr	QR コード/バーコード値（半角英数字） カードは、1 ユーザーあたり 8 枚まで登録可能です。 (カード ID/アクセスオンカード/モバイルカード/QR コード/バーコード/Wiegand カードの合算値が 8 枚まで) 複数 ID 登録する場合は、「/」で区切って記入してください。 QR コード/バーコード（ BioStar2 QR を除く ）利用時は、出力されます。	×	
複数可	Wiegand カード ID –	Wiegand カードフォーマット用 ID（10 進数 半角数字） カードは、1 ユーザーあたり 8 枚まで登録可能です。 (カード ID/アクセスオンカード/モバイルカード/QR コード/バーコード/Wiegand カードの合算値が 8 枚まで) 複数 ID 登録する場合は、「/」で区切って記入してください。 各 Wiegand フォーマットに合わせたカード ID を登録可能です。 Wiegand カード利用時は、出力されます。	×	
1-2	ビジュアル顔画像 face_image_file1 face_image_file2	FaceStation F2 用 顔画像ファイルパス 顔画像と一緒に配置することで、指定の画像ファイルをビジュアル顔として登録できます。 登録する顔の数に合わせ、列数を変更可能です。 各列には、 xxxxx.jpg のように、拡張子を含めたファイル名を記載します。 そのファイルは、インポートする CSV ファイルと同じフォルダに配置しておく必要があります。	×	入力
1	PIN コード pin	ユーザーPIN コード	×	入力

なお、インポート時は、列のカラムを指定してインポート可能なため、列の順番は自由で構いません。
また、ご利用の環境に必要な項目(列)だけの CSV を作成することで対応可能です(必須　列参照)。

[ポイント1]
ファイルの先頭行となる　カラム行は、作成されても、省略でも構いません。これにより、インポートの際の開始行の指定を変更してください。(カラム行がある場合は、2 行目から。ない場合は、1 行目から)
また、カラムは、インポート時の目安として使用するだけとなりますので、カラム名自体の変更や、列順の変更をされても構いません。

[ポイント 2]
ユーザーID は、1～ となりますが、BioStar2 では、初期値で 1 は、管理者ユーザーとなります。
通常は、ユーザーID 2～ ご利用ください。

[ポイント 3]
CSV ファイルで扱えるユーザーデータは、上記の内容となります。
認証用指紋データ、および　認証用顔データは、CSV では扱えません。

[ポイント 4]
既存データがある状態で、CSV でユーザーデータをインポートする場合、必ず、CSN は、指定し直すようにしてください。
ユーザーのユーザーグループを変更する場合であっても、CSN を指定しない csv ファイルでのインポートを行うと、
既存では設定してあった CSN データが指定されなくなったため、全ユーザーが、「カードなし」と判断され、カードデータが解除されてしまします。CSN については、毎回、既存ユーザーの分も必ず指定するようにしてください。
(CSN だけではなく、他の項目も同様です。CSV で追加インポートする際は、既存ユーザー分も再度指定してください。)

[ポイント 5]
指紋データ および 顔データについては、ユーザー情報を上書きでインポートしても削除されることはありません。

[ポイント 6]
モバイル CSN は、ポータルサイトの設定が レギュラー の場合、1 枚ごとにクレジットに紐づきます。
モバイルアクセス ポータルサイトと連携の設定をした状態でのインポートの際は、よく注意してインポートしてください。
間違ってしまった場合は、その間違った番号で発行されてしまい、ライセンス(クレジット数)が減ってしまいます。
返金や、クレジット数の補填は致しかねます。

14.1 ユーザーデータの CSV エクスポート(CSV ファイルで保存)

ユーザーデータを、CSV ファイルで保存する方法を以下に示します。
CSV ファイルでの出力では、指紋データや、顔データ、アクセス権限情報は出力できません。

CSV ファイルの出力は、ユーザーの画面から行います。
ユーザー一覧の中から、CSV 出力の対象とするユーザーに、チェックをつけてください。

本ソフトウェアでは、項目を選択する際に、個別に選択していく場合は、200 項目までしか選択できません。
表示範囲のリストのすべてにチェックをつける場合は、
右図で示す場所のカラム行のチェックボックスにチェックをしてください。
表示されている範囲の項目すべてにチェックが入ります。

しかし、それでも、最大で、200 件までチェックが入る状態であり、
個別の選択の最大数となります。
201 件目の個別のチェックはできません。
このため、201 件以上の場合は、個別チェックではなく、
全項目の一斉のチェックが必要となります。
この場合は、右図の示す位置の三角マークをクリックしてください。
メニューが表示されますので、「すべて選択」を選んでください。
この場合は、全項目がチェックされた状態となります。

CSV エクスポートの対象とするユーザーの選択が完了したら、画面右上の [...] をクリックし、CSV エクスポートをクリックします。

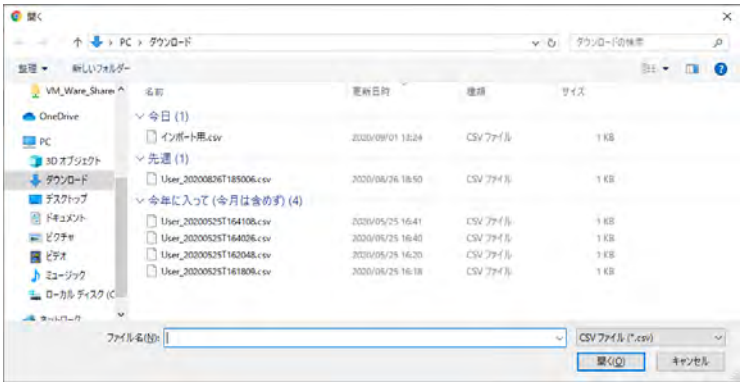
これにより、Google Chrome で設定されているダウンロード場所に、CSV ファイルが保存されます。

14.2 ユーザーデータの CSV インポート(CSV ファイルからのユーザー登録)

ユーザー情報を、CSV 形式でインポートする(登録する)方法について記載します。
(インポートするための CSV ファイルのフォーマットは、11 章を参考にしてください。)
CSV ファイルのインポートは、ユーザーの画面から行います。

画面右上の [...] をクリックし、CSV インポートをクリックします。

右図のような画面が表示されます。
インポートするために準備した、
CSV ファイルを選択してください。



ファイルを選択すると、右図のような画面になります。
もし、CSV ファイルの先頭行がカラム行の場合は、2 行目からを
開始行としてください。
先頭行からデータがある場合は、1 行目からにしてください。
そして、 次へ をクリックしてください。

ファイルの先頭行を読み、右図のように、どの項目と、
どの列を連携させるかを決める画面が表示されます。
各項目が、CSV ファイルのどの列のデータを読み込むかを
決めます。
(初期値は、列順のため、順番通りの場合は、一致します。)
必要に応じ、変更してください。
また、いろいろと変更した場合でも、右上の 再定義 を
クリックすることで、CSV ファイルを読み込んだ時の初期値に
戻ります。
そして、連携内容を確認し、問題ない場合は、この画面の

右側のバー（右図 赤点線枠）を一番下まで下げます。
右側のバーを下げると、続きがあります。
念のため、内容を最後まで確認し、上書きの設定を行います。

CSV ファイルのデータのうち、既に BioStar2 の中に存在する
ユーザーの ID が重複している行がある場合、
・CSV ファイルのデータを使わない
・CSV ファイルのデータで PC データを上書きする
のどちらかを選択します。

選択後、 次へ をクリックしてください。

正しく、インポートできると、「アップロード成功」と表示されます。
もし、エラー画面が表示される場合は、内容を確認し、
CSV ファイルのフォーマットを確認してください。

15 ユーザーデータ のデータファイル エクスポート/インポートについて

BioStar 2 では、ユーザーデータを専用の形式で、エクスポート/インポートが可能です。

CSV のエクスポート/インポートと異なり、データファイルは外部ストレージ（USB）に保存し、指紋データや顔データもエクスポート/インポートが可能です。最大 50 万人のユーザーを移動できます。

注意：古いファームウェアバージョンを使用しているデバイス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。必ず最新バージョンのファームウェアを使用してください。

ただし、用途はバックアップ及び復元用あるいは、オフライン端末へのユーザー転送用であり、データの変更はできません。

15.1 ユーザーデータの データファイルエクスポート（データファイル（tgz 形式）での保存）

本章では、ユーザーデータを専用形式で保存する方法について記載します。

データファイルの出力は、ユーザーの画面から行います。

ユーザー一覧の中から、データ出力の対象とするユーザーに、チェックをつけてください。

本ソフトウェアでは、項目を選択する際に、個別に選択していく場合は、200 項目までしか選択できません。

表示範囲のリストのすべてにチェックをつける場合は、

右図で示す場所のカラム行のチェックボックスにチェックをしてください。

表示されている範囲の項目すべてにチェックが入ります。

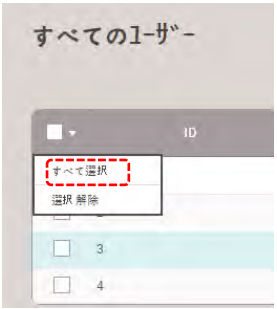
しかし、それでも、最大で、200 件までチェックが入る状態であり、個別の選択の最大数となります。201 件目の個別のチェックはできません。このため、201 件以上の場合は、

個別チェックではなく、全項目の一斉のチェックが必要となります。

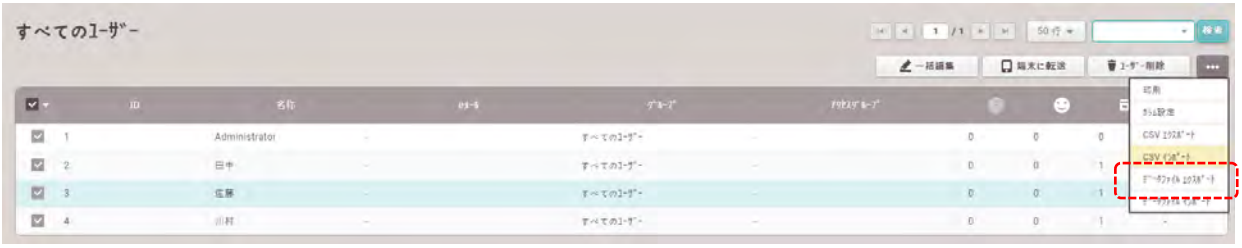
この場合は、右図の示す位置の三角マークをクリックしてください。

メニューが表示されますので、「すべて選択」を選んでください。

この場合は、全項目がチェックされた状態となります。



データファイル出力の対象とするユーザーの選択が完了したら、画面右上の ••• をクリックし、データファイルエクスポートをクリックします。



以下の画面が表示されます。

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てください。

選択後、 適用 をクリックしてください。

ファイルのダウンロードが始まります。

これにより、Google Chrome で設定されていた場所に、tgz 形式のデータファイルが保存されます。

注意:

・端末からのみ直接登録されたビジュアル顔データをエクスポートできます。他の方法(画像ファイルのアップロード、CSV インポート、モバイル端末など) で登録したデータはエクスポートできません。

・端末が正しく選択されていることを確認してください。間違った端末のデータファイルは認識できません。

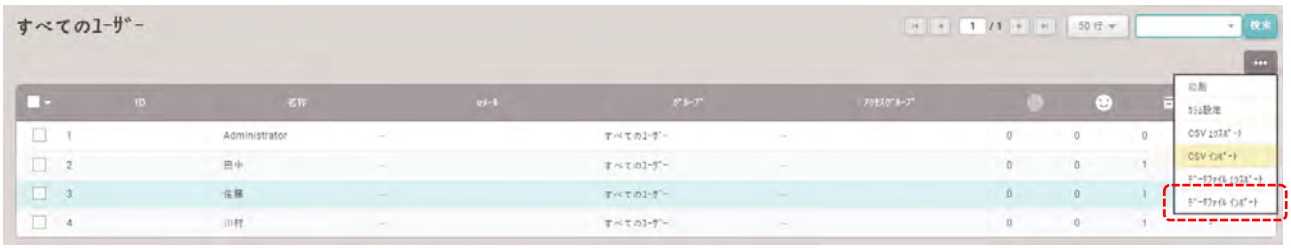
15.2 ユーザーデータのデータファイルインポート(ﾃﾞｰﾀﾌｧｲﾙ(tgz 形式)からのﾕｰｻﾞｰ登録)

本章では、専用形式(tgz 形式)のユーザーデータをインポートする方法について記載します。

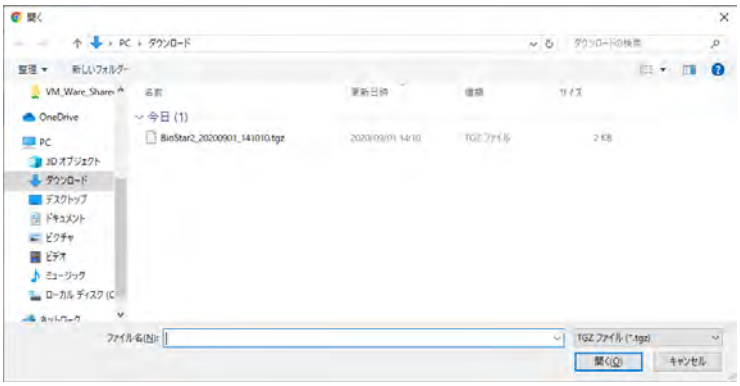
※注意点として、データファイルをインポートした場合、対象のユーザー情報は上書きされます。
予期せぬユーザーが上書きされてしまわないよう、気をつけてご利用ください。

データファイルのインポートは、ユーザーの画面から行います。

画面右上の [...] 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。



右図のような画面が表示されます。
インポートするために準備した、
tgz ファイルを選択してください。



正しく、インポートできると、「アップロード成功」と表示されます。
次に端末にデータを転送します。
データファイル出力の対象とするユーザーの選択が完了したら、画面右上の [端末に転送] をクリックします。

右の図のような、転送先の端末を選択する画面が出ます。
転送先に☑を入れて、下部の「ユーザー情報に違いが
あった場合、上書きします」にも☑をつけ、「転送」ボタンを
クリックしてください。

※これらのデータファイルは、BioStar2 ソフトウェアにもインポートすることができますが、認証機にも直接インポートすることが可能です。
FAT32 形式でフォーマットをした USB メモリに、tgz 形式のファイルをコピーし、認証機の USB コネクタに挿してください。そして、認証機のメニュー画面で、 設定 ＞ 端末 ＞ USB メモリ ＞ インポート と進み、データをインポートすることで、そのユーザーデータで認証することが可能となります。

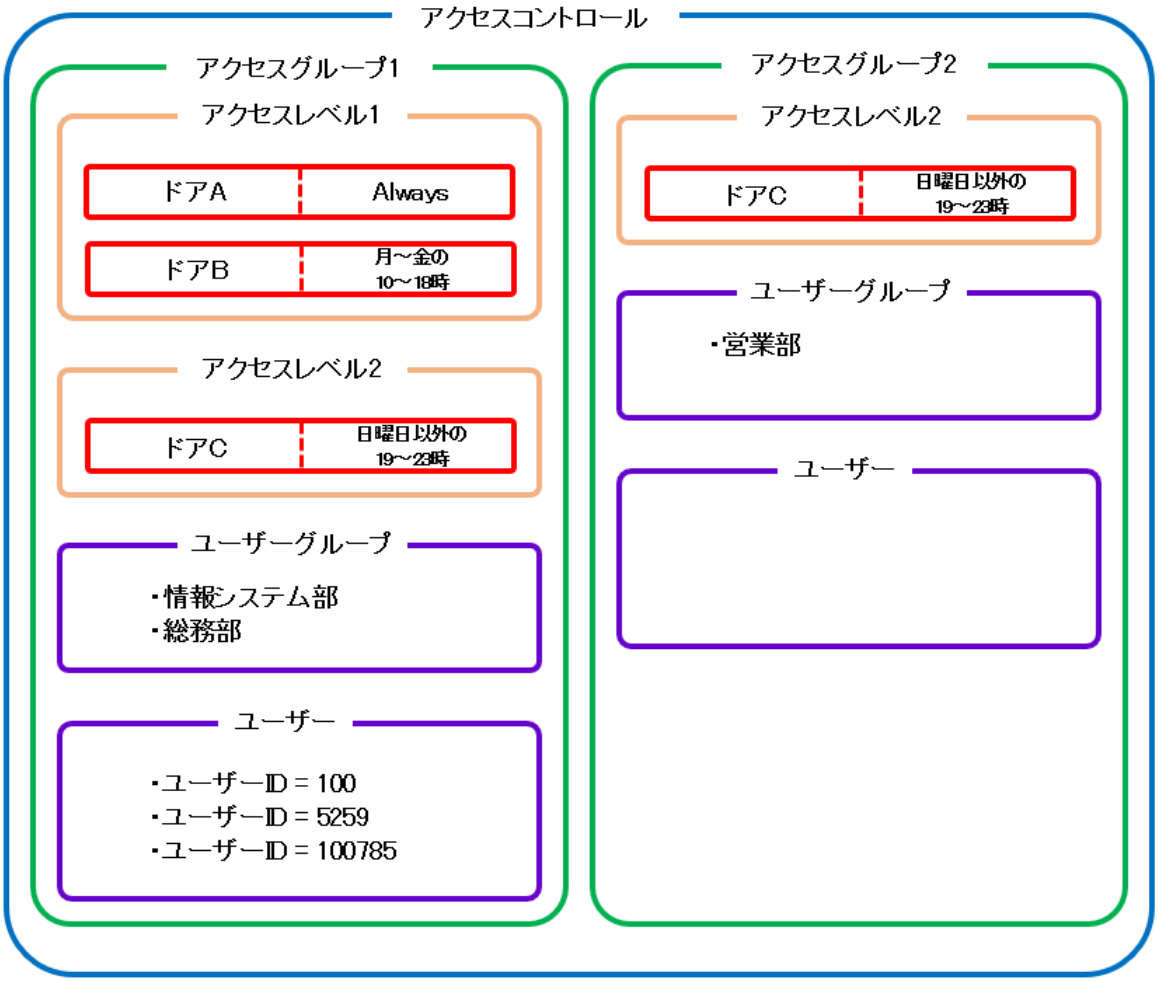
16 アクセスコントロールの指定・変更

アクセスコントロールとは、「どのユーザーが、どのドアを、いつ通行できるか？」を設定するアクセスの権限を意味します。
BioStar2 システムでは、

「どのドアを？いつ？」を決定する部分を、“アクセスレベル”と呼び、
「どのアクセスレベルに 誰が？」の内容の部分を、”アクセスグループ”と呼びます。
アクセスグループの 「誰が？」の部分は、個別のユーザーID でも設定できますし、ユーザーグループ（部署）でも設定可能です。

アクセスコントロールを設定するためには、あらかじめ「ドア」と「誰」、「いつ」 の作成が必要です。

アクセスコントロールの概念を以下に示します。



上記の設定例の場合、

・情報システム部 に属する人、総務部に属する人、ユーザーID 100/5259/100785 の 3 名は、
ドア A に対し、毎日 24 時間/ドア B に対し、月～金曜の 10～18 時/ドア C に対し、日曜以外の 19～23 時にアクセスが可能です。

・そして、営業部 に属する人は、ドア C に対し、日曜以外の 19～23 時にアクセスが可能です。

このような形で、アクセスコントロールの機能で、アクセスレベルとアクセスグループを設定しながら、
誰が？どのドアを？いつ認証できる？を設定していきます。

16.1 アクセスレベルの作成（どのドアに？いつ？の設定）

本章では、前ページの例に沿って、作成の流れを説明します。

前ページの例では、アクセスレベルが 2 つ 存在します。「アクセスレベル 1」と「アクセスレベル 2」です。

そのアクセスレベルの中で設定している部品は、

・ドア A/ドア B/ドア C の 3 つのドア

・Always/月～金の 10～18 時/日曜日以外の 19～23 時 の 3 つのスケジュール

となります。

3 つのドアについては、ドアの設定（24.1 章）を参照してください。

3 つスケジュールについては、スケジュールの項目の設定（21.7 章）を参照してください。

まず、左側のメニューで、「アクセスコントロール」をクリックします。すると、以下のような画面が表示されます。

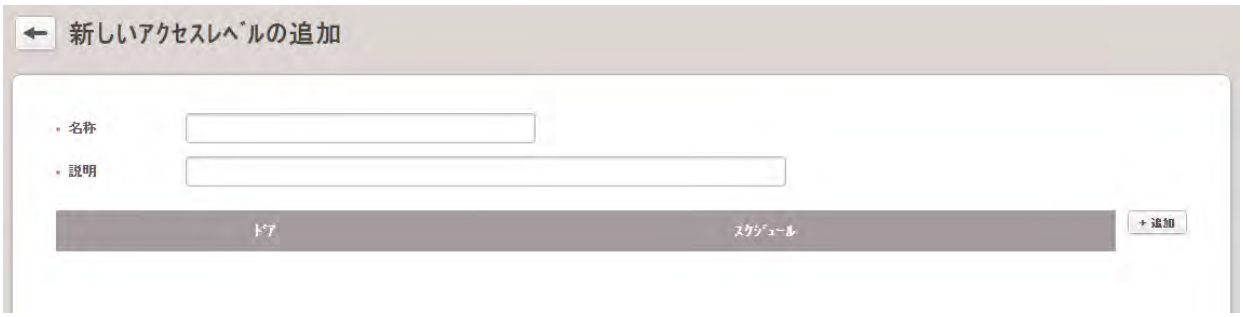
エレベーター制御可能なライセンスが適用されている場合は、上記のように「フロアレベル」に関する項目も表示されます。

ライセンスが、エレベーター制御可能な状態でない場合は、「アクセスグループ」と「アクセスレベル」に関する項目だけが表示されます。

アクセスレベルを作成するため、 

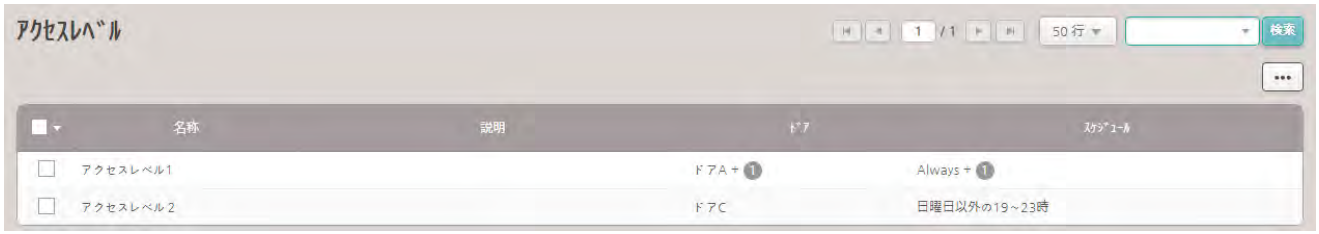
をクリックします。

以下の画面が表示されますので、名前を決めて、「＋追加」ボタンを使いつつ、設定します。



同様に、もう1つのアクセスレベル2も作成します。

作成が完了すると、以下のような一覧画面になります。



各アクセスレベルで、項目の部分は、1 つ分しか表示できないため、複数ある場合は、 

のように、
「代表名＋①」などのように、数字で表示されます。（1つしかない場合は、その1つの名称が表示されます。）

※スケジュール部分については、21.7 章を参照し事前に作成しておいていただく内容で記載しておりますが、
アクセスレベル作成時に、同時にスケジュールも作成することも可能です。
その場合は、スケジュールを選択する欄の一番下に表示される、「＋スケジュールの追加」をクリックしてください。

16.2 アクセスグループの作成（どのアクセスグループに？誰が？の設定）

本章では、前ページまでの例に沿って、作成の流れを説明します。

前ページまでの例では、アクセスグループが 2 つ 存在します。「アクセスグループ 1」と「アクセスグループ 2」です。

そのアクセスグループの中で設定している部品は、

・アクセスレベル1とアクセスレベル2 の 2 つのアクセスレベル

・情報システム部/総務部/営業部 の 3 つのユーザーグループ

・100/5259/100785 の 3 人のユーザーID のユーザー

となります。

3 つのユーザーグループについては、ユーザーグループの作成（24.1 章）を参照してください。

まず、左側のメニューで、「アクセスコントロール」をクリックします。すると、以下のような画面が表示されます。

エレベーター制御可能なライセンスが適用されている場合は、上記のように「フロアレベル」に関する項目も表示されます。ライセンスが、エレベーター制御可能な状態でない場合は、「アクセスグループ」と「アクセスレベル」に関する項目だけが表示されます。

アクセスグループを作成するため、  をクリックします。

以下の画面が表示されます。

ここでも、適用されているライセンスにより、画面が少し異なります。エレベーターが制御可能なライセンスが適用されている場合、以下の画面のように、フロアレベル を含めた 4 列が表示されますが、エレベーターの制御を可能とするライセンスが適用されていない場合は、フロアレベル の項目を除いた 3 列が表示されます。

まず、アクセスグループ 1 に関する部分を設定します。「＋追加」をクリックしながら以下のように設定します。

設定が完了したら、画面右下の「適用」ボタンをクリックします。

同様に、もう1つのアクセスグループ2も作成します。

作成が完了すると、以下のような一覧画面になります。

各アクセスグループで、項目の部分は、1 つ分しか表示できないため、複数ある場合は、
「代表名＋②」などのように、数字で表示されます。（1つしかない場合は、その1つの名称が表示されます。）

※アクセスレベル部分については、16.1 章を参照し事前に作成しておいていただく内容で記載しておりますが、
アクセスグループ作成時に、同時にアクセスレベルも作成することも可能です。
その場合は、アクセスレベルを選択する欄の一番下に表示される、「＋アクセスレベル追加」をクリックしてください。

16.3 アクセスコントロールを利用しない設定方法

前の章までは、アクセスコントロールの説明を記載しましたが、BioStar2 システムでアクセスコントロールを使わずに利用する方法があります。

この方法の場合、端末にユーザーデータが転送されているユーザーは全員認証資格を持つこととなります。

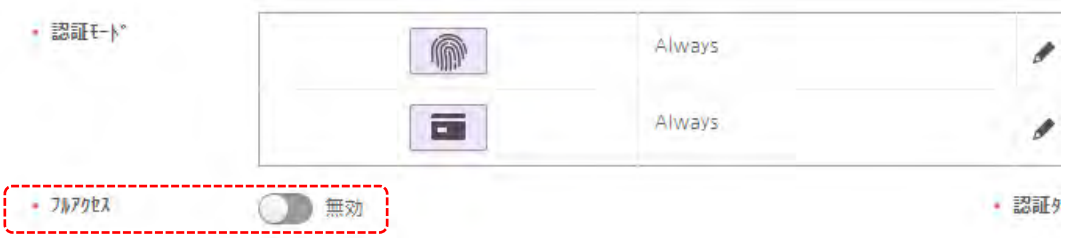
端末にデータを送ることで認証資格となり、端末からデータを削除することで認証できなくなります。

アクセスコントロールを利用する方が、鍵を開けることができる人や、日時を細かく設定できるため、本方法の利用は推奨しておりませんが、「全員が通れてよい。」などの単純な利用法の場合は、設定は簡単となります。

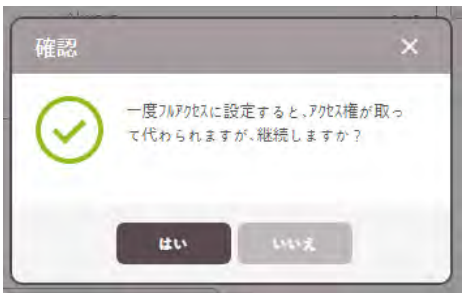
以下に手順を説明します。

まず、アクセスグループ/アクセスレベルを確認し、該当の端末が設置されたドアが、アクセスグループに割り当たっていないことを確認してください。
もし、割り当たっている場合は、削除してください。
（この時点では、ユーザー情報が端末内にあっても、全員認証エラーとなります。）

次に、「端末」メニューから、該当の端末のクリックし、端末の設定に入ります。
機種により、表示位置は、少し異なりますが、認証モードの表示の少し下に「フルアクセス」という設定があります。



この項目を「有効」にすることで、端末内に資格データがあるユーザーは、認証できるようになります。
有効に変更しようとすると、左図のメッセージが表示されます。「はい」をクリックして切り替えてください。



もし、アクセスグループからの設定が削除できていない場合は、右図の画面が表示されます。
また、逆に、端末をフルアクセスに設定した状態にしていて、アクセスコントロールを利用すると以下の画面が出ます。

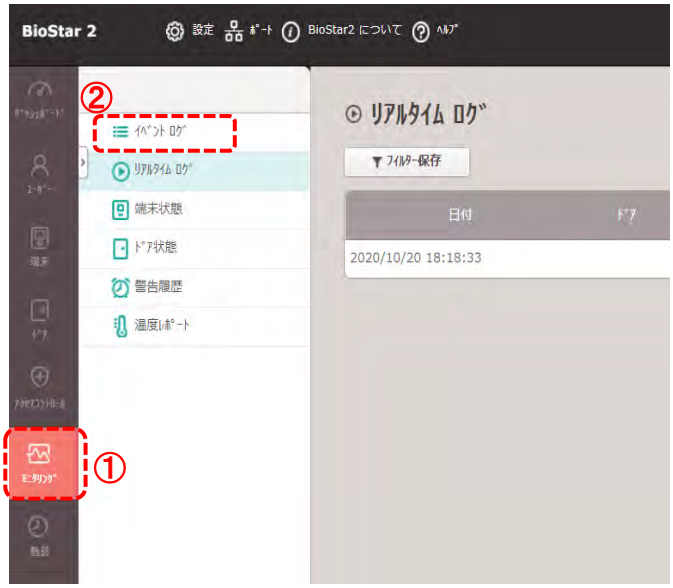
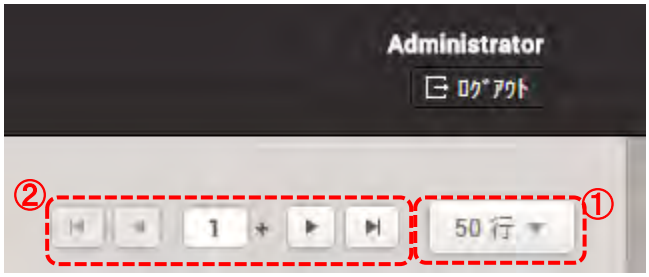
この場合は、先に、端末の設定で、「フルアクセス」を無効にしてから再設定してください。

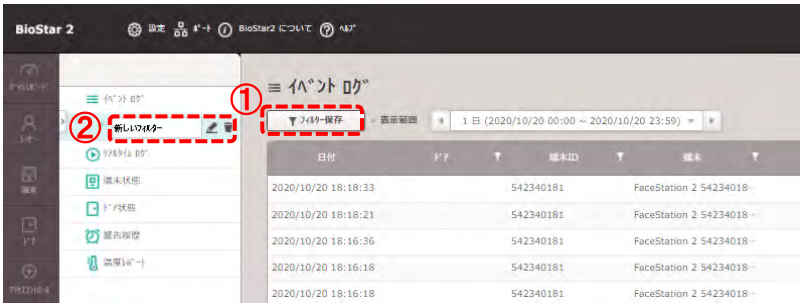
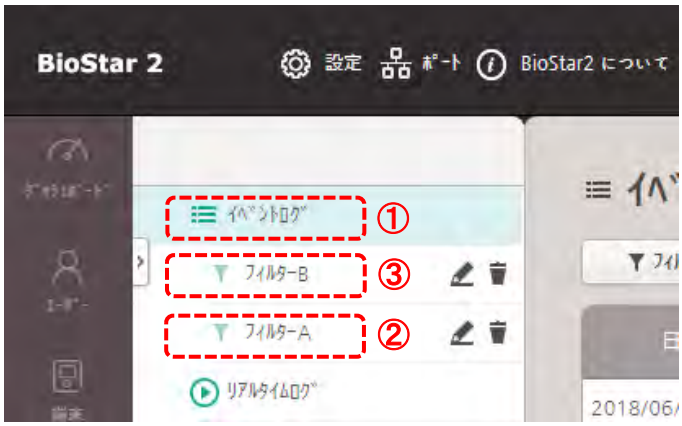
17 ログ（動作状況）の確認

ログの確認画面では、各動作内容が確認でき、一部状態の制御が可能です。

17.1 イベントログの確認

イベントログの確認では、過去のイベントログを確認することが可能です。
また、カラム毎にフィルタリングの設定が可能です。

説明図	操作内容
	① イベントログを確認するために、「モニタリング」をクリックしてください。 ② 「イベントログ」をクリックしてください。 ※右側画面が、イベントログの画面になります。この時点で、表示した時点から過去の分が表示されています。
	① 一度に表示する件数を変更する場合は、クリックして、変更してください。 ※25/50/100/200 から選択可能です。 ② 先頭/最終ページの切替や、1 ページずつの切替、ページ指定が可能です。
	カラムのフィルタアイコンを利用し、各列のフィルタリングが可能です。 ① 各項目のフィルタアイコンをクリックすると、内容のフィルタリングが可能です。
	左図のように、各列について、フィルタリングされた情報が表示されます。 ① 各項目のフィルタリングを削除する場合は、フィルタリング項目の横の「X」をクリックしてください。

説明図	操作内容
	① 作成したフィルタリングパターンを保存しておく場合は、「フィルター保存」をクリックしてください。 ② 「新しいフィルター」という名前で、設定が保存されます。 自由な名称に変更してください。
	複数のフィルターを保存した場合、左図のようになります。 ① 「イベントログ」の部分をクリックすると、フィルターなしの情報を表示します。 ② 「フィルター A」の部分をクリックすると、フィルター A の設定が適用された状態で表示します。 ③ 「フィルター B」の部分をクリックすると、フィルター B の設定が適用された状態で表示します。
	フィルターについて、 ① 「ペン」マークをクリックすると、フィルターの名称が再変更できます。 ② 「ゴミ箱」マークをクリックすると、フィルターを削除することが可能です。

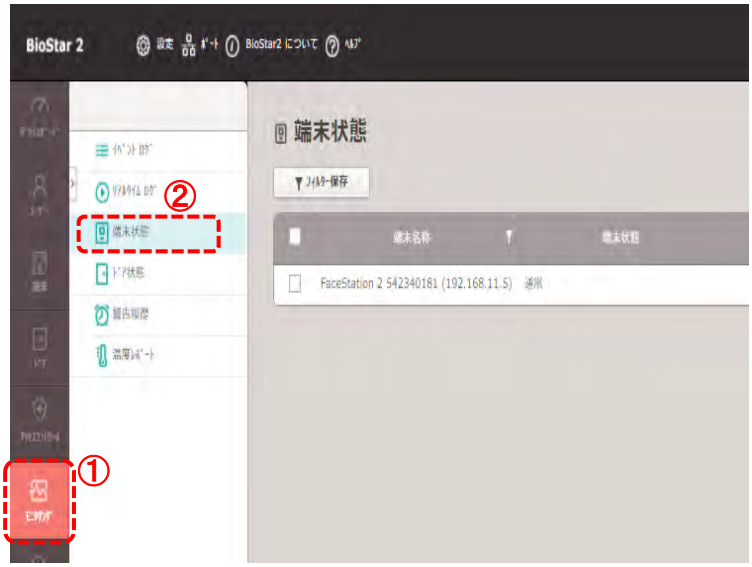
17.2 リアルタイムログの確認

リアルタイムログは、本画面を表示している時に、端末でのイベントがあると、ログを自動的に表示します。
現在の動作全般を確認する場合に、本画面をご利用ください。

説明図	操作内容
	① リアルタイムログを確認するために、「モニタリング」をクリックしてください。 ② 「リアルタイムログ」をクリックしてください。 ※右側画面が、リアルタイムログの画面になります。表示した時点ではデータがありませんが、ログが発生すると、表示されます。
	① リアルタイムログ画面は、イベントがある毎に、どんどん、ログが流れてしまうため、固定したいときは、「一時停止」をクリックしてください。 ※再度、同じボタンをクリックすると「再開」します。 ② 画面上の表示に区切りを付け、一度、見た目を削除したい場合は、「クリア」ボタンをクリックしてください。画面上のログがクリアされます。 ※再度、ログを見る場合は、イベントログから参照してください。
	フィルターについては、イベントログと同様です。

17.3 端末状態の確認

端末状態は、端末の現在及び、最後のイベント状態を表示します。
一覧で端末の状態を確認したい場合に、本画面をご利用ください。

説明図	操作内容
	① 端末状態を確認するために、「モニタリング」をクリックしてください。 ② 「端末状態」をクリックしてください。 ※右側画面が、端末状態の画面になります。
	① 警報が発生している場合も確認可能です。 ② 警報が発生している端末にチェックをしてください。 ③ 「アラームを解除」をクリックすることでアラームを解除できます。
	フィルターについては、イベントログと同様です。

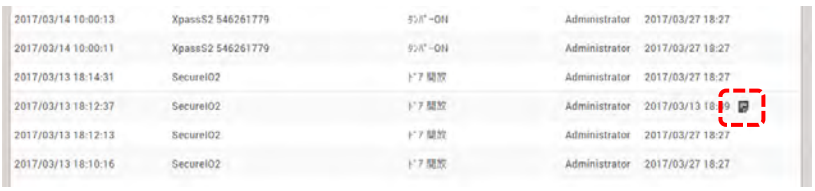
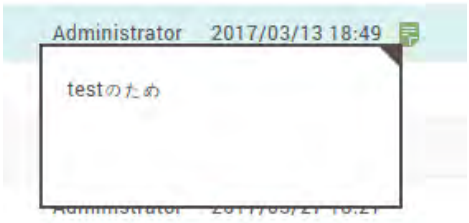
17.4 ドア状態の確認

ドア状態は、ドアの現在及び、ドアリレー状態、アラーム状態、最後のイベント状態を表示します。
また、ドアに対する制御が可能です。
一覧でドアの状態を確認したい場合に、本画面をご利用ください

説明図	操作内容
	① ドア状態を確認するために、「モニタリング」をクリックしてください。 ② 「ドア状態」をクリックしてください。 ※右側画面が、端末状態の画面に なります。
	① 警報が発生している場合も確認可能です。 ② 警報が発生している場合は、該当のドアに☑をしてください。 ③ 「警報を解除」ボタンで解除できます。
	また、同画面で、ドアの制御が可能です。 ① 再操作するまで、ドアを施錠したままとする場合は、「連続施錠」をクリックしてください。 ② 再操作するまで、ドアを解錠したままとする場合は、「連続解錠」をクリックしてください。 ③ ドアを通常の状態に戻す場合は、「連続状態」をクリックしてください。 ④ ドアを 1 回だけ解錠する場合は、「1 回解錠」をクリックしてください。 ⑤ 火災報知アラームや、認証なしドアオープン、ドア開放などのアラームを解除する場合は、「警報を解除」をクリックしてください。 ⑥ APB のアラームが発生している場合は、「APB リセット」をクリックしてください。
	フィルターについては、イベントログと同様です。

17.5 警報履歴の確認

アラート（警告）履歴は、BioStar システムでアラートが発生した場合の履歴を一覧で確認できます。
また、アラートが発生した際にコメントを付けて記憶させたアラートについては、そのコメントを一緒に確認することが可能です。

説明図	操作内容
	① ドア状態を確認するために、「モニタリング」をクリックしてください。 ② 「警報履歴」をクリックしてください。 ※右側画面が、警報履歴の画面になります。
	① 警報には、コメントをつけることが可能です。コメントの付いているデータは、左図の用に、コメントがあることを表すアイコンが表示されます。 このコメントアイコンをクリックすると、内容が表示されます。
	左図の画面のように、コメントの画面が表示され、その際に残したコメントが表示されます。
	フィルターについては、イベントログと同様です。

17.6 温度レポート

ユーザーの温度情報を含めたイベントが一覧で確認できます。

説明図	操作内容
	① 温度状態を確認するために、「モニタリング」をクリックしてください。 ② 「温度「レポート」をクリックしてください。 ※右側画面が、温度情報を含む履歴の画面になります。
	① 希望の期間を設定し、履歴を表示できます。 をクリックする②の画面が表示され、1日、3日、1 週、1月、3月、6月、カスタムから選択できます。 ③ 温度の単位を変更できます。 ④ 前後のページに移動します。 ⑤ 1 頁に表示するリスト行数を設定します。 ⑥ クリックすると、印刷、CSV ファイルへのエクスポート、カラムの変更ができます。

端末の装置の表示温度は、小数点1桁までですが、BioStar2 の表示は小数点 2 桁までとなります。

端末装置の表示は小数点 2 桁目を四捨五入しています。

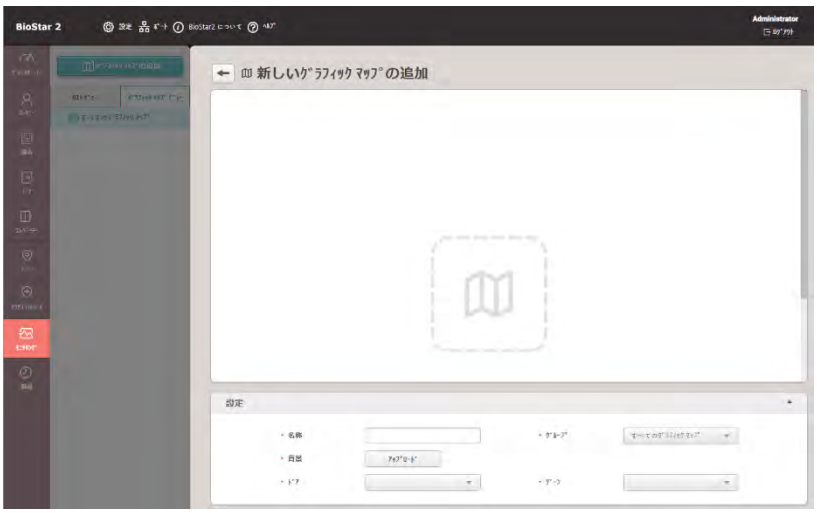
17.7 グラフィックマップビュー

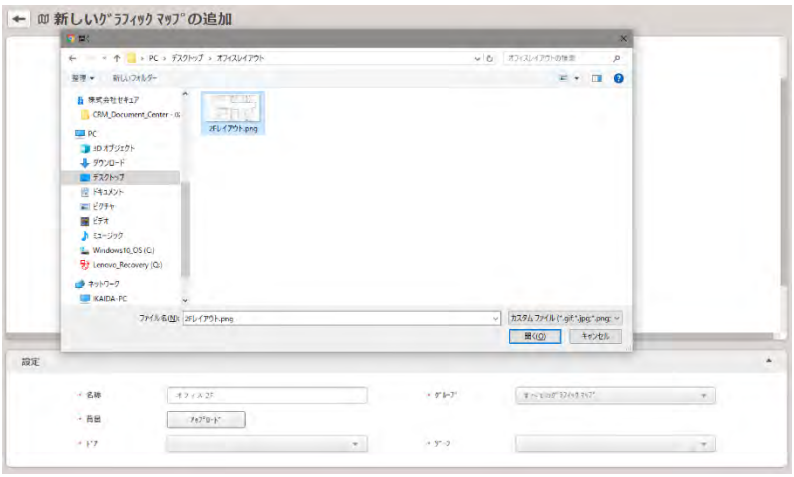
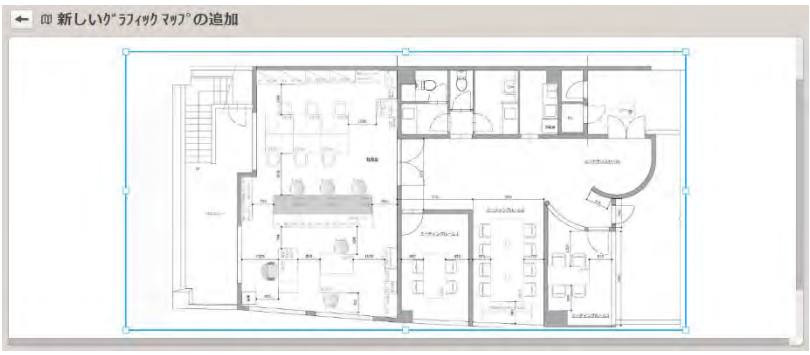
本項目は、追加でアクセスコントロールのライセンスを登録した場合に利用可能となります。

グラフィックマップビューとは、ご利用の環境に応じて、ご利用の建物の地図画像等から、画面上にドアを載せ、地図上でわかりやすくドアの状態を確認する画面です。

グラフィックマップビューの作成・変更・確認は、以下の方法で行います。

17.7.1 グラフィックマップビューの作成

説明図	操作内容
	① グラフィックマップビューを表示・編集するために、「モニタリング」をクリックしてください。 ② 「グラフィックマップビュー」をクリックしてください。 ※ライセンスが登録されている場合に、表示されます。
	① はじめての場合は、グラフィックマップビューは、未作成のため、「 グラフィックマップの追加 」をクリックしてください。
	左図の画面のように、グラフィックマップの編集をする画面になります。

説明図	操作内容
	① 名称を設定します。 ② 「グラフィックマップビュー」をグループ管理する場合は、グループを選択してください。 ③ グラフィックマップビューの背景となる画像を指定します。アップロードボタンをクリックしてください。
	アップロードボタンを押すと、背景となるレイアウトの画像を選択する画面になります。 画像ファイルを選択してください。 ※gif/jpg/jpeg/png/bmp ファイルが選択可能です。
	選択した画像が読み込まれます。 水色の枠の各端、および、中央部をドラッグアンドドロップし、好みの位置・拡大率に調整します。
	① ドアの項目で、グラフィックマップビューに表示するドアに☑を付けます。 ② ゾーンの項目でも、グラフィックマップビューに表示する項目に☑を付けます。 アンチパスバックと火災報知ゾーンが選択可能ですが、火災報知ゾーンは表示上確認できません。
	ドア及びゾーンを選ぶと、マップ上に表示されますので、ドラッグアンドドロップで、お好みの位置になるように調整します。 そして、配置が完了したら画面下部の「適用」をクリックします。

17.7.2 グラフィックマップビューの編集・削除

説明図	操作内容
	① グラフィックマップビューを編集するために、「モニタリング」をクリックしてください。 ② 「グラフィックマップビュー」をクリックしてください。 ※ライセンスが登録されている場合に、表示されます。
	① 作成済みのグラフィックマップビューを再編集する場合は、ペンのアイコンをクリックしてください。 ② 作成済みのグラフィックマップビューを削除する場合は、ゴミ箱のアイコンをクリックしてください。
	編集の方法は、作成時と同様です。 17.7.1 章を参照してください。

17.7.3 グラフィックマップビューの確認

説明図	操作内容
	① グラフィックマップビューを確認するために、「モニタリング」をクリックしてください。 ② 「グラフィックマップビュー」をクリックしてください。 ※ライセンスが登録されている場合に、表示されます。
	① 複数のグラフィックマップビューがある場合は、表示したいグラフィックマップビューをクリックしてください。
	イベントが発生すると、左図のように画面で確認が可能です。

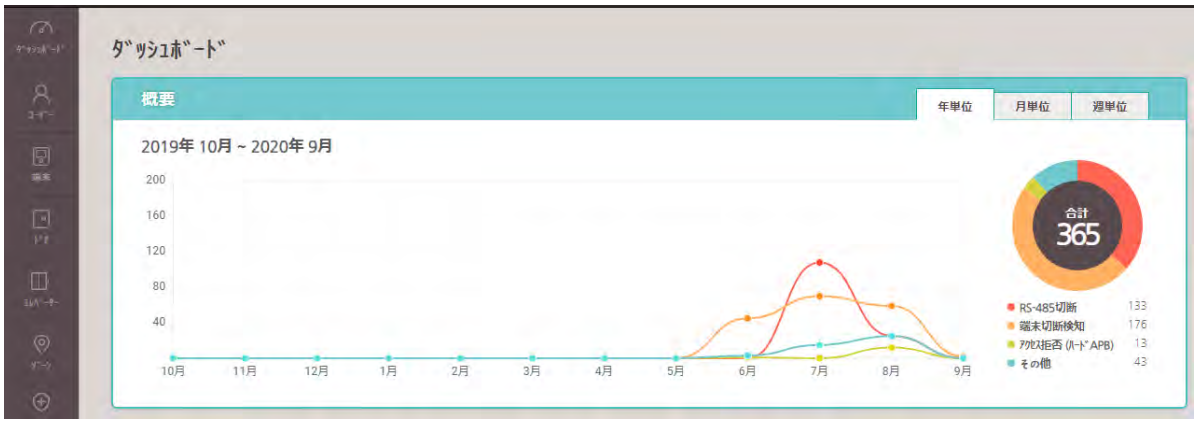
18 警告に対するコメント記載

警告とは、BioStar2 システムで予定外のイベントが発生した際に、画面にポップアップさせたり、音を鳴らしたりなど、特定の動作に対して、注意喚起させる機能です。
どのイベントで警告を発生させるかは、事前に設定されています。設定の方法については、21.8 章を参照してください。

BioStar2 に web ブラウザからログインしていて、
セッションタイムアウト時間内の場合に、警告を設定しているイベントが発生すると、右図のような画面がポップアップします。

これは、通常の「認証成功」や「認証失敗」ではなく、
警告として注意喚起する内容のイベントの場合に発生します。

また、これらのイベントが、ダッシュボード画面にも表示されます。



基本的には、警告としてあがるイベントのため、すぐに気が付けるように、未確認の警告として記録されています。
ポップアップされた画面で、「確認」を押した場合は、確認済みの警告として扱われます。

未確認の警告がある場合は、画面右下のマークも、右図上段のように
「N」マークが表示されます。

未確認の警告がない場合は、右図下段のように、「N」マークがない状態で
表示されます。

運用としては、警告があがったら、確認をして確認済み とすることで、次の警告に気が付きやすい状態を継続する。という運用方法を推奨します。

18.1 ポップアップした警告に対する操作

BioStar2 の画面を表示している間に発生した警告は、画面上にポップアップします。

この画面で、「無視」をクリックした場合は、警告内容が、
「未確認の警告」という扱いになり、ポップアップ画面が閉じます。

コメント欄を入力する場合は、入力し、「確認」をクリックすることで、
「確認済みの警告」という扱いになります。

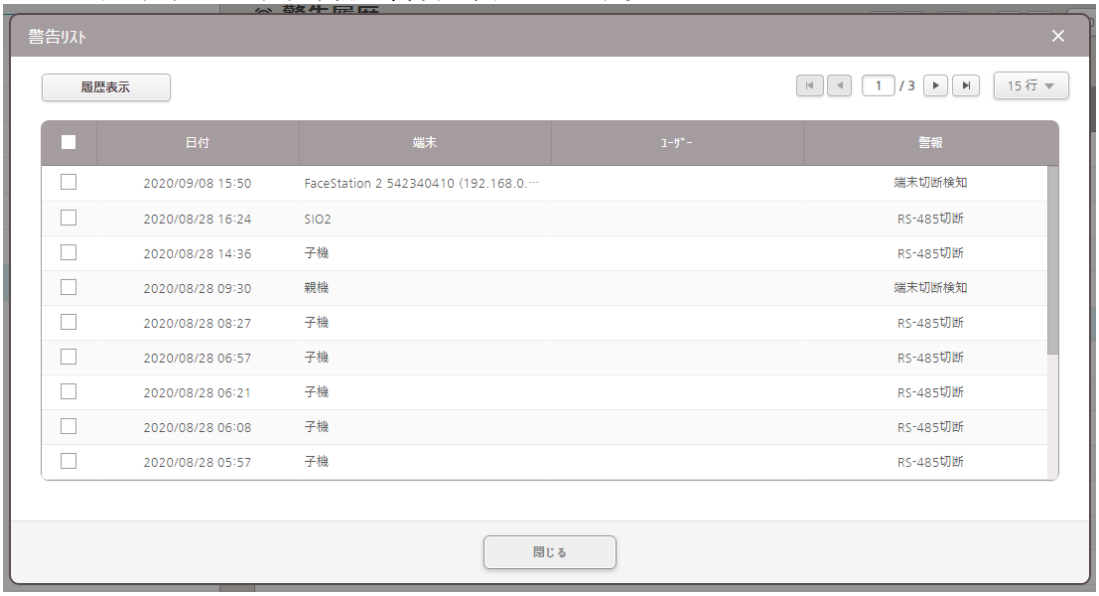
例えば、コメント欄に、
「メンテナンスのため、電源の再起動実施」 などと記載していただくと、後で見たときに区別しやすくなります。

コメント未記入で、「確認済み警告」とすることも可能ですし、その場は画面を閉じるために、「無視」をクリックしていただくことも可能です。

18.2 未確認の警告を確認・再編集する方法

一度、警告がポップアップした際に、「無視」をクリックした未確認の警告を確認する場合は、画面右下の  をクリックしてください。

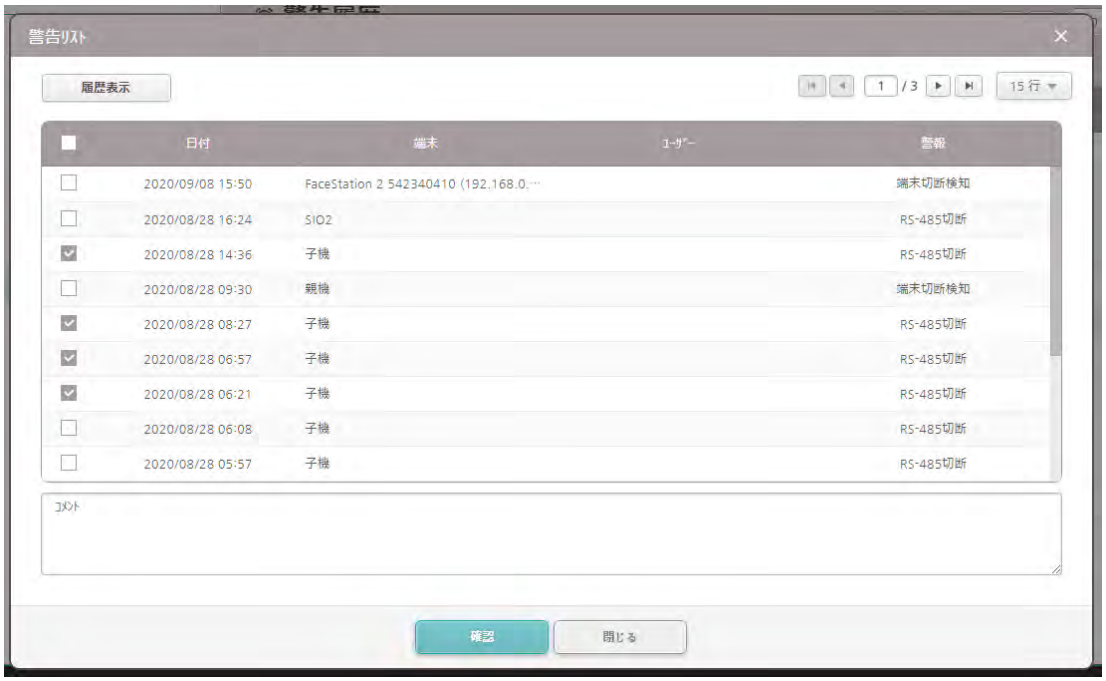
以下のように、今までで、未確認の警告が表示されます。



ここで、確認したい内容に☑を付けます。

（複数項目の同時確認も可能です。）

いずれかの項目に☑をすると、画面が以下のように変化します。



改めて、コメント欄が表示されますので、必要な場合は、コメント欄に記入し、「確認」を押してください。

☑を付けた項目は、確認済みとなります。

なるべく、すべての項目を「確認済み」としていただくことを推奨します。

18.3 確認済みの警告を再確認する方法

確認済みの警報を、再度確認する場合は、以下の方法で実施してください。

「モニタリング」 →「警告履歴」と操作してください。

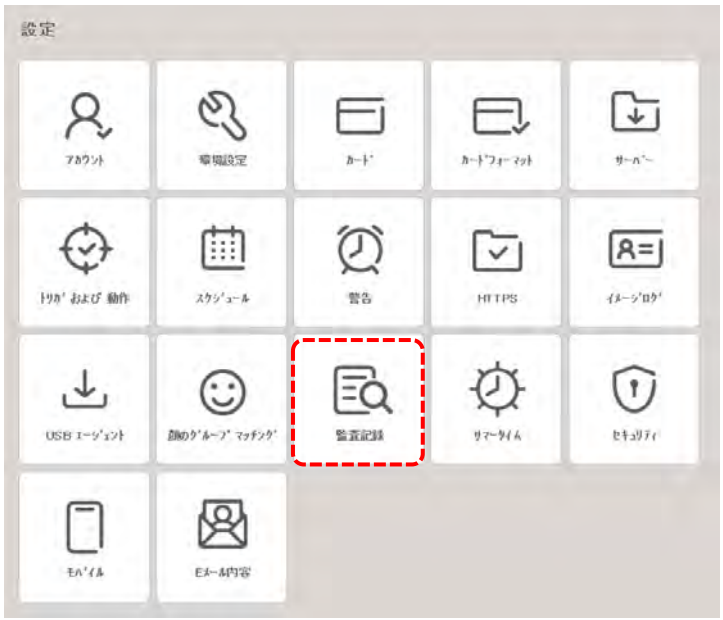
その説明については、17.5 章のモニタリング部を参照してください。

19 監査記録の確認

本システムでは、WEB ブラウザから操作した履歴を確認することができます。

確認を行う場合は、以下の画面で「設定」をクリックしてください。

右のような画面が表示されますので、
「監査記録」をクリックしてください。



監査記録の画面が表示されます。監査記録の画面では、最後の 1 ヶ月と最後の 3 ヶ月分をすぐに確認できる機能があります。こちらをクリックすると、設定中のフィルターを無視して、最後の 1 ヶ月および 3 ヶ月の監査記録を表示され確認ができます。

表示初期は、全項目の監査記録が表示されます。
表示される項目について説明をいたします。

・日時：事象発生日時が表示されます。
・ユーザー：事象発生時ログインユーザー
・BioStar 操作権限：ユーザーの操作権限が表示されます。
・ログイン元：操作時に接続された PC の IP アドレスが表示されます。
・カテゴリ：操作内容および発生元のカテゴリが表示されます。
・ターゲット：操作端末や操作者が表示されます。
・操作：操作内容概要
・変更：変更/更新内容

となります。

続いて、フィルター機能について説明します。各表示項目は、それぞれ、フィルターをかけて表示することが可能です。
フィルターはフリーキーワードまたは固定キーワードで行うことができます。

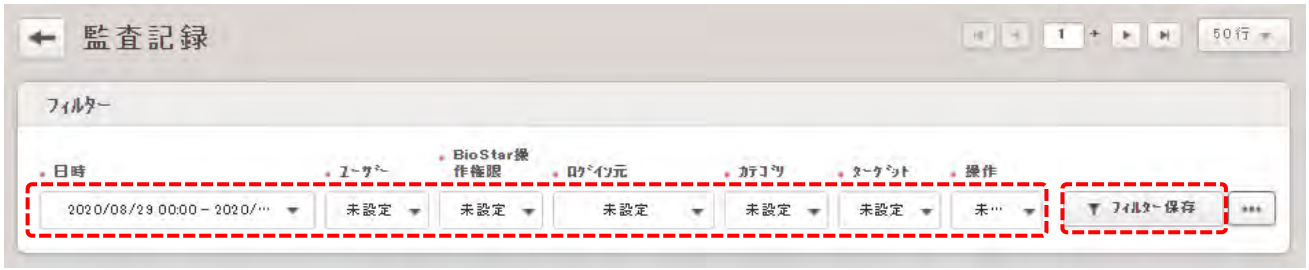
フリーキーワードの場合を説明します。
ターゲットの 未設定 をクリックする右の画面が表示されます。
フィルターをかけたいワードを赤枠の部分に入力し、「Enter」を押してください。
（入力した文字の部分一致でフィルターがかかり候補表示されます。）

例えば、「t」を入力した場合は右の画面が表示されます。
「t」を含む項目がすべて表示されますので、フィルターをかけたい項目を
クリックしてください。
下図のように表示されます。間違って選択した場合は 🗑 をクリックし
削除してください。

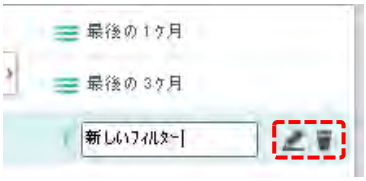
最後に、「条件の追加」をクリックすると、選択した項目でフィルターがかかります。

続いて、固定キーワードの場合を説明します。
カテゴリの 未設定 をクリックする右の画面が表示されます。
フィルターをかけたいワードが表示されますので、選択したいワードに☑を
入れてください。
最後に、「条件の追加」をクリックすると、選択した項目でフィルターがかかります。

また、そのフィルター設定自体を、名称を付けて保存することが可能です。



その場合は、「フィルター保存」 フィルター保存 をクリックすると、
右の画面が出ますので、フィルター名称を入力してください。
名称の修正・削除は、 をクリックしてください。



また、保存されたフィルターをクリックすると、フィルターを適用した状態の表示となります。

監査記録のページ切り替えや、1 ページあたりの表示件数を切り替える場合は、
を操作してください。

また、CSV ファイルで内容を出力することが可能です。 … をクリックしてください。
表示されたメニューから、「CSV エクスポート」を選択すると、自動的に、CSV ファイルのダウンロードが開始されます。
同様に「カラム設定」を選択することで、表示項目を減らすことも可能です。

20 勤怠の結果修正とレポート表示

BioStar2 システムは、簡易的な勤怠システムとしても利用することが可能です。
本章では、BioStar システムを勤怠システムとして利用する場合の運用上でよく使うと考えられる機能について、記載します。
本章の説明では、設定は完了していることを前提とし、日常の運用に関する部分を記載します。
設定については、別途、設定編（**エラー! 参照元が見つかりません。**章）をご確認ください。

20.1 基本操作および、確認可能方式

勤怠のデータは、以下の 3 つの方法で確認可能です。

- BioStar2 の画面で表示
- 表示した内容を CSV ファイルに出力
- 表示した内容を PDF ファイルに出力

ここでは、それぞれの確認の方法について記載します。

勤怠の結果を参照するために、右の画面の「勤怠」をクリックしてください。
下のような勤怠の画面が表示されます。まず、「レポート」をクリックしてください。
勤怠の表示内容を過去にフィルタリングされたものが表示されます。
（下図のような初期値が用意されていますが、変更・追加・削除が可能です。）
今後、利用する場合は、こちらをクリックしてください。
検索条件のフィルター条件が復元されます。

本説明では、こちらの初期値は使わず、表示内容を設定する方法で記載します。上の図で「フィルター追加」をクリックしてください。
画面の内容について、次のページで説明します。

① 勤怠の表示名称を入力してください。(一時的に表示するだけであれば、空欄でも構いません。)

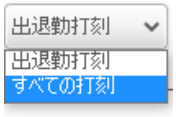
⑦と組み合わせて、今後もこの設定を利用する場合は、区別のつけやすい名称を入力してください。

② レポート表示の種別を選択してください。以下の種類から選択可能です。

レポート種別	内容
日	日を第一優先とし、指定したユーザーの勤怠情報がユーザーごとに表示されます。 (範囲内の日ごとにソートされ、それぞれの日に個人ごとの勤務時間が表示されます。)
日の概要	日を第一優先とし、指定したユーザー全員分のその日の合計の勤怠情報が表示されます。 (範囲内の日、それぞれで、全員の合計勤務時間を確認したい場合に利用します。)
個人	個人を第一優先とし、勤怠情報が日ごとに表示されます。 (個人ごとに、ソートされ、それぞれの日の勤怠情報を見たい時に利用します。)
個人概要	個人を第一優先とし、指定した範囲の日で合計した勤怠情報が表示されます。 (それぞれの個人の月の合計値などを確認する場合に利用します。)
休暇	休暇のタイムコードを指定することで、期間内に指定した休暇のタイムコードを利用した 人や日付の情報を表示します。
補足または補足数	日を第一優先とし、ユーザーごとに、補足情報(遅刻や早退、欠勤など)を表示します。
修正済み打刻ログ記録	勤怠情報を後から修正した場合、修正履歴の一覧を表示します。
労働警報時間	指定した時間以上の労働時間があるユーザーを検索します。また、特定の曜日・時間・メールアドレスに 警告メールを送信することが可能です。

③ レポート種別で「個人」を選択したときのみ表示されます。

右の図のように、「出退勤打刻」または「すべての打刻 」から選択できます。



④ 各レポート種別のレポート表示のカラムを変更することが可能です。

例として、レポート種別が 日 を選択した場合の初期値のカラムは、以下となります。

レポート種別ごとに、カラムを削除したり、追加で表示したりを設定できます。

⑥と併せて、表示対象者のフィルタリングになります。⑤で選択したユーザーグループの中から、⑥で更にユーザーを選択する形となります。

⑤を選択しない場合は、⑤で All Users を選択した場合と同様で、⑥で全ユーザーが選択できます。

⑤を選択した場合は、選択したグループの中から、⑥でユーザーを選択します。

⑤だけを選択し、⑥を選択しない場合は、⑤で選択したグループの全員が対象となります。

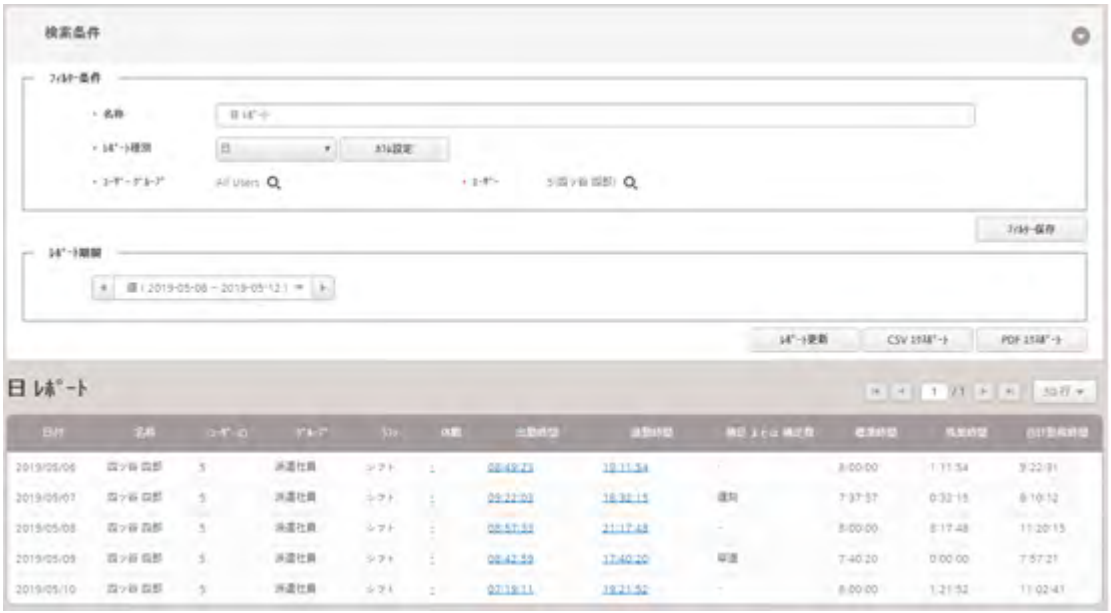
⑤ ⑤と組み合わせてご利用ください。

⑥ ここまでの①～⑥の設定値を記録することが可能です。

⑦ レポートとして表示する期間を選択します。 日/週/月/カスタム 単位で選択可能です。 カスタム以外の場合は、左右矢印のボタンで、選択している範囲で、前後の変更が可能です。

カスタムの場合は、選択すると、開始日と終了日が表示されますので、それぞれをクリックしカレンダーで選択します。

⑧ ①～⑧までの検索条件に合わせて、データを画面下部に表示します。



⑨ ⑨と同様の計算と、その結果を CSV 出力することが可能です。

クリックすると、結果を表示し、その後、ダウンロードが始まります。

⑩ ⑨と同様の計算と、その結果を PDF 出力することが可能です。

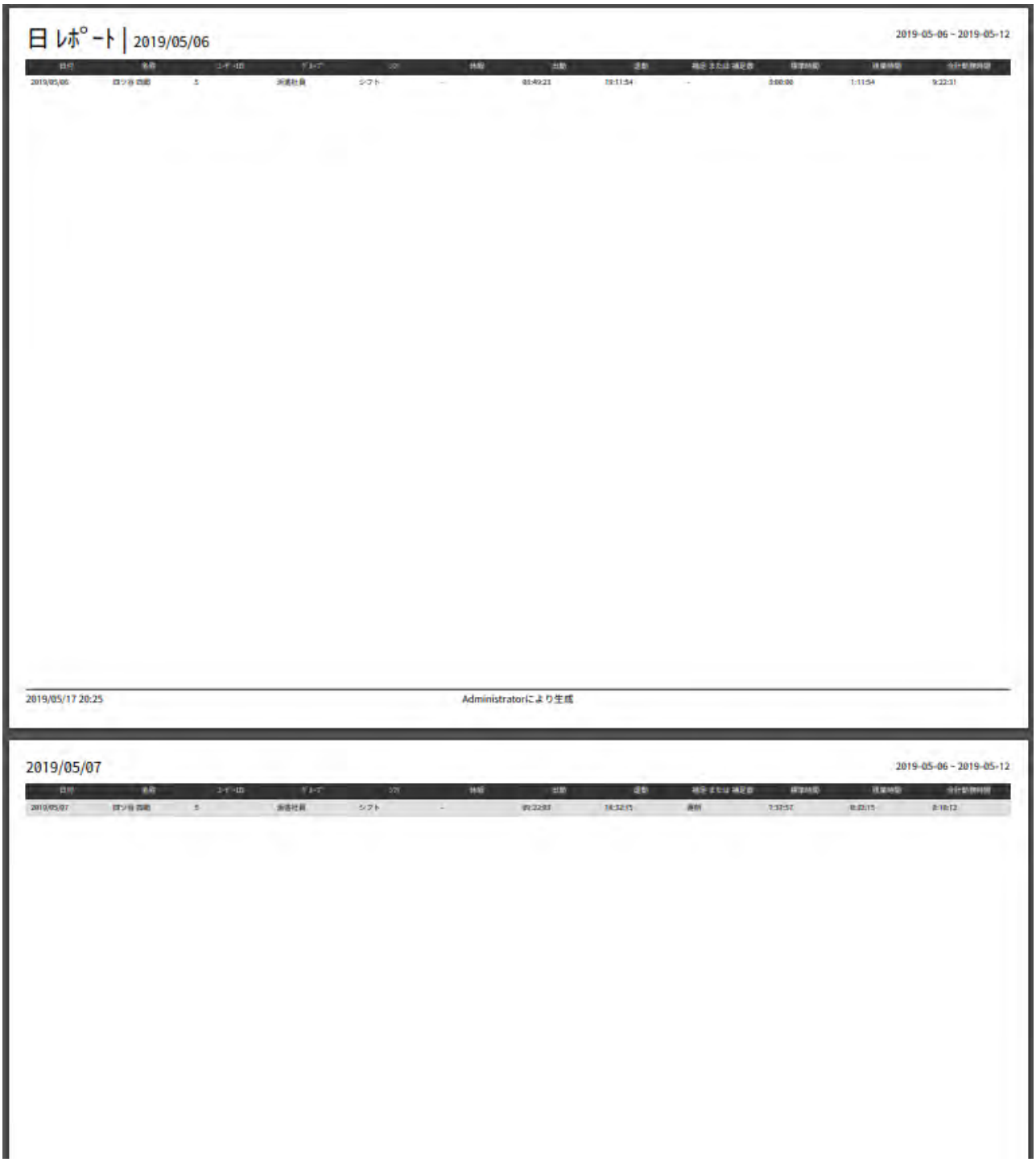
クリックすると、結果を表示し、その後、新しいタブで PDF を表示します。(ブラウザでポップアップを許可する必要があります。)

それぞれの表示イメージを次のページに示します。

CSV ファイルに出力

日付	名称	ユーザーID	グループ	シフト	休暇	出勤	退勤	補足 または 補足数	標準時間	残業時間	合計勤務時間
"2019/05/06"	"四ツ谷 四郎"	"5"	"All Users/派遣社員"	"シフト"	"-"	"08:49:23"	"19:11:54"	"-"	"8:00:00"	"1:11:54"	"9:22:31"
"2019/05/07"	"四ツ谷 四郎"	"5"	"All Users/派遣社員"	"シフト"	"-"	"09:22:03"	"18:32:15"	"遅刻"	"7:37:57"	"0:32:15"	"8:10:12"
"2019/05/08"	"四ツ谷 四郎"	"5"	"All Users/派遣社員"	"シフト"	"-"	"08:57:33"	"21:17:48"	"-"	"8:00:00"	"3:17:48"	"11:20:15"
"2019/05/09"	"四ツ谷 四郎"	"5"	"All Users/派遣社員"	"シフト"	"-"	"08:42:59"	"17:40:20"	"早退"	"7:40:20"	"0:00:00"	"7:57:21"
"2019/05/10"	"四ツ谷 四郎"	"5"	"All Users/派遣社員"	"シフト"	"-"	"07:19:11"	"19:21:52"	"-"	"8:00:00"	"1:21:52"	"11:02:41"

PDF ファイルに出力



※PDF は、日単位や、ユーザー単位で、ページを切り替えて出力します。

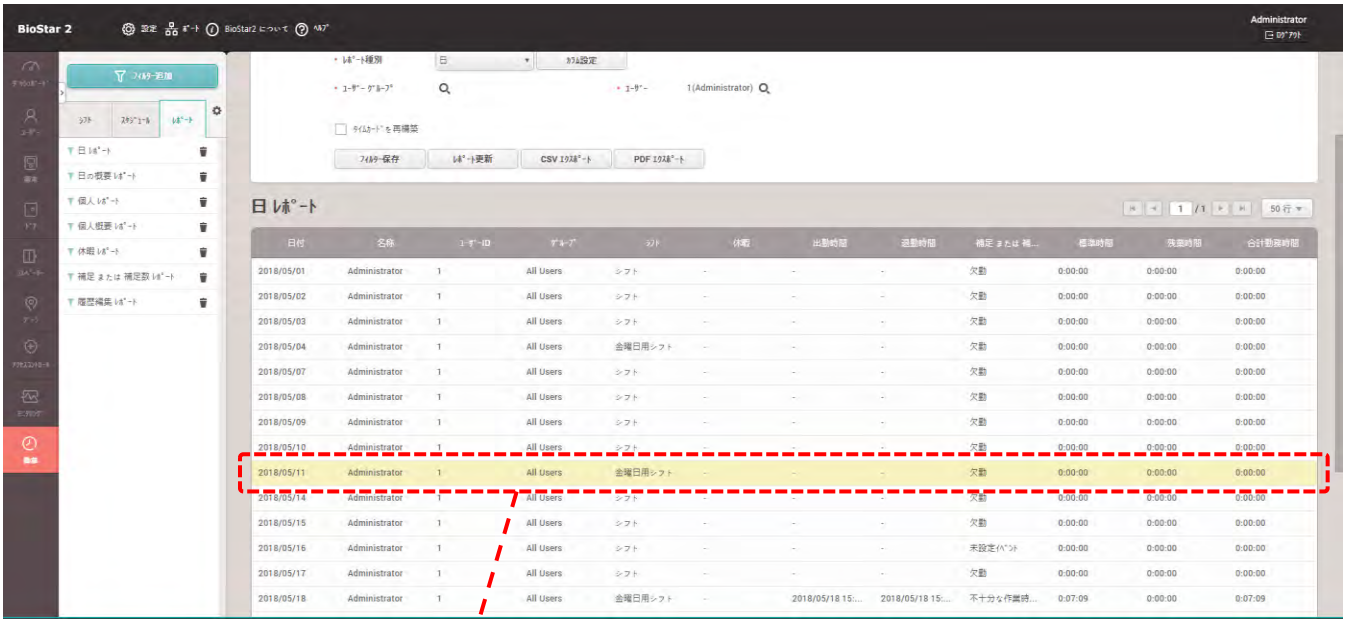
上記例は、日単位での出力のため、1 日辺り 1 ページで表示されています。

20.2 出力内容の詳細表示

BioStar2 勤怠のレポート表示は、更に詳細を表示することが可能です。レポート種別が、

日 / 個人 / 休暇 / 補足または補足数 / 修正済み打刻ログ記録

の場合は、レポート表示した内容をクリックすると、以下の各日の詳細表示画面に遷移します。



各日をクリックすると、その日の詳細を表示

この画面から、更にクリックして、様々な機能に分岐します。

それぞれの機能は、この後に記載します。

20.2.1 一時スケジュール（シフト）の変更・削除

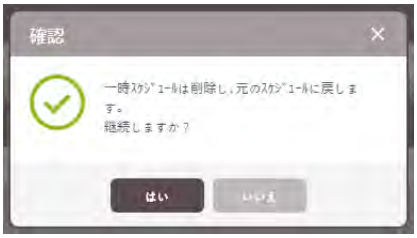
基本的には、ユーザーにはシフトが割当てられ、それがスケジュールとして組まれています。この予定されたシフトを、一時的なスケジュールとして変更することが可能です。出力内容の詳細表示 20.2 章の画面のシフトの部分をクリックしてください。

シフト部をクリックすると、一時スケジュール画面を表示

この画面で、区別のつく名称を入力し、新しいシフトノ選択、対象期間、対象ユーザーを設定し、「適用」をクリックすると反映されます。

上記の様に、対象のシフトが変更されます。（2018/5/11 が、「金曜日用シフト」から、「シフト」に変更されました。）

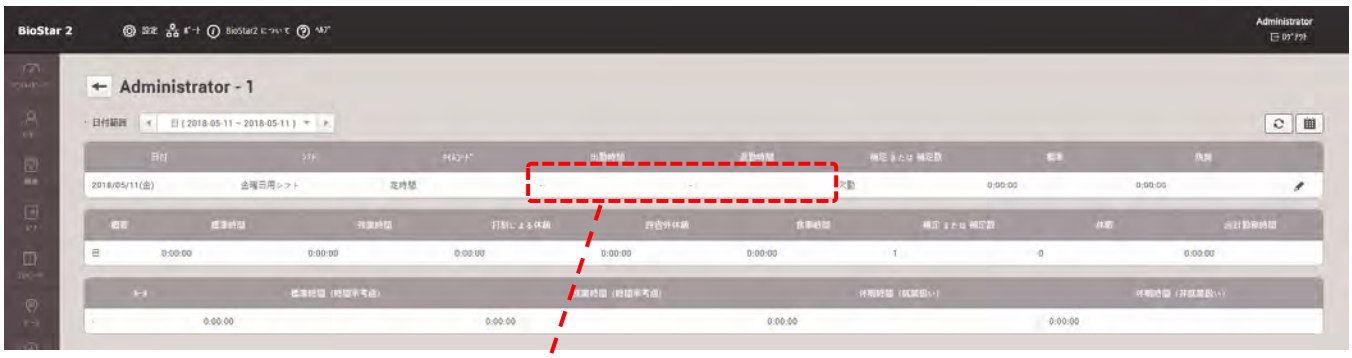
また、変更したシフトをもとに戻す場合は、このシフト部分を、再度クリックしてください。
以下の確認画面を表示します。元のスケジュールに戻す場合は、「はい」をクリックしてください。



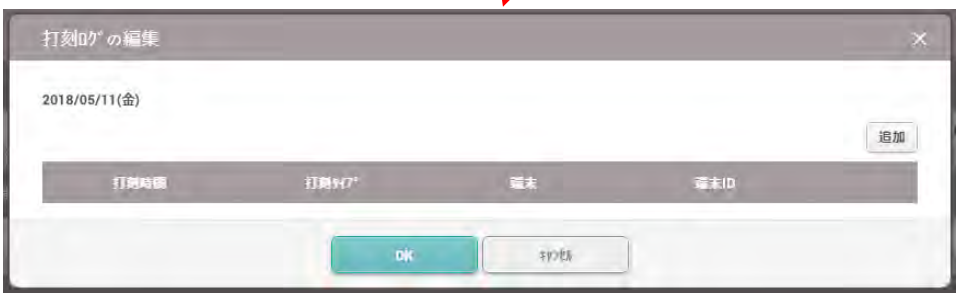
その後、レポートデータを再表示すると、シフトが元通りに戻ったことを確認できます。

20.2.2 出勤時間・退勤時間の修正（打刻データ修正）

打刻データを後から修正することが可能です。20.2 章の画面の出勤時間 および 退勤時間の部分をクリックしてください。



出勤時間・退勤時間部をクリックすると、
打刻ログの編集画面を表示



元が欠勤の日の場合は、データが空欄状態ですが、打刻がある場合は、打刻済みの内容が表示されます。
「追加」ボタンをクリックすると、以下のように入力枠が表示されます。

日付・時間と打刻タイプ（出勤や退勤など）を設定し、☑ をクリックすると反映されます。
 をクリックすると、この編集状態を解除します。☑をクリック後は、一時確定になります。
再編集する場合は、 マークを、作成したデータ自体を削除する場合は、 マークをクリックしてください。
変更後、適用すると、以下のように、打刻の修正が行われます。
（出勤を 9:00 退勤を 18:30 とした例）

20.2.3 休暇の登録（適用）

作成済みの休暇情報を登録することが可能です。20.2 章の画面の✎の部分をクリックしてください。

✎ マークをクリックすると、
休暇の編集画面を表示

① 休暇編集の対象日が表示されます。

② 休暇管理で事前に作成している時間規則の中から、登録する休暇の時間規則を選択してください。

③ 休暇の時間が必要な場合（AM 半休や PM 半休、少時間休暇など）の場合に、☑を入れてください。
④部分が、日だけではなく、時間も入力できるようになります。

④ 休暇の開始と終了を設定してください。（③で時間指定に☑した場合は、時間まで指定してください。）

⑤ 休暇の時間が日にち単位、または、時間単位で表示されます。（④で指定した分の時間が表示されます。）

⑥ 選択ユーザーのみではなく、他のユーザーにも適用する場合は、指定してください。

⑦ 承認時のコメントとして、メモの様に休暇の理由等を記載することが可能です。（空欄でも構いません。

⑧ ①～⑦の情報で登録して良い場合は、「OK」をクリックしてください。

⑨ 休暇編集をやめる場合は、「キャンセル」をクリックしてください。

打刻データが無く、欠勤と扱われた日が、本来は休暇だった場合に、登録すると次のページのような画面になります。

① 取得した休暇が表示されます。就業扱いの休暇登録した時間規則のため、出勤・退勤の時間が表示されています。

② 就業時間として、8 時間表示になっています。

③ このシフトには食事控除が含まれているので、その分の 1 時間であることが表示されています。

④ 休暇を 1 つ取得したので、休暇 の部分が 1 と表示されます。

⑤ この日の全体としての標準時間が 8 時間であることが表示されます。

⑥ 休暇時間（就業扱い）が 9 時間であることが表示されます。

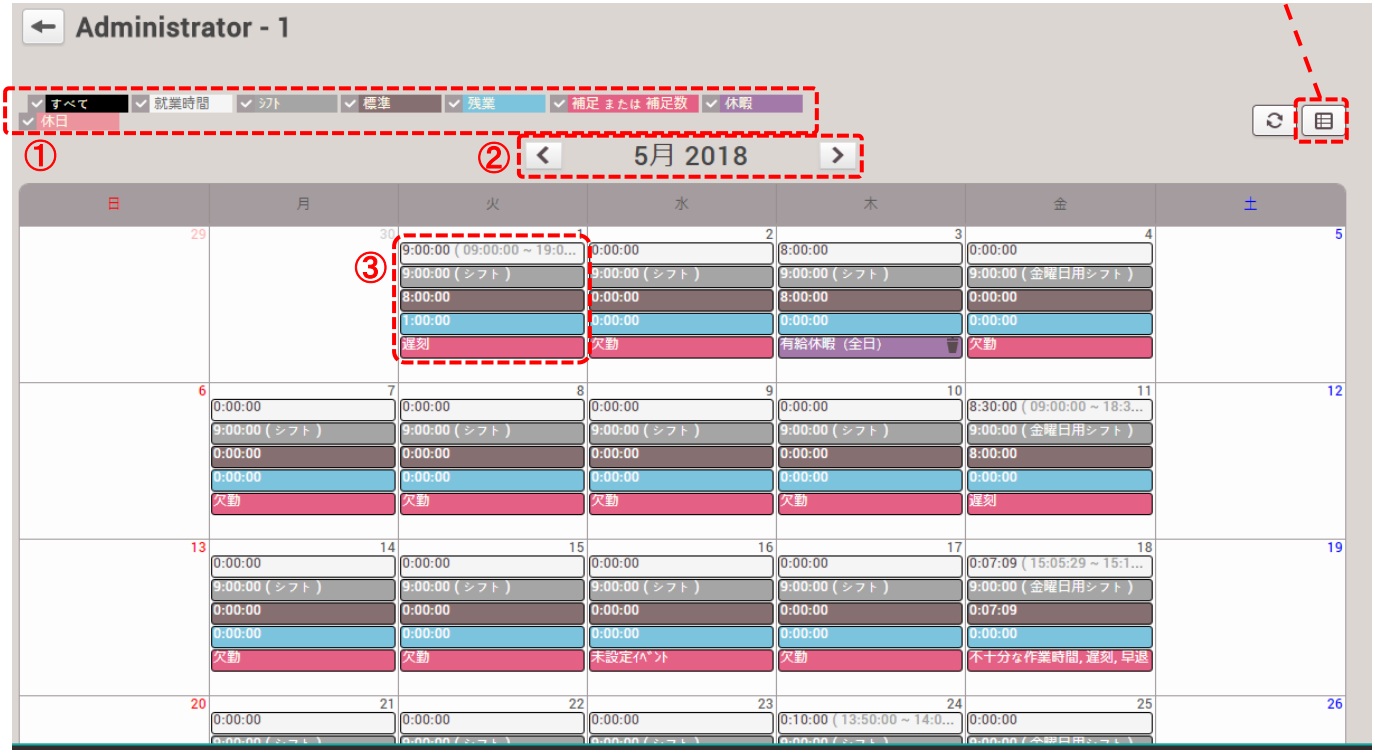
もし、非就業休暇の時間規則（届出欠勤や、無断欠勤（自己都合欠勤））を選択した場合は、非就業扱いの時間が表示され、標準時間としては、0 となります。

また、もし、この休暇情報を取り消す場合は、①の右端の をクリックしてください。
以下の確認画面が表示され、「はい」をクリックすると、休暇情報を削除します。

20.2.4 カレンダータイプ表示

詳細内容表示の画面から、カレンダータイプの表示に変更することが可能です。

右上のボタンをクリックすると、画面表示がカレンダー表示になります。
また、カレンダー表示の右上のボタンで、リスト表示に戻ります。



① 表示する項目にフィルタリングをかけることが可能です。☑のオン/オフで、カレンダーの表示項目が変化します。

② 表示対象の月を左右の矢印で変更可能です。

③ 対象者のその日の情報を表示します。

白:就業時間 / 灰色:シフトとしての時間とシフト名 / こげ茶:標準勤務時間 / 残業:水色 / ピンク:補足 / 紫:休暇

薄ピンク:祝日

各色の項目をクリックすると、以下の画面に遷移します。

白:打刻ログの編集画面(20.2.2 章参照)

灰色:休暇編集画面(20.2.3 章参照)

こげ茶、水色、ピンク、薄ピンク: クリック不可

紫:項目は削除不可だが、横の アイコンのクリックにより、休暇登録を削除可能

また、カレンダー下部には、該当ユーザーの月単位の情報が表示されます。

なお、本情報は確認のみで、クリックにより別画面での編集等はできなくなっています。

20.3　出力内容の詳細表示（その他表示時）

BioStar2 勤怠のレポート表示は、更に詳細を表示することが可能です。レポート種別が、

個人概要

の場合は、レポート表示した内容をクリックすると、以下の各日の詳細表示画面に遷移します。

該当の個人に対して、日の範囲のデータが一覧表示となります。

日付	ｼﾌﾄ	ﾀｲﾑｺｰﾄﾞ	出勤時間	退勤時間	補足 または 補足数	標準	残業
2018/05/01(火)	シフト	定時間	2018/05/01 09:00:...	2018/05/01 19:00:...	遅刻	8:00:00	1:00:00
2018/05/02(水)	シフト	定時間	-	-	欠勤	0:00:00	0:00:00
2018/05/03(木)	シフト	定時間	-	-	-	8:00:00	0:00:00
	休暇	有給休暇（全日）	2018/05/03 09:00:...	2018/05/03 18:00:...	-	-	-
2018/05/04(金)	金曜日用シフト	定時間	-	-	欠勤	0:00:00	0:00:00
2018/05/07(月)	シフト	定時間	-	-	欠勤	0:00:00	0:00:00
2018/05/08(火)	シフト	定時間	-	-	欠勤	0:00:00	0:00:00
2018/05/09(水)	シフト	定時間	-	-	欠勤	0:00:00	0:00:00
2018/05/10(木)	シフト	定時間	-	-	欠勤	0:00:00	0:00:00
2018/05/11(金)	金曜日用シフト	定時間	2018/05/11 09:00:...	2018/05/11 18:30:...	遅刻	8:00:00	0:00:00
2018/05/14(月)	シフト	定時間	-	-	欠勤	0:00:00	0:00:00
2018/05/15(火)	シフト	定時間	-	-	欠勤	0:00:00	0:00:00
2018/05/16(水)	シフト	定時間	-	-	未設定ｲﾍﾞﾝﾄ	0:00:00	0:00:00
2018/05/17(木)	シフト	定時間	-	-	欠勤	0:00:00	0:00:00

① 各日のシフトをクリックすると、一時スケジュールの変更が可能です。（20.2.1 参照）

② 出勤時間・退勤時間をクリックすると、打刻ログの編集が可能です。（20.2.2 参照）

③ 休暇以外の部分は、 マークをクリックすることで、休暇編集画面を表示します。
休暇の部分は、 マークをクリックすると休暇を削除します。

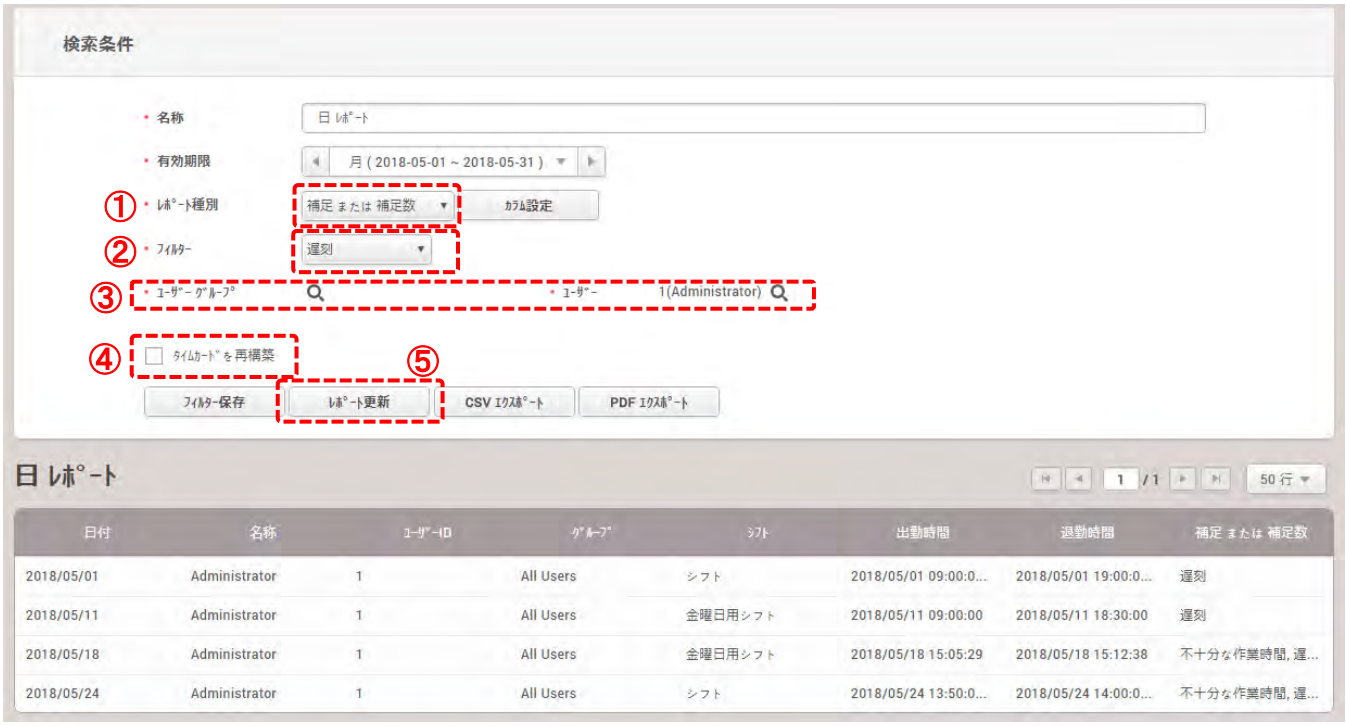
また、画面下部には、月単位の勤怠情報を表示します。

概要	標準時間	残業時間	打刻による休憩	許容外休憩	食事時間	補足 または 補足数	休暇	合計勤務時間
月	24:17:09	1:00:00	0:02:02	0:00:00	3:00:00	26	1	25:47:09

ﾙｰﾙ	標準時間（時間率考慮）	残業時間（時間率考慮）	休暇時間（就業扱い）	休暇時間（非就業扱い）
-	24:17:09	1:12:00	9:00:00	0:00:00

20.4 補足 を活用した表示

勤怠データの表示方法として、「補足または補足数」の表示項目で、補足内容を選択して表示することが可能です。
例えば、「遅刻したユーザーの情報だけが知りたい。」などの場合に有効です。
以下の例は、遅刻した時の情報のみを表示する例です。



① レポート種別に、「補足または補足数」を選択します。

② フィルターに「遅刻」を選択します。

③ 対象とするユーザーを選択します。

④ 過去に表示した値の場合は、☑なし。念の為、再計算する場合は、☑を入れます。

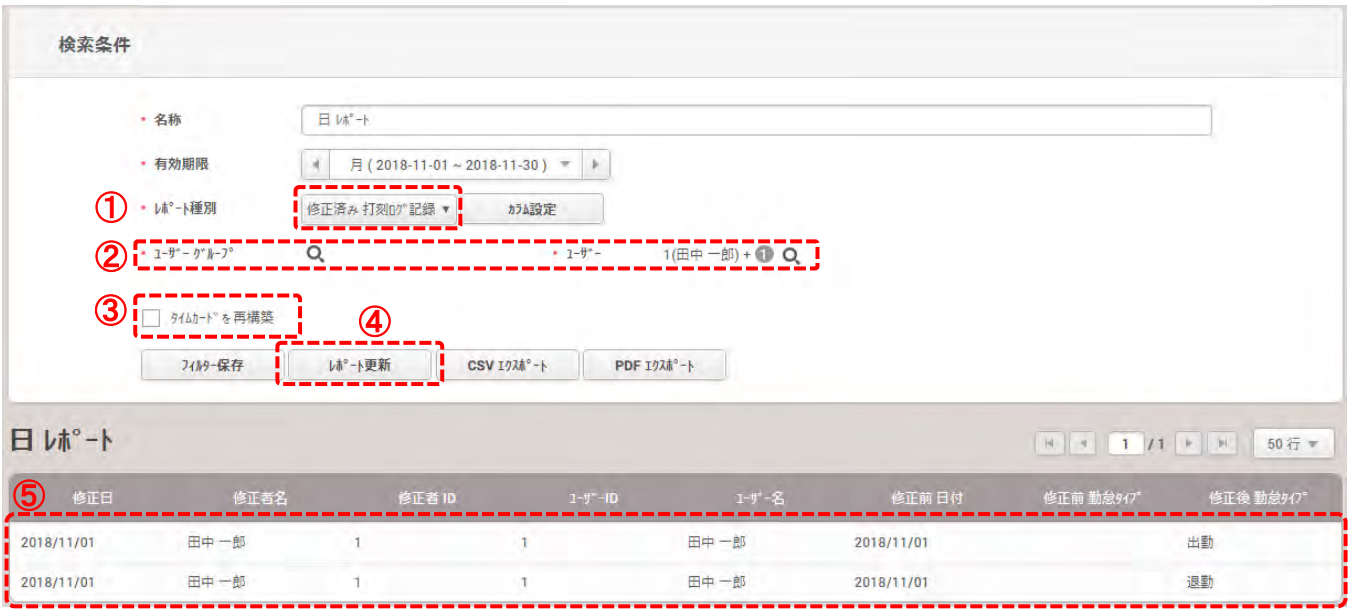
⑤ 「レポート更新」ボタンをクリックします。

これにより、補足に「遅刻」を含むデータが表示されます。

20.5 修正履歴の確認

勤怠データの修正をした場合、その修正データを確認することが可能です。

以下の例は、出勤/退勤時間を変更した時の例です。



① レポート種別に、「修正済み打刻ログ記録」を選択します。

② 対象とするユーザーを選択します。

③ 過去に表示した値の場合は、☑なし。念の為、再計算する場合は、☑を入れます。

④ 「レポート更新」ボタンをクリックします。

⑤ ソフトウェアで、時刻や内容を修正したデータが表示されます。

修正日・修正者・修正者の ID と、修正されたユーザーID とユーザー名、修正前の日付と修正前・修正後の勤怠タイプが表示されます。

これにより、手入力で修正した内容が確認可能です。

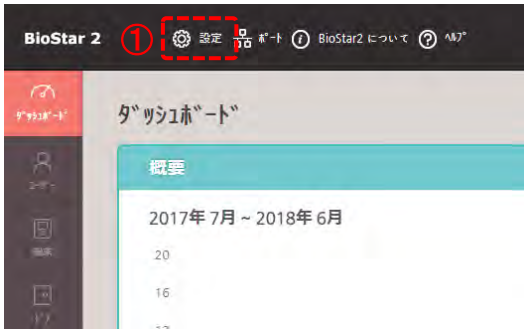
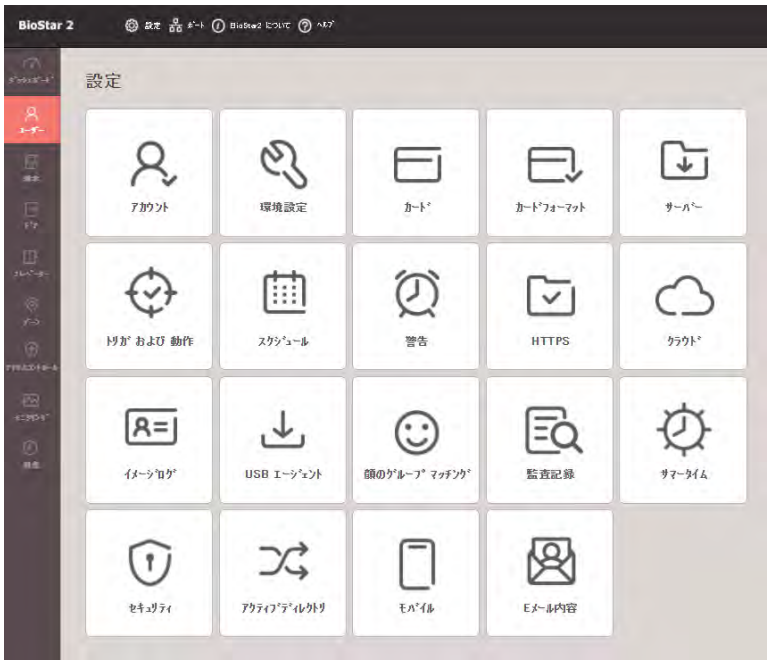
設定編

以降では、BioStar システムの設定について記載します。
変更される内容によっては、正しく動作しなくなる場合もございます。
設定変更は、ご注意の上実施願います。

設定編（システムの管理者の方向け）

21 BioStar2 の設定

BioStar2 ソフトウェアの全体の設定項目について記載します。ログインするユーザーの権限により表示される範囲が変化し

説明図	操作内容
	① BioStar2 にログインし、「設定」をクリックしてください。
	左図の画面が表示されます。 設定したい項目をクリックしてください。 以下の章で、それぞれについて説明します。 （表示内容については、適用されているライセンスにより異なります。） ・アカウント（21.1 章） ・環境設定（21.2 章） ・カード（21.3 章） ・カードフォーマット（21.4 章） ・サーバー（21.5 章） ・トリガ および 動作（21.6 章） ・スケジュール：（21.7 章） ・警告（21.8 章） ・HTTPS（21.9 章） ・クラウド（21.10 章） ・イメージログ（21.11 章） ・USB エージェント（21.12 章） ・顔のグループマッチング（21.13 章） ・監査記録（21.14 章） ・サマータイム（21.15 章） ・セキュリティ（21.16 章） ・アクティブディレクトリ（21.17 章） ・モバイル（21.18 章） ・E メール内容（21.19 章）

ます。本マニュアルでは、管理者でログインした場合を前提として記載します。設定画面を表示するには、以下の手順で表示してください。

21.1 アカウント 項目

アカウント項目では、BioStar2 にログインするユーザー単位で持つ権限を確認・新規追加することができます。
通常、初期状態でアカウントの画面に進むと、以下のようになります。

初期値で、5 種類のユーザー権限があり、作成するユーザーに対し、権限を付与することが可能です。
上記の 5 種類で足りない場合は、左上の「カスタムレベルの追加」ボタンをクリックし、個別設定のアカウントのレベルを作成することが可能です。例えば 以下のようなアクセス権限の作成・設定が可能です。

この様に、アクセスレベルを作成・適用すると、カスタムアクセスレベルが作成されます。
作成が完了すると、次回以降、ユーザーを作成するたびに、カスタムレベルも合わせユーザーの権限が設定できるようになります。

21.2 環境設定 項目

環境設定項目では、BioStar2 の基本的な設定を変更することが可能です。以下のような画面になります。

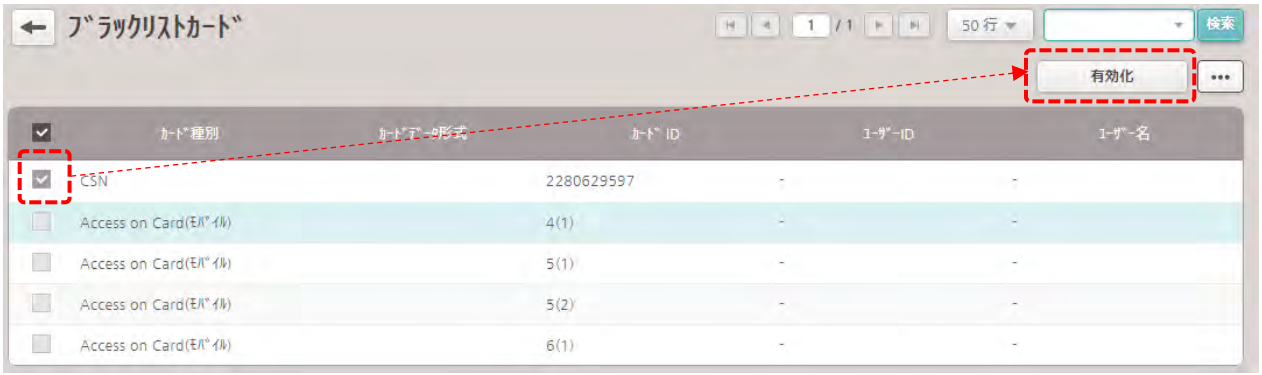
言語については、利用される方に合わせて設定してください。タイムゾーンは、(UTC+9:00) を選択してください。
サマータイムは、日本国内では、空欄でご利用ください。日付形式および時刻形式は、ご利用に合わせ選択してください。
効果音の項目については、追加する場合は、「＋追加」をクリックし、追加してください。BioStar2 システムに追加すると、他の設定部分で PC から音声を再生する際に利用できます。「＋追加」をクリックすると、以下の画面が表示されます。

音声名称を決め、「参照」ボタンをクリックし、wav ファイルか、mp3 ファイルから選択して、「追加」をクリックして登録してください。

21.3 カード 項目

BioStar2 システムに登録されているカード内容を表示します。また、カードの状態として、未割当カード, 割当済みカード, ブラックリストカードをそれぞれ、確認することも可能です。また、ブラックリストカードに関しては、ブラックリストから解除することができます。

1 の項目から、それぞれをクリックすると、右側の表示項目がフィルタリングされた状態で表示されます。
また、①の項目で、ブラックリストカードを選択した場合は、ブラックリストの一覧に、チェックボックスが表示されます。
1つでも☑すると、画面右上にブラックリストから解除するための「有効化」ボタンが表示されます。
「有効化」をクリックすると、ブラックリストから解除されます。



なお、アクセス オン カードは、削除できません。

21.4 カードフォーマット 項目

カードフォーマット項目では、Wiegand のフォーマットと、スマートカードのフォーマットを設定することが可能です。

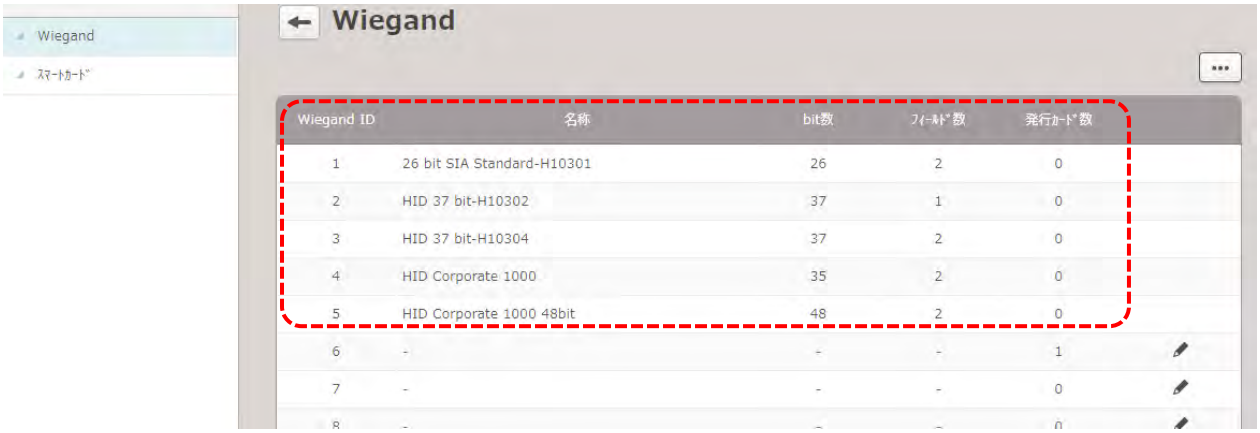
21.4.1 Wiegand

21.4.1.1 Wiegand(ウィーガンド) とは

Wiegand とは、入退室管理の製品の通信規格です。
相手側の製品も Wiegand に対応している場合、製品間でデータの受け渡しをすることが可能です。
例えば、2 台の製品を接続する場合、どちらかがデータを送信し、相手側がデータを受信する。という仕組みであり、データは、設定により一方通行となります。
BioStar の認証機は、送信(出力)側としても、受信(入力)側としても機能することが可能です。
また、本章では、Wiegand のフォーマットについての説明を記載します。実際の認証機の設定は、23.2 章を参照してください。

21.4.1.2 Wiegand カードフォーマット(標準)

通信をする場合は、送信側と受信側で、データフォーマットのルールを事前に決めておく必要があります。
Wiegand カードフォーマットは、その通信内容を事前に設定する部分となります。
BioStar2 では、世界的に標準化されているフォーマット 5 種類を標準で利用可能です。



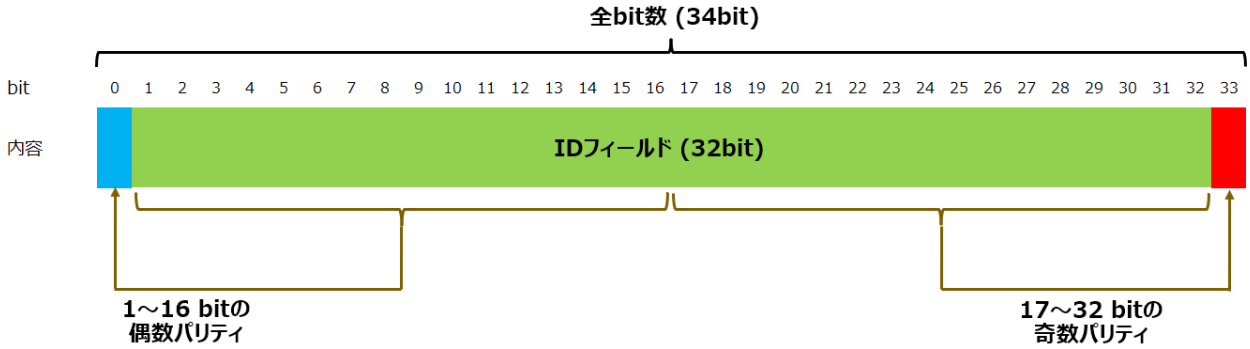
21.4.1.3 Wiegand カードフォーマット(カスタマイズ)

標準 5 種類の Wiegand フォーマットで合わない場合は、6 番目～15 番目まで、10 種類のフォーマットを作成可能です。
ここでは、以下の条件に合うように、6 番目にカスタマイズフォーマットを作成する場合の例を記載します。
通信する相手と同じフォーマットである必要があるため、通信内容は、通信相手側と調整してください。

条件 例(通信相手側から提示されたフォーマットが以下の場合)

- ファシリティフィールド :なし
- ID フィールド(ユーザーID/カード ID 選択) :開始 bit 1 から、bit 長 32
- パリティ bit :偶数 bit 0 範囲 bit1～16 bit 長 16
  :奇数 bit 33 範囲 bit 17～32 bit 長 16
- 全 bit 長 :34bit

図示すると以下のようになります。



この内容を Wiegand フォーマットで作成すると、以下のようになります。

6 番目のフォーマットとして、作成するため、フォーマット 6 番目の をクリック

図に沿って、フォーマットを指定します。

なお、上記例では、ファシリティコードフィールドが無しの例でしたが、もし、ファシリティコードフィールドを利用する場合は、ファシリティコード フィールドにチェックを入れると、以下のように範囲が設定できます。

どの範囲が、ファシリティコードフィールドなのかを設定してください。

設定が完了したら、画面下の 適用 をクリックし、完了となります。

指定した場所に、フォーマットが作成されます。

再編集する場合は、 をクリック、削除する場合は、 をクリックしてください。

21.4.1.4 Wiegand カードフォーマットの検討ポイント

Wiegand カードフォーマットを検討するためのポイントを説明します。

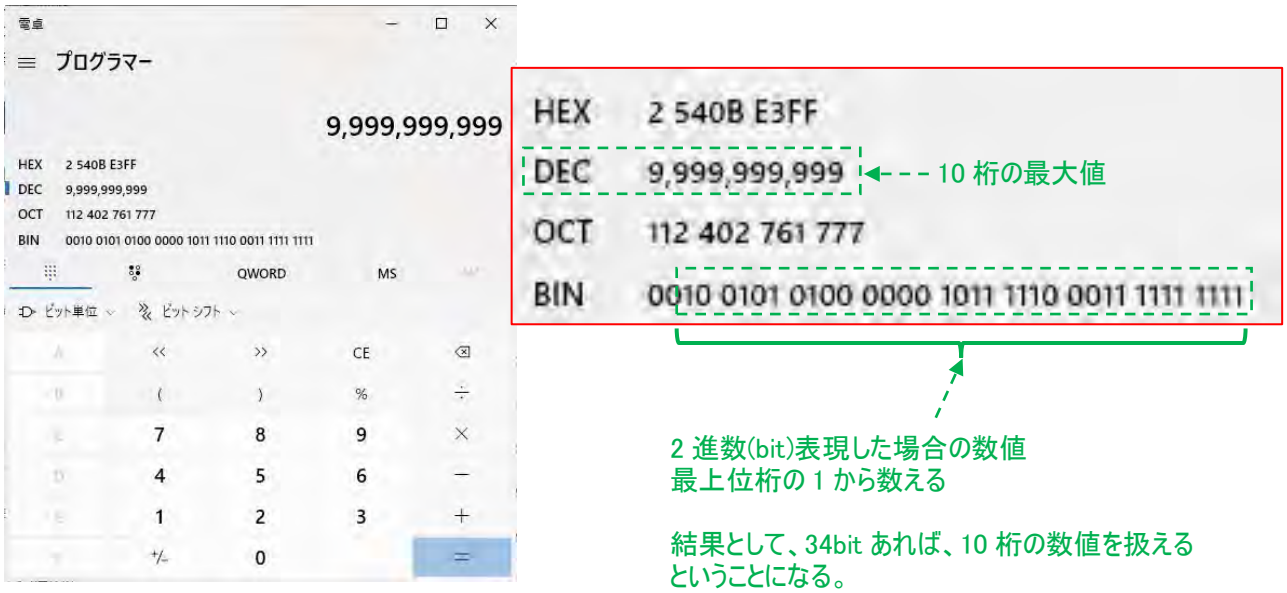
[ポイント1]
ファシリティコードは、フォーマット上、必要な場合にご利用ください。設定した開始 bit～終了 bit の範囲で、
通信上、自動的に値が設定されます。通信相手側で必要ない場合は設定する必要はありません。

[ポイント 2]
ID フィールドは、最大で何桁の数字を送るか/受けるか？ あるいは、何 bit 送るか？/受けるか？を
前提に検討してください。

例えば、カードをかざした時の、カード CSN を そのまま Wiegand で送る/受ける とする場合は、カードの種類により
以下の設定値となります。

- Mifare Classik/Standard 1K/4K 32bit
- Mifare Ultralight 56bit
- DESFire EV1 64bit
- FeliCa 64bit
- EM 64bit

あるいは、ユーザーID を、転送する場合は、その桁数は、何桁の数字になるか？
例えば利用する範囲のユーザーID が、最大で、10 桁の場合、最大の数字は、9999999999 となります。
この数字を、bit 表現で考えます。(Windows の電卓を「プログラマ電卓モード」にし、利用する方法で記載します。)



［ポイント 3］
パリティ bit は、通信エラーをチェックするための bit です。
必ず必要と言う訳ではありませんが、パリティ bit を持たないと、通信中にデータ化けをした場合に違う値として扱われてしまうため、パリティ bit を設定することを推奨します。
（パリティ bit の設定により、通信中にデータ化けしたことが判断できれば、再送を要求し、正しい値を通信することが可能です。）
それぞれのパリティ bit は、以下の内容となります。

偶数パリティ: 指定した範囲の bit 内の 1 の数を数え、その数が、偶数の場合は、0/奇数の場合は、1 とする。
奇数パリティ: 指定した範囲の bit 内の 1 の数を数え、その数が、奇数の場合は、0/偶数の場合は、1 とする。

21.4.2 スマートカード

21.4.2.1 スマートカード とは

スマートカードとは、通常の IC カードのカード固有の ID（CSN）を利用せず、ユーザー領域と呼ぶ利用可能なメモリ領域に、専用のコードを書き込み、そのメモリ領域を利用する方法です。
スマートカードが利用可能なカードの種類は、

・Mifare および、DESFire

となります。
Mifare Ultralight カード, FeliCa カード, EM カード, ISO15693 カード(iCODE-SLI) は、スマートカードとしては、利用できません。
（BioStar2 としては、 iClass および iClass Seos カードもスマートカードとして利用できますが、弊社取り扱いの認証機では、利用できません。）

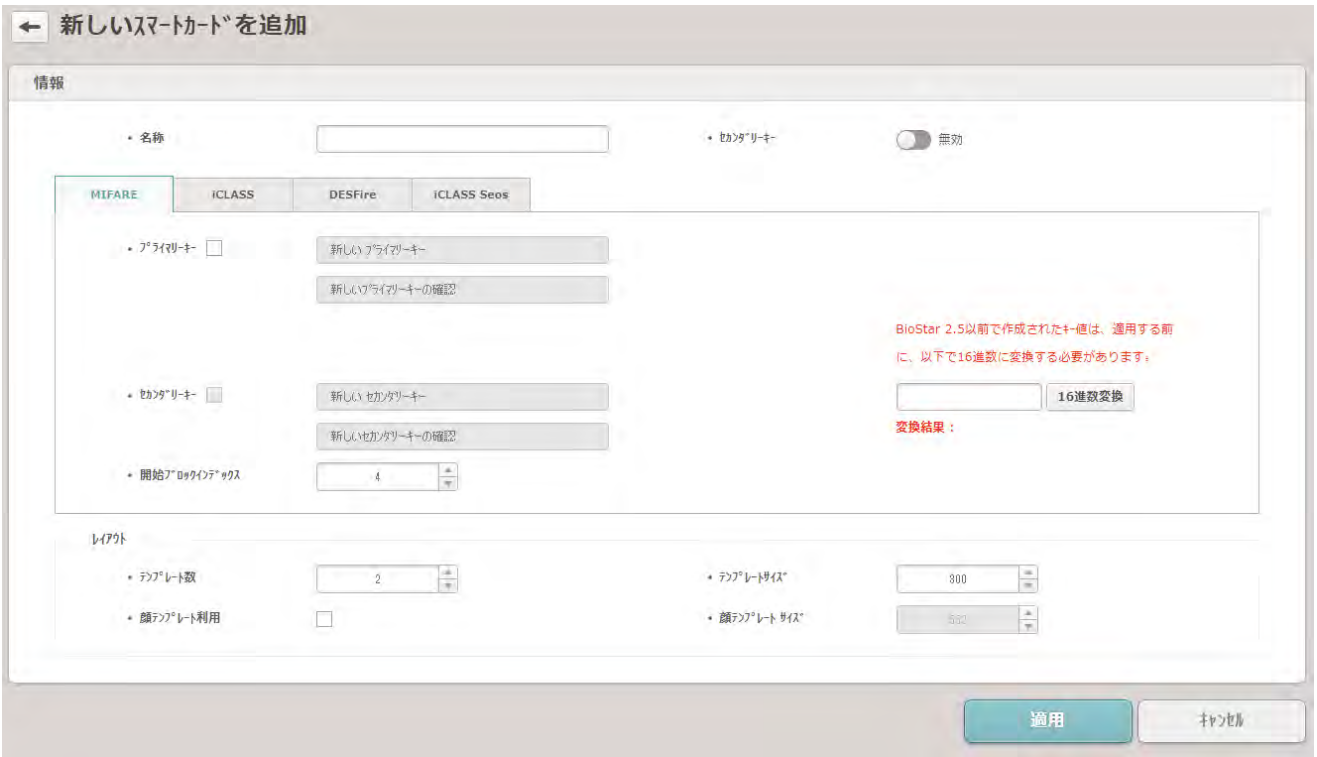
スマートカードは、カード側と認証機側に共通のパスワードを設定することも可能です。
但し、一度、カードにパスワードを書き込み、忘れてしまうと、ユーザー領域を書き換えることができなくなります。
（初期化もできません。）
このため、カードにパスワードを書き込む際は、注意してご利用ください。

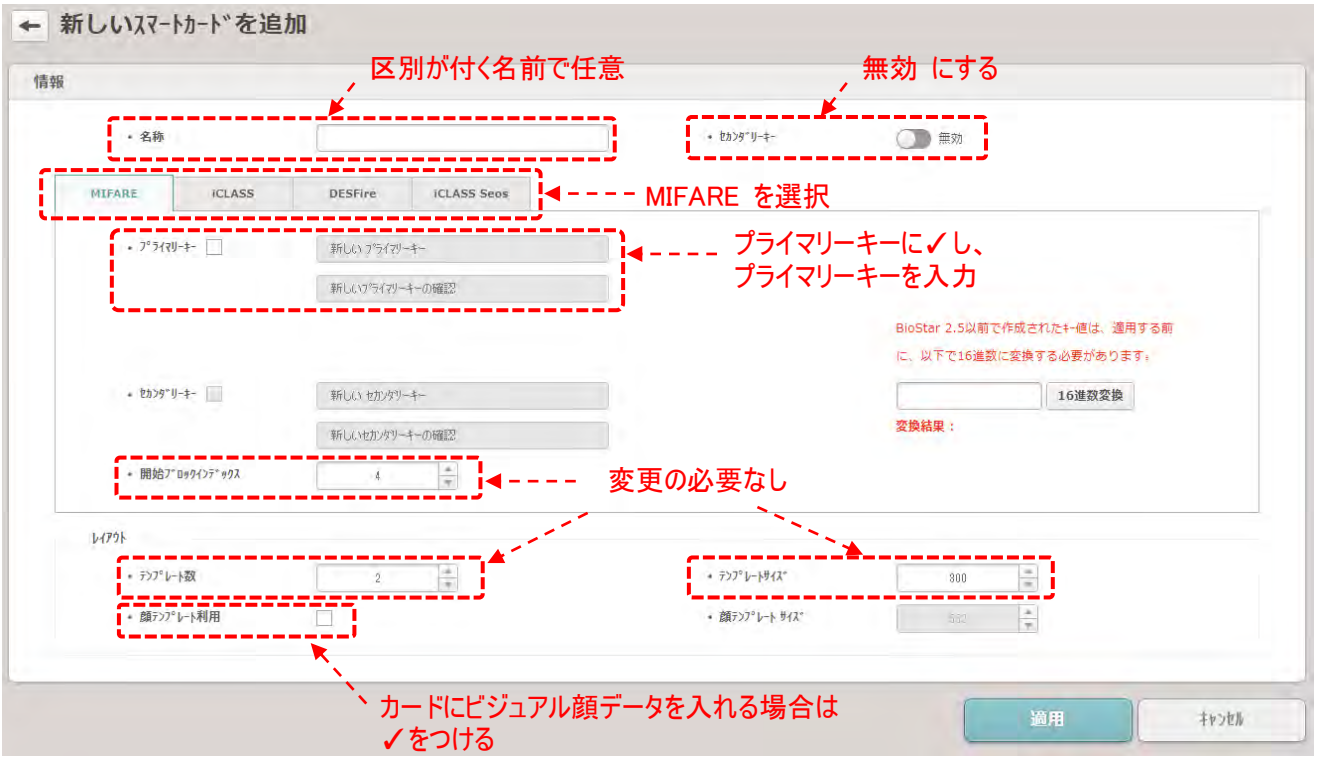
また、スマートカードは、カードのみとして利用することも可能ですが、カードに指紋情報や、ビジュアル顔情報を書き込み、「カード＋指紋」 や、「カード＋ビジュアル顔」として利用することも可能です。
この場合は、最初にカードをかざした際にカードから 指紋やビジュアル顔情報を認証機が読み出し、その後、指紋やビジュアル顔を入力することで、認証機内にユーザー情報を格納しておかなくても認証できるようにすることができます。

21.4.2.2 スマートカードフォーマット（カスタマイズ）

スマートカードフォーマットには、初期状態での標準フォーマットは存在しません。ご利用に合わせて、カスタマイズフォーマットを作成する形になります。

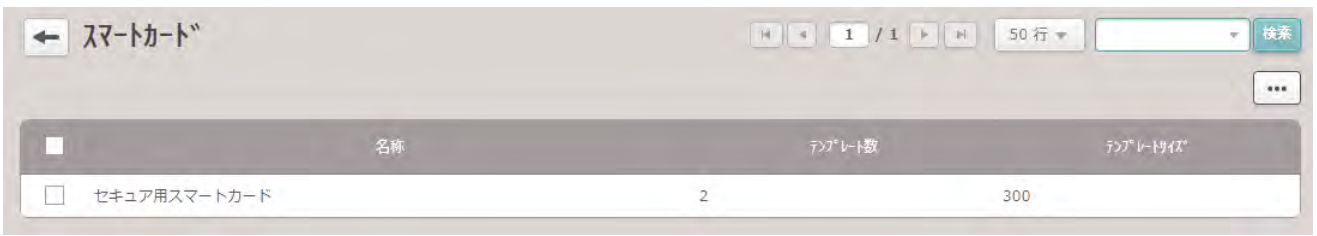
スマートカードを選択し、 スマートカードの追加 をクリックします。
ここでは、例として、MIFARE カードを利用したスマートカード フォーマットを作成します。
また、プライマリーキーを設定する例とします。
（セカンダリーキーは、書き込んだプライマリーキーを書き換える際に利用します。）
また、本例では、指紋をカードに登録できるフォーマットにすることを前提とします。





プライマリーキー および セカンダリーキーは、16 進数 6 バイト(12 文字) で入力します。
16 進数は、0～9 の数字 及び a～f までの文字となります。

設定後、 適用 をクリックすると、以下のようにフォーマットが作成されます。



21.5 サーバー 項目

サーバー設定では、BioStar2 サーバー側の設定を変更可能です。
各項目について、説明します。

【一般設定】項目

① BioStar2 サーバーとして動作する IP アドレスを設定します。サーバーPC が有線 LAN や、WiFi など、複数の IP アドレスを持つ場合に、BioStar サーバーが、どの IP アドレスで動作するかを指定します。「任意」を設定すると、動きが不安定になりかねないため、BioStar の端末とつながるネットワークコントローラーの IP アドレスを指定してください。

② BioStar サーバーの端末がアクセスしてくるポート番号を指定します。(初期値:51212)必要に応じ変更してください。

③ Web ブラウザから接続情報が残っている時間を指定します。上記の例の場合、60 分無操作後に、再度、操作しようとすると、一度、BioStar2 のログイン画面に戻り、再ログインを要求されます。最大 10080 分(7 日間)まで設定できます。

④ 端末から、BioStar サーバーへのログのアップデート方法を、手動/自動 で選択可能です。手動を選択した場合は、モニタリング画面のイベントログの画面に、端末からログをアップデートする操作を行うボタンが表示されます。

⑤ Web サーバーのプロトコルが、HTTP か、HTTPS かを選択可能です。HTTPS が初期値となっており、その場合は、設定の HTTPS 項目から、証明書をダウンロードし、保護された通信を行うことを推奨します。

【ユーザー/端末管理】項目

① 自動ユーザー同期は、利用しない/すべての端末/すべての端末（端末からのユーザー更新含む）/端末ごと（アクセス権限があるユーザーのみ） から選択できます。（初期値は、すべての端末 になっています。）

自動ユーザー同期の場合は、PC のユーザーデータの変更（追加・変更・削除）を行って、適用した際に、自動的に端末に送られます。利用しないを設定した場合は、PC 側のユーザー情報を変更しても、端末と同期しないため、追加・変更・削除の反映は、手動で実施する必要があります。すべての端末（端末からのユーザー更新含む）は、資格情報についてのみ更新されます。（ユーザー名称を変更した場合は、PC 側には反映されず、同期した時点で、PC のユーザー名が転送されます。） 端末ごと（アクセス権限があるユーザーのみ）を選択した場合は、該当の端末にアクセスコントロールで設定されていて許可がでるユーザーグループおよびユーザーが同期されます。

② モバイルカード（スマートフォン NFC や、BLE（Bluetooth Low Energy）をご利用の場合は、有効にしてください。）

但し、対象機種のみとなることと、BioStar サーバーがインターネット環境に接続でき、スマートフォンで BioStar2 モバイルアプリを利用することが前提となります。）

③ 基本的には、初期値、推奨の Suprema をご利用ください。

④ ユーザーID の管理方法を数字のみか、アルファベット等の文字を含むかを変更可能です。但し、アルファベットは、BioLite Net 等一部の機種では利用できません。ご利用の認証機がアルファベットの対象機種かをご確認ください。

⑤ 接続している端末リストから、登録用端末を選択することが可能です。登録用端末として登録しておくと、顔・指紋・カードの登録の際に、どの端末で登録するか？を選択しますが、その際に、一番上に登録用として表示され、リストから探すことが容易になります。

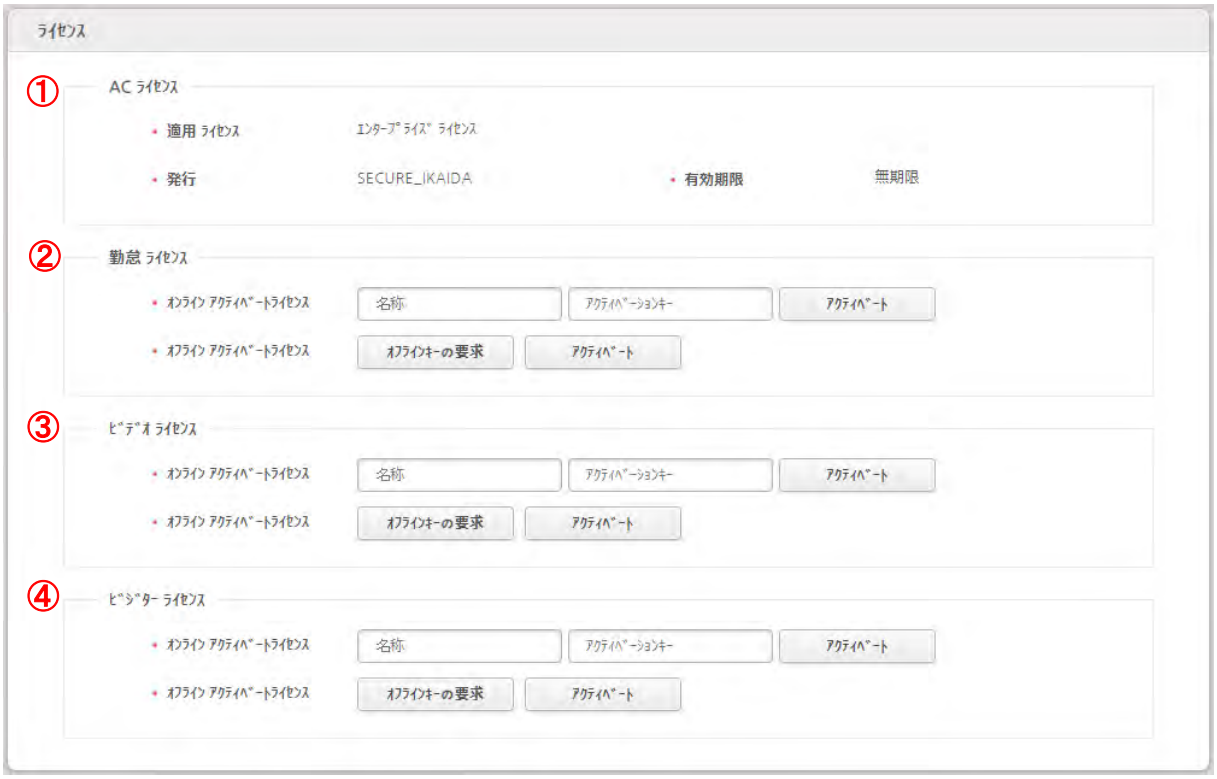
⑥ ユーザー単位で登録できる情報に、名前や、電話番号、E メールアドレスなどがありますが、カスタムユーザーフィールドを追加することで、登録できる情報を増やすことが可能です。項目数は、10 種類まで追加することが可能です。なお増やせるタイプは、テキストボックス、数字ボックス、コンボボックス の 3 種類です。コンボボックスの項目を設定する場合、”;(セミコロン)“で項目を区切り設定してください。

・社員番号と、出身地を増やした例

⑦ アクセスオンカードを発行する際に、その際の個人情報を発行時に削除するかどうか？を選択可能です。削除すると、アクセスオンカードを発行し、指紋情報などを移した時に、PC 側からは情報が削除されます。

⑧ アクセスコントロールのイベントログの削除期間を設定すると、PC にログがたまりすぎない設定にすることができます。但し、指定した日以前のログは削除されてしまい、確認できなくなりますので、ご注意ください。

【ライセンス】項目



① AC ライセンスは、アクセスコントロール関連の追加機能を利用とするライセンスです。ゾーン機能や、エレベーター機能、サーバーマッチング機能等の利用可否が変化します。また、BioStar2 で管理できるドアの数がラインセンスにより変化します。（上図は、アドバンスドライセンスが登録済みの例です。）

以下にライセンスの種類と機能差を記載します。

項目 ＼ ライセンス種別	Starter スターター	Basic ベーシック	Standard スタンダード	Advanced アドバンスド	Professional プロフェッショナル	Enterprise エンタープライズ
ユーザー数	制限なし					
端末数	1,000台					
ドア数（最大数）	5	20	50	100	300	1,000
ゾーン機能	－		利用可（100ゾーンまで）			
クラウド経由接続	－		利用可			
エレベーター	－			利用可		
グラフィックマップビュー	－			利用可		
サーバマッチング	－			利用可		

② 勤怠ライセンスは、以下の 2 種類となります。以下にライセンスの種類と機能差を記載します。

項目 ＼ ライセンス種別	Starter スターター	Standard スタンダード	Advanced アドバンスド	Professional プロフェッショナル
ユーザー数	100	500	1,000	制限なし
スケジュール数	制限なし			
対応シフト種別	固定/フレックス/フローティング			

ライセンスをご購入頂いた場合は、弊社から ライセンスキー（用紙）を納品させていただきます。登録する場合は、インターネットに接続している状態で、会社名とライセンス番号を入力し、「アクティベート」をクリックしていただくことで可能です。もし、インターネットに接続していない場合は、

「オフラインキーの要求」ボタンをクリックし、会社名とライセンス番号を入力し、「ダウンロード」をクリックしてください。ライセンスファイルをダウンロードすることが可能となります。そのライセンスファイルを、弊社担当者にメールで送付してください。メーカーに確認後、アクティベート用のファイルを返送させていただきます。その後、下段の「アクティベート」ボタンを押し、ファイル参照で、アクティベート用のファイルを登録すれば完了となります。

③ ビデオライセンスは、弊社では取り扱っておりません。

④ 訪問者ライセンスは、弊社では取り扱っておりません。

【サーバーマッチング】項目

サーバーマッチング機能とは、端末内にユーザーの認証データを持たない状態で、認証動作の後、サーバーにユーザー情報の確認を行い、そこで、認証を行います。BioStar2 サーバーとのネットワークが常時接続されていることが必要となりますが、端末内にユーザーデータを持たなくて良い。というメリットもあります。

① サーバーマッチング利用の場合は、有効にしてください。また、各端末側でも、サーバーマッチングの利用設定を行う必要があります。
ここだけを有効にしてもサーバーマッチング動作にはなりませんので、ご注意ください。

② サーバーマッチングの高速モードを利用する場合は、有効にしてください。但し、認証の精度が少し下がる可能性があります。

③ 同時にサーバーマッチングを行う数を設定してください。増やすと、サーバー側の負荷が増大する可能性があります。

④ 指紋のセキュリティレベルを設定してください。値を小さくすると誤認証（他人受入）は発生しづらくなりますが、本人拒否が発生する可能性が高くなります。

⑤ 顔のセキュリティレベルを設定してください。値を小さくすると誤認証（他人受入）は発生しづらくなりますが、本人拒否が発生する可能性が高くなります。
登録レベルと利用者数などに合わせ、設定してください。

【システムログレベル設定】項目

データベースに格納するシステムログの期間と、ログのレベルを設定できます。システムログの保存期間は、120 日まで設定でき、0 日にすると削除を行いません。システムログは、

システム / デバッグ / ネットワーク / Web / SQL / Web ソケット

の種類があり、それぞれのレベルとして、

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 及び 未使用

が選択できます。左のレベルを選ぶと、それより右のレベルがすべて含まれます。(未使用を選択するとその項目のログは取得しません。)

例えば、

「システム」の部分で、「インフォメーション」を選択すると、「システム」のログについては、インフォメーションとワーニングとエラーを記録します。

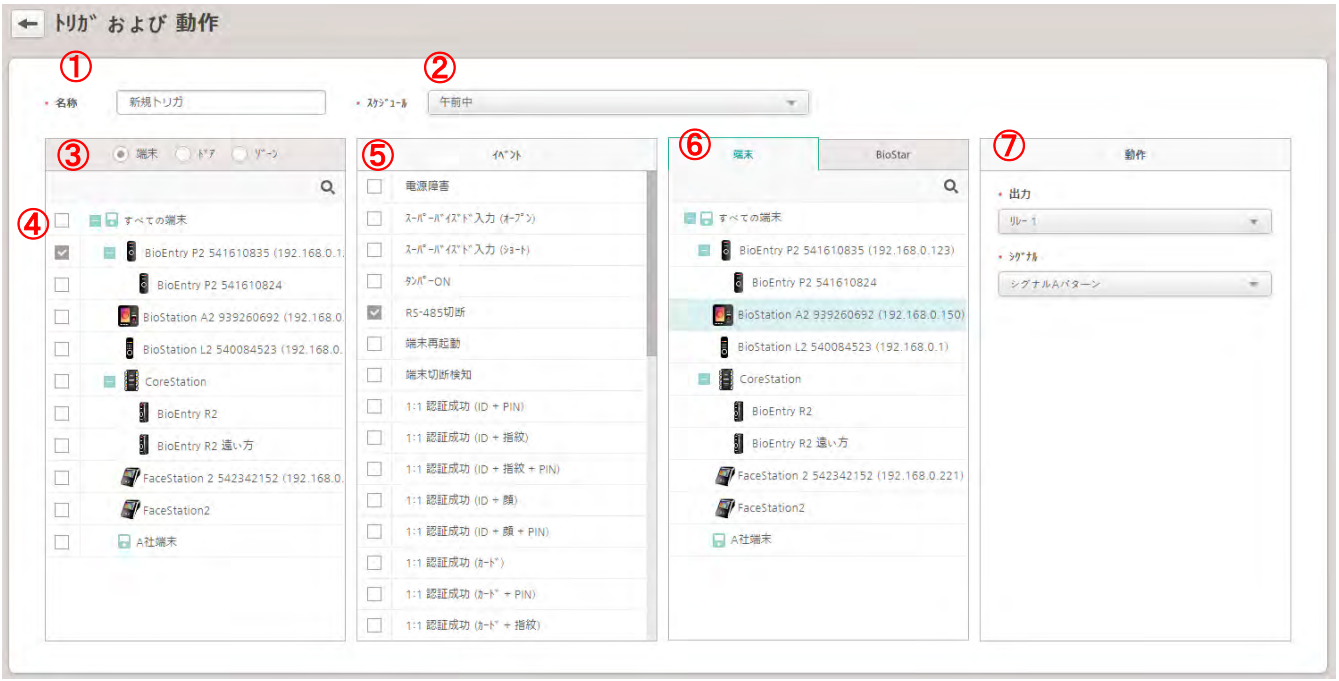
「ネットワーク」の部分で、「トレース」を選択すると、「ネットワーク」のログについては、トレースを含め全種類のログが記録されます。

① システムログの保存期間を指定します。(初期値:60) 0～120 で選択可能で、0 にすると削除しません。

② 項目ごとに、ログを記録するレベルを選択してください。

21.6 トリガおよび動作 項目

トリガおよび動作項目では、端末 か、ドア か、ゾーン で、各イベントが発生した場合に、接続されている端末 または、BioStar2 サーバーで、どのような動作を行うか？を設定することが可能です。また、その設定内容を、どのスケジュール（日時）で有効とするかを設定することが可能です。



① トリガの名称を入力します。

② このトリガが適用されるスケジュールを選択します。

③ トリガの発生元を 端末 / ドア / ゾーン から選択します。（ゾーンは、対象のライセンスが登録されていると表示されます。）

④ ③で選んだ種類の内容が表示されます。対象を選択してください。

⑤ ③で選んだ内容により、それぞれのイベントが表示されます。イベントを選択してください。

⑥ 動作させる内容を選択します。動作させる対象を 端末か BioStar から選択してください。

⑦ ⑥で「端末」を選択した場合は、リレー出力をすることが可能です。リレーポート番号と、出力パターンを指定してください。（出力パターンは、事前に作成したものから選択します。）

⑥で「BioStar」を選択した場合は、BioStar がメール送信サーバーとネットワークで接続されていれば、メールを送信することが可能です。メールサーバーの設定や、送付先の設定は、以下の画面のようになります。

メールサーバー設定画面

メール送信先 指定画面

21.7 スケジュール 項目

BioStar2 では、様々な設定項目に、「スケジュール」が出てきます。本項目では、スケジュールの作成・編集と、祝日の作成・編集が可能です。事前にスケジュールを作成しておくことで、様々な画面で利用することができます。
なお、BioStar2 システムは、初期値のスケジュールとして、「Always」と言う項目があります。このスケジュールは、削除・変更はできません。毎日、24 時間のスケジュールとなりますので、用途に応じご利用ください。
本書の例としては、2 つ目のスケジュールとして、「イベント実施スケジュール」というスケジュールを作成する例を記載します。

スケジュール画面に進み、画面左上の「スケジュールの追加」をクリックすると、スケジュールの作成画面になります。

① スケジュールの名称を入力します。

② スケジュールの説明を入力します。（空欄でも構いません）

③ 週/日 から選択します。 日を選択すると、1 サイクルの日数と、開始日を選択可能です。

④ 各曜日 または、X 日目のスケジュールを作成します。

アイコンは、上の行と同じ設定値で良い時にクリックすると、上の行をコピーします。

アイコン 及び、グラフ部分のクリックは、その曜日の対象時間の編集モード画面に遷移します。

アイコンは、その曜日または X 日目のデータを削除します。

⑤ 更に、上記のスケジュールに祝日のスケジュールを追加する場合は、祝日スケジュール の項目に☑を入れ、祝日を選択することができます。
☑を入れると ⑥部分が表示されます。

⑥ 祝日を選択してください。（祝日を事前に作成しておく必要があります。）

上図の様に、スケジュールを作成します。

また、前ページの例の祝日部分で利用していますが、事前に、「三賀日」という祝日を作成しました。
スケジュール画面に進み、画面左上の「祝日の追加」をクリックすると、祝日の作成画面になります。

① 祝日の名称を入力します。

② 祝日の説明を入力します。（空欄でも構いません）

③ 祝日に登録する日を選択します。カレンダーマークをクリックするとカレンダーが表示されますので、そこから入力してください。
また、繰り返しとして、毎年なのか、1 年限定なのかを選択できます。
不要な場合は、ゴミ箱アイコンで、追加する場合は、「＋追加」から行ってください。

これで、祝日を作成することが可能です。

21.8 警告 項目

警告項目は、様々なイベントが発生する中で、警告対象として画面にポップアップしたり、ログ上で色を変化させたり強調したり、音声を再生するために設定します。

以下の画面で、各警告項目を設定します。

① チェックボックスは、そのイベント内容を、警告としてポップアップの対象とするかどうかを設定します。☑をしたものは、ポップアップの対象となります。

② ポップアップの表示や音声の変更有無がわかります。

①に☑が入っている場合は、標準の警告画面が表示されます。

①に☑が入っている場合は、カスタマイズした警告画面が表示されます。

①に☑が入っている場合は、指定した音声が再生されます。

これらの設定は、 部分をクリックすると変更可能です。

初期値

変更後

なお、音声ファイルと再生オプションの部分は、21.2 章の効果音の部分に追加した内容から選択可能です。

21.9 HTTPS 項目

21.5 章の⑥項目で、Web サーバープロトコルが HTTPS に設定されている場合は、本項目が表示されます。

「証明書ダウンロード」ボタンをクリックすることで、サーバー証明書がダウンロードされます。このサーバー証明書を正しくインストールすることで、BioStar2 サーバーがサーバー認証の対象として登録されます。
これにより、BioStar2 サーバーと Web ブラウザ間で保護された通信が実現します。

21.10 クラウド 項目

クラウド経由アクセスを利用すると、インターネット経由でも BioStar2 にアクセスすることが可能になります。本設定を利用するためには、以下の内容を満たす必要があります。

・BioStar2 サーバーが、インターネットに常時接続されていること
・21.16 章 ログインパスワードの パスワードレベル が、「中」以上に設定されていること
・サブドメイン名が、既に利用されていないこと

① クラウド経由アクセスをする場合は、有効にしてください。適用するためには、②③を入力する必要があります。
② クラウド経由の際のサブドメイン名を入力してください。(他の方の利用と重複しない必要があります。)
③ 適用後、管理者の認証を要求するメールが届きます。そのためのメールアドレスを指定してください。
④ 基本的には変更しないでください。特別に別のクラウド経由サーバーにアクセスさせる場合に変更することもできます。

注意事項:

・DDNS 経由のアクセスとなるため、メーカーの DDNS サーバーが、メンテナンスやトラブルで停止している場合は、アクセスできない場合があります。
・Suprema 社からのサービス確認応答に、7 日間以上 サーバーPC が応答できない場合は、再認証しないとクラウド経由アクセスができなくなります。
・管理者 E メール宛で届くメールの URL にアクセスし、認証する必要があります。
・BioStar2 がクラウドで動作するわけではありません。クラウドを経由して BioStar2 にアクセスすることが可能となります。

21.11　イメージログ 項目

カメラを内蔵している機種に対して、各種イベント発生時に写真を記録することが可能です。その際に、どのイベントで、どのスケジュールで写真を撮影するかを指定することが可能です。（本設定は、サーバー側として設定するもので、標準とする設定を行います。

実際には、各端末で、この標準に追加・削除を行い、撮影する内容を決定します。

（23.2 章のイメージログ部分を参照ください。）

【プリセット】項目

① 撮影をするイベントと、スケジュールを指定してください。追加する場合は、「＋追加」ボタンを。削除する場合は、項目のゴミ箱アイコンをクリックしてください。

【削除オプション】項目

① イメージログが多くなった場合に、自動的に削除する設定にすることが可能です。削除しない場合は、「未設定」を選択してください。
削除する場合は、MB / GB / 日 / 週 / 月 から、削除条件を選択してください。

② ①で指定した項目の削除条件を入力してください。単位は、①の設定内容により変化します。

③ どのタイミングで削除するかを選択できます。アップロードごと / 日ごと / 週ごと / 月ごと から選択できます。

【保存先パス設定】

イメージログの保存パスをサーバーPC 側で保存可能です。

【ユーザープロファイルイメージオプション】項目

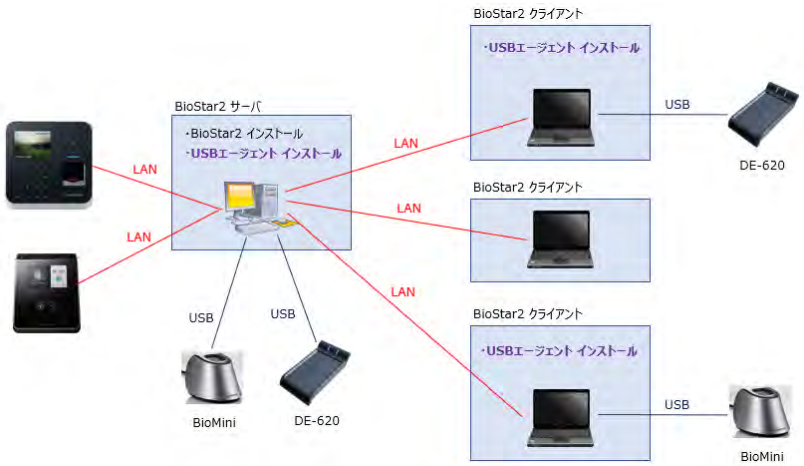
☑を入れた場合は、ログに対し、写真がない場合はユーザープロファイルの画像を表示します。

入力例「.¥imagelog¥」 表示は「 .₩imagelog₩ 」となります。

21.12 USB エージェント 項目

USB デバイスエージェントは、卓上指紋登録機（BioMini） および 卓上カード登録機（DE-620 または、パソリ RC-S380 および RC-S300）を利用する場合のドライバ 及び アプリケーションになります。上記装置を接続する PC に、事前にインストールする必要があります。

なお、パソリをご利用の場合は、更に、NFC ポートソフトウェアを事前にインストールしておく必要があります。



上図の様に、USB 機器を直接接続するパソコンには、USB エージェントをインストールする必要があります。
このため、そのソフトウェア（インストーラー）を、以下の画面よりダウンロードしインストールしてご利用ください。

① クリックすると、USB エージェントのインストーラ（USB Device Agent Setup.exe）がダウンロードされます。インストール時は、管理者でログインしてインストールを行ってください。

② DE-620 および、パソリで、カードを読み込ませた時のバイトの横込み順を指定します。通常は、MSB でご利用ください。

③ USB エージェントが動作するポート番号を指定してください。（初期値は 8081 です）

21.13 顔のグループマッチング 項目

顔のグループマッチングは、顔認証装置をご利用の場合は、グループを絞ることで、認証をしやすくすることと、1:N 認証の場合に、登録可能な顔の数を、3,000 から、5,000 に増やすことが可能です。

但し、1:N 認証の場合、通常であれば、接近すると顔認証モードになり、そのまま認証できますが、本機能を利用する場合は、近づくと、グループの選択画面が表示され、グループ選択後に、顔認証モードとなり、その後、認証することになります。

画面上で、自分の所属するグループを 1 タッチする動作が必要となります。

① 顔のグループマッチング機能の、使用 / 未使用 を選択してください。

② グループマッチングを行なえる端末は FaceStation 2 のみです。追加する場合は、「＋追加」をクリックし追加してください。
削除する場合は、端末の横のゴミ箱アイコンをクリックしてください。

③ マッチンググループを選択します。グループ名は、端末の選択画面に表示される名称です。
ユーザーグループは、BioStar のユーザーグループから該当のユーザーグループを選択してください。
最大 10 個のグループを作成できます。ユーザーグループに含まれる顔が 3，000 件を超える場合は、マッチンググループに設定できません。
そのグループ内の顔の数が表示されます。登録を削除する場合は右側のゴミ箱アイコンをクリックして削除してください。

21.14 監査記録 項目

監査記録については、設定はないため 19 章の運用編をご参照ください。

21.15 サマータイム 項目

国内では、サマータイム制度がないため、ここでは説明を省略させていただきます。

21.16 セキュリティ 項目

セキュリティ項目では、ログイン情報、端末の暗号化通信に関する設定を変更することが可能です。

① ログインパスワードのレベルを選択します。パスワード設定の最低条件が変わります。

② パスワードの有効期限を「有効」に設定することで、日単位の設定ができます。

③ ログインの試行回数を「有効」に設定することで、指定時間の間に、何回までログインの試行が許されるかを設定できます。

④ パスワードの変更回数を「有効」に設定することで、1 日あたりの最大変更回数を設定できます。

BioStar 2 と端末間の通信は、証明書を使用して保護することができます。端末の暗号化通信を「使用」に設定されている場合、BioStar 2 は証明書を作成し端末に送信します。端末は、この証明書を使用して BioStar 2 とデータ交換をするため安全な通信路を使用することができます。 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。

サーバー及び端末の暗号化キーの手動管理を「使用」に設定すると、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。

注意事項：端末との通信暗号化を設定した場合は、端末の通信が途切れている時に設定を戻さないようにしてください。

端末との通信ができていない時に、BioStar2 側だけ設定を変更すると、端末とは接続できなくなります。

この場合は、端末を一度、工場出荷時リセットしてください。

【工場出荷時のリセット方法】

・リセットボタンを長押し、「ピロリン」と鳴ったら離し、その後リセットボタンをすばやく3回押す。しばらくすると、「ピロリン」とリセット音が鳴り、リセットが完了する。

⑤ サーバー上の個人データを暗号化する場合は、「使用」に設定してください。（初期値は、未使用です。）「使用」にすると、⑥が表示されます。資格情報データや個人情報を含むすべての機密データが暗号化されてデータベースに格納されます。

⑥ 個人データの暗号化キーを設定します。「変更」 をクリックし、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。

⑦ 端末と BioStar2 間の通信を暗号化する場合は、「使用」に設定してください。(初期値は、未使用です。)「使用」にすると、⑧⑭が表示されます。

⑧ BioStar2 標準以外の外部の証明書を利用する場合は、「使用」にしてください。(初期値は、未使用です。)「使用」にすると、⑨～⑬が表示されます。

⑨ 外部証明書のルート証明書ファイルを「アップロード」ボタンをクリックして、選択してください。

⑩ 外部証明書の公開鍵証明書ファイルを「アップロード」ボタンをクリックして、選択してください。

⑪ 外部証明書の秘密鍵ファイルを「アップロード」ボタンをクリックして、選択してください。

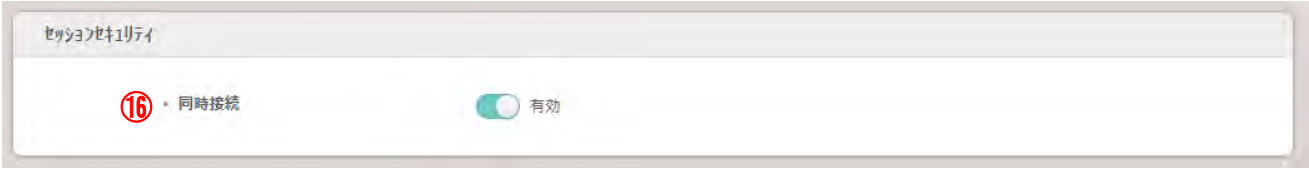
⑫ 外部証明書の秘密鍵パスフレーズを入力してください。

⑬ ⑫の確認入力です。⑫と同内容を入力してください。

⑭ 暗号化キーを手動管理する場合は、「使用」を選択してください。⑮が表示されます。

⑮ 手動管理の場合の暗号化キーを設定してください。「変更」ボタンを押すと、以下の画面を表示します。

データ暗号化キーと管理者パスワードを、それぞれ、2 回ずつ入力して、OK をクリックしてください。



⑯ 同じ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した場合、同じアカウントで同時に接続しようとすると、以前にログインしていたユーザーがログアウトされます。

21.17 アクティブ ディレクトリ 項目

アクティブディレクトリ項目を設定する場合は、ユーザーID の管理を数字ではなく、アルファベットも許可する必要があります。

21.5 章の【ユーザー/端末 管理】項目で、ユーザーID 種別を アルファベット に設定する必要があります。

また、現時点で、弊社では本機能はサポートしておりません。ご利用においては、お客様責任でお願いいたします。

このため、本章では、説明は省略させていただきます。

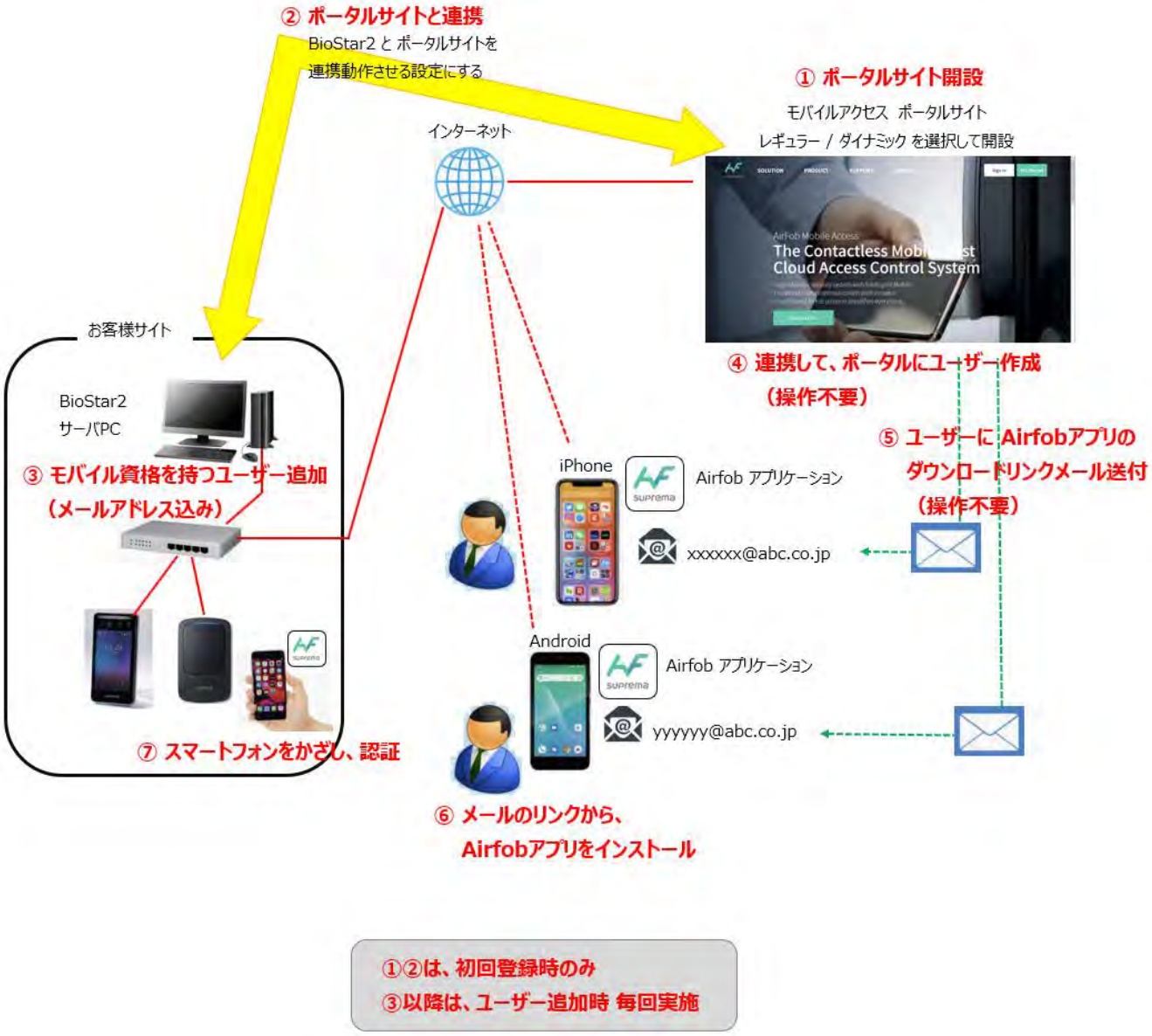
21.18 モバイル 項目

21.18.1 モバイルカードについて

21.18.1.1 モバイルカードとは

モバイルカードとは、IC カードの代わりに、スマートフォンとスマートフォンアプリを利用し、認証する方法です。
認証機に対し、スマートフォン（iPhone(BLE) および Android(BLE/NFC)）を、かざすことで認証することができるようにする機能です。
※iPhone の場合は、BLE(Bluetooth Low Energy)のみとなります。
Android の場合は、BLE 及び、NFC(搭載機種 且つ HCE 仕様)が利用可能です。

21.18.1.2 モバイルカードを利用するためのシステム構成 および 流れ



21.18.1.3 モバイルカードを利用するために必要なライセンス(クレジット)

モバイルカードを利用するためには、利用に応じてライセンス(クレジット)が必要になります。
このライセンスは、BioStar2 のライセンス(21.5 章)とは異なり、モバイルカードの利用に合わせて必要なライセンスとなります。
以下、このライセンスのことを、クレジットと表記します。
なお、クレジットには、2 種類のタイプがあり、クレジット と メンテナンスクレジット が、あります。
メンテナンスクレジットは、後述の レギュラータイプのサイトでのみ ご利用いただけます。
クレジットについては、必要数を弊社よりご購入ください。

21.18.1.4 モバイルアクセス ポータルサイトの種類

モバイルアクセス ポータルサイトは、サイト開設は無料です。
また、サイト開設時に、レギュラー または ダイナミック のいずれかのタイプを選択して頂く形になります。

なお、サイト作成時のログインアカウント(メールアドレス)、パスワードは、お忘れにならないようお願いいたします。
クレジットのアクティベートや、機器のメンテナンス時にログインする必要がございます。

サイトのタイプの詳細については、下記の表をご参照ください。

サイトのタイプ / 項目	レギュラー	ダイナミック
クレジットの消費条件	[新規のスマートフォンとして扱う場合] スマートフォン 1 台に対して、 1 クレジットを消費 [スマートフォンの機種変更など 既存ユーザーの更新] 更新 1 回に対し、1 メンテナンスクレジットを消費	認証機 1 台につき、1 ヶ月で 1 クレジットを消費
認証機台数とクレジットの関係	関係なし	毎月認証機台数分のクレジット消費
スマートフォン台数とクレジットの関係	利用者追加時に、スマートフォン台数分のクレジット消費	関係なし
クレジットの種類	クレジット/メンテナンスクレジット	クレジット
特徴	スマートフォンの新規追加や、変更がなければ、初回の人数分のクレジットのみで永年利用可能 (スマートフォン台数とクレジット数が比例、認証機台数は関係なし)	毎月、認証機台数に比例し、クレジットは消費するが、スマートフォン台数は制限なし

21.18.1.5 クレジット と メンテナンスクレジットの違い

クレジットについては、21.18.1.3 章で概要は説明しましたが、本章では、
・クレジット
・メンテナンスクレジット
の違いについて記載します。

クレジットについては、ポータルサイトが レギュラー か ダイナミック か のタイプによって、消費のされ方が異なります。
[レギュラーの場合]
・スマートフォンの台数 1 台 に対し、1 クレジット消費
・認証機の台数には関係しない

[ダイナミックの場合]
・スマートフォンの台数には関係しない
・認証機の台数 1 台 に対し、1 ヶ月で、1 クレジット消費

となります。

メンテナンスクレジットについては、ポータルサイトが レギュラー の場合にのみ利用可能です。

・登録済みの 1 台のスマートフォンについて、情報の変更が可能です。
つまり、新たに 1 台のスマートフォンの利用を追加することはできません。
機種変更など、1 台のスマートフォンの情報を変更するために 1 メンテナンスクレジットを利用します。

レギュラー サイトの場合、以下のようになります。
・**クレジット** を使えば、**利用できるスマートフォンを 1 台追加することができる**（上限台数が 1 増える）
・**メンテナンスクレジット** を使えば、**利用できるスマートフォンの上限数は変わらない**が、不要なスマートフォンを登録解除する代わりに、新たにスマートフォンを登録できる

21.18.1.6 モバイルカードを利用する際の注意事項

モバイルカードを利用する際には、以下の点にご注意ください。

・BioStar2 サーバーPC が、常時インターネットに接続されている必要があります。
個人情報を含んだ PC の外部接続となりますので、セキュリティ対策等のご注意をお願い致します。

・BioStar2 で登録した個人情報は、自動的にメーカーの管理するモバイルアクセス ポータルサイトに登録されます。
モバイルカードをご利用の場合は、この旨、ご理解のほどをお願い致します。

・モバイルアクセス ポータルサイトは、メーカー（Suprema）の管理となります。このため、メンテナンス等で、一時的にアクセスできなくなる。などの可能性が考えられます。このような場合があることをご承知おきください。

・モバイルカードを利用される場合は、各ユーザーのスマートフォンに専用のアプリケーション（Airfob アプリ）をインストールする必要があります。

・すべてのスマートフォンで、動作を保証するものではございません。

・ご購入いただきましたクレジットは、ご返金できません。

・弊社より、クレジットをご購入頂いた場合は、ライセンスコードを発行させていただきます。
お客様側で、モバイルアクセス ポータルサイトにログインし、ライセンスコードをアクティベートしてご利用ください。

・操作のミスにより（例えば、CSV インポートですべてのユーザーに再発行してしまう等）、誤ってクレジットを利用してしまった場合に関しましても、利用してしまったクレジットについては、保証できません。

・作成されたモバイルアクセス ポータルサイトの管理は、お客様にて行っていただきます。
弊社では、管理をお受け致しません。
（認証機故障などによる交換の際には、モバイルアクセス ポータルサイトへのログインが必要となります。
この際に、ログインできないと、作業が進まなくなりますので、事前にログイン確認をお願い致します。）

・iPhone（BLE）/Android(BLE)をご利用の場合、普段より、他の接続のため Bluetooth 電源を ON にされている方は、影響は少ないと思いますが、普段、Bluetooth を OFF にしてご利用されている方は、スマートフォンのバッテリーの消費が激しくなります。その旨、ご理解ください。

・モバイルアクセス ポータルサイトは、英語表記となります。日本語表記はありませんので、ご承知おきください。

・モバイルアクセス ポータルサイトは、BioStar2 のアクセスと取り合いになります。ポータルサイトの画面を操作する際は、BioStar2 の画面を閉じておいてください。（そうしないと、ポータルサイトが突然ログアウトさせられます）

21.18.2 モバイルアクセス ポータルサイトの開設

21.18.2.1 モバイルアクセス ポータルサイトの開設に必要なもの

モバイルアクセス ポータルサイトの開設には、以下のもの/状態が必要となります。

[事前準備が必要な内容]
・モバイルアクセス ポータルサイトにアクセス可能な PC
・メール受信を確認できるメールアドレス(後に、管理者メールアドレスとなります。)

[開設時に決めないと行けない内容]
・ログイン パスワード
・サイトの種類(レギュラー / ダイナミック)

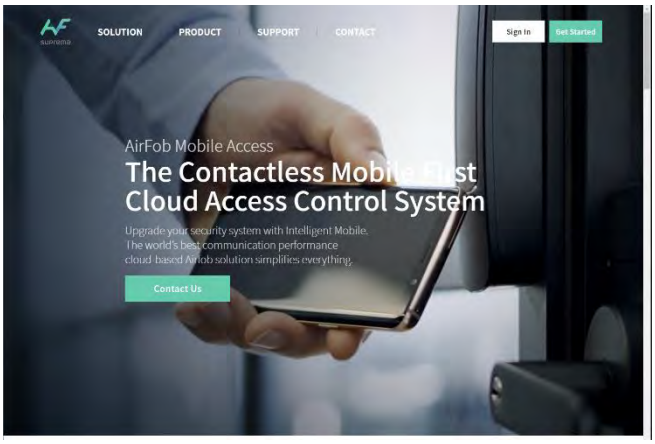
21.18.2.2 モバイルアクセス ポータルサイトの利用タイミング

モバイルアクセス ポータルサイトは、基本的には、初回に作成し、BioStar2 とリンクさせると、普段はログインされる必要はございません。以下の作業時のみ、ログインが必要となります。
・残りクレジット数の確認
・クレジットを追加でご購入いただき、そのライセンスコードを適用する場合
・認証機故障などのメンテナンスの場合(基本的には、弊社担当者が操作)
・その他、設定内容等を変更されたい場合

21.18.2.3 モバイルアクセス ポータルサイトの開設

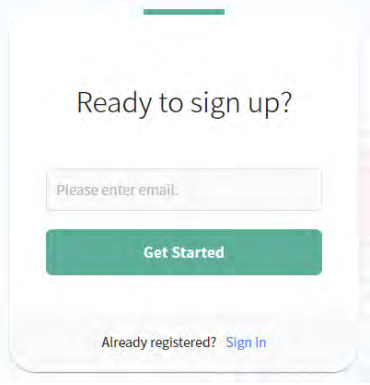
モバイルアクセス ポータルサイト(以下 ポータルサイト)開設の為、下記の URL にアクセスします。
(WEB ブラウザのお気に入り 等に登録しておくことを推奨します。)
https://mc.mocainc.com/en

ポータルサイトのトップ画面が表示されます。(2021/10 時点のデザイン : デザインは変更される場合があります。)

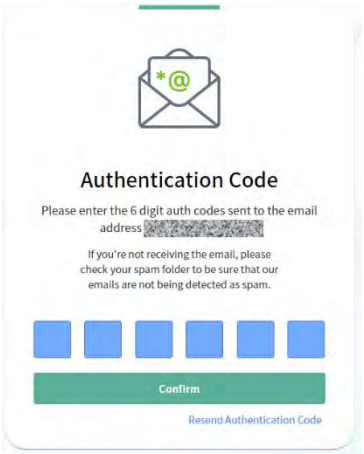


初回は、新規登録となりますので、右上の Get Started をクリックしてください。

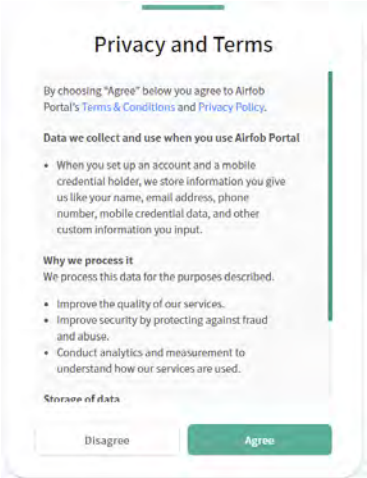
以下の画面が表示されます。



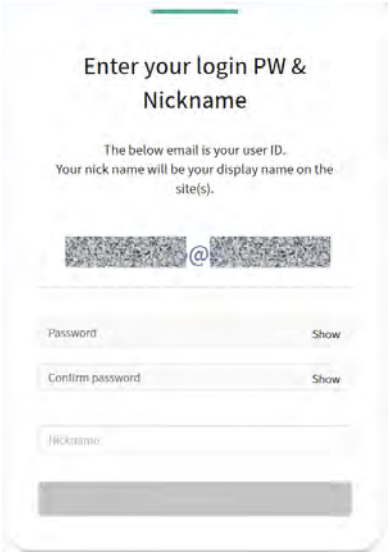
メールアドレスを入力し、Get Started をクリックします。



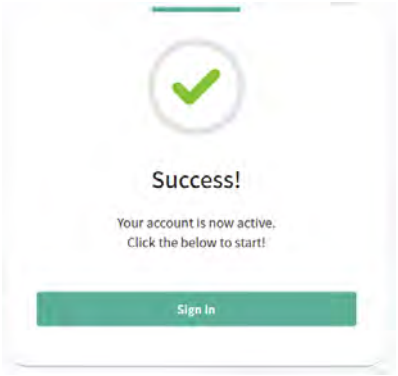
上の画面で入力したメールアドレスに、AIRFOB からメールが届きます。
メール内の 6 桁の Verification Code を入力し、
Confirm をクリックします。



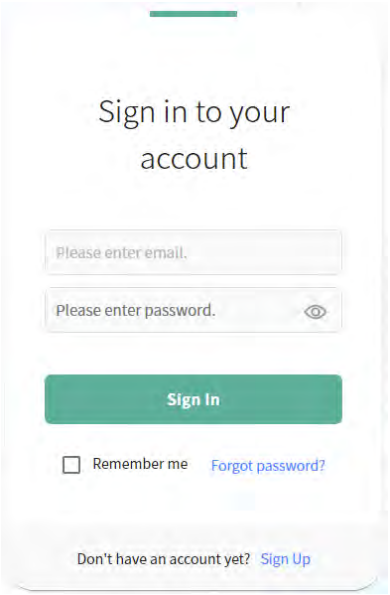
プライバシーと条件の条項をご確認いただき、同意される場合は、
Agree をクリックして、進んでください。
同意できない場合は、ブラウザを閉じて終了してください。



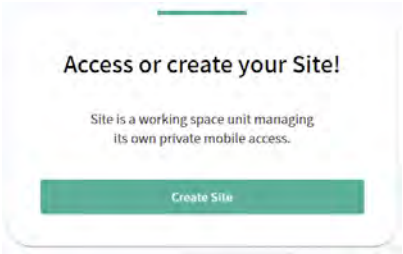
ログインパスワードの設定と、ニックネームの設定画面が表示されます。
ログインパスワードを確認も含め、2 回入力します。
数字を含めて 8～64 文字の範囲のパスワード入力が必要です。
入力が完了したら、 Create Account をクリックします。



サイトの作成に成功しました。
次にサインインするために、 Sign In をクリックします。

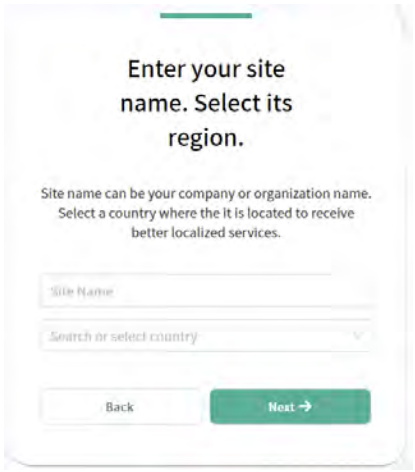


ログイン画面が表示されます。
メールアドレスとパスワードを入力し、 Sign In をクリックします。



ログインすると、ポータルサイトの作成画面になります。

をクリックします。

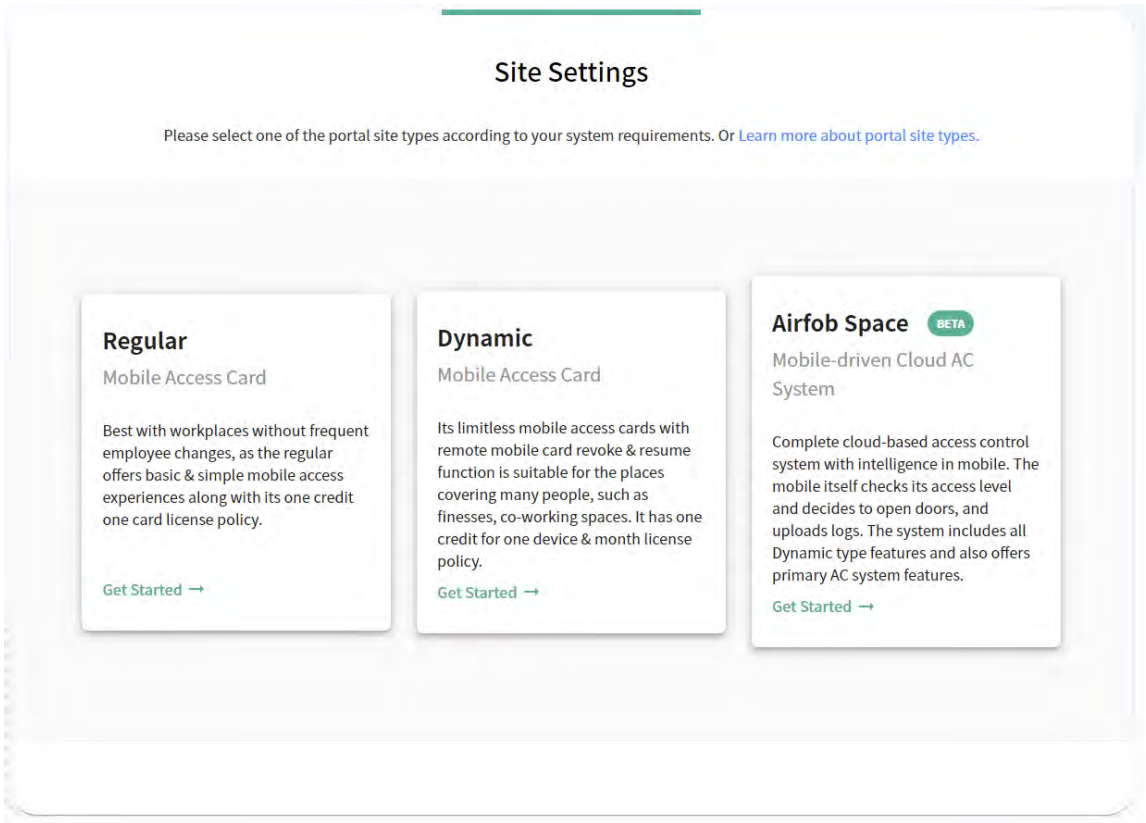


サイト名（会社名）を入力し、国を選択します。例として以下のようにします。

完了したら、

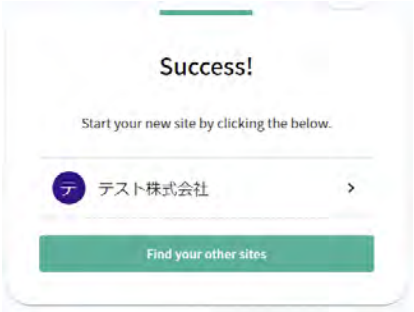
をクリックします。

次に、サイトの種類を レジューラー / ダイナミック から選択します。



レギュラー / ダイナミックの いずれかの Get Started → を クリックします。

（※ 一番右の Airfob Space は、専用のプログラムが必要で、弊社ではサポートしていません。）



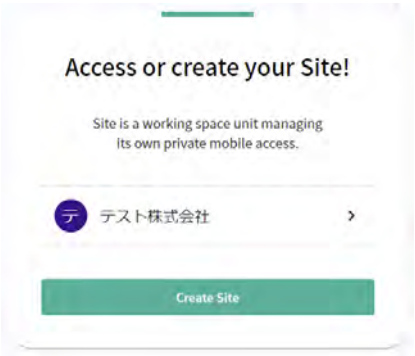
これで、ポータルサイトの開設が完了しました。

21.18.3 モバイルアクセス ポータルサイトとの連携

モバイルアクセス ポータルサイトが開設できたら、次は、BioStar2 と、モバイルアクセスポータルサイトを連携します。
まずは、モバイルアクセスポータルサイトにログインします。
初回にポータルサイトを作成時にアクセスした以下の URL に、再度アクセスします。

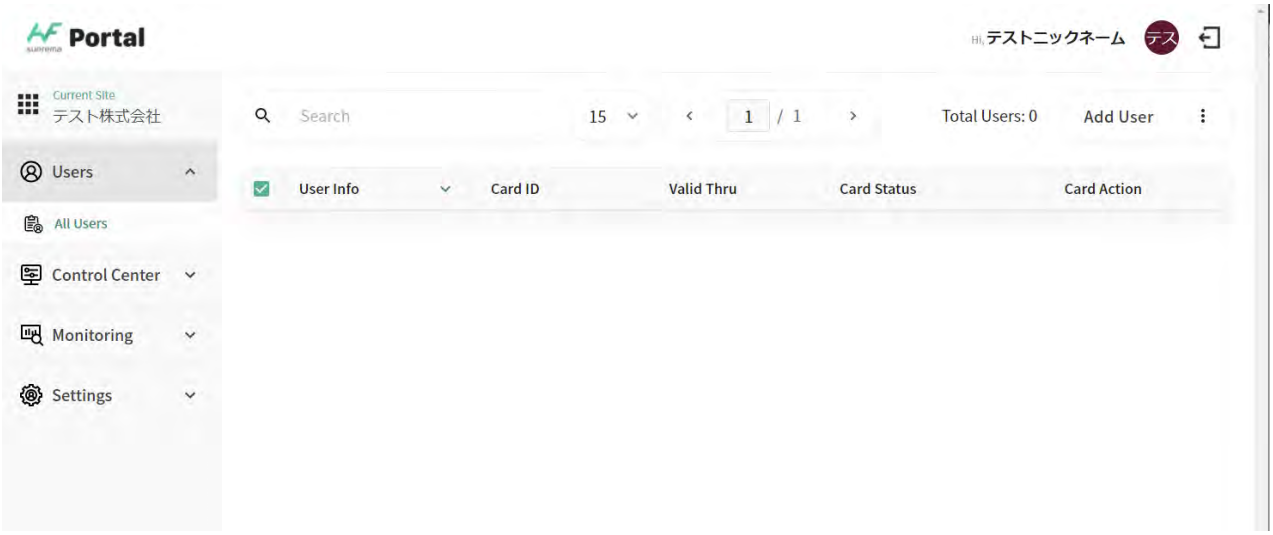
https://mc.mocainc.com/en

アクセスしたら、 Sign In をクリックし、ユーザー名/パスワードを入力し、ログインします。

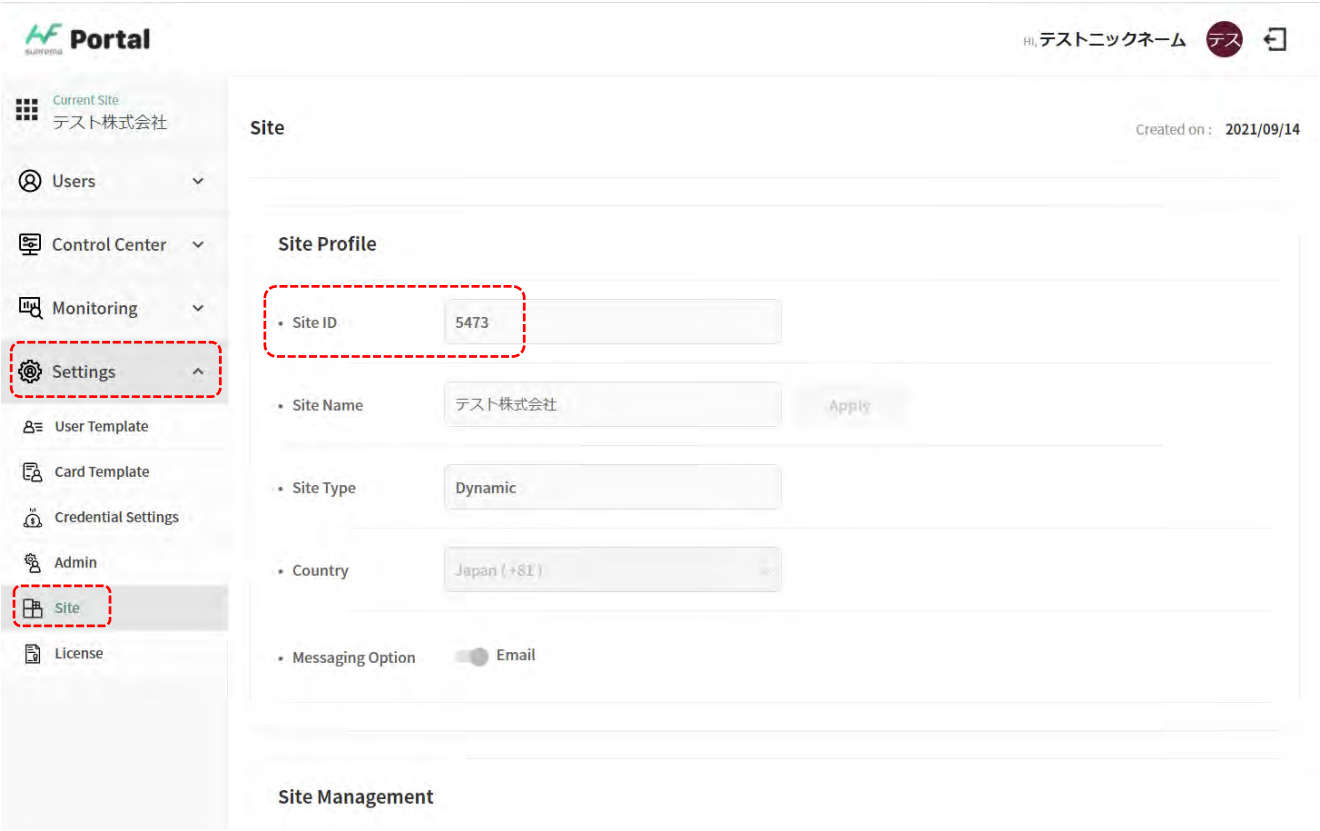


ログインすると、この画面になります。左図のポータルサイト名をクリックします。

以下の画面となります。(ダイナミック タイプの例です。レギュラーの方が表示される項目が少なくなります。)



画面左側のメニューで、[Settings] → [Site] をクリックします。

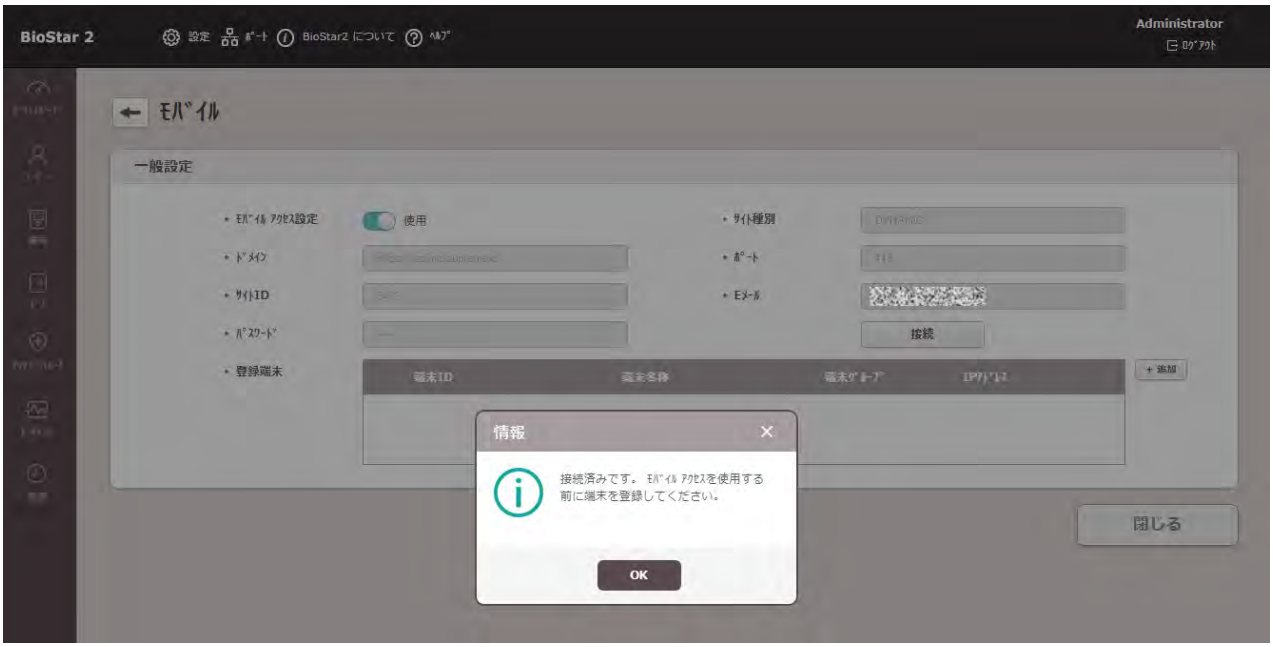


上記画面で、サイト ID を確認してください。
（上記の例の場合は、 Site ID が 5473 であることがわかります。）
サイト ID を確認したら、ポータルサイトの画面は閉じていただいて構いません。

次に、BioStar2 にログインし、[設定]→[モバイル]と進んでください。

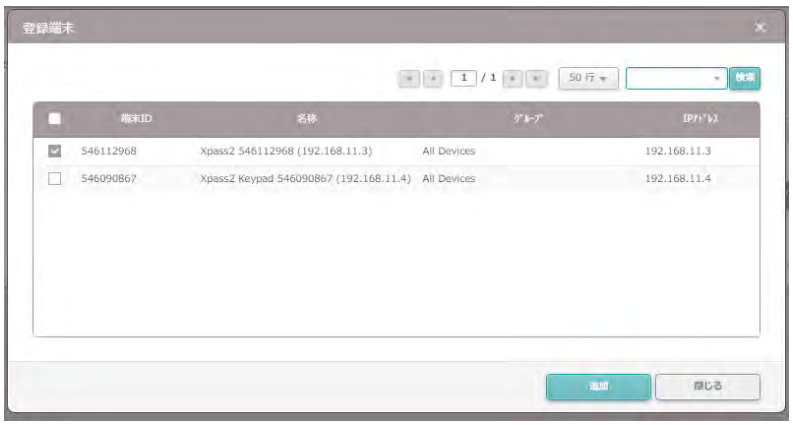
モバイルアクセス設定を「使用」に変更し、以下の内容を設定します。
・サイト ID　　：ポータルサイトで確認したサイト ID を入力します。
・E メール　　：ポータルサイトのログインアカウントの E メールアドレスを入力します。
・パスワード　　：ポータルサイトのログインのパスワードを入力します。
そして、入力したら、 接続 をクリックしてください。

正しく接続できると、以下の画面が表示されます。



事前に、BioStar2 にモバイルで利用する認証機を登録してください。（端末登録の方法は、23.1 章を参照してください。）

BioStar2 に認証機の登録が完了していたら、 + 追加 をクリックし、認証機の一覧から、モバイルアクセスに利用する認証機にチェックをつけて、 追加 をクリックしてください。



ここまでで、BioStar2 とポータルサイトの連携は完了です。

21.18.4 モバイルアクセス ポータルサイトとの利用方法

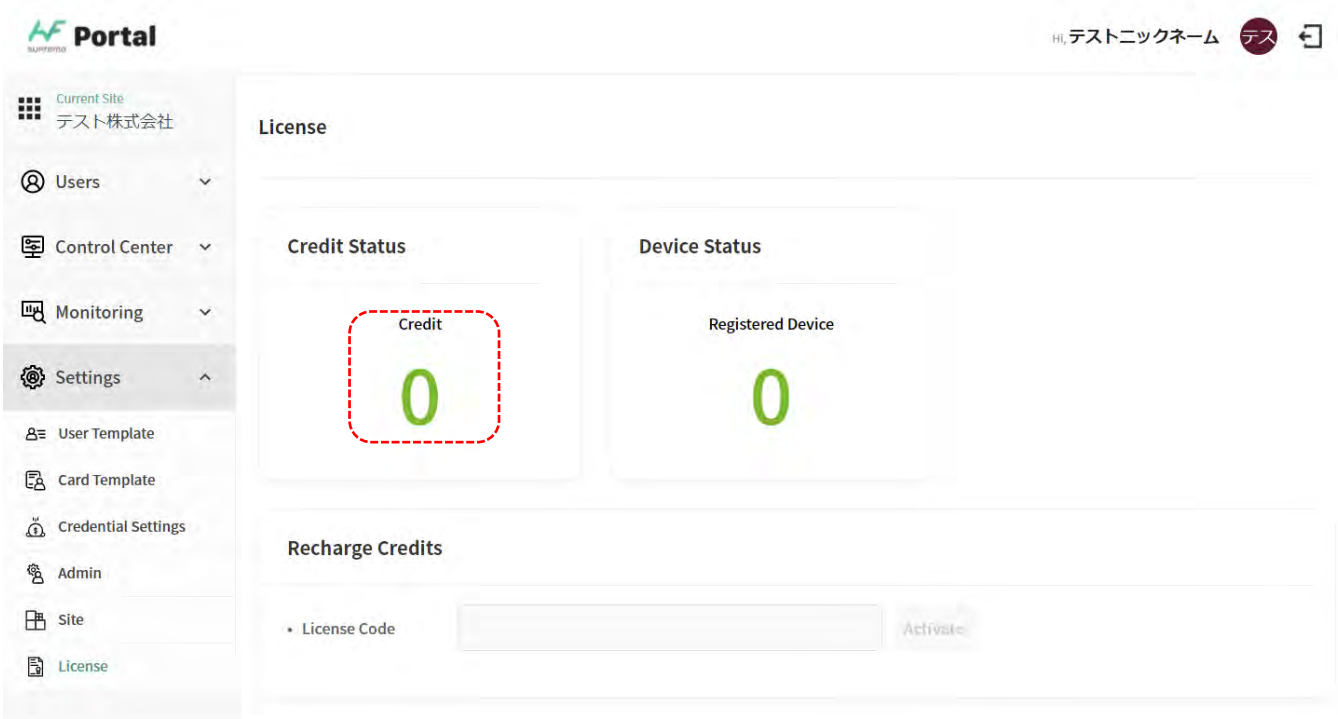
モバイルアクセス ポータルサイトは、21.18.2.2 章で説明させていただいたように、BioStar2 と連携させると、
直接ログインして利用する機会は、多くありません。

クレジット数の確認や、クレジットご購入後の適用時に、ログインしご利用ください。
また、クレジット数の確認や適用以外のご確認事項は弊社までお問い合わせください。

21.18.4.1 クレジット数の確認

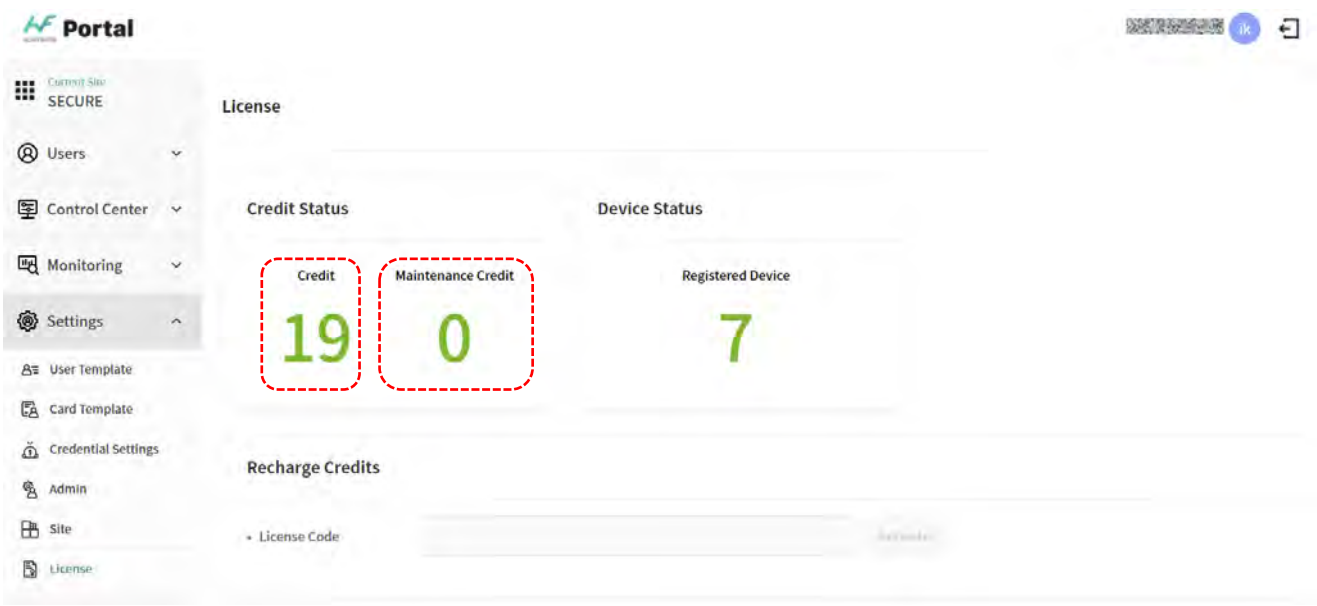
ポータルサイトにログインし、[Settings] → [License] と進んでください。
※ポータルサイトの種類により、表示内容が異なるため、それぞれの画面で説明します。

[ダイナミック サイト]



上記の例の場合、ダイナミック サイトなので、クレジットの数だけとなります。
クレジット数の残りが 0 であることがわかります。
(サイト開設時は、0 からスタートします。)

[レギュラー サイト]



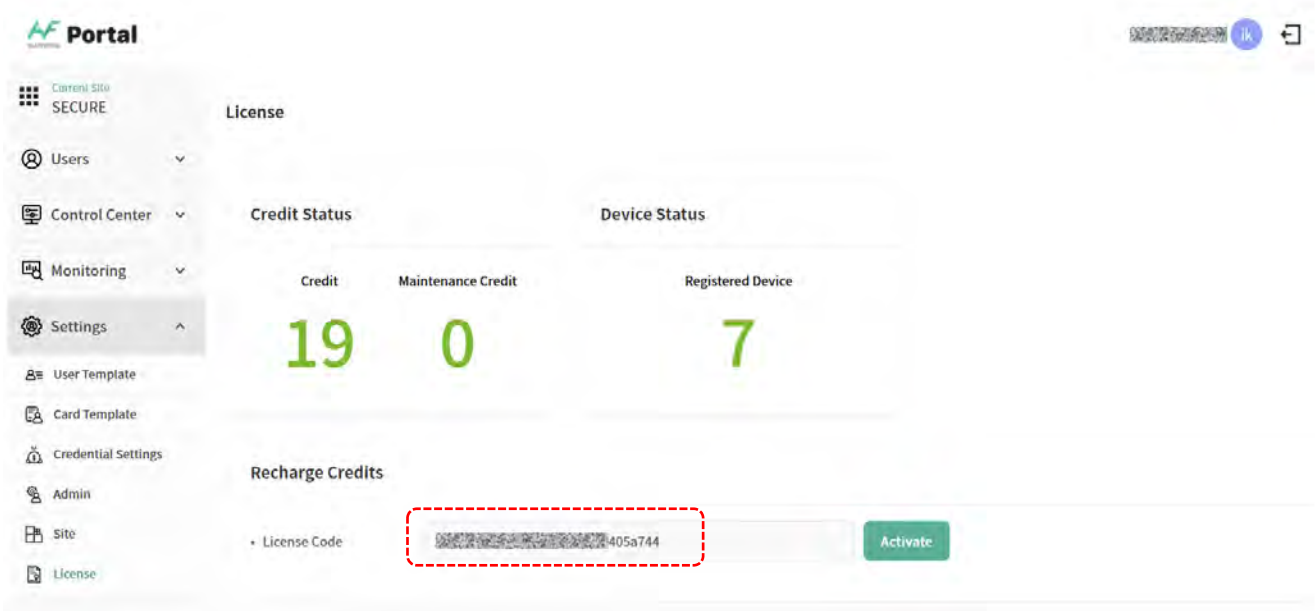
上記の例の場合、レギュラー サイトなので、クレジット 及び メンテナンスクレジットの数が表示されます。
クレジット数の残りが 19 メンテナンスクレジット数の残りが 0 であることがわかります。

21.18.4.2 クレジットの適用

ポータルサイトにログインし、[Settings] → [License] と進んでください。
弊社より クレジット(または メンテナンスクレジット)をご購入頂いた場合、弊社から、ライセンスコードを送らせていただきます。

ライセンスコードは、32 文字の英数字となります。

お受け取りになられたら、下図の赤枠の License Code 部分に入力し、 Activate をクリックし、登録してください。



これにより、ご購入いただいたクレジット数が反映されます。

21.18.4.3 ログイン パスワード変更

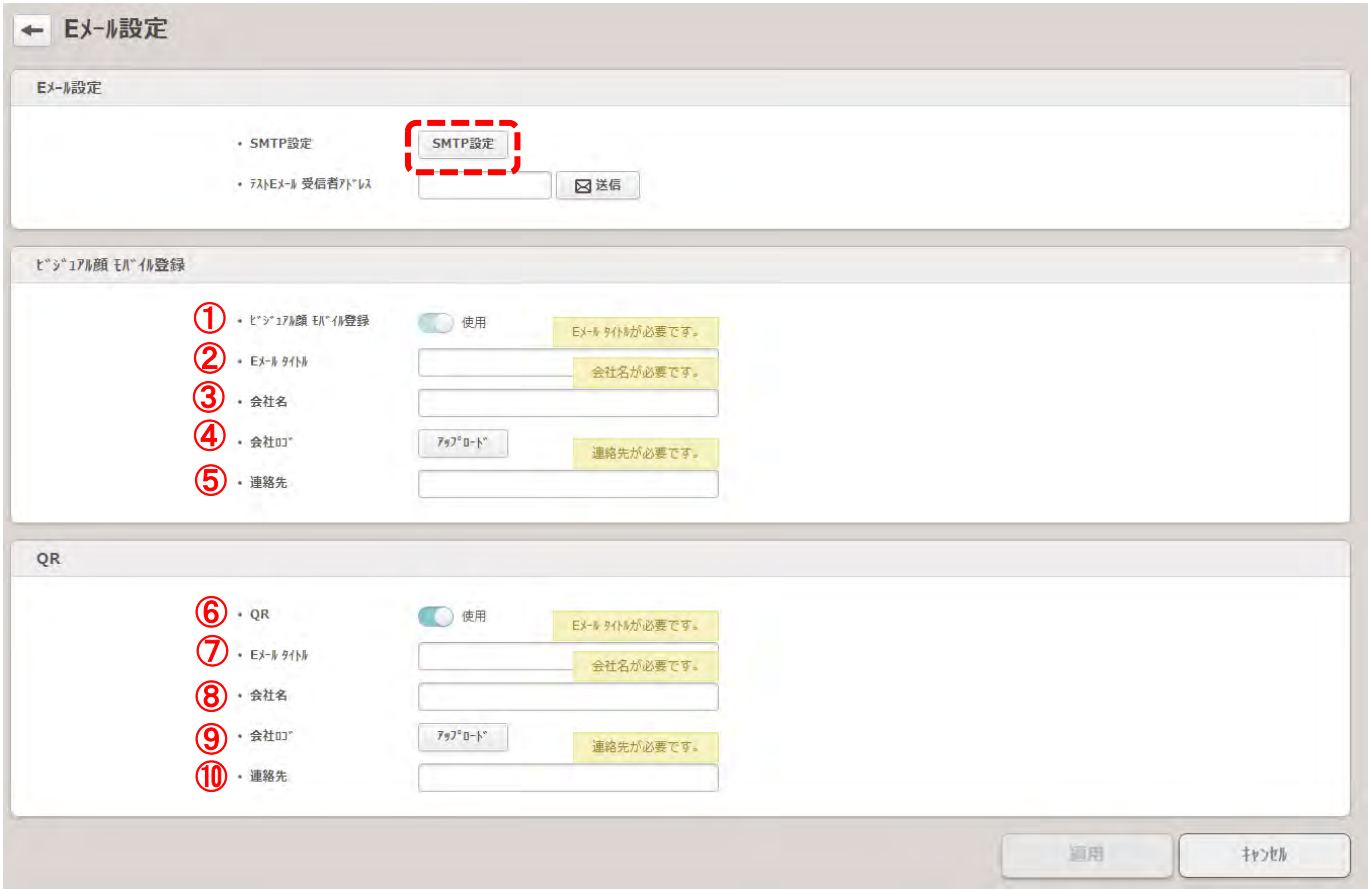
ポータルサイトは、一定期間パスワードを変更しない場合に、ログイン時、パスワードの変更要求が表示されます。
セキュリティの維持のためには、パスワードを定期的に変更してください。
なお、変更された場合は、新しいパスワードをお忘れにならないよう管理をお願い致します。

21.19 Eメール内容 項目

ビジュアル顔の登録リンク先を E メールにて送信する場合、および、BioStar2 QR コードを E メールにて送信する場合のための設定を行ないます。

タイトル、本文、署名、SMTP（Simple Mail Transfer Protocol）などの内容を入力します。

また、設定確認のため、テスト用の E メールを送信することが可能です。



メールを送信するためには、送信メールサーバ（SMTP）の設定を行う必要があります。SMTP 設定　ボタンをクリックすると以下の画面を開きます。

利用可能な SMTP サーバーの設定を入力し、適用をクリックしてください。

設定完了後、「適用」をクリックし、テスト E メール受信アドレスに、
確認用のメールアドレスを入力し、「送信」をクリックしてください。
正しくテストメールが受信できたら、SMTP の設定は完了となります。

[ビジュアル顔のモバイル登録]メールについて

このメールは、FaceStationF2 をご利用頂いている場合に、スマートフォンを利用して、その方の顔を登録可能とする機能です。
ユーザー情報を作成した後（必須：メールアドレス）、そのユーザーに対し、ビジュアル顔のモバイル登録メールを送ることで、
そのメールをスマートフォンで受け取ったユーザーは、メールのリンクの指示に従い、自身の顔を撮影し、その写真をアップロードすることで、
ビジュアル顔の登録が完了する。 と言う機能です。

① ビジュアル顔のモバイル登録を利用する場合は、「使用」 と設定してください。「使用」とすると、②～⑤の設定が表示されます。
② ビジュアル顔のモバイル登録メールのメールタイトルを設定してください。
③ ビジュアル顔のモバイル登録メールに表示される会社名を設定してください。
④ 会社のロゴマークを「アップロード」をクリックし指定してください。（ファイル形式は、GIF、JPG、JPEG、JPE、JFIF、PNG,）
⑤ ビジュアル顔のモバイル登録メールに記載される連絡先のメールアドレスを指定してください。

[QR]メールについて

このメールは、BioStar2 の資格情報で、BioStar2 QR コードをもたせた際に、自動的に該当ユーザーに対して、QR コードをメールで送付する機能です。

⑥ QR コードを利用する場合は、「使用」と設定してください。「使用」とすると、⑦～⑩の設定が表示されます。
⑦ QR コードの送付メールのメールタイトルを設定してください。
⑧ QR コードの送付メールの会社名を設定してください。
⑨ 会社のロゴマークを「アップロード」をクリックして指定してください。（ファイル形式は、GIF、JPG、JPEG、JPE、JFIF、PNG,）
⑩ QR コードメールに記載される連絡先のメールアドレスを指定してください。

22 システムのバックアップ および 復元

BioStar2 システムでは、システムのデータをデータベースで管理しています。

BioStar2 システム自体、およびデータベースをバックアップしておくことで、サーバーPC のデータ破損や、PC 自体の破損があった際に、データの回復ができる可能性があります。

このため、システムおよび、データベースの定期的なバックアップを推奨します。

なお、バックアップには、手動で実施するシステム全体のバックアップ・復元（リストア）と、データベースのバックアップのみですが、自動で、定期的に実施する方法があります。

本章では、これらのシステム及び、データベースのバックアップ取得方法と、復元（リストア）方法について記載します。

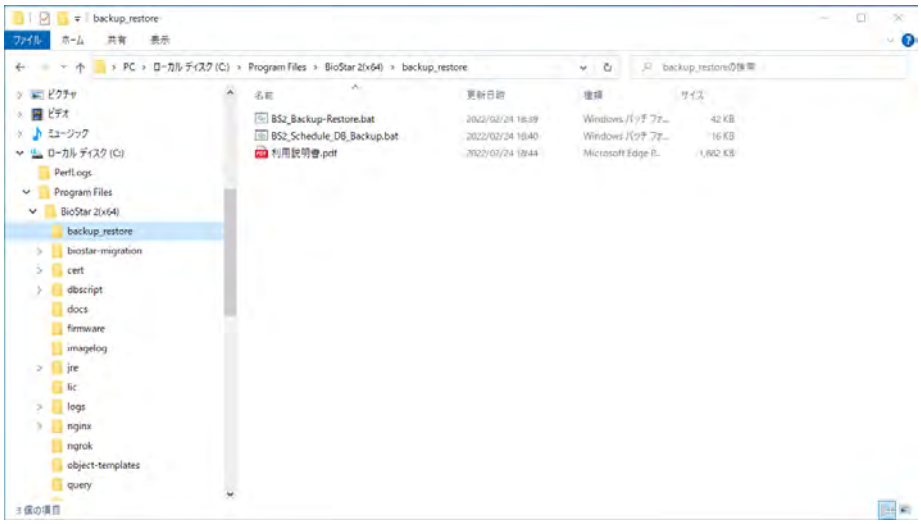
以下にも説明を記載しますが、より詳細な説明は、同梱の「manual.pdf」 を参照してください。

22.1 手動でのバックアップ および リストア

手動で、バックアップおよび、リストアを行うためには、以下の手順で行ってください。

サーバーPC で、エクスプローラーを開き、以下の場所にアクセスしてください。

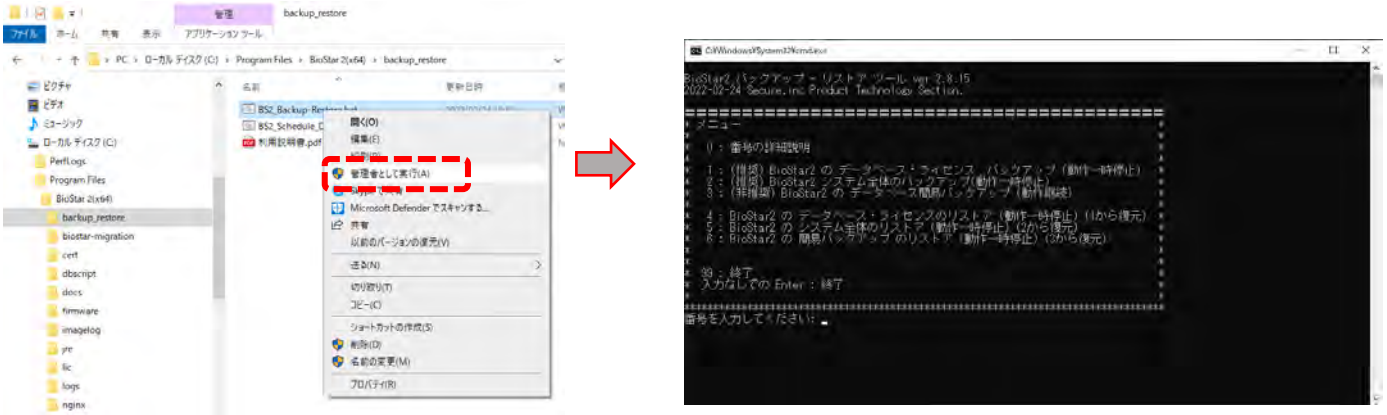
C:¥Program Files¥BioStar 2(x64)¥backup_restore



アクセスすると、上記のように、3つのファイルがあります。手動でのバックアップ・リストアを行う際は、その中の

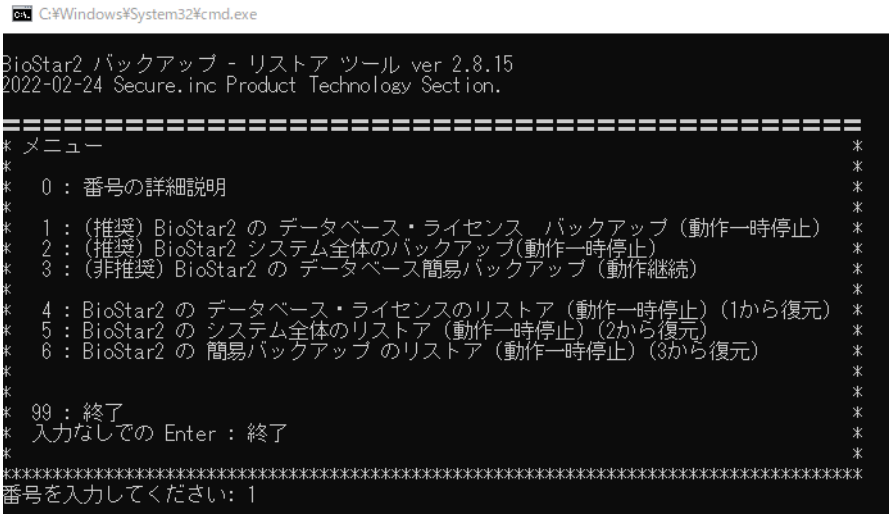
BS2_Backup-Restore.bat

を、右クリックして、**管理者として実行**を行ってください。右に示す画面が表示されます。



22.1.1 データベース・ライセンス のバックアップについて（手動）

データベース・ライセンスのバックアップを取得する場合は、メニューで、1 を入力してください。



1 を入力した場合は、BioStar2 の動作を一時的に停止し、データベース および ライセンスのバックアップを取得します。

※ライセンスは、PC に紐付いていますので、バックアップを取っていても、同一の PC でのみ利用可能です。

他の PC では、ライセンスを利用できません。ライセンスを他の PC に振り返る場合は、弊社までご連絡ください。

グローバルゾーン（26.1 章）の利用や、サーバーマッチング（21.5 章）の利用などをされている場合は、その間、動作しなくなります。

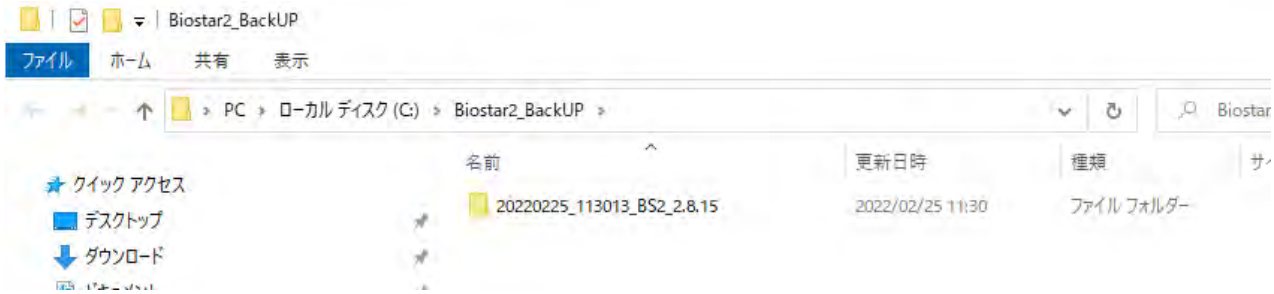
このため、サーバーの動作が一時停止しても問題の無い時間帯に実施していただくか、3 を入力してバックアップを取得してください。

本バックアップでは、ファイルシステム単位で、データベースのデータも含め、ライセンスや、設定状況ごとバックアップします。

このため、データベース簡易バックアップと比較し、容量が大きくなります。

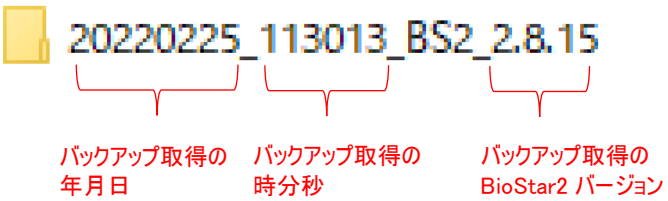
C ドライブにバックアップしますので、空き容量を考慮しながら、ご利用いただくようお願い致します。

データベース・ライセンスのバックアップが完了すると、自動的にフォルダが開きます。



バックアップの出力先は、 **C:¥Biostar2_BackUP** フォルダになります。

フォルダ名は、以下のルールで生成されます。

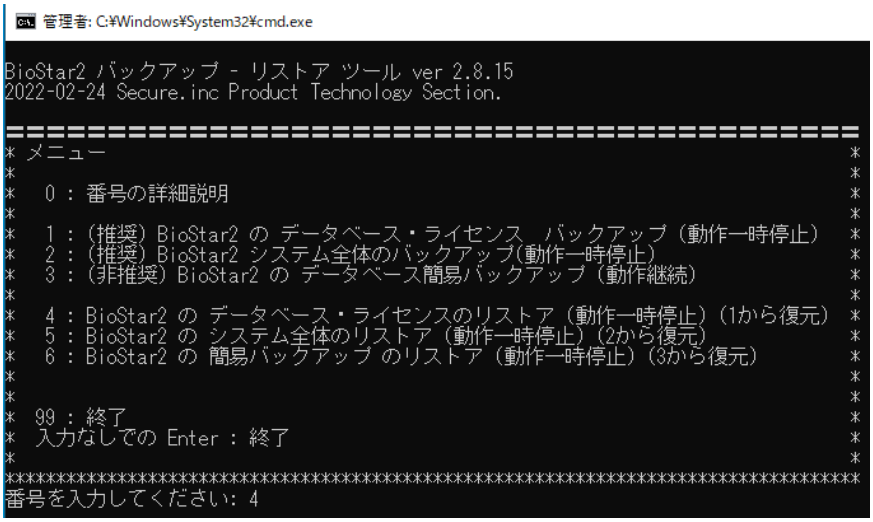


フォルダのまま、保存するか、フォルダごと圧縮をして保管してください。

（フォルダを保管のために圧縮した場合は、標準的な圧縮形式で、3 分の 1 くらいのサイズになります。）

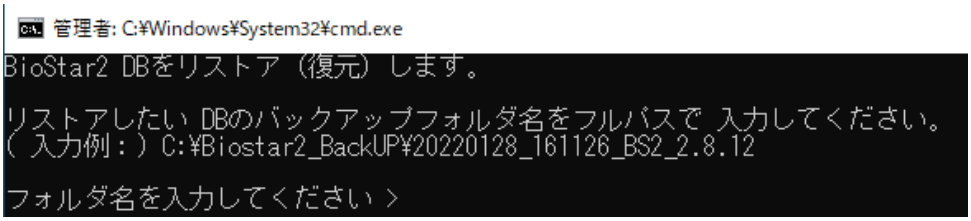
22.1.2 データベース・ライセンス のリストアについて（手動）

データベース・ライセンスのバックアップを復元する場合は、メニューで、4 を入力してください。



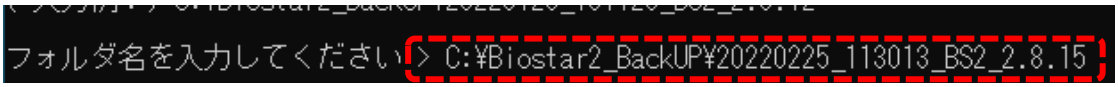
4 を入力した場合は、BioStar2 の動作を一時的に停止し、データベース および ライセンスのバックアップを取得します。

以下の画面を表示します。



リストアしたいデータベース・ライセンスのバックアップフフォルダを、入力例のように入力します。

例えば、前のページの例にあげたバックアップフォルダを復元する場合は、以下のように入力し、”Enter”を押します。

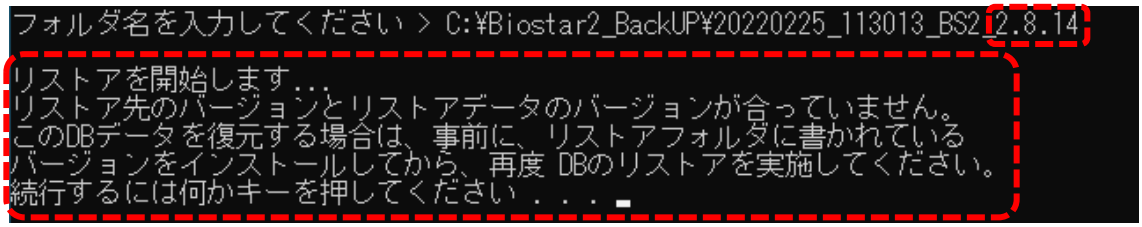


BioStar2 を停止し、リストアが始まり、その後、BioStar2 を開始します。

なお、データベース・ライセンスのリストアの際は、リストア前に同一のバージョンの BioStar2 がインストールされている必要があります。

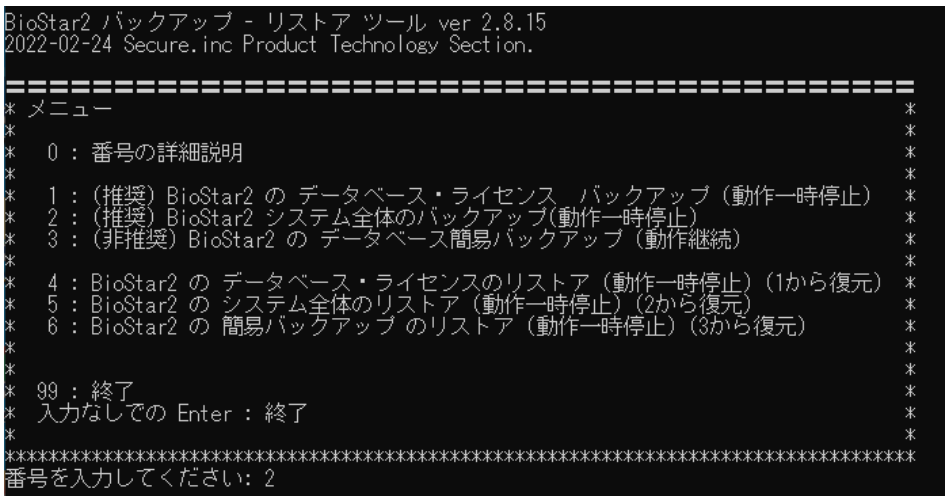
もし、異なるバージョンの BioStar2 に対して、バックアップフォルダをリストアしようとすると、以下のような表示になります。

（例：BioStar 2.8.15 の環境に、2.8.14 のバックアップフォルダをリストアしようとした場合）



22.1.3 システムのバックアップについて（手動）

システムのバックアップを取得する場合は、メニューで、2 を入力してください。



2 を入力した場合は、BioStar2 の動作を一時的に停止し、システムのバックアップを取得します。

グローバルゾーン（26.1 章）の利用や、サーバーマッチング（21.5 章）の利用などをされている場合は、その間、動作しなくなります。

このため、サーバーの動作が一時停止しても問題の無い時間帯に実施していただくか、3 を入力してバックアップを取得してください。

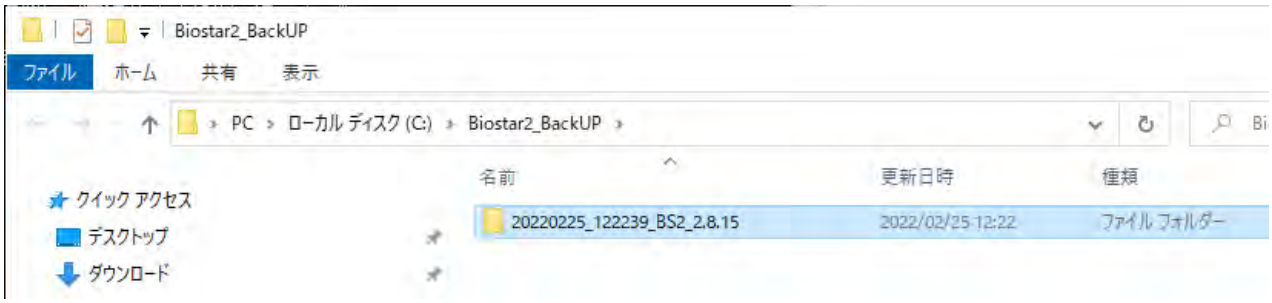
システムのバックアップでは、データベースのデータも含め、ライセンスや、設定状況ごとバックアップします。

このため、データベースのみのバックアップと比較し、容量も大きくなりますし、その分、時間もかかります。

C ドライブにバックアップしますので、空き容量を考慮しながら、ご利用いただくようお願い致します。

（利用状況により、必要な容量は変化しますが、目安としては、30GB 程度の空き容量は必要になります。）

システムのバックアップが完了すると、自動的にフォルダが開きます。



バックアップの出力先は、 **C:¥Biostar2_BackUP** フォルダになります。

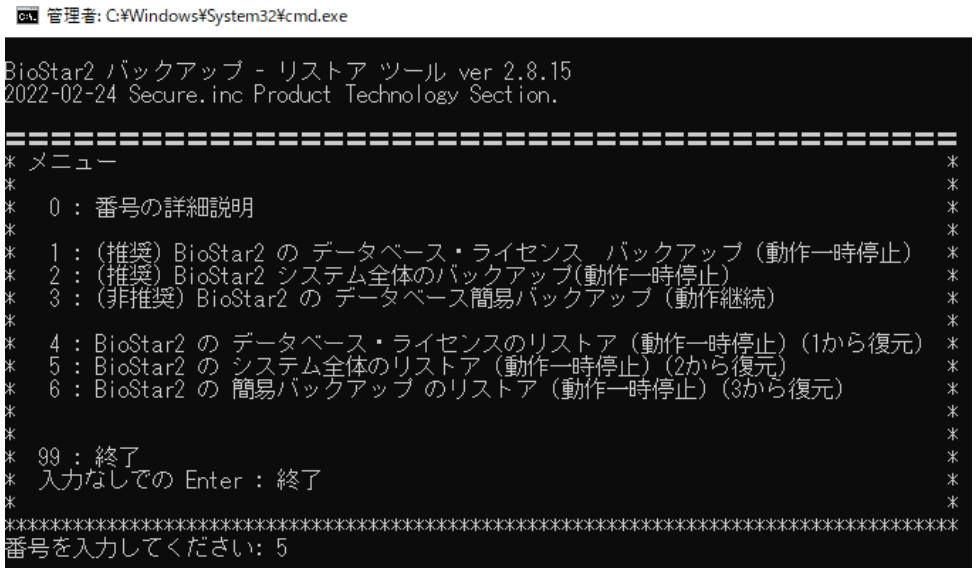
フォルダ名の生成ルールは、22.1.1 と同様です。

フォルダのまま、保存するか、フォルダごと圧縮をして保管してください。

（フォルダを保管のために圧縮した場合は、標準的な圧縮形式で、3 分の 1 くらいのサイズになります。）

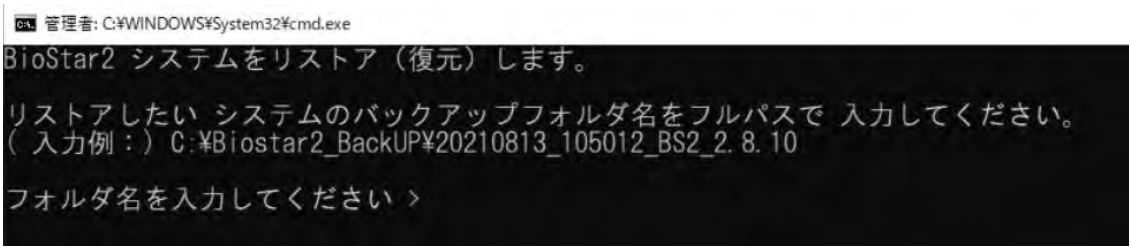
22.1.4 システムのリストア（復元）について（手動）

システムを復元する場合は、メニューで、**5** を入力してください。



システムをリストアする場合は、BioStar2 の動作を停止し、リストアします。

“5” を入力し、“Enter”を押してください。以下のような画面になります。



リストアしたいシステムのバックアップフォルダを、入力例のように入力します。

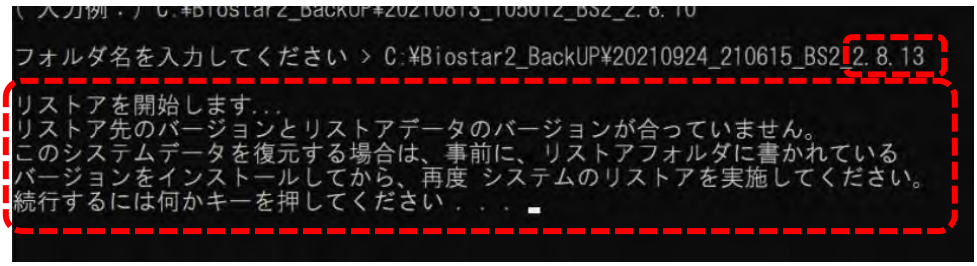
例えば、前のページの例にあげたバックアップフォルダを復元する場合は、以下のように入力し、”Enter”を押します。

BioStar2 を停止し、リストアが始まり、その後、BioStar2 を開始します。

なお、システムのリストアの際は、リストア前に同一のバージョンの BioStar2 がインストールされている必要があります。

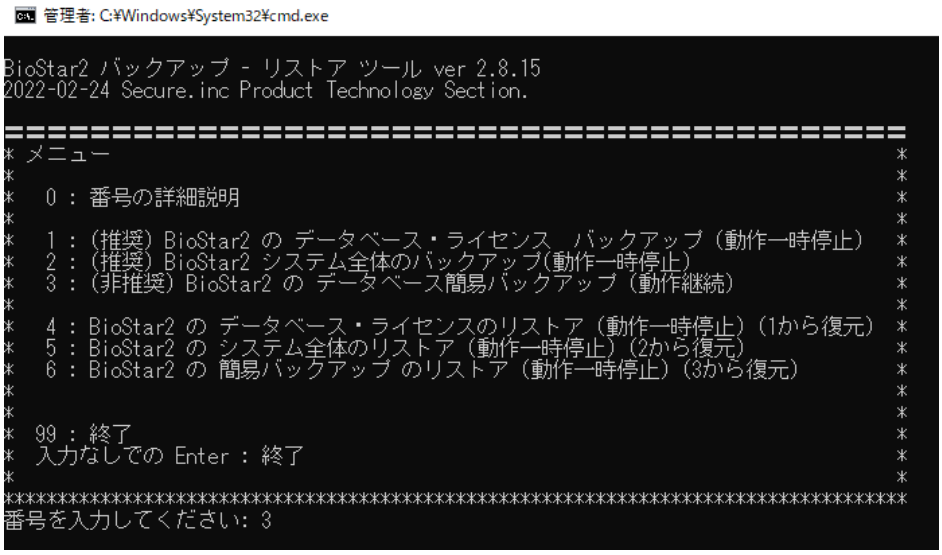
もし、異なるバージョンの BioStar2 に対して、バックアップフォルダをリストアしようとすると、以下のような表示になります。

（例：BioStar 2.8.15 の環境に、2.8.13 のバックアップフォルダをリストアしようとした場合）



22.1.5 データベースのバックアップについて（手動）

データベースのバックアップを取得する場合は、メニューで、3 を入力してください。

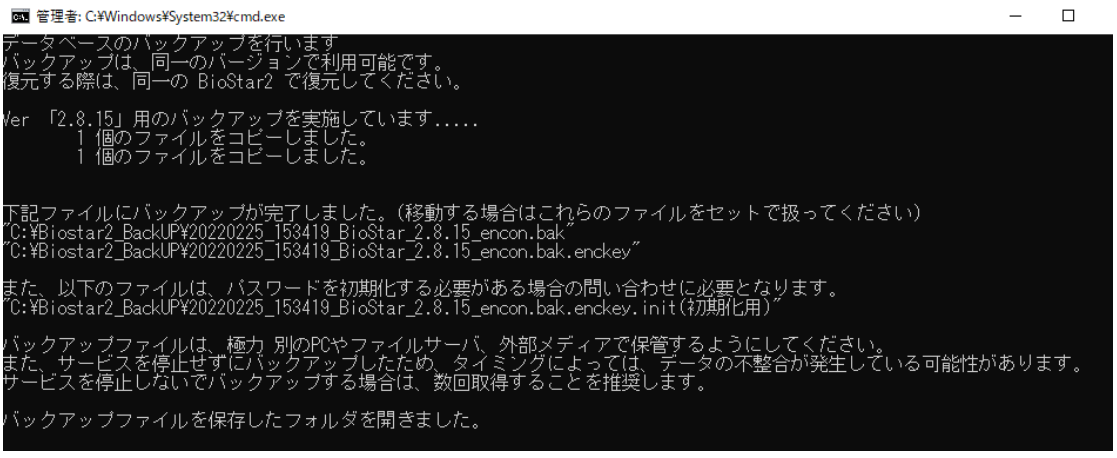


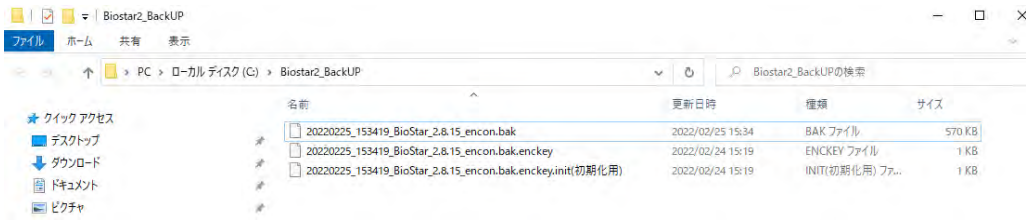
3 を入力した場合は、BioStar2 の動作を停止せず、動作させたまま、データベースの簡易バックアップを取得します。

但し、動作中（データが途中で変更される可能性がある状態）にバックアップを取得するため、バックアップ開始直後のデータ部分と、バックアップ終了直前のデータ部分で、データの矛盾が発生する場合があり、バックアップデータが不完全になってしまう場合が考えられます。

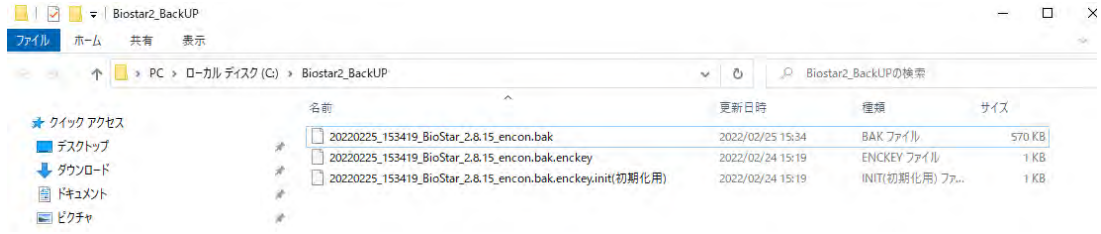
安全なバックアップを取得するためには、機能を一時的に停止し、データ更新を止めた状態で行ったほうが良いため、1 でのバックアップを推奨します。

バックアップが完了すると、自動的にフォルダが開きます。



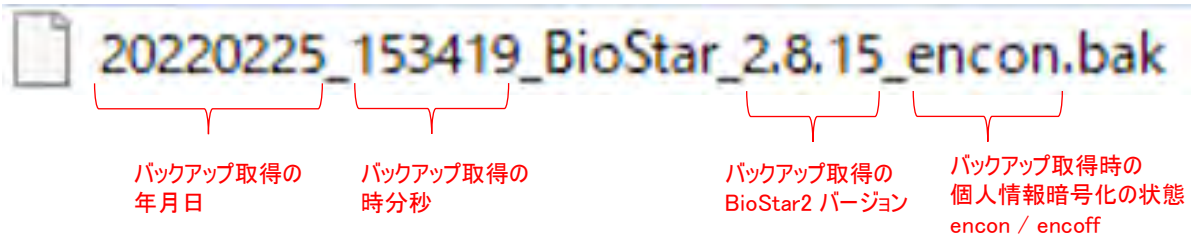


開かれたフォルダの、 **C:¥Biostar2_BackUP** フォルダには、以下の 3 ファイルが出力されます。



データベースを保管する際は、3 つのファイルを セットで保管しておいてください。

ファイル名は、以下のルールで生成されます。

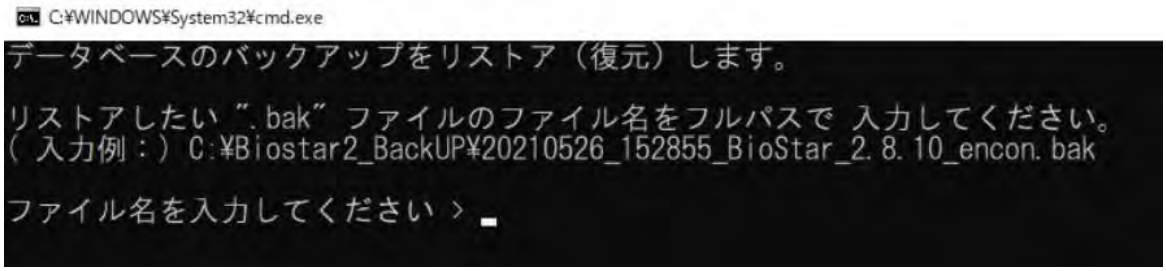


22.1.6 データベースのリストア(復元)について(手動)

データベースの簡易バックアップを復元する場合は、メニューで、**6** を入力してください。

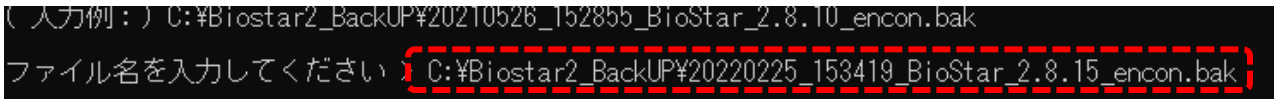
データベースをリストアする場合は、BioStar2 の動作を停止し、リストアします。

“6” を入力し、“Enter”を押してください。以下のような画面になります。



リストアしたいデータベースのバックアップファイルを、入力例のように入力します。

例えば、前のページの例にあげたバックアップファイルを復元する場合は、以下のように入力し、”Enter”を押します。

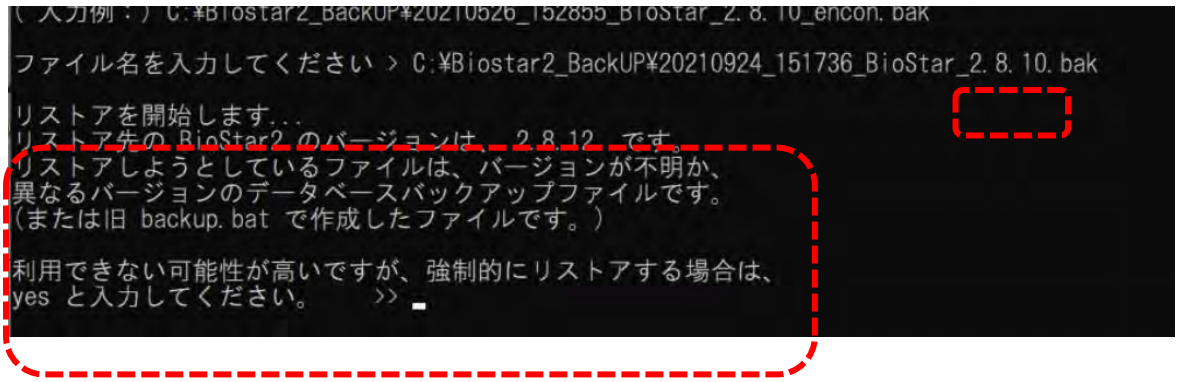


BioStar2 を停止し、リストアが始まり、その後、BioStar2 を開始します。

なお、データベースのリストアの際は、同一のバージョンの BioStar2 である必要があります。

もし、異なるバージョンのバックアップファイルをリストアしようとすると、以下のような表示になります。

（例：BioStar 2.8.12 の環境に、2.8.10 のバックアップファイルをリストアしようとした場合）



異なるバージョンでリストアすると、正しく動作しません。通常は、no と入力し、作業を止め、BioStar2 バージョンを合わせてください。

しかし、承知の上で強制的にリストアする場合は、上記で、“yes”と入力し、作業を継続することも可能です。

また、BioStar2 のバージョン 2.8.8 以降は、データベース内の個人情報部分を更に暗号化することが可能です。

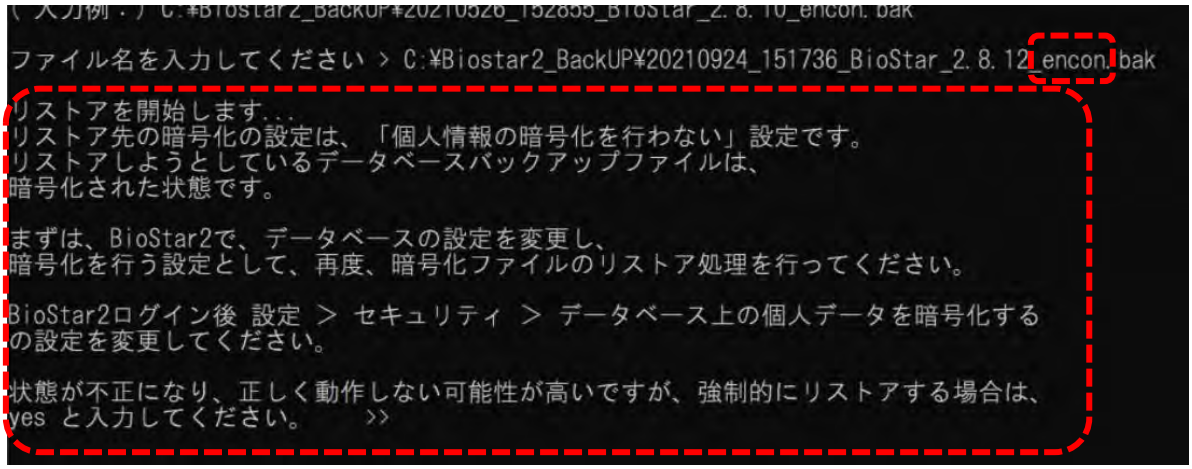
この設定を含めた内容がバックアップされています。

・個人情報暗号化の設定が ON になっていない環境に、暗号化済みのデータベースバックアップをリストア

・個人情報暗号化の設定が ON になっている環境に、暗号化していないデータベースのバックアップをリストア

の 2 つのパターンは、矛盾が生じ、動作しなくなります。

この場合も同様に警告を表示します。



リストア前には、リストア先の環境と、リストアするファイルの環境を一致させてください。承知の上で強制的にリストアする場合は、

“yes”と入力し、作業を継続することも可能です。

22.2 自動でのデータベースバックアップ

22.1 章では、BioStar2 のバックアップについて、手動で実行する方法について説明しました。

本章では、データベースのバックアップのみとなりますが、Windows のタスクスケジューラで設定し、自動で定期的に取得する方法について記載します。

但し、古くなったものを削除する機能はありませんので、定期的なバックアップファイルの容量の確認と、古くなった不要なファイルの削除は

手動で行うようにしてください。

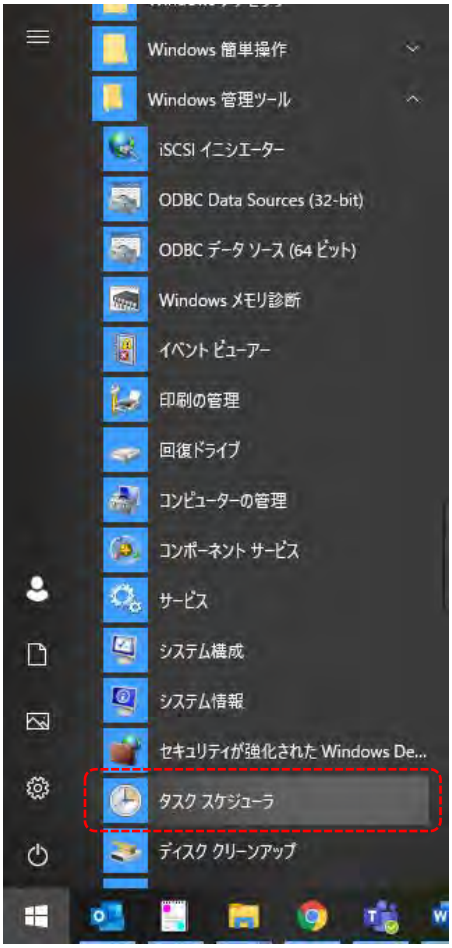
なお、定期的なバックアップを実施するのは、BioStar2 をインストールしたサーバーPC で実施します。

ここでは、定期バックアップの紹介として、OS が Windows10 の場合の例を記載します。

（他のバージョンの OS でも基本的には同じです。）

右図のように、スタートメニューから、

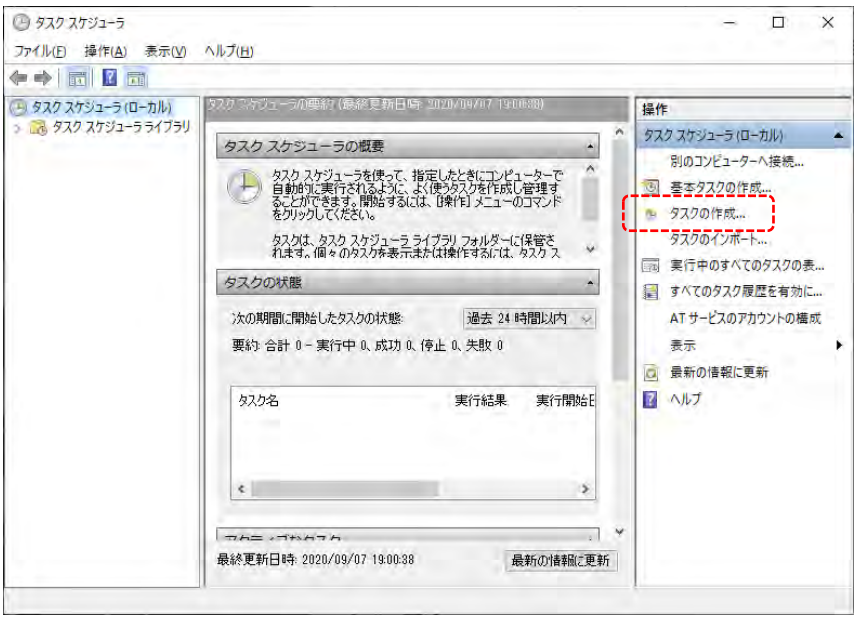
Windows 管理ツール 内の タスク スケジューラー を実行します。



なお、本例では、月に 1 回 毎月 1 日の朝バックアップを取得するように設定します。

実際には、ご都合の良いタイミングで動作するように設定してください。

以下のような画面が表示されます。



タスクの作成 をクリックします。

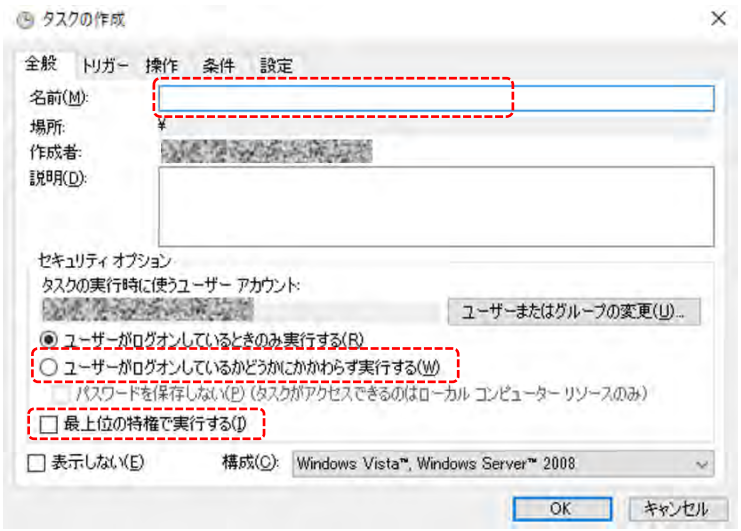
まずは、[全般] タブで、名前を入力します。

ここでは、 **BioStar2 定期バックアップ** とします。

（名前は区別が付けば構いません。）

「ユーザーがログオンしているかどうかにかかわらず実行する」

を選択し、「最上位の特権で実行する」にチェックを入れます。



次に、[トリガー]タブをクリックします。

最初は、空欄の画面が表示されますので、[新規]ボタンを

クリックしてください。

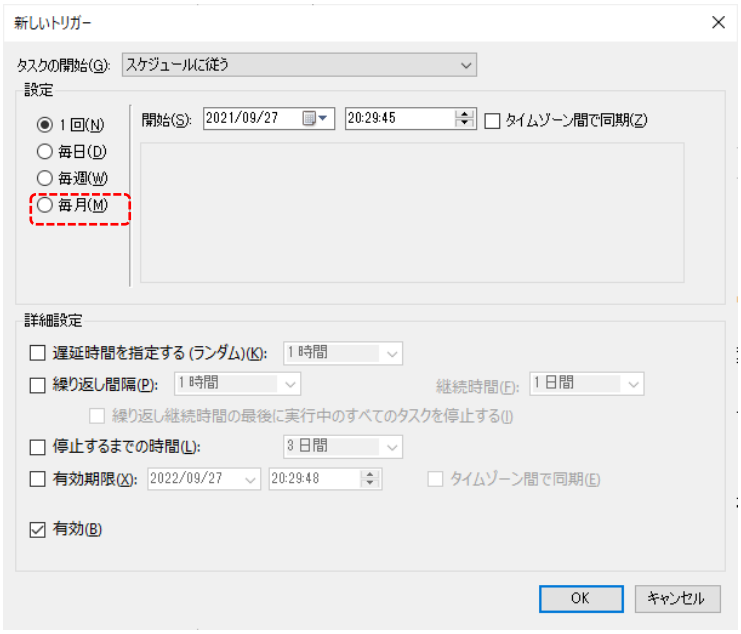
右図の画面が表示されたら、

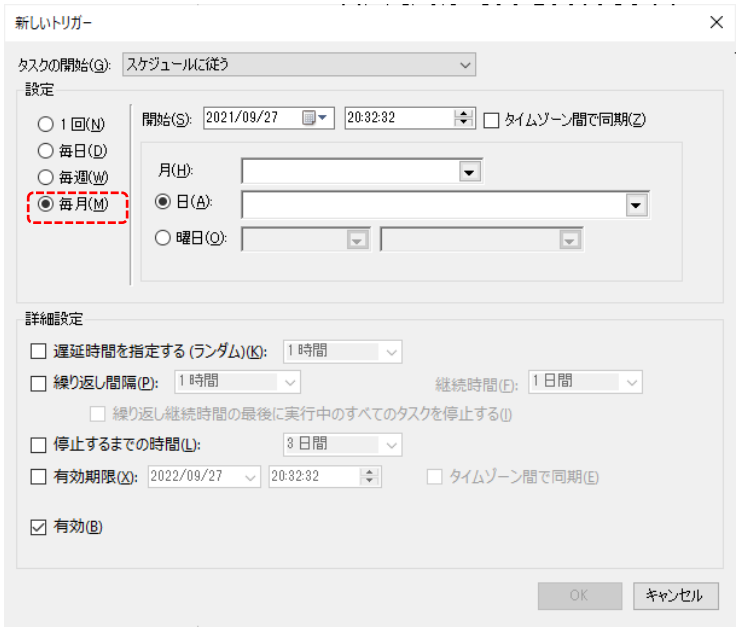
[毎月]を選択ししてください。

画面が、右下の画面になります。

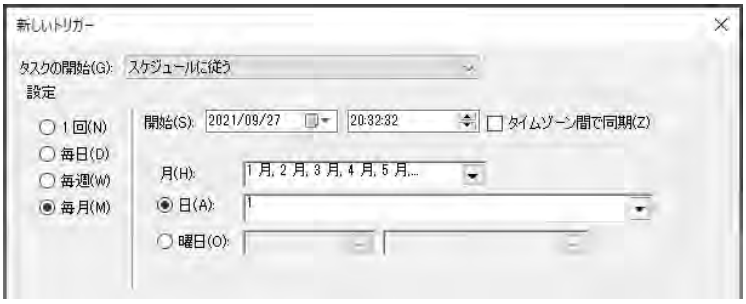
[月]の項目で、[すべての月を選択]を選択し、

[日]の項目で、[1]日を選択してください。





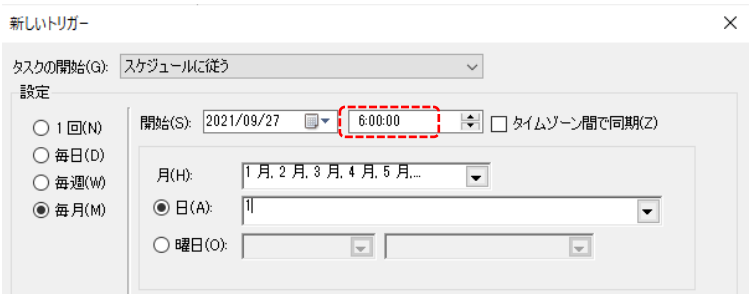
右図のように、すべての月の 1 日に動作。
という設定になります。



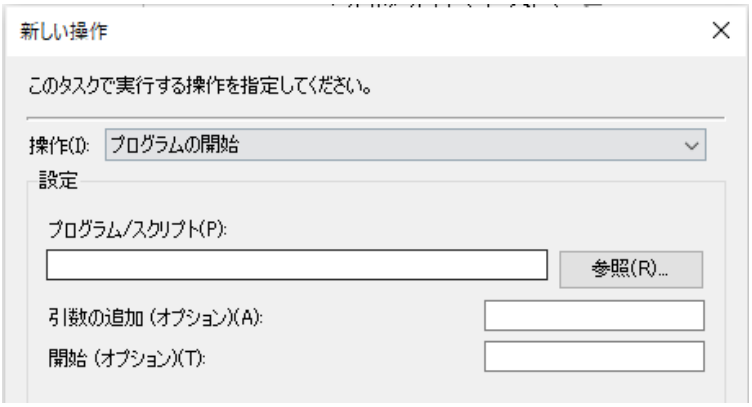
また、開始時間ですが、開始日自体は、
設定した日が入力されますが、毎月 1 日に設定しているので、
そのままで構いません。
しかし、開始時間は朝に設定したいため、時間を設定します。

ここでは、毎月 1 日の朝 6 時からバックアップ処理を動作させる設定例とします。

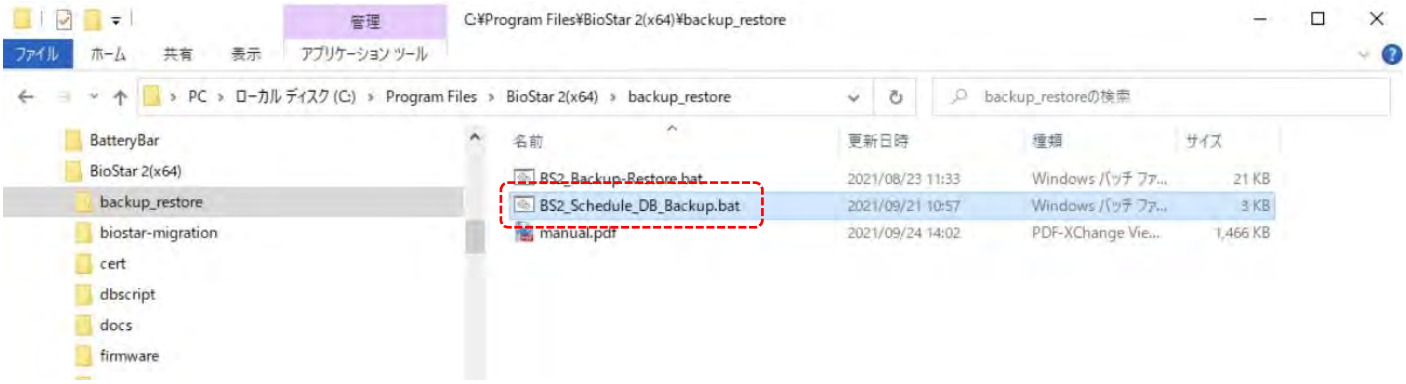
右図のように、開始の日にちは影響ありませんが、
時間を設定します。
設定が完了したら、[OK]をクリックします。



次に、[操作]タブをクリックします。
最初は、空欄の画面が表示されますので、[新規]ボタンを
クリックしてください。



右図の画面が表示されたら、[参照]ボタンをクリックし、
BioStar2 のインストールフォルダの中の、
backup_restore フォルダ内の
BS2_Schedule_DB_Backup.bat
を選択します。



ここまで、設定したら、[条件][設定]の 2 つのタブが残っていますが、そのまま、[OK]をクリックしてください。

最後に管理者で実行するための確認画面が表示されます。

管理者のユーザー名とパスワードを指定して、
[OK]をクリックすると完了します。

あとは、指定の日時にバックアップ処理が動作しますので、
空き容量に注意しつつ、他の PC やファイルサーバに移すなど、
管理をお願いいたします。

なお、もし、管理者の Windows ログインのパスワードを変更した場合は、本処理が動作しなくなりますので、
こちらの設定のパスワードも再度変更してください。

また、自動でバックアップを取得したファイルですが、手動のデータベースバックアップと同じ内容となります。
このため、これを利用してデータベースのリストアを行う場合は、22.1.6 章の方法で実施してください。

23 端末の設定

BioStar2 システムでは、端末を利用する前に 端末を BioStar2 システムに登録します。
端末の登録の方法は、「端末の検索」→「検出」→「端末追加」の流れとなります。
端末を追加した後、端末ごとに各種設定が可能です。

23.1 端末の追加

BioStar2 システムで端末を追加するには、端末の物理的な接続方法により方法が変わります。
本章では、以下 3 タイプの端末追加方法について記載します。

- ・LAN 接続の端末を UDP で検索して追加する
- ・LAN 接続の端末を TCP で IP アドレス指定により検索して追加する
- ・RS-485 接続の子機端末を 検索して追加する

（Wiegand 接続については、弊社機器同士での接続ではないため、省略します。）

なお、同じ端末で接続方法を変更する場合などは、以前の接続方法が残っていると新しい接続方法の検索ができません。新しい接続方法の端末を検索する場合は、事前に、その端末の旧接続情報を削除してください。

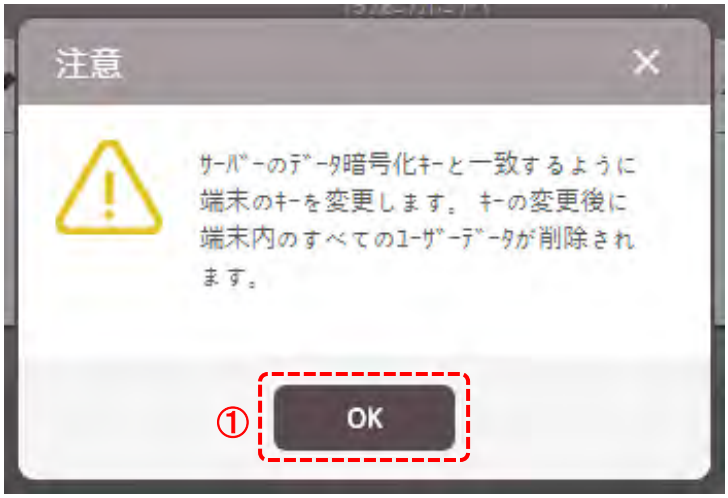
23.1.1 LAN 接続端末 UDP での検索・追加

BioStar2 システムで、LAN 接続の端末を検索・追加する場合は、端末と BioStar2 サーバーPC が、通信できる状態にあることが必要となります。サーバーPC と端末がきちんとルーティングされ通信できる環境にあるか、または、同セグメントの環境にあることを確認してください。
また、BioStar2 の端末は初期値として DHCP に設定されています。（端末のネットワーク設定値をリセットした場合も、DHCP の設定に戻ります。）このため、DHCP サーバーが存在するネットワークに接続してご利用ください。
（端末が液晶および 10 キーを装備している機種は、端末からネットワーク設定値を変更可能です。）

ここでは、以下の条件での操作例を記載します。

BioStar2 サーバーPC	:192.168.0.252/24
端末（BioEntryP2）	:DHCP 設定
DHCP サーバー兼 GW	:192.168.0.254/24
過去の BioStar2 登録	:BioEntryP2 が登録されていないこと
端末ポート番号	:初期値（51211）であること

説明図	操作内容
	① 検索・追加対象の BioEntryP2 が、端末のリストに登録されていないことを確認
	① UDP で検索する場合は、左図の「端末検索」ボタンをクリックしてください。
	左図のように、端末が検出されます。 検出されない場合は、以下のことが考えられます。 ・DHCP サーバーが、ネットワーク内に存在しない ・端末の起動が完了していない ・ネットワークケーブルが正しく接続されていない ・端末が、端末->サーバー に設定されている
	前画面で、検出されたがネットワーク設定値が予定と異なる場合は、「IP アドレス設定」ボタンを押すことで、左図の画面となり、IP アドレスを変更できる場合があります。 変更後、しばらくして、再度端末検索することで、更新された IP アドレスの端末を検出することが可能です。

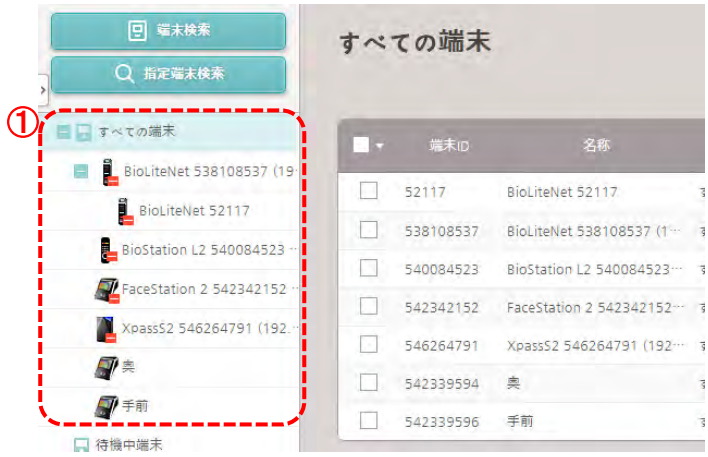
説明図	操作内容
	① 検出ができた状態で、端末を追加する際は、「追加」ボタンをクリックしてください。
	① 左図の注意画面が表示されます。 「OK」をクリックしてください。
	① 端末が追加されたことをお知らせする画面が表示されます。 「OK」をクリックしてください。
	ツリー表示部と、リスト表示部に、追加した端末が表示され、BioStar2 で管理可能な状態となります。

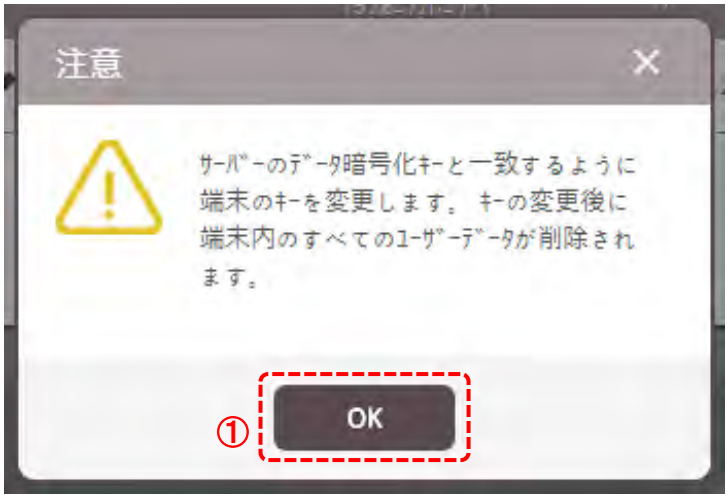
23.1.2 LAN 接続端末 TCP での検索・追加

BioStar2 システムで、LAN 接続の端末を TCP で検索・追加するためには、端末の IP アドレスが事前にわかっている場合に有効です。UDP と異なり、TCP の場合は、確実に端末と通信し検索することが可能です。
（端末が液晶および 10 キーを装備している機種で、IP アドレスが固定設定可能な場合に有効です。）

ここでは、以下の条件での操作例を記載します。

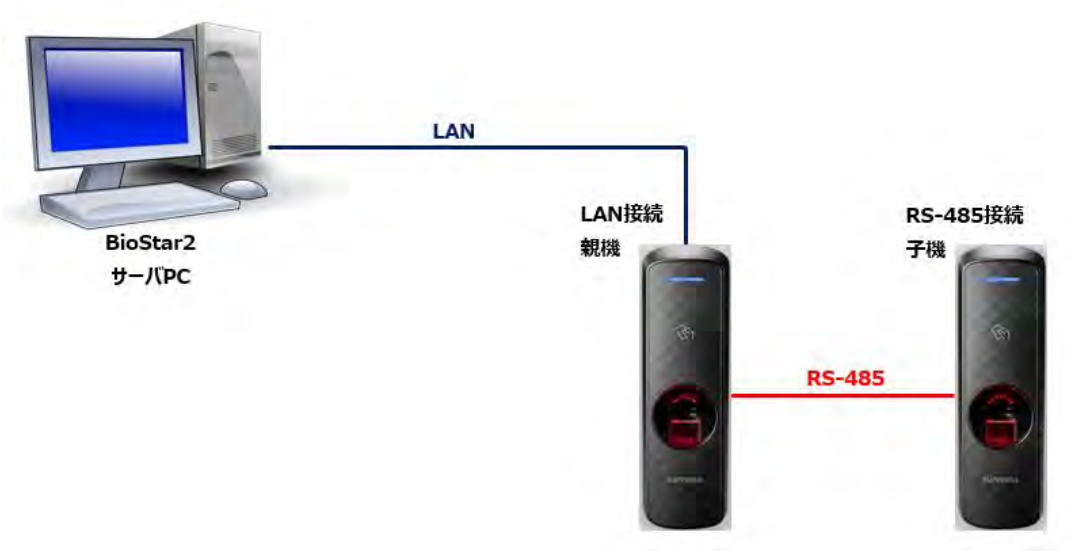
BioStar2 サーバーPC :192.168.0.252/24
端末（BioEntryP2） :192.168.0.123
DHCP サーバー兼 GW :192.168.0.254/24
過去の BioStar2 登録 :BioEntryP2 が登録されていないこと
端末ポート番号 :初期値（51211）であること

説明図	操作内容
	① 検索・追加対象の BioEntryP2 が、端末のリストに登録されていないことを確認
	① TCP で検索する場合は、左図の「指定端末検索」ボタンをクリックしてください。
	① 検索したい端末の IP アドレスを入力してください。（端末ポートは、基本的に変更する必要はありません。初期値で、51211 となります。） ② 入力が完了したら、「検索」ボタンをクリックしてください。

説明図	操作内容
	① 左図の様に検索結果が表示されます。 「追加」ボタンをクリックしてください。
	① 左図の注意画面が表示されます。 「OK」をクリックしてください。
	① 端末が追加されたことをお知らせする画面が表示されます。 「OK」をクリックしてください。
	ツリー表示部と、リスト表示部に、追加した端末が表示され、BioStar2 で管理可能な状態となります。

23.1.3 RS-485 接続の子機端末の検索・追加

RS-485 接続の端末を追加するためには、接続方法が以下のようになっている必要があります。



RS-485 の子機として接続できる端末は、以下となります。

・各認証端末

・拡張 I/O ユニット（Secure I/O2, DM-20, OM-120）

また、親機の機種により、以下の条件が付加されます。

親機が、顔認証機（FaceStation2）の場合

子機は 1 台までとなります。

このため、子機に FaceStation2 と拡張 I/O ユニットを同時に接続することはできません。

親機が、指紋認証機の場合

子機は 7 台までとなります。指紋認証機と、カード認証機と、拡張 I/O ユニットを接続可能です。

親機が、カード認証機の場合

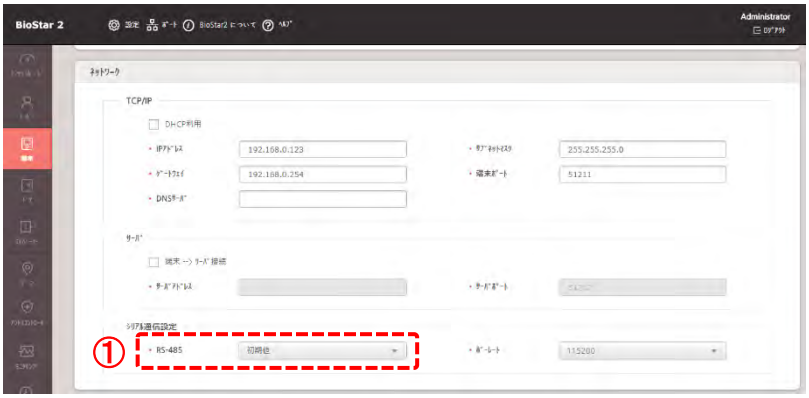
子機は 31 台までとなります。カード認証機と、拡張 I/O ユニットを接続可能です。

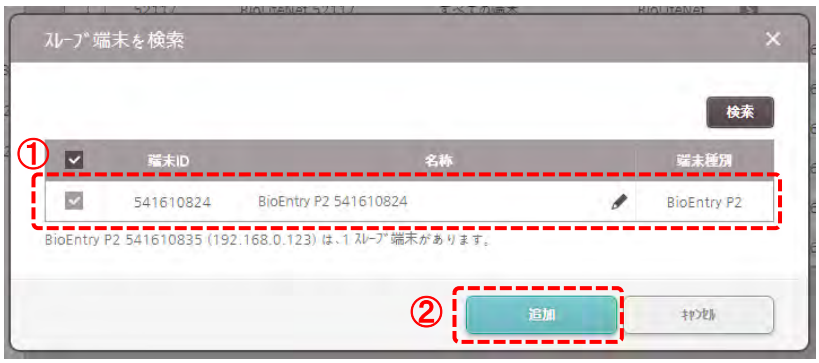
RS-485 接続の子機を検索・追加する場合は、親機の RS-485 の設定が、「マスター」になっていることと、
子機の RS-485 の設定が、「初期値」または、「スレーブ」となっていることが必要です。
（子機の RS-485 設定が、「初期値」の機種を検索後に端末追加すると、自動的に「スレーブ」に変更されます。）

本章の説明では、親機となる LAN 接続の端末は、前章で追加し終わっていることを前提とします。
追加後からの説明を記載します。

ここでは、以下の条件での操作例を記載します。

BioStar2 サーバーPC　：192.168.0.252/24
DHCP サーバー兼 GW　：192.168.0.254/24
過去の BioStar2 登録　：BioEntryP2（親機・子機 共に）が、登録されていないこと
端末ポート番号　：初期値（51211）であること
親機端末（BioEntryP2）：192.168.0.123 （説明開始時は、RS-485 設定は「初期値」）
子機端末（BioEntryP2）：DHCP（説明開始時は、RS-485 設定は「初期値」）
親機端末（BioEntryP2）：LAN 接続で、BioStar2 に端末追加済みの状態

説明図	操作内容
	① 「端末」メニューをクリックし、端末画面にしてください。 ② 親機となる追加済みの端末をクリックしてください。
	① 端末の設定が表示されたら、少し下方向にスクロールし、「ネットワーク」項目の中のシリアル通信設定の RS-485 設定の部分を、「初期値」から、「マスター」に変更し、画面下部の「適用」をクリックしてください。
	① 設定を変更すると、リストの親機の部分に、左図の様にマスター端末を意味する M のアイコンが表示されます。

説明図	操作内容
	① マスター端末に設定した親機を右クリックすると、メニューが表示されます。 ② 表示されたメニューから、「スレーブ端末を検索」をクリックしてください。 ※右クリックのメニューに「スレーブ端末を検索」の項目が表示されない場合は、その端末の RS-485 の設定を、「マスター」にした後で、適用されているかを確認してください。
	① 検索が行われ、子機の端末が検出されます。（複数台接続されている場合は、同時に複数台検出されます。） 追加する端末に☑がついていることを確認してください。 ② 「追加」をクリックすると☑がついている端末を追加します。 ※もし、検出されない場合は、以下のことが考えられます。 ・子機の端末の RS-485 も「マスター」に設定されている。 ・子機の電源が入っていない。 ・RS-485 の配線が、正しくつながっていない。 ・終端抵抗が正しく配線されていない。
	① 端末が追加されたことをお知らせする画面が表示されます。 「OK」をクリックしてください。
	① 子機は、親機の 1 段下位に追加表示されます。 ② 子機は、スレーブ端末を意味する S のアイコンが表示されます。

注意事項：RS-485 の**端末を追加した途端**に、RS-485 切断 の警告が表示され、その後、接続できない場合があります。

本原因は、RS-485 初回接続時に、マスターとスレーブ間でセキュリティ機能として共通の鍵を持つため、
マスターとスレーブの端末の組み合わせが変化すると、この状態となります。
（移設や、接続の変更を行う場合は、スレーブ端末は必ずリセットが必要です。）
（スレーブ端末が、DM-20/OM-120/Secure I/O2 の場合は、INIT ボタンを長押ししてください。）
この場合は、一度、スレーブ端末を削除し、リセットした上で、再度、検索・追加を行ってください。
（改めて、リセットの後、新たなるマスター端末の鍵を記録します。）

23.2 端末の設定

端末の設定は、共通部分は多くありますが、機種により多少異なります。
本章では、部分ごとに記載します。

23.2.1 【情報】項目

① 端末の名称を入力できます。端末追加時に、端末種別・端末 ID・IP アドレスから、仮名称が決まります。
設置位置など、自由に名称を変更可能です。

② 端末固有のシリアル番号を表示します。(変更はできません)

③ 端末の内部のファームウェア(プログラム)のバージョンを表示します。新しい端末のプログラムがある場合は、横の「ファームウェアアップグレード」ボタンをクリックし、端末のプログラムのバージョンを更新することが可能です。

④ 端末の内部のカーネル(ベースプログラム)のバージョンを表示します。(ファームウェアと連動し更新されます。)

⑤ 端末の設定値を初期化します。「リセット」ボタンをクリックすると、端末内のユーザーデータと、ログデータ以外は、全て初期化されます。

⑥ 端末の設定値を初期化します。「ネットワーク設定以外」ボタンをクリックすると、端末内のユーザーデータと、ログデータと、端末のネットワーク設定部分以外が初期化されます。

⑦ 日本国内では、(UTC+9:00) でご利用ください。(この設定が初期値の場合、端末の時計表示が 9 時間異なる表示になります。)

⑧ 日本国内では、サマータイムは利用しません。

⑨ 端末グループを作成して管理する場合は、事前に作成したグループから選択してください。

⑩ 端末の種別(機種名)が表示されます。(変更はできません)

⑪ 端末の詳細タイプ(機種詳細)が表示されます。(変更はできません)

⑫ 端末のハードウェアバージョンが表示されます。(変更はできません)

⑬ 詳細設定の「トリガおよび動作」で端末利用不可にした場合(外部入力などの設定によりロックさせることができます。)解除ボタンを押すことで、ロックを解除します。

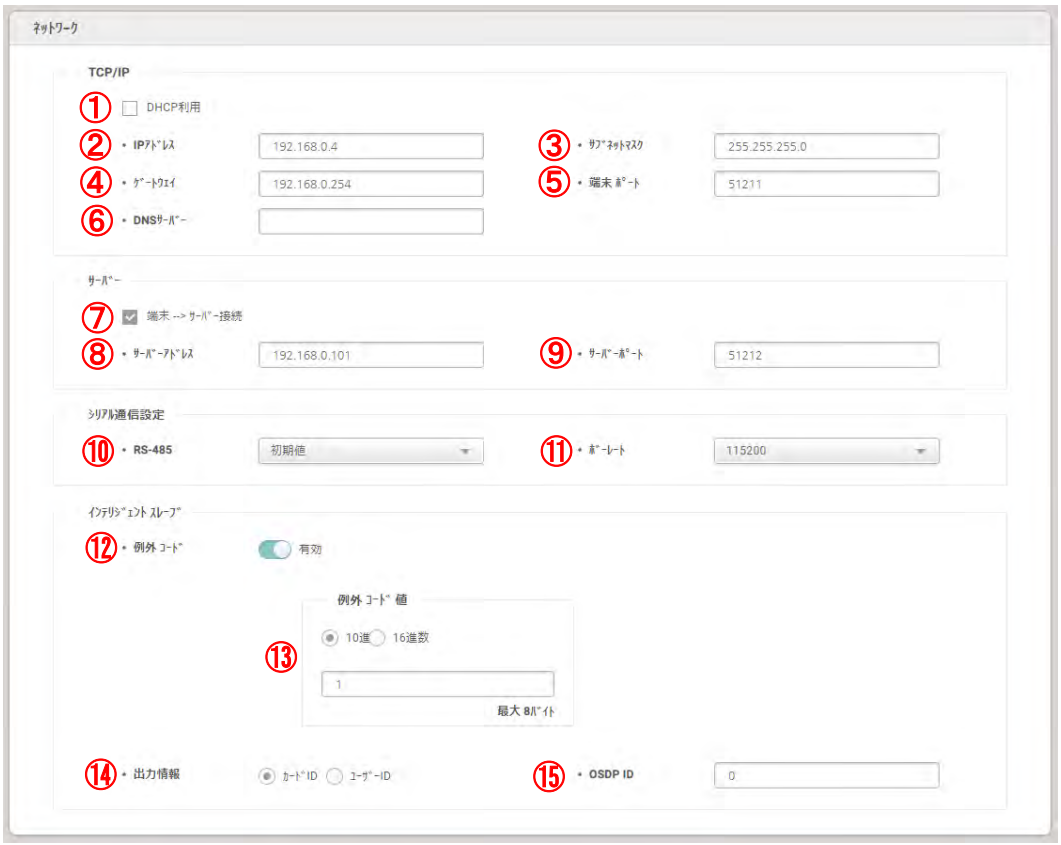
⑭ BioStar2 サーバーPC と端末の時刻を同期させる場合に☑を入れてください。(この☑を入れると、⑮の部分が設定できなくなります。

⑮ 端末の日時を表示します。(⑭で時刻同期に☑している場合は、変更できません。)

⑯ 端末の設定日時を改めて端末から取得します。(⑮の表示を変更した場合など、改めて端末日時を取得しなおします。)

⑰ 端末に⑮の日時を設定します。(⑭で時刻同期に☑している場合は、変更できません。)

23.2.2 【ネットワーク】項目



① 端末のネットワーク設定で、DHCP（自動取得）を利用する場合は、☑を入れてください。（☑した場合は、②③④は、入力できません）

② 端末の IP アドレスを入力してください。

③ 端末のサブネットマスクを入力してください。

④ 端末のゲートウェイを入力してください。

⑤ 端末の PC 側からの待受通信ポート番号（端末側ポート番号）を設定してください。（初期値：51211）

⑥ 端末の DNS サーバーアドレスを入力します。（但し、BioStar2.6 では動作しません。空欄で構いません。）

⑦ 端末から BioStar2 サーバーに通信を開始する場合は、☑を入れてください。

☑を入れることで、⑧⑨が入力可能となります。（端末-- >サーバー接続の内容は以下となります。）

⑧ 端末-- >サーバー接続する場合の接続先サーバーIP アドレスを指定してください。

⑨ 端末-- >サーバー接続する場合の接続先サーバーポート番号を指定してください。（初期値 51212）

⑩ RS-485 接続をする場合に マスター/スレーブ または、初期値を選択してください。
初期値 を選択した場合は、端末側のファームウェアのバージョンが対応している場合、⑫以降が表示され設定可能となります。

⑪ RS-485 の通信速度を指定してください。(通常は 115200 です。通信環境が悪い場合等は下げてご利用ください。)

⑫ インテリジェントスレーブの例外コードを 有効とすると、⑬が表示されます。

⑬ 例外コードを有効にした場合に、その値を、10 進数 または 16 進数で設定します。8 バイトまでの範囲で設定してください。

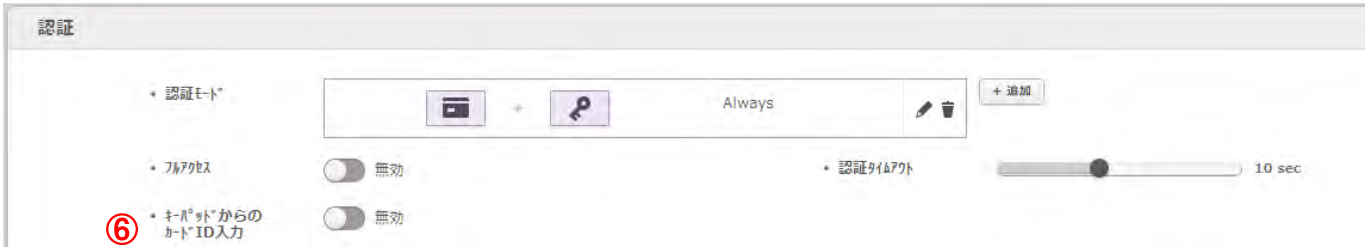
⑭ インテリジェントスレーブの出力情報を カード ID または ユーザーID から選択します。

⑮ OSDP の ID を設定してください。

※インテリジェントスレーブ機能とは、RS-485 を利用し、OSDP のコントローラーの配下に弊社端末を接続します。更に、端末で 1:1 または 1:N の認証を行い、その結果を、サードパーティーのコントローラーに送信する機能です。通常のスレーブ端末と異なり、スレーブ端末が認証を行い、その結果を RS-485 OSDP 経由で出力することが可能となります。

23.2.3 【認証】項目

Xpass2 等の場合



① 端末としての認証方式を選択する場合に利用します。例えば、上図の例の場合、指紋認証のみで認証可能なスケジュールは、Always（常時）であり、カード認証後、指紋を入力する運用も Always（常時）となります。仮にカードをかざしただけで、ドアを開けられるようにしたい場合は、この設定では対応できません。また、矛盾があるような設定も組み合わせられません。（例えば、カードのみでドアが開く設定があるのに、追加で、「カード＋指紋」の方式を追加する。など。これは、カードのみで認証できるので、その後の「＋指紋」の部分が不要という意味です。）

上記例で、変更する場合は、指紋のみでも認証し、カードのみでも認証するパターンが多くなります。つまり、矛盾を避けるためには、カード＋指紋の設定を変更し、カードのみにする。というやり方になります。カード＋指紋の横にあるペンのマークのアイコンをクリックすると、以下の画面が表示されます。

左図は指紋認証機の例ですが、顔認証機の場合は、指紋の代わりに「顔」のアイコンが表示されます。

スケジュールについては、初期値では、Always しかありませんが、スケジュールを作成することで、曜日や時間帯などを指定できます。

② 有効にすると、端末にユーザー情報があるユーザーは認証可能となります。アクセスコントロールで指定した内容ではなく、端末内のユーザー情報のみで認証する。アクセスコントロールを利用せず、端末にユーザー情報があるユーザーは認証 OK とする場合は、こちらを有効にしてください。

③ 端末内のユーザー数が多い場合に、認証に時間がかかるようになりますが、どの時点でタイムアウトするかを選択することができます。（初期値の 5 秒であれば、基本的には変更の必要はありません。）3 秒～20 秒の間で設定できます。

④ サーバーマッチングとは、認証用のユーザーデータを端末に持たず、認証操作の後、サーバーに問い合わせ、認証可否の判断を行います。本機能は、カードと指紋の場合に利用可能です。但し、本機能を利用するためには、AC コントロールライセンスが必要となります。また、サーバーでの認証となりますので、サーバーと通信ができない場合は、全て認証エラーとなります。

⑤ 認証後、顔写真を撮影可能な機種の場合、顔の検知を条件とすることが可能です。その際の検知のレベルを、通常/高/最高から選択してください。(**BioStation A2 のみ**)

⑥ 有効にすると、カードデータを入力することにより認証されます。「カードデータ＋＃」の操作です。

23.2.3.1 【顔認証部分（顔認証端末の画面でのみ表示）】

FaceStation2の場合

① 通常/高/最高から選択します。高や最高にすると、認証するための条件が厳しくなり認証しづらくなる可能性がある代わりに、誤認証として扱ってしまう可能性も減ります。（初期値は、通常 です。）

② 認証機は移動体を捉えると、自動的に顔認証モードになります。このときの移動体と検知するための感度を設定します。オフにすると、自動的には顔認証モードにならなくなります。オフの設定の場合、液晶画面をタップすることにより認証できるようになります

③ 偽装認証を防止するロジックの稼働レベルを設定します。（初期値は、未使用 です。）

④ 有効にした場合、端末でユーザー追加を行う際に、登録顔の重複チェックを行います。BioStar2 からユーザー登録を指示した場合は行いません。

⑤ 顔の登録時にタイムアウトするまでの秒数を設定します。

⑥ 顔認証機を設置する場所の周囲の明るさを調整してください。通常/明るい/自動 から選択してください。

⑦ 簡易顔登録を使用するかどうかを設定します。「有効」に設定すると、1 ステップで登録できます。「無効」に設定すると、3 ステップで登録します。高品質に登録するには「無効」を選択してください。この機能は、FaceStation 2 のみの機能です。

FaceStationF2 の場合

① ①～④および⑥は前項の FaceStation2と同様です。

⑤ 動作モードの高速マッチングかヒュージョンマッチングを選択すます。ヒュージョンマッチングを選択すると、偽顔検出レベルの選択ができます。

23.2.3.2 【指紋認証部分（指紋認証機能を有する端末の画面でのみ表示）】

① 通常/高/最高から選択します。高や最高にすると、認証するための条件が厳しくなり認証しづらくなる可能性がある代わりに、誤認証として扱ってしまう可能性も減ります。（初期値は、通常 です。）

② 指紋センサーの感度を設定します。（初期値は 7（最高）です。）

③ 指紋のテンプレートの種類が表示されます。（推奨は、Suprema です。）

④ 指紋認証後、端末の液晶画面に指紋のイメージ画像を表示するかどうか選択可能です。有効にするとイメージ表示を行います。

⑤ 認証機での指紋登録の際に、登録品質により再度、登録するか？等の拡張登録メッセージが表示されます。

⑥ 指紋登録時、指紋が入力されるまでの待機時間を設定します。（初期値は、10 秒です。）

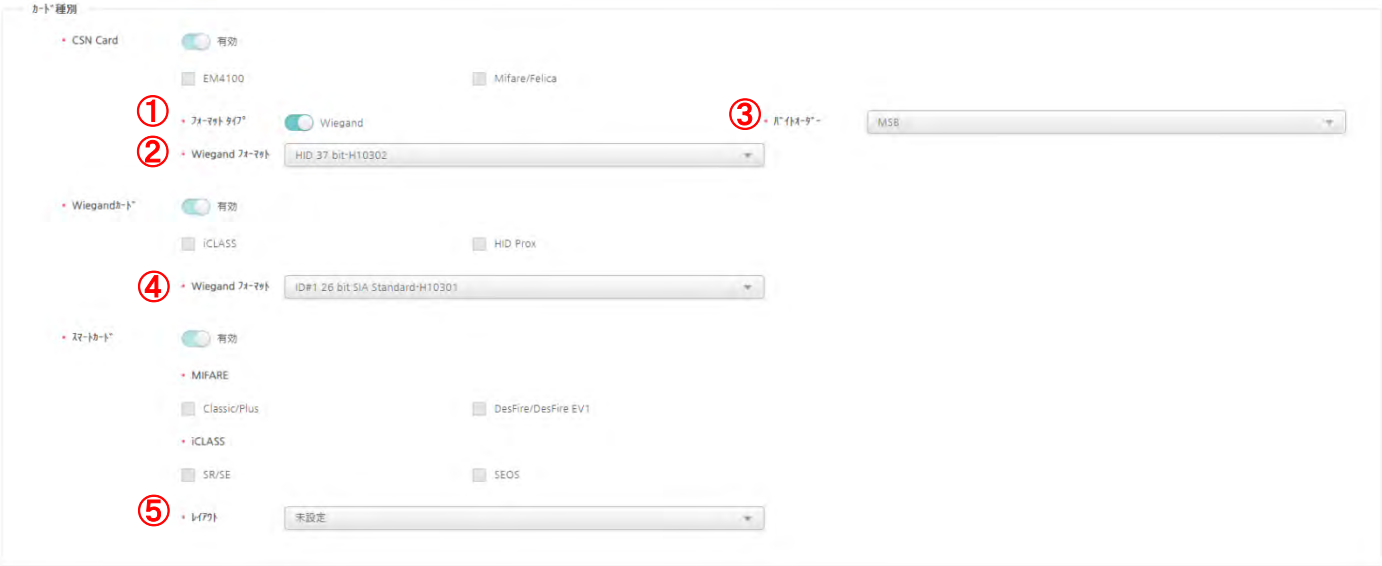
⑦ 1:N 認証の場合の認証速度（指紋の照合速度）を調整できます。（初期値は、 自動です。指紋数により調整されます。）

⑧ 指紋認証後、端末内で指紋を探す処理を行いますが、その処理のタイムアウト時間を設定します。（初期値は、5 秒です。）
認証機に登録されている指紋の数が多い場合は、タイムアウト時間を伸ばしてご利用ください。

⑨ 指紋センサー部を、指を乗せたときに自動 ON にするか、常時 ON にしておくか選択します。（初期値は自動 ON です。）

⑩ 認証機が生体指紋検知機能を持っている場合に設定可能です。認証に少し時間がかかるようになりますが、生体の指紋でないと認証できなくなります。

23.2.3.3 【カード種別部分】



① 通常/Wiegand から選択可能です。カード認証の結果を Wiengand で出力する場合は、Wiengad を選択してください。(Wiegand の設定にしたときは、②の項目が表示され設定可能になります。)

② ①で Wiegand を選択した場合に、Wiegand としての出力フォーマットを指定できます。

③ カード ID をメモリ上のどちらの向きから読み出すかを設定します。BioStar2 の標準は、MSB となります。他のシステムとの整合性を合わせる等の条件がある場合は、変更してください。

④ Wiegand で使用するデータフォーマットを指定します。(弊社の取扱機種では、Wiegand カードは利用できません。)
作成した Wiegand カードフォーマットについては、21.4.1.3 章を参照してください。

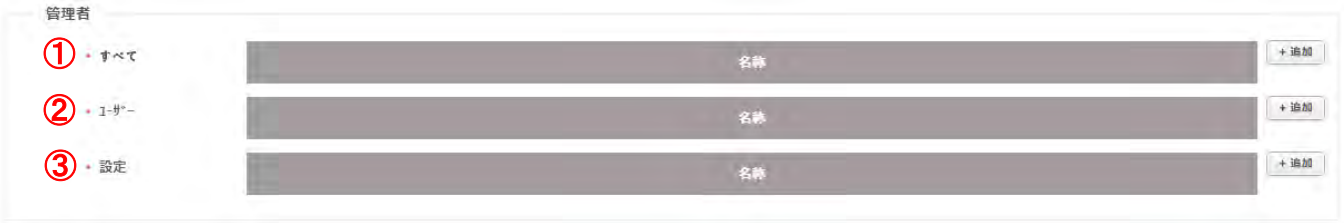
⑤ スマートカードを利用する場合は、スマートカードのフォーマットを作成します。作成したフォーマットを、ここで指定することで、端末で利用できるようになります。通常のカード(Mifare/FeliCa/EM)の場合は、スマートカードでは無いため、ここは未設定としてください。
スマートカードのフォーマット作成については、21.4.2.2 章を参照してください。

23.2.4 【詳細設定】項目

詳細設定の項目は、端末の設定画面に入った直後は、縮小表示されている状態です。

上記、赤枠内の部分をクリックし、表示を拡張してください。

23.2.4.1 【管理者部分】



① 認証機の端末メニューの管理者を設定します。「すべて」の項目の管理者を最初に登録してください。「＋追加」ボタンでユーザーを選択することで登録することができます。ここで管理者を1人でも登録することで、端末のメニュー画面にロックが掛かります。メニュー画面に進むためには、端末の指示に従い、管理者の方が認証してください。最大 1,000 人の管理者を追加および管理できます。

② ①の部分で管理者が指定された上で、効果があります。(①が空欄の場合は、②だけ指定しても意味がありません。)②で指定したユーザーは、認証機の「ユーザー」「ｲﾍﾞﾝﾄﾛｸﾞ」のメニューにのみアクセス可能となります。「＋追加」ボタンでユーザーを選択することで登録することができます。なお、ここで設定したユーザーの管理者は、同レベルの「ユーザー」の管理者ユーザー および、「設定」の管理者ユーザーについては、ユーザー情報を更新することができません。
管理者であるユーザーのユーザー情報を変更する場合は、「すべて」の管理者ユーザーである必要があります。

③ ①の部分で管理者が指定された上で、効果があります。(①が空欄の場合は、③だけ指定しても意味がありません。)③で指定したユーザーは、認証機の「ユーザー」以外のメニューにアクセス可能となります。「＋追加」ボタンでユーザーを選択することで登録することができます。

※各管理者は、1000 名まで指定可能です。

23.2.4.2 【勤怠部分】

① 勤怠としても利用する場合、端末側の勤怠の設定が可能です。 未使用/ユーザー選択/スケジュール/最終選択内容/固定 から選択することが可能です。選択により②③の表示が変化します。

② ①が、「ユーザー選択」 の場合に表示されます。勤怠の必須入力が、「未使用」の場合は、勤怠の内容を選択せずとも認証するとドアを開くことが可能です。但し、勤怠のイベントの入力忘れ が発生する可能性があります。勤怠の必須入力を「使用」にした場合は、認証と勤怠の入力が揃った時点でドアを開くことができるようになります。(先に認証をした場合は、すぐにドアは開かず、勤怠イベントを入力する画面に遷移します。)

③ 勤怠イベントは、①の選択により設定項目が変化します。以下で、それぞれの場合の説明を致します。

[ユーザー選択] および [最終選択内容]

各勤怠イベントボタンの文字をどう表示するかを設定することができます。それぞれのボタンの内部処理の種類は、別途勤怠の設定画面で設定します。

[スケジュール]

各勤怠イベントボタンの文字の表示内容と、そのイベントボタンと認識するスケジュールを指定します。上記の例の場合、作成したスケジュールの「午前中」という時間帯は、Code1：出勤となり、「午後」の時間帯は、Code：2 退勤となります。

スケジュール内の時間が重複しないようにしてください。

［固定］

勤怠モードを「固定」にした場合は、どのファンクションキーで固定とするかを選択します。また、各種ボタンの表示内容を選択します。

23.2.4.3 【表示/音声部分】

表示/音声の部分については、液晶を装備する認証機と液晶の無い認証機で大きく異なります。それぞれ記載します。

［液晶あり認証機］

① 認証機の言語を変更可能です。日本語は、「カスタム」になります。バージョンアップ等で、英語版に戻った場合は、再度、「リソースアップデート」ボタンから、新しい日本語化のリソースファイルを指定し、日本語に戻す必要があります。

② 認証機の効果音のボリュームを変更します。

③ 認証機で操作をしていない場合の液晶画面のバックライトを消灯させる時間を変更可能です。

④ スクリーンセーバー機能の有無を設定します。端末を使用していないときに LCD 画面の輝度を下げることで、不要なエネルギー消費を削減します。

（FaceStation 2 および FaceStation F 2 のみ）

⑤ 有効にすると、英語の音声ガイダンスが発話されます。無効にすると、代わりに効果音が鳴ります。

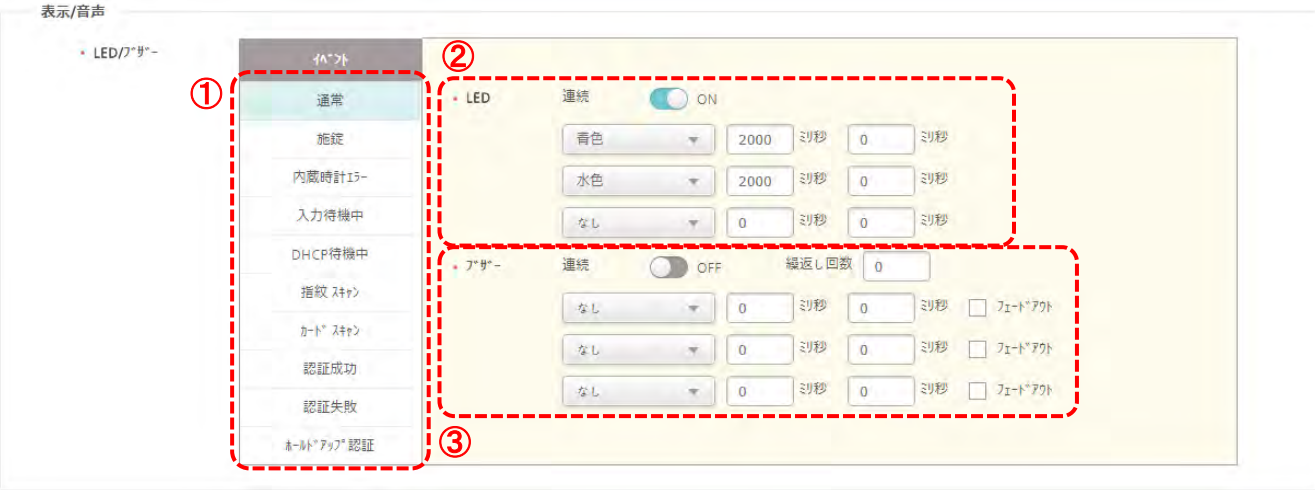
⑥ 認証機の待機画面の表示を変更できます。「通常」を選択すると、初期値の画面が表示されます。「ロゴ」を選択すると背景画像が選択可能です。また、スライドショーの機能も利用可能です。「お知らせ」を選択すると、簡易メッセージを入力することが可能です。

⑦ 認証機の起動時の効果音と、認証成功時の効果音と認証失敗時の効果音を選択することが可能です。変更する場合は、一度ファイルを選択し、その後、下の「更新」をクリックした後、画面下部の「適用」をクリックしてください。

⑧ 認証機で操作をしていない場合に、メニュー画面から待機画面に自動的に戻るまでの時間を設定できます。

⑨ 認証成功や、認証失敗など、イベントによりメッセージが表示されます。そのメッセージが消え、待機画面に戻るまでの時間を設定できます。

［液晶なし認証機］



液晶なしの認証機では、各イベントの際に、LED の色や点灯間隔、ブザーの音階や時間を変更することができます。

① 発生イベントに合わせて、変更が必要な内容を選択します。クリックすると、その時点で設定されている内容が、画面右側に表示されます。

② ①で設定したイベントに対し、状態 LED の色を指定することが可能です。

色の変化を連続で繰り返すか、繰返し回数を設定します。3 段階まで色と秒数を指定します。また、その後の LED の OFF 時間を指定します。上記の例の場合、LED は、繰返しを連続として、

青の点灯が 2000 ミリ秒 その後の OFF は、0 ミリ秒（つまり OFF 時間は無し）

水色の点灯が 2000 ミリ秒 その後の OFF は、0 ミリ秒（つまり OFF 時間は無し）

3 色目は、無し

結果として、青 2000 ミリ秒/水色 2000 ミリ秒の点灯を繰返します。

③ ①で設定したイベントに対し、ブザーの音を指定することが可能です。（通常 のイベントは、音は鳴らないため、認証成功の音を参考にします。）

認証成功時は、ブザーの連続は、OFF で、繰返しを 1 回としています。

低音階が 200 ミリ秒 その後の OFF は、0 ミリ秒（つまり OFF 時間は無し） フェートアウト有り

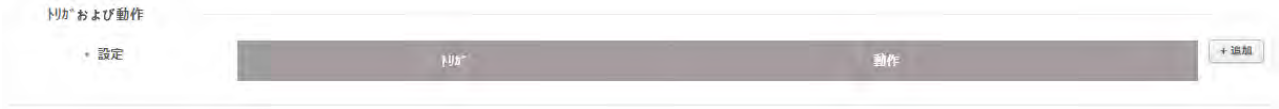
中音階が 200 ミリ秒 その後の OFF は、0 ミリ秒（つまり OFF 時間は無し） フェードアウト有り

高音階が 1000 ミリ秒 その後の OFF は、0 ミリ秒（つまり OFF 時間は無し） フェードアウト有り

結果として、認証成功時は、♪ ピロリーン と鳴ります。

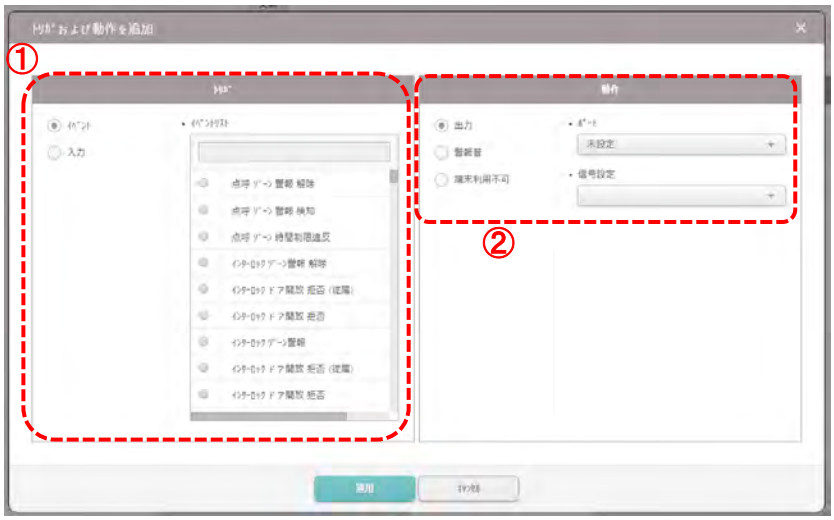
23.2.4.4 【トリガおよび動作部分】

端末で、指定したイベントが発生した場合や、端末の入力信号線を検知した場合に、端末に動作を行わせることができます。



動作を追加する場合は、右側の「＋追加」をクリックし、追加していきます。

クリックすると以下の画面が表示されます。



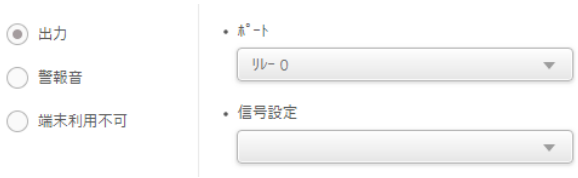
① トリガを、「イベント」または「入力」を選択します。まずは、「イベント」を選択した場合について記載します。

イベントを選ぶと、次に、何のイベントが発生したときかを選択します。

② 次に、①のイベントが発生した場合の動作を以下から選択します。

・出力　　:その端末（または端末に接続されている拡張 I/O ユニット）のリレーから、接点の出力を行います。

出力するリレーポートと、信号を設定・選択可能です。

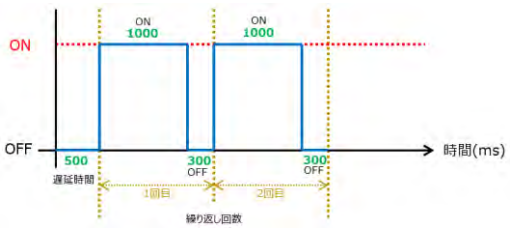


信号設定については、作成済みのものを選択するか、新規に作成する場合は、「＋シグナルの追加」を選択してください。

追加する場合は、以下の画面が表示されます。

追加後、「適用」をクリックし、選択してください。

左図の信号の場合は、以下のような動きになります。

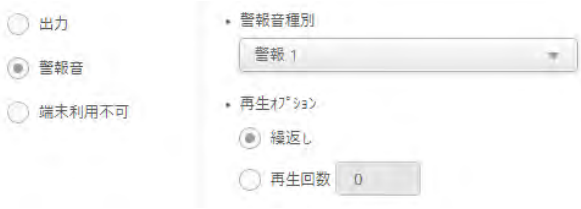


注意：リレースイッチは最終状態を維持しますので、例えば、OFF：0 ミリ秒　の指定をすると、その前の ON の状態が継続されてしまいます。

最終を OFF にするシグナルの場合は、10 ミリ秒程度は、OFF の信号を出力してください。

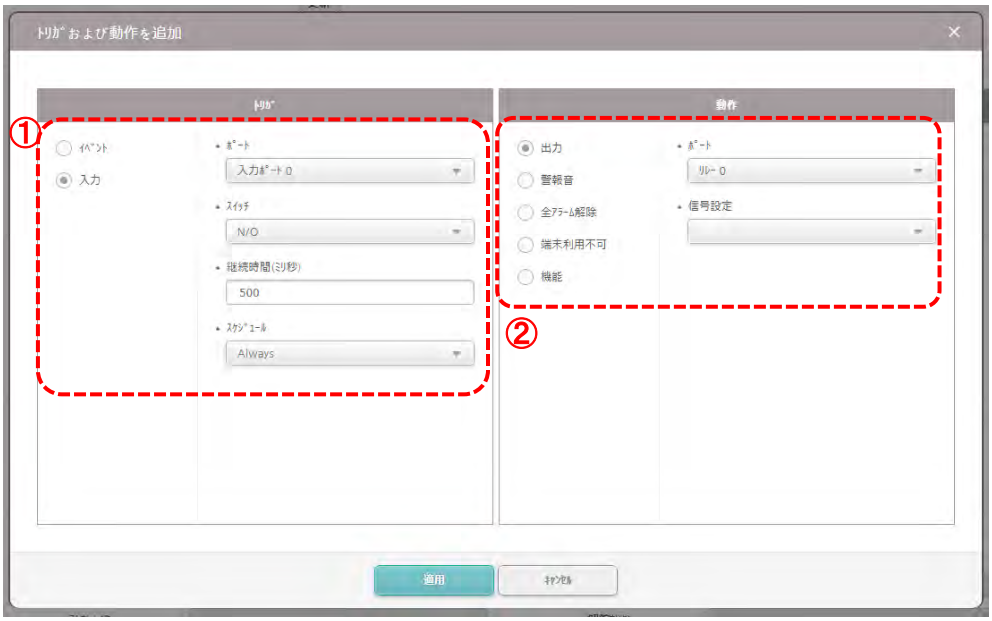
また、出力回数で 0 を指定すると、リレー出力を繰り返します。

・警報音　　：その端末から警告音を鳴らします。出力する警告音の種別と警告音の再生条件（繰り返しか回数指定か）を指定します。



・端末利用不可　：この端末が使用不可となりロックします。
ロックを解除する場合は、端末の設定の「端末操作ロック」から行ってください。

次に、①の部分で、「入力」を選んだ場合は、以下の画面となります。



①　トリガを、「イベント」または「入力」を選択します。「入力」を選択した場合について記載します。
入力を選んだ場合は、入力を検知するポート番号、入力を検知するための相手側のスイッチ状態、検知と扱う秒数、検知をする時間帯を設定します。

②　次に、①のイベントが発生した場合の動作を以下から選択します。

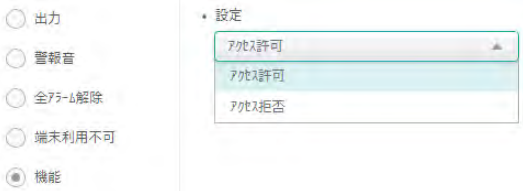
・出力　　：その端末（または端末に接続されている拡張 I/O ユニット）のリレーから、接点の出力を行います。
前ページのイベント発生時の出力と同様です。

・警報音　　：その端末から警告音を鳴らします。出力する警告音の種別と警告音の再生条件（繰り返しか回数指定か）を指定します。
前ページのイベント発生時の警報音と同様です。

・全アラーム解除　：端末で発生しているアラームがあった場合に、それらを解除します。

・端末利用不可　：この端末が使用不可となりロックします。
前項のイベント発生時の端末利用不可と同様です。

・機能　　：端末で、アクセス許可（認証成功）とアクセス拒否（認証失敗）の画面および音声を表示します。



23.2.4.5 【イメージログ部分】

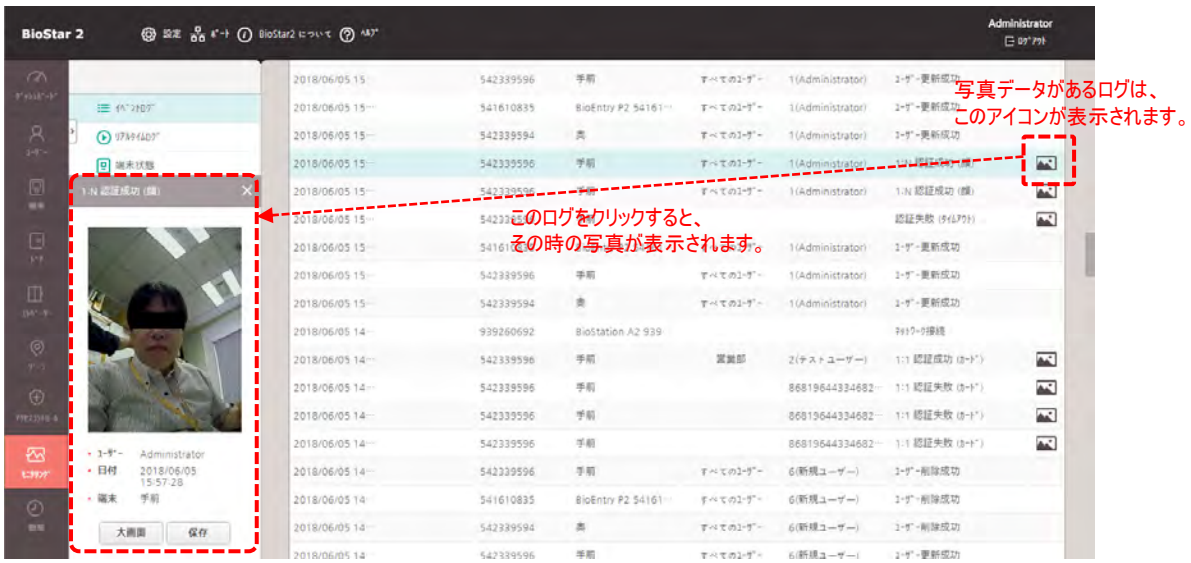
認証時撮影用のカメラが内蔵された機種の場合、カメラ撮影するイベントを選択可能です。

① 認証時や、認証失敗時など、それぞれのイベント発生時に、その時の写真を撮影する場合は、イメージログを有効にしてください。

②の内容が表示されます。

② 写真を撮影するイベントを、追加・削除・スケジュールの変更が可能です。

撮影したデータは、モニタリング画面で確認できます。



23.2.4.6 【Wiegand 部分】

Wiegand 規格で他のメーカーの端末と接続した場合に利用することが可能です。

① 認証機を Wiegand の入力/出力 どちらとして利用するかを設定します。

② 入力として利用する場合に、入力のフォーマットを選択します。相手側出力端末と合わせてください。

個別にフォーマットを作成する場合は、設定 → カードフォーマット で作成してください。

③ 出力する場合のモードを選択してください。「通常」を選ぶと、フェールコードの値を選択できるようになります。

フェールコードの値は、0x00 か、0xFF から選択可能です。

出力されるフォーマットは、23.2.3.3 の②の Wiengand フォーマットに沿って出力されます。もし、未設定の場合は、標準の 26bit フォーマットに沿って出力されます。

また、「バイパス」を選択すると、読み込ませたカード ID が出力されます。

④ Wiegand 通信仕様のパラメーターです。相手側機器と同じ値に設定してください。

（20～100μ秒の範囲で設定可能です。）

⑤ Wiegand 通信仕様のパラメーターです。相手側機器と同じ値に設定してください。

（200～20000μ秒の範囲で設定可能です。）

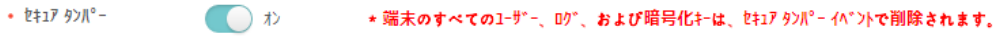
⑥ 認証したユーザーの所持する先頭のカード ID を出力するか、認証したユーザーのユーザーID を出力するかを選択します。

23.2.4.7 【インターフォン部分】

対応する SIP サーバーが限られているため、弊社としては未サポートとなります。

23.2.4.8 【セキュア タンパー部分】

セキュアタンパー機能のオン/オフが切替可能です。(対応端末のみ)



本機能を「オン」にした場合、端末を取り外しタンパー機能が動作すると、

・端末本体内部のユーザーデータ

・端末本体内部のログデータ

・端末の暗号化キー

が、削除されます。

もし、端末のメンテナンス等で端末を外す場合は、注意してください。

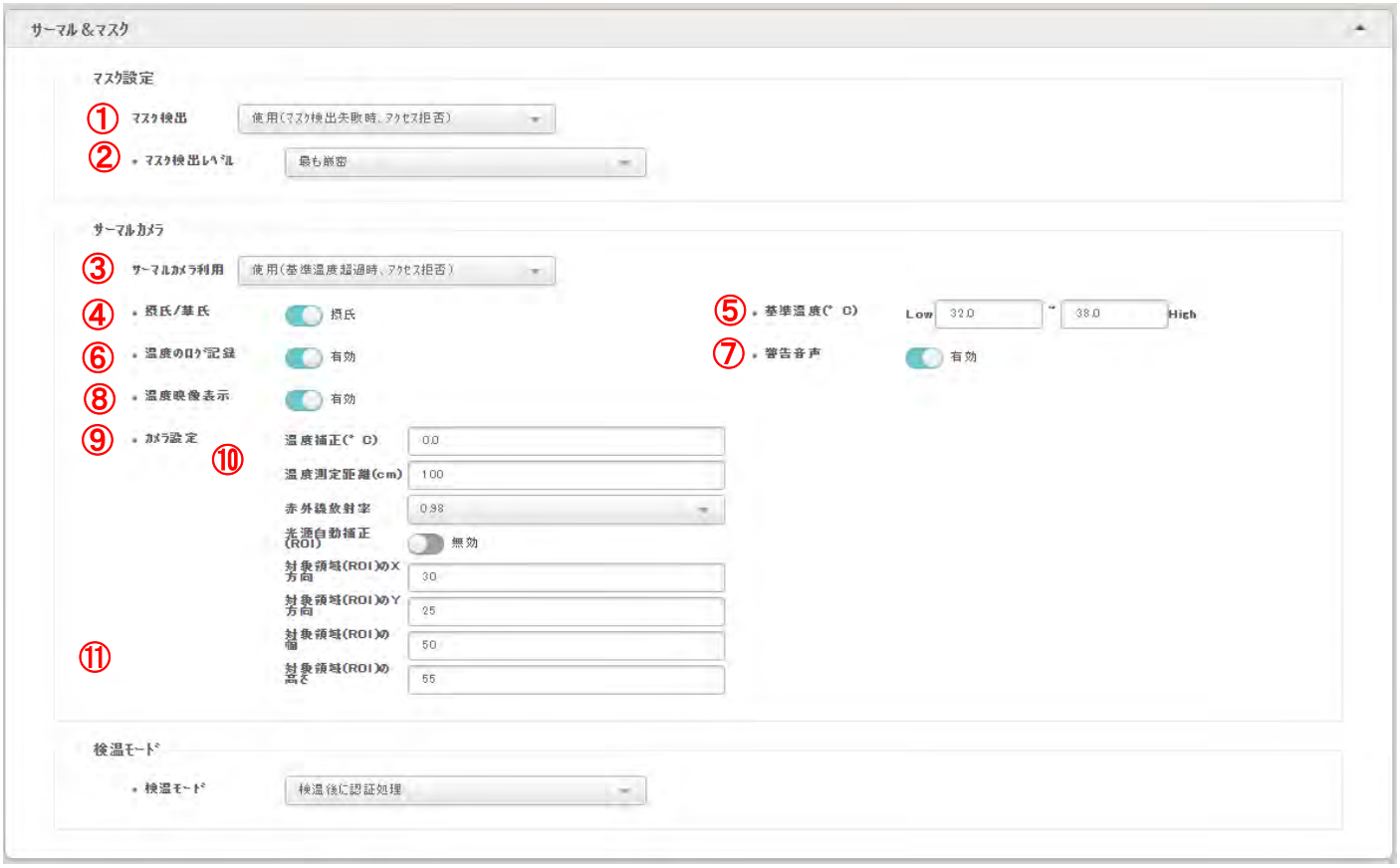
23.2.5 【サーマル＆マスク】項目

サーマルカメラの詳細設定を行ないます。

顔認識デバイスを備えたサーマルカメラは、アクセスポイントを通過するユーザーの温度を測定し、設定されたしきい値より

高い温度のユーザーのアクセスを制限します。また、FaceStationF2 は、マスクを検出し、マスクのないユーザーへのアクセスを制限することもできる。

FaceStationF2 の設定画面



① マスク検出機能を使用するかどうか設定をします。「使用(マスク検出失敗時、アクセス拒否)」を選択すると、マスクを着けていないユーザーの認証を拒否します。「使用(マスク検出失敗時、アクセス可)」を選択すると、マスクを着けていないユーザーも認証できます。イベントログに「マスク未検出」と認証成功が記録されます。

② マスク検出の感度を厳密/より厳密/最も厳密から設定します。

③ サーマルカメラを使用するかどうかを設定します。「使用（基準温度超過時、アクセス拒否）」を選択すると、設定した基準温度より高い温度ユーザーの認証を拒否します。「使用（基準温度超過時、アクセス可）」を選択すると、設定された基準温度よりも高い温度のユーザーも認証できます。イベントログに「異常温度検出(基準温度超過)」と認証成功が記録されます。

④ 温度の単位を変更します。

⑤ アクセス等を制限する温度の上限下限を設定します。検出された温度が基準温度の範囲外のユーザーはアクセス等を制限することができます。

⑥ 温度データを保存するか、しないかの設定を行ないます。「無効」を選択するとイベントログにも保存されません。

⑦ 「有効」に設定すると端末から「Exceeded Threshold temperature」とメッセージが流れます。無効の場合は、「認証失敗音」が流れます。

⑧ 「有効」に設定すると端末の液晶画面に赤外線の温度計測イメージを表示します。

⑨ 正確に測定するために、サーマルカメラの設定を行ないます。

・温度補正： 端末の使用環境に応じて、測定温度を補正します。(-5.0℃から 5.0℃までの数値が入力できます)

・温度測定距離： ユーザーと端末の温度測定距離を 50cmから 130cmの間で設定できます。

・赤外線放射率： 0.95/0.97/0.98 から選択します。人間の皮膚からの放射率は 0.98 に設定するのが一般的です。

・光線自動補正（ROI） ⑩を無効に設定すると、ROI の値を手動で設定できるようになります。

⑪ 検温モードの設定を行ないます。

・認証処理後に検温：

FaceStation2の画面

① サーマルカメラを使用するかどうかを設定します。「使用（基準温度超過時、アクセス拒否）」を選択すると、設定した基準温度より高い温度ユーザーの認証を拒否します。「使用（基準温度超過時、アクセス可）」を選択すると、設定された基準温度よりも高い温度のユーザーも認証できます。イベントログに「異常温度検出(基準温度超過)」と認証成功が記録されます。

② 温度の単位を変更します。

③ アクセス等を制限する温度を設定します。検出された温度が基準温度より高いユーザはアクセス等を制限することができます。

④ 温度データを保存するか、しないかの設定を行ないます。「無効」を選択するとイベントログにも保存されません。

⑤ 「有効」に設定すると端末から「Exceeded Threshold temperature」とメッセージが流れます。無効の場合は、「認証失敗音」が流れます。

⑥ 「有効」に設定すると端末の液晶画面に赤外線の温度計測イメージを表示します。

⑦ 正確に測定するために、サーマルカメラの設定を行ないます。

・温度補正： 端末の使用環境に応じて、測定温度を補正します。(-5.0℃から 5.0℃までの数値が入力できます)

・温度測定距離： ユーザーと端末の温度測定距離を 50cmから 130cmの間で設定できます。

・赤外線放射率： 0.95/0.97/0.98 から選択します。人間の皮膚からの放射率は 0.98 に設定するのが一般的です。

・光線自動補正(ROI)の値を設定します。

30 25 50 55

47 45 15 10

23.3 端末の再接続

端末の接続モードが、「サーバー --->端末」に設定されている場合、接続情報を更新しないと、端末が切断された状態の場合があります。このような場合は、端末の再接続をすることで、接続情報を再接続することが可能です。

説明図	操作内容
	① 「端末」メニューをクリックし、端末画面にしてください。 ② 再接続したい端末を右クリックしてください。 ③ 「再接続」を選択してください。 ※再接続が選択できるのは、LAN 接続の端末のみです。RS-485 の子機は、再接続の必要はありません。

23.4 端末別ユーザー情報の整理

基本的には、PC のユーザー情報と、端末のユーザー情報は同期していますが、例えば、液晶付きの端末から、端末のメニューを利用してユーザー情報を追加した場合など、PC 側とのユーザー情報にズレが発生する場合があります。
このような場合に、各端末のその時点のユーザー情報を確認することが可能です。
また、そこからの操作も可能です。（本内容については、5.2 章を参照してください。）

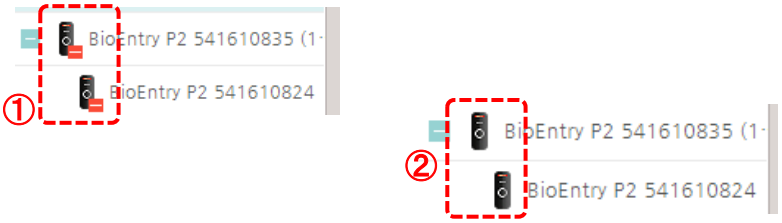
23.5 端末の同期

PC 側で管理している端末の情報（ユーザー情報や、端末設定情報、アクセスコントロール情報等）と、実際に端末にある情報を一致させる場合に利用します。

説明図	操作内容
	① 「端末」メニューをクリックし、端末画面にしてください。 ② 同期が取れていない端末は、端末にオレンジ色の三角の！マークが表示されます。
 	[同期する端末が 1 台の場合]（左図） ① 同期したい端末を右クリックしてください。 ② 「端末と同期」をクリックしてください。 ※一度、端末内ユーザー情報を削除してから同期する場合は、「データ削除＆端末同期」をクリックしてください。 [同期する端末が複数台の場合]（右図） ③ 同期したい端末に☑をいれてください。 ④ 表示される「端末と同期」ボタンをクリックしてください。
	① 同期の結果が表示されます。確認後、「OK」ボタンをクリックしてください。
	① 端末の同期エラーマークが解除されます。

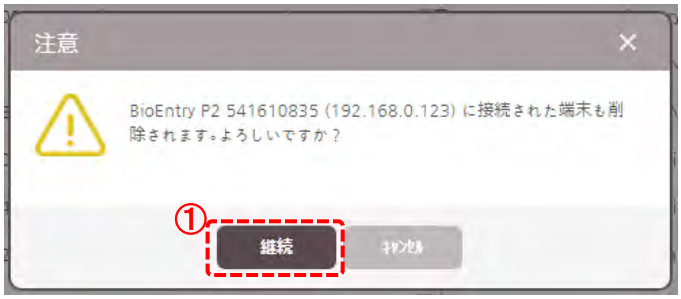
23.6 端末の再起動

BioStar2 管理ソフトから、端末を再起動する場合は、以下の操作を行ってください。

説明図	操作内容
	① 「端末」メニューをクリックし、端末画面にしてください。 ② 再起動したい端末を右クリックしてください。 ③ 「端末の再起動」を選択してください。
	① 端末の再起動中は、進入禁止マークが表示されます。 ② 再起動が完了すると、端末との接続が回復します。

23.7 端末の削除

管理ソフト上、不要となった端末は、削除することができます。しかし、端末を削除するためには、その端末が設定上、フリー状態である必要があるため、削除する前に、ドアへの関連性を無くす必要があります。

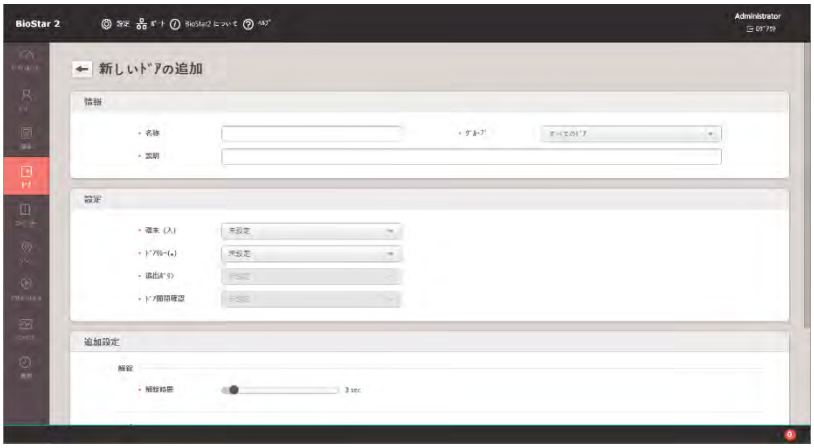
説明図	操作内容
	① 「端末」メニューをクリックし、端末画面にしてください。 ② 削除したい端末を右クリックしてください。 ③ 「端末を削除」を選択してください。
	① 確認画面が表示されたら、「継続」ボタンをクリックしてください。
	① 削除に成功すると、左図の画面が表示されます。「OK」をクリックし画面を閉じてください。
	① ドアの設定が残っていると、左図の上のエラーが表示されます。その場合は、「OK」をクリックして画面を閉じてください。 ② 「ドア」メニューをクリックし、ドアの一覧を表示します。 ③ 該当の端末が使われているドアを見つけ、ドアを削除し、再度、端末削除を行ってください。

24 ドアの設定

ドアの設定について、最初に、ドアの追加方法について記載します。

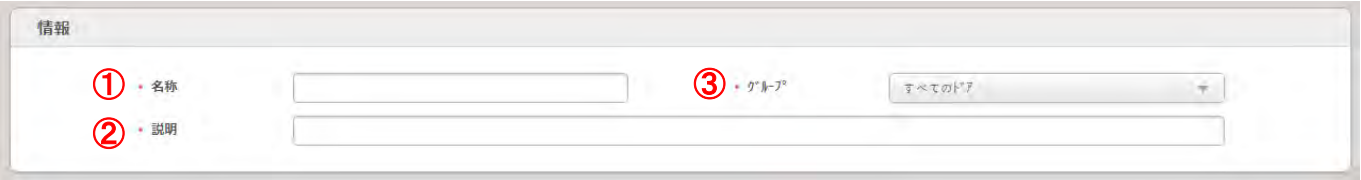
また、その後、部分ごとに記載します。

24.1 ドアの追加

説明図	操作内容
	① 「ドア」メニューをクリックし、ドア画面にしてください。 ② 「ドアの追加」をクリックしてください。
	ドアの追加画面が表示されます。

ドアの設定画面の各項目については、次ページ以降で、部分ごとに記載します。

【情報】項目



① ドアの名称を入力します。区別するための名称ですので、なるべくわかりやすい名称を入力してください。（大会議室入口　など）

② 備考欄です。空欄でも構いません。（メモ欄とお考えください。）

③ ドアをグループ管理する場合は、事前に作成しておくドアグループから選択してください。

※なおドアグループの作成方法は、3 章のユーザーグループの作成を参考にしてください。

【設定】項目

① ドアに入る側の端末を選択してください。（RS-485 接続の親機を選択すると、②の項目が表示されます。）

② ドアから出る側の端末を選択してください。（①の親機に子機として接続されている端末から選択してください。）

③ どの端末をドアのリレーにするか選択します。親機に接続されている機器のすべてのリレーから選択可能です。

④ 退出ボタンを設定する場合は、退出ボタンが接続される端末と、その入力チャンネルを指定してください。

未設定以外を選択すると、⑤項目が表示されます。

※退出ボタンを利用されない場合は、「未設定」を選択してください。

⑤ ④で利用する退出ボタンの種類を、N/O または、N/C から選択してください。

退出ボタンを押したときに、入力信号線がショートするタイプのボタンの場合は、N/O を選択してください。

退出ボタンを押したときに、ショートしていた入力信号線が、ショート解除状態となるタイプのボタンの場合は、N/C を選択してください。

⑥ ドア開閉確認のため信号線を接続する端末と、その入力チャンネルを指定してください。

未設定以外を選択すると、⑦項目が表示されます。

※ドア開閉確認を利用されない場合は、「未設定」を選択してください。

⑦ ⑥で利用するドアの開閉確認のセンサーの種類を、N/O または、N/C から選択してください。

ドアを閉めた状態の時に、センサーの信号線がショートした状態になるセンサーの場合は、N/C を選択してください。

ドアを閉めた状態の時に、センサーの信号線がショート解除状態となるセンサーの場合は、N/O を選択してください。

⑧ 通行確認 APB 機能を利用時は、ON にしてください。ドアセンサーの情報を元に、該当端末は、APB の状態判断を行います。

本設定を ON にした場合は、認証をしてもドアを開けない限り、該当者が通行したと判断しません。

【追加設定】項目

① 設定項目③で指定したドアリレーを、認証成功時に何秒間動かすか？を設定します。（初期値は 3 秒です。）
認証する端末から、ドアまでの距離に応じて変更してください。

② 設定項目⑥のドア開閉確認を指定すると表示されます。ドアを閉じた時に、すぐに施錠するかどうかを設定します。
例えば、①で、ドアの解錠時間を 10 秒に設定していた場合、本設定を「ON」としていると、認証成功から 10 秒未満で、ドアの開閉があった場合、その時点でドアリレーが OFF になります。（必ずしも、解錠時間の 10 秒を解錠しているわけではなくなります。）
本設定を「OFF」にした場合は、認証成功から 10 秒間は、ドアリレーが ON のままとなりますので、認証成功から 10 秒間の間は、何度でも、ドアの開閉が可能です。（また、本項目を ON とすると、③が非表示となります。）

③ 設定項目⑥のドア開閉確認を指定し、且つ②が「OFF」の場合に表示されます。例えば、①で、ドアの解錠時間を 10 秒に設定していた場合、本設定を「ON」にすると、認証成功から 10 秒経過した時点で、仮にドアが開きっぱなしだとしても、ドアリレーを OFF にします。本設定を「OFF」にした場合は、解錠時間が 10 秒に設定されていても、ドアを閉めるまでは、ドアリレーが ON のままとなります。

④ 二重認証をどちら側の端末で利用するかを設定します。（利用しない/入る側/出る側 の 3 択です。もし、両側で利用する場合は、入/出の端末をそれぞれ LAN 接続とし、それぞれのドア設定の入側として指定してください。）
なお、二重認証とは、「カード＋指紋」などの 2 種類の認証と言う意味ではなく、「A さんの後の B さん」のような 2 人認証のことを指します。

⑤ 未設定/2 回目指定 から選択します。「未設定」を選択した場合は、認証許可を持つユーザーの中から 2 人の認証となります。順番は問いません。「2 回目指定」を選択した場合は、⑥が表示され、2 回目のユーザーグループを指定することになります。利用例としては、「1 人目の認証は誰でも良いが、2 人目は、課長職以上」のような利用方法が挙げられます。

⑥ ⑤で 2 回目指定をした場合に、表示されます。事前に作成したユーザーグループから 2 回目として設定するユーザーグループを選択してください。

⑦ 二重認証での認証方法を利用するスケジュールを選択してください。

⑧ 1 人目が認証してから、2 人目が認証するまでの二重とみなすタイムアウト時間を指定してください。

⑨ 共連れを検知に使用する端末を指定します。
但し、共連れ検知機能の対応機種は、BioStar2 用機種のみとなります。
XPass Slim S2 V2 や、BioLite Net V2 は、対応しません。

⑩ ⑨で利用する共連れセンサーの種類を、N/O または、N/C から選択してください。
共連れを検知した時に、センサーの信号線がショートした状態になるセンサーの場合は、N/C を選択してください。
共連れを検知した時に、センサーの信号線がショート解除状態となるセンサーの場合は、N/O を選択してください。

【アンチパスバック】項目

アンチパスバックとは、各ユーザーが、入る側/出る側に順番に認証しないといけないルールの機能となります。

ドア単位でのアンチパスバックを指定することができます。本項目で設定できるアンチパスバックは、ゾーンのアンチパスバックではなく、ドア単位のアンチパスバックとなります。本項目自体が表示されるためには、LAN 接続の親機と、RS-485 接続の子機が、入側/出側の端末として設定されており、どちらかの機種のリレースイッチがドアリレーに設定されている必要があります。

① 利用しない/ソフト APB/ハード APB から選択してください。

アンチパスバックを利用しない場合は、「利用しない」を選択してください。ソフト APB またはハード APB を選択した場合は、②項目が表示されます。ソフト APB とは、システム上はアンチパスバックの判断をしますが、利用者にとっては認証成功となり通常通りドアが開きます。但し、システムのログとしては、ソフト APB の違反として記録されます。(どのくらいのユーザーがアンチパスバック違反をするか？を調べたい時などに利用します。

ハード APB とは、システム上のログも残しますし、アンチパスバック違反の場合エラー表示としてドアが開きません。

② アンチパスバックの解除時間を設定します。

初期値の 1440 分は、24 時間分となります。この設定の場合は、APB エラーとなっても、翌日(24 時間以降後)認証すれば通れる。となります。

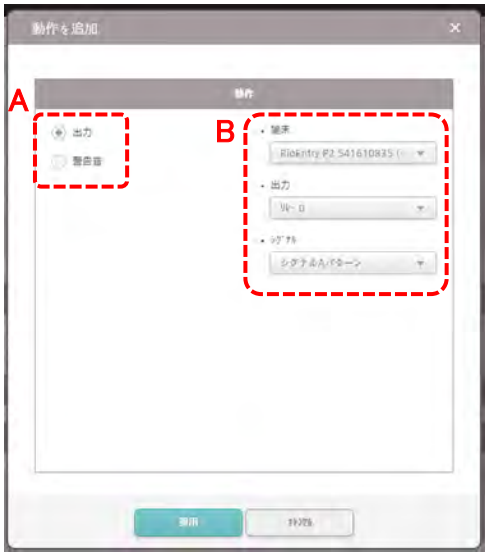
もし、完全にアンチパスバックを行う場合は、0 分を指定してください。この場合は、システムからリセットするまでは、アンチパスバックが有効のままとなります。

また、本項目は、通常ライセンスの簡易アンチパスバックとなります。このため、全ユーザーが対象となります。(管理者だけは除外。や、登録者は除外。等はできません。)

【警報】項目

本項目では、ドア開放や、認証なしドアオープン、アンチパスバックの違反等が発生した場合に、警報を行う設定をすることが可能です。項目はドアの開閉信号により対応可能なものなので、設定項目の⑥のドアの開閉確認を設定した場合に表示されます。

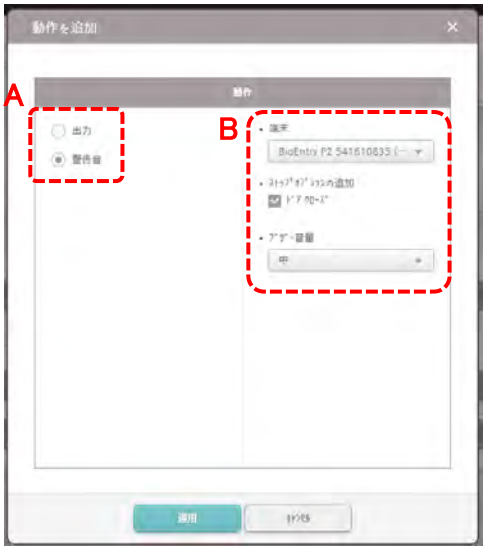
① ドア開放とは、ドアを閉めずに開けっ放しにしていた場合に、その旨を通知する機能です。②の秒数と合わせ、設定します。
このドア開放を検知した際に、どのような動作をさせるかを設定することが可能です。
初期値では、ドア開放が発生した時は、特別な動作はせず、BioStar2 にログインしている場合にのみ、警告ダイアログが表示されます。
警告ダイアログ以外の通知を行いたい場合は、ドア開放発生時の警報動作を追加することができます。
追加する場合は、右側の「＋追加」ボタンをクリックしてください。以下の画面が表示されます。



A の部分では、端末の動作を選択します。「出力」か「警告音」から選択します。
「出力」を選択した場合は、B の部分で、

・どの端末の？
・どのリレースイッチチャンネルを利用して？
・どのシグナルを出力するか？

を選択します。シグナルについては、23.2 章 端末設定 の「トリガおよび動作」を参照してください。



A の部分で、「警告音」を選択した場合は、B の部分で、

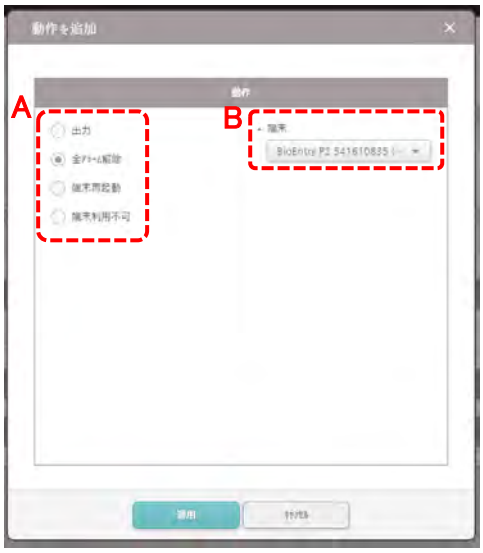
・どの端末から？
・警告音のストップ条件として、ドアクローズにするか？
・警告音の音量は？

を選択します。ストップ条件のドアクローズに☑を入れない場合は、ドア開放の警告音が鳴った際に、ドアを閉じても警告音が鳴り止みません。
停止するためには、BioStar2 管理ソフトから停止する必要があります。

② ドア開放と検知するまでの秒数を指定します。

③ 認証せずにドアが開いた場合や、出口ボタンを押さずにドアが開いた場合は、端末から見てドアを開けていないのにドアが開けられた。と判断し、「認証なしドアオープン」の発生を検知します。認証なしドアオープンの発生時も、ドア開放と同様にリレースイッチからシグナルを出力したり、端末から音声を鳴らしたりすることが可能です。認証なしドアオープン時の警報動作を追加する場合は、右の「＋追加」をクリックしてください。
表示される画面と、その設定方法はドア開放の時と同様のため、ドア開放の設定を参照してください。

④ アンチパスバックの違反発生時に動作を設定することが可能です。アンチパスバック違反の際に行う動作は、右の「＋追加」から指定可能です。



A 部分で、「出力」を選択した場合は、ドア開放の場合と同様です。
A 部分で、「全アラーム解除」を選択した場合は、B 部分で
・どの端末の全アラームを解除するか？
を指定します。

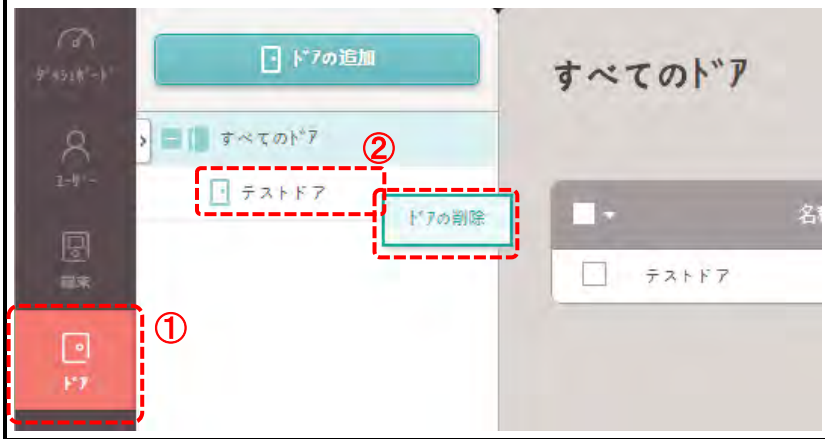
A 部分で、「端末再起動」を選択した場合は、B 部分で、
・どの端末を再起動するのか？
を指定します。

A 部分で、「端末利用不可」を選択した場合は、B 部分で、
・どの端末を利用不可にするのか？
を指定します。
※利用不可にした端末のロックを解除する場合は、端末の設定の「端末操作ロック」から行ってください

これで、ドアのすべての設定が完了です。
最後に、ドアの追加画面の一番下の「適用」ボタンをクリックし設定を反映してください。

24.2 ドアの削除

端末を撤去した場合など、不要になったドア設定は、削除することが可能です。

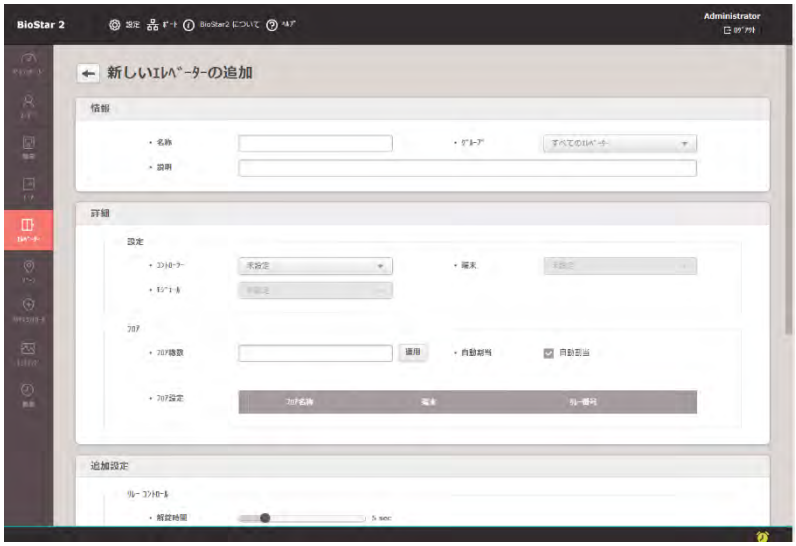
説明図	操作内容
	① 「ドア」メニューをクリックし、ドア画面にしてください。 ② 削除したいドアを右クリックし、「ドアの削除」をクリックしてください。
	① 「はい」をクリックすることで、ドアが削除されます。 ※但し、ドアが、ゾーンに割り当てられている場合は、先にゾーンの設定からドアを解除していただき、その後でドアを削除してください。

25 エレベーターの設定

端末と OM-120 を使用し、エレベーターのフロア制御を設定します。

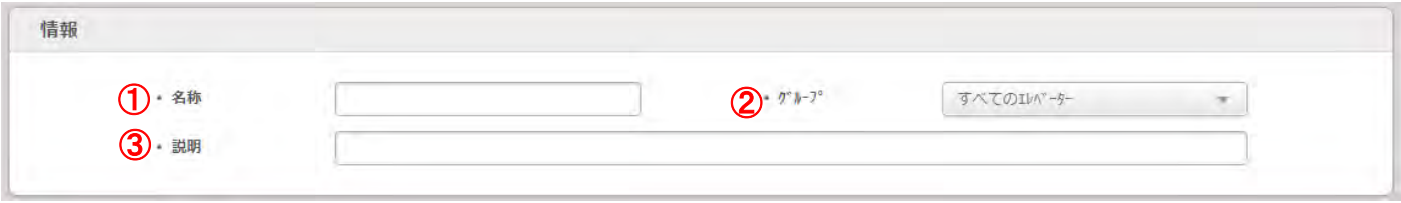
※エレベーターのメニューを表示するのは、アドバンスド以上のライセンスが必要です。

25.1 エレベーターの追加

説明図	操作内容
	① 「エレベーター」メニューをクリックしてください。 ② 「エレベーターの追加」をクリックしてください。
	ドアの追加画面が表示されます。 情報、詳細、追加設定、警報の設定を行ないます。 すべての情報を編集したら、「適用」をクリックしてください。

エレベーターの設定画面の各項目については、次ページ以降で、部分ごとに記載します。

【情報】項目



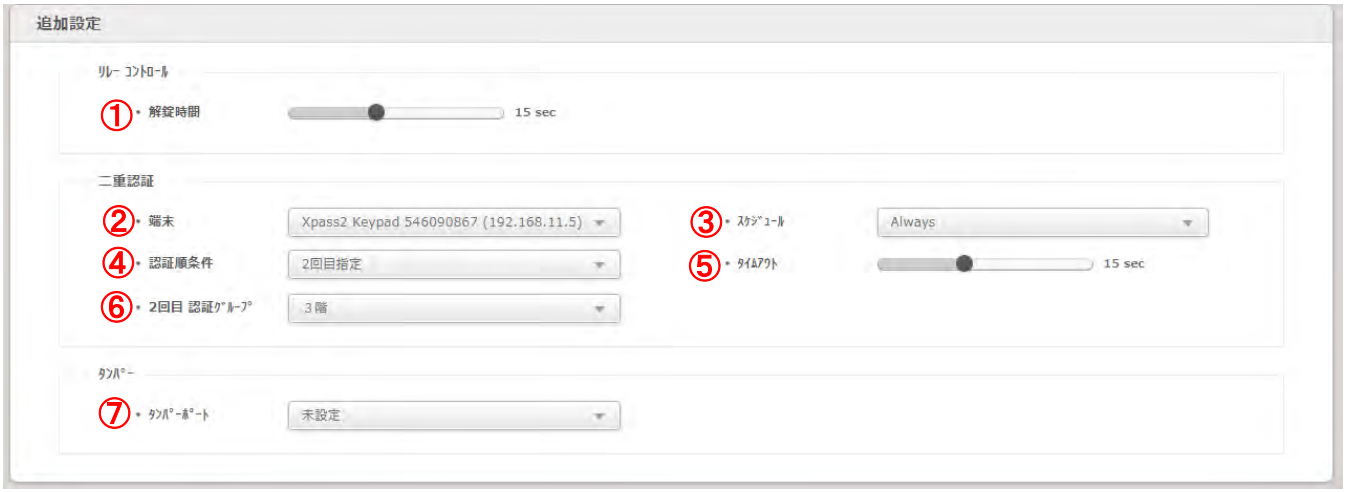
① 名称を入力してください。
② エレベーターのグループを設定します。
③ エレベーターの簡単な説明を入力します。

【詳細】項目

エレベーターとフロア情報に関連付ける端末を選択できます。

① 登録済みの機器一覧から OM-120 を制御する端末を選択します。マスターになる端末を選択できます。
② 認証に使用する端末を選択します。最大4台まで選択できます。
③ OM-120 を選択します。
④ OM-120 で制御するフロアの合計数を入力し⑤「適用」をクリックします。
最大 192 フロアまで入力できます。
⑥ フロア設定のリレー番号を自動で割り当てる時には☑を入れます。
リレー番号は連続した順序で割り当てられます
フロア数を 5 フロアで自動割当てに☑を入れた場合は以下の様な画面になります。

【追加設定】項目



① 設定した時間だけリレーが動作します。認証により、リトリガブル動作を行ないます

② 重認証を行なう端末を選択します。選択すると③④⑤の項目が表示されます。

③ 重認証を実施するスケジュールを設定します。必要なスケジュールがない場合は、「＋スケジュールの追加」をクリックしてください。

④ 証順番を設定します。「2 回目指定」をクリックすると⑥項目が表示されます。
「未設定」に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とリレー出力されます。
「2 回目指定」にすると「2 回目　認証グループ」で指定し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。

⑤ 初の認証情報が認証された後、2 番目の認証情報を認証するためのタイムアウト時間を設定します。
最初のユーザーが認証された後、タイムアウト時間内に 2 番目のユーザーが認証されない場合、リレー出力は行いません。

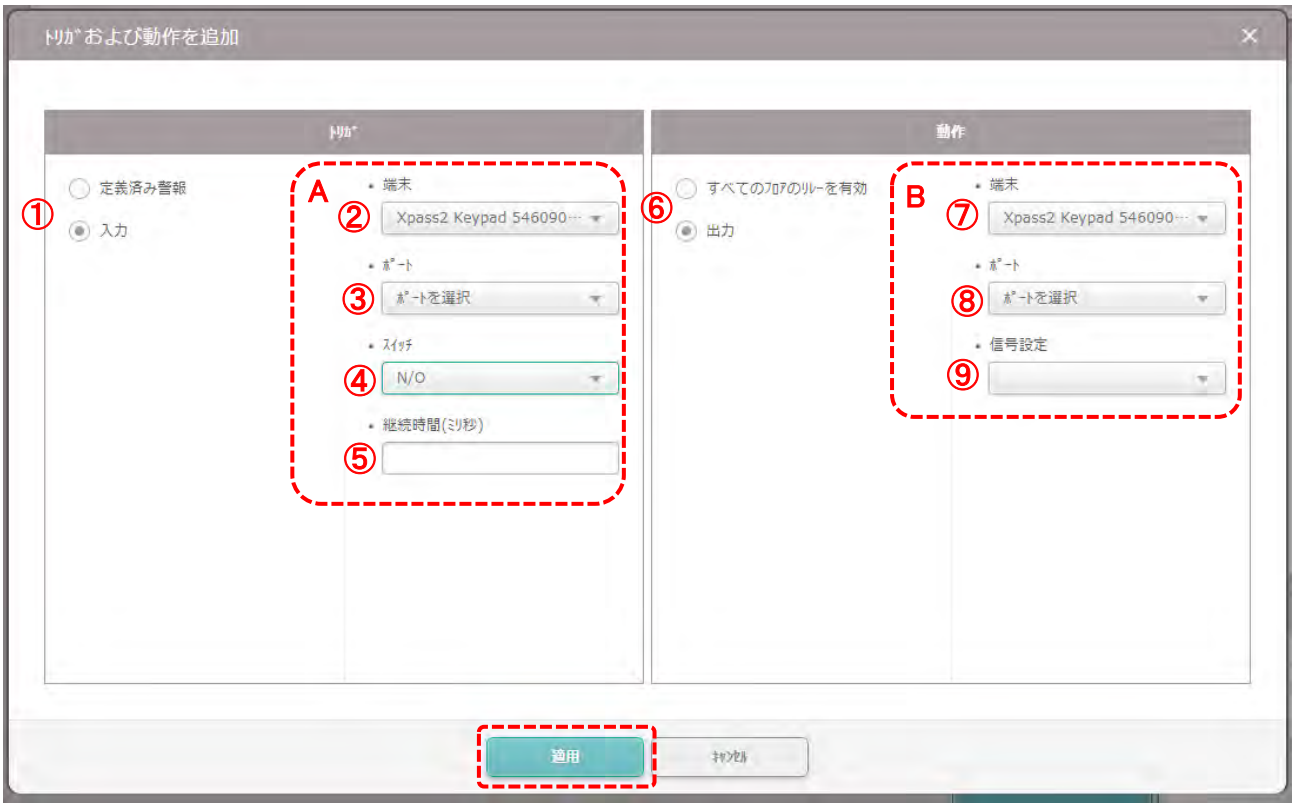
⑥ 回目に認証するアクセスグループを指定します。

⑦ タンパー信号を出力するポートを設定します。

【警報】項目

タンパー入力や別の入力信号を検出したときの動作を設定できます。

「＋追加」をクリックしてください。



① 「入力」を選択すると「A」の項目が表示されます。「定義済み警報」を選択するには、前項のタンパー設定で出力ポートを選択しておく必要があります。

② 入力に使用する端末を選択します。

③ ②で選択した端末の入力ポートを選択します。

④ 接点入力を選択します。

⑤ 接点入力の継続時間を入力します。入力した時間（ミリ秒）を継続すると検知します。入力を検知するとモニタリングのフロア状態の「警報を解除」をクリックするまで状態が保持されます。

⑥ 「出力」を選択すると「B」の項目が表示されます。「すべてのフロアのリレーを有効」を選択すると、トリガ入力を検知するとすべてのフロアのリレーが動作します。

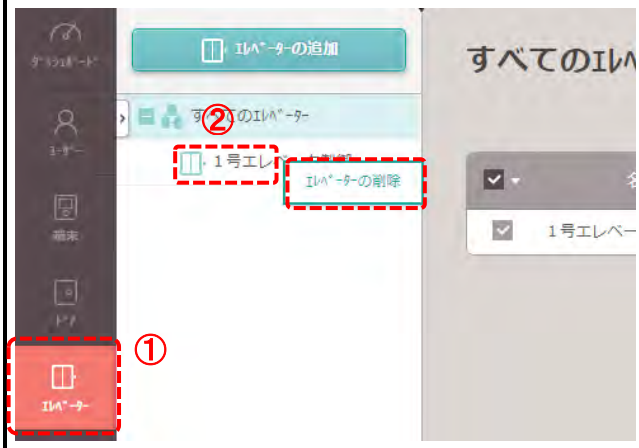
⑦ 出力に使用する端末を選択します。

⑧ ⑦で選択した出力ポートを選択します。

⑨ 出力信号を選択します。一覧に表示されない場合は「＋シグナルの追加」を選択し、設定してください。

設定が終わりましたら「適用」をクリックしてください。

25.2 エレベーターの削除

説明図	操作内容
	① 「エレベーター」メニューをクリックし、エレベーター画面にしてください。 ② 削除したいエレベーターを右クリックし、「エレベーターの削除」をクリックしてください。
	③ 「はい」をクリックすることで、エレベーターが削除されます。

26 ゾーンの設定

本項目は、追加でアクセスコントロールのライセンスを登録した場合に利用可能となります。

ゾーンとは、基本的には、複数のドア（端末）を連携させたエリアのことを呼びます。（但し、一部、ゾーンと関係しない機能も含みます。）

本章は、ゾーン関連で設定できる機能について記載します。また、注意点として各ゾーンの機能は全種類の端末で動くわけではありません。

一部の機種では、動作できないゾーンもありますので、ご注意ください。

26.1 ゾーンの種類

本 BioStar2 システムのゾーンには、以下の 2 種類のゾーンがあります。

・ローカルゾーン

・グローバルゾーン

それぞれについて、記載します。

【ローカルゾーン】

ローカルゾーンとは、1 台の LAN 接続の親端末から、RS-485 で、複数台の子機が接続されている状態で、その中の数台、あるいは全ての端末を指定したゾーンのことを指します。（ポイントとしては、**そのゾーンの中には LAN 接続の端末は必ず 1 台** となります。）

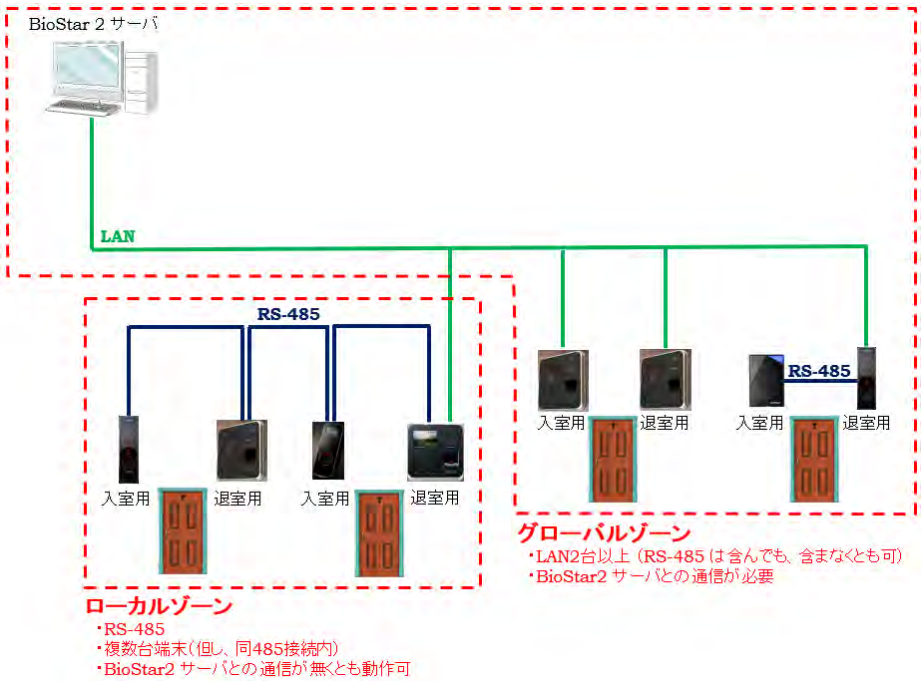
この場合、ゾーンの機能の管理者は、LAN 接続の親端末となります。このため、PC との通信がない場合でも動作可能です。

【グローバルゾーン】

グローバルゾーンとは、複数台の LAN 接続の端末が含まれるゾーンのことを指します。

（ポイントとしては、**そのゾーンの中には LAN 接続が複数台**となります。）

この場合、ゾーン機能の管理者は、PC となります。このため、ゾーンの機能が継続して動作するためには、PC を常に起動しておく必要があります。



26.2 アンチパスバックゾーン

アンチパスバック（以下 APB）ゾーンは、24.1 章のドアの設定内で行う APB の設定より機能を強化した APB を行うことが可能です。

ゾーンに関わる全端末を、それぞれ、入側/出側で指定し、ゾーンとして入退出の管理が可能となります。

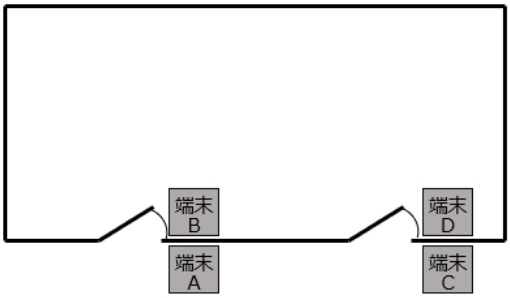
（本機能は、BioStar2 対応端末の全端末で利用可能です。）

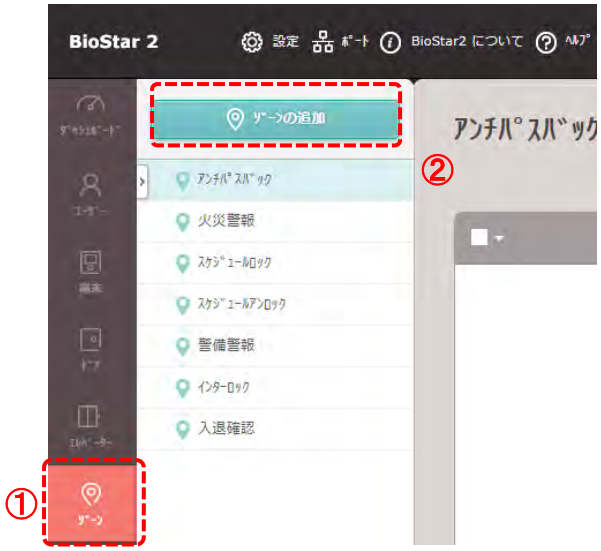
例えば、以下のような大きな部屋にドアが複数ある場合、APB ゾーンの設定では、端末 A および C を入室端末。端末 B および D を退室端末として設定します。これにより、

- A から入り、B で出る
- A から入り、D で出る
- C から入り、B で出る
- C から入り、D で出る

が成立するようになります。

APB ゾーンの作成方法について記載します。



説明図	操作内容
	① 「ゾーン」メニューをクリックし、ゾーン画面にしてください。 ② 「ゾーンの追加」をクリックしてください。
	① 左図の画面が表示されます。「アンチパスバック」を選択してください。 ② 「適用」をクリックしてください。 APB の設定画面が開きます。 次ページは設定画面について記載します。

① APB ゾーンの名前を入力してください。

② ゾーンの種別が APB であることが表示されます。（変更はできません。）

③ ゾーンのモードを「ローカル」か「グローバル」から選択してください。グローバルを選択すると、⑩の設定項目が表示されます。
ローカルに設定すると RS-485 に接続されている機器が⑦⑧に指定できます。グローバルに設定すると Biostar2 に登録されているすべての機器が⑦⑧に指定できます。

④ この APB ゾーンの有効/無効を変更することができます。完全に削除したくないが機能として一時的に停止させたい場合は、「無効」を選択してください。

⑤ APB の種類を「ソフト」と「ハード」から選択可能です。ソフト APB とは、システム上はアンチパスバックの判断をしますが、利用者にとっては認証成功となり通常通りドアが開きます。但し、システムのログとしては、ソフト APB の違反として記録されます。
（どのくらいのユーザーがアンチパスバック違反をするか？を調べたい時などに利用します。ハード APB とは、システム上のログも残しますし、アンチパスバック違反の場合エラー表示としてドアが開きません。）

⑥ アンチパスバックの解除時間を設定します。初期値の 1440 分は、24 時間分となります。この設定の場合は、APB エラーとなっても、24 時間経過以降に認証すれば通れることとなります。もし、完全にアンチパスバックを行う場合は、0 分を指定してください。この場合は、システムからリセットするまでは、アンチパスバックが有効のままとなります。また、APB エラーの動作の解除時間は、最後に発生した事象からカウントされます。（リトリガブル動作）

⑦ アンチパスバックを適用する範囲を設定できます。[ON] に設定されている場合は、入口および出口のドア操作に応じて、アンチパスバックが適用されます。オフに設定すると、ドア操作に関係なく、ユーザーの認証に従ってアンチパスバックが適用されます。「ドア設定に従う」に設定すると、ドアのアンチパスバック規則が適用されます。

⑧ 入室端末として設定する端末を選択してください。本例では、A と C の 2 台の端末を選択することになります。

⑨ 退室端末として設定する端末を選択してください。本例では、B と D の 2 台の端末を選択することになります。
⑦、⑧を設定することにより、「警報」設定画面が現れます。その説明が必要と思われます。

⑩ ③でグローバルゾーンを選択した場合に表示されます。管理者である PC と LAN の通信が成立しなかった場合の対応を以下から選択し、設定します。※現在下記の仕様通りに動作してないと思います。2020.9.14 現在）

・認証資格により解錠　　：本来の認証資格があれば、通過を許可します。

・APB ログを記録し、認証資格により解錠　　：APB エラーであることは記録し、通過を許可します。

・APB ログを記録し、ドアは施錠　　：APB エラーであることを記録し、通過を許可しません。

なお、③でローカルゾーンを選択した場合は、本項目は表示されませんが、ローカルゾーンの場合は、RS-485 の通信ができない場合は、その時点で認証ができません。このため、ローカルゾーンの場合は、通信ができないと無条件でエラーとなり解錠はできません。

⑪　バイパスグループは、この APB ゾーンの除外者となるグループを設定することができます。全ユーザーが対象で良い場合は、未使用としてください。管理者ユーザーなど、一部の方は APB の対象としない。という場合に、そのユーザーグループを指定してください。

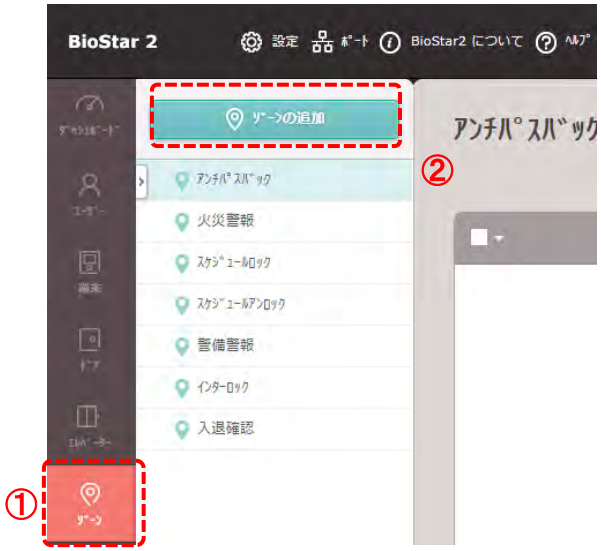
設定が完了したら、画面下部の「適用」をすると、有効になります。

26.3 火災報知ゾーン

火災報知ゾーンは、火災報知器との連動により、信号線をもらうことで、ゾーン内のドアを無条件で解錠する機能です。

（本機能は、BioStar2 対応端末の全端末で利用可能です。）

火災報知ゾーンの作成方法について記載します。

説明図	操作内容
	① 「ゾーン」メニューをクリックし、ゾーン画面にしてください。 ② 「ゾーンの追加」をクリックしてください。
	① 左図の画面が表示されます。「火災報知」を選択してください。 ② 「適用」をクリックしてください。 火災報知の設定画面が開きます。 次ページは設定画面について記載します。

① 火災報知ゾーンの名前を入力してください。

② ゾーンの種別が火災報知であることが表示されます。(変更はできません。)

③ ゾーンのモードを「ローカル」か「グローバル」から選択してください。
(グローバルゾーンで設定する場合は、管理機能を有する PC と通信できないと、火災報知ゾーンが動作しないことをご注意ください。PC との通信が復旧した時点で動作します。)

④ この火災報知ゾーンの有効/無効を変更することができます。完全に削除したくないが機能として停止させたい場合は、「無効」を選択してください。

⑤ 火災報知の信号線が入った場合に、解錠するドアを選択してください。(③の接続法の範囲の中から複数のドアが選択可能です。)

⑥ エレベーターの中からアクセス可能とするフロアを選択してください。(別途エレベーター用拡張ユニット利用時)

⑦ 端末 / 入力

「端末/入力」となっている部分は、⑤で指定したドアに割当てられている端末の中で、有効な入力チャンネルを選択してください。
「スイッチ」の部分は、火災報知器からの信号が、通常時ショートしていない状態なら「N/O」を選択し、通常時にショートしている場合は、「N/C」を選択してください。また、検知までの時間をミリ秒で指定してください。
もし、設定を削除する場合は、ゴミ箱のアイコンをクリックしてください。

⑧ 警報動作については、火災報知が発生した場合に、ゾーン内でリレースイッチを利用していない端末あるいは、拡張ユニット等のリレースイッチのチャンネルがあいている場合に、リレースイッチによる接点出力が可能です。「＋追加」で、出力リレーチャンネルと、出力シグナルを設定することが可能です。

設定が完了したら、画面下部の「適用」をすると、有効になります。

火災報知ゾーンは、設定をしておき、火災報知器が発動し接点信号を出力すると、認証機が受け取り鍵を開けっ放しにする機能です。

火災報知器との通信線部分の焼け落ちなどを考慮し、火災報知器側が復旧させたとしても、復旧時は、連動しない仕組みになっています。
解錠状態を戻すためには、火災報知器が復旧していることを確認の上、以下の操作を行ってください。

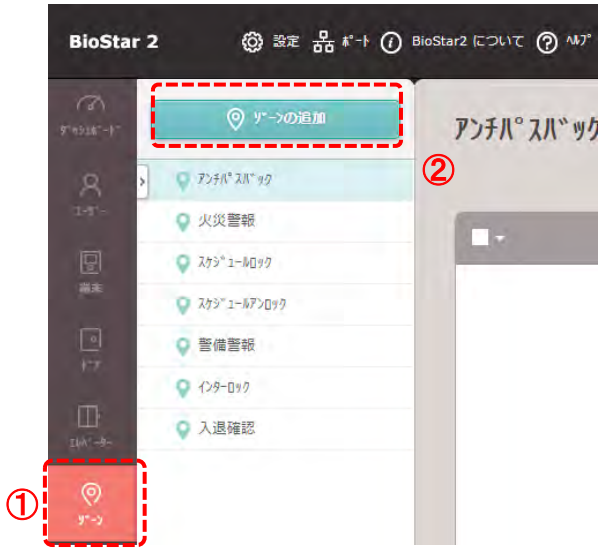
BioStar2 で、
　モニタリング　→　ゾーン状態　→　該当の火災報知ゾーンにチェック　→　アラームを解除　をクリック
この操作により、鍵が再びロックされ（通常運用状態）ます。

26.4 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、特定の日時の範囲では、自動的に強制施錠する機能です。基本的にはスケジュールロック中は認証しても解錠できません。本機能は、ゾーンの設定メニュー内にありますが、ゾーン機能を有さず、ドア単位で設定する機能となります。

（本機能は、BioStar2 対応端末の全端末で利用可能です。）

スケジュールロックゾーンの作成方法について記載します。

説明図	操作内容
	① 「ゾーン」メニューをクリックし、ゾーン画面にしてください。 ② 「ゾーンの追加」をクリックしてください。
	① 左図の画面が表示されます。「スケジュールロック」を選択してください。 ② 「適用」をクリックしてください。 スケジュールロックの設定画面が開きます。 次ページは設定画面について記載します。

① スケジュールロックゾーンの名前を入力してください。

② ゾーンの種別がスケジュールロックであることが表示されます。(変更はできません。)

③ このスケジュールロックゾーンの有効/無効を変更することができます。完全に削除したくないが機能として停止させたい場合は、「無効」を選択してください。

④ スケジュールロック中で認証できない時間帯の時に、出口ボタンを有効とするか、出口ボタンでもロック状態で開かなくするか選択してください。

⑤ スケジュールロックの対象とするドアを選択してください。(ドアは 1 つしか選択できません。)

⑥ スケジュールロックの対象とするスケジュールを選択してください。(事前にスケジュールの作成をしておき、その中から選択する形となります。)

⑦ スケジュールロックによる認証エラー発生時の動作を選択してください。指定する場合は、右の「＋追加」より指定してください。

選択可能な警報の種類は、リレーによるシグナル出力 / 端末の全アラーム解除 / 端末の再起動 / 端末の利用不可(ロック)の 4 種類となります。(ドアのアンチパスバック警告と同様です。詳細は、ドアのアンチパスバック警告部を参照してください。)

⑧ スケジュールロック時でも、認証が成功し、ドアを解錠できるアクセスグループを選択することが可能です。(事前にアクセスグループを作成しておき、その中から選択する形となります。)

設定が完了したら、画面下部の「適用」をすると、有効になります。

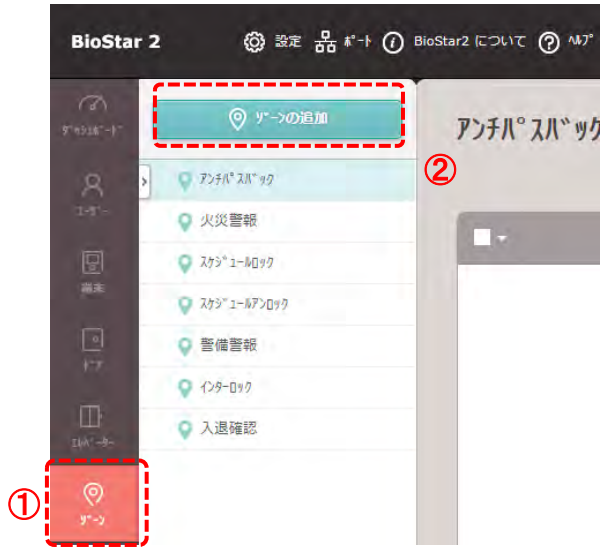
26.5 スケジュールアンロックゾーン

スケジュールアンロックゾーンは、特定の日時の範囲では、自動的に強制解錠する機能です。

本機能は、ゾーンの設定メニュー内にありますが、ゾーン機能を有さず、ドア単位で設定する機能となります。

（本機能は、BioStar2 対応端末の全端末で利用可能です。）

スケジュールロックゾーンの作成方法について記載します。

説明図	操作内容
	① 「ゾーン」メニューをクリックし、ゾーン画面にしてください。 ② 「ゾーンの追加」をクリックしてください。
	① 左図の画面が表示されます。「スケジュールアンロック」を選択してください。 ② 「適用」をクリックしてください。 スケジュールアンロックの設定画面が開きます。 次ページは設定画面について記載します。

① スケジュールアンロックゾーンの名前を入力してください。

② ゾーンの種別がスケジュールアンロックであることが表示されます。(変更はできません。)

③ このスケジュールアンロックゾーンの有効/無効を変更することができます。完全に削除したくないが機能として停止させたい場合は、「無効」を選択してください。

④ 有効にすると、⑦のアクセスグループに属するユーザーが認証を受けて、スケジュールのロックが解除されます。(本項目を有効とした場合、どのグループのユーザーなら良いか？を指定するため、⑦が表示されます。)本設定をしておけば、誰も到着していない場合に、指定されたスケジュールで解錠になってしまうことを防げます。

⑤ 解錠する施設をドアまたはエレベーターに設定できます。ドアを選択すると、ドアのリストがアクティブになりますので、スケジュールされたロック解除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、エレベーターのリストがアクティブになりますのでスケジュールされたロック解除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。エレベーターの階を選択できます。(上記画面は、ドアを選択した画面になっています。)

⑥ スケジュールアンロックの対象とするスケジュールを選択してください。(事前にスケジュールの作成をしておき、その中から選択する形となります。)

⑦ スケジュールアンロックの対象とするドア(ドアは 1 つしか選択できません。)または、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。

⑧ スケジュールアンロック発動の際に、④で、ユーザーの認証からスケジュールの開始とする時、どのユーザーにそれを許可するか？をアクセスグループで選択することとなります。(事前にアクセスグループを作成しておき、その中から選択する形となります。)

注意:別のスケジュールアンロックゾーンですでに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。

設定が完了したら、画面下部の「適用」をすると、有効になります。

26.6 警備警報ゾーン

警備機能は、端末を警備モードにし、認証できなくする機能です。ゾーン内の端末に対し、代表の端末から警備を開始/解除の操作を行い警備モードにすることが可能です。また、端末からの操作ではなく、外部の警備システムの信号を受信することで、連動して警備の開始/解除を行うことも可能です。警備の開始のトリガはどれであっても、端末を警備モードとし、警備中にドアを開けられないようにすることが目的です。

（***本機能は、BioStar2 対応端末のうち、BioStar2 専用機種で利用可能です。BioLiteNet V2/XpassSlim S2 V2 では利用できません。また、対応している機種であっても、対応している新しい FW にする必要があります。2018/5 以降の FW にてご利用ください。もし、FW が古い場合は、FW のアップデートにより利用可能となります。***）

警備ゾーンの利用には、大きく以下の 2 種類があります。

・端末から警備 開始/解除操作を行い、警備をする。

・ビルの警備システムなど、外部信号を受信し、警備をする。

それぞれの方法について記載します。

以下、警備ゾーンの作成方法と、その画面の説明を記載します。

説明図	操作内容
	① 「ゾーン」メニューをクリックし、ゾーン画面にしてください。 ② 「ゾーンの追加」をクリックしてください。
	① 左図の画面が表示されます。「警備警報」を選択してください。 ② 「適用」をクリックしてください。 警備の設定画面が開きます。 次ページは設定画面について記載します。

26.6.1 端末操作を警備の開始/解除トリガとする場合

端末の操作により、警備を開始/解除する場合について記載します。端末からの警備開始/解除は、以下の 2 つの方法で行うことができます。

・端末のボタン操作により、警備の開始/解除の操作を行い、その後、認証することで警備の開始/解除を行う。

・警備用のカードを登録し、そのカードをかざしてから、認証をすることで警備の開始/解除を行う。

また、警備の開始/解除に応じて、リレースイッチから接点出力をすることもできます。これにより、警備の開始/解除の状態を別システムに伝えることも可能です。

【情報 ， 設定 ， 警備/解除設定】項目

① 警備ゾーンの名前を入力してください。

② ゾーンの種別が警備であることが表示されます。(変更はできません。)

③ 警備ゾーンは、「ローカル」のみのサポートです。(変更はできません。)

④ この警備ゾーンの有効/無効を変更することができます。完全に削除したくないが機能として停止させたい場合は、「無効」を選択してください。

⑤ 警備の対象とするドアを選択してください。(ローカルゾーン内のドアは複数選択できます。)

⑥ 警備開始操作から、実際に警備が開始されるまでの遅延時間を設定可能です。(但し、開始のみ動作します。解除も入力変更は可能ですが、警備を解除する際に遅延させる必要性がないため、時間を変更しても動作は変わりません。解除の時間は 0 秒としてください。)

⑦ 必要に応じて、警備用カードを作成することが可能です。例えばご利用の端末が、BioEntryW2 や、BioEntryP2 の場合、ボタンが無いため、警備開始のトリガを与えることができません。その場合は、警備用カードを作成し、トリガにすることができます。ファンクションキーがついている機種は、警備用カードを作らなくてもご利用が可能です。

警備用カードはエリアごとに作成することとなります。他の警備エリアで共通のカードを作成することができませんので、ご注意ください。

（どの警備エリアでも警備開始/解除できる「マスター警備カード」のようなものは作成できません。）

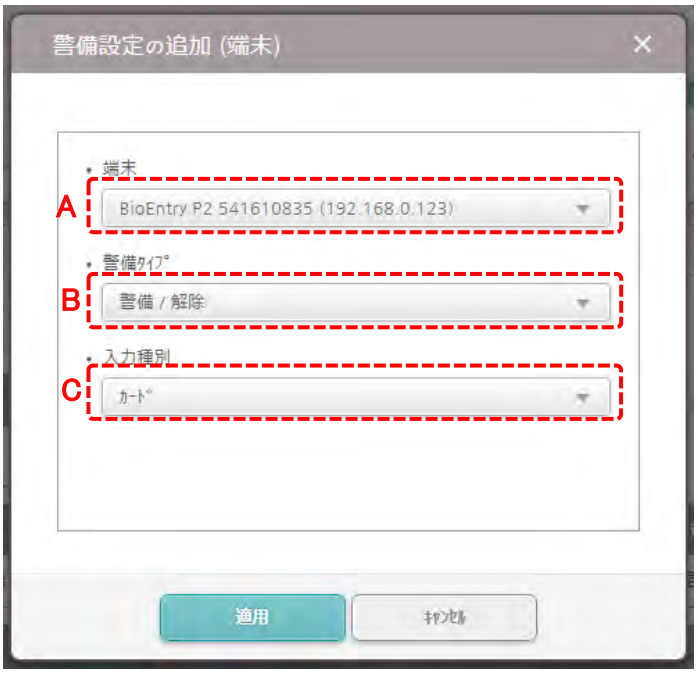
作成する場合は、「＋追加」をクリックすると、ユーザーのカード登録と同じ画面になりますので、新しいカードを読み込ませ登録してください。

（ユーザーに割りあたっている認証用カードとも重複することはできません。）

⑧ 警備カードまたは、警備開始/解除の操作後、認証することで警備の開始/解除ができるユーザーのアクセスグループを指定してください。

⑨ 警備の開始/解除に利用する端末と、その動作方法について設定します。「＋追加」をクリックして設定してください。

以下の画面が表示されます。



A 部分は、警備のゾーンに含む端末を選択します。

⑤で選択したドアに割当てられている端末単位で、

追加してください。

B 部分では、その端末で可能な操作を選択します。

警備 ， 解除 ，警備/解除

から選択します。

（警備 は、警備を ON するのみです。解除には使えません。

解除 は、警備を OFF するのみです。開始には使えません。

警備/解除 は、両方の操作が可能です。）

C 部分は、操作方法を選択します。

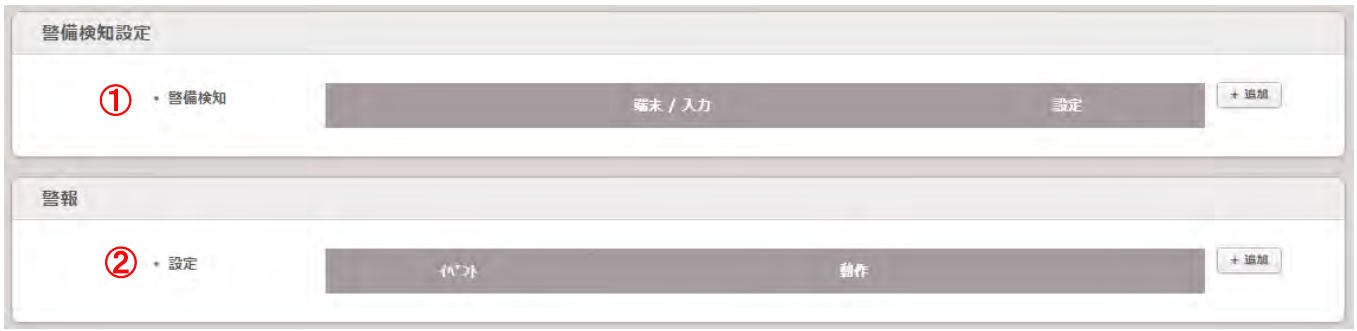
カード，キー，カードまたはキー

から選択します。

（カードは警備用カードで操作します。キーは、操作キー付きの端末で表示され、設定可能です。カードまたはキーは、操作キー付きの端末で、カードでもキーでも対応可能となります。）

⑩ 外部信号線を受信し、警備の開始/解除を行う場合に利用します。本章では、端末操作をトリガとする警備についてのため、本項目は利用しません。

【警備検知設定 ， 警報】項目

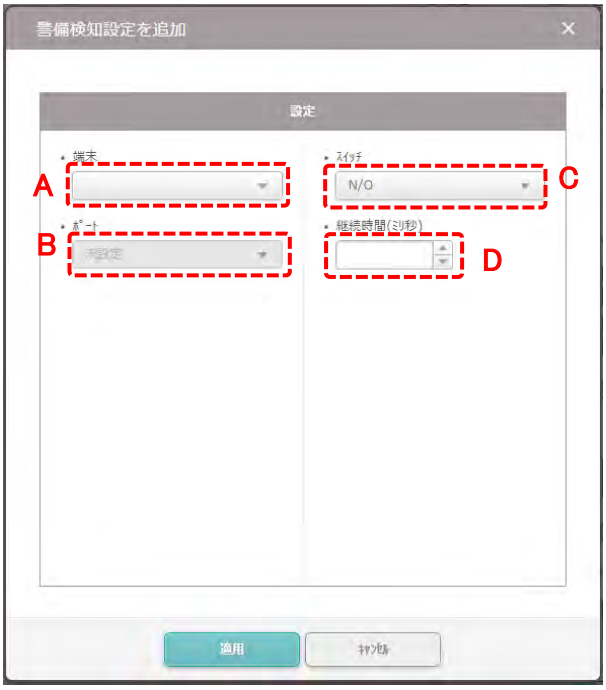


① 追加の侵入検知の信号受信線および、その種類と検知時間を設定します。【情報 ， 設定 ， 警備/解除設定】項目の⑤で指定したドアのドアセンサーは、自動的に、侵入検知に利用されます。それ以外に、別の信号線として侵入検知の判断に利用するチャンネルと種類、判断時間を指定してください。

・警備ゾーンとして指定したドア:ドア開閉確認チャンネルが、侵入検知に利用されます。

・追加で、侵入検知に利用するチャンネルを、必要に応じて、「＋追加」で指定してください。

「＋追加」をクリックすると、以下の画面が表示されます。



A 部分では、侵入検知に利用する端末を選択してください。

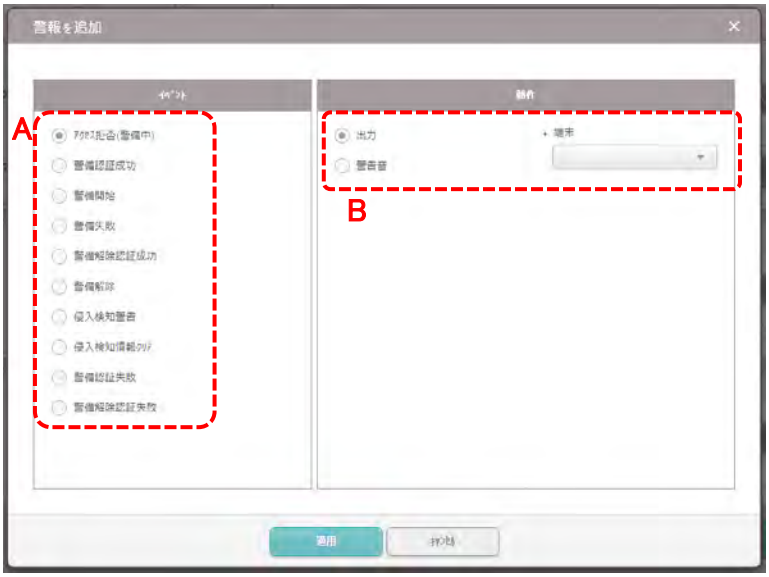
B 部分では、A で選択した端末の侵入検知に使うポート(チャンネル)を選択してください。

C 部分では、侵入検知の信号線の通常状態が、N/O か N/C かを選択してください。(ドアが閉まっている時の信号線が、ショートした状態となる場合は、ここは、N/C を選択してください。ドアが開いたときがショート状態となる場合は、N/O を選択してください。)

D 部分では、侵入と検知するまでの状態継続時間を指定してください。

設定が完了したら、「適用」をクリックしてください。

② 警備に関するイベントが発生した場合に、動作を指定する場合は、ここで追加してください。右側の「＋追加」をクリックすることで、イベントに対する動作を指定することが可能です。「＋追加」をクリックすると、次のページの画面を表示します。



A 部分では、動作を決めるトリガとなるイベントについて選択します。各イベントは以下の条件の時に発生とみなします。

- ・アクセス拒否（警備中）　：端末で警備が掛かっている際に、認証すると発生します。
- ・警備認証成功　：警備を開始する際に認証が必要となり、その認証が成功の時に発生します。
- ・警備開始　：警備を開始した時に発生します。
- ・警備失敗　：警備を開始しようとした際に失敗すると発生します。（ドアが開いているのに警備をしようとした時など）
- ・警備解除認証成功　：警備を解除する際に認証が必要となり、その認証が成功の時に発生します。
- ・警備解除　：警備を解除した時に発生します。
- ・侵入検知警告　：警備中にドアが開かれ侵入を検知した際に発生します。
- ・侵入検知情報クリア　：侵入検知警告の情報がクリアされた時に発生します。
- ・警備認証失敗　：警備を開始する際に認証が必要となり、その認証が失敗の時に発生します。
- ・警備解除認証失敗　：警備を解除する際に認証が必要となり、その認証が失敗の時に発生します。

B 部分では、A のイベント発生時の動作を選択します。動作は、「出力」と「警告音」から選択可能です。

「出力」については、出力する端末を選び、その端末に接続されているリレースイッチ（未使用状態であること）を選択し、出力するシグナルを選択します。出力シグナルについては、端末の「トリガおよび動作」の設定と同様です。そちらを参照してください。

「警告音」については、警告音を鳴らす端末と、その音量を選択してください。

ここで、BioStar2 の端末で、警備の開始/解除を行い、外部システム（ビルの警備システム等）へ信号を出力する場合は、A の部分で、警備開始と、警備解除のイベントに登録します。警備開始のイベントで「出力」を選択し、シグナルに警備開始用のシグナルを作成し、登録します。同様に、警備解除のイベントで「出力」を選択し、シグナルに警備解除用のシグナルを作成し、登録します。

警備開始時は、接点出力を 1 ショット、警備解除時は、接点出力を 2 ショットと言う場合は、繰り返し回数でシグナルを作成してください。

あるいは、警備中はメーク、警備解除中はブレーク という場合は、次のページのような設定にしてください。

警備開始シグナル

警備解除シグナル

【警備を開始/解除する操作】

警備を設定し、実際に端末を使って操作する場合は以下の方法で行ってください。

カード(警備カード)利用 (可能性:BioStar2 世代の全機種 / BioLiteNet V2 と Xpass Slim S2 V2 を除く)

警備用カード作成し、警備用カードで認証後、各ユーザーの認証(顔/指紋/カード/10 キー)を行ってください。

キー(ファンクションキー)利用 (可能性:BioStation2/BioStationA2/BioStationL2/BioLiteN2/FaceStation2/FaceStationF2)

10 キー無し機種は、液晶画面の「警備」アイコンをクリックし、警備の確認が表示されたら認証してください。

10 キーあり機種は、F1 を長押しすると、警備開始/F2 を長押しすると警備解除となります。その後、警備の確認が表示されたら認証してください。

26.6.2 外部信号を警備の開始/解除トリガとする場合

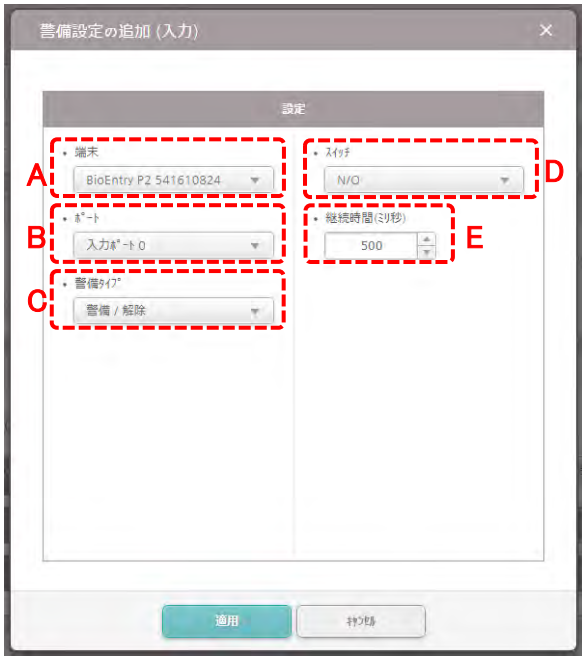
外部からの信号を受信することで、端末の警備を開始/解除する場合について記載します。本方法は、BioStar2 端末から警備の開始/解除を行わず、ビルの警備システム等から警備の開始/解除情報を受信し、認証できなくする場合に利用します。ビルの警備信号に合わせ、端末に認証ロックをかける場合にご利用可能です。

【情報 ， 設定 ， 警備/解除設定】項目

① 警備ゾーンの基本情報を設定します。26.6.1 章の部分を参考にしてください。

② 26.6.2 章の内容で、端末側から警備を開始/解除する場合に利用します。本章では外部トリガを利用した場合について記載しますので、設定不要となります。

③ 外部の警備信号を受信する端末/ポート番号と、その信号からどう動くか？と、判断時間等を設定可能です。設定する場合は、「＋追加」をクリックし、内容を設定してください。「＋追加」をクリックすると、以下の画面を表示します。



A 部分 外部信号を受信する端末を選択してください。

B 部分 A で選択した端末の入力ポートを指定してください。

C 部分 警備の開始，解除，開始/解除 を選択してください。

D 部分 メークされたら警備を開始、ブレークで警備を解除の場合は、N/O ブレークされたら警備を開始、メークで警備を解錠の場合は、N/C を選択してください。

E 部分 警備を開始/解除と判断するための信号継続時間を指定してください。

【侵入検知設定 ， 警報】項目

26.6.1 と同様です。そちらを参照ください。

26.7 インターロックゾーン

インターロックは、同ゾーンの中で、開けられるドアを1つまでにするシステムです。「入る時に利用したドアを閉めないと、次のドアが開けられない。」というシステムで利用することが想定されます。

（**本機能は、BioStar2 対応端末のうち、CoreStation 専用です。他の端末では利用できません。**

また、新しい FW にする必要があります。2018/5 以降の FW にてご利用ください。

もし、FW が古い場合は、FW のアップデートにより利用可能となります。）

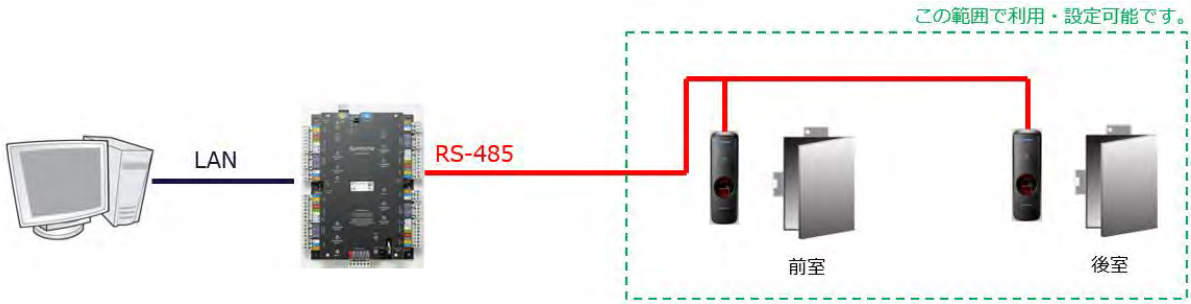
なお、インターロックゾーンは、ローカルゾーンでのみの対応となり、**最低限 2 つのドアが必要**となり、最大 4 つのドアまで使用できます。

インターロックゾーンとして設定されている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として設定されたドアは、火災警報ゾーン以外のゾーンに設定することはできません。

また、**LAN 端末は、インターロックゾーンの端末としては利用できません**。

インターロックゾーンが利用可能な例を示します。



以下、インターロックゾーンの作成方法と、その画面の説明を記載します。

説明図	操作内容
	① 「ゾーン」メニューをクリックし、ゾーン画面にしてください。 ② 「ゾーンの追加」をクリックしてください。
	① 左図の画面が表示されます。「インターロック」を選択してください。 ② 「適用」をクリックしてください。 インターロックの設定画面が開きます。 次ページは設定画面について記載します。

① インターロックゾーンの名前を入力してください。

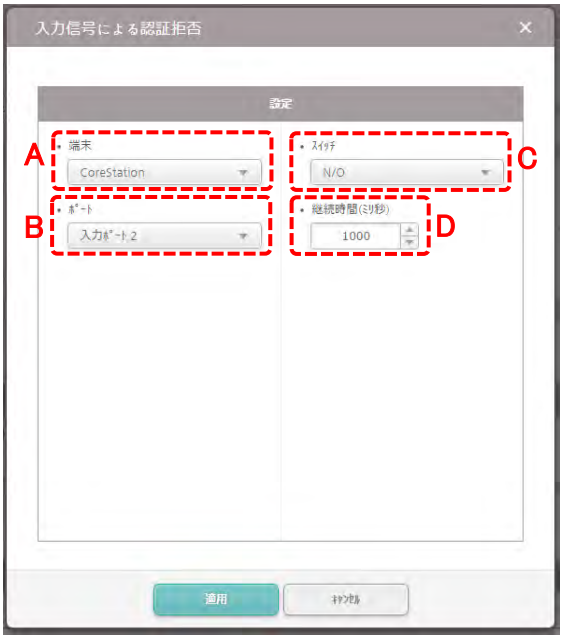
② ゾーンの種別が、インターロックであることが表示されます。(変更はできません。)

③ インターロックゾーンは、「ローカル」のみのサポートです。(変更はできません。)

④ このインターロックゾーンの有効/無効を変更することができます。完全に削除したくないが機能として停止させたい場合は、「無効」を選択してください。

⑤ インターロックの対象とするドアを選択してください。(ローカルゾーン内のドアで 2 つ以上選択してください。)
この項目を選択すると、⑥以下が表示されます。
なお、もし、⑤が選択できない場合は、インターロックを利用できる条件を満たしていません。RS-485 のみ接続の端末が割りあたったドアが、2 つ以上あるかを確認してください。

⑥ 外部から信号を入力すると、ドアの開いている/開いていないに関わらず、認証を不可にすることが可能です。条件を追加する場合は、右側の「+追加」をクリックしてください。以下の画面が表示されます。



A の部分では、外部からの信号を受信する端末を選択してください。

B の部分では、A の端末の信号を受信するポートを選択してください。

C の部分では、ショートされた時に受信と判断する場合は、「N/O」を、ショート状態が解除された場合に受信と判断する場合は、「N/C」を選択してください。

D の部分では、外部からの信号を受信したと判断するまでの時間を指定してください。

設定後、「適用」をクリックすることで反映されます。

⑦　インターロックのイベント発生時の動作を指定します。追加する場合は、右側の「＋追加」をクリックしてください。以下の画面が表示されます。

A の部分については、

・インターロック認証拒否

・インターロック認証拒否（入力信号）

が選択可能です。どちらを選択しても、B の部分については、設定内容は同様です。

インターロック認証拒否は、１箇所のドアが開いていて、他では認証できない時にイベント発生となります。

（標準的なインターロックの発生）

インターロック認証拒否（入力信号）は、⑥の部分で、外部入力により強制的に認証拒否とした場合に、イベント発生となります。

B の部分については、「出力」と「警告音」が選択可能です。「出力」を選択した場合（上画面）は、リレースイッチで出力する端末の選択、その端末のポートの選択、出力シグナルの選択となります。出力シグナルについては、端末の設定のトリガおよび行動の部分を参照してください。

「警告音」を選択した場合は、警告音を鳴らす端末を選択し、ブザーの音量を選択してください。

設定が完了したら「適用」ボタンをクリックしてください。

すべての設定が完了したら、画面下の「適用」ボタンをクリックすることで、インターロックゾーンが適用されます。

26.8 入退確認ゾーン

入退確認ゾーンは、あるゾーンを指定し、そのゾーンに入った人/そのゾーンから出た人を管理する機能です。

決められたゾーンへの入/退を管理したい場合や、災害時の避難確認などに利用することが想定されます。

（**本機能は、BioStar2 対応端末のうち、BioStar2 専用機種で利用可能です。BioLiteNet V2/XpassSlim S2 V2 では利用できません。**

また、対応している機種であっても、対応している新しい FW にする必要があります。2018/5 以降の FW にてご利用ください。

もし、FW が古い場合は、ファームウェアのアップデートにより利用可能となります。）

なお、入退確認ゾーンは、グローバルゾーンでのみの対応となり、**BioStar2 サーバーが起動していることが必要**となります。

利用時は、BioStar2 サーバーを停止しないようにしてください。

以下、入退確認ゾーンの作成方法と、その画面の説明を記載します。

説明図	操作内容
	① 「ゾーン」メニューをクリックし、ゾーン画面にしてください。 ② 「ゾーンの追加」をクリックしてください。
	① 左図の画面が表示されます。「入退確認」を選択してください。 ② 「適用」をクリックしてください。 入退確認の設定画面が開きます。 次ページは設定画面について記載します。

① 入退確認ゾーンの名前を入力してください。

② ゾーンの種別が、入退確認であることが表示されます。(変更はできません。)

③ 入退確認ゾーンは、「グローバル」のみのサポートです。(変更はできません。)

④ この入退確認ゾーンの有効/無効を変更することができます。完全に削除したくないが機能として停止させたい場合は、「無効」を選択してください。

⑤ 入退確認ゾーンに入ったと判断するために利用する端末を選択してください。

⑥ 入退確認ゾーンから出たと判断するために利用する端末を選択してください。

⑦ 入退確認ゾーンの確認対象とするユーザーを指定します。(事前に作成したアクセスグループを指定してください。)

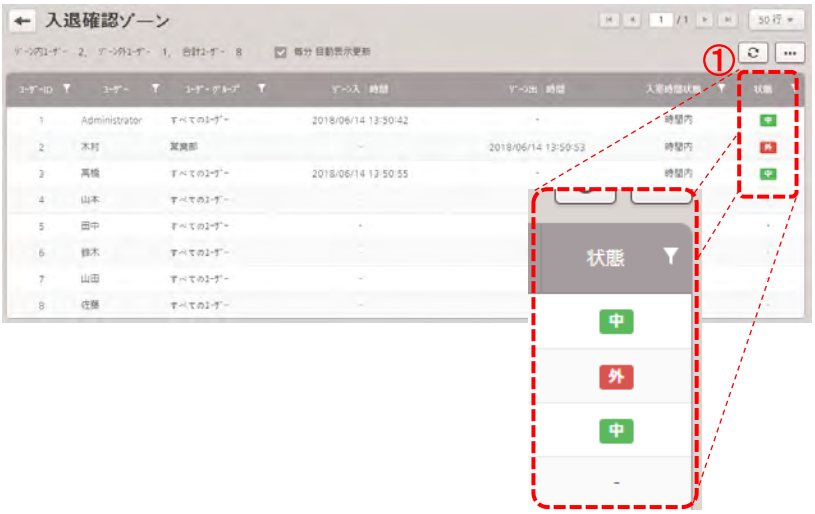
⑧ 入室状態が継続した時、どれだけの時間で警告とするかを指定してください。警告なしの場合は、0 分を指定してください。

⑨　⑧の時間以上に入室が継続した場合、警報となります。その際に何か動作をする場合は、指定してください。
指定する場合は、右側の「＋追加」をクリックしてください。以下の画面が表示されます。

A の部分については、入退確認ゾーン警報検知のイベントが選択できます。

B の部分については、「出力」と「警告音」が選択可能です。「出力」を選択した場合（上画面）は、リレースイッチで出力する端末の選択、その端末のポートの選択、出力シグナルの選択となります。出力シグナルについては、端末の設定のトリガおよび行動の部分を参照してください。
「警告音」を選択した場合は、警告音を鳴らす端末を選択し、ブザーの音量を選択してください。
設定が完了したら「適用」ボタンをクリックしてください。

ゾーンの設定が完了したら、画面右下の「適用」をクリックすることで、設定が反映されます。
設定した内容に合わせた入退室の確認は、次のページのように行ってください。

説明図	操作内容
	① 「モニタリング」メニューをクリックし、モニタリング画面にしてください。 ② 「ゾーン状態」をクリックしてください。 ③ 該当の入退管理ゾーンの行の右端の「入退状態」のボタンをクリックしてください。
	対象者の一覧が表示されます。 入退室の履歴がない状態の場合は、左図の様に表示されます。 ① ゾーン内のユーザー数/ゾーン外のユーザー数/合計ユーザー数が表示されます。 ② 毎分自動表示更新 に☑を入れると、本画面が毎分更新されます。 （入退室に合わせたリアルタイム更新ではありませんのでご注意ください。） ③ すぐに確認する場合は、手動更新のボタンをクリックしてください。
	① 入退室の記録がある場合は、左図の様に、入退確認ゾーンの中にいるか、外にいるかが表示されます。
	① 最大入室継続時間で指定した時間よりも多く入室状態が続いた場合は、左図の様に、警報が発生しピンクの帯となります。そして、入室時間状態の列に「時間超過」と表示されます。

26.9 混雑制限ゾーン

混雑制限ゾーンは、事前にゾーンを作成し、入室端末 および 退室端末を設定し、その際に、入室可能な最大人数を設定します。

認証により、その部屋に入室している人数が最大人数になると、入室ができなくなる。という機能です。

なお、本機能は、

・FaceStation2　　ファームウェアバージョン v1.1.1 以降

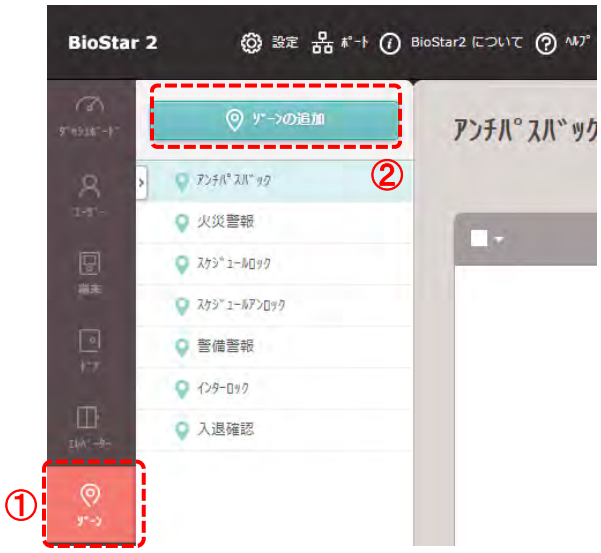
・FaceStation F2　　ファームウェアバージョン v1.5.0 以降

でのみ利用可能です。他の機種ではご利用いただけません。

また、混雑制限ゾーンは、グローバルゾーンでのみの対応となり、**BioStar2 サーバーが起動していることが必要**となります。

利用時は、BioStar2 サーバーを停止しないようにしてください。

以下、混雑制限ゾーンの作成方法と、その画面の説明を記載します。

説明図	操作内容
	① 「ゾーン」メニューをクリックし、ゾーン画面にしてください。 ② 「ゾーンの追加」をクリックしてください。
	① 左図の画面が表示されます。「混雑制限」を選択してください。 ② 「適用」をクリックしてください。 混雑制限の設定画面が開きます。 次ページは設定画面について記載します。

① 混雑制限ゾーンの名前を入力してください。

② ゾーンの種別が、混雑制限であることが表示されます。(変更はできません。)

③ 混雑制限ゾーンは、「グローバル」のみのサポートです。(変更はできません。)

④ この混雑制限ゾーンの有効/無効を変更することができます。完全に削除したくないが機能として停止させたい場合は、「無効」を選択してください。

⑤ 入室 の判断として利用する端末を選択してください。

⑥ 退室 の判断として利用する端末を選択してください。

⑦ 入室可能とする最大人数を入力してください。

⑧ 入室済み人数の自動リセット(入出済みを 0 人とする)機能をご利用の場合は、発動する時間を設定してください。

⑨ 最大人数まで行くまでに、途中で 2 段階 警告通知が可能です。必要に応じて設定してください。
1 段階目/2 段階目で警告を発生させる人数を入力してください。

⑩ 端末と通信が取れない場合、入室/退室の両方を許可するか、退室のみを許可するかを設定してください。

⑪ 入室しても、通常の人数としては、カウントされないアクセスグループを指定することができます。

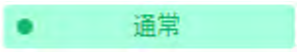
設定が完了したら、[適用]をクリックしてください。

次のページの画面になります。

ゾーンが作成されると、上記の表示になります。

① 作成した混雑制限ゾーンの名称が確認できます。また、名称の後ろの ⚙ をクリックすると、前のページの設定画面になります。

② ゾーンの状態を表示します。



人数警告 1 段階目に達していない場合

人数警告 1 段階目に達した場合

入室制限人数 に達した場合

③ 現時点の 入室人数と、制限人数が確認できます。

共連れなどにより、実際とずれてしまったときの為、 ⊖ ⊕ のボタンにより、現在入室人数を調整することが可能です。

④ バイパスグループで登録されているユーザーの入室人数が表示されます。

こちらにカウントされる人数は、③の人数には加算・減算されません。

⑤ クリックするとゾーンの動作状態が確認できます。

⑥ 画面をフルスクリーン表示する場合にクリックしてください。(実際に、認証機横にモニターなどで表示する場合の利用方法です。)

※ESC キーを押すと、画面が戻ります。

警告 1 人数/警告 2 人数/混雑制限 などは、警報イベントが発生します。

警報発生時には、21.6 章で記載した内容が設定可能です。(リレースイッチを動作させる/メールを送信する 等)

また、混雑制限ゾーンを設定した場合、FaceStation2 および、FaceStation F2 の待機時の画面は以下の表示となります。

(写真 左:警告 1 人数前 / 中央:警告 1～制限値まで / 右:混雑制限人数に達した場合)

【FaceStation2】

【FaceStation F2】

27 勤怠の設定

BioStar2 システムは、勤怠システムとしても利用することが可能です。
本章では、BioStar システムを勤怠システムとして利用する場合の設定について記載します。
（勤怠システムとしてご利用されない場合は、設定の必要はございません。）

27.1 勤怠システム利用の初回設定

勤怠の初期設定を利用する場合は、右の図の
「勤怠」 

をクリックしてください。

次ページの画面が出ます。
もし、下図のような画面が表示されましたら、管理者 ID および
パスワードを入力し「登録」をクリックしてください。
Biostar2 のログイン画面に戻りますので、再度ログイン
してください

弊社の標準でのインストールの場合、

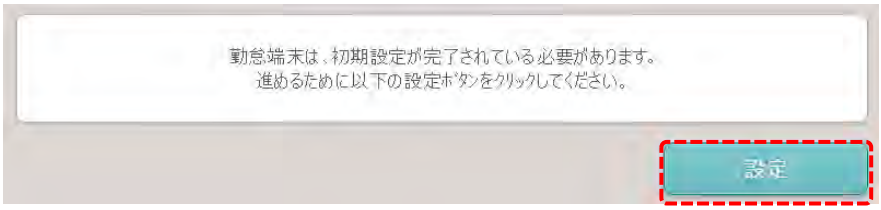
ユーザーID： admin

パスワード： Admin1234

となります。

次に前述の「勤怠」 

をもう一度クリックしてください。
下図の画面が出ましたら、「設定」をクリックしてください。



下図の画面が出ます。未登録端末の中から、勤怠に使用する端末に☑をいれてください。

＋登録 をクリックしてください。

送信者情報の「編集」をクリックすると、勤怠の警告をメールで送信することができます。

右図の設定内容を入力し、「適用」をクリック
してください。（内容については、システム管理者
等にご確認ください。）

各種データをエクスポートすることができます。
そのデータ出力の項目区切りを「，」または「/」
を選択できます。

すべての設定が終了したら、 をクリック
してください。

27.2 勤怠端末の設定

勤怠に使用する端末の設定を行います。 設定 をクリックしてください。

端末の勤怠モードの設定画面が表示されます。勤怠モードと、各キーのイベントを設定します。

① 勤怠モードの選択です。未使用、ユーザー選択、スケジュール、最終選択内容、固定から選択します。
それぞれの動作については以下の通りです。

- ・未使用 : 勤怠端末として利用しません。
- ・ユーザー選択 : 利用者が端末のボタンを押して、勤怠イベントを選択利用します。
- ・スケジュール : 時間帯に応じて、設定してある勤怠イベントとなります。
- ・最終選択内容 : 利用者が最後に押した端末のボタンの勤怠イベントが保持されます。
- ・固定 : 端末毎に、勤怠イベントを固定とします。

② 勤怠イベントの設定です。各モードに合わせたイベントの表示内容と、勤怠タイプを選択してください。
勤怠タイプは、出勤、退勤、休憩開始、休憩終了、食事開始、食事終了から選べます。
注意:勤怠イベントを変更すると、過去のイベント内容も変更されてしまいます。

③ 勤怠モードのユーザー選択と固定を選択したときにそれぞれ表示されます。

- ・ユーザー選択の場合は、勤怠必須入力の選択になります。

「はい」を選択すると、操作時に勤怠入力が必須になります。また。「いいえ」を選択した場合は、操作時に勤怠入力を行わなくても端末装置の動作が継続できます。

・固定選択の場合は、固定勤怠キーの選択になります。

固定したい勤怠イベント釦を選んでください。

④ 設定が終了しましたら、「適用」をクリックしてください。設定が反映されます。

27.3 時間規則の作成

勤怠では、勤怠管理、残業管理、休暇管理の時間に対して、割増率 及び 管理上の色の設定をすることが可能です。この項目の事を、「時間規則」と呼びます。

勤怠の設定をする上では、必ず、1つ以上の時間規則が必要となります。

時間規則の設定内容は、他の設定で引用します。他の設定で引用すると時間規則の設定内容が変更できなくなります。

説明図	操作内容
	① 時間規則を作成するため、「勤怠」をクリックしてください。
	① 「シフト」のタブをクリックしてください。 ② 「時間規則」の項目をクリックしてくだい。 ③ 「時間規則の追加」をクリックしてください。

ここまでの操作で、時間規則の作成画面になります。

画面の内容について、次のページで説明します。

① 時間規則の名称を入力してください。(区別が付く名前を推奨します。名前でソートされて表示しますので、頭に 0, 1, 2・・とか A,B,C・・とか付加すると希望通りの順に並びます。)

② 説明を追記できます。(空欄でも構いません。メモ代わりにご利用ください。)

③ 勤怠管理 / 残業管理 / 休暇管理 から選択可能です。休暇管理を選択すると、以降の表示が変更になる部分があります。

④ ③で、勤怠管理 または 残業管理を選択した場合に表示されます。賃金の割増率を変更できます。

例: 勤怠管理の「定時間」は、1, 残業管理の残業時間帯は、1.2, 残業管理の深夜残業時間帯は、1.5 などと利用できます。

選択した倍率で、勤務時間として計算されます。(仮に、1.5 とした場合、実際に 10 分働くと、15 分と表示・計算されます。)

⑤ 各時間規則を次の「シフトの作成」画面で、割当てます。その際に、色で区別されることになるため、各時間規則を何色で表示するか？を指定する形となります。他の時間規則と区別しやすい色を選択してください。

⑥ 時間規則の作成を適用して、新たに別の時間規則を追加する場合に、クリックしてください。

⑦ 時間規則の作成を適用して、次の「シフト作成」の画面に進みます。時間規則の作成が現行の物だけで良い場合はこちらをクリックしてください。

⑧ 時間規則の作成を適用して、時間規則の画面に戻ります。複数の時間規則を作成する場合は、こちらをクリックしてください。

種別に「休暇管理」を選択した場合

⑨ 休暇管理 を選択した場合、⑩以降の表示となります。

⑩ 就業扱い休暇 / 非就業扱い休暇 を選択してください。

例:就業扱い休暇は、有給休暇のような考え方で、勤務時間として扱います。

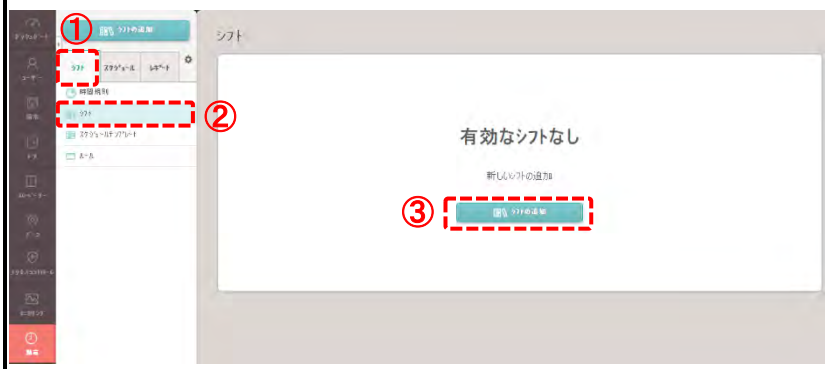
非就業扱い休暇は、届け出休暇や、無断欠勤のような考え方で、勤務時間としては扱わない休暇となります。

⑪ ⑨で休暇管理を選択した場合は、「適用して新規追加」と「適用」ボタンのみとなります。

上記のように、必要な時間規則を作成してください。

27.4 シフトの作成

1 日分の勤務スケジュールの作成を行います。本システムでは、1 日分の勤務時間を「シフト」と呼びます。
シフトは、固定時間のシフトとフレックス時間のシフトを作成可能です。ここでは、前項の時間規則の作成にて、
以下の時間規則を作成済みとして説明をします。

説明図	操作内容
	① シフトを作成するため、「勤怠」をクリックしてください。
	① 「シフト」のタブをクリックしてください。 ② 「シフト」の項目をクリックしてください。 ③ 「シフトの追加」をクリックしてください。

ここまでの操作で、シフトの作成画面になります。
画面の内容について、次のページで説明します。

① シフトの名称を入力してください。(区別が付く名前を推奨します。)

② 説明を追記できます。(空欄でも構いません。メモ代わりにご利用ください。)

③ 固定時間 / フレックス時間 / フローティング時間 から選択可能です。
選択内容により、以降の表示が切り替わります。

④ 日の勤怠データとして考えた際に、どの時間で日を区切るかを指定します。上記の様に、5 時 を指定した場合は、
当日 5 時～翌日 5 時までを、当日の勤務時間として考えます。
日の前/後の時間を許可にした場合は、前日分と、翌日分の勤務時間として換算する時間を設定可能です。

⑤ ファンクションキーを備えていない端末をご利用の場合は、明示的に「出勤」「退勤」を記録することができません。このため、④で指定した日の枠の中で、自動的に、最初の認証を出勤とし、最後の認証を退勤とする場合は、「はい」を設定してください。「いいえ」を選択した場合は、最初と最後のデータに出勤や退勤の情報が付与されません。

種別(③)で、固定時間 を選んだ場合

⑥ ④の日の開始時間が、小さな▼(エメラルドグリーン)で表示されます。

⑦ ④の日の前/後の時間が、小さな▼(焦げ茶)で表示されます。

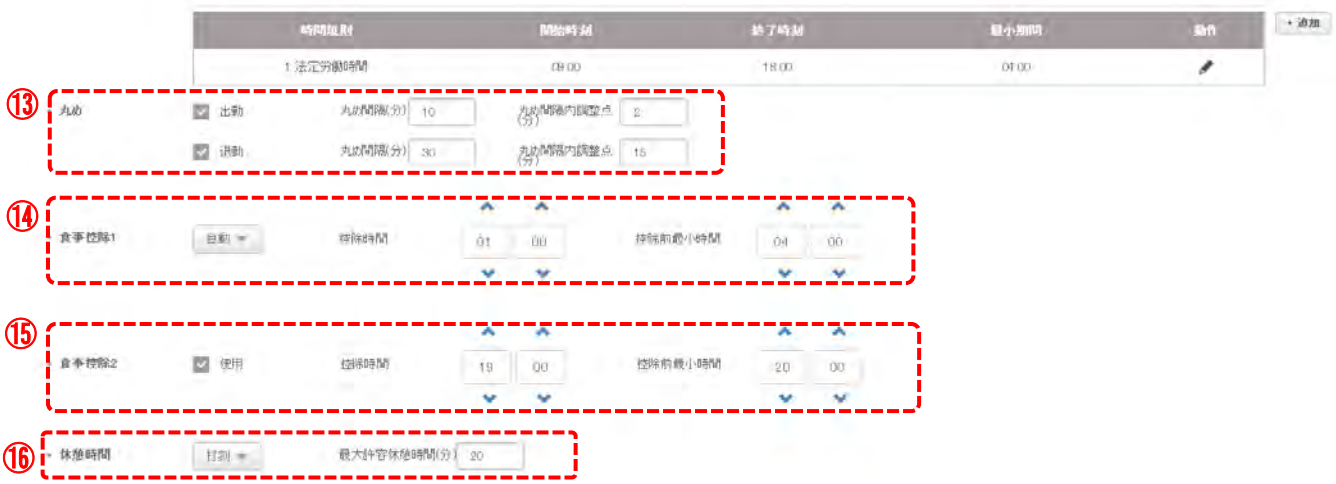
⑧ ⑨以降で、1 日のシフトとして時間規則を登録し、作成していきます。それぞれの時間規則の指定時間が指定色で表示されます。

⑨ 時間規則を選択します。勤怠管理の時間規則を必ず設定する必要があります。(勤怠管理の時間規則は、1 日に 1 つの登録です)
それ以外に、残業管理の時間規則は、複数登録することが可能で最大 5 個まで可能です。

⑩ 該当の時間規則の開始と終了時間を指定します。⑧のグラフと連動します。また、勤務時間として認める最短時間を設定可能です。
上記の例の場合、9:00～18:00 の間で、最低 4 時間は勤務しないと、不十分な作業時間として 0 分とします。4 時間以上は勤務したが、開始・終了の時間に未達の場合は、遅刻や早退として、勤務時間を扱います。

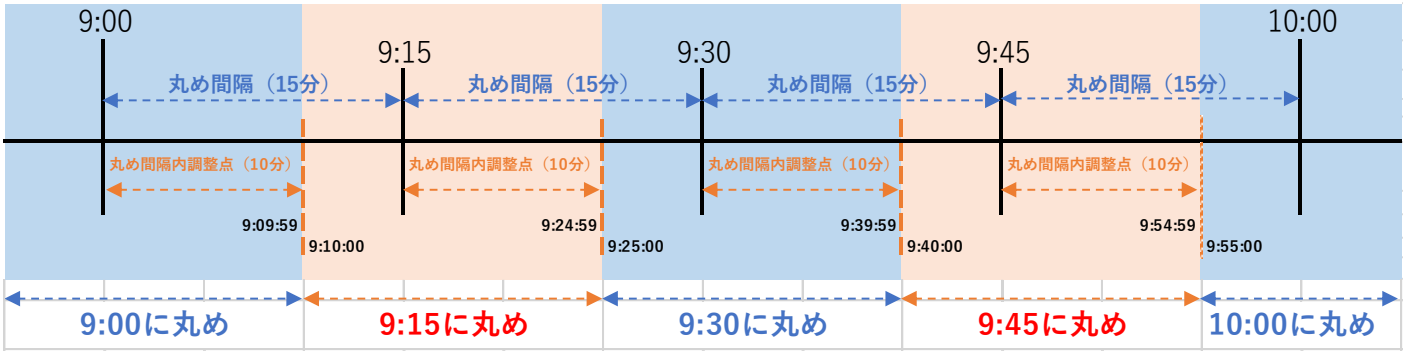
⑪ 時間猶予について、使用 に☑を入れた場合は、出勤と退勤について、それぞれ猶予する時間(分)を設定可能です。
遅刻/早退の判定に猶予を設定したい場合は、☑を入れてご利用ください。

⑫ 追加 ボタンをクリックすると、⑨～⑪の範囲で設定した内容が、追加されます。



⑬ 丸めは、出勤と退勤でそれぞれ別に設定することが可能です。☑をすると右側に、値の設定欄が表示されます。
丸め間隔は、何分単位で丸めるか？の刻み幅を設定します。例えば、丸め間隔を 15 に設定したら、
各時間の 00 / 15 / 30 / 45 のどこかの時間が、出勤または退勤時間となります。
丸め間隔内基準点は、丸め間隔の中のどこを基準に、どちら方向に丸めるか？を指定します。それを、早い時間側からの時間位置で指定します。

丸め間隔を 15 分　丸め間隔内基準点を 10 分 とした場合の例を以下に記載します。



食事控除 1 は、打刻利用/自動/固定 から選択可能です。
打刻利用を選択した場合は、液晶付きの認証機をご利用の場合、ファンクションキーを押して、食事休憩開始/食事休憩終了を認証して使うことになります。自動を選択した場合は、上記の図のように 4 時間働いたら、1 時間分は食事控除として勤務時間から差し引く。というような設定が可能です。固定を選択すると、X 時～X 時の間は食事休憩とする。という固定値の設定となります。

⑭ 食事控除 2 は、食事控除に追加して、2 回目の食事控除を設定する場合に利用します。食事控除 2 を利用する場合は、使用に☑を入れてください。食事控除 1 と同方式の入力となります。上図の例は、あまり良くない例ですが 20 時間働いた場合に、19 時間を差し引く形になります。

⑮ 休憩時間は、なし/打刻/固定 から選択可能です。 なしの場合は、特定の休憩時間を設けません。打刻の場合は、休憩開始/休憩終了の打刻処理分を計算し、勤務時間から差し引きます。固定 の場合は、休憩時間を指定する画面になります。
打刻を選択した場合で、ある程度の時間範囲は休憩を許容する場合は、最大許容休憩時間を設定してください。（0 に設定すると、許容はなしで、休憩を取ったら取った分、合計時間から減算されます。）

時間規則を追加する場合

ここまでは、通常時間の業務について 1 つの時間規則を追加する方法を記載しています。

残業時間や深夜残業時間などを追加する場合は、以下の手順で行ってください。

① 通常勤務の時間規則の情報の横の「＋追加」ボタンをクリクします。

② 上図の赤枠の部分が表示されます。

③ 時間規則を選択してください。

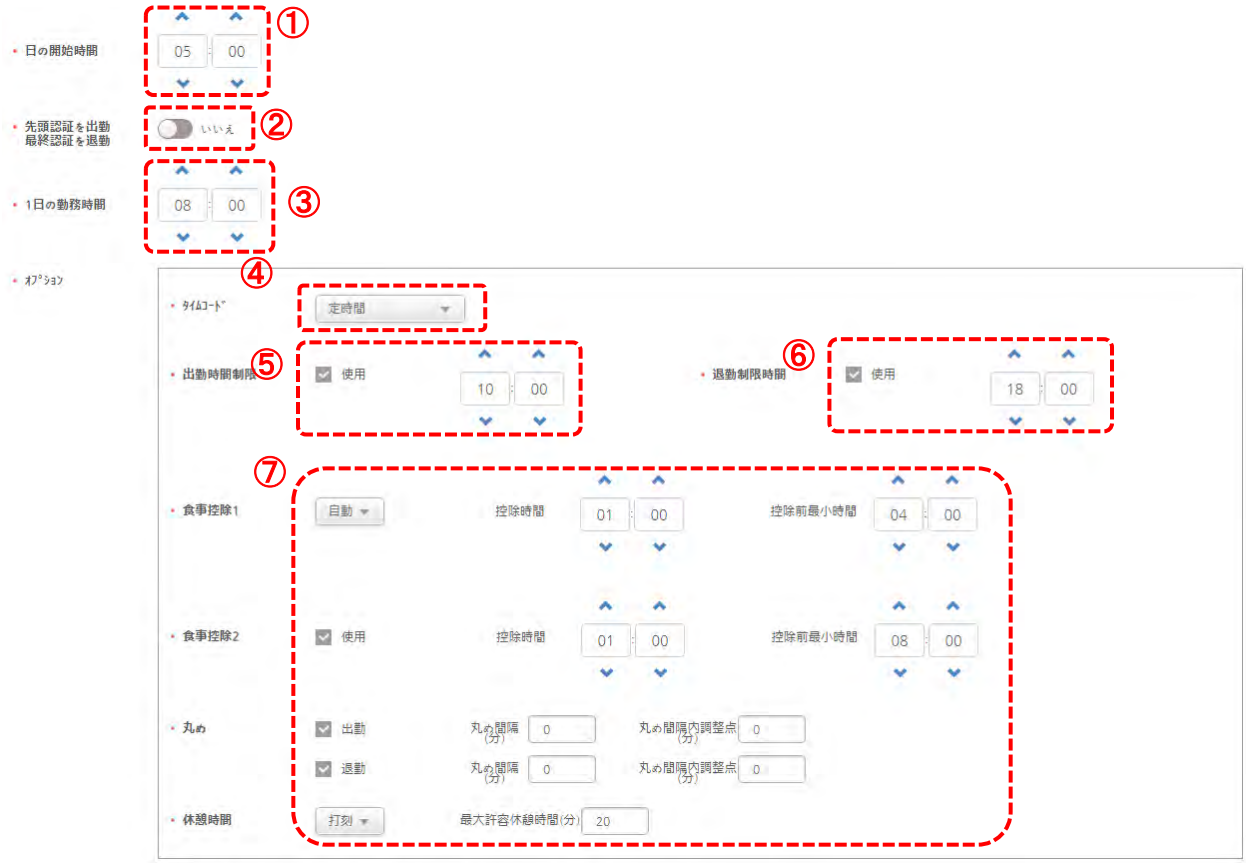
以下の画面表示に切り替わります。

開始時刻、終了時間、最小時間、必要な場合は、丸めとその時間を調整してください。

④ 「追加」ボタンをクリックしてください。

1 日単位のスケジュールの作成が完了したら、最後に、「適用」をクリックしてください。

種別(③)で、フレックス時間 を選んだ場合



① フレックス時間の 1 日の開始時間を設定してください。

② 当日の認証記録の最初を出勤/最後を退勤として扱うか？を選択してください。

③ 1 日の最低基準となる勤務時間を設定してください。

④ 勤怠管理の時間規則の中から、登録する時間規則を選択してください。

⑤ 出勤時間の制限をもたせる場合は、☑を入れ、その時間を指定してください。

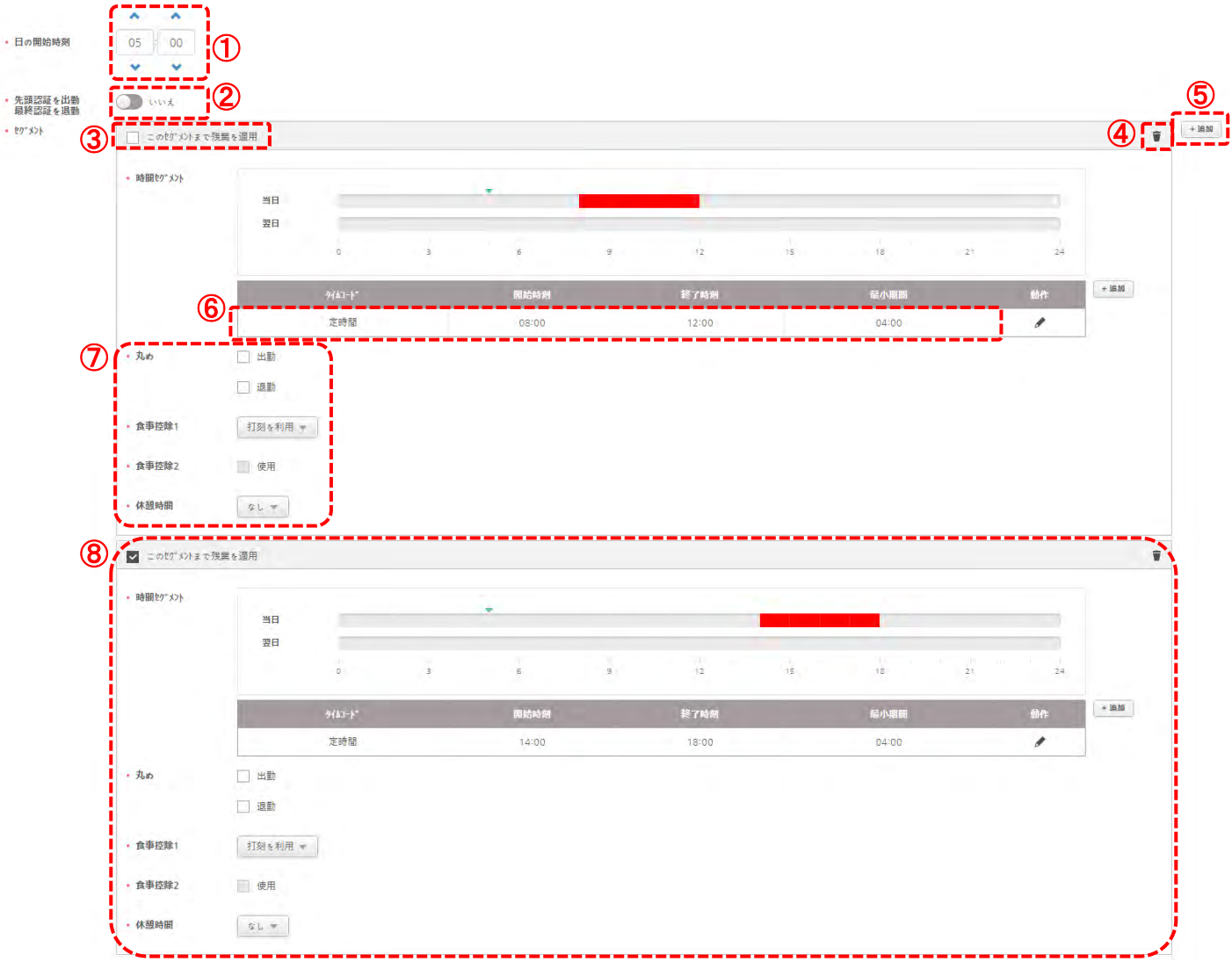
⑥ 退勤時間の制限をもたせる場合は、☑を入れ、その時間を指定してください。

⑦ 食事控除 1 と食事控除 2 と丸めと、休憩時間については、固定時間の時と同様です。そちらを参照してください。

このように、1 日単位のシフトを作成してください。

種別(③)で、フローティング時間 を選んだ場合

フローティング時間は、勤怠管理時間を区切り、部分的な勤務時間として組み合わせができる機能です。このため、残業管理の時間規則を利用することはできません。フローティングシフトは、最大 5 つのシフト設定が可能であるため、毎日、勤務時間が変わるような勤務形態の方は効率的に利用することが可能です。



① フローティング時間の 1 日の開始時間を設定してください。

② 当日の認証記録の最初を出勤/最後を退勤として扱うか？を選択してください。

③ 複数のフローティング設定(塊)がある場合に、どのセグメントまで残業を適用するか？を☑を入れて設定します。

④ 該当のフローティング設定を削除する場合にクリックしてください。

⑤ フローティング設定を追加する場合にクリックしてください。

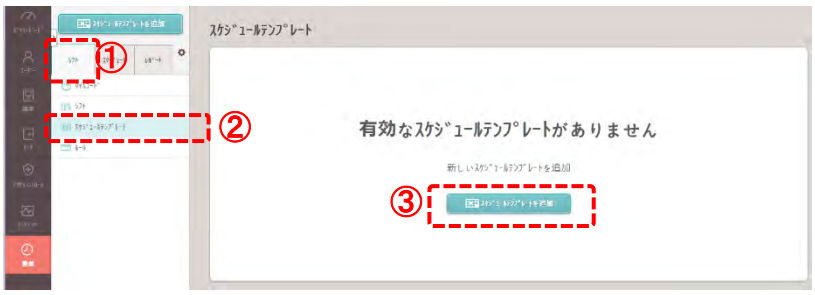
⑥ フローティング設定内の時間を設定してください(設定方法は固定時間を参照してください。)。

⑦ 食事控除 1 と食事控除 2 と丸めと、休憩時間については、固定時間の時と同様です。そちらを参照してください。

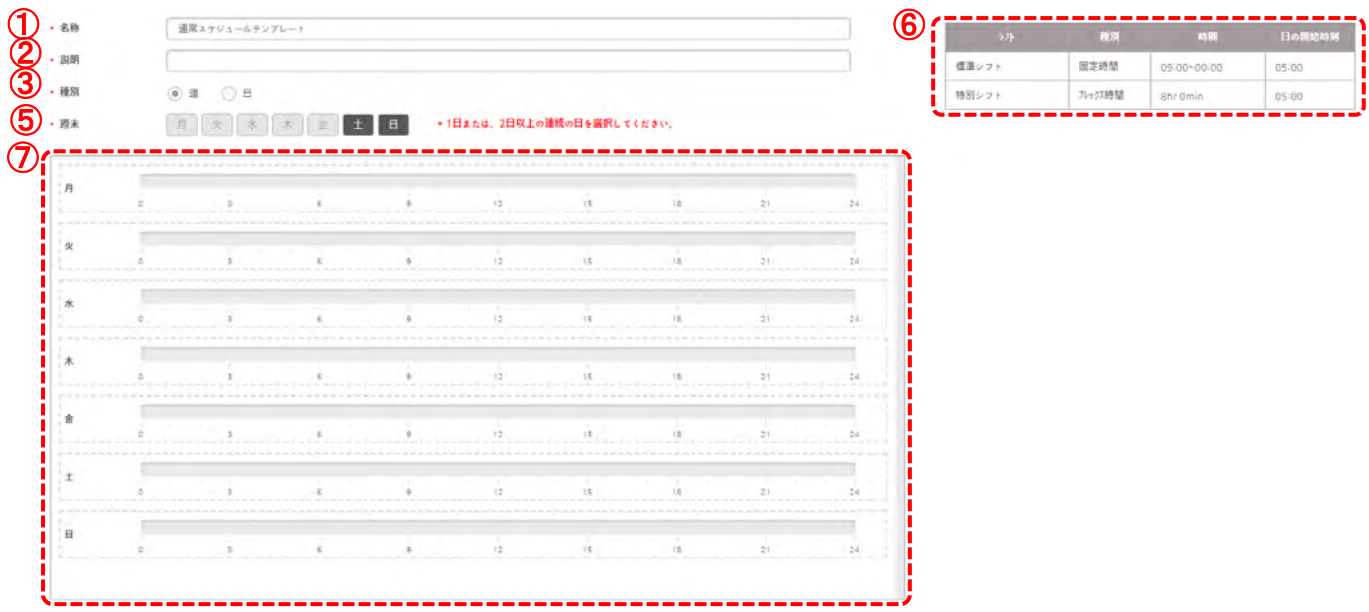
⑧ 2 つ目以降のフローティング設定も、必要に応じて同様に設定してください。

27.5 スケジュールテンプレートの作成

1 週間単位、あるいは、指定日数単位で、シフトの設定を行います。これらのシフトの組み合わせを設定したものを、本システムでは、「スケジュールテンプレート」と呼びます。

説明図	操作内容
	① スケジュールテンプレートを作成するため、「勤怠」をクリックしてください。
	① 「シフト」のタブをクリックしてください。 ② 「スケジュールテンプレート」の項目をクリックしてください。 ③ 「スケジュールテンプレートの追加」をクリックしてください。

ここまでの操作で、スケジュールテンプレートの追加画面になります。
画面の内容について、次のページで説明します。



① スケジュールテンプレートの名称を入力してください。(区別が付く名前を推奨します。)

② 説明を追記できます。(空欄でも構いません。メモ代わりにご利用ください。)

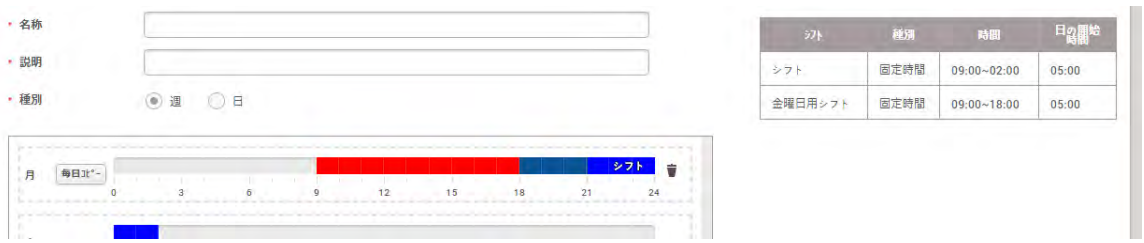
③ 週 / 日 から選択可能です。選択内容により、以降の表示が切り替わります。

④ ③で「日」を選択した場合は、何日周期にするか？の選択項目が表示されます。
1～90 の範囲で入力してください。

⑤ 週末の設定は、1 日 または 2 日以上の連続した日を選択してください。

⑥ 作成済みのシフトがリスト表示されます。周期的シフトを作成するため⑥から⑦に対し、ドラッグアンドドロップし、各日のスケジュールを作成します。

⑦ ⑥からのドラッグアンドドロップを受け付けます。ドロップされると、時間が表示され、削除用のゴミ箱マークも表示されます。
また、⑥の先頭の日にドロップした場合は、同じものを毎日分コピーできるように「毎日コピー」のボタンが表示されます。



一般的なスケジュールテンプレートの場合は、設定するシフトを月曜日の部分にドラッグアンドドロップし、「毎日コピー」ボタンをクリックし、毎日にコピーした後、土曜日と日曜日のゴミ箱アイコンをクリックすると、簡単にスケジュールテンプレートが作成できます。

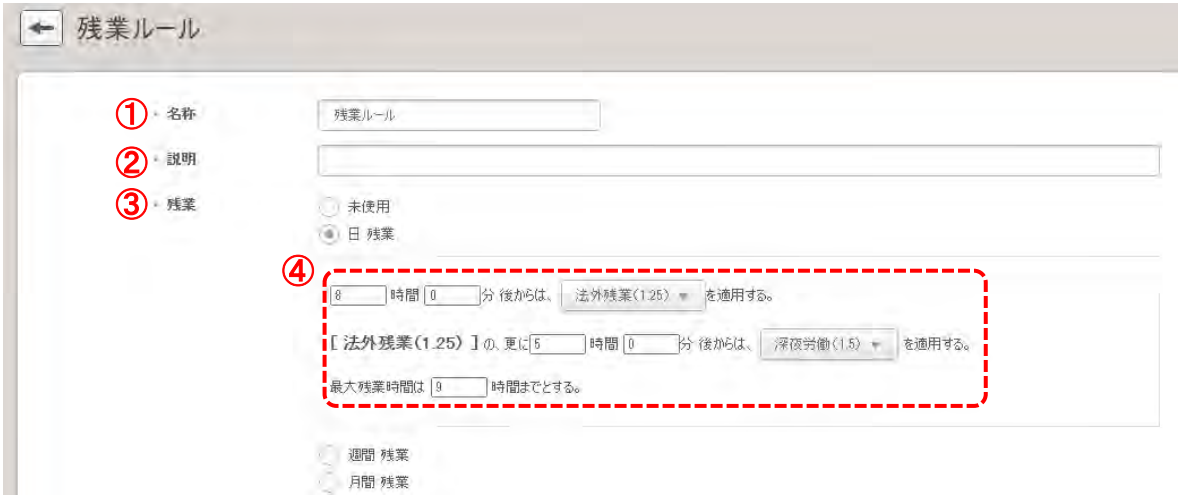
27.6 ルールの作成

残業時のルールを設定する事が可能です。残業時の時間率を個別に利用する場合に、本設定を利用可能です。

説明図	操作内容
	① ルールを作成するため、「勤怠」をクリックしてください。
	① 「シフト」のタブをクリックしてください。 ② 「ルール」の項目をクリックしてください。 ③ 「ルールの追加」をクリックしてください。

ここまでの操作で、ルールの追加画面になります。
画面の内容について、次のページで説明します。

1 日単位の超過勤務時間、1 週間単位の超過勤務時間、および 1 か月単位の超過勤務時間のルールを決めることができます。通常の勤務時間の後に適用する超過勤務時間の時間規則（賃金の割増率）を設定し、特定の時間の後に別の超過作業時間の時間規則を適用することができます。
また、最大超過勤務時間を設定して、従業員の超過勤務時間を制限することもできます。



① ルールの名称を入力してください。（区別が付く名前を推奨します。）

② 説明を追記できます。（空欄でも構いません。メモ代わりにご利用ください。）

③ 未使用 / 日 残業 / 週間 残業 / 月間 残業 から選択可能です。

未使用 以外を選んだ時は、④部分が表示されます。

④ ③で選択した残業に対し、特別にルールを適用することが可能です。設定できる内容は以下となります。

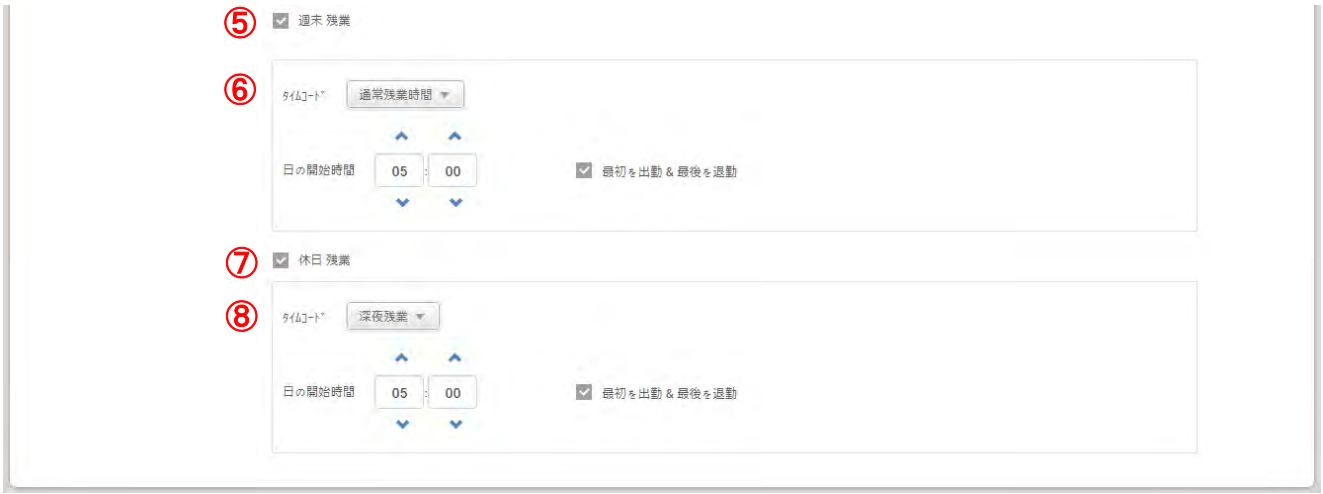
・〇時間〇分後からの残業時間とし、時間規則（賃金の割増率）を決めます。

・その後、更に 〇時間〇分後からの残業時間の時間規則（賃金の割増率）を決めます。

・最大で、許可する残業時間は 〇時間までと決めます。

の内容を設定可能です。

上記の設定をすると、一日の勤務時間は8時間（1時間の休憩を含む）、その後時間外を 5 時間実施した場合の時間外割増率を1．25倍、それ以降の時間外割増率は1．5倍とし、一日の最大時間外勤務時間は9時間とした場合です。（22 時以降、深夜残業割増という設定はできません。）



⑤ 個別ルールで、週末（土曜日・日曜日）の残業を個別に指定する場合は、☑を入れてください。

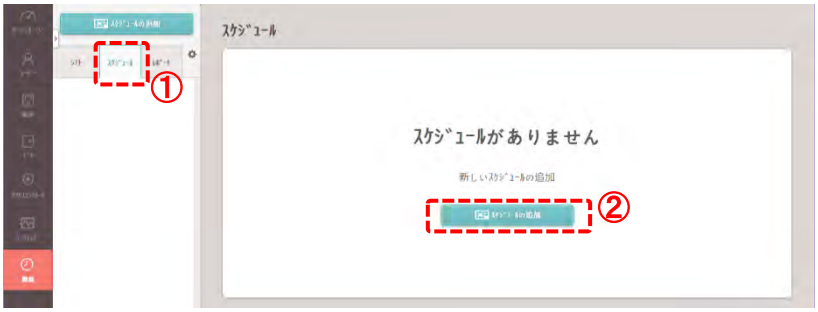
⑥ ⑤に☑した場合、週末の時間規則と、日の開始時間、最初と最後の認証を出退勤と判断するか？を指定してください。

⑦ 個別ルールで、祝日（土曜日・日曜日ではなく、BioStar2 の祝日として指定した日）の残業を個別に指定する場合は、☑を入れてください。

⑧ ⑥に☑した場合、祝日の時間規則と、日の開始時間、最初と最後の認証を出退勤と判断するか？を指定してください。

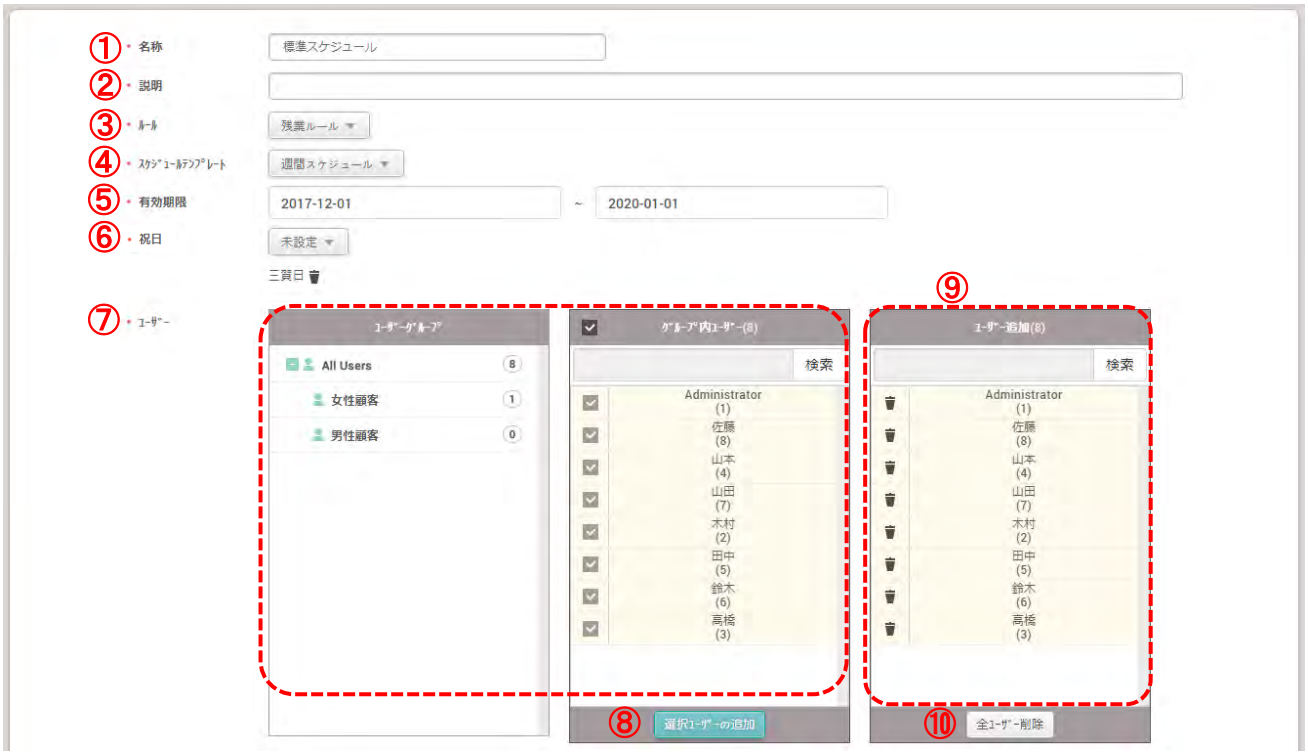
27.7 スケジュールの作成

勤怠のスケジュールに対し、対象ユーザーや期間、等の設定を行います。

説明図	操作内容
	① スケジュールを作成するため、「勤怠」をクリックしてください。
	① 「スケジュール」のタブをクリックしてください。 ② 「スケジュールの追加」をクリックしてください。

ここまでの操作で、スケジュールの追加画面になります。

画面の内容について、次のページで説明します。



① スケジュールの名称を入力してください。(区別が付く名前を推奨します。)

② 説明を追記できます。(空欄でも構いません。メモ代わりにご利用ください。)

③ ルールを選択してください。(作成済みの残業ルールから選択可能です。使用しない場合は、「未設定」を選択してください。)

④ このスケジュールのベースとなるスケジュールテンプレートを選択してください。(作成済みのスケジュールテンプレートから選択可能です。)

⑤ このスケジュールの有効期間を選択してください。

⑥ 祝日(土日ではなく、BioStar2 システムで祝日に指定した日)がある場合は、指定してください。
指定すると、下に表示されます。不要な場合は、ゴミ箱アイコンをクリックして指定解除してください。

⑦ このスケジュールの対象とするユーザーに☑をつけて選択してください。勤怠ライセンスを適用していない場合は、99 ユーザーまで登録可能です。
(勤怠ライセンスを適用している場合は、全ユーザーを登録することができます。)

⑧ ⑦で対象とするユーザーを選択したら、「選択ユーザーの追加」クリックしてください。選択したユーザーが、⑨のリストに表示されます。
⑨のリストに入ったユーザーが勤怠管理の対象となります。

⑨ 勤怠管理の対象ユーザーの一覧が表示されます。対象から除外する場合は、各ユーザーのゴミ箱アイコンをクリックしてください。

⑩ 勤怠対象ユーザーを全員解除する場合に「全ユーザー削除」をクリックしてください。

設定後、画面下の「適用」ボタンをクリックすると、決定されます。

28 トラブルシューティング（FAQ）

ここでは、よくある質問をまとめ、対策方法を記載します。

28.1 BioStar2 の画面が表示されなくなってしまった

以前まで BioStar2 に接続できていた場合で、突然、接続できなくなった場合は、以下の内容が考えられます。

- ・BioStar2 サーバーPC あるいは、サーバーPC プログラムが停止している
- ・BioStar2 サーバーPC の IP アドレスが変更され、クライアント PC からサーバーPC に通信できていない
- ・対象ではないブラウザでアクセスしている
- ・クライアント PC の web ブラウザが、プロキシサーバーを利用する設定になっている
- ・BioStar2 サーバーPC のウィルス対策ソフト等の更新により、ファイアーウォールが有効になった
- ・データベースのデータが破損し、動作できない

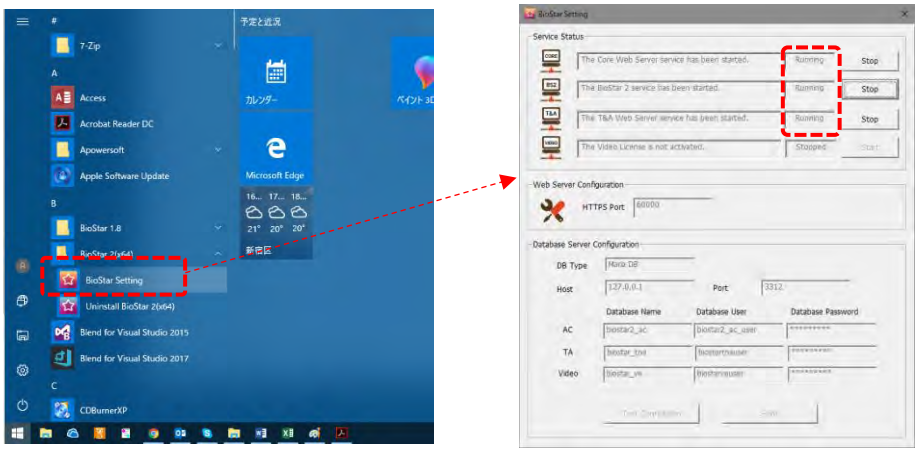
など。

以下の内容を確認してください。

① BioStar2 サーバープログラムが、動作しているか？を確認してください。

サーバーPC のスタートメニューから、BioStar2 グループの BioStat setting を起動してください。

そして、上部 3 段のプログラムが、「 Running 」となっていることを確認します。



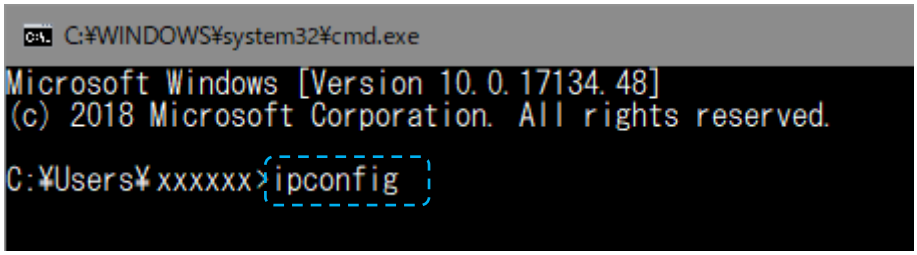
もし、Running になっていない場合は、その横の「 Start 」ボタンをクリックして Running にしてください。

② BioStar2 サーバーPC の現在の IP アドレスを確認してください。

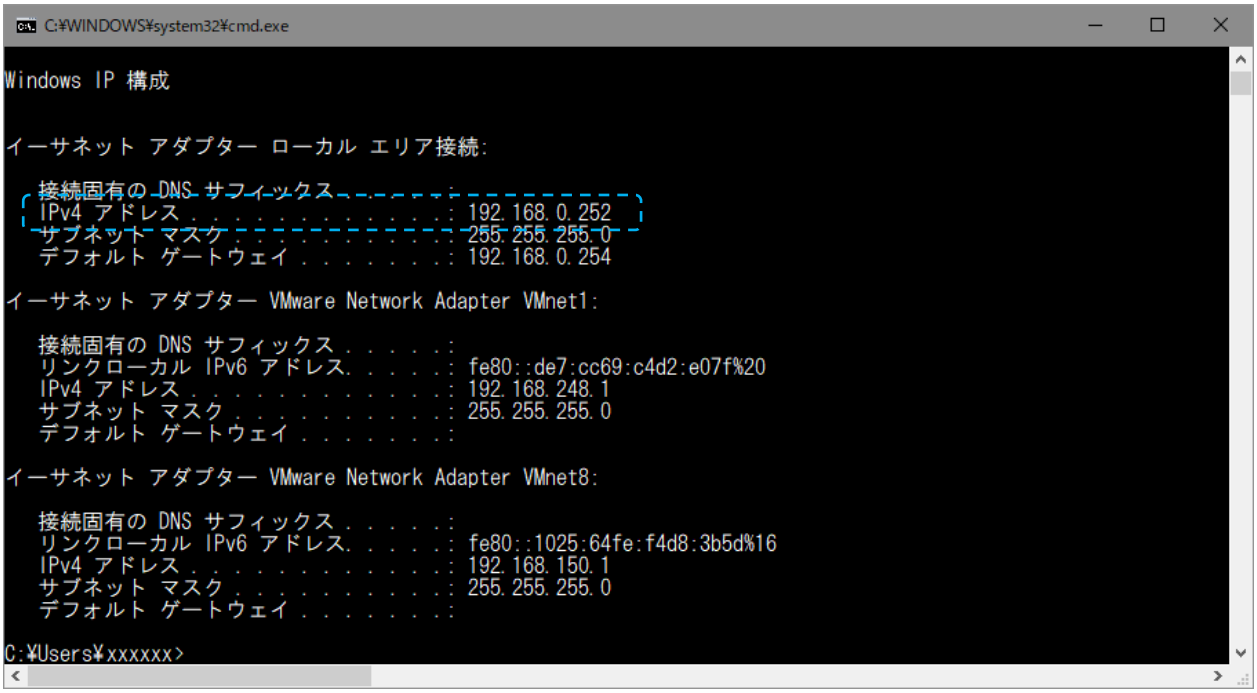
まずは、BioStar2 サーバーがインストールされている PC で、コマンドプロンプトを起動します。

（起動方法がわからない場合は、 + を押して、“ファイル名を指定して実行”のダイアログが出たら、cmd と入力し、OK をクリックしてください。）

コマンドプロンプトの画面が表示されたら、「 ipconfig 」と入力し、Enter を押してください。

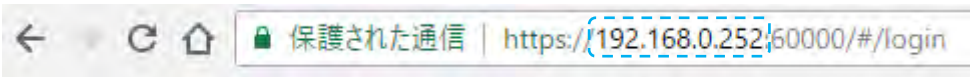


以下のような画面が表示されます。

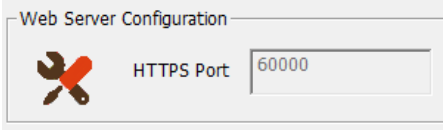


ローカルエリア接続 または、ワイヤレスネットワーク接続の **IPv4 アドレス** を確認してください。
※基本的には、ワイヤレスネットワークでの接続は推奨していないため、通常は、ローカルエリア接続となっています。
確認が終わったら、コマンドプロンプトは、右上の「 X 」をクリックし、画面を閉じてください。

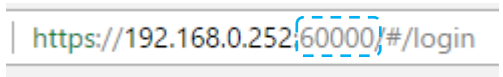
そこで、クライアント側（表示しようとしている側）の google chrome の BioStar2 のアクセス先を確認してください。



正しく、サーバーPC をアクセス先としてアクセスしていることを確認してください。
また、念の為、①の画面の中段で表示されているポート番号と、クライアント側のポート指定も一致していることを確認してください。



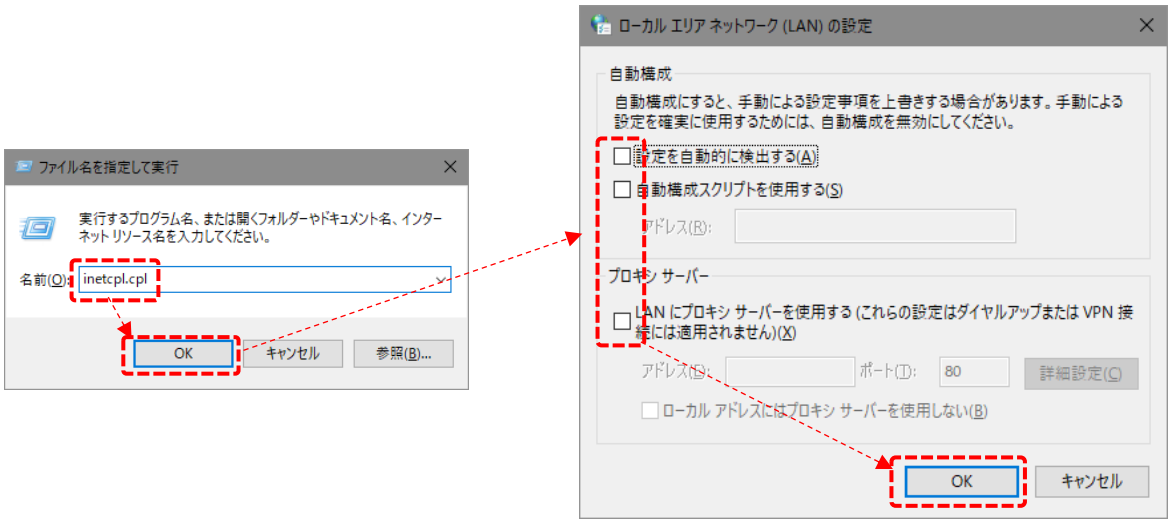
（サーバー側は、ポート番号 60000 で動作）



（クライアント側も、ポート番号 60000 を指定してアクセス）

③ 対象の web ブラウザの確認をしてください。
対象の web ブラウザは、google chrome のみです。
ご利用のブラウザが、edge や Internet Explorer や、Firefox や、Opera 等で無いことを確認してください。

④ 設定によっては、インターネットを利用するために、PC にプロキシサーバーを利用している場合があります。
この場合、指定したアクセス先がプロキシサーバーでブロックされてしまい表示できない場合があります。
このような場合は、一度、インターネットオプションで、プロキシサーバーの利用を OFF にしてください。
（起動方法がわからない場合は、 + を押して、“ファイル名を指定して実行”のダイアログが出たら、
inetcpl.cpl と入力し、OK をクリックしてください。）
インターネットのプロパティ画面が開いたら、「接続」タブ、「LAN の設定」と進み、
ローカル エリアネットワーク（LAN）の設定画面で、全ての☑をはずしてください。



これにより、BioStar2 のアクセス可否を確認してください。
もし、アクセスできるようになった場合は、代わりにインターネットへのアクセスができなくなっているはずです。
特定の IP アドレスだけ、プロキシサーバーの利用を除外する必要がありますので、プロキシサーバーの設定者と相談してください。

⑤ ファイアーウォールにより、BioStar2 サーバーへのアクセスが制限された可能について、確認が必要となります。
まずは、PC にウィルス対策ソフトが入っている場合は、そのソフトのファイアーウォールの機能を OFF にしてください。
次に、PC 側の Windows ファイアーウォールの設定で、Windows ファイアーウォールを OFF にしてご確認ください。

⑥ 上記すべてをご確認いただいても原因が不明な場合は、他の問題が考えられますので、弊社までご連絡ください。

28.2 BioStar2 にログインはできるが、端末がつながらない

以前まで端末が接続できていた状態で、突然、接続できなくなった場合は、以下の内容が考えられます。

・LAN ケーブルや HUB の電源など、通信できない理由が発生した
・サーバーPC の IP アドレスが変更され、端末→サーバー 接続の IP のサーバーアドレスが有効でない
・他の BioStar サーバーがあり、端末への接続が取り合いになっている
・RS-485 の接続情報が失われ、再接続できない状態になっている

など。

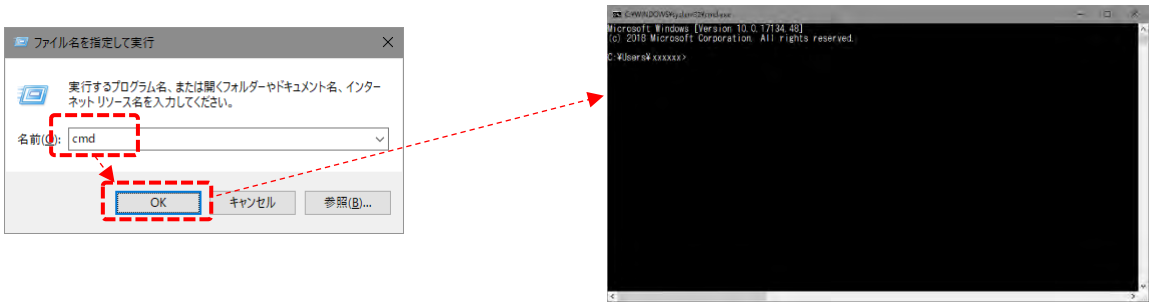
以下の内容を確認してください。

① 対象の端末に通信が通るか確認してください。(LAN 接続端末の場合)

※本確認は、サーバーPC から行う必要があります。もし、クライアント PC をご利用の場合は、参考にはなる可能性はありますが、確実ではありません。BioStar2 サーバーと、端末の通信を確認する必要があります。

まずは、BioStar2 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起動します。

(起動方法がわからない場合は、 + を押して、“ファイル名を指定して実行”のダイアログが出たら、cmd と入力し、OK をクリックしてください。)



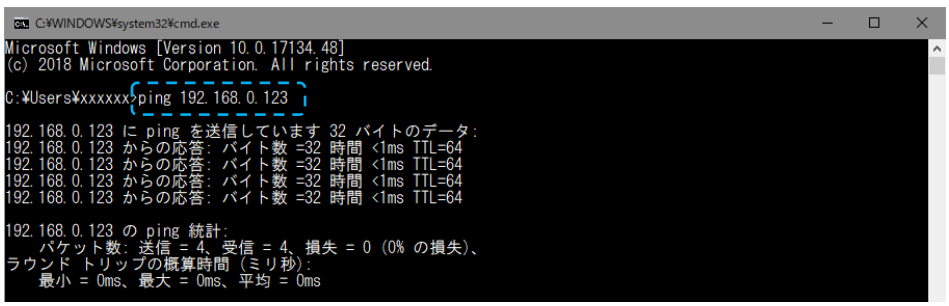
次に、端末の IP アドレスに対し、ping コマンドを実行します。

コマンドの入力は、

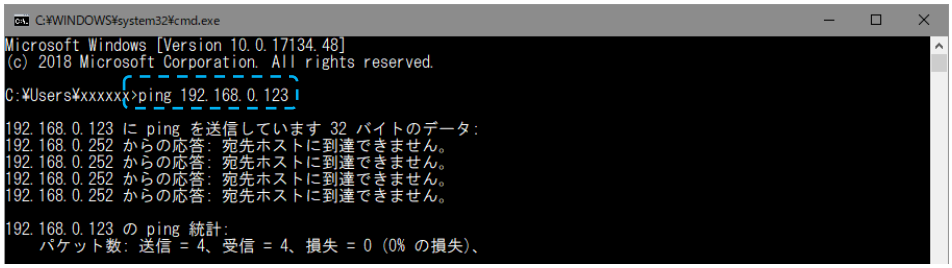
ping [IP アドレス]

となります。(例:端末が、192.168.0.123 の場合、ping 192.168.0.123 と入力)

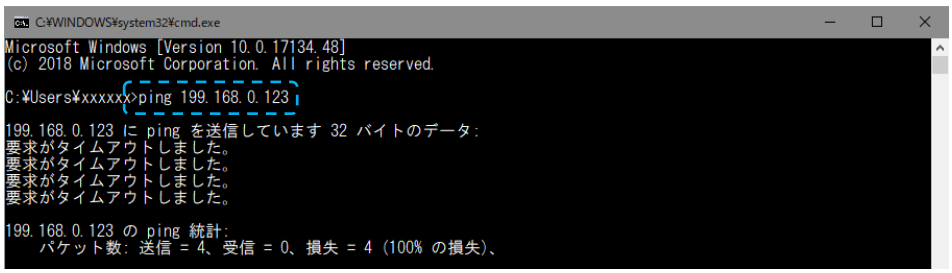
・通信が成立している場合



・通信が成立していない場合



または、サーバーPC と端末が異なるセグメントにいる場合は、以下のようになる場合があります。



通信が成立している場合は、端末の設定による部分と、他の BioStar との取り合いになっている可能性があります。端末側のサーバー設定とサーバーPC の IP アドレスを確認してください。
通信が成立していない場合は、まずは、端末の電源や、LAN ケーブルの抜け、その他、途中の HUB の接続などを確認してください。接続が問題無さそうな場合は、端末の電源を OFF/ON し、確認してください。

② LAN 接続端末の場合、端末の設定を、「 端末→サーバー 」のモードとし、端末にサーバーIP を設定した場合は、
端末からサーバーPC に向け、通信を行います。このため、このサーバーIP が間違う(あるいは変わる)と、端末が接続できなくなります。
接続はできなくとも、端末に設定されている過去のサーバーIP は表示されますので、過去に設定されたサーバーの IP アドレスと、現在のサーバーの IP アドレスが一致しているかを確認してください。

③ 2 つの BioStar2 サーバーが存在するかを確認した上で、片方がアクセスしっぱなし(画面を表示した状態)になっていないか？を確認してください。

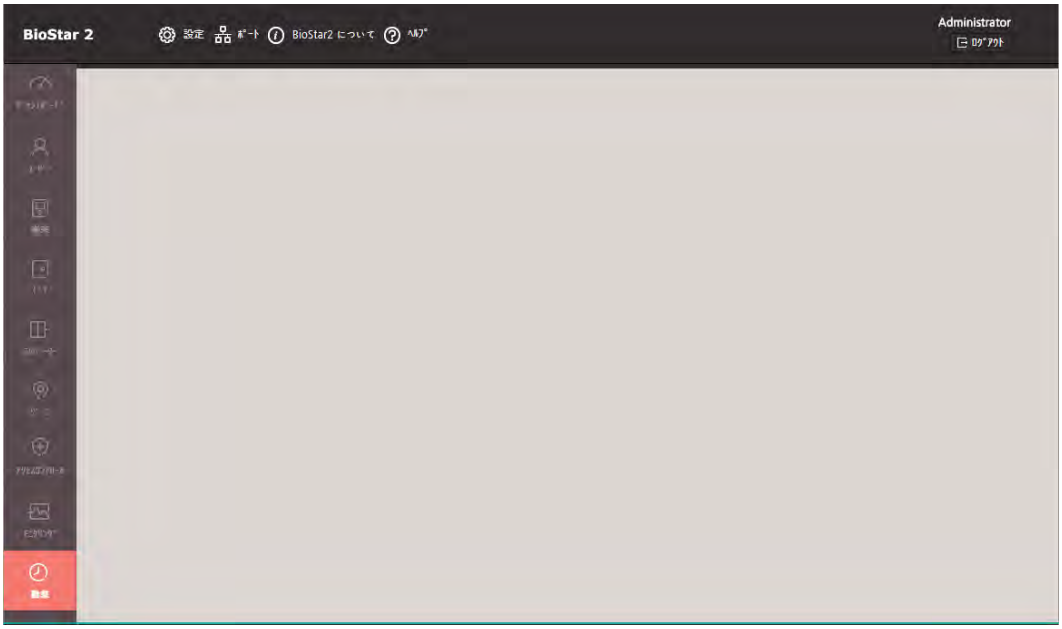
④ RS-485 接続の場合、親機との通信が途切れると、別の親機と認識してしまい、接続できなくなる場合があります。この場合は、端末を削除し、子機を初期化し、再度、端末追加を行う必要がある場合があります。

28.3 プライバシーが保護されない。という画面が表示される

プライバシーが保護されていない。という画面が表示される理由は、サーバーに対して、HTTPS の通信をする際に、サーバー証明書が正しくインストールされていない場合に表示されます。BioStar2 サーバーに対し、初めてアクセスする場合は、表示されます。プライバシーを保護する HTTPS の通信を行うためには、サーバー証明書をインストールする必要があります。
以下の方法で、サーバー証明書をインストールしてください。
サーバー証明書のインストール方法については、インストール DVD の中のシステム一式インストール手順書の 5 章で記載しています。そちらをご参照ください。

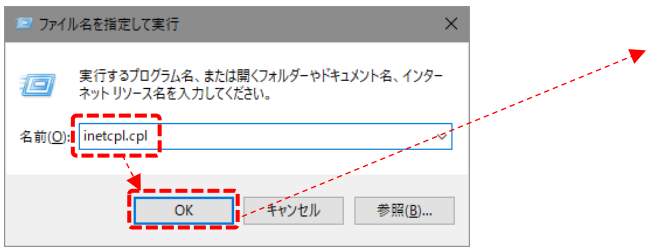
28.4 勤怠画面が表示されない（勤怠画面の後、動作が遅い）

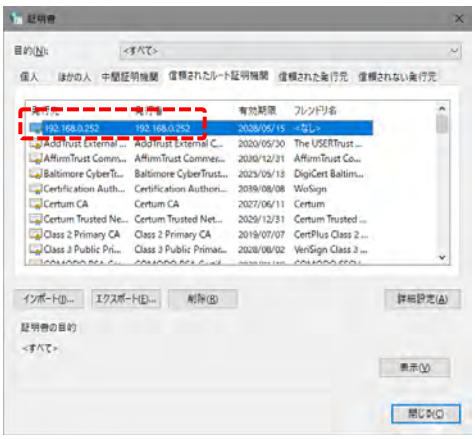
「勤怠」メニューにアクセスした場合に勤怠の画面が表示されない場合があります。



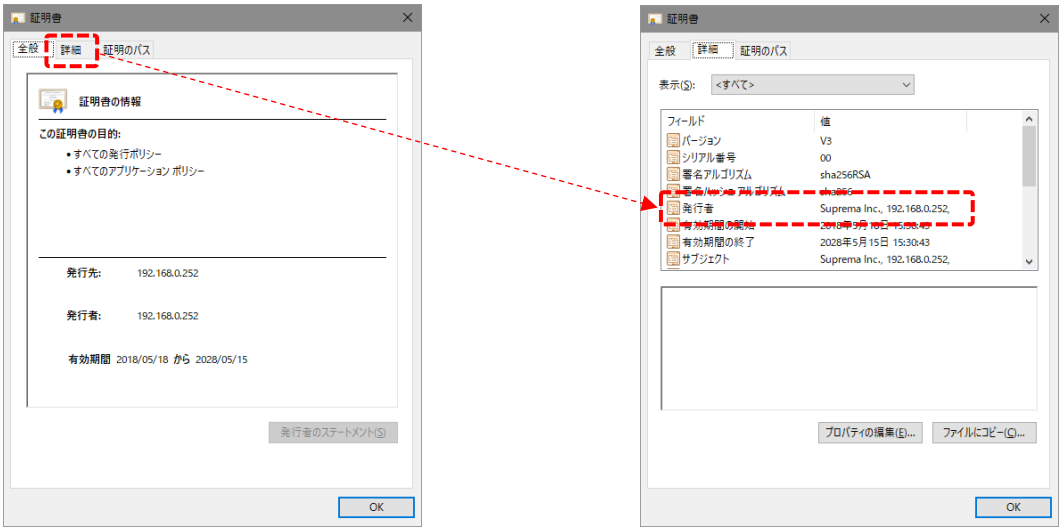
この場合は、HTTPS の証明書が、当初の予定のものと異なっていることが要因です。HTTPS 証明書をインストール後、BioStar2 サーバーの IP アドレスが変更になった場合などに、このような症状となります。
対策として、新しい BioStar2 サーバーの IP アドレス宛で、再度、HTTPS の証明証をインストールする必要があります。
（また、対象外の web ブラウザをご利用の場合も、このようになりますので、web ブラウザが google chrome であることも同時にご確認ください。）

対応手順として、まずは、インターネットのプロパティを表示します。
（起動方法がわからない場合は、 + を押して、“ファイル名を指定して実行”のダイアログが出たら、
inetcpl.cpl と入力し、OK をクリックしてください。）
インターネットのプロパティ画面が開いたら、「コンテンツ」タブ、「証明書」と進み、
証明書の画面で、「信頼されたルート証明書機関」のタブをクリックし、発行先と発行者が、両方共、IP アドレスの項目を探してください。





両方共 IP アドレス表記の項目を見つけたら、W クリックしてください。以下の画面が表示されます。
「詳細」タブをクリックしてください。



発行者の部分に、「 Suprema Inc., 」と入っていたら、それが対象となります。
OK ボタンをクリックし、前の画面に戻ったら、「削除」ボタンをクリックして、削除してください。
（削除の確認画面が表示されますので、「OK」をクリックして、削除してください。）
その後、再度、証明書の登録を行うと、勤怠の画面が表示できるようになります。
証明書の登録の方法は、28.3 章をご確認ください。

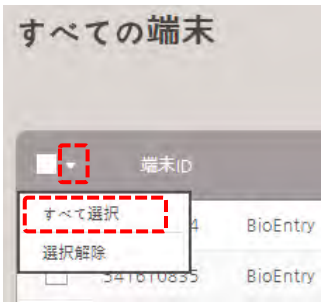
28.5 ユーザーが 200 名以上選択できない

本ソフトウェアでは、個別に選択した場合は、200 ユーザーまで選択可能です。また、全員選択した場合は、全員を選択可能です。200 名以上を個別に選択することはできません。また、この機能はユーザーに限らず、端末や他の画面でも有効です。

「200 項目以上の全部」のような選択をする場合にご利用ください。

左の□をクリックした場合は、そのページに表示されている全項目が☑されます。この方法では、表示件数を最大の 200 件にしていた場合に、200 件が選択されます。

右の▼をクリックすると、以下の表示となります。



表示されたメニューで、「 すべて選択 」をクリックすると、全項目が選択状態となります。

28.6 ログイン ID やパスワードを忘れ、ログインできなくなってしまった

ログイン ID や、パスワードがわからなくなり、BioStar2 にログインできなくなってしまった場合は、弊社の作業員が伺わせていただく必要があります。その場合は、弊社までご連絡ください。

28.7 BioStar2 のデータベースをバックアップ，復元したい

22 章をご確認ください。

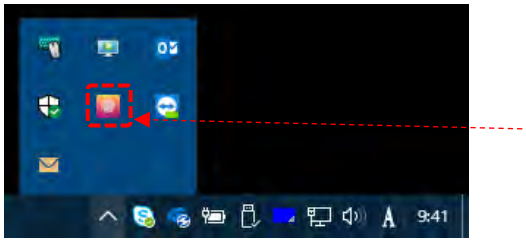
（Windows のタスクスケジューラに登録することで、定期的にバックアップを作成することも可能です。）

28.8 USB カード登録機、USB 指紋登録機が利用できない

機器を認識する USB エージェントプログラムが動作していないことが考えられます。USB 接続機器を利用する場合は、利用する PC に USB エージェントをインストールし、利用時には実行する必要があります。実行されているか確認し、実行されていない場合は、実行してください。

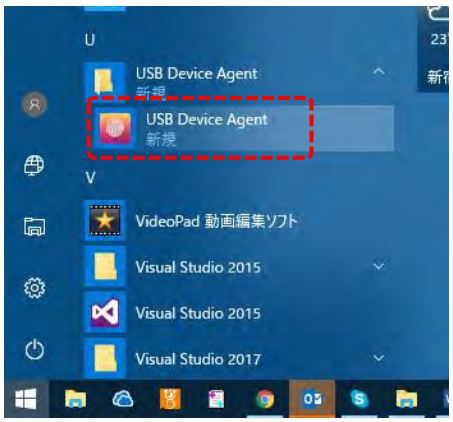
実行されているか？ の確認方法

タスクトレイ（拡張した領域も含めて）に、USB エージェントのアイコンが出ているか？を確認してください。



実行されていない場合の実行方法

スタートメニューの中から、USB Device Agent のプログラムを実行してください。
その後、USB 機器を一度、取り外し、再度、BioStar2 の画面で、確認してください。



また、もし、ご利用の PC では過去に利用したことがない場合は、最初にドライバソフトウェアのインストールが必要です。

サーバー証明書のインストール方法については、インストール DVD の中のシステム一式インストール手順書の 4 章で記載しています。そちらをご参照ください。