

Biostar2.6.1 取扱説明書

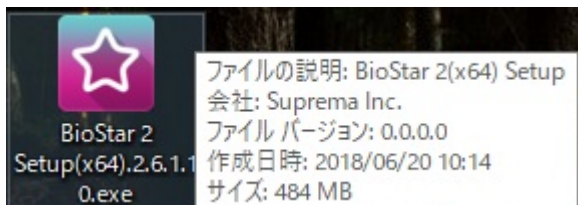
第 2 版

ソフト Ver.	Biostar2.6.1.10
作成日	平成 30 年 7 月 13 日
最終更新日	平成 30 年 7 月 13 日

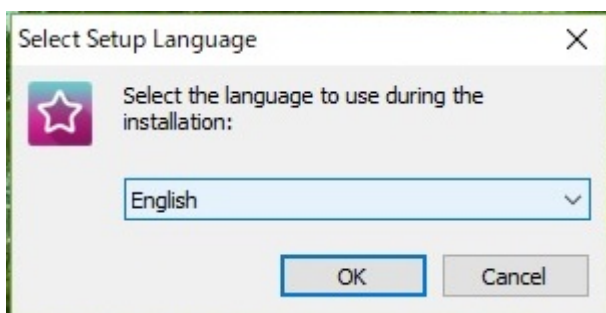
目次

Biostar2.6.1 取扱説明書	1
目次	2
Biostar2.6.1 のインストール	3
Google Chrome のインストールと設定	16
Google Chrome のパスワードの管理設定	25
Biostar2.6.1 の起動	26
ユーザーの作成	28
ユーザーの削除	30
ユーザーの無効	31
アクセスグループの作成	32
ドアの作成	36
資格の作成	37
アクセスコントロールの動作	40
資格の作成(ユーザー個別)	40
ヘルプの参照	42
ログの種類	43
ドアの連続施錠の設定	46
Biostar2.5.0 ベーシックエディションでの 1 ドア用のアンチパスバックの設定	47
二重認証(ユーザーと誰かが一緒に 2 人で端末認証しないと開かない)の設定	51
ホールドアップ指紋の設定	52
Bio-mini の設定	53
DM-20 の接続	59

BioStar2.6.1 のインストール



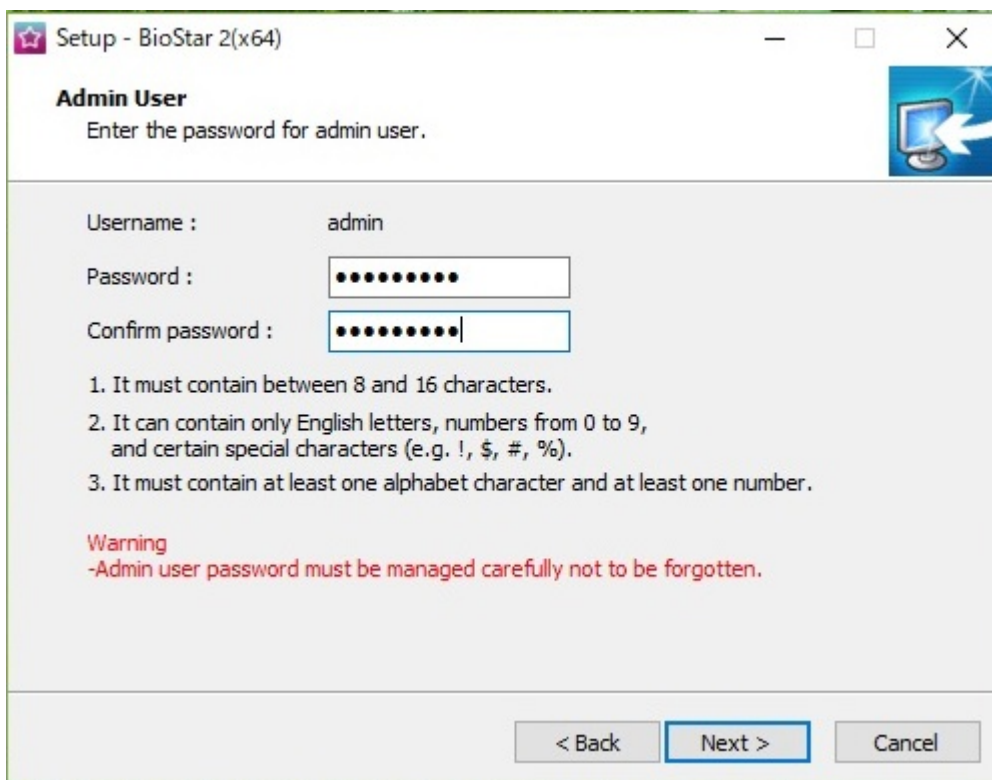
<https://www.supremainc.com/en/content/biostar-2-installer> から 64 ビットまたは 32 ビットの何れかの BioStar2.6.1.10 をダウンロードします。ダウンロードした実行ファイルを実行します。



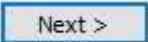
「English」を選択して **OK** をクリックします。

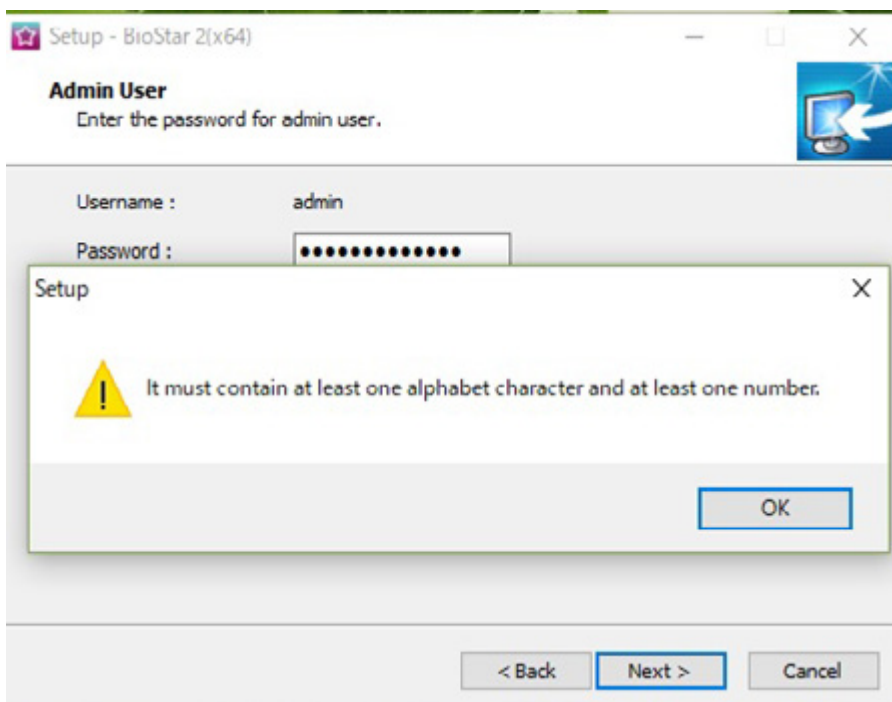


「I accept the agreement」にチェックを入れて **Next >** をクリックします。

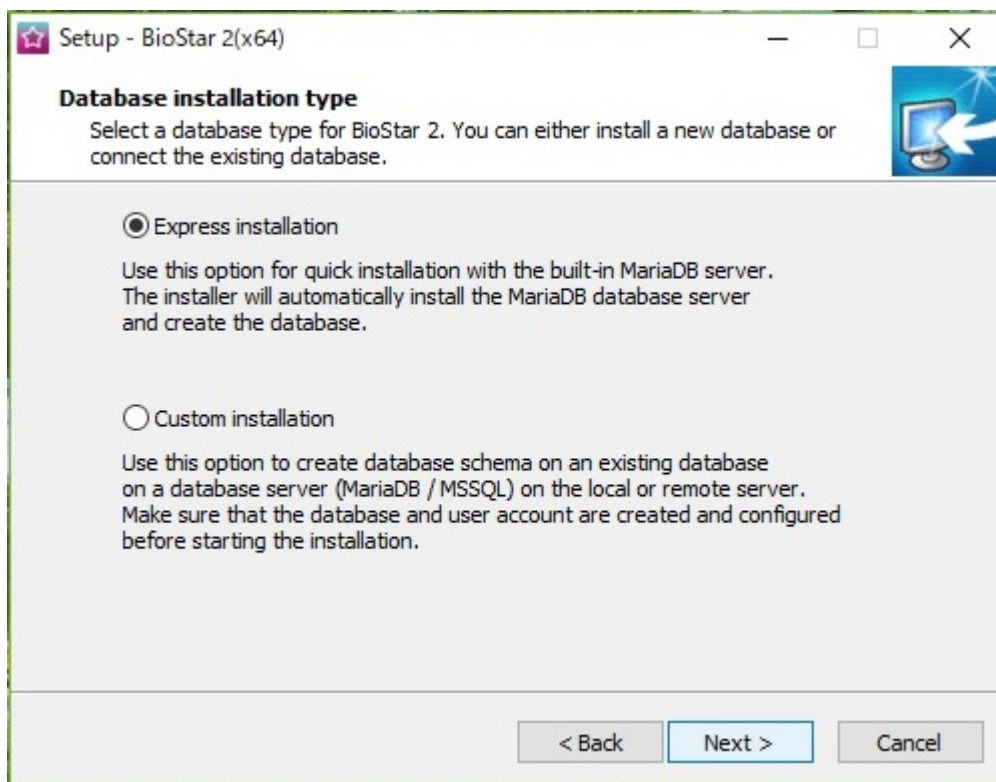


admin のパスワードは 8～16 文字でなければなりません。英語の文字、0～9 の数字、および特定の特殊文字(たとえば、!、\$、#、%)のみを含むことができます。少なくとも 1 つのアルファベット文字と少なくとも 1 つの数字を含む必要があります。管理者のパスワードは忘れないように注意深く管理する必要があります。

パスワードを入力し、 をクリックします。



形式が正しくないと再入力を促されます。 をクリックして入力し直してください。



特に指定が無ければ Express installation にチェックを入れて **Next >** をクリックします。



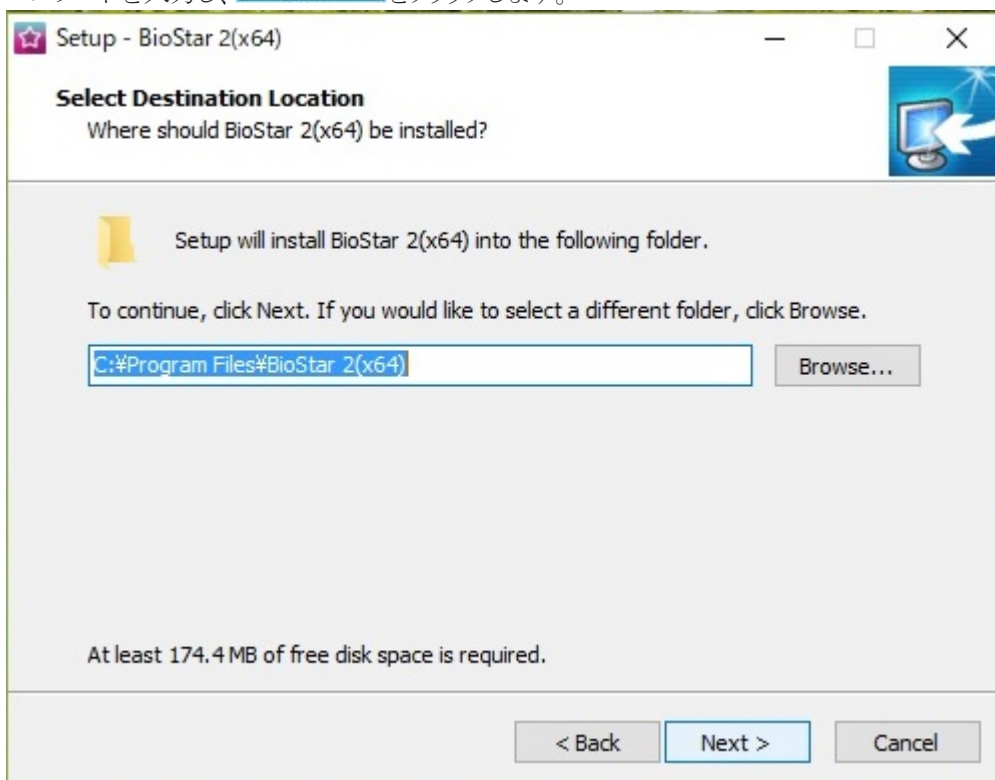
データベースの root アカウントのパスワードを入力します。

root のパスワードは 8～16 文字でなければなりません。英語の文字、0～9 の数字、および特定の特殊文字(たとえば、!、\$、#、%)のみを含むことができます。少なくとも 1 つのアルファベット文字と少なくとも 1 つの数字を含む必要があります。管理者のパスワードは忘れないように注意深く管理する必要があります。

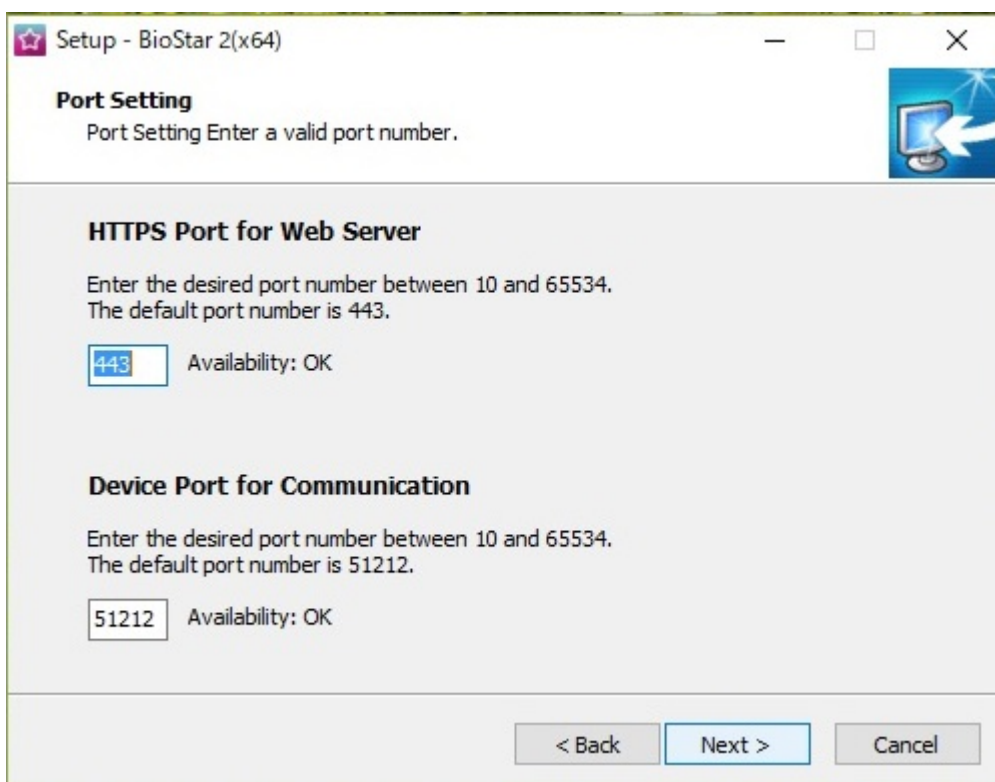
ルートアカウントのパスワードは、AC、TA、Video DB の初期パスワードとしても使用されます。

パスワードが失われた場合、バージョンのアップグレードと DB のバックアップ/復元はできません。

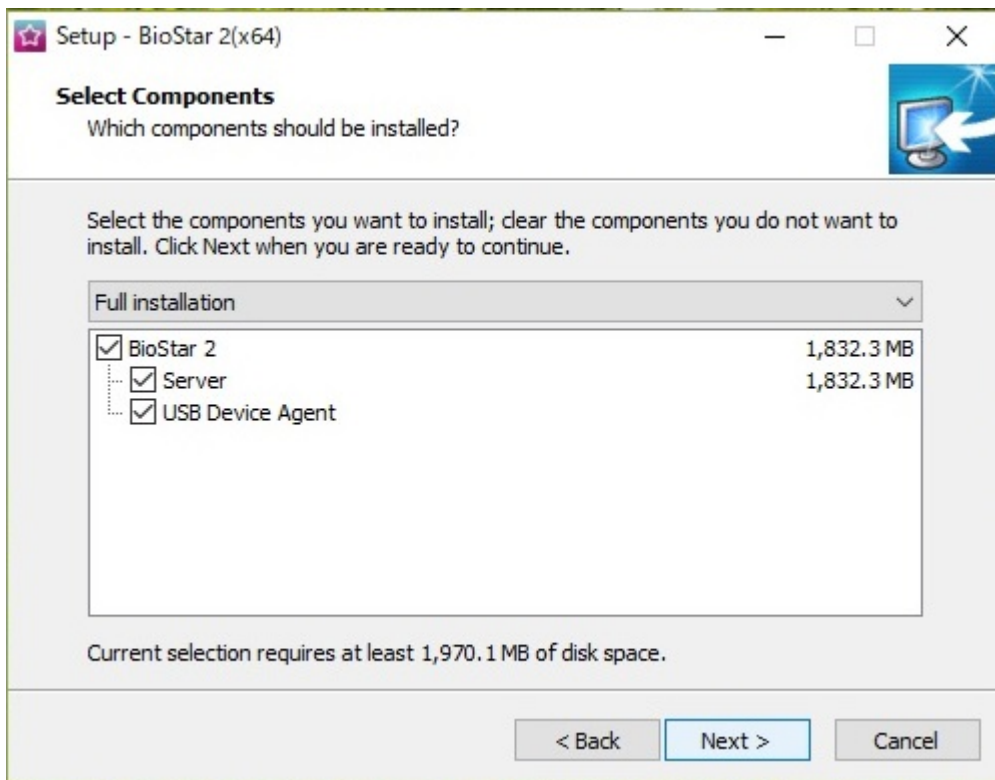
パスワードを入力し、**Next >** をクリックします。



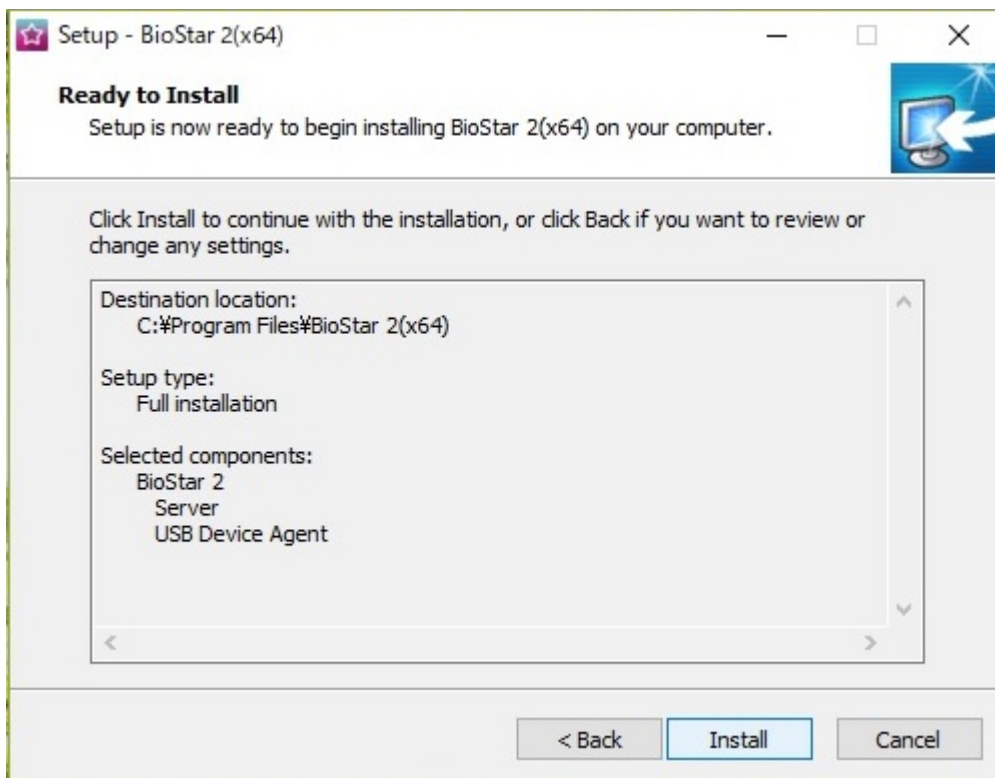
Next > をクリックします。



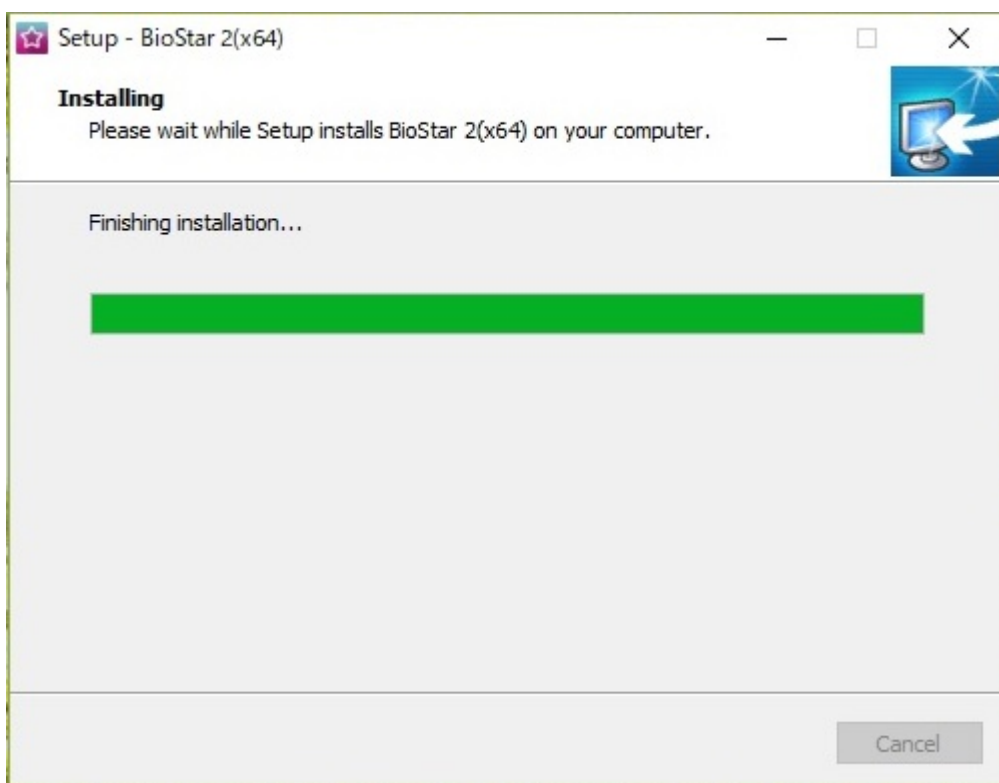
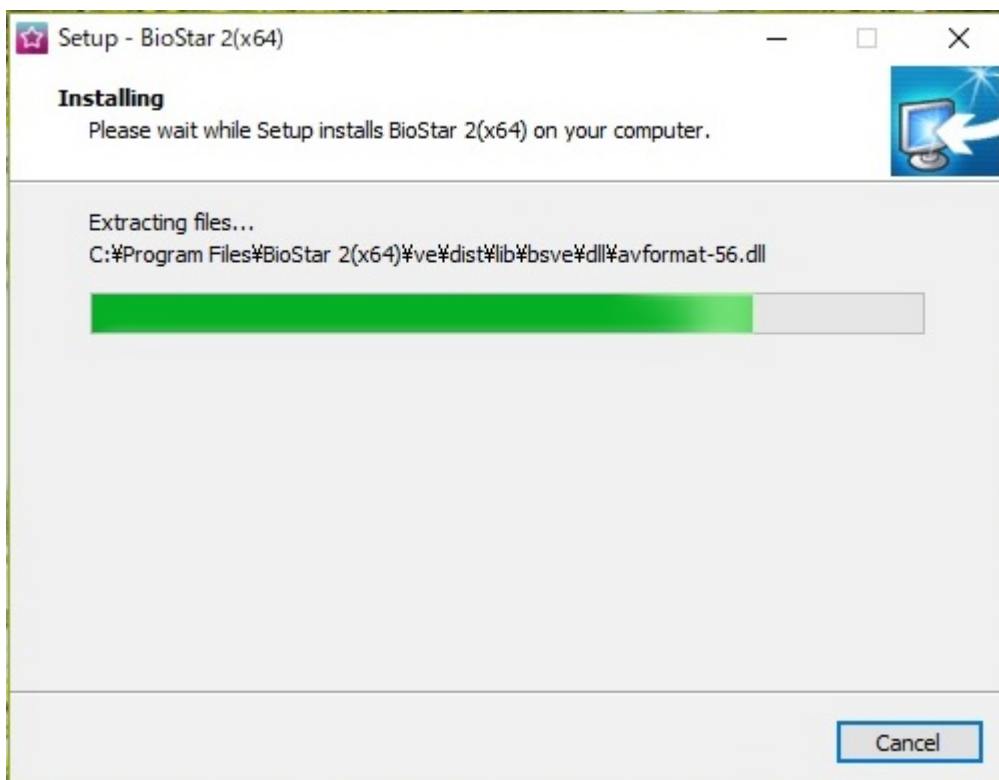
特に変更が無ければ、そのまま **Next >** をクリックします。



特に変更が無ければ、そのまま **Next >** をクリックします。



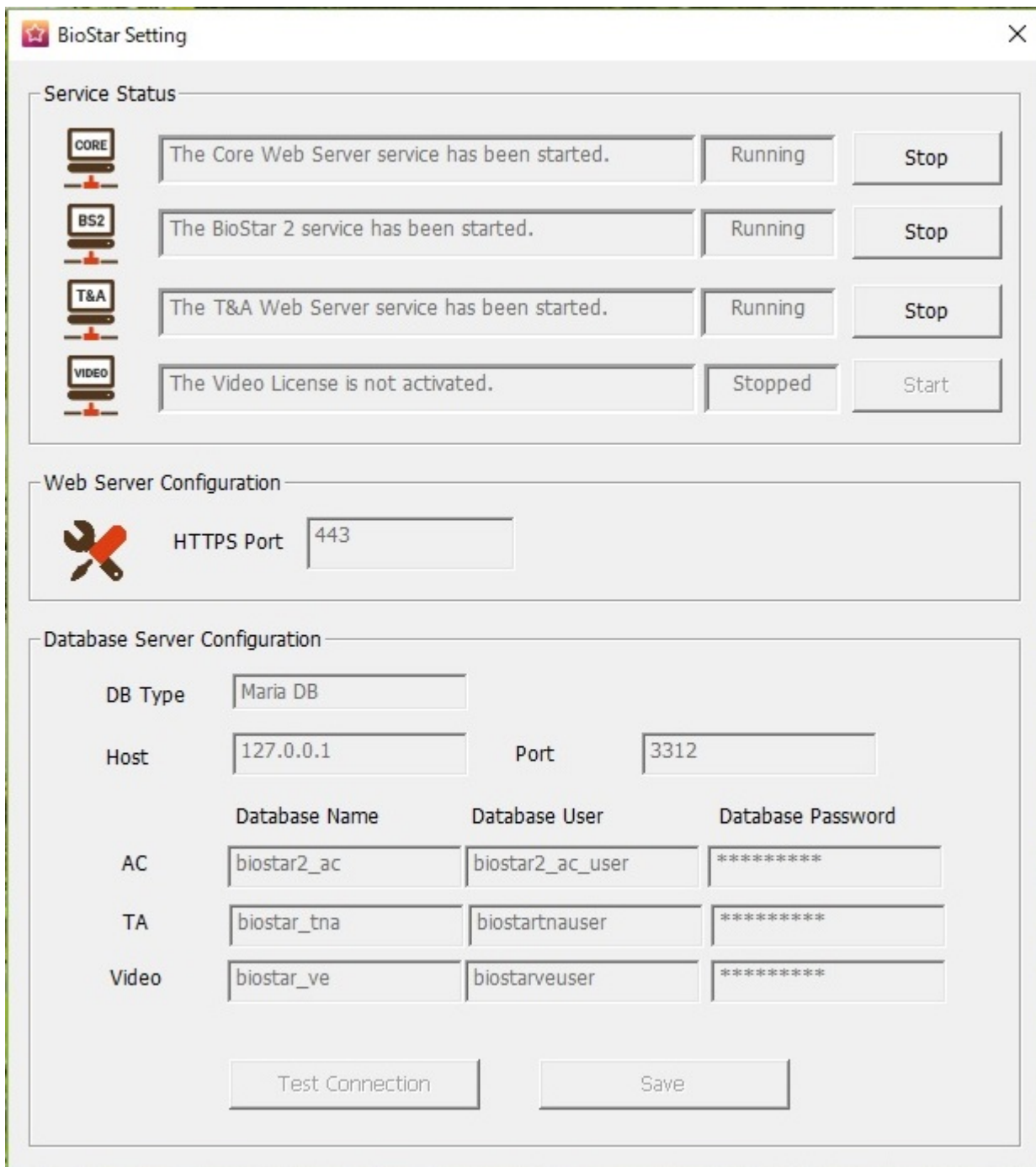
Install をクリックします。



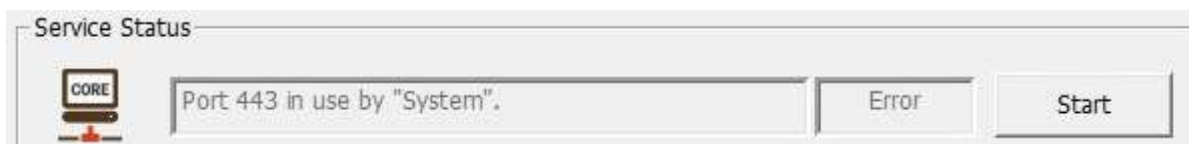
Finishing installation...と表示されても暫く待ちます。

```
C:\Program Files\BioStar 2(x64)\db-convert.exe
2018-Jun-19 08:00:25 <info> Maria DB connection info:
2018-Jun-19 08:00:25 <info> Address: 127.0.0.1:3312
2018-Jun-19 08:00:25 <info> ID: root
2018-Jun-19 08:00:25 <info> Database: biostar2_ac
2018-Jun-19 08:00:25 <info> Connect to database OK.
2018-Jun-19 08:00:25 <info> Execute C:\Program Files\BioStar 2(x64)\dbscript\maria\ac_maria_init.sql Error on Stop = false
2018-Jun-19 08:00:25 <info> Execute (CREATE TABLE IF NOT EXISTS T_USR...) OK.
2018-Jun-19 08:00:25 <info> Execute (ALTER TABLE T_USRCRD ADD PRIMARY...) OK.
2018-Jun-19 08:00:25 <info> Execute (CREATE TABLE IF NOT EXISTS T_BLK...) OK.
2018-Jun-19 08:00:25 <info> Execute (ALTER TABLE T_BLKL ADD UNIQUE UN...) OK.
2018-Jun-19 08:00:26 <info> Execute (ALTER TABLE T_BLKL ADD UNIQUE UN...) OK.
2018-Jun-19 08:00:26 <info> Execute (CREATE TABLE IF NOT EXISTS T_ACS...) OK.
2018-Jun-19 08:00:26 <info> Execute (ALTER TABLE T_ACSGRUSS ADD PRIMA...) OK.
2018-Jun-19 08:00:26 <info> Execute (CREATE TABLE IF NOT EXISTS T_DRG...) OK.
2018-Jun-19 08:00:26 <info> Execute (CREATE TABLE IF NOT EXISTS T_DR ...) OK.
2018-Jun-19 08:00:26 <info> Execute (CREATE TABLE IF NOT EXISTS T_CRD...) OK.
2018-Jun-19 08:00:26 <info> Execute (ALTER TABLE T_CRDISSHIS ADD UNIO...) OK.
2018-Jun-19 08:00:27 <info> Execute (CREATE TABLE IF NOT EXISTS T_CRD...) OK.
2018-Jun-19 08:00:27 <info> Execute (CREATE TABLE IF NOT EXISTS T_DEV...) OK.
2018-Jun-19 08:00:27 <info> Execute (ALTER TABLE T_DEVOPRMD ADD PRIMA...) OK.
2018-Jun-19 08:00:28 <info> Execute (CREATE TABLE IF NOT EXISTS T_TAK...) OK.
2018-Jun-19 08:00:28 <info> Execute (ALTER TABLE T_TAKEY ADD PRIMARY ...) OK.
2018-Jun-19 08:00:28 <info> Execute (CREATE TABLE IF NOT EXISTS T_DEV...) OK.
2018-Jun-19 08:00:28 <info> Execute (ALTER TABLE T_DEVWGD ADD PRIMARY...) OK.
```

そのまま待ちます。



BioStar Setting の画面が表示されます。



Service Status に Error が表示されている場合は、PC の設定を見直してください。PC に IIS が導入されていると HTTPS ポート(443 番)が Error になる場合があります。



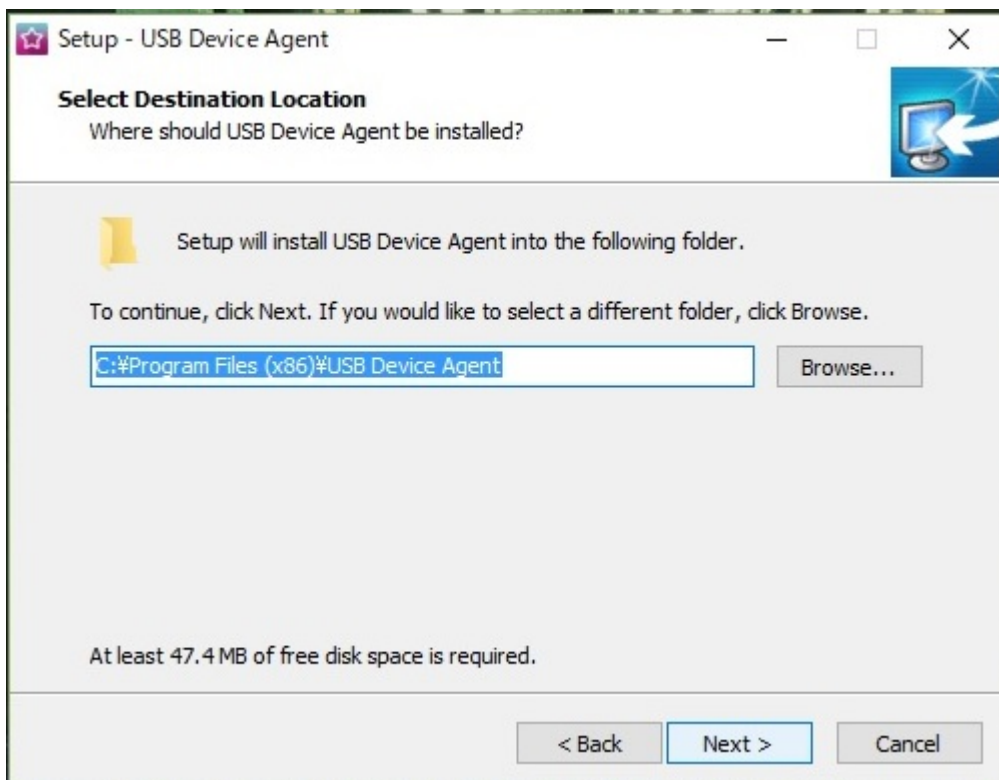
Finish をクリックします。 Install USB Device Agent にチェックを入れておくとUSBデバイスのセットアップが継続して行われます。



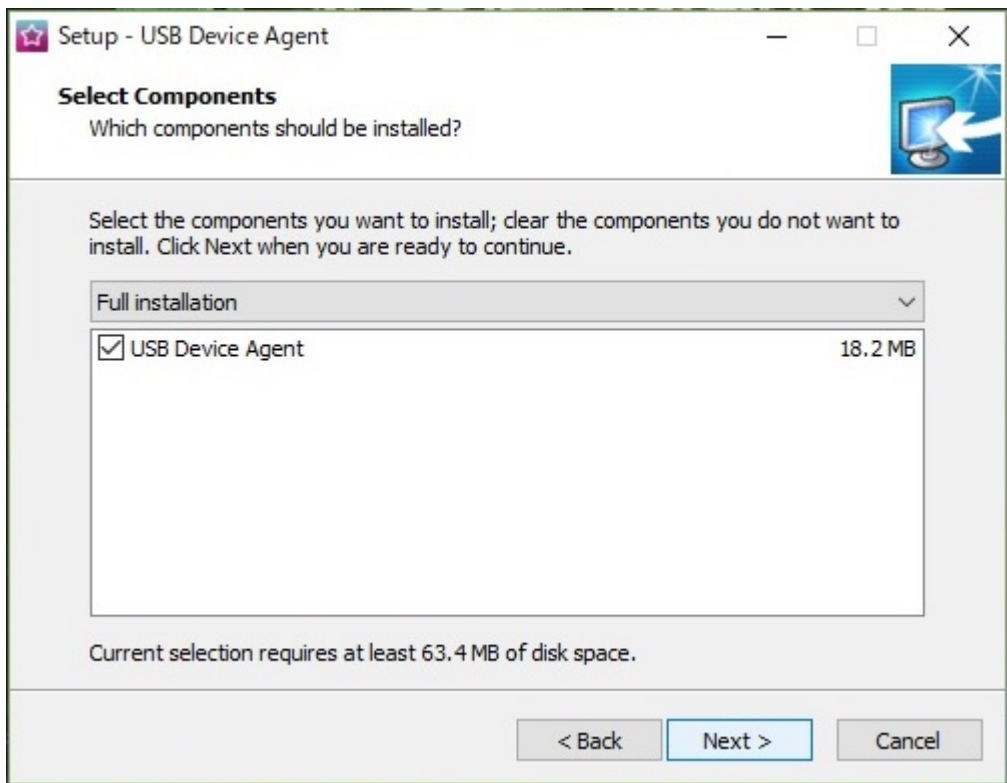
English を選択して **OK** をクリックします。



I accept the agreement にチェックを入れて **Next >** をクリックします。

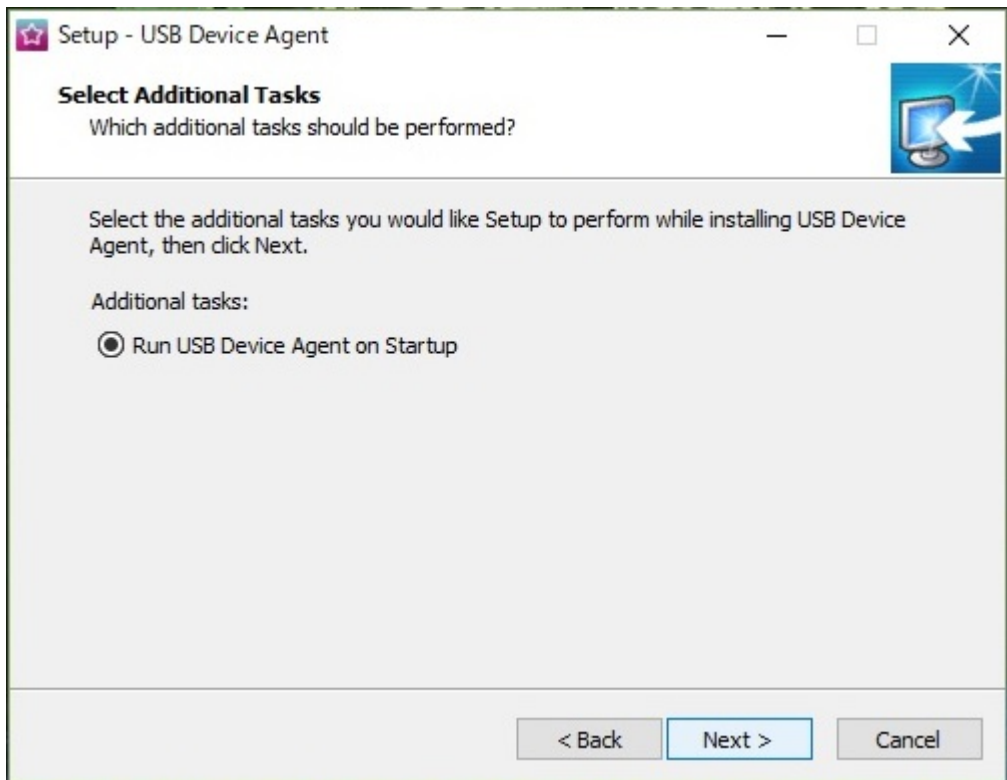


特に変更が無ければ、**Next >** をクリックします。



Next >

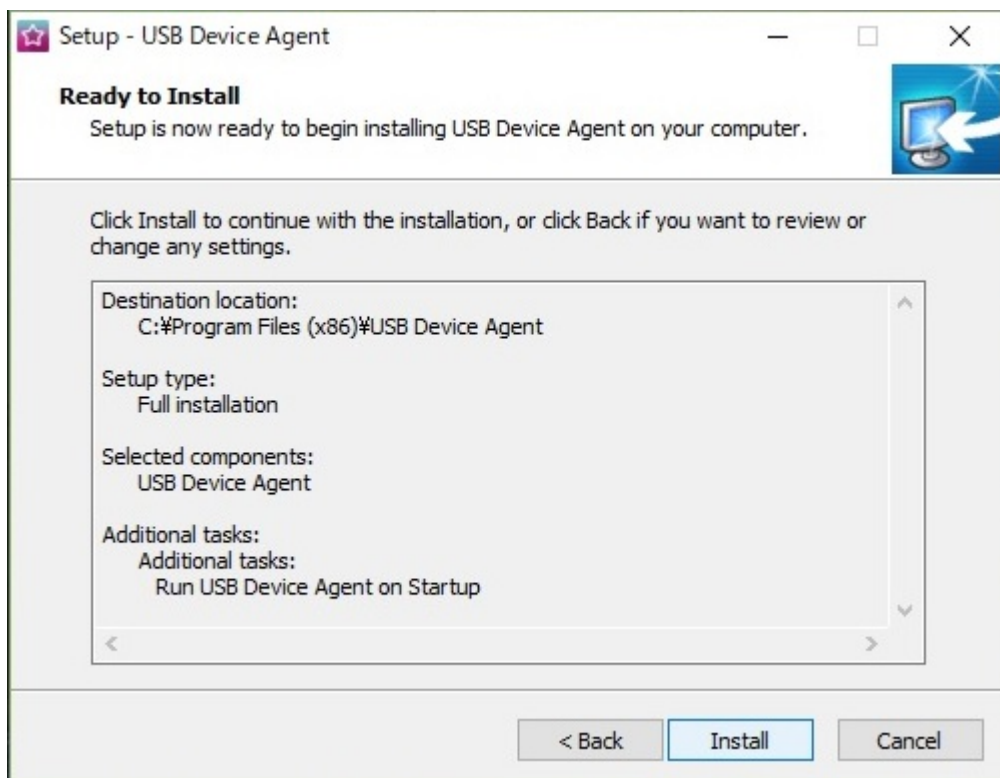
をクリックします。



Next >

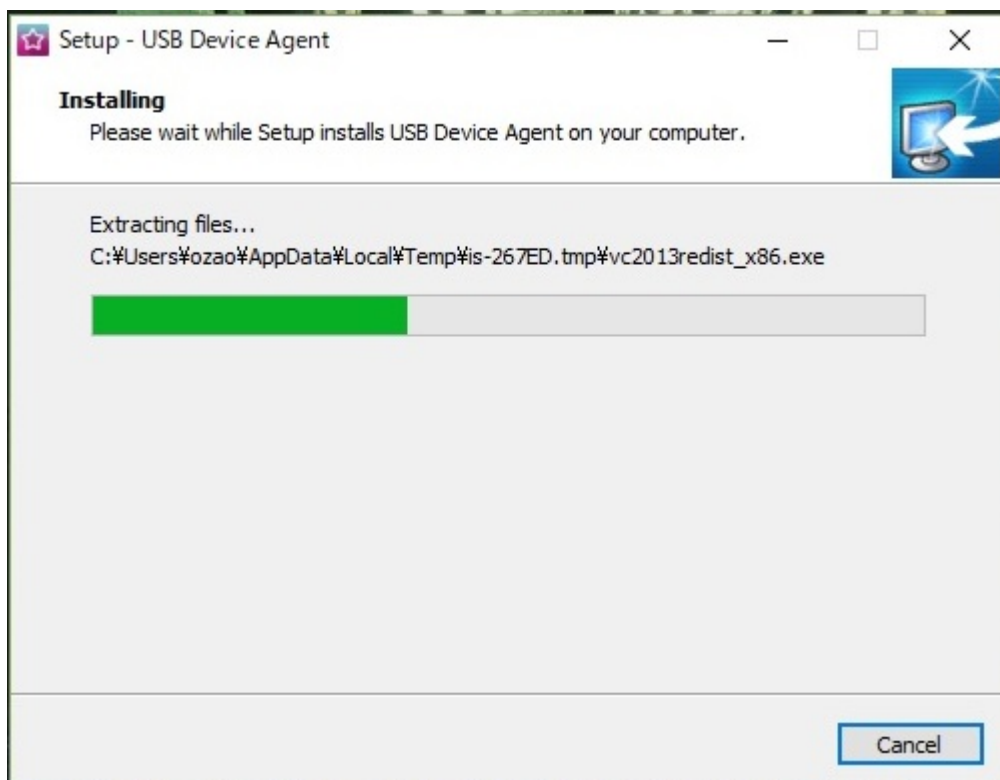
Run USB Device Agent on Startup にチェックが入っていることを確認して

をクリックします。



Install

をクリックします。





特に変更が無ければ、Yes, restart the computer now にチェックを入れてそのまま **Finish** をクリックします。PC が再起動します。

Google Chrome のインストールと設定

BioStar の WEB ブラウザとして Google Chrome Ver49 以降が動作推奨されています。

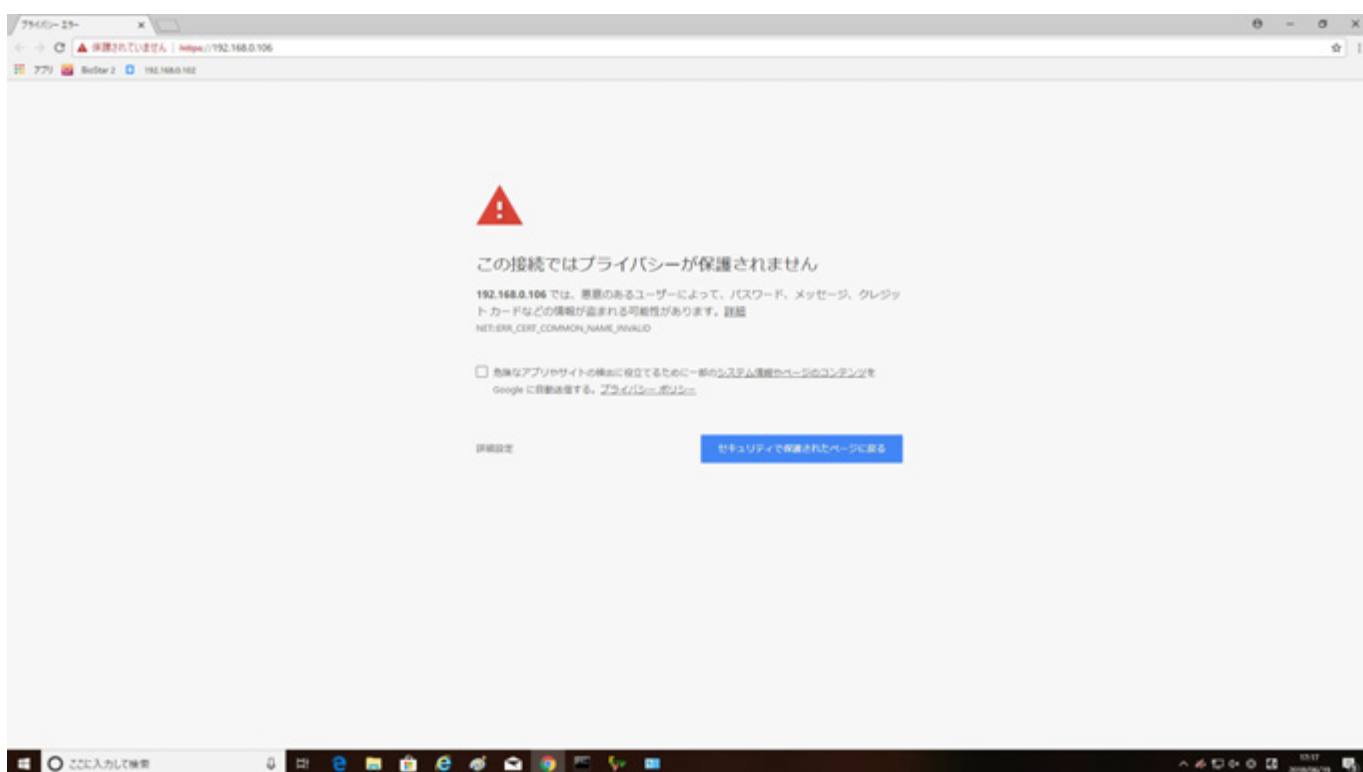
Google Chrome Ver49 以降をインストールしてください。

<https://www.google.co.jp/chrome/browser/desktop/index.html>

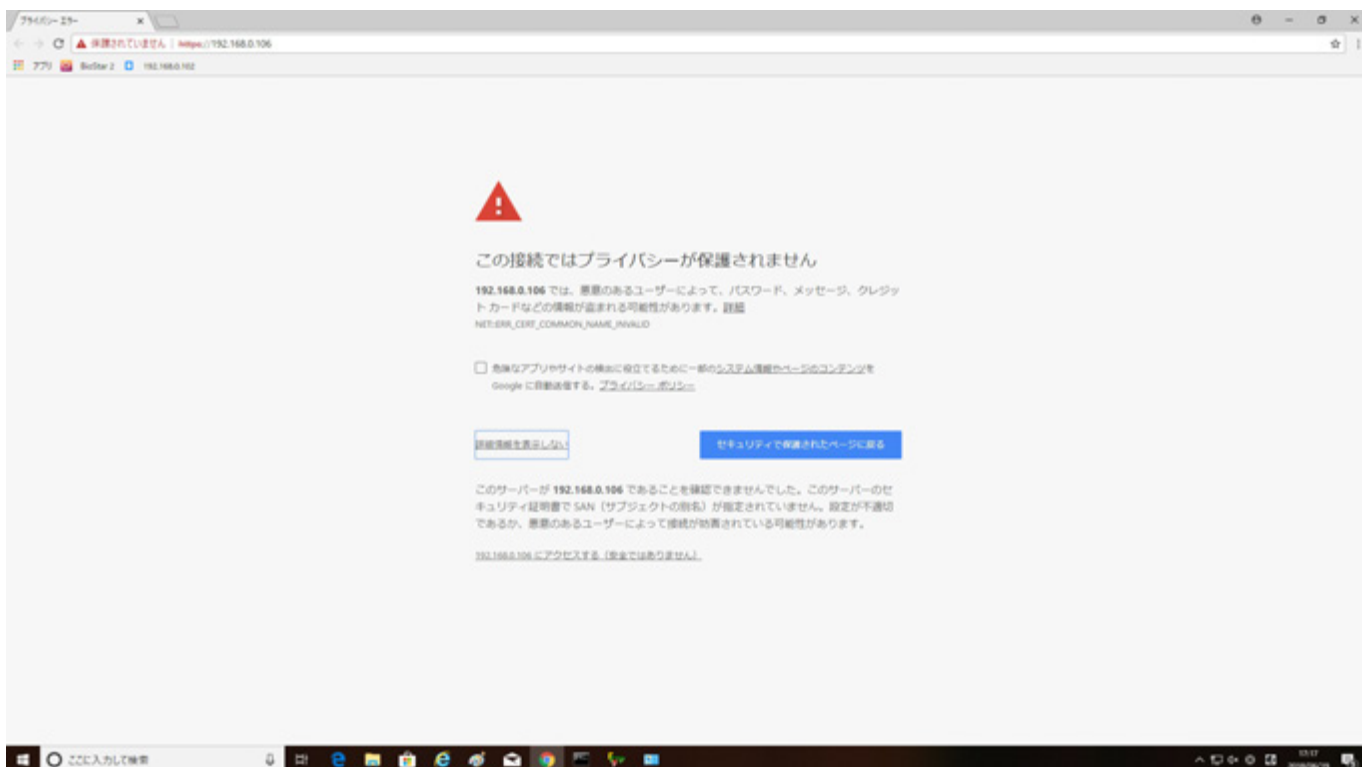
BioStar2.6.1 をインストールして初めて Google Chrome から BioStar2 にアクセスした時、以下のような表示になる場合があります。



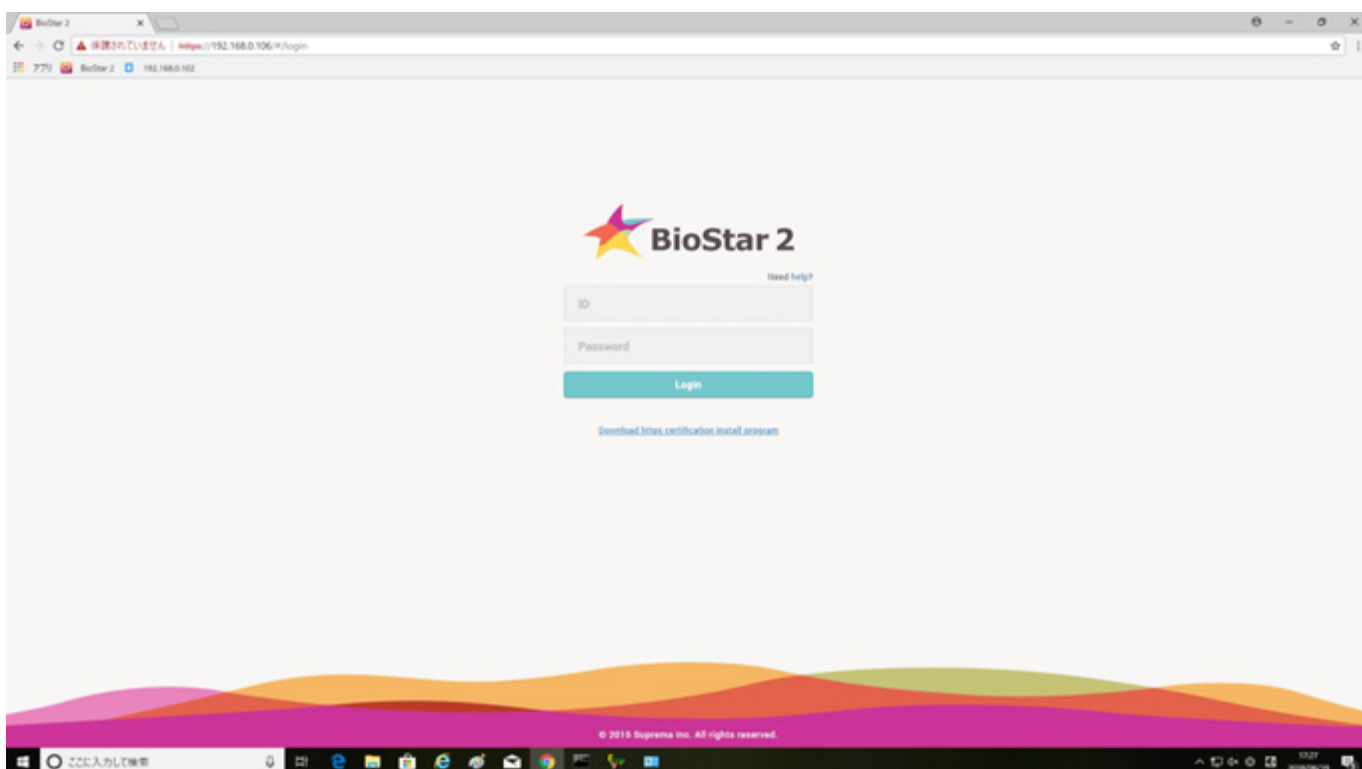
BioStar 2 (Start Page)アイコンをクリックします。



詳細設定 をクリックします。



インストールしたローカル IP アドレス(写真の例では 192.168.0.106)にアクセスする(安全ではありません)をクリックします。



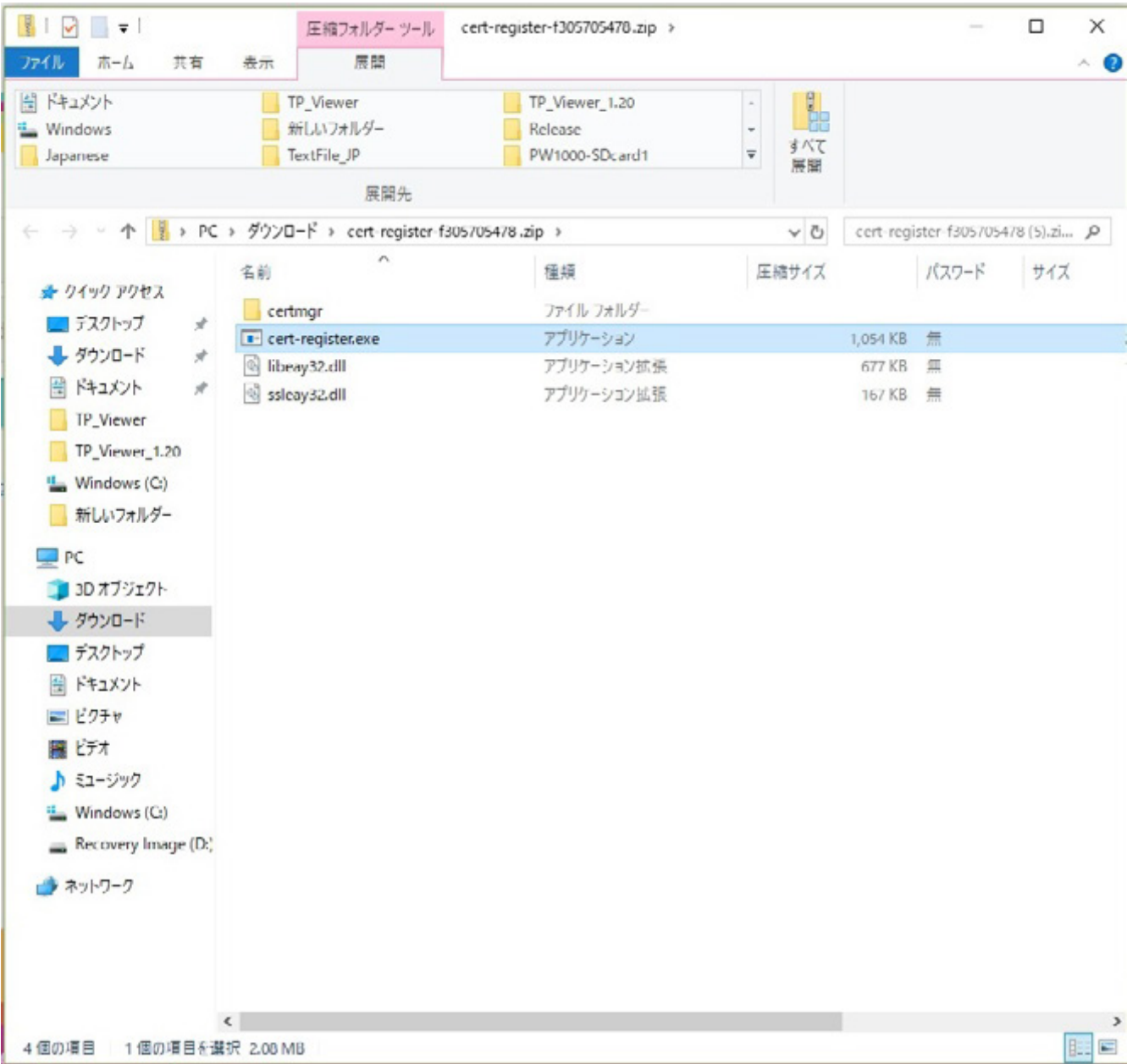
BioStar 2 のログイン画面が表示されます。IDとPASSWORD(P4 に同じ)を入力して Login します。左上の https://の表示が「保護されていません」になっています。

[Download https certification install program](#)

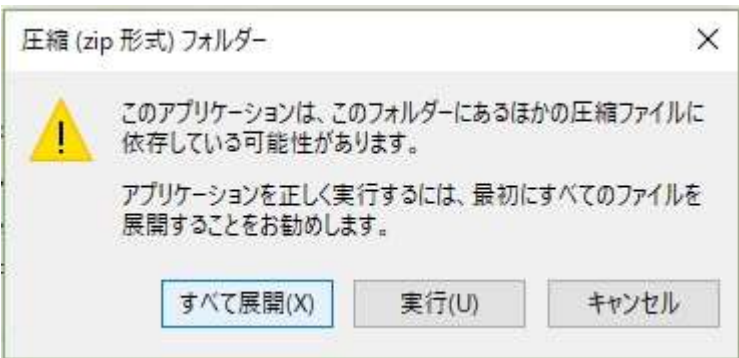
Login の下の「Download https certification install program」をクリックします。証明書のダウンロードが始まります。



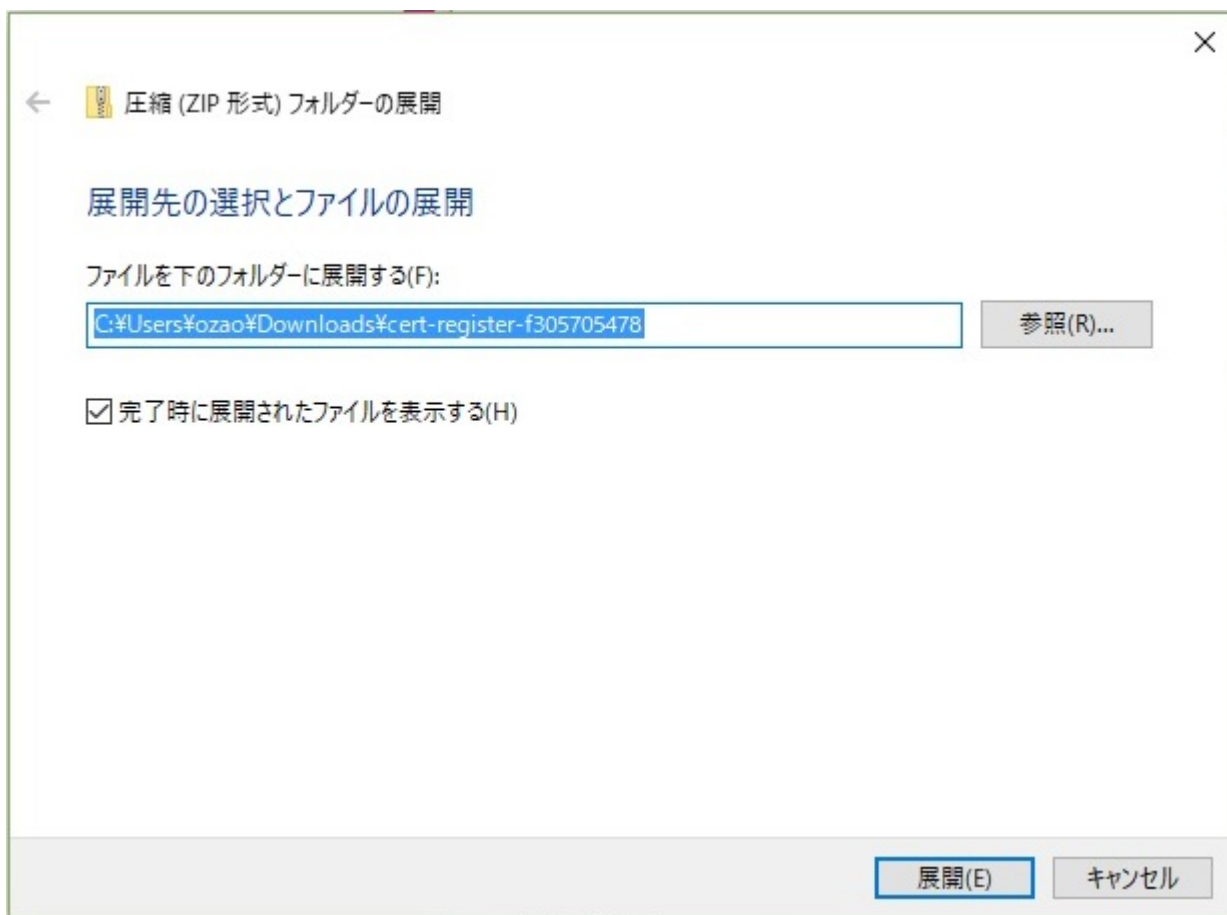
左下の「cert-register-f3057....zip」をクリックします。エクスプローラーが開き Zip ファイルの中身が表示されます。

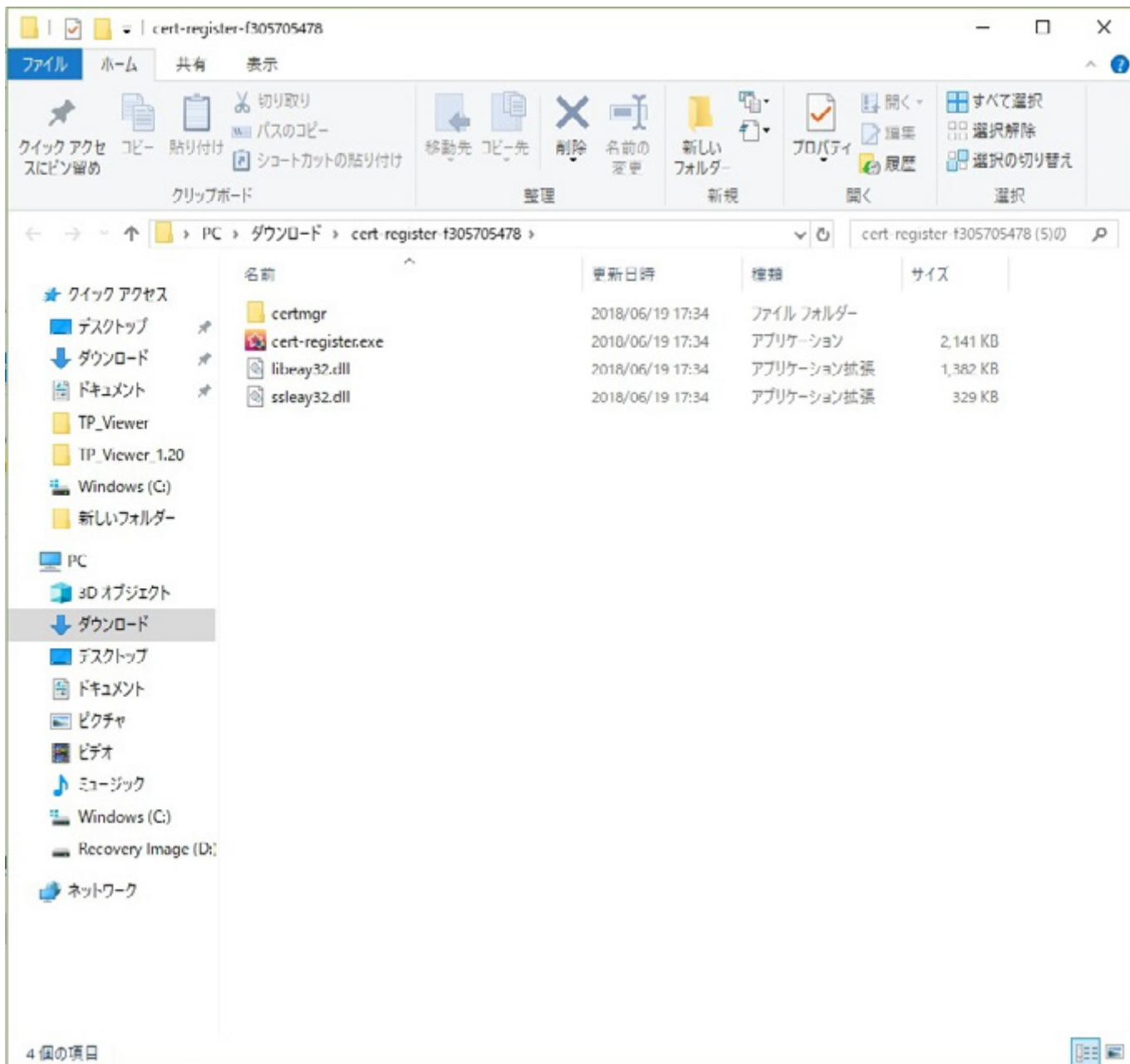


“cert-register.exe”をダブルクリックします。



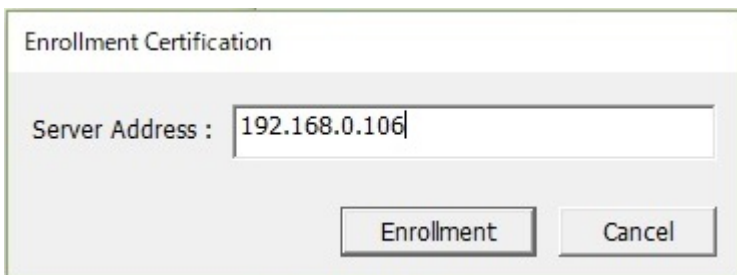
すべて展開(X) をクリックします。





名前	更新日時	種類	サイズ
certmgr	2018/06/19 17:34	ファイル フォルダー	
cert-register.exe	2018/06/19 17:34	アプリケーション	2,141 KB
libeay32.dll	2018/06/19 17:34	アプリケーション拡張	1,382 KB
ssleay32.dll	2018/06/19 17:34	アプリケーション拡張	329 KB

展開されたフォルダが開きますので、“cert-register.exe”をダブルクリックして実行します。



Enrollment Certification というウィンドウが表示され、Server アドレスの入力を求められます。この例の場合は、BioStar 2 をインストールしたローカル IP アドレス「192.168.0.106」を入力します。



はい(Y)

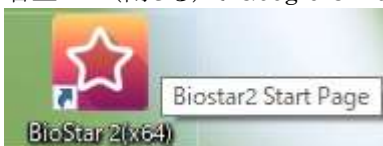
をクリックして、証明書をインストールします。



[OK]をクリックします。

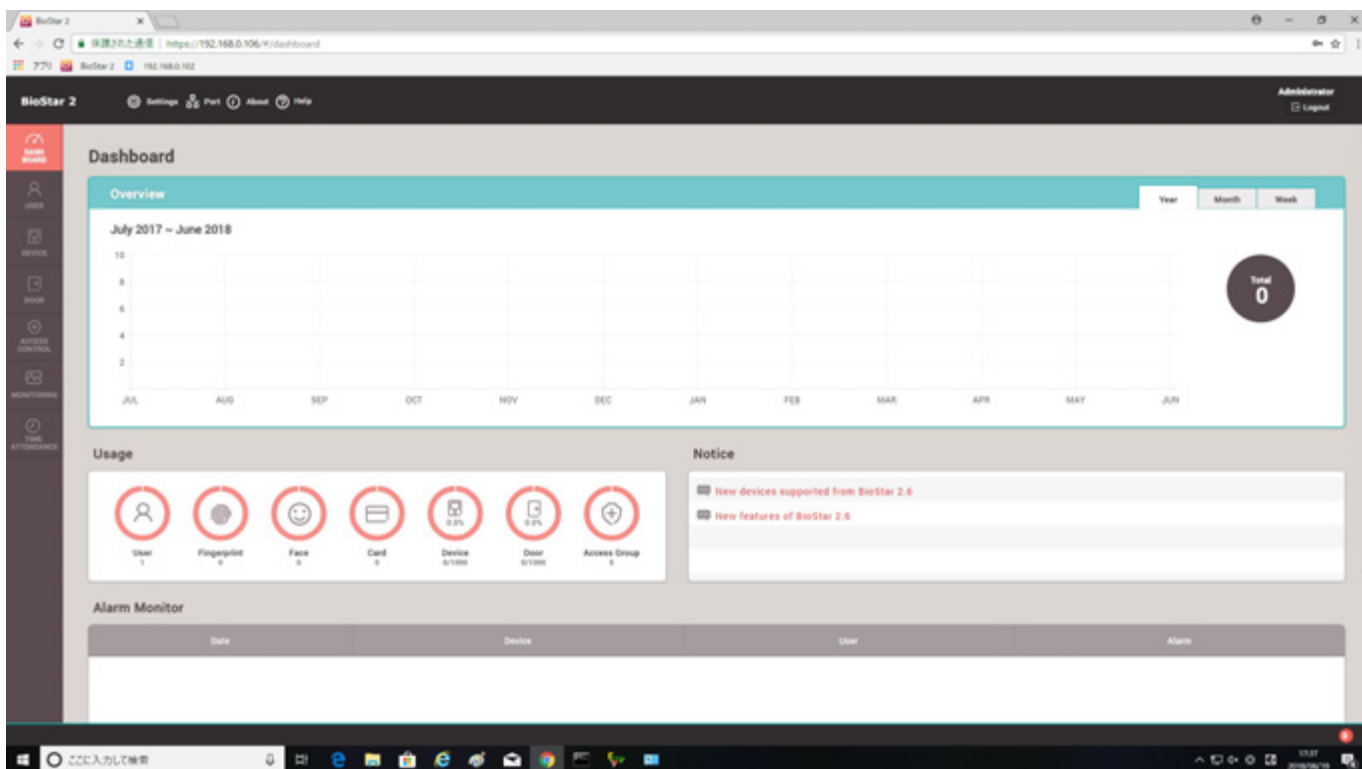
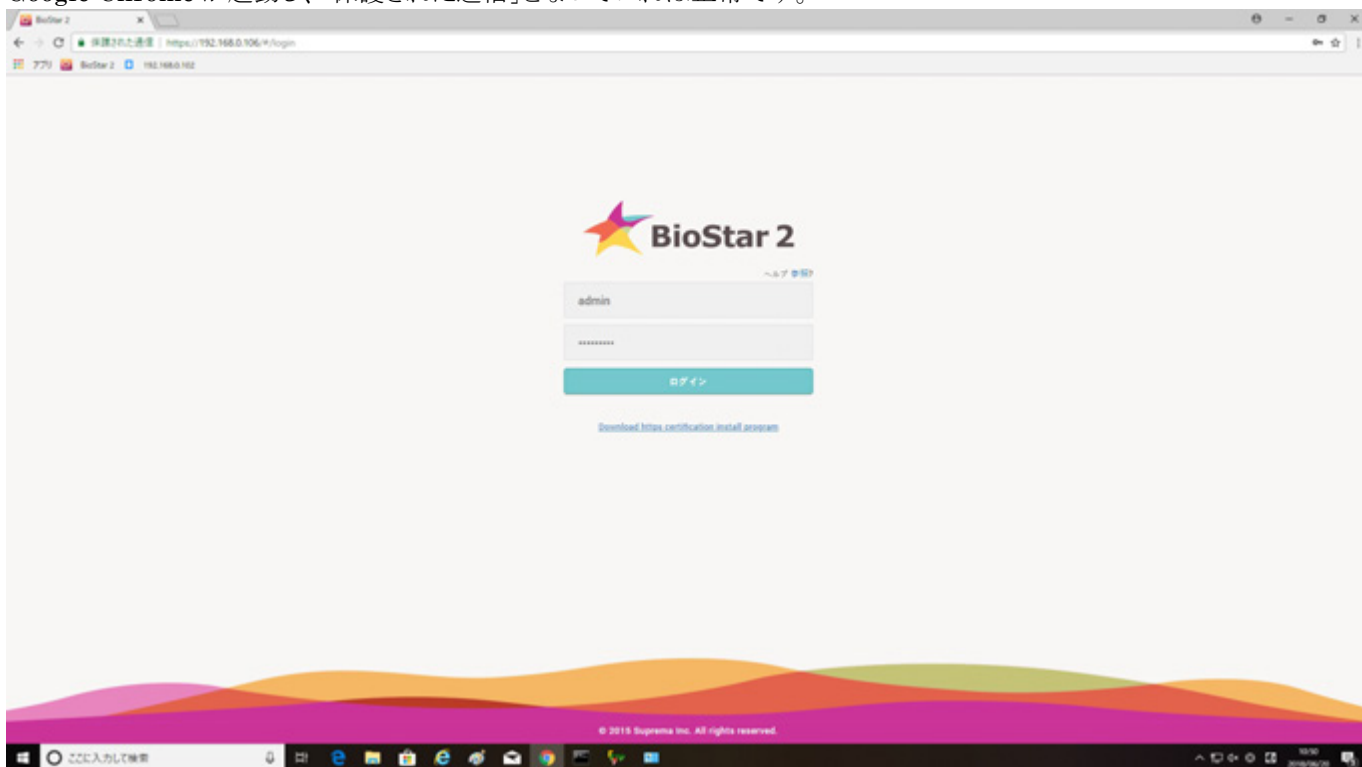


右上の×(閉じる)で Google Chrome を閉じます。

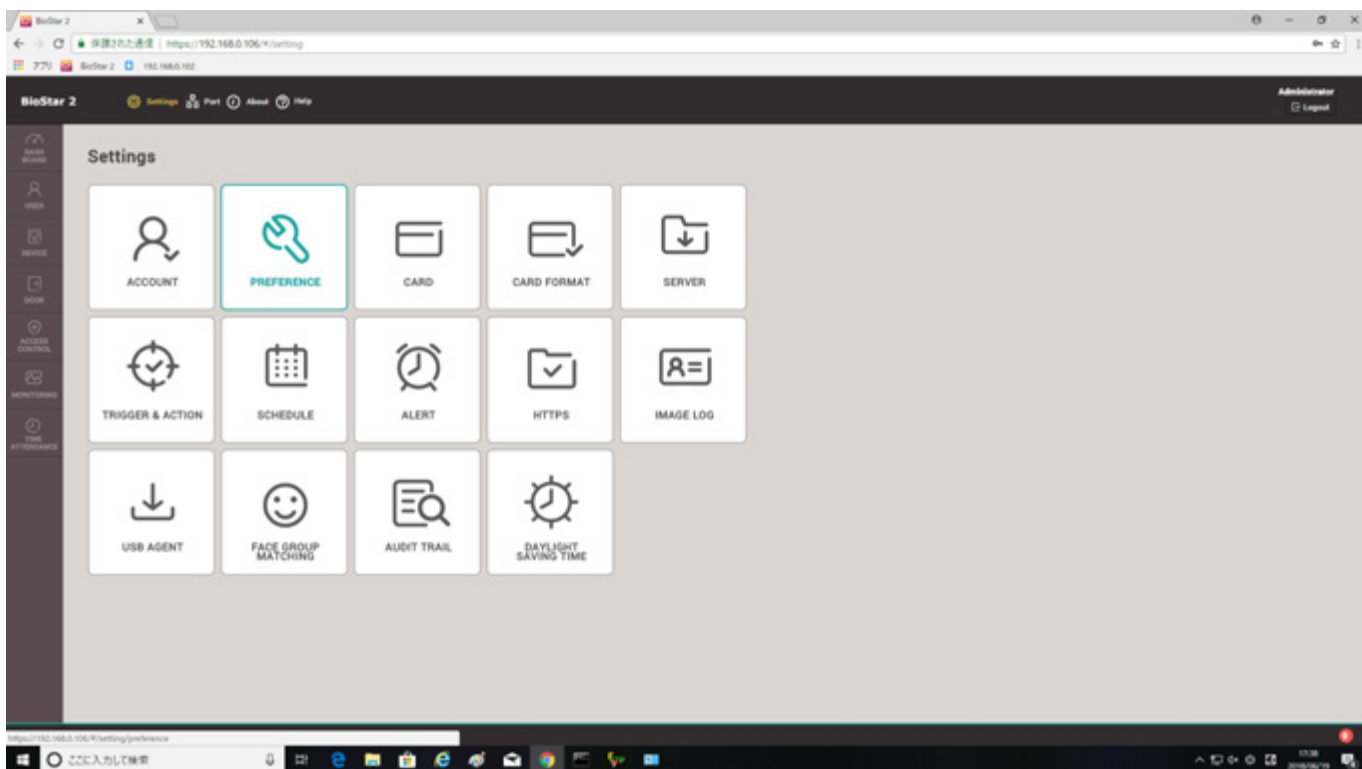


BioStar 2 (Start Page)アイコンをクリックします。

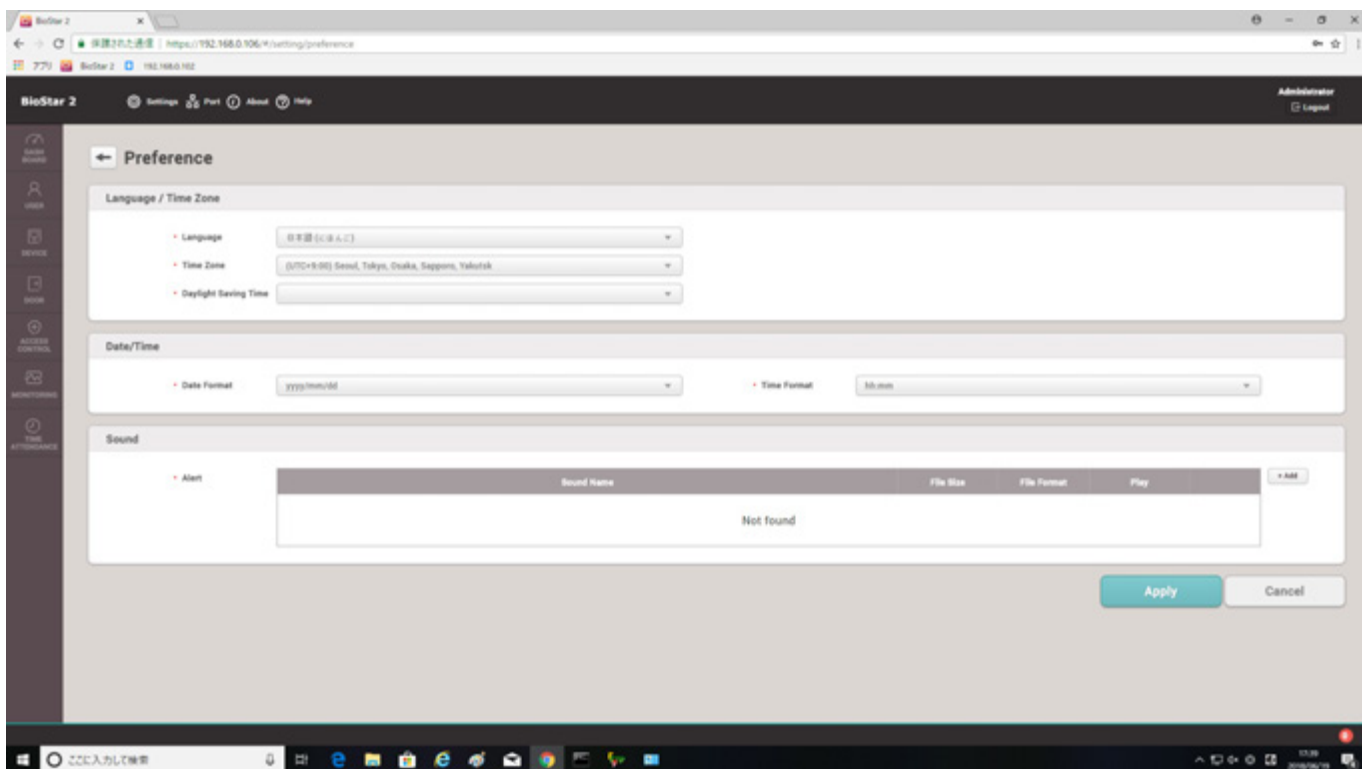
Google Chrome が起動し、「保護された通信」となっていれば正常です。



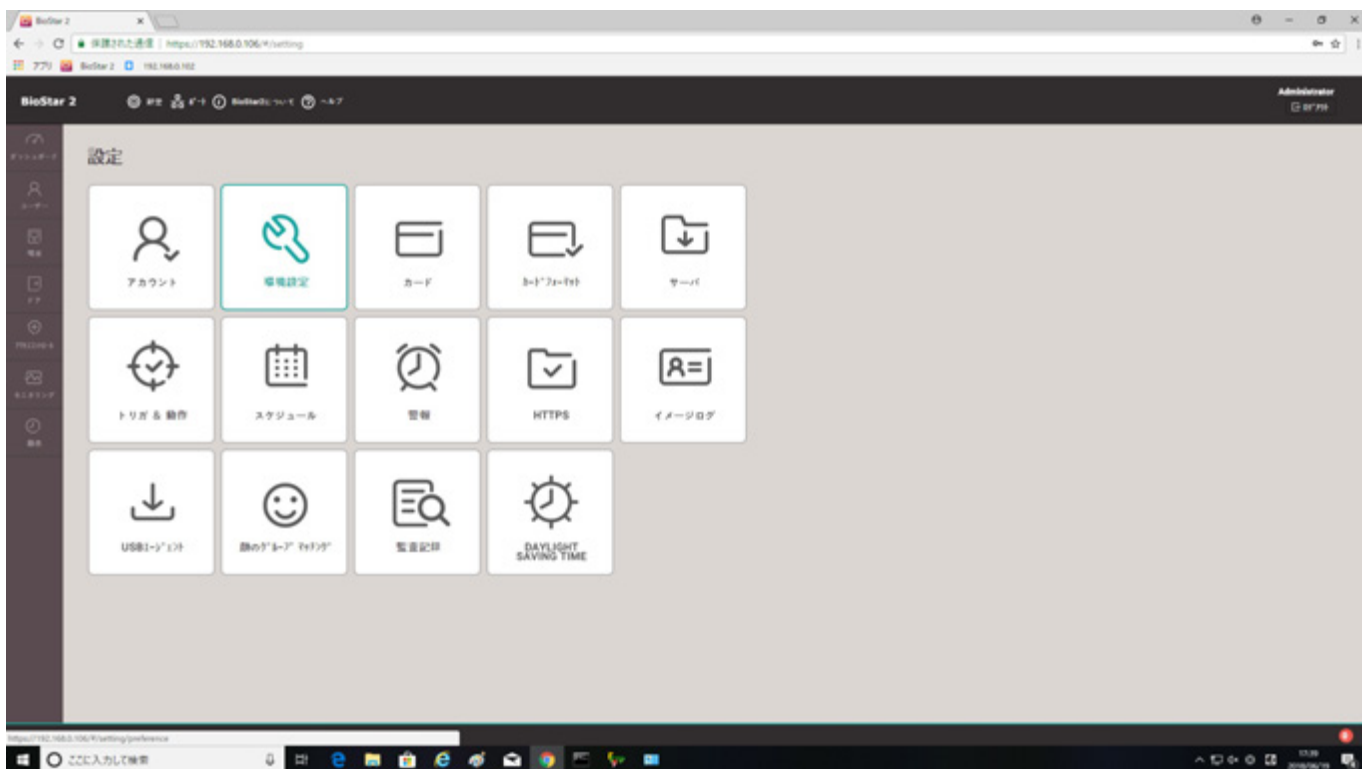
画面上部の  をクリックします。



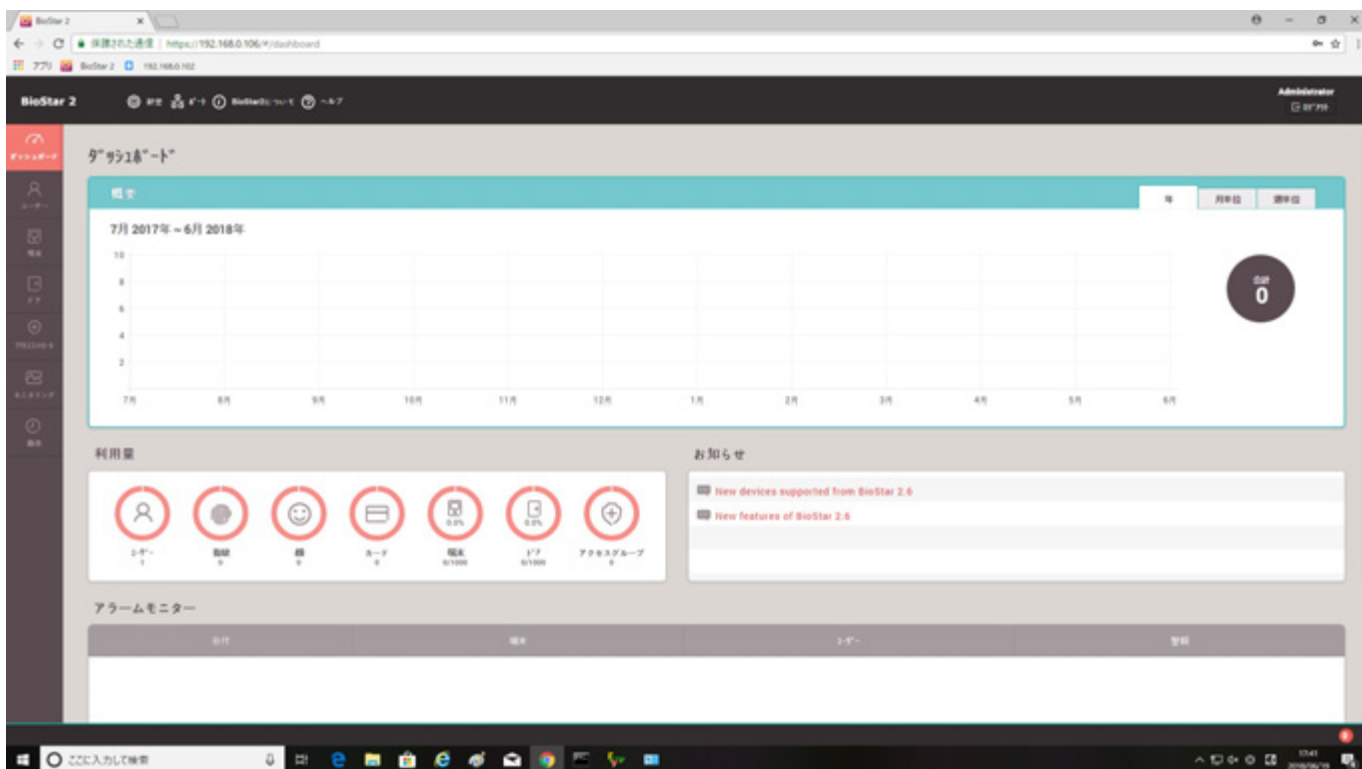
「PREFERENCE」をクリックします。



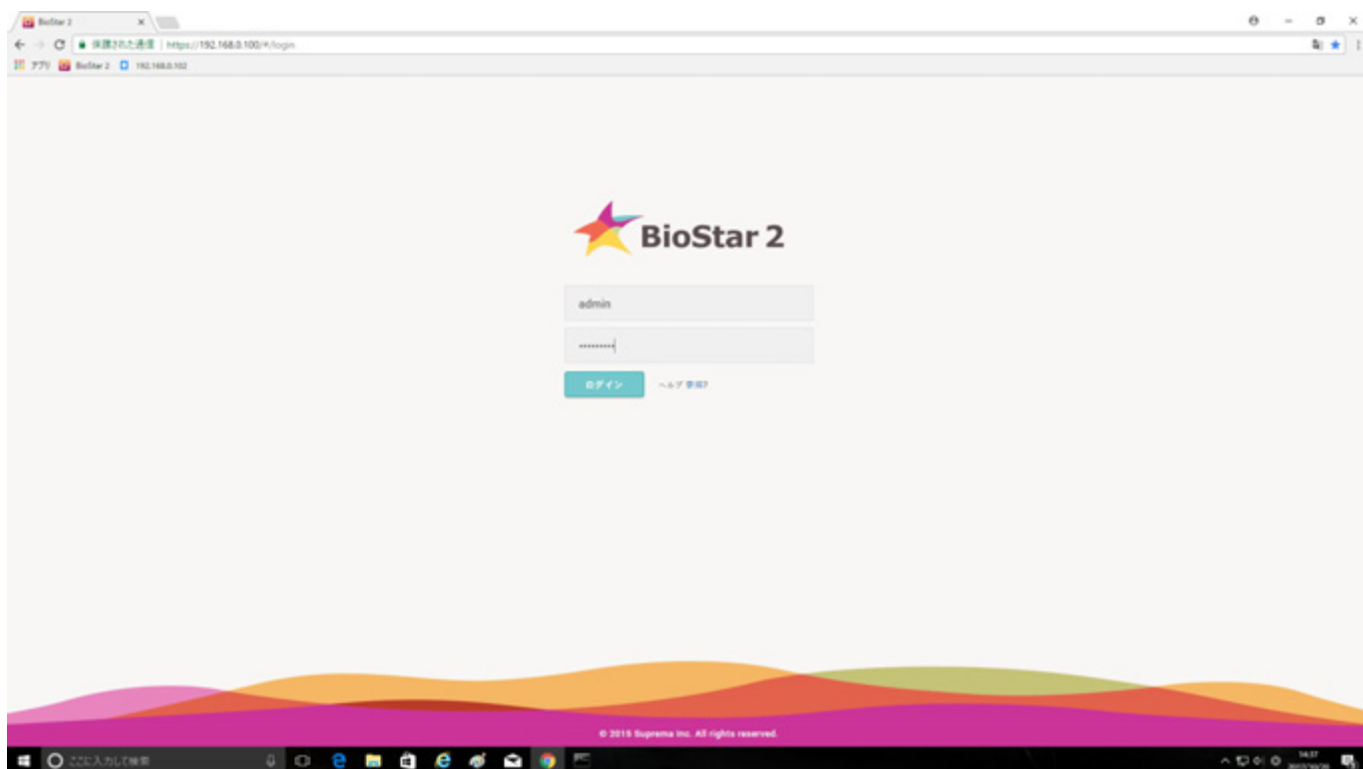
Language で「日本語 (にほんご)」をクリックして **Apply** をクリックします。



「ダッシュボード」をクリックしてダッシュボードに戻ります。





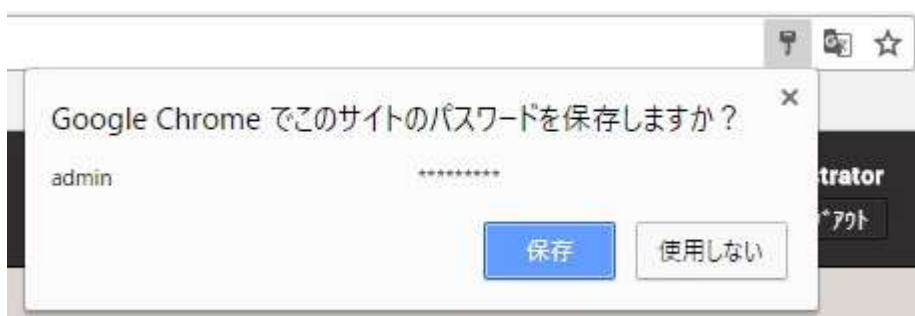
Google Chrome のパスワードの管理設定



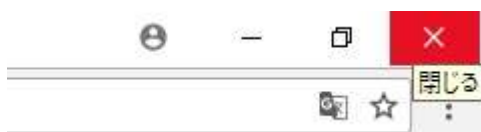
BioStar2 へのログイン時に毎回 ID と PASSWORD を入力したくない場合、Google Chrome のパスワードの管理機能を使用してパスワードを保存することが出来ます。




または  または  の形の鍵のアイコン(パスワードを保存)をクリックします。



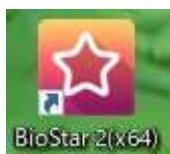
 をクリックします。



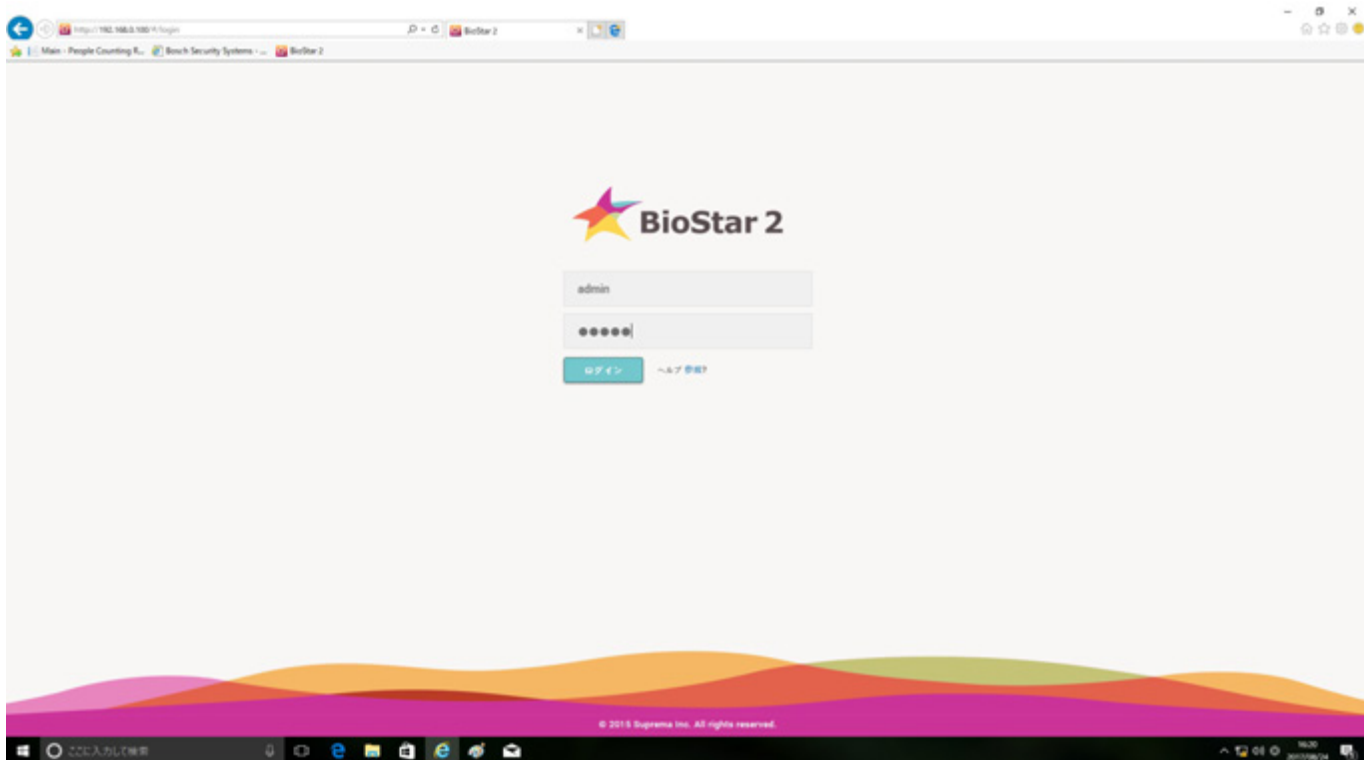
右上の閉じるで Google Chrome を終了します。

次の起動時から、ID と PASSWORD 欄に自動的に入力されますので、 ボタンをクリックするだけで済むようになります。

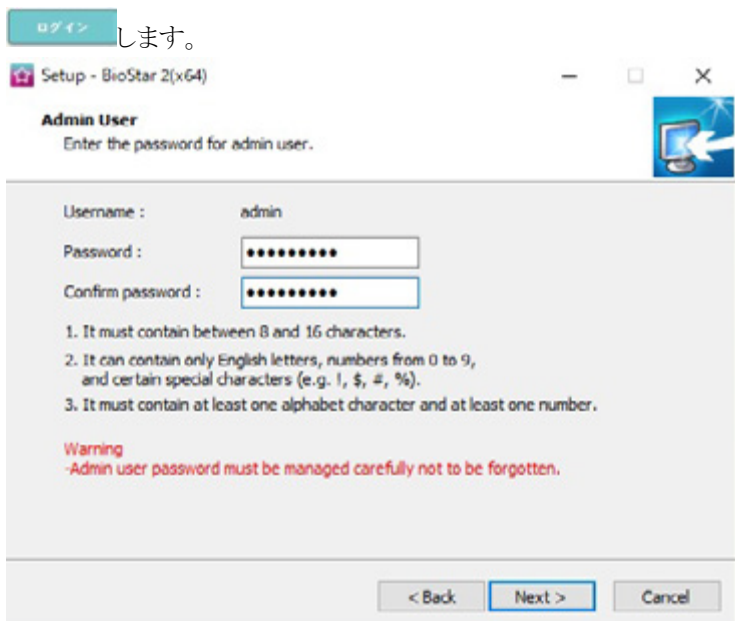
BioStar2.6.1 の起動



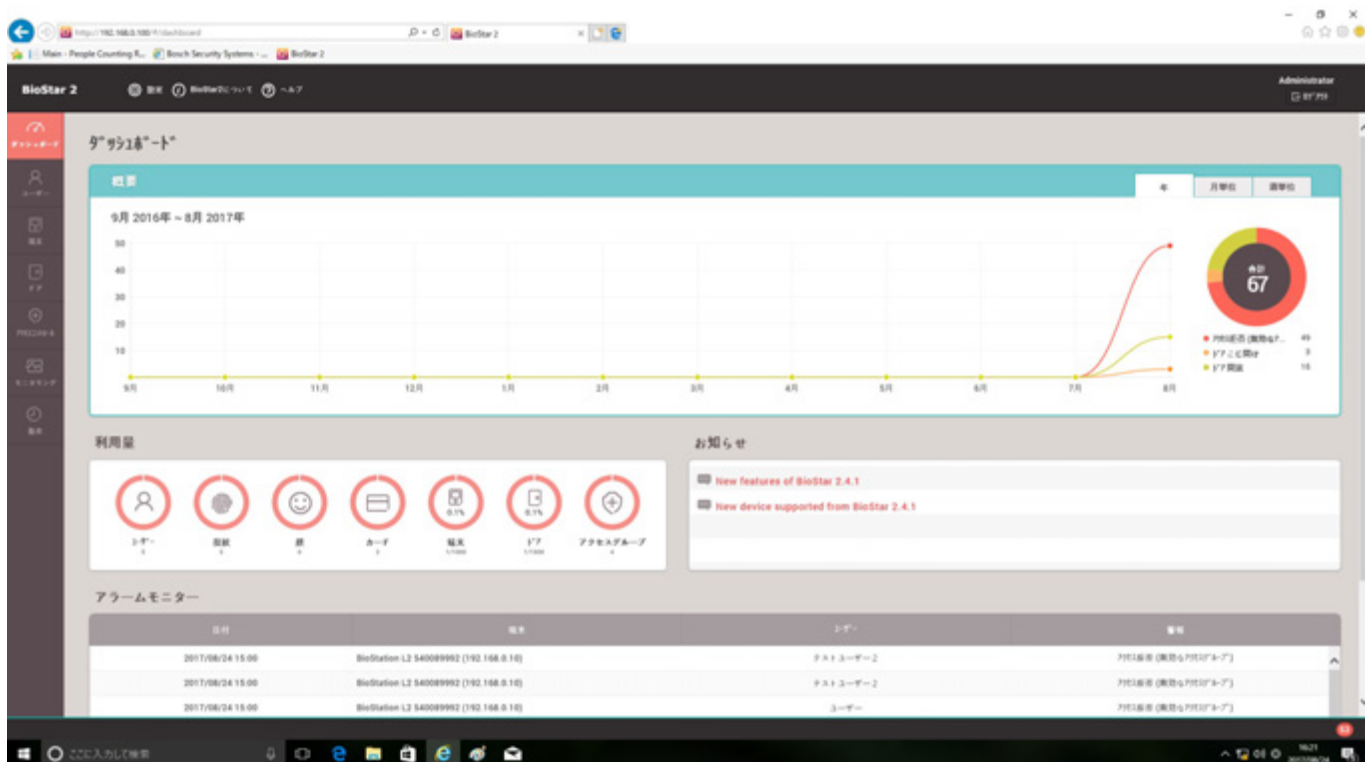
BioStar2(x64)アイコンをダブルクリックします。



admin/password (デフォルトは admin/BioStar2 2.5.0.203.exe のインストール時に入力したパスワード)を入力して

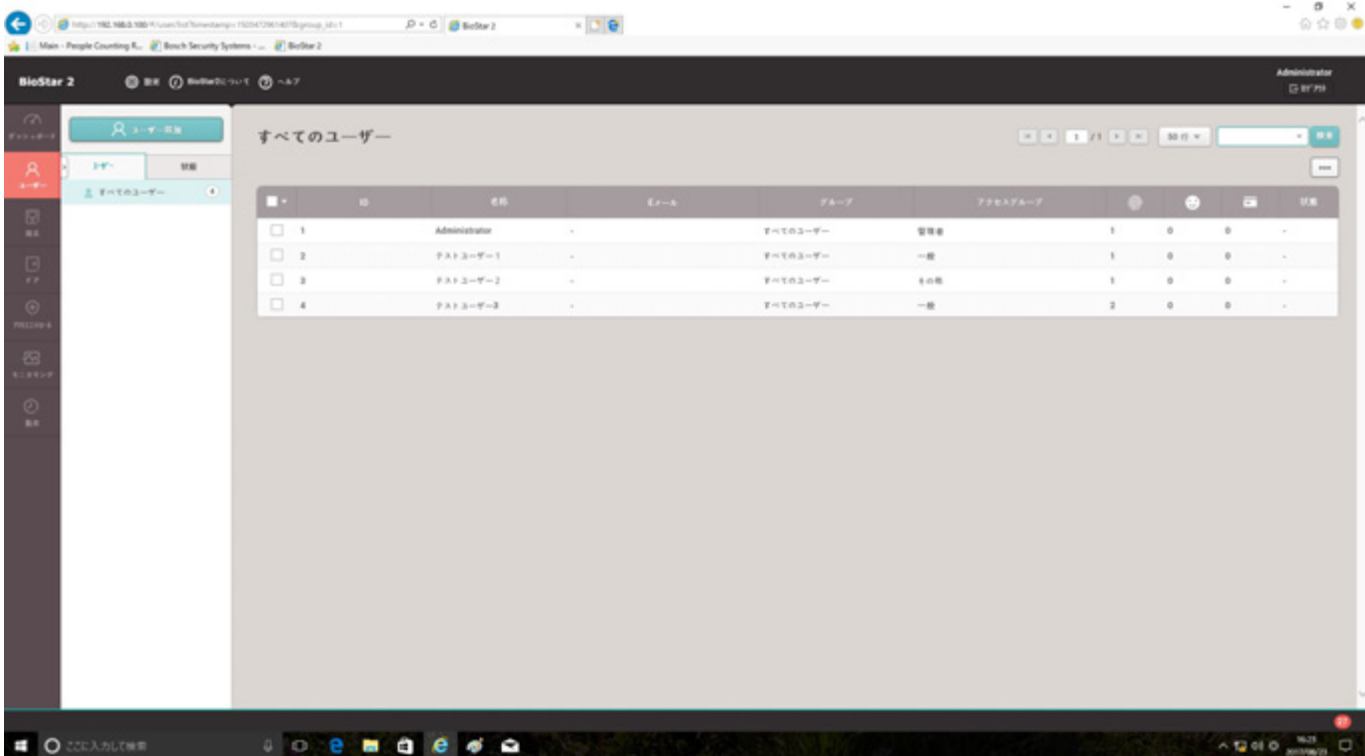


admin のパスワードは 8～16 文字でなければなりません。英語の文字、0～9 の数字、および特定の特殊文字(たとえば、!、\$、#、%)のみを含むことができます。少なくとも 1 つのアルファベット文字と少なくとも 1 つの数字を含む必要があります。管理者のパスワードは忘れないように注意深く管理する必要があります。

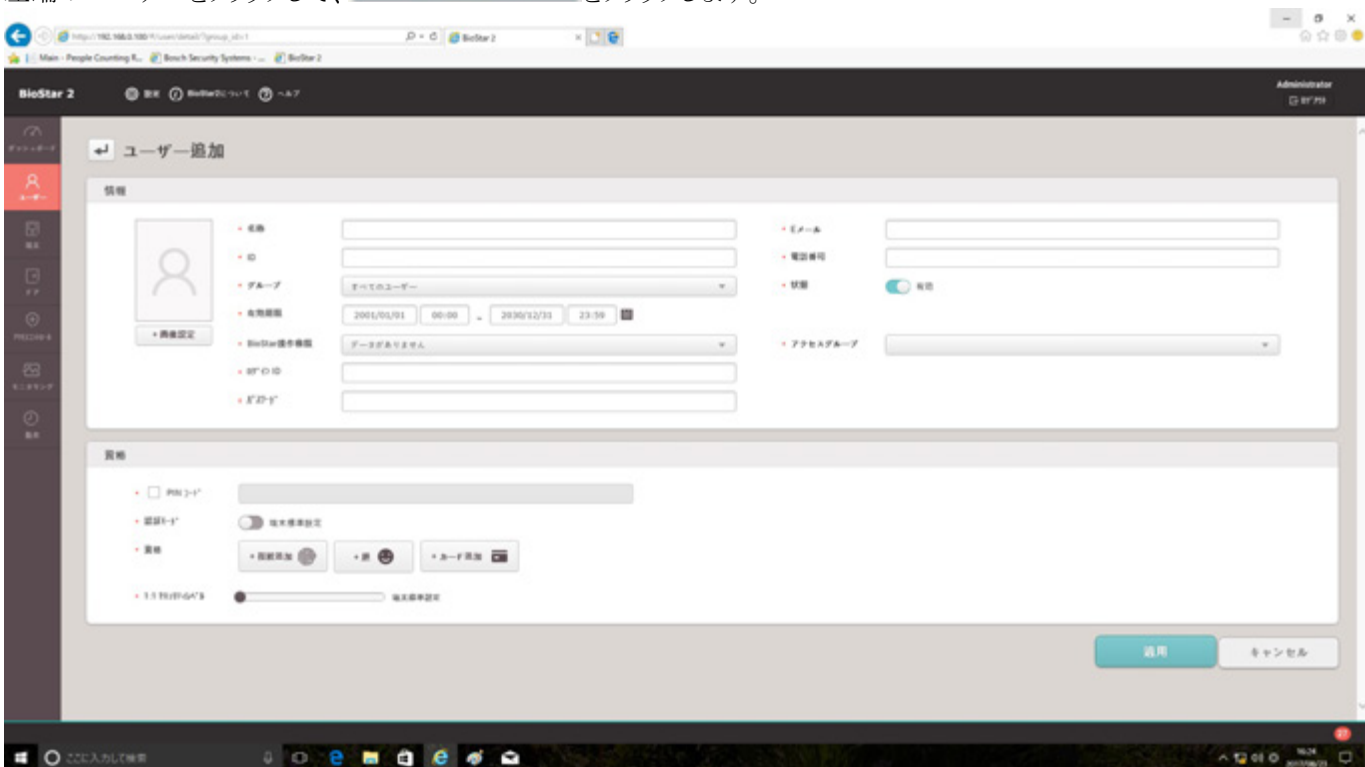


ログインするとダッシュボードが表示されます。

ユーザーの作成



左端のユーザーをクリックして、**ユーザー追加** をクリックします。



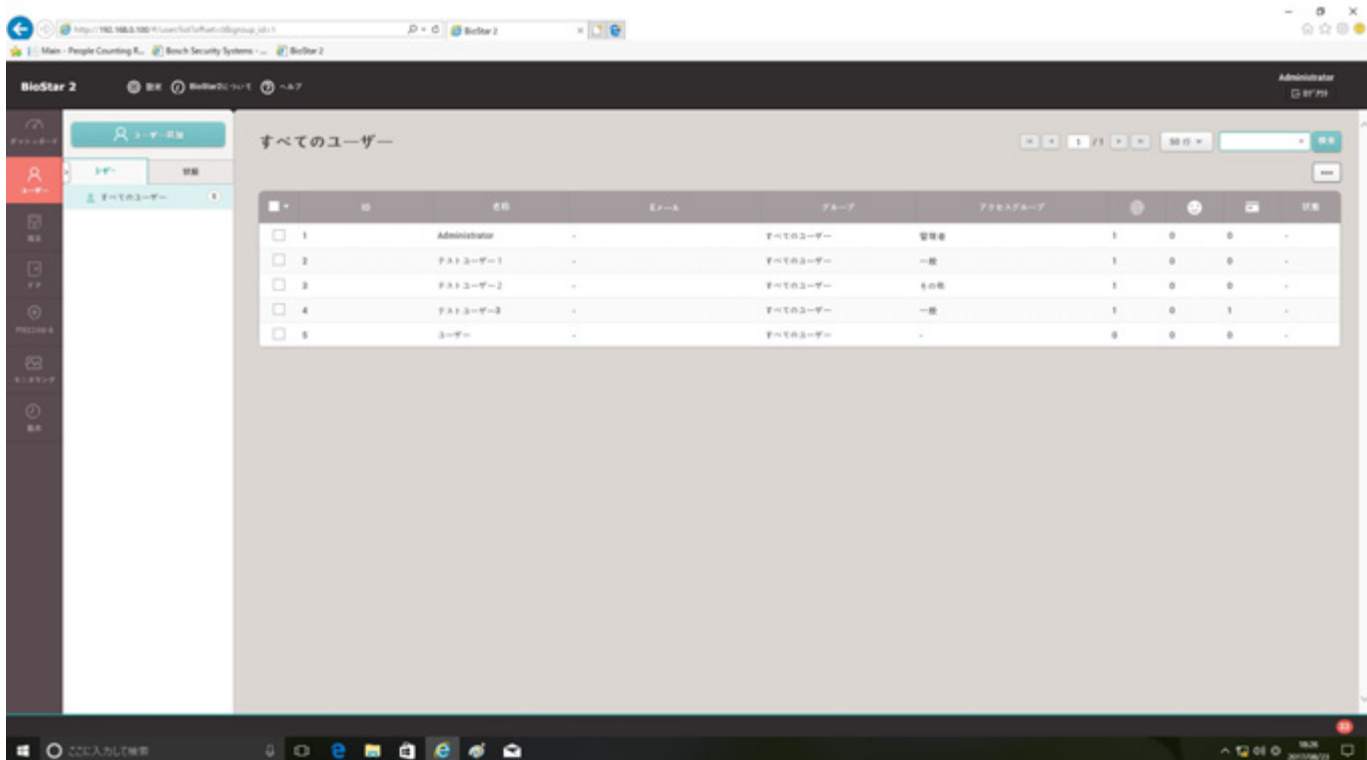
ユーザー設定には、大きく分けて「情報」と「資格」の2つの項目があります。情報には名称・ID・グループ(デフォルトで「すべてのユーザー」)・有効期限・Biostar 動作権限・ログイン ID・パスワード・Eメール・電話番号・状態(デフォルトで「有効」)・アクセスグループがあります。資格には認証に使用するデータとしての入力があります。PIN コード・認証モード・資格・1:1セキュリティレベルがあります。

情報には最低限 ID (1~4294967294 の範囲) があればユーザーを登録できますが、名称(個人名)を入力しておくとも明示しやすくなります。

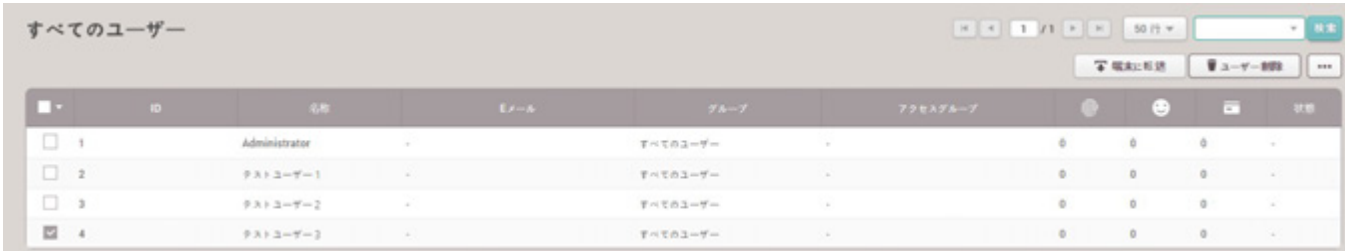
• 名称

• ID

をクリックすると、ユーザーが作成されます。




ユーザーの削除



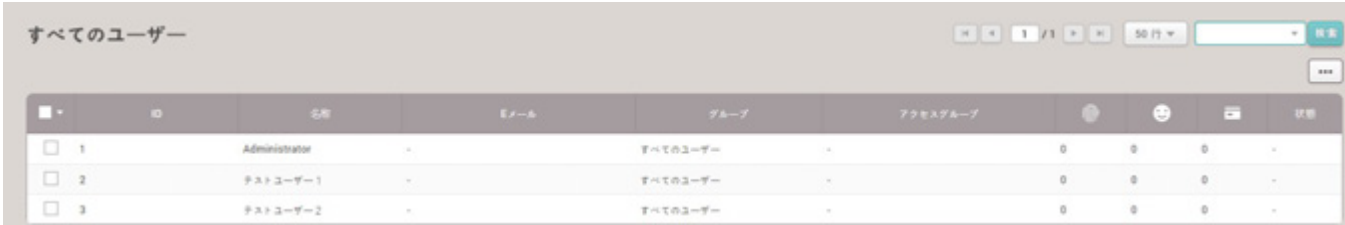
すべてのユーザー

ID	名前	メール	グループ	アクセスグループ					
<input type="checkbox"/>	1	Administrator	-	すべてのユーザー	-	0	0	0	-
<input type="checkbox"/>	2	テストユーザー1	-	すべてのユーザー	-	0	0	0	-
<input type="checkbox"/>	3	テストユーザー2	-	すべてのユーザー	-	0	0	0	-
<input checked="" type="checkbox"/>	4	テストユーザー3	-	すべてのユーザー	-	0	0	0	-

削除したいユーザーに を入れます。右上に  が表示されます。



「はい」をクリックします。

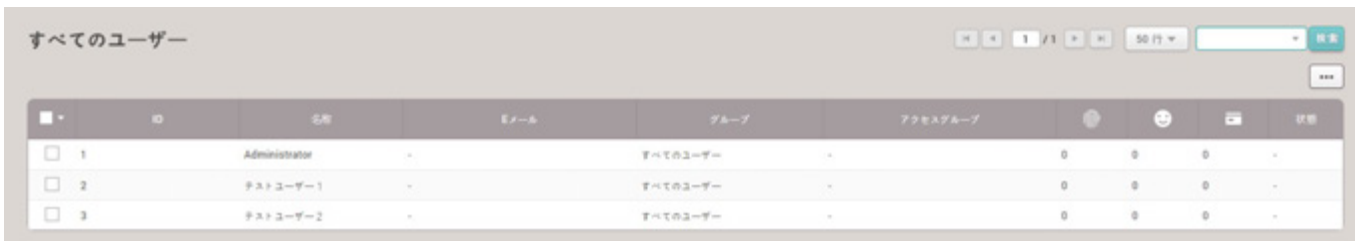


すべてのユーザー

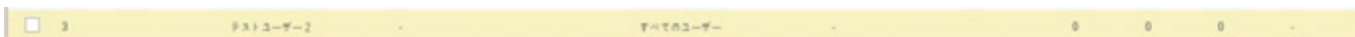
ID	名前	メール	グループ	アクセスグループ					
<input type="checkbox"/>	1	Administrator	-	すべてのユーザー	-	0	0	0	-
<input type="checkbox"/>	2	テストユーザー1	-	すべてのユーザー	-	0	0	0	-
<input type="checkbox"/>	3	テストユーザー2	-	すべてのユーザー	-	0	0	0	-

ユーザーが削除されます。

ユーザーの無効



無効にしたいユーザーをクリックします。



ユーザーの情報が表示されます。



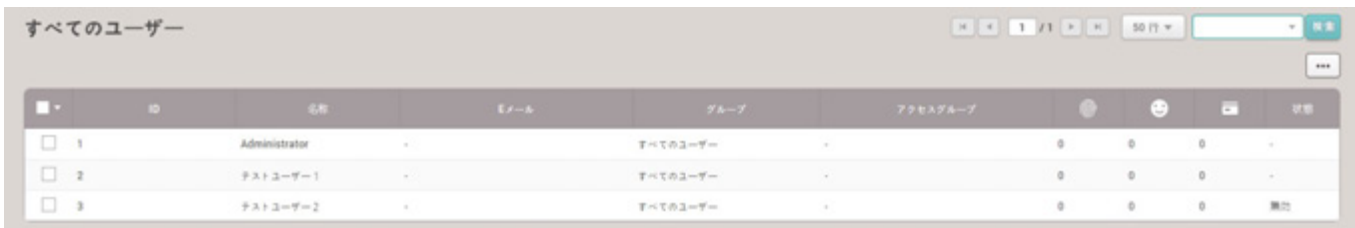
ユーザーの状態を有効から無効に変更します。



をクリックします。

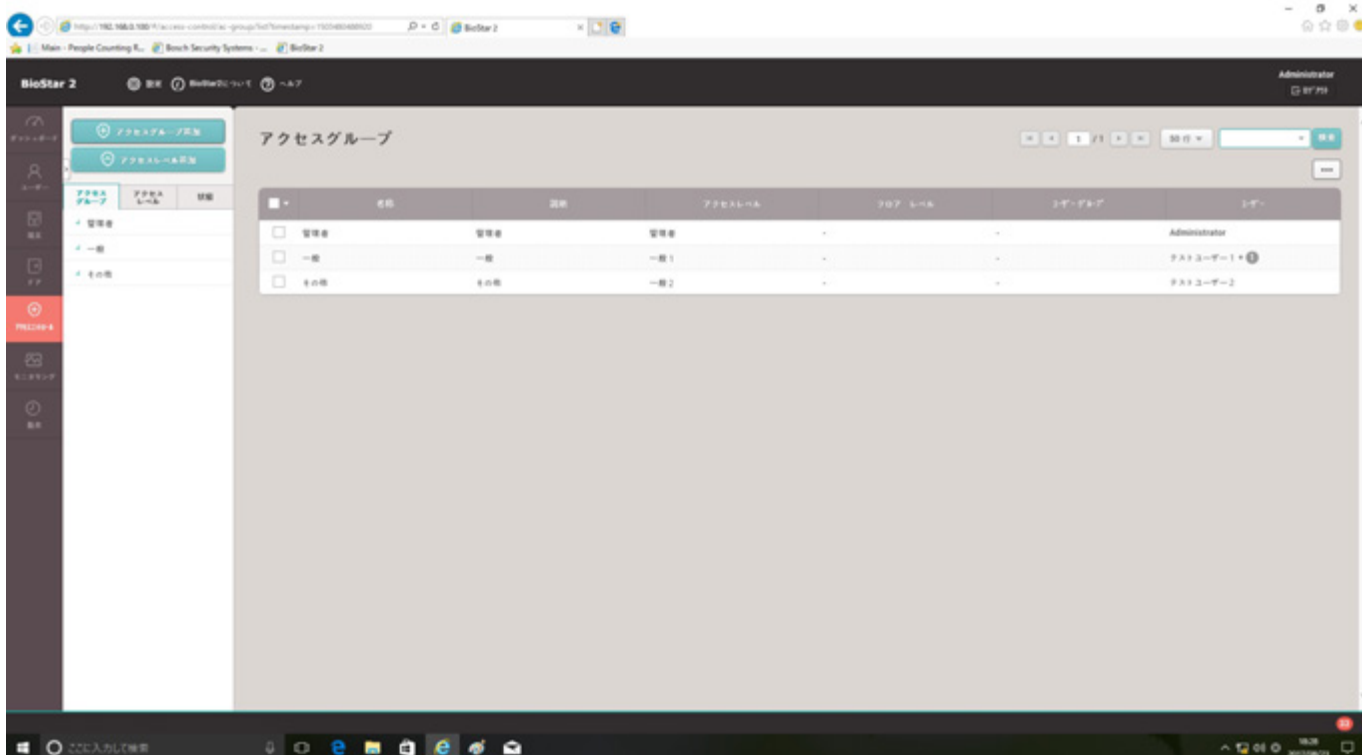


「OK」をクリックします。

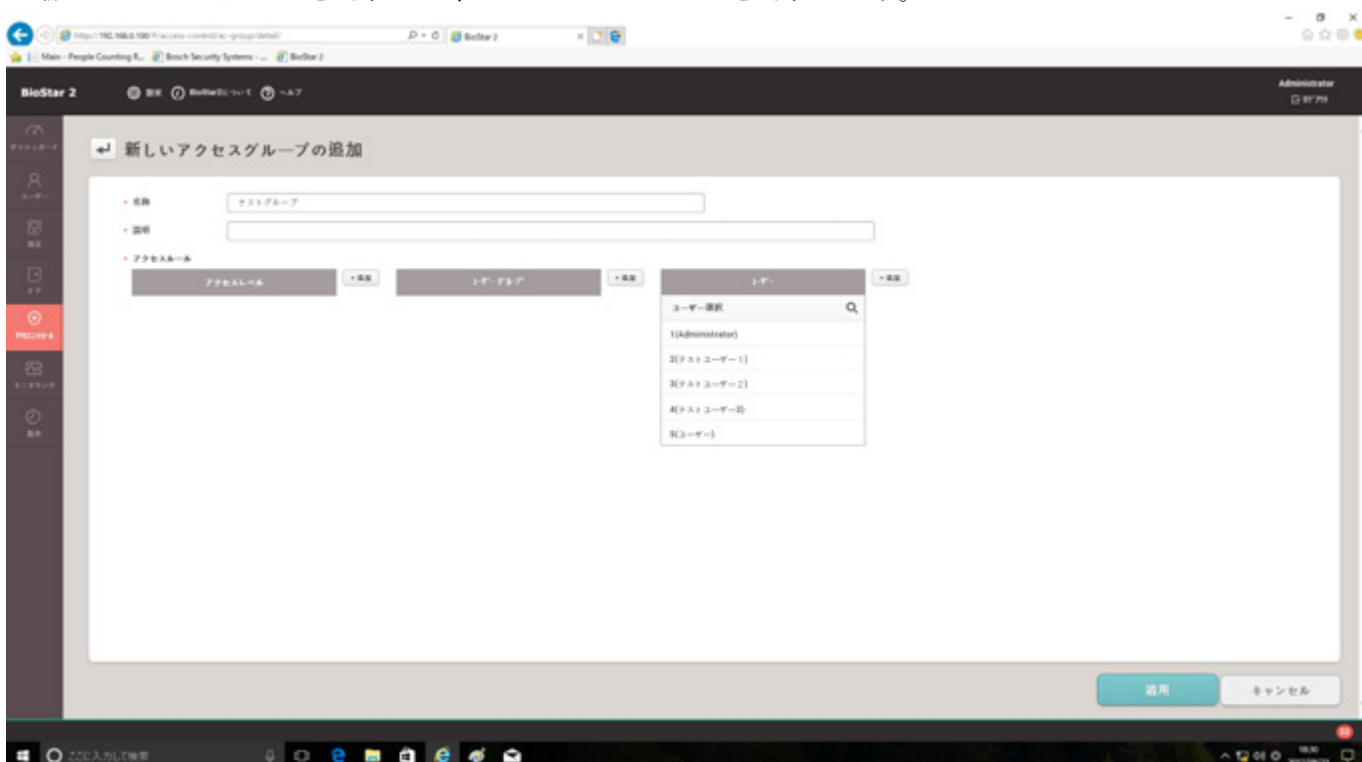


ユーザーが無効になります。

アクセスグループの作成



左端のアクセスコントロールをクリックして、**アクセスグループ追加** をクリックします。



アクセスグループには名称・説明・アクセスレベルがあります。
 アクセスレベルには最低限、アクセスレベルとユーザーもしくはユーザーグループが必要になります。例ではアクセスレベルとユーザーを登録します。

アクセスルールの各項目の右側にある **+追加** をクリックすると、Biostar2.4.1 に登録されている情報が表示されます。



先の項で作成した ID5 のユーザーが一番下に表示されていますので、これをクリックします。

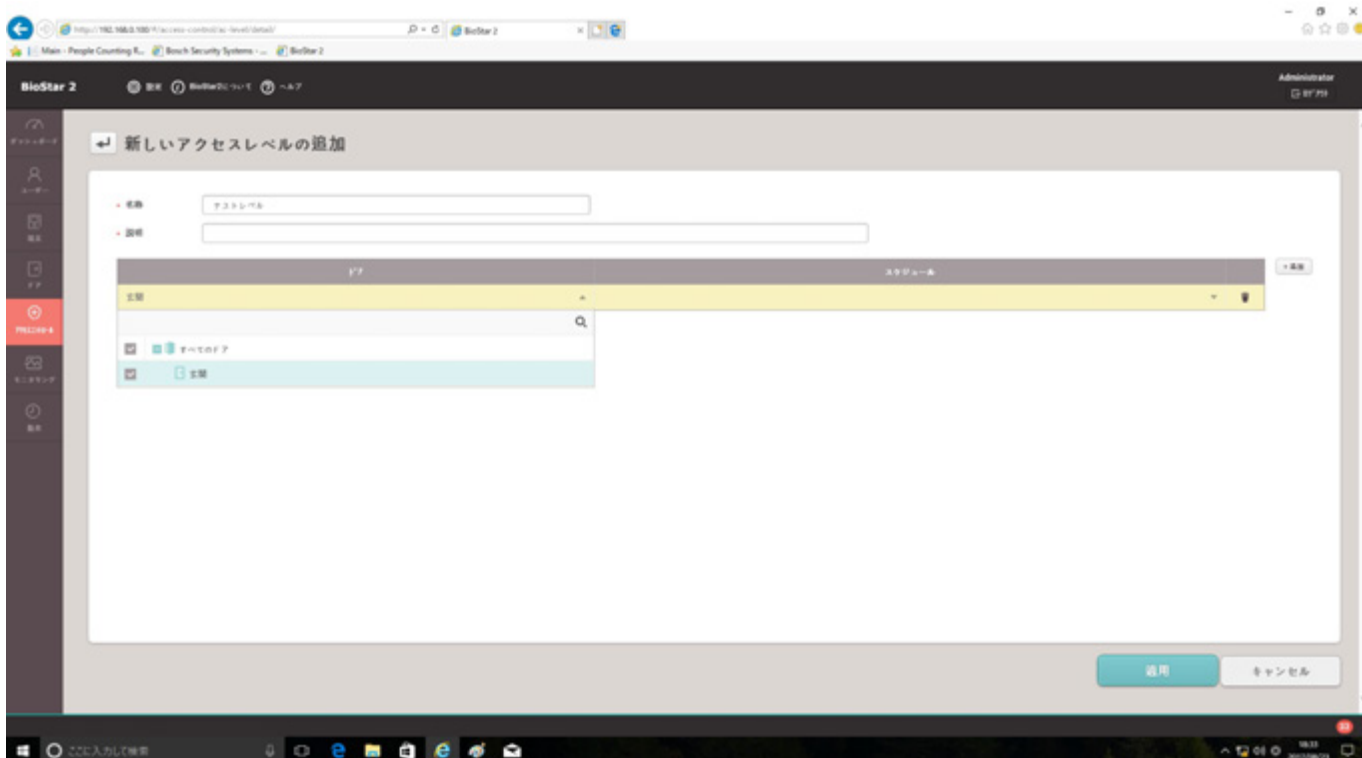


のように選択されて表示されます。

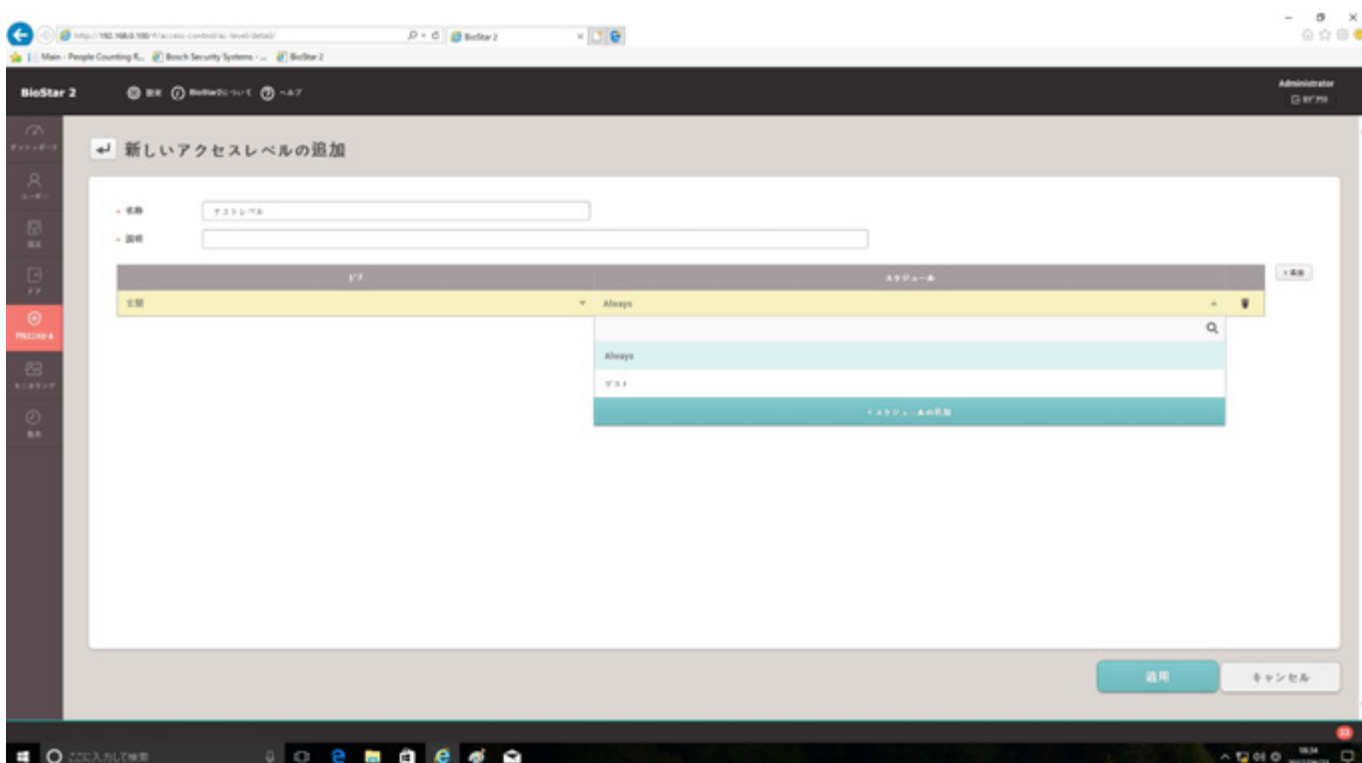
同様にアクセスレベル追加でアクセスレベルを追加します。アクセスレベルの右側の **+追加** をクリックします。



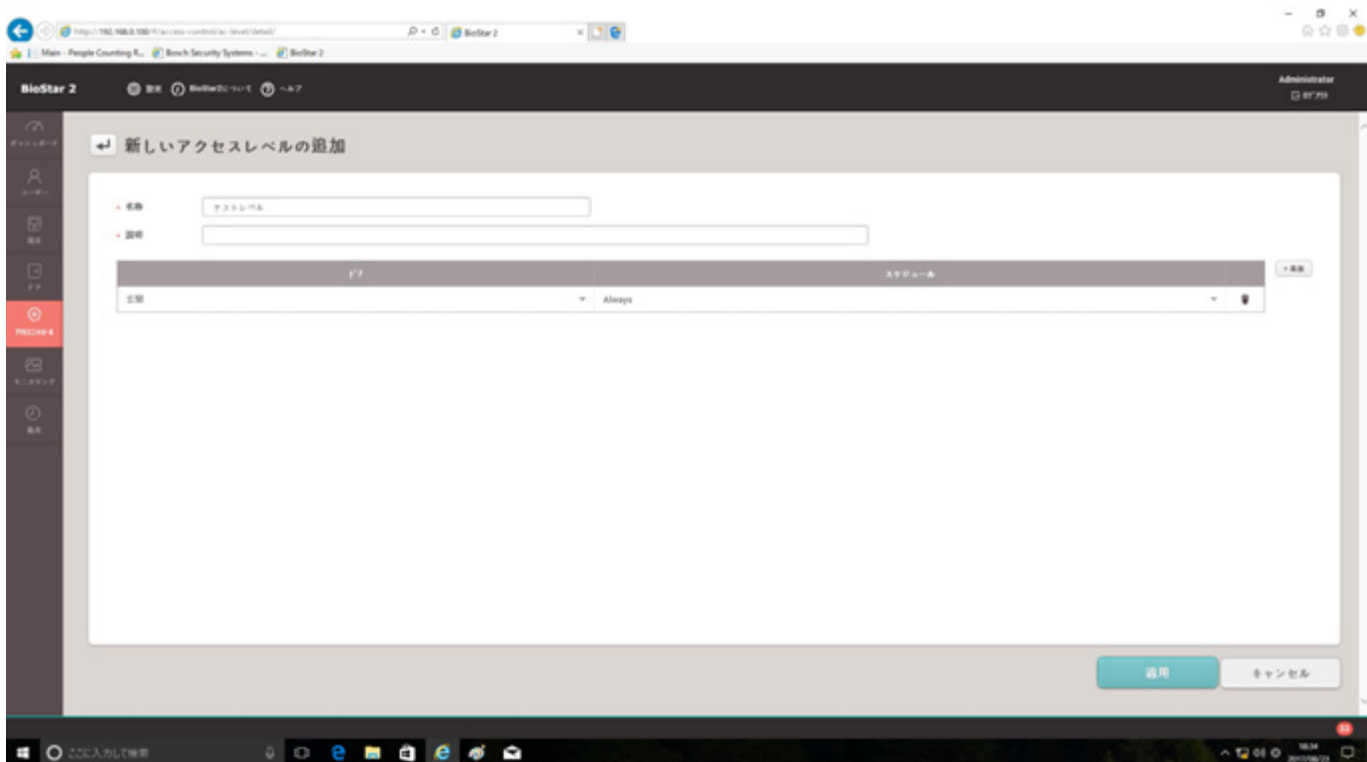
アクセスレベルを作成するには **+アクセスレベル追加** をクリックします。



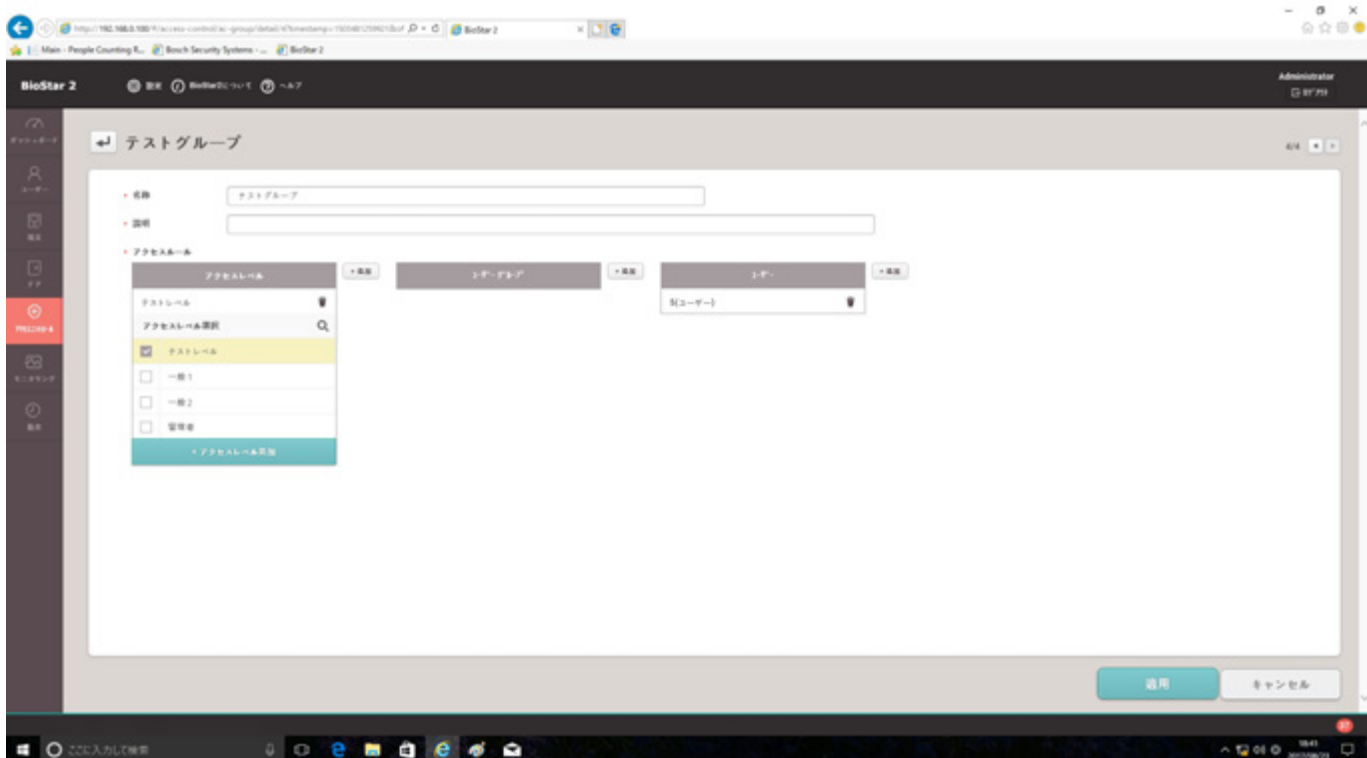
新しいアクセスレベルの追加が開きます。「ドア」を作成していない場合はドアの作成を行ってください。



スケジュールは特に指定しなければ「Always」で構いません。
Always では、端末が設置されたドア入口は、常時いずれかの認証が必要です。
スケジュールでは、スケジュール設定した時間範囲のみ認証が必要な設定ができます。

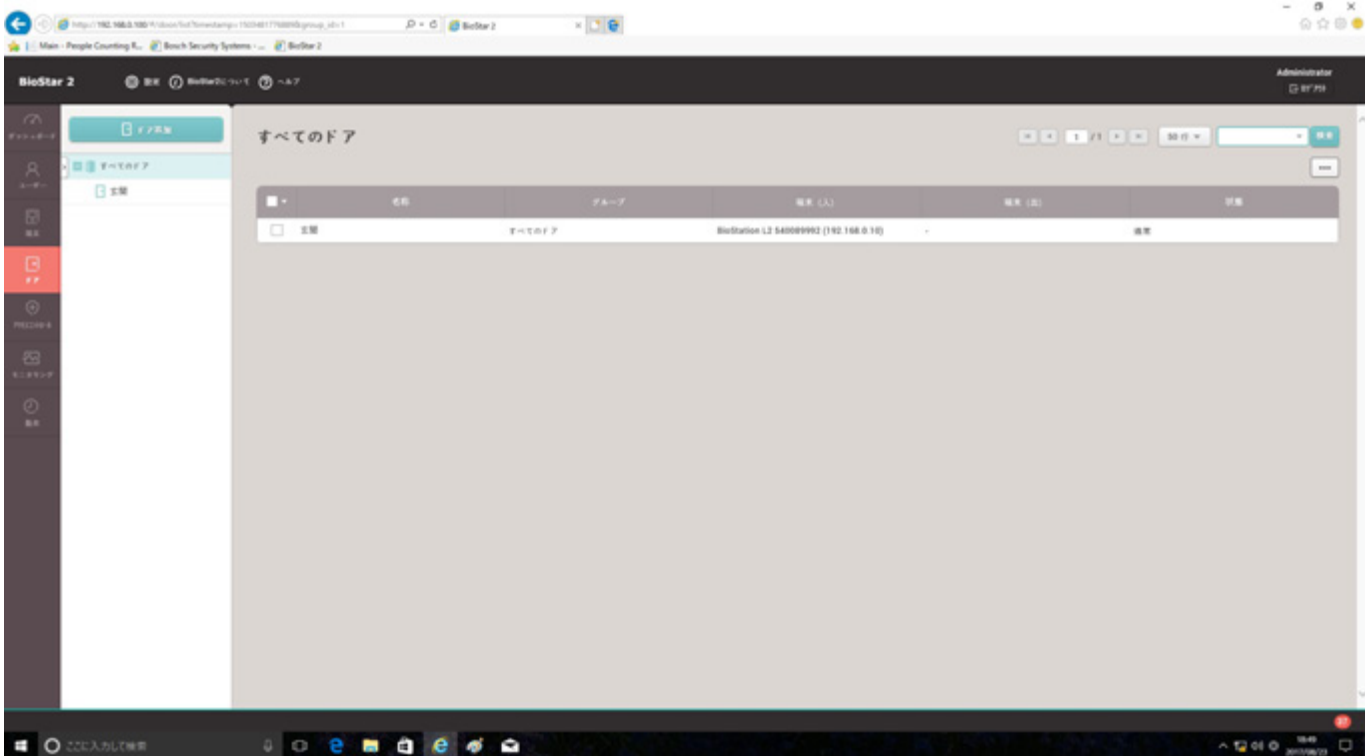


適用 をクリックすると、アクセスレベルが作成されます。

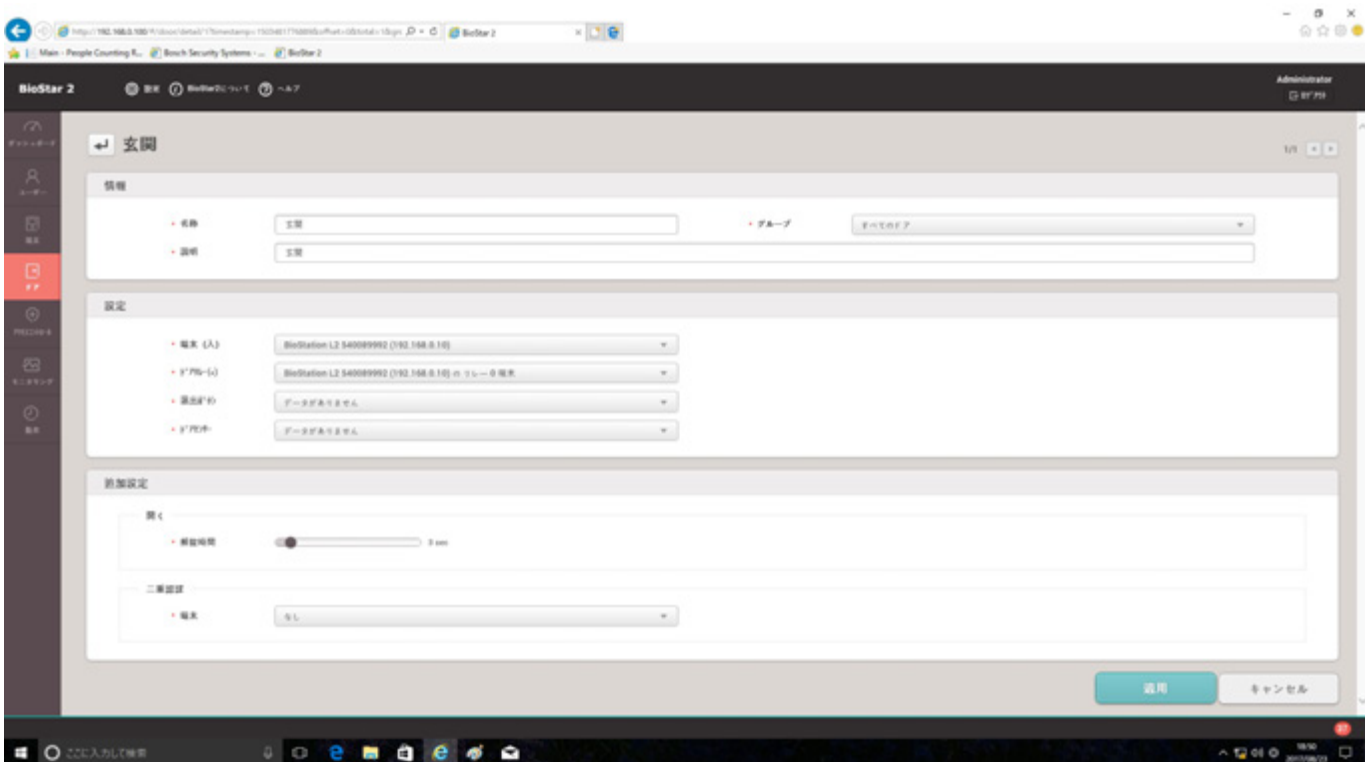


同様にアクセスレベルをグループで選択します。
適用 をクリックすると、アクセスグループが作成されます。

ドアの作成



ドアを作成するには、左端のドアを選択し、**ドア追加** をクリックします。

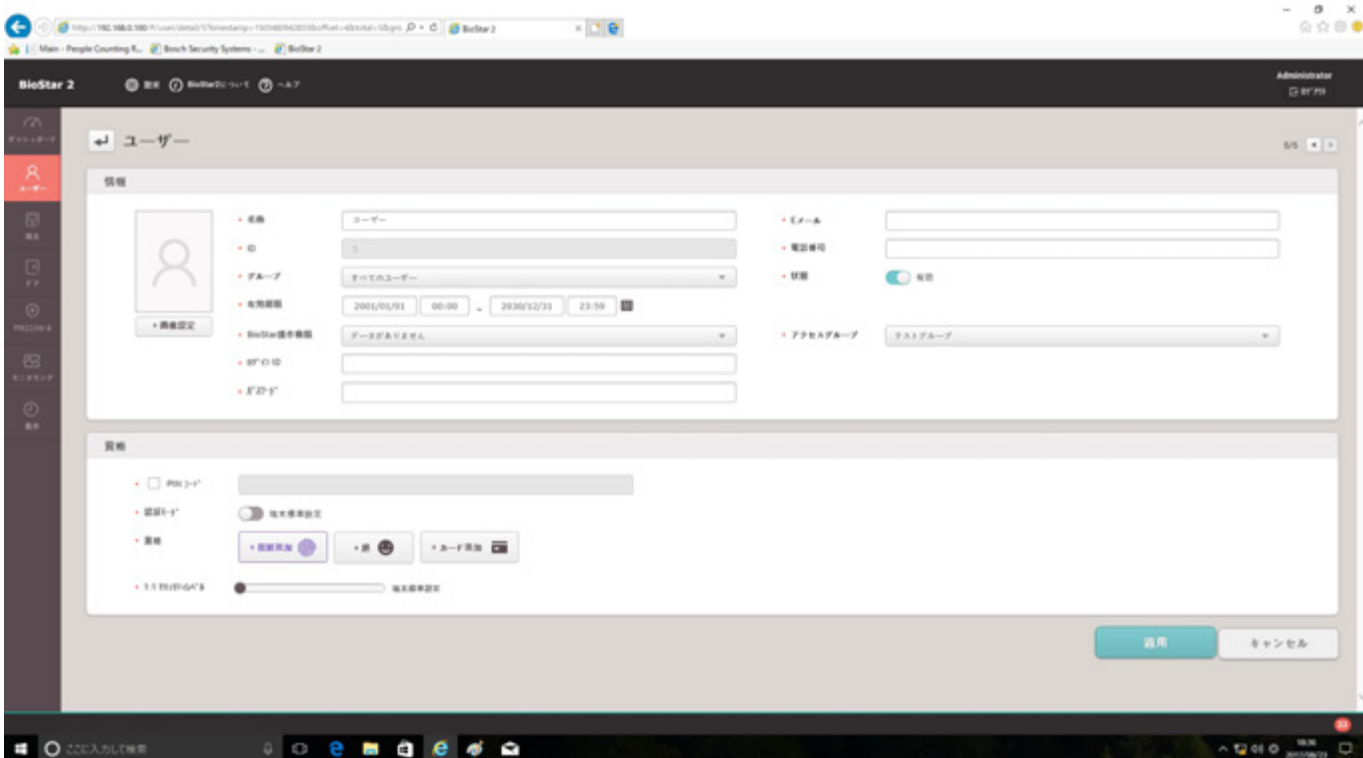


ドアは大きく分けて「情報」・「設定」・「追加設定」があり、情報には名称・グループ・説明があります。設定には端末(入)・ドアリレー(*)・退出ボタン・ドアセンサーがあります。追加設定には、解錠時間・端末の二重認証の設定があります。
 ※通常は工事の時点で設定されているので設定の必要はありません。

適用 をクリックすると、ドアが作成されます。

資格の作成

・指紋追加



ユーザーから資格で追加したい認証方法を選択クリックします。



指紋を追加する場合は、+指紋追加を選んでクリックしてください。



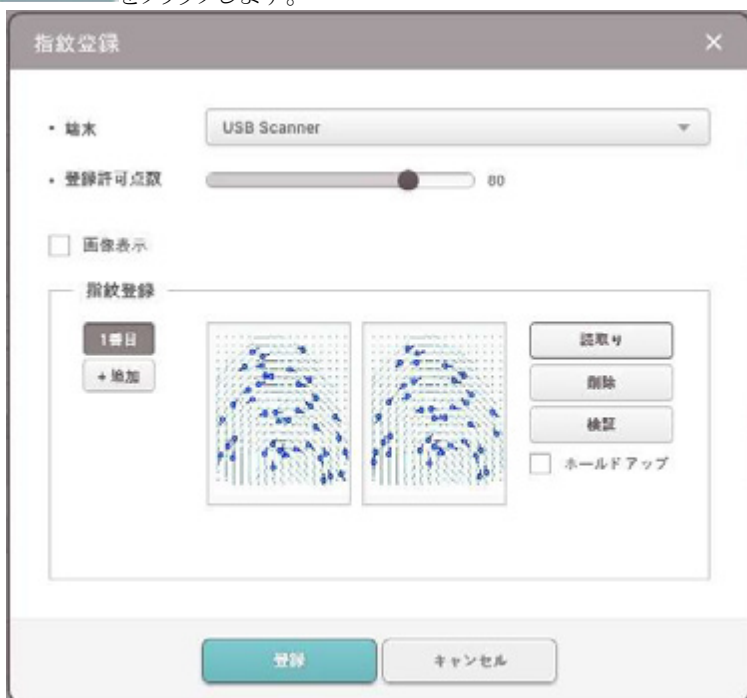
Biostar2.4.1 をインストールした PC に USB Scanner (bio mini) が接続されている場合は、端末を“USB Scanner”に設定してください。BioStationL2 などの端末で読み取る場合は端末を適宜変更してください。

+ 追加 をクリックして最大 10 本までの指紋が登録できます。読取り をクリックしてください。

画面の指示に従って、指を装置にかざしてください。読み取りが成功すると以下のような画面が表示されますので、

登録

をクリックします。



登録

をクリックして登録されると、資格欄の下部に登録情報が表示されます。

種別	ホドアール形式	数量	ホド管理
指紋	-	1	

適用

をクリックすると、認証資格が作成され、接続されている端末との同期が行われます。



このような表示が出たら、**Ok** をクリックしてください。

・カード追加



カードを追加する場合は、+カード追加を選んでクリックしてください。

カード種別などは適宜変更してください。

読み出しカード をクリックして、カードリーダーにカードを読み込ませます。

カード ID を読み込むと、番号が表示されます。

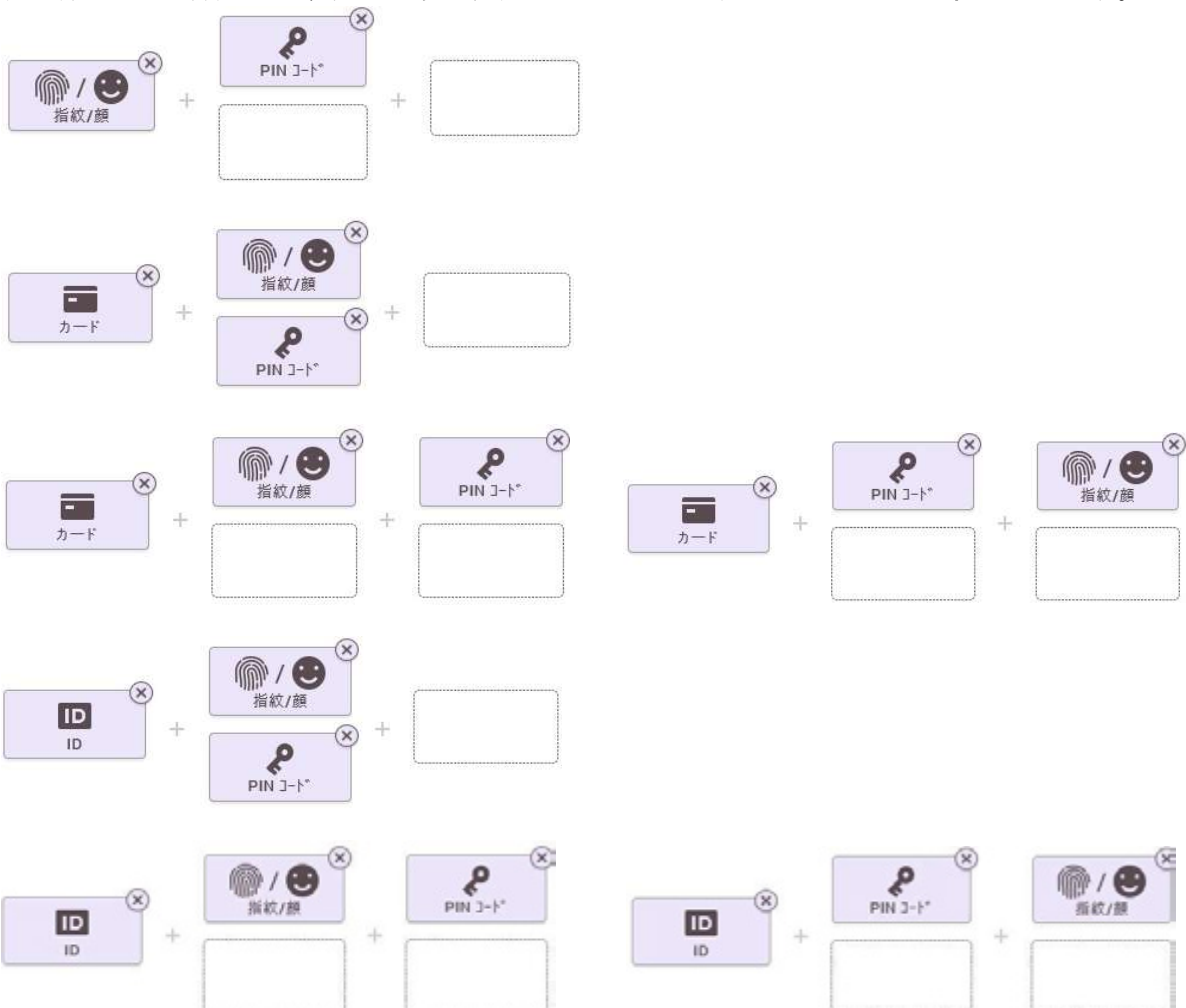
種別	カード ID 形式	枚数	カード種別
種別	-	1	
CSN	-	ID: 83035517998309286	

登録 をクリックして登録されると、資格欄の下部に登録情報が表示されます。

+追加 をクリックすると、新しい認証モードの追加が表示されます。



組み合わせには制約があり、指定した次の認証モードがグレイアウトして選択できない状態になります。



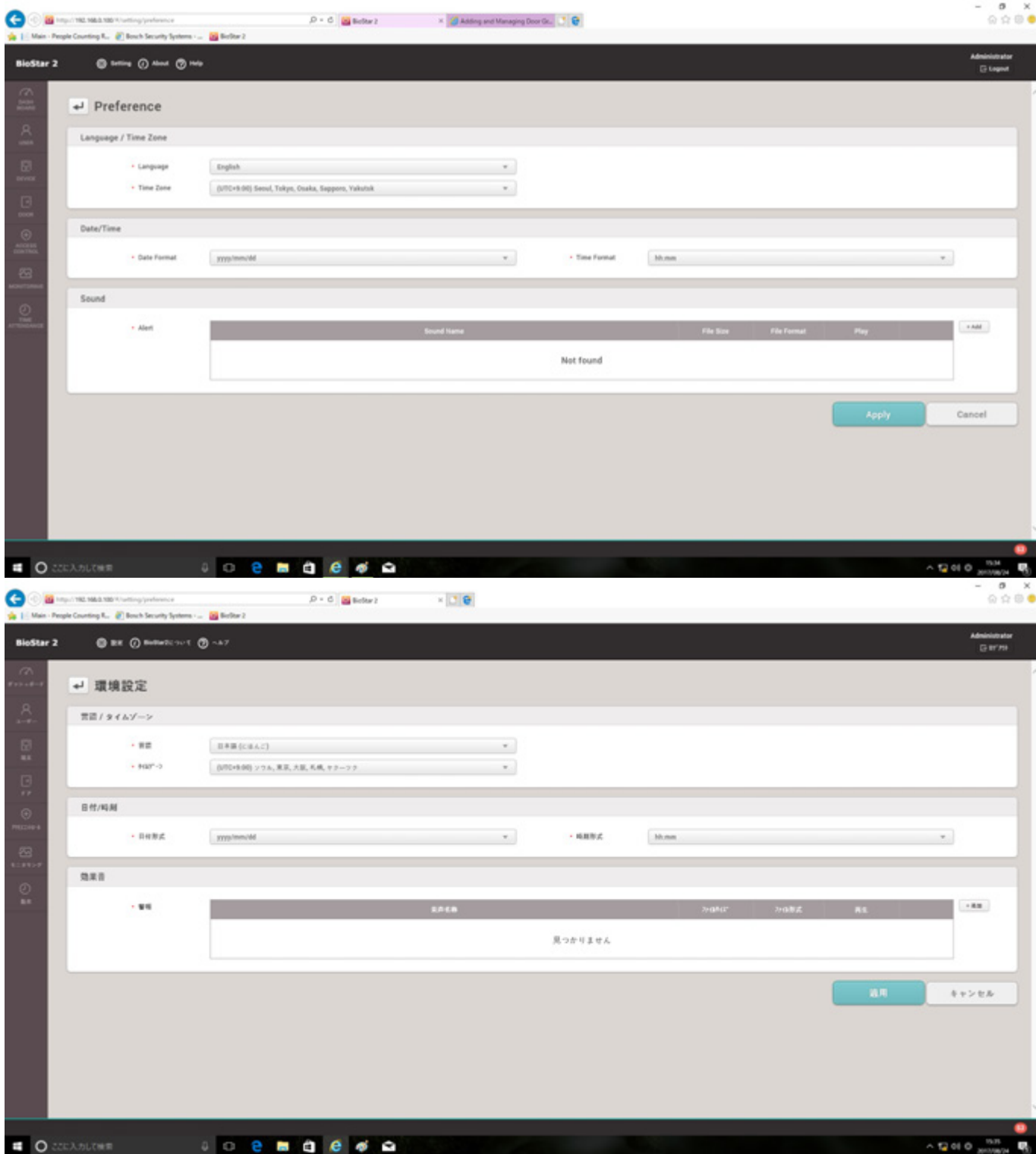
•PIN コードは端末のテンキーを使用して数値を入力します。

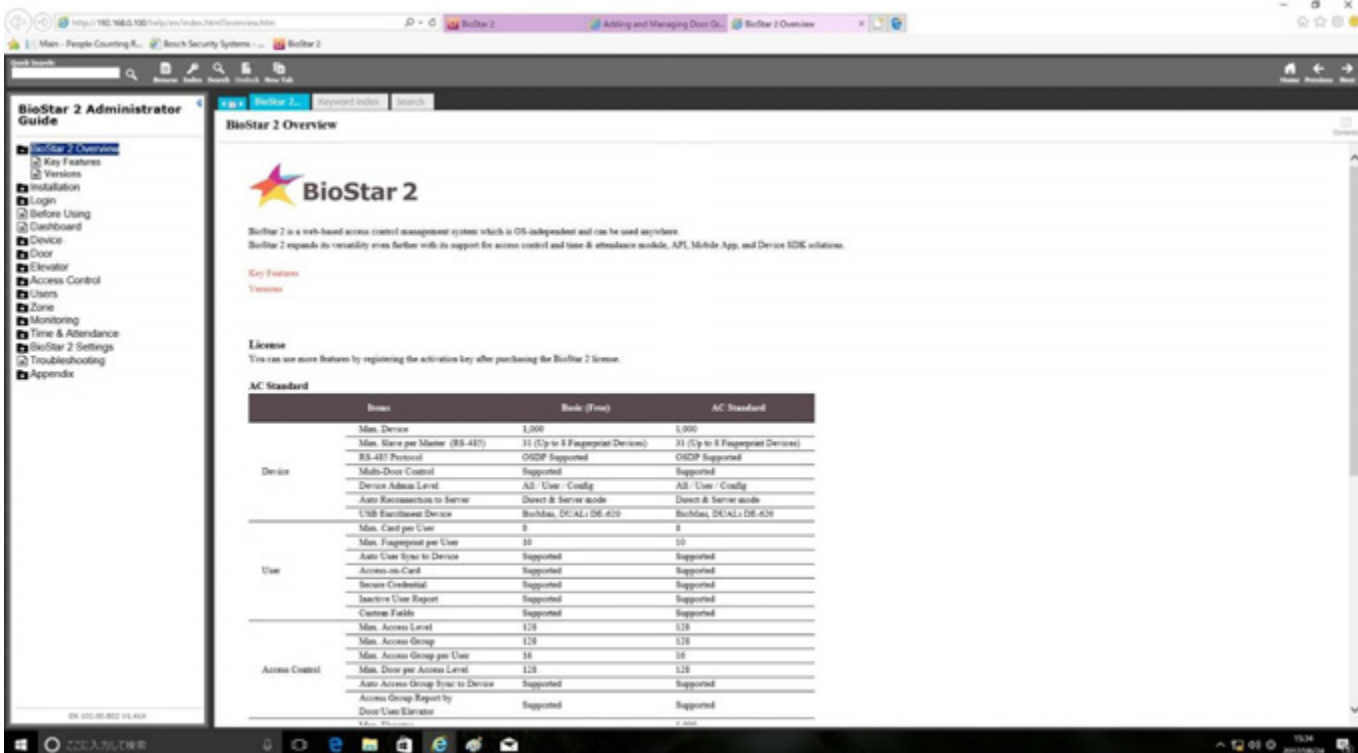


•ID はユーザーの ID 番号です。例、先のユーザー (P.32) の場合は“5”になります)

ヘルプの参照

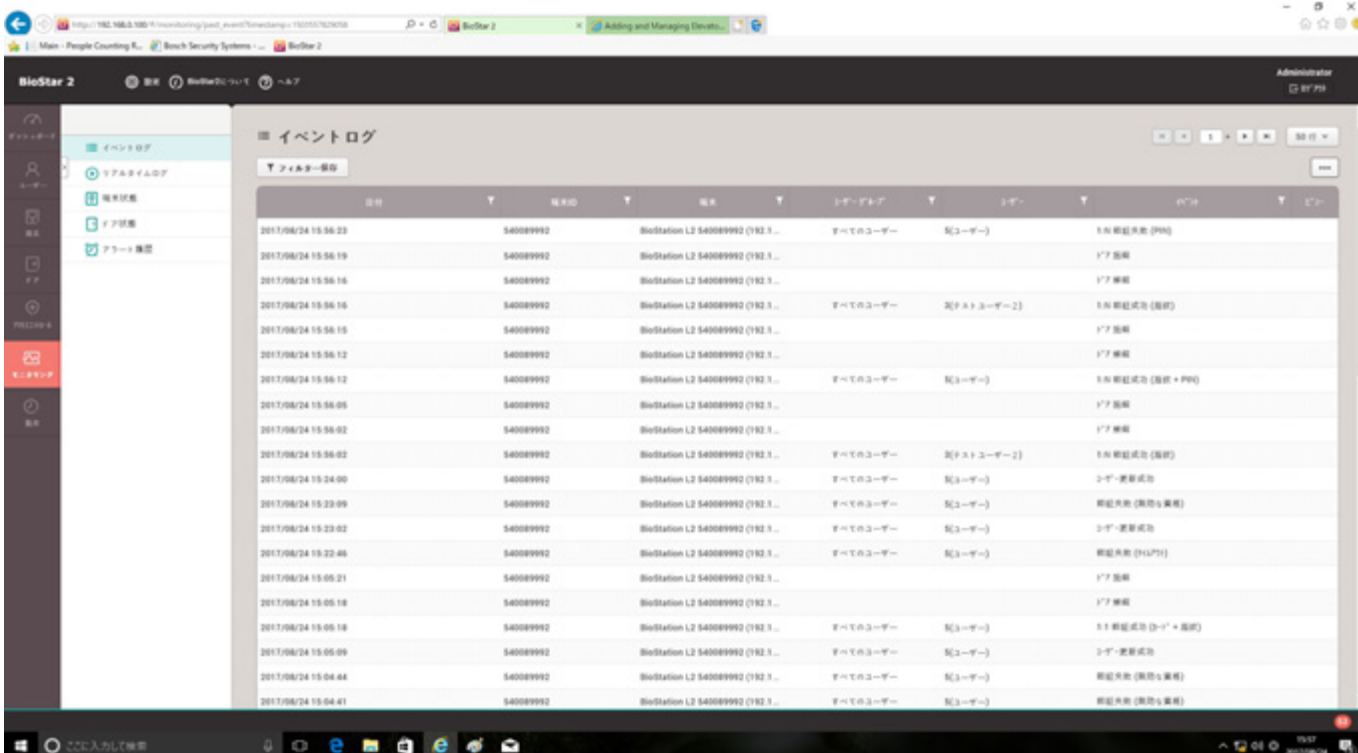
環境設定から言語を English から日本語にしても、ヘルプは英語のままになります。



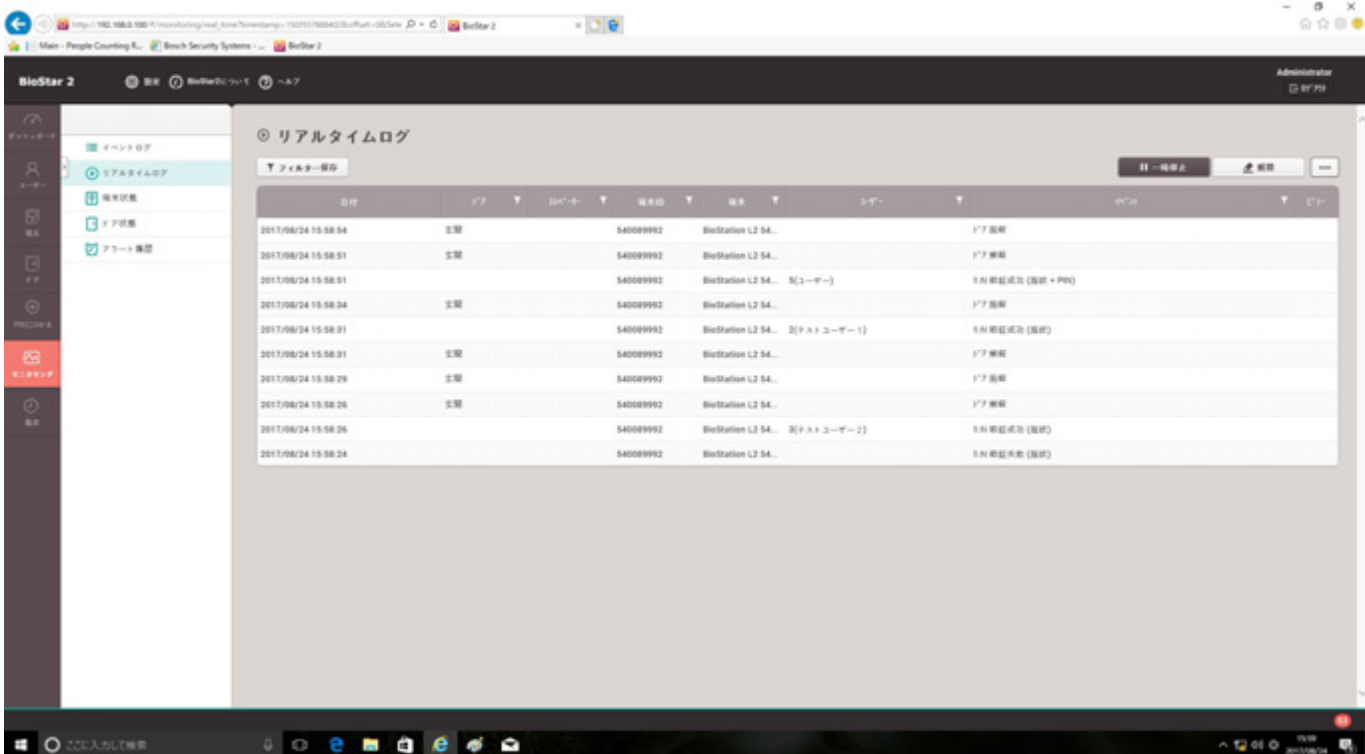


ログの種類

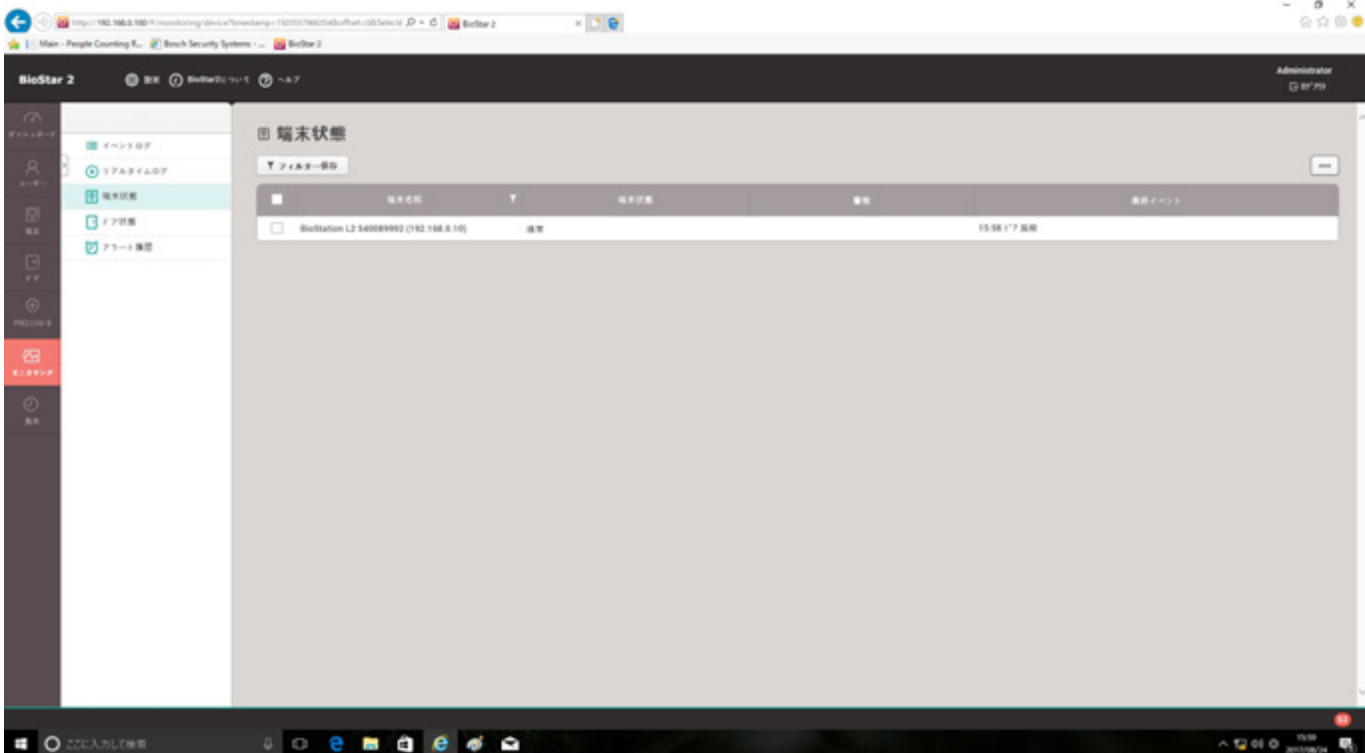
- ・イベントログ



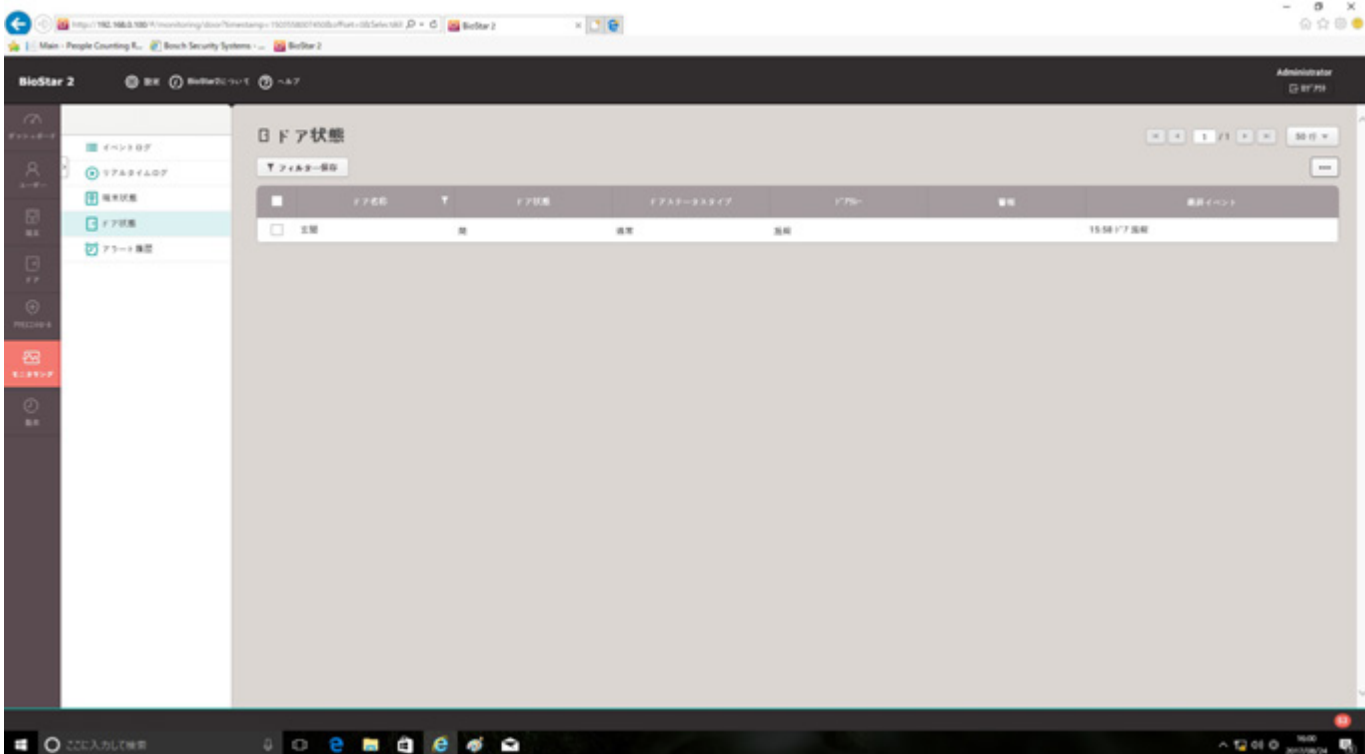
・リアルタイムログ



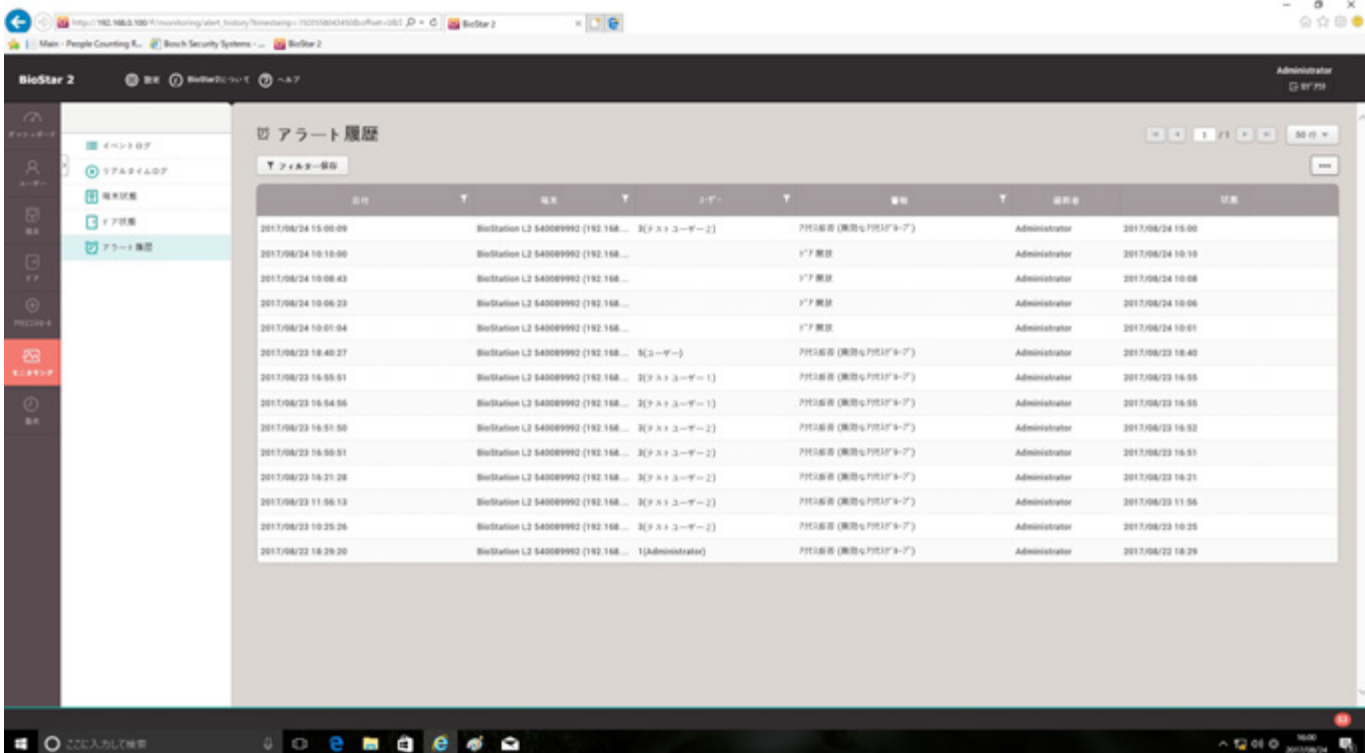
・端末状態



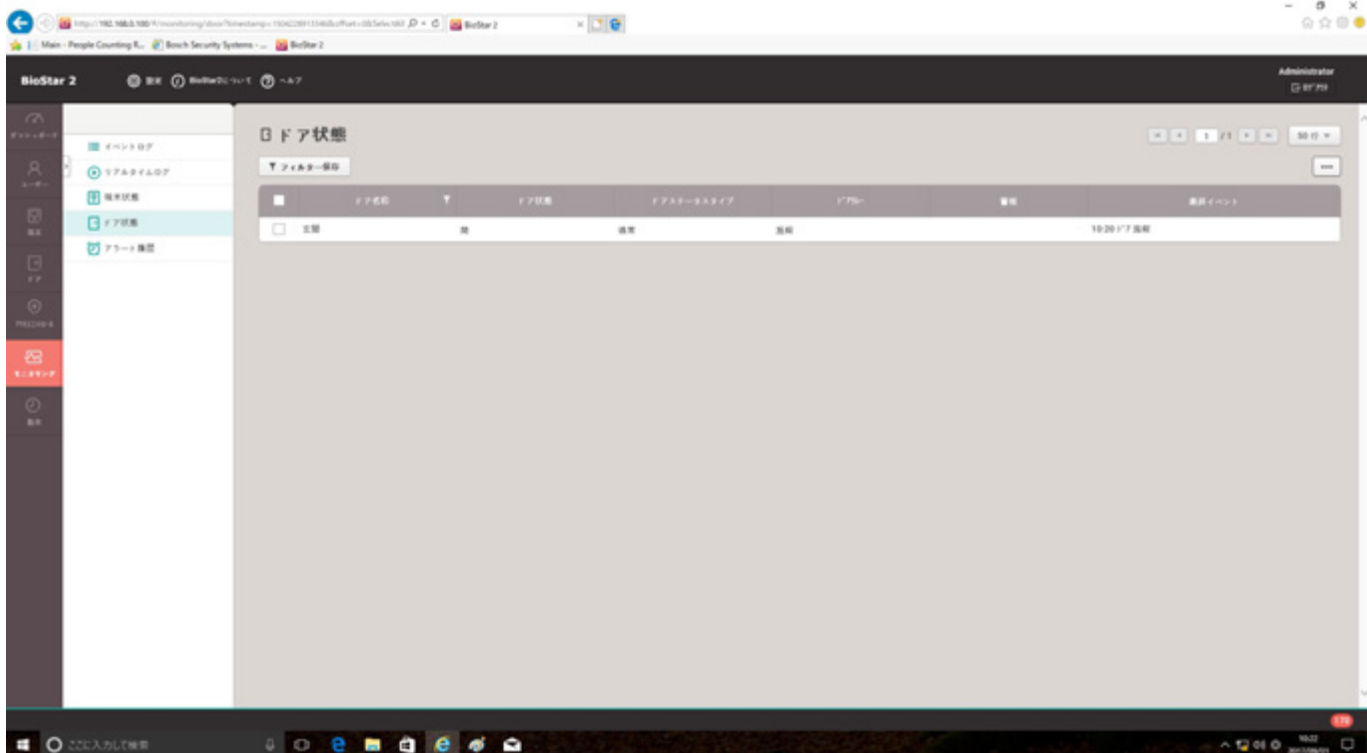
・ドア状態



・アラーム履歴



ドアの連続施錠の設定



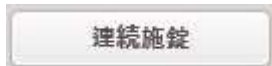
連続施錠・連続解錠が必要なドアの設定をします。モニタリングのドア状態を選択します。



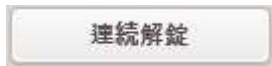
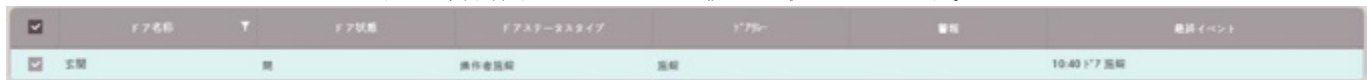
連続施錠・連続解錠が必要なドアにチェックを入れます。



上部に連続施錠・連続解錠・連続施錠解除・開く・アラームを解除・APBリセットのボタンが表示されます。



をクリックすると、操作者によるドアの連続施錠状態になります。



をクリックすると、操作者によるドアの連続解錠状態になります。



をクリックすると、操作者によるドアの連続施錠・連続解錠の状態を解除します。



をクリックすると、操作者によるドアの一回解錠の状態になります。

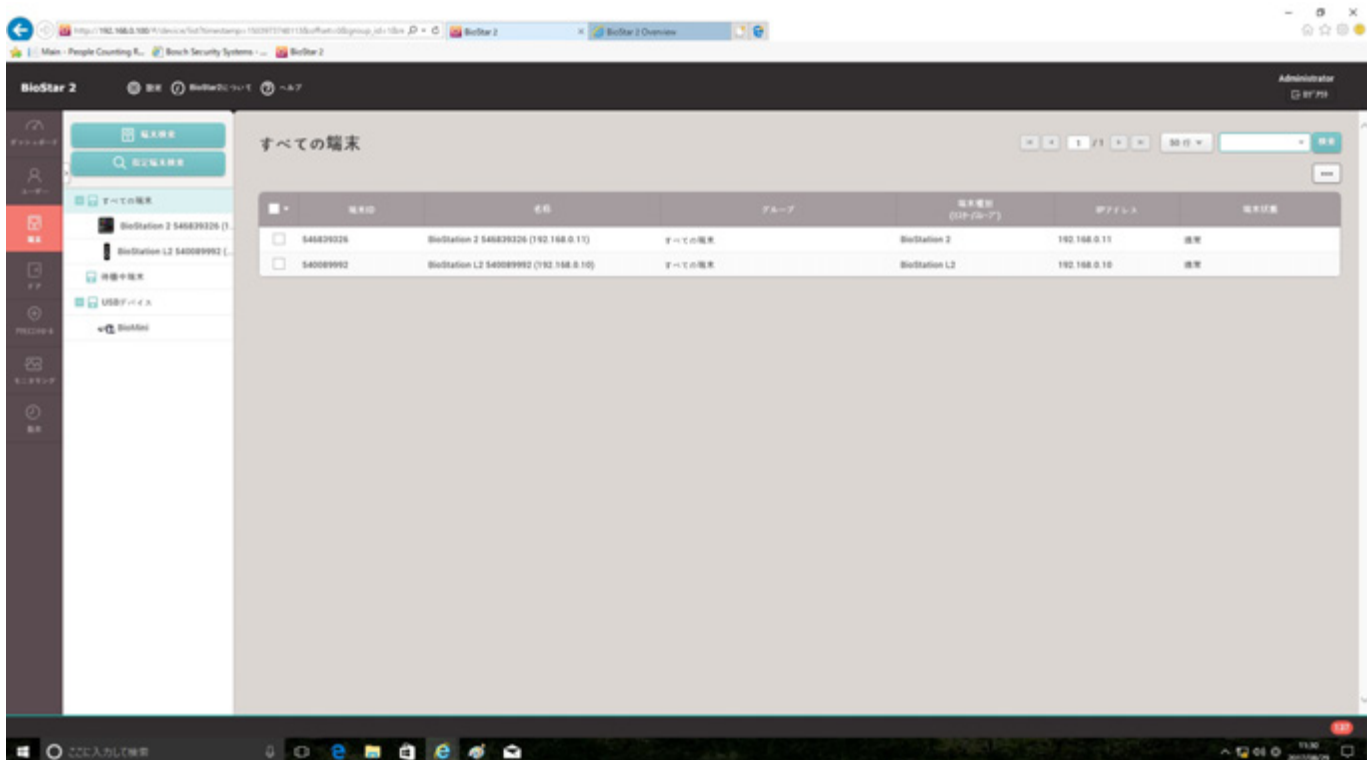


をクリックすると、操作しているドアの警報状態を解除(アラームをクリア)します。



をクリックすると、操作しているアンチパニックドアのリセットをします。

Biostar2.5.0 ベーシックエディションでの 1 ドア用のアンチパスバックの設定



マスター/スレーブとなる 2 台の端末を LAN 接続し Biostar2.5.0 に登録する。
それぞれの端末間の RS-485 を接続する。

【マスター側】のネットワークのシリアル通信設定を“マスター”に設定し、ボーレートを入力する(デフォルトは 115200bps)



【スレーブ側】のネットワークのシリアル通信設定を“スレーブ”に設定し、ボーレートを入力する(デフォルトは 115200bps)

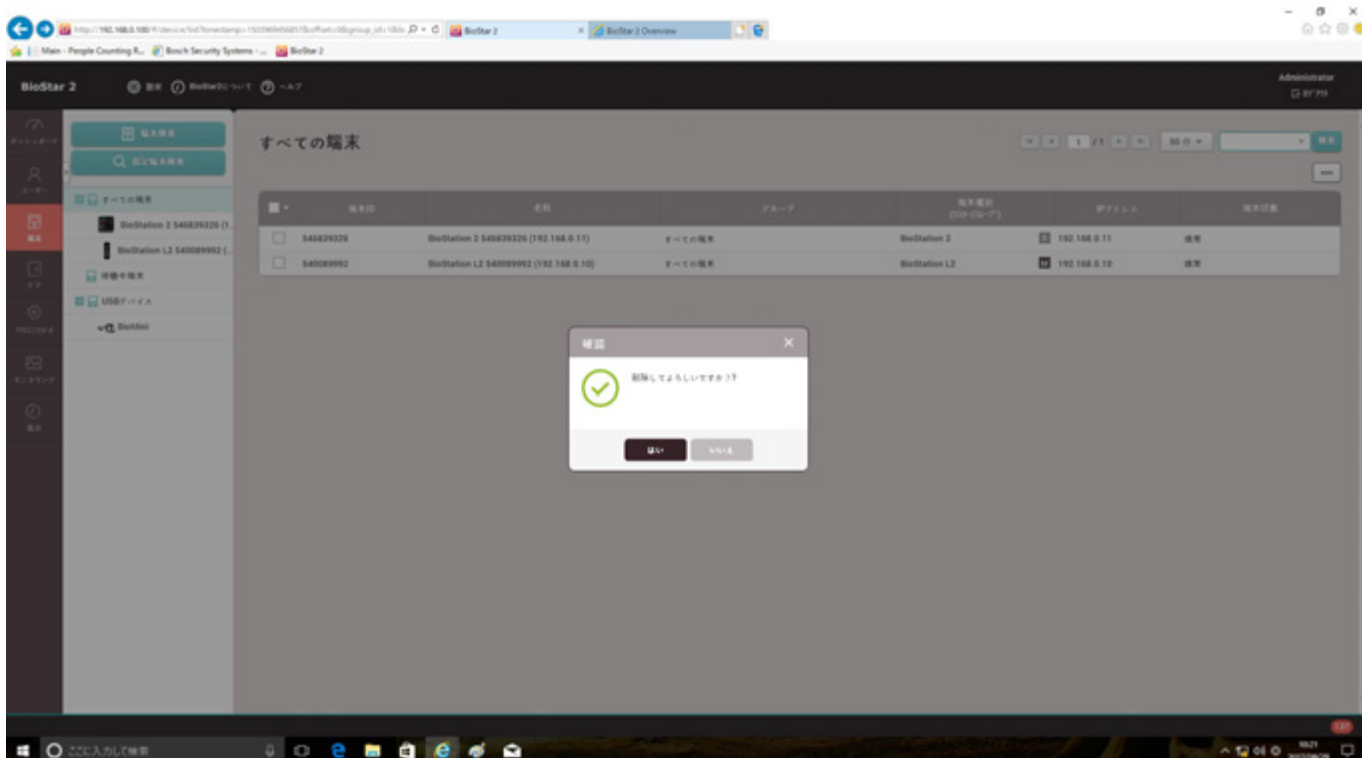


端末ID	名称	グループ	端末種別 (ポート/グループ)	IPアドレス	端末状態
546829326	BioStation 2 546829326 (192.168.0.11)	すべての端末	BioStation 2	192.168.0.11	通常
540089992	BioStation L2 540089992 (192.168.0.10)	すべての端末	BioStation L2	192.168.0.10	通常

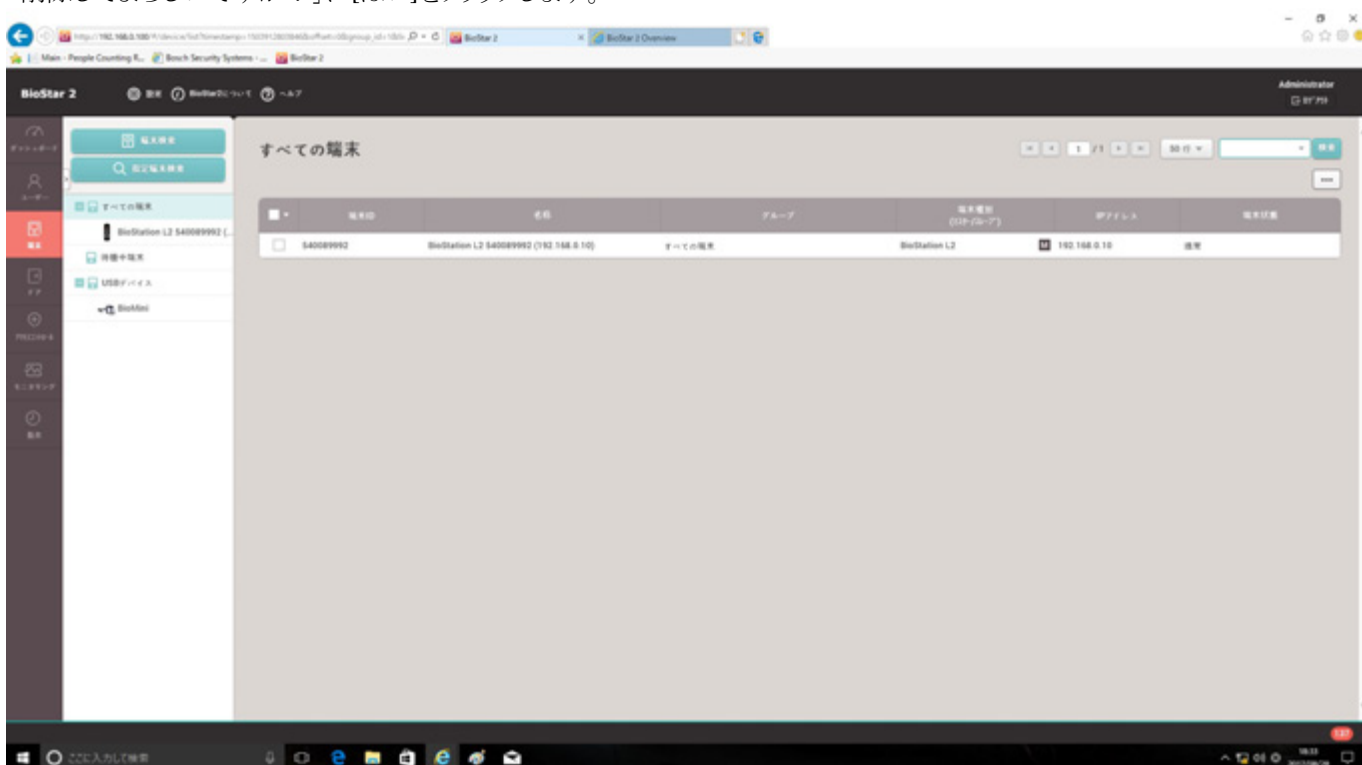
マスターに[M]、スレーブに[S]の表示が付きまます。



スレーブとなる側の端末アイコンの上で右クリックし、“端末を削除”をクリックします。



「削除してよろしいですか?」に[はい]をクリックします。



スレーブ側の端末が削除されました。

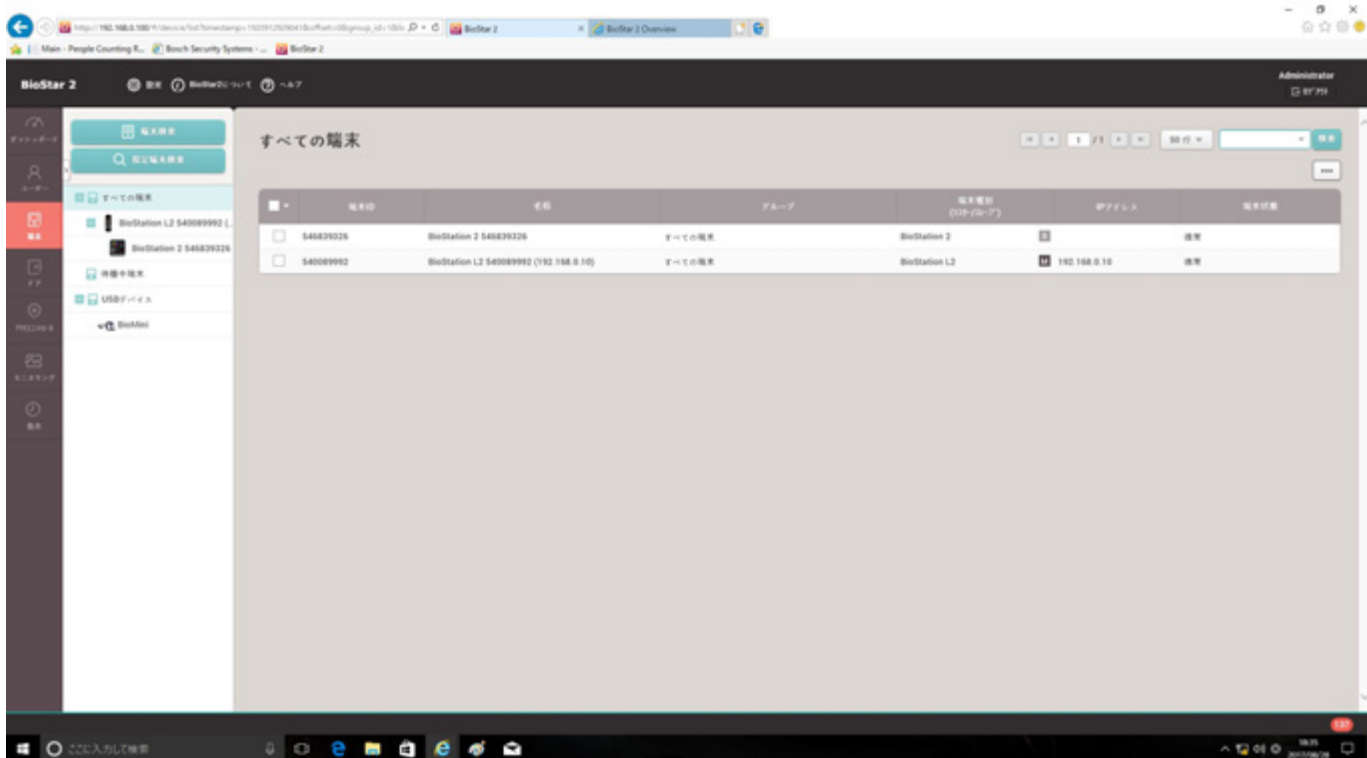


マスターとなる側の端末アイコンの上で右クリックし、“スレーブ端末を検索”をクリックします。

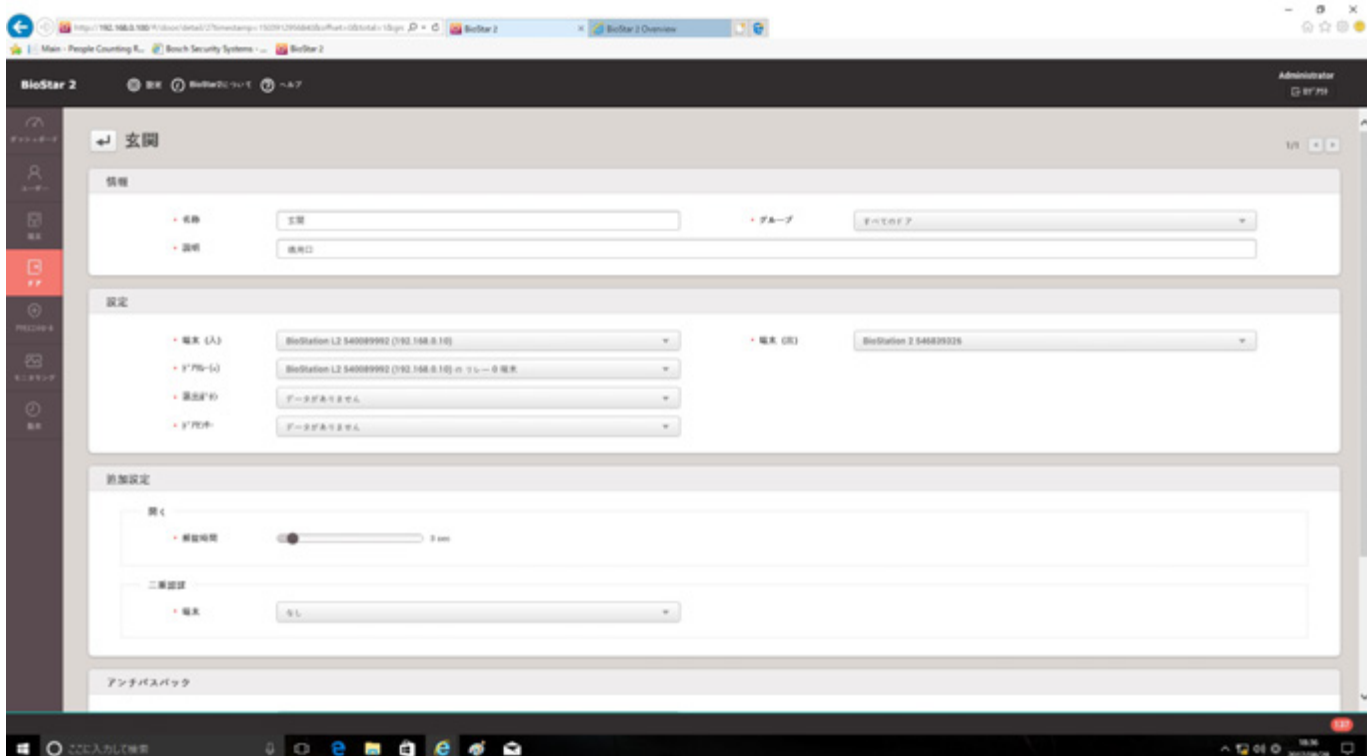


[追加]をクリックします。





スレーブに設定した端末がマスターの配下に入ります。



ドアを選択して、端末(出)にスレーブ端末を指定します。



アンチパズバックに種別を設定します。ハード APB を指定してください。



※通常は工事の時点で設定されているので設定の必要はありません。

適用 をクリックすると、アンチパズバックのドアが作成されます。

二重認証(ユーザーと誰かが一緒に2人で端末認証しないと開かない)の設定



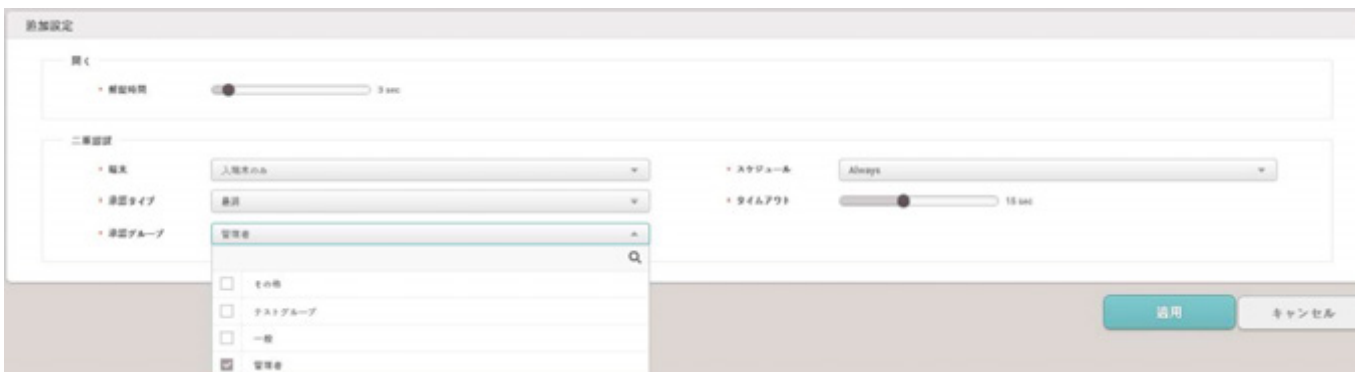
端末は入端末のみが選択できます。出端末のみはアンチパスバックを設定していないと指定できません。



承認タイプは「データがありません」と「最終」が選択できます。

「データがありません」は、アクセスグループに関係なく2人のユーザーと一緒に端末認証すればドアを開けることができます。順序は関係ありません。

「最終」では、入室したいユーザーが端末認証し、後で承認グループに設定のある別のユーザーが端末認証すればドアを開けることができます。



「最後」を指定した場合、承認するアクセスグループを指定することができます。

例えば、これを設定したドアから入室したいユーザーは管理者と一緒になければ端末認証出来ないので入室を制限するような設定が出来ます。

ホールドアップ指紋の設定



誰かに脅されて指紋登録をする場合など、ホールドアップ状態であることを知らせるために、ホールドアップにチェックを入れて登録するとホールドアップ指紋として登録出来ます。
この指紋を使って端末認証すると以下のようにアラームが上がります。



イベントログ

日時	端末ID	端末	ユーザID	ユーザ	内容
2017/08/29 16:02:23	540089992	BioStation L2 540089992 (192.1...			1:F指紋
2017/08/29 16:02:20	540089992	BioStation L2 540089992 (192.1...			1:F指紋
2017/08/29 16:02:20	540089992	BioStation L2 540089992 (192.1...	すべてのユーザ	1 (Administrator)	1:N非顔認証成功 (指紋)

リアルタイムログ

日時	1:F	1:M	端末ID	端末	ユーザ	内容
2017/08/29 16:02:23	実行		540089992	BioStation L2 54...		1:F指紋
2017/08/29 16:02:20			540089992	BioStation L2 54...	1 (Administrator)	1:N非顔認証成功 (指紋)


アラート履歴

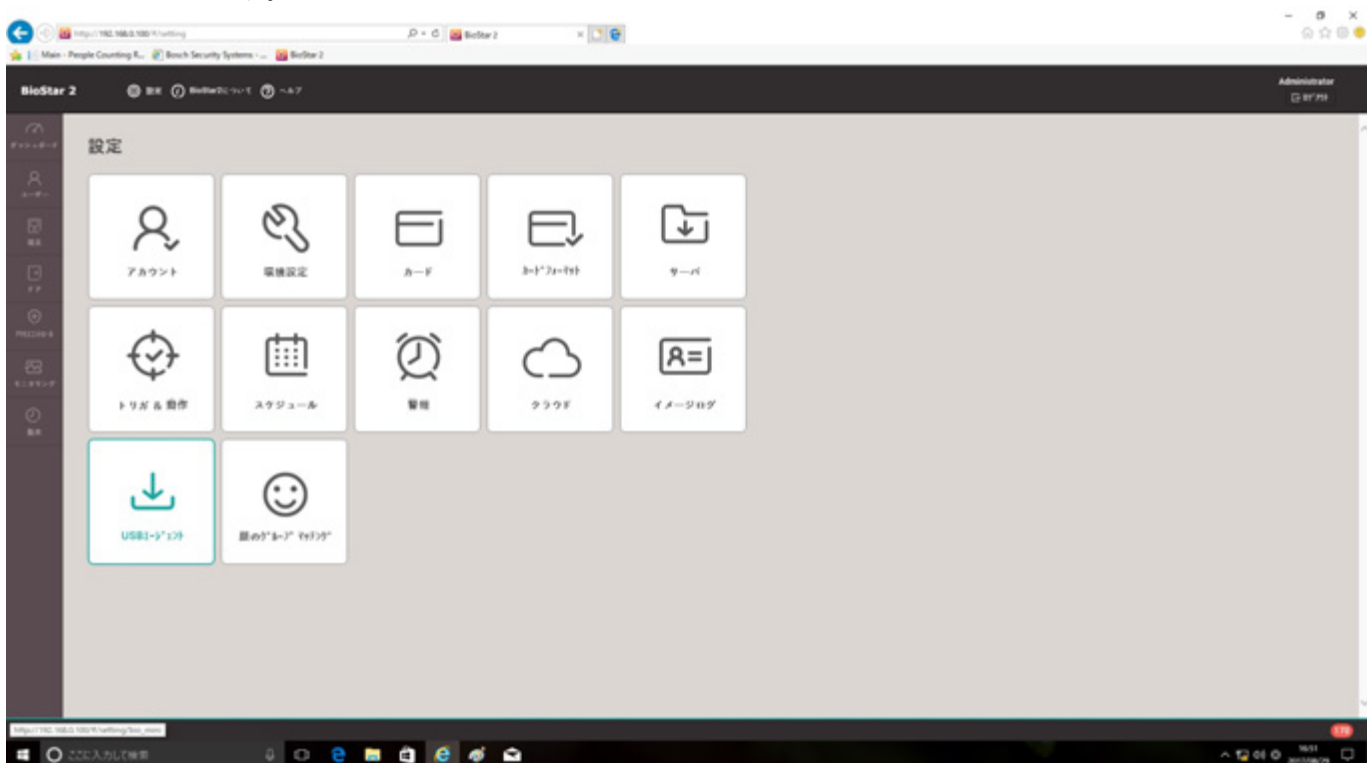
日時	端末	ユーザ	メッセージ	送信者	状態
2017/08/29 16:02:20	BioStation L2 540089992 (192.168...	1 (Administrator)	1:N非顔認証成功 (指紋)	Administrator	

Bio-mini の設定

BioStar2.5.0.203 をインストールした際に、USB Device Agent をインストールしている場合は不要です。



 **設定** をクリックします。



[USB エージェント] をクリックします。



[ダウンロード] をクリックします。



[実行]をクリックします。

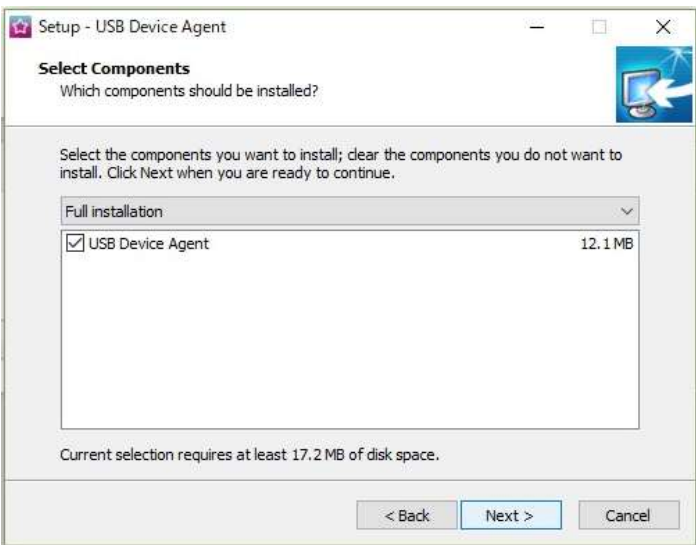


OK

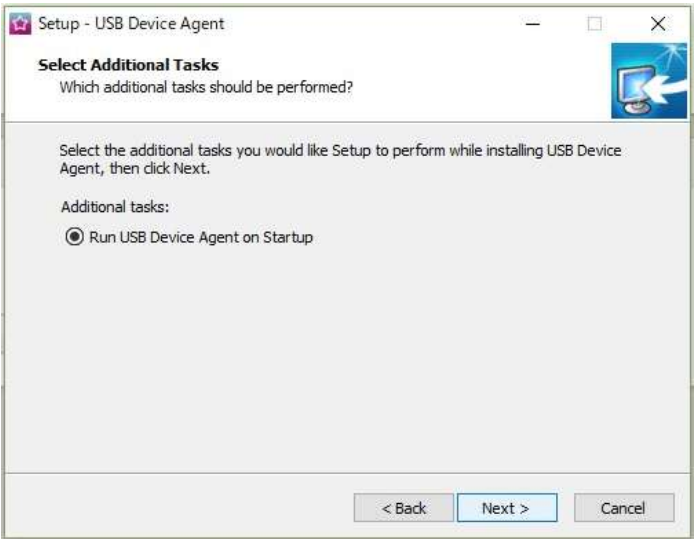
をクリックします。



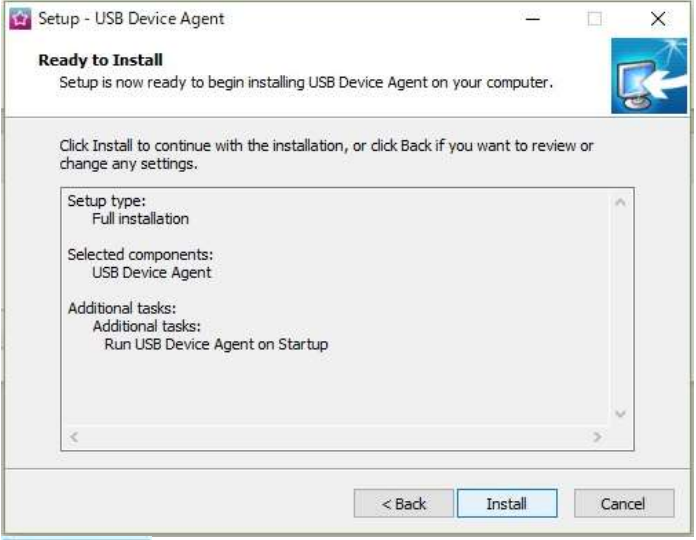
[I accept the agreement]にチェックを入れて **Next >** をクリックします。



Next > をクリックします。



Next > をクリックします。



Install をクリックします。



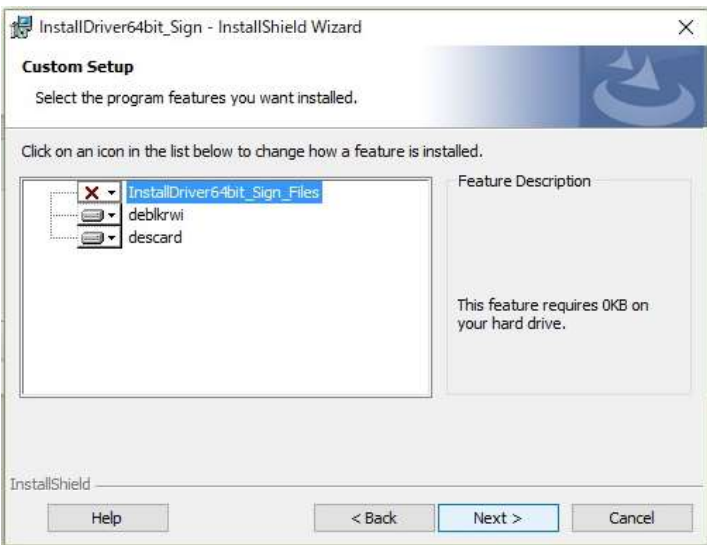
Finish をクリックします。



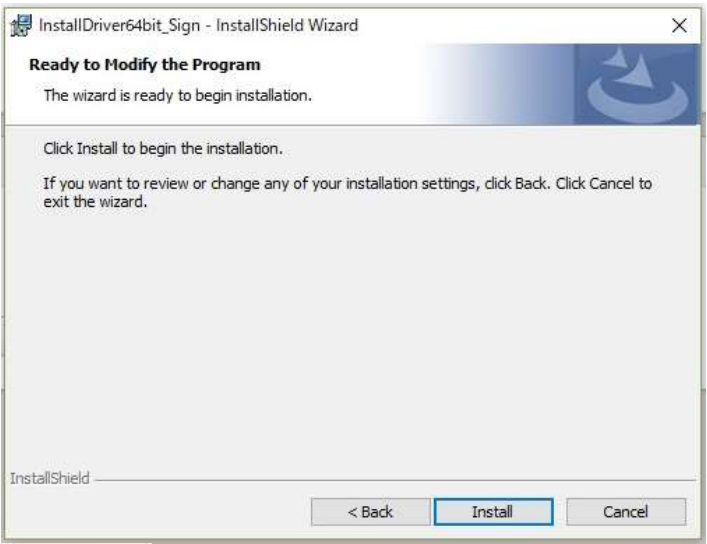
Next > をクリックします。



Next > をクリックします。



Next > をクリックします。

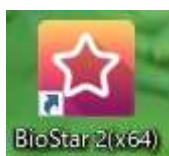


Install をクリックします。



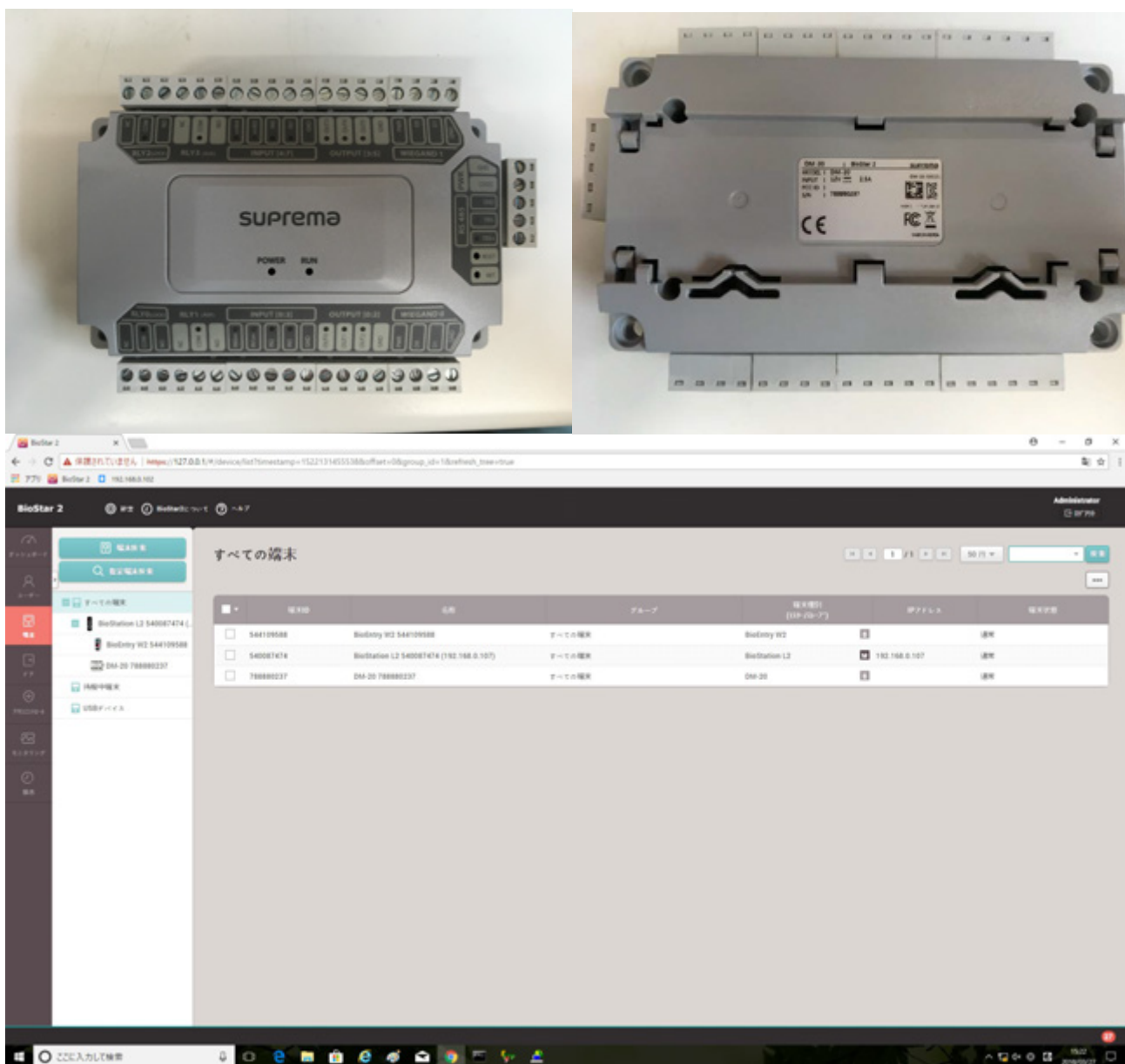
Finish をクリックします。

Bio-mini の USB を PC の USB ポートに挿します。

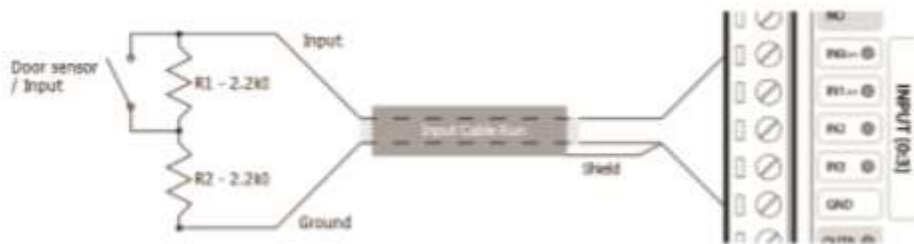
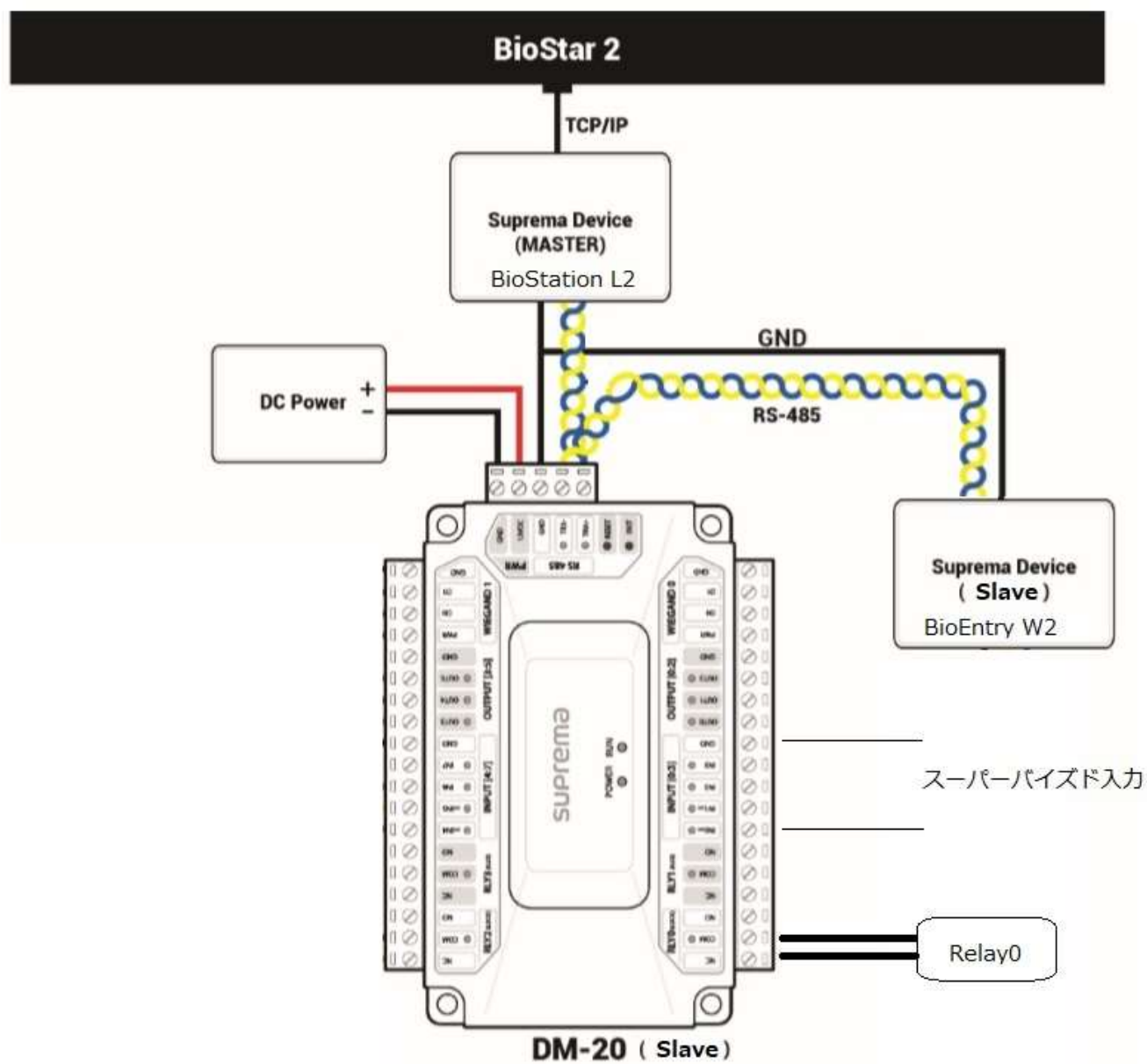


一度、Biostar2.4.1(ブラウザ)を閉じて、再度 BioStar2(x64)をクリックして起動し直します。
端末の USB デバイス欄に BioMini の表示が出ていれば使用可能です。

DM-20 の接続



DM-20 は Master デバイスの配下にて RS485 の Slave デバイスとして認識されます。



State	DM-20 LED Status	Circuit Resistance
ON	Green	2.2 k Ω
OFF	Off	4.4 k Ω
Open	Orange	Infinite k Ω
Short-Circuit	Red	0

[LED Status and Circuit Resistance of DM-20 based on the device's state]

① Note

- You can use the following resistors for the DM-20. 1 k Ω , 2.2 k Ω , 4.7 k Ω , 10 k Ω .



STATE ON (緑)

STATE OFF (消灯)

STATE OPEN (橙)

STATE SHORT (赤)

DM-20 788880237

情報

- 名前: DM-20 788880237
- 機種種別: DM-20
- 製造ID: DM00
- ソフトウェアID: 0.0.0
- 電圧ID: 788880237
- ファームウェアバージョン: 1.1.2
- BIOSバージョン: 0.0.0

拡張登録

キーボード入力

イベント	キーボード	キーボード入力値
0	キーボード入力	2.20
1	キーボード入力	3.00
4	キーボード入力	4.20
5	キーボード入力	180

適用 キャンセル

イベントログ

フィルター: 検索 表示期間: 1日 (2018/03/29 00:00 - 2018/03/29 23:59)

日付	ID	ユーザ	イベント	IP	IPV6	ユーザ
2018/03/29 11:05:27	788880237	DM-20 788880237				177 成功
2018/03/29 11:05:26	788880237	DM-20 788880237				177 成功
2018/03/29 11:05:24	788880237	DM-20 788880237				177 成功
2018/03/29 11:05:22	788880237	DM-20 788880237				177 成功
2018/03/29 11:05:22	540067474	BioStar2 L2 540067474 (192.168.0...	管理者			178 (202/078 (0/0))
2018/03/29 11:05:03	788880237	DM-20 788880237				177 成功
2018/03/29 11:05:03	788880237	DM-20 788880237				177 成功
2018/03/29 11:04:56	788880237	DM-20 788880237				177 成功
2018/03/29 11:04:53	788880237	DM-20 788880237				177 成功
2018/03/29 11:04:50	788880237	DM-20 788880237				177 成功
2018/03/29 11:04:50	540067474	BioStar2 L2 540067474 (192.168.0...	管理者			178 (202/078 (0/0))
2018/03/29 11:03:22	788880237	DM-20 788880237				177 成功
2018/03/29 11:03:20	788880237	DM-20 788880237				177 成功
2018/03/29 11:03:20	788880237	DM-20 788880237				177 成功
2018/03/29 11:03:20	788880237	DM-20 788880237				177 成功
2018/03/29 11:03:19	788880237	DM-20 788880237				177 成功
2018/03/29 11:03:17	788880237	DM-20 788880237				177 成功
2018/03/29 11:03:17	788880237	DM-20 788880237				177 成功
2018/03/29 11:03:17	788880237	DM-20 788880237				177 成功

