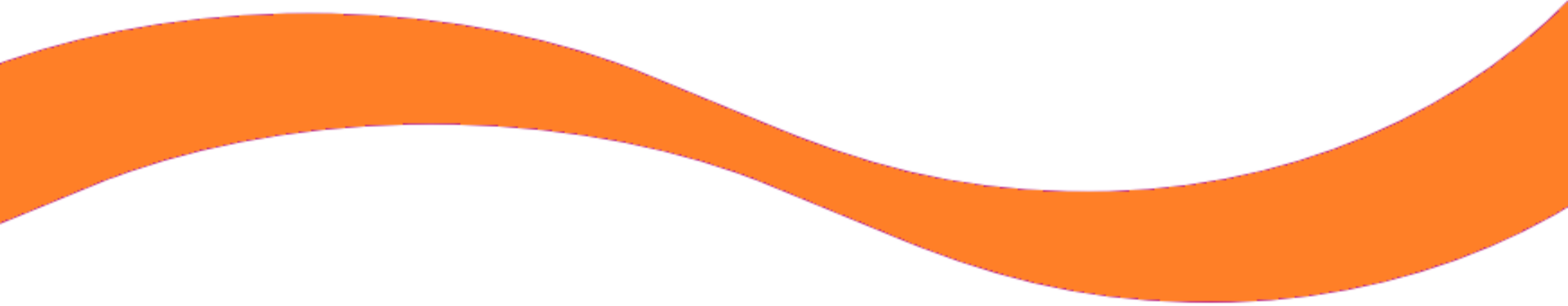


USER GUIDE

SA-FSF2-DB

日本語
Version 1.02

SECURE



目次

安全上の注意	3	日付&時刻 設定	32
はじめに	4	サマータイム設定	33
操作について	4	端末情報	34
基本構成	5	メモリ情報	35
各部の名称	6	USBメモリ	36
各部機能	7	セキュアタンパー	37
ケーブルおよびコネクタ	8	端末再起動	38
正しい顔の登録と認証方法	10	初期設定に戻す	39
管理メニュー	11	ユーザーID種別	40
トップメニュー	11	ログ検索	41
ユーザー情報の登録	12	ログ削除	42
ユーザー情報の編集	15	ログ使用量	43
すべてのユーザーの削除	16	障害報告前のチェックリスト	44
ユーザー使用量の確認	17	製品仕様	45
認証モード	18	製品仕様	45
認証モードの変更	19	寸法	46
認証モードの削除	20		
サーバーマッチング	21		
顔	22		
勤怠モード	26		
表示&音声	27		
ネットワーク設定	28		
サーバー設定	29		
シリアル設定	30		
リレー設定	31		

安全上の注意

- 本製品をご利用頂く方々への危害や損害を未然に防ぐために、本取扱説明書及び取り付け説明書をよくお読みになり、大切に保管し、本製品を正しくお使い下さい。

注意

設置

- ・直射日光や紫外線の下に設置しないでください。製品の破損、誤動作、変色、変形の恐れがあります。
- ・本製品を暖房の近くなど、高温が直接当たる場所に設置しないで下さい。

利用時

- ・本製品を分解・修理・改造しないで下さい。故障の原因となります。万一、分解・改造された場合は、保証対象外となります。
- ・製品を、本取扱説明書で定めた用途以外にはご使用しないで下さい。

警告

設置

- ・外部にケーブル(特に電源ケーブル)をむき出しにしないで下さい。
- ・本製品の近くに磁石を置かないで下さい。又、陰極線管、テレビなどのような磁力を発生させる機器は、本製品の誤作動・故障の原因になりかねますので、避けてください。
- ・Secure I/O2や他の電気錠と、本装置は、独立した電源を利用してください。

利用時

- ・落下すると故障の原因となりますので移動させる際は十分ご注意下さい。
- ・掃除する際、水を直接かけて掃除したり、ベンジン、シンナー、アルコールなどを含ませて拭かないで下さい。感電・故障・火災などの原因になりかねます。

操作について

- パスワードは他人に公開しないように注意して管理し、定期的に変更するようにしてください。
正しく運用されないと、他人に利用されてしまう場合があります。
- 強制的な力や、尖ったものでボタンを押さないでください。
製品の故障が発生します。
- 汚れた手や異物で指紋接触装置を汚染したり、損傷したりしないように注意してください。
指紋認証性能の低下や、製品の故障が発生する可能性があります。
- SA-FSF2-DB は、静電容量式の タッチスクリーンとボタンを利用しています。雨天により湿度が高く湿ったり、製品表面に多量の水がついたりする場合は、使用前に乾いたタオルで拭き取ってください。

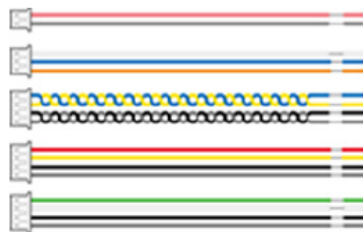
RTCバッテリー

間違った種類のバッテリーに交換すると、爆発の原因となることがあります。
該当する地域 または 国際廃棄規則に従って、バッテリーは廃棄してください。

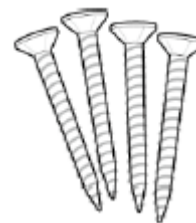
基本構成品



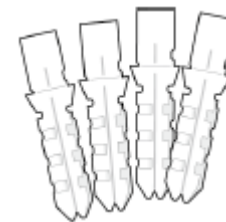
SA-FSF2-DB



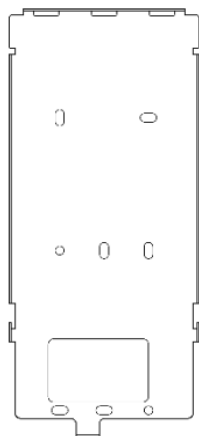
接続ケーブル (5)



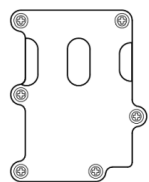
ブラケット固定用ビス (6)



アンカー (6)



ブラケット

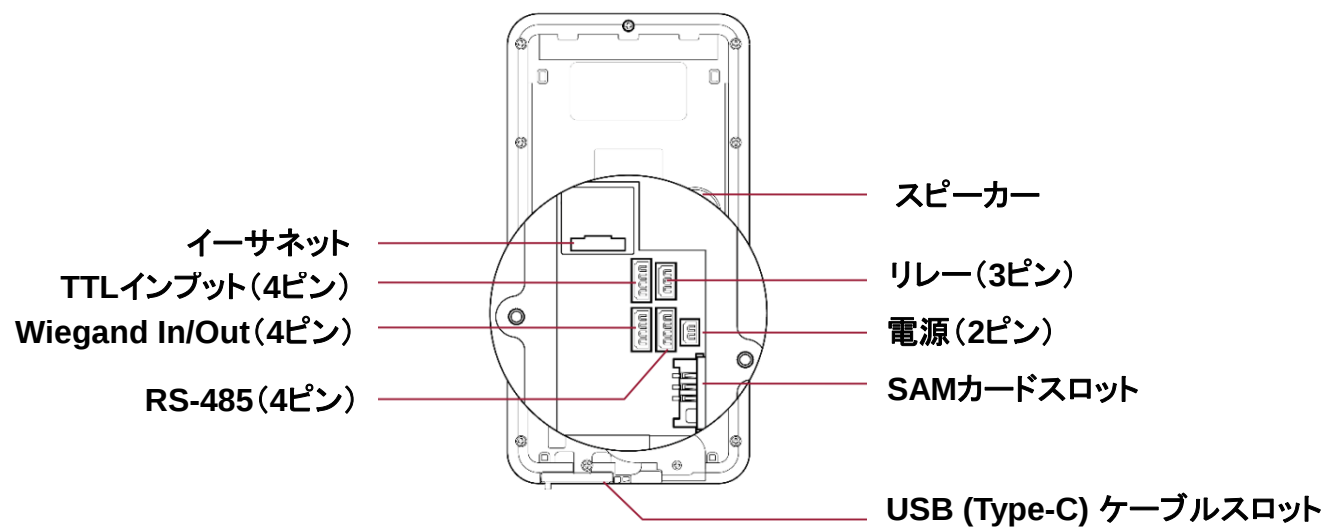
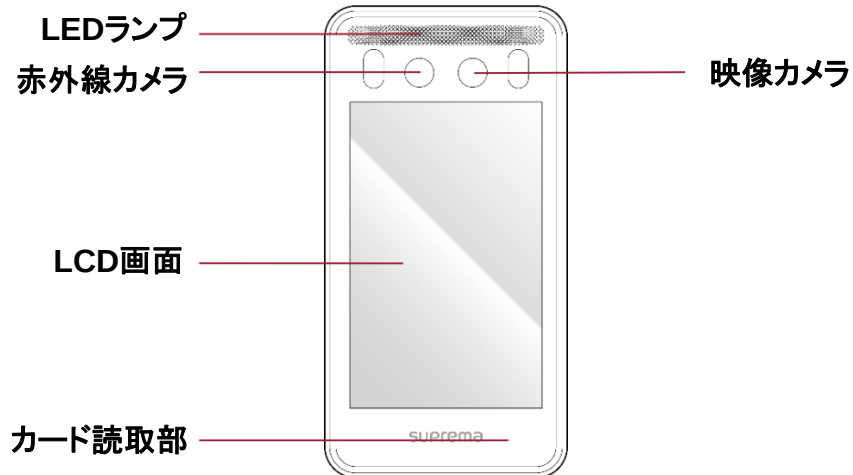


ケーブルカバー

ブラケット
固定ねじ(星形)120Ω 抵抗
(終端抵抗用)

ダイオード

各部の名称



各部機能

名称	機能
LEDランプ	暗い状態で、ユーザーが検出された場合に光ります
赤外線カメラ	赤外線映像イメージをキャプチャします。
映像カメラ	実映像をキャプチャします。
LCD画面	画面確認と操作を行います。
カード読取部	認証に利用するカードを読取ります。
スピーカー	端末の音声を出力します。
イーサネット	イーサネットケーブルを接続します。
TTLインプット(4ピン)	TTLインプットケーブルを接続します
リレー(3ピン)	リレーケーブルを接続します。
Wiegand In/Out(4ピン)	Wiegand インプット および アウトプット ケーブルを接続します。
電源(2ピン)	電源ケーブルを接続します。
RS-485(4ピン)	RS-485ケーブルを接続します。
SAMカードスロット	SAMカードを挿入します。
USB (Type-C) ケーブルスロット	USBケーブルを接続します。

ケーブル 及び コネクタ

電源



ピン番号	名称	色
1	PWR+VDC	赤(白 ストライプ)
2	PWR GND	黒(白 ストライプ)

リレー



ピン番号	名称	色
1	RLY NO	白
2	RLY COM	青
3	RLY NC	橙

RS-485



ピン番号	名称	色
1	485 TRXP	青
2	485 TRXN	黄
3	485 GND	黒
4	SH GND	灰

ケーブル 及び コネクタ

TTLインプット



ピン番号	名称	色
1	TTL IN0	赤
2	TTL IN1	黄
3	TTL GND	黒
4	SH GND	灰

Wiegand インプット 及び アウトプット



ピン番号	名称	色
1	WG D0	緑
2	WG D1	白
3	WG GND	黒
4	SH GND	灰

正しい顔の登録と認証方法

顔登録時の注意事項

- ・顔を登録するときは、端末と顔の距離を 60cm～100cmに保ってください。
- ・表情を変えないように注意してください。
- ・目や眉毛を覆わないように注意してください。
- ・マスクやサングラスは着用しないでください。
- ・画面に2つの顔が入らないように注意してください。(1回に 1人ずつ登録してください。)
- ・画面の指示通りでないと、顔の登録に時間がかかったり、失敗したりする場合があります。

顔認証時の注意事項

- ・顔が端末の画面中央に表示されていることを確認します。
ガイドラインが表示されたら、画面に表示される指示に従ってください。
- ・顔の一部が防止、マスク、眼帯、サングラスで覆われていると認証に失敗する場合があります。端末が眉毛と顔の両方を認識できるように顔を覆わないようにしてください。

トップメニュー

1.  をクリックして、管理者資格レベルで認証してください。
2. 目的のメニューを選択してください。

 Note

管理者が指定されていない場合、 を押すとメニュー画面が表示されます。

ユーザー情報の登録

顔やカードなどのユーザー情報を登録できます。

1.  をクリックして、管理者資格レベルで認証してください。
2. ユーザー を選択し、 をタップし、登録する資格情報を選択します。
ユーザー登録には2つのステップがあります。資格情報が登録された後、いくつかのオプションが利用可能になります。

1 2 ユーザー追加



(名称を入力)

1

 顔  カード  PIN

1 2 ユーザー追加



(名称を入力)

1

 顔  カード  PIN

操作権限 なし

期間 2001/01/01 ~ 2030/12/31

拡張 個別認証モード 未使用

次へ

保存

ユーザー情報の登録

- ・  : ユーザーの画像を設定します。
- ・ ユーザー名 : ユーザー名を入力してください。(アルファベットのみ)
- ・ ID : 1~429467295までの数字を入力して、ユーザーIDとして登録します。
ユーザーIDタイプが英数字に設定されている場合、英数字と記号(_、-)の組み合わせをIDに使用できます。
最大32文字まで入力できます。
- ・ 顔 : ユーザー認証用の顔を登録します。「顔」>「次へ」を押して、画面の指示に従って顔を登録します。
追加で顔を追加するには、 を押します。顔の登録の詳細については、「正しい顔の登録と認証方法」を参照してください。
- ・ カード : ユーザー認証用のカードを登録します。「カード」>「次へ」を押して、ユーザーに割り当てるカードをスキャンします。追加のカードを登録するには、 を押します。
- ・ PIN : 使用したいPINを入力してください。確認のために同じPINを再入力します。漏洩を防ぐために、4~16桁の数字を入力してください。
- ・ 操作権限 : ユーザーに割り当てるレベルを選択します。

Note

利用できるメニューは、設定した操作権限レベルによって異なります。

- ・ なし : これは一般的なユーザーレベルです。メニューにアクセスできません。
- ・ 管理者 : すべてのメニューにアクセスできます。
- ・ 設定管理者 : 認証、表示と音声、端末、ネットワーク、イベントログのメニューにアクセスできます。
- ・ ユーザー管理者 : ユーザーおよびイベントログメニューにアクセスできます。

- ・ 期間 : ユーザーアカウントを使用するための有効期限を設定します。
- ・ 拡張個別認証モード : ユーザーに応じて認証方法を変更可能です。拡張個別認証モードを使用するかどうかを設定が可能です。このモードでは、顔を含むユーザーの認証方法を組み合わせることができます。それ以外の場合は、端末の基本認証モードを使用できます。BioStar から変更できます

3. 保存するために、OKをタップしてください。

ユーザー情報の登録

顔の登録

1.  をクリックして、管理者資格レベルで認証してください。
2. ユーザー を選択し、 をタップしてください。
3.  顔を選択し、「次へ」をタップしてください。
4. 顔と画面の間の距離を調整し、端末のカメラをまっすぐ見ます。
5. 顔が正常にキャプチャされたら、[OK]> [保存]を押します。
写真を撮り直すには、[再撮影]を押します。

Note

- ・顔を登録するときは、端末と顔の距離を60cmから100cmに保ってください。
- ・表情を変えないように注意してください。
- ・目や眉毛を覆わないように注意してください。
- ・マスクやサングラスは着用しないでください。
- ・画面に2つの顔を表示しないように注意してください。一度に1人ずつ登録してください。
- ・画面の指示に従わないと、顔の登録に時間がかかったり、失敗したりする場合があります。

ユーザー情報の編集

ユーザー管理者または管理者は、登録済みのユーザー情報を変更可能です。
ユーザーの顔やカードを追加したり、PINとレベルを変更したりなど編集可能です。

1.  をクリックして、管理者資格レベルで認証してください。
2. ユーザー を選択し、 をタップしてください。
3. 検索パターンを選択します。すべて、ユーザーID、名前、顔、カードで、ユーザーを検索できます。
4. 検索結果から、編集したいユーザーを選択します。
5. 「ユーザー情報の登録」を参照して情報を変更し、「OK」を押します。
ユーザーを削除する場合は、 を選択して、「OK」を押します。

Note

アクセスグループはBioStar2を利用して登録できます。
アクセスグループの登録の詳細については、BioStar2 マニュアルを参照してください。

すべてのユーザーの削除

登録されている全ユーザーをすぐに削除することも可能です。

1.  をクリックして、管理者資格レベルで認証してください。
2. ユーザー を選択し、 をタップしてください。
3. [すべて削除]に☒をし、[OK]を押します。
4. 確認画面が表示されます。更に、[OK]を押すと、全ユーザーが削除されます。
Click to add text

ユーザー使用量の確認

登録ユーザー数、顔数、カード数が一目でわかります。

1.  をクリックして、管理者資格レベルで認証してください。
2. ユーザー を選択し、 をタップしてください。 ユーザー使用量情報が表示されます。



認証モード

認証モードを設定します。顔/PIN/カード/IDの組み合わせや、スケジュールも設定可能です。
【認証モードの登録】

1.  をクリックして、管理者資格レベルで認証してください。
2. 認証 > 認証モード を選択し、 をタップしてください。
3. + をタップして、使用したいモードを選択してください。追加するには、この手順を繰り返してください。
4. スケジュールをタップして、スケジュールを選択してください。

Note

- ・選択した認証モードを組み合わせですべてを順番に認証することも、選択した認証モードの一部のみを組み合わせで認証することも可能です。
たとえば、認証モードを  +  +  と組み合わせる場合、ユーザーはカード、顔、およびPINを認証する必要があり、認証モードを  +  /  と組み合わせる場合、ユーザーは最初にカードと顔またはPINを認証します。
- ・BioStar2 でスケジュールを設定できます。事前設定されたスケジュールがない場合は、[常に]のみを選択できます。
- ・スケジュールの設定に関する詳細な内容については、BioStar2 マニュアルを参照してください。

5. OK をタップして設定を保存します。

認証モードの変更

認証方法を変更することができます。

1.  をクリックして、管理者資格レベルで認証してください。
2. 認証 > 認証モード を選択してください。
3. 変更する認証モードを選択します。
4. 「認証モードの登録」を参照して認証モードを変更し、「OK」を押します

認証モードの削除

認証方法を削除することができます。

1.  をクリックして、管理者資格レベルで認証してください。
2. 認証 > 認証モード を選択してください。
3.  を押して、削除する認証モードを選択します。複数の項目を選択できます。
4. 「OK」を押して、確認画面が表示されたら、更に「OK」を押します。

サーバーマッチング

サーバーマッチングを設定できます。端末ではなく、BioStar2側で ユーザー認証マッチングが実行されます。端末にユーザー情報が多い場合や、端末が部屋外に設置されている場合に使用すると有効です。

1.  をクリックして、管理者資格レベルで認証してください。
2. 認証 > 認証モード を選択し、サーバーマッチングを有効にしてください。

Note

- ・カードとユーザーIDの認証の場合にのみ利用可能です。
(顔認証の場合は利用できません。)
- ・サーバーマッチングオプションを使用する場合は、Biostar2 と端末の両方で、アクティブ化する必要があります。BioStar 2で、サーバーマッチング設定を設定する方法については、BioStar2のマニュアルを参照してください。

顔

顔認証についての設定を変更することが可能です。

1.  をクリックして、管理者資格レベルで認証してください。
2. 認証 > 顔 を選択してください。
3. 目的の項目を選択し、設定してください。

- ・周囲の明るさ: 周囲の明るさを検出し、赤外線LEDの強度を調整します。
設置環境に応じて設定を変更してください。
- ・モーションセンサー感度: 端末の近くの動きを検出するための感度を設定します。
モーションセンサーが オフ に設定されている場合は、液晶画面をタッチしてから顔を認証します。
- ・登録タイムアウト: 設定時間内に顔が登録されない場合、顔の登録をキャンセルします。
- ・認証タイムアウト: 設定時間内に認証が完了しない場合、認証を失敗とします。
- ・重複チェック: 顔を登録するときに、重複を確認できます。
- ・顔検出設定: 検出領域のサイズと位置を調整して、顔認識領域を設定します。

Note

顔検出設定のオプションのデフォルト値を維持することをお勧めします。
各オプションのデフォルト値は次のとおりです。

- ・最大顔回転角度: 15
- ・最小顔幅: 66
- ・最大顔幅: 250
- ・顔認識領域の開始位置: 144
- ・顔認識領域の幅: 432

- ・セキュリティレベル: 1: N認証のセキュリティレベルを設定します。



顔

- ・動作モード: 1:N認証のセキュリティレベルを設定します。
 - フュージョンマッチング: 顔認証の精度を上げる為に、視覚カメラと赤外線カメラの両方を使用します。
 - ウォークスルー: 端末は、認証距離内で一時停止することなく認証地点を通過するユーザーを判定します。
- ・偽造顔検出: 写真などの偽の顔を使用した利用者認証を防止します。動作モードがフュージョンマッチングに設定されている場合に使用できます。
- ・詳細設定: マスク検出、赤外線カメラなどの顔認識の設定を行います。
 - 検温モード: 認証と検温の順番を設定できます。
 - 温度警告音: 利用者がマスクを着用していない時、または測定された温度が事前設定された基準温度よりも高い時に、警告音を鳴らします。
 - マスク検出: マスク検出モードを設定して、ユーザーがマスクを着用しているかどうかを検出します。
[使用(該当時 アクセス拒否)]を選択すると、マスクを着用していない利用者の認証が拒否され、イベントログが保存されます。
[使用(該当時 ログ記録し、アクセス可)]を選択すると、マスクを着用していない利用者は認証することができ、イベントログを保存します。
 - サーマルカメラ: サーマルカメラのオプションを設定します。
[使用(該当時 アクセス拒否)]を選択すると、事前設定された基準温度よりも高い温度の利用者の認証が拒否され、イベントログを保存します。
[使用(該当時 ログ記録し、アクセス可)]を選択すると、事前設定された基準温度よりも高い温度のユーザーは、認証するでき、イベントログを保存されます。

Note

- ・マスク検出 または サーマルカメラが、有効になっている時は、使用法に応じて、検温モードを設定します。
 - 認証処理後に検温: 認証が成功した後の温度を測定します。
 - 検温後に認証処理: 利用者が事前設定された基準温度を超過していない場合にのみ認証します。
このモードが有効になっている場合、利用者の温度が基準温度を超えていることが検出されると、ユーザーのIDの認証は、行われません。
 - 検温のみ: 認証なしで温度を検出します。
このモードでは、事前設定された基準温度の範囲内の利用者が、IDやアクセス権を確認せずにアクセス可能です。
(基準温度内なら未登録のユーザーでもアクセス可能です。)

顔

 Note

- ・マスク検出 または サーマルカメラが、有効になっている時は、使用法に応じて、検温モードを設定します。
 - 認証処理後に検温: 認証が成功した後の温度を測定します。
 - 検温後に認証処理: 利用者が事前設定された基準温度を超過していない場合にのみ認証します。
このモードが有効になっている場合、利用者の温度が基準温度を超えていることが検出されると、ユーザーのIDの認証は、行われません。
 - 検温のみ: 認証なしで温度を検出します。
このモードでは、事前設定された基準温度の範囲内の利用者が、IDやアクセス権を確認せずにアクセス可能です。
(基準温度内なら未登録のユーザーでもアクセス可能です。)
- ・サーマルカメラを有効にすると、詳細設定を行うことができます。
 - 摂氏/華氏: 温度の単位を変更します。
 - 基準温度: アクセスを制限する基準温度を設定します。
基準温度を超えていることが検出された利用者は、サーマルカメラの設定によっては、アクセスを拒否されます。
 - 温度のログ記録: 温度データを保存します。有効にすると、認証ログと温度ログの両方が保存されます。無効にすると、
認証ログのみが保存されます。
 - 温度映像表示: 端末の画面に赤外線画像を表示します。
 - 光源自動補正 (ROI): 端末の近くに周囲光源がある場合、赤外線カメラが被写体の温度を誤って測定する可能性があります。
温度を自動的に測定し、周囲の光源温度を検出しないようにサーマルカメラを設定できます。
 - カメラ構成: 正確な測定のためにサーマルカメラ設定を構成します。
- ・サーマルカメラを有効にすると、環境に応じて正確に測定できるようにサーマルカメラの設定を構成できます。
 - 温度測定距離(cm): 利用者と端末の距離を設定します。
 - 赤外線放射率: 利用者の温度を正確に測定するように放射率を設定します。
 - 対象領域(ROI)のX方向(%) / 対象領域(ROI)のY方向(%) / 対象領域(ROI)の幅(%) / 対象領域(ROI)の高さ(%):
端末の視野に光源がある場合、目的の被写体の代わりにそれらが検出される場合があります。ROI(対象領域)の
サイズと位置を調整して、温度測定領域を設定します。
 - 温度補正: サーマルカメラを設定して、周囲条件を自動的に測定する温度値を調整の有効/無効を設定できます。
 - 補正温度: 温度補正を有効にした場合、補正値を設定できます。

顔

 Note

・最高のパフォーマンスを得るには、カメラ構成設定の初期値を設定いただくことをお勧めします。

各設定値の初期値は次のとおりです。

- 温度測定距離(cm) : 100
- 赤外線放射率 : 0.98
- 対象領域(ROI)のX方向(%) : 30
- 対象領域(ROI)のY方向(%) : 25
- 対象領域(ROI)の幅(%) : 50
- 対象領域(ROI)の高さ(%) : 55

・サポートされているサーマルカメラはTCM10-FSF2です。

勤怠モード

勤怠モードの登録方法を設定できます。

1.  をクリックして、管理者資格レベルで認証してください。
2. 認証 > 勤怠 を選択してください。
3. 目的の項目を選択し、設定してください。

- ・勤怠モード: 勤怠モードを使用する方法を選択します。
- ・勤怠コード: 勤怠イベントを登録できます。勤怠コード >  を選択して、勤怠イベントを登録し、アイコン / 勤怠イベント名 / スケジュールを設定します。
- ・勤怠 必須: 認証時に利用者が、勤怠イベントを選択するように設定します。
勤怠イベントを選択するまで、認証してもドアの鍵が開きません。
- ・固定勤怠キー: 管理者が選択した勤怠イベントが固定で使用されるように設定します。
このオプションは、勤怠モードで、[固定] を選択した場合に、設定できるようになります。
- ・ジョブコード: ジョブコードを利用するかどうか？が選択できますが、
ジョブコードは別のシステム用の機能のため、弊社では、
利用できません。

 勤怠

勤怠 モード	ユーザー操作
勤怠 コード	1
勤怠 必須	☒
ジョブコード	☐



表示 & 音声

端末の 表示と音声の設定を変更することができます。

1.  をクリックして、管理者資格レベルで認証してください。
2. 表示 & 音声 を選択してください。
3. 目的の項目を選択し、設定してください。

- ・ホーム画面: ホーム画面の背景に表示する項目を選択します。
- ・言語: 使用する言語を設定します。
- ・端末個別メッセージ: 利用者が認証した時に、画面に表示される個別メッセージを使用するかどうかを設定します。
SDK利用時に、端末にプライベートメッセージを設定できます。
- ・サーバー個別メッセージ: 利用者が認証した時に、画面に表示される個別メッセージを使用するかどうかを設定します。
WEB API利用時に、端末にサーバープライベートメッセージを設定できます。
端末で、サーバー個別メッセージの設定が有効になっていたとしてもサーバーでメッセージを設定していない場合、画面に表示しません。
- ・メニュータイムアウト: メニュー画面が自動的に消える時間(秒単位)を設定します。
設定時間内にボタン入力がない場合は、ホーム画面に戻ります。
- ・メッセージタイムアウト: 設定完了メッセージまたは情報メッセージが自動的に消えるまでの時間(秒単位)を設定します。
- ・バックライトタイムアウト: LCD画面の照明を自動的にオフにする時間(秒単位)を設定します。
- ・音声案内: アラーム音の代わりに音声案内を使用するように設定します。
- ・音量: 音量を 10段階で設定可能です。



ネットワーク設定

端末の ネットワーク の設定を変更することができます。
【イーサネット】

1.  をクリックして、管理者資格レベルで認証してください。
2. ネットワーク > イーサネット を選択してください。
3. 目的の項目を選択し、設定してください。

- ・DHCP: DHCPを使用するかどうかを設定します。
DHCP設定が無効になっている場合、IPアドレス、ゲートウェイ、サブネットマスク、およびDNSを変更できます。
- ・端末ポート: 端末の接続ポート番号を変更できます。
- ・IPアドレス: 端末のIPアドレスを表示します。
DHCP設定が無効の場合に変更可能です。
- ・ゲートウェイ: 端末のゲートウェイを表示します。
DHCP設定が無効の場合に変更可能です。
- ・サブネットマスク: 端末のサブネットマスクを表示します。
DHCP設定が無効の場合に変更可能です。
- ・DNS: DNSサーバアドレスを設定します。

4. OK をタップして設定を保存します。



← イーサネット OK	
TCP/IP	
DHCP	☒
端末 ポート	51211
IP アドレス	192.168.14.201
ゲートウェイ	192.168.14.1
サブネットマスク	255.255.255.0
DNS	192.168.0.1

サーバー設定

1.  をクリックして、管理者資格レベルで認証してください。

2. ネットワーク > サーバー を選択してください。

3. 目的の項目を選択し、設定してください。

- ・端末 -> サーバー: 入力情報を使用して、端末からサーバーに接続信号を直接送信できます。[サーバー]-> [端末]を選択すると、サーバーIP、サーバーURL、サーバーポートを入力できません。
- ・サーバーIP: BioStar2がインストールされているPCのIPアドレスを入力します。入力は、[端末]-> [サーバー] が接続モードに設定されている場合にのみ受け入れられます。
- ・サーバーURL: サーバーIPの代わりに、サーバーURLを入力します。入力は、[端末]-> [サーバー] が接続モードに設定されている場合にのみ受け入れられます。
- ・サーバーポート: BioStar2 がインストールされているPCのポートを入力します。入力は、[デバイス]-> [サーバー] が接続モードに設定されている場合にのみ受け入れられます。

4. OK をタップして設定を保存します。



← サーバー編集 OK

端末 -> サーバー ☒

サーバーIP IPアドレスを入力

サーバーURL URLを入力

サーバーポート 51212

シリアル設定

1.  をクリックして、管理者資格レベルで認証してください。
2. ネットワーク を選択してください。
3. 目的の項目を選択し、設定してください。
 - ・RS-485: RS-485 のモードを選択します。
 - ・ボーレート: 目的のボーレートを選択します。
4. OK をタップして設定を保存します。

シリアル設定

RS-485

初期値

ボーレート

115200

リレー 設定

端末の リレー作動時間 と 退出ボタンの入力ポートを設定できます。

1.  をクリックして、管理者資格レベルで認証してください。
2. 端末 > リレー を選択してください。
3. 目的の項目を選択し、設定してください。

- ・リレー: リレーを有効にするかどうかを設定できます。
作動時間 と 退出ボタンの入力ポートを設定するには、このオプションを有効にする必要があります。
- ・作動時間: ユーザー認証が実行された時に、リレースイッチが動作する
(鍵が開いている)時間を設定します。
- ・退出ボタン: 退出ボタンが接続されている入力ポートを選択します。
(退出ボタンを物理的に接続する配線のチャンネルを選択してください。)



リレー	☒
作動時間	3秒
退出ボタン	未使用



日付 & 時刻 設定

日付と時刻を設定できます。正確なログデータを収集するために、日付と時刻を正確に設定してください。

1.  をクリックして、管理者資格レベルで認証してください。
2. 端末 > 日付 & 時刻 を選択してください。
3. 目的の項目を選択し、設定してください。

- ・日時: 現在の日付と時刻を確認してください。
手動で変更するには、時刻同期を無効にします。
- ・タイムゾーン設定: 現在地の時間基準を設定します。(日本の場合: UTC +09:00)
- ・時刻同期: サーバーと時刻を同期することができます。
- ・日付フォーマット: 日付形式を設定します。YYYY/MM/DD か MM/DD/YYYY か、DD/MM/YYYY から選択できます。
- ・時刻フォーマット: 時間形式を設定します。24時間 表示 または AM / PM 表示のいずれかを選択できます。

←
日時

日時	2020/08/27 AM 05:09:48
タイムゾーン設定	UTC
時刻同期	☒
フォーマット	
日付フォーマット	YYYY/MM/DD
時刻フォーマット	AM/PM

◀
🏠
☰

サマータイム 設定

端末にサマータイムを適用することができます。
開始時刻と終了時刻を正しく設定してください。

1.  をクリックして、管理者資格レベルで認証してください。
2. 端末 > サマータイム を選択し、 を押してサマータイムを追加します。
3. 目的の項目を選択し、設定してください。
 - ・名称: サマータイムの名称を設定してください。
 - ・開始月/開始週/開始日/開始時間:
サマータイムの開始の詳細を設定してください。
 - ・終了月/終了週/終了日/終了時間:
サマータイムの終了の詳細を設定してください。
4. OK をタップして設定を保存します。

← サマータイム追加 OK	
名称	サマータイム1
開始月	1月
開始週	1週
開始曜日	日曜
開始時間	00:00
終了月	1月
終了週	1週
終了曜日	日曜
終了時間	00:00

端末情報

モデル名、端末ID、シリアル番号、ファームウェアバージョン、およびMACアドレスを確認できます。

1.  をクリックして、管理者資格レベルで認証してください。
2. 端末 > 端末情報 を選択してください。
モデル名、端末ID、シリアル番号、ハードウェア、FW、カーネル、MACなどの情報を表示します。

メモリ情報

メモリ使用量の状態を表示します。

1.  をクリックして、管理者資格レベルで認証してください。
2. 端末 > メモリ情報 を選択してください。
端末のメモリ使用量を表示します。



USB メモリ

USBメモリを接続して、以下の用途に利用できます。

- ・利用者情報を端末にインポートする
- ・ログと利用者情報を端末からエクスポートする
- ・ファームウェアをアップグレードする

1.  をクリックして、管理者資格レベルで認証してください。

2. 端末 > USB メモリ を選択してください。

3. 目的の項目を選択し、設定してください。

- ・インポート: 接続したUSBメモリから、利用者情報をインポートします。
- ・エクスポート: エクスポートしたい利用者情報を接続したUSBメモリにエクスポートします。
- ・ファームウェアアップグレード: USBメモリにファームウェアファイルを格納し、ファームウェアをアップデートすることができます。

 Note

サポートされているUSBメモリの種類は次のとおりです。異なるUSBメモリを使用すると、正しく動作しない場合があります。

- ・ Samsung Electronics: SUM-LSB 8GB, SUM-PSB 8GB, SUM-PSB 16GB, SUM-BSG 32GB
- ・ LG Electronics: XTICK J3 WINDY 8GB, SMART USB MU1 White 8GB, MU 1 USB 32GB, MU28GBC 32GB, XTICK MOBY J1 16GB
- ・ SanDisk: Cruzer 16GB, Cruzer Blade CZ50 4GB, Cruzer Blade CZ50 32GB, CZ48 Ultra USB 3.0 64GB, CZ80 USB3.0 64GB, CZ52 64GB, Cruzer Glide Z60 128GB, Cruzer Force CZ71 32GB
- ・ Sony: Micro Vault Click 8GB, MicroVault CLICK 16GB, USM-SA1 32GB
- ・ Transcend: JetFlash 760 8GB, JetFlash 760 32GB, JetFlash 500 8GB
- ・ Memorette: MINI500 8GB
- ・ A-DATA: S102 PRO 8GB
- ・ Trigem Pastel 8GB

← USB メモリ	
インポート	>
エクスポート	>
ファームウェア アップグレード	>



セキュア タンパー

セキュアタンパーを利用すると、端末が取りはずされた時に、端末内 利用者データ, ログを削除することができます。

1.  をクリックして、管理者資格レベルで認証してください。
2. 端末 を選択してください。
3. セキュア タンパー を有効にすると、タンパー イベントが発生した時(端末が背面ブラケットから取り外された時)に、登録利用者情報、すべてのログが削除されます。

端末再起動

端末を再起動することができます。

1.  をクリックして、管理者資格レベルで認証してください。
2. 端末 > 端末再起動 を選択してください。
3. 「OK」を押して、確認画面が表示されたら、更に「OK」を押します。

初期設定に戻す

端末設定、ネットワーク設定、および管理者レベルを初期化します。

1.  をクリックして、管理者資格レベルで認証してください。

2. 端末 > 初期設定に戻す を選択してください。

- ・すべての設定: 端末のすべての設定をリセットします。OK を押すと、すべてを初期化します。
- ・ネットワーク設定を保持: ネットワーク設定を除いた部分をリセットします。OK を押すと、ネットワーク設定以外を初期化します。

3. 初期化すると端末が再起動します。

Note

- ・初期化すると、管理者レベルも初期化されます。初期化後は、必ず 管理者レベルを再設定してください。
- ・初期化しても 言語設定は維持されます。

ユーザーID種別

端末に登録する利用者IDの種類を、英字、数字、記号(_、-) の組み合わせに設定できます。

1.  をクリックして、管理者資格レベルで認証してください。
2. 端末 > ユーザーID種別 を選択してください。
3. 目的の項目を選択し、設定してください。

ログ検索

検索条件を設定してログを検索できます。

1.  をクリックして、管理者資格レベルで認証してください。
2. イベントログ を選択してください。すべてのログが表示されます。
3.  を押して、特定のログを検索する条件を変更してください。
4. OK を押してください。条件に一致するログが表示されます。

検索		OK
日時	2001/01/01 00:00~2030/12/31 23:59	
イベント	すべて	
勤怠イベント	すべて	
ユーザーID	IDを入力	



ログ削除

保存されたすべてのログを削除することができます。

1.  をクリックして、管理者資格レベルで認証してください。
2. イベントログ を選択してください。
3. すべてのログを削除するために、 を押して、OKを押してください。

ログ使用量

ログの使用量を確認することができます。

1.  をクリックして、管理者資格レベルで認証してください。
2. イベントログ を選択し、 を押してください。
端末のイベントログとイメージログの容量を確認できます。



障害報告前のチェックリスト

カテゴリ	問題	解決方法
電源	電源は供給されているが、端末が動作しない。	端末と背面ブラケットが離れていると、タンパースイッチが働き動作しないことがあります。
		電源アダプター や 電源ケーブルを確認してください。
PIN	PINコードを忘れてしまいました。	通常のユーザーPINの場合は、管理者にPINを要求してもう一度入力します。
		管理者PIN を忘れてしまった場合は、設置会社にお問い合わせください。
	PINコードを入力し、OKボタンを押しましたが、ドアが開きません。	登録されたPINが正しく入力されているか確認してください。
		PINを最近変更したかどうか確認してください。
顔	顔は登録されていますが、顔認証はスムーズに行えず、エラーが頻繁に発生します。	PINを覚えていない場合は、管理者にPINを確認し、再度、入力してください。
		“正しい顔の登録と認証方法”を確認し、再度、顔を登録してください。
	突然、顔認証ができなくなった。	多数の顔が登録されている場合は、認証タイムアウト を変更して再試行してください。
電気錠	ドアを閉めたが、ロックがかからない。	“正しい顔の登録と認証方法”を確認し、再度、顔を登録してください。
時刻	突然、時間が狂ってしまった。	電気錠が誤動作している可能性があります。設置会社を通じて検査を受けてください。
管理者アクセス	管理者PINを失ったため、管理者モードにアクセスできません。	SA-FSF2-DB はバッテリーが内蔵されていますが、電源が供給されていない場合、長期間使用すると内蔵バッテリーが消耗し、時間が間違ってしまうことがあります。時刻を修正する方法は、「日付 & 時刻」を参照してください。
		管理者は SA-FSF2-DB でアクセス権を付与するため、管理者だけが管理メニューにアクセスできます。
		管理メニューにアクセスする必要がある場合は、必要な手順でPINを発行することができます。
		パスワードを発行する手順については、インストール会社にお問い合わせください。

製品仕様

カテゴリ	特徴	仕様	カテゴリ	特徴	仕様
資格情報	生体認証	顔	容量	最大ユーザー数 (1:1)	100,000
	非接触カード	125kHz EM, 13.56MHz MIFARE/DESFire/DESFire EV1/FeliCa		最大ユーザー数 (1:N)	50,000 : 顔認証 100,000 : カード認証
	読み込み可能距離(※)	MIFARE/DESFire: 50mm EM, FeliCa: 30mm		最大テキストログ数	5,000,000
	モバイル	NFC, BLE		最大イメージログ数	50,000
一般	CPU	1.8GHz デュアルコア + 1.4GHz クアッドコア	インターフェース	イーサネット	10/100Mbps auto MDI/MDI-X
	メモリ	16GB Flash + 2GB RAM		RS-485	1ch Master/Slave (切替式)
	液晶	7インチ カラー タッチパネル (800 x 1280 ピクセル)		Wiegand	1ch Input または 1ch Output
	サウンド	16bit		TTL入力	2ch 入力
	動作温度	-20℃ ~ 50℃		リレー	1 出力
	ストレージ対応温度	-40℃ ~ 70℃		USB	USB 2.0 (ホスト)
	動作湿度	0% ~ 80% (結露なし)		タンパー	サポート
	ストレージ対応湿度	0% ~ 90% (結露なし)	電氣的仕様	電源	電圧: 12~24V DC 電流: 最大2.5A
	カメラ	2M ピクセル		スイッチ入力 V _{HI}	最小: 3V 最大: 5V
	防水性能	IP65		スイッチ入力 V _{LI}	最大: 1V
	寸法 (幅×高さ×奥行)	119.8mm x 223mm x 23.5mm		スイッチプルアップ抵抗	4.7kΩ (入力ポートは、4.7kΩでプルアップされています)
	重量	端末本体: 585g ブラケット: 181g (ネジ類含む)		Wiegand出力 V _{OHI}	4.8V 以上
	認証	CE, FCC, KC, RoHS, REACH, WEEE		Wiegand出力 V _{OLI}	0.2V 以下
	認証距離	0.5 ~ 1.3m		Wiegand出力プルアップ抵抗	内蔵プルアップ 1kΩ
顔	認証高	1.4 ~ 1.9m		リレー	電圧: 最大 30V DC 電流: 1A 最大 2A
	マッチング速度	0.5 秒以下			
	偽装顔検知	サポート			

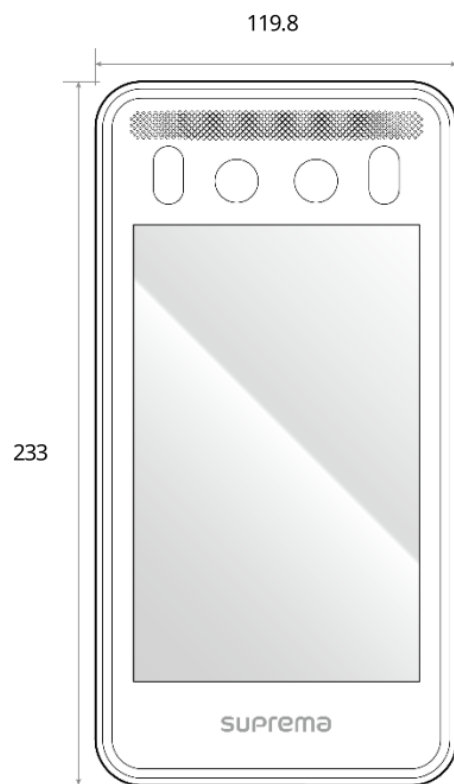
※カードの読み込み可能距離は、設置環境により異なります。

SECURE

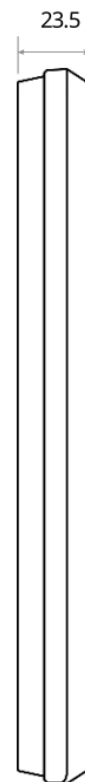
株式会社 セキュア
〒160-0220東京都新宿区西新宿二丁目6-1
新宿住友ビル20F
URL : www.secureinc.co.jp

寸法

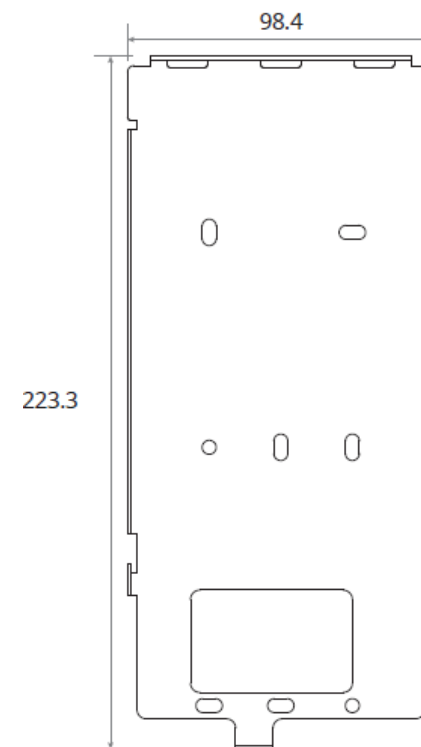
(単位:mm)



< 正面 >



< 側面 >



< ブラケット >