人体測温顔認識アクセス端末

マニュアル

V1.9.

目次

変更履歴

1.6	初版
1.7	FAQ、注意事項を追加
1.8	FAQ 編集
1.9	DSS ライセンス導入方法更新

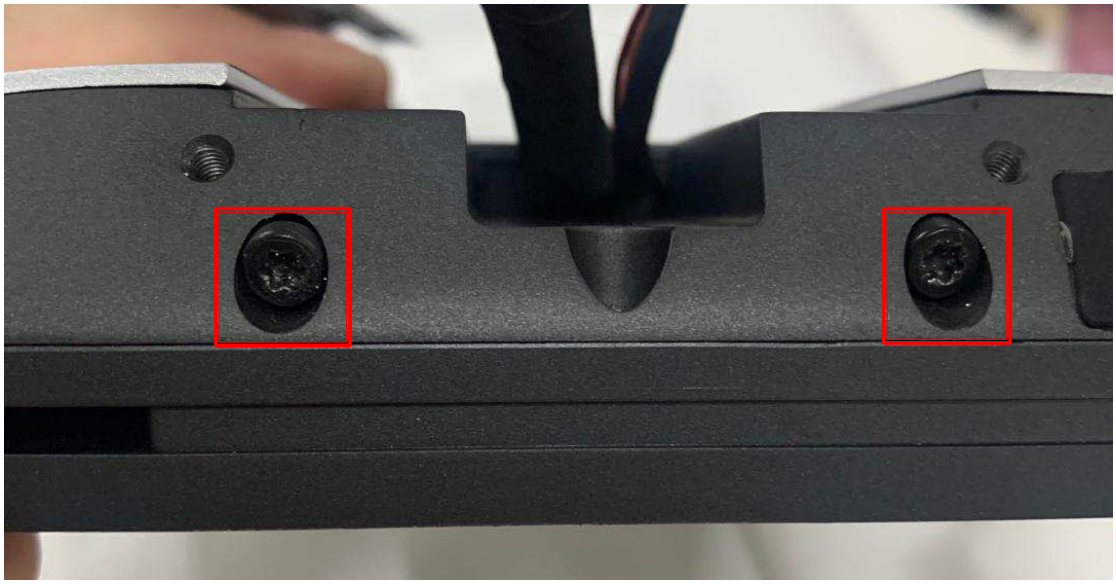
※ご使用の機器にようては、本書と一部異なる画面及び文言になる場合があります。

一、設置方法

1、ASI7213X-T1 設置方法

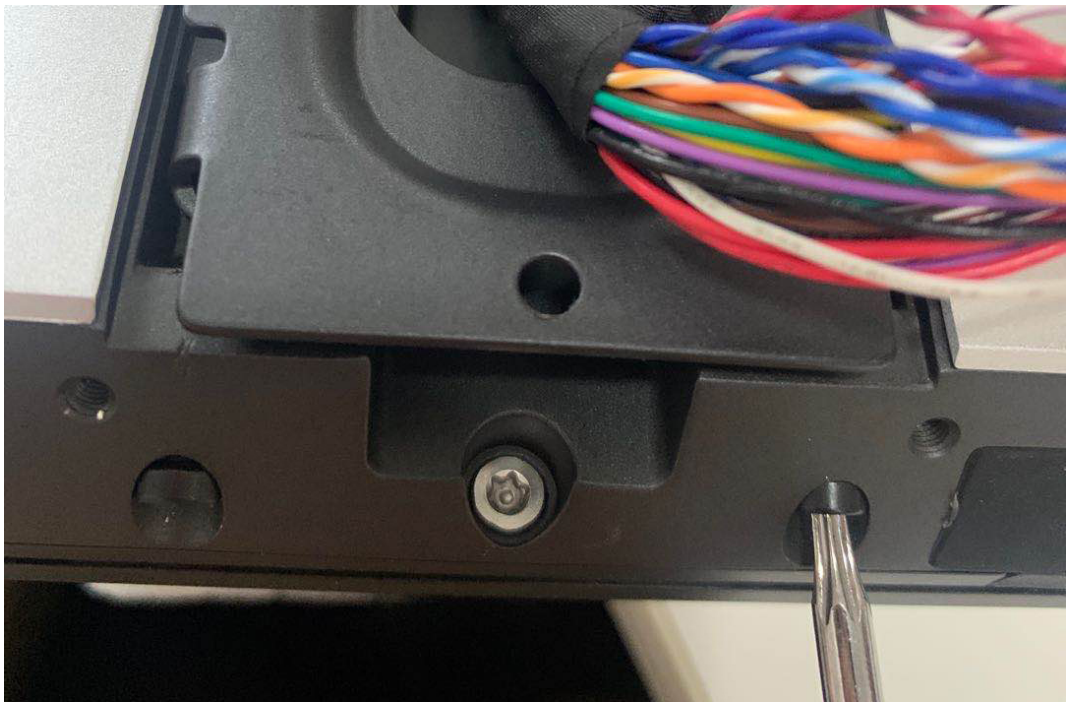
① 内容確認

② 底面の二つネジを緩みます



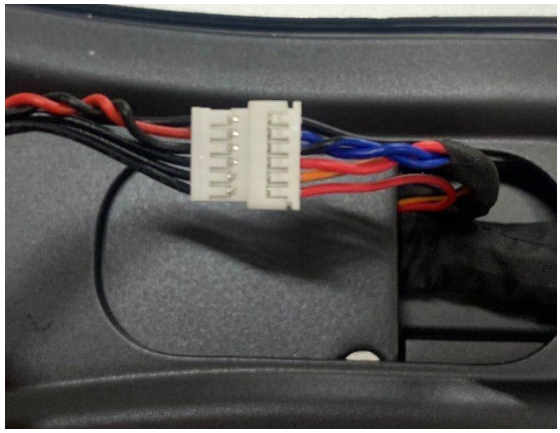
③ 機器裏面の取り付け孔で取り付け板金を設置します（本体のケーブルは板金の孔を通ります）

④ 底部のネジで板金を固定します



⑤ 測温モジュールを板金の上部に置きます、ケーブルは板金の孔を通ります、後ろからネジで測温モジュールを固定します


⑥ 測温モジュールと本体を繋ぎます

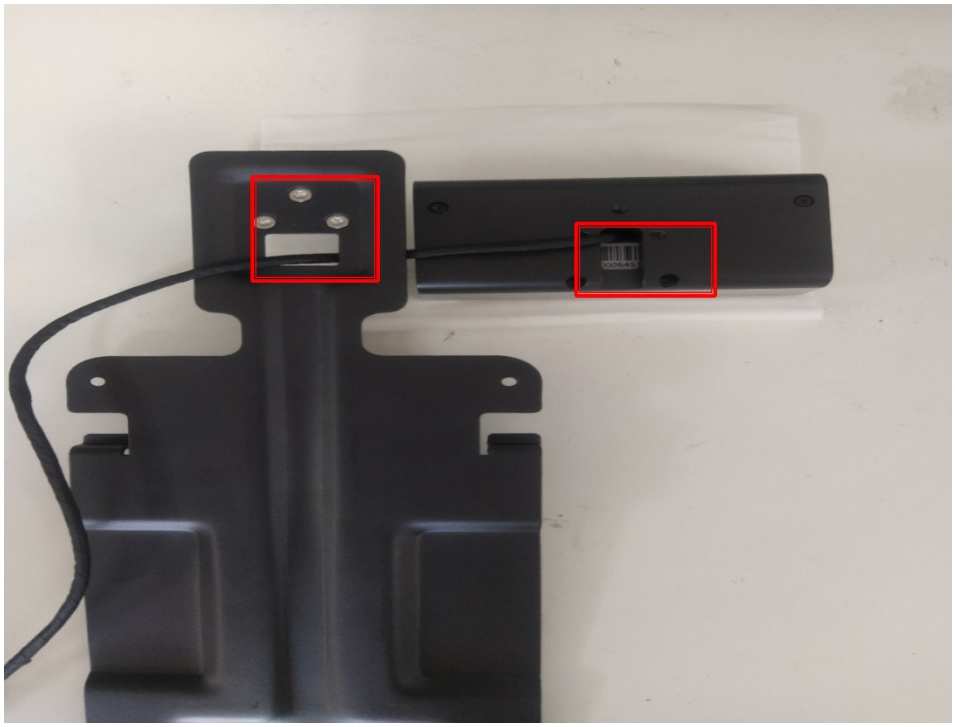



⑦ 設置完了

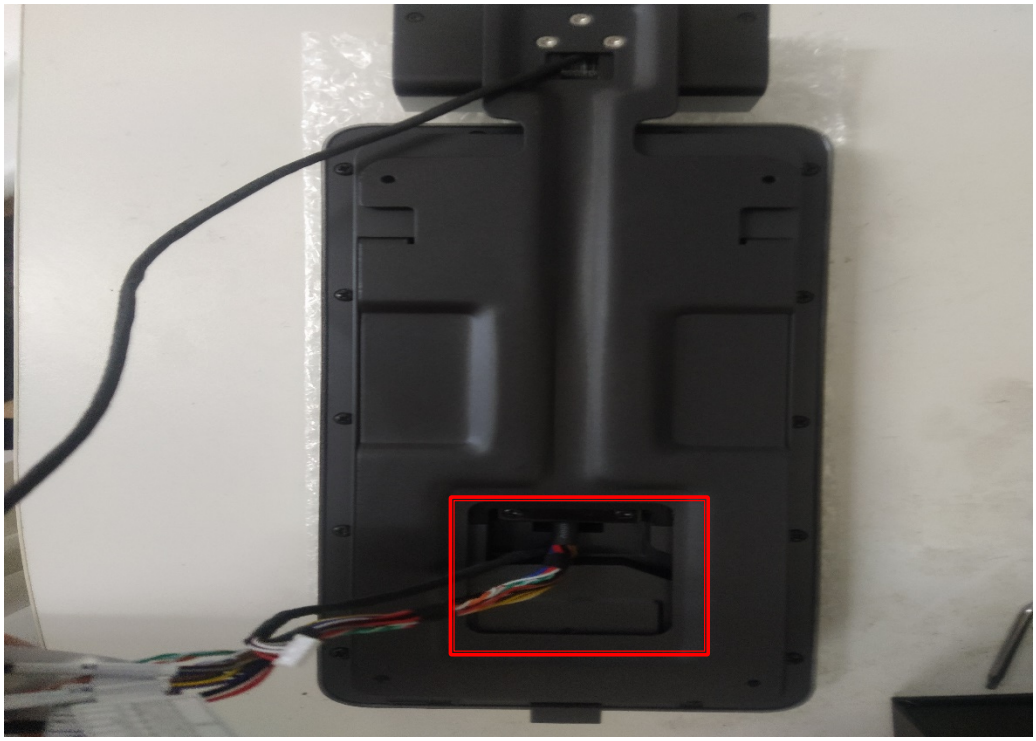
2、ASI7213Y-T1 設置方法

① 内容確認

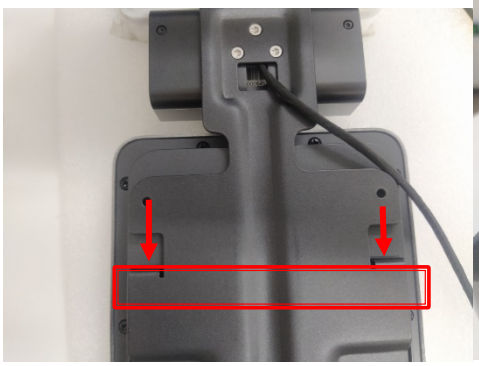
② 測温モジュールを板金の上部に置きます、ケーブルは板金の孔を通ります、後ろからネジで測温モジュールを固定します

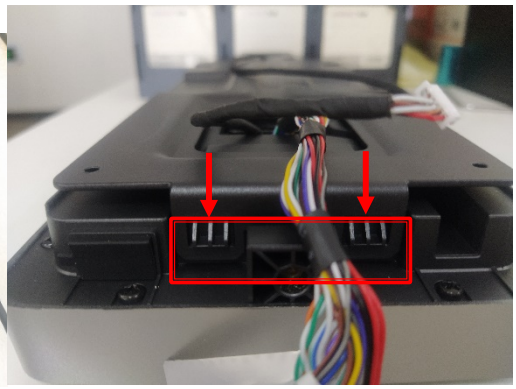


③ 機器裏面の取り付け孔で取り付け板金を設置します（本体のケーブルは板金の孔を通ります）

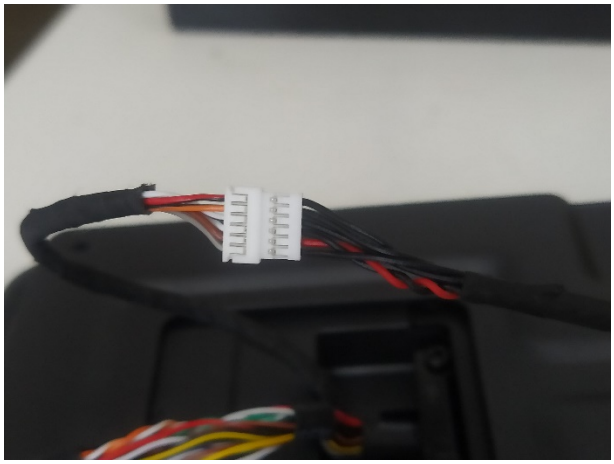


④ ４つのところはしっかり当て嵌まっていることを確認して、底部のネジで板金を固定します





⑤ 測温モジュールと本体を繋ぎます



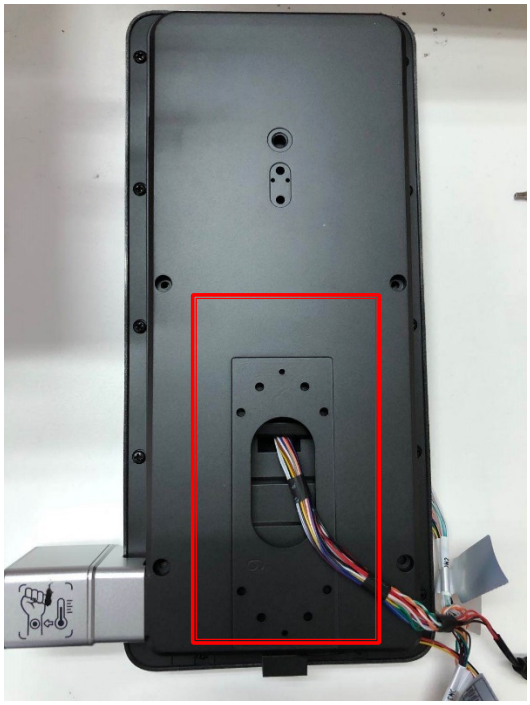
⑥ 設置完了

3、ASI7213Y0-V3-T0 設置方法

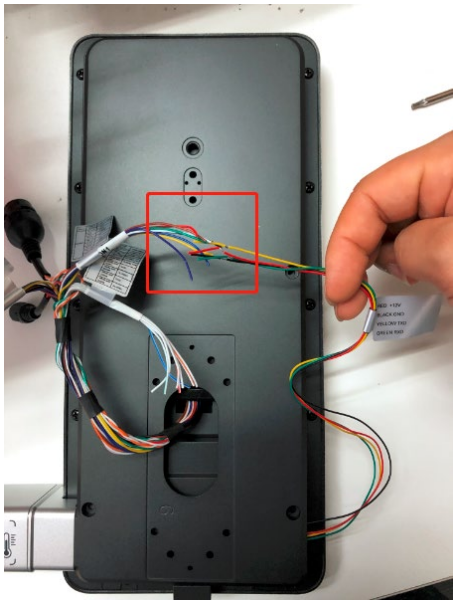
① 内容確認

② 四つネジで手首測温モジュールを板金に固定します

③ 機器本体裏面のケーブルは板金の孔を通ります



④ 測温モジュールと機器本体を繋ぎます。接線方法は
機器 CON1 の赤線と測温モジュールの赤線を繋ぎ;
CON1 の黒線と測温モジュールの黒線を繋ぎ;
CON1 の黄線と測温モジュールの緑線を繋ぎ;
CON1 の紫線と測温モジュールの黄線を繋ぎ;



⑤ 設置完了

4、接続と設置

① ケーブル接続

アクセスコントローラーは、サイレン、リーダー、ドアの接点などのデバイスに接続する必要があります。ケーブル接続については、下記を参照してください。

ケーブル接続

ポート	ケーブル色	ケーブル名	詳細
CON1	Black	RD−	外部カードリーダーのマイナス電極
	Red	RD+	外部カードリーダーの正極
	Blue	CASE	外部カードリーダーの改ざんアラーム入力
	White	D1	ウィーガンドD1入力（外部カードリーダーに接続）/出力（コントローラーに接続）
	Green	D0	ウィーガンドD0入力（外部カードリーダーに接続）/出力（コントローラーに接続）
	Brown	LED	外部リーダーインジケーターに接続
	Yellow	B	RS-485負極入力（外部カードリーダーに接続）/出力（コントローラーに接続、またはドア制御セキュリティモジュールに接続) セキュリティモジュールが有効になっている場合は、アクセス制御セキュリティモジュールを別途購入する必要があります。 セキュリティモジュールは、電力を供給するために別個の電源を必要とします。 セキュリティモジュールが有効になると、終了ボタン、ロックコントロール、および消防リンケージは無効になります。
	Purple	A	RS-485正極入力（外部カードリーダーに接続）/出力（コントローラーに接続、またはドアコントロールセキュリティモジュールに接続) セキュリティモジュールが有効になっている場合は、アクセス制御セキュリティモジュールを別途購入する必要があります。 セキュリティモジュールは、電力を供給するために別個の電源を必要とします。 セキュリティモジュールが有効になると、終了ボタン、ロックコントロール、および消防リンケージは無効になります。
CON2	White and red	ALARM1_NO	アラーム1出力ポート：NO(ノーマルオープン)
	White and orange	ALARM1_COM	アラーム1出力ポート：コモン
	White and blue	ALARM2_NO	アラーム2出力ポート：NO(ノーマルオープン)
	White and gray	ALARM2_COM	アラーム2出力ポート：コモン
	white and green	GND	共通GND
	White and Brown	ALARM1	アラーム1入力ポート
	White and yellow	GND	共通GND
	White and purple	ALARM2	アラーム2入力ポート
CON3	Black and red	RX	RS-232受信ポート
	Black and orange	TX	RS-232送信ポート
	Black and blue	GND	共通GND
	Black and gray	SR1	ドア接触検知に使用 Used for door contact detection.
	Black and green	PUSH1	ドアNo.1のドアオープンボタン Door open button of door No.1
	Black and Brown	DOOR1_COM	ロック制御共通ポート
	Black and yellow	DOOR1_NO	ロック制御ポート：NO（ノーマルオープン）
	Black and purple	DOOR1_NC	ロック制御ポート：NC（ノーマルクローズ）

② 設置環境

- アクセスコントローラーから 0.5 メートル離れた場所に光源がある場合、最低照度は 100 ルクス以上である必要があります。
- アクセスコントローラーは、窓とドアから少なくとも 3 メートル、照明から 2 メートル離れた屋内に設置することをお勧めします。
- 逆光や直射日光を避けてください。

周囲照明の要件

蝋燭:約 10Lux 電球:約 100∽850Lux 日光:≧1200Lux

温度検知の要件

· 温度監視ユニットは、屋内の無風環境（屋外から比較的離れた場所）に設置し、周囲温度を 15°C∽32°C に維持することをお勧めします。

· 温度監視ユニット平衡化するため、電源投入後 20 分以上経過してからご使用ください。

· 屋外には設置しないでください。

· 日光、風、冷気、冷房と温風の空調などの要素は、人体の表面温度とアクセスコントローラーの動作状態に簡単に影響を及ぼし、監視された温度と実際の温度との間に温度偏差を引き起こしますので、ご注意ください。

· 温度監視の影響因子

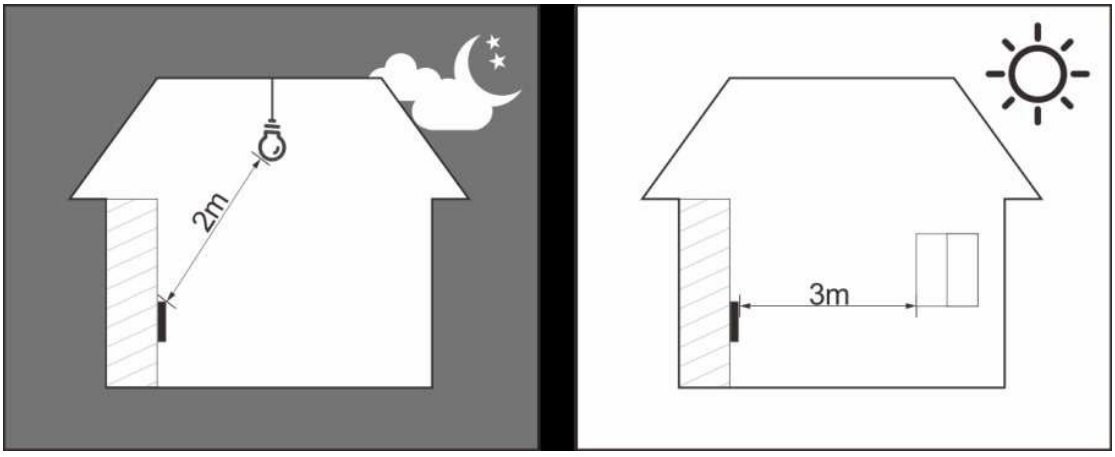
・風：風は額から熱を奪います。これは、温度監視の精度に影響します。

・発汗：発汗は、体が自動的に冷えて熱を放散します。汗をかくと、体温も下がります。

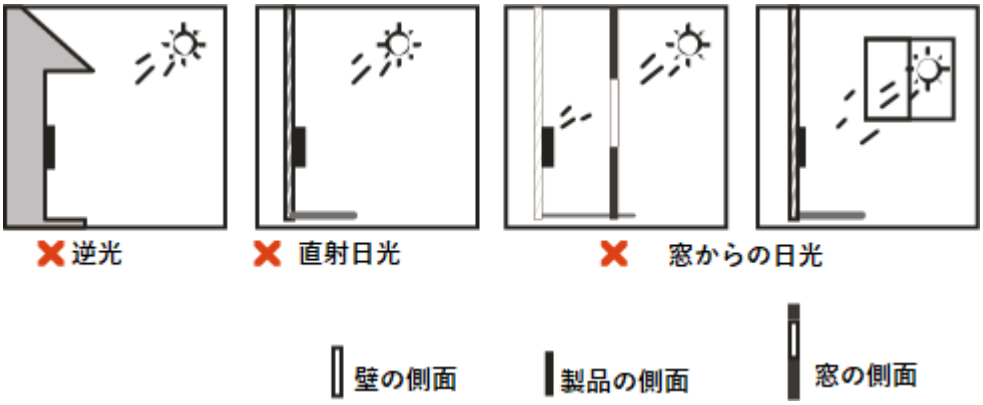
・室温：室温が低いと人体の表面温度が下がります。室内温度が高すぎると、人体が発汗し始め、温度監視の精度に影響を与えます。

・温度監視ユニットは、波長10um∽15um の光波に敏感です。
太陽、蛍光灯の光源、エアコンの吹き出し口、暖房、冷気の吹き出し口、ガラスの表面での使用は避けてください。

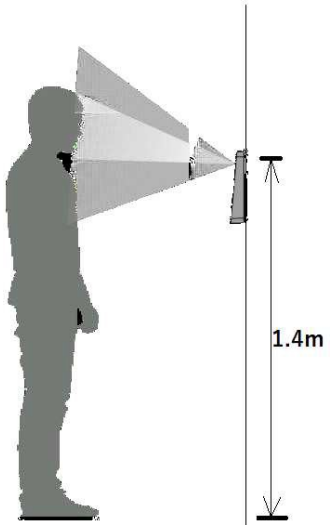
推奨設置場所

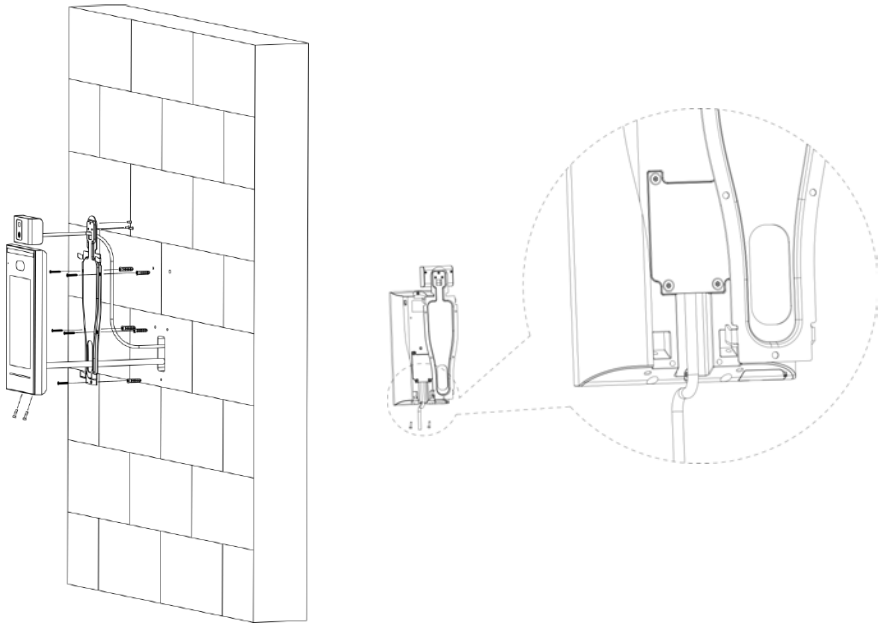


推奨しない設置位置



③　設置取付





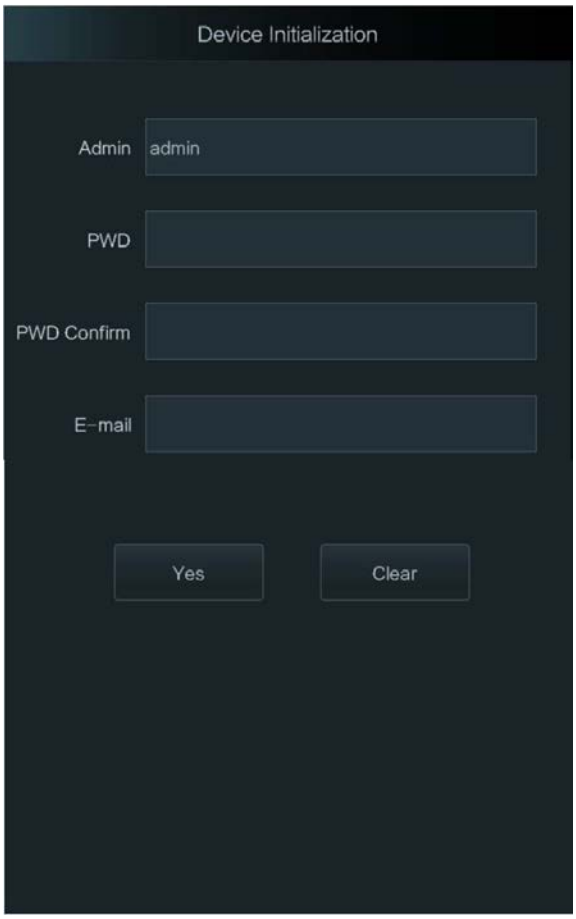
カメラと地面の間の距離が 1.4 メートルであることを確認します。

壁掛け方法

二、設定

機器の初期設定、ユーザー追加方法、顔認識設定などの紹介です。

1、機器初期化



① 初めて電源を入れる場合は初期化画面が表示されます

- このインターフェイスで設定された管理者とパスワードは、Web 管理プラットフォームへのログインに使用されます。
- 管理者のパスワードは、管理者がパスワードを忘れた場合に、入力した電子メールアドレスを使用してリセットできます。
- パスワードは、8~32 文字の空白以外の文字で構成され、大文字、小文字、数字、特殊文字（ '";: ＆を除く）の少なくとも 2 種類の文字を含む必要があります。

(詳細なリセット方法は、「FAQ　1、機器本体 FAQ」をご参照ください。)

「admin」はデフォルト設定されています、変更できません。「パスワード」をタッチして、パスワードを設定し

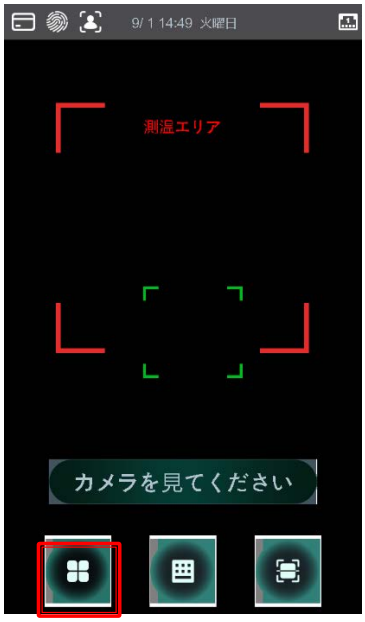
ます、右上の「√」で保存します

② 同じ方法で「パスワード確認」と「E メール」を設定して、「Yes」で admin 情報を保存します

③ 設置完了

2、メイン画面に入る

① 待機画面で左下のボタンをタッチします



② 表示された画面で四つの方式があります

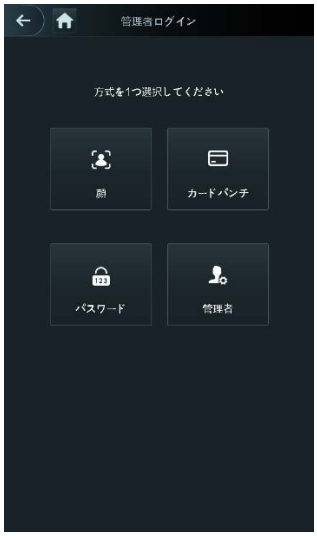
1）顔：顔で認証します

2）カードパンチ：カードで認証します

3）パスワード：ユーザーID とパスワードで認証します

4）管理者：「管理者」アカウントで認証します

1）~3）はユーザーを追加する必要がありますので、今回は「管理者」アカウントで認証します



③ 「管理者」アカウントを選択する場合、ID は固定されていますので、ID 入力は不要、パスワードだけを入力します、「√」で認証します

④　パスワードが正しく入力される場合はメイン画面が表示されます

ユーザー	ユーザーの追加、編集、削除などの操作
アクセス	解錠時間帯、方式なのの設定
接続	ネット、シリアルポート、wiegand などの設定
システム	本体時間、顔認識関係のパラメータなどの設定
USB	USB メモリーを利用して、情報の導入と導出、アップグレード
特徴	機器に関する暗号化設定
録画	解錠履歴
自動テスト	機器状態を確認するための機能テスト
装置情報	機器の使用容量とシステムバージョン情報

3、web でアクセス

①　機器の IP アドレス情報を確認

1）メイン画面で「接続」をタッチします

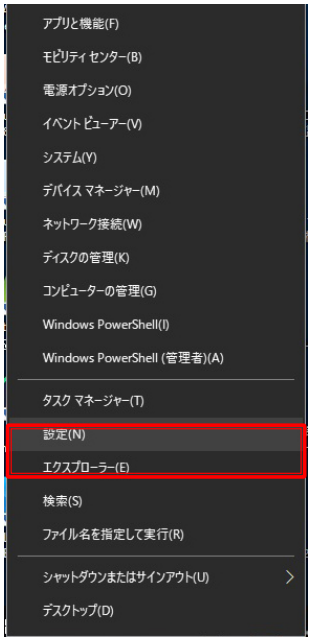
2) 「ネットワーク設定」をタッチします

3) 「IP アドレス」をタッチします

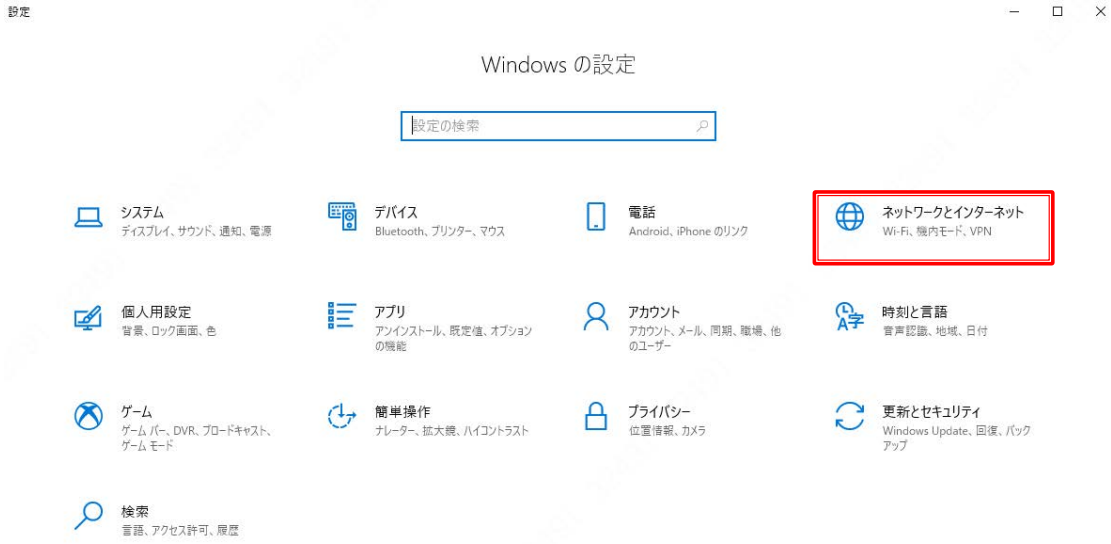
4) 機器のポートは 1000M と 100M 二つがあります。選択によってポートの情報が表示されます。

② PC のポート設定を調整します

1) PC の左下の  を右クリックして、「設定」を選択します

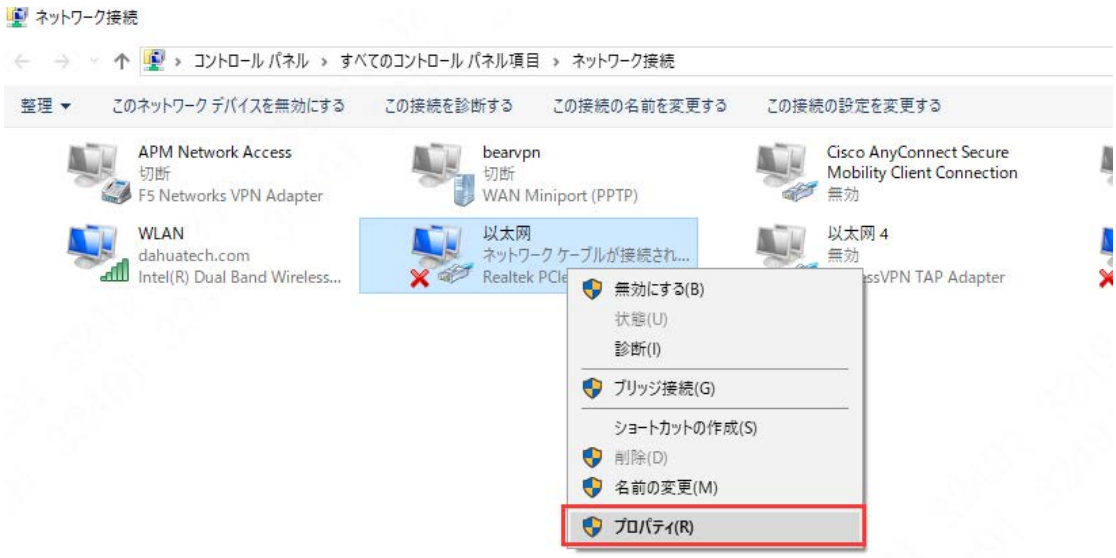


2) 「ネットワークとインターネット」を選択します

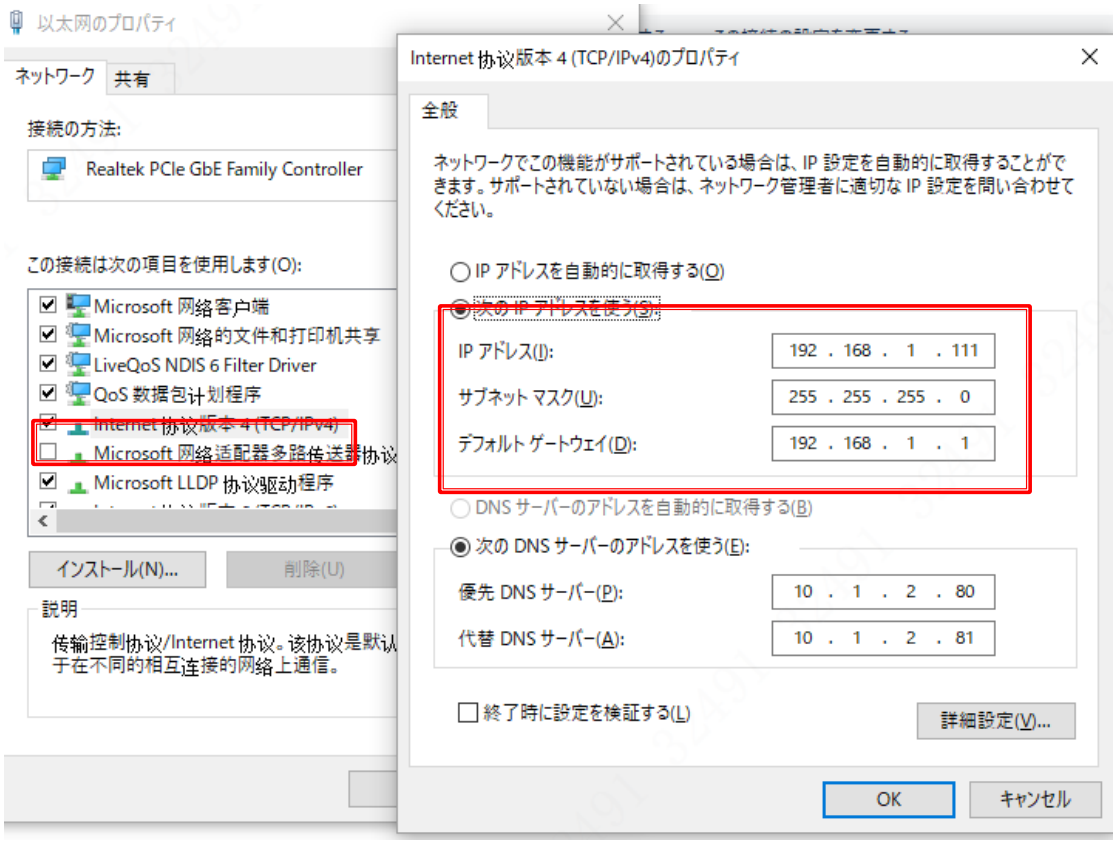


3) 「イーサネット」画面で「アダプターのオプションを変更する」を選択します

4) lan ポートの配置ファイルで右クリックして、「プロパティ」を選択します

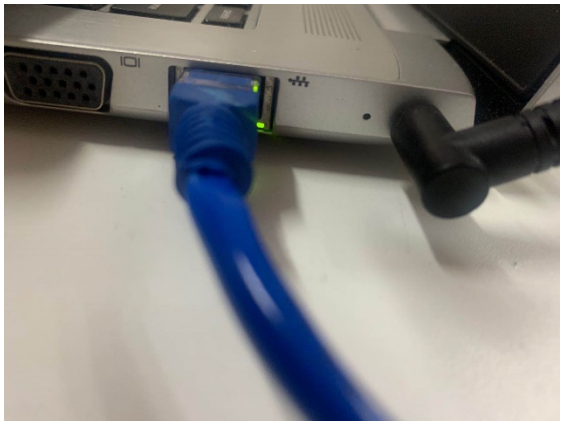


5) 「TCP/IPv4」でダブルクリックして、機器と同じネットワークセグメントの IP アドレスを設定します。

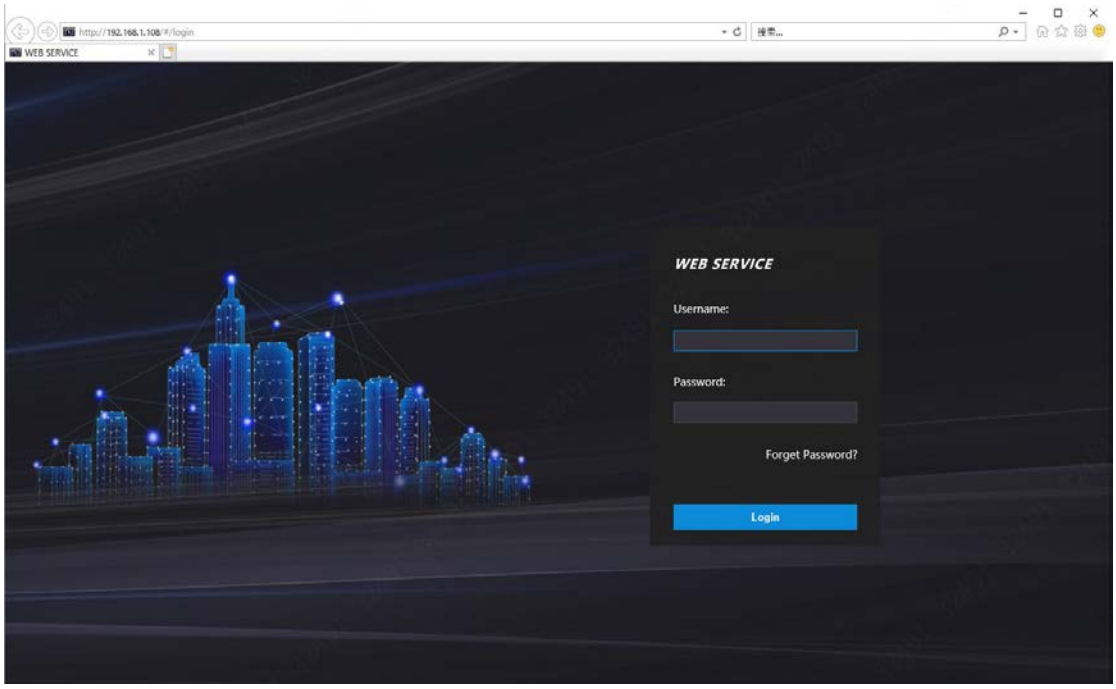


③ PC から機器をアクセスします

1) lan ケーブルで PC と機器を繋ぎます

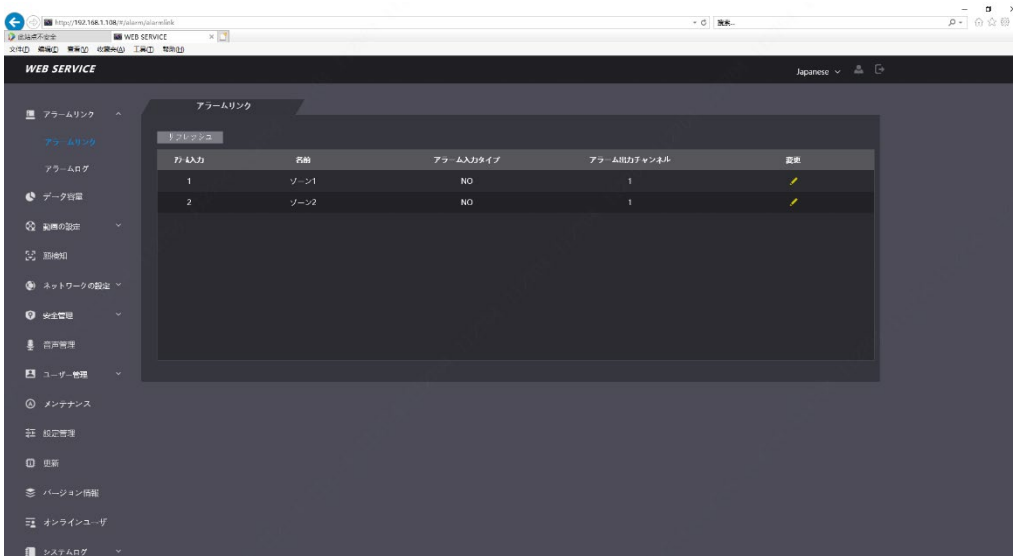


2) PC で「Internet Explorer」に機器の IP アドレス（192.168.1.108）を入力して、アクセスします



3) Admin アカウントのユーザー名とパスワードを入れて、ログインします

4) ログインした後は web 経由で機器を設定することができます



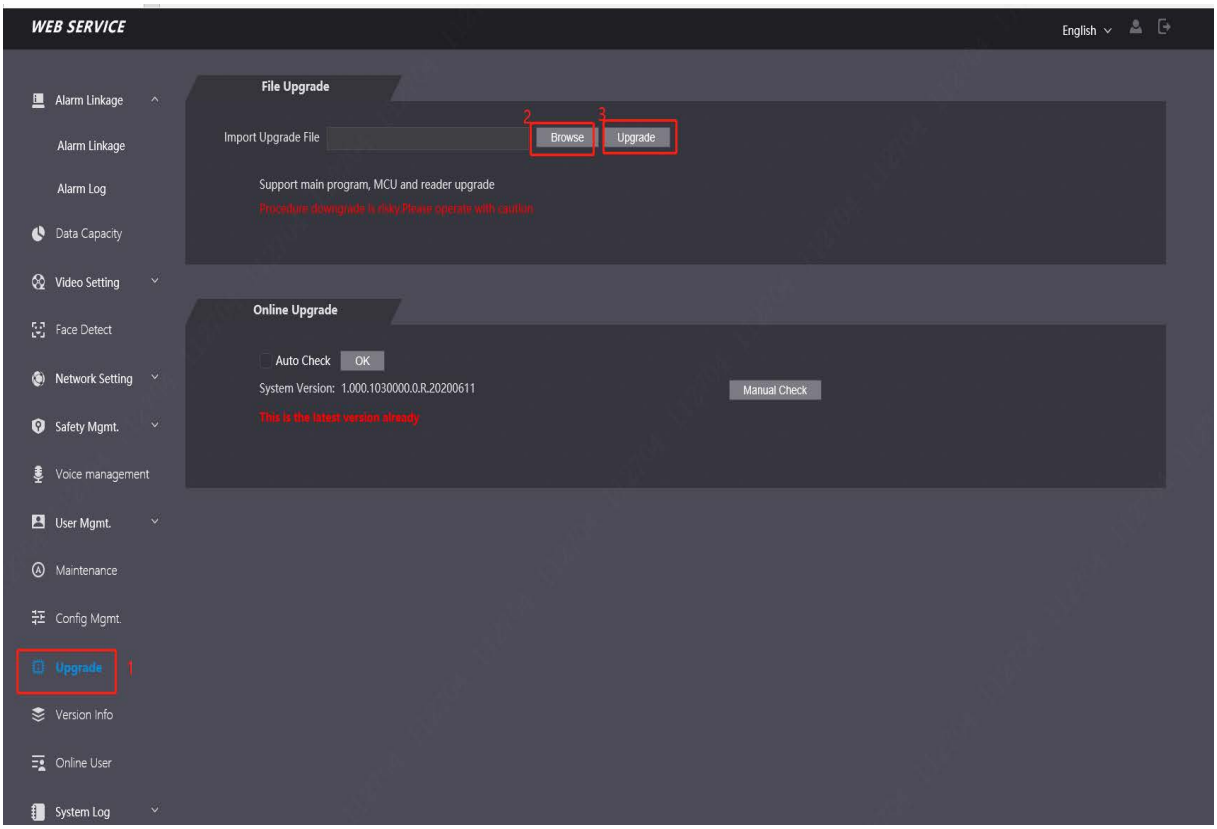
4、機器をアップグレード

① 用意すべきもの:

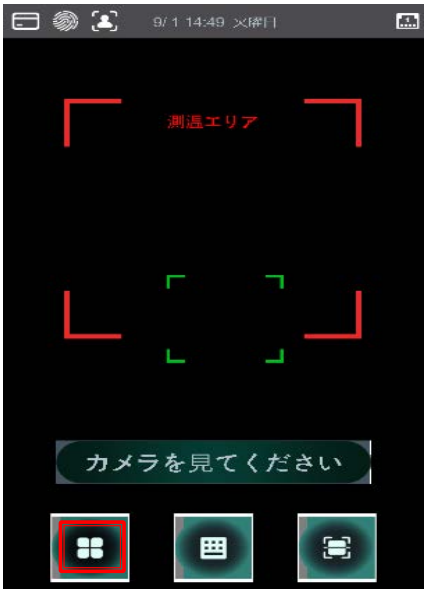
- アクセスコントローラー端末×1
- パソコン（PC）×1
- LAN ケーブル×1
- 日本語のファームウェアを PC にダウンロードしてください。

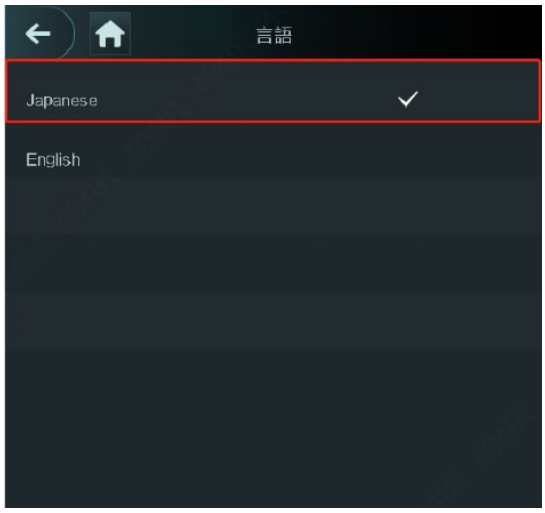
（日本語のファームウェアのダウンロード先は弊社サポート窓口までご連絡ください。）

② パソコンと端末を Web 側にログインした後、「Upgrade」>「Browse」の順で進み、ダウンロードしたファームウェアを選択して、「Upgrade」をクリックします。



③　アップグレード後、機器は自動的に再起動します。再起動後、機器で言語を日本語に設定します。機器は再起動後、日本語画面になります。





④　アップグレードと設定は完了です。

5、ユーザー追加

①　メイン画面で「ユーザー」をタッチします。

②　「新規ユーザー」をタッチします。

③ 「ユーザーID」と「名前」をタッチして、設定します。

詳しい説明は下記となります。

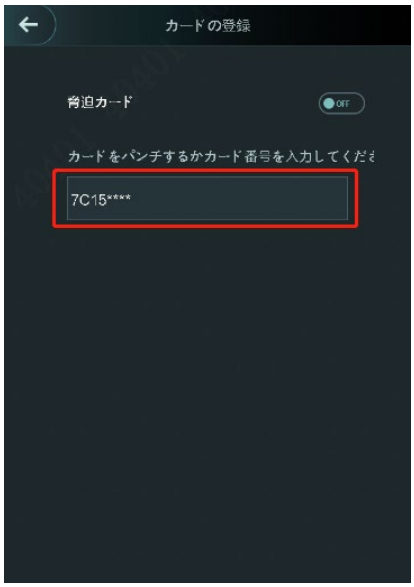
項目	詳細
ユーザー ID	ユーザーIDを入力します。IDには、数字、文字、およびそれらの組み合わせを使用できます。IDの最大長は32文字です。
名前	名前は最大32文字（数字、記号、文字を含む）で入力してください。
顔	顔が写真キャプチャフレームの中央にあることを確認してください。アクセスコントローラーが新しいユーザーの顔の写真を自動的に撮影します。
カード	ユーザーごとに最大5枚のカードを登録できます。カード登録インターフェースで、カード番号を入力するか、カードをスワイプすると、 アクセスコントローラーによってカード情報が読み取られます。カード登録インターフェースで強迫カード機能を有効にすることができます。 ドアのロックを解除するために強迫カードが使用された場合、アラームがトリガーされます。
パスワード	ロック解除パスワード。最大8文字まで登録可能です。
ユーザーレベル	新しいユーザーのユーザーレベルを選択できます。2つのオプションがあります。 ・ User：ユーザーはロック解除権限のみを持っています。 ・ Admin：管理者はロックを解除することができ、各設定の権限も持っています。
期間	ユーザーがロックを解除できる期間を設定できます。
休日プラン	ユーザーがロックを解除できる休日プランを設定できます。
有効日付	ユーザーのロック解除情報を有効にする期間を設定できます。
ユーザーレベル	6つのレベルがあります。 ・ General：General ユーザーは通常どおりロックを解除できます。 ・ Blacklist：ブラックリストのユーザーがロックを解除すると、サービス担当者にプロンプトが表示されます。 ・ Guest：ゲストは特定の時間にドアのロックを解除できます。設定した時間を超えると、ロックを解除することはできません。 ・ Patrol：ユーザーは認識状況を追跡できますが、ロック解除の権限はありません。 ・ VIP：ロックを解除すると、サービス担当者がプロンプトを表示します。 ・ Special：ロックを解除すると、ドアが閉まるまでに5秒の遅延があります。

利用時間	ユーザーレベルがゲストの場合、ユーザーがドアのロックを解除できる最大回数を設定できます。

④ 「顔」をタッチして、顔情報を登録します。写真と「録画されました!」が表示されたら、「録画」ボタンで顔を登録します。もしもう一度顔が撮影したい場合は「もう一度録画する」ボタンを押してください。

⑤ 「カード」をタッチして、カードを登録します。一つユーザーは最大 5 枚のカードを登録できます。まずは一番上のカードを選択します。

下図が表示される時、端末のカードリーダーのところにカードを置いて、カード情報が読込します。カード情報が表示されたら、左上の「←」で情報を保存します。



備考：カードの設定画面で「脅迫カード」という項目があります、この選択が「on」にしたら、設定されたカードが脅かしカードになります。このカードは解錠できますが、同時にアラームも発報します。

⑥ 最後にパスワード「パスワード」とユーザーレベル「ユーザーレベル」を設定します。

「ユーザーレベル」は「ユーザー」と「管理者」二つの選択肢があります。

「ユーザー」の場合はただ解錠できます。

「管理者」 の場合はこのユーザーがメイン画面に入って、機器の設定も変更できます。「二、設定」-「2、メイン画面に入る」-「②　」の 1）~3）の認証方式が利用可能です。

6、顔認識と測温パラメータ調整

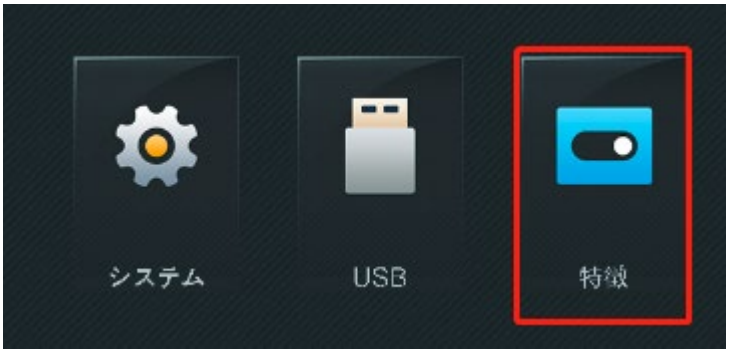
① メイン画面で「システム」を選択して、次の画面で「顔パラメータ」を選択します。

② 「顔パラメータ」画面で顔認識と測温のパラメータが調整できます各項目を説明します。

顔認識閾値	顔認識の閾値、認識の精度に影響があります。
顔認識の最大偏角	顔認識の顔角度
瞳孔間距離	瞳孔間距離、顔認識の距離に影響があります、小さい数値を設定すると、遠距離でも認識できます。
認識タイムアウト（秒）	連続二回顔認識解錠成功の提示間隔。
認識間隔(秒)	解錠権限はない人の顔が検知されるから、エラーが出すまでの時間です。
偽造防止有効	生命体認識。On にすると、写真などの解錠が不可になります。
温度測定	体温測定機能の on/off
温度エリア枠	体温測定エリア表示の on/off
測温距離(cm)	体温測定の距離に影響があります
温度設定値(℃)	体温異常の閾値
温度校正値(℃)	体温が正しく測らない場合校正用のパラメータです。
マスクモデル	テストなし：マスク検知 off マスク注意：マスク未着用の場合提示します マスク阻止：マスク未着用の場合解錠できません
温度単位	℃/℉表示の切替

7、解錠画面表示モード

① メイン画面で「特徴」を選択して、次の画面で「結果フィードバック」を選択します。



② 「結果フィードバック」画面で認識する時の画面表示モードが設定できます各項目を説明します。

成否	解錠成否を表示します
名前のみ	解錠成否を表示します
ユーザーの写真と名前	ユーザーの写真と名前を表示します
写真比較と名前	写真比較と名前を表示します

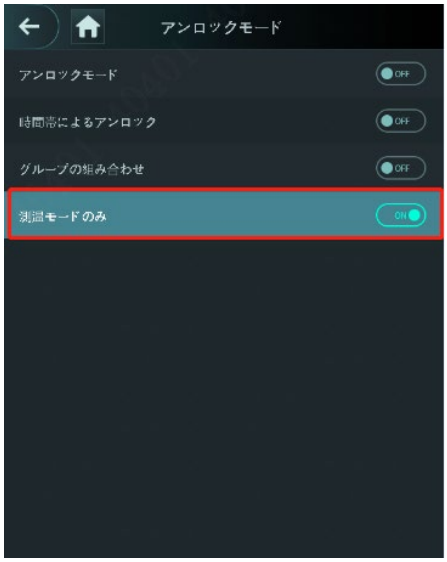
9、体温のみで解錠

顔、カードなどを認識しない、体温のみで解錠できます。

① メイン画面で「アクセス」をタッチします。

② 「アンロックモード」を選択します

③ 「測温モードのみ」を有効します



10、USB

- ユーザー情報をエクスポートして更新する前に、USB が挿入されていることを確認してください。エクスポートまたは更新中は、USB を引き出したり、その他の操作を行ったりしないでください。そうしないと、エクスポートまたは更新が失敗します。
- USB を使用して別のアクセスコントローラーに情報をインポートする前に、
  1 つのアクセスコントローラーから USB に情報をインポートする必要があります。
- USB を使用してプログラムを更新することもできます。

① **USB エクスポート**

USB を挿入した後、アクセスコントローラから USB にデータをエクスポートできます。エクスポートされたデータは暗号化されており、編集できません。

Step 1　「USB エクスポート」を選択します。USB エクスポートインターフェイスが表示されます。

Step 2　エクスポートするデータタイプを選択します。エクスポートの確認のプロンプトが表示されます。

Step 3　OK をタップします。エクスポートされたデータは USB に保存されます。

② **USB インポート**

別のアクセスコントローラーにインポートできるのは、1 つのアクセスコントローラーからエクスポートされた USB 内のデータのみです。

Step 1　「USB インポート」を選択します。USB インポートインターフェイスが表示されます。

Step 2　インポートするデータタイプを選択します。インポートの確認のプロンプトが表示されます。

Step 3　OK をタップします。USB フラッシュドライブのデータがアクセスコントローラーにインポートされます。

③ **USB 更新**

USB フラッシュドライブを使用してシステムを更新できます。

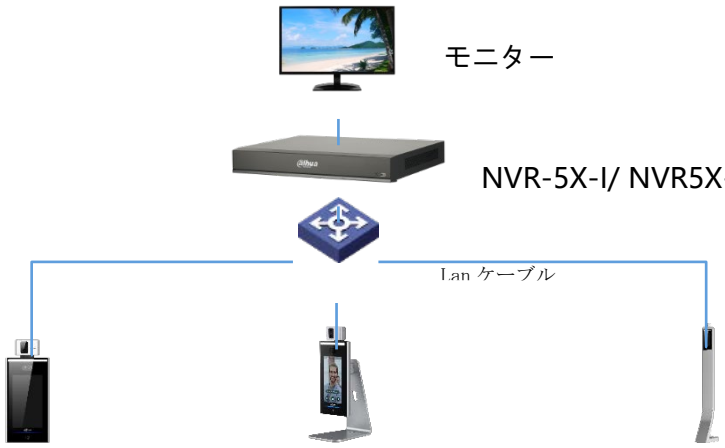
Step 1　更新ファイルの名前を「update.bin」に変更し、「update.bin」ファイルを USB ドライブのルートディレクトリに保存します。
※Web へのログインに使用するコンピューターがデバイスと同じ LAN にあることを確認します。
1000M ネットワークポートのデフォルトの管理アドレスは 192.168.1.108 で、100M ネットワークポートのデフォルトの管理アドレスは 192.168.2.108 です。

Step 2　「USB 更新」を選択します。更新の確認のプロンプトが表示されます。

Step 3　OK をタップします。更新が開始され、更新が完了するとアクセスコントローラーが再起動します。

三、NVR レコーダーと連携

システム構成:端末 + NVR



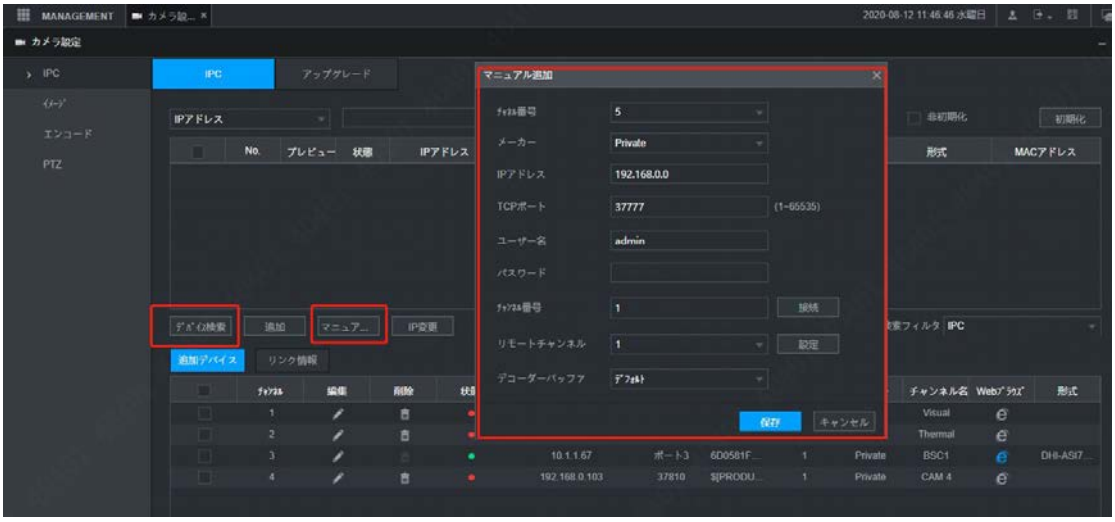
壁掛け　　卓上式　　スタンディン

※以上は参考となります。

1、端末を追加

① NVR Web にログイン、「Management」→「カメラ設定」をクリックします。

② 「デバイス検索」で機器を追加します、或いは「マニュアル追加」で、機器のユーザー名とパスワードを入力して、「保存」をクリックします。



③ 追加した後、メイン画面で「AI」>「パラメータ設定」>「DoorAccessControl」をクリックします。ご希望に応じて「体温は閾値以外」と「マスク異常」を設定します。

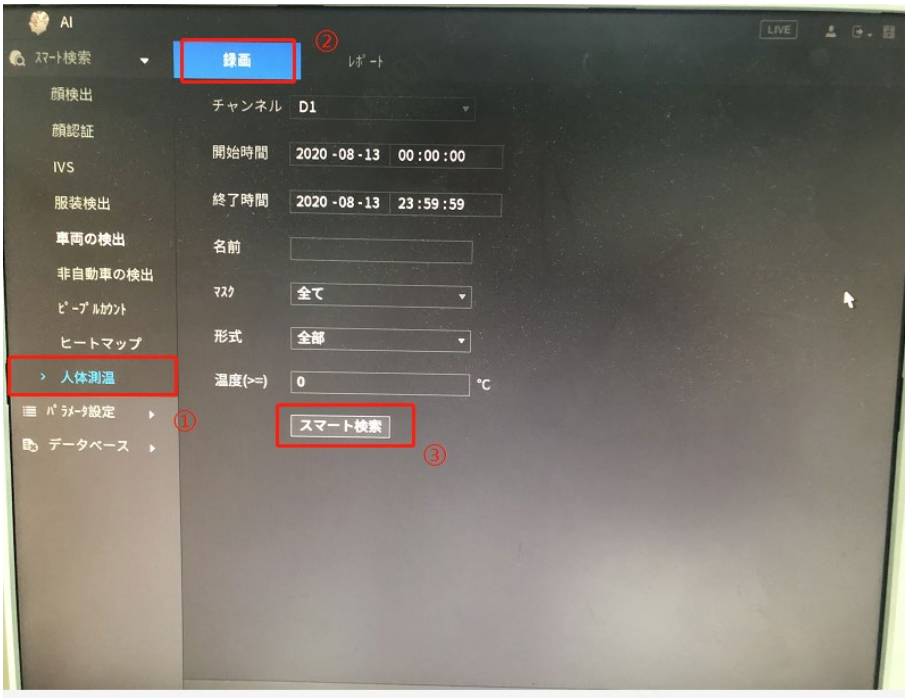
2、AI モード表示

① モニターのライブビュー画面で右クリックして、AI モードを選択します。
右側に顔と機器に登録した顔の比較情報が表示されます。

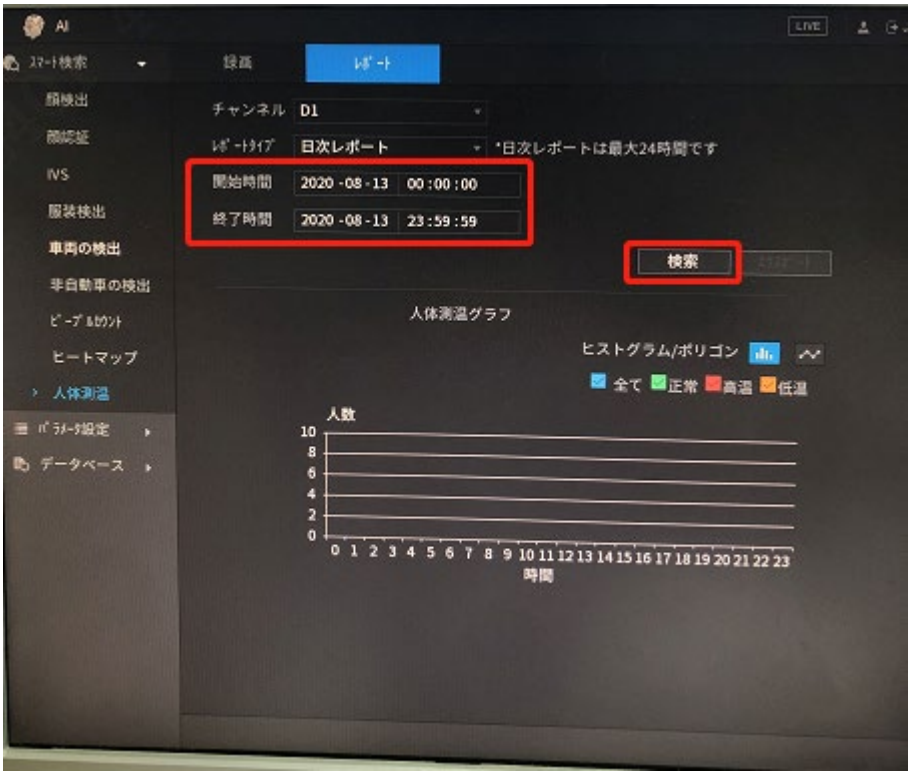
3、スマート検索

① [AI]>[スマート検索]>[人体測温]>チャネルと開始時間、終了時間を選択>[スマート検索]をクリックします。

② 対応する録画が表示、選択したら再生できます。

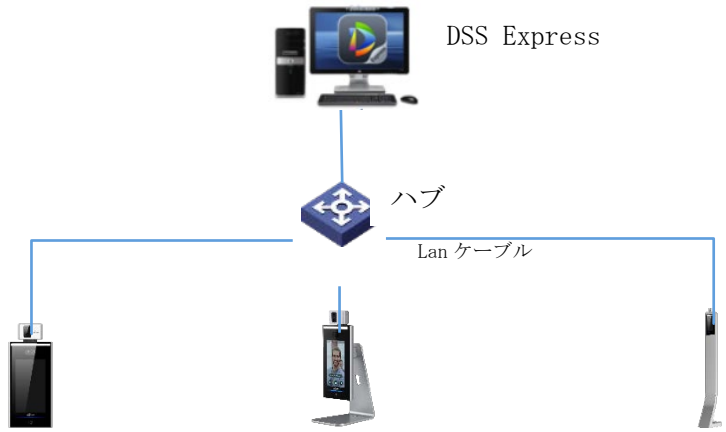


④ 「レポート」で開始時間、終了時間を選択、レポートをエクスポートできます。


AI
LIVE
スマート検索
録画
レポート
顔検出
顔認証
IVS
服装検出
車両の検出
非自動車の検出
ピープルカウント
ヒートマップ
人体測温
パラメータ設定
データベース
チャンネル D1
レポートタイプ 日次レポート
*日次レポートは最大24時間です
開始時間 2020-08-13 00:00:00
終了時間 2020-08-13 23:59:59
検索
人体測温グラフ
ヒストグラム/ポリゴン
全て 正常 高温 低温
人数
10
8
6
4
2
0
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23
時間

四、管理ソフト（DSS Express)

システム構成:端末＋PC ソフト(Dss Express)



※以上はご参考となります

1、DSS Express サーバーをインストール

DSS Express のダウンロード先は、サポート窓口までご連絡ください。

① スペック要求

DSS サーバースペック要求	
推奨スペック	CPU: Intel® Xeon® CPU E3-1220 v5 @3.00GHz RAM: 18 GB Network adapter: 1Gps DSS installation directory space: Over 500 GB
最低スペック	CPU: i3-2120 RAM: 8 GB Network adapter: 1Gps DSS installation directory space: Over 200 GB
システム	Support Win7 and later systems.

② サーバー IP アドレスを設定

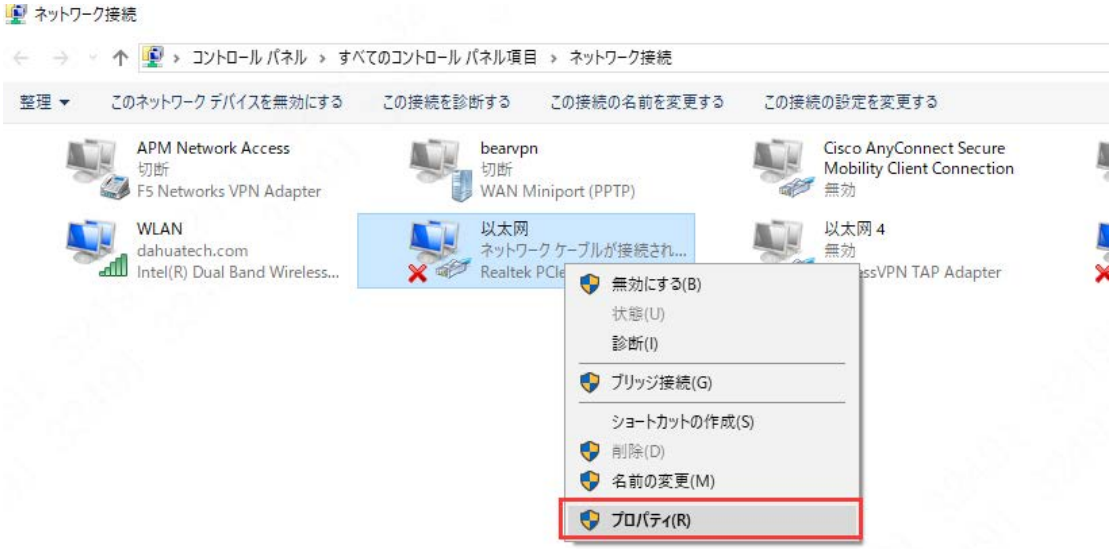
PC は DSS サーバーに当たって使うですので、つまりサーバーの IP は PC の IP です。PC の IP を変更、ネットワーク内の他のデバイスとの接続が良好であることを確認します。まず PC の IP を設定します。

1) PC の左下の  を右クリックして、「設定」を選択します

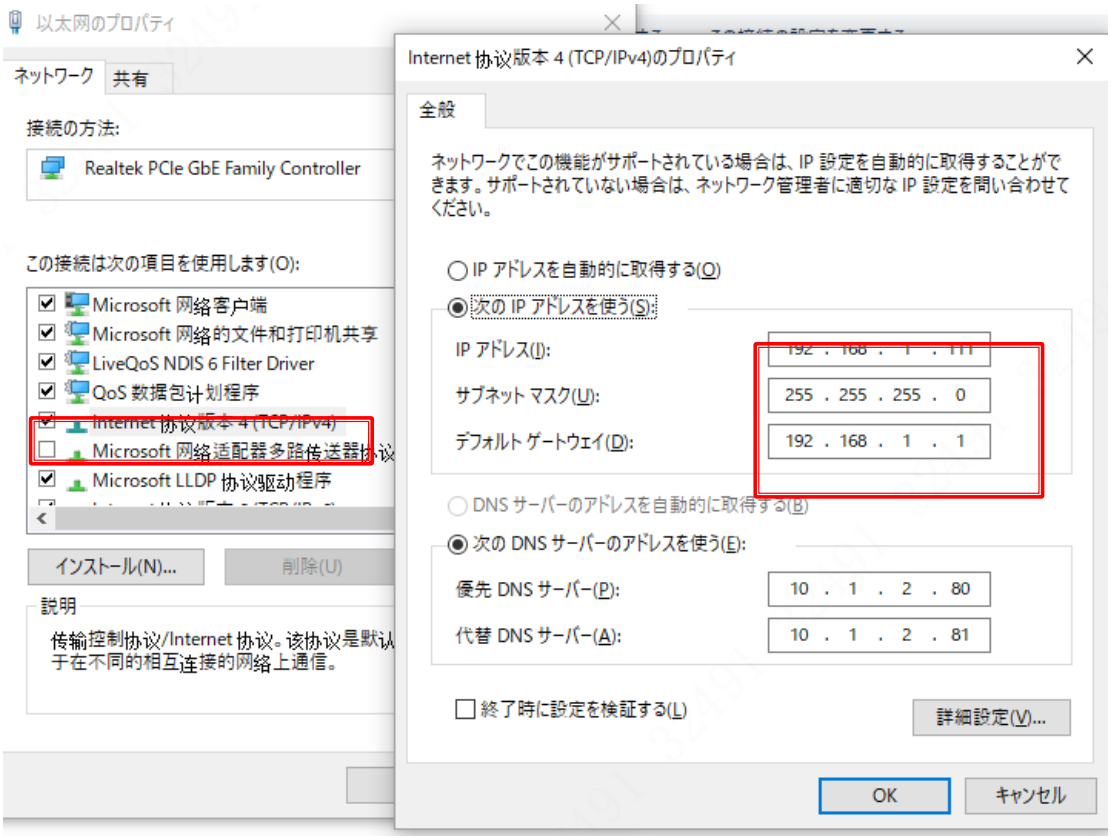
2) 「ネットワークとインターネット」を選択します

3) 「イーサネット」画面で「アダプターのオプションを変更する」を選択します

4) lan ポートの配置ファイルで右クリックして、「プロパティ」を選択します



5) 「TCP/IPv4」でダブルクリックして、機器と同じネットワークセグメントの IP アドレスを設定します。

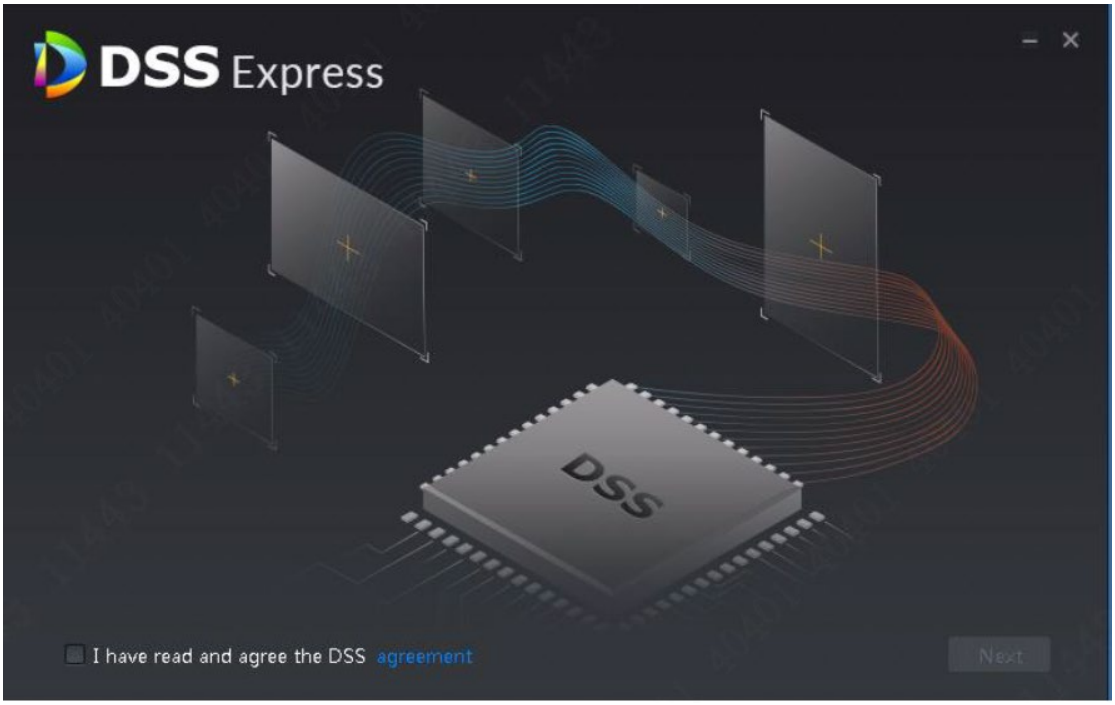


IP 設定完了。

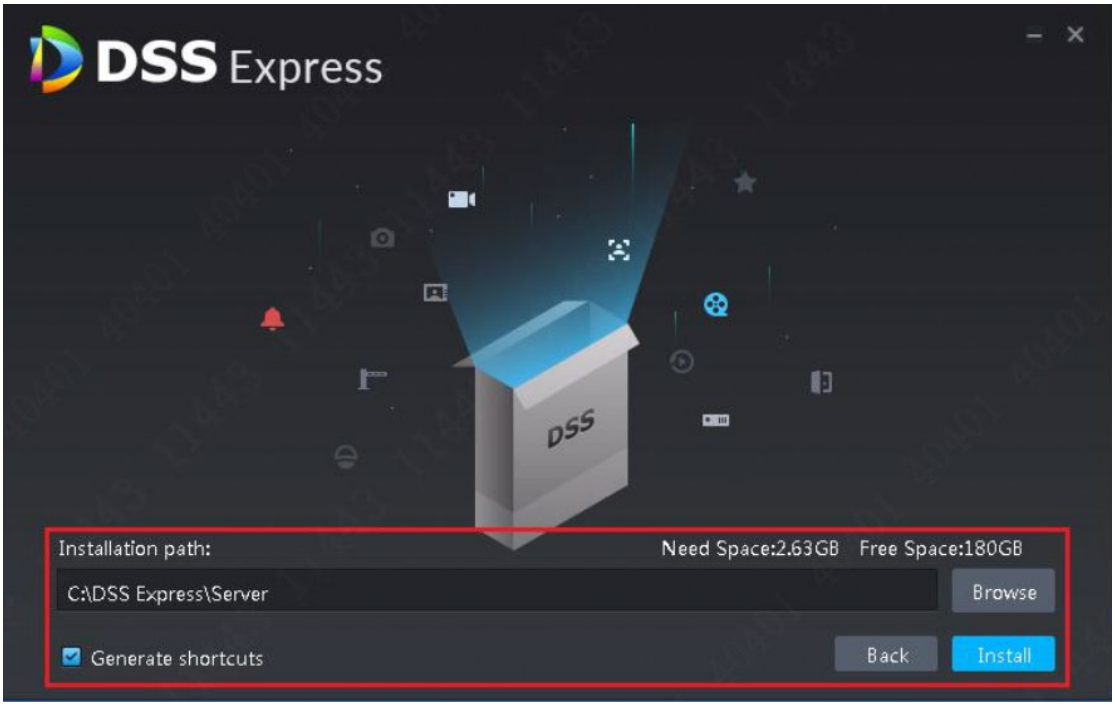
③　DSS サーバーをインストール

1)　 

DSS プログラムをダブルクリックします。



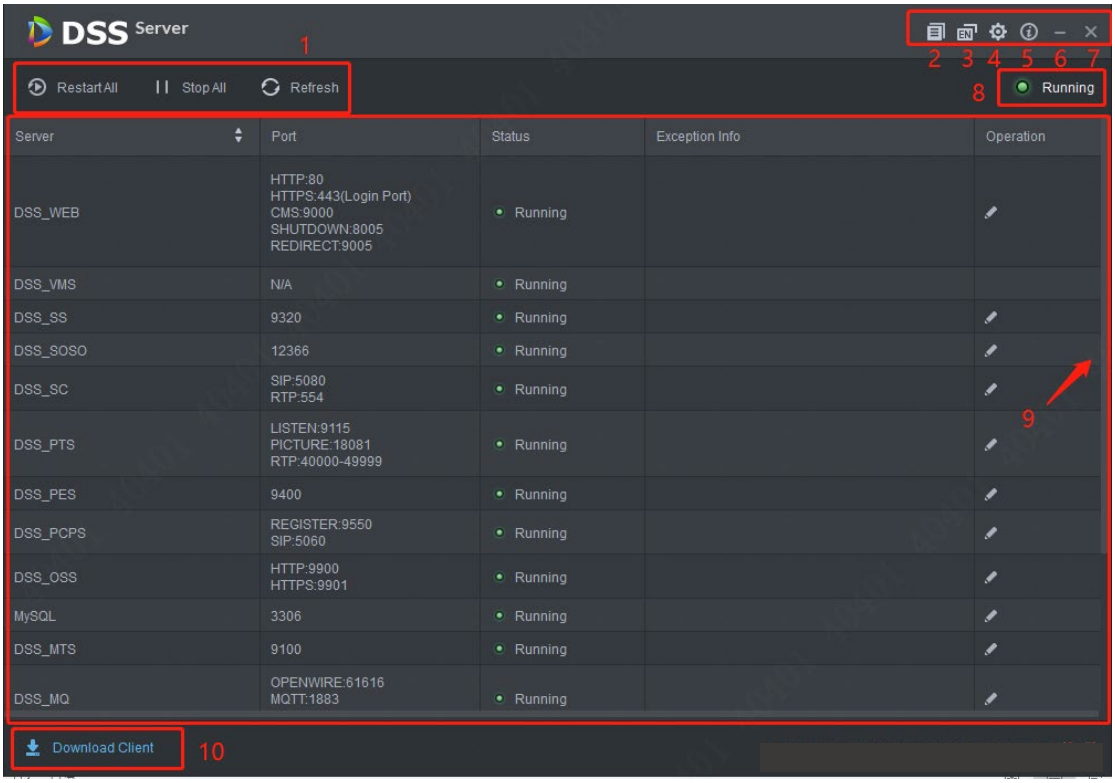
2)　「I have read and agree the DSS agreement」を選択して、「next」をクリックします。



3) 「Browse」をクリックして、インストールパスを選択、「install」をクリック。

4) システムはインストールの進捗を表示していて、5~10 分がかかります。

5) 「Run」をクリックして、下記のようにサーバーのメイン画面が表示されます。



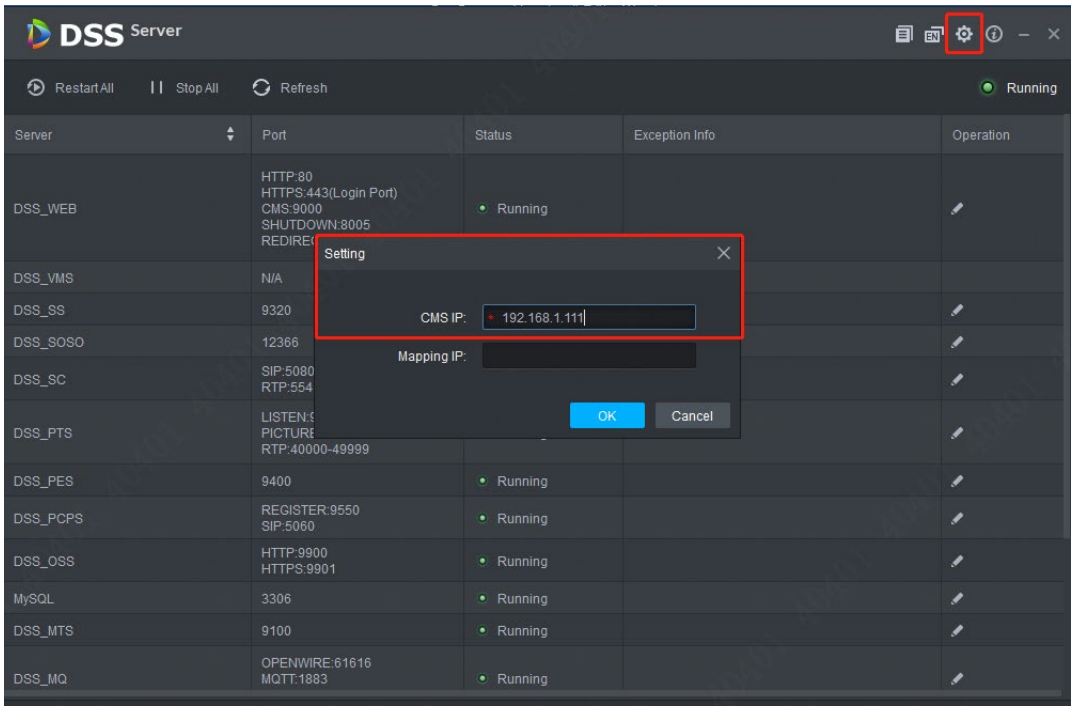
6) モジュール説明

No.	機能	説明
1	サービス管理	□ □ Restart All をクリックして、全てのサービスを再起動します。 □ □ Stop All をクリックして、全てのサービスを停止します。 □ □ Restart All をクリックして、全てのサービスを刷新します。
2	マニュアル	アイコンをクリックして、DSS ユーザーマニュアルを取得します。
3	言語	アイコンをクリックして言語を切り替えます。
4	設定	CMS IP をサーバー IP アドレスとして設定します。
5	について	このアイコンをクリックして、ソフトウェアのバージョンが表示されます。
6	最小化	画面最小化にします。
7	閉じる	ツールを閉じます。
8	サーバーの状態	□ Starting サービス起動中。 □ Unavailable サービス異常。 □ Stopping サービスが停止しています。 □ Running 全てのサービスが正常に実行されています。 □ Stopped 全てのサービスが停止します。
9	ディスプレイ	各サービスの詳細と状態を表示します。をクリックしてサーバーポートを変更できます。変更する場合、システムが自動的に再起動します。

10	クライアントダウンロード	Download Client をクリックして、Web 端画面に入り、DSS クライアントをインストールできます。

2、DSS Express クライアントをインストール

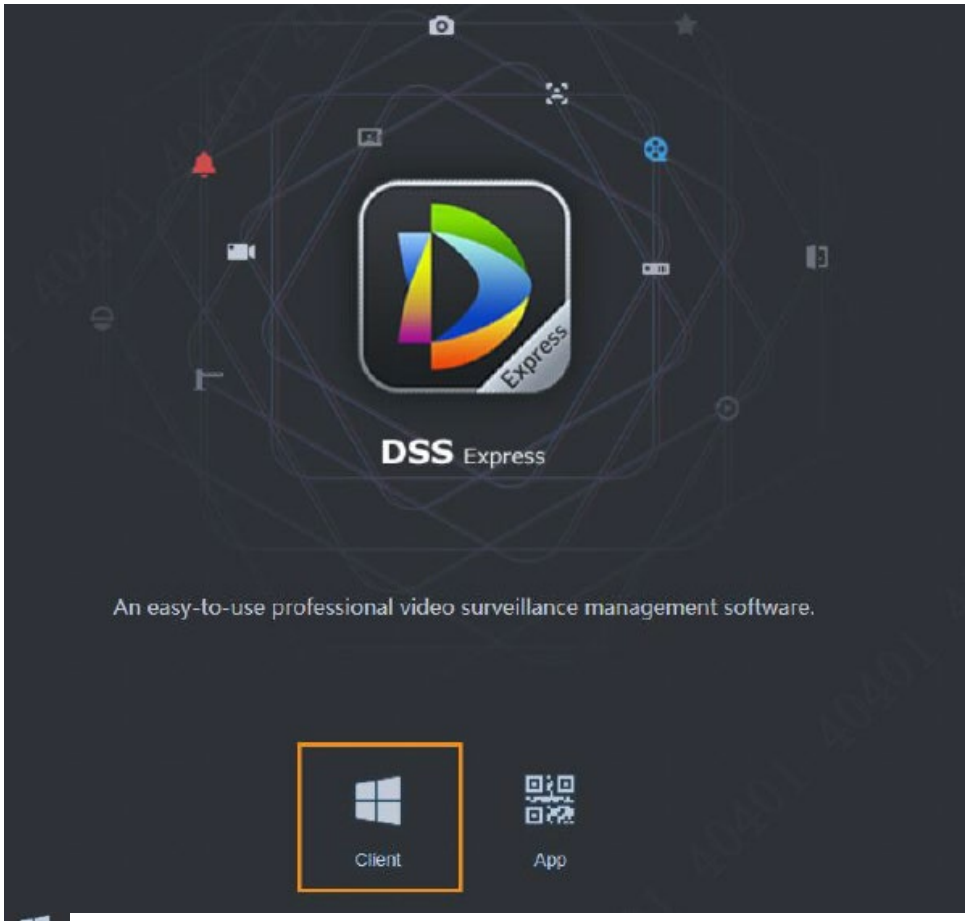
① をクリックして、CMS IP に PC の IP を入力します。



② 右上が Running になると、左下の Download Client をクリック、Web 端画面に入ります。

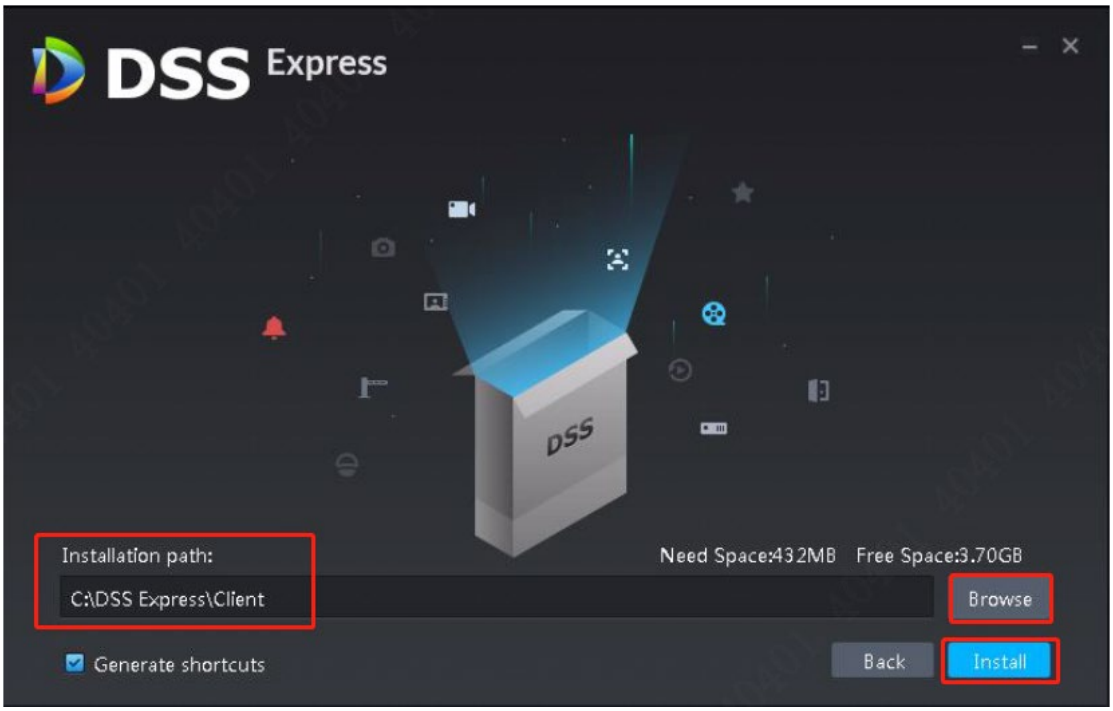
※下記のような安全提示が出来る場合、「高級」をクリックして、「引き続き」をクリックします。

表示される画面の「詳細」>「Web ページへ移動(非推奨)」をクリックします



をダブルクリックして、DSS クライアントをダウンロードします。

③ 「I have read and agree the DSS agreement」を選択、「next」をクリックします。

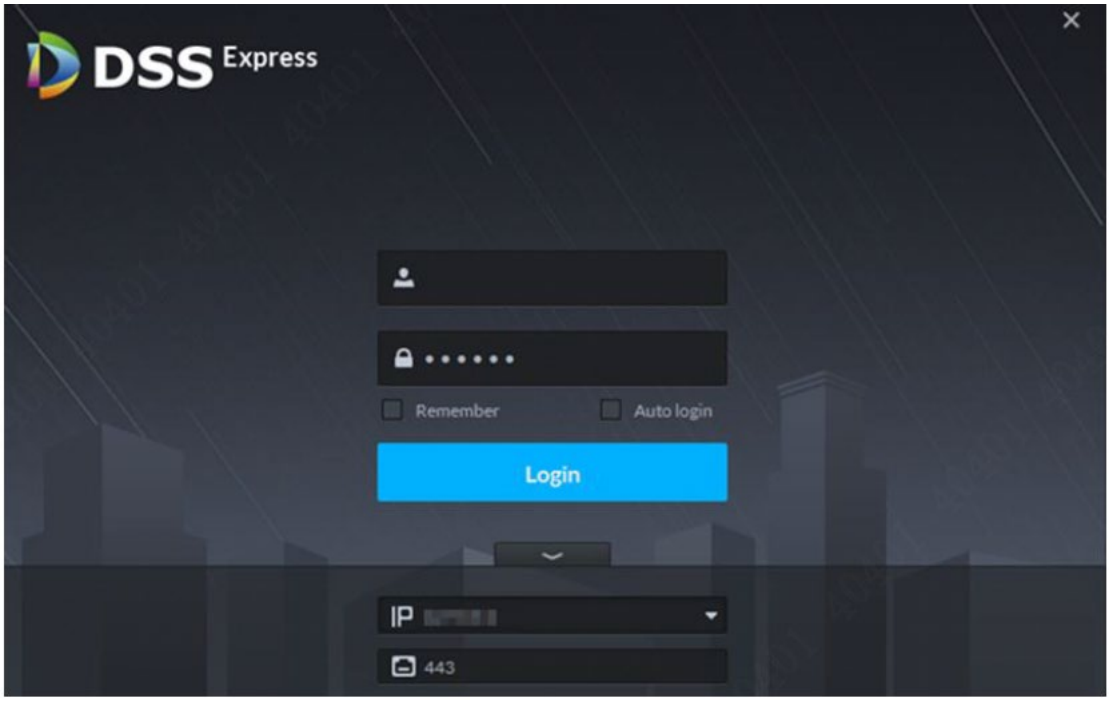


④ 「Browse」をクリックして、インストールパスを選択、「install」をクリック。

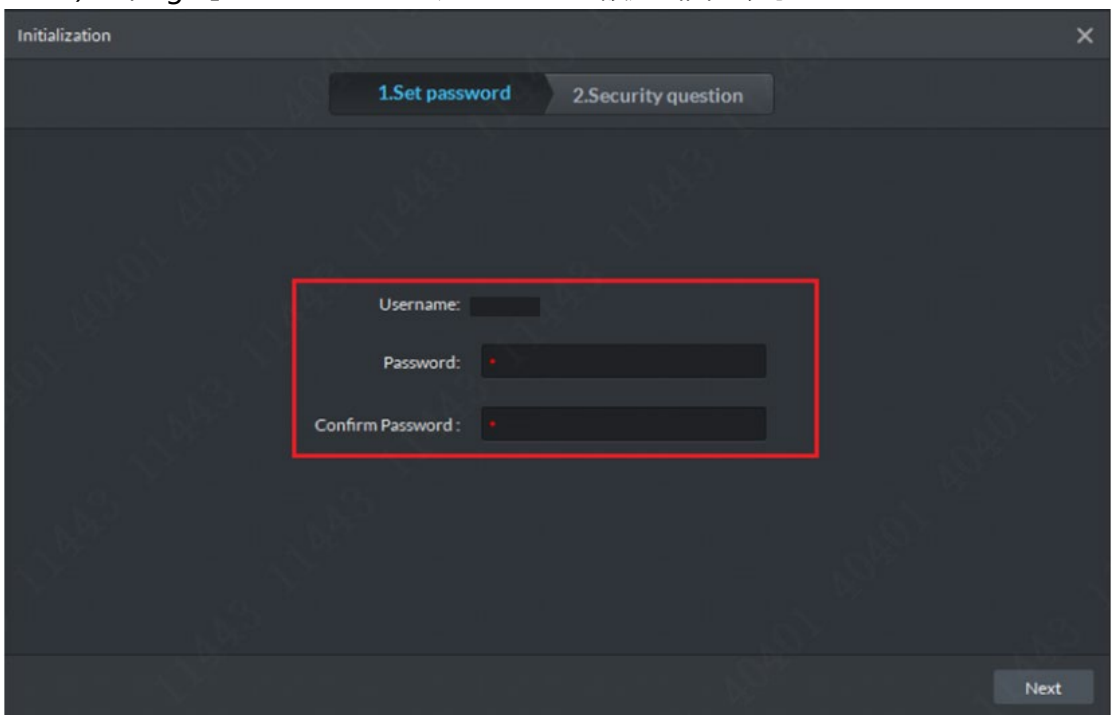
⑥ 3~5 分かかって、DSS クライアント をインストール完了。

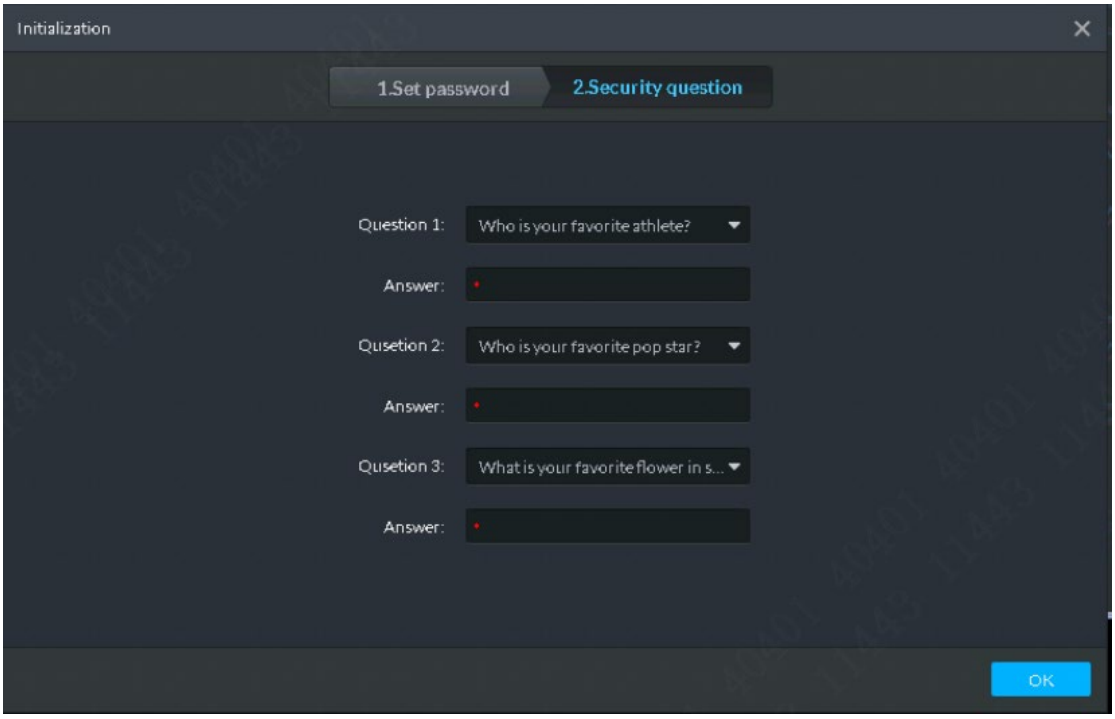
⑦ DSS クライアント初期化設定

1) 「Run」をクリックして、或いは をダブルクリックして、ログイン画面が表示されます。



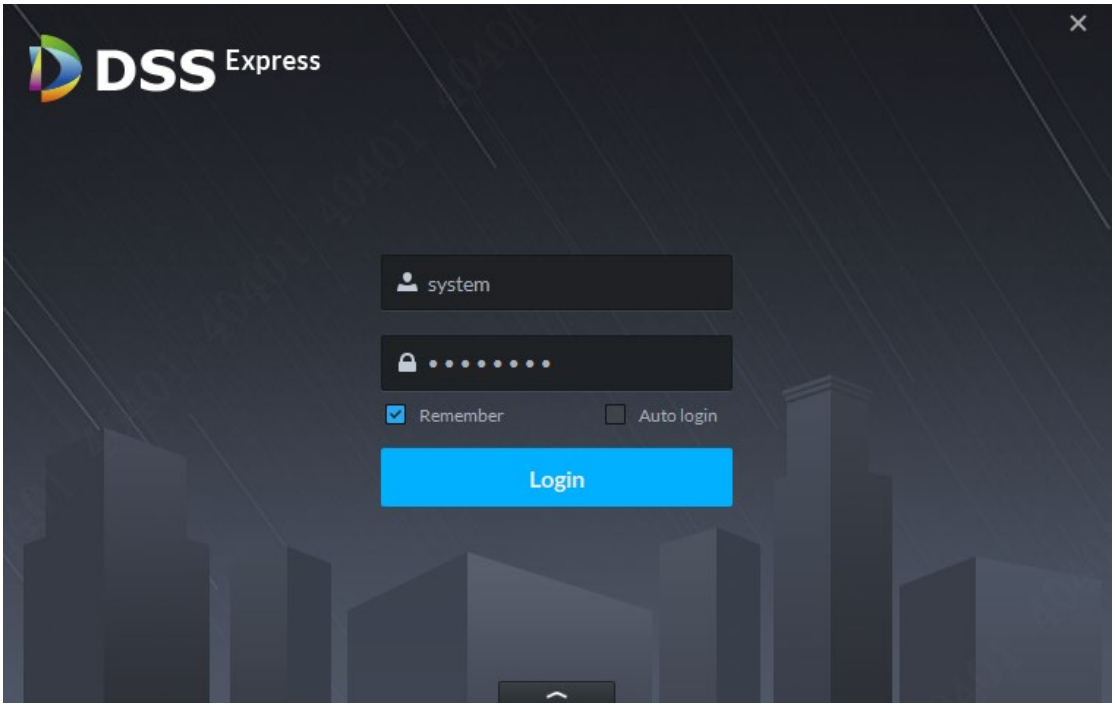
2) ユーザ名とパスワードを入力します。
3) 出荷時のデフォルトのユーザ名は system で、パスワードは 123456 です。
4) [redacted]をクリックして、サーバーの IP と HTTP ポート番号を入力します。
HTTP ポートはデフォルトで 443 です。
5) 「login」をクリックして、パスワード設定画面が表示されます。



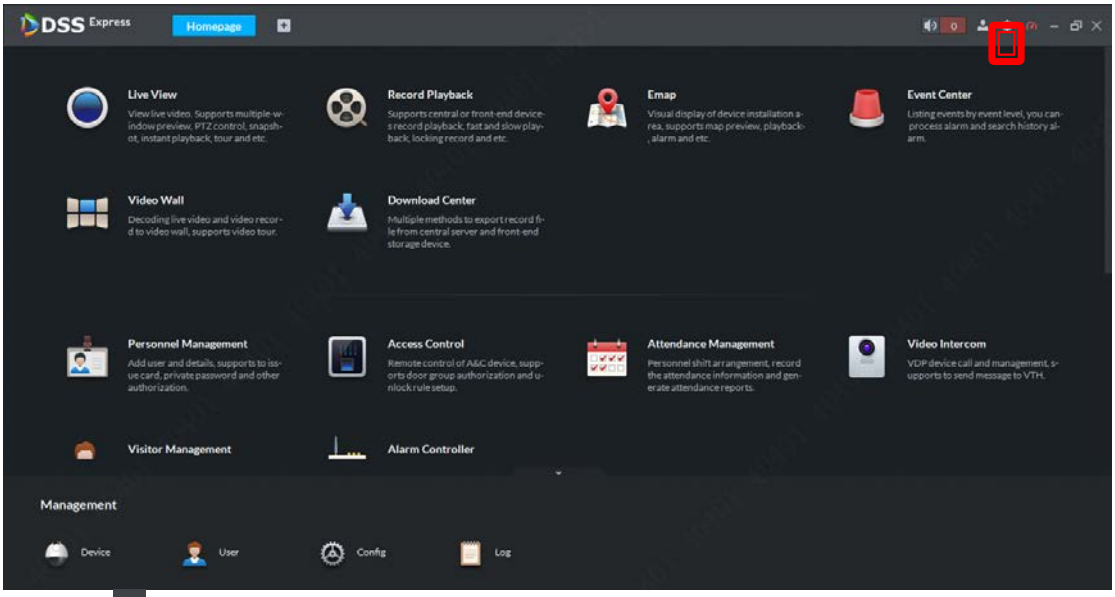


6) ユーザー名、パスワード、問題と回答を入力して、「OK」をクリックします。

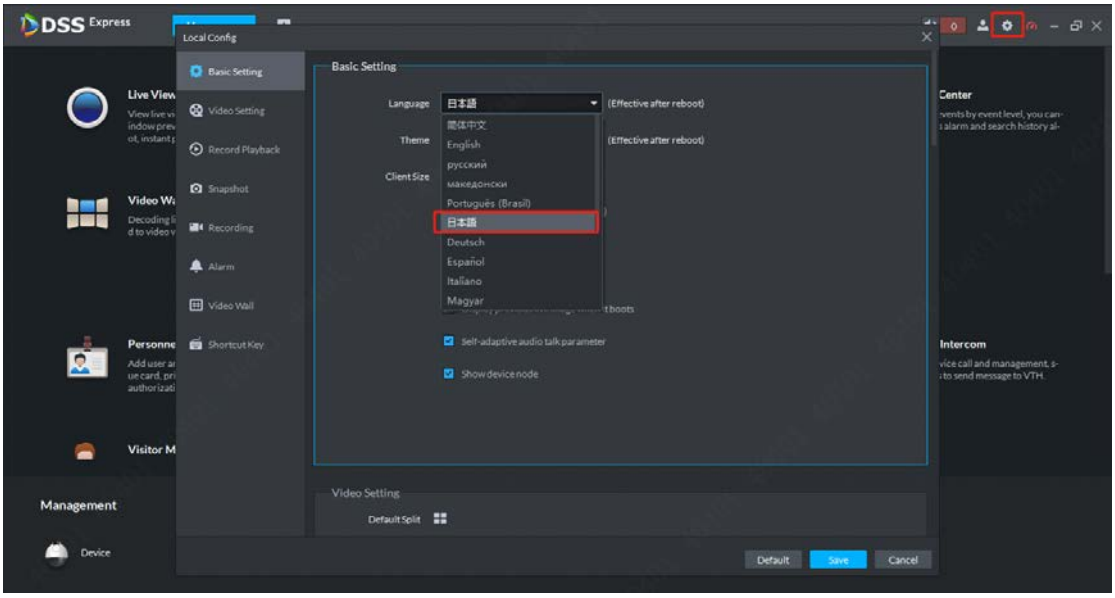
7) デスクトップの  をダブルクリック、「login」をクリックします。



8) 登録完了。

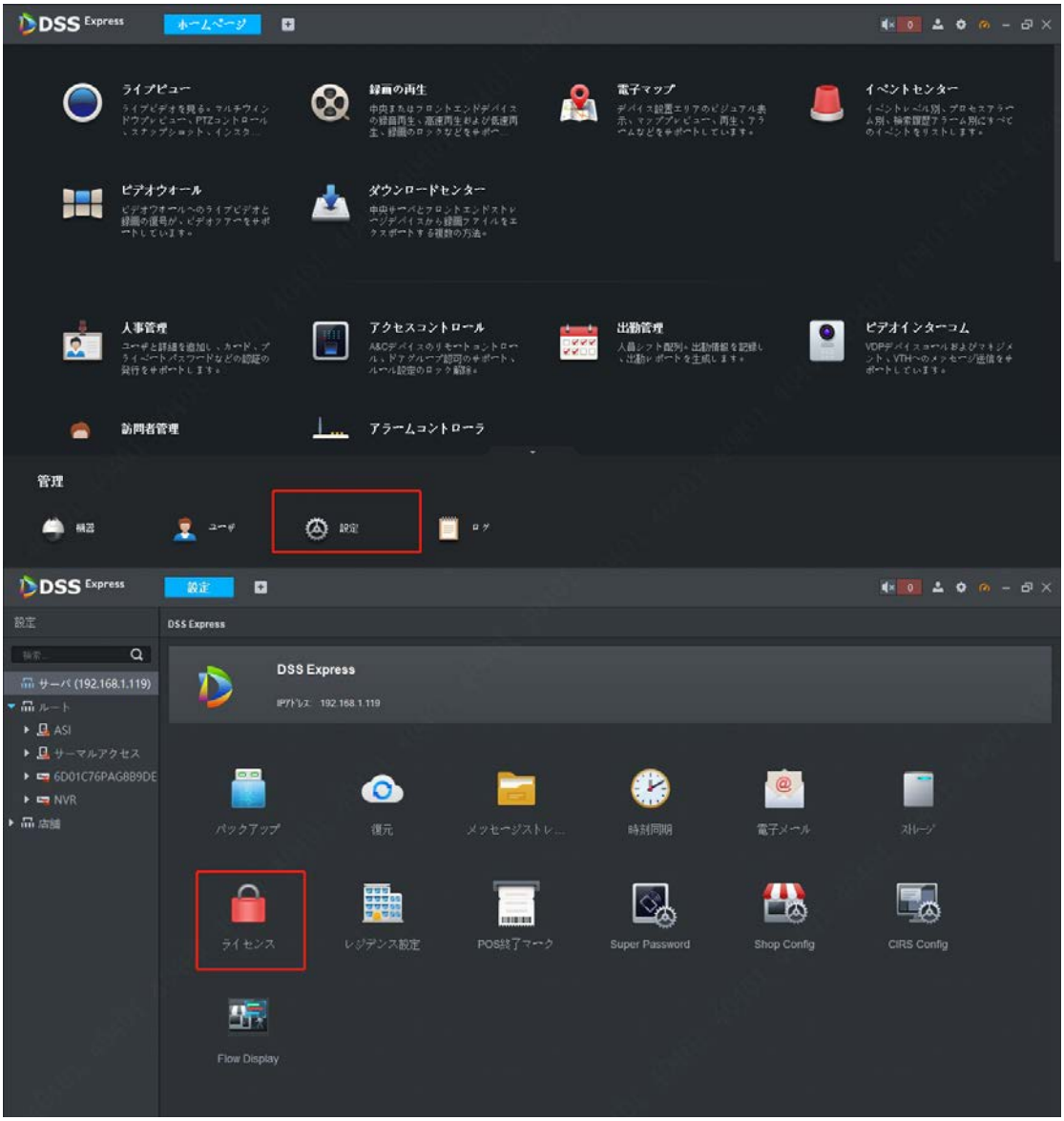


8) をクリックして、「language」で日本語に切り替えて、再起動します。



3、ライセンス導入 ※有償オプション

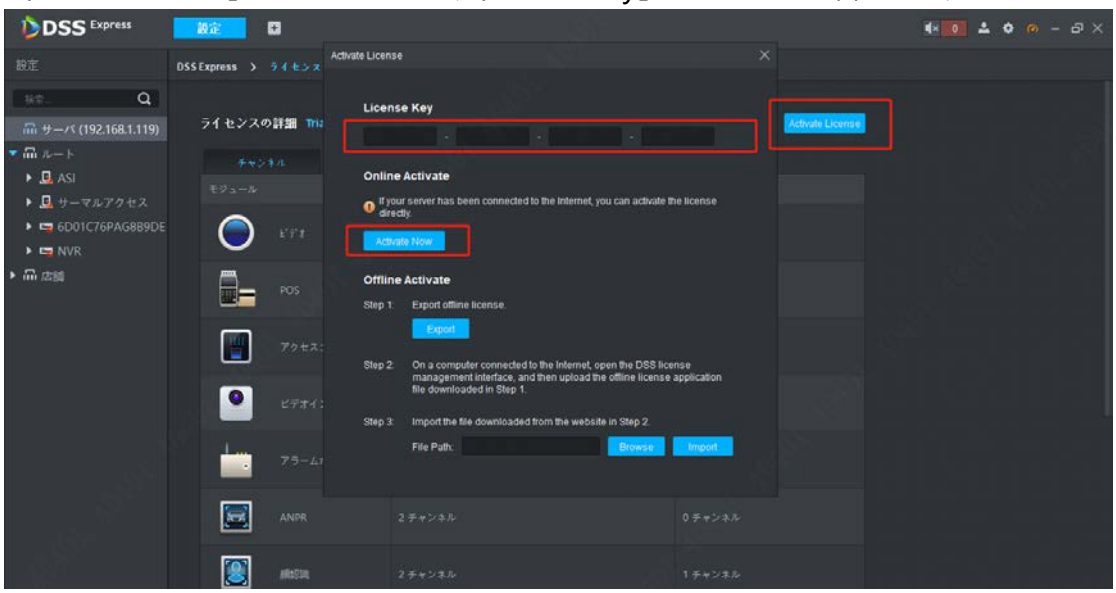
① ライセンスを受け取った場合、「設定」の画面で「ライセンス」をダブルクリックします。



② ライセンスをオンライン導入

※online 導入の場合、ネットワークと接続する必要があります。

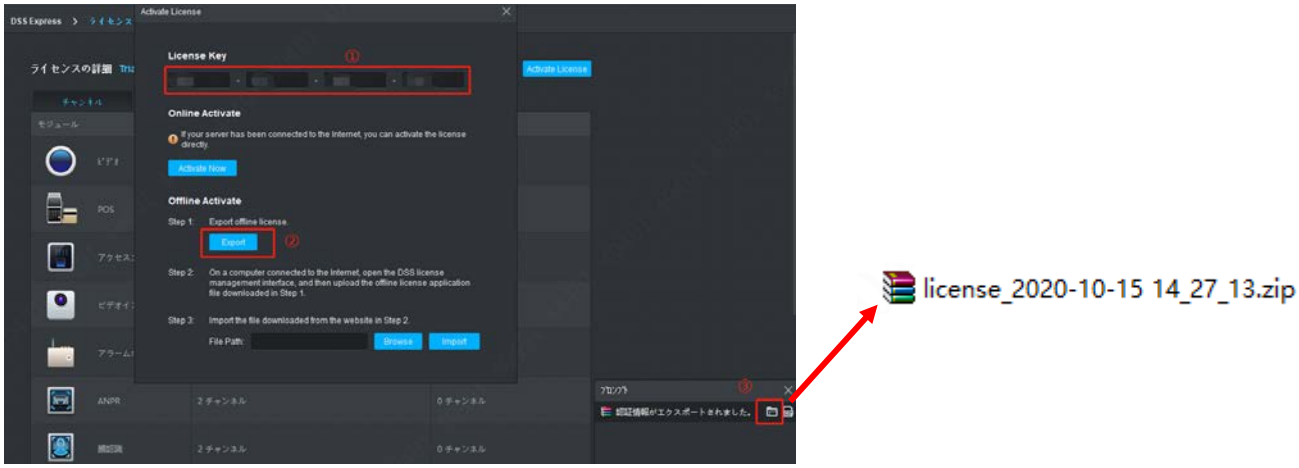
a.「Active License」をクリックして、「license key」でライセンス番号を入力します。



b.「Active now」をクリック、導入完了。

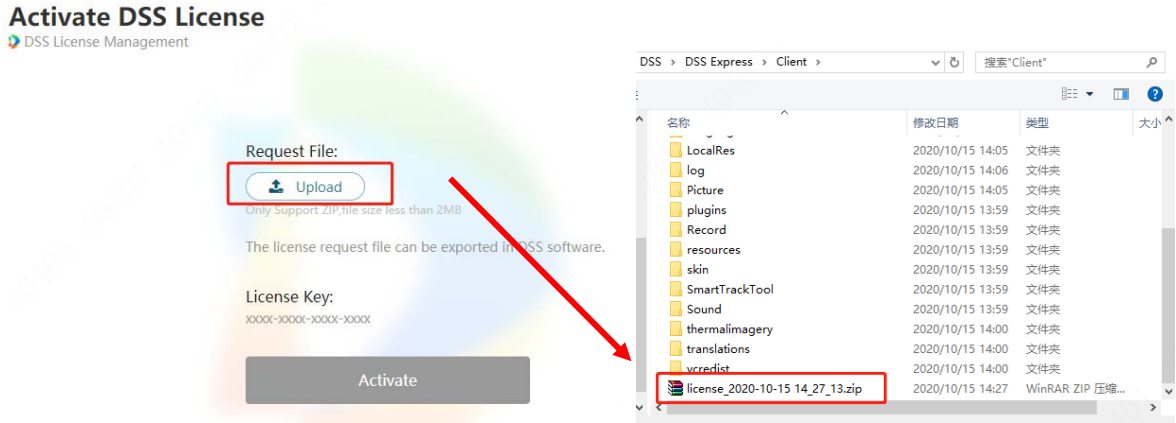
③ ライセンスをオフラインで導入

a.「license key」でライセンス番号を入力して、「export」をクリックします。認証情報の Zip ファイルがエクスポートされます。

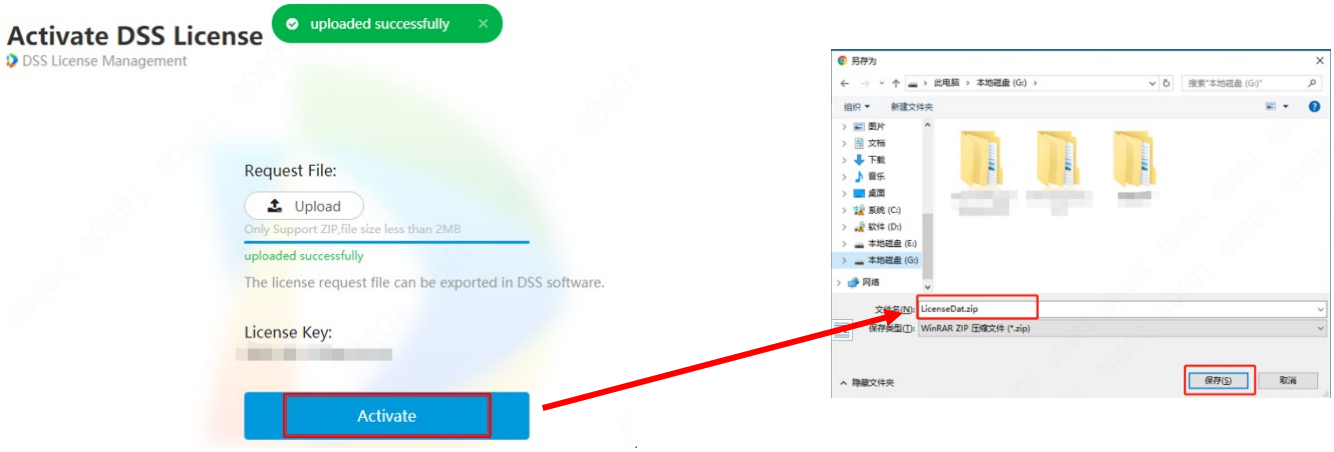


b. 受け取ったライセンスファイルを開いて、「Offline Activation Link」をクリック、次の画面で「activate license」をクリックします

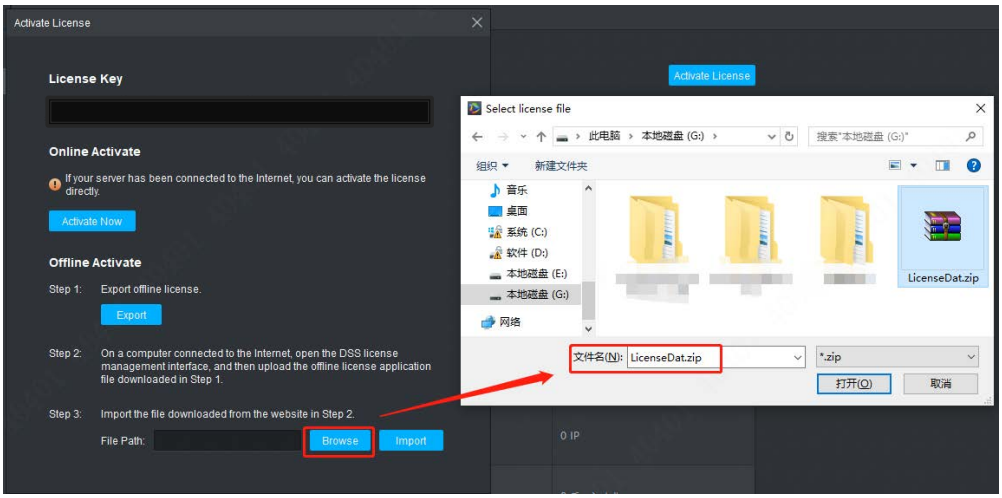
c.「upload」をクリック、さっきエクスポートされた zip ファイルを選択して、「開く」をクリックします



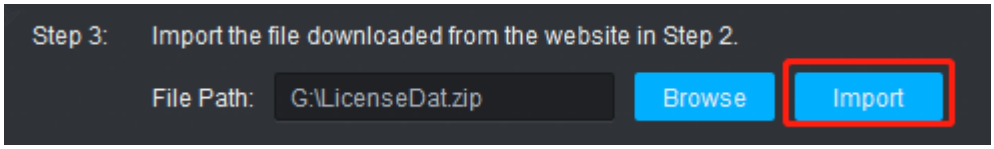
d．アップロード完了後、「Activate」をクリック、「licenceDat.zip」というファイルをエクスポートします



e．「step3」でエクスポートされた「licenceDat.zip」を選択

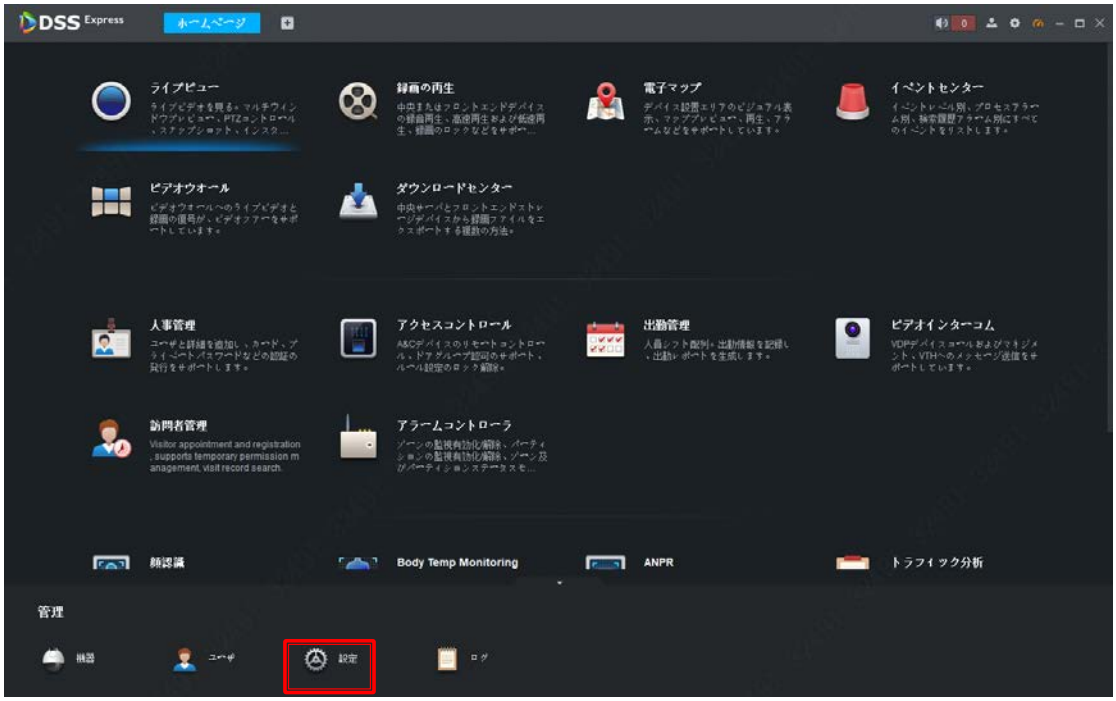


f．「import」をクリックして、ライセンスオンライン導入完了

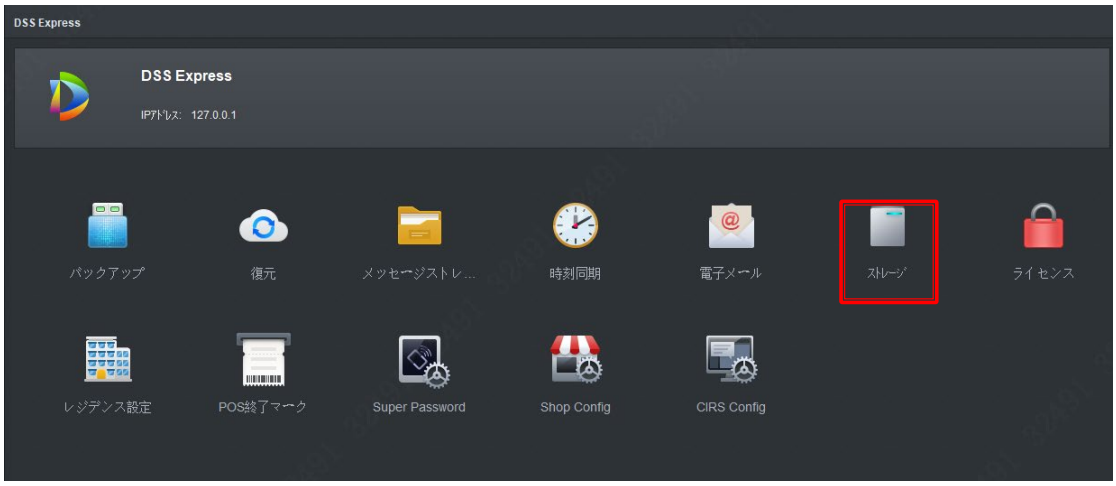


4、Express のストレージ設定

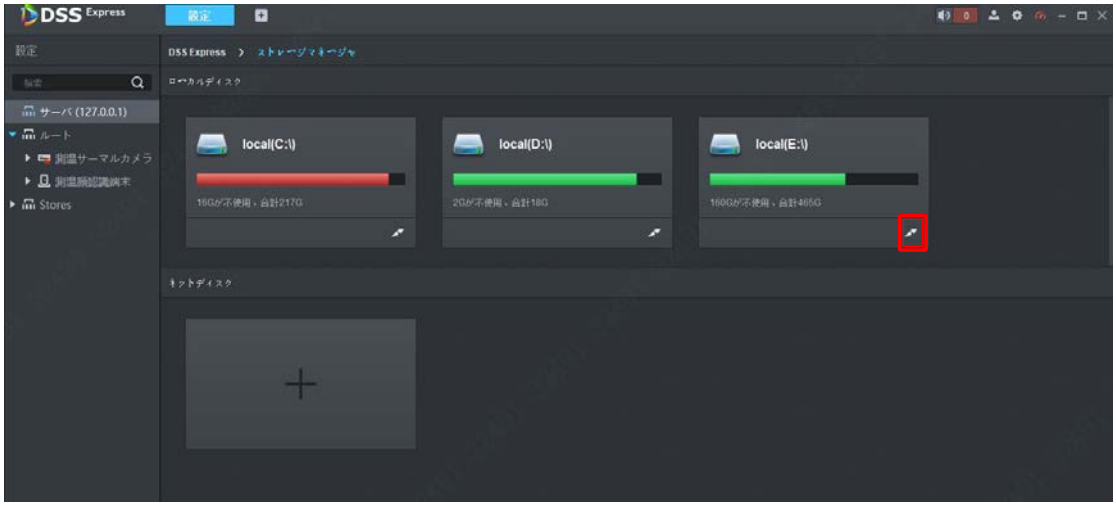
①　「ホームページ」画面で「設定」をクリックします



② 「ストレージ」をクリックします

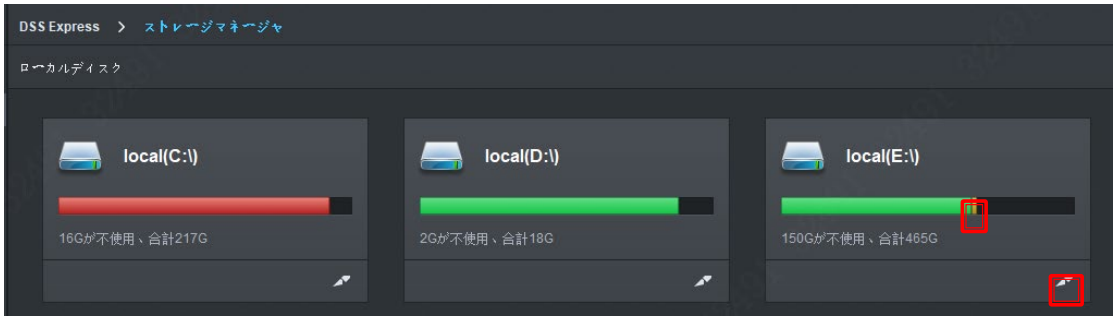


③ 画像、或いはビデオを保存したディスクの右下のアイコンをクリックします



④ ストレージサイズを設定して、プルダウンメニューから「ビデオ」を選択します。「√」で保存します

⑤ 先設定したビデオストレージの色が黄色になったら、もう一度右下のアイコンをクリックします



⑥ サイズを設定して、タイプを「一般写真」に設定して、保存します

⑦ 設定完了

五、入退管理（DSS Express)

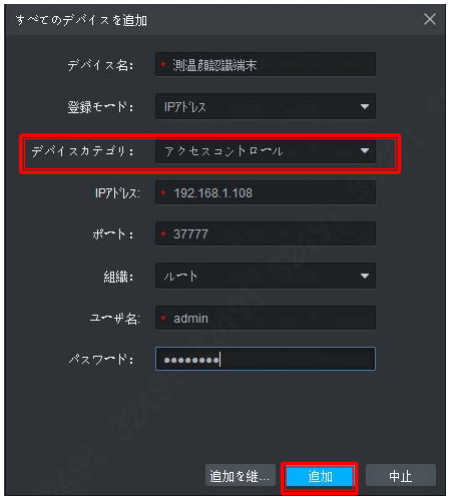
ASI7213X-T1/ ASI7213Y-T1 は DSS Express 管理ソフトと一緒に使うことが出来ます。DSS Express で ASI7213X-T1/ ASI7213Y-T の人員管理、イベント連携、解錠記録確認など操作が出来ます。

1、アクセス端末追加

① 「ホームページ」画面で「機器」をクリックします

② 「追加」ボタンをクリックして、機器の情報画面を呼び出します

③ 必要の情報を入力して、カテゴリを「アクセスコントロール」に設定して、「追加」ボタンをクリックして、機器を追加します。



④ 機器を追加した後は機器の編集ボタンを押します

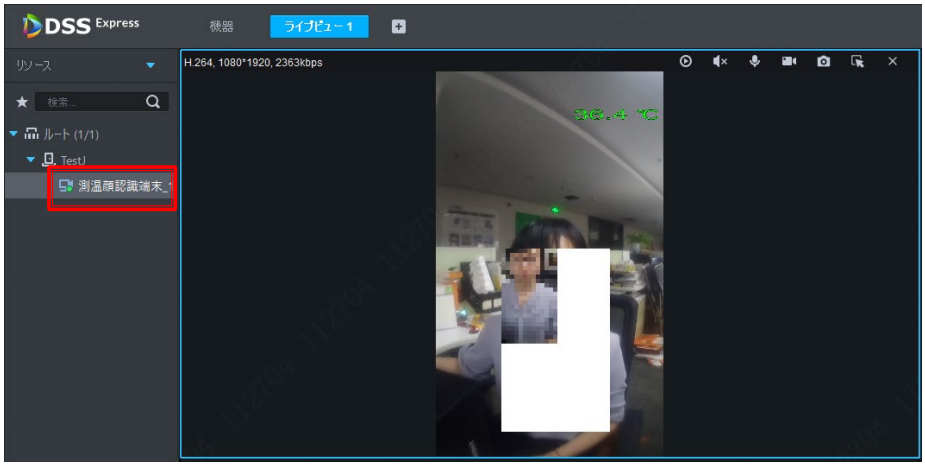
⑤ タグ「ビデオチャンネル」を選択して、チャンネル番号に「1」を入力して、特徴の項目に「IVS アラーム」と「顔検出」を設定します。

⑥ アクセス端末のライブ映像確認

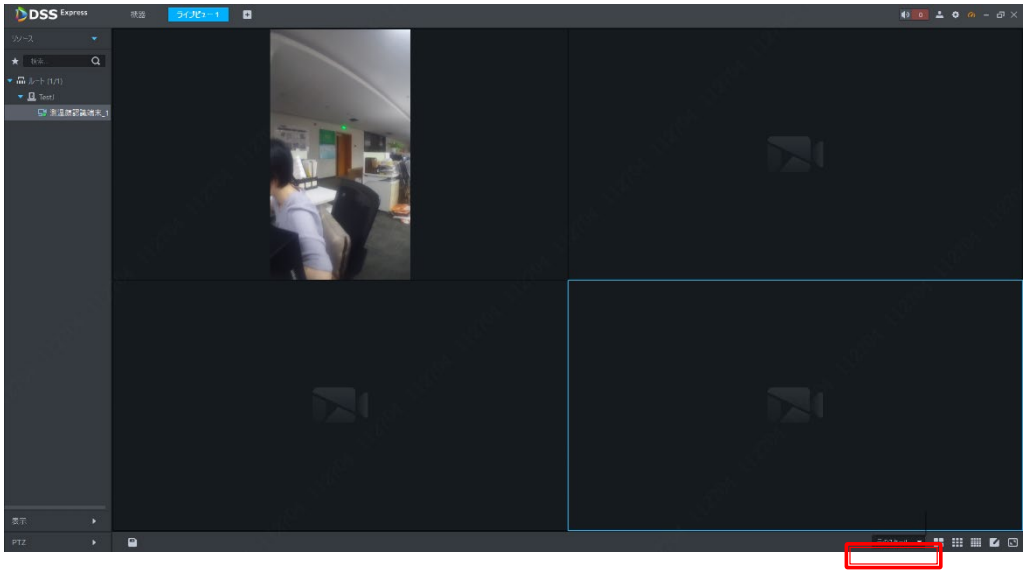
1) 「+」ボタンで新しい「ホームページ」を開けます

2) 「ライブビュー」をクリックします

3) アクセス端末のチャンネルをダブルクリックして、ライブ映像が表示されます



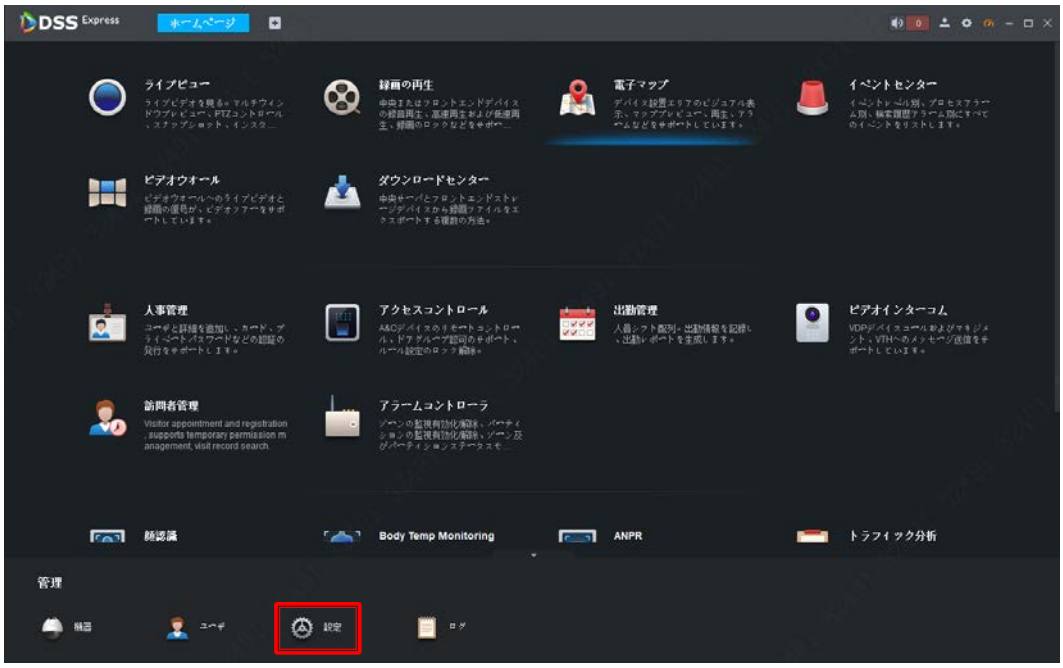
4) 右下のドリップダウンメニューをクリックして、「元のスケール」を選択して、端末と同じスケールで表示できます。



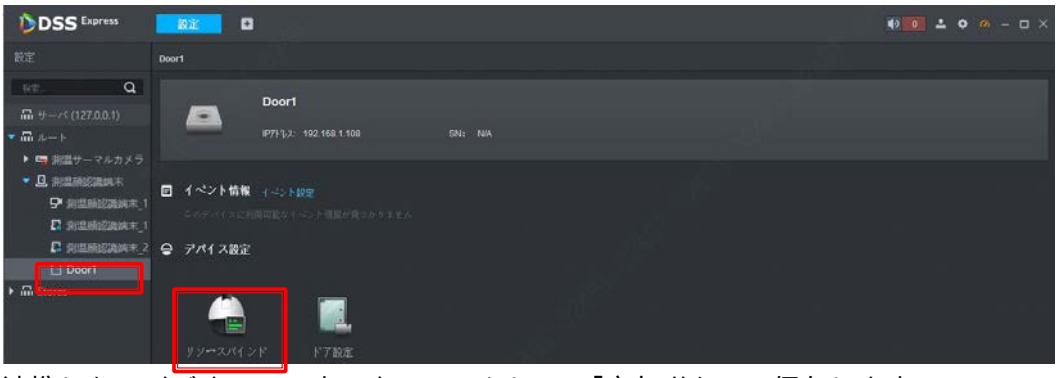
2、アクセス端末設定

① アクセス端末とビデオチャンネルの紐付き（解錠イベントでリアルタイム映像確認用）

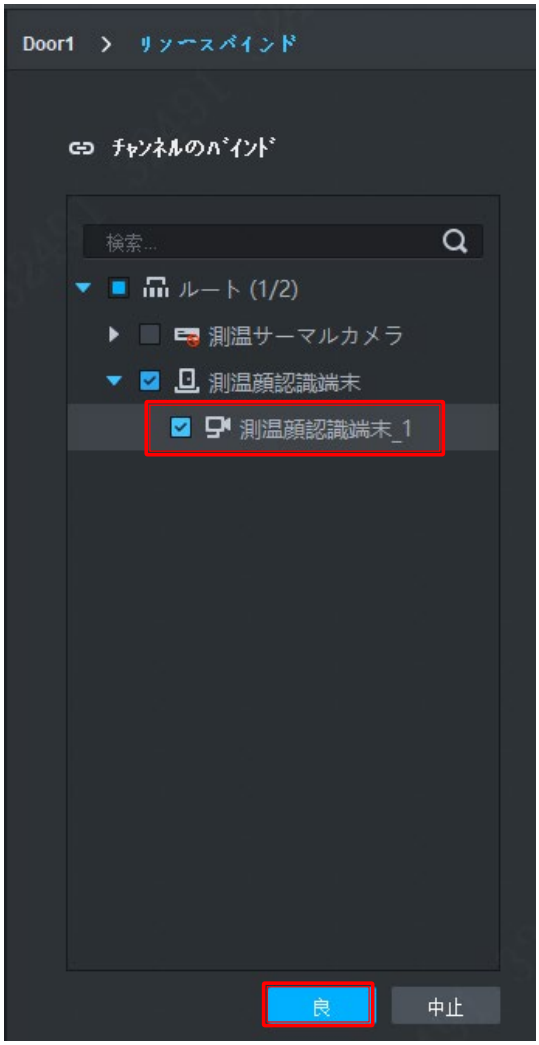
1) 「ホームページ」画面で「設定」をクリックします



2) 機器一覧からアクセス端末を選択して、展開された項目に「Door1」を選択します。右の画面の「リソースバインド」をクリックします。



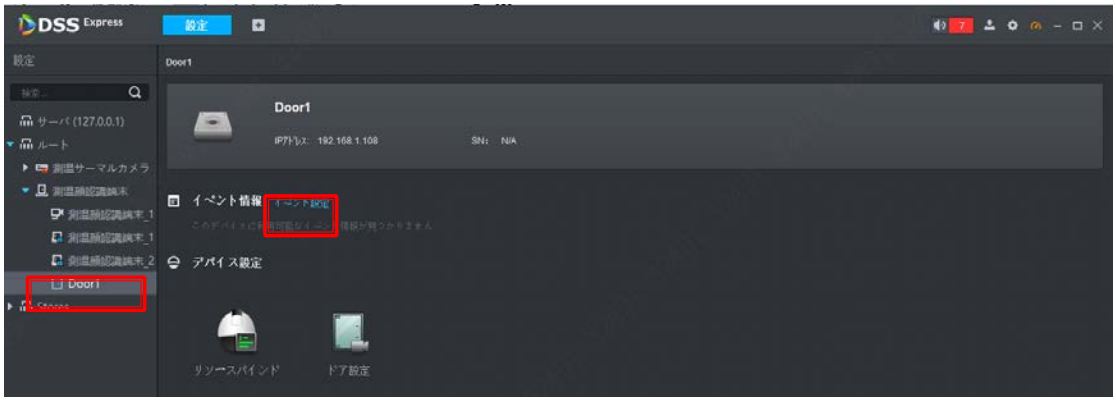
3) 連携したいビデオチャンネルをチェックして、「良」ボタンで保存します



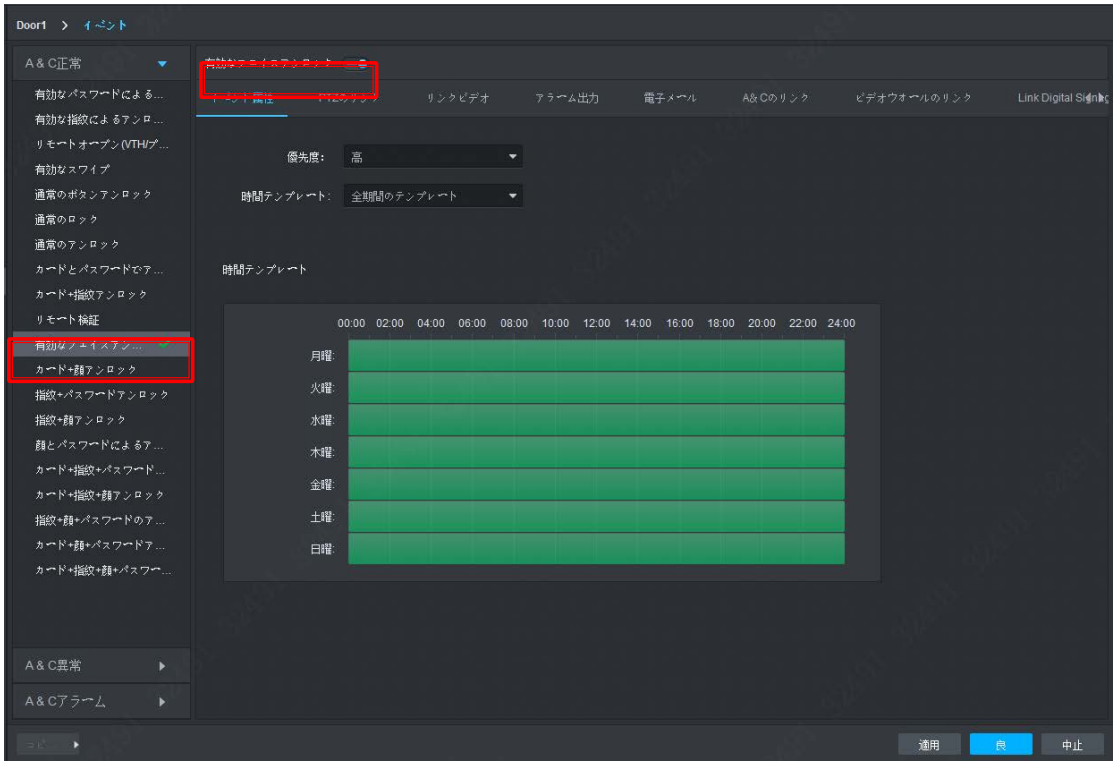
4) 設定完了

② 解錠録画とスナップショット設定（顔認識解錠が例として説明します）

1) 「Door1」を選択して、「イベント設定」を選択します

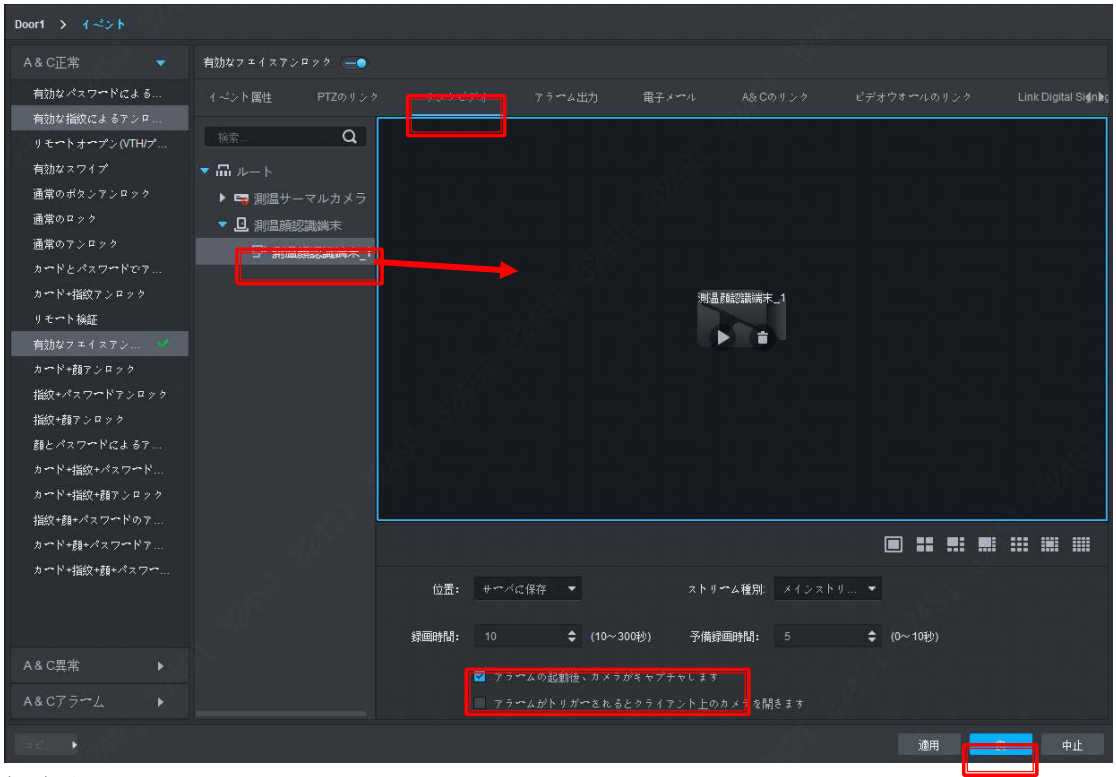


2) 「A&C 正常」で「有効なフェイスアンロック」を選択して、有効します。



3) タグ「リンクビデオ」を選択して、映像表示エリアに保存したいビデオチャンネルをドラッグして、「アラームの起動後、カメラがキャプチャします」をチェックして、「良」で保存します。

※複数ビデオチャンネルの映像を保存したい場合は映像表示エリアしたの  で調整してください。

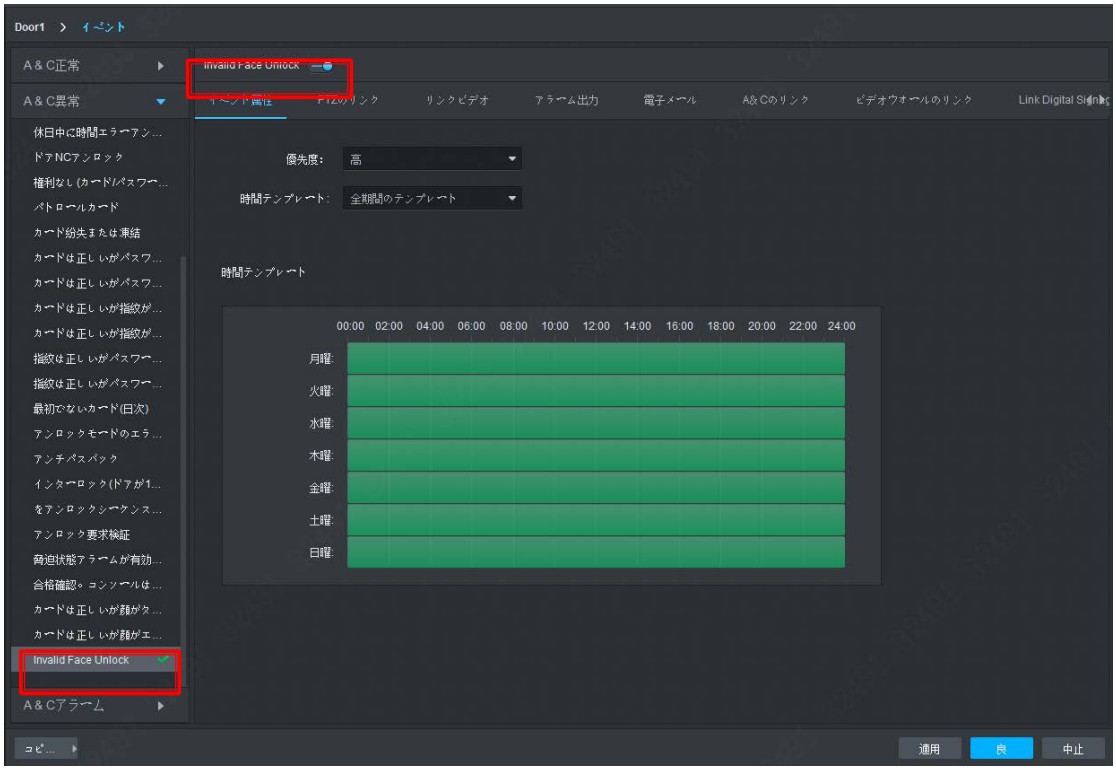


4) 設定完了

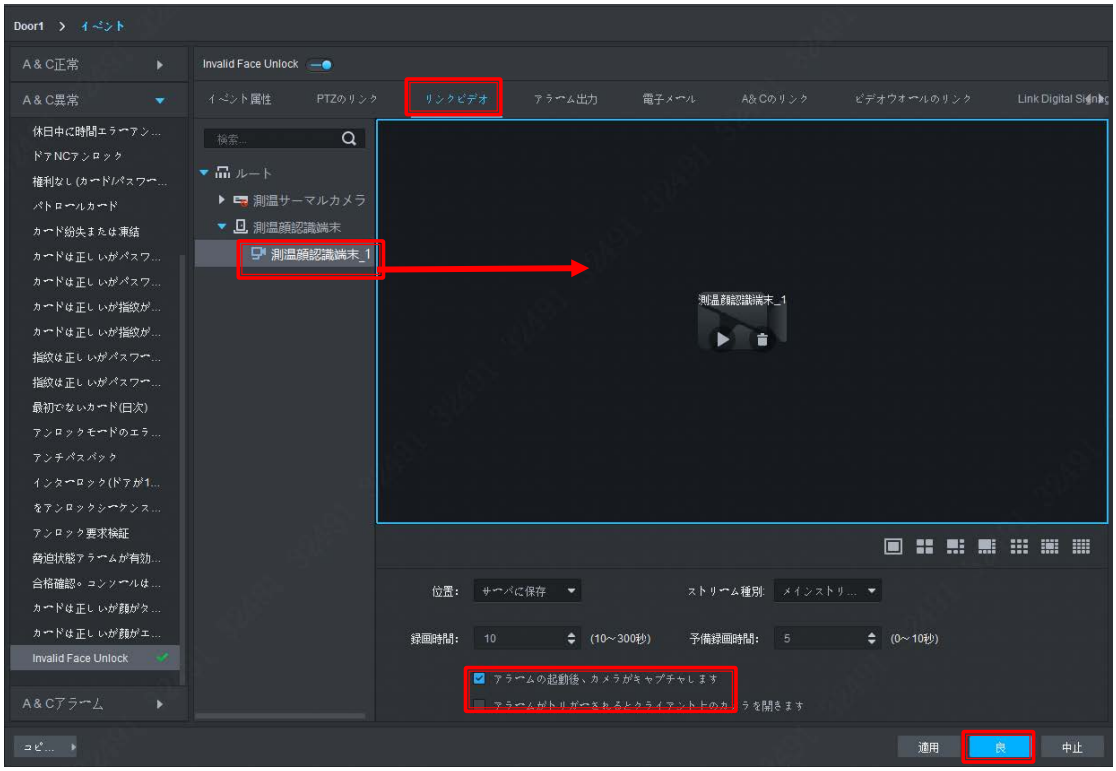
③ 異常イベント録画とスナップショット設定（体温異常など）

1) 「Door1」を選択して、「イベント設定」を選択します

2) 「A&C 異常」で「Invalid Face Unlock」を選択して、有効します。



3) タグ「リンクビデオ」を選択して、映像表示エリアに保存したいビデオチャンネルをドラッグして、「アラームの起動後、カメラがキャプチャします」をチェックして、「良」で保存します。

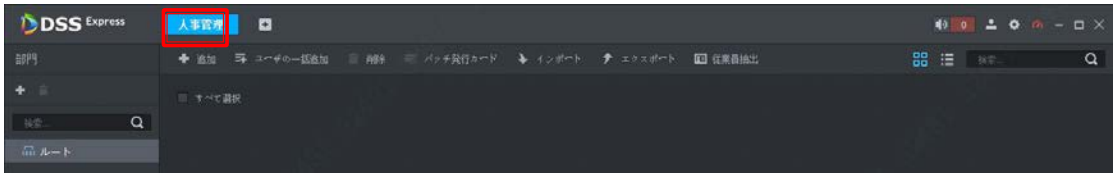


4) 設定完了

3、ユーザー追加

① 「ホームページ」画面で「人事管理」をクリックします

② 「追加」ボタンをクリックします

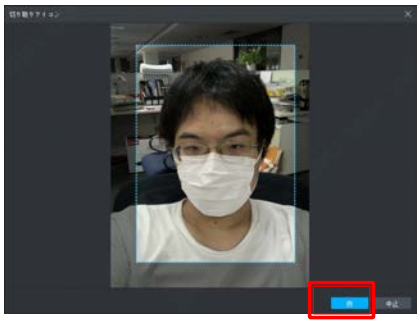


③ ユーザー情報を入力します。

1) ユーザー写真追加

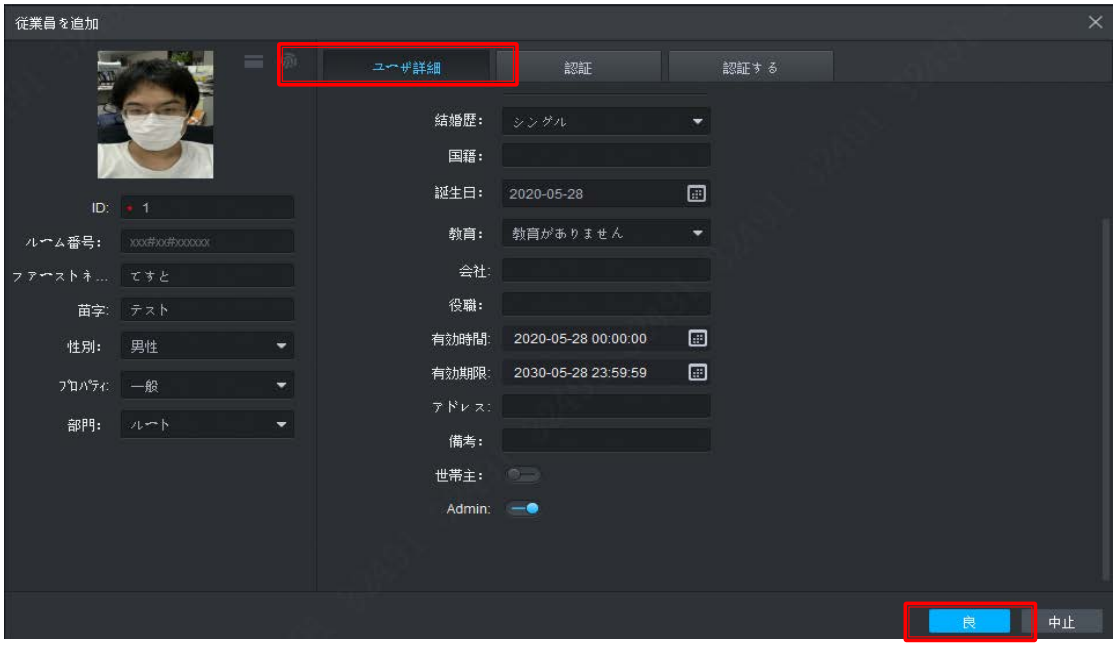
マウスをユーザー写真の枠に移動して、表示されたリンク「画像をアップロード」をクリックします。

PC からアップロードしたい写真を選択して、顔の部分を切り出して、「良」ボタンをクリックします



2) ユーザーの ID と他の必要の情報を入力します。

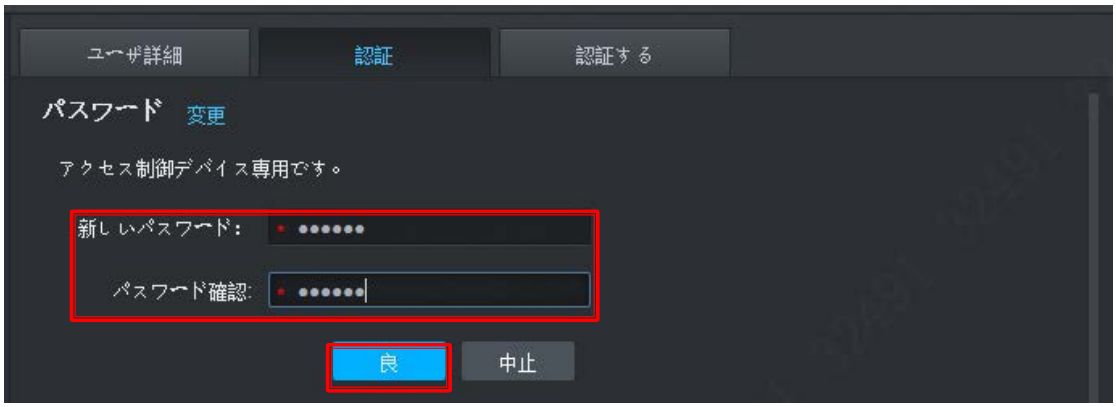
「ユーザー詳細」の一番下で「admin」項目があります、この項目をチェックすると、このユーザーが機器本体で設定の変更ができます。



3) ユーザーの解錠パスワードを設定します

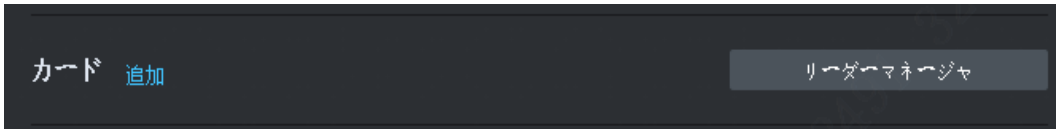
「認証」タグを選択して、「変更」をクリックします

パスワードと確認用のパスワードを入力して、「良」ボタンで保存します。

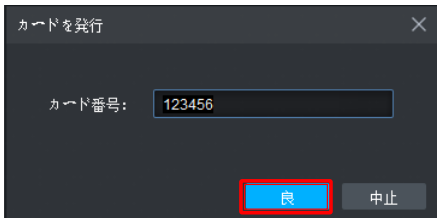


4) ユーザーの解錠カードを追加します

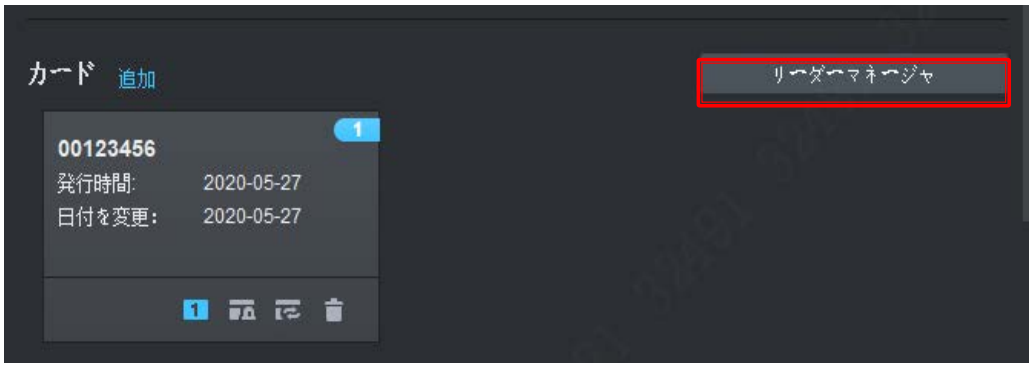
i. カード番号がわかる場合は「追加」をクリックします



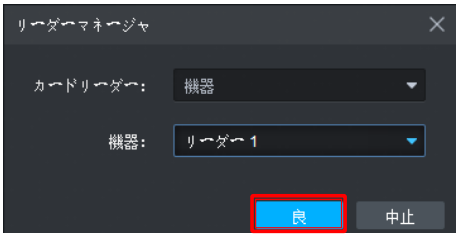
手動カード番号を入力して、「良」ボタンで保存します。



ii. カード番号が分からない場合は右の「リーダーマネージャ」をクリックします

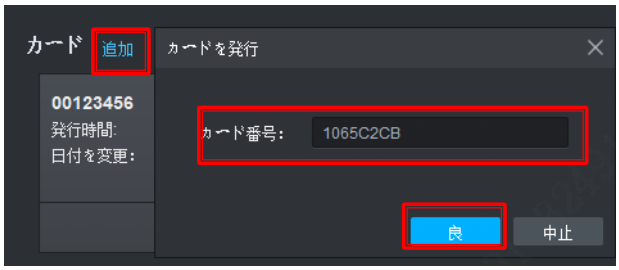


追加されたアクセス端末の「リーダー1」を選択して、「良」ボタンで保存します。



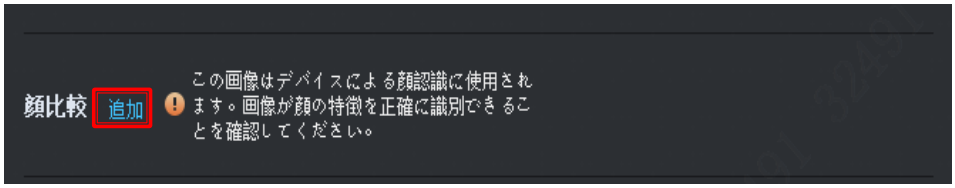
もう一度「追加」をクリックして、次の画面が出る時はカードをアクセス端末のリーダーでスキャン

して、カード番号を読み込みます。「良」ボタンで保存します。

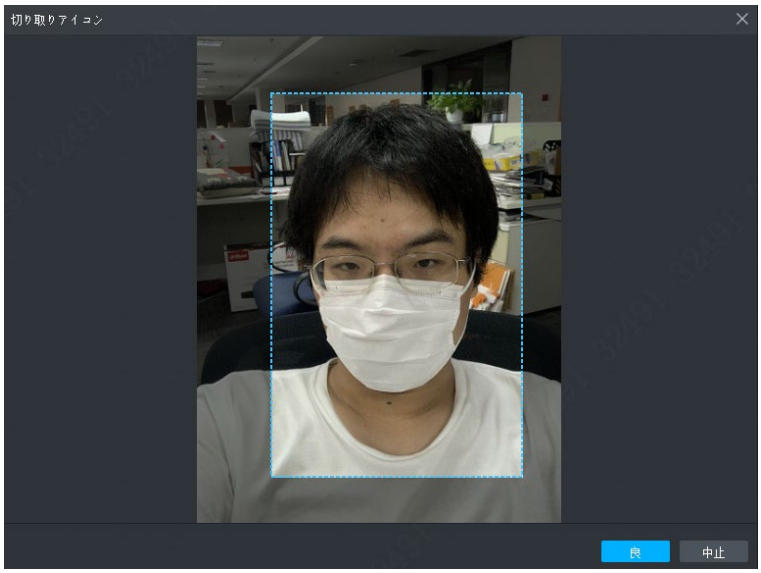


5) ユーザーの解錠用の顔情報を登録します。

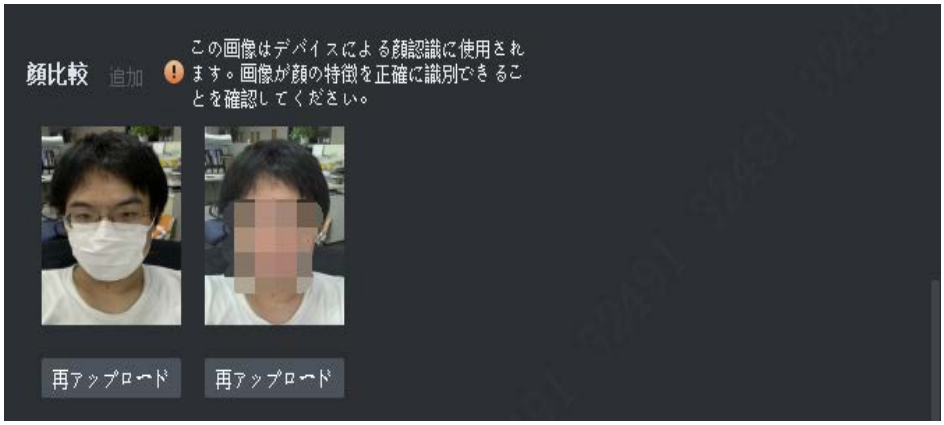
i. 「追加」をクリックします



ii. PC からユーザーの写真を選択して、顔の部分を切り出して、「良」ボタンで保存します。



iii. 一つユーザーは二枚の写真（マスク有/無）をアップロードできます

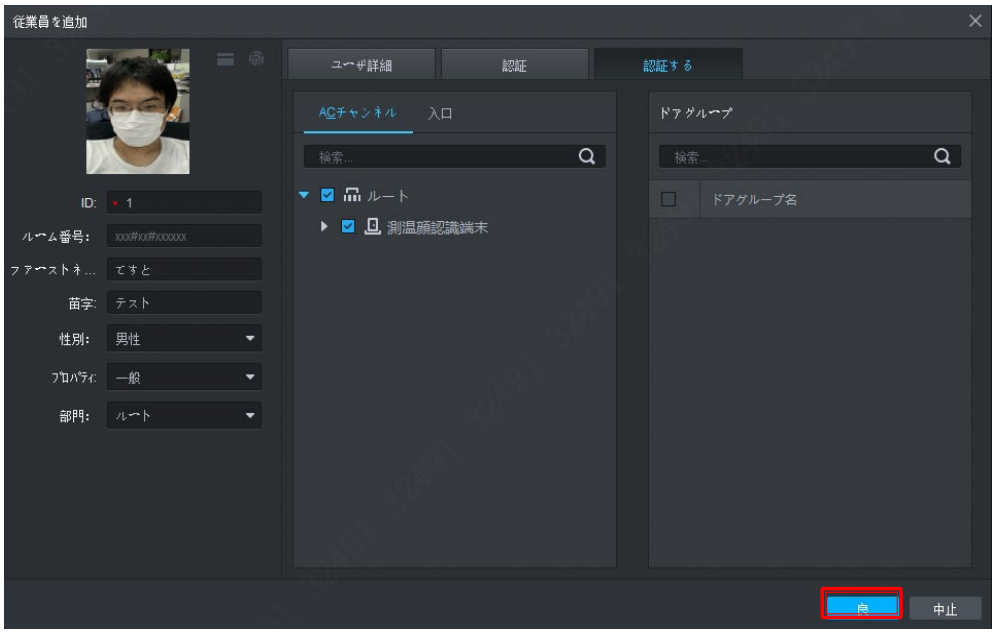


※アップロード写真の説明：写真は jpg ファイルが必要です。写真は 75kb 以下が必要、300x300≤解像度≤600x600（お勧め解像度は 500x500)。写真の中には最大一つの顔、顔の部分は写真全体の 2/3 を超えないこと、写真の比例は水平：垂直≤1：2。

6) ユーザー情報をアクセス端末に共有

「認証する」タグをクリックして、共有したい端末をチェックします

7) 「良」ボタンで保存します。



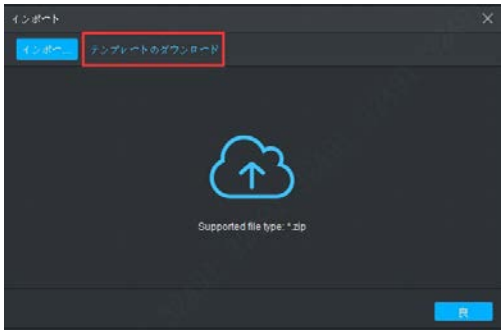
8) ユーザー追加完了

4、ユーザー一括追加

excel ファイルと写真ファイルを利用して、複数のユーザーを一括追加することができます。

① 「人事管理」の「インポート」をクリックします

② 「テンプレートのダウンロード」リンクでテンプレートをダウンロードします

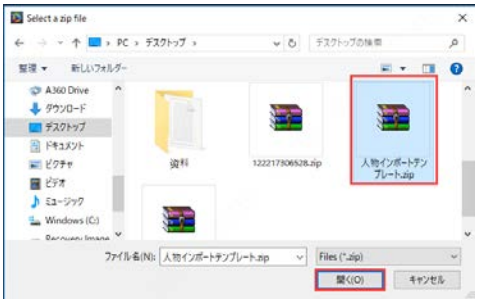


③ ダウンロードした zip ファイルに右クリックして、解凍します。
解凍されたフォルダー内、四つのファイルがあります。
「Person Import Template_ja.xlsx」はユーザーの情報ファイルです。
「Head.jpg」はユーザーが表示される時使う写真です。
「Face1.jpg」と「Face2.jpg」は認識用の写真です、一つユーザーは最大二枚アップロードできます。

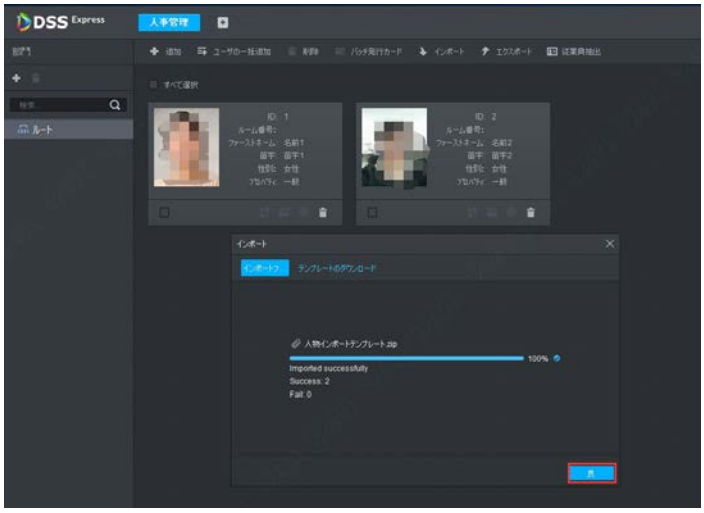
④ xlsx でユーザーの情報を編集して、写真はフォルダー内に置きます。

⑤ 編集完了のフォルダーを右クリックして、zip の圧縮ファイルを作ります。

⑥ 「インポートファイル」ボタンをクリックして、⑤で作られた zip を選択して、インポートします。



⑦ インポート成功したら下記の画面の様にユーザーの情報が表示されます。「良」ボタンでインポート画面を閉じます。



一括インポートされたユーザーの情報を認識端末に一括転送します。

⑧ 「ホームページ」で「アクセスコントローラ」をクリックします

⑨ 機能一覧から「アクセスレベル」を選択します

⑩ 「ドアグループ」で「追加」ボタンをクリックします

⑪ 「ドアグループ名」を入力して、「時間テンプレート」と「休日スケジュール」を設定して、同じグループをしたいアクセス端末をチェックして、「良」ボタンで新しいグループを作ります。

⑫ 「ドアルール」をクリックします

⑬ 「追加」ボタンをクリックします

⑭ 「ドアルール名」を入力して、ユーザーを選択して、ユーザー情報を同期したいドアグループを選択して、「良」ボタンで情報を同期します。

⑮ 情報同期完了したら、下記の画面が表示します

5、ユーザー編集

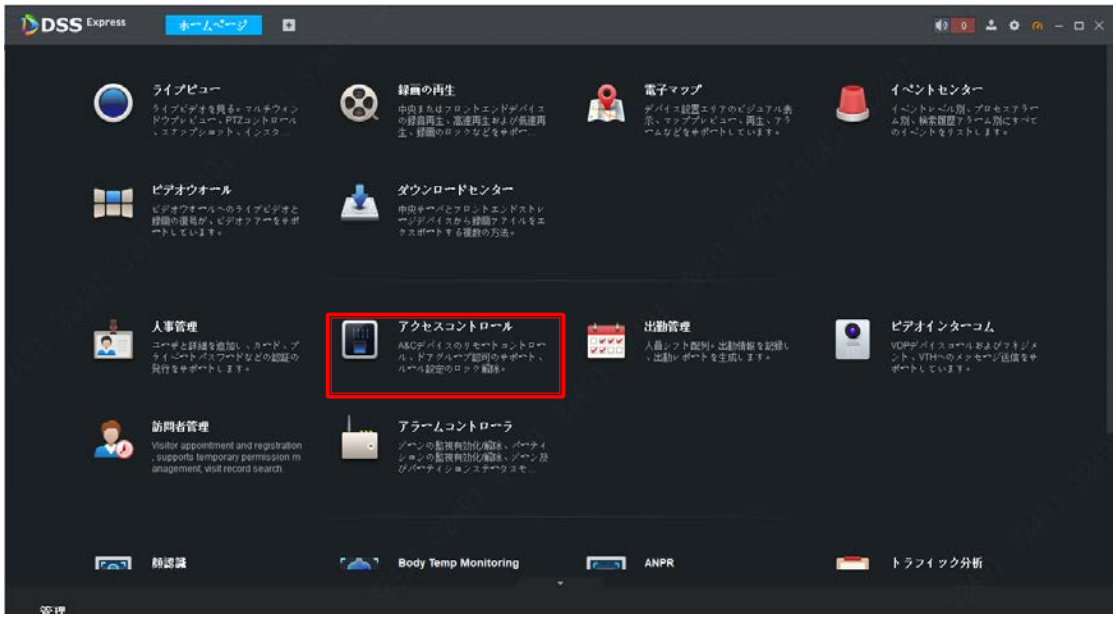
マウスでユーザーをダブルクリックすると、ユーザーを編集できます

6、ユーザー削除

ユーザーをチェックして、「削除」ボタンで削除できます

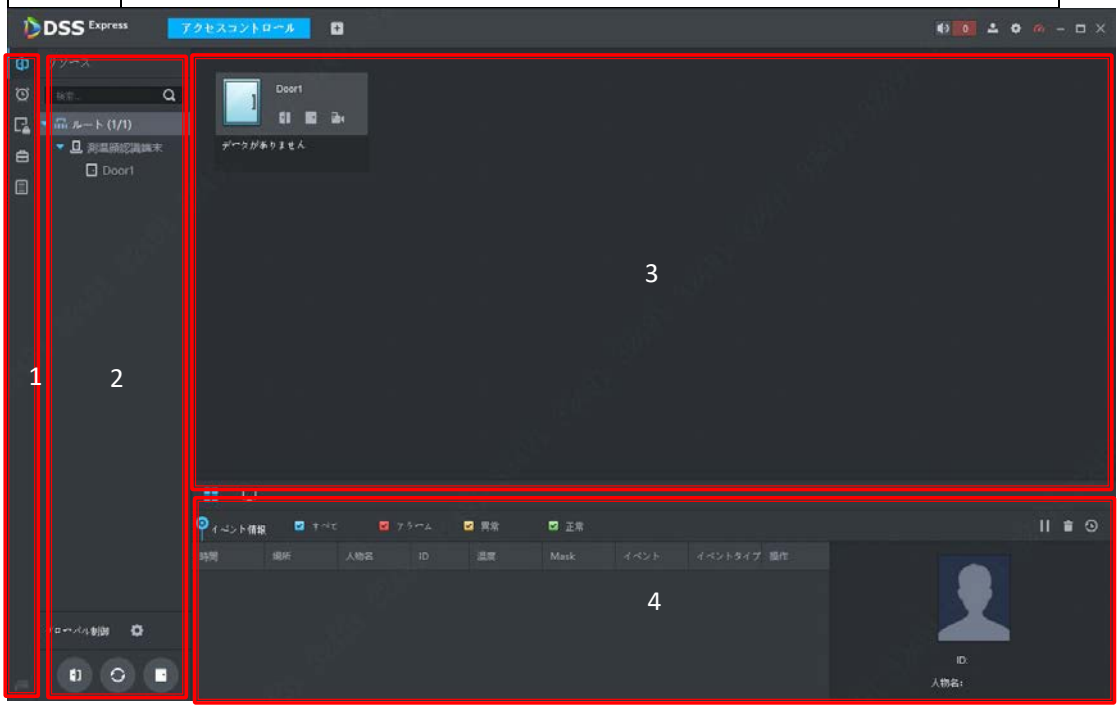
7、リアルタイムで解錠記録を確認

① 「ホームページ」で「アクセスコントロール」をクリックします



② 「アクセスコントロール」画面説明

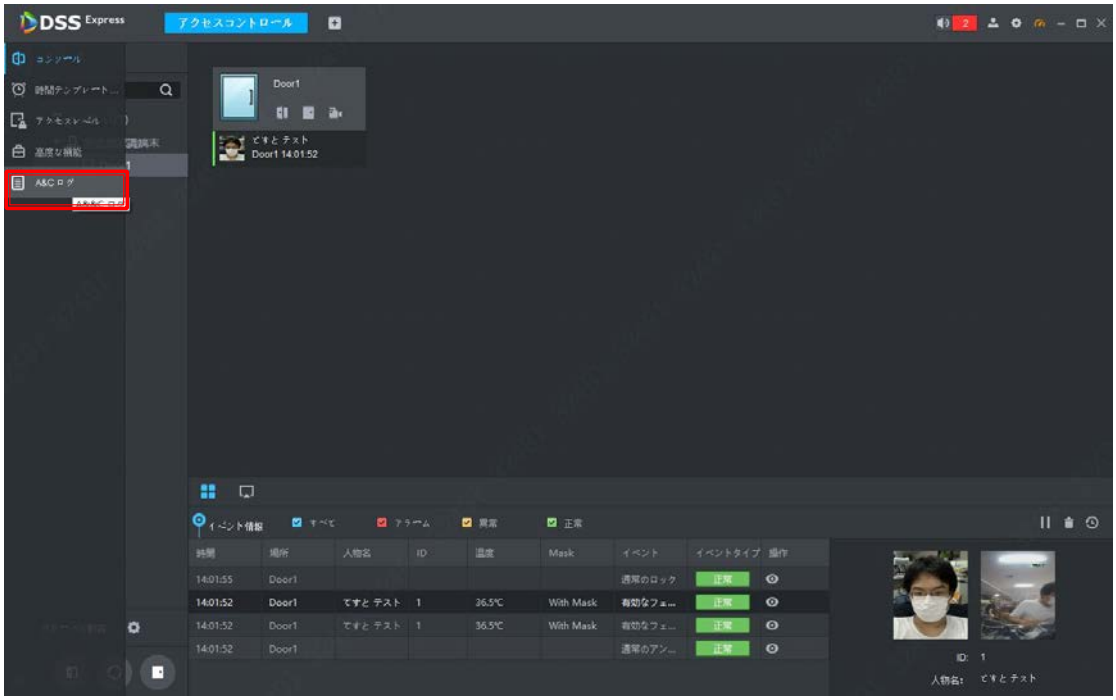
項番	説明
1	機能パネルです。リアルタイムの解錠記録管理、機器のログなどを確認できます。
2	機器の一覧リストです、機器を右クリックして、解錠、施錠などができます。
3	機器の一覧リストです、各ドアのパネルのアイコンをクリックして、解錠、施錠などができます。
4	リアルタイムの解錠イベントです。解錠時間、場所、ユーザー、体温、マスク有無などを確認できます。写真、映像なども確認できます。



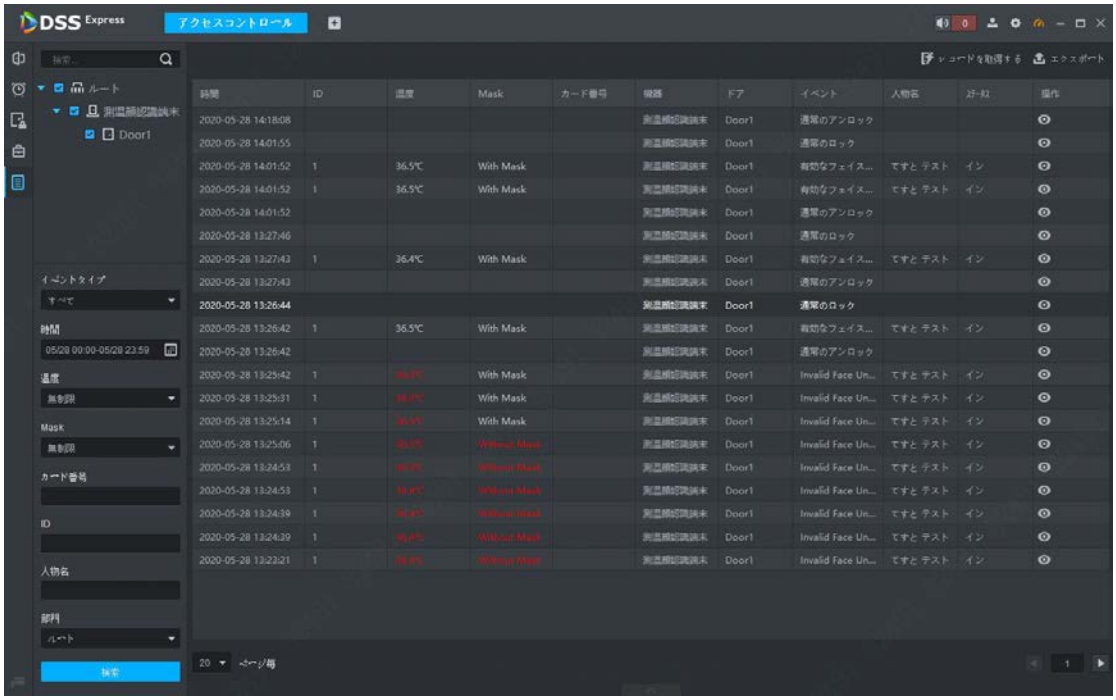
③ イベントを選択して、操作ボタンを押して、ライブ映像、スナップショット、録画を確認できます。

8、ログ確認

① 「アクセスコントロール」画面で、マウスを左の機能パネルに移動して、パネルを展開します。一番下の「A&Cログ」をクリックします。



② 左の機器一覧で機器を選択して、検索条件を設定して、「検索」ボタンで機器のログを確認します。


DSS Express
アクセスコントロール
ルート
Door1
イベントタイプ
すべて
時間
05/28 00:00-05/28 23:59
温度
無制限
Mask
無制限
カード番号
ID
人物名
部門
ルート
検索
レコードを取得する
エクスポート
時間
ID
温度
Mask
カード番号
機器
ドア
イベント
人物名
ｿｰﾄ
操作
2020-05-28 14:18:08
2020-05-28 14:01:55
2020-05-28 14:01:52
2020-05-28 14:01:52
2020-05-28 14:01:52
2020-05-28 13:27:46
2020-05-28 13:27:43
2020-05-28 13:27:43
2020-05-28 13:26:44
2020-05-28 13:26:42
2020-05-28 13:26:42
2020-05-28 13:25:42
2020-05-28 13:25:31
2020-05-28 13:25:14
2020-05-28 13:25:06
2020-05-28 13:24:53
2020-05-28 13:24:53
2020-05-28 13:24:39
2020-05-28 13:24:29
2020-05-28 13:23:21
測温顔認識端末
Door1
通常のアンロック
通常のロック
36.5℃
With Mask
Without Mask
有効なフェイス...
Invalid Face Un...
てすと テスト
イン
20
ページ/毎
1

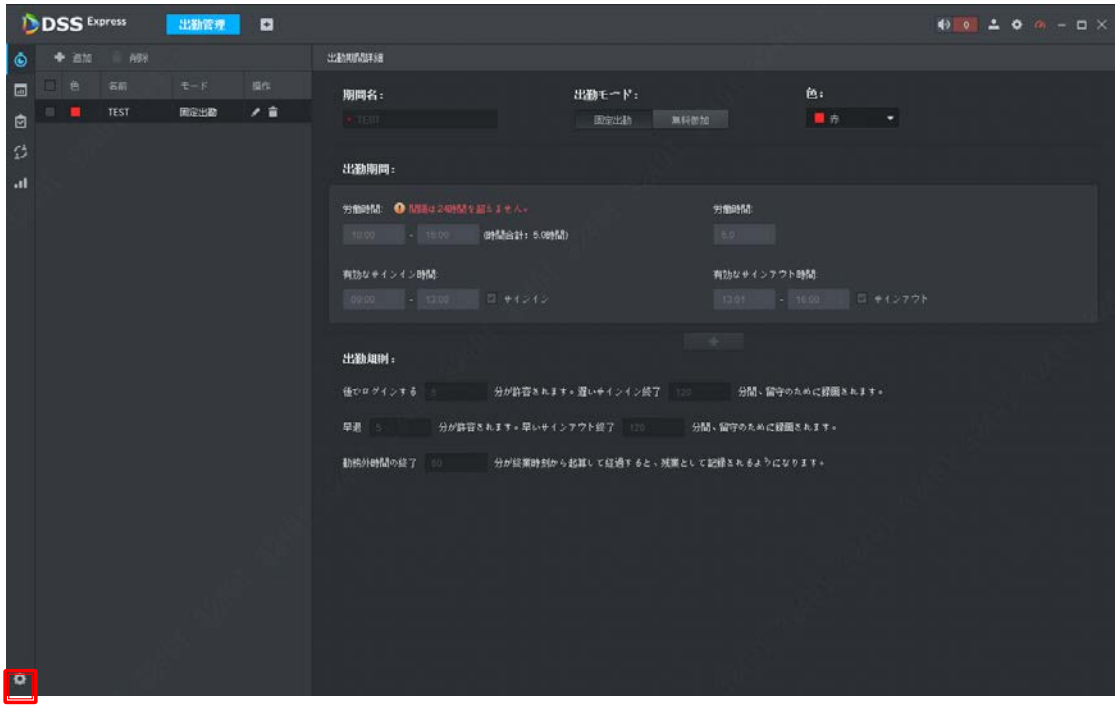
五、勤怠管理（DSS Express)

DSS Express を利用する場合、ASI7213X-T1 で社員の勤怠管理も出来ます。

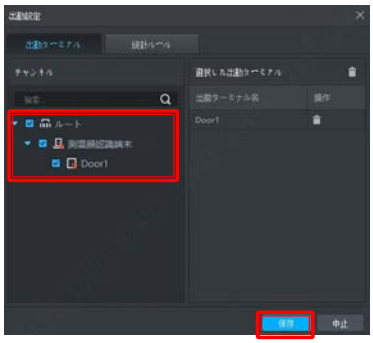
1、勤怠管理用の端末の管理

① 「ホームページ」画面で「出勤管理」を選択します

② 左下の歯車をクリックします



③　機器一覧で勤怠管理用の端末をチェックして、「保存」ボタンで保存します。

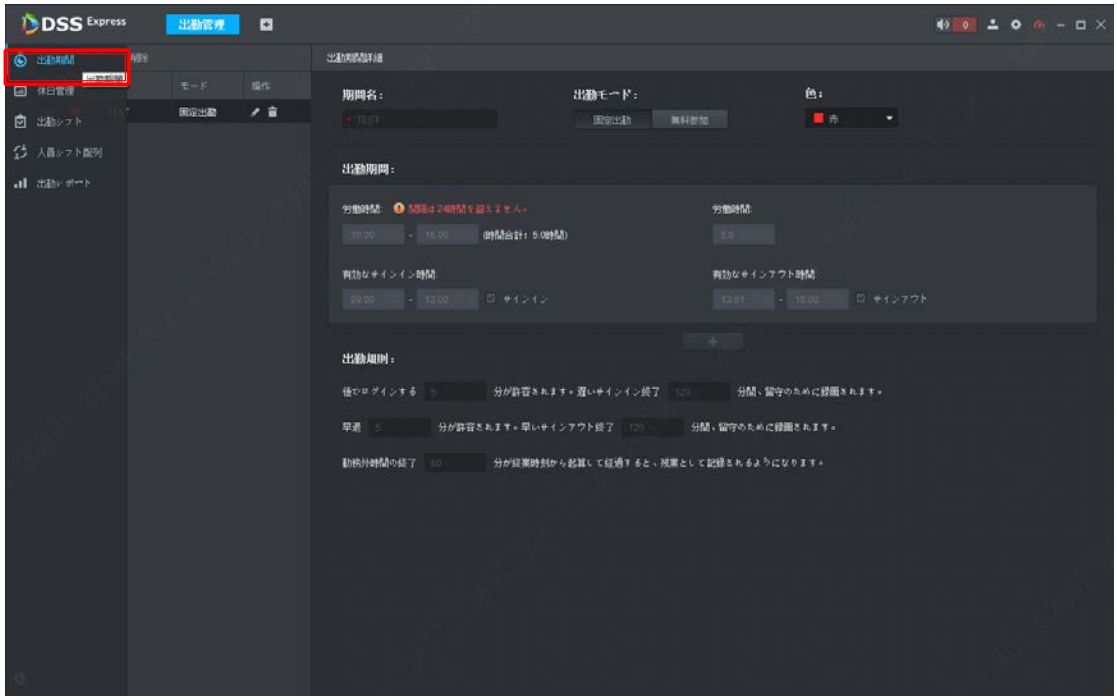


④　勤怠の計測時刻ルールに関して設定必要があるなら、「統計ルール」で設定してください。

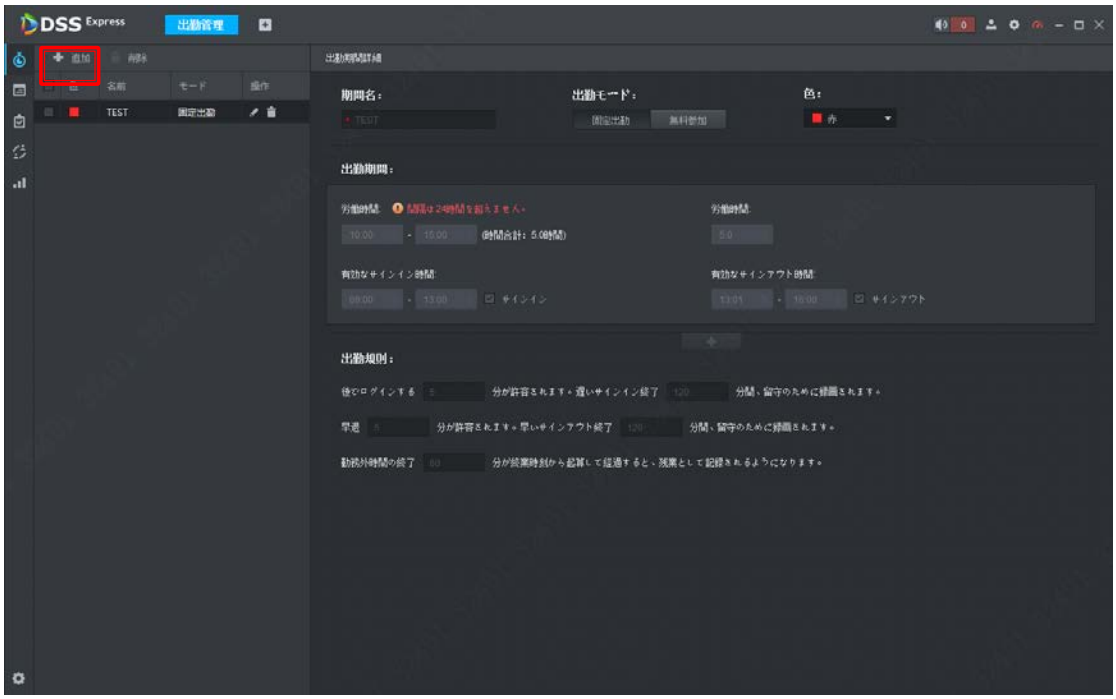
2、出勤期間管理

この画面で勤怠の期間の計測ルールが設定できます

①　左の一覧で「出勤期間」を選択します



② 左上の「＋追加」ボタンで期間を新規します



③ 期間名、出勤モード、カレンダーで表示する色を設定して、モードによって詳しいルールを設定して、保存します。

モードは二種類があります、出勤時刻固定の固定出勤と出勤時刻フリーの自由出勤（画面では無料参加）

1） 固定出勤

出勤期間は最大二つが設定できます（例えば午前中と午後それぞれ設定)。

出勤時間

❶仕事開始と終了時間です

❷仕事時間です

❸有効なサインイン期間。有効な期間以内、かつ仕事開始時間前だたら、正常のサインインになります、仕事開始時間後だたら、遅刻/欠勤になります。

❹有効なサインアウト期間。有効な期間以内、かつ仕事終了時間前だたら、早退/欠勤になります、仕事開始時間後だたら、正常のサインアウトになります。

出勤規則

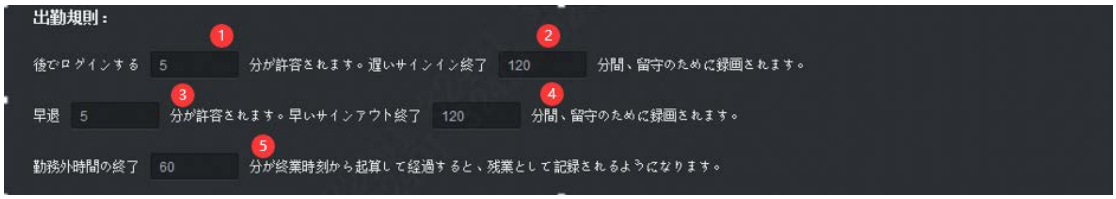
❶仕事開始以後何分以内のサインインは遅刻になりません。

❷仕事開始以後何分以外のサインインは欠勤になります。

❸仕事終了時間前、何分以内のサインアウトは早退になりません。

❹仕事終了時間前、何分以外のサインアウトは欠勤になります。

❺仕事終了時間後、何分後のサインアウトは残業として記録されます。



2) 自由出勤

出勤規則

❶何時間の仕事シフト。

❷最終のサインイン時間。制限しない場合は時間を問わず、有効なサインイン記録になります。

❸記録された稼働時間です。

❹最終のサインアウト時間です。

❺残業時間です。チェックしない場合は何時間でも残業になれない、チェックする場合は設定された時間後は残業になります。

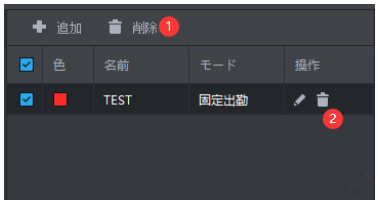
❻サインイン/サインアウトのルールです。奇数回の認証はサインイン、偶数回の認証はサインアウト。また、設定された時間以内の再認証で記録として保存されません。

④ 出勤期間変更。左の期間一覧リストで変更したい期間のペンのアイコンをクリックしたら、出勤期間が変更できます。

⑤ 出勤期間削除。

方法一：削除したい期間をチェックして、上の「削除」ボタンをクリックします。

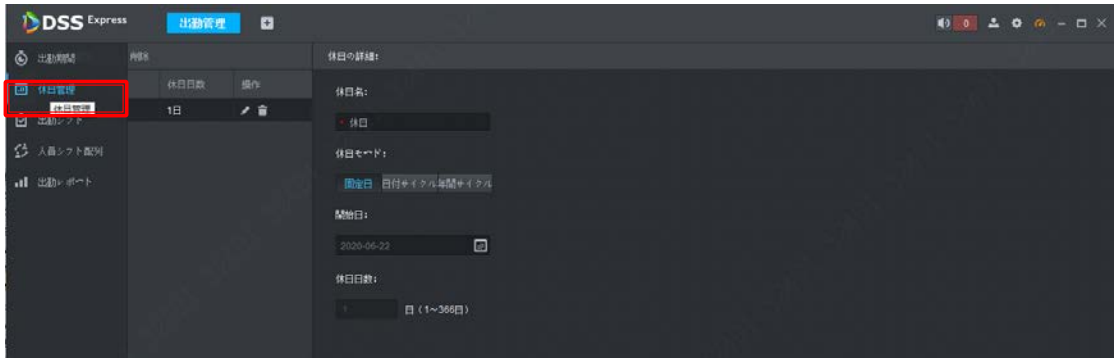
方法二：削除したい期間のゴミ箱アイコンクリックして、削除します。



3、休日管理

この画面で休日が管理できます。出勤期間を設定しても、休日が設定されたら、この日の出勤は残業になります。

① 左の一覧で「休日管理」を選択します



② 左の「＋追加」ボタンで休日を新規します。

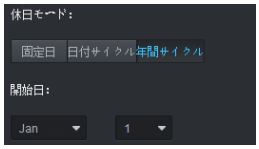
③ 休日名と休日日付を設定して、右下の「保存」ボタンで保存します。

休日モードは三つがあります。

1） 固定日：固定日の場合は休日開始日付を設定必要があります、このモードなら、設定日付の年は固定されます。

2) 日付サイクル：日付サイクルの場合は曜日指定が必要です

3) 年間サイクル：月と日を設定する必要があります



④ 休日変更。左の休日一覧リストで変更したい休日のペンのアイコンをクリックしたら、休日が変更できます。

⑤ 休日削除。

方法一：削除したい休日をチェックして、上の「削除」ボタンをクリックします。

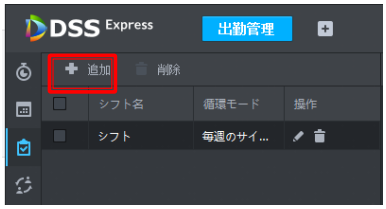
方法二：削除したい休日のゴミ箱アイコンクリックして、削除します。

4、出勤シフト管理

この画面で出勤シフトが管理できます。ニーズによって、日別/週別/月別三つ種類のシフトが作成できます。

① 左の一覧で「出勤シフト」を選択します

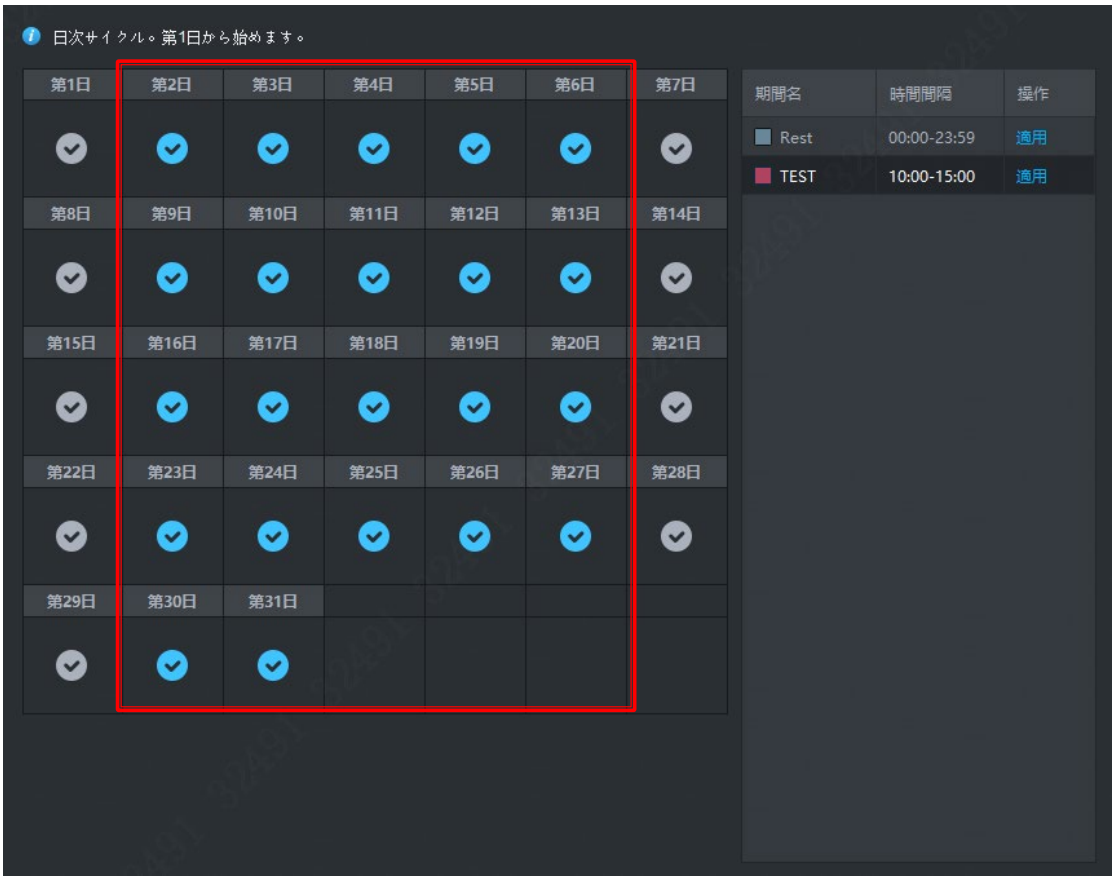
② 左の「＋追加」ボタンで出勤シフトを新規します



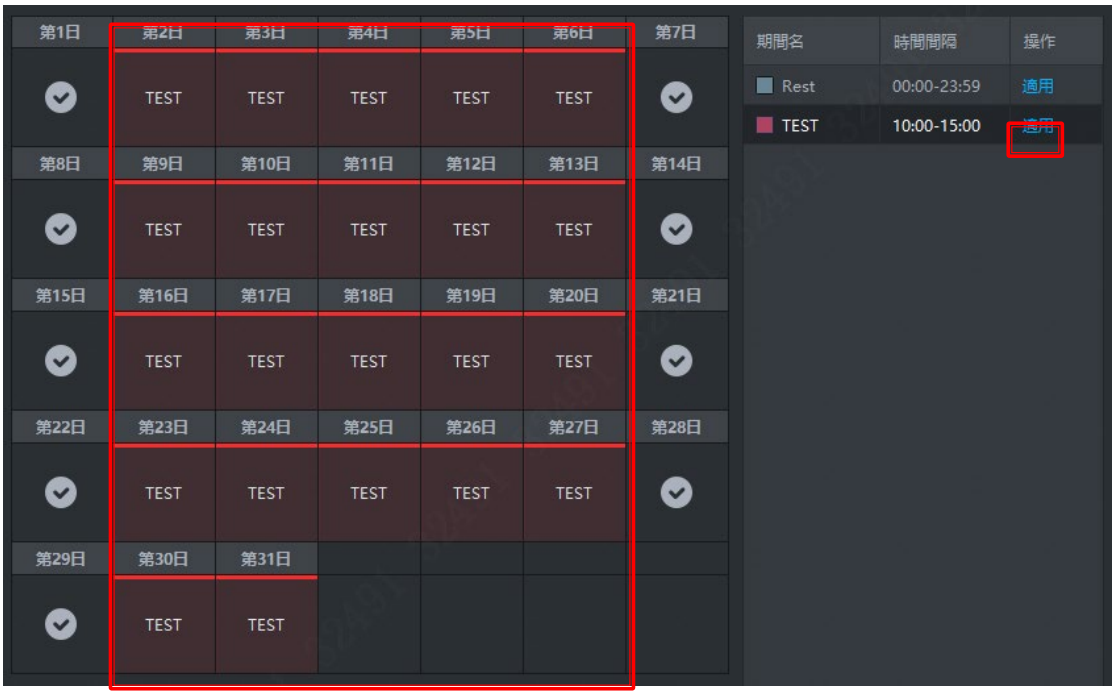
③ シフト名と各日の出勤期間を設定して、右下の「保存」ボタンで保存します。

1) 出勤期間指定

i. 期間を設定した日付をクリックして、選択された日付が青いアイコンで表示されます



ii. 日付を設定した後適用したい期間の「適用」ボタンをクリックして、選択された日付の色が期間の色になります



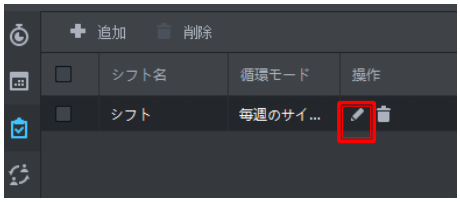
2) モード説明

i. 日別（昼）：日別で出勤期間を繰り返します。一回循環の日付数を設定する必要があります。

ii. 週別：週別で出勤期間を繰り返します。一回循環の週間数を設定する必要があります。

iii. 月別：月別で出勤期間を繰り返します。一回循環の月数を設定する必要があります。月の切替は左の矢印で操作します。

④ 出勤シフト変更。左の出勤シフト一覧リストで変更したい出勤シフトのペンのアイコンをクリックしたら、出勤シフトが変更できます。



⑤ 出勤シフト削除。

方法一：削除したい出勤シフトをチェックして、上の「削除」ボタンをクリックします。

方法二：削除したい出勤シフトのゴミ箱アイコンクリックして、削除します

5、人員シフト配列

この画面で「人事管理」で作られた社員に対して、個人/部署全体に対して、出勤シフトが設定できます。

① 左の一覧で「人員シフト配列」を選択します

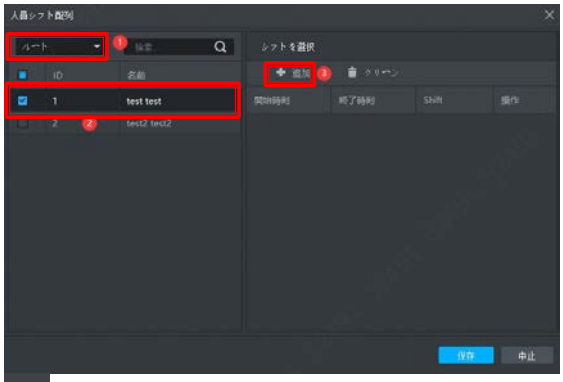
② 人員シフトを設定します

1) ボタンで部署に対して、部署全員に同じシフトを適用します

左側で設定したい部署を選択して、右側で適用期間とシフトを設定して、「良」で保存します。

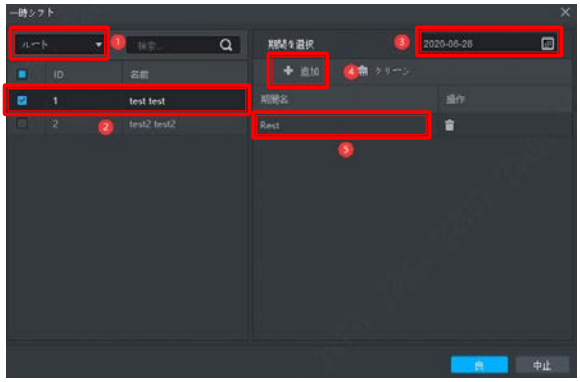
2) ボタンで個人に対して、シフトを設定します

部署を選択して、設定したい人員をチェックして、右側の「+追加」ボタンでシフトを追加して、適用期間とシフトを設定して、「保存」で保存します。



3) ボタンで個人に対して、一時のシフトを設定します

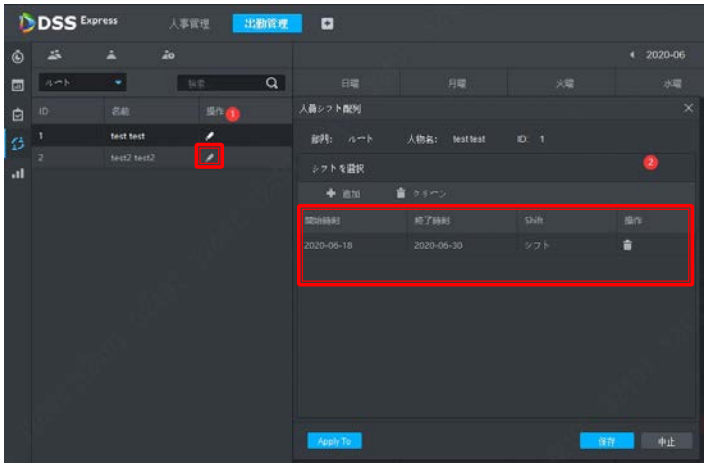
部署を選択して、設定したい人員をチェックして、右側で日付を設定した後、「+追加」ボタンでシフトを追加して、適用した期間名を設定して、「良」で保存します。



※一時シフトはカレンダーで日付を選択して、ダブルクリックでも編集できます。

③ シフト変更

人員リストからペンのアイコンをクリックしたら、人員シフトが変更できます。

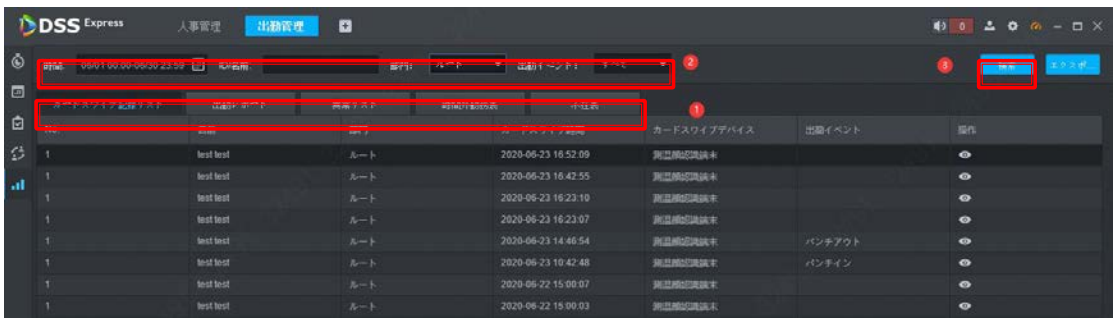


6、出勤レポート

この画面で社員に対して、サインイン/サインアウト、出勤の記録などが確認できます。

① 左の一覧で「出勤レポート」を選択します。

② レポートは 5 種類があります、レポートを選択して、時間などを設定したら、記録が検索できます。



カードスワイプ記録リスト：サインイン/サインアウトの記録です

出勤レポート：出勤時間、残業時間、外出時間などの記録です
異常リスト：遅刻、早退の記録です
時間外勤務表：残業の記録です
不在表：外出の記録です

六、FAQ

1、機器本体 FAQ

1.1. 電源投入後、アクセスコントローラーが起動されていないが。

⇒12V 電源が正しく接続されているか、電源ボタンが押されているかを確認してください。

1.2 アクセスコントローラーの電源を入れた後、顔は認識できないのですが。

⇒「メインメニュー」->「アクセス」->「アンロックモード」で「顔」、及び「アンロックモード」はオンであるかを確認してください。

1.3 アクセスコントローラーと外部コントローラーが Wiegand ポートに接続されている場合、出力信号はないですが。

⇒アクセスコントローラーの GND ケーブルと外部コントローラーが接続されているかを確認してください。

1.4 ユーザーの顔は認識されているが、他のユーザーの情報が表示されていないが、。

⇒人間の顔をインポートするときは、周囲に人がいないことを確認してください。登録された顔データを削除して、もう一度登録し直してください。

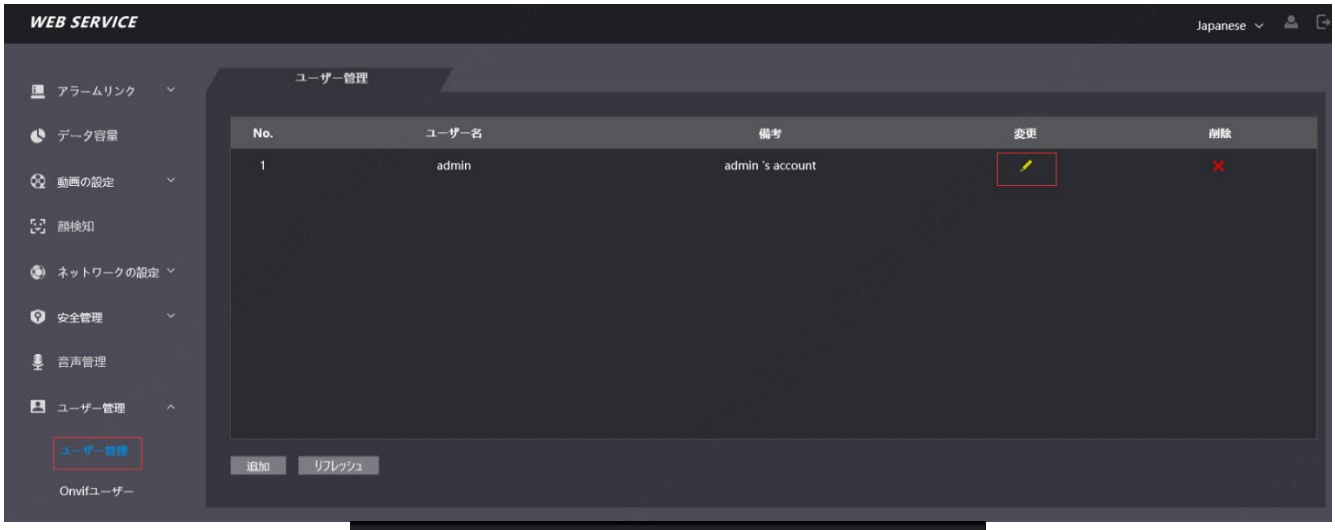
システム→顔パラメータ→顔認識閾値の数値を大きくしてみてください。

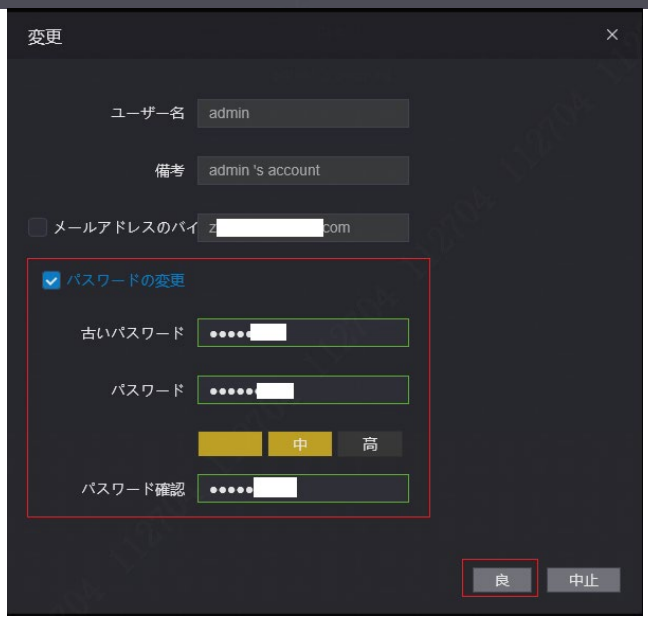
1.5 管理者用のパスワードを変更したい場合、どうしたら良いでしょうか。

⇒

1.6.1 パスワードは忘れられていない場合

アクセスコントローラーの Web 側で変更することはできます。Web 側にログインして、下記の図を参照して変更してください。





1.6.2　パスワードは忘れられた場合

初期化の際に、メールアドレスを入力していない場合

パスワードのリセット ツールでパスワードをリセットすることはできます。

※パスワードをリセットするにはツールが必要ですので、弊社サポート窓口までお問合せください。

① 「General_ConfigTool_ChnEng_V5.000.0000000.0.R.20200426.exe」をインストールします。

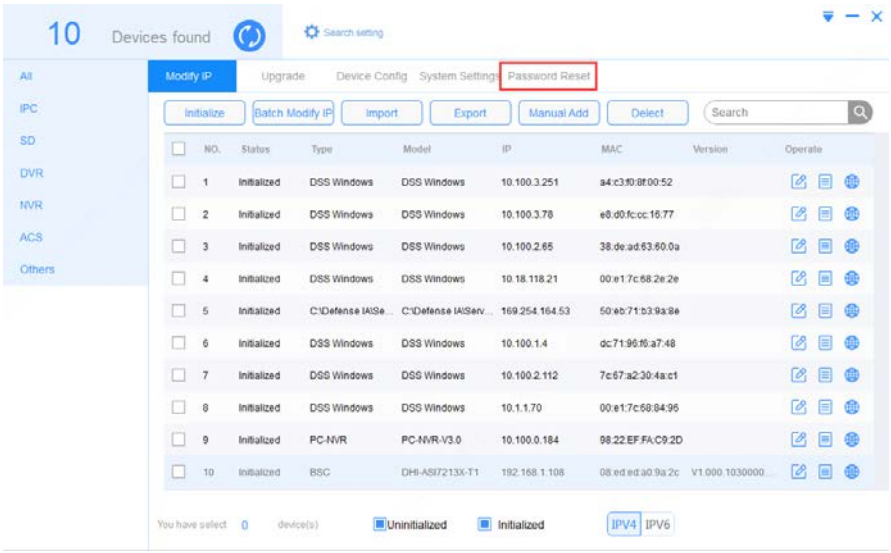
② パスワードリセット

②.1 XML ファイル/QR コードでパスワードをリセットできます。

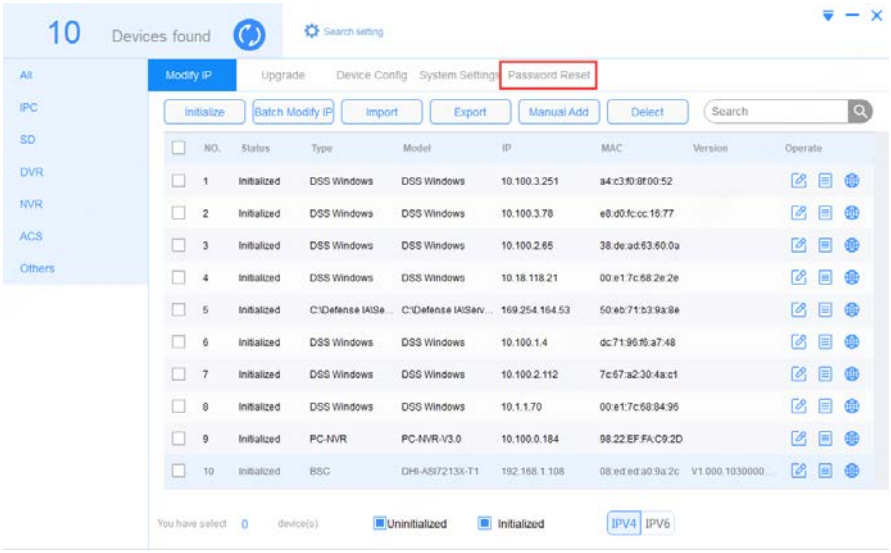
②.2 ロカールネットワークの機器のみパスワードをリセットできます。

③ XML ファイルでパスワードをリセットします。

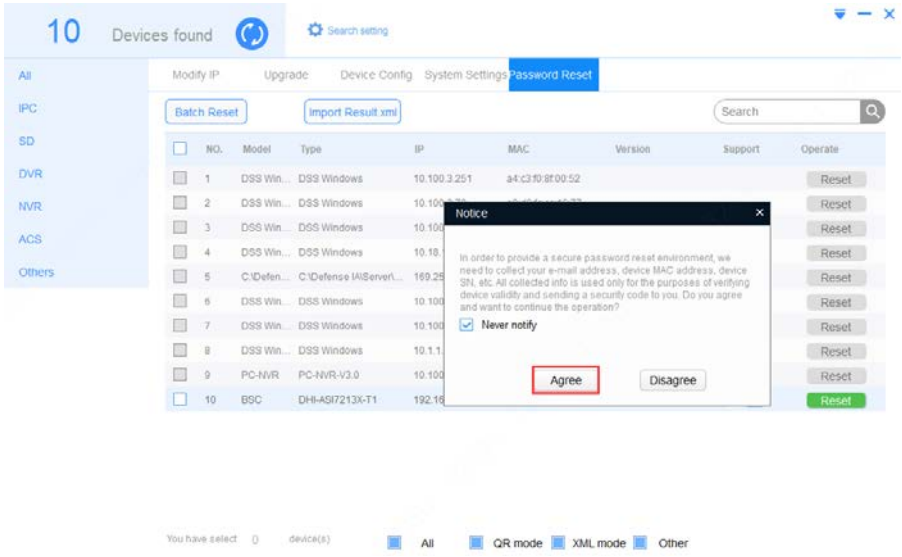
③.1 「Password Reset」をクリックします。



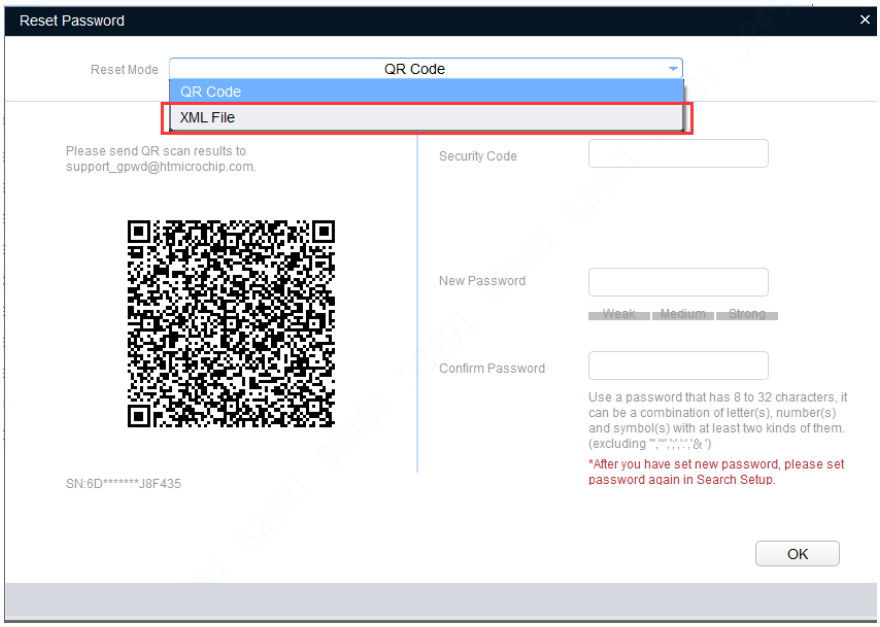
③.2 「Reset」ボタンをクリックします。



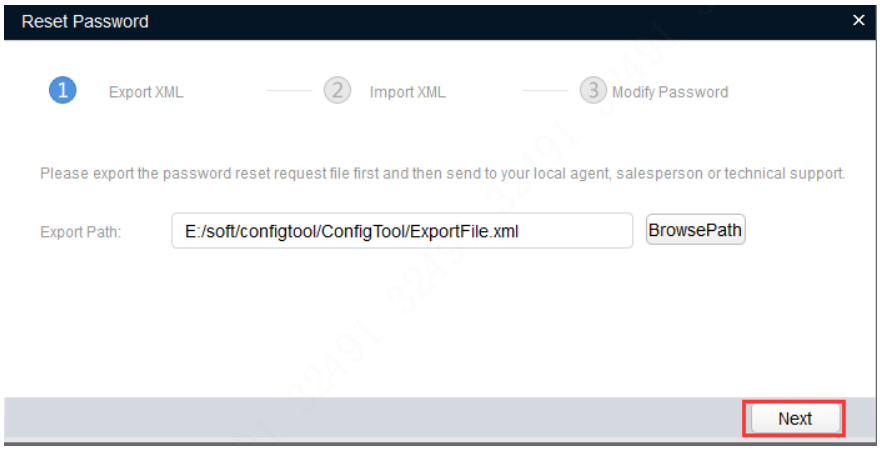
③.3 「Agree」ボタンをクリックします



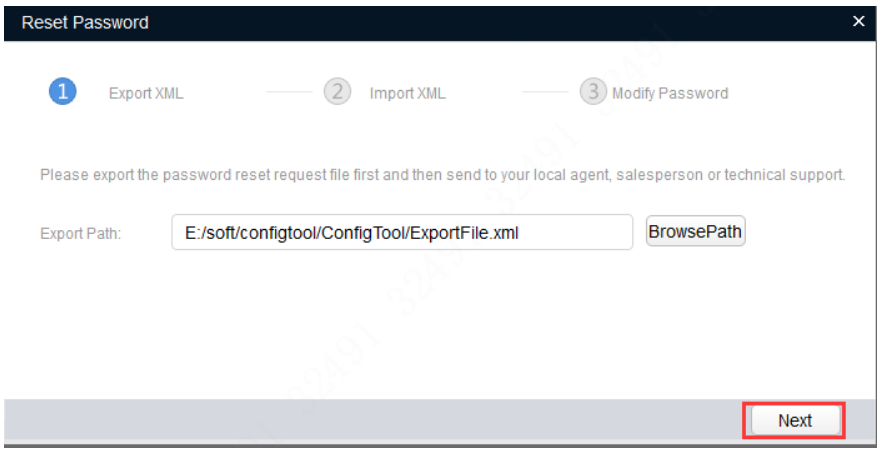
③.4 「XML File」を選択します。



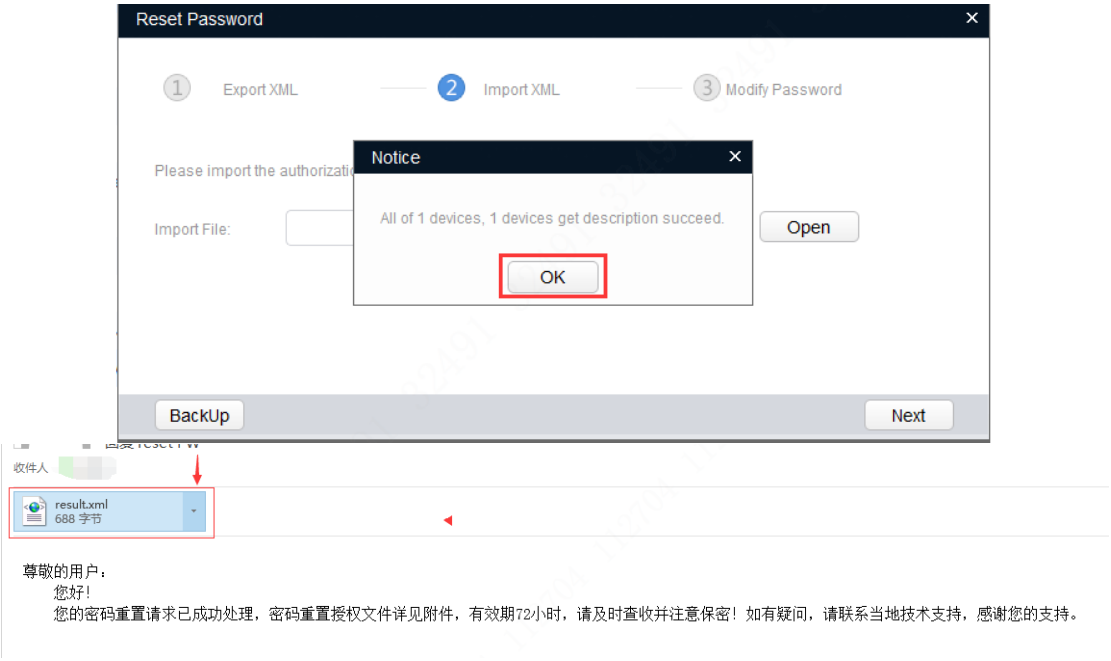
③.5 「OK」をクリックします。



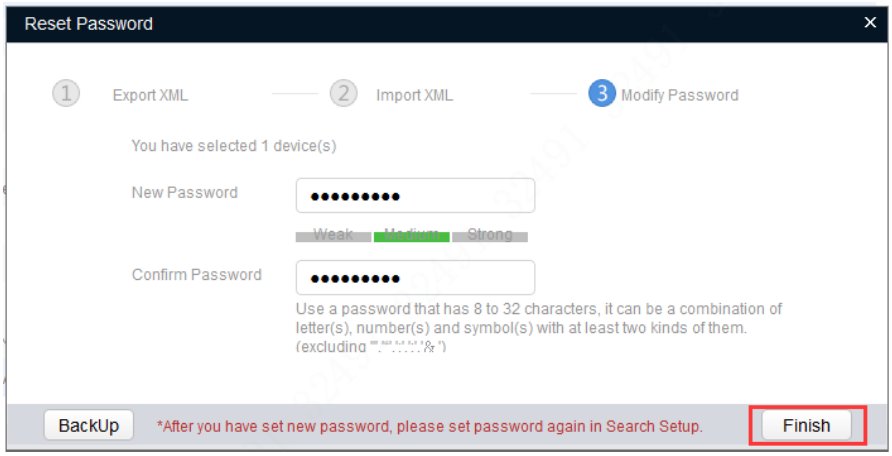
③.6 パスを設定して、「Next」でエクスポートします。



③.7 エクスポート完了したら、「OK」ボタンを押します。エクスポートされたファイルを下記のメールへ送信します: support_gpwd@htmicrochip.com。数分後、メールで「result.xml」ファイルをもらいます。



③.8　新しいパスワードを設定して、「Finish」ボタンでパスワードを変更します。

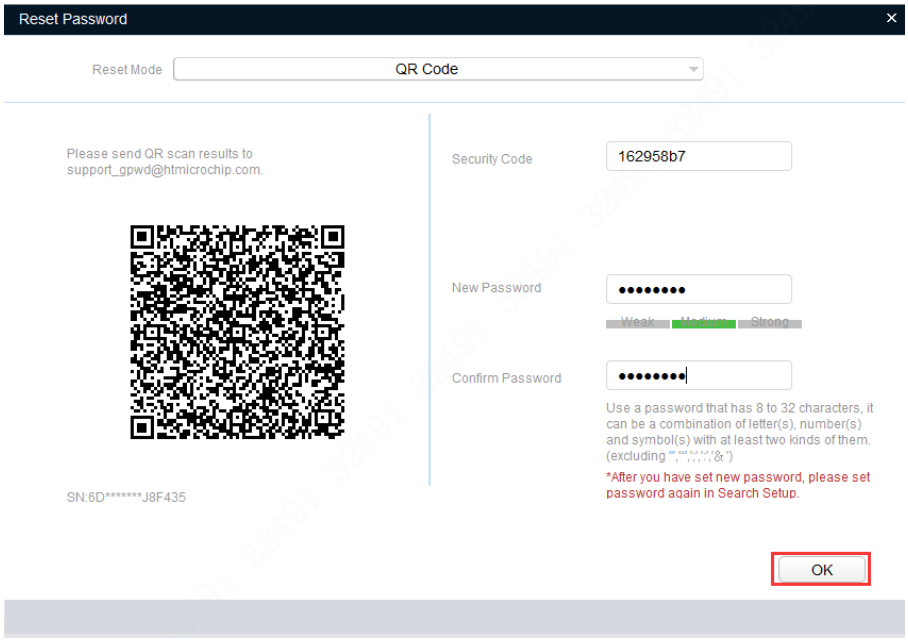


④　初期化の際に、メールアドレスを入力した場合

コードでパスワードをリセットします

④.1　もし初期設定する際メールを設定したことがあるなら、QR コードでリセットできます。「Reset」ボタンをクリックして、「QR Code」を選択して、QR コードをスキャンして、内容をを下記のメールへ送信します：support_gpwd@htmicrochip.com。数分後、設定されたメールで「Security Code」をもらいます。

④.2　もらったコードを入力して、パスワードを設定して、「OK」ボタンでパスワードを変更します。


Reset Password
Reset Mode
QR Code
Please send QR scan results to support_gpwd@htmicrochip.com.
SN:6D*******J8F435
Security Code
162958b7
New Password
Weak
Strong
Confirm Password
Use a password that has 8 to 32 characters, it can be a combination of letter(s), number(s) and symbol(s) with at least two kinds of them. (excluding '",',;:.`&')
*After you have set new password, please set password again in Search Setup.
OK

付録１　温度監視の注意事項

① 電源投入後１５分以上にわたって温度監視ユニットをウォームアップして、温度監視ユニットが熱平衡に達するようにします。
② 温度監視ユニットを室内の無風環境に設置し、室内の周囲温度を 15℃∽32℃ に維持してください。
③ 温度監視ユニットに直射日光が当たらないようにしてください。
④ 温度監視ユニットを光源のあるガラスに向けて設置しないでください。
⑤ 温度監視ユニットを熱源から離して設置してください。
⑥ 日光、風、冷気、冷房と温風の空調などの要素は、人体の表面温度に影響を及ぼし、監視されている温度と実際の温度との間に温度偏差が発生します。
⑦ 発汗は、体が自動的に冷えて熱を放散する方法でもあります。これにより 、監視されている温度と実際の温度との間に温度偏差が生じます。
⑧ 定期的に（2 週間ごとに）温度監視ユニットを保守してください。
温度センサーと距離センサーの表面にあるほこりを柔らかくほこりの出ない布でやさしく拭いて、清潔に保ちます。

付録２　　顔認識のメモ

記録/比較

登録前

① メガネ、帽子、ひげは、顔認識のパフォーマンスに影響を与える可能性があります。
② 帽子をかぶるときは眉毛を覆わないでください。
③ デバイスを使用する場合は、ひげのスタイルを大幅に変更しないでください。顔認識がうまくできない可能性があります。
④ 顔を清潔に保ちます。
⑤ デバイスを光源から少なくとも 2 メートル、窓またはドアから少なくとも
⑥ メートル離れた位置に設置してください。逆光や直射日光の影響で顔認識パフォーマンスに影響を与える可能性があります。

登録中

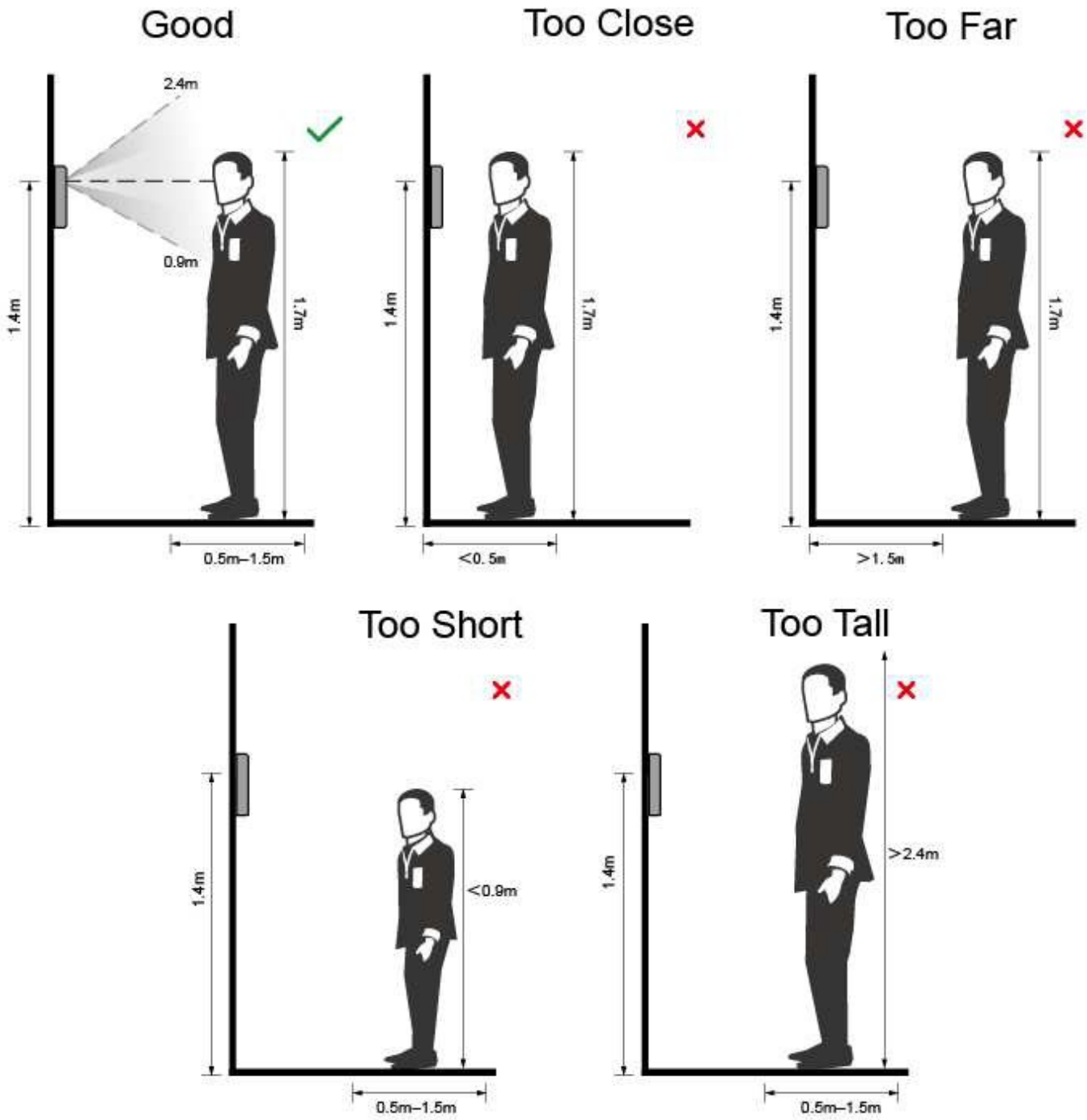
① あなたの顔の写真が自動的にキャプチャされます。

② 頭や体を振らないでください。登録に失敗することがあります。

③ 2 つの顔が同時にキャプチャフレームに表示されないようにしてください。

顔の位置

① 顔が適切な位置にない場合、顔認識に影響を与える可能性があります。



顔の登録・認識条件

① 顔全体が覆われていなく、額が髪で覆われていないことを確認してください。

② 顔画像の記録に影響を与えるメガネ、帽子、ひげ、その他の顔の装飾品を着用しないでください。

③ 目を開けて、顔の表情なしで、顔をカメラの中心に向けます。

④ 顔を記録するとき、または顔を認識しているときは、顔をカメラに近づけたり遠ざけたりしないでください。

⑤ DSSexpress を介して顔画像をインポートする場合、写真は jpg ファイルが必要です。写真は 75kb 以下が必要、300x300≤解像度≤600x600（お勧め解像度は 500x500）。
顔が画像領域全体の 2/3 を占めておらず、アスペクト比が 1：2 を超えていないことを確認してください。

付録 3　サイバーセキュリティの推奨事項

サイバーセキュリティは単なる流行語ではありません。
インターネットに接続されているすべてのデバイスに関係します。
IP ビデオ監視はサイバーリスクの影響を受けにくいですが、
ネットワークやネットワーク化されたアプライアンスを保護および強化するための基本的な手順を実行することで、攻撃の影響をさらに受けにくくなります。
以下は、より安全なセキュリティシステムを作成するためのヒントと推奨事項です。
基本的な機器のネットワークセキュリティのために実行する必要があるアクション：

① 強力なパスワードを使用する

1) パスワードを設定するには、次の提案を参照してください。

2) 長さは 8 文字以上でなければなりません。
3) 少なくとも 2 種類の文字を含みます。文字タイプは、大文字と小文字、数字、記号が含まれます。
4) アカウント名またはアカウント名を逆の順序で含めないでください。
   - 123、abc などの連続した文字は使用しないでください。
   - 111、aaa などの重複文字を使用しないでください。

② ファームウェアとクライアントソフトウェアを適時に更新する

1) 標準手順に従って、システム（NVR、DVR、IP カメラなど）のファームウェアを最新の状態に保ち、システムに最新のセキュリティパッチと修正プログラムが確実にインストールされるようにする ことをお勧めします。機器がパブリックネットワークに接続されている場合、
2) 「アップデートの自動チェック」機能を有効にして、
3) 製造元がリリースしたファームウェアアップデートのタイムリーな情報を取得することをお勧めします。
4) クライアントソフトウェアの最新バージョンをダウンロードして使用することをお勧めします。

③ 機器のネットワークセキュリティを向上させるための推奨事項:

1) 物理的保護
   機器、特にストレージデバイスを物理的に保護することをお勧めします。
   たとえば、特別なコンピュータルームとキャビネットに機器を配置し、よく行われたアクセス制御許可とキー管理を実装し、ハードウェアの損傷、リムーバブル機器（USB フラッシュディスクなど）の不正な接続など、許可されていない人物が物理的な接触を実行するのを防ぎます。
2) パスワードを定期的に変更する
   推測またはクラックされるリスクを減らすために、パスワードを定期的に変更することをお勧めします。
3) パスワードの設定と更新、タイムリーな情報のリセット
   機器はパスワードリセット機能をサポートしています。エンドユーザーのメールボックスや
   パスワード保護に関する質問など、パスワードをリセットするための関連情報をすぐに設定してください。情報が変更された場合は、時間内に変更してください。パスワード保護の質問を設定するときは、簡単に推測できるものを使用しないことをお勧めします。
4) アカウントロックを有効にする
   アカウントロック機能はデフォルトで有効になっています。アカウントのセキュリティを確保するために、この機能をオンにしておくことをお勧めします。攻撃者が間違ったパスワードで数回ログインしようとすると、対応するアカウントとソース IP アドレスがロックされます。
5) デフォルトの HTTP およびその他のサービスポートを変更する
   デフォルトの HTTP およびその他のサービスポートを 1024 から 65535 の間の任意の数のセットに変更することをお勧めします。これにより、部外者が使用しているポートを推測できるリスクを軽減できます。
6) HTTPS を有効にする
   安全な通信チャネルを通じて Web サービスにアクセスできるように、HTTPS を有効にすることをお勧めします。
7) ホワイトリストを有効にする
   ホワイトリスト機能を有効にして、指定された IP アドレスを持つ人を除く全員がシステムにアクセスできないようにすることをお勧めします。したがって、必ずコンピュータの

IP アドレスと付属機器の IP アドレスをホワイトリストに追加してください。

8) MAC アドレスバインディング
ゲートウェイの IP および MAC アドレスを機器にバインドして、ARP スプーフィングのリスクを軽減することをお勧めします。

9) アカウントと権限を適切に割り当てる
ビジネス要件および管理要件に従って、合理的にユーザーを追加し、最小限の権限セットをユーザーに割り当てます。

10) 不要なサービスを無効にし、セキュアモードを選択する
不要な場合は、リスクを減らすために、SNMP、SMTP、UPnP などの一部のサービスをオフに することをお勧めします。必要に応じて、セーフモードを使用することを強くお勧めします。これには、次のサービスが含まれますが、これらに限定されません。
- SNMP：SNMP v3 を選択し、強力な暗号化パスワードと認証パスワードを設定します。
- SMTP：メールボックスサーバーにアクセスするには、TLS を選択します。
- FTP：SFTP を選択し、強力なパスワードを設定します
- AP ホットスポット：WPA2-PSK 暗号化モードを選択し、強力なパスワードを設定します。

11) オーディオおよびビデオ暗号化送信
オーディオおよびビデオデータの内容が非常に重要または機密である場合は、暗号化された送信機能を使用して、送信中にオーディオおよびビデオデータが盗まれるリスクを軽減することをお勧めします。
注意：暗号化された伝送は、伝送効率のいくらかの損失を引き起越す可能性があります。

12) 安全な監査
・オンラインユーザーを確認する：オンラインユーザーを定期的に確認して、デバイスが不正にログインしていないか確認することをお勧めします。
・機器ログを確認する：ログを表示することで、デバイスへのログインに使用された IP アドレスとその主要な操作を確認できます。

13) ネットワークログ
機器の保存容量には限りがあるため、保存されるログは限られています。ログを長期間保存 する必要がある場合は、ネットワークログ機能を有効にして、重要なログがネットワークログサーバーと同期してトレースできるようにすることをお勧めします。

14) 安全なネットワーク環境を構築する
機器の安全性を確保し、潜在的なサイバーリスクを軽減するために、次のことをお勧めします。
・ルーターのポートマッピング機能を無効にして、外部ネットワークからイントラネットデバイスに直接アクセスしないようにします。
・ネットワークは、実際のネットワークニーズに応じて分割および分離する必要があります。2 つのサブネットワーク間に通信要件がない場合は、VLAN、ネットワーク GAP、および その他のテクノロジーを使用してネットワークを分割し、ネットワーク分離効果を実現することをお勧めします。
・802.1x アクセス認証システムを確立して、プライベートネットワークへの不正アクセスのリスクを軽減します。
・デバイスが攻撃されるリスクを軽減するために、デバイスのファイアウォールまたはブラックリストとホワイトリストの機能を有効にすることをお勧めします。

以上です。