



EG-Keeper  
管理アプリケーション  
ユーザーズマニュアル

Version 0.3.0

2020/6/16

株式会社WDS

## 改訂履歴

Ver.	変更箇所／内容	変更日時	作成者
0.1	新規作成	2020/5/21	WDS
0.2	機能説明追加	2020/6/7	WDS
0.3	起動時間について	2020/6/16	WDS

## 目次

1. 概要	4
2. 製品の特徴	4
3. 外部インターフェース	4
4. クライアントの操作	5
4.1. 端末管理	5
4.2. 操作環境	5
4.3. 設定	6
4.3.1. 端末の登録	6
4.3.1.1. 端末の検索	6
4.3.1.2. 端末の登録	6
4.3.2. 端末の設定	7
4.3.2.1. Device Param	7
4.3.2.2. IPアドレス設定	7
4.3.2.3. WIFI設定	8
4.3.2.4. Upload Setting	8
4.3.2.5. Private Cloud setting	8
4.3.2.6. Upload Setting	8
4.3.2.7. Algrithom Setting	9
4.3.2.8. マスク装着状態／体温状態チェック実施設定	9
4.3.2.9. ディスプレイの設定	10
4.3.2.10. 音声パターン設定	10
4.3.2.11. 体温状態チェック閾値設定	10
4.3.2.12. ビデオ 設定	11
4.3.3. 端末のファームウェアアップデート	11
4.4. ユーザー管理	12
4.4.1. ユーザー追加	12
4.4.2. ファイルからユーザー追加	13
4.4.3. ユーザー編集	13
4.4.4. ユーザーの削除	14
4.4.5. 登録ユーザー同期	15
4.4.6. 作成ユーザーの削除	16
4.4.7. ブラックリストとホワイトリスト	17
4.4.8. 認証制限の付与	18
4.4.9. ユーザーアクセス情報	20
5. データクエリ	21
5.1. 認証記録の確認	21
5.2. 認証記録のエクスポート	21
5.3. スナップショット取得	22
6. クイックアクセスガイド	23
6.1. 簡易操作手順一覧	23
6.2. ユーザー登録時の設定内容	23
7. お問い合わせ先	24

## 1. 概要

本製品は、エッジ処理で高速かつ正確に顔認証ができるAIエッジ解析カメラ”Eeye”を搭載し、マスク着用でも顔認証が可能な顔認証パネルで、同時サーモグラフによる体温検知機能も搭載し、顔認証と合わせて地温検知による入退出管理が可能な顔認識システムとなります。

## 2. 製品の特徴

本製品の特徴は以下となります。

- 人が近づくと、デバイスは自動的にアクティベートされます。
- 7インチLCD搭載で操作ガイダンスやフェイスフレームを表示し、リアルタイムの顔検出が可能です。
- 写真やビデオの偽造防止機能を搭載しております。
- 顔認識距離は最大1メートル、高さの範囲は1.4m～1.9mの範囲で測定が可能です。
- 最大30,000人まで登録が可能です。
- 顔認証だけでなく複数の認証方法に対応しております。
- 顔の比較時間≤0.5秒/人。認識率≥99%で解析が可能です。
- TCP / IPおよびUSBインターフェースを介して認証情報の管理が可能です。
- オフラインモードでも動作可能なため、インターネット未接続でも認証が可能です。

### ※ご注意:

Eg-Keeperに電源を投入してから15分から20分間は放置してください。  
サーモセンサーの自動キャリブレーションがその間行われ、温度が安定いたします。  
電源投入直後では体温が高めに出てしまいます。

## 3. 外部インターフェース

本製品は、既存システムと連携が可能となるよう複数のインターフェースを有しています。



## 4. クライアントの操作

### 4.1. 端末管理

本製品の操作については、Windows用の専用の管理ソフトウェア(ARFaceManager.exe)にて操作します。本章以降で、管理ソフトウェアの操作方法について説明いたします。

### 4.2. 操作環境

本製品の設定を実施する場合、以下図のように管理ソフトウェアがインストールされたPCと本製品とが同一ネットワーク内にある必要があります。

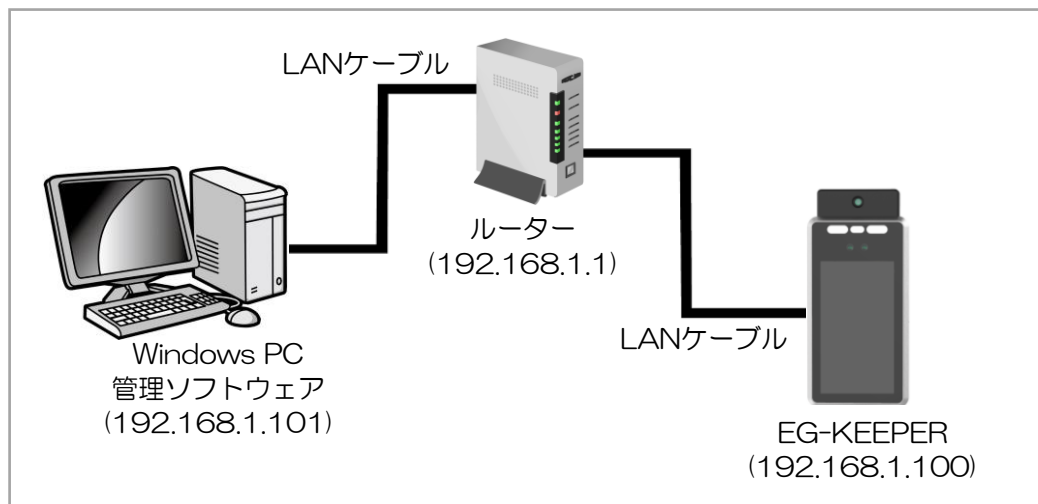


図:EG-KEEPER設定環境

なお、PC側では、管理ソフトウェアを起動フォルダの構成は以下となります。

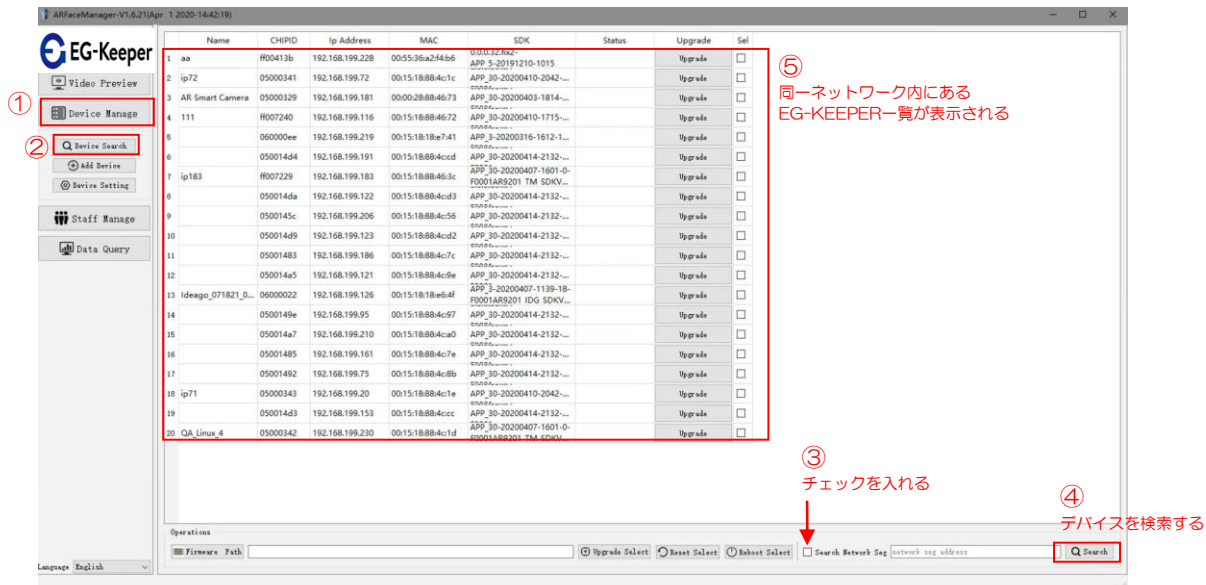
PC-TOOL		
—	ARFaceManager_V1.6.27.exe	:管理ソフトウェア
—	staff.xlsx	:ファイル登録用フォーマットファイル
—	res	:ログファイル格納フォルダ
—	192.168.1.100	:端末データ格納フォルダ(端末と接続し、起動後自動で生成)
—	attend	:端末内部にて保存している画像データ保存フォルダ
—	faces	:端末登録済みユーザー画像データ
—	snapshot	:端末にて取得したスナップショット画像可能フォルダ

## 4.3. 設定

### 4.3.1. 端末の登録

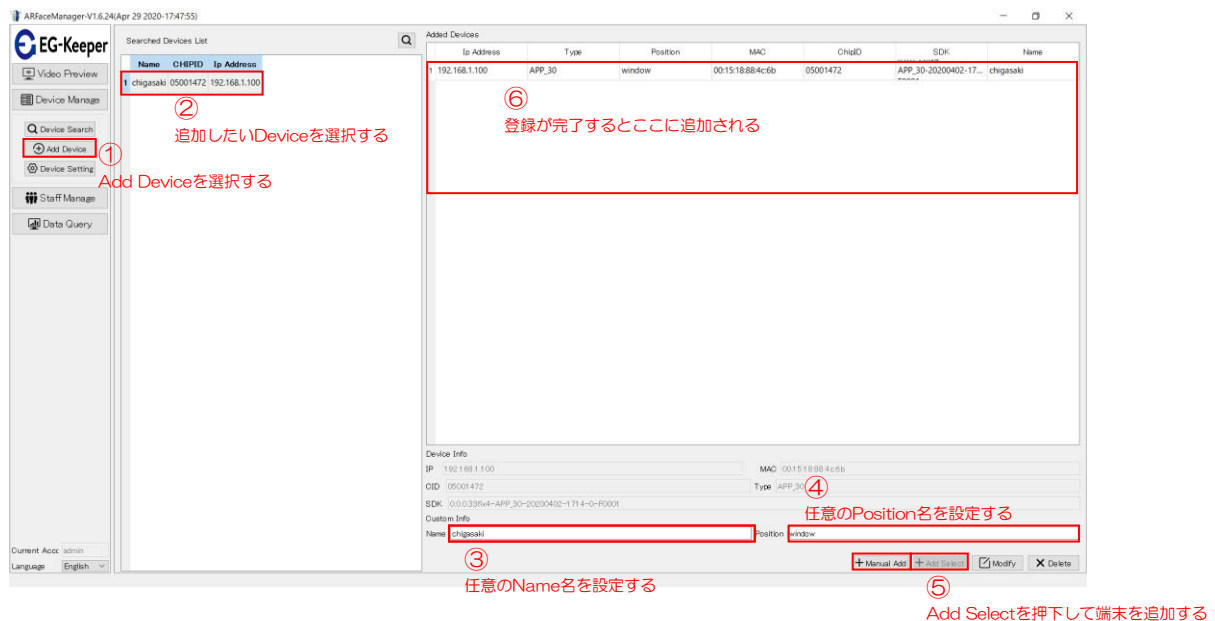
#### 4.3.1.1. 端末の検索

コントロールパネルの左側で、[Device Manage]-> [Device Search]を選択後、右下の“Search Network Seg”にチェックを入れた後、“Search”を押下して追加する端末を検索します。



#### 4.3.1.2. 端末の登録

端末検索後、コントロールパネルの左側で、[Device Manage]-> [ADD Device]を選択し、“Searched Devices List”内に表示されたリストより追加する端末を選択し、“Custom Info”項目の“Name”と“Position”欄に任意のデータを入力し“Add Select”を押下すると端末が登録されます。



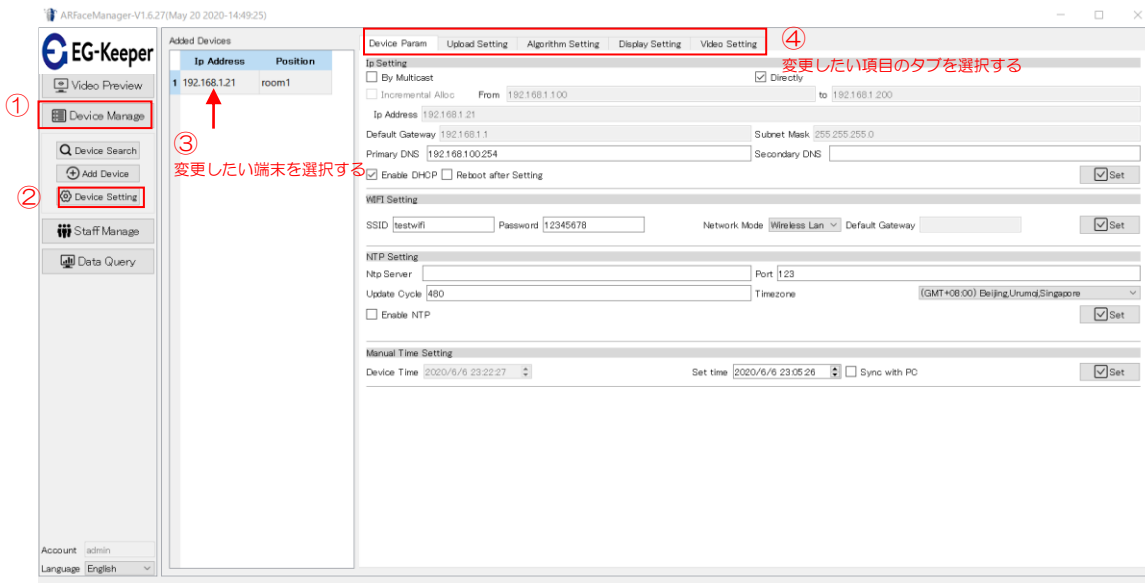
#### 4.3.1.3. 端末の設定

追加した端末毎に以下の設定が可能です。設定手順については、コントロールパネルの左側で、[Device Manage]->[Device Setting]を選択後、右側画面上部のタブを選択して設定を実施します。

[Device Param] / [Upload Setting] / [Algrithom Setting] / [Display Setting] / [Video Setting]

#### 4.3.1.4. Device Param

本設定では、登録したデバイスのインターネット設定を実施します。

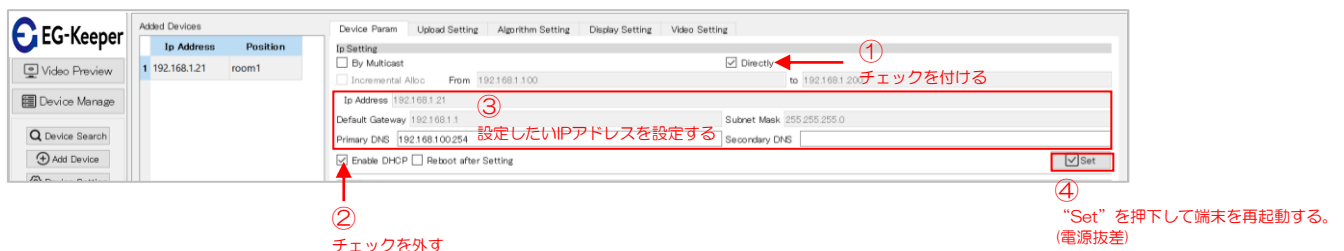


IP Setting	端末のIPアドレスを設定します。
WIFI Setting	端末を無線接続する場合の設定を実施します。
NTP Setting	端末の時刻を設定する際のNTPサーバーの設定を実施します。
Manual Time Setting	手動で端末の時刻を設定します。

変更した内容を有効にする場合、各項目内にある[Set]ボタンを押下します。

#### 4.3.1.5. IPアドレス設定

端末のIPアドレスを変更したい場合、“Ip Setting”で設定を変更します。



ルータへ接続されている場合、デフォルトでDHCP有効となっている為、自動でIPアドレスが割り振られています。個別でIPアドレスを設定したい場合、“Directly”にチェックを入れ、“Enabale DHCP”のチェックを外します。

マルチキャストIPアドレスを設定したい場合、“By Multicast”にチェックを入れ、“IP Address”へアドレスを入力します。合わせて、“Default Gateway”、“Subnet Msk”、“Primary DNS”のアドレスも設定して“Set”ボタンを押下します。

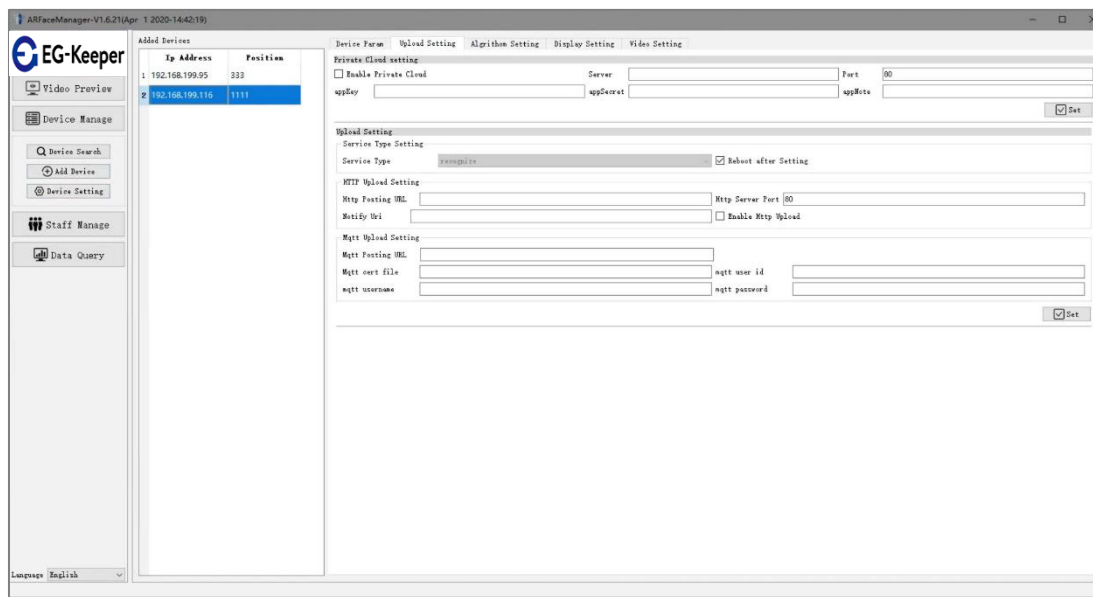
#### 4.3.1.6. WIFI設定

端末を無線接続したい場合、接続先無線ルータの”SSID“、”Password“を設定し、[Network Mode]を”Wireless Lan”に設定します。



#### 4.3.1.7. Upload Setting

本設定では、管理データをアップロードするクラウドサーバーの設定を実施します。



Private Cloud setting	端末のIPアドレスを設定します。
Upload Setting	端末の時刻を設定する際のNTPサーバーの設定を実施します。

#### 4.3.1.8. Private Cloud setting

本項目では、接続するクラウドサーバーの設定を実施します。実施手順は以下となります。

1. [Enable Private Cloud]にチェックしてください。
2. Server IPアドレス、ポート、appKey、appSecret、appNoteを入力します。  
※appKey / appSecret / appNoteについてはクラウドサーバー側から入手する必要があります。
3. 「Set」を押下するとサーバー側と同期します。

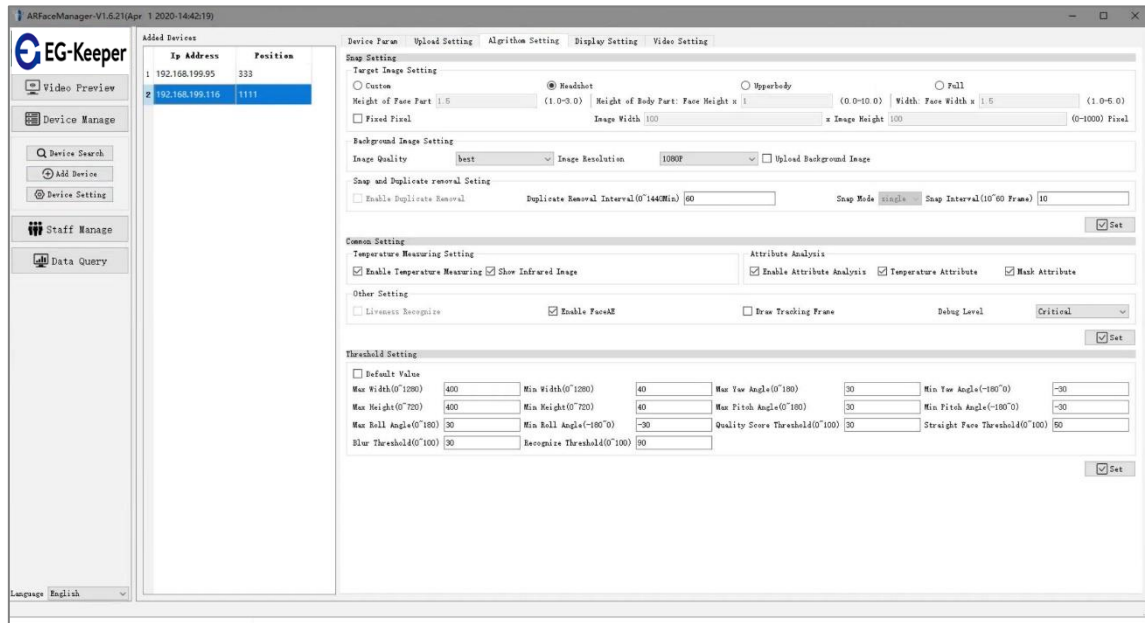
#### 4.3.1.9. Upload Setting

本項目では、クラウドサーバーへデータをアップロードする場合のプロトコルの設定を実施します。  
なお、対応するプロトコルは、HTTPおよびMQTTをサポートしており、同時に利用することも可能です。



#### 4.3.1.10. Algrithom Setting

本設定では、認証を実施する際の設定値を設定します。設定可能な項目は、以下となります。  
設定項目としては、画像判定範囲 / 背景画像 / 閾値 / その他パラメータの設定が可能です。

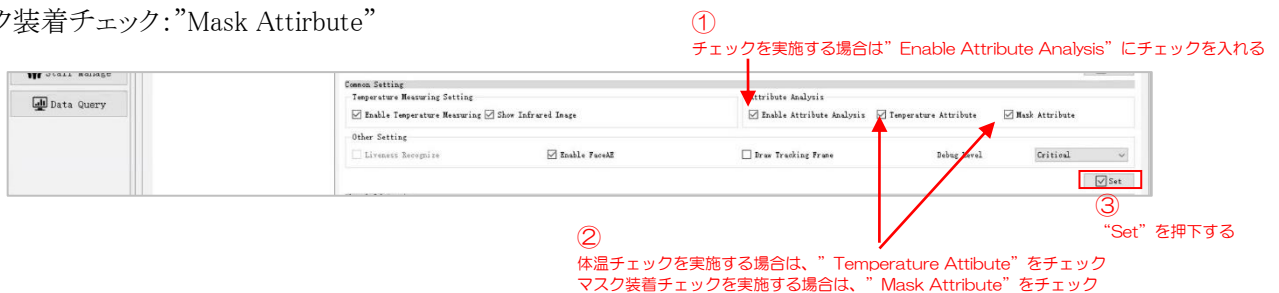


#### 4.3.1.11. マスク装着状態／体温状態チェック実施設定

端末でマスク装着状態や体温チェックを実施したい場合、Common Setting の【Attribute Analysis】項目で以下にチェックを実施します。

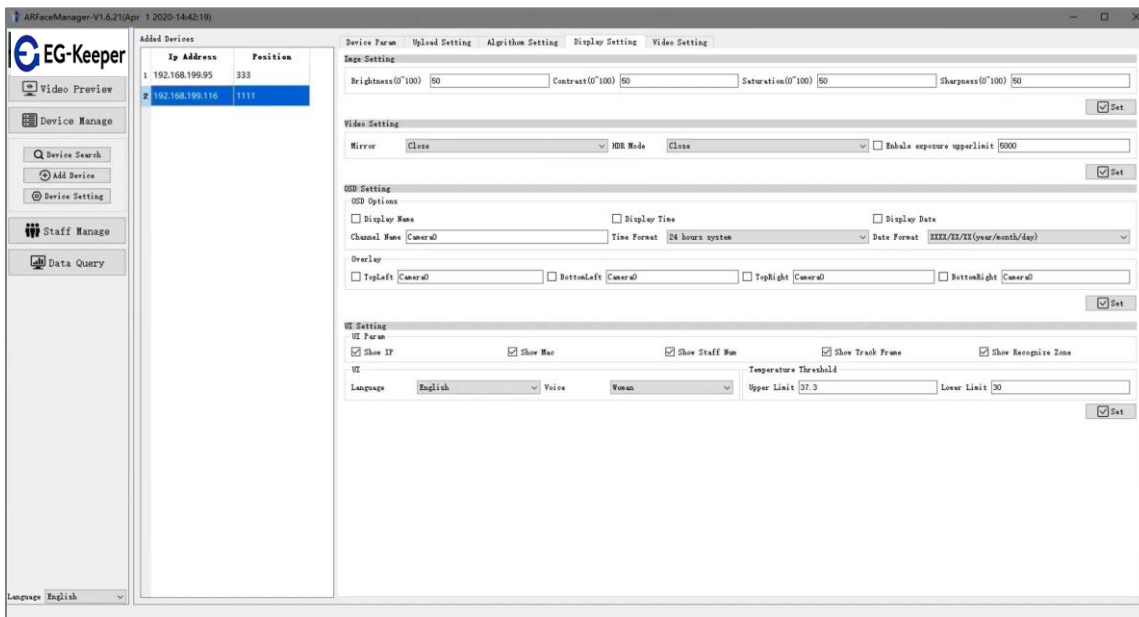
チェックを実施する場合は、必ず”Enable Attribute Analysis”にチェックをいれてください。その後、個別でチェックを実施したい項目にチェックを実施します。

体温状態チェック:”Temperature Attribute”  
マスク装着チェック:”Mask Attribute”



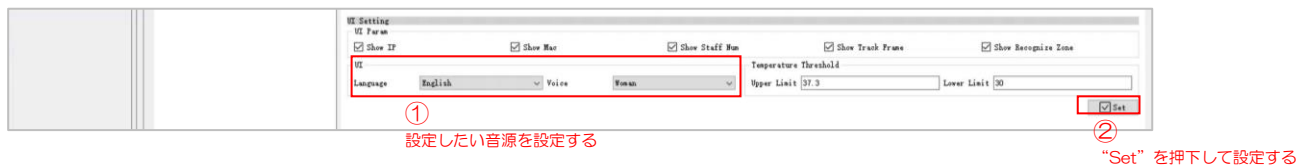
#### 4.3.1.12. ディスプレイの設定

本設定では、ディスプレイの設定値を設定します。設定項目は、以下となります。  
設定項目としては、ディスプレイの明暗や認証時の音声および表示項目などの設定が可能です。



#### 4.3.1.13. 音声パターン設定

音声案内をする際の音源の変更をしたい場合、Attendace Machine Settingsの【UI】項目で変更します。



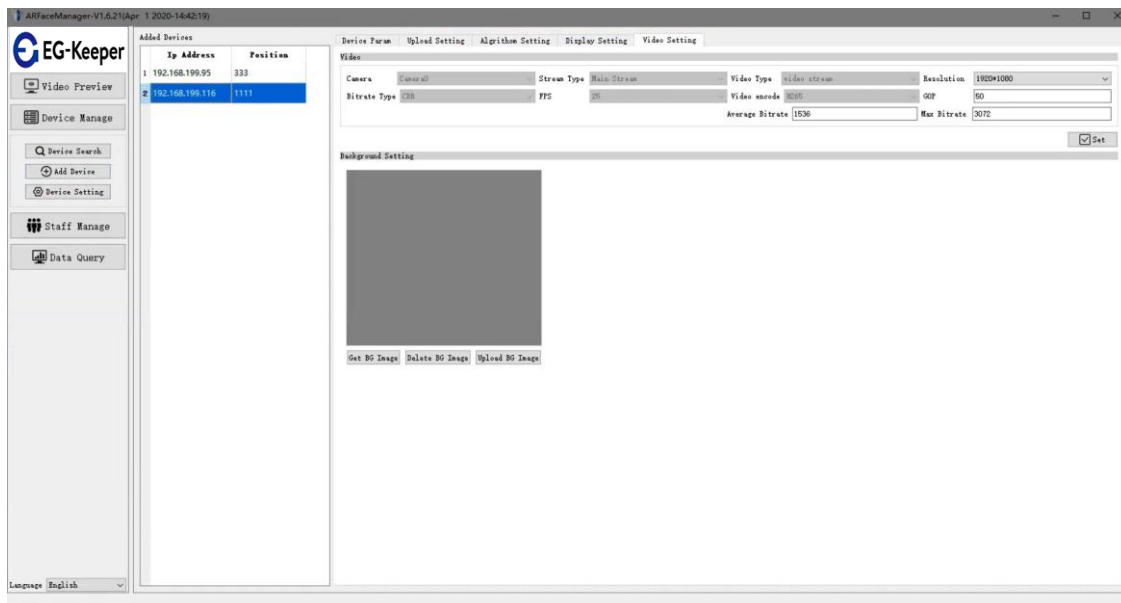
#### 4.3.1.14. 体温状態チェック閾値設定

体温状態のチェックの閾値を変更したい場合、Attendace Machine Settingsの【Temperature Threshold】項目で変更します。



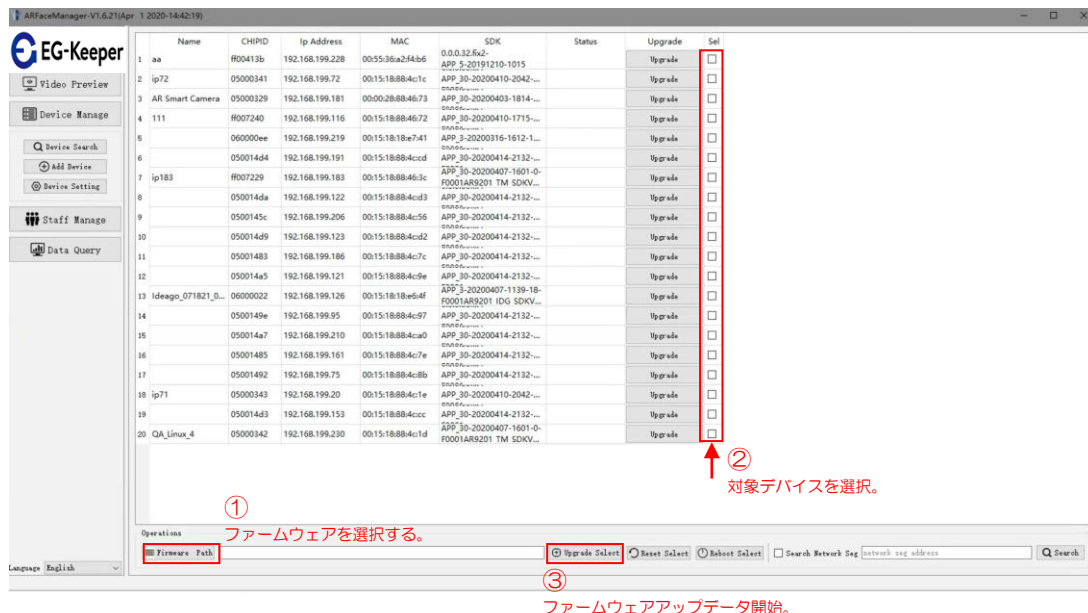
#### 4.3.1.15. ビデオ 設定

本設定では、映像方式の設定を実施します。なお、サポートフォーマットとしては、H.265およびH.264となります。



#### 4.3.2. 端末のファームウェアアップデート

端末検索後、左下の”Firmware Path”を押下してPC上に保存したファームウェアファイルを選択します。ファームウェア選択後、アップデートしたい端末の横の”Sel”ボックスにチェックをいれ、”Upgrade Select”ボタンを押下します。ボタン押下後暫くすると”Status”箇所へ進捗状況が表示されます。

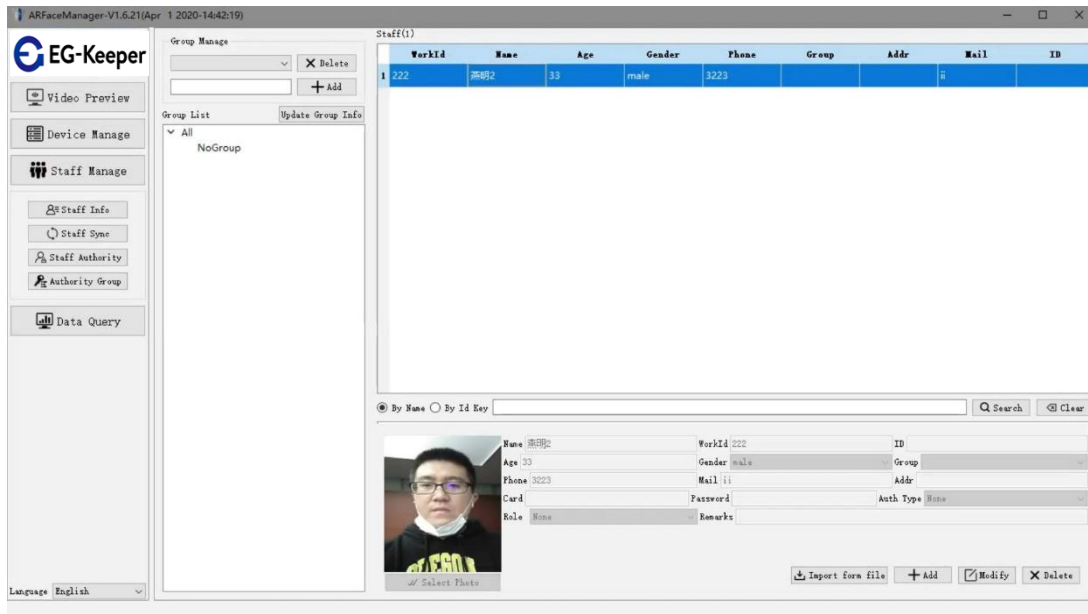


## 4.4. ユーザー管理

本章では、端末で認証するユーザーの管理方法について記載します。

### 4.4.1. ユーザー追加

コントロールパネルの左側で、[Staff Manage]-> [Staff Info]を選択します。

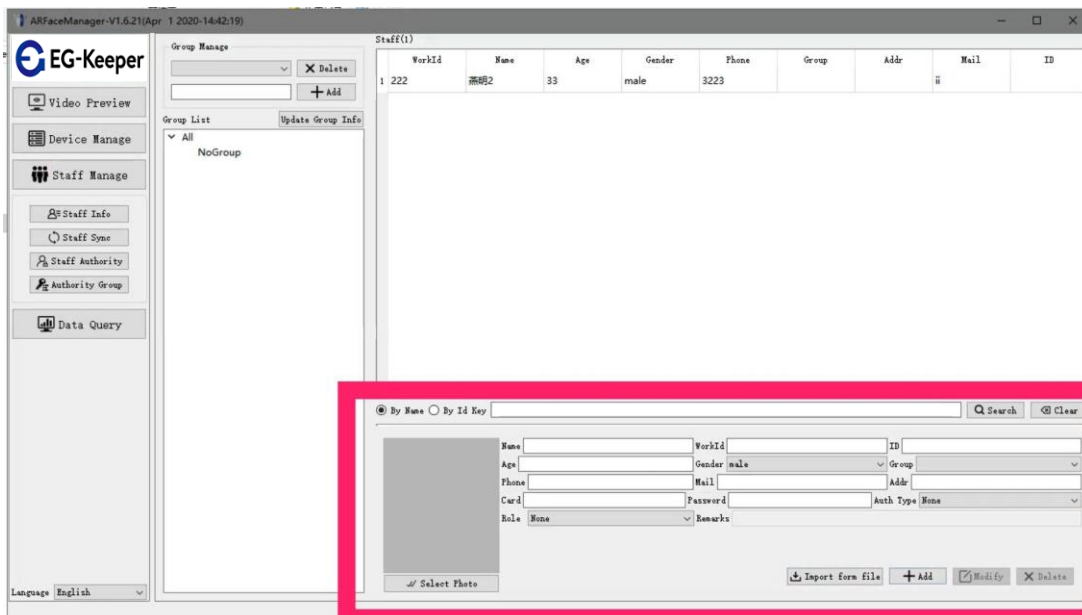


1. 画面右下の「Add」ボタンを押下するとユーザー情報が編集可能となります。

なお、[name]、[WorkId] (1~9999999)、[ID]、[Select Photo]の登録は必須となります。

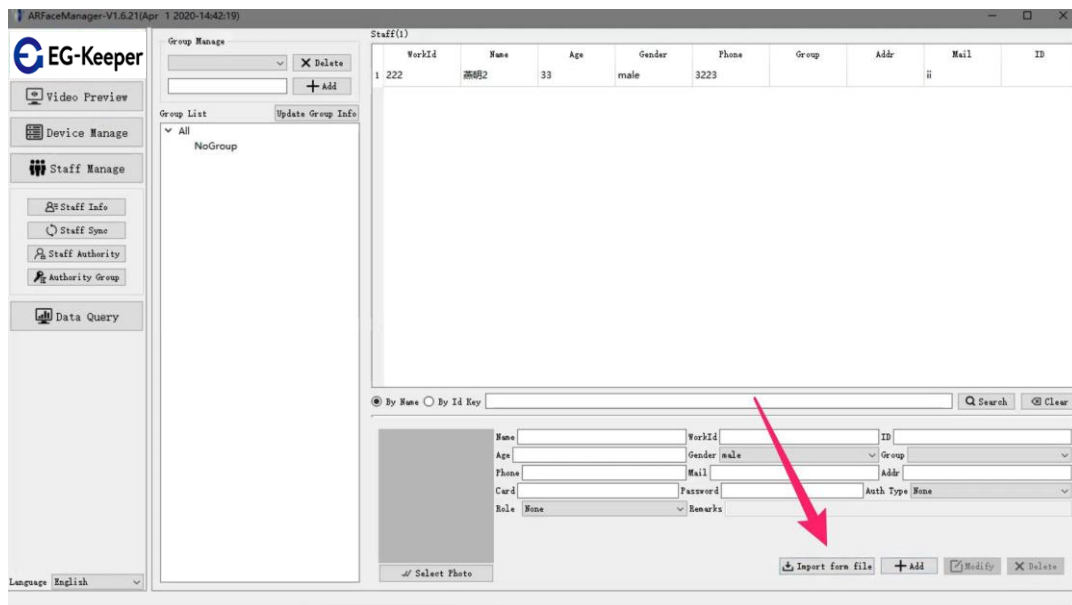
パラメータ記載後、[Add]ボタンを押下するとユーザー情報がローカルデータベースに登録されます。

(端末側へはまだ登録されていません。)



#### 4.4.2. ファイルからユーザー追加

コントロールパネルの左側で、[Staff Manage]-> [Staff Info]を選択します。

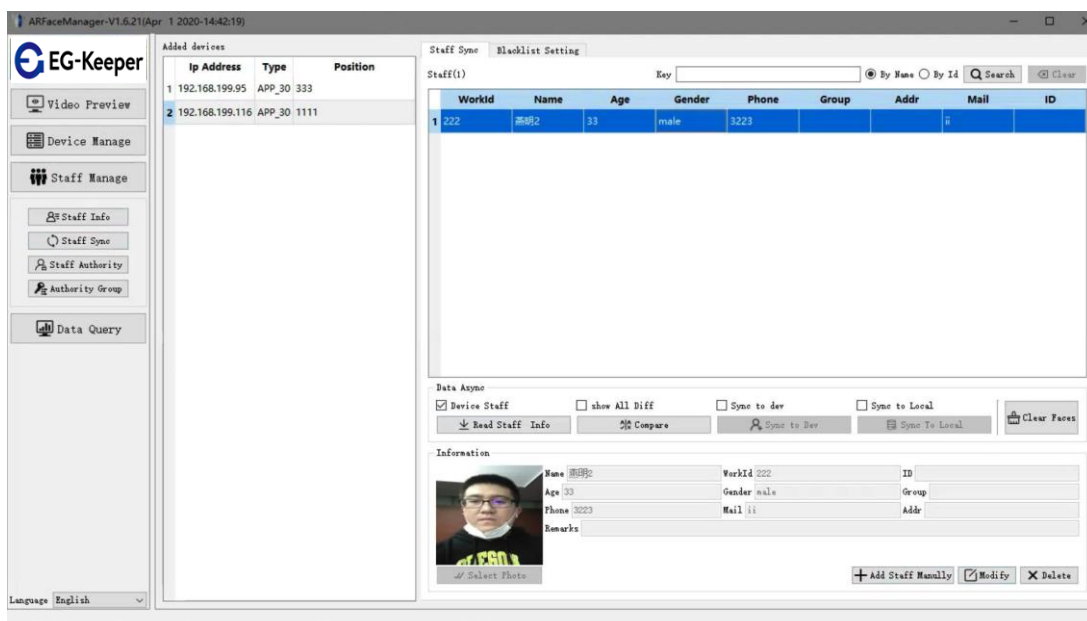


1. 画面右下の「Import from file」ボタンを押下し、登録したい情報が記載されたエクセルファイルを選択し、ファイルを読み込むことで一括登録が可能となります。

#### 4.4.3. ユーザー編集

登録済のユーザーを編集する場合、コントロールパネルの左側で、[Staff Manage]-> [Staff Sync]を選択します。

1. 画面右下の「Modify」ボタンを押下し、登録した情報の編集を行います。変更完了後、[Confirm]ボタンを押下して編集を終了します。



#### 4.4.4. ユーザーの削除

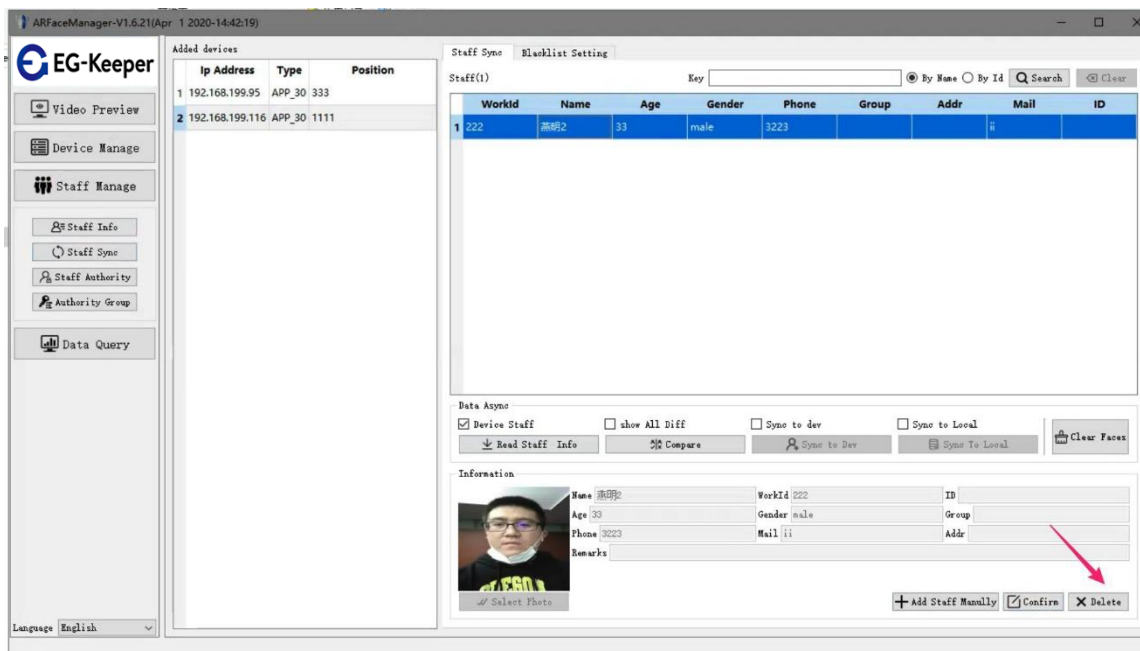
登録済のユーザーを削除する場合、コントロールパネルの左側で、[Staff Manage]-> [Staff Sync]を選択します。

- 削除

削除したいユーザーを選択し、画面右下の「Delete」ボタンを押下します。

- 一括削除

複数のユーザーを一括で削除したい場合、Ctrlキーを押して複数のユーザーを選択するか、Ctrl + Aキーを押してすべてのユーザーを選択し、画面右下の「Delete」ボタンを押下します。

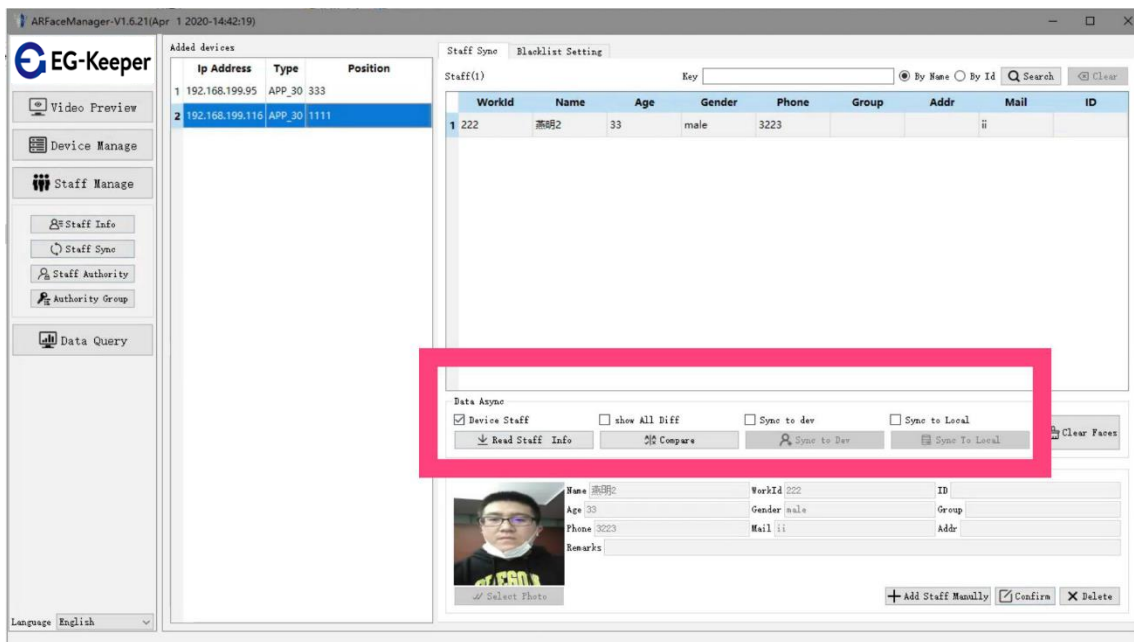


#### 4.4.5. 登録ユーザー同期

管理アプリにて登録したユーザーを端末側と同期するための方法は以下となります。

登録済のユーザーを編集する場合、コントロールパネルの左側で、[Staff Manage]-> [Staff Sync]を選択します。

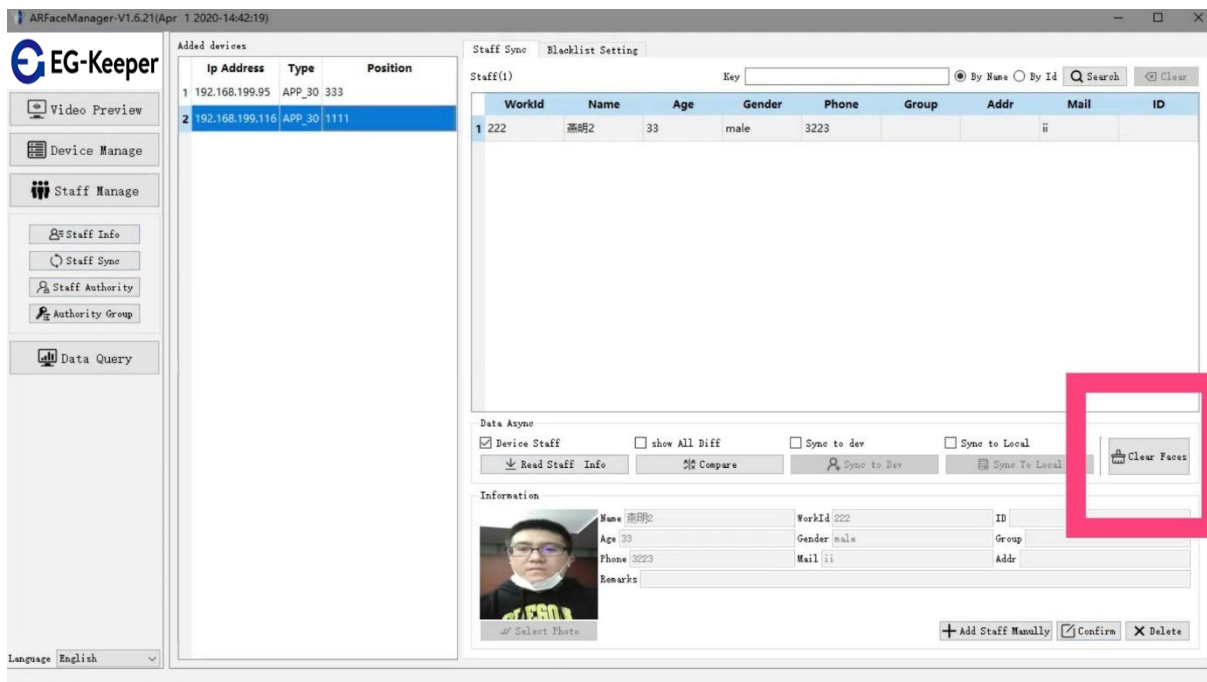
1. 画面中央のData Async欄内の「Read Staff Info」ボタンを押下し、管理アプリ側で管理しているユーザー一覧を表示します。
2. 「Syow All Diff」ボタンを押下し、端末側に登録済みのユーザー一覧と比較を実施します。  
※黄色は、情報がPC側にあるが端末側にはないことを示します。  
灰色は、情報が端末側に既に登録済だが、PC側にはないことを示します
3. 「Sync to dev」ボタンを押下し、PC側の情報を端末側へインポートします。
4. 「Sync to local」ボタンを押下し、端末側の情報をエクスポートし、PC側管理情報と同期させます。



#### 4.4.6. 作成ユーザーの削除

作成したユーザーを削除する場合、コントロールパネルの左側で、[Staff Manage]-> [Staff Sync]を選択します。

1. 画面中央のData Async欄内の「Clear Faces」ボタンを押下し、ユーザーを削除します。
2. 「Read Staff Info」ボタンを押下し、ユーザーがクリアされているかどうか確認ができます。

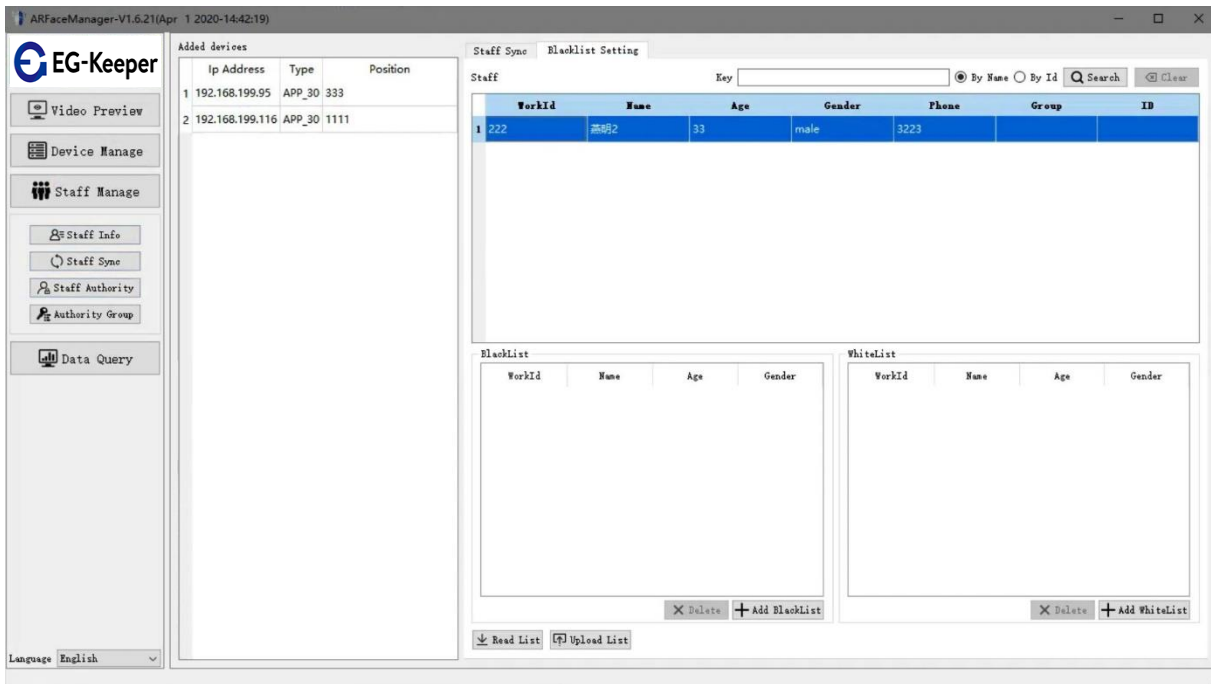




#### 4.4.7. ブラックリストとホワイトリスト

端末側で利用するブラックリストとホワイトリストを作成する場合、コントロールパネルの左側で、[Staff Manage]-> [Staff Sync]を選択し、[Blacklist Setting]のタブを開きます。

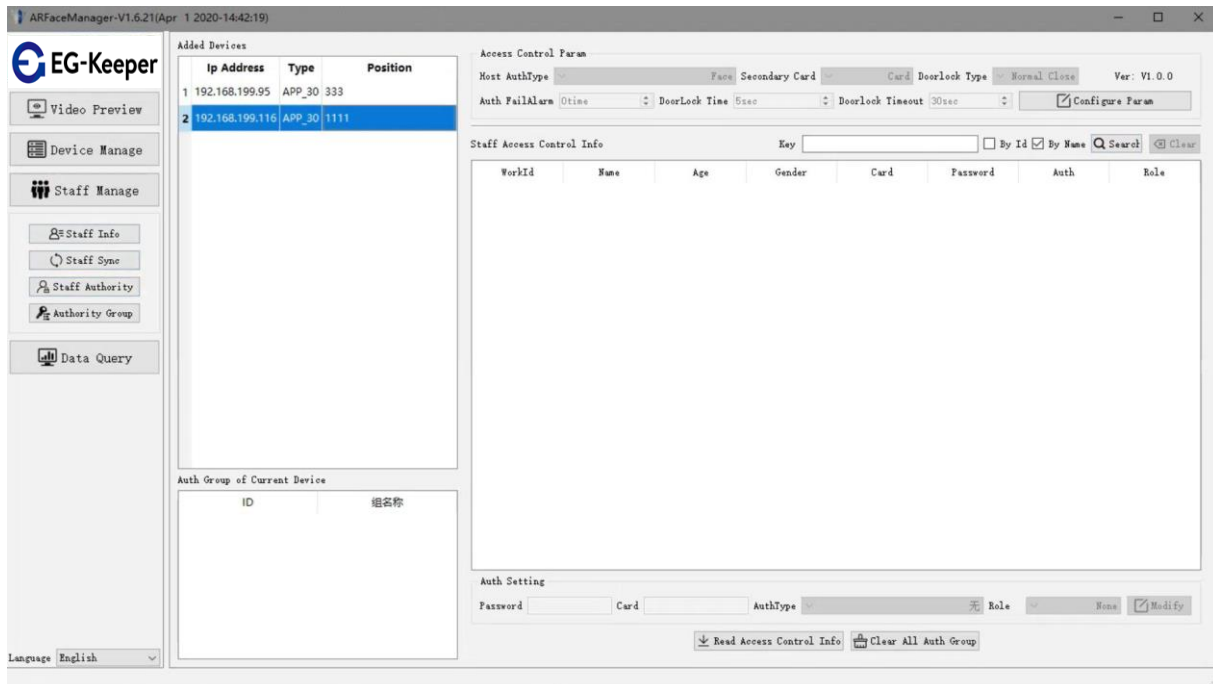
1. ブラックリストを設定したいデバイスを[Added devices]より選択します。
2. ブラックリストに追加したいユーザー[Staff]欄より選択します。
3. 「Add BlackList」ボタンを押下してリストを作成します。  
※whiteListに登録したい場合は、「Add WhiteList」ボタンを押下します。
4. 作成したリストを「Upload List」を押下して、端末側へアップロードします。



#### 4.4.8. 認証制限の付与

端末へ認証制限を実施する場合、コントロールパネルの左側で、[Staff Manage]-> [Staff Authority]を選択します。

1. Access Control Paramの[Configure Param]を押下し認証方法を設定します。  
※設定項目については、以下の表を参照。
2. 作成完了後、[Confirm]ボタンを押下します。



Access Control param	説明	備考
Host Auth Type	端末側で実施する認証方法を設定します。認証方法については、以下の表を参照。	現状、顔認証のみサポート
Secondary Card	カード認証での設定を実施します。	現状、カードのスイープとパスワードのみサポート
Doorlock Type	電子キーの状態を設定します。	0 - 通常閉(default) 1 - なし 2 - 通常開
Auth FailAlarm	認証失敗回数を設定します。	0-9。デフォルトは0で、試行が失敗してもアラームは鳴りません。
DoorLock Time	認証後もドアが開けられない場合にアラームがなるように設定します。	1~255秒。デフォルトでは5秒。
Doorock Timeout	ドアが開いたままの状態の時、アラームがなるように設定します。	1~255秒。デフォルトでは30秒。

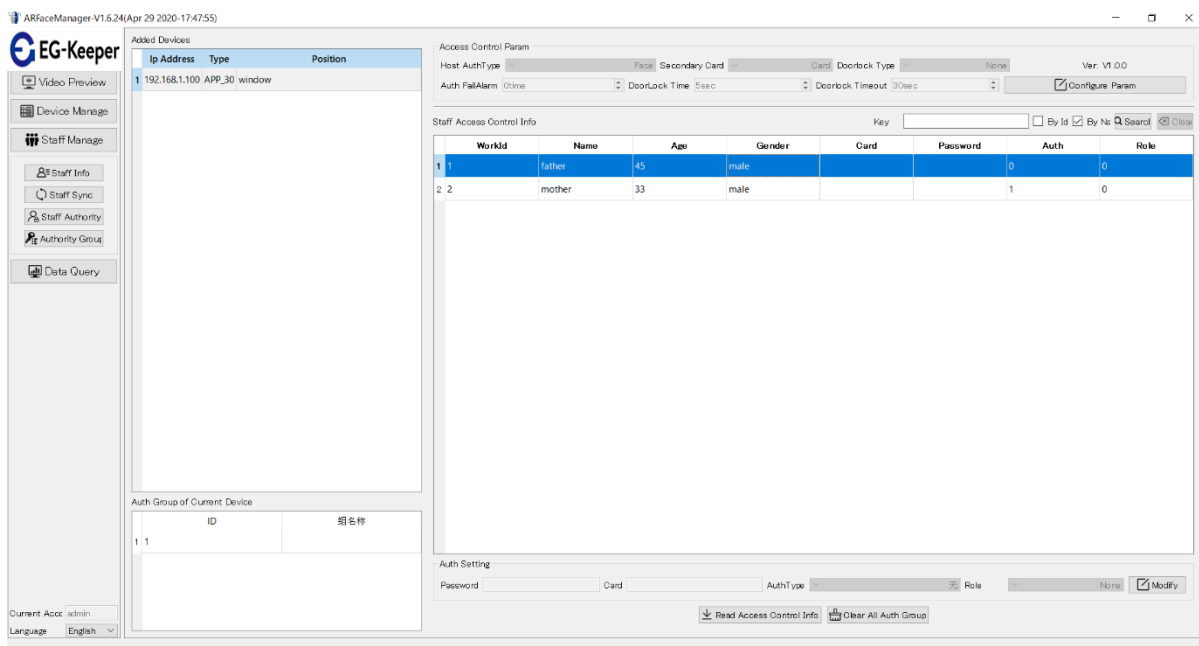
認証方法の組合せ一覧は以下となります。なお、認証方法で”/”はどちらかで認証が可能。”+”は全てで認証が可能といった組み合わせとなります。

認証組合せパターン
顔
顔/指紋
顔/指紋/パスワード
顔/指紋/カードスワイプ
顔/指紋/パスワード/カードスワイプ
顔/パスワード
顔/パスワード/カードスワイプ
顔/カードスワイプ
指紋
指紋/パスワード
指紋/カードスワイプ
指紋/パスワード/カードスワイプ
パスワード
パスワード/カードスワイプ
カードスワイプ
顔+指紋
顔+指紋+パスワード
顔+指紋+カードのスワイプ
顔+指紋+パスワード+カードのスワイプ
顔+パスワード
顔+パスワード+カードスワイプ
フェイス+カードスワイプ
指紋+パスワード
指紋+カードのスワイプ
指紋+パスワード+カードのスワイプ
パスワード+カードのスワイプ

#### 4.4.9. ユーザーアクセス情報

端末へのユーザー認証状況を確認する場合、コントロールパネルの左側で、[Staff Manage]-> [Staff Authority]を選択します。

1. [Read Access Control Info]を押下します。
2. 登録済ユーザーのアクセス状況が確認できます。



The screenshot shows the EG-Keeper application interface. The left sidebar contains navigation options: Video Preview, Device Manage, Staff Manage, Staff Info, Staff Sync, Staff Authority, Authority Group, and Data Query. The main area is titled 'Access Control Param' and includes a table for 'Staff Access Control Info'. The table has columns for WorkId, Name, Age, Gender, Card, Password, Auth, and Role. Two rows are visible: one for 'father' (Age 45, Gender male) with Auth 0, and one for 'mother' (Age 33, Gender male) with Auth 1. Below the table, there are buttons for 'Read Access Control Info' and 'Clear All Auth Group'. The bottom status bar shows 'Current Acc: admin' and 'Language: English'.

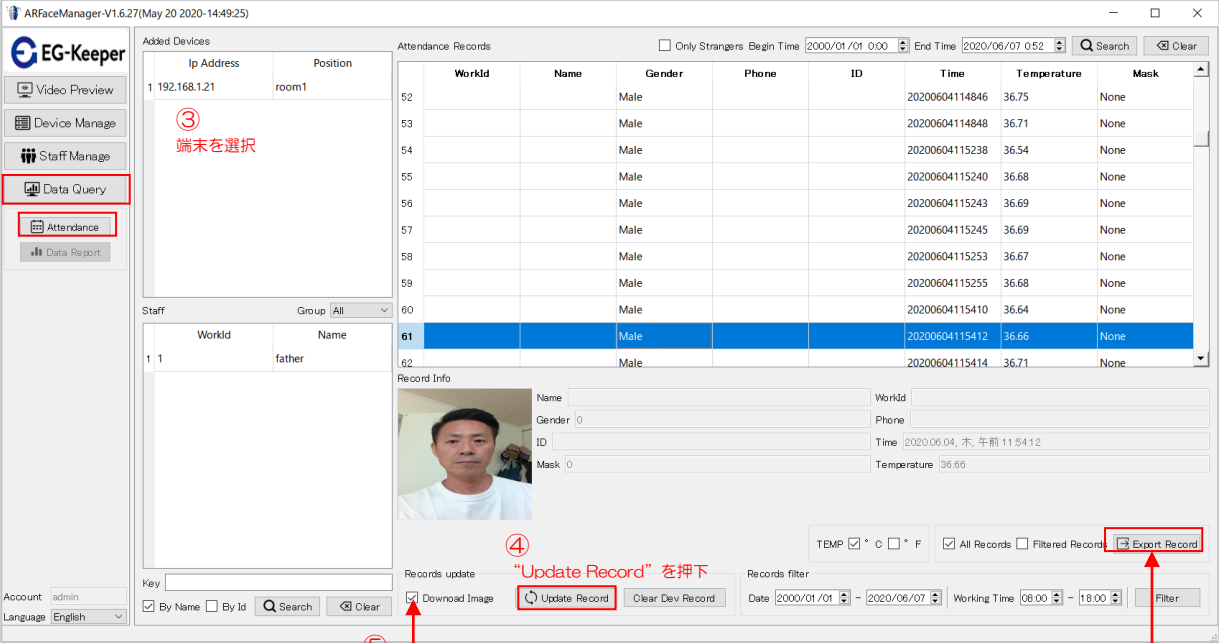
WorkId	Name	Age	Gender	Card	Password	Auth	Role
1	father	45	male		0	0	
2	mother	33	male		1	0	

## 5. データクエリ

### 5.1. 認証記録の確認

端末での認証した情報を確認する場合、コントロールパネルの左側で、[Data Query]-> [Attendance]を選択します。

1. 確認したい端末を選択し、[Update Record]を押下します。
2. 端末側で認証したユーザーの記録が一覧に表示されます。



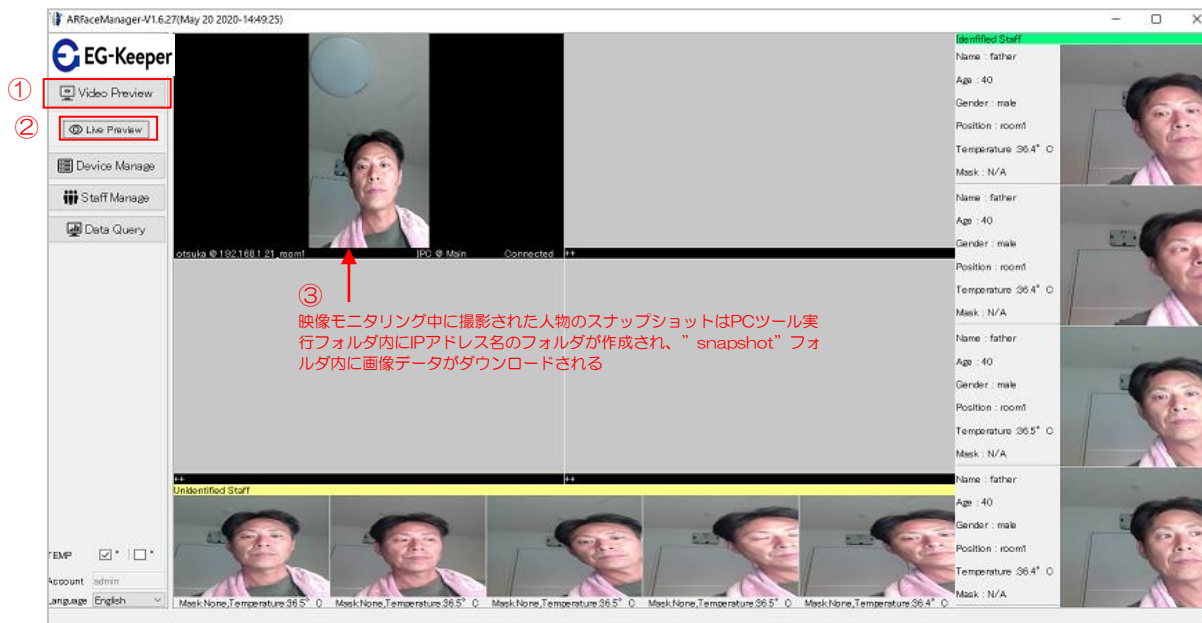
The screenshot shows the ARFaceManager-V1.6.27 application interface. The sidebar on the left contains buttons for 'Data Query' (1) and 'Attendance' (2). The main area displays a table of 'Attendance Records' with columns for Workid, Name, Gender, Phone, ID, Time, Temperature, and Mask. A record with Workid 61 is selected. Below the table is the 'Record Info' section, which includes a photo of a man and fields for Name, Gender, ID, Time, and Temperature. The 'Export Record' button (6) is highlighted in the bottom right. At the bottom of the interface, there are buttons for 'Download Image', 'Update Record' (4), and 'Clear Dev Record'. A red arrow points to the 'Update Record' button with the text '“Update Record” を押下'. Below the interface, there are two red annotations: (5) 'チェックするとPCツール実行フォルダ内にIPアドレス名のフォルダが作成され、“attend”フォルダ内に画像データがダウンロードされる' and (6) 'PCツール実行フォルダ内にIPアドレス名のフォルダが作成され、その下に”日付+時間.xlsx”名のファイルがダウンロードされる'.

### 5.2. 認証記録のエクスポート

1. 記録したデータをPCへダウンロードする場合、[Export Record]ボタンを押下するとエクセルファイルがダウンロードされます。

### 5.3. スナップショット取得

端末の前を通過した人物のスナップショットを取得する場合、【Video Preview】→【Live Preview】を選択し、リアルタイムに映像をモニタリングしておく必要があります。



## 6. クイックアクセスガイド


ここでは、製品を購入後すぐにご利用頂くための簡易操作手順について記載します。

### 6.1. 簡易操作手順一覧

管理ソフトウェアへ端末を登録する		実施する内容	記載ページ
手順①	操作環境を構築する	4.2. 操作環境のネットワークを構成する	5ページ
手順②	端末を検索する	4.3.1.1. 端末の検索を実施する	6ページ
手順③	端末を登録する	4.3.1.2. 端末の登録を実施する	6ページ
端末へユーザーを登録する(1人)			
手順①	管理ソフトウェアへユーザーを追加する	4.4.1. ユーザー追加を実施する	12ページ
手順②	端末に管理ソフトで追加したユーザーを登録する	4.4.5. 登録ユーザー同期を実施する	15ページ
端末へユーザーを登録する(複数同時)			
手順①	管理ソフトウェアへファイルから同時に複数のユーザーを登録する	4.4.2. ファイルからユーザー追加	13ページ
手順②	端末に管理ソフトで追加したユーザーを登録する	4.4.5. 登録ユーザー同期を実施する	15ページ
ネットワーク設定を変更する			
手順①	端末設定メニューを開く	4.3.2. 端末の設定を実施する	7ページ
手順②	デバイスパラメータのIPアドレスを変更する	4.3.2.2. IPアドレス設定を実施する	7ページ
マスク装着／体温状態チェックを実施する			
手順①	端末設定メニューを開く	4.3.2. 端末の設定を実施する	7ページ
手順②	端末のAlgrithom Settingを設定する	4.3.2.7. Algrithom Settingを開く	9ページ
手順③	マスクの装着／体温状態チェックを設定する	4.3.2.8. マスク装着状態／体温状態チェック実施設定を設定する	9ページ
認証記録を確認する／ファイルへ出力する			
手順①	認証記録を参照する	5.1. 認証記録の確認を実施する	21ページ
手順②	認証記録をファイルへ出力する	5.2. 認証記録のエクスポートを実施する	21ページ
手順③	スナップショットを取得する	5.3. スナップショット取得を実施する	22ページ

### 6.2. ユーザー登録時の設定内容

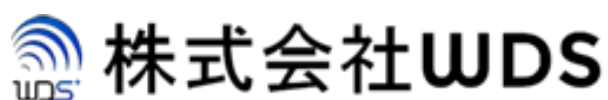
ユーザーを登録する際に記入する各設定項目の内容について記載します。

 <p>顔認証に利用する写真</p> <p>Select Photo</p>	Name	ユーザー名	WorkId	端末への登録番号	ID	社員番号など
	Age	年齢	Gender	male 性別(male / female)	Group	管理する所属グループ
	Phone	電話番号	Mail	メールアドレス	Addr	住所
	Card	カード認証利用時の暗証番号	Password	パスワード認証時のパスワード	Auth Type	None 認証方式
	Role	None 付与権限設定	Remarks	備考欄		
	<p>Import form file    + Add    Modify    Delete</p>					

## 7. お問い合わせ先

お問合せ、ご質問につきましては以下へご連絡ください。

お問合せ先メールアドレス：[info@wd-s.com](mailto:info@wd-s.com)



株式会社WDS(ダブリューディーエス)

〒116-0013

東京都荒川区西日暮里2-22-1 ステーションプラザタワー504号