

ロジテック 顔認証コネクトデバイスⅡ LTC-FPT50/IP専用 勤怠連携導入前チェックリスト

ご注意

設置・設定及び勤怠連携設定サービスをご利用のお客様は**本チェックリストの実施結果を導入準備シートのチェック項目へ記入**をお願いします。
記載漏れがある場合はサービスの提供を保留とさせていただく場合があります。スムーズな導入に向けて事前確認のご協力をお願い申し上げます。

Vol.1

ロジテックINAソリューションズ株式会社

No	区分	カテゴリ	使用する機能	確認事項	対応者	チェック
1	導入前	設置・設定サービス	導入全般	設置サービスに必要な「導入準備シート」にネットワーク情報および各種設定値を漏れなく記入し、設置希望日の3週間前までに提出してください。サービス当日までにネットワーク設計（Windows PC/サーバー＝管理PC、顔認証端末に関する設定情報、相互通信環境）を完了してください。	導入先の総務・管理部門の方	☐
2	導入前	設置・設定サービス	統合管理ソフト 打刻データ連携ツール 勤怠連携	統合管理ソフトと打刻データ連携ツールをインストールする管理PCを用意してください。運用に支障がない場合、稼働中のPC/サーバーもご利用いただけます。 ※WindowsのクライアントOSまたはサーバOSは、OSサポート期間が終了していないこと ※PCスペックはOSが必要とする最低スペックおよび【 統合管理ソフト動作要件 】 🔗 を満たすこと	導入先の総務・管理部門の方	☐
	導入前	設置・設定サービス	統合管理ソフト 打刻データ連携ツール	統合管理ソフト・打刻データ連携ツールのパッケージは、設置サービス当日に弊社が派遣するスタッフがUSBメモリに保存して持参します。USBメモリの持ち込みができない場合、事前にダウンロード案内をさせていただきます。お客様にて管理PCのデスクトップ上に解凍・保存のご協力をお願いします。	導入先の総務・管理部門の方	☐
3	導入前	検証機 動作環境要件	統合管理ソフト 製品機能全般	下記①～③の動作環境確認をお願いします。 ご不明な点は、 【biometrics-support@elecom.co.jp】 へお問い合わせください。 ①検証機および統合管理ソフト（試用版）を使用して、事前にお客様の管理用PC環境およびネットワーク環境での動作確認をお願いします。⇒【 疎通テスト方法 はこちら】 ※検証機のご用意は、お気軽にエレコム営業担当までご連絡ください。 ②統合管理ソフト（試用版）のダウンロードは下記リンクよりお願いします。 ⇒シリアル番号【55P2174006409】を入力して【 試用版ダウンロード 】 🔗 からお願いします。 ③ダウンロード後、管理PCへ統合管理ソフト（試用版）をインストールしてください。 インストール中に、お使いのPC環境が動作要件を満たしているかの確認が自動で行われます。 ⇒【 インストール手順 】 🔗 【 ソフトウェア環境テスト方法 】	・導入先の総務・管理部門の方 ・エレコム営業担当	☐
4	導入前	ネットワーク	統合管理ソフト 打刻データ連携ツール	管理PC（統合管理ソフト）および顔認証端末は、相互通信できる必要があります。離れた拠点間で運用する場合、VPN環境が必要です。検証機での疎通テスト「手順： P4 」を参照してください。	導入先のネットワーク管理者の方	☐
5	導入前	ネットワーク	統合管理ソフト 顔認証デバイス	管理PCおよび顔認証端末に割り当てられるIPアドレスは、固定IPアドレスで運用します。また、安定した通信を確保するため有線LAN接続（PoE対応）をご利用ください。	導入先のネットワーク管理者の方	☐
6	導入後	ネットワーク	統合管理ソフト 顔認証デバイス	管理PC及び顔認証端末が故障した際、故障前に割り当てられていた固定IPアドレスを再利用して新しい端末に設定します。これによりスムーズに運用を再開できます。	導入先のネットワーク管理者の方	☐
7	導入前	ネットワーク	無線/有線LAN 外部通信	顔認証端末は、 ネットワーク通信リスト（P7） に記載の宛先に通信を行います。外部アクセスを制限されている場合、通信リスト内容をホワイトリストへ登録して通信を許可してください。	導入先のネットワーク管理者の方	☐
8	導入前	ネットワーク	無線LAN	無線LANの認証方式はWPA/WPA2です。電波環境の改善が必要な場合、サービス当日までに対応を完了してください。なお、利用可能なWi-Fi規格は以下の通りです。 通信方式 IEEE 802.11 ac/a/b/g/n(2.4GHz/5GHz) 認証方式 WPA-PSK / WPA2-PSK 暗号化方式 CCMP(AES) / TKIP	導入先のネットワーク管理者の方	☐
9	導入前	ネットワーク	無線LAN (2.4GHz)	Wi-Fi規格の2.4GHz帯（b/g/n）は、障害物に強く、遠くまで電波が届く特性がありますが、一方で電波干渉を受け易い周波数帯ですが、設置環境に複数のAPや機器（Bluetooth製品や家電製品など）が存在する場合、5GHz帯へ変更または設置場所を変更してください。 200V電源付近や変電室付近、業務用エアコン付近は電波干渉が発生します。端末の設置を避けてください。	導入先のネットワーク管理者の方	☐

2

No	区分	カテゴリ	使用する機能	確認事項	対応者	チェック
10	導入前	セキュリティ	勤怠連携 打刻データ連携ツール	打刻データ連携ツールが動作する管理PCにセキュリティソフトが動作している場合、打刻データ連携ツールが動作する「フォルダ」及び「バッチファイル（*.bat）」を監視対象から除外設定をお願いします。セキュリティソフトにより動作制限や意図しない動作をする場合があります。下記は除外設定の参考ページですが、ソフトの種類やバージョンにより内容が異なる場合があります。各メーカーへお問い合わせをお願いします。 ※シマンテック社の除外設定（ご参考） https://support.norton.com/sp/ja/jp/home/current/solutions/v3672136 ※トレンドマイクロ社の除外設定（ご参考） https://helpcenter.trendmicro.com/ja-jp/article/tmka-18479	導入先のネットワーク管理者の方	☐
11	導入前	動作環境要件	勤怠連携 打刻データ連携ツール	当社が提供する打刻データ連携ツールは手動実行のプログラムです。自動実行するにはWindowsタスクスケジューラを使用する必要があります。タスクスケジューラを設定する場合、Administrator用の管理者アカウントとパスワードをご用意ください。なお、お客様ご自身で設定する場合、ユーザーズマニュアルをご参考にしてください。※【打刻データ連携ツールの実行方法】	ネットワーク管理者の方	☐
12	導入前 導入後	設置環境	勤怠打刻	1名が顔認証から打刻完了まで数秒かかります。打刻渋滞防止のため、顔認証端末1台あたりの利用人数（目安:50名以下）を、複数端末で負荷分散してください。	導入先の総務・管理部門の方	☐
13	導入前 導入後	設置環境	顔認証 生体検知機能	顔認証は、顔の特徴点を分析して本人特定を行うため「製品本体画面または被写体に直射日光や差し込み光、LED照明などの光が直接あたる場所」を避け、輪郭の白飛びや背景と同化、光が反射するものなどを避けてください。 ※ショーケースなどガラス越しの認証は顔認証端末のLEDが反射して認証できません。	導入先の総務・管理部門の方	☐
14	導入前 導入後	生体情報	認証精度	<u>生体認証機器の性質上、本人拒否（未登録判定）または他人受入（誤認判定）を完全に防ぐことはできません。</u>顔認証端末本体または本体以外で撮影する時は、<u>パスポート写真を撮影する時と同じ条件で撮影をお願いします。</u>認証率が悪い・誤認証が発生する場合、顔登録をやり直すことで改善します。詳細は誤認証発生時の再撮影フローを参照してください。 ※【顔登録・顔認証ガイドライン】	導入先の従業員の方	☐
15	導入時	バックアップ	バックアップ	<u>統合管理ソフトの「バックアップ」機能を使ってデータベースのバックアップを必ず行ってください。</u> 設置サービス当日までに外部ストレージをご用意いただければ、弊社でバックアップの設定をします。なお、管理PCや外部ストレージの故障等によるデータ消失やバックアップデータのデータに関する保証はできません。	導入先のお客様	☐
16	導入時	顔登録	ユーザー番号	ユーザー番号は、勤怠管理システム上で管理される、個人を特定するための社員番号やタイムカードコードなど一意の識別番号を入力します。この番号を照合して勤怠管理システムへ打刻データを登録します。	導入先のお客様	☐

顔認証コネクデバイス 検証機による疎通テスト

- 顔認証端末の検証機を2週間お貸しすることができます。検証機（以下「ターゲット端末」という）のお申込みは、エレコム営業担当までお問い合わせください。
※台数に限りがございます。お問い合わせ後に納期のご連絡をいたします。
- お客様にて拠点間の連携に必要なネットワーク（VPN環境含む）が構築されていることが前提となります。

疎通テストの方法 ①「管理用PC」から「顔認証デバイス」へ疎通テスト

- 「管理用PC」から「顔認証デバイス」へ疎通テスト（test-netconnectionコマンド）
 1. 管理用PC（統合管理ソフトウェアと打刻データ連携ツールをインストールするPC）を用意します。
 2. 事前にターゲット端末を設置予定の拠点に送付しネットワークに接続します。
 3. 予め決めた固定IPアドレスをターゲット端末に設定します。
※使用する固定IPアドレスは、DHCP（ルーター）側の設定で割り当て範囲から除外する必要があります。
設定詳細はネットワーク管理者へお問い合わせください。

IPアドレス設定方法

https://dl.logitec.co.jp/downloadfile/DLfile/LST-M/LTC-FPT50IP_um.pdf#page=243

4. 管理PCのWindows PowerShellを起動します。ターゲット端末のIPアドレスを使い、以下のコマンドを入力して通信テストを行います。

PowerShell : > test-netconnection [顔認証デバイスのIPアドレス]
入力例 : > test-netconnection 192.168.10.153

5. 通信テストの結果、ターゲット端末と通信ができることを確認します。
Falseの場合、ネットワーク管理者にご相談の上、原因究明と対策をお願いします。

テスト成功 → PingSucceeded:True

テスト失敗 → PingSucceeded:False

```
PS C:\> test-netconnection 192.168.10.153

ComputerName      : 192.168.10.153
RemoteAddress     : 192.168.10.153
InterfaceAlias    : イーサネット 2
SourceAddress     : 192.168.10.145
PingSucceeded     : True
PingReplyDetails (RTT) : 10 ms
```

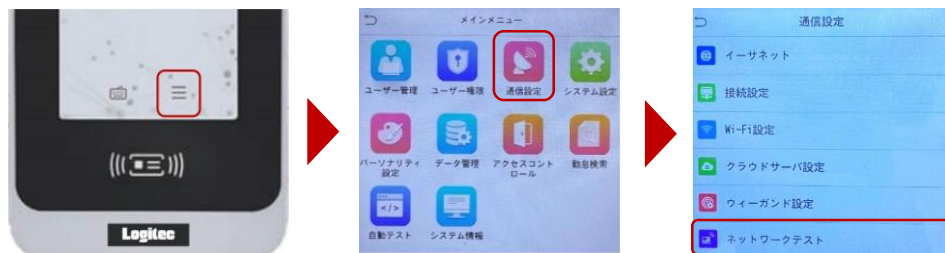
```
PS C:\> test-netconnection 192.168.10.152
警告: Ping to 192.168.10.152 failed -- Status: DestinationHostUnreachable

ComputerName      : 192.168.10.152
RemoteAddress     : 192.168.10.152
InterfaceAlias    : イーサネット 2
SourceAddress     : 192.168.10.145
PingSucceeded     : False
PingReplyDetails (RTT) : 0 ms
```

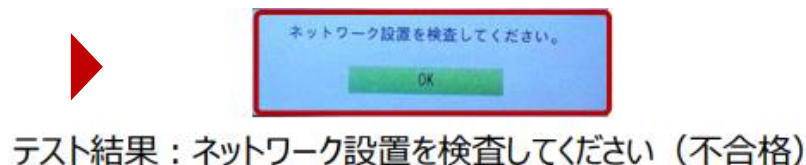
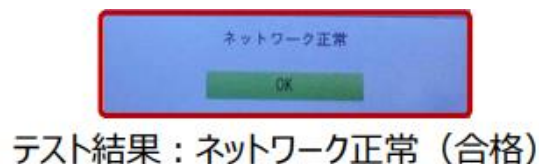
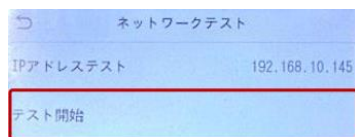
疎通テストの方法 ②「顔認証デバイス」から「管理PC」へ疎通テスト

●「顔認証デバイス」から「管理PC」へ疎通テスト（Pingコマンド）

1. 管理用PC（統合管理ソフトウェアと打刻データ連携ツールをインストールするPC）を用意します。
※管理用PCは実際に使用されるPC/サーバーを用意いただくことを推奨します。
2. 事前にターゲット端末を設置予定の拠点に送付しネットワークに接続します。
3. 予め決めた固定IPアドレスを管理PCに設定します。
※使用する固定IPアドレスは、DHCP（ルーター）側の設定で割り当て範囲から除外する必要があります。
設定詳細はネットワーク管理者へお問い合わせください。
4. 顔認証デバイスの右下の「三」をタップして「メインメニュー」を表示し、「通信設定」の「ネットワークテスト」をタップします。



5. 「3」で設定した管理PCの IP アドレスを「IPアドレステスト」へ入力し「テスト開始」をタップします。



疎通テストの方法 ③ 同一ネットワークの「PC」から「管理PC」へ疎通テスト

- 統合管理ソフトウェア（試用版）がインストールされていること
統合管理ソフトウェア（試用版）のダウンロードは下記よりお願いします。【[試用版ダウンロード](#)】
※ダウンロード認証に必要なシリアルナンバー（S/N）：55P2174006409
- お客様にて拠点間の連携に必要なネットワーク（VPN環境含む）が構築されていることが前提となります。
- 「PC」から「管理PC」へ疎通テスト（test-netconnectionコマンド）
 1. 管理用PC（統合管理ソフトウェアと打刻データ連携ツールをインストールするPC）を用意します。
※管理用PCは実際に使用されるPC/サーバーを用意いただくことを推奨します。
 2. 予め決めた固定IPアドレスを管理用PCに設定します。
 3. 同一ネットワークに接続されたPC（普段お使いの業務用PC）を用意します。
 4. PCのWindows PowerShellを起動します。管理PCのIPアドレスを使い、以下のコマンドを入力して通信テストを行います。
※テストを実施するポートは2つ（8098/8088）です。

PowerShell : > test-netconnection [管理PCのIPアドレス] -port 8098
入力例 : > test-netconnection 192.168.10.145 -port 8098

PowerShell : > test-netconnection [管理PCのIPアドレス] -port 8098
入力例 : > test-netconnection 192.168.10.145 -port 8098

5. 通信テストの結果、ターゲット端末と通信ができることを確認します。
Falseの場合、ネットワーク管理者にご相談の上、原因究明と対策をお願いします。

テスト成功 → TcpTestSucceeded:True

```
PS C:\Users\NittaTo> test-netconnection 192.168.10.145 -port 8098

ComputerName      : 192.168.10.145
RemoteAddress     : 192.168.10.145
RemotePort        : 8098
InterfaceAlias     : Wi-Fi
SourceAddress     : 192.168.10.158
TcpTestSucceeded  : True

PS C:\Users\NittaTo> test-netconnection 192.168.10.145 -port 8088

ComputerName      : 192.168.10.145
RemoteAddress     : 192.168.10.145
RemotePort        : 8088
InterfaceAlias     : Wi-Fi
SourceAddress     : 192.168.10.158
TcpTestSucceeded  : True
```

テスト失敗 → TcpTestSucceeded:False

```
PS C:\Users\NittaTo> test-netconnection 192.168.154.224 -port 8080
警告: TCP connect to (192.168.154.224 : 8080) failed
警告: Ping to 192.168.154.224 failed with status: TimedOut

ComputerName      : 192.168.154.224
RemoteAddress     : 192.168.154.224
RemotePort        : 8080
InterfaceAlias     : イーサネット 2
SourceAddress     : 203.236.140.29
PingSucceeded     : False
PingReplyDetails (RTT) : 0 ms
TcpTestSucceeded  : False
```

統合管理ソフトウェア 環境テスト方法

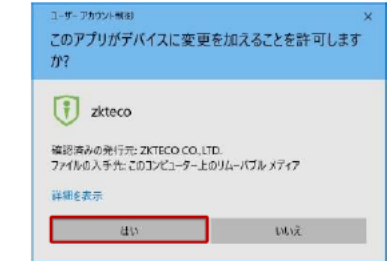
注意事項

- ✓ インストールする前に、システムにインストールされているウイルス対策ソフトを終了することをお勧めします。
- ✓ ウィルス対策ソフトが異常を検出する場合、プログラム及びフォルダの除外設定をお願いします。

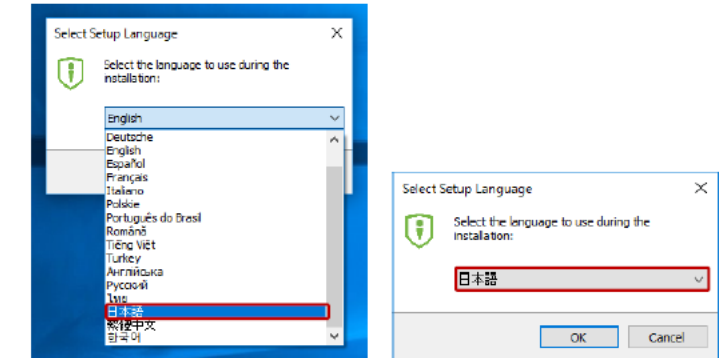
1. ダウンロードしたファイルを解凍し、フォルダ内の実行ファイル（setup.exe）をダブルクリックします。なお、ユーザーアカウント制御で「このアプリがデバイスに変更を加えることを許可しますか？」と表示される場合は「はい」をクリックします。


setup.exe

※管理ソフトのバージョンはダウンロードするタイミングで異なる場合があります。



2. セットアップおよび管理ソフトの使用言語（日本語）を選択し、「OK」をクリックします。日本語以外はサポート対象外です。



3. 管理ソフトをインストールするハードウェア環境が管理ソフトの動作に適した環境であるのかテストをします。Windows ファイアーウォールなど、ウイルス対策ソフトがインストールされている場合は「警告」が表示されます。「無視」をクリックしてインストールを進めます。何らかの「エラー」が表示された場合は、判定結果（エントリ）をクリックして案内に従ってください。



テスト項目（略称）	説明
管理ユーザー	インストールの実行アカウントが管理者権限であることを確認します。
環境変数	管理ソフトから設定する環境変数を確認します。
ソフトウェアの競合	管理ソフトと競合するソフトウェアが存在しないのか確認します。
サービスポート	管理ソフトが使用する特定のポート番号が利用できるのか確認します。
ウイルス対策ソフトウェア	ウイルス対策ソフトの有効・無効を確認します。通信許可など、管理ソフトの動作に必要な設定をします。
互換性	管理ソフトと互換性があるシステム（Windows 系 OS）であるのかを確認します。
利用可能なシステムメモリ	管理ソフトが動作するために必要なシステムメモリ容量であるのかを確認します。

連携に必要なものと役割

提供	必要な製品・ソフト	用途	準備方法
エレコム ロジテック	①顔認証デバイス	タイムレコーダー	販売店様へお問い合わせください
	②統合管理ソフトウェア*1	ユーザー・記録・端末の一元管理	ご注文後にライセンスキーのご案内
	③打刻データ連携ツール*1	打刻データを指定フォルダへ出力	
お客様	④Windowsパソコン *2	打刻データ連携ツールを動作させる	既存PC・サーバまたは新規にご購入
	⑤勤怠管理システム	勤怠管理を行うシステム	既存システムまたは新規導入
	⑥ネットワーク(VPN等) *3	製品・ソフト間で通信できる環境	情報システムの方へお問い合わせ

連携イメージ

※点線は、⑥ネットワーク（LANまたはVPN環境）



*1 お客様でご用意いただくWindowsパソコンにインストール（共存）して使用します。

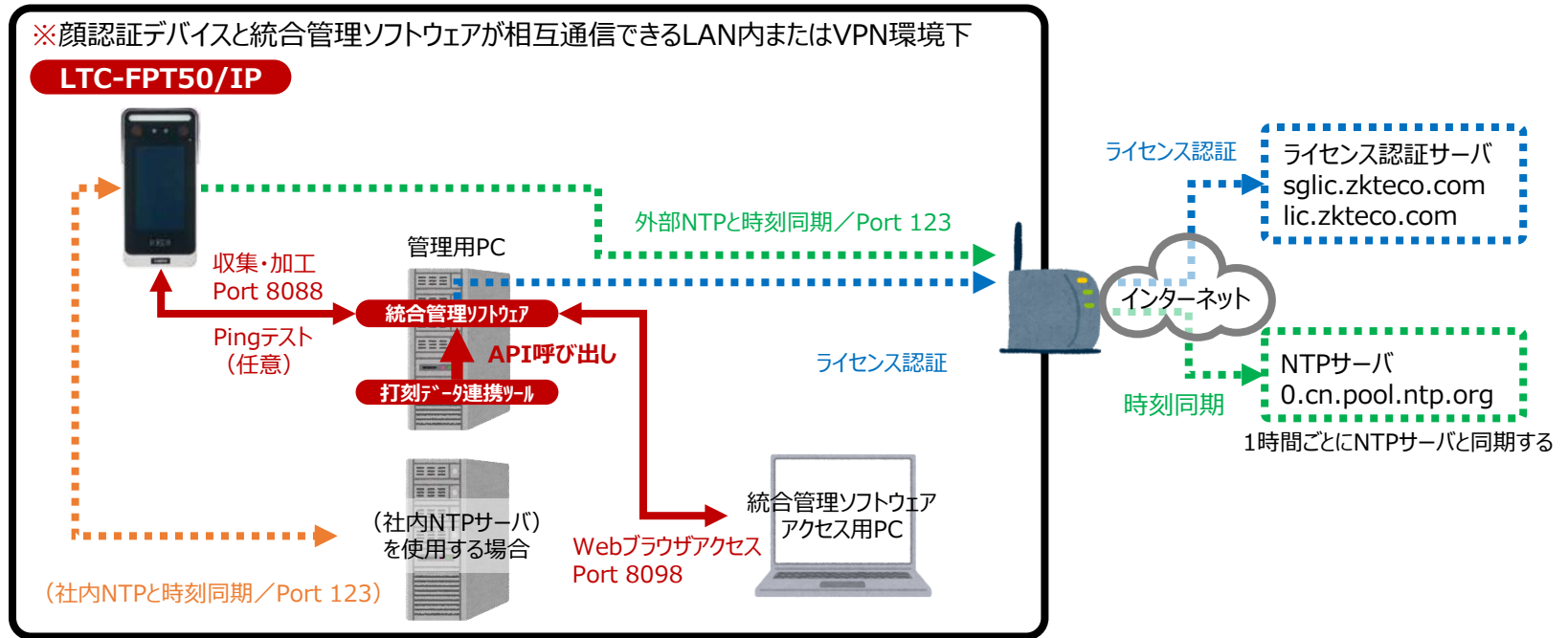
*2 OSメーカーのサポート期間が終了しておらず、各OSが動作する推奨スペックを満たしていること。

*3 複数拠点の場合、必要な製品・ソフト間で通信できるように、お客様には予めVPN環境など、ネットワークの設計・構築をお願いしております。
離れた拠点でも顔認証デバイスやデータ連携ツールがローカルIPアドレスを指定して通信できる事がが必要です。

*4 初期値は勤怠管理システムの種類により異なります。ネットワークフォルダの指定はできません。

*5 勤怠管理システムの種類により連携方法は（CSV出力／API）は異なります。

ネットワーク通信リスト



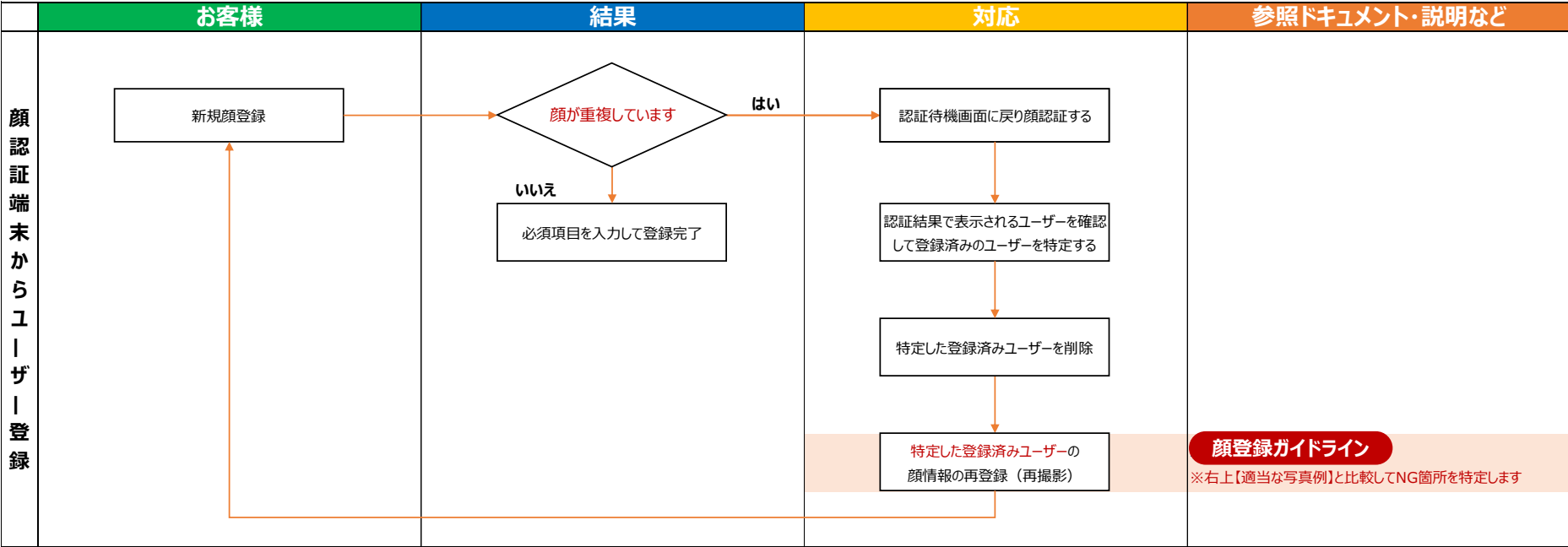
【通信許可リスト】… 外部アクセスを制限されている場合、下記の通信リストをホワイトリストへ追加してください

対象システム	宛先FQDN		プロトコル	宛先ポート	用途
統合管理ソフトウェア	外部サーバ	sglic.zkteco.com lic.zkteco.com	TCP	—	ライセンス認証
顔認証デバイス	管理用PC	—	TCP	8088 (初期値*)	統合管理ソフトウェアと端末の相互通信
	社内NTPサーバ	お客様が指定するFQDN/IPアドレス	UDP	123	時刻同期
	外部NTPサーバ	0.cn.pool.ntp.org*	UDP	123	時刻同期
	管理用PCなど	—	ICMP	—	PINGテスト
打刻データ連携ツール (管理用PC)	管理用PC	—	TCP	8098 (初期値*)	統合管理ソフトウェアAPI呼び出し・データ生成
統合管理ソフトウェア アクセス用PC	管理用PC	—	TCP	8098 (初期値*)	統合管理ソフトウェアの操作・閲覧用

*初期値で利用するFQDN/ポート番号です。お客様の環境により変更される場合、変更後の情報でホワイトリストへ追加します。

誤認証発生時の対応フロー

誤認証発生要因	他人と判別ができる量の特徴点が抽出できていません。抽出できた特徴点が少ないほど他人として判定されやすくなります。 特徴点の抽出量は、写真の撮影方法（撮影ガイドラインに則っているか否か）に依存します。
誤認証解消方法	新規登録するユーザーと、登録済みのユーザーの両方の写真を再撮影します（誤認証は顔写真の再撮影が唯一の解消方法です）。



【ご参考】
顔認証は、撮影した写真から抽出された特徴点（特徴量）を比較して本人を認証します。本人を特定するために比較する特徴が多いほど、他人との違いを判断することができます。特徴点の抽出は、[顔登録ガイドライン](#) に則り、フルHD（1920×1080）以上の解像度で撮影することで、より多くの情報を抽出することができます。

例えば、Aさんは100点の特徴が登録され、Bさんは1000点の特徴が登録されたとすると、Bさんの特徴の中にAさんの特徴が含まれる、例えば目の大きさ・位置がにている、輪郭が似ている場合があり、BさんがAさんとして誤認証されてしまいます（逆にAさんがBさんとして誤認証される場合もあります）。この場合、誤認証を回避するためにAさんも1000点の特徴が抽出できれば、目の大きさ・位置や輪郭が似ていたとしても、その他の特徴を比較することで、AさんとBさんの違いを判断することができます。このため、Aさんの写真を撮り直して再登録する必要があります。

但し、AさんもBさんも、どのくらいの特徴を抽出して登録できているのかを調べることはできないため、**誤認証が発生した場合はAさんとBさんの両方を“同じ撮影基準（＝[顔登録ガイドライン](#)）”で撮影して再登録する必要があります。**