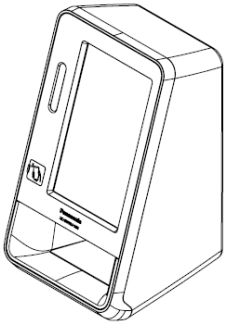
Panasonic

取扱説明書（本体編）

顔認証付きカードリーダー

品番　XC-STFR3J-MN



この冊子は
「本体編」
です。

この冊子は、「本体編」です。
先に付属の「取扱説明書　準備編」をご覧いただき、
本機の準備を実施してください。

・アプリケーションソフトのインストール
・お手入れ
など

このたびは、パナソニック製品をお買い上げいただき、まことにありがとうございます。

- 取扱説明書をよくお読みのうえ、正しく安全にお使いください。
- イラストや機能、画面、仕様など本書の内容に関して、将来予告なしに変更することがあります。

Published in Japan

A0626-1076

目次

1 本体と付属品の確認 4

2 各部の名称と働き 5

2.1 正面側の名称と働き 5
2.2 背面側の名称と働き 6
2.3 底面側の名称と働き 8

3 本機のセットアップ 9

3.1 初期アカウント 10
3.2 画面設定(拡大縮小) 13
3.3 アプリケーションソフトのインストール 15
3.3.1 アプリケーションソフトのインストール 15
3.3.2 アプリケーションソフトの手動起動方法について 18
3.3.3 管理者用 PIN コードの設定について 18
3.4 バックアップ手順 19
3.4.1 バックアップを取得するデバイスの準備 19
3.4.2 バックアップの作成 20
3.5 リカバリー手順 23
3.5.1 リカバリーデータの準備 23
3.5.2 リカバリー環境(回復環境)の起動 23
3.6 アプリケーションのアンインストール方法(参考) 27
3.7 機関認証情報設定ツールについて 29
3.8 自己診断ツール 30
3.9 モニタレス運用時の自動ログイン設定 34
3.10 顔認証付きカードリーダー専用物理テンキーの利用について 36

4 管理画面について 37

4.1 管理画面の表示項目について 37
4.2 モード(運転モード) 39
4.3 状態 39
4.4 メッセージ 40
4.5 画面メッセージ編集ツール 40
4.6 端末再起動 42
4.7 最小化 42
4.8 設定 43
4.8.1 音量 44
4.8.2 画面輝度 44
4.8.3 テンキーの配置 45
4.8.4 管理者用 PIN コード 45
4.8.5 患者画面サマリー表示 46
4.8.6 障害時の自動復旧(再起動) 47
4.9 端末電源オフ 47

4.10 アプリ終了 48
4.11 端末画面での管理画面表示 48

5 OS 設定について（出荷時設定済） 50

5.1 電源プラン及び電源ボタンの定義 50
5.2 電源オフ・スリープ設定 53
5.3 USB 省電力設定 55
5.4 ランタイムソフトのインストール 57
5.5 仮想ディスプレイドライバー 57
5.6 ディスプレイのグループポリシー設定 58
5.7 システム復元の有効化 62

6 ご使用にあたっての注意事項 64

6.1 USB ポートの電流制限 64
6.2 情報漏洩リスク 65
6.2.1 ネットワーク接続の情報漏洩リスク 65
6.2.2 ユーザー認証に関する情報漏洩リスク 65
6.3 FAN の回転数について 66
6.4 ユーザー切替について 66
6.5 カード置台の取り扱いについて 67
6.6 ソフトウェアライセンス情報について 67

7 故障かな ！？ 68

付録 A リモートアクセスの導入（UltraVNC） 70

A-1 リモートアクセスの導入（UltraVNC） 72
A-1.1 顔認証付きカードリーダー側のインストール手順 73
A-1.2 顔認証付きカードリーダー側の設定 77
A-1.3 医療システム側への UltraVNC 導入 79
A-2 リモートアクセス例 83
A-2.1 リモートアクセス手順 84

1 本体と付属品の確認

お買い上げいただいたパッケージには、以下のものが同梱されています。ご使用前に内容をご確認ください。

万一、同梱品に不足がある場合は、お買い上げの販売店、またはご相談窓口までご連絡ください。

●本体 1 台
（のぞき見防止フィルター付き）



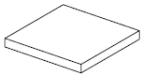
●ACアダプター 1 個



●電源コード 1 本



●転倒防止パッド 4 個



●六角レンチ 1 本
（二面幅 3 mm 背面カバー用）



●取扱説明書 準備編 1 冊

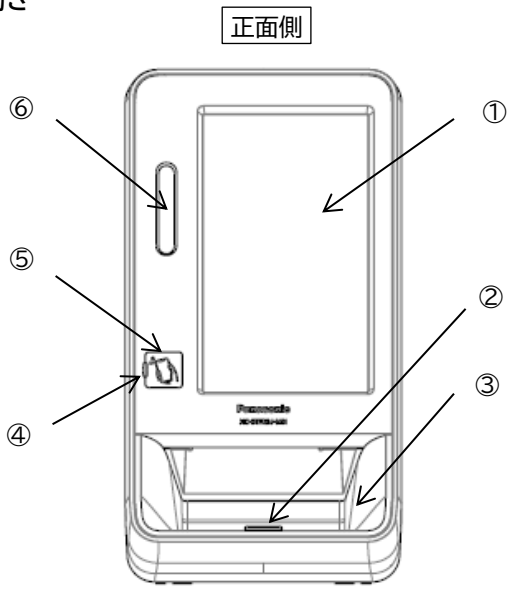


※製品のイラストは、実物と異なる場合があります。

2 各部の名称と働き

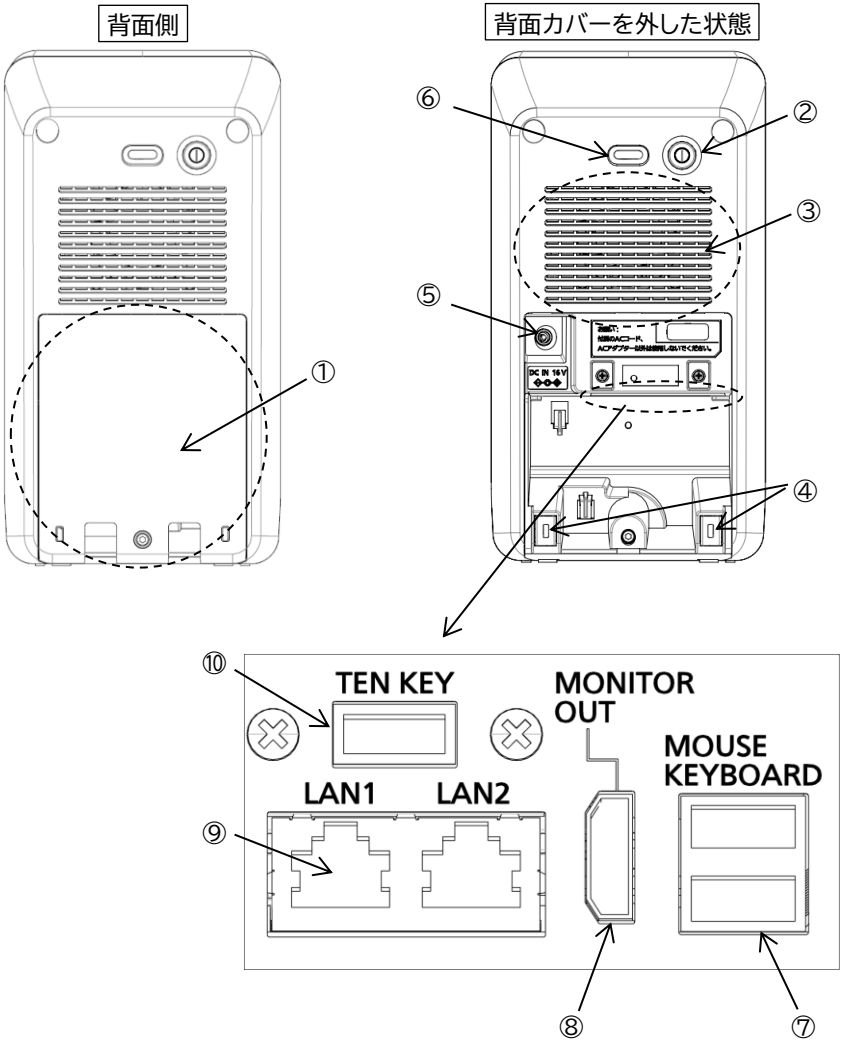
各部の名称と働きを説明します。

2.1 正面側の名称と働き



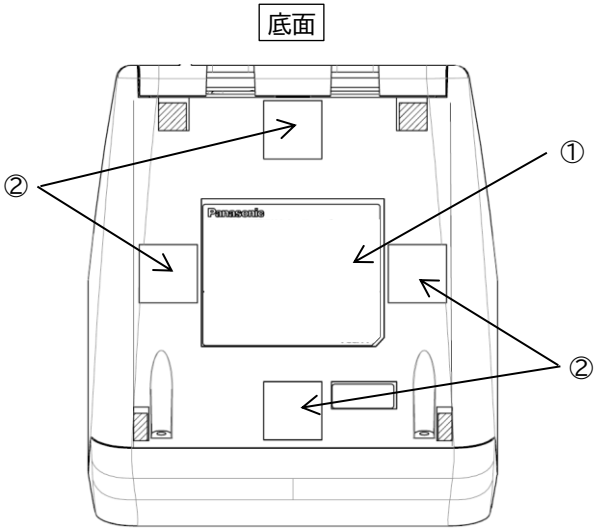
番号	名称	働き
①	タッチパネル付きディスプレイ （のぞき見防止フィルター付き）	画面表示と各操作
②	スピーカー	音声の出力
③	カード置台	マイナンバーカードの読み取り台
④	前面インジケーター	スマートフォンの読み取り時に点灯
⑤	スマホ読取部	スマートフォンの読み取り箇所
⑥	顔認証カメラ	顔認証時の撮影カメラ

2.2 背面側の名称と働き



番号	名称	働き
①	背面カバー	外部接続ポートのカバー
②	電源スイッチ	端末の起動／終了
③	通風孔	内部の熱の排出
④	セキュリティスロット	市販の盗難防止用ワイヤーの取り付けスロット （スロットサイズ：約 3×7 mm）
⑤	DC IN端子	付属ACアダプターの電源コード接続口
⑥	背面インジケーター	端末の状態表示ランプ
⑦	キーボード／マウス ポート	キーボード、マウス用 USBポート
⑧	モニター ポート	HDMI ポート
⑨	LAN ポート	有線 LAN（Ethernet）ポート
⑩	テンキー ポート	顔認証付きカードリーダー専用物理テンキー用 （別売品）USB ポート

2.3 底面側の名称と働き



番号	名称	働き
①	主銘板	端末情報の表示
②	転倒防止パッド貼付け部	付属品の転倒防止パッド貼付け位置（4 か所）

3 本機のセットアップ

本機を動作させるために必要な顔認証付きカードリーダーアプリケーションソフト(以下、アプリケーションソフト)をセットアップする手順について説明します。

【事前準備】

① 医療機関等向け総合ポータルサイトに掲載の「医療機関等向け 資格確認端末のセットアップ手順書 資格確認端末編【Windows11】」に従い、〔操作2～操作9〕までの手順を完了してください。(操作1については、3.1 初期アカウントを参照ください。)
② 顔認証付きカードリーダー 取扱説明書 準備編に従い、機器接続をおこなってください。
③ マイナンバーカードをご準備ください。
④ ソフトウェアのライセンス及び使用許諾を事前に確認ください(こちら)。

【セットアップ手順】

セットアップは、以下の手順でおこないます。

① 管理者アカウント(OqsComApp)のパスワード設定
② 画面設定
③ アプリケーションソフトのインストール
④ 顔認証用アカウント(デバイス ID)の登録、管理者PINコードの設定
⑤ 動作確認
⑥ イメージバックアップの取得

3.1 初期アカウント

出荷時には管理者アカウント(OqsComApp)があらかじめ設定されています。
セキュリティ確保のため、以下に示す手順によりパスワードを速やかに設定してください。

「医療機関等向け 資格確認端末のセットアップ手順書　資格確認端末編
【Windows11】」の〔操作1〕を参照してください。

出荷状態のユーザー名と初期パスワード
- ・ユーザー名:　　OqsComApp
- ・パスワード:　　なし

【パスワード変更手順】
※必須手順のため、**必ず実施**してください。

① Windows キーを押して「設定」をクリックします。



② 「アカウント」→「サインインオプション」→「パスワード」の順にクリックし、最後に「追加」をクリックします。





③ 「パスワードの生成」のウィンドウが立ち上がりますので、そこでパスワードを設定し、「次へ」をクリックします。

（このパスワードは、忘れると端末にログインできなくなりますので、ご注意ください。）



④ 「完了」をクリックして設定完了します。



3.2 画面設定(拡大縮小)

本機のディスプレイ表示を正しくおこなうため、表示サイズを 100 %に設定します。「医療機関等向け 資格確認端末のセットアップ手順書　資格確認端末編【Windows11】〔操作3〕 ディスプレイ設定の変更」で、すでに実施済の場合は実施する必要はありません。

① Windows キーを押して「設定」をクリックします。



② 「システム」→「ディスプレイ」を選択します。



③ 「拡大縮小とレイアウト」で「拡大/縮小」を 100 % に設定します。



④ ウィンドウを閉じて設定完了します。

◎ポイント◎
・表示サイズが 100 %以外に設定されていると、画面レイアウトが崩れてアプリケーションが正常に表示されない場合があります。

3.3 アプリケーションソフトのインストール

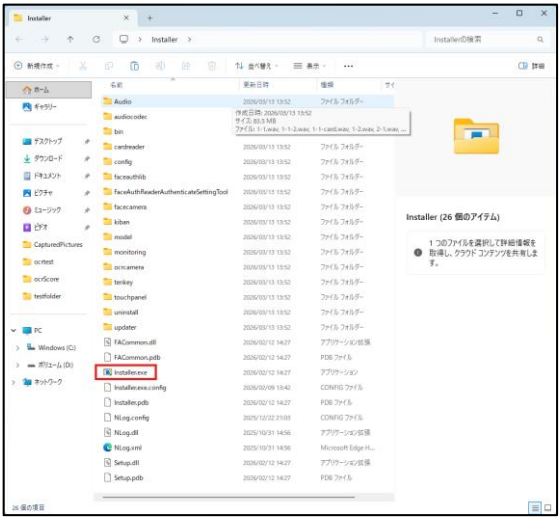
アプリケーションソフトのインストールについて説明します。

3.3.1 アプリケーションソフトのインストール

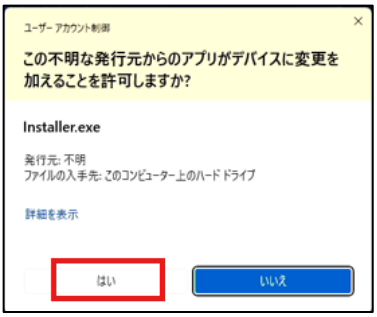
① デスクトップ上にある「Installer」をダブルクリックしてフォルダを開きます。



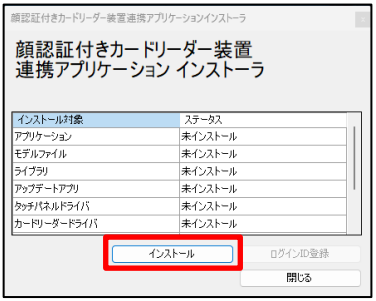
② 「Installer.exe」をダブルクリックするとインストーラーが起動します。

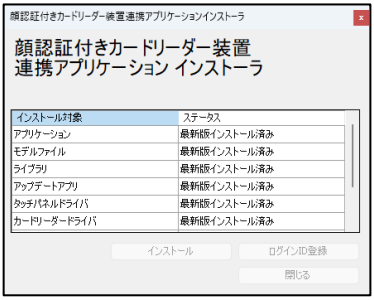


③　ユーザーアカウント制御のポップアップが表示された場合は、「はい」をクリックします。



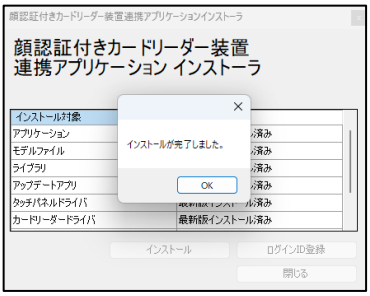
④　インストーラーが起動しますので、「インストール」をクリックします。





※インストールにはしばらく時間がかかります。完了するまでそのままお待ちください。

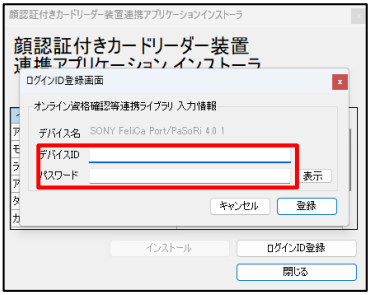
⑤ インストール完了を確認します。



完了したら「OK」をクリックします。

⑥ 顔認証用アカウント（デバイス ID）の登録画面が表示されるまで、しばらくそのままで待ちます（接続機器を認識するまで約 1 分程度かかります）。

デバイス ID とは、「医療機関等向け資格確認端末のセットアップ手順書（資格端末編）【Windows11】」に従って作成した顔認証用アカウントを指します。最新版の「医療機関等向け資格確認端末のセットアップ手順書（資格端末編）【Windows11】」は、医療機関等向け総合ポータルサイトから入手できます。



⑦ 顔認証用アカウント（デバイス ID）の登録画面が表示されましたら、デバイス名とパスワードを入力して、「登録」をクリックします。その後、再起動を促すポップアップが表示されるので端末を再起動してください。無操作の場合 1～2 分後に再起動します。



3.3.2 アプリケーションソフトの手動起動方法について

※アプリケーションソフトは OS 起動時に自動で起動されますので、通常はデスクトップ画面上からのアプリケーションソフト手動起動操作は不要です。

顔認証付きカードリーダーのアプリケーションを手動で起動するには、デスクトップに生成されている顔認証付きカードリーダーアプリケーションのアイコンをダブルクリックします。認証情報設定ツール、SelfDiagnosis(自己診断ツール)のアイコンについては、それぞれの項目についてのページを参照ください。



3.3.3 管理者用 PIN コードの設定について

顔認証付きカードリーダーのタッチパネル付きディスプレイにおいて、アプリケーションの管理画面を表示することができます。管理画面の表示には、管理者用の PIN コードが必須となりますので、以下の項目を参照の上、設定してください。

4.8.4 管理者用 PIN コード
4.11 端末画面での管理画面表示

※後述するバックアップをおこなう前に必ず設定ください。

3.4 バックアップ手順

顔認証付きカードリーダーのセットアップ完了後、オンライン資格確認の一連の動作が正常におこなえることを確認したうえで、システムのバックアップを必ず取得してください。

【手順】
① バックアップを取得するデバイスの準備
② バックアップの作成

※バックアップは、ネットワークや電子証明書などの各種設定完了後、実際にオンライン資格確認がおこなえることを確認したうえで実施してください。

3.4.1 バックアップを取得するデバイスの準備

外部記憶装置にバックアップする場合(推奨):
別途 USB で接続できる SSD(ソリッドステートドライブ)か HDD(ハードディスクドライブ)を用意し、顔認証付きカードリーダー背面にあるキーボード／マウス ポートあるいはテンキーポートに接続します。

内蔵記憶装置にバックアップする場合:
外部記憶装置が準備できない場合は、顔認証付きカードリーダーのDドライブにバックアップ領域を確保していますので、D ドライブに必ずバックアップを取得してください。バックアップにあたっては、Dドライブに他のデータが入っていないか確認してください。もし、他のデータがある場合は(過去のバックアップデータを含む)、削除するか必要に応じてデータを退避してください。

※Dドライブに保存した場合、本体のSSD自体が故障した場合は復元できません。そのため外部記憶装置にバックアップしていただくことを強く推奨します。

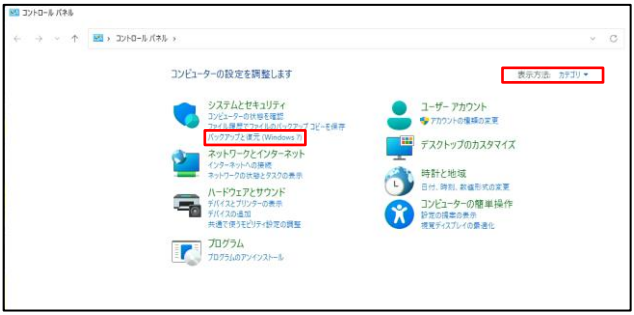
3.4.2 バックアップの作成

以下の手順に従ってバックアップを取得します。

① Windows キー ＋ R を押し、「ファイル名を指定して実行」を開きます。
② control と入力し、「OK」をクリックし、コントロールパネルを開きます。



③ コントロールパネルが表示されますので、表示方法を「カテゴリ」に変更し、「バックアップと復元(Windows 7)」をクリックします。



④ 「システムイメージの作成」をクリックします。



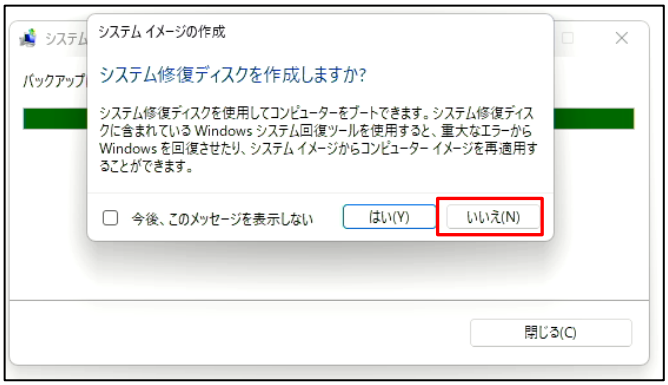
⑤　バックアップ先を指定して、「次へ」をクリックします。
（画像では、Dドライブにバックアップする例で説明します）



⑥　バックアップする対象を確認の上、「バックアップの開始(S)」をクリックします。

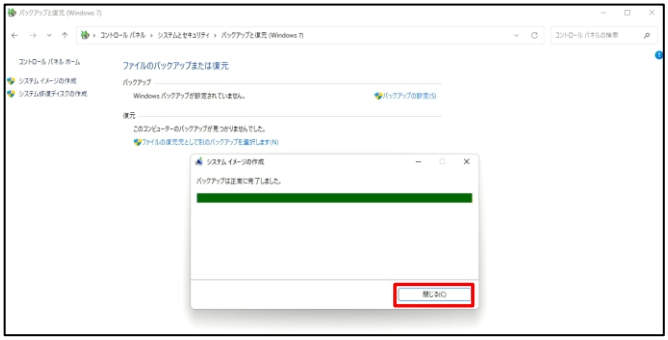


⑦ 「システム修復ディスクを作成しますか？」のポップアップが表示されるので、ディスクを作成しない場合は「いいえ」をクリックします。



※　システム修正ディスクは、作成することも可能です。

⑧ バックアップが終了したら「閉じる」をクリックし、バックアップ先に「WindowsImageBackup」のフォルダが作成されていることを確認してください。



バックアップ取得に関するお願いおよび免責事項

本機器に内蔵される Windows PC に保存されているデータおよびシステム環境につきましては、障害発生時に備え、お客様ご自身の責任において、定期的にバックアップを取得し、適切に保管・管理していただきますようお願いいたします。

なお、バックアップの取得状況の如何にかかわらず、本機器の使用または故障、障害、修理作業その他の事由により発生したデータの破損、消失、またはシステム環境の損失につきまして、当社は一切の責任を負いかねます。

3.5 リカバリー手順

本手順は、「3.4 バックアップ手順」でバックアップ(WindowsImageBackup)を取得している場合 に実施できます。

【手順】

① リカバリーデータの準備

② リカバリー環境(回復環境)の起動

3.5.1 リカバリーデータの準備

外部記憶装置からリカバリーする場合:

バックアップデータが保存されている SSD(ソリッドステートドライブ)か HDD(ハードディスクドライブ)を顔認証付きカードリーダー背面にあるキーボード／マウス ポートあるいはテンキーポートに接続します。

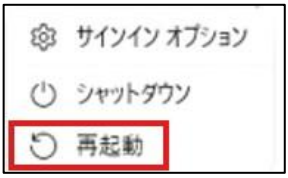
内蔵記憶装置からリカバリーする場合:

顔認証付きカードリーダーのDドライブからリカバリーをおこないますので、Dドライブに「WindowsImageBackup」というフォルダが存在することを確認してください。

3.5.2 リカバリー環境(回復環境)の起動

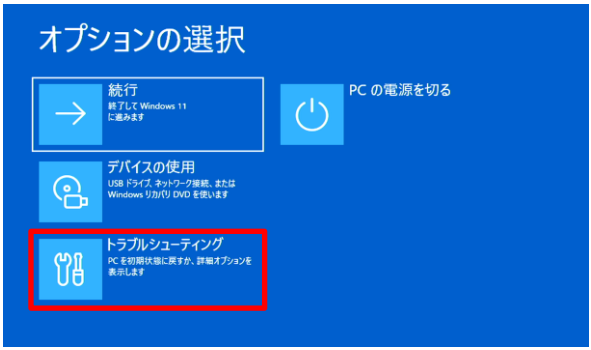
リカバリー環境は、シフトキーを押しながら再起動をおこなうことで起動します。

【Shift キー＋再起動】



【リカバリー処理】

① 再起動すると、オプション選択画面が起動しますので、「トラブルシューティング」をクリックします。



② 「詳細オプション」をクリックします。



③ 詳細オプション画面において「その他の修復オプションを表示」をクリックします。



④　詳細オプション画面において「イメージでシステムを回復」をクリックします。



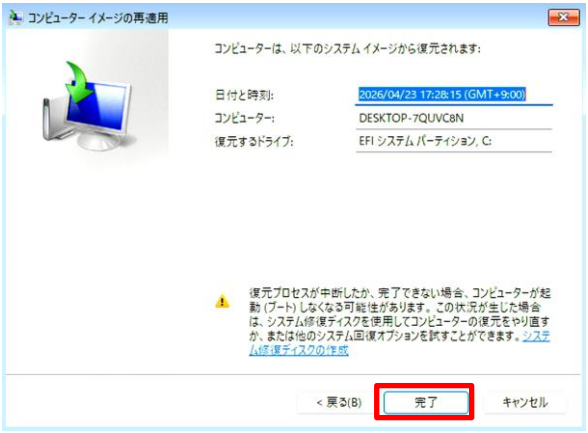
⑤　リカバリーデータ内容を確認し、「次へ(N)」をクリックします。



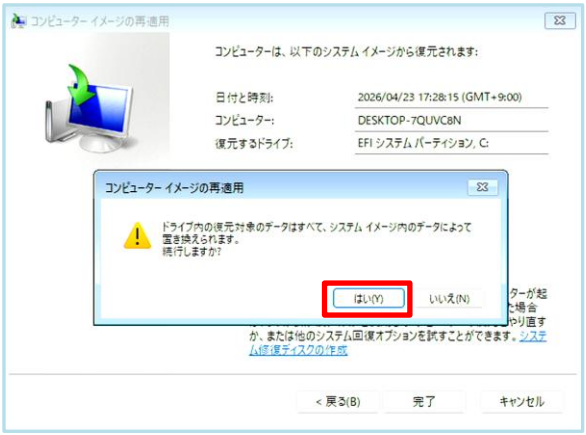
⑥　「次へ(N)」をクリックします。



⑦ 「完了」をクリックします。



⑧ 「はい」をクリックしてリカバリー処理を開始します。



リカバリー処理が開始されます。

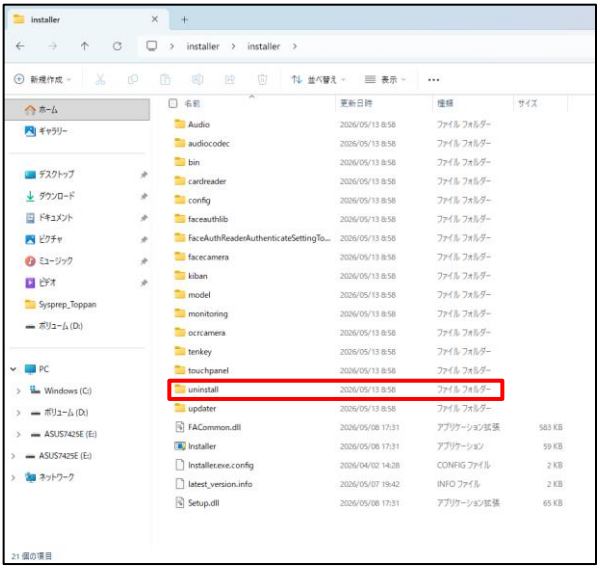


⑨ 完了すると自動で再起動して完了となります。

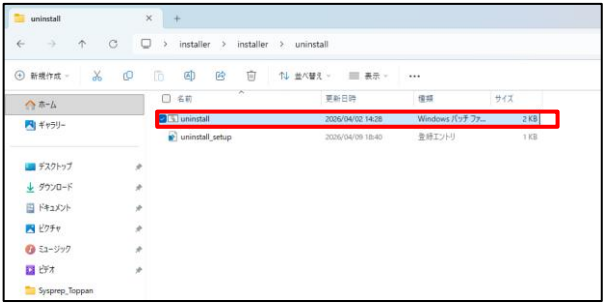
3.6 アプリケーションのアンインストール方法(参考)

① デスクトップ上にある「Installer」をダブルクリックしてフォルダを開きます。

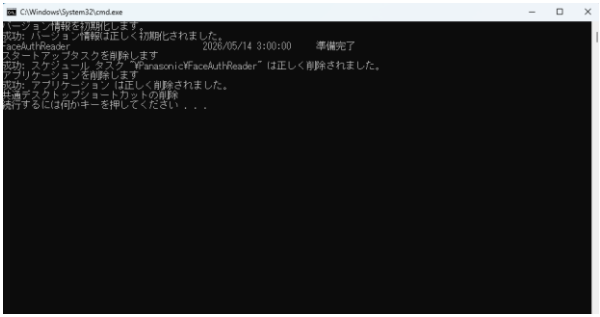
② 「uninstall」フォルダを開きます。



③ 「uninstall」フォルダにある「uninstall.bat」をクリックして実行します。



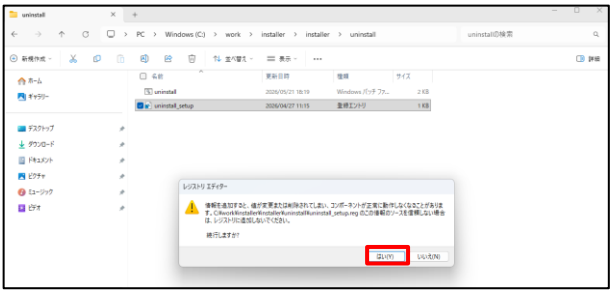
④　コマンド実行画面が表示され、終了メッセージが表示されます。



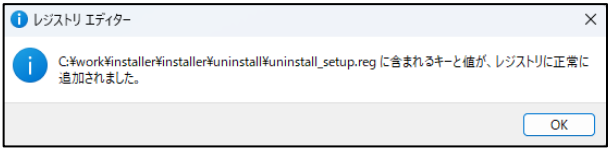
⑤　「uninstall」フォルダにある「uninstall_setup」をクリックして実行します。



⑥　警告画面がでますが、「はい(Y)」を選択してください。



以下の画面が表示されたら完了となります。



3.7 機関認証情報設定ツールについて

機関認証情報設定ツールは、以下の場合に使用します。

・機関認証用電子証明書の入れ替えをおこなう場合
・顔認証用アカウント(デバイス ID)のパスワード変更をおこなった場合
・新規に顔認証用アカウント(デバイス ID)を登録する場合

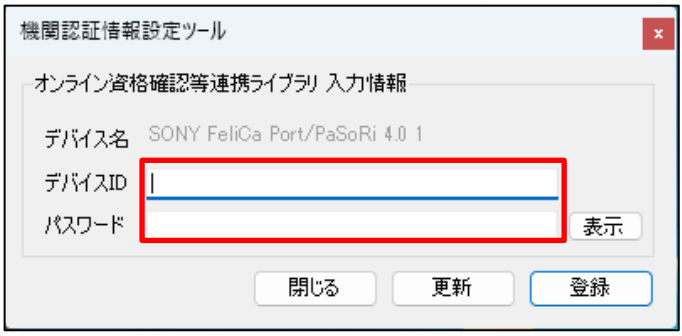
【起動方法】

① 最初に、顔認証付きカードリーダーのアプリケーションソフトを終了してください。

② 次にデスクトップに生成されている機関認証情報設定ツールのショートカットをダブルクリックします。**なお、起動には30秒ほど要しますので、そのまましばらくお待ちください。**



機関認証情報設定ツールが起動すると以下のような入力画面が立ち上がります。デバイス名には「SONY Felica ・・」と表示されます。「医療機関等向け 資格確認端末のセットアップ手順書 資格確認端末編【Windows11】」(*1) にて作成した顔認証用アカウント(デバイス ID)とパスワードを設定します。



新規に登録をおこなう場合は、「登録」ボタンを、更新をおこなう場合は、「更新」ボタンを押します。

(*1)
最新の「医療機関等向け 資格確認端末のセットアップ手順書 資格確認端末編【Windows11】」は、医療機関等向け総合ポータルサイトから入手可能です。

③ 「登録／更新に成功しました。」というメッセージが表示されると完了です。



3.8 自己診断ツール

本製品には、動作状態をお客様ご自身で確認できる「自己診断ツール」が搭載されています。本ツールでは、機器の動作を実際にご確認いただきながら、画面の案内に従って診断をおこなうことができます。
以下の手順に従って、セットアップを行ってください。

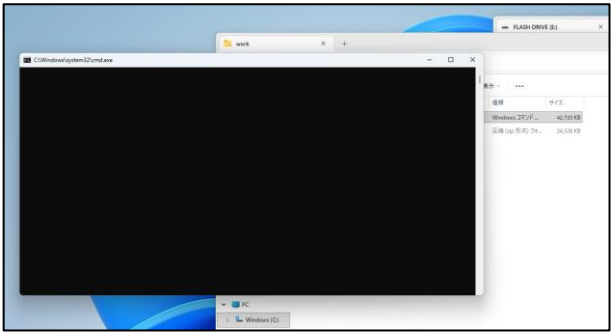
【初期セットアップ方法】

① 以下のフォルダにある SelfDiagnosis_Vx.x.xをダブルクリックします。

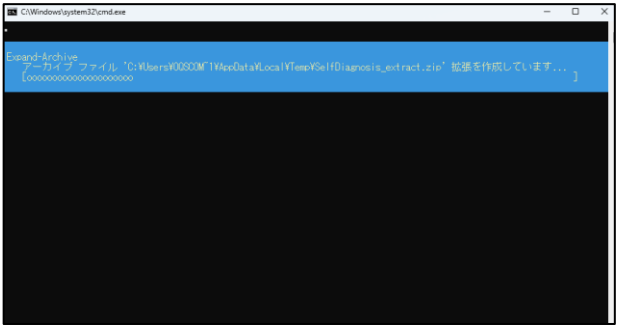
C:¥work¥SelfDiagnosis_V x.x.x　　X.X.X はバージョン情報



② cmd プロンプトが立ち上がりますので、しばらくそのままで待ちます。



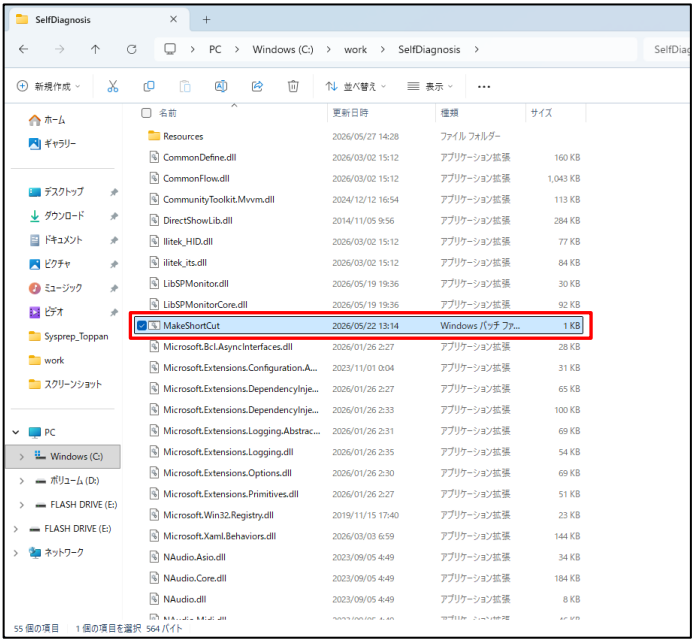
しばらくするとプログラムが展開され、フォルダが生成されます。



③ 生成された SelfDiagnosis フォルダを確認し、フォルダの中を確認します。



④ フォルダの中にある「MakeShortCut」をクリックします。すると、デスクトップ上にプログラムのショートカットが作成されます。



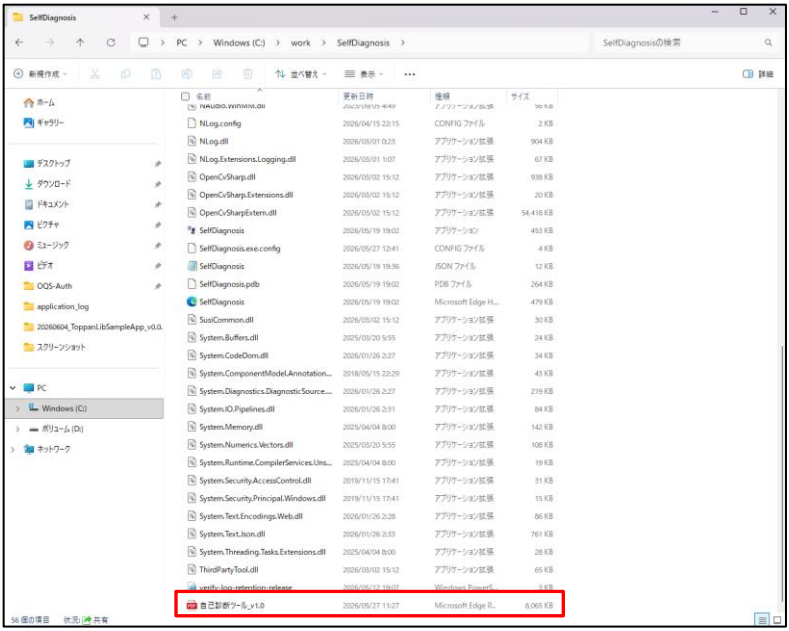
⑤ ショートカットアイコンの確認

デスクトップ上に以下のショートカットが作成されたことを確認します。
本ショットカットをクリックすると自己診断ツールが起動します。



⑥　自己診断ツール　操作手順は、以下に資料がございますので、ご参照ください。

C:¥work¥SelfDiagnosis¥自己診断ツール_Vx.x.pdf　X.X はバージョン情報



3.9 モニタレス運用時の自動ログイン設定

本製品は、初期設定後、リモートアクセスでの運用などを想定し、外部モニターやキーボード、マウスなどを接続しない「モニタレス運用」が可能です。

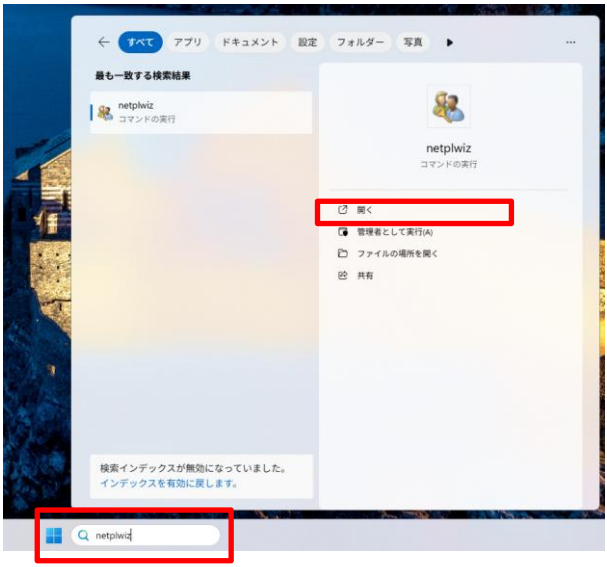
注意：障害発生時や管理画面での各種設定をおこなう際には、外部モニター、キーボード、およびマウスの接続が必要です。

モニタレス運用時には、Windows OS への自動ログインの設定をおこなう必要があります。以下の手順に従って設定をしてください。

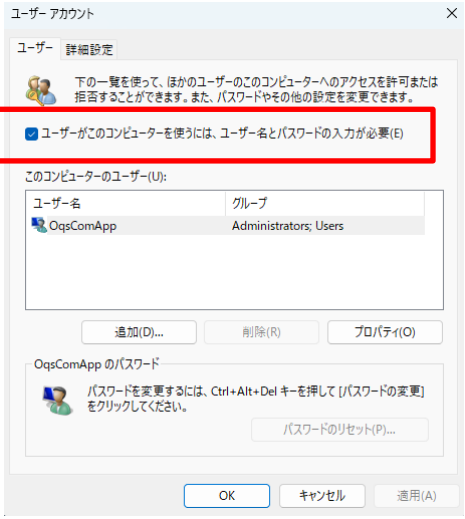
【Windows OS への自動ログインの設定方法】

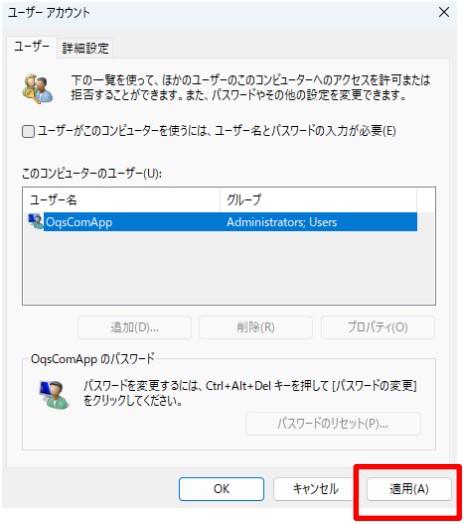
① netplwiz の起動

検索ボックスに「netplwiz」と入力し、「開く」をクリックします。

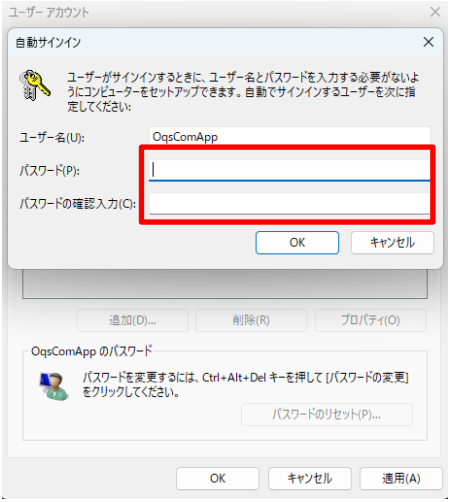


② 「ユーザー名とパスワード入力が必要」のチェックを外し、「適用」をクリックします。





③ 「自動サインイン」のウィンドウが開いたら、自動ログインする Windows のアカウントパスワードを入力し、「OK」をクリックします。



④ WindowsOS を再起動し、自動でログインすることを確認します。

3.10 顔認証付きカードリーダー専用物理テンキーの利用について

別売品の顔認証付きカードリーダー専用物理テンキー(以降 テンキー)を利用する場合は、以下の手順でおこないます。

① 専用テンキーポートにテンキーを接続します。
(取扱説明書(準備編) 4章をご参照ください。)
② アプリケーションソフトを起動します。

注意:
・テンキーポートに接続ください。
・アプリケーション起動前に接続しておく必要があります。アプリケーション動作中に抜き差しすると正しく認識されません。
・テンキー接続中は、音声案内開始時にテンキー接続の案内がアナウンスされます。

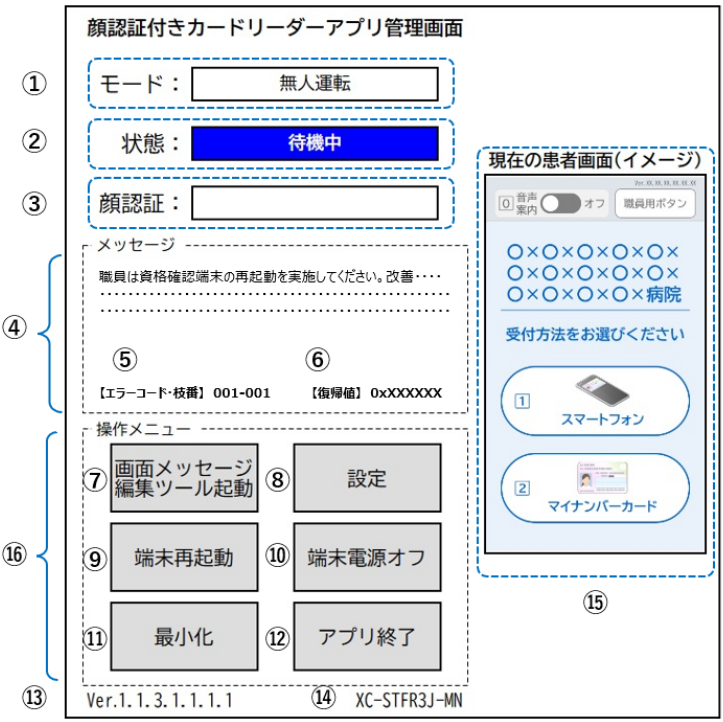
4 管理画面について

本章では、アプリケーションソフトを起動した際に表示される管理画面の構成と各機能について説明します。

管理画面では、端末の状態確認、運転モードの確認、エラー内容の確認、操作メニューの選択をおこなえます。

4.1 管理画面の表示項目について

アプリケーションソフトを起動した際に表示される管理画面（患者画面サマリー表示有の場合）を示します。



番号	項目	説明
①	モード	現在の運転モードを表示します
②	状態	アプリケーションおよび端末の動作状態を表示します
③	顔認証結果	顔認証の判定結果を表示します
④	メッセージ	障害発生時や注意が必要な場合にメッセージを表示します ※別の表示事象が発生するまでメッセージは残ります
⑤	エラーコード・枝番	発生したエラーの番号を表示します
⑥	復帰値	エラー発生時などにおける復帰情報を表示します
⑦	画面メッセージ編集ツール起動	画面メッセージ編集ツールを起動します
⑧	設定	音量・画面設定・テンキー設定などをおこなうための各種設定画面を開きます
⑨	端末再起動	端末を再起動する画面を表示します ※状態が「待機中」の時のみ使用できます
⑩	端末電源オフ	端末の電源をオフにします ※状態が「待機中」の時のみ使用できます
⑪	最小化	管理画面を最小化します
⑫	アプリ終了	アプリケーションソフトを終了します ※状態が「待機中」のときのみ使用できます
⑬	バージョン	アプリケーションソフトのバージョンを表示します
⑭	端末名	端末の品番を表示します
⑮	表示イメージ	患者向け画面のプレビューを表示します ※初期状態では表示されません(→患者画面サマリー表示)
⑯	操作メニュー	管理画面から行える操作メニューを表示します

4.2 モード（運転モード）

モードの項目では端末の動作モードを表示します。

運転モード	説明
無人運転	顔認証／パスワード認証、スマホ（iPhone/Android）による資格確認モード
PIN 認証固定	顔認証を行わず、パスワード認証、スマホ（iPhone/Android）による資格確認モード
目視確認	本人確認を対面でおこない、カード読み取りのみの資格確認モード

4.3 状態

状態の項目ではアプリケーションの動作状態を表示します。動作状態は以下の通りです。

状態	説明
起動中	アプリケーション起動中であることを示します
待機中	アプリケーションが待機中であることを示します
使用中	資格確認をおこなっていることを示します
終了中	アプリケーションが終了処理をおこなっている状態を示します
顔認証不可	顔認証による本人認証ができない状態です ※運転モードを切り替えることで運用継続が可能な場合があります
システムエラー	運用できないエラーが発生している状態です ※支払基金提供の「トラブルシューティング編」に従い対処してください

4.4 メッセージ

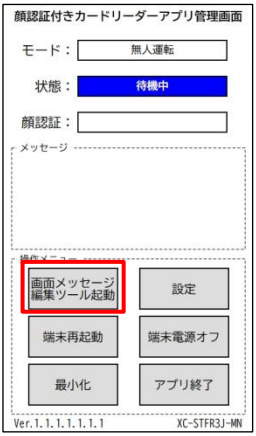
メッセージには、運用中に発生したエラー内容や注意メッセージが表示されます。下部にはエラーコードや復帰値なども表示されますので、エラーが発生した場合には、これらの情報を確認するようにしてください。

◎エラーコード表示例◎
患者はマイナンバーカードが正しく置かれているか確認してください。再度同様のエラーが表示される場合は、受付窓口に連絡してください。
【001:マイナンバーカードの認識不可】

4.5 画面メッセージ編集ツール

画面メッセージ編集ツールでは、端末の各種画面に表示される施設名や案内メッセージを編集できます。

① 「画面メッセージ編集ツール起動」をクリックします。



② 編集したい更新対象にチェックを入れてください。
（下部のスクロールバーを動かし、字数制限などの隠れている項目も参照ください）



③ メッセージを編集後、「登録」をクリックしてください。



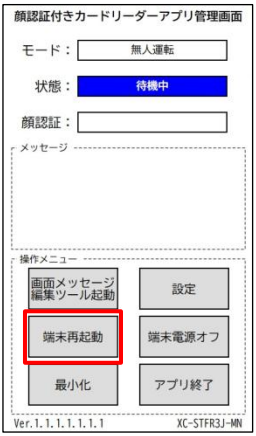
④ 登録が完了したら、右上の「×」ボタンをクリックすると「終了確認」画面が表示されますので、「端末再起動」をクリックしてください。





4.6 端末再起動

管理画面から端末を再起動する場合に使用します。クリックすると再起動の確認画面が表示されますので、「はい」を選択してください。



4.7 最小化

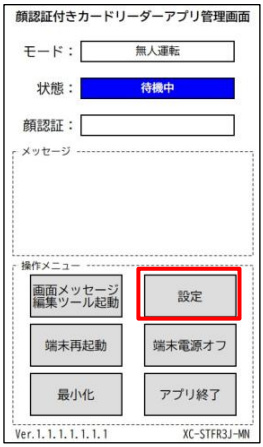
管理画面を最小化表示する場合に使用します。最小化すると、画面上の表示は非表示となり、タスクバーに格納されます。



4.8 設定

設定では、音量・画面輝度・テンキー設定など、各種設定を変更できます。

① 管理画面の操作メニューより「設定」をクリックします。

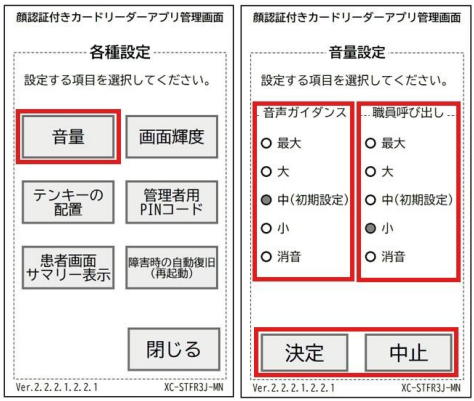


② 各種設定が表示されますので、設定したい項目を選択してクリックしてください。



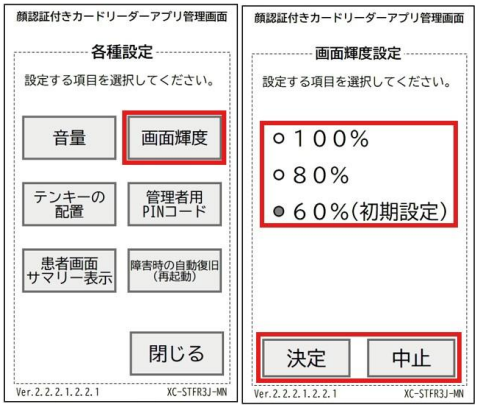
4.8.1 音量

「音量」設定では、「音声ガイダンス」と「職員呼び出し」の音量が変更できます。「音声ガイダンス」は音声案内をおこなう際の音量で、「職員呼び出し」は職員を呼び出す際の音量になります。音量設定画面にて、音量を選択し「決定」ボタンをクリックします。



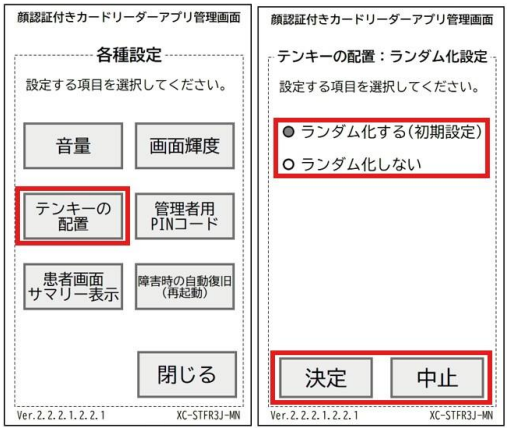
4.8.2 画面輝度

「画面輝度」設定では、端末画面のバックライト輝度の調整をおこなうことができます。画面輝度設定画面にて、設定する輝度を選択し、「決定」ボタンをクリックします。



4.8.3 テンキーの配置

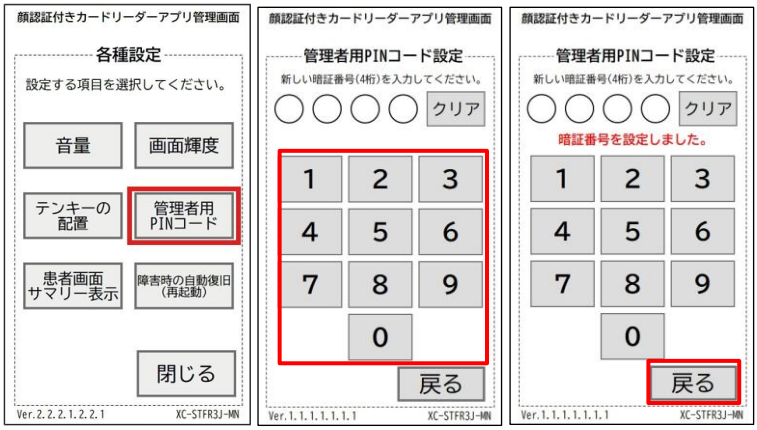
「テンキーの配置」では、PIN 入力画面で使用するテンキーの配置をランダム化するか、しないかを選択ができます。いずれかを選択し、「決定」ボタンをクリックします。



4.8.4 管理者用 PIN コード

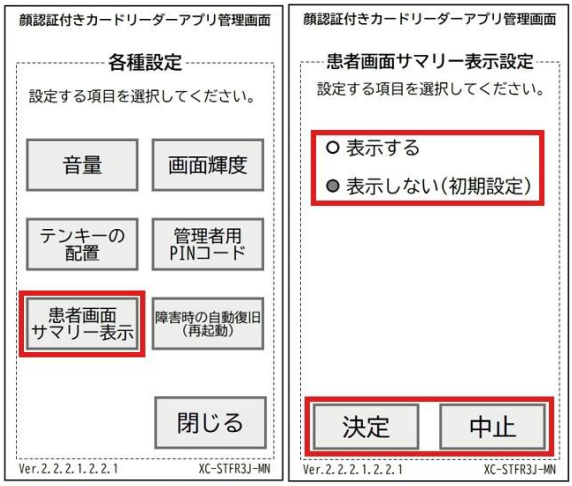
「管理者用 PIN コード」では、顔認証付きカードリーダー本体の画面から管理画面を開く際の PIN コードを設定します。設定する PIN コードを入力してください。「暗証番号を設定しました」というメッセージが表示されたら、「戻る」ボタンをクリックします。

※管理者用 PIN コードは必ず設定してください。（初期値　0000）

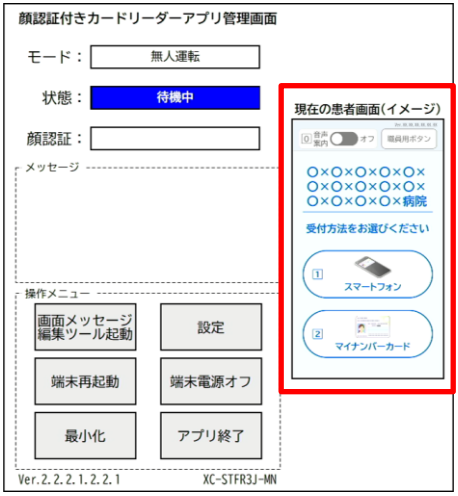


4.8.5 患者画面サマリー表示

端末に表示されている患者向け画面(待機画面・読取中画面など)のサマリー表示を管理画面に表示するかどうかを設定します。いずれかを選択し、「決定」ボタンをクリックします。

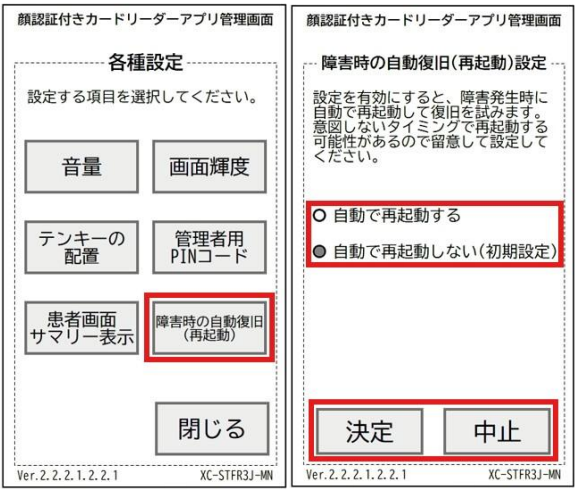


本設定を実施すると、管理画面に「患者画面サマリー表示」が表示されるようになります。
※プライバシーに配慮し、実際の表示画面でなくイメージ画像を表示します。



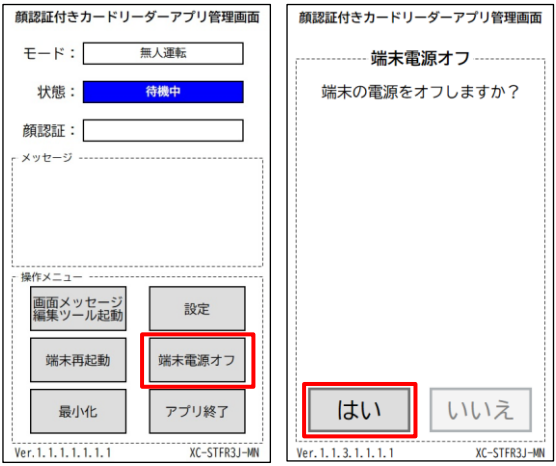
4.8.6 障害時の自動復旧(再起動)

本アプリケーションでは、アプリケーションや端末異常が発生した際に、自動で端末を再起動して復旧を試みる機能が実装されています。ここでは本機能の有効／無効を設定します。いずれかを選択し、「決定」ボタンをクリックします。



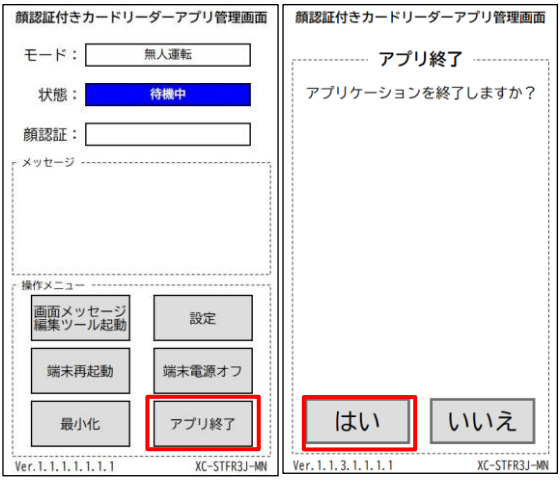
4.9 端末電源オフ

管理画面から端末の電源をオフする場合に使用します。クリックすると確認画面が表示されます。端末電源をオフする場合は、「はい」を選択します。



4.10 アプリ終了

管理画面からアプリケーションのみを終了する場合に使用します。クリックすると確認画面が表示されます。アプリケーションを終了する場合は、「はい」を選択します。



4.11 端末画面での管理画面表示

顔認証付きカードリーダー本体のタッチパネル付きディスプレイにおいて、以下のように管理画面を表示することが可能です。



【端末から管理画面へアクセスする方法】

① 規定のタッチ操作をおこないます。
待ち受け画面の下図の位置を、左→右→左→右の順で4回タッチします。
※画面が自動スリープ(未操作時に画面が自動で暗くなる機能)している場合は、画面を一度タッチして、明るくしてから操作してください。



② 管理者用 PIN コードを入力すると管理画面が表示されます。
PIN コードの設定は、事前設定が必要です。設定は「4.8.4 管理者用 PIN コード」を参照のこと



5 OS 設定について（出荷時設定済）

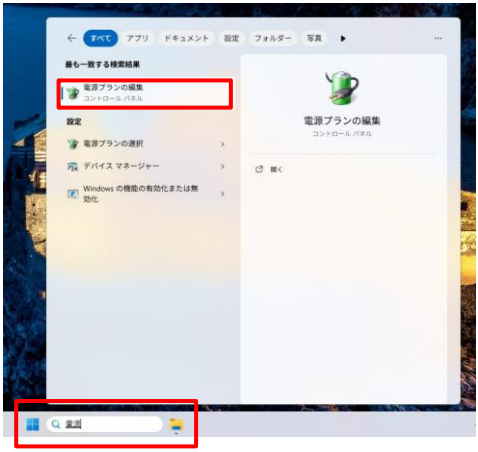
本章では、OS の出荷時設定について説明します。本設定は、顔認証付きカードリーダーのアプリケーションを安定して動作させるために必要になります。

これらの設定は原則として出荷時点で適用済みですが、Windows Update などにより設定が変更される場合がありますので、設定項目を確認する場合や、運用中に画面表示や動作に問題が発生した場合は、各項目の設定をご確認ください。

5.1 電源プラン及び電源ボタンの定義

本機では、専用の推奨電源プランを標準設定として出荷しています。電源プランは、以下の手順で確認できます。

① タスクバーにある検索窓より「電源プランの編集」を入力すると、検索結果に「電源プランの編集」が表示されるのでクリックします。



② 「電源プランの編集」のウィンドウが開きます。
現在のプランが「XC-STFR3J-MN」になっていることを確認します。



現在のプランが「XC-STFR3J-MN」以外の場合は、③以降の手順を引き続き実施します。

③ プラン変更方法（例: 電源プランが「バランス」になっている場合）
「キャンセル」をクリックします。



④ 「XC-STFR3J-MN」を選択します。



⑤　次に「電源ボタンの動作を選択する」をクリックします。



⑥　「電源ボタンを押したときの動作」が「シャットダウン」になっていること、「高速スタートアップ」のチェックが外れていることを確認します。変更した場合は、下部にある「変更の保存」をクリックして終了してください。



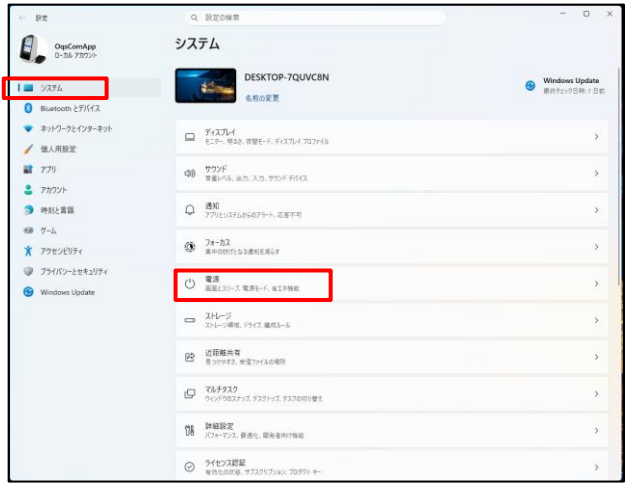
5.2 電源オフ・スリープ設定

本機のアプリケーションは画面オフやスリープ設定が有効になっていると正常に動作しない場合があります。以下の手順に従って確認してください。

① Windows ボタンを押して「設定」をクリックします。



② 「システム」→「電源」の順にクリックします。



③ 「画面、スリープ、休止状態のタイムアウト」をクリックします。



④ 「画面、スリープ、休止状態のタイムアウト」をすべて「なし」に設定されていることを確認します。



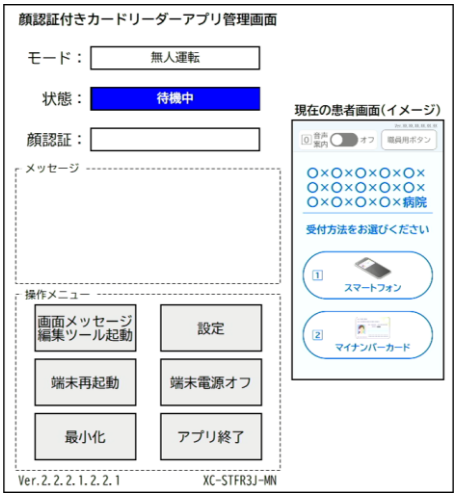
◎ポイント◎

・画面オフ／スリープ設定は変更しないでください。正常に動作しない場合があります。

5.3 USB 省電力設定

本機は、内蔵 USB 機器が安定して動作するよう、**USB ポートの省電力機能を無効**にする設定がされています。以下の手順に従って確認してください。

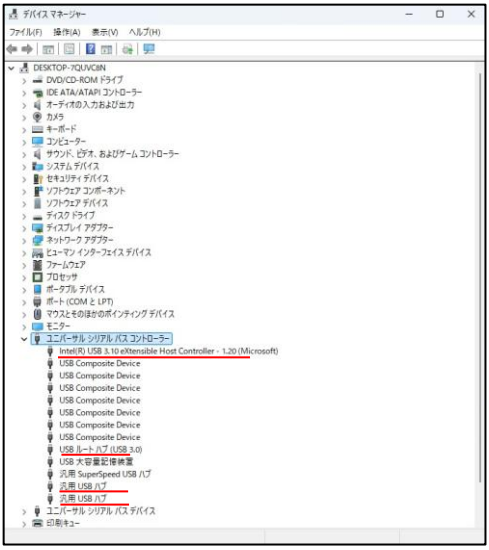
① 顔認証付きカードリーダーの管理画面が起動していることを確認します。



② Windows ボタンを右クリックしてデバイスマネージャーを開きます。



③ 「ユニバーサル シリアル バス コントローラー」を展開し、下図の4つのデバイスについて、それぞれ右クリックして「プロパティ」をクリックします。



④ プロパティ画面で「電源の管理」タブを開き、「電力の節約のために、・・・・オフできるようにする(A)」のチェックが外れていることを確認します。



5.4 ランタイムソフトのインストール

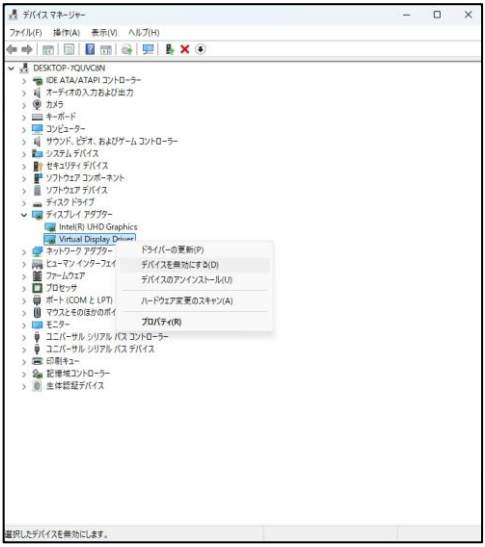
本機のアプリケーションソフトの動作に必要なランタイムソフト(Visual C++ 再頒布可能パッケージ)が導入されています。

入手先
https://learn.microsoft.com/ja-jp/cpp/windows/latest-supported-vc-redist?view=msvc-170
※2026 年4月時点

5.5 仮想ディスプレイドライバー

本機のアプリケーションソフトの動作に必要な仮想ディスプレイドライバーが設定されています。

入手先
https://github.com/VirtualDrivers/Virtual-Display-Driver
※2026 年 3 月時点での最新バージョンです。
仮想ディスプレイドライバーは、デバイスマネージャーから、確認することが可能です。



5.6 ディスプレイのグループポリシー設定

本機のディスプレイのグループポリシー設定が、以下のようになっていることを確認してください。

【グループポリシー設定】

以下 2 つの設定が正しく行われていることを確認してください。

・複数のディスプレイモードを構成する：[複製]

・複製したモニターに優先される解像度ソースを設定する：[外部]

※これらの設定は出荷時に適用済みですが、変更されている場合は再設定してください。

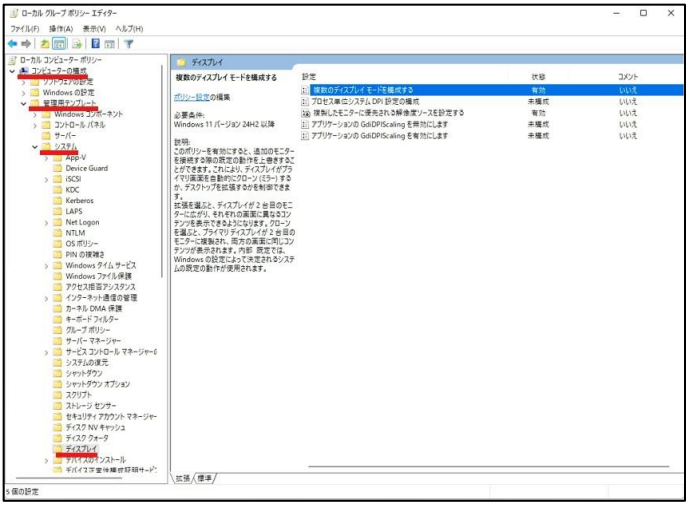
① Windows キー ＋ R を押して、「ファイル名を指定して実行」を開きます。

② gpedit.msc と入力し、「OK」をクリックします。

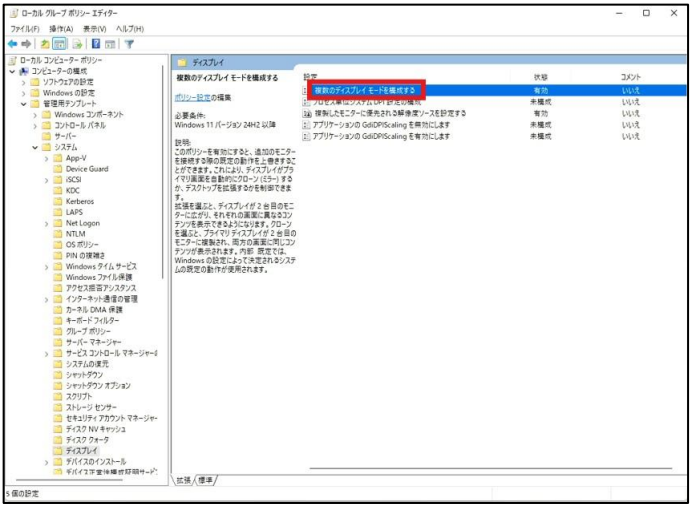


③　ローカルグループポリシーエディターで下記の順に開きます。

【コンピューターの構成】>【管理用テンプレート】>【システム】>【ディスプレイ】



④　「複数のディスプレイモードを構成する」をダブルクリックします。



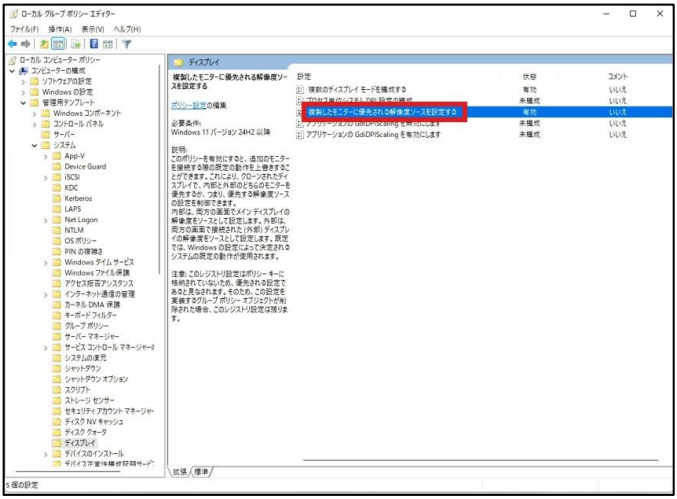
⑤ 「**有効**」を選択します。

⑥ オプション欄で「**複製**」を選択します。

⑦ 「適用」→「OK」をクリックします。



⑧ 項目③と同じフォルダ内にある「複製したモニターに優先される解像度ソースを設定する」をダブルクリックします。



⑨ 「**有効**」を選択します。

⑩ オプション欄で「**外部**」を選択します。

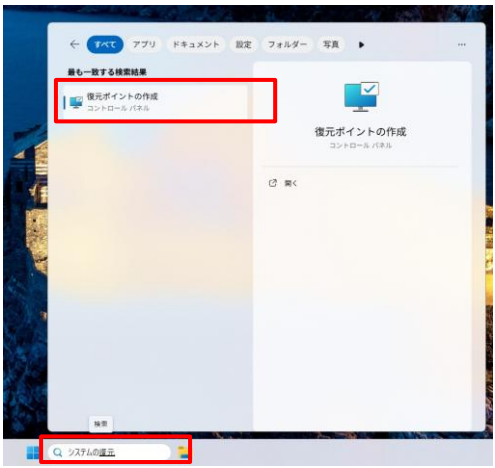
⑪ 「適用」→「OK」をクリックします。



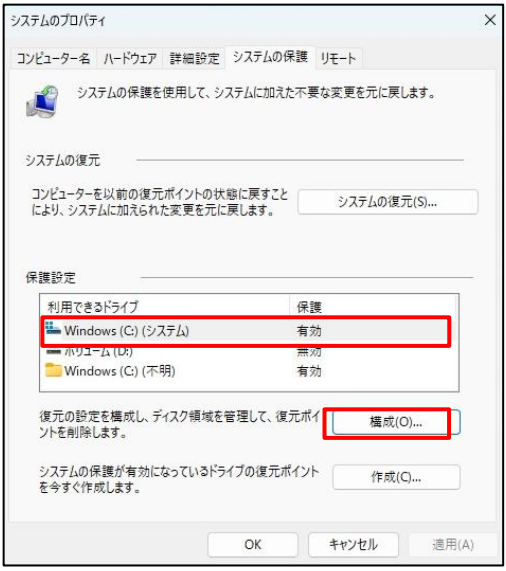
5.7 システム復元の有効化

本機では、Windows システム復元機能を有効化設定しています。
以下の手順で確認ができます。

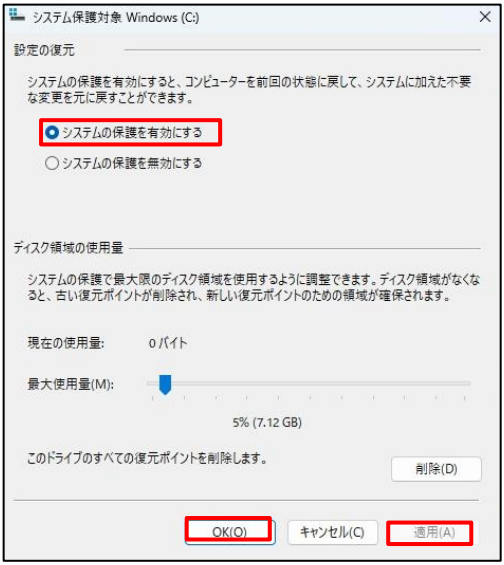
① タスクバーにある検索窓に「システム復元」と入力し、「復元ポイントの作成」をクリックします。



② システムのプロパティを開きます。Windows(C:)(システム)を選択し、「構成」をクリックします。



③ 「システムの保護を有効にする」が選択されていることを確認します。



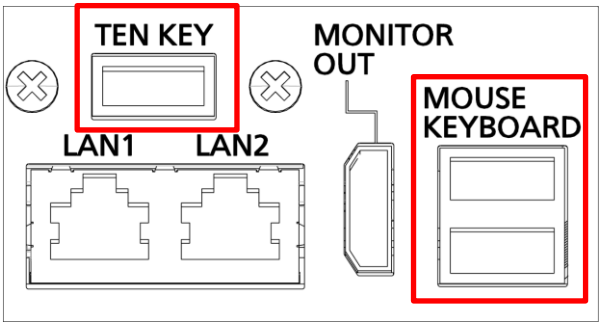
6 ご使用にあたっての注意事項

本機のご使用にあたっての注意事項について説明します。また、取扱説明書(準備編)に記載の注意事項もご参照ください。

6.1 USB ポートの電流制限

本機の USB ポートは、TEN KEY 用と MOUSE･KEYBOARD 用とで、対応する規格が異なります。TEN KEY 用は USB2.0 で最大供給電流は 500mA になります。

MOUSE･KEYBOARD 用は USB3. 2で最大供給電流は 900mA になります。バックアップデータの取得時等において、USB機器を接続する場合は、機器の規格に対応したポートに接続するようにご注意ください。



6.2 情報漏洩リスク

6.2.1 ネットワーク接続の情報漏洩リスク

本機はネットワークに接続して使用するため、不適切な設定や運用により、患者情報や認証情報等の重要な情報が外部へ漏洩するおそれがあります。

以下の点に留意してください。

- 本機は、医療機関内の適切に管理されたネットワークに接続してください。
- 外部ネットワーク(インターネット等)との接続は、ファイアウォールや VPN 等により適切に保護された環境で行ってください。
- 不要なポートの開放や通信設定は行わないでください。
- セキュリティパッチやソフトウェア更新を適切に適用し、常に最新の状態で使用してください。
- ネットワーク構成の変更時は、情報セキュリティ責任者の管理のもと実施してください。

本機は、システム異常や予期しない動作が発生した場合、正常状態への復旧を目的として端末の再起動をおこなう機能を備えています。これにより、一時的な障害や不正な通信等の影響を受けた場合でも、システムの継続運用を支援します。

6.2.2 ユーザー認証に関する情報漏洩リスク

本機はオンライン資格確認において、利用者の認証情報を取り扱います。不適切な管理は不正利用や情報漏洩につながるおそれがあります。

- ID・パスワード等の認証情報は厳重に管理し、第三者と共有しないでください。
- 不正アクセスや不審な挙動を検知した場合は、直ちに使用を停止し管理者へ報告してください。

6.3 FAN の回転数について

本機は、顔認証アプリケーションの起動時に FAN の回転数を自動的に確認します。経年変化などにより回転数が規定値を下回った場合、警告が表示されることがあります。

顔認証アプリケーションを再起動しても警告が繰り返し表示される場合は、自己診断ツールで一度状態を診断してください。診断後も警告が表示される場合は、ご相談窓口までお問い合わせください。

6.4 ユーザー切替について

本機は、Windows のユーザーアカウント「OqsComApp」での運用を前提としています。ユーザー切替をおこなう場合は、必ず事前にログアウトを実施してください。ログアウトを行わずにユーザー切替を行った場合、正常に動作しない可能性があります。

6.5 カード置台の取り扱いについて

カード置台にシール等を貼るのは避けてください。カード券面を正しく識別できなくなる可能性があります。

6.6 ソフトウェアライセンス情報について

本製品には、オープンソースソフトウェアおよび各種ドライバー、ライブラリーが含まれています。

・Apache License 2.0 に基づき提供されるソフトウェア
・New BSD License (The 3-Clause BSD License) に基づき提供されるソフトウェア
・The MIT License に基づき提供されるソフトウェア
・zlib License に基づき提供されるソフトウェア
・ソニー株式会社　NFC デバイスドライバ使用許諾契約書に基づき提供されるソフトウェア

これらのソフトウェアは、それぞれのライセンス条件に基づいて利用されています。各ソフトウェアの使用許諾条件(ライセンス文書)については、以下のフォルダをご確認ください。

C:¥work¥Licenses¥

7 故障かな ！？

顔認証付きカードリーダーに異常が発生した場合、その症状を確認し、以下に示す症状別の対処を実施してください。

症状	考えられる原因	対処方法
画面が表示されない	・アプリケーションソフトが起動していない。	・アプリケーションソフトを起動してください(→3. 3. 2 アプリケーションソフトの手動起動方法について)。
	・電源が切れている。	・ACアダプターに電源コードを接続してください(→準備編 4.3 各機器ケーブルの接続)。
	・ディスプレイの電源が切れている。または PC がスリープしている。	・電源とスリープ設定についてご確認ください(→5. 2 電源オフ・スリープ設定)。
	・Windows へのログイン操作中にアプリケーションが起動した場合、画面が表示されないことがあります。	・アプリケーションソフトを終了し、再度起動してください。
マイナンバーカードが読めない	・本人のマイナンバーカードを置いていない。	・本人のマイナンバーカードを置いてください。
	・マイナンバーカードがケースに入った状態になっている。	・マイナンバーカードをケースから取り出し、カード単体でカード置台に置いてください。
	・顔写真のない裏面を上にして置いている。	・顔写真面を上にした状態でカード置台に置いてください。
	・パスワードがロックしている。	・市町村窓口でロック解除、再設定をおこなってください。
	・カード置台に案内シールなどを貼っている。	・カードを正しく読み取るためには、カード置台にはらないようにしてください。
	・電波を発する機器がある。	・盗難防止タグ解除装置等、普段目に見えないところにある場合もございます。

症状	考えられる原因	対処方法
顔認証できない	・写真が不鮮明、マスクを深く着用しているなどで顔の特徴が十分にとれていない。	・マスクを外してから再度実施してください。
	・電子証明書の有効期限がきれている。	・市町村窓口で電子証明書の更新をおこなってください。
	・顔認証付きカードリーダーでの顔撮影時の条件　顔、環境が満たされていない。	・マスクやサングラスを外してください。 ・明るい場所や逆光がないところで使用してください。 ・顔をモニタガイドの枠内に収めてください。
	・顔認証カメラのレンズが汚れている。	・顔認証カメラ周囲を清掃してください。強くこするとカメラレンズに傷が入る可能性があります。
	・カメラに近づき過ぎている。	・カメラから少し離れて再度実施してください。指定の枠内に顔をいれるようにしてください。
背面インジケーターが消灯しない	電源スイッチを長押し(4 秒以上)等で強制終了をおこなった場合、消灯処理が正しく行われない。	・再起動し、通常の終了処理を再度おこなってください。

※管理画面にエラーコードが表示されておらず、かつ上記対処を行っても改善されない場合、自己診断ツールにより、機器の状態を確認することができます。
詳しくは、こちらを参照ください。

付録 A リモートアクセスの導入（UltraVNC）

リモートアクセスソフト（UltraVNC）を導入することで、医療システム側の端末から内蔵 PC を遠隔操作ができるようになります。

導入にあたってのご注意：

UltraVNC はフリーソフトウェアであり、当社での動作確認は行っておりますが、ソフトウェア自体の性能・動作・将来的な更新内容について、当社が保証するものではありません。詳細な使い方や設定方法については、インターネット上の公開情報やソフトウェア配布元のドキュメントをご参照ください。

また、UltraVNC の導入および運用にあたっては、以下の点についてあらかじめご理解いただきますようお願いいたします。

■1. UltraVNC ソフトウェアに関する保証範囲について

・ソフトウェア自体の不具合

・将来バージョンでの仕様変更

について、当社は保証いたしかねます。

■2. 導入に必要なネットワーク設定について

UltraVNC の利用には、お客様環境に応じたネットワーク設定（ポート開放、ファイアウォール設定、アドレス体系の調整など）が必要となります。これらの設定は当社のサポート対象外となるため、設置ベンダー、システムインテグレーターへのご相談を推奨いたします。

■3. 通信障害・ネットワークトラブルについて

リモートアクセスやネットワーク設定に起因する下記の事象は、当社の「顔認証付きカードリーダー機器」に関するサポート対象外となります。

・通信断（切断）・遅延

・外部ネットワーク経路の不具合

・UltraVNC 利用中の接続障害

・ネットワークのセキュリティ設定によるアクセス不可

■4. セキュリティ対策に関する責任範囲

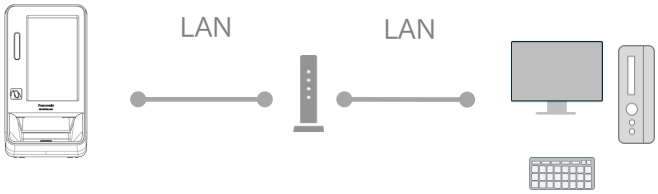
UltraVNC の利用にあたって必要となる認証設定、暗号化の有無、パスワード管理、アクセス権限の設定などのセキュリティ対策は、お客様の管理責任範囲となります。不適切な設定による情報漏洩等について当社は責任を負いかねます。

■5. UltraVNC に関するお問い合わせについて

UltraVNC の操作方法・トラブルシューティング・設定手順など、ソフトウェアそのものに関するお問い合わせにはお答えできません。必要に応じ、ソフトウェア提供元の情報や公開コミュニティをご利用ください。

A-1 リモートアクセスの導入（UltraVNC）

本書では、UltraVNC を用いて顔認証付きカードリーダーへリモートアクセスするための手順を説明します。主な構成は次のとおりです。



顔認証付きカードリーダー
（UltraVNC サーバー）

お使いの医療システム
（UltraVNC ビューワー）

事前準備

次のものをご準備ください。

・UltraVNC（64bits 版）（https://uvnc.com/）
・セットアップ作業を完了した顔認証付きカードリーダー本体
・自動ログインの設定（こちらを参照）

A-1.1 顔認証付きカードリーダー側のインストール手順

導入する Ultra VNC(64bits)版を入手します。(正式サイト https://uvnc.com/からダウンロードすることができます。)ダウンロードしたインストーラーは USB メモリなどを利用して、顔認証付きカードリーダー本体へコピーします。なお、コピー先は、デスクトップやドキュメントフォルダなど、特に指定はありません。

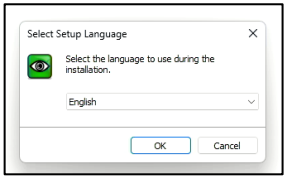
① コピーしたインストーラーをクリックして実行します。

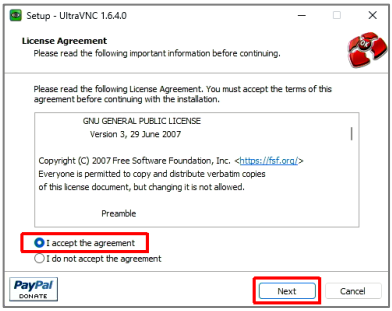


② ユーザーアカウント制御(UAC)の警告画面が表示された場合は、「はい」をクリックして続行します。

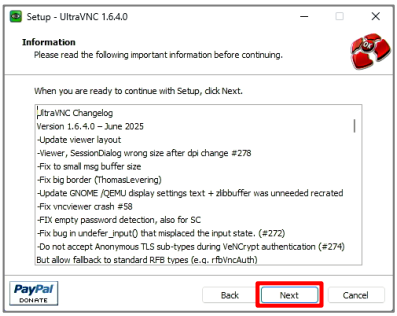


③ 言語を選択します。使用許諾が表示されますので、内容を確認の上、同意の項目にチェックを入れて「Next」をクリックします。

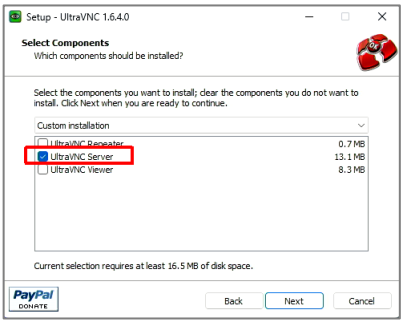




④ 情報表示を確認して「Next」をクリックします。



⑤ インストールするコンポーネントの選択画面が表示されますので、「UltraVNC Server」にチェックを入れて「Next」をクリックします。



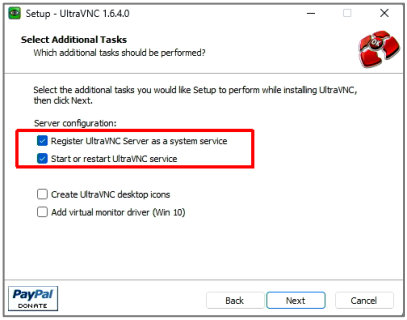
⑥　追加で実行するタスクを選択します。

以下の2項目についてチェックを入れて「Next」をクリックします。

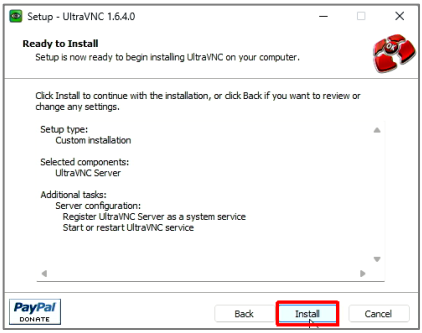
・「Register UltraVNC Server as a system service」

・「Start or restart UltraVNC service」

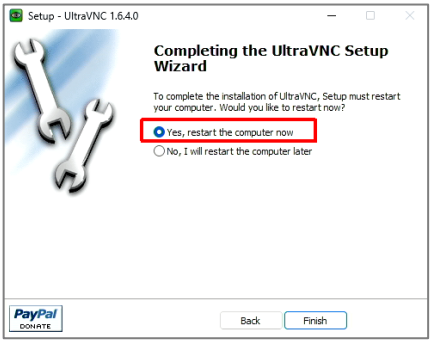
なお、「Add virtual monitor driver」は選択しないでください。



⑦ 「Install」をクリックします。



⑧ インストールが完了したら、「Finish」をクリックして再起動します。



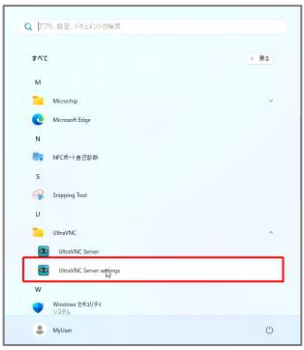
A-1.2 顔認証付きカードリーダー側の設定

ここでは UltraVNC の環境設定について説明します。

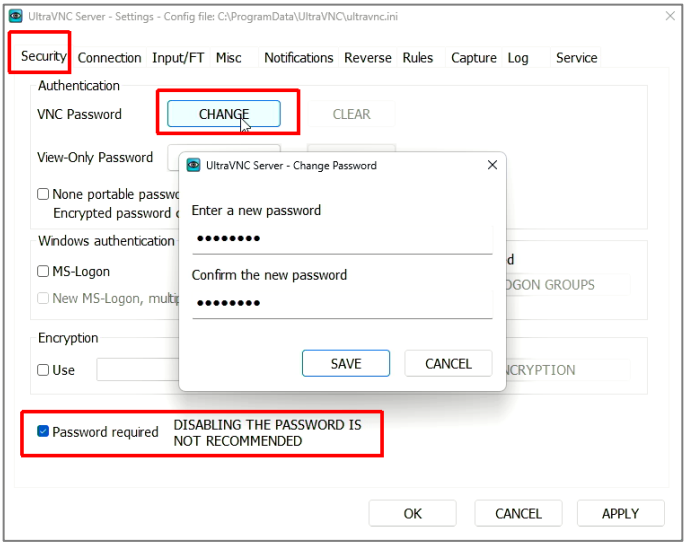
UltraVNC のインストールが完了したら、再起動後、管理者権限のあるユーザーでWindowsにログインし、UltraVNC の設定画面を開きます。

① Windows のスタートメニューを開き、「UltraVNC Server Settin」を開きます。
すべて＞UltraVNC ＞ UltraVNC Server Settings





② 「Security」タブにおいて、VNC Password を設定します。



CHANGE ボタンを押すとパスワードの変更画面が表示されますので、リモートアクセスする際に入力するパスワードを設定してください。
下部にある「Password required」にチェックが入っていることを確認してください。

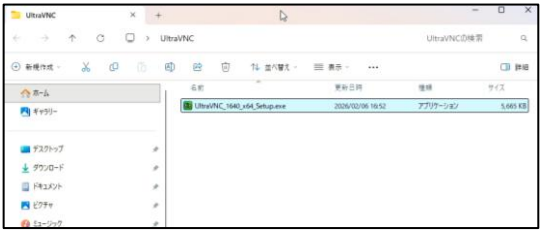
以上で基本設定は終わりです。

A-1.3 医療システム側への UltraVNC 導入

ここでは、リモート元になるお使いの医療システムへの UltraVNC の導入方法について説明します。

リモート元にする Windows の PC に合わせて Ultra VNC（64bits あるいは 32bits）版を入手します。（正式サイト https://uvnc.com/からダウンロードすることができます。）ダウンロードしたインストーラーは USB メモリなどを利用して、リモート元の端末へコピーします。

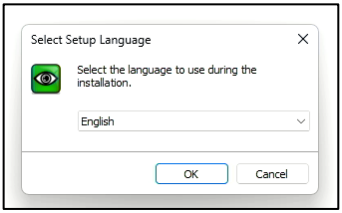
① コピーしたインストーラーをクリックして実行します。

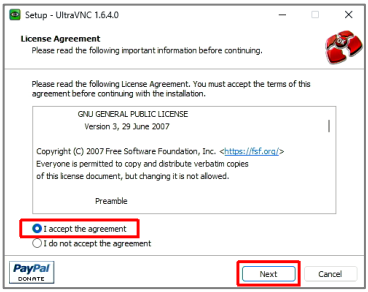


② ユーザーアカウント制御（UAC）の警告画面が表示された場合は、「はい」をクリックして続行します。

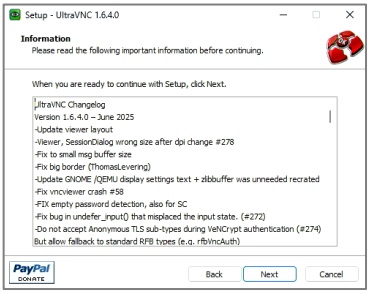


③ 言語を選択します。使用許諾が表示されますので、内容を確認の上、同意の項目にチェックを入れて「Next」をクリックします。

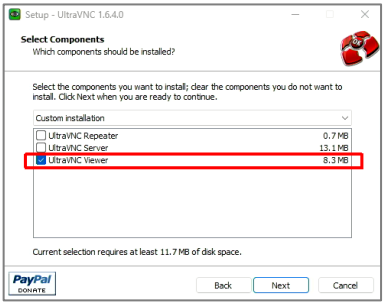




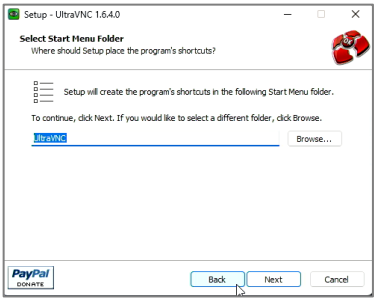
④ 情報表示を確認して「Next」をクリックします。



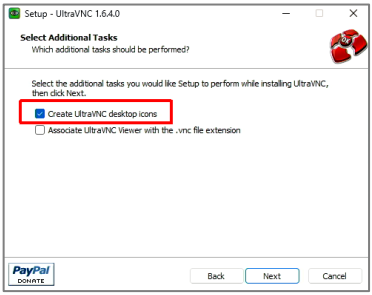
⑤ インストールするコンポーネントの選択画面が表示されますので、「UltraVNC Viewer」にチェックを入れて「Next」をクリックします。



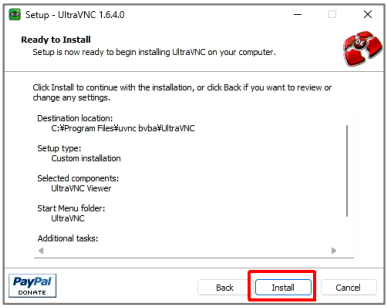
⑥ インストール先を確認して「Next」をクリックします。



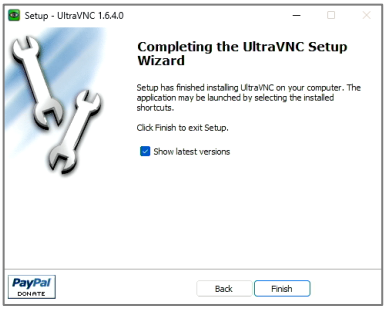
⑦ 「Create UltraVNC desktop icons」にチェック入れて「Next」をクリックします。



⑧ 「Install」をクリックします。

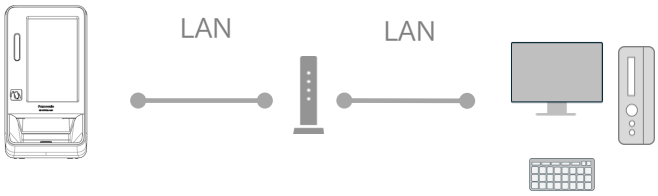


⑨　インストールが完了したら、「Finish」をクリックして再起動します。



A-2 リモートアクセス例

ここでは、以下のネットワーク設定(例)がおこなわれているという前提でリモートアクセスの手順を説明します。



顔認証付きカードリーダー
(UltraVNC サーバー導入)

お使いの医療システム
(UltraVNC ビューワーの導入)

顔認証付きカードリーダー(Ultra VNC サーバー側)

IP アドレス	192.168.1.11
サブネットマスク	255.255.255.0

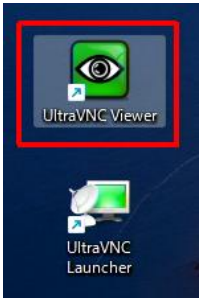
お使いの医療システム(Ultra VNC ビューワー側)

IP アドレス	192.168.1.10
サブネットマスク	255.255.255.0

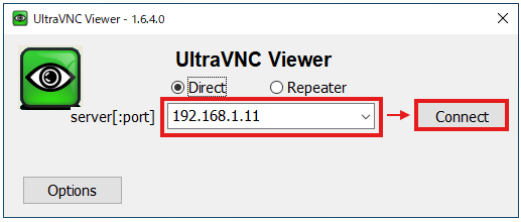
※上記 IP アドレスは設定例となります。ご使用のネットワーク環境に応じて設定する必要があります。

A-2.1 リモートアクセス手順

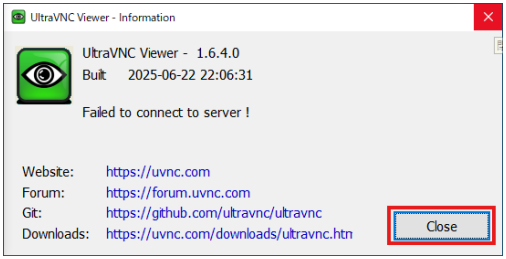
① 医療システム側にインストールした UltraVNC ビューワーを起動します。デスクトップ上の UltraVNC Viewer をクリックします。



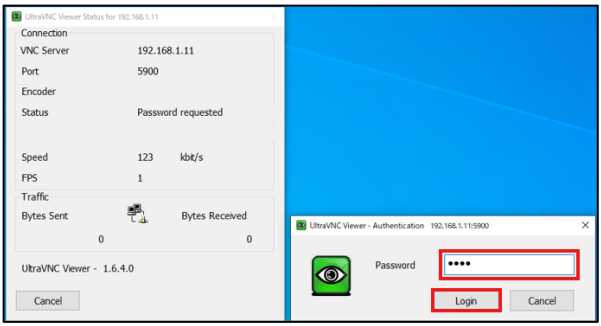
② リモートアクセス先を入力します。
ここでは顔認証付きカードリーダーにリモートアクセスするので、IP アドレス 192.168.1.11 を入力して「Connect」をクリックします。



IP アドレスが間違っていると下記が表示されて接続できません。「Close」をクリックして再度①の手順から実施していただき、正しい IP アドレスを入力してください。

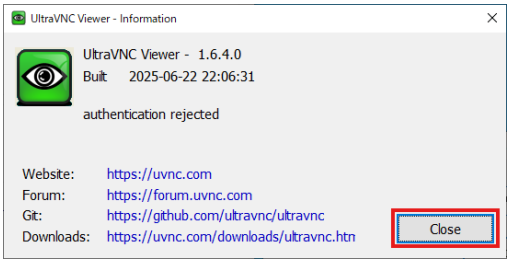


③　パスワード(ここでは1234)を入力して「Login」をクリックします。

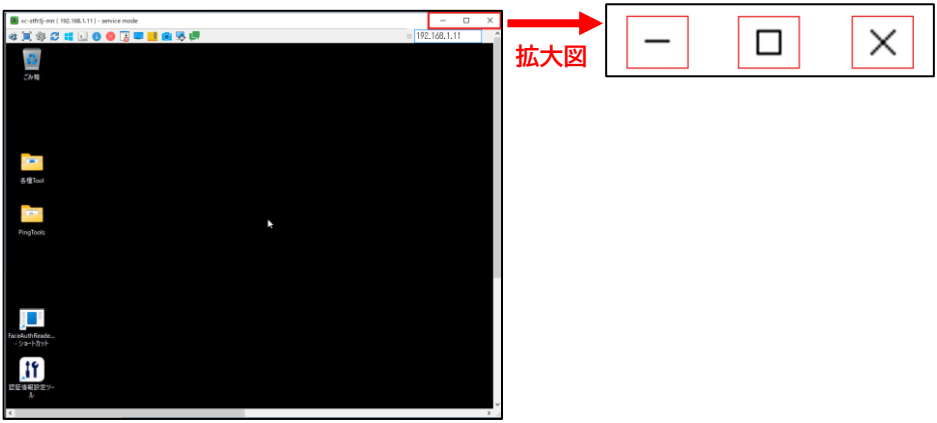


※設定したパスワードを入力します。

パスワードが間違っていると下記が表示されて接続できません。「Close」をクリックして再度①の手順から実施していただき、正しいパスワードを入力してください。



④　ログインに成功すると顔認証付きカードリーダーにリモートアクセスされます。
　　表示された画面を最小化するには「—」、最大化するには「□」、リモートアクセスを終了するには「×」をクリックします。



⑤最大化された画面を最小化するには「—」、元のサイズに戻すには「🗗」、リモートアクセスを終了するには「×」をクリックします。



パナソニック コネクト株式会社

〒104-0061　東京都中央区銀座八丁目21番1号

© Panasonic Connect Co., Ltd. 2026