

指 静 脈 認 証 シ ス テ ム
J O H M O N

静

紋

取扱説明書 ソフトウェア編 J300



取扱説明書はよく読み、保管してください。

- ・ 本製品をお使いになる前に本取扱説明書をよく読み、十分理解し、正しくお使いください。
- ・ お読みになったあとは、保証書とともに、いつでもすぐに参照できる所に大切に保管してください。

CDR-22517

重要なお知らせ

- 本書の内容の一部または全部を、無断で転載あるいは引用することを禁止します。
- 本書の内容については将来予告なしに変更することがあります。
- 本書の記述内容について万一ご不審な点や誤りなど、お気づきのことがありましたら、お買い求め先へご一報くださいますようお願いいたします。
- 本取扱説明書に記載された株式会社日立ソリューションズの製品は、全て現状のままで販売、または利用許諾されるものです。
- 株式会社日立ソリューションズは、本取扱説明書に従わない使用はもとより、製品または製品の使用から生じたいかなる損害(逸失利益、その他の間接損害を含む)についても責任を負いません。保証と責任の全体はハードウェア編「7 保証範囲」をご覧ください。

製品の信頼性について

- ・ ご購入いただきました製品は、一般事務用を意図して設計・製作されています。生命、財産に著しく影響のある高信頼性を要求される用途への使用は避けてください。このような使用に対する万一の事故に対し、弊社は一切責任を負いません。一般事務用製品が不適当な、高信頼性を必要とする用途
 - ・ 化学プラント制御、医療機器制御、緊急連絡制御など
- ・ 他の認証装置との併用については動作保証していません。

規制、対策などについて

■ 電波障害自主規制について

この装置は、一般財団法人 VCCI 協会の基準に基づくクラス B 情報技術装置です。この装置は、家庭環境で使用することを目的としています。この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。その場合は、テレビやラジオなどからできるだけ離したり、テレビやラジオなどのアンテナの向きを変えたりしてみてください。

■ 輸出規制について

本製品を輸出される場合には、外国為替及び外国貿易法の規制ならびに米国の輸出管理関連法規などの規制をご確認の上、必要な手続きをお取りください。この装置に付属する周辺機器やソフトウェアも同じ扱いになります。なお、ご不明な場合は、弊社営業担当にお問い合わせください。

著作権

All rights reserved.

© Hitachi Solutions, Ltd. 2006, 2022.

© Hitachi, Ltd. 2006, 2022.

本書は株式会社日立ソリューションズおよび(株)日立製作所が全ての版權を所有しています。本書の著作権は、国内法および国際条約により保護されています。

株式会社日立ソリューションズの書面による同意なしでは、本取扱説明書は一部たりとも、

① 複製・複写・転送・検索機能を持つ記憶装置へ記録すること。

② 他の言語やコンピュータ言語へ翻訳すること。

を禁止しています。また、これらの手段として、電子的、機械的、磁氣的、光学的などのいかなる方法を用いても同じです。

静紋 は 株式会社日立ソリューションズの登録商標です。

Windows は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Windows Server は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Microsoft Limited Permissive License (Ms-LPL)

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

1. Definitions

The terms “reproduce,” “reproduction,” “derivative works,” and “distribution” have the same meaning here as under U.S. copyright law.

A “contribution” is the original software, or any additions or changes to the software.

A “contributor” is any person that distributes its contribution under this license.

“Licensed patents” are a contributor’s patent claims that read directly on its contribution.

2. Grant of Rights

(A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

(B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

3. Conditions and Limitations

(A) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.

(B) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

(C) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

(D) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

(E) The software is licensed “as-is.” You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

(F) Platform Limitation- The licenses granted in sections 2(A) & 2(B) extend only to the software or derivative works that you create that run on a Microsoft Windows operating system product.

目次

1	はじめに.....	8
1.1	お問い合わせ先.....	8
1.2	前提条件.....	9
2	ソフトウェアのインストール.....	12
2.1	インストールの前に.....	12
2.2	指静脈認証ソフトウェアのインストール.....	13
2.3	指静脈認証ソフトウェアのサイレントインストール.....	21
2.4	以前のバージョンからのアップデートについて.....	23
2.5	以前のバージョンからのサイレントアップデートについて.....	26
2.6	ドライバインストールの確認.....	27
3	初回時管理者登録.....	34
4	ソフトウェアのアンインストール.....	43
4.1	指静脈認証ソフトウェアのアンインストール.....	43
4.2	指静脈認証ソフトウェアのサイレントアンインストール.....	48
5	認証機能.....	49
5.1	Windows ログオン（静紋認証の場合）.....	51
5.2	Windows ログオン（ID と静紋認証の場合）.....	55
5.3	Windows ログオン（静紋と二要素用パスワード認証の場合）.....	60
5.4	Windows ログオン（ID と静紋と二要素用パスワード認証の場合）.....	66
5.5	Windows ログオン（ID と静紋と Windows パスワード認証の場合）.....	72
5.6	スクリーンセーバーロック解除（静紋認証の場合）.....	77
5.7	スクリーンセーバーロック解除（ID と静紋認証の場合）.....	81
5.8	スクリーンセーバーロック解除（静紋と二要素用パスワード認証の場合）.....	85
5.9	スクリーンセーバーロック解除（ID と静紋と二要素用パスワード認証の場合）.....	90
5.10	スクリーンセーバーロック解除（ID と静紋と Windows パスワード認証の場合）.....	95
6	ユーザー管理機能.....	99
6.1	新規ユーザーの登録.....	104
6.2	指情報の追加.....	113
6.3	指情報の変更.....	118
6.4	指情報の削除.....	121
6.5	二要素認証の設定.....	122
6.6	緊急用パスワードの設定.....	123
6.7	認証方法の変更.....	125
6.8	ログ出力設定.....	127
6.9	ビープ音の ON/OFF.....	128
6.10	アンインストール用パスワードの設定.....	129
6.11	認証の練習.....	131

6.12 ログの参照.....	132
6.13 フィルタオプションの設定	133
6.14 なりすまし防止強化レベル設定	134
6.15 ユーザー管理画面の終了	135
7 ログの参照	136
7.1ログオン関係のログ	137
7.2管理ログ	138
7.3ログオン関係のログと管理ログ	139
7.4リモート接続のログ	140
7.5テキスト形式での出力.....	140
7.6その他の機能.....	140
8 緊急用パスワードの利用.....	143
8.1Windows Server 2012 / Windows 8.1 / Windows Server 2012 R2 のログオン・ ロック解除の場合.....	143
8.2Windows 10 / Windows Server 2016 / Windows Server 2019 / Windows 11 の ログオン・ロック解除の場合	144
8.3ユーザー管理機能のロック解除の場合	145
9 Windows パスワードの変更.....	147
9.1Windows Server 2012 / Windows 8.1 / Windows Server 2012 R2 をお使いの場 合	148
9.2Windows 10 / Windows Server 2016 / Windows Server 2019 / Windows 11 を お使いの場合	149
10 リモートデスクトップ環境で使用するための設定.....	150
10.1 リモート接続元パソコンに本製品をインストール.....	152
10.2 リモート接続元パソコンで必要な設定.....	153
10.3 リモート接続先パソコンに本製品をインストール.....	156
10.4 リモート接続先パソコンで初回時管理者登録を実行	157
10.5 リモート接続先パソコンで必要な設定.....	158
10.6 リモート接続先パソコンで行うリモートログオン設定	159
10.7 リモートログオンの実行	161
11 二要素用パスワードの変更.....	164
12 ソフトウェア仕様	166
13 トラブルシューティング	168
14 付録.....	182
14.1 スクリーンセーバーの設定について	182

1 はじめに

このたびは、指静脈認証システム「静紋」^{じょうもん}（以下、本製品と呼びます）をお買い上げいただき、まことにありがとうございます。

本書は、「取扱説明書ソフトウェア編」です。本製品を初めてお使いになる方のために、本製品のソフトウェアの使用方法を説明しています。

マニュアルの説明している画面およびイラストは一例です。機種によっては、異なる場合があります。説明の都合で、画面のアイコンやイラストのケーブルなど、一部省略している場合があります。

URL、お問い合わせ先、画面などは、マニュアル制作時点のものです。

1.1 お問い合わせ先

本製品についての技術的なお問い合わせは静紋テクニカルサポート窓口でご回答いたしますので、次のE-Mail でお問い合わせください。

また、お問い合わせの前に本書巻末の「14 トラブルシューティング」をお読みになり現象をご確認ください。

静紋テクニカルサポート窓口

E-Mail : johmon-support@hitachi-solutions.com

以下のウェブサイトにて最新の製品情報を掲載しております。併せてご参照ください。

日立ソリューションズ「静紋」ホームページ
<https://www.hitachi-solutions.co.jp/johmon/>

※上記URLは予告なしに変更される場合があります。上記URLが見つからない場合は、弊社ホームページ(<https://www.hitachi-solutions.co.jp/>)よりアクセスしてください。

1.2 前提条件

本製品をお使いになるためには、お使いのパソコンが以下の機種や OS である必要があります。対応していることをご確認ください。

① 対応機種・OS

対応機種	対応 OS
PC/AT 互換機	[32 ビット OS] Windows 8.1 Update 無印 / Pro / Enterprise Windows 10 Enterprise 2016 LTSC (Version 1607 相当) Windows 10 Enterprise LTSC 2019 (Version 1809 相当) Windows 10 Home / Pro / Enterprise Version 21H1 Windows 10 Home / Pro / Enterprise Version 21H2 Windows 10 Enterprise LTSC 2021 (Version 21H2 相当) [64 ビット OS] Windows Server 2012 Standard Windows 8.1 Update 無印 / Pro / Enterprise Windows Server 2012 R2 Update Standard Windows 10 Enterprise 2016 LTSC (Version 1607 相当) Windows 10 Enterprise LTSC 2019 (Version 1809 相当) Windows 10 Home / Pro / Enterprise Version 21H1 Windows 10 Home / Pro / Enterprise Version 21H2 Windows 10 Enterprise LTSC 2021 (Version 21H2 相当) Windows Server 2016 Standard Windows Server 2019 Standard Windows 11 Home / Pro / Enterprise Version 21H2 Windows 11 Home / Pro / Enterprise Version 22H2 ※いずれも日本語 OS ※Windows 7 / Windows Server 2008 / Windows Server 2008 R2 / Windows 10 Version 1703 / Windows 10 Version 1709 / Windows 10 Version 1809 / Windows 10 Version 1903 / Windows 10 Version 1909 / Windows 10 Version 2004 への対応は終了しました
搭載 CPU	各 OS で規定されているシステム要件に準じます
メモリ	各 OS で規定されているシステム要件に準じます ※インストールされているソフトウェアなど、ご使用の環境によっては、最小メモリ所要量より多くのメモリ容量が必要になる場合があります

② 対応ドメイン

Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019

③ ハードディスク

空き容量50MB以上

④ 対応リモートデスクトップ接続プログラム

シェルバージョン 6.0 ～ 10.0.22621

コントロールバージョン 6.0 ～ 10.0.22621

リモートデスクトッププロトコル 6.0 ～ 10.11

重要

- Windows のログオン画面を置き換えるアプリケーションとの併用はできません。それらのソフトウェアを必ずアンインストール後、本製品をインストールしてください。

(例)

弊社製品 静紋Jシリーズおよびそれらの認証装置に付属するソフトウェア
弊社製品 AuthentiGate 等

- お使いの OS の種類によって、使用するインストーラが異なります。また、1 つの OS に対して複数をインストールすることはできません。
- 本製品をご利用になるためには、あらかじめ Windows のユーザーにパスワードを設定しておく必要があります。
- Windows 10 または Windows 11 で指静脈認証方式によるリモートデスクトップ接続をご使用になる場合、ネットワークの伝送状況によっては接続エラーとなる場合があります。
- パスワード代替入力機能のサポートは終了しました。

2 ソフトウェアのインストール

インストールおよびアンインストールはお使いのパソコンの Administrators グループに属するユーザーで行ってください。

重要

Windows サービスパックのアンインストールを行うと、USB のドライバが自動的に削除され、認証装置が認識できなくなる場合があります。そのため、サービスパックのアンインストールを行う場合は Windows の標準認証に戻してください。Windows の標準認証への戻し方は取扱説明書の [6.7 認証方法の変更] を参照してください。

2.1 インストールの前に

静紋がインストールされていないパソコンにインストールする場合は、[2.2 指静脈認証ソフトウェアのインストール]を参照してください。

J300 の以前のバージョンからアップデートを行う場合は、[2.4 以前のバージョンからのアップデートについて]を参照してください。

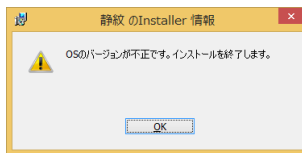
重要

- ・ 静紋 J300 は、静紋 J100, J200, J210 からのアップデートには対応しておりません。静紋 J300 をご使用になる前に、現在お使いのバージョンのマニュアルを参照して、以前のソフトウェアをアンインストールしてください。また、指静脈データに互換性がないため、再度、指静脈の登録が必要になります。

2.2 指静脈認証ソフトウェアのインストール

以下に、インストールの手順を示します。

お使いのOSの種類に対応していないインストーラを起動すると、以下の画面が表示され、インストールに失敗します。正しいインストーラを実行してください。
なお、インストーラを互換モードで起動した場合、お使いのOSの種類に対応していないインストーラを起動しても以下の画面が表示されない場合があります。

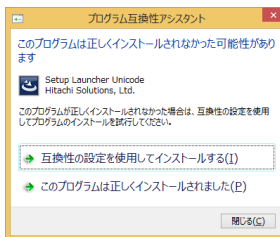
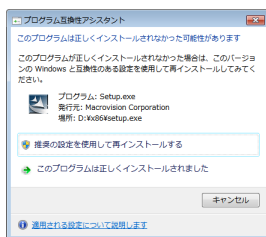


インストールに失敗した場合、以下の画面が表示される場合があります。必ず[閉じる]をクリックして画面を終了させてください。それ以外の操作をすると、不正にインストールが行われ、指静脈認証ソフトウェアが正常に動作しなくなります。インストールしてしまった場合、「14 トラブルシューティング」を参照して再インストールを行ってください。



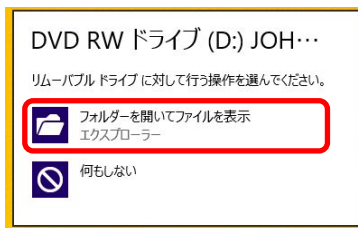
重要

- 指静脈認証ソフトウェアをインストールするパソコンでは、以下のような設定をしないでください。
 - 「フォントサイズ」を「標準」以外に設定する。この設定を行うと、アプリケーションのメッセージが正常に表示されない問題が生じる場合があります。
- インストールに失敗していない場合にも、以下のような画面が表示されることがあります。[キャンセル]または[閉じる]をクリックして画面を終了させてください。

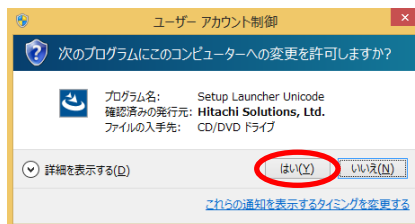


- Windows Server 2012 / Windows 8.1 / Windows Server 2012 R2 / Windows 10 / Windows Server 2016 / Windows Server 2019 / Windows 11 の場合、本インストーラでは「他のユーザー」というユーザーを自動で作成します。このユーザーには100文字以上のランダムなパスワードが設定されています。このユーザーに対して設定の変更を行わないようにしてください。このユーザーを削除すると指静脈による認証でサインインできなくなります。

- ① 本製品に同梱されている「アプリケーション CD-ROM」をお使いのパソコンのCD-ROM ドライブに挿入します。お使いの環境によっては右の画面が表示される場合があります。その場合は[フォルダーを開いてファイルを表示]をクリックします。



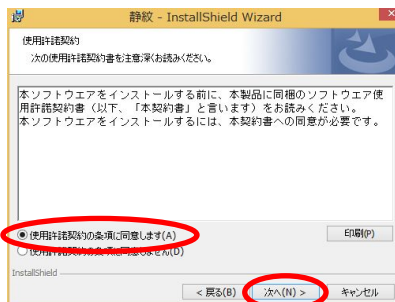
- ② 32 ビット OS へインストールする場合は、CD-ROM ドライブの「x86」フォルダに収録されている「setup_x86.exe」を起動します。64 ビット OS へインストールする場合は、CD-ROM ドライブの「x64」フォルダに収録されている「setup_x64.exe」を起動します。お使いの環境によっては右の画面が表示される場合があります。その場合は[はい(Y)] ボタンをクリックします。表示されない場合は次の手順へ進みます。



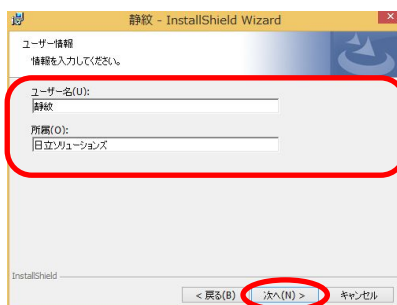
- ③ お使いのパソコンに指静脈認証ソフトウェアを初めてインストールする場合は、右の画面が表示されます。[次へ(N)] ボタンをクリックします。



- ④ 使用許諾契約が表示されます。内容をご確認いただき、許諾される場合は「使用許諾契約の条項に同意します(A)」をチェックし、[次へ(N)] ボタンをクリックします。



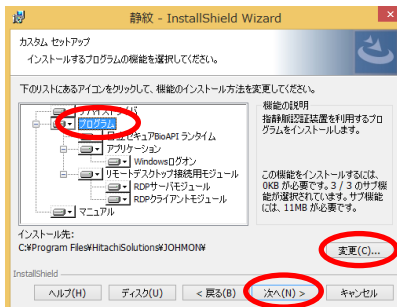
- ⑤ ユーザー名、所属を入力して、[次へ(N)] ボタンをクリックします。



- ⑥ セットアップのタイプを選択して、[次へ(N)] ボタンをクリックします。「カスタム(S)」を選択した場合は、インストール先や、インストールするソフトウェアの種類を選択することができます。初回時は「完全(C)」を選択することをお勧めします。



- ⑦ 「カスタム」を選択した場合は右の画面が表示されます。インストールするソフトウェアを選択します。インストールするソフトウェアを選択して、[次へ(N)] ボタンをクリックします。
- インストール先を変更する場合は「プログラム」をクリックした後に [変更(C)] ボタンをクリックします（「プログラム」がクリックされていない状態では [変更(C)] ボタンをクリックすることはできません）。



[変更(C)] ボタンをクリックすると右の画面が表示されます。この画面ではインストール先を変更できます。インストール先は (C:\Program Files\HitachiSolutions\JOHMON) が初期値になっています。表示されているインストール先で良ければ、[OK] ボタンをクリックします。



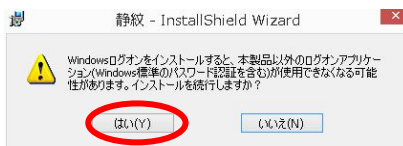
重要

下記フォルダへのインストールはサポートしておりません。

- ・ ネットワークフォルダ
- ・ 圧縮属性フォルダ
- ・ 暗号化属性フォルダ

また、インストールしたフォルダに対してアクセス権を変更しないでください。正常に動作しない恐れがあります。

- ⑧ 手順⑥、⑦終了後に右の画面が表示されることがあります。
警告をよく読み、問題ないことを確認した上で[はい(Y)]ボタンをクリックします。



[いいえ(N)]をクリックすると、手順⑥または手順⑦の画面に戻りますので、選択をやり直してください。

重要

他製品のログオンアプリケーションがインストールされているパソコンに対してWindows ログオンをインストールすると、他製品のログオンアプリケーションが使用できなくなり、それによって重大な問題を引き起こす可能性があります。
上記の警告画面が表示された場合は、必ず他製品のマニュアル等を熟読し、ログオンアプリケーションが使用できなくなっても問題ないことを確認してから、インストールを続行してください。

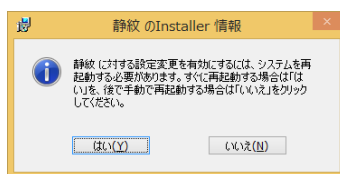
- ⑨ インストールの準備が完了すると右の画面が表示されます。[インストール] ボタンをクリックします。



- ⑩ インストールが完了すると右の画面が表示されます。
(⑦で選択したソフトウェアによっては、表示されるメッセージが異なります)



お使いのパソコンによっては、右の画面が表示される場合があります。この画面で[はい(Y)]をクリックすると自動的にパソコンを再起動します。[いいえ(N)]をクリックするとインストールをいったん終了しますが、手動でパソコンを再起動するまでインストールが完了しない状態になります。

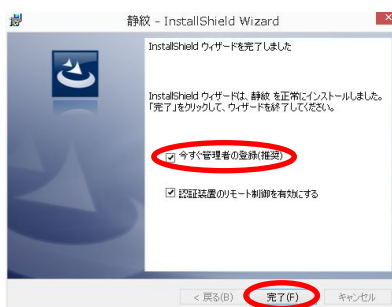


この画面が出た場合は、パソコンを再起動した後に、本書の[6 ユーザー管理機能]を参照してユーザー管理を起動し、[3 初回時管理者登録]を参照して管理者の登録を行ってください。

- ⑪ 指静脈認証ソフトウェアは管理者の登録を行わないと利用することができません。引き続き管理者の登録を行うことを推奨します。管理者の登録を行う場合は「今すぐ管理者の登録（推奨）」をチェックして、「完了」ボタンをクリックします。

「今すぐ管理者の登録（推奨）」のチェックを行わずに「完了」ボタンをクリックした場合は、ユーザー管理機能の初回起動時に管理者の登録を行います。その際は、必ず Administrators グループに属するユーザーで行ってください。

管理者の登録については[3 初回時管理者登録]を参照してください。



本製品をリモートデスクトップ環境で使用する場合は、「認証装置のリモート制御を有効にする」をチェックして「完了」ボタンをクリックします。本製品をリモートデスクトップ環境で使用方法については、「11 リモートデスクトップ環境で使用するための設定」を参照してください。

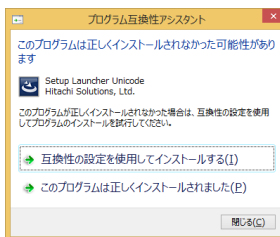
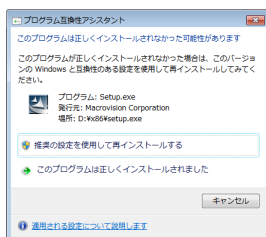
以上でソフトウェアのインストールは完了です。

2.3 指静脈認証ソフトウェアのサイレントインストール

以下に、サイレントインストールの手順を示します。

重要

- 指静脈認証ソフトウェアをインストールするパソコンでは、以下のような設定をしないでください。
 - 「フォントサイズ」を「標準」以外に設定する。この設定を行うと、アプリケーションのメッセージが正常に表示されない問題が生じる場合があります。
- インストールに失敗していない場合にも、以下のような画面が表示されることがあります。[キャンセル]または[閉じる]をクリックして画面を終了させてください。



- Windows Server 2012 / Windows 8.1 / Windows Server 2012 R2 / Windows 10 / Windows Server 2016 / Windows Server 2019 / Windows 11 の場合、本インストーラでは「他のユーザー」というユーザーを自動で作成します。このユーザーには100文字以上のランダムなパスワードが設定されています。このユーザーに対して設定の変更を行わないようにしてください。このユーザーを削除すると指静脈による認証でサインインできなくなります。

- ① [管理者として実行(A)]を指定し、コマンドプロンプトを起動してください。
- ② カレントディレクトリをインストールプログラムが格納されている場所に移動します。
- ③ 下記コマンドを実行します。(32 ビット OS の場合は「x86」フォルダに収録されている「setup_x86.exe」、64 ビット OS の場合は「x64」フォルダに収録されている「setup_x64.exe」を使用してください。)
なお、手順の中で使用する「△」は、半角スペースを示します。

<32 ビット OS の場合>

```
> setup_x86.exe△/s△/v"/qn"
```

<64 ビット OS の場合>

```
> setup_x64.exe△/s△/v"/qn"
```

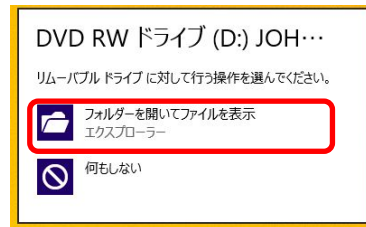
2.4 以前のバージョンからのアップデートについて

以下に、アップデートの手順を示します。

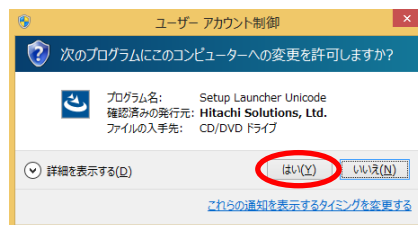
重要

パスワード代替入力機能のサポートは終了しました。
本バージョンにアップデートすると、パスワード代替入力機能は、お使いの PC から削除されます。

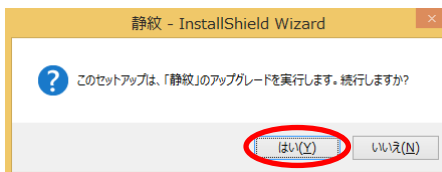
- ① 本製品に同梱されている「アプリケーション CD-ROM」をお使いのパソコンの CD-ROM ドライブに挿入します。
お使いの環境によっては右の画面が表示される場合があります。その場合は[フォルダーを開いてファイルを表示]をクリックします。



- ② 32 ビット OS へインストールする場合は、CD-ROM ドライブの「x86」フォルダに収録されている「setup_x86.exe」を起動します。64 ビット OS へインストールする場合は、CD-ROM ドライブの「x64」フォルダに収録されている「setup_x64.exe」を起動します。
お使いの環境によっては右の画面が表示される場合があります。その場合は[はい(Y)]ボタンをクリックします。
表示されない場合は次の手順へ進みます。



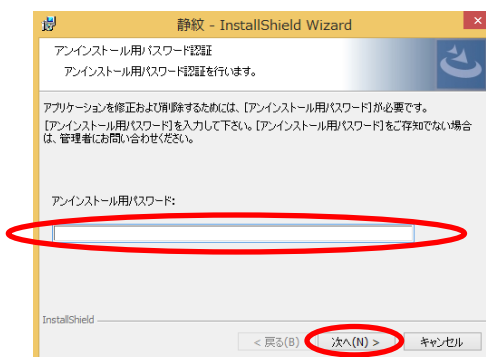
- ③ 右の画面が表示されるので、
[はい(Y)] ボタンをクリックし
ます。



- ④ 右の画面が表示されるので、
[次へ(N)] ボタンをクリック
します。



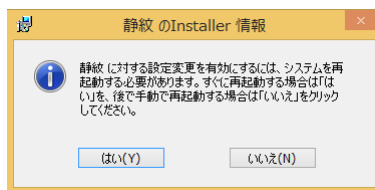
- ⑤ アンインストール用パスワ
ードを設定している場合に
はパスワード入力ダイアロ
グが表示されます。ユーザー
管理機能から設定したパス
ワードを入力し、[次へ(N)]
をクリックします。



- ⑥ アップデートが完了すると右の画面が表示されます。
[完了(F)]ボタンをクリックします。



お使いのパソコンによっては右の画面が表示される場合があります。その場合はパソコンを再起動してください。再起動せずにパソコンを使用すると、パソコンが不安定になることがあります。



以上でアップデートは完了です。

2.5 以前のバージョンからのサイレントアップデートについて

以下に、サイレントアップデートの手順を示します。

重要

パスワード代替入力機能のサポートは終了しました。
本バージョンにアップデートすると、パスワード代替入力機能は、お使いの PC から削除されます。

- ① [管理者として実行(A)]を指定し、コマンドプロンプトを起動してください。
- ② カレントディレクトリをインストールプログラムが格納されている場所に移動します。

下記コマンドを実行します。(32 ビット OS の場合は「x86」フォルダに収録されている「setup_x86.exe」、64 ビット OS の場合は「x64」フォルダに収録されている「setup_x64.exe」を使用してください。)

なお、手順の中で使用する「△」は、半角スペースを示します。

<32 ビット OS の場合>

```
> setup_x86.exe△/s△/v"/qn"
```

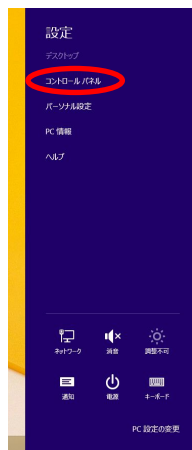
<64 ビット OS の場合>

```
> setup_x64.exe△/s△/v"/qn"
```

2.6 ドライバインストールの確認

2.6.1 Windows Server 2012 / Windows 8.1 / Windows Server 2012 R2 をお使いの場合

- ① 「設定」チャームを表示して、「コントロール パネル」をクリックします。



- ② [デバイスとプリンターの表示]をクリックします。



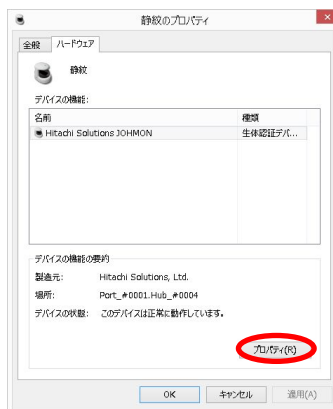
- ③ デバイスとプリンター画面が表示されます。画面内に表示されている[静紋]アイコンをダブルクリックします。



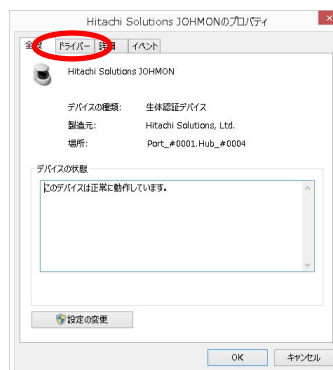
- ④ デバイスのプロパティ画面が表示されます。画面上部の[ハードウェア]タブをクリックします。



- ⑤ 右の画面が表示されたら、[プロパティ (R)] をクリックします。

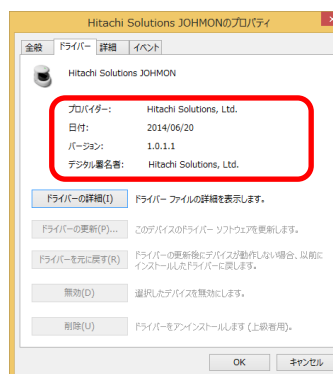


- ⑥ ドライバのプロパティ画面が表示されます。[ドライバー] タブをクリックします。

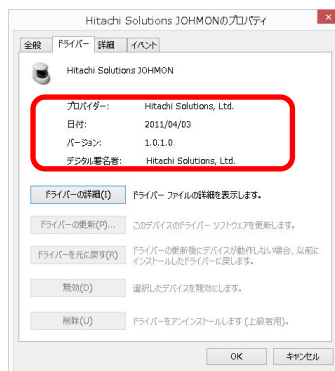


- ⑦ 以下の項目を確認します。

・32 ビット OS をお使いの場合
[プロバイダー] が [Hitachi Solutions, Ltd]
[日付] が [2014/06/20]
[バージョン] が [1. 0. 1. 1]

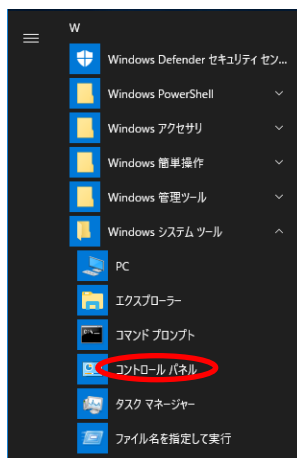


・64 ビット OS をお使いの場合
 [プロバイダー] が [Hitachi
 Solutions,
 Ltd.]
 [日付] が [2011/04/03]
 [バージョン] が [1.0.1.0]

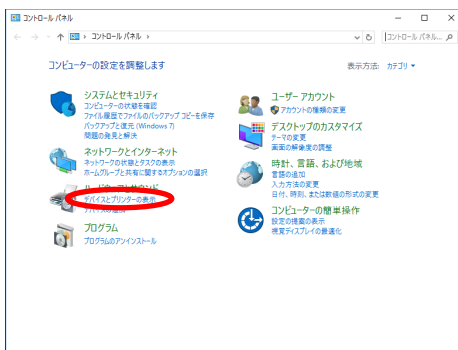


2.6.2 Windows 10 / Windows Server 2016 / Windows Server 2019 / Windows 11 をお使いの場合

- ① 画面左下のスタートメニューをクリックして、開いたメニューから [Windows システム ツール] を展開し、[コントロール パネル] をクリックします。



- ② [デバイスとプリンターの表示]をクリックします。



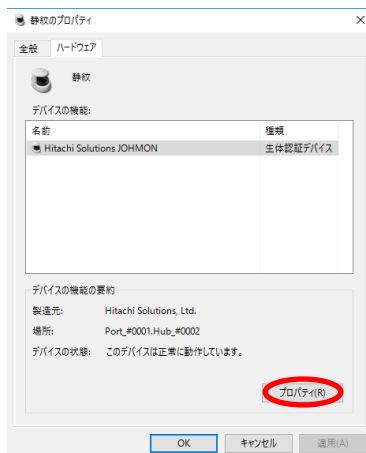
- ③ デバイスとプリンター画面が表示されます。画面内に表示されている[静紋]アイコンをダブルクリックします。



- ④ デバイスのプロパティ画面が表示されます。画面上部の[ハードウェア]タブをクリックします。



- ⑤ 右の画面が表示されたら、[プロパティ(R)] をクリックします。

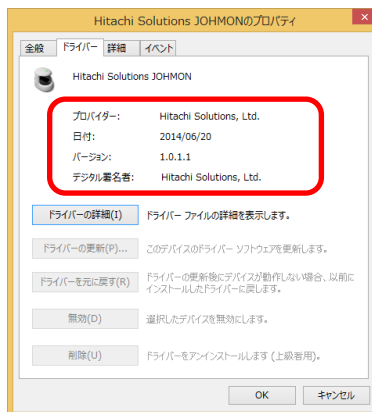


- ⑥ ドライバのプロパティ画面が表示されます。[ドライバー] タブをクリックします。

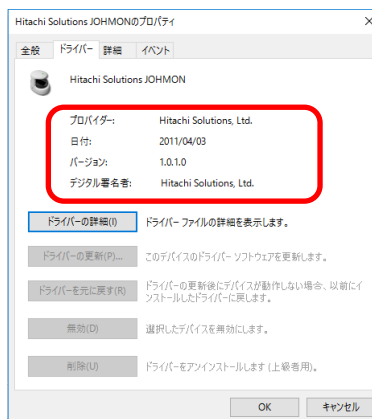


⑦ 以下の項目を確認します。

・32 ビット OS をお使いの場合
[プロバイダー]が[Hitachi
Solutions, Ltd]
[日付]が[2014/06/20]
[バージョン]が[1.0.1.1]



・64 ビット OS をお使いの場合
[プロバイダー]が[Hitachi
Solutions,
Ltd.]
[日付]が[2011/04/03]
[バージョン]が[1.0.1.0]



3 初回時管理者登録

指静脈認証ソフトウェアのインストール完了時に「今すぐ管理者の登録(推奨)」をチェックした場合や、ユーザー管理機能の初回起動時に管理者登録画面が表示されます。ユーザー管理機能の起動方法に関しては「6 ユーザー管理機能」を参照してください。

[Step1] 指情報の登録

[Step1] では管理者登録に必要な情報の入力、登録する指の部位を決定します。

- ① 以下の画面が表示されます。

ユーザー情報

現在 Windows にログオン中のユーザー情報が表示されます。お使いのパソコンが Active Directory 環境下にある場合は、ユーザー情報の項目に「DNS 形式でログオン」のチェックボックスが表示されます。「DNS 形式でログオン」のチェックボックスにチェックを行うことにより「ログオン先」のダイアログボックスが DNS 形式に変更されます。

初回時管理者登録では登録者名以外のユーザー情報を変更することはできません。ユーザー情報が管理者として登録を行いたいユーザーと異なる場合は、登録を行いたいユーザーでWindows にログオンし直してください。

登録者名には、後の管理を容易にするために指情報の登録を行う方の氏名を入力することをお勧めします。最大で全角/半角共に 20 文字までの情報を入力できます。

重要

- 「@」が含まれているユーザーアカウントで初回時管理者登録を実行した場合、初回時管理者登録を正しく行うことができません。(Microsoft アカウントを除く)
- [DNS 形式でログオン] をチェックした場合、[ログオン先] ダイアログボックスには、現在ログオンしているアカウントが実際に登録されているドメインが表示されます。例えば、子ドメインにアカウントを作成し、その子ドメインと信頼関係を結んでいる親ドメインをログオン先としてログオンしている場合でも、表示されるのは子ドメイン側の DNS 名となります。
- 登録するユーザーは、あらかじめ Windows パスワードが設定されている必要があります。
- DomainAdmins グローバルグループは Administrators ローカルグループに所属している必要があります。デフォルトで所属しているため、削除しないようにしてください。
- ローカルグループに所属していないユーザーを管理者として登録する場合は、このユーザーはドメインのアカウントで Windows へログオンしておく必要があります。
- Microsoft アカウントを登録した場合、ログオン先にメールアドレスの「@」より後の文字列が設定されます。

パスワード

- Windows 用パスワードは登録するユーザーに設定されている Windows 用パスワードを入力します。127 文字まで入力することができます。
- 緊急用パスワードは認証装置を使わずにログオンする場合に使用します。Windows 用のパスワードと同じにする必要はありません。また、緊急用パスワードは本製品におけるすべての管理者に共通です。127 文字まで入力することができます。

指の部位

登録する指の部位を指定します。爪の部分をクリックすることにより登録する指を指定します。指の部位は初期設定では**右手中指**となっています。

認証方式

認証方式を変更することができます。認証方式には、「静紋」認証方式と「ID と静紋」認証方式の二つの認証方式を選ぶことができます。それぞれの認証方式の特徴は次の通りです。

- 静紋認証方式(1:N 認証方式)
登録した全ての指静脈の中から比較して本人を特定します。
- ID と静紋認証方式(1:1 認証方式)
予め本人を特定するためのユーザー ID を入力し、ユーザー ID に登録されている指静脈と比較して本人を特定します。この認証方式を選択した場合は、認証のセキュリティレベル(認証のしやすさ)を変更できます。

ID と静紋認証方式を利用する場合は「1:1 認証を利用可能とする」にチェックを入れます。

チェックを入れた場合、「セキュリティレベル」が選択できるようになります。セキュリティレベルを変更することで、認証のしやすさを 5 段階で変えることができます。

重要

- セキュリティレベルは「高」へ近づけるに従い、より厳しく認証を行います。他人を受け入れづらくなりますが、本人も認証しにくくなる場合があります。

備考

認証に必要な情報ではありません。最大で全角/半角共に 50 文字までの情報を入力できます。

- ② Windows 用パスワード、緊急用パスワード、緊急用パスワード（確認）を入力し、指の部位を選択します。必要に応じて認証方式、備考欄に入力し、[撮影開始(S)] ボタンをクリックします。

緊急用のパスワードについては、本書「8 緊急用パスワードの利用」を参照してください。

初回時管理者登録

Step 1: 指情報の登録 Step 2: 緊急用パスワード Step 3: 緊急用パスワード(確認) Step 4: 緊急用パスワード(確認) Step 5: 登録結果

初回時管理者登録

1. ユーザー情報

登録者名(R) johnson

ユーザー(U) johnson

ログオン先(L) V014-1554, 8187Cのユーザー

ユーザーの増減(A) 管理者

2. パスワード

Windows用(P) ●●●●●●

緊急用(E) ●●●●●●

緊急用確認(V) ●●●●●●

緊急用(パスワード)は文字以上、英大文字・英小文字・数字・記号をそれぞれ文字は使用してはならない

3. 指の部位

左手 右手

4. 認証方式

☒ 1 認証を使用可能とする(I)

セキュリティレベル(T) 中

備考(B)

撮影開始(S) キャンセル

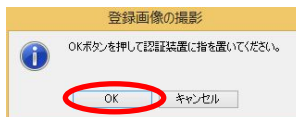
重要

- 緊急用パスワードは以下の条件を満たす必要があります。
 - 6 文字以上であること
 - 英大文字、英小文字、数値を少なくともそれぞれ 1 文字以上使用すること
- 緊急用パスワードは重要ですので、お忘れのないよう管理してください。もし忘れてしまった場合はお使いのパソコンが利用できなくなる場合があります。
- 撮影中は認証装置の認証ゾーンに指以外のものを登録しないでください。誤動作の原因となる場合があります。
- 本製品は生体情報を利用しているため健康状態により登録や認証に失敗することがあります。
- ユーザー名とログオン先を同名に設定できません。

[Step2]～[Step4] 静脈撮影

[Step1] で入力した情報を元に管理者権限を持つ指を撮影します。[Step2] ～ [Step4] まで撮影は3回行われます。

- ① 右の画面が表示されます。[OK] ボタンをクリックするか、[Enter] キーを押下します。



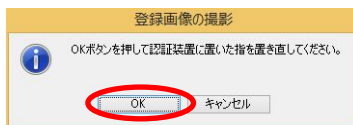
- ② 画面の指示に従い、認証装置に指を置きます。



重要

- ・ 乳幼児や極端に指が細い方(指の幅が 10mm 未満)、太い方(指の幅が 25mm 以上)、指が短い方(指が認証ゾーンの先まで届かない方)は、指の登録や認証に失敗する場合があります。
- ・ 認証ができなくなった場合(成長期の子供で指の状態が変わる場合等)は、下記の手順に従い指情報を再度登録してください。
 1. 該当の指情報を削除する。指情報の削除については、「6.4 指情報の削除」を参照してください。
 2. 再度「指情報の追加」を行う。指情報の追加については、「6.2 指情報の追加」を参照してください。
- ・ 認証装置の認証ゾーンに指以外のものを置かないでください。誤動作の原因となる場合があります。
- ・ 撮影中は認証装置の接続を切断しないでください。
- ・ 撮影中や指を認証装置に置いているときにはお使いのパソコンをロック、ログオフ、シャットダウン、スリープ状態、休止状態、スタンバイ状態にしないでください。システムが不安定になる場合があります。

- ③ 「ピッ」というピープ音が鳴り、右の画面が表示されれば撮影成功です。指を離して [OK] ボタンをクリックするか、[Enter] キーを押下します。「ピーー」というピープ音が鳴り、状態表示 LED が赤の点灯に変わり、エラー画面が表示されれば撮影失敗です。10 秒以内に撮影が終わらない場合もピープ音が鳴り、エラー画面が表示されます。
- ピープ音と状態表示 LED については「取扱説明書 ハードウェア編」の「2.1 認証装置の各部の名称と機能」を参照してください。
- また、正しく登録を行えない場合は本書巻末の「14 トラブルシューティング」を参照してください。
- 認証装置のピープ音の設定を [OFF] にしている場合は、ピープ音は鳴りません。ピープ音の設定方法については「6.9 ピープ音の ON/OFF」を参照してください。
- ④ 指静脈撮影は正確な情報を得るために 3 回行われます。③の画面が表示されるので、あと 2 回の撮影を行います。



重要

- ・ 撮影時には必ず指を置き直してください(一度、認証ゾーンから指を抜き、再度、指を認証ゾーンに置いて下さい)。置き直しをしないと正しく認証されない場合があります。

[Step5] 登録結果

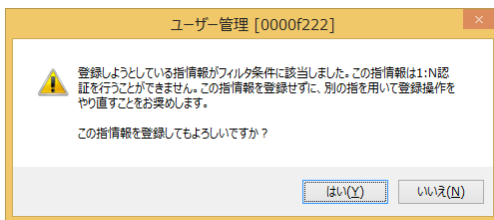
[Step2] ～ [Step4]で撮影した情報を元にシステムに指情報の登録を行います。

- ① 3回の撮影に成功すると、右の画面が表示されます。
[OK] ボタンをクリックするか、[Enter] キーを押下します。撮影に失敗した場合は本書巻末の「14 トラブルシューティング」を参照してください。



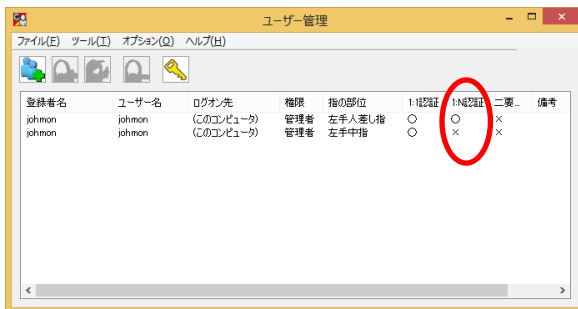
重要

3回の撮影に成功した後に以下の画面が表示されることがあります。



この画面で「はい」をクリックして登録を続行した場合、その指は1:N認証では使用できず、1:1認証でしか使用することができなくなります。1:N認証をお使いになる場合は、必ず「いいえ」をクリックして登録をやり直してください。

登録されている指が1:N認証に使用できるかどうかはユーザー管理画面で確認できます(「1:N認証」が「○」ならば1:N認証に使用できます)。



- ② [ユーザー管理画面]が表示されますので、「6 ユーザー管理機能」を参照してください。
- ③ Windows のログオフ/再起動後、認証画面になりますので、本書「5 認証機能」を参照してWindows へログオンしてください。ログオン後に、インストールされている全ての機能が利用可能になります。

重要

指のけがなどにより、指静脈による認証が行えなくなる場合がありますので、複数の指を登録して運用してください。複数の指の登録方法については本書「6.2 指情報の追加」をご覧ください。

4 ソフトウェアのアンインストール

インストールおよびアンインストールはお使いのパソコンの Administrators グループに属するユーザーで行ってください。

重要

- ・ アンインストール中はお使いのパソコンをロック、ログオフ、シャットダウン、スリープ状態、休止状態、スタンバイ状態にしないでください。いずれかの状態からの復帰後にシステムが不安定になる場合があります。
- ・ アンインストールすると登録されている指情報がすべて削除されます。

4.1 指静脈認証ソフトウェアのアンインストール

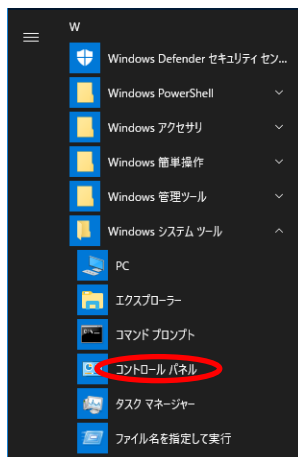
以下に、アンインストールの手順を示します。

- ① ・ Windows Server 2012 / Windows 8.1 / Windows Server 2012 R2 をお使いの場合
[設定] チャームを表示して、[コントロール パネル] をクリックします。



・Windows 10 / Windows Server 2016 / Windows Server 2019 / Windows 11 をお使いの場合

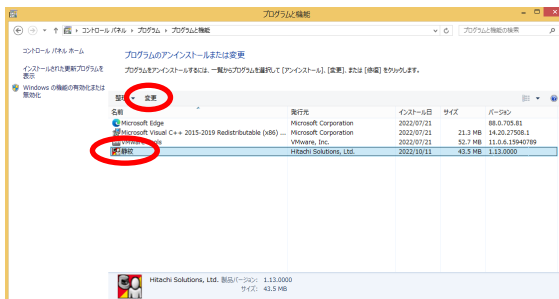
画面左下のスタートメニューをクリックして、開いたメニューから[Windows システム ツール]を展開し、[コントロール パネル]をクリックします。



- ② [プログラム]の[プログラムのアンインストール]をクリックします。



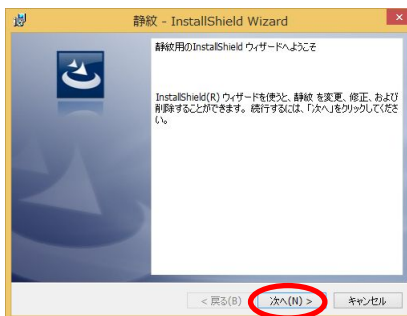
- ③ インストールされているプログラムが表示されます。
[静紋]を選択し、
[変更]ボタンをクリックします。



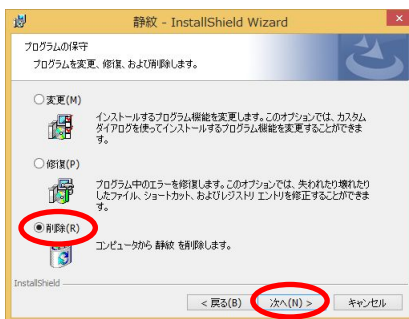
- ④ アンインストール用パスワードを設定している場合にはパスワード入力ダイアログが表示されます。ユーザー管理機能から設定したパスワードを入力し、[次へ(N)]をクリックします。



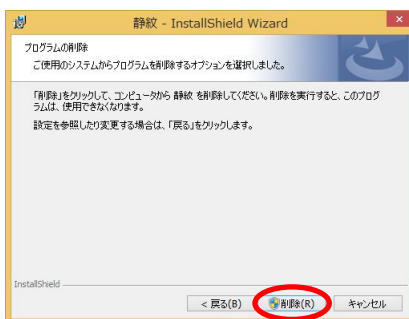
- ⑤ 右の画面が表示されます。[次へ(N)]ボタンをクリックします。



- ⑥ 右の画面が表示されます。「削除(R)」を選択し、「次へ(N)」ボタンをクリックします。



- ⑦ 右の画面が表示されます。「削除(R)」ボタンをクリックするとアンインストール処理を開始します。



- ⑧ アンインストールに成功すると右の画面が表示されます。「完了(F)」をクリックします。



お使いのパソコンによっては、右の画面が表示される場合があります。この画面で[はい(Y)]をクリックすると自動的にパソコンを再起動します。[いいえ(N)]をクリックするとインストールをいったん終了しますが、手でパソコンを再起動するまでアンインストールが完了しない状態になります。



この画面が表示された場合は、いずれかの方法でパソコンを再起動してください。

以上でアンインストールは完了です。

重要

- アンインストールをコントロールパネルから行った場合、新規インストール時に自動的に作成された「他のユーザー」というユーザーが削除されずに残る場合があります。その場合、[コントロールパネル]の[ユーザーアカウント]から手動で削除してください。
- Windows 10 / Windows Server 2016 / Windows Server 2019 / Windows 11 において、Windows の[設定]の[アプリと機能]からはアンインストールできません。

4.2 指静脈認証ソフトウェアのサイレントアンインストール

以下に、サイレントアンインストールの手順を示します。

- ① [管理者として実行(A)]を指定し、コマンドプロンプトを起動してください。
- ② カレントディレクトリをインストールプログラムが格納されている場所に移動します。
- ③ 下記コマンドを実行します。(32 ビット OS の場合は「x86」フォルダに収録されている「setup_x86.exe」、64 ビット OS の場合は「x64」フォルダに収録されている「setup_x64.exe」を使用してください。)。
なお、手順の中で使用する「△」は、半角スペースを示します。

<32 ビット OS の場合>

```
> setup_x86.exe△/s△/v"/qn△REMOVE=ALL"
```

<64 ビット OS の場合>

```
> setup_x64.exe△/s△/v"/qn△REMOVE=ALL"
```

5 認証機能

本製品は、指の静脈を撮影することにより個人認証を行う「バイオメトリクス（生体認証）」のシステムであり、認証装置、および指静脈認証ソフトウェアから構成されます。認証機能では、次の機能を提供します。

- Windows のログオンマネージャに対する指静脈を用いた認証機能
（お使いのパソコンへのローカルログオン機能、Windows ドメインへのログオン機能）
- Windows スクリーンセーバーのロック解除に対する指静脈を用いた認証機能
認証方式には、「静紋」認証方式、「ID と静紋」認証方式の二つの認証方式を選ぶことができます。それぞれの認証方式の特徴は次の通りです。
 - 静紋認証方式(1:N 認証方式)
登録した全ての指静脈の中から比較して本人を特定します。
 - ID と静紋認証方式(1:1 認証方式)
予め本人を特定するためのユーザーID を入力し、ユーザーID に登録されている指静脈と比較して本人を特定します。

また、二要素認証を有効にすることで、1:N 認証方式の認証として「静紋と二要素用パスワード」認証、1:1 認証方式の認証として「ID と静紋と二要素用パスワード」認証、「ID と静紋と Windows パスワード」認証を使用できます。二要素用パスワードとは、ユーザー管理機能が独自に管理するパスワードです。それぞれの認証の特徴は次の通りです。

- 静紋と二要素用パスワード認証(1:N 認証方式)
登録した全ての指静脈と二要素用パスワードの中から比較して本人を特定します。
- ID と静紋と二要素用パスワード認証(1:1 認証方式)
予め本人を特定するためのユーザーID を入力し、ユーザーID に登録されている指静脈と二要素用パスワードと比較して本人を特定します。
- ID と静紋と Windows パスワード認証(1:1 認証方式)
予め本人を特定するためのユーザーID と Windows パスワードを入力し、ユーザーID に登録されている指静脈と比較して本人を特定します。本認証はユーザー管理機能で登録した Windows パスワードを使用せず、入力した Windows パスワードで認証を行います。Windows ログオン時およびスクリーンセーバーのロック解除時のみ使用可能です。

重要

- ・ 乳幼児や極端に指が細い方(指の幅が 10mm 未満)、太い方(指の幅が 25mm 以上)、指が短い方(指が認証ゾーンの先まで届かない方)は、指の登録や認証に失敗する場合があります。
- ・ 認証ができにくくなった場合(成長期の子供で指の状態が変わる場合等)は、下記の手順に従い指情報を再度登録してください。
 1. 該当の指情報を削除する。指情報の削除については、「6.4 指情報の削除」を参照してください。
 2. 再度「指情報の追加」を行う。指情報の追加については、「6.2 指情報の追加」を参照してください。
- ・ 認証装置の認証ゾーンに指以外のものを置かないでください。誤動作の原因となる場合があります。
- ・ 撮影中は認証装置の接続を切断しないでください。
- ・ 撮影中や認証装置に指を置いているときには、お使いのパソコンをロック、ログオフ、シャットダウン、スリープ状態、休止状態、スタンバイ状態にしないでください。システムが不安定になる場合があります。
- ・ 1:1 認証方式の認証において、Active Directory の環境下でご使用になる場合、以下のいずれかの方法で認証を行ってください。
 - ・ ユーザプリンシパル名 (UPN) 形式を使用せずに (ユーザーID とログオン先の入力を分けて) ユーザー登録を行い、そのユーザーID で認証を行ってください。
 - ・ ユーザプリンシパル名 (UPN) 形式で登録したユーザーID を使用する場合、ログオン画面の「他のユーザー」のアイコンからユーザーID を入力して認証を行ってください。

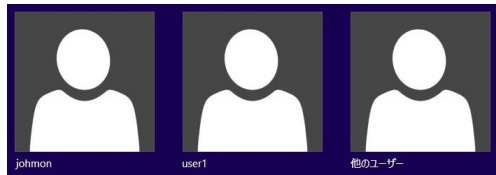
5.1 Windows ログオン（静紋認証の場合）

5.1.1 Windows Server 2012 / Windows 8.1 / Windows Server 2012 R2 をお使いの場合

- ① Windows 起動時に右の画面が表示されます。
(Windows のセキュリティポリシー設定で「対話型ログオン: Ctrl+Alt+Del を必要としない」を「有効」に設定している場合は表示されません)



- ② [Ctrl] キーと [Alt] キーと [Delete] キーを同時に押下すると右の画面が表示されます。
(コンピュータの設定によっては右の画面から表示されます。)



右の画面にはユーザーの一覧画面が表示されます。

なお、前回のログオン方法によっては、ユーザーの一覧画面が表示されず、ユーザーが選択された画面が表示されることがあります。そのユーザーでログオンしない場合は「←」ボタンをクリックして、ユーザー一覧画面に戻ってください。

- ③ 「他のユーザー」を選択すると、右の画面が表示されます。



- ④ [→]ボタンをクリックすると右の撮影画面が表示され、状態表示LEDが緑の点滅をします。ログオンするユーザーの指を認証装置に置きます。



重要

- ・ 認証中は認証装置の接続を切断しないでください。
- ・ 認証中はお使いのパソコンをロック、ログオフ、シャットダウン、スリープ状態、休止状態、スタンバイ状態にしないでください。いずれかの状態からの復帰後に正しい認証が行われず、システムが不安定になる場合があります。

- ⑤ 「ピピッ」というビープ音が鳴り、状態表示 LED が緑の点灯に変われば認証成功です。

「ピーー」というビープ音が鳴り、状態表示 LED が赤の点灯に変われば認証失敗です（一瞬赤が点灯し、すぐに緑の点灯に変わります）。

撮影画面において 10 秒以内に撮影が終わらない場合もビープ音が鳴りエラー画面が表示されます。

ビープ音と状態表示 LED については「取扱説明書 ハードウェア編」の「2.1 認証装置の各部の名称と機能」を参照してください。

また、正しく認証を行えない場合は本書巻末の「14 トラブルシューティング」を参照してください。

認証装置のビープ音の設定を [OFF] にしている場合は、ビープ音は鳴りません。ビープ音の設定方法については本書「6.9 ビープ音の ON/OFF」を参照してください。

重要

- ・ 認証に連続 10 回失敗すると、5 分間認証を受け付けません。
- ・ ②もしくは③の画面で [シャットダウン] ボタンを無効にしたい場合は、Windows のセキュリティポリシー設定で「シャットダウン: システムをシャットダウンするのにログオンを必要としない」を「無効」にしてください。

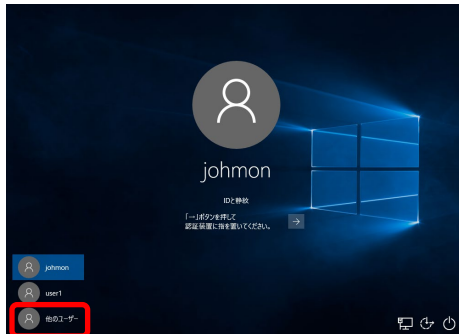
5.1.2 Windows 10 / Windows Server 2016 / Windows Server 2019 / Windows 11

をお使いの場合

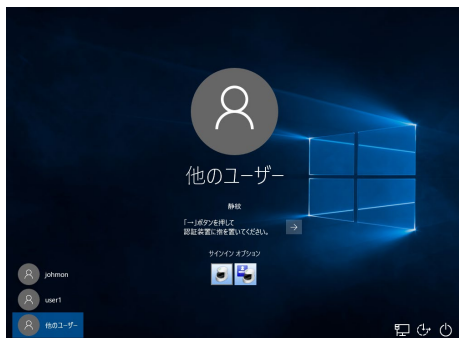
- ① Windows 起動時に右の画面が表示されます。
(Windows のセキュリティポリシー設定で「対話型ログオン: Ctrl+Alt+Del を必要としない」を「有効」に設定している場合は表示されません)



- ② [Ctrl] キーと [Alt] キーと [Delete] キーを同時に押下すると右の画面が表示されます。
(コンピュータの設定によっては右の画面から表示されます。)
左のユーザー一覧から[他のユーザー]をクリックします。



- ③ 右の画面が表示されます。



- ④ [→] ボタンをクリックすると右の撮影画面が表示され、状態表示 LED が緑の点滅をします。ログオンするユーザーの指を認証装置に置きます。



重要

- ・ 認証中は認証装置の接続を切断しないでください。
- ・ 認証中はお使いのパソコンをロック、ログオフ、シャットダウン、スリープ状態、休止状態、スタンバイ状態にしないでください。いずれかの状態からの復帰後に正しい認証が行われず、システムが不安定になる場合があります。

- ⑤ 「ピピッ」というビープ音が鳴り、状態表示 LED が緑の点灯に変われば認証成功です。

「ピピー」というビープ音が鳴り、状態表示 LED が赤の点灯に変われば認証失敗です（一瞬赤が点灯し、すぐに緑の点灯に変わります）。

撮影画面において 10 秒以内に撮影が終わらない場合もビープ音が鳴りエラー画面が表示されます。

ビープ音と状態表示 LED については「取扱説明書 ハードウェア編」の「2.1 認証装置の各部の名称と機能」を参照してください。

また、正しく認証を行えない場合は本書巻末の「14 トラブルシューティング」を参照してください。

認証装置のビープ音の設定を [OFF] にしている場合は、ビープ音は鳴りません。ビープ音の設定方法については本書「6.9 ビープ音の ON/OFF」を参照してください。

重要

- ・ 認証に連続 10 回失敗すると、5 分間認証を受け付けません。
- ・ ②もしくは③の画面で [シャットダウン] ボタンを無効にしたい場合は、Windows のセキュリティポリシー設定で「シャットダウン: システムのシャットダウンにログオンを必要としない」を「無効」にしてください。

5.2 Windows ログオン（ID と静紋認証の場合）

5.2.1 Windows Server 2012 / Windows 8.1 / Windows Server 2012 R2 をお使いの場合

- ① Windows 起動時に右の画面が表示されます。
(Windows のセキュリティポリシー設定で「対話型ログオン: Ctrl+Alt+Del を必要としない」を「有効」に設定している場合は表示されません)



- ② [Ctrl] キーと [Alt] キーと [Delete] キーを同時に押下すると右の画面が表示されます。
(ユーザーの設定によっては右の画面から表示されます。)



右の画面にはユーザーの一覧画面が表示されます。

なお、前回のログオン方法によっては、ユーザーの一覧画面が表示されず、ユーザーが選択された画面が表示されることがあります。そのユーザーでログオンしない場合は「←」ボタンをクリックして、ユーザー一覧画面に戻ってください。

- ③ ログオンするユーザーを選択すると、右の画面が表示されます。



ユーザー一覧画面にログオンしたいユーザーがない場合、「他のユーザー」を選

択し、サインインオプションでをクリックした後に、ログオンしたいユーザー名を入力してください。



- ④ [→] ボタンをクリックすると右の撮影画面が表示され、状態表示LEDが緑の点滅をします。ログオンするユーザーの指を認証装置に置きます。



- ⑤ 「ビピッ」というビープ音が鳴り、状態表示 LED が緑の点灯に変われば認証成功です。
- 「ビピー」というビープ音が鳴り、状態表示 LED が赤の点灯に変われば認証失敗です（一瞬赤が点灯し、すぐに緑の点灯に変わります）。
- 撮影画面において 10 秒以内に撮影が終わらない場合もビープ音が鳴りエラー画面が表示されます。
- ビープ音と状態表示 LED については「取扱説明書 ハードウェア編」の「2.1 認証装置の各部の名称と機能」を参照してください。

また、正しく認証を行えない場合は本書巻末の「14 トラブルシューティング」を参照してください。

認証装置のビープ音の設定を [OFF] にしている場合は、ビープ音は鳴りません。ビープ音の設定方法については「6.9 ビープ音の ON/OFF」を参照してください。

重要

- ・ 認証に連続 10 回失敗すると、5 分間認証を受け付けません。
- ・ ②もしくは③の画面で [シャットダウン] ボタンを無効にしたい場合は、Windows のセキュリティポリシー設定で「シャットダウン: システムをシャットダウンするのにログオンを必要としない」を「無効」にしてください。

5.2.2 Windows 10 / Windows Server 2016 / Windows Server 2019 / Windows 11

をお使いの場合

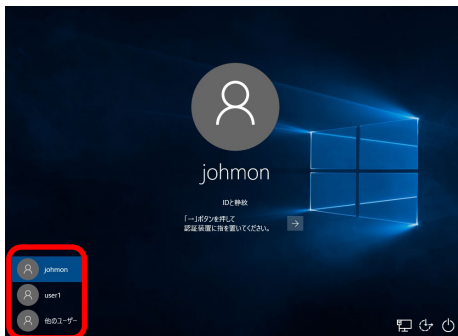
- ① Windows 起動時に右の画面が表示されます。
- (Windows のセキュリティポリシー設定で「対話型ログオン: Ctrl+Alt+Del を必要としない」を「有効」に設定している場合は表示されません)



- ② [Ctrl] キーと [Alt] キーと [Delete] キーを同時に押下すると右の画面が表示されます。

(コンピュータの設定によっては右の画面から表示されます。)

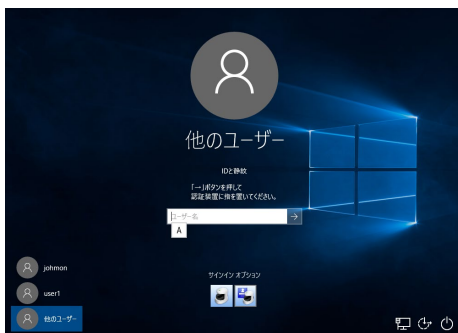
表示されたユーザーでログオンしない場合、左のユーザー一覧からユーザーを選択します。



ユーザー一覧にログオンしたいユーザーがない場合、「他のユーザー」を選択し、サインインオプションで



をクリックした後に、ログオンしたいユーザー名を入力してください。



なお、前回のログオン方法によっては、はじめに「他のユーザー」が選択された画面が表示されることがあります。

- ③ [一] ボタンをクリックすると右の撮影画面が表示され、状態表示 LED が緑の点滅をします。ログオンするユーザーの指を認証装置に置きます。



- ④ 「ピピッ」というビープ音が鳴り、状態表示 LED が緑の点灯に変われば認証成功です。
- 「ピーー」というビープ音が鳴り、状態表示 LED が赤の点灯に変われば認証失敗です（一瞬赤が点灯し、すぐに緑の点灯に変わります）。
- 撮影画面において 10 秒以内に撮影が終わらない場合もビープ音が鳴りエラー画面が表示されます。
- ビープ音と状態表示 LED については「取扱説明書 ハードウェア編」の「2.1 認証装置の各部の名称と機能」を参照してください。

また、正しく認証を行えない場合は本書巻末の「14 トラブルシューティング」を参照してください。

認証装置のビープ音の設定を [OFF] にしている場合は、ビープ音は鳴りません。ビープ音の設定方法については「6.9 ビープ音の ON/OFF」を参照してください。

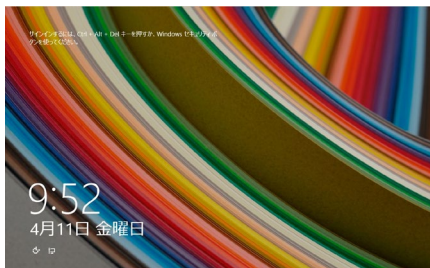
重要

- ・ 認証に連続 10 回失敗すると、5 分間認証を受け付けません。
- ・ ②の画面で [シャットダウン] ボタンを無効にしたい場合は、Windows のセキュリティポリシー設定で「シャットダウン: システムのシャットダウンにログオンを必要としない」を「無効」にしてください。

5.3 Windows ログオン（静紋と二要素用パスワード認証の場合）

5.3.1 Windows Server 2012 / Windows 8.1 / Windows Server 2012 R2 をお使いの場合

- ① Windows 起動時に右の画面が表示されます。
(Windows のセキュリティポリシー設定で「対話型ログオン: Ctrl+Alt+Del を必要としない」を「有効」に設定している場合は表示されません)



- ② [Ctrl] キーと [Alt] キーと [Delete] キーを同時に押下すると右の画面が表示されます。
(コンピュータの設定によっては右の画面から表示されます。)



右の画面にはユーザーの一覧画面が表示されます。

なお、前回のログオン方法によっては、ユーザーの一覧画面が表示されず、ユーザーが選択された画面が表示されることがあります。そのユーザーでログオンしない場合は「←」ボタンをクリックして、ユーザー一覧画面に戻ってください。

- ③ 「他のユーザー」を選択すると、右の画面が表示されます。



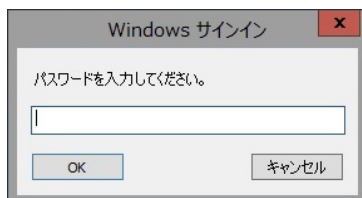
- ④ [→]ボタンをクリックすると右の撮影画面が表示され、状態表示LEDが緑の点滅をします。ログオンするユーザーの指を認証装置に置きます。



重要

- ・ 認証中は認証装置の接続を切断しないでください。
- ・ 認証中はお使いのパソコンをロック、ログオフ、シャットダウン、スリープ状態、休止状態、スタンバイ状態にしないでください。いずれかの状態からの復帰後に正しい認証が行われず、システムが不安定になる場合があります。

- ⑤ 右のパスワード入力画面が表示されるので、二要素用パスワードを入力し[OK]ボタンをクリックします。



- ⑥ 「ビピッ」というビープ音が鳴り、状態表示 LED が緑の点灯に変われば認証成功です。
「ビピー」というビープ音が鳴り、状態表示 LED が赤の点灯に変われば認証失敗です（一瞬赤が点灯し、すぐに緑の点灯に変わります）。
撮影画面において 10 秒以内に撮影が終わらない場合もビープ音が鳴りエラー画面が表示されます。
ビープ音と状態表示 LED については「取扱説明書 ハードウェア編」の「2.1 認証装置の各部の名称と機能」を参照してください。
また、正しく認証を行えない場合は本書巻末の「14 トラブルシューティング」を参照してください。

認証装置のビープ音の設定を [OFF] にしている場合は、ビープ音は鳴りません。ビープ音の設定方法については本書「6.9 ビープ音の ON/OFF」を参照してください。

重要

- 認証に連続 10 回失敗すると、5 分間認証を受け付けません。
- ②もしくは③の画面で [シャットダウン] ボタンを無効にしたい場合は、Windows のセキュリティポリシー設定で「シャットダウン: システムをシャットダウンするのにログオンを必要としない」を「無効」にしてください。

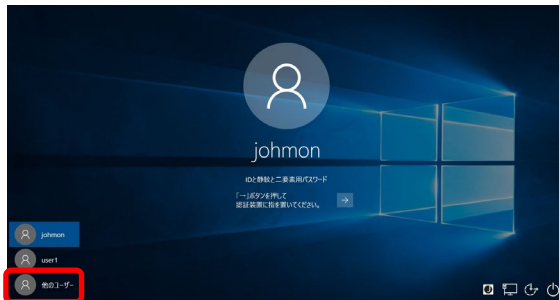
5.3.2 Windows 10 / Windows Server 2016 / Windows Server 2019 / Windows 11

をお使いの場合

- ① Windows 起動時に右の画面が表示されます。
(Windows のセキュリティポリシー設定で「対話型ログイン: Ctrl+Alt+Del を必要としない」を「有効」に設定している場合は表示されません)

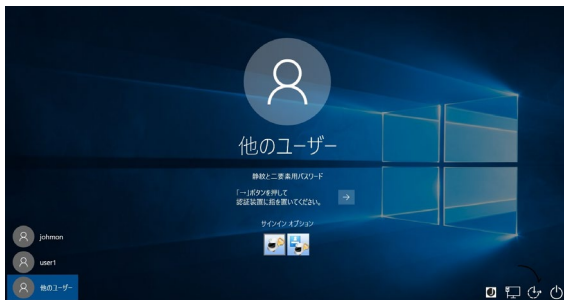


- ② [Ctrl] キーと [Alt] キーと [Delete] キーを同時に押下すると右の画面が表示されます。
(コンピュータの設定によっては右の画面から表示されます。)



左のユーザー一覧から[他のユーザー]をクリックします。

- ③ 右の画面が表示されます。



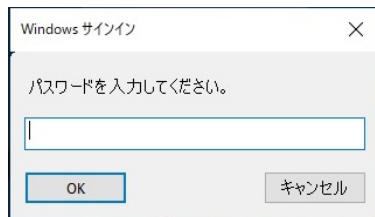
- ④ [→] ボタンをクリックすると右の撮影画面が表示され、状態表示 LED が緑の点滅をします。ログオンするユーザーの指を認証装置に置きます。



重要

- ・ 認証中は認証装置の接続を切断しないでください。
- ・ 認証中はお使いのパソコンをロック、ログオフ、シャットダウン、スリープ状態、休止状態、スタンバイ状態にしないでください。いずれかの状態からの復帰後に正しい認証が行われず、システムが不安定になる場合があります。

- ⑤ 右のパスワード入力画面が表示されるので、二要素用パスワードを入力し[OK]ボタンをクリックします。



- ⑥ 「ピピッ」というビープ音が鳴り、状態表示 LED が緑の点灯に変われば認証成功です。
「ピーー」というビープ音が鳴り、状態表示 LED が赤の点灯に変われば認証失敗です（一瞬赤が点灯し、すぐに緑の点灯に変わります）。
撮影画面において 10 秒以内に撮影が終わらない場合もビープ音が鳴りエラー画面が表示されます。
ビープ音と状態表示 LED については「取扱説明書 ハードウェア編」の「2.1 認証装置の各部の名称と機能」を参照してください。
また、正しく認証を行えない場合は本書巻末の「14 トラブルシューティング」を参照してください。

認証装置のビープ音の設定を [OFF] にしている場合は、ビープ音は鳴りませ

ん。ビープ音の設定方法については本書「6.9 ビープ音の ON/OFF」を参照してください。

重要

- 認証に連続 10 回失敗すると、5 分間認証を受け付けません。
- ②もしくは③の画面で [シャットダウン] ボタンを無効にしたい場合は、Windows のセキュリティポリシー設定で「シャットダウン: システムのシャットダウンにログオンを必要としない」を「無効」にしてください。

5.4 Windows ログオン（ID と静紋と二要素用パスワード認証の場合）

5.4.1 Windows Server 2012 / Windows 8.1 / Windows Server 2012 R2 をお使いの場合

- ① Windows 起動時に右の画面が表示されます。
(Windows のセキュリティポリシー設定で「対話型ログオン: Ctrl+Alt+Del を必要としない」を「有効」に設定している場合は表示されません)



- ② [Ctrl]キーと[Alt]キーと[Delete]キーを同時に押下すると右の画面が表示されます。
(ユーザーの設定によっては右の画面から表示されます。)



右の画面にはユーザーの一覧画面が表示されます。

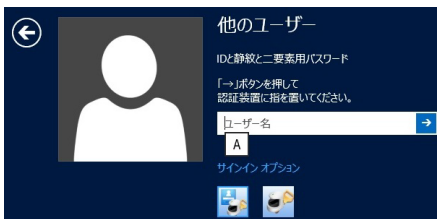
なお、前回のログオン方法によっては、ユーザーの一覧画面が表示されず、ユーザーが選択された画面が表示されることがあります。そのユーザーでログオンしない場合は「←」ボタンをクリックして、ユーザー一覧画面に戻ってください。

- ③ ログオンするユーザーを選択すると、右の画面が表示されます。



ユーザー一覧画面にログオンしたいユーザーがない場合、「他のユーザー」を選択し、サインインオプションで

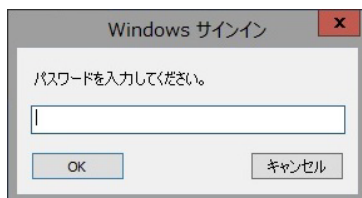
をクリックした後に、ログオンしたいユーザー名を入力してください。



- ④ [→]ボタンをクリックすると右の撮影画面が表示され、状態表示LEDが緑の点滅をします。ログオンするユーザーの指を認証装置に置きます。



- ⑤ 右のパスワード入力画面が表示されるので、二要素用パスワードを入力し[OK]ボタンをクリックします。



- ⑥ 「ピピッ」というビープ音が鳴り、状態表示 LED が緑の点灯に変われば認証成功です。
「ピーー」というビープ音が鳴り、状態表示 LED が赤の点灯に変われば認証失敗です（一瞬赤が点灯し、すぐに緑の点灯に変わります）。
撮影画面において 10 秒以内に撮影が終わらない場合もビープ音が鳴りエラー画面が表示されます。
ビープ音と状態表示 LED については「取扱説明書 ハードウェア編」の「2.1 認証装置の各部の名称と機能」を参照してください。

また、正しく認証を行えない場合は本書巻末の「14 トラブルシューティング」を参照してください。

認証装置のビープ音の設定を [OFF] にしている場合は、ビープ音は鳴りません。ビープ音の設定方法については「6.9 ビープ音の ON/OFF」を参照してください。

重要

- ・ 認証に連続 10 回失敗すると、5 分間認証を受け付けません。
- ・ ②もしくは③の画面で [シャットダウン] ボタンを無効にしたい場合は、Windows のセキュリティポリシー設定で「シャットダウン: システムをシャットダウンするのにログオンを必要としない」を「無効」にしてください。

5.4.2 Windows 10 / Windows Server 2016 / Windows Server 2019 / Windows 11

をお使いの場合

- ① Windows 起動時に右の画面が表示されます。
(Windows のセキュリティポリシー設定で「対話型ログオン: Ctrl+Alt+Del を必要としない」を「有効」に設定している場合は表示されません)



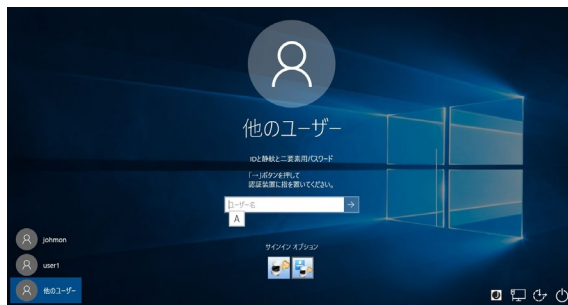
- ② [Ctrl] キーと [Alt] キーと [Delete] キーを同時に押下すると右の画面が表示されます。
(コンピュータの設定によっては右の画面から表示されます。)



表示されたユーザーでログオンしない場合、左のユーザー一覧からユーザーを選択します。

ユーザー一覧にログオンしたいユーザーがない場合、「他のユーザー」を選択し、サインインオプションで

をクリックした後、ログオンし



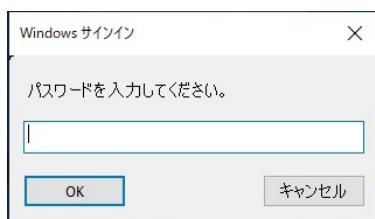
たいユーザー名を入力してください。

なお、前回のログオン方法によっては、はじめに「他のユーザー」が選択された画面が表示されることがあります。

- ③ [→] ボタンをクリックすると右の撮影画面が表示され、状態表示 LED が緑の点滅をします。ログオンするユーザーの指を認証装置に置きます。



- ④ 右のパスワード入力画面が表示されるので、二要素用パスワードを入力し[OK] ボタンをクリックします。



- ⑤ 「ピピッ」というビープ音が鳴り、状態表示 LED が緑の点灯に変われば認証成功です。
「ピーー」というビープ音が鳴り、状態表示 LED が赤の点灯に変われば認証失敗です（一瞬赤が点灯し、すぐに緑の点灯に変わります）。
撮影画面において 10 秒以内に撮影が終わらない場合もビープ音が鳴りエラー画面が表示されます。
ビープ音と状態表示 LED については「取扱説明書 ハードウェア編」の「2.1 認証装置の各部の名称と機能」を参照してください。

また、正しく認証を行えない場合は本書巻末の「14 トラブルシューティング」を参照してください。

認証装置のビープ音の設定を [OFF] にしている場合は、ビープ音は鳴りません。ビープ音の設定方法については「6.9 ビープ音の ON/OFF」を参照してください。

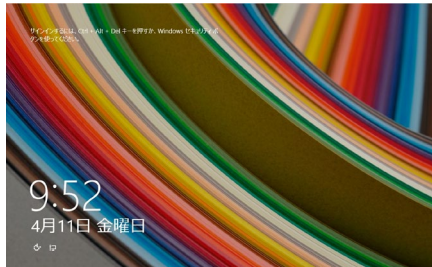
重要

- 認証に連続 10 回失敗すると、5 分間認証を受け付けません。
- ②の画面で [シャットダウン] ボタンを無効にしたい場合は、Windows のセキュリティポリシー設定で「シャットダウン: システムのシャットダウンにログオンを必要としない」を「無効」にしてください。

5.5 Windows ログオン（ID と静紋と Windows パスワード認証の場合）

5.5.1 Windows Server 2012 / Windows 8.1 / Windows Server 2012 R2 をお使いの場合

- ① Windows 起動時に右の画面が表示されます。
(Windows のセキュリティポリシー設定で「対話型ログオン: Ctrl+Alt+Del を必要としない」を「有効」に設定している場合は表示されません)



- ② [Ctrl] キーと [Alt] キーと [Delete] キーを同時に押下すると右の画面が表示されます。
(ユーザーの設定によっては右の画面から表示されます。)



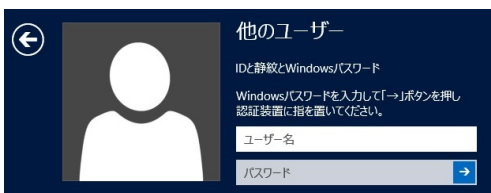
右の画面にはユーザーの一覧画面が表示されます。

なお、前回のログオン方法によっては、ユーザーの一覧画面が表示されず、ユーザーが選択された画面が表示されることがあります。そのユーザーでログオンしない場合は「←」ボタンをクリックして、ユーザー一覧画面に戻ってください。

- ③ ログオンするユーザーを選択すると、右の画面が表示されますので、Windows パスワードを入力します。



ユーザー一覧画面にログオンしたいユーザーがない場合、「他のユーザー」を選択し、ログオンしたいユーザー名と Windows パスワードを入力してください。



- ④ [→] ボタンをクリックすると右の撮影画面が表示され、状態表示 LED が緑の点滅をします。ログオンするユーザーの指を認証装置に置きます。



- ⑤ 「ビピッ」というビープ音が鳴り、状態表示 LED が緑の点灯に変われば認証成功です。
- 「ビピー」というビープ音が鳴り、状態表示 LED が赤の点灯に変われば認証失敗です（一瞬赤が点灯し、すぐに緑の点灯に変わります）。
- 撮影画面において 10 秒以内に撮影が終わらない場合もビープ音が鳴りエラー画面が表示されます。
- ビープ音と状態表示 LED については「取扱説明書 ハードウェア編」の「2.1 認証装置の各部の名称と機能」を参照してください。

また、正しく認証を行えない場合は本書巻末の「14 トラブルシューティング」を参照してください。

認証装置のビープ音の設定を [OFF] にしている場合は、ビープ音は鳴りません。ビープ音の設定方法については「6.9 ビープ音の ON/OFF」を参照してください。

重要

- ・ 認証に連続 10 回失敗すると、5 分間認証を受け付けません。
- ・ ②もしくは③の画面で [シャットダウン] ボタンを無効にしたい場合は、Windows のセキュリティポリシー設定で「シャットダウン：システムをシャットダウンするのにログオンを必要としない」を「無効」にしてください。

5.5.2 Windows 10 / Windows Server 2016 / Windows Server 2019 / Windows 11

をお使いの場合

- ① Windows 起動時に右の画面が表示されます。
(Windows のセキュリティポリシー設定で「対話型ログオン: Ctrl+Alt+Del を必要としない」を「有効」に設定している場合は表示されません)

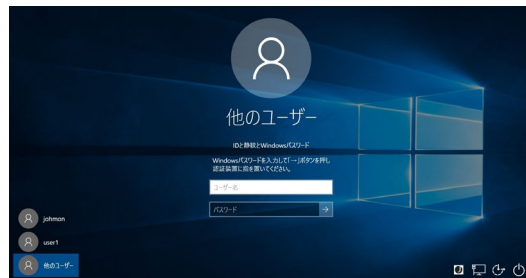


- ② [Ctrl] キーと [Alt] キーと [Delete] キーを同時に押下すると右の画面が表示されます。
(コンピュータの設定によっては右の画面から表示されます。)
表示されたユーザーでログオンしない場合、左のユーザー一覧からユーザーを選択します。



ユーザー一覧にログオンしたいユーザーがない場合、「他のユーザー」を選択し、ログオンしたいユーザー名を入力してください。

なお、前回のログオン方法によっては、はじめに「他のユーザー」が選択された画面が表示されることがあります。



- ③ [→] ボタンをクリックすると右の撮影画面が表示され、状態表示 LED が緑の点滅をします。ログオンするユーザーの指を認証装置に置きます。



- ④ 「ピピッ」というビープ音が鳴り、状態表示 LED が緑の点灯に変われば認証成功です。
「ピーー」というビープ音が鳴り、状態表示 LED が赤の点灯に変われば認証失敗です（一瞬赤が点灯し、すぐに緑の点灯に変わります）。
撮影画面において 10 秒以内に撮影が終わらない場合もビープ音が鳴りエラー画面が表示されます。
ビープ音と状態表示 LED については「取扱説明書 ハードウェア編」の「2.1 認証装置の各部の名称と機能」を参照してください。

また、正しく認証を行えない場合は本書巻末の「14 トラブルシューティング」を参照してください。

認証装置のビープ音の設定を [OFF] にしている場合は、ビープ音は鳴りません。ビープ音の設定方法については「6.9 ビープ音の ON/OFF」を参照してください。

重要

- ・ 認証に連続 10 回失敗すると、5 分間認証を受け付けません。
- ・ ②の画面で [シャットダウン] ボタンを無効にしたい場合は、Windows のセキュリティポリシー設定で「シャットダウン: システムのシャットダウンにログオンを必要としない」を「無効」にしてください。

5.6 スクリーンセーバーロック解除（静紋認証の場合）

5.6.1 Windows Server 2012 / Windows 8.1 / Windows Server 2012 R2 をお使いの場合

- ① スクリーンセーバー起動中に操作を行うと、右の画面が表示されます。
(Windows のセキュリティポリシー設定で「対話型ログオン: Ctrl+Alt+Del を必要としない」を「有効」に設定している場合は表示されません)



- ② [Ctrl] キーと [Alt] キーと [Delete] キーを同時に押下すると右の画面が表示されます。
(ユーザーの設定によっては右の画面から表示されます。) ロックされているユーザーが選択された画面が表示されます。



重要

①または②の画面が表示されない場合は、本書「15.1 スクリーンセーバーの設定について」を参照しパスワードによる保護を有効にしてください。

- ③ [→] ボタンをクリックすると、右の撮影画面が表示され、状態表示LEDが緑の点滅をします。
ログオンしているユーザーの指を認証装置に置きます。



- ④ 「ピピッ」というビープ音が鳴り、状態表示 LED が緑の点灯に変われば認証成功です。

「ビピー」というビープ音が鳴り、状態表示 LED が赤の点灯に変われば認証失敗です（一瞬赤が点灯し、すぐに緑の点灯に変わります）。

撮影画面において 10 秒以内に撮影が終わらない場合もビープ音が鳴りエラー画面が表示されます。

ビープ音と状態表示 LED については「取扱説明書 ハードウェア編」の「2.1 認証装置の各部の名称と機能」を参照してください。

また、正しく認証を行えない場合は本書巻末の「14 トラブルシューティング」を参照してください。

認証装置のビープ音の設定を [OFF] にしている場合は、ビープ音は鳴りません。ビープ音の設定方法については「6.9 ビープ音の ON/OFF」を参照してください。

重要

- ・ 認証に連続 10 回失敗すると、5 分間認証を受け付けません。
- ・ ログオンしているユーザーのみがロックを解除することができます。

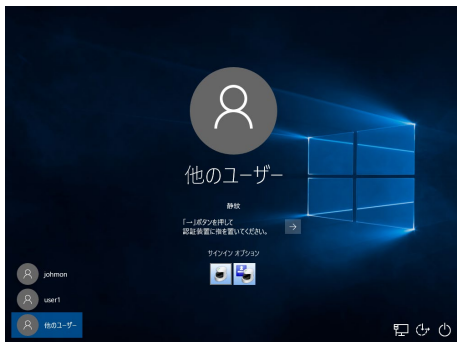
5.6.2 Windows 10 / Windows Server 2016 / Windows Server 2019 / Windows 11

をお使いの場合

- ① スクリーンセーバー起動中に操作を行うと、右の画面が表示されます。
- (Windows のセキュリティポリシー設定で「対話型ログオン: Ctrl+Alt+Del を必要としない」を「有効」に設定している場合は表示されません)



- ② [Ctrl] キーと [Alt] キーと [Delete] キーを同時に押下すると右の画面が表示されます。(ユーザーの設定によっては右の画面から表示されます。)



重要

①または②の画面が表示されない場合は、本書「15.1 スクリーンセーバーの設定について」を参照しパスワードによる保護を有効にしてください。

- ③ [→] ボタンをクリックすると、右の撮影画面が表示され、状態表示 LED が緑の点滅をします。ログオンしているユーザーの指を認証装置に置きます。



- ④ 「ピピッ」というピープ音が鳴り、状態表示 LED が緑の点灯に変われば認証成功です。
「ピピー」というピープ音が鳴り、状態表示 LED が赤の点灯に変われば認証失敗です（一瞬赤が点灯し、すぐに緑の点灯に変わります）。
撮影画面において 10 秒以内に撮影が終わらない場合もピープ音が鳴りエラー画面が表示されます。
ピープ音と状態表示 LED については「取扱説明書 ハードウェア編」の「2.1 認証装置の各部の名称と機能」を参照してください。
また、正しく認証を行えない場合は本書巻末の「14 トラブルシューティング」を

参照してください。

認証装置のビープ音の設定を [OFF] にしている場合は、ビープ音は鳴りません。ビープ音の設定方法については「6.9 ビープ音の ON/OFF」を参照してください。

重要

- 認証に連続 10 回失敗すると、5 分間認証を受け付けません。
- ログオンしているユーザーのみがロックを解除することができます。
- Windows 10 または Windows 11 では、Windows のグループポリシーの「ユーザーの簡易切り替え」の設定によって、ロック解除の画面表示が変わる場合があります。本マニュアルでは、「ユーザーの簡易切り替え」が“有効”の場合の手順を示しています。

5.7 スクリーンセーバーロック解除（ID と静紋認証の場合）

5.7.1 Windows Server 2012 / Windows 8.1 / Windows Server 2012 R2 をお使いの場合

- ① スクリーンセーバー起動中に操作を行うと、右の画面が表示されます。
(Windows のセキュリティポリシー設定で「対話型ログオン: Ctrl+Alt+Del を必要としない」を「有効」に設定している場合は表示されません)



- ② [Ctrl]キーと[Alt]キーと[Delete]キーを同時に押下すると右の画面が表示されます。
(ユーザーの設定によっては右の画面から表示されます。)
ロックされているユーザーが選択された画面が表示されます。



重要

- ①または②の画面が表示されない場合は、本書「15.1 スクリーンセーバーの設定について」を参照しパスワードによる保護を有効にしてください。
- ③ [→]ボタンをクリックすると右の撮影画面が表示され、状態表示LEDが緑の点滅をします。
入力したユーザーの指を認証装置に置きます。



- ④ 「ピピッ」というビープ音が鳴り、状態表示 LED が緑の点灯に変われば認証成功です。

「ビピー」というビープ音が鳴り、状態表示 LED が赤の点灯に変われば認証失敗です（一瞬赤が点灯し、すぐに緑の点灯に変わります）。

撮影画面において 10 秒以内に撮影が終わらない場合もビープ音が鳴りエラー画面が表示されます。

ビープ音と状態表示 LED については「取扱説明書 ハードウェア編」の「2.1 認証装置の各部の名称と機能」を参照してください。

また、正しく認証を行えない場合は本書巻末の「14 トラブルシューティング」を参照してください。

認証装置のビープ音の設定を [OFF] にしている場合は、ビープ音は鳴りません。

ビープ音の設定方法については「6.9 ビープ音の ON/OFF」を参照してください。

重要

- ・ 認証に連続 10 回失敗すると、5 分間認証を受け付けません。
- ・ ログオンしているユーザーのみがロックを解除することができます。

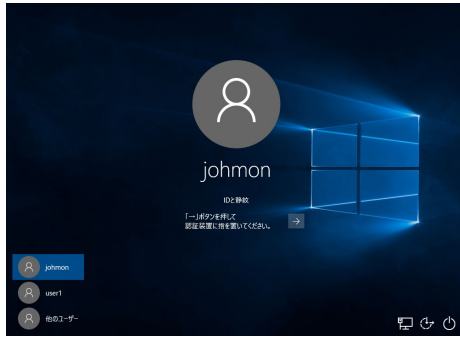
5.7.2 Windows 10 / Windows Server 2016 / Windows Server 2019 / Windows 11

をお使いの場合

- ① スクリーンセーバー起動中に操作を行うと、右の画面が表示されます。
（Windows のセキュリティポリシー設定で「対話型ログオン：Ctrl+Alt+Del を必要としない」を「有効」に設定している場合は表示されません）



- ② [Ctrl] キーと [Alt] キーと [Delete] キーを同時に押下すると右の画面が表示されます。
(ユーザーの設定によっては右の画面から表示されます。)
ロックされているユーザーが選択された画面が表示されます。



重要

①または②の画面が表示されない場合は、本書「15.1 スクリーンセーバーの設定について」を参照しパスワードによる保護を有効にしてください。

- ③ [→] ボタンをクリックすると右の撮影画面が表示され、状態表示 LED が緑の点滅をします。
入力したユーザーの指を認証装置に置きます。



- ④ 「ピピッ」というビープ音が鳴り、状態表示 LED が緑の点灯に変われば認証成功です。
「ピーー」というビープ音が鳴り、状態表示 LED が赤の点灯に変われば認証失敗です（一瞬赤が点灯し、すぐに緑の点灯に変わります）。
撮影画面において 10 秒以内に撮影が終わらない場合もビープ音が鳴りエラー画面が表示されます。
ビープ音と状態表示 LED については「取扱説明書 ハードウェア編」の「2.1 認証装置の各部の名称と機能」を参照してください。
また、正しく認証を行えない場合は本書巻末の「14 トラブルシューティング」を参照してください。
認証装置のビープ音の設定を [OFF] にしている場合は、ビープ音は鳴りません。
ビープ音の設定方法については「6.9 ビープ音の ON/OFF」を参照してください。

重要

- ・ 認証に連続 10 回失敗すると、5 分間認証を受け付けません。
- ・ ログオンしているユーザーのみがロックを解除することができます。
- ・ Windows 10 または Windows 11 では、Windows のグループポリシーの「ユーザーの簡易切り替え」の設定によって、ロック解除の画面表示が変わる場合があります。本マニュアルでは、「ユーザーの簡易切り替え」が“有効”の場合の手順を示しています。

5.8 スクリーンセーバーロック解除（静紋と二要素用パスワード認証の場合）

5.8.1 Windows Server 2012 / Windows 8.1 / Windows Server 2012 R2 をお使いの場合

- ① スクリーンセーバー起動中に操作を行うと、右の画面が表示されます。
（Windows のセキュリティポリシー設定で「対話型ログイン: Ctrl+Alt+Del を必要としない」を「有効」に設定している場合は表示されません）



- ② [Ctrl] キーと [Alt] キーと [Delete] キーを同時に押下すると右の画面が表示されます。
（ユーザーの設定によっては右の画面から表示されます。）



ロックされているユーザーが選択された画面が表示されます。

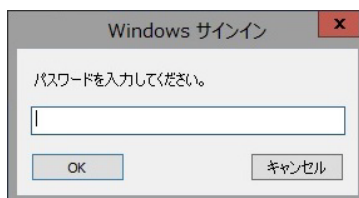
重要

①または②の画面が表示されない場合は、本書「15.1 スクリーンセーバーの設定について」を参照しパスワードによる保護を有効にしてください。

- ③ [→] ボタンをクリックすると、右の撮影画面が表示され、状態表示 LED が緑の点滅をします。
ログオンしているユーザーの指を認証装置に置きます。



- ④ 右のパスワード入力画面が表示されるので、二要素用パスワードを入力し [OK] ボタンをクリックします。



- ⑤ 「ピピッ」というビープ音が鳴り、状態表示 LED が緑の点灯に変われば認証成功です。

「ピーー」というビープ音が鳴り、状態表示 LED が赤の点灯に変われば認証失敗です（一瞬赤が点灯し、すぐに緑の点灯に変わります）。

撮影画面において 10 秒以内に撮影が終わらない場合もビープ音が鳴りエラー画面が表示されます。

ビープ音と状態表示 LED については「取扱説明書 ハードウェア編」の「2.1 認証装置の各部の名称と機能」を参照してください。

また、正しく認証を行えない場合は本書巻末の「14 トラブルシューティング」を参照してください。

認証装置のビープ音の設定を [OFF] にしている場合は、ビープ音は鳴りません。ビープ音の設定方法については「6.9 ビープ音の ON/OFF」を参照してください。

重要

- ・ 認証に連続 10 回失敗すると、5 分間認証を受け付けません。
- ・ ログオンしているユーザーのみがロックを解除することができます。

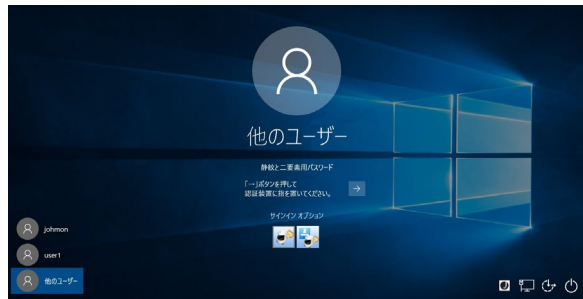
5. 8. 2 Windows 10 / Windows Server 2016 / Windows Server 2019 / Windows 11

をお使いの場合

- ① スクリーンセーバー起動中に操作を行うと、右の画面が表示されます。
(Windows のセキュリティポリシー設定で「対話型ログオン: Ctrl+Alt+Del を必要としない」を「有効」に設定している場合は表示されません)



- ② [Ctrl] キーと [Alt] キーと [Delete] キーを同時に押下すると右の画面が表示されます。
(ユーザーの設定によっては右の画面から表示されません。)



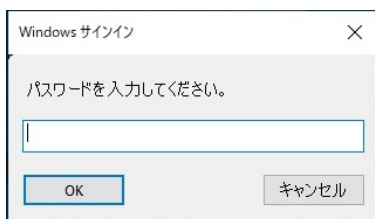
重要

- ①または②の画面が表示されない場合は、本書「15.1 スクリーンセーバーの設定について」を参照しパスワードによる保護を有効にしてください。

- ③ 「←」 ボタンをクリックすると、右の撮影画面が表示され、状態表示 LED が緑の点滅をします。ログオンしているユーザーの指を認証装置に置きます。



- ④ 右のパスワード入力画面が表示されるので、二要素用パスワードを入力し[OK]ボタンをクリックします。



- ⑤ 「ピピッ」というビープ音が鳴り、状態表示 LED が緑の点灯に変われば認証成功です。
「ビピー」というビープ音が鳴り、状態表示 LED が赤の点灯に変われば認証失敗です（一瞬赤が点灯し、すぐに緑の点灯に変わります）。
撮影画面において 10 秒以内に撮影が終わらない場合もビープ音が鳴りエラー画面が表示されます。
ビープ音と状態表示 LED については「取扱説明書 ハードウェア編」の「2.1 認証装置の各部の名称と機能」を参照してください。
また、正しく認証を行えない場合は本書巻末の「14 トラブルシューティング」を参照してください。
- 認証装置のビープ音の設定を [OFF] にしている場合は、ビープ音は鳴りません。ビープ音の設定方法については「6.9 ビープ音の ON/OFF」を参照してください。

重要

- 認証に連続 10 回失敗すると、5 分間認証を受け付けません。
- ログオンしているユーザーのみがロックを解除することができます。
- Windows 10 または Windows 11 では、Windows のグループポリシーの「ユーザーの簡易切り替え」の設定によって、ロック解除の画面表示が変わる場合があります。本マニュアルでは、「ユーザーの簡易切り替え」が“有効”の場合の手順を示しています。

5.9 スクリーンセーバーロック解除（ID と静紋と二要素用パスワード認証の場合）

5.9.1 Windows Server 2012 / Windows 8.1 / Windows Server 2012 R2 をお使いの場合

- ① スクリーンセーバー起動中に操作を行うと、右の画面が表示されます。
(Windows のセキュリティポリシー設定で「対話型ログオン: Ctrl+Alt+Del を必要としない」を「有効」に設定している場合は表示されません)



- ② [Ctrl] キーと [Alt] キーと [Delete] キーを同時に押下すると右の画面が表示されます。
(ユーザーの設定によっては右の画面から表示されます。)
ロックされているユーザーが選択された画面が表示されます。



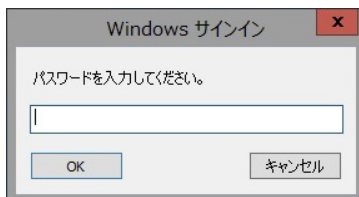
重要

①または②の画面が表示されない場合は、本書「15.1 スクリーンセーバーの設定について」を参照しパスワードによる保護を有効にしてください。

- ③ [→]ボタンをクリックすると右の撮影画面が表示され、状態表示LEDが緑の点滅をします。入力したユーザーの指を認証装置に置きます。



- ④ 右のパスワード入力画面が表示されるので、二要素用パスワードを入力し[OK]ボタンをクリックします。



- ⑤ 「ピピッ」というビープ音が鳴り、状態表示LEDが緑の点灯に変われば認証成功です。
「ピーー」というビープ音が鳴り、状態表示LEDが赤の点灯に変われば認証失敗です（一瞬赤が点灯し、すぐに緑の点灯に変わります）。
撮影画面において10秒以内に撮影が終わらない場合もビープ音が鳴りエラー画面が表示されます。
ビープ音と状態表示LEDについては「取扱説明書 ハードウェア編」の「2.1 認証装置の各部の名称と機能」を参照してください。
また、正しく認証を行えない場合は本書巻末の「14 トラブルシューティング」を参照してください。
認証装置のビープ音の設定を[OFF]にしている場合は、ビープ音は鳴りません。
ビープ音の設定方法については「6.9 ビープ音のON/OFF」を参照してください。

重要

- ・ 認証に連続10回失敗すると、5分間認証を受け付けません。
- ・ ログオンしているユーザーのみがロックを解除することができます。

5.9.2 Windows 10 / Windows Server 2016 / Windows Server 2019 / Windows 11

をお使いの場合

- ① スクリーンセーバー起動中に操作を行うと、右の画面が表示されます。
(Windows のセキュリティポリシー設定で「対話型ログオン: Ctrl+Alt+Del を必要としない」を「有効」に設定している場合は表示されません)



- ② [Ctrl] キーと [Alt] キーと [Delete] キーを同時に押下すると右の画面が表示されます。
(ユーザーの設定によっては右の画面から表示されます。)
ロックされているユーザーが選択された画面が表示されます。



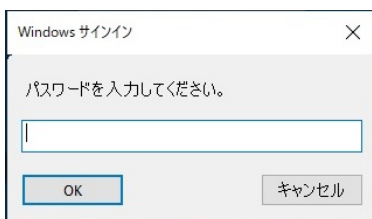
重要

①または②の画面が表示されない場合は、本書「15.1 スクリーンセーバーの設定について」を参照しパスワードによる保護を有効にしてください。

- ③ [→] ボタンをクリックすると右の撮影画面が表示され、状態表示 LED が緑の点滅をします。
入力したユーザーの指を認証装置に置きます。



- ④ 右のパスワード入力画面が表示されるので、二要素用パスワードを入力し[OK] ボタンをクリックします。



- ⑤ 「ピピッ」というビープ音が鳴り、状態表示 LED が緑の点灯に変われば認証成功です。

「ピピー」というビープ音が鳴り、状態表示 LED が赤の点灯に変われば認証失敗です（一瞬赤が点灯し、すぐに緑の点灯に変わります）。

撮影画面において 10 秒以内に撮影が終わらない場合もビープ音が鳴りエラー画面が表示されます。

ビープ音と状態表示 LED については「取扱説明書 ハードウェア編」の「2.1 認証装置の各部の名称と機能」を参照してください。

また、正しく認証を行えない場合は本書巻末の「14 トラブルシューティング」を参照してください。

認証装置のビープ音の設定を [OFF] にしている場合は、ビープ音は鳴りません。ビープ音の設定方法については「6.9 ビープ音の ON/OFF」を参照してください。

重要

- 認証に連続 10 回失敗すると、5 分間認証を受け付けません。
- ログオンしているユーザーのみがロックを解除することができます。
- Windows 10 または Windows 11 では、Windows のグループポリシーの「ユーザーの簡易切り替え」の設定によって、ロック解除の画面表示が変わる場合があります。本マニュアルでは、「ユーザーの簡易切り替え」が“有効”の場合の手順を示しています。

5.10 スクリーンセーバーロック解除（ID と静紋と Windows パスワード認証の場合）

5.10.1 Windows Server 2012 / Windows 8.1 / Windows Server 2012 R2 をお使いの場合

- ① スクリーンセーバー起動中に操作を行うと、右の画面が表示されます。
(Windows のセキュリティポリシー設定で「対話型ログオン: Ctrl+Alt+Del を必要としない」を「有効」に設定している場合は表示されません)



- ② [Ctrl] キーと [Alt] キーと [Delete] キーを同時に押下すると右の画面が表示されます。
(ユーザーの設定によっては右の画面から表示されます。)



ロックされているユーザーが選択された画面が表示されますので、Windows パスワードを入力します。

重要

①または②の画面が表示されない場合は、本書「15.1 スクリーンセーバーの設定について」を参照しパスワードによる保護を有効にしてください。

- ③ [→]ボタンをクリックすると右の撮影画面が表示され、状態表示LEDが緑の点滅をします。入力したユーザーの指を認証装置に置きます。



- ④ 「ピピッ」というビープ音が鳴り、状態表示LEDが緑の点灯に変われば認証成功です。
「ピピー」というビープ音が鳴り、状態表示LEDが赤の点灯に変われば認証失敗です（一瞬赤が点灯し、すぐに緑の点灯に変わります）。
撮影画面において10秒以内に撮影が終わらない場合もビープ音が鳴りエラー画面が表示されます。
ビープ音と状態表示LEDについては「取扱説明書 ハードウェア編」の「2.1 認証装置の各部の名称と機能」を参照してください。
また、正しく認証を行えない場合は本書巻末の「14 トラブルシューティング」を参照してください。
認証装置のビープ音の設定を[OFF]にしている場合は、ビープ音は鳴りません。
ビープ音の設定方法については「6.9 ビープ音のON/OFF」を参照してください。

重要

- ・ 認証に連続10回失敗すると、5分間認証を受け付けません。
- ・ ログオンしているユーザーのみがロックを解除することができます。

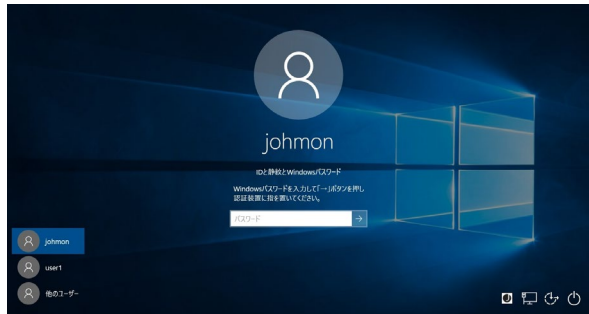
5. 10. 2 Windows 10 / Windows Server 2016 / Windows Server 2019 / Windows 11

をお使いの場合

- ① スクリーンセーバー起動中に操作を行うと、右の画面が表示されます。
(Windows のセキュリティポリシー設定で「対話型ログオン: Ctrl+Alt+Del を必要としない」を「有効」に設定している場合は表示されません)



- ② [Ctrl] キーと [Alt] キーと [Delete] キーを同時に押下すると右の画面が表示されます。
(ユーザーの設定によっては右の画面から表示されます。) ロックされているユーザーが選択された



画面が表示されますので、Windows パスワードを入力します。

重要

①または②の画面が表示されない場合は、本書「15.1 スクリーンセーバーの設定について」を参照しパスワードによる保護を有効にしてください。

- ③ [一] ボタンをクリックすると右の撮影画面が表示され、状態表示 LED が緑の点滅をします。
入力したユーザーの指を認証装置に置きます。



- ④ 「ピピッ」というビープ音が鳴り、状態表示 LED が緑の点灯に変われば認証成功です。
「ピーー」というビープ音が鳴り、状態表示 LED が赤の点灯に変われば認証失敗です（一瞬赤が点灯し、すぐに緑の点灯に変わります）。
撮影画面において 10 秒以内に撮影が終わらない場合もビープ音が鳴りエラー画面が表示されます。
ビープ音と状態表示 LED については「取扱説明書 ハードウェア編」の「2.1 認証装置の各部の名称と機能」を参照してください。
また、正しく認証を行えない場合は本書巻末の「14 トラブルシューティング」を参照してください。
認証装置のビープ音の設定を [OFF] にしている場合は、ビープ音は鳴りません。
ビープ音の設定方法については「6.9 ビープ音の ON/OFF」を参照してください。

重要

- ・ 認証に連続 10 回失敗すると、5 分間認証を受け付けません。
- ・ ログオンしているユーザーのみがロックを解除することができます。
- ・ Windows 10 または Windows 11 では、Windows のグループポリシーの「ユーザーの簡易切り替え」の設定によって、ロック解除の画面表示が変わる場合があります。本マニュアルでは、「ユーザーの簡易切り替え」が“有効”の場合の手順を示しています。

6 ユーザー管理機能

新規ユーザーの登録、指情報の追加、変更、削除等はユーザー管理機能により行います。

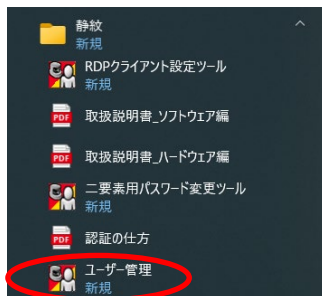
ユーザー管理機能を起動するには、以下の手順を実行します。

- ① ・Windows Server 2012 / Windows 8.1 / Windows Server 2012 R2 をお使いの場合

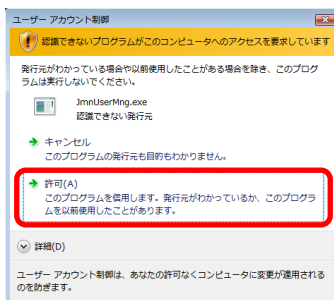
スタートメニューから、[スタート] → [アプリ]
→[ユーザー管理]をクリックします。



・Windows 10 / Windows Server 2016 / Windows Server 2019 / Windows 11 をお使いの場合
スタートメニューから、[すべてのアプリ]→
[静紋]→[ユーザー管理]をクリックします。



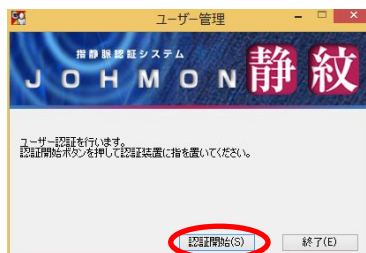
- ② 右の画面が表示される場合があります。表示された場合は[許可(A)]をクリックしてください。
表示されない場合は次の手順へ進みます。



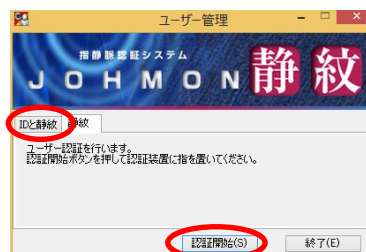
- ③ 右の画面が表示されます。

1:1 認証が利用可能でない場合と利用可能である場合とで表示される画面が異なります。

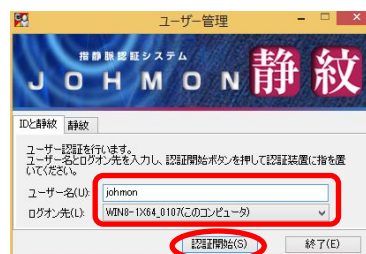
静紋認証を行う場合は、[認証開始] ボタンをクリックします。



1:1 認証が利用可能である場合は、ID と静紋認証を行うことができます。ID と静紋認証を行う場合は、[ID と静紋] タブをクリックします。



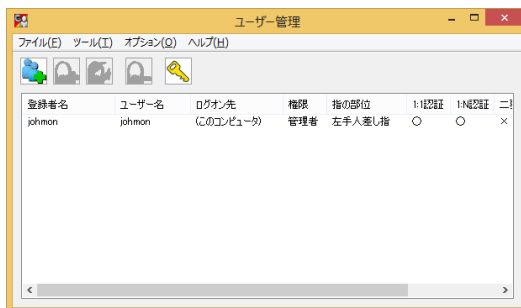
- ④ [ID と静紋] タブをクリックすると右の画面が表示されます。管理者として登録されているユーザーIDを入力し、ログオン先を選択して、[認証開始] ボタンをクリックします。



- ⑤ 右の撮影画面が表示されます。管理者権限のあるユーザーの指を認証装置に置きます。



「ピピッ」というビープ音が鳴り、状態表示 LED が緑の点灯に変われば認証成功です。認証が確認できれば、「ユーザー管理」画面が表示されます。



「ピーー」というビープ音が鳴り、状態表示 LED が赤の点灯に変われば認証失敗です。10 秒以内に撮影が終わらない場合もビープ音が鳴りエラー画面が表示されます。ビープ音と状態表示 LED については「取扱説明書 ハードウェア編」の「2.1 認証装置の各部の名称と機能」を参照してください。また、正しく認証を行えない場合は本書巻末の「14 トラブルシューティング」を参照してください。

認証装置のビープ音の設定を「OFF」にしている場合は、ビープ音は鳴りません。ビープ音の設定方法については「6.9 ビープ音の ON/OFF」を参照してください。

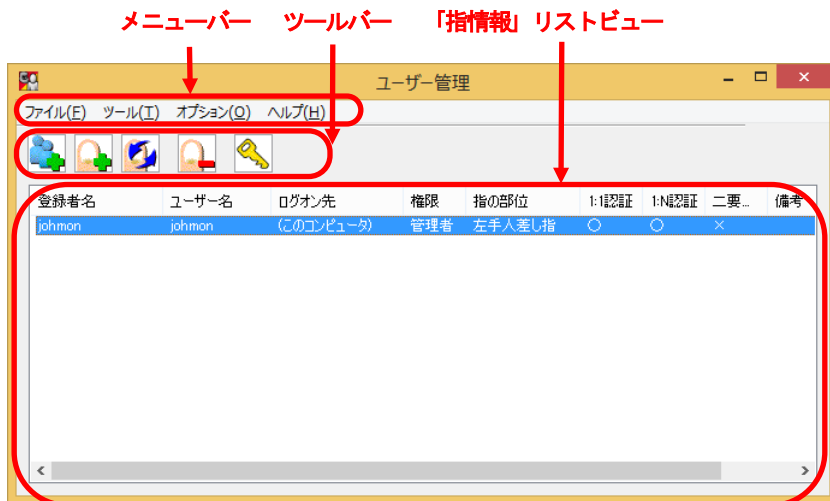
重要

- ユーザー管理機能を起動したまま、離席等を行わないように注意してください。離席時はユーザー管理機能を終了させてください。
- 認証に成功しても、ユーザーの指が管理者権限を持っていない場合は「ユーザー管理」画面は表示されません。このような場合には下記の画面が表示されますので、[OK] ボタンをクリックして、管理者権限のあるユーザーの指で再度、認証を行ってください。



- 二要素認証が有効に設定されていた場合でも、ユーザー管理機能の起動時の認証は、「ID と静紋」認証または「静紋」認証になります。
- ユーザー管理機能を起動中に DPI の設定を変更した場合は、ユーザー管理機能のアプリケーションを一旦終了させ、再起動する必要があります。アプリケーションを再起動しないと、ユーザー管理機能の画面が正常に表示されない問題が生じる場合があります。

⑥ 「ユーザー管理」画面の画面構成は以下のようになっています。



「指情報」 リストビュー

「ログオン先」欄には、ログオン先がローカルコンピュータの場合は「(このコンピュータ)」、ログオン先がドメインの場合にはドメイン名が表示されます。

ツールバー



: 新規ユーザーの登録を行います。



: 指情報の追加を行います。



: 指情報の変更を行います。



: 指情報の削除を行います。




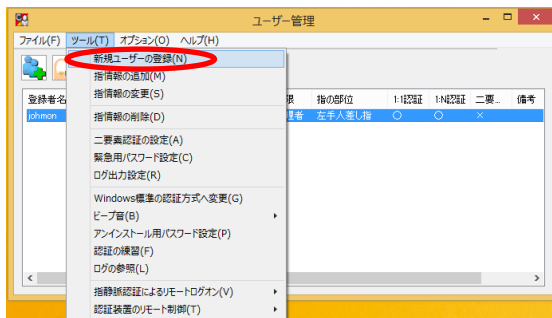
: 緊急用パスワードの設定を行います。

6.1 新規ユーザーの登録

新規ユーザーを作成することができます。

作成するユーザーは既に Windows のユーザーアカウントとして登録されパスワードが設定されている必要があります。Windows のユーザーアカウントが登録されていない場合は、Windows のユーザーアカウントを登録し、パスワードを設定してください。

「ユーザー管理」画面のメニューバーから[ツール (T)] → [新規ユーザーの登録 (N)] をクリックするか、ツールバーの  アイコンをクリックします。



[Step1] 指情報の登録

Step1 ではユーザー登録に必要な情報の入力、登録する指の部位を決定します。

- ① 以下の画面が表示されます。

ユーザー情報

登録者名には、後の管理を容易にするために指情報の登録を行う方の氏名を入力することをお勧めします。登録者名には、全角/半角共に 20 文字まで入力できます。登録する Windows のユーザー名、ログオン先、およびユーザーの権限を入力します。ログオン先の初期設定は現在のログオン先です。変更する場合はプルダウンメニューから選択します。ユーザーの権限の初期設定は一般ユーザーです。

本製品がインストールされたパソコンが Active Directory の環境下で動作している場合、ユーザー名をユーザプリンシパル名 (UPN) 形式での入力を行うことができます。ユーザー名にはまず UPN プレフィックスを入力します。続けて「@」が入力された時点で「ログオン先」のダイアログボックスが無効化されますので、UPN サフィックスの部分を入力します。

1. ユーザー情報

登録者名 (R)	静紋
ユーザー (U)	johmon@johmon.domain.co.jp
ログオン先 (L)	[Disabled Dropdown]
ユーザーの権限 (A)	一般ユーザー

Microsoft アカウントの場合、ユーザー名にメールアドレスを入力してください。

管理者として登録したい場合には、Administrators グループに属するユーザーの情報を入力して、プルダウンメニューから管理者を選択してください。

重要

- ユーザー名を UPN 形式、または Microsoft アカウントのメールアドレスを入力する場合を除き、「@」を含むユーザー名をご使用になることはできません。
- 登録するユーザーは、あらかじめ Windows 用パスワードが設定されている必要があります。
- Microsoft アカウントを登録する場合、そのアカウントが Windows のアカウントとして設定されている必要があります。

パスワード

ユーザーの Windows 用パスワードを入力します。127 文字まで入力することができます。

Windows パスワードを使用した二要素認証が有効の場合は、パスワードの入力を省略できます。(二要素認証の設定については、本書「6.5 二要素認証の設定」参照)

指の部位

登録する指の部位を指定します。爪の部分をクリックすることにより登録する指を指定します。指の部位は初期設定では右手中指となっています。指ごとに権限を変えることができます。

認証方式

認証方式を変更することができます。認証方式には、「静紋」認証方式と「ID と静紋」認証方式の二つの認証方式を選ぶことができます。それぞれの認証方式の特徴は次の通りです。

- ・ 静紋認証方式(1:N 認証方式)
登録した全ての指静脈の中から比較して本人を特定します。
- ・ ID と静紋認証方式(1:1 認証方式)
予め本人を特定するためのユーザーID を入力し、ユーザーID に登録されている指静脈と比較して本人を特定します。この認証方式を選択した場合は、認証のセキュリティレベル(認証のしやすさ)を変更できます。

ID と静紋認証方式 (1:1 認証方式) を利用する場合は「1:1 認証を利用可能とする」にチェックを入れます。

チェックを入れた場合、「セキュリティレベル」が選択できるようになります。セキュリティレベルを変更することで、認証のしやすさを5段階で変えることができます。

認証方式の設定は次の二要素認証でも有効になります。

- ・ 静紋と二要素用パスワード認証(1:N 認証方式)
- ・ ID と静紋と二要素用パスワード認証(1:1 認証方式)
- ・ ID と静紋と Windows パスワード認証(1:1 認証方式)

重要

- ・セキュリティレベルは「高」へ近づけるに従い、より厳しく認証を行います。
他人を受け入れづらくなりますが、本人も認証しにくくなる場合があります。

備考

認証に必要な情報ではありません。最大で全角/半角共に 50 文字までの情報を入力できます。

- ② ユーザー名、ログオン先、ユーザーの権限、Windows 用パスワードの入力、認証方式の選択をし、指の部位を選択した後に、[撮影開始(S)] ボタンをクリックします。

The screenshot shows the '新規ユーザーの登録' (New User Registration) window. It contains the following elements:

- 1. ユーザー情報 (User Information):** Fields for '登録者名(R)' (Registration Name), 'ユーザーID' (User ID), 'ログオン先(L)' (Login Destination), and 'ユーザーの権限(A)' (User Permissions). The '登録者名' and 'ユーザーID' fields are highlighted with a red box.
- 2. パスワード (Password):** A field for 'Windows用(P)' (Windows Password) with a strength indicator. This field is highlighted with a red box.
- 3. 指の部位 (Finger Position):** Two diagrams of hands (left and right) with numbered circles (1-5) indicating the specific finger areas to be scanned. This section is highlighted with a red box.
- 4. 認証方式 (Authentication Method):** A section with a checkbox for '認証方式(認証方式)' (Authentication Method) and a dropdown menu for 'セキュリティレベル(S)' (Security Level). This section is highlighted with a red box.
- Buttons:** A '撮影開始(S)' (Start Shooting) button at the bottom right and a 'メニューへ戻る(B)' (Return to Menu) button at the bottom right.

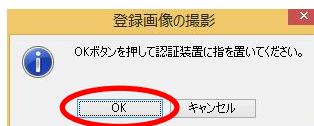
重要

- 指以外のものを登録しないでください。誤動作の原因となります。
- Domain Admins グローバルグループはAdministrators ローカルグループに所属している必要があります。デフォルトで所属していますので、削除しないようにしてください。
- ローカルグループに所属していないユーザーを管理者として登録する場合は、このユーザーはドメインのアカウントでWindows ヘログオンしておく必要があります。
- ユーザー名とログオン先を同名に設定できません。
- Windows パスワードを使用した二要素認証を有効にして「パスワード」の入力を省略した場合、Windows パスワードを使用した二要素認証以外の設定に変更すると認証できなくなります。設定を変更した場合は、「指情報の変更」から「パスワード」を再設定してください。（本書「6.3 指情報の変更」参照）

[Step2] ～ [Step4] 静脈撮影

[Step1] で入力した情報を元に登録するユーザーの指を撮影します。[Step2] ～ [Step4] まで撮影は3回行われます。

- ① 右の画面が表示されます。
[OK] ボタンをクリックします。または
[Enter] キーを押下します。



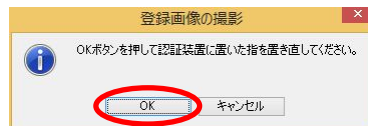
- ② 画面の指示に従い、認証装置に指を置きます。



重要

- ・ 乳幼児や極端に指が細い方(指の幅が 10mm 未満)、太い方(指の幅が 25mm 以上)、指が短い方(指が認証ゾーンの先まで届かない方)は、指の登録や認証に失敗する場合があります。
- ・ 認証ができにくくなった場合(成長期の子供で指の状態が変わる場合等)は、下記の手順に従い指情報を再度登録してください。
 1. 該当の指情報を削除する。指情報の削除については、本書「6.4 指情報の削除」を参照してください。
 2. 再度「指情報の追加」を行う。指情報の追加については、本書「6.2 指情報の追加」を参照してください。
- ・ 撮影中は認証装置の認証ゾーンに指以外のものを置かないでください。誤動作の原因となる場合があります。(手袋や絆創膏等の指を覆うものや指輪)
- ・ 撮影中は認証装置の接続を切断しないでください。
- ・ 撮影中はお使いのパソコンをロック、ログオフ、シャットダウン、スリープ状態、休止状態、スタンバイ状態にしないでください。いずれかの状態からの復帰後に正しい認証が行われず、システムが不安定になる場合があります。

- ③ 「ピッ」というビープ音が鳴り、右の画面が表示されれば撮影成功です。指を離して [OK] ボタンをクリックするか、[Enter] キーを押下します。



「ビピー」というビープ音が鳴り、状態表示 LED が赤の点灯に変わり、エラー画面が表示されれば撮影失敗です。10 秒以内に撮影が終わらない場合もビープ音が鳴りエラー画面が表示されます。ビープ音と状態表示 LED については「取扱説明書 ハードウェア編」の「2.1 認証装置の各部の名称と機能」を参照してください。

また、正しく登録を行えない場合は本書巻末の「14 トラブルシューティング」を参照してください。

認証装置のビープ音の設定を [OFF] にしている場合は、ビープ音は鳴りません。ビープ音の設定方法については「6.9 ビープ音の ON/OFF」を参照してください。

- ④ 指静脈撮影は正確な情報を得るために3回行われます。③の画面が表示されるので、あと2回の撮影を行います。

重要

- ・ 撮影時には必ず指を置き直してください(一度、認証ゾーンから指を抜き、再度、指を認証ゾーンに置いて下さい)。置き直しをしないと正しく認証されない場合があります。

[Step5] 登録結果

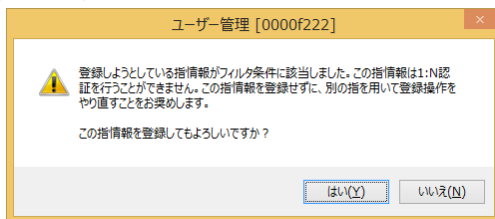
[Step2] ～ [Step4] で撮影した情報を元にシステムに指情報の登録を行います。

- ① 3回の撮影に成功し、新規ユーザー登録が成功すると、右の画面が表示されます。
[OK] ボタンをクリックするか、[Enter] キーを押下します。
撮影に失敗した場合は本書巻末の「14 トラブルシューティング」を参照してください。



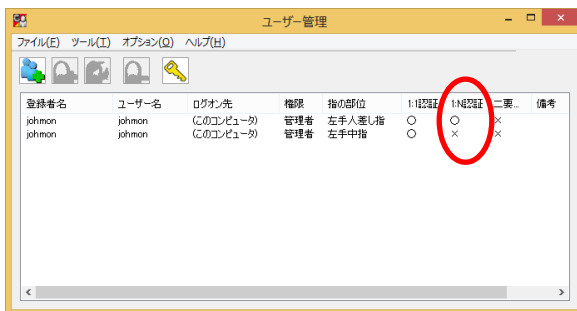
重要

- 指のけがなどにより、指静脈による認証が行えなくなる場合がありますので、1 ユーザーに対し 2 本以上の指を登録して運用してください。複数の指の登録方法については本書「6.2 指情報の追加」をご覧ください。
- 3 回の撮影に成功した後に以下の画面が表示されることがあります。



この画面で「はい」をクリックして登録を続行した場合、その指は1:N 認証では使用できず、1:1 認証でしか使用することができなくなります。1:N 認証をお使いになる場合は、必ず「いいえ」をクリックして登録をやり直してください。


登録されている指が1:N 認証に使用できるかどうかはユーザー管理画面で確認できます(「1:N 認証」が「○」ならば1:N 認証に使用できます)。

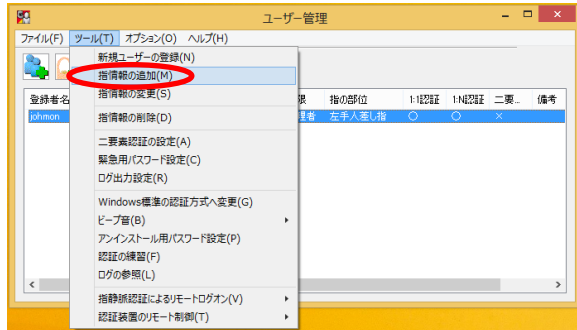


- Microsoft アカウントを登録した場合、ログオン先にメールアドレスの「@」より後の文字列が設定されます。

6.2 指情報の追加

同一アカウントに対して指情報を追加することができます。

指情報リストビューから指情報を追加したいユーザーを選択し、「ユーザー管理」画面のメニューバーから[ツール(T)] → [指情報の追加(M)]をクリックするか、ツールバーの  アイコンをクリックします。



[Step1] 指情報の登録

Step1 では指情報の登録に必要な情報の入力、登録する指の部位を決定します。

- ① 以下の画面が表示されます。
追加したい指の部位を選択します。



指の部位

登録する指の部位を指定します。爪の部分をクリックすることにより登録する指を指定します。指の部位は初期設定では右手中指となっています。

- ② 指情報の追加を行うため「撮影開始(S)」ボタンをクリックします。



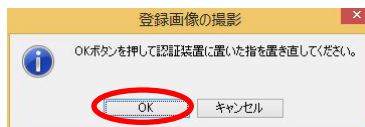
重要

- ・ 指以外のものを登録しないでください。誤動作の原因となります。

[Step2] ～ [Step4] 静脈撮影

[Step1] で入力した情報を元に登録するユーザーの指を撮影します。[Step2] ～ [Step4] まで撮影は3回行われます。

- ① 右の画面が表示されます。
指を認証装置に置いて「OK」ボタンをクリックします。または「Enter」キーを押下します。



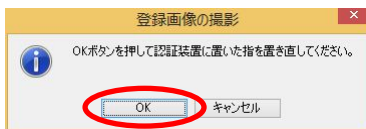
- ② 画面の指示に従い、認証装置に指を置きます。



重要

- ・ 乳幼児や極端に指が細い方(指の幅が 10mm 未満)、太い方(指の幅が 25mm 以上)、指が短い方(指が認証ゾーンの先まで届かない方)は、指の登録や認証に失敗する場合があります。
- ・ 認証ができにくくなった場合(成長期の子供で指の状態が変わる場合等)は、下記の手順に従い 指情報を再度登録してください。
 1. 該当の指情報を削除する。指情報の削除については、本書「6.4 指情報の削除」を参照してください。
 2. 再度「指情報の追加」を行う。指情報の追加については、本書「6.2 指情報の追加」を参照してください。
- ・ 撮影中は認証装置の認証ゾーンに指以外のものを置かないでください。誤動作の原因となる場合があります。
- ・ 撮影中は認証装置の接続を切断しないでください。
- ・ 撮影中はお使いのパソコンをロック、ログオフ、シャットダウン、スリープ状態、休止状態、スタンバイ状態にしないでください。いずれかの状態からの復帰後に正しい認証が行われず、システムが不安定になる場合があります。
- ・ 異なるアカウントにおいて同一の指を複数回登録しないようにしてください。誤動作の原因となります。

- ③ 「ピッ」というビープ音が鳴り、右の画面が表示されれば撮影成功です。指を離して [OK] ボタンをクリックするか、[Enter] キーを押下します。「ビピー」というビープ音が鳴り、状態表示 LED が赤の点灯に変わり、エラー画面が表示されれば撮影失敗です。10 秒以内に撮影が終わらない場合もビープ音が鳴りエラー画面が表示されます。ビープ音と状態表示 LED については「取扱説明書 ハードウェア編」の「2.1 認証装置の各部の名称と機能」を参照してください。また、正しく登録を行えない場合は本書巻末の「14 トラブルシューティング」を参照してください。



認証装置のビープ音の設定を [OFF] にしている場合は、ビープ音は鳴りません。ビープ音の設定方法については「6.9 ビープ音の ON/OFF」を参照してください。

- ④ 静脈撮影は正確な情報を得るために3回行われます。
③の画面が表示されるので、あと2回の撮影を行います。

重要

- ・ 撮影時には必ず指を置き直してください(一度、認証ゾーンから指を抜き、再度、指を認証ゾーンに置いて下さい)。置き直しをしないと正しく認証されない場合があります。

[Step5] 登録結果

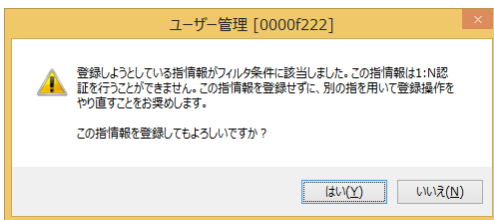
[Step2] ～ [Step4] で撮影した情報を元にシステムに指情報の登録を行います。

- ① 3回の撮影に成功し、指情報の追加が成功すると、右の画面が表示されます。
[OK] ボタンをクリックするか、[Enter] キーを押下します。
撮影に失敗した場合は本書巻末の「14 トラブルシューティング」を参照してください。



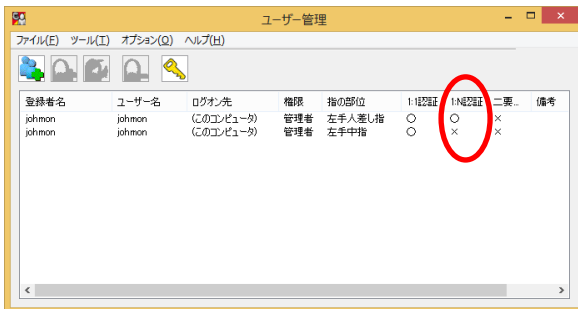
重要

3回の撮影に成功した後に以下の画面が表示されることがあります。




この画面で「はい」をクリックして登録を続行した場合、その指は1:N認証では使用できず、1:1認証でしか使用することができなくなります。1:N認証をお使いになる場合は、必ず「いいえ」をクリックして登録をやり直してください。

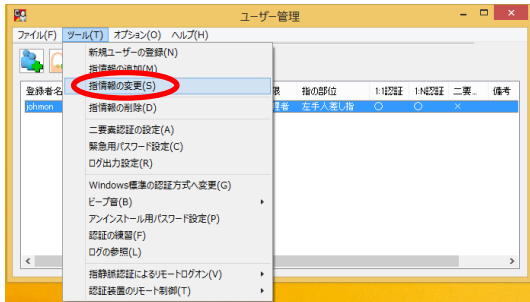
登録されている指が1:N認証に使用できるかどうかはユーザー管理画面で確認できます(「1:N認証」が「○」ならば1:N認証に使用できます)。



6.3 指情報の変更

指情報を変更することができます。指静脈データは変更しないため、撮影は行いません。

- ① 指情報リストビューから指情報を変更したいユーザーを選択し、「ユーザー管理」画面のメニューバーから[ツール (T)] → [指情報の変更 (S)] をクリックするか、ツールバーの  アイコンをクリックします。



- ② 右の画面が表示されます。

指情報の変更

登録者名(R) johnon

権限(A) 管理者

認証方式 ☒ 1: 1: 認証を利用可能とする(I)

セキュリティレベル(I) 中

備考(B)

ユーザー(U) johnon

ログオン先(L) WIN-P6T563L4P3E(このコンピュータ)

パスワード(P) ●●●●●●

☐ ユーザー情報の変更(M)

☐ 二要素認証/パスワードの変更(D)

二要素認証/パスワード(E)

二要素認証/パスワードの確認(V)

変更(O) キャンセル

- ③ [ユーザー情報の変更(M)]にチェックマークを入れたあと、変更する箇所に入力します。
- 二要素用パスワードを変更する場合は、[二要素用パスワードの変更(D)]にチェックマークを入れたあと、[二要素用パスワード(E)]と[二要素用パスワードの確認(V)]を入力します。

入力後に[変更]ボタンをクリックします。

チェック後に入力可能

権限・・・・・・・・・・一般ユーザーか管理者を選択します。管理者は100 指まで登録できます。管理者は最低1 人登録が必要です(管理者として最低1 指の登録が必要)。そのため、管理者の最後の指情報は変更できません。

認証方式・・・・・・・・・・1:1 認証での利用を許可する場合にはチェックします。

備考・・・・・・・・・・備考を変更する場合は書き換えます。

ユーザー情報の変更・・ユーザー情報を変更する場合はチェックします。

ユーザー名・・・・・・・・Windows のユーザー名を入力します。(※1) (※2)

ログオン先・・・・・・・・ユーザーのログオン先を指定します。

パスワード・・・・・・・・Windows ログオン用のパスワードです。127 文字まで入力することができます。

二要素用パスワードの変更・・二要素用パスワードを変更する場合はチェックします。二要素用パスワードを使用した二要素認証の設定が有効の場合にのみ変更可能です。(本書「6.5 二要素認証の設定」参照)

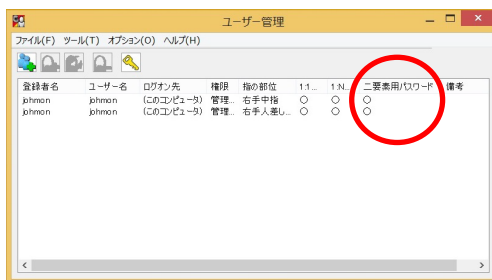
二要素用パスワード・・・・・・・・二要素用パスワードを入力します。127 文字まで入力することができます。

二要素用パスワードの確認・・確認のための二要素用パスワードを入力します。127 文字まで入力することができます。

- ※1 Active Directory の環境下で動作している場合、ユーザー名をユーザプリンシパル名 (UPN) 形式での入力を行うことができます。ユーザー名にはまず UPN プレフィックスを入力します。続けて「@」が入力された時点で「ログオン先」のダイアログボックスが無効化されますので、UPN サフィックスの部分を入力します。
- ※2 Microsoft アカウントの場合、ユーザー名にメールアドレスを入力してください。


重要

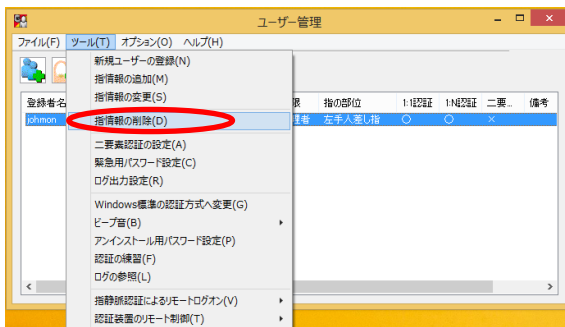
- ユーザー名を UPN 形式、または Microsoft アカウントのメールアドレスを入力する場合を除き、「@」を含むユーザー名をご使用になることはできません。
- ユーザー名に Microsoft アカウントを入力して変更した場合、ログオン先にメールアドレスの「@」より後の文字列が設定されます。
- 二要素用パスワードは 8 文字以上の条件を満たす必要があります。
- 二要素用パスワードが登録されているかどうかはユーザー管理画面で確認できます（「二要素用パスワード」が「○」ならば二要素用パスワードが登録されています）。



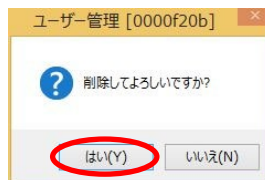
6.4 指情報の削除

指情報を削除することができます。

- ① 指情報リストビューから指情報を削除したいユーザーを選択し、「ユーザー管理」画面のメニューバーから[ツール (T)] → [指情報の削除 (D)] をクリックするか、ツールバーの  アイコンをクリックします。



- ② 右の画面が表示されるので、[はい(Y)] ボタンをクリックします。または [Enter] キーを押下します。



- ③ 指情報が削除され、「ユーザー管理」画面に戻ります。

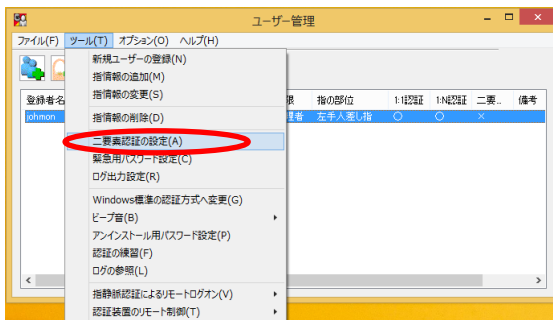
重要

管理者は最低1人登録が必要です(管理者として最低1指の登録が必要)。そのため、管理者の最後の指情報は削除できません。

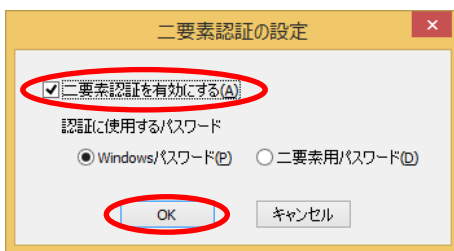
6.5 二要素認証の設定

二要素認証を行うかを設定することができます。

- ① 「ユーザー管理」画面のメニューバーから[ツール(T)]→[二要素認証の設定(A)]をクリックします。



- ② 右の画面が表示されます。
「二要素認証を有効にする(A)」をチェックすると、二要素認証が有効になり、「認証に使用するパスワード」が選択できます。



二要素認証にWindowsパスワードを使用する場合は「Windows

パスワード(P)」をチェックし、[OK]ボタンをクリックします。

二要素認証に二要素用パスワードを使用する場合は「二要素用パスワード(D)」をチェックし、[OK]ボタンをクリックします。

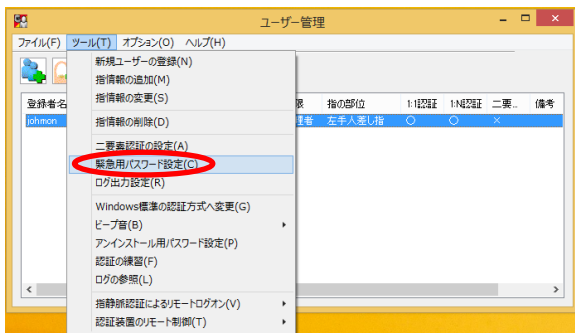
「二要素認証を有効にする(A)」をチェックしないで[OK]ボタンをクリックすると、二要素認証が無効になります。

6.6 緊急用パスワードの設定

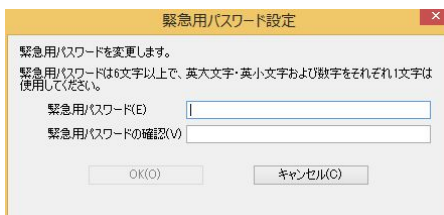
緊急用パスワードを設定することができます。

緊急用パスワードは指静脈認証ができなくなった場合に利用します。忘れないようにしてください。

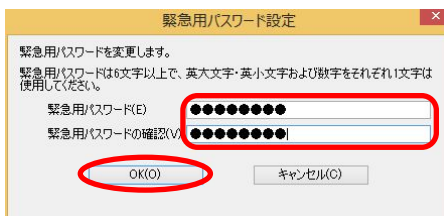
- ① 「ユーザー管理」画面のメニューバーから[ツール(T)]→[緊急用パスワード設定(C)]をクリックするか、ツールバーの🔑アイコンをクリックします。



- ② 右の画面が表示されます。



- ③ 緊急用パスワードを入力します。
確認のためもう一度緊急用パスワードを入力して、[OK]ボタンをクリックします。
127 文字まで入力することができます。



- ④ 緊急用パスワードが設定され、「ユーザー管理」画面に戻ります。

重要

緊急用パスワードは管理者のみ操作することが可能であり、ユーザーごとに設定することはできません。また、緊急用パスワードは以下の条件を満たす必要があります。

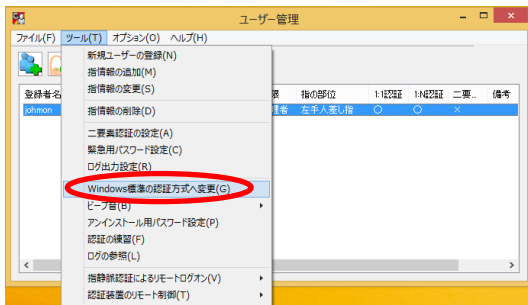
- 6 文字以上であること
- 英大文字、英小文字、数値をそれぞれ少なくとも 1 文字以上使用すること

6.7 認証方法の変更

システムの認証方式を指静脈認証方式から Windows 標準の認証方式へ、また、Windows 標準の認証方式から指静脈認証方式へ変更することができます。

- ・ システムの認証方式を従来の Windows 標準の認証方式（パスワード認証）に戻す場合

- ① 「ユーザー管理」画面のメニューバーから [ツール(T)] → [Windows 標準の認証方式へ変更(G)] をクリックします。



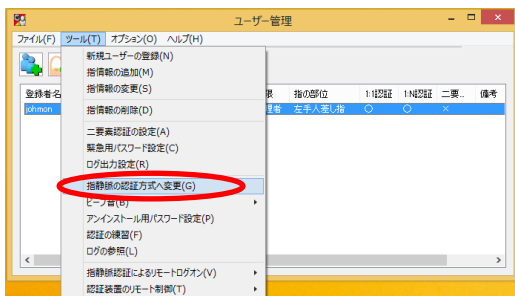
- ② 右の画面が表示されるので、[はい(Y)] ボタンをクリックします。または [Enter] キーを押下します。



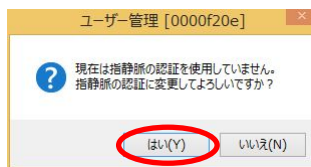
- ③ ログオフすると認証方式の変更が有効になります。

- ・ 再び指静脈認証方式に戻す場合

- ① 「ユーザー管理」画面のメニューバーから [ツール(T)] → [指静脈の認証方式へ変更(G)] をクリックします。



- ② 右の画面が表示されるので、[はい(Y)] ボタンをクリックします。または [Enter] キーを押下します。



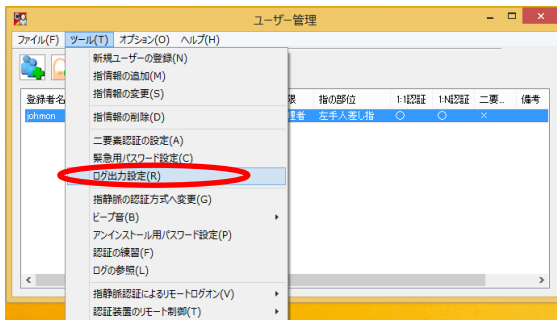
- ③ ログオフすると認証方式の変更が有効になります。

6.8 ログ出力設定

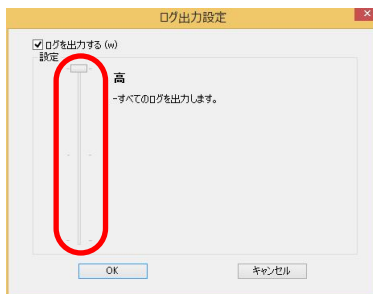
ログ出力のレベルを設定することができます。

本製品では、ログオン時やコンピュータのロック解除時等に、ログを Windows のイベントビューアへ出力することが可能です。

- ① 「ユーザー管理」画面のメニューバーから[ツール(T)]→[ログ出力設定(R)]をクリックします。



- ② 右の画面が表示されます。ログの出力レベルを変更したい場合は、スライダーバーで設定します。

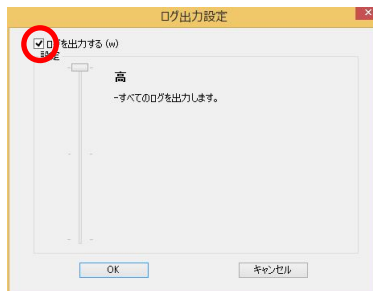


高：すべてのログを出力します。

中：ログオンやロック解除ではすべてのログを出力します。ユーザー管理機能では失敗のログを出力します。

低：ログオン失敗時やロック解除失敗時など、認証失敗のログのみ出力します。

- ③ ログを出力しない場合は、チェックボックスのチェックを外してください。

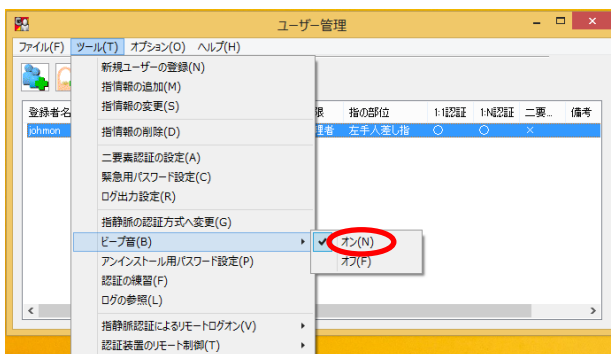


6.9 ビープ音の ON/OFF

認証装置のビープ音を鳴らすか鳴らさないかを設定することができます。認証装置は、認証を行う際にビープ音で状態を知らせます。

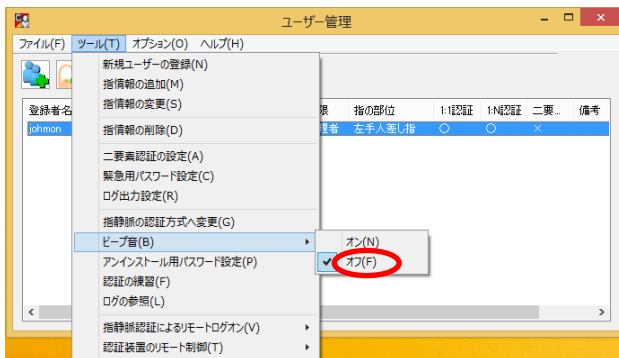
・ ビープ音を鳴らす場合

「ユーザー管理」画面のメニューバーから[ツール(T)] → [ビープ音(B)] → [オン(N)]をクリックします。



・ ビープ音を鳴らさない場合

「ユーザー管理」画面のメニューバーから[ツール(T)] → [ビープ音(B)] → [オフ(F)]をクリックします。

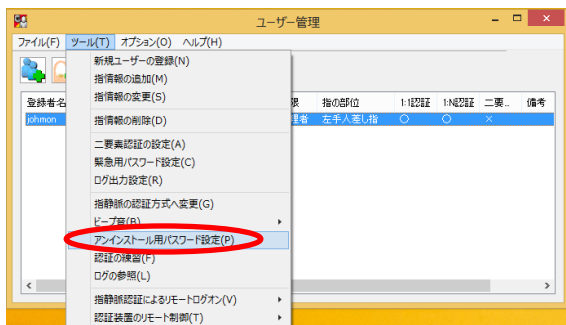


6.10 アンインストール用パスワードの設定

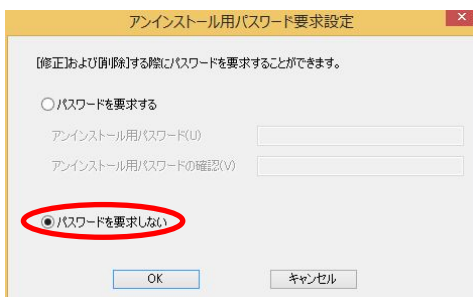
管理者以外が勝手にアンインストールできないように、アンインストール時にパスワードを要求するように設定することができます。

① 「ユーザー管理」

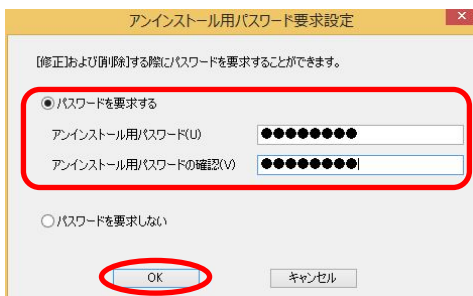
画面のメニューバーから[ツール(T)] → [アンインストール用パスワード設定(P)]をクリックします。



② 右の画面が表示されます。はじめはアンインストール用パスワードが設定されていないため、[パスワードを要求しない] がチェックされています。



③ [パスワードを要求する] をチェックし、エディットボックスにアンインストール用パスワードを入力します。127 文字まで入力することができます。入力後 [OK] ボタンをクリックします。



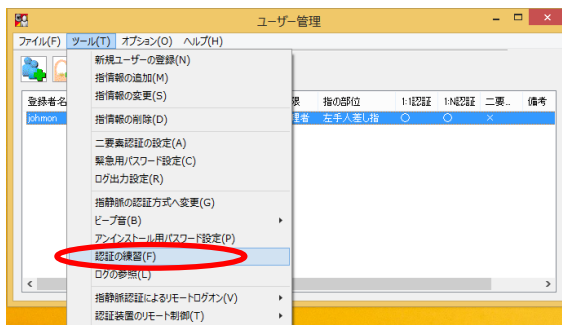
- ④ 右の画面が表示されますので [OK] ボタンをクリックしてください。



6.11 認証の練習

登録した指静脈に対して、認証の練習を行うことができます。

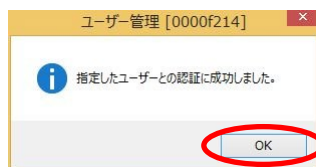
- ① 指情報リストビューから認証の練習をしたいユーザーを選択し、「ユーザー管理」画面のメニューバーから[ツール(T)] → [認証の練習(F)] をクリックします。



- ② 撮影画面が表示されるので、登録した指を置きます。



- ③ 「ビピッ」というビープ音が鳴り、状態表示 LED が緑の点灯に変わり、右の画面が表示されれば認証成功です。指を離して [OK] ボタンをクリックするか、[Enter] キーを押下します。



「ビピー」というビープ音が鳴り、状態表示

LED が赤の点灯に変わり、エラー画面が表示されれば認証失敗です。

10 秒以内に撮影が終わらない場合もビープ音が鳴りエラー画面が表示されます。ビープ音と状態表示 LED については「取扱説明書 ハードウェア編」の「2.1 認証装置の各部の名称と機能」を参照してください。

また、正しく認証がされない場合は本書巻末の「14 トラブルシューティング」を参照してください。

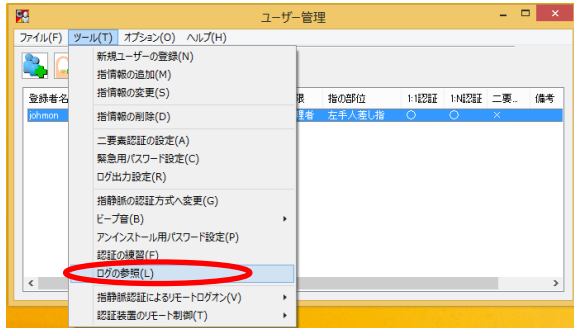
- ④ 認証装置のビープ音の設定を [OFF] にしている場合は、ビープ音は鳴りません。ビープ音の設定方法については「6.9 ビープ音の ON/OFF」を参照してください。

6.12 ログの参照

本製品が出力した Windows のイベントログを一覧表示できます。

[ユーザー管理] 画面のメニューバーから [ツール(T)] → [ログの参照(L)] をクリックします。

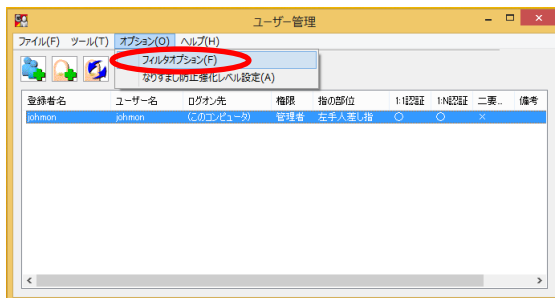
ログの参照については「7 ログの参照」を参照してください



6.13 フィルタオプションの設定

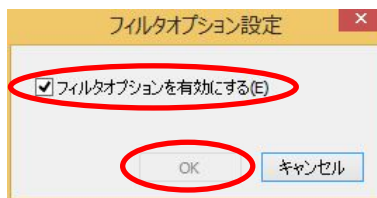
フィルタオプションの設定を行うことができます。

- ① [ユーザー管理] 画面のメニューバーから[オプション(O)] → [フィルタオプション(F)]をクリックします。



- ② 右の画面が表示されます。

「フィルタオプションを有効にする(E)」には現在の設定内容が反映されています(フィルタオプションが有効に設定されている場合にチェックされている状態になります)。



「フィルタオプションを有効にする(E)」をチェックして[OK]ボタンをクリックすると、フィルタオプションが有効になります。

「フィルタオプションを有効にする(E)」をチェックしないで[OK]ボタンをクリックすると、フィルタオプションが無効になります。

重要

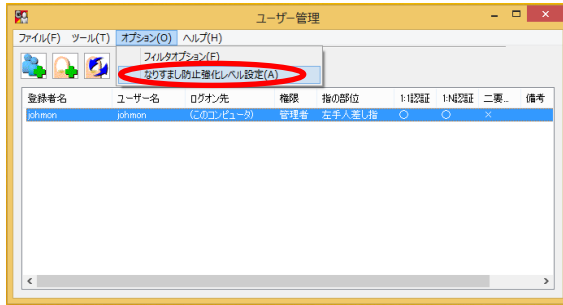
フィルタオプションを有効にすると、撮影したデータがフィルタリングされ、登録および認証に適さない状態のデータが使用できなくなります。フィルタオプションによって登録および認証ができなかった場合は、[14 トラブルシューティング]を参照してください。

登録および認証に適さない状態のデータが使用されることを防ぐため、フィルタオプションによって登録や認証がしにくくなるなどの理由が無い限りは、フィルタオプションを有効にして運用してください。

6.14 なりすまし防止強化レベル設定

なりすまし防止機能の強化レベルを設定することができます。

- ① 「ユーザー管理」画面のメニューバーから[オプション(O)] → [なりすまし防止強化レベル設定(A)] をクリックします。



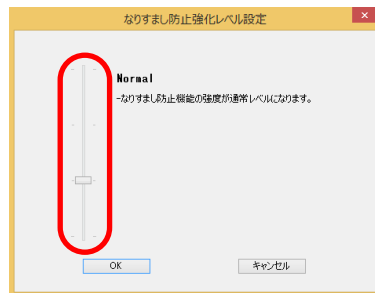
- ② 右の画面が表示されます。なりすまし防止強化レベルを変更したい場合は、スライダーバーで設定します。

Extend : なりすまし防止機能の強度が最も高くなります。

High : なりすまし防止機能の強度が通常レベルよりも高くなります。

Normal : なりすまし防止機能の強度が通常レベルになります。

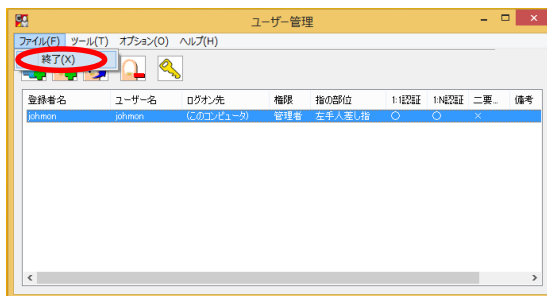
Low : なりすまし防止機能の強度が通常レベルよりも低くなります。



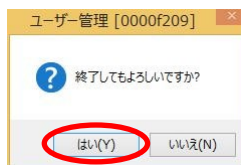
6.15 ユーザー管理画面の終了

ユーザー管理画面を終了するには以下の手順を実行してください。

- ① [ユーザー管理] 画面のメニューバーから[ファイル(F)] → [終了(X)] をクリックします。

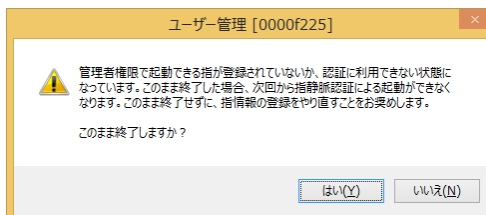


- ② 右の画面が表示されます。[はい(Y)] をクリックするとユーザー管理画面を終了します。



重要

ユーザー管理画面を終了する際に以下の画面が表示されることがあります。



この画面で[はい(Y)]をクリックしてユーザー管理画面を終了した場合、次回から指静脈認証によってユーザー管理画面を起動することができなくなります(緊急用パスワードによる起動は可能です)。

この画面が表示された場合は、やむを得ない場合を除き、必ず[いいえ(N)]をクリックしてユーザー管理画面に戻り、指情報の登録をやり直してください。

7 ログの参照

本製品のログのみを一覧表示で参照したい場合は、ユーザー管理機能からログの参照を選択します。以下の画面が表示されます。

[illegible]

ログの参照は以下の4つの方法で行うことができます。

- ・ ログオン関係のログ
- ・ 管理ログ
- ・ ログオン関係のログと管理ログ
- ・ リモート接続のログ

重要

本製品では、ログを Windows のアプリケーションログに出力します。設定によってはログが書き込まれなかったり、古いログが削除されたりします。Windows アプリケーションログの設定方法については Windows のヘルプを参照してください。

7.1 ログオン関係のログ

[ログオン関係のログ] ではログオン画面、Windows のセキュリティ画面、ロック画面で行った認証に関するログの一覧参照ができます。[日付、時刻、アカウント、コンピュータ、区分、ログ内容] の情報が表示されます。この情報を参照するには、[ログ情報] 画面のメニューバーから [表示(V)] → [ログ選択(L)] → [ログオン関係のログ(C)] をクリックします。



日付	時刻	アカウント	コンピュータ	区分	ログ内容
2022/10/11	18:22:12	WIN	Win81586	C	認証成功: 静脈認証に成功しました。Windowsへサインインします。(サ...
2022/10/11	19:22:00	NONE	Win81586	C	失敗: Windowsへサインインできませんでした。
2022/10/11	19:22:06	NONE	Win81586	C	成功: 緊急用パスワード認証に成功しました。
2022/10/11	19:22:08	NONE	Win81586	C	失敗: 緊急用パスワード認証に失敗しました。
2022/10/11	19:22:02	NONE	Win81586	C	認証失敗: Windowsへサインインできませんでした。
2022/10/11	19:20:34	NONE	Win81586	C	認証成功: 認証に成功しました。スクリーンロックを解除します。(サ...
2022/10/11	19:20:28	NONE	Win81586	C	認証失敗: スクリーンロックを解除できませんでした。
2022/10/11	19:19:38	NONE	Win81586	C	認証成功: 認証に成功しました。スクリーンロックを解除します。(サ...

重要

Windows 10 または Windows 11 では、Windows のグループポリシーの「ユーザーの簡易切り替え」の設定によって、ログオン画面とロック画面の認証を区別せずに、どちらもログオン画面の認証のログとして出力される場合があります。

7.2 管理ログ

「管理ログ」ではユーザー管理機能で行った認証、撮影に関するログの一覧参照ができます。[日付、時刻、アカウント、コンピュータ、区分、ログ内容]の情報が表示されます。この情報を参照するには、[ログ情報]画面のメニューバーから[表示(Y)] → [ログ選択(L)] → [管理ログ(M)]をクリックします。



7.3 ログオン関係のログと管理ログ

「ログオン関係のログと管理ログ」ではログオン関係のログ、管理ログ両方のログの一覧参照ができます。[日付、時刻、アカウント、コンピュータ、区分、ログ内容]の情報が表示されます。この情報を参照するには、[ログ情報]画面のメニューバーから[表示(V)]→[ログ選択(L)]→[ログオン関係のログと管理ログ(B)]をクリックします。

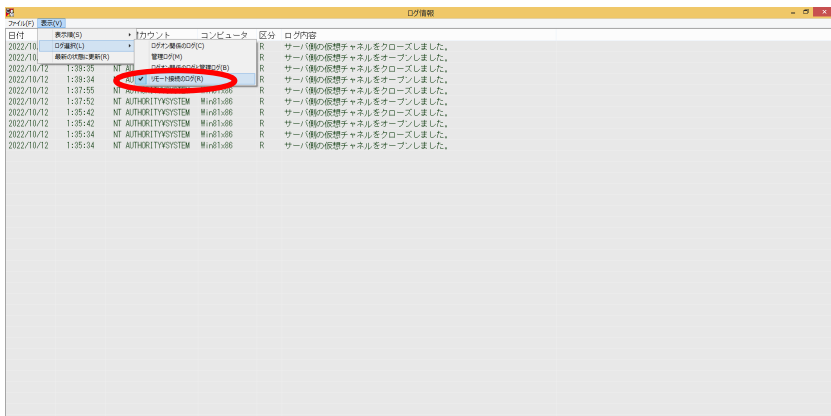
ログ情報			
ファイル	表示(V)		
日付	表示欄(S)	イベント	コンピュータ 区分 ログ内容
2022/10/10	09:00:11	...	ログファイルの作成(C)
2022/10/10	09:00:11	...	管理者 ユーザー管理機能の起動時認証に成功しました。(00001611)
2022/10/10	09:00:11	...	管理者 ユーザー名を認識できませんでした。または静かな認証に失敗しました。...
2022/10/10	09:00:11	...	警告: 静かな認証に成功しました。Windowsサインインします。(サ...
2022/10/10	09:25:02	...	失敗: Windowsサインインできませんでした。
2022/10/10	09:25:05	...	終了時処理 正常に終了しました。(00001610)
2022/10/10	09:25:07	Win81-888... Win81-888	M 管理者 ユーザー管理機能の起動時認証に成功しました。(00001611)
2022/10/10	09:25:10	Win81-888... Win81-888	M 緊急用/パスワード認証 ユーザー管理機能の起動時認証に成功しました...
2022/10/10	09:25:10	Win81-888... Win81-888	M 緊急用/パスワード認証 緊急用/パスワードの認証に失敗しました。(000...
2022/10/10	09:24:51	Win81-888... Win81-888	M 終了時処理 正常に終了しました。(00001610)
2022/10/10	09:24:38	Win81-888... Win81-888	M 起動時認証 ユーザー管理機能の起動時認証に成功しました。(00001611)
2022/10/10	09:24:29	Win81-888... Win81-888	M 起動時認証 ユーザー名を認識できませんでした。または静かな認証に失敗し...
2022/10/10	09:22:12	NONE Win81-888	C 認証成功: 緊急用/パスワード認証に成功しました。
2022/10/10	09:22:08	NONE Win81-888	C 認証失敗: 緊急用/パスワード認証に失敗しました。
2022/10/10	09:22:06	NONE Win81-888	C 認証失敗: 緊急用/パスワード認証に失敗しました。
2022/10/10	09:22:02	NONE Win81-888	C 認証失敗: Windowsサインインできませんでした。
2022/10/10	09:20:34	NONE Win81-888	C 認証成功: 認証に成功しました。スクリーンロックを解除します。(サ...
2022/10/10	09:20:28	NONE Win81-888	C 認証失敗: スクリーンロックを解除できませんでした。
2022/10/10	09:19:38	NONE Win81-888	C 認証成功: 認証に成功しました。スクリーンロックを解除します。(サ...
2022/10/10	09:17:28	Win81-888... Win81-888	M 初回管理者登録 登録に成功しました。 ログオン先:(このコンピ...
2022/10/10	09:05:29	Win81-888... Win81-888	M 終了時処理 正常に終了しました。(00001610)
2022/10/10	09:05:27	Win81-888... Win81-888	M アンインストール用/パスワードの検定 アンインストール用/パスワード...
2022/10/10	09:05:14	Win81-888... Win81-888	M 初回管理者登録 登録に成功しました。 ログオン先:(このコンピュ...

重要

Windows 10 または Windows 11 では、Windows のグループポリシーの「ユーザーの簡易切り替え」の設定によって、ログオン画面とロック画面の認証を区別せずに、どちらもログオン画面の認証のログとして出力される場合があります。

7.4 リモート接続のログ

[リモート接続のログ]ではリモート接続に関するログの一覧参照ができます。[日付、時刻、アカウント、コンピュータ、区分、ログ内容]の情報が表示されます。この情報を参照するには、[ログ情報]画面のメニューバーから[表示(Y)] → [ログ選択(L)] → [リモート接続のログ(R)]をクリックします。



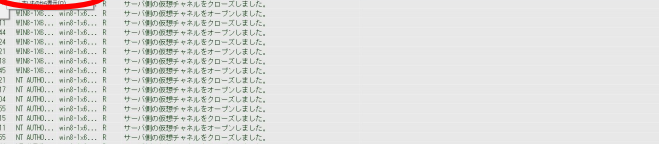
日付	時刻	アカウント	コンピュータ	区分	ログ内容
2022/10/12	1:37:35	NT AUTHORITY\SYSTEM	Win81-686	R	サーバ側の仮想チャネルをクローズしました。
2022/10/12	1:37:35	NT AUTHORITY\SYSTEM	Win81-686	R	サーバ側の仮想チャネルをオープンしました。
2022/10/12	1:37:35	NT AUTHORITY\SYSTEM	Win81-686	R	サーバ側の仮想チャネルをクローズしました。
2022/10/12	1:37:35	NT AUTHORITY\SYSTEM	Win81-686	R	サーバ側の仮想チャネルをオープンしました。
2022/10/12	1:37:35	NT AUTHORITY\SYSTEM	Win81-686	R	サーバ側の仮想チャネルをクローズしました。
2022/10/12	1:37:35	NT AUTHORITY\SYSTEM	Win81-686	R	サーバ側の仮想チャネルをオープンしました。
2022/10/12	1:37:35	NT AUTHORITY\SYSTEM	Win81-686	R	サーバ側の仮想チャネルをクローズしました。
2022/10/12	1:37:35	NT AUTHORITY\SYSTEM	Win81-686	R	サーバ側の仮想チャネルをオープンしました。
2022/10/12	1:37:35	NT AUTHORITY\SYSTEM	Win81-686	R	サーバ側の仮想チャネルをクローズしました。
2022/10/12	1:37:35	NT AUTHORITY\SYSTEM	Win81-686	R	サーバ側の仮想チャネルをオープンしました。

7.5 テキスト形式での出力

表示しているログ情報をテキストファイルに書き出すことができます。この機能を使用するには[ファイル(F)] → [テキスト形式で出力(S)]をクリックします。

7.6 その他の機能

- 表示順の変更
 - 一覧表示しているログを時系列に昇順、降順に並び替えることができます。
 - [表示(Y)] → [表示順(S)] とクリックし、[新しいものから表示(N)] [古いものから表示(O)] のどちらか希望する方をクリックします。



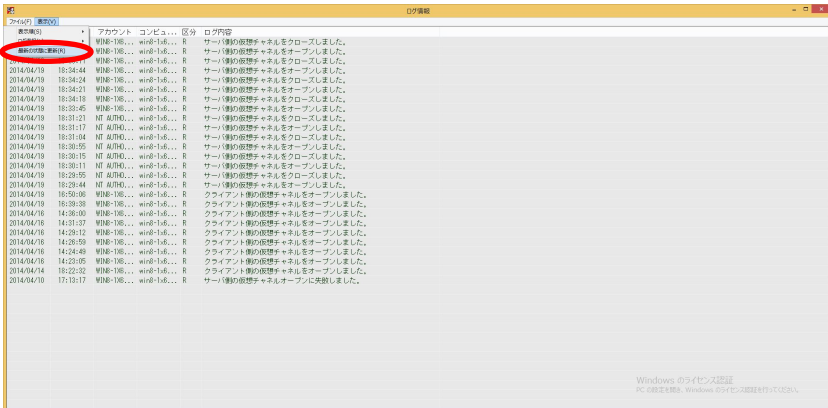
The screenshot displays the Windows Event Viewer interface. The left-hand pane shows the 'Security' log selected under 'Windows Logs'. The main pane displays a list of security events. A red circle highlights the 'Security' column header. The list includes events such as 'Successful logon' (Event ID 4624) and 'Password change' (Event ID 4725). The 'Source' column shows 'Microsoft Windows' and the 'Task Category' column shows 'Security'.

日時	レベル	ソース	タスクカテゴリ	ID	メッセージ
2014/04/09 18:35:11	情報	Microsoft Windows	Security	4624	Successful logon
2014/04/09 18:34:44	情報	Microsoft Windows	Security	4624	Successful logon
2014/04/09 18:34:24	情報	Microsoft Windows	Security	4624	Successful logon
2014/04/09 18:34:18	情報	Microsoft Windows	Security	4624	Successful logon
2014/04/09 18:33:45	情報	Microsoft Windows	Security	4624	Successful logon
2014/04/09 18:31:21	情報	Microsoft Windows	Security	4624	Successful logon
2014/04/09 18:31:17	情報	Microsoft Windows	Security	4624	Successful logon
2014/04/09 18:31:04	情報	Microsoft Windows	Security	4624	Successful logon
2014/04/09 18:30:55	情報	Microsoft Windows	Security	4624	Successful logon
2014/04/09 18:30:15	情報	Microsoft Windows	Security	4624	Successful logon
2014/04/09 18:30:11	情報	Microsoft Windows	Security	4624	Successful logon
2014/04/09 18:29:55	情報	Microsoft Windows	Security	4624	Successful logon
2014/04/09 18:29:44	情報	Microsoft Windows	Security	4624	Successful logon
2014/04/09 18:29:08	情報	Microsoft Windows	Security	4624	Successful logon
2014/04/09 18:28:38	情報	Microsoft Windows	Security	4624	Successful logon
2014/04/09 18:28:00	情報	Microsoft Windows	Security	4624	Successful logon
2014/04/09 18:21:37	情報	Microsoft Windows	Security	4624	Successful logon
2014/04/09 18:20:52	情報	Microsoft Windows	Security	4624	Successful logon
2014/04/09 18:20:59	情報	Microsoft Windows	Security	4624	Successful logon
2014/04/09 18:24:48	情報	Microsoft Windows	Security	4624	Successful logon
2014/04/09 18:22:05	情報	Microsoft Windows	Security	4624	Successful logon
2014/04/09 18:22:32	情報	Microsoft Windows	Security	4624	Successful logon
2014/04/09 17:31:37	情報	Microsoft Windows	Security	4624	Successful logon

- ・ 最新の情報に更新

読み込み直し、最新のログを表示します。

[表示(V)] → [最新の状態に更新(R)] をクリックします。



8 緊急用パスワードの利用

認証装置の故障や認証装置が接続されていない場合等の理由でWindowsに復帰できなくなった場合やスクリーンセーバーのロック解除ができなくなった場合に、緊急用パスワードを用いてログオンすることができます。

8.1 Windows Server 2012 / Windows 8.1 / Windows Server 2012 R2 のログオン・ロック解除の場合

緊急用パスワードは右の画面のようにユーザーが選択されている場合に利用できます。



上記の場合に、[Ctrl] キーと [Alt] キーと [q] キーを同時に押下することによって、右の画面が表示されます。緊急用パスワードを入力します。

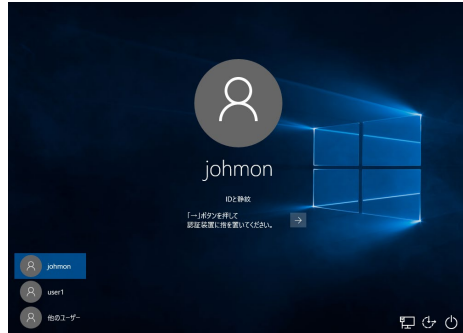
[→] ボタンをクリックすると、Windows のユーザー名とパスワードの認証画面が表示されます。



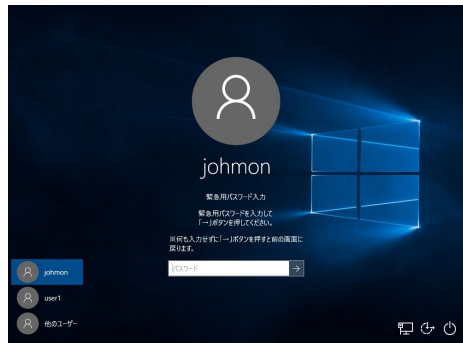
8.2 Windows 10 / Windows Server 2016 / Windows Server 2019 /

Windows 11 のログイン・ロック解除の場合

緊急用パスワードは右の画面のようにユーザーが選択されている場合に利用できます。



上記の場合に、[Ctrl] キーと [Alt] キーと [q] キーを同時に押下することによって、右の画面が表示されます。緊急用パスワードを入力します。
[→] ボタンをクリックすると、Windows のユーザー名とパスワードの認証画面が表示されます。



8.3 ユーザー管理機能のロック解除の場合

緊急用パスワードは右の認証前の画面が表示されている場合に利用できます。



上記の場合に、[Ctrl] キーと [Alt] キーと [q] キーを同時に押下することによって、右の画面が表示されます。緊急用パスワードを入力します。



[OK] ボタンをクリックすると、ユーザー管理機能が起動します。

重要

- 緊急用パスワードを用いてログオンした場合、ロック解除の画面は Windows 標準の認証方式になります。指静脈認証を用いてログオンした場合のみ、ロック解除画面で指静脈認証方式を利用できます。
- Windows 10 または Windows 11 では、緊急用パスワードでログオンした場合に、ロック解除の動作が Windows のグループポリシーの設定によって変わることがあります。グループポリシーの「ユーザーの簡易切り替え」の設定によって、ロック解除が Windows 標準の認証方式になる場合と、指静脈認証方式になる場合があります。

9 Windows パスワードの変更

Windows パスワードの変更に関する内容を記します。

重要

ユーザーのパスワード変更を Windows のコントロールパネルから行わないでください。必ず、本章「9 Windows パスワードの変更」から行ってください。

コントロールパネルからパスワードを変更した場合、指静脈認証ソフトウェアで管理しているパスワードと整合性が取れなくなりログオンできなくなります。

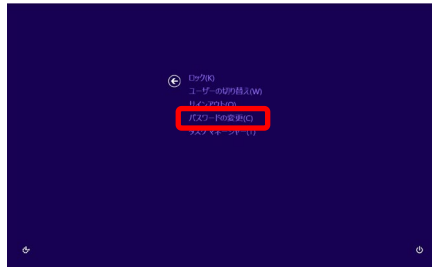
- パスワードの長さに関して

Windows ではパスワード 0 文字（パスワード無し）を許可していますが、本製品では許可していません。必ず 1 文字以上で登録してください。

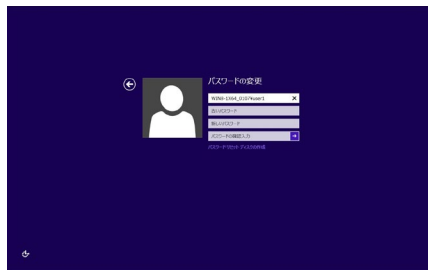
パスワード入力は 255 文字まで入力できますが、入力文字数は 127 文字以下にしてください。128 文字以上入力した場合は、本書「6.3 指情報の変更」のパスワード確認でエラーになります。

9.1 Windows Server 2012 / Windows 8.1 / Windows Server 2012 R2 をお使いの場合

ユーザーのパスワードを変更する場合には[Ctrl] キーと [Alt] キーと [Del] キーを同時に押下することによって表示される右の画面からパスワードを変更します。
[パスワードの変更(C)] ボタンをクリックします。



以下の画面が表示されます。



ユーザー名・・・・・・ ログオンユーザーのユーザー名です。(※1) (※2)
古いパスワード・・ 現在の Windows ログオン用のパスワードを入力します。
新しいパスワード・・ 新しい Windows ログオン用のパスワードを入力します。

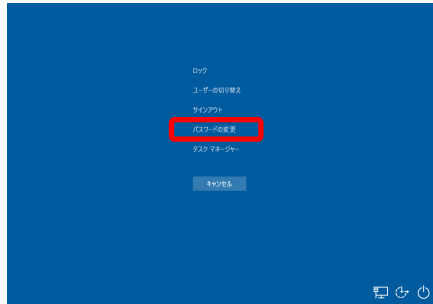
※1 Active Directory の環境下で動作している場合、ユーザー名をユーザプリンシパル名 (UPN) 形式での入力を行うことができます。ユーザー名にはまず UPN プレフィックスを入力します。続けて「@」が入力された時点で「ログオン先」のダイアログボックスが無効化されますので、UPN サフィックスの部分を入力します。

※2 Microsoft アカウントでサインインしている場合、Windows パスワードを変更できません。

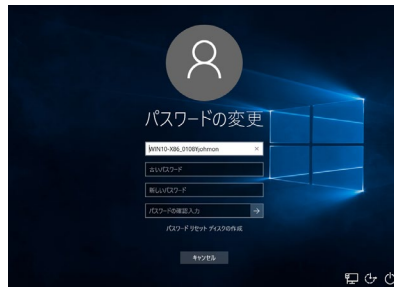
以上の情報を入力して [→] ボタンをクリックすると、Windows ログオン用のパスワードを変更することができます。

9.2 Windows 10 / Windows Server 2016 / Windows Server 2019 / Windows 11 をお使いの場合

ユーザーのパスワードを変更する場合には[Ctrl] キーと [Alt] キーと [Del] キーを同時に押下することによって表示される右の画面からパスワードを変更します。
[パスワードの変更(C)] ボタンをクリックします。



以下の画面が表示されます。



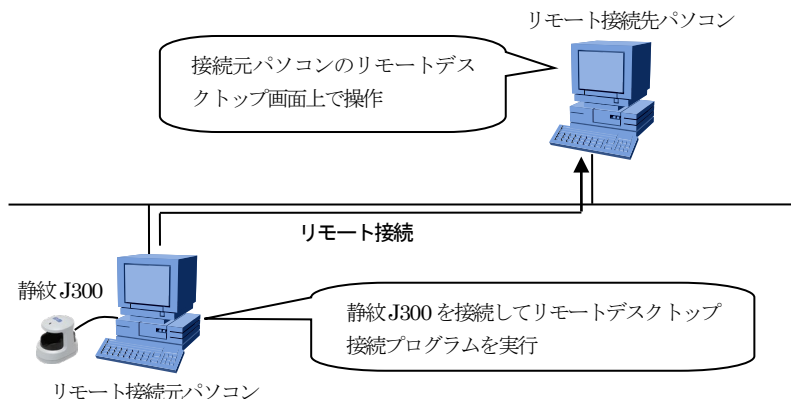
- ユーザー名・・・・・・ ログオンユーザーのユーザー名です。(※1) (※2)
古いパスワード・・・・・ 現在の Windows ログオン用のパスワードを入力します。
新しいパスワード・・・・・ 新しい Windows ログオン用のパスワードを入力します。

- ※1 Active Directory の環境下で動作している場合、ユーザー名をユーザプリンシパル名 (UPN) 形式での入力を行うことができます。ユーザー名にはまず UPN プレフィックスを入力します。続けて「@」が入力された時点で「ログオン先」のダイアログボックスが無効化されますので、UPN サフィックスの部分を入力します。
※2 Microsoft アカウントでサインインしている場合、Windows パスワードを変更できません。

以上の情報を入力して [→] ボタンをクリックすると、Windows ログオン用のパスワードを変更することができます。

10 リモートデスクトップ環境で使用するための設定

本製品がインストールされているパソコンへリモート接続して、本製品の各機能を使用することができます。また、リモートログオンの認証を指静脈認証方式で行うことができます。



リモートデスクトップ環境で本製品を使用するためには、リモート接続先パソコンと、リモート接続元パソコンとで、それぞれ設定を行う必要があります。設定は以下の手順で行ってください。

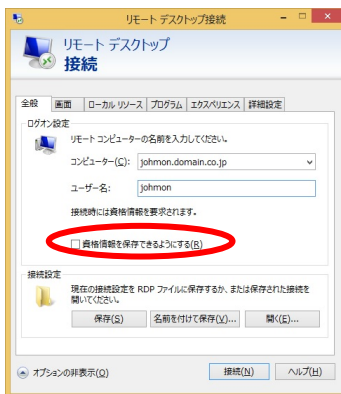
1. リモート接続元パソコンに本製品をインストールします
 2. リモート接続元パソコンで必要な設定を行います(ユーザーごとに実施)
 3. リモート接続先パソコンに本製品をインストールします
 4. リモート接続先パソコンで初回時管理者登録を行います
 5. リモート接続先パソコンで必要な設定を行います
 6. リモート接続先パソコンでリモートログオンの設定を行います(※)
- ※ リモートログオン時認証を指静脈で行いたい場合にのみ実施してください

なお、上記手順3～6については、リモート接続元パソコンからリモートログオンした状態で行うことができます。

上記の各手順について以下で説明します。

重要

- ・ リモート接続した状態で更に別のパソコンへリモート接続した場合、指静脈認証や指情報の登録が行えなくなりますのでご注意ください。
- ・ リモートデスクトップ接続プログラムを実行する際には、必ず「資格情報を保存できるようにする」チェックボックスをオフにしてください。このチェックボックスをオンにした場合、リモートログオンに失敗する可能性があります。



- ・ リモートデスクトップ環境において指静脈認証や指情報の登録を行っている途中で、リモート接続を終了しないでください。指静脈認証ソフトウェアの動作が不安定になり、パソコンの再起動が必要になる可能性があります。
- ・ リモートデスクトップ環境において指静脈認証や指情報の登録を行っている途中で、指静脈認証ソフトウェアが異常終了した場合、指静脈認証ソフトウェアを再起動しても指静脈認証や指情報の登録が行えなくなる場合があります。その場合は、一度リモートデスクトップ接続プログラムを終了し、再度リモートデスクトップ接続プログラムを実行してください。
- ・ リモート接続先にインストールする本製品と、リモート接続元にインストールする本製品とは、必ずバージョンを合わせてください。本製品のバージョンが異なる場合、認証装置が正しく動作しない可能性があります。
- ・ Windows 10 または Windows 11 で指静脈認証方式によるリモートデスクトップ接続をご使用になる場合、ネットワークの伝送状況によっては接続エラーとなる場合があります。

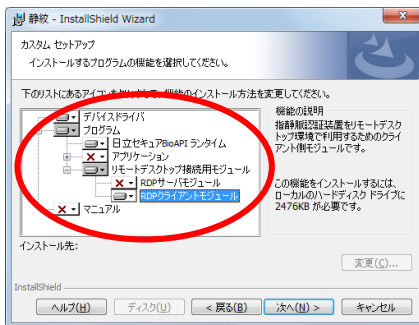
10.1 リモート接続元パソコンに本製品をインストール

リモート接続元パソコンに本製品をインストールします。既にインストールされている場合は、本手順は不要です。

インストールの方法は、[2 ソフトウェアのインストール]を参照してください。

インストールの途中、セットアップのタイプを選択する画面で「カスタム」を選択した場合は、インストールするソフトウェアを選択することができますが、その場合は少なくとも以下のソフトウェアを選択してください。

- ・ デバイスドライバ
- ・ 日立セキュア BioAPI ランタイム
- ・ RDP クライアントモジュール



10.2 リモート接続元パソコンで必要な設定

リモート接続元パソコンで必要な設定を行います。以下の手順を実行してください。

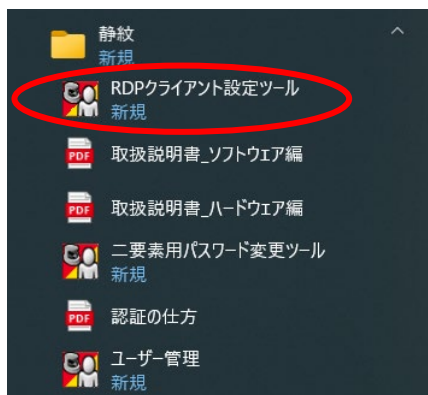
重要

- リモート接続元パソコンでの設定は、リモート接続を行うユーザーごとに実行する必要があります。あるユーザーで設定を行った後でも、別のユーザーでログインしてリモート接続を行う場合には、再度設定を行ってください。

- ① Windows Server 2012 / Windows 8.1 / Windows Server 2012 R2 をお使いの場合、[スタート] → [アプリ] → [静紋] → [RDP クライアント設定ツール] をクリックします。



Windows 10 / Windows Server 2016 / Windows Server 2019 / Windows 11 をお使いの場合、スタートメニューから、[すべてのアプリ] → [静紋] → [RDP クライアント設定ツール] をクリックします。

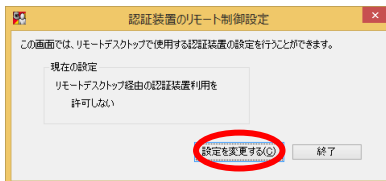


重要

- RDP クライアント設定ツールを実行する際に、「別のユーザーとして実行」や「管理者として実行」などは用いしないでください。それらを用いて実行した場合、設定が正しく行われない可能性があります。

- ② 右の設定画面が表示されます。

[現在の設定]が[リモートデスクトップ経由の認証装置利用を許可する]であった場合は、そのまま[終了]をクリックして終了します。



[現在の設定]が[リモートデスクトップ経由の認証装置利用を許可しない]であった場合は、[設定を変更する(C)]をクリックします。

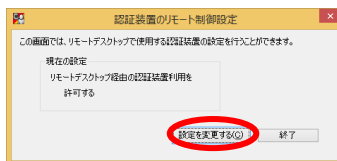
- ③ メッセージを確認し、[はい(Y)]をクリックします。



- ④ メッセージを確認し、[OK]をクリックします。



- ⑤ 設定画面が再度表示されます。[現在の設定]が[リモートデスクトップ経由の認証装置利用を許可する]に変更されていることを確認し、[終了]をクリックして終了します。



重要

- RDP クライアント設定ツールで設定を変更した後は、必ず一度リモートデスクトップ接続プログラムを終了してください。リモートデスクトップ接続プログラムを終了しない場合、設定の変更が反映されません。

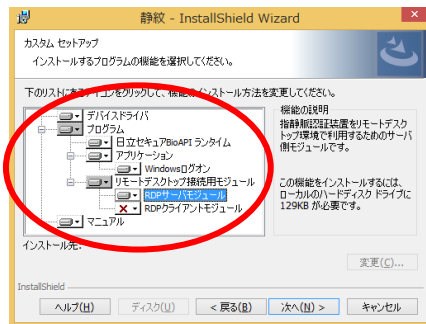
10.3 リモート接続先パソコンに本製品をインストール

リモート接続先パソコンに本製品をインストールします。既にインストールされている場合は、本手順は不要です。

インストールの方法は、[2 ソフトウェアのインストール]を参照してください。

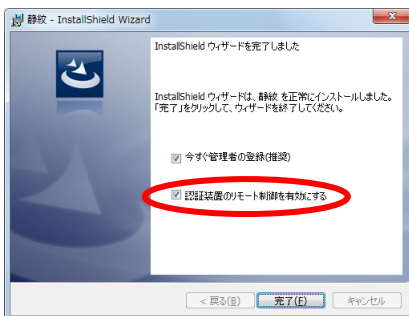
インストールの途中、セットアップのタイプを選択する画面で「カスタム」を選択した場合は、インストールするソフトウェアを選択することができますが、その場合は少なくとも以下のソフトウェアを選択してください。

- 日立セキュア BioAPI ランタイム
- RDP サーバモジュール
- Windows ログオン



ただし、[11.4 リモート接続先パソコンで初回時管理者登録を実行]をリモートログオンした状態で行わない場合(ローカルログオンした状態で行う場合は、上記のソフトウェアに加えて、「デバイスドライバ」も選択してください。

また、インストールの完了画面で[認証装置のリモート制御を有効にする]をチェックしてから[完了]をクリックして終了した場合、リモート接続先パソコンで必要な設定が自動的に行われます。その場合は、[11.5 リモート接続先パソコンで必要な設定]を行う必要はありません。



10.4 リモート接続先パソコンで初回時管理者登録を実行

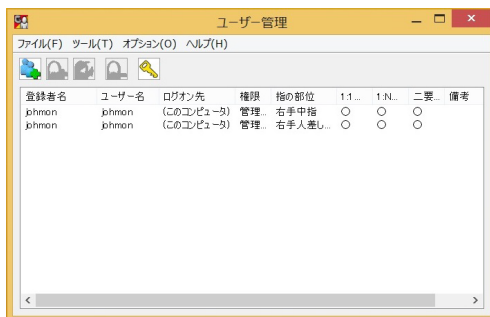
リモート接続先パソコンで初回時管理者登録を行います。既に登録済みの場合は、本手順は不要です。

初回時管理者登録の方法は、[3 初回時管理者登録]を参照してください。

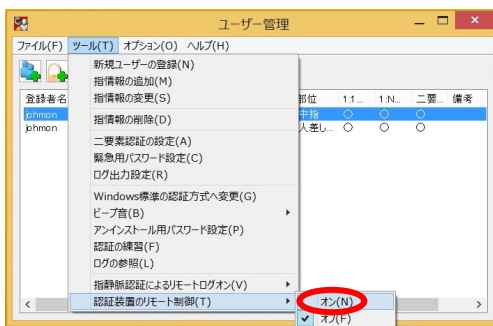
10.5 リモート接続先パソコンで必要な設定

リモート接続先パソコンで必要な設定を行います。以下の手順を実行してください。

- ① [6 ユーザー管理機能]の
手順に従い、ユーザー管
理機能を起動します。



- ② [ユーザー管理] 画面の
メニューバーから[ツ
ール (T)] → [認証装置
のリモート制御(T)] →
[オン(N)]をクリックし
ます。



10.6 リモート接続先パソコンで行うリモートログオン設定

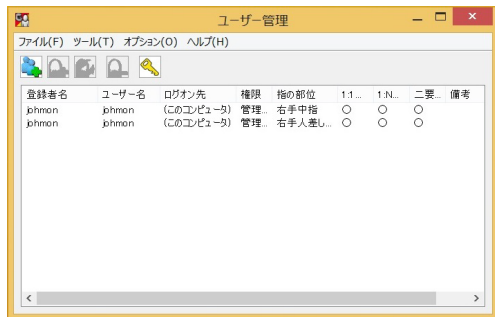
リモートログオン時の認証を指静脈認証方式に変更するための設定を行います。また、リモートログオン時の認証を Windows 標準の認証方式に戻すこともできます。

リモートログオン時の認証を指静脈認証方式にする必要がない場合は、本手順は不要です。

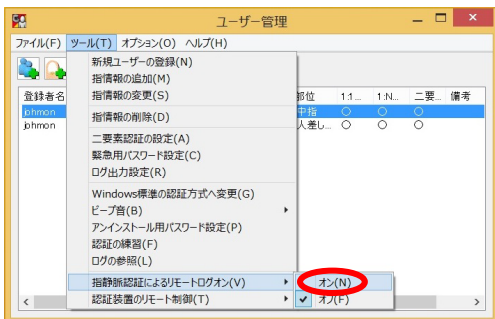
この設定はリモート接続先パソコンで実行します。以下の手順を実行してください。

- ・ リモートログオン時の認証を指静脈認証方式に変更する場合

- ① [6 ユーザー管理機能]の手順に従い、ユーザー管理機能を起動します。

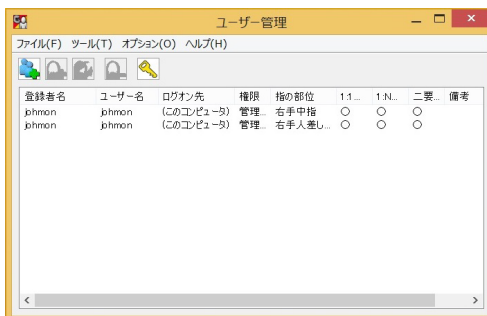


- ② 「ユーザー管理」画面のメニューバーから[ツール(T)] → [指静脈認証によるリモートログオン(V)] → [オン(N)]をクリックします。

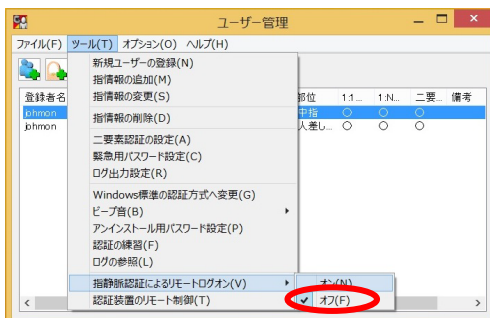


- ・ リモートログオン時の認証を Windows 標準の認証方式に戻す場合

- ① [ユーザー管理機能] の手順に従い、ユーザー管理機能を起動します。



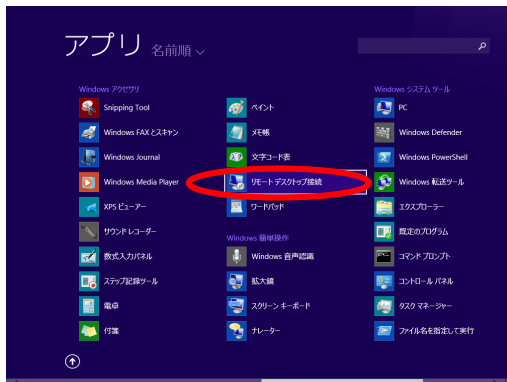
- ② 「ユーザー管理」画面のメニューバーから[ツール (T)] → [指静脈認証によるリモートログオン (V)] → [オフ (F)] をクリックします。



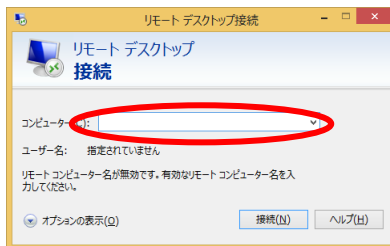
10.7 リモートログオンの実行

これまでに説明した設定を行った上でリモート接続を行うと、指静脈認証によるリモートログオンを行うことができます。以下に、指静脈認証によるリモートログオンの手順を示します。

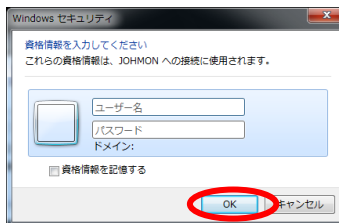
- ① リモート接続元パソコンで、Windows に付属のリモートデスクトップ接続プログラムを起動します。



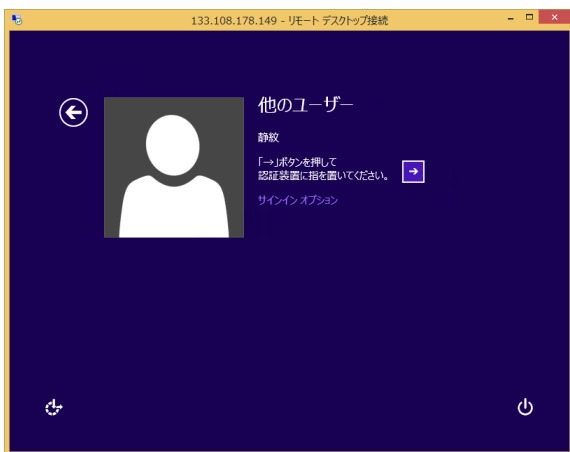
- ② リモート接続先パソコンのコンピュータ名を入力し、[接続(N)]をクリックします。



- ③ お使いのリモートデスクトップ接続プログラムのバージョンや設定によっては、右のような画面が表示されますので、ユーザー名とパスワードを入力して[OK]をクリックします。



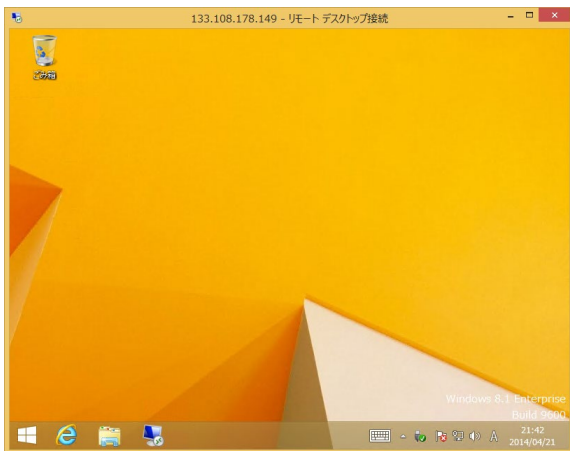
- ④ 指静脈認証によるログオン画面が表示されます。
[5 認証機能]と同様の手順で指静脈認証によるログオンを実行します。



重要

- リモートログオンでも緊急用パスワードを利用することができます。ただし [8.1 Windows Server 2012 / Windows 8.1 / Windows Server 2012 R2 のログオン・ロック解除の場合]とは異なり、リモートログオンの場合は、緊急用パスワードを用いた場合でも、ロック解除画面は指静脈認証方式になります。

- ⑤ ログオンに成功するとリモートデスクトップの画面が表示されます。



11 二要素用パスワードの変更

二要素認証で使用するための二要素用パスワードを Users グループ権限のユーザーで変更することができます。

以下に、二要素用パスワードの変更の手順を示します。

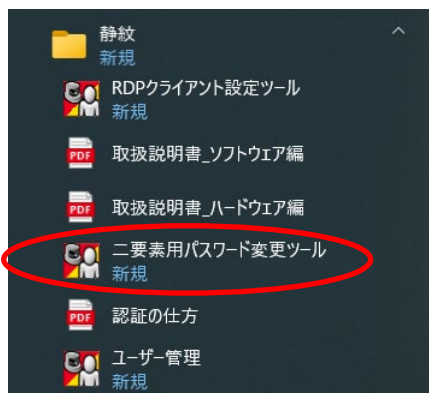
- ① ・Windows Server 2012 / Windows 8.1 / Windows Server 2012 R2 をお使いの場合

スタートメニューから、[スタート] → [アプリ] → [二要素用パスワード変更ツール]をクリックします。



- ・Windows 10 / Windows Server 2016 / Windows Server 2019 / Windows 11 をお使いの場合

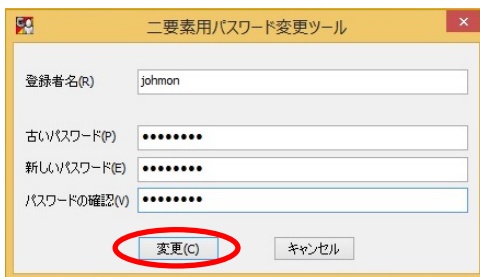
スタートメニューから、[すべてのアプリ] → [静紋] → [二要素用パスワード変更ツール]をクリックします。



② 右の画面が表示されます。



③ [登録者名(R)], [古いパスワード(P)], [新しいパスワード(E)], [パスワードの確認(Y)]を入力し、[変更(C)]ボタンをクリックします。



登録者名・・・・・・・・登録者名を入力します。

古いパスワード・・・・・・・・変更前の二要素用パスワードを入力します。127 文字まで入力することができます。

新しいパスワード・・・・・・変更後の二要素用パスワードを入力します。127 文字まで入力することができます。

パスワードの確認・・・・・・確認のための変更後の二要素用パスワードを入力します。127 文字まで入力することができます。

重要

- 二要素用パスワード変更ツールを起動するためには、あらかじめ二要素用パスワードを使用した二要素認証の設定を有効にしておく必要があります。
- 二要素用パスワードは8文字以上の条件を満たす必要があります。

12 ソフトウェア仕様

適応パソコン	機種	PC/AT 互換機
	CPU	各 OS で規定されているシステム要件に準じます
	メモリ	各 OS で規定されているシステム要件に準じます ※インストールされているソフトウェアなど、ご使用の環境によっては、最小メモリ所要量より多くのメモリ容量が必要になる場合があります
	HDD	空き容量：50MB 以上 ※1
	インターフェース	USB2.0/1.1 ※4
対応 OS		[32 ビット OS] Windows 8.1 Update 無印 / Pro / Enterprise Windows 10 Enterprise 2016 LTSC (Version 1607 相当) Windows 10 Enterprise LTSC 2019 (Version 1809 相当) Windows 10 Home / Pro / Enterprise Version 21H1 Windows 10 Home / Pro / Enterprise Version 21H2 Windows 10 Enterprise LTSC 2021 (Version 21H2 相当) [64 ビット OS] Windows Server 2012 Standard Windows 8.1 Update 無印 / Pro / Enterprise Windows Server 2012 R2 Update Standard Windows 10 Enterprise 2016 LTSC (Version 1607 相当) Windows 10 Enterprise LTSC 2019 (Version 1809 相当) Windows 10 Home / Pro / Enterprise Version 21H1 Windows 10 Home / Pro / Enterprise Version 21H2 Windows 10 Enterprise LTSC 2021 (Version 21H2 相当) Windows Server 2016 Standard Windows Server 2019 Standard Windows 11 Home / Pro / Enterprise Version 21H2 Windows 11 Home / Pro / Enterprise Version 22H2 ※いずれも日本語版のみ
対応ドメイン		Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
対応リモートデスクトップ接続プログラム		シェルバージョン 6.0 ～ 10.0.22621 コントロールバージョン 6.0 ～ 10.0.22621 リモートデスクトッププロトコル 6.0 ～ 10.11
認証	登録指数	最大 100 指 (管理者 : 1～100 指) (一般ユーザー : 最大 99 指)
	認証時間 ※2	USB2.0 接続時 : 約 2 秒 ※3 USB1.1 接続時 : 約 4 秒
機能		・Windows ログオンおよびスクリーンセーバーロック解除時の指静脈による認証

※1 登録する指の数により必要な空き容量は変動します。

※2 認証開始から認証終了までの時間

(指を置いて撮影が可能になってからの時間です。指の置き方によっては認証時間が長くなる場合があります。)

※3 撮影終了から認証終了までの時間は1秒以下です。

(バックグラウンドの処理によっては時間が掛かる場合があります。)

※4 USB1.1 では一部のパソコンで動作しない場合があります。

USB1.1 はUSB2.0 と比べて転送速度が遅いため、認証時間が遅くなります。

パソコンのUSB2.0 のポートにUSB1.1 のハブを経由して使用しないでください。

13 トラブルシューティング

システムの運用中になんらかのトラブルが発生した場合には、下記静紋テクニカルサポート窓口にご相談する前にトラブルシューティングをご覧ください。

明らかにハードウェア障害と思われる場合は、ご購入先にご連絡ください。

静紋テクニカルサポート窓口

E-Mail : johmon-support@hitachi-solutions.com

以下のウェブサイトにて最新の製品情報を掲載しております。併せてご参照ください。

日立ソリューションズ「静紋」ホームページ

<https://www.hitachi-solutions.co.jp/johmon/>

※上記 URL は予告なしに変更される場合があります。上記 URL が見つからない場合は、弊社ホームページ(<https://www.hitachi-solutions.co.jp/>)よりアクセスしてください。

■ 認証装置に USB ケーブルを繋いだが、状態表示 LED が緑点灯しない

USB ケーブルを繋いだが、状態表示 LED が点灯しない場合は、次の原因が考えられます。

- ・ 認証装置用のドライバが正しく組み込まれていない
→ 「2.6 ドライバインストールの確認」を参照して、お使いのパソコンに正しくドライバが組み込まれているかを確認してください。
- ・ お使いのパソコンの USB ポートが誤動作した
→ お使いのパソコンを再起動してください。
- ・ ハードウェアの故障が考えられます
→ ご購入先、または本書「1.1 お問い合わせ先」の静紋テクニカルサポート窓口にご連絡ください。

■ 認証開始時や認証完了時にビーブ音が鳴らない

- ・ ビーブ音の設定が OFF になっていないかを確認してください
→ ビーブ音の設定方法については、本書「6.9 ビーブ音の ON/OFF」を参照してください。
- ・ ハードウェアの故障が考えられます
→ ご購入先、または本書「1.1 お問い合わせ先」の静紋テクニカルサポート窓

口にご連絡ください。

■ 指情報の登録に失敗する

「タイムアウトしました。」のダイアログが表示される場合

本製品での撮影時間は1回につき最大10秒となっています。10秒で撮影できなかった場合は該当のダイアログが表示されます。

制限時間内に撮影が終わらないのは次の原因が考えられます。

・撮影中に指が動いている

→ 撮影中は指を認証ゾーンに正しく置き、撮影が終了するまで動かさないでください。

・指の表面が汚れている（荒れている）

指をけがした状態、手荒れした状態、土ぼこり等で汚れている状態で撮影を行おうとした場合、正しい画像が得られないために撮影が終わらない場合があります。

→ けが・手荒れのない手で撮影を行うか、手を綺麗にしてから再度撮影をしてください。

・指が太すぎる（細すぎる）

指が細すぎたり太すぎたりする場合（指の幅が10mm未満もしくは25mm以上の場合）、正しい画像が得られないために撮影が終わらない場合があります。

→ 「指を伸ばしてみる」「指を深く入れる」「指を浅く入れる」等の指の置き方を試してください。一般的には指先をくぼみの部分に当てて、真っ直ぐにした状態で撮影を行ってください。

・認証装置の認証ゾーン部が汚れている

認証装置の認証ゾーン部に、指紋の跡や汚れがある状態で撮影を行おうとした場合、正しい画像が得られないために撮影が終わらない場合があります。

→ 「取扱説明書 ハードウェア編」の「4 認証装置のお手入れ」をお読みいただき、認証ゾーン部の汚れを取り除いてから再度撮影をしてください。

「指の撮影に失敗しました。操作をやり直してください。」のダイアログが表示される場合

本製品の指情報の登録は同じ部位を3回撮影し、それぞれの情報を比較すること

で行っています。該当のダイアログが表示されるのは次の原因が考えられます。

- ・撮影中に指が動いている

→ 撮影中は指を認証ゾーンに正しく置き、撮影が終了するまで動かさないでください。

- ・3回の撮影を通して認証装置への指の置き方が均一でない

→ できるだけ一定の置き方で3回の撮影を行ってください。

「フィルタ条件に該当したため登録を中止しました。別の指を登録することをお奨めします。」のダイアログが表示される場合

本製品では、撮影したデータをフィルタリングすることで、認証に適さないデータが登録されないようにしています。このダイアログが表示された場合は、以下の対処法を実施してください。

- ・指の置き方を変えてみる

→製品に添付の「登録・認証の仕方」をお読みいただき、正しい置き方を確認した上で撮影を行ってください。

- ・別の指を登録してみる

→登録する指を変えて撮影を行ってください。

- ・フィルタオプションを無効にする

→上記の対処法によっても登録ができない場合は、フィルタオプションを無効にしてください。フィルタオプションを無効にする方法は[6.13 フィルタオプションの設定]を参照してください。

■ 指情報の登録時に警告が表示される

「登録しようとしている指情報がフィルタ条件に該当しました。この指情報を登録せずに、別の指を用いて登録操作をやり直すことをお奨めします。この指情報を登録してもよろしいですか？」のダイアログが表示される場合

本製品では、撮影したデータをフィルタリングすることで、認証にあまり適さないデータに対して登録を続行してもよいかの警告を表示するようにしています。このダイアログが表示された場合は、登録を続行することは可能ですが、以下の対処法により再度登録を実施することをお奨めします。

- ・指の置き方を変えてみる

→製品に添付の「登録・認証の仕方」をお読みいただき、正しい置き方を確認した上で撮影を行ってください。

- ・別の指を登録してみる

→登録する指を変えて撮影を行ってください。

■ 認証に失敗する

「タイムアウトしました。」のダイアログが表示される場合

本製品での認証時間は1回の認証につき最大10秒となっています。10秒で認証できなかった場合は該当のダイアログが表示されます。

制限時間内に認証が終わらないのは次の原因が考えられます。

- ・認証中に指が動いている

→ 認証中は指を認証ゾーンに正しく置き、認証が終了するまで動かさないでください。

- ・指の表面が汚れている（荒れている）

指をけがした状態、手荒れした状態、土ぼこり等で汚れている状態で認証を行おうとした場合、正しい画像が得られないために認証が終わらない場合があります。

→ けが・手荒れのない手で認証を行うか、手を綺麗にしてから再度認証をしてください。

- ・指が太すぎる（細すぎる）

指が細すぎたり太すぎたりする場合（指の幅が10mm未満もしくは25mm以上の場合）、正しい画像が得られないために認証が終わらない場合があります。

→ 「指を伸ばしてみる」「指を深く入れる」「指を浅く入れる」等の指の置き方を試してください。一般的には指先をくぼみの部分に当てて、真っ直ぐにした状態で認証を行ってください。

- ・認証装置の認証ゾーン部が汚れている

認証装置の認証ゾーン部に、指紋の跡や汚れがある状態で撮影を行おうとした場合、正しい画像が得られないために撮影が終わらない場合があります。

→ 「ハードウェア編」の「4 認証装置のお手入れ」をお読みいただき、認証ゾーン部の汚れを取り除いてから再度撮影をしてください。

静紋 J200/J210 から静紋 J300 に換えた場合

静紋 J300 と静紋 J200/J210 では、互換性がありません。静紋 200/J210 から静紋 J300 に交換した場合は、ドライバとソフトウェアの再インストールが必要になります。また、指静脈データに互換性がないので、再度、指静脈の登録が必要になります。

「認証に失敗しました。」のダイアログが表示される場合

認証に失敗するのは次の原因が考えられます。

・指情報の登録を行っていない

→管理者権限を持つユーザーで登録の確認を行ってください。登録されていないければ、認証に必要な指情報の登録を行ってください。

・指を正しく置いていない

→登録時と同様の置き方で指を認証ゾーンに正しく置いてください。
登録が正しく行われていないと認証できないことがありますので、指情報を再登録してください。再登録は、該当の指情報を削除し、再度「指情報の追加」を行ってください。なお、指情報の削除は本書 [6.4 指情報の削除] を、指情報の追加は本書 [6.2 指情報の追加] をそれぞれ参照してください。また、初回登録時などは、認証の練習機能を使用して、認証の練習を行うことをお勧めします。(本書[6.11 認証の練習]参照)

・指の状態が登録時と異なる

→認証ができにくくなった場合(成長期の子供で指の状態が変わる場合等)は、指情報を再度登録してください。再登録は、該当の指情報を削除し、再度「指情報の追加」を行ってください。
なお、指情報の削除は本書「6.4 指情報の削除」を、指情報の追加は本書「6.2 指情報の追加」をそれぞれ参照してください。

「ログオンできません。」のダイアログが表示される場合

コントロールパネルから Windows のパスワードを変更した場合、本製品で管理している Windows のパスワードと整合性が取れなくなりエラーダイアログが表示されます。

正しくログオンできない場合は、緊急用パスワードを用いて認証を行ってください。緊急用パスワードに関しては本書「8 緊急用パスワードの利用」をお読みく

ださい。

「フィルタ条件に該当しました。」のダイアログが表示される場合

本製品では、撮影したデータおよび登録済みのデータをフィルタリングすることで、認証に適さないデータでは認証できないようにしています。このダイアログが表示された場合は、以下の対処法を実施してください。

・指の置き方を変えてみる

→製品に添付の「登録・認証の仕方」をお読みいただき、正しい置き方を確認した上で撮影を行ってください。

・別の指で認証してみる

→複数の指を登録している場合は、別の指で認証を行ってください。

・指を登録し直す

→上記の対処法を実施しても認証できない場合は、認証できない指の指静脈データを削除し、新たに登録し直してください。指静脈データの削除については[6.4 指情報の削除]を、指の登録については[6.2 指情報の追加]を参照してください。

・フィルタオプションを無効にする

→指を登録し直せない場合は、フィルタオプションを無効にしてください。フィルタオプションを無効にする方法は[6.13 フィルタオプションの設定]を参照してください。

■ 認証が開始されない

認証装置を接続しているのに「使用可能な認証デバイスがありません。」のダイアログが表示される場合

・認証開始状態になっていない

→ 認証装置を接続すると状態表示 LED は点灯しますが、すぐに認証を開始することができません。接続後 5 秒ほどお待ちください。

→ エラーコード:02xxxxxx (x は任意の数字) が表示された場合は、USB コネクタの抜き差し、あるいは別の USB ポートへの接続をお試しください。
上記をお試しいただいても認証できない場合は、ハードウェアの故障が考えられます。

お手数ですが、ご購入先もしくは静紋テクニカルサポート窓口にご連絡ください。

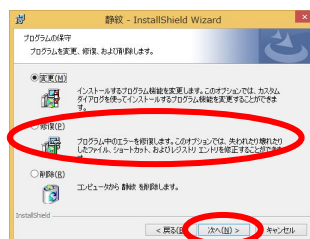
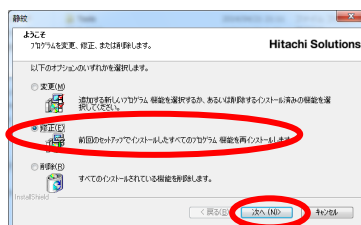
- ・ 認証装置用のドライバが正しく組み込まれていない

→ 本書「2.6 ドライバインストールの確認」を参照して、お使いのパソコンに正しくドライバが組み込まれているかを確認してください。

- ・ 異なる認証装置が接続されている場合

→ 認証装置を修理で交換した場合、複数の認証装置を使用している場合等で、ドライバをインストールしたときと異なる認証装置を接続すると、Windows ログオン時やユーザー管理機能の認証時に「使用可能な認証デバイスがありません。」と表示される場合がありますので、元の装置を接続するか、下記手順に従いソフトウェアの再インストールを行ってください。(Windows ログオン画面では、元の装置を接続するか緊急用パスワードでログオン後、ソフトウェアの再インストールを行ってください。)

1. 本製品に同梱されている「アプリケーション CD-ROM」をお使いのパソコンの CD-ROM ドライブに挿入します。
2. 「4 ソフトウェアのアンインストール」の①～②の手順に従い「プログラムの追加と削除」を起動してください。
3. ③の手順実行時に[変更]ボタンをクリックします。アンインストール用パスワードを設定している場合は、⑤の手順に従ってください。
4. 右のいずれかの画面が表示されます。
[修正(E)] または [修復(P)] を選択し、[次へ(N)] ボタンをクリックしてください。



5. 指静脈認証ソフトウェアのインストールの終了後、お使いのコンピュータの再起動を行います。

なお、インストール時と再インストール時の CD-ROM ドライブのドライブレターが異なる場合には、エラーダイアログが表示される場合があります。この場合は、現在の CD-ROM ドライブのドライブレターを入力してください

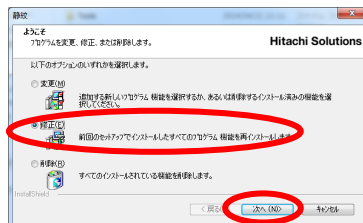
■ ユーザー管理機能が起動できない

ユーザー管理機能が起動できないのは次の原因が考えられます。

- ・ お使いのパソコンの Administrators グループに属しているユーザーでログオンしていない
→ Administrators グループに属しているユーザーでログオンしてください。
 - ・ 認証に失敗する
→ 本書トラブルシューティングの「認証に失敗する」をご覧ください。
 - ・ 「他のユーザーが実行中です。アプリケーションを終了します。」と表示される
→ お使いのパソコンにリモート接続して利用しているユーザーがユーザー管理機能を使用中である可能性があります。そのようなユーザーがいないかどうか確認してください。
 - ・ 「ワークステーション サービスが開始されていません」と表示される
→ お使いのパソコンで「Workstation」という名前の Windows サービスプログラムが停止している可能性があります。このサービスプログラムが動作していない場合、ユーザー管理機能を起動することはできません。システムの管理者に問い合わせ、「Workstation」サービスプログラムを開始してください。
 - ・ 指静脈認証ソフトウェアが起動しない
→ なんらかの原因でユーザー管理機能が起動できなくなった場合は、指静脈認証ソフトウェアの再インストールを行うことにより正しく動作させることができる場合があります。下記手順に従い再インストールを行ってください。
1. 本製品に同梱されている「アプリケーション CD-ROM」をお使いのパソコン

の CD-ROM ドライブに挿入します。

- 「4.1 指静脈認証ソフトウェアのアンインストール」の①～②の手順に従い「プログラムの追加と削除」を起動してください。
- ③の手順実行時に[変更]ボタンをクリックします。アンインストール用パスワードを設定している場合は、⑤の手順に従ってください。
- 右のいずれかの画面が表示されます。
[修正(E)]を選択し、[次へ(N)]ボタンをクリックしてください。



- 指静脈認証ソフトウェアのインストールの終了後、お使いのコンピュータの再起動を行います。

なお、インストール時と再インストール時の CD-ROM ドライブのドライブレターが異なる場合には、エラーダイアログが表示される場合があります。この場合は、現在の CD-ROM ドライブのドライブレターを入力してください。

それでも起動しない場合は本書「4 ソフトウェアのアンインストール」でソフトウェアを削除した後、再度「2 ソフトウェアのインストール」を参照してソフトウェアをインストールしてください。

■ 認証装置を接続するとハードウェアインストールウィザードが起動する

ドライバのインストールが完全に行われていない場合

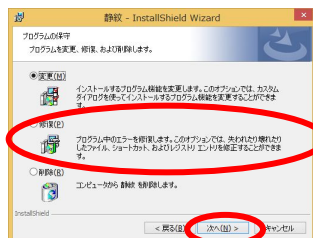
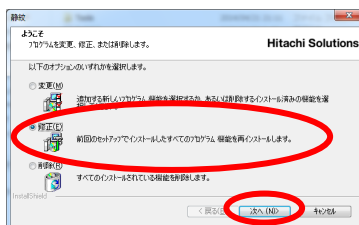
ドライバのインストールが完了していない可能性があります。本書の「2 ソフトウェアのインストール」を参照して、正しくインストールを行ってください。

異なる認証装置が接続されている場合

認証装置を修理で交換した場合、複数の認証装置を使用している場合等で、ドライバをインストールしたときと異なる認証装置を接続した場合、ハードウェアインストールウィザードが起動する場合があります。その場合は、下記手順に従いソフトウェアの再インストールを行ってください。(Windows ログオン画面では「使用可能な認証デバイスがありません。」と表示されますので、元の装置を接続するか緊急用パスワードでログオン後、ソフトウェアの再インストールを行ってください。)

1. 本製品に同梱されている「アプリケーション CD-ROM」をお使いのパソコンのCD-ROM ドライブに挿入します。
2. 「4.1 指静脈認証ソフトウェアのアンインストール」の①～②の手順に従い「プログラムの追加と削除」を起動してください。
3. ③の手順実行時に「変更」ボタンをクリックします。アンインストール用パスワードを設定している場合は、⑤の手順に従ってください。

4. 右のいずれかの画面が表示されます。[修正(E)]を選択し、[次へ(N)] ボタンをクリックしてください。



5. 指静脈認証ソフトウェアのインストールの終了後、お使いのコンピュータの再起動を行います。

なお、インストール時と再インストール時のCD-ROM ドライブのドライブレターが異なる場合には、エラーダイアログが表示される場合があります。この場合は、現在のCD-ROM ドライブのドライブレターを入力してください。

■ Windows をアップグレードする場合の注意

指静脈認証ソフトウェアをお使いの Windows 8.1 を Windows 10 にアップグレードする場合、指静脈認証ソフトウェアのアンインストールが必要です。指静脈認証ソフトウェアのアンインストール後、Windows をアップグレードし、その後で指静脈認証ソフトウェアを再度インストールしてください。

■ インストール時にエラーが発生する場合

「本製品と競合するソフトウェアがインストールされている可能性があります。」のダイアログが表示される場合

本製品と競合するソフトウェアがインストールされている場合、本製品をインストールすることができません。このダイアログが表示された場合は、競合するソフトウェア (AuthentiGate 等) がインストールされている可能性があります。そのような場合は、それらをアンインストールした上で再度本製品のインストールを実行してください。

■ ローカル PC および AD サーバに同名の Windows ユーザーが存在する場合、緊急用パスワードを入力する操作でアカウント名のみの画面が表示され先に進めない

ドメインに参加している Windows Server 2012 / Windows 8.1 Update / Windows Server 2012 R2 / Windows 10 / Windows Server 2016 / Windows Server 2019 / Windows 11 で Windows ログオン連携機能を用いている場合、ローカル PC および AD サーバに同名の Windows ユーザーが存在している場合、緊急用パスワードを入力する操作 (Ctrl+Alt+q 押下時) でアカウント名のみの画面が表示され先に進めない現象が発生します。そのため、以下の方法で回避してください。

- ・ Windows Server 2012 / Windows 8.1 / Windows Server 2012 R2 をお使いの場合
1. 「他のユーザー」を選択後、「8.1 Windows Server 2012 / Windows 8.1 / Windows Server 2012 R2 のログオン・ロック解除の場合」に従い緊急用パスワードでログオンしてください。

2. ローカル PC の Windows ユーザーを削除してください。

・ Windows 10 / Windows Server 2016 / Windows Server 2019 / Windows 11 をお使いの場合

1. 「他のユーザー」を選択後、「8.2 Windows 10 / Windows Server 2016 / Windows Server 2019 / Windows 11 のログオン・ロック解除の場合」に従い緊急用パスワードでログオンしてください。
2. ローカル PC の Windows ユーザーを削除してください。

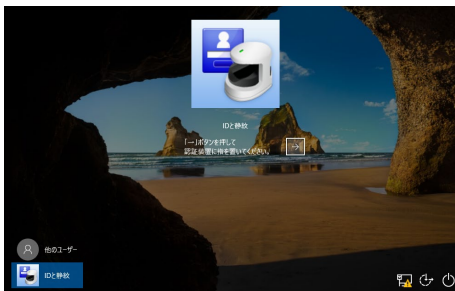
■ドメイン参加環境において、初回管理者登録時にログオン先に何も表示されない

ドメインに参加している環境で、初回時管理者登録を実施した際、AD サーバの設定等の影響により、ログオン先に何も表示されなくなる場合があります。この状態になると、ログオン先は非活性のため手入力を行うことができず、そのまま撮影開始しようとする「ログオン先が入力されていない」旨のエラーとなり、先に進むことができません。そのような場合は、下記の手順を実施してください。

1. ローカルユーザーでログオンします。
2. ユーザー管理アプリを起動し、「3 初回時管理者登録」に従い、初回時管理者登録を実行してください。
3. ユーザー管理アプリを終了し、再起動を行います。
4. 「8 緊急用パスワードの利用」に従い、緊急用パスワードを使用し、ドメインユーザーでログオンします。
5. ユーザー管理アプリを起動し、「8.3 ユーザー管理機能のロック解除の場合」に従い、緊急用パスワードでログオンします。
6. 登録したユーザーを選択した状態で、「6.3 指情報の変更」に従い、「指情報の変更」画面を表示させた後、「ユーザー情報の変更」チェックボックスを ON にし、ドメインユーザーに変更してください。ただし、「ログオン先」が空の場合は UPN 形式でドメイン名を手入力してください。UPN 形式とは、<ユーザー名>@<ドメイン名>のようにユーザー名とドメイン名を @ (アットマーク) でつなげた形式です。

■ドメイン参加環境において、コンピュータ起動時または再起動時に、サインイン画面の表示が崩れる

ドメインに参加している Windows Server 2012 / Windows 8.1 / Windows Server 2012 R2 / Windows 10 / Windows Server 2016 / Windows Server 2019 / Windows 11 において、ネットワークの接続等の問題により、コンピュータ起動時または再起動時に、右の画面のようにサインイン画面の表示が崩れる場合があります。そのような場合は、ご使用の AD サーバにて、Windows のグループポリシーの「コンピュータ起動時とログオン時にネットワークを常に待つ」の設定を「有効」にしてください。



それでも回避ができない場合は、ご使用の AD サーバにて、Windows のグループポリシーの「対話型ログオン：最後のユーザー名を表示しない」の設定を「有効」にしてください。

■アップデート後に Windows ログオンが Windows 標準の認証方式から指静脈認証方式に変わる

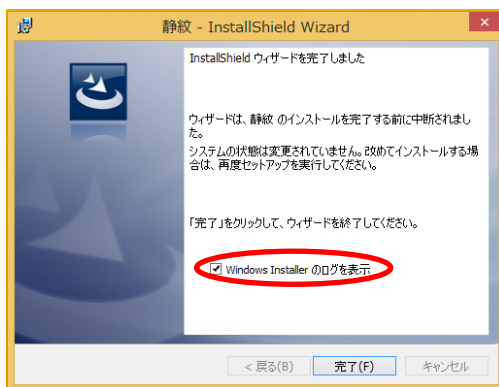
01-08 以前で Windows ログオンを指静脈認証方式にした状態で 01-09 にアップデートし、その後に Windows 標準の認証方式に戻した状態で本バージョンにアップデートすると、指静脈認証方式に変わる場合があります。そのような場合は、登録済みの指情報もしくは緊急用パスワードを使用して一旦 Windows ログオンしていただいた後に、ユーザー管理機能の「6.7 認証方法の変更」に従い、Windows ログオンの認証方式の変更をしてください。

■静紋のインストール失敗後に Windows Installer のログを表示しようとするとエラーが発生する

静紋のインストールに失敗すると、ご使用の環境によっては右の画面のように「Windows Installer のログを表示」のチェックボックスが表示される場合があります。

この状態において「Windows Installer のログを表示」にチェックを行い、[完了(F)] ボタンをクリックすると、「ディレクトリ マネージャが初期化されていません。」のエラーが表示される場合があります。

このエラーが発生しても静紋のインストールは問題なく中断されていますので、インストール失敗時に表示されたエラーの内容に従い、対処してください。



14 付録

14.1 スクリーンセーバーの設定について

スクリーンセーバーロックを指静脈認証によって保護する場合は、スクリーンセーバーの設定で、[再開時にログオン画面に戻る(R)] をチェックしてください。

