

NeoFace Monitor クラウド版

シンクライアント端末への適応について

2023 年 6 月

日本電気株式会社

ご注意

- ・ NeoFace、NeoFace Monitor ならびに Bio-IDiom は、日本電気株式会社の商標または登録商標です。
 - ・ Windows、Active Directory ならびに Azure Active Directory (Azure AD) は米国およびその他の国における Microsoft Corporation の商標または登録商標です。
 - ・ ウイルスバスタークラウドはトレンドマイクロ株式会社の登録商標です。
 - ・ 本書は日本電気株式会社の著作物です。著作権法により、お客様が個人で使用する以外の目的で、日本電気株式会社の許可なしに本書の一部または全部を複製することは禁じられています。
 - ・ 本書の内容に関しては、将来予告なしに変更することがあります。
 - ・ 本書に掲載されている画像イメージなどは実際のものとは異なる場合があります。
 - ・ 本書に記載されているシステム名、製品名は開発メーカーの商標または登録商標です。なお、TM、®マークは明記しておりません。
-

目次

1. はじめに.....	1
1.1. 本書の構成.....	2
1.2. 注意事項.....	2
2. クライアントのセットアップの準備.....	5
2.1. 動作環境.....	5
2.2. プロキシの設定.....	6
3. NFM クラウド版クライアントのインストール.....	9
3.1. 設定変更ツールを使用して UWF を無効化する.....	10
3.2. NeoFace Monitor クラウド版 クライアントをインストール.....	12
3.3. 設定変更ツールを使用して UWF を有効化する.....	27
3.4. 設定変更ツールを使用して個別の除外設定を行う.....	28

1. はじめに

本書は、NeoFace Monitor クラウド版クライアントのシンクライアント端末へのインストールについて説明しています。

本書で対応する製品のバージョンは以下のとおりです。

- ・ NeoFace Monitor クラウド版 クライアント (64bit) : Version 1.3.0

本書で「シンクライアント端末」と呼ぶ場合、次の端末を指します。

- ・ NEC 製シンクライアント端末
- ・ Windows 10 以降の OS を搭載している端末

本書で使用している記号の意味は、以下のとおりです。

記号	意味
	遵守すべき事柄や特に注意すべき点を示します。
	本文に記載されている情報に関する解説・補足情報を示します。

本書では、以下の略称と総称を使用しています。

- NeoFace Monitor クラウド版 クライアント (64bit) : NFM クラウド版クライアント

1.1. 本書の構成

本書の構成について説明します。運用シーンに合わせてご参照ください。

運用場面	参照先
NeoFace Monitor クラウド版 クライアントのセットアップの準備。	第 2 章
NeoFace Monitor クラウド版 クライアントをインストールする。	第 3 章

1.2. 注意事項

- Windows のログオン先について
Windows のログオン先がドメインの場合は、本製品をインストールする前に Active Directory ドメインへの参加を行ってください。
または、Windows のログオン先が Azure AD の場合は、本製品をインストールする前に Azure AD への参加を行ってください。
- Windows 10 でのご利用について
Windows 10 をご利用の場合は、『NeoFace Monitor クラウド版 クライアントユーザーズマニュアル』の「11. Windows 10 でのご利用について」をご参照ください。
- 個人情報の取り扱いについて
NFM クラウド版クライアントの登録・照合・識別の各処理にて生成、利用される NFM 利用者データ（顔特徴抽出データ・ID を含む）には、個人情報が含まれています。それらデータの取り扱いに十分留意し、お客様の責任において適切なセキュリティ対策を施してください。
- 他の Windows ログオン製品との併用について
NFM クラウド版クライアントは Windows 以外のカスタマイズ Credential Provider（SKYSEA Client View、CyberLink YouCam、NEC Authentication Agent など）および他の生体認証製品との共存はサポートしておりません。そのため、他の Windows ログオン製品がインストールされている場合は、アンインストールしてから、NFM クラウド版クライアントのインストールを行うようお願いいたします。
- カメラを使用する他アプリケーションとの併用について
NFM クラウド版クライアントは Windows ログオンおよび画面ロック解除、常時認証機能の際にカメラを使用します。カメラを使用する他のアプリケーションと併用できませんのでご注意ください。
- OS 環境について
NFM クラウド版クライアントは x64 バージョンをご用意しています。

- Windows パスワードの注意点
インストールする前に、Windows アカウントに Windows パスワードが設定されていることを必ず確認してください。Windows パスワードが未設定の場合、Windows ログオンできなくなります。
NFM クラウド版クライアントは 64 文字以上の Windows パスワードに対応しております。Windows パスワードが 64 文字以上の場合、インストールする前に 63 文字以下になるように Windows パスワードを変更してください。
- 管理ポータル上に登録する Windows パスワードについて
NeoFace Monitor クラウド版における Windows アカウントの新規追加時の Windows パスワード設定操作、および再設定操作では、Windows の登録内容と同じ Windows パスワードを設定してください。Windows と異なる値を設定した場合、Windows ログオンできなくなります。
- Windows パスワードの入力制限について
NeoFace Monitor クラウド版をご利用中のシステムでは、Windows パスワードに半角スペースを使用することができません。
- 画面表示のちらつきについて
Windows ログオン時、もしくは画面ロック解除時に、端末の種類によっては、Windows ログオンもしくは画面ロック解除画面の表示がちらつくことがあります。動作に支障はありません。
- OS 起動時間について
本ソフトウェアをインストールすることによって、OS 起動時のログオン画面への遷移が遅くなる可能性があります。
- 対応するアカウントについて
本製品は Windows アカウント(ローカルアカウント・ドメインアカウント)または Azure AD アカウントに対応しています。上記以外のアカウントは対応していません。
- Microsoft アカウントの注意点
Windows 10、Windows 11 搭載端末へ NFM クラウド版クライアントをインストールする場合、対象端末に Microsoft アカウントしか存在していない場合にはインストールが正常完了せず、製品を利用することができません。
- タブレット端末の画面回転について
Windows タブレットの画面の自動回転へは対応していません。NFM クラウド版クライアントの画面は常に固定表示となります。(NEC 製タブレット PC のみ自動回転に対応しています)
- InfoCage PC セキュリティとの連携について
NEC の統合型 PC セキュリティソフトウェアである InfoCage PC セキュリティと NFM クラウド版クライアントを連携させる場合は双方の動作環境、連携バージョンをご確認のうえ、インストールしてください。

- 顔の登録、認証について

NeoFace Monitor クラウド版では顔の登録、認証を行う際に両目が開いている必要があります。顔の登録、認証を行えない場合は、パスワードによる代替認証をご利用いただくことができます。

- NeoFace Monitor をインストールした PC の使用を終了する場合について

NeoFace Monitor は認証情報を取り扱う製品のため、PC の廃棄や譲渡など、PC の使用を終了する場合は、必ず NeoFace Monitor をアンインストールしてください。

2. クライアントのセットアップの準備

2.1. 動作環境

本製品の動作確認済みのシンクライアント端末は次の通りです。

- Express5800 シリーズ US320g
- VersaPro シリーズ
 - Windows 10 IoT Enterprise 2016 LTSB モデル
 - Windows 10 IoT Enterprise 2019 LTSC モデル
 - Windows 10 IoT Enterprise 2021 LTSC モデル
 - Windows 11 IoT Enterprise 21H2/22H2 モデル



- ・ 検証外のシンクライアント端末に関しては、NeoFace Monitor 製品主幹部門へご相談ください。
- ・ シンクライアントへの設定変更ツール (Atrust Client Setup、Unified Write Filter (UWF)) についてはシンクライアント端末の提供元にお問い合わせください。

2.2. プロキシの設定

インターネットの接続環境がプロキシサーバーを経由している場合は、以下の設定を行ってください。

1. ローカルグループポリシー^{※1}を起動する。
2. [ローカル コンピューター ポリシー]–[コンピューターの構成]–[管理用テンプレート]–[Windows コンポーネント]–[Internet Explorer]を押下する。
3. [コンピューター別にプロキシを設定する(ユーザー別ではなく)]を[有効]に設定する。
4. [スタート]–[設定]–[ネットワークとインターネット]–[プロキシ]を順に押下
5. Windows OS のバージョンが Windows 10 の場合は、本手順をスキップし手順 6 へ進む。
Windows 11 の場合、[手動プロキシ セットアップ]–[プロキシ サーバーを使う]の [セットアップ] または [編集] を押下する。



^{※1} ローカルグループポリシーの起動については、本章末尾の「※ローカルグループポリシーの起動方法」をご参照ください。

6. [手動プロキシ セットアップ]の[プロキシ サーバーを使う]をオンにし、プロキシ サーバーの設定を行う。

手動プロキシ セットアップ

イーサネットまたは Wi-Fi 接続にプロキシ サーバーを使います。これらの設定は、VPN 接続には適用されません。

プロキシサーバーを使う

オン

アドレス ポート

次のエントリで始まるアドレス以外にプロキシ サーバーを使います。エントリを区切るにはセミコロン (;) を使います。

ローカル (イントラネット) のアドレスにはプロキシ サーバーを使わない

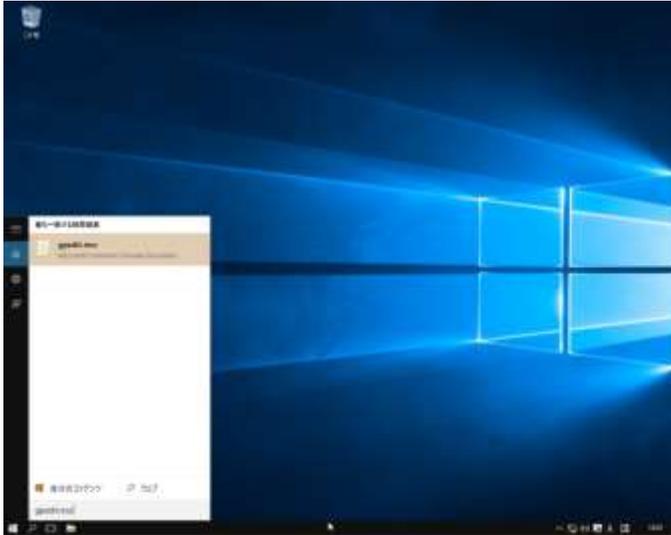
保存

NFM クラウド版クライアントは手動プロキシ セットアップで設定されたプロキシサーバーの情報を元にプロキシを使用するため、自動プロキシ セットアップでスクリプトファイルを使用するように設定されている場合でも、手動プロキシ セットアップの設定を行ってください。

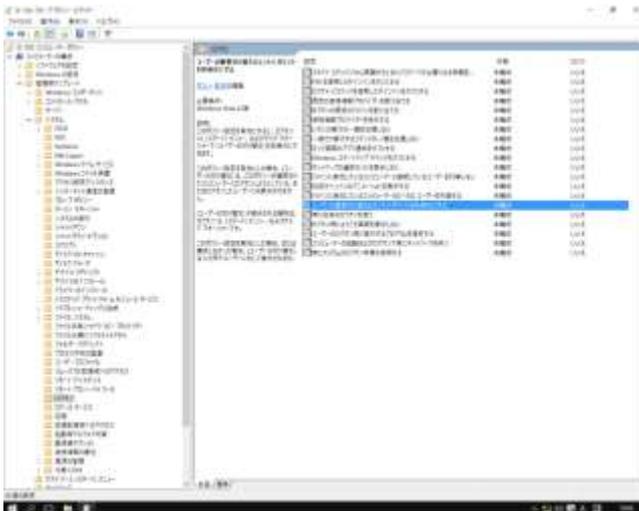
自動プロキシ セットアップと手動プロキシセットアップの両方が有効に設定されている場合、自動プロキシ セットアップを優先します。そのため既存の動作には影響ありません。

※ローカルグループポリシーの起動方法(Windows 10 の場合)

1. 「Web と Windows を検索」(画面左下の虫眼鏡マーク)を押下し、「gpedit.msc」と入力して「Enter」キーを押下します。



2. 「ローカルグループポリシーエディター」が起動します。変更したい設定箇所を編集します。各設定の変更方法詳細については Microsoft 社の情報をご参照ください。



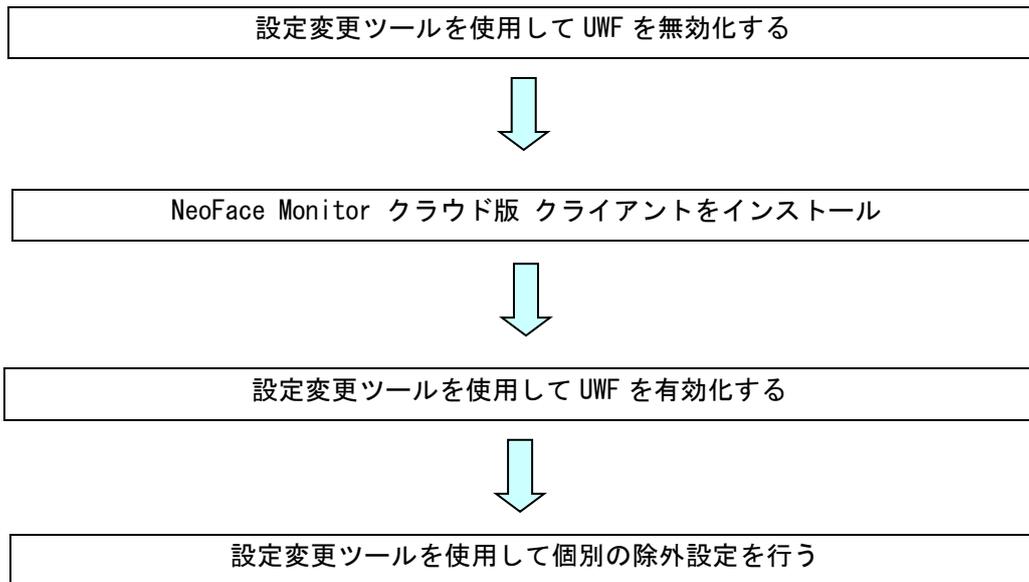
3. 編集したローカルグループポリシーを反映するため、Windows 再起動します。

以上で、ローカルグループポリシーの変更は完了となります。

3.NFM クラウド版クライアントのインストール

シンクライアントのセットアップ手順は、以下の通りです。

本書では、例として、インストールする端末に Express5800 シリーズ US320g、VersaPro シリーズ (Windows 10 IoT Enterprise 2016 LTSC モデル、Windows 10 IoT Enterprise 2019 LTSC モデル、Windows 10 IoT Enterprise 2021 LTSC モデル) へのインストールを例にして説明します。



NFM クラウド版クライアントの利用方法については、『NeoFace Monitor クラウド版ユーザーズマニュアル』をご覧ください。

3.1. 設定変更ツールを使用して UWF を無効化する

1. Administrators 権限、または Domain Admins 権限で対象の Windows にログオンします。
また、他のアプリケーションが動作している場合は、終了します。
2. UWF を無効化します。機種により方法が異なります。

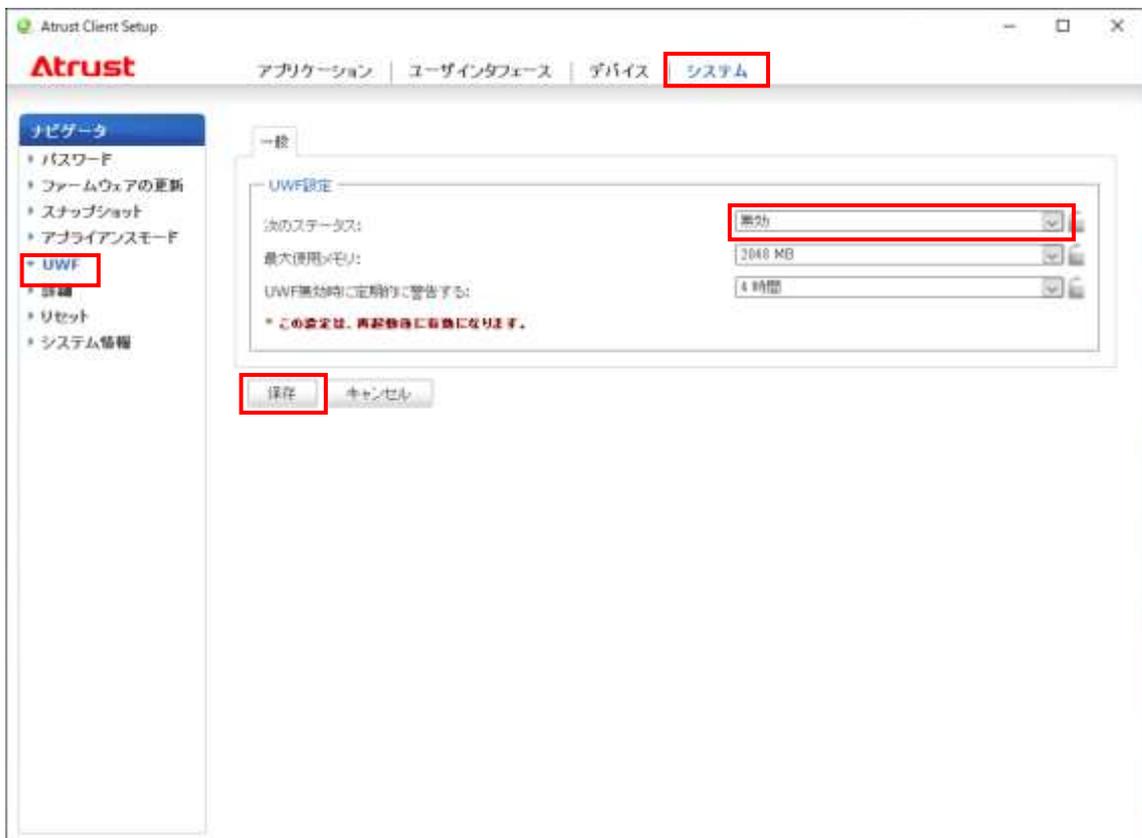
[Express5800 シリーズ US320g]

設定変更ツール Atrust Client Setup を使用して UWF を無効化します。

設定変更ツールの画面で「システム」－「UWF」を順に押下します。

「次のステータス」のプルダウンメニューを押下して「無効」を選択します。

[保存]を押下します。再起動を求められたら、再起動をしてください。



[VersaPro シリーズ]

設定変更ツールのコマンドモードで UWF を無効化します。

「スタート」-「Windows システム ツール」を順に押下して、「コマンド プロンプト」を右クリックし、「その他」-「管理者として実行」を順に押下して、コマンドプロンプトを管理者として開きます。

コマンドプロンプトで次のコマンドを実行します。

- UWFMgr.exe filter disable

コマンド実行後、シンクライアント端末を再起動します。

3.2. NeoFace Monitor クラウド版 クライアントをインストール



NFM クラウド版クライアントは 64 文字以上の Windows パスワードに対応していません。Windows パスワードが 64 文字以上の場合、インストールする前に 63 文字以下になるように Windows パスワードを変更してください。



NFM クラウド版クライアントは全角または半角 21 文字以上の Windows アカウント名に対応していません。

Azure AD 表示名は全角 10 文字以下(半角 20 文字以下)の英数字記号、および以下以外の常用漢字を使用してください。

記号 : 「~」「//」「||」「¢」「&」「~」「~」「~」「~」「~」

漢字 : 「叱」「填」「剝」「頬」



インターネットの接続環境がプロキシサーバーを経由している場合は、NFM クラウド版クライアントソフトのインストールの前に、必ず「2.2. プロキシの設定」を実施してください。



インストール済みの状態で同じバージョンのインストーラを実行すると、アンインストールが開始されます。再インストールする場合は、『NeoFace Monitor クラウド版ユーザーズマニュアル』の「5.1. NFM クラウド版クライアントソフトのアンインストール手順」を参照しアンインストールしてから、インストールをしてください。



Windows 端末に 2 台以上のカメラが接続されている場合(タブレット PC など)は、インストール終了後の顔画像の登録を実施する前に、必ず『NeoFace Monitor クラウド版ユーザーズマニュアル』の「4.3. 複数カメラ搭載時(タブレット PC など)のカメラの確認と切替え」をご実施ください。



ウイルスバスタークラウドをお使いの場合、NFM クラウド版クライアントのインストール中、誤って不正なファイルと検知する場合があります。NFM クラウド版クライアントのインストール開始前から完了するまで、ウイルスバスタークラウドのリアルタイムスキャンの設定を無効化してください。

1. NFM 利用者登録メールに記載されている URL をクリックし、[NeoFace Monitor クラウド版 管理ポータル]を開きます。



The screenshot shows the login page for the NeoFace Monitor Cloud Management Portal. The page has a dark blue header with the logo and the text "NeoFace Monitor クラウド版 管理ポータル". The main content area is light gray and contains a white login form. The form includes the following elements:

- Tenant information: "テナント: NFM" with a small icon.
- Label: "NFM利用者ID(メールアドレス)".
- Input field for the user ID.
- Label: "パスワード".
- Input field for the password.
- A dark blue "ログイン" button.
- A link: "パスワードを忘れた方はこちら".

2. [NFM利用者ID(メールアドレス)]と[パスワード]を入力し、[ログイン]を押下します。

3. [NeoFace Monitor クライアントソフトのダウンロード]が表示されます。
[次へ]を押下して下さい。



4. ダウンロード画面が表示されます。



[テナント表示コード]、[テナントアクセスキー]、[テナント秘密鍵]はクライアントソフトのインストール時に必要な情報になります。メモしておいてください。

5. [ダウンロード]ボタンを押下してください。操作を選んでくださいと表示されたら、[開く]を選択します。他の作業後にインストールする場合は、[保存]を選択します。

NeoFace Monitorクライアントソフト ダウンロード

クライアントソフトインストール時に必要な情報になります。
ダウンロードボタンを押す前にメモしておいてください。

テナント表示コード

テナントアクセスキー

テナント秘密鍵

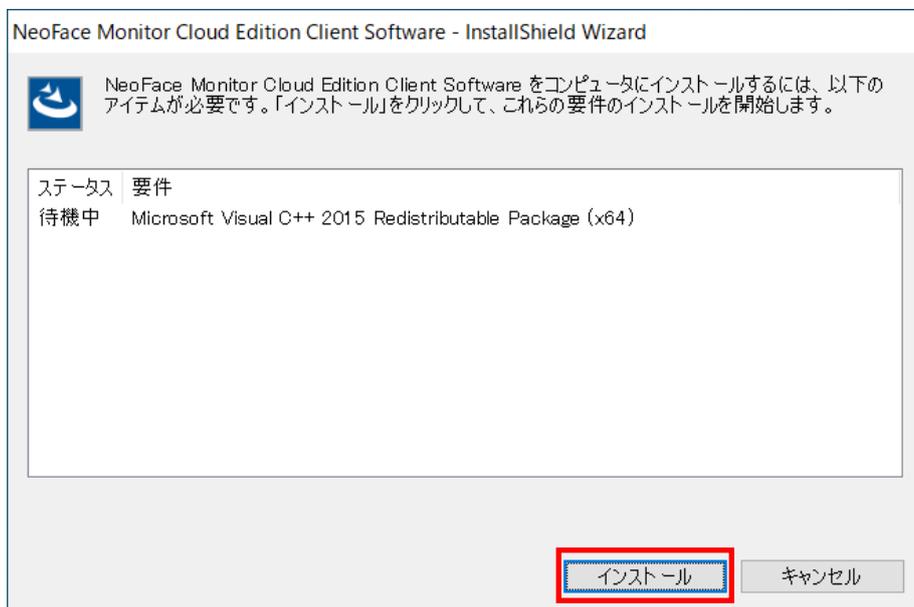
ダウンロード

6. Windows アカウント (Administrators 権限 または Domain Admins 権限) で、対象の Windows に Windows ログオンしている場合は、手順 7. に進みます。
そうでない場合は、それらの権限の Windows アカウントでログオンしてください。
また、他のアプリケーションが動作している場合は、終了します。
7. 手順 5. にて [開く] を選択した場合は、手順 8. に進みます。
[保存] を選択した場合は、ダウンロードした setup_x64_cl.exe を右クリックし、[管理者として実行] を押下します。

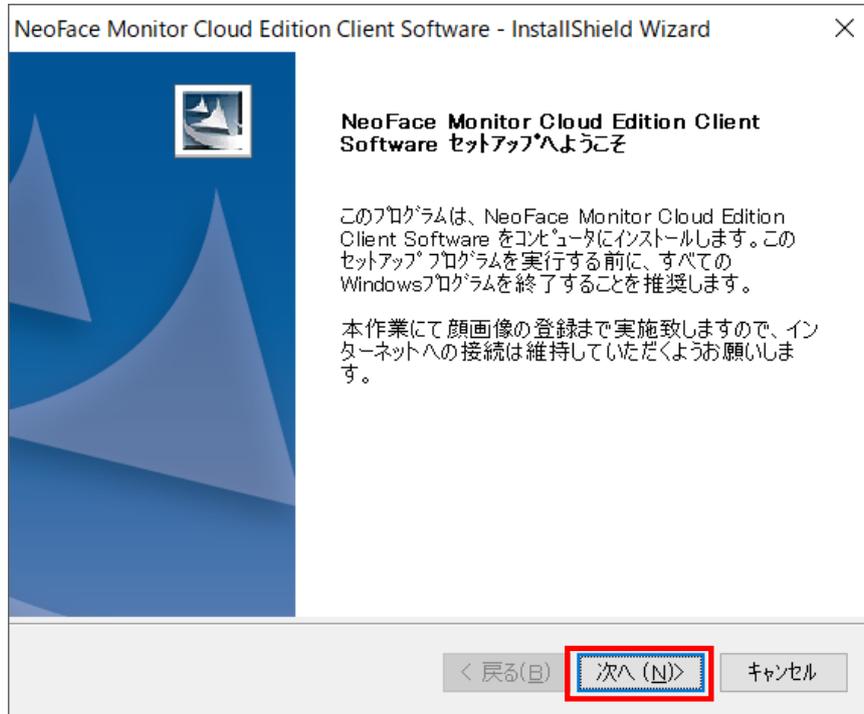
8. 以下のような確認を求められた場合は、[はい]を押下します。
インストールのための設定画面に移ります。



以下のような画面が表示された場合は、[インストール]を押下してください。
NFM クラウド版クライアントソフトのインストールに必要なソフトウェアです。



9. [NeoFace Monitor Cloud Edition Client Software セットアップへようこそ]ダイアログが表示されます。
[次へ]を押下します。

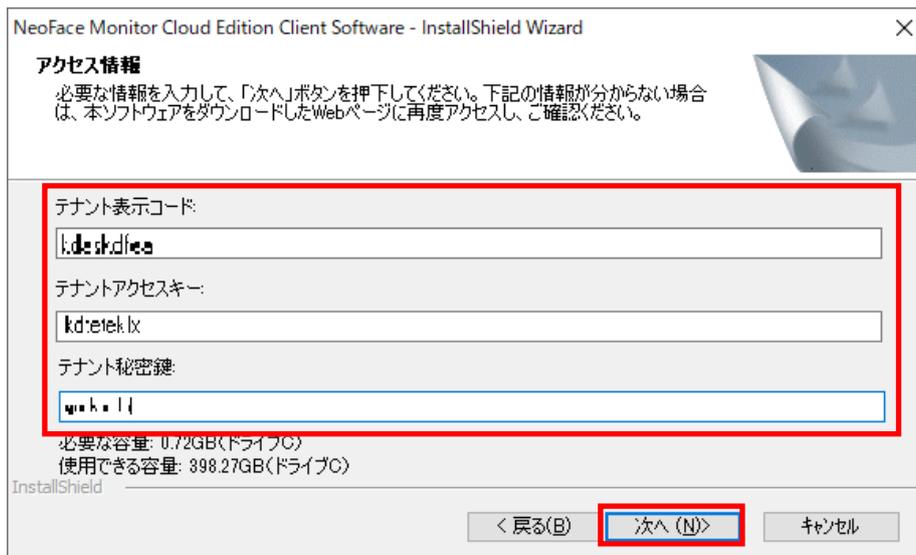


10. [使用許諾契約] ダイアログが表示されます。表示されている内容をご確認ください。
同意される場合は、[使用許諾契約の全条項に同意します]を選択して[次へ]を押下します。



同意されない場合は[キャンセル]を押下し、インストールを中止します。

11. [アクセス情報] ダイアログが表示されます。[NeoFace Monitor クライアントソフト ダウンロード]時にメモしておいた[テナント表示コード]、[テナントアクセスキー]、[テナント秘密鍵]を入力します。[次へ]を押下します。



12. [Windows アカウント情報] ダイアログが表示されます。

[Windows アカウント種別]で「ローカル」もしくは「ドメイン」を選択した場合は、[Windows アカウント]と[Windows パスワード]、[Windows アカウント種別]そして[コンピュータ名]か[ドメイン名]いずれか表示された項目の入力および選択をし、[インストール]を押下します。

[Windows アカウント種別]で「Azure AD」を選択した場合は、[表記名]と[Azure AD パスワード]、[Windows アカウント種別]、[Azure AD ドメイン名]そして[ユーザプリンシパル名]の入力および選択をし、[インストール]を押下します。

なお、ダイアログの入力欄には、あらかじめ現在 Windows へログオン中の Windows アカウント名、コンピュータ名などの情報が入力されています。

インストール後に Windows ログオンする際に利用する Windows アカウントまたは表示名が入力されている情報と異なる場合は変更をしてください。

インストールが始まります。



各項目において未入力がある場合は、インストール処理は完了しますが、顔画像の登録を行いません。

NFM 利用者（一般ユーザー）による顔画像登録や Windows アカウントと NFM 利用者の紐付けを行う場合は、『NeoFace Monitor クラウド版ユーザーズマニュアル』の「7.2. Windows ログオン方法」の手順 1. を参照し、次回 Windows ログオン時に顔画像登録や紐付けを行ってください。

13. 顔画像の登録を行います。

インストール中に顔画像登録ツールの認証ダイアログが表示されます。

顔画像登録する利用者の[利用者 ID (メールアドレス)]と[パスワード]を入力し、[OK]を押下します。

顔画像登録を行わない場合は[キャンセル]を押下し、顔画像登録を中止します。
キャンセルした場合は、手順 19. に進んでください。



複数の NFM 利用者（一般ユーザー）で 1 つの Windows アカウントを共有する場合は、キャンセルせず顔画像登録と紐付けを行ってください。

Windows アカウントを共有している場合、次回 Windows ログオン時に顔画像登録や紐付けが行えない場合があります。



キャンセルしてもインストールは完了します。

NFM 利用者（一般ユーザー）による顔画像登録や Windows アカウントと NFM 利用者の紐付けを行う場合は、『NeoFace Monitor クラウド版ユーザーズマニュアル』の「7.2. Windows ログオン方法」の手順 1. を参照し、次回 Windows ログオン時に顔画像登録や紐付けを行ってください。



Windows 端末に 2 台以上のカメラが接続されている場合（タブレット PC など）は、[OK]を押下する前に、必ず本書の『NeoFace Monitor クラウド版ユーザーズマニュアル』の「4.3. 複数カメラ搭載時（タブレット PC など）のカメラの確認と切替え」をご実施ください。

14. Windows アカウントと NFM 利用者の紐付け画面が表示されます。

[Windows アカウント情報] ダイアログ画面で入力した Windows アカウントと、前項で入力した NFM 利用者の紐付け有無が表示されます。紐付けされている、または紐付けする場合は[OK]を押下してください。

Windowsアカウントとの紐付け | NeoFace Monitor クラウド版

WindowsアカウントはNFM利用者と紐付けします。OKボタンを押下してください。

NFM利用者ID

Windowsアカウント名

Windowsパスワード

Windowsアカウント種別 ローカル ドメイン Azure AD

コンピュータ名

紐付けがされてなく紐付けと顔画像登録をしない場合、または紐付けされていて顔画像登録をしない場合は、[キャンセル]を押下し、中止します。

キャンセルしてもインストールは完了します。



NFM 利用者（一般ユーザー）による顔画像登録や Windows アカウントと NFM 利用者の紐付けを行う場合は、『NeoFace Monitor クラウド版ユーザーズマニュアル』の「7.2. Windows ログオン方法」の手順 1. を参照し、次回 Windows ログオン時に顔画像登録や紐付けを行ってください。

15. 個人情報の同意確認ダイアログが表示されます。

※ 既に個人情報の取扱いに同意済みの場合は表示されません。

[個人情報の取扱いについて(告知文へリンク)]を押下し表示される内容を確認し、同意される場合は、[上記の個人情報の取扱いに同意します。] をチェックして [OK] を押下します。



同意されない場合は[キャンセル]を押下し、顔画像登録を中止します。

16. 顔画像撮影画面が表示されます。

※ 既に顔画像が登録されている場合は表示されません。

[撮影]を押下します。



[姓]、[ミドルネーム]、[名]はそれぞれ 80 文字まで登録可能ですが、顔画像撮影画面には 20 文字までしか表示されません。

顔撮影のときは下記に注意してください。

- ・ カメラに向かって正面を向いてください。

- ・ 顔をはっきり映してください。

全体が暗いか、影などで顔がはっきり映っていない場合は、明るさを調整してください。また、背後に太陽光や照明の映り込みがある場合は、光源が入り込まないようにしてください。



- ・ 認識枠に顔を合わせてください。
- ・ まばたきをしないでください。
- ・ サングラスやマスクをしないでください。
- ・ 他の人が映らないようにしてください。



認識枠

【撮影に失敗した場合】

顔画像の撮影に失敗した場合は、画像が赤い枠で表示され、以下のメッセージが表示されます。

顔の位置やカメラの接続などを確認して[撮り直し]を押下し、手順 16. からやり直してください。また、何度も失敗する場合は、システム管理者にお問い合わせください。

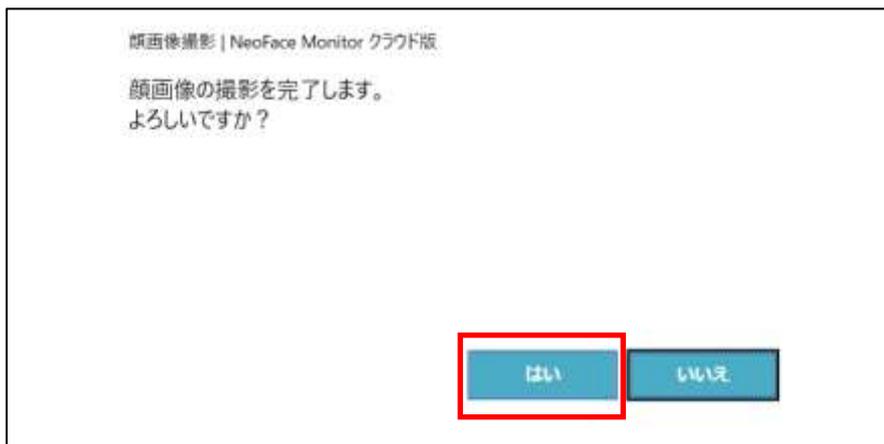
このエリアに撮影のヒントが表示されます。
撮影がうまくできないときは、参考にしてください。



17. 撮影された顔画像が表示されます。
撮影を終了する場合は、[撮影完了]を押下します。



18. 以下のメッセージが表示されますので、[はい]を押下します。



撮影された顔画像が管理ポータルに登録されます。

19. [InstallShield Wizard の完了]ダイアログが表示されたらインストールは終了です。
[はい、今すぐコンピュータを再起動します。] を選択して [完了]を押下します。
OS を再起動します。



インストール手順は以上です。



Windows 再起動後から、UWF の無効、有効にかかわらず顔認証での Windows ログオンのご利用が可能です。

3.3. 設定変更ツールを使用して UWF を有効化する

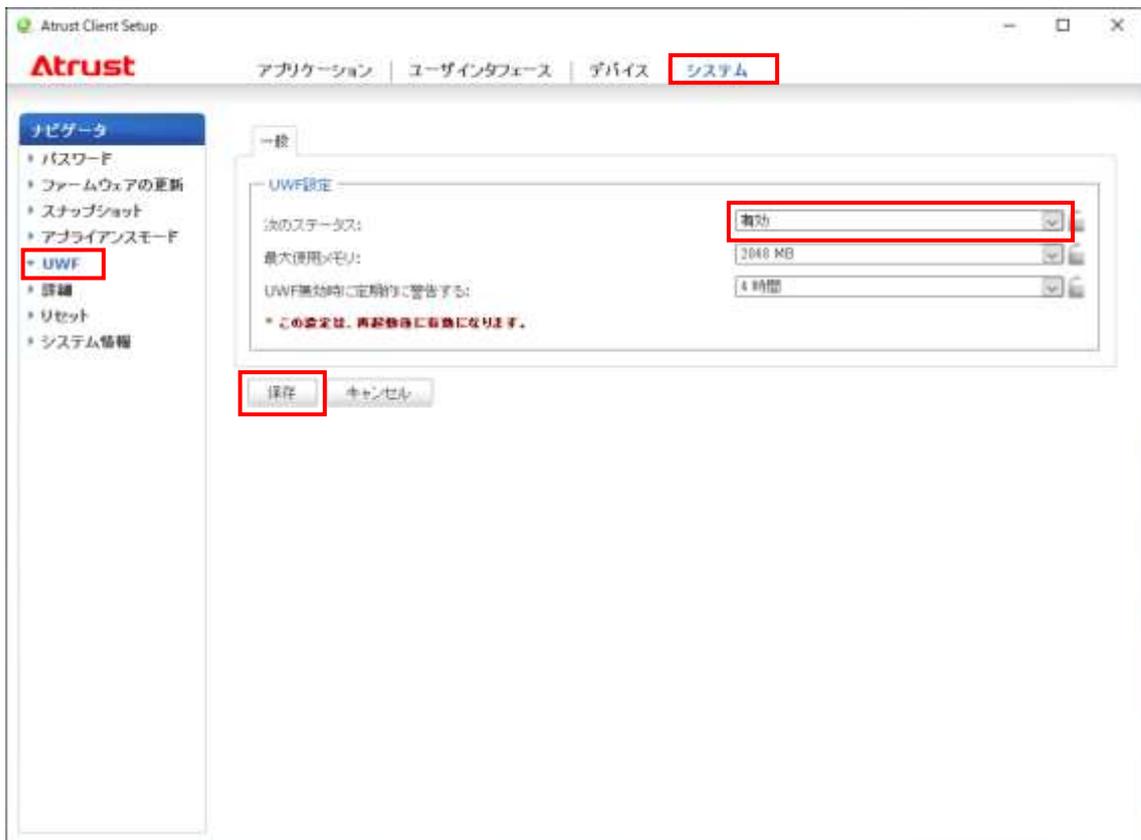
1. UWF を有効化します。機種により方法が異なります。

[Express5800 シリーズ US320g]

設定変更ツール Atrust Client Setup を使用して UWF を有効化します。

設定変更ツールの画面で「システム」－「UWF」を順に押下します。

「次のステータス」のプルダウンメニューを押下して「有効」を選択します。[保存]を押下します。再起動を求められたら、再起動をしてください。



[VersaPro シリーズ]

設定変更ツールのコマンドモードで UWF を有効化します。

「スタート」－「Windows システム ツール」を順に押下して、「コマンド プロンプト」を右クリックし、「その他」－[管理者として実行]を順に押下して、コマンドプロンプトを管理者として開きます。

コマンドプロンプトで次のコマンドを実行します。

- UWMGR.EXE filter enable

コマンド実行後、シンクライアント端末を再起動します。

3.4. 設定変更ツールを使用して個別の除外設定を行う

1. 設定変更ツールのコマンドモードで本製品が使用するフォルダやレジストリに除外設定を行います。

「スタート」-「Windows システム ツール」を順に押下して、「コマンド プロンプト」を右クリックし、「その他」-[管理者として実行]を順に押下して、コマンドプロンプトを管理者として開きます。

コマンドプロンプトで次の5つのコマンドを実行します。

- UWMGR File Add-Exclusion "C:¥Program Files¥NEC¥NeoFaceMonitor¥setting"
- UWMGR File Add-Exclusion "C:¥ProgramData¥NEC¥NeoFaceMonitor¥DataBase"
- UWMGR File Add-Exclusion "C:¥ProgramData¥SafeNet Sentinel"
- UWMGR File Add-Exclusion "C:¥NEC"
- UWMGR Registry Add-Exclusion "HKEY_LOCAL_MACHINE¥SOFTWARE¥NEC¥NeoFace"

コマンド実行後、シンクライアント端末を再起動します。

セットアップ手順は以上です。

NFM クラウド版クライアントの利用方法については、『NeoFace Monitor クラウド版ユーザーズマニュアル』をご覧ください。