

ARCACLAVIS NEXT

クライアント^{V2.1}操作ガイド

株式会社両備システムズ

改訂履歴

2024/11/30 15 版

目次

1. 本書について	9
1.1. 本書の表記	9
1.2. 用語	10
2. 概要	11
2.1. ARCACLAVIS NEXT クライアントの概要	11
2.2. 動作環境	11
2.3. セットアップ	11
2.4. スタートメニュー	12
2.4.1. NEXT クライアントモニター起動	13
2.4.2. NEXT 製品診断データ送信設定	14
2.5. ワンタイムパスワード認証の概要	15
2.5.1. ワンタイムパスワードシークレットの発行	16
2.5.2. ワンタイムパスワード認証	18
2.5.3. ワンタイムパスワードシークレットのリセット	20
3. NEXT Signin	22
3.1. NEXT Signin 機能の概要	22
3.2. サインイン認証	23
3.2.1. ICカードを利用したサインイン認証	23
3.2.2. 顔情報を利用したサインイン認証	30
3.2.3. スマートフォンの Authenticator アプリを利用したサインイン認証	45
3.2.4. Windows 自動認証を利用したサインイン認証	54
3.2.5. 複数の Windows アカウントによるサインイン	57

3.2.6. Windows パスワードをサインイン時に設定する	59
3.2.7. Windows アカウントの手入力.....	60
3.2.8. NEXT パスワードの有効期間	60
3.2.9. Windows パスワードの有効期間	60
3.2.10. NEXT 認証できない場合	61
3.2.11. ワンタイムパスワードの有効時間	63
3.3. パスワードの変更	64
3.3.1. NEXT パスワードの変更	64
3.3.2. Windows パスワードの変更.....	68
3.4. コンピューターのロック、ロック解除	72
3.4.1. コンピューターをロックする	72
3.4.2. コンピューターのロック解除をする.....	72
3.5. サインアウト、シャットダウン	79
3.6. ユーザーを切り替えてサインイン.....	80
3.7. 認証方式を切り替えてサインイン、ロック解除.....	83
3.8. NEXT 緊急パスワード認証でのサインイン、ロック解除.....	85
3.9. NEXT 管理者パスワード認証でのサインイン、ロック解除	87
3.10. Windows 標準認証でのサインイン、ロック解除.....	90
3.11. NEXT セーフモードでのサインイン、ロック解除	93
3.11.1 概要	93
3.11.2. NEXT セーフモードでサインイン、ロック解除	94
3.12. エラーメッセージ	96
3.12.1 IC カード認証時のエラーメッセージ	96

3.12.2 顔認証時のエラーメッセージ	98
3.12.3 ワンタイムパスワード認証時のエラーメッセージ	102
4. 認証情報の登録	104
4.1. ICカード登録	105
4.2. 顔情報登録	107
4.3. ワンタイムパスワード認証の情報登録	113
4.4. エラーメッセージ	118
4.4.1 ICカード登録時のエラーメッセージ	118
4.4.2 顔登録時のエラーメッセージ	120
4.4.3 ワンタイムパスワードシークレット発行時のエラーメッセージ	123
5. キャッシュ	125
5.1. 概要	125
5.2. オフラインの判定条件	125
5.3. オフライン時の NEXT パスワードの有効期限	126
5.4. オフライン時の NEXT アカウントのロックアウト	126
5.5. Windows ドメインコントローラーに対してオフライン時の Windows へのサインイン	126
5.6. オフライン時の Windows 自動認証	127
5.7. オフライン時の Windows パスワード変更	127
5.8. オフライン時の NEXT 緊急パスワード認証	127
5.9. オフライン時の NEXT 管理者パスワード認証	127
5.10. オフライン時の認証情報の登録	128
5.11. キャッシュの有効期間	128

5.12. キャッシュの更新	128
6. NEXT 離席モニター	129
6.1. 概要	129
6.2. NEXT 離席モニターによる離席監視.....	130
6.3. タスクトレイメニュー	135
6.4. 離席モニター画面	136
6.4.1. 照合待機中画面	136
6.4.2. 照合中画面	138
6.5. トースト通知.....	140
6.6. カメラ使用不能な場合の動作	142
6.7. 使用する顔情報.....	143
7. 自動認証	144
7.1. 概要	144
7.2. NEXT 自動認証プレイヤーによる自動認証	144
7.3. 起動	146
7.3.1. NEXT 自動認証プレイヤーの起動手順	146
7.3.2. NEXT 自動認証プレイヤーを利用できる NEXT ユーザーのロール設定	148
7.3.3. オフライン利用について	148
7.3.4. ユーザーの切り替えについて	148
7.4. 画面構成	149
7.5. 再生	150
7.5.1. プレイヤーメイン画面.....	150

7.5.2. 自動認証詳細画面	153
7.5.3. 自動認証プレイヤー再生例	154
7.5.4. 再生時のエラーメッセージ	173
7.6. 利用者による入力設定の編集	174
7.6.1. ユーザー設定画面	174
7.6.2. ユーザー入力値の設定手順	176
7.6.3. ユーザー入力値の編集許可	178
7.7. サーバー同期	179
7.8. 製品情報	181
7.9. エラーメッセージ	182
8. ユーザーポータル	183
8.1. 画面構成	183
8.2. サインイン	185
8.2.1. パスワード認証でのサインイン	185
8.2.2. ワンタイムパスワード認証でのサインイン	188
8.3. NEXT パスワード変更	191
8.4. ICカードの削除	192
8.5. ワンタイムパスワードシークレットの発行	194
8.6. スマートフォンの Authenticator アプリへの登録	198
8.7. ワンタイムパスワードシークレットのリセット	200
8.8. エラーメッセージ	202
付録	203

NEXT クライアントにリモートデスクトップ接続したら.....	203
IC カード認証、顔認証、ワンタイムパスワード認証のサインインオプションが表示されない....	203
NEXT 緊急パスワード認証、NEXT 管理者パスワード認証が表示されている場合	203
NEXT のサインインオプションはいずれも表示されず、Windows 標準資格プロバイダーが表示される場合	204
NEXT のサインインオプションはいずれも表示されず、Windows 標準資格プロバイダーも表示されない場合 ..	204
NEXT パスワード変更について.....	205
NEXT ユーザーの状態と NEXT 認証の可否	206
IC カード認証、顔認証	206
ワンタイムパスワード認証	206
NEXT 緊急パスワード認証.....	207

1. 本書について

株式会社両備システムズ 認証セキュリティ製品「ARCACLAVIS NEXT」をご利用いただき、誠にありがとうございます。

ARCACLAVIS NEXT（アルカクラヴィス ネクスト、以下、NEXT）は、パスワードによる認証にICカード認証や生体認証を組み合わせた二要素認証により、多くの情報を扱うコンピューター利用時の確実な本人認証を実現し、なりすまし、不正行為、情報漏えいを防ぐための認証強化を行うことができるセキュリティ製品です。

本書は、ARCACLAVIS NEXT のクライアントの操作について説明するクライアント操作ガイドです。

1.1. 本書の表記

本書は、以下に示す表記、記号、四角囲い付きスタイルで記載しています。

表記例	説明
<OK>、<キャンセル>、<次へ>、<適用>	ボタン名は、“<>”で囲んで表しています。
[ファイル]-[開く]	メニューのコマンドの選択順を表しています。
「ダイアログ名」、「入力値」、「画面名」、「ファイル名」	“ ”で囲んでいる箇所は、ダイアログ名や入力値などを表しています。
チェックする、チェックしない、チェックをはずす、オンする、オフする	チェックボックスなどを選択する/選択しない、ON/OFF することを表しています。
[Ctrl]キー	キーは、“[]”で囲んで表しています。
[Ctrl]+[Alt]+[Del]キー	“+”で連結しているキー表記は、同時に複数のキーを押すことを表しています。
※	注釈を表しています。補足説明、コメントを記載しています。
サインイン/サインアウト	「サインイン/サインアウト」「ログオン/ログオフ」の操作、機能名称は「サインイン/サインアウト」を使用して記載しています。



ご利用にあたり、注意いただきたい事項について説明します。



補足的な情報について説明します。

1.2. 用語

ARCACLAVIS NEXT の用語については、「ARCACLAVIS NEXT 用語集」を参照してください。

2. 概要

2.1. ARCACLAVIS NEXT クライアントの概要

ARCACLAVIS NEXT クライアント（以下、NEXT クライアント）とは、NEXT マネージャーで設定されたクライアント設定を利用して、NEXT クライアントソフトウェアをインストールしたコンピュータのことです。ユーザーは、ICカードや生体情報、ワンタイムパスワードなどの認証情報を利用して本人認証を行うことで NEXT クライアントにサインインします。NEXT クライアントは、本人認証に成功したユーザーの設定情報を NEXT サーバーからダウンロードし、その後の動作を決定します。

認証情報として IC カードを利用する場合、IC カード内の特定の情報を ID 情報として読み取るだけで、IC カードには書き込み処理を一切行わないため、既存の IC カードを一旦、回収して専用の情報を書き込む必要がなく、配布済みの IC カードをそのまま NEXT クライアントで利用することができます。

認証情報として顔情報を利用する場合、管理者の設定によって利用者側での顔情報登録ができます。

認証情報としてワンタイムパスワードを利用する場合、管理者の設定によって利用者側でワンタイムパスワードシークレットをスマートフォンの Authenticator アプリに登録することができます。

これにより、ARCACLAVIS NEXT システムの導入・展開を容易に行うことができます。

2.2. 動作環境

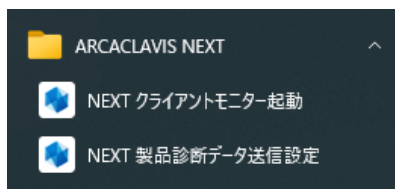
動作環境については、「ARCACLAVIS NEXT 動作環境一覧」を参照してください。

2.3. セットアップ

NEXT サーバー、NEXT クライアント、NEXT 離席モニター、NEXT 自動認証プレイヤーのセットアップについては、「ARCACLAVIS NEXT セットアップガイド」を参照してください。

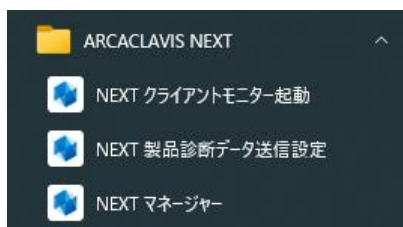
2.4. スタートメニュー

NEXT クライアントをインストールすると、スタートメニューに「NEXT クライアントモニター起動」、
「NEXT 製品診断データ送信設定」が追加されます。



NEXT クライアント(無料版)をインストールすると、スタートメニューに「NEXT クライアントモニター起動」、
「NEXT 製品診断データ送信設定」「NEXT マネージャー」が追加されます。

スタートメニューの「NEXT マネージャー」については、「ARCACLAVIS NEXT エディションガイド」を
参照してください。

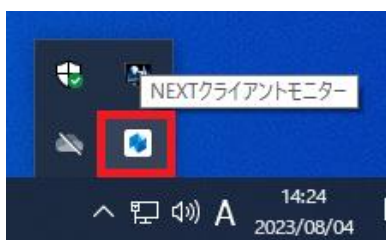


2.4.1. NEXT クライアントモニター起動

NEXT クライアントモニターは、NEXT クライアントの NEXT 認証サービスが停止していることの通知やロック解除時に自動で離席モニターを起動するなどの機能があります。

ロック解除時に離席モニターを起動する機能は、NEXT クライアントがインストールされているコンピューターに離席モニターがインストールされている場合に限りです。

Windows へサインイン後、NEXT クライアントモニターがタスクトレイの常駐アプリとして起動します。



タスクトレイで NEXT クライアントモニターが起動されていない場合、Windows のスタートメニューから「ARCACLAVIS NEXT」 - 「NEXT クライアントモニター起動」を実行してください。

NEXT クライアントにサインイン時、かつ NEXT クライアントモニターが起動中の場合、トースト通知が表示されます。

NEXT クライアントモニターで表示されるトースト通知は以下となります。

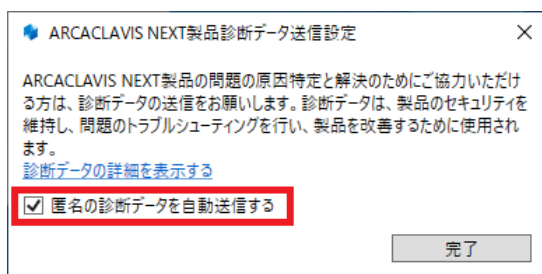
トースト通知のメッセージ内容	説明
クライアントモニターを開始しました	タスクトレイで NEXT クライアントモニターが起動されていない状態で、Windows のスタートメニューから「ARCACLAVIS NEXT」 - 「NEXT クライアントモニター起動」を実行した場合に表示されます。 ※既に NEXT クライアントモニターが起動中の場合は表示されません。
認証サービスが停止しているため、一部機能が使用できない場合があります 再起動しても認証サービスが停止している場合は、製品ヘルプを参照ください	NEXT セーフモードに移行した場合、または NEXT クライアントの NEXT 認証サービス「Js.Ssol.WebAPI.Server.Service」が停止中の場合に表示されます。 NEXT クライアントで使用する NEXT 認証サービスを手動で起動する手順については、「ARCACLAVIS NEXT トラブルシューティングガイド」を参照してください。

2.4.2. NEXT 製品診断データ送信設定

NEXT クライアントをご利用中に問題が発生した際、クラッシュレポートを送信する設定です。初期設定は、クラッシュレポートを送信する設定となっています。

クラッシュレポートの送信を無効化する場合は、以下の手順を行ってください。

1. NEXT クライアントがインストールされているコンピューターに管理者権限のユーザーでサインインしてください。
2. Windows のスタートメニューから「ARCACLAVIS NEXT」 - 「NEXT 製品診断データ送信設定」を実行してください。
3. 「ARCACLAVIS NEXT 製品診断データ送信設定」が起動されますので、「匿名の診断データを自動送信する」のチェックを外して<完了>ボタンをクリックしてください。



Info 送信される情報は、マイクロソフト社の App Center SDK によって収集されるデータとなります。

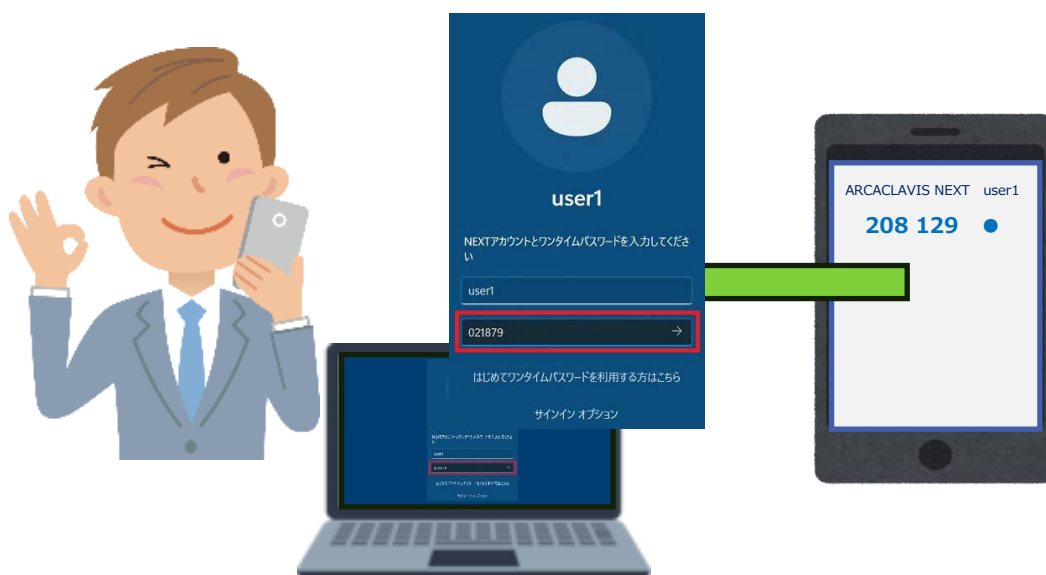
詳細は、以下の URL を参照してください。

App Center SDK によって収集されるデータ

<https://learn.microsoft.com/ja-jp/appcenter/sdk/data-collected>

2.5. ワンタイムパスワード認証の概要

ARCACLAVIS NEXT では、スマートフォンの Authenticator アプリを利用した 6 桁の数字によるワンタイムパスワード認証を利用できます。



ARCACLAVIS NEXT のワンタイムパスワード認証を利用するうえでの主なフローは以下の通りです。

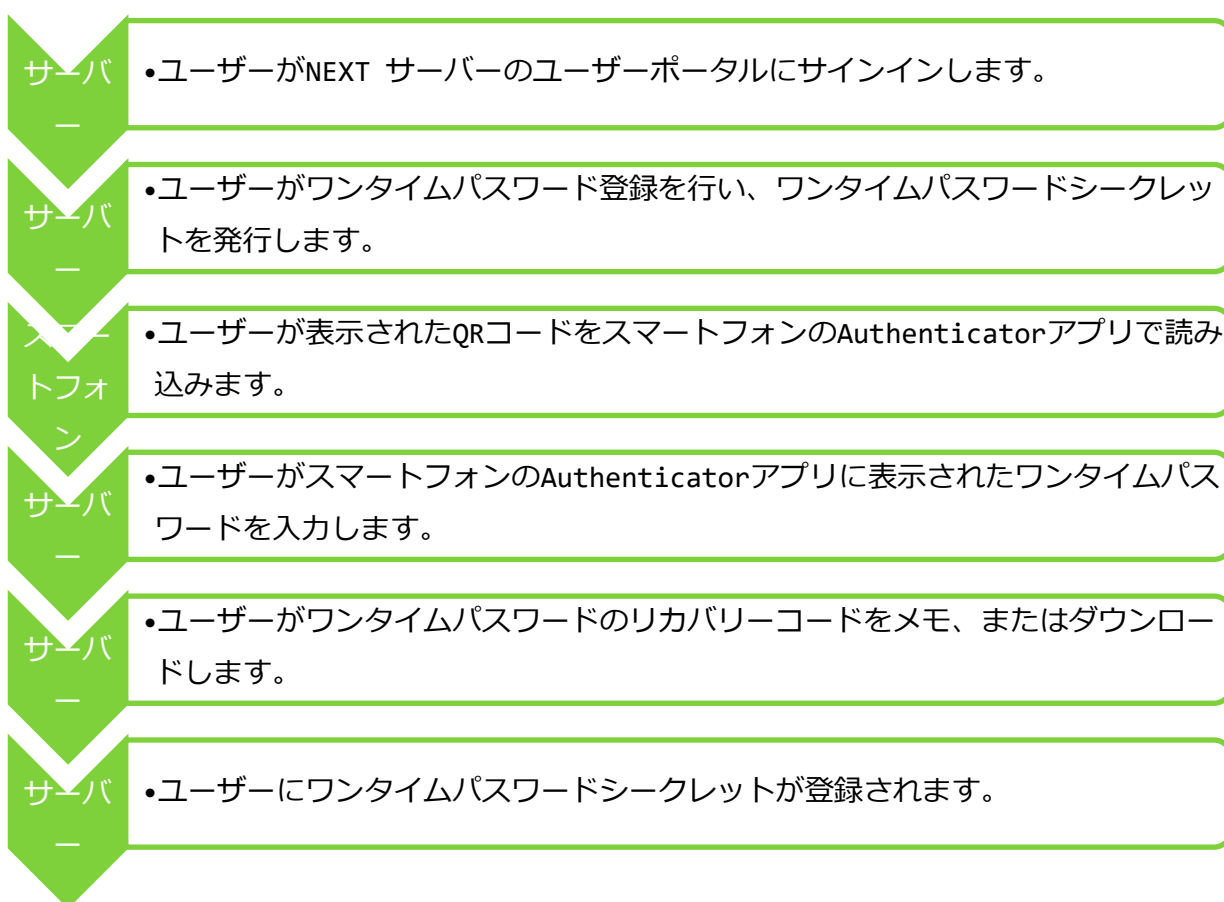
フロー	説明
ワンタイムパスワードシークレットの発行	ワンタイムパスワード認証を利用するうえでの事前準備として、ユーザーがワンタイムパスワードシークレットの発行を行います。
ワンタイムパスワード認証	ユーザーがワンタイムパスワードシークレットの発行を行うと、以下の機能を使用することができます。 <ul style="list-style-type: none"> ワンタイムパスワード認証による NEXT クライアントへのサインイン ワンタイムパスワード認証による NEXT マネージャーへの二段階認証
ワンタイムパスワードシークレットのリセット	ワンタイムパスワードシークレットを発行したスマートフォンを故障／紛失し、これまで利用していたスマートフォンを利用ができなくなった場合、ワンタイムパスワードシークレットを一度リセットし、再度ワンタイムパスワードシークレットを発行します。

2.5.1. ワンタイムパスワードシークレットの発行

ワンタイムパスワードシークレットの発行は、NEXT サーバーのユーザーポータル、またはNEXT クライアントで行うことができます。

Info NEXT サーバーの管理者ポータルでは、ワンタイムパスワードシークレットを発行することはできません。

1. NEXT サーバーのユーザーポータルでワンタイムパスワードシークレットを発行する場合は、以下の手順で行ってください。



Info NEXT サーバーのユーザーポータルでワンタイムパスワードシークレットを発行する手順については、「8.5. ワンタイムパスワードシークレットの発行」を参照してください。

2. NEXT クライアントでワンタイムパスワードシークレットを発行する場合は、以下の手順で行ってください。

クライアント

•ユーザーがNEXT クライアントのサインイン画面からワンタイムパスワード認証を選択します。

クライアント

•ユーザーがワンタイムパスワード登録を行い、ワンタイムパスワードシークレットを発行します。

スマートフォン

•ユーザーが表示されたQRコードをスマートフォンのAuthenticatorアプリで読み込みます。

クライアント

•ユーザーがスマートフォンのAuthenticatorアプリに表示されたワンタイムパスワードを入力します。

クライアント

•ユーザーがワンタイムパスワードのリカバリーコードをメモします。

クライアント

•ユーザーにワンタイムパスワードシークレットが登録されます。

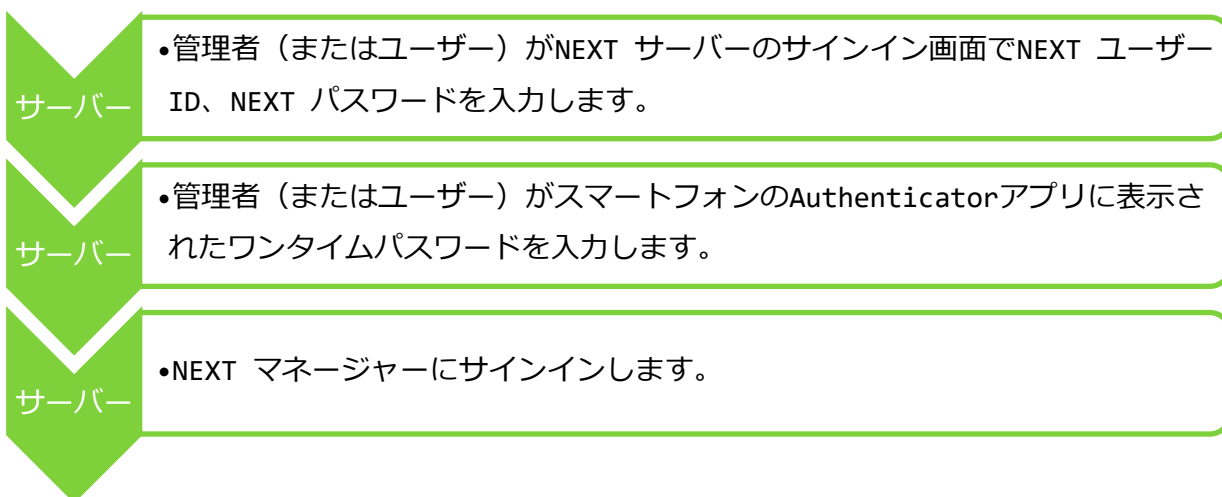
Info

NEXT クライアントでワンタイムパスワードシークレットを発行する手順については、「4.3. ワンタイムパスワード認証の情報登録」を参照してください。

2.5.2. ワンタイムパスワード認証

ワンタイムパスワード認証は、NEXT サーバー、および NEXT クライアントで行います。
ワンタイムパスワード認証を行う場合は、ワンタイムパスワードシークレットが発行済である必要があります。

1. NEXT サーバーでワンタイムパスワード認証を行う場合は、以下の手順で行ってください。



Info NEXT サーバーの管理者ポータルでワンタイムパスワード認証を行う手順については「ARCACLAVIS NEXT 管理者ガイド」を、ユーザーポータルでワンタイムパスワード認証を行う手順については「8.2.2. ワンタイムパスワード認証でのサインイン」を参照してください。

2. NEXT クライアントでワンタイムパスワード認証を行う場合は、以下の手順で行ってください。

ク
ラ
イ
ア
ン
ト

•ユーザーがNEXT クライアントのサインイン画面からワンタイムパスワード認証を選択します。

ク
ラ
イ
ア
ン
ト

•ユーザーがNEXT ユーザーID、NEXT パスワードを入力します。

ク
ラ
イ
ア
ン
ト

•ユーザーがスマートフォンのAuthenticatorアプリに表示されたワンタイムパスワードを入力します。

ク
ラ
イ
ア
ン
ト

•Windowsにサインインします。

Info

NEXT クライアントでワンタイムパスワード認証を行う手順については、「3.2.3. スマートフォンの Authenticator アプリを利用したサインイン認証」を参照してください。

2.5.3. ワンタイムパスワードシークレットのリセット

ユーザーのワンタイムパスワード認証を解除する場合、またはワンタイムパスワードシークレットを発行したスマートフォンが故障／紛失した場合に、リカバリーコードを使用してワンタイムパスワードシークレットのリセットを行う必要があります。

ワンタイムパスワードシークレットのリセットは、NEXT サーバーで行います。

対応者および手段		ワンタイムパスワードシークレットを発行したスマートフォンの利用が不可（故障／紛失など）	
		ユーザーはリカバリーコードの利用が可能	ユーザーはリカバリーコードの利用が不可（紛失など）
管理者	管理者ポータルで対象ユーザーのワンタイムパスワードシークレットをリセットする	○	○
ユーザー	ユーザーポータルにリカバリーコードを使用してサインインし、ワンタイムパスワードシークレットをリセットする	○	×

1. NEXT サーバーの管理者ポータルでワンタイムパスワードシークレットをリセットする場合は、以下の手順で行ってください。

サーバー

- 管理者がNEXT サーバーの管理者ポータルにサインインします。

サーバー

- 管理者がワンタイムパスワードシークレットをリセットするNEXT ユーザーのワンタイムパスワード設定画面を開きます。

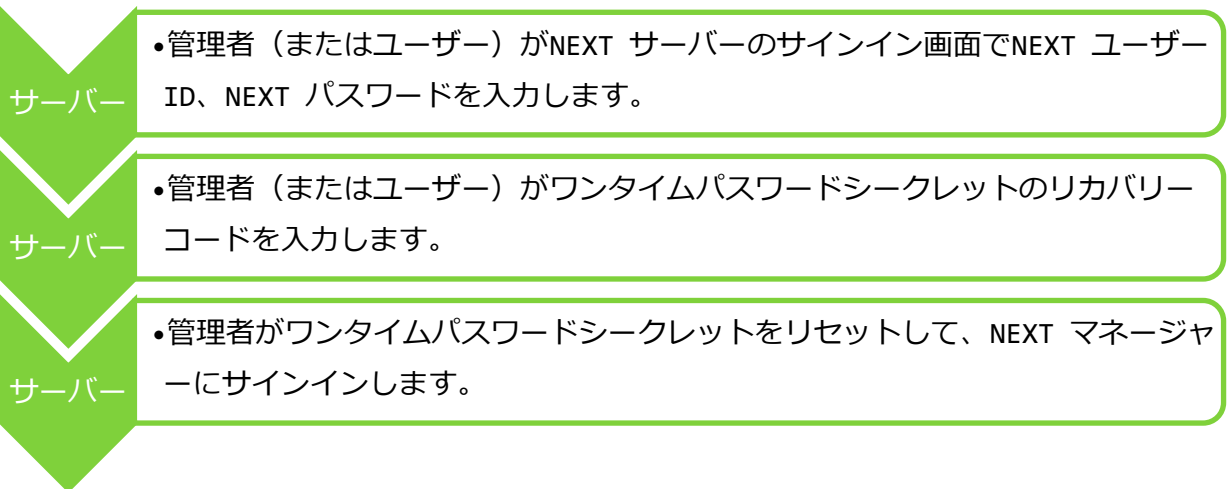
サーバー

- 管理者がワンタイムパスワードシークレットをリセットします。

Info

NEXT サーバーの管理者ポータルでワンタイムパスワードシークレットをリセットする手順については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。

2. NEXT サーバーでリカバリーコードを使用してワンタイムパスワードシークレットをリセットする場合は、以下の手順で行ってください。



Info NEXT サーバーでリカバリーコードを使用してワンタイムパスワードシークレットをリセットする手順については、「ARCACLAVIS NEXT トラブルシューティングガイド」を参照してください。

3. NEXT Signin

3.1. NEXT Signin 機能の概要

情報の入り口となるクライアントコンピューターを使用するユーザーの「本人認証」を強化することは、ローカルやネットワーク上のデータを保護することに繋がります。

この「本人認証の強化」を Windows へのサインイン時に適用することができるのが ARCACLAVIS NEXT の Signin 機能です。

Windows へのサインイン認証はコンピューターの起動後最初に行われる認証であり、また、ユーザーが初回のサインイン後に行うロック解除も、ローカルやネットワーク上のデータを保護するための「本人認証」です。NEXT Signin 機能では、この「本人認証」を認証方式や認証で利用する要素を組み合わせ設定、選択していただき、「本人認証の強化」を行います。



NEXT クライアントは、Windows の資格情報プロバイダー (Credential Provider) を利用するソフトウェアです。資格情報プロバイダーは Windows の OS が標準で提供するサインイン機能を拡張するために提供されている機能です。ユーザーの認証の方法として、IC カードや生体情報を利用するなどのカスタマイズを可能にしています。他社製品で同様に資格情報プロバイダーを利用しているアプリケーションは、NEXT クライアントと同じ環境にインストールして使用できない場合があります。ご注意ください。

3.2. サインイン認証

NEXT クライアントへのサインイン時に表示される画面、操作方法について説明します。NEXT クライアントのサインイン時の画面や認証手段は、NEXT マネージャーのユーザー情報の設定、クライアント設定により変わります。

3.2.1. IC カードを利用したサインイン認証

NEXT の IC カード認証機能がインストールされている PC では、Windows 起動時に以下のような初期画面が表示されます。この NEXT によるロックによって、不正なユーザーによる利用者 PC への Windows サインインを制御しています。






サインイン画面とサインイン方法は、NEXT マネージャーのユーザー情報の設定、クライアント設定により変わります。







クライアント設定			サインイン時に入力するもの	サインイン画面の参照先
NEXT パスワードを入力する	Windows ユーザー ID を自動入力する	Windows に自動サインインする		
オン	オンまたはオフ ※「Windows に自動サインイン」の設定を優先するため、いずれの設定でも可	オン	<ul style="list-style-type: none"> ・ IC カード ・ NEXT パスワード 	パターン 1








クライアント設定			サインイン時に入力するもの	サインイン画面の参照先
NEXT パスワードを入力する	Windows ユーザーIDを自動入力する	Windows に自動サインインする		
オン	オン	オフ	<ul style="list-style-type: none"> ・ IC カード ・ NEXT パスワード ・ Windows パスワード ※ユーザー情報に「Windows アカウント」の設定が1つも無い場合は、Windows ユーザーIDも入力する必要があります。	パターン 2
オン	オフ	オフ	<ul style="list-style-type: none"> ・ IC カード ・ NEXT パスワード ・ Windows ユーザーID ・ Windows パスワード 	パターン 3
オフ	オンまたはオフ ※「Windows に自動サインイン」の設定を優先するため、いずれの設定でも可	オン	<ul style="list-style-type: none"> ・ IC カード 	パターン 4
オフ	オン	オフ	<ul style="list-style-type: none"> ・ IC カード ・ Windows パスワード ※ユーザー情報に「Windows アカウント」の設定が1つも無い場合は、Windows ユーザーIDも入力する必要があります。	パターン 5
オフ	オフ	オフ	<ul style="list-style-type: none"> ・ IC カード ・ Windows ユーザーID ・ Windows パスワード 	パターン 6

サインイン画面のパターンは以下のようになります。

サインイン認証の画面の「ユーザーを選択」は左下のユーザー一覧からユーザーを選択している場合を、「他のユーザーを選択」はドメイン環境で表示される「他のユーザー」を選択した場合の、それぞれのサインイン認証の画面の成功時の遷移を表しています。

パターン	サインイン認証の画面	
パターン 1	ユーザーを選択	
	他のユーザーを選択	
パターン 2	ユーザーを選択	
	他のユーザーを選択	

パターン		サインイン認証の画面		
パターン 3	ユーザーを選択			
	他のユーザーを選択			
パターン 4	ユーザーを選択			
	他のユーザーを選択			
パターン 5	ユーザーを選択			
	ユーザーを選択			

パターン	サインイン認証の画面			
	他のユーザーを選択			
パターン 6	ユーザーを選択			
	他のユーザーを選択			

ICカードを使って Windows へサインインするには、以下の操作を行います。

ここでは、パターン 5 の設定で、ユーザーを選択し、ICカードと Windows パスワード入力でサインインする流れを例示します。

1. Windows を起動します

Windows 起動時に以下の初期画面が表示されます。

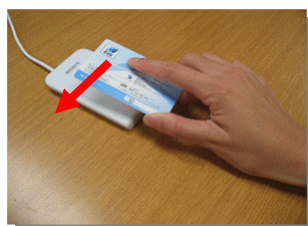


Info ICカード認証（ICカードで認証します）以外の表示になっている場合は、「サインイン オプション」で「ICカード認証」に切り替えてください。
詳細は、「3.7. 認証方式を切り替えてサインイン、ロック解除」を参照してください。

Info 表示される「サインイン オプション」は管理者の設定によります。「ICカード認証」を利用してサインイン、画面ロックの解除を行いたい場合は、認証方式として「ICカード認証」を有効化する必要があります。

2. ICカードリーダー/ライターにICカードをセットします

上記画面が表示されている状態で、ICカードリーダー/ライターにICカードをセットします。



3. Windows へサインインします

Windows サインインの「パスワード」を入力し、[Enter]キーを押すか、[→]アイコンをクリックします。



Info 「パスワード」を入力するエリアの「目のアイコン」をクリックしている間は、入力したパスワードを表示することができます。ご注意の上でご利用ください。

4. Windows へのサインインが完了します

Windows のデスクトップが表示されます。



Info Windows 認証では、サインイン先を変更することができます。
設定方法は、「3.6. ユーザーを切り替えてサインイン」を参照してください。

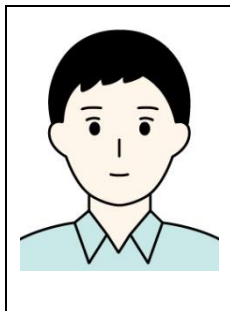


「NEXT パスワードを入力する」が無効でかつ IC カードを IC カードリーダー/ライターにセットした状態で PC を起動すると、セーフモードになる場合があります。
起動時にセーフモードとなった場合、少し時間をおいてから IC カードを IC カードリーダー/ライターにセットし直すと IC カード認証に成功します。

3.2.2. 顔情報を利用したサインイン認証

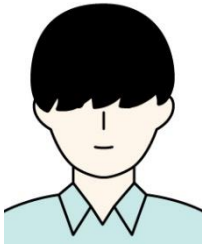










顔認証時に撮影される顔画像は、以下を参考にしてください。

➤ 良い顔画像の例



➤ 顔認証時に向かない顔画像の例

顔が揺れている	影がかかっている	逆光	白飛び	顔を傾けている (仰ぎ)
顔を傾けている (俯き)	顔を傾けている (横向き)	サングラス着用	帽子着用	マフラー着用

				
髪が目にかかっている	目、耳、口などの顔の一部を隠している	まばたき・目を閉じている	大きく口を開いている	メガネの角度で目の位置が不明瞭 1
				
メガネの角度で目の位置が不明瞭 2	顔の一部しか写っていない	複数人の写り込み	ぼやけている	カメラの解像度が不十分
				
写真でなりすます				

NEXT の顔認証機能がインストールされている PC では、Windows 起動時に以下のような初期画面が表示されます。この NEXT によるロックによって、不正なユーザーによる利用者 PC への Windows サインインを制御しています。

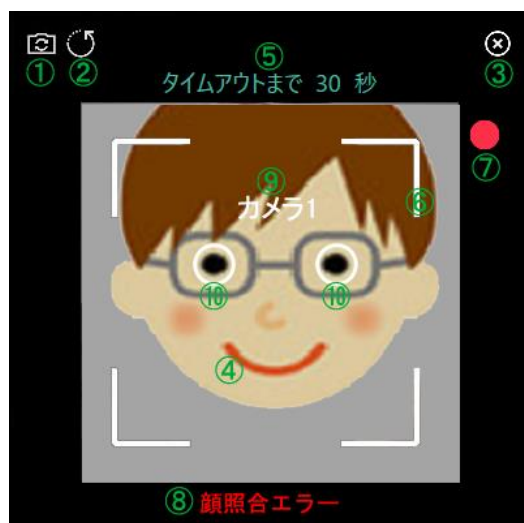


「NEXT ユーザーID」「NEXT パスワード」を入力し、[Enter]キーを押すか、[→]アイコンをクリックすると、顔照合を行います。

クライアント設定で「照合画面を表示する」の設定によって表示される画面が異なります。

「照合画面を表示する」がオフの場合	「照合画面を表示する」がオンの場合
	

以下に照合画面のデザイン、および各項目について説明します。



No	項目	補足
①	カメラ切り替えボタン	2つ以上カメラが接続されている場合、別のカメラに切り替わります。
②	カメラ回転ボタン	キャプチャ画像が90度ずつ回転します。
③	閉じるボタン	照合画面を閉じます。
④	キャプチャ画像	カメラからの画像が表示されます。
⑤	照合タイムアウト時間(秒)	30秒からカウントダウンし、0秒になると照合エラーとなります。 ※顔情報登録時は表示されません。
⑥	ガイド	顔認証が成功しやすくなる目安として表示しているガイドです。 ガイドの中に顔全体が映るように調整してください。
⑦	照合マーカー	顔照合中に表示されます。
⑧	メッセージ	顔照合の失敗時に「顔照合エラー」と表示されます。
⑨	カメラ番号	「カメラ切り替え」ボタンを押下時に使用されているカメラ番号が表示されます。 ※カメラ番号は1秒でフェードアウトします。
⑩	目のガイド	顔認証が成功しやすくなる目安として表示している目のガイドです。 2つの丸の中に両目が映るように調整してください。

NEXT ユーザーが利用する顔認証時に、まばたき検知機能を使用することができます。

まばたき検知機能とは、顔認証時に対象人物のまばたきをチェックする機能であり、写真によるなりすましを防ぐことができます。顔照合はまばたき検知後に行われます。また、まばたき検知は照合タイムアウト時間が 0 秒になるまで行います。

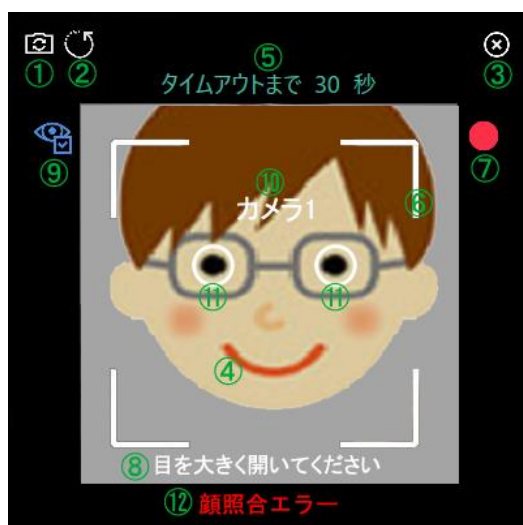
Info 目の座標が正しく取得できない環境だとまばたき検知に失敗する可能性があります。まばたき検知に成功しない場合は、以下の点に注意すると成功しやすくなります。

- ・室内が極端に暗い環境は避けてください。
- ・逆光のある環境は目が判別しにくくなります。
- ・サングラスを掛けている場合は外してください。

まばたき検知機能を有効にする場合は、クライアント設定の顔認証オプションで「強化する」を設定する必要があります。

なお、「強化する」を設定した場合は、クライアント設定の登録時に「照合画面を表示する」が自動的にオンに設定されます。

以下に顔認証オプションで「強化する」を設定したことによりまばたき検知機能が有効時の照合画面のデザイン、および各項目について説明します。

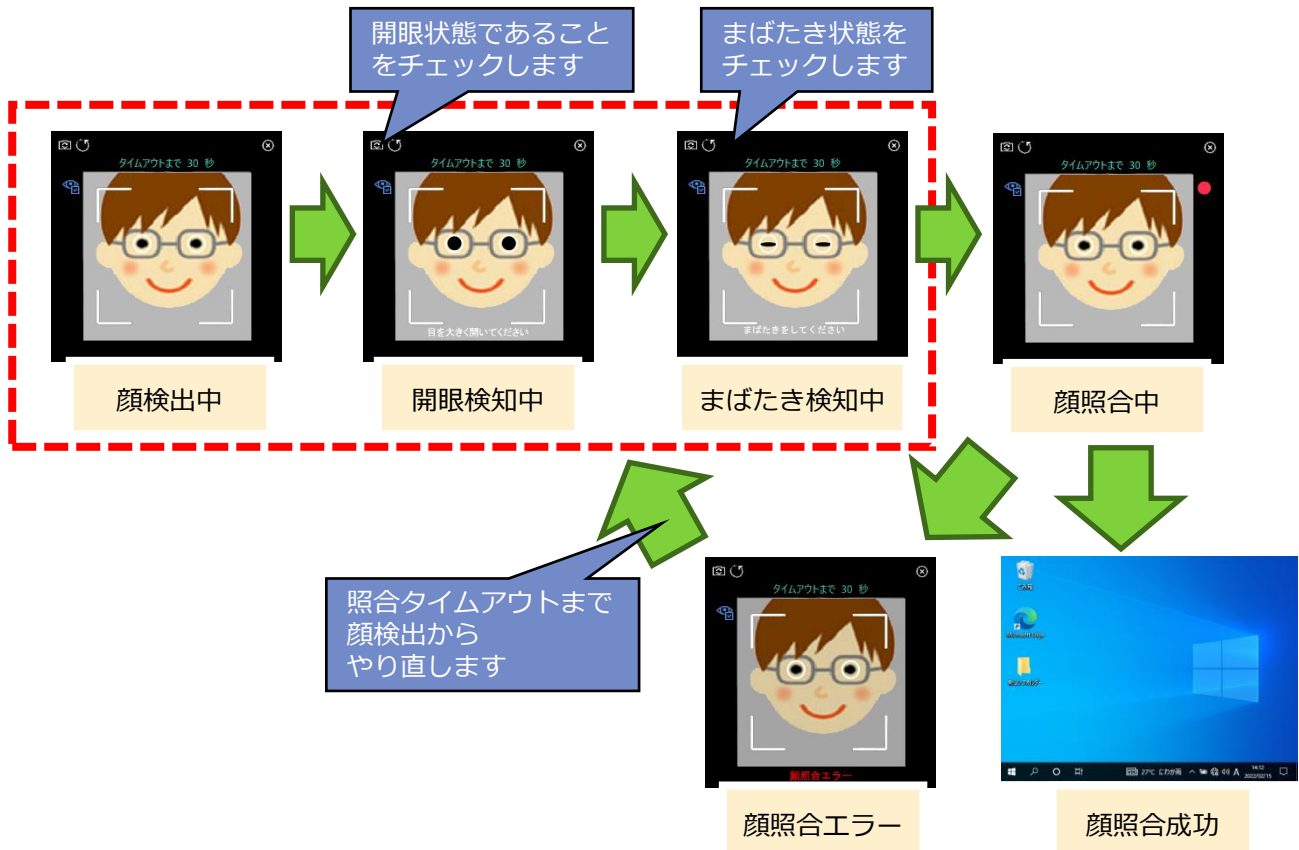


No	項目	補足
①	カメラ切り替えボタン	2つ以上カメラが接続されている場合、別のカメラに切り替わります。
②	カメラ回転ボタン	キャプチャ画像が90度ずつ回転します。
③	閉じるボタン	照合画面を閉じます。
④	キャプチャ画像	カメラからの画像が表示されます。
⑤	照合タイムアウト時間(秒)	30秒からカウントダウンし、0秒になると照合エラーとなります。 ※顔情報登録時は表示されません。
⑥	ガイド	顔認証が成功しやすくなる目安として表示しているガイドです。 ガイドの中に顔全体が映るように調整してください。
⑦	照合マーカー	顔照合中に表示されます。
⑧	メッセージ	まばたき検知の操作を指示するためのメッセージが表示されます。 メッセージ内容は、まばたき検知の状態によって切り替わります。 詳細は後述の「まばたき検知のメッセージ」を参照ください。
⑨	まばたき検知設定	クライアント設定の顔認証オプションで「強化する」が設定されている場合に表示されます。
⑩	カメラ番号	「カメラ切り替え」ボタンを押下時に使用されているカメラ番号が表示されます。 ※カメラ番号は1秒でフェードアウトします。
⑪	目のガイド	顔認証が成功しやすくなる目安として表示している目のガイドです。 2つの丸の中に両目が映るように調整してください。
⑫	エラーメッセージ	顔照合の失敗時に「顔照合エラー」と表示されます。

まばたき検知のメッセージは以下の通りです。

まばたき検知の状態	メッセージ	文字色
開眼検知中	目を大きく開いてください	白色
まばたき検知中	まばたきをしてください	白色

まばたき検知機能の流れは以下の通りです。



顔認証の状態	状態の説明
顔検出中	顔を検出しています。 カメラに向かって顔を正面に向けて、ガイドの中に顔全体が映るように調整してください。
開眼検知中	開眼状態をチェックしています。 カメラに向かって目を大きく開いてください。
まばたき検知中	まばたきを検知しています。 カメラに向かってまばたきをしてください。
顔照合中	顔を照合しています。
顔照合エラー	顔照合に失敗しました。 再度顔検出からやり直してください。
顔照合成功	顔照合に成功しました。

サインイン画面とサインイン方法は、NEXT マネージャーのユーザー情報の設定、クライアント設定により変わります。




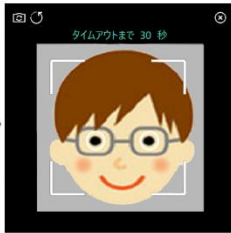

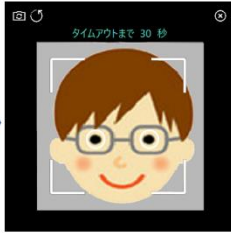

クライアント設定			サインイン時に入力するもの	サインイン画面の参照先
NEXT パスワードを入力する	Windows ユーザーIDを自動入力する	Windows に自動サインインする		
オン	オンまたはオフ ※「Windows に自動サインイン」の設定を優先するため、いずれの設定でも可	オン	<ul style="list-style-type: none"> ・顔情報 ・NEXT ユーザーID ・NEXT パスワード 	パターン 1
オン	オン	オフ	<ul style="list-style-type: none"> ・顔情報 ・NEXT ユーザーID ・NEXT パスワード ・Windows パスワード ※ユーザー情報に「Windows アカウント」の設定が 1 つも無い場合は、Windows ユーザーIDも入力する必要があります。	パターン 2
オン	オフ	オフ	<ul style="list-style-type: none"> ・顔情報 ・NEXT ユーザーID ・NEXT パスワード ・Windows ユーザーID ・Windows パスワード 	パターン 3
オフ	オンまたはオフ ※「Windows に自動サインイン」の設定を優先するため、いずれの設定でも可	オン	<ul style="list-style-type: none"> ・顔情報 ・NEXT ユーザーID 	パターン 4
オフ	オン	オフ	<ul style="list-style-type: none"> ・顔情報 ・NEXT ユーザーID ・Windows パスワード ※ユーザー情報に「Windows アカウント」の設定が 1 つも無い場合は、Windows ユーザーIDも入力する必要があります。	パターン 5

クライアント設定			サインイン時に入力するもの	サインイン画面の参照先
NEXT パスワードを入力する	Windows ユーザーIDを自動入力する	Windows に自動サインインする		
オフ	オフ	オフ	<ul style="list-style-type: none">・顔情報・NEXT ユーザーID・Windows ユーザーID・Windows パスワード	パターン6














サインイン画面のパターンは以下のようになります。

サインイン認証の画面の「ユーザーを選択」は左下のユーザー一覧からユーザーを選択している場合を、「他のユーザーを選択」はドメイン環境で表示される「他のユーザー」を選択した場合の、それぞれのサインイン認証の画面の成功時の遷移を表しています。

※以下の図の中にある照合画面は、クライアント設定で「照合画面を表示する」を選択している場合に表示されます。

パターン	サインイン認証の画面	
パターン 1	ユーザーを選択	 
	他のユーザーを選択	 
パターン 2	ユーザーを選択	  
	他のユーザーを選択	  

パターン	サインイン認証の画面	
<p>パターン 3</p> <p>ユーザーを選択</p>		
	<p>他のユーザーを選択</p>	
<p>パターン 4</p> <p>ユーザーを選択</p>		
	<p>他のユーザーを選択</p>	

パターン	サインイン認証の画面			
パターン 5	ユーザーを選択			
	他のユーザーを選択			
パターン 6	ユーザーを選択			
	他のユーザーを選択	 		

顔認証を使って Windows へサインインするには、以下の操作を行います。

ここでは、パターン 5 の設定で、ユーザーを選択し、顔情報、NEXT ユーザーID と Windows パスワード入力でサインインする流れを例示します。

※クライアント設定で「照合画面を表示する」をオンに設定している場合の例示となります。

1. Windows を起動します

顔認証機能がインストールされている利用者 PC では、Windows 起動時に以下の初期画面が表示されます。「NEXT ユーザーID」を入力し、[Enter]キーを押すか、[→]アイコンをクリックします。



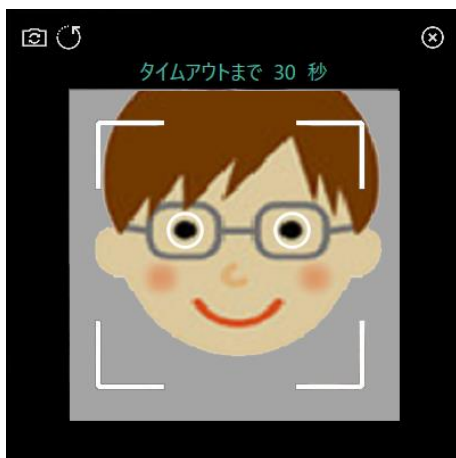
Info 顔認証以外の表示になっている場合は、「サインイン オプション」で切り替えてください。
詳細は、「3.7. 認証方式を切り替えてサインイン、ロック解除」を参照してください。

Info 表示される「サインイン オプション」は管理者の設定によります。「顔認証」を利用してサインイン、画面ロックの解除を行いたい場合は、認証方式として「顔認証」を有効化する必要があります。

Info 前回、顔認証、またはワンタイムパスワード認証に成功し、Windows へのサインインが成功していた場合は、「NEXT ユーザーID」にサインインを行った NEXT ユーザーの NEXT ユーザーID が自動で入力されます。
ただし、NEXT セーフモードでの認証成功時は対象外となります。

2. 顔認証を行います

照合画面が表示された後に Web カメラが起動し、顔情報の照合を行いますので、Web カメラに顔を向けてください。



Info カメラが複数ある場合は、「カメラ切り替え」ボタンを押下して顔認証で使用したいカメラに切り替えてください。インカメラ、アウトカメラがある場合も、顔認証で使用したいカメラに切り替えてください。
顔認証、または顔情報登録で最後に使用したカメラを記憶して、次回以降は記憶したカメラを使用します。

Info クライアント設定で「照合画面を表示する」をオフに設定している場合は、照合画面が表示されず以下の画面が表示されます。



カメラが複数ある場合、[カメラ切り替え]をクリックして、顔認証で利用するカメラを選択してください。インカメラ、アウトカメラがある場合も、[カメラ切り替え]をクリックして、顔認証で利用するカメラを選択してください。
顔認証、または顔情報登録で最後に使用したカメラを記憶して、次回以降は記憶したカメラを使用します。

Info 「顔照合エラー」や「顔認証に失敗しました」とエラーが表示される場合は、「ARCACLAVIS NEXT トラブルシューティングガイド」を参照してください。

3. Windows へサインインします

Windows サインインの「パスワード」を入力し、[Enter]キーを押すか、[→]アイコンをクリックします。



Info 「パスワード」を入力するエリアの「目のアイコン」をクリックしている間は、入力したパスワードを表示することができます。ご注意の上でご利用ください。

4. Windows へのサインインが完了します

Windows のデスクトップが表示されます。



Info Windows 認証では、サインイン先を変更することができます。設定方法は、「3.6. ユーザーを切り替えてサインイン」を参照してください。

3.2.3. スマートフォンの Authenticator アプリを利用したサインイン認証

NEXT のワンタイムパスワード認証機能がインストールされている PC では、Windows 起動時に以下のような初期画面が表示されます。この NEXT によるロックによって、不正なユーザーによる利用者 PC への Windows サインインを制御しています。






サインイン画面とサインイン方法は、NEXT マネージャーのユーザー情報の設定、クライアント設定により変わります。





クライアント設定			サインイン時に入力するもの	サインイン画面の参照先
NEXT パスワードを入力する	Windows ユーザーIDを自動入力する	Windows に自動サインインする		
オン	オンまたはオフ ※「Windows に自動サインイン」の設定を優先するため、いずれの設定でも可	オン	<ul style="list-style-type: none"> • NEXT ユーザーID • NEXT パスワード • ワンタイムパスワード 	パターン 1



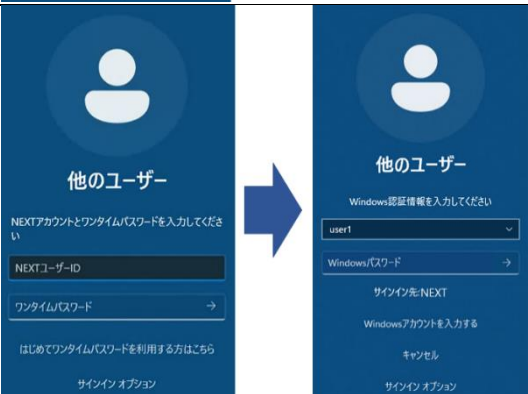

クライアント設定			サインイン時に入力するもの	サインイン画面の参照先
NEXT パスワードを入力する	Windows ユーザーID を自動入力する	Windows に自動サインインする		
オン	オン	オフ	<ul style="list-style-type: none"> ・NEXT ユーザーID ・NEXT パスワード ・ワンタイムパスワード ・Windows パスワード ※ユーザー情報に「Windows アカウント」の設定が 1 つも無い場合は、Windows ユーザーID も入力する必要があります。	パターン 2
オン	オフ	オフ	<ul style="list-style-type: none"> ・NEXT ユーザーID ・NEXT パスワード ・ワンタイムパスワード ・Windows ユーザーID ・Windows パスワード 	パターン 3
オフ	オンまたはオフ ※「Windows に自動サインイン」の設定を優先するため、いずれの設定でも可	オン	<ul style="list-style-type: none"> ・NEXT ユーザーID ・ワンタイムパスワード 	パターン 4
オフ	オン	オフ	<ul style="list-style-type: none"> ・NEXT ユーザーID ・ワンタイムパスワード ・Windows パスワード ※ユーザー情報に「Windows アカウント」の設定が 1 つも無い場合は、Windows ユーザーID も入力する必要があります。	パターン 5
オフ	オフ	オフ	<ul style="list-style-type: none"> ・NEXT ユーザーID ・ワンタイムパスワード ・Windows ユーザーID ・Windows パスワード 	パターン 6

サインイン画面のパターンは以下のようになります。

サインイン認証の画面の「ユーザーを選択」は左下のユーザー一覧からユーザーを選択している場合を、「他のユーザーを選択」はドメイン環境で表示される「他のユーザー」を選択した場合の、それぞれのサインイン認証の画面の成功時の遷移を表しています。

パターン	サインイン認証の画面	
パターン 1	ユーザーを選択	
	他のユーザーを選択	
パターン 2	ユーザーを選択	

パターン	サインイン認証の画面	
	他のユーザーを選択	
パターン 3	ユーザーを選択	
	他のユーザーを選択	
パターン 4	ユーザーを選択	

パターン	サインイン認証の画面	
	他のユーザーを選択	
パターン 5	ユーザーを選択	
	他のユーザーを選択	
パターン 6	ユーザーを選択	

パターン	サインイン認証の画面			
	<p>他のユーザーを選択</p>			

ワンタイムパスワードを使って Windows へサインインするには、以下の操作を行います。
ここでは、パターン 5 の設定で、ユーザーを選択し、NEXT ユーザーID、ワンタイムパスワードと Windows パスワード入力でサインインする流れを例示します。

1. Windows を起動します

Windows 起動時に以下の初期画面が表示されます。

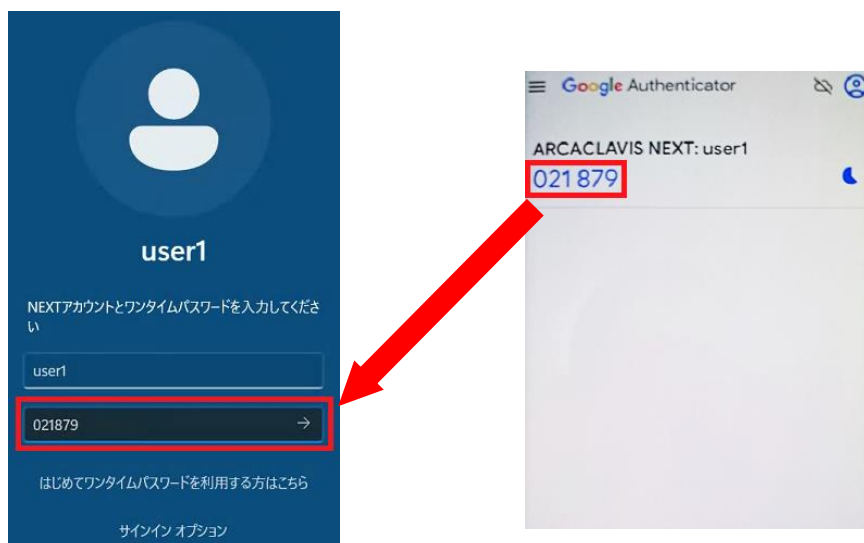


Info ワンタイムパスワード認証以外の表示になっている場合は、「サインイン オプション」で「ワンタイムパスワード認証」に切り替えてください。
詳細は、「3.7. 認証方式を切り替えてサインイン、ロック解除」を参照してください。

Info 表示される「サインイン オプション」は管理者の設定によります。「ワンタイムパスワード認証」を利用してサインイン、画面ロックの解除を行いたい場合は、認証方式として「ワンタイムパスワード認証」を有効化する必要があります。

Info 前回、顔認証、またはワンタイムパスワード認証に成功し、Windows へのサインインが成功していた場合は、「NEXT ユーザーID」にサインインを行った NEXT ユーザーの NEXT ユーザーID が自動で入力されます。
ただし、NEXT セーフモードでの認証成功時は対象外となります。

2. 「NEXT ユーザーID」とスマートフォンの Authenticator アプリに表示されている「ワンタイムパスワード」を入力します。



Info ワンタイムパスワードは 30 秒ごとに更新され、有効時間を過ぎたワンタイムパスワードは無効となります。ワンタイムパスワードの有効時間については、「3.2.11. ワンタイムパスワードの有効時間」を参照してください。

3. Windows へサインインします

Windows サインインの「パスワード」を入力し、[Enter]キーを押すか、[→]アイコンをクリックします。



Info 「パスワード」を入力するエリアの「目のアイコン」をクリックしている間は、入力したパスワードを表示することができます。ご注意の上でご利用ください。

4. Windows へのサインインが完了します
Windows のデスクトップが表示されます。



Info Windows 認証では、サインイン先を変更することができます。
設定方法は、「3.6. ユーザーを切り替えてサインイン」を参照してください。

3.2.4. Windows 自動認証を利用したサインイン認証

NEXT マネージャーのクライアント設定で「Windows に自動サインインする」がオンの場合、ユーザー情報の「Windows アカウント」で設定されている「Windows ユーザーID」と「Windows パスワード」で Windows に自動認証することができます。

Windows 自動認証は以下の認証方式で利用できます。

- ・ IC カード認証
- ・ 顔認証
- ・ ワンタイムパスワード認証
- ・ NEXT 緊急パスワード認証

Windows 自動認証時に、Windows アカウントが無効化されているなどで、サインインができない場合は、Windows サインイン画面に遷移します。キャンセルをクリックすることで各資格情報プロバイダーの初期画面に戻ります。管理者に Windows 自動認証で利用する Windows アカウントの状態をご確認ください。

Windows 自動認証時に、NEXT ユーザー情報の「Windows アカウント」の設定が 1 つも無い場合は、エラーとなり、「Windows アカウントが未登録のため、ログインすることはできません」とメッセージが表示されます。管理者に NEXT ユーザー情報の Windows 自動認証で利用する Windows アカウントの設定をご確認ください。

NEXT クライアントが NEXT サーバーと通信できないオフライン状態でも、キャッシュがあるユーザーは、Windows 自動認証が行えます。

オフライン状態のときに Windows パスワードを変更した場合、NEXT サーバーと通信できないため、変更後の Windows パスワードは保存されません。そのため、サインイン/ロック解除の度に Windows 自動認証はエラーとなり、Windows パスワードの再入力が必要となります。NEXT サーバーと通信できるオンライン状態で、Windows パスワードの再入力を行うことで、NEXT サーバーに Windows パスワードが保存され、次回以降、Windows 自動認証が行えます。

Windows パスワードなしの Windows アカウント設定は、Windows パスワードが未設定の状態と区別できないため、都度、Windows パスワード入力画面が表示されます。

Info Windows 自動認証を利用する NEXT ユーザー情報に、Windows パスワードの設定がされていない場合については、「3.2.6. Windows パスワードをサインイン時に設定する」を参照してください。

Info ユーザー情報の「Windows アカウント」に複数の「Windows ユーザーID」を設定して、複数の Windows アカウントでの自動サインインも可能です。複数の Windows アカウントによるサインインの詳細は、「3.2.5. 複数の Windows アカウントによるサインイン」を参照してください。

ここでは、ICカードを使って Windows へ自動サインインする場合として、「3.2.1. ICカードを利用したサインイン認証」のパターン1の設定で、ユーザーを選択し、ICカードとNEXTパスワード入力でサインインする流れを例示します。

1. Windows を起動します

Windows 起動時に以下の初期画面が表示されます。



Info ICカード認証（ICカードで認証します）以外の表示になっている場合は、「サインインオプション」で「ICカード認証」に切り替えてください。
詳細は、「3.7. 認証方式を切り替えてサインイン、ロック解除」を参照してください。

2. ICカードリーダー/ライターにICカードをセットします

上記画面が表示されている状態で、ICカードリーダー/ライターにICカードをセットします。

ICカードが検出されると、「ICカード：検出済み」と表示されます。



3. NEXT パスワードを入力します

「NEXT パスワード」を入力し、[Enter]キーを押すか、[→]アイコンをクリックします。



4. Windows へのサインインが完了します

Windows のデスクトップが表示されます。

Windows アカウントは、ユーザー情報に設定されている Windows アカウント設定を利用して自動サインインします。



Info Windows 認証では、サインイン先を変更することができます。
設定方法は、「3.6. ユーザーを切り替えてサインイン」を参照してください。

3.2.5. 複数の Windows アカウントによるサインイン

ユーザー情報の「Windows アカウント」に複数の「Windows ユーザーID」を設定している場合、複数の Windows アカウントによるサインインを選択することができます。

ここでは、複数の「Windows ユーザーID」が設定されている NEXT ユーザーで、IC カードを使って Windows へ自動サインインする場合として、「3.2.1. IC カードを利用したサインイン認証」のパターン 1 の設定で、他のユーザーを選択して、IC カードと NEXT パスワード入力でサインインする流れを例示します。

1. Windows を起動します

Windows 起動時に以下の初期画面が表示されます。



Info IC カード認証 (IC カードで認証します) 以外の表示になっている場合は、「サインイン オプション」で「IC カード認証」に切り替えてください。
詳細は、「3.7. 認証方式を切り替えてサインイン、ロック解除」を参照してください。

2. IC カードリーダー/ライターに IC カードをセットします

上記画面が表示されている状態で、IC カードリーダー/ライターに IC カードをセットします。
IC カードが検出されると、「IC カード: 検出済み」と表示されます。

3. NEXT パスワードを入力します

「NEXT パスワード」を入力し、[Enter]キーを押すか、[→]アイコンをクリックします。

4. Windows ユーザーID をリストから選択します
「Windows ユーザーID」を選択します。



5. Windows へのサインインが完了します
Windows のデスクトップが表示されます。
Windows アカウントは、ユーザー情報に設定されている複数の Windows アカウント設定から、選択した Windows アカウント設定を利用して自動サインインします。



Info Windows 認証では、サインイン先を変更することができます。
設定方法は、「3.6. ユーザーを切り替えてサインイン」を参照してください。

3.2.6. Windows パスワードをサインイン時に設定する

NEXT マネージャーのクライアント設定で「Windows に自動サインインする」がオンで、ユーザー情報の「Windows パスワード」が設定されていない Windows アカウントでサインインする場合、ユーザーは Windows パスワードを設定しないと NEXT クライアントにサインインできません。

最初のサインイン時に下図が表示されます。サインインする Windows アカウントに設定する「Windows パスワード」を入力し、[Enter]キーを押すか、[→]アイコンをクリックします。設定した Windows アカウントで Windows 認証を行います。認証に成功すると、Windows パスワードの設定が保存され、次回以降は Windows に自動サインインします。認証に失敗した場合は設定が保存されず、次回サインイン時に再度下図が表示されます。



Info 最初のサインインによる設定時に、Windows パスワードの有効期限切れでエラーとなった場合は、Windows パスワード変更画面を表示します。変更が完了したら、変更後のパスワードを保存し、次回以降は Windows に自動サインインします。

3.2.7. Windows アカウントの手入力

NEXT マネージャーのクライアント設定で「Windows ユーザーID を自動入力する」がオフで、かつ「Windows に自動サインインする」がオフの場合、下図のようにサインイン画面に「Windows アカウントを入力する」が表示され、Windows ユーザーID、Windows パスワードをユーザーが手入力してサインインできます。

Windows 認証画面では、「Windows アカウントを入力する」と「Windows アカウントを選択する」をクリックすることで、それぞれのサインイン認証画面を切り替えることができます。



Info NEXT マネージャーのクライアント設定で「Windows ユーザーID を自動入力する」がオフで、「Windows に自動サインインする」がオンの場合でも、ユーザー情報に「Windows アカウント」の設定が1つも無い場合は、Windows ユーザーID を手入力する必要があります。

3.2.8. NEXT パスワードの有効期間

NEXT マネージャーのポリシー設定で NEXT パスワードの有効期間を設定している場合、有効期限が切れると、NEXT パスワードの変更画面が表示されます。新しい NEXT パスワードに変更してください。NEXT パスワードの変更については、「3.3.1. NEXT パスワードの変更」を参照してください。

3.2.9. Windows パスワードの有効期間

ローカルまたはドメインのセキュリティポリシーで Windows パスワードの有効期間を設定している場合、有効期限が切れると、Windows パスワードの変更画面が表示されます。新しい Windows パスワードに変更してください。

Windows パスワードの変更については、「3.3.2. Windows パスワードの変更」を参照してください。

3.2.10. NEXT 認証できない場合

NEXT クライアントの操作は、管理者が設定する NEXT マネージャーのポリシー設定、ユーザー設定や、Windows のドメインセキュリティポリシーやユーザーアカウント設定の内容によって各種の制限を受けます。ここでは、NEXT マネージャーのポリシー設定、ユーザー設定の制限により NEXT 認証できない場合について説明します。

・NEXT ユーザーの無効化

管理者によって NEXT ユーザーが無効化されている場合、「ユーザーがロックされています」のメッセージが表示されてサインインできません。再びサインインできるようにするためには、管理者が NEXT ユーザーを有効にする必要があります。



・NEXT ユーザーの有効期間

管理者によって NEXT ユーザーに有効期間が設定されている場合、有効期間を過ぎると、「ユーザーの有効期限切れです」のメッセージが表示されてサインインできません。再びサインインできるようにするためには、管理者が NEXT ユーザーの有効期間を変更する必要があります。



・NEXT ユーザーのロックアウト

管理者によってポリシー設定で「NEXT ユーザーのロックアウトのしきい値」が設定されている場合、ユーザーがNEXT 認証に失敗した回数が設定されたしきい値に達すると、NEXT ユーザーがロックアウトされて、「ユーザーがロックされています」のメッセージが表示されてサインインできません。再びサインインできるようにするためには、管理者がロックアウトを解除する必要があります。

NEXT ユーザーのロックアウトの動作仕様およびロックアウトの解除方法については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。



・オフライン状態でのキャッシュの有効期間

管理者によってポリシー設定で「オフライン有効日数」が設定されている場合、設定されている日数以上のオフライン状態が続くと、「オフライン有効期限が切れています」のメッセージが表示されてサインインできません。再びサインインできるようにするためには、NEXT サーバーとNEXT クライアントを通信できる状態にして、サインインする必要があります。



オフライン状態でNEXT クライアントを利用している場合、NEXT 認証に失敗してもNEXT サーバーと通信できないため、ロックアウトの失敗回数はカウントされません。

・ワンタイムパスワードの有効時間

ワンタイムパスワードは30秒ごとに更新され、有効時間をすぎたワンタイムパスワードは使用できません。詳細は、「3.2.11. ワンタイムパスワードの有効時間」を参照してください。

3.2.11. ワンタイムパスワードの有効時間

ワンタイムパスワードの有効時間は30秒となるため、ご利用のコンピューターとスマートフォンの時間がずれにくい環境での利用が前提となります。

スマートフォンの Authenticator アプリに表示されるワンタイムパスワードは、30秒ごとに更新されます。ワンタイムパスワードが更新され、有効時間を過ぎたワンタイムパスワードを入力した場合は認証失敗となるため、ワンタイムパスワードの入力が間に合わない場合は、次のワンタイムパスワードが表示されるのを待ってから入力してください。

頻繁にワンタイムパスワードの認証に失敗する場合は、「ARCACLAVIS NEXT トラブルシューティングガイド」を参照してください。

Info ワンタイムパスワードの有効時間を伸ばす設定は、セキュリティの関係上、用意していません。
ワンタイムパスワードの更新間隔は、RFC6238 基準であり、更新間隔はデフォルト値として30秒を推奨しています。また、スマートフォンの Authenticator アプリも同様にワンタイムパスワードの更新間隔は30秒となっています。

3.3. パスワードの変更

3.3.1. NEXT パスワードの変更

NEXT マネージャーのポリシー設定で 以下の設定のとき、NEXT パスワードの変更画面が表示されます。新しい NEXT パスワードに変更してください。

ポリシー設定	説明
「初回サインイン時に NEXT パスワードを変更する」がオン	<ul style="list-style-type: none"> ・ユーザーが初めて NEXT 認証を行うとき ・管理者が NEXT マネージャーで NEXT ユーザーのパスワードをリセットしたとき <p>サインイン認証だけでなく、IC カード登録、顔情報登録を行うときにも NEXT 認証が必要なため、これらの登録時が初めての NEXT 認証の場合があります。</p>
「NEXT パスワード有効日数」に 1 以上の日数を設定	<ul style="list-style-type: none"> ・NEXT パスワード最終更新日から「NEXT パスワード有効日数」を過ぎたとき <p>NEXT パスワード最終更新日は NEXT マネージャーの NEXT ユーザー一覧で確認できます。</p>

Info NEXT パスワードを変更する画面によって、更新される内容が異なります。詳細は、「付録 NEXT パスワード変更について」を参照してください。

ここでは、ICカードとNEXTパスワード入力で初回サインインするときのNEXTパスワード変更の流れを例示します。

「3.2.1. ICカードを利用したサインイン認証」のパターン1の設定で、行います。

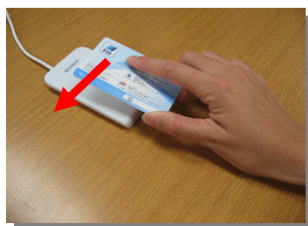
1. Windows を起動します

Windows 起動時に以下の初期画面が表示されます。



2. ICカードリーダー/ライターにICカードをセットします

上記画面が表示されている状態で、ICカードリーダー/ライターにICカードをセットします。



3. NEXTパスワードを入力します

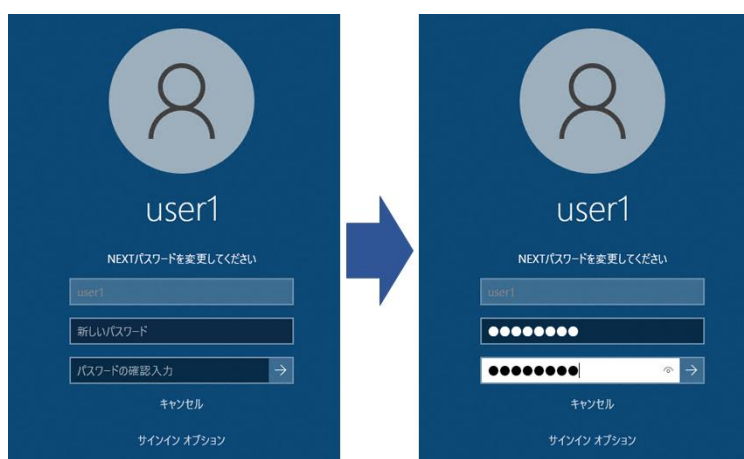
「NEXTパスワード」を入力し、[Enter]キーを押すか、[→]アイコンをクリックします。



4. NEXT パスワードの変更を促すメッセージが表示されます
<OK>ボタンをクリックします。



5. NEXT パスワードの変更画面が表示されます
「新しいパスワード」、「パスワードの確認入力」に新しく設定する「NEXT パスワード」を入力し、
[Enter]キーを押すか、[→]アイコンをクリックします。



Info 前回と同じ NEXT パスワードへの変更はできません。
[新しいパスワード]は、現在の NEXT パスワードと異なるパスワードを設定してください。

6. Windows へのサインインが完了します

NEXT パスワード変更が完了し、そのまま Windows にサインインし、Windows のデスクトップが表示されます。



3.3.2. Windows パスワードの変更

Windows パスワードは、管理者が設定するドメインセキュリティポリシーやユーザーアカウント設定の内容によって、変更を行う必要があります。これらの設定により Windows からパスワード変更が求められた場合、NEXT クライアントの各資格情報プロバイダーは、ユーザーに Windows パスワードの変更を行う画面を表示します。たとえば、Windows パスワードの有効期限切れのときや、Windows ユーザーのプロパティで「ユーザーは次回ログオン時にパスワードの変更が必要」がオンのときに表示されます。

ここでは、IC カードと NEXT パスワード入力でサインインするときに、Windows からパスワード変更が要求されたときの Windows パスワード変更の流れを例示します。

「3.2.1. IC カードを利用したサインイン認証」のパターン 1 の設定で、行います。

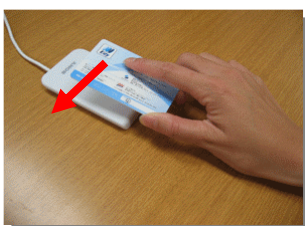
1. Windows を起動します

Windows 起動時に以下の初期画面が表示されます。



2. IC カードリーダー/ライターに IC カードをセットします

上記画面が表示されている状態で、IC カードリーダー/ライターに IC カードをセットします。



3. NEXT パスワードを入力します

「NEXT パスワード」を入力し、[Enter]キーを押すか、[→]アイコンをクリックします。



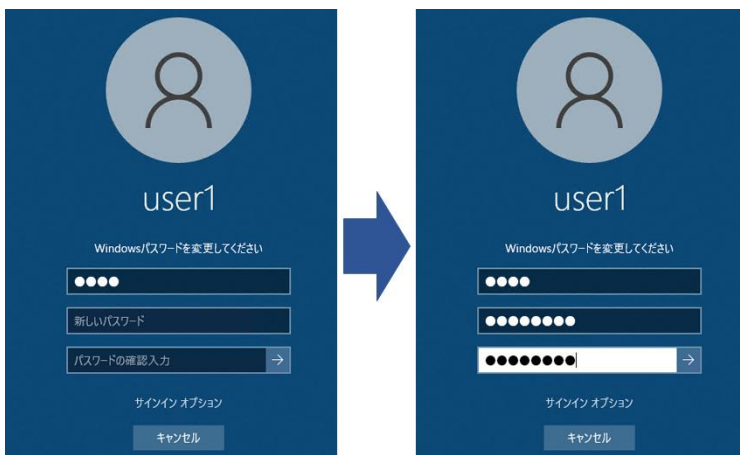
4. Windows パスワードの変更を促すメッセージが表示されます

<OK>ボタンをクリックします。



5. Windows パスワードの変更画面が表示されます

「新しいパスワード」、「パスワードの確認入力」に新しく設定する Windows パスワードを入力し、[Enter]キーを押すか、[→]アイコンをクリックします。



6. Windows パスワードの変更が終了したメッセージが表示されます
<OK>ボタンをクリックします。



入力した新しい Windows パスワードが、Windows が求める複雑さ、長さ、履歴などの要件を満たしていない場合、以下のメッセージが表示されます。再度、要件を満たすように新しい Windows パスワードを入力してください。



7. Windows へのサインインが完了します

Windows パスワード変更が完了し、そのまま Windows にサインインし、Windows のデスクトップが表示されます。



Info 正しく Windows パスワード変更が終了した場合、NEXT ユーザー情報の Windows アカウントの Windows パスワードには、新しい Windows パスワードを保存し直します。NEXT マネージャーのクライアント設定の「Windows に自動サインインする」がオンの NEXT クライアントでは、次回以降、新しい Windows パスワードで自動サインインが行われます。



[Ctrl]+[Alt]+[Del]キーを押して表示されるオプション画面から[パスワードの変更]を行うと、NEXT ユーザー情報の Windows アカウントの Windows パスワードに保存できません。この[パスワードの変更]は Windows 標準資格情報プロバイダーのためです。

3.4. コンピューターのロック、ロック解除

3.4.1. コンピューターをロックする

以下の方法により、手動でコンピューターにロックをかけることができます。

- ・ [Windows]+[L]キーを押します。
- ・ [Ctrl]+[Alt]+[Del]キーを押して表示されるオプション画面から[ロック]をクリックします。
- ・ [スタートメニュー]-[ユーザー名]-[ロック]をクリックします。

また、Windows 10 のスクリーンセーバーの設定で、「待ち時間」に任意の時間を入力し、「再開時にログイン画面に戻る」にチェックを入れることで、スクリーンセーバーから復帰した時にロックをかけることができます。

Info Windows 10 のアップデートによって、設定、操作手順、機能などが異なる場合があります。

3.4.2. コンピューターのロック解除をする

IC カードを使って Windows の画面ロックを解除するには、以下の操作を行います。

ここでは、「3.2.1. IC カードを利用したサインイン認証」のパターン 5 の設定で、ユーザーを選択し、IC カードと Windows パスワード入力でサインインして、ロックしている状態からロック解除する流れを例示します。

1. IC カードリーダー/ライターに IC カードをセットします

以下の画面が表示されている状態で、IC カードリーダー/ライターに IC カードをセットします。



2. Windows へサインインします

Windows サインインの「パスワード」を入力し、[Enter]キーを押すか、[→]アイコンをクリックします。



3. 画面ロック解除が完了します

IC カード認証完了後、Windows のデスクトップが表示されます。



顔認証を使って Windows の画面ロックを解除するには、以下の操作を行います。

ここでは、「3.2.2. 顔情報を利用したサインイン認証」のパターン 5 の設定で、ユーザーを選択し、顔情報、NEXT ユーザーID と Windows パスワード入力でサインインして、ロックしている状態からロック解除する流れを例示します。

※クライアント設定で「照合画面を表示する」をオンに設定している場合の例示となります。

1. NEXT ユーザーID を入力します

顔認証機能がインストールされている利用者 PC では、ロック解除時に以下の画面が表示されます。

「NEXT ユーザーID」は入力されていますので、[Enter]キーを押すか、[→]アイコンをクリックします。

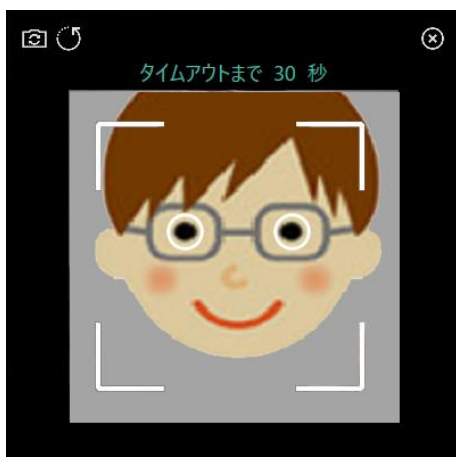


Info 顔認証以外の表示になっている場合は、「サインイン オプション」で切り替えてください。
詳細は、「3.7. 認証方式を切り替えてサインイン、ロック解除」を参照してください。

Info 前回、顔認証、またはワンタイムパスワード認証に成功し、Windows のロック解除が成功していた場合は、「NEXT ユーザーID」にロック解除を行った NEXT ユーザーの NEXT ユーザーID が自動で入力されます。
ただし、NEXT セーフモードでの認証成功時は対象外となります。

2. 顔認証を行います

照合画面が表示された後に Web カメラが起動し、顔情報の照合を行いますので、Web カメラに顔を向けてください。



Info カメラが複数ある場合は、「カメラ切り替え」ボタンを押下して顔認証で使用したいカメラに切り替えてください。インカメラ、アウトカメラがある場合も、顔認証で使用したいカメラに切り替えてください。
顔認証、または顔情報登録で最後に使用したカメラを記憶して、次回以降は記憶したカメラを使用します。

Info クライアント設定で「照合画面を表示する」をオフに設定している場合は、照合画面が表示されず以下の画面が表示されます。



カメラが複数ある場合、[カメラ切り替え]をクリックして、顔認証で利用するカメラを選択してください。インカメラ、アウトカメラがある場合も、[カメラ切り替え]をクリックして、顔認証で利用するカメラを選択してください。
顔認証、または顔情報登録で最後に使用したカメラを記憶して、次回以降は記憶したカメラを使用します。

Info 「顔照合エラー」や「顔認証に失敗しました」とエラーが表示される場合は、「ARCACLAVIS NEXT トラブルシューティングガイド」を参照してください。

3. Windows へサインインします

Windows サインインの「パスワード」を入力し、[Enter]キーを押すか、[→]アイコンをクリックします。



4. 画面ロック解除が完了します

Windows のデスクトップが表示されます。

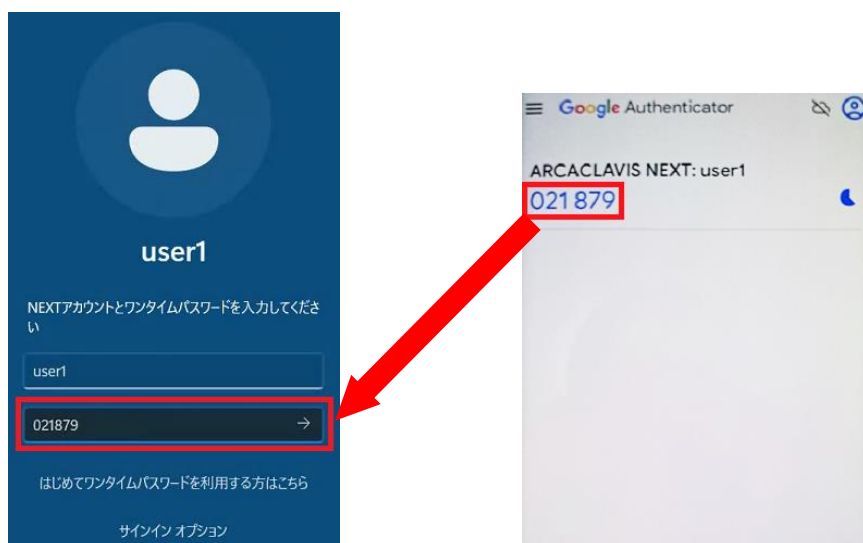


ワンタイムパスワード認証を使って Windows の画面ロックを解除するには、以下の操作を行います。
ここでは、「3.2.3. スマートフォンの Authenticator アプリを利用したサインイン認証」のパターン 5 の設定で、ユーザーを選択し、NEXT ユーザーID、ワンタイムパスワードと Windows パスワード入力でサインインして、ロックしている状態からロック解除する流れを例示します。

1. NEXT ユーザーID を入力します

ワンタイムパスワード認証機能がインストールされている利用者 PC では、ロック解除時に以下の画面が表示されます。

「NEXT ユーザーID」は入力されていますので、「ワンタイムパスワード」を入力して[Enter]キーを押すか、[→]アイコンをクリックします。



Info ワンタイムパスワード認証以外の表示になっている場合は、「サインイン オプション」で切り替えてください。
詳細は、「3.7. 認証方式を切り替えてサインイン、ロック解除」を参照してください。

2. Windows へサインインします

Windows サインインの「パスワード」を入力し、[Enter]キーを押すか、[→]アイコンをクリックします。



3. 画面ロック解除が完了します
Windows のデスクトップが表示されます。



3.5. サインアウト、シャットダウン

サインアウト/シャットダウンするには、以下の方法があります。

- ・[スタートメニュー]-[ユーザー名]-[サインアウト]または、[スタートメニュー]-[ユーザー名]-[シャットダウン]を選択します。
- ・[Ctrl]+[Alt]+[Del]キーを押して表示されるオプション画面から[サインアウト]または、画面右下に表示される<電源>ボタンから[シャットダウン]をクリックします。
- ・サインイン認証画面で、画面右下に表示される<電源>ボタンから[シャットダウン]をクリックします。

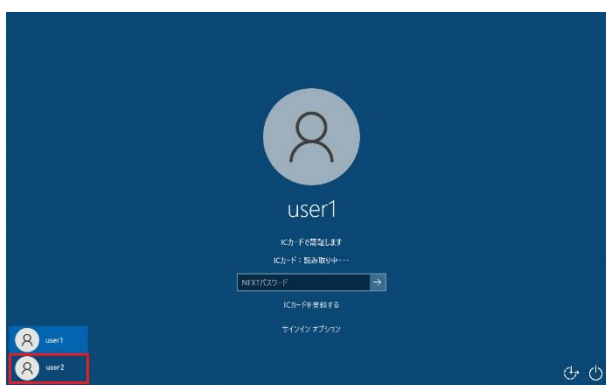
3.6. ユーザーを切り替えてサインイン

あるユーザーが画面ロックしている PC で、別のユーザーに切り替えてサインインしたい場合は、以下の手順で行います。

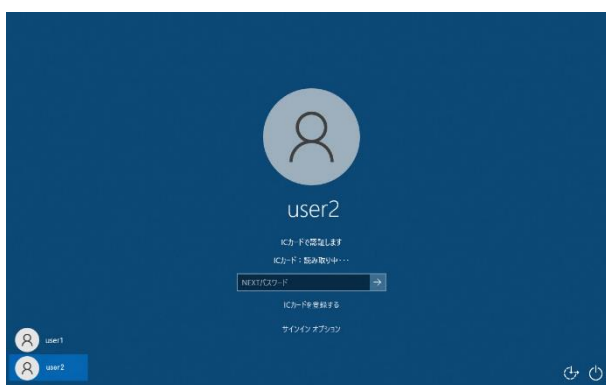
使用環境によって表示画面が異なりますので、使用環境に応じた手順を行ってください。

➤ ワークグループ環境

1. 画面ロックされている状態で切り替えたいユーザー名をクリックします
左下に表示されているユーザー名をクリックします。
ここでは、「User2」をクリックします。



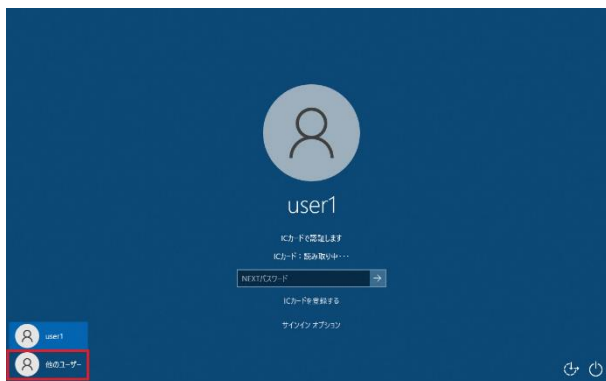
2. 切り替えたユーザー名が表示されます



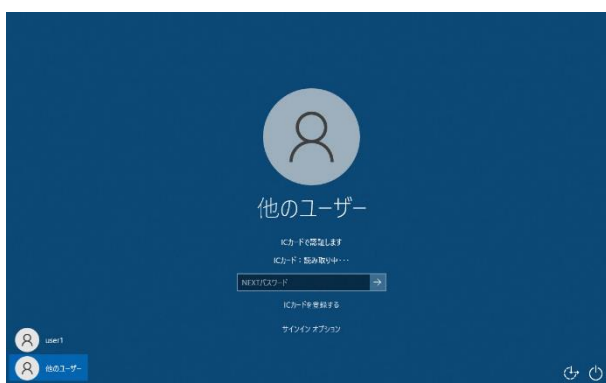
以降の操作は、[3.2.1. IC カードを利用したサインイン認証]、[3.2.2. 顔情報を利用したサインイン認証]、[3.2.3. スマートフォンの Authenticator アプリを利用したサインイン認証]と同様です。それぞれの手順を参照してサインインしてください。

➤ ドメイン環境

1. 画面ロックされている状態で[他のユーザー]をクリックします
左下に表示されている他のユーザーをクリックします。



2. 「他のユーザー」が表示されます



以降の操作は、[3.2.1. IC カードを利用したサインイン認証]、[3.2.2. 顔情報を利用したサインイン認証]、[3.2.3. スマートフォンの Authenticator アプリを利用したサインイン認証]と同様です。それぞれの手順を参照してサインインしてください。

Info Windows 認証では、NEXT マネージャーのユーザー情報に設定されている Windows アカウント設定を使用します。

Windows ユーザーID に別のドメイン、ローカルコンピューターを指定することで、サインイン先を変更することができます。詳しくは以下補足を参照ください。

Info

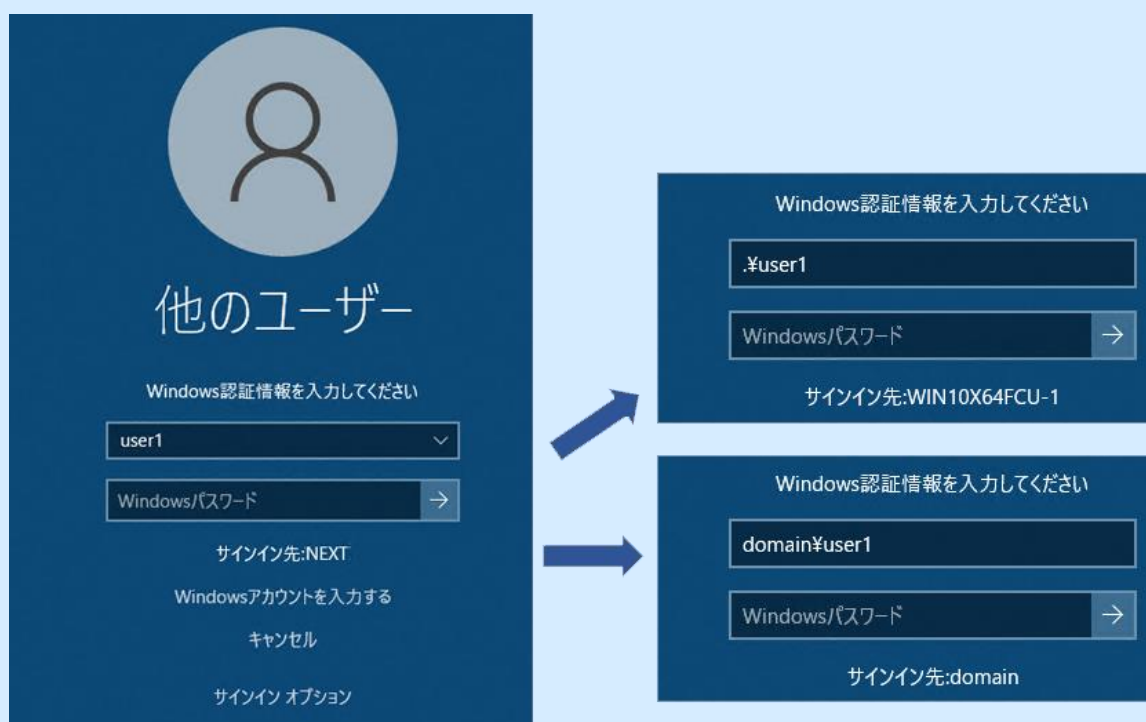
- ・ドメインに参加している PC では「サインイン先」はドメインが選択されていますので、そのままドメインにサインインできます。
- ・ワークグループに参加している PC では「サインイン先」はローカルコンピューターが選択されていますので、そのままローカルコンピューターにサインインできます。
- ・ドメインに参加している PC で、違うドメインやローカルコンピューターにサインインする場合は、Windows ユーザーID に「.¥」や「¥」を使用します。

サインイン先の変更例を以下に記載します。

「NEXT」のドメインに参加している場合、「NEXT」のドメインにサインインできます。Windows ユーザーID に「.¥User1」を入力すると、ローカルコンピューターにサインインできます。

Windows ユーザーID に「domain¥User1」を入力すると、「domain」の別ドメインにサインインできます。

※「Windows アカウントを入力する」でも同様にサインイン先を変更できます。

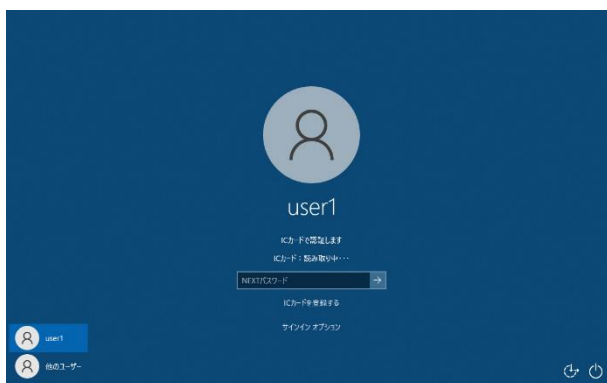


3.7. 認証方式を切り替えてサインイン、ロック解除

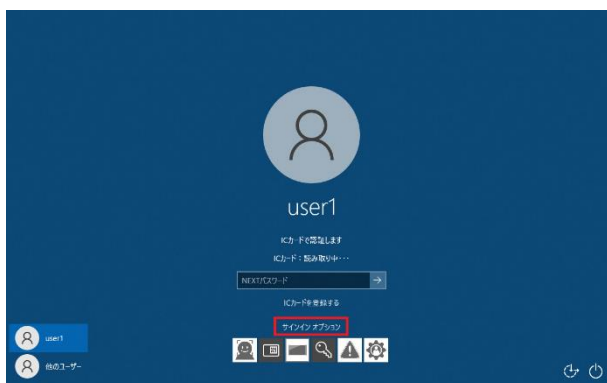
サインイン時や画面ロック解除時に、認証方式を切り替えてサインインや画面ロックを解除したい場合は、以下の手順で行います。

以下の例は、「最初のサインイン時はICカード認証でサインインした後、画面ロック解除時に顔認証を利用するケース」です。他のケースでは「サインイン オプション」で選択する認証方式を変えることで同様の操作になります。

1. ICカード認証でサインインした後、画面ロックすると以下の画面が表示されます



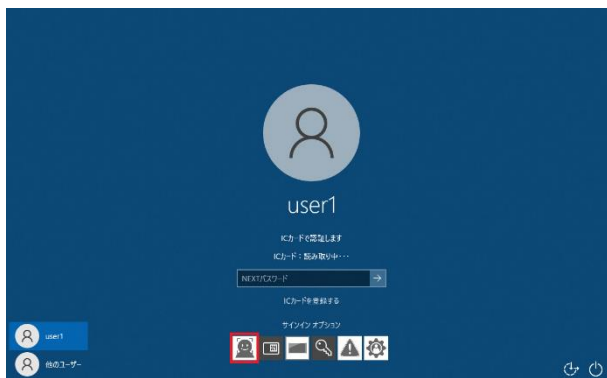
2. 「サインイン オプション」をクリックします
サインインオプションのアイコンが表示されます。



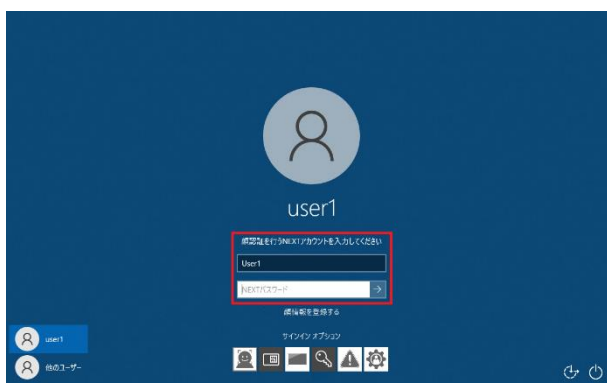
Info 表示される「サインイン オプション」は、管理者の設定によります。

3. 利用したい認証方式のアイコンをクリックします

ここでは、顔認証を利用して画面ロックを解除したいので、[顔認証]のサインインオプションアイコンをクリックします。



4. 顔認証用のサインイン画面に切り替わります



以降の操作は、「3.2.2. 顔情報を利用したサインイン認証」と同様です。手順を参照してサインインしてください。

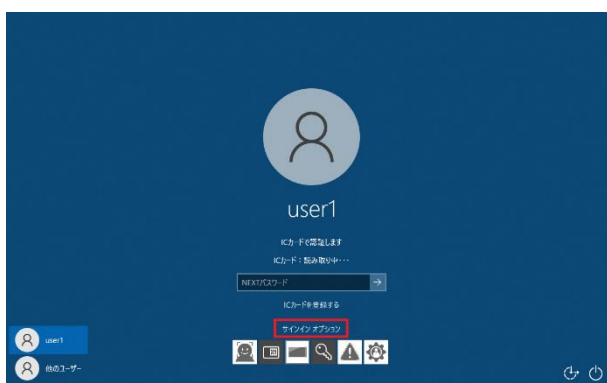
3.8. NEXT 緊急パスワード認証でのサインイン、ロック解除

NEXT 緊急パスワード認証は、IC カードを忘れた、外出先でカメラが壊れてしまった場合などに NEXT ユーザーID と NEXT 緊急パスワードの入力による認証を行うことにより、NEXT クライアントの機能を有効にしたままコンピューターを利用するための機能です。

オフライン状態で NEXT 緊急パスワード認証でのサインイン、ロック解除はできますが、Windows 自動認証を使用するには、そのコンピューターに IC カード、顔認証などで NEXT 認証を行いサインインしたことがあり、サインインしようとするユーザーのキャッシュが存在する必要があります。キャッシュが存在しない場合は、Windows 自動認証が行えませんので、手動で Windows 認証を行ってください。

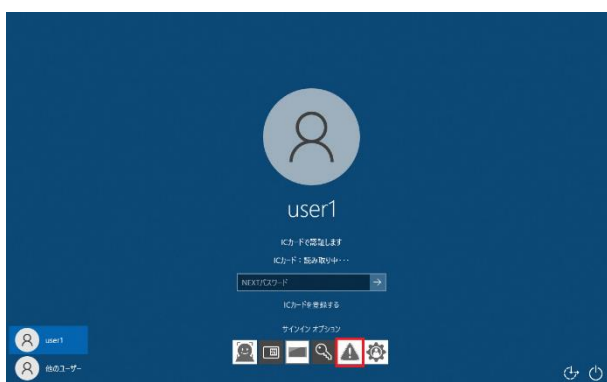
ここでは、IC カードを使って Windows へ自動サインインする「3.2.1. IC カードを利用したサインイン認証」のパターン 1 の設定から、NEXT 緊急パスワード入力でサインインする流れを例示します。

1. 管理者から通知された NEXT 緊急パスワードを用意します
2. 「サインイン オプション」をクリックします
サインインオプションのアイコンが表示されます。

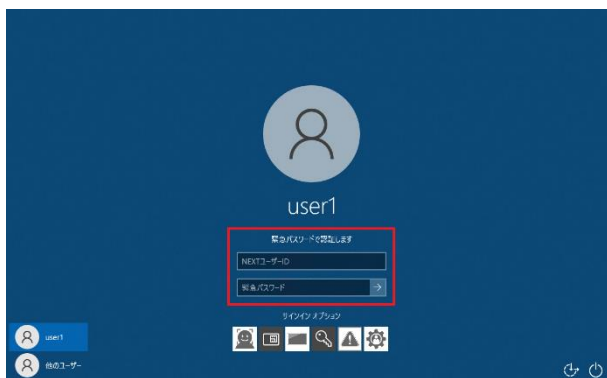


Info 表示される「サインイン オプション」は管理者の設定によります。「NEXT 緊急パスワード認証」を利用してサインイン、画面ロックの解除を行いたい場合は、認証方式として「NEXT 緊急パスワード認証」を有効化する必要があります。

3. [緊急パスワード認証]のアイコンをクリックします

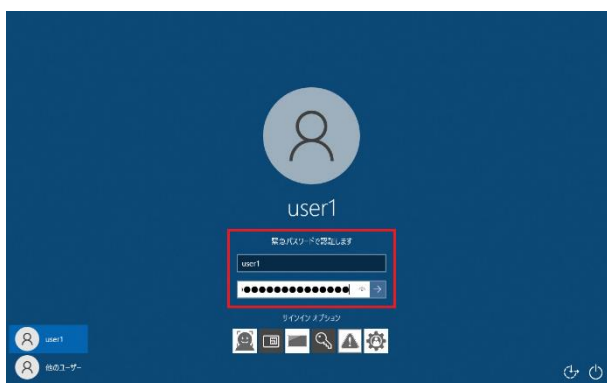


4. NEXT 緊急パスワード認証用のサインイン画面に切り替わります



5. NEXT 緊急パスワードを入力します

「NEXT ユーザーID」、NEXT 管理者から通知された「NEXT 緊急パスワード」を入力し、[Enter]キーを押すか、[→]アイコンをクリックします。



6. Windows へのサインインが完了します

Windows のデスクトップが表示されます。



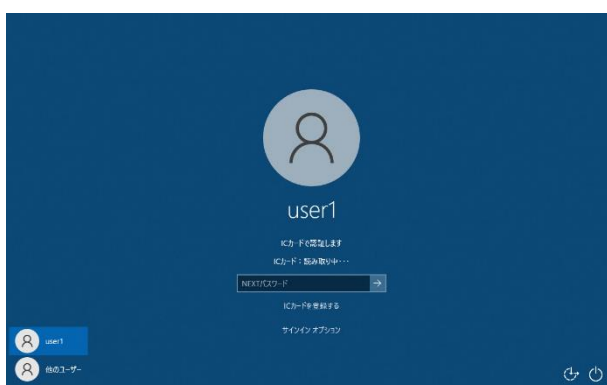
Info Windows 認証では、サインイン先を変更することができます。
設定方法は、「3.6. ユーザーを切り替えてサインイン」を参照してください。

3.9. NEXT 管理者パスワード認証でのサインイン、ロック解除

PCのメンテナンスや設定のために、利用者ではなく、管理者がコンピューターにサインインしたい場合、「NEXT 管理者パスワード」を利用して、ロック画面を解除し、Windows サインインすることができます。「NEXT 管理者パスワード」を知っている管理者であれば、管理者のICカードや顔情報を利用しなくても以下の手順によってロック画面を解除することができます。

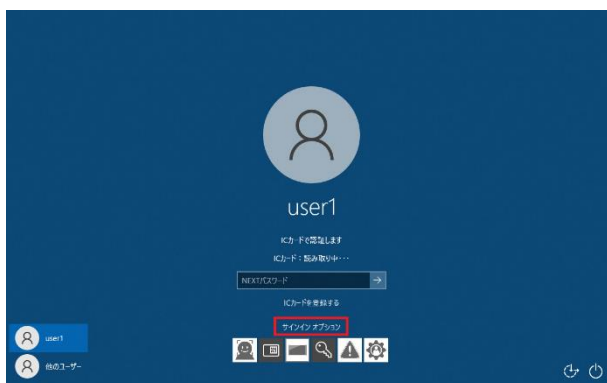
1. Windows を起動します

Windows 起動時に以下の初期画面が表示されます。ここでは IC カード認証が前回の認証で選ばれている場合の表示です。



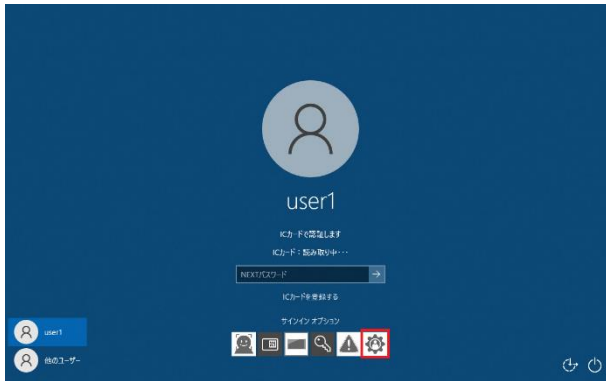
2. 「サインイン オプション」をクリックします

サインインオプションのアイコンが表示されます。

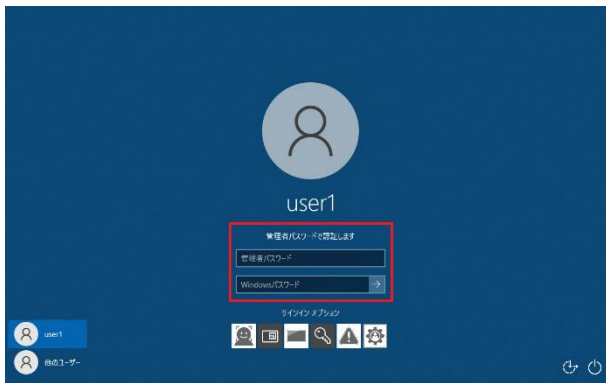


Info 表示される「サインイン オプション」は管理者の設定によります。「NEXT 管理者パスワード認証」を利用してサインイン、画面ロックの解除を行いたい場合は、認証方式として「NEXT 管理者パスワード認証」を有効化する必要があります。

3. [管理者パスワード認証]のアイコンをクリックします

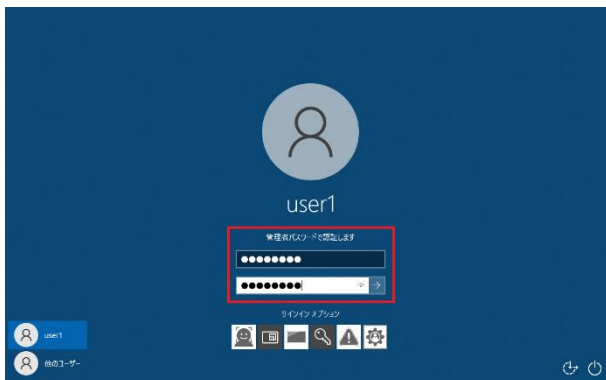


4. NEXT 管理者パスワード認証用のサインイン画面に切り替わります



5. NEXT 管理者パスワード、Windows パスワードを入力します

「NEXT 管理者パスワード」、Windows サインインの「Windows パスワード」を入力し、[Enter] キーを押すか、[→]アイコンをクリックします。



6. Windows へのサインインが完了します
Windows のデスクトップが表示されます。

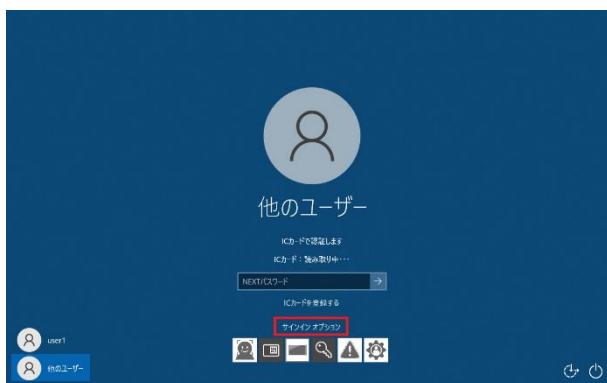


3.10. Windows 標準認証でのサインイン、ロック解除

Windows 標準認証は、マイクロソフト社が用意しているパスワードによる Windows のサインイン認証であり、NEXT 認証を使用しないで Windows へサインインする機能です。

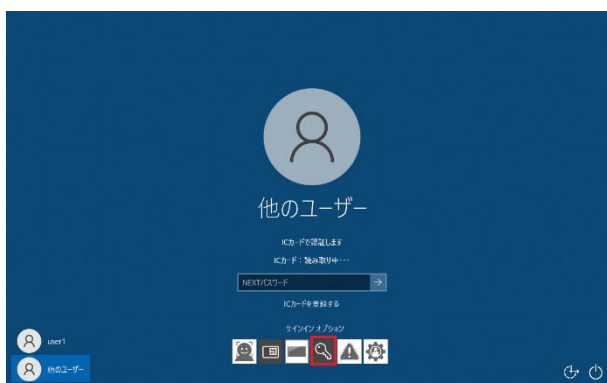
Windows 標準認証でサインインする流れを例示します。

1. 「サインイン オプション」をクリックします
サインインオプションのアイコンが表示されます。



Info 表示される「サインイン オプション」は管理者の設定によります。「Windows 標準認証」を利用してサインイン、画面ロックの解除を行いたい場合は、認証方式として「Windows 標準認証」を有効化する必要があります。

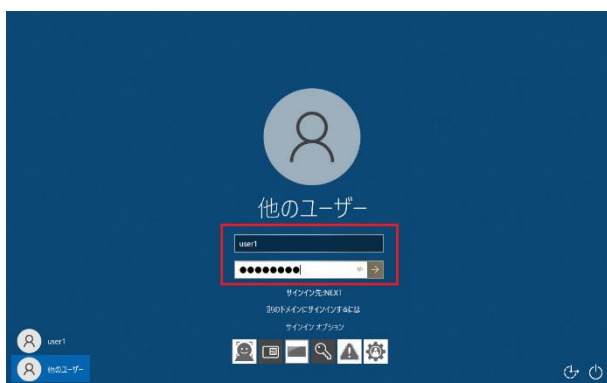
2. [Windows 標準認証]のアイコンをクリックします



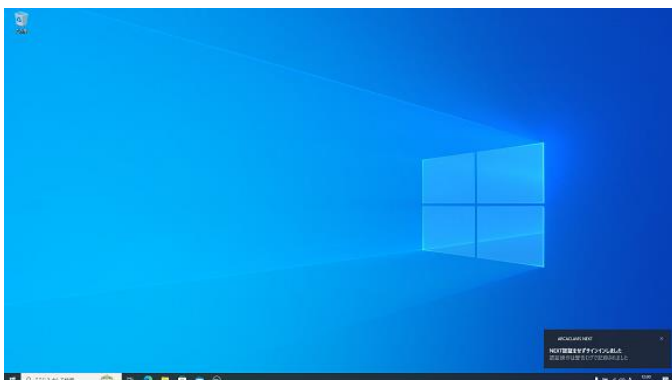
3. Windows 標準認証用のサインイン画面に切り替わります



4. サインインするローカル、またはドメインアカウントの「ユーザー名」「パスワード」を入力し、[Enter] キーを押すか、[→]アイコンをクリックします。



5. Windows へのサインインが完了します
Windows のデスクトップが表示されます。



Info Windows 認証では、サインイン先を変更することができます。
設定方法は、「3.6. ユーザーを切り替えてサインイン」を参照してください。

Info Windows 認証でサインインした場合は、以下のトースト通知が表示されます。



3.11. NEXT セーフモードでのサインイン、ロック解除

3.11.1 概要

NEXT クライアントの「NEXT セーフモード」とは、NEXT クライアントによる NEXT 認証が不全の状態を検知したときに自動的に移行されるモードのことです。NEXT クライアント内のシステムで異常な状態を検知し、NEXT セーフモードに自動的に移行します。NEXT セーフモードに移行した場合は、Windows アカウント情報を入力して Windows へサインイン後、コンピューターを再起動し、再度 NEXT 認証を行ってください。

NEXT セーフモードに移行する条件は、NEXT クライアントで認証処理の継続ができない異常が発生した場合です。

NEXT セーフモードに移行した後、Windows アカウント情報を入力して Windows へサインインした場合は、以下のイベントログが出力されます。

レベル	ソース	メッセージ
情報	ARCACLAVIS NEXT	セーフモードに移行したため、Windows アカウント情報のみでサインインを行いました。

Info セーフモードに移行した後、サインインオプションで Windows 標準認証に切り替えて Windows へサインインした場合は、イベントログは出力されません。



Info NEXT クライアントによる NEXT 認証時にオフラインと判定された後で、NEXT クライアント内のシステムで異常な状態を検知した場合、最大で 60 秒経過後に NEXT セーフモードになります。Windows 標準認証でサインイン後、コンピューターを再起動し、NEXT 認証を行ってください。

3.11.2. NEXT セーフモードでサインイン、ロック解除

ここでは、ICカードを使って Windows へ自動サインインする「3.2.1. ICカードを利用したサインイン認証」のパターン 1 の設定で、NEXT 認証が不全の状態が検知され、NEXT セーフモードに変更された状態から、Windows 標準認証でサインインし、再起動後、復帰するまでの流れを説明します。

1. サインイン、またはロック解除時に NEXT 認証します
通常通り、ICカード認証を行います。



2. NEXT 認証の不全が検知され、NEXT セーフモードに移行されました

「NEXT 認証中にエラーが発生しました。Windows アカウント情報を入力してサインインを行ってください。PC を再起動してもエラーが発生する場合は、管理者へご連絡ください。」と下図のように表示されますので、「OK」ボタンを押下します。



3. Windows パスワードの入力を行います

Windows パスワードを入力し、[Enter]キーを押すか、[→]アイコンをクリックします



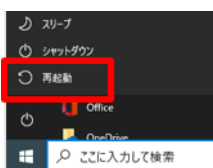
4. Windows へのサインインが完了します

Windows のデスクトップが表示されます。



5. 再起動します

ファイルの保存などの準備が終わったら、[スタートメニュー]-[電源]-[再起動]を選択し、再起動します。



Info セーフモード時に Windows 標準認証でサインインした後は、Windows の再起動を行い、再度 NEXT 認証をご利用ください。

3.12. エラーメッセージ

3.12.1 IC カード認証時のエラーメッセージ

NEXT クライアントへ IC カード認証でサインインする際に表示される代表的なエラーメッセージは下記のとおりです。

出力メッセージ	対応方法
IC カードがセットされていません	IC カードが読み取れませんでした。 IC カードリーダーの接続、および IC カードリーダーに IC カードが正しくセットされているか確認してください。
NEXT パスワードが入力されていません	NEXT パスワードが入力されていません。 IC カード認証を行う NEXT ユーザーID の NEXT パスワードを入力してください。
認証エラー	入力された NEXT パスワードが正しくありません。 IC カード認証を行う NEXT ユーザーID の NEXT パスワードを正しく入力してください。
NEXT ユーザーが見つかりません	未登録の IC カードがセットされています。 IC カード認証を行う場合は、IC カードが登録されている必要があります。 詳細は、「4.1. IC カード登録」を参照してください。
初回 NEXT パスワード変更が必要です	IC カード認証を行う前に新しい NEXT パスワードに変更する必要があります。 詳細は、「3.3.1. NEXT パスワードの変更」を参照してください。
NEXT パスワードの有効期限切れです	IC カード認証を行う前に新しい NEXT パスワードに変更する必要があります。 詳細は、「3.3.1. NEXT パスワードの変更」を参照してください。
ユーザーの有効期限切れです	NEXT ユーザーが利用できる有効期間が切れています。 再びサインインできるようにするためには、管理者が NEXT ユーザーの有効期間(終了)の日付を変更する必要があります。 「有効期間(終了)」の設定については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。

出力メッセージ	対応方法
ユーザーがロックされています	<p>NEXT ユーザーが無効化、またはロックアウトされています。</p> <p>再びサインインできるようにするためには、管理者が NEXT ユーザーを有効化する必要があります。</p> <p>NEXT ユーザーの有効化については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。</p> <p>ユーザーが NEXT 認証に失敗した回数が設定されたしきい値に達すると、NEXT ユーザーがロックアウトされます。</p> <p>再びサインインできるようにするためには、管理者がロックアウトを解除する必要があります。</p> <p>NEXT ユーザーのロックアウトの動作仕様およびロックアウトの解除方法については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。</p>
オフライン有効期限が切れています	<p>オフライン状態でのキャッシュ有効期間が切れています。</p> <p>管理者が設定している「オフライン有効日数」以上の期間、オフライン状態が続くとサインインできません。</p> <p>再びサインインできるようにするためには、NEXT サーバーと NEXT クライアントを通信できる状態にして、サインインする必要があります。</p> <p>「オフライン有効日数」については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。</p>
NEXT 認証中にエラーが発生しました。Windows アカウント情報を入力してサインインを行ってください。PC を再起動してもエラーが発生する場合は、管理者へご連絡ください。	<p>IC カード認証を行った際にセーフモードへ移行しました。</p> <p>「OK」ボタンを押下して、Windows アカウント情報を入力して Windows へサインインしてください。</p> <p>詳細は、「3.11.2. NEXT セーフモードでサインイン、ロック解除」を参照してください。</p> <p>頻繁にセーフモードへ移行する場合は、「ARCACLAVIS NEXT トラブルシューティングガイド」を参照してください。</p>

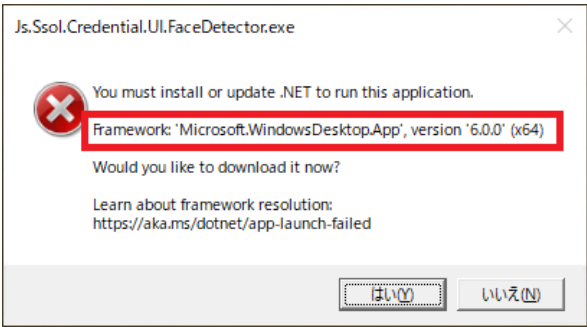
3.12.2 顔認証時のエラーメッセージ

NEXT クライアントへ顔認証でサインインする際に表示される代表的なエラーメッセージは下記のとおりです。

出力メッセージ	対応方法
初期化処理でエラーが発生しました	<p>照合画面の初期化処理に失敗しました。</p> <p>サインインオプションから顔認証を選択し、再度顔認証を行ってください。</p>
顔照合エラー	<p>顔情報が未登録の状態、または顔照合に失敗しました。</p> <p>顔認証を行う場合は、顔情報が登録されている必要があります。</p> <p>詳細は、「4.2. 顔情報登録」を参照してください。</p> <p>頻繁に顔照合に失敗する場合は、「ARCACLAVIS NEXT トラブルシューティングガイド」を参照してください。</p>
顔の検出ができませんでした	<p>カメラが接続されていない、カメラが故障している、またはマイクロソフト社の Teams や Skype など、他のアプリケーションでカメラが使用中のため、カメラが使用不能な状態となっています。</p> <p>繰り返し表示される場合は、「ARCACLAVIS NEXT トラブルシューティングガイド」の「3.3.4. 「顔の検出ができませんでした」と繰り返し表示される」を参照してください。</p> <p>※NEXT サーバーのクライアント設定で「顔照合時に照合画面を表示する」が有効時に表示されます。</p>
カメラが接続されていません	<p>カメラが接続されていない、カメラが故障している、またはマイクロソフト社の Teams や Skype など、他のアプリケーションでカメラが使用中のため、カメラが使用不能な状態となっています。</p> <p>※NEXT サーバーのクライアント設定で「顔照合時に照合画面を表示する」が無効時に表示されます。</p>
NEXT ユーザーIDが入力されていません	<p>NEXT ユーザーIDが入力されていません。</p> <p>顔認証を行う NEXT ユーザーIDを入力してください。</p>

出力メッセージ	対応方法
NEXT パスワードが入力されていません	NEXT パスワードが入力されていません。 顔認証を行う NEXT ユーザーID の NEXT パスワードを入力してください。
認証エラー	入力された NEXT ユーザーID、または NEXT パスワードが正しくありません。 顔認証を行う NEXT ユーザーID、および NEXT パスワードを正しく入力してください。
NEXT ユーザーが見つかりません	入力された NEXT ユーザーID は存在していません。 顔認証を行う NEXT ユーザーID を正しく入力してください。
初回 NEXT パスワード変更が必要です	顔認証を行う前に新しい NEXT パスワードに変更する必要があります。 詳細は、「3.3.1. NEXT パスワードの変更」を参照してください。
NEXT パスワードの有効期限切れです	顔認証を行う前に新しい NEXT パスワードに変更する必要があります。 詳細は、「3.3.1. NEXT パスワードの変更」を参照してください。
ユーザーの有効期限切れです	NEXT ユーザーが利用できる有効期間が切れています。 再びサインインできるようにするためには、管理者が NEXT ユーザーの有効期間(終了)の日付を変更する必要があります。 「有効期間(終了)」の設定については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。
ユーザーがロックされています	NEXT ユーザーが無効化、またはロックアウトされています。 再びサインインできるようにするためには、管理者が NEXT ユーザーを有効化する必要があります。 NEXT ユーザーの有効化については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。 ユーザーが NEXT 認証に失敗した回数が設定されたしきい値に達すると、NEXT ユーザーがロックアウトされます。 再びサインインできるようにするためには、管理者がロックアウトを解除する必要があります。 NEXT ユーザーのロックアウトの動作仕様およびロックアウトの解除方法については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。

出力メッセージ	対応方法
オフライン有効期限が切れています	<p>オフライン状態でのキャッシュ有効期間が切れています。管理者が設定している「オフライン有効日数」以上の期間、オフライン状態が続くとサインインできません。</p> <p>再びサインインできるようにするためには、NEXT サーバーと NEXT クライアントを通信できる状態にして、サインインする必要があります。</p> <p>「オフライン有効日数」については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。</p>
プロバイダーが見つかりません	<p>ライセンスの変更、ライセンスの有効期限切れなどにより顔認証の機能が使用不可となっています。</p> <p>ライセンスについては、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。</p>
アプリケーションエラーが発生しました	<p>顔認証用のランタイム「RS OLFACE」がインストールされていない、または利用者の PC に何らかの問題が発生している可能性があります。</p> <p>「RS OLFACE」がインストールされているかご確認ください。</p> <p>「RS OLFACE」については、「RS OLFACE インストールマニュアル」を参照してください。</p> <p>「RS OLFACE」がインストールされている場合は、一度コンピュータを再起動して、再度顔認証を行ってください。</p>
顔認証画面を強制終了しました	<p>顔認証画面の応答がないため、顔認証画面を強制終了しました。</p> <p>サインインオプションから顔認証を選択し、再度顔認証を行ってください。</p> <p>RS OLFACE がアンインストールされており、かつカメラが接続されている場合に表示されることがあります。</p> <p>ARCACLAVIS NEXT クライアントをアンインストールし、再度 ARCACLAVIS NEXT クライアントと RS OLFACE をインストールした後に、再度、顔認証を行ってください。</p>

出力メッセージ	対応方法
<p>NEXT 認証中にエラーが発生しました。 Windows アカウント情報を入力してサインインを行ってください。PC を再起動してもエラーが発生する場合は、管理者へご連絡ください。</p>	<p>顔認証を行った際にセーフモードへ移行しました。 「OK」ボタンを押下して、Windows アカウント情報を入力して Windows へサインインしてください。 詳細は、「3.11.2. NEXT セーフモードでサインイン、ロック解除」を参照してください。</p> <p>頻繁にセーフモードへ移行する場合は、「ARCACLAVIS NEXT トラブルシューティングガイド」を参照してください。</p> <p>RS OLFACE がアンインストールされており、かつカメラが接続されていない場合に表示されることがあります。 ARCACLAVIS NEXT クライアントをアンインストールし、再度 ARCACLAVIS NEXT クライアントと RS OLFACE をインストールした後に、再度、顔認証を行ってください。</p>
<p>顔認証画面を強制終了しました</p> <p>You must install or update .NET to run this application. Framework: {ミドルウェア名} Would you like to download it now? Learn about framework resolution: https://aka.ms/dotnet/app-launch-failed</p>	<p>NEXT クライアントに必要なミドルウェアがインストールされていない、またはミドルウェアの更新が必要です。 インストールされていないミドルウェアをインストールしてください。</p> <p>NEXT クライアントに必要なミドルウェア、各ミドルウェアのバージョンについては、「ARCACLAVIS NEXT 動作環境一覧」を参照してください。</p> <p>エラーが発生した際に表示される以下ダイアログから、ミドルウェアを特定することが可能です。 (下記例では、「Microsoft Windows Desktop Runtime」が未インストール、または更新が必要となります)</p> 

3.12.3 ワンタイムパスワード認証時のエラーメッセージ

NEXT クライアントへワンタイムパスワード認証でサインインする際に表示される代表的なエラーメッセージは下記のとおりです。

出力メッセージ	対応方法
NEXT ユーザーIDが入力されていません	NEXT ユーザーIDが入力されていません。 ワンタイムパスワード認証を行う NEXT ユーザーID を入力してください。
NEXT パスワードが入力されていません	NEXT パスワードが入力されていません。 ワンタイムパスワード認証を行う NEXT ユーザーID の NEXT パスワードを入力してください。
認証エラー	入力された NEXT ユーザーID が正しくありません。 ワンタイムパスワード認証を行う NEXT ユーザーID を正しく入力してください。
NEXT パスワード認証エラー	入力された NEXT ユーザーID の NEXT パスワードが正しくありません。 ワンタイムパスワード認証を行う NEXT ユーザーID の NEXT パスワードを正しく入力してください。
ワンタイムパスワード認証エラー	入力された NEXT ユーザーID のワンタイムパスワードが正しくありません。 ワンタイムパスワード認証を行う NEXT ユーザーID のワンタイムパスワードを正しく入力してください。
NEXT ユーザーが見つかりません	入力された NEXT ユーザーID は存在していません。 ワンタイムパスワード認証を行う NEXT ユーザーID を正しく入力してください。
初回 NEXT パスワード変更が必要です	ワンタイムパスワード認証を行う前に新しい NEXT パスワードに変更する必要があります。 詳細は、「3.3.1. NEXT パスワードの変更」を参照してください。
NEXT パスワードの有効期限切れです	ワンタイムパスワード認証を行う前に新しい NEXT パスワードに変更する必要があります。 詳細は、「3.3.1. NEXT パスワードの変更」を参照してください。
ユーザーの有効期限切れです	NEXT ユーザーが利用できる有効期間が切れています。 再びサインインできるようにするためには、管理者が NEXT ユーザーの有効期間(終了)の日付を変更する必要があります。 「有効期間(終了)」の設定については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。

出力メッセージ	対応方法
ユーザーがロックされています	<p>NEXT ユーザーが無効化、またはロックアウトされています。</p> <p>再びサインインできるようにするためには、管理者が NEXT ユーザーを有効化する必要があります。</p> <p>NEXT ユーザーの有効化については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。</p> <p>ユーザーが NEXT 認証に失敗した回数が設定されたしきい値に達すると、NEXT ユーザーがロックアウトされます。再びサインインできるようにするためには、管理者がロックアウトを解除する必要があります。</p> <p>NEXT ユーザーのロックアウトの動作仕様およびロックアウトの解除方法については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。</p>
オフライン有効期限が切れています	<p>オフライン状態でのキャッシュ有効期間が切れています。管理者が設定している「オフライン有効日数」以上の期間、オフライン状態が続くとサインインできません。</p> <p>再びサインインできるようにするためには、NEXT サーバーと NEXT クライアントを通信できる状態にして、サインインする必要があります。</p> <p>「オフライン有効日数」については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。</p>
NEXT 認証中にエラーが発生しました。Windows アカウント情報を入力してサインインを行ってください。PC を再起動してもエラーが発生する場合は、管理者へご連絡ください。	<p>ワンタイムパスワード認証を行った際にセーフモードへ移行しました。</p> <p>「OK」ボタンを押下して、Windows アカウント情報を入力して Windows へサインインしてください。</p> <p>詳細は、「3.11.2. NEXT セーフモードでサインイン、ロック解除」を参照してください。</p> <p>頻繁にセーフモードへ移行する場合は、「ARCACLAVIS NEXT トラブルシューティングガイド」を参照してください。</p>

4. 認証情報の登録

NEXT 認証に必要な認証情報は、NEXT マネージャーから登録を行うことができますが、NEXT マネージャーのクライアント設定により NEXT クライアントから登録を行うこともできます。これにより、大規模環境での導入や既にユーザーに配布済みの IC カードを利用する環境でも、簡単に ARCACLAVIS NEXT システムを導入できます。

NEXT クライアントで認証情報を登録するには、以下の条件を満たす必要があります。

- ・クライアント設定で「IC カード認証」、「顔認証」、「ワンタイムパスワード認証」がオンになっている
 - ・クライアント設定で「IC カード認証」の「未登録時に IC カードの登録を許可する」、「顔認証」の「登録を許可する」または「再登録を許可する」、「ワンタイムパスワード認証」がオンになっている
 - ・認証情報を登録する NEXT ユーザーが有効期間含め、有効状態である
 - ・認証情報を登録する NEXT ユーザーは、NEXT サーバーに対しての認証に成功する
 - ・認証情報を登録する NEXT クライアントと NEXT サーバーがオンラインで通信できる状態である
- ※オフライン状態でも「IC カードを登録する」、「顔情報を登録する」、「はじめてワンタイムパスワードを利用する方はこちら」のリンクから登録作業は可能ですが、登録時にエラーとなります。

なお、既に登録済みの IC カードの場合、同じ IC カードを登録することはできません。別の IC カードを用意するか、登録済みの IC カードを削除する必要があります。

また、既にワンタイムパスワードシークレットが発行されている場合は、ワンタイムパスワードシークレットを発行することはできません。NEXT マネージャーの管理者ポータル、またはユーザーポータルでワンタイムパスワードシークレットのリセットを行う必要があります。

ご利用のスマートフォンを変更する場合などワンタイムパスワードシークレットの再発行が必要な場合は、ワンタイムパスワードシークレットのリセット、およびワンタイムパスワードシークレットの発行を行い、スマートフォンの Authenticator アプリへ再登録する必要があります。

ワンタイムパスワードシークレットの発行については、「4.3. ワンタイムパスワード認証の情報登録」を参照してください。

スマートフォンの Authenticator アプリへの登録については、「8.6. スマートフォンの Authenticator アプリへの登録」を参照してください。

ワンタイムパスワードシークレットのリセットについては、「8.7. ワンタイムパスワードシークレットのリセット」を参照してください。

4.1. IC カード登録

ここでは、IC カードを使って Windows へ自動サインインする場合の「3.2.1. IC カードを利用したサインイン認証」のパターン 1 の設定で、ユーザーを選択し、IC カードを登録して、そのままサインインする流れを例示します。

1. Windows を起動します

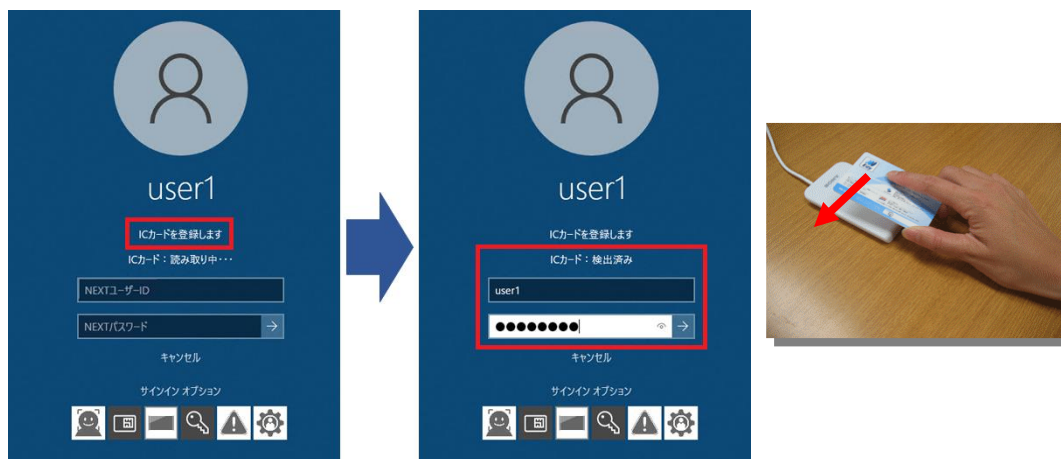
Windows 起動時に以下の初期画面が表示されます。

[IC カードを登録する]をクリックします。



Info 「IC カードを登録する」が表示されない場合は、NEXT マネージャーのクライアント設定でユーザーによる登録が許可されていません。クライアント設定をご確認ください。

2. 登録する IC カードのセット、IC カードを登録する NEXT ユーザーID、NEXT パスワードを入力します
登録する IC カードを、IC カードリーダー/ライターに IC カードをセットします。
IC カードが検出されると、「IC カード：検出済み」と表示されます。
登録する「NEXT ユーザーID」、「NEXT パスワード」を入力し、[Enter]キーを押すか、[→]アイコンをクリックします。



3. Windows へのサインインが完了します
NEXT 認証が成功し、IC カード登録が完了すると、そのまま Windows サインインが行われ、Windows のデスクトップが表示されます。
Windows アカウントは、ユーザー情報に設定されている Windows アカウント設定を利用して自動サインインします。

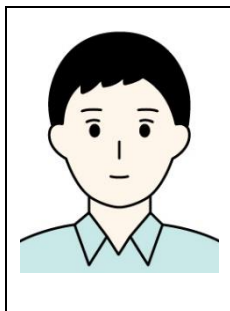


Info NEXT マネージャーのクライアント設定で「Windows に自動サインインする」がオフの場合は、Windows 認証後に、Windows のデスクトップが表示されます。

4.2. 顔情報登録

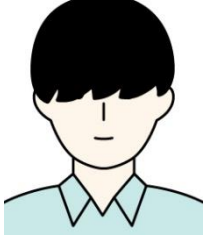







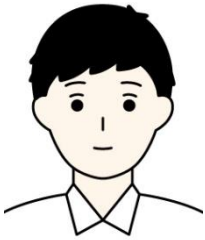
顔情報登録時に撮影する顔画像は、以下を参考にしてください。

➤ 良い顔画像の例



➤ 顔情報登録時に向かない顔画像の例

顔が揺れている	影がかかっている	逆光	白飛び	顔を傾けている (仰ぎ)
顔を傾けている (俯き)	顔を傾けている (横向き)	サングラス着用	マスク着用 ※	帽子着用

				
マフラー着用	髪が目にかかっている	目、耳、口などの顔の一部を隠している	まばたき・目を閉じている	大きく口を開いている
				
メガネの角度で目の位置が不明瞭 1	メガネの角度で目の位置が不明瞭 2	顔の一部しか写っていない	複数人の写り込み	ぼやけている
				
カメラの解像度が不十分	写真でなりすます	撮影から数年経過している		

※顔情報登録時はマスク着用しないでください。顔認証時はマスク着用での顔認証は可能です。

顔情報登録時は、クライアント設定で「照合画面を表示する」の設定がオン/オフに関わらず、必ず照合画面が表示されます。

照合画面のデザインは、状態によって変わります。

以下に照合画面のデザイン、および各項目について説明します。



No	項目	補足
①	カメラ切り替えボタン	2つ以上カメラが接続されている場合、別のカメラに切り替わります。
②	カメラ回転ボタン	キャプチャ画像が 90 度ずつ回転します。
③	閉じるボタン	照合画面を閉じます。
④	目のガイド	顔登録が成功しやすくなる目安として表示している目のガイドです。 2つの丸の中に両目が映るように調整してください。
⑤	ガイド	顔登録が成功しやすくなる目安として表示しているガイドです。 ガイドの中に顔全体が映るように調整してください。
⑥	キャプチャ画像	カメラからの画像が表示されます。
⑦	撮影ボタン	カメラからの画像を使用して顔検出が開始されます。
⑧	カメラ番号	「カメラ切り替え」ボタンを押下時に使用されているカメラ番号が表示されます。 ※カメラ番号は 1 秒でフェードアウトします。
⑨	撮影キャンセルボタン	顔検出を中断します。
⑩	メッセージ	顔登録時のメッセージが表示されます。
⑪	登録ボタン	撮影した顔画像を使用して顔登録を行います。
⑫	キャンセルボタン	撮影した顔画像を破棄して顔登録を中断します。
⑬	エラーメッセージ	顔登録時のエラーメッセージが表示されます。
⑭	登録マーカー	顔情報登録中に表示されます。

ここでは、顔認証を使って Windows へ自動サインインする場合の「3.2.2. 顔情報を利用したサインイン認証」のパターン 1 の設定で、ユーザーを選択し、顔情報を登録して、そのままサインインする流れを例示します。

1. Windows を起動します

Windows 起動時に以下の初期画面が表示されます。

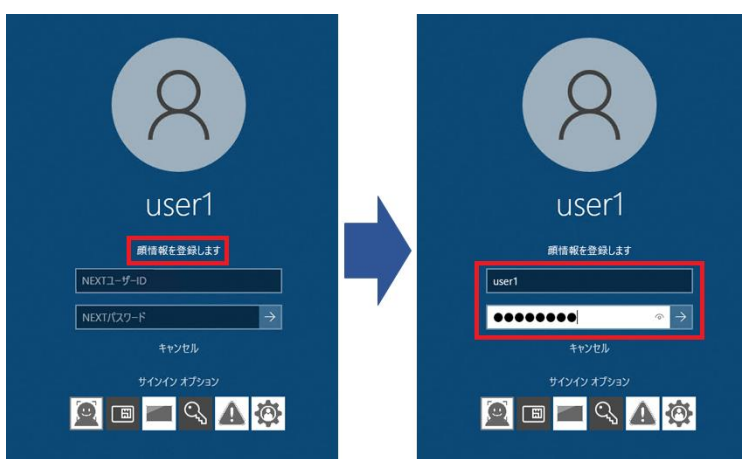
[顔情報を登録する]をクリックします。



Info 「顔情報を登録する」が表示されない場合は、NEXT マネージャーのクライアント設定でユーザーによる登録が許可されていません。クライアント設定をご確認ください。

2. 顔情報を登録する NEXT ユーザーID、NEXT パスワードを入力します

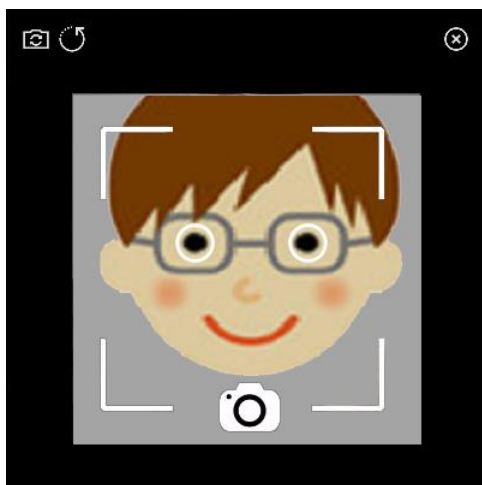
顔情報を登録する「NEXT ユーザーID」、「NEXT パスワード」を入力し、[Enter]キーを押すか、[→]アイコンをクリックします。



3. <撮影>ボタンをクリックします

照合画面が表示された後にカメラが起動しますので、<撮影>ボタンをクリックします。

顔情報登録時は、「マスクを使用する」の設定に関わらず、マスク非着用の状態で行ってください。



Info カメラが複数ある場合は、<カメラ切り替え>ボタンを押下して顔情報登録で使いたいカメラに切り替えてください。インカメラ、アウトカメラがある場合も、顔情報登録で使いたいカメラに切り替えてください。
顔認証、または顔情報登録で最後に使用したカメラを記憶して、次回以降は記憶したカメラを使用します。

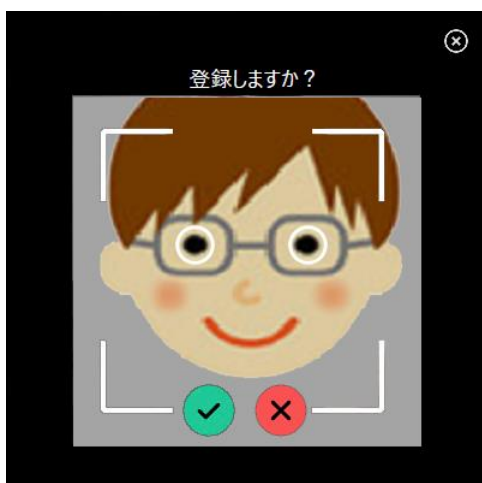
4. カメラに顔を向けて顔検出を行います

顔検出を行いますので、カメラに顔を向けてください。



Info <撮影キャンセル>ボタンをクリックすると、顔検出を中断して手順3へ戻ります。

5. <登録>ボタンをクリックして顔情報を登録します
顔検出が行われたため、<登録>ボタンをクリックします。



Info <キャンセル>ボタンをクリックすると、検出した顔情報を破棄して手順3へ戻ります。

Info 顔情報の登録に失敗した場合、「顔認証データの生成に失敗しました」とエラーが表示されます。その後、照合画面が終了して「顔の検出ができませんでした」とエラーが表示されます。
手順2から再度顔登録を行ってください。

6. Windowsへのサインインが完了します

NEXT 認証が成功し、顔情報登録が完了すると、そのままWindowsサインインが行われ、Windowsのデスクトップが表示されます。

Windowsアカウントは、ユーザー情報に設定されているWindowsアカウント設定を利用して自動サインインします。



Info NEXT マネージャーのクライアント設定で「Windowsに自動サインインする」がオフの場合は、Windows認証後に、Windowsのデスクトップが表示されます。

4.3. ワンタイムパスワード認証の情報登録

ここでは、ワンタイムパスワードを使って Windows へ自動サインインする場合の「3.2.3. スマートフォンの Authenticator アプリを利用したサインイン認証」のパターン 1 の設定で、ユーザーを選択し、ワンタイムパスワードシークレットを発行して、そのままサインインする流れを例示します。

1. Windows を起動します

Windows 起動時に以下の初期画面が表示されます。

[はじめてワンタイムパスワードを利用する方はこちら]をクリックします。



The image shows a Windows login screen for a user named 'user1'. At the top, there is a user icon and the name 'user1'. Below that, the text reads 'NEXTアカウントとワンタイムパスワードを入力してください'. There are three input fields: 'NEXTユーザーID', 'NEXTパスワード', and 'ワンタイムパスワード' with a right-pointing arrow icon. Below these fields is a red-bordered box containing the text 'はじめてワンタイムパスワードを利用する方はこちら'. At the bottom, there is a 'サインイン オプション' button.

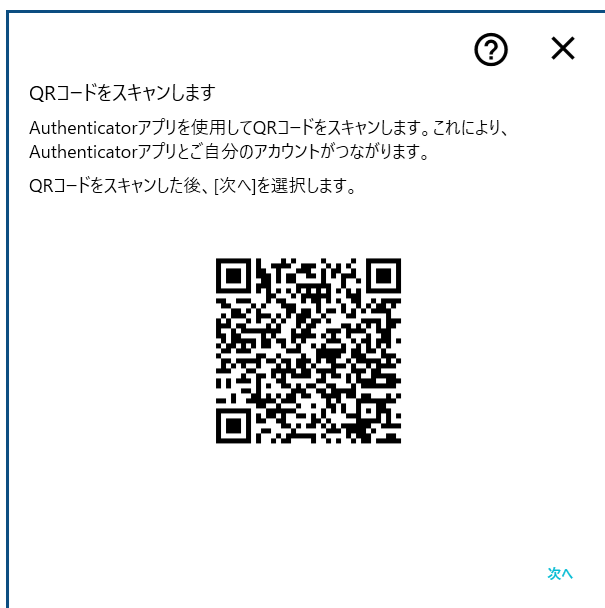
2. ワンタイムパスワードシークレットを発行する NEXT ユーザーID、NEXT パスワードを入力します。ワンタイムパスワードシークレットを発行する「NEXT ユーザーID」、「NEXT パスワード」を入力し、[Enter]キーを押すか、[→]アイコンをクリックします。



The image shows the same Windows login screen for 'user1'. The text 'NEXTアカウントを入力してください' is now visible. The 'NEXTユーザーID' and 'NEXTパスワード' input fields are highlighted with a red box. The 'ワンタイムパスワード' field and the 'はじめてワンタイムパスワードを利用する方はこちら' link are no longer visible. The 'サインイン オプション' button is at the bottom.

3. ワンタイムパスワードの認証情報を登録するための QR コードを表示します

ワンタイムパスワードシークレットが発行され、ワンタイムパスワード認証情報を登録するための QR コードが表示されます。

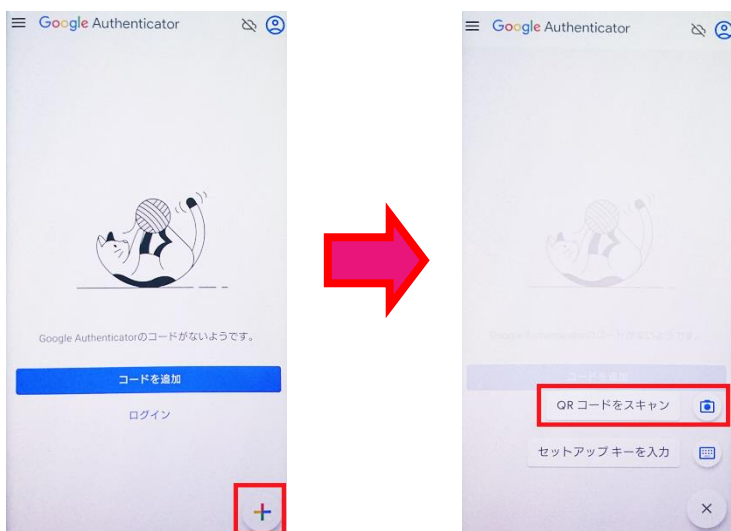


4. スマートフォンの Authenticator アプリを起動します

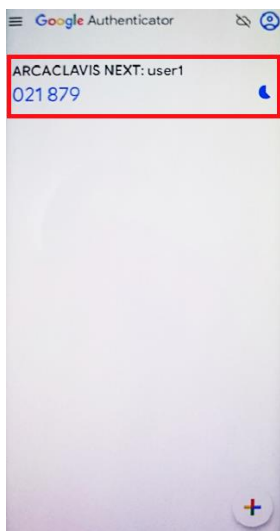
スマートフォンの Authenticator アプリを起動してください。

5. スマートフォンの Authenticator アプリで QR コードを読み取ります

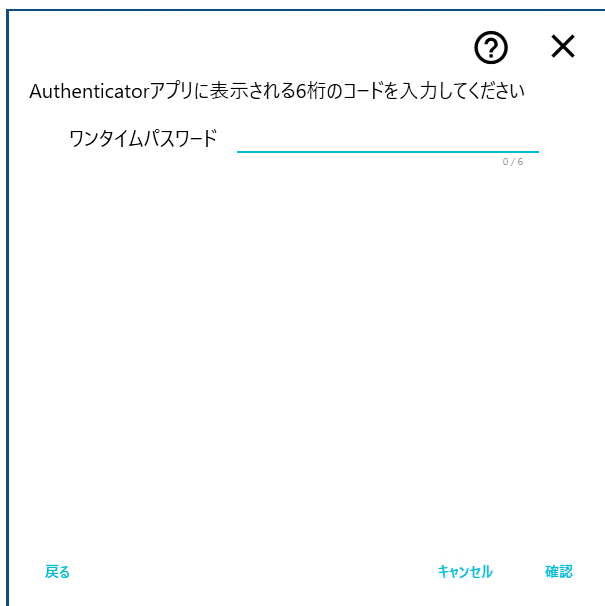
スマートフォンの Authenticator アプリの画面右下に表示されている<+>ボタンをタップして、[QR コードをスキャン]をクリックし、ワンタイムパスワード認証情報を登録するための QR コードを読み取ってください。



6. スマートフォンの Authenticator アプリにワンタイムパスワードの認証情報が登録されます
スマートフォンの Authenticator アプリに NEXT ユーザーのワンタイムパスワード認証の情報が登録されます。



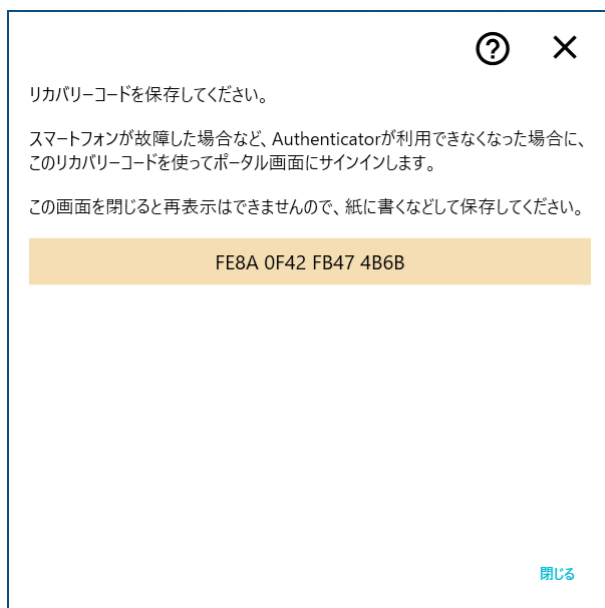
7. NEXT クライアントのワンタイムパスワード認証情報を登録する QR コードが表示されている画面の<次へ>ボタンをクリックしてください。
8. スマートフォンの Authenticator アプリに表示されているワンタイムパスワードを入力し、<確認>ボタンをクリックしてください。

A screenshot of the input screen within the Authenticator app. At the top right, there are icons for help (a question mark in a circle) and close (an 'X'). The main text reads 'Authenticatorアプリに表示される6桁のコードを入力してください'. Below this, there is a label 'ワンタイムパスワード' followed by a text input field. The input field contains a blue horizontal line and the text '0 / 6' at the bottom right. At the bottom of the screen, there are three buttons: '戻る' (Back) on the left, 'キャンセル' (Cancel) in the center, and '確認' (Confirm) on the right.

9. リカバリーコードが表示されます。

本画面を閉じるとリカバリーコードの再表示はできなくなります。

リカバリーコードを保存し、<閉じる>ボタンをクリックしてください。

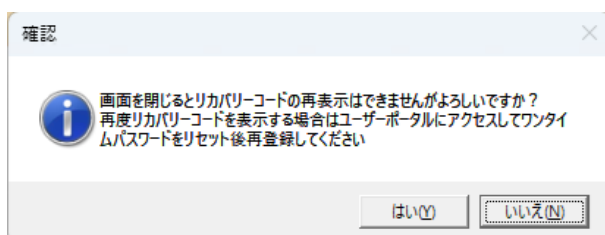


Info リカバリーコードは、スマートフォンの紛失や破損によってワンタイムパスワードの生成ができない場合、ワンタイムパスワードを無効にして再度サインインが可能な状態に復旧させるために使用します。
リカバリーコードを使用する手順については、「ARCACLAVIS NEXT トラブルシューティングガイド」を参照してください。

10. 確認画面が表示されます。

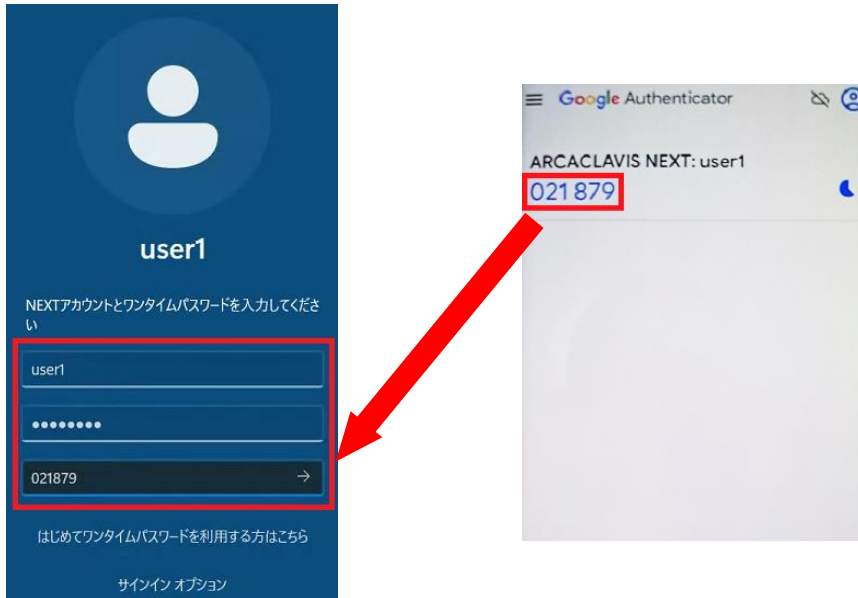
リカバリーコードの保存が終わっていただければ、<はい>ボタンをクリックしてください。

再度リカバリーコードを表示する場合は、<いいえ>ボタンをクリックしてください。



1 1. NEXT アカウントとワンタイムパスワードを入力します

ワンタイムパスワード認証でサインインする「NEXT ユーザーID」、「NEXT パスワード」、スマートフォンの Authenticator アプリに表示されている「ワンタイムパスワード」を入力し、[Enter]キーを押すか、[→]アイコンをクリックします。



1 2. Windows へのサインインが完了します

NEXT 認証が成功し、ワンタイムパスワード認証の情報登録が完了すると、そのまま Windows サインインが行われ、Windows のデスクトップが表示されます。

Windows アカウントは、ユーザー情報に設定されている Windows アカウント設定を利用して自動サインインします。



Info NEXT マネージャーのクライアント設定で「Windows に自動サインインする」がオフの場合は、Windows 認証後に、Windows のデスクトップが表示されます。

4.4. エラーメッセージ

4.4.1 ICカード登録時のエラーメッセージ

NEXT クライアントへICカード登録を行う際に表示される代表的なエラーメッセージは下記のとおりです。

出力メッセージ	対応方法
ICカードがセットされていません	ICカードが読み取れませんでした。 ICカードリーダーの接続、およびICカードリーダーにICカードが正しくセットされているか確認してください。
NEXT ユーザーIDが入力されていません	NEXT ユーザーIDが入力されていません。 ICカード登録を行うNEXT ユーザーIDを入力してください。
NEXT パスワードが入力されていません	NEXT パスワードが入力されていません。 ICカード登録を行うNEXT ユーザーIDのNEXT パスワードを入力してください。
認証エラー	入力されたNEXT パスワードが正しくありません。 ICカード登録を行うNEXT ユーザーIDのNEXT パスワードを正しく入力してください。
NEXT ユーザーが見つかりません	入力されたNEXT ユーザーIDは存在していません。 ICカード登録を行うNEXT ユーザーIDを正しく入力してください。
初回NEXTパスワード変更が必要です	ICカード登録を行う前に新しいNEXT パスワードに変更する必要があります。 詳細は、「3.3.1. NEXT パスワードの変更」を参照してください。
NEXT パスワードの有効期限切れです	ICカード登録を行う前に新しいNEXT パスワードに変更する必要があります。 詳細は、「3.3.1. NEXT パスワードの変更」を参照してください。
ICカードの再登録は許可されていません	入力されたNEXT ユーザーIDは、ICカードの再登録が許可されていません。 ICカードの再登録許可については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。
登録済のICカードです	セットされているICカードは、既に別のユーザーで使用中です。 別のICカードを使用してください。
オフラインのため継続できません	オフライン状態では、ICカード登録を行うことができません。 ICカード登録はオンライン状態で行ってください。
ユーザーの有効期限切れです	NEXT ユーザーが利用できる有効期間が切れています。 再びサインインできるようにするためには、管理者がNEXT ユーザーの有効期間(終了)の日付を変更する必要があります。 「有効期間(終了)」の設定については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。

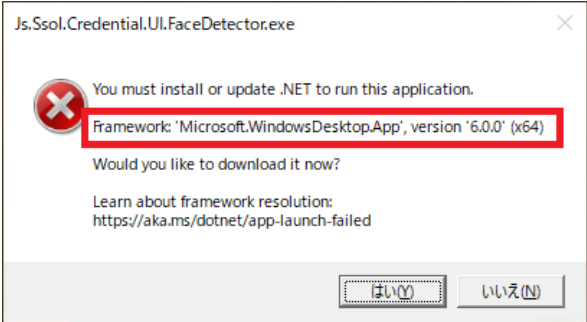
出力メッセージ	対応方法
ユーザーがロックされています	<p>NEXT ユーザーが無効化、またはロックアウトされています。</p> <p>再びサインインできるようにするためには、管理者が NEXT ユーザーを有効化する必要があります。</p> <p>NEXT ユーザーの有効化については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。</p> <p>ユーザーが NEXT 認証に失敗した回数が設定されたしきい値に達すると、NEXT ユーザーがロックアウトされます。</p> <p>再びサインインできるようにするためには、管理者がロックアウトを解除する必要があります。</p> <p>NEXT ユーザーのロックアウトの動作仕様およびロックアウトの解除方法については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。</p>
オフライン有効期限が切れています	<p>オフライン状態でのキャッシュ有効期間が切れています。</p> <p>管理者が設定している「オフライン有効日数」以上の期間、オフライン状態が続くとサインインできません。</p> <p>再びサインインできるようにするためには、NEXT サーバーと NEXT クライアントを通信できる状態にして、サインインする必要があります。</p> <p>「オフライン有効日数」については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。</p>

4.4.2 顔登録時のエラーメッセージ

NEXT クライアントへ顔登録を行う際に表示される代表的なエラーメッセージは下記のとおりです。

出力メッセージ	対応方法
初期化処理でエラーが発生しました	照合画面の初期化処理に失敗しました。 再度、顔情報の登録を行ってください。
顔の検出ができませんでした	顔情報の登録に失敗、またはカメラが使用不能な状態となっています。 頻繁に顔情報の登録に失敗する場合は、「ARCACLAVIS NEXT トラブルシューティングガイド」の「3.3. 顔認証」を参照してください。 繰り返し表示される場合は、「ARCACLAVIS NEXT トラブルシューティングガイド」の「3.3.4. 「顔の検出ができませんでした」と繰り返し表示される」を参照してください。 カメラが接続されていない、カメラが故障している、またはマイクロソフト社の Teams や Skype など、他のアプリケーションでカメラが使用中の場合、カメラが使用不能な状態となります。
顔認証データの生成に失敗しました	顔認証データの生成に失敗しました。 再度、顔情報の登録を行ってください。
NEXT ユーザーIDが入力されていません	NEXT ユーザーIDが入力されていません。 顔登録を行う NEXT ユーザーIDを入力してください。
NEXT パスワードが入力されていません	NEXT パスワードが入力されていません。 顔登録を行う NEXT ユーザーIDの NEXT パスワードを入力してください。
認証エラー	入力された NEXT ユーザーID、または NEXT パスワードが正しくありません。 顔登録を行う NEXT ユーザーID、および NEXT パスワードを正しく入力してください。
NEXT ユーザーが見つかりません	入力された NEXT ユーザーID は存在していません。 顔登録を行う NEXT ユーザーID を正しく入力してください。
初回 NEXT パスワード変更が必要です	顔登録を行う前に新しい NEXT パスワードに変更する必要があります。 詳細は、「3.3.1. NEXT パスワードの変更」を参照してください。

出力メッセージ	対応方法
NEXT パスワードの有効期限切れです	顔登録を行う前に新しい NEXT パスワードに変更する必要があります。 詳細は、「3.3.1. NEXT パスワードの変更」を参照してください。
顔情報の再登録は許可されていません	入力された NEXT ユーザーID は、顔情報の再登録が許可されていません。 顔情報の再登録許可については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。
オフラインのため継続できません	オフライン状態では、顔登録を行うことができません。 顔登録はオンライン状態で行ってください。
ユーザーの有効期限切れです	NEXT ユーザーが利用できる有効期間が切れています。 再びサインインできるようにするためには、管理者が NEXT ユーザーの有効期間(終了)の日付を変更する必要があります。 「有効期間(終了)」の設定については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。
ユーザーがロックされています	NEXT ユーザーが無効化、またはロックアウトされています。 再びサインインできるようにするためには、管理者が NEXT ユーザーを有効化する必要があります。 NEXT ユーザーの有効化については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。 ユーザーが NEXT 認証に失敗した回数が設定されたしきい値に達すると、NEXT ユーザーがロックアウトされます。 再びサインインできるようにするためには、管理者がロックアウトを解除する必要があります。 NEXT ユーザーのロックアウトの動作仕様およびロックアウトの解除方法については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。
オフライン有効期限が切れています	オフライン状態でのキャッシュ有効期間が切れています。 管理者が設定している「オフライン有効日数」以上の期間、オフライン状態が続くとサインインできません。 再びサインインできるようにするためには、NEXT サーバーと NEXT クライアントを通信できる状態にして、サインインする必要があります。 「オフライン有効日数」については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。

出力メッセージ	対応方法
プロバイダーが見つかりません	<p>ライセンスの変更、ライセンスの有効期限切れなどにより顔登録の機能が使用不可となっています。</p> <p>ライセンスについては、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。</p>
アプリケーションエラーが発生しました	<p>顔認証用のランタイム「RS OLFACE」がインストールされていない、または利用者の PC に何らかの問題が発生している可能性があります。</p> <p>「RS OLFACE」がインストールされているかご確認ください。</p> <p>「RS OLFACE」については、「RS OLFACE インストールマニュアル」を参照してください。</p> <p>「RS OLFACE」がインストールされている場合は、一度コンピュータを再起動して、再度顔登録を行ってください。</p>
<p>NEXT 認証中にエラーが発生しました。</p> <p>Windows アカウント情報を入力してサインインを行ってください。PC を再起動してもエラーが発生する場合は、管理者へご連絡ください。</p>	<p>RS OLFACE がアンインストールされており、かつカメラが接続されていない場合に表示されることがあります。</p> <p>ARCACLAVIS NEXT クライアントをアンインストールし、再度 ARCACLAVIS NEXT クライアントと RS OLFACE をインストールした後に、再度、顔認証を行ってください。</p>
<p>顔認証画面を強制終了しました</p> <p>You must install or update .NET to run this application.</p> <p>Framework: {ミドルウェア名}</p> <p>Would you like to download it now?</p> <p>Learn about framework resolution: https://aka.ms/dotnet/app-launch-failed</p>	<p>NEXT クライアントに必要なミドルウェアがインストールされていない、またはミドルウェアの更新が必要です。</p> <p>インストールされていないミドルウェアをインストールしてください。</p> <p>NEXT クライアントに必要なミドルウェア、各ミドルウェアのバージョンについては、「ARCACLAVIS NEXT 動作環境一覧」を参照してください。</p> <p>エラーが発生した際に表示される以下ダイアログから、ミドルウェアを特定することが可能です。</p> <p>(下記例では、「Microsoft Windows Desktop Runtime」が未インストール、または更新が必要となります)</p> 

4.4.3 ワンタイムパスワードシークレット発行時のエラーメッセージ

NEXT クライアントへワンタイムパスワードシークレットの発行を行う際に表示される代表的なエラーメッセージは下記のとおりです。

出力メッセージ	対応方法
NEXT ユーザーID が入力されていません	NEXT ユーザーID が入力されていません。 ワンタイムパスワードシークレットの発行を行う NEXT ユーザーID を入力してください。
NEXT パスワードが入力されていません	NEXT パスワードが入力されていません。 ワンタイムパスワードシークレットの発行を行う NEXT ユーザーID の NEXT パスワードを入力してください。
認証エラー	入力された NEXT パスワードが正しくありません。 ワンタイムパスワードシークレットの発行を行う NEXT ユーザーID の NEXT パスワードを正しく入力してください。
NEXT ユーザーが見つかりません	入力された NEXT ユーザーID は存在していません。 ワンタイムパスワードシークレットの発行を行う NEXT ユーザーID を正しく入力してください。
初回 NEXT パスワード変更が必要です	ワンタイムパスワードシークレットの発行を行う前に新しい NEXT パスワードに変更する必要があります。 詳細は、「3.3.1. NEXT パスワードの変更」を参照してください。
NEXT パスワードの有効期限切れです	ワンタイムパスワードシークレットの発行を行う前に新しい NEXT パスワードに変更する必要があります。 詳細は、「3.3.1. NEXT パスワードの変更」を参照してください。
シークレットが登録済みのためユーザーポータルで確認してください	既にワンタイムパスワードシークレットが発行されています。 NEXT クライアントでワンタイムパスワードシークレットの発行を行う場合は、NEXT マネージャーのユーザーポータルでワンタイムパスワードシークレットのリセットを行う必要があります。 ワンタイムパスワードシークレットのリセットについては、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。
オフラインのため継続できません	オフライン状態では、ワンタイムパスワードシークレットの発行を行うことができません。 ワンタイムパスワードシークレットの発行はオンライン状態で行ってください。

出力メッセージ	対応方法
ユーザーの有効期限切れです	<p>NEXT ユーザーが利用できる有効期間が切れています。</p> <p>再びサインインできるようにするためには、管理者が NEXT ユーザーの有効期間(終了)の日付を変更する必要があります。</p> <p>「有効期間(終了)」の設定については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。</p>
ユーザーがロックされています	<p>NEXT ユーザーが無効化、またはロックアウトされていません。</p> <p>再びサインインできるようにするためには、管理者が NEXT ユーザーを有効化する必要があります。</p> <p>NEXT ユーザーの有効化については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。</p> <p>ユーザーが NEXT 認証に失敗した回数が設定されたしきい値に達すると、NEXT ユーザーがロックアウトされます。再びサインインできるようにするためには、管理者がロックアウトを解除する必要があります。</p> <p>NEXT ユーザーのロックアウトの動作仕様およびロックアウトの解除方法については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。</p>
オフライン有効期限が切れています	<p>オフライン状態でのキャッシュ有効期間が切れています。管理者が設定している「オフライン有効日数」以上の期間、オフライン状態が続くとサインインできません。</p> <p>再びサインインできるようにするためには、NEXT サーバーと NEXT クライアントを通信できる状態にして、サインインする必要があります。</p> <p>「オフライン有効日数」については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。</p>

5. キャッシュ

5.1. 概要

NEXT では、NEXT クライアントにサインインするユーザーの設定情報を NEXT サーバーに保持しています。NEXT クライアントは、サインインしたユーザーの設定情報を必要に応じて NEXT サーバーからダウンロードし、その設定内容に応じて動作します。ただし、NEXT サーバーに接続できない状態ではユーザー情報を取得できないため、NEXT クライアントは認証などが正常に動作できません。

これに対応するため、NEXT クライアントではサインインしたユーザーについて NEXT サーバーから取得した設定情報を、キャッシュとしてローカルに保存することができます。NEXT サーバーに接続できない状態（オフライン状態）でも、NEXT サーバーに接続できる状態（オンライン状態）で一度サインインしたことがあれば、そのときのキャッシュを使用してサインインすることが可能です。

キャッシュを利用してサインインする場合でも、ユーザーは、Windows 自動認証を行うことができます。

5.2. オフラインの判定条件

以下のいずれかに該当する場合、オフライン状態になります。

- NEXT クライアントの IP アドレスが、オフラインネットワークアドレス設定に一致する場合
- オンライン認証タイムアウト値に設定した時間が経過しても、NEXT サーバーからの応答が返ってこない場合
 - ※ネットワークが遅い、NEXT サーバーがビジー状態など
- NEXT サーバーに接続できない場合
 - ※接続待ち時間は以下となります。
 - オンライン認証タイムアウト値に設定した時間、接続待ちを行います。ただし、Windows の仕様により、最大接続待ち時間は 21 秒となります。
 - NEXT クライアントの IP アドレスが、オフラインネットワークアドレス設定に一致する場合は、即時オフラインと判定されます。

Info オフラインネットワークアドレスについては、管理者ガイドを参照ください。

5.3. オフライン時の NEXT パスワードの有効期限

NEXT パスワードの変更は、オフラインでキャッシュを利用している期間は、できません。NEXT サーバーに反映できないためです。このため、オフラインでキャッシュを利用している期間は、NEXT パスワードの有効期限はチェックされません。

Info 顔照合エラー時はオフライン認証となるため、NEXT パスワードの有効期限切れのチェックは行われません。

5.4. オフライン時の NEXT アカウントのロックアウト

オフラインでキャッシュを利用している期間は、NEXT パスワード認証の失敗回数はカウントされません。NEXT サーバーに反映できないためです。このため、オフラインでキャッシュを利用している期間は、NEXT アカウントのロックアウトは発生しません。

NEXT サーバーと接続してオンラインで NEXT 認証をしているときにアカウントのロックアウト状態になっていると、そのままオフラインでキャッシュを利用するときにはアカウントのロックアウト状態のままになります。解除するには、オンライン状態で、管理者により NEXT マネージャーで「パスワードリセット」による解除後に、NEXT クライアントで NEXT 認証できることを確認後にオフラインでご利用ください。

5.5. Windows ドメインコントローラーに対してオフライン時の Windows へのサインイン

Windows ドメインコントローラーに対してオフラインでサインイン先を Windows ドメインにしてサインインするには、事前にオンラインでドメインにサインインし、Windows ユーザープロファイルをローカルに作成しておく必要があります。

NEXT クライアントにキャッシュが存在する状態でも、一度もサインインしていないドメインユーザーで Windows ドメインコントローラーに対してオフラインで NEXT クライアントにサインインすることはできません。

なお、サインイン先がローカルの場合は、ローカルアカウントに存在するユーザーであれば、一度もサインインしていなくても Windows ドメインコントローラーに対してオフラインで NEXT クライアントにサインインできます。

5.6. オフライン時の Windows 自動認証

キャッシュの NEXT ユーザー情報に Windows 自動認証に利用する Windows アカウントの設定があれば、オフラインでも Windows 自動認証が行えます。

オフライン状態で NEXT 緊急パスワードでのサインイン、ロック解除はできますが、Windows 自動認証を使用するには、そのコンピュータに IC カード、顔認証などで NEXT 認証を行いサインインしたことがあり、サインインしようとするユーザーのキャッシュが存在する必要があります。キャッシュが存在しない場合は、Windows 自動認証が行えませんが、Windows サインイン認証は手動で行ってください。

5.7. オフライン時の Windows パスワード変更

オフライン状態のときに Windows パスワードを変更した場合、NEXT サーバーと通信できないため、変更後の Windows パスワードは保存されません。そのため、サインイン/ロック解除の度に Windows 自動認証はエラーとなり、Windows パスワードの再入力が必要となります。NEXT サーバーと通信できるオンライン状態で、Windows パスワードの再入力を行うことで、NEXT サーバーに Windows パスワードが保存され、次回以降、Windows 自動認証が行えます。

5.8. オフライン時の NEXT 緊急パスワード認証

NEXT 緊急パスワード認証は、オフラインでもサインイン、ロック解除が行えます。

ただし、Windows 自動認証を使用するには、そのコンピュータに IC カード、顔認証などで NEXT 認証を行いサインインしたことがあり、サインインしようとするユーザーのキャッシュが存在する必要があります。キャッシュが存在しない場合は、Windows 自動認証が行えませんが、Windows 認証は手動で行ってください。

また、オフライン時は NEXT ユーザーがロックアウトの場合でも、NEXT 緊急パスワード認証は利用できます。オンライン時は、NEXT ユーザーがアカウントロックの場合、NEXT 緊急パスワード認証は利用できません。先に当該 NEXT ユーザーのアカウントロックを解除してください。

5.9. オフライン時の NEXT 管理者パスワード認証

NEXT 管理者パスワード認証は、オフラインでもサインイン、ロック解除が行えます。

5.10. オフライン時の認証情報の登録

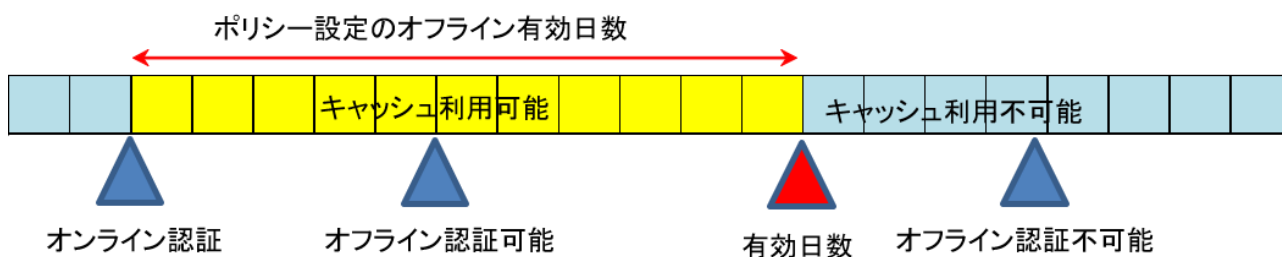
認証情報の登録は、オフラインではできません。認証情報の登録はオンラインで行ってください。

Info オフライン状態で NEXT クライアントの利用を開始する場合の手順については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。

5.11. キャッシュの有効期間

NEXT クライアントは NEXT サーバーと接続できない場合、キャッシュを利用して NEXT 認証を行います。

キャッシュを利用して NEXT 認証できる期間を「オフライン有効日数」と言い、期間は下図のようになります。



「オフライン有効日数」は、NEXT マネージャーのポリシー設定で期間を設定することが可能です。

「オフライン有効日数」が“0”の場合は、無期限で使用できます。

有効期限が切れるとキャッシュの内容は無効になり、オフライン状態のときにキャッシュでのサインインができなくなります。

再びサインインできるようにするためには、NEXT サーバーと NEXT クライアントを通信できる状態にして、サインインする必要があります。

5.12. キャッシュの更新

キャッシュは、以下のタイミングで最新の状態に更新されます。

NEXT 認証時に、NEXT サーバー上のユーザー情報の更新状態を確認し、更新されている場合はキャッシュを最新の状態に更新します。認証情報の登録時も、登録後にサインインするため、このサインイン時に含まれます。

NEXT パスワードや Windows パスワードの変更など、NEXT サーバー上のユーザー情報を更新する処理（操作）を行った場合、キャッシュも更新します。

6. NEXT 離席モニター

6.1. 概要

NEXT 離席モニターとは、NEXT 顔認証で Windows にサインイン、またはロック解除後に定期的に顔照合を行うことにより離席を監視し、離席検出時に画面をロックする機能です。

Info 離席モニターの機能を使用する場合は、NEXT クライアントがインストールされているコンピューターに NEXT 離席モニターがインストールされている必要があります。
NEXT 離席モニターのインストール手順は、「ARCACLAVIS NEXT セットアップガイド」を参照してください。

Info NEXT 離席モニターの設定は、NEXT マネージャーの「クライアント設定」-「アプリケーション設定」-「離席モニター」で行うことが可能です。
NEXT 離席モニターの設定手順は、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。

Info NEXT 離席モニターを使用する場合は、NEXT 顔認証が行える環境が必要となります。

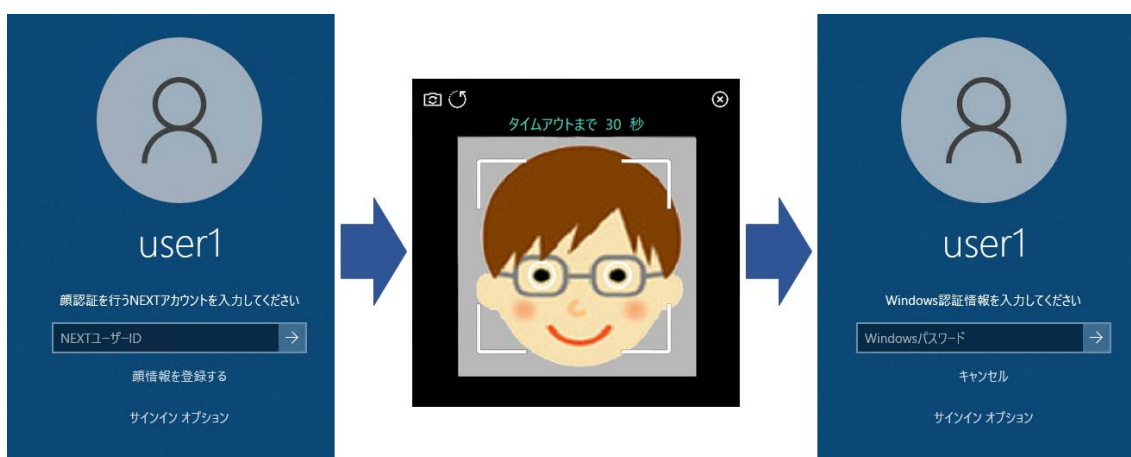
6.2. NEXT 離席モニターによる離席監視

NEXT 離席モニターを使用する場合は、NEXT クライアントがインストールされているコンピューターに NEXT 顔認証を行って Windows へサインイン、または、ロック解除する必要があります。

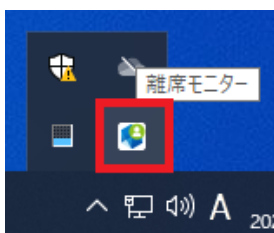
Info NEXT 顔認証以外で Windows へサインインした場合は、NEXT 離席モニターによる離席監視は行われません。

ここでは、顔認証を使って Windows へサインインし、NEXT 離席モニターを使用する流れを例示します。

1. 顔認証を行い、Windows へサインインします。



2. Windows へサインイン後、NEXT 離席モニターがタスクトレイの常駐アプリとして起動します。

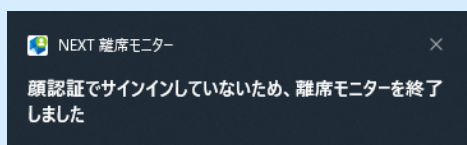


Info NEXT 離席モニターは、Windows へのサインイン時に自動的に起動されます。ロック時は離席監視が停止され、ロック解除時に離席監視が再開されます。

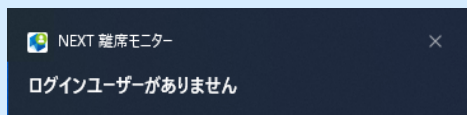
Info NEXT 離席モニターは、スタートメニューに追加されます。起動は自動で行われますのでスタートメニューから起動する必要はありません。

Info NEXT 顔認証以外で Windows へサインインし、スタートメニューから NEXT 離席モニターは起動した場合は、下記トースト通知が表示されます。

<NEXT IC カード認証、NEXT 緊急パスワード認証時>



<NEXT 管理者パスワード認証、Windows 標準認証時>



Info 離席モニターの表示設定については、「6.3. タスクトレイメニュー」を参照してください。

Info トースト通知のメッセージ一覧については、「6.5. トースト通知」を参照してください。

3. Windows へのサインイン後、NEXT マネージャーの「モニタリング間隔(秒)」で設定した時間、離席監視による顔照合を行いません。

Info 「モニタリング間隔(秒)」は離席を監視する間隔です。
設定の詳細については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。

離席モニターの設定「モニター表示」がオン(初期状態はオフ)の場合は、NEXT マネージャーの「モニタリング間隔(秒)」で設定した時間、照合待機中画面が表示されます。

照合待機中画面では、照合開始までの時間がカウントダウンメッセージとして表示されます。



Info 「照合待機中画面」の詳細については、「6.4.1. 照合待機中画面」を参照してください。

4. NEXT マネージャーの「モニタリング間隔(秒)」で設定した時間経過後、離席監視による顔照合を行います。

離席監視による顔照合は、NEXT マネージャーの「照合時間(秒)」で設定した時間繰り返します。

Info 「照合時間(秒)」は、カメラが起動し、照合を実行する時間です。
設定の詳細については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。

離席モニターの設定「モニター表示」がオンの場合は、NEXT マネージャーの「照合時間(秒)」で設定した時間の間、照合中画面が表示されます。

照合中画面では、カメラからの画像と、画面ロックまでの時間がカウントダウンメッセージとして表示されます。



Info 「照合中画面」の詳細については、「6.4.2. 照合中画面」を参照してください。

5. 離席監視による顔照合が NEXT マネージャーの「照合時間(秒)」の間に成功した場合は離席していないと判断し、手順 3~4 を繰り返します。

「照合時間(秒)」で設定した時間内に離席監視による顔照合が成功しなかった場合は、画面がロックされます。

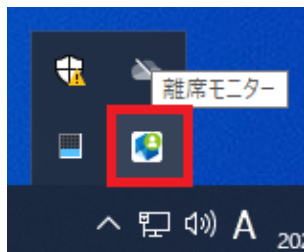


Info 「照合失敗時に離席モニター画面を表示する」がオンに設定されている状態で、照合時間内に顔照合が成功しなかった場合は、離席モニター画面が非表示の場合でも離席モニター画面が表示され、離席監視による再照合が行われます。

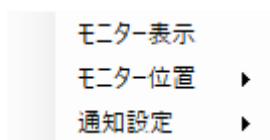
「照合失敗時に離席モニター画面を表示する」の設定については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。

6.3. タスクトレイメニュー

NEXT 離席モニターは、タスクトレイの常駐アプリとして起動します。



タスクトレイの離席モニターを右クリックすることで、離席モニターの表示設定を変更することができます。



項目名	説明
モニター表示	クリックすると離席モニター画面を表示します。
モニター位置	離席モニター画面の表示位置を指定することができます。 <ul style="list-style-type: none"> ・左下配置 離席モニター画面を Windows 画面の左下に表示させます。 ・右下配置 離席モニター画面を Windows 画面の右下に表示させます。 初期値：右下配置
通知設定	離席モニターのイベントによるトースト通知の表示有無を指定することができます。 <ul style="list-style-type: none"> ・表示する イベントによるトースト通知が表示されます。 ・表示しない イベントによるトースト通知が表示されません。 ただし、一部のトースト通知は、設定に関わらず表示されます。 詳細は「6.5. トースト通知」を参照してください。 初期値：表示しない

6.4. 離席モニター画面

離席モニターの「モニター表示」をクリックした場合、離席モニター画面が表示されます。

離席モニター画面では、照合中画面に切り替わるまでのカウントダウン表示、または、離席監視による顔照合の状態が表示されます。

6.4.1. 照合待機中画面

以下に照合待機中画面のデザイン、および各項目について説明します。



No	項目	補足
①	カウントダウンメッセージ (秒)	「照合開始まで 56 秒」などのメッセージが表示されます。NEXT マネージャーの「モニタリング間隔(秒)」で設定した秒数からカウントダウンし、0 秒になると照合中画面に切り替わります。
②	カメラ切り替えボタン	離席監視による顔照合で使用するカメラを設定します。2 つ以上カメラが接続されている場合、別のカメラに切り替わります。
③	カメラ回転ボタン	離席監視による顔照合で使用するカメラを回転します。押下するたびにカメラの回転角度を 90 度ずつ回転します。 ※使用するカメラが使用不可の状態でもカメラの回転角度の変更は可能となります。
④	閉じるボタン	照合待機中画面を閉じて、モニター表示の設定をオフにします。
⑤	キャプチャ画像	イメージ画像が表示されます。カメラ切り替えボタンをクリックすると、接続されているカメラからの画像が表示されます。


No	項目	補足
⑥	カメラ番号	「カメラ切り替え」ボタンを押下時に使用されているカメラ番号が表示されます。 ※カメラ番号は1秒でフェードアウトします。

Info 離席モニターを初めて使用する場合は、NEXT 顔認証で使用しているカメラ設定を使用しますが、<カメラ切り替え>ボタン、<カメラ回転>ボタンをクリックすると、離席モニター用のカメラ設定がユーザーごとに作成され、NEXT 顔認証とは別のカメラ設定となります。離席モニターで使用するカメラ設定は、ユーザーごとに保持します。NEXT 顔認証時のサインイン、ロック解除時のカメラ設定は、コンピューターで共通となっています。

6.4.2. 照合中画面

以下に照合中画面のデザイン、および各項目について説明します。



No	項目	補足
①	カウントダウンメッセージ (秒)	「画面ロックまで 17 秒」などのメッセージが表示されます。NEXT マネージャーの「照合時間(秒)」で設定した秒数からカウントダウンし、0 秒になると画面をロックします。
②	カメラ切り替えボタン	離席監視による顔照合で使用するカメラを設定します。2 つ以上カメラが接続されている場合、別のカメラに切り替わります。
③	カメラ回転ボタン	離席監視による顔照合で使用するカメラを回転します。押下するたびにカメラの回転角度を 90 度ずつ回転します。 ※使用するカメラが使用不可の状態でもカメラの回転角度の変更は可能となります。
④	閉じるボタン	照合中画面を閉じて、モニター表示の設定をオフにします。
⑤	キャプチャ画像	離席監視による顔照合で使用するカメラからの画像が表示されます。 ※「キャプチャ画像」に表示される画像は、「カメラ切り替え」ボタン、または「カメラ回転」ボタンを押下した際のスナップショットで更新されます。 ※カメラが使用不可の場合、キャプチャ画像の代わりにカメラ使用不可のアイコン  が表示されます。
⑥	ガイド	離席監視による顔照合が成功しやすくなる目安として表示しているガイドです。
⑦	メッセージ	離席監視による顔照合のメッセージが表示されます。表示されるメッセージは下表を参照してください。

No	項目	補足
⑧	カメラ番号	「カメラ切り替え」ボタンを押下時に使用されているカメラ番号が表示されます。 ※カメラ番号は1秒でフェードアウトします。

メッセージに表示される文言は以下の通りです。

メッセージ内容	説明
顔照合エラー	離席監視による顔照合に失敗した場合に表示されます。
カメラが使用できません	離席監視による顔照合で使用するカメラが使用できない場合に表示されます。
照合してください	NEXT マネージャーの「照合時間(秒)」で設定した時間内に離席監視による顔照合が成功せず、再照合を行う場合に表示されます。
ロックしました	NEXT マネージャーの「照合時間(秒)」で設定した時間内に離席監視による顔照合が成功せず、画面がロックした場合に表示されます。
認証サービスが停止したため、離席モニターを停止しました	離席モニターが使用できない状態となっている場合に表示されます。

6.5. トースト通知

離席監視による顔照合の結果、画面ロック通知などのメッセージをトースト通知で表示します。

トースト通知は、タスクトレイに常駐している離席モニターの「通知設定」で表示の切り替えが可能です。一部のトースト通知は「通知設定」が「表示しない」に設定されていても通知されます。

離席モニターで表示されるトースト通知は以下となります。

トースト通知のメッセージ内容	説明	通知設定が「表示しない」時の動作
カメラが使用できません	離席監視による顔照合で使用するカメラが使用できない場合に表示されます。 別のカメラを使用する場合は、「カメラ切り替え」ボタンをクリックしてください。 「カメラ切り替え」ボタンについては、「6.4. 離席モニター画面」を参照してください。	表示しない
照合してください	NEXT マネージャーの「照合時間(秒)」で設定した時間内に離席監視による顔照合に成功せず、再照合を行う場合に表示されます。 再照合は、NEXT マネージャーの「照合失敗時に離席モニター画面を表示する」がオンの場合に行われます。 「照合失敗時に離席モニター画面を表示する」の設定については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。	表示しない
ロックしました	NEXT マネージャーの「照合時間(秒)」で設定した時間内に離席監視による顔照合に成功せず、画面がロックした場合に表示されます。	表示される
N 秒ロックを保留しました ※N：離席モニター停止時間(秒)	ロック保留画面で「ロックを保留」ボタンをクリックした場合に表示されます。 「ロック保留画面」については、「6.6. カメラ使用不能な場合の動作」を参照してください。	表示しない
顔認証でサインインしていないため、離席モニターを終了しました	NEXT IC カード認証、NEXT 緊急パスワード認証でサインイン、または、ロック解除時に表示されます。	表示される
ログインユーザーがありません	NEXT 管理者パスワード認証、Windows 標準認証でサインイン、または、ロック解除時に表示されます。	表示される
離席モニターの設定がありません	離席モニターのライセンスがない状態で離席モニターを実行	表示される

トースト通知のメッセージ内容	説明	通知設定が「表示しない」時の動作
離席モニターの初期化に失敗したため終了します	NEXT 離席モニターに何らかの障害が発生しています。 コンピューターを再起動して、再度離席監視を行ってください。	表示される
認証サービスが停止したため、離席モニターを停止しました	離席モニターが使用できない状態となっている場合に表示されます。 コンピューターを再起動して、再度離席監視を行ってください。	表示される

6.6. カメラ使用不能な場合の動作

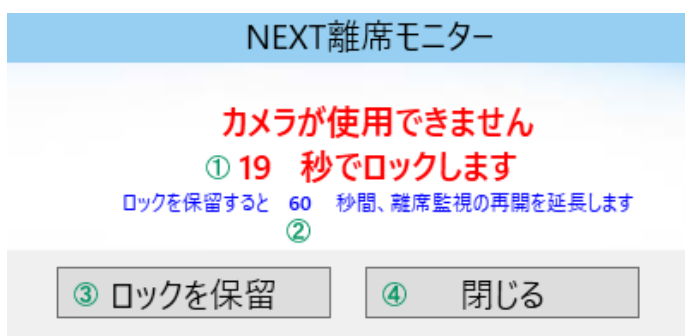
離席モニターでは顔照合を行うため、カメラを使用しますが、以下の状態ではカメラ使用不能な状態として判断します。

- ・ 離席モニターで使用するカメラが接続されていない、故障している
- ・ 離席モニターで使用するカメラが別アプリケーションで使用
 マイクロソフト社の Teams や Skype など、他のアプリケーションでカメラが使用中の場合、離席モニターはカメラ使用不能な状態となります。

離席監視による顔照合を行う際にカメラ使用不能な状態と判断した場合は、NEXT マネージャーの「カメラ使用不能時にモニターを一時停止する」を ON に設定することにより、ロック保留画面が表示され、画面のロックを保留することができます。

Info 「カメラ使用不能時にモニターを一時停止する」がオフに設定されている場合は、ロック保留画面が表示されずにロックされます。
 「カメラ使用不能時にモニターを一時停止する」の設定については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。

以下にロック保留画面のデザイン、および各項目について説明します。



No	項目	補足
①	ロック状態までのカウントダウンメッセージ(秒)	NEXT マネージャーの「照合時間(秒)」で設定した秒数からカウントダウンし、0 秒になるとロック状態となります。
②	ロック保留による延長メッセージ(秒)	「ロック保留ボタン」をクリックした場合の動作が表示されます。
③	ロック保留ボタン	NEXT マネージャーの「離席モニター停止時間(秒)」に設定した時間、離席監視を停止します。 「離席モニター停止時間(秒)」については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。
④	閉じるボタン	ロック保留画面を閉じます。 「照合時間(秒)」経過後、ロック状態となります。

6.7. 使用する顔情報

離席モニターの顔照合では、サインインしている NEXT ユーザーの顔情報を使用します。

NEXT ユーザーの顔情報が登録されていない、またはオフラインで顔情報を取得できない場合は、離席監視による顔照合が失敗となります。

離席監視による顔照合に成功しない場合は、サインインしている NEXT ユーザーの顔情報が登録されているかご確認頂き、オンライン環境で NEXT 認証を利用したサインイン、または、ロック解除を行ってください。

離席モニターで使用する顔情報の取得は、NEXT 認証を利用したサインイン、または、ロック解除後、離席モニターの初回認証時のみとなります。

NEXT サーバーの顔情報を更新後、最新の顔情報を使用して離席モニターを使用する場合は、再度サインイン、または、ロック解除を行ってください。

7. 自動認証

7.1. 概要

自動認証は、アプリケーションやリモートデスクトップへのログインなどの操作を予め設定した自動認証情報を使用して自動入力を行うことで認証する機能です。

自動認証の実行は、NEXT 自動認証プレイヤーから行います。

7.2. NEXT 自動認証プレイヤーによる自動認証

NEXT 自動認証プレイヤーは、NEXT サーバーに登録されている自動認証設定、および自動入力設定を使用して自動認証を行う機能です。

たとえば、アプリケーションの起動、ユーザーID やパスワードの入力、クリック操作などの操作を自動で実行することが可能です。

自動認証設定、および自動入力設定は NEXT ユーザーごとに設定が可能です。

Info 自動認証プレイヤーの機能を使用する場合は、NEXT クライアントがインストールされているコンピューターに NEXT 自動認証プレイヤーがインストールされている必要があります。NEXT 自動認証プレイヤーのインストール手順は、「ARCACLAVIS NEXT セットアップガイド」を参照してください。

Info 自動認証設定、および自動入力設定は、NEXT 自動認証クリエイター、および NEXT マネージャーから設定を行います。自動認証設定、および自動入力設定の設定手順は、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。

NEXT 自動認証プレイヤーを起動すると、ログインしている NEXT ユーザーの自動認証設定を取得します。メニューから[再生]をクリックし、実行したい自動認証設定の左にある再生ボタンを押下することで自動認証が実行されます。

また、編集ボタンを押下して自動認証時に入力されるユーザーID やパスワードを変更することもできます。変更した自動認証情報は[サーバー同期(再生設定)]をクリックすることで NEXT サーバーへ同期することも可能です。

Info 自動認証プレイヤーの再生手順については、「7.5.3. 自動認証プレイヤー再生例」を参照してください。

Info 自動認証プレイヤーの機能は、オフラインでも使用することが可能ですが、変更したユーザー情報を NEXT サーバーへ同期することはできません。

Info NEXT 自動認証プレイヤーは、以下いずれかの NEXT 認証が成功した場合に有効となります。

- ・NEXT IC カード認証
- ・NEXT 顔認証
- ・NEXT 緊急パスワード認証

(NEXT 管理者パスワード認証、Windows 標準認証で Windows へサインインした場合は、NEXT 自動認証プレイヤーは無効となり、下記画面が表示されます)



7.3. 起動

NEXT 自動認証プレイヤーを起動するまでの手順を説明します。

7.3.1. NEXT 自動認証プレイヤーの起動手順

1. NEXT クライアントで NEXT 認証を行い、サインインします。

Info NEXT クライアントの認証方式の内、管理者パスワード認証で認証した場合は自動認証プレイヤーを使用できません。

2. Windows のスタートメニューから「NEXT 自動認証プレイヤー」を実行します。



Info NEXT 自動認証プレイヤーをインストールすると、デスクトップに NEXT 自動認証プレイヤーのショートカットが作成されます。デスクトップのショートカットからも実行が可能です。



3. NEXT 自動認証プレイヤーが起動します。



7.3.2. NEXT 自動認証プレイヤーを利用できる NEXT ユーザーのロール設定

NEXT 自動認証プレイヤーはいずれのロール設定でも使用できます。

ロール	NEXT 自動認証クリエイターの使用
管理者	使用可能です
サブシステム利用者	使用可能です
ポータル利用者	使用可能です

Info ロール設定については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。

7.3.3. オフライン利用について

オフライン状態、または管理サーバーに接続できない状態でも NEXT 自動認証プレイヤーは使用できます。但し、サーバー同期はオフライン状態、または管理サーバーに接続できない状態では実行できません。

Info 「サーバー同期」については、「7.7. サーバー同期」を参照してください。

7.3.4. ユーザーの切り替えについて

NEXT 自動認証プレイヤーを起動中に別の NEXT ユーザーでサインインした場合は、新しくサインインした NEXT ユーザーの NEXT ユーザー情報を取得し、NEXT 自動認証プレイヤーを再読み込みして、プレイヤーメイン画面を表示します。

NEXT ユーザー情報を取得できない場合は、「ログインユーザーがありません」のエラーメッセージが表示されます。

7.4. 画面構成

NEXT 自動認証プレイヤーは、以下の操作から起動ができます。

- ・スタートメニュー「ARCACLAVIS NEXT」 - 「NEXT 自動認証プレイヤー」を実行
- ・デスクトップショートカット「NEXT 自動認証プレイヤー」を実行

NEXT 自動認証プレイヤーを起動すると、下記プレイヤーメニュー画面が表示されます。

左側のメニューボタンエリアと右側のメニューコンテンツエリアから構成されています。

メニューボタンエリアの各メニューをクリックすると、メニューコンテンツエリアに表示、または別の画面に遷移して表示されます。

タイトル名とサインイン中の NEXT ユーザーID は、ヘッダーエリアに表示されます。

エラー等のメッセージは画面下の情報エリアに表示されます。



メニューボタンエリアに表示される項目は、以下のとおりです。

項目	説明
再生	プレイヤーメイン画面へ遷移します。 プレイヤーメイン画面については、「7.5.1. プレイヤーメイン画面」を参照してください。
サーバー同期(再生設定)	メニューコンテンツエリアにサーバー同期メニュー画面が表示されます。 サーバー同期メニュー画面については、「7.7. サーバー同期」を参照してください。
製品情報	メニューコンテンツエリアに製品情報メニュー画面が表示されます。 製品情報メニュー画面については、「7.8. 製品情報」を参照してください。

7.5. 再生

NEXT 自動認証プレイヤーでは、自動認証設定を再生することができます。

また、自動認証設定でユーザーの編集が許可されている場合は、ユーザーID、パスワードなどの入力値の編集を行うことが可能です。

Info 入力値の編集については、「7.6.3. ユーザー入力値の編集許可」を参照してください。



7.5.1. プレイヤーメイン画面

プレイヤーメニュー画面で[再生]をクリックすると、プレイヤーメイン画面に遷移します。

プレイヤーメイン画面では、NEXT 認証でサインインした NEXT ユーザーに割り当てられた自動認証設定の一覧表示、各自動認証設定の再生、編集をすることができます。

以下にプレイヤーメイン画面のデザイン、および各項目について説明します。



No	項目	説明
①	戻る	<p>プレイヤーメニュー画面に戻ります。</p> <p>ただし、NEXT サーバーに同期していないデータがある場合は、「変更をサーバーと同期しますか？」の確認ダイアログが表示され、選択内容によって遷移する画面が変わります。</p> <p>[OK]ボタン押下時：サーバー同期メニュー画面に遷移します。</p> <p>[キャンセル]ボタン押下時：プレイヤーメニュー画面に戻ります。</p> <p>※プレイヤーメニュー画面に戻る場合は、前回表示した画面に戻ります。</p>
②	設定名検索	<p>検索したいキーワードを入力後に[Enter]キーで、「自動認証設定名」を検索することができます。</p> <p>検索条件：中間一致、大文字小文字を区別しません。</p>
③	設定名	<p>自動認証設定の設定名が表示されます。</p> <p>ヘッダーの[設定名]をクリックすることでコンテンツエリアの内容を「設定名」で並び替えます。</p> <p>※クリックするたびに「昇順」→「降順」と切り替わります。</p>
④	ステータス	<p>自動認証設定の再生結果が表示されます。</p> <ul style="list-style-type: none"> ・自動認証が成功時：再生成功 ・自動認証が失敗時：再生エラー ・自動認証が未実行：(空白) <p>※画面の再読み込みを行うとステータスの結果は消去されます。</p> <p>ヘッダーの[ステータス]をクリックすることでコンテンツエリアの内容を「ステータス」で並び替えます。</p> <p>※クリックするたびに下記順の並びに切り替わります。</p> <ul style="list-style-type: none"> ・「再生成功」→「再生エラー」→「空白(未再生)」 ・「空白(未再生)」→「再生エラー」→「再生成功」
⑤	再生日時	<p>自動認証設定を再生した日時が表示されます。</p> <p>※画面の再読み込みを行うと再生日時は消去されます。</p> <p>ヘッダーの[再生日時]をクリックすることでコンテンツエリアの内容を「再生日時」で並び替えます。</p> <p>※クリックするたびに下記順の並びに切り替わります。</p> <ul style="list-style-type: none"> ・「再生日時が新しい順」→「空白(未再生)」 ・「空白(未再生)」→「再生日時が古い順」
⑥	再生	自動認証設定を再生します。
⑦	編集	<p>自動認証詳細画面に遷移します。</p> <p>自動認証詳細画面では、自動認証設定の編集を行うことができます。</p>
⑧	アイコン	<p>自動認証タイプの簡易アイコンが表示されます。</p> <p> : Edge</p> <p> : リモートデスクトップ接続</p>

No	項目	説明
⑨	メッセージ	<p>自動認証を再生した場合のメッセージが表示されます。</p> <ul style="list-style-type: none"> ・自動認証が再生中：再生開始 ・自動認証が成功時：再生終了 ・自動認証が失敗時：実行エラー：{エラーメッセージ} <p>※「エラーメッセージ」については、「7.5.4. 再生時のエラーメッセージ」を参照してください。</p>

Info 自動認証設定の再生中は、NEXT 自動認証プレイヤーの操作はできません。再生中は下記画面のように表示されます。



Info NEXT 自動認証プレイヤーを起動中に別のNEXT ユーザーでサインインした場合は、新しくサインインしたNEXT ユーザーのNEXT ユーザー情報を取得し、NEXT 自動認証プレイヤーを再読み込みして、プレイヤーメイン画面を表示します。NEXT ユーザー情報を取得できない場合は、「ログインユーザーがありません」のエラーメッセージが表示されます。

7.5.2. 自動認証詳細画面

自動認証詳細画面は、プレイヤーメイン画面で自動認証設定名の[編集]をクリックすると表示されます。自動認証詳細画面では、自動認証設定の詳細が表示され、再生、編集することができます。

以下に自動認証詳細画面のデザイン、および各項目について説明します。



No	項目	説明
①	戻る	プレイヤーメイン画面に戻ります。 ただし、NEXT サーバーに同期していないデータがある場合は、「変更をサーバーと同期しますか？」の確認ダイアログが表示され、選択内容によって遷移する画面が変わります。 [OK]ボタン押下時：サーバー同期メニュー画面に遷移します。 [キャンセル]ボタン押下時：プレイヤーメイン画面に戻ります。
②	再生	自動認証設定を再生します。 「再生対象チェック」にチェックが付いている操作のみ再生します。
③	設定名	詳細表示されている自動認証の設定名が表示されます。
④	再生対象チェック	[再生]をクリックした場合に操作を再生するかどうかを指定します。

No	項目	説明
⑤	操作編集	<p>ユーザー設定画面に遷移します。</p> <p>ユーザー設定画面では、「操作情報」を編集することができます。</p> <p>ユーザー設定画面については、「7.6.1. ユーザー設定画面」を参照してください。</p> <p>※自動認証設定でユーザーによる編集が許可されていない場合は、「操作編集」ボタンは表示されません。</p> <p>詳細は、「7.6.3. ユーザー入力値の編集許可」を参照してください。</p>
⑥	操作情報	<p>操作名、自動入力設定値などの操作情報が表示されます。</p> <p>表示される項目は、操作タイプにより異なります。</p>
⑦	メッセージ	<p>自動認証を再生した場合のメッセージが表示されます。</p>

7.5.3. 自動認証プレイヤー再生例

ここでは、「Edge Web フォーム」と「リモートデスクトップ接続」の再生例を記載します。

再生する前に、各再生例に記載している前提設定を行う必要があります。

「NEXT 自動認証クリエイター」、および「NEXT 自動認証プレイヤー」については、前提設定を行った後に「サーバー同期」を行ってください。

Info NEXT 自動認証クリエイターの操作手順は、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。

Info NEXT 自動認証プレイヤーで自動認証を再生時、操作コンテンツによっては時間がかかり、再生エラーとなる場合があります。

その場合は、NEXT 自動認証クリエイターの各操作コンテンツの「リトライ時間(秒)」を長く設定することにより解消されます。

NEXT 自動認証クリエイターの設定手順は、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。

Edge Web フォームの再生例 管理者による設定の再生

ここでは、利用者が「NEXT ユーザーID」、「NEXT パスワード」の設定、および入力を行わず、管理者が事前に設定した自動入力設定値を自動入力して、認証を行う例を説明します。

下記に自動認証設定を再生する流れを例示します。

- ・自動で Edge ブラウザが起動する
- ・自動で NEXT マネージャーのログイン画面を表示する
- ・管理者が設定した NEXT ユーザーID「User1」が自動入力される
- ・管理者が設定した NEXT パスワード「password」が自動入力される
- ・自動で「サインイン」ボタンをクリックし、サインインする

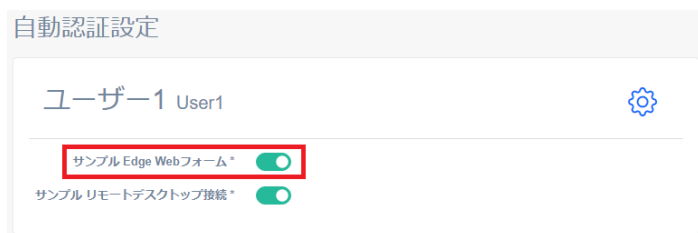
【NEXT 自動認証クリエイター 前提設定】

NEXT 自動認証クリエイターで下記の自動認証設定が作成されている必要があります。

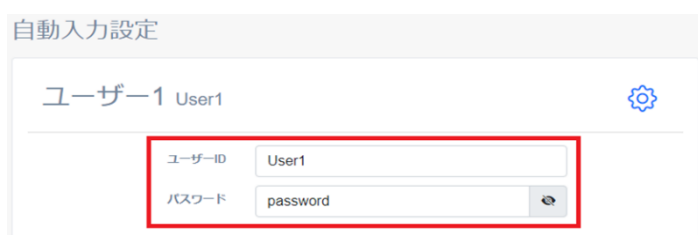
操作	フロー																												
Edgeブラウザの実行	<table border="1"> <tr> <td><input checked="" type="checkbox"/></td> <td></td> <td>操作 実行ファイル 引数 リトライ時間(秒)</td> <td>Edgeブラウザの実行 Edgeブラウザアプリケーション 5</td> </tr> <tr> <td>URL入力操作</td> <td> <table border="1"> <tr> <td><input checked="" type="checkbox"/></td> <td></td> <td>操作 Url リトライ時間(秒)</td> <td>URL入力操作 https://192.168.4.134/Account/Login? ReturnUrl=%2F 5</td> </tr> <tr> <td>ユーザーID入力操作</td> <td> <table border="1"> <tr> <td><input checked="" type="checkbox"/></td> <td></td> <td>操作 自動入力設定値 編集許可 リトライ時間(秒)</td> <td>ユーザーID入力操作 ユーザーID False 5</td> </tr> <tr> <td>パスワード入力操作</td> <td> <table border="1"> <tr> <td><input checked="" type="checkbox"/></td> <td></td> <td>操作 自動入力設定値 編集許可 リトライ時間(秒)</td> <td>パスワード入力操作 パスワード False 5</td> </tr> <tr> <td>クリック操作</td> <td> <table border="1"> <tr> <td><input checked="" type="checkbox"/></td> <td></td> <td>操作 リトライ時間(秒)</td> <td>クリック操作 5</td> </tr> </table> </td> </tr> </table> </td> </tr> </table></td></tr></table></td></tr></table>	<input checked="" type="checkbox"/>		操作 実行ファイル 引数 リトライ時間(秒)	Edgeブラウザの実行 Edgeブラウザアプリケーション 5	URL入力操作	<table border="1"> <tr> <td><input checked="" type="checkbox"/></td> <td></td> <td>操作 Url リトライ時間(秒)</td> <td>URL入力操作 https://192.168.4.134/Account/Login? ReturnUrl=%2F 5</td> </tr> <tr> <td>ユーザーID入力操作</td> <td> <table border="1"> <tr> <td><input checked="" type="checkbox"/></td> <td></td> <td>操作 自動入力設定値 編集許可 リトライ時間(秒)</td> <td>ユーザーID入力操作 ユーザーID False 5</td> </tr> <tr> <td>パスワード入力操作</td> <td> <table border="1"> <tr> <td><input checked="" type="checkbox"/></td> <td></td> <td>操作 自動入力設定値 編集許可 リトライ時間(秒)</td> <td>パスワード入力操作 パスワード False 5</td> </tr> <tr> <td>クリック操作</td> <td> <table border="1"> <tr> <td><input checked="" type="checkbox"/></td> <td></td> <td>操作 リトライ時間(秒)</td> <td>クリック操作 5</td> </tr> </table> </td> </tr> </table> </td> </tr> </table></td></tr></table>	<input checked="" type="checkbox"/>		操作 Url リトライ時間(秒)	URL入力操作 https://192.168.4.134/Account/Login? ReturnUrl=%2F 5	ユーザーID入力操作	<table border="1"> <tr> <td><input checked="" type="checkbox"/></td> <td></td> <td>操作 自動入力設定値 編集許可 リトライ時間(秒)</td> <td>ユーザーID入力操作 ユーザーID False 5</td> </tr> <tr> <td>パスワード入力操作</td> <td> <table border="1"> <tr> <td><input checked="" type="checkbox"/></td> <td></td> <td>操作 自動入力設定値 編集許可 リトライ時間(秒)</td> <td>パスワード入力操作 パスワード False 5</td> </tr> <tr> <td>クリック操作</td> <td> <table border="1"> <tr> <td><input checked="" type="checkbox"/></td> <td></td> <td>操作 リトライ時間(秒)</td> <td>クリック操作 5</td> </tr> </table> </td> </tr> </table> </td> </tr> </table>	<input checked="" type="checkbox"/>		操作 自動入力設定値 編集許可 リトライ時間(秒)	ユーザーID入力操作 ユーザーID False 5	パスワード入力操作	<table border="1"> <tr> <td><input checked="" type="checkbox"/></td> <td></td> <td>操作 自動入力設定値 編集許可 リトライ時間(秒)</td> <td>パスワード入力操作 パスワード False 5</td> </tr> <tr> <td>クリック操作</td> <td> <table border="1"> <tr> <td><input checked="" type="checkbox"/></td> <td></td> <td>操作 リトライ時間(秒)</td> <td>クリック操作 5</td> </tr> </table> </td> </tr> </table>	<input checked="" type="checkbox"/>		操作 自動入力設定値 編集許可 リトライ時間(秒)	パスワード入力操作 パスワード False 5	クリック操作	<table border="1"> <tr> <td><input checked="" type="checkbox"/></td> <td></td> <td>操作 リトライ時間(秒)</td> <td>クリック操作 5</td> </tr> </table>	<input checked="" type="checkbox"/>		操作 リトライ時間(秒)	クリック操作 5
<input checked="" type="checkbox"/>		操作 実行ファイル 引数 リトライ時間(秒)	Edgeブラウザの実行 Edgeブラウザアプリケーション 5																										
URL入力操作	<table border="1"> <tr> <td><input checked="" type="checkbox"/></td> <td></td> <td>操作 Url リトライ時間(秒)</td> <td>URL入力操作 https://192.168.4.134/Account/Login? ReturnUrl=%2F 5</td> </tr> <tr> <td>ユーザーID入力操作</td> <td> <table border="1"> <tr> <td><input checked="" type="checkbox"/></td> <td></td> <td>操作 自動入力設定値 編集許可 リトライ時間(秒)</td> <td>ユーザーID入力操作 ユーザーID False 5</td> </tr> <tr> <td>パスワード入力操作</td> <td> <table border="1"> <tr> <td><input checked="" type="checkbox"/></td> <td></td> <td>操作 自動入力設定値 編集許可 リトライ時間(秒)</td> <td>パスワード入力操作 パスワード False 5</td> </tr> <tr> <td>クリック操作</td> <td> <table border="1"> <tr> <td><input checked="" type="checkbox"/></td> <td></td> <td>操作 リトライ時間(秒)</td> <td>クリック操作 5</td> </tr> </table> </td> </tr> </table> </td> </tr> </table></td></tr></table>	<input checked="" type="checkbox"/>		操作 Url リトライ時間(秒)	URL入力操作 https://192.168.4.134/Account/Login? ReturnUrl=%2F 5	ユーザーID入力操作	<table border="1"> <tr> <td><input checked="" type="checkbox"/></td> <td></td> <td>操作 自動入力設定値 編集許可 リトライ時間(秒)</td> <td>ユーザーID入力操作 ユーザーID False 5</td> </tr> <tr> <td>パスワード入力操作</td> <td> <table border="1"> <tr> <td><input checked="" type="checkbox"/></td> <td></td> <td>操作 自動入力設定値 編集許可 リトライ時間(秒)</td> <td>パスワード入力操作 パスワード False 5</td> </tr> <tr> <td>クリック操作</td> <td> <table border="1"> <tr> <td><input checked="" type="checkbox"/></td> <td></td> <td>操作 リトライ時間(秒)</td> <td>クリック操作 5</td> </tr> </table> </td> </tr> </table> </td> </tr> </table>	<input checked="" type="checkbox"/>		操作 自動入力設定値 編集許可 リトライ時間(秒)	ユーザーID入力操作 ユーザーID False 5	パスワード入力操作	<table border="1"> <tr> <td><input checked="" type="checkbox"/></td> <td></td> <td>操作 自動入力設定値 編集許可 リトライ時間(秒)</td> <td>パスワード入力操作 パスワード False 5</td> </tr> <tr> <td>クリック操作</td> <td> <table border="1"> <tr> <td><input checked="" type="checkbox"/></td> <td></td> <td>操作 リトライ時間(秒)</td> <td>クリック操作 5</td> </tr> </table> </td> </tr> </table>	<input checked="" type="checkbox"/>		操作 自動入力設定値 編集許可 リトライ時間(秒)	パスワード入力操作 パスワード False 5	クリック操作	<table border="1"> <tr> <td><input checked="" type="checkbox"/></td> <td></td> <td>操作 リトライ時間(秒)</td> <td>クリック操作 5</td> </tr> </table>	<input checked="" type="checkbox"/>		操作 リトライ時間(秒)	クリック操作 5						
<input checked="" type="checkbox"/>		操作 Url リトライ時間(秒)	URL入力操作 https://192.168.4.134/Account/Login? ReturnUrl=%2F 5																										
ユーザーID入力操作	<table border="1"> <tr> <td><input checked="" type="checkbox"/></td> <td></td> <td>操作 自動入力設定値 編集許可 リトライ時間(秒)</td> <td>ユーザーID入力操作 ユーザーID False 5</td> </tr> <tr> <td>パスワード入力操作</td> <td> <table border="1"> <tr> <td><input checked="" type="checkbox"/></td> <td></td> <td>操作 自動入力設定値 編集許可 リトライ時間(秒)</td> <td>パスワード入力操作 パスワード False 5</td> </tr> <tr> <td>クリック操作</td> <td> <table border="1"> <tr> <td><input checked="" type="checkbox"/></td> <td></td> <td>操作 リトライ時間(秒)</td> <td>クリック操作 5</td> </tr> </table> </td> </tr> </table> </td> </tr> </table>	<input checked="" type="checkbox"/>		操作 自動入力設定値 編集許可 リトライ時間(秒)	ユーザーID入力操作 ユーザーID False 5	パスワード入力操作	<table border="1"> <tr> <td><input checked="" type="checkbox"/></td> <td></td> <td>操作 自動入力設定値 編集許可 リトライ時間(秒)</td> <td>パスワード入力操作 パスワード False 5</td> </tr> <tr> <td>クリック操作</td> <td> <table border="1"> <tr> <td><input checked="" type="checkbox"/></td> <td></td> <td>操作 リトライ時間(秒)</td> <td>クリック操作 5</td> </tr> </table> </td> </tr> </table>	<input checked="" type="checkbox"/>		操作 自動入力設定値 編集許可 リトライ時間(秒)	パスワード入力操作 パスワード False 5	クリック操作	<table border="1"> <tr> <td><input checked="" type="checkbox"/></td> <td></td> <td>操作 リトライ時間(秒)</td> <td>クリック操作 5</td> </tr> </table>	<input checked="" type="checkbox"/>		操作 リトライ時間(秒)	クリック操作 5												
<input checked="" type="checkbox"/>		操作 自動入力設定値 編集許可 リトライ時間(秒)	ユーザーID入力操作 ユーザーID False 5																										
パスワード入力操作	<table border="1"> <tr> <td><input checked="" type="checkbox"/></td> <td></td> <td>操作 自動入力設定値 編集許可 リトライ時間(秒)</td> <td>パスワード入力操作 パスワード False 5</td> </tr> <tr> <td>クリック操作</td> <td> <table border="1"> <tr> <td><input checked="" type="checkbox"/></td> <td></td> <td>操作 リトライ時間(秒)</td> <td>クリック操作 5</td> </tr> </table> </td> </tr> </table>	<input checked="" type="checkbox"/>		操作 自動入力設定値 編集許可 リトライ時間(秒)	パスワード入力操作 パスワード False 5	クリック操作	<table border="1"> <tr> <td><input checked="" type="checkbox"/></td> <td></td> <td>操作 リトライ時間(秒)</td> <td>クリック操作 5</td> </tr> </table>	<input checked="" type="checkbox"/>		操作 リトライ時間(秒)	クリック操作 5																		
<input checked="" type="checkbox"/>		操作 自動入力設定値 編集許可 リトライ時間(秒)	パスワード入力操作 パスワード False 5																										
クリック操作	<table border="1"> <tr> <td><input checked="" type="checkbox"/></td> <td></td> <td>操作 リトライ時間(秒)</td> <td>クリック操作 5</td> </tr> </table>	<input checked="" type="checkbox"/>		操作 リトライ時間(秒)	クリック操作 5																								
<input checked="" type="checkbox"/>		操作 リトライ時間(秒)	クリック操作 5																										

【NEXT マネージャー 前提設定】

NEXT ユーザーID「User1」の自動認証設定名「サンプル Edge Web フォーム」が有効に設定されている必要があります。



NEXT ユーザーID「User1」の自動入力設定の「ユーザーID」が「User1」、「パスワード」が「password」に設定されている必要があります。



【再生手順】

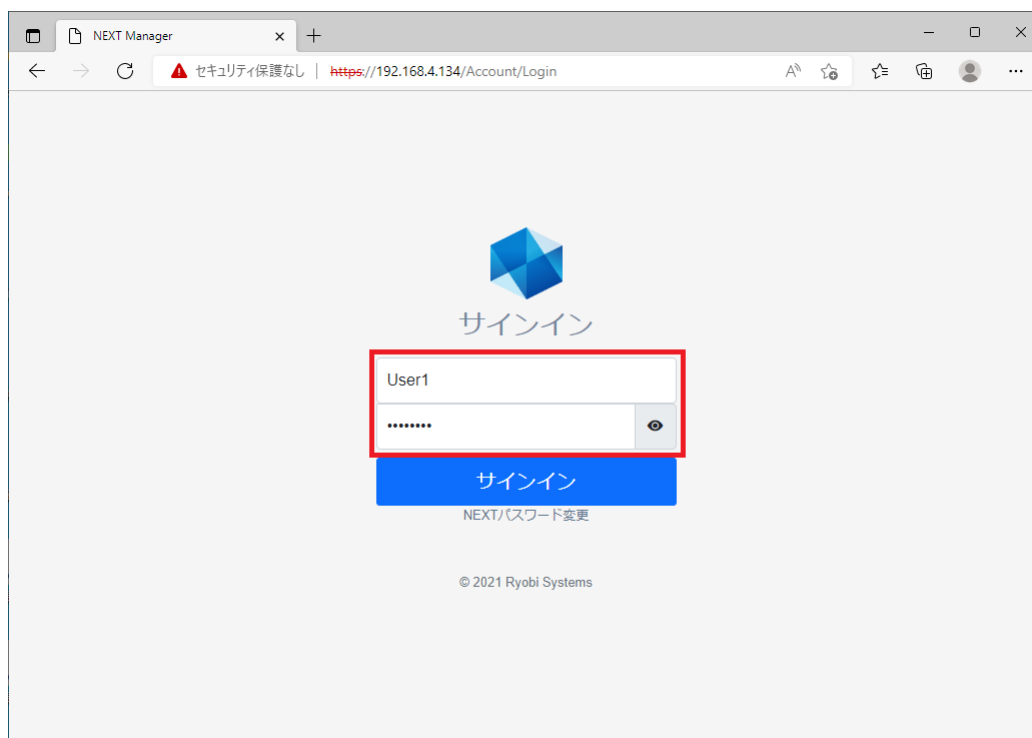
1. ICカード認証または顔認証またはNEXT 緊急パスワード認証で、Windowsへサインインします。
2. デスクトップショートカットの「NEXT 自動認証プレイヤー」をダブルクリックして、NEXT 自動認証プレイヤーを起動します。
3. メニューボタンエリアの[再生]をクリックします。



4. 設定名「サンプル Edge Web フォーム」の[再生]ボタンをクリックします。



5. 自動で Edge ブラウザ アプリケーションが開き、NEXT マネージャーが表示されます。
6. 「NEXT ユーザーID」と「NEXT パスワード」が自動で入力されます。



7. [サインイン]ボタンが自動でクリックされ、NEXT マネージャーに自動でサインインされます。

Edge Web フォームの再生例 利用者による自動入力設定での再生

ここでは、「ユーザーの編集を許可する」が ON に設定されており、利用者が「NEXT ユーザーID」、「NEXT パスワード」の設定、および入力を行って、認証を行う例を説明します。

Info 「ユーザーの編集を許可する」については、「7.6.3. ユーザー入力値の編集許可」を参照してください。

下記に自動認証設定を再生する流れを例示します。

- ・自動で Edge ブラウザが起動する
- ・自動で NEXT マネージャーのログイン画面を表示する
- ・「ユーザーID 入力画面」を表示し、ユーザーが「ユーザーID」を入力する
- ・「パスワード入力画面」を表示し、ユーザーが「パスワード」を入力する
- ・自動で「サインイン」ボタンをクリックし、サインインする
- ・ユーザーが入力した「ユーザーID」、「パスワード」を保存することで、次回以降の再生時に利用できるようにする

※「NEXT 自動認証プレイヤー 前提設定」で、各操作コンテンツの「ユーザー入力値」を未設定(設定値が空)としているため、初回のみ「ユーザーID」と「パスワード」はユーザーによる入力が必要となる例です。

【NEXT 自動認証クリエイター 前提設定】

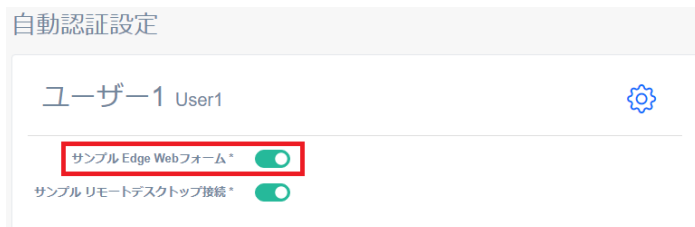
NEXT 自動認証クリエイターで下記の自動認証設定が作成されている必要があります。

※「ユーザーID 入力操作」と「パスワード入力操作」の「編集許可」が True に設定されている必要があります。

操作	プロ
Edgeブラウザの実行	操作 実行ファイル Edgeブラウザアプリケーション 引数 リトライ時間(秒) 5
リモートデスクトップの実行	
入力操作	操作 Url https://192.168.4.134/Account/Login? ReturnUrl=%2F リトライ時間(秒) 5
パスワード入力操作	操作 自動入力設定値 ユーザーID入力操作 編集許可 True リトライ時間(秒) 5
キー送信操作	操作 自動入力設定値 パスワード入力操作 編集許可 True リトライ時間(秒) 5
URL入力操作	操作 リトライ時間(秒) 5
ユーザーID入力操作	操作 リトライ時間(秒) 5
ハイパーリンク操作	
クリック操作	操作 リトライ時間(秒) 5

【NEXT マネージャー 前提設定】

NEXT ユーザーID「User1」の自動認証設定名「サンプル Edge Web フォーム」が有効に設定されている必要があります。



【NEXT 自動認証プレイヤー 前提設定】

No	条件	参考画像
1	<p>「サンプル Edge Web フォーム」の自動認証詳細画面で、操作コンテンツ「ユーザーID入力操作」の[操作編集]ボタンをクリックして、「ユーザー入力値」が設定されていないことを確認してください。</p> <p>※「ユーザー入力値」に値が設定されている場合は、再生時にユーザーID入力画面は表示されず、ユーザー名は自動で入力されます。</p>	
2	<p>「サンプル Edge Web フォーム」の自動認証詳細画面で、操作コンテンツ「パスワード入力操作」の[操作編集]ボタンをクリックして、「ユーザー入力値」が設定されていないことを確認してください。</p> <p>※「ユーザー入力値」に値が設定されている場合は、再生時にパスワード入力画面は表示されず、パスワードは自動で入力されます。</p>	

【再生手順】

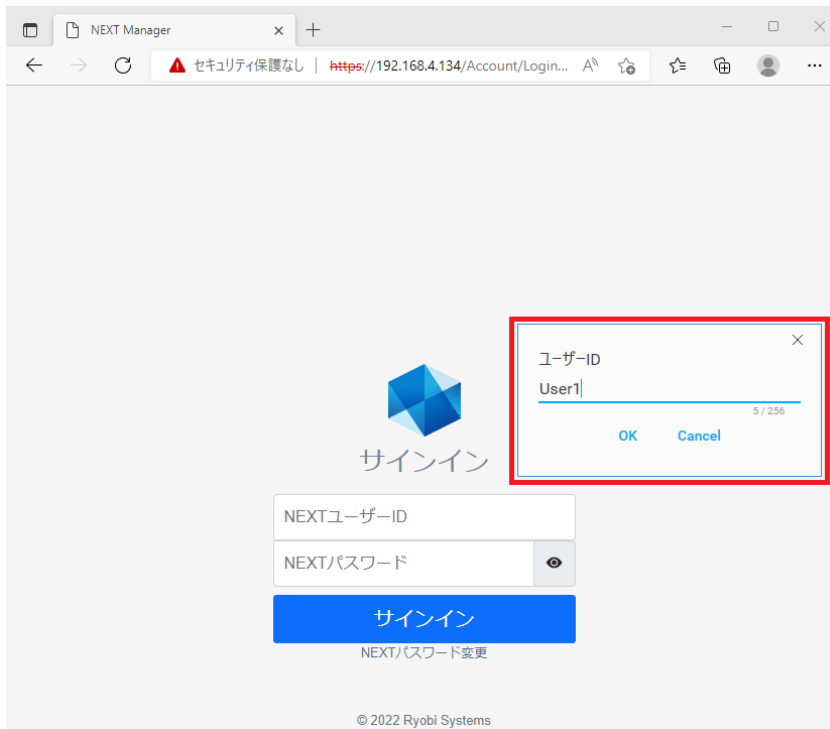
1. ICカード認証または顔認証またはNEXT 緊急パスワード認証で、Windowsへサインインします。
2. デスクトップショートカットの「NEXT 自動認証プレイヤー」をダブルクリックして、NEXT 自動認証プレイヤーを起動します。
3. メニューボタンエリアの[再生]をクリックします。



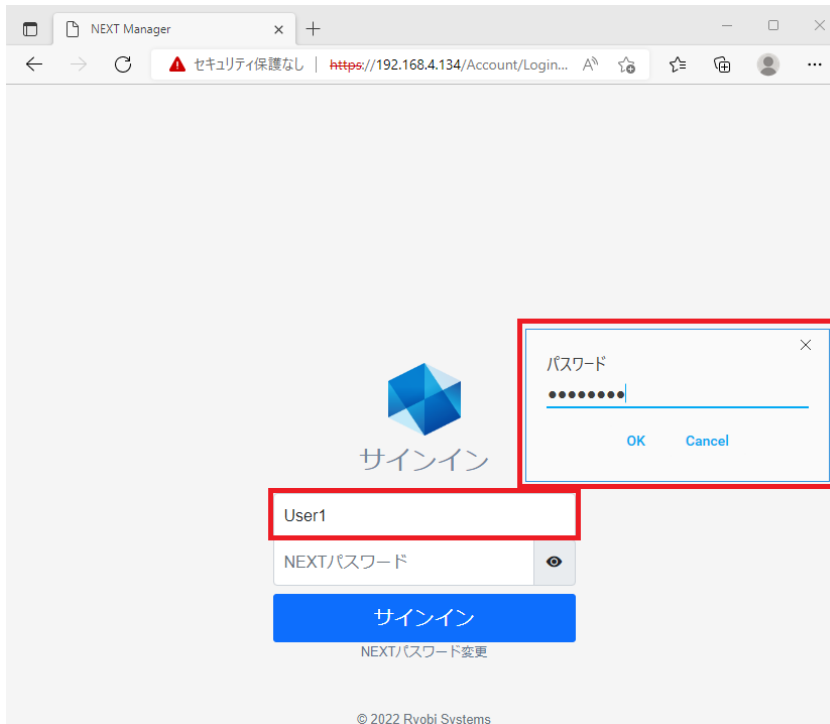
4. 設定名「サンプル Edge Web フォーム」の[再生]ボタンをクリックします。



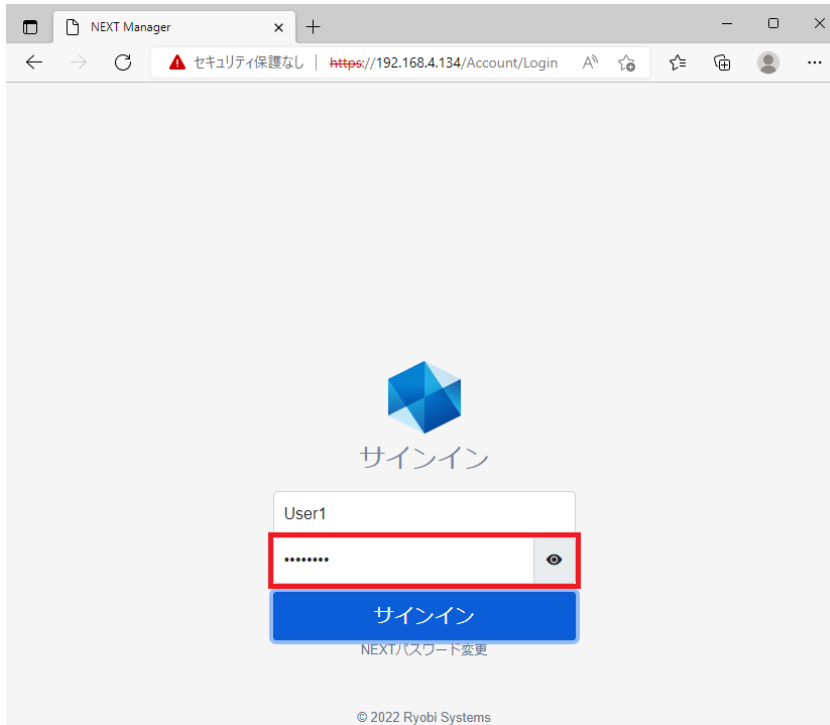
5. 自動で Edge ブラウザ アプリケーションが開き、NEXT マネージャーが表示されます。
6. ユーザーID 入力画面が表示されるので、「ユーザーID」を入力して、[OK]ボタンをクリックください。



7. Edge ブラウザ上の「NEXT ユーザーID」に手順 6 で入力したユーザーIDが自動入力されます。続けてパスワード入力画面が表示されるので、「パスワード」を入力して、[OK]ボタンをクリックください。（入力したパスワードは伏字表示となります）



8. Edge ブラウザ上の「NEXT パスワード」に手順 7 で入力したパスワードが自動入力されます。



9. [サインイン]ボタンが自動でクリックされ、NEXT マネージャーに自動でサインインされます。

10. サーバー同期を実行してください。

Info 自動認証を一度再生させると、入力した「ユーザーID」、および「パスワード」が NEXT 自動認証プレイヤーに保存され、「サーバー同期」を実行することにより NEXT サーバーへ情報が送信され、同期されます。
これにより、次回以降の再生時は、手順 6、手順 7 で行った入力作業が省略され、[再生] ボタンをクリックするだけで NEXT マネージャーに自動でサインインされます。
サーバー同期については、「7.7. サーバー同期」を参照してください。

リモートデスクトップ接続の再生例 管理者による設定の再生

ここでは、利用者がリモートデスクトップ接続に使用する「パスワード」の設定、および入力を行わず、管理者が事前に設定した自動入力設定値を自動入力してリモートデスクトップへの接続を行う例を説明します。

下記に自動認証設定を再生する流れを例示します。

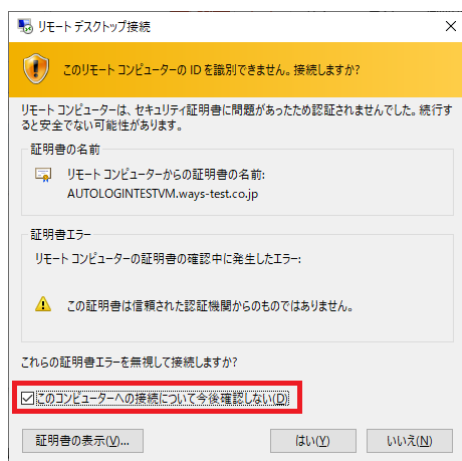
- ・自動でリモートデスクトップ接続のアプリケーションを起動する
- ・資格認証ダイアログが表示される
- ・管理者が設定したパスワード「password」が自動入力される
- ・自動で「OK」ボタンをクリックし、接続する

【リモートデスクトップ接続のアプリケーション 前提設定】

自動認証で接続するコンピューターに対して、一度リモートデスクトップ接続のアプリケーションで接続しておく必要があります。

1. [スタートメニュー]-[リモートデスクトップ接続]をクリックして、リモートデスクトップ接続のアプリケーションを起動してください。
2. [コンピューター]に自動認証で接続するコンピューター名を入力して、[接続]ボタンをクリックしてください。
3. コンピューターにログオンが可能な[ユーザー名]と[パスワード]を入力して、[OK]ボタンをクリックしてください。
4. リモートデスクトップ接続時に表示される「セキュリティ証明書」を表示させない設定しておく必要がありますので、このコンピューターへの接続について今後確認しない」にチェックを付けて[はい]ボタンをクリックしてください。

※セキュリティ証明書が表示されない場合は、手順 4 は省略してください。



Info リモートデスクトップに使用する Windows 資格情報が登録済みである場合は、Windows 資格情報を削除する必要があります。Windows 資格情報を削除する手順については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。

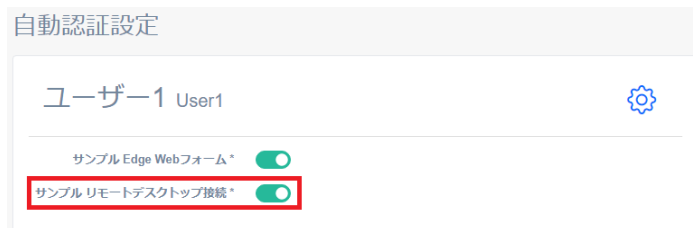
【NEXT 自動認証クリエイター 前提設定】

NEXT 自動認証クリエイターで下記の自動認証設定が作成されている必要があります。

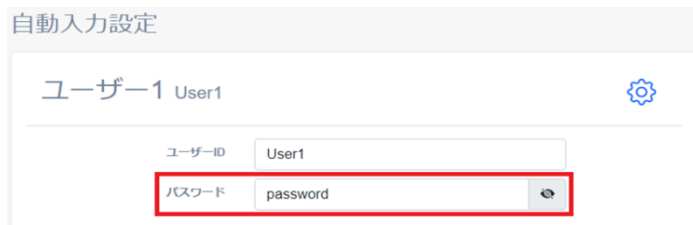


【NEXT マネージャー 前提設定】

NEXT ユーザーID「User1」の自動認証設定名「サンプル リモートデスクトップ接続」が有効に設定されている必要があります。



NEXT ユーザーID「User1」の自動入力設定の「パスワード」が「password」に設定されている必要があります。



【再生手順】

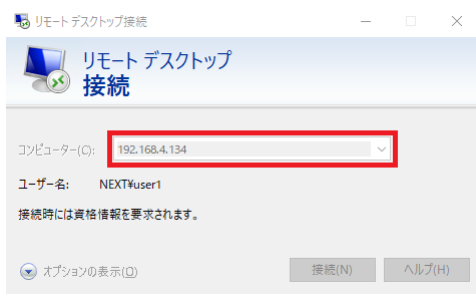
1. ICカード認証または顔認証またはNEXT 緊急パスワード認証で、Windowsへサインインします。
2. デスクトップショートカットの「NEXT 自動認証プレイヤー」をダブルクリックして、NEXT 自動認証プレイヤーを起動します。
3. メニューボタンエリアの[再生]をクリックします。



4. 設定名「サンプル リモートデスクトップ接続」の[再生]ボタンをクリックします。

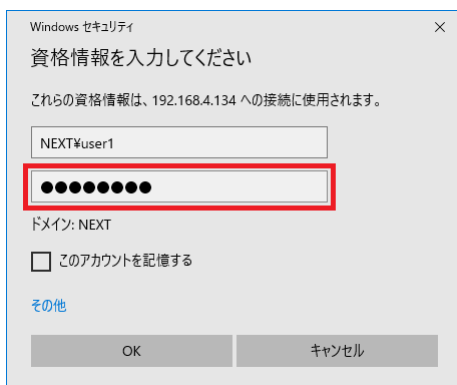


5. 自動でリモートデスクトップ接続 アプリケーションが開きます。



Info ログインするユーザー名は、Windows 資格情報に登録されている情報が使用されます。

6. 資格認証ダイアログが表示され、「パスワード」が自動で入力されます。



7. [OK]ボタンが自動でクリックされ、リモートデスクトップに自動で接続されます。

リモートデスクトップ接続の再生例 利用者による自動入力設定での再生

ここでは、「ユーザーの編集を許可する」が ON に設定されており、利用者が「パスワード」の設定、および入力を行ってリモートデスクトップへの接続を行う例を説明します。

Info 「ユーザーの編集を許可する」については、「7.6.3. ユーザー入力値の編集許可」を参照してください。

下記に自動認証設定を再生する流れを例示します。

- ・自動でリモートデスクトップ接続のアプリケーションを起動する
- ・資格認証ダイアログが表示される
- ・「パスワード入力画面」を表示し、ユーザーが「パスワード」を入力する
- ・自動で「OK」ボタンをクリックし、接続する
- ・ユーザーが入力した「パスワード」を保存することで、次回以降の再生時に利用できるようにする

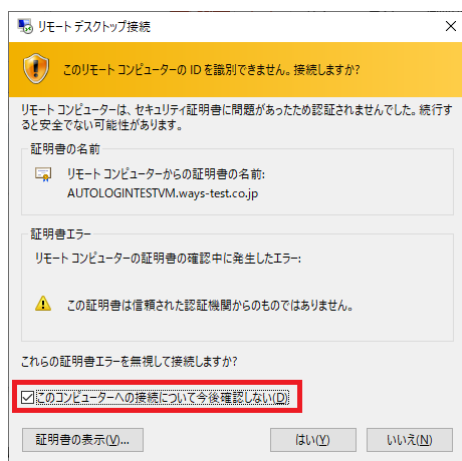
※「NEXT 自動認証プレイヤー 前提設定」で、操作コンテンツ「パスワード入力操作」の「ユーザー入力値」を未設定(設定値が空)としているため、初回のみ「パスワード」はユーザーによる入力が必要となる例です。

【リモートデスクトップ接続のアプリケーション 前提設定】

自動認証で接続するコンピューターに対して、一度リモートデスクトップ接続のアプリケーションで接続をしておく必要があります。

1. [スタートメニュー]-[リモートデスクトップ接続]をクリックして、リモートデスクトップ接続のアプリケーションを起動してください。
2. [コンピューター]に自動認証で接続するコンピューター名を入力して、[接続]ボタンをクリックしてください。
3. コンピューターにログオンが可能な[ユーザー名]と[パスワード]を入力して、[OK]ボタンをクリックしてください。
4. リモートデスクトップ接続時に表示される「セキュリティ証明書」を表示させない設定しておく必要がありますので、このコンピューターへの接続について今後確認しない」にチェックを付けて[はい]ボタンをクリックしてください。

※セキュリティ証明書が表示されない場合は、手順 4 は省略してください。



Info リモートデスクトップに使用する Windows 資格情報が登録済みである場合は、Windows 資格情報を削除する必要があります。Windows 資格情報を削除する手順については、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。

【NEXT 自動認証クリエイター 前提設定】

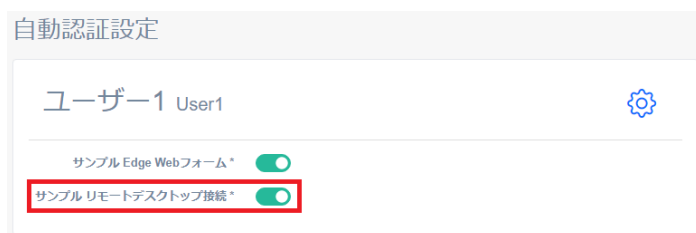
NEXT 自動認証クリエイターで下記の自動認証設定が作成されている必要があります。

※「パスワード入力操作」の「編集許可」が True に設定されている必要があります。



【NEXT マネージャー 前提設定】

NEXT ユーザーID「User1」の自動認証設定名「サンプル リモートデスクトップ接続」が有効に設定されている必要があります。



【NEXT 自動認証プレイヤー 前提設定】

No	条件	参考画像
1	<p>「サンプル リモートデスクトップ接続」の自動認証詳細画面で、操作コンテンツ「パスワード入力操作」の[操作編集]ボタンをクリックして、「ユーザー入力値」が設定されていないことを確認してください。</p> <p>※「ユーザー入力値」に値が設定されている場合は、再生時にパスワード入力画面は表示されず、パスワードは自動で入力されます。</p>	

【再生手順】

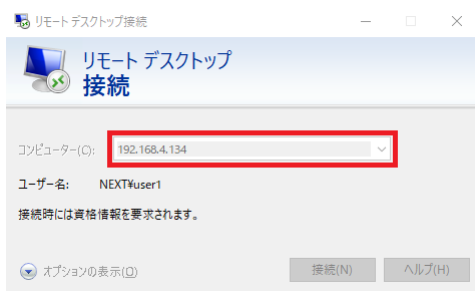
1. ICカード認証または顔認証またはNEXT 緊急パスワード認証で、Windowsへサインインします。
2. デスクトップショートカットの「NEXT 自動認証プレイヤー」をダブルクリックして、NEXT 自動認証プレイヤーを起動します。
3. メニューボタンエリアの[再生]をクリックします。



4. 設定名「サンプル リモートデスクトップ接続」の[再生]ボタンをクリックします。

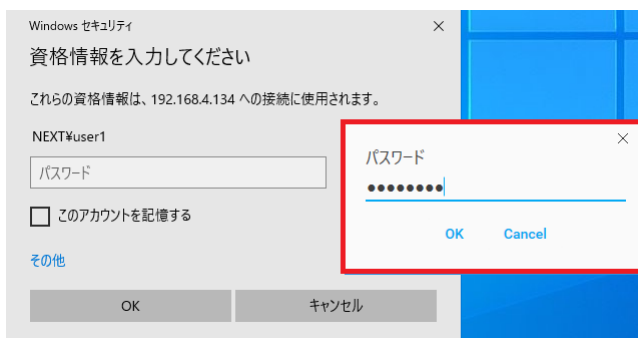


5. 自動でリモートデスクトップ接続 アプリケーションが開きます。



Info ログインするユーザー名は、Windows 資格情報に登録されている情報が使用されます。

6. 資格認証ダイアログが表示された後、パスワード入力画面が表示されるので、「パスワード」を入力して、[OK]ボタンをクリックください。（入力したパスワードは伏字表示となります）



7. 資格認証ダイアログ内のパスワードに入力した[パスワード]が自動入力され、自動でリモートデスクトップに接続されます。

8. サーバー同期を実行してください。

Info 自動認証を一度再生させると、入力した「パスワード」が NEXT 自動認証プレイヤーに保存され、「サーバー同期」を実行することにより NEXT サーバーへ情報が送信され、同期されます。

これにより、次回の再生時は手順 6 で行った入力作業が省略され、[再生]ボタンをクリックするだけで NEXT マネージャーに自動でサインインされます。

サーバー同期については、「7.7. サーバー同期」を参照してください。

7.5.4. 再生時のエラーメッセージ

NEXT 自動認証プレイヤーで自動認証設定の再生時に表示されるエラーメッセージは下記のとおりです

出力メッセージ	対処方法	操作タイプ
入力要素が見つかりません:%S	<p>操作する対象が見つかりませんでした。</p> <p>NEXT 自動認証クリエイターで作成された自動認証設定の操作情報に誤りがある可能性があります。 NEXT 自動認証クリエイターから操作情報を再設定してください。</p> <p>画面遷移やロードに時間がかかっている可能性があります。 NEXT 自動認証クリエイターで「リトライ時間(秒)」を長めに調整してください</p> <p>NEXT 自動認証クリエイターについては、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。</p> <p>凡例： %S：コントロール要素情報エリアの AutomationId</p>	すべて
フォーカスセットできません	<p>操作する対象へのフォーカスセットに失敗しました。</p> <p>NEXT 自動認証クリエイターで作成された自動認証設定の操作情報に誤りがある可能性があります。 NEXT 自動認証クリエイターで操作情報を再設定してください。 NEXT 自動認証クリエイターについては、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。</p>	キー送信操作
操作の実行に失敗しました	<p>自動操作の実行に失敗しました。</p> <p>利用者の PC に何らかの問題が発生している可能性があります。 一度 PC を再起動して、再度 NEXT 自動認証プレイヤーで自動認証設定を再生してください。</p>	すべて

7.6. 利用者による入力設定の編集

7.6.1. ユーザー設定画面

自動認証時に入力される情報は、NEXT 自動認証プレイヤーのユーザー設定画面で編集することができます。

ユーザー設定画面は、自動認証詳細画面で[操作編集]ボタンをクリックすると表示されます。

ユーザー設定画面では、操作情報の詳細画面が表示され、自動入力設定値を編集することができます。

以下にユーザー設定画面のデザイン、および各項目について説明します。

No	項目	説明
①	戻る	自動認証詳細画面に戻ります。 ※コンテンツエリアの内容に変更があった場合は保存せずに戻ります。 その場合、確認ダイアログは表示されません。
②	保存	コンテンツエリアの変更内容を保存して、自動認証詳細画面に戻ります。
③	コンテンツエリア	各コンテンツの設定内容が表示されるエリアです。 コンテンツの設定値に下線が表示されている項目は、編集が可能です。 ※コンテンツエリアの内容は、操作ごとに異なります。 ※「パスワード入力操作」時の「ユーザー入力値」は伏字表示となります。
④	コントロール要素 情報エリア	コントロール要素の情報が表示されます。

自動認証の再生時に入力する「ユーザーID」や「パスワード」は、自動認証プレイヤーの各操作コンテンツに設定されている「ユーザー入力値」が自動で入力されます。

NEXT自動認証

← 戻る | 保存

操作	ユーザーID入力操作
ユーザー個別設定値	使用しない
自動入力する値	
リトライ時間(秒)	5
ユーザー入力値	user1

7.6.2. ユーザー入力値の設定手順

「ユーザー入力値」の設定手順について説明します。

1. NEXT 自動認証プレイヤーを起動します。
2. プレイヤーメニュー画面で、[再生]をクリックします。
3. プレイヤーメイン画面で、[編集]ボタンをクリックします。
4. 自動認証詳細画面で、「ユーザー入力値」を変更する操作の[操作編集]ボタンをクリックします。

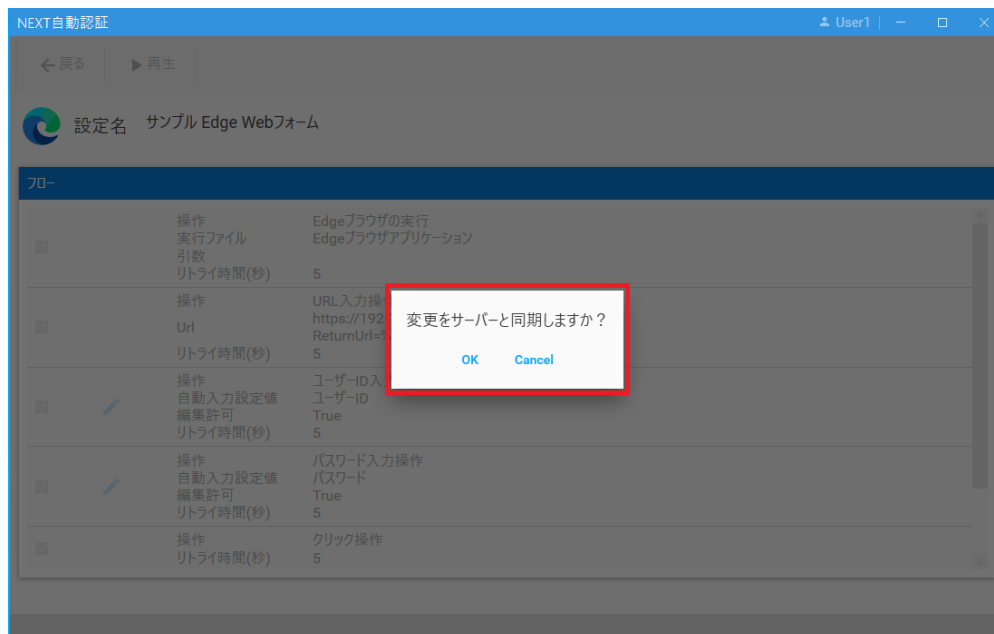


Info 自動認証設定の「ユーザーの編集を許可する」が OFF に設定されている場合は、自動認証詳細画面の[操作編集]ボタンが表示されません。
詳細は、「7.6.3. ユーザー入力値の編集許可」を参照してください。

5. ユーザー設定画面で、「ユーザー入力値」の値を変更し、[保存]ボタンをクリックします。保存すると自動認証詳細画面に戻ります。



6. [戻る]ボタンをクリックすると、「変更をサーバーと同期しますか？」の確認ダイアログが表示されます。



- [OK]ボタンを押下：サーバー同期メニュー画面が表示されますので、サーバー同期を行ってください。
サーバー同期については、「7.7. サーバー同期」を参照してください。
[Cancel]ボタンを押下：プレイヤーメイン画面に戻ります。

Info NEXT 自動認証プレイヤーの次回起動時、変更した「ユーザー入力値」を使用する場合は、「サーバー同期」を行う必要があります。

7.6.3. ユーザー入力値の編集許可

自動認証設定の操作コンテンツ「ユーザーID入力操作」や「パスワード入力操作」の「ユーザーの編集を許可する」のチェック状態によって、NEXT 自動認証プレイヤーにおける各操作コンテンツの編集可否が変わります。

「ユーザーの編集を許可する」が ON の場合は、自動認証詳細画面で「ユーザー入力値」の編集が可能となりますが、OFF の場合は「ユーザー入力値」の編集が不可となり、NEXT マネージャーの自動入力設定値が使用されます。

下図は「ユーザーの編集を許可する」が ON/OFF のそれぞれの場合の自動詳細画面の例です。

【自動認証設定内容】

- ・操作コンテンツ「ユーザーID入力操作」の「ユーザーの編集を許可する」が OFF
- ・操作コンテンツ「パスワード入力操作」の「ユーザーの編集を許可する」が ON

【NEXT 自動認証プレイヤーの自動詳細画面】



7.7. サーバー同期

プレイヤーメニュー画面で[サーバー同期(再生設定)]をクリックすると、サーバー同期メニュー画面に遷移します。

サーバー同期メニュー画面では、NEXT サーバーとデータを同期することができます。

以下にサーバー同期メニュー画面のデザイン、および各項目について説明します。

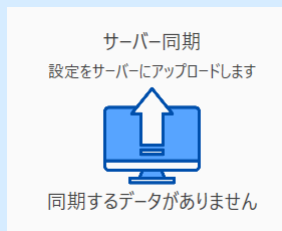


No	項目	説明
①	実行	<p>サーバー同期を実行します。</p> <p>[実行]ボタンをクリックすると、「同期しますか？」の確認ダイアログが表示されます。</p> <p>[OK]ボタン押下時：NEXT 自動認証プレイヤーで変更のあった設定値をNEXT サーバーへ送信し、同期されます。</p> <p>[Cancel]ボタン押下時：確認ダイアログを閉じて、サーバー同期は実行しません。</p>

サーバー同期を実行すると、下記のように画面が表示されます。



Info NEXT 自動認証プレイヤーで設定値に変更がない場合は、下記のように表示され、サーバー同期は実行できません。



サーバー同期の実行時に表示されるエラーメッセージは以下のとおりです。

出力メッセージ	対応方法
サーバーに接続できません	オフライン状態、または NEXT サーバーに接続できない状態です。NEXT サーバーに接続できる環境か確認して、再度サーバー同期を実行してください。
ユーザーが見つかりません:{NEXT ユーザーID}	サーバー同期を実行した NEXT ユーザーIDが NEXT サーバーに登録されていません。NEXT サーバーに該当の NEXT ユーザーが登録済みか確認して、再度 NEXT クライアントへサインインし直してください。
サーバーエラーが発生しました	NEXT クライアント、または NEXT 自動認証プレイヤーに何らかの障害が発生しています。マシンを再起動して、再度 NEXT 自動認証プレイヤーを実行してください。

7.8. 製品情報

プレイヤーメニュー画面で[製品情報]をクリックすると、製品情報メニュー画面に遷移します。製品情報メニュー画面では、NEXT 自動認証プレイヤーのバージョン情報が表示されます。

以下に製品情報メニュー画面のデザイン、および各項目について説明します。



No	項目	説明
①	製品情報	インストールされている NEXT 自動認証プレイヤーのバージョンが表示されます。

Info NEXT 自動認証プレイヤーが正常にインストールされていない場合は、下記のように表示されます。



7.9. エラーメッセージ

NEXT 自動認証プレイヤーの起動時に表示されるエラーメッセージは下記のとおりです。

出力メッセージ	対応方法
ログインユーザーがありません	NEXT ユーザー情報の取得に失敗しました。 再度 NEXT クライアントへ下記いずれかの NEXT 認証でサインインし直してください。 <ul style="list-style-type: none">・NEXT IC カード認証・NEXT 顔認証・NEXT 緊急パスワード認証
サーバーエラーが発生しました	NEXT クライアント、または NEXT 自動認証プレイヤーに何らかの障害が発生しています。 マシンを再起動して、再度 NEXT 自動認証プレイヤーを実行してください。
アプリケーションエラーが発生しました	NEXT 自動認証プレイヤーに致命的なエラーが発生しました。 マシンを再起動して、再度 NEXT 自動認証プレイヤーを実行してください。

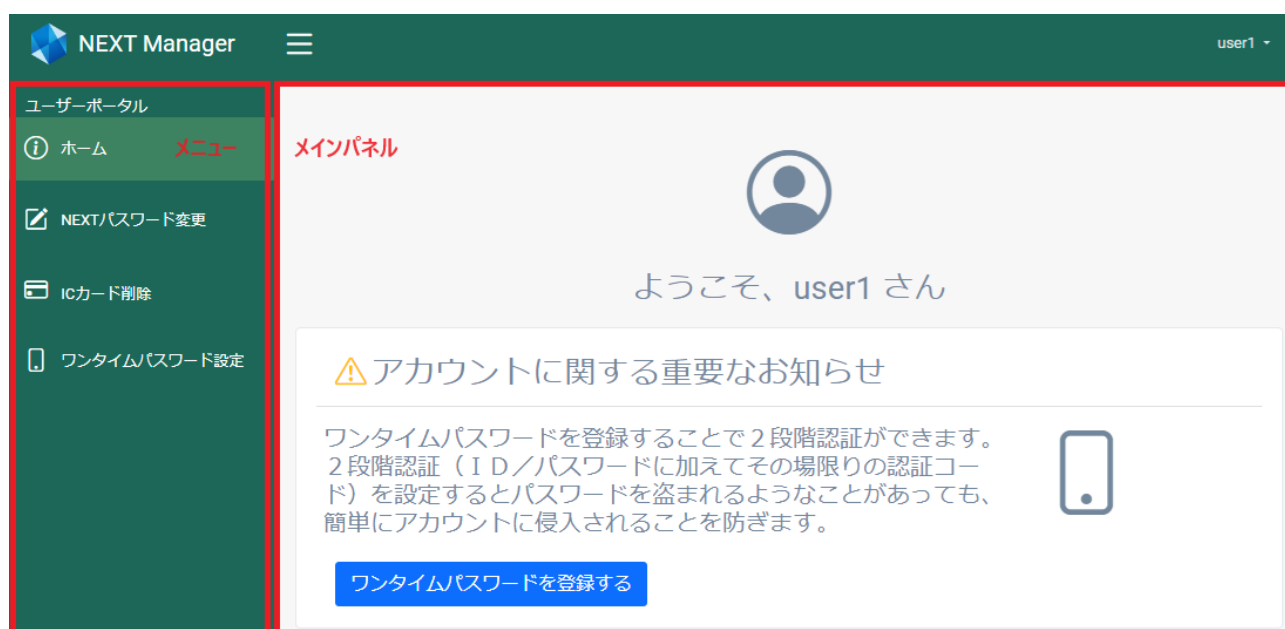
8. ユーザーポータル

ユーザーポータルとは、ユーザーが NEXT マネージャーにサインインして自身のユーザー情報の設定をするポータルサイトです。

ユーザー自身の NEXT パスワード変更や IC カードのリセット、ワンタイムパスワードを利用するためのワンタイムパスワードシークレットの発行、およびリセットが行えます。

8.1. 画面構成

ユーザーポータルは、左側のメニューと右側のメインパネルから構成されています。各メニューをクリックすると、メインパネルに対応するページが表示されます。



メインパネルは、通知メッセージがある場合とない場合で画面が異なります。

■通知メッセージがある場合



■通知メッセージがない場合



No	項目	補足
①	NEXT ユーザー名	ユーザーポータルにサインインした NEXT ユーザー名が表示されます。
②	通知エリア	通知メッセージが表示されるエリアです。 複数の通知メッセージがある場合は全て表示されます。
③	通知メッセージ	通知するメッセージが表示されます。
④	ARCACLAVIS NEXT 製品サイト	クリックすると、ARCACLAVIS NEXT の製品サイトを別ウィンドウで開きます。
⑤	製品情報、マニュアル	クリックすると、ARCACLAVIS NEXT の製品マニュアルサイトを別ウィンドウで開きます。

8.2. サインイン

ユーザーポータルへのサインインについて説明します。

ユーザーポータルは、管理者、またはポータル利用者のみサインインできます。

Info 管理者ポータルについては、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。

8.2.1. パスワード認証でのサインイン

パスワード認証を利用して NEXT マネージャーのユーザーポータルへサインインする場合は、以下の手順で行ってください。

1. NEXT マネージャーの URL を Web ブラウザで開きます。
2. ユーザーポータルのサインイン画面が表示されます。



Info 管理者ポータルのサインイン画面が表示されている場合は、<ポータル利用者サインイン>をクリックしてください。



3. サインインするユーザーの「NEXT ユーザーID」、「NEXT パスワード」を入力し、<次へ>ボタンをクリックしてください。



The screenshot shows a login interface with a blue cube logo at the top. Below the logo is the text 'サインイン'. There are two input fields: the first contains 'user1' and the second contains '.....'. A blue button labeled '次へ' is positioned below the password field. Below the button is the text '管理者サインイン'. At the bottom, there is a copyright notice '© 2024 Ryobi Systems'.

Info ワンタイムパスワードシークレットが発行済の場合は、<次へ>ボタンをクリックすると下記画面が表示され、ワンタイムパスワードの入力が必要となります。
「8.2.2. ワンタイムパスワード認証でのサインイン」を参照してください。

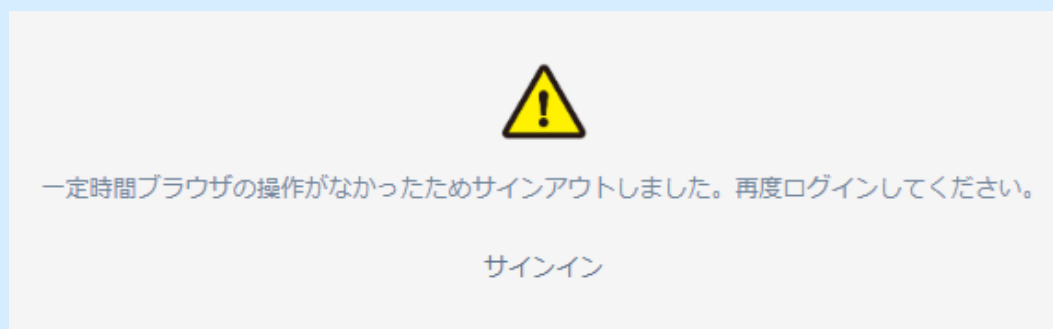


The screenshot shows a login interface with a blue cube logo at the top. Below the logo is the text 'サインイン'. There is one input field labeled 'ワンタイムパスワード'. A blue button labeled '次へ' is positioned below the input field. Below the button are two links: '別の方法を試す' and '他のアカウントでサインインする'. At the bottom, there is a copyright notice '© 2024 Ryobi Systems'.

4. ユーザーポータルのダッシュボードが表示されます。



Info ユーザーポータルにサインイン後、一定時間ブラウザの操作がないと下記画面が表示され、自動的にサインアウトされます。再度サインインし直してください。



8.2.2. ワンタイムパスワード認証でのサインイン

ワンタイムパスワード認証を利用して NEXT マネージャーのユーザーポータルへサインインする場合は、以下の手順で行ってください。

1. NEXT マネージャーの URL を Web ブラウザで開きます。
2. ユーザーポータルのサインイン画面が表示されます。



Info 管理者ポータルのサインイン画面が表示されている場合は、<ポータル利用者サインイン>をクリックしてください。



- サインインするユーザーの「NEXT ユーザーID」、「NEXT パスワード」を入力し、<次へ>ボタンをクリックしてください。



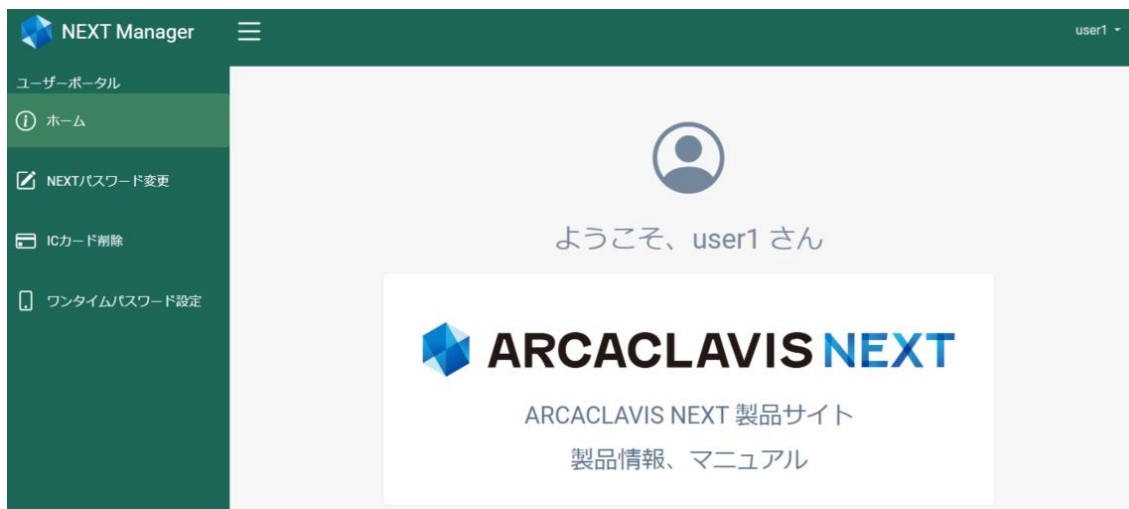
The screenshot shows a login interface with a blue geometric logo at the top. Below the logo is the text 'サインイン'. There are two input fields: the first contains 'user1' and the second contains '.....'. A blue button labeled '次へ' is positioned below the password field. Below the button are the links '管理者サインイン' and '© 2024 Ryobi Systems'.

- スマートフォンの Authenticator アプリを開き、表示されているワンタイムパスワードを入力して、<次へ>ボタンをクリックしてください。



The screenshot shows a login interface with a blue geometric logo at the top. Below the logo is the text 'サインイン'. There is one input field labeled 'ワンタイムパスワード'. A blue button labeled '次へ' is positioned below the input field. Below the button are the links '別の方法を試す' and '他のアカウントでサインインする'. At the bottom is the text '© 2024 Ryobi Systems'.

5. ユーザーポータルのダッシュボードが表示されます。



Info ユーザーポータルにサインイン後、一定時間ブラウザの操作がないと下記画面が表示され、自動的にサインアウトされます。再度サインインし直してください。



8.3. NEXT パスワード変更

1. 「8.2. サインイン」の手順に従ってNEXT マネージャーのユーザーポータルにサインインしてください。
2. メニューの「NEXT パスワード変更」をクリックしてください。



3. 「NEXT パスワード」「新しいNEXT パスワード」「確認用NEXT パスワード」を入力してください。

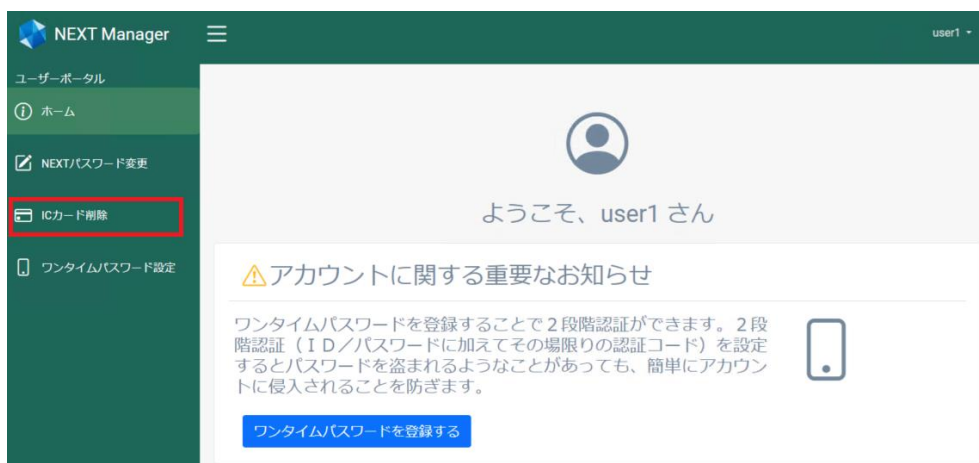


4. <登録>ボタンをクリックしてください。

8.4. ICカードの削除

NEXT ユーザーに登録されている IC カードを削除するには、以下の手順で行います。

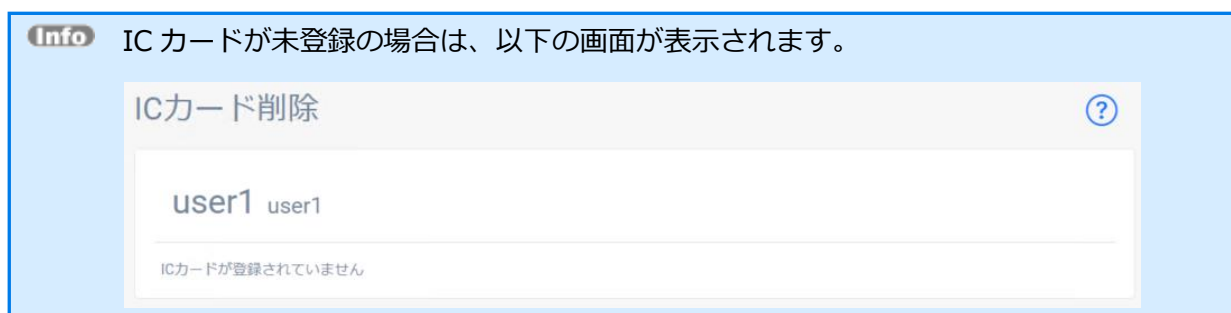
1. 「8.2. サインイン」の手順に従って NEXT マネージャーのユーザーポータルにサインインしてください。
2. メニューの「ICカード削除」をクリックしてください。



3. <削除>ボタンをクリックしてください。



Info ICカードが未登録の場合は、以下の画面が表示されます。

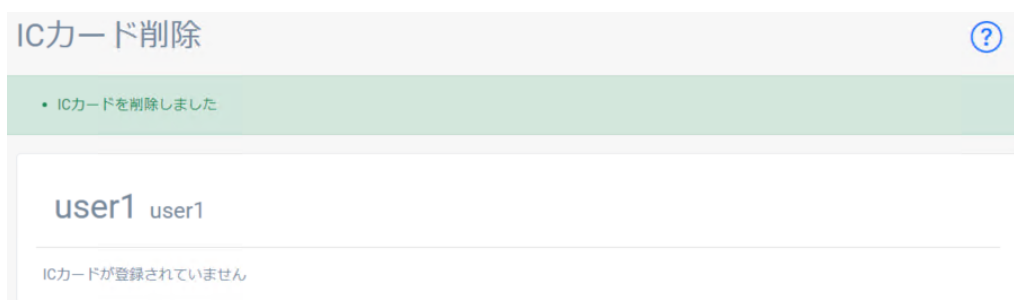


4. 「NEXT パスワード」を入力し、<削除>ボタンをクリックしてください。



A modal dialog box with a close button (X) in the top right corner. The text inside reads: "ICカードを削除します。本人確認のため、NEXTパスワードを入力してください。" Below the text is a text input field labeled "NEXTパスワード*" with a toggle eye icon to its right. At the bottom right, there are two buttons: a red button labeled "削除" and a grey button labeled "閉じる".

5. ICカードが削除されます。



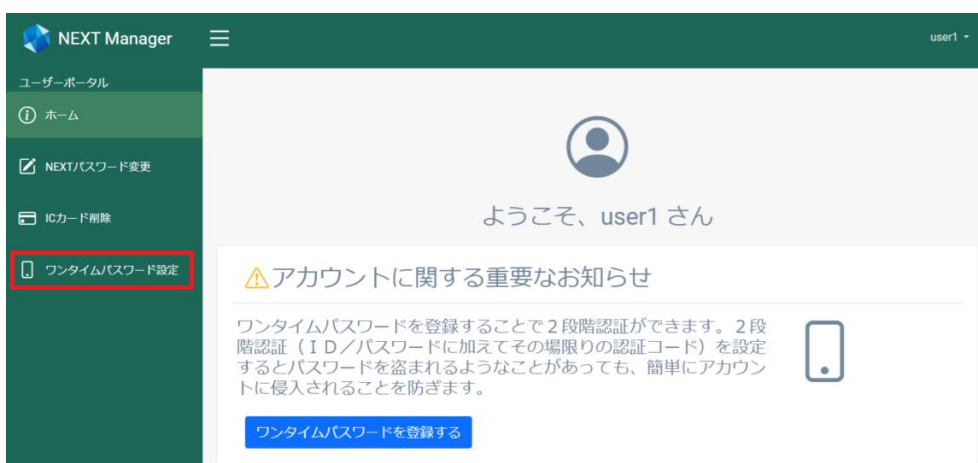
A confirmation screen titled "ICカード削除" with a help icon (?) in the top right. A green banner at the top contains the message "• ICカードを削除しました". Below this is a white box containing the text "user1 user1" and a horizontal line. At the bottom of the white box, it says "ICカードが登録されていません".

8.5. ワンタイムパスワードシークレットの発行

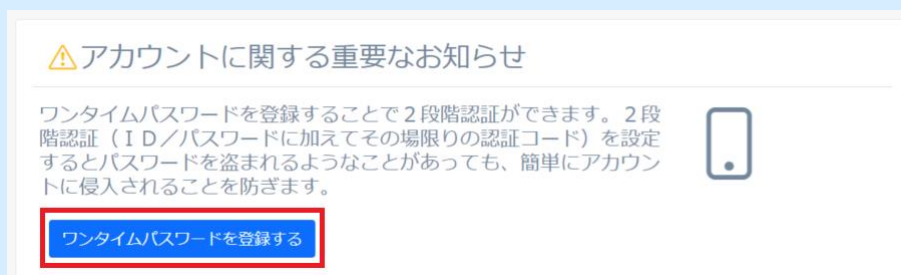
利用者のNEXT ユーザーにワンタイムパスワードを設定する場合は、以下の手順で行ってください。

Info ワンタイムパスワードを設定する場合は、あらかじめスマートフォンに Authenticator アプリがインストールされている必要があります。
詳細は、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。

1. 「8.2. サインイン」の手順に従ってNEXT マネージャーのユーザーポータルにサインインしてください。
2. メニューの「ワンタイムパスワード設定」をクリックしてください。



Info ワンタイムパスワードが未設定の場合は、メインパネルにワンタイムパスワードの有効化についての通知メッセージが表示されます。
<ワンタイムパスワードを登録する>ボタンをクリックしてもワンタイムパスワードを設定する画面が表示されます。



3. ワンタイムパスワード設定画面が表示されます。<発行>ボタンをクリックしてください。



ワンタイムパスワード設定

user1 user1

ワンタイムパスワードシークレットが登録されていません

発行

4. 「NEXT パスワード」を入力し、<次へ>ボタンをクリックしてください。



ワンタイムパスワードシークレットを発行します。
本人確認のため、NEXTパスワードを入力してください。


NEXTパスワード*

次へ 閉じる

5. ワンタイムパスワードシークレットが発行され、QRコードで表示されます。



スマートフォンのAuthenticatorでQRコードを読み込んでください。
AuthenticatorはGoogleAuthenticator,Microsoft Authenticatorが使用できます。
スマートフォンのアプリストアからインストール下さい。



次へ 閉じる

Info Authenticator アプリの使い方は、スマートフォンにインストールされている Authenticator アプリのヘルプなどを参照してください。

6. 表示されている QR コードをスマートフォンの Authenticator アプリで読み込み、NEXT ユーザーを登録してください。



Info スマートフォンの Authenticator アプリへ登録する手順については、「8.6. スマートフォンの Authenticator アプリへの登録」を参照してください。

7. <次へ>ボタンをクリックしてください。



8. スマートフォンの Authenticator アプリに表示されているワンタイムパスワードを入力して、<次へ> ボタンをクリックしてください。



A screenshot of a mobile application window titled "Authenticator". The window contains the text "Authenticatorに表示されたワンタイムパスワードを入力してください。" (Please enter the one-time password displayed in the Authenticator). Below this is a text input field labeled "ワンタイムパスワード*" (One-time password*). At the bottom of the window are three buttons: "戻る" (Back), "次へ" (Next), and "閉じる" (Close).

9. ワンタイムパスワードのリカバリーコードが表示されます。
リカバリーコードをメモした後に<閉じる>ボタンをクリック、または<リカバリーコードをダウンロードする>ボタンをクリックした後に<閉じる>ボタンをクリックしてください。
ワンタイムパスワードのリカバリーコードは、ワンタイムパスワードシークレットを発行したスマートフォンを紛失した場合に必要となります。
詳細は、「ARCACLAVIS NEXT トラブルシューティングガイド」を参照してください。



A screenshot of a dialog box with a red header "[重要]" (Important) and a close button "×". The main text reads: "リカバリーコードを保存してください。スマートフォンが故障した場合など、Authenticatorが利用できなくなった場合に、このリカバリーコードを使ってポータル画面にサインインします。この画面を閉じると再表示はできませんので、ダウンロードする、紙に書くなどして保存してください。" (Please save the recovery code. In case of a smartphone malfunction, etc., you can sign in to the portal screen using this recovery code if the Authenticator becomes unusable. Closing this screen means it cannot be displayed again, so please download it, write it on paper, etc. to save it). Below the text is a yellow box containing the recovery code "F23E 03DA 2A07 46AE". A green button "リカバリーコードをダウンロードする" (Download recovery code) is positioned below the code box. A "閉じる" (Close) button is located at the bottom right of the dialog.

10. ワンタイムパスワードシークレットが登録されます。



A screenshot of the "ワンタイムパスワード設定" (One-time password settings) screen. The title bar includes a help icon "?". A green banner at the top states "ワンタイムパスワードシークレットを発行しました" (One-time password secret has been issued). Below this, the user is identified as "user1 user1". The main text says: "ワンタイムパスワードシークレットが登録済みです。QRコードを再表示する場合、ワンタイムパスワードシークレットをリセットする必要があります。リセット後はAuthenticatorのワンタイムパスワードが使用できなくなるため、再登録が必要です。" (The one-time password secret is registered. When you need to re-display the QR code, you need to reset the one-time password secret. After resetting, the one-time password in the Authenticator will be unusable, so you need to re-register). A red "リセット" (Reset) button is located at the bottom left.

8.6. スマートフォンの Authenticator アプリへの登録

利用者がスマートフォンの Authenticator アプリにワンタイムパスワードシークレットを登録するには、以下の手順で行います。

ここでは、Google Authenticator アプリに登録する流れを例示します。

Authenticator アプリのバージョンによっては操作、画面、ボタンなどが若干異なることがあります。

予めご了承ください。

1. 「8.5. ワンタイムパスワードシークレットの発行」の手順に従ってワンタイムパスワードシークレットを発行してください。
2. スマートフォンの Google Authenticator アプリを起動してください。
3. 画面右下に表示されている<+>ボタンをクリックしてください。



4. [QR コードをスキャン]をクリックしてください。



5. 表示されている QR コードをスマートフォンの Google Authenticator アプリで読み取ってください。
6. ワンタイムパスワードシークレットを発行した NEXT ユーザーが Google Authenticator アプリに登録されます。



No	項目	補足
①	ワンタイムパスワードシークレットを発行した NEXT ユーザー名	ワンタイムパスワード設定を行った NEXT ユーザー名が表示されます。 ARCACLAVIS NEXT:[NEXT ユーザー名]
②	ワンタイムパスワード	ワンタイムパスワード設定で使用する 6 桁のワンタイムパスワードです。 ワンタイムパスワードは 30 秒ごとに自動で更新されます。
③	30 秒タイマー	ワンタイムパスワードが更新されるタイミングを示すタイマーです。 ●が全て表示されていると残り 30 秒となっていて、●が全て消えるタイミングでワンタイムパスワードが更新されます。

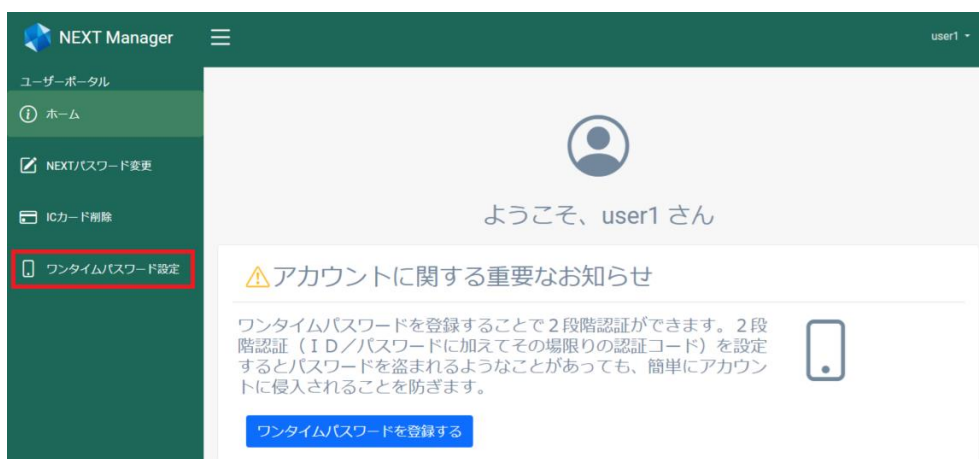
8.7. ワンタイムパスワードシークレットのリセット

ご使用のスマートフォンを変更する場合、ワンタイムパスワードシークレットをリセットし、新しいスマートフォンの Authenticator アプリで再度 NEXT ユーザーを登録する必要があります。

NEXT ユーザーに登録されているワンタイムパスワードシークレットをリセットするには、以下の手順で行います。

Info スマートフォンの紛失や破損によってワンタイムパスワードの生成ができない場合、リカバリーコードを使用してワンタイムパスワードを無効することができます。詳細は、「ARCACLAVIS NEXT トラブルシューティングガイド」を参照してください。

1. 「8.2. サインイン」の手順に従って NEXT マネージャーのユーザーポータルにサインインしてください。
2. メニューの「ワンタイムパスワード設定」をクリックしてください。



3. <リセット>ボタンをクリックしてください。

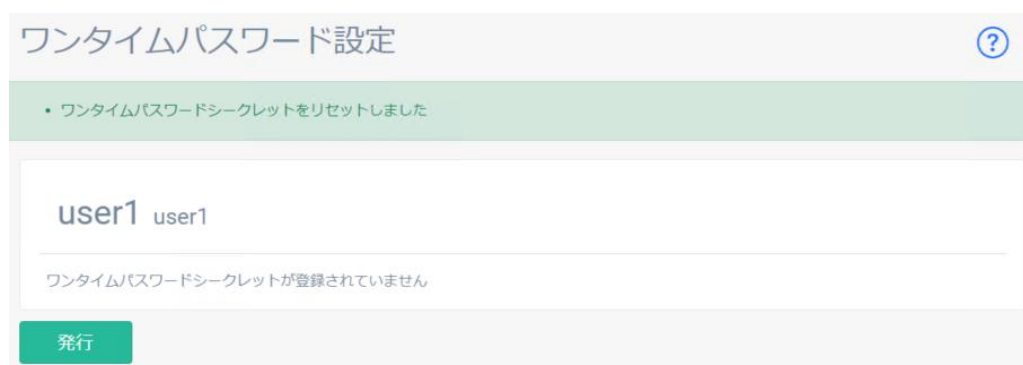


4. 「NEXT パスワード」を入力して「確認しました」にチェックを入れ、<リセット>ボタンをクリックしてください。



A modal dialog box with a red title bar containing the text 「重要」 (Important) and a close button (X). The main content area contains the text: 「ワンタイムパスワードシークレットをリセットするとAuthenticatorで使用しているワンタイムパスワードが使用できなくなります」 (Resetting the one-time password secret will make the one-time password used with Authenticator unusable). Below this text is a text input field labeled 「NEXTパスワード*」 (NEXT Password*) with a toggle eye icon to its right. At the bottom of the dialog, there is a checkbox labeled 「確認しました」 (I have confirmed) which is currently unchecked, followed by a red button labeled 「リセット」 (Reset) and a grey button labeled 「閉じる」 (Close).

5. ワンタイムパスワードシークレットがリセットされます。




A screenshot of the 'ワンタイムパスワード設定' (One-time Password Settings) page. The page title is 'ワンタイムパスワード設定' with a help icon (question mark) to its right. Below the title is a green notification bar with the text: 「ワンタイムパスワードシークレットをリセットしました」 (One-time password secret has been reset). The main content area shows the text 'user1 user1' and a message below it: 「ワンタイムパスワードシークレットが登録されていません」 (One-time password secret is not registered). At the bottom of the main content area is a green button labeled 「発行」 (Issue).

Info ワンタイムパスワードシークレットをリセットした場合は、スマートフォンの Authenticator アプリに登録した NEXT ユーザーの削除も合わせて行ってください。削除する手順については、スマートフォンにインストールされている Authenticator アプリのヘルプなどを参照してください。

8.8. エラーメッセージ

ユーザーポータルで NEXT パスワード変更、およびワンタイムパスワード設定を行う際に表示される代表的なエラーメッセージは下記のとおりです。

出力メッセージ	対応方法
確認用パスワードが一致しません	<p>入力した[新しい NEXT パスワード]と[確認用 NEXT パスワード]が一致していません。</p> <p>再度、[新しい NEXT パスワード]と[確認用 NEXT パスワード]を入力してください。</p>
パスワードポリシーに反していません。長さや使用する文字種別を確認してください。	<p>入力した[新しい NEXT パスワード]がパスワードポリシーに反しています。</p> <p>再度、[新しい NEXT パスワード]を入力してください。</p> <p>NEXT ユーザーのパスワードポリシーは「ポリシー設定」で設定されています。</p> <p>詳細は、「ARCACLAVIS NEXT 管理者ガイド」を参照してください。</p>
NEXT ユーザーID、NEXT パスワードが正しくありません	<p>入力した[NEXT パスワード]が正しくありません。</p> <p>正しい [NEXT パスワード]を入力してください。</p> <p>本エラーが発生した場合、エラー回数がカウントアップされます。エラー回数がポリシー設定の「NEXT ユーザーのロックアウトのしきい値」を超えた場合は、下図のようにエラー画面が表示され、ロックアウトされます。</p> <div style="text-align: center;">  <p>ユーザーがロックされています。管理者までご連絡ください。</p> <p>サインイン</p> </div>
同一のパスワードには変更できません	<p>前回と同じ NEXT パスワードへの変更はできません。</p> <p>[NEXT パスワード]と[新しい NEXT パスワード]は、異なるパスワードを設定してください。</p>

付録

NEXT クライアントにリモートデスクトップ接続したら

NEXT クライアントにソフトウェアがインストールされているコンピューターにリモートデスクトップ接続した場合、「IC カード認証」や「顔認証」、「ワンタイムパスワード認証」などの認証デバイスを利用した認証方式は利用できません。

「緊急パスワード認証」や「管理者パスワード認証」による認証デバイスを利用しない認証方式をご利用ください。

IC カード認証、顔認証、ワンタイムパスワード認証のサインインオプションが表示されない

ハードドライブ（HDD、SSD など）の障害などで NEXT のモジュールが読み込めない、欠損された場合など、ご利用の認証方式のサインインオプションが表示されない場合、モジュールや設定を再インストールすることで再配置する必要があります。以下の手順をご確認ください。

NEXT 緊急パスワード認証、NEXT 管理者パスワード認証が表示されている場合

1. NEXT 緊急パスワード認証または NEXT 管理者パスワード認証を利用し、Windows の管理者権限を持つユーザーでサインインします
「NEXT 緊急パスワード認証」によるサインインは、「3.8. NEXT 緊急パスワード認証でのサインイン、ロック解除」を参照してください。
「NEXT 管理者パスワード認証」によるサインインは、「3.9. NEXT 管理者パスワード認証でのサインイン、ロック解除」を参照してください。
Windows アカウントは、管理者権限を持つユーザーでサインインしてください。
2. NEXT クライアントインストーラーを再インストールしてください
NEXT クライアントのインストールは、「ARCACLAVIS NEXT セットアップガイド」を参照してください。
3. IC カード認証、顔認証、ワンタイムパスワード認証が正しく動作することを確認してください
IC カード認証の利用は「3.2.1. IC カードを利用したサインイン認証」を、顔認証の利用は「3.2.2. 顔情報を利用したサインイン認証」を、ワンタイムパスワード認証の利用は「3.2.3. スマートフォンの Authenticator アプリを利用したサインイン認証」を参照してください。

NEXT のサインインオプションはいずれも表示されず、Windows 標準資格プロバイダーが表示される場合

1. Windows 標準資格プロバイダーを利用し、Windows の管理者権限を持つユーザーでサインインします
以降は、[NEXT 緊急パスワード認証、NEXT 管理者パスワード認証が表示されている場合]の手順 2.以降と同様ですので、参照してください。

NEXT のサインインオプションはいずれも表示されず、Windows 標準資格プロバイダーも表示されない場合

1. Windows OS のセーフモードで PC を起動し、Windows の管理者権限を持つユーザーでサインインします
Windows OS のセーフモードで PC を起動する方法については、以下の URL を参照してください。

Windows 10 のセーフ モードで PC を起動する

<https://support.microsoft.com/ja-jp/help/12376/windows-10-start-your-pc-in-safe-mode>

以降は、[NEXT 緊急パスワード認証、NEXT 管理者パスワード認証が表示されている場合]の手順 2.以降と同様ですので、参照してください。

NEXT パスワード変更について

NEXT パスワードを変更する画面によって、更新する内容が異なります。

NEXT パスワードを更新する際は、下表の内容にご注意ください。

➤ NEXT マネージャーで NEXT パスワードを変更する

画面	NEXT パスワード	NEXT パスワード最終更新日	ロックアウト
NEXT ユーザーの編集	変更前と同値	更新しない	解除しない
	変更前と異なる値	更新する	解除しない
NEXT ユーザーの パスワードリセット	変更前と同値	更新する	解除する
	変更前と異なる値		

➤ NEXT クライアントから NEXT パスワードを変更する

画面	NEXT パスワード	NEXT パスワード最終更新日	ロックアウト
NEXT パスワードの変更	変更前と同値	更新する	解除しない
	変更前と異なる値		

NEXT ユーザーの状態と NEXT 認証の可否

IC カード認証、顔認証

アカウントの状態によって NEXT クライアントに NEXT 認証でサインインできるかどうかが変わります。

認証の可、不可	NEXT サーバーとの通信環境	アカウントの状態
NEXT 認証が可能	オフラインのとき	<ul style="list-style-type: none"> ・NEXT パスワードが有効期限切れ ・初回サインイン時に NEXT パスワード変更が必要
NEXT 認証が不可	オンライン、オフラインとも	<ul style="list-style-type: none"> ・NEXT ユーザーが無効 ・NEXT ユーザーが有効期限切れ ・NEXT ユーザーがロックアウトされている
	オフラインのとき	<ul style="list-style-type: none"> ・NEXT ユーザーがオフライン有効日数の期限切れ
NEXT パスワード変更後に NEXT 認証が可能	オンラインのとき	<ul style="list-style-type: none"> ・NEXT パスワードが有効期限切れ ・初回サインイン時に NEXT パスワード変更が必要

ワンタイムパスワード認証

アカウントの状態によって NEXT クライアントにワンタイムパスワード認証でサインインできるかどうかが変わります。

認証の可、不可	NEXT サーバーとの通信環境	アカウントの状態
ワンタイムパスワード認証が可能	オンライン、オフラインとも	<ul style="list-style-type: none"> ・NEXT ユーザーがロックアウトされている ・NEXT パスワードが有効期限切れ（ワンタイムパスワード認証のみ利用する設定がされている状態）
ワンタイムパスワード認証が不可	オンライン、オフラインとも	<ul style="list-style-type: none"> ・NEXT ユーザーが無効 ・NEXT ユーザーが有効期限切れ
	オフラインのとき	<ul style="list-style-type: none"> ・NEXT ユーザーがオフライン有効日数の期限切れ
NEXT パスワード変更後にワンタイムパスワード認証が可能	オンライン、オフラインとも	<ul style="list-style-type: none"> ・初回サインイン時に NEXT パスワード変更が必要 ・NEXT パスワードが有効期限切れ（NEXT 認証とワンタイムパスワード認証の両方を利用する設定がされている状態）

NEXT 緊急パスワード認証

アカウントの状態によって NEXT クライアントに NEXT 緊急パスワード認証でサインインできるかどうかが変わります。

認証の可、不可	NEXT サーバーとの通信環境	アカウントの状態
NEXT 緊急パスワード認証が可能	オフラインのとき	<ul style="list-style-type: none">• NEXT ユーザーが無効• NEXT ユーザーが有効期限切れ• NEXT ユーザーがロックアウトされている• NEXT ユーザーがオフライン有効日数の期限切れ
	オンライン、オフラインとも	<ul style="list-style-type: none">• NEXT パスワードが有効期限切れ• 初回サインイン時に NEXT パスワード変更が必要
NEXT 緊急パスワード認証が不可	オンラインのとき	<ul style="list-style-type: none">• NEXT ユーザーが無効• NEXT ユーザーが有効期限切れ• NEXT ユーザーがロックアウトされている

編集・著作 株式会社両備システムズ

ARCACLAVIS は、株式会社両備システムズの登録商標です。

記載されている社名、製品名等は各社の商標または登録商標です。

記載されている内容は予告なく変更される場合があります。あらかじめご了承ください。

本書の内容については万全を期して作成致しましたが、万が一不審な点や誤り、記載漏れなどのお気づきの点がありましたらご連絡ください。

また、株式会社両備システムズの許可なく、複製・改変などを行うことはできません。