# ユーザー操作マニュアル
# 共通操作
# ログイン

# 目次

製品にログイン ..... 3
パスワード定期変更 ..... 11
２段階認証 ..... 13
顔・指紋（パスキー）で認証 ..... 17
ログインできなかった場合 ..... 30

# 製品にログイン

## ▶ ログイン

各製品にログインします。初めてのご利用の場合、ブラウザの設定をご確認ください。
詳細は「可視化経営システム 動作ブラウザ制約事項」を参照してください。

1. ブラウザを起動して、下記URLを入力し、ログイン画面を表示します。

- **NI Collabo 360**
  https:// ドメイン名 /ni/niware/
- **Sales Force Assistant 顧客創造**
  https:// ドメイン名 /ni/nisfa/
- **Sales Force Assistant 顧客深耕**
  https:// ドメイン名 /ni/nicrm/
- **Sales Force Assistant 顧客深耕AO**
  https:// ドメイン名 /ni/nisfa/
- **Sales Force Assistant ABM**
  https:// ドメイン名 /ni/nisfa/
- **Sales Quote Assistant**
  https:// ドメイン名 /ni/nisqa/
- **Sales Billing Assistant**
  https:// ドメイン名 /ni/nisba/
- **Approach DAM**
  https:// ドメイン名 /ni/nisfa/
- **MapScorer**
  https:// ドメイン名 /ni/nimsc/
- **nyoibox**
  https:// ドメイン名 /ni/nyoibox/

2. ログインID、パスワードを入力して「ログイン」ボタンをクリックします。パスワードは、”●”表示となります。入力情報が正しければ、ポータル画面が表示されます。



補足

- ログインID、パスワードが不明な場合は、自社のシステム管理者にご確認ください。
- パスワード入力を複数回間違えると、ログインできなくなる場合があります。自社のシステム管理者にご確認ください。
- ログインID は、システム設定画面でのみ変更することができます。自社のシステム管理者にご確認ください。
- システム設定でパスワードの変更を許可されている場合、パスワードをオプション設定画面から変更できます。
  詳細は「パスワード変更」を参照してください。
- パスワード定期変更が設定されている場合、ログイン後にパスワード変更要求画面が表示されます。
  入力条件にあうパスワードを入力してください。
  詳細は「パスワード定期変更」を参照してください。
- パスワード定期変更とは、設定された期間以降にパスワードの変更が必要となるセキュリティ強化の機能です。
  システム設定でパスワードの定期変更を設定している場合に表示されます。
  設定内容については、自社のシステム管理者へご確認ください。
- 2段階認証が設定されている場合、ログイン後に認証画面が表示されます。
  認証方式は2通りあります。認証方式に応じてパスワードを入力してください。
  詳細は「2段階認証」を参照してください。
- NI Collabo 360ではログインと同時に在席状況を「在社」にするログイン方法があります。
  詳細は、行先伝言共有の「ログインと同時に在席状況を在社にする」を参照してください。

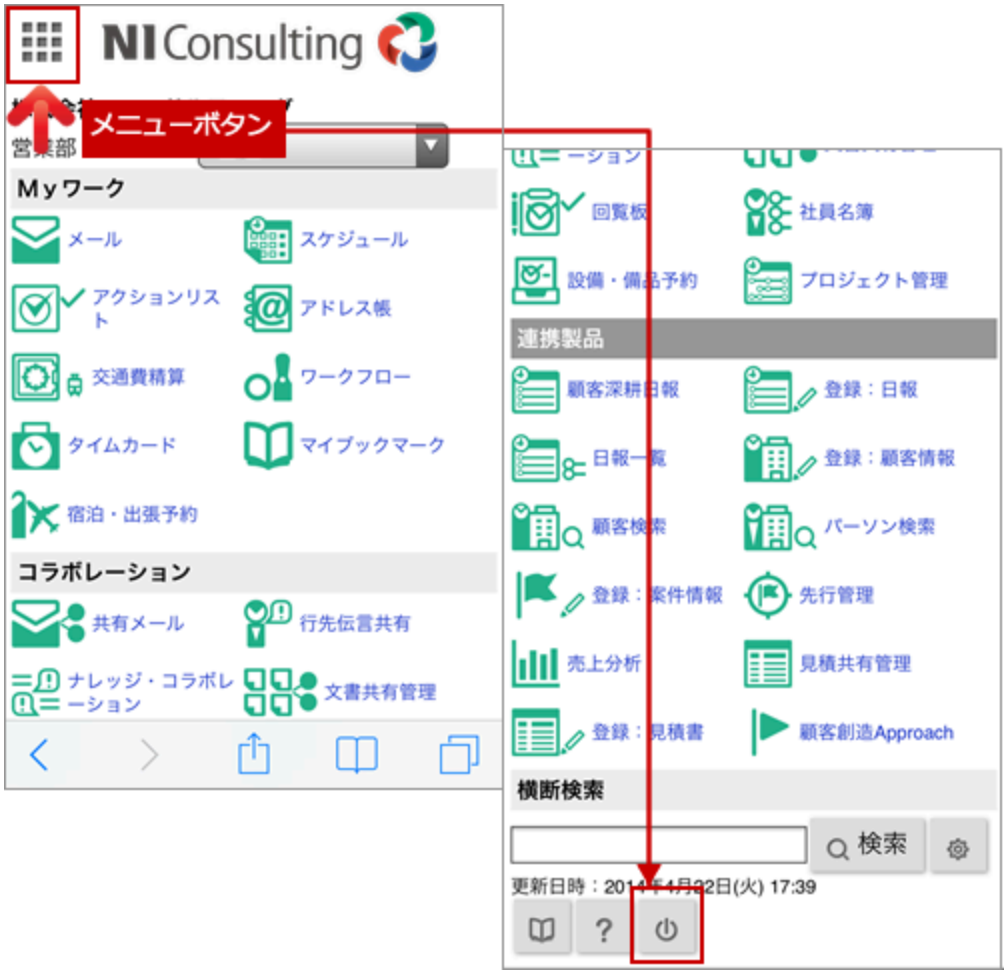
## ▶ ログアウト

- **NI Collabo 360**

1. スマートフォンの場合は、「ログアウト」ボタンはメニューの中にあります。




2. スマートフォンの場合は、「ログアウト」ボタンはメニューの中にあります。



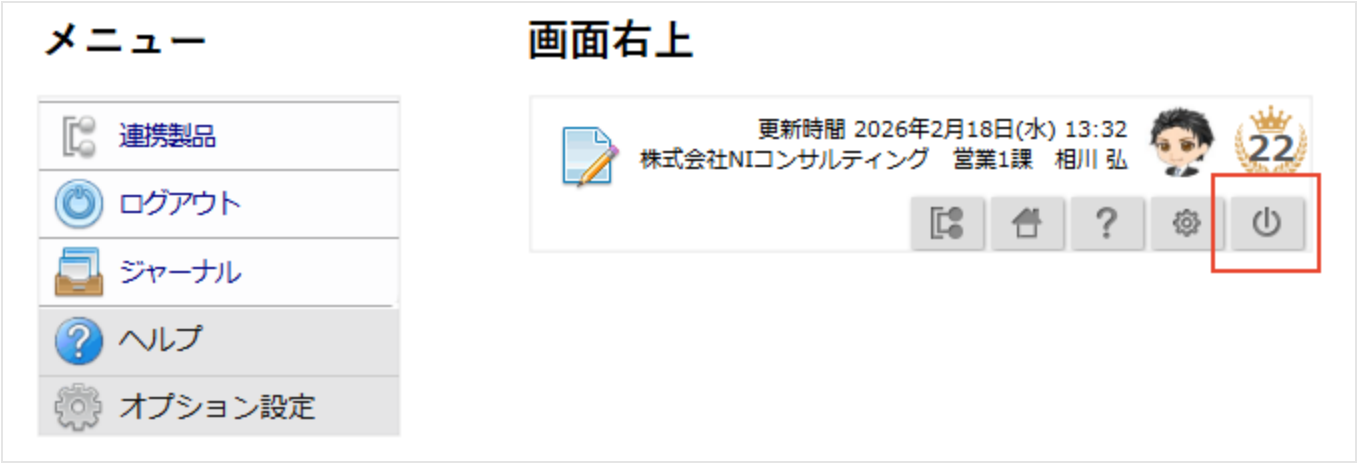
補足

- **退社（ログアウト）について**
  ポータル画面の上部のプルダウンメニューから「退社（ログアウト）」を選択すると、在席状況を退社に変更すると同時にログアウトを行うことができます。



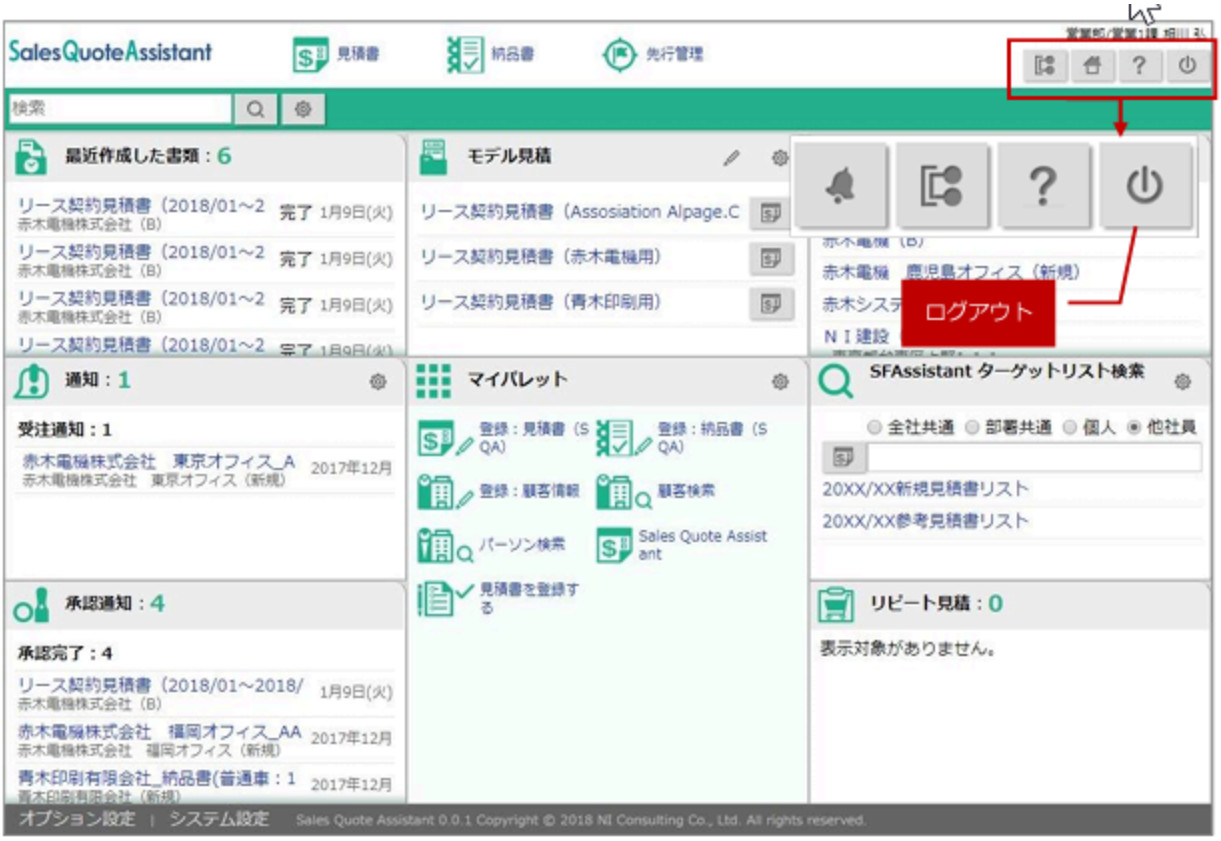

- **Sales Force Assistant シリーズ および Appraoch DAM**

1. 左メニューまたは画面右上の「ログアウト」ボタンをクリックします。



- **Sales Quote Assistant**

1. 画面右上の「ログアウト」ボタンをクリックします。



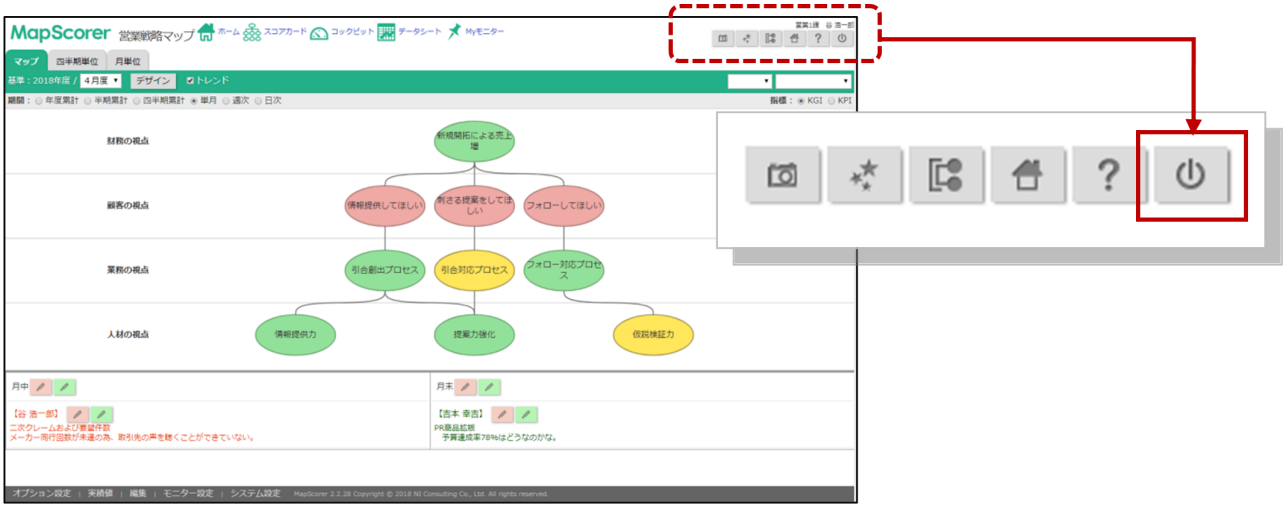
- **Sales Billing Assistant**

1. 画面右上の「ログアウト」ボタンをクリックします。



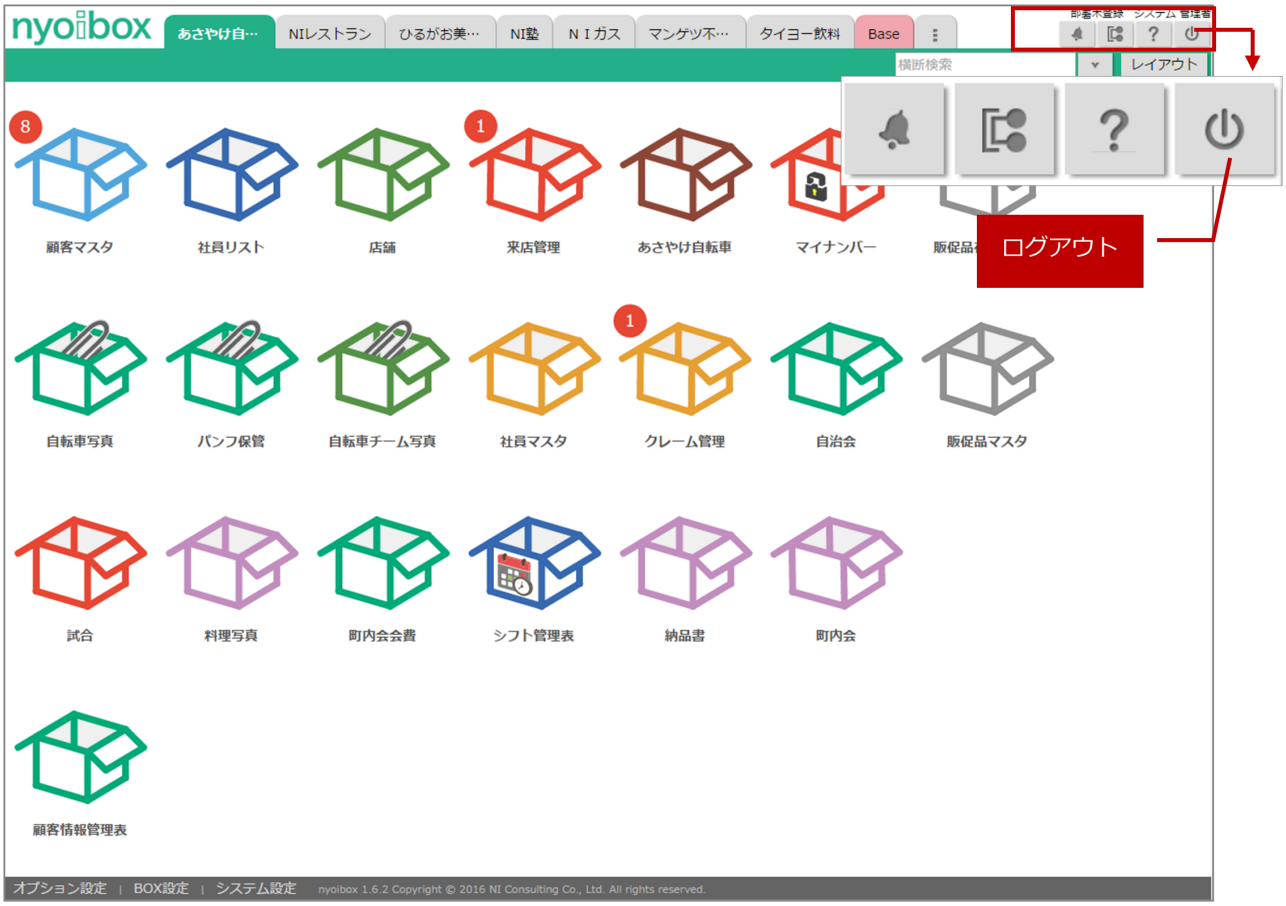
- **MapScorer**

1. 画面右上の「ログアウト」ボタンをクリックします。




- **nyoibox**

1. 画面右上の「ログアウト」ボタンをクリックします。



# パスワード定期変更

## ▶ パスワード定期変更方法について

補足

- パスワード定期変更とは、設定された期間以降にログインすると強制的にパスワード変更を促す機能です。
  システム設定側でパスワード定期変更の設定がある場合のみ表示されます。
  変更間隔/入力条件については、システム管理者へご確認ください。

## ▶ パスワードの変更方法

パスワード定期変更とは、設定された期間以降にログインすると強制的にパスワード変更を促すセキュリティ機能です。
※システム設定側でパスワード定期変更の設定がある場合のみ表示されます。変更間隔/入力条件については、システム管理者へご確認ください。

1. ログイン画面からログインID、パスワードを入力し、「ログイン」 ボタンをクリックします。
   ⇒「パスワード変更要求」画面が表示されます。




2. 新しい「パスワード」「パスワード（確認）」を入力し、再度 「登録」をクリックします。
   ※パスワードは「●」で表示されます。
   ※過去に利用したパスワードが利用できない場合があります。

# ２段階認証

## ▶ 2段階認証について

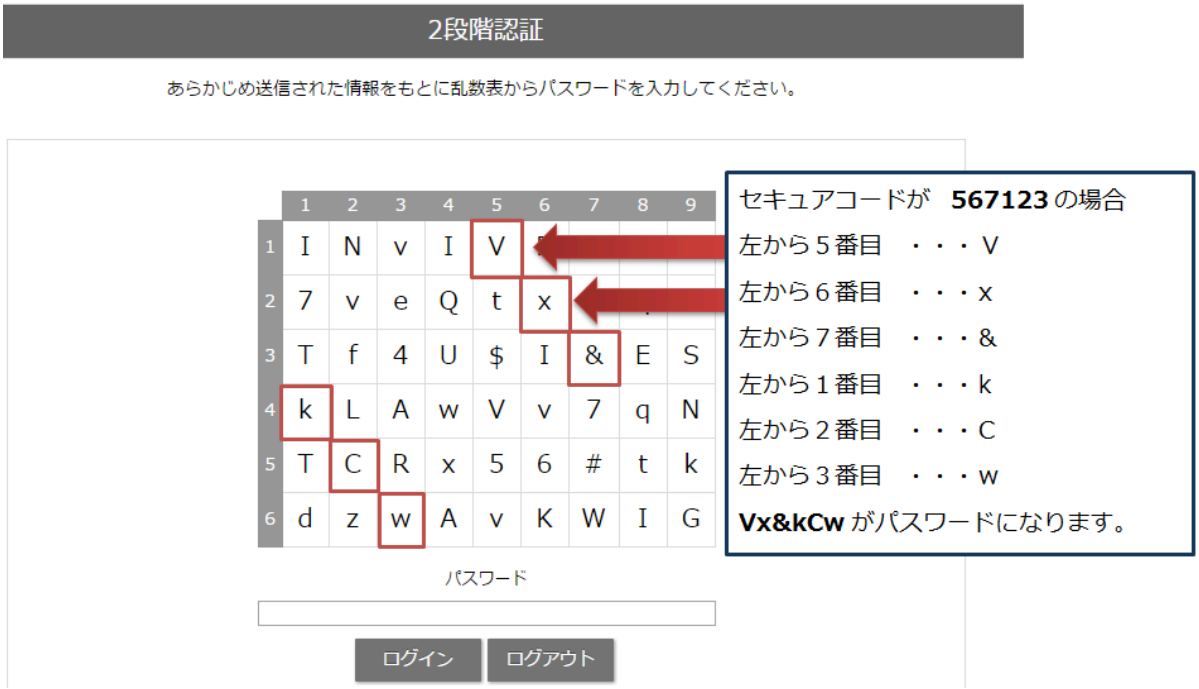
2段階認証は通常の製品ログインに加えてパスワード確認を行うことで、より安全にログインするための仕組みです。当社では、携帯メールアドレス宛にパスワードを送信する方式と、6桁の数値（以下、「セキュアコード」といいます。）による認証方式を提供しています。

## ▶ 携帯メールアドレス宛にパスワードを送信




1. 認証画面を開くと携帯メールアドレス宛にパスワードが送信されます。
2. 送信されたパスワードをフォームに入力しログインボタンをクリックしてください。
   認証が出来ない場合は、ログアウトし再度認証をおこなってください。

# ▶ セキュアログイン




**補足**

- 事前に携帯メールアドレス宛にとどいたセキュアコードをもとにログインします。
- セキュアコードは一度しか送信されませんので、メールの内容を忘れないようにしてください。
- セキュアコードの数字は表の左からの位置を意味しています。

セキュアコードが「５６７１２３」の場合。
５は左から５番目の「V」
６は左から６番目の「x」
７は左から７番目の「&」
１は左から１番目の「k」
２は左から２番目の「C」
３は左から３番目の「w」
パスワードは「**Ｖｘ＆ｋＣｗ**」になります。

## ▶ 2段階認証を利用するためには

2段階認証を利用するには、システム設定の「２段階認証」をご参照ください。

# 顔・指紋（パスキー）で認証

## ▶ パスキーとは

パスワードなしでアカウントにログインできる、簡単かつ安全な方法です。
パスキーを設定すると、パソコンやスマートフォンの画面ロックの解除方法（指紋認証や顔認証など）と同じ方法でログインできます。

- パスワードを覚えたり入力したりする手間がなくなります。
- 指紋認証や顔認証などにより、パソコンやスマートフォンから簡単にログインできます。
- 従来のパスワードと異なり、パスキーは推測されたり使い回されたりすることがないため、攻撃者から情報を安全に保護できます。
- パスキーは、フィッシングやパスワード漏洩などのサイバー攻撃に強いため、パスワードよりも安全です。

補足

以下は、プラットフォームベンダー（Apple、Google、Microsoft）によるパスキーの概要です。

- Apple Developer – パスキーの概要
- Google セーフティーセンター – パスキーのパスワードレス認証
- Microsoft – パスキーの概要

## ▶ パスキーの有効化

パスキーを利用するには、あらかじめパソコンやスマートフォンで画面ロックを設定が必要です。
すでに設定済みの場合は再設定の必要はありませんが、念のためご確認ください。

弊社製品がパスキーをサポートしているOSは以下のとおりです。
ブラウザは最新バージョンの使用を推奨します。

| OS | OSの対応バージョン | ブラウザ |
|---|---|---|
| Windows | Windows 11 23H2以上 | Microsoft Edge, Chrome |
| iOS | iOS 17.2.1以上 | Safari |
| macOS | macOS 14以上 | Safari |
| Android | Android 12以上 | Chrome |

## Windows

アカウント設定のサインイン オプションで「Windows Hello」を有効にします。

1. Windowsのスタートメニューから「設定」をクリックします。
2. Windowsの設定画面のメニューから「アカウント」を開き、「サインイン オプション」をクリックします。



3. Windows Helloの認証方法を選択します。
   顔認証(Windows Hello)や指紋認証(Windows Hello)をクリックします。




4. [セットアップ]をクリックしてWindows Helloを有効化します。
   画面の指示に従って、セットアップを実施します。

### 補足

- Windows Helloで顔認証や指紋認証をセットアップするには、あらかじめPIN（暗証番号）の設定が必要です。
- 認証方法にて「このオプションは現在使用できません」と表示される場合、お使いのデバイスは非対応になります。
  - USB接続の指紋リーダーやカメラを追加することで、ご利用いただける場合もあります。
  - 顔認証を使用するには、Windows Hello対応のカメラが必要です。

### iOS

顔認証（または指紋認証）で画面ロックを解除する設定をします。

1. 「設定」>「Face ID（または Touch ID）とパスコード」から、顔認証（または指紋認証）を有効にします。
   Face ID（または Touch ID）を使用するには、あらかじめパスコードの設定が必要です。

> 補足
>
> - Apple サポート：iPhoneでFace IDを設定する
> - Apple サポート：iPhoneでTouch IDを設定する

### macOS

指紋認証で画面ロックを解除できるように設定します。
Touch IDに対応したデバイスでのみ設定できます。

1. 「システム設定」>「Touch IDとパスワード」から、指紋認証を有効にします。

> 補足
>
> - Apple サポート：MacでTouch IDを設定する

### Android

指紋認証または顔認証で画面ロックを解除できるように設定します。

1. 「画面ロック」の設定から、指紋認証または顔認証を有効にしてください。
   設定方法は、Androidデバイスの機種やバージョンによって異なる場合があります。

> 補足
>
> - 顔認証を利用するには、パスキーのセキュリティ基準を満たすデバイスが必要です。
>   画面ロックの解除が可能でも、パスキーには対応していない場合があります。
> - 設定方法の詳細については、各メーカーのサポート情報をご確認ください。

## ▶ パスキーを登録

1. 弊社製品にログインし、「オプション設定」を開きます。
2. 「基本設定」タブに移動し、「指紋・顔（パスキー）で認証」をクリックします。

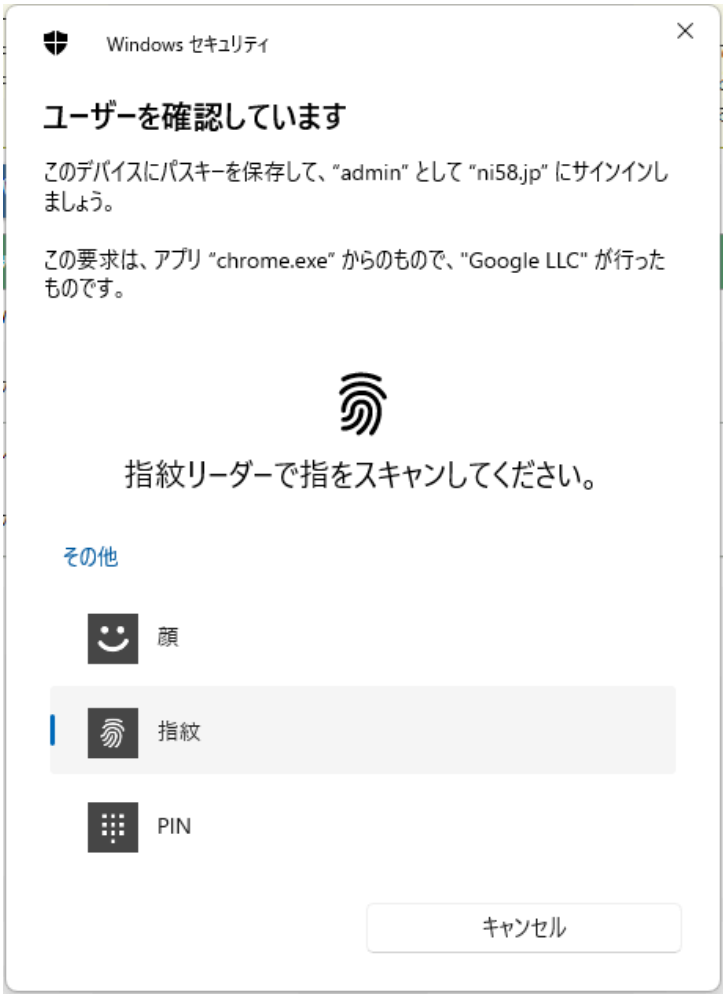



3. 「このデバイスでパスキーを作成」ボタンをクリックします。




4. 指紋や顔などによるパスキー認証が求められますので、認証を行ってください。
   なお、認証の手順はご利用のデバイスによって異なります。

**Windowsの場合**


Windows セキュリティ
ユーザーを確認しています
このデバイスにパスキーを保存して、"admin" として "ni58.jp" にサインインしましょう。
この要求は、アプリ "chrome.exe" からのもので、"Google LLC" が行ったものです。
指紋リーダーで指をスキャンしてください。
その他
顔
指紋
PIN
キャンセル


Windows セキュリティ
保存されたパスキー
Windows Hello を使用して、顔、指紋、または PIN でサインインできるようになりました。
admin
ni58.jp
OK

補足

- パスキーの作成は、必ずご本人が行う必要があります。
  管理者が代理で設定することはできません。
- パスキーは、信頼できるご自身のデバイスで作成してください。
  他の人と共有しているデバイスで作成すると、保存されたパスキーが第三者に使用される可能性があります。
- 指紋や顔などの生体情報は、デバイス内にのみ保存され、外部と共有されることはありません。
- 複数のデバイスをご利用の場合は、各デバイスごとにパスキーを作成する必要があります。
  ただし、Apple・Google・Microsoftなどのアカウントにログインしている場合は、同じアカウントでログインしている他のデバイスにパスキーが同期されることがあります。
  なお、パスキーを設定した場合でも、パスワードは引き続きご利用いただけます。

## ▶ パスキーでログイン

### ログイン手順

1. ログイン画面を開きます。
   ID入力欄をクリックすると、デバイスに保存されているパスキーが表示されます。
   表示された中から、利用するパスキーを選択してください。



2. 指紋や顔などによるパスキー認証が求められますので、画面の案内に従って認証を行ってください。
   なお、認証の手順はご利用のデバイスによって異なります。

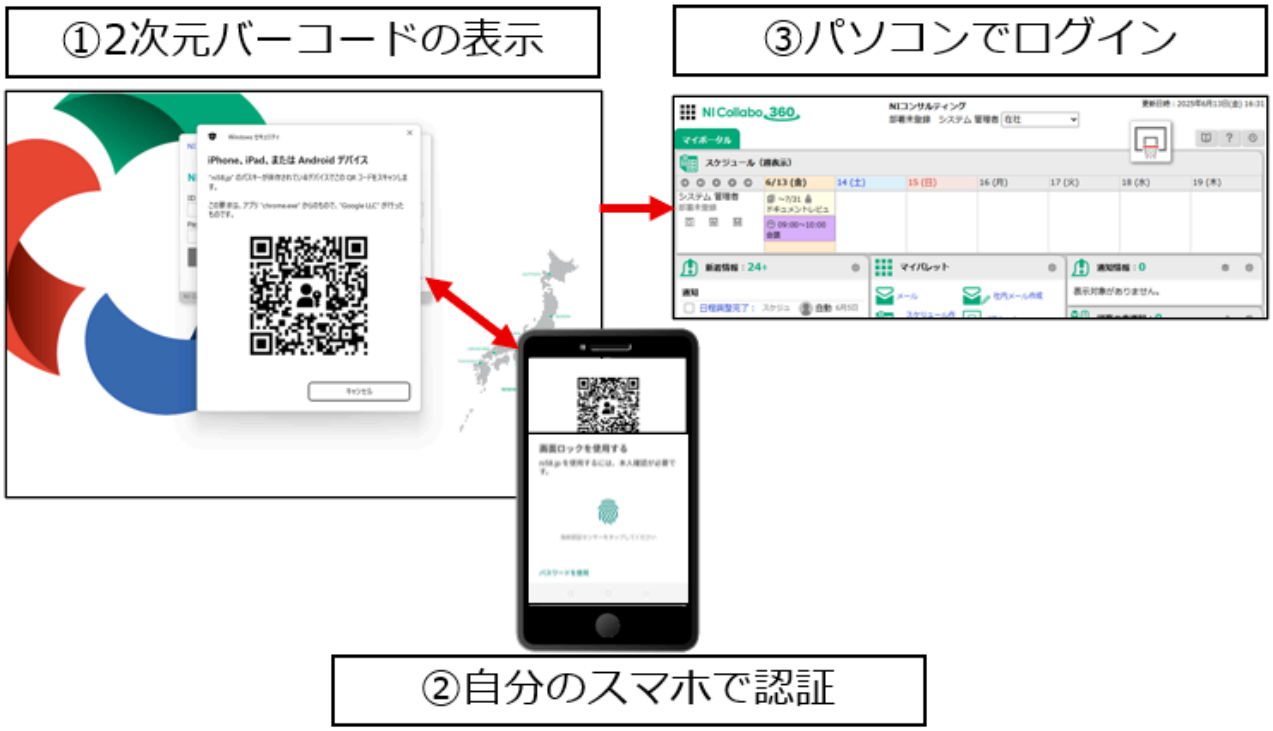



3. 認証に成功すると、ログインできます。

### クロスデバイス認証で利用

他の人と共用するパソコンや、パスキーが登録されていないデバイスから製品にログインする場合は、
パソコンに表示される2次元バーコードをスマートフォンで読み取り、認証を行うことができます。

1. パソコンのログイン画面で「別のデバイスのパスキーを使用」を選択し、2次元バーコードを表示させてください。
2. パスキーが保存されているスマートフォンで2次元バーコードをスキャンしてください。
   パスキーによる認証を求められるので、認証をしてください。
3. 認証に成功すると、パソコンでログインできます。




> **補足**
>
> - パソコンとスマートフォンの両方でBluetooth接続が可能である必要があります。
> - デバイスごとに操作方法が異なるため、詳細については「デバイスごとのサポート」を参照してください。

## ▶ パスキーを削除

1. 弊社製品にログインし、「オプション設定」を開きます。
2. 「基本設定」タブに移動し、「指紋・顔（パスキー）で認証」をクリックします。
3. 削除したいパスキーの「削除」ボタンをクリックし、確認画面が表示されたら「はい」をクリックしてください。

### 補足

- パスキーを削除すると、そのパスキーではログインできなくなります。
  削除後も、必要に応じて新しいパスキーを作成できます。
- パスキーは登録したデバイスにも保存されています。
  デバイスで同期し削除される場合もありますが、削除されない場合はデバイスでもパスキーを削除してください。
- デバイスごとに操作方法が異なるため、詳細については「デバイスごとのサポート」を参照してください。

## ▶ デバイスごとのサポート

パスキーは、デバイスのOSやブラウザに依存します。
詳細については、各プラットフォームベンダーのサポート情報を参照してください。

- Microsoft Learn：Windowsの場合
- Appleサポート：iPhoneの場合
- Appleサポート：iPadの場合
- Appleサポート：Macの場合
- Googleヘルプ：Androidの場合

# ログインできなかった場合

## ▶ ログインできない理由

- 入力されたIDやPasswordが間違っている可能性があります。
  ブラウザのパスワード記憶をご利用の場合、お使いのブラウザの設定をご確認ください。
- Password入力ミスによりロックアウトされている可能性があります。
  設定されている規定回数のPassword間違いがあると、セキュリティ保護のためロックアウトされます。
  ロックアウトは設定により、時限解除か管理者が解除するまでロックされたままとなります。
- アカウントが使用停止になっている可能性があります。
  ログインアカウントが使用停止、または削除されている場合はログインできません。
- このパスキーは使用できません。
  選択したパスキーの使用が停止されている可能性があります。

## ▶ システム管理者ではない場合

- システム設定権限をお持ちの管理者までご連絡ください。
  パスワードの上書きや、ロックアウト解除など、確認及び設定変更を行って頂くようお伝えください。

## ▶ システム管理者の場合

- 他にシステム設定権限をお持ちの管理者がいる場合は、作業を行って頂くようお伝えください。
  システム設定権限をお持ちの管理者が不在の場合や、操作方法が不明な場合は、ＮＩコンサルティング サポートデスクへご連絡ください。