スマートフォン向けアプリ
認証する[iOS]

目次

認証する[iOS] 3

認証する[iOS]

▶ 認証方法の種類

アプリを利用するために、下記のいずれかの方法で認証を行います。

- QRコード認証
  アプリを利用する端末とは別に、QRコードを表示するための端末が必要です。
- パスワード認証
  連携先URL・ID・パスワードを入力して認証します。他の端末が手元にない場合にご利用ください。

認証には連携先製品のログイン情報が必要です。アプリによって連携先製品が異なります。

連携先製品	**利用可能なアプリ**
NI Collabo 360	NI Calendar NI Collabo NOW ! NI 経費精算 Reader NI Collabo Attention ! NI Collabo UP ! NI Collabo Mail NI Collabo バスケット NI Collabo Video Uploader Ultimate Backupアプリ
Sales Force Assistantシリーズ	SFAssist マッピングアシスト

▶ QRコード認証

1. アプリで読み取るQRコードを表示するため、アプリを利用する端末とは別の端末を使い、ブラウザで連携先製品（NI Collabo 360またはSales Force Assistantシリーズ）にログインします。
2. 「オプション設定＞基本設定＞スマートフォンアプリ＞認証」に遷移するとQRコードが表示されます。
   「NI Collabo 360」ポータル画面下部の「アプリ認証」から開くこともできます。
3. アプリを起動して認証情報の画面を開きます。
4. 「QRコード認証」ボタンをタップしてカメラを起動します。
   QRコードを読み取るため、カメラの使用権限を許可してください。
5. 起動したカメラでQRコードを読み取ってください。



▶ パスワード認証

1. アプリを起動して認証情報の画面を開きます。
2. 連携先URLを入力してください。
   連携先URLはブラウザで連携先製品（NI Collabo 360またはSales Force Assistantシリーズ）にログイン後、「オプション設定＞基本設定＞スマートフォンアプリ＞認証」に遷移すると記載されています。
   ※「NI Collabo 360」ポータル画面下部の「アプリ認証」から開くこともできます。
   ※スマートフォンまたはタブレットで画面表示すると、連携先URLの横に「コピー」ボタンが表示され、コピー&ペーストで入力することができます。
3. 連携先製品（NI Collabo 360またはSales Force Assistantシリーズ）にログインする際のID・Passwordを入力してください。接続ができれば完了です。



▶ クライアント証明書による端末認証

> Hint
>
> - 本機能は通常はシステム管理者からの連絡・案内があってから利用する機能です。特に案内がない、あるいは、ご利用の予定がなければ本節は読み飛ばしてください。

はじめに

NIコンサルティングが提供しているスマートフォンアプリでは、特定端末からのアクセスのみを許可する手段としてクライアント証明書を利用した通信方式をサポートしています。
クライアント証明書を使うためには対象アプリ内に使用する証明書を最初に一度だけ取り込む必要があります。ただし、取り込んだ証明書の有効期限が切れたなどの理由で証明書を更新する場合は再度取り込みが必要になります。

証明書をアプリ内に配置するため、Windows PCまたはMacと対象アプリがインストールされているiOSデバイス（iPhone、iPad）を有線ケーブルで接続する必要があります。

> Hint
>
> - 証明書はiOS標準のキーチェーンサービスによって対象アプリ間で共有されるため、NIコンサルティングが提供している他のアプリで証明書を取り込んであれば改めて取り込む必要はありません。
> ※他社製アプリはこの共有された証明書は利用できません。

事前にご用意いただくもの

- クライアント証明書ファイル
  秘密鍵を含むPKCS#12形式のファイル（拡張子が.p12または.pfxのファイル）、および秘密鍵を保護しているパスフレーズ。
  ※証明書ファイル名は固定とする必要があり「niconsul.p12」に変更してください。
  ※パスフレーズなしの証明書には対応していません。
- MacまたはWindows PC
  証明書をアプリ内に転送するため、Windows PCまたはMacとiOSデバイス（iPhone、iPad）を有線ケーブルで接続する必要があります。

クライアント証明書をアプリに取り込む

macOS Mojave以前またはWindows PCをお使いの場合は「iTunes経由の場合」を参照してください。
macOS Catalina以降をお使いの場合は「Finder経由の場合」を参照してください。

iTunes経由の場合

1. 入手したクライアント証明書ファイルのファイル名を**「niconsul.p12」**に変更します。
2. MacまたはWindows PCに対象となるiOSデバイスをケーブルで接続し、iTunesを起動します。
3. iTunes上で対象のiOSデバイスを選択し、設定の「ファイル共有」を表示します。
4. ファイル共有の「App」から対象アプリを選択し、右側の「（選択したアプリ名）の書類」ビューにファイル名を「niconsul.p12」としたクライアント証明書ファイルをドラッグ＆ドロップするか、下部の「ファイルを追加」ボタンからクライアント証明書ファイルを選択しアプリ内に証明書を配置します。
5. iOSデバイス上で証明書を配置したアプリを起動します。上記操作をする前にアプリを起動していた場合は、アプリの再起動が必要です。
6. アプリの認証情報画面の下部にある「クライアント証明書を使用する」のスイッチをタップすると、証明書のパスワードが要求されます。ここで**秘密鍵を保護しているパスフレーズ**を入力してください。
7. 取り込みが成功すると証明書の識別名（エイリアス名）が設定画面に表示されます。
   アプリからの通信時にクライアント証明書を要求されると、自動的にこの証明書を提示して通信するようになります。



Finder経由の場合

1. 入手したクライアント証明書ファイルのファイル名を**「niconsul.p12」**に変更します。
2. Macに対象となるiOSデバイスをケーブルで接続し、Finderを起動します。
3. Finder上で対象のiOSデバイスを選択し、「ファイル」を表示します。
4. ファイル名を「niconsul.p12」としたクライアント証明書ファイルを対象アプリへドラッグ＆ドロップして追加します。
5. iOSデバイス上で証明書を配置したアプリを起動します。上記操作をする前にアプリを起動していた場合は、アプリの再起動が必要です。
6. アプリの認証情報画面の下部にある「クライアント証明書を使用する」のスイッチをタップすると、証明書のパスワードが要求されます。ここで**秘密鍵を保護しているパスフレーズ**を入力してください。
7. 取り込みが成功すると証明書の識別名（エイリアス名）が設定画面に表示されます。
   アプリからの通信時にクライアント証明書を要求されると、自動的にこの証明書を提示して通信するようになります。



Hint

- クライアント証明書を使う環境でQRコード認証を行う際、QRコード画面をHTTPSで開く必要があります。これはQRコードに含まれている接続用のURLはその画面を開いたときのURLに応じて作成されるためです。
- iTunesまたはFinder経由でアプリ内に配置した証明書ファイル（niconsul.p12）は自動では削除されません。削除が必要な場合はiTunesまたはFinderからの操作で削除してください。

クライアント証明書をアプリから破棄する

クライアント証明書が不要になった場合は、以下の手順でアプリ内から破棄します。

1. アプリの認証情報画面内の「クライアント証明書を使用する」のスイッチをOFFにします。
2. 確認ダイアログで「削除」を選択すると、アプリ内に取り込まれている証明書が破棄されます。
