スマートフォン向けアプリ
認証する[Android]

目次

認証する[Android] 3

認証する[Android]

▶ 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。

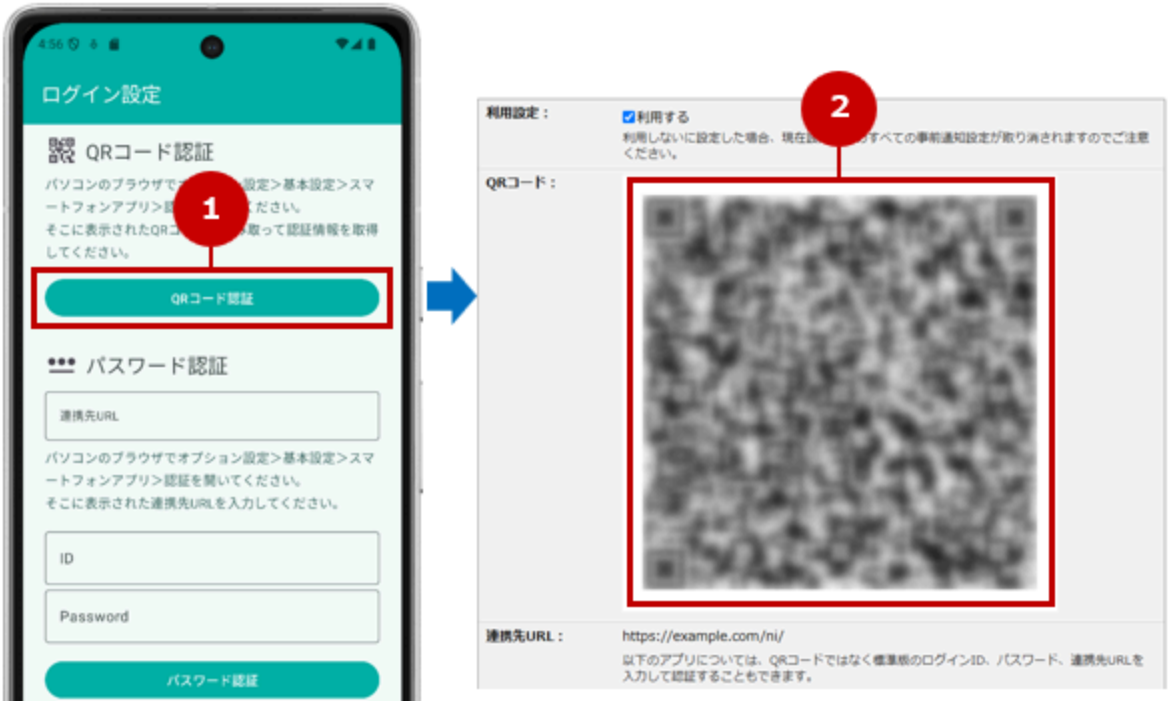
- QRコード認証
  アプリを利用する端末とは別に、QRコードを表示するための端末が必要です。
- パスワード認証
  連携先URL・ID・パスワードを入力して認証します。他の端末が手元にない場合にご利用ください。

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。

証明書ファイルをダウンロードするなど、あらかじめAndroid端末内の参照できる領域に証明書ファイルの配置が必要です。

> Hint
>
> - 証明書はAndroid標準のセキュリティ領域で管理されます。このセキュリティ領域はOS内の共通のため、他のアプリからも参照することが可能です。
> - 証明書の取り込みはアプリごとに行う必要はありませんが、どの証明書利用するのか選択する操作はアプリごとに必要です。
> - **Android OSのセキュリティ仕様上、OSにクライアント証明書をインストールすると画面のロック（PIN、顔認証、指紋認証など）が必須になります。**Androidデバイスの画面ロックを設定していない場合、後述の操作中にOSの画面ロックの方法を設定するよう要求されるため、その場合は適切な画面ロックを設定してください。

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。
- 中間CA証明書ファイル
  クライアント証明書の妥当性を証明する認証局の証明書です。

クライアント証明書をアプリに取り込む

ここではクライアント証明書を証明書発行元のWebページからAndroid OS内にダウンロードしたとして説明します。
Androidデバイスの画面ロックを設定していない場合、操作中にOSの画面ロックの方法を設定するよう要求されるため、その場合は適切な画面ロックを設定してください。

1. クライアント証明書ファイルをタップするか、あるいはAndroid OSのシステムの「設定>セキュリティ」の「ストレージからのインストール」で対象のクライアント証明書ファイルを選択します。
2. 証明書を抽出するためのパスワードの入力が要求されます。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。
3. 続いて証明書の名称の入力が要求されます。通常は人が理解しやすい名称が自動でセットされますが、名称が省略されている場合は長い文字列が表示される場合があります。そのままでも利用できますが、任意のわかりやすい名称に変更することを推奨します。
4. エラーがなければ取り込みに成功です。
5. 次にクライアント証明書を利用したいアプリを起動します。
6. アプリ内の認証情報画面の「クライアント証明書を使用する」のスイッチをONにすると、証明書の選択ダイアログが表示されます。
7. ここで先ほど登録した証明書を選択し許可します。
8. 証明書を選択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。

中間CA証明書ファイルをOSにインストールする

こちらは該当ファイルが提示されている場合にのみ行います。
ここでは証明書を証明書発行元のWebページからAndroid OS内にダウンロードしたとして説明します。

1. 証明書ファイルをタップするか、あるいはAndroid OSのシステムの「設定> セキュリティ」の「ストレージからのインストール」で対象の中間CA証明書ファイルを選択します。
2. インストールに成功すると「設定> セキュリティ」の「信頼できる認証情報」にユーザーが追加したCA証明書として登録されていることを確認できます。

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取り込まれている証明書を破棄します。

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。
   この状態でアプリは証明書を使わない通信に戻ります。

OSにインストールされている証明書は引き続き残っているため、それらを削除するには「設定> セキュリティ」から「認証ストレージの消去」を選択してください。ただし、この操作はユーザーによって追加されたすべてのクライアント証明書がリセットされるため（個別に指定ができません）、他に必要な証明書がインストールされていないことを確認してから実行することを推奨します。
