



本書はWindows 10 端末に証明書をインストールする際の手順を記載しています。

※Windows 10以外の端末をご利用の場合は、ポータルサイトよりWindowsアイコンをクリックし「Windows 10以外はこちら」をご確認ください。

- ① 利用者証明書管理システムのログイン画面にアクセスし、管理者から通知された「証明書取得用No」および「証明書取得用パスワード」を入力し「ログイン」をクリックします。



- ② セキュアクラウドへの接続設定画面でクライアント証明書のダウンロードアイコンをクリックします。





③ ダウンロードファイルの「開く」をクリックします。

※ご利用のブラウザにより表示が異なります。

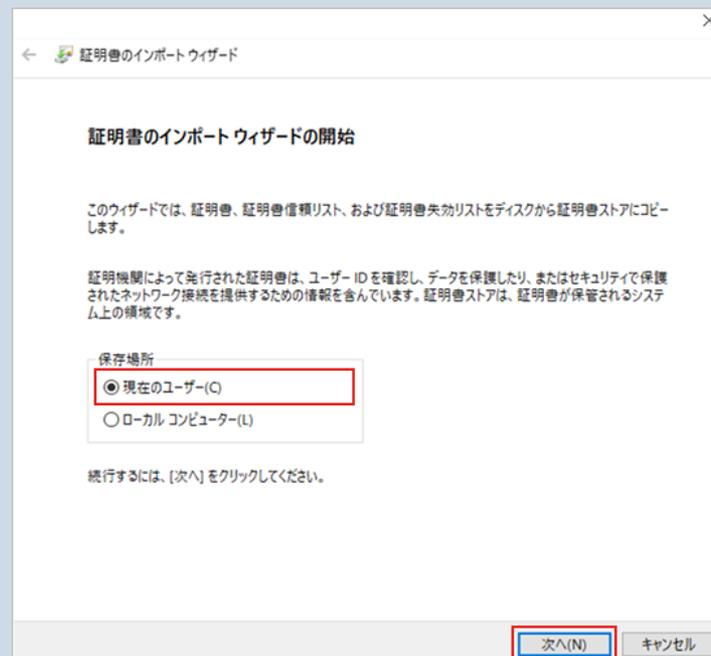
(「保存」をクリックした場合、通常は“ダウンロード”か“マイプロファイル”にファイルが保存されます。任意の場所に保存する場合は、保存先を忘れないようにしてください。ダウンロードした証明書ファイルを開くと、次の手順に進めます。)



④ 証明書のインポートウィザードの開始が表示されます。

保存場所が「現在のユーザー」であることを確認し、「次へ」をクリックします。

※複数のアカウントでWindows端末にサインインしている場合は、それぞれのアカウント毎に証明書のインストールが必要です。(アカウント毎に保存場所を「現在のユーザー」に設定し、証明書のインストールをします。)





- ⑤ インポートするファイルが指定されていることを確認し、「次へ」をクリックします。

証明書インポートウィザード

インポートする証明書ファイル

インポートするファイルを指定してください。

ファイル名(F):
C:\Users\Administrator\Downloads\1115_12345678.p12 参照(R)...

注意: 次の形式を使うと 1 つのファイルに複数の証明書を保管できます:

- Personal Information Exchange- PKCS #12 (.PFX, .P12)
- Cryptographic Message Syntax Standard- PKCS #7 証明書 (.P7B)
- Microsoft シリアル化された証明書ストア (.SST)

次へ(N) キャンセル

- ⑥ 「パスワード」に「証明書取得用パスワード」を入力後、「次へ」をクリックします。

証明書インポートウィザード

秘密キーの保護

セキュリティを維持するために、秘密キーはパスワードで保護されています。

秘密キーのパスワードを入力してください。

パスワード(P):
[Redacted Password Field] パスワードの表示(D)

インポートオプション(O):

- 秘密キーの保護を強力にする(E)
このオプションを有効にすると、秘密キーがアプリケーションで使われるたびに確認を求められます。
- このキーをエクスポート可能にする(M)
キーのバックアップやトランスポートを可能にします。
- 仮想化ベースのセキュリティを使用して秘密キーを保護する(エクスポート不可)(P)
- すべての拡張プロパティを含める(A)

次へ(N) キャンセル



⑦ 証明書ストアを自動的に選択させるか、指定するかを選択し、「次へ」をクリックします。

※特に指定がなければ「自動的に選択する」の状態のまま「次へ」をクリックします。

証明書ストア

証明書ストアは、証明書が保管されるシステム上の領域です。

Windows に証明書ストアを自動的に選択させるか、証明書の場所を指定することができます。

証明書の種類に基づいて、自動的に証明書ストアを選択する(U)

証明書をすべて次のストアに配置する(P)

証明書ストア:
 参照(R)...

次へ(N) キャンセル

⑧ 証明書のインポートウィザードの完了が表示されたら「完了」をクリックします。

証明書のインポートウィザードの完了

[完了] をクリックすると、証明書がインポートされます。

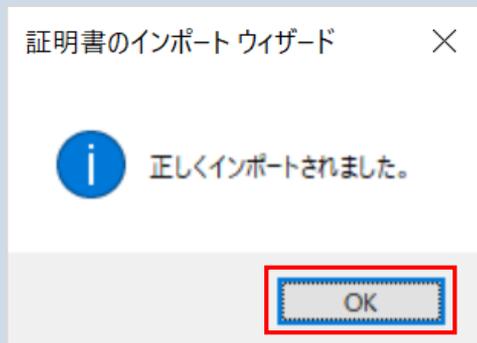
次の設定が指定されました:

選択された証明書ストア	ウィザードで自動的に決定されます
内容	PFX
ファイル名	C:\Users\Administrator\Downloads\F115_12345678.p12

完了(E) キャンセル



- ⑨ 「正しくインポートされました。」と表示されたら「OK」をクリックします。



以上で証明書の
インストール作業は完了です。