

サービス認証（ログイン）時に求められる認証要素^{※1}数の変更について

2023年8月11日に「共通認証（シングルサインオン, SSO）のリニューアルについて（重要）」でお知らせいたしました通り、2023年8月16日に共通認証（シングルサインオン, SSO）をリニューアルいたしました。その際に、学院内のネットワーク上の認証につきまして、当面の間は1要素のみが求められることをご案内いたしておりましたが、この度当初のご案内通り半年間の移行期間を終了し、2024年3月1日より共通認証で必須となる認証要素を、以下の通り変更いたします。

1. 共通認証で必須とする認証要素^{※1}に関する方針

共通認証では、全ユーザー（ただし当面の間は非専任教員、大学・短期大学の学生、中学部・高等部生を除く）については、表1のとおり、多要素認証を必須とする方針です。

表1 ユーザー種別・時期ごとの認証（ログイン）時に求められる認証要素^{※1}数

共通認証	教職員	専任教員	非専任教員	大学・短期大学の学生	その他 ^{※3}
	業務クライアント配付対象者	左記以外			
変更日：2024年3月1日～	2要素 (機密データを扱うシステムは デバイス認証を含む3要素)	2要素 ^{※2}	学内) 1要素 (当面の間)	学内) 1要素 (当面の間)	学内) 1要素 (当面の間)
			学外) 2要素	学外) 2要素	学外) 2要素

- ※1 認証（=ICTの世界における本人確認）のための確認手段のことを指します。「パスワード」も認証要素の一つです。
※2 学院内のネットワーク上でも、必須条件として2要素が求められます。
※3 研究員（大学院研究員、研究科研究員、専門職大学院研究員、理工学部研究員、受託研究員）、その他いずれにも該当しない方で大学のシステム利用IDをお持ちの方。

2. 2要素認証に必要な設定について

手持ちのデバイスの種類に応じた初期設定が必要です。詳細は、<https://ict.kwansei.ac.jp/sso-first-login>

注意事項

- a) ICTスキルに自信がある方を除き、初期設定には一定の時間が掛かります。初回ログイン時（=初期設定が必要となるタイミング）には、時間に余裕のある時に行ってください。
b) デバイスに登録した生体認証情報はデバイス外には送信されません（共通認証システムに送信されるのは、デバイス上での生体認証結果（成功か失敗か）のみです）

- ① **スマートフォンやタブレット（iOS/iPadOS/Android）を所有しているユーザー**
専用アプリ（Okta Verify）をインストール・設定いただきます。
生体認証対応のスマートフォンであれば、初期設定以後はパスワードの入力なしで、設定したスマートフォンやタブレットが手元にある限り、あらゆるデバイス上で共通認証へのログインが可能です（生体認証非対応の場合は、パスワードの入力が引き続き必要です）
- ② **PC(Windows/macOS)を所有しているユーザー**
専用アプリ（Okta Verify）をインストール・設定いただきます。生体認証（Windows Hello/Touch ID）対応のPCであれば、初期設定以後はパスワードの入力なしで当該PC上での共通認証へのログインが可能です（生体認証非対応の場合は、パスワードの入力が引き続き必要です）。
- ③ **個人で利用するPC・スマートフォンが無いユーザー**
ICTサポートまでお問い合わせください（<https://ict.kwansei.ac.jp/support>）。

