Science Tokyo ID 初期設定マニュアル(医歯学系)



2025.4 ITヘルプデスク





- 1. IDと初期パスワード/Science Tokyo Gmail アドレスの確認(必須)
- 2. パスワードの変更(必須)
- 3. 多要素認証 メール認証設定(必須)
- 4. 多要素認証 アプリ認証設定
- 5. パスワード再発行用メールアドレスの登録(必須)
- 6. 多要素認証 FIDO2認証設定
- 7. 初期設定後のログイン方法

SCIENCE TOKYO Science Tokyo Gmail アドレスの確認(必須)

Science Tokyo ID について

1. IDと初期パスワード/

Science Tokyoでは旧大学での認証システムに加えて、 新しい認証システム|Science Tokyo 認証システム」を導入いたしました。 旧認証システム(統合ID)とは利用できるサービスが異なりますので、 受領後はどちらも必ず初期設定を行ってください。

Science Tokyo Gmail について

Science Tokyo Gmailにつきましては、Science Tokyo Gmail のWebページをご参照ください。

IDと初期パスワードの確認方法について

統合ID及び学内LANアカウントを保有する方には、TMDUメール(@tmd.ac.jp) 宛に Science Tokyo ID 通知書(ID通知書)の受領用のURLを送付します。





2. パスワードの変更(必須)

「ユーザー名」の欄にScience Tokyo ID(以下、ID)を入力してください。
 これは、ID通知書記載の英小文字4文字+数字4文字(合計8文字)のものです。

・「パスワード」の欄に初期パスワードを入力して、「次へ」ボタンをクリックしてください。



2. パスワードの変更(必須)

新しいパスワードを設定

	パスワード変更 ログ	
	パスワードを変更してください。	
	~	
現在のパスワード	現在のパスワード	
 パスワードは、10文字以上 また、英小文字、英大文号 なお、使用できる記号は 	.99文字以内で指定ください。 2、数字、記号から各々1文字以上含める必要があります。 -!#\$%&*,.::@[] +='''()?^_`{}~<> のみとなります。	
 パスワードは、10文字以上 また、英小文字、英大文号 なお、使用できる記号は 	.99文字以内で指定ください。 2、数字、記号から各々1文字以上含める必要があります。 -!#\$%&*,.::@[] +='''()?^_`(}~<> のみとなります。	
 パスワードは、10文字以上 また、英小文字、英大文等 なお、使用できる記号は ペ、新しいパスワード 	.99文字以内で指定ください。 롣、数字、記号から各々1文字以上含める必要があります。 -!#\$%&*:@[] +='"()?^_`()~<> のみとなります。 新しいパスワード	
 パスワードは、10文字以上 また、英小文字、英大文等 なお、使用できる記号は ペ 新しいパスワード ダ 新しいパスワードの確認 	.99文字以内で指定ください。 F、数字、記号から各々1文字以上含める必要があります。 -!#\$%&*:@[] +=``'()?^_`{}~<> のみとなります。 新しいパスワード 新しいパスワード	

	5 75 72 1							
		多要素認証 (FIDO2)	多要素認証 (OTP)	ロ グ				
直近1週間のログを表示し	,ます。							
					2			
日時	結果	操作						
2025/02/17 09:59:04	成功	パスワード変更						

パスワードが変更されると「ログ」に「パスワード変更」が掲載されます。 ※結果が「処理中」となっている場合、しばらくしたら「成功」となります。 「成功」になるまで待つ必要はありません。

「現在のパスワード」の欄に初期パスワードを入力し、

条件を満たした「新しいパスワード」を2箇所に入力して、「保存」ボタンをクリックしてください。 10文字以上99文字以内、かつ英小文字、英大文字、数字、記号から各1文字以上含めること 使用できる記号は -!#\$%&*,..;@[]|+='"()?^_{}~<> のみ





3.多要素認証 メール認証設定(必須)

多要素認証(OTP)のメール認証を設定する

 多要素認証 (FIDO2) 多要素認証 (OTP) ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●		アナ	 カウント	
多要素認証 (OTP) を設定してください。 P アプリ認証 未設定		多要素認証 (FIDO2)	多要素認証 (OTP)	ログ
 ◆ アプリ認証 未設定 		多要素認証 (0	TP) を設定してください。	
	🌣 アプリ認証	未設定		◆設定
▲メール認証 未設定 ◆設定	▶ メール認証	未設定		◆設定

素認証 (FIDO2)	多要素認証 (OTP)	ログ				
メーノ	ル認証設定					
入力したメールアドレスにワンタイムパスワードを送信して、制限時間内に届いたワンタイムパスワードを設定してください。						
ワンタイムパス	マードを送信しました。					
必須	@gmail.cor	m				
4	コワンタイムパスワードを	送信する				
必 須 6村	桁の数字					
	パスワードを送信して、 ワンタイムパス	バスワードを送信して、制限時間内に届いたワンク ワンタイムバスワードを送信しました。				

- ・上部の帯の項目の中から「多要素認証(OTP)」をクリックして選択してください。 その後「メール設定」の行の右端の「設定」ボタンをクリックしてください。
- 「メールアドレス」欄にワンタイムパスワード受信のためのメールアドレスを入力してください。
 メールアドレスを入力したら、「ワンタイムパスワードを送信する」ボタンをクリックしてください。
 確実に受信して確認ができるメールアドレスを登録してください
 Science Tokyo Gmail アドレス(***@m.isct.ac.jp)および SaaSアドレス(***@saas.isct.ac.jp)は設定しないこと
 キャリアメール(携帯電話会社から提供されるメールアドレス)は非推奨





ワンタイムパスワードを受信

Extic ログイン用ワンタイムパスワード 受信トレイ×				アナ	コウント		
noreply@ex-tic.com		ポータル	プロフィール	パスワード変更	多要素認証 (FIDO2)	多要素認証 (OTP)	ログ
ログイン用のワンタイムパスワードです。 ワンタイムパスワード: 194648 有効期限: 2025年02月17日 10時13分59秒		0	▶アプリ認証	未設定		✿ 設定	
	•	2	メール認証	設定済	1	≥解除	
 ← 返信 ← 転送 ② 							
		設定が完了	了すると「多	要素認証 (OTF) のメール認証	が「設定済み」	となりま

す。

- ・入力したメールアドレスにワンタイムパスワードを記載したメールが送信されます。
 作業を行っているウィンドウはそのままに、別ウィンドウもしくは機器でメールを確認してください。
- ・メールに記載されている6桁のワンタイムパスワードを「ワンタイムパスワード」欄に入力して、
 「設定」ボタンを押してください。

4.多要素認証 アプリ認証設定



アプリ認証について

アプリ認証では、ワンタイムパスワードをメール経由ではなく、アプリから受け取ります。 デバイス(スマートフォンやタブレット等)にインストールされたアプリには種となるコードが記録され、 そのコードと時刻から、アプリはその都度、ワンタイムパスワードを生成します。 (注)時刻が間違っていると、ワンタイムパスワードが正しく生成されません。

また、アプリ認証はお使いのスマートフォン等に設定されますので、 機種変更をするとアプリ認証は使用できなくなり、再設定が必要です。 ※院内スマートフォンには設定できません。

アプリ認証の設定を始める前に、 App Store (iOS) またはGoogle Play Store (Android) から 「**Google Authenticator**」をインストールしてください。



iOS



Android

4.多	要	素認	2証	アプ	リ認	証設定				SCIENCE TOKYO
多要素	表認認	証(OT	P)のア	アプリ認識	証を設え	官する	ボータル ブロフ	アカウント マール パスワード変更 多要素認証 (FIDO2)	多 要素認証 (OTP) ログ	
			アナ	ウント				アプリ認証設定		_
	ポータル	プロフィール	パスワード変更	多要素認証 (FIDO2)	多要素認証 (OTP)	ログ	ソフトウェアトークンアフ 制限時間内に表示され	プリで下記の QRコードを読み取るか、表示される シークレットキ るトークンを設定してください。	ーを入力してください。	
	*	✿ アプリ認証	未設定		✿設定		闘 QR ⊐ード			
	2	マメール認証	設定済	8	●解除					
								シークレットキーを表示する	c	
							<i>ゆトークン</i>	 例) 012345 執設定 		

- ・上部の帯の項目の中から「多要素認証(OTP)」をクリックして選択してください。 その後「アプリ設定」の行の右端の「設定」ボタンをクリックしてください。
- ・画面に表示されているQRコードを「Google Authenticator」のアプリで読み取ってください。(※) アプリ上で生成されたトークンを「トークン|欄に入力して、 「設定|ボタンを押してください。 ※アプリを起動して、画面右下の①ボタンを押して「QRコードのスキャン」を選び、カメラをQRコードに向けてください。 トークン(ワンタイムパスワード)として6桁の数字が生成されます。

				アナ	コウント
	アカウント		ポータル プロフィール	パスワード変更	多要素認証 (FIDO2) 多要素認証 (OTP)
ボータル プロフィール パスワー	⁵ 変更 多要素認証 (FIDO2) 多要素認証 (OTP) ログ			テストメー	ルを送信しました。
≗ ユーザー名		-	- ユーザー名		×
▲ 表示名			,表示名		
■ メールアドレス	@m.isct.ac.jp		3 メールアドレス		@m.isct.ac.jp
🕿 バスワード再発行用メールアドレス 🔽	例) example@example.com	2	■ パスワード再発行用メールアドレ	z ?	edia.libtmdu@gmail.com
	☑テストメールを送信する	_			コテストメールを送信する
					四 保存

・上部の帯の項目の中から「プロフィール」をクリックして選択してください。

5.パスワード再発行用メールアドレスの登録

- (注)複数ある認証方式のうち1つ以上設定が完了していないと「プロフィール」は表れません。
- 「パスワード再発行用メールアドレス」の欄に、パスワード再発行用メールアドレスを入力してください。
- メールアドレスを入力後、「テストメールを送信する」をクリックしてください。

※設定するメールアドレスはメール認証と同じメールアドレスでも構いません

- Science Tokyo Gmail アドレス(***@m.isct.ac.jp)および SaaSアドレス(***@saas.isct.ac.jp)は設定しないこと

SCIENCE TOKYO



テストメールを受信する

[テストメール] Extic パスワード再発行用ワ	リンタイムパスワード GEFレイ×	
noreply@ex-tic.com To 自分 マ 	10:12 (5 分前) 🕁 🙂	≪テストメールが届かない場合≫ ・メールアドレスを再度確認する
 パスワード再発行用のワンタイムパスワードです。 ワンタイムパスワード : XXXX 有効期限 : XXXX		・述惑メールボックス内を確認する ・受信可能リストに「ex-tic.com」の ドメインを追加する
← 返信 → 転送 ④		・別のメールアドレスを試す

・入力したメールアドレスにシステムからメールが届くかどうかを確認してください。

メールが届いていれば「保存」ボタンをクリックしてください。

	ポータル	プロフィール	パスワード変更	多要素認証 (FIDO2)	多要素認証 (OTP)	¤ ″	
直近1週間のログを表示します。							
							€更新
日時	結果	扬	操作				
2025/02/17 10:13:18	成功	7	プロフィール更新				





FIDO2認証とは

多要素認証(FIDO2)を設定することで、パスキーのしくみにより 指紋認証や顔認証などを使って認証することができます。 ※入学・入職時期によっては、設定可能となるまで時間がかかる場合があります。

また、ご利用のPC、認証器、OS、Webブラウザの組み合わせによっては FIDO2認証ができない場合がありますので、導入前に必ず動作確認を実施してください。

下記サイトに「FIDO2動作確認済み認証器」の情報が公開されていますので、ご参照ください。 <u>https://www.exgen.co.jp/extic/specs.html</u>





FIDO2認証を設定する

・認証器を接続、または搭載したデバイスで Science Tokyoポータルサイトにログインします。 「多要素認証(FIDO2)」タブを選択→「新しい認証器を追加」をクリックします。



 \times

OK

٠ Windows ヤキュリティ 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、 して "tmdu.extic.com" にサインインしましょう。 この要求は、アプリ "msedge.exe" からのもので、 "Microsoft Corporation" が行ったものです。 କ୍ତି 認証器の追加 指紋リーダーで指をスキャンしてください。 その他 🛾 表示名 🛜 必須 例) Yubico 斎 指紋 例) Security Key by Yubico . PIN 別のデバイスを使用する ◆追加する ★キャンセル キャンセル ・ご利用の認証器を選択し、認証を行います。 • Windows ヤキュリティ 保存されたパスキー ・保存されたパスキーが表示されたら「OK」をクリックします。 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。 認証器が追加されていれば設定完了です。 tmdu.ex-tic.com

※ご利用の認証器によって認証方法が異なります ※Windows Hello等を設定済みのデバイスでは、すぐに認証に遷移する場合があります

認証器を追加

☺備考

・任意の表示名を入力し、「追加する」をクリックします。

6.多要素認証 FIDO2認証設定



Х

7.初期設定後のログイン方法



<u>Science Tokyo ポータルサイト</u>にアクセス

「ユーザー名」欄にScience Tokyo IDを入力してください。

パスワードレス認証を設定していない場合(①)、または、パスワードレス認証を設定済みだが、 OTPを使って認証する場合(②)は、次の画面で新しく設定したパスワードを入力してください。 ※②の場合は右側のパスワードのタブを選択してください。

		2
バスワード再発行用メールアドレスをmist.ac.jp 以外のメールアドレスに忘れず必ず設定してくださ い。本学の諸規則を通守してください。 【問い合わせ先】 science-foltwo-portal-guery@gsic titech ac in	a. K27-F	パスワードレス パスワード
▲ ユーザー名	→ 次へ	+3 パスワードレス認証
→ 次へ	× キャンセル	× キャンセル
 ●パスワードを忘れましたか ●メンテナンス情報はこちら 	 ● パスワードを忘れましたか ●メンテナンス情報はこちら 	 ●パスワードを忘れましたか ●メンテナンス情報はこちら

7.初期設定後のログイン方法

多要素認証(OTP)メール認証/アプリ認証

パスワードを「パスワード」欄に入力し、「次へ」ボタンをクリックしてください。

多要素認証の設定状況により認証方法が最大3つ表示されますので、 「ワンタイムパスワードメール認証」もしくは 「ワンタイムパスワードアプリ認証」を選択し、OTPにて認証を行ってください。





