

東北学院大学 統合認証アカウント：統合認証アカウント利用者ガイド

統合認証アカウント利用者ガイド

～統合認証システム利用マニュアル～

第 3.00 版/2025. 9. 29

東北学院大学 情報システム部 情報システム課

1. 本書について.....	- 2 -
2. サービス概要①：統合認証システムと統合認証アカウントについて.....	- 2 -
2.1. 統合認証システム（Extic）とは.....	- 2 -
2.2. 統合認証アカウントについて.....	- 2 -
2.3. 利用できる本院の IT サービス.....	- 2 -
2.4. 利用対象者.....	- 2 -
2.5. 利用上の注意.....	- 2 -
3. サービス概要②：統合認証アカウントの多要素認証について.....	- 4 -
3.1. アプリ認証（Time based One Time Password: TOTP 方式）.....	- 4 -
3.2. メール認証（Mail One Time Password: MOTP 方式）.....	- 5 -
3.3. FIDO2 認証（Fast IDentity Online 2: パスワードレス方式）.....	- 5 -
4. 利用ガイド：ログイン編.....	- 6 -
4.1. 統合認証システムと認証連携システムの認証用 URL（独自認証画面を除く）.....	- 6 -
4.2. Google アカウントと Microsoft アカウントの 2 段階認証.....	- 7 -
4.3. 統合認証システムでの ID とパスワード認証、パスワードレス認証（FIDO2 認証）.....	- 8 -
4.4. 統合認証システムでの多要素認証.....	- 10 -
5. 設定概要：統合認証システムにおける必須設定項目.....	- 12 -
5.1. 統合認証アカウントを新規で発行された方.....	- 12 -
5.2. 統合認証アカウントの設定を変更したい方.....	- 13 -
6. 設定ガイド①：統合認証アカウントのパスワード変更.....	- 13 -
6.1. パスワード変更手順①（現在のパスワードが分かる）.....	- 13 -
6.2. パスワード変更手順②（現在のパスワードが分からない、パスワードの有効期限が切れた）.....	- 16 -
7. 設定ガイド②：多要素認証（アプリ認証）を設定する.....	- 19 -
7.1. Google Authenticator または Microsoft Authenticator を利用する場合.....	- 19 -
7.2. Google Chrome 拡張機能を利用する場合.....	- 26 -
8. 設定ガイド③：多要素認証（メール認証）を設定する.....	- 31 -
9. 設定ガイド④：パスワード再発行用メールアドレスの登録.....	- 35 -

1. 本書について

本書では、東北学院の教職員および東北学院大学の学生等の構成員が、ご自身の統合認証アカウントを適切に管理・運用するためのガイドとして、統合認証システムにおける各種操作手順や多要素認証を利用するための参考手順を掲載いたします。

2. サービス概要①：統合認証システムと統合認証アカウントについて

2.1. 統合認証システム (Extic) とは

本院共有の認証システムで、本院で運用される様々な IT サービスとアカウント情報の連携を行っております。

2.2. 統合認証アカウントについて

統合認証システムから、東北学院の教職員および東北学院大学の学生等の構成員に対して発行される一意のアカウントです。(本院の IT サービスによっては、ID のみ、または、ID とパスワードを組合せて統合認証アカウントと呼ぶ場合がありますのでご注意ください。)

2.3. 利用できる本院の IT サービス

統合認証アカウントで利用できる本院の IT サービスの詳細については、東北学院大学 IT ナビ「統合認証アカウント」の掲載内容をご確認ください。

2.4. 利用対象者

- 学部生・大学院生、科目等履修生、特別聴講学生、聴講生、研究生、専門職大学院研修生等
- 教育職員（専任・非常勤）、事務職員（専任・非専任）
 - 統合認証アカウントの有効期間は、学校法人東北学院の所属資格を有する期間（退職、除籍、任期満了まで）です。失効後も一部サービスを一時的に利用できることがありますが、これは猶予期間としてのみ扱われます。
 - 名誉教授向け統合認証アカウントの利用には、利用者本人による総務課への申請が必要です。また、本アカウントで利用できるサービスには制限があります。

2.5. 利用上の注意

本院の IT サービスを利用する場合（統合認証アカウントの利用も含めて）は、東北学院大学 IT ナビ「利用案内（サイトポリシー）」の「コンピュータとネットワークの利用について」の事項をご一読の上、遵守ください。

また、統合認証システムの利用における注意事項は、以下のとおりです。

■利用場所の制限について

統合認証システムにおいて、学外ネットワークに接続した機器から認証を行う場合は、多要素認証が必要です。

■利用時間の制限について

統合認証システムでは、認証後にブラウザを閉じた場合や認証から 8 時間経過した場合は、再度認証が必要です。

■アカウントの一時ロック

不正アクセス防止のため、統合認証システムへのログインを 5 回連続で失敗すると、アカウントが一時的にロックされます。ロックは 30 分後に解除されますので、その後に再度ログインしてください。(30 分以内に自主解除することはできません。)

■パスワードについて

- 統合認証アカウントのパスワードは、セキュリティ対策のため、最終変更日から 365 日の有効期限を設けています。有効期限を迎えた場合、本院の IT サービスが利用できなくなりますのでご注意ください。
- 統合認証システムでパスワードを変更すると、新しいパスワードは統合認証システムの連携サービスにも同期されます。
- パスワード変更後、統合認証システムではすぐに新しいパスワードを利用できますが、統合認証システムの連携サービスへの同期には時間がかかる場合があります。(閑散期は 5～10 分、繁忙期は数時間程度)
- パスワードの設定については、複雑性の条件や履歴を管理しておりますので、パスワード変更ページの記載事項をご確認ください。
- パスワードの有効期限に関するお知らせは、有効期限 20 日前に、利用者が事前登録した「パスワード再発行用メールアドレス」宛に配信されます。

■パスワード再発行手続きについて

- 「パスワードが分からなくなった」「パスワードの有効期限が切れた」等で、本院の IT サービスにログインできない場合は、
 - 統合認証システムのログイン画面の「パスワードを忘れましたか？」か、パスワード再発行ページからパスワードを再発行してください。(利用者が「パスワード再発行メールアドレス」を事前登録しておく必要があります。)
- パスワード再発行用メールアドレスを事前登録していなかった場合や、パスワード再発行用メールアドレスにメールが届かない場合は、
 - 教職員証・学生証をお持ちの上、各キャンパスの情報処理センター窓口、または土樋 1 号館情報システム課までお越しください。(遠隔対応は行っておりません。)

■定期的な設定の見直しについて

携帯電話の機種変更やキャリア変更、プロバイダ変更等により、統合認証アカウントの設定変更が必要になった場合は、速やかに再設定してください。

また、統合認証アカウントの設定内容について、定期的な見直しをお願いいたします。

3. サービス概要②：統合認証アカウントの多要素認証について

本学の統合認証システム(Extic)では、統合認証アカウントの認証時に、ID とパスワードの認証と合わせて、アプリ認証とメール認証、FIDO2 認証のいずれかと組合せた多要素認証が必要となります。

※多要素認証は学外ネットワークからの認証時のみ動作します。学内ネットワークの場合は、ID とパスワードのみの認証（FIDO2 設定時はパスワードレス認証も利用できるよう）になります。

※学内ネットワークとは、キャンパス内無線 LAN（TGWIFI）や教職員が大学施設で利用している有線接続サービス等が該当します。

3.1. アプリ認証（Time based One Time Password: TOTP 方式）

認証アプリに表示される OTP（One Time Password）を利用して認証する方法です。

アプリ認証では、統合認証システムとインストールした認証アプリを連携させ、認証アプリに表示される OTP（One Time Password）を Extic 認証画面へ入力することでサービスを利用できる仕組みです。

アプリ認証を行うためには Authenticator（オーセンティケーター）と呼ばれる OTP（One Time Password）を生成するアプリケーションが必要です。

Authenticator（オーセンティケーター）は特に指定はございません。自身の利用環境に合う Authenticator を一つ選び、インストールおよび設定を行ってください。

なお、本書では参考情報として、以下に記載するアプリケーションの設定の流れを掲載しています。

Authenticator	Android	iOS	Windows	macOS
 Google Authenticator（目次参照）	○	○	×	×
 Microsoft Authenticator（目次参照）	○	○	×	×
 Google Chrome 拡張機能（目次参照）	×	×	○ (※)	○ (※)

※Google Chrome がインストールされていることが前提条件です。

【Google Authenticator を利用する場合の補足事項】

Google Authenticator を利用する場合は、設定するアカウント種別を選ぶことができます。下図を参考に自身に合ったアカウント形態を選択してください。それぞれメリットとデメリットがありますので必ずご確認ください。

アカウント形態	おすすめする方	注意点
アカウント無し	- Authenticator の使用頻度が低い方は、アカウント無しでの設定がおすすめです。 →設定が簡易で、時間がかかりません。	Google Authenticator を複数端末にインストールする場合、その都度設定作業が必要となります。

Gmail アカウント (個人所有)	・すでに個人の Gmail アカウントで Authenticator を利用中の方は、既存アカウントでの設定がおすすめです。 →複数端末で Google Authenticator を利用する場合は、設定が同期されるため都度の設定が不要です。	・ Gmail アカウントのパスワードを変更する度に再度設定が必要です。
Gmail アカウント (大学提供)	・個人の Gmail 環境を使用したくない方、業務で使用するアカウントを統一したい方は、大学提供の Gmail アカウントでの設定がおすすめです。	・統合認証アカウントのパスワードを変更する度に再度設定が必要です。 ※本院ではセキュリティ強化を目的として、一定期間ごとのパスワード変更が必須です。

3.2. メール認証 (Mail One Time Password: MOTP 方式)

登録したメールアドレス (MOTP アドレス) 宛へ送信されるメールに記載された OTP (One Time Password) を利用して認証する方法です。

メール認証では、統合認証システムに多要素認証設定で登録したメールアドレス宛へ送信されるメールに記載された OTP (One Time Password) を Extic 認証画面へ入力することでサービスを利用できる仕組みです。

個人所有のキャリアメールアドレスやフリーメールアドレス (Gmail・Yahoo mail 等) を設定してください。なお、本書では参考情報として設定の流れを掲載しています。

利用できないメールアドレス	主なメールサービス
*. tohoku-gakuin. ac. jp / *. tohoku-gakuin. jp	学生メール、教職員メール等

※大学で提供しているメールサービスを利用する際の認証でも OTP が要求されるため、設定するメールアドレスは学外のメールアドレスである必要があります。

※登録するメールアドレスで受信制限等を設定している場合は、「noreply@ex-tic.com」からのメールを受け取れるようにしてください。

3.3. FIDO2 認証 (Fast IDentity Online 2: パスワードレス方式)

端末搭載の認証器 (Touch ID / Face ID / Windows Hello) を利用した生体認証等 (FIDO2 認証の規格に準拠した機器) を利用して認証する方法です。

FIDO2 認証の設定は端末により異なるため利用ガイドは用意しておりません。

4. 利用ガイド：ログイン編

4.1. 統合認証システムと認証連携システムの認証用 URL（独自認証画面を除く）

統合認証システムと連携している本院の IT サービスのうち、多要素認証の対象であるサービスのログイン URL は以下のとおりです。（東北学院大学 IT ナビ「統合認証アカウント」参照）

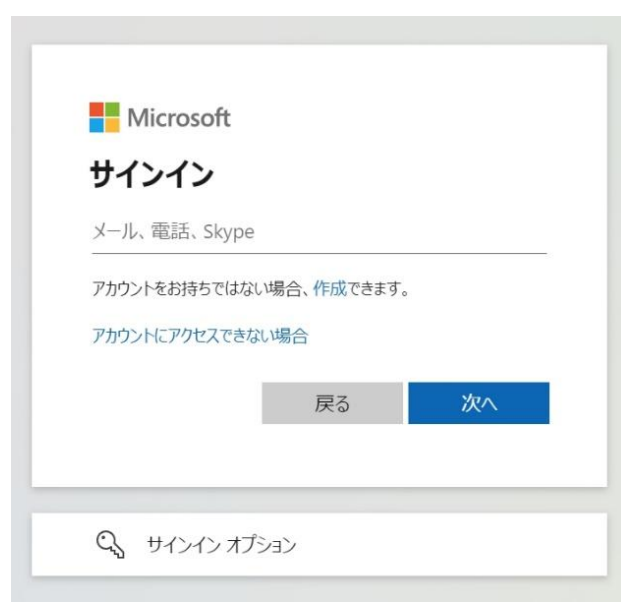
サービス・システム名称	ログイン用 URL
統合認証システム (Extic)	https://tg.ex-tic.com/
MYTG	https://unipa.mytg.tohoku-gakuin.ac.jp/uprx/ShibbolethAuthServlet
TG-folio	https://tg-folio.tohoku-gakuin.ac.jp/start/auth/login
Box	https://tohoku-gakuin.account.box.com/
SPC Leak Detection	https://spclld.spcloud.jp/lcc
教職員ポータル (Garoon)	https://tohoku-gakuin.cybozu.com/g/
DEEPMail	https://webmail.ipc.tohoku-gakuin.ac.jp/
Google Workspace for Education	https://accounts.google.com/
Microsoft365	https://portal.office.com/

※学術認証フェデレーション関連は、SP によって URL が異なるので記載を省略いたします。

※これらのサイトはすべて統合認証システムで認証を行っているため、いずれかのサービスにログインすると、同じ WEB ブラウザから他のサービスにアクセスする際に認証を省略できる場合があります。

4.2. Google アカウントと Microsoft アカウントの 2 段階認証

前節で記載したサービスやシステムの内、Google アカウントと Microsoft アカウントはそれぞれ、専用サイトにて、利用するためのアカウントを指定する必要があるため、他のサービスと異なり、2 段階の認証が要求されます。

Google アカウント	Microsoft アカウント
Step1	Step1
https://accounts.google.com/	https://portal.office.com/
 The image shows the Google Chrome login page. It features the Google logo at the top, followed by the text 'Chrome へのログイン' and 'お客様の Google アカウントを使用'. Below this is a text input field for 'メールアドレスまたは電話番号'. There are links for 'メールアドレスを忘れた場合' and 'ご自分のパソコンでない場合は、ゲストモードを使用して非公開でログインしてください。'. At the bottom, there is a link to 'アカウントを作成' and a blue button labeled '次へ'.	 The image shows the Microsoft sign-in page. It features the Microsoft logo at the top, followed by the text 'サインイン'. Below this is a text input field for 'メール、電話、Skype'. There are links for 'アカウントをお持ちではない場合、作成できます。' and 'アカウントにアクセスできない場合'. At the bottom, there are two buttons: '戻る' and '次へ'.
学生：{統合認証アカウント} @g. tohoku-gakuin. ac. jp	学生：{統合認証アカウント} @m. tohoku-gakuin. ac. jp
職員：{統合認証アカウント} @g. tohoku-gakuin. ac. jp {統合認証アカウント} @g. tohoku-gakuin. jp	職員：{統合認証アカウント} @m. tohoku-gakuin. jp
Step2	Step2
 The image shows the Tohoku Gakuin login screen. It features a blue background with a white login box. The box contains the text '学校法人 東北学院' and a list of instructions. Below the instructions is a text input field for 'ユーザー名' and a blue button labeled '次へ'.	 The image shows the Tohoku Gakuin login screen. It features a blue background with a white login box. The box contains the text '学校法人 東北学院' and a list of instructions. Below the instructions is a text input field for 'ユーザー名' and a blue button labeled '次へ'.
専用サイトで Google アカウントを指定したあとは統合認証システムに自動遷移するので以降の手順は他のサービスと同様となります。	専用サイトで Microsoft アカウントを指定したあとは統合認証システムに自動遷移するので以降の手順は他のサービスと同様となります。

4.3. 統合認証システムでの ID とパスワード認証、パスワードレス認証（FIDO2 認証）

本節では統合認証システム (Extic) や認証連携システム（独自認証画面を除く）での統合認証アカウントを利用した認証方法を記載します。

※初期パスワードの変更、多要素認証のアプリ認証・メール認証、パスワード再発行用メールアドレスの登録が完了している前提で記載します。

※学外ネットワークからの利用の場合は、次節記載の多要素認証も要求されます。

※パスワードレス認証は試験的な運用となります。

- 1) [ユーザー名]にログインしたい統合認証アカウントの ID を入力し、[次へ]をクリックします。

※WEB ブラウザ (Google Chrome、Safari、Microsoft Edge 等) の言語設定により英語表記になる場合があります。

※統合認証アカウントの ID を半角英数字小文字で入力してください。

利用者ガイド等の利用の詳細はこちら

- 2) [パスワード]にログインしたい統合認証アカウントのパスワードを入力し、[次へ]をクリックします。

※ログインを 5 回連続で失敗するとアカウントが一時的にロックされ、ログインできなくなります（一時ロック：30 分間（解除不可））。

※多要素認証の FIDO2 認証を設定済みの方は、設定済みのデバイスからのご利用であれば、左図の[パスワードレス認証]を選択することで、パスワードを入力せず、ログインができます。FIDO2 認証で登録したデバイスでの認証でない場合は、[パスワード]タブを選択すると、上の図のようにパスワード入力画面が表示されますのでパスワードを入力し、[次へ]をクリックします。

＜多要素認証の FIDO2 認証未設定の場合のパスワード認証画面＞

The screenshot shows a login interface for '学校法人 東北学院' (Seiwa Gakuin University). It features a blue header with the university logo. Below the header, there is a white box containing instructions in Japanese about the authentication system and login rules. A red rectangle highlights the 'パスワード' (Password) input field and the '次へ' (Next) button. Below the input field is a 'キャンセル' (Cancel) button. At the bottom, there are links for 'パスワードを忘れましたか' (Forgot your password?), 'メンテナンス情報はこちら' (Maintenance information is here), and '東北学院大学ITナビ' (Seiwa Gakuin University IT Navi). The footer indicates '© 2016 EXIGEN NETWORKS Co., Ltd.'.

＜多要素認証の FIDO2 認証設定済の場合のパスワードレス認証画面＞

The screenshot shows a login interface for '学校法人 東北学院' (Seiwa Gakuin University). It features a blue header with the university logo. Below the header, there is a white box containing two tabs: 'パスワードレス' (Passwordless) and 'パスワード' (Password). The 'パスワード' tab is selected and highlighted with a red rectangle. Below the tabs is a large blue button labeled 'パスワードレス認証' (Passwordless authentication) and a 'キャンセル' (Cancel) button. At the bottom, there are links for 'パスワードを忘れましたか' (Forgot your password?), 'メンテナンス情報はこちら' (Maintenance information is here), and '東北学院大学ITナビ' (Seiwa Gakuin University IT Navi). The footer indicates '© 2016 EXIGEN NETWORKS Co., Ltd.'.

ここをクリックすると上の画面に遷移

4.4. 統合認証システムでの多要素認証

本節では、学外ネットワークからの接続の際、「4.3. 統合認証システムでの ID とパスワード認証」の認証の後に多要素認証が要求された場合の認証方法を説明します。まず、認証手順を説明する前に、多要素認証のアプリ認証、メール認証、FIDO2 認証の設定状態の組合せにより次のように認証画面が変動します。

■FIDO2 認証設定時と通常パスワード認証時の画面差

多要素認証 FIDO2 未設定	多要素認証 FIDO2 設定済

※パスワードレス認証＝多要素認証の扱いであるため、学外ネットワークからでも 2 段階認証は不要です。

■ID とパスワード認証後の多要素認証画面差

アプリ認証のみ		メール認証のみ		FIDO2 認証のみ			
アプリ認証とメール認証		アプリ認証と FIDO2 認証		メール認証と FIDO2 認証		すべて	

※複数設定パターンでアプリ認証をクリックすると[アプリ認証のみ]の画面に、メール認証をクリックすると[メール認証のみ]の画面に、パスワードレス認証をクリックすると[FIDO2 認証のみ]に遷移します。

※以降に ID とパスワード認証後の多要素認証利用手順を記載しますが、前提として、「4. 3. 統合認証システムでの ID とパスワード認証」の後からの手順となります。また、多要素認証を複数設定しているかの状態は利用者の設定状況によるため、ここでは「アプリ認証のみ」と「メール認証のみ」を掲載します。

<メール認証のみ>

- 1) [ワンタイムパスワードを送信]をクリックします。



- 2) ワンタイムパスワードを送信したメッセージを確認してから、メール認証設定を行ったメールアドレスのメールボックスを確認し、ワンタイムパスワードを確認します。
- 3) 2)で確認したワンタイムパスワードを[ワンタイムパスワード]に入力し、[次へ]をクリックします。



※ワンタイムパスワードは10分程度で有効期限が切れるので、期限内か確認し、期限が切れている場合は再度1)を行ってください。

<アプリ認証のみ>

1) アプリ認証設定を行ったアプリケーションを起動し、ワンタイムパスワードを確認します。

2) 1)で確認したワンタイムパスワードを[ワンタイムパスワード]に入力し、[次へ]をクリックします。

※ワンタイムパスワードは 20-30 秒程度で自動更新されるので、入力する時間が少ない場合は一度更新されるのを待ってから入力することを推奨します。



5. 設定概要：統合認証システムにおける必須設定項目

5.1. 統合認証アカウントを新規で発行された方

初期状態の統合認証アカウントでは、本院の IT サービスを利用できないため、アカウントを新規で発行された方（学生・教職員）は、各自で次の設定を必ず行ってください。

①	初期パスワードの変更	アカウント利用準備システム利用者マニュアル参照
②	多要素認証：アプリ認証の登録	7 章参照
③	多要素認証：メール認証の登録	アカウント利用準備システム利用者マニュアル参照
④	パスワード再発行用メールアドレスの登録	アカウント利用準備システム利用者マニュアル参照

アカウント利用準備システムでは、上記 4 項目のうち、②以外を一括で設定することができます。設定手順は、「アカウント利用準備システム利用者マニュアル」をご参照ください。

なお、一度設定した後の変更には、統合認証システムをご利用ください。

5.2. 統合認証アカウントの設定を変更したい方

パスワードを変更したい	1-1	現在のパスワードが分かる[6.1 節参照]
	1-2	現在のパスワードが分からない、パスワードの有効期限が切れた[6.2 節参照]
	1-3	1-2 でメールが届かない[2.5 節参照] ※「■パスワード再発行手続きについて」の2項目
多要素認証：アプリ認証の登録	2-1	多要素認証のアプリ認証の登録 多要素認証のアプリ認証の変更[7 章参照]
多要素認証：メール認証の登録	3-1	多要素認証のメール認証の登録 多要素認証のメール認証の変更[8 章参照]
パスワード再発行用メールアドレスの登録	4-1	パスワード再発行用メールアドレスの登録 パスワード再発行用メールアドレスの変更[9 章参照]
多要素認証：FIDO2 認証の登録	5-1	手順の用意はありません。

6. 設定ガイド①：統合認証アカウントのパスワード変更

6.1. パスワード変更手順①（現在のパスワードが分かる）

多要素認証：FIDO2 認証が未設定であることを前提に記載します。

FIDO2 認証を設定している場合、認証画面の外観が変わるため、4.3 節を参考にしてください。

- 1) 統合認証システム(Extic)のパスワード変更サイト
(<https://tg.ex-tic.com/idm/user/password/>) にアクセスすると、次のようなログイン画面が表示されます。



The screenshot shows the login page for 学校法人 東北学院 (Hokkai Gakuin University). It includes a login form with fields for ユーザー名 (Username) and a button labeled 次へ (Next). A red box highlights the login instructions and a warning about account lockout after 5 failed attempts. Another red box highlights the footer text: パスワードを忘れましたか (Forgot your password?), メンテナンス情報はこちら (Maintenance information is here), and 東北学院大学ITナビ (Hokkai Gakuin University IT Navigator). Two callout boxes provide additional information: one points to the login instructions stating '注意事項を記載。都度更新されます。' (Notes are recorded. Updated regularly.), and another points to the footer stating '利用者ガイド等の利用の詳細はこちら' (Details of using the User Guide, etc., are here).

- 2) [ユーザー名]にログイン
したい統合認証アカウン
トの ID を入力し、[次へ]
をクリックします。

※WEB ブラウザ (Google Chro
me、Safari、Microsoft Edge
等) の言語設定により英語表
記になる場合があります。

※統合認証アカウントの ID を
半角英数字小文字で入力して
ください。

- 3) [パスワード]にログイン
したい統合認証アカウン
トのパスワードを入力
し、[次へ]をクリックし
ます。

※ログインを 5 回連続で失敗
するとアカウントが一時的に
ロックされ、ログインできな
くなります (一時ロック：30
分間 (解除不可))。

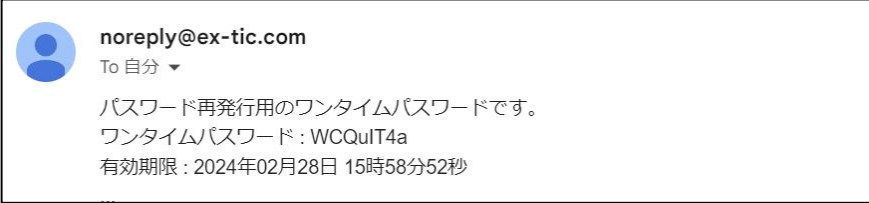
※WEB ブラウザが ID とパスワ
ードを記憶するか確認がある
場合は任意で設定してくださ
い。ただし、初期設定の場
合、初期パスワードはすぐに
変更するので、この場合は記
憶させないことを推奨しま
す。

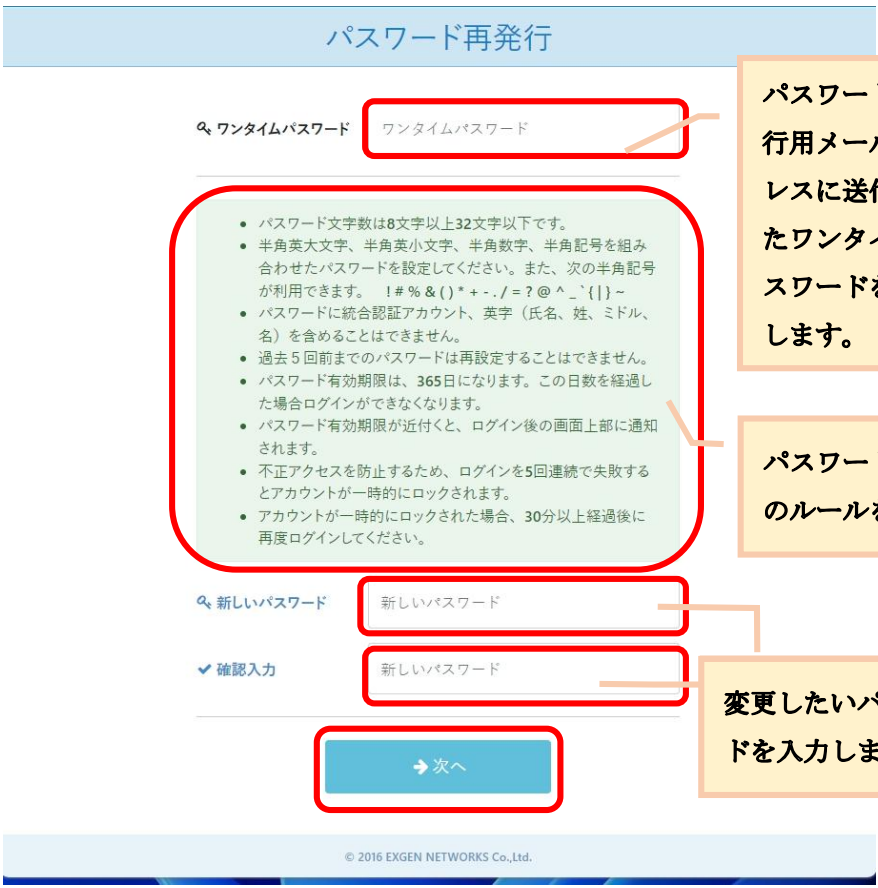
4) 条件分岐	■初期設定の方、既存アカウントで学内ネットワークから接続の方 自動で 5) に進みます。 ■既存アカウントで多要素認証未設定の方 「7. 設定ガイド②：多要素認証（アプリ認証）を設定する」と「8. 設定ガイド③：多要素認証（メール認証）を設定する」の両方の設定を行って から、画面上部の[パスワード変更]タブを選択すると 5) に進みます。  ■既存アカウントで多要素認証設定済で学外ネットワークから接続の方 利用者の多要素認証の設定に応じて認証画面が異なります。4.4 節記載の いずれかの認証方法で、多要素認証を行うと 5) に進みます。
5) [現在のパスワード]にログインで利用したパスワードを入力します。 6) 「新しいパスワード」と「新しいパスワードの確認」にパスワード設定のルールを満たす新しいパスワードを入力します。 ※入力ミスで再ログインがで きるケースが多いです。手 入力ではなく、Word やエディ タなどで入力した文字列が目 に見える状態のものをコピー し、貼り付ける方法での設定 することを推奨します。特に 記号はスマートフォンで入力 しやすいものを選択すること も踏まえ設定してください。 7) 「保存」をクリックしま す。	■初期設定時の画面（状態によりタブに表示される項目が変わります。）  初期パスワード or 既存パスワード パスワード設定 のルールを確認 変更したいパスワー ドを入力します。 ■初期設定パスワード変更後の統合認証システムのタブ  ■初期設定パスワード、多要素認証設定後の統合認証システムのタブ 

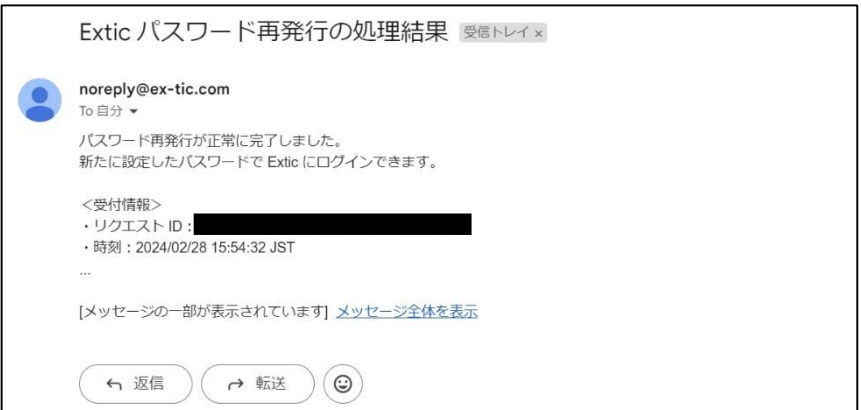
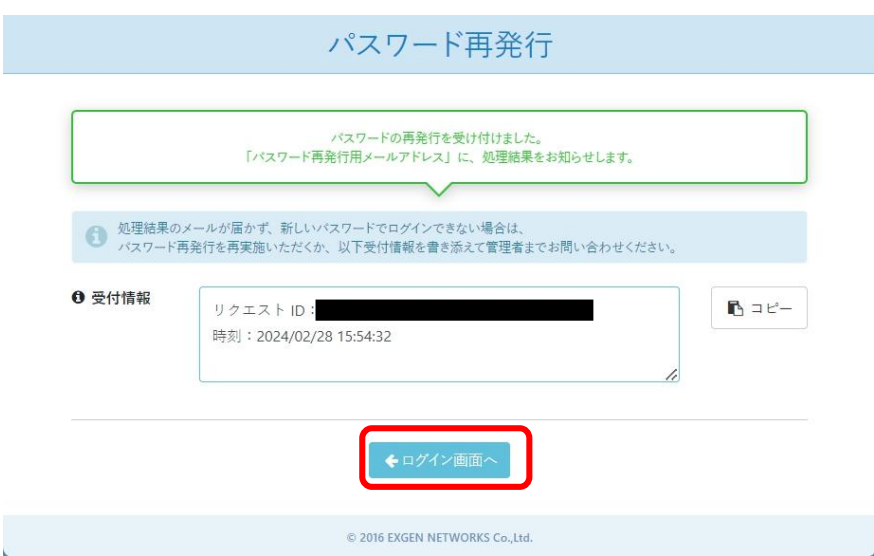
8) パスワード処理の結果の画面が表示されますので [結果] が処理中の表示から変わるまで、何度か [更新] をクリックします。	
9) [結果] が成功となれば、パスワード変更は完了です。 ※「2.5. 利用上の注意」に記載のとおり、連携システムに変更したパスワードが同期されるのに、数分から数時間程度かかる場合があります。まずは、変更したパスワードでログインを試みていただき、仮にログインができない場合は、数分お待ち頂き、それでもログインができない場合は、パスワード変更前のパスワードでログインを行ってください。	

6.2. パスワード変更手順②（現在のパスワードが分からない、パスワードの有効期限が切れた）

本手順は、利用者が「パスワード再発行用メールアドレス」を事前登録している場合のみ利用できます。パスワード再発行用メールアドレスを事前登録していなかった場合や、パスワード再発行用メールアドレスにメールが届かない場合は、2.5. 節の「パスワード再発行手続きについて」をご確認ください。

1) 統合認証システム(Extic) (https://tg.ex-tic.com/) にアクセスし、ログイン画面の下部にある[パスワードを忘れましたか]をクリックします。 	
2) [メールアドレス]に利用者にて設定したパスワード再発行用メールアドレスを入力し、[送信する]をクリックします。 事前に登録したパスワード再発行用メールアドレスを入力	
3) 事前に登録したパスワード再発行用メールアドレス宛にワンタイムパスワードが送付されることを確認します。 ※メールが届かない場合この機能は利用できません。2.5 節記載の手続きに移行してください。	 ※特定条件でスレッドとしてグループ化され表示がされる場合があります。有効期限等確認し、最新のものを利用ください。または、ご利用のメールのスレッド表示を解除もご検討ください。

4) 「ワンタイムパスワード」に3) で届いたワンタイムパスワードを入力します。 5) 「新しいパスワード」と「確認入力」にパスワード設定のルールを満たす新しいパスワードを入力します。 ※入力ミスで再ログインができなくなるケースが多いです。手入力ではなく、Word やエディタなどで入力した文字列が目に見える状態のものをコピーし、貼り付ける方法で設定することを推奨します。 6) 「次へ」をクリックします。	 パスワード再発行 ワンタイムパスワード 新しいパスワード 確認入力 次へ パスワード再発行の処理を受け付けたと表示されます。
7) パスワード再発行の処理を受け付けたと表示されます。	 パスワード再発行 パスワードの再発行を受け付けました。 「パスワード再発行用メールアドレス」に、処理結果をお知らせします。 処理結果のメールが届かず、新しいパスワードでログインできない場合は、 パスワード再発行を再実施いただくか、以下受付情報を書き添えて管理者までお問い合わせください。 受付情報 リクエスト ID: [redacted] 時刻: 2024/02/28 15:54:32 コピー ログイン画面へ パスワード再発行の処理を受け付けたと表示されます。

8) 処理が完了すると、パスワード再発行用メールアドレス宛に連絡が届きますので、このメールの受信をもってパスワード変更は完了となります。	
9) 8)のメールを確認してから、[ログイン画面へ]をクリックし、設定変更したパスワードでログインができるかお試しください。	

7. 設定ガイド②：多要素認証（アプリ認証）を設定する

ご利用の端末によって設定方法が異なりますので、ご自身の環境に合わせて設定を行ってください。

- スマートフォンまたはタブレットをお持ちの方
⇒ 「6.1. Google Authenticator または Microsoft Authenticator を利用する場合」へ
- スマートフォンまたはタブレットをお持ちでない方（PC 利用）
⇒ 「6.2. Google Chrome 拡張機能を利用する場合」へ

7.1. Google Authenticator または Microsoft Authenticator を利用する場合

本節でのアプリ認証の設定は、以下の流れで行います。

1. アプリケーションの初期設定
2. 統合認証システム(Extic)での設定画面の表示
3. アプリケーションでの統合認証アカウントの登録
4. 統合認証システム(Extic)での設定

以降の手順は設定する前に次の点をご確認ください。

- ・アプリ認証をインストールする端末は常に携帯するスマートフォンやタブレットを推奨します。
- ・アプリ認証の設定は、QRコードを利用する方法と、セットアップキーを利用する方法があります。
 - ※ QRコードを利用する場合、QRコードの撮影が必要であるため端末が2台必要となります。
 - ※ セットアップキーを利用する場合、端末1台で設定可能です。
- ・アプリケーションはアップデート等で画面イメージがすぐに更新されます。また、すでに個人で学外のサービス利用でご利用いただいている場合や端末のダークモード、画面設定など、利用者環境に応じて設定の流れや画面イメージが異なることがありますので、本書掲載事項は参考としてご認識いただき、本書にとらわれずアプリの指示に従って設定を行ってください。

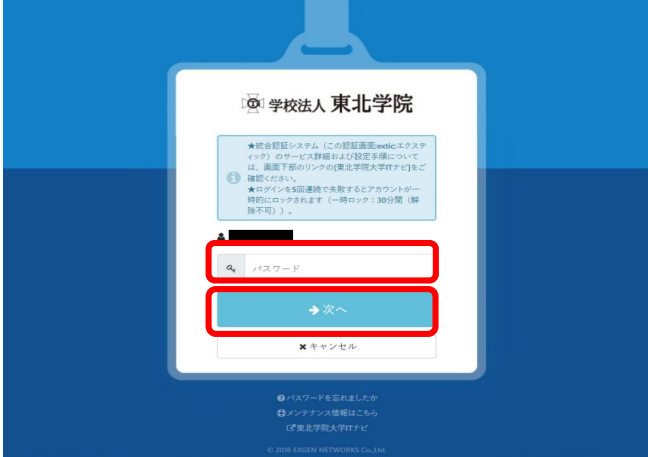
(1) アプリケーションの初期設定

	Google Authenticator	Microsoft Authenticator
1) スマートフォンまたはタブレットにアプリケーションをインストールします。	iOS(AppStore)  Android(GooglePlay) 	iOS(AppStore)  Android(GooglePlay) 
2) アプリケーションを起動し、画面の内容に沿って操作を進めます。		

3) 使用するアカウント形態によって、操作方法が異なります。 ➤ 個人所有または大学提供の Gmail アカウントで設定する場合 画面の流れに従ってサインインを行います。 ➤ アカウント無しで設定する場合 [アカウントなしで使用／スキップ]をクリックします。		
4) 右図のような画面が表示されましたら、次の設定手順へお進みください。		

(2) 統合認証システム(Extic)での設定画面の表示

以降手順上、毎回ログインを行うように記載がされておりますが、すでにログイン済みであれば、認証手順は読み飛ばしてください。また、多要素認証の FID02 認証未設定の前提で記載します。FID02 認証を設定済みの場合、パスワード入力画面のデザインが変わります。その際の手順は 4.3 節を参考にしてください。

1) 統合認証システム(Extic) (https://tg.extic.com/) にアクセスし、[ユーザー名]にログインしたい統合認証アカウントの ID を入力し、[次へ]をクリックします。 ※WEB ブラウザ (Google Chrome、Safari、Microsoft Edge 等) の言語設定により英語表記になる場合があります。 ※統合認証アカウントの ID を半角英数字小文字で入力してください。	
2) [パスワード]にログインしたい統合認証アカウントのパスワードを入力し、[次へ]をクリックします。 ※ログインを 5 回連続で失敗するとアカウントが一時的にロックされ、ログインできなくなります (一時ロック：30 分間 (解除不可))。	
3) 条件分岐	■初期設定の方 初回パスワード変更後の流れであれば自動で 5) に進みます。 ■既存アカウントで多要素認証未設定の方 自動で 5) に進みます。 ■既存アカウントで学内ネットワークから接続の方 自動で 4) に進みます。 ■既存アカウントで多要素認証設定済で学外ネットワークから接続の方 利用者の多要素認証の設定に応じて認証画面が異なります。4.4 節記載のいずれかの認証方法で、多要素認証を行うと 4) に進みます。

- 4) ログイン後、画面上部の[多要素認証 (OTP)]をクリックしてください。



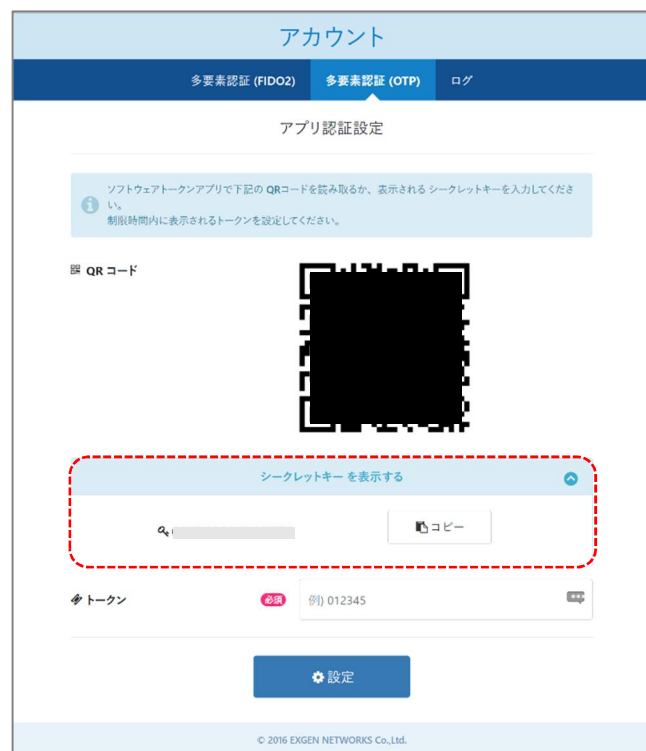
- 5) [アプリ認証]の[設定]をクリックします。

※ スマートフォンの機種変更等で連携済みのアプリを変更したい場合は、[解除]をクリックし、表示されるポップアップの[解除]を選択してから再設定をします。

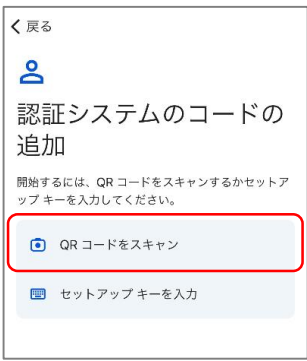
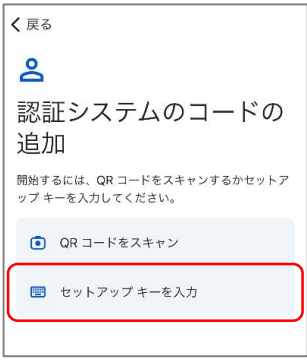


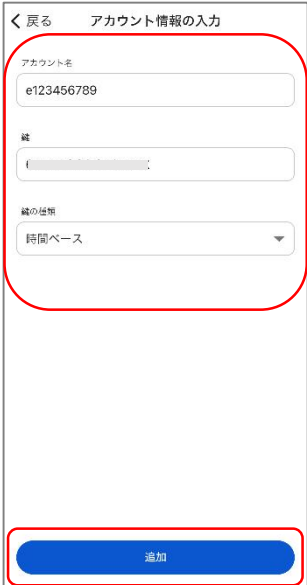
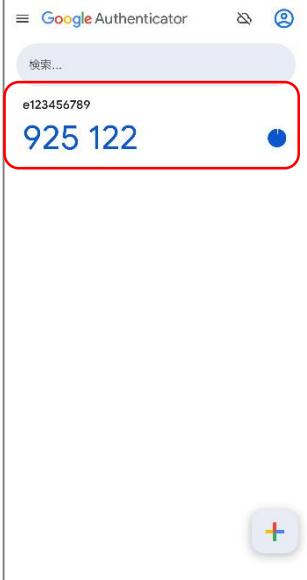
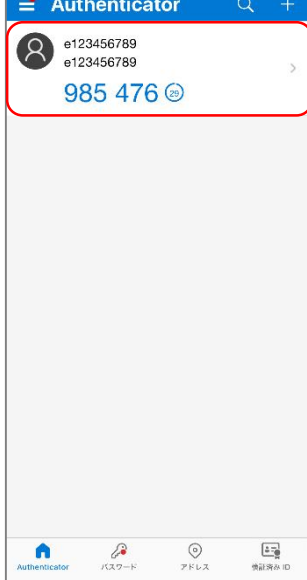
- 6) QR コードが表示されるので、次の設定手順に進んでください。

※シークレットキーは、アプリケーションを操作するスマートフォンまたはタブレット以外の機器をお持ちでない場合に必要となります。必要に応じて、「シークレットキーを表示する」よりご確認ください。



(3) アプリケーションでの統合認証アカウントの登録

	Google Authenticator	Microsoft Authenticator
1) アプリケーションのホーム画面を開き、[コード/アカウントを追加]をクリックします。		
2) 条件分岐 ・端末 2 台で作業している場合は、<u>QR コードを用いた設定</u>へ ・端末 1 台で作業している場合は、<u>セットアップキーを用いた設定</u>へ		
■ <u>QR コードを用いた設定</u> ※別の端末で QR コードを表示できる場合のみ、利用できます。 ➤ Google Authenticator [QR コードをスキャン]をクリックします。 ➤ Microsoft Authenticator [その他]をクリックします。 カメラが起動しますので、別の端末で表示している Extic 設定画面の QR コードを読み取ります。		
■ <u>セットアップキーを用いた設定</u> ➤ Google Authenticator [セットアップキーを入力]をクリックします。 ➤ Microsoft Authenticator [その他]をタップし、カメラ画面で[またはコードを手動で入力]をクリックします。		

アカウント情報の入力画面に遷移しますので、次の情報を入力し、[追加/完了]をクリックします。 ・アカウント名： 統合認証アカウントのユーザーID ・鍵／秘密鍵： Extic の設定画面で表示された シークレットキー ・鍵の種類（Google Authenticator のみ）： 時間ベース		
3) 6桁のワンタイムパスワードが表示されたら、次の設定手順へお進みください。		

(4) 統合認証システム(Extic)での設定

- 1) Extic の設定画面に戻り、[トークン]にアプリケーションで表示されたワンタイムパスワードを入力し、[設定]をクリックします。

※ワンタイムパスワードは 20-30 秒程度で自動更新されるので、入力する時間が少ない場合は一度更新されるのを待ってから入力することを推奨します。

- 2) [アプリ認証]が設定済に変われば完了です。

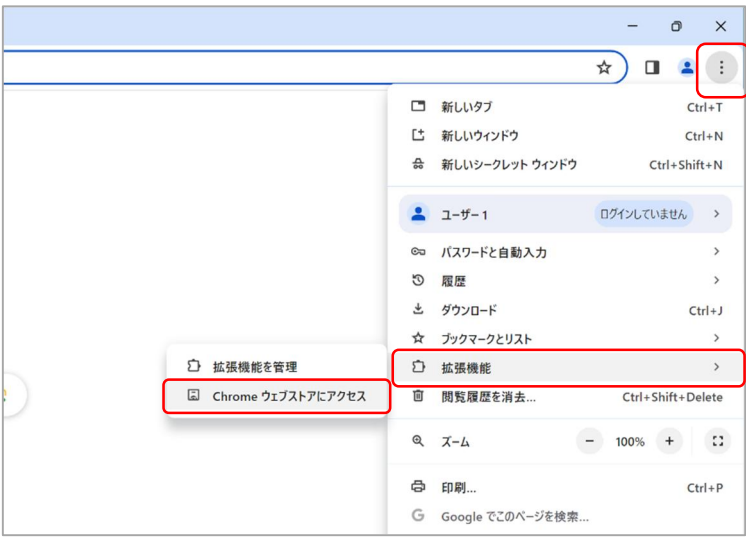
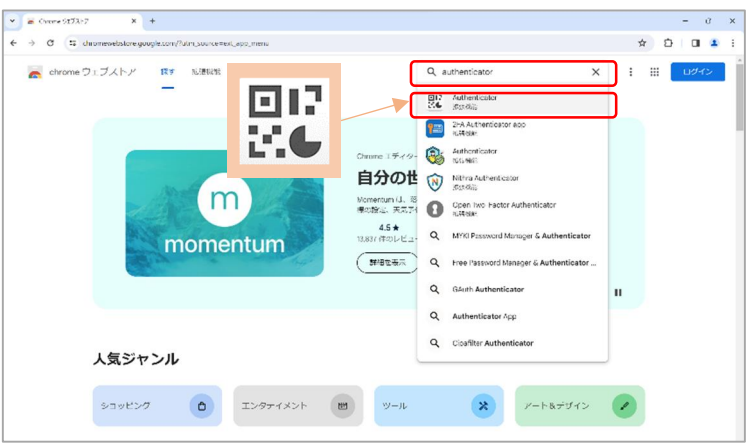
7.2. Google Chrome 拡張機能を利用する場合

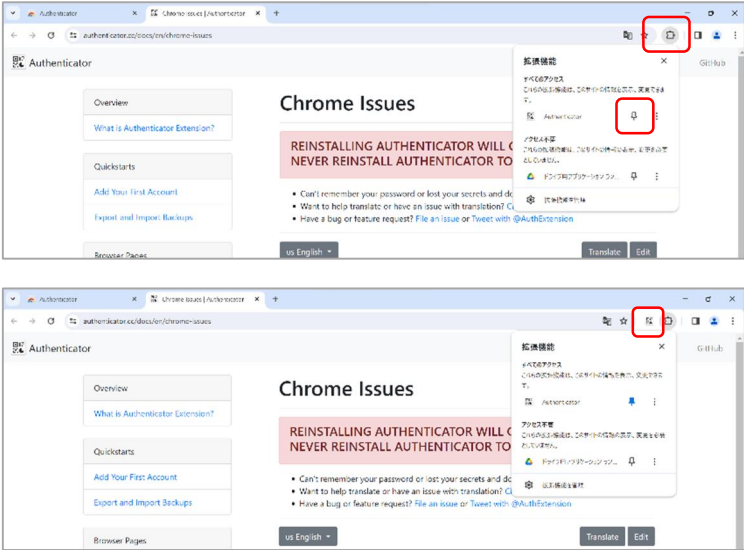
以降の手順は設定する前に次の点をご確認ください。

- ・Google Chrome 拡張機能での利用を推奨する方は次のような方になります。
 - ・スマートフォンまたはタブレットをお持ちでない方
 - ・スマートフォンに Authenticator をインストールしたくない方で、かつ、ノート PC を常に持ち歩く方
 - ・学外から統合認証アカウントを利用しない方で、かつ、事務室などの常設 PC のみをご利用の方
- ・以降の手順は PC に Google Chrome がインストールされていることが前提で記載します。
- ・ゲストモードやシークレットモードでは拡張機能を追加できません。
- ・学生・教職員共用 Google アカウント (@g. tohoku-gakuin. ac. jp) は拡張機能をご利用できません。個人所有の Gmail アカウントで WEB ブラウザにサインインするか、教職員専用 Google アカウント (@g. tohoku-gakuin. jp) をご利用ください。
- ・アプリケーションはアップデート等で画面イメージがすぐに更新されます。また、すでに個人で学外のサービス利用でご利用いただいている場合や端末のダークモード、画面設定など、利用者環境に応じて

設定の流れや画面イメージが異なることがありますので、本書掲載事項は参考としてご認識いただき、本書にとらわれずアプリの指示に従って設定を行ってください。

(1) アプリケーションの初期設定

1) Google Chrome を起動し、画面右上の [:] > [拡張機能] > [Chrome ウェブストアにアクセス] をクリックします。	
2) 検索窓に [Authenticator] と入力します。今回は右図アイコンの Authenticator を使用しますので、表示された候補の中からクリックします。	
3) [Chrome に追加] をクリックし、[拡張機能を追加] してください。	

4) 右図のような画面が表示されましたら、画面右上の[拡張機能アイコン (パズルのピースのようなマーク)] をクリックし、Authenticator を[ピン留め]すると、画面上部に追加した拡張機能のアイコンが表示されます。 5) 次の設定手順へお進みください。	
---	--

(2) 統合認証システム (Extic) での設定画面の表示と設定

1) 「7.1. Google Authenticator または Microsoft Authenticator を利用する場合」の「(2) 統合認証システム (Extic) での設定画面の表示」に記載している手順(1)～(5)と同様の手順を行ってください。	
2) QR コードの画面が表示されますので、ピン留めした[Authenticator]アイコンをクリックします。	

- 3) [鉛筆マーク]をクリックしてください。



- 4) [+]マーク>[QR コードをスキャン]をクリックします。



5) QR コードをカーソルで囲むよう指示されますので、Extic のアカウント画面に表示されている QR コードを囲みます。(カーソルを QR コードの左上に移動させ、マウスの左クリックを押しながら、右下へ動かすことで囲めます) 6) 成功すると「●●追加されました。」というメッセージが表示されますので、「OK」をクリックします。	
7) 設定完了後、Google Chrome の「Google Authenticator アイコン」をクリックします。 8) ワンタイムパスワードが表示されますので、アプリ認証設定の「トークン」に入力し、「設定」をクリックします。	
9) [アプリ認証]が設定済に変われば完了です。	

8. 設定ガイド③：多要素認証（メール認証）を設定する

以降手順上、毎回ログインを行うように記載されていますが、すでにログイン済みであれば、認証手順は読み飛ばしてください。また、多要素認証の FIDO2 認証未設定の前提で記載します。FIDO2 認証を設定済みの場合、パスワード入力画面のデザインが変わります。その際の手順は 4.3 節を参考にしてください。

- 1) 統合認証システム(Extic) (<https://tg.ex-tic.com/>) にアクセスし、[ユーザー名]にログインしたい統合認証アカウントの ID を入力し、[次へ]をクリックします。

※WEB ブラウザ (Google Chrome、Safari、Microsoft Edge 等) の言語設定により英語表記になる場合があります。

※統合認証アカウントの ID を半角英数字小文字で入力してください。

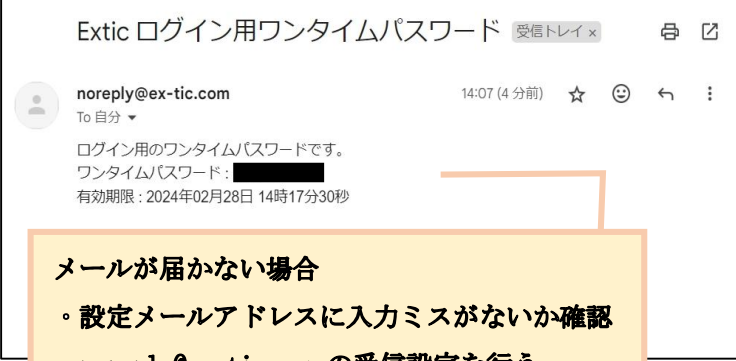


- 2) [パスワード]にログインしたい統合認証アカウントのパスワードを入力し、[次へ]をクリックします。

※ログインを 5 回連続で失敗するとアカウントが一時的にロックされ、ログインできなくなります（一時ロック：30 分間（解除不可））。



3) 条件分岐	■初期設定の方 初回パスワード変更後の流れであれば自動で 5) に進みます。 ■既存アカウントで多要素認証未設定の方 自動で 5) に進みます。 ■既存アカウントで学内ネットワークから接続の方 自動で 4) に進みます。 ■既存アカウントで多要素認証設定済で学外ネットワークから接続の方 利用者の多要素認証の設定に応じて認証画面が異なります。 4. 4 節記載のいずれかの認証方法で、多要素認証を行うと 4) に進みます。
4) ログイン後、画面上部の[多要素認証 (OTP)]をクリックしてください。	
5) [メール認証]の[設定]をクリックします。 ※登録しているメールアドレスを変更したい場合は、[解除]をクリックし、表示されるポップアップの[解除]を選択してから再設定をします。 	■多要素認証設定状態により画面の状態が異なります 

6) [メールアドレス]に個人所有のメールアドレスを入力します。 ※パスワード再発行用メールアドレスと同じアドレスの登録を推奨します。	
メールアドレスに「tohoku-gakuin.ac.jp」と「tohoku-gakuin.jp」が含まれているものは登録できません。また、この設定は統合認証システム内でユニークである必要があります。複数のアカウントをご利用の場合は同一のアドレスは設定できません。	
7) [メールアドレス] の入力後、[ワンタイムパスワードを送信する]をクリックします。 ※このメッセージは送信を試みたという意味で、メールアドレスが存在せず、実際には送信が行えない場合も同様のメッセージがでます。	
8) [メールアドレス]に設定したメールアドレスでワンタイムパスワードのメールを受信できたことを確認します。 ※ワンタイムパスワードの有効期間は約 10 分です。	 メールが届かない場合 ・設定メールアドレスに入力ミスがないか確認 ・noreply@ex-tic.com の受信設定を行う (やり方はご利用サービスにご確認ください) ・別のメールアドレスを試す

- 9) 8) で届いたワンタイムパスワードを
[ワンタイムパスワード]に入力し、
[設定]をクリックします。

- 10) [メール認証]が設定済に変われば完了です。

※[設定済]の横の[i]にカーソルを合わせると現在設定のメールアドレスを確認できます。

※メール認証の再設定を行い、登録しているアドレスを変更した場合は、併せて「パスワード再発行用メールアドレス」の変更も行ってください。(9章参照)

9. 設定ガイド④：パスワード再発行用メールアドレスの登録

以降手順上、毎回ログインを行うように記載がされておりますが、すでにログイン済みであれば、認証手順は読み飛ばしてください。また、多要素認証の FIDO2 認証未設定の前提で記載します。FIDO2 認証を設定済みの場合、パスワード入力画面のデザインが変わります。その際の手順は 4.3 節を参考にしてください。

- 1) 統合認証システム(Extic) (<https://tg.ex-tic.com/>) にアクセスし、[ユーザー名]にログインしたい統合認証アカウントの ID を入力し、[次へ]をクリックします。

※WEB ブラウザ (Google Chrome、Safari、Microsoft Edge 等) の言語設定により英語表記になる場合があります。

※統合認証アカウントの ID を半角英数字小文字で入力してください。

- 2) [パスワード]にログインしたい統合認証アカウントのパスワードを入力し、[次へ]をクリックします。

※ログインを 5 回連続で失敗するとアカウントが一時的にロックされ、ログインできなくなります (一時ロック：30 分間 (解除不可))。

3) 条件分岐	■初期設定の方 初回パスワード変更、および、多要素認証の設定の流れであればすでにログイン済みですので、4)に進んでください。もし、初回パスワード変更、および、多要素認証の設定前であれば、自動的に設定が必要な画面に遷移しますので該当する手順をご確認ください。 ■既存アカウントで多要素認証未設定の方 「7. 設定ガイド②：多要素認証（アプリ認証）を設定する」と「8. 設定ガイド③：多要素認証（メール認証）を設定する」の両方の設定を行ってから、画面上部の[プロフィール]タブを選択すると 5)に進みます。  ■既存アカウントで学内ネットワークから接続の方 自動で 4)に進みます。 ■既存アカウントで多要素認証設定済で学外ネットワークから接続の方 利用者の多要素認証の設定に応じて認証画面が異なります。4.4 節記載のいずれかの認証方法で、多要素認証を行うと 4)に進みます。
4) ログイン後、画面上部の[プロフィール]をクリックしてください。	

- 5) [パスワード再発行用メールアドレス]に個人所有のメールアドレスを入力します。

※多要素認証（メール認証）と同じアドレスの登録を推奨します。

メールアドレスに「tohoku-gakuin.ac.jp」と「tohoku-gakuin.jp」が含まれているものは登録できません。また、この設定は統合認証システム内でユニークである必要があります。複数のアカウントをご利用の場合は同一のアドレスは設定できません。

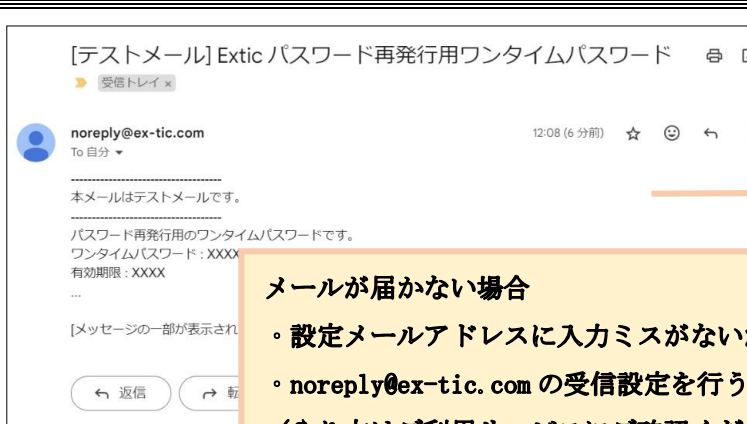
- 6) [パスワード再発行用メールアドレス]の入力後、[テストメールを送信する]をクリックします。

※登録だけで満足し、メール受信確認を怠り、登録ミス等を検知できないケースが多く発生しています。必ずテストメールを受信できることを確認してください。

- 7) [パスワード再発行用メールアドレス]に設定したメールアドレスに「テストメールを送信した」というメッセージが表示されることを確認します。

※このメッセージは送信を試みたという意味で、メールアドレスが存在せず、実際には送信が行えない場合も同様のメッセージがでます。

- 8) [パスワード再発行用メールアドレス]に設定したメールアドレスでテストメールが受信できたことを確認します。



メールが届かない場合

- ・ 設定メールアドレスに入力ミスがないか確認
- ・ noreply@ex-tic.com の受信設定を行う
(やり方はご利用サービスにご確認ください)
- ・ 別のメールアドレスを試す

- 9) テストメールの受信が確認できたら、再度設定画面にもどり、[保存]をクリックします。



右のようなメッセージがでた場合は、5) に戻り、別のメールアドレスを設定ください。

入力されたパスワード再発行用メールアドレスはすでに登録されています。別のメールアドレスを入力してください。

入力されたパスワード再発行用メールアドレスは利用できません。別ドメインのメールアドレスを入力してください。

- 10) プロフィール更新の結果の画面が表示されますので[結果]が処理中の表示から変わるまで、何度か[更新]をクリックします。
- 11) プロフィール更新の[結果]が成功となれば、パスワード再発行用メールアドレスの登録は完了です。

※パスワード再発行用メールアドレスの再設定を行い、登録しているアドレスを変更した場合は、併せて「多要素認証設定のメール認証」の登録も変更してください。(8章参照)

