多要素認証 CAS
認証シード登録手順書

第 1.3 版

2022 年 1 月 26 日

多要素認証 CAS

多要素認証 CAS では、名大ID とパスワードの他に、
「認証コード」と呼ばれる 30 秒ごとに変化する 6 桁の数字を認証に用います(下図参照)。

この認証コードは、認証シードを登録した認証アプリ(スマホ、PC)、もしくは、ハードウェアトークンに表示された物を使います。ハードウェアトークンは購入に公費や私費の支出を伴うため、なるべく多くの方々に、認証アプリ(スマホ、PC)を利用する形で利用いただけると幸いです。

認証アプリへの認証シードの新規登録

以下、代表的な認証アプリへの登録の手順を示します。
最低、どれか 1 つだけセットアップすれば良いです。利便性のため、常用する複数の機器でセットアップするのも OK です。

Google Authenticatorへの認証シード登録
Microsoft Autenticatorへの認証シード登録
WinAuth(Windows用アプリ)への認証シード登録
Step Two(macOS用アプリ)への認証シード登録

30 秒更新の OATH-TOTP 規格(時間ベース)を受け付ける認証アプリでしたら、どの認証アプリでも問題ありません。各自が使いやすい物を使って下さい。

目次

Google Authenticator への認証シード登録 3
Microsoft Authenticator への認証シード登録 9
WinAuth(Windows用アプリ)への認証シード登録 15
Step Two(macOS用アプリ)への認証シード登録 23
多要素認証 CAS に関する Q&A 28
多要素認証 CAS の利用テスト 29
ハードウェアトークンによる多要素認証 CAS の利用申請 31

Google Authenticator への認証シード登録

Google Authenticator の準備

Google Play (Android)や App Store (Apple)から、 Google Authenticator を手持ちのスマートフォンにインストールします。

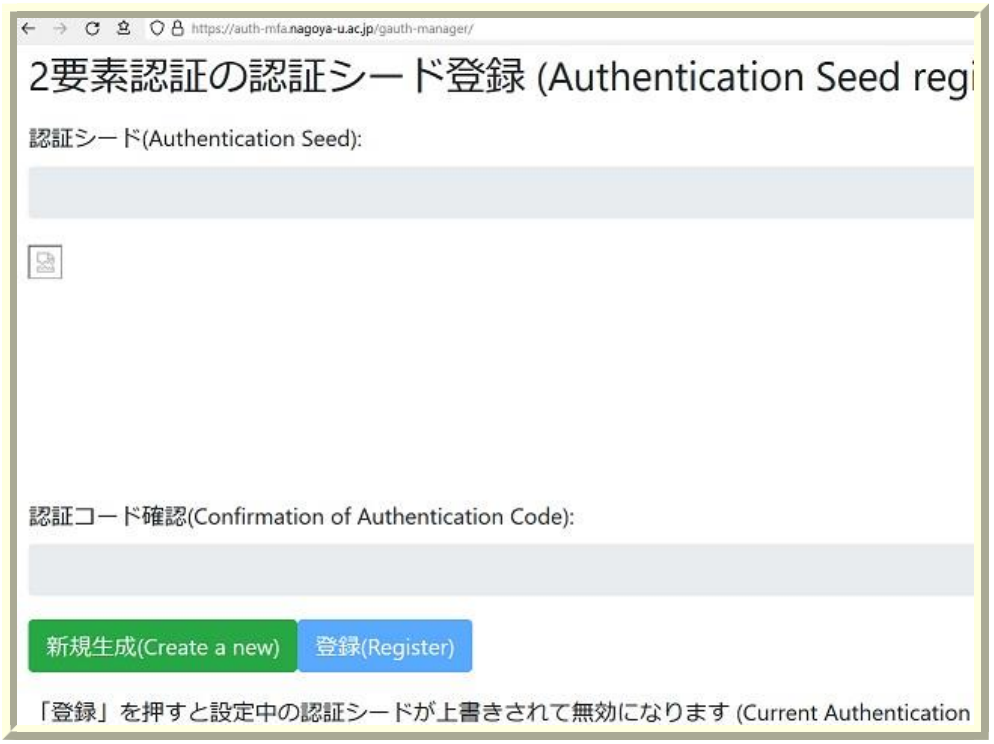
認証シード管理ページへのログインと認証シード生成

多要素認証 CAS 認証シード管理ページ に接続すると、名大ID とパスワードによる認証を求められます。入力して認証します。

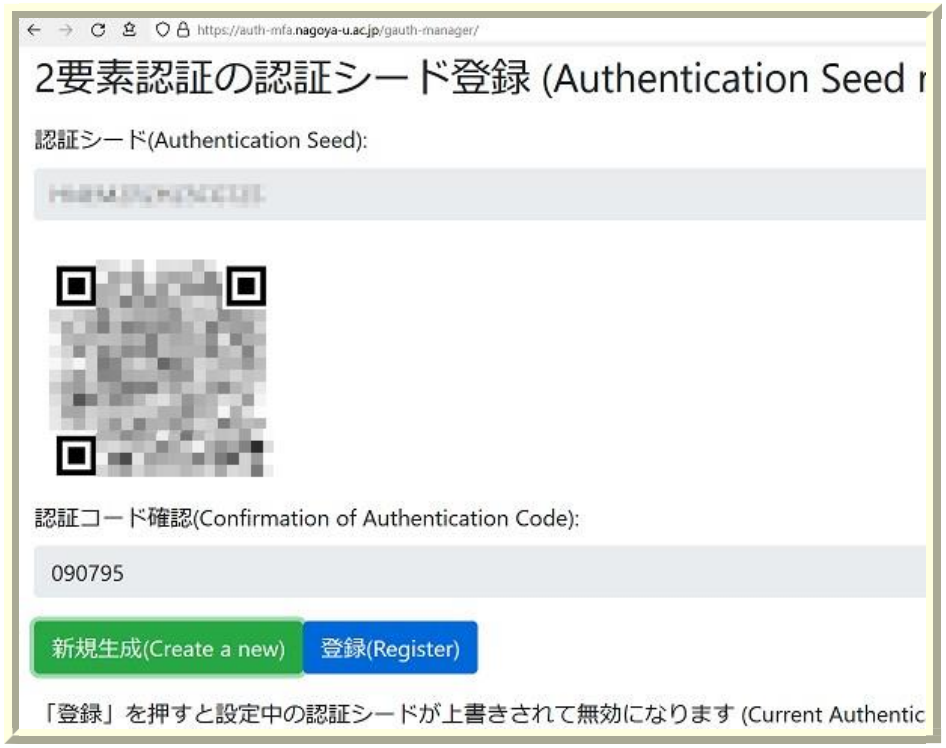
安全に認証シードを配布するため、一時的な例外を除いて、認証シード管理ページへのログインは、名古屋大学のキャンパス内のネットワークからしか許可しておりません。

「新規生成」ボタンを押すと認証シードが生成されます。

既に設定した認証シードを再表示することはできません。 一般的なパスワードのリセット時と同様、新たな認証シードを生成して登録する形のみの対応となります。



生成された認証シードが、「認証シード(英数字による表示)」と「QR コード」の形で提示されます



認証シード管理ページ側の「登録」を押さないと認証シードが CAS サーバに登録されません。 認証アプリへの認証シード登録後、忘れずに「登録」を押して認証シードを CAS サーバに登録して下さい。

間違って認証シードを新規生成してしまっても、「登録」を押す前ならば既存の認証シードは残っています。「登録」を押さずに多要素認証 CAS 認証シード管理ページを閉じて下さい。

Google Authenticator への認証シード登録の手順

初めて Google Authenticator を使う人

Google Authenticator を開くと、以下の画面が出ます。「開始」を押して次に進みます。

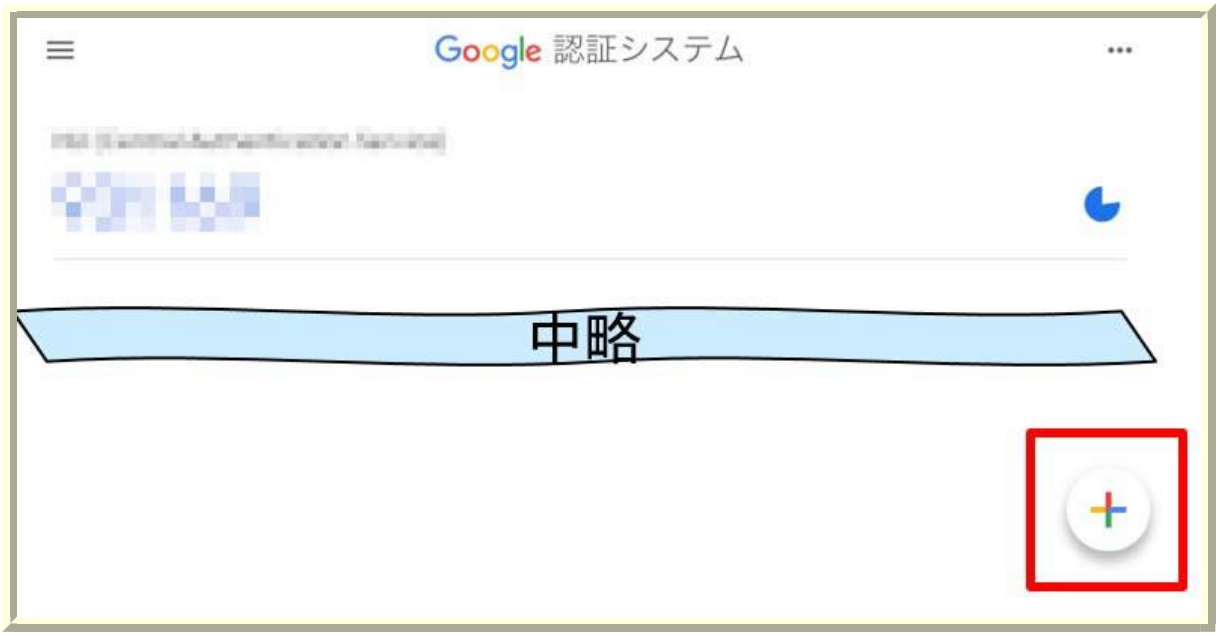
次の、認証シード登録方法の選択が出ます。「QR コードをスキャン」を選択して下さい。

「Authenticator がカメラの利用を求めています」と聞かれますので、許可します。

すでに Google Authenticator を使っている人

Google Authenticator を立ち上げた後、右下の「+」マークを押して、新規認証シードの登録を開始します。

認証シード登録方法の選択が出ますので、「QR コードをスキャン」を選択して下さい。



QR コードによる認証シード登録

カメラがついているスマートフォンで「QR コードをスキャン」を選択すると、QR コードスキャン画面が立ち上がります。

認証シード管理ページ上の QR コードをスキャンして下さい。

「NU(Central_Authentication_Service)」の名前で認証シードが登録されます。

画面の「認証コード確認」と Microsoft Authenticator の 6 桁の数字が合っているか確認して下さい。

> 合わない場合、端末の時間が大きくずれていることが考えられます。

「認証コード確認」と Google Authenticator の 6 桁の数字が合っているのを確認できたら、 **認証シード管理ページ側の「登録」を忘れずに押して認証シードを CAS サーバに登録して下さい。**

登録の後、名大ID アカウントで多要素認証が可能になったことは、こちらの多要素認証 CAS 認証テストページから確認できます。ぜひ試しておいて下さい。

認証シード(セットアップキー)の手入力による認証シード登録

新規認証シード登録時に「セットアップキーを入力」を選択すると、以下のセットアップキー(認証シード)入力画面が立ち上がります。

・「アカウント名」に自分が分かりやすい識別名をつけて下さい。
アカウント名は、「名大ID と関連している」様子を見せない記述を推奨します。
・「キーの種類」は「時間ベース」を選択して下さい。
・「キー」の欄に「認証シード」を入力して下さい。
・アルファベットは小文字で入力しても問題ありません。
・0(ぜろ)と O(オー)、1(いち)と I(アイ)を迷う場面があるかもしれませんが、見た目がまぎらわしい物は同じ扱いにされていますので、安心して好きな方で入力して下さい。

画面の「認証コード確認」と Google Authenticator の 6 桁の数字が合っているか確認して下さい。

合わない場合、端末の時間が大きくずれていることが考えられます。

「認証コード確認」と Google Authenticator の 6 桁の数字が合っているのを確認できたら、 **認証シード管理ページ側の「登録」を忘れずに押して認証シードを CAS サーバに登録して下さい。**

登録の後、名大ID アカウントで多要素認証が可能になったことは、こちらの多要素認証 CAS 認証テストページから確認できます。ぜひ試しておいて下さい。

Microsoft Authenticator への認証シード登録

Microsoft Authenticator の準備

Google Play (Android)や App Store (Apple)から、 Microsoft Authenticator を手持ちのスマートフォンにインストールします。

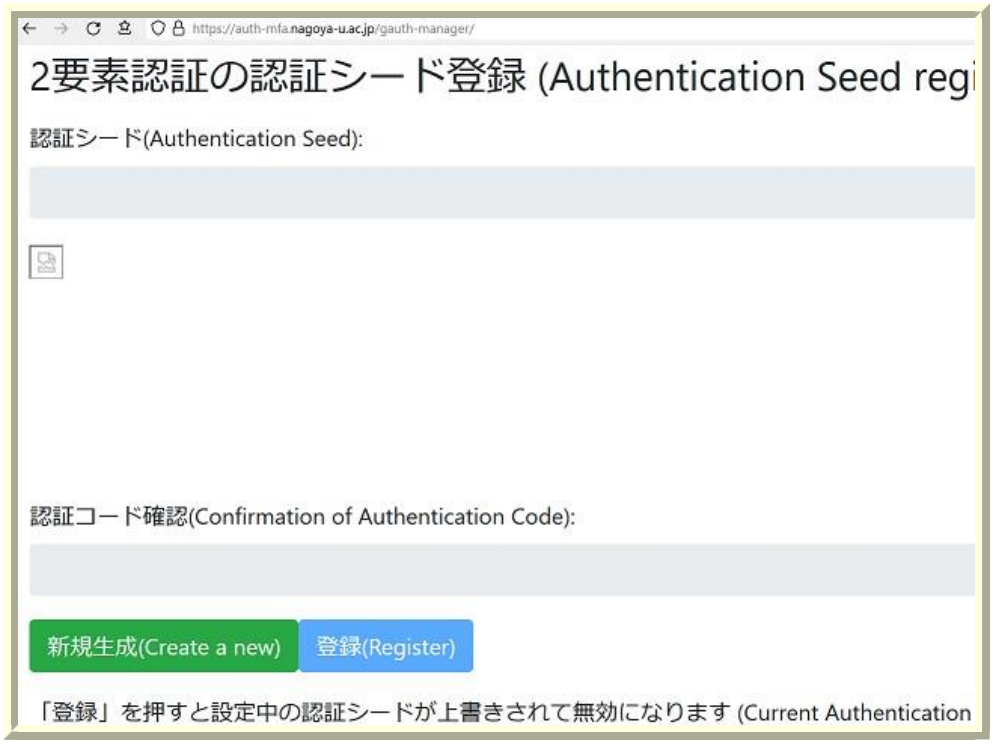
認証シード管理ページへのログインと認証シード生成

多要素認証 CAS 認証シード管理ページ に接続すると、名大ID とパスワードによる認証を求められます。入力して認証します。

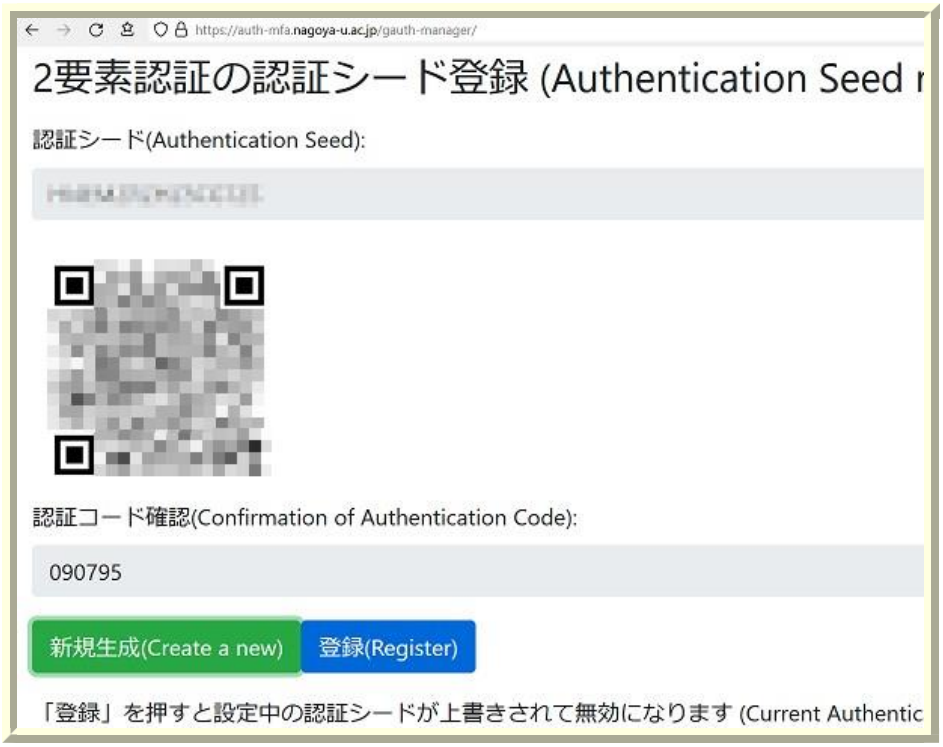
安全に認証シードを配布するため、一時的な例外を除いて、認証シード管理ページへのログインは、名古屋大学のキャンパス内のネットワークからしか許可しておりません。

「新規生成」ボタンを押すと認証シードが生成されます。

既に設定した認証シードを再表示することはできません。 一般的なパスワードのリセット時と同様、新たな認証シードを生成して登録する形のみの対応となります。



生成された認証シードが、「認証シード(英数字による表示)」と「QR コード」の形で提示されます。



認証シード管理ページ側の「登録」を押さないと認証シードが CAS サーバに登録されません。 認証アプリへの認証シード登録後、忘れずに「登録」を押して認証シードを CAS サーバに登録して下さい。

間違って認証シードを新規生成してしまっても、「登録」を押す前ならば既存の認証シードは残っています。「登録」

を押さずに多要素認証 CAS 認証シード管理ページを閉じて下さい。

Microsoft Authenticator への認証シード登録の手順

初めて Microsoft Authenticator を使う人

Microsoft Authenticator を開くと、データ収集の同意画面が出ます。選択肢が無いので、「同意します」を押して次に進みます。（後ほど、アプリ設定のログの項目にある「使用状況データ(アプリ機能向上のため…)」を停止することを推奨します）

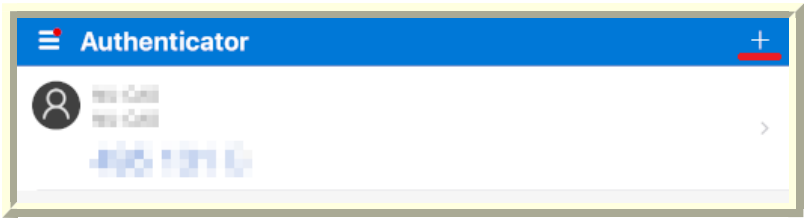
Microsoft Authnticator から Microsoft アカウントへのサインインを求められます。「QR コードをスキャンします」を選択します。もちろん、必要性な方はサインインしていただいてもかまいません。

QR コードのスキャン画面になります。「Authenticator がカメラの利用を求めています」と聞かれますので、許可し

ます。

すでに Microsoft Authenticator を使っている人

Microsoft Authenticator を立ち上げた後、右上の「+」マークを押して、新規認証シードの登録を開始します。



多要素認証を利用するサービスの選択が出ますので、「他のアカウント(Google、Facebook など)」を選択して下さい。

QR コードによる認証シード登録

QR コードスキャン画面から、認証シード管理ページ上の QR コードをスキャンして下さい。

「NU(Central_Authentication_Service)」の名前で認証シードが登録されます。

画面の「認証コード確認」と Microsoft Authenticator の 6 桁の数字が合っているか確認して下さい。

> 合わない場合、端末の時間が大きくずれていることが考えられます。

「認証コード確認」と Microsoft Authenticator の 6 桁の数字が合っているのを確認できたら、 **認証シード管理ページ側の「登録」を忘れずに押して認証シードを CAS サーバに登録して下さい。**

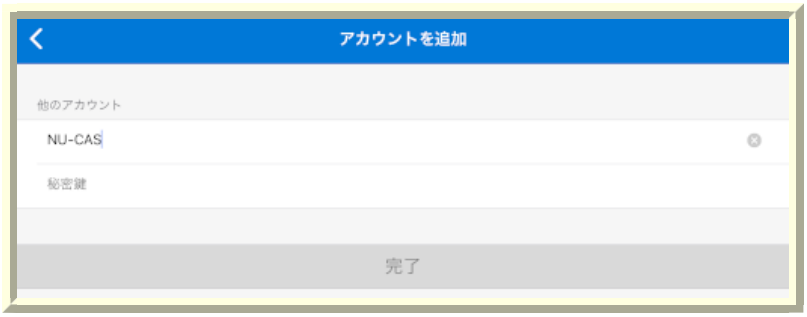
登録の後、名大ID アカウントで多要素認証が可能になったことは、こちらの多要素認証 CAS 認証テストページから確認できます。ぜひ試しておいて下さい。

認証シード(コード)の手入力による認証シード登録

QR コードスキャン用のカメラの画面で「またはコードを手動で入力」を選択します。

以下のコード(認証シード)入力画面が立ち上がります。

> **「アカウント名」に自分が分かりやすい識別名をつけて下さい。**
> **アカウント名は、「名大ID と関連している」様子を見せない記述を推奨します。**
> **「秘密鍵」の欄に「認証シード」を入力して下さい。**
> **アルファベットは小文字で入力しても問題ありません。**
> **0(ぜろ)と 1(いち)は出てきません。必ず O(オー)と I(アイ)を入力して下さい。**



画面の「認証コード確認」と Microsoft Authenticator の 6 桁の数字が合っているか確認して下さい。

> **合わない場合、端末の時間が大きくずれていることが考えられます。**

「認証コード確認」と Microsoft Authenticator の 6 桁の数字が合っているのを確認できたら、 認証シード管理ページ側の「登録」を忘れずに押して認証シードを CAS サーバに登録して下さい。

登録の後、名大ID アカウントで多要素認証が可能になったことは、こちらの多要素認証 CAS 認証テストページから確認できます。ぜひ試しておいて下さい。

WinAuth(Windows用アプリ)への認証シード登録

WinAuth のダウンロード

WinAuth のダウンロードページに行き、最新の WinAuth 3.5.1 をダウンロードします。

ZIP 圧縮ファイルなので、解凍して WinAuth.exe を取り出して下さい。

認証シード管理ページへのログインと認証シード生成

多要素認証 CAS 認証シード管理ページ に接続すると、名大ID とパスワードによる認証を求められます。入力して認証します。

安全に認証シードを配布するため、一時的な例外を除いて、認証シード管理ページへのログインは、名古屋大学のキャンパス内のネットワークからしか許可しておりません。

「新規生成」ボタンを押すと認証シードが生成されます。

既に設定した認証シードを再表示することはできません。 一般的なパスワードのリセット時と同様、新たな認証シードを生成して登録する形のみの対応となります。

生成された認証シードが、「認証シード(英数字による表示)」と「QR コード」の形で提示されます。

認証シード管理ページ側の「登録」を押さないと認証シードが CAS サーバに登録されません。 認証アプリへの認証シード登録後、忘れずに「登録」を押して認証シードを CAS サーバに登録して下さい。

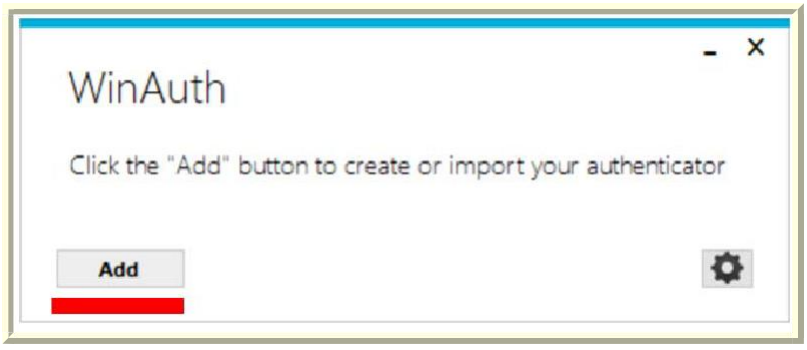
> 間違って認証シードを新規生成してしまっても、「登録」を押す前ならば既存の認証シードは残っています。「登録」を押さずに多要素認証 CAS 認証シード管理ページを閉じて下さい。

WinAuth への認証シード登録

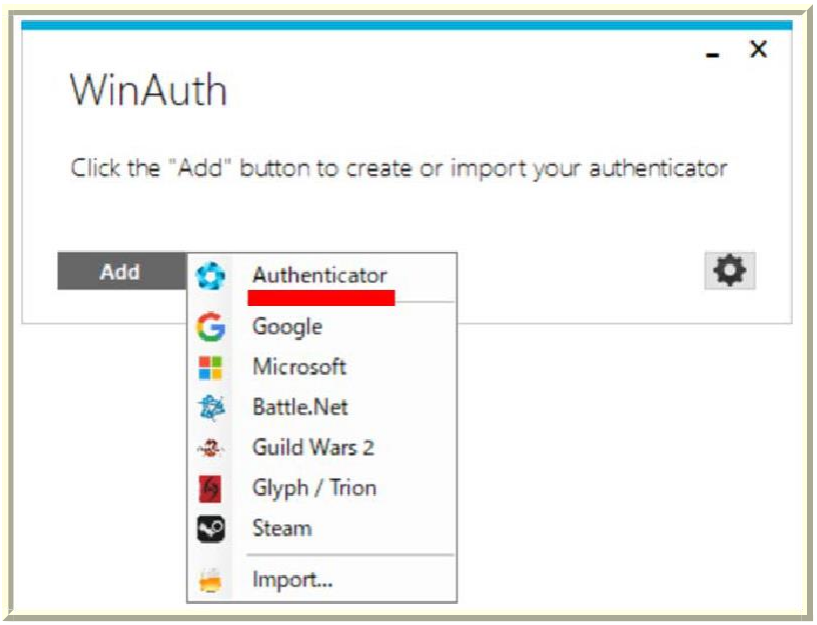
WinAuth 初回起動時には、認証シード登録を促されます。

「Add」を選択して認証シード登録へ進んで下さい。

すでに WinAuth を使っている人も、別の画面から同様に「Add」を選択して認証シード登録へ進めます。



多要素認証を利用するサービスの選択画面が出ますが、名大CAS は選択肢に無いため、一番上の Authenticator を選択して下さい。



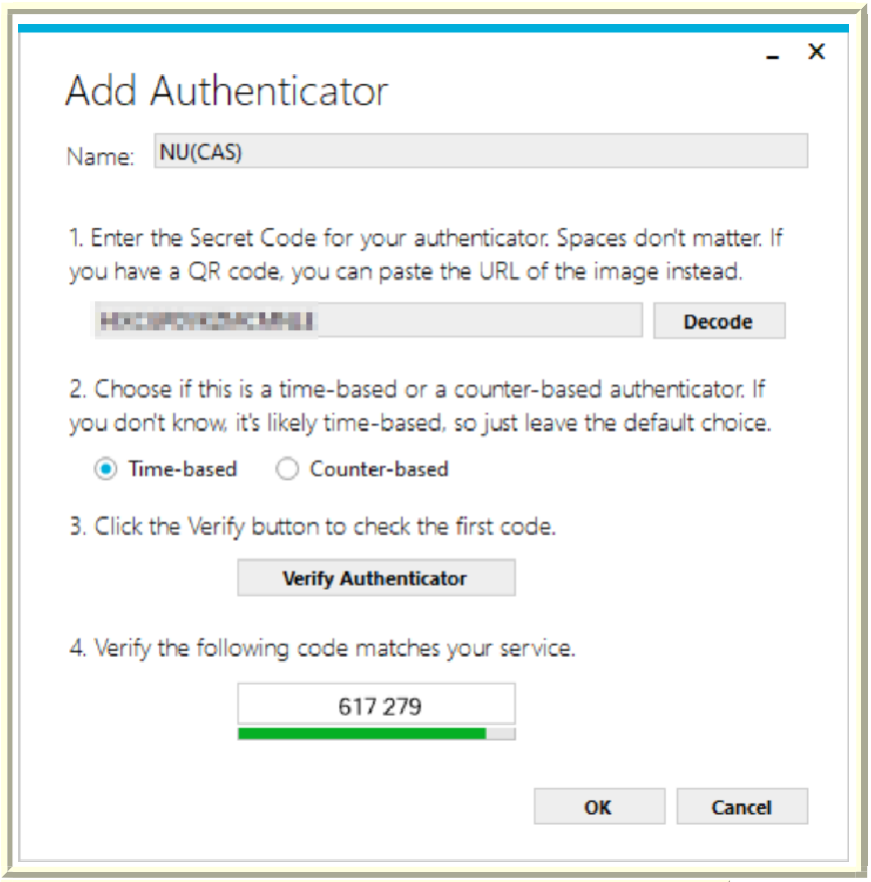
サービス名(Name)、認証シード値(1.)、認証シード生成方式(2.)を入力します。サービス名(Name)には好きな名前を入れて下さい。ただし認証シード値を使う名大ID そのものを入れるのは避けて下さい。

> 認証シード値(1.)には、多要素認証 CAS 認証シード管理ページで提示された「認証シード」を入力して下さい。認証シード生成方法(2.)は「Time-based」を選択して下さい。

3.の「Verify Authenticator」を押すと 4.に認証シード値を元に生成した 6 桁の数字が出ます。

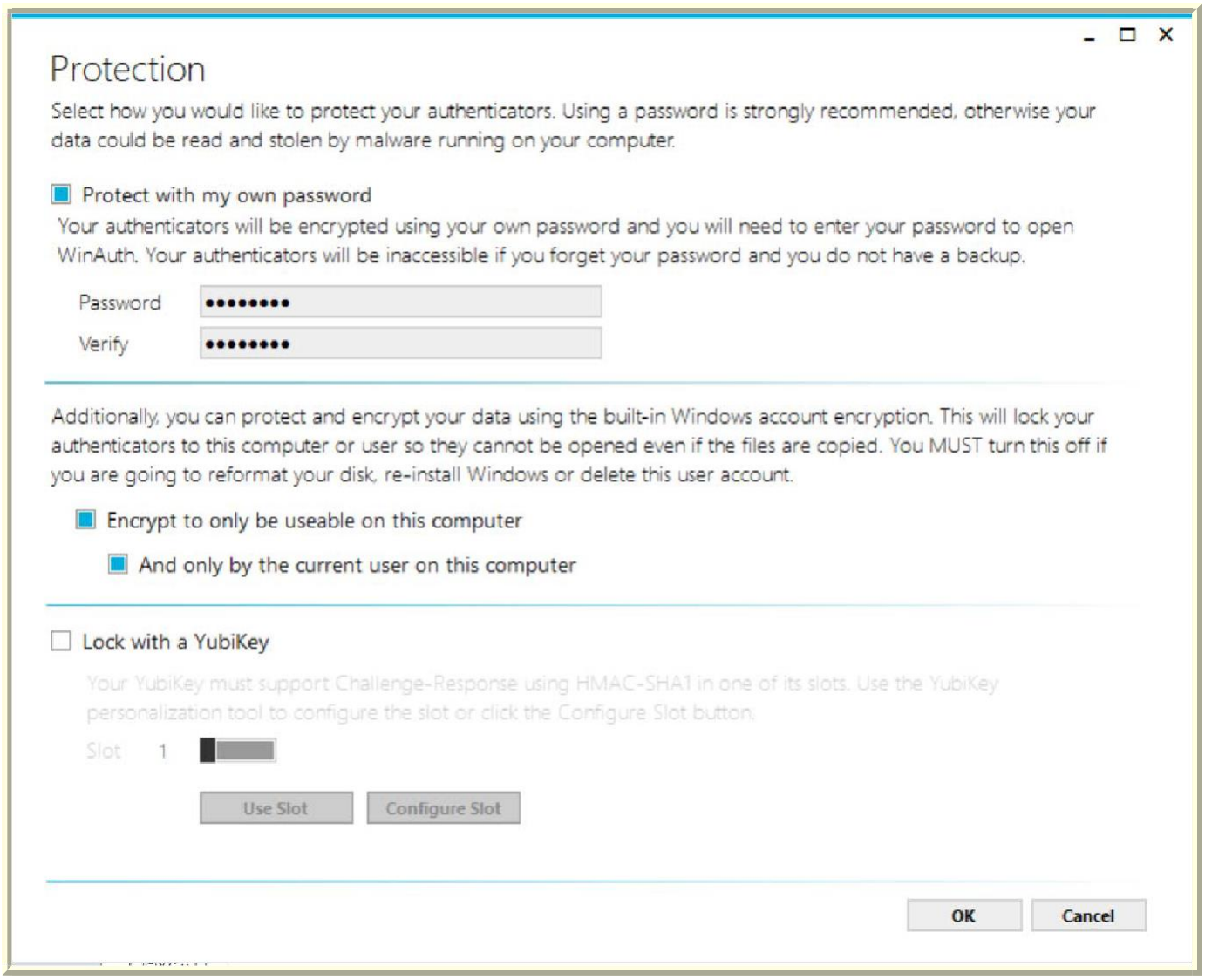
多要素認証 CAS 認証シード管理ページの「認証コード確認」欄と WinAuth の 6 桁の数字が合っているか確認して下さい。合っているならば OK を押して下さい。

> 合わない場合、端末の時間が大きくずれていることが考えられます。



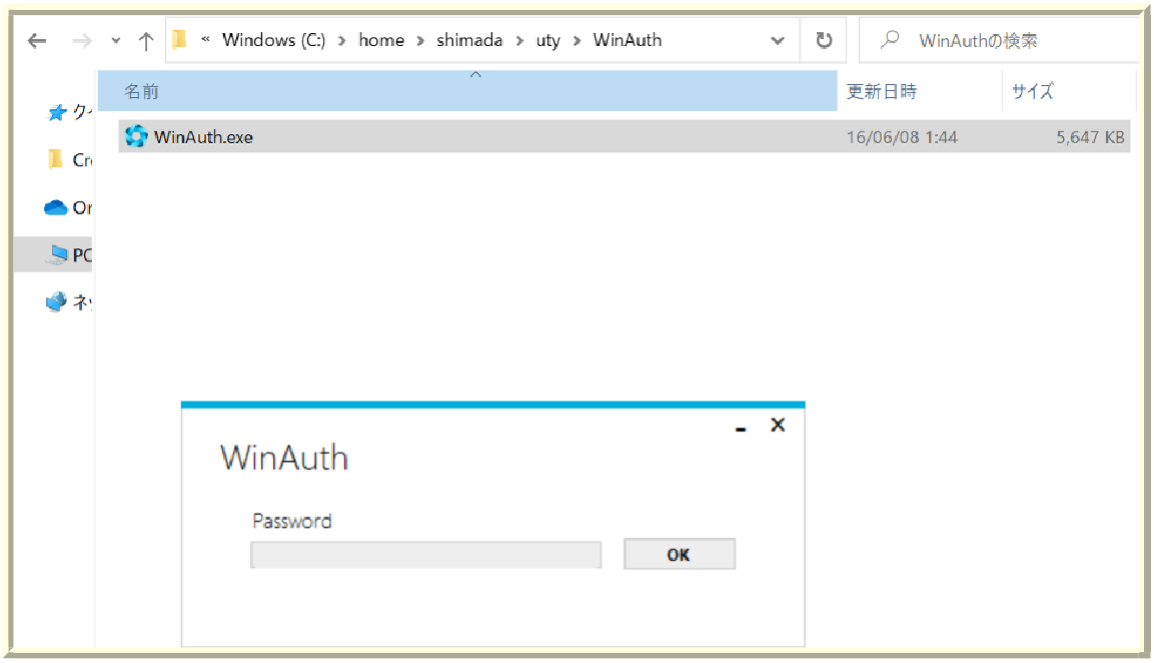
次は WinAuth の保護の設定を行います。

・「Protect with my own Password」の項目で WinAuth 起動時に要求されるパスワードを設定できます。
・「Password」と「Verify」にパスワードを入れて設定して下さい。必ず、名大ID とは別のパスワードにして下さい。
・「Encrypt to only be useable on this computer」と「And only by the current user on this computer」を設定することで、悪意のある人が他のコンピュータにコピーしたりして利用することができなくなります。



WinAuth の利用

WinAuth.exe をダブルクリックすることで起動します。パスワードを設定してあると、パスワードを要求されます。

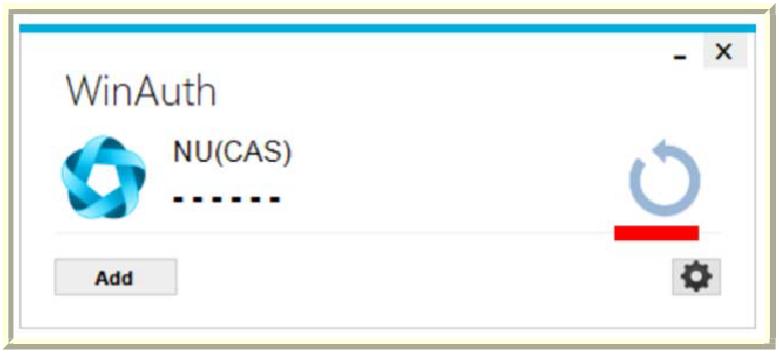


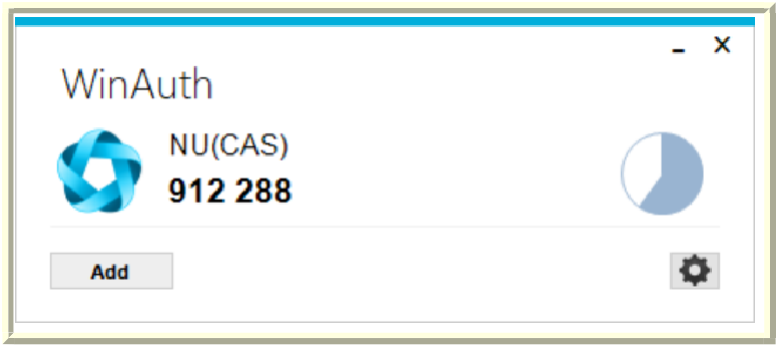
各サービスの多要素認証に必要となる 6 桁の数字が表示されます。

> 各サービス名右側の更新マークをクリックしないと表示されない点に注意して下さい。

WinAuth に表示されている 6 桁の数字と、認証シード管理ページの「認証コード確認」に表示されている確認用認証コードが一致することを確認して下さい。

> 合わない場合、PC の時間が大きくずれていることが考えられます。





「認証コード確認」と WinAuth の 6 桁の数字が合っているのを確認できたら、 認証シード管理ページ側の「登録」を忘れずに押して認証シードを CAS サーバに登録して下さい。

登録の後、名大ID アカウントで多要素認証が可能になったことは、こちらの多要素認証 CAS 認証テストページから確認できます。ぜひ試しておいて下さい。

WinAuth に関する Q&A

Q: WinAuth に設定したパスワードを忘れてしまいました。

A: 以下のファイルを削除して下さい。ただし、認証シードも含めて WinAuth の設定全てが消えます。C:¥Users(※)(ユーザ名)¥AppData¥Roaming¥WinAuth¥winauth.xml

(※) 「Users」の代わりに「ユーザー」と表記されていることもある点に注意

Step Two(macOS用アプリ)への認証シード登録

Step Two のダウンロード

Mac App Store の Step Two のページに行き、最新の Step Two をダウンロードします。

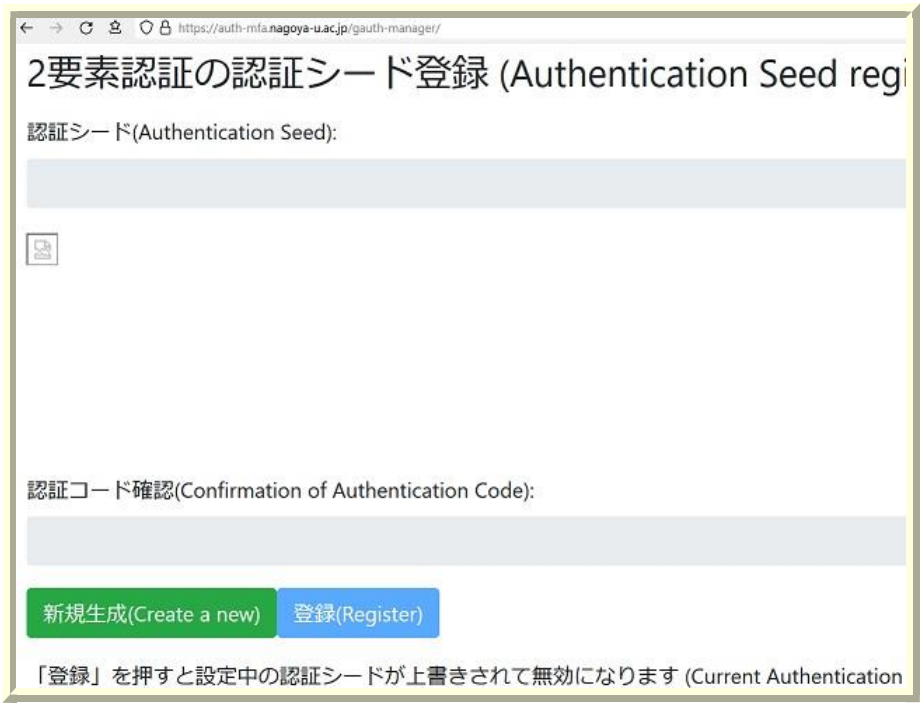
認証シード管理ページへのログインと認証シード生成

多要素認証 CAS 認証シード管理ページ に接続すると、名大ID とパスワードによる認証を求められます。入力して認証します。

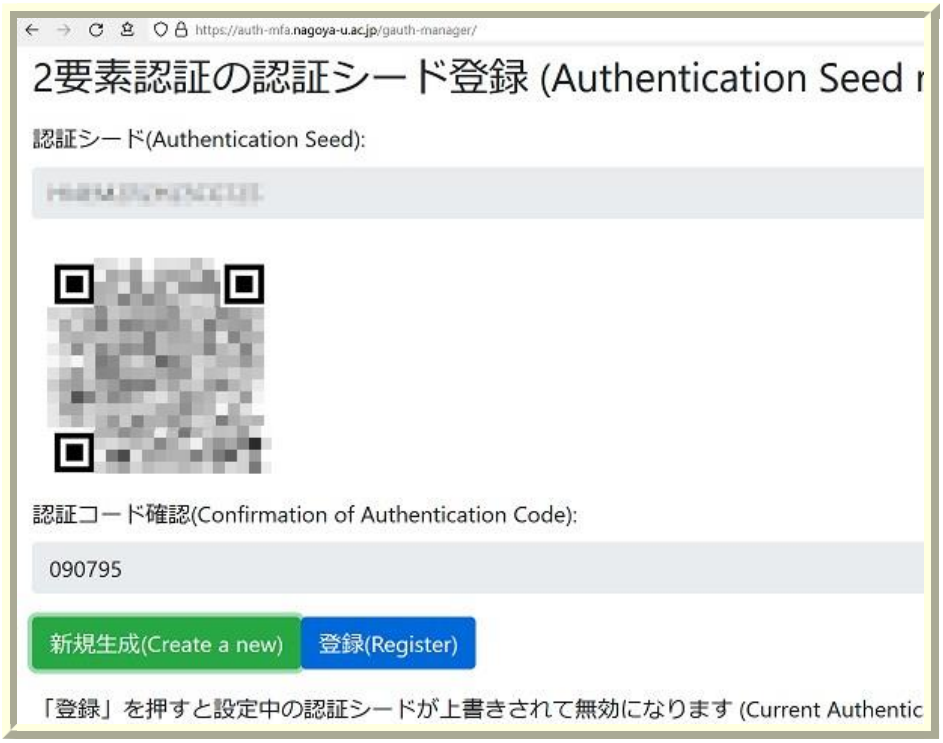
安全に認証シードを配布するため、一時的な例外を除いて、認証シード管理ページへのログインは、名古屋大学のキャンパス内のネットワークからしか許可しておりません。

「新規生成」ボタンを押すと認証シードが生成されます。

既に設定した認証シードを再表示することはできません。 一般的なパスワードのリセット時と同様、新たな認証シードを生成して登録する形のみの対応となります。



生成された認証シードが、「認証シード(英数字による表示)」と「QR コード」の形で提示されます。



認証シード管理ページ側の「登録」を押さないと認証シードが CAS サーバに登録されません。 認証アプリへの認証シード登録後、忘れずに「登録」を押して認証シードを CAS サーバに登録して下さい。

> 間違って認証シードを新規生成してしまっても、「登録」を押す前ならば既存の認証シードは残っています。「登録」を押さずに多要素認証 CAS 認証シード管理ページを閉じて下さい。

Step Two への認証シード登録(QR コード利用)

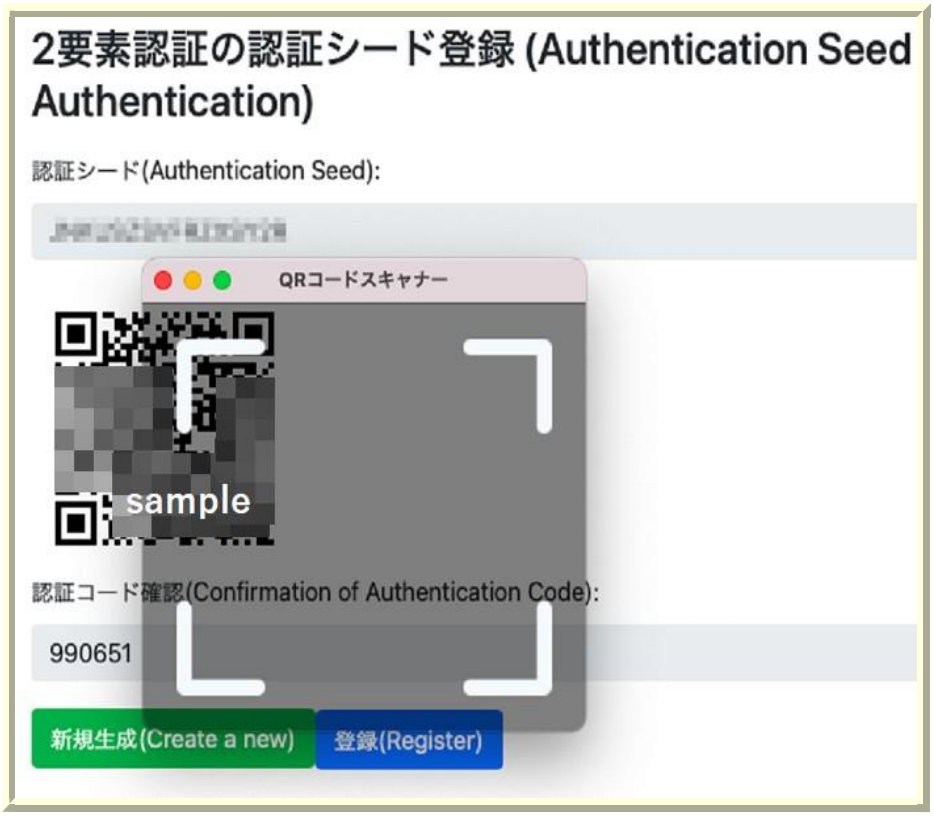
Step Two 初回起動時には、認証シード登録を促されます。

「+ボタン」をクリックして認証シード登録へ進んで下さい。

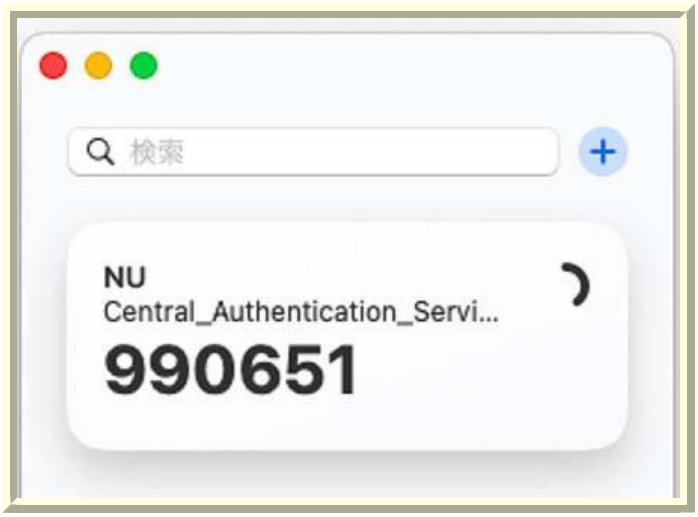
すでに Step Two を使っている人も、別の画面から同様に「+ボタン」を選択して認証シード登録へ進めます。

「+ボタン」を押すと認証シード登録方法を聞かれます。「2 段階認証 QR コードをスキャン」を選択します。

QR コードのスキャン用ウィンドウが出ますので、ウェブブラウザ上の QR コードに合わせてスキャンします。



Step Two に認証シードが登録され、サービス名と認証コードの組が表示されます。



Step Two に表示されている 6 桁の数字と、認証シード管理ページの「認証コード確認」に表示されている確認用認証コードが一致することを確認して下さい。

> 合わない場合、PC の時間が大きくずれていることが考えられます。

「認証コード確認」と Step Two の 6 桁の数字が合っているのを確認できたら、 認証シード管理ページ側の「登録」を忘れずに押して認証シードを CAS サーバに登録して下さい。

登録の後、名大ID アカウントで多要素認証が可能になったことは、こちらの多要素認証 CAS 認証テストページから確認できます。ぜひ試しておいて下さい。

英数字の認証シードによる登録

何らかの理由により QR コードを読めない場合、英数字の認証シードによる登録も可能です。認証シード登録方法の選択で「アカウントを手動で設定」を選択して下さい。

「シークレットキー」の項目に認証キーを入力して下さい

「アカウント名」と「メールアドレスまたはユーザーネーム」の項目は、各自で識別が容易な名前をつけて下さい。

> ただし、覗き見対策のため、自身の名大ID や全学メールアドレスをそのまま書くことは避けて下さい。

登録後は、Step Two に表示されている認証コードと、認証シード登録ページに表示されている確認用認証コードが一致することを確認して下さい。

「認証コード確認」と Step Two の 6 桁の数字が合っているのを確認できたら、 **認証シード管理ページ側の「登録」を忘れずに押して認証シードを CAS サーバに登録して下さい。**

登録の後、名大ID アカウントで多要素認証が可能になったことは、こちらの多要素認証 CAS 認証テストページから確認できます。ぜひ試しておいて下さい。

多要素認証 CAS に関する Q&A

Q: 複数の端末に認証シードを登録しても良いのでしょうか?
A: はい。スマホと PC とか、セキュリティを担保できる範囲で利便性のために複数端末への登録を行ってかまいません。多要素認証 CAS 認証シード登録ページから認証シードを登録する時に、登録したい複数端末を準備しておいて、それら全てに登録して下さい。

Q: スマートフォンを新しくしたが、スマートフォン側で認証アプリの移行処理を忘れてしまった。
A: 認証アプリへの認証シードの登録にありますように、 学内から多要素認証 CAS 認証シード登録ページにアクセスして、新たな認証シードを生成して登録して下さい。 新たな認証シードを登録すると、既存の認証シードは使えなくなる点に注意して下さい。

Q: スマートフォンの認証アプリにクラウドバックアップ機能があるのですが、使って大丈夫でしょうか?
A: 信用のできる認証アプリでしたらバックアップを使ってかまいません。

Q: スマートフォンを紛失してしまったので、新たなスマートフォンに認証シードを登録したい。
A: 認証アプリへの認証シードの登録にありますように、 学内から多要素認証 CAS 認証シード登録ページにアクセスして、新たな認証シードを生成して登録して下さい。 新たな認証シードを登録すると、既存の認証シードは使えなくなる点に注意して下さい。

Q: ハードウェアトークンを紛失してしまったので、ただちにハードウェアトークンの無効化処理を行いたい。
A: IT ヘルプデスクに職員証/学生証を持参し、 ハードウェアトークンの無効化の依頼を出して下さい。

Q: 新たなハードウェアトークンを登録したい。
A: ハードウェアトークンの利用登録(暫定)の手続きに従い、 新しいハードウェアトークンの利用登録を行って下さい。 登録後、古いハードウェアトークンは使えなく点にご注意下さい。

Q: 学内向け情報サービスで CAS 認証を使っているのですが、多要素認証 CAS への移行作業は多いのでしょうか?
A: CAS サーバの参照部分を、多要素認証 CAS サーバへの参照に書き換えるだけ済みます。先行して移行した事例では 2,3 行の変更で済んでおります。

Q: 多要素認証についてもっと知りたい。
A: 多要素認証に関する Tips なる読み物を準備しました。

多要素認証 CAS の利用テスト

多要素認証 CAS の利用のテスト用に、 多要素認証 CAS 認証テストページ を準備してあります。

利用テストの手順

多要素認証 CAS 認証テストページ に行くと、まず、名大ID とパスワードの入力を求められます。

すでに CAS 側で名大ID とパスワードが受け付けられている場合、いきなり 2 要素目の認証コード(6 桁の数字)の入力を求められる点に注意して下さい。

名大ID とパスワードが正しかった場合、2 要素目の認証コード(6 桁の数字)の入力を求められます。

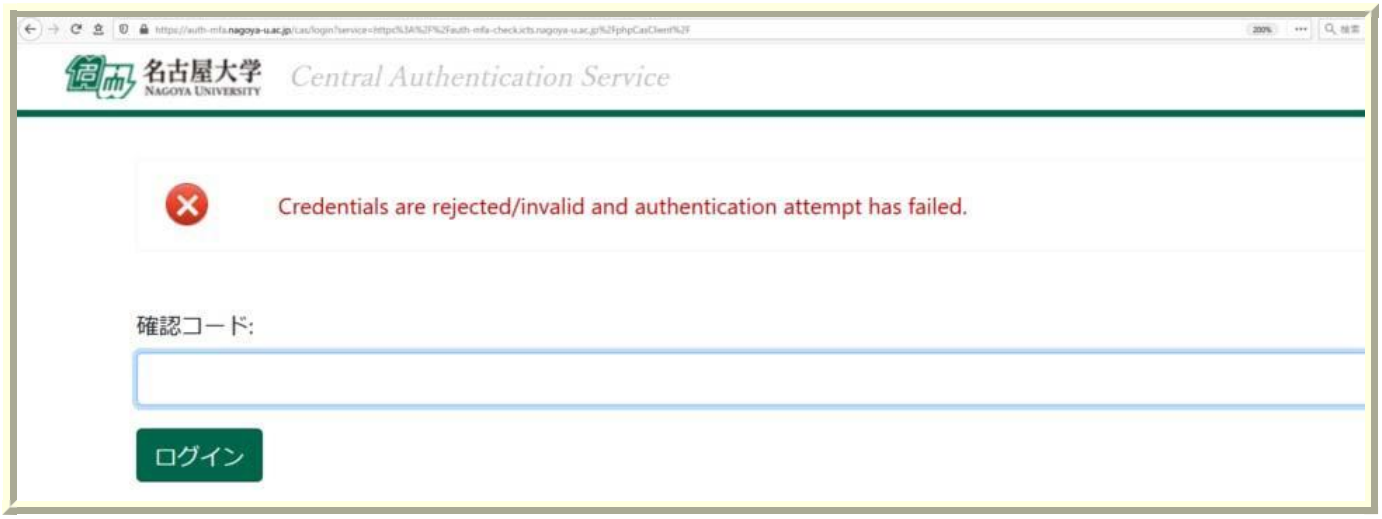
手元の認証アプリやハードウェアトークンの認証コードの数字を見て、数字を入力して下さい。

前後の時間の数字も受け付ける設定をしていますので、入力中や入力後に数字が変わってしまった場合でも、そのまま認証を進めて下さい。

認証コード入力による認証が成功した場合、以下の認証成功を示すページに移ります。
**　これで利用テストは終わりですので、ページを閉じて下さい。**

認証が失敗した場合は以下のページが表示されます。　再度、表示されている認証コードを入力して下さい。

何度も失敗する場合、下方の「認証がうまくいかない場合」の各項目を確認して下さい。



認証がうまくいかない場合

認証アプリを動かしている端末の時間がずれている

→端末の時間を正確な時間に合わせて下さい 間違った認証シードを登録している

→再度、シード登録からやりなおして下さい

ハードウェアトークンの時間が大幅にずれている

→ハードウェアトークンの利用申請を再度やり直した上、登録時に相談して下さい

ハードウェアトークンによる多要素認証 CAS の利用申請

ハードウェアトークンの利用を希望する場合、部局予算等でハードウェアトークンを購入した上で、ハードウェアトークンを多要素認証CASに登録する形を取っていただきます。

ハードウェアトークンの入手

多要素認証 CAS に利用可能なハードウェアトークンの仕様は「30 秒更新の OATH-TOTP 規格で、6 桁の認証コードを出力するもの」です。仕様を満たしていれば、ハードウェア　トークンのメーカは問いません。

多要素認証 CAS へのハードウェアトークンの登録には、ハードウェアトークンにあらかじめ書き込まれている認証シードが必要になります。ハードウェアトークン販売業者からハードウェアトークンとともに納品される「BASE32 エンコード済みの認証シード」は無くさないように厳重に保管しておいて下さい。

現在、利用実績のあるハードウェアトークンは以下の通りになります。購入に関する相談があるならば、多要素認証 CAS プロジェクト(multiauth@icts.※)までお願いします。(※: nagoya-u.ac.jp)
飛天ジャパン ワンタイムパスワード(TOP)トークン

ハードウェアトークンの認証シードの多要素認証 CAS への登録

Microsoft 365（機構アカウント）にログインした状態で以下の Forms(多要素認証 CAS ハードウェアトークン申請)を記入して電子的に申請した上で、本人確認用の職員証/学生証を持参して情報基盤センター1F IT ヘルプデスクまで来訪し、申請に対する本人確認を行って下さい。認証シードの登録完了後に、連絡先電子メールにシード登録が完了した旨の通知メールを送ります。

ハードウェアトークン利用申請

何らかの理由で Microsoft 365 を使えないなど、Forms で電子申請できな場合は、以下の Word 版の利用申請書を記入した上で、本人確認用の職員証/学生証を持参して情報基盤センター1F IT ヘルプデスクまで来訪し、申請と本人確認を行って下さい。

Word版ハードウェアトークン利用申請書(Formsが使えない人)

ハードウェアトークンを利用した多要素認証

ハードウェアトークンのボタンを押したときに表示される 6 桁の数字が、認証の 2 要素目(認証コード)になります。具体的な認証の進め方は、多要素認証の利用テストのページに記されています。

ハードウェアトークン利用申請に関する Q&A

Q: ハードウェアトークンを紛失してしまったので、ただちにハードウェアトークンの無効化処理を行いたい。
A: IT ヘルプデスクに職員証/学生証を持参し、ハードウェアトークンの無効化の依頼を出して下さい。

Q: 新たなハードウェアトークンを登録したい。
A: 本 Web ページの手続きに従い、改めて新しいハードウェアトークンの利用登録を行って下さい。登録後、古いハードウェアトークンは使えなく点にご注意下さい。

Q: ハードウェアトークンを紛失してしまって認証できないが、急ぎの業務がある。
A: 少数ですが、貸し出し用のハードウェアトークンを準備しておりますので、IT ヘルプデスクにご相談下さい。