カスタム認証利用ガイド

はじめに

Generative AI FW（以降、本サービス）のデフォルトの認証方式は以下です。

- 本サービスに登録したユーザ情報で認証する。認証にはメールアドレスとパスワードを利用する

本書では、デフォルト以外の認証方式（カスタム認証）について解説しています。カスタム認証として選択できる方式は以下があります。

- **ユーザID認証**：本サービスに登録したユーザ情報で認証する。認証にはユーザIDとパスワードを利用する
- **IdP連携（Entra ID）認証**：本サービス外部のEntra IDと連携し、そのユーザ情報で認証する
- **IdP連携（Active Directory）認証**：本サービス外部のActive Directoryと連携し、そのユーザ情報で認証する

本書では カスタム認証の各方式を利用時の Generative AI FW の動作や操作方法について説明します。

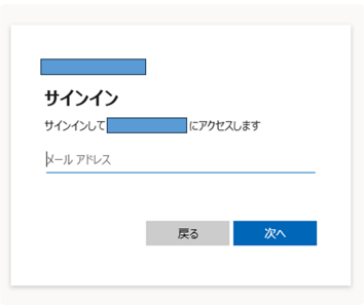
認証方式の確認方法

お使いの本サービスがどの認証方式で運用されているかを、チャットUI/管理ポータルへのログイン時の認証フォームで簡易的に判断することが可能です。認証方式の確認方法は以下の通りです。ただし一部の認証方式は認証フォームのみでは完全に特定できないため、サービスの管理者や構築作業者にお問い合わせください。

デフォルトの認証方式の場合、ログイン時の認証フォームの入力欄に[メールアドレス]と表示されます。

ユーザID認証、あるいは、IdP連携（Active Directory）認証の場合、ログイン時の認証フォームの入力欄に[ユーザー名]と表示されます。

IdP連携（Entra ID）認証の場合、他と異なり以下のようなEntra ID の認証フォームが表示されます。



1. ユーザID認証

1.1 概要

デフォルトの認証方式と異なり、ログイン時の認証情報にユーザIDとパスワードを用いる方式です。
登録するユーザにメールアドレスが割り当てられていない場合や、認証時にメールアドレス形式以外の認証情報を用いたい場合にご利用ください。

ユーザID認証利用時のGenerative AI FW の動作は以下のようになります。

- ユーザ登録時に、ユーザIDを指定します。emailの指定は任意です。
- UIへのログイン時、認証はユーザIDとパスワードで行います。

1.2 ログイン

ログイン時の認証情報入力画面は、以下の表記となります。
ユーザー名にはユーザ追加時に指定した「ユーザID」を入力してください。

> 認証情報入力画面の表記は「ユーザー名」ですが、ユーザ登録時の「名前」ではなく「ユーザID」の情報を用います。

> 初期ユーザや認証方式変更前に作成したユーザでログインする場合、ユーザー名にはユーザのメールアドレスを指定してください。

1.3 ユーザ管理

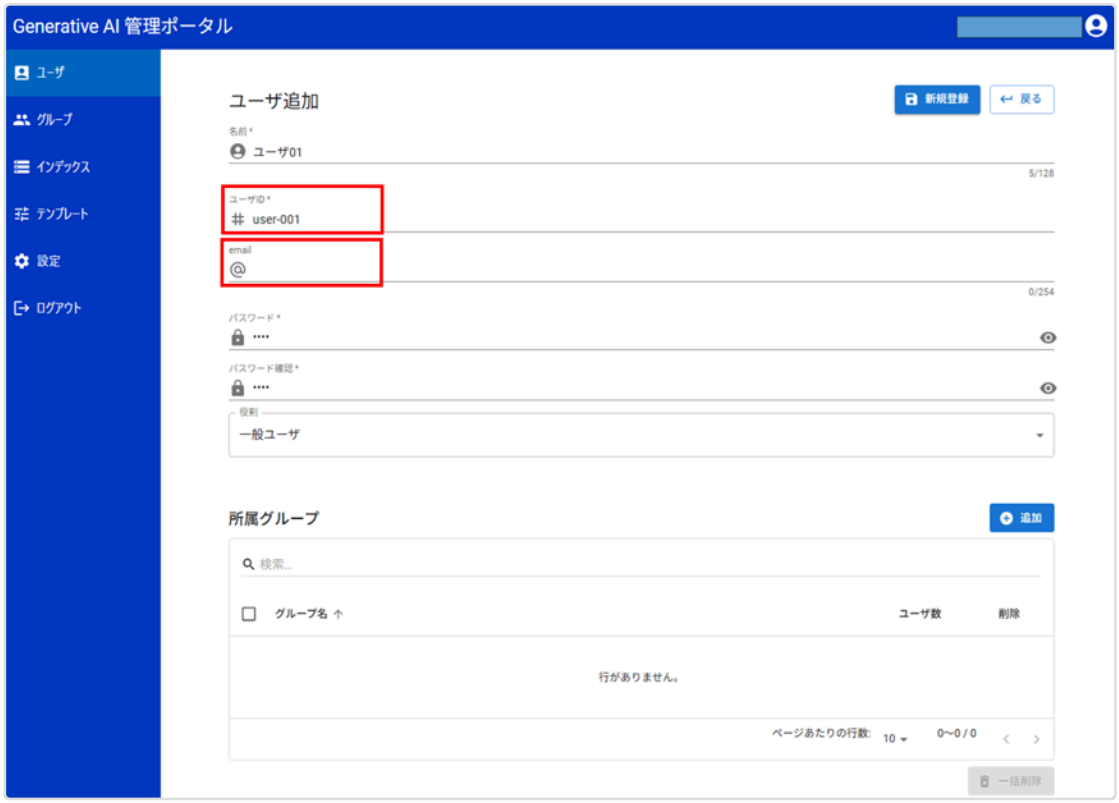
基本的な操作は 「管理ポータル操作ガイド(基本操作編)」を参照ください。ここでは、ユーザID認証方式を利用するうえでの差分を中心に説明します。

1.3.1 ユーザ追加

ユーザID認証の場合、ユーザ追加時に「ユーザID」を指定する必要があります。ここで指定したユーザIDをログインの際の認証情報として利用します。
デフォルトの認証方式と異なり、「email」 の入力は任意です。

> ユーザIDとして利用できる文字は英数字および+.-_@で、最大文字数は128です。英字の大文字・小文字は区別しません。

> 認証基盤であるKeyclokのメールアドレスに関するポリシーは、emailに設定した値には適用されません。



1.3.2 ユーザ編集

デフォルトの認証方式と異なり、「email」 も変更可能です。それ以外はデフォルトの認証方式と変わりません。

1.3.3 ユーザ削除

デフォルトの認証方式と手順は変わりません。

1.4 ユーザID認証時の動作

デフォルトの認証方式との機能の差異は以下の通りです。

対象機能	差異の内容
認証画面	• チャットUI・管理ポータルにログイン時の認証画面では、メールアドレス/パスワードの代わりに、ユーザID/パスワードを入力します • パスワードの初期化する必要がある場合、システム管理者にパスワードを初期化するよう依頼してください。
管理ポータルユーザ管理	• ユーザ登録時、ユーザIDを指定する必要があります。ここで指定したユーザIDは認証情報として用いられます。 • ユーザ登録・編集時、email の指定は必須ではありません。 • ユーザー覧表示で、email の代わりに ユーザIDを表示します。 • ログインユーザの役割変更、削除が可能です。 • 認証基盤であるKeyclokのメールアドレスに関するポリシーは、emailに設定した値には適用されません。
監査ログ	対話履歴ログのユーザIDの項目には、作成時に指定したユーザIDが出力されます。 管理ポータル画面操作ログのユーザIDの項目には、<UUID>@example.com という形式のIDが出力されます。これは、KeyCloak の GenaiRealm の Users で確認できるユーザの Email 属性に登録された値です。 アクセスログの username の項目には、作成時に指定したユーザIDが出力されます。

2. IdP連携(Entra ID)認証

2.1 概要

お客様が利用されているEntra IDのユーザ情報で認証し本サービスのUIにログインできるようにする認証方式です。
IdP連携(Entra ID)認証利用時の Generative AI FW の動作は以下のようになります。

- ユーザの登録・変更・削除は Generative AI FW 管理ポータル ではなく、連携先の Entra ID で行います
  - ただし、Generative AI FW 上の役割や所属グループの指定は Generative AI FW 管理ポータル で行う必要があります
- 連携先の Entra ID に登録されたユーザは、全員チャットUIにログインする事ができます。ログイン時には Entra ID に登録された認証情報を利用します

- 連携先の Entra ID に登録されたユーザのうち、Generative AI FW 管理ポータルで役割を組織管理者と指定されたユーザが、Generative AI FW 管理ポータルにログインできます。ログイン時には Entra ID に登録された認証情報を利用します
- 連携先の Entra IDに存在しないユーザ、削除されたユーザは、Generative AI FWのチャットUI・管理ポータルにログインする事は出来ません

2.2 ログイン方法

ログイン時の認証情報入力画面は、連携先のEntra IDのものになります。
ログインに利用する情報は、連携先の Entra ID の設定に依存します。入力内容が不明の場合、連携先の Entra IDの管理者に問い合わせてください。

2.3 Entra ID ユーザの役割・所属グループの変更

連携先の Entra ID のユーザの Generative AI FW 上の属性は、デフォルトでは以下となります。

Generative AI FW 上の属性	値
名前	Entra ID のユーザの表示名
email	なし
ユーザID（※1）	Entra ID の ユーザのオブジェクト ID
役割	一般ユーザ
所属グループ	なし すべてのユーザが自動的に所属するグループである「ALL USERS GROUP」には所属しています

（※1）ユーザIDは、カスタム認証利用時のみ利用される属性です。カスタム認証利用時の管理ポータルのユーザー一覧・ユーザ追加・ユーザ編集ページで表示されます

役割や所属グループ等の Generative AI FW 上のユーザ属性をデフォルトから変更したい場合、管理ポータルで指定する必要があります。
指定方法には、以下の2種類の方法があります。

1. 該当ユーザがチャットUIを利用する前に事前に指定する
2. チャットUIに一度以上ログインしたユーザの属性を後から変更する

2.3.1 Entra ID ユーザ の属性を事前に指定する

Entra IDユーザがチャットUIを利用する前に属性を指定する場合、管理ポータルで該当ユーザを登録する操作を行います。

> 本操作を行う事で、該当ユーザは初回のログイン時点でこの操作で指定した役割や所属グループに従ったリソースを利用できます。
> 本操作で役割を組織管理者に指定したユーザは、最初から管理ポータルにログインする事が可能になります。

1. 組織管理者ユーザで、管理ポータルにログインします。左メニューからユーザを選択しユーザー覧ページを表示します。
2. 追加ボタンをクリックし、ユーザ追加ページを表示します。
3. ユーザ追加ページで、予め属性を指定したいユーザの情報をいれ、新規登録ボタンをクリックします。
   - ユーザIDには、対象の Entra ID ユーザのオブジェクトIDを入力してください
   - 名前に対象ユーザを表す名前を入力してください。 Entra ID の表示名と一致する必要はありません
   - email は任意項目です
   - 該当ユーザに与えたい権限に応じて、役割・所属グループを指定してください

2.3. 2チャットUIに一度以上ログインしたEntra ID ユーザの属性を変更する

Entra ID ユーザで チャットUIにログインすると、該当ユーザが Generative AI FW にデフォルトの属性で登録されます。
そのユーザの属性を変更する場合、管理ポータルで該当ユーザを編集する操作を行います。

1. 組織管理者ユーザで、管理ポータルにログインします。左メニューからユーザを選択しユーザ一覧ページを表示します。
2. 対象のユーザを一覧から探して編集アイコンををクリックし、ユーザ編集ページを表示します。
    - ユーザ一覧の名前にはEntra ID ユーザの表示名、ユーザIDにはEntra IDのオブジェクトIDが表示されます。それらの情報から対象のユーザを特定してください。
3. ユーザ編集ページで属性を変更し、更新ボタンをクリックします。

2.4 Entra ID ユーザの削除

連携先の Entra ID からユーザを削除することで、そのユーザは Generative AI FW のチャットUI・管理ポータルにログインする事は出来なくなります。
ただし、一度でもチャットUIにログインした事のあるユーザの場合、Generative AI FW にもユーザ情報が残ります。お手数ですが該当ユーザを管理ポータルからも削除してください。

1. 組織管理者ユーザで、管理ポータルにログインします。左メニューからユーザを選択しユーザ一覧ページを表示します。
2. 対象のユーザを一覧から探して削除アイコンををクリックし、ユーザ情報を削除します。

2.5　IdP連携(Entra ID)認証時の動作

デフォルトの認証方式との機能の差異は以下の通りです。

対象機能	差異の内容
認証画面	• チャットUI・管理ポータルにログイン時の認証画面は、Entra IDのものになります。Entra IDの認証情報を入力してください。

	• パスワード初期化については連携先のEntra IDで実施してください
管理ポータルユーザ管理	• ユーザ登録時、ユーザIDとしてEntra IDのユーザのオブジェクトIDを入力する必要があります。 • ユーザ登録・編集時、email の指定は必須ではありません。 • ユーザー一覧表示で、email の代わりに ユーザIDを表示します。 • ログインユーザの役割変更、削除が可能です。 ◦ 誤ってすべてのEntra ID ユーザの組織管理者を削除してしまった場合、「IdP連携(Entra ID) セットアップガイド」の「5.2. Generative AI FW のユーザもログインできるようにする」の手順を行い、Generative AI FW のユーザ で再度 Entra ID の組織管理者ユーザを登録してください
監査ログ	対話履歴ログのユーザIDの項目には、Entra ID ユーザのオブジェクトIDが出力されます。ユーザを識別するにはメールアドレスの列を確認してください。 管理ポータル画面操作ログのユーザIDの項目には、Entra ID ユーザのサービスプリンシパル名が出力されます。 アクセスログの username の項目には、Entra ID ユーザのオブジェクトIDが出力されます。

3 IdP連携(Active Directory)認証

3.1 概要

お客様が利用されているActive Directoryのユーザ情報で認証し本サービスのUIにログインできるようにする認証方式です。
IdP連携(Active Directory)認証利用時の Generative AI FW の動作は以下のようになります。

- ユーザの登録・変更・削除は Generative AI FW 管理ポータル ではなく、連携先の Active Directory で行います。
  - ただし、Generative AI FW 上の役割や所属グループの指定は Generative AI FW 管理ポータル で行う必要があります
- 連携先の Active Directory の 連携時に指定したディレクトリに 登録されたユーザは、全員チャットUIにログインする事ができます。ログイン時には Active Directory に登録された認証情報を利用します

- 連携先の Active Directory に登録されたユーザのうち、Generative AI FW 管理ポータルで役割を組織管理者と指定されたユーザが、Generative AI FW 管理ポータルにログインできます。ログイン時には Active Directory に登録された認証情報を利用します
- 連携先の Active Directory に存在しないユーザ、削除されたユーザは、Generative AI FW のチャットUI・管理ポータルにログインする事は出来ません

3.2 ログイン方法

ログイン時の認証情報入力画面は、以下の表記となります。
ユーザー名には連携先のActive Directoryの「ユーザログオン名」を指定してください。パスワードにはActive Directoryの該当ユーザのパスワードを指定してください。

ユーザー名として入力するActive Directoryの「ユーザログオン名」には、<name>@<domain> や <domain>¥<name> の形式ではなく、ドメイン名を含まない名前部分のみを指定してください。

本サービスのログインに利用するActive Directory 上のユーザには、「ユーザログオン名」と「ユーザログオン名(Windows2000より前)」の両方の名前が設定されている必要があります。

- 「ユーザログオン名」と「ユーザログオン名(Windows2000より前)」が異なる場合、本サービスのログイン時には「ユーザログオン名(Windows2000より前)」を利用してください
- 「ユーザログオン名」が設定されていないユーザは本サービスを利用できません。
  Active Directory で該当ユーザの「ユーザログオン名」を設定してください。「ユーザログオン名」の変更が本サービスに反映され利用可能になるまでに最大24時間かかります

初期ユーザや連携前に作成したユーザでログインする場合、ユーザー名のフォームにはユーザのメールアドレスを指定してください。

本サービスからActive Directoryユーザのパスワードを変更する事は出来ません。そのため、次回ログイン時にパスワード変更が必要な状態のユーザは本サービスにログインできません。
パスワード変更を完了後、本サービスにログインしてください。

3.3 Active Directory ユーザの役割・所属グループの変更

連携先の Active Directory のユーザの Generative AI FW 上の属性は、デフォルトでは以下となります。

Generative AI FW 上の属性	値
名前	Active Directory のユーザログオン名(ドメイン部分を含まない)
email	なし
ユーザID（※1）	Active Directory の ユーザのオブジェクトID
役割	一般ユーザ
所属グループ	なし すべてのユーザが自動的に所属するグループである「ALL USERS GROUP」には所属しています

（※1）ユーザIDは、カスタム認証利用時のみ利用される属性です。カスタム認証利用時の管理ポータルのユーザー一覧・ユーザ追加・ユーザ編集ページで表示されます

役割や所属グループ等の Generative AI FW 上のユーザ属性をデフォルトから変更したい場合、以下の手順で管理ポータルで指定する必要があります。

3.3.1 Active Directory ユーザの属性を変更する

Active Directory ユーザで チャットUIにログインすると、該当ユーザが Generative AI FW にデフォルトの属性で登録されます。
そのユーザの属性を変更する場合、管理ポータルで該当ユーザを編集する操作を行います。

1. 組織管理者ユーザで、管理ポータルにログインします。左メニューからユーザを選択しユーザ一覧ページを表示します。
2. 対象のユーザを一覧から探して編集アイコンををクリックし、ユーザ編集ページを表示します。
   - ユーザ一覧の名前にはActive Directoryのログオン名、ユーザIDにはActive Directoryのオブジェクト IDが表示されます。それらの情報から対象のユーザを特定してください。
3. ユーザ編集ページで属性を変更し、更新ボタンをクリックします。

3.4 Active Directory ユーザの削除

連携先の Active Directoryからユーザを削除することで、そのユーザは Generative AI FW のチャットUI・管理ポータルにログインする事は出来なくなります。
ただし、一度でもチャットUIにログインした事のあるユーザの場合、Generative AI FW にもユーザ情報が残ります。お手数ですが該当ユーザを管理ポータルからも削除してください。

1. 組織管理者ユーザで、管理ポータルにログインします。左メニューからユーザを選択しユーザ一覧ページを表示します。
2. 対象のユーザを一覧から探して削除アイコンををクリックし、ユーザ情報を削除します。

3.5 IdP連携(Active Directory)認証時の動作

デフォルトの認証方式との機能の差異は以下の通りです。

対象機能	差異の内容
認証画面	• チャットUI・管理ポータルにログイン時の認証画面では、Active Drectoryのユーザログオン名(ドメイン部分含まず)とパスワードを入力します

	• パスワード初期化については連携先のActive Drectoryで実施してください
管理ポータルユーザ管理	• 管理ポータルからのユーザ登録は出来ません。 • ユーザ編集時、email の指定は必須ではありません。 • ユーザー覧表示で、email の代わりに ユーザIDを表示します。 • ログインユーザの役割変更、削除が可能です。
監査ログ	対話履歴ログのユーザIDの項目には、Active Directory ユーザのオブジェクトIDが出力されます。ユーザを識別するにはメールアドレスの列を確認してください。 管理ポータル画面操作ログのユーザIDの項目には、Active Directory ユーザのサービスプリンシパル名(ドメイン部分を含むログオン名)が出力されます。 アクセスログの username の項目には、Active Directory ユーザのログオン名(ドメイン部分含まず)が出力されます。