カスタム認証セットアップガイド

1. はじめに

本書は、Generative AI FW のシステム構築者、運用管理者のための説明書です。Generative AI FWの認証方式の変更手順について解説しています。認証方式を変更したい場合のみ、本書をお読みください。

1.1. カスタム認証とは

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、認証方式をデフォルト以外の方式(カスタム認証)に変更する方法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。認証にはメールアドレスではなくユーザ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(シングルフォレスト・シングルドメイン構成)と連携し、そのユーザ情報で認証する

本書は認証方式をカスタム認証に変更する方法について解説しています。
各認証方式で出来るようになる事や各方式での操作方法については、「カスタム認証利用ガイド」を参照ください。

> ⚠ 運用開始前にどの認証方式を利用するかを決定し、本ガイドに示す手順で認証方式の設定を実施してください。
> 運用開始後にデフォルトの認証方式に戻す、あるいは、別のカスタム認証方式に変更することはできません。

> ⚠ ユーザやグループに使用できる文字制限があります。詳細は別紙の注意制限事項ガイドを確認してください。

1.2. 用語定義について

用語定義については「スタートアップマニュアル（概要編)」をご確認ください。

1.3. 動作環境

対応するIdPの詳細は「セットアップガイド」の「動作環境」をご確認ください。

1.4. 機能差異

各認証ではユーザ・グループ管理機能に差異があります。詳細は以下の通りです。ここでの初期認証とはメールアドレスとパスワードでログインするデフォルトの認証方式です。

認証方式	ユーザ作成タイミング	グループ所属タイミング（ユーザ変更）	ユーザ・グループの同期機能
初期認証	事前登録	事前登録	無
カスタム認証（ユーザID認証）	事前登録	事前登録	無
カスタム認証（Entra ID）	初回ログイン時／事前登録	初回ログイン後／事前登録	無
カスタム認証（Active Directory）	初回ログイン時／事前登録	初回ログイン後／事前登録	有

初期認証ではユーザ作成は事前に行う必要がありましたが、カスタム認証を行うことにより一部ではユーザが初回ログインした際に、Generative AI FW側のユーザを自動で作成することが可能です。これにより管理者のユーザ作成の負担を軽減させることが可能です（初回ログイン時は一般ユーザで作成されます）。なお、事前登録は一括操作も可能です。詳細は「管理ポータル操作ガイド（基本操作編）」を参照してください。また、カスタム認証（Active Directory）では同期コマンドを用いることで、Active Directoryのユーザ・グループ情報をGenerative AI FWのユーザ・グループ情報と同期させることができます。作成だけでなく、グループの所属変更や削除にも対応しております。同期は手動または自動で行うことができるため、Active Directoryのユーザ・グループ情報をエクスポートし、管理者側で内容を変更して同期させることが可能です。詳細は「Active Directoryとの同期設定」を参照してください。また各カスタム認証ごとの機能差異はユーザ・グループ管理機能以外にもあります。詳細は後述の内容を確認してください。

2. ユーザID認証利用時の設定

認証方式として、ユーザID認証を利用する場合の手順を示します。

2.1 前提条件

- 本書の手順は「セットアップガイド」の実施が事前に完了している必要があります
  - 合わせて「正常性確認ガイド」の確認も事前に実施いただくことも推奨します
- 本書の手順はKeycloakの管理者ユーザの認証情報が必要です
- 本書の手順はGenerative AI FW のサーバにログオンした状態での操作が必要です。その際、サーバの管理者ユーザなどの**管理者権限を持つユーザで行う必要**があります

2.2 セットアップ

⚠ 本手順を実行すると、Generative AI FWサービスが再起動します。

1. 管理者アカウントでGenerative AI FWのサーバにログオンします。一般ユーザでしかログオンできない環境の場合は以下を実行し、管理者ユーザに昇格させてください。

```
sudo -i
```

2. 以下のコマンドを実行し、ユーザID認証の有効化を開始します。

```
bash /opt/nec/genai/setup/idp_setup.sh enable --type keycloak-userid
```

3. 以下のように、KeyCloakの管理者パスワードを要求されます。パスワードを入力しEnterキーを押してください。

```
Enter KeyCloak administrator password:
```

4. 最後に以下が表示されれば完了です。

```
All processes completed successfully.
```

3. IdP連携(Entra ID)認証利用時の設定

認証方式として、IdP連携(Entra ID)認証を利用する場合の手順を示します。

3.1 前提条件

- 本書の手順は「セットアップガイド」の実施が事前に完了している必要があります
  - 合わせて「正常性確認ガイド」の確認も事前に実施いただくことも推奨します
- 本書の手順は連携先の Entra ID に アプリケーションを登録できる権限を持つユーザでの操作が必要です
- 本書の手順はKeycloakの管理者ユーザの認証情報が必要です
- 本書の手順はGenerative AI FW のサーバにログオンした状態での操作が必要です。その際、サーバの管理者ユーザなどの**管理者権限を持つユーザで行う必要**があります。
- IdP連携は閉域環境（インターネットに接続できない環境）では利用できません。
- Entra IDとのhttps通信にHTTP Proxyを必要とする環境の場合、[セットアップガイド」の[proxy、証明書対応]を参照し proxy server や証明書の指定をしてください。
  - 連携先のEntra ID との通信に独自のCA証明書が必要な環境の場合、上記手順に加え、Generative AI FWサーバの以下のディレクトリに証明書を配置してください。

```
/opt/nec/genai/certs/keycloak/
```

ℹ 運用開始後は配置した証明書の有効期限に留意して、期限が切れる前に新しい証明書に置き換えてください

3.2 セットアップの流れ

EIdP連携(Entra ID)認証のセットアップの流れを示します。

1. Entra ID に連携用のアプリケーションを登録する
2. Generative AI FW で Entra ID連携を有効にする
3. Generative AI FW に 最初の管理者ユーザを登録する
4. Generative AI FW にログインできるユーザを Entra ID ユーザに限定する

2の手順の後、Generative AI FW には Generative AI FW に登録されたユーザ(初期ユーザ等)と、Entra ID ユーザの両方がログイン可能な状態になります。
3の手順で Entra IDユーザを少なくとも一人 Generative AI FW の管理者として登録し、Entra ID ユーザが正しくログインできる事を確認した後、4の手順で ログイン可能なユーザを Entra ID ユーザに限定します。

3.3 セットアップ

3.3.1 Entra ID に連携用のアプリケーションを登録する

Entra ID に Generative AI FW の 認証で用いるアプリケーションを登録してください。アプリケーションのリダイレクト先のURLは以下を指定してください。

```
https://<ドメイン名>/keycloak/realms/GenaiRealm/broker/entraid/endpoint
```

<ドメイン名>には、外部PCからGenerative AI FW のサーバにアクセスする際の以下URLに使用するドメイン名を指定します。
/opt/nec/genai/config/genai.env の GENAI_DOMAIN に指定した値と同じものを利用してください。

以降の手順で以下の情報が必要となるため、控えておいてください。

- クライアントID
- クライアントシークレット
- OpenID Connect メタデータドキュメントのURL

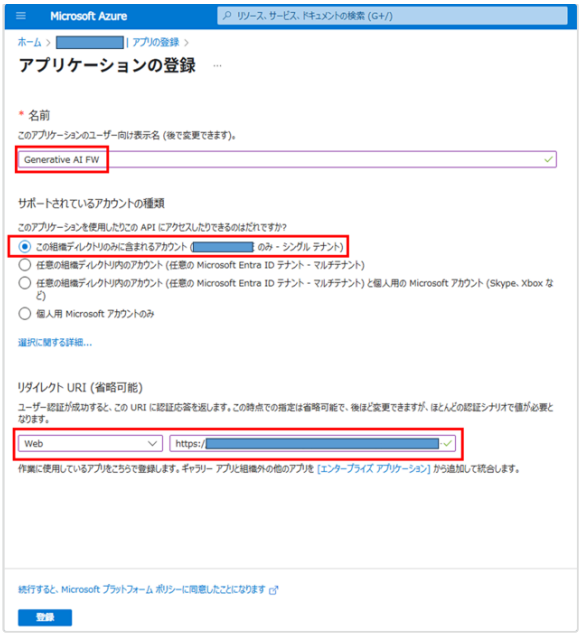
以下に操作の例を示します。連携先の Entra ID の設定や管理ルールに従って読み替えてください。

3.3.1.1 Azure portalにサインインする

1. Azure portalにサインインします。
2. 必要があれば、連携対象のディレクトリに切り替えます。
3. Azure potalメニューからEntra IDを選択します。

3.3.1.2 Entra IDのアプリケーション登録

1. 左側のナビゲーションパネルで「アプリの登録」を選択します。
2. 「＋新規登録」を選択します。
3. アプリケーションの登録ページで下記を入力し、「登録」ボタンをクリックします。
   - **名前:**《任意の名前》
   - **サポートされているアカウントの種類:** この組織ディレクトリに含まれるアカウント
   - **リダイレクトURL:**
     - **プラットフォームの選択:** Web
     - **URL:** 《控えておいたKeycloakのリダイレクトURLを入力する》



4. 作成したアプリの概要ページに表示されるアプリケーション（クライアント）IDをコピーして控えておきます。
5. 「エンドポイント」をクリックします。
6. OpenID Connect メタデータドキュメントのURLをコピーして、控えておきます。

3.3.1.3 アプリケーションへの管理者の同意の付与

1. 作成したアプリケーションの APIのアクセス許可 ページで、「<テナント名>に管理者の同意を与えます」をクリックし、管理者の同意を付与してください。

3.3.1.4 Client Secret の発行

1. 左側のナビゲーションパネルで「管理」→「証明書とシークレット」を選択します。
2. 「クライアント シークレット」にある「新しいクライアントシークレット」をクリックします。
3. 以下を入力し、「追加」を選択します。
   - **説明:** keycloak
   - **シークレットの有効期限**: 任意の有効期限を入力する

4. 表示されるシークレットの「値」をコピーして控えておきます。

3.3.2 Generative AI FW で Entra ID連携を有効にする

⚠ 本手順を実行すると、Generative AI FWサービスが再起動します。

1. 管理者アカウントでGenerative AI FWのサーバにログオンします。一般ユーザでしかログオンできない環境の場合は以下を実行し、管理者ユーザに昇格させてください。

```
sudo -i
```

2. 以下のコマンドを実行し、Entra ID 連携の有効化を開始します。

```
bash /opt/nec/genai/setup/idp_setup.sh enable --type entraid
```

3. 以下のように、KeyCloakの管理者パスワードを要求されます。パスワードを入力しEnterキーを押してください。

```
Enter KeyCloak administrator password:
```

4. 以下のように、Entra IDアプリケーション作成の確認が表示されます。[Entra ID に連携用のアプリケーションを登録する]の手順によってアプリケーションをEntra IDに作成済みであれば、 `y` を入力して Enterキーを押して次に進んで下さい。まだの場合は `n` を入力して Enterキーを押して処理を中断してください。アプリケーション作成後に再度手順 1 から実施してください。

```
Please create an application in the EntraID for federation.
Please specify the following URI as the Redirect URI:
 - https://domain-name/keycloak/realms/GenaiRealm/broker/entraid/endpoint
Please note the following information of the created application:
- OpenID Connect metadata document URL
- Client ID
- Client Secret

Have you completed creating the application and confirming the information? [y/n]:
```

5. 以下のように、Entra IDアプリケーションの OpenID Connect メタデータドキュメントのURLを要求されます。入力しEntraキーを押してください。

```
Please enter OpenID Connect information:
OpenID Connect metadata document URL (example: https://(中略)/openid-configuration):
```

   - 以下の表示となった場合、メタデータドキュメントのURLを用いた各エンドポイントの取得に失敗した事を表します。前手順で入力したURLが正しいこと、該当URLへの通信が可能なネットワーク構成であることを確認してください。 `1` を入力しEnterキーを押すと、再度本手順をやり直せます。 `2` を入力しEnterキーを押すと、処理を中断します。設定を見直し、再度手順 1 から実施してください。

```
Failed to retrieve metadata from the specified URL.

What would you like to do?
1. Retry with a different URL
2. Cancel configuration
Please select [1/2]:
```

   - 以下の表示となった場合、メタデータドキュメントのURLを用いて必要なエンドポイントを取得できた事を表します。この内容で登録して良い場合は `y` を入力しEnterキーを押してください。別のメタデータドキュメントのURLに変更する場合は、 `n` を入力して Enterキーを押してください。

```
Please confirm the retrieved OpenID Connect information:
  Metadata URL          : https://login.microsoftonline.com/{tenant-id}/v2.0/.well-known/openid-configuration
  Token Endpoint        : https://login.microsoftonline.com/{tenant-id}/oauth2/v2.0/token
  JWKS URI              : https://login.microsoftonline.com/{tenant-id}/discovery/v2.0/keys
  Issuer                : https://{tenant-id}.ciamlogin.com/{tenant-id}/v2.0
  Authorization Endpoint: https://login.microsoftonline.com/{tenant-id}/oauth2/v2.0/authorize
  End Session Endpoint  : https://login.microsoftonline.com/{tenant-id}/oauth2/v2.0/logout
  User Info Endpoint    : https://graph.microsoft.com/oidc/userinfo

Would you like to proceed with this configuration? [y/n]:
```

6. 以下のように、Entra IDのアプリケーションのクライアントIDとクライアントシークレットが要求されます。それぞれ入力しEnterキーを押してください。

```
Please enter EntraID client information:
Client ID (example: 12345678-1234-1234-1234-123456789012):
Client Secret:
```

   - 入力内容に問題なければ、以下の確認に対して `y` を入力してEnterキーを押してください。別の値に入力しなおす場合 `n` を入力してEnterキーを押してください。

```
Please confirm the entered information:
  Client ID    : d12345678-1234-1234-1234-123456789012
  Client Secret: ****************************************

Would you like to proceed with this configuration? [y/n]:
```

7. 最後に以下が表示されれば、設定がすべて正しく行われている事を示します。以下の表示なくコマンドが終了した場合、設定内容を見直し再度セットアップ手順を実行してください。

```
All processes completed successfully.
```

3.3.3 Generative AI FW に 最初の管理者ユーザを登録する

3.3.3.1 Entra ID の ユーザでチャットUIにログインする

1. Generative AI FW の組織管理者にしたい Entra ID ユーザで、チャットUIにログインします。ログイン時の認証画面で Entra ID のボタンをクリックして、Entra IDのユーザでログインしてください。

2. ログインできる事を確認後、右上のユーザ名をクリックして表示されるメニューからログアウトしてください。

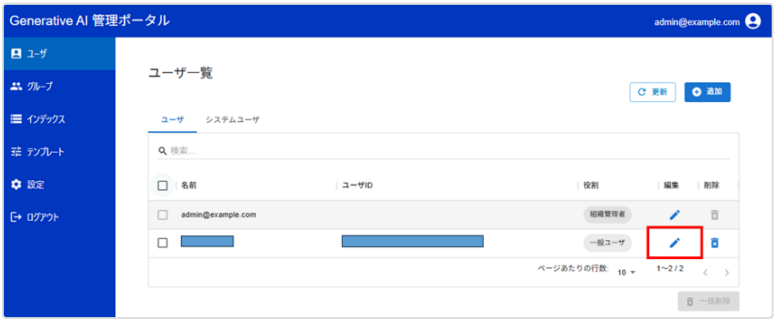
ログインに失敗する場合、Entra IDに登録したアプリケーションの設定や、Entra ID連携有効化時に指定したパラメータが正しくないことが考えられます。
Entra ID連携有効化をやり直す場合、[Generative AI FW で Entra ID連携を無効にする]の手順を実施後に再度[Generative AI FW で Entra ID連携を有効にする]の手順を実施してください。

3.3.3.2 Entra ID の ユーザの役割を組織管理者に変更する

1. Generative AI FW の組織管理ユーザ（Entra IDユーザではなく、Generative AI FW に登録済みのユーザ。初期ユーザや初期ユーザで作成した組織管理者ユーザを指す）で、管理ポータルにログインします。
Generative AI FW のユーザでログインする場合、ログイン時の認証画面で Entra ID のボタンをクリックせず、ユーザー名とパスワードに認証情報を入力してサインインボタンをクリックしてください。

ユーザー名には登録時に指定したメールアドレスを指定してください。

2. ログインした管理ポータルでユーザー覧ページを開きます。チャットUIにログインしたEntra IDユーザを一覧さがし、編集アイコンをクリックしてください。



3. 遷移したユーザ編集画面で、役割を組織管理者に変更し、変更ボタンをクリックします。

4. 左メニューからログアウトをクリックしてログアウトしてください。

> Entra ID ユーザでチャットUIに一度でもログインすると、そのユーザは自動的に Generative AI FW に登録されます。
> 登録されたユーザは、管理ポータルから役割や所属グループを変更することが可能です。

> 組織管理者のEntra ID ユーザを登録した後も、組織管理者のGenerative AI FW ユーザ(初期ユーザ等)を1名は削除せずに残すことを推奨します。
> 誤って組織管理者のEntra IDユーザをすべて削除した際に、新しく組織管理者ユーザを追加することができなくなります。

3.3.4 Generative AI FW にログインできるユーザを Entra ID ユーザに限定する

> 本手順を実施後、連携先のEntra ID ユーザ以外は Generative AI FW へログインできなくなります。
> 1名以上のEntra ID ユーザが管理ポータルにログインできる事を確認後に、本手順を実施してください。

1. 管理者アカウントでGenerative AI FWのサーバにログオンします。一般ユーザでしかログオンできない環境の場合は以下を実行し、管理者ユーザに昇格させてください。

```
sudo -i
```

2. 以下のコマンドを実行し、ログインユーザをEntra ID ユーザに限定する設定を開始します。

```
bash /opt/nec/genai/setup/idp_setup.sh useidp --type external
```

3. 以下のように、KeyCloakの管理者パスワードを要求されます。パスワードを入力しEnterキーを押してください。

```
Enter KeyCloak administrator password:
```

4. 最後に以下が表示されれば完了です。

```
All processes completed successfully.
```

> 本手順実施後はチャットUI・管理ポータルのログイン時にEntra IDの認証画面が直接表示されます。
> 初期ユーザ等のEntra IDのユーザではないユーザではログインできなくなります。

3.3.5 Generative AI FW で Entra ID連携を無効にする

Entra IDとの連携設定の中で指定するパラメータを間違えたといった理由で[Generative AI FW で Entra ID連携を有効にする]の手順の後に連携設定をやり直したい場合、一度連携設定を無効化した後、有効化の手順を再実行する必要があります。

以下に、連携設定を無効化する手順を示します。

1. 管理者アカウントでGenerative AI FWのサーバにログオンします。一般ユーザでしかログオンできない環境の場合は以下を実行し、管理者ユーザに昇格させてください。

```
sudo -i
```

2. 以下のコマンドを実行し、Entra ID 連携設定の無効化を開始します。

```
bash /opt/nec/genai/setup/idp_setup.sh disable --type entraid
```

3. 以下のように、KeyCloakの管理者パスワードを要求されます。パスワードを入力しEnterキーを押してください。

```
Enter KeyCloak administrator password:
```

4. 最後に以下が表示されれば完了です。

```
All processes completed successfully.
```

3.4 運用中の設定変更

3.4.1 Entra ID の クライアントシークレットの更新

Entra ID の アプリケーションのクライアントシークレットを更新する場合、以下の手順に従ってください。

1. 管理者アカウントでGenerative AI FWのサーバにログオンします。一般ユーザでしかログオンできない環境の場合は以下を実行し、管理者ユーザに昇格させてください。

```
sudo -i
```

2. 以下のコマンドを実行し、Entra ID 連携設定の更新を開始します。

```
bash /opt/nec/genai/setup/idp_setup.sh update --type entraid
```

3. 以下のように、KeyCloakの管理者パスワードを要求されます。パスワードを入力しEnterキーを押してください。

```
Enter KeyCloak administrator password:
```

4. 以下のように、Entra IDのアプリケーションのクライアントIDとクライアントシークレットが要求されます。それぞれ入力しEnterキーを押してください。

```
Please enter EntraID client information:
Client ID (example: 12345678-1234-1234-1234-123456789012):
Client Secret:
```

   - 入力内容に問題なければ、以下の確認に対して `y` を入力してEnterキーを押してください。別の値に入力しなおす場合 `n` を入力してEnterキーを押してください。

```
Please confirm the entered information:
  Client ID    : d12345678-1234-1234-1234-123456789012
  Client Secret: ****************************************

Would you like to proceed with this configuration? [y/n]:
```

5. 最後に以下が表示されれば完了です。

```
All processes completed successfully.
```

3.4.2 Generative AI FW のユーザもログインできるようにする

[Generative AI FW にログインできるユーザを Entra ID ユーザに限定する] の手順を取り消し、初期ユーザ等の Generative AI FW ユーザでもログイン出来るようにする為の手順です。

> 組織管理者のEntra IDユーザをすべて削除した場合等、管理ポータルにログインできるEntra IDユーザがいなくなってしまった場合に、本手順を活用してください。
>
> 本手順実行後に、[Generative AI FW に 最初の管理者ユーザを登録する]と[Generative AI FW にログインできるユーザを Entra ID ユーザに限定する] の手順を再度実行してください。

1. 管理者アカウントでGenerative AI FWのサーバにログオンします。一般ユーザでしかログオンできない環境の場合は以下を実行し、管理者ユーザに昇格させてください。

```
sudo -i
```

2. 以下のコマンドを実行し、ログインユーザをEntra ID ユーザに限定する設定の解除を開始します。

```
bash /opt/nec/genai/setup/idp_setup.sh useidp --type both
```

3. 以下のように、KeyCloakの管理者パスワードを要求されます。パスワードを入力しEnterキーを押してください。

```
Enter KeyCloak administrator password:
```

4. 最後に以下が表示されれば完了です。

```
All processes completed successfully.
```

4. IdP連携(Active Directory)認証利用時の設定

認証方式として、IdP連携(Active Directory)認証を利用する場合の手順を示します。

4.1 前提条件

- 本書の手順は「セットアップガイド」の実施が事前に完了している必要があります
  - 合わせて「正常性確認ガイド」の確認も事前に実施いただくことも推奨します
- 本書の手順は連携先のActive Directoryに登録されたユーザの認証情報が必要です
- 本書の手順はKeycloakの管理者ユーザの認証情報が必要です
- 本書の手順はGenerative AI FW のサーバにログオンした状態での操作が必要です。その際、サーバの管理者ユーザなどの**管理者権限を持つユーザで行う必要**があります。

4.2 セットアップの流れ

IdP連携(Active Directory)認証のセットアップの流れを示します。

1. 連携先のActive Directoryの情報を確認する
2. Generative AI FW で Active Directory 連携を有効にする
3. Active Directoryとの同期を手動もしくは自動化で実施する（実施は任意）

1の手順で連携先のActive Directoryの情報を確認し、その情報を用いて 2の手順を実施します。

4.3 セットアップ

4.3.1 連携先のActive Directoryの情報を確認する

連携先のActive Directory の以下の情報を収集し控えます。

項目	説明	例
Active Directory URL	連携するActive Directory にアクセスするためのURL。 LDAPを利用する場合は ldap:// で始まるURLとなる。 LDAPSを利用する場合は ldaps:// で始まるURLとなる。 ⚠ Windows Server 2025 の Active Directory の場合、ldaps のみをサポートします。	ldaps://ad.example.com:636 ldap://ad.example.com:389
Active Directory bind user DN	連携のために、連携先のActive Directoryを参照するためのユーザを1名登録する必要がある。そのユーザのDN。	CN=service,CN=Users,DC=example,DC=com
Active Directory bind user password	上記Bind Userのパスワード。	
User registration directory DN	連携先のActive Directoryの本サービスのログインを許可するユーザを登録しているコンテナ・OU(組織単位)のDN。ここで指定したコンテナ・OUの直下に登録されているユーザが対象となる。	CN=Users,DC=example,DC=com
LDAPS で利用するCA証明書	Active Directoryへの接続に LDAPS を用い、かつ、サーバ証明書の検証に独自のCA証明書が必要な場合のみ必要。 該当する証明書ファイル(PEM、または、PKCS12)を後続の手順で利用する。	

4.3.2 Generative AI FW で Active Directory 連携を有効にする

⚠ 本手順を実行すると、Generative AI FWサービスが再起動します。

1. 管理者アカウントでGenerative AI FWのサーバにログオンします。一般ユーザでしかログオンできない環境の場合は以下を実行し、管理者ユーザに昇格させてください。

```
sudo -i
```

2. LDAPSで独自のCA証明書が必要な場合は、Generative AI FWサーバの以下のディレクトリに証明書を配置してください。

```
/opt/nec/genai/certs/keycloak/
```

ℹ 運用開始後は配置した証明書の有効期限に留意して、期限が切れる前に新しい証明書に置き換えてください

3. 以下のコマンドを実行し、Active Directory 連携の有効化を開始します。

```
bash /opt/nec/genai/setup/idp_setup.sh enable --type ad
```

4. 以下のように、KeyCloakの管理者パスワードを要求されます。パスワードを入力しEnterキーを押してください。

```
Enter KeyCloak administrator password:
```

5. 以下のように、[連携先のActive Directoryの情報を確認する]の手順で控えた情報が要求されます。それぞれ入力しEnterキーを押してください。

```
Please enter Active Directory connection information:
Active Directory URL (example: ldaps://ad.example.com:636, ldap://ad.example.com:389):
Active Directory bind user DN (example: CN=service,CN=Users,DC=example,DC=com):
Active Directory bind user password:
User registration directory DN (example: CN=Users,DC=example,DC=com):
```

   - 入力内容に問題なければ、以下の確認に対して `y` を入力してEnterキーを押してください。別の値に入力しなおす場合 `n` を入力してEnterキーを押してください。

```
Please confirm the entered information:
  Active Directory URL          : ldaps://ad.example.com:636
  Bind user DN                  : CN=service,CN=Users,DC=example,DC=com
  Bind user password            : ************
  User registration directory DN: CN=Users,DC=example,DC=com
```

6. 最後に以下が表示されれば、設定がすべて正しく行われている事を示します。以下の表示なくコマンドが終了した場合、設定内容を見直し再度セットアップ手順を実行してください。

```
All processes completed successfully.
```

7. 連携ができた事を確認するために、[カスタム認証利用ガイド]の手順で、Active Directoryユーザでのチャット UIへログイン出来る事を確認します。

ℹ ログインに失敗する場合、以下の原因が考えられます。

- Generative AI FW サーバからActive Directory までのネットワーク到達性に問題がある
- ldaps で利用する証明書が正しくない、または期限が切れている
- Active Directory連携有効化時に指定したパラメータが正しくない

上記設定やネットワーク構成に問題がないかを確認してください。Active Directory連携有効化をやり直す場合、[Generative AI FW で Active Directory 連携を無効にする]の手順を実施後に再度[Generative AI FW で Active Directory 連携を有効にする]の手順を実施してください。

⚠ 組織管理者のActive Directoryユーザを登録した後も、組織管理者のGenerative AI FW ユーザ(初期ユーザ等)を1名は削除せずに残すことを推奨します。
誤って組織管理者のActive Directoryユーザをすべて削除した際に、新しく組織管理者ユーザを追加することができなくなります。

8. Active directoryとの同期を行う場合は後述の「Active Directoryとの同期設定」を実施してください。

4.3.3 Generative AI FW で Active Directory 連携を無効にする

Active directoryとの連携設定の中で指定するパラメータを間違えたといった理由で[Generative AI FW で Active Directory 連携を有効にする]の手順の後に連携設定をやり直したい場合、一度連携設定を無効化した後、有効化の手順を再実行する必要があります。

以下に、連携設定を無効化する手順を示します。

1. 管理者アカウントでGenerative AI FWのサーバにログオンします。一般ユーザでしかログオンできない環境の場合は以下を実行し、管理者ユーザに昇格させてください。

```
sudo -i
```

2. 以下のコマンドを実行し、Active Directory 連携設定の無効化を開始します。

```
bash /opt/nec/genai/setup/idp_setup.sh disable --type ad
```

3. 以下のように、KeyCloakの管理者パスワードを要求されます。パスワードを入力しEnterキーを押してください。

```
Enter KeyCloak administrator password:
```

4. 最後に以下が表示されれば完了です。

```
All processes completed successfully.
```

> 本手順は無効化する手順のため、再度有効化の手順実施が必要です。先述の「Generative AI FW で Active Directory 連携を有効にする」の手順を最初から実施してください。

4.4 運用中の設定変更

4.4.1 Active Directory bind userの更新

Active Directory bind user やそのパスワードを変更する場合、以下の手順に従ってください。

1. 管理者アカウントでGenerative AI FWのサーバにログオンします。一般ユーザでしかログオンできない環境の場合は以下を実行し、管理者ユーザに昇格させてください。

```
sudo -i
```

2. 以下のコマンドを実行し、Active Directory 連携設定の更新を開始します。

```
bash /opt/nec/genai/setup/idp_setup.sh update --type ad
```

3. 以下のように、KeyCloakの管理者パスワードを要求されます。パスワードを入力しEnterキーを押してください。

```
Enter KeyCloak administrator password:
```

4. 以下のように、Active Directory bind user 情報要求されます。それぞれ入力しEnterキーを押してください。

```
Please update Active Directory bind user information:
Active Directory bind user DN (example: CN=service,CN=Users,DC=example,DC=com):
Active Directory bind user password:
```

   - 入力内容に問題なければ、以下の確認に対して `y` を入力してEnterキーを押してください。別の値に入力しなおす場合 `n` を入力してEnterキーを押してください。

```
Please confirm the entered information:
  Bind user DN                  : CN=service,CN=Users,DC=example,DC=com
  Bind user password            : ************

Would you like to proceed with this configuration? [y/n]:
```

5. 最後に以下が表示されれば完了です。

```
All processes completed successfully.
```

5. Active Directoryとの同期設定

Generative AI FWではActive Directoryのユーザ・グループ情報をGenerative AI FW側のユーザ・グループ情報に同期させることができます。

同期は同期コマンドを用いて以下の順序で行います。

1. Active Directoryのユーザ・グループ情報をファイルにエクスポートする
2. １でエクスポートしたファイルを編集する（任意）
3. Generative AI FWにエクスポートしたファイルをインポートする

> 本手順はあくまでもユーザ・グループ情報を同期することが対象です。テンプレートやインデックスなどの認可のための操作についてはユーザ・グループ登録後に管理ポータル画面から実施してください。

同期方法には手動で同期コマンドを実行する方法と自動で同期させる方法があります。以下を参照しにどちらで行うか選択してください。

⚠ 初回同期時は手動での同期にて実施してください。自動での同期は同期処理が安定して動作することを確認してから使用することを推奨します。

同期方法	メリット	デメリット
手動での同期	• 管理者権限の付与などをユーザ登録前に行うことができる • ユーザ名やグループ名、メンバー所属などを任意に変更することができる	• インポート前にエクスポートしたファイルを編集する必要がある
自動での同期	• 定期的に同期を自動で行うことができる • エクスポートしたファイルを編集する必要がない	• Active Directoryのユーザ・グループ情報とGenerative AI FW側のユーザグループ情報が一致している必要がある • Generative AI FWの管理者にする場合はユーザ登録後に管理ポータル画面から行う必要がある

5.1 同期対象

同期対象のユーザ・グループの条件は以下の通りです。

グループ

コマンドのパラメータとして指定したコンテナや組織単位(OU)配下のグループのうち、以下の条件を満たすグループが対象です。

- 種別がセキュリティグループである（配布グループではない）
- 予めActive Directoryに用意されている組み込みグループではない

ユーザ

コマンドのパラメータとして指定したコンテナや組織単位(OU)配下のユーザが対象です。

5.2 動作環境

- Active Directoryとの同期を自動するためにはGenerative AI FW のサーバとは別にWindows端末が必要になります。同期コマンドの動作環境は以下の通りです。
  - Windows 11
  - Windows PowerShell 5.1 以上
  - PowerShell 7.5以上
- 自動設定手順にはWindowsのタスクスケジューラ機能を使用します。

ℹ 本コマンドを実行するPowerShell の実行ポリシーは、RemoteSigned 等、署名のないローカルスクリプトを実行可能なポリシーとしてください。

例えば、現在Windowsにログインしているユーザの実行ポリシーを RemoteSigned に変更するには PowerShell で以下を実行してください。

```
Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope CurrentUser -Force
```

5.3 Generative AI FW側でのセットアップ（手動・自動共通）

1. 管理者アカウントでGenerative AI FWのサーバにログオンします。一般ユーザでしかログオンできない環境の場合は以下を実行し、管理者ユーザに昇格させてください。

```
sudo -i
```

2. 以下のコマンドを実行し、Active Directory 連携と同期するための管理APIを公開します。

```
cd /opt/nec/genai/setup
bash admin_api_setup.sh
```

3. 下記が表示されれば完了です。

```
Admin API route setup succeeded
```

5.4 同期コマンドセットアップ（手動・自動共通）

同期コマンドは別紙「はじめに」に記載する「マニュアルURL」のサイトにアクセスし、その他の項目にあるActive Directory同期コマンドをダウンロードすることで入手できます。解凍して使用してください。

以下のファイルが含まれています。

ファイル名	説明
Export-ADUserGroup.ps1	Active Directoryのユーザ・グループ情報をファイルにエクスポートするコマンド。
Export-ADUserGroup.ini.template	Export-ADUserGroup.ps1 の設定ファイルのテンプレート。 設定ファイルでパラメータを指定する場合、本ファイルの末尾の .tempalte を削除したうえで編集してください。
Import-GenAIUserGroup.ps1	Generative AI FWにエクスポートしたファイルをインポートするコマンド。
Import-GenAIUserGroup.ini.template	Import-GenAIUserGroup.ps1 の設定ファイルのテンプレート。 設定ファイルでパラメータを指定する場合、本ファイルの末尾の .tempalte を削除したうえで編集してください。
Run-ADSync.ps1	Export-ADUserGroup.ps1 と Import-GenAIUserGroup.ps1 を順に実行し、Active DirectoryとGenerative AI FWの同期を実行するコマンド。 自動での同期を行う場合にこのコマンドを利用します。

5.4.1 同期コマンドの配置と設定ファイルの作成

同期コマンドを実行するWindows端末で以下の操作を行います。

1. 同期コマンドを任意の場所に解凍します
2. Export-ADUserGroup.ini.templateとImport-GenAIUserGroup.ini.templateをそれぞれExport-ADUserGroup.iniとImport-GenAIUserGroup.iniにファイル名を変更します
3. Export-ADUserGroup.iniとImport-GenAIUserGroup.iniをそれぞれ編集し、各項目を設定します

> 設定ファイルに指定するパラメータの詳細は、「Active Directory 同期コマンド リファレンスガイド」を参照してください。

> パラメータは、設定ファイルを用いずコマンドの引数として指定することも可能です。詳細は、「Active Directory 同期コマンド リファレンスガイド」を参照してください。

5.5 手動での同期手順

Active Directory 同期コマンドを手動で実行し、任意のタイミングでActive Directory のユーザ・グループ情報を Generative AI FW に同期する手順について説明します。
本手順は同期コマンドを配置したWindows端末上で行います。

5.5.1 Active Directory からの ユーザ・グループ情報のエクスポート

1. PowerShell で同期コマンドを配置したディレクトリに移動します。

```
PS C:\> Set-Location C:\adsync\
PS C:\adsync>
```

2. Export-ADUserGroup.ps1 を実行します。

```
PS C:\adsync> .\Export-ADUserGroup.ps1
グループ情報取得完了: 5 件
ユーザー情報取得完了: 7 件
=== 全ての処理が正常に完了しました ===
PS C:\adsync>
```

「=== 全ての処理が正常に完了しました ===」と表示されれば成功です。
代わりに別のエラーメッセージが表示された場合、パラメータで指定した値やActive Directoryとのネットワーク環境を見直してください。

5.5.2 エクスポートされたユーザ・グループ情報の編集

1. エクスプローラーでパラメータ `ExportDirectoryPath` で指定したディレクトリに移動します。

2. ad_user_info.csv を メモ帳やExcelで開き、役割を変更したいユーザの authority 列を編集して上書き保存します。

	A	B	C	D	E	F	G	H
1	user id	user name	authority	group name 1	group name 2	group name 3	group name 4	group name 5
2	cc55f922-d127-42f6-a71d-fbe2cfc977f7	USER01						
3	c6f55e74-ca51-41e7-98ef-a036e256dbfd	USER02		GROUP-A				
4	cc836092-ba89-4ec3-9ae6-e4306e3a1ba2	USER03		GROUP-A	GROUP-B			
5	038f3bcc-691c-4a22-aba1-dca2b034de1f	USER04		GROUP-A	GROUP-B	GROUP-C		
6	e8f698b3-8ee0-48d4-ad44-5f02dc43a669	USER05	indexes:documents	GROUP-A	GROUP-B	GROUP-C	GROUP-D	
7	cb0debfa-ee93-4b7b-9f46-9e36e7038a74	USER06	admin	GROUP-A	GROUP-B	GROUP-C	GROUP-D	GROUP-E

authority 列に指定可能な値は、「Active Directory 同期コマンド リファレンスガイド」を参照してください。

Export-ADUserGroup.ps1 が出力する ad_user_info.csv の authority 列はすべて空白となっています。空白のまま Generative AI FW にインポートした場合のユーザの役割は以下です。

- 既に該当ユーザが Generative AI FW に作成されている場合は、インポートによって役割を変更されません。現在の役割が維持されます
- 該当ユーザが Generative AI FW に存在せず、インポートによって作成する場合、役割は「一般ユーザ」となります

初回の同期時に authority を編集し役割を変更した場合でも、2回目以降の同期では authority を編集する必要はありません。

ad_group_info.csv や ad_user_info.csv の authority 以外の項目の変更は推奨しません。Active Directory と異なる状態でユーザやグループが同期されてしまいます。
もし変更を行う場合は、手動・自動の同期を行う都度、ad_group_info.csv や ad_user_info.csv に同じ変更を加えてください。

5.5.3 Generative AI FW へのユーザ・グループ情報のインポート

1. PowerShell で同期コマンドを配置したディレクトリに移動します。

```
PS C:\> Set-Location C:\adsync\
PS C:\adsync>
```

2. Import-GenAIUserGroup.ps1 を実行します。

```
PS C:\adsync> .\Import-GenAIUserGroup.ps1
グループ情報をCSVから読み込みました: (件数: 5)
++グループ作成
対象:5, 成功:5, 失敗:0, 未実施:0
対象グループをすべて作成しました。
++グループ削除
対象:0, 成功:0, 失敗:0, 未実施:0
削除対象のグループはありません
ユーザー情報をCSVから読み込みました: (件数: 7)
++ ユーザー作成
対象:7, 成功:7, 失敗:0
対象ユーザーをすべて作成しました
++ ユーザー更新
対象:0, 成功:0, 失敗:0
対象ユーザーはありません
++ ユーザー削除
対象:0, 成功:0, 失敗:0
対象ユーザーはありません
=== 全ての処理が正常に完了しました ===
PS C:\adsync>
```

「=== 全ての処理が正常に完了しました ===」と表示されれば成功です。

代わりに別のエラーメッセージが表示された場合、パラメータで指定した値やGenerative AI FWとのネットワーク環境を見直してください。

5.6 自動での同期手順

Active Directory 同期コマンドをタスクスケジューラに登録し、定期的に自動で同期を行う手順について説明します。
自動化のセットアップはWindows端末上で行います。

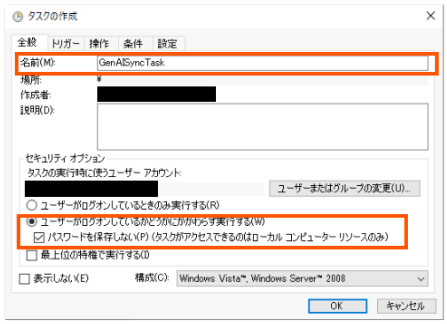
5.6.2 Windowsタスクスケジューラの設定

- 同期間隔は 1 日に 1 回程度を推奨します。短いと処理が完了しない可能性があります。

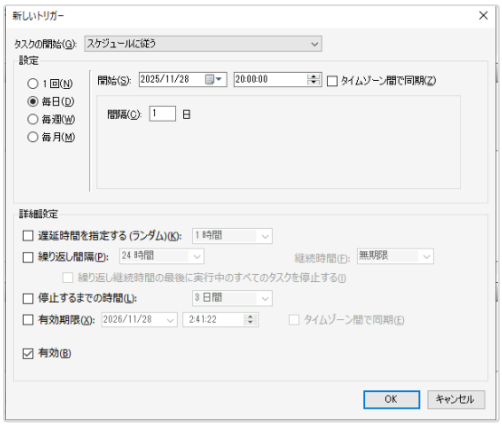
- タスクを登録するユーザは管理者権限（Administratorsグループに所属するユーザ）で登録してください。権限を持たない場合、「ユーザがログオンしているかどうかにかかわらず実行する」機能を使用することができません。

1. Windowsタスクスケジューラを開き、下記のようにタスクの作成ボタンを押下します。

2. 画像の赤枠のように全般タブの名前に「GenAISyncTask」を指定します。また、画像のセキュリティオプションの赤枠の「ユーザーがログオンしているかどうかにかかわらず実行する」を選択し、「パスワードを保存しない」にチェックを入れます。



3. トリガータブを開き、新規ボタンを押下します。下記のようなウィンドウが表示されるため、ここで同期スクリプトの実行間隔を設定します。設定後、OKボタンを押します。
   毎日20:00に1回実行する設定の場合、下記画像のような設定になります。



4. 操作タブを開き、新規ボタンを押下します。下記のようなウィンドウが表示されるため、参照ボタンからPowershellの実行ファイルを選択します。
   そして、引数の追加に `-ExecutionPolicy RemoteSigned -File "<Run-ADSync.ps1のパス>"` を入力しOKボタンを押下します。
   (Powershell 7の場合はデフォルトで `"C:¥Program Files¥PowerShell¥7¥pwsh.exe"` に存在します)

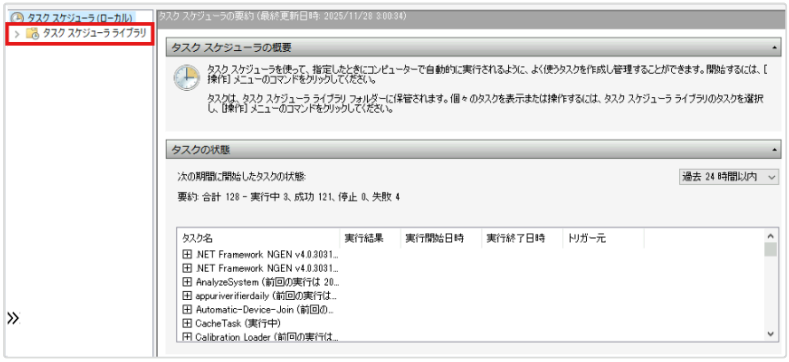
事前に「同期コマンドの配置と設定ファイルの作成」で作成した設定ファイルに設定値を設定しておいてください。

5. タスクの作成画面でOKボタンを押して完了です。

5.6.3 実行したタスクスケジューラのタスク結果の確認手順

「Windowsタスクスケジューラの設定」で設定した同期タスクの実行結果の確認手順を説明します。

1. Windowsタスクスケジューラを開き、タスクスケジューラライブラリをクリックし選択します。

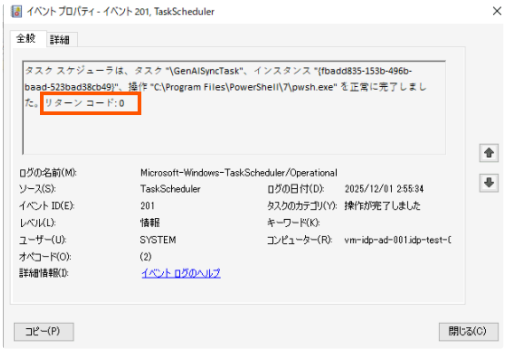


2. 表示される一覧にある「GenAISyncTask」をクリックし選択します。

3. 下の画面の履歴タブを選択し、表示される一覧の中に「操作が完了しました」という項目が複数あります。それぞれ選択しダブルクリックして確認します。

4. 画像のようなダイアログウィンドウ表示され、その中に表示される「リターンコード」の値が0ならば、正常に操作が完了しています。

   0以外のときは、「Active Directory 同期コマンド リファレンスガイド」の「ログ」の章を参照し、ログを確認してください。



5.7 Active Directoryとの同期設定の解除

Active Directoryと同期の解除手順を示します。同期解除は同期処理をしていないことを確認の上実施してください。

5.7.1 Generative AI FW側での同期解除手順（手動・自動共通）

同期のために設定した管理用APIを非公開に変更します。手順は以下の通りです。

1. 管理者アカウントでGenerative AI FWのサーバにログオンします。一般ユーザでしかログオンできない環境の場合は以下を実行し、管理者ユーザに昇格させてください。

```
sudo -i
```

2. 以下のコマンドを実行し、Active Directory連携と同期するための管理APIを非公開にします。

```
cd /opt/nec/genai/setup
bash admin_api_setup.sh delete
```

3. 下記が表示されれば完了です。

```
Admin API route deletion succeeded
```

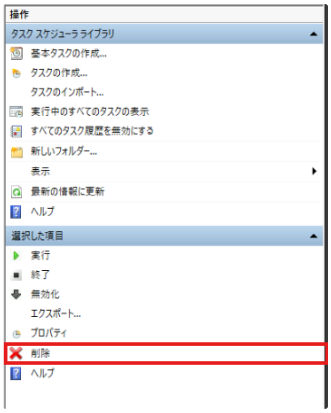
5.7.2 作成したWindowsタスクスケジューラタスクの削除

以下の手順は同期を自動化した場合のみ実施してください。自動化していない場合は実施不要です。

1. Windowsタスクスケジューラを開き、タスクスケジューラライブラリをクリックし選択します。

2. 表示される一覧にある「GenAISyncTask」をクリックし選択します。

3. 右側に表示される操作欄の中で「選択した項目」配下にある削除を押下してタスクを削除します。



4. 「このタスクを削除しますか」というダイアログが表示されるため、「はい」を押下して完了です。