Active Directory 同期コマンド リファレンスガイド

本ガイドでは、Active Directory 同期コマンドの詳細を説明します。利用方法については「カスタム認証セットアップガイド」の「Active Directoryとの同期設定」を合わせて参照ください。

Active Directory 同期コマンドは、カスタム認証の一つである IdP連携(Active Directory)認証 を利用する場合に、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するためのコマンドです。

以下の2つのコマンドを提供しています。

- **Export-ADUserGroup.ps1**: Active Directoryからユーザ・グループの情報を取得し、ファイルに出力する
- **Import-GenAIUserGroup.ps1**: ユーザ・グループ情報をファイルから読み込み、その内容と一致するように Generative AI FW のユーザ・グループ情報を追加・変更・削除する

Export-ADUserGroup.ps1 の出力ファイルが、**Import-GenAIUserGroup.ps1** の入力ファイルになります。これらのコマンドを順番に実行することで、Active Directory の ユーザ・グループ情報を Generative AI FW に同期することができます。

1. Export-ADUserGroup.ps1

指定した Active Directory のユーザ・グループを読み込み、ファイルに出力します。対象のユーザ・グループは以下です。

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。

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

1.1 コマンド引数

```
Export-ADUserGroup.ps1 -ADDomain <DOMAIN> -ADPort <PORT NUMBER> [ -UseLDAPS ] -ADUser <USER NAME> -ADPass <PA
                       -ADUserDNList <DN LIST> -ADGroupDNList <DN List>
                       [ -Insecure ] [ -ExportDirectoryPath <PATH> ] [ -LogBackupNum <NUMBER> ]
```

1.2 設定ファイルフォーマット

コマンドの引数として指定できる値は、設定ファイルで指定することも可能です。
コマンドと同じディレクトリに、 `Export-ADUserGroup.ini` という名前のファイルを以下のフォーマットで配置すると、このファイルの値を読み込みます。
設定ファイル内に指定したパラメータは、コマンドの引数の指定を省略できます。(後述の引数の表で必須となっているパラメータは、引数か設定ファイルのどちらかで指定が必要です。)
設定ファイルと引数の両方で指定したパラメータは、引数で指定した値を優先します。

`ADUserDNList` と `ADGroupDNList` に複数のDNを指定する場合は、複数行記載してください。

設定ファイルは ;(セミコロン)で始まる行をコメントとして扱います。

<パラメータ名>=<値>の形式で列挙します。

- = の前後に空白を含めないでください。また、値をダブルコーテーションやシングルコーテーションで囲まないでください。
- パラメータを省略する場合、<値>の部分だけでなく、パラメータの行自体を記載しないかコメントアウトしてください。

```
ADDomain=<DOMAIN>
ADPort=<PORT NUMBER>
UseLDAPS=true|false
ADUser=<USER NAME>
ADPass=<PASSWORD>
ADUserDNList=<DN 1>
ADUserDNList=<DN 2>
...
ADGroupDNList=<DN 1>
ADGroupDNList=<DN 2>
...
Insecure=true|false
ExportDirectoryPath=<PATH>
LogBackupNum=<NUMBER>
```

1.3 パラメータ

引数、または、設定ファイルで指定可能なパラメータについて説明します。

パラメータ	必須	意味	例
`-ADDomain <DOMAIN>`	必須	エクスポートする Active Directory のドメイン	`adserver.abc.com`
`-ADPort <PORT NUMBER>`	必須	Active Directory とのLDAP通信に利用するポート番号。	`389`

		Active Directory では、LDAPの場合は389、LDAPSの場合は636がデフォルト値です。	
-ADUser <USER NAME>	必須	本コマンドでActive Directory のユーザ・グループ情報を閲覧するために利用するユーザ名。 エクスポートするActive Directory 上のドメインユーザを指定してください。	User01
-ADPass <PASSWORD>	必須	-ADUser で指定したユーザのパスワード	P@ssw0rd
-UseLDAPS	任意	Active Directory との通信に LDAP ではなく LDAPS を利用する。 コマンド引数では値の指定は不要ですが、設定ファイルで指定する場合は true または false を値として指定してください。(true: LDAPSを利用する。false: LDAPSを利用しない(LDAPを利用する))	
-ADUserDNList <DN LIST>	必須	エクスポートするユーザの範囲を表すDN。コンテナや組織単位(OU)やドメイン(DC)を指すDNを指定してください。その配下のすべてのユーザが同期対象となります。 ⚠ Active Directory との連携設定時に、「User registration directory DN 」として指定したDNを利用してください。	"CN=Users,DC=adserver,DC=abc,DC=com"
-ADGroupDNList <DN LIST>	必須	エクスポートするグループの範囲を表すDNのリスト。コンテナや組織単位(OU)やドメイン(DC)を指すDNを指定してください。その配下のすべてのグループが同期対象となります。 ℹ 複数のDNを指定する場合、引数渡しの場合は右の例のようにカンマ区切りで指定してください。設定ファイルでは複数行で指定してください。	"ON=Tokyo,DC=adserver,DC=abc,DC=com","ON=Hukuoka,DC=adserver,DC=abc,DC=com"

`-Insecure`	任意	Active Directory へのLDAPS接続時に証明書の検証をスキップする。 コマンド引数では値の指定は不要ですが、設定ファイルで指定する場合は true または false を値として指定してください。(true: 検証をスキップする。false: 検証をスキップしない) ℹ 自己署名証明書を利用している場合は検証に失敗するため、本オプションを利用してください。	
`-ExportDirectoryPath <PATH>`	任意	Active Directoryから取得したユーザ・グループ情報のエクスポートファイルを出力するディレクトリのパス。 存在しないディレクトリを指定した場合はコマンドは失敗します。 省略した場合、本コマンドの配置ディレクトリに出力します。	`C:¥Users¥user1¥genaiimport`
`-LogBackupNum <NUMBER>`	任意	本コマンドの実行時のログファイルのバックアップ数。本コマンドは実行する都度を実行すると毎回新しいファイルにログを出力します。過去に実行した際のログをこのパラメータで指定した数だけ保持します。 1-100 を指定してください。省略時のデフォルト値は5です。	`10`

1.3.1 パラメータ設定例1: LDAP で接続。Usersコンテナのユーザ、ドメインすべてのグループを同期する

引数で指定する場合

```
Export-ADUserGroup.ps1 -ADDomain ”adserver.example.com” -ADPort 389 -ADUser ”GenAISyncOperator” -ADPass ”ewqo
                       -ADUserDNList ”CN=Users,DC=adserver,DC=example,DC=com” -ADGroupDNList ”DC=adserver,DC=
```

設定ファイルで指定する場合

```
ADDomain=adserver.example.com
ADPort=389
ADUser=GenAISyncOperator
ADPass=ewqo9bru
ADUserDNList=CN=Users,DC=adserver,DC=example,DC=com
```

```
ADGroupDNList=DC=adserver,DC=example,DC=com
```

1.3.2 パラメータ設定例2: LDAPS で接続。LDAPSの証明書は自己署名証明書を利用。組織単位 Org01 のユーザ、グループを同期する

引数で指定する場合

```
Export-ADUserGroup.ps1 -ADDomain "adserver.example.com" -ADPort 636 -UseLDAPS -ADUser "GenAISyncOperator" -AD
                       -ADUserDNList "OU=Org01,DC=adserver,DC=example,DC=com"
                       -ADGroupDNList "OU=Org01,DC=adserver,DC=example,DC=com" `
                       -Insecure
```

設定ファイルで指定する場合

```
ADDomain=adserver.example.com
ADPort=636
UseLDAPS=true
ADUser=GenAISyncOperator
ADPass=ewqo9bru
ADUserDNList=OU=Org01,DC=adserver,DC=example,DC=com
ADGroupDNList=OU=Org01,DC=adserver,DC=example,DC=com
Insecure=true
```

1.4 終了コード

終了コード	意味
0	正常終了
1	異常終了

1.5 出力ファイル

正常終了した場合、Actove Directory から取得したユーザ情報を記載したファイル `ad_user_info.csv` とActove Directoryから取得したグループ情報を記載したファイル `ad_group_info.csv` を `ExportDirectoryPath` で指定したディレクトリに出力します。

> 出力先に同名の既存のファイルがあった場合は内容が上書きされます。

それぞれのフォーマットを以下に示します。

ad_user_info.csv

1行目はラベルで2行目以降にユーザの情報が並びます。1行が1ユーザを表しています。

```
user id,user name,authority,group name 1,group name 2,...
<USER ID>,<USER NAME>,<AUTHORITY>,<GROUP NAME 1>,<GROUP NAME 2>,...
<USER ID>,<USER NAME>,<AUTHORITY>,<GROUP NAME 1>,<GROUP NAME 2>,...
```

ラベル	値	補足

<table>
<tr><td>user id</td><td><Active Directory の <code>objectGUID</code> ></td><td>ユーザID。Generative AI FW にインポートする際のユーザIDに利用します。</td></tr>
<tr><td>user name</td><td><Active Directory の <code>sAMAccountName</code> ></td><td>ユーザ名。Generative AI FW にインポートする際のユーザ名に利用します。</td></tr>
<tr><td>authority</td><td><空白></td><td>ユーザの役割。出力時は常に空白。空白の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しません
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
役割を指定する場合は以下の文字列を指定してください。<table><tr><th>値</th><th>意味</th></tr><tr><td><code>general</code></td><td>一般ユーザ</td></tr><tr><td><code>admin</code></td><td>組織管理者</td></tr><tr><td>以下の値の1つ以上の組み合わせ。複数指定する場合は、:（コロン）で区切る(例： <code>users:groups</code> ）
<code>users</code>
<code>groups</code>
<code>indexes</code>
<code>documents</code>
<code>templates</code></td><td>それぞれ、以下の意味を持つ。
ユーザ管理者
グループ管理者
インデックス管理者
ドキュメント管理者
テンプレート管理者</td></tr></table></td></tr>
<tr><td>group name n</td><td><ユーザが所属しているグループの名前。Active Directory の <code>CN</code> ></td><td>グループ名。Generative AIにインポートする際のユーザ所属のグループ名に利用します。</td></tr>
</table>

ad_group_info.csv

1行目はラベルで2行目以降にグループの情報が並びます。1行が1つのグループの情報です。

```
group name
<GROUP NAME>
```

```
3 <GROUP NAME>
```

ラベル	値	補足
group name	<Active Directory の `CN`>	グループ名。Generative AIにインポートする際のグループ名に利用します。

1.6 ログ

コマンドを実行する都度新しいファイルにログを出力します。最新の実行ログとは別に、過去 `LogBackupNum` 回分のログが保持されます。
コマンドと同じディレクトリに、 `Export-ADUserGroup.log` という名前のファイルでログを出力します。
過去のログは `Export-ADUserGroup.log.n` という名前で、nには1-100の数字が入ります。1が前回実行時のログ、5は5回前に実行したときのログを表しています。

2. Import-GenAIUserGroup.ps1

ユーザ・グループ情報ファイルを読み込み、同じ内容になるように、Generative AI FW のユーザ・グループの情報を変更します。

> Active Directory側のグループ名を変更する場合は注意が必要な場合があるため、後述の「注意事項」を一読したうえでコマンドを実行するようにお願いします

2.1 コマンド引数

```
1 Import-GenAIUserGroup.ps1 -GADomain <DOMAIN> [ -GAPort <PORT NUMBER> ] [ -GAUserMail <MAIL ADDRESS> ]
2                           [ -GAUserID <USER ID> ] -GAAPIKey <API Key>
3                           [ -Delete ] [ -Insecure ] [ -ImportDirectoryPath <PATH> ] [ -LogBackupNum <NUMBER>
```

2.2 設定ファイルフォーマット

コマンドの引数として指定できる値は、設定ファイルで指定することも可能です。
コマンドと同じディレクトリに、 `Import-GenAIUserGroup.ini` という名前のファイルを以下のフォーマットで配置すると、このファイルの値を読み込みます。
設定ファイル内に指定したパラメータは、コマンドの引数の指定を省略できます。（後述の引数の表で必須となっているパラメータは、引数か設定ファイルのどちらかで指定が必要です。）
設定ファイルと引数の両方で指定したパラメータは、引数で指定した値を優先します。

> 設定ファイルは ；（セミコロン）で始まる行をコメントとして扱います。

> ⚠ <パラメータ名>=<値>の形式で列挙します。

- = の前後に空白を含めないでください。また、値をダブルコーテーションやシングルコーテーションで囲まないでください。
- パラメータを省略する場合、<値>の部分だけでなく、パラメータの行自体を記載しないかコメントアウトしてください。

```
GADomain=<DOMAIN>
GAPort=<PORT NUMBER>
GAUserMail=<MAIL ADDRESS>
GAUserID=<USER ID>
GAAPIKey=<API Key>
Delete=true|false
Insecure=true|false
ImportDirectoryPath=<PATH>
LogBackupNum=<NUMBER>
```

2.3 パラメータ

引数、または、設定ファイルで指定可能なパラメータについて説明します。

パラメータ	必須	意味	例
`-GADomain <DOMAIN>`	必須	同期先のGenerative AI FWのドメイン。	`genai.abc.com`
`-GAPort <PORT NUMBER>`	任意	Generative AI FW に https でアクセスするためのポート番号。本パラメータを省略時は、Generative AI FW のデフォルトのポート番号である 443 を利用します。	`8080`

`-GAUserMail <MAIL ADDRESS>`
 	
`-GAUserID <USER ID>`
	どちらか一方は必須	Generative AI FW の操作で利用する、Generative AI FW の管理者ユーザの識別子。
		Generative AI FW に登録されている(管理ポータルのユーザ一覧で表示される)ユーザを指定してください。
		
		Active Directory ユーザの場合は、Generative AI FW の管理ポータルのユーザ一覧・ユーザ編集画面で確認できる ユーザIDを `GAUserID` に指定してください。
		初期ユーザ等の Generative AI FW ユーザの場合は、Generative AI FW の管理ポータルのユーザ編集画面で確認できる emailを `GAUserMail` に指定してください。
			`admin@example.com`
			
			`e94047f5-37db-4746-96f5-43c08ce5403e`

		このパラメータで指定したユーザの役割変更や削除が行われるインポートは失敗します。本パラメータには、Generative AI FW の初期ユーザ（admin@example.com）を `GAUserMail` で指定する事を推奨します。	
`-GAAPIKey <API Key>`	必須	Generative AI FW の API の APIキー。	`682af577ddee41de8ea9090a7b71c1ec`
`-Delete`	任意	指定した場合、`ad_user_info.csv` に存在せずGenerative AI FW に存在するユーザ、`ad_group_info.csv` に存在せず Generative AI FW に存在するグループをを削除します。省略した場合、ユーザ・グループ情報の作成・変更は行いますが削除は行いません。 コマンド引数では値の指定は不要ですが、設定ファイルで指定する場合は true または false を値として指定してください。(true: 削除する。false: 削除しない) 初期値は削除しない設定になっています。不要なユーザ・グループを削除する場合のみ削除する設定に切り替えることを推奨します	
`-Insecure`	任意	Generative AI FW へのHTTPS接続時に証明書の検証をスキップする。 コマンド引数では値の指定は不要ですが、設定ファイルで指定する場合は true または false を値として指定してください。(true: 検証をスキップする。false: 検証をスキップしない) 自己署名証明書を利用している場合は検証に失敗するため、本オプションを利用してください。	
`-ImportDirector`	任意	インポートするファイルが配置されたディレクトリのパス。	`C:¥Users¥user1¥genaiimport`

`yPath <PATH>`		Export-ADUserGroup.ps1 が出力したファイルが配置されているディレクトリを指定してください。本コマンドは指定されたディレクトリの `ad_user_info.csv` と `ad_group_info.csv` を読み込みます。 存在しないディレクトリを指定した場合や、上記のファイル名のファイルが存在しないディレクトリを指定した場合は、コマンドは失敗します。 省略した場合、本コマンドの配置ディレクトリの`ad_user_info.csv` と `ad_group_info.csv` を読み込みます。	
`-LogBackupNum <NUMBER>`	任意	本コマンドの実行時のログファイルのバックアップ数。本コマンドは実行する都度を実行すると毎回新しいファイルにログを出力します。過去に実行した際のログをこのパラメータで指定した数だけ保持します。 1-100 を指定してください。省略時のデフォルト値は5です。	`10`

2.3.1 パラメータ設定例1: 初期ユーザを利用して同期し、ユーザ・グループの削除も同期する。Generative AI FW は 自己署名証明書を利用

引数で指定する場合

```
Import-GenAIUserGroup.ps1 -GADomain ”genai.example.com” -GAUserMail ”admin@example.com” -GAAPIKey ”XXXXX” -De
```

設定ファイルで指定する場合

```
GADomain=genai.example.com
GAUserMail=admin@example.com
GAAPIKey=75534eb26ad346388f98b16ec13b23fe
Delete=true
Insecure=true
```

2.3.2 パラメータ設定例2: ADユーザを利用して同期。ユーザ・グループの削除は同期しない

引数で指定する場合

```
Import-GenAIUserGroup.ps1 -GADomain ”genai.example.com” -GAUserId ”bbdfed0b-8bb0-4d98-bc62-57d8e085e232” -GAA
```

設定ファイルで指定する場合

```
GADomain=genai.example.com
GAUserId=bbdfed0b-8bb0-4d98-bc62-57d8e085e232
GAAPIKey=XXXX
```

2.4 終了コード

終了コード	意味
0	正常終了
1	異常終了。原因は標準出力を参照。

2.5 入力ファイル

本コマンドは、`ImportDirectoryPath` に配置された、Active Directory から取得したユーザ情報を記載したファイル `ad_user_info.csv` と、Active Directory から取得したグループ情報を記載したファイル `ad_group_info.csv` を読み込みます。

`ad_user_info.csv` と `ad_group_info.csv` は Export-ADUserGroup.ps1　が出力したファイルを利用してください。

2.6 ログ

コマンドを実行する都度新しいファイルにログを出力します。最新の実行ログとは別に、過去 `LogBackupNum` 回分のログが保持されます。
コマンドと同じディレクトリに、 `Import-GenAIUserGroup.log` という名前のファイルでログを出力します。
過去のログは `Import-GenAIUserGroup.n` という名前で、nには1-100の数字が入ります。1が前回実行時のログ、5は5回前に実行したときのログを表しています。

3. 注意事項

- Active Directory は OU が異なる場合同じグループ名(CN)を利用可能ですが、本コマンドは同じグループ名が含まれる複数のOUの情報を同期することはできません
- Generative AI に、Active Directory のグループと同じ名前のグループが複数存在する場合、その中のどのグループが利用されるかは不定です
- **Active Directoryでユーザ名を変更した場合でも変更前と変更後のユーザは同一として扱われます。そのため変更後に必要な操作は特にありません。変更後のユーザ名でログインしてください。**
- **Active Directory で グループ名を変更した場合、Genrative AI FW では別のグループとして扱われます。そのため、以下の手順に従い削除することを強く推奨します。**

a. Active Directory側にてグループ名を変更します（変更前のグループ名はメモしておいてください）
b. 同期用コマンドを用いてGenerative AI FWに変更内容を反映します。ただし、Import-GenAIUserGroup.ps1のパラメータ`Delete`の値は必ずfalse(引数を利用する場合は `-Delete` を指定しない)で実行してください。
c. 反映後、テンプレート、インデックスなどのメニューから変更前のグループが付与されているものを検索し、変更前のグループを所属から除外し、変更後のグループに新たに所属するよう設定を変更してください。変更後のグループ名が認可設定に使用されてないようにしてください。
d. 管理ポータル画面から変更後のグループ名が使用されていないことを確認したうえで、再度同期用コマンドを用いてGenerative AI FWに変更内容を反映します。Import-GenAIUserGroup.ps1のパラメータ`Delete`の値は必ずtrue(引数を利用場合は `-Delete` を指定する)で実行してください。

- Active Directory上で無効なユーザであっても、Generative AI FW に同期されます
- Active Directory の 組み込みグループ、配布グループは同期対象外です
- 操作の進捗確認がタイムアウトしました（最大試行回数: 720）というログが出ている場合は、同期処理自体は継続中のためしばらく待つと反映されます