JCCH・セキュリティ・ソリューション・システムズ

プライベート認証局 Gléas ホワイトペーパー

LDAP Managerとのクライアント証明書の管理連携

Ver. 1.0
2017 年 6 月

目次

1. はじめに

1.1. 本書について

本書では、弊社製品「プライベート認証局 Gléas」で発行したクライアント証明書を利用して、エクスジェン・ネットワークス株式会社のID管理製品「LDAP Manager」と連携してクライアント証明書の発行をおこなう環境を構築するための設定例を記載します。

本書に記載の内容は、弊社の検証環境における動作を確認したものであり、あらゆる環境での動作を保証するものではありません。弊社製品を用いたシステム構築の一例としてご活用いただけますようお願いいたします。

1.2. 本書における環境

本書における手順は、以下の環境で動作確認を行っています。

- メタディレクトリ：LDAP Manager 6.8
  ※以後、「LDAP Manager」と記載します
  ※以下のプラグインを利用しています
  - CSV→LDAP反映&CSV→LDAPグループメンテナンスプラグイン
  - LDAP→CSV反映プラグイン
  - LDAP→AD反映&ADグループメンテナンスプラグイン

  ※以下のWindows Server（ドメインコントローラ）上に構築しています
- Active Directory：Microsoft Windows Server 2012 R2 Standard
  ※以後、「AD」と記載します
- JS3 プライベート認証局 Gléas （バージョン1.14.6）
  ※以後、「Gléas」と記載します

以下については、本書では説明を割愛します。

- LDAP Managerおよび追加プラグインのインストールと基本的な設定
- LDAP ManagerからADへのID連携
- Gléasでのアカウント登録や各種証明書発行
- Windows ServerやWindowsドメインのセットアップ

これらについては、各製品のマニュアルをご参照いただくか、各製品を取り扱っている販売店にお問い合わせください。

1.3. 本書における構成

本書では、以下の構成で検証を行っています。

【クライアント証明書発行】

1. LDAP Managerコンソールから CSVプラグインを利用して、ユーザIDの追加をおこなう
2. LDAP Managerは、ADへのアカウント同期をおこない、かつGléasのIDM連携APIを利用してアカウント登録／証明書発行依頼をおこなう

【クライアント証明書失効】

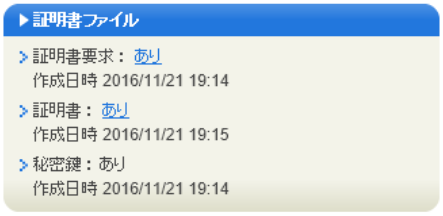
1. LDAP Managerコンソールから CSVプラグインを利用して、ユーザIDの削除をおこなう
2. LDAP Managerは、ADの対象ユーザアカウントを無効にし、かつGléasのIDM連携APIを利用してアカウント削除／証明書の失効依頼をおこなう

2. Gléas での事前設定

Gléas に対し API アクセスをするためには、事前に API アクセス用のクライアント証明書を指定しておく必要があります。

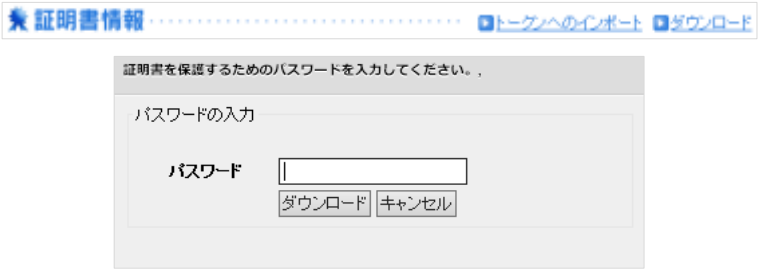
※ 下記設定は、Gléas 納品時等に弊社で設定を既に行っている場合があります

Gléasの管理者画面（RA）にログインし、API管理者とするユーザアカウントの証明書詳細画面に移動し、[証明書：あり]のリンクより証明書ファイル（.crtファイル）をダウンロードします。



その後、画面上部の[▶管理者]リンクより管理者一覧 ＞ API管理者の詳細画面に移動します。
次に、[参照]ボタンをクリックし、さきほどダウンロードした証明書をアップロード（登録）します。

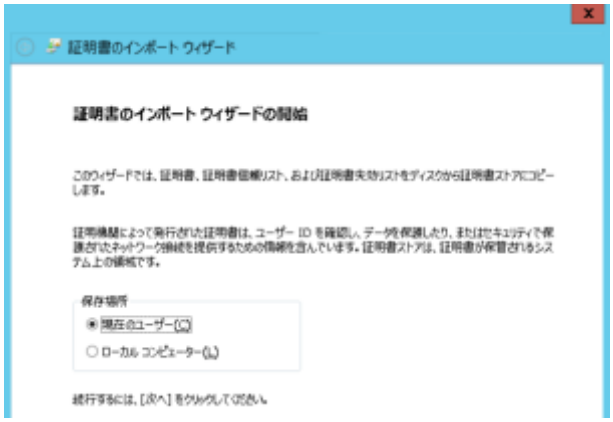
またLDAP ManagerサーバからのAPIアクセスのために証明書詳細画面の[▶ダウンロード]リンクより証明書ファイル（.p12ファイル）をダウンロードしておきます。



※ダウンロード時に入力を要求されるファイルの保護パスワードはLDAP Managerホスト（Windows Server）に証明書をインポートする際に必要となります

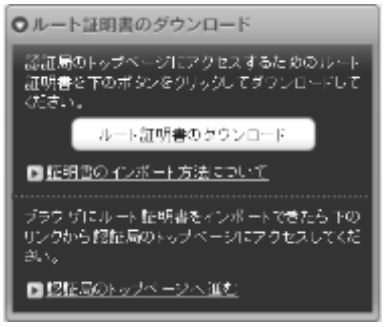
以上でGléas側の設定は終了です。

LDAP Managerホストにこの証明書ファイルを移動し、ダブルクリックすると起動するウィザードにしたがい証明書をインポートします。



インポート後に、コントロールパネル ＞ インターネットオプション ＞[コンテンツ]タブ ＞ [証明書] ＞ [個人]タブより証明書の拇印を確認しておきます（後述するPowerShellスクリプトからGléasへのアクセスに必要な情報になります)。

また、RA用証明書を発行しているGléasの管理用CAを信頼する必要があります。GléasにhttpでアクセスするとルートCA証明書のダウンロードができるので、そのファイルを開いて[証明書のインストール]をクリックし、[信頼されたルート証明機関]にインポートします。

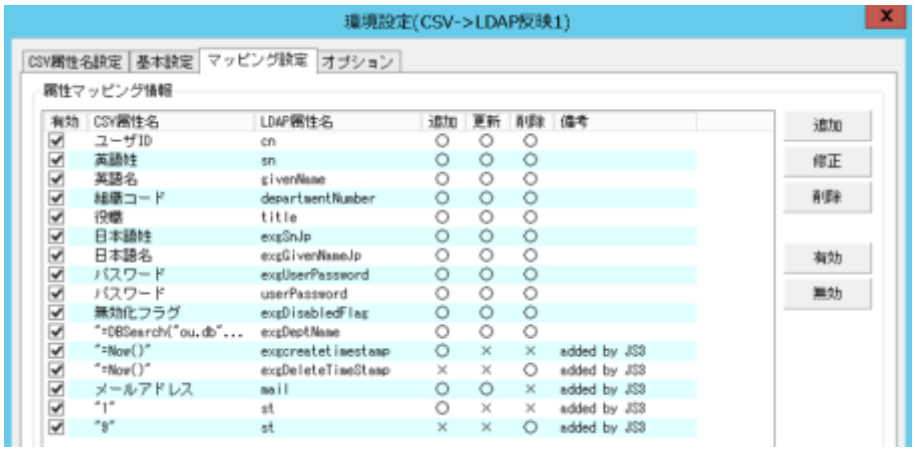


3. LDAP Managerの設定

3.1. CSV→LDAP プラグイン設定

LDAP Manager コンソールを起動し、[環境設定] > [CSV→LDAP] > [CSV->LDAP 反映 1]を開き、マッピング設定をおこないます。

本検証では、ID 追加・削除に関して st 属性をそのフラグとしています（ID 追加時には 1、ID 削除時には 9、データ連携完了時には 3.2 項で設定するリバースマッピング機能を使い 0 をセットします）。



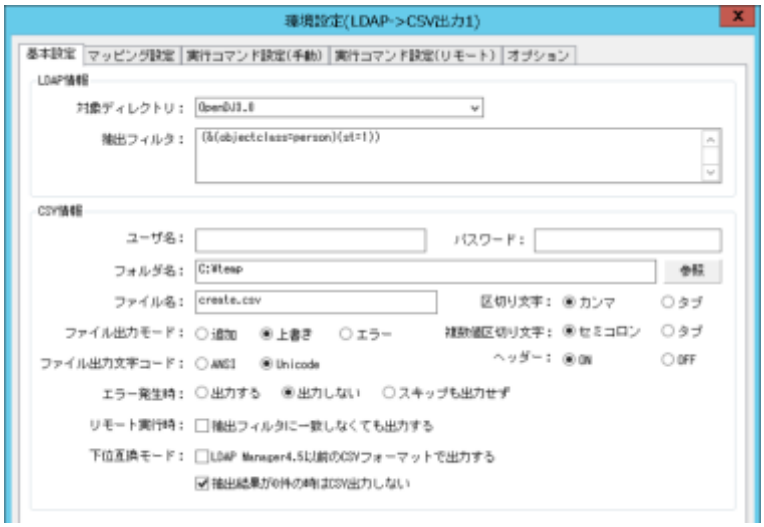
※マッピング設定で指定したい属性が表示されない場合は、[環境設定] > [ディレクトリ属性設定] より属性追加をおこないます

設定完了後、[OK]をクリックします。

3.2. LDAP→CSV プラグイン設定

ID 追加時のデータ連携処理用に[環境設定] > [LDAP->CSV 出力 1]を開き、「基本設定」タブで各項目の設定をおこないます。

- 抽出フィルタ（検索条件）は、st=1 を含むものにします
- フォルダ名・ファイル名は、あとで設定する Gléas アップロード用スクリプトにあわせておきます
- 区切り文字：カンマを選択
- ファイル出力モード：上書きを選択
- ファイル出力文字コード：Unicode を選択
- エラー発生時：出力しないを選択
- ヘッダー：ON を選択
- 下位互換モード：[抽出結果が 0 件の時は CSV 出力しない]をチェック



「マッピング設定」タブで、以下の設定をおこないます。

- 属性マッピング情報で以下を設定します

LDAP 属性名	CSV 属性名
cn	cn
exgSnJp	sn
exgGivenNameJP	givenName
exgUserPassword	password
mail	mail

※Gléas の API 仕様上、CSV の cn、sn、givenName 属性は必須項目になります

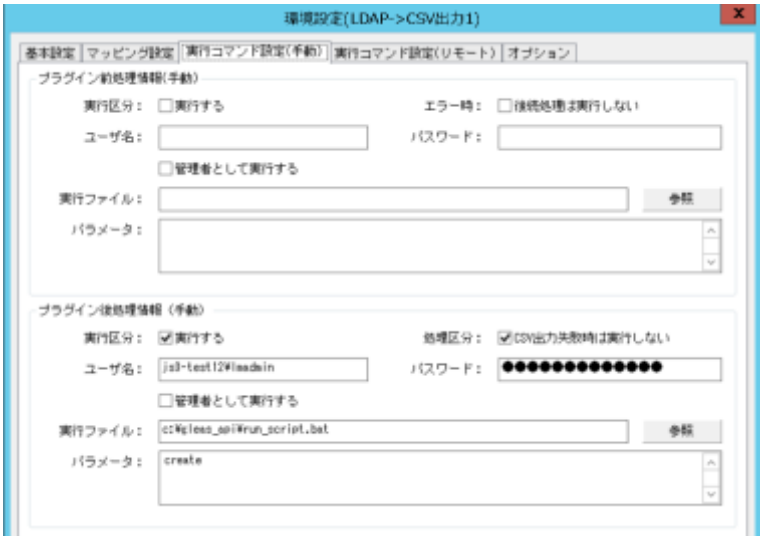
※CSV の password 属性は、Gléas の証明書配布サイト（UA）のログインに利用されます。Gléas UA では、LDAP/AD 内のパスワードを利用することも可能なので、その場合はこの項目は不要となります

- リバースマッピング情報で以下を設定します

値	LDAP 属性名
0	st

「実行コマンド設定（手動)」タブのプラグイン後処理情報（手動）で、以下の設定をおこないます。

- 実行区分：[実行する]をチェック
- 処理区分：[CSV 出力失敗時は実行しない]をチェック
- ユーザ名・パスワードには、実行ユーザ情報を入力
- 実行ファイル：起動するスクリプト（バッチファイル）のファイルパスを入力
- パラメータ：スクリプト実行時の引数を指定



Gléas への API 連携用スクリプトとして、本検証では以下を作成しています。

【スクリプト起動用バッチファイルのサンプル】
LDAP Manager の実行コマンド設定では、直接 PowerShell スクリプトを起動できないためバッチファイルを指定し PowerShell スクリプトを起動させています。

```
%SystemRoot%¥System32¥WindowsPowerShell¥v1.0¥powershell.exe ^
-Command "c:¥gleas_api¥csvUpload.ps1 %1"
```

【Gléas 連携用スクリプト（PowerShell）のサンプル】

```
#Gleasアクセス情報
$gleasHostName = "gleas.example.com"
$certHash = "1ff12dff8b61eb271befabb82648826cb74c0bd9" #API証明書の拇印
switch($args[0])
{
   "create" {
      $uri = "https://" + $gleasHostName + "/ra/entities/notify/create"
      break
   }
   "destroy" {
      $uri = "https://" + $gleasHostName + "/ra/entities/notify/action"
   }
}

#入出力ファイル
$folderPath = "c:¥temp¥"
$csvFilePath = $folderPath + $args[0] + ".csv"
$resultFilePath = $folderPath + $args[0] + "_result.txt"

#POSTデータ作成
$contentType = "multipart/form-data"
$boundary = [guid]::NewGuid().ToString()
$lf = "`r`n"
```

```
$codePage = “iso-8859-1”
$fileBin = [System.IO.File]::ReadAllBytes($csvFilePath)
$enc = [System.Text.Encoding]::GetEncoding($codePage)
$fileContent = $enc.GetString($fileBin)

$bodyLines = (
    "--$boundary",
    "Content-Disposition: form-data; name=`"csv`"",
    "Content-Type: application/octet-stream$lf",
    $fileContent,
   "--$boundary",
   "Content-Disposition: form-data; name=`"request_cert`"$lf",
   "true",
    "--$boundary--$lf"
) -join $lf

#Gleasへのデータアップロード
$response = (Invoke-WebRequest -Method Post -Uri $uri `
-Body $bodyLines -ContentType "$contentType; boundary=$boundary" `
-CertificateThumbprint $certHash)

#HTTPステータスコード(正常時は200)
$response.StatusCode | Out-File $resultFilePath

#処理結果メッセージ、トランザクションID、アップしたファイルのダイジェスト値の取得
$content = write $response | select -Expand Content | ConvertFrom-Json
$content.message | Out-File $resultFilePath -append
$content.trans_id | Out-File $resultFilePath -append
$content.digest | Out-File $resultFilePath -append

exit
```

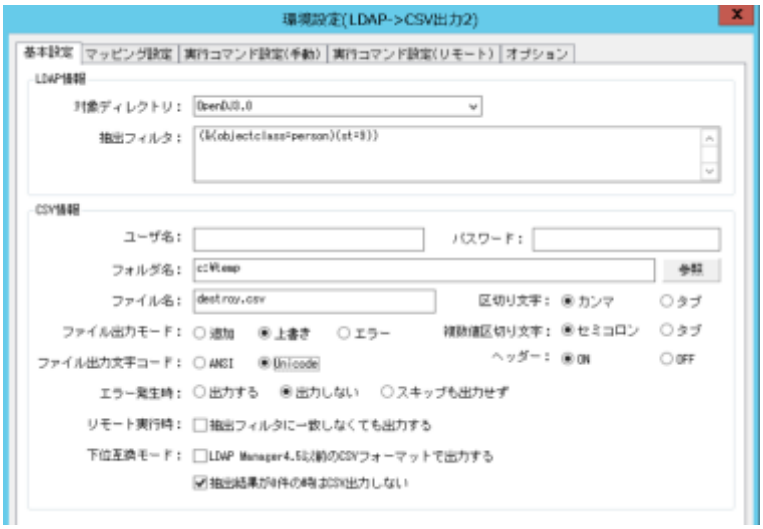
※データ連携（CSV ファイルのアップロード）の実行結果は、HTTP のステータスコードで知ることができます。正常だと 200 が返ってきます

※アップロード正常完了＝処理予約であり、実際の処理がおこなわれるまで 1~2 分のタイムラグが発生します。処理結果を取得するには、アップロード完了時に得られるトランザクション ID を用いて、処理終了後に Gléas に問い合わせる必要があります

設定完了後、[OK]をクリックします。

ID 削除時のデータ連携処理用に[環境設定] > [LDAP->CSV 出力 2]を開き、「基本設定」タブで各項目の設定をおこないます。

- 抽出フィルタ(検索条件)は、st=9 を含むものに
- 他項目は[LDAP->CSV 出力 1]と同じ（ファイル名などは適宜変更）



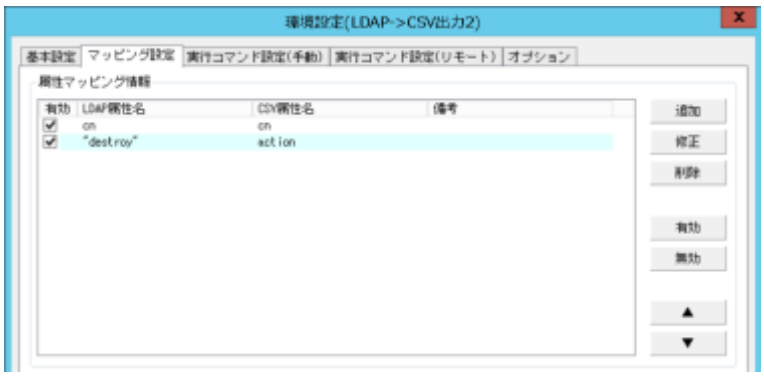
「マッピング設定」タブで、以下の設定をおこないます。

- 属性マッピング情報で以下を設定

LDAP 属性名	CSV 属性名
cn	cn
“destroy”　※単一値	action

- リバースマッピング情報で以下を設定

値	LDAP 属性名
0	st



「実行コマンド設定（手動）」タブのプラグイン後処理情報（手動）は、[LDAP->CSV出力 1]と同じですが、連携スクリプトの内容の関係上、実行ファイルのパラメータを”destroy”にします。

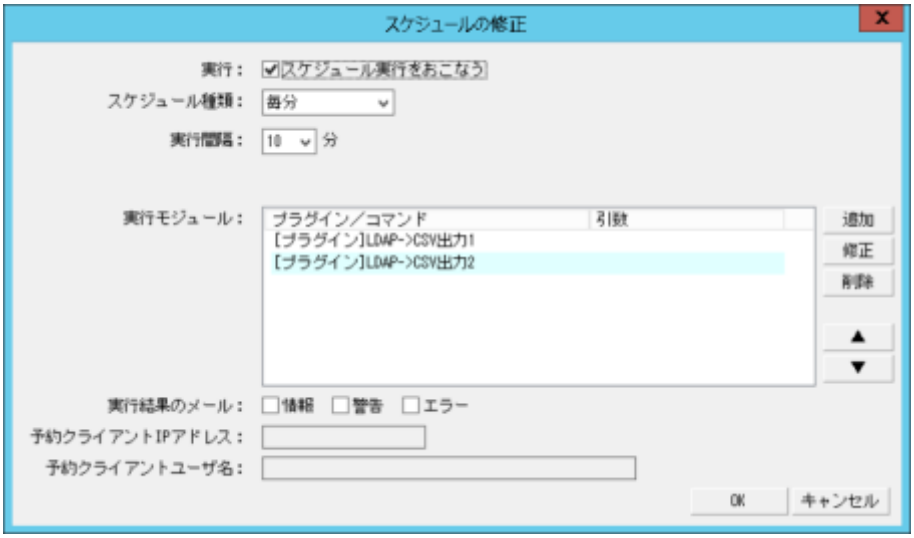
設定完了後、[OK]をクリックします。

3.3. プラグインの定期実行設定

LDAP->CSV 自動出力 を定期実行させる設定をおこないます。
[環境設定] > [基本設定] > [スケジュール管理]タブを開き、[スケジュール追加]ボタンをクリックし、以下を設定します。

- [スケジュール実行をおこなう]にチェック
- スケジュール種類と実行間隔は、データ更新頻度を設定
- 実行モジュールは[追加]をクリックし、先に設定した LDAP->CSV 出力 1 および 2 を設定

以下は最少間隔の 10 分ごとにデータ連携をおこなう例です。



設定完了後、[OK]をクリックします。

LDAP Manager での設定は以上です。

4. LDAP ManagerとGléasのデータ連携

4.1. ID 追加と証明書発行

以下の内容の CSV ファイルを準備し、CSV->LDAP 反映プラグイン設定で指定したフ

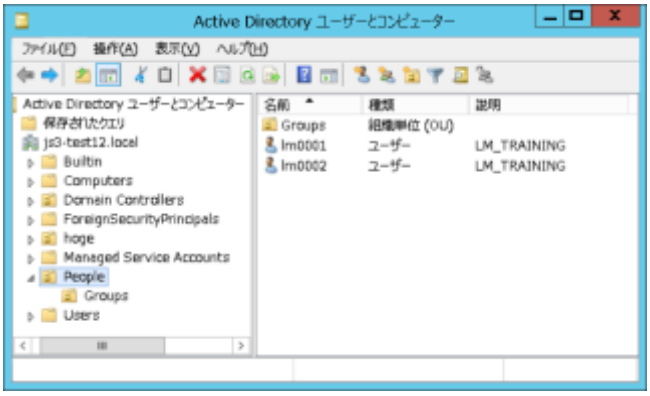
ォルダに配置します。

ChangeType	ユーザID	英語姓	英語名	日本語姓	日本語名	パスワード	役職	組織コード	無効化フラグ	メールアドレス
add	lm0001	test	ichiro	テスト	一郎	P@ssw0rd	担当	1001	0	test01@jcch-sss.com
add	lm0002	test	jiro	テスト	二郎	P@ssw0rd	担当	1001	0	test02@jcch-sss.com

LDAP Manager コンソールで、[手動実行] > [CSV->LDAP] > [CSV プラグイン実行 1]を選択し、CSV ファイルからの ID 取り込みをおこないます。
成功するとコンソールに以下のログエントリが表示されます。

```
2017/06/01 16:56:00 – [CSV プラグイン実行 1]合計：2 件 正常処理：2 件(追加：2、更新：0、削除：0) スキップ処理：0 件 エラー処理：0 件
```

CSV プラグイン実行 1 に、LDAP->AD 反映 の実行が設定されている場合は、AD に ID 情報が伝搬されます。



また定期実行のタイミングで LDAP→CSV 出力 プラグインが実行され、成功するとコンソールに以下のログエントリが表示されます。

```
2017/06/01 17:02:00 – [LDAP->CSV 出力 1] 合計：2 件 正常処理：2 件 スキップ処理：0 件 エラー処理：0 件 後処理：成功
```

連携が正常におこなわれると、Gléas RA の [登録申請者一覧]メニューより連携されたユーザ情報が表示されます。

[全て許可する]、あるいは一件ずつ[許可する]ことにより登録申請が承認され、クライアント証明書の発行まで自動でおこなわれます。

※この許可操作は、自動承認機能を利用することにより自動化が可能です

※発行通知メール送信機能が有効な場合は、証明書発行後に指定されたメールアドレス宛に証明書発行通知が配信されます

4.2. ID 削除（無効化）と証明書失効

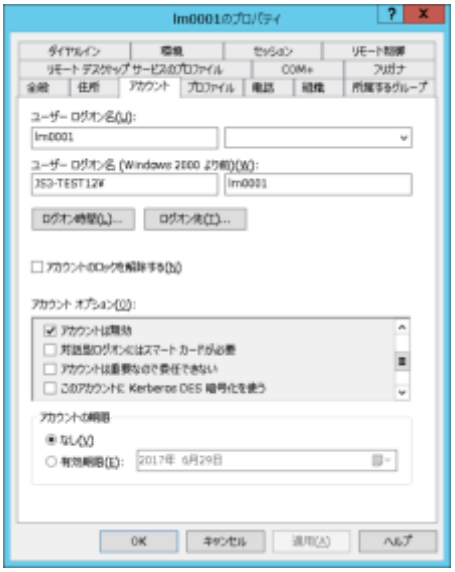
以下の内容の CSV ファイルを準備し、CSV->LDAP 反映 プラグインの設定で指定したフォルダに配置します。

ChangeType	ユーザID	無効化フラグ
del	lm0001	1
del	lm0002	1

LDAP Manager コンソールで、[手動実行] > [CSV->LDAP] > [CSV プラグイン実行 1]を選択し、CSV ファイルからの ID 取り込みをおこないます。
成功するとコンソールに以下のログエントリが表示されます。

```
2017/06/01 17:26:00 – [CSV プラグイン実行 1]合計：2 件 正常処理：2 件(追加：0、更新：0、削除：2) スキップ処理：0 件 エラー処理：0 件
```

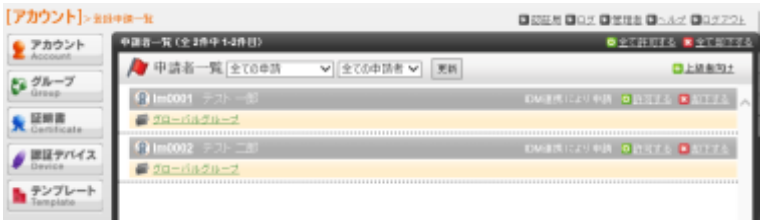
CSV プラグイン実行 1 に、LDAP->AD 反映 の実行が設定されている場合は、AD に情報が伝搬されユーザアカウントは無効にされます（アカウント削除方法が無効に設定されている場合）。



また定期実行のタイミングで、LDAP→CSV 出力 プラグインが実行され成功するとコンソールに以下のログエントリが表示されます。

```
2017/06/01 17:32:00 – [LDAP->CSV 出力 2] 合計：2 件 正常処理：2 件 スキップ処理：0 件 エラー処理：0 件 後処理：成功
```

連携が正常におこなわれると、Gléas RA の [登録申請者一覧]メニューより連携されたユーザ情報（削除申請）が表示されます。



[全て許可する]、あるいは一件ずつ[許可する]ことにより削除承認され、証明書の失効まで自動でおこなわれます。

※この許可操作は、自動承認機能を利用することにより自動化が可能です

5. 問い合わせ

ご不明な点がございましたら、以下にお問い合わせください。

■LDAP Managerに関するお問い合わせ先

エクスジェン・ネットワークス株式会社
営業部
TEL: 03-3518-8055

■Gléasや本検証に関するお問い合わせ

株式会社JCCH・セキュリティ・ソリューション・システムズ
営業本部
Tel:　050-3821-2195
Mail:　sales@jcch-sss.com