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

SyncTrustとのクライアント証明書の管理連携

Ver. 1.0
2020 年 1 月

目次

1. はじめに 4
1.1. 本書について 4
1.2. 本書における環境 4
1.3. 本書における構成 4
2. Gléas での事前設定 5
3. SyncTrust の設定 7
3.1. CSV 出力設定 7
3.2. グループ設定 10
3.3. タスクスケジューラの設定 11
4. SyncTrust と Gléas のデータ連携 13
4.1. ユーザアカウント作成と証明書発行 13
4.2. ユーザアカウント削除と証明書失効 14
4.3. タスクの実行結果 15
5. 問い合わせ 15

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」と、株式会社カスタムテクノロジーのID管理製品「SyncTrust Identity Manager」とを連携してクライアント証明書の管理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。

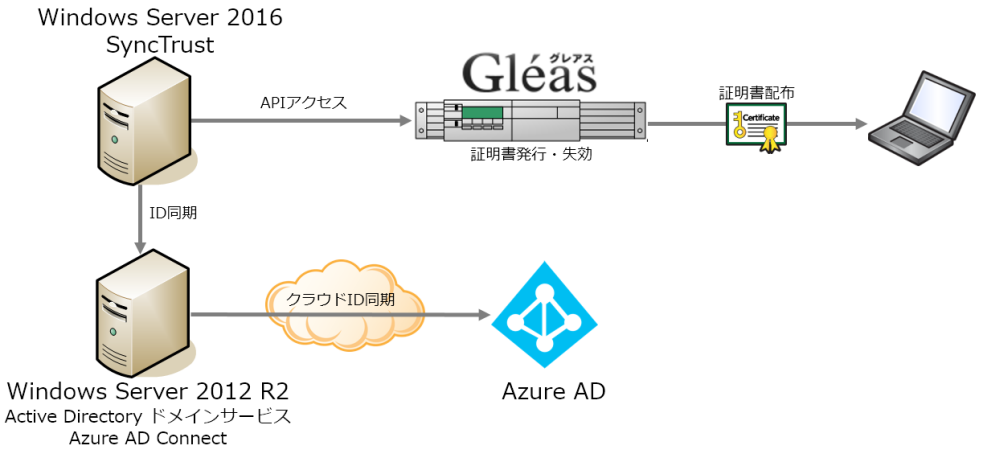
1.2. 本書における環境

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。

- ID管理システム：SyncTrust Identity Manager バージョン4.1.0
  ※Windows Server 2016 にインストールしています。また、OS付属のタスクスケジューラも利用しています
  ※以後、「SyncTrust」と記載します
- JS3 プライベート認証局 Gléas （バージョン2.1.3）
  ※以後、「Gléas」と記載します

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. SyncTrust Web管理画面からユーザIDを作成する
2. SyncTrust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. SyncTrust Web管理画面からユーザIDを削除する
2. SyncTrustは、ADの対象ユーザアカウントを削除し、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

本構成において以下事項については、本書では説明を割愛します。

- SyncTrustのインストールおよび基本的な設定
- Active DirectoryへのID連携、またAzure ADとのID連携
- Gléasの基本操作
- Windows ServerやWindowsドメインのセットアップ

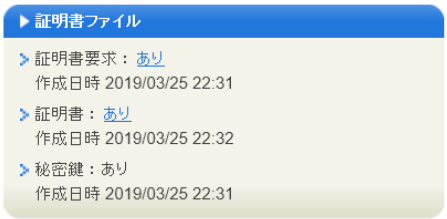
これらについては、各製品のマニュアルをご参照いただくか、各製品を取り扱う販売店にお問い合わせください。

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

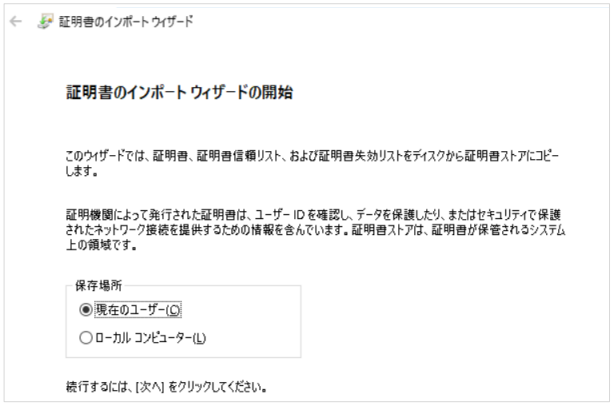
（登録）します。

またSyncTrustを動かしているサーバからGléasへのAPIアクセスのため、API管理者の証明書詳細画面の[▶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。

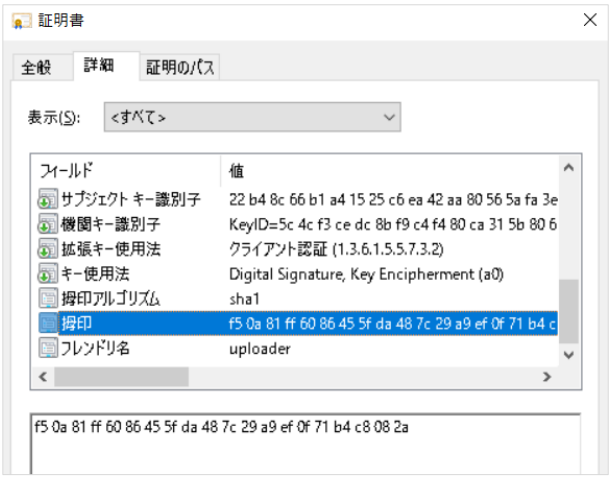
ダウンロード時に入力を要求されるファイルの保護パスワードはSyncTrustを動かしているサーバに証明書をインポートする際に必要となります。

以上でGléas側の設定は終了です。

SyncTrustを動かしているサーバにこの証明書ファイルを配置し、ダブルクリックすると起動する証明書のインポートウィザードにしたがい証明書をインポートします。

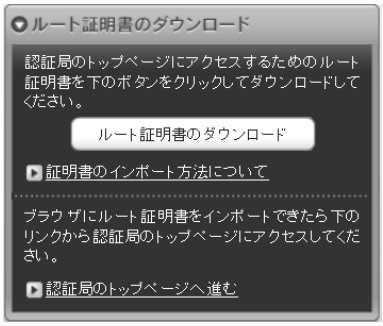


インポート後に、コントロールパネル ＞ インターネットオプション ＞ [コンテンツ]タブ ＞ [証明書] ＞ [個人]タブより証明書の拇印を確認しておきます（後述するPowerShellスクリプトからGléasへのアクセスに必要な情報になります)。



また、GléasのRA証明書を発行しているGléas内部管理用CAを信頼する必要があります。

Gléasにhttpで接続するとルート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. SyncTrustの設定

3.1. CSV 出力設定

SyncTrust 管理 Web 画面にログインし、左メニューより[アプリケーション管理] ＞ [アプリケーション設定]を開き、[新規アプリケーション設定]をクリックします。

[基本設定]欄で以下を設定します。

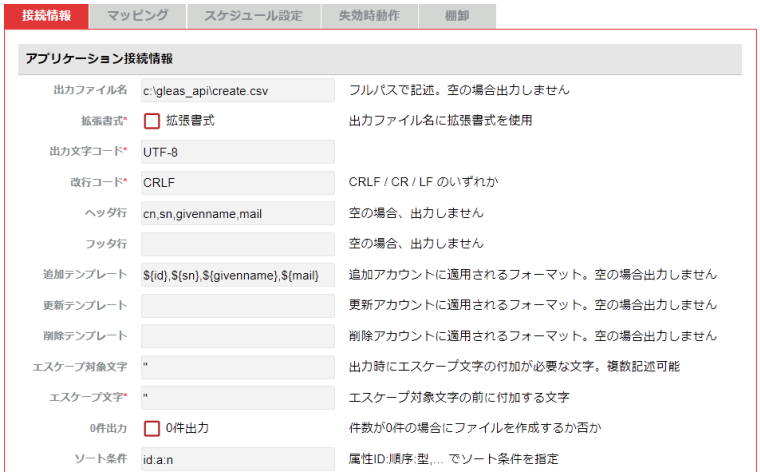
- [アプリケーション・コネクタ]には、”CSV 差分コネクタ”を選択
- [アプリケーション]には、任意の名称を入力

[次へ]をクリックします。

その下に表示される[詳細]欄の[接続情報]タブで以下を設定します（ユーザアカウント作成・証明書発行用 CSV）。

- [出力ファイル名]に、CSV ファイルの出力先パスを入力
- [出力文字コード]は、”UTF-8”を入力
- [ヘッダ行]に、以下を入力
  cn,sn,givenname,mail
- [追加テンプレート]に、以下を入力
  ${id},${sn},${givenname},${mail}
- [0 件出力]は、チェックを外す

※本件では、Gléas のエンドユーザ画面（UA）へのログイン時のパスワード認証は Active Directory を参照することを想定しています。もし Gléas 内部にそのパスワードを持たせる場合は、CSV にパスワード属性も加える必要があります。詳細は最終章のお問い合わせ先までお問い合わせください。

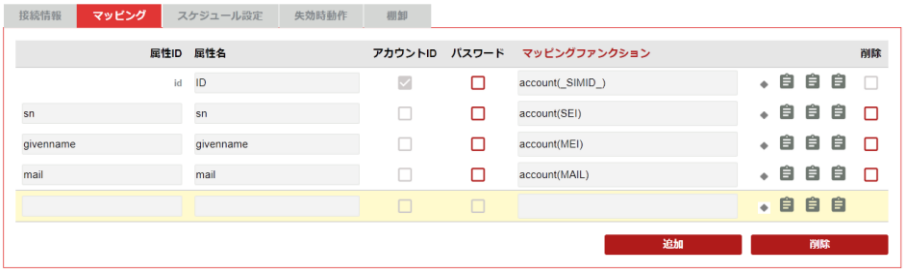


そのまま設定を続けます。（ユーザアカウント削除・証明書失効用 CSV）

- [出力ファイル名]に、CSV ファイルの出力先パスを入力

- [ヘッダ行]に、以下を入力
  cn,action
- [削除テンプレート]に、以下を入力
  ${id},destroy
- [0 件出力]は、チェックを外す

[マッピング]タブで属性 ID を作成し、SyncTrust の項目 ID とのマッピングをおこないます。以下は設定例です。



※項目 ID は、左側メニューの[アカウント管理設定] > [プロフィール設定]で確認することが可能です

[スケジュール]タブでこのアプリケーションの実行タイミングを指定します。
以下は、毎日 12 時と 18 時に CSV 作成タスクを自動起動する場合の例になります。

上記の設定をおこなったのち、保存します。

3.2. グループ設定

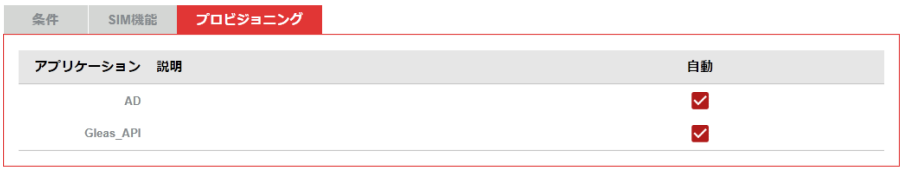
SyncTrust 管理 Web 画面で、[グループ管理] > [グループ設定]を開き、[新規グループ設定]をクリックし、以下の設定をおこないます。

- [グループ名]には、任意のグループ名称を入力
- [グループ種別]には、”カスタムグループ”を選択

[次へ]をクリックします。

その下に表示される[詳細]欄の条件タブで、全ユーザアカウントがこのグループに入るよう設定します。

[プロビジョニング]タブで、3.1 項で作成したアプリケーションに対し[自動]をチェックします。



上記の設定をおこなったのち、保存します。

3.3. タスクスケジューラの設定

3.2 で生成される CSV を Gléas に送信するスクリプトを用意します。

【Gléas 連携用スクリプト（PowerShell）のサンプル】

```
#Gleasアクセス情報
$gleasHostName = "example.jcch-sss.com"
$certHash = "f50a81ff6086455fda487c29a9ef0f71b4c8082a" #API管理者用証明書の拇印

#TLS1.2対応
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12

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(SyncTrustでのCSVファイル出力設定とあわせる)
$folderPath = "C:¥gleas_api¥"
$csvFilePath = $folderPath + $args[0] + ".csv"
$resultFilePath = $folderPath + $args[0] + "_result.txt"

#CSVファイルがなければ何もせず終了(タスクスケジューラに結果コード1を残す)
if(!(Test-Path $csvFilePath)){
   exit 1
}

#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
$content = `
[System.Text.Encoding]::UTF8.GetString( [System.Text.Encoding]::GetEncoding("ISO-
8859-1").GetBytes($response.content) ) | ConvertFrom-Json
$content.message  | Out-File $resultFilePath -append
$content.trans_id | Out-File $resultFilePath -append
$content.digest   | Out-File $resultFilePath -append

Remove-Item $csvFilePath  #処理終了後にCSVファイルを削除

exit 0
```

※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、実際のユーザアカウント登録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。登録処理結果を取得するには、アップロード時のレスポンスに含ま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

Windows のタスクスケジューラで、スクリプトを自動実行させるために以下の設定をおこないます。

- [トリガー]タブでは、SyncTrust でCSV ファイルを作成した後のタイミングで、スクリプトを起動させるように設定
- [操作]タブでは、Gléas に CSV ファイルを送信するためのスクリプトを実行させるよう設定

  ※本環境では前項のサンプルスクリプトを動作させるための設定として、以下の通りにしています

  [プログラム/スクリプト]

  %SystemRoot%¥System32¥WindowsPowerShell¥v1.0¥powershell.exe

  [引数の追加]

  -Command "スクリプトファイル名.ps1 create(或いは destroy)"

  [開始]

  スクリプトファイル.ps1 の配置されているフォルダパス

4. SyncTrustとGléasのデータ連携

4.1. ユーザアカウント作成と証明書発行

SyncTrust 管理コンソールよりユーザアカウントを作成します。

SyncTrust での作成完了後に、3.1 項で設定したタイミングで、上記のアカウント名・姓・名・メールアドレスを含む CSV が作成され、3.3 項で設定したタイミングで Gléas にデータ送信されます。

送信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。

アカウント名部分をクリックすると、申請の詳細を確認できます。

申請登録一覧画面で、[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. ユーザアカウント削除と証明書失効

SyncTrust 管理コンソールより、ユーザアカウントを削除します。

SyncTrust での削除完了後に、3.1 項で設定したタイミングで、上記のアカウント名・姓・名・メールアドレスを含む CSV が作成され、3.3 項で設定したタイミングで Gléas にデータ送信されます。

送信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。

アカウント名部分をクリックすると、申請の詳細を確認できます。

[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、そのユーザアカウント向けに発行された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

4.3. タスクの実行結果

タスクスケジューラで、登録したタスクの実行結果を確認します。

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。

■SyncTrustに関するお問い合わせ先

カスタムテクノロジー株式会社

営業グループ

Tel:　　03-5210-2991

Mail:　　info@ctech.co.jp

■Gléasや本検証内容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