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CA Gléas ホワイトペーパー

AccessMatrix Universal Sign-On (USO)での
クライアント証明書認証を用いた認証設定

Ver.2.0
2014 年 4 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CA Gléas」で発行したクライアント証明書・を利用して、i-Sprint Innovations社が開発し、株式会社ハイ・アベイラビリティ・システムズ（HAS）が日本国内で販売するAccessMatrix Universal Sign-in (USO)で認証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。

弊社では試験用のクライアント証明書の提供も行っております。検証等で必要な場合は、最終項のお問い合わせ先までお気軽にご連絡ください。

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。

- AccessMatrix USO サーバ： CentOS 6.5
  Apache Tomcat 7.0.34
  AccessMatrix 5.1.2.1225-SP1
  ※以後、「AccessMatrixサーバ」と記載します
- JS3 プライベートCA Gléas （バージョン1.11）
  ※以後、「Gléas」と記載します
- クライアントPC： Microsoft Windows 7 Professional (32ビット)
  Internet Explorer 10
  USOクライアント 5.1.2.1225
  ※以後、「PC」と記載します
- USBトークン： SafeNet eToken 5100
  SafeNet Authentication Client 8.2.85.0 評価版
  ※以後、「eToken」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。

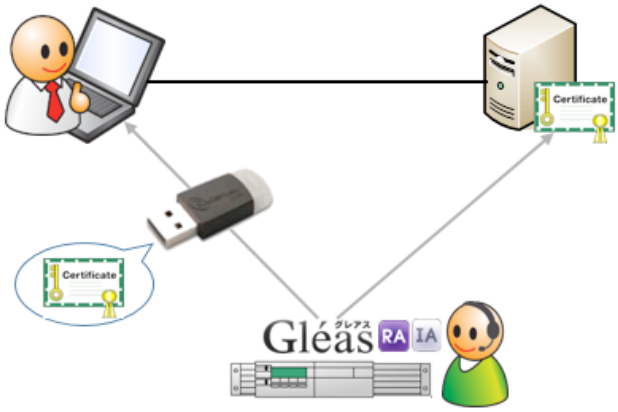
- AccessMatrixサーバのインストール及び基本設定
- Gléasでのユーザ登録やクライアント証明書発行等の基本設定

- PCのネットワーク設定等の基本設定、USOクライアントのインストール方法
- eTokenや付属ソフトウェアのインストール方法

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。



1. サーバ証明書は、Gléasより発行してAccessMatrixサーバのJavaキーストアにインポートする。クライアント証明書は、Gléasより発行してeTokenに格納し利用者に渡す
2. 利用者はPCよりAccessMatrixサーバにアクセスし、eTokenに格納されたクライアント証明書認証とPIN（暗証番号）による二因子認証をおこなう
3. クライアント証明書のサブジェクトCN（一般名）をユーザIDとしてAccessMatrixサーバにログインする
4. ログイン成功後にUSOクライアントよりシングルサインオン可能となる

2. AccessMatrixサーバでの設定

2.1. ルート証明書及びサーバ証明書のインポート

Gléas よりルート証明書（PEM 形式）をダウンロードします。
Gléas のルート証明書（デフォルトの発行局）は以下からダウンロードできます。
http://fqdn/crl/ia1.pem

ダウンロードしたファイルを AccessMatrix サーバにコピーして Java キーストアに

格納します。ここではキーストアの名前を cacerts.jks としています。

```
# keytool -import -keystore cacerts.jks -alias gleas_rootca -file ia1.pem
```

画面の指示にしたがい、インポートします。
ここで入力するキーストアのパスワードは Tomcat の設定で利用します。

Gléas の管理画面よりサーバ証明書をダウンロードします。
ダウンロードしたファイルを AccessMatrix サーバにコピーして Java キーストアに格納します。ここではダウンロードしたサーバ証明書のファイル名を servercert.p12、キーストアの名前を keystore.jks としています。

```
# keytool -importkeystore -srckeystore servercert.p12 -srcstorepass [サーバ証明書ダウンロード時に設定したパスフレーズ] -srckeypass [サーバ証明書ダウンロード時に設定したパスフレーズ] -srcstoretype PKCS12 -destkeystore keystore.jks -destkeypass [キーストアに設定するパスワード] -deststorepass [キーストアに設定するパスワード] -deststoretype JKS  -alias [Gléas のサーバアカウント名]
```

キーストアに設定するパスワードは Tomcat の設定で利用します。

2.2. Tomcat の設定

<AccessMatrix のインストールディレクトリ>/tomcat/conf/server.xml をエディタで開き、SSL ポート 8443 の設定を以下の通りおこないます。

```
<Connector
        port="8443" minSpareThreads="5"
        enableLookups="false" disableUploadTimeout="true"
        keepAliveTimeout="900000" maxKeepAliveRequests="-1"
        acceptCount="100"  maxThreads="200"
        scheme="https" secure="true" SSLEnabled="true"
        keystoreFile="サーバ証明書をインポートしたキーストアファイル(keystore.jks)"
        keystorePass="サーバ証明書をインポートしたキーストアファイルのパスワード"
        clientAuth="false"
        sslProtocol="TLS"
                ciphers="TLS_RSA_WITH_AES_128_CBC_SHA,
                        TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
                        TLS_DHE_DSS_WITH_AES_128_CBC_SHA"
/>
```

また同ファイルの SSL ポート番号 8444 を以下の通り設定します。

```
<Connector
        port="8444" minSpareThreads="5"
        enableLookups="false" disableUploadTimeout="true"
        keepAliveTimeout="900000" maxKeepAliveRequests="-1"
        acceptCount="100"  maxThreads="200"
        scheme="https" secure="true" SSLEnabled="true"
        keystoreFile="サーバ証明書をインポートしたキーストアファイル(keystore.jks)"
        keystorePass="サーバ証明書をインポートしたキーストアファイルのパスワード"
        truststoreFile="ルート証明書をインポートしたキーストアファイル(cacerts.jks)"
        truststorePass="ルート証明書をインポートしたキーストアファイルのパスワード"
        clientAuth="true"
        crlFile="失効リストファイル（PEM 形式）"
        sslProtocol="TLS"
                ciphers="TLS_RSA_WITH_AES_128_CBC_SHA,
                        TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
                        TLS_DHE_DSS_WITH_AES_128_CBC_SHA"
```

※Gléas でのデフォルト認証局の失効リスト（CRL）は次の URL から取得できます。
http://{Gléas のホスト名 or IP アドレス}/crl/crl_ia1.pem
認証局で証明書を失効しても、Tomcat 側の CRL が自動的に更新されるわけではなく、また、CRL に記載されている NextUpdate（次の更新予定）を過ぎたものは無効な情報と判断され、全ての接続を拒否します。
失効した証明書での認証を拒否したい場合や、NextUpdate の日付が過ぎる前に、新しい CRL ファイルを取得し既存の CRL ファイルと置き換えが必要になります。また、置き換えた CRL を反映するには Tomcat のサービス再起動が必要になります。

<AccessMatrix のインストールディレクトリ>/tomcat/webapps/am5/WEB-INF/classes/amsystem.properties をエディタで開き、以下の 2 つの既存の設定（製品にバンドルされるテスト用の証明書の使用に関する設定）をコメントアウトして無効にします。

```
#com.isprint.am.server.xmlrpc.XmlRpcServlet.$simCert.file=conf/testagent.cer
#com.isprint.am.server.soap.WrappedWSServlet.$simCert.file=conf/testagent.cer
```

2.3. AccessMatrix 管理コンソールでの設定

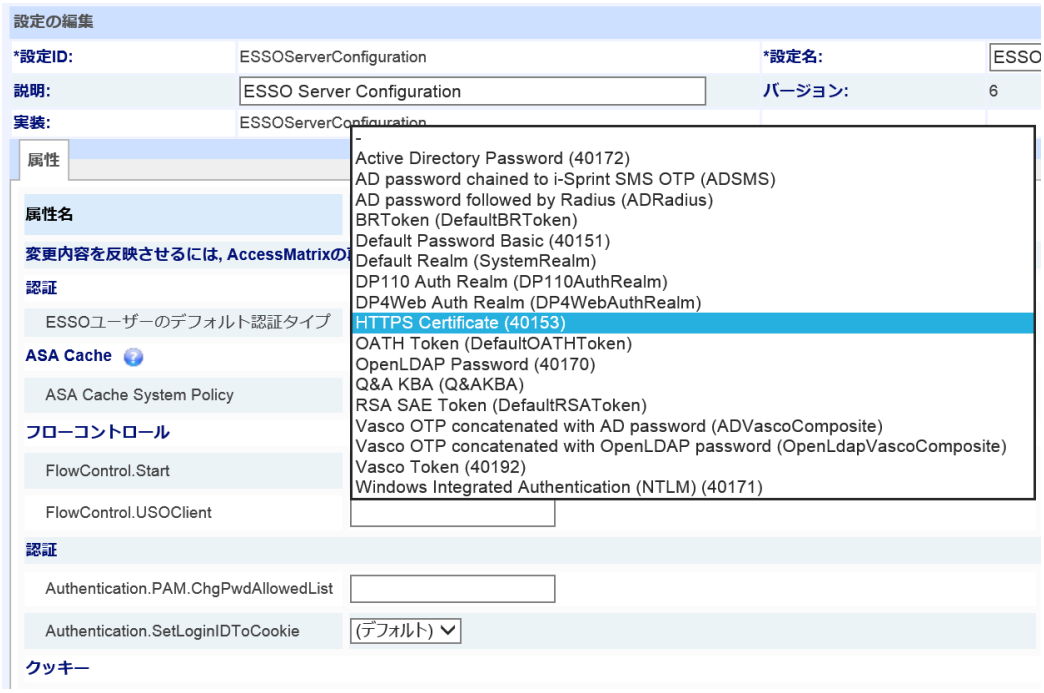
AccessMatrix 管理コンソールにログインします。

[設定] > [Authentication Workflow] > [ユーザ検索モジュール] から CertificateDnLookup を検索し、その Certificate Filter を以下の通り変更します。

```
id=Subject.CN
```

[設定] > [Authentication Workflow] > [認証レルム] から 40153 HTTPS Certificate を検索し、[全ユーザにこの認証レルムを自動的に割り当てる]を True に変更します。

[設定] > [ESSO] > [サーバー]を選択し、[ESSO ユーザのデフォルト認証タイプ]を[HTTPS Certificate (40153)] に変更します。



[設定] > [ESSO] > [クライアント]を選択し、[Client Certificate Port]が 8444 (Default)

であることを確認します。

Merge Login Menu	No *(デフォルト)*	Specifies whether Login to Server and PSE Login menu is being integrated. User will be logged in to server when connection is available, otherwise user will be switched to PSE Login.
Maximum PSE Login (in days)	0 *(デフォルト)*	Specifies maximum time for user to login to PSE only. Default value is 0 day which means PSE Login never expired.
ClientCertificatePort	8444 *(デフォルト)*	Applicable only for realm 40153. It needs secondary https port which "clientAuth" is set into true for authentication/re-authentication. You also need to activate respective connectors in server.xml file.
PSE File Custom Directory		Specifies custom directory to save PSE File. If this value is not set, PSE File will be saved to default directory which is USOClient application data folder.
Hide PSE File	No *(デフォルト)*	Specifies PSE File hidden attribute activation. If this value is set to Yes, PSE file will be hidden, otherwise PSE file will be created with default attribute.
		(Optional) When set to an application file, it will be launched automatically by ESSO client

以上の設定後、Tomcat のサービス再起動をします。

ユーザ画面の[ログインアカウント]タブを見ると、HTTPS Certificate(40153)が自動的に割り当てられているのが確認できます。

ユーザーの閲覧

***ユーザーID:**	testuser01	***ユーザー名:**	testuser01
説明:		**バージョン:**	80
***インタラクティブ:**	Yes *(デフォルト)*	**ユーザーストア:**	DefaultStore
識別名 (DN):		**アカウントステータス:**	Activated
セグメント:			
ログイン:	前回ログイン Tue Mar 25 2014 10:41:50 (IPアドレス 192.168.20.251)	**ログアウト:**	前回ログアウト Fri Mar 21 2014 17:56:05
	前回ログイン失敗 Fri Mar 21 2014 18:17:22 (IPアドレス 192.168.20.251)		
トークン共有グループID:			

属性 | メンバーシップ | ESSOエンタイトルメント | **ログインアカウント** | 管理者権限 | アプリケーション権限 | ログインセッションの持続

認証レルム	自動	ステータス	開始日時	終了日時				
HTTPS Certificate (40153)	Yes	有効						

ログインモジュール	認証レルムシーケンス	ステータス	パスワード変更を強制する	連続ログイン失敗回数	連続ログイン失敗回数 (パスワード変更時)	開始日時	終了日時	Last Password Change Date
ClientCertificateOverSSL		Activated	No	0	0			

編集 | 削除 | 戻る | パスワードリセット | トークンの割り当て

3. GléasでのUSBトークンの準備

GléasのRAに管理者ログインし、認証用に発行した証明書の詳細画面まで移動します。

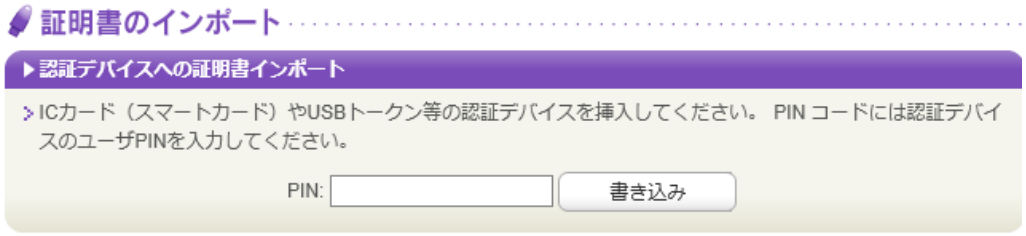
エンドユーザ用の認証デバイスを管理者端末に接続し、画面上部の[トークンへのインポート]をクリックします。

※ Gléasの認証デバイス管理機能からeTokenの操作をおこなう場合、その管理者用端末にSafeNet Aithentication Client（SAC）がインストールされている必要があります

※ 本手順に先立ち以下の設定も必要となりますが、ここでは説明を省略します

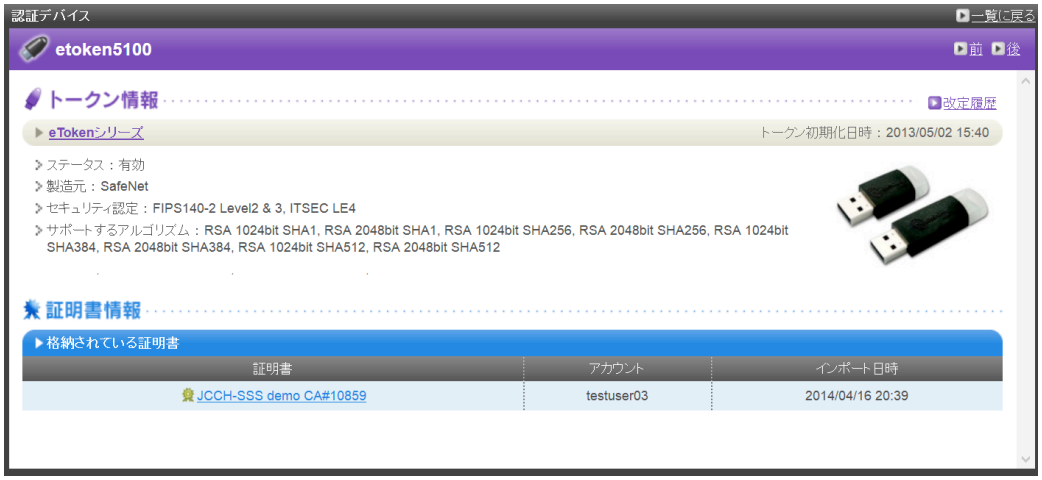
- Gléasの管理者設定で、管理するデバイスをSafeNet eTokenに設定
- SAC、或いはGléasで認証デバイスの初期化をしておく

認証デバイスに初期化時などに設定したPIN（暗証番号）を入力し、証明書のインポートを行います。



元の画面に戻ればインポートは成功です。
この時に画面を下にスクロールしていくと、インポート先のデバイス情報が付加されています。

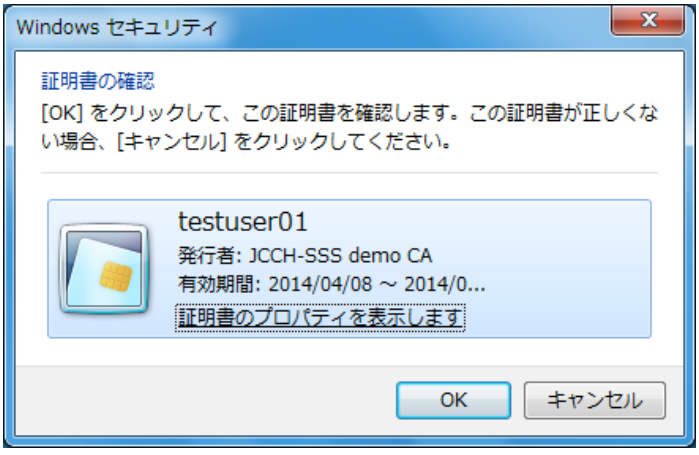
また[認証デバイス]メニューでは、この認証デバイスにインポートした証明書を確認することが可能となります。



以上で、認証デバイスの準備は終了です。

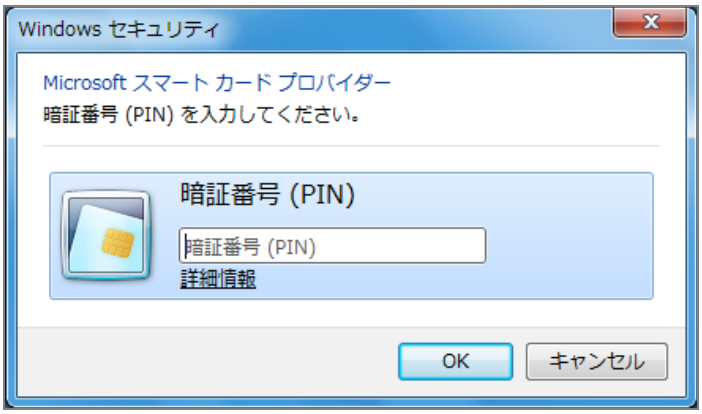
4. AccessMatrixへのログイン

eTokenをPCに挿入した状態でInternet Explorerを起動するか、USOクライアントを起動しAccessMatrixサーバへアクセスします。
証明書の確認ダイアログに、eTokenに格納されているクライアント証明書が表示されるので[OK]をクリックします。



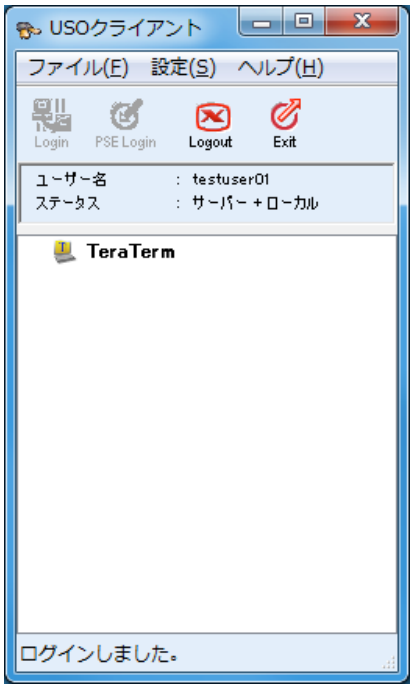
※Internet Explorerのセキュリティ設定で、[既存のクライアント証明書が1つしか存在しない場合の証明書の選択]を有効に設定されている場合（あるいはその設定が有効になっているゾーン（イントラネットゾーンなど）にAccessMatrixサーバのURLが設定されている場合）、提示可能な証明書が一枚しかストアになければ上記の[証明書の確認]は表示されません。

その後、PIN入力ダイアログが表示されるのでPINを入力します。



なお、SafeNet Authentication Clientがインストールされている端末では、上記とは異なるPINの入力ダイアログが表示されます

USOクライアントへのログインが完了すると、管理者に指定されたシングルサインオン可能なアプリケーションが表示されます。



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。

■Gléasや検証用の証明書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

Tel: 050-3821-2195

Mail: sales@jcch-sss.com

■AccessMatrix USOに関するお問い合わせ

株式会社ハイ・アベイラビリティ・システムズ

ソリューション＆コンサルティング事業部　ソリューション営業部

Tel: 03-5730-8870

Mail: inquiry_desk@ha-sys.co.jp