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

～HP IceWall SSO 連携～

クライアント証明書認証によるシングルサインオン環境構築 設定例

Ver.1.0
2013 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」で発行する電子証明書と、日本セーフネット株式会社の認証デバイス「eToken シリーズ」、及び日本ヒューレット・パッカード株式会社の Web シングルサインオンソリューション「HP IceWall SSO」を利用したシングルサインオン環境を構築するための手順や設定例について記載します。

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。

- 【Web シングルサインオンソリューション】日本ヒューレット・パッカード株式会社 HP IceWall SSO（バージョン 10.0）
  ※日本 HP 社の IceWall 評価環境を利用。
  －CentOS 6.0 x64 上で動作
  －IceWall サーバ／認証サーバ：Apache 2.2.15
  －認証データベース：OpenLDAP 2.4.19
  ※CentOS は評価環境として使用。HP IceWall SSO の正式なサポート OS としては対象外となりますのでご留意ください。
  ※以降、本文中は「IceWall SSO」と記載します。
- 【認証局】JS3 プライベート CA Gléas （バージョン 1.10）
  ※以降、「Gléas」と記載します。
- 【認証デバイス】日本セーフネット株式会社 USB トークン「SafeNet eToken5100」及び IC カード「SafeNet eToken4100」
  ※以降、「USB トークン」、「IC カード」、総称して「認証デバイス」と記載します。
- 【PC】Windows7 Professional 64bit, InternetExplorer9
  ※以降、「PC」または「クライアント端末」と記載します。

- 【iPad】iOS5.1

  ※以降、「iPad」または「クライアント端末」と記載します。

1.3　本書内で使用する用語ついて

本書内で使用する用語について、下記の通り定義します。

- RA 画面：プライベート CA Gléas の RA 管理者操作画面
- UA 画面：プライベート CA Gléas のユーザ申込局の画面
- 管理者：Gléas の管理者
- []：画面上に表示されるボタンやリンクを指す
- 押下：クリック、選択状態で Enter キー押下、タップ等の操作を指す

1.4　本書内で使用する用語、割愛事項について

本書においては、以下についての説明を割愛します。

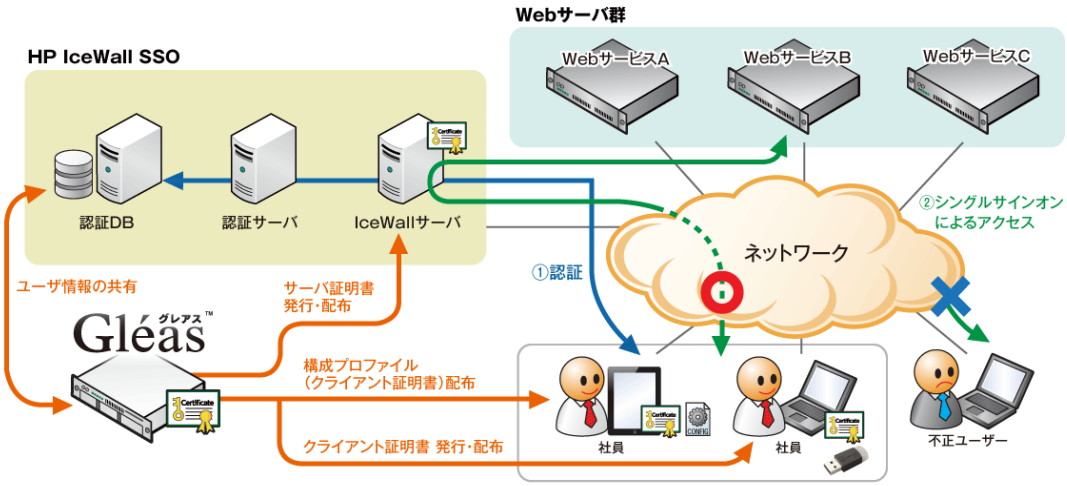
- Gléas でのアカウント新規作成やクライアント証明書発行等の基本操作方法
- 各機器におけるネットワーク設定
- IceWall SSO 検証環境の利用申請方法、IceWall SSO 検証環境の構築方法、及び基本基本操作方法
- IceWall SSO を利用してコンテンツにログインするユーザアカウントの登録方法

※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等にお問い合わせください。

1.5　本書における構成

■IceWall SSO と連携する場合の構成例

（連携概念図）



（手順概要）

1. Gléas で、各種証明書（サーバ証明書、クライアント証明書）を発行します。
2. IceWall SSO に、サーバ証明書を格納し、クライアント証明書情報を登録します。
3. シングルサインオンの認証に利用する認証デバイスやクライアント端末に、クライアント証明書を格納します。
4. クライアント端末のブラウザから、IceWall SSO のシングルサイン用の URL にアクセスし、シングルサインオンによるコンテンツへのアクセスを行います。

2 利用する証明書の準備

2.1 サーバ証明書、CA 証明書の準備

IceWall SSO に格納して利用するサーバ証明書を Gléas にて発行し、ダウンロードします。
合わせて、Gléas のルート証明書(CA 証明書)をダウンロードします。

プライベート CA Gléas をご利用のお客様へ

Ⅰ. Gléas からダウンロードしたサーバ証明書は PKCS#12 という形式になっているため、PEM 形式に変換・分離する必要があります。

1. PKCS#12 ファイルより証明書を取得

   openssl pkcs12 –in ssl-server.p12 –clcerts –nokeys –out iwsrv.crt

2. PKCS#12 ファイルより秘密鍵を取得

   openssl pkcs12 –in ssl-server.p12 –nocerts –nodes –out iwsrv.key

Ⅱ. CA 証明書は次の URL からダウンロードできます。

http://{Gléas のホスト名 or IP アドレス}/crl/ia1.pem

※上記内容におけるファイル名はサンプルであり、本書の以降の内容ではその通りの名前であることを前提として記載します。
※サーバ証明書の発行・ダウンロード手順については、Gléas のオンラインヘルプ等をご参照ください。

2.2　クライアント証明書の準備

IceWall SSO を利用するユーザのアカウントを Gléas 上にも作成して、クライアント証明書を発行します。

通常、Gléas に登録するアカウントの「アカウント名」が、発行されたクライアント証明書のサブジェクトにおける cn の値となります。本書では、この証明書内の cn の値を、IceWall SSO での認証時のユーザ ID として参照・利用する設定例となっています。そのため、Gléas に作成するアカウントのアカウント名を、IceWall SSO を利用するユーザのユーザ ID と同一の内容で登録します。

▽Gléas RA 画面　アカウント新規作成画面でのアカウント名入力箇所

※Gléas でのアカウントの新規作成方法及び証明書の発行方法詳細は、Gléas のオンラインヘルプ等をご参照ください。

3 HP IceWall SSO の設定

3.1 HP IceWall SSO の設定

IceWall SSO でクライアント証明書を使った認証を有効にするため、クライアント証明書オプション※を利用するための設定を行います。
※別途ライセンスの購入が必要です。本ライセンスを購入することで、IceWall SSO の当該機能を使用できます。詳細は日本 HP 社にお問い合わせください。

■手順

1. Web サーバの設定追加（Apache の設定方法）

   /etc/httpd/conf.d/ssl.conf

   上記設定ファイルにおいて、:443 をリッスンさせるため、:443 の<VirtualHost> ディレクティブを編集します。

   認証時にクライアント証明書を要求する設定にして、サーバ証明書・CA 証明書の指定を行います。

```
    :
<VirtualHost _default_:443>
    :
SSLCACertificatePath /etc/pki/tls/ca_certs
SSLCACertificateFile /etc/pki/tls/ca_certs/ia1.cer
    :
SSLVerifyClient require
SSLVerifyDepth 10
    :
SSLCertificateFile /etc/pki/tls/server/iwsrv.crt
    :
SSLCertificateKeyFile /etc/pki/tls/server/iwsrv.key
    :
Alias /img/ "/opt/icewall-sso/dfw/html/image/"
SetEnv LD_LIBRARY_PATH "/opt/icewall-sso/lib/dfw:/usr/lib"
ScriptAlias /fw/ "/opt/icewall-sso/dfw/cgi-bin/"
    :
<Directory "/opt/icewall-sso/dfw/cgi-bin">
SSLOptions +StdEnvVars +ExportCertData
</Directory>
    :
</VirtualHost>
```

2. 認証データベースの拡張

クライアント証明書情報を保存する認証データベースの属性を指定します。

/opt/icewall-sso/certd/config/dbattr.conf

上記設定ファイル内を下記の通りに設定します。

- 発行時シリアルナンバー（事前にクライアント証明書のシリアルナンバーを登録しておく属性）⇒RASERIAL
- 提示時シリアルナンバー（初回認証成功時に、提示されたクライアント証明書のシリアルナンバーを登録する属性）⇒BSSERIAL
- 証明書有効期間（初回認証成功時に、提示されたクライアント証明書の有効期間を登録する属性）⇒VDATE

```
   :
RASERIALNO=RASERIAL
IWSERIALNO=BSSERIAL
CERTEXPDATE=VDATE
   :
```

3. 証明書使用時の動作設定

/opt/icewall-sso/dfw/cgi-bin/dfw.conf

クライアント証明書サブジェクトの cn の値をユーザ ID として参照するために、上記ファイル内に下記の通り設定します。

```
   :
CC_UID=CN
   :
```

4. 認証モジュールの設定変更

認証モジュールの設定ファイルを、クライアント証明を利用する場合の設定に変更します。

/opt/icewall-sso/certd/config/cert.conf

上記設定ファイル内で、下記の通りに設定します。

```
   :
ACCCTRLFLG=2
   :
```

3.2　サーバ証明書、ルート証明書の格納

3.1 の手順 1 で指定した通りに、準備していたサーバ証明書とルート証明書を格納します。

※手順に記載したディレクトリ構成はサンプルであり、本書ではその通りの構成で動作確認を行うことを前提として記載しています。
※サーバへのファイルのアップロード方法については、本書では割愛します。

3.3　クライアント証明書情報の格納

クライアント証明書のシリアルナンバーの値を、認証データベースに事前に登録します。Gléas の RA 画面では、シリアルナンバーは 10 進数で表示されます。この値を 16 進数に変換した値を、該当するユーザのエントリーの RASERIAL 属性(3.1 の手順 2 で指定した属性)の値として登録します。

例）：Gléas の管理画面でシリアルナンバーが『#10178』と表示されている場合は、RASERIAL 属性に値『27c2』を登録します。

▽Gléas RA 画面　証明書詳細画面上でのシリアルナンバーの表示

※上記は、データベースが OpenLDAP の場合の内容となります。
※データベースへのデータの書き込み方法は、利用するデータベースの種類に依存するため本書では割愛します。

※Gléas では、データベースへの証明書情報の登録を自動で行うようカスタマイズする事も可能です。詳細は弊社営業までお問い合わせください。

4 クライアント端末での操作手順（PC）

4.1 認証デバイスへのクライアント証明書の格納

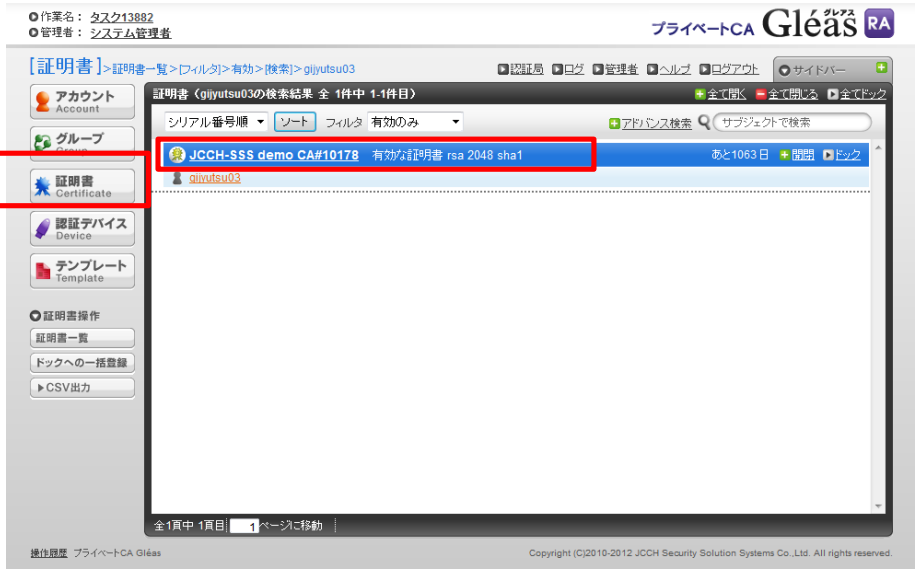
Gléas を使って、認証デバイスにクライアント証明書を格納します。

■手順

1. Gléas RA 画面に管理者の証明書を使って PC からアクセスし、[証明書でログイン]を押下してログインします。

2. ログイン後、RA 画面上部の[管理者]を押下して管理者の一覧を表示させ、ログイン中の管理者を選択して管理者設定の画面を表示させます。次に「管理するトークン」のセレクトボックスで「SafeNet eToken」を選択して、[保存]を押下します。

3. [証明書]→[証明書一覧]と押下して、証明書の一覧を表示させます。次に、一覧から認証デバイスにインポートする証明書を選択して証明書の詳細画面を表示させます。



4. 認証デバイスを PC に接続して、[トークンへのインポート]を押下します。
※使用する認証デバイスは初期化済みで、User PIN を設定済みの前提とします。

5. User PIN を入力して、[書き込み]を押下します。

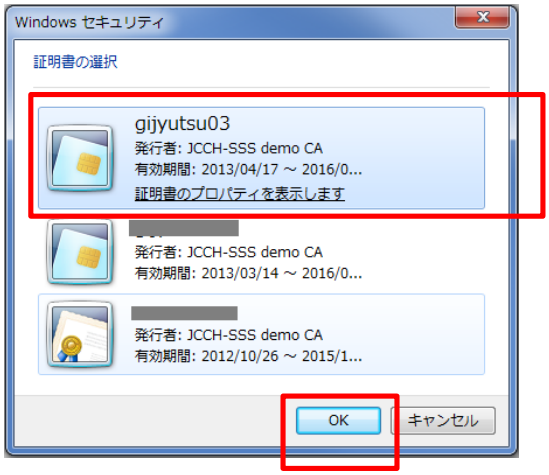
※認証デバイスへの書き込みが成功すると、証明書の詳細画面が表示されます。

4.2　HP IceWall SSO を利用したシングルサインオンの実施

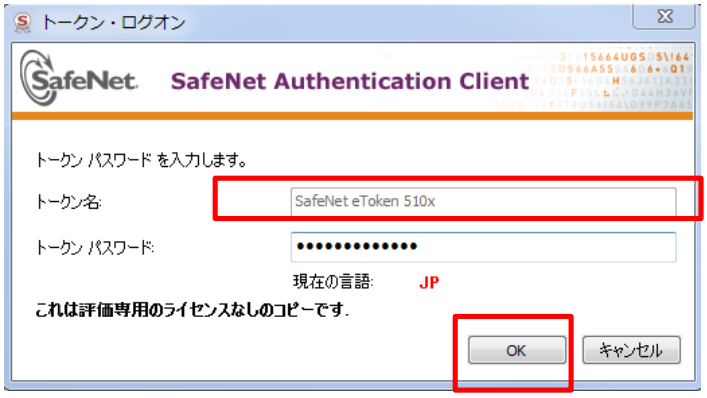
■手順

1. 認証デバイスを接続した PC のブラウザにて、IceWall SSO のシングルサインオン用の URL にアクセスします。
   ※URL は、IceWall SSO の設定・構築した環境によって異なります。

2. クライアント証明書を選択するダイアログが表示されるので、ログインするユーザ用の証明書選択して[OK]を押下します。



3. 「トークンパスワード」の入力を求められるので、User PIN を入力して[OK]を押下します。



※設定・環境によって、Web サイトのセキュリティ警告が表示される場合があります。警告の内容をよくご確認の上、問題が無い場合に[サイトの閲覧を続行する]を押下して次画面を表示させてください。

※証明書の選択画面が数回表示される場合もあります。その場合は、前出の手順と同様に利用する証明書を選択して[OK]を押下して、操作を進めてください。

4. ログイン画面で、ユーザ ID と組みになっているパスワードを入力して[送信]を押下します。

5. ログインに成功してアクセス権が有った場合、コンテンツがブラウザ上で表示されます。

＜動作検証内容＞
下記の通り、Gléas で発行した証明書を使って、IceWall SSO による認証及びシングルサインオンが行えることを確認しました。

◆ 上記手順でログインした後、アクセス権の有る異なるコンテンツの URL にアクセスすると、認証画面を経ずに直接コンテンツが表示される。

◆ 上記手順でログインした後、アクセス権の無い異なるコンテンツの URL にアクセスすると、「アクセス権限エラー」となりエラーメッセージが表示される。

◆ 一度ログアウトして、再度アクセス権の有るコンテンツの URL にアクセスした場合は、認証画面が再び表示される。

◆ 一度ログアウトして、再度アクセス権の無いコンテンツの URL にアクセスした場合は、認証画面が表示される。ログインを行った場合は、ログインは成功するが「アクセス権限エラー」となりエラーメッセージが表示される。

※IceWall SSO には、ログイン後にアクセス権のあるコンテンツへのリンクを集めた画面を動的に生成して表示するダイナミックメニューポータル機能など、本書記載以外の機能がありますが、今回は主に認証・ログイン機能についての動作検証結果を記載するものとして割愛しています。

5 クライアント端末での操作手順（iOS）

5.1 iPad へのクライアント証明書の格納

Gléas の UA にアクセスして、クライアント証明書を含む構成プロファイルのインポートを行います。

■手順

1. Gléas UA のログイン画面で、証明書が発行されたユーザのユーザ名とパスワードを入力して、[ログイン]を押下します。

2. UA 画面にログイン後、[構成プロファイルのダウンロード]を押下します。

3. [インストール]を押下します。

4. [インストール]を押下します。

5. [完了]を押下します。

6. ブラウザの表示に戻るので、[ログアウト]を押下します。

※インポートされた構成プロファイルは、設定 ＞ 一般 ＞ プロファイル で表示される一覧に追加されます。追加されたプロファイルを選択して、内容を確認する事ができます。

5.2　HP IceWall SSO を利用したシングルサインオンの実施

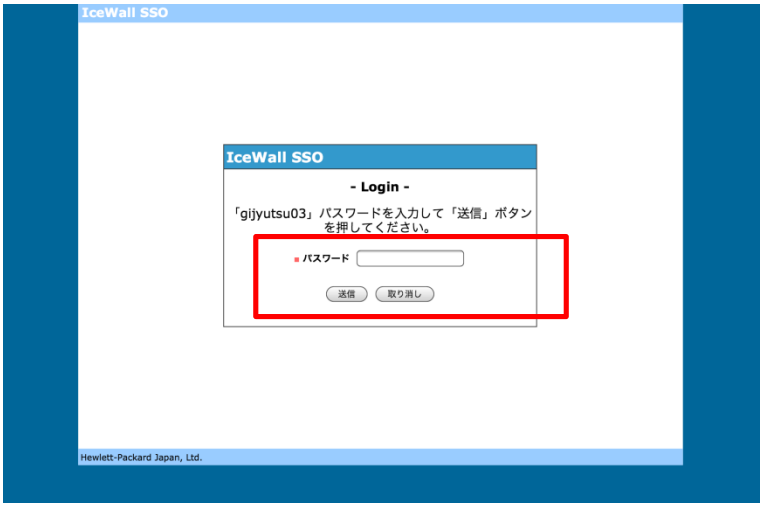
■手順

1. クライアント証明書をインポートした iPad のブラウザにて、IceWall SSO のシングルサインオン用の URL にアクセスします。

2. ダイアログが表示されるので、[続ける]を押下します。

3. 証明書選択用のダイアログが表示されるので、ログインするユーザ用の証明書を押下します。

4. ログイン画面で、ユーザ ID と組みになっているパスワードを入力して[送信]を押下します。



5. ログインに成功してアクセス権が有った場合、コンテンツがブラウザ上で表示されます。

＜動作検証内容＞
※動作検証内容および結果は、PC での場合と同様となります。

6 お問い合わせ先

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。

■HP IceWall SSO に関するお問い合わせ先
日本ヒューレット・パッカード株式会社
テクノロジーコンサルティング統括本部
IceWall ソフトウェア本部
　お問い合わせ：
http://h50146.www5.hp.com/products/software/security/icewall/iwsoftware/contact.html

■Gléas や検証用の証明書、SafeNet 社製品購入に関するお問い合わせ先
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