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

Secioss Linkを利用したSAMLシングルサインオン（Salesforce編）

Ver.1.0

2012 年 10 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」で発行した電子証明書を利用して、セシオス株式会社の提供するシングルサインオン（SSO）サービス「Secioss Link」を経由してsalesforce.com Co.,Ltd.の提供するSalesforceに対しSecurity Assertion Markup Language（SAML）を用いたシングルサインオン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。

- 【SSOサービス】Secioss Link
- 【認証局】JS3 プライベートCA Gléas （バージョン1.9）
  ※以後、「Gléas」と記載します
- 【アプリケーション】Salesforce – Developer Edition
  ※以後、「Salesforce」と記載します
- 【クライアント：PC】Microsoft Windows 7 Professional SP1
  ※以後、「PC」と記載します
- 【クライアント：タブレット】Apple iPad （iOS 5.0.1）
  ※以後、「iPad」と記載します

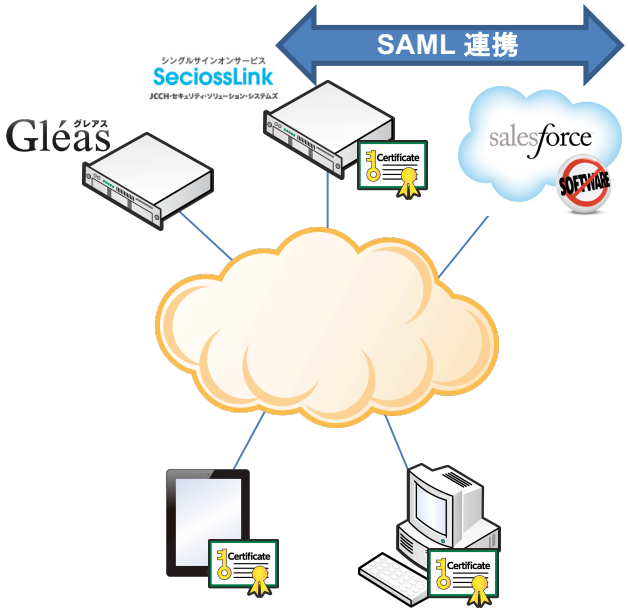
以下については、本書では説明を割愛します。

- Salesforceの設定
- Secioss Linkのシングルサインオン設定
  ※セシオス株式会社のWEBサイトでSalesforce認証連携を含めたSecioss Linkの設定方法を記載したマニュアルが公開されていますので、構築時の参考にしてください
  参考URL：http://support.secioss.co.jp/docs/SlinkManagementGuide.pdf
- Gléasでのユーザ登録やクライアント証明書発行等の基本操作

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. デバイス（PC・iPad）はGléasよりクライアント証明書を取得する
2. ブラウザであらかじめ設定するURLにアクセスすると、Secioss Linkに転送される（SeciossLinkからのアクセスに限定する場合は、SeciossLinkに管理者ログインし、画面上部のメニューより[シングルサインオン]をクリックします。左ペインの [Salesforce]をクリックし、右ペインにある[パスワードの同期]からプルダウンで[ランダムパスワード]を選択）
3. Secioss Linkでは有効なクライアント証明書を要求されるので、Gléasより取得した証明書による認証をおこなう
4. さらにユーザIDとパスワードによる認証がおこなわれる。この時のユーザIDはクライアント証明書のサブジェクトのcn（Common Name）が利用される（ここを省略する方法も説明する）
5. Secioss Linkへのログインに成功すると、自動的にSalesforceに転送される

2. Secioss Link の設定

2.1. 信頼する認証局の設定

Secioss Linkに管理者としてログインし、画面上部のメニューより[システム]をクリックします。左ペインの[システム管理]メニューより[テナント情報]をクリックすると、右ペインに以下の設定画面が表示されるので以下を設定します。

- [証明書のサブジェクト]には、アクセスを許可するクライアント証明書のサブジェクトを入力（前方一致か後方一致で空欄不可。3つまで入力可能）
- [CA証明書]には、[ファイルを選択]ボタンを押して事前に準備したGléasの認証局証明書を選択しインポート
- [CRLのURL]には、失効リスト（CRL）の取得用のURLを入力

  ※GléasのデフォルトのCRL配布ポイントは以下のとおりです。Secioss Linkからアクセス可能である必要があります

  http://hostname.example.com/crl/ia1.crl

  ※Secioss Linkは、失効リストを定期的に自動取得します

2.2. 認証ルールの作成

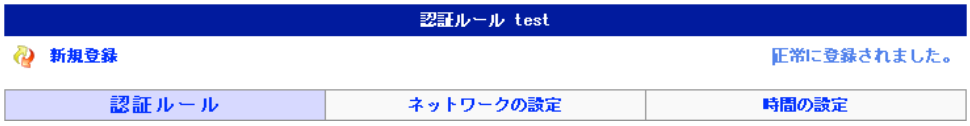
上部メニューより[認証] > [新規登録]をクリックします。
新規設定画面で以下を設定します。

以下を設定します。

- [ID]には、認証ルールを識別する任意の ID 名を入力
  [認証方法]には、[証明書認証]と[ID/パスワード認証]を[追加 AND >]を使って選択
  ※パスワード入力を省略したい場合は、[証明書認証]だけにすることも可能
- [優先度]には、他の認証ルールと併用する場合の優先度を選択（数字が大きい方が優先）
- [クライアント端末]には、[Web ブラウザ] [iPad]にチェック

設定後、[登録]をクリックします。

認証ルールが作成されると、このルールを適用するクライアントのアクセス元 IP アドレスの制限（[ネットワークの設定]）や、時刻による制限（[時間の設定]）の指定が可能となります。



Secioss Link の設定は以上です。

Secioss Link では複数の WEB サービスにシングルサインオンをおこなう際などに、

特定の WEB サービス（Salesforce 等）に限定してクライアント証明書認証を追加するような設定も可能です。
詳細は[アクセス制御]メニューを参照してください。本ドキュメントでは説明は省略します。

3. Gléasの管理者設定（PC）

GléasのUA（申込局）より発行済み証明書をクライアントPCにインポートできるよう設定します。
※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

3.1. UA（ユーザ申込局）設定

GléasのRA（登録局）にログインし、画面上部より[認証局]をクリックし[認証局一覧]画面に移動し、設定を行うUA（申込局）をクリックします。

[申込局詳細]画面が開くので、[基本設定]部分で以下の設定を行います。

- [証明書ストアへのインポート]をチェック
- [証明書ストアの選択]で[ユーザストア]を選択
- 証明書のインポートを一度のみに制限する場合は、[インポートワンスを利用する]にチェック

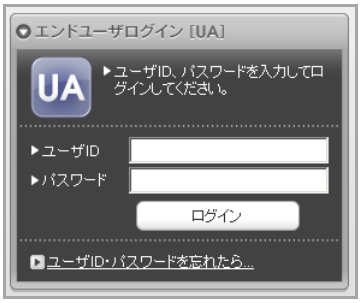
設定終了後、[保存]をクリックし設定を保存します。
各項目の入力が終わったら、 [保存]をクリックします。

以上でGléasの設定は終了です。

4. クライアント側での操作（PC）

4.1. クライアント証明書のインストール

Internet ExplorerでGléasのUAサイトにアクセスします。
ログイン画面が表示されるので、Gléasでのユーザ IDとパスワードを入力しログインします。



ログインすると、ユーザ専用ページが表示されます。
[証明書のインポート]ボタンをクリックすると、クライアント証明書のインポートが行われます。
※初回ログインの際は、ActiveXコントロールのインストールを求められるので、画面の指示に従いインストールを完了してください。

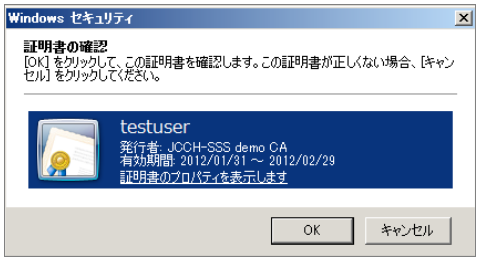
「インポートワンス」を有効にしている場合は、インポート完了後に強制的にログアウトさせられます。再ログインしても[証明書のインポート]ボタンは表示されず、再度のインポートを行うことはできません。

4.2. Salesforce へのシングルサインオン

Internet Explorer（IE）でSalesforceへアクセスします。URLは以下のとおりです。
https://jlink.secioss.com/saml/saml2/idp/SSOService.php?spentityid=<Salesforce のエンティティID>
Secioss Linkに転送されます。
※2回目以降のアクセスは、Salesforceログイン後のURLも利用できます。

初回アクセス時にはテナントIDの入力を求められますので、入力して[選択]をクリックします。

クライアント証明書の選択ダイアログが出現します。証明書を確認して[OK]をクリックします。
※IEの設定によっては、クライアント証明書の選択ダイアログが出ない場合もあります

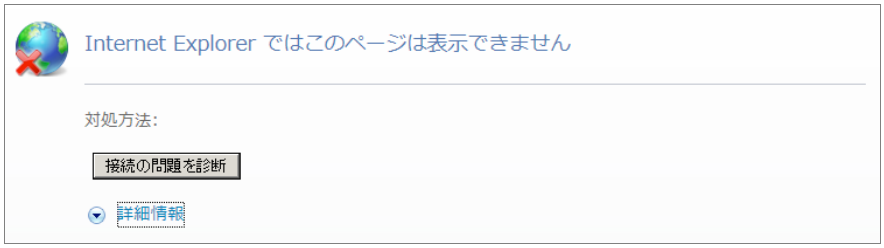


Secioss Linkのログイン画面が表示されます。
ユーザ名はクライアント証明書のサブジェクトのcn値にSecioss Linkのテナント ID が付加されたものとなります。

Secioss Linkでのログインパスワードを入力し、[ログイン]を入力するとSalesforce ログイン後の画面に転送されます。

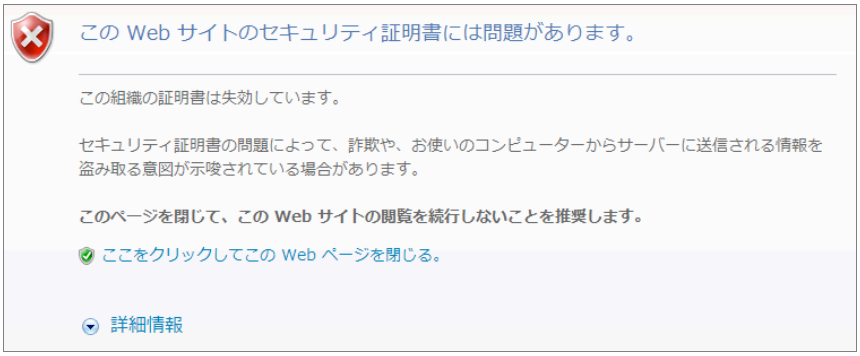
Secioss Linkにユーザ登録されていないサブジェクトcn値を持つクライアント証明書や、[テナント情報]で設定したものと異なるサブジェクトの証明書でアクセスした場合は以下のとおりエラーとなります。

クライアント証明書のない状態でアクセスすると以下のとおりエラーとなります。



失効したクライアント証明書でアクセスすると以下のとおりエラーとなります。

※失効情報がSecioss Linkに伝搬されている必要があります



5. Gléasの管理者設定（iPad）

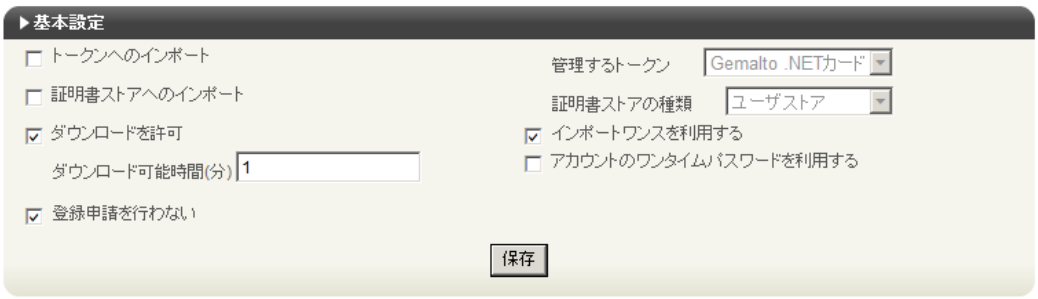
※下記設定は、Gléas 納品時等に弊社で設定を既に行っている場合があります

5.1. UA（ユーザ申込局）設定

GléasのRA（登録局）にログインし、画面上部より[認証局]をクリックし[認証局一覧]画面に移動し、iPad用となるUA（申込局）をクリックします。

[申込局詳細]画面が開くので、[基本設定]部分で以下の設定を行います。

- [ダウンロードを許可]をチェック
- [インポートワンスを利用する]のチェック、[ダウンロード可能時間(分)]の設定
  この設定を行うと、GléasのUAからダウンロードしてから、指定した時間（分）を経過した後に、構成プロファイルのダウンロードが不可能になります（「インポートロック」機能）。このインポートロックにより複数台のiPadへの構成プロファイルのインストールを制限することができます。



[認証デバイス情報]の[iPhone/iPadの設定]までスクロールし、[iPhone/iPad用UAを利用する]をチェックします。

構成プロファイル生成に必要となる情報を入力する画面が展開されるので、以下設定を行います。

- [iPhone用レイアウトを利用する]にチェック
- [iPhone構成プロファイル基本設定]の各項目を入力
  ※[名前]、[識別子]、[プロファイルの組織名]、[説明]は必須項目となります
  ※[削除パスワード]を設定すると、iPadユーザが設定プロファイルを削除する際に管理者が定めたパスワードが必要となります（iPadユーザの故意や誤操作等による構成プロファイルの削除を防止できます）

設定終了後、[保存]をクリックして設定を保存します。

以上でGléasの設定は終了です。

6. クライアント側での操作（iPad）

GléasのUAに接続し、発行済みのクライアント証明書・構成プロファイルのインポートを行います。

6.1. 構成プロファイルのインストール

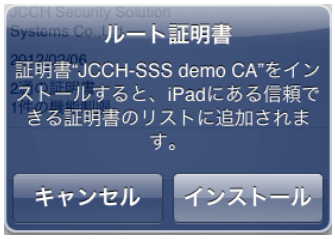
iPadのブラウザ（Safari）でGléasのUAサイトにアクセスします。
ログイン画面が表示されるので、ユーザIDとパスワードを入力しログインします。

ログインすると、そのユーザ専用ページが表示されるので、[構成プロファイルのダウンロード]をタップし、ダウンロードを開始します。
※インポートロックを有効にしている場合は、この時点からカウントが開始されます

ダウンロードが終了すると、自動的にプロファイル画面に遷移するので、[インストール]をタップします。
なお、[詳細]をタップすると、インストールされる証明書情報を見ることが可能ですので、必要に応じ確認してください。

インストール途中に、以下のようなルート証明書のインストール確認画面が現れま

すので、[インストール]をクリックして続行してください。
※ここでインストールされるルート証明書は、通常Gléasのルート認証局証明書になります。



インストール完了画面になりますので、[完了]をタップしてください。

元のUA画面に戻りますので、[ログアウト]をタップしてUAからログアウトしてください。

以上で、iPadでの構成プロファイルのインストールは終了です。

なお、インポートロックを有効にしている場合、[ダウンロード]をタップした時点より管理者の指定した時間を経過した後にUAに再ログインすると、以下の通り「ダウンロード済み」という表記に変わり、以後のダウンロードは一切不可能となります。

この他に、iOS端末の識別番号を用いて端末を限定してクライアント証明書を配布することも可能です。詳細は弊社営業担当までお問い合わせください。

6.2. Salesforce へのシングルサインオン

SafariでSalesforceへアクセスします。URLは以下のとおりです。
https://jlink.secioss.com/saml/saml2/idp/SSOService.php?spentityid=<Salesforce のエンティティID>
※2回目以降のアクセスは、Salesforceログイン後のURLも利用できます。

提示可能なクライアント証明書が一枚の場合は、何も表示されずそのままSecioss Linkのログイン画面になります。
（提示可能な証明書が複数ある場合は選択ダイアログが出現しますので、適切な証明書を選択してください）
ユーザ名はクライアント証明書のサブジェクトのcn値にSecioss Linkのテナント ID が付加されたものとなります。

Secioss Linkでのログインパスワードを入力し、[ログイン]を入力するとSalesforceログイン後の画面に転送されます。

Secioss Linkにユーザ登録されていないサブジェクトcn値を持つクライアント証明書や、[テナント情報]で設定したものと異なるサブジェクトの証明書でアクセスした場合は次のとおりエラーとなります。

クライアント証明書のない状態でアクセスすると以下のとおりエラーとなります。

失効したクライアント証明書でアクセスするとSecioss Linkのログイン画面まで進むことができません。

※失効情報がSecioss Linkに伝搬されている必要があります。

7. 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

■Secioss Linkに関するお問い合わせ

株式会社セシオス

Tel: 03-6265-0448

Mail: slink-bplats@secioss.co.jp

管理者ガイド：

http://support.secioss.co.jp/docs/SlinkManagementGuide.pdf

ユーザガイド：

http://support.secioss.co.jp/docs/SlinkUserGuide.pdf