

# 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

Copyright by JCCH Security Solution Systems Co., Ltd., All Rights reserved

- JCCH・セキュリティ・ソリューション・システムズ、JS3 およびそれらを含むロゴは日本および他の国における株式会社 JCCH・セキュリティ・ソリューション・システムズの商標または登録商標です。Gléas は株式会社 JCCH・セキュリティ・ソリューション・システムズの商標です。
- ・その他本文中に記載されている製品名および社名は、それぞれ各社の商標または登録商標です。
- ・ Microsoft Corporation のガイドラインに従って画面写真を掲載しています。

#### プライベート CA Gléas ホワイトペーパー Secioss Linkを利用したSalesforceへのシングルサインオン

#### 目次

1. はじる	めに
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
2. Secio	oss Link の設定6
2.1.	信頼する認証局の設定6
2.2.	認証ルールの作成7
3. Gléa	s の管理者設定(PC)8
3.1.	UA(ユーザ申込局)設定8
4. クラ・	イアント側での操作(PC)9
4.1.	クライアント証明書のインストール9
4.2.	Salesforce へのシングルサインオン10
5. Gléa	s の管理者設定(iPad)13
5.1.	UA(ユーザ申込局)設定13
6. クラ・	イアント側での操作(iPad)14
6.1.	構成プロファイルのインストール14
6.2.	Salesforce へのシングルサインオン17
7. 問い	合わせ19

### 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
- 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
- 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。

テナント jcch-sss.com				
	テナント			
テナントID	jcch-sss.com	2		
テナント名	JCCH・セキュリティ・ソリューション・システムズ			
最大ユーザ数	10			
現在のユーザ数	2			
サービス	サービスプロバイダの登録数 10 Google Apps Postini Salesforce			
機能	証明書認証			
証明書のサブジェクト				
CA証明書	参照			
CRLØ)URL	1			
	保存	2		
1				

- [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。

認証ルール				
🖓 新規登録				
	認証)	ν- <i>ν</i>		
ID	test	<u>_</u>		
認証方法	認証方法一覧 D/パスワード認証 前明書認証 追加 AND > 追加 OR >	選択した認証方法 証明書認証 D/パスワード認証 ▲ ▽ 削除		
優先度	1 💌			
クライアント端末	☑ Webブラウザ □ 携帯電話 □ スマートフォン ☑ iPad			

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。

認証ルール test				
役 新規登録         正常に登録されまし				
認証ルール	ネットワークの設定	時間の設定		

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、

プライベート CA Gléas ホワイトペーパー Secioss Linkを利用したSalesforceへのシングルサインオン

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。

UA 申込局	
► <u>Gleas Generic UA</u>	Gleas デフォルト申込局

[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

V	証明書ストアへのインボート	証明書ストアの種類	ユーザストア	-
	ダウンロードを許可	☑ インボートワンスを利用す	ち	

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。

2ーザ情	報の確認・変更			
▶ユーザ	登録日時:2011/02/01(	09:36		
>メールアドレJ >パスワード: (証明書情)	₹: 			
a seriorester.		シリアル	有効期限	証明書ストアヘインボート
	光门间			

「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。

ユーザ情報		_		
רב אגד 🖉	ザ さんのページ			► <u>a</u> leź
▶ ユーザ情報	の確認・変更			<u>~</u>
▶ユーザ	登録日時: 2011/02/01 09:36			
<ul> <li>&gt; 姓: テスト 名</li> <li>&gt; ユーザロ: testus</li> <li>&gt; メールアドレス:</li> <li>&gt; パスワード: *****</li> <li>* 証明書情報</li> <li>* 発行法スモリロー</li> </ul>	: ユーザ Ser 			
#	発行局	シリアル	有効期限	証明書ストアヘインポート
<u>\$1</u>	JCCH-SSS demo CA	#9735	2012/02/29	ダウンロード済み
				T

### 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。

(Jacoba)

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。

eciossLin	<b>⊚</b> secio		
ログイン			
	ユーザ名	testuser@jcch-sss.com	
	パスワード		

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。

chatter	すべて検索	
Jcch-sss	● 3047 ■	
<ul> <li>メッセージ 1</li> </ul>	今何をしていますか?	おすすめ 追加
<ul> <li>私の Chatter</li> <li>自分</li> <li>オックマーク</li> </ul>	<u>共有</u> 更新私の Chatter * 並び替え:投稿コメントE	クロファイルを記入 自己紹介を作成し、写 真をアップロードします。 スキップ >
品 すべての Chatter	さんが公開グループ すべてのJoch-sss を作成しました。 2012/08/07(1649)・コメント・ いいね	Ueno Yasuhiro 先月参加 ⊖ フォローする
● グループ ■ ファイル		トピックのトレンド <u>#Topic</u> を投稿に追加して、トレンドを 広げましょう。頻繁に使用されるトピック がトレンドになります。

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。

SeciossLink		Øsecioss
	証明書が間違っています 戻る	

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。

Ø	Internet Explorer ではこのページは表示できません
	刘処方法:
	接続の問題を診断
	⊙ 詳細情報

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 プライベート CA Gléas ホワイトペーパー Secioss Linkを利用したSalesforceへのシングルサインオン



### 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。

▶基本設定	
□ トークンへのインボート	管理するトークン Gemalto .NETカード 👤
□ 証明書ストアへのインポート	証明書ストアの種類 ユーザストア 🗾
☞ ダウンロードを許可	▼ インボートワンスを利用する
ダウンロード可能時間(分)	🗖 アカウントのワンタイムバスワードを利用する
▶ 登録申請を行わない	
	保存

[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)

▶ iPhone / iPadの設定		
☑ iPhone/iPad 用 UA を利	用する	
画面レイアウト		
☑ iPhone 用レイアウトを使	用する	☑ ログインバスワードで証明書を保護
OTA(Over-the-air)		
OTAエンロールメントを利	用する	🔲 接続する iOS デバイスを認証する
OTA用SCEP URL		
OTA用認証局	デフォルトを利用	
iPhone 構成プロファイル基	本設定	
名前(デバイス上に表示)	プライベートCA Gleas	
識別子(例: com.jcch- sss.profile)	com.jcch-sss.demo-mdm	
プロファイルの組織名	JCCH・セキュリティ・ソリューション・システムズ	
ii 兑8月	SSO用構成プロファイル	
削除パスワード	•••••	

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。

🖉 認証デバイス情報

### 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。

				Jəta-fca $\operatorname{Gle}\ddot{\operatorname{as}}$ ${\mathbb U}$
テストユー	-ザ さんのページ]			■ <u>ログアウト</u>
ユーザ情報		_	_	
🙎 テスト:	ユーザ さんのページ			▶ <u>ヘルブ</u>
▶ ユーザ情	報の確認・変更			
▶ ユーザ	登録日時	: 2011/02/01 09:36		
》 姓 : テスト 》 ユーザID : te 》 メール :	名 : ユーザ astuser			
<b>★</b> 証明書情	報			
▶ 発行済み証明	明書			
#	発行局	シリアル	有効期限	ダウンロード
<u>\$1</u>	JCCH-SSS demo CA	#9735	2012/02/29	構成プロファイルのダウンロード

※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。

AN AN	プライベートCA Gleas JCCH・セキュリティ・ソリューション・システムズ	
	◎検証済み	
記明	SSO用構成プロファイル	
署名入り	JCCH Security Solution Systems Co.,Ltd.	
受信日	2012/02/06	
内容	2通の証明書 1件の機能制限	

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。

				プライベートca Gléäs UA
[テスト ユー!	げ さんのページ]			■ ログアウト
ユーザ情報		_		
🙎 テスト ユ	ーザ さんのページ	_	_	▶ <u>ヘルプ</u>
2 ユーザ情幸	₩ の確認・変更 ······			
▶ ユーザ	登録日時 : 2	011/02/01 09:36		
》 姓 : テスト 4 》 ユーザID : test 》 メール :	h:ユーザ iuser			
★ 証明書情幸	<b>R</b> · · · · · · · · · · · · · · · · · · ·			
▶ 発行済み証明				
#	発行局	シリアル	有効期限	ダウンロード
<u>\$1</u>	JCCH-SSS demo CA	#9735	2012/02/29	ダウンロード済み

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	<b>≙</b> +
SeciossLinl	ĸ		@secioss
ログイン			
	ユーザ名	testuser@jcch-sss.com	
	パスワード		
		(1712)	

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。

chotter.	すべて検索 検索	
Jcch-sss		へいさ 💡
2	● 投稿 🌇 ファ-イル & リンク	🛛 🖓 同僚を招待
喿 Xvtz—V 1	今何をしていますか?	おすすめ 追加
<ul> <li>それの Chatter</li> <li>自分</li> <li>オックマーク</li> <li>オックマーク</li> </ul>	<u>共有</u> 更新私の Chatter × 並び替え 投稿&コメント日 ×	<b>プロファイルを記入</b> 自己紹介を作成し、写 真をアップロードします。 スキップ >
<ul> <li>▲ 人</li> <li>▲ 人</li> <li>● グループ</li> </ul>	CAUNICARD/DI - フリント (VCR) 2012/08/07(1649)・コメント・(VCR)	Ueno Yasuhiro 氏月参加 ウォローする トピックのトレンド
📔 דידע 🛛		#Topic を投稿に追加して、トレンドを 広げましょう。頻繁に使用されるトピック がトレンドになります。

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。

×	SECIOSS	<b>●</b> +
SeciossLink		@secioss
	証明書が間違っています 戻る	

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。

このWebには証明書が必要です
必要な証明書がインストールされて いません。
了解

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: <u>sales@jcch-sss.com</u>

#### ■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: <u>slink-bplats@secioss.co.jp</u>

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