



Gluegent Gate

汎用SAML for SPオプションサービス仕様書



目次

概要	2
SAMLについて	3
プロファイル仕様	3
バインディング仕様	3
認証シーケンス仕様	3
シーケンス	4
シングルサインオン	4
シングルログアウト	5
連携情報の交換	6
IdP側の情報	6
IdP側SAML情報	6
SP側の情報	7
管理情報	8
SP側SAML情報	8
アクセス権の付与	11
ユーザー詳細画面	11
アクセス権限ルール	12
ログインテスト	13
SP Initiated SSOの場合	13
IdP Initiated SSOの場合	13
付録	14
サービス固有のユーザー名/パスワードを登録するには	14
サービス固有のユーザー名/パスワードを削除するには	14



表記例

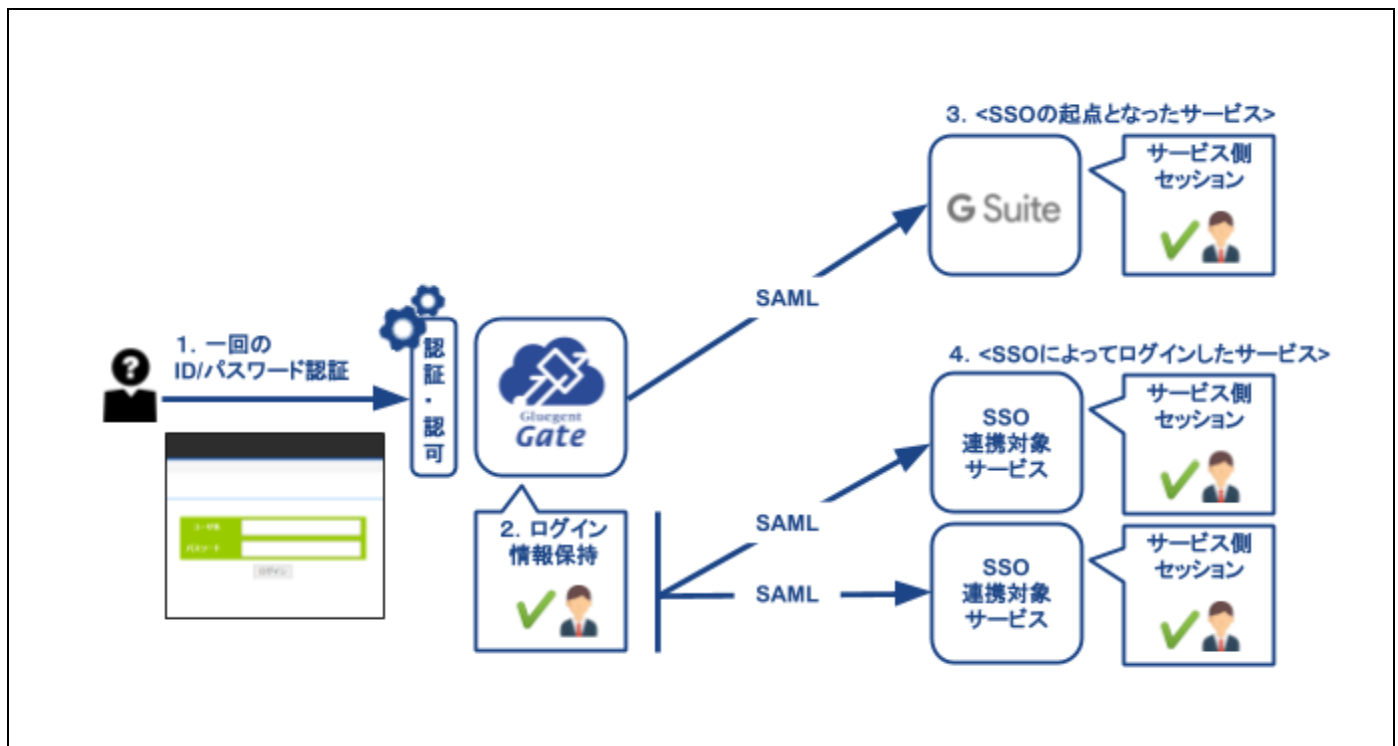
IdP	Identity Providerの略。本資料ではGluegent Gateを指します。
SP	Service Providerの略。本資料ではターゲットとなるWebサービスを指します。

概要

Gluegent Gateは、各SSO連携対象サービスのログイン情報を保持し、SSO連携対象サービスへのログインに際して、シングル・サインオンを実現します。

※汎用SAML for SPオプションは対象サービスとの認証連携を担います。連携対象サービスへのユーザー同期は行いません。

※本オプションはすべてのサービスとの連携を保証するものではありません。





SAMLについて

Security Assertion Markup Language (SAML) は、異なるシステム異なるサービス間で認証情報を交換するために、標準化団体OASISによって策定されたXML仕様です。Gluegent GateではSAML2.0標準に準拠します。

<https://www.oasis-open.org/standards#samlv2.0>

プロフィール仕様

Gluegent GateがSSO連携対象とするのはWebブラウザを介したWebサービスであり、Web Browser SSO Profileをサポートします。

バインディング仕様

Web Browser SSO Profileにおける認証情報の交換方式には、一般的なHTTP Redirect Binding並びにHTTP POST Bindingを採用しています。

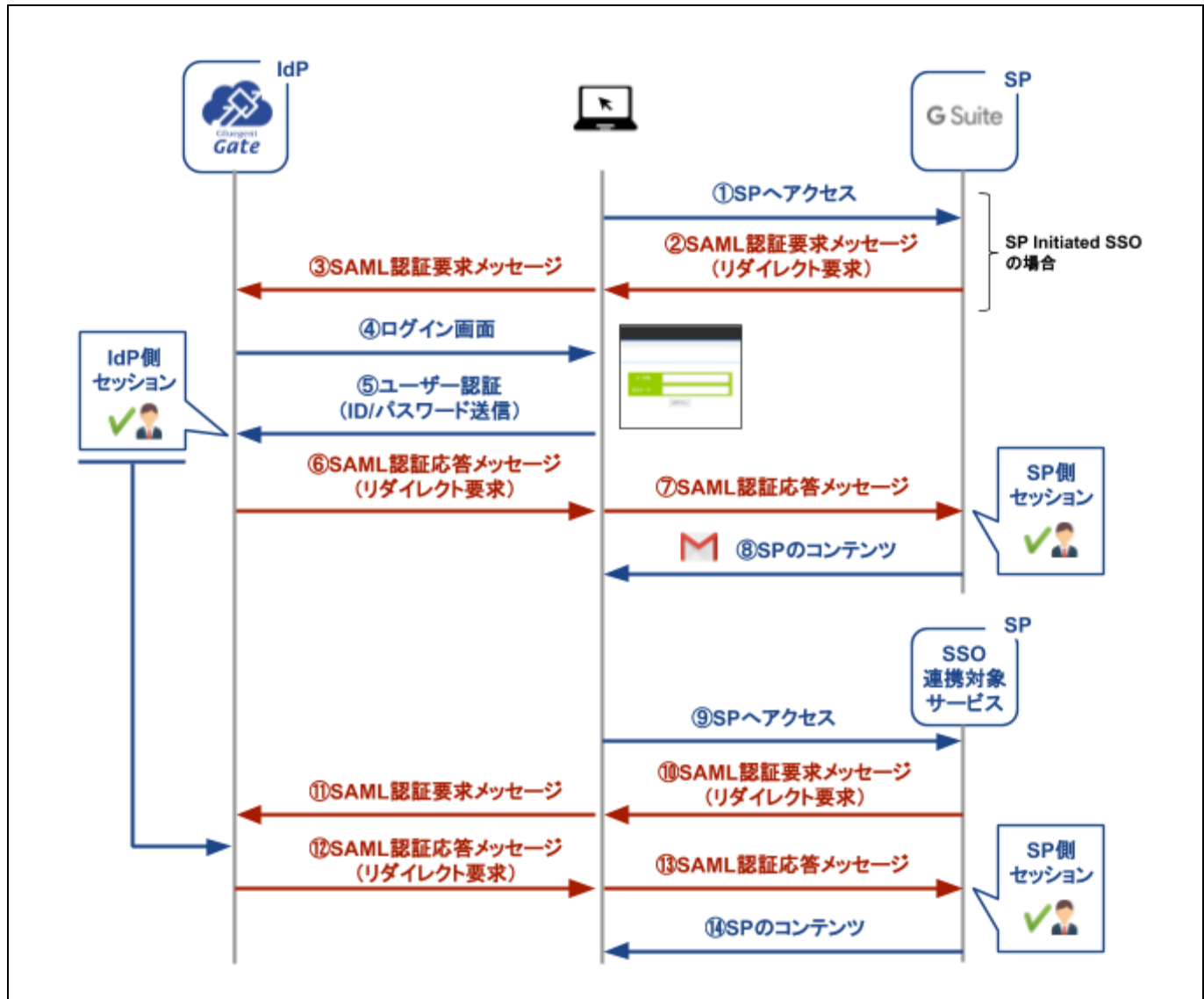
認証シーケンス仕様

Gluegent GateはSP Initiated SSOとIdP Initiated SSOをサポートします。



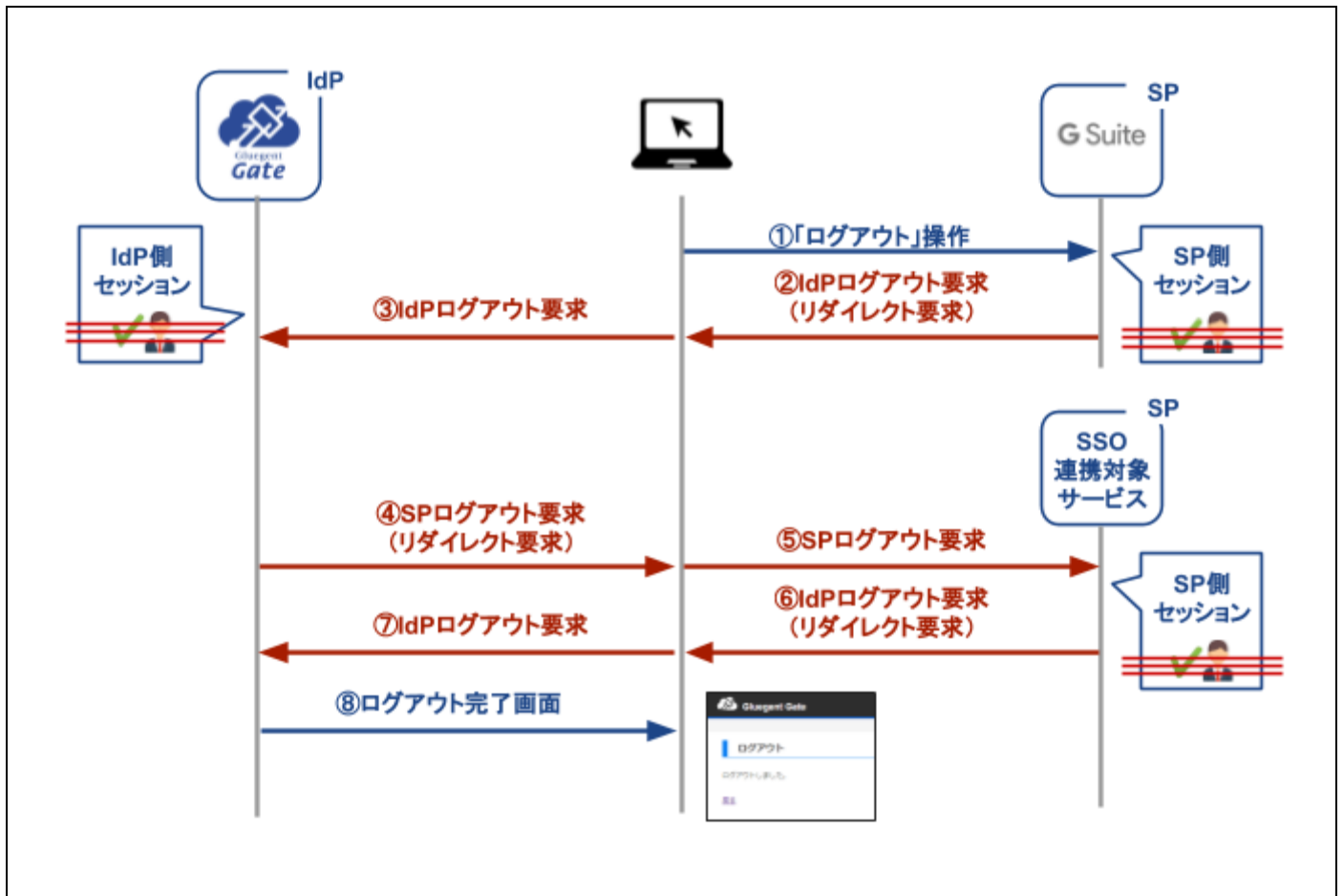
シーケンス

シングルサインオン





シングルログアウト





連携情報の交換

SAMLによるシングルサインオンを実現するには、予めIdPとSPが互いに連携情報（メタ情報）を教え合い、信頼関係を構築する必要があります。

IdP側の情報

SPに設定するIdP（Gluegent Gate側）のメタ情報です。

IdP側SAML情報

ログインURL	SPから認証要求を受けるURLです。（SingleSignOnService Location） <a href="https://auth.gluegent.net/saml/saml2/idp/SSOService.php?tenant=<テナントID>">https://auth.gluegent.net/saml/saml2/idp/SSOService.php?tenant=<テナントID> ※<テナントID>部分はGluegent GateテナントIDに置き換えてください。
ログアウトURL	SPからログアウトの要求を受けるURLです。 <a href="https://auth.gluegent.net/saml/saml2/idp/initSLO.php?RelayState=/saml/logout.php&logout=<サービスID>">https://auth.gluegent.net/saml/saml2/idp/initSLO.php?RelayState=/saml/logout.php&logout=<サービスID> ※<サービスID>部分は管理情報で設定したサービスIDに置き換えてください。
パスワード変更URL	ユーザーがGluegent Gate上の自身のパスワードを変更する為のURL https://auth.gluegent.net/user/password.php ※ユーザー自身のパスワード変更をさせたくない場合は以下のURLを利用ください。 https://auth.gluegent.net/static/denied_change_password.html
エンティティID	Gluegent Gateからの認証応答（SAMLアサーション）に含まれる識別子。「発行者」とも呼ばれます。（EntityDescriptor entityID） <a href="https://slink.seciooss.com/<テナントID>">https://slink.seciooss.com/<テナントID> ※<テナントID>部分はGluegent GateテナントIDに置き換えてください。
認証応答に含まれるユーザーIDの場所	Subject要素内のNameID要素に格納
認証応答の署名検証の公開鍵	< Gluegent Gate管理画面「システム」－「idP証明書」にて、「使用中」となっている証明書をダウンロードしてください。>
認証応答の暗号化	無し



SP側の情報

IdPIに設定するSP側の情報です。

SP側の仕様をご確認の上、Gluegent Gate管理画面－「シングルサインオン」－「SAMLサービスプロバイダ」－「サービスプロバイダ登録」から連携対象サービスを登録してください。





管理情報

シングルサインオン | SAML 一覧 登録 設定

サービスプロバイダー登録

サービスプロバイダー	
割り当てるライセンス ※	SAML 1: 10 ユーザー ▼
サービスID ※	<input type="text"/> -example.com
サービス名 ※	<input type="text"/>

割り当てるライセンス (必須)	サービスプロバイダーの設定を行うライセンスを選択します。
サービスID (必須)	Gluegent GateがSPを識別するためのID。任意の値で構いません サービスIDに記号は使用できません。英数字のみ使用可能です。 ※既に登録されたSAML SPとは重複できません。
サービス名 (必須)	Gluegent Gate管理画面上の表示名。任意の値で構いません

SP側SAML情報

SP側からGluegent Gateへの認証要求、並びにGluegent GateからSPへの認証応答に関する設定です。

※SP側のSAML仕様に関する設定となる為、具体的な設定値、入力値につきましてはSP側（連携対象サービス側）ベンダーへご確認ください。

エンティティID ※	<input type="text"/>
Assertion Consumer Service	<input type="text"/> <input type="button" value="追加"/>
ログアウトURL	<input type="text"/> <input type="checkbox"/> ログアウトの署名
デフォルトRelayState	<input type="text"/>
アクセス先URL	<input type="text"/>
IDの属性	urn:oasis:names:tc:SAML:2.0:nameid-format:persistent ▼
ユーザーIDの属性	ユーザーID ▼

送信する属性	<input type="checkbox"/> ユーザーID	属性名	seciossSystemId
	<input type="checkbox"/> ユーザーID@テナントID	属性名	uid
	<input type="checkbox"/> メールアドレス	属性名	mail
	<input type="checkbox"/> 社員番号	属性名	employeeNumber
	<input type="checkbox"/> 姓	属性名	sn
	<input type="checkbox"/> 名	属性名	givenName
	<input type="checkbox"/> 別名	属性名	displayName
	<input type="checkbox"/> 組織	属性名	ou
	<input type="checkbox"/> 地域	属性名	seciossLocaleCode
	<input type="checkbox"/> 言語	属性名	preferredLanguage
	<input type="checkbox"/> ユーザーグループ	属性名	seciossUserGroup
	<input type="checkbox"/> セキュリティグループ	属性名	seciossSecurityGroup
	<input type="checkbox"/> プロファイル	属性名	seciossBusinessRole
送信する属性 (固定値)	属性名	<input type="text"/>	値 <input type="text"/>
	条件指定 属性名	<input type="text"/>	<input type="button" value="▼"/> 値 <input type="text"/>
	<input type="button" value="追加"/>		
証明書	<input type="button" value="ファイルを選択"/>	選択されていません	
署名アルゴリズム	<input type="text" value="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>		
リクエストの署名検証	<input type="checkbox"/> 有効		
レスポンスの署名	<input type="checkbox"/> 有効		
アサーションの暗号化	<input type="checkbox"/> 有効		
メタデータ	<input type="button" value="ファイルを選択"/>	選択されていません	<input type="button" value="読み込む"/>
ポータルに表示するロゴ画像	ロゴ画像が公開されているURLを入力してください。 <input type="text"/>		
ユーザー同意取得	<input type="checkbox"/> 有効 <input type="checkbox"/> 属性値の更新後に再度同意を取得		

※ は必須項目です。

エンティティID (必須)

SPからの認証要求 (SAMLリクエスト) に含まれる識別子。「エンティティID」や「発行者」とも呼ばれます。Gluegent Gateは、本設定値とSPからの認証要求に含まれる識別子を照らし合わせ、要求元のSPを識別・検証します。

※既に登録されたSAML SPとは重複できません。

ACS(Assertion Consumer Service) (必須)

Gluegent GateからSPへの認証応答 (SAMLアサーション) の送信先URL。「Assertion Consumer Service」とも呼ばれます。

ログアウトURL	シングルログアウトを行う場合のSP側のログアウトURL。Gluegent Gateと連携された他のSPでログアウトされた際に、連動して本設定値のURLにアクセスし、このSPからのログアウトを試行します。
デフォルトRelayState	IdP-Initiatedの場合のみ使用します。
アクセス先URL	ユーザーポータルに表示するリンクのアクセス先URL。
IDの属性 (必須)	<p>SPに送信するIDの形式を以下から選択します。</p> <ul style="list-style-type: none"> ●urn:oasis:names:tc:SAML:2.0:nameid-format:persistent ●urn:oasis:names:tc:SAML:2.0:nameid-format:transient ●urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress ●urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified <p>■ persistent (永続ID) は、ユーザーログイン毎にSPに送信するIDを次項のGluegent Gateの属性から選択することができます。</p> <p>■ transient (一時ID) は、ユーザーログイン毎にランダムな値がIDとしてSPに送信されます。(次項の「ID属性」では「Transient ID」を選択してください)</p> <p>■ emailAddressは、メールアドレスをIDとしてSPに送信されます。(次項の「ID属性」では「メールアドレス」を選択してください)</p>
ユーザーIDの属性 (必須)	<p>前項に関連し、SPがIDとして認識する属性を以下から選択します。</p> <ul style="list-style-type: none"> ●ユーザーID ●ユーザーID@テナントID ●メールアドレス ●社員番号 ●サービス個別のログインID ●Transient ID <p>■前項で「persistent」を選択した場合は、Transient ID 以外を選択してください。</p> <p>■前項で「transient」を選択した場合は、Transient IDを選択してください。</p> <p>■前項で「emailAddress」を選択した場合は、メールアドレスを選択してください。</p> <p>※サービス個別のログインIDを使用するには「サービス固有のユーザー名/パスワードを登録するには」を参照してください。</p>
送信する属性	追加要素として、Gluegent Gateの持つ属性値を、SPに任意の属性名で送信することができます。送信する属性をチェックし、属性名を指定します。この属性はSAMLレスポンス内のAttributeStatement 要素内に含まれます。
送信する属性 (固定値)	追加要素として、固定の属性値を任意の属性名で送信することができます。属性名・値を指定します。この属性はSAMLレスポンス内のAttributeStatement 要素内に含まれます。条件指定ではGluegent Gateの持つ属性の値とマッチした場合にこの属性値を送信させることができます。

証明書	「サービスプロバイダへのパスワード送信」でパスワードを送信する場合や「アサーションの暗号化」を有効にした場合に、値を暗号化するための公開鍵（pem形式）をアップロードします。
署名アルゴリズム	上記証明書の署名アルゴリズムを選択します。デフォルトはSHA-256が選択されています。
リクエストの署名検証	リクエストの署名検証を実施する場合はチェックをオンにします。
レスポンスの署名	レスポンスの署名を有効にする場合はチェックをオンにします。
アサーションの暗号化	有効のチェックをオンにすると暗号化します。
サービスプロバイダへのパスワード送信	もしGluegent GateからSPへの認証応答内にパスワードを含める必要がある場合、その形式を選択します。 <ul style="list-style-type: none"> ● なし ○ シングルサインオンのパスワード ○ サービス個別のパスワード ○ ランダムパスワード ※サービス個別のパスワードを使用するには「サービス固有のユーザー名/パスワードを登録するには」を参照してください。
メタデータ	上記で設定する代わりにメタデータを読み込むことで設定ができます。
ポータルに表示するロゴ画像	このSPのアイコンがポータルに表示されます。この時に使うロゴ画像のURLを指定します。

アクセス権の付与

Gluegent Gateに連携対象サービスを登録したら、そのサービスに対するアクセス権を設定します。アクセス権は [ユーザー詳細画面](#) と [アクセス権限ルール](#) で設定します。対象サービスへのログインを試みるユーザーは、そのどちらの設定も施されることでログインが許可されます。

ユーザー詳細画面

ユーザーの詳細画面の「許可するサービス」にて、連携対象サービスにチェックを入れます。

(中略)



権限	なし ▼ 管理対象の組織 全て ▼
許可するサービス	<input checked="" type="checkbox"/> G Suite <input checked="" type="checkbox"/> saml チェック
通知用メールアドレス	<input type="text"/>

※ は必須項目です。

アクセス権限ルール

アクセス権限ルールの新規作成画面にて、連携対象サービスに対するルールを作成します。

🔒 アクセス権限 | 新規登録

アクセス権限	
ID ※	<input type="text"/>
アクセス先のサービス ※	<input type="checkbox"/> G Suite <input checked="" type="checkbox"/> saml <input type="checkbox"/> 管理コンソール <input type="checkbox"/> ユーザポータル
要求される認証方式	<div>選択した認証方法 未選択</div> <div><input type="button" value="追加"/> <input type="button" value="削除"/> <input type="button" value="▲"/> <input type="button" value="▼"/></div> <div>認証方法一覧</div> <div><input type="checkbox"/> ID/パスワード認証 <input type="checkbox"/> ワンタイムパスワード (トークン) <input type="checkbox"/> ワンタイムパスワード (メール認証) <input type="checkbox"/> スマートフォン認証 <input type="checkbox"/> PC端末認証 <input type="checkbox"/> アクセスキー認証 <input type="checkbox"/> アクセスキー確認</div>
クライアント	<input type="checkbox"/> ブラウザ PC <input type="checkbox"/> ブラウザ スマートフォン <input type="checkbox"/> ブラウザ タブレット <input type="checkbox"/> 携帯電話
権限の状態	有効 ▼

※ は必須項目です。



ログインテスト

SP Initiated SSOの場合

連携対象サービスにてSAMLによるSSOの有効化を行い、サービスへのログインを試みてください。Gluegent Gateのログイン画面にリダイレクトされ、サービスにログインができるかを確認してください。

IdP Initiated SSOの場合

連携対象サービスにてSAMLによるSSOの有効化を行い、以下のURLにアクセスしてください。Gluegent Gateのログイン画面が表示され、サービスにログインできるかを確認してください。

<https://auth.gluegent.net/saml/saml2/idp/SSOService.php?spentityid=<エンティティID>&tenant=<テナントID>>

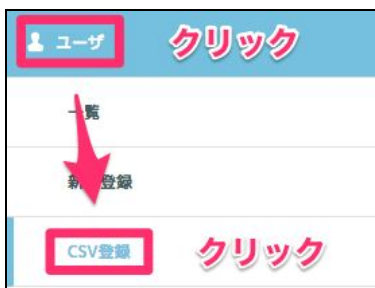
※<エンティティID>は「[SP側SAML情報](#)」で設定したURL (entityID) 値です。

付録

サービス固有のユーザー名/パスワードを登録するには

Gluegent GateユーザIDや、社員番号、メールアドレスの他に、連携対象サービス毎のユーザー名とパスワードを登録することが可能です。

「ユーザー」 - 「CSV登録」をクリックします。



「サービスのログインID登録」をクリックします。

表示されているフォーマットのCSVを作成しアップロードします。

変更も同じフォーマットで「サービスのログインID」と「サービスのパスワード」の値を変えてアップロードしてください。



ユーザ | CSV登録

登録 削除 サービスのログインID登録

サービスのログインID登録 **クリック**

ユーザ情報

CSVファイル 選択されていません

●CSVファイルの形式は次のようになります。
ユーザID,サービス,サービスのログインID,サービスのパスワード
登録可能なサービス
- sami- (saml)

登録

サービス固有のユーザー名/パスワードを削除するには

登録時のフォーマットで「サービスのログインID」と「サービスのパスワード」を空にしたCSVをアップロードします。



Gluegent Gate
汎用SAML for SPオプションサービス仕様書

2020年10月26日
サイオステクノロジー株式会社

※本書に記載されている製品名及び会社名は、各社の商標または登録商標です。
※本書の内容の無断転載および改変を禁止します。