Gluegent Gate

汎用SAML for IdPオプションサービス仕様書

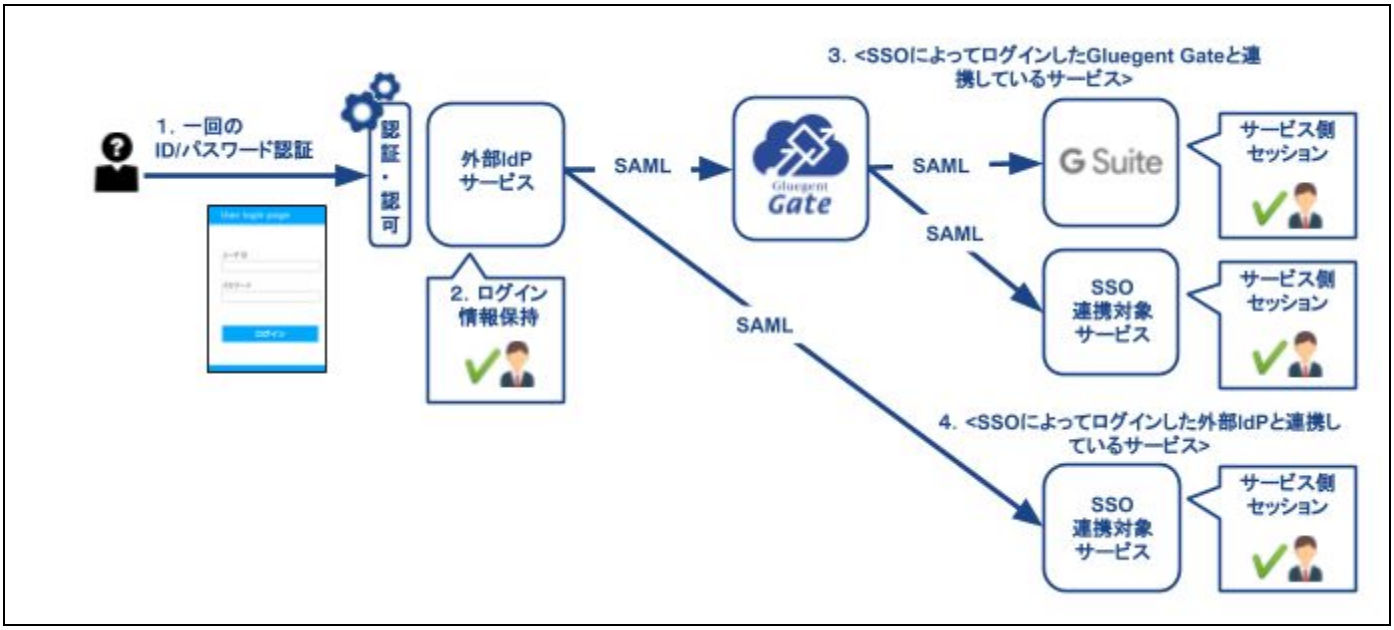
目次

表記例

IdP	Identity 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。
SP	Service Providerの略。本資料ではGluegent Gateを指します。

概要

Gluegent Gateは、外部IdPサービスのログイン情報を保持し、Gluegent Gateにて連携している各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 IdPオプションは外部IdPサービスとの認証連携を担います。外部IdPサービスへのユーザー同期、及び外部IdPサービスから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からの連携を保証するものではございません。



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

プロファイル仕様

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

バインディング仕様

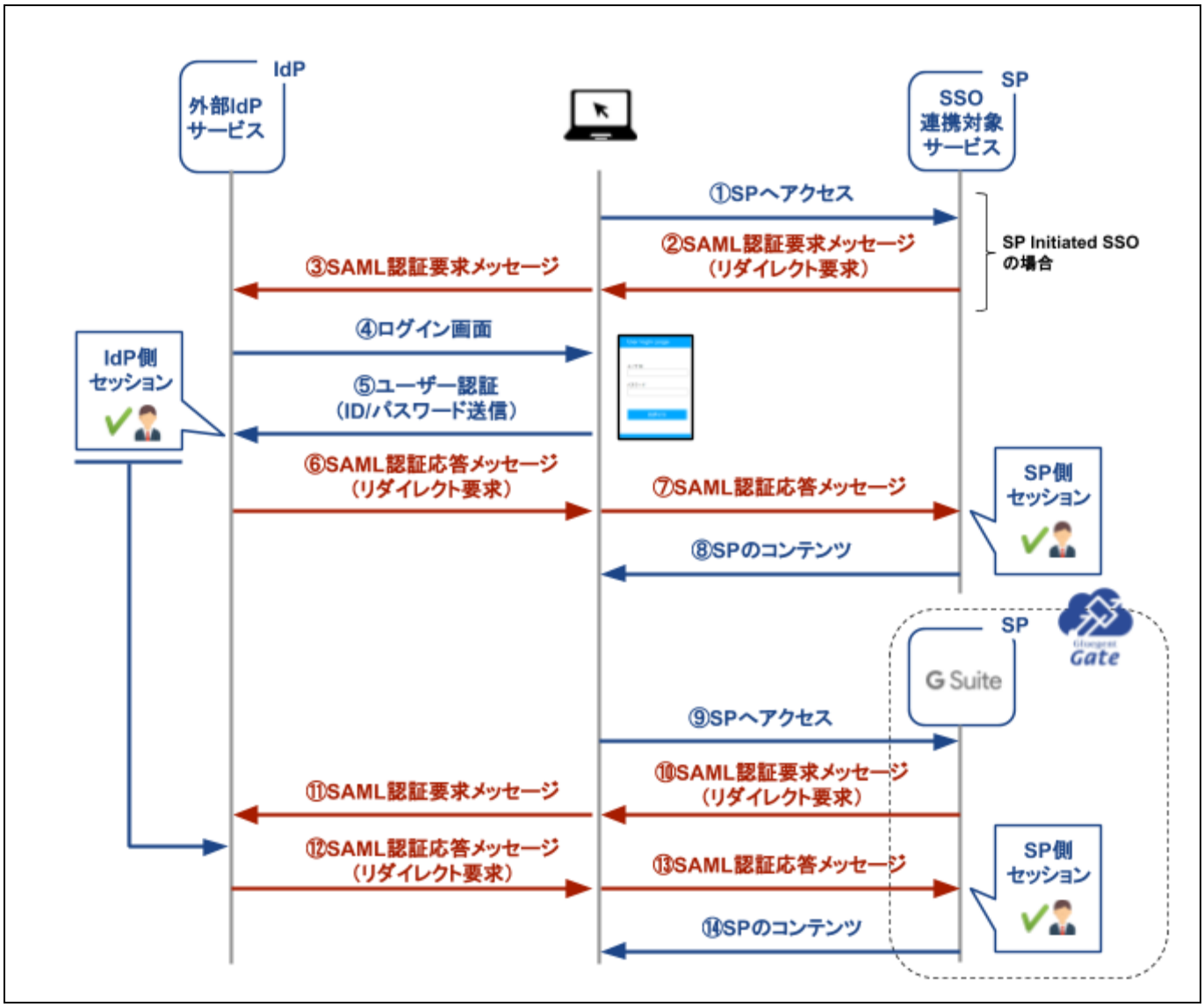
Web Browser SSO Profileにおける認証情報の交換方式には、一般的なHTTP Redirect Binding並びにHTTP POST Bindingを採用しています。

認証シーケンス仕様

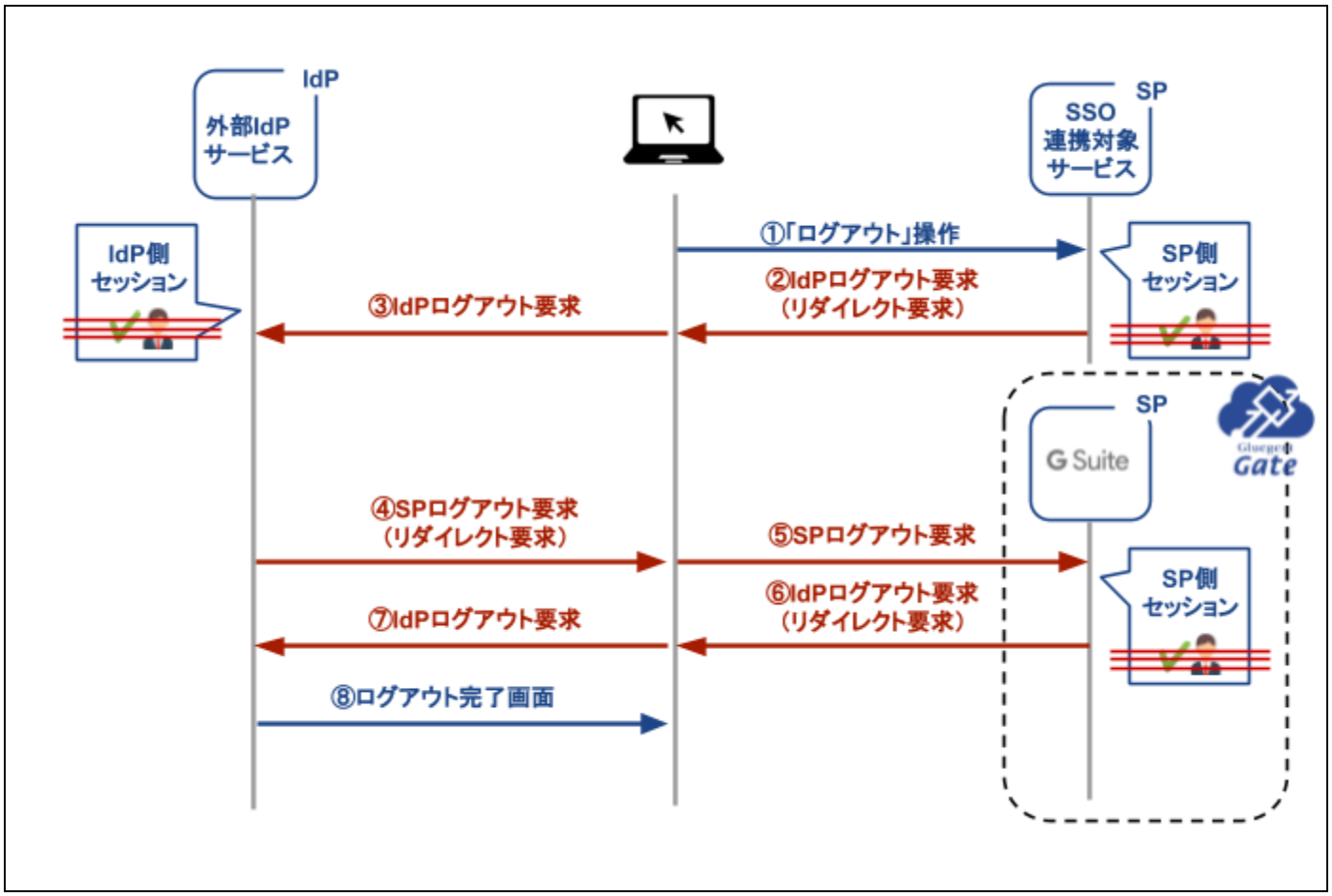
Gluegent GateはSP Initiated SSOとIdP Initiated SSOをサポートします。

シーケンス

シングルサインオン



シングルログアウト[1]



[1] シングルログアウトは現在はご利用いただけません。今後の機能拡充により対応予定です。

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（Gluegent Gate側）に設定するIdPのメタ情報です。
IdP側の仕様をご確認の上、Gluegent Gate管理画面ー「シングルサインオン」ー「SAML IDプロバイダ」から連携サービスを登録してください。

IdP側SAML情報

エンティティID（必須）	IdP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）
名前（必須）	名前を入力します。
ログインURL（必須）	SPへのログインの要求を受けるURLです。

ログアウトURL	SPからログアウトの要求を受けるURLです。SAMLログアウトを行う場合は「SAMLログアウト」のチェックをONにします。
送信するエンティティID	テナント固有のエンティティIDがある場合、チェックをONにします。
IDの属性	ログイン時に使用するIDの属性を「ユーザID」「メールアドレス」「社員番号」から選択します。
SAML公開鍵	IdP側の証明書をアップロードします。

SP側の情報

IdPに設定するSP(Gluegent Gate)側の情報です。

SP側SAML情報

Gluegent Gate側からIdPへの認証要求、並びにIdPからGluegent Gateへの認証応答に関する設定です。
※IdP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IdP側（連携対象サービス側）ベンダーへご確認ください。

URL（entityID）（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。
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。
IDの形式（必須）	SPに送信するIDの形式を選択します。 Gluegent Gateでは以下の形式に対応しています。 ● um:oasis:names:tc:SAML:2.0:nameid-format:**persistent** ● um:oasis:names:tc:SAML:2.0:nameid-format:**transient** ● um:oasis:names:tc:SAML:1.1:nameid-format:**emailAddress**
ユーザIDの属性（必須）	前項に関連し、SPがIDとして認識する属性を選択します。 ■前項で「persistent」を選択した場合は、本項では Transient ID 以外を選択してください。 ■前項で「transient」を選択した場合は、本項では Transient IDを選択してください。 ■前項で「emailAddress」を選択した場合は、本項では メールアドレスを選択してください。 ※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。

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 認証ルール と アクセス権限ルール で設定します。IdPからGluegent Gate経由で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。

認証ルール / アクセス権限ルール

認証ルール / アクセス権限ルール画面にて、「SAML認証」を選択します。

認証ルール

アクセス権限ルール

ログインテスト

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。IdP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。

Gluegent Gate
汎用SAMLオプションサービス仕様書

2020年10月1日
サイオステクノロジー株式会社