IdPの概要

IdPの概要

まず、IdPの動作について簡単に説明します。

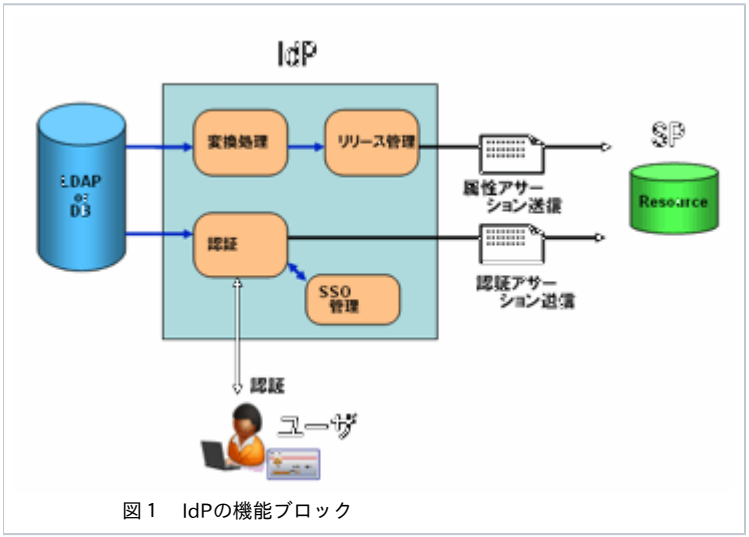

図１　IdPの機能ブロック

図１　IdPの機能ブロックは、IdPの機能を単純化したブロックで示しています。IdPはSPからの要求を受けて、以下の２つの動作を行います。

ユーザを認証する

ユーザがSPにアクセスすると、SPはIdPにリダイレクトを行います。IdPはこれを受けてユーザの認証を行います。認証方式としては、ID／パ スワード認証や、クライアント証明書による認証等の認証方式が設定可能です。また、IdPはユーザのCookieを確認して、既に認証済みである場合は、 ２回目以降のユーザに対する認証は行わず、シングルサインオン機能を実現します。

ユーザの属性を安全に送信する

SPが要求する属性を、LDAPもしくはDBから取得して、SPに送信します。この際、下記を行います。

- LDAPに格納されている情報を元にして、SPが要求する属性とするために、名称の変更や、ドメインの追加といった変換を行います（図１の変換機能）。
- SPに送信して良いかどうか、ポリシーを確認します。各属性が送信可能である場合、SAML2.0に準拠して安全に属性を送信します（図１のリリース機能）。