SPの概要

SPの概要

まず、SPの動作について簡単に説明します。

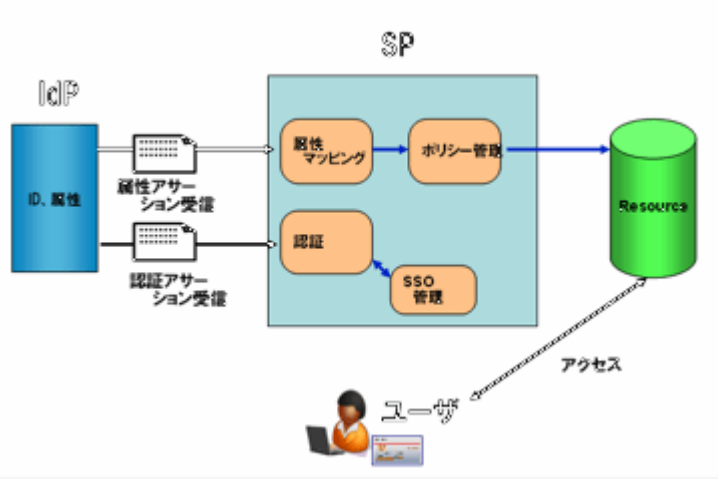

図１　SPの機能ブロック

図１ SPの機能ブロックは、SPの機能を単純化したブロックで示しています。SPはIdPと連携して、以下の２つの動作を行います。

・ユーザの認証をIdPに要求する
・ユーザの属性を安全にIdPから受信して、アプリケーションに渡す

■認証要求

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、IdPにユーザの認証を要求します。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。
ユーザの認証が行われると、SPはIdPから認証アサーションを受信してユーザを認証したことを確認します。ただし、認証アサーションが示すのはユーザを認証したという事実のみで、そのユーザが誰かという情報は含みません。

■属性の安全な受信

IdPは認証アサーションに加えて、ユーザの属性を属性アサーションに入れてSPに返信します。SPはこれを受信して、下記を行います。

属性アサーションから属性を取得して、属性の名称をIdP間で利用する名称から、アプリケーションに渡すための名称に変換する。(図１の属性マッピング機能)

属性値が許容されるものかどうか、フォーマットなどをポリシーに従ってチェックします。問題がない場合は、属性をアプリケーションに渡します。（図１のポリシー管理機能）
アプリケーションでは属性を受け、この属性によりユーザに対する認可判断を行います。

以降のページでは、SPの構築手順を示すとともに、上記機能の設定方法、および、これらの機能を用いてSPを運用するための方法について説明します。