6W-08

# シングルサインオン技術を用いたマルチサインオン方式の提案

石塚　貴　　岡本　学
Takashi Isizuka　　Manabu Okamoto
神奈川工科大学大学院 情報工学専攻

## 1．はじめに

強いセキュリティが求められている．より安全に認証を行うためにはパスワードだけでなく，生体認証や IC カード等を使った認証が必要となる．しかし生体認証や IC カードのようなハードウェアを必要とする認証の場合，実施するサイトへの負担が大きくなる欠点がある．本論文では，サービスプロバイダ(SP)が様々な種類の認証を提供する各アイデンティティプロバイダ(IdP)を複数利用することで強いセキュリティを実現するマルチサインオン方式を提案する．SP 自体には認証手段に関わる設備等の準備が不要で，ユーザは自由に必要な IdP を選択し，各 IdP が認証結果とともにポイント化された「認証スコア」を SP に提供する．本論文では認証スコアを交換する方法としてシングルサインオン・プロトコルを利用する．

## 2．マルチサインオンおよび提案方式

提案するマルチサインオン方式では，各 IdP が提供する認証結果をポイント化し，これら「認証スコア」を規定値以上集めることで認証を行う仕組みをとる．「認証スコア」とは各 IdP の認証手段のレベルに応じて全体的にポイント化された数値であり，例えば，ID・パスワードは 10 点，バイオメトリクス認証は 20 点，IC カードは 30 点などと手段に合わせて差をつけて設定することができる．SP のサービスを利用するため，ユーザは複数の IdP を渡り歩き，スコアを稼いでまわることになる．図 1 に構成概念図を示す．

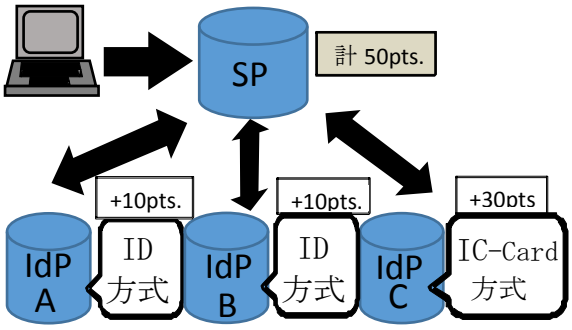


図 1．構成概念図．

ここで我々は認証結果の流通と認証スコアの提供にシングルサインオン技術を用い，その主たる標準技術である OpenID[1)]を利用する．OpenID では sReg や OpenID AX，最近発表された OpenID Connect 等でユーザの属性値をサーバ間で交換することが可能であり，我々の認証スコアについても属性値として交換させる方式をとる．SP では積算されるスコアを計算する．

図 2 に主に認証部分のシーケンスを示す．

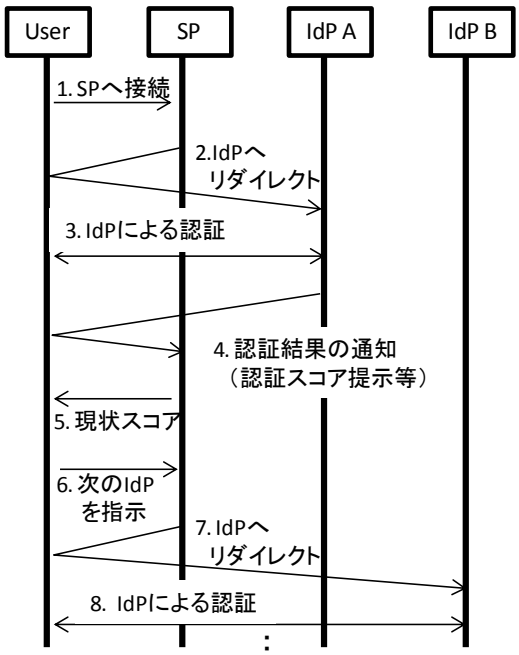


図 2．基本シーケンス．

1. ユーザは利用したい SP にアクセスする．ここで SP はユーザに対し，ログインするために必要な認証スコアを表示する．画面イメージを図 3 に示す．ここの例では SP にログインするために必要なポイントは 400 点となっている．


図 3．SP アクセス画面

2. ユーザは IdP を自由に選択する．実際には IdP ボタン（アイコン）を押すと IdP にリダイレクトされる．

3. IdP では図 4 のように各 IdP の認証方法に従ってユーザはログインを行う．図 4 の IdP では ID・パスワードによる認証だが，IdP によっては IC カードや指紋認証による認証を行う場合がある．


図 4. IdP 認証画面

4. IdP の認証に成功した場合，ユーザは SP にリダイレクトされる．この際，シングルサインオン・プロトコルにより「認証結果」が通知される．ここで認証結果に認証スコアを含める方式（OpenID の sReg 方式を流用した場合）と，ここではその後の情報交換に利用するトークンを認証結果に追加して送付する方式とがある（OpenID Connect 等）．

5. SP は IdP から送付された認証結果を評価し，問題なければその「認証スコア」を現状のユーザの点数に加点する．あるいはシーケンス図では省略してあるがここで受け取ったトークンを利用し SP と IdP 間で情報交換し，そこで「認証スコア」を獲得し合計点に加える．SP に提供する．SP はスコアを合計得点に加算する．図 5 の例では合計点が 100 点に加算されている．

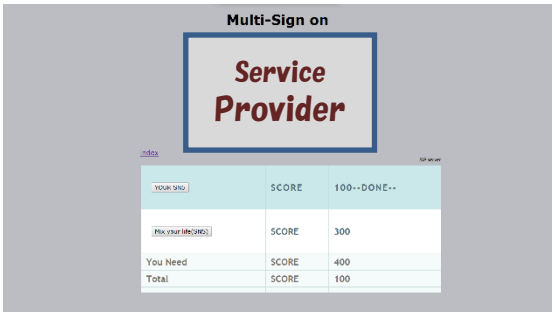


図 5. 得点加算後の SP 画面

6. ユーザは再び IdP を自由に選択しアクセスする．

7. 図 6 の例では，IdP が PKI 証明書認証を行っている．ここで提供される認証スコアは 300 点である．


図 6. PKI 証明書認証の IdP 画面

なおユーザはこのように上記のステップ 3，4，5 を繰り返し，認証スコアを稼いで周る．

8. 合計の認証スコアが規定の認証スコアを超えた場合にはじめて，SP にログインできるボタンが表示される．図 7 にイメージ図を示す．この例ではすでに規定の 400 点を獲得している．あとはユーザがログインボタンを押すだけで SP にログインすることができる．

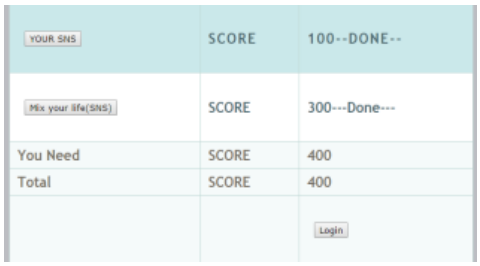


図 7. 認証スコアが規定値を超えた IdP 画面

これはシングルサインオン方式の標準の手順だが，このステップ４「認証結果通知」の中で認証スコアを提示するか，ここでトークンを提供し，そのトークンと交換でのちに認証スコアを取得する方式をとる．

## 3. 今後の課題

本方式を利用すれば自前で認証手段を準備できない SP も強いセキュリティを必要とするビジネスに参加できる「セキュリティ・プラットフォーム」を構築できる．今後は現状 OpenID Connect 等で交換されるユーザ情報として認証スコア等は含まれていないため，これら標準化や認証スコアの決め方等を検討する必要がある．

## 参考文献

1) OpenID, http://openid.net/.