



# UMIN シングルサインオン(SSO) 説明資料

UMINセンター

## UMIN ID・パスワードを使って、 UMIN SSOサーバが、 外部のWebサイトの認証代行

- 利用者がUMINシングルサインオンを対応の外部Webサイトをアクセスすると、自動的にUMIN SSOサーバへ自動転送される。



- 利用者がUMIN SSOサーバにUMIN IDとパスワードを入力



- UMIN SSOサーバが、入力されたUMIN IDとパスワードを認証し、認証に成功すると、外部Webサイトに成功の旨と利用者の属性情報を通知



- 外部Webサーバは、利用者に情報サービス提供を開始





# UMIN SSOで使用するソフト・技術仕様

- **SSO認証技術**

**SAML 2.0**

**(Security Assertion Markup Language)**

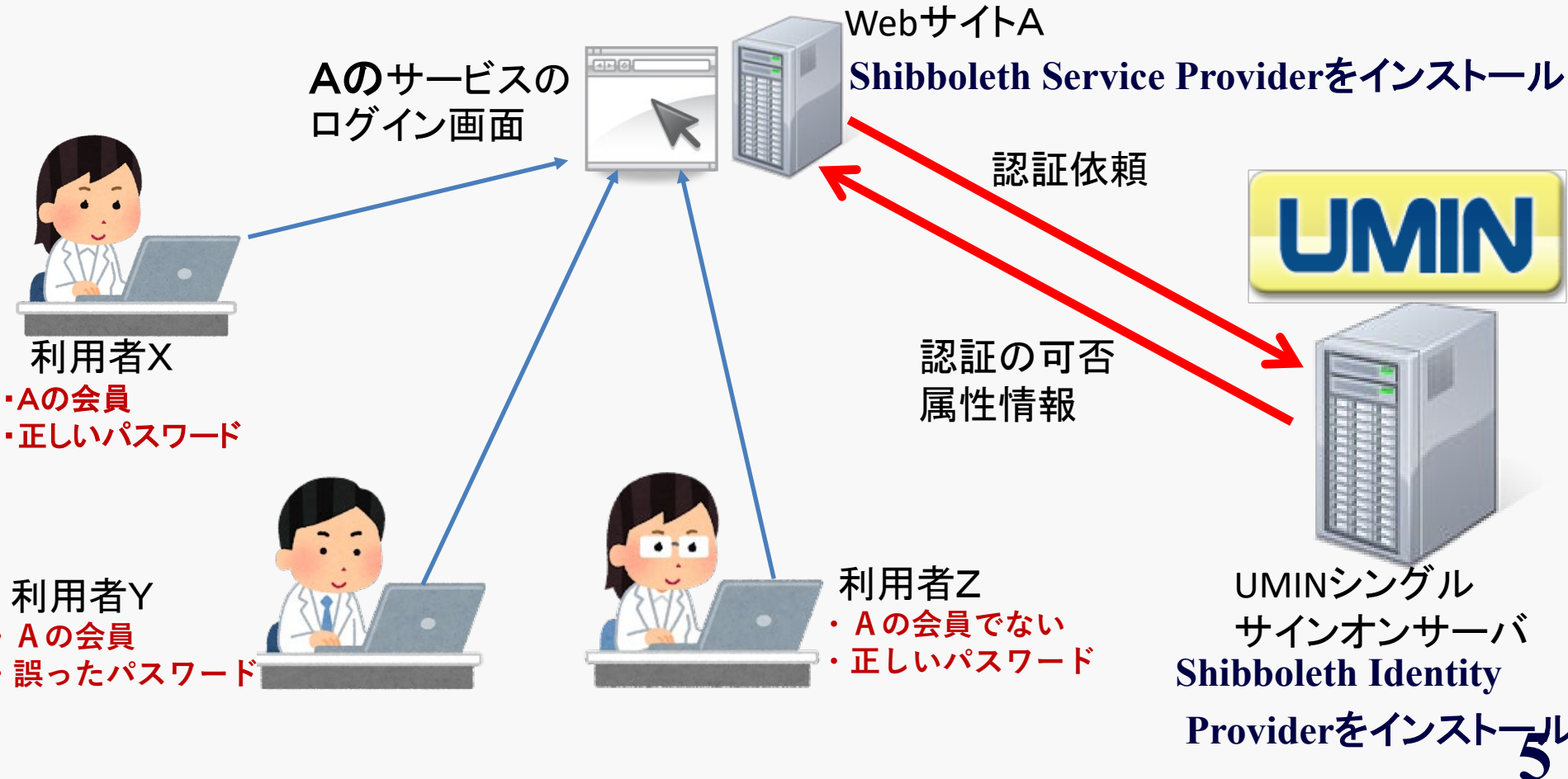
- **使用ソフトウェア**

**Shibboleth**

**(GPLライセンスのオープンソースソフトウェア)**



# UMIN SSOの動作 ー全体図





# UMIN SSOの動作 一利用者X



利用者X

- ・Aの会員
- ・正しいパスワード

1. 利用者Xが、サイトAにアクセス
2. サイトAは、UMIN SSOサーバに自動転送・認証を依頼
3. 利用者Xは、UMIN SSOサーバのログイン画面に、UMIN IDとパスワードを入力
4. UMIN SSOサーバが、利用者Xの認証に成功(正しいパスワード)
5. UMIN SSOサーバが、WebサイトAに送信する利用者Xの属性情報を利用者Xに提示
6. 利用者Xが、自分の属性情報をWebサイトAに送信することを、UMIN SSOサーバに許可(2回目以降はこの処理は自動、属性情報の提供がない場合は実施されない。)
7. UMIN SSOサーバが、利用者Xの認証結果と属性情報を、サイトAに提供
8. サイトAが、利用者Xが自らの会員であることを確認(Aの会員)
9. サイトAは、属性情報を活用して、利用者Xに情報サービスを提供



# UMIN SSOの動作 一利用者X

## 手順1~3

1. 利用者Xが、サイトAにアクセス

利用者X  
・Aの会員  
・正しいパスワード



アクセス



2. サイトAは、UMIN SSOサーバに自動転送・認証を依頼  
利用者X

・Aの会員  
・正しいパスワード



3. 利用者Xは、UMIN SSOサーバのログイン画面に、UMIN IDとパスワードを入力

利用者X  
・Aの会員  
・正しいパスワード



ログイン画面

UMIN IDとパスワード





# UMIN SSOの動作 一利用者X

## 手順4~6

4. UMIN SSOサーバが、利用者Xの認証に成功(正しいパスワード)

利用者X  
・Aの会員  
・正しいパスワード



サイトA



認証成功

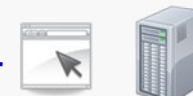
UMIN SSOサーバ

5. UMIN SSOサーバが、WebサイトAに送信する利用者Xの属性情報を利用者Xに提示  
(2回目以降はこの処理は自動、属性情報の提供がない場合は実施されない。)

利用者X  
・Aの会員  
・正しいパスワード



属性情報確認画面



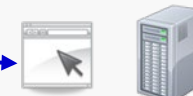
UMIN SSOサーバ

6. 利用者Xが、自分の属性情報をWebサイトAに送信することを、UMIN SSOサーバに許可  
(2回目以降はこの処理は自動、属性情報の提供がない場合は実施されない。)

利用者X  
・Aの会員  
・正しいパスワード



属性情報提供許可



UMIN SSOサーバ





# UMIN SSOの動作 一利用者X 手順7~8

7. UMIN SSOサーバが、利用者Xの認証結果と属性情報を、サイトAに提供

利用者X  
・Aの会員  
・正しいパスワード



8. サイトAは、利用者XがサイトAの会員であることを確認

利用者X  
・Aの会員  
・正しいパスワード



9. サイトAは、属性情報を活用して、利用者Xに情報サービスを提供

利用者X  
・Aの会員  
・正しいパスワード



情報サービス提供





# UMIN SSOの動作 —利用者Y



利用者Y

- ・ Aの会員
- ・ 誤ったパスワード

1. 利用者Yが、サイトAにアクセス
2. サイトAは、UMIN SSOサーバに自動転送・認証を依頼
3. 利用者Yは、UMIN SSOサーバのログイン画面に、UMIN IDとパスワードを入力
4. UMIN SSOサーバが、利用者Yの認証に失敗(間違ったパスワード)
5. 終了



利用者Z

- ・ Aの会員でない
- ・ 正しいパスワード

1. 利用者Zが、サイトAにアクセス
2. サイトAは、UMIN SSOサーバに自動転送・認証を依頼
3. 利用者Zは、UMIN SSOサーバのログイン画面に、UMIN IDとパスワードを入力
4. UMIN SSOサーバが、利用者Zの認証に成功(正しいパスワード)
5. UMIN SSOサーバが、WebサイトAに送信する利用者Zの属性情報を利用者Zに提示
6. 利用者Zが、自分の属性情報をWebサイトAに送信することを、UMIN SSOサーバに許可(2回目以降はこの処理は自動、属性情報の提供がない場合は実施されない。)
7. UMIN SSOサーバが、利用者Zの認証結果と属性情報を、サイトAに提供
8. サイトAが、利用者Zが自らの会員ではないことを確認(Aの会員でない)
9. 終了

## 1. 外部サーバがUMIN提供のSSO認証を活用

- UMIN 一般系SSO
- UMIN INDICE系(症例登録用)SSO

## 2. UMINのホームページホスティングサーバで、UMINが提供のSSOを活用(一般系SSO)

- PLAZA SSO
- SQUARE SSO
- OASIS SSO
- ISLET SSO

# 1. 外部サーバで、 UMIN提供のSSO認証を活用

UMIN一般系  
SSOサーバ

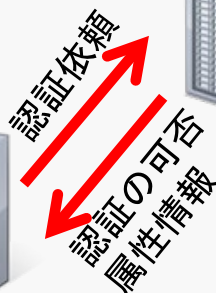


UMIN 症例登録用 (INDICE系)  
SSOサーバ

Pのサービスの  
ログイン画面



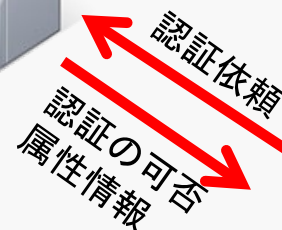
WebサイトP



Qのサービスの  
ログイン画面

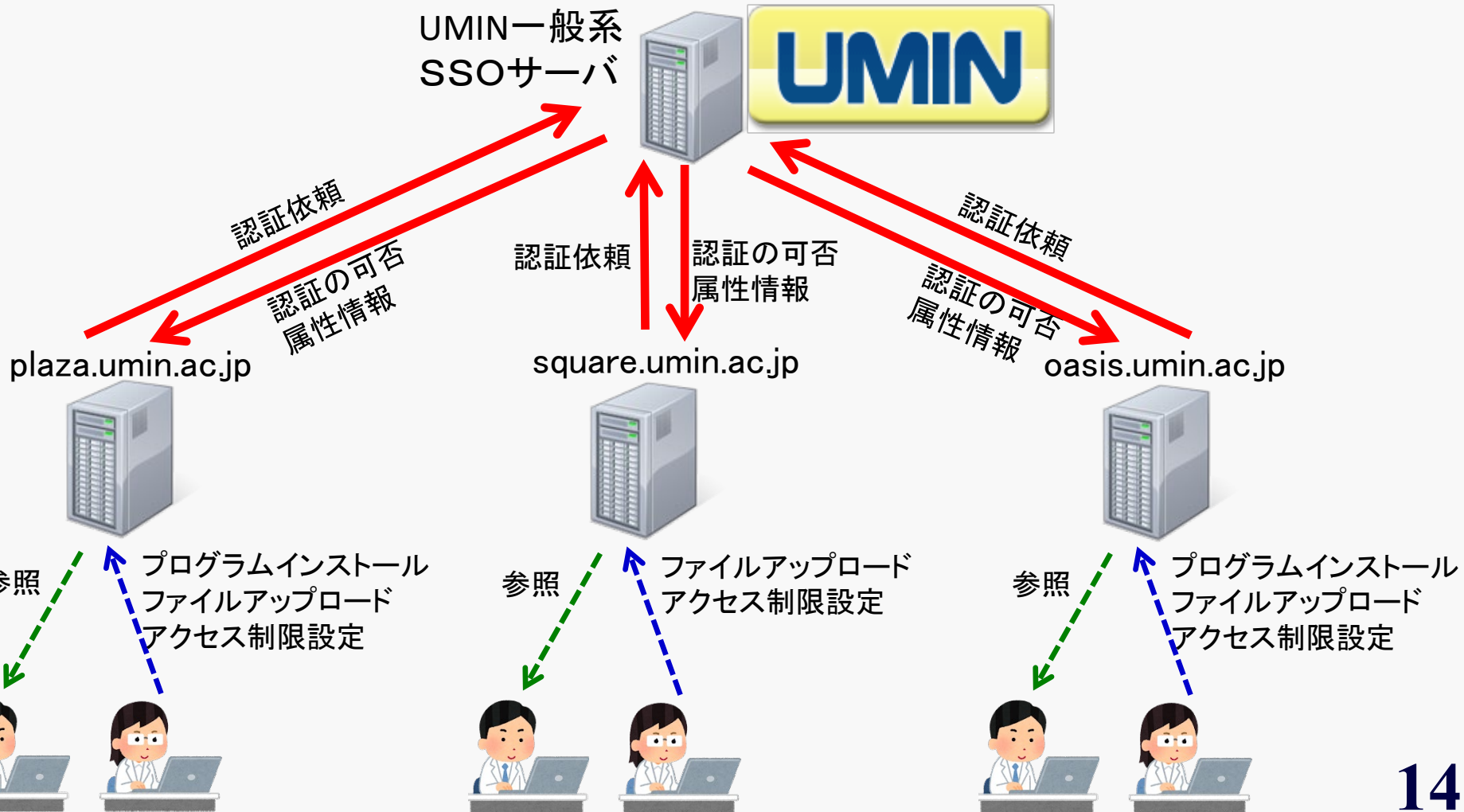


WebサイトQ





## 2. UMINのホームページホスティングサーバで、UMINの提供のSSOを活用(1) 概要





## 2. UMINのホームページホスティングサーバで、UMIN自身の提供SSOを活用(2) アップロード

- plaza.umin.ac.jpでのアップロード例  
(/home/sample-project/html/)

- ./ → 一般公開のWebページ
- ./cgi-bin/ → 一般公開のCGIプログラム
- ./sso-html/ → アクセス制限付きのWebページ  
(.htaccessがあれば該当者のみ、なければUMIN利用者全員)
- ./sso-cgi-bin/ → アクセス制限付きのCGIプログラム  
(.htaccessがあれば該当者のみ、なければUMIN利用者全員)



## 2. UMINのホームページホスティングサーバで、UMINの提供のSSOを活用(3) アクセス設定法

1. アクセス可能なUMIN IDのリストを開設者が把握して指定する方法  
(原則としてこちらをご利用ください)

.htaccessでアクセス可能なUMIN IDのリストを指定するか、  
もしくはWebアプリケーションでアクセス可能なUMIN IDかどうかをチェックして  
ください。

2. UMIN IDの属性からアクセスの可否を判断する方法  
(特殊な場合を除き、こちらの方法はご利用できません)

Webアプリケーションで、UMIN IDの属性を抽出して、アクセス可能なUMIN ID  
かどうかをチェックしてください。

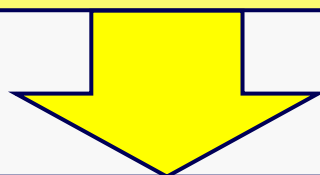


1. 関係者専用ホームページやアプリケーション、EDCのためのID、パスワード管理 (ID・パスワード発行、パスワード再発行、その他の問合せ対応) が不要！

## 2. 高い安全性と信頼性

- UMINの信頼性の高いSSOサーバ
- 米国防省も利用のSAML 2.0技術

- 一般系と症例登録用 (INDICE系) のパスワードの両方に対応
- 外部サーバで、UMIN SSOサービスを活用可能
- UMINのホームページホスティングサーバでも、UMIN SSOサービスを活用可能
- 各大学・学会等では、関係者専用ホームページ・アプリケーション、EDCの運用等に活用可能



- UMIN SSOという公的な医学系利用者認証基盤を全国で共同利用  
⇒利用者IDとパスワード管理する機関は、1つあればよい