

# UMIN

## UMIN シングルサインオン(SSO)

1

UMIN Infrastructure for Academic Activities  
University hospital Medical Information Network 大学病院医療情報ネットワーク

# UMIN UMIN SSOとは

UMIN ID・パスワードを使って、UMIN Single Sign On(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に対応の外部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

2

UMIN Infrastructure for Academic Activities  
University hospital Medical Information Network 大学病院医療情報ネットワーク

# UMIN UMIN SSOのサービス概要

- サービス対象 大学、学会、研究グループ等
- 利用料金 無料
- UMIN IDのパスワード 一般系パスワード  
症例登録用(INDICE系)パスワード
- SSOの認証技術 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)
- 現在の主な利用団体等
  1. 一般系 : 共用試験実施機構(CATO)
  2. 症例登録用: National Clinical Database(NCD)

3

UMIN Infrastructure for Academic Activities  
University hospital Medical Information Network 大学病院医療情報ネットワーク

# UMIN 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)

4

UMIN Infrastructure for Academic Activities  
University hospital Medical Information Network 大学病院医療情報ネットワーク

# UMIN SSOとは?

利用者X  
• Aの会員  
• 正しいパスワード

利用者Y  
• Aの会員  
• 誤ったパスワード

利用者Z  
• Aの会員でない  
• 正しいパスワード

Single Sign On(SSO)とは、ID Provider (IdP)と呼ばれるサーバによる一度のIDの認証によって、複数のサーバの認証 (SP=Service Provider) を行う仕組み

会員制WebサイトA  
=Service Provider (SP)  
Shibboleth Service Providerをインストール

会員制WebサイトB  
=Service Provider (SP)  
Shibboleth Service Providerをインストール

UMIN

シングルサインオンサーバ  
= ID Provider (IdP)  
Shibboleth Identity Providerをインストール

認証 (ID、パスワードチェック等) 依頼  
認証の可否、属性情報の提供

5

UMIN Infrastructure for Academic Activities  
University hospital Medical Information Network 大学病院医療情報ネットワーク

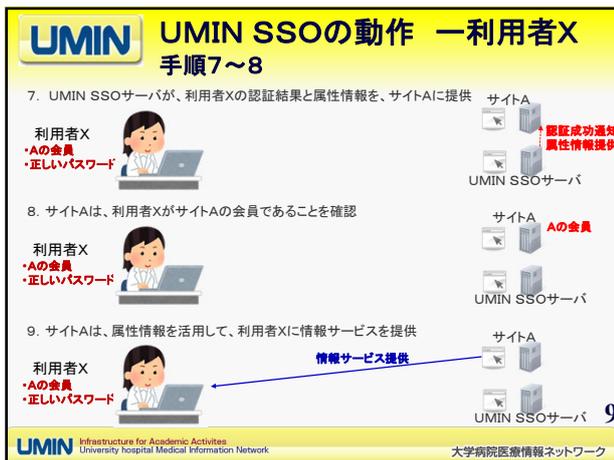
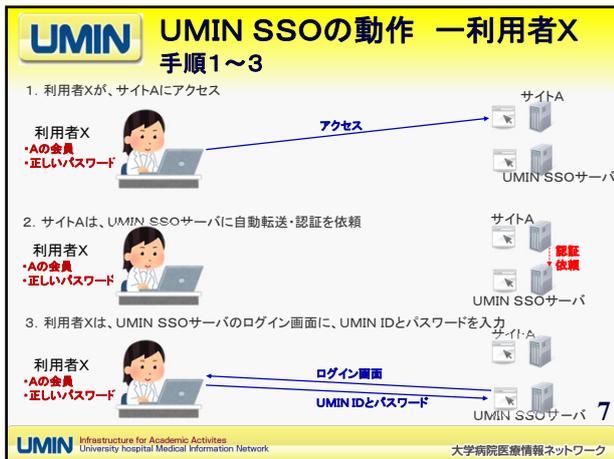
# UMIN UMIN SSOの動作 一利用者X

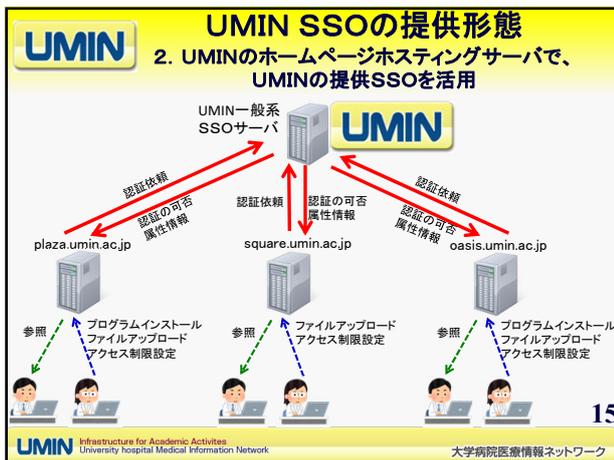
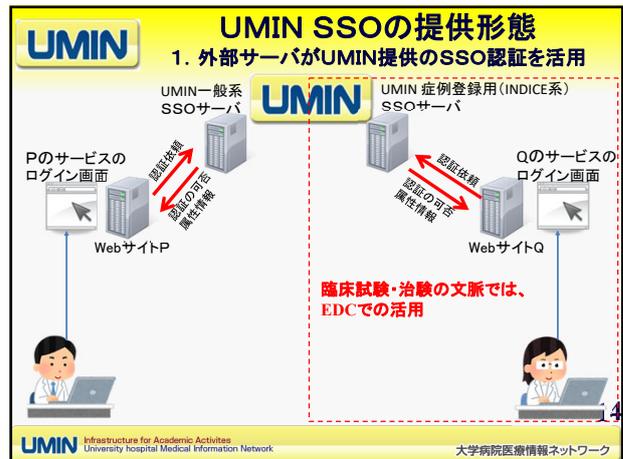
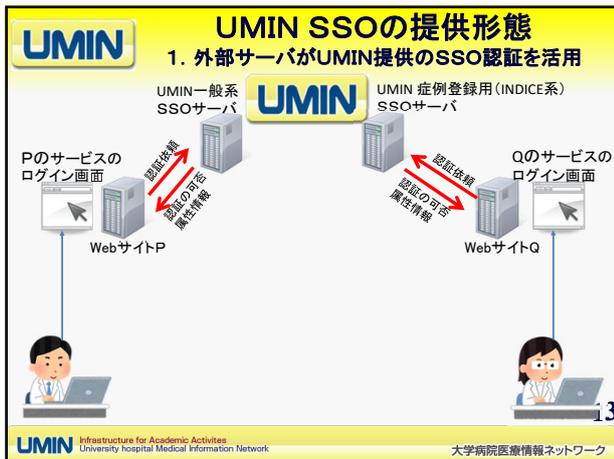
1. 利用者Xが、サイトAにアクセス
2. サイトAは、UMIN SSOサーバに自動転送・認証を依頼
3. 利用者Xは、UMIN SSOサーバのログイン画面に、UMIN IDとパスワードを入力
4. UMIN SSOサーバが、利用者Xの認証に成功 (正しいパスワード)
5. UMIN SSOサーバが、WebサイトAに送信する利用者Xの属性情報を利用者Xに提示
6. 利用者Xが、自分の属性情報をWebサイトAに送信することを、UMIN SSOサーバに許可 (2回目以降はこの処理は自動、属性情報の提供がない場合は実施されない。)
7. UMIN SSOサーバが、利用者Xの認証結果と属性情報を、サイ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

利用者X  
• Aの会員  
• 正しいパスワード

6

UMIN Infrastructure for Academic Activities  
University hospital Medical Information Network 大学病院医療情報ネットワーク





### UMIN SSOの提供形態

#### 2. UMINのレンタルホームページサーバが、UMIN自身の提供SSOを活用

- 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)

UMIN  
Infrastructure for Academic Activities  
University hospital Medical Information Network  
大学病院医療情報ネットワーク

### UMIN サーバと利用者IDの組み合わせ

1. 自前のサーバ	自前の利用者ID
2. 委託先のサーバ	自前の利用者ID
3. 自前のサーバ	UMIN SSO
4. 委託先のサーバ	UMIN SSO
5. UMIN PLAZAサーバ	自前の利用者ID
6. UMIN SQUAREサーバ	自前の利用者ID
7. UMIN PLAZAサーバ	UMIN SSO
8. UMIN SQUAREサーバ	UMIN SSO

UMIN  
Infrastructure for Academic Activities  
University hospital Medical Information Network  
大学病院医療情報ネットワーク

### UMIN 各大学、学会、研究グループ等のメリット

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

↓

- 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!
- 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

UMIN  
Infrastructure for Academic Activities  
University hospital Medical Information Network  
大学病院医療情報ネットワーク

・ UMIN ID・パスワードの運用管理費用は固定費  
⇒SSOが使われれば使われるほど利用件数の当りの  
経費は低下

1. UMINは、大学、学会、研究グループ等のSSO利用  
の如何にかかわらず、UMIN ID・パスワードの運用管  
理はしなければならない。

2. UMINは、大学、学会、研究グループ等がはいくら  
使っても運営管理経費の増加はほとんどない。

19