SQUARE/PLAZA
シングルサインオン
（Single Sign On = SSO）
説明資料

UMINセンター

SQUARE/PLAZA SSOとは

UMIN ID・パスワードを使って、
UMIN SSOサーバが、
UMINのSQUARE/PLAZAに開設されたWebサイトの認証を代行

- 利用者がSQUARE/PLAZAサーバ上に開設された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、SQUARE/PLAZAサーバ上に開設されたWebサイトに成功の旨と利用者の属性情報を通知
- SQUARE/PLAZAサーバ上に開設されたWebサイトは、利用者に情報サービス提供を開始

SQUARE/PLAZA SSOの サービス仕様

- サービス対象

⇒SQUARE/PLAZA で開設されたすべてのWebサイト

- 利用料金

⇒無料

- 提供ID・パスワード

⇒UMIN IDと一般系パスワード

（症例登録用パスワードは使えません）

SQUARE/PLAZA SSOで使用のソフト・技術仕様

- SSO認証技術

SAML 2.0

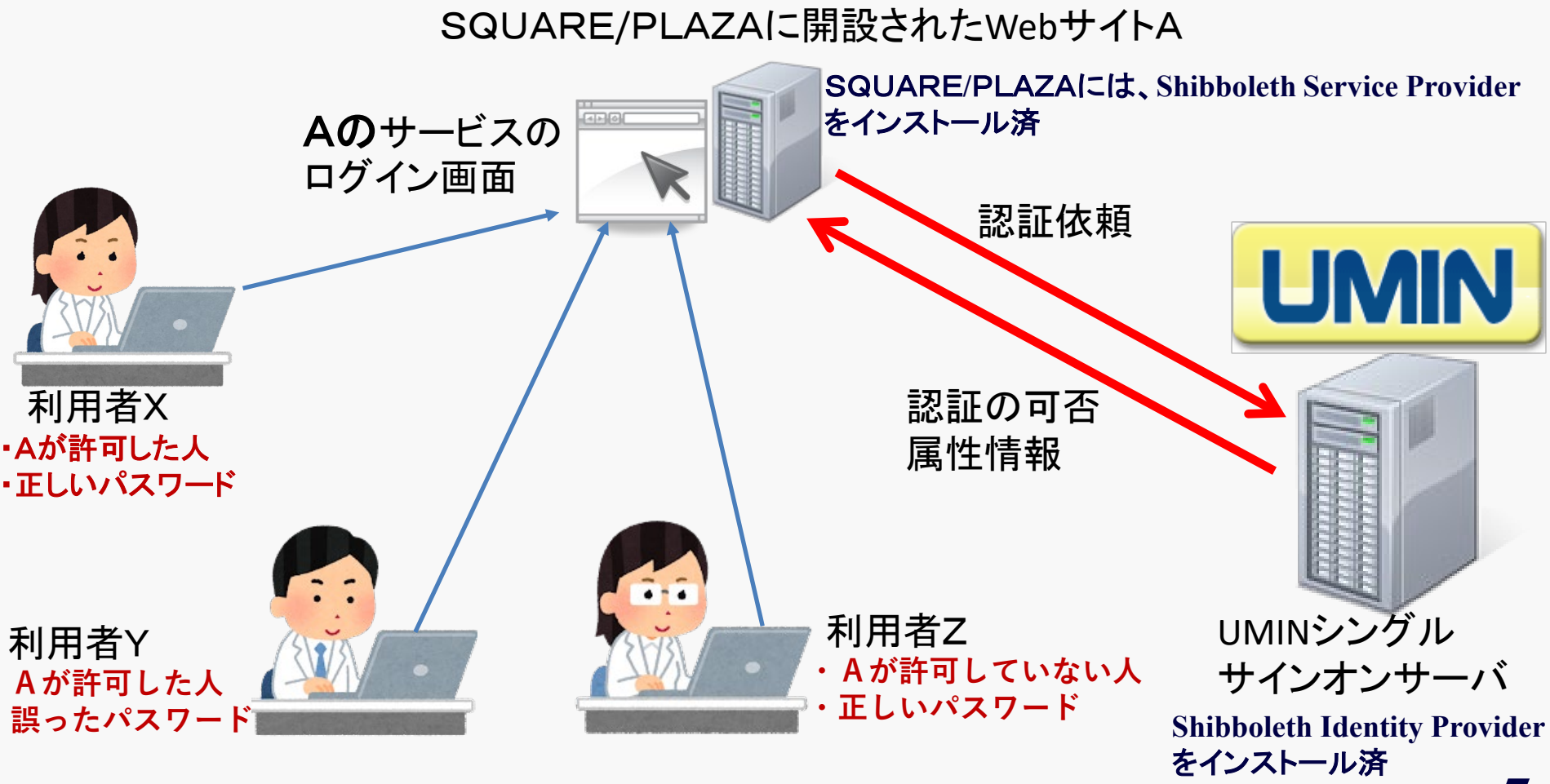
（Security Assertion Markup Language）

- 使用ソフトウエア

Shibboleth

（GPLライセンスのオープンソースソフトウエア）

SQUARE/PLAZA SSOの動作 全体概要



アクセス可能なUMIN IDの指定方法（1）

- plaza.umin.ac.jpでのアップロード例
  （square.umin.ac.jpも同様）

WebサイトAのドキュメントルートを“/home/website-a/html/”とする。
（外部から参照するためのURLは、”https://plaza.umin.ac.jp/website-a/”）

./　→一般公開のWebページ（アクセス制限がかからない）
./cgi-bin/　→一般公開のCGIプログラム（アクセス制限がかかない）
./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）

アクセス可能なUMIN IDの指定方法（2）

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。

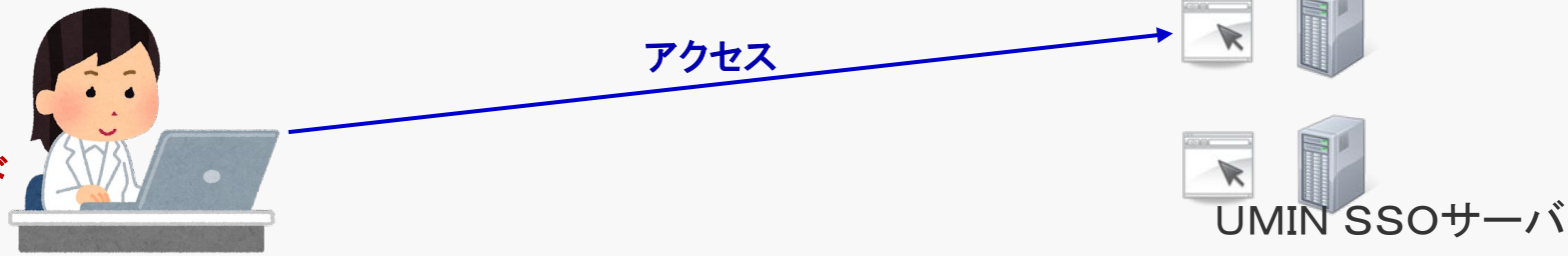
SQUARE/PLAZA SSOの動作 ー利用者X

利用者X
・Aの会員
・正しいパスワード

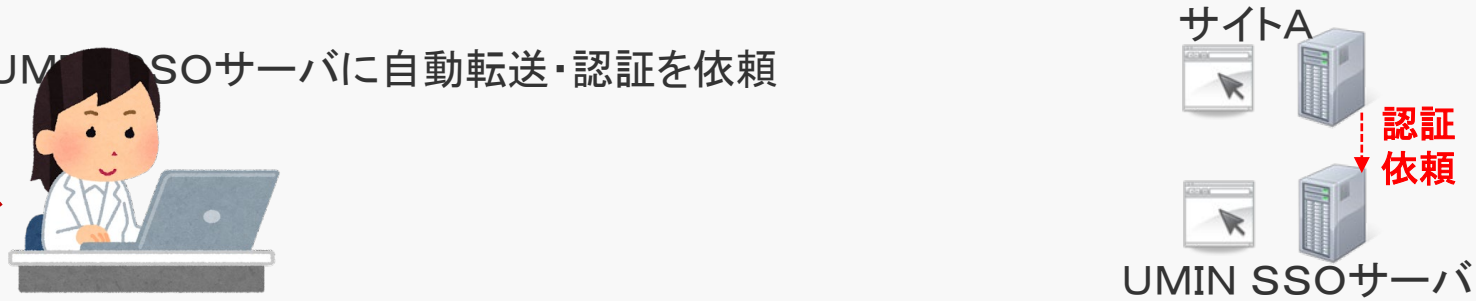
1. 利用者Xが、サイトAにアクセス
2. サイトAは、UMIN SSOサーバに自動転送・認証を依頼
3. 利用者Xは、UMIN SSOサーバのログイン画面に、UMIN IDとパスワードを入力
4. UMIN SSOサーバが、利用者Xの認証に成功（正しいパスワード）
5. UMIN SSOサーバが、WebサイトAに送信する利用者Xの属性情報を利用者Xに提示
6. 利用者Xが、自分の属性情報をWebサイトAに送信することを、UMIN SSOサーバに許可
（2回目以降はこの処理は自動、属性情報の提供がない場合は実施されない。）
7. UMIN SSOサーバが、利用者Xの認証結果と属性情報を、サイトA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

SQUARE/PLAZA SSOの動作　ー利用者X　手順1～3

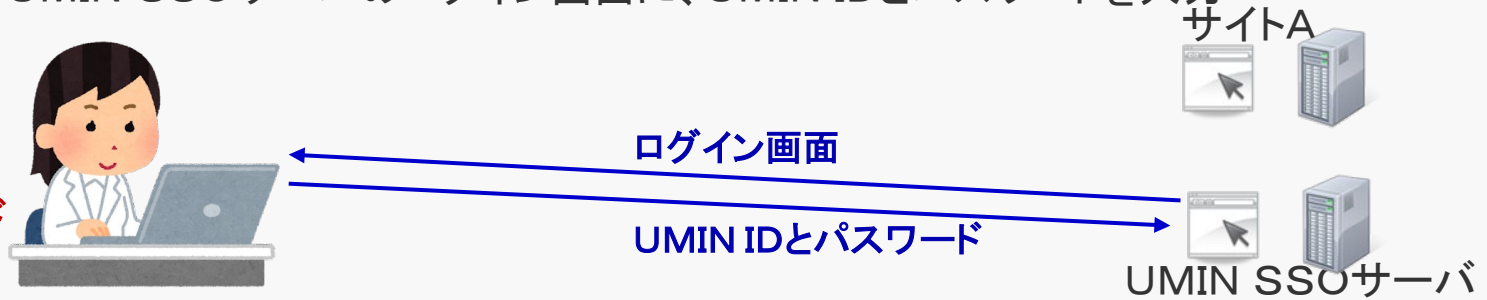
1．利用者Xが、サイトAにアクセス



2．サイトAは、UMIN SSOサーバに自動転送・認証を依頼



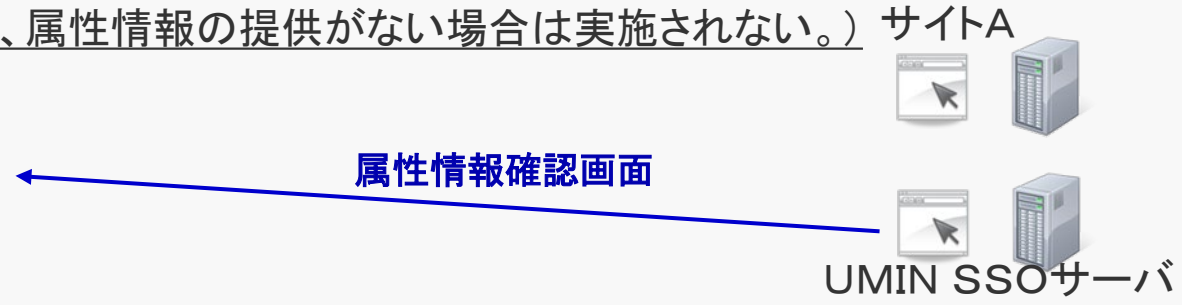
3．利用者Xは、UMIN SSOサーバのログイン画面に、UMIN IDとパスワードを入力



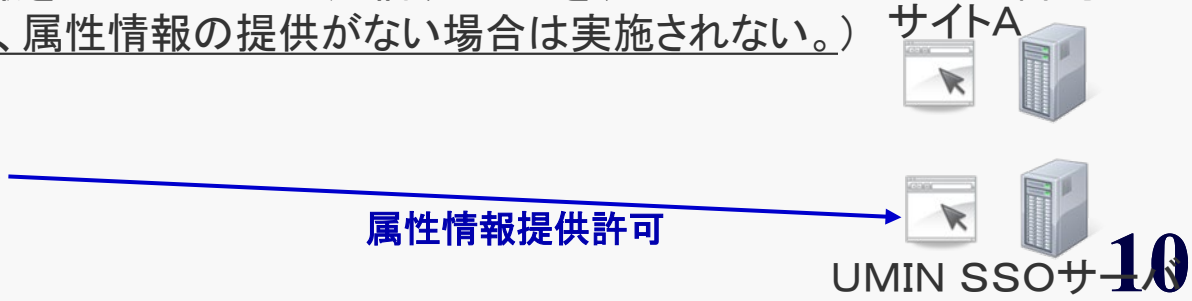
SQUARE/PLAZA SSOの動作　一利用者X 手順4～6

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）

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。）



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。）



SQUARE/PLAZA 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

SQUARE/PLAZA SSOの動作　ー利用者Y

利用者Y
・Ａの会員
・誤ったパスワード

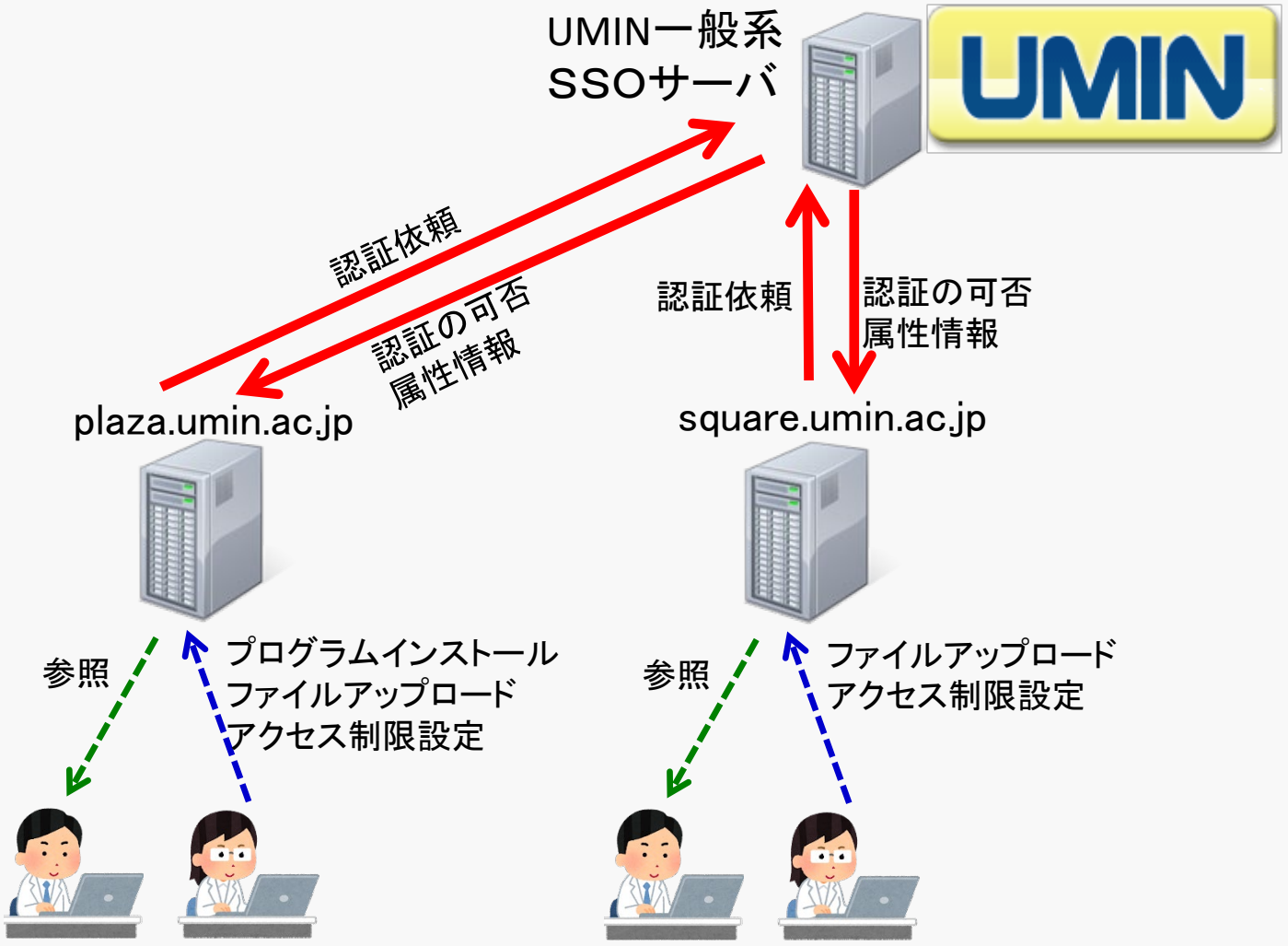
1. 利用者Yが、サイトAにアクセス
2. サイトAは、UMIN SSOサーバに自動転送・認証を依頼
3. 利用者Yは、UMIN SSOサーバのログイン画面に、UMIN IDとパスワードを入力
4. UMIN SSOサーバが、利用者Yの認証に失敗（間違ったパスワード）
5. 終了

SQUARE/PLAZA SSOの動作　ー利用者Z

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

SQUARE/PLAZA SSOの提供形態
UMINの提供SSOを活用



SQUARE/PLAZAでホームページを開設する団体、個人のメリット

1. 関係者専用ホームページやアプリケーションのための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

SQUARE/PLAZA SSO　まとめ

- SQUARE/PLAZAでホームページを開設するすべての団体、個人が無料で利用可能
- UMIN IDと一般系のパスワードで認証
- 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作業を集約