

機構統合認証を用いた専攻 Web アプリケーションの再開発

○中村成美、島田啓史

情報通信技術支援室 情報システム構築技術グループ

はじめに

本学では国立大学法人東海国立大学機構（以下、機構）となったことを機に、Web アプリケーション（以下、Web アプリ）の認証を名古屋大学認証基盤サービスから機構統合認証サービス（以下、機構統合認証）へ移行する方針となった。これに伴い、当グループが管理している専攻 Web アプリについて、機構統合認証を用いて再開発を行った。

対象の Web アプリは、将来にわたって安定した管理ができるように複数人の職員で開発を行うこととし、開発は PHP フレームワークの Laravel を用いた。機能は既存の Web アプリとほぼ同様としたが、モバイル端末で表示した時のデザインを改良した。認証は Shibboleth を使用し、認可については、laravel-shibboleth^[1]というモジュールをベースに実装を行った。これらの内容について報告を行う。

1 Web アプリの機能

Web アプリの動作環境を表 1 に示す。

本 Web アプリは、専攻関係者（工学部電気電子情報工学科、大学院工学研究科電気工学専攻、電子工学専攻、情報・通信工学専攻所属の教職員・学生）のみが利用できるシステムであり、1)学生掲示板、2)会議室予約、3)受賞者情報掲載、4)教員公募掲載の機能がある。

表 1. Web アプリの動作環境

種別	バージョン
OS	Rocky Linux 9
データベース (DB)	MariaDB 10.5
Web サーバ	Apache 2.4
SP サーバ	Shibboleth SP 3.5
プログラミング言語	PHP 8.2
PHP フレームワーク	Laravel 11
CSS フレームワーク	Bootstrap 5

1.1 学生掲示板機能

学生掲示板の表示画面の例を図 1 に示す。掲示板はタイトルをクリックすると詳細ページが表示される。また、詳細ページから PDF を出力することができる。PDF 出力機能は、学生用に設置してある掲示板に紙ベースで出力したいと専攻事務室から要望があったため、実装を行った。各記事には公開期限が設定されており、設定日を過ぎると過去情報ページへ移動される。過去情報は過去 2 年度分が閲覧可能である。



図 1. 学生掲示板の表示画面

1.2 会議室予約機能

会議室予約の表示画面の例を図2に示す。会議室ごとに予約状況をカレンダー表示（月単位）で確認することができる。日付部分をクリックすると、全部屋の予約状況が表示される。会議室の予約登録については、管理者と一般利用者によって予約可能期間が異なっており、管理者は一般利用者権限の予約可能期間を変更することができる（図2黄色ボタン）。今回の再開発では、視認性向上のため、カレンダー表示と予約状況の表示部分の実装方法をHTMLのテーブルタグからJavaScriptのライブラリに変更した。



図2. 会議室予約の表示画面

1.3 受賞者情報掲載機能

受賞者情報の登録ページを図3に示す。受賞者情報の登録時に、情報を表示させる言語ページを「和英選択」から選択する。「和文」を選択した場合は日本語ページ、「英文」の場合は英語ページ、「両方」は日本語・英語の両ページに掲載される。受賞者一覧（教員）ページを図4に示す。登録時に選択する身分情報（受賞者の職名または学年の項目）によって、学生と教員で表示されるページを分けている。

受賞者情報登録

掲載者が学生の場合、入力後に教員または研究室秘書に入力した旨を伝え、入力内容を確認してもらってください。

和英選択 *

☒ 和文 ☐ 英文 ☐ 両方

受賞名(和文)

受賞者(和文)

受賞名(英文)

受賞者(英文)

受賞日 *

※クリックするとカレンダーが表示されます。受賞日をクリックしてください。

受賞者の職名または学年 *

(選択してください)

図3. 受賞者情報登録ページ

日本語ページ

最近の出来事一覧	受賞者一覧(教員)	受賞者一覧(学生)	最終更新日: 2025年03月03日
このページは、名古屋大学電気工学専攻、電子工学専攻、情報・通信工学専攻関連教員の受賞を紹介するものです。			
※電気系関係者は、学内向情報ページへログインすると受賞者情報を登録することができます。			
受賞者情報登録 更新・削除			
受賞日	受賞名	職名	受賞者 【所属研究室】
2025-03-01	電気学会 ○○委員会 若手奨励賞	助教	名大 花子 【○○研究室】
2025-02-28	○○学会 優秀発表賞	教授	名大 太郎 【○○研究室】
2025-02-28	電気学会 ○○ 優秀論文賞	助教	名大 花太郎 【○○研究室】

図4. 受賞者一覧（教員）ページ

1.4 教員公募情報掲載機能

教員公募情報登録ページを図5に示す。本機能は、教職員のみが登録可能である。教員公募情報一覧の例を図6に示す。登録時に選択した公募期限日を過ぎると、公募情報は公募期限切れの情報ページへ移動される。

教員公募情報登録

公募期限 *

2025/03/04

タイトル *

内容 *

登録者氏名 *

登録者Email *

図5. 教員公募情報登録ページ

教員公募情報

登録 更新・削除

公募期限内の情報 公募期限切れの情報

タイトル	〇〇大学院工学研究院 教員公募
公募期限	2025年03月28日
内容	1. 募集人員 准教授または助教 2. 専門分野 〇〇データサイエンス 3. 所属 〇〇〇講座 4. 締切 令和7年3月28日（金） ※詳細は資料ファイルをご覧ください。
資料ファイル	202501151.pdf
連絡先メールアドレス	test@test.nagoya-u.ac.jp
登録者	事務局
最終更新日	2025年03月03日

図6. 教員公募情報一覧

1.5 デザイン変更

デザインを変更した箇所について図7に示す。具体的には、学内向情報メニュー（①）の表示位置を変更した。旧デザインでは、モバイル端末で表示するとメニューが一番下に表示されてしまい、画面をスクロールしなければ見ることができなかった。そのため、新デザインでは、画面上部に表示される学内向情報メニューボタンをクリックするとメニュー項目がボタンの下に表示されるようにした（②）。



図7. デザイン変更箇所

また、ログインしているユーザの機構アカウント名が表示されるようにした（③）。旧デザインは、ログインしているユーザ情報の表示がなかったが、新デザインでは、機構アカウント名を見やすい位置に表示させ、Web アプリにログイン中であることが一目見て分かるようにした。

2 認証・認可について

本 Web アプリは、1 章で述べたとおり専攻関係者のみが利用できるように、アクセス制限を行っている。機構統合認証の後、認可処理により専攻関係者であれば、Web アプリを利用できる仕組みである。

2.1 認証

認証とは、ユーザが誰であるかを確認するプロセスである。本 Web アプリでは、機構の構成員であるかを確認している。認証は Shibboleth Service Provider(SP) v3.5 を使用した。SP は、ユーザと Identity Provider(IdP) に認証要求を送信するサーバ（専攻 Web アプリサーバに該当）であり、IdP はユーザの認証情報を保存・管理するサーバである。SAML 認証とは、シングルサインオンを実現するための認証方法の一つで、XML を基盤としたセキュリティ情報交換のための標準仕様である。

機構統合認証の流れを図 8 に示す。まず、ユーザがブラウザから SP にアクセスすると、SP は SAML 要求を生成し、ブラウザを通して IdP へリダイレクトする（①～③）。IdP は SAML 要求を解析し、ユーザとの間で認証を行う（④、⑤）。認証が完了した後、IdP は SAML 応答を発行し SP へリダイレクトする（⑥、⑦）。SP は、SAML 応答を確認しユーザに Web アプリの機能を提供する（⑦、⑧）。

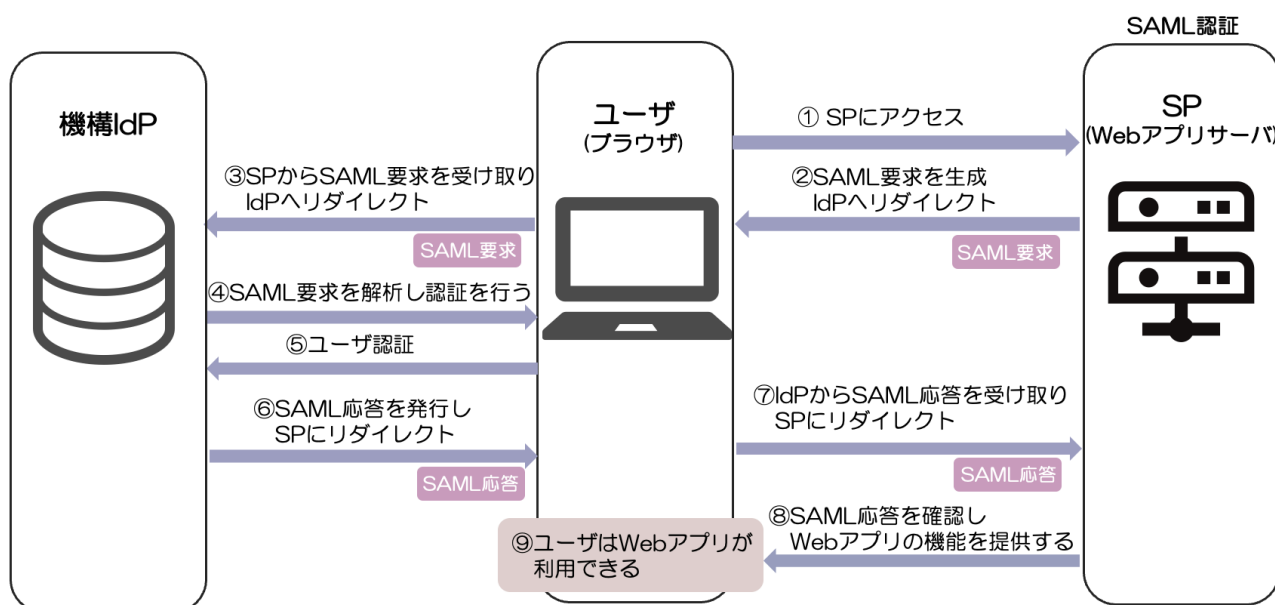


図 8. 機構統合認証の流れ

2.2 laravel-shibboleth

Laravel には認証・認可機能が実装されているが、今回の Web アプリ開発において、Laravel の標準機能に独自の改良を行うと、セキュリティや運用開始後のメンテナンスリスクが高まるため、標準で提供される機能についてはそのまま使用したいと考えた。そこで、米イリノイ大学で使用されている laravel-shibboleth という認可モジュールを用いることにした。laravel-shibboleth は、Shibboleth SP の認証情報をもとに認可処理を行った後、Laravel の認証を通すモジュールである。この認可モジュールを機構統合認証に対応する形に改良した。

2.3 認可

認可とは、認証されたユーザが特定のアクションを実行することを許可する処理であり、本 Web アプリでは専攻関係者であるかを判断する（図8の⑦と⑧の間で行われる）。本 Web アプリにおける、laravel-shibbolethを用いた認可処理の流れを図9に示す。機構統合認証後に得られたユーザデータは SP 内に保持されているため、laravel-shibboleth ベースの認可モジュールが、認証後のユーザデータを SP から取得し、Web アプリ DB 内のユーザテーブル情報と照合して認可処理を行う。

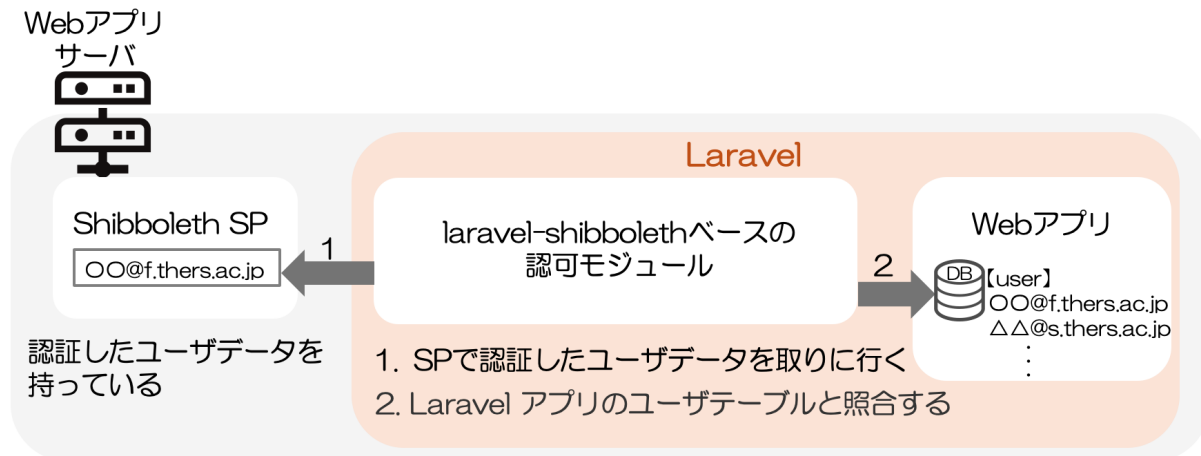


図9. 認可処理の流れ

認可の条件を図10に示す。機構IDは、1人に対して1つしか発行されない生涯IDであり、内部的に利用されるIDである。それに対し、機構アカウントは、利用者の身分毎に発行され、Web アプリ等にログインする際に用いられるアカウントである^[2]。教職員がWeb アプリにログインした場合は、認証後にSPから取得したユーザデータと、事前に管理者がDBに登録している機構IDまたは機構アカウントと一致すれば認可される。学生の場合は、初回ログイン時に、認証されたユーザデータに含まれる所属コードと、Web アプリ内に事前設定してある所属コードを照合し一致すれば認可され、機構IDと機構アカウントがDBに新規登録される。学生の2回目以降のログイン時は、教職員同様、機構IDまたは機構アカウントがDBに存在すれば認可される。なお、学生が進学・転科・卒業で本専攻所属ではなくなった場合、適時DBから削除する予定である。

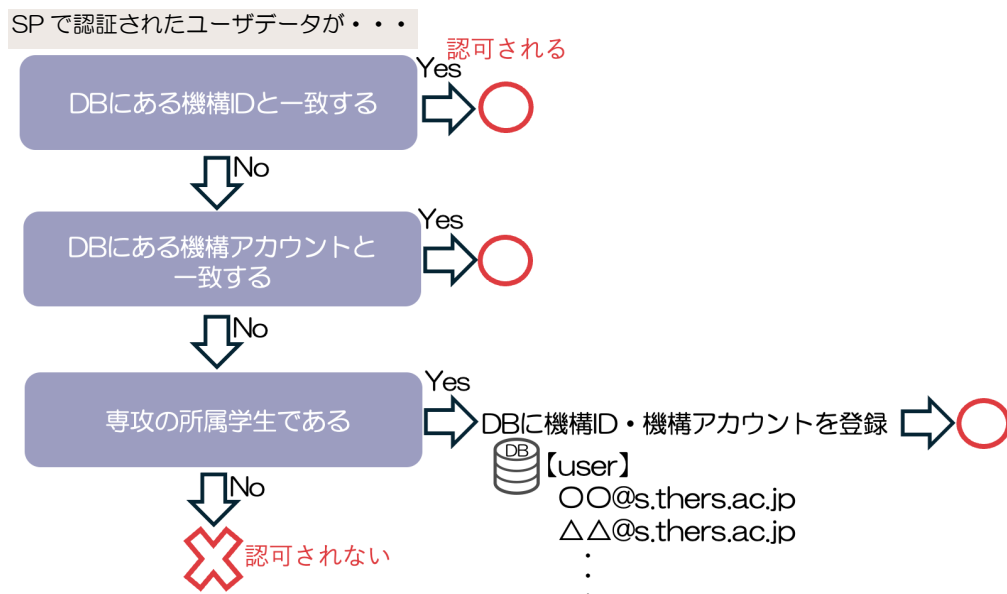


図10. 認可の条件

3 まとめ

専攻 Web アプリの再開発を通して、機構統合認証を実装した Web アプリの構築方法を理解することができた。認可について、認証後に得られたユーザデータをどのように扱う実装がよいかの調査・検証に時間がかかった。今後、機構統合認証を用いた Web アプリを開発する際、今回の知識を役立てていきたいと思う。

参考文献

- [1] laravel-shibboleth <https://bitbucket.org/dpazuic/laravel-shibboleth/src/master/>
- [2] 青木 学聡, “「法人統合がもたらす大学情報環境のリノベーション」”, AXIES 教育技術開発部会 第17回研究会, 2023年8月, https://edtech.axies.jp/_media/sites/16/2023/09/17-2-2.Aoki_.pdf