Vol.2012-IOT-18 No.1
2012/6/28

教育向けWebアプリケーションのためのShibbolethを用いた学務情報のセキュアな伝達方法の提案

足立 紘亮[1,a)]　寺門 卓馬[2]　國宗 永佳[3]　新村 正明[2]

概要：Web 技術の向上や e-learning の普及に伴い，大学の各授業で Web アプリケーションを利用する機会が増えている．また，アプリケーションごとに，利用者の身分や学部等によってアクセス制限や利用権限を与える為には，学務の履修情報を用いた認可が必要となる．しかし，セキュリティ上その情報へのアクセス可能範囲は制限されている場合が多い．そこで本稿では，Shibboleth を用いた学務情報のセキュアな伝達方法の提案とその利用例について述べる．

キーワード：シボレス，e ラーニング，セキュリティ，クラウドサービス

Proposal of the secure method that transfers academic data using Shibboleth for educational web applications

Kosuke Adachi[1,a)]　Takuma Terakado[2]　Hisayoshi Kunimune[3]　Masaaki Niimura[2]

Abstract: Along with the the popularization of e-learning and improvement of web technology, teachers starting to use web applications for their classes. Each applications are able to control accesses and give roles to user based on academic data, but not all of applications are able to because it is heavily-secured data. In this paper, we propose the secure method that transfers academic data using Shibboleth for educational web applications.

Keywords: Shibboleth, e-Learning, Security, Cloud service

1. はじめに

近年，Web 技術の向上に伴い Web アプリケーションを利用した学習支援システムが大学の授業に組み込まれる機会が増えている．またその利用形態は，予習や復習に利用されるものや，授業内で講義と合わせて利用するブレンディッドラーニング等様々である．学習支援システムとしては Learning Management System(LMS) や Course Management System(CMS) 等が世界的に広く利用されており，代表例として Moodle[1]，Blackboard Learn[2]，Sakai[3] 等が存在する．

信州大学においても，2008 年度より Moodle を利用した e-Learning を行われている．さらに，機能性や操作性の観点から単一の学習支援システムだけでは大学内の様々な講義形態に対応できないと判断し，複数の教育支援システムを統合的に管理・運用する為の教育基盤システム「eALPS」を開発し運用を行なっている [4]．

eALPS では学務情報を利用することにより，各授業に合わせた教育支援システムの提供を可能としているが，セキュリティポリシーにより学務情報へのアクセス可能な範囲は制限されている．このことから，システム運用が可能なネットワークが制限される為，クラウドサービス等を利用した柔軟なシステム構成が行えず，開発や運用に関わる

[1] 信州大学大学院工学系研究科
Graduate School of Science and Technology, Shinshu University
[2] 信州大学大学院理工学系研究科
Division of Science and Technology, Shinshu University
[3] 信州大学工学部
Faculty of Engineering, Shinshu University
[a)] adachi@seclab.shinshu-u.ac.jp

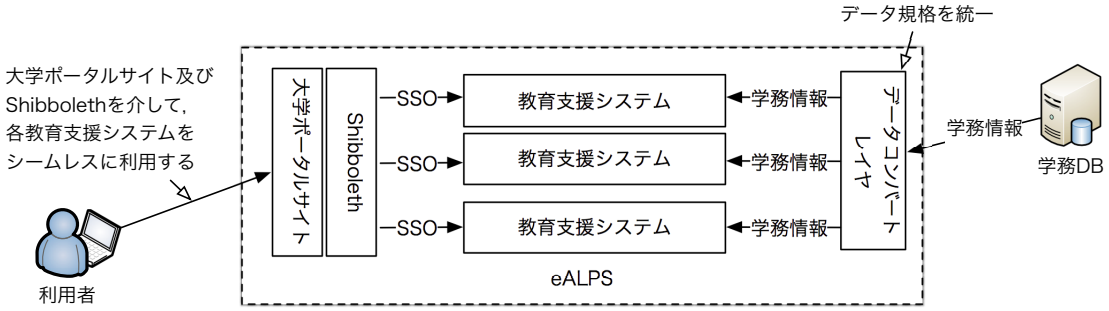

図 1 eALPS のシステム構造
Fig. 1 Structure of eALPS

コストの増加や可用性の確保が困難になる等の問題を招いている．

本稿では，この問題に関する解決策として，Shibboleth[5] を用いた学務情報のセキュアな伝達方法を提案し，その利用例について述べる．

2. 教育基盤システム 「eALPS」

eALPS は疎結合による各教育支援システムの統合的な管理・運用を実現している．ここで疎結合とは，各システムが持つ様々な規格の差を吸収する事で，システム間の独立性を保ったまま情報の共有を実現する手法である．

図 1 に eALPS の構成図を示す．各システムでは授業の開講情報や履修登録情報，学生や教員の身分情報等の学務情報を利用することで，利用者に対する学部や学科，身分等を考慮した権限の付与や，履修登録情報に基づいたシステムへの自動利用登録等を実現している．これにより利用者は自ら利用登録することなく，適切な利用権限の基で各システムを利用することが可能となる．

また各システムは互いに独立している為，学務情報の取り扱い方は様々である．そこで eALPS では各システムの疎結合を実現する為に，学務情報をシステムへ伝達する際，データ構造を変換するデータコンバートレイヤを用いて各システムの規格の差を吸収している．ここでデータコンバートレイヤとは，データの変換及び転送を行うレイヤであり，各システムに合わせたスクリプト群で構成されている．

更に eALPS では，Shibboleth を用いて統合認証基盤を構築しており，各システムへのシングルサインオンや学術認証フェデレーション (GakuNin)[6] への参加を実現している．

3. eALPS が抱える問題

図 2 は eALPS と学務データベースとのネットワーク上の関係を簡易的に表したものである．なお実際のネットワーク構成とは異なる為，本稿ではネットワークの構成例として掲載している．

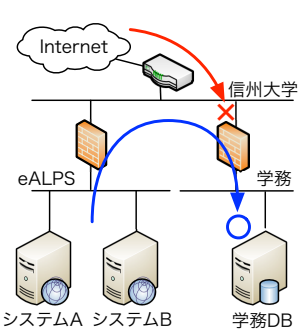

図 2 ネットワーク構成例 1
Fig. 2 Example network 1

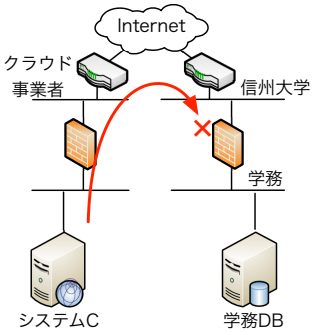

図 3 ネットワーク構成例 2
Fig. 3 Example network 2

現在 eALPS 上で管理・運用しているシステムは全て eALPS ネットワーク上に存在しており，また学務情報が格納されているデータベース (学務 DB) は学務ネットワーク上に存在している．そしてセキュリティポリシー上，学務 DB へのアクセスは，学務ネットワークのファイアウォールによって eALPS ネットワークからのみに制限されている．

ここで開発及び運用コストの削減や可用性の確保等の為に，Infrastructure as a Service(IaaS) や Platform as a service(PaaS) といったクラウドサービスを利用しようとした場合 (**図 3**)，eALPS ネットワーク外から学務 DB へアクセスすることは出来ない為，それらのサービスは学務情報を利用することは不可能である．さらに別のネットワーク上でシステムを運用する必要がある場合も同様である．

この様にネットワーク構成やセキュリティポリシーによって，学務情報へのアクセス可能な範囲が制限される為，システムを運用する環境が制限される．よって柔軟なシステム構成が行えず，開発や運用に関わるコストの増加や可用性の確保が困難になる等の問題を招いている．

4. 解決手法の提案

4.1 学務情報へのアクセス可能範囲の拡張について

3 の問題は，セキュリティポリシーを緩和し，学務情報のアクセス可能範囲を拡張することによって解決する．図 3 の場合，システム C が持つ IP や FQDN からのアクセスを学務ネットワークのファイアウォールが許可すれば，ク

ラウドサービス等を利用した柔軟なシステム構成が可能となる．

しかしアクセス可能な範囲の拡張は，不正アクセス等の対象を広げる事となり，学務情報が外部に漏洩してしまう危険性が高まる．特に学務情報は重要な個人情報である為，外部への公開及び漏洩は避けなければならず，不正アクセスの検知及び防止，セキュアな通信経路の確保等の堅牢なシステム構築が必要となる．

さらに，アクセス可能な範囲を拡張する為には，学務ネットワークのファイアウォールの設定をサービスごと個別に変更する必要がある．その為対象となるシステムが増加する事によって，ファイアウォールの管理が困難になると考えられる．

この様に，アクセス可能範囲を拡張する場合は，より堅牢なシステム構築やファイアウォールの設定変更等が必要となる為，eALPS 全体の構築や運用に関わるコストが増大する．

4.2 Shibboleth を用いた情報伝達方法の提案

Shibboleth では，認証処理を行う Identity Provider(IdP) とサービスの提供を制御する Service Provider(SP) により，認証基盤を構築する．また，Security Assertion Markup Language(SAML) を用いることで，認証情報及び認可情報のセキュアな交換を行い，シングルサインオンを実現している．

Shibboleth の認証及び情報伝達について**図 4** を用いて説明する．ここで，User DB とはユーザの認証情報が格納されているデータベースである．

(1) SP へアクセスする．
(2) 未認証の場合，IdP へリダイレクトされる．
(3) IdP は認証画面を表示し，ユーザから ID とパスワードを受取り，認証処理を行う．
(4) 認証が完了すると，SP へリダイレクトされる．この際，認可情報を伝達する．
(5) SP は認可情報に基づいてページを表示する．

認証が済んでいる場合は (3) の処理が省略され，SP へのシングルサインオンが実現される．

図 5 は Shibboleth の構成要素と図 2 及び図 3 を含めたネットワーク構成図である．なお，各サービスを提供している Web サーバには SP が組み込まれているものとし，学務 DB はユーザの認証情報を取扱う User DB としての役割を担うものとする．また，学務情報へのアクセスは eALPS ネットワークからのみ可能であるものとする．

ここでシステム C への学務情報の伝達は以下のように行われる．

(1) ユーザがシステム C(SP) へアクセスする．
(2) 未認証の場合，IdP へリダイレクトされる．
(3) IdP は認証画面を表示し，ユーザから ID とパスワードを受取り，UserDB を利用し認証処理を行う．
(4) 認証が完了すると，システム C(SP) へリダイレクトされる．この際，学務 DB から学務情報を取得しシステム C へと伝達する．

この様に，学務情報は利用者の認証時に伝達される．

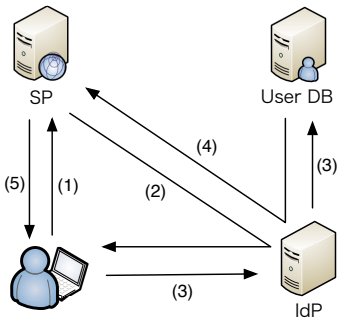

図 4 Shibboleth による認証と情報伝達
Fig. 4 Authentication and data transfer by using Shibboleth

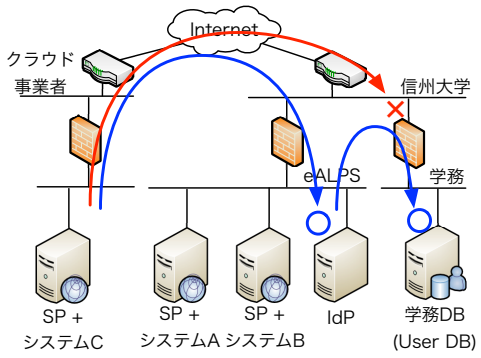

図 5 Shibboleth を含めたネットワーク構成例
Fig. 5 Example network including Shibboleth

この手法を用いる事によって，セキュリティポリシーを変更することなく eALPS 以外のネットワークへ学務情報をセキュアに伝達することが可能となる．さらに，この手法は各システムの Shibboleth 対応のみで実現可能である為，開発コストを抑えることが可能である．

4.3 本提案手法の eALPS への適用

提案手法を取り入れた際の eALPS の構造は**図 6** の様に変更される．主な変更点は Shibboleth による学務情報の伝達とデータコンバートレイヤの配置場所である．提案手法では学務情報を Shibboleth(IdP) に渡す必要がある為，データコンバートレイヤが IdP と学務 DB の間に入る構造となる．また，IdP には伝達する情報を各 SP に対して取捨選択する機能があり，データコンバートレイヤから渡される情報を適切な SP へと伝達するよう設定している．

5. 提案手法の利用例

提案手法の利用例として，Moodle への自動履修登録方法

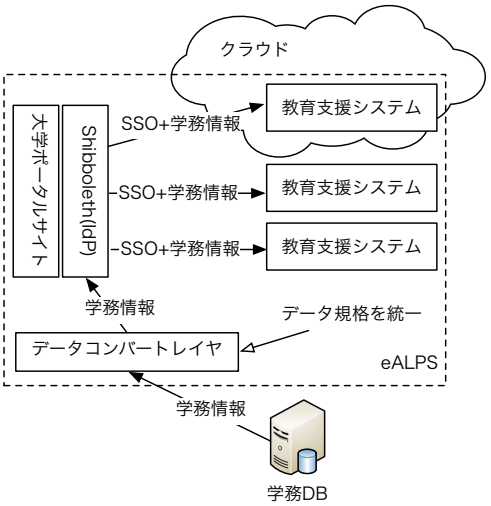

図 6 eALPS の新システム構造
Fig. 6 New structure of eALPS

表 1 伝達する学務情報
Table 1 Transferring academic data

	参照 ID	説明
履修登録情報	stRegCode	学生権限で登録する授業コード
	teRegCode	教員権限で登録する授業コード
	taRegCode	TA 権限で登録するコード

について説明する．本例では 図 5 の様なネットワーク構成を想定しており，Moodle はクラウド事業者ネットワーク上のマシンにインストールされているものとする．なお検証した Moodle のバージョンは 2.1 である．また，Moodle が動作している Web サーバには既に SP がインストールされており，適切な設定が施されているものとする．

5.1 自動履修登録の手順

バージョン 2.0 以降の Moodle には自動履修登録用のプラグインが予め用意されており，LDAP サーバや DB サーバ等から履修登録情報を取得し，Moodle 内のコース情報と同期する．なお，伝達される情報は**表 1** のとおりである．

履修登録情報は Moodle のロール (利用権限) ごとに分けられており，利用者が Moodle へログインする際に情報が伝達し，自動的に履修登録される．例えば，”ネットワーク”と”データベース”を履修しており，”プログラミング言語”の TA を行なっている学生が Moodle へログインすると，stRegCode として”ネットワーク, データベース”，taRegCode として”プログラミング言語”という情報が伝達される．Moodle はこの伝達された情報を基に，学生権限又は TA 権限を付加して履修登録を行う．

しかし，学務 DB はクラウド事業者ネットワークからはアクセス出来ない為，提案手法を用いて履修登録情報を伝達する．

5.2 自動履修登録プラグインの開発

Moodle には Shibboleth から伝達される情報を基に自動履修登録を行うプラグインは存在しない．しかし，Shibboleth から伝達される情報は，環境変数として保存される為，既存のプラグインからの参照は容易である．そこで，既存のプラグイン内の LDAP サーバへ問い合わせる箇所を環境変数への参照に変更することで 5.1 の動作を実現した．

6. おわりに

本稿では学務 DB のアクセス可能範囲を拡張することなく，範囲外のネットワークに対してセキュアに学務情報を伝達する手法を提案した．この手法を利用することにより，クラウドサービスを利用した開発及びコストの削減や可用性の確保等の柔軟なシステム構成が可能となる．今後はこの手法を利用した教育支援システムの開発を進めることで，eALPS のコンテンツの充実を目指す．

参考文献

[1] Moodle.org: About(online)，入手先 ⟨http://moodle.org/about/⟩ (2012.06.05).
[2] Blackboard: Blackboard Learn — Accelerate Online Learning with the Blackboard Learn Platform(online)，入手先 ⟨http://www.blackboard.com/Platforms/Learn/Products/Blackboard-Learn.aspx⟩ (2012.06.05).
[3] Sakai Project: About Sakai — Sakai Project(online)，入手先 ⟨http://www.sakaiproject.org/about-sakai⟩ (2012.06.05).
[4] 五月女雄一，鈴木彦文，新村正明：学習者データの交換による教育支援システムの疎結合で構成される教育基盤システム「eALPS2.0」，情報処理学会研究グループ報告，第 10 回 CMS 研究発表会，pp.1-4，(2008).
[5] Internet2: Shibboleth - About(online)，入手先 ⟨http://shibboleth.net/about/index.html⟩ (2012.06.05).
[6] 国立情報学研究所: 学術認証フェデレーション学認 GakuNin — プロジェクト概要 — Shibboleth — 学術認証フェデレーション，入手先 ⟨https://www.gakunin.jp/docs/fed⟩ (2012.06.05).