Vol.2009-IOT-5 No.6
2009/5/28

ポータルサイトの強制表示とシングルサインオン

大谷 誠[†1] 江藤博文[†1] 渡辺健次[†2]
只木進一[†1] 渡辺義明[†2]

近年，大学などにおいて，利用者毎の情報提供や，複数の Web 情報システムの連携を行うために，それらのポータルとなるサイトが必要とされるようになってきた．しかしながら，このようなポータルサイトは通常，利用者が能動的に閲覧を行う必要があり，また，大学の全構成員の利用者属性に応じた情報提供を確実に行う手段が無いのが現状である．

そこで，我々は定期的に利用者にポータルサイトを強制的に表示させるシステムを構築した．また，このシステムはシングルサインオンに対応しており，各 Web 情報システムへのゲートウェイとしての機能を果たすことができる．

Forced Display of Portal Site with Single Sign-On

Makoto Otani,[†1] Hirofumi Eto,[†1] Kenzi Watanabe,[†2]
Shin-ichi Taadaki[†1] and Yoshiaki Watanabe[†2]

A portal site is needed for appropriate information services to users, and co-operation of multiple Web information systems, in the university. However, the user needs to visit such a portal site actively. So, there is no means to provide the information appropriate for users certainly.

We developed the system which implements forced display for the portal site to users. This system has single sign-on function. And this system serves as the gateway to each Web information system.

†1 佐賀大学 総合情報基盤センター
Computer and Network Center, Saga University
†2 佐賀大学 理工学部
Faculty of Science and Engineering, Saga University

1. はじめに

近年，大学などにおいて，利用者への情報提供や各種情報サービスを目的とした多種多様な Web 情報システムが運用されるようになってきた．これらの Web 情報システムは用途毎に構築される場合が多く，通常は利用者が用途に応じてそれぞれのシステムにアクセスしなければならない．このため，各システムを利用しやすいようにポータルサイトにまとめるといった，利便性を向上させる取り組みも行われている[1]．

しかしながら，このようなポータルサイトを用いて情報提供を行う場合でも，利用者がポータルサイトへ能動的かつ定期的にアクセスしないと，様々な情報を効果的に提供することはできない．ポータルサイトへアクセスの習慣が身についていない利用者に対しては，情報提供自体が難しい．また，ポータルサイト上で Web 情報システムをまとめて提供しても，各システムを使用するごとに，個別に利用者認証が行われてしまうと，利便性が損なわれる．

そこで我々は，大学の全構成員の利用者属性に応じた情報提供を確実に行う手段として，Web 利用時にポータルサイト定期的かつ強制的に表示させるシステム (以下，ポータルサイト強制表示システム) を構築した．このシステムは，Web を利用する際に認証を行い，その認証情報をもとにしてポータルサイトで利用者の属性情報に応じた情報を提示できる．また，この際の認証はシングルサインオンに対応しており，ポータルサイトからシングルサインオンに対応した Web 情報システムにアクセスした際は再度認証が必要ない．よってこのシステムは，ポータルサイトにおいて利用者に応じた情報を提供するとともに，各 Web 情報システムのゲートウェイとしての機能を果たす．

多くの人が日常的に利用する Web 利用時に認証を行い，大学のポータルサイトを強制的に表示することで，大学からの広報，連絡事項，予定などを表示し，利用者への情報の伝達を円滑に行うことが可能となる．このような情報は，メールを用いた連絡が一般的であるが，本システムでは，必要な情報が強制的にポータルサイトに表示されるため，必要な情報のメールを取捨選択して読む作業が必要なくなる．利用者をポータルサイトに定期的かつ確実に導くことは，組織の情報伝達にとって非常に有効な方法である．本稿では，このポータルサイト強制表示システムについて報告する．

© 2009 Information Processing Society of Japan

Vol.2009-IOT-5 No.6
2009/5/28

2. ポータルサイト強制表示システムに必要な機能とその実現

この章では，ポータルサイトの強制表示に必要な機能と，その実現方法について述べる．

2.1 システムの実現

ポータルサイト強制表示システムを，各 Web 情報システムのゲートウェイシステムとして実現すること考える．利用者が Web を利用しようとする際に，ゲートウェイとなる本システムでシングルサインオン認証を行い，認証成功後に Web への通信路を開くとともにポータルサイトを強制表示し，情報提供を行う．また，一定時間経過後に Web への通信路を閉じ，再度ポータルを強制するための機能，およびシステム利用の際の記録を行う機能も備える．このようなシステムを構築するためには，次に示す機能をそれぞれ実現していく必要がある．

(1) 認証画面を提示する機能
(2) シングルサインオン認証を行う機能
(3) Web 通信の制御を行う機能
(4) 利用者の情報を記録する機能

以下では，上記の機能の実現について述べる．

2.2 認証画面を提示する機能

認証画面を提示する機能ついては，Web サービスで利用する認証であることから，利便性からも Web ブラウザを用いた認証を行う．認証画面の強制的な表示については，ファイアウォールの機能を用いて認証前の Web 通信 (80 番ポート) を奪い取り，代わりにシングルサインオンの認証ページを応答することによって実現する．これについては，次節で述べる．

また，本来表示を行う予定であった Web サイトは，認証終了後にポータルサイトとは別に表示する機能も実現する．

2.3 シングルサインオン認証を行う機能

ポータルサイトや，各 Web 情報システムにシングルサインオンを行うためには，ポータルサイト強制表示システム，ポータルサイト，Web 情報システムそれぞれが，シングルサインオン認証に対応する必要がある．

本システムにおけるシングルサインオンの認証には，Shibboleth を利用することとした[2]．

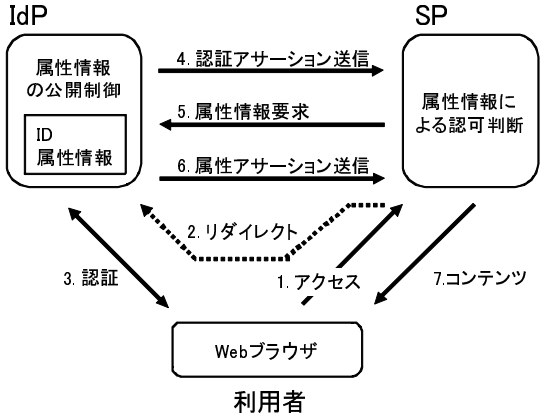

図 1 Shibboleth の動作

この Shibboleth は，Internet2 の教育機関向けプロジェクトである MACE (Middleware Architecture Committee for Education) で開発された SAML ベース (OpenSAML) の認証システムである．Shibboleth は，利用者の認証と利用者の属性を提供する IdP(Identity Provider)，IdP からの属性情報によりサービスを提供する SP(Service Provider)，IdP が複数存在する場合に，IdP のリストを提供する DS(Discovery Service) で構成される．

Shibboleth の動作を**図 1** に示す．利用者は初めに SP 上に構築されたウェブサービスにアクセスする．そのリクエストは，IdP にリダイレクトされ，利用者は IdP において認証を行う．IdP で認証に成功すると，SP に認証アサーション (Assertion) が送信される．SP は IdP にアプリケーション実行に必要な利用者の属性を要求し，IdP は要求された属性アサーションを返す．この属性に基づき SP 上のウェブサービスから利用者にコンテンツが送信される．SP を利用可能な IdP が複数存在する場合，DS が IdP のリストを提供し，利用者はその中から自分が利用する IdP を選択することによって認証を行い，コンテンツにアクセスを行う．

ポータルサイト強制表示システムにおいては，この表示システムが SP として動作するとともに，利用者の Web アクセスやポータルサイトの表示を制御する．利用者の Web アク

© 2009 Information Processing Society of Japan

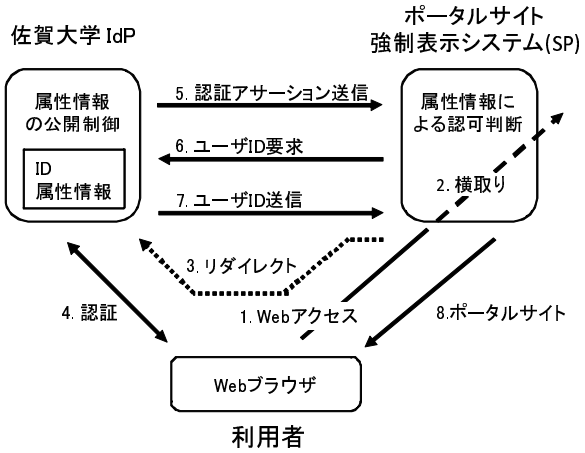

図 2 ポータルサイト強制表示システムの動作

セスを横取り，IdP で認証を行わせ，認証に成功した場合に IdP からの利用者の属性情報をもとに，ポータルサイトの表示を行う (**図 2**)．また，ポータルサイトからリンクされる各 Web 情報システムを，Shibboleth によるシングルサインオンに対応させることで，再認証を行わずに，Web 情報システムの利用が可能とする．

2.4 Web 通信の制御を行う機能

Web 通信の開放については，シングルサインオン認証成功後にファイアウォールによって実現する．これにより，通常どおりに Web 通信を利用できるようになる．

また，一定時間経過後にファイアウォールの機能を用いて Web 通信を閉鎖する．これによって，再度認証ページが表示可能な状態となる．なお，Web 通信以外の通信は，常に通信路を開放し，認証に関係なく利用できるように設定しておく．

2.5 利用者の情報を記録する機能

利用情報として，Shibboleth における IdP および SP の利用ログの他に，syslog によって，ポータルサイト強制表示システムの利用状況を記録する機能を実装する．これにより，利用者のポータルサイトへのアクセス状況を一元的に把握することができる．

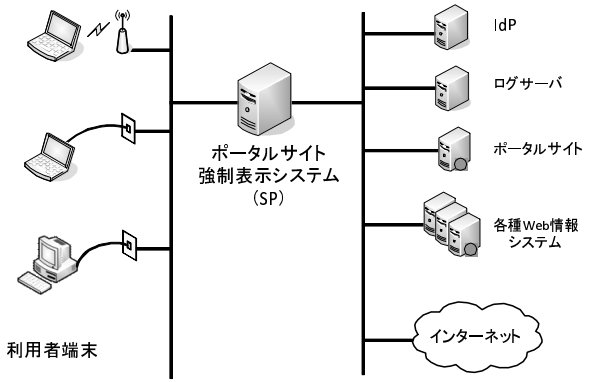

図 3 システム構成

以上のように，ポータルサイト強制表示システムでは，認証ページとポータルサイトの提示に伴う Web 通信制御にはファイアウォールを，シングルサインオンには Shibboleth を，利用者情報の記録には，syslog を用いる．

3. ポータルサイト強制表示システムの概要

この章では，ポータルサイト強制表示システムの構成や，利用者からの利用，システム内部の流れについて述べる．

3.1 構　　成

図 3 にシステム構成を示す．ポータルサイト強制表示システムは，利用者端末のネットワークとの間に，ゲートウェイとなるよう設置し，そこを通過する Web 通信のパケットをファイアウォールで制御することによってポータルサイトを表示するシステムである．利用者の認証は，シングルサイン認証を行うために IdP を用いる．

図 4 にソフトウェア構成を示す．ポータルサイト強制表示システムのソフトウェアは，佐賀大学で開発・運営しているネットワーク利用者認証システムである Opengate をもとにして構築した[3,4]．

ポータルサイト強制表示システムのサーバプログラムは，Web サーバから CGI として起

© 2009 Information Processing Society of Japan

Vol.2009-IOT-5 No.6
2009/5/28

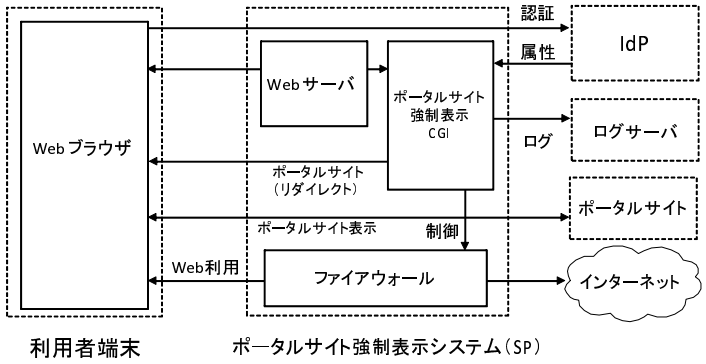

図 4 ソフトウェア構成

動される．利用者の Web ブラウザにポータルサイトを表示するとともに，ポータルサイトの再表示のためのファイアウォールの制御を行う．

ポータルサイト強制表示システムは，FreeBSD 上で構築されており，ファイアウォールの制御には ipfw，Web サーバには Apache を用いている．

3.2 利 用 手 順

ポータルサイト強制表示システムが動作している環境で，ネットワークを利用した際のポータルサイトの表示の利用手順を以下に示す．

(1) 利用者は，Web 以外の通信を特に制限なく利用できる．

(2) 利用者が Web ブラウザを用いて任意の URL へアクセスを行うと，通信が奪い取られ，ユーザ ID とパスワードを要求する認証ページ (**図 5**) が送られてくる．

(3) 利用者は，この認証ページにユーザ ID とパスワードを入力する．

(4) 認証に成功すると，ユーザの属性情報に応じたポータルサイト (**図 6**) の内容が表示されるとともに，(2) で最初にアクセスしようとしていた URL ページも別ウィンドウ (ブラウザの設定によっては，別タブ) で表示される．

(5) 認証成功後，設定時間 (12 時間) が経過するまで，利用者は Web やその他の通信を自由に利用することができる．

(6) 設定時間経過後 (12 時間) に，(1) の動作に戻る．

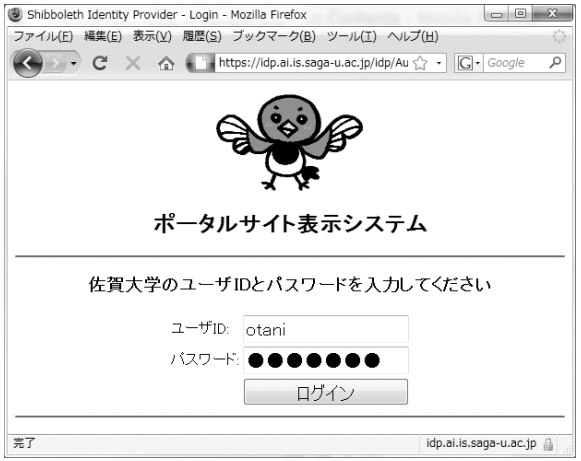

図 5 認証ページ

図 6 ポータルサイト (例)

3.3 システムの動作

利用者が，上で示した手順を行った場合のシステムの基本動作を以下に示す．

(1) Web アクセスのパケットがポータルサイト強制表示システムに届くと，ファイアウォールの ipfw は，ポータルサイトの表示の判断を行い，表示をする場合は，ローカルの

© 2009 Information Processing Society of Japan

Web サーバの HTTP ポートへと forward する．

(2) 利用者が (1) において本来表示予定であった Web サイトの URL を，Web ブラウザの Cookie へ保存する．

(3) ローカルの Web サーバ (SP) は，認証要求を行うため，IdP へ通信をリダイレクトさせる．

(4) 利用者によって，ユーザ ID とパスワードが入力され認証に成功すると，IdP は，認証アサーションを SP に送る．SP は，IdP に属性情報 (ユーザ ID) を要求する．

(5) IdP は，属性情報の応答の可否を判断し，SP へ属性情報 (ユーザ ID) を応答する．

(6) 属性情報を受け取ったポータルサイト強制表示システムは，CGI を起動しファイアウォールで Web 通信を開放するとともに，属性に応じたポータルサイトの内容を表示する．

(7) 上記の (2) で Cookie に保存していた Web サイトをポータルサイトとは別に表示する．

(8) 設定時間経過後 (12 時間) に，CGI が認証後に追加したファイアウォールルールを削除し (1) の動作に戻る．

4. ポータルサイト強制表示システムの各機能

この章では，ポータルサイト強制表示システムの各機能について述べる．

4.1 利用者の認証

ポータルサイト強制表示システムは，Shibboleth による認証を用いるため，システムそのものは，認証に直接関与していない．システムが Shibboleth の SP として動作し，認証の成功した利用者のユーザ ID を Shibboleth に IdP に要求・取得することによってポータルサイトを表示する．また，このポータルサイト強制表示システムは，複数の IdP を利用する必要がある場合でも，設定により Shibboleth の DS(**図 7**) を用いて IdP の選択を行い，認証を行うことが可能である．

4.2 ポータルサイトの強制表示

ポータルサイト表示のための Web 通信の制御は，FreeBSD 標準のパケットフィルタリング型のファイアウォールである ipfw を用いている．ipfw は制御ルールを列挙することで，パケットの送信元，送信先，ポート番号などとルールを比較し，最初に合致したルールに従い，パケットの制御を行う．

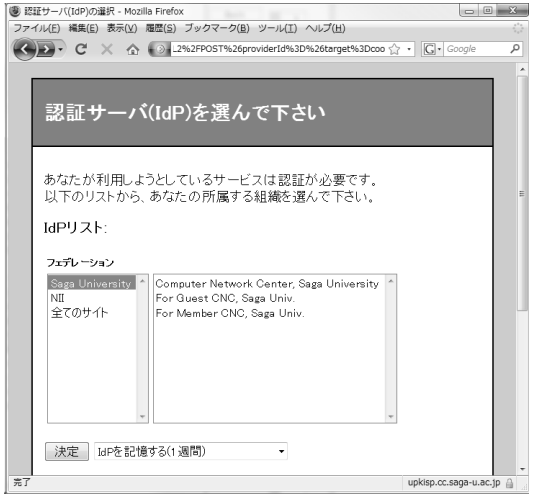

図 7 DS による IdP の選択

制御ルールの最後尾には全て許可のルールを置き，ポータルサイトの表示のための HTTP に対する IP Forward ルールをそれより優先順位の高い位置に置いておく．認証成功後に CGI が追加するアクセス許可のルールを，これらよりさらに優先順位の高い位置に置くことで，認証後に Web アクセスも通常どおり利用可能としている．設定時経過後に CGI が追加したファイアウォールルールを削除することにより，再度ポータルサイトの強制表示が可能な状態となる．ポータルサイトを表示してから再度ポータルサイトを表示するまでの時間は設定により柔軟に変更することが可能である．

最上位のルールとして，通過や拒否のルールを書くことで，常に開放もしくは閉鎖状態に置くサービスを指定することもできる．また，認証成功後に CGI が追加するルールより優先順位の低い拒否ルールを設置することで，認証成功後に初めて利用可能とするサービスも細かく指定できる．このように，ファイアウォールのルールをカスタマイズすることによって，細かな通信の制御も可能である．

4.3 利用者情報の記録

ポータルサイト強制表示システムは，ポータルサイト表示の際に，利用者のユーザ ID，利

© 2009 Information Processing Society of Japan

用者端末の IP アドレス，Mac アドレス，利用開始時刻を syslog の機能を用いて記録する．また，Web 通信の閉鎖の際は，上記の情報に加えて，その情報も記録する．また，Shibboleth における IdP での認証，SP の利用状況などは，別途 Shibboleth の利用履歴として保存される．

なお，Mac アドレスはポータルサイト強制表示システムから把握できる Mac アドレスであり，ルータ配下からの利用の場合は，ルータの Mac アドレスとなる．

5. 考察と課題

この章では，ポータルサイト強制表示システムの課題や考察について述べる．

5.1 スケーラビリティ

このポータルサイト強制表示システムの目的は，多くの人が日常的に利用する Web 利用時に認証を行い，ポータルサイトを強制的に表示することで利用者毎の情報伝達を円滑に行うことである．よって，大学の全構成員が利用することが想定される．たとえば佐賀大学の全構成員は約 1 万人であり，この利用規模においても，ポータルサイト強制表示システム，ポータルサイト，認証を行う IdP それぞれが，負荷なく利用できる必要がある．

5.2 ポータルサイトによる情報提供

このシステムは，大学のポータルサイトを強制的に表示し，そこで大学からの広報，連絡事項，予定など，利用者毎の情報を提供する．このため，このポータルサイトに，利用者毎に伝達するための情報を登録していく必要がある．これらの登録手段や，効率的は表示のさせ方，運用体制などについては，別途検討の必要がある．

5.3 Web 情報システムのシングルサインオン対応

大学内には既存の Web 情報システムが多数ある．また，大学に次々の新しい Web 情報システムが発生する．これらをシングルサインオン対応にし，ポータルサイトと結びつけることで，利用者の利便性が向上するとともに，シングルサインオン環境及びそれと連携したポータルサイトの価値が向上する．よって，今後情報システムをシングルサインオン対応とするための，手順の整理や支援体制の構築が必要である．既存の情報システムの中には，シングルサインオン対応が困難なものがあると思われる．このようなシステムのために，擬似的なシングルサインオン等を検討する必要がある．

5.4 シングルログインとログアウト

Shibboleth は SAML ベースのシングルサインオンソフトウェアである．SAML には，特定のサービスのログアウトで，シングルサインオンしている全てのサービスからログアウトするシングルログアウトの仕様がある．しかし，現在のところ，Shibboleth はシングルログアウトに対応していない．Web ブラウザを終了した際に，シングルサインオン時に認証で利用した Cookie を開放することで，簡易的なログアウトを実現している．

また，ポータルサイト強制表示システムでは，ポータルサイトの表示にはファイアウォールを用い，認証には Shibbleth を用いている．よって，ポータルサイトの表示間隔と，再認証を行わせるタイミングを個別に制御することも可能である．このような適切なポータルサイトの表示間隔や認証のタイミングは，運用しながら柔軟に決定していく必要があると思われる．

6. ま と め

大学の全構成員の利用者属性に応じた情報提供を確実に行う手段として，Web 利用時にポータルサイト定期的かつ強制的に表示させるシステムを構築した．多くの人が日常的に利用する Web 利用時に認証を行い，大学のポータルサイトを強制的に表示することで，大学からの広報，連絡事項，予定などを表示し，利用者への情報の伝達を円滑に行うことが可能となる．利用者をポータルサイトに定期的かつ確実に導くことは，組織の情報伝達にとって非常に有効な方法である．

参 考 文 献

1) 梶田将司, 内藤久資, 平野靖, 瀬川午直, 小尻智子, 間瀬健二, 名古屋大学ポータルによる情報サービスの統合と課題, 情報処理学会研究報告. DSM, [分散システム/インターネット運用技術], Vol.2007,No.72 (2007)
2) Shibboleth, http://shibboleth.internet2.edu/
3) Opengate とシングルサインオン，江藤博文，大谷誠，渡辺健次，只木進一，情報処理学会研究報告,2009-IOT-4,pp.259-264 (2009).
4) HTTP コネクションの監視により利用終了検知を行うネットワーク利用者認証システムの開発とその円滑な導入，大谷誠，江藤博文，渡辺健次，只木進一，渡辺義明，情報処理学会論文誌，Vol.50, No.3, pp.1032-1042 (2009)

© 2009 Information Processing Society of Japan