Shibboleth と OpenAM の連携による 認証レベルを考慮した統合認証システムの構築

河野 圭太 [1)], 稗田 隆 [1)], 中村 素典 [2)]

1) 岡山大学 情報統括センター
2) 国立情報学研究所
keita@cc.okayama-u.ac.jp

Construction of Integrated Authentication System Considering Authentication Levels with Cooperation between Shibboleth and OpenAM

Keita Kawano[1)], Takashi Hieda[1)], Motonori Nakamura[2)]

1) Center for Information Technology and Management, Okayama University
2) National Institute of Informatics

概要：岡山大学では，2016 年 3 月に統合認証システムを更改した．新システムでも，旧システムと同様に，Shibboleth を中心とした認証連携を推進することにしたが，新システムでは，安全性強化のため，ID・パスワードによる認証に加えて，ワンタイムパスワードによる認証を要求できることが求められた．ただし，これを常に強制することは，利用者の利便性低下につながる恐れがあるため，サービスの管理者または利用者が必要とする場合にのみ，追加の認証として実行されることが望ましいと考えた．岡山大学では，Shibboleth の認証を OpenAM と連携させることにより，これを実現するシステムを構築したので報告する．

1　はじめに

近年，シングルサインオンの実現による利用者の利便性向上と，認証機能の一元化によるシステムの安全性向上を目的として，各組織において，統合認証システムの整備が進んでいる．とりわけ，大学等の高等教育機関においては，学術認証フェデレーション（日本では「学認」）との親和性を考慮し，Shibboleth を用いた統合認証システムの構築事例が多数報告されている[1],[2].

岡山大学でも，以前より，Shibboleth を中心とした認証連携を推進してきたが, 2016 年 3 月に教育・研究支援情報システムの一部として更改した新システムにおいても，これを継続することにした[3]．ただし，旧システムでは，Shibboleth 自体の認証として，ID・パスワードによる認証しか提供しておらず，高い安全性が求められるサービスでの利用に問題があった．そこで，新システムでは，より強固な認証を提供できることが求められた．

しかしながら，利用するサービスに関わらず，常に強固な認証を要求することは，利用者の利便性を低下させることにつながりやすい．そこで，岡山大学では，サービスの管理者または利用者が必要とする場合にのみ，追加の認証が実行されることが望ましいと考えた．これを実現するため，「常に ID・パスワード認証のみ」,「学外からは追加の認証を必須」,「学内からも追加の認証を必須」の 3 レベル（以降, 認証レベルと呼ぶ）を定義し，サービスごと，利用者ごとに必要な認証レベルを選択できるようにした．

岡山大学では, Shibboleth の認証を OpenAM と連携させることにより，これを実現するシステムを構築したので報告する．

2　関連技術

Shibboleth は複数の組織間で安全な認証連携・属性交換を実現するためのオープンソースソフトウェアであり，学認を含む多くの学術認証フェデレーションで利用されている．Shibboleth IdP V2 は 2016 年 7 月 31 日に EoL を迎え，全てのサポートを終了したため，多くの組織において，Shibboleth IdP V2 から Shibboleth IdP V3 への

移行が行われた．岡山大学でも，システムの更改に合わせて，Shibboleth IdP V2 から Shibboleth IdP V3 への移行を行った．

Shibboleth IdP V3 では，Shibboleth IdP V2 と比較して，認証コンテキストに関する処理が高度化されたため，Shibboleth IdP V3 の機能を利用して 3 段階の認証レベルによる運用を実現することも検討した[4]．しかしながら，標準の機能だけでは学内からの利用と学外からの利用で認証の方式を変更できないことが問題となった．また，Shibboleth IdP V2 では，同様の機能を提供するプラグインが存在していたが，Shibboleth IdP V3 への対応が不透明であり，採用できなかった[5]．

OpenAM も Shibboleth と同様に，Web シングルサインオンを実現するためのソフトウェアである．岡山大学では，以前より，幾つかのサービスに対して，リバースプロキシ方式によるシングルサインオンを提供していたため，新システムでも，リバースプロキシサーバに OpenAM エージェントを導入し，この運用を継続することにした．OpenAM は Shibboleth と同様に SAML による認証連携を実現できることに加えて，OpenID Connect にも対応するなど，新技術への即座な対応も期待した．

Shibboleth と OpenAM の連携は，これまでにも幾つかの組織で実施されている[6]．しかしながら，これらは Shibboleth IdP V2 に関するものであり，また，本報告のように，サービスごと，利用者ごとに異なる認証レベルを考慮したものではない．

3　認証レベルを考慮した統合認証システムの構築

3.1 認証レベルの考慮

統合認証システムの利用により，様々なサービスの認証を統合できる．これらのサービスの中には，保有する情報資産の機密性が高く，高い安全性が求められるものも存在し得るため，統合認証システムにおいて，強固な認証を実行できることが要求される．しかしながら，一般的に，強固な認証を実現する仕組みの多くは煩雑な運用を必要とするため，常にこれを利用者に強制することは，利便性の低下につながる恐れがある．

そのため，身元保証レベル（Level of Assurance：LoA）という概念の下，利用するサービスごとに認証の方式を変更する方法が確立されつつある[7]．利用するサービスが保有する情報資産の機密性に応じて，適切に複数の認証方式を使い分けることにより，著しい利便性の低下を招くことなく，必要な安全性を確保できる．

岡山大学でも，表 1 に示すような 3 段階の認証レベルを定義し，サービスごとに選択できるようにした．レベル 1 は従来と同様に，学内・学外からの利用に関わらず，常に ID・パスワード認証を要求するもの，レベル 2 は学外からの利用に関しては追加の認証を要求するもの，レベル 3 は学内からの利用に関しても追加の認証を要求するものとした．また，これらのレベル選択は，サービスの管理者だけでなく，サービスの利用者が選択できることも重要と考え，利用者によるレベルの選択も実現することにした．これにより，セキュリティ意識の高い利用者が，自発的に認証レベルを高めることを期待した．

表 1　認証レベルの定義

レベル	内容
1	常にID・パスワード認証のみ
2	学外からは追加の認証を必須
3	学内からも追加の認証を必須

3.2 ワンタイムパスワード認証の利用

前節で示したように，レベル 2，レベル 3 の認証では，従来の ID・パスワードによる認証に加えて，追加の認証を要求することにした．この追加の認証には，モバイルアプリまたは電子メールを利用したワンタイムパスワード認証を採用した．追加の認証による運用を軌道に乗せるためには，簡単な手続きで利用できることに加えて，この仕組みを利用できない利用者を作らないことが重要と考え，2 種類の方法を選択できるようにした．

3.3 Shibboleth と OpenAM の連携

前述したように，岡山大学では，以前より，幾つかのサービスに対して，リバースプロキシ方式によるシングルサインオンを提供していた．しかしながら，Shibboleth によるシングルサインオンとは独立したシステムとして構成されており，運用上の課題となっていた．新システムでも OpenAM と連携したリバースプロキシサーバの導入により，このサービスを継続することにしたが，2 つのシステム間の認証を連携し，利用者に対しては，統

一したシングルサインオンサービスとして提供することが求められた.

これを実現する方法として，OpenAM に Shibboleth SP を導入し，Shibboleth IdP の認証でシステムを統一する方法と，Shibboleth IdP に OpenAM のエージェントを導入し，OpenAM の認証でシステムを統一する方法が考えられたが，OpenAM では，標準の機能により，岡山大学が必要とする 3 種類の認証レベルを用いた運用を実現できたため，後者の方法を採用した.

Shibboleth IdP では，RemoteUser ログインフローや，External ログインフローを用いて，Shibboleth 自体の認証に外部システムの認証を利用できる．今回は RemoteUser ログインフローを利用し，Shibboleth 自体の認証を OpenAM で実行できるようにした. 具体的には, RemoteUser ログインフローに該当する URL を OpenAM エージェントの保護対象に設定し，OpenAM で未認証であれば，OpenAM の認証画面へリダイレクトされるように設定した.

ただし，単純に 1 つの RemoteUser ログインフローを定義し，OpenAM エージェントの保護対象とするだけでは, OpenAM からは Shibboleth IdP と連携するサービス群が 1 つの巨大なサービスとして見えてしまい，サービスごとに認証レベルを選択する運用ができない．そこで，表 2 に示すように，Shibboleth IdP において RemoteUser ログインフロー（に該当する URL）を認証レベルごとに用意し，OpenAM 側では接続元 IP アドレスと対象 URL によって, 制御を変更するようにした.

表 2　認証レベルと URL の紐づけ

レベル	URL
1	/idp/Authn/OUL1
2	/idp/Authn/OUL2
3	/idp/Authn/OUL3

また，これらのログインフローごとに，異なる AuthnContextClassRef を定義し，サービス側の設定で要求する認証レベルを変更できるようにした. ただし, 実際には, サービス側の設定変更は歓迎されないことが多いため，サービス管理者の依頼を受けて，Shibboleth IdP 側の設定を変更し，これを実施することを基本とする予定である.

3.4 OpenAM 認証レベルとの紐づけ

OpenAM では，複数の認証モジュールを定義でき, モジュールごとに認証レベル（以降, OpenAM 認証レベルと呼ぶ）を設定できる．また，接続元 IP アドレスと対象 URL ごとに認可条件を設定でき，基本の認証で必要な認可条件を満たせなければ，追加の認証を求めることができる.

そこで，ID・パスワード認証を OpenAM 認証レベル 0，モバイルアプリによるワンタイムパスワード認証と電子メールによるワンタイムパスワード認証を共に OpenAM 認証レベル 3 に設定し，サービスごとの認証レベル（以降，岡山大学認証レベルと呼ぶ）との間で，表 3 に示すような紐づけを行った．岡山大学認証レベル 1 および学内からの岡山大学認証レベル 2 のサービス利用に関しては OpenAM 認証レベル 0 を，学外からの岡山大学認証レベル 2 および岡山大学認証レベル 3 のサービス利用に関しては OpenAM 認証レベル 3 を認可条件とした．これにより，サービスの管理者の要求による認証レベルの選択を実現できるようになった.

表 3　認可条件の設定

岡山大学認証レベル	アクセス元	認可条件（OpenAM認証レベル）
1（ID・パスのみ）	学内	0
	学外	0
2（学外から追加）	学内	0
	学外	3
3（学内も追加）	学内	3
	学外	3

次に，利用者の要求による認証レベルの選択を実現するため, 上述の設定に対して, 設定の追加, 変更を行った．まず，認証モジュールとして，LDAP 上の属性に応じて認証成否を制御できるアダプティブリスク認証を追加した．ここでは，LDAP 上に「利用者が常にレベル 2 以上の認証を要求するかどうか」を示す属性を用意し,「要求しない」場合に OpenAM 認証レベル 2 が獲得できるようにした．この認証と ID・パスワード認証を認証連鎖という機能を用いて逐次的に実行させ，ID・パスワードによる基本認証の成功後に，利用者が獲得する OpenAM 認証レベルを制御できるようにした．すなわち，ID・パスワード認証に成功した利用者が常にレベル 2 以上の認証を要求している場合には OpenAM 認証レベル 0，常にレベ

ル 2 以上の認証を要求していない場合には OpenAM 認証レベル 2 を獲得できるようにした.

これと共に，表 3 に示した紐づけを表 4 に示すように変更し，学外から岡山大学認証レベル 1 のサービスを利用する場合の認証を制御できるようにした．これにより，常にレベル 2 以上の認証を要求しない利用者はアダプティブリスク認証で獲得した OpenAM 認証レベル 2 で認証を終えることができる一方で，常にレベル 2 以上の認証を要求する利用者には追加の認証としてワンタイムパスワード認証を求める運用ができるようになった.

表 4　認可条件の設定（変更後）

岡山大学認証レベル	アクセス元	認可条件（OpenAM認証レベル）
1（ID・パスのみ）	学内	0
	学外	2
2（学外から追加）	学内	0
	学外	3
3（学内も追加）	学内	3
	学外	3

なお，LDAP 上の「利用者が常にレベル 2 以上の認証を要求するかどうか」を示す属性は，岡山大学における認証情報を一元的に管理する統合認証管理システムにおいて，ワンタイムパスワード認証に関する情報と共に，利用者自身で制御できるようにした.

4　おわりに

本研究では，Shibboleth の認証を OpenAM と連携させることにより，サービスごと，利用者ごとに認証レベルを選択できるシステムを構築した.

現在，システム移行に伴う運用上の都合により，本機能の実運用には至っていないが，今後は，これを早急に実施し，実運用に伴う課題を明らかにする予定である.

謝辞

本研究の一部は JSPS 科研費 26330158 の助成を受けたものである.

本システムの構築に多大なるご尽力を賜ったオープンソース・ソリューション・テクノロジ株式会社，株式会社ハイエレコン，株式会社日立製作所各位に厚く御礼申し上げます.

参考文献

[1] 只木進一，江藤博文，大谷誠，渡辺健次：認証基盤の効率化と「学認」への対応，情報処理学会研究報告，Vol.2012-IOT-17，No.10 (2012).

[2] 松平拓也，笠原禎也，高田良宏，東昭孝，二木恵，森祥寛：大学における Shibboleth を利用した統合認証基盤の構築，情報処理学会論文誌，Vol.52，No.2, pp.703-713 (2011).

[3] 河野圭太，藤原崇起，大隅淑弘，岡山聖彦，山井成良，稗田隆：岡山大学における生涯 ID を実現する統合認証システムの構築，学術情報処理研究，No.15, pp.171-175 (2011).

[4] Shibboleth Consotium: Configuring the IdP for the Multi-Context Broker Model - Identity Provider 3 – Confluence (online), available from <https://wiki.shibboleth.net/confluence/display/IDP30/Configuring+the+IdP+for+the+Multi-Context+Broker+Model> (accessed 2016-08-04).

[5] 松平拓也：Shibboleth 用多要素認証導入のための技術ガイド (online)，入手先 <https://www.gakunin.jp/?action=pages_view_main&active_action=repository_view_main_item_detail&item_id=227&item_no=1&page_id=85&block_id=227> (参照 2016-08-04).

[6] 中國真教：Shibboleth と OpenAM を組み合わせたハイブリッド型シングルサインオン認証基盤の構築, 第 6 回統合認証シンポジウム, pp.77-96 (2012).

[7] Chehab, M.I. and Abdallah, A.E.: Assurance in Identity Management Systems, Proc. IAS 2010, pp.216-221 (2010).