学術情報処理研究 No.21
2017年9月

ShibbolethとOpenAMの連携による認証レベルを制御可能なシングルサインオン基盤の構築*

Construction of Single Sign-On Infrastructure Capable of Controlling Authentication Levels with Cooperatioin between Shibboleth and OpenAM

河野 圭太†, 稗田 隆†, 中村 素典‡

Keita KAWANO†, Takashi HIEDA†, Motonori NAKAMURA‡

keita@okayama-u.ac.jp

岡山大学 情報統括センター†
国立情報学研究所‡
Center for Information Technology and Management, Okayama University†
National Institute of Informatics‡

概要

岡山大学では，利用者の利便性向上を目的として，各種サービスのシングルサインオン化を進めてきた．しかしながら，従来のシングルサインオン基盤では，利用者を認証する方式として，ID・パスワード認証のみを提供しており，連携するサービスの増加につれて，安全性の確保が新たな課題となっていた．そこで，2016 年 3 月に更改した新統合認証システムでは，シングルサインオン基盤の認証方式として，ワンタイムパスワード認証の採用を決定した．しかしながら，従来の ID・パスワード認証に加えて，常にワンタイムパスワード認証を要求することは，利用者の負担が大きいと考え，サービスの管理者や認証サーバの管理者が当該サービスの認証強度を高めたい場合，または，利用者が自身が利用するサービス全体の認証強度を高めたい場合にのみ，ワンタイムパスワードによる追加の認証が求められるようにした．岡山大学では，Shibboleth と OpenAM を連携させることにより，このような要求を満たすシングルサインオン基盤を構築した．

キーワード

統合認証，認証連携，シングルサインオン，多要素認証，認証レベル

1 はじめに

近年，大学等の高等教育機関においても，教育や研究，業務目的で利用する情報サービスの数が，増加の一途を辿っている．これらのサービスそれぞれで利用者に認証を求め，ID・パスワード等のクレデンシャルを提出させることは，利用者の利便性を著しく低下させるため，一度の認証で複数のサービスを利用可能とするシングルサインオン基盤（統合認証システム）の導入が進んできた [2, 3, 4]．とりわけ，近年，クラウドサービスの利用が拡大する中，組織内だけでなく，組織外の情報サービスも含めたシングルサインオン環境の構築が重要な課題になっている [5, 6]．

学術界では，認証フェデレーションと呼ばれる共同体の構築により，組織の枠を超えた情報サービスの相互・共同利用に関する取り組みも進んでいる [7]．各組織が，認証フェデレーションが定めたポリシーを遵守し，互い

*本論文は文献 [1] の内容を発展させたものである．

に信頼し合うことで，認証連携を実現できるため，利用者は，自組織のサービスと同様に，他組織のサービスをシングルサインオン利用できる．日本では，国立情報学研究所が運営する「学認（GakuNin）」がその役割を担っており，学術 e-リソースを利用する大学や，学術 e-リソースを提供する機関・出版社等が参加している [8]．インターフェデレーションと呼ばれる認証フェデレーション間の連携も進んでおり，さらなる利用者の利便性向上が期待されている [9]．

このような背景から，岡山大学においても，学認が使用する Shibboleth を中心に，学内の情報サービスやクラウドサービス，学認サービスとのシングルサインオンを実現する基盤を構築してきた [10]．しかしながら，従来のシングルサインオン基盤では，利用者を認証する方式として，文献 [11] で報告した一部の例外を除き，ID・パスワード認証のみを提供しており，連携するサービスの増加につれて，安全性の確保が新たな課題となっていた [12]．

そこで，2016 年 3 月に更改した新統合認証システムでは，シングルサインオン基盤の認証に，多要素認証を導入することとし，その方式として，ワンタイムパスワード認証の採用を決定した．利用者を認証する際に，従来の ID・パスワード認証に加えて，ワンタイムパスワード認証を要求することにより，知識（Something You Know）による認証に加えて，所有（Something You Have）による認証を実現できるようになり，安全性の向上が期待された [13, 14]．

ところが，利用する場所やサービスに関わらず，常に追加のワンタイムパスワード認証を要求することは，利用者の利便性低下につながるため，この問題を解決することが求められた．そこで，岡山大学では，サービスの管理者や認証サーバの管理者が当該サービスの認証強度を高めたい場合，または，利用者が自身が利用するサービス全体の認証強度を高めたい場合にのみ，ワンタイムパスワードによる追加の認証を要求するシステムを構築することで，利便性の提供と安全性の向上のトレードオフを図ることにした．具体的には，「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」の三つの認証レベルを定義し，サービスの管理者や認証サーバの管理者による当該サービスに対する認証レベルの要求と利用者による自身が利用するサービス全体に対する認証レベルの要求の組み合わせに応じて，最終的に要求される認証レベルを制御できるようにした．

岡山大学では，従来，シングルサインオン基盤の中心として利用していた Shibboleth と，リバースプロキシ型のシングルサインオン基盤構築のため新たに導入した OpenAM の認証を連携させることにより，学内外の様々なサービスの利用に際して，要求する認証レベルを制御可能なシングルサインオン基盤を構築した．

2 関連技術

Shibboleth は，OASIS で策定された SAML 標準に基づき，組織間のシングルサインオン・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る [15]．学認などの学術認証フェデレーションとの親和性を考慮し，岡山大学を含む多くの組織で Shibboleth IdP V2 が利用されていたが，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．そのため，2016 年 3 月に更改を予定していた岡山大学の新統合認証システムの検討段階においても，Shibboleth IdP V3 によるシステム構築が求められた．

Shibboleth IdP V3 では，一つの認証方式（認証フローとして実装される）に対して複数の AuthnContextClassRef を紐づけることが非推奨ではなくなり，また，RequestedAuthnContext の Comparison 属性を正しく処理できるようになるなど，Shibboleth IdP V2 と比較して，幾つかの機能改善が見られた [16]．ID・パスワード認証の結果として得られる属性値から，2 要素認証の適用を制御する機能（Initial Authentication および Attribute Lookup 機能）も存在していたため，これらの機能を組み合わせ，目的とする認証レベルの制御を実現することも検討した [17]．

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方式を変更できないことが問題となった．Shibboleth IdP V3 では，標準で用意されている認証フローだけでなく，独自に開発した認証フローを組み込むことも容易にできるため，要求を満たす認証フローを新たに開発することも検討した．しかしながら，最終的にリース契約の一部としてシステムの構築や保守を外部業者に委託する予定があり，Shibboleth IdP V3 自体もリリース直後でノウハウの不足や機能変更のリスクがあることから，極力，基本機能には手を加えないこととした[1]．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 への対応が計画されておらず，採用できなかった [18]．

なお，Shibboleth IdP V3.3.0 では，多要素認証を扱う認証フローが実装され，各種条件に応じて認証フローの組み合わせ実行を制御できるようになるなど，現在も認証の高度化へ向けた機能拡張が行われている [19]．

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．OpenAM の利用により，連携システムにエージェントを導入し，認証連携を実現するエージェント方式や，SAML

[1]実際，Initial Authentication および Attribute Lookup 機能は，既に非推奨になっている [16]．

や OpenID Connect によるフェデレーション方式のシングルサインオンを実現できる．また，リバースプロキシにエージェントを導入することによって，リバースプロキシ方式のシングルサインオンも実現できる．岡山大学では，以前より，幾つかの学内サービスに対して，リバースプロキシ方式のシングルサインオンを提供しており，この機能を継続させる必要があったため，OpenID Connect への対応など，今後の発展への期待も含めて，OpenAM の導入を決定した．

Shibboleth と OpenAM を連携させる取り組みは，これまでにも幾つかの組織で実施されてきた [20]．これらの取り組みでは，Shibboleth IdP に OpenAM のエージェントを導入し，Shibboleth IdP での認証を OpenAM で実施することによって，学内外の様々なサービスのシングルサインオンを実現していた．しかしながら，我々が知る限り，これらは Shibboleth IdP V2 に関するものであり，また，本論文のように，それぞれのサービス（Shibboleth SP）の管理者や認証サーバの管理者，利用者の要求に応じて，認証レベルを制御できるものではなかった．

また，文献 [21] では，Shibboleth IdP での認証を Office 365 の認証（ADFS）と連携させることにより，多要素認証に対応したシングルサインオン基盤を構築した事例が報告されている．この取り組みでは，Shibboleth IdP を Shibboleth SP としても動作させ，ADFS と SAML で認証連携する方法が採用されている．文献 [21] では，本来の Shibboleth SP に応じて，あるいは，学外か学内かに応じて，多要素認証を行うかどうかを変更することができないことが，課題として挙げられている．

3 認証レベルを制御可能なシングルサインオン基盤の構築

3.1 岡山大学認証レベルの規定

前述したように，安全性を向上させるため，利用する場所やサービスに関わらず，常に追加のワンタイムパスワード認証を要求することは，利用者の利便性低下につながる．この問題に関しては，Level of Assurance（LoA）や Assurance Level と呼ばれる身元保証レベルを規定し，利用するサービスごとに認証方式を変更する方法が確立されつつある [22, 23]．例えば，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，複数の認証方式を適切に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，この方針を採用し，岡山大学認証レベルとして，表 1 に示すような 3 段階のレベルを規定し，利用するサービスごとに要求する認証方式を変更することにした．レベル 1 は従来のシステムと同様に，学内・学外からの利用に関わらず，常に ID・パスワード認証のみで要求を満たすもの，レベル 2 は，学内からの利用に関しては，ID・パスワード認証のみで要求を満たすものの，学外からの利用に関しては，ID・パスワード認証に加えて，追加の認証を要求するもの，レベル 3 は，学内・学外からの利用に関わらず，ID・パスワード認証に加えて，追加の認証を要求するものとした．

表- 1: 岡山大学認証レベルの規定

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

利用者の多くは日中は学内におり，学内ネットワークを経由して各種サービスにアクセスすることが想定されることから，レベル 2 のような認証レベルを規定することにより，学内の利用者の利便性を低下させることなく，学外からの攻撃に対処できると考えた．

今後，順次，各種サービスの認証レベルをレベル 2 や 3 に移行することを計画しているが，普及の初期段階においては，様々な利用者に対する利用者支援の問題から，運用の変更に時間がかかることが想定された．一方で，セキュリティ意識が高い利用者からは，このような機能を早期に全面的に適用できることが求められると考え，後述するように，このようなレベル選択を，サービスの管理者や認証サーバの管理者だけでなく，利用者自身が実施できるようにした．

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，岡山大学認証レベル 2 および 3 では，従来の ID・パスワード認証に加えて，追加の認証を要求するようにした．このため，追加の認証として利用する認証方式を選定する必要があったが，本学では，実装の容易性および利用者の操作性を考慮し，ワンタイムパスワード認証を採用することにした．ワンタイムパスワード認証は，個人向けの Gmail などでも利用できるため，教育的な効果も期待した．

具体的には，モバイルアプリを利用したワンタイムパスワード認証，電子メールを利用したワンタイムパスワード認証の 2 種類の方法を利用できるようにした．文献 [24] には，電子メールによる所有の確認はしてはならないことが記載されているが，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，これらの 2 種類の方法を同レベルの方法として，利用者が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，幾つかの学内サービスに対して，リバースプロキシ方式のシングルサインオンを提供していた．ところが，従来のシステムでは，リバースプロキシ方式のシングルサインオンサービスと，Shibboleth によるシングルサインオンサービスが，それぞれ独立したシステムとして運用されており，両者のシステム間でシングルサインオンが実現できないことが課題となっていた．

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，リバースプロキシ方式のシングルサインオンサービスを継続することにしたが，利用者の利便性を向上させる目的から，Shibboleth によるシングルサインオンサービスとの連携を行い，統一したシングルサインオンサービスとして運用できることが求められた．

そこで，一方のシステムを他方のシステムのシングルサインオン対応サービスの一つとして扱い，認証機能を一方のシステムで一元的に実施することで，統一的なシングルサインオンサービスを実現することにした．これを実現する方法として，OpenAM に Shibboleth SP を導入し，Shibboleth IdP の認証で全体の認証を制御する方法と，Shibboleth IdP に OpenAM のエージェントを導入し，OpenAM の認証で全体の認証を制御する方法が考えられた．

岡山大学では，Shibboleth IdP V2 と OpenAM の連携方法として他大学で実績があること，OpenAM では標準の認証モジュール（認証方式の実装）として，モバイルアプリを利用したワンタイムパスワード認証，電子メールを利用したワンタイムパスワード認証のいずれも利用できることから，後者の方法を採用した．

そこで，Shibboleth IdP に OpenAM のエージェントを導入することになったが，これに関しては，Shibboleth IdP V3 の標準機能として用意されている RemoteUser ログインフローを用いて，容易に実現できる．具体的には，Shibboleth IdP に RemoteUser ログインフローを定義し，フロー実行時に呼び出される URL を OpenAM エージェントの保護対象に設定する．これによって，Shibboleth IdP で認証が求められた際に，OpenAM で未認証であれば，OpenAM の認証画面へリダイレクトさせ，認証を実施し，OpenAM で認証済みであれば，Web サーバの環境変数によって，認証情報を Shibboleth IdP へ引き渡すことができる．

しかしながら，単純に一つの RemoteUser ログインフローを定義し，その URL を OpenAM エージェントの保護対象に設定するだけでは，OpenAM からは Shibboleth IdP と連携するサービス群が巨大な一つのサービスとして見えてしまい，サービスの管理者や認証サーバの管理者による当該サービスに対する要求に応じて認証レベルを制御する運用ができないことが問題となった．この問題を解決するため，Shibboleth IdP に三つの RemoteUser ログインフローを定義し，フロー実行時に呼び出される URL によって，要求されている認証レベルを OpenAM 側で把握できるようにした．

表- 2: 岡山大学認証レベルと URL の紐づけ

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

具体的には，システムでサポートするログインフローを定義する general-authn.xml に authn/OUL1，authn/OUL2，authn/OUL3 の三つを定義するとともに，予め/system/flows/authn に用意されている RemoteUser ログインフローの定義ファイルを流用し ，/flows/authn/OUL1/，/flows/authn/OUL2/，/flows/authn/OUL3/にそれぞれの定義ファイルを用意した [16]．これにより，それぞれの岡山大学認証レベルに対して，表 2 に示す URL をログイン用の URL として紐づけることができた．さらに，これらのログインフローを有効化するため，idp.properties（idp.authn.flows）や web.xml を変更した．

また，サービス側の設定で認証レベルを制御できるように，これらのログインフローにそれぞれ異なる AuthnContextClassRef を設定した．図 1 に，岡山大学認証レベル 1 に相当する authn/OUL1 に関する，general-authn.xml の設定例を示す．紙面の都合上，図 1 では，一部の属性等を省略している．岡山大学認証レベル 1 は従来の ID・パスワード認証に相当するため，独自の AuthnContextClassRef（http://okayama-u.ac.jp/oul1）だけでなく，標準の AuthnContextClassRef（urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport）を併記している．

ただし，実際の運用においては，たとえ学内サービスであったとしても，サービス側に設定変更を依頼するよりも，IdP 側で設定変更を実施する方が容易なため，当該サービスの管理者と調整し，認証レベルを決定した上で，認証サーバの管理者が IdP 側の設定変更で対応している．具体的には，図 2 に例を示すような形で，IdP の relying-party.xml において，サービスごとに認証レベルを設定している．図 2 は，「https://sp.example.org」を ID とするサービスに対して，岡山大学認証レベル 3 を指定する場合の設定例である．紙面の都合上，図 2 でも，一部の属性等を省略している．

```
<bean id="authn/OUL1" parent="shibbole
th.AuthenticationFlow">
 <property name="supportedPrincipals">
  <list>
   <bean parent="shibboleth.SAML2Authn
ContextClassRef" c:classRef="urn:oasis
:names:tc:SAML:2.0:ac:classes:Password
ProtectedTransport" />
   <bean parent="shibboleth.SAML2Authn
ContextClassRef" c:classRef="http://ok
ayama-u.ac.jp/oul1" />
  </list>
 </property>
</bean>
```

図- 1: general-authn.xml の設定例（一部省略）

```
<bean parent="RelyingPartyByName" c:rel
yingPartyIds="https://sp.example.org">
 <property name="profileConfigurations">
  <list>
   <bean parent="SAML2.SSO" p:authentic
ationFlows="#{{'OUL3'}}" />
  </list>
 </property>
</bean>
```

図- 2: relying-party.xml の設定例（一部省略）

3.4 OpenAM 認証レベルとの紐づけ

OpenAM では，予め用意されている認証モジュールをシステムに登録することにより，容易に様々な認証方式を利用できる [25]．また，それぞれの認証モジュールに，認証成功時に得られる認証レベル（以降，必要に応じて OpenAM 認証レベルと呼ぶ）を設定でき，利用するサービスに対して現在の認証レベルが不足していれば，利用者に追加の認証を求めることもできる．利用するサービスに必要な認証レベルは，OpenAM エージェントが保護対象とする URL ごと，利用者の接続元 IP アドレスごとに設定できる．

そこで，利用する三つの標準の認証モジュールを組み込み，表 2 のように岡山大学認証レベルごとに用意した URL に対して，接続元 IP アドレスと必要な認証レベルの組み合わせを認可条件（ポリシー）として定義することで，目的とする制御を実現することにした．

まず，認証モジュールとして，ID・パスワード認証のための LDAP 認証モジュール，モバイルアプリを利用したワンタイムパスワード認証のための OATH 認証モジュール，電子メールを利用したワンタイムパスワード認証のための HOTP 認証モジュールを登録し，それぞれの認証レベルを 0，3，3 に設定した．また，LDAP 認証モジュールがデフォルトの認証モジュールになるように（認証連鎖と呼ばれる機能を）設定した．

表- 3: 岡山大学認証レベルと認可条件の紐づけ

岡山大学 認証レベル （URL）	認可条件	
	アクセス元	**OpenAM** 認証レベル
1：ID・パスのみ （/idp/Authn/OUL1）	学内	0
	学外	0
2：学外から追加 （/idp/Authn/OUL2）	学内	0
	学外	3
3：学内からも追加 （/idp/Authn/OUL3）	学内	3
	学外	3

さらに，岡山大学認証レベルと認可条件との間で，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 URL に関しては，ID・パスワード認証に相当する 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 URL に関しては，ワンタイムパスワード認証に相当する OpenAM 認証レベル 3 を認可条件とした．なお，表 3 におけるアクセス元の設定は，実際には，OpenAM（認証サーバ）の管理画面において，対象となる IP アドレスの範囲を指定して行った．

これにより，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 に関しては，デフォルトの LDAP 認証モジュール（ID・パスワード認証）での認証成功で得られる OpenAM 認証レベル 0 で認可条件を満たし，Shibboleth IdP の RemoteUser ログインフローによる認証が成功する．一方，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 に関しては，OpenAM 認証レベル 0 では認可条件を満たさないため，セッションアップグレードと呼ばれる機能が働き，認可条件の OpenAM 認証レベル 3 を満たす認証モジュールである OATH 認証モジュール（モバイルアプリを利用したワンタイムパスワード認証）および HOTP 認証モジュール（電子メールを利用したワンタイムパスワード認証）の選択画面が表示される．

図 3 に実際の選択画面を示す．図 3 で「受取方法」を選択し，「送信」ボタンをクリックすると，選択した認証モジュールで再認証が行われ，認証に成功すれば，結果として得られる OpenAM 認証レベル 3 で認可条件を満たし，同様に，Shibboleth IdP の RemoteUser ログインフローによる認証が成功する．

このようにして，サービスの管理者や認証サーバの

図- 3: 認証モジュールの選択画面

管理者による当該サービスに対する要求に応じた認証レベルの制御に関しては，Shibboleth IdP と連携するサービスに対しても，表 1 に示した 3 段階のレベルによる運用を実現できるようになった．

次に，利用者による自身が利用するサービス全体に対する要求に応じた認証レベルの制御を実現するため，上述の設定に対して，設定の追加，変更を行った．ここで，基本的な方針として，利用者による自身が利用するサービス全体に対する要求に応じた認証レベルの制御に関しては，後述する管理システムを用いて，利用者が自身が利用するサービス全体に対して常に岡山大学認証レベル 2 以上の認証（少なくとも学外からは追加の認証を必須）を要求するかどうかを指定できるようにすることにした．

表 4 に，サービスの管理者や認証サーバの管理者が当該サービスに対して要求する岡山大学認証レベルおよび利用者が自身が利用するサービス全体に対して要求する岡山大学認証レベルと最終的に要求される岡山大学認証レベルの関係を示す．表 4 に示すように，利用者は，サービスの管理者や認証サーバの管理者が当該サービスに対して岡山大学認証レベルを要求していない場合や岡山大学認証レベル 1 を要求している場合に，最終的に要求される岡山大学認証レベルを 2 に変更するかどうかを指定できる．

この実現のため，まず，認証モジュールとして，LDAP 上の属性（プロファイル属性と呼ばれる）等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モジュールを追加した．これとともに，LDAP 上に「利用者が常に岡山大学認証レベル 2 以上の認証を要求するかどうか」を示す属性を用意し，「要求する」場合にはこのモジュールの認証を失敗とし，「要求しない」場合にはこのモジュールの認証を成功として OpenAM 認証レベル 2 を得られるようにした．この認証モジュールと LDAP 認証モジュールを認証連鎖と呼ばれる機能を用いて逐次的に実行させ，ID・パスワード認証の成功時に，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岡山大学認証レベル 2 以上の認証を要求している場合には OpenAM 認証レベル 0，要求していない場合には OpenAM 認証レベル 2 が獲得できるようにした．

表- 4: 管理者および利用者が要求するレベルと最終的に要求されるレベルの関係

管理者が要求するレベル	利用者が要求するレベル	最終的なレベル
要求なし	要求なし	1
	常に 2 以上	**2**
1	要求なし	1
	常に 2 以上	**2**
2	要求なし	2
	常に 2 以上	2
3	要求なし	3
	常に 2 以上	3

表- 5: 認証連鎖の設定例

インスタンス（認証モジュール）	条件
LDAP 認証	必須
アダプティブリスク認証	十分
アダプティブリスク認証	十分

表 5 に，このための認証連鎖の設定例を示す．認証連鎖の設定では，インスタンスという項目で適用する認証モジュールを選択し，条件という項目でその認証モジュールによる認証の成功時，失敗時の動作を定義する．定義した認証モジュールは，上から順に実行される．

まず，1 行目の LDAP 認証モジュールを「必須」と定義することで，この認証モジュールによる認証（ID・パスワード認証）が成功することが求められる[2]．LDAP 認証モジュールによる認証に成功すると，OpenAM 認証レベル 0 を獲得し，引き続き，2 行目のアダプティブリスク認証モジュールによる認証へと処理が進む．この認証モジュールは，上述した利用者ごとの認証方式を制御するための認証モジュールであり，「十分」と定義することにより，この認証モジュールによる認証（利用者が常に岡山大学認証レベル 2 以上を要求していないことの確認）が成功すると，OpenAM 認証レベル 2 を獲得し，認証動作を終える．3 行目のアダプティブリスク認証は，本来は不要な認証モジュールであるが，OpenAM に，2 行目の認証モジュールによる認証に失敗した場合にも，

[2]岡山大学の実際の環境では，LDAP 認証モジュールが「必要」と定義されているが，「必須」の方が望ましいため，そのように記載している．

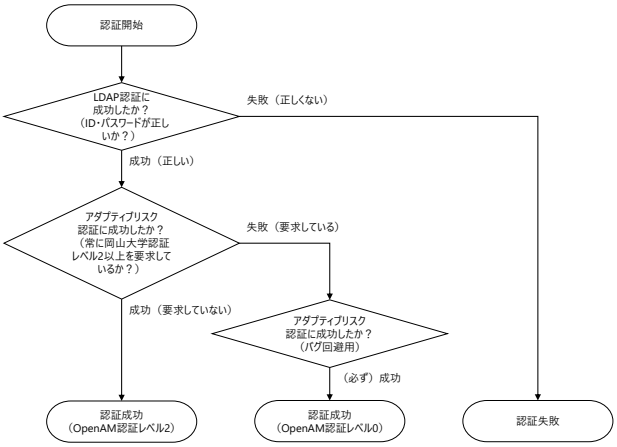

図- 4: 認証の成否と獲得する OpenAM 認証レベル

OpenAM 認証レベル 2 を獲得してしまうバグが存在していたため，必ず認証に成功し，OpenAM 認証レベルを 0 に戻すためのモジュールとして追加している．

図 4 に，表 5 のそれぞれの認証モジュールによる認証の成否により，最終的な認証の成否と獲得する OpenAM 認証レベルがどのように決定されるかを表すフローチャートを示す．

このような認証連鎖の設定とともに，表 3 に示した岡山大学認証レベルと認可条件の紐づけを，表 6 のように変更した[3]．つまり，学外からの岡山大学認証レベル 1 の URL に関して，認可条件となる OpenAM 認証レベルを 0 から 2 に変更した．これにより，常に岡山大学認証レベル 2 以上の認証を要求しない利用者は ID・パスワード認証の成功後に得られる OpenAM 認証レベル 2 によって学外からの岡山大学認証レベル 1 の認可条件を満たし，認証を終える一方で，常に岡山大学認証レベル 2 以上の認証を要求する利用者は ID・パスワード認証の成功後に得られる OpenAM 認証レベル 0 では学外からの岡山大学認証レベル 1 の認可条件を満たさず，追加の認証としてワンタイムパスワード認証が要求される運用ができるようになった．このように，学外からの岡山大学認証レベル 1 の URL に関する認可条件を変更することにより，実質的に，利用者が自身が利用するサービス全体に対して常に岡山大学認証レベル 2 以上を要求できるようにした．

3.5 利用者によるワンタイムパスワード認証の設定

ワンタイムパスワード認証に用いる電子メールアドレスの登録，モバイルアプリを設定（シークレットキーを登録）するための QR コードの作成，常に岡山大学

[3]OpenAM 認証レベル 1 は，Windows Desktop SSO 認証モジュールと呼ばれる認証モジュールのために確保していたが，運用上の理由から，現在は利用していない．

表- 6: 岡山大学認証レベルと認可条件の紐づけ（変更後）

岡山大学 認証レベル（URL）	認可条件	
	アクセス元	**OpenAM** 認証レベル
1：ID・パスのみ（/idp/Authn/OUL1）	学内	0
	学外	**2**
2：学外から追加（/idp/Authn/OUL2）	学内	0
	学外	3
3：学内からも追加（/idp/Authn/OUL3）	学内	3
	学外	3

認証レベル 2 以上を要求するかどうかの選択は，岡山大学の認証情報を一元的に管理する統合認証管理システムに新しく作成した「セキュリティ」というメニューによって，利用者自身が行えるようになっている．

ワンタイムパスワード認証に用いる電子メールアドレスの登録は，パスワードを忘れた場合の回復手段として利用する電子メールアドレスを兼ねており，パスワード再設定機能のために電子メールアドレスを登録した利用者も，結果的に，ワンタイムパスワード認証を使える利用者となる．これらについては，独立した項目とすることで，ワンタイムパスワード認証には電子メールアドレスを使わない選択肢を提供することも考えたが，当面は簡便性を優先することにした．

岡山大学では，OATH 認証モジュールによって提供しているワンタイムパスワード認証において，Time-Based One-Time Password（TOTP）方式を採用しているため，管理システム上に表示される QR コードを，Google Authenticator や Microsoft Authenticator などの汎用的なワンタイムパスワード生成アプリで読み取ることにより，モバイルアプリを利用したワンタイムパスワード認証の実行が可能になる．

図 5 に，Microsoft Authenticator をワンタイムパスワード生成アプリとして利用した場合の実際の画面を示す．一つ目のアカウントが，今回作成したアカウントであり，Office 365（二つ目）や Microsoft アカウント（三つ目）等のアカウントと同様に，利用できる．

また，常に岡山大学認証レベル 2 以上を要求するかどうかの選択は，「2 段階認証（学外から）」という項目を「使用する」または「使用しない」に設定することで行う．現時点では，「使用しない」をデフォルトにしている．

図 6 に，実際に統合認証管理システムに作成した「セキュリティ」メニューの一部を示す．

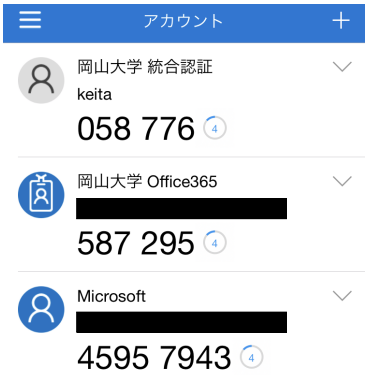

図- 5: Microsoft Authenticator を利用した場合

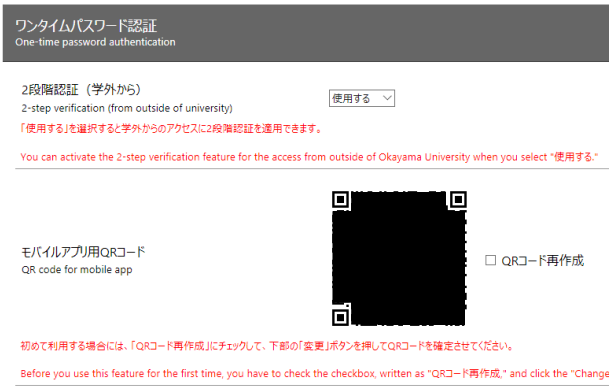

図- 6: 「セキュリティ」メニューの一部

4 運用状況と今後の課題

岡山大学では，2017 年 4 月に，SSL-VPN システムの更改を行った．このシステムが SAML に対応しており，学外から学内ネットワークへ接続する重要な役割を果たすことから，岡山大学認証レベル 3 を要求するサービスとして，運用を開始することにした．サービスの特性上，学内で接続テストを実施後，学外で利用するケースが多いと考え，認証レベルを 2 ではなく，3 に設定した．

VPN サービスは一部の利用者にとっては非常に重要なサービスであり，サービス更改の周知直後は，新しいサービスの利用方法に関する問い合わせが多く寄せられた．ワンタイムパスワード認証のために事前の設定が必要であることに気づいておらず，ワンタイムパスワードを要求すると，エラーが発生するという問い合わせも多かった．周知文書にも事前の設定が必要であることは記載していたが，説明を読まずにサービスを使ってみた利用者も多かったと考えられる．これについては，エラー画面の内容を分かりやすくするなど，利用者インタフェースの改善が求められる．

また，モバイルアプリを利用する場合，現在のシステムでは，システムの欠陥により，図 6 の画面に初めてアクセスする際に表示される QR コードを利用せず，一度 QR コードを再作成してから利用を開始する必要がある[4]．運用開始当初，この問題に気づけておらず，これに関する問い合わせも幾つか寄せられた．2 台目のモバイル端末にワンタイムパスワード生成アプリを登録する際に，再度 QR コードを作成し直してしまう利用者も見受けられた．現在，設定画面の注意事項として，初回時に QR コードを再作成することを記載しているが，これについても，分かりやすい利用者インタフェースへの改善を検討する必要がある．

また，岡山大学では，全学必修の教養教育科目（情報処理入門 1）として，学部 1 年生の 1 学期に，情報リテラシー教育を実施している [26]．この科目は，複数のクラスを複数の教員で実施しているが，基本的には講義内容を統一している．講義では，岡山大学の情報システムの利用方法に関する話題も取り扱っており，今年度より，パスワード再設定機能やワンタイムパスワード認証機能についても説明を加えた．時間の関係上，簡易な説明に留めざるを得なかったが，複数の学生がこれらのセキュリティに関する設定を実施してくれた．

表 7 に，運用開始から約一か月半が経過した 2017 年 5 月 23 日現在，統合認証管理システム上で，セキュリティに関する設定を変更している利用者数を示す．表 7 は，学生（学部 1 年生とそれ以外を区別），教職員の別に，ワンタイムパスワード認証に（およびパスワードを忘れた場合の回復手段として）用いる電子メールアドレスを登録している利用者数，モバイルアプリを設定（シークレットキーを登録）するための QR コードを（再）作成した利用者数，常に岡山大学認証レベル 2 以上を要求している（「2 段階認証（学外から）」を「使用する」に設定している）利用者数を示している．

まず，学部 1 年生については，簡易なものながらも講義中に説明を加えた甲斐もあり，約 2,300 名中 280 名が電子メールアドレスを登録していた．多くの学生は，パスワードを忘れた場合の回復手段を意識して電子メールアドレスを登録したのではないかと推察されるが，これにより，10%強の新入生が，ワンタイムパスワード認証を利用できる環境を整えたことになる．

また，QR コードを（再）作成した学部 1 年生，常に岡山大学認証レベル 2 以上を要求する設定をした学部 1 年生も，それぞれ 16 名，45 名存在した．電子メールアドレスの登録者数に対してこれらの値が少ないのは，これらの応用的な利用方法については，時間の関係上，講義中の説明も省略されがちであったことが原因であると考えられる．今後，より多くの新入生にセキュリティに関する設定を実施してもらうためには，講義中の説明を強化し，設定のための時間を確保することも求められるが，限られた講義時間の中，このための時間を確保す

[4] 一度 QR コードを再作成する手順を踏まなければ，ワンタイムパスワードの生成に必要なシェアードシークレットの一部がシステムに登録されない欠陥がある．

表- 7: セキュリティに関する設定を変更している利用者数

	学生		教職員
	学部 1 年生	それ以外	
電子メールアドレス登録者数	280	131	238
QR コード（再）作成者数	16	55	134
レベル 2 以上要求者数	45	55	107

ることは容易ではない．

学部 1 年生以外の利用者については，SSL-VPN サービスの利用者が中心であると推察される．これらの利用者については，学部 1 年生と比較して，QR コードの（再）作成者数が多くなっている．これは，ワンタイムパスワード認証の利用を目的としてセキュリティに関する設定を実施した利用者が多かったからであろう．また，SSL-VPN サービスの利用マニュアルには常に岡山大学認証レベル 2 以上を要求する機能についての説明は加えていないが，この機能を設定している利用者の割合も，同様に多くなっている．このことから，昨今の情勢から，利用者自身のセキュリティ意識も高まってきていることがうかがえる．

また，本研究では，Web シングルサインオンを対象として，ワンタイムパスワード認証の利用による安全性の強化を図ったが，岡山大学の環境では，教職員向けの電子メールシステムや学生向けの Gmail などで，Web シングルサインオンを利用しない，独自の認証が利用されている．前述の統合認証管理システムの設定で，これらの認証に用いるパスワードを Web シングルサインオン用（統合 ID 用）のパスワードとは独立して設定できる機能も提供しているが，より高い安全性を提供するためには，これら非 Web 系のシステムの対応についても，強化を進める必要がある．

なお，例えば Office Professional Plus 2016 のアプリケーションのように，Shibboleth 等との認証連携に対応し，他の Web サービスと類似の手順（同じ画面）で認証を実施できるアプリケーションも出始めているが，アプリケーションが認証時に利用する専用ウィンドウの表示領域が狭く，サイズを変更できないため，Web ブラウザを想定して作られた画面の一部が表示されないことがある．例えば，岡山大学では，文献 [27] の Shibboleth IdP の機能を用いて，他サービスに個人属性を送信することへの確認画面を表示するようにしているが，図 7 に示すように，この画面がすべて表示されず，ウィンドウサイズの変更やスクロールバーによる表示領域の移動ができないことから，この画面より先に進めなくなる利用者が時折発生している[5]．

[5]そのまま「Enter」キーを押すとデフォルトの「（個人属性の送信に）同意しない」ボタンが選択され，先に進めなくなるため，「Tab」キーで表示領域をボタンの位置まで移動させ，「（個人属性の送信に）同意する」ボタンを選択する必要がある．

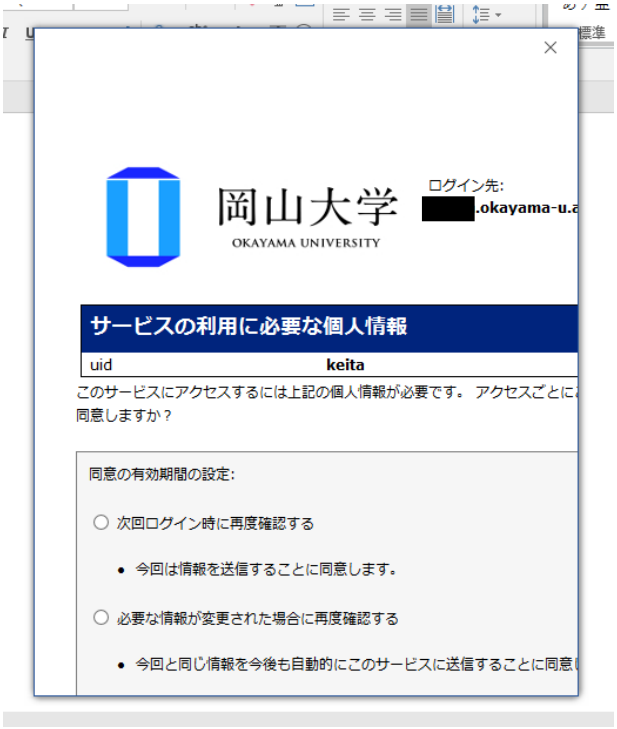

図- 7: Office 認証時の専用ウィンドウ

さらに，岡山大学では生涯メールサービスを提供しており，卒業生や退職者も利用者に含まれている．今後，ワンタイムパスワード認証をより積極的に活用していくためには，卒業生や退職者を含めた利用者支援の体制を整備していくことが重要である．

5 おわりに

本研究では，Shibboleth と OpenAM の認証を連携させることにより，サービスの管理者や認証サーバの管理者による当該サービスに対する認証レベルの要求と利用者による自身が利用するサービス全体に対する認証レベルの要求の組み合わせに応じて，最終的に要求される認証レベルを制御可能なシングルサインオン基盤を構築した．

まず，安全性を向上させるため，従来の ID・パスワード認証に加えてワンタイムパスワード認証を利用することとし，3 段階の岡山大学認証レベルを規定した．この認証レベルに従って，Web サービスに対する統一的な

認証制御を実現するため，Shibboleth IdP に OpenAM のエージェントを導入し，全体の認証を OpenAM で制御することにした．

ただし，純粋にこれをするだけでは Shibboleth IdP と連携するサービス群が巨大な一つのサービスとして見えてしまい，サービスの管理者や認証サーバの管理者による当該サービスに対する要求に応じて認証レベルを制御することができない問題があった．本研究では，Shibboleth IdP で認証レベルごとのログインフローを用意し，それぞれに対する OpenAM の認可条件を適切に制御することで，これを解決した．また，利用者による自身が利用するサービス全体に対する要求に応じて認証レベル制御を実現するための拡張も行った．

現在，ワンタイムパスワード認証を活用したセキュリティの向上に関する取り組みは，限られた利用者にしか周知できておらず，実際にこの機能を利用している利用者数もまだまだ少ない状況である．運用上の課題も幾つか見つかっているため，これらの課題を解決するとともに，利用者数の拡大へ向けて，全学的な周知を強化し，対象のサービスも増やしていく予定である．

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] 河野圭太，稗田隆，中村素典 : 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，大学 ICT 推進協議会 2016 年度年次大会，WD16 (2016).

[2] 多田充 : ユーザ負担を考慮したワンタイムパスワード認証システム，学術情報処理研究，No.20, pp.97–104 (2016).

[3] 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).

[4] 松浦健二，上田哲史，佐野雅彦 : 複数認証基盤に対応する複合 SSO 環境でのユーザエクスペリエンス，学術情報処理研究，No.16, pp.138–145 (2012).

[5] 西村浩二 : 広島大学におけるクラウドサービス利用と認証連携，第 8 回統合認証シンポジウム，pp.25–36 (2015).

[6] 松平拓也，笠原禎也，高田良宏，東昭孝，二木恵 : 学認との融合化を視野に入れた金沢大学統合認証基盤の構築と運用，学術情報処理研究，No.16, pp.41–50 (2012).

[7] REFEDS: Federations - REFEDS (online)，入手先 ⟨https://refeds.org/federations⟩ (参照 2017-07-07).

[8] 国立情報学研究所 : 学術認証フェデレーション学認 GakuNin (online)，入手先 ⟨https://www.gakunin.jp/⟩ (参照 2017-07-07).

[9] 山地一禎 : 学認の利用価値を高めるサービス連携最新動向，第 8 回統合認証シンポジウム，pp.69–85 (2015).

[10] 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).

[11] 河野圭太，藤原崇起，稗田隆 : 岡山大学事務情報システムにおける Shibboleth との連携を考慮した多要素認証の導入，情報処理学会研究報告，Vol.2014-IOT-27, No.5 (2014).

[12] 長谷川孝博，松村宣顕，高橋秀年，井上春樹 : 大学情報基盤におけるパスワード定期更新の運用と利用者動向，学術情報処理研究，No.17, pp.107–114 (2013).

[13] 情報処理推進機構 : オンライン本人認証方式の実態調査 報告書 (online)，入手先 ⟨http://www.ipa.go.jp/security/fy26/reports/ninsho/index.html⟩ (参照 2017-07-07).

[14] Phillip J. Windley: Digital Identity, O'Reilly (2005).

[15] Shibboleth Consortium: Shibboleth (online)，入手先 ⟨https://shibboleth.net/⟩ (参照 2017-07-07).

[16] Shibboleth Consortium: AuthenticationConfiguration - Identity Provider 3 - Shibboleth Wiki (online)，入手先 ⟨https://wiki.shibboleth.net/confluence/display/IDP30/AuthenticationConfiguration⟩ (参照 2017-07-07).

[17] Shibboleth Consortium: Configuring the IdP for the Multi-Context Broker Model - Identity Provider 3 - Shibboleth Wiki (online), 入手先 ⟨https://wiki.shibboleth.net/confluence/display/IDP30/Configuring+the+IdP+for+the+Multi-Context+Broker+Model⟩ (参照 2017-07-07).

[18] 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/?active_action=repository_view_main_item_detail&page_id=85&block_id=227&item_id=227&item_no=1⟩ (参照 2017-07-07).

[19] Shibboleth Consortium: MultiFactorAuthnConfiguration - Identity Provider 3 - Shibboleth Wiki (online), 入手先 ⟨https://wiki.shibboleth.net/confluence/display/IDP30/MultiFactorAuthnConfiguration⟩ (参照 2017-07-07).

[20] 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).

[21] 野口宏，大瀧保広，高橋幸雄，鎌田賢：Office365 と Shibboleth の多要素認証対応 SSO 環境の構築，学術情報処理研究，No.20, pp.82–89 (2016).

[22] National Institute of Standards and Technology: NIST SP 800-63 Digital Identity Guidelines (online), 入手先 ⟨https://pages.nist.gov/800-63-3/⟩ (参照 2017-07-07).

[23] ITU-T: Entity authentication assurance framework, Recommendatioin ITU-T X.1254 (2012).

[24] National Institute of Standards and Technology: NIST Special Publication 800-63B (online), 入手先 ⟨https://pages.nist.gov/800-63-3/sp800-63b.html⟩ (参照 2017-07-07).

[25] ForgeRock: OpenAM Administration Guide - Docs - ForgeRock BackStage (online), 入手先 ⟨https://backstage.forgerock.com/docs/openam/11.0.0/admin-guide/chap-auth-services⟩ (参照 2017-07-07).

[26] 稗田隆，河野圭太，岡山聖彦：反転学習とグループ学習を組み合わせた多人数 e ラーニング講義の実践，第 18 回学術情報処理研究集会発表論文集，pp.45–50 (2014).

[27] Shibboleth Consortium: ConsentConfiguration - Identity Provider 3 - Shibboleth Wiki (online), 入手先 ⟨https://wiki.shibboleth.net/confluence/display/IDP30/ConsentConfiguration⟩ (参照 2017-07-07).