学内サービスにおける多要素認証の導入における検討

加藤 大弥[1]　藤尾 正和[2]　高橋 健太[2]　林 達也[1]　砂原 秀樹[1]

概要：学内のサービスに対する認証の多くは ID/Password を用いている. しかしながら,2017 年 6 月に改正された NIST SP800-63-3 の影響により Password 認証は大きな変革を迎えようとしている. そこで, さまざまな認証基盤や認証技術だけではなく, 実際に構築・運用する際の連携モデルや登録モデルを考慮し, さらに利用するユーザーに対するユーザビリティやアクセスコントロールについても念頭をおいた学内サービスへの要素認証の導入ついて検討する.

Investigation of the Implementation of Multi-Factor Authentication in University Web Contents

DAIYA KATO[1]　MASAKAZU FUJIO[2]　KENTA TAKAHASHI[2]　TATSUYA HAYASHI[1]
HIDEKI SUNAHARA[1]

1. はじめに

教育機関においてインターネットでの情報公開は一般的になり, 特に大学においては受験生や保護者・不特定多数に対する情報公開だけではなく学生に対する情報提供ページを限定的に公開するといったことが行われている. これらの限定的なページへのアクセスコントロールは大きく分けて,1.Password のみ,2. 単一 ID 要素/Password,3. 複数 ID 要素 (User 名, 学籍番号等)/Password の 3 種類が一般的であると考えられる. しかし, 近年では CPU/GPU の計算能力の向上による Password 解析の高速化, クラウドベースの Virtual Machine が簡単かつ安価に借りられるようになったことなどから,Password 単体における認証は危険に晒されていといわれている. これを解決する手法としては,Password の定期変更や英数字・大文字・特殊文字を少なくとも一文字利用するといった Password の複雑性を問うということが一般的に行われている. そんな中, アメリカ国立標準技術研究所-NIST が公開しているアメリカ政府機関向け Digital Authentication 実装ガイドラインである SP800-63 が十年ぶりに大幅に改定され SP800-63-3[1] が正式に公開された. このガイドラインは, 法的な影響力がなく本実装を強制する影響力も存在してはいない. しかし, その研究成果と実績から世界中で参考にされており影響力が非常に高い文書になっている. 本ガイドラインで大幅に改定された項目として Password の取扱が挙げられ,1. 定期変更をしてはならない,2. 複雑性を要求するべきではない,3.8 文字以上であること, という内容が記載されている. これらの根拠としては, 定期変更や複雑性の要求により Password,Password1,Password1!等の潜在的な脆弱性がある Password を使用する頻度が高まることが判明したことが挙げられている. このことから, 総務省の「国民のための情報セキュリティサイト [2]」ではすでに運用・管理について方針を変更しており, 教育機関においても Password での認証について検討する必要が十分にあると考えられる.

また, 学部・研究科等で複数のコンテンツを持つ教育機関では, 図 1 のように各コンテンツごとに ID/Password を設ける場合も見られ, 複数のパスワードを記憶しなければならない点から容易に記憶できる Password を利用するということが助長されている恐れもある.

そこで本研究では, このようなコンテンツにおける認証を改善するための参考として,NIST SP800-63-3 を基に学内サービスにおける多要素認証の導入と認証要素の検討を行う. まず,SP800-63-3 には Digital Authentication における強度レベルが設定されている. そのレベルは,Identity Assurance Level,Authenticator Assurance Leve,Federation Assurance Level にわけられており, 本研究では学内コンテン

[1] 慶應義塾大学大学院 メディアデザイン研究科
[2] 日立製作所 研究開発グループ

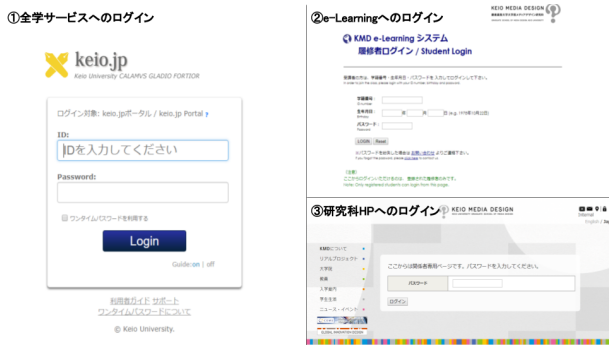

図 1　学内サービスにおける複数のアカウントでのログインの例

ツという点から AAL と FAL に焦点をあてその重要度からレベル分けを行い, 対応する認証方式をユーザビリティと運用を念頭に置きつつ検討する. また,SP800-63-3 だけではなく Password を利用しない認証として注目されている FIDO や OAuth2.0 や OpenID Connect のような認可技術, テンプレート保護型の認可技術であるテンプレート公開型生体認証基盤 (PBI), それらを管理するための Identity Provider の導入に関するコスト等の検討を行うことで, 安全性だけではなく運用可能性の面においても検討を行う.

2. 関連研究

2.1 NIST SP800-63-3 Digital Identity Guidelines

NIST が公開している Digital Identity Guidelines[1] はアメリカ政府機関向けの実装ガイドである. 前条でも述べたとおり, 本ガイドラインには法的な影響力こそないがその実績から世界中で参考にされているものである. 認証を大きく分けて Identity Assurance Level(IAL),Authenticator Assurance Level(AAL),Federation Assurance Level(FAL) の 3 つ柱で構成し, それぞれの Level の組み合わせから認証強度の保証を考察している. 本研究では大学機関という限られた組織内での認証であるため IAL は定められているものとし, 特に AAL と FAL について考察を行う.

2.2 教育機関における認証

教育機関における認証技術としては, 平成 21 年から国立情報学研究所が運用している, 学術認証フェデレーション学認 GakuNin[3] が挙げられる. 学認は学術 e-リソースを利用する大学, 学術 e-リソースを提供する機関・出版社等から構成された連合体のことであり, 他大学や商用のサービスにおいても 1 つのパスワードを利用し, かつ ID・パスワードの再入力を行わずに利用できる環境を実現することが可能になっている. これによりユーザーは複数のパスワードを覚えることがなくなり,SP800-63-3 で懸念されている簡単なパスワードを生成・利用する可能性が減少すると考えられる. しかし, 学内サービスのすべてを学認に登録するためには審査という面で相当の労力になる懸念があり運用上現実的ではない. また, 学認において多要素認証を実現するための考察は行われており,[4] 認証が導入可能性だけではなく当時の Digital Identity Guidelines である P800-63 の LoA を考慮した運用の検討も行っている [5]. しかし, 複数のサービス・プロバイダに対してアクセスコントロールが困難であることなどの問題があり実現するためには構築上のコストが高くなってしまうことがわかる.

2.3 認証・認可技術

SP800-63-3 の認証要素でも取り上げられている通り認証技術は日々発展している.OTP 認証や USB トークンを利用した認証, 近年スマートフォンで用いられている指紋認証や顔判別認証は一般的なものになりつつある. また, 指紋などの生体情報は比較的容易に偽造することが可能であることが知られていることから, 単純な生体認証だけではなく日立システムズの指静脈認証のような, 指静脈の情報から電子署名を作成したのちに PKI を用いた認証を行うとで偽造を困難にする認証方式も開発されている.

堅牢な認証デバイス間で相互運用性が欠如している現状を変革し, ユーザーが複数のユーザー名とパスワードを作成して記憶しなければならないという問題の解決を目的として FIDO(Fast IDentity Online) といった新しい認証標準の策定も積極的に行われている.FIDO では, ユーザー認証におけるパスワードへの依存を軽減するために, オープンで拡張性と相互運用性があるメカニズムを定義する仕様を開発しており,Yubico が販売している Yubikey[6] では, すでに USB トークンとして Google などの主要なサービスの認証を行うことが可能になっている.

認証技術の他にもユーザーに一時的に権限を与えることを目的とした認可技術の発展も著しい. 学認でも用いられている Shibboleth[7] やソーシャルログインに用いられている OAuth2.0[8],OpenID Connect[9] が有名である.OAuth2.0 では登録されている ID から認可を受けることで不特定多数のユーザーにアクセストークンを付与することでサービスを利用できる許可を与えることが可能になっている.Shibboleth と OpenID Connect では認可技術を応用してユーザーを識別し, アクセスコントロールが付加された認証を行うことが可能になっている. また, アクセスコントロールを行えるため同様の仕組みを有しているサービスに対して Single Sign On(SSO) を実現し,1 つのパスワードのみで不特定多数のサービスを利用することができる.OAuth と OpenID Connect においては, トークンと呼ばれる様々な情報が付与されている鍵のようなものを利用して認証認可を行っている.

3. 認証基盤構築における運用要件と検討

3.1 認証手法に関する検討

学内における認証基盤を構築するにあたって, 認証手法とフェデレーションを行うための要件を SP800-63-3 を参

考にして考察を行う. 認証手法については SP800-63-3B で定められており,Authenticator Assurance Level(AAL:認証器保証レベル) で 3 段階のレベルで定められている. 各レベルと内容については表 1 に示す. また, 認証を行うために用いられる認証器を図 2 に示す.

表 1 Authenticator Assurance Level

AAL Level	
AAL1	幅広く利用可能な認証技術を使った単一要素認証器を利用. ある程度の保証を提供.
AAL2	多要素認証器の所持, または 2 つの単一要素認証器の組み合わせが求められる. 高い確実性を提供.
AAL3	暗号プロトコルを介した鍵の所持証明に基づいている. 検証主体なりすまし耐性を持った”堅牢な”の暗号認証器が必要. 極めて高い確実性を提供する.

図 2 Authenticator のタイプ

まず, 認証器と実際の運用コストについて考察を行う. 学内におけるユーザーの殆どは, 学生であり毎年数百人単位の新規・退会する ID を管理することになる. そのため物理的なトークンを各個人ごとに用意することは容易ではなく,AAL3 を実現するよう堅牢な認証器は高価であることが多く実現可用性は低いと考察できる. これは,AAL2 でも同様であり, 多要素認証器は高価であり導入は困難である. しかし, 実際の認証強度の面から考えると認証強度が高い AAL2,3 を導入するにこしたことはない. そこで考えられる方法としては, 単一要素認証器を組み合わせた認証を利用する方法とアクセスコントロールを用いた特定ユーザーへの多要素認証器の貸付である. 単一認証を組み合わせる場合, 使用する Authenticator を選択するにあたり, パスワード単体での認証とバイオメトリクスを用いた認証に関しては.

- Password は 8 文字以上, 最低 64 文字を許容, ペースト機能の許容, パスワード変更をすべきではない
- バイオメトリクスは, 確率的な要素であるため決定的ではなく,Authenticator としてカウントせず補助的な認証器としてのみしか認めない

ということを最初に考慮する必要がある. そのため, 組み合わせの例としては, 記憶シークレット, 単一要素 OTP デバイスや単一要素暗号ソフトウェアが挙げられる. 記憶シークレットは Password を用いた認証, 単一要素暗号ソフトウェアは Google が提供している Google Authenticator が挙げられ,Google Authenticator PAM module[10] という Server Side に OTP 認証を実装するモジュールがオープンソースとして公開されている. 単一要素暗号ソフトウェアには端末ごとに保存されているクライアント証明書が挙げられる. その他にも限定的ではあるが一部の iPhone に搭載されている TouchID や FaceID を利用したデバイスから OTP などを発行する多要素 OTP デバイスやバイオメトリクスの例外として挙げられるバイオメトリクステンプレートを PKI などで保護されクレデンシャルを無効化するための手法を有している日立システムズの SHIELD PBI 指静脈認証サービス [11] を利用することも可能である.

3.2 フェデレーションに関する検討

フェデレーションについては表 2 に示す.Bearer Assertion とは誰に対して利用を許可するのかを確認せずに行うという意味合いである. すべての FAL において IdP を設置することが必須になっており,FAL2,3 については Assertion に対する Relying Party(RP,Auth Client) の公開鍵による暗号化が必要になる.FAL3 ではさらに Assertion に対して鍵を用意し, 紐づく鍵の所有を証明しなければならない.

次に,IdP と RP の登録に関する Federation Model について検討する.Model は 4 種類存在しており, 学内サービスで利用するという点において様々なサービスが乱立しているという観点から,IdP と RP を手動で登録を行う Manual Registration とトランザクション時に自動で登録を行う Dynamic Registration が現実的であると考えられる. この 2 つの大きな違いとしては White List が運用できるか否か, ユーザーの RP への接続時に同意を求めるか否かである.IdP と RP の大まかな登録の仕組みは酷似しているため, 選択する判断基準としては,RP 利用時にユーザーへの同意を求める周りに任意の RP を White List として運用することが可能な前者か, ユーザーへの同意を必要としない代わりに IdP から周知されている安全な場所に RP を設置しなければならない後者かを, 各々が運用している学内サービスの場所と運用コストを考慮する必要がある. 一方で学認は団体に参加することで得られる権威のもとで IdP と RP を特定の審査を行うことで登録を実現している Federation Authorities のモデルであると考えられるため, 学認の定める Authoritiy の元で審査が行われ IdP や RP が容認されない可能性あると考えられため自由な運用は困難である.

次に, ユーザー情報をどのように IdP と RP の間でやり取りをするかの Assertion Presentation を考える. 基本的には,Back-Channel か Front-Channel で Assertion のやり

表 2 Federationr Assurance Level

FAL Level	
FAL1	Bearer assertion, Singed by IdP
FAL2	Bearer assertion, Signed by IdP and encrypted to RP.
FAL3	Holder of key assertion, Signed by IdP and encrypted to RP.

取りが行われることになっている. 大きな違いとしては前者においては, ユーザーの Assertion の受け渡しが IdP と RP 間で行われるのに対し, 後者はユーザーが RP のコンテンツを利用する際にブラウザ上に直接 Assertion が送付されるという点である. 今回検討している学内サービスでは図 1 のような複数の RP に対して IdP から Assertion をやり取りすることを考えた場合, 前者では RP は第三者 (Subscriber を含む) による傍受・改ざんの可能性を最化しつつ Assertion を IdP に直接要求することが可能になっているが, 後者は Assertion が第三者 (Subscriber 自身を含む) に渡ってしまうためシステム情報の漏洩の可能性があるため複数の RP に対しての利用は推奨されていない. よって,Assertion Presentation に関しては Back-Channel モデルを利用することが推奨される.

4. 認証基盤構築における技術的要件と考察

前章により洗い出された運用に必要な要項から実際に IdP を構築するために,IdP と RP との連携・多要素認証への対応・運用コストの面で検討を行う. 本研究では SAML,OpenID Connect を候補として考察する. そもそも,SAML と OpenID Connect の違いとしては,SAML では運用前に, メタデータや証明書の交換を行うことで信頼関係（トラストサークル）を構築する必要がある.OpenID Connect では, どの RP も認証連携できるという原則の元で信頼関係を構築する必要がない. また, 前者では IdP-RP 間で仮名 ID を使用することで ID 連携を行っているが OpenID Connect ではグローバル URL による OpenID で認証連携を行っている. このことから,SAML は使用する Web サービスの範囲が厳格に定められているサービス群に対しての利用,OpenID Connect は Open な Web サービス間の認証連携が求められる際に利用することが良いとわかる.

まず IdP と RP の連携について考察する. 学内サービスという限定された範囲での運用を行うため SAML のが良いように思われる. しかし,SAML の問題点としては RP に対する SAML SP の実装コストが高く,IdP と PR の連携検証が非常に難しいということが挙げられる. 一方で OpenID Connect では URL を利用した Open な IdP 連携が可能であり RP に対しては認証フローを元に既存の構成をほとんど崩すことなく実装することが可能になっている. しかし,Open な IdP であるためセキュリティ上のリスクがあり, 特定の人のみがアクセスできるようなアクセス制限などを実装をする必要がある.

次に多要素認証への対応について考察する.SAML では前に述べたように RP 側での実装が困難であること,10 年前からメジャーアップデートが行われていないことから,OTP やイメージマトリックス認証などの特定の認証にのみにしか対応しておらず近年用いられている多要素認証の導入は困難である.OpenID Connect では OAuth2.0 を元にした token のやり取りによる認可を応用して API として認証をおこなっているため様々な要素の認証規格にかかわらず認証を行うことが可能になっている. それだけではなく FIDO などの他の認証オープンスタンダードにも連携が行われている.

最後に運用コストについて考察する. 運用コストに関しては,SAML では基本的に連携している相手のみと認証を行うが厳密な制約がない OoenID Connect では不特定多数の RP や悪意のあるユーザーからの認証要求が発生する可能性がある. そのため, 後者では定期的に連携している RP の確認や RP とのアクセスコントロール,IdP に保管されている token の管理を行わなければならない.

以上のことから本研究では運用コストはかかってしまうものの, 本来の目的である Password による認証の危険性を考慮することと多要素認証への対応が柔軟であり, どのようなサービスにおいても対応しやすい OpenID Connect を採用することとする.

5. 学内サービス運用モデルの検討と提案

5.1 IdP の選定

以上の考察を踏まえて実際に学内サービスを運用モデルを検討する. まず IdP について検討する.OpenID Connect に対応した IdP を構築する方法を本研究では 2 種類検討した. まず, フルスクラッチで IdP を構築する方法である. これは OpenID Connect を開発している OpenID Foundation が C#,Java,Javascript などの様々なライブラリを公開している [12]. しかし, フルスクラッチでの構築は導入コストが高いため今回は考慮しないものとした. 次にパッケージのデプロイがあり,IdP の構築としては広く一般的な手法である. 本手法についても OpenID Foundation 認定している IdP を複数公開しており, 代表的な IdP としては, ソーシャルログインに優れている Auth0[13] や比較的新しく更新頻度が多い Keycloak[14], 多彩な WebAPI が実装されている MITREid Connect[15] があげられる. その中から本研究では,OTP や FIDO といった多くの多要素認証が導入されている Keycloak と,WebAPI による認証が可能であることで既存の学内サービスとの連携が容易であると考察できる MITREid Connect による IdP の構築を検討する.

5.2 多要素認証の導入と認証モデル

Password 以外の認証方式の導入の検討を行う. 本研究で

考えられる多要素認証を導入するシナリオとしては, 多要素認証によるユーザビリティの創出と多要素認証によるアクセスコントロールを提案する.

多要素認証によるユーザビリティの創出

3.1 で挙げた通り,Password による認証については 8 文字以上で辞書にのっていないようなものを使用しなければならないことから”s1AkL!78”のようなユーザーが覚えることが困難な場合があり Password による認証が使用しづらくなる可能性が考えられる. そこで, ユーザーが認証を行う環境や状態によって認証方式を選択することを可能にすることでユーザーの認証への負担を減らすことができると考えた. また, 覚えにくいという点から Password のメモを取り紛失してしまうといったソーシャルハック予防できるのではいかと考える. イメージを図 3 に示す. 例としてスマートフォンで生成される OTP や USB トークンを利用することでユーザー負担をかけずに比較的容易に認証を行うことが可能になり, 紛失した場合のリスクが比較的軽度に抑えることが可能になる. さらに PBI 指静脈認証では, 前述のように認証器を保持せずに指をかざすだけで認証を行うことができると考えられる. 考えられる利用シナリオとしては, 大学図書館にある検索サービスにおいて, ユーザーログインを行う場合や研究室等に置かれているマシンから研究室のクラウドストレージや学内の e-learning システムにアクセスする場合のような設置されているマシンからログインする場合においてユーザビリティを担保することができる考えられる.

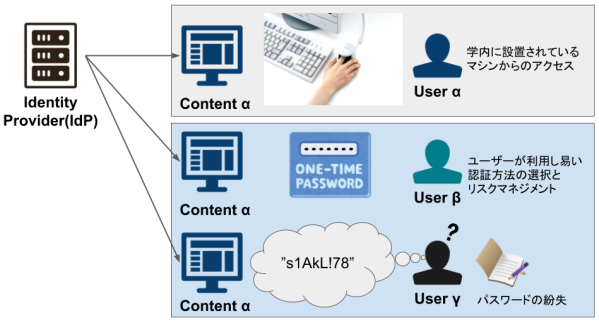

図 3　ユーザーによる認証要素の選択イメージ

多要素認証によるアクセスコントロール

次に考えられるのは, 各ユーザーに与えられている権限のアクセスコントロールである. ここでは,e-learning システムを例として置き, イメージを図 4 に示す.e-learning システムには,{ 閲覧権限がある一般的な学生, 受講生へのメールの送付や授業資料をアップロードを行うことができるような編集権限を持つ Teaching Assistant のような学生や学生部の職員, 提出された課題の閲覧や採点を行うことが可能な管理権限をもつ教職員 } のロールが存在していると仮定する. この場合においては, 管理者権限を持つ教職員のアカウントは閲覧が許されているアカウントよりも重要度は高いと考えられるが, ほとんどの場合において運用コストと構築コストの面から学生と教職員に対する認証要素が同じ (ID/Password による認証) である. そこで, この権限の重要度を考慮して権限の弱い一般的なユーザーに対しては Password での認証, 教職員に対しては Password の使用は認めず OTP と指静脈認証の 2 段階認証を行い権限に対する認証の重み付けを実施することでアクセスコントロールとアカウントが奪われた際のリスク軽減を実現できると考える.

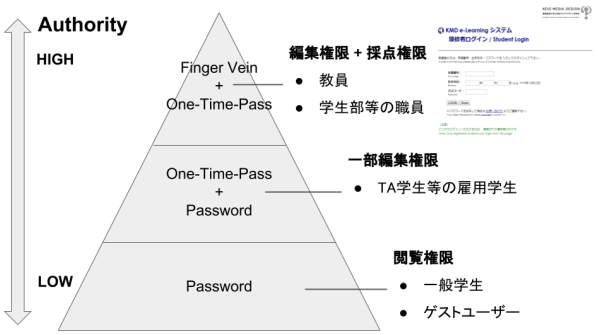

図 4　認証要素によるアクセスコントロールのイメージ

6. 学内サービスの構成の提案

以上のさまざまな面での検討を踏まえ, 実際の学内サービスの構成モデルをユーザビリティモデルとアクセスコントロールモデルとして提案する. 本提案は著者の考慮した学内環境を参考にした例である. 基本的な構成要素を表 3 に示す.RP は Certified OpenID Connect Implementations[12] に,Ruby,Java,C#などの主要な言語に対応したライブラリが用意されている. 認証基盤については, 考えうる認証基盤の一例を挙げており, 表中のカッコ内には OpenID Connect に対応しやすいモジュールを記載している.IdP と RP の連携と動作に関しては, 学内におけるさまざまなサービスに対応しやすいことを考慮し, ホワイトリスト方式によって手動で RP を登録する Manual Registration,Assertion Presentation では, 複数の RP を用いるために安全性を考慮した最小構成である Back-Channel Presentation を採用した. これらを踏まえ, それぞれの詳しい構成モデルと認証フローの例を次に示す.

6.1 ユーザビリティモデル

ユーザビリティモデルでの構成を図 5 に, 考えうる認証フローの例を図 6 に示す. 本モデルでは, ユーザーが一つのコンテンツに対して環境や使用するマシンに合わせて任意の認証方式を利用する構成となっている. 基本的な流れとしてはユーザーが選択した認証方式を元に認証サーバーにログインリクエストを送り,IdP がすでに対応している認証

表 3　提案するモデルにおける基本的な構成要素

構成要素	
IdP	MITREid Connect or Keycloak
RP	OpenID Connect RP Libraries
認証基盤	ID/Password,FIDO-U2F (YubiKey),OTP (Google Authenticator PAM module),PBI (SHIELD PBI)
Federation	Manual Registration
Assertion Presentation	Back-Channel Presentation

に関しては IdP でログインを行う. 指静脈認証などの対応していな要素に関しては認証サーバーで一度認証を行い, 認証が成功した場合に client_token を IdP に受け渡す. その後どちらの場合においてもユーザーは接続する RP への認可の合意を行うことで IdP から id_token が発行され認証サーバーに送られる. 最終的に認証サーバーで検証し,RP のコンテンツへリダイレクトすることでログインが完了する仕組みになっている.

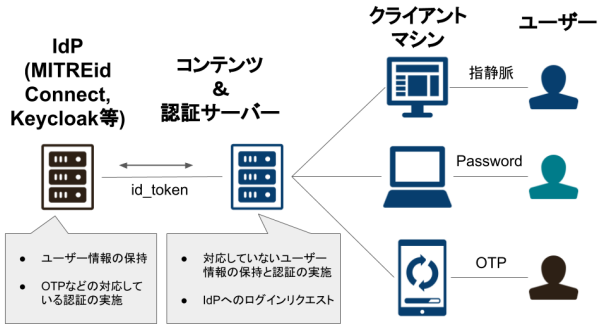

図 5　ユーザビリティを配慮したモデル

最初のログインリクエストにおいて選択された認証手法に基づいた認証画面をリダイレクトし, 四角で囲まれている範囲内において柔軟に認証を行う構築を行うものとしている. しかし, この手法においては IdP が対応していない認証を行う場合において, 認証サーバーでの認証結果として IdP にユーザーの ID/Password を送信しなければならない可能性がある. そのためセキュリティリスクや IdP の WebAPI での比較的安全な検証方法の検討を行う必要がある.

6.2　アクセスコントロールモデル

アクセスコントロールモデルでの構成を図 7 に, 考えうる認証フローの例を図 8 に示す. 本モデルでは, ユーザーの保持している権限に対して認証要素を決定する構成になっている. 基本的な流れとしてはユーザーが最初に ID/Password(ID/OTP も可) による認証を行い, その情報を元に IdP から事前に登録されているロール情報が付随された Code が返却される. その後ロール情報を元に認証サーバーは追加の認証が必要かどうかを判断し必要な回数だけ認証と検証を行う. すべての認証において正しいと判断された場合にのみ Code を IdP に渡すことで id_token の発行を行う. 最終的に認証サーバーにおいて id_token に記載されている iss,aud,sub もしくはロールの情報からコンテンツへのリダイレクト URL を変更することでロールごとの任意のページへ遷移する仕組みになっている.

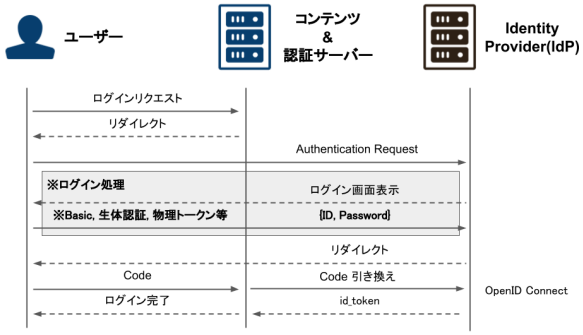

図 6　図 5 における認証フローの例

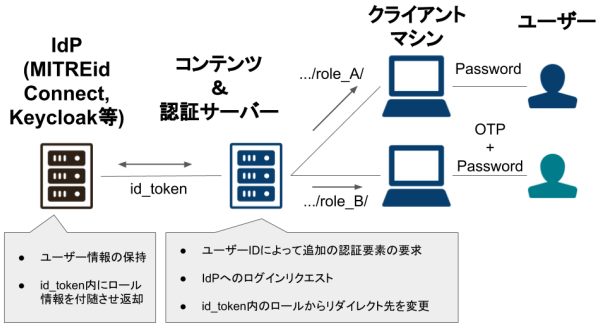

図 7　アクセスコントロールを配慮したモデル

本モデルにおいては, 登録四角で囲まれた範囲内においてロール情報を元に追加の認証が必要か否か判断している. しかし, 判断のタイミングとして提案している通り Code を IdP に渡す前に検証を行うか, 一度 Code を IdP に渡し id_token が返却された後に検証を行うべきかは定かではなく, セキュリティ面でのリスクの洗い出しや技術的な可能性の検証を行う必要がある.

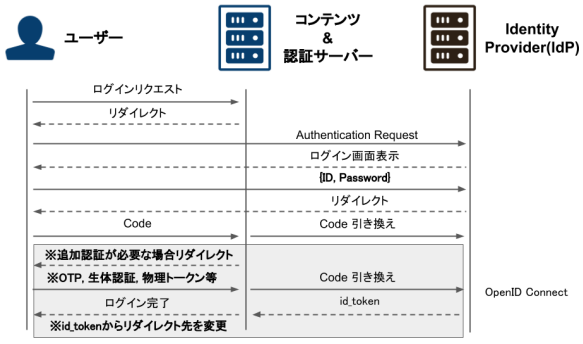

図 8　図 7 における認証フローの例

7. 結論

本研究では, 学内サービスにおいて一般的に Password が用いられているだけではなく, 複数サービスに対しての異なるパスワードを利用しなければならない現状から,SP800-63-3 をもとに安全性の担保とユーザビリティの向上を目指して認証基盤と多要素認証の検討を行った. また, その検討に対して考えられる学内サービスの認証基盤とコンテンツの構成モデルを提案した. 今後は提案したモデルを元に認証フローの検証や認証に必要なモジュールの開発を行う. また, 実際に構築・運用テストを実施し.IdP や RP, 各種認証器が正しく動作するか・学内サービスとして機能するかどうかの評価・実ユーザーに対するユーザビリティ評価・運用者の運用コストの評価を行う予定である.

参考文献

[1] NIST Digital Identity Guidelines 入手先 ⟨https://pages.nist.gov/800-63-3/⟩ (参照 2018-05-14).

[2] 国民のための情報セキュリティサイト 安全なパスワード管理入手先 ⟨http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/staff/01.html⟩ (参照 2018-05-14).

[3] 国立情報学研究所 学術認証フェデレーション 学認 GakuNin 入手先 ⟨https://www.gakunin.jp/⟩(参照 2018-05-14).

[4] 河野圭太, 中村素典. "Shibboleth IdP における LoA を考慮した認証方式グループ化機能の開発." 研究報告インターネットと運用技術 (IOT) 2014.2 (2014): 1-6.

[5] 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." 研究報告セキュリティ心理学とトラスト (SPT) 2014.5 (2014): 1-6.

[6] Yubico — YubiKey Strong Two Factor Authentication 入手先 ⟨https://www.yubico.com/⟩ (参照 2018-05-14)

[7] Shibboleth Consortium 入手先 ⟨https://www.shibboleth.net/⟩ (参照 2018-05-14)

[8] OAuth 2.0 入手先 ⟨https://oauth.net/2/⟩ (参照 2018-05-14)

[9] Welcome to OpenID Connect 入手先 ⟨hhttp://openid.net/connect/⟩ (参照 2018-05-14)

[10] Google Authenticator PAM module 入手先 ⟨https://github.com/google/google-authenticator-libpam⟩ (参照 2018-05-14)

[11] 株式会社日立システムズ SHIELD PBI 指静脈認証サービス入手先 ⟨https://www.hitachi-systems.com/solution/s0307/pbi/⟩ (参照 2018-05-14).

[12] Certified OpenID Connect Implementations, 入手先 ⟨http://openid.net/developers/certified/⟩(参照 2018-05-14).

[13] OpenID Connect Supported by Auth0 入手先 ⟨https://auth0.com/docs/protocols/oidc⟩ (参照 2018-05-14).

[14] KEYCLOAK, Open Source Identity and Access Management 入手先 ⟨https://www.keycloak.org⟩(参照 2018-05-14).

[15] Welcome to MITREid Connect 入手先 ⟨https://id.mitre.org/connect/⟩ (参照 2018-05-14).