紹　　介

学認始めました

永 井 孝 幸[*1]、山 岡 裕 美[*2]
nagai@kit.ac.jp[*1]、yamaoka@kit.ac.jp[*2]

1. はじめに

京都工芸繊維大学は「学術認証フェフェデレーション（学認）」の運用フェデレーションへの参加手続きを 2017 年 5 月に終え、学認で提供される各種サービスを利用できるようになりました。本稿では学認の仕組みと利用できるサービスについて紹介します。

2. 学認とは

学認とは、国立情報学研究所（NII）と大学等の学術機関、学術サービスを提供する大学・企業・出版社によって構成される「学術認証フェデレーション」のことで、各組織のユーザ認証基盤を使って学外の学術サービスを安全に利用できるようにするための仕組みです。

学外のサービスを利用する際、それぞれのサービスにユーザアカウントを登録してパスワードを発行するというやり方は手間がかかるだけでなく、パスワード情報を外部サービスに預けることから、外部サービスで情報漏洩が起きた場合に自分のパスワード情報が漏洩するリスクも抱えることになります。学認の提供する認証連携の仕組みを用いることでこれらの問題を避けることが出来ます［1］。

学認の枠組みでは関係者間の信頼関係が重要になります。学外サービスの提供者（Service Provider, 以下 SP）は各大学のユーザ認証基盤（Identity Provider, 以下 IdP）が適切なユーザ認証を行うことを前提として学術サービスを提供し、各大学は学外サービスのセキュリティが適切に保たれていることを前提としてサービスを利用します。学認上で提供される代表的なサービスに電子ジャーナルがありますが、もし大学の認証基盤が適切に運営されていなければ本来利用資格を持たない第三者が不正に電子ジャーナルにアクセスできてしまうことになります。もし学外サービスのセキュリティが適切に保たれていなければクラッカーなどの攻撃によって乗っ取られてしまい、利用者が気付かずに偽サイトに誘導されてしまうという被害を受けることも考えられます。そのため、学認では認証連携に用いる技術・セキュリティ水準に関して「学認技術運用基準」を定め、基準を満たす機関だけが参加できるようになっています［2］。

2.1 学認を支える技術

サービスを提供するサーバと認証基盤が同じ大学の中に存在する場合は、学内ネットワークに閉じて認証情報をやりとりします。これに対し学認ではインターネットを介して大学の認証基盤と学外サービスの間で認証情報をやりとりするため、認証情報の盗聴や改ざん、詐称に対して強い仕組みを用いる必要があります。

このような要求を満たす認証連携方式として、学認では SAML（ Security Assertion Markup Language ）認証［3］を用いています。SAML 認証ではユーザに関する情報を IdP と SP の間で XML 形式のメッセージとしてやりとりしますが、各メッセージに対して暗号化・電子署名を施すことで盗聴や改ざん、詐称を防いでいます。各 SP はユーザ認証が必要になった時点で IdP にユーザ認証を依頼し、ユーザ認証の結果（ユーザ ID と SP に要求されたユーザ属性）だけを受け取ります。このため、パスワードに関する情報を外部サービスに渡すこと無く認証を行うことができます。また、認証結果として外部サービスに返すユーザ ID には匿名化 ID を用いるのが標準です。匿名化 ID とは本人を特

[*1] 情報科学センター　准教授
[*2] 高度技術支援センター　技術専門職員

定することが困難となるようにハッシュ関数などを用いて生成されたIDのことで、外部サービスの管理者が利用者を特定できないようにするために用いられます。もし学内でのユーザIDをそのまま外部サービスに送り返すと個人特定につながりプライバシーが侵害される恐れがあります。匿名化IDを用いればこの心配はありません。

2.2 運用フェデレーション参加までの道筋

SAML認証に対応した認証サーバの実装はInternet2プロジェクトで開発されたShibboleth［4］が代表で、学認技術運用基準でもShibbolethの利用が推奨されています。最近ではShibboleth以外にSimpleSAMLphp、OpenAM、CAS等のオープンソースソフトウェアでもSAML認証を利用できるようになってきていますが学認技術運用基準を全て満たすには足りない部分があり、学認に参加するにはShibbolethを使って認証サーバを構築することが避けて通れません。

京都工芸繊維大学では2010年度にSystem8を導入した時点で全学の認証基盤としてShibbolethを導入していました。ところが、今回の学認参加までに7年かかっています。これは何故かというと認証連携を実現するには技術要件を満たす認証サーバだけでなく、ユーザアカウントの発行管理や利用規程の整備も含めた組織全体での体制作りが必要になるためです。

体制作りの上で最初の壁になるのが学認で利用するユーザIDの割当てです。先ほど説明したように学認では匿名化IDを用いますが、「同一人物に対して同一の匿名化IDを割当てること」が条件となっています。学認への参加条件を満たすには、学認サービス用の匿名アカウントを新たに全員に配付して使ってもらうことも考えられますが、匿名化IDは覚えにくく、アカウント情報の配付やパスワード管理の手間を考えるとできれば避けたいところです。既存のユーザアカウントでShibbolethにログインし、学認のサービスを使うときには自動で自分用の匿名化IDに読み替えるようになっている方が便利です。そこで、既存アカウントと学認サービス用の匿名化IDの対応表を作ることになります。

現状、情報科学センターのサービスを利用する時は「CISアカウント」を使ってユーザ認証を行っていますが、このCISアカウントは学部生・院生・教員・職員などの「身分」に対して発行されています。このため、学部から大学院に進学したり、TAに採用されたりした時には新しいCISアカウントが割当てられ、1人で複数のCISアカウントを持つことになります。同一人物がどのCISアカウントでログインしても同じ匿名化IDに読み替えられるようにするには、発行済みのCISアカウントがどの人物に対して発行されたものかをデータベース化すればよいのですが、データベース化するには個人を一意に識別するためのIDが必要です。ここでしばらく足踏み状態だったのですが、個人識別用IDとして2015年度末に「統一アカウント」が策定され、CISアカウントと個人の対応付けデータベースを整備するための土台が整いました。この統一アカウントは「生涯メールサービス」のアカウントとして用いるために策定されたものですが、学認用の認証基盤ではこの統一アカウントを元にして匿名化IDを自動生成しています。

次の壁は法律への対応です。国立大学法人の場合、個人情報の取り扱いは「独立行政法人等の保有する個人情報の保護に関する法律」［5］に準じます。学認の場合、サービスによってはユーザ属性として電子メールアドレスを利用しますが、個人が特定できる電子メールアドレスは個人情報に該当するため、利用者に無断で外部サービスに利用することは禁止されています。サービスを利用する前に利用者から明示的に許諾を得る必要があります（いわゆるオプトイン方式）。また法律ではありませんが国立大学においても「政府機関の情報セキュリティ対策のための統一基準」［6］に基づいたセキュリティ対策を行うことが求められており、認証基盤自体のセキュリティ対策だけでなくサービス運用規程の整備も必要です。

学術認証フェデレーションに関する規定として2017年に「学術認証フェデレーション認証連携サービス運営ポリシー」「ユーザ属性情報の外部送信に関する同意取得実施手順」［7］を

定め、「学認技術運用基準」を満たす認証サーバを新たに情報科学センターにて構築しました。既存の Shibboleth サーバを学認に対応させるには統一アカウント情報との連携やオプトイン方式に対応するための改修が必要になりますが、2018 年度から新システム（System10）に切り替わることを考えて今回は新たな Shibboleth サーバを内製することにしました。2017 年 5 月に学認への正式参加手続きを完了し、その後アカウント原簿の整備や認証連携動作の試験を経て 6 月には本学が契約している学認対応電子ジャーナルを利用できるようになりました。また、今回構築した学認用認証サーバを用いることで、人事労務課が実施する「ストレスチェック」において、外部業者の提供する「クラウド型ストレスチェックシステム」の円滑な導入を実現しました。

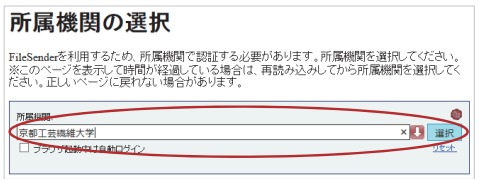
3. 学認連携サービスの紹介

利用できるサービス、利用手順について紹介します。

3.1 国立情報学研究所が提供するサービス

FileSender（ファイル共有サービス）
https://filesender.nii.ac.jp/
対象：本学の教員・職員・学生
サービス内容：大容量ファイル転送サービス
利用手順：
(1) ログインをクリックします。

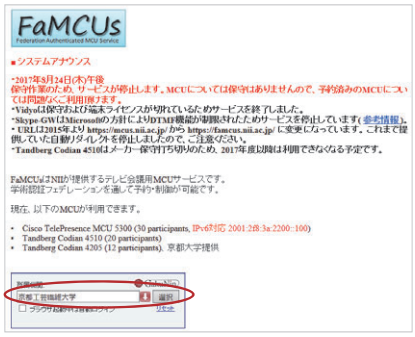
(2) 所属機関の⬇をクリックし［京都工芸繊維大学］を選択し［選択］をクリックします。



(3) 認証情報を入力し、サービスに送信される情報の確認、同意を行います。

(4) ログインが完了しサービスを利用することができます。

FaMCUs（テレビ会議多地点接続サービス）
https://famcus.nii.ac.jp/
対象：本学の教員・職員
サービス内容：テレビ会議用 MCU サービス
利用手順：
(1) 所属機関の⬇をクリックし［京都工芸繊維大学］を選択し［選択］をクリックします。

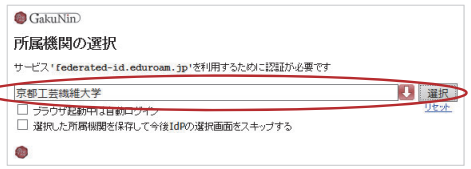


(2) 認証情報を入力し、サービスに送信される情報の確認、同意を行います。

(3) ログインが完了しサービスを利用することができます。

eduroam 認証連携 ID サービス
https://federated-id.eduroam.jp/
対象：本学の教員・職員
サービス内容：eduroam のアカウント発行
利用手順：
(1) ［ログイン］をクリックします。

(2) 所属機関の⬇をクリックし［京都工芸繊維大学］を選択し［選択］をクリックします。



(3) 認証情報を入力し、サービスに送信される情報の確認、同意を行います。

(4) ログインが完了しサービスを利用することができます。

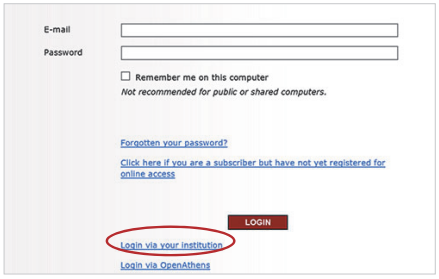
3.2 出版社が提供する電子ジャーナルサービス

以下の電子ジャーナルについて、学認による認証を行うことで学外からの利用時に VPN 接続が不要となります。

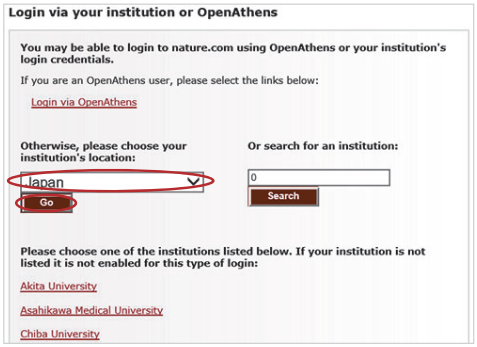
Nature Publishing Group
http://www.nature.com/
対象：図書館利用資格を満たす教職員・学生

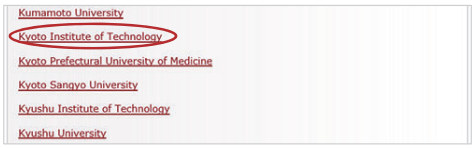
利用手順：
(1) トップページ右上の［login］をクリックします。

(2) ［Login via your institution］をクリックします。

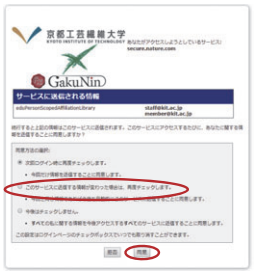


(3)「Otherwise, please…」の項目にて［Japan］を選択し［Go］をクリックします。
［Go］のボタンの下にリストが表示されますので［Kyoto Institute of Technology］をクリックします。



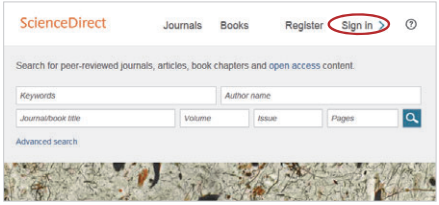


(4) 認証情報を入力し、サービスに送信される情報の確認、同意を行います。

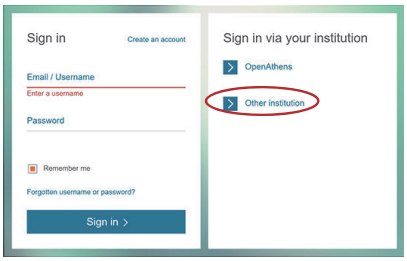


(5) ログインが完了しサービスを利用することができます。

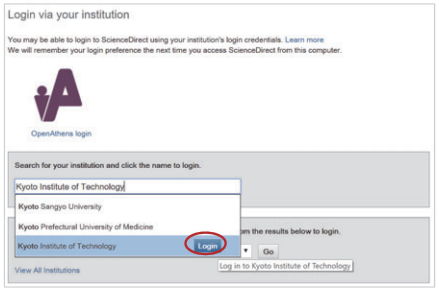
ScienceDirect
http://www.sciencedirect.com/
対象：図書館利用資格を満たす教職員・学生
利用手順：
(1) トップページ右上の［Sign In］をクリックします。



(2)［Other institution］をクリックします。

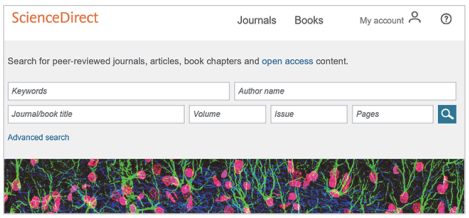


(3)「Search for your …」にて「kyoto」と入力すると［Kyoto Institute of Technology］がリストアップされます。
マウスポイントを当て［login］をクリックします。



(4) 認証情報を入力し、サービスに送信される情報の確認、同意を行います。

(5) ログインが完了しサービスを利用することができます。



Scopus
http://www.scopus.com/
対象：図書館利用資格を満たす教職員・学生
利用手順：
(1) トップページの［所属機関を選択してログイン］をクリックします。

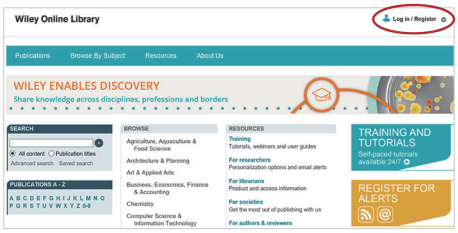
(2)「所属機関を選択し…」にて「kyoto」と入力すると［Kyoto Institute of Technology］がリストアップされます。マウスポイントを当て［login］をクリックします。

(3) 認証情報を入力し、サービスに送信される情報の確認、同意を行います。

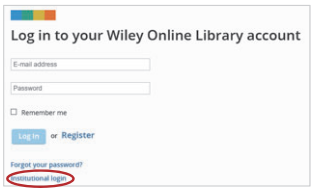
(4) ログインが完了しサービスを利用することができます。

WILEY ONLINE LIBRARY
http://onlinelibrary.wiley.com/
対象：図書館利用資格を満たす教職員・学生
利用手順：

(1) トップページ右上の［Log in / Register］をクリックします。



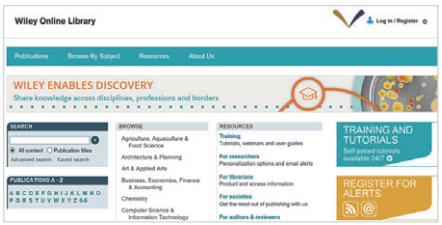
(2)［Institutional login］をクリックします。



(3)「kyoto」と入力すると［Kyoto Institute of Technology］がリストアップされますので選択し［Log in］をクリックします。

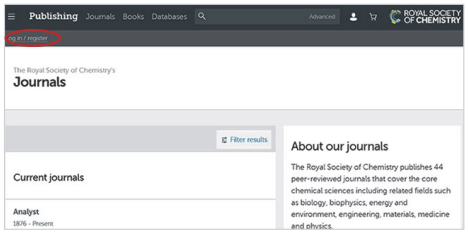
(4) 認証情報を入力し、サービスに送信される情報の確認、同意を行います。

(5) ログインが完了しサービスを利用することができます。

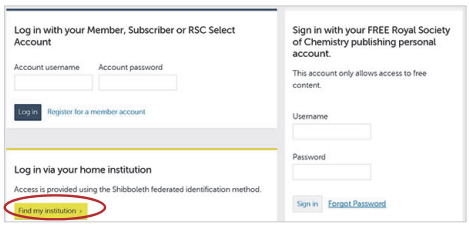


Royal Society of Chemistry
http://pubs.rsc.org/en/journals
対象：図書館利用資格を満たす教職員・学生
利用手順：

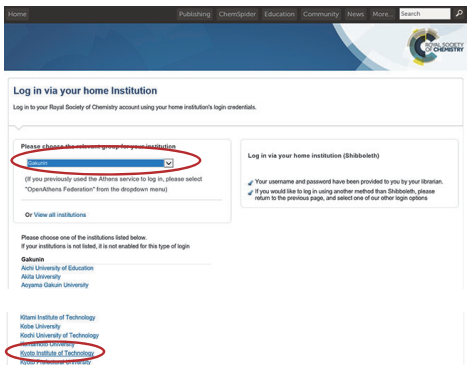
(1) トップページ右上の［Log in / Register］をクリックします。



(2)［Find my institution］をクリックします。

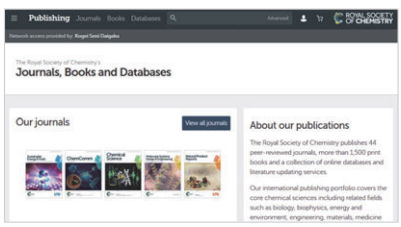


(3)［Please choose …］にて［Gakunin］をクリックすると画面上にリストが表示されますので［Kyoto Institute of Technology］を選択します。



(4) 認証情報を入力し、サービスに送信される情報の確認、同意を行います。

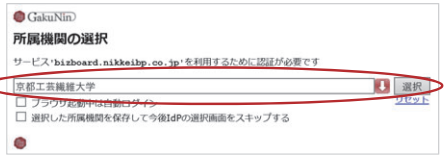
(5) ログインが完了しサービスを利用することができます。



日経 BP 記事検索サービスアカデミック版
http://bizboard.nikkeibp.co.jp/academic/
対象：図書館利用資格を満たす教職員・学生
利用手順：

(1) コンテンツを閲覧するとログインページが表示されます。［学認アカウントで利用する］をクリックします。

(2) 所属機関の⬇をクリックし［京都工芸繊維大学］を選択し［選択］をクリックします。



(3) 認証情報を入力し、サービスに送信される情報の確認、同意を行います。

(4) ログインが完了しコンテンツを閲覧することができます。

3.3　Microsoft 社が提供するサービス

Microsoft Imagine Standard
https://kit-jp.onthehub.com/
対象：Microsoft Imagine 利用資格を満たす教職員・学生

図 1　京都工芸繊維大学用 Microsoft Imagine Web ストア

Microsoft Imagine Standard では Microsoft Azure for Students、Windows Server、SQL Server に加えて Visual Studio 等の開発ツールを利用することができます。Microsoft Imagine Premium ではこれに加えて Windows10 等のクライアント OS、Microsoft Visio、Microsoft Project、SharePoint Server 等の本格的なソフトウェア開発ツールを利用することができます。学生・教職員は教育および研究目的であれば、Microsoft Imagine によって提供されるソフトウェアを自分の PC にインストールすることができます。

ただし、Microsoft Imagine で提供されるソフトウェアは教育・研究目的での利用に限られていることに注意が必要です。事務局・情報センター等での業務利用やインフラとしての利用は認められていません。例えば、学科のメールサーバーやデータベースに用いることはできませんし、商用システムや実稼動システムに用いることもできません。また、教職員についても全員が利用できるわけではなく、科目担当者や非商業的研究のために雇用された者など、教育・研究や学生の技術サポートに関与する教職員に限って利用が認められています［8］［9］。

図 2　Azure for Students で試作した WordPress サイト

Microsoft Imagine にはソフトウェアをオンライン配付するための「ELMS（Electronic License Management System）Web ストア」と呼ばれる仕組みが用意されており、学認を使った本人確認に対応しています。学認の運用フェデレーション参加に合わせて京都工芸繊維大学用の Web ストア（図 1）を開設し、利用資格を満たすユーザが自分でソフトウェアをダウンロードできるようにしました。

Microsoft Imagine Standard の利用資格があれば Microsoft のクラウドサービスである「Microsoft Azure for Students［10］」も無償で利用することができます。Azure の全機能が利用できるわけではありませんが Web サーバやデータベースサーバを構築することができますので、PHP や JavaScript を使った Web アプリケーションを作成するには十分な機能があります。図 2 は動作テスト用に作成した WordPress サイトの画面ですが、このように CMS を使った Web サイトを作ることまでできます。「研究用にちょっとした Web アプリケーションを作る必要があるけれども、サーバまで自分で用意するのは難しい」というような場合に役に立つでしょう。

4.　学認連携サービスの使い方

学認に連携したサービスを利用するには各サービスのログイン用ページにアクセスした後、ユーザ名・パスワードを入力し本人確認を行います。その後、引き続き各サービスの利用規

約・ユーザ属性送信の内容に同意する操作を行う必要があります。(図3)

本人確認から同意までの一連の流れについて、情報科学センター内に設置した動作テスト用サービスを例に説明します

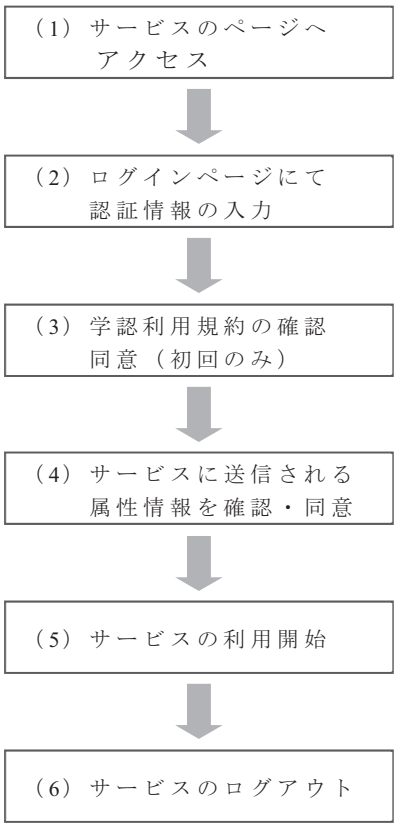
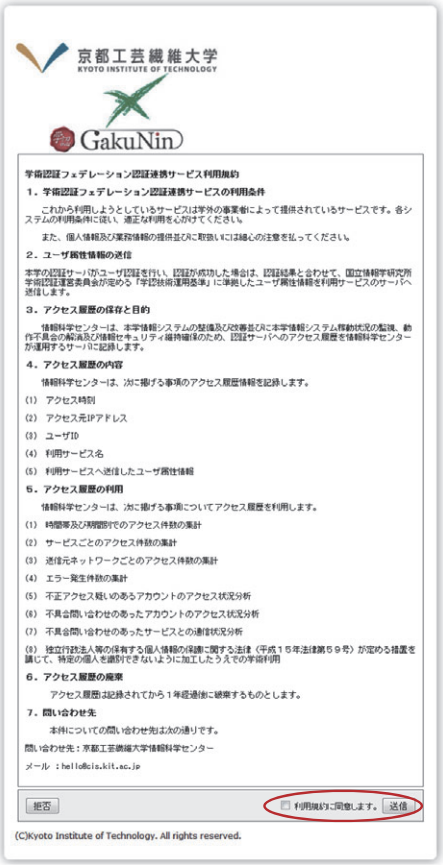


図3　学認連携サービスの使い方の流れ

(1) 動作テスト用サービスにアクセスし[Login Test]をクリックします。
URL：https://idp.cis.kit.ac.jp/

(2) 認証情報を入力します。

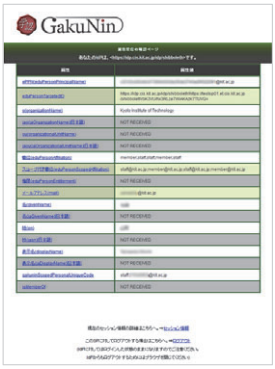
(3) 学認利用規約を確認し同意を行います。「利用規約に同意します。」にチェックを入れ［送信］をクリックします。



(4) サービスに送信される属性情報を確認し同意を行います。初めてサービスを利用する場合、情報の送信に同意するかどうか、また次回ログイン時の確認について選択する必要があります。情報の送信に同意できない場合は［拒否］をクリックします。同意方法の確認については希望

の項目を選択しますが「このサービスに送信する情報が変わった場合は、再度チェックします。」を推奨します。最後に［同意］をクリックします。

(5) サービスの利用を開始します。動作テスト用サービスでは、ユーザ属性を表示する画面に遷移します。



(6) 再度 https://idp.cis.kit.ac.jp/ にアクセスし Logout のリンクをクリックします。

5. 終わりに

2010 年の Shibboleth 導入から 7 年を経て本学でも学認上のサービスを利用できるようになりました。学内の認証基盤を使って学外サービスを安全に利用できるようにする仕組みは、今後インターネット上で提供されるクラウド型サービスを本学の活動に取り入れるうえで不可欠です。SAML 認証に対応した商用サービスには Amazon Web Service、Office365、GSuite、Box、Dropbox、Evernote 等があり、技術的には認証連携設定を追加するだけでこれらのサービスを本学の認証基盤を通じて利用することができます（サービスによっては SAML 認証を利用するための追加料金が必要になります）。

大学の認証基盤を用いてユーザ認証を行うことで、ユーザ本人が学内にいなくても本学に籍を有する者であることが保証できます。学内構成員にだけ利用を認める電子ジャーナルのようなサービスでは、学内ネットワークからのアクセスかどうかで利用を制限する方式がこれまで用いられてきましたが、認証基盤を強化することで学外からでも学内構成員としてアクセスできるようになります。留学やインターンシップなどキャンパス外での活動が増えるにつれて、学内のサービスを学外から安全に利用するための仕組みが重要になっていきます。

2018 年に導入する次期システム System10 では全学の Shibboleth サーバと学認用の Shibboleth サーバを統合して使い勝手をよくするとともに、多要素認証を取り入れたセキュリティの向上も実現する予定です。

6. 参考文献

［1］ Shibboleth による学術認証フェデレーションへの参加メリット
https://www.gakunin.jp/fed/benefit/

［2］ 運用フェデレーション参加手続き
https://www.gakunin.jp/join/production/

［3］ Security Assertion Markup Language（SAML）v2.0
https://www.oasis-open.org/standards#samlv2.0

［4］ Shibboleth

https://www.internet2.edu/products-services/trust-identity/shibboleth/
［5］ 独立行政法人等の保有する個人情報の保護に関する法律
http://law.e-gov.go.jp/htmldata/H15/H15HO059.html
［6］ 政府機関の情報セキュリティ対策のための統一基準、内閣サイバーセキュリティセンター
https://www.nisc.go.jp/active/general/kijun01.html
［7］ 情報科学センター Web「学認」
http://www.cis.kit.ac.jp/gakunin
［8］ 教育機関向け Microsoft Imagine 利用ガイドライン
https://www.microsoft.com/ja-jp/education/imagine-institutions.aspx#guidelinesForInstitutions
［9］ Microsoft Imagine よく寄せられる質問
https://imagine.microsoft.com/ja-jp/institutions/faq
［10］ Microsoft Azure for Students
https://imagine.microsoft.com/en-us/Catalog/Product/99