Vol.2010-IOT-8 No.37
2010/3/2

学術認証フェデレーションに基づくキャンパスネットワークの認証機構

藤村喬寿[†]　田島浩一[††]　大東俊博[††]
西村浩二[††]　相原玲二[††]

近年、モバイル PC の普及等によるネットワークの利用形態の変化に伴って、外出先組織でのネットワークの利用の需要が高まっている。しかし、ネットワークセキュリティ意識の高まりからネットワーク基盤として利用者認証を設ける組織が増えており、会議や共同研究等で訪問した他組織の構成員に対してネットワークの利用者認証を提供するための仕組みが必要となる。本稿ではキャンパスネットワークを利用するため、シングルサインオンのための学術認証フェデレーションに基づき連携する他組織構成員への利用者認証機構を提案する。

An Authentication Mechanism for Campus Networks based on UPKI Federation

Takatoshi Fujimura[†], Kouichi Tashima[††], Toshihiro Ohigashi[††], Kouji Nishimura[††] and Reiji Aibara[††]

These days, public network service is expanding of the mobile computer widely spreads. Especially network service at visited institutions is also increasing among academic research organizations. Even though network authentication provides the secure network infrastructure, it's necessary to support the user authentication not only for own organization members but for visitors. We propose an authentication mechanism for campus networks based on UPKI federation.

1. はじめに

近年、PC は電子メール、文章作成、調べ物、電子コンテンツの閲覧といった機能から、ビジネス、教育、娯楽といった私たちの生活の中心的な存在になっている。これは Web 技術の発展に伴い Web を利用した様々なサービスの展開が PC の機能を拡張し重要性を高めたことが影響している。また、モバイル PC がワークスペースを簡単に持ち運べる利点から広く普及し、外出先での書類の修正や電子メールの確認といった作業に広く活用されてきている。これらの要因により、ネットワークの利用形態は大きく変化し、外出先の組織でネットワーク利用の需要が高まっている。

しかし、ネットワークセキュリティ意識の高まりからネットワーク基盤の一つとして LAN に機器を接続する際のネットワークの利用者認証が一般的になってきているため、会議や共同研究等で訪問した他組織の構成員に対してネットワークの利用者認証を提供するための仕組みが必要となっている。LAN 接続時の利用者認証は、企業内のネットワークのみならず大学等の教育機関においても広く普及している[1)2)]。そのため、事前に利用申請を行い、ゲストアカウントを登録することにより他組織の構成員にネットワークの利用者認証を提供している組織もある。しかしながら、このような事前の手続きは利用者の負担となり、かつ急な訪問を行う場合に利便性が悪いといった欠点がある。その問題に対して認証連携を行うことで他組織の構成員に無線 LAN 環境におけるネットワークの利用者認証を可能にする eduroam[3)]も注目を集めている。

一方で現在、国立情報学研究所が中心となり全国の大学等の教育組織間でシングルサインオン(SSO)のための学術認証フェデレーションが構築されており、多くの組織が Web サービスの利用認証の統一と相互間でのサービス提供のための認証連携を目的として参加している。我々は既に構成員を対象としたネットワーク認証と Web サービスの SSO 化の提案[4)]を行っているが、今回はその拡張として他組織の構成員を対象としたサービスの提案を行う。これにより eduroam と類似の機能に加え、Web サービスの SSO 化が実現できる。

以下では、まず 2 節で関連研究として行われている認証連携技術の現状について述べる。3 節で今回提案する学術フェデレーションに基づくキャンパスネットワークの認証機構の概要について述べる。4 節では広島大学キャンパスネットワークにおける本認証機構の実装計画について述べる。5 節では、まとめと実装における今後の課題について述べる。

[†] 広島大学総合科学研究科
Graduate School of Integrated Arts and Sciences, Hiroshima University
[††] 広島大学情報メディア教育研究センター
Information Media Center, Hiroshima University

Vol.2010-IOT-8 No.37
2010/3/2

2. 認証連携

関連研究として、認証連携技術について述べる。

2.1 シングルサインオン（SSO）

Web 技術発達により様々な Web アプリケーションが普及し活用されるようになり、その存在は欠かすことのできないものになっている。また、それに伴い Web アプリケーション利用の際の認証の機会が増加している。その認証機会の増加による利用者負荷の軽減を実現する技術として SSO 技術がある。

SSO 技術は、認証連携によって一回の認証で利用権限のある全てのサービス利用を実現するとともに、認証情報の一元管理を行うことでユーザが ID やパスワードの複数管理の負荷を解消する。

その注目は高く、多くの研究組織でサービスの開発や、他組織との認証連携の際に問題となってくる利用者のプライバシー保護のための技術 [5]、更には SAML と OpenID といった異なる仕様を用いた SSO システム間での連携方法[6]などが提案されている。

2.2 Shibboleth

組織内サービスの利用者認証に統一されたアカウントが利用される場合、アカウントの管理組織とサービスの管理組織が同一となるため問題はない。しかし、他組織のサービスの利用者認証の際にその統一されたアカウントが利用された場合、アカウントの管理組織ではない他組織へアカウント情報が公開されることになるためセキュリティ上問題である。そこで組織間で認証連携し、他組織のサービスを利用する際に自組織の IdP（Identify Provider）を利用して認証を行うシステムとして Shibboleth[7]がある。

Shibboleth は、SAML を実装した認証のための属性交換のためのオープンソースである。サービスの提供を行う SP (Service Provider) 、利用者認証を行う IdP、SP に対して複数の IdP が存在する場合に IdP のリストの提供を行う DS（Discovery Service）から構成される。SP は共通のサービスの利用ポリシに添った信頼関係を単数または複数の IdP との間で築くことによって他組織の IdP を利用した認証を可能にする。認証の際に IdP は SP に対して認証結果と利用ポリシで決められた最小限のアカウント情報のみ提示する。これによって、統一されたアカウントを利用した他組織サービスの利用認証をセキュアに行うことができる。さらに、全国の大学等と国立情報学研究所の連携で Shibboleth をベースとした学術認証フェデレーションの構築の試みが行われており将来的に実運用レベルで広く教育機関の間での認証連携されることが期待されている。

上記のような理由から、本稿で提案するシステムでは Shibboleth を利用している。Shibboleth の認証手順について図 1 に示す。

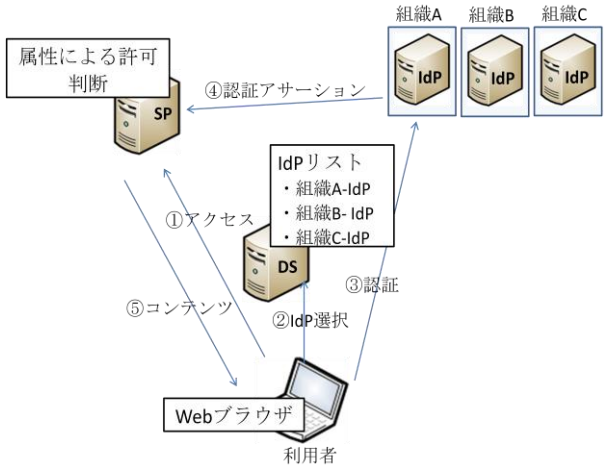

図 1 Shibboleth の認証手順

2.3 eduroam

eduroam は欧州の TERENA で開発された複数の教育研究機関の無線 LAN ローミング基盤として欧州のみならず日本を含めたアジア太平洋地域で広く展開されている。認証連携の仕組みは加入している組織間で RADIUS サーバ (Remote Authentication Dial-In User Service Servers) のプロキシツリーを構成し他組織での認証の際に認証情報を自組織の RADIUS サーバまでプロキシを行い IEEE802.1x を利用した認証が可能になるというものである。

2.4 代理認証方式

eduroam の問題点として規模の増大に伴いプロキシツリーが大きくなり、上位プロキシのシステム停止によるリスクや、プロキシ数の増加によるシステムの認証負荷の増加などの安定性が問題となっている。

この問題点を解決する方法として代理認証方式の提案がされている [8]。その方法は、国内の TOP の RADIUS プロキシといったツリーの上位の認証システムの直下に代理認証システムを設置し、利用者のローミング用のアカウントの発行をさせる。代理認証システムは各機関の認証システムと認証連携することによって、各機関で認証を受けた利用者へのアカウント発行を実現する。これによってプロキシツリーの階層数を減らし安定性を高めるといったものである。

3. 学術認証フェデレーションに基づくネットワークの認証機構

本節では、本稿で提案する認証機構の概要について述べる。

3.1 訪問先組織でのネットワーク利用

近年、各組織で組織のポリシ、ネットワークの状況や利用形態に添ったネットワークの構築がされている。また、セキュリティ意識の高まりから、そのネットワークの基盤としての利用者認証が一般的になっている。そのため、会議や共同研究等で訪問した他組織の構成員へネットワーク認証を提供するためには事前申請といった手続きもしくは、eduroam のような仕組みが必要となっている。

3.2 学術認証フェデレーション

国立情報学研究所の主導で平成 21 年度より全国の大学等と国立情報学研究所の認証連携を目的として学術認証フェデレーション [9]の構築・運用が本格的に開始された。学術認証フェデレーションに加入組織の構成員は統一されたアカウントで学内の Web サービスの利用者認証はもとより学外でも、そのアカウントで利用者認証を行うことが可能になる。これによって、様々なサービスを加入組織間で相互に提供し合うことができため、その展開に広く期待されている。

3.3 提案する認証機構

学術認証フェデレーションに基づくキャンパスネットワーク認証の実現は、フェデレーションへ加入する組織からの訪問者に対し、ネットワーク利用の事前申請等の作業を必要しないキャンパスネットワークの利用者認証の提供し、外出先の組織でのネットワーク利用への強い需要へ応えること可能にする。本提案は、フェデレーションによって認証連携された IdP と、組織内のネットワークの利用者認証システムが自動的に連携して動作することで実現される。他組織からの訪問者は、認証連携された IdP によって認証される。そのため、訪問者はネットワーク認証を行う前に自組織の IdP へアクセスし認証ができるようにする。認証が確認できた訪問者には、一時的にネットワークの利用者認証の可能な状態が提供される。利用者認証が可能な状態は一時的に有効なアカウント(一時アカウント)の発行によって提供され、その後自動的にネットワーク認証が行われることで、訪問者はネットワークの利用者認証が可能になる。

訪問者は自分の組織の IdP にのみ認証情報を送信し認証を行う。そのため自分のアカウントが管理されている組織外へアカウントの情報が漏えいする心配のないセキュアな認証が実現できる。動作を図 2 に示す。

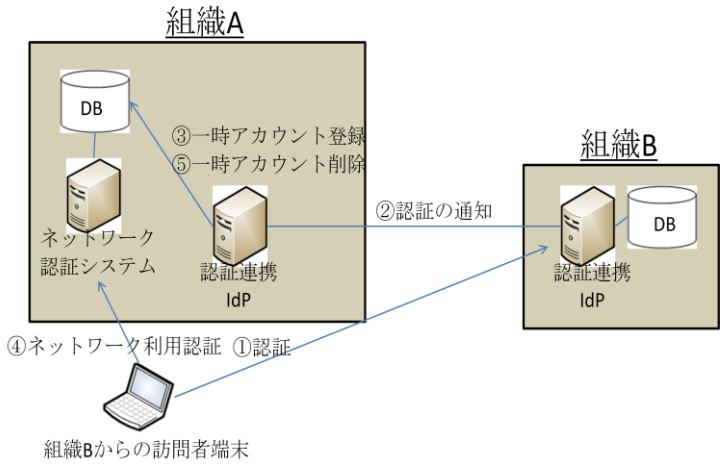

図 2 提案する認証機構

4. 広島大学キャンパスネットワークにおける実装計画

4.1 HINET2007

広島大学では、2008 年度から新キャンパスネットワーク HINET2007（以下 HINET2007）の運用を開始した。HINET2007 は約 2 万人の広島大学の構成員が利用する大規模キャンパスネットワークである。HINET2007 ではネットワークの一元的な管理、運用を目的としてファイアウォールに加え利用者認証もネットワーク側に持たせているため、全学的にネットワークの利用者認証が求められる。

LAN に接続された端末の認証は、各フロアに設置された認証スイッチによって行われる。認証スイッチでの認証は、ネットワークの水際での認証が可能になるとともに、認証要求が集中する始業時間帯でも各認証スイッチで分散して認証処理を行うことで認証の集中を避け、より確実な認証の提供を実現する。

HINET2007 では、認証スイッチの Web 認証機能が利用されている。Web 認証は Web ブラウザが動作する環境であれば OS の種類やバージョンなどに関係なく利用者認証が可能である。大規模なネットワークでは Windows OS や Mac OS、Unix など様々な OS が様々なバージョンが混在しているため OS に依らず、IEEE802.1x 認証のように認証のためのソフトウェアも必要としない Web 認証は運用面での負担の軽減ができる。

また、キャンパスネットワークという特徴から、学生のノート型 PC などの移動型の端末がネットワークに接続する機会が多い。Web 認証では事前登録などが必要なくこのような端末からでもネットワークの利用が可能である。このようなネットワークの利用形態とポリシが考慮され HINET2007 は認証スイッチベースで構成されている。

図 3 に HINET2007 の概要を示す。

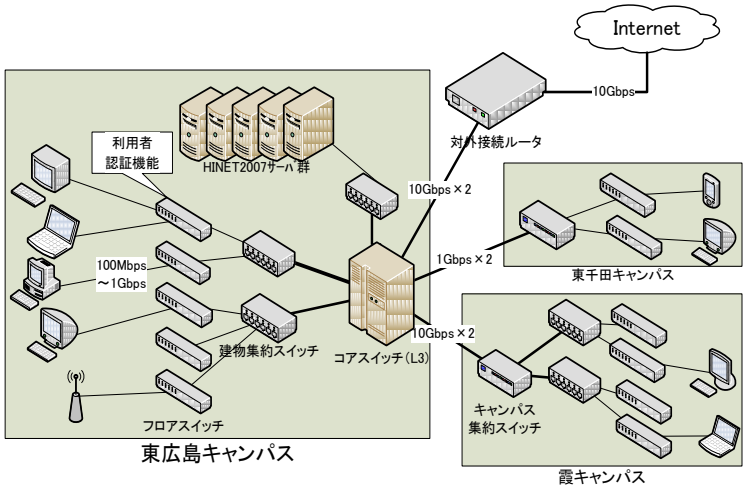

図 3　HINET2007 の概要

4.2 認証システム概要

国立情報学研究所は Shibboleth をベースとした学術認証フェデレーションの構築を行っている。そこで、認証システムを Shibboleth の SP 上で動作させることで認証連携を利用しフェデレーションの加入組織の構成員へのネットワークの利用者認証の提供を実現した。

利用者の認証と利用権限の確認は Shibboleth によって行われる。Shibboleth で認証が確認されると、まず本実装システムは、アクセスにきた利用者の一時アカウントの登録を行う。次に、その一時アカウントの認証情報を認証スイッチに送信するための HTML を Web ブラウザに返し HINET2007 のネットワーク利用者認証を行わせる。このように学術認証フェデレーションに基づいて行う Shibboleth での認証を HINET2007 の認証システムへ自動的に連携させている。

一時アカウントの生成においては、認証スイッチで利用できるユーザ ID の最大文字数である 32 文字という制約から IdP から利用者を特定する要素として提供される eduParsonPrincipalName（以後 eppn）を利用せずに[年 月 日 サーバ ID 利用者カウンタ]といった形式で本システムへのアクセス毎にユニークなものを生成する。パスワードについても同様な理由から 32 文字のものを生成する。以下のように、秘密鍵 K と生成したユニークなユーザ ID から HMAC-SHA256 アルゴリズムを利用してハッシュ値をとり、その上位 32 文字をパスワードとした。

$$\text{パスワード} = \text{上位 32 バイト}\left(\text{HMAC-SHA256}(K, \text{ユーザ ID})\right)$$

このとき、秘密鍵 K を 256 ビットなど十分長くかつ複雑な値にしたならば、たとえ不正利用者が過去に使用されたパスワードを入手出来たとしても新規ユーザ ID に対応するパスワードを作ることを困難にできる。

さらに、利用者のログに生成したユーザ ID と eppn の対応を保存している。これによって、訪問者による HINET2007 のポリシ外利用があった場合に eppn から不正利用者を追跡できる。以下にパスワード、ユーザ ID、eppn の例を示す。

パスワード: jkd0sogm48qmkfkold0gkdif8ogdml4f
ユーザID　: 20100302-FedTest1-12
eppn　　: 0123456@hiroshima-u.ac.jp

4.3 認証システムの動作

学術認証フェデレーションに基づいた HINET2007 の認証についての動作を図 4 に示す。Web ブラウザを通し、以下のような手順で訪問者にネットワークの利用者認証の提供が行われる。

①Web ブラウザが起動すると認証スイッチは SP へのリダイレクトを返す。
②SP は訪問者に自組織を選択させるため DS へのリダイレクトを返す。
③DS は IdP リストの提供を行い訪問者に自組織の IdP を選択させる。
④訪問者は IdP で認証を行う。
⑤IdP から SP へ認証結果が送信される。
⑥SP は一時アカウント登録する。
⑦SP は認証スイッチへ認証情報を送信するためのリダイレクトを返す。
⑧認証スイッチへ認証情報が送信されネットワークの利用者認証が完了する。
⑨SP は登録した一時アカウントの削除を行う。

この間に訪問者は端末の Web ブラウザを起動して自組織を選択して IdP の認証ページで認証情報を入力する操作のみで HINET2007 の利用者認証を行うことができるため、訪問者はその他の動作を意識する必要が無い。

Vol.2010-IOT-8 No.37
2010/3/2

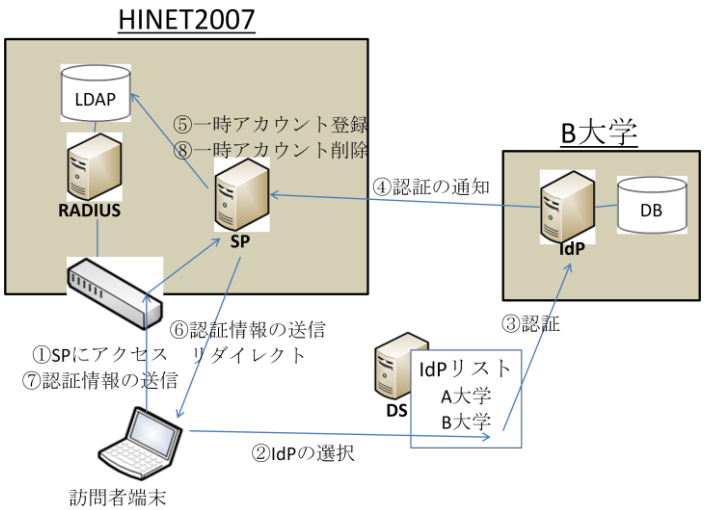

図 4　HINET2007 における実装

4.4 プロトタイプシステム

現在、HINET2007 の実装に向け開発している本システムのプロトタイプの動作について図 5 に示し、表 1 にその測定環境を示す。表 2 に 10 回試行した際の処理時間を示す。

表 1　測定環境

	CPU	Memory	OS
SP/DS	Intel(R) Pentium(R) 4 CPU 1.90GHz	1GB	Cent OS 5.3
RADIUS	AMD Athlon(tm) XP 1800+	512MB	Cent OS 5.3
LDAP	VIA Esther processor 1000MHz	512MB	Cent OS 5.3
IdP	VIA Esther processor 1000MHz	512MB	Cent OS 5.3
利用者端末	Intel(R) Core™2 Duo CPU T8300 2.40GHz	4GB	Windows 7
認証SW	AlaxalA AX3630S-24T		

表 2　認証処理時間

	1	2	3	4	5	合計
最少時間[sec]	0.06	0.36	0.71	0.07	0.05	1.53
平均時間[sec]	0.11	1.06	0.95	0.13	0.06	2.31
最大時間[sec]	0.15	1.20	1.20	0.30	0.10	2.57

実装するにあたって、本システムは多くの利用者からの集中したアクセスを受けることが想定されるため、アクセスの集中時にも確実かつ高速な処理が行えるような実装を行っていく必要がある。

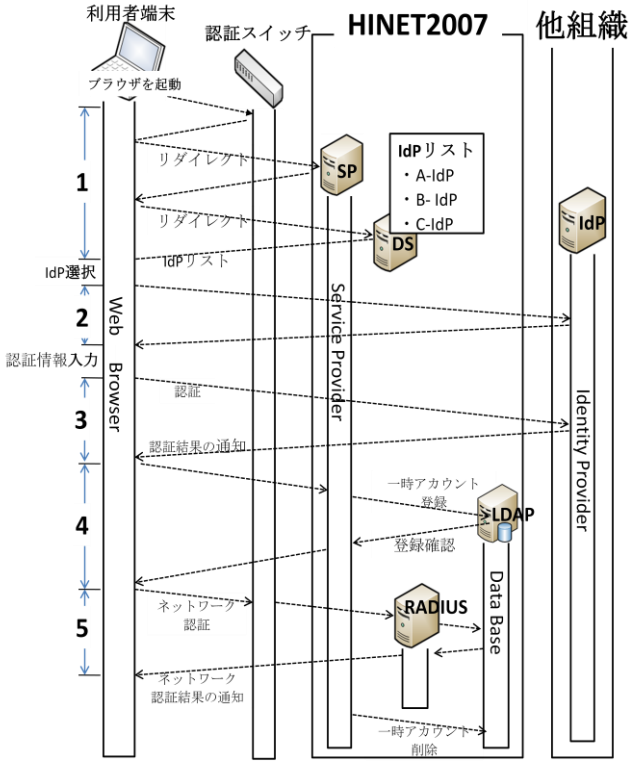

図 5　プロトタイプシステム

5. 終わりに

本稿では、各組織でネットワーク基盤としての利用者認証が一般的になっている現状を踏まえた上で、外出先の機関でのネットワーク利用への強い需要に応えるために学術認証フェデレーションに基づいたキャンパスネットワークの認証機構の提案を行った。本提案は、学術認証フェデレーションを利用しているためフェデレーションに参加している多くの組織に対してキャンパスネットワークの利用者認証の提供を実現するとともに、第 4 節で示した HINET2007 の実装計画のように、本システムは簡単に組織で実装できる。また、学術認証フェデレーションは eduroam のようなツリー状の認証連携の形態ではなく、並列な関係にある連携された IdP がお互いに認証結果を信頼し合うことで認証連携しているため、規模の拡大に伴う安定性の低下がない。セキュリティの点でも、ネットワーク利用のための認証システムと分けて認証連携された IdP を設けることによって訪問者のアカウント情報などのプライバシーに考慮した。

本システムの課題として、学内の構成員情報があるデータベースに対し動的にアカウントの登録・削除を行うことに対しては、ポリシ上の問題があることが多く、システム専用のデータベースの構築などを考える必要などの問題がある。データベースの運用ポリシの問題、システム利用の集中時にも耐えられる実装の実現、訪問者がネットワークを利用する上でのポリシの検討などを十分に行っていくことで本システムの実運用は十分可能だと考えている。

謝辞

本システムの設計と実装ついて議論にご参加頂いた広島大学情報メディア教育研究センターの関係者に心から感謝いたします。

参 考 文 献

1) 相原玲二，西村浩二，岸場清悟，田島浩一，近堂徹，“利用者認証機能を持つ大規模キャンパスネットワークの構築”, 電子情報通信学会 2008 年総合大会 BS-8-7, pp.116-117 (2008).
2) 江藤博文，大谷誠，渡辺健次，只木進一，“Opengate とシングルサインオン”，情報処理学会研究報告書，2009-IOT-4，pp. 69-72 (2003).
3) 国立情報学研究所 ネットワーク運営・連携本部 認証作業部会 eduroam グループ：http://www.eduroam.jp/
4) 藤村喬寿，西村浩二，相原玲二，“大規模キャンパスネットワークにおける SSO 認証の設計と実装”，信学技報，IA2009-60(2009-11)，pp. 13-18 (2009).
5) 大野遼平，岡村真吾，藤沢融，“Shibboleth IdP におけるユーザ主導の属性解放ポリシ管理手法 “，2010 年暗号と情報セキュリティシンポジウム予稿集，3E1-4，CDROM，(2010).
6) 福田裕二郎，伊藤宏樹，横澤成彦，篠田庄司，“シングルサインオンにおける SAML と OpenID の連結手法の考察”，2010 年暗号と情報セキュリティシンポジウム予稿集，3E1-3，CDROM, (2010).
7) Internet2 Middleware Architecture Committee for Education(MACE)Directory Working Group：http://middleware.internet2.edu/dir/
8) 山口一郎，鈴木孝明，大和純一，若山永哉，後藤英昭，曽根秀昭，“セキュアかつ低コストなキャンパスローミングを実現するための代理認証”，信学技報，IA2009-64(2009-11), pp. 37-40 (2009).
9) 国立情報学研究所 UPKI イニシアチブ学術認証フェデレーション：https://upki-portal.nii.ac.jp/SSO