O-018

次世代統合認証基盤の構築に向けた大学サービスの利用環境の解析

Analysis of the use environment of university services for the construction of next generation integrated authentication infrastructure

藤田 翔也†　松平 拓也　高田 良宏　笠原 禎也

Shoya Fujita　Takuya Matsuhira　Yoshihiro Takata　Yoshiya Kasahara

1. 序論

金沢大学(以下，本学という)では，平成 22 年 3 月より金沢大学統合認証基盤(Kanazawa University Single Sign On: 以下，KU-SSO という)を運用している[1][2][3]．KU-SSO は学術認証フェデレーション(GakuNin:以下，学認という)[4]が採用する Shibboleth[5]を利用し，一度のログインで複数の独立したサービスを利用できるシングルサインオン環境(以下，SSO という)及びユーザの属性情報を情報システム間で安全に共有する仕組みを実現している．しかし，KU-SSO と連携する学内の情報サービスが年々増加し，人事給与，財務，評価など，より重要な情報を取り扱うサービスも連携対象となっている現状を考えると，今後，よりセキュアな認証機構の構築が必須である．

現在は，重要度の高いサービスを学外から利用する際には，KU-SSO による認証の前に，使用する ID/PW が異なる VPN 接続を必要とし，この二つを併用することで学外からの悪意あるアクセスを防いでいる．しかし，本学の VPN は，iOS や Android を搭載した端末で利用できない上に，VPN との相性により SP が提供するサービスがうまく動作しない事例もある．さらに，ID/PW だけでサービスによって異なる認証レベルを提供していくことは困難なため，今後ますます増えると考えられる幅広いサービスの提供を可能とする新たな認証機構を検討する段階に来ている．

このような問題意識を背景に，本稿では，本学ユーザの KU-SSO を介したサービス利用状況を，認証ログ情報から解析・評価し，安全で快適なサービスを提供するための多要素認証やリスクベース認証などを備えた次世代統合認証基盤の設計に反映することを目的とする．

2. KU-SSO

2.1 Shibboleth 認証

Shibboleth は主に Identity Provider(以下，IdP という)，Service Provider(以下，SP という)，Discovery Service(以下，DS という)の 3 つのサーバで構成される．IdP は，大学などの組織単位で構成され，ユーザの認証を行うサーバである．また，IdP 自身はユーザの情報を持たず，LDAP などの認証基盤を参照し，特定の情報を抽出して SP へ送信する．SP は，ユーザに対して各種サービスを提供するサーバである．DS は，DS に登録されている組織の全 IdP のリストを提示し，ユーザに自分の所属する組織の IdP を選択させるサーバである．Shibboleth の基本的な認証の流れは図 1 に示す通りである．

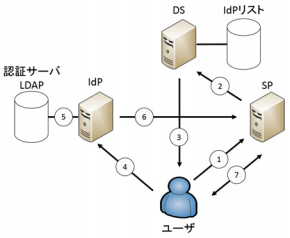

図 1 Shibboleth 認証の流れ

2.2 KU-SSO の概要

本学のユーザが学内の SP を利用する際には，IdP で認証を行う．認証に用いる金沢大学 ID は，常勤教職員・非常勤教職員，学生などを問わず，本学に関わる構成員すべてに付与される生涯 ID である．

本学内で提供される SP 群は，学内からはすべてアクセス可能であるが，給与明細 SP や予算執行支援 SP などの重要度の高い SP は学外からのアクセスを制限しており，VPN を利用するか事前に VPN に接続する必要がある．しかしこれは，一般ユーザにとって，自身が今どのようなネットワーク環境を利用しているのかを認識することが非常に難しい．また序論で述べたように，現状の VPN に様々な技術的課題があることも，問題点の一つである．

3. 大学サービスの利用環境の解析

前述の問題を解決するためには，VPN を利用せずとも多要素認証やリスクベース認証などの技術を利用して，SP の重要度に合わせて認証レベルを段階的に設定し，ユーザが各 SP を利用する際に各 SP が要求する認証レベルをパスできる機構を構築することが望ましい．本研究ではまず，現行システムでユーザがどのようなネットワーク環境で KU-SSO ならびに付随する SP を利用しているのかを把握することを目的に利用状況調査を実施した．解析には KU-SSO の認証に用いられている Shibboleth の IdP ログを使用した．今回使用する IdP ログの属性情報は以下のとおりである．

- requestTime（ユーザがアクセスした時間）
- remoteHost（ユーザがアクセスしたときの IP アドレス）
- relyingPartyId （ユーザがアクセスした SP の URL）
- principalName（ユーザの金沢大学 ID）

上記の情報を用いることで，各ユーザが KU-SSO にアクセスした時間や場所，SP を取得することができる．

解析の結果について示す．なお，2013 年 2 月から 2014 年 2 月までの 13 か月分のログファイルを利用している．

まず，総アクセス数に対するアクセス場所の割合を図 2 に示す．総アクセス数の平均が 501,474 件であるのに対し，学外からのアクセス数の平均は 217,466 件であり，学外からの利用需要も高いことが読み取れる．

† 金沢大学　Kanazawa Univ.

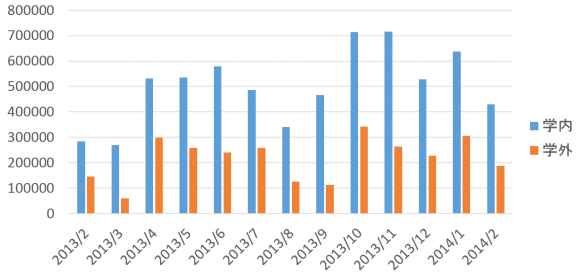

図 2 総アクセスにおけるアクセス場所の割合

次に学外からのアクセスが制限されている予算執行支援 SP について調査した．同 SP へアクセスできるのは，教職員及び非常勤職員である．図 3 の左に予算執行支援 SP への学外(VPN)からのアクセス数を右に総アクセス数を示す．なお，予算執行支援 SP は 2013 年 4 月から運用されているため，それ以降のデータのみを使用している．また，図 4 に 2014 年 2 月における同 SP へのアクセス時間帯の推移を示す．図 3 と同様に VPN からのアクセス時間帯，右に総アクセス時間帯を示している．

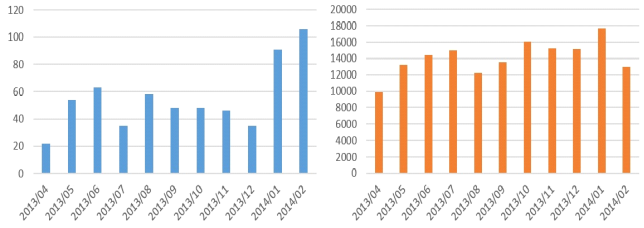

図 3 予算執行支援 SP へのアクセス数

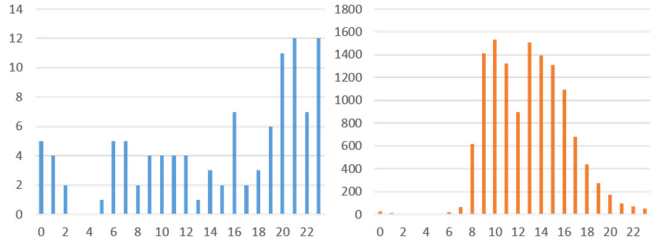

図 4 2014 年 2 月のアクセス時間帯の推移

図 3 において，2014 年 2 月の予算執行支援 SP への総アクセスが 13,000 件に対し，VPN からのアクセスは 106 件であり，割合は 0.82%であった．また，平均して月 12,101 件，2014 年 1 月は 17,674 件のアクセスがあり，同 SP は頻繁に利用されていることがわかる．また，学外(VPN)からの利用が非常に少ないが，徐々に利用が増えていることがわかる．図 4 において，この月の利用者が最も多い 10 時台の総アクセス 1,531 件に対し，学外(VPN)は 4 件であり割合は 0.26%である．しかし，23 時台は 51 件に対し，12 件であり割合は 23.5%である．このことから，学外(VPN)からの利用は夜間に需要があることがわかる．

4. 大学サービスの利用環境の解析の評価

前章で述べた解析の結果について評価する．本学の情報サービスへの学外からの利用需要が比較的高いにも関わらず，学外からのアクセスが制限されている SP については学外(VPN)からの利用がほとんど浸透していないこと，しかしながら夜間を中心に VPN を介したサービスが利用されていることが明らかになった．これは，夜間などの勤務時間外においても学外からのサービス利用は潜在的にあるが，VPN の敷居の高さが利用を阻害していることを示唆していると考えられる．

今後，ユーザのサービス利用の利便性を高めるためには，十分なセキュリティレベルを維持しつつ，学外からの SP へのアクセスを簡便化することが必要であろう．学外からのアクセスにおいて，KU-SSO そのものに多要素認証を導入し，認証のレベルを向上させることで，VPN を利用せずとも予算執行支援 SP などにアクセスできる環境を構築する方法が考えられる．例えば，もともと VPN を介さなくても学外から利用できた SP は今まで通りの金沢大学 ID による認証を行い，予算執行支援 SP などのより高いセキュリティレベルが要求される SP は追加の認証を要求することで安全性を保証する．これにより，制限 SP へのアクセスに対し，冒頭で述べた VPN における技術的難点も克服でき，利用環境を選ばずに行うことができると考えられる．

今回は利用ログからの解析によって，ユーザの利用動向の調査を行ったが，今後は，ユーザが KU-SSO 及び傘下の SP の利用，VPN による利用制限など，現在の環境に対して，どのような印象・要求を持っているのか，アンケート調査などで具体的に把握する必要がある．これらのデータをもとに，各 SP に対する認証レベルの設定や次世代統合認証基盤を構築していく上で，セキュアだけでなく，利便性も考慮した設計を行う必要がある．

5. 結論

本稿では，次世代統合認証基盤の構築に向けた大学サービスの利用環境の解析を行った．Shibboleth 認証のログファイルを用いることで，ユーザの利用状況の調査を実施した．現状の KU-SSO では，学外(VPN)の使用頻度が低いことを示した．しかし，アクセス数は近年増えてきており学外からのアクセス需要が高まっていることや夜間になると利用者が増えることを示した．そこで，多要素認証等を用いることで，iOS や Android など，近年広く普及している端末に対しても対応し，ユーザは利用する時間や環境を選ばすにアクセスでき，よりセキュアで高いアクセシビリティを持った統合認証基盤を構築することが今後の課題と言える．

参考文献

[1] 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)
[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] 松平 拓也，笠原 禎也，高田 良宏，東 昭孝，二木 恵，藤田 翔也，“金沢大学における統合認証基盤の現状と課題”，大学 ICT 推進協議会 2013 年度年次大会(AXIES2013)論文集，W3E-4 (CD-ROM)，(2013)
[4] 学術認証フェデレーション，https://www. gakunin. jp (accessed 2014. 06)
[5] Shibboleth， http://shibboleth. net/ (accessed 2014. 06)