様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

# 科学研究費助成事業　　研究成果報告書

令和　３ 年　 ６ 月　 １ 日現在

機関番号：１３３０１
研究種目：基盤研究(C)（一般）
研究期間：2017～2020
課題番号：１７Ｋ０１０７６

研究課題名（和文）スーパーグローバル時代の大学間連携の展開を担う安全・安心な教育連携基盤の実現

研究課題名（英文）Realization of a safe and secure educational collaboration among universities in the age of super globalization

研究代表者
松平　拓也（MATSUHIRA, Takuya）

金沢大学・総合技術部（情報）・主任技術職員

研究者番号：５０３９７１９７

交付決定額（研究期間全体）：（直接経費）　　3,500,000円

研究成果の概要（和文）：大学の枠組みを超え、地域や分野に応じて大学間が相互に連携し、社会の要請に応えるための活動が盛んになっている。本研究課題では、様々な情報システムを大学間で相互利用する際、各大学における認証方式の多様化・広域化が進む中、大学毎に認証レベルにばらつきが出ることの無いように、認証レベルを維持可能なアーキテクチャを開発し、取り扱う情報の重要度に応じた適切なレベルでの利用者認証が可能な大学間教育連携基盤を目指した。

研究成果の学術的意義や社会的意義
本研究課題を実現したことにより、各大学における認証レベルを適切に維持した上で、大学間におけるシームレスな情報システム群の相互連携を安全・安心に実現できるようになり、大学間教育連携の更なる活性化が見込まれる。

研究成果の概要（英文）：Beyond the framework of one university, universities are collaborating with each other according to regions and fields to meet the demands of society. In this research project, when various information systems are used between universities, even if authentication methods are becoming more diverse at each university, I have developed an architecture in order not to the authentication level will not vary from university to university. The architecture enables user authentication at an appropriate level according to the importance of the information handled.

研究分野：認証連携

キーワード：情報システム　トラストフレームワーク　Federation　Shibboleth　GakuNin

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

大学の枠組みを超え、地域や分野に応じて大学間が相互に連携し、社会の要請に応えるための活動が盛んになっている。連携成果を十分に得るためには、各大学が既に保持している情報システム群を最大限有効活用することが必要不可欠である。しかし、近年、パスワードリスト攻撃の増加に伴い、ユーザ認証方式において最もスタンダードである ID とパスワード（以降、ID/PW と記載）による認証の不正ログインが相次いで報告されている。そのため、最近では、ID/PW 認証に加えて、IC カード認証や指紋認証など ID/PW 以外のもので認証させる「多要素認証」がスタンダードになりつつある。多要素認証方式の種類はオープンソースのものや企業の製品など様々な種類のものが数多く存在する。そのため、各大学における認証方式の多様化・広域化はますます進んでいくと考えられる。

２．研究の目的

本研究課題では、様々な情報システムを大学間で相互利用する際、各大学における認証方式の多様化・広域化が進む中、大学毎に認証レベルにばらつきが出ることの無いように、認証レベルを維持可能なアーキテクチャを開発し、取り扱う情報の重要度に応じた適切なレベルでの利用者認証が可能な大学間教育連携基盤を目指した。

３．研究の方法

本章では，大学が多要素認証を導入する際の基本方針およびその基本方針に基づき実装したアーキテクチャであるリスクベース認証機構の概要について述べる．

(1) 多要素認証導入方針の定義

多要素認証はパスワード認証に比べてセキュアであるが，認証に手間がかかる点と特定の所有物が必要になる点が課題である．そこで，大学が多要素認証を導入するにあたり，以下の 2 点を方針として定義した．

1．サービスの重要度に応じて認証レベルを変更可能

従来の認証レベルで十分なサービスはパスワード認証で対応し，高いレベルを必要とするサービスにおいては，ユーザの利用環境に応じて多要素認証を要求する仕組みとする．サービスの重要度に応じて多要素認証を要求することで、ユーザの利便性を維持しながらセキュアな環境が構築できる．

2．複数の多要素認証方式から選択可能

多様な構成員が在籍する大学において特定の所有物を全員に保持させるのは困難である．そこで，全員に同じ多要素認証方式を指定するのではなく，複数の多要素認証方式を用意し，その中からユーザが選択できるようにする．ユーザが選択できることで，トータルで全構成員が多要素認証を扱える環境を整備できる．

(2) リスクベース認証機構の特徴

上記の導入方針に従い，リスクベース認証機構の実装を行った．リスクベース認証機構の特徴は以下の 3 点である．

1．ユーザの IP アドレスに応じて要求する認証方式を変更可能

リスクの判定には、ユーザのアクセス元 IP アドレスを用いた．例えば，大学内からのアクセスは安全で，大学外からのアクセスはリスクがあると考えた場合，学内 IP アドレスからのアクセスに対してはパスワード認証を要求し，学外 IP アドレスからのアクセスに対しては多要素認証を要求することができる．

2．複数の認証方式を選択可能（or/and 条件）

or 条件は，複数の認証方式から自分が利用可能な認証方式を選択できるようにする方法で，トータルのカバー率を向上できる．例えば，多要素認証方式Ａでの認証が困難な場合でも多要素認証方式Ｂで認証が可能な場合はサービスが利用できる．and 条件は，複数の認証方式を必須にできる方法で，非常に重要な情報を扱うサービスに適用することでセキュリティの向上が可能になる．例えば，多要素認証方式Ａと多要素認証方式Ｂ両方の認証に成功して初めてサービスが利用可能になる．

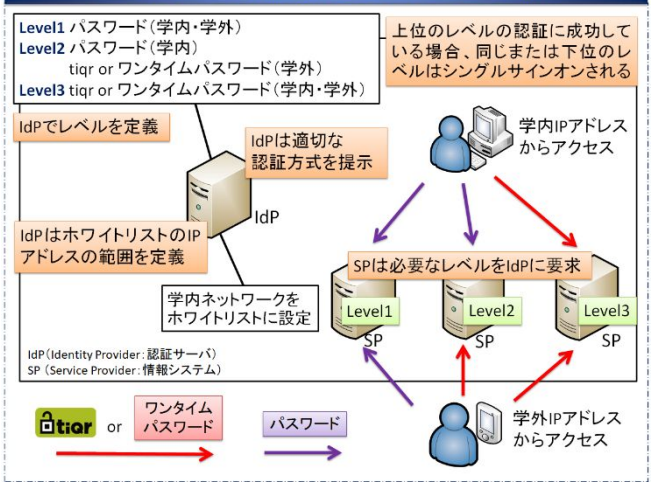
3．認証方式をレベルとして抽象化

1，2 の特徴を組み合わせて，認証方式をレベルとして抽象化できる．例えば，レベルを 1 から 3 までの三段階の設定にして，レベル 1 は全ての IP アドレスからのアクセスにおいてパスワード認証を要求する．レベル 2 は学内 IP アドレスからのアクセスはパスワード認証とするが，学外 IP アドレスからのアクセスは多要素認証Ａまたは多要素認証Ｂを要求する．レベル 3 は全ての IP アドレスからのアクセスにおいて多要素認証Ａおよび多要素認証Ｂの両方を要求する．このように，レベルの階層化および各レベルの動作を定義できるようにした．

(3) リスクベース認証機構の金沢大学への適用

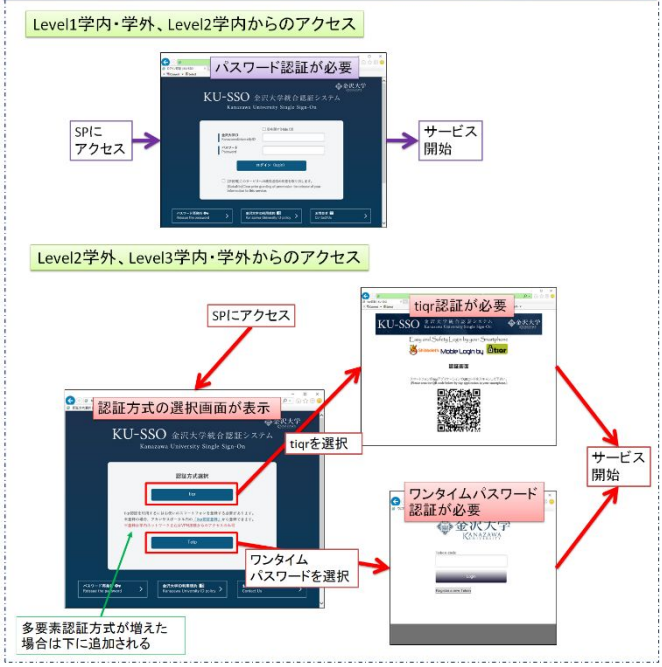
開発したリスクベース認証機構を金沢大学統合認証基盤（Kanazawa University Single Sign On（以下，KU-SSO という））に適用し、大規模環境での動作検証を実施した．本学では，これまで各部署・部局が独立して構築・運用していた情報システムの融合化の一環として，KU-SSO を構築し，ミドルウェアとして Shibboleth と呼ばれるオープンソースソフトウェアを採用し，一度の認証でユーザに許可された情報システムを全て利用可能とするシングルサインオンおよびユーザの属性情報を情報システム間で安全に共有する仕組みを提供している．2021 年 3 月現在，30 以上の学内情報システムが統合認証基盤に対応している．

図1 リスクベース認証機構を導入したKU-SSO概念図




リスクベース認証機構を導入した KU-SSO 環境について説明する．リスクベース認証機構を導入した KU-SSO 概念図を図 1 に示す．図中の IdP は認証サーバ（Identity Provider），SP はサービス提供サーバ（Service Provider）をそれぞれ表す．このように，学内ネットワークを内部と定義し，3 段階のレベルを定義している．各レベルの SP にアクセスした場合のそれぞれの動作を図 2 に示す．レベル 1 を要求する SP にアクセスした場合は，従来どおりパスワード認証を行い，認証に成功した場合サービスを利用することができる．レベル 2 を要求する SP に対して学内からアクセスした場合も同様である．次に，レベル 2 を要求する SP に対して学外からアクセスした場合，およびレベル 3 を要求する SP にアクセスした場合は，このように，認証方式を選択する画面を表示し，ユーザに適切な認証方式を選択させ，ユーザがその認証に成功した場合にサービスを利用することができる．なお，本学で用意した多要素認証方式は，tiqr とワンタイムパスワードである．tiqr はオランダの SURFnet が提供するオープンソースソフトウェアのアプリケーションで，スマートフォン（所有物）と PIN（知識）による多要素認証方式である．このような KU-SSO という大規模な環境において実運用を行い、安定した動作を確認することができ、本アーキテクチャの大規模環境下でのアベイラビリティおよびスケーラビリティを実証できた。

図2 各レベルでの動作




## ４．研究成果

本研究課題において、次世代認証基盤の展開を担う新しいアーキテクチャを新開発し、さらに開発したアーキテクチャの大規模環境下における実証実験を実施した。さらに、実証実験の際、多要素認証方式を複数用意し、重要度に応じたセキュリティレベルの更なる向上を検証し、認証方式の選択肢を増やすことによる、利用者の利便性に配慮したアーキテクチャとしての検証も行った。その結果として、大規模な環境においても本アーキテクチャの安定した動作を実証でき、本アーキテクチャの大規模環境下におけるアベイラビリティおよびスケーラビリティが実証できた。なお、本アーキテクチャは、国立情報学研究所（NII）が中心となって進められ、現在大学間認証連携の主流となっている学術認証フェデレーション（GakuNin）において採用されている Shibboleth と呼ばれるオープンソースソフトウェアをベースとしており、今後は多くの大学・機関が利用できるように進めていく予定である。

５．主な発表論文等

〔雑誌論文〕　計7件（うち査読付論文　2件／うち国際共著　0件／うちオープンアクセス　5件）

| | |
|---|---|
| １．著者名<br>松平拓也 | ４．巻<br>KEK Proceedings 2019-13 |
| ２．論文標題<br>金沢大学における柔軟かつ効果的に多要素認証導入可能な統合認証環境の構築 | ５．発行年<br>2020年 |
| ３．雑誌名<br>技術研究会2020千葉大学報告集 | ６．最初と最後の頁<br>198-199 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>なし | 査読の有無<br>無 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>－ |

| | |
|---|---|
| １．著者名<br>二木恵 , 東昭孝 , 笠原禎也 , 高田良宏 , 森祥寛 , 松平拓也 | ４．巻<br>23 |
| ２．論文標題<br>経年運用から見た金沢大学における緊急連絡システム（C-SIREN）の実績報告 | ５．発行年<br>2020年 |
| ３．雑誌名<br>大学情報システム環境研究 | ６．最初と最後の頁<br>30-38 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>なし | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>－ |

| | |
|---|---|
| １．著者名<br>上杉喜彦,佐藤正英,笠原禎也,大野浩之,高田良宏,井町智彦,森祥寛,東昭孝,NakasanChawanat,二木恵,濱貴幸,西川直樹,松平拓也,松能誠仁,富田洋 | ４．巻<br>(1) |
| ２．論文標題<br>金沢大学総合メディア基盤センターおけるISMS | ５．発行年<br>2019年 |
| ３．雑誌名<br>大学ICT推進協議会2019年度年次大会（AXIES2019）論文集 | ６．最初と最後の頁<br>SF4-6 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>なし | 査読の有無<br>無 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>－ |

| | |
|---|---|
| １．著者名<br>MIYAMOTO Takehiro、KASAHARA Yoshiya、TAKATA Yoshihiro、MATSUHIRA Takuya、HAYASHI Masaharu、MATSUKI Atsushi、UEDA Nozomu | ４．巻<br>28 |
| ２．論文標題<br>Construction of data management system for repository | ５．発行年<br>2018年 |
| ３．雑誌名<br>Joho Chishiki Gakkaishi | ６．最初と最後の頁<br>306～309 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.2964/jsik_2018_306 | 査読の有無<br>無 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>－ |

| | |
|---|---|
| １．著者名<br>仲山 悠也，笠原 禎也，高田 良宏，松平 拓也，東 昭孝 | ４．巻<br>IPSJ Symposium Series Vol.2017 |
| ２．論文標題<br>大学向けリスクベース認証アルゴリズムの検討 | ５．発行年<br>2017年 |
| ３．雑誌名<br>インターネットと運用技術シンポジウム論文集 | ６．最初と最後の頁<br>pp.50-57 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>なし | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>－ |

| | |
|---|---|
| １．著者名<br>宮本 健弘，笠原 禎也，高田 良宏，松平拓也，林 正治，松木 篤，上田 望 | ４．巻<br>Vol.27, No.4 |
| ２．論文標題<br>金沢大学における研究データ公開用リポジトリの構築の試み | ５．発行年<br>2017年 |
| ３．雑誌名<br>情報知識学会誌 | ６．最初と最後の頁<br>pp.337-342 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.2964/jsik_2017_037 | 査読の有無<br>無 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>－ |

| | |
|---|---|
| １．著者名<br>東 昭孝，笠原 禎也，堀井 祐介，高田 良宏，二木 恵，森 祥寛，松平 拓也，佐藤 剛，辻谷 友紀，山中 玲 | ４．巻<br>F6-2 |
| ２．論文標題<br>金沢大学における次世代教務システムおよび次世代全学ポータルシステムの構築 | ５．発行年<br>2017年 |
| ３．雑誌名<br>教育システム情報学会第42回全国大会予稿集 | ６．最初と最後の頁<br>pp.463-464 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>なし | 査読の有無<br>無 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>－ |

〔学会発表〕　計3件（うち招待講演　1件／うち国際学会　1件）

| |
|---|
| １．発表者名<br>Takuya Matsuhira |
| ２．発表標題<br>Realization of an effective multi-factor authentication environment based on risk base in Shibboleth |
| ３．学会等名<br>TNC19（国際学会） |
| ４．発表年<br>2019年 |

| |
|---|
| １．発表者名<br>二木 恵，東 昭孝，笠原 禎也，高田 良宏，森 祥寛，松平 拓也 |
| ２．発表標題<br>経年運用から見た金沢大学における緊急連絡システム（C-SIREN）の実績報告 |
| ３．学会等名<br>第28回国公立大学情報システム研究会(IS研)総会 |
| ４．発表年<br>2020年 |

| |
|---|
| １．発表者名<br>松平　拓也 |
| ２．発表標題<br>金沢大学における多要素認証 |
| ３．学会等名<br>学術情報基盤オープンフォーラム2018（招待講演） |
| ４．発表年<br>2018年 |

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

| | 氏名<br>（ローマ字氏名）<br>（研究者番号） | 所属研究機関・部局・職<br>（機関番号） | 備考 |
|---|---|---|---|

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

| 共同研究相手国 | 相手方研究機関 |
|---|---|