様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２８ 年　 ５ 月 １６ 日現在

機関番号：１３３０１
研究種目：若手研究(B)
研究期間：2013～2015
課題番号：２５７５００８０

研究課題名（和文）ユーザエクスペリエンスを重視した安全・安心な大学間教育連携基盤の実現

研究課題名（英文）Safe and secure authentication mechanism in consideration of the convenience of users

研究代表者
松平　拓也（MATSUHIRA, Takuya）

金沢大学・総合メディア基盤センター・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）　　3,000,000円

研究成果の概要（和文）：近年、大学間で連携して様々な活動を行う機会が増加している。本研究課題では、各大学が保持する様々な情報システム群を安全・安心に相互利用できるための大学間認証連携基盤の実現を目指した。実現に向けて、利用者の利便性を重視しながらも、各情報システムが扱う情報の重要度に応じて適切なレベルでの利用者認証が可能な機構の確立と、現在主流となっているID・パスワード認証よりセキュアな多要素認証に関する研究開発を行った。

研究成果の概要（英文）：In recent years, opportunities for various collaborative activities among universities are increasing. In this research, I aimed at the realization of the authentication infrastructure among universities that users can use information systems held by each university safely and securely. I carried out establishing of the mechanism which can selects the appropriate level of authentication method in accordance with the importance of the each information system in consideration of the convenience of users. And we researched and developed about multi-factor authentication which is more secure than password authentication.

研究分野：組織間認証連携

キーワード：情報システム　Shibboleth　GakuNin　フェデレーション　トラストフレームワーク　多要素認証

１．研究開始当初の背景

近年、大学間で連携して様々な活動を行う機会が増加している。連携して活動を行うために、各大学が保持している Learning Management System (LMS)や履修登録・成績管理などの様々な情報システム群を相互に利用できる、大学の壁を超えたシームレスかつ安全・安心な教育連携環境が求められている。そのためには、機関の違いを意識することなく、ユーザを正しく認証したうえで、ユーザの特性に応じたきめ細やかなアクセス制御が必要となる。

最近では、大学間認証連携基盤として、学術認証フェデレーション(GakuNin)が主流となってきている。GakuNin を利用することで、自大学でユーザを管理することなく、他大学のユーザ認証およびアクセス制御が可能になる。しかし、多くの大学では GakuNin における認証を ID・パスワードで行っている。近年、総当り攻撃の高度化やパスワードリスト攻撃の急増に伴い、ID・パスワードに起因するセキュリティインシデントが多く報告されてきており、もはや ID・パスワードによる認証方式だけでは攻撃の脅威から身を守ることは困難といわざるを得ない状況である。そのため、ID・パスワード認証よりセキュアな多要素認証の導入が焦眉の課題である。但し、多要素認証は一般的にパスワード認証より複雑な認証であり、多要素認証を強いることによるユーザエクスペリエンスの低下が懸念される。

このような背景から、アクセスする情報システムの重要度に応じて認証方式をフレキシブルに使い分けることで、ユーザエクスペリエンスを維持しながらも、守るべきところを確実に守る安全・安心な大学間教育連携基盤の構築が必要になると着想するに至った。

２．研究の目的

本研究では、ユーザの利便性（ユーザエクスペリエンス）を重視しながらも、各大学が保持する様々な情報システム群を安全・安心に相互利用できるための大学間認証連携機構の実現を目的とする。実現に向けて、ユーザの利便性を重視しながらも、各情報システムが扱う情報の重要度に応じて適切なレベルでのユーザ認証が可能な仕組みを目指した。

３．研究の方法

本研究では、主として(1) 認証方式選択機構(Gakunin mUlti Authentication mechanism with Risk-based Decision(GUARD)プラグイン)の開発、(2)多要素認証方式の実装の 2 点を中心に行った。

(1) GUARD プラグインの開発

現在、GakuNin 参加大学の多くは、ID・パスワード（知識）認証を用いているが、知識だけではなく、本人だけが持つ IC カードやスマートフォンなど（所有物）を組み合わせた多要素認証への移行が重要となる。ただし、多要素認証は ID・パスワード認証に比べて認証に手間がかかることや、特定の所有物がないと認証できないなどの留意点がある。そのため、多要素認証を必須とするのではなく、ID・パスワード認証や多要素認証も含めた複数の認証方式の中から情報システムが要求したレベルを満たす認証方式をユーザに提示可能な GUARD プラグインの開発を行った。

本プラグインでは、認証サーバ（Identity Provider（IdP)）において ID・パスワード認証方式をレベル 1、ある多要素認証方式をレベル 2 というように認証方式の強度に応じてレベルを規定する。情報システム(Service Provider(SP))は、自身のサービス利用に必要な認証レベルを IdP に通知する。これにより、従来の認証レベルで十分な SP にはこれまでどおり ID・パスワード認証（レベル 1）で対応する一方、より高いレベルを要求する SP に対しては、多要素認証（レベル 2）を提示することを可能とした。さらに、IdP では IP アドレスのホワイトリストを定義できるように実装した。このことで、SP は信頼できる IP アドレス（ホワイトリスト）からのアクセスではレベル 1、それ以外の IP アドレスからのアクセスには多要素認証（レベル 2）を要求できるリスクベース認証も実現した。

本プラグインの独創的な点として、一度上位レベルで認証に成功した場合、別 SP にアクセスした際に下位または同一レベルの認証を要求されてもシングルサインオンできることが挙げられる。これにより、異なる認証レベルの SP にアクセスする場合においても、できる限りユーザの利便性を維持することができる。また、SP 側の設定において認証レベルを IdP に伝えるだけの最小変更に留めた。そして、認証レベルの定義が未設定の SP が存在していても当該 SP に対してはこれまで通りの認証が行われるため、部分的に本機構を適用することも可能である。さらに、本機構は GakuNin で広く普及している Shibboleth のプラグインとして開発した。そのため、多くの大学で本プラグインを容易に導入可能である。

(2) 多要素認証方式の実装

本研究では、多要素認証方式として、①tiqr 認証、②YubiKey 認証、③UPKI パス認証の 3 つの多要素認証方式を実装した。

①　tiqr 認証

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ある。tiqr はスマートフォン（所有物）と PIN(知識)による多要素認証方式である。スマートフォンのカメラで QR コードをスキャンし、PIN を入力するだけで認証が完了する。スマートフォンは多くのユーザが既に所

持していることから、新規に所有物を配布する必要がないというメリットがある。

② UPKI パス認証

UPKI パス認証は、リーダに IC カードをかざして PIN コードによる認証に成功すると、「クライアント証明書」と呼ばれる電子的な身分証明書を使用したセキュアな認証を行うことが可能となる。また、職員証・学生証が IC カードであれば新規に所有物を配布する必要がないというメリットがある。

③ YubiKey 認証

YubiKey とは、Yubico 社が開発したワンタイムパスワードを生成することが可能な USB デバイスである。YubiKey デバイス（所有物）と ID・パスワード（知識）の多要素認証である。USB キーボードとして動作するため、OS やブラウザに依存することなく利用できるメリットがある。また、YubiKey をタッチするだけという簡単な操作性もメリットである。

想定として、tiqr 認証は学生を、UPKI パス認証は教職員を、YubiKey はそれ以外の構成員をターゲットとした。そして、このように、3 種類の多要素認証方式を提供し、GUARD プラグインにより、ユーザに自分が利用可能な認証方式を選択させることで、トータルとして多くのユーザに多要素認証方式を適用可能となる。

4．研究成果

研究成果として、本研究で開発した GUARD プラグインおよび多要素認証方式を金沢大学統合認証基盤に組み込んだ場合の動作例を説明する。

3 章で説明したとおり、以下の 2 点が重要なポイントとなる。

(1) 複数の多要素認証方式から選択可能

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、ユーザが選択できるようにすることで、トータルで全構成員が多要素認証を扱える環境を実現する。

(2) 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 ID・パスワード認証で対応し、高いレベルを要求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ことで、ユーザの利便性を維持することができる。

図 1 に動作概念図を示す。このように、学内ネットワークをホワイトリストとし、ユーザのアクセス元も考慮して、3 段階のレベルを定義する。レベル 1 を要求する SP にアクセスした場合の動作例を図 2 に示す。このように、従来どおり、ID・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の動作例を図 3 に示す。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。

このように、本学の認証基盤に組み込んだ場合に、正しく動作していることが検証できた。

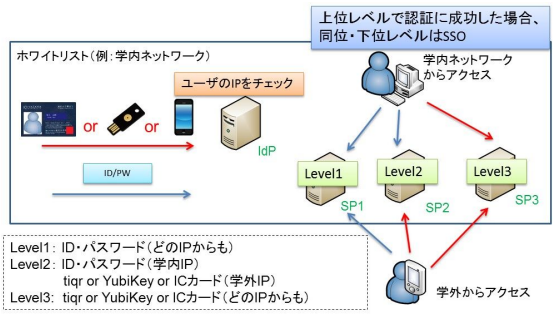

図 1 動作概念図

図 2 Level1 および Level2(学内)アクセス例

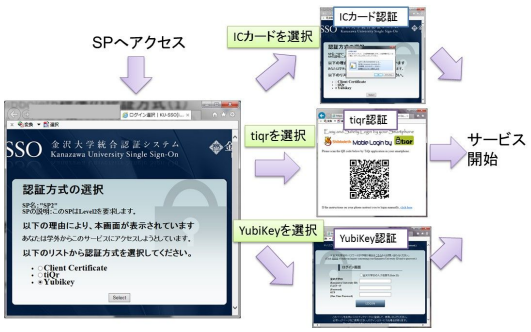

図 3 Level2(学外)および Level3 アクセス例

本研究では、ユーザの利便性（ユーザエクスペリエンス）を重視しながらも、各大学が保持する様々な情報システム群を安全・安心に相互利用できるための大学間認証連携機構の実現を目的とし、ユーザの利便性を重視しながらも、各情報システムが扱う情報の重要度に応じて適切なレベルでのユーザ認証が可能な仕組みを実現した。

今後も、実環境での問題点の洗い出しと改善を重ね、GakuNin におけるスタンダードとなるよう整備を続けていく予定である。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 10 件）

① 東 昭孝, 笠原 禎也, 高田 良宏, 二木 恵, 松平 拓也, 学生の教学支援としてのアカンサスポータルの利用度解析, 査読有, 学術情報処理研究, No.19, 2015, pp.58-67
http://nipc2015.auecc.aichi-edu.ac.jp/contents/pdf/a058.pdf

② 松平 拓也, 中村 素典, 山地 一禎, 西村 健, 高田 良宏, 笠原 禎也, 学術組織間デジタル資料分散共有システム「ARCADE」の開発, 査読有, 情報処理学会論文誌, Vol.55 No.5, 2014, pp.1485-1497
http://id.nii.ac.jp/1001/00101154/

③ 高田 良宏, 東 昭孝, 富田 洋, 藤田 翔也, 松平 拓也, 二木 恵, 笠原 禎也, 金沢大学における情報システム融合化の試み（続報）～情報サービスのワンストップ化から情報流通のワンストップ化へ～, 査読無, 大学 ICT 推進協議会 2014 年度年次大会(AXIES2014)論文集, 2014, T2A-19（電子版）

④ 富田 洋, 岩佐 靖彦, 松原 志野, 東 昭孝, 二木 恵, 松平 拓也, 高田 良宏, 笠原 禎也, 堀井 祐介, パソコン相談カウンターによるワンストップサービスとサポート窓口支援システムの開発, 査読無, 2014 PC カンファレン論文集, 2014, pp.72-73
http://gakkai.univcoop.or.jp/pcc/2014/papers/pdf/pcc086.pdf

⑤ 東 昭孝, 笠原 禎也, 高田 良宏, 二木 恵, 松平 拓也, 森 祥寛, 金沢大学全ポータルシステム（アカンサスポータル）の開発思想と運用状況, 査読有, 大学情報システム環境研究, Vol.16, 2013, pp.23-34

⑥ 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, 査読無, 大学 ICT 推進協議会 2013 年度年次大会(AXIES2013)論文集, 2013, W3E-4 (電子版)

⑦ 藤田 翔也, 松平 拓也, 高田 良宏, 笠原 禎也, "uApprove.jp"を活用した金沢大学と大学コンソーシアム間の認証連携, 査読無, 大学 ICT 推進協議会 2013 年度年次大会(AXIES2013)論文集,2013, T1A-16(電子版)

⑧ 二木 恵, 笠原 禎也, 高田 良宏, 東 昭孝, 松平 拓也, 全学ポータルの多言語化の試み～留学生参加による英語版サイトの改善～, 査読無, 大学 ICT 推進協議会 2013 年度年次大会(AXIES2013)論文集, 2013, W1E-4(電子版)

⑨ 東 昭孝, 笠原 禎也, 高田 良宏, 二木 恵, 松平 拓也, 学内情報システムの融合化～全学ポータルを中心としたデータ連携～, 査読無, 大学 ICT 推進協議会 2013 年度年次大会(AXIES2013)論文集, 2013, T1A-17(電子版)

⑩ 富田 洋, 岩佐 靖彦, 松原 志野, 東 昭孝, 松平 拓也, 二木 恵, 高田 良宏, 笠原 禎也, 堀井 祐介, パソコン相談カウンターによるワンストップサービスの実現 ～プロジェクト管理ソフトウェアを活用した窓口業務の効率化～, 査読無, 大学 ICT 推進協議会 2013 年度年次大会 (AXIES2013) 論文集, 2013, T1A-14(電子版)

〔学会発表〕（計 16 件）

① 東 昭孝, 笠原 禎也, 高田 良宏, 堀井 祐介, 森 祥寛, 二木 恵, 村田 記, 松平 拓也, 富田 洋, 松原 志野, 金沢大学における生涯 ID 管理, 2015 年度北陸地区(国公立）大学情報システム研究会, 2016.1.26, ヴィサージュ（石川県金沢市）

② 馬渕 嵩大, 笠原 禎也, 高田 良宏, 松平 拓也, 山地 一禎, 林 正治, 科学データ解析・公開に最適なデータ公開システムの開発, 平成 27 年度電気関係学会北陸支部連合大会, 2015.9.12-13, 金沢工業大学（石川県野々市市）

③ Takuya Matsuhira, Yoshiya Kasahara, Yoshihiro Takata, Motonori Nakamura, Kazutsuna Yamaji, Takeshi Nishimura, Proposal of introducing multi-factor authentication flexibly, TNC15 Networking Conference 2015, Poster, 15-18 June 2015, Porto(Portugal)

④ 松平 拓也, 大学におけるクライアント証明書利用イメージ, 学術情報基盤オープンフォーラム 2015, 2015.6.11-12, 国立情報学研究所（東京都千代田区）

⑤ 松平 拓也, 安全で使いやすい認証とセキュリティ, ID・認証連携とデータ連携による地域 ICT イノベーション・ワークショップ@金沢, 2015.6.10, 石川県政記念しいのき迎賓館（石川県金沢市）

⑥ 松平 拓也, 大学統合認証基盤における多要素認証について, 平成 26 年度第 2 回学術情報基盤オープンフォーラム, 2015.2.3, 国立情報学研究所（東京都千代田区）

⑦ 松平 拓也, 金沢大学統合認証基盤（KU-SSO）更新に向けた取り組み ～クライアント証明書の活用～」, 第 8 回統合認証シンポジウム, 2015.1.23, 佐賀大学（佐賀県佐賀市）

⑧ 松平 拓也, ID パスワードの限界に備える多要素認証の最新動向, 大学 ICT 推進協議会 2014 年度年次大会 企画セッション:ID パスワードの限界に備える多要素認証の最新動向（W3G 認証連携部会),

2014.12.10, AER（アエル）ビル（宮城県仙台市）

⑨ 藤田 翔也, 松平 拓也, 高田 良宏, 笠原 禎也, 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, 第 13 回情報科学技術フォーラム（FIT2014), 2014.9.3, 筑波大学（茨城県つくば市）

⑩ Takuya Matsuhira, Yoshiya Kasahara, Yoshihiro Takata, Motonori Nakamura, Kazutsuna Yamaji, Takeshi Nishimura, Safe and secure authentication mechanism in consideration of the convenience of users, TERENA Networking Conference 2014, Poster, 19-22 May 2014, Dublin(Ireland)

⑪ 松平 拓也, Shibboleth 用多要素認証導入のための技術ガイド, 学認春 CAMP2014, 2014.5.30, 国立情報学研究所（東京都千代田区）

⑫ Takuya Matsuhira, Method of introducing the multi-factor authentication effectively in university, Lead Facilitator at SIFULAN Workshop on Identity Federation and Eduroam-Shibboleth (EduShib) Global Wifi Roaming, 28-30 April 2014, Kuala Lumpur(Malaysia)

⑬ 笠原 禎也, 馬渕 嵩大, 松平 拓也, 高田 良宏, 後藤由貴, あけぼの VLF 観測データ公開システムの構築計画, 平成 25 年度名古屋大学太陽地球環境研究所研究集会, 2014.3.14. 名古屋大学（愛知県名古屋市）

⑭ Takuya Matsuhira, Motonori Nakamura, Kazutsuna Yamaji, Takeshi Nishimura, Yoshiya Kasahara, Yoshihiro Takata, Development of authentication method selection plug-in of Shibboleth IdP, the Asia Pacific Advanced Network(APAN) 37th Meeting, 20-24 January 2014, Bandung(Indonesia)

⑮ 松平 拓也, Shibboleth における認証方式選択機構の開発, 大学 ICT 推進協議会 2013 年度年次大会 企画セッション:クラウド時代の認証基盤（F2G 認証連携部会), 2013.12.20, 幕張メッセ国際会議場（千葉県千葉市）

⑯ 藤田 翔也, 松平 拓也, 高田 良宏, 笠原 禎也, ユーザ属性情報送付の承認機能を有する認証機能の構築, 平成 25 年度 電気関係学会北陸支部連合大会, 2013.9.21-22, 金沢大学（石川県金沢市）

６．研究組織

(1)研究代表者

松平　拓也（MATSUHIRA, Takuya）

金沢大学・総合メディア基盤センター・主任技術職員

研究者番号：50397197