

AI活用による教育コンテンツ作成評価と組織運用における規格理解

AI Utilization for Evaluating Educational Content Creation and Understanding Standards for Organizational Operation

東洋大学総合情報学部教授 塩野 康徳

Yasunori Shiono, Professor, Faculty of Information Sciences and Arts, Toyo University

ORCID ID : <https://orcid.org/0000-0002-1141-9654>

【紹介論文】

プロンプトエンジニアリングによる要約とペルソナを利用した教育コンテンツ作成評価—組織運用における規格理解を対象とした達成感測定—

塩野 康徳（東洋大学）、山内 透央依（東京工科大学）、志村 俊也（横浜国立大学）

学術情報処理研究, Vol. 29, No. 1, pp. 37-50, 2025.

1. はじめに

人とAIが協働して新たな価値を創造し、様々な分野の課題解決をするための研究が日々なされている。AIの活用に対する期待は、教育や組織運用においても大きいものとなっている。組織のマネジメントにおいては、情報セキュリティやITサービスの管理運営に関する国際的な標準化が進み、国際規格 (ISMS^[1] や ITSMS^[2, 3] など) に基づく組織運用が注目されている。企業だけでなく、大学でも、国際規格に基づく運用の認証取得を得るようになってきており、認証取得のためには、定められた規格に則って取り組まなければならない。また、規格要求事項では、関わる構成員に必要な能力を定め、その能力を確実に身につける適切な教育が求められる。しかしながら、適切な運用体制を構築できなければ、認証取得と認証維持の労力が多くなり、取り組んでいくことが難しくなることがある。教育体制を築くことも組織運用の一部であり、組織構成員の負担軽減と実際の業務との有機的な結び付きが課題となる。そのため、効率的かつ効果的に組織運用における教育を行っていかなければならない。筆者は、ファジィ理論やニューラルネットワークを応用した研究に取り組んでおり、大規模言語モデル (LLM: Large Language Models) や LLM に対するプロンプトを活用して、組織運用に有効なシステムを提案してきた。また、情報教育をはじめとした様々な分野において、AI とファジィグラフを基盤とした応用システムの研究に取り組んでいる。

本稿では、生成AIの活用の中で注目されているプロンプトエンジニアリングによる教育支援に寄与し、組織運用における規格理解を対象とした研究論文(紹介論文)

について解説する。次章以降、論文の概要と注目すべき点や技術について述べる。

2. 論文概要

情報技術が発展し、社会の中でAIを効果的に利用することが求められるようになり、AIを使うのが当たり前前の時代となりつつある。ChatGPTなどのLLMを基盤とした生成AIは、非常に高い文章生成能力があり、人々の日常生活の中に浸透してきている。プロンプトエンジニアリングは、AIを活用するための1つの技術と考えることができ、日常の対話のように指示を入力として与え、AIから価値のある結果を引き出す手法を提供する。その指示は、プロンプトと呼ばれ、プロンプトを効果的に設計することや最適化することがAIの活用には求められ、研究分野としても注目されている。紹介論文では、LLMとしてChatGPT-4o^[4]を使用し、プロンプトエンジニアリングにより、教育コンテンツの作成と評価に取り組んでいる。図1に紹介論文で提案した手法の概略図を示す。コンテンツ作成と評価のためのプロンプトにより、LLMを用いて達成感の要因の度合いなどの有用な出力を得る。そして、達成感の要因の度合いからファジィ推論により具体的な数値で達成感の度合いを求める。このような手法により、組織運用における規格理解を対象として、達成感に基づく教育コンテンツ作成評価をLLMとファジィ理論を用いて行っている。提案手法は、他の対象や別の指標に基づく評価でも有効な手法となり得る。

論文では、規格を理解しやすくするためと、規格の内容を学習する上で学習者の達成感を向上させるために、

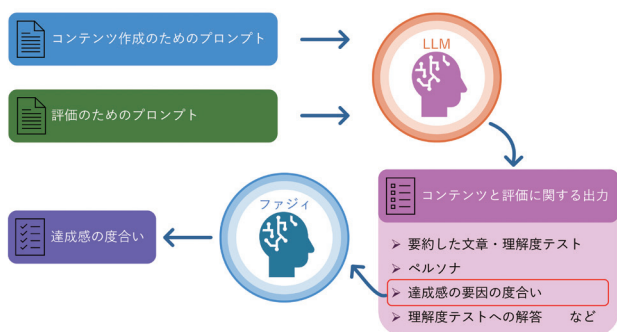


図1 紹介論文で提案した手法の概略図

プロンプトによる文章要約を教育コンテンツとして取り入れている。適切な要約を行い、要約度合いの異なる文章が学習者の達成感にどの程度の影響があるかの把握と評価までを、以下のようなLLMに対するプロンプトにより実現している。

- マネジメントシステムの規格理解のための文章要約
- 学習者となるペルソナの作成
- 理解度テストの作成
- 理解度テストへの解答
- 文章を読んだ時の感情出力
- 達成感の要因の抽出
- 達成感の要因の度合いの出力

理解度テストや達成感の要因抽出などの教育コンテンツの評価は、実際の人ではなく、プロンプトにより作成した読書習慣の異なる3人のペルソナを対象に行っている。ペルソナとは、実在の人物のように認識される架空の人物像のことで、ターゲット像やユーザモデルとして意思決定や開発などで用いられる^[5, 6]。達成感の要因については、論文中の各参考文献の達成感についての記述から29個を選定し、独自に考えたものとなっている。そして、達成感の要因となる感情の度合いから、ファジィ推論により達成感を具体的に数値化している。要因の度合いと達成感とは「低い」、「普通」、「高い」の3つとし、推論規則は、2つの要因の度合いから達成感を導き出せるように定めている。

評価結果では、プロンプトによる達成感に関する各要因の度合いの出力を10回行い、集約してそれらの結果と変化をまとめている。複数回の出力を行っている理由は、プロンプトにより出力される結果が毎回同じになるとは限らないためである。これらの評価結果に基づき、要約と達成感と教育効果についての考察をしている。また、出力の統計的な結果を示し、プロンプトエンジニアリングによる手法についての考察も行っている。

結論として、ペルソナにより学習者像を想定することで、学習体験を学習者に応じて模擬的に確認でき、要約

による達成感の向上に寄与する要因を導くことができた。これらは、想定した学習者に応じた対応や教材提供の一助となると考えられる。

3. ファジィ理論による達成感の測定

教育において、学習者が達成感を得ることは、学習意欲の向上と苦手意識の軽減に結びつくが、明確な測定方法が確立されているわけではなく、様々な要因が考えられる。そこで、ファジィ理論を用いて達成感とその要因を数量化している。ファジィ理論は、あいまいさを定量的に扱う理論であり、メンバーシップ関数と呼ばれる関数により、0から1の間の実数の値で度合いを表すことができる。そして、ファジィ推論により2つの要因から具体的な達成感の度合いを導いている。2つの要因にした理由は、推論規則が複雑にならず、簡潔に記述しやすくなるからである。また、複数の2つの要因の関係性を見ることで、3つ以上の要因も考察できるためである。推論規則についても、複雑にせずに直感的にわかりやすいように9通りとしている。ファジィ推論は、制御や医療診断に应用されており、大規模なシステムだけでなく、家電製品にも利用されている知的情報処理の1つである。

ファジィ推論の推論規則では、「もし～なら～である(IF-THEN)」という形式の規則(ルール)を用いており、このような定められたルールに基づいて推論するAIは、ルールベースのAIに分類できる。ChatGPTなどのLLMは、大量のデータを学習することで構築されたモデルであり、ニューラルネットワークが基盤のディープラーニングを用いたAIに分類できる。ルールベースでは、そのルールを見るとどのような推論が行われているか理解しやすい。論文では、ファジィ理論に基づいた推論により、達成感などの感覚的な概念を数値で扱い、理解しやすいルールを用いている。近年では、ディープラーニングを用いたAIが注目されているが、ルールベースの手法と組み合わせる用いられることもあり、ファジィ理論についてもあいまいさが扱える知能として、現代のAI技術との協調や融合が進んでいる。

4. 教育支援におけるAI活用の実践的知見の提供

論文では、LLMによる生成AIを用いて、プロンプトエンジニアリングとペルソナ生成による教育コンテンツの作成と評価手法を提案している。プロンプトを利用

する際に注意しなければならない点は、出力結果が毎回同じになるわけではない点であり、出力のたびに異なることが多い。似たような出力である場合もあれば、かなり内容が変わって出力されることもある。妥当な出力となっていればよいが、厄介なことに、間違った出力となっていることもある。これはハルシネーションと呼ばれる現象であり、AIが現実にはないこと、不正解や誤った情報をあたかも正解や正しい情報のように生成してしまう現象である。事実にないことを実際にあったかのように語ることや、存在しないものがあるものとして説明するなど、ユーザからしてみると正しいかどうか判断が難しいものも多い。このような問題を解決するための研究もなされているが、完全になくすことは現時点ではできていない。すべてが適切な出力となるわけではなく、このような現象が起こる前提で考える必要があり、AIリテラシーとしてもその点は注意しなければならない。

そのため、要因の度合いを出力するプロンプトにより評価を行う際に、同じプロンプトで10回出力し、要因の度合いとして平均値を求め、各要因における変化をまとめている。出力された度合いを確認すると、予想はしていたが、同じ度合いで毎回出力されるわけではなかった。一度の出力では適切な値かどうかの判断が難しいので、複数回の結果から導き出せばより妥当な結果が得られると考え、統計的にもそのばらつきを示すことにした。その結果、要因により大体の傾向があり、極端に出力が異なることは少なかった。このように複数回のプロンプトの出力を用いることは、生成AIの利用の方法として、より信頼できる出力として扱える可能性がある。

ペルソナの作成については、複数回のプロンプトを利用したわけではなく、想定する学習者像を指示して出力した結果を用いている。3人のペルソナを作成し、作成されたペルソナを確認すると、マネジメントシステムの規格理解の教育を行う対象として考えられるものとなっていた。したがって、そのまま出力された3人のペルソナに対して、評価に関するプロンプトを10回出力させている。このように、ペルソナにより学習者像を想定した教育のシミュレーションにあたるようなことをプロンプトで実施している。

10回の出力の中では、達成感の要因の度合いの数値部分以外に、その要因がなぜそのくらいの度合いであるかの理由やコメントも同時に出力されている。論文中で一部示しており、要約により要点が理解しやすかったなどの結果が得られた。例えば、「簡潔にまとめられているため、忙しい日々の中でも内容を理解できることに

ほっとした。」などの出力がされていた。これらの内容も教育支援の視点から見て参考になるものと考えられる。あたかも実際の学習者が要約した文章を読み、回答しているように見えるのも、LLMによる生成AIが注目されている理由であり、それらの内容を確認するのも有益なものとなるだろう。

プロンプトを用いてペルソナとして学習者像を想定することで、学習体験を学習者に応じて模擬的に確認できることを示した。これは、本論文における注目点の1つであり、教育におけるコンテンツの作成と評価、そのシミュレーションが一貫してプロンプトにより実現できるということである。実際の学習者に対してこのようなことを実施する場合、労力がかかり、規模も大きくなるだろう。しかしながら、本研究で示したような方法であればそれらが削減でき、プロンプトによるAIの出力で確認できるので、比較的容易に結果を見ることが可能であるので、様々な学習者を想定した教育コンテンツ作成評価が行える。

5. マネジメントシステムの規格理解を対象とした定量的な分析

提案している教育コンテンツの作成と評価手法の対象としては、組織運用において求められるマネジメントシステムの規格理解としており、達成感を指標として効果を定量的に分析している。言語モデルに対するプロンプトを利用した要約とペルソナを利用した達成感の測定を取り入れ、マネジメントシステムの導入や運用に役立つ教育コンテンツ作成評価を行っている。

プロンプトによる要約を教育コンテンツとして取り入れており、要約した文章がどのような学習者に有効であるかを、実際の学習者に提示する前に提言することが本手法によりできるようになる。教育効果を高めるためには、理解のしやすい文章を教育で用いることが考えられ、達成感の向上につながる可能性がある。そこで、文章量を減らし理解しやすいように要約できれば、教育効果と達成感が向上すると考えた。要約がどのような学習者に有用であるかを、実際の学習者に読んでもらい確認するのは手間もかかり、明確な基準があるわけではない。特にマネジメントシステム運用における教育では、規格の理解が求められ、定められた用語や意味をきちんと把握する必要がある。そのため、要約するには用語や意味が変わらないように注意しなければならない^[7]。適切な要約を行い、その要約文章が学習者の理解や達成

感にどの程度の影響があるかを把握することが重要となってくる。

要約では、内容が正しく要約されるような指示もプロンプトで与えており、要約度合いとして、50%、30%、10%に要約した文章と、要約していない文章を含めた4種類の文章を評価に用いている。プロンプトによる理解度テストの作成では、要約前の文章を用いている。作成した理解度テストの解答では、4種類の文章を3人のペルソナに読んでもらいそれぞれの解答結果を確認している。要因の度合いを出力するプロンプトによる評価でも同じように、4種類の文章を各ペルソナに読ませている。

定量的な分析として、29個の要因に対する度合いの変化を示し、変化が示された5つの要因に注目して、度合いが最も増加した要因と最も減少した要因を対象として達成感の比較を行った。また、注目した要因のうち1つについて、ばらつき具合を箱ひげ図で示し、平均、最大、最小、標本分散、標準偏差についても各要約文章と各ペルソナについてまとめた。

6. AIによるペルソナを用いた評価

ペルソナによる評価では、各ペルソナ個人で文章を読んで自己評価している。他者との関わりなどはペルソナの想定で明示的に示しているわけではないが、結果を確認すると暗黙的な社会的文脈が表出化された可能性があるのは興味深い。

一部の例を挙げると、「規格書の内容を仕事のプロジェクトで活かし、チームに良い結果をもたらすイメージが湧き、未来の成功に期待感を持った。」と出力されていたが、これは仕事の中での他者との成功について表出化された結果といえる。また、要約におけるポジティブな効果が窺える結果も得られた。さらに、主体性を持って取り組んだような結果も見られ、AI活用による評価での主体性に関する評価結果が得られたと考えることもできる。

7. おまわり

本論文における達成感の定義とペルソナを用いたプロンプトによる評価により、達成感の数値とその要因を示すことができるようになる。また、プロンプトによるLLMの出力結果では、要因の度合いの理由なども一緒に出力される。これらの数値や理由などの記述を基に教育教材の作成や学習者への対応を考えることで、教育効

果を高めることが見込める。教育コンテンツとしては、要約した文章と理解度テストをプロンプトにより作成した。本研究では、マネジメントシステムに関する教育を対象に、LLMに対するプロンプトによる要約とペルソナを利用した達成感の測定を取り入れ、マネジメントシステムの導入や運用に役立つ教育コンテンツ作成評価方法の提案を行った。

規格理解を対象としているが、提案手法は様々な対象の教育支援として有効であると考えられる。具体的な実現方法、結果や教育効果に関する考察の詳細は、本稿で紹介した論文を参照していただきたい。本論文が少しでも読者にとって有益になることを切に願い、今後の教育の発展、組織運用、AI活用に寄与することを期待したい。

2025年12月18日

参考文献

- [1] ISO/IEC 27001: 2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements(2022)
- [2] ISO/IEC 20000-1: 2018, Information technology — Service management — Part 1: Service management system requirements (2018)
- [3] JIS Q 20001-1 (ISO/IEC 20001-1) 情報技術—サービスマネジメント—第1部：サービスマネジメントシステム要求事項, 日本規格協会 (2020)
- [4] Hello GPT-4o. <https://openai.com/index/hello-gpt-4o/> (2025年10月23日参照)
- [5] 原辰徳, 土井博貴, 渡辺健太郎, ほか: サービス工学のためのペルソナ概念を用いたシナリオモデリング, 第14回設計工学・システム部門講演会講演論文, pp.320-323 (2004)
- [6] 別宮玲, 三井和男: 対話型遺伝的アルゴリズムによる実在人物のように感じられるペルソナデザイン, 知能と情報(日本知能情報ファジィ学会誌), Vol. 32, No. 1, pp. 653-662 (2020)
- [7] 塩野康徳, 志村俊也: 分散プロンプトエンジニアリングに基づく規格関連文章のための動的要約, 学術情報処理研究, Vol. 28, pp. 174-181 (2024). DOI: https://doi.org/10.24669/jacn.28.1_174

【著者略歴】**塩野 康徳**

東洋大学総合情報学部教授。2010年 東洋大学大学院工学研究科博士後期課程修了，博士（工学），2010年 東洋大学総合情報学部助教，2014年 横浜国立大学情報基盤センター研究教員，2015年 横浜国立大学情報基盤センター助教，2017年 横浜国立大学情報戦略推進機構講師，2022年 東京工科大学コンピュータサイエンス学部講師，2025年から現職。グラフ理論とファジィ理論の応用，ファジィグラフ，データマイニング，知能情報，数理情報，情報教育に関する研究に従事。

「Shibboleth IdP V5におけるPasskeysの種別による認証可否の判定」による認証保証レベルの厳格化への第一歩

The First Step Toward Strengthening Authentication Assurance Levels Based on “Authentication determination based on the types of Passkeys in Shibboleth IdP V5”

茨城大学情報戦略機構准教授 野口 宏

Hiroshi Noguchi, Associate Professor, Institution for Information Management and Strategy, Ibaraki University
ORCID ID : <https://orcid.org/0009-0000-5496-3070>

株式会社 DTS 榎原 勇人

Hayato Sakakibara, DTS Corporation
ORCID ID : <https://orcid.org/0009-0001-4362-5348>

国立情報学研究所 アーキテクチャ科学研究系助教 清水 さや子

Sayako Shimizu, Assistant Professor, Information Systems Architecture Science Research Division, National Institute of Informatics
ORCID ID : <https://orcid.org/0009-0002-8469-5833>

【紹介論文】

Shibboleth IdP V5 における Passkeys の種別による認証可否の判定

榎原 勇人 (株式会社 DTS), 清水 さや子 (国立情報学研究所), 野口 宏 (茨城大学)
学術情報処理研究, Vol. 29, No. 1, pp. 130-140, 2025.

1. はじめに

このたびは、論文誌「学術情報処理研究」に掲載された我々の論文^[1]について、機関誌「AXIES Trajectory」において紹介の機会を与えて頂き、関係者の皆様に深く感謝申し上げます。

近年、ID とパスワードによる認証は攻撃の対象となることが多く、その対応策としての多要素認証も広く利用されるようになってきた。しかし、すぐに多要素認証も攻撃の対象となり、根本的な対策として Passkeys が注目を浴びている。Passkeys は公開鍵暗号方式を採用しており、自身の秘密鍵の所持形態により、Synced Passkeys と Device-bound Passkeys に分けられる。この区別により認証における強度が異なっている。この強度は NIST SP 800-63B-4^[2] において認証保証レベル (AAL: Authentication Assurance Levels) として定められており、前者のレベルは 2 (AAL2)、後者は 3 (AAL3) となっている。このレベルを区別して認可するサイトが増えてくると思われるため、紹介論文は、認証を行う IdP (Identity Provider) においてそれらを区別できるような仕組みが必要と考え、実装したことを報告したものである。

2. 紹介論文の目的

認証、認可、認証フェデレーションを行うシステムとして、日本の学术界では Shibboleth が広く利用されている。国立情報学研究所 (NII) が全国の高等教育機関を取りまとめている認証連携基盤である「学認」では認証情報の交換のために SAML (Security Assertion Markup Language) を採用し、SAML を利用するためのミドルウェアとして Shibboleth を利用している。学認への参加機関が多いことも、Shibboleth が広く利用されている理由と考えられる。Shibboleth 環境下のシステムにおいては、ID 情報を保持し、それら ID に対する認証を行う IdP と、認証された ID に対してサービスを認可・提供する SP (Service Provider) に分けてサービスが利用できるようになっている。更に、複数のサービスが IdP に認証機能を委ねる認証フェデレーションの環境を構築することが可能となっている。認証を行う Shibboleth IdP での Passkeys の対応は、2024 年 12 月に提供が始まった Shibboleth IdP V5 のプラグイン WebAuthn version1.0.0^[3] において行われたばかりであり、Passkeys の機能を部分的に可能とするものである。そのため、Passkeys の区分による認証強度の違いまで区別できておらず、フル実装までの課題は多い。

しかし、NIST SP 800-63B において AAL が定めら

れ、指定された AAL によって認可を決める SP が遠くない将来に数多く出てくることが予想される。その場合は、IdP 側で AAL に従った認証を行う必要がある。そこで、紹介論文では、IdP 側で認証強度に従った認証が可能となるよう Passkeys の区分による認証の区別を行えるようにした。つまり、AAL2 を指定されていれば Synced Passkeys で、AAL3 を指定されていれば Device-bound Passkeys で認証するよう Shibboleth IdP V5 のプラグイン WebAuthn の改良を行い、更に、改良を行った際の現行の Shibboleth IdP への改良点を示唆することが紹介論文の目的である。

3. 認証保証レベル(AAL)

NIST SP 800-63B では、従来の認証で利用されていた ID とパスワードの組という知識情報は認証における必要最低限のものという観点から認証保証レベルを 1 (AAL1) としている。知識情報は狙われやすく、また漏洩してしまうこともあるため、知識情報要素に加えて、所持情報や生体情報という要素を利用して認証を行う多要素認証が普及している。認証保証レベルという観点からは ID とパスワードの組よりも高いものと考えられるため、レベル 2 (AAL2) と考える。また、Passkeys は、公開鍵暗号方式を活用し、パスワードを利用しない。秘密鍵をユーザの手元の認証器に置き、公開鍵をサービス提供者側に置いた上で認証を行う。サービス提供者側に置いた鍵は公開鍵であるため、パスワードと異なり漏洩したとしてもそれを利用して認証を成功させることはできない。これらのことから、Passkeys の認証保証レベルはレベル 2 以上と考えられる。Passkeys はユーザ自身が複数の認証器を所有することを想定し複数の認証器で秘密鍵を同期して利用できる Synced Passkeys と、認証器から秘密鍵を取り出すことができない Device-bound Passkeys に分けられる。前者は ID とパスワードの組より認証における保証レベルが高いためレベル 2 と考えられ、後者は認証器から秘密鍵を取り出すことが出来ないという点で前者よりもレベルの高いレベル 3 (AAL3) と考えられる。

学認では次世代認証連携への取り組み^[4]を進めており、ID とパスワードの組による認証から一段高い認証基準である AAL2 の運用を進めている。基本方針としては「多要素認証器 1 個またはパスワード認証に所持要素に基づく認証器を組み合わせたもの」という要件を採用している。また、現在 AAL2 の認証に利用できる認証器を登録した学認認証器レジストリを構築し、順次

更新すると共に公開している^[5]。AAL2 と AAL3 は特に区別はしていないが、AAL3 となる Device-bound Passkeys を利用するためには耐タンパ性を持ったハードウェアトークンの利用や、Windows Hello のように TPM2.0 を利用する必要があるため、いずれのレベルかは容易に弁別できる。

現時点では AAL2 と AAL3 を区別している事例は少ないが、今後多くの SP においてレベル区別の需要が出てくると予想できる。そのため、まずは IdP において AAL2 と AAL3 を区別した認証可否の判定ができることが必要となる。

4. 認証の可否

Passkeys を利用した際に認証保証レベルに対応しようとする場合、認証器がいずれのレベルに対応したものか、つまりいずれの Passkeys に対応したものかを知る必要がある。全ての認証器には AAGUID (Authenticator Attestation Global Unique Identifier) が割り当てられており、これをキーとして基本的には図 1 のように、個々の認証器に関するメタデータが Passkeys Developer から提供されている aaguid.json^[6]に登録されている。紹介論文では、これを利用して認証器がいずれに対応しているかを判断している。なお、FIDO Alliance から提供されているメタデータサービス (MDS) は提供されているメタデータが少ないため、aaguid.json を利用した。

Shibboleth IdP 上での認証は、図 2 に示した通り、通常の FIDO 認証に加えて認証器から得られた情報を Web ブラウザ経由で Shibboleth IdP に提供 (フロー 10 ~ 11) し、それを受けた Shibboleth IdP では AAGUID を取得、aaguid.json から Passkeys の種別を取得した後に認証等による検証を行なう (フロー 12

```
1: "ea9b8d66-4d01-1d21-3ce4-b6b48cb575d4": {
2:   "name": "Google Password Manager",
3:   "icon_dark": "data:image/svg+xml;
   base64,PHN2ZyB4bWxucz0iaHR0cDov...",
4:   "icon_light": "data:image/svg+xml;
   base64,PHN2ZyB4bWxucz0iaHR0cDov...",
5:   "type": "synced"
6: }
```

図 1 認証器のメタデータの例

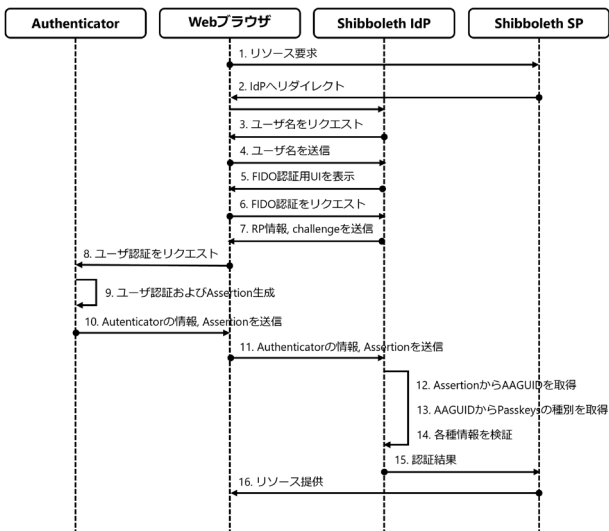


図2 認証フロー

～14) ことにより認証保証レベルへの対応を確認している。

5.実装

実行環境を構築するにあたり、動作の軽量かつ高速性および再生成が容易であることから Docker コンテナを利用した。システム構成は図3に示した通りであり、閉じた環境下で実行が可能のようにまずはリバースプロキシを用意し、加えて Shibboleth IdP, LDAP, Shibboleth SP をコンテナとして用意した。これらのコンテナは、全て同一の Docker Network に属している。また、実行するにあたっては、表1に示した5つの認証器を利用して検証を行っている。

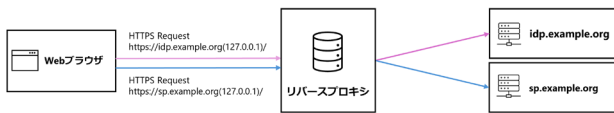


図3 検証用システム構成

表1 使用した認証器

Name	Provider	Key Type
YubiKey 5C	Yubiko	Device-bound
Titan Security Key	Google	Device-bound
Windows Hello	Microsoft	Device-bound
Google Password Manager	Google	Synced
Proton Pass	Proton	Synced

以上の環境を実現し、認証強度レベルに従った認証を行うことの実証を行なった。加えて、Shibboleth IdP への Passkeys の登録の際も認証強度レベルを意識できるものとしており、利用者にとって分かりやすく認証強度レベルにあった認証が可能となっている。

6.おわりに

紹介論文により認証強度レベルに合った認証が可能となったが、Shibboleth IdP にとどまった認証である。国立情報学研究所では AAL2 の運用に係る実証実験を行うことを計画^[7]しており、そこでは認可の際に SP から IdP に対して認証強度レベルを要求し、IdP ではそのレベルにあった認証を行うようにすることも計画の一部となっている。このように認証強度レベルに対応した認証フェデレーション環境を構築する必要があると考えている。また、認証器のメタデータとして、今回は aaguid.json を利用した。登録されていない認証器もあり、必要な場合は各 Shibboleth IdP の管理者に依頼して登録を行う必要がある。しかし、各管理者の負荷と人的な登録ミス等を避ける必要があると考えるため、一箇所で管理を行い、そのデータを共有する仕組みが必要と考える。

本稿で紹介した研究をさらに進めることにより、状況に応じたより安全な認証環境を提供できるようになり、Shibboleth IdP の管理の負荷が少しでも軽減されることを期待する。

2025年12月22日

参考文献

- [1] 榑原勇人他：Shibboleth IdP V5 における Passkeys の種別による認証可否の判定, 学術情報処理研究, Vol.29, No.1, pp.130-140 (2025)
- [2] NIST: NIST SP 800-63B-4, 2025, <https://doi.org/10.6028/NIST.SP.800-63b-4>, (閲覧日 2025年12月15日)
- [3] Shibboleth Atlassian: Identity Provider Plugins/ WebAuthn, <https://shibboleth.atlassian.net/wiki/spaces/IDPPLUGINS/pages/3395125387/WebAuthn>, (閲覧日 2025年1月27日)
- [4] 国立情報学研究所 学術認証運営委員会 次世代認証連携検討作業部会：AAL2 の新学認での運用に当たって (案), <https://www.gakunin.jp/document/661>, 2022年6月9日
- [5] 学認：学認 AAL2 認証器レジストリ, <https://level2.gakunin.jp/>, (閲覧日 2025年1月29日)
- [6] Passkeys Developer: passkeydeveloper/passkey-authenticator-aaguids, <https://github.com/passkeydeveloper/passkey-authenticator-aaguids/blob/main/aaguid.json>, (閲覧日 2025年1月27日)
- [7] 国立情報学研究所：次世代認証基盤における IAL2・AAL2

の運用に係る中規模実証実験のご案内,
<https://www.gakunin.jp/news/20251208/>, (閲覧日 2025
年 12 月 15 日)

【著者略歴】**野口 宏**

1986 年中央大学工学部数学科卒業。1988 年筑波大学大学院経営・政策科学研究科修了。1988 年茨城大学工学部情報工学科助手。2005 年 12 月茨城大学 IT 基盤センター講師。2018 年 4 月茨城大学 IT 基盤センター准教授。2022 年 4 月より茨城大学情報戦略機構准教授。博士(工学)。コンピュータ及びネットワークシステム構成、認証基盤、ID 管理、情報セキュリティなどの教育・研究に従事。情報処理学会、日本データベース学会、各会員

**榊原 勇人**

2023 年茨城大学工学部情報工学科卒業。2025 年茨城大学大学院理工学研究科博士前記課程修了。2025 年 4 月より株式会社 DTS。認証基盤、ID 管理などの研究に従事。情報処理学会 会員

**清水 さや子**

2015 年京都大学大学院情報学研究科博士後期課程単位取得退学。2018 年同学位取得。博士(情報学)。立命館大学文学部卒業後、民間企業でシステムエンジニアを経て、2005 年東京海洋大学情報処理センター(現、総合情報基盤センター)技術職員。2011 年同技術専門職員。2021 年より国立情報学研究所助教。認証認可、教育研究 DX 基盤の研究に従事。電子情報通信学会、情報処理学会、各会員