

CAS ベースの RDM 認証・認可機構の漸増開発と アセスメント評価

菊地 伸治¹ 内藤 裕幸¹ 門平 卓也¹ 谷藤 幹子¹

受付日 2020年8月17日, 再受付日 2020年11月8日/2020年12月20日,

採録日 2021年1月26日

概要: 国立研究開発法人物質・材料研究機構における Research Data Management (RDM) は、多様な研究領域を支える多様で異質な計測・研究システム群間のデータ交換・流通・管理・利活用を支援して研究データのライフサイクルを管理することを指向している。シングルサインオンに関する要求実現のため、認証機構には Central Authentication Service (CAS) を採用し、認可実施のため、人員・組織マスターデータ管理と統合して実装されている。多様で異質なシステム群間のデータ交換・流通を実現するためには、認証・認可機構自身が多様な認証方式・認可資源を統合的に扱う HUB の役割を負う必要がある。E-Science, Scientific Workflow と連携する RDM では新たに急伸している領域故に、種々の試行錯誤も見受けられ、成熟化に向かう Service Oriented Architecture (SOA) におけるセキュリティフレームワークとは異なる様相に映る。本稿では、未だ発展途上ではあるがケーススタディとして物質・材料研究機構における RDM に組み込まれた認証・認可機構の概略、設計上の変遷（認可管理との連携・名寄せ・多重化・API 管理）を概説するとともに、SOA におけるセキュリティフレームワークで簡易アセスメントを実施、そこで見出される差異について評価・考察を述べ、RDM における認証・認可機構に関する理解の一助とする。

キーワード: 研究データ管理, 認証・認可

Applying Incremental Delivery Process in developing CAS based Authentication and Authorization Mechanism in RDM and its Assessment

SHINJI KIKUCHI¹ HIROYUKI NAITO¹ TAKUYA KADOHIRA¹ MIKIKO TANIFUJI¹

Received: August 17, 2020, Revised: November 8, 2020/December 20, 2020,

Accepted: January 26, 2021

Abstract: Research Data Management (RDM) at National Institute for Materials Science has been developed to support a whole of activities in life cycle of research data, such as exchanging, distributing, managing and utilizing them among various and heterogeneous measurement and research systems for various research areas. Accordingly, Central Authentication Service (CAS) is adopted as the authentication mechanism and enhanced by integrating with the human resource and organization master data management for authorization to fulfill the native requirements for single sign-on. In order to realize data exchange and distribution among these systems, the authentication and authorization mechanism itself must act as the role of HUB that handles various authentication methods and authorized resources in the integrated manner. Due to natures in arising area newly linked with E-Science and Scientific Workflow, various trials could be naturally adopted in RDM, and this looks so different from the matured security framework in Service Oriented Architecture (SOA). As a case study, this paper presents the outline of the authentication and authorization mechanism incorporated in the RDM at National Institute for Materials Science, including the transition during design phases. Along with an overview, a brief assessment is carried out with the security framework in SOA, and we also review the differences found there for characterizing the authentication and authorization mechanism in RDM.

Keywords: RDM, authentication and authorization

1. はじめに

材料科学分野では近年、世界規模で Material Informatics と呼ばれる材料科学とデータ科学を融合した取り組みが進展している。Material Informatics とは、蓄積された膨大な実験データ、計算機能力の向上により算出可能となった膨大な計算データを入力として統計学、パターン認識等のデータ解析技法を用いてプロセスと特性間、異なる特性間に成り立つ法則性を抽出・発見・予想する、さらにはテキストマイニングで得られる大量データに機械学習や深層学習の AI 的处理を加えることで材料探索する、を含んで新たな材料開発を加速することを含意する [1], [2], [3]. 「第四の科学手法」の提唱から 10 年以上を経過した今日、類似の動きは材料科学分野に限らず Cyber-Physical-Society-System として概念化され、新たに一般化されたパラダイムとして定着・進展してきている。広く散在する大量なデータをシステムティックに収集・集積のうえ、機械学習の適用により新たな知見を獲得する当該パラダイムはクラウドコンピューティング・機械学習の成熟化に伴い、ますます深化している [4], [5], [6]. その結果、研究開始の創出期から実用に向けた適用応用期までに創出される一連の研究データをシームレス・高品質に管理・提供できる研究データ管理プラットフォームの構築と実現が分野横断に要求され、世界規模で進展している [7], [8].

以上の背景を受けて国立研究開発法人物質・材料研究機構では、材料科学にかかわる各種データを ‘つくる’, ‘ためる’, ‘使う’, ‘公開する’ という 4 機能が相互に関係した Material Informatics 環境の実現に向けて材料データプラットフォームの構築を進めてきた [9], [10]. この中では多様で異質な計測・研究システム群を用いて実施される実験/シミュレーション等の研究活動の結果として産出される研究上の一次データを組織的に管理する RDM の設計・実装が中心課題の一つである [11]. すでに初期版の設計と実装を終え、実際の研究現場への適用・定着化・改善に向けた強化に重心が移っている。多様で異質な計測・研究システム群間のデータの交換・流通のためには、RDM に対してシングルサインオンの実現が重要な要求事項となる。特に認証・認可機構自身が潜在的に、多様な認証方式、認可資源を統合的に扱い、人員組織マスタ管理と統合化した HUB の役割も求められる。このため、[12], [13] で記されたように国内外の研究機関で採択実績のある Central Authentication Service (CAS) を採用のうえ、認可機構実現のために人員・組織マスタデータ管理と統合して実装、当該機構の要求に合致する強化拡張を施してきた。

以上のように実装が進んでいる RDM であるが E-Science, Scientific Workflow と連携する形で新たに急伸している領域ゆえに種々の試行錯誤も含み、十二分に成熟しているわけではない。これは組み込まれた認証・認可機構でも同様である。これに対して Enterprise 系の業務システムのサービス化ではシングルサインオンを実現する認証・認可機構への要求は進展・定着し、SOA におけるセキュリティフレームワークの一要素としてすでに成熟化段階にある。このため RDM における認証・認可機構の実装では、そのようなフレームワークから種々咀嚼のうえ、方針を策定しながら、具体的なソリューションへマッピングする必要がある。妥当な開発プロセスで実装することが求められる。本稿では発展途上を前提に、物質・材料研究機構における RDM に組み込まれた認証・認可機構の概略、漸増型プロセスモデルで設計・実装を進めた際の変遷（認可管理との連携・名寄せ・多重化・API 管理）を一つのケーススタディとして概説する。そのうえで、SOA におけるセキュリティフレームワークで簡易アセスメントを実施、そこで見出される差異について評価・考察を述べる。材料科学分野以外の方針への応用も考慮して RDM 構築における認証・認可機構に関する理解の一助とする。

以下、本稿の構成を述べる。続く 2 章ではシステム全体の背景・構成を概説する。3 章では CAS を用いた認証・認可機構の構成について概説する。本稿の最も重要な章である 4 章では、当該プラットフォームにおける認証・認可機構とその周辺機能の開発に漸増型プロセスモデルを適用した発展過程を概説し、総括を行う。5 章では RDM に関連の深い E-Science, Scientific Workflow 領域における認証・認可機構の位置付けを概説の後、SOA におけるセキュリティフレームワークの概説と筆者らの実装への簡易アセスメントを行う。その後、この対比による差異について評価、分析、考察を述べる。6 章では本稿の貢献点を示し、結言とする。

2. システム全体の背景・構成と認証・認可機構の位置付け

2.1 システム全体に関する背景・要求事項

本章では認証・認可機構を含むシステム全体に関する背景・要求事項について概説する。当該機構における RDM は、当該機構固有の要求に基づき、既存もしくは先行する GakuNin RDM [14] 等のサービスを適用せず、当該機構内で管理する材料データプラットフォーム基盤上に展開・運用している。これは複数の理由に基づく。第一は GakuNin RDM は全国の大学・研究機関への汎用サービスの提供を指向しているゆえに広学域な連携を指向するのに対して、当該機構の RDM では種々計測・実験システムと直接連携する必要や、より専門性の高い材料科学分野を扱う必要があり、狙い・機能の点で一致していないこと、第

¹ 国立研究開発法人物質・材料研究機構 (NIMS), 統合型材料開発・情報基盤部門 (MaDIS)
National Institute for Materials Science (NIMS), Tsukuba, Ibaraki 305-0044, Japan

二は導入～開発時期に重複があり、GakuNin RDMの本格的なサービス開始を待ってから当該機構に適用する場合、時期に関して許容できない等、のプロジェクト管理上の理由である。さらに産業財産権に基づくデータ保護に対するコンセンサスが成熟していない段階で当該機構の管轄外にデータを配置するリスクも否定できない。このため当該機構では材料科学分野に特化したRDMを構築するとともに、先行するGakuNin RDMを主管する国立情報学研究所との組織的連携の下、GakuNin RDM実装を通して習得した設計・運用上の知見の教授を受ける方針で進めてきている。これに基づき当該機構のRDMを構築するにあたりGakuNin RDMで評価・採用されたOSSであるOpen Science Framework (OSF)[15]の適用がプロジェクトの当初段階から検討され、当該機構固有の要求に応じたカスタマイズ開発を含んで構築することがシステム全体の背景事項となっている。

[8]では、RDMの分類・評価ポイントが記されている。ここではアーキテクチャに基づくデータ配置・機能供給形態、メタデータ、並びに拡張に対するAcceptance等を定義している。さらに研究途上のStaging段階のデータ管理、プロジェクト終了後の長期保存の二つの異なるフェーズも定義している。ただし、ここでは材料科学分野固有の要求事項に関するメトリクスまでは言及していない。裾野の広い材料科学分野の研究データ管理で特記すべき点は、[11]での指摘のとおり、利用する実験・計測装置、扱う手法・試料、並びに課題等が多様であるゆえ、研究データ管理に向けた共通的な業務プロセスモデルの定義に困難

な点が存在し、この解決に向けて様々な技術要素群を取り込む必要があること、である。それらを[11]の記述に基づき具体的に記すと下記になる。

“他分野と共通な技術要素のみならず、材料科学分野固有の要件も考慮して様々な技術要素を取り込んでいる。前者に関する具体的要素としては、従来からの強い要求がある研究データの来歴管理、それを支える研究データの識別・一意性管理のためのPIDサービス、データ信頼性保証の仕組み等であり、後者には多様で領域特有性の強いデータをハンドリングするため、オントロジを含んだメタデータの流通、計測装置・システム等から大量の研究データの収集を実現する柔軟性を持つアダプタ等である。”

当該プラットフォームでは、研究データ来歴管理については未成熟段階にとどまるが、データ信頼性保証の仕組みの一つとしては、他分野と共通技術要素であり、本稿で説明する認証・認可基盤も含まれる。また上記PIDサービスとは永続識別子(Persistent Identifier)取得・管理サービスであり、実装されている。そして当該プラットフォーム全体としては、上記を含めて[11]のとおり材料科学分野における「高付加価値科学データ創出」を指向することも期待される。

図1は上記メタデータ形式を説明するため、当該プラットフォームで扱うデータ・記述群を内容・抽象度に応じて分類し、それをどのような物理データ形式に対応付けるか、を記載した概念図である[11]。ここでは材料科学の論点に基づく共通形式を目指している。具体的には[11]

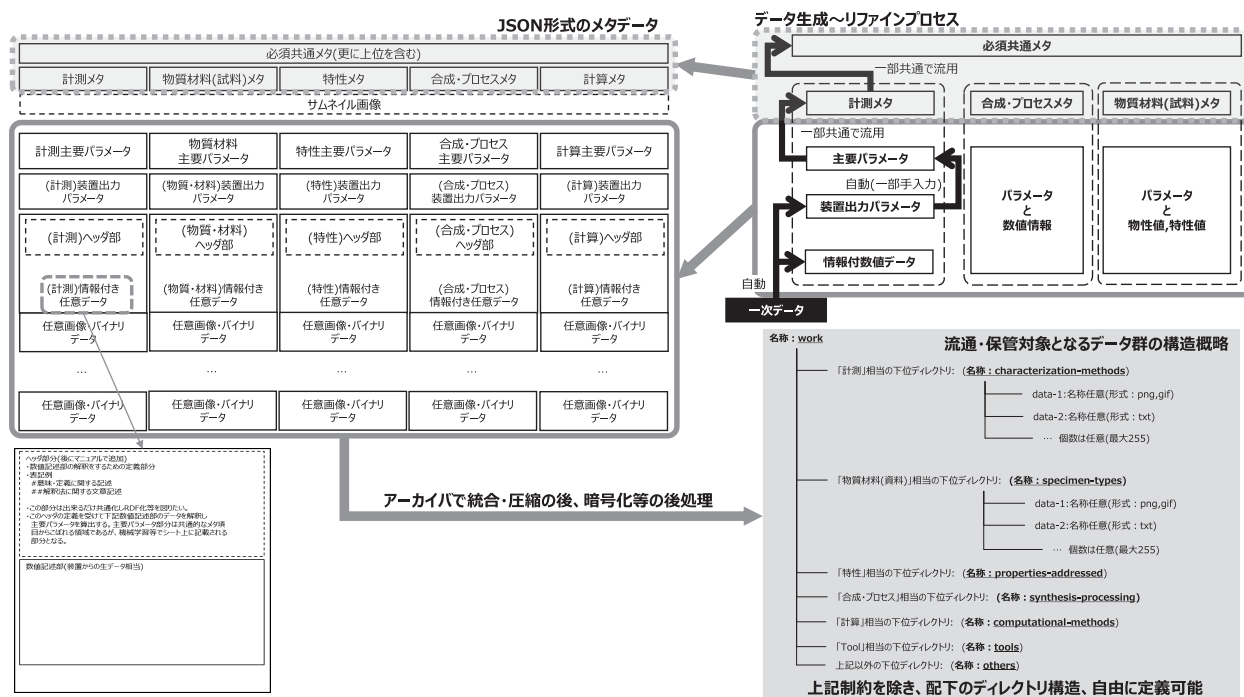


図1 材料データプラットフォームで扱う研究データ構造に関する概念図 [11]

Fig. 1 Conceptual Model of the Research Data Structure in Material Data Platform. [11]

に基づき下記で説明される。

“図中左側のマトリックスは、その中心概念を表現しており、材料科学分野で生成される諸研究データの分野内容を横軸に、その記述抽象度を縦軸にして分類したものである。当該マトリックスの最上位行は、研究データそれ自体の生成日付や作成者等のいわゆる研究データに関する書誌情報に相当し、抽象度が最も高く分野に関係無く全てのユースケースで共通的に利用される。その意味で「必須共通メタ」として定義される。サムネイル画像を除き、当該必須共通メタデータ以下の行は、分野内容毎に分類される。分野内容は材料科学の論点でその研究データの特徴を記述するための項目群であり、「物質材料」と「合成・プロセス」を与件とした結果、得られる「特性」を記載することを基本とし、その際の「計測手法」、もしくはシミュレーション等により評価されることも考慮して「計算」の記述群を含む。この5要素を選択的に利用させることで、多様な材料科学研究の方法・ユースケースに対して可能な限り共通的に適用されることを目指している。これに対してマトリックスの縦軸に相当する記述抽象度は、計測装置・シミュレーションプログラム等自体が生成する機械可読のバイナリデータを最下層とし、人による可読性を向上する目的で抽象化・アノテーション化を図ったものが、より上位に位置付けられる。このマトリックス定義に基づき、当該プラットフォームで扱う研究データ群を如何に物理的にマッピングするかが決まる。”

図1の「必須共通メタ」並びにその直下の「計測メタ」「物質材料（試料）メタ」「特性メタ」「合成・プロセスメタ」「計算メタ」の部分は JSON:APIv1.0 形式に準拠した Json インスタンスで記述・流通される。それ以外の層は複数の物理ファイル群で記載されるゆえにアーカイブでファイルに統合・圧縮されて管理・流通される [11]。

以上のような材料科学分野固有の抽象化を含む技術要素群を組み込んだとしても、共通的な業務プロセスモデルを定義することには本質的には困難な点も認められる。特に適用初期にみられる関連オントロジ・語彙・マスタデータ等の情報資産が稚拙で発展途上にある段階では、その傾向はさらに助長される。このため、接続システム数を限定したうえで、当該プラットフォームが提供するサービスを試行的に適用、それを段階的スパイラルに繰り返すことで発展させるアプローチを取る必要がある。これを受けて、業務プロセスは試行適用～課題抽出～更新・最終確定の一連のサイクルを完了するまで、粗いユースケースのみを定義、プロセス成熟度・練度を発展させながらシステムを充足させることも必然的に求められる。従来、当該機構はプロジェクト個別に研究データ管理を実施してきたが、組織横断的に研究データ管理を実施することは途に着いたばかりである。データ管理の成熟度モデルである Data Manage-

ment Maturity Model (DMM)[16] から見た場合、まず定着化を重視し Level.1 から Level.2 段階の移行を急ぐ必要がある。それゆえに例えば [17], [18] で扱われる要求等については外延機能として独立に実装のうえ、段階的発展の中で組み込むべきであり、当該機構での RDM 自身の当面の優先事項にはならない。

以上の背景に基づき認証・認可機構の実装においても付随する制約が存在する。具体的には適用する OSF に付随した CAS をベースに認証・認可機構を構築すること、並びにそれを漸増的に拡張することである。

2.2 システム全体の構成概要

図2は当該プラットフォームの上位構造であるアプリケーション群の構成要素を記した UML (Unified Modeling Language) 配置図である。一つの長方形はサイトを意味し、これらサイト間の関係は、呼び出し方式の指定の代わりに有向線で記し、呼び出し関係（依存関係）を意味する。また図中、灰色で塗り分けられている部分は、当該プラットフォームを構成するネットワークのうち、セキュアな内部セグメント領域であり、それ以外は DeMilitarized Zone (DMZ) 上のセグメント等に相当する。

図2を機能的に分解すると大きく二つに分化される。図下半分に相当する業務プロセスを扱う機能群、もう一方は図上半分に相当し、業務プロセスを支援するための情報資源管理機能/ユーティリティ機能群である。前者の業務プロセスを扱う機能群は、(i) Data Collection System (DCS) と称する研究データの発生源・これらの統制機能、(ii) 実験/シミュレーション等の研究活動成果として産出される研究上の一次データを組織・集中的に管理する Research Data Management (RDM) Server 等の研究データ管理機能、そして (iii) Material Data Repository (MDR) の様な研究データの公開機能が該当し、これらをシームレスに連携させた一つのワークフローでもある。ここで (i) Data Collection System (DCS) は、[17] のような実験データの集約・発生管理に相当する。これに対して (ii) の Research Data Management (RDM) Server は、本稿で述べる RDM の中心機能であり、研究途上の Staging 段階のデータ管理、プロジェクト終了後の長期保存を実現する機能である。最後の (iii) Material Data Repository (MDR) は [8] で定義される ‘Dissemination Capability’ を実現する機能に相当する。各要素に関する定義・説明は既に [11] にて概説されているので参照されたい。

2.3 認証・認可機構の位置付け

本稿で概説する認証・認可機構は、材料科学分野に限定された機能ではない。しかし当該プラットフォームでの要求とは、前節の (i) DCS, (ii) RDM, (iii) MDR を含めてすべての関連するサブシステムに対してシングルサインオ

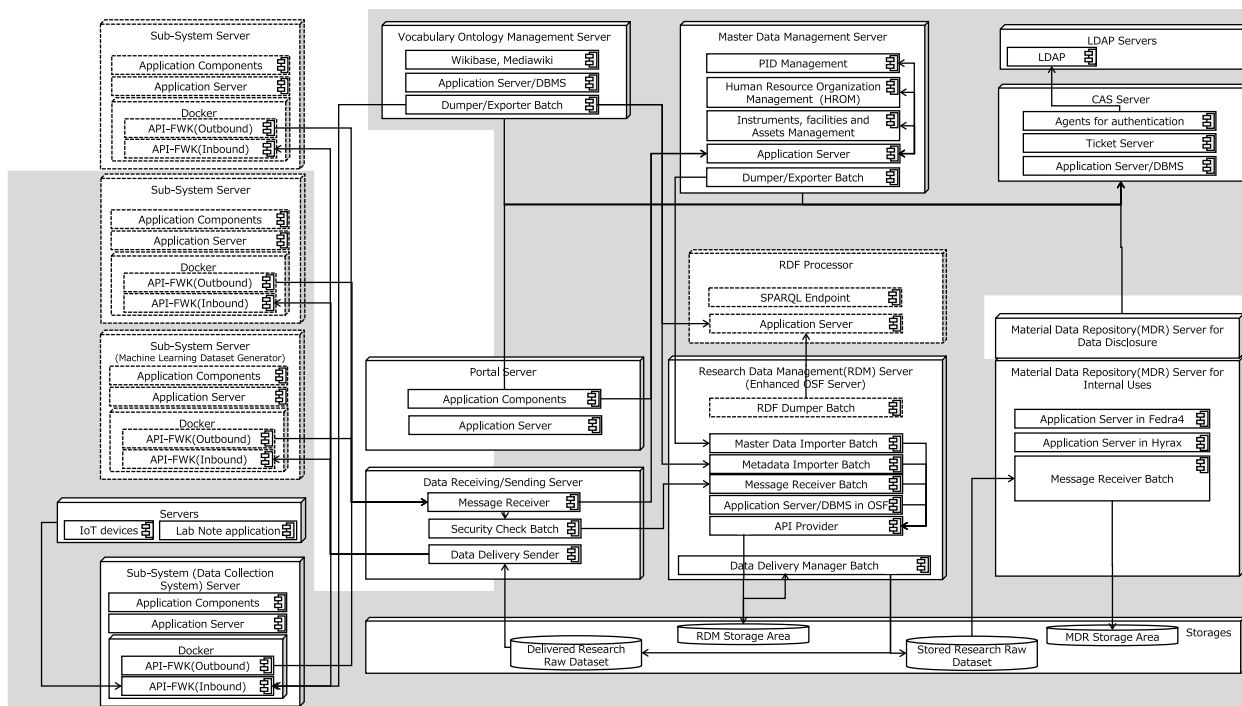


図 2 UML 配置図による材料データプラットフォームの上位構造アプリケーションのアーキテクチャ構成 [11]

Fig. 2 Architecture of the Application Layer of Material Data Platform in UML Deployment Diagram [11].

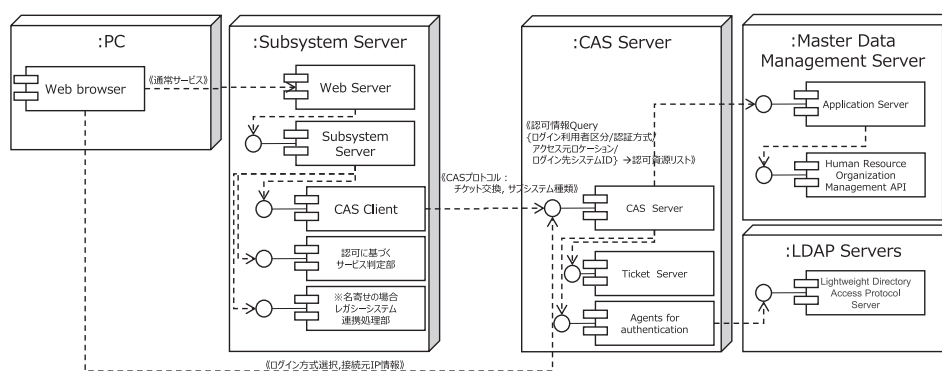


図 3 認証・認可機構の構成概要

Fig. 3 Outline of Configuration of Authentication and Authorization Mechanism.

ンを実現することである。具体的には適用する OSS である OSF に付随した CAS をベースに認証・認可機構を構築する必要がある。CAS 自身は CAS プロトコル以外にも Bridge パターンを用いた Plug-In により旧来の Outh2 [19], OpenID [20], SAML(1,2) [21] 等の認証連携プロトコルをサポートできるが、さらに潜在的に多様な認可資源を統合的に扱い人員・組織マスタデータ管理と統合した HUB 化を実現することが要求される。本稿では以後、この認証・認可機構に関する構成とその漸増的な拡張過程に限定して説明し、その妥当性について検証・考察をする。認証・認可機構が材料科学分野に限定されるものではないゆえに、他分野で同等な機構を構築する際に、本稿記載の知見が応用できることを期待する。

3. 認証・認可機構の構成

図 3 は認証・認可に関連する機能部分を中心に記した UML 配置図である。ただし、主要コンポーネント間の呼び出し関係を中心に記しており、ネットワークドメイン上の配置については省略している。このため実際には Web Application Firewall (WAF) 等のコンポーネント等が介在する。図中左側は、種々のサービスを提供する各種サブシステムをモデル化したもので、シングルサインオンの実現のため CAS-Client を組み込んでいる。サブシステムの実装言語に応じて CAS-Client の標準ライブラリが提供されており、それを組み込むことになる。ただし、サブシステム本体でも認可結果に応じてサービスを提供するか否かを判断するロジックを追加実装する必要がある。さらにサブシステム自身が、独自に認証機構を実装のうえ、すでに

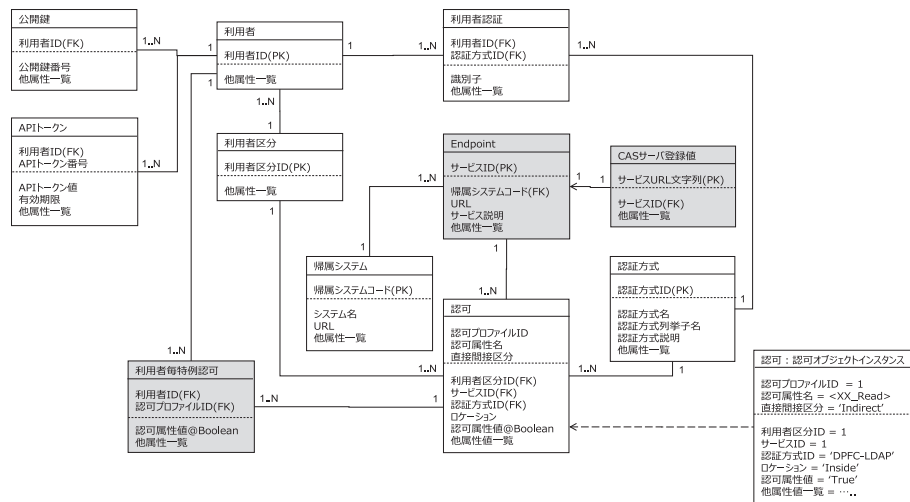


図4 認可資源に関連した主要情報モデル

Fig. 4 Main Part of Information Model related with Authorization Resources.

運用している場合もある。この場合、CAS を用いたシステム全体で管理される認証情報、メンテナンスプロセスで不整合が発生し得る。本来、しかるべきマスタデータ管理を実施、そのようなセマンティクス上のインターオペラビリティを確保する必要があるが、そのような対処に対して種々の制約も存在する。そこで必要に応じてサブシステムごとに拡張組込機能として「レガシーシステム連携処理部」を設ける。これによりサブシステム内で、認証情報の対応管理を実施する。図中右側の CAS Server はシングルサインオンの認証、並びに認可を実施する上での中核的な役割を持ち、前述のように認可を中心に強化拡張を施している。認可機構の強化にあたっては、[13] のような先行事例も存在する。ここでのアプローチでは API トークンを利用すること、認可資源を人員組織マスタ管理内で管理する点で [13] とは差異が存在する。CAS のプロトコルに従い CAS Server が認証情報を確認するため、複数の認証サービスと連携する。具体的には当該機構の職員向けの NIMS LDAP サービスを始めとして、そこでの運用ポリシーに合致しない新たな認証を扱うローカル LDAP サービスである DPFC LDAP、並びに学認サービス、Open Researcher and Contributor ID (ORCID) サービス等である。さらに API トークンと認可情報を取得する目的で、人事組織マスタ管理である Human Resource Organization Manager (HROM) の API を呼び出す。これはオリジナルの CAS の機能としては実装されていない API 呼び出しであり、前述の独自に強化拡張した部分である。認可資源に関する情報管理は HROM Server 内に実装されており、その主要情報モデルは図 4 の Entity-Relationship (ER) 図上のサブセットとなる。

図4では後述図8における第二次拡張への対応部分を含んで記載しており、それが図4の灰色に塗り分けられたエンティティ群に相当する。第一次開発では認可エンティ

ティのインスタンス群を束ねる Endpoint エンティティと
 帰属システムエンティティとの関連は 1:1 であるため
 Endpoint エンティティは実装されず、認可エンティティ
 のインスタンスは「利用者区分」「サービス ID（帰属シス
 テムコード）」「認証方式 ID」「ロケーション」で一意に保
 持される。ここで「利用者区分」とは、個々利用者が帰属
 するロールに相当し、当該機構職員、もしくは訪問研究員
 等のグレード等である。認証方式 ID とは、前述の当該機
 構の職員向けの NIMS LDAP サービス、NIMS LDAP
 サービスに含まれない認証を扱う DPFC LDAP、学認
 サービス、ORCID サービス、さらには個々のサービス独
 自の認証情報のカテゴリである。当該機構の場合、研究者
 が大きな構成人口を占めるため、時限プロジェクトにおけ
 る任期制職員、Sabbatical による訪問研究員、受け入れ大
 学院生等の中短期雇用者も多く存在する。このため実運用
 上、単一の認証機構だけでは不十分との要求も存在してお
 り、安定的な運用への移行を考慮して上記のような「利用
 者区分」と複数認証機構の導入を図っている。ただし初期
 段階では設計上の対応のみとし、実装は限定的になった。
 以上により、自ずと同一人物に複数認証方式の識別子を付
 与できる必要があり、図 4 の情報モデル上ではその対応が
 なされるとともに、名寄せ対応として同一人物に対する一
 つの永続識別子（Persistent Identifier）の付与ができるよ
 うになっている。図 4 の右下には認可エンティティのイン
 スタンス例を併記している。認可資源は当該エンティティ
 のインスタンス群として定義管理される。その主キーは意
 味解釈を含まない認可プロファイル ID であるが、実際には
 認可属性名とのタプルで認可資源が定義される。認可属
 性名は「認可対象オブジェクト×プリミティブ操作」を意
 味する固有文字列が指定される。以上の呼び出し関係、情
 報モデルを介して認証・認可機構が実装され、CAS Serv-
 er を中心に人員組織マスタ管理と統合化した HUB 機能が

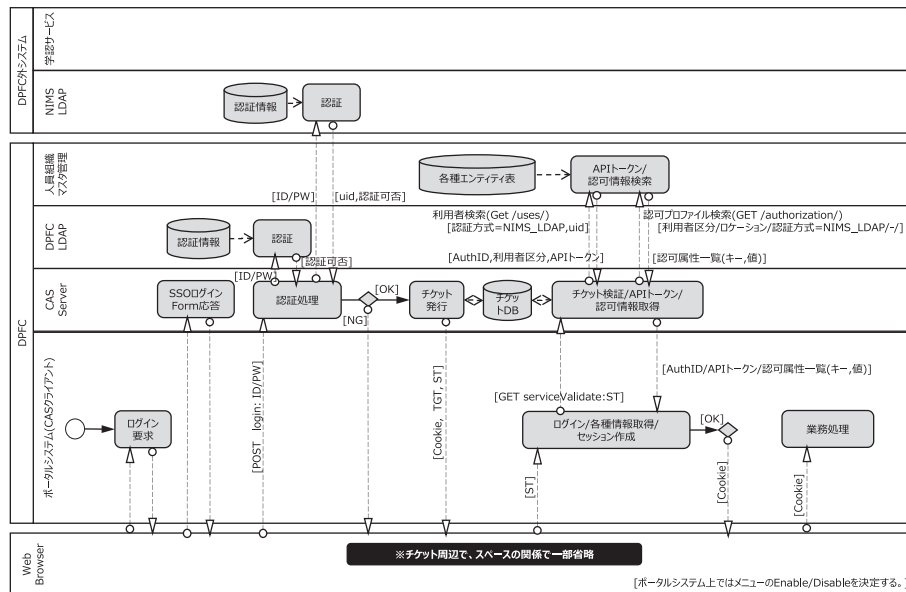


図5 認証・認可プロセス手順 (1/2)

Fig. 5 Procedure of Authentication and Authorization Process. (1/2)

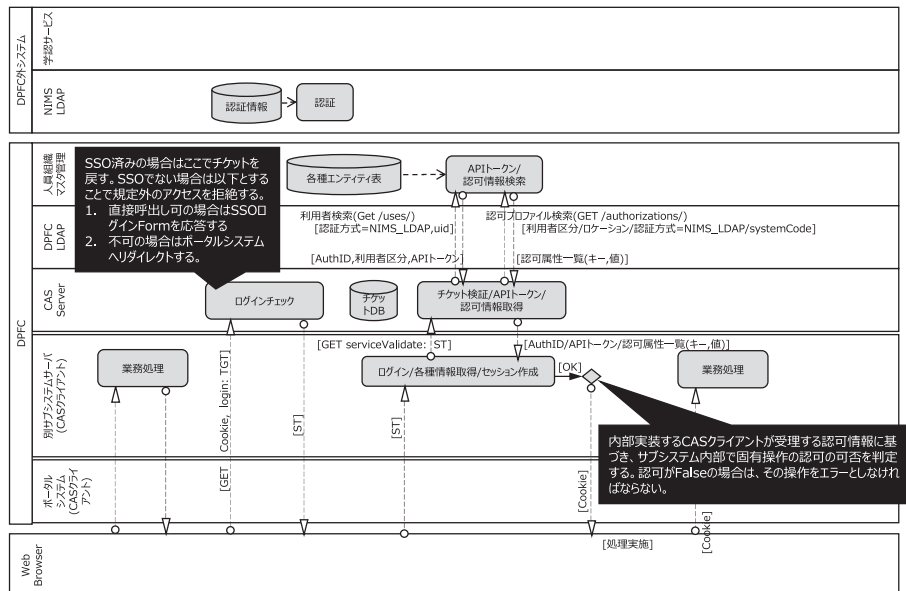


図6 認証・認可プロセス手順 (2/2)

Fig. 6 Procedure of Authentication and Authorization Process. (2/2)

実現される。

図5、並びに図6はBusiness Process Model and Notation (BPMN) 図で記した認証・認可プロセスの手順である。図5はシングルサインオンの基本手順であり、図6は各サブシステム本体で認可属性値に応じてサービスを提供するか否かを判断するロジックについて特記したものである。図5ではCAS-Clientを組み込んだサブシステムとしてポータルシステムを例示している。ここでログイン要求を行うとCAS Version3のプロトコルに従い、CAS Serverにリダイレクト後、シングルサインオンのためのFormがダウンロードされる。ここでは当初オリジナルのものを利用したが、前述複数認証機構の導入を考慮し、独自強化し

たものと入れ替えている。CAS Serverの内部では大きく、(i) 認証処理、(ii) チケット検証、(iii) APIトークン/認可情報取得の処理がなされる。(iii) APIトークン/認可情報取得の処理は、[13]を参照のうえで当該機構にてCAS Serverを強化拡張した部分である。この結果、図5においてはログイン利用者がアクセスしうるサブシステム群の一覧が認可属性一覧としてAPIトークンとともに戻される。これに対して図6の場合、指定サブシステムがアクセスし得るか否かの可否結果が戻される。これらはいずれも図中「ログイン/各種情報取得/セッション作成」の終盤段階で処理される。その後、図5の場合はポータルシステムが、認可されたサブシステムのみをEnable表示に切り替える。

指定サブシステムの場合、図 6 で明示されたように認可拒否の際、認証エラーとして扱われ、それ以外はシングルサインオンの後、後続の業務処理が、サブシステム上で実施される。

4. 漸増型プロセスモデルによる発展過程

4.1 概要

本章では当該プラットフォームに対する要求の変遷に基づく認証・認可機構とその周辺機能の開発プロセスの発展過程を概説する。最初に本節で要求事項、並びに背景となる手法の概説を行う。続く 4.2 節、4.3 節では実際の実装に関して説明を行った後、最後の 4.4 節で総括を行う。2 章で言及したように裾野の広い材料科学分野では、利用する実験・計測装置、扱う手法・試料、課題等の多様性ゆえに、研究データ管理に向けた共通的な業務プロセスモデルの定義には本質的な困難が伴う。そのため接続システム数を限定したうえで、当該プラットフォームが提供するサービスを試行適用、それを段階的スパイラルに繰り返すことで発展させるアプローチを取っている。これに基づき業務プロセスは、当初、粗いユースケースのみを定義のうえ、プロセス成熟度・練度を進化させながらシステム自身を充足させることになる。これは認証・認可機構とその周辺機能に対しても同様に適用される。このため、これら機能の実装でも漸増型プロセスモデルを採用することが合理的判断となる。図 7 は漸増型プロセスモデルの概念図である [22]。このプロセスモデルでは、当初の段階で中核となる核部分と一部選択機能の開発・供給に注力する。その後の増加分は核部分を元にした機能追加となる。この開発モデルが成功裏に効果を発揮するための適用要件は、機能を随時増加させる際にシステム構築レベルで大規模な再構成を不要にできるか、否かによる。いわばアーキテクチャ設

計解の安定性が一つの主要要因となる。逆に核部分の作り直し等のアーキテクチャ設計解の不安定な状況は、管理リスクとして説明されている。

4.2 実際の開発プロセスと中核機能開発

図 8 は実装に到る開発プロセスの主要部について Data Flow Diagram (DFD) を拡張してモデル化したものである。図中のノードは図 8 の凡例に記したように要求項目、成果物、プロセス、実装・内容の 4 分類で記載している。図 8 の左側には要求項目群が記されており、右側はそれに基づいて実行された実装について途上のものも含んで記す。図 8 では現実のプロジェクト実施上、詳細に表現しきれていない部分も少なからず存在しているが、本質的な事項を優先して取捨しているため、それらを省略している。

実際の開発では、前述漸増型プロセスモデル定義に基づき厳密に工期・フェーズを分割して実施計画を定義したわけではないが、3 フェーズ以上に分割された形で進めることになった。第一期はアーキテクチャ上の基本構成を決めるフェーズであり「第一次開発」と称される一連のプロセスである。第二期は「第一次拡張・強化イテレーション」と呼ばれるフェーズ、第三期は「第二次拡張・強化イテレーション」と呼ばれるフェーズに相当する。このプロセス上は未だに進捗途上であり、本稿執筆段階では「第一次拡張・強化イテレーション」の途上にある。

実際にフェーズ分割を決定するにあたっては複数要因が存在する。ただし業務プロセスを試行適用～課題抽出～改善を段階的に繰り返すことでプロセス成熟度・練度を発展させるスパイラル的なアプローチを採用するため、業務プロセス実施にあたっての必要最低限の機能を、予算・人的資源等のプロジェクト制約とバランスを取りながら決定することが支配的であり、これがフェーズ分割の基本原則になっている。

認証・認可機構の核部分を含んだ「第一次開発」を開始する際、要求事項・中心課題は「研究データの集積・サブシステム各サイト間でのデータの交換・流通・管理、並びに利活用」に資する必要機能の提供であった。アーキテクチャ上の要求は [11] で概説している。このためアーキテクチャ設計に相当する核部分開発では、論理上要求される必須の機能群が複数存在し、開発を実施した。その一つは人員・組織に対する永続的識別子 (Persistent Identifier) の付与である。前章で説明した複数の認証機構のサポートについても当初から要求された。「第一次開発」は、認証・認可機構の核部分を含むゆえにおおむね Waterfall 型の開発に従っているが、技術上のリスク評価、新たな概念ゆえの要求の曖昧さなどから実際には Waterfall プロセス中に寄生する小スパイラルプロセス等も存在した。たとえば、図 3 で説明したサブシステム自身が、独自でレガシーの認証機構を実装している場合、拡張組込機能として「レ

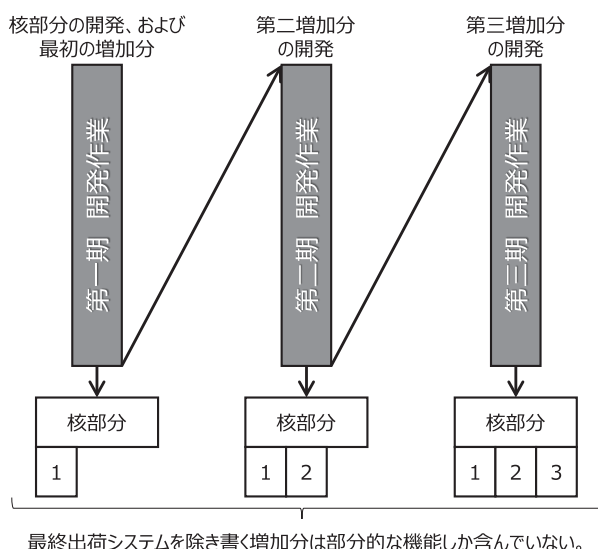


図 7 漸増型プロセスモデルの概要 [22]

Fig. 7 Outline of Incremental Delivery Process Model [22].

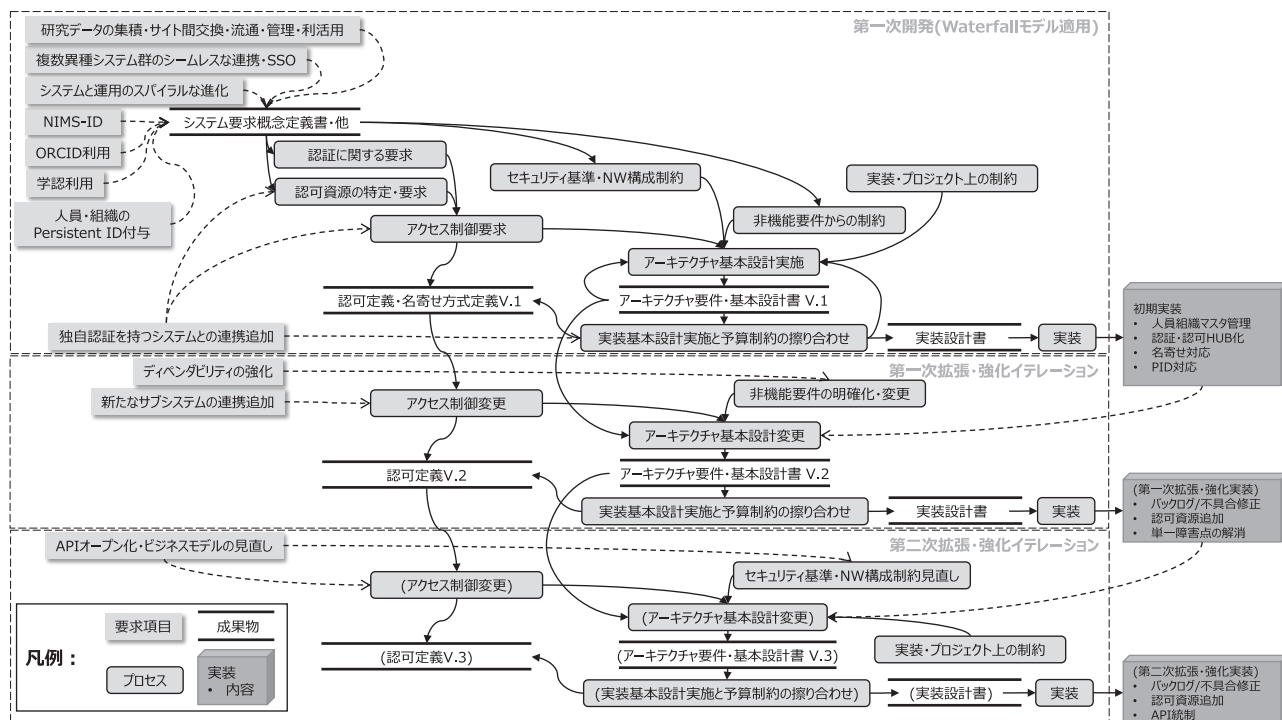


図 8 認証・認可機構とその周辺機能の開発プロセスとその要求の変遷

Fig. 8 Transition of Development Process of Authentication and Authorization Mechanism and its peripheral Functions and their Requirements.

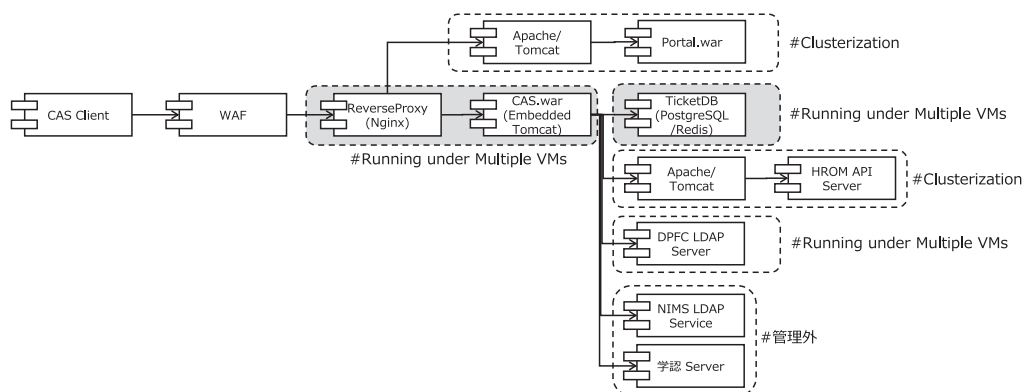


図 9 単一障害点の解消に向けた認証・認可機構の構成概要

Fig. 9 Outline of Configuration of Authentication and Authorization Mechanism to solve a Single Point of Failure.

ガシーシステム連携処理部」を設けた「名寄せ」機能が必要になる。この対処は典型的な後戻り～設計上の調整に相当している。図 8 上では「独自認証を持つシステムの連携追加」という名称で記載する要求項目に相当する。このような事態に従い、「アーキテクチャ要件・基本設計書」は数度の更新作業がなされている。認証・認可機構の核部分を含んだ「第一次開発」の結果、人員組織マスタ管理の基本アーキテクチャの確立・実装、認証・認可の HUB 化、同一人物・組織各々に対する一つの永続識別子 (Persistent ID) の付与等が実装された。その後、システム管理者、並びに人選・許可された最低人数の利用者による試行評価が実施されている。

4.3 拡張・強化に関する開発

「第一次開発」では利用者の想定見積数については概略把握しているものの、その前提には不確定要因も含み、その意味でセキュリティ以外の処理可能スループット数や、可用性等については精度が高く明確な見積を定義できる状況にはなっていない。しかし認証・認可の HUB 化が進むことで単一障害点に対するリスクが顕在化され、対策を具体化する必要が出てきた。そこで拡張・強化が必要となった。「第一次拡張・強化イテレーション」では上記「単一障害点の解消」以外にも取りこぼしたバックログ、新たな認可資源の追加も重点的に扱われた。具体的には図 8 に記すような対策を取っている。

図 9 は「単一障害点の解消」に向けて認証・認可機構

の構成を見直した図である。図9は、図3のUML配置図上の認証・認可機構の主要コンポーネント群で明示されていない実装コンポーネント群を追加、コンポーネント群間の呼び出し関係をより明確に示している。たとえば、図3では一般化してApplication Serverと記載しているコンポーネントは、図9では実装明確化のためApache/Tomcat等に変更、CAS Serverも実装状況を説明する意味でCAS.warと記している。さらにネットワーク上の重要な機能であるWAF, Reverse Proxy (Nginx)も明示した。強化計画対象の実装コンポーネント群は灰色で塗られた部分に相当する。単一障害点を排除し可用性を向上するためには、呼び出し関係のある実装コンポーネント群の多重化・冗長化する必要がある。強化計画対象の実装コンポーネント群は可用性に直接影響を与える部分であり複数の独立したVirtual Machine上での実装を検討している。本来、可用性を向上させるためには、関連する全実装コンポーネント群、具体的にはHROM API Server等に対してもクラスタ化を適用する必要があるが、これらは現設計において影響力が大きく、予算上の制約もあるため「第一次拡張・強化イテレーション」の中では見送り、段階を踏んで拡張することを予定している。

本稿執筆段階では第一次拡張・強化実装の終了までには至っていないが、すでに「第二次拡張・強化イテレーション」についても見通されている。これは「第一次開発」で中心課題とした「研究データの集積・サブシステム各サイト間でのデータの交換・流通・管理」の運用モデルから、新たな情報提供モデルを追加・提供することである。「研究データの集積・サブシステム各サイト間でのデータの交換・流通・管理」にまつわる機能だけでは、当該プラットフォームが管理する研究データを組織外部に提供、利活用を促進するには限界がある。そこで、新たにAPI群を各サブシステムに対して定義・実装、それを外部公開することで研究データの利活用を促進させる、と言うデータ提供戦略に基づく要求の変化である。当該事項に関しては、図8上では「APIオープン化・ビジネスモデルの見直し」として記載されている。ビジネスモデルの更新にあたっては認証・認可機構のうち、特に認可機構に対して大きな影響を与える。各サブシステムでAPI提供機能を準備することにとどまらず、これを模する認証・認可を統制する図4の情報モデル上では、灰色のエンティティ群と関連派生エンティティ群の追加と、運用データのマイグレーション等が必要になる。第一次開発において、認可情報は帰属システムエンティティとEndpointエンティティの関連は1:1で扱われたが、新たな要求により1:Nの関連で実装される必要がある。これとともに各APIへのアクセスを、おのおの認可資源として扱うことも必要になる。これにより、図9のUML配置図の中のReverse Proxy (Nginx)の周辺に利用統制を行うためのAPI-Gateway機能、並びに

かつてのUniversal Description, Discovery, and Integration (UDDI)のGreen pages相当のAPIカタログ検索が必要になる。

4.4 総括

前節までに記した実装プロセスの発展過程を漸増型プロセスモデルの適用要件から総括する。「第一次開発」では認証・認可機構の核部分の開発を含み、一部では寄生する小スパイラルプロセスも実施したが、人員組織マスタ管理の基本アーキテクチャの確立・実装、認証・認可のHUB化、同一人物・組織各々に対する一つの永続識別子(Persistent ID)の付与等を実現した。これによりRDM定着化を目指すための業務プロセスの試行、特にシステム管理者、並びに人選・許可された最低人数の利用者による試行評価が実施された。

続く「第一次拡張・強化イテレーション」では「第一次開発」で重点化していなかった単一障害点に関する課題に対処している。この課題は、認証・認可機構のHUB化が進むほど、サービス品質維持に対してはリスクになることに基づく。ここでは図9に記した実装コンポーネント群の冗長化・クラスタリング等の利用により対処している。ただし、図4の情報モデルに対して大きな影響を与えておらず、漸増型プロセスモデルの適用要件の範囲にとどまっている、と解釈できる。

上記に対して「第二次拡張・強化イテレーション」は、新たにAPI群を各サブシステムに対して定義・実装、それを外部公開する、というデータ提供戦略に基づく要求変化に起因している。これにより図4の情報モデルに対して大きな影響を与えることを概説した。この点から見ると、アーキテクチャ設計の安定性が重要な適用要件である漸増型プロセスモデルにはそぐわない事態に映る。ただしすでに説明したとおりScrap and Rebuildまで必要とされるとは言えず、一部の情報モデルの入れ替えと新たな機能要素の追加にとどまることも想定される。これは疎結合指向のアーキテクチャゆえの柔軟性の高さによる、と考える。疎結合指向のアーキテクチャは、漸増型プロセスモデルのリスクを緩和し、適用要件を拡大し得ることも示唆される。

5. セキュリティフレームワーク論点から見た認証・認可機構機能の評価と考察

本章では従来の関連領域について説明した後に、筆者らの実装に対して簡易アセスメントのうえで評価する。5.1節ではRDMに関連の深いE-Science, Scientific Workflow領域における従来の認証・認可を概説する。5.2節ではSOAにおけるセキュリティフレームワークの概説と筆者らの実装への簡易アセスメントを行う。5.3節ではその結果に基づき、前節の設計上の変遷を交えて評価・分析・考察を行う。

5.1 E-Science, Science Workflow 領域における認証・認可

筆者らは RDM における認証・認可機構に関する開発は、それ自身が独立した研究分野というよりも E-Science, Scientific Workflow 等の基盤の外延機能として扱われてきたと考えている。さらにこれら E-Science, Scientific Workflow を含んでセキュリティ要件に関する網羅度・完全度を一般論として評価することは、本稿の範囲外でもある。そこで本稿では RDM を E-Science, Scientific Workflow と連携して新たに急伸している領域ととらえるが、これら領域の中でどのように扱われてきたか、を概説するにとどめる。それとともに、当該認証・認可機構の位置付けを評価せず、他実装の状況を述べるにとどめる。

E-Science 領域は 20 年来、グリッドコンピューティングの応用として発展し、現在に至る。「第四の科学手法」の提唱がなされた 2010 年前後のグリッド領域のセキュリティ技術については [23] で概説している。ここでは、NAREGI ミドルウェア [24] を例にグリッド上でのシームレスなジョブ転送、実行、スケジューリングを実施するため証明書、シングルサインオン、権限移譲等を解説している。この点では一定の機能実装について検討されている。しかしセキュリティ要件に関する網羅度・完全度に関しては明確な言明があるわけではない。[5] では SOA 化が進んだなかでの Scientific Workflow に関して包括的なサーベイを実施しているが、ここでもセキュリティ要件に対する明示的記述は少なく Verification and Validation の一環の位置付けと見なされているだけにとどまる。Provenance 領域と比較すると、網羅度・完全度の評価を含めたセキュリティ要件に対する検証には改めて検討する余地があると考え。この点に関しては Scientific Workflow のリファレンスモデルを扱う [25] や Provenance に基づくロールベースのアクセス制御機構について提案している [26] で

も同様の印象を受ける。検証済みの言明ではないが、その背景としては「第四の科学手法」の提唱がなされた 2010 年頃までは E-Science, Scientific Workflow 領域では、既存実装や Web サービスで一般的であった OpenID [20], SAML [21] 等の方式を採用することが支配的であったことも示唆される。

近年では [27] のように、Globus Auth の下で OAuth2 [19] と OpenID [20] を用いた認証・認可機構についても実装が進んでいる。ここでは巨大データのハンドリングを、GridFTP を介して実現するためのパターンを提案している。要求に関しては筆者らの図 2 のアーキテクチャと同等のことが認められるが、筆者らの実装では CAS 適用がプロジェクト上の前提であり、その是非・優劣を単純比較することはできない。

5.2 セキュリティフレームワーク論点から見た実装の簡易アセスメント

前述のように筆者らの認証・認可機構に対する評価を従来関連研究だけでは与えられないため、SOA におけるセキュリティフレームワークを元に評価を行う。E-Science 領域での認証・認可の位置付けとは対照的に、シングルサインオンを実現する認証・認可機構は Enterprise 系の業務システムのサービス化においては進展し、SOA におけるセキュリティフレームワークの一つの重要要素として定義、すでに成熟化に向けての段階にある。図 10 は 2010 年以前に [28], [29] により提示された SOA セキュリティリファレンスモデルである。このモデルは論理モデルとして定義されることから、実装技術上の影響とは独立に進展し、そのフレームワークに基づくソリューションは成熟の段階にあると考えられる。付録における表 1 は原著に基づく各主要機能と筆者らの実装における対応状況を簡易アセスメントとして記す。主要機能の概要定義については、

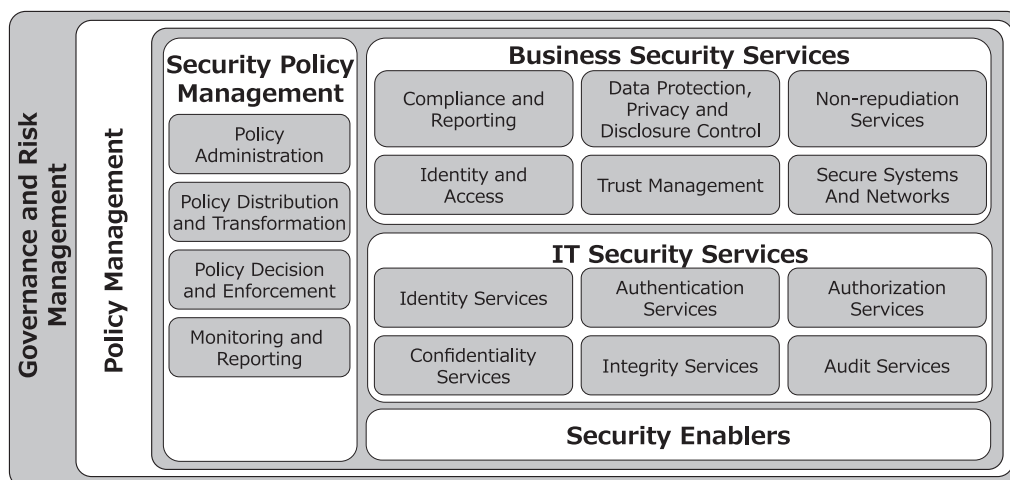


図 10 SOA セキュリティリファレンスモデル [27], [28]

Fig. 10 SOA Security Reference Model. [27], [28]

自明事項も存在するため、第一階層のもののみを記し、必要に応じて説明の中で補足する。この類の事項は開発実行主体の持つ技術的成熟度と、プロジェクト上の制約・組織上の政策等の外的制約事項にも大きく依存する。また開示できる範囲でしか記載できない制約もあるため、一部項目は概要レベルの説明にとどめる。

5.3 考察

本節では筆者らの実装に対して SOA におけるセキュリティフレームワークを用いて簡易アセスメントした結果を評価し、4 章を振り返りながら要因等进行分析、考察する。最初に結果に対する全体鳥瞰を行ったうえで、表 1 で特記すべき要素について解説する。その後、本稿の中心課題である認証・認可機構に関する評価を行う。

表 1 で記載したように SOA のセキュリティフレームワークの論点から改めて簡易アセスメントした結果、図 8 のシステム要求概念定義書、並びにアーキテクチャ要件・基本設計書 V.1 の中では、フレームワーク上の各要素項目に対する必要性の認識はされ、いずれかの形で設計解が記述されていた。ただし、現実には実装・適用度合いでの凸凹、斑があることは否めない。差異として表出する事項は、言わば凸凹として認識され、適用充足度・設計品質と言い換えることもできる。

表 1 の中では「Data Protection, Privacy and Disclosure Control」「Identity and Access」に特記すべき事項が 2 点存在する。[28] では Data Protection Management とは、業務情報保護と一連の操作の際の対応能力として定義されており、Disclosure Control の中で開示制御を行うことになる。特記すべき一点目は、開示制御を検討する際の構造的な難しさである。当該ケースで難航した事項は、開示に際しての FAIR Data Principle (Findable, Accessible, Interoperable, Re-usable) とデータ所有権、並びにデータ開示にまつわるビジネスモデル等の方針策定に関することである。新規領域であるほど、その合意形成には時間を要し、種々のステークホルダとの関係整理、要求調整は設計・運用を困難なものにする。そして、これらは直接、認可資源定義として扱われる。二点目は開示制御のメンテナンスに関することである。図 8 の認証・認可機構とその周辺機能の開発プロセス変遷でみられたように漸増型プロセスモデルでのイテレーションのたびに新たに認可されるべき資源・サブシステム群が追加されている。プラットフォームである以上、このような認可資源の追加は随時、定常的に発生する。認可資源の定義、迅速な管理作業は重要な検討事項である。

IT Security Services でも特記すべき事項は存在する。[28] では Business Security Services における Trust Management については、組織間・システム間の相互信頼を担保する事項・方式と説明され、暗号に関する仕様、電

子署名の適用によるデータ受理プロセスが主な考慮点となる。表 1 での Confidentiality Services で記載のとおり、初期段階からその対策は試みられてきているが、実装設計段階と並行になされる予算・他制約との擦り合わせの結果、実際には実装段階で AP での利用データに対して GNU Privacy Guard を用いた暗号・復合化処理の実装は延期された。同様なプロジェクト制約上の事情は Audit Services に対してもなされている。本来、E-Science ゆえに Provenance の重要性は認識されてきたが、シングルサインオンの実装に依存してこれらの機能は意味を持つ。各種制約下では Audit Services の実現・Provenance の充実以前に重点化する事項も存在する。以上を例にすると RDM の実装では、その複雑性故に、従来以上にコンポーネント化・マイクロサービス化への対応と実装順序に関する戦略策定が必要になることが示唆される。

最後に IT Security Services の認証・認可機構としての十分性、並びに図 8 の認証・認可機構とその周辺機能の開発プロセスの変遷からみた妥当性について言及する。前述のように CAS 適用についてはプロジェクト上の前提であること、並びに [13] での指摘のとおり、採用した CAS の実装では認可機構に関する機能上の欠落が存在するため、これを強化拡張することは必然であり、本稿でその是非を評価することは意味をなさない。逆に本稿では認可機構のアーキテクチャ、特に図 4 の認可情報の主要情報モデルに関する評価が重要になる。3 章、4 章で記したとおり、当該情報モデルの策定は初期のシステム要求概念定義書等をその根拠としている。その時点でのニーズに基づき、認可情報は「利用者区分」「サービス ID (帰属システムコード)」「認証方式 ID」「ロケーション」で一意性が決まることで要求を満足した。特に認可資源そのものについて、陽に情報モデルに表現せずに、すべてコンテンツとして管理されることで、すべてではないが柔軟に認可資源定義の統廃合がやりやすくなる。ただし、今後の認可資源定義の増大化に従い、しかるべきインスタンスの検索・特定が必要になるため、認可資源定義に関するアノテーションや認可資源間の制約検証が重要になる。この点では情報モデル上でも拡張が必要になる。これに対して、第二拡張・強化イテレーションでみられるような新たなビジネスモデルに追従して認可資源に関する構造を変更できることに対する弱いメンテナンス性については、疎結合指向のアーキテクチャゆえの柔軟性の高さに助けられているとはいえ、本来、検討の余地が残る。具体的には各エンティティに対して、メタ情報を与えることで再構成可能とする対処等である。E-Science ゆえに新規ユースケースが想定される中での「軟構造化」への要求は、パッケージ適用が一般的になった業務系アプリケーションよりも遥かに高いと想定される。この点での工夫は考慮すべき点である。

6. おわりに

本稿ではケーススタディとして物質・材料研究機構における RDM に組み込まれた認証・認可機構の概略、設計上の変遷（認可管理との連携・名寄せ・多重化・API 管理）の概説を行い、SOA におけるセキュリティフレームワークに基づく簡易アセスメント・対比のうえで、そこで見出される差異を評価した。本稿の主要な貢献事項は、下記 3 点になる。

- (1) 共通的な業務プロセスモデルの定義に困難が伴うゆえに、当該プラットフォームが提供するサービスを試行適用、それを段階的スパイラルに繰り返すことで発展させるアプローチを取っているため、認証・認可機構の実装でも漸増型プロセスモデルを採用したが、本稿ではケーススタディとしてその発展過程を明示した。
- (2) 設計されたアーキテクチャの安定性が漸増型プロセスモデルの適用条件であることを示すとともに、適用するにあたってのフェーズ分割要因を明示した。さらに総括として評価を行い、戦略の見直しに伴う要求変化では、アーキテクチャ設計の安定性に影響を与え、漸増型プロセスモデルの適用条件を外れ得るケースもあることを記した。さらに疎結合指向のアーキテクチャにより、漸増型プロセスモデルのリスクを緩和し、適用要件が拡大することも示唆した。
- (3) E-Science, Scientific Workflow 領域の持つ多様性や新たに急伸している領域ゆえに、本質的に種々の試行錯誤も含み得るため、ソフトウェアアーキテクチャの視点からは想定できる限りのカスタマイズポイントを組み込む努力をするべきことが改めて示唆された。これは要求が安定していると思われる認証・認可機構でも例外とは言えないことを本稿では記した。具体的には認可資源のインスタンスをコンテンツ化すること、コンポーネントベースの構成、情報モデル自身にメタ情報を与えることで構成を可変とする手法・パターンの適用が挙げられる。

当該機能は未だ発展途上ではある。今回の結果を受けて適正な形で発展を図る予定である。

謝辞 本稿のような Cyber-Physical-Society-System という新たな領域を扱うことに対しては、深い関連知識と確実なコンサルティング力・プロセス管理能力・各種技術力等を持ったパートナーとの連携が欠かせない。実装にあたって貢献をいただいたパートナー各位に対して、謹んで感謝の意を表する。

参考文献

- [1] 知京豊裕：マテリアルインフォーマティクスの現状と課題～海外の動向と日本の挑戦，情報知識学会誌，Vol.27, No.4, pp.297–304 (2017).
- [2] 上島伸文，及川勝成：技術解説～計算材料科学・工学の最新動向，電気製鋼，Vol.87, No.1, pp.21–26 (2016).
- [3] Liu, Y., Zhao, T., Ju, W. and Shi, S.: Materials discovery and design using machine learning, Journal of Materials, Vol.3, Issue 3, pp.159–177 (2017).
- [4] Hey, T., Tansley, S. and Tolle, K.: Published by Microsoft Research (2009), ISBN: 978-0-9825442-0-4, <<https://www.microsoft.com/en-us/research/publication/fourth-paradigm-data-intensive-scientific-discovery/?from=http%3A%2F%2Fresearch.microsoft.com%2Fen-us%2Fcollaboration%2Ffourthparadigm%2F>>.
- [5] Liew, C.S., et al: Scientific Workflows: Moving Across Paradigms, ACM Computing Surveys, Vol.49, No.4, Article 66 (2016).
- [6] 山田直史，高島洋典，山田直史：超スマート社会（Society5.0）実現に向けて，情報管理，Vol.60, No.5 (2017).
- [7] 大学 ICT 推進協議会：学術機関における研究データ管理に関する提言 (2019). <<https://axies.jp/report/publications/proposal/>>.
- [8] Amorim, R.C., Castro, J.A., da Silva, J.R. and Ribeiro, C.: A comparison of research data management platforms: architecture, flexible metadata and interoperability, Universal Access in the Information Society, Vol.16, pp.851–862 (2017).
- [9] NIMS Now, 2019.1 月号，<<https://www.nims.go.jp/publicity/nimsnow/vol19/hdfqf100000aoslh-att/hdfqf100000aosp0.pdf>>.
- [10] 谷藤幹子：材料データプラットフォームシステムの設計と構築，月刊機能材料，Vol.40, No.10, 2020 年 10 月号 (2020).
- [11] 菊地伸治，門平卓也，鈴木峰晴，内藤裕幸：高付加価値科学データ創出を指向した研究データ管理プラットフォームのアーキテクチャ，信学技報，Vol.119, No.66, SC2019-2, pp.7–17 (2019).
- [12] <<https://www.apereo.org/projects/cas>>.
- [13] 内藤久資，梶田将司，小尻智子，平野靖，間瀬健二：大学における統一認証基盤としての CAS とその拡張，情報処理学会論文誌，Vol.47, No.4, pp.1127–1135 (2006).
- [14] <<https://rcos.nii.ac.jp/service/rdm/>>.
- [15] <<https://osf.io/>>.
- [16] <<https://cmmiinstitute.com/data-management-maturity>>.
- [17] Romanos, N., et al.: Innovative Data Management in advanced characterization: Implications for materials design, Materials Today Communications, Vol.20, 11 pages, DOI: 10.1016/j.mtcomm.2019.100541 (2019).
- [18] Yosipof, A., Shimanovich, K. and Senderowitz, H.: Materials Informatics: Statistical Modeling in Material Science, Molecular Informatics, Vol.35, pp.568–579, DOI: 10.1002/minf.201600047 (2016).
- [19] The OAuth 2.0 Authorization Framework, <<https://tools.ietf.org/html/rfc6749>>.
- [20] OpenID specifications, <<http://www.openid.net/>>.
- [21] Security Assertion Markup Language (SAML) V2.0 Technical Overview, <<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html>>.
- [22] M.A. Ould: Strategies for Software Engineering -The Management of Risk and Quality -, John Wiley & Sons, Ltd, (1990) (邦訳：古宮誠一，本位田真一：ソフトウェア技術者のためのプロジェクト管理の成功への秘訣，共立出版株式会社) (1993).
- [23] 鶴澤武士：グリッドを実現する グリッドミドルウェア基盤，情報処理，Vol.51, No.2, pp.120–126 (2010).
- [24] <<https://middleware.naregi.org/Download/>>.
- [25] Lin, C., Lu, S., Fei, X., Chebotko, A., Pai, D., Lai, Z.,

- Fotouhi, F. and Hua, J.: A Reference Architecture for Scientific Workflow Management Systems and the VIEW SOA Solution, *IEEE Transactions on Services Computing*, Vol.2, Issue.1, pp.79–92 (2009).
- [26] She, W., Zhu, W., Ling Yen, I., Bastani, F. and Thuraishingham, B.: Role-Based Integrated Access Control and Data Provenance for SOA Based Net-Centric Systems, *IEEE Transactions on Services Computing*, Vol.9, Issue.6, pp.940–953 (2016).
- [27] Chard, K., et al.: The Modern Research Data Portal: a design pattern for networked, data-intensive science, *PeerJ Computer Science*, 4:e144, DOI: 10.7717/peerj-cs.144 (2018).
- [28] Dreibelbis, A., Hechler, E., et al.: *Enterprise Master Data Management*, IBM Press (2008).
- [29] Buecker, A., Ashley, P., Borrett, M., Lu, M., Muppidi, S. and Readshaw, N.: *Understanding SOA Security Design and Implementation*, [ibm.com/redbooks](http://www.redbooks.ibm.com/redbooks/pdfs/sg247310.pdf), <http://www.redbooks.ibm.com/redbooks/pdfs/sg247310.pdf> (2007).

付録

付録 A.1 表.1

表 1 SOA セキュリティリファレンスモデルの項目定義と簡易アセスメントの結果

Table 1 Results of our brief Assessment with Definitions of items in SOA Security Reference Model.

項目	概略定義	要素項目	当該機構，材料データプラットフォームでの対応策
Business Security Services	事業体のセキュリティ運用，もしくは事業を成功裏に治めるため特定されるべき高水準のセキュリティに関わるサービスであり，組織内の基盤のあらゆる面で遵守されるべきセキュリティ・プライバシー対策の由来となるべき事項である．	Compliance and Reporting	当該機構では材料データプラットフォーム構築以前から CSIRT(Computer Security Incident Response Team)が組織，運用されていたと伴に，当該プラットフォーム構築の一環として PSIRT(Product Security Incident Response Team)を組織し，運用を開始している．管理プロセスは ITIL (Information Technology Infrastructure Library)に基づき定義の上でマッピングを図り，定着化を進めている．現在，初期定義と実運用作業のマッピング・擦り合わせの途上であり，未成熟の段階にある． 特記すべき点は「Data Protection, Privacy and Disclosure Control」「Identity and Access」「Trust Management」である．これは図 8 中のシステム要求概念定義書の中では抽象的に記述されていたが，実際には上位の Administration 組織で継続的に討議されている事項もある．詳しくは本文中で言及する．
		Data Protection, Privacy and Disclosure Control	
		Non-repudiation Services	
		Identity and Access	
		Trust Management	
		Secure Systems and Networks	
Security Policy Management	Business Security Services と IT Security Services を統合するものであり，整合が取れ実施可能な対策を定義・管理する機能である．	Policy Administration	
		Policy Distribution and Transformation	
		Policy Decision and Enforcement	
		Monitoring and Reporting	
IT Security Services	企業体の各要素に対してセキュリティの機能として調達・配信される基盤的な技術要素である．	Identity Services	これは抽象層であり，多様な認識別ソースから識別情報を管理・共有・連携・アクセスするためのフレームワークである．Identity Foundation/Provisioning/Propagation のサブ要素を持つ．当該プラットフォームでは認識別ソースは全てマスタ管理として扱い，バッチデータ交換・API 呼び出し・GUI による提供の枠組みで管理している．
		Authentication Services	認証に関する機能である．3 章に記した構成を持つ．
		Authorization Services	認可に関する機能である．3 章に記した構成を持つ．
		Confidentiality Services	データ機密性に関する機能であり，認可された利用者以外はデータ・情報の暗号化を施すことで開示禁止とする．これは通信路と AP での利用データ上での考慮が必要で，第一次開発段階から重点設計事項として定義された．しかし第一次開発段階のリリース対象が機構内の利用者を中心としているためリスク発生頻度は軽微と判断され，AP での利用データに対して GNU Privacy Guard を用いた暗号・復号化処理の実装は延期されている．
		Integrity Services	データ完全性保全に関する機能で，マルウェア混入や不審者による不正アクセスに依る改竄・破壊対策である．図 8 の第一次開発段階から実装されている．
		Audit Services	監視・監査に向けてのログ収集に関する機能であり，第一次開発段階では必要最低限以外は実施されておらず，第一次拡張・強化イテレーションから具体的に実施している． Provenance の点で考慮すべきであるが，一部は本文中で言及する．
Security Enablers	IT Security Services によりその機能が実行されるために利用される各種要素のことであり暗号，リボジトリ，H/W 等の総称である．		この機能は図 8 の第一次開発段階で明示されていると伴に H/W 等は並行して実施された材料データプラットフォーム基盤の基本設計の中で具体化されている．本稿の範囲外のため割愛する．



菊地 伸治（非会員）

1987年東北大学大学院工学研究科修了，2013年会津大学大学院コンピュータ理工学研究科修了，博士（コンピュータ理工学）。1987年～2014年日本電気株式会社・生産技術開発/ソフトウェア開発グループ/中央研究所/公共システム開発本部等に所属，2014年～2018年会津大学特任教授，2018年から国立研究開発法人物質・材料研究機構 NIMS エンジニア，電子情報通信学会/IEEE Computer Society/ACM 各会員，現在，電子情報通信学会サービスコンピューティング研究会委員長。



内藤 裕幸（非会員）

国立研究開発法人物質・材料研究機構 NIMS エンジニア。



門平 卓也（非会員）

2001年早稲田大学大学院理工学研究科資源および材料工学専門分野博士後期課程退学，2004年博士（工学），JST-CREST 研究員等を経て2007年国立研究開発法人物質・材料研究機構に入所，調査分析業務等を経て物質・材料研究機構主幹エンジニア，2014年から材料工学分野におけるデータ活用型研究のための基盤構築業務に従事。



谷藤 幹子（非会員）

日本大学文理学部物理学科卒業，University of Leeds 国際学修了（修士）。2005年物質・材料研究機構に入所，2017年より統合型材料開発・情報基盤部門材料データプラットフォームセンター長，材料データプラットフォーム DICE の構築に携わる。応用物理学会会員。内閣府オープンサイエンスの推進に関する検討会委員。