

データ科学

Vol.5

目次

所長挨拶:

専門分野の n 乗、掛けるデータサイエンス

特集:

- 1 データサイエンスコンペティションの歩み
～専門知識とデータ科学をつなぐ実践教育～
- 2 統計エキスパート人材育成プロジェクト
第3期大学統計教員育成研修 参加報告
- 3 日立ソリューションズ・データ科学センター共催セミナー
AI エージェントとセキュリティ

2026 年 9 月

専門分野の n 乗、掛けるデータサイエンス

2026 年度よりデータ科学センターの所長を務めております酒井です。よろしくお願いいたします。

データ科学センターの主要なミッションとして、早稲田大学における多様な専門分野にデータサイエンスを浸透させることにより、各分野をさらに強化することが挙げられます。さて、本センターに所属する先生方は、既にデータサイエンティストとして高度なスキルをお持ちの上で各自の専門分野の研究に取り込んでおられます。従って、全学に比して極めて小規模ながら、このミッションの成功事例を自ら示す研究者グループとして活躍してくださっているものと思います。

日頃より、専門分野とデータサイエンスの掛け算のみならず、専門分野と専門分野の掛け算、すなわち学際的研究の意義を痛感しております。例えば本センターの先生方の専門分野は、統計的学習理論、統計的因果推論、情報理論、材料科学、計算論的精神医学、自然災害科学、進化生物学、認知神経心理学、地質学、計量経済学など、データサイエンスそのものに限らず多種多様です。このように多様な専門の先生方が同じセンターで一緒に仕事をしていると、お互いの研究作法からの「学び」も多いにあるのではないかと思います。

以下、私個人の研究分野に関連して、私が見て感じたことと、他分野の視点から私自身の分野を省みて感じたことを例示したいと思います。

検索システムや対話システムの評価方法などを専門とする私から見ると、他分野で広く使われている評価指標に違和感を覚えることがあります。情報検索（半世紀以上前は図書館から文献を探す研究分野でした）の分野で生まれた再現率という評価指標は、全正解のうちどれくらいが検索できたか、すなわち「検索もれの少なさ」を表す指標です。さて、検索結果の評価に「Recall@1 の平均値」が広く使われている研究分野があります。Recall@1 は「検索結果最上位における再現率」を意味しますが、これは私から見ると以下のようにどう考えても腑に落ちない指標です。

ケース A: 各検索クエリについて正解が 1 件しかない状況。この場合、Recall@1 は Precision@1 もしくは Hit@1 という、最上位が正解であれば 1、そうでなければ 0 という指標に一致します。わざわざ「全正解」を考慮する再現率という言葉を持ち出すことはないと思います。

ケース B: 各検索クエリについて正解が $N(>1)$ 件ある状況。 N は定数です。例えば $N=5$ のとき、Recall@1 の最大値は 1 でなく 0.2 です。どう頑張っても 0.2 にしかならないのに、何の但し書きもなく Recall@1 の平均値を論文で報告しても有益であるとは思えません。

ケース C: 第 i 番目の検索クエリに対し正解が $N(i)$ 件ある状況、すなわち正解件数にばらつきがある場合。このとき、既に見たように、Recall@1 の最大値は例えば $N(i)=1$ であれば 1 ですが $N(i)=5$ であれば 0.2 です。取りうる値の範囲がまちまちの Recall@1 を平均して報告するのは好ましくないと思います。

以上のように、ある研究分野の「しきたり」に対し、他の分野の研究者が違和感を覚えることはよくあるでしょう。当然、私の分野の「しきたり」についても、他の分野から見ればおかしく思える側面が多々あるはずです。例えば、医学、経済学、心理学の分野の一部では、統計的検定にまつわる p-hacking（統計的有意差を報告できるように実験結果をこねくりまわすこと）や HARKing: Hypothesising(*) After the Results are Known（実験結果が出てから研究仮説の辻褄を合わせること）の問題に対処するために、実験を始める前に研究仮説を公にする preregistration が実践されていると聞きます。これに比べ私の分野では、そもそも検定自体をさぼっていたり、多重比較が適切に行われていなかったり、検定力に基づくサンプルサイズの検討がされていなかったりと、だいぶん遅れているように感じます。例えば検索エンジン会社のもつ膨大なデータによる実験下では、サンプルサイズが極めて大きく統計的検定の出番がないケースも多々あるのですが、まあこれは言い訳です。コンピュータサイエンティストである私の場合、上記のような気付きはお医者さまとの共同研究や他分野の書籍を読むことから得られることが多いです。

私の限られた経験に基づき議論しましたが、異分野から自分の知らなかった有用な研究作法を謙虚に吸収しながら、「専門分野×データサイエンス」を超えて「専門分野の n 乗×データサイエンス」のような広い視野に立った研究を行えば、日本もまだまだ世界と戦えるのではないのでしょうか。

(*) 英国綴り

データサイエンスコンペティションの歩み

—専門知識とデータ科学をつなぐ実践教育—

早稲田大学データ科学センター 野村 亮

1. はじめに

早稲田大学データ科学センターでは、文系・理系を問わず、学生が実際のデータを用いてデータ科学を実践的に学ぶ機会として、2019年度から毎年、データサイエンスコンペティションを開催している。2025年度には第7回を迎え、毎年100名を超える学生がエントリーする全学的な行事へと成長した。

本コンペティションの目的は、単に分析精度や高度な手法を競うことではない。学生が自ら問題を設定し、必要なデータを選び、分析結果を検証・考察し、他者に説明するまでの一連の過程を経験することにある。本稿では、これまでの7回を振り返りながら、コンペティションがどのように発展し、早稲田大学のデータ科学教育に何をもたらしてきたかを考えたい。

2. コンペティションの出発点

第1回は2019年7月、参議院議員選挙の結果予測を課題として、データ科学総合研究教育センター（当時）と政治経済学術院の共催により開催された。参加チームは、政党の得票率や候補者の当落を予測し、実際の選挙結果との差だけでなく、予測モデルの内容についても評価を受けた。現実の出来事を対象とし、結果が明らかになる前に予測を提出するという緊張感のある課題であった。

この第1回には、その後のコンペティションにも引き継がれる二つの特徴が既に表れていた。一つは、現実の課題と実際のデータを用いることである。もう一つは、予測精度や当落予測の正否といった数値上の成績だけでなく、どのような問いを立て、なぜそのデータと分析手法を選び、結果をどう解釈したかを重視することである。

3. データと問題設定の広がり

第2回（2020年度）では、商学学術院との共催により、株式会社ADKマーケティング・ソリューションズから提供された生活者総合調査等のマーケティングデータを用いた。各チームは共通の企業データを起点としながら、自由にテーマを設定して分析と発表を行った。新型コロナウイルス感染症の影響

を受けてオンライン開催となったが、企業が保有する実データに学生が向き合う産学連携型の取り組みとして、新たな展開を示した。

第3回（2021年度）は人間科学学術院との共催で、「SDGs×データサイエンス」をテーマに開催された。学生はSDGsの17目標から自らの関心領域を選び、オープンデータを組み合わせて多面的に分析した。47チーム149名がエントリーし、当日は約120名が参加した。テーマは感染症、食品ロス、子どもの成長、ジェンダー、気候変動、情報の偏りなど多岐にわたり、同じ大きな社会課題に対しても、専門や関心によって異なる問いが生まれることを示した。

第4回（2022年度）は教育・総合科学学術院との共催で、みずほ銀行が提供する統計データサービス「Mizuho Insight Portal (Mi-Pot)」を利用し、各種金融取引等に関する統計データを分析対象とした。37チームが発表会に参加し、防災、公共政策、地域分析、居住地の推薦など、金融データの一般的な用途を越える多様な提案が行われた。オンライン開催でありながら120名以上が参加し、回を重ねるごとに分析と発表の水準が向上していることも確認された。

第5回（2023年度）は理工学術院との共催で、日本経済新聞社の36か月分の新聞記事データを共通の分析対象とした。約30チームがエントリーし、第1回以来4年ぶりに対面で開催された。当日は学生、審査員、関係者等を含む約130名が来場した。ポスター発表やコーヒブレークを通じて、学生同士のほか、学生と審査員との間でも直接議論が交わされた。こうした交流は、他者の分析から学ぶというコンペティションの側面を改めて際立たせた。

第6回（2024年度）は、早稲田大学データ科学センターの単独主催により、「早稲田大学で過ごす中で抱いた興味や問題意識へのデータ科学的アプローチ」を共通テーマとして開催された。学生は、分析対象とするオープンデータを自ら選択した。さらに第7回（2025年度）では、独立行政法人統計センターおよび総務省統計局の後援を受け、統計センターによる国勢調査データの作成に関する講演も実施された。いずれもエントリー数は100名を超えており、第7回の会場には学生を含めて当日約120名が来場した。

こうして振り返ると、初期のコンペティションでは共通課題や企業提供データを分析することが中心であったのに対し、近年は、学生が自ら問いを立て、適切な公開データを探し、分析プロセス全体を設計する方向へと比重が移っている。これは、データを「与えられたもの」として扱う段階から、目的に応じてデータを選び、その限界も含めて考える段階への発展といえる。

4. 専門知識とデータ科学の「二刀流」

データサイエンスという言葉から、理工系の学生が中心の催しを想像するかもしれない。しかし、実際には人文社会系を含む多様な学部・研究科から学生が参加してきた。例えば第7回（2025年度）では、エントリーした学生のうち、理工系の学部および大学院に所属する学生はおよそ16%であった。

学生の発表で特に興味深いのは、所属する学術分野で学んだ専門知識が問題設定に反映される点である。公共経済学を学ぶ学生は政策課題をデータによって検証し、推薦システムを研究する学生はその知見を応用して新たなサービスを提案する。分析対象に関する知識があるからこそ、データから意味のある問いを引き出し、結果を慎重に解釈できる。

同じデータを用いても、チームによって着目点も結論も異なる。他チームの発表を聞いた学生からは、異なる視点からの分析に刺激を受けたという声が聞かれる。総合大学である早稲田大学において全学的なコンペティションを開催する意義は、データ科学を一つの専門領域に閉じず、多様な専門知が交わる共通言語として機能させることにある。

5. 分析手法の先にある学び

ソフトウェアの高度化や生成AIの普及など、分析環境の発展によって、一定の知識があれば高度な手法を試すことは以前より容易になった。一方、複雑な手法を用いること自体が、分析の価値を保証するわけではない。目的や問題設定に合わない手法を用いれば、もっともらしく見える誤った結論を導くおそれがある。

コンペティションで重視してきたのは、課題設定、データ選定、分析手法、得られた知見、プレゼンテーションを総合的に評価することである。基礎的な分析であっても、問いとの対応が明確で、データの性質と限界を理解し、結果を適切に説明できることが重要である。第7回の閉会挨拶でも、松嶋敏泰センター所長から、データを揃えることの難しさに気づくこと、そして「本当にやりたい目的のためにどう分析すべきか」を考えることの重要性が改めて示された。

学生は数か月にわたり、チームで役割を分担しながら、データの収集・加工、分析、検証、資料作成、発表、質疑応答に取り組む。うまくいかなかった分析を見直し、他者の質問を受けて自分たちの前提を再検討する経験も含め、通常の講義だけでは得にくい実践的な学びとなっている。

6. 今後に向けて

7 回の開催を通じて、コンペティションは早稲田大学のデータ科学教育における実践の場として定着した。一方で、今後取り組むべき課題がある。第一は、参加者の裾野をさらに広げることである。高度な手法が、初学者にとって参加の壁とならないようにする必要がある。データ科学教育プログラムの履修者が、学んだ知識を試す次の一步として参加できる導線と支援が必要である。

第二は、専門知識とデータ科学の双方をさらに深めることである。コンペティションをきっかけに生まれた問いや分析を、卒業論文、修士論文、共同研究などへ発展させることもできる。所属分野の専門性とデータ科学の高度な実践力を併せ持つ「二刀流」の人材を育てるためには、コンペティションを一過性の行事に終わらせず、教育科目や研究プログラム、教材と有機的に接続させることが重要である。

その基盤の一つが、センターが継続的に開発しているデータ科学教育プログラムと、その内容に即して刊行を進めているテキストシリーズ「ライブラリ データ科学」である[1]。本シリーズは、記述統計・推測統計・ベイズ統計といった異なる立場からの問題設定を、意思決定という統一的な視点から体系化するもので、『データ科学入門 I～IV』が既に刊行されている。今後は「回帰と分類のデータ科学」「時系列構造のデータ科学」など、コンペティションで学生が実際に用いる分析手法に対応する巻も順次刊行される予定であり、課題への取り組みを通じて生じた関心を、体系的な学びへと接続する足がかりとなることが期待される。

さらに、より研究志向の強い学生に対しては、大学院生を対象とする「データ科学研究力養成プログラム」が受け皿となる。本プログラムでは、参加者が所属研究科での研究とは別に、センター教員の指導のもとでデータ科学そのものに関する研究演習や論文作成に取り組む。参加者はデータ科学の研究者を志す者に限られず、データ科学の研究力を各自の専門分野で活用することが期待されている。コンペティションで芽生えた問題意識を、こうした教育科目・教材・研究プログラムへと段階的につなぐ導線を今後さらに整えていきたい。

第三は、学内外の交流をさらに推進することである。企業や公的機関からのデータ提供、実務家による審査と助言、異なる学院の学生同士の交流は、分析を現実の課題と結びつけるうえで大きな役割を果たしてきた。特に第 7 回で実現した統計センターとの官学連携は、公的統計に関する専門的知見と大学の教育活動を結びつけるものであり、学生がデータの来歴や特性を踏まえて分析することの重要性を学ぶ貴重な機会となった。また、総務省統計局からも後援を受け、公的機関の支援・協力のもとで実践的な

教育を展開することができた。データの適切な利用と安全管理に留意しつつ、産学官の連携を通じて、学生が社会の課題に向き合う機会を今後も広げていく必要がある。

7. おわりに

データサイエンスコンペティションは、順位を競うだけの場ではない。学生が自ら問いを立て、データと向き合い、専門知識と分析手法を結びつけ、得られた結果を他者と議論する学修の場である。第1回から第7回まで、扱うデータや開催形式は変化してきたが、この基本的な目的は一貫している。

今後も、データ科学を一部の専門家だけのものとせず、多様な学問分野と社会の課題をつなぐための力として育てていきたい。コンペティションが、学生一人ひとりにとって、データによって自らの問題意識を確かめ、新しい知見を生み出す出発点となることを期待している。

参考文献

[1] 松嶋敏泰 監修，早稲田大学データ科学教育チーム 著：『データ科学入門Ⅰ～Ⅳ』，サイエンス社。

統計エキスパート人材育成プロジェクト

第3期大学統計教員育成研修 参加報告

早稲田大学データ科学センター講師 望月泰博

私は、2024年4月から2026年3月まで、文部科学省「統計エキスパート人材育成プロジェクト」の第3期生として「大学統計教員育成研修」に参加し、2年間の研修課程を修了した。本プロジェクトは、デジタル・トランスフォーメーションの進展に伴ってデータ分析能力を有する人材への需要が高まる一方、大学などにおいて統計学を専門的に教育できる教員が不足しているという課題を背景に、2021年度に開始された事業である。統計数理研究所を中核機関とする「統計エキスパート人材育成コンソーシアム」が実施主体となり、大学院修士課程の学生に統計学を教授できる「大学統計教員」を育成するとともに、育成された教員が各大学における統計教育の中核となり、さらに多くの「統計エキスパート」を育成する仕組みを構築することを目的としている。研修では、単に統計解析の手法を身につけるにとどまらず、「基本的な統計学」「発展的な統計学」に加え、自身の専門分野と統計学を融合した大学院レベルの科目を担当できる能力を身につけることが目標とされている。

第3期研修は、約半年ごとの4つのクールに分けて2年間実施された。研修生全員とメンターが参加する「全体研修」と、シニア大学統計教員をメンターとする少人数のゼミ形式による「グループ研修」に加え、医療統計、統計的時系列分析、統計的因果推論、機械学習など、各分野を専門とするメンターが担当する講義科目が開講された。さらに、各自の関心や専門に応じて、コンサルテーション演習、教材開発演習、共同研究演習などの実践的な演習科目を選択して履修する構成となっており、研修の大部分はオンラインで進められた。この他、全国の参画大学などを会場とする中間報告会や、統計関連学会連合大会における企画セッションなども実施され、普段はオンラインで交流する異なる専門分野の研修生やメンターと直接議論できる貴重な機会となった。

研修の中で特に多くの時間を費やした活動の一つが、全体研修として行われた「模擬講義」および「公開模擬講義」であった。研修生には、第1クールでは基礎的な統計学、第2クールでは発展的な統計学、第3・第4クールでは自身の専門分野と統計学を融合させた内容というように、段階を追って難度を高めながら講義を行うことが求められた。講義後には、他の研修生やメンターから、講義内容、構成、説明方法などについてフィードバックを受け、それを踏まえて講義方法について修練を重ねた。自分自身がある統計的概念を理解していることと、それを他者が理解できる形で説明できることは必ずしも同じではない。講義を準備する過程では、どの程度まで数式を用いるべきか、理論的な説明と具体例をどのような順序で配置すべきか、受講者がどこでつまづく可能性があるかなどを改めて考える必要があった。こうした作業を繰り返すことによって、統計学の知識そのものを再確認すると同時に、その知識を構造化し、受講者に伝わる形へと組み替えるという教育上の視点を身につけることができたと考えている。また、

他の研修生による模擬講義を聴講することも、自分とは異なる説明方法や教材構成に触れる機会となり、自身の授業設計を振り返る上で有益であった。各研修生がそれぞれの専門や教育経験を生かした講義を行う中で、私自身は、データ科学センターが提供する講義科目を参考に、理論的な説明だけでなく、Pythonを用いた実践的な演習を組み込んだ講義を行った。

統計学およびデータサイエンスに関する専門講義では、各分野を専門とするメンター陣による講義を通じて、幅広い知識を得ることができた。医療統計、統計的時系列分析、統計的因果推論、多変量解析、観察研究の統計的方法、機械学習、多重比較法など、多岐にわたる科目が開講された。一部の科目は必修である一方、それ以外についても各自の関心や専門性に応じて聴講することができる仕組みとなっていた。私自身は、岩崎学先生による「統計的因果推論」や、赤穂昭太郎先生による「機械学習基礎」などを履修したほか、時間の許す限りさまざまな講義に参加した。自身の専門に近い内容だけでなく、これまで十分に触れる機会のなかった統計分野について体系的に学べたことは、本研修の大きな利点の一つであった。

グループ研修では、各研修生が自身の専門分野や研究上の関心に応じて異なるメンターのゼミに所属した。私は行動経済学に関連する研究を行っていることから、統計学・計量経済学を専門とする国友直人先生のゼミに所属した。グループ研修では、国友先生から模擬講義の資料や発表について継続的にご指導いただいたほか、北川源四郎先生、椿広計先生をはじめとする先生方による講義を拝聴する機会にも恵まれた。また、国友先生が内閣府からの依頼を受けて行っていたコンサルテーションに同席する機会もあり、統計学の専門知識が実際の政策課題に対してどのように活用されるのかを間近で見ることができたことは、他では得難い経験であった。

このほか、選択制の実践的な演習として、共同研究演習や教材開発演習にも取り組んだ。まず、国友先生との共同研究演習では、「過適合と二重降下現象」をテーマとする研究に取り組んだ。一般に、モデルを複雑にしすぎると訓練データへの過適合が生じ、未知のデータに対する予測性能が低下すると考えられている。一方、近年の機械学習では、モデルの複雑さをさらに高めることで、いったん悪化した汎化性能が再び改善する「二重降下 (double descent)」と呼ばれる現象が注目されている。この現象を統計学の観点から検討したことは、既存の分析手法を単に利用するだけでなく、その背景にある統計的性質や理論そのものを研究対象として考える経験となった。この研究については研修終了後も継続して取り組んでいる。また、教材開発演習では、統計的学習の代表的な教科書である *An Introduction to Statistical Learning* に関連する日本語教材の作成に携わった。同書の内容を詳細に読み込み、教材として再構成する作業を通じて、統計的学習について理解を深めることができた。また、第3期研修生全員で「基本的な統計学」の講義資料スライドを共同作成したことも、大きな経験であった。私の担当部分については、メンターの一人として第3期研修を中心的に取りまとめたくださった中西寛子先生から詳細なコメントをいただき、教材の構成や説明方法を改めて考える貴重な機会となった。

2年間の研修を振り返ると、最も大きな収穫は、これまで身につけてきた統計学やデータ分析の知識を改めて体系化すると同時に、それを教育や研究指導へと展開する視点を得たことである。また、第3期生には医学、工学、薬学、物理学、農学、社会科学、教育学など多様な分野を背景とする研究者が参加しており、異なる領域において統計学・データサイエンスがどのように利用され、どのような教育上・研究上の課題が存在するのかを知ることができた。さらに、メンターの先生方や他の研修生との交流を通じて築かれた人的ネットワークも、今後の教育・研究活動を進めていく上で大きな財産になると考えてい

る。こうした多くの学びや経験、そして新たな人的ネットワークを得る機会を、2年間にわたり業務の一環として与えていただいたデータ科学センターの皆様、この場を借りて改めて御礼申し上げたい。

最後に、2026年3月をもって2年間の大学統計教員育成研修を修了したが、本研修の意義は修了そのものではなく、ここで得た知識、教育・研究経験、そして人的ネットワークを、今後の教育・研究活動へと継続的に還元していくことにありと考えている。データサイエンスやAIが研究のみならず社会のさまざまな場面で急速に浸透する中、データサイエンスの考え方や適切な活用方法を次の世代に伝えることの重要性は、今後ますます高まっていくだろう。私自身は、本研修で培った経験をデータ科学センターにおける教育・研究活動に活かし、統計的手法を単に適用できるだけでなく、その前提や限界を理解し、データから得られる結果を適切に解釈できる人材を育成することで、本プロジェクトが目指す「統計エキスパート人材育成」の循環に貢献していきたい所存である。また、現在は第4期の大学統計教員育成研修が進められているほか、2026年度からは後継事業として「高度統計人材育成強化拠点形成事業」が開始され、統計学教員の育成が引き続き進められる予定である。今後、本プロジェクトで培われた成果やネットワークがさらに発展し、統計学を基盤として次代のデータサイエンス・AIを支える人材育成の輪が一層広がっていくことを期待したい。

日立ソリューションズ・ 早稲田大学データ科学センター 共催セミナー -AI エージェントとセキュリティ-

1. AI とセキュリティ、双方の専門家がその最前線を語り合う

2026 年 3 月 18 日（水）、早稲田キャンパスにて、株式会社日立ソリューションズと早稲田大学データ科学センター共催のもと、「AI エージェントとセキュリティ」をテーマとしたセミナーを開催した。

早稲田大学と日立ソリューションズは、データ科学分野におけるセキュリティ領域を中心とした人材育成と産学連携促進を目的に、2020 年に学術交流協定を締結している。本セミナーでは、技術の進化と社会実装が急速に進む生成 AI や AI エージェントと、それに伴うセキュリティリスクについて、日立ソリューションズの有識者と早稲田大学の教員が登壇し、講演およびパネルディスカッションが行われた。司会進行は、早稲田大学データ科学センター教務主任である須子統太准教授が務めた。

講演に先立ち、早稲田大学データ科学センターの小林学教授から、本セミナーをはじめとする早稲田大学データ科学センターと日立ソリューションズとの連携や、早稲田大学グローバル・エデュケーション・センターにて開講される提携講座の科目「未来社会を創るセキュリティ最前線」の紹介があり、セキュリティへの意識が重要になる中、講座やセミナーを通じて、参加者にもその最先端の状況に触れ、未来について一緒に考えてほしいとその意義を語った。続いて、日立ソリューションズシニアセキュリティエバンジェリストである扇健一氏が登壇。日立グループの情報通信分野における中核企業として、「DX by AX toward SX」のスローガンのもと、世界各国で AI を活用したデジタルトランスフォーメーションを推進していることを紹介した。また、本セミナーの主題であるセキュリティについて、鉄道やエネルギーなど、社会インフラにおける OT (Operational Technology) 環境のデジタル化に携わる同社にとって、サイバーセキュリティは重点事業の一つであると強調。ホワイトハッカーを始めとする高度なセキュリティ人材の育成や、企業に対する啓発とコンサルティング、EU のサイバーレジリエンス法への対応など、多様な側面から取り組みを進めていることを示した。

2. AI 時代における専門家の意義とビジネスにおけるセキュリティ事例

講演の前半は、「ビジネスで AI を相棒にするために考える、セキュリティのリスク」と題し、AI 時代における専門家のあり方や、日立ソリューションズにおけるセキュリティ対策の事例について、日立ソリューションズ シニアセキュリティアナリストの米光一也氏と扇氏が語った。

同社のホワイトハッカーとして長年活躍している米光氏は、ハッキングに対する高度なセキュリティ技術で、日立グループに対するサイバー攻撃への対応の最前線で活動している。自身のキャリアの中で、ホワイトハッカーという肩書きが、第三者からの専門性への理解を深め、コンサルティングや講演、取材といった活動につながってきたと述べ、参加者にも、今回のセミナーを通じて専門家をめざすうえで、肩書きは大切にしたいとメッセージを送った。

また、東京大学経済学研究科の小川光教授のコラム記事を紹介。AI による論文執筆のエピソードの捉え方に、今後の AI 社会でどう生きていくかというセンスが問われるとした。その上で、自身の見解として、「単なる AI での出力と、実際の社会実装では、必要となるスキルが全く違う。長年積み重ねてきた経験が物を言う領域があり、同じ専門家だからこそ、小川教授のコラムからも『余力』を感じた」と結んだ。



続いて登壇した扇氏は、シニアセキュリティエバンジェリストとしての自身の経歴とともに、日立ソリューションズが開発を進める AI エージェントの事例について紹介した。

同社のグループ企業である Hitachi Solutions America では、取引先との契約時における負荷軽減と効率化に向けて、AI エージェントの活用を進めている。軍事転用可能な技術や製品の移転は、各国の法律で厳しく管理されている一方、申請は年間 2,000 件にも及び、申請側と審査側双方にとって大きな負担となっていた。こうした背景のもと、輸出管理、取引予定顧客のスクリーニング、ふるいわけ業務を行う AI エージェントが開発されている。

ただし、セキュリティリスクについては試行錯誤の最中であり、プロンプトインジェクションのリスクを指摘。「企業が持つ機密情報を守るためには、攻撃に対するガードを高める必要がある。その一方で、AI の利便性を下げることには慎重でなければならない。両者のバランスを取ることが今後の課題である」とした。



3. 急速に進化するエージェントック AI と近年の事例

講演の後半は、小林教授が登壇し、「AI ワークフローの作成と活用」をテーマに、AI エージェントの現状について実際の事例やデモンストレーションを交えて解説した。

小林教授は、AI エージェントの普及が爆発的に進んでおり、2025 年が AI エージェント元年と呼ばれていることを紹介。また、エージェント AI の定義として、単に入力に対して出力を返すだけではなく、特定の目的を持ち、タスクを分解して、必要に応じた他の AI を始めとする外部環境とインタラクションして、タスクを自動実行する AI システムであるとした。さらに、目標設定から設計、推論、協調、改善といった PDCA サイクルまで行うようになった AI はエージェンティック AI と呼ばれ、近年は両者の垣根がなくなりつつあり、OpenAI や NEC はエージェンティック AI に用語を統一していることを指摘した。



こうしたエージェンティック AI の製品事例として、Google の Opal や NotebookLM、Claude Code について、デモンストレーションを実施。誰でも気軽にエージェンティック AI を活用できる環境が提供されていることを紹介した。また、講演の結びとして、エージェンティック AI は利便性が高い一方、その中身を知ることが重要だと指摘。「何をやりたいのか、AI が実際にどのように動いているのかを理解し、得られた結果を検証していくことが必要である」と述べた。

4. サイバー攻撃の事例から考える、AI とセキュリティの結節点

パネルディスカッションは「AI エージェント時代のセキュリティ」をテーマに、日立ソリューションズから扇氏、米光氏、データ科学センターからは小林教授、須子准教授、望月泰博講師が登壇した。司会是小林教授が務めた。

まずは小林教授が、直近に発生したサイバー攻撃の事例へ言及。扇氏が具体的な企業を上げつつ、その現状を解説した。扇氏は、とりわけ 2025 年 9 月に発生した食品・飲料メーカーへの被害の規模、社会への影響も大きかったとし、ランサムウェアの攻撃目標が基幹データの存在するデータセンターへ深化していると言及。バックアップデータが存在しても、多くの企業で実際の復旧作業のノウハウが蓄積されていないという問題点を指摘した。

続いて、小林教授はプロンプトインジェクション^{※1}について概要を紹介。AI に対する攻撃を実例とともに参加者に示した。扇氏は IT ベンダーから AI ファイアウォールの提供が始まっているが、コストの面からハードルが高いと分析。米光氏はそれに加え、MCP (Model Context Protocol) や A2A (Agent to Agent) といった AI の参照先に関するセキュリティ脅威の議論が進んでいるものの、対策の具体的な実装の議論はこれからである現状を示した。望月講師は、論文審査における AI の査読結果改ざんの可能性を上げ、当面は別 PC の使用など、物理的な切り分けが必要になるのではとした。こうした議論を受け須子准教授は、個人が AI によって自由にアプリを開発できる今、製品側が介入できる領域の限界や、自然言語を使用した攻撃への対応の難しさを指摘。米光氏はこれを受け、「プロンプトインジェクションは、ポピュラーな脅威として挙げられるが、そもそも誰の何を守るかという視点が必要。セキュリティの限界がある中で、誰のためのセキュリティなのかについて、一考の余地がある」とまとめた。

話題は AI エージェントに対するセキュリティに移り、小林教授から OpenClaw に関する説明が行

われた。2026 年に公開された OpenClaw は、汎用性と利便性の高さから急速に人気となった一方で、当初からセキュリティ面における課題が数多く発見され、サンドボックス上で操作する NemoClaw も発表された。こうした現状を前に、扇氏は AI エージェントが進化し、ユーザーが意図しないセキュリティインシデントが起きうる以上、企業は慎重な姿勢をとらざるを得ないと説明。使用するサービスの明確化やアクセス制限と ID 管理を徹底した上で、ゼロトラスト※2 の対応を意識するしかないとした。扇氏は、利便性とリスクのバランスをとる上でも、セキュリティの専門家の役割はより重要になっていると付け加えた。望月講師は、ユーザー側の視点として、AI への理解を深める必要があるとし、須子准教授は ASI アライアンスの話題に触れ、ブロックチェーン技術と組み合わせた安全性の担保の試みが進んでいることを紹介した。

小林教授から最後の論点として、今後求められる人材像について話題が振られると、扇氏はフィジカル AI の普及に触れた上で、「必要なのは倫理観。フィジカル AI の開発と並行して、それをガードする AI の開発を進めなければならない。コストはかかるが、社会実装が進む今だからこそ、取り組んでいくことが重要」と述べた。米光氏は日本におけるセキュリティ人材の不足を指摘し、実務能力に加えて、ステークホルダーの意見をすり合わせてアイデアを実現させる能力が求められるとした。望月講師は、データ科学センターにて日頃受けている学生からのデータ科学研究相談の内容に触れ、「意思決定をしていくためには、ざっくりとでもいいのでまずは知識を身につけ、広い視点からポイントを絞って確認することが重要である」と述べ、そのための教育の重要性を伝えた。最後に須子准教授は、AI 時代におけるセキュリティ意識の重要性にあらためて言及するとともに、「攻撃と対策がイタチごっこになる中で、セキュリティの最前線で活躍する『超専門家』の役割が重要になる。AI が実務を代替できる以上、どのフィールドにおいても専門的な知識や人材は今後さらに求められていく」と述べ、パネルディスカッションの議論を総括した。



- ※1 攻撃者が第三者の利用する AI に対し、プロンプトや AI が読み込むテキスト・画像などに悪意のある指示を埋め込み、本来の指示よりもその内容を優先させることで、情報漏えいや不正な処理など、意図しない動作を引き起こす攻撃手法
- ※2 社内外を問わず、全てのユーザーやマシン、デバイス、通信を信用せずにセキュリティ上必要な確認や対策を行なうこと

早稲田大学データ科学センター機関紙「データ科学」第5号

発行日	2026 年 9 月 10 日
編集	小林 学
発行者	酒井 哲也
発行所	早稲田大学データ科学センター 〒169-8050 東京都新宿区西早稲田 1 丁目 6-1 1 号館 3 階
