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、肩書きは大切にして欲し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ティック 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。司会は小林教授が務めた。

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