HITACHI
Inspire the Next

News Release

2024年4月4日
株式会社日立ソリューションズ

日立ソリューションズが「AIとセキュリティの交差点」セミナーを早稲田大学と共同開催

理系・文系の学生向けにAI技術の最新動向を事例にセミナーを実施し、次世代セキュリティ人財育成に貢献

株式会社日立ソリューションズ（本社：東京都品川区、取締役社長：山本 二雄／以下、日立ソリューションズ）は、3月6日、「AIとセキュリティの交差点～技術革新の中の安全確保～」セミナーを早稲田大学の学生向けに、同大学データ科学センターと共同開催しました。早稲田キャンパスで開催された本セミナーの参加者は47名で、そのうち文系の学生が約4割となりました。

企業では安全な社会づくりに向けて職種に関係なくセキュリティ知識が不可欠となりつつある中、日立ソリューションズはセキュリティ人財のすそ野を広げることを目的に、データサイエンス分野の人財育成を強化する早稲田大学にて、情報セキュリティの授業を実施しています。本セミナーでは、急速に社会に普及するAI技術の最新動向を題材に、AIがサイバー攻撃を受ける事例やAIを悪用したサイバー攻撃の事例から、セキュリティについて理解を深めました。

早稲田大学 データ科学センターの小林 学教授と中原 悠太講師による事例紹介の後、日立ソリューションズのホワイトハッカーやセキュリティコンサルタントを務め、大学で非常勤講師として授業を行う社員とのパネルディスカッションが行われました。参加した学生からはさまざまな質問が出され、次世代を担う学生たちが技術革新が進展した未来社会における安全確保について考える機会となりました。

日立ソリューションズは重点事業のひとつであるセキュリティの知見をもとに次世代人財育成を支援し、社会のSX（サステナビリティ・トランスフォーメーション）に貢献していきます。

■セミナー実施の背景と目的

日立ソリューションズは、長年にわたるセキュリティ事業で培った知見を次世代人財育成に生かすことを目的に、早稲田大学と学術交流協定を締結しました。情報セキュリティの授業は、2019年度から実施しています。

昨今、生成AIをはじめとするAIやIoT、ビッグデータなどの技術が進歩するとともに、企業のDXの推進やクラウドサービスの利用が拡大しています。高度化・複雑化したAIシステムが幅広い産業に浸透する中、AIシステムに対するサイバー攻撃やAIの悪用に対抗するセキュリティの確保が喫緊の課題となっており、企業においては職種や業種に関係なくセキュリティの知識の重要性がますます高まっています。

そこで、日立ソリューションズは早稲田大学とともに、データサイエンスとしてAIを研究する教員や、ビジネスの最前線でセキュリティの課題解決に取り組む社員による「AIとセキュリティの交差点～技術革新の中の安全確保～」セミナーを実施し、次世代を担う学生たちと未来における安全・安心なデジタル社会について、考える場を設けることにしました。

株式会社 日立ソリューションズ
本社　〒140-0002東京都品川区東品川四丁目12番7号
ホームページ:https://www.hitachi-solutions.co.jp/

日立ソリューションズ

■「AI とセキュリティの交差点～技術革新の中の安全確保～」セミナーについて

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は、サイバーセキュリティ月間の 2024 年 3 月 6 日、学生を対象にセミナーを開催しました。

<事例紹介：AI の技術動向と AI システムに関するセキュリティリスク>

早稲田大学 データ科学センターの小林 学教授と中原 悠太講師が、AI 技術の最新動向や AI そのもののセキュリティについて、画像・音声データなどを使ったデモンストレーションを含めた事例紹介を行いました。


事例紹介を行う小林 学教授と中原 悠太講師

<パネルディスカッション：「AI への攻撃に対する安全確保」・「AI の悪用に対する安全確保」>

パネルディスカッションでは、小林教授をモデレータに、パネリストとして日立ソリューションズ ホワイトハッカーの米光一也、セキュリティコンサルタントの扇 健一、中原講師が登壇しました。

最初に小林教授より、「AI への攻撃に対する安全確保」について、データ汚染、モデル汚染、モデル搾取・データ搾取といった攻撃方法について紹介されました。その後、誰がどのように考えて安全確保に取り組むべきか、従来のセキュリティの考え方で安全確保できるのか、議論が行われました。「AI に対する攻撃が高度化する一方で、社会に実装されるレベルで脅威となるためにはまだいくつかハードルがあると思う。セキュリティ対策の考え方として、システム全体で捉え、どこかで脅威を検知できる仕組みを導入するというアプローチは不変であると改めて実感した」「セキュリティの専門家だけでなく、データサイエンティストもセキュリティバイデザインの考え方で攻撃に遭わないための仕組みづくりを考えていかないと、これからの時代は対応できなくなるかもしれない」といった意見があがりました。

続いて、「AI の悪用に対する安全確保」について、小林教授より、テキスト生成 AI による標的型攻撃や個人情報の抽出が行われた事例が紹介され、誰がどのように注意すべきか、議論が行われました。「オープンな技術として利用される以上、ある程度は脅威として想定せざるを得ないと思う。また攻撃のためのコストが下がってきていることも深刻に考えなければならない」「AI 技術の進化で脆弱性を悪用したゼロデイ攻撃のリスクが高まり、ますますサイバーレジリエンスの考え方が求められるのではないか」といった意見があがりました。

株式会社 日立ソリューションズ
本社　　〒140-0002 東京都品川区東品川四丁目12番7号
ホームページ: https://www.hitachi-solutions.co.jp/

日立ソリューションズ


パネルディスカッションの様子

■参加した学生からアンケートで寄せられた声・感想

アンケート回答者の全員から内容に満足という回答があったほか、以下の意見が得られました。

・座学のみでは得られないような現場の知見を得ることができてよかった。

・企業の取り組みや AI について、初心者でもわかりやすい説明があり、詳しく知ることができた。

・非常にわかりやすく興味を引き立てる説明だった。攻撃事例を初めて知ることができた。

・セミナーに参加してセキュリティに興味を持った。講座の受講を検討したいが、前提条件はあるか。

■セミナー開催概要

テーマ：「AI とセキュリティの交差点～技術革新の中の安全確保～」

日時／会場：2024 年 3 月 6 日（水）10：00～12：00／早稲田キャンパス 7 号館 207 教室

主催：早稲田大学データ科学センター、株式会社日立ソリューションズ

共催：早稲田大学高度データ関連人材育成プログラム

開催報告：https://www.waseda.jp/inst/cds/news/4380

■日立ソリューションズと早稲田大学との取り組み

早稲田大学は、グローバルな視点で問題解決に貢献できるリーダーの育成に取り組んでいます。その中の一つとしてグローバルエデュケーションセンターに「データ科学」の科目群を設置し、AI、IoT、ビッグデータなどのデータサイエンス分野における高度な専門知識を持つ人財育成に取り組んでいます。

日立ソリューションズは、セキュリティ分野で、AIや生体認証などを活用し、コンサルティングからシステム構築、運用、教育まで、企業のニーズに合った最先端のソリューションをトータルに提供してきました。

そこで、セキュリティ事業のノウハウを次世代人財育成に生かすことを目的に、2019年から広く人文社会系の学生も対象にした提携講座を毎年実施しています。2020年2月にはセキュリティをはじめとするデータサイエンス分野の人財育成および産学連携促進を目的に学術交流協定を締結し、毎年、時事に基づいたテーマを設定した学生向けのセミナーを共同開催しています。2023年9月には、「サステナビリティの実現に欠かせない、次世代のセキュリティ人財の育成」というテーマで、小林教授と須子統太准教授、日立ソリューションズの米光、扇の4名による座談会を行い、日立ソリューションズのステークホルダーを対象としたコミュニケーションツール「サステナビリティ・アクションブック2023」に掲載しました。

株式会社 日立ソリューションズ
本社　　〒140-0002　東京都品川区東品川四丁目12番7号
ホームページ：https://www.hitachi-solutions.co.jp/

日立ソリューションズ

■講座「未来社会を創るセキュリティ最前線」について

日立ソリューションズは、2019 年から毎年、早稲田大学のデータ科学センターの正規科目として、セキュリティの基本知識と実践的なスキルを学ぶことを目的に授業を実施しています。

授業では、第一線で活躍するホワイトハッカーやセキュリティコンサルタントが講師を務め、企業が直面するセキュリティの課題やその対策について、ケーススタディやハッキング体験などを通じて行われました。来年度も 6 月より「未来社会を創るセキュリティ最前線」を開講する予定です。

■日立ソリューションズのセキュリティ事業

日立ソリューションズは 20 年以上、社会を支える重要インフラやさまざまな企業のセキュリティ対策を支援し、お客さまの課題に合わせたソリューションを提供してきました。その分野は、情報セキュリティ、制御セキュリティ、クラウドサービス、IoT と多岐にわたります。ホワイトハッカーを擁するセキュリティエキスパートが高度な知識や技術を活用し、コンサルティングからシステム構築、運用・保守、インシデント対応まで、包括的にサポートしてきました。これらのノウハウを基に、サイバー攻撃の侵入・被害を前提として、サイバー攻撃の被害を最小限に留め、事業継続を実現する新しい視点でのセキュリティ対策「サイバーレジリエンス」をはじめとしたソリューションで、企業のセキュリティ対策をトータルで支援します。

URL：https://www.hitachi-solutions.co.jp/security/sp/solution/task/cyber_resilience.html

■ 日立ソリューションズの社会貢献活動

URL：https://www.hitachi-solutions.co.jp/company/sustainability/community/

■ 「サステナビリティ・アクションブック 2023」

URL：https://www.hitachi-solutions.co.jp/-/media/Project/DefaultSite/Company/sustainability/SustainabilityActionBook_2023.pdf

■ 商品・サービスに関するお問い合わせ先

URL：https://www.hitachi-solutions.co.jp/inquiry/

――

――

株式会社 日立ソリューションズ
本社　　〒140-0002 東京都品川区東品川四丁目12番7号
ホームページ: https://www.hitachi-solutions.co.jp/

日立ソリューションズ