セキュリティ・キャンプ2025ミニ（オンライン開催）

応募期間延長
9/15(月) → 9/29(月)

2025年10月18日（土）～10月19日（日）

オンライン方式による専門講座

応募締切：2025年9月15日（月）16時

ステップアップを目指す学生のための、全国どこからでも参加できるオンラインイベントです。
全国大会を目指す方も、さらにスキルを伸ばしたい方も、ぜひご参加ください！

■開催概要

日程	2025年10月18日(土) 9:00 ～ 10月19日(日) 17:30 (土日2日間のオンライン講義)
講義実施方式	Zoom、Discord、Kintoneを使用したオンライン形式による開催
参加資格	日本国内に居住する、2026年3月31日時点において25歳以下の大学院生・学生・生徒・児童
定員	40名 選考あり
主催	一般社団法人セキュリティ・キャンプ協議会、独立行政法人情報処理推進機構(IPA)
費用	無料 (PCやネット環境は受講者ご自身でご用意いただく必要があります)
URL	https://www.security-camp.or.jp/minicamp/online2025.html

■プログラム

1日目 10月18日 土曜日 9:00～18:00	
9:00	『開会式』 セキュリティ・キャンプ協議会
9:30	『倫理講義』 西尾 太一 氏 大阪地方裁判所第21民事部(知的財産権部)判事
10:10	休憩
10:20	『LLMアプリの脅威と安全な作り方』 湯浅 潤樹 氏 サイボウズ株式会社 近年、ChatGPTをはじめとする大規模言語モデル(LLM)を用いたアプリケーションが急速に広がっています。しかしその裏では、従来のWebアプリとは異なる新しい脆弱性や設計上の落とし穴も数多く報告されています。 この講義では、特にRAG(Retrieval-Augmented Generation)と呼ばれるLLM活用パターンを例に、どのような脅威が存在するのかを探ります。脅威モデリングという手法で「どこに危険が潜んでいるのか」を考え、実際にLLMアプリを操作しながら「本当に危険なことが起きるのか？」を検証することで、安全なLLMアプリの作り方を学びます。
13:20	昼食休憩
14:20	『RFCを読んで実装してみよう！』 小林 麟太郎 氏 慶應義塾大学 本講義では、インターネット技術の標準的な仕様を策定するRFCを読みこみ、実装までの一連のプロセスをご体験いただきます。英文で書かれ、とっつきにくい印象があるRFCですが、実装とセットで読み込むと、より容易に理解することが可能です。 ハンズオンとしては、Tor等のトラヒック匿名化や、企業等におけるフィルタリングなど様々な用途で用いられている、比較的身近なSOCKS5プロトコルを取り上げます。RFCを読み込みながら、SOCKSプロキシをRustの標準ライブラリであるstd::netを用いて自作し、実際にトラヒックが転送されている様子を確認することで、みんなで感動を共有できればと思います。 また時間上可能であれば、簡単なインスペクション機能やユーザ認証によるトラヒックの識別といった、より実践的な実装についても取り扱う場合がございます。
17:20	コミュニケーションタイム
18:00	1日目講義終了

■プログラム（続き）

2日目 10月19日 日曜日 9:00～17:30	
09:00	『Windows バイナリ実験講座』 大杉 浩太郎 氏 富士通ディフェンス＆ナショナルセキュリティ株式会社 多くの企業向け環境で Windows が採用されていることもあり、マルウェア解析などの実業務においては、Windows バイナリ（PE ファイル、プロセスなど）に関連した知識が要求されます。 この講座では、実験やcrackme 形式の演習問題を通して、Windowsバイナリとその解析手法、エクスプロイト手法等について、マニアックかつ実践的な知識を学びます。 また、具体的な知識だけではなく、ソフトウェア・リバースエンジニアリングの中で直面する様々な困難に対して、切り込んでいく力を身につけていただくことも目的としています。 リバースエンジニアリングは根気のいる作業ですが、時間をかければ理解できるようになります。一緒にバイナリ畑を歩いていきましょう!
12:00	昼食休憩
13:00	『触って学ぶ、マルチエージェントシステム・セキュリティ』 高江洲 勲 氏 三井物産セキュアディレクション株式会社 本講義では、AIエージェント同士が連携して動作する「マルチエージェントシステム（Multi-Agent-System: MAS）」におけるセキュリティリスクと対策を、ハンズオンを通じて学びます。 近年、AutoGenのようなAIエージェント・フレームワークやMCP, A2AのようなAIエージェント・プロトコルが急速に進化し、複数のAIエージェントが役割分担しながらタスクを自律的に実行するMASの利用が広がっています。その一方で、AIエージェント間通信の改ざんやAIエージェントが利用する外部ツールの偽装など、MAS特有の攻撃手法も登場しており、従来のセキュリティ対策だけでは対策できない課題が見えてきました。 本講義では、AIエージェントや外部ツールの偽装、プロンプトインジェクションの連鎖など、MAS特有のセキュリティリスクを再現・分析し、攻撃と防御の両面からその本質を学びます。 AIセキュリティやマルチエージェントシステムの開発に関心のある方に向け、「机上の調査だけでは見えないMAS特有の脅威」と「実用的な対策技術」を、ハンズオンを通じて学べる内容となっています。ぜひ一緒に、AIエージェント時代のセキュリティを学びましょう。
16:00	休憩
16:10	『閉会式』 セキュリティ・キャンプ協議会
16:30	コミュニケーションタイム
17:30	解散

■募集要項（事前にご確認ください）

応募条件	・日本国内に居住する、2026年3月31日時点において25歳以下の大学院生・学生・生徒・児童 ・2025年10月18日時点で18歳未満の場合、本大会の参加について保護者の同意を得ていること（参加が決定した際に保護者の同意書を提出していただきます） ・応募者は、演習で使用する下記条件のPCを開催期間中に使用できること - 応募者自身がキャンプに使用するオンラインサービス 、ソフトウェアを使用できること - あらかじめ指定した解析ツール、開発環境等が動作するスペックのCPU、メモリ残量、SSDまたはHDD20GB程度のの空き容量があること ・応募者は通信容量無制限または、オンライン講習に必要な容量の通信機器（有線LAN、無線LAN等）を開催期間中に使用できること（無料Wi-Fiスポット、飲食店や公共施設などの無料 Wi-Fiサービスを利用しての受講はできません） ・開催期間中に応募者が受講するスペース、または自室があること（図書館などの公共施設、飲食店等での受講はできません） ・講義ではミーティングツールを使用予定ですが、講義に接続・参加するための、ヘッドフォンやイヤフォン、マイク、カメラが使用できること ・Rustの簡単なコーディングが可能なこと。（あまり書いたことがない方でも大歓迎です。） ・x86のWindows環境の準備を推奨（Arm版のWindowsでも不可能ではないですが、サポートはできないかもしれません。） ・C、C++、x86 のアセンブリ、Python を勉強している、または書けるようになりたい方 ・Binary Ninja、IDA Pro、WinDbg などの解析ツールを使ってリバースエンジニアリングに挑戦している （しようとしている） 方 ・PC上でLinux（Ubuntu）が動作すること（WindowsならばWSL2が動作すること） ・PCにDockerがインストールされている、またはインストールできること ・セキュリティまたは、プログラミングに関して、講習を受けられるだけの基礎知識と積極的に取り組む姿勢を持っていること ・別途定める「セキュリティ・キャンプ2025ミニ（オンライン開催）」実施規定を遵守できること

■募集要項（事前にご確認ください） つづき

申込方法	以下のセキュリティ・キャンプ協議会のWebページからお申込みください。 https://www.security-camp.or.jp/minicamp/online2025.html#Id03
申込締切	9月29日（月）16:00必着（16:00までに到着したものを有効とします）
参加者決定のお知らせ	審査の上、10月3日（金）までにメールまたは電話にて連絡します。
留意事項	・申込者多数の場合には、参加できないことがあります。参加者は、申込書の記入必要事項及び選考問題の回答内容を審査の上、地方在住者、過去のセキュリティ・キャンプ全国大会／ネクストに未参加の方を優先に選考します。 ・参加が決定された方には、応募条件を満たすことを証明する書類（学生証のコピーや学校が発行する在籍証明書等）、参加誓約書（参加規程を遵守する旨の誓約）、倫理行動宣誓書、その他主催者が必要と定める書類を提出していただきます。 ・主催、マスコミ各社により、写真・動画撮影、取材などが行われることがあります。氏名・学校・顔写真などを含む受講時の様子が広報、啓発の目的で公開される場合がございます。 ・本事業の成果をはかることを目的として、参加後アンケートや定期的にその後の活動状況についてフォローアップ調査を実施させていただきます。参加はアンケート回答必須となるため事前にご了承ください。 ・受講およびイベント参加中は、20歳以上であっても、飲酒・喫煙を禁止します。 ・「セキュリティ・キャンプ2025（オンライン開催）」に参加した方でも、セキュリティ・キャンプ全国大会や他のミニキャンプの応募は可能です。

■講師プロフィール

西尾 太一（にしお たいち）

私立六甲高校を卒業後、東京大学理学部、早稲田大学法務研究科を経て、2012年1月に大阪地方裁判所判事補に任官。以後、札幌地方裁判所、神戸地方裁判所姫路支部、名古屋地方裁判所を経て現職。途中、2年間弁護士職務経験を行い、その際、OWASPKansaiのメンバーに加入。以後、セキュリティコミュニティで勉強中。資格マニア（情報処理安全確保支援士・測量士・電気工事士・電験3種・工事担任者総合通信・電気通信主任技術者等）

湯浅 潤樹（ゆあさ じゅんき）

サイボウズ株式会社に所属し、プロダクトセキュリティ関連業務に従事。
2022年のセキュリティ・ネクストキャンプを修了し、2023年には全国大会でBトラックのチューター、2024年にはミニキャンプで講師を経験。
趣味は釣り、最近の興味分野はLLMアプリのセキュリティ。

小林 麟太郎（こばやし りんたろう）

Global Cybersecurity Camp 2022 Taiwan 修了。
2024年度未踏「ゼロトラストネットワークアクセスの導入を容易にするクラウド型プロキシの開発」に取り組む。

大杉 浩太郎（おおすぎ こうたろう）

セキュリティ・キャンプ全国大会2017を修了。
その後EDRを用いたフォレンジックを経験し、現職では低レイヤーを軸に研究業務に従事している。

高江洲 勲（たかえす いさお）

情報処理安全確保支援士。CISSP。
AIセキュリティに着目し、機械学習アルゴリズムの脆弱性に関する研究（Security for AI）や、機械学習を用いたセキュリティタスク自動化の研究（AI for Security）を行っている。研究成果は、世界的に著名なハッカーカンファレンスであるBlack Hat Arsenal（ASIA・USA・EURO）やDEFCON（Demo Labs・AI Village）、CODE BLUE、AVTOKYO、BSides（Tokyo・Singapore）等で発表している。近年はセキュリティ・キャンプ（2019年より講師、また2022年からは講師兼プロデューサーとして参画）やSECCONワークショップの講師、国際的なハッカーカンファレンスであるHack In The BoxのAIセキュリティ・コンペティションで審査員を務める等、教育にも力を入れている。

セキュリティ・キャンプ2025ミニ（オンライン開催） 問合せ窓口
一般社団法人セキュリティ・キャンプ協議会事務局 〒102-0093 東京都千代田区平河町2-16-1平河町森タワー 株式会社ラック内
TEL 03-6757-0196 Email info@security-camp.or.jp