■開催概要

日　　程	2024年4月27日(土)13:00(受付開始12:30)～2024年4月28日(日)16:00　2日間
会　　場	東京都立産業技術高等専門学校 品川キャンパス 〒140-0011 東京都品川区東大井1-10-40
参加資格	日本国内に居住する、2025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	講義は4トラックにて実施、各トラックの定員は以下のとおり Aトラック、Bトラック、Cトラック、Dトラック:それぞれ20名
主　　催	東京都立産業技術高等専門学校、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)
後　　援	経済産業省関東経済産業局、東京都、警視庁、国立研究開発法人情報通信研究機構(NICT)、 東京商工会議所、特定非営利活動法人日本ネットワークセキュリティ協会(JNSA)、 一般社団法人ICT-ISAC、一般社団法人高度ITアーキテクト育成協議会(AITAC)、 一般社団法人日本コンピュータセキュリティインシデント対応チーム協議会(NCA)、 特定非営利活動法人デジタル・フォレンジック研究会(IDF)、 中央職業能力開発協会(JAVADA)、国立大学法人電気通信大学、情報セキュリティ大学院大学
特別協力	みずほリサーチ＆テクノロジーズ株式会社、株式会社ラック、株式会社セキュアスカイ・テクノロジー
費　　用	無料。ただし会場までの交通費は自己負担でお願いいたします。
U　R　L	https://www.security-camp.or.jp/minicamp/tokyo2024.html
問合せ先	セキュリティ・ミニキャンプ in 東京 2024　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

■プログラム

共通講義　4月27日(土)　13:00～15:00 (受付開始12:30～)	
12:30	受付開始
13:00	『オープニング』『セキュリティ・キャンプ紹介』 一般社団法人セキュリティ・キャンプ協議会ステアリングコミッティ
13:10	『これからのICT人材に求められる倫理とその先にあるもの』 江渕 悠紀氏　最高検察庁刑事部先端犯罪検察ユニット(JPEC)事務取扱検事 国立研究開発法人情報通信研究機構(NICT)協力研究員 優れた技術は人を幸福にも不幸にもします。 ここでは、ICTの技術を持つ方々に求められる倫理と、その先にあるべき未来について、「法」の考え方や、最近の事例を紹介しながら、皆さんと考えていきます。
14:10	写真撮影、移動休憩、icebreak

■プログラム

選択講義 4月27日(土) 15:00～17:30		
15:00	Aトラック	『利用者視点と開発者視点から理解するウェブサイトの安全性』 佐々木 悠太氏 東京大学教育学部 普段私たちは何気なくウェブを利用しています。そのウェブを利用するにあたり、「怪しいメールのリンクはクリックしないように！」といった注意喚起を見かけることがあります。しかし、本当に怪しいリンクをクリックすると危険なのでしょうか？ 本講義の目的は、以下の通りです。 1.利用者として、ウェブサイトの脆弱性を正しく怖がろう 2.開発者として、ウェブサイトの開発にあたって適切な対策をしよう 1 について、正しく怖がるとは、どのような危険があるか、その危険がどのような条件で発生するかを把握することです。本講義では、怪しいサイトにアクセスした時点で利用者が不利益を被るようなシナリオが想定できることを、具体的な実装をまじえながら説明します。 2 について、1 で説明した危険に対して開発者がとれる防御策を説明し、その際にブラウザやフレームワークレベルの防御機構の重要性を説明します。 最後に、開発者としてデプロイするコードだけでなく、開発プロセス全体に注意しなければいけないことを、サプライチェーン問題の事例とともに説明します。
	Bトラック	『CSIRTを体験してみよう！「インシデントレスポンス演習」』 赤荻 真由美氏 みずほリサーチ＆テクノロジーズ株式会社サイバーセキュリティ統括部 インターネットバンキングの不正送金被害に対し、各種ログの調査（Webサーバ、DBサーバ）や被害者をはじめとする関係者（システム部門・業務オーナー）へのヒアリング結果から、攻撃のタイムライン作成、顧客影響・業務影響の確認、対応策の検討、原因究明、経営報告など、一連のインシデント対応プロセスを体験していただきます。 ※CSIRTの動きを中心にした演習。ログ調査（ハンズオン）は全体の2～3割程度となります。 ※ログ調査はサーバに入って調査するわけではなくフラットファイルで用意したもので行っていただきます。 講義を受講するにあたり下記のマシンが必要です。 -サクラエディタとMS Officeが入っていること
	Cトラック	『Wi-Fiルーターを解析してみよう』 吉越 舟氏 株式会社ラック デジタルペンテスト部 本講義は、IoTペネトレーションテストに焦点を当てたハンズオン形式の授業です。 参加者は市販のIoTデバイスの分解やファームウェアの解析を通じて、デバイスの仕組みとIoTデバイスへのペネトレーションテストの実践的なスキルを身につけることができます。 具体的には、IoTデバイスに存在する既知の脆弱性を探し、これらをどのように見つけ、そしてどのような影響があるかを学びます。 講義を受講するにあたり下記のマシンが必要です。 - PCに有線LANに空きポートがあること（USBLANアダプタでも可） - HDDまたはSSDに40GB程度の空き容量があること
	Dトラック	『セキュアプログラミング入門 – ハンズオンで学ぶ脅威と修正方法』 小野里 亮祐氏 株式会社セキュアスカイ・テクノロジー 研究開発部・EASM事業部開発チーム 坂本 昌彦氏 株式会社セキュアスカイ・テクノロジー 診断事業部・システム開発・運用チーム 典型的なWebアプリケーションの脆弱性が作られてしまう過程やその原因、攻撃により発生する脅威や修正方法を、簡単なアプリケーションのソースコードを読みながらハンズオン形式で学びます。
17:30	1日目終了、解散	

■プログラム

選択講義 4月28日(日) 09:30～16:00 (開場 9:00～)		
09:30	Aトラック	『実際のデータを使用しながら学ぶ異常検知技術入門』 大谷 孟宏氏 株式会社日本総合研究所 異常検知技術は、防犯・防災・製造・医療など様々な分野に使用されています。 情報セキュリティ分野においても、近年多様化しているサイバー攻撃や、攻撃予兆を検知するための重要な技術となっています。 本講義ではまず、ハンズオン形式で身近なデータを使用した異常検知に挑戦し、統計的手法と、人工知能(AI)の一種である機械学習を使った手法を用いて、異常検知手法の基礎を学習します。その後、攻撃の痕跡を含むログデータから、異常検知技術を使用して攻撃の発生日時を推定することに挑戦し、異常検知技術の利点と検討すべき点を、皆さんと一緒に考えていきたいと思います。 講義を受講するにあたり下記のマシンが必要です。 - ご自身のGoogleアカウントを使って、Google Colaboratoryを使用できること （プログラミング言語のPythonを用いますが、未経験でも大丈夫です） - ローカル環境でPythonを実行できること(環境構築等の詳細は参加決定後にご連絡します)
	Bトラック	前日から引き続き『CSIRTを体験してみよう！「インシデントレスポンス演習」』
	Cトラック	前日から引き続き『Wi-Fiルーターを解析してみよう』
	Dトラック	前日から引き続き『セキュアプログラミング入門 – ハンズオンで学ぶ脅威と修正方法』
12:00	昼食休憩	
13:00	Aトラック	『ハンズオン形式で学ぶAIの安全性を高める技術入門』 伊東 道明氏 株式会社ChillStack 代表取締役CEO 現在世界中で生成AIを筆頭に様々なAI技術の利活用が急速に進み、各種業務の自動化や効率化による人手不足の解消などが期待されています。 AI技術は様々な利活用ケースが検討されていますが、偶発的または意図的に誤った推論を引き起こすリスクなど、様々なリスクが内在しています。 本講義では、AIに内在するリスクについて、Pythonを用いたハンズオンを通じて体系的に学びます。 講義を受講するにあたり下記のマシンが必要です。 - Google chromeもしくはFirefoxブラウザが立ち上がること
	Bトラック	午前から引き続き『CSIRTを体験してみよう！「インシデントレスポンス演習」』
	Cトラック	午前から引き続き『Wi-Fiルーターを解析してみよう』
	Dトラック	午前から引き続き『セキュアプログラミング入門 – ハンズオンで学ぶ脅威と修正方法』
15:30	『クロージング』アンケート記入等	
16:00	解散	

■参加要項（事前にご確認ください）

参加条件	・日本国内に居住する、2025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 ・2024年4月27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） ・2日間（4/27～28）通して参加が可能なこと ・開催当日において、息苦しさ（呼吸困難）、強いだるさ（倦怠感）、高熱等の強い症状のいずれかがある場合や、下痢の症状、発熱や咳など比較的軽い風邪の症状が数日続いてる場合は、現地での参加を取りやめていただきます。 ・応募者自身がキャンプにて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 - VirtualBox、VMware等、仮想化ソフトウェアの簡単な操作が可能で、前出の環境においてLinuxのコマンド操作が可能なこと - 参加決定後に指定のソフトウェアをインストールし、起動確認できること（詳細は参加決定後にご連絡します） ・応募者は、演習で使用する下記条件のPCを持参できること - HDDまたはSSDに20GB程度の空き容量があること、USB（TypeA）の空きポートがあること、Wi-Fiに接続可能なこと ・【Aトラック】応募者は、下記の条件を満たすこと - ご自身のGoogleアカウントを使って、Google Colaboratoryを当日持参のノートPC上で使用できる状態であること - ローカル環境でPythonを実行できること（環境構築等の詳細は参加決定後にご連絡します） - Google chromeもしくはFirefoxブラウザが立ち上がること ・【Bトラック】応募者は、下記の条件を満たすこと - PCにサクラエディタとMS Officeが入っていること - OSI参照モデルのレイヤ ３４ や Web3 層構造、ゾーニングなどの基礎知識・基本用語を理解していること ・【Cトラック】応募者は、下記の条件を満たすこと - PCに有線LANに空きポートがあること（USBLANアダプタでも可） - HDDまたはSSDに40GB程度の空き容量があること - C言語で書かれたコードを理解できること（ポインタが雰囲気分かる程度で可） ・【Dトラック】応募者は、下記の条件を満たすこと - TypeScript/JavaScriptで書かれたソースコードの読み書きに挑戦できること ・今回の「セキュリティ・ミニキャンプ in 東京 2024 専門講座」では、講義の録画、配信が行われる可能性があることをご承知いただけること ・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・ミニキャンプ in 東京 2024 専門講座」実施規定を遵守できること
申込方法	セキュリティ・キャンプ協議会のホームページよりお申し込みください。 https://www.security-camp.or.jp/minicamp/tokyo2024.html ※選考問題があります。　※全トラックに併願できます。申込ページにて希望順位を登録ください。 ※申込内容に不備があった場合は、事務局より確認のご連絡をする場合がございます。 ※申込された方には、申込受領のメールが自動送信されます。メールが届かない場合は事務局までご連絡ください。
申込締切	3月25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、申込みされた方全員に3月29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、関東地方の方を優先に選考します。 ・会場までの往復の交通機関や宿泊施設は必要に応じてご自身で手配（費用自己負担）してください。 ・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）、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。 ・ミニキャンプ期間中には、マスコミ各社による取材活動が行われることがあります。また、取材された結果が氏名・学校・顔写真を含んだ受講時の様子を含め各メディアに掲載されることがありますので、ミニキャンプに申し込みされる方はその旨事前にご了解ください。 ・講義を主催者側が撮影・記録させていただく場合がございます。撮影した講義の動画等は、後日配信される可能性があることをご了承ください。 ・ミニキャンプの講義の様子は、キャンプ事業の広報活動や技術啓発を目的として撮影、録音し、その内容を公開する場合があります。 ・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。 ・本事業の成果をはかることを目的として、ミニキャンプ参加後、参加者については参加者アンケートの提出を含めて、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（参加者は回答必須）させていただきます。参加を希望される方はその旨事前にご了解ください。 ・「セキュリティ・ミニキャンプ in 東京 2024 専門講座」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

江渕　悠紀（えぶち　ゆうき）

平成19年（2007年）に検事任官後、東京、京都、大阪、沖縄（石垣島）などで勤務。
令和4年（2022年）から国立研究開発法人情報通信研究機構（NICT）に派遣、令和5年（2023年）から同機構の協力研究員に就任。
同年から最高検察庁に勤務し、先端犯罪検察ユニット（JPEC）に所属するとともに、東京大学大学院の実務家教員（非常勤）としても勤務。
使用できるプログラミング言語はPerl、Pythonなど。

佐々木　悠太（ささき　ゆうた）

セキュリティ・キャンプ全国大会 2022 オンライン B トラック（Web セキュリティ）修了生。
アルバイトでウェブ開発に携わっている。

大谷　孟宏（おおたに　たかひろ）

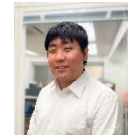
2024年3月に電気通信大学大学院を修了。同年4月、日本総合研究所に入社。UEC Bug Bounty 2019参加をきっかけに、情報セキュリティ分野に興味をもつ。大学では、異常検知技術を用いたIoTネットワーク向けの自律侵入検知について研究。Global Cybersecurity Camp（GCC）2023修了、セキュリティ・ネクストキャンプ2023修了。基板設計からネットワーク、クラウドまで何でも挑戦する。

伊東　道明（いとう　みちあき）

AI×セキュリティに関する分野を専門に活動。セキュリティキャンプ全国大会2015修了/セキュリティキャンプ全国大会 2019～ 講師。IEEE CSPA2018 Best Paper Award, セキュリティキャンプアワード2018最優秀賞を受賞。クリエイター奨学金クマ財団2期生。SECCON2017NOC、ICTSC運営。AIセキュリティに特化した株式会社ChillStackを創業し、不正検知ソリューションを開発提供している。

赤荻 真由美（あかおぎ　まゆみ）

みずほ銀行の個人向けインターネットバンキングのシステム開発の中で不正送金対策をはじめとするセキュリティ対策に従事。2014年からみずほフィナンシャルグループのサイバーセキュリティ専担部署を兼務、2018年からみずほリサーチ＆テクノロジーズ（株）のサイバーセキュリティ専担部署の部長となる。



吉越　舟（よしこし　しゅう）

2019年にネットエージェント入社後、IoTのペネトレーションテストに従事。
1年後ラックに転籍後も継続。
・CTF「ICS Cyber Hacking Challenge 2019」優勝
・CVE-2023-37563、CVE-2020-5635
　→脆弱性2件申請中

小野里　亮祐（おのざと　りょうすけ）

学生時代より株式会社セキュアスカイ・テクノロジーで約4年間のアルバイトの後、2021年に入社。研究開発部に所属しEASMサービス「Dredger」を始めとした自社サービスの開発、学生向けイベントの運営などに携わる。

坂本　昌彦（さかもと　まさひこ）

システム開発会社にてSE/PGとして働いた後、2011年5月にSSTに入社。Webアプリケーション脆弱性診断に従事した後、自社開発の脆弱性スキャナーの開発・運用を担当。