■開催概要

日　　程	2026年4月25日(土)13:00(受付開始12:30)～2025年4月26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、2027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2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：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	申請中
特別協力	株式会社ブロードバンドセキュリティ
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/tokyo2026.html
問合せ先	セキュリティ・キャンプ2026ミニ(東京開催)　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

■プログラム

共通講義　4月25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	『倫理講義』 詳細未定	
14:10	宣誓書記入	
14:20	写真撮影、移動休憩	
14:50	icebreak	
15:00	Aトラック	『Infostealerの手法と対策を学ぼう』 渡邉 雄大氏　九州大学 近年、企業や個人の認証情報を狙うサイバー攻撃において、「Infostealer(情報窃取型マルウェア)」の脅威が高まっています。Infostealerはシステムの破壊などを目的とせず、ブラウザに保存されたパスワードやセッションCookie、暗号資産ウォレットのデータなどを盗み出し、外部の攻撃者へ送信することに特化しています。特に近年は、盗み出されたセッションCookieを悪用することで多要素認証(MFA)を突破されてしまうケースが多発しており、現代のセキュリティ運用において極めて深刻な課題となっています。 本講義では、Infostealerが実際にどのようにして情報を収集し、外部へ持ち出すのか、その内部構造と動作原理を解き明かします。具体的には、以下のような技術要素について学んでいきます。 初期侵入と検知回避: 偽のソフトウェアインストーラーやシェルコマンドなどを経由して端末に侵入し、セキュリティ製品による解析を逃れる手法。 情報の探索と窃取: ブラウザが認証情報を保存しているローカルデータベースへのアクセスや、OSのAPIを悪用して認証情報や機密ファイルを抽出・復号するメカニズム。 データの持ち出し: 窃取したデータを攻撃者のサーバー(C2サーバー)や、クラウドストレージ、一般的なHTTPS通信などを隠れ蓑にして外部へ送信する手法。 この講義の目標は、攻撃者がどのように情報を盗むのかを理解し、対策を考え、正しく対処できるようになることです。模擬的なInfostealerを動作させるハンズオンも計画しています。ぜひこの講義を通して、高度化する脅威に立ち向かうための実践的な知見を身につけましょう！
	Bトラック	『AIエージェント時代のサイバー防衛入門 -攻撃を「守り」に変換する実践ワークショップ』 齊藤 義人氏　株式会社ブロードバンドセキュリティ Webアプリケーションの脆弱性を題材に、攻撃の再現からログ分析、検知ルール作成、是正確認までを一貫して体験します。複数のツールを連鎖実行する「パイプライン」を構築し、AIエージェント時代に求められる「自動化された防御」の考え方を学びます。「攻撃を見つけて終わり」ではなく、防御者として「守れる仕組み」を作る力を養います。 講義を受講するにあたり下記の参加条件があります。 - 16GB以上のRAMを搭載していること - Docker Desktop(Windows/macOS)またはDocker Engine(Linux)がインストールされ、docker composeコマンドが実行可能なこと - ターミナル(コマンドプロンプト/PowerShell/Terminal)で基本的なコマンド操作ができること
17:30	1日目終了、解散	

■プログラム

選択講義 4月26日(日) 09:30～16:00 (開場 9:00～)		
9:30	Aトラック	『DNS通信を用いた情報の持ち出しと対策を考えてみよう』 近藤 匠氏 株式会社オプテージ 近年ランサムウェアによる脅威が増加しており、連日ランサムウェアの感染し情報漏洩が発生といったニュースが報道されています。昨今のランサムウェアは二重脅迫型と呼ばれる暗号化と窃取の二段構成となっており、大事な情報が使えなくなるだけなく、情報漏洩までも発生するようになってきています。 大抵の企業のネットワークでは不要な通信ができないように制限されていることが多い中で、なぜこのような情報漏洩が起きるのでしょうか？ 今回はいくつかある通信手段のうちDNS(Domain Name System)通信にフォーカスを当てどのように通信が成立するのか、また対策としてどのようなことをすべきか考えてみましょう。 講義を受講するにあたり下記のマシンが必要です。 - 仮想環境を2個動かすのでメモリは16GB推奨 - 配布の仮想環境はx86_64環境のため、アーキテクチャが異なる場合は別途手段を用意すること
	Bトラック	『DNSサーバを書いて学ぶ:可観測性とデータ持ち出し対策』 砂川 真範氏 株式会社ブロードバンドセキュリティ 受講者には事前に、Rustで実装したDNSコンテンツサーバ(権威DNS)のサンプルコード (※一部を意図的に欠落)と、開発・検証用VMを配布します。 演習環境は閉域ネットワークで完結し、外部インターネットへの接続は行いません。 前半はDNSの基礎(権威DNS/リゾルバ、問い合わせと応答、QNAME/TYPE/RCODE、ログから分かること)と、DNSが悪用され得る背景(データ持ち出しの入口になり得る、ただし本講義では攻撃手順の再現は目的としない)をレクチャします。 後半はハンズオンとして、配布コードを用いて 1) 単純なDNSコンテンツサーバの完成(最小限のレコード応答) 2) 可観測性向上のためのDNSクエリ構造化ログ実装(時刻・送信元・問い合わせ名・種別・応答コード・応答サイズ等) を行います。 最後に、講師側が用意した「通常通信ログ」と「持ち出しが疑われる通信ログ(例)」を比較分析し、検知観点(何が怪しいか)と抑止策(どう制限するか)、さらに運用(誤検知、例外、ログ取り扱い)まで含めた対策案を検討・共有します。 講義を受講するにあたり下記の条件があります。 - 開発環境用および検証用VMの2つを動かすため、メモリ16GB以上を推奨します。 - Rust言語に関するプログラミング経験があると望ましい。
12:00	昼食休憩	
13:00	Aトラック	『OAuth 2.0 / OpenID Connectのセキュリティ・ベストプラクティスと実践的防御対策』 倉林 雅氏 OpenIDファウンデーション・ジャパン 現代のWebサービスにおいてWeb APIを提供するためのOAuth 2.0やソーシャルログインを実現するOpenID Connectは欠かせない認証・認可技術です。それらの技術を十分に理解せずに実装すると、アカウント乗っ取りや個人情報漏洩を招く重大な脆弱性を生む危険があります。 本講義では、OAuth 2.0 / OpenID Connectの使い方の習得に留まらず、セキュリティ・ベストプラクティスを深く理解し、攻撃者がどこを狙い、エンジニアはどう守るべきかの「本質」を学びます。 本講義は座学による「理論の習得」とハンズオンによる「実践的な対策」の2部構成となります。 座学ではOAuth 2.0 / OpenID Connectの基礎概念と標準仕様で定義されているセキュリティ指針を解説します。 ハンズオンでは、認証・認可サーバーとアプリケーションを構築し、脆弱な実装に対して修正コードを適用しながら対策を学びます。 講義を通じて、Webサービスにおける認証・認可技術の正しい使い方、実装方法を参加者のみなさんと一緒に考えていきます。
	Bトラック	前日から引き続き 『AIエージェント時代のサイバー防衛入門 -攻撃を「守り」に変換する実践ワークショップ』
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、2027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 ・2026年4月25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（4/25～26）通して全ての講義に参加が可能なこと ・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HDDの空き容量を満たすパソコンを持参し、開催期間中に使用できること - Wi-Fiに接続可能なこと - USB（TypeA）の空きポートがあること ・【Aトラック】応募者は、下記の条件を満たすこと - SSDまたはHDDに50GB程度の空き容量があること - 仮想環境を2個動かすのでメモリは16GB推奨 - 配布の仮想環境はx86_64環境のため、アーキテクチャが異なる場合は別途手段を用意すること ・【Bトラック】応募者は、下記の条件を満たすこと - SSDまたはHDDに20GB程度の空き容量があること - 開発環境用および検証用VMの2つを動かすため、メモリ16GB以上を推奨します - Docker Desktop（Windows/macOS）またはDocker Engine（Linux）がインストールされ、docker composeコマンドが実行可能なこと - ターミナル（コマンドプロンプト/PowerShell/Terminal）で基本的なコマンド操作ができること - Rust言語に関するプログラミング経験があると望ましい ・今回の「セキュリティ・キャンプ2026ミニ（東京開催）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・キャンプ2026ミニ（東京開催）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/tokyo2026.html ※応募課題があります。　※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23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27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・キャンプ2026ミニ（東京開催）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

【 Aトラック 】

渡邉 雄大（わたなべ ゆうき）

九州大学工学部電気情報工学科在学中
セキュリティ・キャンプ2024 全国大会 修了
セキュリティ・ミニキャンプ in 北海道 2024 チューター
Sec Hack365 2024 学習駆動コース 優秀修了
GCC 2025 Taiwan 修了
セキュリティ・キャンプ2025 ネクスト 修了
ロボットや低レイヤ分野を趣味に、普段はマイコンや3Dプリンター、PCを触って遊んでいます。

近藤 匠（こんどう たくみ）

株式会社オプテージ セキュリティ技術部 所属。グループ企業ネットワークのセキュリティや社内セキュリティのインシデント対応や脆弱性情報管理などに従事。
普段はおうち仮想基盤（古いミニPCで作ったクラスタ）をいじったり、ちょっとしたコードを書いたりして遊んでいます。
セキュキャン歴
セキュリティ・キャンプ全国大会2020 オンライン 修了
セキュリティ・キャンプ全国大会2021 オンライン チューター
セキュリティ・キャンプ全国大会2025 チューター
その他いくつかのミニキャンプにチューターで参加など

倉林 雅（くらはやし まさる）

一般社団法人OpenIDファウンデーション・ジャパン 理事・エバンジェリスト。
OpenID、OAuth、パスキー（Passkeys）などの認証・認可技術の普及啓発および教育活動に従事。
国内大手インターネット企業において長年、大規模な認証・認可基盤の開発・運用を経験。現在はプロダクトマネージャーとして、安全で利便性の高いデジタルアイデンティティ基盤の構築を牽引している。
主な著書として「パスキーのすべて 導入・UX設計・実装」、監修書籍として「OpenID Connect入門」がある。

【 Bトラック 】

齊藤 義人（さいとう よしと）

2012年よりサイバーセキュリティ専業会社にて脆弱性診断・ペネトレーションテストに従事。現在は同社取締役兼セキュリティサービス本部長。秋田大学、秋田県立大学、山梨大学にてサイバーセキュリティの講師を務める。Hack Fes 2024/2025 登壇。
専門：脆弱性診断、ペネトレーションテスト、インシデント対応
資格：CISSP、情報処理安全確保支援士など

砂川 真範（すながわ まさのり）

BBSecに入社以来、脆弱性診断業務に加え、セキュリティ施策・サービス企画にも従事。ネットワーク／DNSなど基盤領域の理解を土台に、ログ設計・監視・インシデント対応といった「運用で効くセキュリティ」に関心を持つ。個人でも検証用ラボやサイバーレンジ環境を構築し、現象の再現と原因切り分けを通じて、守る側の観点から対策を深めている。今回の講義では、RustでミニDNSコンテンツサーバを完成させ、構造化ログによる可観測性と、データ持ち出しを想定した検知・抑止・運用設計までを体験できる形で紹介する。