セキュリティ・ミニキャンプ in 東京 2023 専門講座

2023年5/13(土)~5/14(日)

会場:東京都立産業技術高等専門学校 品川キャンパス

応募締切:2023年4月10日(月)16時00分

■開催概要

日　　程	2023年5月13日(土)10:30(受付開始10:00)～2023年5月14日(日)17:00　2日間
開催方式	【オフライン開催：Aトラック、Bトラック、Cトラック】 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 【オンライン開催：Dトラック】
参加資格	日本国内に居住する、2024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	キヤノンITソリューションズ株式会社
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/tokyo2023.html

■プログラム

共通講義　5月13日　土曜日　10:30～12:00(受付開始10:00～)	
10:00	受付開始
10:30	『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
11:00	『情報通信技術と倫理』 小林 隆一氏　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 誰もが情報通信技術と無関係では生きられない現代社会において、技術と知識を持っている者はどのようにその力を活かしていくことができるでしょうか。 秩序を維持するための「法」の考え方を紹介するとともに、私たちが社会の中で生きるに当たって求められる「倫理」について考えていきます。
12:00	昼食休憩

■プログラム

選択講義　5月13日　土曜日　13:00~16:00		
13:00	Aトラック （オフライン）	『コンテキストを読み解き進めるモダンWebセキュリティ入門』 齋藤 徳秀氏　株式会社Flatt Security プロフェッショナルサービス事業部 モダンWebの世界では、多くのソフトウェアが”そ結合”な状態でお互いに組み合わされサービスというものを構成しています。例えばクライアント・サーバーモデルのような関係では、クライアントがMPA(Multi Page Application)からSPA(Single Page Application)へと、サーバーはモノリスなアプリケーションからコンテナやIDaaS等のクラウドサービスを組み合わせ作られたクラウドネイティブなバックエンドへと移り変わってきています。 本講義では、そのような中でモダンなWebアプリケーションを構成する、“クライアントアプリケーション”・“サーバーアプリケーション”・“クラウドインフラ”の3つの領域において設計上の”コンテキスト(文脈)”に着目しながら、リアルワールドでよく見られる実装や設定のミスを元に講義を行います。 セキュリティを意識したWebアプリケーションの設計/開発やWebセキュリティに興味がある方は是非参加ください。
	Bトラック （オフライン）	『実践デジタル・フォレンジック』 川崎 隆哉氏　東京都立産業技術高等専門学校　客員准教授 近年ではデジタル・フォレンジックという言葉も少しずつ世の中で認知されるようになってきましたが、実際の調査手法に触れることができる機会はまだ少ないのではないでしょうか。 本講義では、デジタル・フォレンジックの概要や実際の調査手法(Windows10のディスクに残された痕跡の解析)について学んだ後、演習として用意されたあるストーリーに関するデータを調査し、被害者のPCで一体何が起きたのかを報告して頂きます。 本トラックは、デジタル・フォレンジックの調査手法にほとんど触れたことが無い方を想定して作成しています。従って、過去に私が各所で実施した講義やハンズオンイベントに参加された方は、他のトラックに参加した方が大きな学びを得ることができると考えており、本トラックは非推奨です。 勿論、学校や個人でデジタル・フォレンジックの勉強をしていて、実際の調査手法を経験してみたいという方は大歓迎です。教える人が違えば、得れる学びも違う可能性はあると考えます。
	Cトラック （オフライン）	『マルウェア解析入門』 池上 雅人氏、 住田 裕輔氏　　キヤノンITソリューションズ株式会社　サイバーセキュリティラボ あらゆるものがインターネットに繋がっている現在、マルウェア(悪意のあるソフトウェアの総称)感染による被害が深刻化しています。 マルウェアによる被害を正しく評価するためには、マルウェアを解析する必要があります。 本トラックでは、マルウェアを実際に動作させて挙動を確認する手法(動的解析)を学習します。マルウェア解析の経験がない方を対象にコンテンツを作成しています。 初日は動的解析のトレーニングを実施し、サンドボックス上でマルウェアの動作を監視する手法やマルウェアを安全に取り扱う手法を解説します。2日目は実際にマルウェア解析を行い、簡易なレポートを作成する演習を実施します。 講義を受講するにあたり下記のマシンが必要です。 - VirtualBoxでWindows 10の実行が可能であること(Intel互換CPU搭載) -　メモリは4GB以上あること(推奨8GB以上)
	Dトラック （オンライン）	『Windowsイベントログ解析とSIGMAによるDetection Engineering入門』 田中 ザック氏　大和セキュリティ WindowsのDFIR(デジタルフォレンジックとインシデント対応)で最も重要なフォレンジックアーティファクトであるWindowsイベントログを解説した後に、CTF形式でAPTグループが実際に行った攻撃がシミュレートされた環境の痕跡を調査していきます。その後、新しいWindows攻撃をどうやって検知できるかSIGMAルール作成について学びます。学ぶ技術はDFIR、SOCアナリスト、脅威ハンティング等に役立ちます。 講義を受講するにあたり、Windows 10+の端末または仮想マシンが必要です。 メモリは4GB以上、HDDの空き容量は2GB以上が必要です。 以下のツールをインストールする必要があります。 【Visual Studio Code】https://code.visualstudio.com/ 【Windows Terminal】https://apps.microsoft.com/store/detail/windows-terminal/9N0DX20HK701 【Timeline Explorer 2.x】https://ericzimmerman.github.io/#!index.md 【jq】https://stedolan.github.io/jq/
16:00	1日目終了、解散	

■プログラム

選択講義　5月14日　日曜日　09:30～17:00(開場:9:00～)		
09:30	Aトラック (オフライン)	『アクセス制御から学ぶゼロトラストネットワーク入門 -認証プロキシ編-』 河合 将隆氏　NRIセキュアテクノロジーズ株式会社 近年では従来の境界型セキュリティモデルの弱点を抑える新たなモデルとして、ゼロトラストネットワークと呼ばれるセキュリティモデルが注目を集めています。このモデルはコンセプトとして「すべての通信が脅威を内包しているものと仮定して信用せず、常に検証によって信用できるものとそうでないものとを区別すること」「ユーザ本人を識別するための認証を必須とし、認証されたユーザからのアクセス要求であったとしても、そのユーザが正しいことをしているかを常に検証すること」を掲げる一方で、“理想的な”ゼロトラストネットワークの実装にはまだまだ多くの障壁があります。 本講座では、ゼロトラストネットワークの実装方式の一つである認証プロキシによる動的なアクセス制御を通して「ユーザが正しいことをしているかどうかを常に検証すること」の難しさを体験するとともに、実社会での実装例について学びます。
	Bトラック (オフライン)	前日から引き続き『実践デジタル・フォレンジック』
	Cトラック (オフライン)	前日から引き続き『マルウェア解析入門』
	Dトラック (オンライン)	前日から引き続き『WindowsイベントログSIGMAによるDetection Engineering入門』
12:30	昼食休憩	
13:30	Aトラック (オフライン)	『シミュレーションを用いたサイドチャネル解析の体験』 土井 康平氏　電気通信大学大学院 暗号アルゴリズムをハードウェアやソフトウェアで実装したとき、実装されている回路内の消費電力や処理時間、漏えい電磁波などは入力データや処理中の演算によって変化します。このような物理情報が漏えいする経路をサイドチャネルと呼び、サイドチャネルを用いて暗号アルゴリズムを解析する手法をサイドチャネル解析といいます。今回は、シミュレーションを用いてサイドチャネル解析を体験するとともに、その対策方法について触れます。
	Bトラック (オフライン)	午前から引き続き『実践デジタル・フォレンジック』
	Cトラック (オフライン)	午前から引き続き『マルウェア解析入門』
	Dトラック (オンライン)	午前から引き続き『WindowsイベントログSIGMAによるDetection Engineering入門』
16:30	休憩	
16:40	『クロージング』 アンケート記入等	
17:00	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、2024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 ・2023年5月13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（5/13～14）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） ・Aトラック、Bトラック、Cトラック（オフライン）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 - USB（TypeA）の空きポートがあること、Wi-Fiに接続可能なこと ・Dトラック（オンライン）応募者は、下記の条件を満たすこと - 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 ・今回の「セキュリティ・ミニキャンプ in 東京 2023 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 2023 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/tokyo2023.html ※選考問題があります。 ※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	4月10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4月14日（金）までにメールまたは電話にて連絡します。
留意事項	・トラックによって開催方式が異なります。【オフライン開催】Aトラック、Bトラック、Cトラック 【オンライン開催】Dトラック ・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、Aトラック、Bトラック、Cトラックについては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 2023 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

小林 隆一（こばやし りゅういち）

平成21年12月検事任官（東京地検）、平成22年4月 大阪地検
平成23年4月 新潟地検、 平成25年4月 さいたま地検
平成26年4月 東京地検、 平成27年4月 弁護士職務経験（アンダーソン・毛利・友常法律事務所）
平成29年4月 横浜地検小田原支部、 平成30年4月 東京地検
同年9月～令和元年8月 一般財団法人日本サイバー犯罪対策センター（JC3）に派遣
令和2年7月 静岡地検沼津支部
令和4年4月より現職

齋藤 徳秀（さいとう のりひで）

株式会社Flatt Securityに勤務し、Webアプリケーションやサービスインフラに対しての脆弱性診断をはじめ、クラウド診断サービスの立ち上げ、自社のクラウド管理・運用に従事。インターネット上ではあざらしの皮を被りながら日々ビールやご飯の写真を投稿しながらセキュリティの情報収集に勤しむ。2018年のセキュリティ・キャンプ全国大会の開発と運用トラック（Bトラック）を修了し、2019・2020両年に全国大会 Bトラックチューターを経験。2021年全国大会ではBトラック講師。

河合 将隆（かわい まさたか）

NRIセキュアテクノロジーズに勤務し、脆弱性診断、ペネトレーションテストなどの業務に従事。最近では脆弱性診断の傍らBAS（Breach and Attack Simulation）ツールに関する新サービスを立ち上げつつ、ペネトレーションテストサービスのさらなる強化に務める。
セキュリティ・キャンプ全国大会修了（2018）。enPiT-Security（SecCap）修了（2021）。IPA ICSCoE中核人材育成プログラム講師（2020, 2021）。APN ALL AWS Certifications Engineers（2022, 2023仮）。GPEN。肩が痛い。

土井 康平（どい こうへい）

電気通信大学大学院在学中。2021年にセキュリティキャンプ参加、同年よりセキュリティを学び始める。その後は運営サポートのためにチューターなどとして参加、現在は大学院在学の傍ら、ハードウェアセキュリティの研究を行う。最近は推しの引退が続いて満身創痍。

川崎 隆哉（かわさき たかや）

2012年にセキュリティベンダーに新卒として入社し、デジタル・フォレンジック技術を用いた不正調査に従事。現在は、ユーザ企業のCSIRTの一員としてインシデントレスポンスやセキュリティ監視業務を行う。デジタル・フォレンジック技術の普及に繋がる各種活動を行なっており、一般社団法人や高等専門学校等においてデジタル・フォレンジックの講義を担当。
・Japan Security Analyst Conference 2020 speaker
-自作ツールを使用したMac Forensicsの調査効率化-
https://jsac.jpcert.or.jp/archive/2020/index.html
・新しい調査手法（未知のアーティファクト）に関する研究
-https://padawan-4n6.hatenablog.com/entry/2018/02/22/131110

池上 雅人（いけがみ まさと）

欧州のアンチウイルスベンダーにてマルウェア解析技術を学び、帰国後はマルウェア解析業務に従事。サイバーセキュリティの調査研究やレポート執筆も行っている。CISSP・GREM・GCIH。

住田 裕輔（すみだ ゆうすけ）

キヤノンITソリューションズにおいて、マルウェアアナリストとして、マルウェアレポート執筆やウェブセミナー登壇などの業務に従事。

田中 ザック（たなか ざっく）

アメリカ生まれアメリカ育ち、中学生の頃からIT、セキュリティ、日本語を独学する。2006年に神戸デジタル・ラボ（KDL）に入社し、セキュリティチームを立ち上げる。ネットワーク・スマホアプリ・ウェブ診断/ペネトレーションテスト、フォレンジック調査、インシデント対応、無線ハッキング、ソーシャルエンジニアリング等々幅広くセキュリティを勉強し、様々なセキュリティサービスを作る。2007年からカーネギーメロン大学日本校で研究し、2012年から大和セキュリティというコミュニティを立ち上げ、2016年からSANSの講師を務める。13種のGIACの資格を保持する。

セキュリティ・ミニキャンプ in 東京 2023 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