IoTハッキング・セキュリティトレーニング

本トレーニングは初級～中級者向けの、IoTデバイスに対するハンズオン中心のセキュリティトレーニングです。

IoTデバイスの調査・テスト実績を有する当社のエンジニアにより、そのノウハウを基に、Wi-Fiルーターを通じてソフトウェア／ハードウェア解析をはじめとした基礎的なIoTハッキング手法を受講者が体験することで、機器の脆弱性について理解を深められるトレーニングを提供します。また、車載ECUを模擬したソフトウェアを通じて基礎的なCANのハッキング手法を体験することで、ECUの脆弱性についても理解できます。

3日間のトレーニングで「組込みデバイスへのハッキング」、「ファームウェアに対するリバースエンジニアリング」、「バイナリエクスプロイト」、「CANプロトコルへのハッキング」など多くのトピックを学べます。

日時　**2025年10月15日(水)～17日(金)**
各日 9:30 ～ 18:00 予定

場所　**株式会社ベリサーブ**
本社セミナールーム

お申し込みはこちら

トレーニングの様子

車載用機器、IoT機器、医療機器に対する脆弱性診断やペネトレーションテストなど、さまざまなセキュリティ事案に精通した当社エンジニアが講師を務めます。

開催概要

日　程	2025年10月15日（水）～ 17日（金）　各日9:30～18:00予定 （申込受付期間は 9月29日（月）の 10:00までとなります。お早めにお申し込みください。）
会　場	〒101-0061　東京都千代田区神田三崎町3-1-16　神保町北東急ビル9階 株式会社ベリサーブ　本社セミナールーム JR中央・総武線、都営地下鉄 三田線【水道橋】駅より徒歩4分 東京メトロ 半蔵門線、都営地下鉄 三田線・新宿線【神保町】駅より徒歩6分 東京メトロ 半蔵門線・東西線、都営地下鉄 新宿線【九段下】駅より徒歩7分
参加費	396,000 円（税込） ・早割（8月 22 日までの申し込み）　330,000 円（税込） ・超早割（8月 8 日までの申し込み）294,800 円（税込）
定　員	15名（最少催行人数：4名）お申し込み受付中
対　象	・IoTデバイスおよびIoTシステムのセキュリティについて学びたいとお考えの方 ・Linuxの基本操作のご経験がある方
主　催	株式会社ベリサーブ
注意事項	●本セミナーは有償です。お申し込み受付後、当社担当よりお支払い方法と受講の流れについてご連絡します。 ●お申し込みは法人の方のみとさせていただきます。 ●イベントの様子を記事として公開するために撮影が入ります。 ●最少催行人数に満たない場合は、中止となる場合がございます。 ●本トレーニングの申し込みページ内に記載している申込規約をご確認いただき、同意の上でお申し込みください。
必要な持ち物	本トレーニングの受講にPCが必要となります。 当日はPCをご持参ください。受講に必要なPCの詳細スペックは裏面に記載しております。 PCをご準備いただくことが難しい方向けに、当社にてレンタルPCのご提供が可能です。（有償） お申し込み時にお知らせください。
詳細・お申し込み	主な講座内容は裏面または本トレーニングのお申し込みページをご覧ください。 URL：https://contact.veriserve.co.jp/public/seminar/view/12755

コース概要・プログラム

Day 1

IoTセキュリティアーキテクチャの内部概念、既知のIoTデバイスの脆弱性およびケーススタディに慣れ親しんでいただくところから始まります。

そして、IoTデバイスのファームウェアを取得してリバースエンジニアリングしていただき、セキュリティ上の問題を発見し、実際に悪用できることを確認します。

Day 2

実際のIoTデバイスを分解して、回路基盤の持つコンポーネントを理解し、その知識をもとにデバイスのルートを取得するところから始まります。

続いて、UARTのエクスプロイト、デバイスからフラッシュチップの内容をダンプするなどのトピックについても学習します。

Day 3

車載アーキテクチャの内部概念およびCANプロトコルを理解いただくところから始まります。

そして、車載を模擬したシミュレーション環境にて、CAN通信の盗聴および再送攻撃したり、車載ECUのセキュリティ機能の一つであるUDSのSecurity Accsess認証への攻撃といった車載ECUへのサイバー攻撃に関する基本的なテクニックを学びます。

主な習得内容

- IoTデバイスへ基礎的な攻撃
- デバイスファームウェアの抽出と分析
- バイナリのデバッグと逆アセンブル
- ファームウェアのダンプ、ハードウェアとソフトウェアのデバッグ
- IoTデバイスの通信機能への攻撃
- 車載ネットワークの基礎知識
- CANバスの盗聴、再送攻撃
- UDSプロトコルを用いた攻撃の一例 その他

受講に必要なPC環境

当日お持ち込みいただくPCには、以下の環境が必要になります。

- OS Windowsのみ（Windows11を推奨）
- メモリ 最低8GB（16GB以上を推奨）・HDD 50GB以上の空き容量
- OSの管理者権限があるユーザでログインできること
- USBメモリの読み込みができること
- USBポートが2つ以上
- ウィルス対策ソフトウェアを管理者権限で停止、解除ができること
- 無線LANアダプタ（会場の無線LANに接続可能なこと）※無線規格：IEEE802.11a/b/g/n/ac
- VMwareもしくはVirtualBoxをインストール可能であること
  ※VMwareもしくはVirtualBoxが、快適に動作可能な環境が必要であること

お申し込み受付中！お気軽にお問い合わせください。

加速しよう、未来を。
VERISERVE
https://www.veriserve.co.jp

東京都千代田区神田三崎町 3-1-16 神保町北東急ビル 9階

お問い合わせ先
sol_event@veriserve.co.jp

お申し込みはこちら