

コースコード：VER-IOTHACK

税込価格：825,000円 (税抜価格：750,000円)

日数：3日間

## 前提条件

- ・一般的なOS、コンピュータ・アーキテクチャ、ネットワーキングに関わる基本的な知識
- ・IoTに関する基本的な知識 本トレーニングの受講にPCが必要となります。ご受講にはPCをご用意いたしますが、もし、PCを持参される場合には、以下の受講に必要なPC環境をご参照ください。  
<b>受講に必要なPC環境・Intel 2GHz以上・メモリ 最低4GB (8GB以上を推奨)・OS Windows 7以降 64bit・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メモリの読込ができること・USBポートが2つ以上
- ・ウイ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。

## 受講対象者

IoTデバイス・IoTシステムのセキュリティについて学びたい方

## コース概要

2024.9.11-13の開催では、講師にAttify社のAditya Gupta氏をお迎えします。Attify社ではこれまで100を超える多くのIoTデバイスを調査、テストしてきました。本トレーニングでは、そのノウハウをもとに、IoTデバイスに対するハッキング方法を紹介し、「スマートデバイス」のセキュリティを破る、攻撃的なアプローチをご紹介します。

3日間のトレーニングでは、組み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、無線規格 (BLE: Bluetooth Low Energy) を用いたエクスプロイトなど、その他多くのトピックについて学んでいただきます。

トレーニングにご参加いただいた方は、トレーニング中に使用する \$ 1,000相当のハッキングキットをお持ち帰りいただけます。

## 目的

- ・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
- ・UART、SPI、JTAGの悪用、JTAGのデバッグとそれを用いたエクスプロイト
- ・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デバイスのクラウドやモバイル機能への攻撃
- ・スニффイング、リプレイ、MITM、無線通信による攻撃、BLEによるエクスプロイト
- ・ARMとMIPSのリバースエンジニアリング、従来型攻撃と非従来型攻撃の手法
- ・プラットフォームへの攻撃、など

## アウトライン

以下の実践を通して、ARMやMIPSアーキテクチャのエクスプロイト、ファームウェアの抽出とデバッグ、ファームウェアのエミュレーションなどの概念を学びます。

1日目



- ・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
- ・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
- ・セキュリティ上の問題を発見し、実際に悪用される可能性の認識

## 2日目

- ・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、デバイスのルートを取得
- ・UARTの 익스프로イト
- ・JTAGのデバッグ

- ・デバイスからフラッシュチップの内容をダンプする

利用するツールや配布資料と共にこれらのノウハウを学習し、さまざまなIoTデバイスにも適用することができます。

## 3日目

デバイスをリモートから攻撃するために必要なノウハウを学びます。

- ・BLEを使用したデバイスを盗聴して攻撃
- ・攻撃に利用するカスタムラジオを作成
- ・ツールと演習を組み合わせることで、実際に攻撃者がIoTデバイスに侵入するために必要なことを学習します。

### < b > 主な習得内容 < /b >

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  
UART、SPI、JTAGの悪用、JTAGのデバッグと、それをういた 익스프로イト  
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デバイスのクラウドやモバイル機能への攻撃  
スニффィング、リプレイ、MITM、無線通信による攻撃、BLEによる 익스프로イト  
ARMとMIPSのリバースエンジニアリング、従来型攻撃と非従来型攻撃の手法  
プラットフォームへの攻撃 その他

### 注意事項：お申し込みの注意点

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。

本セミナーで利用する教材は英語です。

講師も英語でセミナーを進めますが、英語から日本語の逐次通訳が入ります。

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。

本受講には申込規約がございます。下記をご確認いただき、同意の上でお申し込みください。

[https://www.veriserve.co.jp/download/pdf/iot\\_hacking\\_st2024.pdf](https://www.veriserve.co.jp/download/pdf/iot_hacking_st2024.pdf)