募集要項別紙

平成29年度　沖縄型産業中核人材育成事業

テーマ名：
「IoT機器のセキュリティ評価・検証プロセスを修得する上級エンジニアの育成プログラム」
～講習プログラムの内容について～

一般社団法人
重要生活機器連携セキュリティ協議会

講習プログラムの受講対象・特徴

●本研修プログラムの特徴・得られる知識

IoT機器におけるセキュリティを中心とした検証技法を習得できるプログラム設計
①国際標準に准じて策定された「CCDS IoTセキュリティ評価検証ガイドライン」に沿って、具体的な演習を行うことで、メーカーの求めるIoT機器検証プロセス全般の習得を目指す
②ネットワークセキュリティ分野では一般的となっているアタックツールを用いて、IoT機器の脆弱性評価方法の習得が可能
（テスト要件の策定、評価ツール実行と解析手順、結果の報告方法など）
③座学と演習を１セットとした実践的な研修方式
④イーラーニングによる受講後のオンライン復習が可能

●受講していただきたい方

①IoT機器のセキュリティ評価・検証スキルを習得したい評価検証エンジニアの方
②IoT機器に潜在する脆弱性の見極め方や具体的な対策立案の知識を習得したい開発エンジニアの方
③新規ビジネスとして、セキュリティ評価・検証業務へ事業拡大していきたい技術リーダー・マネージメントを担当されている方

講習プログラム概要

講義ポイント：CCDS「IoTセキュリティ評価検証ガイドライン」をベースに、セキュリティ評価検証手法の習得を目指す

１）実際の機器を対象に、脆弱性検証（アタック）を実施
２）基本的な脆弱性ツール（OSS）の内容と操作を習得
（スキャン、アタックツールの利用）
３）既知の脆弱性を有する機器（WiFiモデムルータ）を対象に
管理者権限として侵入するところまでの演習を実施
４）OWASP、OTAのフレームワークを活用したセキュリティ
対策の立案、検証要件の策定プロセスを習得する
５）リスク評価手法（CVSSv3）の理解と実際の評価業務への
応用方法

※講習プログラムの内容については、受講希望企業の要望を踏まえ、修正を行うため、変更の可能性がある。

１日目の講習プログラム（Aパート）

研修テーマ		種別	時間	担当
「導入～研修開始にあたって」 ①講師自己紹介 ②研修の全体スケジュールと各研修の目標 －作成する検証成果物と実習のGoal －CCDSガイドラインとの関係性 ③IoT機器で発生している脆弱性の事例とは？		講義	90分	CCDS
内容	研修初日として、4日間の研修内容がどのようにCCDSのガイドラインにつながっているいのか、また4日間の研修で何を習得をして欲しいのか、各プログラムで作成する成果物を説明し、Goalイメージを持ってもらう。 IoT機器において発生している脆弱性の事例（Miraiやランサムウェア、台湾製ルータの訴訟問題、Jeepのハッキング事例など）をもとに、セキュリティ課題が社会的な問題となっており、既にビジネスの領域においても金銭的な損失につながっていることを理解してもらう。 同時に具体的な脆弱性について、典型的なパターンをビデオ教材で説明し、どのような現象が発生するのかをイメージしてもらう。			
	休憩		15分	

１日目の講習プログラム（Bパート）

研修テーマ	種別	時間	担当
「セキュリティ検証環境の構築方法を学ぶ」(各グループ)	演習	90分	CCDS
内容	今後の研修に使用する検証環境の構築を実習形式で行う。 研修終了後も各自が実践できるように、Linuxの仮想環境構築から、検証ツール(OSS)のインストールまでを体験的に学習する。 ■環境構築の実習手順 ①受講者PCのOSにHyper-Vを設定 ②Hyper-Vを利用し、Linux(Ubuntu)の仮想環境を構築 ③仮想環境に各検証ツールのインストールを実施 －NMAP －Hydra(crunch) －LOIC ④インストール後の動作チェックを実施 ⑤研修利用環境への切替を行う。		
効果測定	①実習内容を完遂できたかどうか（講師が各受講者を確認） ②効果測定テスト：1日目の講義と実習内容から10問程度のテストを実施		

２日目の講習プログラム（Aパート）

研修テーマ	種別	時間	担当
「セキュリティ評価検証のツールを学ぶ」 ①講師自己紹介（マストトップ　松本氏） ②セキュリティ検証に活用するツールの種類と目的 ③ツールの選定と接続に必要な実施手順 －インターフェイス・プロトコル調査 －入出力の解析（ポートスキャン等） ④実習用ツールのオペレーションと結果の解析手順 －NMAP、OpenVAS、Aircrack_NG＋hydraを個別に説明	講義	45分	マストトップ
内容	IoT機器のセキュリティ評価検証に活用可能なツールの種類や、目的を体系的に理解し、目的に合ったツールの選定方法を学ぶ。また、実際にツールを利用するにあたり、接続に必要な事前調査の手順や、オペレーション方法、出力結果の解析方法を、今後実習で使用する４種のツールを例に学んでいく。		
「セキュリティ検証ツールのオペレーション実習①～環境構築」(グループワーク)	演習	45分	マストトップ
内容	NMAP（ポートスキャンツール）、OpenVAS（脆弱性スキャンツール）、Aircrack_ng（WiFiパスワード解析ツール）＋hydraの４種を使用し、ツールと検証対象（DUT）との接続に必要に手順から、オペレーションの方法、出力された検証結果の解析方法までを、ハンズオン形式の実習にて習得する。		
	休憩	15分	

２日目の講習プログラム（Bパート）

研修テーマ		種別	時間	担当
「セキュリティ検証ツールのオペレーション実習② ～オペレーション・結果解析」(グループワーク)		演習	45分	マストトップ
内容	脆弱性サーバとしてMetasploitable2(予め脆弱性が組み込まれているサーバ環境)を使用することで、実際に脆弱性が検出された場合に、どのように結果が出力され、どのように解析すれば良いのかを体験的に学習することができる。			
実習結果の確認・フィードバック		演習	45分	マストトップ
内容	各グループで実施したハンズオンの結果を確認し、実習内容についての質疑応答を行う。不明点があれば、補足説明も含め、フィードバックを行う。			
効果測定	①各グループで実習を完遂できたかどうか（講師が各受講者を確認） ②効果測定テスト：2日目の講義と実習内容から10問程度のテストを実施			

３日目の講習プログラム（Aパート）

研修テーマ	種別	時間	担当
「セキュリティ評価検証仕様の策定プロセス」 ①策定プロセス全体の流れ ②評価検証計画書の策定手順 ③システム構成図を用いたリスク想定 ④リスク対策のためのフレームワークを学ぶ ⑤仮説の検証～検証ツールや検証手法を選定する	講義	45分	CCDS
内容	IoT機器のセキュリティ検証の仕様を具体的にどのように策定すべきかをガイドラインの記載プロセスに沿って学んでいく。まず最初にIoT機器のシステム構成図をもとにしたリスクを想定し、想定リスクに対して、情報セキュリティのフレームワーク（OTA、OWASP）を活用し、必要な対策を示していく。さらに対策が妥当かどうかを検証するための手法や対策を、「検証ツール一覧」から選定することで、一連のプロセスを学ぶことができる。		
「セキュリティ評価検証仕様書の作成実習」(各受講者)	演習	45分	CCDS
内容	講義内容をもとに、実際に下記のステップに沿って、WiFiモデムルータを対象に一連のプロセスを実習形式でトレースすることで、知識を実践的に使えるものにする。 ①システム構成図によるリスク分析シート　⇒リスクを分析する ②想定リスクと必要な対策の記載シート　⇒リスク対策を立てる ③検証ツール・検証手法の選定シート　⇒対策の妥当性を検証する		
効果測定	・受講生から提出された成果物（上記①～③）をもとに、講習内容の理解度、達成度を確認する。		

３日目の講習プログラム（Bパート）

研修テーマ	種別	時間	担当
「セキュリティインシデントレポートの作成方法を学ぶ」 ①レポート発行までのフロー ②品質評価に使用するレポートとの違い ③各記載項目についての説明 ④レポート記載にあたっての注意事項 **「リスク評価手法を学ぶ」** ①セキュリティインシデントの深刻度判定について ②CVSSv3の目的、特徴	講義	45分	CCDS
内容	検証の実施により検出されたインシデントについては、報告レポートを起票し、開発元と情報を共有する必要がある。研修では、ESBRというIPAの記載ガイドラインをもとにCCDSがセキュリティ用に改版された基準に基づき、レポート報告の正しい記載方法や、報告フロー、実際の業務において想定される注意事項等を学ぶ。セキュリティインシデントの深刻度を判定するためのリスク評価手法について、CVSSv3をメインテーマとして学ぶ。各リスクファクターの意味や関係性、計算式と共に、CVSSでは加味されない要素（ファイナンス、健康、生命等）についても理解する。		
「セキュリティインシデントレポートの作成実習」(各受講者)	演習	45分	CCDS
内容	講義で説明した内容に沿って、実際にインシデントレポートの作成を行う。作成はCCDSが開発した「組込み機器評価検証基盤システム」に実装されている作成機能を使用する。3日目の研修で見つかった脆弱性をテーマに作成することで、受講者にここまでの流れが分かりやすい形式とする。作成したインシデントレポートに対して、実際にCVSSによるリスク評価を実施する。		
効果測定	・作成されたインシデントレポートの内容をもとに、講習内容の理解度、達成度を確認する。		

４日目の講習プログラム（Aパート）

研修テーマ	種別	時間	担当
「IoT機器を用いた実務想定の検証演習」（説明） ①実習の進め方について －検証手順の検討 A)仕様策定 B)検証実施 C)報告レポート作成 ②IoT機器と検証ツールの接続環境について ③検証結果の記載方法とグループ発表について	講義	45分	マストトップ
内容	最終日はこれまで学んできたセキュリティ検証プロセスの総括として、実際にIoT機器（WiFiモデルルーター）を使用し、実務想定の検証実習を行う。実習を始めるにあたり、進め方や環境の説明、結果の記載方法等の説明を行う		
「IoT機器を用いた実務想定の検証演習」（実習前半）(グループワーク)	演習	45分	マストトップ
内容	4名×3グループに分かれて、これまでに習得したツールと実際のIoT機器を使用し、実際にセキュリティ検証を実施する。これまで学んだ内容をもとに、4名でディスカッションをしながら、検証仕様を策定する。検証を実施し、簡易版のインシデントレポート作成（タイトル、CVSSv3によるリスク評価値程度）、結果報告レポートの作成までをCCDS検証基盤を用いて行う。※詳細は次ページに記載		
	休憩		15分	

４日目の講習プログラム（Bパート）

研修テーマ		種別	時間	担当
「IoT機器を用いた実務想定の検証演習」（実習後半）(グループワーク)		演習	45分	マストトップ
内容	■使用IoT機器（予定）WiFi無線ルータ ■実習テーマ：「XSSの脆弱性の検出とエクスプロイト手法を学ぶ」 ■実習のステップ ①NMAP、OpenVAS（OwaspZap）による脆弱性スキャン：XSS脆弱性検出 ②Telnetのポートをオープンするためのエクスプロイトコード実行 －実際に標的型メール攻撃を想定したURLリンクからのXSSを試行 ③ルータの管理機能を使用した権限昇格（リモートアクセス） ④管理権限奪取後のリモートアクセス操作 ⑤XSSによる攻撃の仕組みの補足説明 ⑥レポート作成（インシデントレポート、報告レポート）			
「IoT機器を用いた実務想定の検証演習」（発表）(グループワーク)		演習	45分	マストトップ
内容	作成した報告レポートをもとに、各チームの検証結果を１チーム10分でグループ発表を行う。各チームごとに結果に違いがあれば、講師がフォローを行い、チームに気づきを促す。また、研修の最後に、持ち帰りの課題として、これまでの４日間の研修受講レポートに関する説明を行う。後日提出してもらったレポートの内容を受けて、講師陣より個別にメールにてフィードバックを行う。			
効果測定	①実習結果の報告レポートをもとに、講習内容の理解度、達成度を確認する。 ②これまでの４日間の研修に対する受講レポートから、講習効果を確認する。			