IoT セキュリティ教材ガイド

（Ver.1.0）

2020 年 11 月 18 日

独立行政法人情報処理推進機構
社会基盤センター産業プラットフォーム部

1. 教材の目的

本教材は、IoT 機器・システムの設計・開発・運用に携わるエンジニアの養成を目的として、大学院修士課程における 90 分×15 回の 2 単位の授業で使用することを想定して開発されています。大学学部学生への専門授業としても提供可能ですが、情報工学、情報セキュリティ、組込みシステム、ネットワークなどに関する基礎的な知識を習得していることが要件となります。

2. シラバス

コースの目的、到達目標、授業計画、前提知識、教科書と参考書、必要な演習機材、特記事項をシラバスに記しています。授業を追う毎に知識を積み重ね、一連の座学の後に演習を設けているので、授業の順番は大きく変更するべきではありません。授業時間が不足する場合、前半の車載エレクトロニクス、ハードウェアセキュリティ、後半の機能安全、法制度、認証規格、などの授業項目を他のコースで実施あるいは省略することが考えられます。

特記事項として、輸出貿易管理令の規定に従い、海外の受講生には暗号技術を含む「IoT デバイスのセキュリティ機能演習」を提供できないことに注意してください。

3. 投影用教材の構成

授業は 90 分×15 回で構成され、そのうちの 11 回が座学、4 回が演習です。分量は違いますが、いずれもプロジェクターで投影するパワーポイント（PPT）形式となります。教材の中心は、この投影用のパワーポイント資料です。スライドは、40～90 枚程度あるので、2 分で 1 枚程度の説明を加えることを想定しています。スライド数が多い授業でのいくつかのスライドは、（参考）としていますので、資料の提供だけに留めることも考えられます。授業の途中で、5～7 分程度の小テストおよび前回の小テストの解説をするのであれば、1 回の授業は 80 分程度で終えなければなりません。

PPT 教材の一部には、ノート部分に口頭説明に加えるべき補足等が記されているので適宜参照してください。

4. 小テスト、レポート課題

授業の理解度を計り、成績評価の材料とするために小テストを実施することを想定しています。採点しやすいように選択式、正誤式などだけを採用しています。12 問以上を提供していますが、そのうちの 10 問を選ぶ、全部を与えて 5/6 の点にするなど検討してください。全体に易しい内容となっているので、必要に応じてより高度な問題を加えるなど工夫し

てください。

レポート問題は、欠席して小テストを受けられなかった受講生への出題を目的としています。

5. 演習

5-1 IoT デバイスのセキュリティ機能演習

IoT セキュリティの特徴を一通り学び、IoT デバイスの知識を得た後で行う演習です。特に、可搬な IoT デバイスには、人が記憶するパスワードに代わる信頼の基点としてハードウェアで保護された暗号鍵の秘匿手段が必要であることを学ばせます。

セキュリティ機能として TSIP (Trusted Secure IP) を取り上げ、TSIP が備わった MCU として RX65N[1]を用いた暗号通信を演習として行います。RX65N は、評価ボードとして 5 万円程度で販売されています。本演習は、この評価ボードを用いていますが、本演習で使用しない液晶ディスプレイなどの機能もあることから、より小型・安価の GR-PEACH[2]が使える可能性もあります（ただし未確認)。これらの評価ボードは、Windows-PC 上の IDE (統合開発環境)である、Renesas エレクトロニクス社の CS+を用いてプログラムのダウンロードと実行の制御を行います。CS+ は、Renesas 社の Web サイトから無料でダウンロードが可能です。プログラムの大きさが 128kB を越えると有償版を使用する必要がありますが、本演習で扱うプログラムはそれより小さくなっています。このプログラムは、データテクノロジー株式会社[3]の商用の暗号ライブラリおよびシェルを用いています。データテクノロジー株式会社のご厚意により、この教材に同梱されたソースコードを含むライブラリは、IoT セキュリティ教育目的に限り、無償で使用することができますが、再配布は禁じられています。本教材の頒布を受ける機関は、データテクノロジー株式会社に連絡して、「IPA から頒布を受けた IoT セキュリティ用の暗号通信プログラムを教育用に無料で使用したい」旨を伝え、許可を受けてください。

演習では、RX65N が、Windows-PC 上のサーバーと 3 種類の通信を行います。このサーバー上のプログラムとは、Ethernet で送られてくるパケットをそのまま表示するか、設定された暗号鍵で復号して表示します。暗号化をソフトウェアとハードウェアの 2 種類で行います。これらの暗号処理で用いる暗号鍵が漏洩しないかを検査するのが演習の目的です。

演習は、1 台の RX65N 評価ボードを 2 人の受講生で共用し、もう一つのチームとサーバーを共用し、互いのチームの IoT デバイスになりすますことを試行します。したがっ

[1] https://www.renesas.com/jp/ja/products/software-tools/boards-and-kits/starter-kits/renesas-starter-kitplus-for-rx65n.html
[2] https://www.renesas.com/jp/ja/products/gadget-renesas/boards/gr-rose.html
[3] https://www.datec.co.jp

て、4 人で 1 つのグループとなります。1 チームの人数は、1−4 人程度まで変えることができます。

演習環境の構築法は、補助資料に記していますが、WindowsPC にサーバープログラムを載せること、CS+をインストールすること、評価ボードとダムハブを介して接続すること、受講生用の PC に Wireshark をインストールしてネットワークをダムハブに接続してネットワークトラフィックを観測できるようにすることなどが必要です。これらの準備作業を受講生にやらせることもできますが、授業時間が不足するため、あらかじめ、講師側で準備しておくことをお奨めします。演習には、ネットワークを使用しますが、ローカル IP アドレスを与えた閉じたネットワークであり、インターネットとは接続しません。

5-2 脅威分析演習

セキュリティの脅威分析の手法を座学で学んだ後、スマートホーム環境でのセキュリティの脅威がどこに存在するかを分析する演習を行います。次の 5-3 で使用するスマートホームを対象にします。

システムを図に表すために、Draw-IO というフリーソフトウェアを受講生各自の PC にダウンロードして使用させます。

脅威分析手法の学習の一環として、次に行う 5-3 の実習で使用する、Linux 用の脆弱性検査ツールの使用法を習得します。

5-3 脆弱性検査演習

脆弱性検査演習は、2 週にわたって（2 コマで）実施します。

演習用の機材や演習環境の構築法は、付属資料に記しています。付属資料の納品物一覧を Web ブラウザで開くと、必要な書類へのリンクが表示されます。

演習では、受講生用の PC から、脆弱性検査ツールの入った Linux（RasPi）に接続して使います。受講生用の PC からは、また、演習の課題を与え、採点を行う CTF サーバーにも https 接続します。やはり RasPi でエミュレートされスマートホーム環境内の IoT デバイスの脆弱性を検査します。ネットワークは、スマートホームのローカルネットワーク、CTF サーバーのネットワーク、脆弱性検査ツールの走るネットワーク、脆弱性検査の結果の CVE 番号を調査するためのインターネットと複数必要ですが、CVE データベースは、CTF サーバーにダウンロードしてあるので、インターネットは不要です。脆弱性検査のパケットがインターネットに流れるのは好ましくないので、インターネット接続は不要にしてあります。

脆弱性検査ツールは、Linux で実行されます。Wi-Fi トラフィックの観測に WiFi ドライバの設定が必要であり、Linux でないと難しいからです。したがって、この演習に参加する受講生は、Linux にある程度習熟している必要があります。

CTF 形式の演習ガイドは、オープンソースの CTFd で実装されています。課題の与え方やヒントは、CTFd の設定で変えられます。

本演習は、多数のデバイスとプログラムを組み合わせて使用ますので、ソフトウェアのセキュリティアップデートやデータベースの更新のために、準備作業が必要になります。この演習は、一般社団法人 重要生活機器連携セキュリティ協議会[4]が開発したコンテンツを元にしており、その実装には、株式会社マストトップ[5]が関わっています。本演習用の機材の調達や、演習準備・演習授業の補助を依頼することができます。

6. 著作権規定

本教材の著作権は独立行政法人情報処理推進機構（IPA）に帰属します。ただし他の著作者の著作物を引用している箇所がありますので、著作権法に則った利用が必要です。

IoT デバイスのセキュリティ機能演習に使われているプログラムには、有償プログラムが含まれているので、IPA から直接頒布を受けた機関以外では使用できません。

脆弱性検査演習は、すべてオープンソースのソフトウェア等で構成されていますので、複製等を自由に行えます。ただし、Copyleft ライセンスの OSS ソフトウェアに関して改変等を行った場合、そのソースコードの公開義務が生じます。

[4] https://www.ccds.or.jp/
[5] https://mast-top.com/company