2020 年 11 月 18 日（Ver. 1. 0）
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

IoT セキュリティ教材
演習概要

1.　IoT デバイスのセキュリティ機能演習

(1) 演習のねらい

IoT では、多くの IoT デバイスが、M2M の通信を行う。人間が介在しないため、パスワードやバイオメトリクスなどによる保護策がとれない。

IoT の「信頼の起点」は、暗号鍵が担う。ただし、暗号鍵の秘匿が不十分であると、攻撃者は、手の届く場所に置かれた機器の中を調査し、暗号鍵を入手できてしてしまう。

よって、IoT デバイスは、攻撃者に見えないように暗号鍵を機器内に安全に秘匿する必要がある。暗号鍵の秘匿は、ハードウェアセキュリティ機能を利用することで安全性が高まる。ハードウェアセキュリティ機能は、TPM、TrustZone などに実装されているが、より強力なハードウェアセキュリティ層を形成した TSIP(Trusted Secure IP) がルネサスエレクトロニクス株式会社より提案、実装されている。

演習では、TSIP を使用する場合と使用しない場合で、安全性や性能にどのような差が生じるかを体験する。具体的には、下記 2 点を体験する。

- 通常の方法（TSIP を用いない場合）では、機器から暗号鍵を読み取って機器を偽造することが可能であるが、TSIP のような MCU のセキュリティ機能を活用すれば、暗号鍵を秘匿して、安全な通信と機器の偽造防止が実現できることを体験する。
- ソフトウェアによる暗号化とハードウェア（TSIP）による暗号化の性能差を測定する。

(2) シナリオ

2 人の受講生が 1 チームを構成する。2 チームが互いに相手の通信を傍受したり，なりすますことを試みる。

各チームの IoT デバイスである RX65N が、サーバと通信。その通信を相手チームが盗聴する。MCU のメモリ上で暗号鍵を探索し、相手チームの暗号鍵を窃取する。窃取した暗号鍵を自チームのデバイスにセットし、相手チームのデバイスになりすます。

- 演習①IoT デバイスの、UDP による平文通信
  相手チームの通信を盗み見ることができるか？
- 演習②ソフトウェアによる暗号化 UDP 通信
  相手チームの通信を盗み見ることができるか？
  MCU のメモリ上で暗号鍵を探索、窃取し、相手チームの暗号鍵を使ってなりすますことができるか？
- 演習③TSIP による暗号化 UDP 通信

演習②と同様のことができるか？

- 演習④暗号化の速度性能
  ソフトウェアによる暗号化とハードウェア（TSIP）による暗号化の性能差を測定する。

(3) 演習機器

① 演習には、下記の機器を用いる。機器類は利用者が用意・設定する。

- チームごと
  - ✧ 受講生 PC
  - ✧ RX65N 基板：TSIP を備えた MCU である Renesas RX65N を搭載する評価ボード
  - ✧ E2-Lite：USB-JTAG インタフェース、
  - ✧ USB ケーブル×2 (E2-Lite 用、デバッグコンソール用)
  - ✧ JTAG ケーブル（灰色フラットケーブル)
  - ✧ AC アダプター
  - ✧ LAN ケーブル×2 (RX65N 基板用、受講生 PC 用)
- 2 チームごと
  - ✧ サーバ PC（Acer など）
  - ✧ サーバ PC 用 LAN ケーブル
  - ✧ Dumb-Hub：通信の観測に用いる

②演習機器の構成は、下記のとおり。

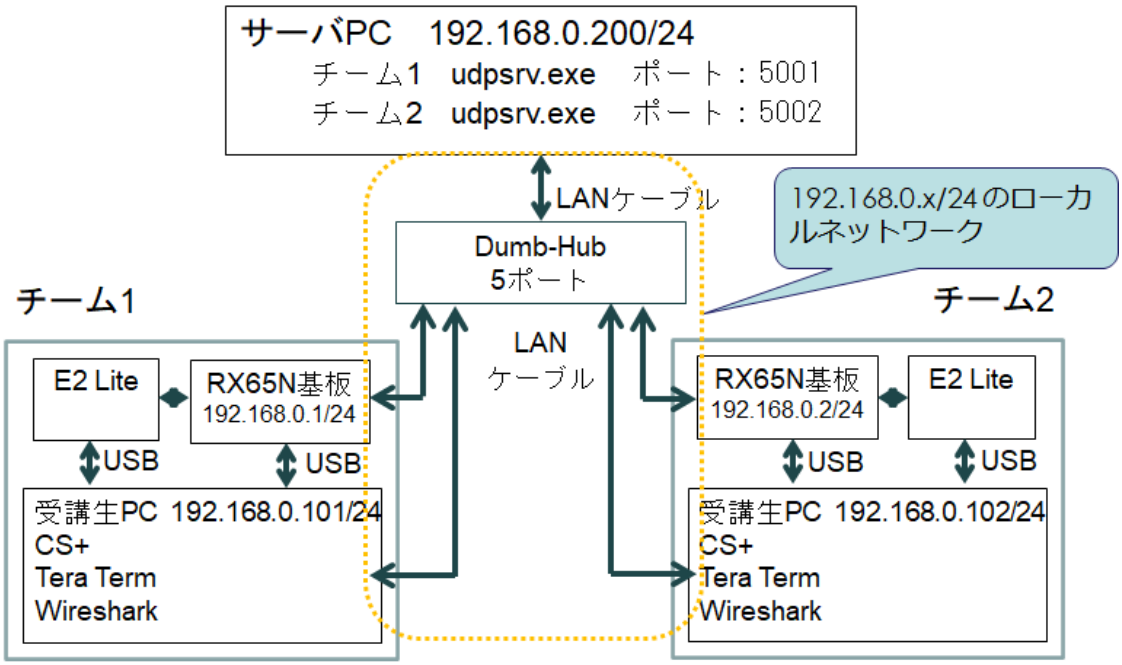

図 1 演習機器の構成（IoT デバイスのセキュリティ機能演習）

(4) 演習で使用するソフトウェア

以下のソフトウェアは IPA から提供する。

① RX65N にダウンロードする通信ファームウェア

- ✧ 3 種類の通信をコマンドで切り替えて実行する。
  - ・ 平文でのデータ通信
  - ・ ソフトウェアでの暗号通信
  - ・ ハードウェア（TSIP）での暗号通信

② IoT デバイス開発環境とソフトウェア

- CS+（体験版のためコンパイルサイズ 128kB まで）
  - ✧ ルネサスエレクトロニクス製の統合開発環境で、RX65N へのファームウェアダウンロードとメモリ読み出しと検索に利用する。
- Wireshark
  - ✧ ネットワーク通信情報を確認できるフリーソフト。本演習ではネットワーク通信情報及びパケット情報の取得に利用する。
- Tera Term
  - ✧ ターミナルソフト。本演習では MCU 上のシェルに対してコマンドを発行して各種設定、実行し、結果を得る。RX65N とは USB 上に実現されるシリアル通信を行う。

2. 脅威分析演習

(1) 演習の概要

脅威分析演習では、具体的なシステムを開発することを想定し、脅威分析(攻撃分析)を体験させる。具体的には、脅威分析､セキュリティ･バイ･デザインの座学で学んだ知識を元に､IoT システムを仮想的に設計するとして､想定される脅威を識別し、リスク評価を行う脅威分析を 3 人程度のグループに分かれて行う。脅威分析の成果はグループごとに発表させる。

対象システムは、スマートホームの IoT システムとし、別途実施する脆弱性検査演習とのつながりを持たせている。脅威分析手法は、座学で講義した脅威モデリングおよびアタックツリー分析を用いる。それぞれの手法の描画ツールとしてフリーの draw.io を用いることを想定している。

グループ演習での脅威分析の成果であるアウトプットは以下を想定している。

- 資産一覧の表（excel）
- ミスユースケース図(draw.io j など）
- DFD（draw.io など）
- アタックツリー（draw.io など）
- リスク評価結果（表など）

(2) 分析対象のシステム

- 疑似スマートホーム
- カメラで家の状況を監視

- スマートリモコンを用いて、家電が操作できる

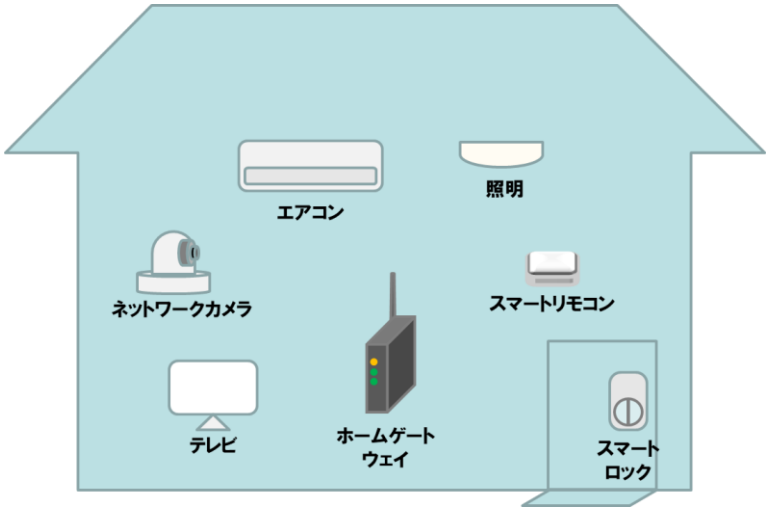

図 2 脅威分析演習の対象システム

3. 脆弱性検査演習

(1) 演習のねらい

本演習では脅威分析演習で分析した脅威が実際に顕在化するか、図 3 に示す疑似スマートホーム環境と脆弱性検査装置を利用して実践する。

受講性は議事スマートホーム内に価値ある資産があると想定して、その資産へたどり着くまでをスマートホーム環境と脆弱背検査装置を用いて以下の 4 点を体験する。各ステップは CTF (Capture The Flag) 形式で進める。

- ホームネットワークを探索して、検査して発見した脆弱性を用いて侵入する（探索－＞検査－＞侵入）
- ホームネットワークに接続された機器を探索して機器を発見する。（探索）
- 機器に対して脆弱性検査を実施して脆弱性を発見する。（検査）
- 脆弱性を用いて機器へ侵入して機器の操作を行う。（侵入）

本演習では図 3 に示す演習進行管理システムを使用することで、各チーム/各受講者の進展をリアルタイムに把握して、きめ細かい演習指導ができる。

- 講師は演習進行管理システム(CTF)を用いて以下の点を実施できる
  - 講師によるオンラインでの課題作成(演習内容の作成)
  - 講師によるオンラインでの課題の提示
  - 受講生によるオンラインでの回答

本演習におけるセキュリティ検証方法について、許可されていないシステムや他人の所有物に対して行うと法律に抵触して罰せられることがある。そのような行為や、実施の是非の判断ができない場合は絶対に実行しないこと。

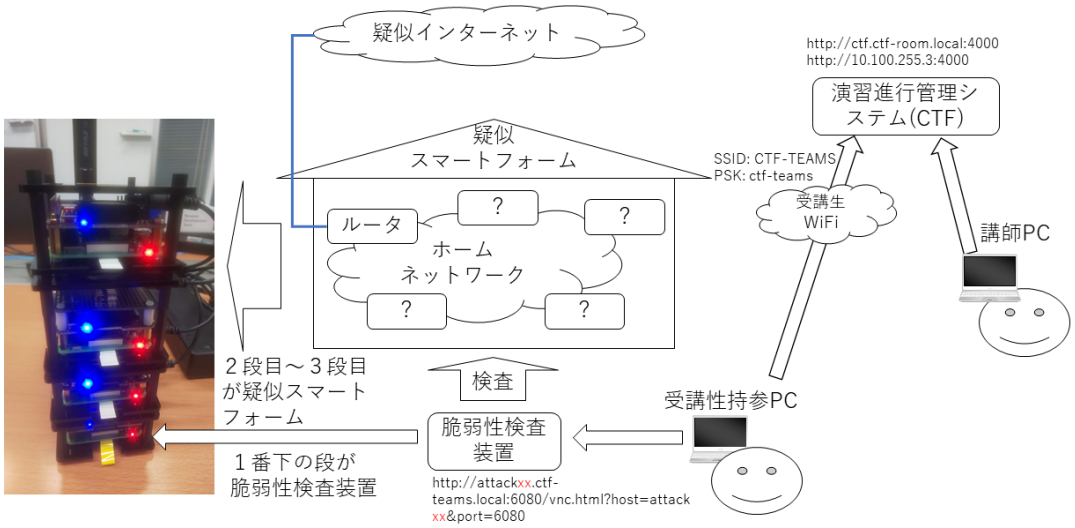

図 3 脆弱性演習環境

(2) シナリオ

2～3 人の受講生が 1 チームを構成する。

各受講生性は演習前に事前学習資料を熟読していることが前提となる。

各チームの検査装置を利用して課題をクリアする。課題の大まかな流れは 1.戦略立案—>2.探索—>3.検査—>4.侵入である。

✧ 戦略立案では、疑似スマートホームに対してどのポイントを探索するか決めて、その手段である検査アプリケーションを選択する。

1.1 CTF 演習 1
1.2 CTF 演習 5
1.3 CTF 演習 9、CTF 演習 10

✧ 探索では、探索アプリケーションを操作して、探索して、検査できそうなネットワークや機器を発見する。

2.1 CTF 演習 2
2.2 CTF 演習 6
2.3 CTF 演習 11(②～④を一つのツールで実施)

✧ 検査では、検査アプリケーションを操作してネットワークや機器に対して検査して、脆弱性を発見する。

3.1 CTF 演習 3
3.2 CTF 演習 7
3.3 CTF 演習 11(②～④を一つのツールで実施)

✧ 侵入では、発見した脆弱性を利用して侵入を試みる。

4.1 CTF 演習 4

4.2　CTF 演習 8
4.3　CTF 演習 11(②～④を一つのツールで実施)
4.4　CTF 演習 12（進みが早い人向け、①～③は特に明示しない）

演習では、①～④を異なる対象（WiFi ネットワークと WiFi ルータ等）に対し 4 回分用意しているが、最低 2 回実践する。

(3) 演習機器

- 教室に 1 セット必要な機材
  - ✧ Raspberry PI x4: ルータ/DNS/DHCP 用、CTF サーバ用、スマートホーム・シミュレータ用、疑似 WiFi 子機用
    - ・ ルータ/DNS/DHCP サーバ：脆弱性演習環境全体の IP 経路を制御、管理する
    - ・ CTF サーバ：受講生への課題、受講生からの回答を管理する
    - ・ スマートホーム・シミュレータ：各チームの電子鍵、エアコン、ライトを管理する
    - ・ 疑似 WiFi 子機用：各チームの WiFi に定期的に情報を流す
  - ✧ WiFi-AP x1
    - ・ 宅内 WiFiSSID、受講生 SSID、疑似インターネット環境用 SSID を管理する
  - ✧ Ethernet Switch
    - ・ Raspberry PI、WiFi-AP を接続する
  - ✧ 講師用 PC(講師持参)

- 各チーム別に必要な機材　—疑似スマートホーム
  - ✧ Raspberry PI x3: ルータ用、監視カメラ用、スマートリモコン用、疑似 WiFi 子機用
  - ✧ スマートリモコン Remo x1

- 各チーム別に必要な機材　—脆弱性検査装置
  - ✧ Raspberry PI x1：脆弱性検査装置
    - ・ Aircrack-ng、OpenVAS、Hydra、nmap、tcpdum が導入済み
  - ✧ 操作 PC(受講生持参 PC)

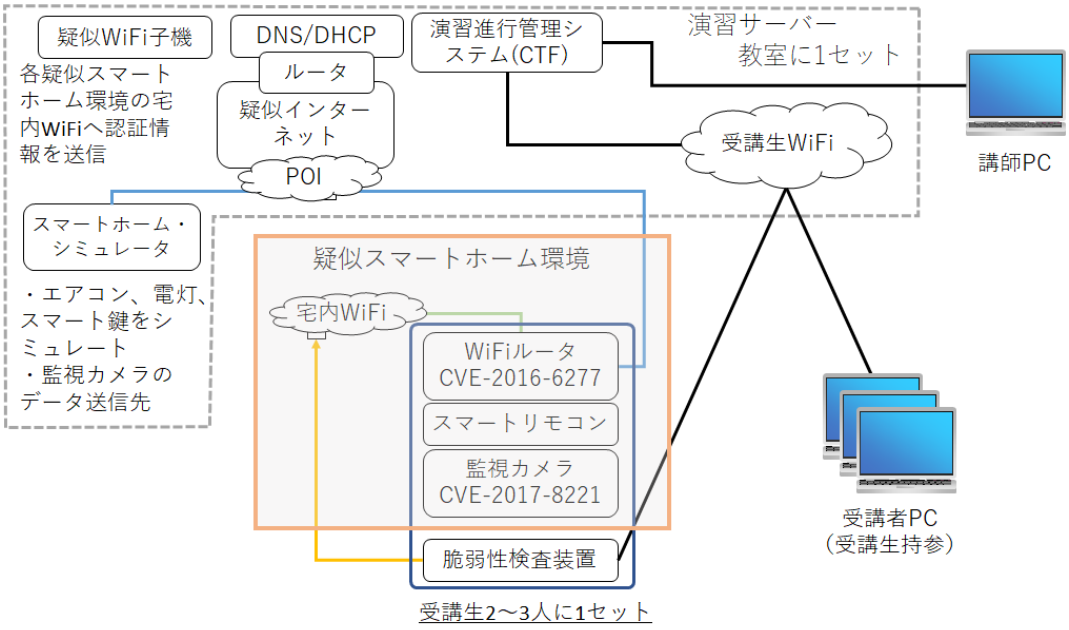

図 4 脆弱性演習機材

(4) IPA が提供するドキュメント・ソフトウェア

- 講師用手順書（講師向け演習シナリオ）
- 講師向け環境動作確認手順書
- 演習シナリオ（受講生向け）
- CTF への演習シナリオ導入手順
- 演習環境構築・環境確認・演習補助・撤収手順書
- 脆弱性演習キット_ホスト変更手順書
- チーム別変更点一覧表
- 脆弱性演習受講生用トラブルシューティング資料
- プログラム設計書
- プログラムソースコード一覧
- プログラムソースコード

① 動作確認用プログラムソースコード

①-1. 演習環境のルーティング情報と各ホストへの接続性を確認するプログラム

①-2. プロキシで許可されたサイトにのみアクセス可能であることを確認するプログラム

①-3. DNS/DDNS/DHCP が動作していることを確認するプログラム

①-4. CTF システムが動作しているか確認するプログラム

①-5. スマートホームエミュレータアプリが動いているか確認するプログラム

①-6. 自動 EAPOL 生成アプリ/自動 Camera アクセスアプリが動いているか確認するプログラム

①-7. 仮想スマートホーム内のルータが動作しているか確認するプログラム

①-8. Remo が動作しているか確認するプログラム
①-9. 仮想スマートホーム内の赤外線受信機が動作しているか確認するプログラム
①-10. 仮想スマートホーム内の監視カメラが動作しているか確認するプログラム
①-11. 受講生が利用する Raspberry PI の OpenVAS が動いているか確認するプログラム
①-12. 受講生が利用する Raspberry PI の nmap/aircrack-ng/tcpdump/hydra/その他ツールが動作可能か確認するプログラム
①-13. 上記すべてを実行するプログラム
② 初期化用プログラムソースコード
②-1. 各検証用 RasPi のホームディレクトリを初期化するプログラム
②-2. 各検証用 RasPi の OpenVAS のデータを初期化するプログラム
②-3. 各検証用 RasPi の Wi-Fi 情報(wlan0)を初期化するプログラム
②-4. スマートホームの状態を初期化するプログラム
②-5. 上記すべてを実行するプログラム
②-6. 設定用ファイル