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

実践的 IoT セキュリティ
シラバス

1. 授業のねらいと到達目標

各種センサーを搭載する小さなデバイスを数多くネットワークすることで、新しいサービスを提供しようとする IoT のセキュリティが懸念されている。本講義では、IoT のビジョンから始めて、IoT デバイスと IoT ネットワークのそれぞれにおけるセキュリティの脅威と対策の方法を学ぶ。特に、一般の PC 系の IT にはない、組み込み・制御・ハードウェアなどのセキュリティの脅威を予測し、安全なシステムやサービスを設計・開発する方法、その安全性を検証し、長期間安全に運用する方法を学ぶ。IoT デバイスを実際に操作して暗号通信を行う演習、スマートホームの模擬環境に対する脅威分析と脆弱性検査の演習によって、IoT セキュリティを体得する。

2. 到達目標

以下を到達目標とする。

- IT 系の情報システムのセキュリティと IoT のセキュリティの違いがわかる
- IoT によって拡大する可能性の高いセキュリティリスクが理解できる
- IoT デバイスや IoT サービスをセキュアに構成するための方向性が理解できる
- IoT システムを運用するときに配慮すべき事項がわかる
- IoT を取り巻く法制度、政府のガイドラインや国際標準が理解できる

3. 授業計画

全 15 コマ（1 コマ 90 分）から成る。第 1 回および演習授業を除く 11 回の授業内で小テストを実施する。

回	テーマ	項目
1	IoT のビジョンと IoT セキュリティ	IoT の特徴、IoT セキュリティの侵害事例、IoT のアーキテクチャ、IoT セキュリティのガイドライン
2	IoT デバイスと実世界インタフェース	組込みシステム、IoT デバイス、組込プロセッサ（MCU)、リアルタイム処理、デバイスインタフェース
3	制御システムセキュリティ	制御とは、センサーとセキュリティ、工場の制御システム、制御系ネットワーク、重要インフラの IoT 化

4	IoT ネットワークとエッジコンピューティング	IoT ネットワークに対する脅威、IoT 無線ネットワーク、IoT 向け通信プロトコル、エッジ（フォグ）コンピューティング
5	ハードウェアセキュリティとセキュアデバイス	IoT のハードウェア攻撃、非侵襲攻撃、侵襲攻撃、半侵襲攻撃、改ざん対策レベルと攻撃難易度
6	IoT デバイスのセキュリティ(演習)	IoT デバイスのデータ保護、暗号鍵、暗号通信、平文通信、なりすまし、TSIP
7	車載エレクトロニクスのセキュリティ	コネクティッドカーの情報セキュリティと攻撃事例、車載 LAN、Black Hat USA、DEFCON
8	IoT の機能安全	機能安全と本質安全、安全分析手法(リスク分析、ハザード分析)、セキュリティとセーフティ
9	セキュリティ・バイ・デザインと脅威分析(1)	セキュリティ・バイ・デザインとは、ソフトウェア開発ライフサイクル、被害分析、ミスユースケース
10	セキュリティ・バイ・デザインと脅威分析(2)	攻撃分析、脅威モデリング、アタックツリー、脅威分析、セキュリティ設計、セキュアプログラミング、検証
11	IoT の脅威分析 (演習)	スマートホームの脅威分析、IoT デバイスの脆弱性検査計画
12	IoT を取り巻く法制度	IoT の法的定義・構造、Internet・of・Things それぞれに関する法、利用者の保護に関する法、課題と展望
13	IoT セキュリティの運用と規格	記録・ログ、セキュリティアップデート、IoT セキュリティ情報の収集と共有、IoT セキュリティの規格・認証
14	IoT の脆弱性検査(演習)	スマートホームの脆弱性検査１
15	IoT の脆弱性検査(演習)	スマートホームの脆弱性検査２

「つながる世界の開発指針」と授業内容との対応

大項目		指針		授業
方針	つながる世界の安全安心に企業として取組む	1	安全安心の基本方針を策定する	①IoT のビジョンと IoT セキュリティ　⑫IoT を取り巻く法制度　⑬IoT セキュリティの運用と規格

		2	安全安心のための体制人材を見直す	(⑬IoT セキュリティの運用と規格)
		3	内部不正やミスに備える	⑫IoT を取り巻く法制度　⑨セキュリティ・バイ・デザインと脅威分析(1)
分析	つながる世界のリスクを認識する	4	守るべきものを特定する	⑧IoT の機能安全　⑩セキュリティ・バイ・デザインと脅威分析(2)
		5	つながることによるリスクを想定する	④IoT ネットワークとエッジコンピューティング　③制御システムセキュリティ　⑦車載エレクトロニクスのセキュリティ
		6	つながりで波及するリスクを想定する	⑨セキュリティ・バイ・デザインと脅威分析(1)
		7	物理的なリスクを認識する	②IoT デバイスと実世界インタフェース　⑦車載エレクトロニクスのセキュリティ　⑤ハードウェアセキュリティとセキュアデバイス
設計	守るべきものを守る設計を考える	8	個々でも全体でも守れる設計をする	①IoT のビジョンと IoT セキュリティ　⑩セキュリティ・バイ・デザインと脅威分析(2)
		9	つながる相手に迷惑をかけない設計をする	⑥IoT デバイスセキュリティ(演習)　⑬IoT セキュリティの運用と規格
		10	安全安心を実現する設計の整合性をとる	⑧IoT の機能安全　⑨セキュリティ・バイ・デザインと脅威分析(1)　⑬IoT セキュリティの運用と規格
		11	不特定の相手とつないでも安全を確保できる設計	⑥IoT デバイスのセキュリティ機能演習　⑬IoT セキュリ

				ティの運用と規格
		12	安全安心を実現する設計の検証、評価を行う	⑭⑮IoT の脆弱性検査(演習) ⑬IoT セキュリティの運用と規格
保守	市場に出た後も守る設計	13	自身がどのような状態かを把握し、記録する機能	⑬IoT セキュリティの運用と規格
		14	時間がたっても安全安心を維持する機能を設ける	③制御システムセキュリティ　⑬IoT セキュリティの運用と規格
運用	関係者と一緒に守る	15	出荷後も IoT リスクを把握し、情報発信する	⑫IoT を取り巻く法制度 ⑬IoT セキュリティの運用と規格
		16	出荷後の関係事業者に守るべきことを伝える	⑬IoT セキュリティの運用と規格
		17	つながるリスクを一般利用者に知らせる	①IoT のビジョンと IoT セキュリティ　⑬IoT セキュリティの運用と規格

4. 教科書（学生が履修するにあたって必携のもの）

授業で表示する講義資料の PDF を事前に提供する。授業および自宅学習で参照すること。

5. 参考書

(1) つながる世界の開発指針　第 2 版　情報処理振興機構
https://www.ipa.go.jp/sec/publish/tn16-002.html

(2) 荻野司、伊藤公祐、小野寺正、「押さえておくべき IoT セキュリティ」、一般社団法人重要生活機器連携セキュリティ協議会編、インプレス、2018

(3) 桑野雅彦、中森章、「ARM マイコン Cortex-M 教科書」、CQ 出版、2016.

(4) 鄭立、「IoT ネットワーク LPWA の基礎 –SIGFOX, LoRa, NB-IoT-」、2017

そのほかの参考書は、授業で示す。

6. 前提となる知識や技術

必要な知識は、授業中でも適宜説明するが、本講義をより深く理解するために、以下に関わる基礎的な知識を備えておくことが望ましい。

- コンピュータ －CPU、メモリ、LSI などのハードウェア要素
- ネットワーク －OSI 参照モデル、プロトコル、TCP/IP、無線 LAN
- オペレーティングシステム －カーネル、プロセス、メモリ保護
- IT セキュリティ －暗号、認証、ファイアウォール、マルウェア、脆弱性
- 情報工学一般 －アルゴリズム、データ型、関数などの概念

第 12 回、13 回で実施する脆弱性検査演習では、Linux PC を操作する。授業の前半で脆弱性検査ツール使用法の説明資料を配付するので、各自で Linux の使い方に習熟しておくことを推奨する。

7. 成績評価の方法

- 単元ごと 5 分間、全 11 回の選択式小テスト、演習の進度、およびレポートにより評価する。
- 欠席して小テストが受けられない場合、レポートによって埋め合わせることができる。レポート課題は、授業中に提示する。
- 講義への積極的な参加で加点する。
- レポートは、定められた期日までに提出しなければならない。

8. 特記事項

- 本授業の第 6 回で実施する「IoT デバイスセキュリティ演習」は、輸出管理の対象となる技術を取り扱うため、日本国の非居住者は受講できない。非居住者とは、日本に引き続いて 6 箇月以上居住していない者を指す。該当者には補講を実施する。