

大学院および社会人を対象にした IoT セキュリティ教育プログラムの開発

松井俊浩¹ 若月里香¹ 大久保隆夫¹

梗概: 大学院の修士学生を対象にした、IoT セキュリティの教育プログラムを開発した。従来の IT セキュリティとは異なって IoT のセキュリティに特徴的な、IoT デバイスにおける暗号鍵の秘匿、デバイスが窃取されることによるハードウェアセキュリティ、制御システムや車載システム、また新しい LPWA など IoT 向きのネットワークのセキュリティ、機能安全との関連させた脅威分析、セキュリティバイデザインなどに焦点を当てている。セキュアデバイスを使った暗号通信、スマートホームの脅威分析と脆弱性検査の演習 4 コマを含む計 15 コマ×90 分の授業を 2 回、また企業向けの 16 コマ集中コースを 1 回実施した。アンケートの結果、学生の関心は高く、学習の効果が確認できた。開発された PPT 教材、演習教材は、本教材開発を委託した IPA から頒布する計画がある。

キーワード : IoT, IoT デバイス, 組込システム, LPWA, スマートホーム, 教材, 演習

Development of IoT Security Education Program for Graduated Schools and Experts

Toshihiro Matsui¹, Rika Wakatsuki¹ and Takao Okubo¹

Abstract: Institute of Information Security has developed an education course for IoT security targeting graduate students and engineers of manufacturing industry. In contrast to traditional IT security for PCs and TCP/IP network, our fifteen-unit IoT security course is programmed to teach securities in embedded systems, composition of the root of trust in IoT devices, hardware security, securities in car electronics and control systems, emerging IoT network security, functional safety, and security-by-design approach. The course also provides four-unit hands-on classes for encrypted communication on secure devices, threat analysis and vulnerability testing for devices and network in a smart home. The course was given twice in regular 15 unit course and 16 unit intensive course for corporate engineers, and evaluated good by the attendees of all classes. In 2020, the course material is planned to be distributed by IPA.

Keywords: IoT, IoT devices, embedded systems, LPWA, smart home, education material, hands-on practices

1. はじめに

2010 年以降、急速に IoT -Internet of Things が普及を始め、総務省等の予測でも、今後の拡大と経済効果が期待されている。しかし、同時に IoT ではこれまで独立していた機器がネットワークに接続されるようになることから、セキュリティ問題が拡大することも予測されている。IPA は、2016 年に名古屋大学の高田広章教授を委員長とする委員会で、IoT セキュリティの問題を議論し、「つながる世界の開発指針」1という冊子として公開した。IT セキュリティの人材不足が指摘されて久しいが、IoT セキュリティについては、さらに人材が乏しいことから、IPA は、「つながる世界の開発指針」を敷衍するべく、2017 年に IoT セキュリティの教育プログラムの開発を情報セキュリティ大学院大学(以下本学)に委託した。本プロジェクトは、約 3 年間で教育カリキュラムと教材を開発し、その後は、IoT セキュリティ教育の実施を開始したい教育機関等にこの教材を無償で頒布して人材育成を強化する狙いがある。本学はすでに教材のほとんどの開発を終え、2 回の正規授業と 1 回の社会人向け集中コースを開講した。その成果を報告する

2. 既存の教育プログラム

インターネットで受講者の募集を行っている IoT セキュリティ関連の講義を調査した。国内では、2 件が見つかった。講義の内容は、1 つは、IoT の適用分野、IoT トポロジ、システムコンポーネント、IoT コミュニケーション、インターネットオペラビリティ、サイバーセキュリティ、ISMS との関連について 6 時間の講義、他は、IoT システムでのセキュリティ適用、業界ごとのセキュリティ技術、ホワイトリスト、SSL/TLS についての半日の講義である。IoT 色は薄い。

海外では、2017 年ころから開講を始めており、2019 年始めの調査では 18 講が見つかった。たとえば、CMU は、「モバイルと IoT セキュリティ」として 20 課の講義を提供しているが、内容はモバイル(スマートフォン)アプリケーションを強調している。University System of Georgia が、オンライン教育システム Coursera を通じて提供している”Cybersecurity and the Internet of Things”は、スマートグリッドやウェアラブルに注目している。Blackhat の 2 日間の講義は、ファームウェア、NFC、bluetooth、マイクロコントローラを講義に含めている。欧州には、IoT ライフサイ

クル～ハードコードされたパスワード～プラットフォームのセキュリティや信頼モデル、またロケーションベースのセキュリティ、サイドチャネル解析などを扱う講義がある。インド(Affity, Bangalore)では、MCUとそのデバイスインターフェースを取り上げた”Offensive IoT Exploitation”という講義がある。その他に、制御システムやSCADA、クラウド、リアルタイムOS、デバッガ、ハードウェアのリバースエンジニアリングなど、広範な項目がIoTセキュリティとして扱われていることがわかった。IoTの重要な特質は、ITのプラットフォームがPCとTCP/IPでほとんど尽くされるのに対し、ハードウェア、ソフトウェア(OS)、ネットワークまたはその組み合わせが多種多様なことである。講義は有料であり、オンラインコースは月に数千円、教室型のコースは、1日当たり5万～10万円で、1～5日間の授業が提供される。

教科書、参考書は、さらに限定的である。我が国では[荻野 司, 2018]が、IoTセキュリティについて論じているが、教科書には向いていない。英語ではIoTのクラッキングを論じた本がいくつかあるが、IoTセキュリティのアーキテクチャ、あるいはMCUを用いた組込みシステムやハードウェアの設計には、別途の本が必要であり、1冊でカバーできる状況はない。

3. 有識者ヒアリング

カリキュラムを検討するに当たって、IoTデバイスベンダーやIoTシステムインテグレータの専門家にヒアリングを行った。以下に聴取したご意見をまとめる。

(1) IoTセキュリティの現状

- 自動車、医療、制御系など業種によって差が大きい。自動車は先行している。
- DEFCON、BlackhatなどでもIoT関係が増えている
- エンドポイントデバイスでは、セキュリティまで手が回っていない。すなわち、組込業界の多くはセキュリティまで手が回らない
- サイドチャネルなど物理攻撃が特に増えているわけではない

(2) 教えるべき事項

- 一般的のITとの違いに注目する。Linuxであれば従来のITとの違いは小さい。
- ハードウェアに近いところ、リバースエンジニアリングも必要。
- 攻撃と防御をセットで教える。IoTの脆弱性検査
- エンドポイントだけでは守り切れない、IoTデバイスとクラウドの接点、すなわちFog層、ゲートウェイでの保護を強調
- 脅威分析、脆弱性検査、運用とマネジメントを強調
- 管理人がいない状況でデバイスが自ら守る設計

- 無線ネットワーク、LPWAは土管なので上位プロトコルでの保護が必要

- IoT向き暗号やセキュアプログラミング

- 個人情報、PL法、認証などの法務と知財

(3) IoTセキュリティ人材像

- セキュリティの全体像を俯瞰できて、システムの実装にも詳しいエンジニア
- 最先端がわかる人、セキュリティ設計できる人

4. 対象とする受講生と前提知識

IoTは、ものに埋め込まれたIT機能であり、ユーザーが操作したり意識することは少なく、また企業の情報システム管理部署が複数なIoTデバイスのすべてを把握することも困難になる。エンタープライズ系のサーバーのソフトウェアには、ソフトウェアとしての免責があるが、ものに組み込まれたファームウェアは分離されず、ものと一体としてPL法で制約される。したがって、IoTのセキュリティを担うのは、ユーザーや運用の専門部署ではなく、IoTシステムの設計者ということになる。本講義は、IoTデバイスを設計・開発する製造業のエンジニアを主な対象とする。

表1 つながる世界の開発指針 (IPA)

Table-1 Guidelines for development in the connected world (Information Processing Agency)

大項目	指針
方針	1 安全安心の基本方針を策定する 2 安全安心のための体制人材を見直す 3 内部不正やミスに備える
分析	4 守るべきものを特定する 5 つながることによるリスクを想定する 6 つながりで波及するリスクを想定する 7 物理的なリスクを認識する
設計	8 個々でも全体でも守れる設計 9 つながる相手に迷惑をかけない設計 10 安全安心を実現する設計の整合をとる 11 不特定の相手とつないでも安全な設計 12 安全安心を実現する設計の検証、評価
保守	13 自身の状態を把握・記録する機能 14 出荷後も安全安心を維持する機能
運用	15 出荷後もIoTリスクを把握・情報発信 16 出荷後の関係事業者が守るべきことを伝える 17 IoTリスクを一般利用者に知らせる

1科目の標準である90分15コマで全くの初心者をIoTの専門家に育てることは困難である。情報工学やセキュリティの基礎知識は習得済みであることを前提とする。情報工学については、コンピュータ、ソフトウェア、オペレーティングシステム、プログラム言語など。ネットワークについては、OSI参照モデル、プロトコル、TCP/IP、HTTP、WiFiなど、セキュリティについては、共通鍵暗号と公開鍵暗号の違い、ハッシュ、機密性・可用性・完全性、各種の認証、脆弱性、セキュリティリスクの種類などである。

これらを基礎知識として、IoTについては、IoTデバイスや組込システムについての知識が必要となるが、これらは前提知識としては要求せず、講義で導入することとした。すなわち、一般的なITセキュリティを知っているが、IoTに特徴的な組込システムについては初心者を対象とする。

5. コースの狙いと構成

IoTにはさまざまな定義があるが、本講では、IDCによる定義、”A network of networks of uniquely identifiable endpoints (or “things”) that communicate without human interaction using IP connectivity.”を中心に据えた。この定義では、ものがTCP/IPを使って世界中につながる、オペレータが関わることのないM2M通信、ネットワークの構成が絶えず変化することの3点が強調される。

また、冒頭で取り上げたつながる世界の開発指針では、表1の17の指針を重要視している。さらに、2節に述べた既設講義が取り上げている項目と3節の有識者の意見を加

味して、表3のような15コマの授業に配置して解説する。ITセキュリティの基礎知識は前提として、組込系、ハードウェアのセキュリティ、信頼の基点、新しいIoTネットワークなどに力点を置き、IoTセキュリティと関連の深い車載と制御システムのセキュリティについても取り入れる。また設計段階でのセキュリティ設計が重要であることから、機能安全から脅威分析を通じてセキュリティ・バイ・デザインを教える。技術だけではなく、関連する法制度や国際標準と認証制度についても講義する。

6. IoTセキュリティの特徴

これまでに一般的なITセキュリティを学んだ学生が、IoTセキュリティインシデントとして最初に学ぶのは、MIRAIマルウェアであろう。MIRAIマルウェアは、デフォルトパスワードで大量の組込システムを乗っ取り、bot化して大規模なDDoS攻撃を起こしたが、telnetにroot+デフォルトパスワードでログインできたという原因を知ったら、なんてばかばかしいと幻滅するかもしれない。しっかりとパスワードを付けることは重要であるが、そこで終わつたのでは、IoTセキュリティの本質に到達できない。

IoTセキュリティに重要な事項は、表2の17項目の指針の通りであるが、本講座では、特に次の2点に力を入れている。1つは、IoTデバイスのハードウェアに信頼の基点(root of trust)を築くことである。MIRAIに置き換えて考えると、しっかりとパスワードを使うとしても、それをデバイス中に安易に保存するだけでは、簡単に漏洩する可能性がある。そのわけは、通常のPC等は、機器をオ

表2 実践的IoTセキュリティ授業のカリキュラム table-2 Curriculum of the Practical IoT Security

回	テーマ	項目
1	IoTのビジョンとIoTセキュリティ	IoTの5層アーキテクチャ、インシデント例、エントリポイント、ITとIoT
2	IoTデバイスと実世界インターフェース	IoTデバイス、組込プロセッサ(MCU)、ARMアーキテクチャ、RTOS、デバッグポート
3	制御システムセキュリティ	制御系、フィールドバス、PLC、SCADA、stuxnet、ホワイトリスト制御
4	IoTネットワークとFogコンピューティング	Bluetooth-LE、blueborne、Wi-Fi、LPWA、フォグコンピューティング
5	車載エレクトロニクスセキュリティ	車載ネットワーク、テレマティクス、ITS、ECU、OBD-2
6	ハードウェアセキュリティとセキュアデバイス	サイドチャネル、侵襲攻撃、信頼の基点、TPM、Trustzone、TSIP
7	IoTセキュアデバイス(演習)	組込システム開発、暗号鍵の保護、MCUのセキュリティ機能、暗号通信
8	IoTの機能安全	機能安全規格、FTA、FMEA、リスク分析、ハザード分析、STAMP、HAZOP
9	IoTの脅威分析	STRIDE、アタックツリー、脅威モデル、CVSS
10	IoTのセキュリティ・バイ・デザイン	セキュリティ開発ライフサイクル、要求分析、セキュリティ設計
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の脆弱性検査(演習)	スマートホーム、Wi-Fiルータ、スマートスピーカーの脆弱性検査
13	IoTの脆弱性検査(演習)	スマートホーム、ショッピングボタンの脆弱性検査
14	IoTを取り巻く法制度	プライバシ、PL法、NICT法、ガイドライン
15	IoTセキュリティの運用と規格・認証	ログ、アップデート、情報共有、CSMS、JTC-1 SC41、CCとEDSA認証、PSIRT

フィス内あるいはサーバーであればデータセンター内に物理的セキュリティを保つて設置することができるが、IoTデバイスは、駐車場のような公共の場所にぞんざいに、長期間置かれる可能性が高いので、物理的に窃取されて、メモリをのぞき見られるからである。

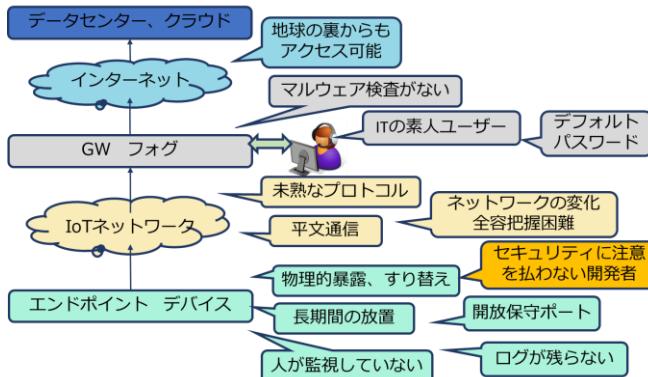


図 1 強調すべき IoT セキュリティの弱点

Figure-1 Security Weak points in IoT

もう一点は、IoT セキュリティの脅威は、パスワードのような保護情報を除くと、情報の漏洩よりも、安全性や可用性への脅威となりやすいことである。PC に慣れた頭では、情報の保護を重要視しやすいが、IoTにおいては、機器の動作を止められることで生産性が落ちるだけでなく、安全機能がストップして人命に関わるような事故につながりかねない。授業では、そのような安全に関わる脅威を予測することをまず教える。IT では、ファイアウォールや IDS のような後付けのセキュリティ対策も有効であるが、IoT では、ユーザーがセキュリティ知識を持っていることはあまり期待できないので、設計時からセキュリティリスクに備えるセキュリティ・バイ・デザインが重要となる。

7. 授業の実施と演習

2017 年度に試行的に授業を行った後、2018 年から実践的 IoT セキュリティを正規授業として実施した。また、2019 年 6 月には、一般の社会人の専門家を対象に集中コースを開学した。前者では 1 クラス約 20 名、後者では 6 名の受講生を迎えた。実践的 IoT セキュリティの授業は、表のような内容で、90 分を 1 限として、10 月から 2 月までの 15 限の授業を実施した。

各授業では、前回の授業の内容を 5 分程度の小テストを課した。学生の評価と授業の効果測定に用いる

学習効果を高めるため、講義には、3 種類の演習(ハンズオン)を取り入れた。演習(ハンズオン)を取り入れると学習効果が上がることはわかっているが、進度が遅くなる、準備にコストがかかるなどの負担があるので、3 種類、4 コマとした。演習の題材は、前節で述べた 2 つの重要課題に備えるものとした。

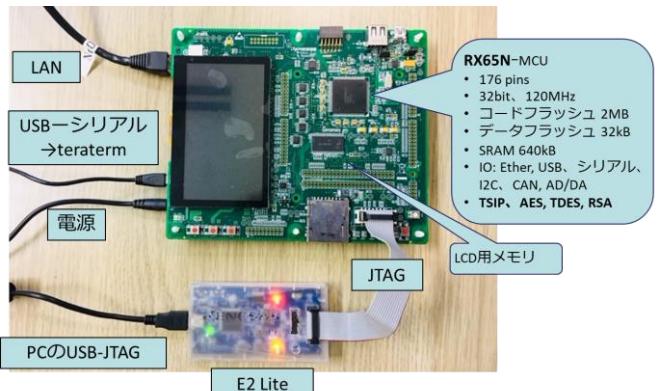
(1) セキュアデバイス演習

IoT デバイスとは、ネットワーク機能を備える組込システムである。IoT デバイスは、人間が介在しない M2M 通信を行うので、人間の記憶に頼ったパスワードが使えず、機器内にパスワードに相当する認証情報あるいは暗号鍵を秘匿しておく必要がある。IoT デバイスの中心には、CPU と不揮発メモリ、入出力インターフェースをワンチップに集積した MCU(マイクロコントローラ、マイコン)が使われる。IoT デバイスに鍵を秘匿して暗号通信を行う演習を実施した。実習機材には、セキュアに暗号鍵を秘匿する機能を持つ RX65N(ルネサスエレクトロニクス社製)を搭載する評価ボードを用いる。

MCU とその開発環境 (CS+) を使ってまず、サーバーと平文通信をし、通信文が簡単に漏洩することを確かめる。次にソフトウェアによる暗号通信を行う。通信の盗聴では暗号文の安全性が保たれるが、IoT デバイス(評価ボード)が攻撃者の手に渡ると、暗号鍵が露見しうる。RX65N に組み込まれたセキュアデバイス機能を用いた場合はどうなるかを調査する。

図 2 暗号通信実験を行うセキュア MCU の評価ボード

Figure-2 Evaluation board of secure MCU for encrypted communication experiment



(2) IoT 脅威分析演習

IoT は、市場展開後のセキュリティ対策が難しいので、設計時にセキュリティを吟味しておくべきである。本講義では、IoT が対象に物理的な操作を加えるために物理的な安全性が重要なことをまず教える。安全について、機能安全の考え方と、安全とセキュリティが相互に影響しあうことを学ぶ。セキュリティの問題がどのような安全問題(リスク)に発展するかを全方位で予想することが重要となる。安全性とセキュリティの重篤度の評価手法や、要求仕様を作成すること、要求仕様に基づいて設計を行うことを教えている。この IoT 脅威分析演習では、家電がスマートスピーカやスマートリモコンで制御される図のようなスマートホームを想定して、そのセキュリティリスクを探し出す課題にチームで取り組む。

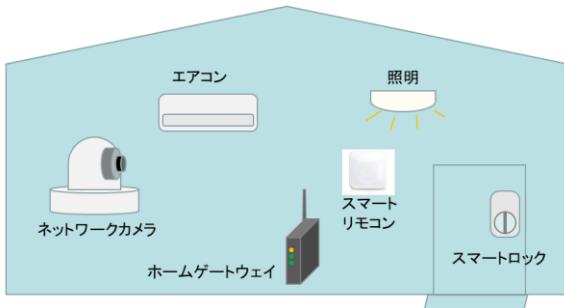


図 3 演習で用いるスマートホームモデル

Figure-2 Model of a smart home studied in the hands-on practice

(3) スマートホームの脆弱性検査演習

前記のスマートホームをシミュレーションする環境をチームで共有し、そこに潜む脆弱性を検出する演習を行う。脆弱性が安定して再現するよう、ホームゲートウェイ、ネットワークカメラは、Raspberry Pi で構成し、実際に過去に発見された脆弱性を仕込んでおく。その他の家電は、シミュレータで実現し、スマートリモコンを通じてオン・オフ制御ができるようになっている。このスマートホームに対して、nmap, aircrack-ng, open-vas などのオープンソースの脆弱性検査ツールを用いて検査を演習する。本演習の開発には、CCDS に多大なご協力を頂いた。

8. 受講者アンケート

受講生には、一連の授業の受講前と受講後に、アンケートに回答してもらった。各コマの授業のキーワードを挙げて、どのくらい理解してていいかを自己評価 5段階で答えてもらっている。正規授業である「実践的 IoT セキュリティ」では、受講前アンケートにおいて授業を受ける理由を、受講後アンケートにおいて受講後の感想を自由記入で記入してもらっている。また、受講後には、授業の評価を 5段階で答えてもらっている。以下にその結果を示す。

(1) 受講前：実践的 IoT セキュリティの授業を受ける理由

- これから重要性が増す、新しい分野である
- 他に IoT セキュリティを勉強できる場がない
- IoT に関するセキュリティ問題が深刻になる可能性がある
- ハードウェアや組込系のセキュリティの見識を深めたい
- IoT セキュリティの法制度を研究したいが、その前提知識として技術も習得しておきたい。社会学系の学生にも理解できる授業を期待する。
- 自身の研究分野との関連が深い。
- 開発の業務内容に直結できそうだ。

(2) 受講後の感想

- 全般にわたり大変勉強になる内容で、業務に活かせる

- 研究において非ネットワーク機器の IoT 化をテーマとしているため、非常に有意義な講義でした。特に Root of Trust に基づいた IoT システムの構築は参考にしたいと思っています。
- 内容が非常に盛り沢山で短期間に吸収するのが大変だったが、非常に役に立った。今後、技術が詳細化していくでしょうが、現時点では俯瞰的にものを理解できて非常に良かった。
- 脅威分析の内容と演習は、これまで体験したことがなかったので、特に非常に有益だった。

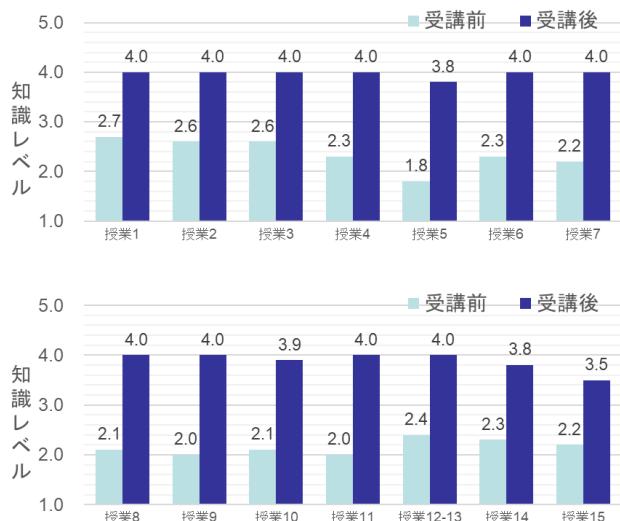


図 4 授業の受講前後の理解度の変化

Figure-3 Changes of the comprehension level before and after the classes

- カリキュラムが盛りだくさんであり、履修してよかったですと心から思える講座だった。来年度の後輩にも履修を勧めたい講座です。スマートホームのハッキング演習が非常に楽しく興味深い内容でした。
- 制御セキュリティ、リスク分析など、自身の研究に活用できる。IoT デバイスの数が多いことによる影響、問題などもカバーされるとよい。また、IFTTT などのクラウドサービスとの連携の実験は面白い。

(3) 改善要望など

- 講義と演習が交互にあると良い。
- 演習において実際にチップに線をつないで読み取るものがあるとより面白いと思った。
- 脅威分析の手順の理解が難しかったので、手順のまとめ講義が欲しい。
- 講義については、毎回小テストを課せられていたので、きちんと復習するペースをつかめて良かった。演習については、事前に演習で必要になる知識やツールを解説してほしかった。初心者には取りつきにくい
- 演習はもっと時間をかけたい。小テストについては復習の励みになり良いと思いました。

- 授業時間に対して資料の分量が多く、時間の都合で省略されたのが残念でした。

9. 授業の効果と評価

表3に数値化した授業の効果の他の集中コースとの比較を示す。実践的IoTセキュリティの正規授業に比べると、社会人向け集中コースの効果が低かった。社会人受講者は、組込みシステムの専門家も交じっており、受講前の知識レベルが高かったことが理由の一つに挙げられる。予復習をする時間がなく、集中的に行う授業の限界も示している。

表3 授業前後の理解度の変化の他授業との比較

Figure-3 Changes of comprehension levels compared with other classes

講義名	受講前	受講後	ゲイン
実践的IoTセキュリティ 2018年度後期 正規授業	2.4	4.0	1.6
(参考) IoTセキュリティ-1 組込システムの基礎 2019年度集中コース	3.0	4.3	1.3
IoTセキュリティ-2 アーキテクチャ 2019年度集中コース	3.0	3.7	0.7
IoTセキュリティ-3 脅威分析、脆弱性検査 2019年度集中コース	2.7	3.7	1.0
CT-1 CSIRT構築入門 2019年度集中コース	2.9	3.8	0.9
CT-2 ネットワークセキュリティ技術演習 2019年度集中コース	2.8	4.0	1.2
CT-3 Webアプリケーション検査演習 2019年度集中コース	2.5	4.5	2.0

表4に受講生による授業の評価を示す。ここでも、正規コースでの満足度の高さに比して、集中コースの限界が示されている。社会人の受講生は、内容としてより高度な授業を求めているとも言える。

表4 受講生による授業の評価

「実践的IoTセキュリティ（正規授業）」レベル別回答数と平均、回答数21

	1	2	3	4	5	平均
内容のレベル	0	0	15	6	0	3.3
教員の講義の仕方	0	0	5	5	11	4.3
講義の総合評価	0	0	0	0	21	5.0

「IoTアーキテクチャー社会人向け集中コース」回答数

	1	2	3	4	5	平均
内容のレベル	0	1	5	0	0	2.8
教員の講義の仕方	0	0	2	3	1	3.8
講義の総合評価	0	0	1	5	0	3.8

「IoTの脅威分析と脆弱性検査－社会人向け集中コース」

	1	2	3	4	5	平均
内容のレベル	0	0	4	1	0	3.2
教員の講義の仕方	0	0	4	0	1	3.4
講義の総合評価	0	0	3	2	1	3.7

10. 教材の頒布

本コースの教材は、他機関で教育に使用できることを念頭において作成した。計1000ページほどのパワポインツライドで作成している。演習機材は、組込デバイス評価ボードやRaspberry Pi等をチーム数分そろえる必要がある。脆弱性検査演習については、CTF形式で課題、ヒント、回答をガイドするWebサイトを構築して頂く。

この他に、典型的な授業を一通りビデオプログラムとして編集してあるので、講師が教え方を学習することにお使い頂ける。教材の一切は、2020年度以降、IPAから提供される予定である。詳細は、IPA社会基盤センター産業プラットフォーム部、小沢理康氏、t-ozawa@ipa.go.jpに問い合わせたい。

11. まとめ

従来、セキュリティに関心の高い業界は、金融や情報通信系、総じて重要インフラ系であったが、組込システムを開発する製造業や、IoTのユーザーとなる重要インフラ系企業の関心も高まっているのに対し、IoTセキュリティ教育の教材や授業が整っていなかった。本学は、IoTセキュリティの大学院レベルの教育用教材と演習を開発し、実際に授業を実施することで、その有効性と受講生の満足度を図ることができた。

IoTは、非常に広範なので、半期の授業では全体を俯瞰するレベルに留まるが、ITとIoTの違いを理解してもらうことができた。受講者の受講後の満足度は、高く、特に演習で理解を深めてもらうことができた。事前に、ITセキュリティと組込システムの両方の基礎が必要である。さらに実践的なIoTセキュリティには、業界・分野ごとに専門講座が必要となる。

参考文献

- 高田広章,他.(2016). つながる世界の開発指針~安全安心なIoTの実現に向けて開発者に認識してほしい重要ポイント~. 情報処理振興機構ソフトウェア高信頼化センター
- 荻野司公祐,小野寺正,一般社団法人重要生活機器連携セキュリティ協議会伊藤.(2018). 企業リスクを避ける押さえておくべきIoTセキュリティ～脅威・規制・技術を読み解く！～. インプレス