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，デバイスの窃取に対抗す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，また社会人向けの 16 コマ×90 分の集中コースを 1 回実施した．アンケートの結果，受講者の関心は高く，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 Graduate Schools and IT Experts

Toshihiro Matsui[1,*], Rika Wakatsuki[1] and Takao Okubo[1]

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 networks, 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計画がある．2019 年ま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

受講者の募集を行っている IoT セキュリティ関連の教育プログラムをインターネットで調査した．国内では，2 件が見つかった．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 年ころから開講され始めており，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 日間のハンズオンコースは，ファームウェア，NFC，Bluetooth，マイクロコントローラを対象に含めている．欧州には，IoT

1 情報セキュリティ大学院大学　Institute of Information Security　*matsui@iisec.ac.jp

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．我が国では荻野らが, IoT セキュリティに関する最初の書籍を著した[2]．タイトルの通り企業にとって実務的な内容になっている．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にはない．

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. 対象とする受講者と前提知識

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雑多な 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．本授業は, IoT デバイスや IoT サービスを設計・開発するエンジニアを主な対象とし、IoT サービスの運用者を含める（図 1）．

1 科目の標準である 1 コマ 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，Wi-Fi 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．

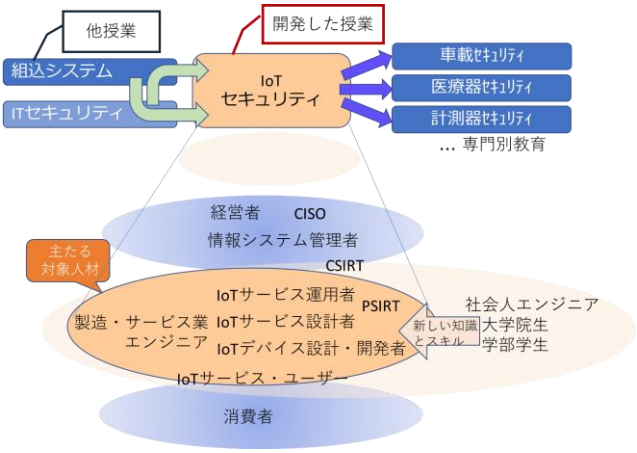

図 1　対象とする学生の専門領域と職域

Figure-1 Expertise and scope of targeted students

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. 授業の狙いと構成

IoT にはさまざまな定義があるが，本授業では，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．

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 2 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すでに習得していることを前提として，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．

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	つながる世界の安全安心に組織的取り組む	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	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
		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	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
		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	市場に出た後も守る設計を考える	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	関係者と一緒に守る	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

表 2　2018 年度「実践的 IoT セキュリティ」授業カリキュラム
Table-2 Curriculum of the Practical IoT Security, 2018

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 ｺﾝﾋﾟｭｰﾃｨﾝｸﾞ	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，アッタクツリー，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

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．しっかりしたパスワードを付けることは重要であるが，そこで終わったのでは，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 1 の 17 項目の指針の通りであるが，本授業では，最初の授業で，図 2 のような 5 層の IoT アーキテクチャの中で，IoT らしい問題が何であるかを示している．さらに，次の 2 点に力を入れて教える．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，しっかりとした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，機器をオフィス内に，あるいはサーバであればデータセンタ内に物理的セキュリティを保っ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，長期間置かれることも多く，物理的に窃取されて，メモリをのぞき見られる可能性が高くなるからである．

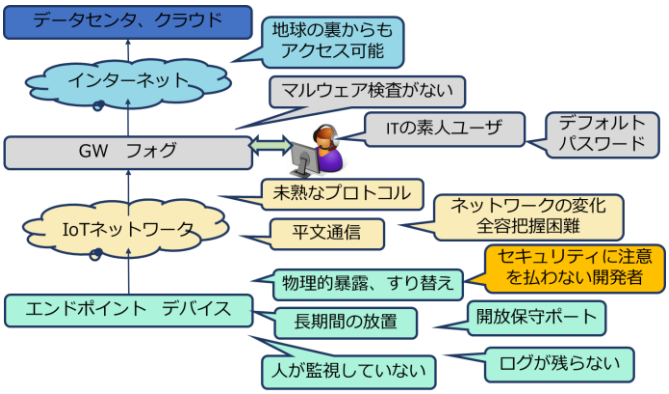

図 2　強調すべき IoT セキュリティの弱点
Figure-2 Security Weak points in IoT

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．この 2 点については，ハンズオン演習も加えて強調する．

6.　授業の実施と演習

2017 年度に試行的に授業を行った後，2018 年度から「実践的 IoT セキュリティ」を正規授業として実施した．実施時期は，2 学期制の後期である．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講した．前者の受講者は本学学生 21 名，主に NW 系企業や官公庁に所属する社会人学生および学部卒で入学した修士 1 年生であった．後者の受講者は 6 名，所属先は，主に電機系企業，IT 系企業であった．「実践的 IoT セキュリティ」の授業は，表 2 のような内容で，90 分を 1 コマとして，10 月から 2 月までの 15 コマの授業を実施した．

各授業では，前回の授業内容について，5 分程度の小テストを課した．この小テストは，受講者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もあるので，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 デバイスの中心には，CPU と不揮発メモリ，入出力インタ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．この秘匿の重要性への理解を深めるため，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

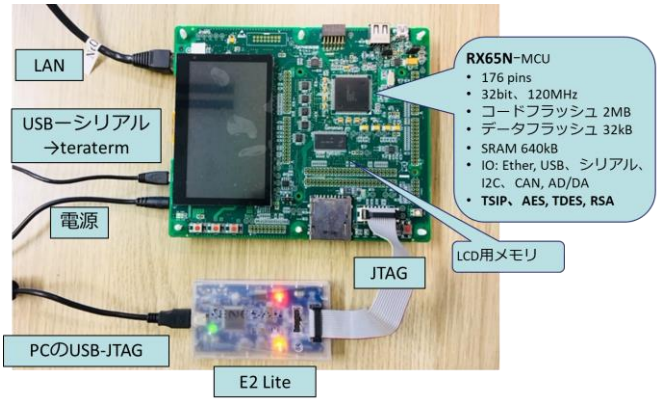

図 3　暗号通信実験を行うセキュア MCU の評価ボード
Figure-3 Evaluation board of secure MCU for encrypted communication experiment

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（図 3）.

まず, IoT デバイス（評価ボード）とその開発環境（CS+）を使って，サーバと平文通信をし，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．最後に，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．

(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イを吟味しておくべきである．本授業では，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になることをまず教える．安全については，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 4 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.

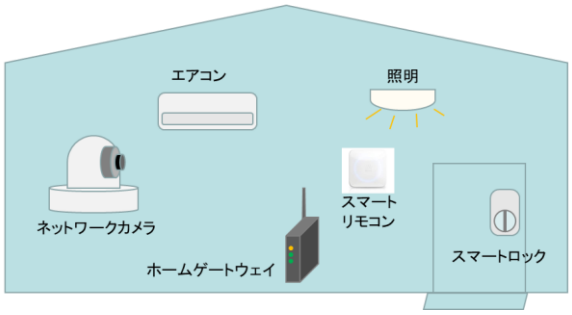

図 4　演習で用いるスマートホームモデル

Figure-4 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いる．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，OpenVAS 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．本演習の開発と実施には，CCDS に多大なご協力を頂いた.

7. 受講者アンケート

受講者には，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．まず，受講前には，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いるかを自己評価 5 段階で答えてもらう．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．文章の表現は、簡単化している。

(1) 受講前：「実践的 IoT セキュリティ」の受講理由

- 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：「実践的 IoT セキュリティ」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．
- カリキュラムが盛りだくさんであり，履修してよかった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．

8. 授業の効果と評価

図 5 に「実践的 IoT セキュリティ」受講前後の項目別理解度の変化を，表 3 に数値化した授業の効果の他授業との比較を示す．「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．集中コースの社会人受講者には，組込システムの専門家もおり，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．集中コースは，話題を関連づけてどんどん吸収できる利点があるが，予復習をする時間がとれないので，何か不明な点が生じた場合は，挽回する間もなく先に進んでしまうことも理由であろう．

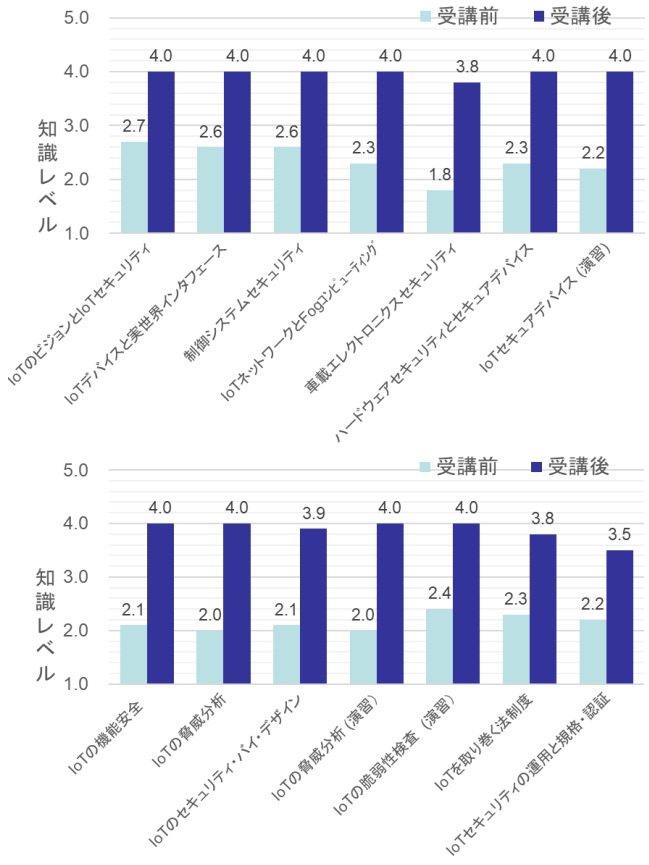

図 5 2018 年度「実践的 IoT セキュリティ」受講前後の理解度の変化

Figure-5 Changes of the comprehension level before and after the classes, 2018

表 4 に受講者による授業の評価を示す．ここでも，正規授業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．集中コースの社会人受講者は，内容としてより高度な授業を求めているとも言える．

表 3 授業前後の理解度の変化の他授業との比較

Table-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
2018年度後期 本学正規授業平均	2.4	3.9	1.5
(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 受講者による授業の評価 レベル別回答数と平均

Table-4

正規授業「実践的 IoT セキュリティ」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

社会人向け集中コース「IoT アーキテクチャ」回答数 6

	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

社会人向け集中コース「IoT の脅威分析と脆弱性検査」回答数 6

	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

9. 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 ページほどのパワーポイントス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 サイトを構築している．すでに教材と演習の骨格は定まったので，特に演習を他機関で実施しやすくする検討を加えている．

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 に問い合わされたい．

10. 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，IoT の普及にともない，組込システムを開発する製造業や，IoT のユーザとなる重要インフラ系企業のセキュリティへの関心も高まっている．一方，IoT セキュリティ教育の教材や授業は整っていなかった．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，その有効性と受講者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．IoT は，未だに標準的なアーキテクチャがそろっていないので，さらに実践的な IoT セキュリティには，業界・分野ごとに実態に即した専門講座が必要となる．また，IoT 製品が市場に出て行くにしたがって，運用段階の IoT セキュリティの比重が高まり，PSIRT の活動が重要になると予測される．

参考文献

[1] 高田広章，他：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（2016）

[2] 荻野司，小野寺正，伊藤公祐，一般社団法人重要生活機器連携セキュリティ協議会（編）：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（2018）